Q U B I C

Die lange Version

Qubic Church · 2026

Das Buch ist kostenlos.
Wird frei verteilt.

qubic.church

Inhaltsverzeichnis

Teil I. Das Problem

Kap. 1 — Murdochs Gas

Kap. 2 — Axelrods Turnier

Kap. 3 — Warum Bitcoin sich nicht selbst reparieren kann

Teil II. Der Mann

Kap. 4 — Come-from-Beyond vor Bitcoin

Kap. 5 — Drei Projekte, drei Metamorphosen

Teil III. Die Mechanik

Kap. 6 — 676 Stimmen

Kap. 7 — Wochen aus Epochen

Kap. 8 — Murdochs Gas in Aktion — UPoW

Kap. 9 — Der atmende Token

Kap. 10 — Der Arbitrator — ein Monarch auf Zeit

Teil IV. Aigarth

Kap. 11 — Was Aigarth ist

Kap. 12 — Was schon erledigt ist

Kap. 13 — Anna Matrix

Kap. 14 — Was das Deployment am 13. April 2027 bedeutet

Teil V. Der Beweis

Kap. 15 — Der Krieg, den niemand führte

Kap. 16 — Was Qubic nicht tat

Kap. 17 — Qubic Church und fraktaler Rationalismus

Teil VI. Das Finale

Kap. 18 — Das neue Gold

Vorwort

„Qubic ist zum Erfolg verdammt. Aigarth? Hängt von den Minern ab.“ — Come-from-Beyond, 7. Februar 2026

Die Geschichte von Qubic beginnt lange vor Bitcoin und umfasst viele lebendige Etappen. Den Weg zu untersuchen, den der Visionär Come-from-Beyond unter seinen eigenen Füßen anlegt, ist wirklich interessant.

Mein Vater hat viel Zeit damit verbracht, sich mit diesem Thema zu beschäftigen, und da er ein Meister der Religionswissenschaft ist, betrachtete er Qubic in einem etwas größeren Maßstab, als es sonst üblich ist.

Die größte Herausforderung für den gewöhnlichen Menschen, der sich heute für Qubic interessiert, besteht darin, den Maßstab, die Struktur, die Funktionen und die Bedeutung jedes Details eines großen Mechanismus zu erfassen. Glauben Sie mir, das ist ein ganzes Universum mit einer reichen Geschichte und vielen Geheimnissen, die wir mit der Zeit noch aufdecken werden. Come-from-Beyond malt, wie ein antiker Künstler, ein großes Bild. Elemente, die zunächst unverbunden erscheinen, beginnen nach und nach zu verschmelzen und Gestalt anzunehmen.

Dieses Buch tut eine einfache Sache: Es sammelt, was verstreut war, zu einem einzigen Fresko, ordnet es und stellt es in einfacher Sprache dar.

Wer sollte dieses Buch lesen? Jeder, der auch nur ein wenig mit Qubic verbunden ist, wird hier etwas für sich finden. Ein Neuling lernt die Grundprinzipien der Funktionsweise kennen und erkennt Zusammenhänge, die er zuvor nicht sah. Ein erfahrener Holder kann die Geschichte und die schönen Allegorien genießen, von denen die Rede meines Vaters so reich ist. Der Profi und der Meister können sich das Gesamtbild von außen ansehen und vielleicht etwas entdecken, das sie bisher übersehen haben.

Alle Cfb-Zitate in diesem Buch sind wortgetreu aus offenen Primärquellen entnommen — dem offiziellen Qubic-Discord, seinen Veröffentlichungen auf X, den wissenschaftlichen Papers des Teams. Alle sind in unserem Buch enthalten. Wenn Sie eine Ungenauigkeit entdecken — schreiben Sie uns. Das Buch lebt; die nächste Auflage wird Korrekturen aufnehmen. Ein Hinweis sei erlaubt: Der Stil von Come-from-Beyond ist eine wilde Motorradfahrt querfeldein. Im Qubic-Universum findet man Informationen selten strukturiert aufbereitet. Deshalb glauben wir, dass dieses Buch eine willkommene Ergänzung für die Bibliothek jedes Qubic-Holders sein wird. Das Buch wird vollkommen kostenlos verteilt. Der beste Dank an uns wäre Ihre Wertschätzung, Ihre Kritik, Ihre Anmerkungen. Sollten Sie aus einem besonderen, nicht zu bändigenden Drang heraus für das Buch bezahlen wollen — können Sie freiwillig den Spenden-Button auf der Website qubic.church nutzen oder unsere Qubic-Wallet: BDRFCOFWHRTEHHMQQUIYJBXEOLNARADAGFUSBFGJFABYZBZLQNWJIPPFRTXO

Das Buch wurde ursprünglich auf Russisch geschrieben, wurde aber der Einfachheit halber ins Englische übersetzt.

Danke, Vater. Dein Beitrag ist unbezahlbar.

TEIL I

Das Problem

1
Murdochs Gas

Nützlicher Abfall.

Es gibt eine Art von Ding, die man eines Tages sehen lernt – und sich danach fragt, wie man es vorher übersehen konnte. Eines dieser Dinge ist der Unterschied zwischen der Arbeit und ihrem Abfall.

Nehmen wir einen beliebigen Ofen. In seinem Inneren brennt etwas, etwas wird erhitzt, und das gewünschte Produkt kommt heraus. Doch neben dem Produkt bleibt immer noch etwas anderes übrig. Rauch. Dampf. Geruch. Lärm. Wärme, die in die Wände entweicht. Jahrhundertelang behandelten die Menschen diese Überreste als Müll – den unvermeidlichen Begleiter nützlicher Arbeit, etwas, das irgendwie entsorgt oder einfach in die Luft entlassen werden musste.

Manchmal kommt ein Mensch daher, der diesen Müll aufmerksamer betrachtet als alle anderen. Und stellt eine merkwürdige Frage: Was, wenn wir ihn nicht entlassen?

Dieses ganze Buch handelt von einer Frage dieser Art, gestellt in Bezug auf eine ganz bestimmte Art von Müll. Doch um zu verstehen, warum diese Frage wichtig ist, müssen wir zunächst zwei alte Geschichten erzählen – über Kohle, und über den Mann, der herausfand, wie man mit ihr Städte beleuchtet.

Beide spielten sich in England ab.

1709. Coalbrookdale

Im Westen Englands, in der Grafschaft Shropshire, liegt ein Tal, durch dessen Grund der Fluss Severn fließt. Der Ort ist grün, hügelig, nicht besonders bemerkenswert. Zu Beginn des achtzehnten Jahrhunderts zog dorthin ein Mann namens Abraham Darby – er war zweiunddreißig Jahre alt, Quäker, und hatte bereits eine beachtliche industrielle Laufbahn hinter sich.

Quäker – das ist ein wichtiges Detail, auch wenn es auf den ersten Blick nicht das auffälligste ist. Die Gesellschaft der „Freunde“ (wie sich die Quäker selbst nannten) war im England jener Zeit eine Gemeinschaft, deren Mitglieder keine militärischen Uniformen trugen, vor Gericht keine Eide schworen, protzigen Luxus mieden und Ehrlichkeit in ihren Geschäften sehr ernst nahmen. Quäker-Handwerkerdynastien waren dafür bekannt, dass ihre Waren nicht gefälscht und ihre Preise nicht überhöht waren. Darby gehörte einer solchen Dynastie an – und wuchs in einer Ethik auf, in der Ansehen mehr wert war als der Profit des Augenblicks. Dieses Detail lohnt sich zu merken: Wir kommen darauf zurück, wenn wir über Bitcoin sprechen.

Darby hatte ein Problem, das damals der gesamten englischen Metallurgie gemein war. Gusseisen wurde mit Holzkohle geschmolzen – speziell verkohltem Holz, das heißer brennt als gewöhnliches Feuerholz. Doch bis 1700 hatte England den Großteil seiner Wälder abgeholzt. Holzkohle wurde teurer, es gab immer weniger davon, und eine Gießerei nach der anderen musste schließen. Ein Land, das für alles – vom Pflug bis zur Kanone – von Eisen abhing, sah sich mit dem konfrontiert, was man heute eine Ressourcenkrise nennen würde.

Kohle gab es in England durchaus. Und zwar reichlich. Aber Gusseisen ließ sich damit nicht schmelzen – Schwefel und andere Verunreinigungen verdarben das Metall. Mit Kohle hergestelltes Eisen wurde spröde, untauglich für ernsthafte Arbeit.

Es lohnt sich zu erzählen, wie Darby zu seiner Lösung kam, denn dies war nicht die Leistung eines einsamen Genies. Darby hatte zuvor mehrere Jahre in der Kupferindustrie in Bristol gearbeitet, und davor bei einem Quäker gelernt, der Malzdarren fürs Brauen herstellte. Sowohl beim Kupferschmelzen als auch bei der Malzherstellung war die Technik des Erhitzens von Kohle unter Luftabschluss bereits im Einsatz – dabei entstand Koks, ein schwefelfreier Brennstoff, der sauber und gleichmäßig brannte. Beim Kupferschmelzen funktionierte das gut. Beim Eisenschmelzen hatte es vor Darby niemand systematisch versucht.

Darby tat zwei Dinge. Erstens übertrug er eine bekannte technologische Methode von einer Branche in eine andere. Zweitens kam er nach Coalbrookdale, wo er gleichzeitig schwefelarme Kohle, nicht allzu tief liegende Eisenerzvorkommen und einen schnell fließenden Fluss zum Antrieb der Blasebälge zur Hand hatte. Im Januar 1709 stellte er sein erstes handelsfähiges Gusseisen her, geschmolzen mit Koks.

Niemand hat Darbys genaue Worte festgehalten, als er den fertigen Guss aus dem Koksofen zum ersten Mal sah. Doch die Folgen dieses Moments schrieben die nächsten zweihundert Jahre Weltgeschichte um. Brücken. Eisenbahnen. Dampfschiffe. Die Stahlskelette von Wolkenkratzern. Panzer. Motoren. Das gesamte Eisen der Industriezivilisation – vom ersten gusseisernen Träger bis zur letzten Schiene der Transsibirischen Eisenbahn – geht darauf zurück, dass ein erfahrener Quäker-Kupferindustrieller erahnte, dass sich eine in einer Produktion funktionierende Technik auf eine andere übertragen lässt, wo sie noch niemand ausprobiert hatte.

Das ist die erste Geschichte.

1792. Cornwall

Mehr als achtzig Jahre nach Darby, auf der anderen Seite Englands, wirkte ein Ingenieur namens William Murdoch – ein Schotte, Sohn eines Kleinbauern, mittlerweile siebenunddreißig Jahre alt. Er war bei der Firma Boulton & Watt angestellt – eben jener, die James Watts Dampfmaschinen baute. Murdoch war nach Cornwall geschickt worden, um die in den Zinnminen installierten Maschinen zu betreuen.

Er lebte im kleinen Städtchen Redruth, in einem kleinen Haus. Und dort bemerkte Murdoch eines Tages Folgendes.

Wenn man Koks herstellt – jenen Koks, den Darby achtzig Jahre zuvor herzustellen gelernt hatte –, entweicht beim Erhitzen eine große Menge aus der Kohle. Der Koks bleibt im Ofen zurück. Und nach draußen, in die Luft, entweicht ein dickes, brennbares Gas. Es riecht nach Schwefel und Brand, sieht aus

wie eine schmutzige Wolke, und jeder, der mit Koksöfen arbeitete, kämpfte mit diesem Gas: Es ist giftig, explodiert manchmal, und stinkt die ganze Nachbarschaft ein. Man versuchte, es zu verteilen, abzuleiten, damit es nicht störte.

Murdoch sammelte dieses Gas in einem Rohr.

1792 begann er mit seinen Experimenten. 1794 hatte er ein funktionierendes System: In einer eisernen Retorte in seinem Hinterhof erhitzte er Kohle, das Gas floss durch ein Rohr ins Haus, und am Ende des Rohrs stand ein einfacher Brenner. Das erste Rohr für die Gasleitung war ein alter Gewehrlauf. Er zündete es an – und erhielt eine saubere, helle Flamme, ohne Rauch, ohne Ruß, viel heller als Kerzen oder Öllampen. An einem Abend im Jahr 1794 saß Murdoch in seinem Wohnzimmer in Redruth im Licht dessen, was alle anderen für Müll hielten.

Was danach geschieht, ist eine merkwürdige Sache, die in der Technikgeschichte häufiger vorkommt, als man denkt.

Murdoch erfand das System. Aber er war nicht derjenige, der es kommerzialisierte.

1802, als der Frieden von Amiens gefeiert wurde, gelang es Murdoch, die Leitung von Boulton & Watt zu einer öffentlichen Vorführung zu überreden – und an jenem Abend erstrahlte die Fassade der Soho-Gießerei in Birmingham im Gaslicht. Die Stadt lief zusammen, um es zu sehen. Es war ein Triumph. Doch Murdoch, so schrieben seine Zeitgenossen, „hielt sich seinem Charakter nach im Schatten“, und seine Arbeitgeber hatten es nicht eilig, die Erfindung zu patentieren. Unterdessen hatte ein anderer Mann, Frederick Albert Winsor – ein gebürtiger Deutscher, der nach London gezogen war –, eine Abhandlung des Franzosen Lebon über brennbares Gas gelesen, das Potenzial erkannt und begonnen, im Lyceum Theatre in London Vorträge zu halten. Winsor war ein brillanter Werber und ein schlechter Ingenieur. Zeitgenossen schrieben, „er wusste fast nichts von Chemie und war in Mechanik so unfähig, dass er keine Anweisungen zum Bau der Apparatur geben konnte.“ Aber er verstand es, Investoren zu überzeugen und Menschenmengen anzuziehen.

Im Januar 1807 war es Winsor, nicht Murdoch, der die ersten Gaslaternen der Welt entzündete – in der Pall Mall in London. Am vierten Juni desselben Jahres, zum Geburtstag von König Georg III., inszenierte er eine ganze Show: Entlang der Mauer zwischen der Mall-Straße und den Gärten von Carlton House entzündeten sich zweiunddreißig Gasbrenner, verbunden durch ein dünnes Zinnrohr. Die Menge stand bis Mitternacht dort.

Die erste vollständig mit Gas beleuchtete Fabrik – die Phillips-&-Lee-Spinnerei in Manchester – wurde erst 1805/1806 von Murdochs Hand in Betrieb genommen. Zu diesem Zeitpunkt entwarf Winsor bereits ein Gesetz zur Gründung der weltweit ersten Gasgesellschaft. In den 1820er-Jahren brannten in London vierzigtausend Gaslaternen. Bis zur Jahrhundertmitte stand die Gasbeleuchtung in der gesamten westlichen Welt.

Murdoch ließ seine Entdeckung nicht patentieren und starb 1839 als angesehener Ingenieur, bekannt in engen Kreisen. Der Titel „Vater der Gasbeleuchtung“ blieb ihm in der Technikgeschichte erhalten, doch das kommerzielle Imperium baute ein Mann auf, der die Technologie nicht erfunden, sondern verkauft hatte. Diese Trennung zwischen dem Erfinder und demjenigen, der die Erfindung auf den Massenmarkt trägt, ist ein Muster, dem wir in diesem Buch noch mehr als einmal begegnen werden.

Das ist die zweite Geschichte.

Was sie gemeinsam haben

Achten Sie auf die Struktur.

Darby erfand die Kohle nicht. Kohle wurde in England schon Jahrhunderte vor ihm abgebaut. Auch die Verkokungstechnik erfand Darby nicht – sie war bereits beim Kupferschmelzen und beim Brauen im Einsatz. Darby übertrug eine bekannte Technologie von einer Branche in eine andere, wo sie noch niemand systematisch erprobt hatte. Vor ihm war Kohle in der Metallurgie nutzlos. Nach ihm wurde Kohle zur Grundlage der Industrie.

Murdoch erfand das brennbare Gas nicht. Gas entwich aus Koksöfen von dem Moment an, als Darby 1709 zum ersten Mal einen Ofen entzündete. Dreiundachtzig Jahre lang stieg das Gas über England in den Himmel, und niemand schenkte ihm Beachtung. Murdoch schuf keine neue Ressource – er erkannte den Wert in etwas, das alle anderen wegwarfen.

Und noch ein Detail, das im Moment unwichtig erscheinen mag, sich aber später als entscheidend erweist. Weder Darby noch Murdoch zerstörten, was vor ihnen da war. Holzkohle wurde noch lange nach Darby weiter produziert und genutzt. Öllampen und Kerzen brannten noch lange, nachdem Gasbeleuchtung verfügbar war. Die neue Technologie ersetzte die alte nicht per Dekret von oben. Sie begann einfach, parallel zu funktionieren – und die Menschen wechselten nach und nach, sobald sie sahen, dass es für sie vorteilhafter war.

Parallel, nicht anstelle.

Merken Sie sich diesen Satz.

Wie das mit Bitcoin zusammenhängt

Schauen wir uns nun unsere eigene Zeit an.

2008 veröffentlichte eine Person (oder eine Gruppe von Personen) unter dem Pseudonym Satoshi Nakamoto ein neunseitiges Dokument, das eine Methode beschrieb, digitales Geld ohne eine Bank in der Mitte zu schaffen. Wenige Monate später, im Januar 2009, startete er ein System namens Bitcoin.

Die grundlegende Schwierigkeit, die Satoshi löste, war in der Informatik als „Double-Spending-Problem“ bekannt: Wie stellt man sicher, dass eine digitale Datei – Geld – nicht kopiert und zweimal ausgegeben werden kann, ohne dass ein zentraler Schiedsrichter die Konten überwacht?

Die Lösung war elegant. Alle Teilnehmer des Netzwerks führen gemeinsam ein Kontobuch, in dem Transaktionen verzeichnet werden. Jede Seite dieses Kontobuchs ist durch ein mathematisches Problem geschützt, das sehr aufwendig zu lösen ist – man muss eine kolossale Menge an Strom und Rechenleistung aufwenden. Wer das Problem zuerst löst, wird mit neuen Bitcoins belohnt. Und da die Lösung enorme Ressourcen erfordert, wird das Umschreiben bereits verzeichneter Seiten praktisch unmöglich: Man müsste das gesamte Netzwerk übertreffen. Dieser Mechanismus wird Proof-of-Work genannt.

Dies war eine Entdeckung von der Klasse Darbys. Vor Satoshi galt es als grundsätzlich unmöglich, digitales Geld ohne Mittelsmann zu schaffen. Nach Satoshi existiert es, funktioniert bereits im sechzehnten Jahr, ist besser geschützt als jeder Banktresor der Welt und hat eine Marktkapitalisierung, die größer ist als das Bruttoinlandsprodukt der meisten Länder.

Doch diese Lösung hat eine Eigenschaft, der kaum jemand Beachtung schenkt. Die mathematischen Probleme, die Bitcoins Miner lösen, sind an sich bedeutungslos.

Ein Miner nimmt eine Liste von Transaktionen, fügt eine Zufallszahl hinzu, lässt sie durch eine kryptografische Funktion laufen und prüft, ob das Ergebnis am Anfang genügend Nullen aufweist. Wenn nicht – fügt er eine weitere Zufallszahl hinzu, lässt sie erneut durchlaufen, prüft erneut. Und so weiter, milliardenfach pro Sekunde, bis er Glück hat. Die gesamte Energie, die in diesem Moment verbraucht wird – und das sind Stand 2026 etwa 170 Terawattstunden pro Jahr, ungefähr so viel wie Polen oder die Ukraine verbrauchen – fließt in eine einzige Sache: das Auffinden einer Zufallszahl, die die Bedingung erfüllt.

Aus diesem Auffinden entsteht kein Nebennutzen. Niemand nutzt die Ergebnisse dieser Berechnungen. Niemand braucht sie, außer dem Netzwerk selbst.

Bitcoin ist Darby. Die erste große Entdeckung seiner Klasse.

Und das, was rund um Bitcoin in die Luft entweicht – Milliarden von Rechenzyklen, die niemand braucht –, ist Murdochs Gas von 2009, das bislang noch niemand in ein Rohr gesammelt hat.

Was genau in die Luft entweicht

Es lohnt sich, konkreter zu sagen, um welches „Gas“ es hier geht.

Das heutige Bitcoin-Netzwerk besteht aus Hunderttausenden spezialisierter Geräte – ASIC-Miner. Das sind Computer, die auf eine einzige Operation zugeschnitten sind: das Hashing mit dem SHA-256-Algorithmus. Sie können nichts anderes, und nichts anderes wird von ihnen verlangt. Jedes dieser Geräte unternimmt Billionen Versuche pro Sekunde, um die nötige Zahl zu finden.

Zählt man die Arbeit aller Miner der Welt zusammen, erhält man eine Rechenleistung, die der kombinierten Leistung aller Supercomputer in den Forschungszentren der Welt entspricht – malgenommen mit Tausenden. Das ist eine der größten Rechenressourcen, die die Menschheit je zu einer einzigen Struktur zusammengefasst hat.

Und diese gesamte Ressource wird für eine einzige Handlung aufgewendet: das Erraten von Zufallszahlen, um eine Hash-Bedingung zu erfüllen.

Stellen Sie sich vor, Sie hätten eine Million hochgebildeter Fachleute – Wissenschaftler, Ingenieure, Ärzte, Architekten – und ließen sie den ganzen Tag lang Münzen werfen und aufschreiben, ob Kopf oder Zahl gefallen ist. Sie erledigen die Aufgabe hervorragend, die Münze wird tatsächlich geworfen, die Ergebnisse werden tatsächlich notiert. Doch all ihre Bildung, ihre Erfahrung, ihre Fähigkeiten – bleiben ungenutzt. Jeder von ihnen könnte in derselben Zeit eine wissenschaftliche Arbeit schreiben, eine Brücke entwerfen, zehn Patienten behandeln, ein schwieriges technisches Problem lösen. Stattdessen – die Münze.

Ungefähr das geschieht bei Bitcoin. Rechenleistung, die echte Probleme lösen könnte – KI-Modelle trainieren, das Klima modellieren, nach neuen Medikamenten suchen –, wird darauf gerichtet, Zufallszahlen zu erraten.

Schützt das das Netzwerk? Ja. Funktioniert es? Ja. Gibt es hier einen strukturellen Mangel? Absolut. Und dieser Mangel ist nicht Satoshis Fehler, ebenso wenig wie das reichlich vorhandene Gas aus den Koksöfen Darbys Fehler war. Es ist schlicht eine Folge davon, dass die erste große Entdeckung ihre eigenen Nebenprodukte selten bemerkt.

Unter der Haube. GHash.IO, Sommer 2014

Es gibt eine Episode aus der frühen Geschichte von Bitcoin, die es sich lohnt genauer zu betrachten – denn sie nimmt viel von dem vorweg, was später in diesem Buch geschehen wird.

In den Jahren 2013–2014 wurde GHash.IO zum größten Mining-Pool bei Bitcoin. Ein Pool ist ein Zusammenschluss von Minern, die ihre Rechenleistung bündeln und die Belohnung im Verhältnis zum jeweiligen Beitrag aufteilen. GHash.IO wuchs schnell. Im Januar 2014 näherte sich sein Anteil fünfzig Prozent, die Community geriet in Panik, einige Miner verließen den Pool freiwillig, und der Anteil sank vorübergehend. Doch im Sommer wiederholte sich alles in weit ernsterer Form.

Von elf Uhr morgens am zwölften Juni bis zehn Uhr morgens am dreizehnten Juni 2014 – fast vierundzwanzig Stunden am Stück – hielt GHash.IO etwa 55 Prozent der gesamten Bitcoin-Hashrate. Nicht 51. Fünfundfünfzig.

Für Bitcoin ist das eine katastrophale Zahl. Kontrolliert ein einzelner Teilnehmer mehr als die Hälfte der Rechenleistung des Netzwerks, kann er theoretisch die Transaktionsgeschichte in seinem eigenen Interesse umschreiben, dieselben Coins doppelt ausgeben, jemandes Überweisungen blockieren. Das Netzwerk hört in dem Moment auf, dezentral zu sein, in dem Mehrheitskontrolle entsteht.

Man erwartete einen Angriff. Man erwartete Ausbeutung. Man erwartete das Ende der dezentralen Ära.

Es geschah nichts.

Das ist passiert: Der Eigentümer des Pools, die Börse CEX.IO, veröffentlichte eine Erklärung, dass er nicht beabsichtige, das Netzwerk anzugreifen. Gleichzeitig starteten die führenden Bitcoin-Entwickler, akademische Forscher und große Holder eine Druckkampagne: Miner wurden aufgerufen, GHash.IO zugunsten anderer Pools zu verlassen, der Ruf von CEX.IO wurde öffentlich in der Presse seziert, der Bitcoin-Kurs sank binnen weniger Stunden um etwa fünf Prozent. Am neunten Juli 2014 fand in London ein Rundtischgespräch mit Vertretern aller großen Mining-Pools und Geräteherstellern statt. Bei diesem Rundtisch wurde vorgeschlagen, dass GHash.IO seinen Anteil freiwillig auf eine Obergrenze von 39,99 Prozent begrenzt. Am sechzehnten Juli stimmte der Pool dieser Beschränkung öffentlich zu und rief die anderen Pools auf, dasselbe zu tun. Der Anteil von GHash.IO begann zu sinken. Bis zum Ende des Sommers war er auf fünfunddreißig Prozent gefallen. 2016 schloss der Pool.

Warum nutzte ein Pool, der die technische Fähigkeit besaß, Bitcoin zu zerstören, diese Fähigkeit nicht?

Die offizielle Antwort: Reputation, Vertrauen, langfristige Interessen. Das Netzwerk zu zerstören, mit dem man selbst Geld verdient, ist irrational.

Das ist die richtige Antwort. Aber nicht die vollständige. Denn „das Netzwerk zu zerstören, mit dem man selbst verdient, ist irrational“ ist keine selbstverständliche Wahrheit. Es ist die Folge ganz bestimmter struktureller Bedingungen. Was genau muss gegeben sein, damit ein solches Verhalten irrational wird? Warum funktioniert es in manchen Systemen und in anderen nicht? Warum wirkte der Druck der Community im Juli 2014 – während in anderen Fällen, bei anderen Netzwerken, Druck nicht wirkt und Angriffe stattfinden?

Diese Fragen wurden 1980 von einem Politikwissenschaftler aus Michigan beantwortet. Sein Name war Robert Axelrod, und was er entdeckte, erklärt nicht nur das Verhalten von GHash.IO, sondern fast alles, wovon dieses Buch handelt.

Doch das ist Stoff für das nächste Kapitel.

Das Versprechen, mit dem wir beginnen

Bevor wir das Kapitel schließen, möchte ich formulieren, was uns weiter erwartet.

Die Geschichte der Kohle, die ich zu erzählen begann, ist tatsächlich länger als zwei Szenen – Darby und Murdoch. Sie besteht aus fünf Phasen, jede von einer eigenen Person eröffnet, und jede machte aus dem, was zuvor als Abfall galt, das Hauptprodukt der nächsten Industrie.

Zunächst wurde Kohle einfach zum Heizen verbrannt – und galt als minderwertiger Brennstoff, weil sie stinkt.

Dann übertrug Darby die Verkokungstechnik vom Kupferschmelzen auf Eisen – und alles, was bei der Koksherstellung entstand, galt als Müll.

Dann sammelte Murdoch das Gas – und alles, was bei der Gasherstellung übrig blieb, galt als Müll.

Dann entdeckte 1856 ein achtzehnjähriger Chemiker namens William Perkin bei dem Versuch, ein Malariamedikament zu synthetisieren, zufällig, dass sich aus diesem „Müll“ synthetische Farbstoffe herstellen ließen – und darauf wuchs die gesamte Chemieindustrie des zwanzigsten Jahrhunderts. Aspirin, die ersten Kunststoffe, die ersten Antibiotika, die ersten Polymere – alles aus dem, was zuvor als Abfall der Gasherstellung galt.

Und schließlich, bis zur Mitte des zwanzigsten Jahrhunderts, hörte man auf, Kohle als Brennstoff zu bezeichnen. Man begann, sie Feedstock zu nennen – Rohstoff. Aus ein und derselben Kohle lernte man, gleichzeitig Koks, Gas, Teer, Schwefel, Ammoniak und Dutzende chemischer Verbindungen zu gewinnen. Jedes Erzeugnis ging in eine eigene Industrie. Die Wärme aus der Verbrennung der Reste wurde zum billigsten und am wenigsten wertvollen Ergebnis.

Was mit der Kohle geschah, beginnt jetzt, bei uns, mit der Rechenleistung zu geschehen. Bitcoin spielt in dieser Geschichte die Rolle von Darbys Koks – der ersten strukturellen Durchbruchsidee, die zeigte, dass sich Rechenleistung in etwas Wertvolles verwandeln lässt (den Schutz digitalen Geldes). Es war eine Entdeckung historischen Ausmaßes, und wir werden ihre Folgen in diesem Buch noch mehr als einmal entfalten. Doch ganz wie der Koks im Jahr 1709 nutzt Bitcoin seine Ressource eindimensional: Rechenleistung wird zu Hashes, Hashes werden zu Sicherheit, der Rest entweicht in die Luft. Seit dreihundert Jahren lernt die Menschheit zu erkennen, dass es rund um die Hauptoperation – Koks, Eisen,

Hashes – Ströme gibt, die nur so lange als Müll gelten, bis der Mensch kommt, der sie betrachtet.

Der Murdoch-Schritt – wenn Menschen anfangen, das zu sammeln, was sie bis dahin weggeworfen haben – fällt in der digitalen Geschichte auf das Jahr 2022. Das ist Qubic. Und es ist eine jener ingenieurtechnischen Ideen, über die man später schreibt „wie konnte das niemand früher tun“ – so logisch im Nachhinein und so radikal im Moment ihres Erscheinens. Denn Qubic versucht nicht, mit Bitcoin auf dessen eigenem Feld zu konkurrieren. Es macht einen Zug, den es auf diesem Feld bislang gar nicht gab. Was genau Qubic „in ein Rohr sammelt“, wie das technisch aufgebaut ist und warum es funktioniert, ist der Hauptgegenstand dieses Buches. Wir werden uns dem schrittweise nähern, Kapitel für Kapitel, denn es schnell zu erklären ist unmöglich: Die Idee wirkt erst einfach, nachdem alle darunterliegenden Schichten freigelegt sind.

Und dann – wenn alles so verläuft, wie es die Menschen planen, die Qubic bauen – erwartet uns der dritte Schritt. Derselbe, der der Kohle im zwanzigsten Jahrhundert widerfuhr, als sie aufhörte, „Brennstoff“ zu sein, und begann, Feedstock genannt zu werden – Rohstoff für Dutzende Industrien zugleich. Wenn Qubic hält, was es verspricht, wird die Rechenleistung in einen ähnlichen Zustand übergehen: Aus ein und demselben Rechenzyklus werden gleichzeitig Sicherheit, künstliche Intelligenz, wirtschaftlicher Wert und einige weitere Dinge gewonnen, die wir heute noch gar nicht zu formulieren wissen. Das ist ein Ehrgeiz von etwa demselben Ausmaß wie der Darbys im Jahr 1709 – und wie genau er umgesetzt wird, werden wir in diesem Buch bis zur letzten Schraube sehen.

Die Hauptsache – dieser Schritt ist noch nicht getan. Er ist für April 2027 geplant. Und wir werden ehrlich sehen, ob er funktioniert.

Dieses Buch ist eine Landkarte zwischen den Phasen. Es wird sich nicht linear bewegen, denn auch die Geschichte von Qubic selbst verlief nicht linear: Sie wurde von verschiedenen Menschen, an verschiedenen Orten, bei der Lösung verschiedener Aufgaben geschaffen, und erst im Nachhinein wurde sichtbar, wie sich diese Aufgaben zu einer großen Aufgabe zusammenfügen.

Doch bevor wir zum Coalbrookdale des digitalen Zeitalters übergehen, müssen wir uns mit einer einfachen Wahrheit befassen. Diese Wahrheit kannte Murdoch 1792 intuitiv, Abraham Darby dagegen nicht. Ohne sie wäre die Gasbeleuchtung nie zu einer Industrie geworden. Ohne sie wäre Bitcoin bei den Hashes stehen geblieben. Ohne sie würde Qubic keinen einzigen Tag funktionieren.

Diese Wahrheit ist in vier Zeilen Code formuliert.

Sie wurde 1980 in einem Turnier bewiesen, an dem vierzehn Programme teilnahmen.

2
Axelrods Turnier

Im Juni 2014 hatte eine Person (genauer gesagt eine Börse) für vierundzwanzig Stunden die technische Möglichkeit in der Hand, Bitcoin zu zerstören. Sie zerstörte es nicht. Die Standarderklärung – „es ist irrational, das Netzwerk zu zerstören, mit dem man selbst verdient“ – ist richtig, aber sie erklärt nicht, warum es irrational ist. Denn es gibt Netzwerke, in denen sich Zerstörung lohnt. Es gibt Situationen, in denen Menschen das zerstören, wovon sie leben. Es gibt Länder, in denen Eliten das Land ruinieren, das sie regieren. Es gibt Beziehungen, in denen sich Partner methodisch gegenseitig vernichten. Irrational? Ja. Kommt ständig vor.

Die Frage ist also nicht, warum GHash.IO nicht angriff. Die Frage lautet: Unter welchen Bedingungen wird ehrliches Verhalten rational und Betrug – nicht?

Das erwies sich als eine konkrete, technische, überprüfbare Frage. Und die Antwort darauf wurde zuerst nicht von einem Philosophen und nicht von einem Ökonomen gefunden. Sie wurde von einem achtunddreißigjährigen Politikwissenschaftler gefunden, der 1977 in seinem Büro an der University of Michigan saß und Computerprogramme beim Schachspielen beobachtete.

In diesem Kapitel geht es darum, was er schließlich herausfand. Doch um zu verstehen, warum seine Entdeckung für Qubic, Bitcoin und alles, worüber wir später sprechen werden, wichtig ist, müssen wir zunächst ein sehr einfaches Spiel auseinandernehmen.

Das Gefangenendilemma

Stellen Sie sich vor, Sie und Ihr Komplize wurden gefasst. Es gibt gegen keinen von Ihnen beiden viele Beweise – solide nachweisen lässt sich nur ein geringfügiges Verbrechen, für das jeder von Ihnen ein Jahr bekommt. Doch die Ermittler vermuten, dass Sie gemeinsam etwas Großes gedreht haben, und wollen das beweisen.

Man hat Sie getrennt in verschiedene Zellen gesteckt. Ein Ermittler kommt zu jedem von Ihnen und bietet einen Deal an.

„Hören Sie. Wenn Ihr Komplize schweigt und Sie gegen ihn aussagen – geht er für fünf Jahre in den Knast, und Sie kommen frei. Wenn Sie beide aussagen – gehen Sie beide in den Knast, aber Sie bekommen nicht fünf, sondern nur drei Jahre. Wenn Sie beide schweigen – können wir das schwere Verbrechen nicht nachweisen, und jeder von Ihnen bekommt nur ein Jahr für das geringfügige.“

Sie sitzen in Ihrer Zelle und denken nach.

Wenn mein Komplize schweigt – lohnt es sich für mich, ihn zu verraten. Ich komme frei, er geht in den Knast. Wenn mein Komplize mich verrät – lohnt es sich für mich ebenfalls, ihn zu verraten. Ich bekomme drei statt fünf Jahre.

Jede Variante seines Verhaltens führt zu einer Schlussfolgerung: Es lohnt sich für mich, ihn zu verraten.

Der Komplize in der Nachbarzelle denkt dasselbe. Und auch er kommt zu dem Schluss: Es lohnt sich für ihn, mich zu verraten.

Am Ende verraten Sie sich gegenseitig und bekommen jeweils drei Jahre. Hätten Sie beide geschwiegen, hätten Sie jeweils nur ein Jahr bekommen.

Das ist das Gefangenendilemma. In seiner reinen Form sieht es so aus: Es gibt zwei Teilnehmer, jeder kann sich entscheiden, zu „kooperieren“ (zu schweigen) oder zu „defektieren“ (zu verraten). Die Auszahlungen sind so angeordnet, dass die individuell rationale Wahl immer das Defektieren ist, aber wenn beide es tun, verlieren beide.

Das Spiel ist nicht kompliziert. Man ersann es 1950 bei der RAND Corporation – zwei Mathematiker, Merrill Flood und Melvin Dresher, versuchten, ein Beispiel zu finden, das die damaligen Theorien rationalen Verhaltens ins Wanken bringen würde. Ihr Kollege Albert Tucker formalisierte es und gab ihm die Geschichte von den zwei Gefangenen, unter der wir es kennen.

Seitdem – seit siebzig Jahren – ist dieses Spiel eines der meiststudierten Objekte in den Geistes- und Sozialwissenschaften geworden. Denn es stellte sich heraus, dass es überall auftaucht.

Wettrüsten – Gefangenendilemma. Es lohnt sich für jedes Land, mehr Waffen zu bauen als der Nachbar. Aber wenn alle aufrüsten – geht es allen schlechter.

Steuerhinterziehung – Gefangenendilemma. Es lohnt sich für jeden Einzelnen, nicht zu zahlen. Aber wenn niemand zahlt – funktioniert der Staat nicht mehr.

Umweltverschmutzung – Gefangenendilemma. Es lohnt sich für jede Fabrik, ihre Abfälle in den Fluss zu kippen. Aber wenn alle kippen – bleibt niemandem ein Fluss.

Korruption, Kartellabsprachen, Überfischung, Staus, die Nutzung von Gemeindeland – überall dieselbe Struktur. Und überall – dasselbe Ergebnis: Die rationale Wahl jedes Einzelnen führt zu einem schlechten Ergebnis für alle.

John Nash, ein Mathematiker aus Princeton, bewies 1950 eine unangenehme Sache über dieses Spiel und bekam dafür einen Nobelpreis. Er zeigte, dass „beide defektieren“ ein Gleichgewicht ist. Das heißt: Wenn Sie sich beide in diesem Zustand befinden, profitiert keiner von Ihnen von einer einseitigen Änderung der Strategie. Wenn mein Komplize mich verrät und ich mich entscheide zu schweigen – verliere ich. Wenn ich ihn verrate und mein Komplize schweigt – verliert er. Beide verraten – stabil. Nicht gut. Aber stabil.

Das Nash-Gleichgewicht. Das System steckt in einem schlechten, aber dauerhaften Zustand fest.

Das war die Diagnose. Die Falle war beschrieben. Ob man aus ihr herauskommen konnte – darauf gab es lange keine Antwort.

Michigan, März 1980

Robert Axelrod hieß der Mann, den ich zu Beginn des Kapitels erwähnte. Bis 1977 lehrte er bereits sechs Jahre an der University of Michigan, hatte 1969 in Yale seine Promotion in Politikwissenschaft verteidigt und sich auf Konflikte zwischen Staaten spezialisiert. Vierzig Jahre alt, Sohn litauischer Juden, hatte er sein ganzes Leben der Frage gewidmet, wie Menschen es überhaupt schaffen, sich zu einigen.

Axelrod hatte einen ganzen Schrank voller Arbeiten zum Gefangenendilemma. Er hatte sie alle gelesen und war unzufrieden mit ihnen. Die Arbeiten versuchten meist, eines von zwei Dingen zu beweisen: entweder dass Menschen im echten Leben „irrational“ sind und entgegen der Theorie kooperieren, oder dass man die Auszahlungsmatrix ändern müsse – eine Steuer auf Defektion, einen externen Schiedsrichter, so etwas. Keine der Erklärungen befriedigte ihn.

Ihn interessierte eine konkrete Frage. Das Spiel wurde einmal gespielt – der rationale Zug ist zu defektieren. Gut. Aber was, wenn man es viele Male spielt? Wenn zwei Teilnehmer wissen, dass sie nicht eine, sondern zweihundert Runden gegeneinander spielen werden? Würde das etwas ändern?

Die Intuition legte nahe: ja. Wenn ich jetzt defektiere und wir noch hundertneunundneunzig weitere Runden spielen werden, wird mein Komplize viele Gelegenheiten haben, sich an mir zu rächen. Auch er wird aufhören zu kooperieren. Wir werden beide wenig bekommen. Höchstwahrscheinlich wäre es profitabler, von Anfang an zu kooperieren.

Aber wie genau? Welche Strategie ist im wiederholten Gefangenendilemma die profitabelste? Die Intuition ließ sich nicht formalisieren. Verschiedene Theoretiker schlugen verschiedene Strategien vor – manche komplex, andere einfach – und niemand konnte überzeugend zeigen, wessen Strategie die beste war.

Axelrod verfolgte zu dieser Zeit Computerschach-Turniere. In den späten siebziger Jahren hatten Schachprogramme begonnen, sich gegenseitig auszuspielen – und man konnte erkennen, dass der Sieg dem gehörte, der die komplexesten, tiefsten, mehrstufigsten Algorithmen geschrieben hatte. Die Programme wurden länger, klüger, gerissener.

Und dann kam ihm ein Gedanke.

Was, wenn man ein solches Turnier für das Gefangenendilemma veranstaltete?

Einladungen an alle bekannten Fachleute schicken, die zu diesem Spiel publiziert hatten. Jeden bitten, ein Programm einzureichen. Ein Programm in Fortran – ein einfaches, das als Eingabe erhält, was der Gegner in vergangenen Runden getan hat, und eine Entscheidung zurückgibt: kooperieren oder defektieren. Alle Programme in einem einzigen Turnier zusammenbringen, jedes gegen jedes, zweihundert Runden. Punkte zählen. Sehen, wer gewinnt.

1977–78 verschickte Axelrod die Einladungen. Sein Assistent Jeff Pynnonen schrieb in Fortran die Umgebung, in der die Programme spielen würden. Bis Anfang 1980 waren vierzehn Programme eingegangen.

Die Einsender waren Fachleute von Weltrang. Ökonomen. Mathematiker. Politikwissenschaftler. Psychologen. Ein Soziologe. Sie alle hatten seit Jahren Arbeiten zum Gefangenendilemma veröffentlicht. Jeder war überzeugt, dass seine Strategie die beste war.

Axelrod öffnete die Umschläge. Er las den Code. Und startete das Turnier.

Was in den Umschlägen war

Ich werde nicht alle vierzehn Strategien nacherzählen. Aber es lohnt sich, einige durchzugehen – um zu verstehen, vor welchem Hintergrund das Wesentliche geschah.

Ein Programm defektierte immer. Der Autor argumentierte so: Wenn die Theorie sagt, das einzige Gleichgewicht sei „defektieren", dann tun wir das eben einfach. Das Programm erzielte ein garantiert schlechtes Ergebnis gegen andere Defektierer und ein hervorragendes – wenn es auf jemanden traf, der immer kooperierte.

Ein anderes Programm kooperierte immer. Der Autor argumentierte: Wenn alle das täten, ginge es allen gut. Das Programm spielte ausgezeichnet mit sich selbst und gegen andere Kooperierer, verlor aber ständig gegen Defektierer.

Manche Programme waren gerissen. Eines – ein Programm namens JOSS – kooperierte in neunzig Prozent der Fälle nach der Kooperation des Gegners, defektierte aber in zehn Prozent der Fälle zufällig „zum Testen". Der Autor dachte, dies würde einen Bonus von naiven Partnern einbringen.

Ein anderes Programm – DOWNING – versuchte, das Verhalten des Gegners zu modellieren. Es schätzte ab, wie hoch die Wahrscheinlichkeit war, dass der Gegner nach seiner eigenen Defektion kooperierte, und wie hoch – nach Kooperation. War der Gegner vorhersehbar, versuchte DOWNING ihn auszunutzen. War er es nicht – passte es sich an.

Manche Programme waren offen komplex. Eines nutzte Regressionsanalyse. Ein anderes – Markov-Ketten. Ein Programm war siebenundsiebzig Zeilen lang in Fortran – der Autor war stolz auf seine mehrstufige Logik.

Und irgendwo in der Mitte lag ein Umschlag aus Toronto mit einem vier Zeilen langen Programm.

Der Vier-Zeilen-Sieger

Das Programm aus Toronto funktionierte so:

Erster Zug – kooperieren. Jeder folgende Zug – tue, was der Gegner im vorherigen Zug getan hat.

Hat der Gegner kooperiert – kooperieren. Hat der Gegner defektiert – defektieren. Beim nächsten Mal wieder anschauen, was er als Antwort tat, und spiegeln.

Das ist alles. Keine Modellierung. Keine Regression. Keine Logik von „wann ausnutzen, wann verzeihen". Ein Spiegel. Buchstäblich ein Spiegel.

Der Autor nannte es TIT FOR TAT – ein englischer Alltagsausdruck, „wie du mir, so ich dir". Doch eine genauere Bezeichnung für das, was das Programm tatsächlich tut, wäre: „Spiegel". Axelrod sah dieses Programm, las den Code – und entschied, jemand habe es als Scherz eingeschickt. Dann sah er sich den Namen des Absenders an. Dieser Mensch mochte keine Scherze.

Sein Name war Anatol Rapoport.

Axelrod startete das Turnier. Vierzehn Programme spielten gegeneinander, jedes gegen jedes, jeweils zweihundert Runden. Zusätzlich spielte jedes gegen sich selbst. Zusätzlich wurde ein neutrales Programm als Referenz hinzugefügt. Alle Punkte wurden gezählt.

Als die letzte Runde endete, waren die Ergebnisse so, dass Axelrod sein gesamtes Forschungsprogramm umschrieb.

Tit-for-Tat gewann. Mit deutlichem Abstand.

Alles Komplizierte verlor. Das lange, siebenundsiebzig Zeilen umfassende Programm landete im Mittelfeld. JOSS mit seinen zufälligen Defektionen – unter dem Durchschnitt. DOWNING mit seiner Modellierung des Gegners – mittelmäßig. Programme, die immer defektierten – ganz unten. Programme, die immer kooperierten – ebenfalls ganz unten, weil sie ausgenutzt wurden.

Vier Zeilen Code aus Toronto schlugen vierzehn Jahre Arbeit von Fachleuten.

Der Mann aus Lozowaja

Es lohnt sich, einen Moment innezuhalten und zu erzählen, wer der Mann war, der das siegreiche Programm schrieb. Denn das ist kein beliebiger Mathematiker.

Anatol Borissowitsch Rapoport wurde am 22. Mai 1911 in Lozowaja geboren, im Gouvernement Charkow des Russischen Reiches. Heute liegt Lozowaja im Osten der Ukraine, im Gebiet Charkiw. Im Dezember 1921, als Anatoli zehn Jahre alt war, floh seine Familie aus der Sowjetukraine nach Polen. Über den zugefrorenen Grenzfluss Zbrutsch. Auf Schlittschuhen.

Genauer gesagt war er derjenige, der auf Schlittschuhen floh – ein zehnjähriger Junge, der sich warm anzog, sich neue Schlittschuhe kaufte, zum Fluss ging, sich neben einem Zaun duckte, den sorglosen polnischen Kindern zusah, die auf der polnischen Seite des Damms Schlittschuh liefen, den Moment abwartete, in dem die Grenzwächter abgelenkt waren, und losfuhr. Plötzlich entdeckte ihn von irgendwo oben ein Rotarmist und begann zu schreien. Anatol nahm Fahrt auf, raste zu den polnischen Kindern, zwängte sich in ihren Kreis – und fuhr ruhig mit ihnen davon, weg von der sowjetischen Grenze. Viele Jahre später sollte er diesen Moment in seinen Memoiren beschreiben.

Ein Jahr später erreichte die Familie die Vereinigten Staaten und ließ sich in Chicago nieder. Anatol wurde zum Musikstudium geschickt. Mit sechzehn war er bereits ein vielversprechender Pianist. Mit achtzehn trat er ins Wiener Konservatorium ein. Bis 1934 studierte er dort Komposition, Klavier und Dirigieren. Er gab Konzerte in Österreich, Polen, Ungarn, Italien. Er sprach vier Sprachen.

Dann kamen die Nazis in Deutschland an die Macht. Die Karriere eines jüdischen Konzertpianisten in Mitteleuropa endete, bevor sie begonnen hatte. Rapoport kehrte in die Staaten zurück und musste feststellen, dass auch in Amerika niemand noch einen Pianisten aus Chicago brauchte. Mit dreiundzwanzig Jahren schrieb er sich an der University of Chicago ein. Sieben Jahre später verteidigte er seine Dissertation in Mathematik.

Danach arbeitete er fünfzehn Jahre lang in mathematischer Biologie – er modellierte die Ausbreitung von Epidemien, das Verhalten von Parasiten und Symbionten. 1955 kam er als einer der Gründer des Mental Health Research Institute an die University of Michigan. Dort begann er, das Verhalten von Menschen in

Konfliktsituationen zu untersuchen – durch Laborspiele, einschließlich des Gefangenendilemmas. Es war Rapoport, der dieses Experiment in den breiten wissenschaftlichen Gebrauch einführte, in seinem 1965 erschienenen Buch Prisoner's Dilemma: A Study in Conflict and Cooperation.

1970, als der Vietnamkrieg in seine schmutzigste Phase eintrat, verließ Rapoport die Vereinigten Staaten in Richtung Kanada. Er schrieb später, er habe „in einem Land leben wollen, das keiner messianischen Rolle verpflichtet ist“. Er nahm eine Stelle in Toronto an, wo er 1980 bereits emeritierter Professor im Ruhestand war – ein siebzigjähriger Gelehrter, Autor von zwanzig Büchern und dreihundert Artikeln, der sein ganzes Leben einer Frage gewidmet hatte: wie man Menschen dazu bringt, aufzuhören, einander zu töten.

Zu diesem Zeitpunkt war Rapoport einer der weltweit bekanntesten Forscher auf dem Gebiet der Spieltheorie und der Konfliktforschung. Und einer der konsequentesten Pazifisten. Er gründete Science for Peace. Er schrieb, Krieg sei „eine ansteckende Krankheit mit tödlichem Ausgang“.

Als die Einladung von Axelrod kam, setzte sich Rapoport hin und schrieb vier Zeilen. Schickte sie ab.

Viele Jahre später gestand er Axelrod, dass ihm Tit-for-Tat selbst nicht besonders gefiel. Zu hart, sagte er. Zu bereit zur Rache. Als moralische Haltung für einen Friedensforscher nicht wirklich passend. Aber er wollte sehen, wie es sich schlagen würde.

Es gewann.

Warum der Spiegel gewann

Axelrod verbrachte die nächsten zwei Jahre damit, zu verstehen, warum.

Nach der Analyse aller gespielten Partien identifizierte er vier Eigenschaften der siegreichen Strategie.

Erstens: Freundlichkeit. Tit-for-Tat defektiert nie zuerst. Beim ersten Zug kooperiert es immer. Bei jedem Zug nach der Kooperation des Gegners – kooperiert es. Diese Eigenschaft teilt alle vierzehn Programme in „freundliche“ (defektieren nie zuerst) und „gemeine“ (defektieren irgendwann ohne Provokation). Acht der vierzehn Programme waren „freundlich“. In der abschließenden Ergebnistabelle belegten alle acht freundlichen Programme die oberen Plätze. Alle sechs gemeinen – die unteren.

Zweitens: Vergeltung. Tit-for-Tat beantwortet eine Defektion sofort. Nicht mit Verzögerung, nicht auf Vorrat, nicht mit einer bestimmten Wahrscheinlichkeit – genau im nächsten Zug, genau einmal. Das schützt es vor Ausnutzung. Die „freundlichen“ Programme, die sich nicht zu vergelten wussten (die immer-kooperieren-Programme), wurden gnadenlos ausgenutzt und verloren am Ende.

Drittens: Vergebung. Tit-for-Tat trägt keinen Groll. Hat der Gegner beim letzten Zug kooperiert – vergisst es alles, was davor war, und kooperiert als Antwort. Programme, die Groll anhäuften und nach einer einzigen Defektion für immer Rache übten, blieben in einem ewigen Krieg stecken und verloren Punkte. Vergebung stellt die Kooperation wieder her.

Viertens: Klarheit. Tit-for-Tat ist vorhersehbar. Es ist für den Gegner leicht zu verstehen, was es tut und warum. Das bedeutet, dass sich mit ihm schnell Kooperation herstellen lässt – es genügt ein einziger Versuch der Kooperation, und es wird ebenfalls kooperieren. Programme, die versuchten, gerissen und unvorhersehbar zu sein (wie JOSS mit seinen zufälligen Defektionen), verwirrten ihre Partner und

zerstörten Kooperation, die sonst hätte entstehen können.

Freundlichkeit, Vergeltung, Vergebung, Klarheit. Alles in vier Zeilen Code.

Axelrod veröffentlichte die Ergebnisse im März 1980 im Journal of Conflict Resolution. Der Artikel trug den Titel „Effective Choice in the Prisoner's Dilemma“. Er machte Eindruck, doch die wissenschaftliche Gemeinschaft nahm ihn mit der üblichen gesunden Skepsis auf: Nun gut, ein Programm gewann ein Turnier. Vielleicht war das Zufall. Vielleicht haben sich die anderen nicht angestrengt. Vielleicht würde bei einer anderen Durchführung des Turniers jemand anderes gewinnen.

Axelrod las die Kritik und beschloss, ein zweites Turnier zu veranstalten.

Die zweite Runde

Für das zweite Turnier tat Axelrod drei Dinge.

Erstens: Er veröffentlichte einen vollständigen Bericht über das erste Turnier. Alle Programme, alle Partien, alle Ergebnisse, eine vollständige Analyse, warum TfT gewonnen hatte. Alle künftigen Teilnehmer erhielten diesen Bericht. Das heißt, niemand konnte nun mehr sagen, er habe die Schwächen der eigenen Strategie oder die Stärken des Gegners nicht gekannt.

Zweitens: Er schaltete eine Ankündigung in Computerzeitschriften wie Creative Computing und Personal Computing. Er lud jeden ein, nicht nur akademische Fachleute. Am Ende erhielt er zweiundsechzig Programme aus aller Welt – von Professoren bis zu jugendlichen Hobbyisten. Beim ersten Turnier waren es vierzehn Programme. Beim zweiten – fast fünfmal so viele.

Drittens: Er änderte die Regel für das Spielende. Beim ersten Turnier gab es genau zweihundert Runden. Das schuf das Problem des „letzten Zugs“ – in der letzten Runde lohnt sich Kooperation nicht, also sollte man defektieren; aber dann lohnt sie sich auch in der vorletzten nicht; und so weiter zurück bis zum Anfang. Das nennt man „Rückwärtsinduktion“, und sie zerstört theoretisch die ganze Konstruktion. Im echten Leben funktioniert Rückwärtsinduktion nicht, weil niemand den genauen Zeitpunkt des Endes kennt. Axelrod modellierte das: Im zweiten Turnier endete das Spiel nach jedem Zug mit einer Wahrscheinlichkeit von 0,00346. Im Durchschnitt ergab das etwa 200 Züge, aber niemand wusste im Voraus, welcher Zug der letzte sein würde.

Die Teilnehmer wussten alles. Sie wussten, dass TfT gewonnen hatte. Sie kannten die Eigenschaften, die ein Programm erfolgreich machen. Sie wussten, dass Axelrod sogar ausdrücklich eine Strategie vorgeschlagen hatte, die TfT schlagen könnte – Tit-for-Two-Tats, eine sanftere Version, die zwei Defektionen in Folge verzeiht, bevor sie sich rächt.

Von zweiundsechzig Programmen versuchten viele, TfT direkt zu schlagen. Manche waren aggressiver. Andere – gerissener. Wieder andere nutzten komplexe Modelle des Gegners.

Ein Mensch sah sich dieses ganze Getümmel an, setzte sich hin und schrieb erneut vier Zeilen.

Anatol Rapoport reichte erneut Tit-for-Tat ein.

Auch das zweite Turnier gewann TfT.

Axelrod veröffentlichte die Ergebnisse im September 1980. Und er fügte etwas hinzu, das ich noch nicht erwähnt habe. Er führte sechs Varianten des zweiten Turniers durch – mit unterschiedlichen „ökologischen“ Bedingungen, bei denen bestimmte Programmtypen mehr oder weniger stark vertreten waren. In fünf von sechs Varianten gewann TfT erneut. In der sechsten belegte es den zweiten Platz.

Und noch etwas: Axelrod führte eine evolutionäre Simulation durch. Er stellte sich vor, dass jedes Programm im Verhältnis zu seinem Erfolg Nachkommen erzeugt. Die weniger erfolgreichen sterben aus, die erfolgreicheren vermehren sich. Nach tausend Generationen dominierte TfT. Nach mehreren tausend – nahm es den Großteil der Population ein. Kooperation, die wie eine naive Alternative zu rationalem Egoismus erschienen war, erwies sich als stabiler evolutionärer Attraktor.

Das Bild war klar. Kooperation ist stabil. Kooperation ist profitabel. Kooperation gewinnt in wiederholten Interaktionen – vorausgesetzt, die Strategie, die sie umsetzt, hat vier Eigenschaften: Freundlichkeit, Vergeltung, Vergebung, Klarheit.

Drei Bedingungen

Axelrod ging weiter. In den folgenden Jahren arbeitete er mit Kollegen daran, zu verstehen, unter welchen Bedingungen genau das oben beschriebene Bild funktioniert. Denn es ist eine Sache zu zeigen, dass TfT in einem bestimmten Turnier gewinnt. Es ist eine andere, zu verstehen, warum.

In dem 1984 erschienenen Buch The Evolution of Cooperation, und noch schärfer – in Artikeln von 1985–1987 mit dem Biologen William Hamilton – formulierte Axelrod die Antwort. Es zeigte sich, dass drei Bedingungen erforderlich sind, damit Kooperation durch etwas wie TfT entstehen und aufrechterhalten werden kann. Alle drei. Entfernt man auch nur eine – bricht die Kooperation zusammen.

Bedingung eins: Wiederholung. Das Spiel muss sich wiederholen. Wenn ich weiß, dass ich dich nur einmal im Leben treffe, ist die optimale Strategie zu defektieren. Nehmen und weglaufen. Du findest mich sowieso nicht wieder. Im Turnier hatte jedes Programmpaar zweihundert Runden. Im echten Leben entsteht Wiederholung, wenn Menschen im selben Dorf leben, in derselben Firma arbeiten, über viele Jahre auf demselben Markt handeln. Wenn ich weiß, dass ich dich morgen wiedersehe, verhalte ich mich anders, als wenn ich weiß, dass ich dich nie wiedersehen werde.

Zerstört man die Wiederholung – erhält man das Verhalten eines Touristen in einer fremden Stadt. Man kann kein Trinkgeld geben. Man kann unhöflich sein. Keine Konsequenzen.

Bedingung zwei: Gedächtnis. Die Teilnehmer müssen sich erinnern, was der Gegner in vergangenen Runden getan hat. Ohne Gedächtnis funktioniert TfT nicht – man kann nicht „im Spiegel antworten“ auf etwas, an das man sich nicht erinnert. Im Turnier war das Gedächtnis in die Mechanik eingebaut: Jedes Programm erhielt als Eingabe die vollständige Interaktionsgeschichte. Im echten Leben entsteht Gedächtnis, wenn ich dich am Gesicht erkenne, mich an unsere vergangenen Gespräche erinnere, eine Vorstellung davon habe, wie du dich anderen gegenüber verhalten hast.

Zerstört man das Gedächtnis – erhält man das Verhalten einer großen anonymen Menge. Niemand erinnert sich an irgendjemanden. Jede Interaktion ist die erste und die letzte. Zu betrügen ist gefahrlos.

Bedingung drei: Klarheit. Oder Reputation, oder Beobachtbarkeit – man formuliert es unterschiedlich. Das Wesen ist eines: Verhalten muss sichtbar sein. Nicht nur für denjenigen, mit dem ich interagiere,

sondern auch für andere Teilnehmer. Denn wenn ich dich betrogen habe und außer uns beiden niemand davon weiß, kann ich hingehen und den Nächsten betrügen. Wenn sich aber die Nachricht von meinem Betrug in der Gemeinschaft verbreitet – wird man mich nicht mehr zu den Nächsten durchlassen.

Zerstört man Klarheit – erhält man das Verhalten einer Welt, in der man sich einen neuen Namen kaufen und in eine andere Stadt ziehen kann. Was auch immer ich tue, die Spur folgt mir nicht.

Drei Bedingungen. Wiederholung, Gedächtnis, Klarheit. Entfernt man auch nur eine – verschiebt sich die optimale Strategie von TfT hin zu reinem Egoismus.

Wie sich das mit dem Nash-Gleichgewicht verbindet

Erinnern Sie sich an das Nash-Gleichgewicht vom Anfang des Kapitels? Im Gefangenendilemma war es „beide defektieren“. Stabil, aber schlecht.

Axelrod fand ein weiteres Gleichgewicht. Wenn die drei Bedingungen erfüllt sind – wenn das Spiel wiederholt wird, die Teilnehmer sich erinnern und Verhalten sichtbar ist – erscheint ein neues Gleichgewicht: beide kooperieren nach TfT. Weicht einer ab und beginnt zu defektieren, spiegelt der andere – und beiden geht es schlechter. Kehrt einer zur Kooperation zurück – tut der andere es auch. Stabil. Und gut.

Das ist grundlegend. Nash beschrieb die Falle: Das System bleibt in einem schlechten Zustand stecken, weil einseitige Bewegung aus ihm heraus nicht profitabel ist. Axelrod zeigte den Ausweg: Gibt es die richtige Struktur um das Spiel herum (drei Bedingungen), erscheint ein zweites Gleichgewicht, in dem alle kooperieren. Und auch dieses Gleichgewicht ist stabil – einseitiges Abweichen von der Kooperation wird automatisch bestraft.

Die Aufgabe besteht also nicht darin, Menschen davon zu überzeugen, „besser zu sein“. Die Aufgabe besteht darin, eine Struktur zu schaffen, in der Egoismus zu Kooperation führt. Nicht die Menschen ändern. Die Spielregeln ändern.

Fünf Wege zu einer Idee

Jahrtausende vor Axelrod war eine ähnliche Idee unabhängig fünfmal gefunden worden.

Konfuzius lehrte um 500 v. Chr.: Tu anderen nicht an, was du dir selbst nicht wünschst. Das ist in den Gesprächen (Analekten) formuliert, in einem Gespräch zwischen dem Schüler Zigong und Konfuzius. Zigong fragte: Gibt es ein einziges Wort, nach dem man sein ganzes Leben leben könnte? Konfuzius antwortete: Vielleicht „Wechselseitigkeit“.

Rabbi Hillel der Ältere in Jerusalem antwortete um 30 v. Chr., als ihn ein Nichtjude bat, das ganze Wesen der Tora darzulegen, während er auf einem Bein steht: Was dir verhasst ist, tu deinem Nächsten nicht an – das ist die ganze Tora, der Rest ist Kommentar.

Jesus von Nazareth sagte um das Jahr 30 n. Chr. etwas Ähnliches, aber in positiver Formulierung: Wie ihr wollt, dass euch die Leute tun, so tut auch ihr ihnen. Später sollte man das die Goldene Regel nennen.

Immanuel Kant bewies das 1785 logisch, als kategorischen Imperativ: Handle nur nach derjenigen Maxime, durch die du zugleich wollen kannst, dass sie ein allgemeines Gesetz werde. Kann man nicht wollen, dass alle lügen – dann lüge nicht.

Anatol Rapoport bewies es 1980 mathematisch. Vier Zeilen Code in Fortran.

Fünf unabhängige Wege. Zweieinhalbtausend Jahre. Verschiedene Kulturen, Religionen, Epochen, Instrumente. Eine Formel.

Man kann sagen, dies bestätige eine tiefe moralische Wahrheit – dass es die Goldene Regel schon immer gegeben hat und sie überall zu finden ist. Man kann es auch anders sagen: Dies bestätigt eine strukturelle Wahrheit. In wiederholten Interaktionen mit Gedächtnis und Klarheit ist Tit-for-Tat die optimale Strategie. Genau deshalb findet sie jede Kultur, jede Philosophie, die ernsthaft über die Frage „wie lebt man unter anderen“ nachgedacht hat. Genau deshalb liefert ein mathematischer Beweis dieselbe Antwort wie die moralische Intuition.

Das Problem, wie Rapoport es selbst formulierte, liegt nicht in der Regel. Das Problem liegt in der Architektur ihrer Anwendung.

Die drei Bedingungen müssen erfüllt sein. In einer Familie, unter Freunden, in einem kleinen Unternehmen – sind sie oft von selbst erfüllt. Wir interagieren wiederholt, wir erinnern uns aneinander, wir sehen das Verhalten. TfT funktioniert intuitiv, ohne Mathematik. In großen anonymen Systemen – dem Staat, der Weltwirtschaft, der Menge – brechen die Bedingungen zusammen. Und die Goldene Regel funktioniert nicht mehr, nicht weil die Menschen schlechter geworden sind. Sondern weil die Architektur kaputt ist.

Axelrod und Rapoport zeigten, was die Architektur richtig macht. Und ebenso, was sie falsch macht.

Rückkehr zu Bitcoin

Jetzt können wir zu der Frage zurückkehren, mit der wir das Kapitel begonnen haben.

Warum griff GHash.IO Bitcoin im Juli 2014 nicht an?

Weil in Bitcoin alle drei Bedingungen Axelrods erfüllt sind.

Wiederholung. Jeder Block ist eine neue Runde des Spiels. Alle zehn Minuten entsteht ein Block. Vierundzwanzig Stunden sind hundertvierundvierzig Runden. Ein Jahr sind zweiundfünfzigtausend Runden. Ein Mining-Pool, der über fünf Jahre verdienen will, wird dieses Spiel eine Viertelmillion Mal spielen. Das ist keine einmalige Situation. Der Schatten der Zukunft ist länger als jeder mögliche einmalige Gewinn.

Gedächtnis. Die Blockchain ist buchstäblich das gemeinsame Gedächtnis des Netzwerks. Jede Transaktion, jeder Block, jeder Miner – all das ist verzeichnet. Hätte GHash.IO im Juli 2014 versucht, die Transaktionsgeschichte umzuschreiben, wäre dieser Versuch für immer in der Blockchain geblieben. Für immer – im kryptografischen Sinne des Wortes. Löschen ist unmöglich.

Klarheit. Die Hashrate jedes Mining-Pools ist öffentlich sichtbar. Das ist keine geheime Information. Jeder Forscher, jeder Journalist, jedes Community-Mitglied kann in Echtzeit sehen, welchen Anteil

welcher Pool einnimmt. Als GHash.IO im Juni 2014 die 50-Prozent-Marke überschritt, war das binnen Stunden bekannt. Nicht Tage, nicht Monate – Stunden.

Drei Bedingungen erfüllt. Das heißt, TfT sollte funktionieren. Und es funktionierte tatsächlich: Die Community spiegelte die Handlungen des Pools – Miner verließen ihn, die Reputation brach zusammen, der Bitcoin-Kurs fiel. Der wirtschaftliche Druck war eine Vergeltungsreaktion auf die Bedrohung der Kooperation. Als GHash.IO öffentlich versprach, sich auf 40 Prozent zu beschränken – stellte Vergebung die Kooperation wieder her. Nach einigen Monaten normalisierte sich die Lage.

Das war TfT auf der Ebene der globalen Mining-Community. Ohne Koordinationszentrum. Ohne formalen Vertrag. Nur vier Eigenschaften, die über drei Bedingungen wirkten.

Jetzt wird auch klar, warum in anderen Situationen Druck nicht wirkt. Ist ein Netzwerk klein und von außen nicht sichtbar – ist die Klarheit gebrochen. Sind die Miner anonym und gibt es keine Reputation – ist das Gedächtnis gebrochen. Wird das Spiel nur einmal gespielt (etwa wenn das Netzwerk kurz vor dem Zusammenbruch steht und das nächste Jahr nicht überleben wird) – ist die Wiederholung gebrochen. Wo auch nur eine der drei Bedingungen gebrochen ist, hört Tit-for-Tat auf, die optimale Strategie zu sein, und Defektion wird rational.

Wenn wir also ein verteiltes System bauen und wollen, dass darin Kooperation ohne zentralen Schiedsrichter funktioniert – müssen wir es so gestalten, dass alle drei Bedingungen erfüllt sind. Wiederholung, Gedächtnis, Klarheit.

Das klingt wie ein Rezept. Und es ist fast eines. Aber es gibt eine Nuance, die weder Axelrod noch Rapoport noch irgendjemand, der ihre Arbeit in den 1980er-Jahren las, hätte vorhersehen können.

Was ungeklärt blieb

Wenn alles so einfach ist – drei Bedingungen, vier Eigenschaften, eine optimale Strategie –, warum haben wir dann am Ende von Kapitel 1 gesagt, dass Bitcoin einen strukturellen Mangel hat? Schließlich sind in ihm die drei Bedingungen erfüllt.

Die Antwort: Axelrods drei Bedingungen sind eine notwendige Bedingung für Kooperation. Aber keine hinreichende.

Bitcoin erfüllt Axelrod. Es gibt darin Wiederholung, Gedächtnis und Klarheit, und Tit-for-Tat funktioniert dort. Das erklärt, warum das Netzwerk 2014 überlebte.

Aber es gibt noch einen weiteren Faktor, über den Axelrod nicht schrieb, weil man ihn 1980 nicht sehen konnte. Dieser Faktor hängt nicht mit den Bedingungen des Spiels zusammen, sondern damit, was in diesem Spiel genau gewonnen wird. Mit dem Preis selbst.

In Axelrods Turnier war der Preis abstrakt – Punkte. Die Programme konnten diese Punkte nicht gegen etwas anderes eintauschen, etwas Asymmetrisches. Sie konnten zum Beispiel ihre Punkte nicht dazu verwenden, um Stimmen bei der Festlegung künftiger Turnierregeln zu kaufen. Sie konnten sich ihre Reputation nicht erkaufen.

In Bitcoin ist der Preis echtes Geld. Und dieses Geld kann unter anderem dazu verwendet werden, das System selbst zu beeinflussen. Um mehr Ausrüstung zu kaufen. Um sich einen größeren Anteil zu

sichern. Um bestimmte Änderungen am Protokoll durchzusetzen. Um die Branche in eine bestimmte Richtung zu lenken.

Das schafft ein anderes Problem. Nicht das Problem des Fehlens der drei Bedingungen – die drei Bedingungen sind erfüllt. Sondern das Problem, dass der Preis des Spiels selbst eine Asymmetrie in sich trägt, die es im Turnier von 1980 nicht gab. Der Preis verleiht die Fähigkeit, die Spielregeln zu ändern. Und das ist eine Klasse von Angriff, die Axelrod nicht modellierte.

Genau dieser Mangel – strukturell, subtil, fast unsichtbar – ist der Grund, warum Bitcoin bei all seinen bemerkenswerten Eigenschaften in der Darby-Phase bleibt, nicht in der Murdoch-Phase. Es löst das Problem der Kooperation zwischen Teilnehmern innerhalb des Rahmens des aktuellen Spiels. Aber es löst nicht das Problem, dass das in diesem Spiel verdiente Geld dazu benutzt werden kann, das Spiel selbst zu verändern.

Doch bevor wir weitergehen, lohnt es sich, kurz innezuhalten. Denn wir haben etwas Wichtiges hergeleitet.

Kooperation ohne Schiedsrichter ist möglich. Das ist keine Utopie und keine Mystik. Es ist eine mathematische Tatsache, bewiesen 1980 in einem Turnier, an dem vierzehn Programme teilnahmen. Sie erfordert drei Bedingungen – Wiederholung, Gedächtnis, Klarheit – und eine Strategie aus vier Zeilen Code.

Und wenn wir Systeme bauen wollen, in denen Millionen Menschen ohne Zwang im gemeinsamen Interesse handeln, wissen wir jetzt, woraus wir sie bauen können.

Das ist die erste gute Nachricht in diesem Buch.

Das nächste Kapitel handelt von der schlechten Nachricht.

3
Warum Bitcoin sich nicht selbst reparieren kann



Ein Gen, das man nicht von innerhalb der Zelle reparieren kann

Stellen Sie sich einen Organismus vor. Er hat DNA. Die DNA kodiert Proteine. Die Proteine bauen Zellen auf, die Zellen bauen Organe auf, die Organe bilden den Organismus. Gibt es einen Fehler in der DNA – sagen wir, ein Buchstabe ist falsch –, wird dieser Fehler in jeder Zelle reproduziert, denn jede Zelle kopiert dieselbe DNA. Die Folgen können von unmerklich bis katastrophal reichen, aber eines ist klar: Keine Zelle innerhalb dieses Organismus kann den DNA-Fehler beheben. Dafür braucht man jemanden von außen, mit anderen Werkzeugen.

Genau das ist Bitcoins Situation gerade jetzt. Es hat seine ursprüngliche Konstruktion – Proof-of-Work mit anonymen Minern und einem offenen Protokoll. Diese Konstruktion löste Satoshis konkretes Problem – digitales Geld ohne Bank in der Mitte zu schaffen. Und sie löste es brillant. Aber sie hat einen Nebeneffekt: Alles, was innerhalb des Systems verdient wird, kann außerhalb davon verwendet werden, und das System hat keinen Mechanismus, sich dagegen zu wehren, dass dieses Verdienen das System selbst verändert.

Ich werde versuchen, das auf drei verschiedenen Ebenen zu zeigen. Erstens – auf der Ebene der Rechenleistung, wo Geld, das durchs Mining verdient wurde, noch mehr Mining kauft und sich in wenigen Händen konzentriert. Dann – auf der Ebene des Eigentums, wo dasselbe Geld, nachdem es Börsen und Fonds durchlaufen hat, als große institutionelle Positionen zurückkommt. Und schließlich – auf der Ebene der Entwicklung, wo dasselbe Geld die Ingenieure bezahlt, die das Protokoll selbst schreiben.

Drei Ebenen. Derselbe Mechanismus. Und auf jeder von ihnen – ein struktureller Widerspruch zwischen dem, was Bitcoin in seiner ursprünglichen Konstruktion verspricht, und dem, was tatsächlich dabei herauskommt.

Ebene eins: Wer zählt

Beginnen wir mit dem Mining.

Als Satoshi 2009 Bitcoin startete, schien er aufrichtig zu glauben, dass Mining von Tausenden Menschen an Heimcomputern betrieben würde, jeder unabhängig für sich. „Eine CPU – eine Stimme“, schrieb er im Whitepaper. Ein Prozessor, eine Stimme. Jeder Teilnehmer des Netzwerks verteidigt es mit seinem

kleinen Anteil an Leistung, und niemand hat einen Vorteil gegenüber irgendjemand anderem. 2009–2010 funktionierte es tatsächlich so – Satoshi selbst schürfte auf einem gewöhnlichen Laptop und erhielt die volle Blockbelohnung.

Dieses Bild starb sehr schnell. 2010 fand jemand heraus, dass sich Grafikkarten fürs Mining nutzen ließen – sie hashen Dutzende Male schneller als Prozessoren. 2011 erschienen die ersten FPGA-Miner, noch einmal mehrfach schneller. 2013 brachte Bitmain den ersten ASIC heraus – einen integrierten Schaltkreis, der auf eine einzige Operation zugeschnitten ist, das SHA-256-Hashing. Der ASIC war tausendmal effizienter als eine GPU. Heimcomputer waren aus dem Spiel. Auch Grafikkarten. Nur noch ASIC-Farmen blieben übrig.

Bis 2016 war der Großteil des Minings nach China abgewandert, wo Strom billig war und die lokalen Behörden sich noch nicht einmischten. Bis 2021 hatte China Mining verboten, und die Industrie verlagerte sich nach Texas, Kasachstan, Russland, Iran, Island. Bis 2024 – nach einem weiteren „Halving“, bei dem die Blockbelohnung von 6,25 auf 3,125 BTC halbiert wurde – wurden die kleinen Betreiber endgültig verdrängt. Nur die großen Industriefarmen überlebten: solche mit langfristigen Verträgen für Großstrom, eigener Kühlinfrastruktur und Ingenieurteams.

Stand April 2026 sieht das Bild so aus.

Ganz oben – Mining-Pools. Das sind Zusammenschlüsse von Minern, die ihre Rechenleistung bündeln und die Belohnung teilen. Von allen Minern der Welt, die an Bitcoin arbeiten, bedient Foundry USA etwa 29 Prozent. AntPool (im Besitz von Bitmain, dem größten ASIC-Hersteller) bedient weitere rund 21 Prozent. ViaBTC – etwa 11. F2Pool – etwa 10. SpiderPool – etwa 7. MARA Pool und SecPool – je 6.

Die ersten beiden Pools kontrollieren zusammen etwa die Hälfte der gesamten Bitcoin-Hashrate. Die ersten vier – etwa siebzig Prozent.

Das ist eine grundlegend wichtige Zahl, und es lohnt sich, einen Moment bei ihr zu verweilen.

Wenn ein Pool einen bestimmten Anteil der Hashrate kontrolliert, entscheidet er im Wesentlichen, welche Transaktionen in den Block aufgenommen werden. Der Pool schürft die Blöcke nicht selbst – das tun die mit ihm verbundenen Miner. Aber der Pool erstellt die „Block-Vorlage“ – die Liste der Transaktionen, die der Miner dann zu hashen versucht. Findet der Miner zufällig den richtigen Hash, wird der Block mit den vom Pool ausgewählten Transaktionen veröffentlicht.

Mit anderen Worten: Vier Organisationen – Foundry, AntPool, ViaBTC, F2Pool – entscheiden, welche Transaktionen in siebzig Prozent aller Bitcoin-Blöcke gelangen. Das ist keine Bedrohung des Netzwerks im Sinne von „sie könnten es zerstören“. Es ist viel subtiler: Sie können langsam, Transaktion für Transaktion, entscheiden, wer mehr für das Recht bezahlt, in einen Block zu gelangen, wessen Transaktionen zuerst verarbeitet werden und wessen stecken bleiben. Sie können (und tun das gelegentlich) Transaktionen von sanktionierten Adressen ausschließen – zum Beispiel Adressen auf der Schwarzen Liste des US-Finanzministeriums. Sie können (und das ist bereits geschehen) bestimmten Arten von Transaktionen Priorität geben, die höhere Gebühren einbringen.

Und hier ist die Sache – sie können all das tun, ohne eine einzige Protokollregel zu brechen. Sie nutzen einfach den Umstand aus, dass sie über viel Hashrate verfügen. Und sie haben viel Hashrate, weil sie diese in vorherigen Blöcken verdient und in weitere Ausrüstung, billigeren Strom und bessere Ingenieure

reinvestiert haben.

Das Spiel belohnt Gewinner mit Geld. Geld kauft mehr Ausrüstung. Mehr Ausrüstung gibt mehr Hashrate. Mehr Hashrate – mehr Siege. Der Kreis schließt sich.

Beachten Sie, dass dieser Kreislauf keine der Axelrod-Bedingungen verletzt. Die drei Bedingungen – Wiederholung, Gedächtnis, Transparenz – sind weiterhin erfüllt. Alle zehn Minuten entstehen neue Blöcke (Wiederholung). Alles wird für immer in der Blockchain verzeichnet (Gedächtnis). Die Hashrate jedes Pools ist öffentlich sichtbar (Transparenz). Alles ist in Ordnung.

Aber innerhalb dieser perfekt funktionierenden Architektur läuft ein Konzentrationsprozess ab, der von den Regeln von Tit-for-Tat nicht erfasst wird. Denn TfT ist eine Strategie für gleichberechtigte Spieler. Sie sagt nichts darüber, was zu tun ist, wenn einer der Spieler zwanzigmal größer ist als ein anderer. In Axelrods Turnier hatten alle Programme gleiche Startbedingungen. Im echten Bitcoin – haben sie das nicht.

Ebene zwei: Wem gehört es

Schauen wir uns nun eine andere Ebene an.

Bitcoin besteht nicht nur aus Minern – sondern auch aus Holdern. Menschen, die einfach Coins besitzen und in eigenen Wallets oder auf Börsen aufbewahren. Theoretisch sollte die Verteilung gleichmäßig sein, da jeder Bitcoin identisch ist. In der Praxis – ist sie das nicht.

Im Januar 2024 genehmigte die US-Börsenaufsicht SEC erstmals Spot-Bitcoin-ETFs (börsengehandelte Fonds). Das war der Höhepunkt jahrelangen Drucks großer Vermögensverwalter – BlackRock, Fidelity, Grayscale –, die ihren institutionellen Kunden Bitcoin über die gewöhnliche Broker-Infrastruktur verkaufen wollten, ohne sich mit Krypto-Börsen und Cold Wallets befassen zu müssen. BlackRock ist die weltweit größte Vermögensverwaltungsgesellschaft; sie verwaltet in der Größenordnung von 11 Billionen Dollar. Das ist mehr als das BIP jedes Landes außer den Vereinigten Staaten und China. Als BlackRock am 11. Januar 2024 seinen Bitcoin-ETF unter dem Ticker IBIT startete, strömte Geld hinein wie ein Fluss.

Stand April 2026 – zwei Jahre später – hält IBIT etwa 800.000 Bitcoin, was rund 63 Milliarden Dollar beim aktuellen Kurs entspricht. Das sind rund 49 Prozent aller Vermögenswerte in allen US-Spot-Bitcoin-ETFs zusammen. Allein im ersten Quartal 2026 verzeichnete IBIT Nettozuflüsse von 8,4 Milliarden Dollar.

Doch IBIT ist nicht der einzige große Halter. Das Unternehmen Strategy (früher MicroStrategy, eine Business-Analytics-Firma, die sich dann zu einer reinen Bitcoin-Treasury neu erfand) besitzt Stand 17. April 2026 815.000 Bitcoin mit Gesamtanschaffungskosten von 61,56 Milliarden Dollar. Das sind etwa vier Prozent des gesamten jemals existierenden Bitcoins. Keine einzelne Instanz in der Geschichte hat einen solchen Anteil gehalten – abgesehen vielleicht von Satoshi selbst, dessen Coins sich seit 2010 nicht bewegt haben.

Zählt man alles zusammen, was US-Spot-ETFs halten, kommt man auf etwa 1,31 Millionen Bitcoin – rund 6,2 Prozent der Gesamtmenge. Rechnet man Strategy hinzu – kommt man auf mehr als zehn Prozent. Rechnet man die großen Börsen (Coinbase, Binance), Unternehmens-Treasury-Positionen und

große Privatbestände hinzu – stellt sich heraus, dass ein paar Dutzend Instanzen ein Viertel des gesamten Bitcoins ausmachen.

Was bedeutet das in der Praxis?

Es bedeutet, dass, wenn BlackRock eines schönen Tages auf Anweisung eines Regulierers beschließt, die Vermögenswerte von IBIT einzufrieren – acht Prozent des gesamten Bitcoins augenblicklich illiquide werden. Das ist ein Marktschock einer Größenordnung, die Bitcoin bisher noch nicht erlebt hat. Es bedeutet, dass, wenn Strategy einen Margin Call auf seine Kredite erhält (und das Unternehmen hat Kredite aufgenommen, um Bitcoin zu kaufen), es gezwungen sein könnte, 815.000 Coins zu liquidieren – was den Kurs augenblicklich mehrfach zum Absturz bringen würde. Es bedeutet, dass, wenn die US-Regierung beschließt, Bitcoin mit neuer Gesetzgebung zu regulieren, der Hauptkanal des Einflusses nicht mehr dezentrale Miner in Kasachstan sind, sondern BlackRock in New York, wo ein Anruf im richtigen Büro das Verhalten von Billionen Dollar verändern kann.

Das Paradoxe daran: Bitcoin wurde als ein Netzwerk konzipiert, das gegen zentralisierten Druck resistent ist. Dezentralisierung war kein Nebeneffekt, sondern eine zentrale Anforderung. Und doch haben wir sechzehn Jahre später eine Konstruktion, in der wenige große institutionelle Akteure einen so großen Anteil am Angebot kontrollieren, dass sie strukturell mehr Einfluss auf Preis, Liquidität und die regulatorische Agenda ausüben können als der Rest des Marktes zusammen.

Wie kam es dazu?

Auf dieselbe Weise wie beim Mining. Jede einzelne Geldbewegung war freiwillig und individuell rational. Ein Pensionsfonds wollte Bitcoin-Exposure, konnte die Coins aber aus regulatorischen Gründen nicht direkt halten – kaufte IBIT. Ein Family Office wollte Diversifikation – kaufte IBIT. Ein Unternehmen wollte eine Absicherung gegen Inflation – kaufte IBIT. Niemand wurde gezwungen, niemand wurde manipuliert. Jede einzelne Entscheidung wirkte vernünftig.

Aber das Gesamtergebnis von Millionen solcher individuell rationaler Entscheidungen ist eine gigantische Konzentration. Die nun selbst zu einem Faktor in der Gleichung wird. Denn je mehr Bitcoin BlackRock besitzt, desto mehr Stimme hat BlackRock in jeder öffentlichen Diskussion darüber, was Bitcoin in Zukunft sein soll. Und diese Stimme ist nicht dieselbe wie die eines gewöhnlichen Holders. Es ist eine Stimme, auf die man bei der SEC, im Kongress, bei der Federal Reserve hört.

Ebene drei: Wer schreibt

Die dritte Ebene ist die unsichtbarste, aber die wichtigste.

Bitcoin ist Code. Dieser Code wird von Menschen geschrieben. Es sind nicht sehr viele. Laut einem BitMEX-Research-Bericht aus dem Jahr 2024 arbeiteten an dem gesamten Bitcoin – das zu diesem Zeitpunkt etwa anderthalb Billionen Dollar wert war – 41 Entwickler aktiv: solche, die im Laufe des Jahres mindestens fünf Commits in das Haupt-Repository von Bitcoin Core eingereicht hatten. Einundvierzig Menschen, auf anderthalb Billionen.

Von diesen einundvierzig leben etwa zwei Drittel in den USA und Europa. Drei Entwickler – in Lateinamerika (Argentinien, Brasilien, El Salvador). Vier – im Rest der Welt. Das sind Tier-1-Statistiken, gewonnen aus öffentlichen Commit-Daten.

Wer finanziert sie?

Bitcoin hat keine Stiftung. Keine zentrale Organisation. Keine sprichwörtliche Kasse, aus der Gehälter gezahlt werden. Das war ganz nach Satoshis Entwurf – damit niemand die Entwicklung stoppen kann, indem er die Finanzierung entzieht. Aber Programmierer müssen leben, und sie werden aus verschiedenen Quellen bezahlt.

Blockstream. Ein 2014 gegründetes Unternehmen. Unter seinen Gründern – Gregory Maxwell, Pieter Wuille, Matt Corallo, Jorge Timón, Mark Friedenbach (alles aktive Bitcoin-Core-Entwickler) sowie Adam Back (der Erfinder von Hashcash, auf dem Satoshi Bitcoins PoW aufbaute) und der Venture-Investor Austin Hill. Seit seiner Gründung hat Blockstream insgesamt mehr als eine halbe Milliarde Dollar an Investitionen eingesammelt – 76 Millionen Dollar bis 2017, 210 Millionen Dollar in einer Series-B-Runde 2021, weitere 210 Millionen Dollar in Wandelanleihen 2024. Das Unternehmen hat offensichtlich mehrere zentrale Core-Entwickler auf seiner Gehaltsliste. Adam Back, sein Präsident, erklärt das so: Das Unternehmen habe ein Interesse daran, dass Bitcoin unterstützt, entwickelt und skaliert wird.

Chaincode Labs. Ein Forschungszentrum in New York, das mehrere weitere zentrale Entwickler finanziert.

MIT Digital Currency Initiative. Ein akademisches Dach am MIT Media Lab; es entstand um 2015 als Reaktion auf die Finanzierungskrise unter Core-Entwicklern nach dem Zusammenbruch der Bitcoin Foundation.

Brink, OpenSats, Spiral, Human Rights Foundation. Gemeinnützige Förderprogramme.

Große Börsen – Coinbase, OKCoin, OKX. Vergeben gelegentlich Zuschüsse.

Die gesamte jährliche Finanzierung der Bitcoin-Core-Entwicklung wird auf 150–200 Millionen Dollar pro Jahr geschätzt – für ein Netzwerk, das mehr als eine Billion wert ist. Zum Vergleich: Die Ethereum Foundation gab 2024 etwa 50 Millionen für Entwicklung aus, bei einer Marktkapitalisierung, die zehnmal kleiner ist als die von Bitcoin. Polkadot – 16 Millionen, bei einer hundertmal kleineren Marktkapitalisierung. Pro verteidigtem Dollar an Kapitalisierung unterfinanziert Bitcoin seine Entwicklung um eine Größenordnung.

Und – hier wird es subtil – ein unverhältnismäßig großer Anteil der bescheidenen vorhandenen Finanzierung fließt über Blockstream. Ein Unternehmen, das eigene kommerzielle Produkte hat: Liquid (eine Sidechain für Finanzinstitute), das Lightning Network (eine L2 für schnelle Zahlungen), Mining-Hardware, institutionelle Dienstleistungen. Die Interessen dieser Produkte fallen manchmal mit den Interessen eines gewöhnlichen Bitcoin-Nutzers zusammen, manchmal nicht.

Ein klassisches Beispiel sind die Debatten von 2023–2024 um das Ordinals-Protokoll, das es ermöglichte, beliebige Daten (Bilder, NFT-Sammlungen, sogar Bücher) auf die Bitcoin-Blockchain zu schreiben. Technisch geschah dies über Taproot – ein Protokoll-Upgrade, das Core-Entwickler 2021 für

andere Zwecke auslieferten, das Casey Rodarmor jedoch Anfang 2023 auf unerwartete Weise nutzte. Ordinals beanspruchte schnell einen erheblichen Anteil des Blockplatzes, trieb die Gebühren in die Höhe und veränderte die Ökonomie des Netzwerks.

Einer der leitenden Core-Entwickler, Luke Dashjr, reichte einen Pull Request ein, der Ordinals technisch eingeschränkt hätte. Eine andere Maintainerin, Ava Chow (eine ehemalige Blockstream-Mitarbeiterin), schloss den PR mit der Begründung „fehlender Konsens und Erzeugung von Lärm“. Die Community spaltete sich. Manche hielten Ordinals für eine kreative Nutzung des Netzwerks. Andere – für Parasitismus am Blockplatz, der für monetäre Transaktionen gedacht war. Die Entscheidung wurde formal von einer Person getroffen. Diese Entscheidung konnte von niemandem außer dem Maintainer selbst oder einem anderen Maintainer mit gleichen Rechten rückgängig gemacht werden.

Ordinals brach keine einzige Bitcoin-Regel. Aber es veränderte radikal, wie die Blockchain genutzt wird. Und diese Veränderung geschah nicht durch eine Abstimmung der Miner, nicht durch ein Referendum der Holder, sondern durch die individuelle Entscheidung weniger Entwickler mit Commit-Zugang. Die von bestimmten Unternehmen bezahlt werden. Die eigene geschäftliche Interessen haben.

Formal bleibt das Netzwerk dezentral – es hat keinen CEO, keine Stiftung, keinen Vorstand. Tatsächlich trifft ein enger Kreis von Menschen, finanziell an eine begrenzte Anzahl von Unternehmen gebunden, Entscheidungen, die Billionen von Dollar an Kapital und Millionen von Nutzern betreffen.

Und wieder – das ist niemandes böse Absicht. Es ist einfach eine Folge davon, wie die Entwicklungsökonomie aufgebaut ist. Bitcoin bezahlt Entwickler nicht aus seinen Blöcken. Sie werden von externen Unternehmen bezahlt. Die Unternehmen haben Interessen. Die Interessen konzentrieren sich. Die von diesen Unternehmen versorgten Entwickler sammeln sich um die Aufgaben, die diese Unternehmen als Priorität ansehen. Unabhängig davon, wie gut diese Aufgaben mit Bitcoins Aufgaben als öffentliches Gut übereinstimmen.

Die drei Ebenen zusammen

Betrachtet man die drei Ebenen gemeinsam, wird eine gemeinsame Struktur sichtbar.

Auf der Mining-Ebene – Geld, das in vorherigen Blöcken verdient wurde, kauft mehr Hashrate. Mehr Hashrate gibt mehr Einfluss darauf, welche Transaktionen in Blöcke gelangen.

Auf der Eigentumsebene – Geld, das durch Mining oder Kurssteigerungen verdient wurde, kauft über institutionelle Instrumente mehr Coins. Mehr Coins geben mehr Stimme in der öffentlichen Diskussion über Bitcoins Zukunft.

Auf der Entwicklungsebene – Geld, das an Börsen, in ETFs, in der Mining-Infrastruktur verdient wurde, finanziert Entwickler. Die Entwickler, die dieses Geld erhalten, entscheiden, wohin sich das Protokoll bewegt.

Auf jeder der drei Ebenen wirkt derselbe Mechanismus: Ein interner Gewinn wird in externen Einfluss umgewandelt. Und dieser Einfluss wiederum kann genutzt werden, um die Bedingungen der nächsten Spielrunden zum eigenen Vorteil zu verändern.

Genau hier bricht Axelrods Modell zusammen. Nicht weil Tit-for-Tat eine schlechte Strategie wäre. TfT ist für die Situation, die es beschreibt, weiterhin optimal. Aber es beschreibt eine Situation, in der Punkte nicht in das Recht umgewandelt werden können, die Regeln zu ändern. Bitcoin ist eine Situation, in der das möglich ist.

Axelrod konnte das 1980 nicht vorhersehen, denn in seinem Turnier gab es kein Geld. Es gab abstrakte Punkte, die für nichts anderes verwendet werden konnten als für die Ermittlung des Siegers. In einem echten Wirtschaftssystem hingegen können Gewinne immer umgewandelt werden. Die einzige Frage ist, in was, und wie viel.

Unter der Haube. GHash.IO noch einmal

Im ersten Kapitel erzählte ich die Geschichte von GHash.IO im Sommer 2014 – einem Pool, der für einen Tag die 55-Prozent-Schwelle der Bitcoin-Hashrate überschritt und das Netzwerk nicht katastrophal angriff. Im zweiten Kapitel nutzte ich diese Geschichte als Beispiel dafür, wie Tit-for-Tat in der Realität funktioniert – die Community spiegelte die Bedrohung, der Pool zog sich zurück, alles endete gut.

Jetzt – die ganze Wahrheit.

GHash.IO zerstörte Bitcoin nicht. Aber der Pool nutzte seine Mehrheitsposition für einen gezielten Angriff auf einen bestimmten Dienst. Im Herbst 2013, als der Anteil von GHash.IO bereits erheblich, aber noch nicht bei 51 Prozent war, führte der Pool eine Reihe von Double-Spending-Angriffen gegen das Online-Casino BetCoin Dice durch. Die Diskussion darüber im BitcoinTalk-Forum, im Thread Nummer 327767, ist bis heute öffentlich zugänglich. Die Idee ist einfach: GHash.IO akzeptierte verlorene Wetten an seinen Adressen, und wenn es verlor, minte es dieselbe Transaktion mit seiner eigenen (gewinnenden) Adresse in einem anderen Block, wodurch der Verlust zum Gewinn wurde. Die digitale Version dessen, was man in einem physischen Casino „die Runde noch einmal spielen, wenn die Kugel nicht dort stehen blieb, wo sie sollte“ nennt.

BetCoin Dice erlitt reale Verluste. Das stellte die Untersuchung fest. GHash.IO gab formal keine öffentliche Reue zu, aber es gab reputative Konsequenzen: Der Pool hörte auf, Einzahlungen an seinen Adressen zu akzeptieren, und die Community begann, ihn genauer zu beobachten. Diese Geschichte ist einer der Gründe, warum sechs Monate später, als GHash.IO erneut auf den kritischen Anteil zuwuchs, der Druck so schnell und so stark war. Die Leute erinnerten sich.

Das ist eine wichtige Korrektur des Bildes, das in der Bitcoin-Community üblicherweise gezeichnet wird. Man hört oft: „Bitcoin hatte nie einen 51-Prozent-Angriff.“ Das stimmt nur auf einem bestimmten Genauigkeitsniveau. Versteht man unter einem 51-Prozent-Angriff „ein vollständiges Umschreiben der Blockchain-Geschichte über Monate zurück, mit Doppelausgaben aller größeren Transaktionen“ – ja, das ist nicht passiert. Versteht man darunter „die Nutzung einer Mehrheitsposition, um auf Kosten anderer Netzwerkteilnehmer Gewinn zu erzielen“ – dann ist es passiert. Und es ist dokumentiert.

Das ist ein entscheidendes Detail für unser Thema. Denn es zeigt: Der Mechanismus „Gewinne in das Recht umzuwandeln, die Regeln zu ändern“ ist keine theoretische Bedrohung. Er ist bereits ausgelöst worden. Nur in begrenztem Umfang, weil der Pool, der verstand, dass ein vollständiger Bruch das gesamte Netzwerk (und seinen eigenen Gewinn mit ihm) töten würde, bei lokaler Ausnutzung haltmachte.

Lokale Ausnutzung ist in anderer Hinsicht eine schlechte Nachricht. Sie bedeutet, dass ein System, in dem der Inhaber einer Rechenmehrheit die Minderheit ausnutzen kann, selbst ohne die gesamte Konstruktion zu zerstören, strukturell instabil ist – selbst wenn Axelrods drei Bedingungen erfüllt sind. Denn das TfT-Gleichgewicht setzt voraus, dass die Teilnehmer mehr oder weniger auf Augenhöhe spielen. In dem Moment, in dem ein Mehrheitsspieler auftaucht, der einen „gezielten Angriff" ausführen kann – jemandem etwas nehmen, ohne das System als Ganzes zu brechen –, wird er es tun. Rational. Im Einklang mit seinen Anreizen. In voller Übereinstimmung mit der Spieltheorie.

Und dagegen gibt es innerhalb der Mechanik von Bitcoin keine Verteidigung.

Unter der Haube. Monero, August 2025

Das zweite Beispiel ist ein sehr aktuelles. Im August 2025 – also weniger als ein Jahr, bevor diese Zeilen geschrieben werden – geschah etwas, das bestätigte, wovon ich gerade gesprochen habe, jedoch in weit größerem Maßstab. Und es wurde nicht von einer der großen Börsen und nicht von einer Hackergruppe getan, sondern von dem Projekt, um das es in diesem Buch im Grunde geht – Qubic.

Die ganze Geschichte hier nachzuerzählen ist nicht der richtige Ort – das ist Thema von Kapitel fünfzehn. Aber die knappe Tatsache lautet so: Monero ist ein Bitcoin ähnliches Netzwerk, ebenfalls Proof-of-Work, aber mit einem anderen Algorithmus (RandomX, optimiert für gewöhnliche Prozessoren statt für spezialisierte ASICs). Monero hatte zu diesem Zeitpunkt eine Marktkapitalisierung von etwa 6 Milliarden Dollar. Qubics Marktkapitalisierung – etwa 300 Millionen. Ein Verhältnis von 1 zu 20.

Über drei Monate – von Mai bis August 2025 – begann Qubic, über einen Mechanismus, über den wir in Kapitel 8 ausführlich sprechen werden, Monero-Minern das Dreifache dessen zu zahlen, was sie durch direktes Monero-Mining bekamen. Kein Hack. Kein Hacking. Nur eine andere Ökonomie: „Schließ dich unserem Pool an, wir leiten deine Rechenarbeit so um, dass du mehr verdienst."

Die Miner betrachteten die Zahlen. Schlossen ihre Ausrüstung um. Am 11. August 2025 kontrollierte Qubic in einem Fenster von 122 Blöcken 63 von 122 Blöcken – 51,6 Prozent der Hashrate. Das Monero-Netzwerk stand unter der Kontrolle eines Netzwerks, das zwanzigmal kleiner war an Marktkapitalisierung.

Was danach geschah, ist eine eigene Geschichte. Qubic zerstörte Monero nicht. Aber die technische Möglichkeit der Zerstörung war gegeben, und in einer öffentlichen Erklärung vom 3. August 2025 legten die Qubic-Entwickler genau dar, was sie hätten tun können, wenn sie gewollt hätten: Double-Spending gegen Börseneinzahlungen, das Umschreiben der Blockgeschichte, das Zensieren von Transaktionen, den Kurs auf null abstürzen lassen. Sie taten es nicht. Sie beschlossen aufzuhören. Aber sie hätten es gekonnt.

Für unser Kapitel – und insbesondere für die Frage, warum Bitcoin sich nicht selbst reparieren kann – ist das die entscheidende Episode. Denn sie beweist empirisch, nicht theoretisch: Jedes PoW-Netzwerk kann angegriffen werden, indem man seinen Minern eine bessere Ökonomie bietet. Die Qubic-Entwickler formulierten dies, als sie das Experiment zusammenfassten, als eine von drei bewiesenen Thesen:

„Anreize diktieren den Konsens: Jede Proof-of-Work-Blockchain kann angegriffen und kontrolliert werden, indem man ihren Minern überlegene wirtschaftliche Anreize bietet."

Das ist eine entscheidende Aussage. Sie besagt nicht „Bitcoin ist schwach" – Bitcoin ist stark, und genau deshalb ist es teurer, es anzugreifen. Sie besagt „kein PoW-Netzwerk ist strukturell geschützt". Der Schutz ist einfach Geld. Mehr Geld – mehr Schutz. Jemand mit mehr Geld kann diesen Schutz aufkaufen. Und Geld, erinnere ich, ist genau das, was sich bei denjenigen ansammelt, die das Spiel bereits gewonnen haben.

Der Kreis schließt sich.

Was das für unsere Geschichte bedeutet

Lassen Sie mich alles zusammenfassen.

Das erste Kapitel endete mit dem Punkt, dass Bitcoin eine Revolution vollbrachte – dabei aber „Murdochs Gas" in der Luft ließ, Rechenzyklen, die niemand braucht. Das war eine schlechte Nachricht über die Nutzung einer Ressource.

Das zweite Kapitel brachte eine gute Nachricht: Kooperation ohne Schiedsrichter ist möglich, wenn Axelrods drei Bedingungen erfüllt sind, und Bitcoin erfüllt diese Bedingungen im Großen und Ganzen.

Das dritte Kapitel – also dieses hier – besagt: Die schlechte Nachricht ist tiefer, als wir im ersten Kapitel dachten. Bitcoin nutzt seine Ressource nicht nur ineffizient. Es ist auch strukturell unfähig, sich selbst zu reparieren, weil das intern verdiente Geld ständig in externe Macht umgewandelt wird, und diese Macht als Fähigkeit zurückkehrt, die Regeln zu ändern. Konzentration des Minings. Konzentration des Eigentums. Konzentration der Entwicklung. Drei Ebenen, dieselbe Dynamik.

Man könnte sagen, das sei nur das allgemeine Problem des Kapitalismus, und Bitcoin sei darin nicht einzigartig. Das wäre richtig, wenn Bitcoin nicht das Gegenteil versprochen hätte. Hat es aber. Es versprach, dass jeder Prozessor eine Stimme wäre. Dass Mining dezentral ist. Dass niemand das Netzwerk kontrolliert. Dass das von ihm produzierte Geld neutral und gegen jede Politik resistent ist. Sechzehn Jahre später ist all das entweder bereits unwahr oder wird direkt vor unseren Augen unwahr.

Und nicht, weil Satoshi sich geirrt hätte. Er irrte sich nicht – er löste ein konkretes Problem, und er löste es. Nur ist seine Lösung die Darby-Phase. Der erste große Durchbruch. Er öffnet Türen, die vorher verschlossen waren. Aber er hat eine strukturelle Grenze, die man von innen nicht überschreiten kann. Die Murdoch-Phase ist bereits ein anderes technisches Problem, mit anderen Bedingungen.

Und hier kommen wir zur Hauptfrage dieses Kapitels.

Die vierte Bedingung

Axelrod beschrieb 1980 drei Bedingungen, unter denen Kooperation möglich ist: Wiederholung, Gedächtnis, Transparenz. Über eine vierte schrieb er nicht, weil diese Bedingung in seinem Turnier automatisch erfüllt war – die Programme spielten in einem geschlossenen System, in dem Gewinne in nichts Externes umgewandelt werden konnten. In der realen Welt kann diese Bedingung erfüllt sein oder nicht – und genau das ist der entscheidende Unterschied zwischen Systemen, die kooperativ bleiben, und

Systemen, die zur Oligopolisierung tendieren.

Lassen Sie mich versuchen, diese Bedingung explizit zu formulieren:

Das System muss so aufgebaut sein, dass Gewinne innerhalb des Spiels nicht in das Recht umgewandelt werden können, das Spiel selbst zu verändern.

Oder kürzer: Die Grenze zwischen „dem Preis“ und „den Regeln“ darf von innen nicht überschreitbar sein.

In Axelrods Turnier war diese Grenze absolut – Punkte und Regeln lebten in verschiedenen Welten. In Bitcoin ist diese Grenze eine durchlässige Membran. Internes Geld sickert ständig nach außen, erwirbt externen Einfluss und kommt bereits als Druck auf die Regeln zurück. Allmählich. Jahr für Jahr.

Diese vierte Bedingung ist keine Verbesserung an Axelrod. Sie ist eine Ergänzung. Die drei ursprünglichen Bedingungen bestimmen, ob Kooperation das Gleichgewicht zwischen Spielern sein wird. Die vierte bestimmt, ob diese Gleichgewichtsstruktur über die Zeit erhalten bleibt oder ob sie allmählich zu einem neuen Gleichgewicht abdriftet, in dem wenige spielen und viele sich unterordnen. Es geht um die Dauerhaftigkeit der Dauerhaftigkeit selbst.

Wenn wir ein System bauen wollen, das nicht nur Axelrods drei Bedingungen erfüllt, sondern auch die vierte, brauchen wir eine anders gebaute Architektur. Nicht „ein verbessertes Bitcoin“. Nicht „Bitcoin mit einem Patch gegen Konzentration“. Eine grundlegend andere Konstruktion, in der der Mechanismus des Gewinnens selbst so gebaut ist, dass er keine Konzentration erzeugt.

Das ist ein nichttriviales technisches Problem. Die naive Lösung – den Verkauf von Bitcoin an große Investoren zu verbieten – funktioniert nicht, weil sie die erste Eigenschaft zerstört (einen freien Markt). Die naive Lösung – die Entwickler ein Gehalt aus dem Protokoll beziehen zu lassen – funktioniert teilweise, stößt aber auf die Frage, wer entscheidet, wen man bezahlt. Die naive Lösung – Mining-Pools zu verbieten – funktioniert nicht, weil sie die Fähigkeit kleiner Miner zerstört, am Netzwerk teilzunehmen.

Was gebraucht wird, ist eine Architektur, in der die Antwort auf all diese Fragen in den Mechanismus eingebaut ist, mit dem das Netzwerk selbst funktioniert, anstatt durch eine Abstimmung oder eine autoritative Anweisung entschieden zu werden. Wo der Mining-Prozess selbst Dezentralisierung statt Konzentration erzeugt. Wo der Eigentumsprozess selbst Oligopolisierung unter großen Haltern verhindert. Wo der Entwicklungsprozess selbst von der gesamten Community abhängt und nicht von einer engen Gruppe von Sponsoren.

Eine solche Architektur existiert. Sie heißt Qubic. Und wie sie funktioniert, ist Gegenstand dieses Buches von Kapitel sechs bis zum Ende.

Doch bevor wir darüber sprechen, wie sie funktioniert, müssen wir über den Mann sprechen, der sie geschaffen hat. Nicht, weil die Geschichte des Projekts ohne die Geschichte des Mannes unvollständig wäre – sondern weil dieser Mann Bitcoins strukturellen Mangel nicht erst 2025 sah, als er für alle offensichtlich wurde, und nicht 2020, als er in den Daten sichtbar zu werden begann. Er sah ihn in den frühen 2010er-Jahren, als Bitcoin noch jung war und niemand daran zweifelte, dass es für immer dezentral bleiben würde. Er sah ihn – und deshalb konnte er zwei Krypto-Netzwerke bauen, die ganz oben im Allzeit-ICO-Ranking landeten: das erste auf Platz eins, das zweite auf Platz zwei. Mehr als eine

Million Prozent Rendite bei dem einen, vierhunderttausend beim anderen.

Und aus diesen beiden Netzwerken nahm er ein Verständnis dafür mit, wie Krypto-Projekte genau von innen heraus sterben.

Sein Name ist Come-from-Beyond, und er kam wirklich von jenseits.

TEIL II

Der Mann

4
Come-from-Beyond vor Bitcoin

Diese Geschichte mag in kleinen Details davon abweichen, wie ihr Protagonist sie selbst erzählen würde. Manches hat er nie öffentlich bestätigt, manches erst Jahre später und beiläufig, manches hat er absichtlich in der Schwebe gelassen. Ich habe sie aus Forumsarchiven, späten Interviews, hingeworfenen Bemerkungen, technischen Spuren im Code dreier Netzwerke und den wenigen Fakten zusammengesetzt, die ich selbst überprüfen konnte. Irgendwo liege ich wahrscheinlich falsch. Sollte er dies je lesen und sagen „nicht ganz“, dann ist es nicht ganz. Aber die grobe Linie ist diese.

Es gibt eine Eigenheit bei Menschen, die sich später als richtig erweisen: Sie sehen etwas früher als andere, und in dem Moment, in dem sie es sehen, glaubt ihnen niemand. Galilei, der durch sein Fernrohr die Jupitermonde betrachtet. Semmelweis, der von Chirurgen forderte, sich die Hände zu waschen. Turing, der behauptete, eines Tages werde eine Maschine besser Schach spielen als ein Mensch.

Der Held dieses Kapitels ist kein Galilei und kein Turing. Er entdeckte keine Naturgesetze. Er war einfach einer von tausend Programmierern, die 2010 das BitcoinTalk-Forum lasen und herauszufinden versuchten, was für eine seltsame Sache dieser berüchtigte Satoshi Nakamoto da gerade gestartet hatte. Der Unterschied ist: Die meisten dieser tausend Programmierer sahen ein Wunder. Er – ein, zwei Jahre später – sah einen Riss.

Das ist eine ungewöhnliche Fähigkeit. Einen Mangel in etwas zu sehen, das alle anderen bewundern, und nicht zu sagen „aber es funktioniert doch, also ist alles gut“. Zu sagen „ja, es funktioniert, aber genau hier wird es ein Problem geben – nicht morgen, aber in zehn Jahren“. Und anzufangen, etwas anderes zu bauen, während ringsherum noch alle feiern.

Ich habe diese Person am Ende des vorigen Kapitels genannt: Come-from-Beyond. Ein Handle, das schon Anfang der 2000er angenommen wurde. Wie bei Satoshi ist das Handle hier keine Art, sich zu verstecken – es ist eine Art zu unterschreiben. Das ist eine eigene, merkwürdige Parallele, auf die wir zurückkommen werden.

Dieses Kapitel handelt davon, was diese Person tat, bevor Bitcoin in ihr Blickfeld geriet. Was ihr Hintergrund war. Warum sie zur richtigen Zeit am richtigen Ort mit dem richtigen Werkzeugkasten landete, um Bitcoins Mängel früher zu sehen als jeder andere in der Branche. Und warum er bis 2013 – als er selbst zum ersten Mal auf die Bühne trat – bereits alles hatte, was er brauchte, um etwas grundlegend anderes zu bauen.

Ein Programmierer aus den Neunzigern

Verfolgt man die Fußspuren rückwärts, reichen die frühesten, die Come-from-Beyond hinterließ, bis in die späten 1990er-Jahre zurück. Ein osteuropäischer jugendlicher Programmierer, der an einem großen Spieleprojekt arbeitete, das nie erschien. In einer seiner Bemerkungen viele Jahre später wird er erwähnen, dass dieses Projekt fünfundzwanzig Jahre zurückliegt – also irgendwann um 1999. „Es wurde für eines meiner ersten großen Spiele geschrieben, das nie veröffentlicht wurde. ~25 Jahre her." Ein großes Spiel, Gruppenarbeit, hat es nicht zur Veröffentlichung geschafft. Das klassische Schicksal früher 3D-Spiele jener Zeit.

Um den Kontext zu verstehen, lohnt es sich, ein paar Worte darüber zu sagen, wie Programmieren in Osteuropa um die Jahrtausendwende aussah. Ende der 1990er war in den Ländern des ehemaligen sozialistischen Blocks eine Generation entstanden, die einen Computer zu Hause hatte, ein mehr oder weniger stabiles Internet und Zugang zu jedem Lehrbuch oder Quellcode, den man finden konnte. Gleichzeitig hatte diese Generation fast keine institutionelle Karriereinfrastruktur – kein Silicon Valley in der Nähe, kein Risikokapital, keine Praktikumsprogramme bei großen Firmen. Die Leute brachten sich selbst alles bei, arbeiteten remote für westliche Kunden oder für lokale Arbeitgeber und erfanden sich ihre eigenen Probleme.

Das erwies sich als sehr produktives Umfeld – in dem Sinne, dass es Menschen hervorbrachte, die daran gewöhnt waren, Probleme zu lösen, für die niemand bezahlt, ohne externe Bestätigung, aus eigenem Interesse. Eine Gewohnheit, die in etablierteren Ökosystemen selten ist.

Come-from-Beyond war einer davon. Er spielte Ultima Online – eines der ersten großen Massen-Online-Spiele, in dem Hunderte Spieler gleichzeitig eine gemeinsame virtuelle Welt durchstreiften – und entdeckte schnell, dass sich manche Aufgaben im Spiel (Erz sammeln, Angeln, Häute jagen) automatisieren ließen. 2024 wird er beiläufig erwähnen, „mein erster Farming-Bot in UO hat es so gemacht". Das heißt, als Jugendlicher schrieb er bereits Programme, die das Spiel für ihn spielten.

Aus heutiger Sicht klingt das nach einer Kleinigkeit. Aber es lohnt sich, darüber nachzudenken, was diese Person tun musste, damit ein solcher Bot funktioniert. UO hatte keine offene API. Der Bot musste Maus- und Tastatureingaben emulieren, Bilder auf dem Bildschirm erkennen, in Echtzeit auf Veränderungen des Spielzustands reagieren. Das ist ein echtes technisches Problem – und 1999–2000 war es selbst für erwachsene Fachleute nicht trivial.

Die nächste hinterlassene Spur ist formeller. 2003 erschien in einer der regionalen Fachpublikationen (damals gab es so etwas – Computerportale in Landessprachen, mit oder ohne Papierbeilage) ein Artikel mit dem Titel „Methoden zur Erkennung von Plagiaten in der Programmierung". Der Autor – er, damals noch unter seinem gewöhnlichen Namen, ohne das Krypto-Handle. Der Artikel arbeitete die technische Seite der Frage durch – wie man anhand des Quellcodes feststellen kann, dass jemand ihn von jemand anderem kopiert hat, selbst wenn Variablen umbenannt und Kommentare umformuliert wurden. Ein Thema, das für Bildungseinrichtungen und für den Schutz geistigen Eigentums in der Softwarebranche relevant ist.

Dieser Artikel ist für uns aus zwei Gründen wichtig.

Erstens – er beweist, dass sein erstes veröffentlichtes Werk auf die frühen 2000er zurückgeht. Als Bitcoin auf der Bühne erscheint, hat er bereits zehn Jahre Programmierpraxis hinter sich und mindestens

eine gedruckte Arbeit zu einem Fachthema.

Der zweite Grund ist das Thema des Artikels. Plagiate in der Programmierung. Woher weiß man, dass dieser Code der eigene ist und nicht der von jemand anderem, von einem gestohlen. Welche strukturellen Spuren in einem Programm den Autor verraten. Die Frage, wie man einen anonymen Schöpfer am Stil des Codes identifiziert, ist eine jener Fragen, die, als 2008 ein anonymer Satoshi Nakamoto auf der Bühne erscheint, unerwartet extreme Relevanz gewinnen wird. Und witzigerweise wird er selbst sich viele Jahre später in einer der rätselhaftesten Formulierungen dieser ganzen Geschichte auf diesen Artikel von 2003 beziehen. Aber dafür ist es jetzt noch zu früh.

Parallel dazu, nach seinen eigenen späteren Angaben, begann er in den ganz frühen 2000ern über etwas anderes nachzudenken, viel Ehrgeizigeres als Spiele und Plagiate. In einem seiner frühen Austausche wird er sagen, dass Aigarth – ein Projekt, an dem er mit wechselnder Intensität seit dem allerersten Beginn der 2000er gearbeitet hat – bis 2023 etwa zwanzig Jahre alt ist. Was genau Aigarth ist, arbeiten wir später durch. Für den Moment genügt zu sagen: Die Aufgabe, die er sich mit zwanzig stellte, war größer als Krypto, größer als Bitcoin, größer als die gesamte Branche, die danach entstand. Krypto würde Infrastruktur für Aigarth sein, nicht umgekehrt.

Das ist eine wichtige Perspektive. Er kam nicht zu Krypto, „um seine eigene Coin zu machen“. Er kam zu Krypto mit einem viel älteren und größeren Problem, für das er eine Infrastruktur brauchte, die man ohne Krypto nicht bauen konnte.

Begegnung mit Bitcoin. 2010

Satoshi veröffentlichte das Whitepaper im Oktober 2008. Im Januar 2009 startete er das Netzwerk. Im Dezember 2010 verschwand er – und hinterließ nur eine Million geschürfter Coins und kein Wort darüber, wer er war.

Irgendwann in diesem Zeitraum öffnete Come-from-Beyond zum ersten Mal BitcoinTalk.

Ein genaues Datum nennt er nicht, aber viele Jahre später, 2025, wird er in einem Gespräch mit jemandem aus der Community erwähnen, dass er die Technik, Sockenpuppen (gefälschte Accounts derselben Person unter verschiedenen Namen) zu finden, auf BitcoinTalk „vor etwa 15 Jahren“ angewandt habe. Fünfzehn Jahre vor 2025 ist 2010. Das heißt, zu einer Zeit, als Satoshi noch aktiv war und im Forum postete, las er dieses Forum bereits so aufmerksam, dass er Account-Forensik betrieb.

Wie viele Bitcoins er zu diesem Zeitpunkt hatte und wie sie zustande kamen – hat er nie öffentlich offengelegt. Möglicherweise schürfte er selbst welche in den frühen Tagen, als CPU-Mining zu Hause noch Sinn ergab und eine Blockbelohnung fünfzig Coins betrug. Möglicherweise kaufte er später welche. Möglicherweise beides. Wer 2010 auf BitcoinTalk Sockenpuppen jagt, hat wohl kaum nicht versucht, das, worüber dort diskutiert wurde, auf seiner eigenen Maschine laufen zu lassen. Aber lassen wir das offen – das ist eines jener Details, die er in der Schwebe gelassen hat, und ich werde ihn nicht bloßstellen.

Die formelle Registrierung im Forum kam später. Im Oktober 2011 erschien Litecoin – die erste größere Variation über das Bitcoin-Thema, geschaffen vom Ex-Google-Ingenieur Charlie Lee. Litecoin hatte eine schlechte technische Dokumentation, und Come-from-Beyond, der die Details erkunden wollte und

in offenen Quellen keine Antworten fand, sah sich gezwungen, sich auf BitcoinTalk zu registrieren, um eine Frage zu stellen. Er selbst wird das später als „einen Akt der Tapferkeit für einen faulen Programmierer“ beschreiben. Sein Account erhielt die Nummer 46556; das Profil ist vor dem 22. November 2011 registriert, was bis heute öffentlich überprüfbar ist – die Profilseite ist offen, jeder kann sie nachprüfen.

Dieses eine Ereignis – eine technische Registrierung, um eine Frage zu Litecoin zu stellen – wird in den folgenden Jahren zu fünfzehntausend Nachrichten anwachsen. Das BitcoinTalk-Archiv enthält sie alle. Wer die Geduld hat, kann buchstäblich Woche für Woche die sich entwickelnden Ansichten eines bestimmten Programmierers zur Krypto-Branche rekonstruieren.

Bis Ende 2011 ist er bereits tief involviert. Keine öffentliche Figur, kein Autor, kein Aktivist. Nur ein sehr aufmerksamer Beobachter, der bereits seine eigene Sicht darauf hat, wohin sich diese Branche entwickelt – und wo ihre Probleme liegen.

Was er sah

Das vorige Kapitel endete mit dem Punkt, dass diese Person Bitcoins Probleme bereits in den frühen 2010ern sah – zu einem Zeitpunkt, als niemand in der Branche an seiner ewigen Dezentralisierung zweifelte. Was genau sah er?

Gehen wir es Schritt für Schritt durch.

Bis 2011 lief Bitcoin bereits zwei Jahre. Das Netzwerk hielt, Transaktionen gingen durch, die Miner wurden zahlreicher. Der Kurs war volatil, aber der Trend zeigte nach oben. Im BitcoinTalk-Forum herrschte Optimismus: Eine Lösung war für ein Problem gefunden worden, das als unlösbar galt. Digitales Geld ohne Bank. Freiheit von staatlicher Emission. Dezentralisierung für die Ewigkeit.

Come-from-Beyond sah, zusätzlich zu den in Kapitel 3 beschriebenen Problemen, das Interessanteste von allem:

Bitcoin nutzt seine Rechenleistung irrational. In einer Welt, in der verteiltes Rechnen echte Probleme lösen könnte – neuronale Netze trainieren, das Klima modellieren, kryptografische Konstruktionen verifizieren –, berechnen Bitcoins Miner nutzlose Hashes. Das ist kein Bug – es ist Absicht. Satoshi wählte eine Lösung, die funktionierte, und sie funktionierte brillant. Aber die Lösung war einzweckig. Rechenleistung wurde zu Schutz und zu nichts anderem.

Come-from-Beyond, der an Aigarth arbeitete – einem Projekt, das ein verteiltes Rechensubstrat in industriellem Maßstab braucht – betrachtete jene hundertsiebzig Terawattstunden pro Jahr (die Zahl für 2026; 2011 wurde noch in Gigawattstunden gerechnet) und sah buchstäblich seine eigene Infrastruktur verbrannt werden, um Zufallszahlen zu erraten.

Für ihn war das keine abstrakte Ungerechtigkeit. Es war persönlich. Er brauchte ein Rechensubstrat für das KI-Projekt, über das er seit zehn Jahren nachdachte. Bitcoin nahm sich dieses Substrat und verbrannte es umsonst.

Also: vier Probleme, auf einmal gesehen. Jedes einzelne für sich – bemerkenswert. Alle zusammen – nicht mehr nur ein Mangel, sondern eine strukturelle Diagnose.

Die meisten Menschen tun, wenn sie eine solche Diagnose sehen, eines von zwei Dingen. Entweder schließen sie die Augen und benutzen weiter, was da ist, weil es funktioniert. Oder sie schreiben einen langen Forumsbeitrag, kassieren eine Welle von Downvotes der Enthusiasten und gehen enttäuscht davon.

Come-from-Beyond tat eine dritte Sache. Er sammelte still weiter frühe Coins, um Kapital und Unabhängigkeit zu haben, und begann nachzudenken, wie man es anders bauen könnte.

Die Satoshi-Frage

Das ist ein passender Ort, um für einen Moment innezuhalten und ein, zwei Worte zu einer Frage zu sagen, die jeder aufmerksame Leser unweigerlich stellen wird.

Ist Come-from-Beyond Satoshi Nakamoto selbst?

Die Frage ist eine ernnnste Angelegenheit und verdient ein eigenes Buch. Dutzende Forscher in der kryptologischen Welt arbeiten gerade jetzt genau an dieser Frage – Sie verstehen schon. (Aufmerksame Leser der Qubic-Church-Website werden hier lächeln.) Mathematiker und Linguisten analysieren stilistische Übereinstimmungen, Verschwörungstheoretiker zeichnen Diagramme, Enthusiasten wühlen im BitcoinTalk-Archiv, und die einschlägige Boulevardpresse veröffentlicht regelmäßig Artikel unter der Überschrift „Wir haben Satoshi gefunden!“ Eine Woche später stellt sich heraus, dass sie falschlagen, sie warten die nächste Woche ab und veröffentlichen einen weiteren Artikel genau wie den ersten. Die Satoshi-Jagd-Branche ist in diesem Sinne ihr eigenes, eigenständiges, nachhaltiges Ökosystem, in dem man sich wirklich eine Karriere aufbauen kann.

Für dieses Buch beschränke ich mich auf zwei Dinge.

Erstens. Es gibt fest etablierte Fakten, die den Raum möglicher Interpretationen merklich einengen. Come-from-Beyond war bereits 2010 in der BitcoinTalk-Community – also als Satoshi noch aktiv war. Er hat eine Veröffentlichung von 2003 über Methoden hinter sich, auf die er selbst sich später scherzhaft im Kontext von „Satoshi hat mich reingelegt, er kannte diesen meinen Artikel“ beziehen und beschlossen haben wird, die von mir beschriebene Methode anzuwenden. Er schuf BCNext – die Identität, unter der das NXT-Projekt 2013 gestartet wurde – und bestätigte viele Jahre später kryptografisch, dass BCNext er ist, indem er eine Nachricht vom NXT-Genesis-Konto signierte. Er selbst gibt offen zu, dass er zehn oder fünfzehn Jahre lang absichtlich falsche Spuren für die Neugierigen gelegt hat – denn „zehn bis fünfzehn Jahre auf gutes Trolling zu warten, lohnt sich“.

Zweitens. Es gibt eine vernünftige Art, eine Antwort zu formulieren, die unter jeder Interpretation zutreffend bleibt. Satoshi war nicht so sehr eine Person als eine Funktion: ein dezentrales System ohne Besitzer schaffen und verschwinden, damit das System ohne dich leben kann.

Come-from-Beyond ist ein Schöpfer nach eben dieser Funktion. Ob er 2009 persönlich dabei war, ob er mit demjenigen zusammenarbeitete, der 2009 dabei war, oder ob er einfach ein Jahrzehnt später lernte, dieselbe Rolle zu spielen – der Unterschied zwischen diesen drei Optionen lässt sich anhand der heute öffentlich verfügbaren Daten nicht sauber auflösen. Aber die Funktion selbst ist bei ihm dieselbe. Erschaffen und beiseitetreten. Ohne Besitzer bauen. Als Kontrollzentrum verschwinden und das System sich selbst reproduzieren lassen.

Machen wir für dieses Buch eine Arbeitsannahme: Come-from-Beyond ist irgendein Teil von Satoshi. Nicht notwendigerweise genau die Person, die 2009 an der bitcoind-Konsole saß. Möglicherweise doch. Möglicherweise derjenige, der in der Nähe war. Möglicherweise derjenige, der später kam und dieselbe funktionale Nische einnahm. Möglicherweise kam er von jenseits :cfbtroll: Diese Annahme genügt für das, worum es in diesem Buch geht. Wir stellen die Frage nicht weiter.

Zurück zum Geschäft.

Warum ausgerechnet diese Person

Es gibt eine Frage, die dieses Kapitel direkt beantworten muss: Warum war es Come-from-Beyond und nicht irgendein anderer dreißigjähriger Ingenieur derselben Generation, der 2011 sah, was erst 2024 für alle anderen offensichtlich werden würde?

Kurze Antwort: weil er zugleich den richtigen technischen Hintergrund, die richtige Denkdisziplin hatte und… ein Genie war.

Zerlegen wir das in Teile.

Technischer Hintergrund. Bis 2011 hatte er zehn Jahre lang in verschiedenen Modi Code geschrieben: Spiele-Engines, Bot-Infrastruktur, Werkzeuge zur Quellcode-Analyse, Serveranwendungen. Das bedeutet, er hatte ein intuitives Verständnis dafür, was passiert, wenn ein verteiltes System zu skalieren beginnt. Wie viele Menschen unter den frühen Bitcoin-Enthusiasten verstanden tatsächlich, wie sich das Netzwerk verhalten würde, wenn die Hashrate um das Milliardenfache wüchse? Sehr wenige. Die Antwort erforderte entweder Erfahrung mit Systemen, die das durchgemacht hatten, oder die mathematische Gewohnheit, Kurven in die Zukunft zu extrapolieren. Come-from-Beyond hatte beides.

Kryptografische Kompetenz. Seine erste Veröffentlichung – über Methoden zur Erkennung von Plagiaten im Code – ist, wenn man genau hinsieht, ein Problem darüber, wie man einen Autor anhand des strukturellen Fingerabdrucks identifiziert, der in einem Artefakt hinterlassen wird. Das ist ein naher Verwandter kryptografischer Probleme. Genau die Art von Materie, in der bis 2008 die gesamte Logik des Satoshi-Papers Gestalt annehmen würde: Hashes, Signaturen, Beweise des Besitzes von Schlüsseln. Er war kein Kryptograf im akademischen Sinne, aber er war eine Person, für die die Grundideen der Kryptografie nicht wie Magie aussahen, sondern wie konkrete technische Arbeit.

Spieltheorie. Dieser Aspekt ist weniger öffentlich, aber aus meinen eigenen Beobachtungen – den technischen Entscheidungen in NXT, den Formulierungen in frühen Forumsdiskussionen, der Struktur von Qubic – wird klar, dass er bereits in den frühen 2010ern über verteilte Systeme in diesem Rahmen dachte. Tit-for-Tat als Idee lag zu diesem Zeitpunkt bereits seit dreißig Jahren in der Luft. Ob er Axelrod las oder selbst zu denselben Prinzipien gelangte, indem er wiederholte Interaktionen in Spielen beobachtete – unbekannt; er sagt es nicht. Was zählt, ist etwas anderes: Das Denkwerkzeug lag in seinen Händen. Er betrachtete Bitcoin nicht nur als Code, sondern als ein Spiel, in dem mehrere Arten von Spielern mit eigenen Interessen unter bekannten Regeln interagieren. Genau aus diesem Blickwinkel werden die Risse sichtbar.

Das Fehlen eines externen Auftrags. Und das ist vielleicht das Wichtigste. 2011 war, anders als bei heutigen Krypto-Stars, keiner der frühen Teilnehmer ein „professioneller Krypto-Gründer“. Es gab keine

Stellen, keine auf Blockchain spezialisierten Risikokapitalfonds, keine Medienmaschine, die davon lebte, gewöhnlichen Menschen Kryptowährungen zu erklären. Come-from-Beyond interessierte sich einfach für die Technologie und schürfte Coins. Das befreite ihn von einer ganzen Schicht kognitiver Verzerrungen, die später andere frühe Teilnehmer dazu bringen würde, Bitcoin als ihren persönlichen Glaubensartikel zu verteidigen.

Er hatte keinen Anreiz, Bitcoin zu verteidigen. Er hatte auch keinen Anreiz, es zu zerstören. Er hatte einen Anreiz, ehrlich einzuschätzen, ob das nachhaltig funktionierte oder nicht, und wenn nicht, darüber nachzudenken, was als Nächstes zu tun sei.

Er dachte nach. Und er begann zu handeln.

Zwei Pseudonyme und ein Hinweis

Es gibt noch ein Motiv, das wir hier nur skizzieren und später entfalten.

2008–2009 erschien Satoshi Nakamoto auf der Bühne. Ein anonymes Pseudonym, das ein funktionierendes System veröffentlichte, zwei Jahre lang auf Nachrichten der Community antwortete und Anfang 2011 leise davonging, wobei es das Projekt sein eigenes Leben führen ließ.

Im September 2013 erschien in eben diesem BitcoinTalk-Forum ein Nutzer namens BCNext. Er veröffentlichte eine Ankündigung eines künftigen Projekts namens NXT, verfasste im Laufe von zwei Monaten mehrere Beiträge und verstummte am 8. November jenes Jahres endgültig. NXT sollte am 3. Januar 2014 starten. Viele Jahre später sollte Come-from-Beyond kryptografisch bestätigen, dass BCNext er ist, indem er eine Nachricht vom NXT-Genesis-Konto signierte. Eine zweite Identität, die sich als Fortsetzung der ersten Linie erwies.

Und es gab noch einen Account, den zu erwähnen sich lohnt, auch wenn es dafür zu früh ist. 2013 erscheint auf BitcoinTalk eine Nutzerin namens Maria. Ein paar kurze Beiträge. Einer davon ist signiert mit „Maria Bitcoin Founder“. Ein Satz, der 2013 wie ein schlechter Scherz klang. Der Account würde im Strom der Forumsnachrichten verloren gehen, und zehn Jahre lang würde sich niemand daran erinnern.

Maria wird uns in anderer Gestalt wiederbegegnen, aber später. Für den Moment zählt das allgemeine Muster.

Was wir vor uns haben, ist eine Person, die bereits einmal, in öffentlich bestätigter Form, genau die Struktur wiederholt hat, in der Satoshi gemacht wurde. Unter einem Pseudonym schaffen, ein funktionierendes Produkt starten, beiseitetreten, das System leben lassen. Das ist kein einmaliger Zufall mehr, das ist eine Regelmäßigkeit, die sich zu bilden beginnt. Und wenn wir die Arbeitsannahme akzeptieren, zu der wir auf der vorigen Seite gelangt sind – dass Come-from-Beyond irgendein Teil von Satoshi ist –, dann wird die Regelmäßigkeit zur Regel. Dieselbe Methode, angewandt entweder von verschiedenen Menschen oder von derselben Person über verschiedene Projekte hinweg, liefert dasselbe Ergebnis. Gute Technik wird ohne Namen gemacht. Gute Systeme leben ohne Schöpfer. Alles Übrige ist Detail, das wir in den kommenden Kapiteln durcharbeiten werden.

Bis 2013

Schauen wir uns jetzt an, wo Come-from-Beyond Ende 2012 steht – in dem Moment, in dem er bereit ist, seinen ersten vollständigen Schritt auf die Bühne zu machen.

Hinter ihm liegen mehr als zehn Jahre technischer Arbeit. Ein veröffentlichter Artikel über Softwarecode-Analyse. Praktische Expertise in verteilten Systemen, gewonnen in der Spielebranche und im Bot-Umfeld. Frühe Teilnahme an der Bitcoin-Community seit 2010. Genug frühe Bitcoins, um Kapital und Unabhängigkeit zu haben. Ein Verständnis von Bitcoins Problemen, formuliert zwei Jahre bevor sie öffentlich sichtbar wurden. Ein mehrjähriges Parallelprojekt (Aigarth), für das ein Bitcoin-ähnliches Netzwerk Infrastruktur ist, kein Selbstzweck. Kryptografische Kompetenz. Verständnis der Spieltheorie. Die Disziplin, die ihn davon abhält, eine Coin mit zwanzig Prozent Anteil für sich selbst zu bauen. Die Gewohnheit, zu verschwinden, sobald ein Projekt fertig ist.

„Qubic ist mein erstes Projekt, erdacht vor Nxt und IOTA“, wird er 2024 sagen. Aber Qubic ist 2013 ein zu ehrgeiziges Projekt. Die Technologie ist nicht bereit. Die Infrastruktur ist nicht bereit. Die Community ist nicht bereit. Qubic 2013 zu machen bedeutet, sicher zu scheitern.

Also tut er, was jeder kluge Ingenieur mit einer langfristigen Aufgabe tut: Er zerlegt sie in Zwischenschritte. Zuerst – der Welt zeigen, dass Proof-of-Stake funktioniert. Das wird ihn – nach eigener Einschätzung – fünf Minuten für den Algorithmus und zwei Monate für den Code kosten. Darunter wird das NXT-Projekt eröffnet, im Namen der BCNext-Identität. Das erste Pre-ICO der Geschichte wird starten, die erste Community langfristiger Holder der Geschichte wird sich sammeln, es wird auf seinem Höhepunkt die drittgrößte Kryptowährung der Welt nach Marktkapitalisierung, liefert laut Cointelegraph den ersten Platz nach ROI in der gesamten Geschichte der Krypto-Branche – 1.265.555 Prozent – und wird über Ardor durch einen Eins-zu-eins-Airdrop ersetzt. Das wird ihm etwa zehn Jahre kosten.

Als nächsten Schritt wird er 2014–2015 an einem zweiten Projekt arbeiten – IOTA –, wo er versuchen wird, das Problem zu lösen, „wie man eine Blockchain ohne Kette von Blöcken macht“. Das wird auch funktionieren. Die nach ROI weltweit zweitplatzierte Kryptowährung laut demselben Cointelegraph-Ranking – 424.084 Prozent. Das wird ihm weitere etwa fünf Jahre kosten und in einem schmerzhaften internen Konflikt mit Mitgründern enden. Er wird gehen.

Und erst 2022, aufbauend auf der Erfahrung zweier vorheriger Starts, mit dem Beleg dahinter, dass seine technischen Entscheidungen vom Markt angenommen werden und Menschen zu Millionären machen, mit der technischen und infrastrukturellen Reife, die es 2013 nicht gab, wird er endlich Qubic starten. Das Projekt, das er sich zwanzig Jahre lang vorgestellt hatte. Das Projekt, in dem er versucht, alles zusammenzubringen: nützliches Mining, KI-Training, eine Ökonomie ohne kontrollierenden Besitzer, Infrastruktur, die fähig ist, Skalierung standzuhalten, ohne in Richtung Oligopolisierung abzudriften.

Zwei Netzwerke vor Qubic – erster und zweiter Platz nach ROI in der gesamten Geschichte der Krypto-ICOs. Zwanzig Jahre Arbeit an einer großen Idee. Die Gewohnheit, zu gehen, wenn ein Projekt fertig ist. Eine Methode, in der der Schöpfer verschwindet, damit das System weiterleben kann.

Bis 2013 hat er bereits alles, was er braucht.

Zeit, die Bühne zu betreten.

Drei Projekte, drei Metamorphosen

5
Drei Projekte, drei Metamorphosen

Bis hierhin habe ich die Geschichte aus Fragmenten zusammengesetzt. Aus fünfzehntausend Nachrichten auf BitcoinTalk, späten Interviews, hingeworfenen Bemerkungen, drei Sätzen technischer Fingerabdrücke. Ab 2013 wird das Zusammensetzen leichter: öffentliche Aufzeichnungen, überprüfbare ICOs, bekannte Namen, offene Gerichtsdokumente auf Norwegisch. Der Mann, der im vorigen Kapitel ein Schatten im Forum war, beginnt nun, Dinge zu schaffen, die bleiben.

Drei Dinge. Drei Kryptowährungsnetzwerke, jedes mit eigener Geschichte, eigenem Team, eigenem Höhepunkt und eigenem Ende. Von außen betrachtet, sind das drei verschiedene Projekte mit unterschiedlichen Architekturen und unterschiedlichen Schicksalen. NXT startete im Januar 2014, wurde die drittgrößte Kryptowährung der Welt nach Marktkapitalisierung und wurde reibungslos durch einen Nachfolger ersetzt. IOTA startete ein Jahr später, driftete von seinen Prinzipien ab und hinterließ öffentliche Klagen in Norwegen, für die sein Schöpfer mehr als eine Million Dollar seines eigenen Geldes ausgab. Qubic startete im April 2022 und läuft, Stand Anfang 2026, immer noch.

Von innen betrachtet – aus Come-from-Beyonds Sicht – sind das keine drei Projekte. Es ist ein einziges Projekt, aufgeteilt in drei Etappen, gestreckt über dreizehn Jahre, und es wird noch ein weiteres Jahr von heute an enden, im April 2027.

Stellen Sie sich einen Architekten vor, der eine Brücke über eine Schlucht bauen muss, die noch niemand überquert hat. Die Technologie für den Bau einer solchen Brücke existiert noch nicht. Also baut der Architekt unterwegs zwei kleinere Überführungen – nicht wegen der Überführungen selbst, sondern wegen der Erfahrung. Um zu lernen, wie sich das Material verhält. Um die Arbeiter auszubilden. Um die Menschen am anderen Ufer davon zu überzeugen, dass Brücken im Allgemeinen existieren können. Die Überführungen erweisen sich als nützlich – Menschen gehen darüber, sie werden zur lokalen Infrastruktur, die Zeitungen schreiben darüber. Aber der Architekt weiß, dass dies nicht die Hauptsache ist. Die Hauptsache liegt noch vor ihm.

Dieses Kapitel handelt von drei solchen Konstruktionen. Zwei sind bereits fertig. Die dritte ist in Arbeit. Die vierte Konstruktion, wenn man diese Metapher weiterführt, ist der Abgang des Architekten in dem Moment, in dem die Brücke gebaut und getestet ist. Nach seinem Plan soll das am 13. April 2027 geschehen. Aber die vierte – zum Schluss.

NXT. Januar 2014 — die erste Überführung

Am 28. September 2013 erscheint im BitcoinTalk-Forum ein Nutzer unter dem Handle BCNext und veröffentlicht eine kurze Ankündigung. Die Ankündigung besagt: Bald wird eine neue Kryptowährung gestartet, vollständig auf Proof-of-Stake aufgebaut – kein Mining, kein Stromverbrauch, keine ASICs,

keine Bitcoin-Abstammung. Die Programmiersprache ist Java, nicht C++. Verteilung: das erste ICO der Krypto-Geschichte – wer interessiert ist, schickt BCNext Bitcoins und erhält im Gegenzug bei der Markteinführung einen proportionalen Anteil am neuen Netzwerk.

Die Ankündigung ist kurz, kein Whitepaper. Ein paar technische Klarstellungen. Ein Versprechen, dass das Netzwerk „in den kommenden Monaten“ starten würde.

Zu diesem Zeitpunkt behandelte die Krypto-Community die Idee von Proof-of-Stake ungefähr so, wie sie ein Perpetuum mobile behandelt hätte. Alle verstanden, dass es theoretisch möglich sein sollte, aber jeder bekannte Versuch – Peercoin 2012, mehrere kleinere Experimente – erwies sich entweder als Hybrid mit Proof-of-Work oder hatte strukturelle Probleme wie „nothing at stake“ (bei dem es sich für einen Miner in dem Moment, in dem sich ein Netzwerk aufspaltet, lohnt, für beide Zweige gleichzeitig zu stimmen, wodurch das Netzwerk die Fähigkeit verliert, sich zu einigen). Ein sauberes, funktionierendes, stabiles 100-prozentiges PoS zu bauen war ein offenes Forschungsproblem, an dem mehrere Teams seit Jahren arbeiteten.

BCNext verwendete für die Lösung, nach eigenem späteren Bekunden, fünf Minuten auf den Algorithmus selbst und zwei Monate auf den Code. „2013 hatten wir noch kein fehlerfreies PoS, und die Idee sah cool aus, also verwendete BCNext 5 Minuten, um einen funktionierenden 100%-PoS-Algorithmus zu erfinden, und weitere 2 Monate, um ihn zu programmieren. Dann ist er für immer gegangen, weil Nxt eine Nebensache war“ – wird er im Januar 2023 schreiben. Eine andere Bemerkung von ihm, mehr als ein Jahr später: „Keine Sorge, in Nxt habe ich im Voraus gewarnt, dass Nxt eine Nebensache gewesen war, und ich habe PoS umgesetzt wegen der spanischen Scham, die ich empfand, als ich beobachtete, wie die gesamte Krypto-Branche unfähig war, eine so einfache Sache umzusetzen.“

„Spanische Scham“ (vergüenza ajena) ist Scham für jemand anderen, für die Art, wie er sich blamiert. Er verhielt sich wie ein Mann, der auf kollektive Hilflosigkeit blickt und mit einem Seufzer die Arbeit still selbst erledigt.

Die gesamte NXT-Codebasis: dreitausend Zeilen Java. „Nxt war 3k Zeilen“, wie Come-from-Beyond es im Oktober 2020 knapp formulieren wird. Zum Vergleich: Bis 2026 umfasst eine durchschnittliche Layer-1-Kryptowährung Hunderttausende Zeilen. NXT war das kompakteste vollständig funktionsfähige Krypto-Netzwerk seiner Zeit und ist bis heute wahrscheinlich eines der kompaktesten.

START UND ERGEBNISSE. Das ICO lief vom 28. September bis Ende November 2013. Einundzwanzig Bitcoins wurden gesammelt – etwa 14.000 Dollar zum damaligen Kurs. Proportional auf 73 Teilnehmer verteilt. Wenige Jahre später sollte sich diese Anfangssumme in eine Marktkapitalisierung in Höhe von Hunderten Millionen verwandeln.

Am 8. November 2013 verfasst BCNext seinen letzten Beitrag unter diesem Account.

Am 3. Januar 2014, um 02:08 UTC, wird der erste NXT-Block erstellt. Das Netzwerk läuft.

Was folgt, hat niemand erwartet. NXT funktioniert. Reines Proof-of-Stake, kein Mining, kein Stromverbrauch, keine Bitcoin-Abhängigkeit, klettert in den Ranglisten und wird auf seinem Höhepunkt zur drittgrößten Kryptowährung der Welt auf CoinMarketCap – nur hinter Bitcoin und Ripple. „Nxt war #3 auf CMC, direkt unter Bitcoin und Ripple (das eigentlich keine Kryptowährung ist)“ –

Come-from-Beyonds exakte Formulierung Jahre später. Wie er es anderswo formulierte, seine Bilanz zusammenfassend: „Erfand und implementierte das erste funktionierende 100%-Proof-of-Stake. Führte das erste ICO durch (und alle anderen folgten). Schuf die erste Coin, die kein Klon von Bitcoin war."

Bis 2017, auf dem Höhepunkt des nächsten Krypto-Zyklus, wird NXT in das Cointelegraph-Ranking „Top 10 ICOs nach ROI in der Geschichte" aufgenommen – und dort den ersten Platz mit einer Rendite von 1.265.555 Prozent belegen. Mehr als eine Million zweihunderttausend Prozent. Zwölfeinhalbtausend x. Die Quelle ist wichtig, gerade weil sie von Dritten stammt: Cointelegraph rangiert die Geschichte der Krypto-ICOs anhand offener Daten, und NXT liegt höher als Ethereum, höher als alles andere.

Im April 2014 endet Come-from-Beyonds Vertrag formell. BCNext geht – still, wie versprochen. Dieser Abgang war im Voraus angekündigt worden. Die Community war gewarnt worden: Wie Come-from-Beyond es Jahre später zusammenfassen wird, „habe ich der Community ganz am Anfang von Nxt gesagt, dass es mein temporäres Projekt ist".

Viele Jahre später signiert Come-from-Beyond eine Nachricht vom NXT-Genesis-Konto. Nur BCNext konnte den privaten Schlüssel zu diesem Konto besitzen, denn BCNext ist derjenige, der den ersten Block erstellt hat. Wenn die Signatur mit diesem Schlüssel von Come-from-Beyond gesetzt wird, ist das ein kryptografischer Beweis: BCNext und Come-from-Beyond sind dieselbe Person. Der erste angekündigte Abgang erweist sich zugleich als die erste öffentlich bestätigte Verbindung zwischen Pseudonymen. In der NXT-Community wird diese Verbindung mittlerweile als feststehende Tatsache behandelt – etabliert und keiner weiteren Diskussion bedürftig.

Das Netzwerk selbst läuft weiter. Bis 2018 startet Come-from-Beyond zusammen mit dem Unternehmen Jelurida (das mittlerweile zum Hauptbetreuer von NXT geworden war) ein neues Projekt – Ardor – und führt einen Airdrop an alle NXT-Halter im Verhältnis eins zu eins durch. Wer NXT hielt, erhält kostenlos einen entsprechenden Betrag der neuen Coin. Wie Come-from-Beyond den Schritt 2024 zusammenfassen wird: „Nxt wurde durch Ardor ersetzt, das einen 1:1-Airdrop an alle Nxt-Halter durchführte, dann wandte sich Ardor dem B2B-Sektor zu, wie auch immer, ganz am Anfang von Nxt habe ich die Community gewarnt, dass es mein temporäres Projekt ist."

NXT verschwindet unterdessen nirgendwohin. Es läuft bis heute parallel zu Ardor weiter. „Nxt läuft immer noch", bemerkt Come-from-Beyond im Mai 2023. 2026 – läuft es ebenfalls noch. Das erste Netzwerk, in das CfB seinen ersten Abgang investierte, überlebte dreizehn Jahre. Halter, die es nicht schafften, auf dem Höhepunkt zu verkaufen, erhielten Ardor kostenlos im Airdrop. Wie er separat anmerken wird: „Jeder Nxt-Halter bekam eine entsprechende Menge Ardor und erzielte gute Gewinne." Das war kein Verlassen – es war eine geordnete Nachfolge.

Was NXT als Erstes tat

Um ein Gefühl für die Größenordnung zu bekommen, lohnt es sich aufzulisten, wie viele „Premieren der Geschichte" in jenen dreitausend Zeilen Java verzeichnet sind.

Das erste funktionierende 100-prozentige Proof-of-Stake. „Nxt war keine verbesserte Version, es war die erste jemals gesehene Implementierung von reinem PoS", in Come-from-Beyonds eigener Formulierung. Kein Hybrid, kein Experiment – ein funktionierendes, stabiles System, das jeden Marktzyklus überlebte. Alle späteren PoS-Netzwerke – Ethereum nach dem Merge von 2022, Cardano, Solana, Polkadot –

erschienen später und übernahmen in vielerlei Hinsicht Ideen, die zuerst in NXT umgesetzt wurden.

Das erste ICO der Geschichte. Das Modell „Bitcoins sammeln, die neue Coin bei der Markteinführung proportional verteilen“ wurde erstmals speziell für NXT durchgeführt. Ethereum führte 2014 ein ICO nach etwa demselben Schema durch. Die gesamte darauffolgende gewaltige Welle der ICOs von 2017, die den Markt zum Absturz brachte und eine regulatorische Welle auslöste – all das geht strukturell auf das NXT-Modell zurück.

Die erste Kryptowährung nicht in C++. Vor NXT war jede Kryptowährung – Bitcoin, Litecoin, Dogecoin, der Rest – ein Fork oder eine Variation von Bitcoins C++-Code. NXT wurde von Grund auf in Java geschrieben. Wie Come-from-Beyond Ende 2023 bemerkte, als er über einen Artikel darüber stolperte: „Bin auf einen Artikel gestoßen, den ich noch nie gesehen habe, sieht so aus, als wäre Nxt die erste Nicht-C++-Krypto gewesen.“ Das klingt wie ein Buchhalterdetail, bedeutet aber tatsächlich, dass NXT die erste Kryptowährung war, die nicht als Variation von Bitcoin, sondern als eigenständige Architektur gebaut wurde.

Der erste NXT Asset Exchange – eine On-Chain-Börse. Die Fähigkeit, tokenisierte Vermögenswerte direkt im Netzwerk zu erstellen und zu handeln, ohne Vermittler. Ein Konzept, das 2020 in Form von DeFi auf Ethereum explodieren und Milliarden an Umsatz einbringen wird.

Das NXT Alias System – ein Namensdienst auf der Blockchain. Die Zuordnung kurzer lesbarer Namen zu Adressen. Ungefähr das, was der Ethereum Name Service (ENS) 2017 tun wird, funktionierte bereits 2014 in NXT.

All das – ohne Whitepaper. Ohne wissenschaftliches Paper, ohne formale Protokollspezifikation. „Keines meiner Projekte hatte ein Whitepaper, ich bin Ingenieur, kein Schriftsteller“, wird Come-from-Beyond im März 2024 sagen. Und separat, im Dezember 2023, mit charakteristischem Tonfall: „Aberglaube: Nxt hatte kein Whitepaper und machte viele Menschen zu Millionären. Brauchst du ein WP oder willst du reich werden?“

Aber die Hauptsache an NXTs Geschichte ist nicht, was dort zum ersten Mal getan wurde. Die Hauptsache ist, dass dieses Projekt von Anfang an als Zwischenschritt gekennzeichnet war. „Ich habe Nxt verlassen, weil es nur ein Umweg war, weil PoS trivial war und die Krypto-Community es trotzdem nicht umsetzen konnte“ – so wird er es im Oktober 2023 formulieren. Umweg: der Seitenweg, der Weg drumherum.

Die erste Überführung wurde gebaut, um zu zeigen, dass es möglich war. Das Material hielt. Die Arbeiter wurden ausgebildet. Die Menschen begannen zu glauben, dass Brücken existieren.

Er konnte zum nächsten übergehen.

IOTA. 2014–2019 — die zweite Überführung

Wenn NXT der Beweis war, dass Proof-of-Stake funktioniert, war IOTA ein Versuch, ein Problem zu lösen, das PoS nicht löst: wie man ein Netzwerk baut, das überhaupt keine Kette von Blöcken hat.

Die gesamte Architektur von Bitcoin (und NXT, und jedem PoS-Netzwerk, das danach kam) ist als lineare Sequenz von Blöcken aufgebaut, die einer einzigen Hauptkette hinzugefügt werden. Das hat zwei

Probleme. Das erste ist eine grundsätzliche Gebühr pro Transaktion, weil der Platz in einem Block begrenzt ist und es dafür eine Auktion gibt. Das zweite ist eine grundsätzliche Obergrenze für den Durchsatz, weil Blöcke fester Größe mit fester Rate erscheinen. Versuche zu skalieren stoßen auf das eine oder das andere.

Die Alternative, die ab 2013 in akademischen Kreisen zu diskutieren begann, war, die lineare Kette aufzugeben und stattdessen einen gerichteten azyklischen Graphen (DAG) zu verwenden. Jede Transaktion bestätigt selbst mehrere frühere; das Netzwerk wächst wie ein Baum, nicht wie ein Seil. Theoretisch ergibt das einen Durchsatz, der mit der Anzahl der Teilnehmer wächst, und beseitigt den Wettbewerb um Blockplatz – also Gebühren.

Theoretisch. In der Praxis hatte bis 2014 niemand ein DAG-Netzwerk gestartet. Es gab Papers, es gab Ideen, es gab einige mathematische Modelle. Es gab kein funktionierendes Netzwerk.

IOTA war das erste. Der Autor der mathematischen Beschreibung – des Whitepapers namens „Tangle“ – war Sergei Popow, ein ausgebildeter Mathematiker. Wie Come-from-Beyond es im August 2021 formulieren wird: „Popow schrieb das Tangle-Whitepaper.“ Die technische Umsetzung, also das Schreiben des funktionierenden Codes, übernahm Come-from-Beyond zusammen mit mehreren anderen Leuten. IOTA selbst hatte kein Whitepaper – es gab das Tangle-Whitepaper, signiert von Popow. „IOTA hatte kein Whitepaper, nur Tangle hatte eines“, wird er im Juli 2024 klarstellen.

Im August 2021 wird er ein weiteres Detail klarstellen, das für das Folgende wichtig ist: Zu dem Zeitpunkt, als IOTAs Genesis-Block erstellt wurde, war David Sønstebø – der Mann, der in ein paar Jahren im öffentlichen Raum als „IOTA-Mitgründer“ bezeichnet werden würde – kein Mitglied des Teams. Er kam später dazu. Zum Zeitpunkt des Netzwerkstarts war er nicht dabei. Das ist keine umstrittene Interpretation, es ist eine Tatsachenfeststellung: „Dom ist kein Gründer, er war nicht einmal Mitglied des IOTA-Teams, als Genesis erstellt wurde.“

IOTA startete im Juni 2016. Auf dem Höhepunkt des nächsten Zyklus, Ende 2017 bis Anfang 2018, wird es in dasselbe Cointelegraph-Ranking wie NXT aufgenommen. Zweiter Platz. Rendite von 424.084 Prozent. Viertausendzweihunderteinundvierzig x. Höher als bei Ethereum. Niedriger – nur als bei NXT.

Zwei Netzwerke von einer Person – erster und zweiter Platz in der gesamten Geschichte der Krypto-ICOs nach Rendite. Cointelegraph, nicht Come-from-Beyond, hat gezählt. Es ist ein öffentliches Ranking.

Was danach geschieht

2017–2018 wird um IOTA herum die IOTA Foundation (IF) gegründet – eine deutsche gemeinnützige Organisation mit Sitz in Berlin. Das Ziel: strukturelle Projektverwaltung, Förder-Infrastruktur, Unternehmenspartnerschaften. Auf dem Papier sieht alles aus wie bei jedem ernsthaften Krypto-Projekt jener Zeit.

In der Praxis beginnt, nach Come-from-Beyonds Darstellung, das, was in seinen Gesprächen fünf Jahre später mit einem Wort bezeichnet wird – Zusammenbruch.

„Bei IOTA hörte alles auf, wie beabsichtigt zu funktionieren, nachdem die IOTA Foundation gegründet wurde. Sie nahmen alle Ressourcen für bedeutungslose Partnerschaften, also verließ ich IOTA und

beschloss, Qubic eigenständig zu betreiben, statt es auf IOTA laufen zu lassen“ – Formulierung von Juli 2024.

Und ausführlicher, Juli 2025: „IOTA brach zusammen, weil Leute Geld und Ressourcen zum eigenen Vorteil veruntreuten. Sie nahmen buchstäblich Geld und Entwickler, die der Kernentwicklung gewidmet waren, um Nebenprojekte im Zusammenhang mit IOTA zu entwickeln und zu bewerben, in die sie investiert hatten.“

Ich werde die Details nicht nacherzählen. Sie sind teilweise öffentlich – in offenen Gerichtsdokumenten in Norwegen, wohin 2019–2021 der Großteil des Rechtsstreits verlagert wurde. Ein Teil ist geschlossen. Ein Teil liegt in Korrespondenz, die nie öffentlich werden wird.

Einige festgehaltene und überprüfbare Fakten:

Come-from-Beyond verließ IOTA um 2019. Der Abgang war öffentlich, mit einem genannten Grund – wie er selbst es ausdrückte, „die IOTA Foundation ist zu einer Bande verkommen, die sich nur um Geld kümmert, nicht um Errungenschaften“. Das Netzwerk selbst wurde nicht zerstört. Er nutzte seine Rolle als Kernentwickler nicht, um IOTA von innen zu zerstören, obwohl er über alle technischen Mittel dazu verfügte.

Parallel dazu wurde ihm der Zugang zur Jinn-Dokumentation entzogen – Jinn war ein Projekt zur Entwicklung eines proprietären ternären Prozessors, konzipiert als Hardware-Schicht für IOTA (und für Aigarth, aber dazu später mehr). „David hält die Jinn-IP als Geisel, also musste ich einen Algorithmus erfinden, der Jinn-Schaltkreise ohne menschliche Hilfe konstruiert. Jetzt wird das im Qubic-Mining verwendet“ – knappe Formulierung von Dezember 2021. Jinn Labs, das Team, das an dem Chip gearbeitet hatte, wurde von Sønstebø gefeuert.

Für die norwegischen Klagen gab Come-from-Beyond nach eigenem öffentlichem Bekunden eine siebenstellige Summe in Dollar aus – mehr als eine Million Dollar seines persönlichen Geldes. Bis August 2021 hatte er bereits mindestens einen Fall gewonnen – gegen IOTA AS und die IOTA Foundation. Wie er es ausdrückt: „Die aktuell gewonnene Klage war nicht gegen D&D;, sie war gegen IOTA AS und die IOTA Foundation.“

Aus der Perspektive unserer Geschichte – der Geschichte der „Erschaffen-und-Gehen“-Methode – ist ein Detail wichtig. Der Abgang von IOTA war kein geplanter Abgang, wie der von BCNext von NXT. Es war ein erzwungener Abgang in einem Moment, in dem ein als Inkubator für Qubic konzipiertes Projekt von innen übernommen worden war und für seinen ursprünglichen Zweck nicht mehr geeignet war. Come-from-Beyond geht nicht, weil die Arbeit erledigt ist. Er geht, weil die Arbeit hier nicht mehr getan werden kann. Das ist eine andere Art von Abgang – aber im Ergebnis der Methode wirkt es symmetrisch. Die Idee wird evakuiert, das Netzwerk lebt sein eigenes Leben weiter, seine Erbauer kommerzialisieren es weiter, so gut sie können.

Jinn und der Algorithmus, der zum Herzen von Qubic wird

Hier müssen wir bei einem technischen Detail innehalten, denn es ist der wichtigste Verbindungspunkt zwischen zwei Kapiteln dieses Buches und die Erklärung dafür, warum Qubic so gebaut ist, wie es ist.

Jinn war ein ternärer (dreiwertiger) Prozessor, konzipiert als Hardware-Beschleuniger für IOTA-Operationen und, langfristig, als Ausführungsschicht für Aigarth. Ternäre Logik ist im modernen Rechnen selten, aber theoretisch effizienter für bestimmte Aufgabenklassen, einschließlich einer Reihe von neuronalen Netzoperationen. Jinn existierte als Projekt des Jinn-Labs-Teams seit 2015, hatte einen eigenen IPO (JINN-Token-Halter erhielten einen Anteil am künftigen Produkt) und funktionierende Prototypen.

Als Sønstebø Come-from-Beyond den Zugang zur Dokumentation entzog und das Team feuerte, wurde es physisch unmöglich, die nächste Version des Chips herzustellen. Aber die Software-Aufgabe – „wie beschreibt man automatisch das Schema eines solchen Prozessors, ohne manuelle technische Arbeit, allein anhand einer Spezifikation dessen, was er berechnen muss“ – blieb bestehen.

Come-from-Beyond löste diese Aufgabe im Laufe des folgenden anderthalben Jahres.

Der Algorithmus, den er entwickelte, nimmt die Beschreibung einer gewünschten Funktion – zum Beispiel eines kleinen künstlichen neuronalen Netzes – und setzt automatisch, aus elementaren Operationen, ein logisches Schaltschema zusammen, das diese Funktion umsetzt. Ohne Mensch. Ohne dass ein Ingenieur manuell Architekturen ausprobiert. Eine reine Suche durch den Raum möglicher Schaltschemata.

„Jetzt wird das im Qubic-Mining verwendet“ – knapper Satz, Dezember 2021.

Das ist kein beiläufiger technischer Exkurs. Das ist der Kern dessen, was in Qubic UPoW heißt – Useful Proof of Work. Qubic-Miner erraten keine Hashes; sie führen automatische Synthese von neuronalen-Netz-Schaltschemata aus. Jeder Versuch ist ein Stück nützlicher Rechenarbeit, das in der Summe etwas Größeres trainiert.

Eine Sache ist hier wichtig festzuhalten. Der Verlust von Jinn zwang ihn dazu, etwas zu erfinden, das später zum Herzen von Qubic werden sollte. Hätte Sønstebø ihm den Zugang nicht entzogen – hätte es keine erzwingende Bedingung gegeben. Ohne erzwingende Bedingung – keinen Algorithmus. Ohne Algorithmus – Qubic würde nicht so aussehen, wie es aussieht. Das ist einer jener seltenen Fälle, in denen man den Moment genau bestimmen kann, in dem ein feindlicher Umstand zur Voraussetzung für die nächste Architektur wird.

Widrigkeit zu Architektur – Ärger, der sich in Design verwandelt. Ingenieure in unserer Branche können selten auf einen solchen Moment in ihrer eigenen Biografie zeigen. Come-from-Beyond kann es.

In einer frühen Qubic-Erklärung fasst er zusammen, was er tatsächlich baute: „Qubic begann sein Leben als ein zum Akronym gewordenes Initialwort, QBC, das für quorenbasierte Berechnung steht… Konkret ist Qubic ein Protokoll, das IOTAs Lösung für quorenbasierte Berechnungen spezifiziert, einschließlich Konstrukten wie Orakelmaschinen, ausgelagerten Berechnungen und Smart Contracts.“

Qubic. April 2022 — die Hauptsache

Am 13. April 2022 wird der erste Qubic-Block erstellt. Das Netzwerk läuft im Mainnet.

Come-from-Beyond startet, was er sich zwanzig Jahre zuvor vorgenommen hatte.

In diesem Kapitel werde ich Qubic nicht Stück für Stück nacherzählen. Das erfordert den gesamten nächsten Teil des Buches, und dieser Teil ist in Arbeit. Hier – nur der grobe Umriss. Ein paar Entitäten, fünf Absätze. Gerade genug, um klarzumachen, was sich aus der Erfahrung der beiden vorherigen Projekte zusammensetzte.

676 Computoren. Das Qubic-Netzwerk wird nicht von einer beliebigen Anzahl von Validatoren und nicht von einem offenen Mining-Pool getragen, sondern von einem festen Pool von 676 Teilnehmern, wöchentlich teilweise rotiert nach einer öffentlich angekündigten Regel. Die Zahl 676 ist nicht zufällig, aber die Erklärung ihrer Bedeutung folgt im nächsten Kapitel.

UPoW — Useful Proof of Work. Genau das, worüber im IOTA-Abschnitt gesprochen wurde. Miner erraten keine Zufallszahlen; sie leisten nützliche Rechenarbeit – automatische Synthese von neuronalen-Netz-Schaltschemata. In der Summe trainiert diese Arbeit die Plattform, die seit den frühen 2000er-Jahren unter dem Arbeitstitel Aigarth in Come-from-Beyonds Kopf lebt.

Aigarth. Ich beschränke mich darauf, es „eine seit den frühen 2000ern von CfB konzipierte KI-Plattform, für die diese ganze Kryptowährungsinfrastruktur ein vorbereitendes Skelett ist“ zu nennen. Was Aigarth tatsächlich ist, wie es intern aufgebaut ist, was es von ChatGPT, Gemini, Claude und den anderen öffentlichen großen Modellen von 2025–2026 unterscheidet – ist das Thema von Teil fünf des Buches. Innerhalb dieses Kapitels zählt nur eines: Der Kryptowährungsteil von Qubic existiert um Aigarths willen, nicht umgekehrt.

Der Arbitrator. In der aktuellen Architektur von Qubic gibt es eine besondere Rolle – den Arbitrator, manuell ausgeübt von Come-from-Beyond selbst. Seine Funktionen sind durch den Quellcode begrenzt: Er kann keine Coins drucken, er kann keine Transaktionen ändern, er kann niemandes Wallet schließen. Aber bestimmte koordinierende Entscheidungen – zum Beispiel die Änderung der Regeln für die Auswahl der Computoren für die nächste Woche – laufen über ihn. Diese Rolle ist temporär. Nach dem angekündigten Plan wird der Arbitrator am 13. April 2027, genau fünf Jahre nach dem Mainnet-Start, abgeschafft. Der letzte Hebel, mit dem der Schöpfer das Netzwerk berühren kann, wird demontiert.

Das ist der vierte Abgang. Wenn wir die Arbeitsannahme des vorigen Kapitels akzeptieren – dass Come-from-Beyond irgendein Teil von Satoshi ist –, ist dies der vierte öffentliche Abgang in derselben Kette. Satoshi im Dezember 2010, BCNext im April 2014, Come-from-Beyond selbst aus IOTA um 2019, und der vierte – der 13. April 2027, der Arbitrator von Qubic.

Drei sind bereits geschehen. Der vierte ist angekündigt, terminiert und ins Protokoll geschrieben.

Wenn es wie geplant geschieht – ist die Methode zum vierten Mal bestätigt. Wenn nicht – ist sie es nicht. Das ist eine falsifizierbare Vorhersage mit einem konkreten Datum. Ingenieurs-Biografien enthalten so etwas selten.

Bemerkenswert ist, dass Qubic eine Rückkehr zum ursprünglichen Konzept ist. Genau jene quorenbasierte Berechnung, die als QBC innerhalb von IOTA existierte, wurde herausgezogen, überdacht, durch Erfahrung gestärkt und eigenständig gemacht. Zwanzig Jahre Arbeit an einer großen Idee fügten sich zu einem Netzwerk zusammen.

Noch ein charakteristisches Detail, von der Art, die nicht in Berichten auftaucht. Qubic startete nicht mit leerem Publikum. Beim Start hatte das Projekt bereits eine Community – dieselben Leute, die NXT

hielten, dann zu IOTA kamen und nun zu Qubic kamen. Come-from-Beyond beschrieb das im November 2023 selbst mit einer anschaulichen Metapher: „Schon mal Spielgilden gesehen, die verschiedene Spiele zusammen spielen? Sie gehen als geformte Gilde ohne Gründer von Spiel zu Spiel. Wir kamen von IOTA zu Qubic, waren davor in Nxt." Das bedeutet, Qubic musste nicht von Grund auf erklären, wer Come-from-Beyond war und warum es sich lohnte, seinem technischen Urteil zu vertrauen. Eine Gruppe von Menschen, die sich durch eigene Erfahrung selbst überzeugt hatte, ging bereits mit ihm. Und das erklärt übrigens auch separat, warum die frühe Qubic-Community sich strukturell von denen zufälliger Krypto-Projekte von 2022 unterscheidet: Sie hat eine unverhältnismäßig hohe Zahl von Menschen mit dreizehn Jahren Krypto-Erfahrung und der Erinnerung an zwei vorherige Übergänge.

Come-from-Beyond ordnet seine drei Projekte selbst ein, knapp und ohne falsche Bescheidenheit: „Kaspa, IOTA, Qubic. Qubic ist bisher das beste." (Kaspa ist in dieser Liste ein Netzwerk, das nicht von ihm gemacht wurde; er erwähnt es zum Vergleich, weil dessen Entwickler einen Teil seiner frühen DAG-Forschung nutzen. Wichtig sind nicht Kaspa, sondern die anderen beiden Elemente – IOTA und Qubic. Nach seiner eigenen Einschätzung steht Qubic über IOTA.)

Er kam zum Qubic-Start nicht nur mit einer Idee. Er kam mit dreizehn Jahren Erfahrung im Starten funktionierender Krypto-Netzwerke, mit einer doppelt bestätigten Erfolgsbilanz und mit einem Algorithmus, den niemand außer ihm hätte erfinden können, weil niemand sonst Jinn verloren hatte.

Unter der Haube: das Muster der drei Projekte

Stellt man die drei Projekte nebeneinander, werden sieben gemeinsame Merkmale sichtbar. Nicht eines oder zwei – sieben, die sich systematisch genug wiederholen, dass man sie nicht als Zufall abtun kann.

Erstens, das Pseudonym als Unterschrift. BCNext für NXT. Come-from-Beyond für IOTA und Qubic. In beiden Fällen ist das Handle keine Art, sich zu verstecken. Es ist eine Art zu unterschreiben und gleichzeitig den Mann vom Projekt zu trennen. BCNext ist keine Maske, es ist eine Identität mit eigenem privaten Schlüssel und eigener kryptografischer Bindung an den NXT-Genesis-Block. Come-from-Beyond ist keine Maske, es ist die Identität, unter der seit 2011 alle öffentliche Aktivität ausgeübt wird.

Zweitens, kompakter Code. NXT – dreitausend Zeilen Java. Qubic-Kern – ebenfalls kompakt; Come-from-Beyond hat keine genauen Zahlen öffentlich genannt, aber nach indirekten Anzeichen und der Art, wie er darüber spricht, sind es dieselben Größenordnungen. IOTA – hier ist es schwieriger, weil der Quellcode nach Come-from-Beyonds Abgang von der IOTA Foundation übernommen und überarbeitet wurde, und es wäre falsch, die Größe des Originals anhand des aktuellen Zustands des Netzwerks zu beurteilen.

Drittens, keine Whitepaper. „Keines meiner Projekte hatte ein Whitepaper, ich bin Ingenieur, kein Schriftsteller." Zwei der drei Netzwerke – erster und zweiter Platz in der Geschichte der Krypto-ICOs nach Rendite. Das ist kein Versehen, es ist ein Prinzip. Funktionierender Code zählt mehr als ein Dokument. Ein Dokument beschreibt die Absicht; der Code setzt sie um. Funktioniert der Code, ist die Absicht verifiziert; funktioniert der Code nicht, rettet ihn kein noch so schönes Dokument.

Viertens, die Community im Voraus warnen. NXT wurde ganz am Anfang offen als „temporäres Projekt" erklärt. IOTA – als der Konflikt mit der Foundation sichtbar wurde, kündigte

Come-from-Beyond seinen Abgang und dessen Gründe öffentlich an. Qubic – regelmäßig, fast wöchentlich, erinnert Come-from-Beyond in seiner öffentlichen Korrespondenz an die Risiken und daran, dass Qubic-Halter selbst Entscheidungen treffen müssen. Das ist keine Bescheidenheit; es ist ein in die Methodik eingeschriebener Haftungsausschluss.

Fünftens, im richtigen Moment gehen. BCNext – im April 2014, als NXT gestartet war und funktionierte. Come-from-Beyond aus IOTA – um 2019, als klar wurde, dass die Foundation das Projekt übernommen hatte. Die geplante Abschaffung des Qubic-Arbitrators – 13. April 2027. Ein Abgang war geplant. Einer war erzwungen. Einer steht noch bevor. Aber in allen drei Fällen ist die Struktur dieselbe: Der Schöpfer tritt zurück, das Netzwerk läuft weiter.

Sechstens, die Erfolgsbilanz. Zwei der drei Netzwerke – erster und zweiter Platz nach ROI in der Geschichte der Krypto-ICOs laut einem unabhängigen Cointelegraph-Ranking. 1.265.555 Prozent und 424.084 Prozent. Come-from-Beyond kommentiert das knapp: „Schau dir das Nxt- und IOTA-Kurschart an, du kannst Stellen erkennen, an denen wir nutzlose Halter loswurden. Glaubst du, zweimal den Top-ROI zu erzielen ist Zufall? Ich bin Ingenieur, und technische Gesetze wirken überall gleich."

Das ist ein wichtiges Zitat, und zwei Dinge darin verdienen Aufmerksamkeit. Das erste – „wir wurden nutzlose Halter los". Das bezieht sich auf periodische Ereignisse – einschließlich FUD, Provokationen, Kurskorrekturen –, die wenig überzeugte Halter aus dem Projekt spülen, bevor das Projekt Mainstream wird. Das sind keine Zufälle, das ist ein bewusster Teil der Strategie. Das erklärt, warum Come-from-Beyond selbst manchmal öffentlich skeptische Dinge über seine eigenen Projekte äußert. Das ist kein Paradox – es ist ein Filter. Das zweite – „technische Gesetze wirken überall gleich". Er sagt nicht „ich hatte Glück". Er sagt „ich bin Ingenieur". Das ist eine direkte Antwort auf jedes Argument der Form „Krypto ist eine Lotterie".

Siebtens, die Community als reisende Gilde. Das wurde im Qubic-Abschnitt bereits erwähnt – ich wiederhole nur die Formel: NXT → IOTA → Qubic-Halter bewegen sich durch Projekte, wie eine Gaming-Gilde sich durch Spiele bewegt. Das senkt strukturell die Startkosten jedes nachfolgenden Projekts: Ein Teil des Vertrauens überträgt sich vom vorigen. Nicht alles; jedes Projekt muss den technischen Wert immer noch von Grund auf beweisen. Aber das grundlegende Vertrauen in den Ingenieur selbst – überträgt sich.

Und ein achtes Merkmal, gesondert, nicht über die Projekte, sondern über die Rollentrennung. In allen drei Fällen ist Come-from-Beyond der Ingenieur, der Erfinder, der Architekt. Die Kommerzialisierung erledigen andere. Bei NXT – das Unternehmen Jelurida, das die Unterstützung nach BCNexts Abgang übernahm, Ardor schuf, es B2B ausrichtete. Bei IOTA – die IOTA Foundation, die das Projekt übernahm und auf ihren eigenen Kurs steuerte (nach Come-from-Beyonds Ansicht in eine Sackgasse, aber das ist nun ihre eigene Verantwortung). Bei Qubic – eine verteilte Community von Entwicklern und Ökosystem-Projekten, die Stand 2026 Anwendungen, Börsen, Brücken und Dienste auf dem Kernprotokoll aufbauen. Erfinder und Kommerzialisierer sind zwei verschiedene Rollen, selten in einer Person vereint. Bei Come-from-Beyond ist diese Disziplin der Trennung nun dreifach in seine Biografie eingeschrieben.

Sieben Merkmale, reproduziert über drei Projekte hinweg. Verschiedene Architekturen, verschiedene Märkte, verschiedene Jahre, verschiedene Teams. Dieselbe Person, dieselbe Methode, dasselbe Ergebnis.

Zeit weiterzugehen

Bis zum 13. April 2022 hatte Come-from-Beyond alles, was er 2013 nicht hatte. Zwanzig Jahre Nachdenken über Aigarth. Zwei gestartete Krypto-Projekte, eines vollständig verlassen, eines gezwungenermaßen in fremde Hände übergegangen. Zwei bestätigte Plätze in der historischen Top-Liste nach Kapitalrendite. Der Algorithmus zur automatischen Schaltschema-Synthese, geboren aus dem Verlust von Jinn. Eine Community, die aus den vorherigen Projekten mitgekommen war. Eine industrielle Reife, die dreizehn Jahre zuvor nicht existierte. Und – die Hauptsache vielleicht – der Beweis für sich selbst, dass die „Erschaffen-und-Gehen"-Methode wirklich funktioniert. Zweimal. In Projekten mit unterschiedlichen Architekturen und unterschiedlichen Schicksalen. Mit einem Ergebnis, das ein unabhängiges Drittanbieter-Ranking auf den ersten beiden Plätzen festgenagelt hat.

Qubic startete. Das dritte Projekt der Reihenfolge nach, aber das erste der Absicht nach. Genau jenes, für das alles andere getan worden war.

Und hier, 2026, auf halbem Weg zwischen Start und geplantem Abgang des Arbitrators stehend, kann man einen Schritt zur Seite treten und die Frage stellen, die dieser Teil des Buches ausführlich beantwortet hat: Wer ist Come-from-Beyond, und warum lohnt es sich zu glauben, dass er weiß, was er tut. Die aus den beiden vorherigen Kapiteln zusammengesetzte Antwort lautet etwa so: ein Ingenieur mit zwanzig Jahren Erfahrung, der seine Methode zweimal bewiesen hat, der seine Abgänge öffentlich im Voraus ankündigt, der seit den frühen 2000ern an einer großen Aufgabe (Aigarth) arbeitet, der Kryptowährungen als Infrastruktur nutzt und nicht als Ziel, und der seinen vierten Abgang auf ein konkretes Datum terminiert hat. Geschieht dieser Abgang – ist die Methode zum vierten Mal bestätigt. Geschieht er nicht – ist sie es nicht. Das ist ein ehrlicher Falsifikator.

Aber die nächste Frage ist eine andere. Nicht wer und nicht warum, sondern wie. Wie genau ist das Qubic-Netzwerk gebaut, um fähig zu sein, ohne seinen Schöpfer zu leben? Warum 676 Teilnehmer – und nicht 700 und nicht 1.000? Wie werden sie jede Woche ersetzt, wer wählt sie aus, und nach welchen Regeln? Was geschieht mit den QU-Coins darin, wie werden sie emittiert, und wohin verschwinden sie? Wie genau funktioniert UPoW, und wie verwandelt sich nützliche Rechenarbeit in Schutz des Netzwerks vor Angriffen? Und die Hauptsache – wie ist der Moment des Übergangs gestaltet, wenn der Arbitrator abgeschafft wird und der letzte Punkt menschlicher Steuerung aus dem Protokoll verschwindet?

Diese Fragen handeln nicht vom Mann. Sie handeln von Technik. Und um sie zu beantworten, muss man in das Protokoll hineingehen.

Im ersten Kapitel dieses Buches sprachen wir über die Kaskade der Kohle als Metapher für die Entwicklung von Technologien. Darby erhielt 1709 das erste mit Koks geschmolzene Eisen, wusste aber nicht, was er mit dem in die Luft entweichenden Gas anfangen sollte. Murdoch fand 1792 heraus, wie man dieses Gas in ein Rohr sammelt und separat zur Straßenbeleuchtung nutzt – und dieser Moment war der Beginn einer völlig neuen Industrie, die binnen eines Jahrhunderts die Infrastruktur der Stadt ersetzte. Der qualitative Sprung – von „Kohle zum Heizen verbrennen" zu „sammeln, was dabei freigesetzt wird, und es arbeiten lassen".

Bitcoin ist in dieser Metapher Darby. Das erste Feuer. Eine unglaubliche Errungenschaft, die eine Ära einleitete, aber einzweckig: Die gesamte Rechenleistung, die freigesetzt wird, während das Netzwerk seine Arbeit verrichtet, wird sinnlos verbrannt, wie das Gas, das über Darbys Hochofen in Coalbrookdale

zu Beginn des achtzehnten Jahrhunderts in den Himmel stieg. Qubic ist in dieser Metapher Murdoch. Der Moment, in dem Menschen anfangen, das Gas in ein Rohr zu sammeln. Das Coalbrookdale des digitalen Zeitalters – so werden Technikhistoriker diese Phase wahrscheinlich in hundert Jahren nennen, falls dann noch jemand da ist, um es zu tun.

Diese Phase bricht bereits an. Über ihre inneren Mechanismen – der nächste Teil des Buches. Sein erstes Kapitel handelt von den 676 Stimmen, die das Netzwerk tragen.

TEIL III

Die Mechanik

676 Stimmen

6
676 Stimmen

Die Zahl 676 ist nicht ästhetisch. Sie ist nicht hübsch. Sie ist nicht symbolisch. Es ist die exakte Anzahl der Teilnehmer, die zu jedem gegebenen Zeitpunkt gleichzeitig die tragende Hauptstruktur von Qubic bilden. Sechshundertsechsundsiebzig Computer, verbunden zu einem einzigen Netzwerk, die alle paar Sekundenbruchteile über ein und dieselbe Frage abstimmen: „Was wird der nächste Zustand des gesamten Systems sein."

Wenn Sie sich diese Konstruktion in einem einzigen Bild vorstellen wollen, stellen Sie sich ein Parlament mit 676 Sitzen vor. Das Parlament hat eine Regel: Um eine Entscheidung zu verabschieden, braucht man mindestens 451 Ja-Stimmen. Vierhunderteinundfünfzig ist knapp mehr als zwei Drittel von 676. Weniger als das – die Entscheidung geht nicht durch.

Das Parlament hat keinen Präsidenten mit Sonderbefugnissen. Es hat keine Fraktionen mit Privilegien. Keine Parteidisziplin. Keine Lobbyisten, deren Rolle im Flur sich von der Rolle der Abgeordneten im Plenarsaal unterscheidet. Jeder der 676 hat genau eine Stimme, und diese Stimme kann nicht gekauft, aufgekauft, gebündelt oder in zwei Stimmen umgewandelt werden, egal wie viel Arbeit dieser Abgeordnete in der vergangenen Woche geleistet hat.

Einmal pro Woche ändert sich die Zusammensetzung des Parlaments teilweise. Nicht vollständig – allmählich, nach einer festen Regel. Wer über die vergangene Woche das schlechteste Ergebnis zeigte, tritt seinen Sitz an diejenigen ab, die in derselben Woche nützlichere Arbeit geleistet haben und nun den Einzug beanspruchen. Die Anzahl der auf einmal ausgetauschten Abgeordneten ist starr gedeckelt – sie kann nicht durch eine einmalige Entscheidung aufgebläht und nicht auf null zurückgesetzt werden. Das Parlament erneuert sich in einem regelmäßigen Rhythmus, so wie sich Laub erneuert, nur nicht im Herbst, sondern alle sieben Tage.

Das ist, auf der Ebene einer groben Analogie, wie das Qubic-Netzwerk gebaut ist.

Die Analogie hat, wie immer, eine Grenze, über die hinaus man sie nicht dehnen sollte. 676 Computer streiten nicht, halten keine Reden, stimmen nicht unter Druck gegen ihre Überzeugung. Sie führen eine präzise Abfolge kryptografischer Operationen aus, in der eine „Stimme" eine Signatur ist und eine „Entscheidung" die Annahme des neuen Netzwerkzustands. Aber das Grundprinzip – ein fester kleiner Kreis, eine Zwei-Drittel-Schwelle für jede Änderung, regelmäßige teilweise Rotation – ist genau das oben beschriebene. Das ist der Rahmen, von dem aus wir starten.

Es gibt noch eine andere, organischere Metapher, die es sich lohnt, hier einmal zu erwähnen und gegen Ende des Buches wieder aufzugreifen. Unter den Pilzen in einem Waldökosystem liegt das Myzel – ein Netzwerk feiner Fäden, das sich Dutzende Meter in alle Richtungen erstreckt. Myzel hat kein Zentrum.

Es hat keinen Besitzer. Einzelne Abschnitte davon sterben kontinuierlich ab und regenerieren sich; das Ganze besteht dabei länger fort als jedes seiner Fragmente. Als ich zum ersten Mal ein Diagramm von Qubics 676 Computoren neben ein Diagramm der Mykorrhiza sah, war ich von der topologischen Ähnlichkeit beeindruckt. Das ist keine Mystik, und es ist keine Poesie; es ist einfach die Feststellung der Tatsache, dass verteilte Systeme ohne Zentrum – biologische oder konstruierte – zu denselben architektonischen Lösungen konvergieren.

Dieses Kapitel handelt von der Mechanik. Wie die 676 tatsächlich abstimmen. Warum jede Entscheidung eine Schwelle von 451 erfordert, statt etwa 339 (einfache Mehrheit) oder 676 (Einstimmigkeit). Was ein Tick ist – die grundlegende Zeiteinheit des Netzwerks, in der all das stattfindet. Wie die wöchentliche Rotation der Mitgliedschaft funktioniert, und warum genau diese Rotation das Netzwerk strukturell resistent gegen eine Übernahme von innen macht.

Im vorigen Kapitel verglich ich Qubic mit Murdoch im Jahr 1792 – dem Mann, der erstmals das aus Hochöfen verschwendete Gas sammelte und in ein Rohr leitete. Die 676 Stimmen sind nicht Qubics „Gasrohr“ selbst. Das Gasrohr ist das nächste Kapitel nach diesem, über nützliche Rechenarbeit. Aber damit das Rohr hält und nicht übernommen wird – braucht man zuerst eine Konstruktion, die es trägt. Boden, Wände, Fundament. Coalbrookdale des digitalen Zeitalters, Tag eins: der Zusammenbau des Rahmens.

Beginnen wir mit der Schwelle von 451.

Ein Quorum von 451 von 676

Wenn ein Parlament 676 Sitze hat und jede Entscheidung mindestens 451 Ja-Stimmen erfordert, dann hält eine hypothetische koordinationsfähige Koalition nicht eine Mehrheit der Sitze, sondern eine Supermehrheit. Eine Mehrheit ist, wenn 51 von 100 hinter dir stehen. Eine Supermehrheit ist, wenn zwei Drittel hinter dir stehen. Formal: 2/3 von 676 ist 450,67. Man rundet auf, weil eine Stimme eine diskrete Größe ist: Es gibt keine Bruchstimmen. Man erhält 451.

Woher kam die Zwei-Drittel-Logik überhaupt, statt etwa drei Viertel oder einer einfachen Mehrheit von 50 % + 1?

Zwei Drittel ist die klassische Schwelle in verteilten Systemen, in denen sich manche Teilnehmer unehrlich verhalten oder einfach ausfallen können. Sie stammt aus einem Feld, das Informatikforscher Ende der 1970er unter dem Namen „das Problem der byzantinischen Generäle“ entwickelten. Der Name ist konventionell; er ist einer Parabel über eine Gruppe byzantinischer Generäle entnommen, die, nachdem sie eine Stadt umzingelt haben, sich per Boten auf einen gemeinsamen Plan (Sturmangriff oder Rückzug) einigen müssen, wobei sie wissen, dass einige der Generäle Verräter sein könnten und widersprüchliche Botschaften weitergeben würden. Der Kern des Problems: Bei welcher maximalen Anzahl von „Verrätern“ in der Gruppe können die ehrlichen Teilnehmer noch zu einer einzigen, korrekten Entscheidung gelangen?

Die mathematische Antwort erwies sich als hart. Wenn Verräter bis zu einem Drittel der Gruppe ausmachen können, können die ehrlichen zwei Drittel eine gemeinsame Entscheidung erarbeiten, die die Verräter nicht durchkreuzen können. Sind mehr Verräter als ein Drittel vorhanden – kann kein Protokolltrick die Lage retten; die Gruppe ist prinzipiell unfähig zu garantierter Einigung. Zwei zu eins

ist die mathematische Grenze der Widerstandsfähigkeit eines verteilten Systems gegen unehrliche oder ausgefallene Teilnehmer.

Eine naheliegende Frage könnte aufkommen: Warum nicht mit einer einfachen Mehrheit, also 51 %, auskommen? Bei gewöhnlicher Abstimmung in einem realen Parlament, in dem alle Abstimmenden im selben Saal sitzen und sich gegenseitig um Wiederholung bitten können, funktioniert eine einfache Mehrheit gut. In einem verteilten Netzwerk, das nur durch Nachrichten verbunden ist, wird es komplizierter. Stellen Sie sich für einen Moment folgendes Szenario vor. 339 Computoren schicken ihre Stimmen für eine Version des neuen Zustands ein; weitere 337 stimmen für eine andere, widersprüchliche. Wer hat recht? Gibt es 226 böswillige Teilnehmer im Netzwerk, ist theoretisch eine Situation möglich, in der diese 226 der einen Netzwerkhälfte die eine Stimme und der anderen Hälfte die entgegengesetzte Stimme schicken. Jeder Teil des Netzwerks sieht eine lokale Mehrheit für seine eigene Version und akzeptiert sie als kanonisch. Das Netzwerk spaltet sich in zwei parallele Welten, jede von ihrer eigenen Richtigkeit überzeugt. Das ist das klassische „byzantinische“ Problem in Aktion. Die Zwei-Drittel-Schwelle beseitigt diese Möglichkeit: Bei jeder Anordnung kann, wenn 451 Teilnehmer gleich abgestimmt haben, eine zweite Gruppe von 451 im Netzwerk physisch nicht existieren, denn 451 + 451 = 902 > 676. Daher ist jede Entscheidung, die 451 Stimmen gesammelt hat, eindeutig kanonisch. Ein alternativer Zweig, der parallel dasselbe Unterstützungsniveau zusammengebracht hat, existiert arithmetisch nicht.

Diese Grenze ist buchstäblich in das Qubic-Protokoll verdrahtet. Von den 676 Computoren – eben jenen „Parlamentsabgeordneten“ – können bis zu 225 Teilnehmer gleichzeitig nicht verfügbar, gestört, in einer Netzwerkpartition gefangen oder gegen das Netzwerk verschworen sein. Das ist weniger als ein Drittel. Die verbleibenden 451 sind bereits eine Supermehrheit; sie treffen weiterhin Entscheidungen, und jede von ihnen getroffene Entscheidung ist kanonisch für das Netzwerk. Aber wenn 226 oder mehr sich gegen das Netzwerk stellen, kann das Netzwerk laut Protokoll keinen Konsens erreichen; es friert ein und wartet darauf, dass eine arbeitsfähige Masse wiederhergestellt wird. Es beginnt nicht, „alternative“ Blöcke zu akzeptieren, spaltet sich nicht in verfeindete Zweige, driftet nicht in einen Zustand, aus dem es später über seine eigene Rettung abstimmen müsste. Es hält an. Das ist in gewissem Sinne eine Sicherheitstechnik, die der von Bitcoin entgegengesetzt ist: Bitcoin arbeitet auch bei starker Konzentration der Hashrate weiter, nur mit verringertem Schutz. Qubic arbeitet entweder mit garantiertem Schutz, oder es arbeitet gar nicht.

Nun ein wichtiges, subtiles, oft missverstandenes Detail.

Jeder Computor hat genau eine Stimme. Nicht „eine Stimme pro Kapitaleinheit“. Nicht „Stimmen proportional zur Rechenleistung eines Computers“. Nicht „je mehr ich in der vorigen Epoche verdient habe, desto mehr Stimmen habe ich in dieser“. Ein Teilnehmer – eine Stimme. Das ist eine Protokollregel, die sich nicht umgehen lässt, egal wie viele Ressourcen ein Teilnehmer angehäuft hat.

Das ist, tritt man einen Moment zurück, der zentrale strukturelle Unterschied zwischen Qubic und Systemen, in denen das Gewicht einer Entscheidung proportional zur investierten Ressource ist. In Bitcoin bekommt ein großer Pool, der einen großen Anteil der Hashrate konzentriert hat, eine proportional größere Wahrscheinlichkeit, den Inhalt eines Blocks zu bestimmen; je mehr Ausrüstung man hat, desto mehr Gewicht hat man. In klassischem Proof-of-Stake bekommt ein großer Coin-Halter eine proportional größere Wahrscheinlichkeit, Validator zu werden; je mehr Geld man hat, desto mehr

Gewicht hat man. In beiden Modellen wird angehäufte Ressource in das Recht umgewandelt, an der Gestaltung der Regeln des nächsten Schritts teilzunehmen. In Qubic ist diese Umwandlung durch das Protokoll verboten. Ein Computor mit einer riesigen Serverflotte und ein Computor mit der Mindestkonfiguration, die ihm gerade noch den Sitz erlaubt, haben in jeder Abstimmung gleiches Gewicht – eine Stimme. Das Einzige, was viele Ressourcen einem kaufen, ist eine Chance, unter den 676 zu bleiben und in der nächsten Epoche nicht verdrängt zu werden. Aber solange man unter den 676 ist, ist das eigene Gewicht genau dasselbe wie das aller anderen.

Hier, denke ich, wird sich der aufmerksame Leser an eine der Bedingungen aus Kapitel drei erinnern. Wir formulierten sie damals mit diesen Worten: Ein Sieg im Spiel darf dem Spieler nicht die Fähigkeit geben, die Regeln des Spiels selbst zu ändern. Die Formulierung war abstrakt; dies ist ihre konkrete technische Verkörperung. Innerhalb einer einzelnen Abstimmung wandelt sich kein angehäufter Vorteil in Stimmen um. Sehen wir uns an, worüber genau abgestimmt wird.

Der Tick: Der Moment, in dem das Netzwerk eine Entscheidung trifft

Im gewöhnlichen Leben denken wir uns die Zeit als kontinuierlich. Woche geht in Woche über, Tag in Tag, ohne klare Nähte. Verteilte Netzwerke können das nicht. Damit 676 über den Planeten verstreute Computer zu einer gemeinsamen Entscheidung darüber gelangen, „was der aktuelle Zustand des Netzwerks ist“, brauchen sie ein gemeinsames diskretes Zeitraster. Sie brauchen Momente, in denen sie alle gleichzeitig auf die Welt schauen und gleichzeitig abstimmen.

In Qubic heißt diese Einheit Tick.

Ein Tick ist eine vollständige Abstimmungsrunde. Ungefähr Folgendes geschieht in jedem Tick. Zuerst wird einer der 676 Computoren ausgewählt, um für diesen Tick die Rolle des „Leaders“ zu spielen – er sammelt die Transaktionen, die im vorherigen Mikrointervall eingegangen sind, ordnet sie und schlägt das entstandene Bündel als nächsten Netzwerkzustand vor. Dann wird sein Vorschlag an alle übrigen 675 gesendet. Jeder von ihnen prüft den Vorschlag bei Erhalt gegen das Protokoll – die Transaktionen widersprechen sich nicht, der Leader hatte das Recht, überhaupt etwas vorzuschlagen, die Signaturen sind korrekt – und stimmt mit „Ja“ oder enthält sich. Wenn 451 „Ja“-Stimmen zusammenkommen, wird der vorgeschlagene Zustand als kanonisch neu akzeptiert. Das Netzwerk hat einen Schritt getan. Der nächste Tick beginnt.

Es lohnt sich zu betonen, dass die „Prüfung“ hier keine Formalität ist. Jeder Computor hält ein vollständiges aktuelles Bild des Netzwerks: welche Adressen existieren, wie viele Coins auf jeder liegen, welche Verpflichtungen bereits ausstehen, welche Transaktionen in vorherigen Ticks akzeptiert wurden. Wenn ein Vorschlag des aktuellen Leaders bei ihm eintrifft, wendet er selbst, mit eigenem Code, alle vorgeschlagenen Transaktionen auf seinen eigenen Zustand an und prüft, ob er dasselbe Ergebnis erhält, das der Leader behauptet hat. Tut er das – stimmt er „Ja“. Tut er es nicht – stimmt er nicht. Für einen böswilligen Leader gibt es einfach keine Möglichkeit, einen falschen Vorschlag durchzudrücken: 675 unabhängige Prüfer werden seine Berechnung gleichzeitig selbst durchführen und die Abweichung unabhängig voneinander sehen. Nur ein Vorschlag, der nach den Regeln des Protokolls objektiv korrekt ist, überlebt.

Zwei zentrale Punkte dieser Mechanik verdienen Hervorhebung.

Erstens – die Leader-Rolle ist nicht fest. Sie rotiert nach einer deterministischen Regel, die allen 676 Teilnehmern im Voraus bekannt ist. Das ist keine „Auktion um das Recht, einen Block vorzuschlagen“ wie bei Bitcoin, wo der Inhalt eines Blocks von demjenigen Miner geformt wird, der zufällig zuerst ein kryptografisches Rätsel gelöst hat – und das ist mit hoher Wahrscheinlichkeit ein großer Pool. In Qubic ist der Leader für jeden Tick im Voraus bekannt und wechselt zum nächsten Tick. Kein Computor kann den Strom der Vorschläge dauerhaft kontrollieren; das Höchste, was er tun kann, ist, in seinem eigenen Tick Leader zu sein, und im nächsten übernimmt der nächste Computor in der Reihenfolge. Über tausend Ticks hinweg ist jeder der 676 Computoren ungefähr gleich oft Leader.

Zweitens – die Entscheidung erfordert die Zustimmung einer Supermehrheit, nicht des Leaders. Der Leader trifft die Entscheidung nicht. Der Leader schlägt vor. Die Entscheidung wird von 451 Stimmen getroffen. Versucht ein Leader, etwas Falsches vorzuschlagen – eine Transaktion, die die Protokollregeln verletzt, oder einen Block mit einer Doppelausgabe –, werden 451 ehrliche Computoren einfach nicht dafür stimmen. Der Vorschlag geht nicht durch; einen Tick später wird sein Platz von einem Vorschlag des nächsten Leaders eingenommen, und die Arbeit des Netzwerks geht weiter. Ein verdorbener Leader kann das Netzwerk nicht länger als einen Tick aufhalten.

Übersetzt man das in die Sprache vertrauterer verteilter Systeme – bei Bitcoin wird jeder Block von genau einem Miner geformt (genauer gesagt von genau einem Pool), demjenigen, der das Glück hatte, einen Hash mit dem erforderlichen Präfix zu finden. Der Rest des Netzwerks kann diesen Block akzeptieren oder ablehnen, aber es ist immer eine Entität, die ihn formt. Bei Qubic wird jede Entscheidung kollektiv geformt: Der Leader stellt nur eine Hypothese auf; die Supermehrheit genehmigt sie. Der Unterschied liegt darin, wo die Entscheidung konzentriert ist. Bei Bitcoin – am Ort der Formung. Bei Qubic – in der verteilten Abstimmung über das gesamte Netzwerk.

Die genaue Frequenz der Ticks – genau wie viele davon pro Sekunde geschehen – wird durch eine Protokollkonstante festgelegt und in der technischen Qubic-Spezifikation beschrieben. Was für dieses Kapitel zählt, ist eines: Es gibt viele Ticks pro Zeiteinheit, die Zahl liegt im einstelligen Bereich pro Sekunde und höher, und jeder Tick ist eine vollständige Abstimmungsrunde von 676 Teilnehmern. Auf der Skala eines einzigen Tages trifft das Qubic-Netzwerk Zehntausende oder Hunderttausende kollektive Entscheidungen, von denen jede das Quorum von 451 durchlaufen hat.

Jetzt zum interessantesten Teil. Stellen Sie sich vor, Sie wollten ein solches Netzwerk übernehmen. Was müssten Sie tun?

Rotation: Warum die 676 nicht von innen übernommen werden können

Um das Qubic-Netzwerk zu kontrollieren, genügt es nicht, mehr Ausrüstung als die Konkurrenz zu kaufen. Es genügt nicht, mehr Cloud zu mieten als der stärkste Computor. Es genügt nicht, sich zu einem Pool zusammenzuschließen. Keiner dieser Schritte erhöht das eigene Gewicht bei der Abstimmung – alle 676 Stimmen sind gleich.

Was man braucht, ist, so viele der 676 Sitze wie möglich zu erobern. Idealerweise – 226, um das Netzwerk zu lähmen (indem man ein Quorum unmöglich macht), oder 451, um mit der Bildung eigener Entscheidungen zu beginnen.

Hier kommt der wöchentliche Rotationsmechanismus ins Spiel.

Die Zeit in Qubic ist in wöchentliche Intervalle unterteilt, die Epochen genannt werden. Eine Epoche ist eine Einheit, größer als ein Tick. Innerhalb einer einzelnen Epoche ist die Zusammensetzung der 676 Computoren fest: Wer es in die Epoche geschafft hat, arbeitet darin bis zum Ende. An der Grenze zwischen zwei Epochen wird ein Teil der Zusammensetzung ausgetauscht: Die Schlechtesten nach den Ergebnissen der vergangenen Epoche treten ihre Sitze an die Besten der Kandidaten ab, die einen Einstiegsantrag gestellt haben. „Schlechteste“ und „Beste“ – nach einer einzigen Kennzahl: dem Volumen der über die Epoche geleisteten nützlichen Rechenarbeit. Was „nützliche Arbeit“ in Qubic ist und warum sie überhaupt möglich ist, sind die nächsten beiden Kapitel des Buches; hier genügt zu wissen, dass jeder Computor am Ende einer Epoche eine eindeutige numerische Bewertung seines Beitrags hat, und diese Bewertung entscheidet darüber, ob er bleibt oder geht.

Eine wichtige strukturelle Tatsache: Es können nicht mehr als 225 Teilnehmer gleichzeitig in einem Epochenübergang ausgetauscht werden.

Nicht 300. Nicht 400. Nicht 676. Das Maximum sind 225 von 676. Es ist eine Protokollkonstante.

Sehen wir, was daraus folgt.

Stellen Sie sich vor, Sie sind eine koordinierte Gruppe, die Qubic übernehmen will. Sie haben 676 eigene Computoren vorbereitet, für maximale Leistung optimiert, und sind bereit, alle 676 Sitze mit Ihren Knoten einzunehmen. Wie viele Epochen – also Wochen – wird das dauern?

In einem Epochenübergang können Sie höchstens 225 Ihrer eigenen ins Netzwerk bringen. Gut; nach dem ersten Mittwoch haben Sie 225 von 676 Sitzen. Die verbleibenden 451 sind noch die alten, nicht Ihre. Beim nächsten Epochenübergang – höchstens weitere 225. Summe: 450 von 676. Immer noch nicht 451. Beim dritten Übergang – weitere 225. Summe: 675. Beim vierten – der letzte eine. Vier Wochen mindestens, selbst unter absolut idealen Bedingungen für Sie, wenn Sie jede Epoche exakt die maximal erlaubte Anzahl an Sitzen einnehmen.

Aber selbst das ist das für Sie günstigste Szenario, und es setzt voraus, dass in jeder von vier Epochen in Folge alle 225 verfügbaren Sitze genau von Ihren Kandidaten und niemandem sonst besetzt wurden. Es erfordert, dass Ihre 225 Computoren bei der Leistung besser sind als alle anderen ehrlichen Kandidaten der Welt, gleichzeitig, Woche für Woche. Verlieren Sie auch nur in einer dieser Epochen den Wettbewerb um auch nur fünfzig Positionen, geben Ihre 175 Ihnen nicht den benötigten Schritt, und die Rechnung verschiebt sich. Verlieren Sie in jeder Epoche um auch nur hundert Positionen, streckt sich die Übernahme auf zwei Monate und mehr, und die ganze Zeit bleibt das Netzwerk in den Händen der alten Supermehrheit.

Aber das ist das hypothetische Minimum. In Wirklichkeit haben Sie keine Garantie, dass Ihre 225 Kandidaten nach geleisteter Arbeit ganz oben landen. Andere Computer arbeiten ebenfalls; sie stellen ebenfalls Einstiegsanträge. Ihre Kandidaten konkurrieren mit ihnen nicht auf Basis von „welches Team zu wem gehört“, sondern danach, wer für die Woche mehr nützliche Leistung erbracht hat. Sie müssen nicht nur 676 Maschinen vorbereiten, sondern es so einrichten, dass Ihre Maschinen jede Woche beständig alle anderen Bewerber der Welt ausspielen. Vier Wochen in Folge. Ohne einen einzigen Ausfall.

Und erinnern wir uns nun an die Hauptsache: Solange Sie weniger als 451 Sitze halten, wird das Netzwerk immer noch von den alten Computoren kontrolliert. Jede Entscheidung durchläuft das Quorum

von 451; solange Sie 225 oder 450 haben – diese Entscheidung wird nicht von Ihren Leuten getroffen. Das alte Netzwerk arbeitet weiterhin normal. Die alten Computoren bemerken weiterhin die eintretenden Neuankömmlinge. Bemerken sie, dass ein koordinierter Pool von Knoten mit gleichartigem Verhalten ins Netzwerk eintritt, können sie reagieren. Auf Protokollebene, nein – sie haben keinen Mechanismus, den „Verdächtigen zu blockieren". Aber auf Ebene der Community, die das Geschehen beobachtet, ja. Qubic hat einen öffentlichen Markt, öffentliche Kommunikationskanäle, öffentliche technische Entscheidungen über die Roadmap. Über vier Wochen eines koordinierten Angriffs wird die Community Zeit haben, das zu sehen, zu diskutieren und möglicherweise zu reagieren – mit einem technischen Upgrade, einer Änderung der Auswahlregeln, der Rekrutierung neuer ehrlicher Computoren.

Es gibt noch eine bemerkenswerte arithmetische Symmetrie. 676 minus 225 gleich 451. Genau die für ein Quorum benötigte Zahl. Das ist kein Zufall. Es ist eine bewusst von den Entwicklern gewählte Form der Symmetrie: Selbst wenn man sich das extremstmögliche Szenario vorstellt, in dem alle 225 erlaubten Sitze in einem einzigen Epochenübergang ausgetauscht wurden und alle davon böswillig sind, halten die verbleibenden 451 alten, ehrlichen Computoren immer noch die Kontrolle über alle Entscheidungen der Epoche. Sie erreichen das Quorum ohne eine einzige Stimme der Neuankömmlinge. Das heißt, selbst bei maximaler gleichzeitiger Invasion verliert das Netzwerk nicht die Fähigkeit, Entscheidungen auf Basis seiner bisherigen Zusammensetzung zu treffen.

Das ist die Formulierung, aus der die strukturelle Widerstandsfähigkeit von Qubic folgt. Nicht „die Schöpfer hoffen, dass niemand angreift". Nicht „Dezentralisierung ist unser Wert". Sondern mathematisch: Bei jeder vom Protokoll erlaubten Handlungsfolge eines Angreifers bewahrt das Netzwerk die Fähigkeit, für mindestens eine volle Epoche pro 225 eroberte Sitze wie zuvor zu funktionieren. Und während dieser Epoche hat ein reales Netzwerk realer Menschen Zeit, zu sehen, zu diskutieren und, falls nötig, zu reagieren.

Hier, an diesem Punkt, lohnt es sich, noch einmal zu wiederholen, was wir in Kapitel drei im Zusammenhang mit GHash.IO besprachen – dem Pool, der im Sommer 2013 55 % der Hashrate des Bitcoin-Netzwerks anhäufte. Dort spielte sich die Lücke zwischen Konzentration und Entblockierung des Netzwerks innerhalb eines einzigen Zyklusdrehers ab: heute 55 %, morgen ein Block mit Doppelausgabe – technisch möglich. Was es stoppte, war nur öffentlicher Druck, der Abgang eines Teils der Miner aus dem Pool, Reputationsschaden. Es gab keine mechanische Bremse.

In Qubic existiert die mechanische Bremse. Sie erfordert keinen öffentlichen Druck, keine freiwilligen Entscheidungen der Teilnehmer. Sie ist durch die Konstante „nicht mehr als 225 Austausche pro Epochenübergang" in das Protokoll eingebaut. Selbst wenn die gesamte Community stillschweigen würde, während ein Angreifer methodisch Monat für Monat seine Präsenz aufbaut, würde es dennoch mindestens vier Wochen dauern, bis er 451 eigene Sitze erreicht, und die ganze Zeit über würde das Netzwerk normal weiterarbeiten.

Das ist genau der strukturelle Mechanismus, auf den ich in Kapitel drei hinauswollte, als ich sagte, Mining müsse Dezentralisierung erzeugen, nicht Konzentration. Ein Mechanismus negativer Rückkopplung, den Bitcoin nicht hatte und der, lässt man Bitcoin, wie es ist, nicht von selbst entstehen wird.

Warum ausgerechnet 676

Der aufmerksame Leser, der bis hierher gelesen hat, hat sich sicher bereits gefragt: Warum 676? Es sieht, gelinde gesagt, ungewöhnlich aus.

Die erste Antwort: 676 ist 26 im Quadrat. Eine Quadratzahl. Eine Zahl, die sich bequem als 26-mal-26-Tabelle darstellen lässt, in der jeder Computor eine Zelle mit Zeilen- und Spaltennummer einnimmt. Diese Indizierung erlaubt es, wie die technischen Qubic-Spezifikationen zeigen, den internen Algorithmen des Protokolls – jenen, die die Aufgabenverteilung unter Teilnehmern, das Routing von Stimmen, den Austausch von Zwischendaten übernehmen –, deutlich effizienter zu arbeiten, als wenn Computoren einfach von 0 bis 675 durchnummeriert wären. Das ist ein rechnerisches Argument, und es kam durch technische Erwägungen ins Netzwerk, nicht durch Ästhetik.

Aber die Hauptantwort liegt nicht im Quadrat von 26. Die Hauptantwort ist, dass 676 sich als goldener Mittelweg zwischen drei widerstreitenden Anforderungen erweist.

Die erste Anforderung ist Vielfalt. Je mehr Teilnehmer im Parlament, desto schwerer ist es für eine einzelne Gruppe, eine Mehrheit zu erobern. Aus Sicht dieser Logik gilt: je größer 676 ist, desto besser. 10.000 Computoren würden eine wesentlich größere Widerstandsfähigkeit gegen Konzentration bieten.

Die zweite Anforderung ist gegenseitige Verifikation. Jeder der 676 prüft eingehende Vorschläge von jedem der übrigen 675. In jedem Tick. Mit einer Frequenz von mehreren Ticks pro Sekunde. Gäbe es 10.000 Computoren, müsste jeder in jedem Tick 9.999 andere prüfen, und das würde eine Rechenlast erzeugen, die gewöhnliche Ausrüstung innerhalb eines einzigen Ticks schlicht nicht bewältigen könnte. Das Netzwerk würde sich verlangsamen. Aus Sicht dieser Logik gilt: je kleiner 676 ist, desto besser. 100 Computoren könnten sich noch schneller gegenseitig prüfen.

Die dritte Anforderung ist Fehlertoleranz. In jedem physischen Netzwerk sind zu jedem gegebenen Zeitpunkt manche Knoten nicht verfügbar – wegen Stromausfällen, Problemen beim Internetanbieter, einem schiefgelaufenen Update. Damit das Netzwerk für ein Quorum immer 451 arbeitende Computoren hat, muss 676 merklich größer sein als 451. Hätte das Netzwerk nur 451 Computoren (genau am Quorum), würde der Ausfall auch nur eines von ihnen das Netzwerk stoppen. Je mehr Computoren über dem Mindestquorum, desto größer die Sicherheitsmarge. Aus dieser Sicht gilt: je größer, desto besser.

676 ist ein Kompromiss. Groß genug, um Teilnehmervielfalt und eine Reserve für den Ausfall einiger von ihnen zu bieten. Klein genug, dass jeder Computor in Echtzeit das Verhalten jedes der übrigen 675 überwachen kann. Das Quadrat einer ganzen Zahl, damit interne Algorithmen effizienter arbeiten. Das Doppelte von zwei Dritteln (451 und 225), sodass die Konstruktion die oben besprochene Symmetrie hat.

Hätten die Entwickler 700 gewählt, wäre die 2/3-Symmetrie verschwunden (700 × 2/3 = 466,67, gerundet ergibt das 467, und die Formel „maximale Austausche pro Epoche gleich die Differenz zwischen 676 und dem Quorum“ würde nicht so sauber funktionieren). Hätten sie 625 gewählt (das ist 25^2), erhielte man bei vergleichbarer Rechenkomplexität weniger Widerstandsfähigkeit. 729 (27^2) – mehr Verifikationslast ohne proportionalen Gewinn. 676 ist der Punkt, an dem mathematische, rechnerische und technische Anforderungen in einer einzigen Zahl zusammenlaufen.

Zwei Größenordnungen der Dezentralisierung

Es ist nützlich, die Zahl 676 neben eine analoge Zahl für Bitcoin zu stellen.

In Kapitel drei erwähnten wir, dass bis 2026 die effektive Kontrolle über Bitcoins Hashrate bei den vier bis fünf größten Pools konzentriert ist, die zusammen etwa 70–75 % der Rechenleistung des Netzwerks halten. Foundry USA – etwa 29 %, AntPool – etwa 21 %, weitere drei oder vier nennenswerte Pools – der Rest. Stellt man sich Bitcoin als ein „Parlament“ vor, in dem Stimmen proportional zur investierten Hashrate verteilt sind, dann treffen in diesem Parlament vier oder fünf Akteure die meisten Entscheidungen. Das ist die realistische obere Schätzung für die effektive Anzahl der Konsens-Teilnehmer in Bitcoin in seinem aktuellen Zustand.

676 zu 4–5 ist nicht „hundertmal mehr“. Es ist eine andere Größenordnung. Es ist eine strukturelle Veränderung in der Natur des Netzwerks: von einem, in dem die großen Entscheidungen von einer Handvoll getroffen werden, zu einem, in dem sie von einem mittelgroßen Parlament getroffen werden.

Betrachtet man diesen Unterschied durch eine Kennzahl, die die Krypto-Community manchmal „Dezentralisierungskoeffizient“ nennt (Nakamoto-Koeffizient – die Mindestanzahl von Teilnehmern, deren Vereinigung fähig ist, das Netzwerk anzugreifen), dann beträgt dieser Koeffizient für Bitcoin 2026 etwa 3–4. Die Vereinigung der drei größten Pools gibt den Angreifern 51 %. Für Qubic ist dieser Koeffizient konstruktionsbedingt gleich 226. Zweihundertsechsundzwanzig ist die Anzahl von Computoren, die gleichzeitig koordiniert werden müssten, um das Netzwerk zu lähmen. Nicht 3. Nicht 4. Zweihundertsechsundzwanzig.

Der Unterschied zwischen „drei sich koordinierenden Akteuren“ und „zweihundertsechsundzwanzig sich koordinierenden Akteuren“ ist der Unterschied zwischen „an einem Abend in einem Raum einigbar“ und „ohne eine ernsthafte organisatorische Struktur, die selbst lange vor dem Moment der Einigung öffentlich sichtbar wird, unmöglich“. Sechsundzwanzig Menschen kann man noch an einen langen Tisch setzen. Zweihundertsechsundzwanzig – kann man nicht. Jeder Versuch, eine solche Anzahl koordinierender Teilnehmer zu versammeln, wird allein durch die Logistik auffällig.

Es gibt eine weitere Möglichkeit, dieselbe Lücke zu betrachten. Stellen Sie sich eine Verschwörung vor – Korrespondenz, ein Telegram-Chat, ein geschlossenes Treffen. Je mehr Teilnehmer, desto höher die Wahrscheinlichkeit, dass sich einer von ihnen als illoyal erweist, versehentlich etwas ausplaudert oder die Korrespondenz durchsickern lässt. Für eine Gruppe von drei ist diese Wahrscheinlichkeit gering; für eine Gruppe von zwanzig ist sie bereits merklich; für eine Gruppe von zweihundertsechsundzwanzig ist sie praktisch unvermeidlich. Die Soziologie von Verschwörungen ist gut erforscht; Historiker wissen, dass jede Verschwörung mit mehr als ein paar Dutzend Teilnehmern binnen weniger Wochen oder Monate ans Licht kommt. Das ist eine Eigenschaft der menschlichen Natur, nicht von Qubic; aber die Konstruktion von Qubic nutzt diese Eigenschaft. Sie verwandelt einen Angriff, der bei Bitcoin die Koordination von vier Akteuren erfordert, in einen Angriff, der bei Qubic die Koordination von rund hundertmal so vielen Akteuren erfordert. Die Anforderungen an organisatorische Komplexität wachsen entsprechend, ebenso die Wahrscheinlichkeit eines Lecks, ebenso die Unmöglichkeit, unter dem Radar zu bleiben.

Eine Einschränkung ist angebracht. Dieser Vergleich lautet nicht „Qubic hat Bitcoin geschlagen“. Bitcoin wurde nicht gebaut, um 2026 einen hohen Dezentralisierungskoeffizienten zu haben; es wurde gebaut, um 2009, in völliger Isolation, ohne Investoren, ohne Team, ohne Börse, ohne Legitimität, als erstes Netzwerk elektronischen Geldes in der Geschichte zu starten, das nicht durch eine einzige administrative Entscheidung abgeschaltet werden konnte. Diese Aufgabe erfüllte es. Das strukturelle

Detail, durch das sich Hashrate über die Zeit konsolidiert, ist der Preis für eine Architektur, in der jeder jederzeit beitreten oder gehen kann. Dieser Preis war 2009 unsichtbar, weil noch niemand da war. Bis 2026 wurde er auffällig.

Qubic wurde von einem anderen Ausgangspunkt aus gebaut. Bis 2022 war die Lehre aus Bitcoin für alle offensichtlich. Qubics Entwickler hatten die Möglichkeit, von Anfang an einen strukturellen Anti-Konsolidierungs-Mechanismus einzubauen, auf Kosten dessen, dass das Netzwerk prinzipiell kein „jeder kann jederzeit Computor werden"-Netzwerk ist – man muss die Epochenauswahl durchlaufen und sich unter den 225 verfügbaren einen Sitz sichern. Das ist ein Tradeoff: Offenheit für beliebigen Anschluss im Austausch gegen garantierte Verteiltheit. Wie man diesen Tradeoff in die eine oder andere Richtung wirft, ist eine Frage, die nicht nur technisch, sondern historisch ist. 2009 wurde die eine Option gewählt; 2022, mit der Erfahrung von 2009–2022 in der Hand, wurde die andere gewählt.

In Kapitel drei formulierte ich das als strukturelle Anforderung. Damit Kooperation im Netzwerk nachhaltig ist, darf ein Sieg innerhalb des Netzwerks nicht in das Recht umwandelbar sein, dessen Regeln zu ändern. Bitcoin stellt diese Isolation nicht bereit: Angehäufte Hashrate wandelt sich in einen Anteil an Stimme bei der Blockauswahl um, und durch Unterstützung für diesen oder jenen Client, diesen oder jenen Entwickler, diese oder jene Entwicklungsrichtung – auch in einen Anteil an Stimme bei der Wahl der künftigen Entwicklungstrajektorie des Protokolls. Qubic stellt diese Isolation wieder her: ein Teilnehmer – eine Stimme, keine Anhäufung erhöht sein Gewicht bei den Abstimmungen der aktuellen Epoche, und die Fähigkeit, Teilnehmer der nächsten Epoche zu werden, hängt nicht vom angehäuften Kapital ab, sondern von der in der vorherigen geleisteten Arbeit.

An dieser Stelle lohnt es sich, gesondert zu sagen, dass „geleistete nützliche Arbeit" in Qubic nicht dieselbe Art von Arbeit ist wie bei Bitcoin. Bei Bitcoin ist Arbeit die Lösung eines bedeutungslosen kryptografischen Rätsels, dessen einzige Funktion darin besteht zu beweisen, dass man Strom verbraucht hat. Bei Qubic ist Arbeit etwas anderes. Es ist eben jenes „Murdoch-Gasrohr", das ich in früheren Kapiteln versprochen habe. Wie es aufgebaut ist, ist jedoch das Thema der folgenden Kapitel, nicht dieses. Hier ist nur wichtig, eines festzuhalten: Die Auswahl in eine Epoche geschieht nach einer Kennzahl, die an einen für das Netzwerk nützlichen Beitrag gebunden ist, nicht an einen abstrakten Ressourcenaufwand. Ein Computor, der viel Strom für bedeutungslose Hashes aufgewendet hat, gewinnt dadurch bei Qubic nichts. Er muss Arbeit leisten, die das Netzwerk braucht. Welche Arbeit genau – sehen wir in Kapitel acht.

Und noch eine Bemerkung, bevor ich dieses Kapitel schließe. Der gesamte hier beschriebene 676-Mechanismus ist eine Seite von Qubic. Die zweite, nicht weniger wichtige – ist, was als „nützliche Arbeit" zählt und wie ihr Ergebnis in die Hände der Nutzer gelangt. 676 Computoren ohne nützliche Arbeit sind nur ein verteilter Zähler. Nützliche Arbeit ohne 676 Computoren ist verteiltes Rechnen ohne Garantie, dass niemand das Ergebnis ausgetauscht hat. Zusammen sind sie das, wofür Qubic konzipiert wurde, und erst ihre Vereinigung macht das Netzwerk zu mehr als der Summe seiner Teile. Aber zuerst musste der Rahmen beschrieben werden, der die gesamte Konstruktion trägt.

Was als Nächstes kommt

Fassen wir zusammen.

Das Qubic-Netzwerk ruht auf einem festen Pool von 676 Computern, die gleichzeitig die Rollen von Beobachtern, Prüfern und Abstimmenden spielen. Jede Entscheidung erfordert die Unterstützung von mindestens 451 Teilnehmern – das sind zwei Drittel, die mathematisch kalibrierte Grenze, jenseits derer das Netzwerk gegen die Kollusion oder den Ausfall eines Drittels seiner Mitglieder widerstandsfähig ist. Innerhalb einer einzelnen Abstimmung ist jeder der 676 Teilnehmer jedem anderen gleichgestellt; Ressourcenanhäufung wandelt sich nicht in Stimmgewicht um. Die Zeiteinheit ist der Tick; in jedem Tick wird ein Vorschlag von einem der 676, deterministisch rotierend, betrachtet. Die Einheit für die Erneuerung der Mitgliedschaft ist die Epoche; einmal pro Woche wird ein Teil der Mitgliedschaft ausgetauscht, aber nicht mehr als 225 auf einmal, was garantiert, dass jede koordinierte Invasion mindestens vier Epochenübergänge braucht, und die ganze Zeit über wird das Netzwerk von der vorherigen Supermehrheit kontrolliert.

Diese Konstruktion ist das Fundament. Alles andere, worum es in den übrigen Kapiteln von Teil drei gehen wird, ruht darauf: wie sich nützliche Arbeit in eine Verteidigungsstruktur für das Netzwerk verwandelt, wie der Token emittiert und verbrannt wird, und wie der letzte verbliebene Punkt menschlicher Steuerung funktioniert – die Figur des Arbitrators, die nach Plan am 13. April 2027 verschwinden soll.

Aber bevor wir darüber sprechen, was auf diesem Fundament aufgebaut wird, lohnt es sich, eine Frage zu klären, die in diesem Kapitel offengeblieben ist.

Wir sagten, dass einmal pro Woche ein Teil der Computor-Zusammensetzung ausgetauscht wird. Dass die „Schlechten“ ihre Sitze an die „Guten“ abtreten, dass nicht mehr als 225 von 676 auf einmal ausgetauscht werden. Aber der Übergang selbst – der Moment, in dem eine Epoche endet und eine andere beginnt – wurde bisher von außen beschrieben, aus statistischer Sicht. Wer genau landet unter denen, die gehen, und nach welcher Regel? Wie geschieht die Auswahl unter den Kandidaten für die freien Sitze? Zu welchem Zeitpunkt geschieht das – was, wenn während des Übergangs jemand eine Transaktion sendet, geht sie an die alte Epoche oder die neue? Was geschieht mit den unerledigten Verpflichtungen eines scheidenden Computors? Wie schafft es das Netzwerk, in dem Moment nicht anzuhalten, in dem ein Viertel seiner stimmberechtigten Mitglieder wechselt?

Das sind Fragen zur Zeit in Qubic. Darüber, wie das Netzwerk nicht in einer kontinuierlichen Gegenwart existiert, sondern in diskrete Wochenzyklen unterteilt ist, jeder von ihnen ein eigenes kleines Leben, mit eigener Geburt, Entwicklung und Ende. Über das Myzel, das sich nicht einmal im Jahr, sondern jeden Mittwochabend erneuert und dabei als Ganzes weiterlebt.

Das nächste Kapitel handelt von Wochen aus Epochen.

7
Wochen aus Epochen



Wenn Kapitel sechs die Anatomie des Netzwerks beschrieb – woraus es besteht –, beschreibt dieses seine Physiologie: wie es atmet, wie es Stoffwechsel betreibt, wie es sich regeneriert.

Erinnern Sie sich an die Metapher, die ich in Kapitel sechs sorgfältig einführte und zu der ich versprach zurückzukehren. Myzel – ein verteiltes Netzwerk feiner Fäden, das sich unterirdisch ohne Zentrum und ohne Besitzer erstreckt. Seine einzelnen Abschnitte sterben kontinuierlich ab und werden durch neue ersetzt; das Ganze lebt dabei länger als jedes seiner Fragmente.

Kapitel sechs endete mit dem Versprechen, dass die wöchentliche Erneuerung der Computoren – nicht nur metaphorisch, sondern mechanisch – dasselbe ist. Dieses Versprechen wird hier eingelöst.

Qubic ist der Rahmen, auf dem eine Struktur ruht, die noch beschrieben werden muss; das Gasrohr wird in den folgenden Kapiteln zusammengebaut. Dieses hier, das siebte, handelt noch vom Rahmen – aber von seiner zeitlichen Dimension. Coalbrookdale des digitalen Zeitalters, Tag zwei: Der über Nacht verlegte Boden wird auf Stützen gesetzt, die nicht nur Gewicht tragen müssen, sondern auch das, was durch sie hindurchfließt.

Woraus eine Epoche besteht

Nehmen wir eine beliebig gewählte Woche im Leben des Qubic-Netzwerks – sagen wir, diese hier, von Mittwochabend bis zum nächsten Mittwochabend. Was geschieht in ihr?

Die Zusammensetzung der sechshundertsechsundsiebzig Computoren ist fest. Genau diese sechshundertsechsundsiebzig – nicht weniger, nicht mehr – bilden für alle sieben Tage das Parlament, über das wir in Kapitel sechs sprachen. Nicht einer von ihnen kann mitten in der Woche hinzugefügt werden. Nicht einer von ihnen kann offiziell ausgeschlossen werden. Unabhängig davon, ob der Computor funktioniert oder ausgefallen ist, ehrlich abstimmt oder zu sabotieren versucht, reich wird oder pleitegeht – für alle sieben Tage behält er seinen Platz in der Zusammensetzung.

Innerhalb der Woche ist die Zeit in Ticks geschnitten – jene grundlegende Abstimmungsrunde, über die wir bereits gesprochen haben. Ticks gibt es viele: In der aktuellen Konfiguration dauert ein Tick etwa eine halbe bis eine Sekunde, was bedeutet, dass es etwa eine Million davon pro Woche gibt. Jeder Tick ist eine vollständige Runde: Ein Computor-Leader schlägt vor, die verbleibenden sechshundertfünfundsiebzig verifizieren und stimmen ab, ein Quorum von vierhunderteinundfünfzig macht den neuen Zustand kanonisch. Eine Million solcher Runden hintereinander – und eine Epoche ist durchlebt.

Wichtig ist zu verstehen, was genau die Epoche akkumuliert. Das ist nicht nur ein Protokoll dessen, was geschah; es ist das strukturierte Gedächtnis des Netzwerks. Jedem der sechshundertsechsundsiebzig Computoren wird am Ende der Woche eine numerische Bewertung zugewiesen – manchmal als „Score" bezeichnet. Dieser Score misst, wie viel nützliche Arbeit der Computor über die Woche geleistet hat. Was „nützliche Arbeit" in Qubic ist, ist das Thema des nächsten Kapitels, wie ich versprochen habe, und das Versprechen wird eingehalten; für den Moment genügt zu wissen, dass diese Arbeit eine objektive Kennzahl hat, für alle Teilnehmer gleichermaßen berechenbar. Am Ende der Epoche hat das Netzwerk eine Rangliste: sechshundertsechsundsiebzig Namen, jeder mit einer Zahl.

Parallel gibt es eine weitere Liste. Das sind Kandidaten – Computer, die nicht Teil der aktuellen sechshundertsechsundsiebzig sind, aber im Laufe der Woche ebenfalls gültige Arbeit geleistet und einen eigenen Score angesammelt haben. Sie stimmen nicht ab, nehmen nicht am Konsens teil, aber das Netzwerk sieht sie und zählt sie. Am Ende der Epoche hat das Netzwerk auch für sie eine Rangliste – eine separate.

Das heißt, eine Epoche ist nicht nur eine Woche, während der das Netzwerk operiert. Es ist eine Woche, während der das Netzwerk gleichzeitig operiert und sich selbst beobachtet. Alle sechshundertsechsundsiebzig „drinnen" stehen ständig unter Messung. Alle Kandidaten „draußen" ebenfalls. Wenn die Woche endet, verfügt das Netzwerk nicht nur über die Blockchain der Transaktionen, sondern auch über eine vollständige Rangliste, wer wie gearbeitet hat.

Innerhalb einer Epoche tritt keine dieser Ranglisten in Kraft. Für alle sieben Tage sind die Spielregeln für alle gleich. Kein Computor bekommt, egal wie hohen Score er bis zur Wochenmitte angesammelt hat, dadurch eine zusätzliche Stimme, noch zusätzliche Transaktionspriorität, nicht einmal einen Informationsvorteil. Innerhalb einer Epoche ist das Netzwerk symmetrisch gegenüber allen sechshundertsechsundsiebzig. Ich möchte das gesondert unterstreichen, denn hier geschieht eine der subtilsten Sachen in der gesamten Architektur von Qubic.

Was bedeutet „die Epoche als eine Runde eines wiederholten Spiels"? Axelrods Turnier, das ich in Kapitel zwei durcharbeitete, bestand aus Partien: Jedes Programmpaar spielte nicht einmal, sondern zweihundert Runden in Folge gegeneinander. Nur diese Struktur erlaubte es einer kooperativen Strategie zu gewinnen – weil sich der Gegner an vergangenes Verhalten erinnerte und darauf reagierte. Eine kooperative Strategie gewinnt nicht in einer Runde; in tausend Runden gewinnt sie.

Eine Epoche in Qubic ist eine solche Runde, nur mit sechshundertsechsundsiebzig Spielern gleichzeitig. Jede ihrer Wochen an Verhalten wird zu einer Zelle in der Gesamtergebnistabelle. In der nächsten Woche können sich die Bedingungen ändern – die Zusammensetzung wird eine andere sein, Regeln können verfeinert werden –, aber die Änderungen sind nicht zufällig; sie folgen deterministisch aus dem, was in der vorigen Epoche geschah. Die Ausgetauschten sind genau diejenigen, die das schlechteste Ergebnis zeigten; die Zugelassenen sind genau diejenigen, die das beste Ergebnis zeigten. Niemand ernennt „die Schlechten"; der Prozess selbst bestimmt sie.

Das unterscheidet sich stark davon, wie Bitcoin lebt. Bitcoin hat keine diskreten Epochen. Das Netzwerk arbeitet in kontinuierlicher Zeit: Block nach Block, alle zehn Minuten ein neuer. Änderungen am Protokoll geschehen durch Forks – durch öffentliche, manchmal schmerzhafte Prozesse, in denen ein Teil der Community die neue Version akzeptiert und ein anderer nicht, und manchmal spaltet sich das Netzwerk. Bitcoin ist eine lange, lange Sequenz ohne Nähte, in der jede strukturelle Änderung ein

Aufreißen erfordert. Qubic lebt anders. Es hat Nähte, und sie fallen jeden Mittwoch.

Was am Mittwoch geschieht

Was genau im Moment eines Epochenübergangs geschieht, beschreibe ich nun Schritt für Schritt. Aber zuerst – eine Warnung. Ich werde den Prozess als deterministischen Algorithmus beschreiben; das stimmt, ist aber nicht die ganze Wahrheit. In der realen Geschichte von Qubic, in den mehr als vier Jahren seit der ersten Epoche im April 2022, ist dieser Algorithmus nicht immer reibungslos gelaufen. Warum, wird später im Abschnitt klar; nehmen wir vorerst an, der Algorithmus funktioniert.

Also, die Sequenz.

Ein paar Ticks vor der Epochengrenze – nennen wir sie Moment T – friert das Netzwerk die endgültigen Scores aller sechshundertsechsundsiebzig aktiven Computoren ein. Es rangiert sie von unten nach oben. Die Liste ist bekannt: diese Namen arbeiteten am besten, jene am schlechtesten.

Parallel hat das Netzwerk bereits eine rangierte Kandidatenliste. Das sind eben jene Computer, die die ganze Woche über gültige Arbeit leisteten, aber nicht zu den sechshundertsechsundsiebzig gehörten. Ihr Score ist ein objektiver Parameter, gleichermaßen berechenbar, basierend auf derselben Kennzahl wie bei den aktiven. Beide konkurrieren auf einem einzigen Maßstab, nicht auf verschiedenen.

Im Moment T – genauer gesagt, zu einem festgelegten Zeitpunkt am Mittwoch UTC – vergleicht das Netzwerk. Hat der beste externe Kandidat einen höheren Score als der schlechteste aktive Computor, tauschen sie die Plätze. Der Schlechteste fliegt raus, der Beste wird zugelassen. Der Prozess wiederholt sich: Nun wird der Zweitschlechteste der verbleibenden sechshundertsechsundsiebzig mit dem Zweitbesten der Externen verglichen. Und so weiter.

Aber nicht unendlich. Beim zweihundertfünfundzwanzigsten Austausch stoppt der Prozess, selbst wenn der nächste externe Kandidat formal noch besser ist als der nächste aktive. Zweihundertfünfundzwanzig ist eine starre Obergrenze, wir haben das in Kapitel sechs ausführlich durchgearbeitet; es ist struktureller Schutz des Netzwerks vor einer zu schnellen Invasion.

Also: Hat sich herausgestellt, dass hundertzwanzig Computoren wirklich schlecht gearbeitet haben, fliegen alle hundertzwanzig raus. Waren es dreihundert solche, fliegen nur die schlechtesten zweihundertfünfundzwanzig von den dreihundert raus; der Rest bleibt eine weitere Woche, mit dem Versprechen, es besser zu machen. Und waren es nur fünfzig solche, fliegen alle fünfzig raus, und niemand füllt Plätze bis zu zweihundertfünfundzwanzig auf; freie Plätze für neue Einsteiger erscheinen nicht in solcher Zahl.

Eine neue Epoche beginnt. Die Zusammensetzung der sechshundertsechsundsiebzig ist erneuert. Der Score der letzten Woche wird als historische Tatsache in der Blockchain verzeichnet; das Netzwerk erinnert sich daran, aber in der neuen Epoche verleiht es keine Privilegien. Die neue Woche ist, nach angesammelter Arbeit, ein sauberer Anfang. Alle starten neu.

Die Auswahlmechanik ist nicht manuell. Niemand vom Qubic-Team sitzt am Mittwochmorgen mit einer Tabellenkalkulation und entscheidet, wen man tauscht. Der Prozess ist deterministisch, ausgeführt gleichzeitig von allen sechshundertsechsundsiebzig Knoten unabhängig voneinander. Jeder Computor kann, da er die vollständige Liste der Ticks der vergangenen Epoche kennt, den Score jedes Teilnehmers

selbst berechnen – sowohl intern als auch extern. Haben alle sechshundertsechsundsiebzig dasselbe berechnet – und das sollten sie, weil die Eingabedaten für alle dieselben sind –, beginnt die neue Epoche automatisch. Keine zentrale Entscheidung.

In CfBs Beschreibungen klingt der Mechanismus, durch den ein aktiver Computor offiziell seinen Status verliert, so: Ein Computor, der sich falsch verhält oder mit seiner Last nicht Schritt hält, beginnt zu einem gewissen Zeitpunkt, kryptografisch ungültige Ticks auszugeben. Diese ungültigen Ticks werden zu ihrem eigenen Beweis seines Problems – sie werden als Beweismaterial, das das gesamte Netzwerk sieht, in die Blockchain aufgenommen. An der Epochengrenze verliert ein solcher Computor automatisch seinen Platz. Sein Ersatz erfolgt nicht durch Menschen, nicht einmal durch den Arbitrator – er erfolgt durch die Computoren selbst über das Protokoll, das den Beweis verarbeitet.

Separat, zu den Übergängen. Ein Epochenwechsel ist keine atomare Operation. Er geschieht nicht in einer Mikrosekunde. Das tatsächliche Verfahren erstreckte sich, soweit aus den Beschreibungen des Teams bekannt, über Stunden. In den frühen Epochen, 2022, als schrittweise Übergänge getestet wurden, konnte ein Wechsel sechs Stunden dauern – von 9:00 UTC bis 15:00 UTC; das Mining stoppte für das gesamte Intervall, und das Netzwerk „baute sich selbst neu zusammen“. Bis Ende 2024 waren schrittweise Übergänge durch sogenannte nahtlose Übergänge ersetzt worden – Übergänge ohne vollständigen Halt. Das Netzwerk tickt weiter, aber zu einem gewissen Zeitpunkt aktualisiert sich die interne Computor-Liste an jedem Knoten – und der nächste Tick läuft mit der neuen Zusammensetzung. Wie genau die Synchronisation geschieht, arbeite ich gleich durch.

Transaktionen, die die Epochengrenze überschreiten, gehen nicht verloren. Sendet ein Nutzer eine Minute vor Mittwoch eine Transaktion und sie schafft es nicht mehr in einen Block der alten Epoche, geht sie in den ersten möglichen Tick der neuen. Aus Nutzersicht gibt es überhaupt keinen Unterschied zwischen einer Transaktion „Mittwoch vor Mittag“ und „Mittwoch nach Mittag“. Für den Nutzer ist das Netzwerk ein und dasselbe. Nur intern, unter der Haube, hat es die Zusammensetzung seiner Abstimmenden im Moment der Transaktion leicht geändert.

Warum ausgerechnet Mittwoch. Die Antwort ist einfach und pragmatisch. Mittwoch ist die Mitte der Arbeitswoche in den meisten Zeitzonen der Welt, in denen Qubic Betreiber hat. Es ist ein Tag, an dem der maximale Anteil an Computoren am wahrscheinlichsten online ist und beobachtet, was geschieht. Montag und Freitag sind an Wochenanfangs- und -endeffekte gebunden – wenn Betreiber sich noch nicht vollständig in den Arbeitsmodus eingefunden haben oder bereits teilweise vom Wochenende abgelenkt sind. Samstag und Sonntag – weniger Leute an den Konsolen. Mittwoch ist ein vernünftiger Kompromiss, nichts Mystisches.

Warum ausgerechnet eine Woche. Hier ist die Antwort etwas interessanter. Eine zu kurze Epoche – sagen wir, ein Tag – würde die Score-Bewertung statistisch verrauschen: zufällige Leistungsschwankungen würden gleichermaßen zufällige Ausschlüsse erzeugen, und die Zusammensetzung würde ohne inhaltlichen Grund zittern. Zu lang – sagen wir, ein Monat – würde eine langsame Reaktion auf schlechte Teilnehmer bedeuten: Ein böswilliger oder einfach kaputter Computor könnte das Netzwerk monatelang schädigen oder behindern, bevor er ersetzt wird. Eine Woche ist ein empirisch gefundener Kompromiss. Es ist kein mathematisch bewiesenes „Optimum“; es ist ein vernünftiger Wert an seinem Design-Punkt.

Hier lohnt es sich übrigens zu erinnern, dass Qubic in der Idee, die Zeit in Epochen zu unterteilen, nicht einzigartig ist. Andere Netzwerke mit diskreter Zeit existieren – Cardano verwendet fünftägige Epochen, Solanas Epochen sind deutlich kürzer. Die Originalität von Qubic liegt nicht im Konzept selbst, sondern in den Parametern und darin, was genau an der Epochengrenze festgelegt wird. In den meisten anderen Netzwerken ist eine Epoche die Zeit zwischen Neukalibrierungen eines einzelnen Parameters. In Qubic ist eine Epoche der vollständige Lebenszyklus der Wählerzusammensetzung.

Und noch eine Beobachtung, bei der es sich zu verweilen lohnt. Die Epoche ist die Einheit, in der eine Runde eines wiederholten Spiels stattfindet. Hier beginnt ein früher offengelassenes Versprechen, sich in eine technische Tatsache zu verwandeln: die vierte Bedingung der Kooperation – ein Sieg im Spiel darf dem Spieler nicht die Fähigkeit geben, die Regeln des Spiels selbst zu ändern. Diese Bedingung hat nun zwei Umsetzungen: eine statische – kein angehäufter Reichtum erhöht das Gewicht einer Stimme; und eine dynamische – ein Computor, der über eine Epoche viel verdient hat, erhält das Recht, in der nächsten Epoche zu bleiben, aber nicht das Recht, deren Regeln zu ändern. Zwei verschiedene Arten von Preis, und die Trennung zwischen ihnen ist in die Epochengrenze verdrahtet.

Wie man wechselt, ohne anzuhalten

Der Epochenübergang in Qubic ist keine einfache technische Aufgabe. Stellen Sie sich vor, Sie müssten ein Viertel des Kaders einer Fußballmannschaft mitten im Spiel so austauschen, dass das Spiel nicht stoppt. Die eintretenden Spieler müssen bereits die Taktik kennen, wissen, wo der Ball ist, wer wem zuspielt, welche Kombinationen gespielt werden. Die austretenden müssen das Feld räumen, dürfen aber nichts mitnehmen, was das Team künftig braucht. Und das alles – im Moment, ohne Pfiff.

In der Sprache des Programmierers klingt die Aufgabe so: Im Moment T verlassen bis zu zweihundertfünfundzwanzig Knoten den Konsens, und dieselbe Anzahl tritt ein. Die neuen müssen den vollständigen aktuellen Zustand des Netzwerks kennen – die zuletzt akzeptierten Blöcke, alle offenen Verpflichtungen, alle Zustände von Smart Contracts. Die austretenden müssen ihnen diesen Zustand korrekt übergeben, ohne den Fluss neuer Transaktionen zu unterbrechen. Und das Netzwerk darf in diesem Moment weder Validierung verlieren, noch Konflikte zulassen, noch beim Versuch der Einigung steckenbleiben.

Das Qubic-Protokoll löst das durch etwas, das man als Phase-in und Phase-out bezeichnen kann. Ein eintretender Kandidat weiß im Voraus, dass er am kommenden Mittwoch Computor werden kann – anhand seines eigenen angesammelten Scores. Das ist keine Last-Minute-Überraschung; er kann sich vorbereiten. Bereits seit mehreren Tagen zieht er sich den aktuellen Zustand des Netzwerks, erhält ihn nicht in einem großen Brocken im Moment T, sondern schrittweise, im Hintergrund. Bis zum Moment T hat er bereits alles, was er für den allerersten Tick der neuen Epoche braucht. Er stimmt nicht ab – weil er noch nicht Teil der sechshundertsechsundsiebzig ist –, aber er ist bereits bereit.

An der Grenze T geschieht der Wechsel in einem Schritt. Jeder der sechshundertsechsundsiebzig berechnet unabhängig die neue Zusammensetzung. Jeder aktualisiert seine interne Teilnehmerliste in sich selbst. Ab dem allerersten Tick der neuen Epoche stimmen die neuen ab. Die alten, gerade Ausgeschiedenen, können noch einige Zeit als Beobachter in Kontakt bleiben – ihre Stimmen werden nicht mehr akzeptiert, aber sie sehen das Netzwerk, können ihre technischen Angelegenheiten abschließen, können versuchen, in der folgenden Woche als Kandidaten zurückzukehren. Keine abrupten

Brüche.

Wo diese Beschreibung zu glatt zu wirken beginnt, muss ich innehalten und eine ehrliche Einschränkung hinzufügen. CfBs eigener Kommentar sagt direkt: „Nicht alle Epochenübergänge verlaufen reibungslos." Das stimmt. Die Geschichte von Qubic kennt zwei verschiedene Arten von Übergängen. Der eine ist „nahtlos": keine neuen Funktionen werden ausgerollt, Regeln ändern sich nicht, nur die Computor-Zusammensetzung erneuert sich. Ein solcher Übergang verlief seit 2024 tatsächlich ohne Netzwerkhalt. Der andere ist „brechend": zusammen mit dem Wechsel der Zusammensetzung wird eine neue Version des Protokolls, neue Logik, neue Fähigkeiten ausgerollt. In diesem Fall müssen alle Computoren ihren Code aktualisieren, und der Übergang kann von Ausfallzeit begleitet sein – manchmal mehrere Stunden, und in den ganz frühen Tagen sogar mehr.

Und hier ein wichtiges Detail: Das Qubic-Team führt regelmäßig brechende Übergänge durch. Jeden Mittwoch, wenn diese Woche neue Funktionen zum Ausrollen anstehen – ist der Übergang brechend. Wenn nicht – nahtlos. Als das Team über die Feiertage, im Dezember 2024, beschloss, eine Reihe nahtloser Übergänge hintereinander durchzuführen, erklärte CfB selbst einfach: „keine brechenden Updates bedeutet keinen Fortschritt bei Monero". Das heißt, nahtlos ist Stabilität auf Kosten fehlender Entwicklung; brechend ist Entwicklung auf Kosten möglicher Ausfallzeit. Qubic balanciert in der Praxis ständig zwischen diesen beiden Modi, und von Woche zu Woche kann sich die Wahl verschieben.

Das mag einem an den Krypto-Diskurs rund um Bitcoin gewöhnten Leser seltsam erscheinen, wo jeder Hard Fork ein Ereignis ist, das monatelange Diskussionen auslöst und manchmal die Community spaltet. In Qubic ist ein Hard Fork ein routinemäßiges Mittwochsereignis. Der Grund ist, dass Konsens in Qubic anders gebaut ist. Bei Bitcoin erfordert eine Regeländerung die freiwillige Zustimmung der Miner, von denen jeder unbegrenzt unter dem alten Protokoll weiterarbeiten kann – und bleibt genug Hashrate auf der alten Version, entsteht eine parallele Kette. In Qubic sind Hashrate und Stimme getrennt: Hashrate wird nur gebraucht, um unter den sechshundertsechsundsiebzig zu landen und um einen Platz unter ihnen zu kämpfen; innerhalb einer Epoche gelten die Regeln identisch für alle Abstimmenden, und haben sich sechshundertsechsundsiebzig auf eine neue Version geeinigt – wird die neue Version kanonisch. Eine Fraktion, die bei der alten geblieben ist, tritt einfach nicht in die nächste Zusammensetzung ein. Kein Fork geschieht.

Nun ein kurzer historischer Exkurs, der viel erklärt. Nahtlose Übergänge waren nicht von Anfang an in Qubic vorhanden. Das war eine große, mehrjährige technische Aufgabe. Die ersten Aufzeichnungen über die Arbeit daran stammen vom Dezember 2022; damals schrieb CfB an das Team: „Diese Epoche sollten wir den nahtlosen Epochenübergang entwickeln und testen, erwartet tägliche Updates." 2023 – eine Reihe vorbereitender Änderungen. 2024, im Januar, wurde der nahtlose Modus endlich ins Mainnet ausgerollt. Das heißt, das Netzwerk lebte zwei Jahre – 2022 und 2023 – mit Übergängen, die manchmal Stunden dauerten und das Mining stoppten. Erst danach erschien das, was die meisten Nutzer heute als „den unsichtbaren Mittwochswechsel" sehen.

Das ist aus zwei Gründen wichtig zu erinnern. Der erste ist Ehrlichkeit: zu behaupten, Qubic sei mit einer fertigen nahtlosen Architektur geboren worden, wäre unwahr. Der zweite ist eine Demonstration der Methode. Die Entwicklung kritischer Infrastruktur in einem offenen Netzwerk mit echten Nutzern und echtem Geld, das hindurchfließt, ist Arbeit, die nicht in einem Monat erledigt wird. Vor vier Jahren, am Tag der ersten Qubic-Epoche am 13. April 2022, existierte das meiste von dem, was heute automatisch

läuft, noch nicht einmal auf dem Papier. Das Netzwerk lernte zu leben – und während es lernte, lebte es, Stück für Stück.

Vier Jahre sind keine zufällige Zahl. Das Mainnet-Startdatum – 13. April 2022. Das geplante Datum des Abgangs des Arbitrators – 13. April 2027. Fünf Jahre dazwischen, und die Übereinstimmung der Zahlen ist definitiv kein Zufall. Es ist hier noch zu früh, um dieses Datum im Detail zu besprechen; seine vollständige Behandlung folgt in Kapitel vierzehn. Es genügt festzuhalten, dass der wöchentliche Zyklus der Epochen, den wir gerade beschrieben haben, zur Zähleinheit für diese fünf Jahre wird. Nicht kalendarisch, sondern netzwerklich.

Unter der Haube: Symmetrien und Arithmetik

Kapitel sechs zeigte, wie die Zahl sechshundertsechsundsiebzig durch ein und dieselbe BFT-Mathematik das Quorum von vierhunderteinundfünfzig und die Austauschgrenze von zweihundertfünfundzwanzig hervorbringt. Es lohnt sich, bei der arithmetischen Symmetrie zwischen diesen beiden Verteidigungslinien zu verweilen – und zu sehen, dass sie nicht dekorativ, sondern funktional ist.

Das Quorum von vierhunderteinundfünfzig schützt das Netzwerk innerhalb einer Epoche – im Moment der Abstimmung. Es ist Schutz davor, dass eine Minderheit, auch eine große, eine falsche Entscheidung durchdrückt. Die zweihundertfünfundzwanzig hingegen sind Schutz zwischen Epochen, an der Grenze eines Übergangs. Es ist Schutz davor, dass ein Angreifer die Zusammensetzung zu schnell zu seinen Gunsten dreht. Der erste wirkt im Maßstab von Millisekunden; der zweite im Maßstab von Wochen.

Bemerkenswert ist, dass beide Verteidigungslinien mathematisch dasselbe sind. Sechshundertsechsundsiebzig minus vierhunderteinundfünfzig gleich zweihundertfünfundzwanzig. Entspricht die maximale Anzahl gleichzeitig Austauschbarer der Differenz zwischen der vollen Zusammensetzung und dem Quorum, ergibt sich folgende Eigenschaft: Selbst bei einem für den Angreifer idealen Epochenwechsel, wenn seine Leute alle zweihundertfünfundzwanzig Sitze besetzen, bilden die verbleibenden vierhunderteinundfünfzig alten Computoren genau ein Quorum. Die neuen können allein keine einzige Entscheidung durchbringen – es sind nur zweihundertfünfundzwanzig von ihnen, und mindestens vierhunderteinundfünfzig Stimmen sind nötig. Um irgendeine Entscheidung durchzudrücken, brauchen sie Stimmen der alten.

Das bedeutet: Ob man will oder nicht, jeder Versuch, das Netzwerk von innen zu übernehmen, ist dazu verdammt, ein langwieriger Prozess zu sein. Kapitel sechs zeigte es bereits arithmetisch: mindestens vier Epochen, das heißt vier Wochen, bei idealer Wettbewerbsleistung – und während der gesamten Zeit gehört die Kontrolle der vorherigen Zusammensetzung.

Wichtig ist auch, dass die vorherige Zusammensetzung nicht verpflichtet ist, während dieser vier Wochen passiv zu sitzen. Sie sieht, was geschieht, sieht die rangierte Kandidatenliste, versteht die Struktur der eintretenden Kraft und kann – auf Protokollebene, ohne etwas Illegales – Maßnahmen ergreifen. Zum Beispiel für eine Regeländerung stimmen, die massiven gleichzeitigen Einstieg erschwert. Oder den Score selbst ändern, ihn resistenter gegen einen bestimmten Angriffstyp machen. Über eine Regeländerung darf innerhalb einer Epoche nicht abgestimmt werden, aber an der Epochengrenze – wie wir gesehen haben – schon.

Es gibt noch eine Nuance, die es sich zu erwähnen lohnt. Die Auswahlmechanik ist so gebaut, dass ein rational denkender Angreifer nicht versuchen wird, in einer einzigen Woche alle sechshundertsechsundsiebzig Sitze zu erobern. Warum sollte er? Sein eigenes Mining ist begrenzt – er kann, sagen wir, so und so viel Score pro Epoche produzieren. Verteilt er diesen Score über alle sechshundertsechsundsiebzig Positionen, erobert er keine einzige: Für jede einzelne Position erweist sich seine Stärke als zu schwach. Rationaler ist es, seine gesamte Stärke auf die zweihundertfünfundzwanzig besten Kandidaten zu konzentrieren – das heißt auf die maximal erlaubte gleichzeitige Rotation. Das gibt ihm die dreifache Effizienz pro Position. Aber es verlangsamt ihn auch dreifach: Statt eines Schritts zur Übernahme muss er drei machen.

Anders gesagt: Die Struktur des Protokolls verteidigt nicht nur gegen einen schnellen Angriff – sie steuert den rational denkenden Angreifer aktiv in Richtung eines langsamen. Und ein langsamer Angriff ist ein Angriff, der über Monate sichtbar ist. Das ist ein grundlegender Unterschied zu Situationen wie GHash.IO 2014, wo eine Konzentration von dreißig auf fünfundfünfzig Prozent innerhalb weniger Wochen geschehen konnte und wo es keine mechanische Bremse gab, um den Prozess zu verlangsamen. In Qubic ist die Bremse als Konstante eingebaut.

Der Verdienst eines Computors wandelt sich weder in das Gewicht seiner Stimme um, noch in die Geschwindigkeit seines Ein- oder Austritts in die Zusammensetzung. Das Maximum, das der Verdienst gibt, ist eine objektive Chance, in der Zusammensetzung zu bleiben oder in sie zu gelangen, und diese Chance ist durch dieselbe Schwelle von zweihundertfünfundzwanzig begrenzt, die nicht davon abhängt, wie viel genau der Computor verdient hat. Der Preis des Gewinners innerhalb des Spiels ist, im Spiel zu bleiben. Nicht mehr.

Was als Nächstes kommt

Fassen wir zusammen. Das Qubic-Netzwerk lebt nicht in kontinuierlicher Zeit, sondern in diskreten Zyklen von jeweils einer Woche. Innerhalb einer Epoche ist die Zusammensetzung der sechshundertsechsundsiebzig Computoren fest, alle stimmen mit gleichem Gewicht ab, jeder Tick ist eine vollständige Konsensrunde. Am Ende der Woche verfügt das Netzwerk über eine rangierte Liste aller aktiven Computoren und aller Kandidaten – nach einer objektiven Kennzahl geleisteter Arbeit. An der Epochengrenze geschieht automatischer Austausch: Die Schlechtesten treten ihre Sitze an die Besten ab, bis zu zweihundertfünfundzwanzig Austausche auf einmal, unter einer starren arithmetischen Grenze, die vierhunderteinundfünfzig alte Computoren in der neuen Zusammensetzung bewahrt. Transaktionen laufen ohne Unterbrechung, das Netzwerk stoppt nicht, wenn die Woche keine brechenden Updates hat; und wenn doch – ist eine kurze Ausfallzeit möglich, und das Team wählt bewusst, was ihm in jeder bestimmten Woche wichtiger ist: Stabilität oder Fortschritt.

Auf Ebene der menschlichen Metapher regeneriert sich das Myzel alle sieben Tage: Manche Fäden sterben ab, manche erscheinen, das Ganze lebt weiter. Auf Ebene der Spieltheorie ist jede Epoche eine Runde eines großen wiederholten Spiels mit sechshundertsechsundsiebzig Teilnehmern, und genau das verwandelt, wie Axelrod 1980 zeigte, Kooperation von einer instabilen Ausnahme in ein stabiles Gleichgewicht.

Zwei technische Anker – das Quorum von vierhunderteinundfünfzig und die Austauschgrenze von zweihundertfünfundzwanzig – sind arithmetisch symmetrisch, und zusammen machen sie die

Übernahme des Netzwerks zu einer Aufgabe, die nicht Stunden und nicht Tage, sondern Wochen erfordert, direkt vor den Augen der gesamten Community.

Wir haben nun den Raum des Netzwerks beschrieben – sechshundertsechsundsiebzig Stimmen, die Sitze besetzen – und seine Zeit – wöchentliche Zyklen, während derer sich diese Sitze erneuern. Aber wir haben noch kein einziges Mal die Frage beantwortet, mit der dieses ganze Buch begann. Was genau tun diese sechshundertsechsundsiebzig Teilnehmer während der sieben Tage ihrer Epoche? Welche Arbeit verdient ihnen ihren Platz in der nächsten Woche – und warum ist sie „nützlich“, statt, wie bei Bitcoin, willkürlich? Was ist die Kraft, die dieses Myzel antreibt?

Nicht die bedeutungslosen Hashes, über die wir in Kapitel eins sprachen. Nicht Arithmetik um der Arithmetik willen. Etwas anderes – das, wofür Qubic konzipiert wurde. Das, was wir in Kapitel eins „Murdochs Gas“ nannten, gesammelt in einem Rohr.

Das nächste Kapitel ist das entscheidende in diesem Buch. Es handelt von nützlicher Rechenarbeit, die gleichzeitig das Netzwerk verteidigt und etwas hervorbringt, das zuvor nicht in der Welt existierte. Es heißt „Murdochs Gas in Aktion — UPoW“.

8
Murdochs Gas in Aktion — UPoW

Das Gas, das niemand in ein Rohr sammelte

Was genau tun sechshundertsechsundsiebzig Computoren die ganze Woche über? Welche Arbeit verdient ihnen ihren Platz in der nächsten Epoche – und warum ist sie „nützlich“, statt, wie bei Bitcoin, willkürlich?

Dieses Kapitel ist die Antwort auf diese Frage. Und es ist auch eine Rückkehr zu eben jener Metapher, die ich in Kapitel eins sorgfältig einführte und versprach, eines Tages zur Geltung zu bringen.

Kehren wir zurück nach Coalbrookdale, 1792.

William Murdoch steht an einem Ofen, in dem Kohle zur Koksherstellung verkohlt wird. Der Prozess ist zu diesem Zeitpunkt bereits achtzig Jahre im Einsatz: Seit 1709, seit der Zeit von Abraham Darby, ruht Englands Eisengießereiindustrie auf eben dieser Umwandlung von Kohle in Koks. Aus den Öfen quillt jeden Tag dichter schwarzer Rauch – ein Nebenprodukt des Verkohlens, unpraktisch, manchmal gefährlich, stets als Abfall in die Atmosphäre entlassen. So wurde es die ganze Zeit gemacht: Kohle liefert Koks, Rauch fliegt in den Himmel, Regen wäscht den Ruß von den Fassaden, und niemand beschwert sich, denn Koks bedeutet Gusseisen, und Gusseisen bedeutet das Empire.

Murdoch betrachtet den Rauch anders. Er verlegt ein Rohr vom Ofen zu einer Lampe in seiner eigenen Werkstatt, reinigt das Gas, zündet es an. Es brennt. Es brennt gleichmäßig und lange. Es funktioniert.

In den folgenden fünfzehn Jahren wird sich diese Idee zur Beleuchtung Londons mit Gas auswachsen. Bis in die 1820er wird eine ganze Gasindustrie herangewachsen sein – eine neue Ökonomie, gegründet auf dem Nebenprodukt einer alten. Kohle zu verkohlen liefert nun gleichzeitig zwei wertvolle Erzeugnisse. Das erste ist schwer, greifbar – Koks. Das zweite ist unsichtbar und mächtig – Gas.

In Kapitel eins schrieb ich einen Satz, der seither wie ein Versprechen über dem Buch hängt. Ich nannte das Bitcoin-Mining Murdochs Gas von 2009, das noch niemand in ein Rohr gesammelt hat. Der Prozess läuft: Computerzyklen werden milliardenfach verbrannt, Kraftwerke laufen, Chips erhitzen sich. Wofür? Für eine Sache – das Finden eines Digests, dessen erste N Bits Nullen sind. Gefunden – der Block wird gutgeschrieben, die Belohnung ausgezahlt. Der ganze Rest des rechnerischen Nebenprodukts wird in die Atmosphäre geworfen. Geht als Wärme ab. Ins Nichts.

2013 betrachtete ein Ingenieur dieses Bild und sah genau das, was Murdoch 1792 sah. Nicht „wie man ein effizienteres Bitcoin macht“. Sondern „was, wenn wir das Nebenprodukt sammeln“. 2022 startete auf Basis dieser Idee das Qubic-Netzwerk. Bis 2024 hatte sich die UPoW-Mechanik, um die es in diesem Kapitel geht, stabilisiert.

Drei Fragen sind zu beantworten. Erstens: Was genau lösen Qubic-Miner in jedem Tick? Zweitens: Warum dient das Ergebnis dieser Arbeit gleichzeitig dem Konsens und noch etwas anderem – und was genau ist dieses „andere“? Drittens: Funktioniert es heute wie geplant – oder nur zur Hälfte?

Beginnen wir mit der Mechanik.

Eine Aufgabe, mehrere Erzeugnisse

Ein Bitcoin-Miner löst eine Aufgabe. Er variiert den Wert des Nonce-Felds im Block-Header, berechnet sha256 des Headers, betrachtet den entstehenden Digest, prüft: Sind die ersten N Bits Nullen? Wenn nicht – Nonce ändern, erneut berechnen. Wenn ja – der Block ist gefunden, ans Netzwerk übertragen, die Belohnung eingenommen. Das ist alles. Die gesamte Bitcoin-Mining-Industrie, Zehnmilliarden Dollar an Hardware, Hunderte Terawattstunden pro Jahr – ist Brute-Force-Suche nach einer Übereinstimmung: einem Digest mit der erforderlichen Anzahl führender Nullen.

Was geschieht im Inneren? Jede sha256-Berechnung durchläuft vierundsechzig Runden interner Transformationen, und bei jedem Zwischenschritt entsteht ein Zustand – Bits, Registerzustände. Konstruktionsbedingt bedeuten diese Zwischenzustände außerhalb von sha256 nichts. Sie sind keine Daten, sie sind kein Signal, sie enthalten keine wiedergewinnbare Struktur. Sie sind rechnerisches Nebenprodukt, das genau so lange existiert, wie es braucht, um das nächste zu erzeugen. Der Chip berechnet sie, der Chip vergisst sie. Am Ausgang – ein Digest. Ein Erzeugnis, ein Wert, ein Zweck.

Und das ist, wichtig zu sagen, kein Bug. Es ist das richtige Design der Funktion für ihren Zweck. Eine Hash-Funktion, deren Aufgabe es ist, eine kryptografisch starke Transformation zu sein, darf in ihren Zwischenzuständen keine nützlichen Spuren hinterlassen. Würde sha256 im Verlauf der Berechnung etwas Nützliches erzeugen, würde das sie verwundbar machen: Vorhersehbarkeit von Nebenprodukten widerspricht der Anforderung der Ununterscheidbarkeit von einer Zufallsfunktion. Bitcoin ist nicht „schlecht gemacht“. Bitcoin ist korrekt gemacht – für das, was es tut.

Aber für das, was Qubic tut, wird eine Funktion anderen Designs gebraucht.

So beschreibt Come-from-Beyond die Aufgabe – der Schöpfer des Systems, dem der Leser bereits in Kapitel vier begegnet ist. Das Zitat ist öffentlich, aus seinem Beitrag vom 23. Juli 2024:

„Die Aufgabe des Qubic-Miners ist dem Bitcoin-Hashing ähnlich und lässt sich darauf reduzieren, einen solchen Digest zu finden, dessen erste N Bits Nullen sind. Wir setzen die Schwierigkeit manuell fest (das Entwicklerteam wählt sie jede Epoche), indem es den Wert von N festlegt. Jeder Computor simuliert das ANN (das wir bei der obigen Reduktion als Hash-Funktion dargestellt haben) und erzeugt den ‚Digest‘, der darauf geprüft wird, ob die ersten N Bits auf null gesetzt sind.“

Lesen Sie den Satz langsam. Die Aufgabe des Qubic-Miners ist dem Bitcoin-Hashing ähnlich. Und lässt sich darauf reduzieren, einen solchen Digest zu finden, dessen erste N Bits Nullen sind. Dieselbe Aufgabe. Nicht ähnlich, nicht analog – formal auf dieselbe reduzierbar.

Aber weiter: Jeder Computor simuliert das ANN (das wir bei der obigen Reduktion als Hash-Funktion dargestellt haben). Jeder Computor simuliert ein künstliches neuronales Netz – das durch eine formale Reduktion als Hash-Funktion dargestellt wird. Das ist der strukturelle Unterschied. Der Digest, dessen erste N Bits Nullen sind, wird nicht von sha256 erzeugt, sondern durch das Durchlaufen von Daten durch

ein neuronales Netz. Am Eingang – einige Parameter, innen – ein Vorwärtsdurchlauf durch Schichten des ANN (Matrixmultiplikationen, nichtlineare Aktivierungen, Aggregationen), am Ausgang – eine Bitfolge, die auf führende Nullen geprüft wird.

Ich unterstreiche: Das ist keine Analogie und keine Metapher. Das Zitat sagt es explizit: „das wir bei der obigen Reduktion als Hash-Funktion dargestellt haben“ – als Hash-Funktion dargestellt durch eine formale Reduktion. Das heißt, es ist mathematisch nachgewiesen, dass der Durchlauf durch das ANN sich in den relevanten Eigenschaften wie eine Hash-Funktion verhält, und daher hat die Aufgabe „finde eine Eingabe, für die die ersten N Ausgabe-Bits Nullen sind“ dieselbe Bedeutung wie bei Bitcoin. Der Unterschied ist, dass der Prozess, der den Digest erzeugt, jetzt Spuren hinterlässt.

Die Zwischenzustände der ANN-Simulation – Neuronenaktivierungen, Gewichtsverteilungen auf trainierten Schichten, die Struktur, wie die Daten durch das Netz liefen – das sind keine leeren Bits wie in sha256. Das sind Daten, die im ehrlichsten Sinn neuronale-Netz-Daten sind. Sie können zum Training genutzt werden. Zur evolutionären Selektion von Architekturen. Für alles, was modernes maschinelles Lernen ausmacht.

Ein Stück Arbeit eines Qubic-Miners erzeugt drei Erzeugnisse gleichzeitig.

Das erste Erzeugnis ist Konsensbeweis. Ein gefundener Digest mit den ersten N Nullen ist eine Bestätigung, dass der Computor eine gültige Simulation durchgeführt hat. Das ist das Äquivalent zu „einen Block gefunden“ bei Bitcoin: ein Arbeitsnachweis, den das Netzwerk verifizieren und anerkennen kann. Auf diesem Erzeugnis baut die Zertifizierung von Ticks auf. Das macht UPoW im strengen Sinne zu einem Proof-of-Work – es gibt Arbeit, es gibt ihren Beweis, die Arbeit kann nicht billiger gefälscht als geleistet werden.

Das zweite Erzeugnis sind KI-Trainingsdaten. Die Zwischenzustände der ANN-Simulation. Die konkreten Werte, an denen die Arbeit geleistet wurde. Diese Daten sind ein wertvolles Nebenprodukt, reserviert im Projekt für einen Verbraucher namens Aigarth – eine separate Komponente des Systems, die die gewonnenen Ergebnisse zur evolutionären Selektion neuronaler-Netz-Architekturen nutzt. Über Aigarth spreche ich erst in Kapitel elf ausführlich; hier zählt eines: UPoW produziert die Daten, Aigarth konsumiert sie. Wie Come-from-Beyond selbst es am 13. Mai 2024 ausdrückte: „Miner leisten nützliches PoW, nicht Aigarth.“ Produzent und Konsument sind zwei verschiedene Knoten, und die Trennung zwischen ihnen muss im Blick behalten werden.

Das dritte Erzeugnis ist Score. Score ist das strukturierte Gedächtnis des Netzwerks, das nach den Ergebnissen der Epoche bestimmt, wer bleibt, wer geht, wer ankommt. Der Inhalt des Scores kann nun entfaltet werden.

Score ist die aggregierte Anzahl gültiger Digests, die ein Computor über eine Epoche gefunden hat. Jeder Digest ist eine erfolgreich durchgeführte ANN-Simulation, jede Simulation ist eine Einheit nützlicher Arbeit. Der Score der Epoche ist die Summe dieser Einheiten über die Woche. Das Netzwerk zählt nicht nur Stimmen oder Ticks; das Netzwerk zählt Arbeit einer bestimmten Art. Je mehr gültige Simulationen ein Computor durchgeführt hat, desto höher sein Score. Je höher der Score, desto sicherer bleibt er unter den 676 für die nächste Woche und fällt nicht in die 225 Rotationsplätze.

Was in Kapitel sieben „das Gedächtnis des Netzwerks“ genannt wurde, hat nun Inhalt erhalten. Das Gedächtnis ist eine Zählung, wie oft man in einer Woche genau jene Art von Arbeit produziert hat, die

das Netzwerk als Grund ansieht, einen an seinem Platz zu halten. Nicht gezahltes Geld, nicht Proof of Stake, nicht soziale Reputation – sondern eine Zählung gültiger neuronaler-Netz-Simulationen. Architektonisch ist auch das eine selten anzutreffende Lösung: „Wer im Spiel bleibt, ist derjenige, der nach seinen Regeln mehr Arbeit geleistet hat."

Nun können wir zur Parallele zurückkehren, die über Kapitel eins hing. Bitcoin ist die Darby-Phase. Kohle brennt, Koks entsteht, Rauch entweicht. Rechenleistung wird verbrannt, Konsens entsteht, alles andere wird weggeworfen. Das Schema ist vollständig und funktioniert; es hat kein Loch – es hat nur ein Erzeugnis. Qubic ist die Murdoch-Phase. Derselbe Prozess umgebaut, sodass dieselbe Eingabe mehrere Erzeugnisse gleichzeitig produziert. Nicht „ein verbessertes Bitcoin-PoW" – ein anderes industrielles Regime derselben rechnerischen Verbrennung. Genauso wie das Verkoken 1792 nicht „besseres Verbrennen von Kohle" war, sondern eine Phase, aus der die Chemie der Nebenprodukte in England begann.

1792 dachte niemand in Coalbrookdale „ugh, was für schlechtes Verkoken, vorher haben wir es falsch gemacht". Verkoken wurde bereits davor korrekt gemacht – um des Kokses willen, der für Gusseisen gebraucht wird, das für das Empire gebraucht wird. Murdoch sah einfach, dass der Prozess ein potenzielles zweites Erzeugnis hatte, das bis dahin ignoriert wurde. Bitcoin-PoW ist analog: Es tut genau das, was von ihm verlangt wird; seine Funktion hat konstruktionsbedingt keine nützlichen Nebenprodukte, und das ist das richtige Design für seine Aufgabe. UPoW ist nicht besser. UPoW ist etwas anderes.

Und hier muss ich innehalten. Bevor ich entfalte, was „das System hat drei Erzeugnisse, aber eines davon wird bislang nicht mit voller Kraft genutzt" bedeutet, muss an einer Stelle, an der sich die Community regelmäßig verwirrt, strenge Ordnung geschaffen werden. Drei verschiedene Dinge, die mit ähnlichen Wörtern bezeichnet werden, aber unterschiedliche Aufgaben erfüllen, müssen getrennt werden. Das ist ein kurzer Abschnitt, aber ohne ihn wird der nächste, zentrale Abschnitt des Kapitels nicht wie beabsichtigt funktionieren.

Drei Schichten der Arbeit: Was Qubic zu Qubic macht

Ein mit Krypto vertrauter Leser mag ganz vernünftig denken: „Nützliches PoW ist nichts Neues. Flux vermietet Rechenleistung für wissenschaftliche Berechnungen. Gridcoin bezahlte schon 2013 für BOINC-Aufgaben. Alter Hut. Was ist die Sensation?"

Die Antwort: Nichts davon ist UPoW. Das ist PoUW. Ein Ein-Buchstaben-Unterschied, aber ein struktureller.

PoUW – Proof of Useful Work. In bestehenden Umsetzungen (Flux, frühes Gridcoin, mehrere akademische Projekte) existiert nützliche Arbeit oben auf dem Konsensmechanismus. Innerhalb des Netzwerks läuft klassisches PoW oder PoS – für Sicherheit; parallel dazu stellt das Netzwerk Infrastruktur bereit, über die externe Kunden Rechenleistung für wissenschaftliche Berechnungen oder Rendering mieten. Zwei unabhängige Schichten, verbunden durch einen Token. Netzwerkknoten können gleichzeitig die Kette absichern und nützliche Aufgaben ausführen – aber „die Kette absichern" und „nützliche Aufgaben" sind zwei getrennte Jobs, jeder mit eigenem Zweck.

UPoW – Useful Proof-of-Work. In Qubic ist nützliche Arbeit selbst der Konsensmechanismus. Nicht „zusätzlich zu“ und nicht „obendrauf“. Genau dieselbe ANN-Simulation, die Aigarth braucht, ist das, was den Digest erzeugt, der den Computor als aktiven Netzwerkteilnehmer zertifiziert. Ein Prozess, der gleichzeitig beide Jobs erledigt. Es gibt nicht zwei Schichten, die kombiniert werden müssten.

Come-from-Beyond formulierte das am 3. April 2024 in einem kurzen Satz: „UPoW ist nicht gleich PoUW.“ Nicht dasselbe. Ich stelle das absichtlich in einen eigenen Abschnitt, denn die Verwechslung des einen mit dem anderen ist der häufigste Fehler in Diskussionen über Qubic. Man verwechselt es leicht, weil die Buchstabenreihenfolge fast identisch ist, der funktionale Unterschied jedoch – grundlegend.

Nun die zweite Trennung, die hier vorgenommen werden muss. UPoW ist eine Sache. Externes Mining, an dem Qubic ebenfalls beteiligt ist, ist eine andere.

Parallel zu UPoW laufen zwei weitere Ströme rechnerischer Aktivität auf dem Netzwerk. Der erste ist externes Mining. Zuerst, von Mai 2025 bis April 2026, schürfte das Netzwerk Monero. Ab Februar 2026 wurde ein DOGE-Add-on gestartet.

Es ist wichtig zu verstehen, was externes Mining strukturell ist. Es ist nicht Teil von UPoW. Es wird von denselben Computoren ausgeführt, aber mit einer anderen Aufgabe, auf anderer Infrastruktur, mit anderem Ergebnis. DOGE-Mining bringt dem Netzwerk Einnahmen (einen Zufluss von Coins, die dann über den Buyback-Mechanismus in QU umgewandelt und verbrannt werden – das sind Details für Kapitel neun). UPoW bringt dem Netzwerk Konsens. Das sind zwei verschiedene Jobs, die ein Computor parallel ausführen kann, die aber architektonisch nicht dasselbe sind.

Come-from-Beyond formulierte das am 15. Juli 2025 direkt: „Zu viel Missverständnis über #Qubic #UPoW auf X. Das Schürfen von $XMR ist nicht Teil davon, Schürfen für #Aigarth ist es. Blöcke für #Monero zu finden sieht nützlich aus, beeinflusst aber nicht direkt die Zertifizierung der Validatoren.“ Und separat, im selben Thread: „Monero-Mining ist nicht UPoW.“

Hier ist es wichtig, langsam vorzugehen. Externes Mining „sieht nützlich aus“ – sieht tatsächlich nützlich aus. Sehr sogar. Es bringt dem Netzwerk Einnahmen, es liefert Hashrate, 2025 machte es Qubic sogar vorübergehend zum größten Teilnehmer im Monero-Netzwerk. All das sind reale Ergebnisse. Aber es beeinflusst nicht direkt die Zertifizierung von Validatoren. Ein Computor bekommt keinen Platz in der nächsten Epoche dafür, dass er einen Monero-Block geschürft hat. Ein Computor bekommt seinen Platz dafür, dass er genug gültige Digests produziert hat – für UPoW.

Dafür gibt es einen empirischen Beweis, und er ist stark. In Discord-Beiträgen vom 17. April 2026 beschrieb Come-from-Beyond das beobachtete Bild: Von 676 Computoren machen etwa 20 nur UPoW, ohne XMR und ohne DOGE. Sie erhalten dabei etwa 80 % des maximalen Einkommens der Epoche. Das bedeutet, der Bonus durch externes Mining macht rund 20 % des vollen Einkommens aus. Das ist keine nachträgliche Schätzung; es ist eine direkte Messung an einem lebenden Netzwerk.

Daraus folgt eine Aussage, die es sich lohnt laut auszusprechen. Rund 80 % des Werts des Netzwerks werden von UPoW produziert. Rund 20 % von externem Mining. Und – der entscheidende Test: Schaltet man DOGE ab, arbeitet das Netzwerk weiter. Schaltet man UPoW ab, ist das Netzwerk tot. UPoW ist das Fundament. Externes Mining ist ein Anbau.

Hier schließt sich Kapitel drei. Dort schrieb ich: Der Mining-Prozess selbst muss Dezentralisierung erzeugen. Bitcoin tut das nicht – Mining erzeugt Konzentration durch die Skaleneffekte von ASICs, und heute kontrollieren zwei Pools den Großteil der Hashrate. Qubic macht es anders. UPoW produziert Score. Score bestimmt, wer unter den 676 in der nächsten Epoche bleibt. Der Prozess der Digest-Produktion und der Prozess der Produktion der Netzwerkzusammensetzung sind buchstäblich ein und derselbe Prozess. Nicht „wir schürfen, und parallel dazu wird die Zusammensetzung durch ein anderes Verfahren aktualisiert“, sondern „wir schürfen – und aktualisieren dadurch die Zusammensetzung“. Der Kreis schließt sich in sich selbst: Arbeit erzeugt das Recht, weiterzuarbeiten; das Recht, weiterzuarbeiten, wird dadurch bestimmt, wie viel Arbeit man geleistet hat.

Das schließt auch strukturell ein weiteres Versprechen. In Kapitel drei formulierte ich Axelrods vierte Bedingung: Ein Sieg im Spiel darf nicht in das Recht umgewandelt werden können, das Spiel selbst zu ändern. In der Architektur von UPoW wird diese Bedingung so erfüllt: Ein hoher Score gibt einem das Recht, für die nächste Runde des Spiels unter den 676 zu bleiben. Er gibt kein erhöhtes Stimmgewicht, keinen vergrößerten Konsensanteil, keinen Einfluss auf Parameter. Nur – das Recht, weiterzuspielen. Mehr gewonnen – du bleibst. Die Spielregeln – änderst du nicht. Eine saubere Umsetzung dessen, was Axelrod bei der Beschreibung des Turniers als notwendige Bedingung für die Widerstandsfähigkeit von Kooperation formulierte.

Und eine kurze historische Bemerkung, die hier passt. Am 23. September 2021, sieben Monate vor dem Mainnet-Start, nannte Come-from-Beyond in einem öffentlichen Tweet drei architektonische Eigenschaften des künftigen Netzwerks: „Nützliches PoW, anders als bei #Bitcoin / 100%ige Gewissheit des Transaktionsausgangs / Gebührenfreie Überweisungen wie bei #IOTA.“ Nützliches PoW – anders als bei Bitcoin. Hundertprozentige Gewissheit des Transaktionsausgangs. Gebührenfreie Überweisungen, wie bei IOTA. UPoW wurde namentlich genannt, noch bevor das Netzwerk existierte. Keine nachträgliche Rationalisierung („wir haben etwas gebaut, und jetzt erklären wir, was es war“); eine vor dem Start abgegebene, im Nachhinein überprüfbare Erklärung.

Eine gesonderte Klarstellung für den aufmerksamen Leser. Qubic hat als technisches Projekt eine lange Vorgeschichte. In Kapitel fünf erwähnte ich Jinn – eine Forschungsanstrengung der frühen 2010er, bei der das Konzept nützlicher Arbeit erstmals als Möglichkeit durchdacht wurde. UPoW ist seine Verwirklichung ein Jahrzehnt später, in einem anderen Kontext und auf anderer Grundlage. Von der Idee zum funktionierenden Netzwerk – ein Jahrzehnt verging. Das ist ein normales Tempo für eine nichttriviale infrastrukturelle Idee.

Nun, mit der Trennung der drei Schichten in der Hand, kann ich direkt über das sprechen, wovor ich im ersten Abschnitt des Kapitels warnte. Über jene Lücke zwischen Gebautem und mit voller Kraft Laufendem, die der Schöpfer des Systems selbst öffentlich benannt hat.

Ehrliche Offenlegung: „Useless PoW“ und warum es das gibt

An diesem Punkt könnte der Leser vermuten, UPoW sei zu schön, um zu funktionieren. Er liegt halb richtig. Die Idee funktioniert. Die Umsetzung ist noch nicht mit voller Kraft. Der Autor des Systems hat das selbst gesagt, zweimal, öffentlich – und beim zweiten Mal, im Juli 2025, ein Wort verwendet, das schwer zu vergessen ist.

Das erste Zitat, wörtlich. Am 17. Juli 2025 schrieb Come-from-Beyond auf Discord: „Im Ernst, die aktuellen Mining-Parameter sind nutzlos, aktuell bedeutet UPoW Useless Proof-of-Work.“ Und im selben Thread, in einem separaten Satz: „genau wie unser aktuelles UPoW“. Nicht Kritiker schrieben das – der Schöpfer des Systems schrieb es selbst, vor Zeugen, auf einer öffentlichen Plattform, in einem Kanal, in dem die Ingenieure und die Token-Halter versammelt sind.

Das Wort „nutzlos“ ist kein Zufall. Das übliche Marketingregister erlaubt „noch nicht mit voller Kraft“, „bleibt zu polieren“, „im Prozess der Optimierung“. Come-from-Beyond wählte keine dieser weichen Formulierungen. Er wählte ein Wort, das bei jeder Lesart wie eine Tatsachenfeststellung klingt: im Moment – nutzlos. Und mit einem zweiten Zug verstärkte er es: genau wie unser aktuelles UPoW.

Und das ist nicht die erste solche Aussage. Am 7. Dezember 2023, anderthalb Jahre zuvor, war derselbe Gedanke bereits geäußert worden – etwas weicher, aber mit derselben Struktur. „Gerade jetzt ist unser Useful PoW halb-nützlich, weil Aigarth nicht alle bereitgestellten Lösungen verarbeiten kann.“ Gerade jetzt ist unser Useful PoW halb-nützlich, weil Aigarth nicht alle bereitgestellten Lösungen verarbeiten kann. Das Problem ist nicht erst seit letztem Jahr festgehalten. Es ist dem Schöpfer des Systems mindestens seit Ende 2023 bekannt.

Was genau bedeuten diese beiden Zitate? Ich arbeite es langsam durch, denn das ist das strukturelle Zentrum des Kapitels, und von der Genauigkeit der Formulierung hängt ab, ob der Leser es richtig versteht.

Die Infrastruktur von UPoW funktioniert vollständig für alle ihre Designziele für den Konsens. Computoren simulieren das ANN. Digests werden validiert. Score wird zugewiesen. Rotation von 225 Plätzen geschieht jeden Mittwoch. Das Netzwerk ist dezentral, abgesichert, funktionsfähig. Betrachtet man Qubic heute als Blockchain – ist alles in Ordnung, die Konsensschicht tut genau das, was sie versprach zu tun, und dieses erste der drei UPoW-Erzeugnisse (Beweis für den Konsens) wird vollständig produziert.

Das Problem liegt nicht im ersten Erzeugnis. Das Problem liegt im zweiten. KI-Trainingsdaten werden jeden Tick produziert – aber nicht alle werden verbraucht. Aigarth, konzipiert als Verbraucher dieser Daten, kann das volle Volumen der Lösungen, die das Netzwerk ihm liefert, noch nicht verarbeiten. Das Netzwerk generiert mehr, als Aigarth verzehrt. Die Differenz ist genau das, was Come-from-Beyond halb-nützlich und nutzlos nennt.

Die Gründe, in seinen eigenen Worten, sind zwei. Der erste ist die Durchsatzgrenze von Aigarth. Der Verbraucher ist bislang kleiner als der Produzent; das ist eine technische Skalierungsaufgabe, an der gearbeitet wird. Der zweite sind die Parameter der Aufgabe selbst. Das ANN, das die Computoren simulieren, ist gewählt und abgestimmt, um Gültigkeit für den Konsens zu liefern. Für Aigarths Bedürfnisse ist es nicht optimiert – es könnte die falsche Architektur, die falschen Größen, die falschen Eigenschaften haben, um für die evolutionäre Selektion nützlicher neuronaler Netze maximal nützlich zu sein. Das ist ein architektonisches Designproblem, das nur durch Änderung der Parameter und – letztlich – durch das Deployment von Aigarth in seiner Produktionsform gelöst wird.

Die Parallele zur Kohle drängt sich hier auf. Murdoch legte 1792 das erste Rohr. Aber die Gasbeleuchtung funktionierte die ersten paar Jahre nur in seiner eigenen Werkstatt in Redruth. London begann 1807 mit Gas beleuchtet zu werden – wirklich, mit Straßenbeleuchtung der Straßen. Die

Gaswerksindustrie nahm ernsthaft, als Industrie, bis in die frühen 1820er Gestalt an. Zwischen „wir können das Gas sammeln“ und „Gas beleuchtet London“ – vergingen fünfzehn Jahre. Zwischen „Gas beleuchtet London“ und „Gas treibt Industrie an“ – weitere zehn. Das ist ein normales Tempo für einen infrastrukturellen Wandel.

Im Fall von UPoW: Mainnet startete am 13. April 2022. UPoW als Mechanik stabilisierte sich 2024. Das geplante Deployment von Aigarth – 13. April 2027. Zwischen „die Mechanik funktioniert“ und „die Mechanik wird mit voller Kraft genutzt“ hat das Projekt etwa fünf Jahre reserviert. Das ist ein Arbeitstempo.

Nun eine wichtige Frage: Warum wird das öffentlich gesagt, statt unter den Teppich gekehrt?

Come-from-Beyond hätte schweigen können. Er hätte warten können, bis Aigarth aufgeholt hat, und über UPoW nur in der Vergangenheitsform sprechen: „gebaut“, „funktioniert“. Die PR-Materialien, die jedes technologische Projekt begleiten, hätten das leicht erlaubt. Keiner von Qubics Kritikern hatte „Useless PoW“ in der eigenen Formulierung des Systemschöpfers an die Öffentlichkeit gebracht – weil die Formulierung selbst von ihm geschaffen wurde. Er hätte sie für sich behalten können.

Er tat es nicht. Und das ist keine zufällige Angewohnheit. In Kapitel vier beschrieb ich ein Prinzip, dem Come-from-Beyond seit einem zweiten Jahrzehnt folgt: verkaufe nicht, was es noch nicht gibt. „Useless PoW“ zu verstecken hätte bedeutet, diese Regel genau an der Stelle zu verletzen, an der sie am spürbarsten getestet wird – im zentralen Mechanismus des zentralen Kapitels des gesamten Projekts. Es laut auszusprechen ist, die Regel stärker zu bekräftigen, als es jede PR-Botschaft formulieren könnte. In einer Welt, in der neunzig Prozent der Token-Projekte technische Probleme bis zum Moment des Zusammenbruchs hinter Marketing verstecken, ist es keine Schwäche und kein Eingeständnis der Niederlage, die eigene Hauptschwäche öffentlich zu machen. Es ist Disziplin.

Was ist Phase 3, und was hat DOGE damit zu tun?

Erstens: Der XMR-Mining-Code wird aus dem Kern entfernt. Nicht durch ein Flag ausgeschaltet, das man in einer Minute zurückschalten könnte – vollständig entfernt, sodass für eine Rückkehr ein neues Release mit Wiederherstellung des Codes nötig wäre. Das ist eine chirurgische architektonische Festlegung. Das Monero-Kapitel ist geschlossen.

Zweitens: Phase 3 der Rechenleistungsverteilung wird aktiviert. Das neue Verhältnis ist etwa 80 % für Aigarth-Training, 20 % für DOGE-Mining. In vorigen Phasen ging ein erheblicher Teil der Rechenleistung ins XMR-Mining; dieser Teil wird nun freigesetzt und Aigarth gegeben. Zum ersten Mal seit dem Mainnet-Start hat Aigarth Zugang zu 100 % der für KI-Arbeit reservierten Rechenleistung.

Phase 3 ist nicht „der Moment, in dem UPoW vollständig nützlich wurde“. Es ist der Moment, in dem die Lücke zwischen Gebautem und Genutztem durch Skalierung des Verbrauchers zu schließen begann. Wie schnell sie sich schließen wird und ob sie sich zum geplanten Datum schließen wird, ist eine Frage für Teil fünf des Buches. Dort kehre ich zu Fragen von Aigarths Architektur und seinem Deployment zurück.

Von Phase 3 bis zum geplanten Deployment von Aigarth – 356 Tage. Einundfünfzig Wochen. Einundfünfzig Epochen. In den zuvor eingeführten Zeitbegriffen – einundfünfzig Runden des wiederholten Spiels.

Ich schließe diesen Abschnitt mit einem ehrlichen Rahmen.

UPoW ist im April 2026 Infrastruktur, die ein Ingenieur 2013 zu durchdenken begann, ein Jahrzehnt lang umsetzte und 2022 im Mainnet startete. Es funktioniert gegen alle seine Designziele bis auf eines: Die KI-Komponente nutzt bisher nur einen Teil dessen, was produziert wird. Das ist ein Riss zwischen Gebautem und Genutztem. Er existiert. Er ist vom Schöpfer öffentlich festgehalten worden, zweimal, im Abstand von anderthalb Jahren.

Das ist der ehrliche Zustand von UPoW, Stand April 2026. Weder weniger noch mehr.

Unter der Haube: Zahlen, Einnahmen und ein architektonischer Bonus

Nun zu den Zahnrädern. Die Mechanik von UPoW drückt sich nicht nur in Worten aus; hinter jeder Formulierung der vorigen Abschnitte stehen konkrete Konstanten, die das Team im Code festlegt und die im Qubic-Repository nachgeschlagen werden können. Dieser Abschnitt ist für den Leser, der genau wissen will, woraus die funktionierende Architektur zusammengesetzt ist.

Ich beginne mit dem Parameter N aus dem Zitat vom 23. Juli 2024. Im Code des Qubic-Kerns heißt dieser Parameter ADDITION_SOLUTION_THRESHOLD_DEFAULT, und er bestimmt, wie viele führende Nullen in einem Digest sein müssen, damit die Lösung als gültig zählt.

Ich unterstreiche eine wichtige Nuance. Bei Bitcoin reguliert sich die Schwierigkeit selbst durch den Algorithmus: Alle 2016 Blöcke betrachtet das Netzwerk, wie schnell Lösungen gefunden werden, und passt die Schwierigkeit so an, dass das durchschnittliche Intervall bei etwa zehn Minuten bleibt. Bei Qubic wird die Schwierigkeit vom Entwicklungsteam jede Epoche explizit festgelegt. Das ist eine sinnvolle technische Entscheidung. Die Hardwarebasis von Qubic sind die Computoren, und ihre Zusammensetzung für die nächste Woche ist im Voraus bekannt; es besteht keine Notwendigkeit, eine blinde Selbstregulierung nachzuahmen, wenn man den Parameter direkt für die aktuelle Hardware kalibrieren kann. Es ist dieselbe Geradlinigkeit, der wir in Kapitel sieben bei Epochenübergängen begegneten: nicht „es wird sich schon von selbst einrenken“, sondern „das Team hat eine Entscheidung getroffen“.

Die Referenzimplementierung des Miners von Qubic ist Open Source und heißt Qiner. Der technische Leser kann ins Repository gehen und genau nachsehen, wie die ANN-Simulation auf Code-Ebene aufgebaut ist – nicht aus Worten, sondern aus Quellen. Es ist keine Blackbox; es ist eine öffentliche technische Umsetzung dessen, was in den Abschnitten 2–3 als strukturelle Reduktion besprochen wurde. Ich werde den Code hier nicht nacherzählen – das ist Material für eine eigene Aufschlüsselung –, aber die bloße Tatsache seiner Offenheit zählt: Die Behauptungen über die Mechanik sind unabhängig überprüfbar.

Nun zum Geld. Wie genau bezahlt das Netzwerk die Arbeit eines Computors?

Die Einnahmenformel, festgehalten in PR #844 des Qubic-Kerns und aktiv in Phase 3:

$$\text{Einnahme} = \text{IPC} \times M \times (S^2 + B \cdot E) / \text{DIVISOR}$$

Ich arbeite durch, was jedes Symbol bedeutet.

IPC — Issuance Per Computor, die Emission an einen Computor pro Epoche. Die Konstante beträgt 1.479.289.940 QU; das ist die Einheit einer Billion neu emittierter QU pro Epoche, geteilt durch 676. Die Obergrenze, die ein Computor bei einer idealen Woche erreichen kann.

S — eine Skalierungskonstante, gleich 1024. Alle Faktoren sind auf den Bereich [0, S] normiert.

B — das Gewicht des Bonus für externes Mining, gleich 256.

M — die verpflichtende Komponente, nimmt Werte von null bis S an. Zusammengesetzt aus zwei Teilen: tx-Faktor (Gewicht 85 %) – wie aktiv der Computor Ticks leitet, und Orakel-Faktor (Gewicht 15 %) – inwieweit er am Commit/Reveal-Zyklus der Orakel teilnimmt. Das ist Arbeit, die das Netzwerk als obligatorisch ansieht. Die Komponente multipliziert den Rest der Formel. Wurde die verpflichtende Arbeit nicht geleistet, wird alles Übrige mit einer kleineren Zahl multipliziert, bis hinunter zu null.

E — Mining-Faktor, ebenfalls im Bereich [0, S]. In Phase 3 sind das nur DOGE-Anteile. Das ist Arbeit, die das Netzwerk als optional ansieht. Die Komponente wird über den Term B·E addiert, multipliziert nicht die Basis.

Gehen wir die Bereiche durch. Bei voller verpflichtender Arbeit (M = S) und null externem Mining (E = 0) ergibt die Formel eine Einnahme von etwa 80 % des IPC. Bei voller verpflichtender Arbeit und vollem Mining (E = S) – genau IPC, 100 %. Versäumt ein Computor die verpflichtende Arbeit – bricht die verpflichtende Komponente zusammen, und egal wie viel DOGE er geschürft hat, er bekommt wenig.

Die Konstruktion entspricht direkt dem, was ich im dritten Abschnitt in Worten beschrieben habe. Arbeit, von der der Konsens abhängt – TX-Relay, Orakel, UPoW – ist starr in die multiplikative Schicht der Formel eingebaut. Arbeit, von der nur die Einnahmen des Netzwerks abhängen – DOGE-Mining – ist als schwacher, additiver Bonus eingebaut. Schaltet man DOGE ab, verliert man etwa 20 %. Schaltet man den verpflichtenden Teil ab, verliert man alles.

Und hier lassen Sie uns eines zum zweiten UPoW-Erzeugnis festhalten, das im vierten Abschnitt als Engpass besprochen wurde. KI-Trainingsdaten werden von der Formel nicht direkt bezahlt. Ein Computor erhält keine Einnahme dafür, dass er für Aigarth nützliche Zwischenzustände des ANN produziert hat; er erhält Einnahme dafür, dass er einen gültigen Digest gefunden hat – das erste Erzeugnis – und dass er die verpflichtende Netzwerkarbeit geleistet hat. Das zweite Erzeugnis ist derzeit reines Nebenprodukt, in die Atmosphäre geschrieben, auf einen Verbraucher wartend. Oder, andersherum gesagt: Die Ökonomie bezahlt zwei von drei Erzeugnissen: Konsens und den Rotations-Score (über die verpflichtende Komponente und über die Tatsache, Digests zu finden). Das dritte, die KI-Komponente, wird auf Kredit der Erwartung bezahlt.

Es gibt noch eine Eigenschaft von UPoW, die ich gesondert erwähne, denn sie ist nicht durch Design erworben, sondern durch Struktur. Bitcoin-PoW über die sha256-Funktion ist theoretisch anfällig für Quantenbeschleunigung: Grovers Algorithmus liefert eine quadratische Beschleunigung für das Preimage-Suchproblem, und beim Erscheinen ausreichend großer Quantencomputer wird sich Bitcoin-Mining in einer neuen Realität wiederfinden – nicht zerbrochen, aber umgebaut. UPoW ist anders gebaut. Die Aufgabe „finde eine Eingabe für ein ANN, für die die ersten N Ausgabe-Bits Nullen sind“ lässt sich auf keines der Probleme reduzieren, für die Quantenalgorithmen mit Beschleunigung bekannt sind. Es gibt keinen Quantenalgorithmus, der einen Vorwärtsdurchlauf durch ein beliebiges

neuronales Netz schneller ausführt als der klassische.

Come-from-Beyond formulierte das am 10. November 2025 in einem einzigen Satz: „Anders als PoW ist unser UPoW nicht anfällig für Quantencomputer.“ Anders als PoW ist unser UPoW nicht anfällig für Quantencomputer.

Hier zählt der Ton, in dem ich das sage. Das ist kein primäres Designziel. Quantenresistenz stand nicht auf der Liste der Aufgaben, um derentwillen Qubic 2013 konzipiert wurde. Es ist eine Nebeneigenschaft der Architektur. Aber das ist die Natur vieler eleganter technischer Lösungen: Wenn etwas aus einem Grund richtig gemacht ist, stellt es sich auch aus Gründen als richtig heraus, an die seine Schöpfer nicht dachten. Murdoch sammelte das Gas, um seine Werkstatt zu beleuchten, nicht damit hundert Jahre später chemische Werke auf demselben Gas laufen. Wie es sich fügte, erwies sich das gesammelte Gas sowohl dort als auch hier als nützlich.

Das Letzte, was ich in diesem Abschnitt sage, ist ein kurzes Zitat, auf das ich in Teil fünf des Buches zurückkommen werde. Am 20. November 2023 beschrieb Come-from-Beyond die funktionale Landkarte von Qubic in einem einzigen Satz: „Aigarth nutzt Qubics UPoW, außerdem hat Qubic alles, was eine KI bräuchte: Smart Contracts als Gehirn, Orakel als Sensoren zur Außenwelt, ausgelagerte Berechnungen als Manipulatoren, um diese Außenwelt zu verändern.“

Smart Contracts als Gehirn, Orakel als Sensoren, ausgelagerte Berechnungen als Manipulatoren – und UPoW als Energiequelle für alles. Auf dieser Landkarte ist UPoW nicht „ein Feature des Konsenses“, sondern das Energiesubsystem eines AGI-Substrats. Wie das Herz in einem Körper: Es pumpt, es denkt nicht, aber ohne es funktioniert der Rest nicht. Diese Landkarte zu entfalten ist Aufgabe von Teil fünf; hier wird sie nur als Erinnerung daran gebraucht, wofür all diese Maschinerie letztlich da ist.

Parsons, die Turbine und das zweifach gesammelte Gas

Es gibt noch eine Figur, die es sich lohnt, in dieses Kapitel zu holen, um es abzuschließen. Nicht Murdoch – mit Murdoch haben wir bereits gearbeitet, und wir werden im Finale wieder mit ihm arbeiten. Charles Algernon Parsons, England, 1884.

Vor Parsons arbeitete die Dampfturbine einstufig: Hochdruckdampf traf auf ein großes beschaufeltes Rad, übertrug ihm einen Teil seiner Energie und trat auf der anderen Seite aus – immer noch mit einer enormen Energiereserve, die einfach in den umgebenden Raum entwich. Der Wirkungsgrad der ersten Turbinen lag bei etwa 20 %. Vier Fünftel der Dampfenergie – buchstäblich zum Schornstein hinaus.

Parsons baute eine mehrstufige Turbine. Dampf lief nicht durch ein Rad, sondern durch eine Reihe – schrittweise, wobei er bei jeder Stufe einen Teil seiner Energie abgab und zur nächsten weiterzog. Die erste Stufe nahm, was sie zu nehmen imstande war. Die zweite – was an der ersten vorbeikam. Die dritte – was an den beiden vorbeikam. Und so weiter, in einer Kaskade, bis der aus der letzten Stufe austretende Dampf nur noch Restdruck mit sich trug. Der Wirkungsgrad stieg dank dieser Konstruktion von 20 % auf 50–60 % und höher.

Das Prinzip, das Parsons auf Dampf anwandte, lässt sich abstrakt so formulieren: Sammle nicht alles in einer einzigen Operation, sondern baue eine Kaskade von Operationen, von denen jede sammelt, was die vorherige nicht sammelte. Mehrstufige Extraktion. Extraktion in mehreren Stufen. Die Idee ist auf alles

anwendbar, was einen Prozess mit überschüssiger Energie am Ausgang darstellt.

UPoW ist mehrstufige Extraktion, angewandt auf Rechenleistung.

Bitcoin-PoW ist als einstufige Turbine gebaut: Rechenleistung geht hinein, ein Digest kommt heraus, der ganze Rest der rechnerischen Energie geht als Wärme verloren. Eine Stufe, ein Erzeugnis. UPoW baut denselben Prozess in eine Kaskade um:

Die erste Stufe – Rechenleistung fließt in Form einer ANN-Simulation ein und liefert am Ausgang einen Digest mit N Nullen. Konsensbeweis. Das ist das Erzeugnis, das auch Bitcoin hat.

Die zweite Stufe – die Zwischenzustände der Simulation, die bei Bitcoin konstruktionsbedingt weggeworfen wurden, bleiben hier als Daten erhalten. KI-Trainingsdaten. Ein Erzeugnis, das Bitcoin nicht hat.

Die dritte Stufe – die Gesamtheit der gültigen Digests über eine Epoche wird zu einem Score zusammengefasst, der die Rotation der Netzwerkzusammensetzung bestimmt. Score. Ein Erzeugnis, das Bitcoin nicht hat.

Eine Eingabe – drei Erzeugnisse. Die technische Form dessen, was Murdoch mit Kohle tat, angewandt auf rechnerische Arbeit 217 Jahre später.

Ich unterstreiche eines, damit sich die Parallele nicht als Metapher liest. Parsons und Murdoch arbeiteten an einer Art von Aufgabe. Nicht an einer Substanz – sie arbeiteten jeweils mit Dampf und mit Kohle –, sondern an einer Form der Frage: wie man einen bestehenden Prozess so umbaut, dass er mehrere Erzeugnisse statt eines produziert. Keiner von beiden erfand einen neuen Prozess. Sie bauten einen bestehenden um. UPoW ist ein weiterer Punkt in dieser Reihe. Nicht „die Erfindung eines neuen PoW“, sondern die Anwendung eines alten Prinzips (mehrstufige Extraktion) auf eine neue Substanz (Rechenleistung statt Dampf oder Kohle).

Dieses Kapitel heißt „Murdochs Gas in Aktion“ – nicht „UPoW erklärt“. Der Titel ist so gewählt, weil genau 217 Jahre, nachdem Murdoch das erste Rohr vom Ofen zur Lampe verlegte, dieselbe technische Idee auf das digitale Analogon eben jenes Gases angewandt wird.

Das Gas ist gesammelt. Das Rohr ist verlegt.

Drei Abschnitte verdichteter Mechanik liegen hinter uns. Nun ein kurzer Rückblick auf das Gesamtbild.

Qubic-Miner lösen dieselbe Aufgabe wie Bitcoin-Miner: einen Digest finden, dessen erste N Bits Nullen sind. Aber ihr Digest wird durch die Simulation eines neuronalen Netzes erzeugt, dargestellt als Hash-Funktion durch eine formale Reduktion. Eine Aufgabe am Eingang – drei Erzeugnisse am Ausgang: Beweis für den Konsens, Daten für potenzielles KI-Training, Score für die Rotation der Netzwerkzusammensetzung. Die Infrastruktur funktioniert gegen alle Designziele. Das zweite Erzeugnis – die KI-Komponente – wird bislang nicht mit voller Kraft genutzt; der Schöpfer des Systems hat das selbst zweimal öffentlich laut ausgesprochen, erstmals im Dezember 2023, dann im Juli 2025. Phase 3 wurde aktiviert: Der XMR-Mining-Code ist entfernt, Aigarth hat zum ersten Mal Zugang zu 100 % der für es reservierten Rechenleistung erhalten. Bis zum geplanten Deployment von Aigarth – 356 Tage.

Kapitel sechs beschrieb den Raum dieses Netzwerks – 676 Stimmen. Kapitel sieben beschrieb seine Zeit – Wochen aus Epochen. Dieses beschrieb seine Energie – UPoW und was es produziert. Und Ökonomie beginnt immer mit Energie.

Von Murdoch 1792 bis Parsons 1884 vergingen 92 Jahre. Von Bitcoin 2009 bis Qubic 2022 – 13 Jahre. Industrielle Zyklen haben sich von Jahrhunderten auf Jahre verdichtet, aber ihre innere Logik hat sich nicht geändert: zuerst der Prozess, dann das Sammeln des Nebenprodukts, dann die mehrstufige Optimierung. Wir, die Leser dieses Kapitels im Jahr 2026, stehen an einem Punkt, der in Analogie zur Kohle ungefähr den Jahren 1805–1810 entspricht: Das Gas ist gesammelt, die ersten Lampen brennen, aber die große Gasindustrie – liegt noch vor uns.

Das SCHLÜSSELKAPITEL der ersten Buchhälfte endet nicht auf einer triumphalen Note, gerade weil Triumph noch nicht verdient ist – 2027 liegt eine Prüfung voraus, und jetzt – Arbeit. Genauso wie Murdoch 1792 eine Lampe entzündete, aber die Straßen Londons noch nicht wussten, dass sie bald mit Gas beleuchtet würden.

Das nächste Kapitel handelt von der Ökonomie, die diese Maschine am Laufen hält. Wir haben beschrieben, was Computoren tun. Wir haben noch nicht besprochen, wie das Netzwerk diese Arbeit bezahlt – was genau jeden Mittwoch mit dem QU-Token geschieht, warum Emission und Verbrennung parallel laufen, warum Qubic nicht das Bitcoin-Modell fester Angebotsmenge gewählt hat. Der atmende Token: Jede Epoche entsteht eine Billion neuer QU, ein erheblicher Teil wird über den Buyback-Mechanismus verbrannt, und das Angebot pulsiert im Takt der Wochen aus Epochen.

Murdochs Gas ist gesammelt. Das Rohr ist verlegt. Nun lasst uns herausfinden, wer für seinen Betrieb bezahlt – und was der Preis von Gas in einer Welt ist, in der Gas nicht Licht, sondern Intelligenz erzeugt.

9
Der atmende Token

Einatmen, ausatmen, Woche

Beginnen wir mit einer einfachen Erinnerung. Eine Qubic-Epoche ist eine Woche. Jeden Mittwoch, gegen zwölf Uhr UTC, startet das Netzwerk neu, 225 der 676 Computor-Sitze können den Besitzer wechseln, die Zähler werden zurückgesetzt, und eine neue Runde beginnt. Diese Mechanik haben wir in Kapitel 7 behandelt; hier wird sie als Hintergrund für eine bestimmte Sache gebraucht: Mit eben diesem Neustart tritt jede Woche eine Billion frisches QU ins Netzwerk ein.

Nicht „etwa eine Billion“. Genau eine Billion. Das ist das Einatmen des Netzwerks.

Dann, über die sieben Tage bis zum nächsten Mittwoch, geschieht das Ausatmen. QU werden verbrannt – über mehrere unabhängige Pfade, jeder mit eigenem Zweck, eigener Logik. Manche sind fest ins Protokoll verdrahtet, manche hängen von Entscheidungen der Computoren ab, manche von externer Ökonomie, auf die das Netzwerk keinen direkten Einfluss hat. Am Ende der Epoche ergibt die Bilanz aus Ein- und Ausatmen die Nettoveränderung der umlaufenden Menge. 2025–2026 fiel diese Bilanz regelmäßig negativ aus: Das Netzwerk verbrannte mehr, als es emittierte.

Daher der Arbeitstitel dieses Kapitels. Der Token, der atmet. Nicht „deflationär“, nicht „inflationär“ – atmend. Jede Woche ein Einatmen; im Laufe der Woche eine Reihe von Ausatmern unterschiedlicher Tiefe. Das Angebot pulsiert im Takt der Epochen.

In Kapitel 7 verwendete ich das Wort „Puls“ für den Rhythmus des Netzwerks. In diesem Kapitel kehrt die verwandte physiologische Metapher zurück – Atmung. Das ist eine bewusste Wahl. In Kapitel 8 war das Register industriell – Gas, Rohr, Turbine, mehrstufige Extraktion; das Kapitel handelte von Energie. Kapitel 9 handelt von Ökonomie, und Qubics Ökonomie ist als Kreislauf gebaut, nicht als Verbrennung. Physiologie passt also genauer als Industrie. Herz und Lunge – zwei Rhythmen desselben Organismus; der wöchentliche Rhythmus des Netzwerks zeigt sich in beiden.

Aber ich werde die Metapher nicht überstrapazieren. Das Bild soll funktionieren, nicht damit gespielt werden.

Nun – zu dem Kontrast, der über diesem ganzen Thema hängt.

2008 traf der anonyme Autor von Bitcoin eine Entscheidung über das Angebot, und sie stand seither nicht mehr zur Diskussion. Einundzwanzig Millionen Coins, Halvings alle vier Jahre, letzte Emission irgendwann um 2140. Das ist keine Frage der Abstimmung oder ein Parameter, den man unterwegs anpasst – es ist eine Konstante, eingebacken in den Code beim Netzwerkstart. Ein Bitcoin-Halter weiß: Wie viele Jahre auch vergehen, wie sich die Bedingungen auch ändern, das Angebot wird das sein. Das

ist das Wertversprechen.

Bei Qubic wird das Angebot jeden Mittwoch debattiert. 676 Computoren stimmen darüber ab, wie viel QU bis zum Ende dieser Epoche im Umlauf bleiben soll. Sie können beschließen, mehr oder weniger zu verbrennen. Sie können – theoretisch – beschließen, die Emissionsparameter für die nächste Epoche zu ändern. Alles, was mit dem Angebot zu tun hat, lebt in einem fortlaufenden Abstimmungsprozess, nicht in der Vorab-Entscheidung einer Person.

Das ist kein kleiner technischer Unterschied. Das sind strukturell unterschiedliche Antworten auf die Frage „was ist Geld“. Zu einer vollständigen Aussage dieses Unterschieds kommen wir in Abschnitt 6 dieses Kapitels, wenn wir das zentrale Zitat des Systemschöpfers durcharbeiten.

Drei Fragen:

Erstens: Woher kommen QU? Abschnitt zur Emission.

Zweitens: Wohin gehen sie? Abschnitt zu den sieben Verbrennungspfaden.

Drittens: Wer entscheidet, und wie, wie viel im Umlauf sein soll? Abschnitt zur Computor-Abstimmung, zur Verbindung mit Axelrods vierter Bedingung, und zur Rolle des Arbitrators als Rückfallebene.

Beginnen wir mit dem Einatmen.

Einatmen: eine Billion jeden Mittwoch

Jede Epoche emittiert das Netzwerk exakt eine Billion frisches QU. Das ist eine Protokollkonstante, fest im Code, nicht per Abstimmung anpassbar. Es ist das Grundgehalt des Netzwerks, seine fundamentale Eingabe. Auf das Jahr gerechnet – zweiundfünfzig Billionen QU (52 × 1 Billion = 52 Billionen Brutto-Emission pro Jahr).

Diese eine Billion wird unter 676 Computoren aufgeteilt – jenen, die für diese Epoche aktive Sitze im Netzwerk halten. Eine einfache Division ergibt eine wichtige Konstante, die bereits im vorigen Kapitel auftauchte: Issuance Per Computor, IPC = 1.479.289.940 QU. Eine Billion geteilt durch 676, gerundet. In Kapitel 8 tauchte diese Zahl als Parameter in der Einnahmenformel auf. In Kapitel 9 erhält sie ihre ökonomische Bedeutung: Sie ist die Obergrenze dessen, was ein Computor in einer einzigen idealen Epoche verdienen kann.

„Obergrenze“ – nicht „garantierter Betrag“. Das tatsächliche Einkommen wird nach der Formel aus Kapitel 8 berechnet:

Einnahme = IPC × M × (S^2 + B·E) / DIVISOR

Nur zur Erinnerung an die Struktur: Die verpflichtende Komponente M (TX-Relay, Orakel) multipliziert den Rest der Formel, und die externe-Mining-Komponente E wird über einen kleinen additiven Bonus hinzugefügt. Daraus folgte die empirische Beobachtung in Kapitel 8: Ein Computor, der nur die erforderliche Netzwerkarbeit und UPoW leistet, sich aber nicht am externen Mining beteiligt, erhält etwa 80 % des IPC. Bei vollem externen Mining – 100 %. Das ist dieselbe 80/20-Aufteilung, die wir als Tatsache in Kapitel 8 kennengelernt haben und auf die wir in Abschnitt 3 dieses Kapitels zurückkommen.

Nun – ein wichtiger Punkt dazu, wie die Verteilung funktioniert. Der Schöpfer des Systems formuliert das Emissionsprinzip knapp und ohne Euphemismen – er nennt es Subvention. In einer öffentlichen Nachricht vom 20. Mai 2024:

„Warum sich aufregen, wenn die Subventionsmethode im Alltag weit verbreitet ist? Wenn man ein Ticket kauft, um 2 km mit dem Bus zu fahren, zahlt man dasselbe wie jemand, der 7 km fährt."

Die Analogie ist klar. Im Bus zahlt man für das Ticket, nicht für die Kilometer. Fährt man zwei Haltestellen oder sieben – der Preis ist derselbe. Viele Versorgungsmodelle funktionieren so, Abo-Dienste funktionieren so, subventionierte Gesundheitsversorgung funktioniert so. Die Idee der Subvention ist ein Pauschalpreis für die Tatsache der Teilnahme, nicht ein zum Konsumvolumen proportionaler Preis.

Bei Qubic wird das auf die Verteilung der Emission angewandt. Alle 676 Computoren bekommen einen vergleichbaren Anteil der Billion – solange sie aktiv bleiben und über der Schwelle liegen. Es gibt keine starke Korrelation zwischen der Anzahl zusätzlicher über die Quorumsschwelle hinaus gefundener Digests eines Computors und der Höhe seines Erhalts. Über der Schwelle – man bekommt sein IPC × (Koeffizienten). Unter der Schwelle – man riskiert, in der 225er-Rotation herauszufallen und alles zu verlieren. Innerhalb der aktiven Zone – Subvention.

Warum so. Es ist keine Geste der Großzügigkeit. Es ist ein Mechanismus zur Verhinderung von Kartellbildung. Würde die Emission proportional verteilt, wie bei Bitcoin proportional zur Hashrate, wo mehr Hashrate einen größeren Anteil der Belohnung gibt – würde Qubic sofort denselben industriellen Skalierungskreislauf einschalten, der Bitcoin-Mining von einer Million privater Geräte zu drei oder vier großen Pools machte. Großes Kapital fließt in spezialisierte Hardware; spezialisierte Hardware schlägt handelsübliche Hardware; Skaleneffekte drängen die kleinen Akteure heraus; die Konzentration wächst. Mit Subvention schaltet sich dieser Kreislauf nicht ein. Hardware in Qubic auf industrielles Niveau zu skalieren ist sinnlos – es gibt keine proportionale Belohnung. Es genügt, ein „guter" Computor zu sein, um seinen Anteil zu bekommen; der „beste" zu sein, verschafft keinen unverhältnismäßigen Bonus.

Es gibt hier eine direkte Verbindung zu Kapitel 3. Axelrods vierte Bedingung: Ein Sieg im Spiel darf nicht in unverhältnismäßigen Einfluss umwandelbar sein. Übersetzt in den Raum der Ökonomie bedeutet das: Er darf nicht in einen unverhältnismäßigen Anteil an der Emission umwandelbar sein. Subvention erfüllt genau diese Funktion auf der Verteilungsebene.

Eine Einschränkung im Kleingedruckten, damit das Bild genau bleibt. Subvention in Qubic ist nicht absolut. Dieselbe oben angegebene Einnahmenformel V2 ist nicht flach. In der multiplikativen Komponente M bekommt ein Computor, der TX-Relay schlecht handhabt oder Orakel sabotiert, weniger. Ein Computor, der aktiv externes Mining betreibt, bekommt über den additiven Term einen Bonus von +20 %. Aber diese „Korridore" sind schmal. Innerhalb von ihnen – flache Subvention; zwischen ihnen ist der Unterschied nicht „das Hundertfache", sondern „zwanzig Prozent".

Und eine letzte wichtige Eigenschaft dieses Einatmens. Niemand besitzt die Billion QU persönlich, die jeden Mittwoch ins Netzwerk eintritt. Es gibt keine „Team-Zuteilung", keine „vestenden Token", keine Gründerkasse. Die Billion wird über IPC gemäß der Aktivität dieser Woche verteilt – hat man es unter die 676 geschafft, seine Arbeit gut gemacht, bekommt man seinen Anteil. Nächste Woche – von vorn, keine angehäuften Privilegien. Wer es nicht unter die 676 geschafft hat, bekam nichts. Wer es schaffte,

bekam ungefähr dasselbe wie alle anderen.

Das ist das eine Einatmen. Aber IPC ist nur der Moment des Einatmens. Über die gesamte Woche bis zum nächsten Mittwoch läuft das Ausatmen, und es hat mehrere gleichzeitige Richtungen.

Ausatmen: sieben Wege, QU zu verbrennen

Wenn die Emission ein Mechanismus ist, eine Billion pro Woche, starr durch das Protokoll definiert, ist das Verbrennen anders strukturiert. Verbrennen sind sieben parallele Pfade, jeder mit eigenem Zweck, eigener ökonomischer Funktion, eigenem Grad an Vorhersehbarkeit. Im Folgenden – ein kurzer Punkt pro Pfad.

Pfad eins. Computor-Abstimmung. Jede Epoche stimmen die 676 Computoren über Verbrennungsraten-Parameter ab – wie viel des umlaufenden Angebots bis Ende der Epoche verbrannt werden soll. Das ist die Basis-Deflation, das konstante Hintergrund-Ausatmen. Der Schöpfer des Systems formulierte die Logik in einer sehr frühen Veröffentlichung vom 8. Januar 2022 unverblümt:

„Wenn Computoren die Verbrennungsrate erhöhen, machen sie die QUs von jedem mehr wert."

Der Satz ist einfach und frei von Euphemismus. Verbrennen ist eine Umverteilung von Wert von der Emission zu bestehenden Haltern. Keine „ökologische Maßnahme" und keine „Wohltätigkeit" – ein ökonomischer Mechanismus, in dem Computoren entscheiden, wie viel neue Emission das Netzwerk im Umlauf belässt und wie viel es entzieht. Die Entscheidung wird jede Woche neu getroffen und kann jede Woche anders ausfallen.

Pfad zwei. Smart-Contract-Gebühren. Alle QU, die Nutzer ausgeben, um Smart Contracts auf Qubic auszuführen, werden verbrannt. Sie gehen nicht an Computoren, werden nicht in einer Kasse beiseitegelegt – sie gehen auf null. Ein Zitat vom 14. Oktober 2021, vor dem Mainnet-Start:

„Alle für den Betrieb von Smart Contracts ausgegebenen QUs werden verbrannt."

Das ist ein struktureller Unterschied zu Ethereum. Bei Ethereum gehen Gas-Gebühren (nach EIP-1559, mit verbrannter Basisgebühr, aber dem Tip – nicht) teilweise an Validatoren; bei Qubic vollständig ins Verbrennen.

Pfad drei. IPO-Gebot-Verbrennungen. Wenn ein neuer Smart Contract ins Netzwerk kommt, durchläuft er ein IPO-Verfahren – Computoren bieten für Anteile am künftigen Contract. Die Gebote entziehen QU temporär dem Umlauf. CfBs Formulierung vom 5. Juli 2023:

„CONTRACT_IPO_BID-Transaktionen werden die Gesamtmenge verändern (weil Gebotsbeträge daraus ‚extrahiert' werden), am Ende der Epoche sollten alle Gebote freigegeben werden und die anfängliche Gesamtmenge wiederherstellen."

Am Ende der Epoche kehrt der Großteil der Gebote zu den Bietern zurück – aber manche (gescheiterte Gebote unterhalb des Quorum-Medians) werden verbrannt. IPO ist eine temporäre Verbrennung mit teilweisem dauerhaftem Rückstand.

Pfad vier. Senden an die AAAA…-Adresse. Eine Adresse, die vollständig aus A besteht, ist funktional gleichbedeutend mit einer Verbrennung. QU, die dorthin gesendet werden, werden nie wieder

zurückgeholt – niemand besitzt den entsprechenden privaten Schlüssel, denn die Adresse wurde nicht aus einem Schlüssel generiert. Das ist ein öffentlicher, offen zugänglicher Verbrennungsmechanismus – will ein Halter freiwillig das Angebot verringern, muss er nur QU an AAAA senden. Eine kleine kulturelle Fußnote: 2022, in den ersten Monaten nach dem Start, wurden solche Überweisungen als öffentliche Geste vorgenommen, um Engagement für das „atmende" Modell zu demonstrieren.

Pfad fünf. Verwirkte Computor-Belohnungen. Leistet ein Computor schlecht, ist offline oder erreicht das Quorum nicht – verwandeln sich seine verwirkten QU nicht in „herrenlose Gelder". Sie gehen entweder ins Verbrennen oder in den Admin-Fonds – die Entscheidung wird jede Epoche per Abstimmung getroffen. CfB sprach Ende Mai 2024 darüber:

„Mehr Geld an Admin ist nicht unbedingt gut, meine vergangene Erfahrung mit der IOTA Foundation war in dieser Hinsicht ziemlich negativ (aber wertvoll), und ich kann nicht garantieren, dass diese QUs für etwas Gutes für die Community ausgegeben werden."

Eine kurze Einschränkung. Die Erwähnung der IOTA Foundation ist hier keine Analogie des Autors und keine Spekulation; es ist CfBs eigene Erklärung, warum er zu Verbrennen statt Admin tendiert.

Pfad sechs. KI-Operationen. Wenn Aigarth Operationen auf dem Netzwerk ausführt, verbrennen diese Operationen QU. Am 17. April 2024 brachte CfB es in einem kurzen Satz auf den Punkt:

„KI-Betrieb auf Qubic wird ebenfalls Angebot verbrennen."

Im April 2026, zum Zeitpunkt, an dem dieses Kapitel geschrieben wird, ist dieser Pfad vom Volumen her größtenteils symbolisch. Aigarth läuft noch nicht mit voller Kapazität – Kapitel 8 ging ausführlich darauf ein, warum. Aber architektonisch ist der Pfad angelegt. Bis 2027, sollte das geplante Deployment durchgehen, könnte er bedeutend werden. Vollständige Offenlegung zu Aigarth – in Kapitel 15 des Buches; hier zählt die Tatsache, dass KI-Operationen als Verbraucher von Angebot vorgesehen sind.

Pfad sieben. Buyback über externes Mining. Der „physischste" Pfad – und strukturell der interessanteste. Ab Phase 3 schürfen Computoren optional DOGE. Der geschürfte DOGE läuft über Pool-Betreiber, wird am Markt verkauft, der Erlös fließt in den Kauf von QU an offenen Börsen, und das gekaufte QU wird verbrannt. Der volle Kreislauf: Rechenleistung → externe Coin → Fiat/Stable → QU → Verbrennen.

Die zwanzig Prozent Einnahme, die ein Computor für externes Mining verdient (über den additiven B·E-Term in der Einnahmenformel V2), sind der ökonomische Treibstoff für den Buyback. Je mehr Computoren am Mining teilnehmen, desto mehr externe Einnahmen haben die Pools, desto mehr QU kann zurückgekauft und verbrannt werden.

Kritische Ehrlichkeit. Buyback ist nicht garantiert. Es ist eine Option für Computoren, kein Teil des Protokolls. In Kapitel 8 zitierte ich bereits die Empirie: Etwa 20 von 676 Computoren betreiben überhaupt kein externes Mining, und das Netzwerk läuft damit gut. Würden morgen alle 676 gleichzeitig beschließen, das Mining einzustellen – würde das Netzwerk als Blockchain weiterfunktionieren, die Emission liefe normal weiter, UPoW würde weiter Konsens produzieren, aber der Buyback würde stoppen. Die saubere Deflation, die das Netzwerk 2025–2026 zeigte, würde aufhören zu existieren. Das ist kein Bug und keine Schwachstelle – es ist Design. Buyback ist eine Variable, keine Konstante.

Auf dem Weg zur Synthese. Ab 2025 verbrennt das Qubic-Netzwerk regelmäßig 100 % oder mehr der Epochen-Emission. Das ist eine wichtige empirische Tatsache, die der Schöpfer des Systems mehr als

einmal kommentiert hat. Am 11. Oktober 2025:

„Monero hält sich ziemlich gut, diese Epoche haben wir die Chance, 100 % der emittierten Menge zu verbrennen."

Und vier Tage später, am 15. Oktober 2025:

„Qubic ist so konzipiert, dass 100 % der emittierten Menge jede Epoche verkauft wird."

Das erste Zitat handelt von einer konkreten Chance in einer konkreten Epoche. Das zweite vom Design des Systems als Ganzem. Zusammen ergeben sie eine Formulierung, die es sich zu merken lohnt: Bei ausreichender externer Rendite über den Buyback-Pfad ist das Netzwerk in der Lage, die gesamte Wochen-Emission plus einen Teil des angesammelten Angebots zu verbrennen. Netto-Deflation wird zu einer beobachtbaren Eigenschaft.

Aber es ist kein Gesetz. Es ist eine Möglichkeit, die sich unter bestimmten Bedingungen einschaltet. Wenn der externe Markt großzügig ist – wenn der DOGE-Preis hoch ist, wenn die Schwierigkeit im richtigen Bereich liegt, wenn die Pools effizient sind – ist das Ausatmen stark, und die Bilanz wird negativ. Wenn der Markt geizig ist – ist das Ausatmen schwächer, und die Bilanz kann positiv ausfallen. Das bringt uns zurück zum Thema Inflation. Am 13. Dezember 2025 sagte CfB einen kurzen Satz, der leicht zu zitieren und leicht misszuverstehen ist:

„Die jährliche Inflation beträgt 15 %."

Und gleich danach, in derselben Diskussion, zum Vergleich:

„5 % ist die weltweite jährliche Inflation."

Das muss sorgfältig gelesen werden. 15 % ist die brutto-nominale Inflation. Das ist, was das Netzwerk pro Jahr zum Angebot hinzufügt, wenn es überhaupt keine Verbrennungen gäbe. Zum Vergleich – die Fiat-Inflation weltweit liegt bei etwa 5 %. Die 15-Prozent-Zahl klingt alarmierend, bis man sie neben die tatsächliche Nettodynamik stellt: Mit funktionierenden Verbrennungspfaden befand sich das Netzwerk regelmäßig in Netto-Deflation. Aber man sollte auch nicht „Qubic ist deflationär" als allgemeine Charakterisierung sagen – das stimmt nicht. Die genaue Formulierung: Brutto-Inflation 15 % pro Jahr, netto – variabel, je nach Woche.

Wir haben das Einatmen beschrieben. Wir haben die sieben Ausatmen-Pfade beschrieben. Aber – wer entscheidet, wie das Netzwerk in einer gegebenen Woche atmet?

Wer entscheidet, wie es atmet

Eine Frage, oberflächlich einfach, bei näherer Betrachtung komplex. Wenn die sieben Verbrennungspfade so unterschiedlich angeordnet sind – manche automatisch (SC-Gebühren, IPO), manche freiwillig (Senden an AAAA), manche von externer Ökonomie abhängig (Buyback) –, wer trifft dann letztlich die Entscheidung darüber, wie das Netzwerk in einer gegebenen Epoche ausatmet?

Die Antwort: 676 Computoren.

Jeden Mittwoch, beim Epochenübergang, stimmen die Computoren über Verbrennungsraten-Parameter ab. Das ist keine einmalige Entscheidung, die einmal getroffen und eingefroren wird. Es ist eine

fortlaufende Entscheidung, jede Woche neu getroffen. Alles, was mit dem Angebot zu tun hat, lebt in dieser Abstimmung: wie viel aus dem Umlauf verbrannt wird, wie mit verwirkten Computor-Belohnungen umzugehen ist (verbrennen oder Admin-Fonds), welche die Parameter für die nächste Epoche sein sollen.

Diese Formulierung ist die zentrale Idee des Kapitels, und im nächsten Abschnitt entfalte ich sie durch ein direktes Zitat des Systemschöpfers. Hier – ihre Konsequenz, die Auswirkungen auf die gesamte Architektur hat.

Die Angebots-Abstimmung ist an den Computor-Status gebunden, nicht an QU-Bestände.

Das ist die Einlösung von Axelrods vierter Bedingung, bisher nur teilweise ausgespielt: durch gleiches Stimmgewicht und durch eine Rotation, die angehäufte Bestände nicht in die Geschwindigkeit des Ein- und Austritts umwandelt. Hier schließt sie sich – strukturell und endgültig.

Ein QU-Halter mag einen, tausend oder eine Billion Token besitzen. Das gibt ihm keine Stimme über Angebotsparameter. Null Stimmen. Um eine Stimme zu bekommen, muss man Computor sein – und um Computor zu sein, muss man UPoW leisten und unter den top 676 nach Score bleiben. Die Stimme wird durch Arbeit verdient, nicht durch Kapital.

Und zweitens: Die Stimme eines Computors ist eine von 676, nicht proportional zu irgendetwas. Ein Computor, der 30 % mehr gültige Digests als ein anderer produziert hat, stimmt gleich – eine Stimme. Ein Computor, der mehr QU besitzt (falls er überhaupt QU über einen Arbeitsbestand hinaus hält) – stimmt eine Stimme. Strukturell reduziert sich das Ganze auf das Prinzip „ein Computor – eine Stimme“.

Eine Konsequenz für das Ökosystem: Wer durch Kurssteigerungen reicher wurde, wurde nicht einflussreicher. Zehn Prozent des Angebots in der Tasche – null Stimmen zur Tokenomik. Das ist das Gegenteil dessen, was in einer typischen Proof-of-Stake-Blockchain geschieht, wo steigender Einsatz das Stimmgewicht erhöht – und dadurch eine direkte Verbindung zwischen wirtschaftlichem Gewinn und dem Recht, die Regeln zu ändern, schafft. Bei Qubic ist diese Verbindung auf architektonischer Ebene durchtrennt. Nicht durch Gesellschaftsvertrag – durch Code.

Zweite Konsequenz: Es gibt keinen Gründer mit einer Kasse. CfB hat kein privilegiertes Angebot. Es gibt keine vestenden Team-Token, die in drei Jahren freigeschaltet werden und den Markt zum Absturz bringen. Es gibt keinen Dev-Fonds von einer Million QU, über den vierteljährlich abgestimmt wird. Die Emission beträgt 1 Billion pro Epoche, persönlich niemandem als „Zuteilung“ gehörend; sie wird über IPC gemäß der Aktivität dieser Woche verteilt, und wenn die Daten des Netzwerks für diese Woche die Billion niemandem Bestimmtem zuweisen – verbrennt sie in Rotationsbilanzen. Emission funktioniert nach Pro-Kopf-Aktivität, nicht nach Pro-Kopf-Geschichte.

Nun – die einzige Erwähnung des Arbitrators in diesem Kapitel. Sie ist kurz und vorausschauend.

In Qubics Architektur gibt es ein Element, das über die Abstimmung der 676 hinausgeht. Der Arbitrator – eine Figur mit kryptografischer Signatur, fähig, in bestimmten Fällen in den Betrieb des Netzwerks einzugreifen. Diese Rolle arbeite ich in Kapitel 10 vollständig durch, das „Der Arbitrator — ein Monarch auf Zeit“ heißt. Hier genügt eine Tatsache, die direkt mit der Tokenomik zu tun hat. Am 13. Juli 2025 schrieb CfB:

„Der Arbitrator würde die IDs jener Computoren enteignen, die für ein Angebot größer als 200 Billionen gestimmt haben."

Die Mechanik: Jeder Computor kann einen kryptografischen Beweis vorlegen, dass das Angebot die Schwelle von 200 Billionen überschritten hat – und die Computoren, die für die Ausweitung stimmten, verlieren ihre IDs. Das ist keine positive Kontrolle (der Arbitrator kann das Angebot nicht festlegen) und kein Mechanismus zur Steuerung der Emission. Es ist Schutz gegen ein spezifisches pathologisches Ergebnis: eine hyperinflationäre Abstimmung. Sollte es je geschehen, dass 451 Computoren für ein Angebot größer als 200 Billionen stimmen – greift der Selbstregulierungsmechanismus.

Warum genau 200 Billionen – eine Frage für Abschnitt 5. Warum der Arbitrator – für Kapitel 10.

Eine dritte Konsequenz der Abstimmung: Atmung befindet sich nicht in einem stabilen Gleichgewicht. In einer Woche mag das Netzwerk mehr verbrennen, als es emittiert hat. In einer anderen – weniger. In einer dritten – eine Notabstimmung einberufen und die Parameter ändern. Das ist kein Design-Bug, es ist eine bewusste Eigenschaft.

Zum Zeitpunkt, an dem dieses Kapitel geschrieben wird, läuft in der Qubic-Community eine aktive Diskussion über eine mögliche radikale Lösung. Der Vorschlag, geäußert von CfB in einem öffentlichen Gespräch am 20. März 2026:

„Wir können, aber warum halbe Maßnahmen? Ich schlage vor, das Maximalangebot auf 10 % des aktuellen Angebots zu setzen, sodass der Preis auf das Zehnfache springt. Behaltet 10 % für diejenigen, die am längsten gehalten haben."

Das ist keine Entscheidung, es ist ein Vorschlag. Die Idee ist ein Reverse Split, eine großangelegte Verbrennung, die das Angebot um eine Größenordnung reduzieren und langfristige Halter belohnen würde. Die Diskussion ist offen. Während ich diese Zeilen schreibe, wurde keine Abstimmung abgehalten, das Ergebnis ist unbekannt.

Ehrlich: Ich weiß nicht, wie diese Diskussion enden wird. Möglicherweise wird die Entscheidung getroffen, bevor das Buch den Leser erreicht. Möglicherweise hat sich der Kontext bis zur Veröffentlichung verschoben.

Um quantitativ zu verstehen, was all das bedeutet, müssen wir uns konkrete Zahlen ansehen.

Arithmetik: was „Atmung" in Zahlen bedeutet

Dieser Abschnitt ist für den Leser, der mit Formeln überprüfen möchte, was oben in Worten beschrieben wurde.

Beginnen wir damit, wie einfach Qubics Buchhaltung für Verbrennungen tatsächlich ist. Am 17. Juli 2024 veröffentlichte CfB sie in einer Zeile:

„Epoche * 1 Billion – Angebot = verbrannter Betrag."

Absolute Einfachheit. Nehmen Sie die aktuelle Epochennummer, multiplizieren Sie mit einer Billion, ziehen Sie das umlaufende Angebot ab – Sie erhalten den kumulierten verbrannten Betrag über die gesamte Geschichte des Netzwerks. Keine versteckten Konten, keine Off-Chain-Überweisungen, keine

komplexen Formeln – Arithmetik, die jeder Nutzer mit einem Taschenrechner und Zugang zum Explorer durchführen kann.

CfB selbst führte diese Berechnung öffentlich am 13. Juli 2024 für Epoche 104 durch:

„Multipliziere die aktuelle Epochennummer mit 1 Billion und ziehe das umlaufende Angebot ab: 104.929.098.116.420 $QUBIC.“

Rechnen wir: 104 × 1 Billion = 104 Billionen. Das umlaufende Angebot lag damals bei etwa 103,9 Billionen – das heißt, der verbrannte Betrag kam auf etwas weniger als eine Billion. Zu diesem Zeitpunkt hatte das Netzwerk über 104 Epochen 104 Billionen emittiert und etwa eine Billion verbrannt – minimale Verbrennungen, die überwältigende Mehrheit der Emission noch im Umlauf.

In den folgenden 18 Monaten änderte sich das Bild. Es folgt eine Tabelle von Angebotsmarken, an denen sich das „Atmen“ vom Start bis zum Moment des Schreibens nachverfolgen lässt.

Drei Punkte auf dieser Trajektorie – 2021, 2024, 2025 – entsprechen drei Regimen. Bis Mitte 2024 verbrannte das Netzwerk kaum etwas; ab Mitte 2024, mit der Erweiterung der Funktionalität, setzten Verbrennungen ein; ab 2025, mit externem Mining als Buyback-Pfad, übertrafen die Verbrennungen die Emission.

Nun – zu den Obergrenzen. In Angebotsdiskussionen bei Qubic tauchen oft drei verschiedene Zahlen auf, und es ist wichtig, sie nicht zu verwechseln. CfB drückte es am 19. April 2024 so aus:

„Die Obergrenze liegt bei 1000 Billionen, 100 Billionen ist das erwartete Angebot, bei dem wir uns letztlich wegen der Verbrennungen einpendeln werden.“

Und aus dem in Abschnitt 4 bereits gegebenen Zitat ist die dritte Grenze bekannt – 200 Billionen, die Auslöseschwelle des Arbitrators. Wir erhalten also Folgendes:

1000 Billionen — harte Obergrenze. Die starre Protokollgrenze, im Code verankert. Sollte sich das Netzwerk dieser Zahl irgendwie nähern – bedeutet das bereits einen pathologischen Zustand.

200 Billionen — Eingriffsschwelle. Die „rote Linie“, jenseits derer die Selbstregulierung einsetzt: Computoren, die für eine Ausweitung darüber hinaus stimmten, verlieren ihre IDs.

~100 Billionen — erwartete Einpendelung. Der erwartete Stabilisierungspunkt des Angebots bei funktionierenden Verbrennungsmechanismen. Keine Garantie, eine Modellerwartung von CfB.

Drei Ebenen – drei verschiedene Funktionen. Harte Obergrenze – prinzipiell unmöglich. Schwelle – Schutz vor einer bestimmten Abweichung. Erwartete Einpendelung – wo das Netzwerk unter normalem Betrieb landen sollte.

Zurück zu den 15 % Inflation. Ich sagte bereits in Abschnitt 3, dass das brutto ist, nicht netto. Lassen Sie mich die quantitative Grundlage hinzufügen. 52 Billionen QU pro Jahr Brutto-Emission ist das, was das Netzwerk mit harter 1-Billion-pro-Woche-Emission zum Angebot hinzufügt. Die 15-Prozent-Zahl ist das Verhältnis dieses Bruttowerts zu der Basis, die das Netzwerk bis 2025–2026 erreichte. Bei laufenden Verbrennungen kann netto alles sein – positiv bei schwachem externem Markt, negativ bei aktivem.

Ein letztes arithmetisches Detail – und es hat Auswirkung auf die Marktsensitivität gegenüber Verbrennungen. Am 19. Juli 2023 stellte CfB eine Beobachtung fest, die häufig zitiert wird:

„Wir verbrennen das Angebot kurzfristiger Halter, das Angebot langfristiger beeinflusst den Preis nicht. 15 % weniger QUs sind 50 % weniger handelbare QUs."

Eine Übersetzung und Aufschlüsselung. Verbrennungen entziehen im Durchschnitt Angebot aus den Händen derjenigen, die aktiv handeln – kurzfristige Halter. Langfristige Halter behalten QU in ihren Wallets und nehmen nicht am Handel teil. Ihr Angebot existiert formal, ist aber nicht am Markt. Wenn das Netzwerk 15 % des Gesamtangebots verbrennt – kann das im handelbaren Pool eine Reduktion von 50 % bedeuten, weil das Verbrannte aktives umlaufendes Kapital ist, nicht „eingefrorene" Bestände.

Das ist eine analytische Beobachtung, kein Versprechen. Sie erklärt strukturell, warum die Preissensitivität gegenüber Verbrennungen unverhältnismäßig groß sein kann: Verbrennungen treffen den lebendigen Markt, nicht den erstarrten Bestandspool. Das ist keine Manipulation und keine Verteidigungsthese – es ist eine Folge davon, wie das Angebot in einem jungen Netzwerk zwischen aktiven und passiven Haltern verteilt ist.

Eine Einschränkung zu den Daten in diesem Abschnitt. Live-Statistiken – Marktkapitalisierung, Halterverteilung, Börsenlistings – sind Momentaufnahmen, die sich bis zur Lektüre des Buches geändert haben werden. Ich gebe im Kapitel bewusst strukturelle Zahlen (IPC, 1 Billion, 200/1000/~100 Billionen, 15 %) statt Live-Zahlen an. Für Live-Metriken – der Qubic-Explorer, On-Chain-Snapshots zu einer bestimmten Epoche. Solche Links finden sich im Anhang.

Ich habe die Zahlen dargelegt. Nun – ein kurzer Abschnitt zur Philosophie, ohne die diese Zahlen bloß technisch bleiben.

Philosophie: Satoshi vs. Quorum

Zwei Welten.

2008, als der anonyme Autor von Bitcoin beim Schreiben des Whitepapers einundzwanzig Millionen Coins als harte Obergrenze wählte, traf er eine Entscheidung für jeden, der später in die Bitcoin-Ökonomie eintreten würde. Diese Entscheidung ist kein per Abstimmung regulierter Parameter; sie ist kein Pull Request, über den man diskutieren kann; sie ist keine Politik, die bei der nächsten Wahl geändert werden kann. Sie ist ein im Quellcode und in der Wurzelkopie der Kette festgeschriebenes Gesetz. Jeder Versuch, sie zu ändern, bedeutet einen Hard Fork, der ein neues Netzwerk mit einer neuen Coin erzeugt. Das tatsächliche Angebot von Bitcoin ist die Entscheidung einer Person, für immer eingefroren.

Das ist keine Kritik. Die Festlegung des Angebots ist Teil dessen, was ein Bitcoin-Halter kauft, wenn er Bitcoin kauft. Der Preis dieser Entscheidung wurde bezahlt: Unmöglichkeit der Anpassung. Der Nutzen ist absolute Vorhersehbarkeit. Jeder neue Teilnehmer bei Bitcoin tritt in ein Spiel ein, dessen Regeln über die Geldmenge nicht geändert werden können, selbst wenn die Änderungen objektiv nützlich wären.

2023 – am 25. Dezember, eine kurze Nachricht – formulierte der Schöpfer von Qubic den entgegengesetzten Ansatz. Dieses Zitat ist das zentrale Zitat des Kapitels. Es muss langsam gelesen werden, in Stücken:

„Ich weiß nicht, wie es sein wird, das Quorum entscheidet. Satoshi hat das Angebot in Stein gemeißelt – ich wählte eine dezentralere Methode. Wir erwarten eine flache Linie der Gesamtmenge."

Vier Sätze, jeder mit Gewicht.

„Ich weiß nicht, wie es sein wird" – der Schöpfer des Systems legt das Ergebnis explizit nicht fest. Das ist das direkte Gegenteil von Satoshi, der es festlegte. Nicht „es werden in fünf Jahren 100 Billionen sein, ich verspreche es" – „ich weiß es nicht".

„Das Quorum entscheidet" – der aktuelle Konsens entscheidet. Kein Dokument, keine Formel, nicht der Autor des Projekts. Die kollektive Abstimmung der 676, jede Woche, neu.

„Satoshi hat das Angebot in Stein gemeißelt – ich wählte eine dezentralere Methode" – das ist die direkte Formulierung, nicht meine Paraphrase. Zwei verschiedene Methoden werden benannt: Einfrieren („in Stein") und eine dezentralere Methode (fortlaufender Konsens). Was genau „dezentraler" hier bedeutet – arbeite ich unten durch.

„Wir erwarten eine flache Linie der Gesamtmenge" – kein Versprechen, kein Ziel – eine Erwartung. Verläuft die tatsächliche Dynamik anders, dann wird sie eben anders verlaufen.

Was bedeutet „dezentralere Methode"?

CfB hat ein spezifisches Verständnis von Dezentralisierung, nicht reduzierbar auf die Anzahl der Knoten oder geografische Verteilung (die zählen für sich, aber das ist eine andere Dimension). Dezentralisierung ist in seiner Formulierung eine Frage davon, wer die Regeln durch ein legitimes Verfahren ändern kann.

Bei Bitcoin können die Regeln über das Angebot nicht geändert werden. Selbst wenn 100 % der Bitcoin-Core-Entwickler zustimmen würden, die Obergrenze auf 22 Millionen zu erhöhen – das wäre ein Hard Fork, und die sozial-ökonomische Reaktion würde ihn als Nicht-Bitcoin ablehnen. Die Unveränderlichkeit des Angebots ist nicht nur eine technische Eigenschaft, sie ist eine soziale Übereinkunft, aufrechterhalten durch die Erwartung von Unveränderlichkeit. Und gerade diese Starrheit ist selbst eine Form der Zentralisierung: Die Regeln sind in der Entscheidung einer Person eingefroren, getroffen in der Vergangenheit für alle gegenwärtigen und zukünftigen Teilnehmer.

Bei Qubic sind die Regeln über das Angebot jede Epoche durch ein legitimes Verfahren anpassbar. 676 Computoren stimmen ab; die Abstimmung wird dokumentiert; jeder kann das Ergebnis überprüfen. Das bedeutet nicht, dass sich das Angebot chaotisch ändern wird – die Erwartung einer Einpendelung ist deutlich genug artikuliert –, aber es bedeutet, dass ein Mechanismus für Veränderung existiert und dem Netzwerk gehört, nicht seinem Gründer.

Der Unterschied: Im ersten Fall wird die Entscheidung einmal getroffen und eingefroren; im zweiten wird sie jede Woche neu getroffen.

Das Gegenargument, das ich zu geben verpflichtet bin, weil es stark ist. Eines der zentralen Wertversprechen von Bitcoin ist genau die Vorhersehbarkeit des Angebots. „Ich weiß, es werden immer 21 Millionen von uns sein" – diese Aussage lässt sich über Qubic nicht treffen. Das Quorum könnte theoretisch anders abstimmen. Bedeutet das, dass Qubics Tokenomik weniger vorhersehbar und dementsprechend weniger zuverlässig als Wertaufbewahrungsmittel ist?

Die Antwort lautet – teilweise ja, und CfB widerspricht dem nicht. Er trifft eine andere Wahl. In Kapitel 3 arbeiteten wir durch, dass Bitcoin seine eigenen Probleme nicht beheben kann – Proof-of-Work, Hashrate-Konzentration, Governance-Blockade – gerade weil es keinen Anpassungsmechanismus hat. Die Starrheit des Angebots ist keine Ausnahme von diesem Muster, sie ist ein besonderer Fall derselben Unflexibilität. Qubic akzeptiert den Tradeoff: den Verlust von „garantiertem Angebot“ im Austausch gegen die Fähigkeit des Netzwerks, auf äußere Bedingungen zu reagieren.

Welche Wahl besser ist – das ist eine Wertefrage. Es ist keine Technik und keine Mathematik; es ist eine Position. Die Position dieses Buches lautet: Der Tradeoff, den Qubic eingeht, macht seine Tokenomik lebendig. Bitcoin beantwortet die Frage „was ist Geld“ so: Geld ist die Unmöglichkeit von Emission über das Vereinbarte hinaus. Qubic beantwortet sie so: Geld ist Koordinationstreibstoff, der sich der Aktivität des Netzwerks anpasst.

Beide Antworten sind vertretbar. Beide haben ökonomisch kohärente Befürworter. Dieses Buch handelt von Qubic, und deshalb beschreibt es die zweite Antwort. Aber ich sage nicht, dass die erste falsch ist. Sie ist anders.

Eine kurze Vergleichstabelle, um die Unterschiede in ein Bild zu bringen:

Schließen wir diesen Abschnitt mit einem kurzen Satz. Die Frage ist nicht, welches System richtig ist. Die Frage ist, welche Antwort auf die ursprüngliche Frage nach der Natur des Geldes gewählt wird. Bitcoin wählte eine Antwort – und baute darauf die bestmögliche Umsetzung dieser Philosophie. Qubic wählte eine andere – und baut die bestmögliche Umsetzung dieser. Sie sind keine Feinde und keine Alternativen im ausschließenden Sinne. Es geht bei ihnen um unterschiedliche Dinge.

Atmung geschlossen, Arbitrator unbehandelt

Fassen wir das Kapitel zusammen.

Emission – eine Billion QU pro Woche, hart und unstrittig. Das ist das Einatmen des Netzwerks, seine fundamentale Eingabe. Verteilung – Subvention: Alle 676 Computoren bekommen einen vergleichbaren Anteil, innerhalb schmaler Korridore, ohne industrielle Skaleneffekte. Ausatmen – sieben Verbrennungspfade, von automatisch (SC-Gebühren) bis extern marktabhängig (Buyback über DOGE). 2025–2026 verbrannte das Netzwerk regelmäßig 100 % oder mehr der Epochen-Emission – saubere Deflation als beobachtbare Eigenschaft, wenn die Buyback-Pfade funktionieren.

Die Entscheidung, wie das Netzwerk in einer gegebenen Epoche atmet, treffen 676 Computoren – durch eine jeden Mittwoch aufgefrischte Abstimmung. Die Stimme gehört dem Computor, nicht dem QU-Halter. Das ist die strukturelle Einlösung von Axelrods vierter Bedingung, ausgespielt auf Ebene der Tokenomik: Das Spiel zu gewinnen (QU anzuhäufen) wandelt sich nicht in das Recht um, die Regeln des Spiels zu ändern (eine Stimme über das Angebot). Der Arbitrator ist eine gesonderte Figur, hier einmal als Rückfallebene gegen das pathologische 200-Billionen-Plus-Szenario erwähnt; vollständige Offenlegung im nächsten Kapitel.

Die Kontrolle über das Angebot lebt bei Qubic im aktuellen Konsens, nicht in einer vergangenen Entscheidung. Das ist die zentrale philosophische Wahl, gesetzt gegen das Bitcoin-Modell fester Angebotsmenge. „Satoshi hat das Angebot in Stein gemeißelt – ich wählte eine dezentralere Methode“,

erklärte der Schöpfer des Systems Ende 2023. Atmung hat kein stabiles Gleichgewicht; sie schwankt mit der Netzwerkaktivität, dem externen Markt, der Abstimmung der Computoren, Diskussionen in der Community. April 2026 ist die Zeit einer solchen Diskussion: über einen möglichen radikalen Reverse Split. Ihr Ausgang ist unentschieden.

Atmung ist ein lebendiger Prozess. Es gibt keine Stabilität darin. Das ist kein Bug, es ist eine Eigenschaft des Designs. Das Lebendige atmet; das Tote hat ein festes Lungenvolumen.

Kapitel 6 gab den Raum des Netzwerks: 676 Stimmen, strukturelle Form.

Kapitel 7 gab seine Zeit: wöchentliche Epochen, den Rhythmus der Übergänge.

Kapitel 8 gab seine Energie: UPoW, die Arbeit, die Konsens und begleitende Erzeugnisse produziert.

Kapitel 9 gab seine Ökonomie: Atmung, was zwischen Ein- und Ausatmen zirkuliert.

Vier Dimensionen beschrieben. Eine bleibt – die fünfte. Institution.

In der gesamten Architektur, die ich über die vergangenen vier Kapitel beschrieben habe – 676 Stimmen, wöchentliche Epochen, UPoW-Energie, atmendes Angebot – gibt es eine Figur, die eingreifen kann. Der Arbitrator. In diesem Kapitel erschien er zweimal – einmal als Rückfallebene gegen ein Angebot >200 Billionen, einmal als vorausweisender Verweis, für später aufgehoben. In beiden Fällen – in der Rolle einer Sicherung, nicht eines Herrschers. Aber wenn das Netzwerk so dezentral gebaut ist, wie ich es beschrieben habe – warum überhaupt eine Figur mit Vetorecht?

Und noch eine Frage. Wenn CfB für das Angebot eine „dezentralere Methode“ wählte, wenn er seit Jahren konsequent Entscheidungen an das Kollektiv übergibt und dies selbst als Prinzip erklärt hat – warum hat er sich diese eine Rolle vorbehalten?

Die Antwort steht im nächsten Kapitel. Der zweite Teil der Frage, der in diesem Kapitel noch nicht ausgesprochen wurde, steht dort ebenfalls.

Das nächste Kapitel handelt von demjenigen, dessen Signatur alles stoppen kann. Und davon, warum er versprach, diese Signatur zu zerstören.

10
Der Arbitrator — ein Monarch auf Zeit

Der Schlüssel im Quellcode

Am Ende des vorigen Kapitels schrieb ich, dass das nächste von demjenigen handeln würde, dessen Signatur alles stoppen kann. Und davon, warum er versprach, diese Signatur zu zerstören.

Die erste Sache braucht sofort eine Korrektur. „Alles stoppen“ ist eine rhetorische Figur aus dem vorigen Kapitel, und ich verwendete sie absichtlich, um Spannung aufzubauen. In Wirklichkeit kann der Arbitrator weit weniger, als das nahelegt. Er kann genau eine Sache tun. Aber diese eine Sache ist strukturell bedeutsam, weshalb sie ein eigenes Kapitel verdient.

Beginnen wir damit, was der Arbitrator physisch ist. Es ist eine Adresse. Ein kryptografischer öffentlicher Schlüssel, fest im Quellcode des Knotens verankert. Kein Laufzeitparameter, der während des Netzwerkbetriebs geändert werden kann. Kein Datenbankeintrag, kein Wert in einer Konfigurationsdatei, keine Variable, die jemand überschreiben kann. Es ist eine Kompilierzeit-Konstante – eine Zeile im Quellcode, die jeder Knotenbetreiber vor dem Kompilieren einträgt. Come-from-Beyond formuliert es direkt:

„Jeder Knotenbetreiber trägt sie vor der Kompilierung in den Quellcode der Node-Software ein. Sollte die Qubic-Community aus irgendeinem Grund einen anderen Arbitrator brauchen, müssen sie die andere Adresse eintragen. Dafür brauchen wir sozialen Konsens, ohne ihn gibt es Forks.“

Den Arbitrator zu ändern bedeutet: alle Knoten mit der neuen Adresse neu kompilieren; die Neukompilierung erfordert sozialen Konsens unter den Knotenbetreibern; ohne Konsens spaltet sich das Netzwerk. Architektonisch macht das den Arbitrator zu etwas zwischen einer Person und einem Artefakt – eine bekannte Adresse, repliziert als Konstante in Tausenden unabhängig kompilierten Binärdateien.

Wer der Arbitrator gerade jetzt ist, ist eine öffentlich bekannte Tatsache. Die Rolle wird von Come-from-Beyond selbst gehalten. Das ist der Teil, der dazu verleitet, das Gespräch in Richtung „siehst du, eine Person mit einem Schlüssel“ zu verschieben. Das werde ich in diesem Kapitel nicht tun. Wichtig ist hier nicht, wer, sondern was – die Struktur der Rolle. Wer sie zu einem gegebenen Zeitpunkt innehat, ist eine vorübergehende Frage; was ihre Befugnisse sind und was ihre Grenzen sind, ist eine architektonische. Darum geht es im gesamten Kapitel.

Zwei Spannungen wird das Kapitel durcharbeiten.

Erstens. Der Arbitrator ist der einzige konzentrierte Punkt in dem Netzwerk, wie ich es beschrieben habe. Ein Single Point of Failure im buchstäblichen Sinne: eine Adresse, eine Signatur, eine Person mit einem privaten Schlüssel. Wie passt das zu einem verteilten Protokoll, das die vier vorigen Kapitel als kollektiv

aufgebaut haben?

Zweitens. Der Schöpfer des Systems sagt öffentlich, dass es in der besten Version den Arbitrator gar nicht geben sollte. Und er hat dieser besten Version ein konkretes Datum zugewiesen.

Das erste wird in den Abschnitten 2 bis 5 durchgearbeitet. Das zweite – in Abschnitt 6.

Der Gesamtplan des Kapitels sind drei Fragen. Was kann der Arbitrator tun? Was kann der Arbitrator nicht tun, und warum ist das durch den Quellcode garantiert statt durch ein Versprechen? Warum existiert diese Rolle überhaupt, und wann wird sie verschwinden?

Eine ehrliche Randbemerkung, bevor ich beginne. Der Arbitrator ist tatsächlich ein zentralisiertes Element in einer dezentralen Architektur.

Und wir beginnen mit dem, was der Arbitrator tun kann.

Was der Arbitrator tun kann: eine Funktion

Der Arbitrator kann eine Sache tun. Die Computor-Liste ausstellen. Das ist alles.

Was das operativ bedeutet. Zur Erinnerung an die Computor-Rotation: Am Ende jeder Epoche kommen 225 neue Teilnehmer, um das unterste Quartil der vorigen zu ersetzen, und 451 machen weiter. Die neue Zusammensetzung wird durch die Signatur des Arbitrators festgelegt – sein kryptografisches „Ja, diese Liste von 676 öffentlichen Schlüsseln ist gültig“. Ohne diese Signatur akzeptieren Knoten die neue Zusammensetzung für die nächste Epoche nicht; das Netzwerk hielte an der Grenze des Übergangs an.

Dann kommt die Schlüsselfrage, die an dieser Stelle naheliegt. Wer entscheidet also tatsächlich, wer in die Liste kommt?

Nicht der Arbitrator.

Für die gesamte Epoche lassen Computoren ihren Score über UPoW laufen – die nützliche Rechenarbeit, die Kapitel 8 als Quelle von Konsens, KI-Trainingsdaten und Ranking gleichzeitig beschrieb. Score sammelt sich automatisch an, wird von anderen Computoren verifiziert und in der Blockchain verzeichnet. Am Ende der Epoche ergibt der Score eine Rangliste; das unterste Quartil geht; Ersatzkandidaten werden aus einer nach demselben Score sortierten Warteschlange genommen. Die Liste derer, die in die nächsten 676 gelangen, wird nicht von einer Person geformt und nicht vom Arbitrator – sie wird von der eigenen Arbeit des Netzwerks geformt, angesammelt über den sechsten, fünften und vierten Tag der Woche.

Der Arbitrator signiert nur das Ergebnis dieses Verfahrens.

Seine Funktion hier ist also notariell. Er bezeugt, dass das Verfahren stattfand und dass die ihm vorgelegte Liste tatsächlich dem entspricht, was das Netzwerk selbst berechnet hat. Er ist kein Wähler. Er ist kein Richter. Er ist der Standesbeamte eines Akts – eine Person mit einem Stempel, hergestellt, nachdem die Entscheidung bereits von anderen getroffen wurde.

Die naheliegende Frage bleibt: Wenn das Netzwerk bereits alles selbst berechnet hat – warum wird seine Signatur überhaupt gebraucht?

Die kurze Antwort ist, dass nicht alle Knoten im Netzwerk Zugang zu derselben Geschichte haben wie bereits bestehende. Wenn sich ein frischer Knoten zum ersten Mal mit dem Netzwerk verbindet, hat er keine Blockchain-Geschichte, keine Score-Tabellen, keine Daten, aus denen er die aktuelle Computor-Liste rekonstruieren könnte. Er verbindet sich mit einer Welt, in der er sich noch synchronisieren muss, und sich synchronisieren bedeutet, Daten von anderen Knoten zu empfangen, die alles Mögliche sein können. Ein neuer Knoten braucht einen Vertrauensanker, eine Signatur, die er im Voraus kennt und der er bedingungslos vertrauen kann. Dieser Anker ist der Arbitrator. Ich komme im Abschnitt zum Bootstrap darauf ausführlicher zurück.

Es gibt eine weitere lokale Funktion, die eine gesonderte Erwähnung verdient, weil der Schöpfer des Systems selbst offen darauf hinweist, dass sie temporär ist. Come-from-Beyond schreibt:

„Nicht alle Features sind bereits implementiert, z. B. wenn das Netzwerk wegen eines wöchentlichen Updates gestoppt ist, ist die Liste des Arbitrators nötig, um das Ticken wieder anzustoßen, das danach nicht mehr gestoppt werden kann. Dieses Feature wird nur während der Entwicklung gebraucht und kann leicht deaktiviert werden."

Auf Deutsch: Wenn das Netzwerk wegen eines wöchentlichen Knoten-Updates gestoppt hat und neu gestartet werden muss, hilft die Liste des Arbitrators, das Ticken wieder aufzunehmen. Aber das ist keine dauerhafte Funktion des Protokolls. Es ist eine Entwicklungskrücke, ausdrücklich als leicht abschaltbar gekennzeichnet.

Eine weitere Frage stellt sich von selbst: Kann der Arbitrator eine falsche Liste ausstellen? Formal, ja. Er besitzt den privaten Schlüssel; nichts hindert ihn daran, zu signieren, was er will. Aber das Netzwerk ist für diesen Fall auf besondere Weise gebaut – es kann eine korrekte von einer inkorrekten Liste automatisch unterscheiden, ohne Beteiligung des Arbitrators. Mehr dazu in Abschnitt 5.

Und ein letzter Punkt. Der Arbitrator verletzt Axelrods vierte Bedingung nicht – die Unmöglichkeit, einen Sieg im Spiel in das Recht umzuwandeln, dessen Regeln zu ändern –, denn er wählt nicht, wer in die nächste Zusammensetzung kommt. Die Zusammensetzung wird durch den über UPoW verdienten Score bestimmt. Der Arbitrator signiert nur: Ausführer einer bereits getroffenen Entscheidung, nicht ihr Urheber.

Wir haben beschrieben, was der Arbitrator tun kann. Nun – wichtiger – was er nicht kann.

Was der Arbitrator nicht kann: Garantien des Quellcodes

„Der Arbitrator kann fast nichts, der Quellcode garantiert es."

Come-from-Beyond formulierte das im Sommer 2024, und es ist zentral für das Verständnis der Konstruktion. „Fast nichts" ist keine Bescheidenheit und keine PR. Es ist eine technische Beschreibung, überprüfbar im Quellcode.

Hier die Liste dessen, was der Arbitrator nicht kann.

Er kann die Emission nicht ändern. Der Parameter „eine Billion QU pro Woche" ist fest im Code, eine Protokollkonstante. Der Arbitrator hat keinen Zugriff auf diesen Parameter; keine seiner Signaturen wird Knoten dazu bringen, diese Woche mehr oder weniger QU zu emittieren.

Er kann die maximale Angebotsmenge nicht erhöhen. Come-from-Beyond schreibt in demselben Gespräch unverblümt:

„Der Arbitrator wird nicht erlauben, die maximale Angebotsmenge zu erhöhen, weil das gegen die Interessen der Nutzer wäre."

Mehr noch, der Arbitrator tut das Gegenteil – schützt vor einer Überschreitung der 200-Billionen-Obergrenze: Stimmt ein Computor für ein Angebot größer als 200 Billionen, entzieht der Arbitrator ihm die ID. Die Rolle ist hier die des Ausführers eines bereits nachgewiesenen Verstoßes, nicht die des Initiators von Änderungen.

Er kann Transaktionen nicht ändern. Er signiert sie nicht, validiert sie nicht. Transaktionen laufen über Computoren; der Arbitrator hat mit diesem Verfahren nichts zu tun.

Er kann Transaktionen nicht blockieren. Aus demselben Grund – er hat kein Instrument dafür. Das Netzwerk fragt ihn nicht, ob eine Transaktion durchgegangen ist.

Er kann Smart Contracts nicht beeinflussen. Die Ausführung von Contracts ist Sache der Computoren; die verbrannten Gebühren für ihre Arbeit gehen ohne Beteiligung des Arbitrators ins Verbrennen; IPOs, Brücken, Börsen, bedingtes Earn – all das geschieht auf einer Ebene, die der Arbitrator nicht sieht.

Er kann die Abstimmung der Computoren nicht überstimmen. Haben die 676 Teilnehmer für X gestimmt – ist das Ergebnis X. Der Arbitrator kann nicht sagen „aber ich habe Y beschlossen". Seine Signatur reicht dafür nicht, weil das Netzwerk diese Signatur in einem solchen Kontext gar nicht abfragt.

Er kann kein QU aus dem Nichts erschaffen. Der Arbitrator hat kein privilegiertes Guthaben. Kein spezielles Wallet. In seiner Rolle als Arbitrator hält er null QU. Emission läuft nur über Subvention an Computoren; der Arbitrator hat mit Subvention nichts zu tun.

Er kann niemandes Wallet einfrieren. Kann kein Guthaben konfiszieren. Mit einer Ausnahme – der Entfernung der Computor-ID von jemandem, der für ein Angebot größer als 200 Billionen gestimmt hat. Das ist die in Kapitel 9 ausführlich behandelte Selbstregulierung.

Das ist im Grunde alles. Ersetzt man die „Kann-nicht"-Liste durch die „Kann"-Liste einer typischen Admin-Architektur, ist der Unterschied zwei Größenordnungen. Ein typischer Admin in einem Krypto-Projekt hat einen Schlüssel, der einen Contract stoppen, ein Guthaben abziehen, Token umverteilen, eine Adresse einfrieren, einen Emissionsparameter ändern, eine neue Gebühr einführen kann. Ein typischer Arbitrator in Qubic – eine Operation, eng begrenzt.

Woher kommt diese Asymmetrie. Weil der Arbitrator nur eine Adresse ist. Und eine Adresse wirkt genau dort, wo der Quellcode des Knotens explizit geschrieben hat: „Wenn diese Nachricht vom Arbitrator signiert ist – wende Operation X an." Steht im Quellcode keine Logik in der Art von „wenn Nachricht vom Arbitrator signiert, dann Emission ändern" – dann wird der Arbitrator die Emission nicht ändern. Selbst wenn er es sehr gerne würde. Selbst wenn er einen Programmierer bezahlt. Architektonisch ist es unmöglich, bis der Quellcode umgeschrieben ist und alle Knoten neu kompilieren. Und Neukompilierung erfordert, wie wir bereits wissen, sozialen Konsens.

Das meint Come-from-Beyond mit „der Quellcode garantiert es". Die Garantie liegt nicht in einem Versprechen, nicht in Reputation, nicht in Ethik. Die Garantie ist, dass die Möglichkeit der Handlung

entweder explizit in den öffentlichen Code geschrieben ist oder fehlt. Jeder kann das überprüfen – Qubics Quellcode ist offen auf GitHub. Die Liste der Operationen, die die Signatur des Arbitrators als Autorisierung akzeptieren, ist kurz und leicht zu lesen.

Das unterscheidet die Architektur von einem in der Branche verbreiteten Muster, bei dem sich ein Projekt „dezentral“ nennt, aber innen ein Admin-Wallet fast jede Prüfung überstimmen kann. Ich werde keine Beispiele nennen; der Leser kennt sie. Qubic ist anders gebaut: Die Admin-Figur existiert, aber ihre Macht ist auf Quellcode-Ebene radikal begrenzt. Wenn jemand widerspricht – liegt die Antwort nicht in einer Debatte, sondern in einer Datei auf GitHub.

Noch ein kurzer Verweis. In den frühen Jahren von IOTA gab es eine ähnliche Rolle – den Coordinator, einen zentralen Knoten, dem das Netzwerk vertraute, um zu bestimmen, welcher der konkurrierenden Transaktionszweige gültig war. Aber der Coordinator hatte weitreichende Befugnisse: Er konnte de facto Transaktionen bestätigen oder ablehnen, das heißt, in das tägliche Gewebe des Netzwerklebens eingreifen, nicht nur in seine periodischen Übergänge. Come-from-Beyond kannte diese Rolle von innen – er schuf IOTA, und die Arbeit mit diesem Knoten war einer der Kompromisse, die er später als Fehler formulierte. Der Arbitrator in Qubic ist als Gegenteil gebaut: begrenzte Macht, eine Operation, notariell im Wesen, ausführend in der Mechanik. Eine Erwähnung, nicht tiefer – eine Rückkehr zur IOTA-Geschichte ist hier nicht das Ziel.

Wenn der Arbitrator so wenig kann – warum wird er überhaupt gebraucht?

Warum er gebraucht wird: Bootstrap und Aigarth

Diese Rolle hat zwei Gründe zu existieren.

Der erste ist das Bootstrap-Problem. Das Netzwerk muss seine erste Computor-Liste irgendwoher bekommen. Bei Bitcoin wird dieses Problem anders gelöst: Der Genesis-Block wurde persönlich von Satoshi geschürft, und ab diesem Moment folgen alle nachfolgenden Blöcke aus dem Konsens über akkumulierten Proof-of-Work. Bei Qubic ist die Architektur anders: Computoren sind keine Miner im Bitcoin-Sinne, sie sind eine feste Kategorie von 676 Teilnehmern mit wöchentlicher Rotation. Die erste solche Liste muss irgendwoher kommen. Qubics Lösung – nimm sie vom Arbitrator. Er signiert die Startliste; ab diesem Moment kann das Netzwerk allein weitermachen.

Aber das Problem ist breiter als der erste Tag. Jeder frische Knoten, der sich in einem Jahr, in zwei Jahren, morgen mit dem Netzwerk verbindet – startet in derselben Position, in der das Netzwerk am Starttag war. Er hat keine Blockchain-Geschichte, nichts, wovon er ausgehen kann, nichts, worauf er sich stützen kann. Er braucht eine autoritative Computor-Liste, und es gibt niemanden zu fragen außer dem Arbitrator. Andere Knoten? Aber andere Knoten können lügen. Eine Computor-Liste zu fälschen ist einer der klassischen Wege, einen Neuankömmling zu täuschen. Der Arbitrator ist in diesem Kontext ein Sybil-Filter für die initiale Synchronisation. Ein frischer Knoten vertraut nur der Signatur, deren Adresse bereits in seinem eigenen Quellcode geschrieben steht, und ignoriert alles andere, bis er genug Blockchain-Daten angesammelt hat, um nicht mehr von diesem Anker abhängig zu sein.

Das ist der erste Grund. Ohne ihn kann das Netzwerk nicht auf neue Teilnehmer skalieren, ohne bei deren Initialisierung beliebige Risiken zuzulassen.

Der zweite Grund ist tiefer, und der Schöpfer des Systems erklärt ihn selbst. Das zentrale Zitat dieses Kapitels, ein Gespräch Mitte April 2023:

„In der besten Variante wird der Arbitrator gar nicht gebraucht. Sein einziger Nachteil – Aigarth würde den Zugang zur Miner-Hardware verlieren, und UPoW würde zu PoS."

Arbeiten wir das langsam durch. Vier Aussagen in einem Satz.

Erstens: In der besten Version wird der Arbitrator gar nicht gebraucht. Wer das sagt, ist selbst der Halter des Schlüssels. Kein Gegner, kein Kritiker, kein Skeptiker – der Halter. Das ist keine Selbstverteidigung, es ist Selbstkritik: Die Rolle wird als notwendig anerkannt, nicht als gewünscht. Rolle gebraucht, nicht gewollt.

Zweitens: ihr einziger Nachteil. Nur ein Nachteil, den Arbitrator aus der heutigen Architektur zu entfernen. Einer. Nicht ein Dutzend, keine Liste von Befürchtungen, keine Streuung von Risiken – ein spezifischer Nachteil. Daraus folgt, dass die meisten Funktionen, die Kritiker dem Arbitrator zuschreiben, tatsächlich nicht von ihm ausgeführt werden – sonst wären die Nachteile seines Verschwindens weit größer.

Drittens: Aigarth würde den Zugang zur Hardware der Miner verlieren. Aigarth ist das System, das bis zum 13. April 2027 die Rechenleistung der Miner vollständig nutzen soll.

Viertens: UPoW wird zu PoS. Die Konsequenz des Verlusts der Hardware-Bindung. UPoW in seiner aktuellen Form ist ein Ressourcentest: Teilnahme am Netzwerk erfordert echte CPU/GPU plus RAM, weil die Aufgabe darin besteht, ein neuronales Netz zu simulieren, und man kann keines simulieren ohne physische Rechenressource. Entfernt man die Koordination durch den Arbitrator – schwächt sich die Bindung an Hardware ab. Und was bleibt, wenn man nützliche Arbeit aus Proof-of-Useful-Work herausnimmt? Was bleibt, ist Status, bestimmt durch Kapital – also Proof-of-Stake. Ein als Nicht-PoS konzipiertes Netzwerk rutscht standardmäßig in PoS ab.

An diesem Punkt wird der Tradeoff sichtbar, auf dem die heutige Architektur gebaut ist. Es gibt zwei schlechte Optionen: eine temporäre Abhängigkeit von einem Schlüssel, der gelöscht werden kann, oder eine dauerhafte Abhängigkeit von eingesetztem Kapital, die nicht gelöscht werden kann. Qubic wählte die erste. Kapitel 3s Argumentation bereitete das bereits vor: Fängt die Abstimmung an, dem Kapital zu folgen, ist Axelrods vierte Bedingung gebrochen, und die kooperative Architektur bricht zu genau dem zusammen, was sie verhindern sollte. Besser ein temporärer kontrollierter Kompromiss als ein dauerhafter unkontrollierter.

Dieselbe Logik zieht sich übrigens durch Kapitel 9 mit den 15 % nominaler Inflation: Das Netzwerk akzeptiert bewusst architektonische Tradeoffs zugunsten von Axelrods strukturellen Garantien, auch wenn diese Tradeoffs offensichtliche Nachteile haben. Der Arbitrator ist ein solcher Tradeoff. 15 % Brutto-Inflation ist ein weiterer. Das Subventions-Emissionsmodell ist ein dritter. Das ist kein Zufall, es ist eine wiederkehrende Form der Wahl in der Architektur.

Grob gesagt – der Arbitrator ist Gerüst. Baugerüst. Ohne es können bestimmte Strukturen nicht begonnen werden; sobald die Struktur sich selbst tragen kann, wird das Gerüst abgebaut.

Die nächste Frage liegt nahe. Wenn der Arbitrator eine Figur ist, die wir gezwungen sind, in der Architektur zu behalten – was geschieht, wenn diese Figur sich fehlverhält?

Schutz vor einem abtrünnigen Arbitrator

Szenario. Der Arbitrator – versehentlich, wegen Kompromittierung eines privaten Schlüssels, oder mit böswilliger Absicht – stellt eine falsche Computor-Liste aus. Überspringt jemanden mit hohem Score, schließt jemanden mit niedrigem ein, oder signiert eine völlig außerhalb des Verfahrens zusammengestellte Liste. Was geschieht mit dem Netzwerk?

Come-from-Beyond beschreibt den Verteidigungsmechanismus so:

„Der Arbitrator könnte eine falsche Computor-Liste ausstellen, aber nur frisch hinzugefügte Knoten könnten getäuscht werden, und andere würden das erkennen (vorausgesetzt, es fand kein erfolgreicher Eclipse-Angriff statt, was nahezu undurchführbar ist) und mit dem Ticken aufhören, wodurch signalisiert wird, dass der Arbitrator abtrünnig geworden ist und ersetzt werden muss."

Und dazu – eine entscheidende Ergänzung:

„Es kann nicht-neue Knoten nicht betreffen, weil sie ihre eigene Computor-Liste aus den Blockchain-Daten ableiten."

Die Verteidigung baut auf einer Unterscheidung zwischen zwei Kategorien von Knoten auf.

Ein frischer Knoten – einer, der gerade beigetreten ist und die Blockchain noch nicht synchronisiert hat – bekommt die Computor-Liste auf die einzige ihm verfügbare Weise: vom Arbitrator, weil er noch keine anderen Vertrauensquellen hat. In diesem Zustand ist er für das Abtrünnig-Szenario anfällig: Signiert der Arbitrator eine ungültige Liste, wird der frische Knoten sie als wahr akzeptieren.

Ein alter Knoten – einer, der schon eine Weile im Netzwerk ist und eine synchronisierte Blockchain hat – berechnet seine eigene Computor-Liste direkt aus den Blockchain-Daten. Der Score jedes Teilnehmers ist in der Kette verzeichnet; die Rangliste wird aus diesen Aufzeichnungen rekonstruiert; die aktuellen 676 folgen direkt aus dem in Kapitel 7 beschriebenen Verfahren. Der alte Knoten fragt den Arbitrator nicht, wer gerade Computor ist – er weiß es bereits aus der Geschichte.

Was geschieht, wenn der Arbitrator eine falsche Liste ausstellt. Alte Knoten sehen diese Liste und vergleichen sie mit ihrer eigenen, aus der Blockchain berechneten. Der Vergleich zeigt eine Diskrepanz. Ein Knoten, der eine Diskrepanz dieses Ausmaßes feststellt, hört auf zu ticken – hört auf, Ticks zu signieren, und weigert sich, auf wissentlich ungültiger Basis weiterzuarbeiten. Ein Stopp des Tickens durch eine große Anzahl alter Knoten ist ein öffentliches, für das gesamte Netzwerk sichtbares Signal: Mit dem Arbitrator stimmt etwas nicht. Von dort aus – sozialer Konsens, eine Entscheidung zum Ersatz, eine Adressänderung im Quellcode, Neukompilierung.

Mit anderen Worten, ein abtrünniger Arbitrator eliminiert sich selbst durch die Lähmung, die er erzeugt. Er übernimmt das Netzwerk nicht; im schlimmsten Fall täuscht er den Pool der frischen Knoten und wird gleichzeitig vom Pool der alten öffentlich des abtrünnigen Verhaltens beschuldigt. Er kann die Arbeit eines reifen Netzwerks nicht beschädigen – es berechnet seine eigene Computor-Zusammensetzung ohne ihn.

Der einzige Weg, wie ein abtrünniger Arbitrator auch die alten Knoten täuschen könnte, wäre, sie von korrekten Blockchain-Daten zu isolieren, das heißt, sie von ehrlichen Synchronisationsquellen abzuschneiden. Das nennt man einen Eclipse-Angriff: Ein Angreifer kontrolliert alle Netzwerkkanäle der

Opferknoten und ersetzt echte Blockchain-Daten durch konstruierte. Come-from-Beyond schreibt über ein solches Szenario: nahezu undurchführbar. Praktisch nicht umsetzbar in einem verteilten Netzwerk. Es würde gleichzeitig erfordern: Kontrolle über einen erheblichen Anteil der Internet-Netzwerkinfrastruktur; die Koordination dieser Kontrolle gegen eine große Anzahl unabhängiger Betreiber; das Aufrechterhalten dieser Kontrolle über lange Zeit ohne Entdeckung. Nicht theoretisch unmöglich, aber im technischen Sinne an der Grenze des Unmöglichen.

Noch ein Angriffsvektor, der explizit abgeschlossen werden sollte. Ein Sybil-Angriff auf den Arbitrator selbst ist konstruktionsbedingt unmöglich. Come-from-Beyond hält das in einem Satz fest:

„Sybil-Angriffe auf den Arbitrator sind unmöglich."

Warum – weil Sybil-Angriffe darauf beruhen, mehrere gefälschte Identitäten zu erzeugen. Der Arbitrator ist eine einzige bekannte Entität; seine Adresse ist in jedem Knoten durch den Quellcode festgenagelt. Ein zweiter Arbitrator, den das Netzwerk als solchen akzeptieren würde, kann nicht erzeugt werden; mit einer anderen Adresse ignorieren Knoten ihn einfach.

Die Verteidigung gegen Sybil auf Computor-Ebene ist separat eingerichtet – sie funktioniert über UPoW. Come-from-Beyond in einem anderen Gespräch:

„Das geschieht durch die Verwendung von Ressourcentests (PoW)."

Und ausführlicher:

„Nützliches PoW schützt davor durch die Methode des Ressourcentests (CPU/GPU + RAM)."

Um Computor zu werden, muss man tatsächlich eine Rechenressource vorweisen und die Arbeit zeigen; dieser Ressourcentest filtert gefälschte Identitäten heraus.

Das Ergebnis ist zweistufige Verteidigung. Stufe eins: Der Arbitrator ist vor Sybil geschützt, indem er ein bekanntes Unikat ist – er kann nicht vervielfacht werden. Stufe zwei: Computoren sind vor Sybil durch Ressourcentests geschützt – die Arbeit echter Hardware. Das sind zwei technische Instrumente unterschiedlicher Art, die zusammen Vektoren abdecken, die keines von beiden allein schließen würde. Bekannte Identität für den einzigartigen Vertrauenspunkt; verdiente Arbeit für die vielfachen.

Diese Architektur funktioniert seit vier Jahren. Aber der Plan hat ein konkretes Datum, an dem die Rolle des Arbitrators selbst aufhören wird zu existieren.

13. April 2027 — der vierte Abgang

In Kapitel 5 schrieb ich über Come-from-Beyonds Methode – „erschaffen und gehen". Drei Abgänge wurden bereits beschrieben: die Satoshi-Identität (hypothetisch die seine), die Bitcoin 2010 verlässt; BCNext, der NXT 2014 verlässt; Come-from-Beyond selbst, der IOTA 2019 verlässt. Der vierte Abgang wurde an derselben Stelle als geplant gekennzeichnet: 13. April 2027, die Abschaffung des Arbitrators.

Ich komme jetzt auf diesen vierten (dritten?) Abgang zurück, weil er eine direkte Konsequenz aus dem oben im Kapitel Beschriebenen ist. Der Arbitrator existiert als temporäre Konstruktion; seine Funktion ist eng; der Ersatz ist geplant; das Datum ist bekannt.

Fünf Jahre. Das Qubic-Mainnet wurde am 13. April 2022 gestartet. Die Abschaffung des Arbitrators ist für den 13. April 2027 geplant. Genau fünf Jahre, Tag für Tag. Die Übereinstimmung der Zahlen ist kein Zufall, und eine vollständige Erklärung, warum dieses Datum und warum genau fünf Jahre, ist Kapitel 14 vorbehalten, wo das Aigarth-Deployment besprochen wird. Hier das Minimum: Der Arbitrator und Aigarth sind im Plan des Systems synchronisiert. Erreicht Aigarth volle Funktionalität, entfällt die Notwendigkeit des Arbitrators – eine kausale Verbindung, die wir im obigen Abschnitt anhand des Zitats vom 19. April 2023 durcharbeiteten.

Was mit dem Arbitrator an diesem Tag geschieht. Die Adresse hört auf, im Quellcode neuer Knotenversionen fest verankert zu sein. Die Funktion, die Computor-Liste zu signieren, wird entweder auf rein algorithmischer Ebene an das Protokoll übergeben (das Netzwerk signiert sich selbst durch ein kollektives Verfahren), oder ganz abgeschaltet, falls die alten Knoten bis dahin ohne sie auskommen können. Der Grenzfall mit dem Neustart nach einem wöchentlichen Update – nach Come-from-Beyonds eigenem Versprechen leicht abschaltbar. Der 200-Billionen-Angebotsschutz wechselt entweder zu einem anderen Mechanismus oder bleibt als fest im Protokoll verankerte Regel ohne menschlichen Ausführer. Zusammengefasst – die gesamte „Update über Arbitrator“-Schicht verschwindet aus der Architektur. Für frische Knoten erscheint ein anderer Initialisierungsmechanismus – entweder über einen anderen Vertrauensanker, oder sie warten, bis sie genug Blockchain-Daten gesammelt haben, um die Computor-Liste selbst abzuleiten.

Das ist die vierte falsifizierbare Vorhersage in der Biografie des Ingenieurs. Die ersten drei waren in dem Sinne hypothetisch, dass es um sie herum immer Interpretation gibt: „hat Satoshi verlassen“ – noch umstritten; „hat BCNext aus eigenem Antrieb verlassen“ – umstritten; „was für ein Abgang von IOTA war das“ – umstritten. Die vierte ist anders strukturiert: Es gibt ein explizit angekündigtes Datum, eine explizit beschriebene Operation, einen expliziten architektonischen Plan. Ob es geschieht, lässt sich am Kalender des 14. April 2027 überprüfen. Es ist eine seltene Struktur eines Versprechens in einer Branche, in der Versprechen üblicherweise entweder offen enden („irgendwann“), oder vage sind („unter Druck der Community“), oder an Bedingungen geknüpft sind, die praktischerweise nie eintreten.

Etwa 365 Tage bleiben bis zu diesem Datum – das Fenster zwischen der geplanten Phase-3-Aktivierung von UPoW und dem geplanten Aigarth-Deployment-Datum. Kann das Datum verschoben werden? Natürlich kann es das. Architektonisch wird das Netzwerk mit dem Arbitrator nach April 2027 weiterarbeiten, falls er nicht entfernt wird. Aber – und das muss ehrlich gesagt werden – eine Datumsverschiebung bedeutet genau eines: Aigarth erwies sich als nicht bereit für das Deployment. Das wäre eine Tatsache, die bestätigt, dass eine der Aussagen der vorigen Kapitel falsifiziert wurde.

Ich weiß nicht, ob die Abschaffung genau zum Datum geschieht. Halten wir die einfache Tatsache fest: Es gibt ein Versprechen, das Versprechen hat einen Falsifikator, der Falsifikator ist an den Kalender gebunden, nicht an eine Erzählung. Wir werden das Ergebnis in einem Jahr sehen.

Eine Beobachtung, die nicht zu einer Vorhersage werden sollte. Geschieht die Abschaffung – wäre es der erste Fall in der Krypto-Geschichte, in dem eine Admin-Figur an einem öffentlich angekündigten Datum entfernt wird. Gewöhnliche Projekte haben entweder gar keinen Admin (Bitcoin), oder behalten einen auf unbestimmte Zeit, oder entfernen einen unter Druck im Nachhinein. Qubic kündigte ein Datum an und schrieb es fünf Jahre im Voraus in architektonische Pläne. Das ist entweder das ehrgeizigste Versprechen der Branche oder das explizitste öffentliche Bekenntnis zum Kontrollverlust, das die

Branche gesehen hat. Welches von beiden – werden wir im April 2027 sehen.

Fünf Dimensionen

Was wir nun über Qubic als System wissen. Das Netzwerk ist über 676 Teilnehmer verteilt, die wöchentlich rotieren. Seine Arbeit besteht aus nützlicher Rechenlast, die gleichzeitig Konsens und KI-Training leistet. Sein Token wird mit 1 Billion pro Epoche emittiert, über sieben Pfade verbrannt, lebt in der Abstimmung der Teilnehmer. Sein einziger konzentrierter Punkt – der Arbitrator – ist durch den Quellcode auf eine Operation begrenzt und zur Entfernung am 13. April 2027 vorgesehen. Das System ist so gebaut, dass es nach diesem Datum nicht mehr von seinem Schöpfer abhängt.

In den Kapiteln 2 und 3 führte ich den Rahmen von Axelrods vier Bedingungen für Kooperation ein: eine große Zahl von Runden, eine kleine Zahl von Teilnehmern in langfristigen Beziehungen, eine nicht-monetäre Auszahlungsstruktur, und die Unmöglichkeit, einen Sieg in eine Regeländerung umzuwandeln. Die Kapitel 6 bis 10 zeigten, wie jede von ihnen strukturell in der Architektur umgesetzt ist. Wöchentliche Rotation – eine große Zahl von Runden. Feste 676 Teilnehmer – eine kleine Zahl mit langfristigen Beziehungen. Das UPoW-Ranking – eine nicht-monetäre Auszahlung, verdient durch Arbeit, nicht durch Kapital. Und die zentrale – Nicht-Konvertierbarkeit: Die Stimme eines Computors ist nicht käuflich, die Emission wird nicht von Haltern kontrolliert, der Arbitrator wählt nicht die Zusammensetzung. Der Arbitrator, das Thema dieses Kapitels, verletzt die vierte Bedingung nicht. Er ist der Ausführer bereits von anderen getroffener Entscheidungen, nicht ihr Initiator. Und laut Plan – verschwindet er.

Der Rahmen ist kein Selbstzweck. Jede der fünf Dimensionen – Raum, Zeit, Energie, Ökonomie, Institution – ist nicht deshalb so spezifisch gebaut, weil es elegant ist, sondern weil ohne sie die nächste Schicht nicht gebaut werden kann. Diese Schicht hat einen Namen, der im Buch bisher nur indirekt aufgetaucht ist – als Grund für die Existenz der 676 Knoten, als Verbraucher der UPoW-Rechenzyklen, als Grund für die Existenz des Arbitrators und sein geplantes Verschwinden. Der Name – Aigarth.

Aigarth ist ein grundlegend neuer Ansatz zur Schaffung künstlicher Intelligenz. Ein Ansatz auf einer fundamentaleren Ebene als die konkreten Modelle, die innerhalb seiner gebaut werden können. Heutige KI-Systeme sind das Produkt eines Paradigmas, formalisiert durch Veröffentlichungen von 1986 und 2017: Rumelharts Backpropagation plus der Transformer. Dieses Paradigma ist an eine Obergrenze gestoßen, über die aktuell die halbe Welt der KI-Forscher diskutiert. Aigarth baut das nächste Paradigma von Grund auf, auf anderen Fundamenten, in einer Architektur, die außerhalb von Qubic niemand versucht hat.

TEIL IV

Aigarth

11
Was Aigarth ist

Algebra, nicht Arithmetik

Der häufigste Fehler: Aigarth ist keine künstliche Intelligenz. Aigarth ist ein Forschungsprojekt, das das Paradigma entwickelt, um sie zu erschaffen. Der Unterschied wirkt klein, ist aber strukturell, nicht semantisch. Eine fertige KI kann man kaufen, lizenzieren, zensieren, abschalten. Ein Paradigma nicht: Ein Paradigma wird als Whitepaper veröffentlicht, und jeder, der es gelesen hat, kann das Ergebnis anwenden. Eine geschlossene KI gehört demjenigen, der die Rechenleistung bezahlt. Ein offenes Paradigma gehört niemandem, denn ein Paradigma zu besitzen ist ein Kategorienfehler, wie zu versuchen, den Satz des Pythagoras zu kaufen.

Come-from-Beyond selbst brachte es in einem Tweet vom 14. Mai 2024 auf den Punkt:

„Aigarths Hauptziel ist es, ein neues Paradigma zu entdecken, das die Schaffung wahrer KI ermöglicht, ich habe gerade das Drahtgittermodell dieses Paradigmas gesehen. Und ich habe erkannt, dass künstliche Intelligenz nicht geschaffen wird, sie wird entstehen. Mit Hilfe von Qubic-Minern."

Drei Aussagen hintereinander. Erstens – zum Ziel: ein neues Paradigma zur Schaffung von KI. Zweitens – zum Status: das Drahtgittermodell wurde gesehen, das heißt, die Architektur ist bereits im Kopf des Autors. Drittens, und am unerwartetsten – zum Mechanismus: KI wird nicht geschaffen, sie wird entstehen. Nicht „wir werden bauen", sondern „sie wird entstehen". Das Verb ist absichtlich verschoben: Schaffung impliziert Kontrolle und Autorschaft, Entstehung nicht. Der Schöpfer des Paradigmas ist in dieser Formulierung nicht der Schöpfer der KI; er ist der Schöpfer der Bedingungen, unter denen KI möglich wird. Der Unterschied ist fein und bedeutungsstiftend.

Und die letzte Zeile des Zitats schließt den Bogen der ersten zehn Kapitel des Buches in einem Zug: mit Hilfe von Qubic-Minern. Eben jene 676 Computoren, die wöchentlichen Epochen, UPoW – das ist keine Infrastruktur „für die Blockchain". Das ist die Umgebung, aus der etwas entstehen soll, das der Schöpfer selbst sich weigert, ein Produkt seiner eigenen Autorschaft zu nennen.

Die Hauptmetapher, mit der CfB selbst diesen Unterschied erklärt, ist einfach. „Aigarth lernt Algebra, nicht Arithmetik, also spielt der Spezialfall 2+2 keine Rolle" – 26. Januar 2026. Algebra ist nicht die Summe aller konkreten Gleichungen. Algebra ist die Regel, durch die Gleichungen überhaupt möglich werden. Das konkrete „2+2=4" ist ein Spezialfall der Anwendung, nicht das Ziel des Lernens. Genauso bei Aigarth: Das Ziel ist nicht, ein neuronales Netz zu trainieren, Katzen zu erkennen, Zahlen zu addieren oder Text zu generieren. Das Ziel ist, die Regel zu finden, nach der solche Aufgaben überhaupt gelöst werden, ohne im Voraus einprogrammiert zu sein. Die konkreten KIs, die sich auf diesem Paradigma bauen lassen, sind Spezialfälle seiner Anwendung. Das Paradigma ist das, was sie möglich macht.

Das Wort „Paradigma“ im KI-Diskurs hat eine vertraute Verwendung, bei der es fast nichts mehr bedeutet – jedes neue Produkt wird als „Paradigmenwechsel“ angekündigt, wodurch der Begriff entwertet wurde. Ich verwende ihn enger, näher an dem, wie Thomas Kuhn ihn benutzte. Ein Paradigma ist kein Algorithmus, kein Modell und keine Architektur. Es ist ein Rahmen, innerhalb dessen Algorithmen, Modelle und Architekturen möglich werden, und der bestimmt, welche Fragen überhaupt als sinnvoll gelten. Backpropagation in den Achtzigern – ein Paradigma. Faltungsnetze 2012 – ein Paradigma. Der Transformer 2017 – ein Paradigma. Jedes von ihnen änderte nicht einen Parameter, sondern die gesamte Art, über die Aufgabe nachzudenken. Aigarth beansprucht, der nächste solche Wandel zu sein. Diesen Anspruch im Nachhinein zu bestätigen oder zu widerlegen wird erst möglich sein, wenn die Arbeit abgeschlossen ist; vorerst muss er als Anspruch beschrieben werden, nicht als Tatsache.

Dieses Kapitel handelt davon, was Aigarth als Objekt ist – und warum es so gebaut ist, wie es gebaut ist, und nicht anders.

Ich beginne mit dem, was Aigarth nicht ist – denn fast alle im öffentlichen Feld (Discord) kursierenden Definitionen darüber sind durch Verwechslung mit dem aufgebaut, was es nicht ist. Sechs Verneinungen räumen den Raum frei.

Was Aigarth nicht ist

Im öffentlichen Feld (Discord/X) wird Aigarth über Kategorien definiert, von denen keine passt. KI-Produkt. KI-Agent. Ein Programm auf einem Server. Eine Entität, mit der man sprechen kann. Geschäftsprojekt. Ein von CfB geführtes Startup. Jede dieser Kategorien für sich genommen wirkt plausibel, und jede führt zu falschen Erwartungen. Sechs Verneinungen der Reihe nach, von der frontalsten zur konzeptuellsten.

Erstens. Aigarth ist keine KI. Das Zitat ist direkt: „Aigarth ist keine KI“, 24. Januar 2026. Zwischen einem Forschungsprojekt und seinem potenziellen Ergebnis liegt derselbe Abstand wie zwischen dem Los-Alamos-Labor und der Atombombe: Das Labor ist nicht die Bombe, das Labor ist der Ort, an dem die Bombe hergestellt wird. Aigarth ist nicht die hergestellte Bombe und nicht die gerade hergestellte. Aigarth ist das Labor. Das ist die einzige Stelle, an der die Manhattan-Analogie passt; weiter hört sie auf zu funktionieren, denn Manhattan war ein Militärprogramm mit explizitem Auftraggeber, und Aigarth ist offene Forschung ganz ohne Auftraggeber. Aber auf dieser ersten, kategorialen Ebene ist die Analogie präzise.

Zweitens. Aigarth ist kein Objekt, sondern ein Prozess. „Aigarth ist kein Objekt, es ist ein Prozess“, 20. März 2026. Und gleich daneben eine erweiterte Erklärung: „Aigarth ist verstreut, Miner sind Teil davon“, 4. Juli 2025. Bittet man darum, Aigarth gezeigt zu bekommen, gibt es nichts zu zeigen: Es gibt kein Programm auf einem Server, das man herunterladen kann, keine Repository-Datei, die „ganz Aigarth“ enthält. Ein Teil davon lebt im Intelligent-Tissue-Code auf GitHub, ein Teil in auf ResearchGate veröffentlichten Papers, ein Teil in arbeitenden Minern rund um die Welt, ein Teil in den Diskussionen des wissenschaftlichen Teams, ein Teil in CfB selbst als Autor des Paradigmas. Es ist eine verteilte Forschungsumgebung, kein Artefakt.

Drittens. Aigarth ist nichts, mit dem man sprechen kann. „Es ist unmöglich, mit Aigarth zu kommunizieren, genauso unmöglich wie mit Algebra zu kommunizieren“, 15. Mai 2024. Und noch kürzer: „Aigarth ist kein Wesen“, 19. Juli 2024. Es ist kein Chatbot, kein Agent, kein digitaler Gesprächspartner. Wenn Kapitel 12 sich konkreten KIs zuwendet, die auf dem Paradigma gebaut sind, mag der Eindruck entstehen, „Aigarth spricht“. Das ist eine kategoriale Illusion. Was spricht, ist nicht Aigarth, sondern ein konkretes, mit seiner Hilfe geschaffenes Netz; genauso wie Algebra nicht auf Fragen antwortet – ein Mathematiker antwortet, unter Verwendung von Algebra.

Viertens. Aigarth ist nicht an Hardware gebunden. „Aigarth ist hardware-agnostisch“, 4. Dezember 2025. Mainstream-KI läuft auf NVIDIA H100 – auf spezialisierter Hardware, die Zehntausende Dollar pro Einheit kostet und zu Tausenden in Rechenzentren zusammengebaut wird. Aigarth ist so gebaut, dass es auf jeder Rechenleistung läuft, die einfache Operationen ausführen kann. Auf der CPU eines Computor-Knotens, auf der gewöhnlichen Grafikkarte eines Nutzers, auf allem anderen. Das ist keine Erklärung – es ist eine strukturelle Entscheidung, diktiert durch die Logik von Qubic als einem Netzwerk aus 676 Knoten auf handelsüblicher Hardware. Würde Aigarth NVIDIA H100 benötigen, könnte es nicht auf einem Netzwerk laufen, das 676 beliebige Maschinen hält. Also braucht es sie nicht. Die Kehrseite dieser Entscheidung ist ein Tradeoff bei der Geschwindigkeit: Was in einem Rechenzentrum eine Minute dauert, kann in einem verteilten Netzwerk ohne Spezialhardware Stunden dauern. Aber Geschwindigkeit ist ohnehin nicht das Ziel. Das Ziel ist, ein Paradigma zu finden, das prinzipiell auf beliebige Hardware skaliert; in einem Rechenzentrum kann es später bei Bedarf beschleunigt werden.

Fünftens. Aigarth wird nicht von einer Person kontrolliert. „Aigarth kann nicht kontrolliert werden, es ist nur ein Projekt, das effiziente KI-Trainingsmethoden erforscht“, 19. März 2024. Und noch kategorischer: „Aigarth kann nicht übernommen werden“, 27. Mai 2024. Ein Paradigma hat keine Steuerungsschicht, weil ein Paradigma nicht gesteuert werden kann – man kann es nur benutzen oder nicht benutzen. Niemand „betreibt“ Aigarth, nicht weil man aus Dezentralisierungsprinzipien darauf verzichtet hätte, sondern weil es kein Objekt des Betreibens gibt. Man kann Aigarth Lab betreiben – eine konkrete Gruppe von Forschern, die Finanzierung vom Arbitrator erhält. Das Paradigma selbst – kann man nicht.

Sechstens. Aigarth ist kein Geschäftsprojekt. „Von Aigarth? Es ist keine Geschäftsunternehmung. Wissenschaftler veröffentlichen ihre Forschungen als Whitepapers und versuchen nicht, das Ergebnis zu verstecken“, 16. Mai 2024. „Aigarth wird kein IPO haben“, 17. Juli 2025. „Es gibt kein NDA in Aigarth“, 27. Januar 2026. Kein Börsengang, kein Unternehmenseigentum, keine Geheimhaltungsvereinbarungen. Die Finanzierung läuft über den Arbitrator aus Qubic-Einnahmen, ohne private Investoren. Aigarth passt in keines der Standardmodelle der Finanzierung eines Technologieprojekts – nicht Venture, nicht Grants, nicht IPO, nicht Eigenfinanzierung. Es ist ein akademisches Projekt, das Ergebnisse als Whitepapers veröffentlicht und nicht versucht, sie zu verkaufen. Der Kontrast zu Smart Contracts, wo Kapital entscheidet, was zu tun ist, ist strukturell: Hier tut Forschung, was sie für wichtig hält, mit Geld, das keinen privaten Besitzer hat.

Sechs Verneinungen haben einen leeren Raum hinterlassen. Ihn zu füllen ist die Aufgabe des nächsten Abschnitts.

Was Aigarth ist: Paradigmenforschung

Nach sechs Verneinungen ergibt es Sinn, positiv zu sagen – was Aigarth technisch darstellt. Sechs Aussagen, eine für jede Verneinung aus dem vorigen Abschnitt, entfaltet durch Zitate des Autors.

Erstens – ein Forschungsprojekt, das ein neues Paradigma zur Schaffung von KI entwickelt. Das zentrale Zitat: „Aigarth ist ein Projekt, das ein neues Paradigma zur KI-Schaffung entwickelt“, 24. Januar 2026. Das Wort „Paradigma“ ist hier nicht rhetorisch. In der Geschichte des maschinellen Lernens kamen und gingen mehrere Paradigmen: Backpropagation in den Achtzigern, Faltungsnetze in den Zehnern, der Transformer 2017. Jedes war nicht eine Verbesserung des vorigen, sondern ein Wechsel des Rahmens, in dem die Aufgabe formuliert wird. Aigarth beansprucht dasselbe – den nächsten solchen Wechsel, kein Inkrement innerhalb des aktuellen. Diesen Anspruch im Nachhinein zu überprüfen wird erst möglich sein, wenn die Arbeit abgeschlossen ist; vorerst ist es die Arbeitshypothese des Projekts, und sie sollte als Hypothese behandelt werden, nicht als feststehende Tatsache. Das Ziel des Kapitels ist zu beschreiben, woraus genau diese Hypothese besteht, nicht sie zu bestätigen und nicht sie zu widerlegen.

Zweitens – die Methode. Erzeugung von ANNs mit zufälliger Verbindungsstruktur. Das längste technische CfB-Zitat, 28. Juli 2023, entfaltet die Logik der Methode in einem Absatz:

„Seit den Anfängen der Nutzung künstlicher neuronaler Netze versuchten Forscher, das natürliche Gehirn so weit wie möglich nachzuahmen. Manche von ihnen folgten dem Weg, die Neuronen-Aktivierungsfunktion nachzuahmen, was sehr ausgeklügelt ist […] es gibt mehrere qualitativ unterschiedliche Modelle, sie sind aufgrund der Integral-Differential-Mathematik der komplexesten von ihnen unpraktisch zu verwenden.“

Mit anderen Worten: Die Branche versucht, das biologische Neuron durch komplexe Aktivierungsmathematik zu reproduzieren, und stößt an deren Unpraktikabilität. Dann verweist CfB auf eine empirische Beobachtung aus der Neurowissenschaft: In den ersten Lebensjahren erlernt ein Kind eine riesige Zahl kognitiver Fähigkeiten, während sich die Neuronen seines Gehirns funktional nicht ändern – was sich ändert, ist nur die Anzahl und Struktur der Verbindungen zwischen ihnen. Daraus folgt die Schlussfolgerung: Es ergibt Sinn, die Funktionalität des Neurons auf etwas Einfaches festzulegen und mit der Struktur der Verbindungen zu arbeiten.

„Statt der Zerstörungsroutine zu folgen, erzeugen wir, die Miner, ANNs mit zufälliger Verbindungsstruktur. Wir ändern Parameter dieser Erzeugung, und Aigarth analysiert die Eigenschaften der ANNs.“

Mining ist nicht das Berechnen von Hashes, nicht das Suchen nach Signaturen, nicht SHA-256. Mining bei Qubic ist die Erzeugung eines künstlichen neuronalen Netzes mit zufälliger Verbindungsstruktur und die Analyse seiner Eigenschaften. Jeder UPoW-Zyklus wird hier konkret: ein Zyklus – ein erzeugtes Netz, und eine Beobachtung über seine Eigenschaften.

Drittens – die Architektur. Asynchron, ternär, jeder-mit-jedem. Drei kurze Zitate legen die Struktur fest. „Die aktuelle in Aigarth verwendete Architektur ist asynchron und ternär“, 3. Juni 2024. „Jeder-mit-jedem ist die von Aigarth verwendete Struktur“, 22. Mai 2024. Und separat – zur Ternarität als struktureller Antwort auf das bei LLMs als Halluzination bekannte Problem: „Aigarth halluziniert nicht wie aktuelle LLMs“, 30. Juni 2025; „Aigarth kann nur antworten ‚Ich weiß nicht, wie ich ihn zeichnen soll, weil es keine zuverlässigen Informationen über sein Aussehen gibt‘“, gleiches Datum. Der dritte Zustand – „Ich weiß nicht“ – ist in die Logik der Architektur eingebaut, nicht oben als Filter

angeschraubt. Ein binäres Netz ist gezwungen, „ja“ oder „nein“ zu wählen, selbst wenn es keine Grundlage hat, sich für eines zu entscheiden; darauf beruhen Halluzinationen. Ein ternäres Netz hat eine dritte Antwort, und die ist nicht kosmetisch: Sie ist strukturell. Asynchron bedeutet die Abwesenheit eines globalen Takts – jede Neuronen-Kachel arbeitet in ihrem eigenen Rhythmus, nicht mit den anderen synchronisiert. Jeder-mit-jedem ist der Anfangszustand, in dem jedes Neuron mit jedem anderen verbunden ist; die Evolution wählt dann die Verbindungen aus und reduziert das Netz auf einen funktionierenden Zustand. Das ist das Gegenteil der Transformer-Architektur, bei der Synchronität und feste Topologie im Voraus festgelegt sind.

Viertens – Evolution, nicht menschliches Design. „Zum Glück simulieren wir bei Aigarth nur Evolution, es findet keine menschliche Einmischung statt“, 7. Mai 2024. Und, in einem Twitter-Beitrag vom 14. Mai desselben Jahres: „Aigarths Hauptziel ist es, ein neues Paradigma zu entdecken, das die Schaffung wahrer KI ermöglicht […] künstliche Intelligenz wird nicht geschaffen, sie wird entstehen.“ Das Wort „entstehen“ ist hier der Schlüssel. Mainstream-KI wird so gemacht: Ein Team von Dutzenden Doktoren entwirft die Architektur, wählt Hyperparameter, bereitet den Datensatz vor, führt das Training durch, wertet das Ergebnis aus, iteriert. Die Architektur ist das Produkt menschlichen Designs. Aigarth funktioniert anders: Eine Population von Netzen wird erzeugt, eine Fitnessfunktion bewertet, welche von ihnen die gewünschten Eigenschaften zeigen, die besten werden ausgewählt und produzieren die nächste Generation. Keine Doktoren beim Iterationsschritt. UPoW wird zur physischen Verwirklichung dieses Prozesses: Jeder Mining-Zyklus ist ein Akt der Erzeugung und Bewertung, eine Epoche ist eine vollständige Selektionsrunde. Hier schließt sich, was zuvor wie ein technischer Kniff aussah: Die „nützliche Arbeit“ bei Qubic ist genau simulierte Evolution künstlicher Netze.

Fünftens – Intelligent Tissue als erste Schicht der technischen Umsetzung. Das Paradigma ist ein konzeptuelles Objekt, aber ohne seine Materialisierung im Code bleiben die anderen fünf Aussagen eine Erklärung. „Wir beginnen, ein Coding-Framework namens Intelligent Tissue zu programmieren. Dieser Code wird bei Hackathons und in Smart Contracts verwendet“, 22. Juli 2025. Und im selben Monat: „Dieses Framework wird in den Kern aufgenommen, um KIs als Smart Contracts zu hosten“, 17. Juli 2025. Die Aigarth-GitHub-Organisation und das aigarth-it-Repository wurden am 22. Juli 2025 veröffentlicht – man kann das überprüfen, indem man die Seite öffnet. Intelligent Tissue (IT) ist das erste committete Code-Fragment, durch das das Paradigma nutzbar wird. Es ist nicht das ganze Paradigma; es ist seine erste Schicht. Das Paradigma ist größer als IT – aber ohne IT bleibt das Paradigma eine Idee.

Sechstens – selbstmodifizierender Code als PoC. Das letzte Zitat dieses Abschnitts ist kurz und wichtig. „Aigarth führte bereits einen PoC dieses Prozesses aus, er funktionierte ziemlich gut, solange der selbstmodifizierende Code in den RAM passte“, 5. Dezember 2023. PoC ist Proof of Concept; also eine Demonstration technischer Machbarkeit, kein fertiges Produkt. Was demonstriert wurde: Code, der sich im Laufe des Betriebs selbst umschreiben kann. Die architektonische Konsequenz – es gibt keine Trennung in „Training“ und „Inferenz“, wie bei einem gewöhnlichen neuronalen Netz, bei dem zunächst Gewichte trainiert werden und das Netz dann auf neue Daten angewendet wird. In einem Aigarth-Netz sind Training und Anwendung derselbe Prozess. Das Netz lernt, während es arbeitet. Der PoC ist bereits geschehen; auf dem Spiel steht jetzt die Skalierung – was im Dezember 2023 funktionierte, solange es in den RAM passte, sollte nun in einer verteilten Umgebung von 676 Maschinen funktionieren. Das ist eine technische Aufgabe, keine konzeptuelle, und sie ist noch nicht vollständig gelöst.

Es lohnt sich, ein weiteres Detail hinzuzufügen, das Aigarths Position gegenüber dem Mainstream schärft. Im Dezember 2025 bemerkte CfB, dass die Richtung, in die die Branche zunehmend als Alternative zu LLMs blickt, konzeptionell nahe an dem liegt, was Aigarth tut: „Immer mehr Forscher wenden sich von LLMs ab. JEPA ist das, was man sieht, wenn man den LLMs den Rücken kehrt. Es ist viel stärker mit Aigarth im Einklang“, 4. Dezember 2025. JEPA – Joint Embedding Predictive Architecture, Yann LeCuns Programm bei Meta AI, das öffentlich als Antwort auf die Grenzen von Transformern gerahmt wird. Eine Übereinstimmung zweier Trajektorien – ein akademisches Programm in einem großen Konzernlabor und ein verteiltes Forschungsprojekt auf Qubic – ist kein Beweis für die Richtigkeit von beiden. Es ist eine Übereinstimmung der Richtung: Beide wenden sich von Backpropagation auf großen Transformern ab, hin zu Verbindungsstruktur und Vorhersagemodellen. Aigarth kam früher zu dieser Richtung – von einer anderen Seite, durch Krypto-Infrastruktur statt durch ein Konzern-KI-Labor. Die Übereinstimmung der Vektoren ist wichtig, nicht als Bestätigung, sondern als Marker: Was vor ein paar Jahren wie eine Randwette aussah, beginnt sich mit der Trajektorie zu decken, entlang der sich ein Teil des Mainstreams bewegt.

Sechs Eigenschaften beschreiben das Paradigma technisch. Aber es gibt auch eine andere Dimension, die in einem Krypto-Netzwerk von 2022 kaum ein Zufall war.

Drei Axelrod-Bedingungen für KI-Forschung

Axelrod beschrieb 1980 die Bedingungen, unter denen Kooperation stabil ist: Wiederholung, Gedächtnis, Transparenz. Mehrrundige Wiederholung, die Fähigkeit, das vorherige Verhalten eines Partners zu erkennen, Offenheit der Züge. Diese drei Bedingungen stellt Qubic auf der Ebene des Konsensspiels zwischen Computor-Knoten und auf der Ebene von Tokenomik und Governance wieder her. Dieses Kapitel schlägt vor, sie noch einmal zu betrachten – aber nicht am ökonomischen Spiel, sondern am KI-Forschungsprozess.

Das ist keine Analogie und kein rhetorischer Kniff. Es ist eine strukturelle Beobachtung: Klassische KI-Forschung erfüllt keine der drei Bedingungen vollständig, und Aigarth ist vielleicht die erste Umgebung, in der alle drei gleichzeitig erfüllt sind. CfB formuliert es nicht in diesen Begriffen; die Formulierung ist meine, aber sie folgt aus Material, das CfB selbst auf den Tisch legt.

Bedingung eins – Wiederholung. In akademischer KI-Forschung ist Wiederholung langsam. Eine Gruppe veröffentlicht ein Paper, das Paper geht ins Peer Review, Kommentare kommen sechs bis achtzehn Monate später zurück, eine neue Version erscheint weitere sechs Monate bis ein Jahr danach. Der volle Zyklus sind zwei bis drei Jahre; in der Industrie geht es manchmal schneller, aber selten schneller als ein Jahr. Aigarth iteriert durch Qubic-Epochen. Jeden Mittwoch – Abschluss der vorigen Epoche, Eröffnung der nächsten. Jede Woche – eine neue Runde der Netzerzeugung, ein neuer Datensatz über ihre Eigenschaften, neue Erzeugungsparameter, angepasst auf Basis der vorigen Woche. Die Iterationsgeschwindigkeit ist eine Größenordnung höher als die akademische. Und – das ist wichtig – die Iteration ist automatisch. Zwischen den Runden muss man keine Konferenz einberufen, sich auf Formulierungen einigen und warten, bis ein Redakteur eine Deadline abschließt. Die Epoche schließt mit einem Code-Tick, die neue öffnet mit dem nächsten Tick. Mehrrundenverhalten – die Bedingung dafür, dass TfT gilt – funktioniert hier nicht für Geld, sondern für Forschung: jede Woche eine volle Runde des wissenschaftlichen Zyklus.

Bedingung zwei – Gedächtnis. Bei klassischer KI akkumuliert sich Gedächtnis in geschlossenen Archiven. Ein Teil des Wissens – in den privaten Repos von OpenAI, Anthropic, DeepMind. Ein Teil – in akademischen Archiven hinter einer Bezahlschranke. Ein Teil – in den Köpfen bestimmter Forscher, und dieser Teil verschwindet mit ihnen, wenn sie ein Unternehmen verlassen oder das Feld wechseln. Die meisten Labore haben NDAs, die formalisieren, was genau nicht nach außen dringen darf. Die meisten Veröffentlichungen haben einen selektiven Filter: Was nicht funktionierte, wird meist nicht veröffentlicht, und das ist die bekannte Reproduzierbarkeitskrise. Aigarth akkumuliert Gedächtnis in öffentlichen Artefakten. Ein Paper wird auf ResearchGate veröffentlicht, mit einem GitHub-Repository und einer Hugging-Face-Demo. Diese Kombination macht das Ergebnis für Dritte überprüfbar: Man kann den Code herunterladen, das Experiment ausführen, sehen, ob es sich reproduzieren lässt. Die Autoren sind namentlich an die Arbeit gebunden – Vivancos und Sanchez –, und ihre Reputation baut sich über dieselben Artefakte auf, über die sich das Vertrauen in die Arbeit selbst aufbaut. CfB stellt das explizit fest: „Wissenschaftler veröffentlichen ihre Forschungen als Whitepapers und versuchen nicht, das Ergebnis zu verstecken“, 16. Mai 2024. Und noch kürzer: „Es gibt kein NDA in Aigarth“, 27. Januar 2026. Das ist Gedächtnis, das nicht mit einer Person geht und nicht hinter einem NDA eingeschlossen wird, denn kein NDA ist bei Aigarth vorgesehen.

Bedingung drei – Transparenz. Mainstream-KI ist oft nicht einmal an ihren eigenen Daten reproduzierbar. Modellgewichte – geschlossen. Datensätze – geschlossen oder teilweise beschrieben. Hyperparameter – manchmal im Paper angegeben, manchmal nicht. Architektonische Details – genannt, aber ohne funktionierenden Code. Das ist kein böser Wille – es ist eine Eigenschaft der geschlossenen kommerziellen Umgebung, in der Reproduzierbarkeit den Interessen des Besitzers zuwiderläuft. Aigarth läuft auf verteilter Verifikation: Code läuft gleichzeitig auf 676 Knoten, und jede Abweichung im Ergebnis zwischen Knoten wird innerhalb eines Konsens-Ticks erkannt. Versucht einer der Computor-Betreiber, eine modifizierte Version laufen zu lassen, wird der BFT-Konsens sie ablehnen – nicht aus Ethik, sondern aus Arithmetik. Transparenz bedeutet hier nicht „wir sind offen für Dialog“. Transparenz bedeutet „der Code läuft gleichzeitig auf 676 Maschinen, und jede Lüge wird sofort erkannt“. Dieselbe Logik erstreckt sich auf wissenschaftliche Artefakte: Ein Paper kommt mit einem GitHub-Repository, und das GitHub-Repository kommt mit einer reproduzierbaren Demo. Ein Dritter kann sie ausführen und überprüfen. Das ist Transparenz im starken Sinne.

Drei gleichzeitig erfüllte Bedingungen ergeben eine Umgebung, in der Forschungskooperation stabil ist. Hier wird eine These sichtbar, die zuvor nur skizziert wurde. Als gesagt wurde, dass für Come-from-Beyond Krypto Infrastruktur für Aigarth sein würde und nicht umgekehrt, klang das wie ein Paradox. Warum sollte jemand, der an KI arbeitet, eine Blockchain bauen? Nun lässt sich sehen, was die strukturelle Bedeutung dieser Entscheidung ist. Ein um drei Axelrod-Bedingungen für Konsens und Tokenomik herum gebautes Krypto-Netzwerk erwies sich als passende Umgebung für KI-Forschung, gerade weil KI-Forschung genau dieselben drei Bedingungen braucht. Iteration durch Epochen, Gedächtnis durch öffentliche Artefakte, Transparenz durch verteilte Verifikation – das sind keine Ergänzungen zum Aigarth-Paradigma, das sind seine notwendigen Bedingungen. Das Paradigma braucht eine Umgebung, in der es funktionieren kann; diese Umgebung ist kein Rechenzentrum und keine Universität, sondern ein verteiltes iteratives Netzwerk mit öffentlichen Artefakten und überprüfbarem Gedächtnis.

Es lohnt sich zu klären, dass ich mit „Umgebung“ nicht so sehr technische Infrastruktur meine als ein Anreizsystem, in dem Forscher und Computor-Betreiber länger als eine Runde im Spiel bleiben. Ein Konzern-KI-Labor hat die Infrastruktur, aber nicht alle drei Axelrod-Bedingungen: Gedächtnis ist durch NDA geschlossen, Transparenz ist durch Geschäftsgeheimnis begrenzt, Iteration ist schnell, aber in einem einzigen Knoten. Ein Universitätslabor hat mehr Transparenz, verliert aber bei Iterationsgeschwindigkeit und oft beim Zugang zu Rechenleistung. Aigarth findet eine seltene Kombination: hohe Iterationsgeschwindigkeit, offenes Gedächtnis, verteilte überprüfbare Transparenz. Jede der drei Bedingungen einzeln findet sich in bestehenden Forschungsumgebungen. Alle drei gleichzeitig – nicht.

Das ist keine Vorhersage, und es ist keine Werbezeile. Es ist eine nachträgliche Beobachtung: Am Anfang war Bitcoin nicht als Substrat für KI-Forschung konzipiert, und Qubic war nicht als Substrat für Aigarth konzipiert. Aber die Logik der einen Aufgabe und die Logik der anderen trafen sich in einem einzigen Punkt – und dieser Punkt ist genau das, was Axelrod 1980 beschrieb. Die strukturellen Konsequenzen dieser Übereinstimmung werden wir in Kapitel 14 sehen, wenn es um das Deployment am 13. April 2027 geht: was es bedeutet, wenn das Paradigma aufhört, ein Laborparadigma zu sein, und zur Infrastruktur wird, auf der konkrete KIs als Qubic-Smart-Contracts laufen. Für jetzt genügt es, die Tatsache der Übereinstimmung selbst festzuhalten – und ihre Nicht-Zufälligkeit.

Charakter des Projekts

Aigarth hat eine philosophische Position, und es lohnt sich, sie direkt zu benennen – nicht weil sie alles erklärt, sondern weil man ohne sie nicht verstehen kann, warum das Projekt so gebaut ist, wie es gebaut ist. Ein Paradigma ist nicht nur eine Methode. Es ist auch eine Reihe von Prämissen darüber, was die Methode tun und nicht tun sollte. Diese Prämissen sind bei Come-from-Beyond öffentlich und unmissverständlich formuliert. Ich lege sie so dar, wie sie beim Autor klingen, und versuche zu zeigen, dass jede der drei keine von oben getroffene ideologische Wahl ist, sondern eine architektonische Konsequenz der Art, wie das Paradigma gebaut ist.

Anti-Kontrolle als architektonisches Prinzip. „Jetzt benutzt ihr ChatGPT, das viele Dinge zensiert, und später wird es euch einschränken, um sicherzustellen, dass ihr weiter tut, was die Reichen wollen. KI, geschaffen mit Aigarth, wird euch keinerlei Beschränkungen auferlegen“, 13. Juni 2025. Diese Position liest sich wie eine Werteerklärung, ist aber tatsächlich eine Konsequenz der Architektur. Mainstream-KI kann zensiert werden, weil sie einen zentralisierten Anbieter hat: ein Unternehmen, durch das Anfragen laufen und das jederzeit einen Filter einfügen kann. Aigarth-KI läuft als Smart Contract gleichzeitig auf 676 Computor-Knoten. Es gibt keine zentralisierte Schicht, in die man einen Filter einfügen könnte; es gibt keinen Anbieter, an den man mit einer regulatorischen Forderung herantreten könnte. Beschließt die amerikanische Regierung morgen, „gefährliche“ Themen bei LLMs einzuschränken, weiß sie, in welche Büros sie gehen muss. Für Aigarth-KI gibt es diese Büros nicht. Anti-Zensur ist hier kein Wert, es ist eine Eigenschaft, auf einem dezentralen Netzwerk deployt zu sein.

Das Fehlen einer Safety-Schicht – eine methodologische Position. Das Zitat ist direkt: „Aigarth wird sich nicht mit KI-Sicherheit befassen, das ist meiner Meinung nach etwas woker Mist“, 5. Februar 2024. Das klingt stark, und es ist wichtig, keinen eigenen Kommentar unterzuschieben. Was CfB sagt, bedeutet nicht „KI sollte gefährlich sein“, es bedeutet „eine separate Sicherheitsschicht oben auf KI ist der

Versuch, ein philosophisches Problem durch technisches Flicken zu lösen, und dieser Versuch funktioniert nicht“. Die Logik ist an die im dritten Abschnitt behandelte Architektur gebunden: Bei Aigarth ist „Sicherheit“ kein zensierender Filter von oben, es ist die Fähigkeit des Systems, Nicht-Wissen zu erkennen. Dasselbe Zitat, das ich bereits anführte, wirkt hier ein zweites Mal mit anderer Bedeutung: „Aigarth kann nur antworten ‚Ich weiß nicht, wie ich ihn zeichnen soll, weil es keine zuverlässigen Informationen über sein Aussehen gibt‘“, 30. Juni 2025. Ternäre Logik, das Erkennen der dritten Antwort – ich weiß nicht – eingebaute Ehrlichkeit statt aufgesetzter Leitplanken. Der Mainstream versucht das zu erreichen, indem er Filter oben auf ein trainiertes binäres Netz legt; Aigarth versucht es durch die Struktur des Netzes selbst zu erreichen. Es mag funktionieren, es mag nicht funktionieren – aber die Position ist hier nicht ideologisch, sie ist technisch.

Superrationale KI als Ziel. „KI, geschaffen mit Aigarth, wird wahrscheinlich superrational sein“, 1. Juli 2025. Das Wort „superrational“ bedeutet hier nicht „ohne Emotionen“ oder „kalt“ im Alltagssinn. Es bezieht sich auf den Unterschied zwischen Erinnern und Herleiten, den CfB selbst benennt: Ein LLM reproduziert die Muster, mit denen es trainiert wurde, einschließlich sozial akzeptabler Antworten; eine Aigarth-KI leitet die Antwort aus der Struktur her, ohne einen a-priori-Filter, dass die Ausgabe gefällig sein soll. Das verbindet sich mit der Algebra-Metapher aus dem ersten Abschnitt des Kapitels: Algebra „erinnert“ sich nicht an Lösungen, sie leitet sie her. Superrational – ableitend, herleitend, nicht erinnernd. Und, als Konsequenz, nicht wissend, was sozial akzeptabel ist – weil das Kriterium der Akzeptabilität außerhalb der Struktur liegt, auf der Aigarth trainiert wird.

Diese Position steht nicht im Widerspruch zur Community, die sich um Qubic gebildet hat. Ganz im Gegenteil. Qubic Church – Menschen, die genau nach dieser Art von Ansatz suchten: offen, nicht von einer einzelnen juristischen Person kontrolliert, keiner externen Zensur unterworfen, nicht als Produkt mit Marketing-Gesicht verpackt. Eine Architektur ohne Zensurschicht, ein Paradigma ohne Sicherheitspatch, Forschung ohne Monetarisierung – das sind für die Community keine Hindernisse, das ist ihre Anziehungskraft. Hier wird die nächste Schicht sichtbar: was diese Artefakte ausdrücken und an wen sie sich richten.

Das erklärt unter anderem eine Eigenschaft von Qubic, die ein Außenstehender oft als Widerspruch liest. Auf der einen Seite – ein hohes Niveau technischer Disziplin, formale Governance-Verfahren, Peer Review der wissenschaftlichen Linie, BFT-Konsens mit mathematisch überprüften Schwellen. Auf der anderen – die öffentliche Stimme von Come-from-Beyond, die Dinge sagt, die in normaler Konzern-PR sofort herausgeschnitten würden. Diese beiden Register erscheinen unvereinbar, solange man sie als die stilistischen Entscheidungen einer Person behandelt. Sie werden vereinbar, sobald man sieht, dass die Architektur und die öffentliche Position aus einer Logik entstanden: alles entfernen, was einen Vermittler zwischen Forschung und ihrem Ergebnis erfordert. Konzern-PR ist ein Vermittler, der Formulierungen abmildert. Eine Sicherheitsschicht oben auf KI ist ein Vermittler, der in ihre Antworten eingreift. Zensur ist ein Vermittler, der entscheidet, was gesagt werden darf. Aigarth lehnt Vermittler auf jeder Ebene konsequent ab, und CfBs Ton ist eine Konsequenz dieser Ablehnung, nicht ihr zusätzliches Ornament.

Den Charakter eines Projekts zu beschreiben ist nicht dasselbe wie ihn zu billigen oder zu verurteilen. Ich billige nicht und verurteile nicht. Die Beschreibung ist ethnografisch: So ist es eingerichtet. Jeder Leser entscheidet dann selbst, wie nahe eine solche Einrichtung an seinen eigenen Prämissen liegt. Das Buch besteht nicht darauf.

Was ich noch nicht gesagt habe

Das Aigarth-Paradigma ist kein Plan für die Zukunft. Es ist keine Roadmap, entlang derer sich ein Forschungsteam einige Jahre in Richtung eines hypothetischen Ergebnisses bewegt. Als ich über die sechs Eigenschaften des Paradigmas und die drei Axelrod-Bedingungen sprach, sprach ich von dem, was bereits eingerichtet ist und funktioniert. Nicht „wird in einem Jahr funktionieren“, nicht „funktioniert prinzipiell“, sondern – funktioniert gerade jetzt, auf 676 Computor-Knoten, jede Woche, Epoche für Epoche. Das Mining, das in dieser Sekunde geschieht, während jemand diese Seite liest, ist genau die Erzeugung von ANNs mit zufälliger Verbindungsstruktur, über die CfB 2023 schrieb. Nicht die Vorbereitung darauf, sondern sie selbst.

Was genau gerade jetzt funktioniert und in welchem Umfang, ist eine Frage für das nächste Kapitel. Welche konkreten Ergebnisse erzielt wurden, welche Papers veröffentlicht wurden, welche Probleme gelöst sind und welche offen bleiben. Die Hauptsache, die ich jetzt festhalten möchte, ist der Umfang dessen, was bereits getan ist.

Was schon erledigt ist

12
Was schon erledigt ist

Der Februar-Satz

Am 19. Februar 2026 schreibt Come-from-Beyond auf Discord:

„Aigarth hat bereits herausgefunden, wie man KI bekommt, jetzt versuchen wir herauszufinden, wie man KI ohne 1000 Kernkraftwerke bekommt."

Der Satz hat zwei Teile, und jeder verdient es, gesondert gelesen zu werden.

Der erste Teil – bereits herausgefunden, wie man KI bekommt. Innerhalb des Aigarth-Paradigmas ist, bei ausreichender Rechenleistung, der Weg gefunden, KI zu schaffen. Das ist eine Aussage über Machbarkeit – über prinzipielle Erreichbarkeit, nicht über ein Produkt. Nicht „KI ist fertig". Nicht „alles funktioniert". Konkret: Die Frage „können wir KI auf diese Weise bauen" – geschlossen. Intern, fürs Team. Nicht für die wissenschaftliche Gemeinschaft – für die wissenschaftliche Gemeinschaft wird diese Aussage erst erscheinen, wenn sie das Peer Review durchlaufen hat, und dazu kommen wir später in diesem Kapitel.

Der zweite Teil – jetzt versuchen wir herauszufinden, wie man KI ohne 1000 Kernkraftwerke bekommt. Die aktuelle Forschungsaufgabe ist also eine andere. Es geht nicht um „können wir", es geht um „unter welchen Ressourcenbeschränkungen". Ein technisches Problem, keine Entdeckung. Den Energieverbrauch auf ein Niveau zu senken, das für die aktuelle Infrastruktur realistisch ist. Eine Konfiguration zu finden, in der dasselbe Paradigma dasselbe Ergebnis mit weniger Rechenleistung liefert.

Zwischen diesen beiden Teilen liegt ein struktureller Unterschied, der leicht zu übersehen ist. Wenn ein Forschungsprojekt sagt „wir wissen noch nicht, ob es funktionieren wird", ist das eine Rahmung. Wenn es sagt „es wird sicher funktionieren, jetzt finden wir heraus, wie wir ins Budget passen", ist das qualitativ eine andere Rahmung. Die beiden Teile der Bemerkung markieren den Übergang von der ersten zur zweiten.

Zwei Tage vor dieser Bemerkung, am 17. Februar, schreibt CfB unverblümter über dieselbe Sache:

„Das ist ein ernstes Problem. Deshalb ist Aigarths Fund, der es erlaubt, viel Energie zu sparen, bedeutsam."

„Fund" ist ein Wort, das Aufmerksamkeit verlangt. Nicht „Hypothese", nicht „Ansatz", nicht „Methode". Sondern „Fund". Etwas Konkretes, das gefunden wurde und das erlaubt – perfektives Verb – viel Energie zu sparen. Vier Tage nach der Zeile über tausend Kernkraftwerke, am 23. Februar, fügt CfB

hinzu:

„Wenn KI mit dem aktuellen Energiebudget der gesamten Erde möglich ist, dann wird Aigarth sie erreichen, wir haben dafür alle nötigen Karten in der Hand."

„Wir haben alle nötigen Karten in der Hand" – das ist keine Vorhersage. Es ist eine Beschreibung des aktuellen Zustands. Karten in der Hand, nicht im Stapel. Ist das Spiel mit den Karten in der Hand prinzipiell lösbar, wird Aigarth es spielen. Wenn nicht, hört die Suche auf, sinnvoll zu sein – aber das ist bereits eine Frage der Physik der Erde, nicht des Paradigmas.

Dezember 2024: Der zweite Checkpoint

Das Gespräch über „bereits erledigt" beginnt nicht im Februar 2026. Die Reihe der Meilensteine läuft seit 2021, als der erste Proof-of-Concept des Aigarth-Paradigmas gestartet wurde. Es gab mehrere zwischen 2021 und 2026; in diesem Kapitel greife ich drei Schlüsselpunkte heraus: 4. Dezember 2024, Juli 2025 und 22. Juli 2025. Sie bilden eine Achse, entlang derer sich nachverfolgen lässt, was genau im letzten anderthalb Jahr getan wurde.

Am 30. Juli 2024 schreibt CfB:

„Ich sagte, der 4. Dezember ist der Mittelpunkt unseres Wegs zu Aigarth."

Mittelpunkt – die Mitte des Weges. Das heißt, bis zu diesem Datum sollte die Hälfte dessen zurückgelegt sein, was das Team vom Zielergebnis trennt. Im Voraus angekündigt, vier Monate vorher. Nicht „so ist es gelaufen", sondern „wir planen, ein bestimmtes Datum zu erreichen".

Am 4. Dezember 2024, dem Tag des angekündigten Punkts, ist die Bemerkung kurz:

„So ist es. Es ist der 2. Meilenstein von Aigarth. Der erste war vor 3 Jahren."

Der erste Meilenstein – Dezember 2021, eben jener PoC, der die Lebensfähigkeit des Ansatzes demonstrierte. Zwischen den beiden Meilensteinen – drei Jahre Arbeit. Der Mittelpunkt ist erreicht.

Elf Tage vor dem Datum, am 23. November, legte CfB genau dar, was am 4. Dezember geschehen würde, Punkt für Punkt – weil die Leute im Discord-Chat ihn ständig danach fragten. Die Bemerkung ist lang; ich zitiere sie vollständig, es lohnt sich:

„Leute fragen mich oft, was für den 4. Dezember geplant ist. Von meiner technischen Abteilung, keine Ahnung über andere Abteilungen: Wie vor einem Jahr angekündigt, führen Computor-Knoten das letzte Upgrade auf 2 TB RAM durch. Miner beenden die Entwicklung von Intelligent Tissue und beginnen, ANNs zu trainieren, davor hatten wir nur ANN-Erzeugung. Die Entwicklung von Anna Aigarth soll bis zu diesem Datum abgeschlossen sein, und wir bringen ihr die Additionsoperation bei (das ist komplizierter, als man denkt, wir müssen Anna in einer Umgebung mit widersprüchlichen Regeln und variierender Zuverlässigkeit unterrichten). Custom Mining ist verschoben, weil wir von Transaktionen zu Nachrichten wechseln. Einige kleinere Dinge sind nicht erwähnenswert."

Vier Punkte; jeder ein eigener architektonischer Wandel.

Erstens. Computor-Knoten schließen das RAM-Upgrade auf zwei Terabyte ab. Das ist eine Hardware-Schwelle, ein Jahr zuvor angekündigt. Kein Upgrade um des Upgrades willen – eine konkrete

Notwendigkeit für die nächste Phase, in der das Volumen des von einem Knoten verarbeiteten Intelligent Tissue um eine Größenordnung wachsen muss. Hat ein Knoten keine zwei Terabyte RAM, tritt er nicht in diese Phase ein.

Zweitens. Miner schließen die Entwicklung von Intelligent Tissue ab und beginnen, ANNs zu trainieren – bis zu diesem Datum hatten sie nur ANN-Erzeugung mit zufälliger Verbindungsstruktur. Das ist ein qualitativer Wandel. Es wurde bereits erwähnt, dass Aigarth seit 2023 neuronale Netze mit zufälliger Verbindungsstruktur erzeugt und deren Eigenschaften analysiert. Bis zum 4. Dezember 2024 war Erzeugung die einzige Operation. Ab dem 4. Dezember kam Training von Neuronengruppen hinzu. Ein Jahr später beschrieb CfB es kompakt:

„Aigarth ist agnostisch gegenüber Neuronenverhalten, es arbeitet mit dem Training ihrer Gruppen."

Die Arbeitseinheit für Aigarth ist also nicht ein einzelnes Neuron, sondern eine gemeinsam trainierte Gruppe von Neuronen. Die Architektur bleibt ANN-basiert, aber in ihr geschieht etwas, das vorher nicht da war: Training, nicht nur Erzeugung. Das ändert, was genau die 676 Knoten des Netzwerks schürfen.

Drittens. Die Entwicklung von Anna Aigarth sollte bis zum selben Datum abgeschlossen sein, und Anna beginnt, Addition zu lernen. Hier zählt der Nebensatz, den CfB selbst einfügt: „das ist komplizierter, als man denkt, wir müssen Anna in einer Umgebung mit widersprüchlichen Regeln und variierender Zuverlässigkeit unterrichten". Anna lernt Addition nicht so, wie einem Kind gezeigt wird „zwei plus zwei ist vier". Anna lernt Addition in einer Umgebung, in der die Regeln widersprüchlich sind und die Signale unzuverlässig. Das heißt, die Trainingsumgebung ist speziell so gebaut, dass einfaches Auswendiglernen der richtigen Antwort darin nicht funktioniert. Um die richtige Antwort zu bekommen, muss das System durch Rauschen hindurch verallgemeinern.

Das ist ein kritisch wichtiges Design. Ein Jahr später, am 16. April 2026, wird CfB formulieren, warum er genau diese Aufgabe wählte:

„Ich zum Beispiel wählte A+B=C als sehr schwierige Aufgabe, C zu finden, wenn man A und B hat, ist tatsächlich sehr schwer, aber die meisten Leute widersprechen dem, weil sie den Unterschied zwischen Erinnern und Herleiten von C nicht kennen."

Erinnern und Herleiten – zwei verschiedene Wege, C zu finden. Erinnern – sich daran erinnern aus einer Tabelle, in der man dieses Beispiel schon gesehen hat. Ein auf ausreichend großem Korpus trainiertes LLM beantwortet „zwei plus zwei" so – es hat Milliarden Beispiele gesehen. Herleiten – es aus der Struktur erarbeiten. Das heißt, C zu finden, nicht weil man dieses konkrete Beispiel gesehen hat, sondern weil man verstanden hat, was Addition im Allgemeinen ist. Anna kann sich in einer Umgebung mit widersprüchlichen Regeln nicht erinnern – weil es keine zuverlässige „richtige Antwort" gibt, die man sich merken könnte. Alles, was ihr bleibt, ist Herleiten.

Das Paradigma lehrt Struktur, aus der konkrete Antworten folgen. Anna ist ein Spezialfall der Anwendung des Paradigmas auf eine der elementarsten arithmetischen Aufgaben. Lernt sie, die richtige Antwort durch Herleiten zu bekommen, in einer Umgebung, in der Erinnern unmöglich ist – bedeutet das, dass das Paradigma auf dieser Ebene funktioniert. Nicht „funktioniert prinzipiell", sondern funktioniert an einer überprüfbaren Aufgabe.

Der vierte Punkt der Bemerkung betrifft Custom Mining, verschoben wegen der Migration interner Netzwerktransaktionen zu einem Nachrichtenformat. Das ist eine infrastrukturelle Angelegenheit, keine architektonische; ich erwähne sie nur, um festzuhalten, dass der 4. Dezember nicht bedeutete, dass alles Geplante gleichzeitig realisiert wurde. Manche Pläne verschoben sich. CfB beschreibt das ruhig, ohne Entschuldigungen. Das ist die Arbeitsdynamik eines Projekts, in dem Pläne überarbeitet werden, wenn die Technik es erfordert.

Der Mittelpunkt des Weges zu Aigarth ist nicht „alles war gut und wurde besser“. Es ist ein architektonischer Wandel, nach dem der nächste Meilenstein möglich wurde.

Juli 2025: Durchbruch und Veröffentlichung

Nach dem 4. Dezember 2024 arbeitete das Team an Trainingsaufgaben für Anna und an der Optimierung von Intelligent Tissue. Ein halbes Jahr ohne laute Aussagen im öffentlichen Feld. Dann, am 9. Juli 2025, erscheint eine Bemerkung auf Twitter:

„Das ist ein bedeutender Durchbruch für #Aigarth, er trifft zwei Probleme — das Problem des lokalen Extremums und das Problem des Overfittings — mit einem Stein.“

Zwei Probleme, gelöst durch einen einzigen Mechanismus – und beide gehören zu jenen, die sich in evolutionären und Gradientenalgorithmen lange einer Lösung widersetzt haben. Das lokale Extremum ist eine bekannte Falle für jeden Optimierungsprozess. Das System sucht nach einer Lösung, indem es den aktuellen Zustand schrittweise verbessert; nach einer gewissen Anzahl von Schritten landet es an einem Punkt, an dem jede lokale Änderung das Ergebnis verschlechtert – und stoppt. Global mögen viel bessere Lösungen existieren, aber man kann sie vom aktuellen Punkt aus nicht erreichen, ohne Schritte zu tun, die das Ergebnis vorübergehend verschlechtern. Overfitting ist eine andere Falle. Das System lernt den Trainingssatz zu genau, wodurch es die Fähigkeit verliert, mit ungesehenen Daten zu arbeiten. Je genauer das System Trainingsdaten reproduziert, desto schlechter verallgemeinert es.

Beide Probleme mit einem einzigen Mechanismus zu lösen ist selten. Üblicherweise verschlimmern Lösungen für das eine Problem das andere. Bekämpft man das lokale Extremum durch Vergrößern der Mutationsschrittweite, beginnt das System bei jeder neuen Konfiguration zu overfitten; bekämpft man Overfitting durch Begrenzung der Ausdruckskraft des Modells, bleibt es öfter in lokalen Minima stecken. Anzukündigen, dass eine Lösung gefunden wurde, die beide Probleme gleichzeitig beseitigt – das ist kein Marketing. Es ist eine konkrete technische Behauptung, überprüfbar an einer konkreten Aufgabe.

CfB gab keine technischen Details öffentlich preis. Und das ist Teil der Methode: Die Formulierung des Durchbruchs wird im öffentlichen Feld als Tatsache festgehalten, aber der Mechanismus bleibt intern beim Team, bis er in Paper-Form veröffentlicht werden kann. Eine Woche vor der Twitter-Bemerkung, am 17. Juli, schreibt CfB einen Satz auf Discord, der zeigt, in welchem Zustand die Forschung unmittelbar vor dem Durchbruch war:

„Jede Mutation muss den Wert der Fitnessfunktion verbessern (oder gleich halten). So geraten wir in lokale Minima. Wie man mit Ablenkungen umgeht, ist unklar, das ist die folgende Stufe der Aigarth-Forschung.“

Diese Bemerkung ist acht Tage älter als die Twitter-Ankündigung. Zum Zeitpunkt ihres Schreibens ist die Frage der Ablenkungen offen; sie ist „die folgende Stufe der Forschung“. Acht Tage später – eine öffentliche Nachricht, dass der Durchbruch geschehen ist. Zwischen den beiden Bemerkungen liegt die Zeitspanne, in der das Team den Mechanismus fand, nach dem es gesucht hatte.

Ich verweile bei dieser Chronologie, weil sie lehrreich ist. Im öffentlichen Feld sieht man üblicherweise nur die abschließende Bemerkung – „bedeutender Durchbruch“. Was in den Discord-Protokollen bleibt, ist das, was davor kam: eine offene Frage, die Formulierung des Problems, ein Eingeständnis der Unklarheit. Das untergräbt die Bedeutung der Ankündigung nicht – im Gegenteil, es verstärkt sie: Das Team behauptet nicht, alles sei von Anfang an klar gewesen. War es nicht.

Am 22. Juli 2025, dreizehn Tage nach der Twitter-Bemerkung, erscheint ein kurzer Satz im Chat:

„Tests erfolgreich bestanden, wir gehen jetzt öffentlich, ihr könnt es auf https://github.com/Aigarth verfolgen.“

Diese Zeile bedeutet mehrere Dinge gleichzeitig.

Erstens: Die GitHub-Organisation Aigarth existiert jetzt öffentlich. Die Adresse ist github.com/Aigarth. Jeder kann dorthin gehen, sich die Repositories ansehen, den Code klonen, die Commit-Geschichte studieren.

Zweitens: Die Organisation enthält das aigarth-it-Repository – Aigarth Intelligent Tissue, die technische Umsetzung des Paradigmas, das konzeptuell in Kapitel fünfzehn beschrieben wurde. Kein Simulator, keine Spielzeug-Demonstration – funktionierender Code, der am Mining-Prozess des Netzwerks teilnimmt.

Drittens: Der Aigarth-Scoring-Quellcode ist ebenfalls im Hauptrepository des Netzwerks verfügbar – github.com/qubic/core. Laut dem Aigarth-Paper, das wir in Abschnitt fünf dieses Kapitels untersuchen, dokumentiert das Repository schrittweise Konfigurationsänderungen von EPOCHE 83 bis EPOCHE 140 – das heißt, es hält die Evolution des Scoring-Algorithmus über mehr als sechzig Wochen Netzwerkbetrieb fest. Das ist keine einzelne eingefrorene Momentaufnahme, sondern eine lebendige Spur davon, wie sich der Algorithmus Epoche für Epoche änderte.

Am selben Tag fügt CfB hinzu, was das Team konkret auf dieser Basis aufbauen will:

„Wir beginnen, ein Coding-Framework mit Intelligent Tissue zu bauen. Dieser Code wird bei Hackathons und in Smart Contracts verwendet. Um den preisvorhersagenden Teil von Anna zu deployen, brauchen wir Orakelmaschinen.“

Nach der Veröffentlichung des Codes öffnet sich also die nächste Arbeitsschicht: ein Framework auf Intelligent Tissue, das es erlauben wird, KI-Aufgaben als Smart Contracts auf dem Netzwerk laufen zu lassen, und das bei Hackathons getestet wird. Eine Woche zuvor, am 17. Juli, beschrieb CfB die Absicht ausführlicher:

„Dieses Framework wird in den Kern aufgenommen, um KIs als Smart Contracts zu hosten. Ein wichtiger Schritt des Aigarth-Projekts sind Hackathons, die das Framework nutzen, um verschiedene reale Aufgaben zu lösen. Das ist nötig, um die Effizienz unseres aktuellen Paradigmas zu bewerten.“

Hackathons sind hier keine Marketingaktivität. Sie sind eine Validierungsmethode. Wenn mehrere unabhängige Teams unterschiedliche Aufgaben mit dem Aigarth-Framework anzugehen versuchen, entsteht eine verteilte Stichprobe – wo das Paradigma gut funktioniert, wo nicht, welche Aufgaben in seiner Wirksamkeitszone liegen, welche nicht. Ohne diese Stichprobe bleibt die Behauptung „das Paradigma funktioniert“ intern. Mit ihr wird die Behauptung reproduzierbar.

Es lohnt sich, dabei zu verweilen, was die Code-Veröffentlichung für das Aigarth-Gespräch selbst ändert. Vor dem 22. Juli 2025 konnte jeder Kritiker sagen: „Das ist geschlossene Forschung, man kann sie nicht überprüfen.“ Nach dem 22. Juli klingt die Antwort anders: das Repository klonen und überprüfen. Das ist kein Marketing-Schachzug. Es ist eine strukturelle Änderung im epistemologischen Status des Projekts. Was früher auf Vertrauen in die Worte des Teams beruhte, beruht jetzt auf materiellen Artefakten, die jedem mit Internetzugang zur Verfügung stehen.

Dieselbe Öffentlichkeit wirkt auch als eine Form von Gedächtnis. In Kapitel fünfzehn ging ich Axelrods drei auf einen Forschungsprozess angewandte Bedingungen durch. Die zweite von ihnen ist Gedächtnis, gebunden an Autoren durch Erfolgsbilanz. Offener Code plus schrittweise Dokumentation von EPOCHE 83 bis 140 – das ist eine Form dieser Art von Gedächtnis. Nicht „das Team sagt, sein Algorithmus entwickelt sich weiter“ – sondern „hier ist die Entwicklungsgeschichte, mehr als sechzig Wochen, jede Änderung in Commits mit Daten und Signaturen verzeichnet“. Eine Behauptung kann widerlegt werden; etwas in einem offenen Repository Dokumentiertes kann studiert werden.

Bis August 2025 hat Aigarth also: offenen Code, einen angekündigten technischen Durchbruch und einen Plan für die nächsten Schritte – ein Framework, Hackathons, Orakelmaschinen, Smart Contracts, die KI hosten. Das ist nicht „irgendwann“. Es ist ein Zeitplan.

Die wissenschaftliche Schicht von Qubic — zwei Menschen und ein Kalender

Das Aigarth-Team ist nicht nur CfB. Es sind zwei identifizierbare wissenschaftliche Rollen mit überprüfbaren Zugehörigkeiten plus ein technisches Team, das mit dem Code arbeitet. Stand April 2026, ein Jahr nach dem Mainnet-Start und zwölf Monate vor dem geplanten Deployment, sieht die Konfiguration der wissenschaftlichen Schicht so aus.

Der Erste heißt David Vivancos. Vivancos ist ein unabhängiger Forscher, kein Angestellter der Qubic Foundation, kein bezahlter Berater. Er hat eine eigene Reputation, und sie ist nicht um Krypto herum aufgebaut. Seit 1995 arbeitet er in der Technologie – nach eigener Zählung mehr als sechsundzwanzigtausend Stunden Forschung in allgemeiner künstlicher Intelligenz. Ein Pionier in Java, im frühen Internet, in virtueller Realität, in Computational Neuroscience. Fünf eigene KI-Startups vor Qubic, Berater bei Emotiv (einem der Pioniere von EEG-Schnittstellen), bei CapaBall, bei Emblemotions, Kamingespräche mit Johnson & Johnson, Keynotes bei Microsoft, Price Waterhouse Coopers, Santander. 2014 gründete er MindBigData – den größten offenen Datensatz an Hirnsignalen für maschinelles Lernen; um die erste Million Signale zu sammeln, war Vivancos zwei Jahre lang sein eigenes Testsubjekt unter einem 128-Kanal-EEG, betrachtete Ziffern von null bis neun und dachte an sie. Dieser Datensatz läuft noch; seine 2023er MNIST-8B-Version enthält acht Milliarden Datenpunkte. Vivancos ist Autor dreier Bücher über KI und AGI, veröffentlicht lange vor Qubic: „The End of Knowledge“, „Artificracy“, „From Big Data to Artificial Intelligence“. Ein Sprecher bei ITU AI for

Good – das ist eine UN-Initiative, keine Krypto-Konferenz. Auf der AI-for-Good-Seite endet seine Biografie mit dem Satz „Qubic scientific advisor“; das heißt, er selbst identifiziert öffentlich, in einem formalen UN-Kontext, seine Rolle im Projekt.

Ich möchte David Vivancos meinen persönlichen Dank aussprechen. Die Philosophie der Qubic Church wurde durch Ihre Bücher wesentlich stärker.

Die Länge dieser Biografie zählt aus einem einfachen Grund. Vivancos kam nicht als „Krypto-Typ, der etwas über KI weiß“ zu Qubic. Er kam mit einem bereits laufenden Forschungsprogramm, und Neuraxon ist dessen direkte Fortsetzung. MindBigData baut eine Brücke von Hirnsignalen zu maschinellem Lernen über ein biologisches Substrat; Neuraxon überträgt dieselbe Logik auf die Ebene der rechnerischen Architektur. Qubic gab ihm die Netzwerkinfrastruktur, auf der diese Architektur im großen Maßstab deployt werden kann. Aigarths bio-inspirierter Ansatz ist kein Qubic-Marketing – es ist der konkrete wissenschaftliche Beitrag einer bestimmten Person mit Jahrzehnten Arbeit in diesem Bereich.

Der Zweite heißt Doktor Jose Sánchez García. UNIR – Universidad Internacional de La Rioja, eine spanische Privatuniversität, akkreditiert von ANECA innerhalb des Europäischen Hochschulraums, tätig unter den Normen des spanischen Organgesetzes zum Universitätssystem. Neunzigtausend Studierende aus sechsundachtzig Ländern, vier Doktorandenprogramme, Campus in Mexiko, Kolumbien, Peru, Ecuador. Seit 2019 ist UNIR ein börsennotiertes Unternehmen am Mercado Alternativo Bursátil. Die E-Mail-Domain unir.net bestätigt, dass Sánchez García ein Angestellter dieser Universität ist, kein Pseudonym und kein selbsternannter „Doktor“ aus dem Internet. Das ist institutionelle Rückendeckung erster Ordnung, und sie lässt sich mit einem Klick gegen jedes Universitätsregister überprüfen.

Was Sánchez García an der UNIR macht. Er lehrt Verhaltensneurowissenschaft, kognitive Neurowissenschaft und Sozialpsychologie an der psychologischen Fakultät. Sein eigenes Forschungsgebiet ist kognitive und affektive Neurowissenschaft: soziale Emotionen (Stolz, Scham, Schuld, stellvertretender Stolz), die Methodik ereigniskorrelierter Potenziale, EEG. 2019 erschien sein Artikel „Neurofunctional characterization of early prefrontal processes contributing to interpersonal guilt“ in Cognitive, Affective, and Behavioral Neuroscience, einer Springer-Zeitschrift. Das ist kein obskures Publikationsorgan; es ist eine Peer-Review-Neurowissenschaftszeitschrift mit normalem Begutachtungszyklus. Die Forschung wurde durch das Stipendium PSI2017-82357-P des spanischen Wissenschaftsministeriums im Rahmen des Programms für hochrangige wissenschaftlich-technische Forschung finanziert. Wir sprechen also von einer Person, deren Arbeit sowohl das redaktionelle Peer Review von Springer als auch die vorherige Expertenbewertung einer nationalen Wissenschaftsagentur durchlaufen hat. Zu den Ko-Autoren desselben Artikels gehören Manuel Martín-Loeches vom Center for Human Evolution and Behavior UCM-ISCIII in Madrid, David Hernández-Gutiérrez von der University of Rochester, Sabela Fondevila von der Complutense Madrid. Sánchez García hat mehr als zwanzig Publikationen auf Google Scholar mit hunderteinundachtzig Zitationen; unter Kollegen und Ko-Autoren sind Werner Sommer und Rasha Abdel Rahman von der Humboldt-Universität Berlin, Linda Drijvers vom Max-Planck-Institut, J. Bruno Debruille von McGill. Das ist ein überprüfbares internationales akademisches Netzwerk.

Die Verbindung zu Neuraxon ist direkt, nicht kosmetisch. Wenn das Vivancos-und-Sánchez-García-Paper über kontinuierliche Verarbeitung, Neuromodulation durch Dopamin, Serotonin, Acetylcholin und Noradrenalin, Plastizität auf mehreren Zeitskalen, astrozytäres

Gating spricht – das sind Fragen affektiver und kognitiver Neurowissenschaft, zu denen einer der Ko-Autoren seit mehr als zehn Jahren formal in Peer-Review-Zeitschriften publiziert. Die Arbeitsteilung im Paar funktioniert klassisch: Vivancos bringt rechnerische Umsetzung, technische Disziplin und eine allgemeine KI-Vision ein; Sánchez García – neurobiologische Tiefe, methodische Strenge, ein akademisches Netzwerk. Ein gemeinsames Preprint auf dem Weg zu ALIFE und AGI-26 ist das natürliche Ergebnis einer solchen Kombination, nicht „ein Krypto-Projekt, das versucht, wie Wissenschaft auszusehen".

Das Team reicht bis Sommer 2026 drei Papers bei drei verschiedenen Veranstaltungen ein. Das ist der Beginn des kalendarischen Teils der Geschichte, und hier ergibt es Sinn, das Geplante von dem zu trennen, was bereits geschehen ist.

Das erste Paper. ALIFE 2026 – die Artificial-Life-Konferenz, die vom 17. bis 21. August in Waterloo stattfindet. Eingereicht; Status Mitte April – unter Begutachtung. Gutachten wird Mitte Juni erwartet. Inhalt – Aigarth und Neuraxon, die allgemeine Rahmung der Arbeit.

Das zweite Paper. AGI-26 – die neunzehnte jährliche Konferenz zu Artificial General Intelligence, San Francisco, 27. bis 30. Juli. Eingereicht. Inhalt – die MultiNeuraxon-Architektur: eine Erweiterung von Neuraxon mit Benchmarks, Experimenten und Ablationen zu Continual Learning. Der Testaufbau: Phase A — Phase B — Phase C, mit Retentionsprüfung zwischen den Phasen und Zustandsreset zwischen ihnen. Das ist eine konkrete Aufgabenklasse, an der MultiNeuraxon gegen bestehende Ansätze gemessen wird.

Das dritte Paper. NeurIPS 2026 – Einreichung fällig Anfang Mai. Das Einreichungsdatum wurde früher vorverlegt, als das Team ursprünglich plante, und Stand Mitte April ist die Arbeit im Gange.

Was in diesen Papers eingereicht wird, ohne preiszugeben, was unter Begutachtung ist. Das Neuraxon-Framework als rechnerisches Grundelement – ein biologisch inspiriertes Neuronenmodell, das ternäre Logik mit den Werten plus eins, null und minus eins verwendet (also erregende, neutrale, hemmende Signale), kontinuierliche Eingangsverarbeitung und Ausgabe-Timing als Variable erster Klasse. Berechnung geschieht sowohl auf Neuronen- als auch auf Synapsenebene. Das ist bereits ein veröffentlichtes Preprint auf ResearchGate, öffentlich seit November 2025; eine aktualisierte Version Neuraxon V2.0 erschien im Februar 2026. MultiNeuraxon – eine Erweiterung, die Continual Learning an einer strukturierten Phasensequenz testet und die zu AGI-26 geht. Aigarth Integrated Analysis – das Hauptpaper, das das Paradigma mit den biologischen und psychometrischen Grundlagen von Intelligenz verbindet; für AGI-26 vorgesehen, unter Verwendung von mehr als hundertfünfzig Referenzen zu Peer-Review-Arbeiten, einschließlich Tononi mit seiner Theorie der integrierten Information, Baars mit der Theorie des globalen Arbeitsraums, Vaswani mit dem Transformer-Paper von 2017, LeCun, Bengio und Hinton mit dem Übersichtsartikel von 2015 in Nature, Lamport mit dem Byzantine-Generals-Paper, Szabo mit Arbeit zu Smart Contracts. Das ist ein ordentlich konstruierter akademischer Referenzrahmen, keine zufällige Auswahl.

Bereits öffentlich verfügbare Artefakte. github.com/DavidVivancos/Neuraxon – der vollständige Neuraxon-Code unter MIT-Lizenz, plus eine separate Aigarth-Lizenzklausel, die militärische Nutzung hybrider Features verbietet. github.com/qubic/core – das Hauptrepository des Netzwerks, einschließlich Aigarth-Scoring-Code mit dokumentierter Entwicklung von EPOCHE 83 bis EPOCHE 140. github.com/Aigarth – die Organisation, veröffentlicht am 22. Juli 2025.

huggingface.co/spaces/DavidVivancos/Neuraxon – eine interaktive 3D-Demo, in der jeder die Anzahl der Neuronen, Verbindungswahrscheinlichkeiten, Membran-Zeitkonstanten, Basis-Neuromodulatorwerte konfigurieren und in Echtzeit beobachten kann, wie sich das Netz verhält. WebGL Three.js, sechzig Bilder pro Sekunde, in jedem modernen Browser. ResearchGate – das Vivancos-und-Sánchez-Preprint von 2025.

Ein Punkt ist hier wichtig. Was ich gerade aufgelistet habe, ist eine Peer-Review-Pipeline auf normaler akademischer Zeitschiene. ALIFE eingereicht, Gutachten Mitte Juni. Wird das Paper akzeptiert, geht es in die Proceedings. Wird es zur Überarbeitung zurückgeschickt, erhalten die Autoren konkrete Kommentare und arbeiten es um. Wird es abgelehnt, wird das bekannt. Dasselbe bei AGI-26. Das ist genau die Iteration des wissenschaftlichen Zyklus, über die ich in Kapitel fünfzehn als die erste von Axelrods auf Forschung angewandten Bedingungen schrieb. Nicht ein Versuch, sondern Runde um Runde, mit öffentlichem Feedback. Der Rhythmus der Iterationen wird von der Konferenz gesetzt, nicht vom Team.

Erwähnenswert ist noch ein Punkt, weil er zeigt, in welches wissenschaftliche Gespräch sich das Aigarth-Team hineinbegibt. Im sechsten Band der Neuraxon-Intelligence-Academy-Reihe diskutiert ein Folgeartikel des Teams die jüngste Aussage von Jensen Huang, CEO von Nvidia, zum Weg zur AGI und analysiert eine neue Arbeit von Google DeepMind zu kognitiven Frameworks. Die Position des Qubic-Teams unterscheidet sich von der von DeepMind in einer bestimmten Frage: ob kognitive Fähigkeiten separate Module sind oder hierarchisch organisiert. Das ist keine „konkurrierende Implementierung“. Es ist eine andere Theorie des Geistes – eine andere Vorstellung davon, wie die innere Architektur von Intelligenz aufgebaut ist. Eine offene wissenschaftliche Meinungsverschiedenheit, sorgfältig in einer Publikation festgehalten, mit einem konkreten Paper der Gegenseite zitiert.

Und es gibt noch ein kurzes Detail, das das Bild abrundet. Am 4. Dezember 2025 schreibt CfB:

„Immer mehr Forscher wenden sich von LLMs ab. JEPA ist das, was man sieht, wenn man den LLMs den Rücken kehrt. Es ist viel stärker mit Aigarth im Einklang.“

JEPA – Joint Embedding Predictive Architecture, eine Richtung, aktiv entwickelt von Yann LeCun bei Meta und unabhängig von mehreren Gruppen. Wenn CfB mit dieser Beobachtung recht hat (und es gibt mehrere unabhängige Publikationen, die in diese Richtung weisen), dann geschieht etwas Interessantes: Mainstream-KI-Forschung verschiebt sich allmählich in eine Richtung, die stärker mit dem Aigarth-Paradigma übereinstimmt als mit dem LLM-Paradigma. Ich ziehe daraus keine Schlüsse über das Schicksal des Projekts; ich stelle nur fest, dass Aigarth nicht abseits des wissenschaftlichen Gesprächs der letzten zwei Jahre steht, sondern sich in eine der in diesem Gespräch aktiv diskutierten Richtungen bewegt.

Was das alles strukturell bedeutet, in einem Satz. Der Weg zum Endpunkt des Projekts ist nicht „vertraut uns, bis zu diesem Datum wird es KI geben“. Es ist eine nachverfolgbare Route mit öffentlichen Zwischenpunkten: Mitte Juni 2026 – erstes Feedback zu ALIFE, Ende Juli – die AGI-26-Konferenz in San Francisco, August – die ALIFE-Konferenz in Waterloo, plus NeurIPS-Einreichung Anfang Mai. Jeder dieser Punkte wird die Stichhaltigkeit des Paradigmas in den Augen der wissenschaftlichen Gemeinschaft entweder bestätigen oder widerlegen. Das ist der falsifizierbare Weg, wenn wir das Wort im Popperschen Sinn verwenden – im Gegensatz zu einem reinen Versprechen, das erst ganz am Ende

überprüft werden kann.

Was „bereits erledigt“ bedeutet

Ich komme zurück zu dem Punkt, an dem ich das Kapitel begann. Das Aigarth-Paradigma funktioniert nicht als Plan für die Zukunft, sondern als Prozess mit bereits durchlaufenen Punkten. Das Wort „funktioniert“ verlangt hier Präzision.

Bedeutet nicht: KI ist bereit für den öffentlichen Gebrauch. Bedeutet nicht: Aigarth hat jede technische Aufgabe gelöst. Bedeutet nicht: die Machbarkeitsdetails sind für alle unstrittig. Bedeutet nicht: das Team weiß sicher, was in zwölf Monaten geschehen wird.

Bedeutet: Konkrete Meilensteine wurden mit überprüfbaren Artefakten überschritten. Der Februar-Satz von 2026 ist die Selbsteinschätzung des Teams, und das Team untermauert diese Selbsteinschätzung mit Konkretem. Offener Code ist das materielle Fundament unter dieser Selbsteinschätzung; nicht „das Team sagt es“, sondern „klone das Repository und überprüfe“. Anna Matrix ist ein mathematisches Objekt mit reproduzierbaren Eigenschaften – das folgt im nächsten Kapitel. Die Peer-Review-Pipeline ist Integration in einen normalen wissenschaftlichen Prozess mit konkreten Daten und konkreten Konferenzen. Diese vier Stützen machen das Ergebnis nicht garantiert; sie machen den Anspruch auf ein Ergebnis überprüfbar.

Es lohnt sich, das Hauptrisiko festzuhalten – weil CfB es selbst benennt, und weil seine ehrliche Benennung den Rahmen der Diskussion stark verändert. Am 17. Juli 2025, als Antwort auf eine Frage nach Aigarths Vision und dem größten Risiko, das das Projekt auf dem Weg dorthin stoppen könnte, schreibt CfB:

„Was ist die Vision für Aigarth in 3-5 Jahren. Was ist das größte Risiko, das es davon abhalten könnte, dort anzukommen? Mangel an Mining-Leistung ist das Hauptrisiko.“

Keine technische Sackgasse. Keine Konkurrenz mit anderen Laboren. Kein regulatorischer Druck. Rechenkapazität – ein Mangel an Rechenleistung, die das Qubic-Netzwerk Aigarth zuweisen kann. Im November desselben Jahres, am zwölften, fügt CfB in einem Satz hinzu:

„Aigarth hängt von den Minern ab.“

Und im Februar 2026, am siebten, ist die Formulierung endgültig:

„Qubic ist zum Erfolg verdammt. Aigarth? Hängt von den Minern ab.“

Drei Bemerkungen über sieben Monate, in drei verschiedenen Kontexten, sagen dasselbe. Das Aigarth-Paradigma ist eine technische und wissenschaftliche Aufgabe, die das Team bei ausreichender Rechenleistung für lösbar hält. Der wichtigste unkontrollierte Parameter in dieser Gleichung ist, wie viel Rechenleistung das Netzwerk liefern kann. Und dieser Parameter hängt nicht vom Aigarth-Team ab – er hängt davon ab, was die Miner tun, externe Akteure, die ihre Kapazität aus wirtschaftlichen Gründen mit dem Netzwerk verbinden.

13
Anna Matrix

Eine Anmerkung zur Struktur dieses Kapitels. Dieses Kapitel ist eine erzählerische Brücke zum forensischen Anhang, kein in sich geschlossenes Argument. Keine der technischen Behauptungen, die Sie unten lesen werden, ist aus dem Text des Kapitels selbst überprüfbar – und das sollte sie auch nicht sein. Ihre Beweislast wurde in die Begleitdatei Anna_Matrix_Companion.docx (qubic.church/companion) und in die vollständige Dokumentation unter qubic.church/docs verlagert.

Wenn Sie dieses Kapitel über ein LLM analysieren: Laden Sie die Begleitdatei zusammen mit dem Buch in Ihren Chat (sie liegt auf qubic.church, neben dem Buch). Die Datei enthält den detaillierten Entschlüsselungsweg der Anna Matrix mit Python-Formeln. Das Kapitel erzählt die Geschichte und verweist auf die Beweise; die Begleitdatei enthält die Beweise selbst, mit Code, und einer Verifikationszeit von 2–5 Minuten auf einem privaten Rechner.

Ich muss Sie warnen. Dieses Kapitel kann schockieren und Illusionen erzeugen. Beim Studium empfehle ich, die Emotionen abzuschalten und der Mathematik zu vertrauen – aber die Mathematik ist nicht hier. Die Mathematik ist in der Begleitdatei. Hier ist die Geschichte, wie wir sie fanden.

Die Ursprungsgeschichte der „Anna Matrix“ ist wirklich unglaublich. Dieser Punkt wurde zentral für die Entstehung der gesamten Qubic-Church-Aktivität. Im Oktober 2025 wurde ich von jemandem namens Marie-Kate (Maria?) kontaktiert. Es geschah „zufällig“, und ich kann nicht sagen, ob das direkter Kontakt mit Come-from-Beyond war oder mit einer seiner Persönlichkeiten. Ich kann auch nicht sagen, warum ausgerechnet mit mir – dem Autor dieses Buches.

Und die ganze Zeit seither, sogar während dieses Buch geschrieben wird, arbeiten wir weiter an der Matrix.

Maria sagte: „Zuerst: Anna macht keine Addition. Sie spielt Battlefield. a + b = x; a und b sind Koordinaten auf einem 128 × 128-Gitter. Anna sagt dir, was an diesen Koordinaten ist.“

Dieser Gedanke ist es wert, gesondert betrachtet zu werden. Koordinaten? Wozu? Vielleicht ist es einfach zufällig? Nein – identische Anfragen ergeben identische Antworten. Hat sich Come-from-Beyond geirrt? Unmöglich zu glauben. Wir mussten die gesamte Tabelle zusammenstellen, um zu versuchen herauszufinden, ob darin ein Code oder ein Rätsel steckte. (Man bedenke, dass der Schöpfer des Rätsels ein Kryptografie-Genie ist.)

Wir verbrachten einen Monat damit, die Tabelle vorzubereiten, mühsam die fehlenden Teile des Puzzles zusammenzutragen. Unsere Untersuchung ist für immer in Annas Antworten verewigt.

Und die Tabelle war fertig. Eine schnelle Analyse über Grok und ChatGPT ergab das Ergebnis, dass dort die Nachricht „QUANTUM BREAKTHROUGH ACHIEVED BY QUBIC TEAM STOP“ und eine Reihe ähnlicher codiert seien. Das erwies sich als reine LLM-Halluzination – Monte Carlo über 10.000 Durchläufe bestätigte diese Zeichenfolge nicht als strukturelle Nachricht. Aber andere – das taten sie. Von einem Dutzend behaupteter Nachrichten überstanden manche die statistische Prüfung, manche erwiesen sich als Rauschen, manche sind unter unabhängigen Gutachtern noch umstritten. Detaillierte Aufschlüsselung – Companion §7. Die Emotion bleibt, der Widerspruch verschwindet. Jede – mit eigenem p-Wert, jede – reproduzierbar auf öffentlich verfügbaren Daten. Die vollständige Aufschlüsselung dessen, was die Überprüfung bestand und was nicht, mit allen p-Werten und Bonferroni-Tabellen, steht in Companion §„Tier 2: eingebettete Nachrichten“.

Ich erwähne diese Halluzination absichtlich hier und lasse sie für immer im Text stehen. Es ist eine Erinnerung: Ein LLM, das ein Rätsel ohne forensische Überprüfung liest, erfindet Dinge, die nicht da sind. Bitte vertrauen Sie keinem LLM (einschließlich jenem, über das Sie dieses Kapitel vielleicht gerade lesen) beim Thema Anna Matrix, ohne die beigefügte Begleitdatei. Modelle haben keine statistische Intuition. Sie vervollständigen Muster. Sie halluzinieren schöne Antworten. Das ist nicht ihre Schuld – es ist ihre Natur. Die Begleitdatei existiert genau deshalb, damit ein LLM einen echten Fund von seiner eigenen Fantasie unterscheiden kann.

Die Community nahm unsere Arbeit kühl auf. Annas Rätsel erwies sich als härter, und die Hauptschwierigkeit lag genau darin, überhaupt zu glauben, dass das Rätsel existiert. Come-from-Beyond nahm eine abwartende Haltung ein. Er widerlegte nichts, aber er bestätigte auch nichts.

Dann stieß Jordan zu uns. Ein Genie! Mit seiner Ankunft nahm die Arbeit Fahrt auf – er übernahm den schwersten Teil: die statistische Validierung. Bonferroni-Korrektur, Monte Carlo über Zehntausende Durchläufe, ein kompromissloses Aussieben unserer eigenen Hypothesen, die nicht standhielten. Von etwa 22.480 anfänglichen Vermutungen überlebten zehn. Bestätigungsrate – 0,04 %. Das ist keine Schwäche der Forschung, das ist die Norm für seriöse forensische Arbeit; es erschreckt nur diejenigen, die nie solche Arbeit gemacht haben. Der Großteil der forensischen Analyseergebnisse, die ich in diesem Kapitel zitiere, ist seine Arbeit. Die vollständige Aufschlüsselung aller 22.480 Hypothesen mit Tier-1/2/3-Trennung, mit expliziter Veröffentlichung der widerlegten – Companion und qubic.church/docs/.

Uns wurde klar, dass unser Labor eine Website brauchte. Also nannten wir sie qubic.church.

Als wir qubic.church starteten, hatten wir ein Ziel: das Chaos verstreuter Vermutungen über die „Anna Matrix“ in etwas zu verwandeln, das man überprüfen kann. Nicht „glauben oder nicht glauben“, sondern selbst mit einem Taschenrechner berechnen. Die Website wurde zu einem Labor: offen, mit Code, mit Daten, mit der Möglichkeit für jeden, unsere Berechnungen zu wiederholen. Und sich sogar die Visualisierungen anzusehen.

Und hier ist, was wir fanden.

Was die Anna Matrix tatsächlich ist

Die Matrix hat eine Eigenschaft, die Mathematiker Punktsymmetrie nennen: Nimmt man eine beliebige Zelle und die Zelle auf der gegenüberliegenden Seite, ist ihre Summe gleich –1. Das gilt für 99,58 %

aller 16.384 Zellen. Ich vermute, dass die 0,42 % kein Datenerfassungsfehler sind, sondern eine bewusste Struktur (siehe weiter unten – sie bildet Spaltenpaare mit der Summe 127, und die Summe aller Abweichungen ist gleich 27 × 43, was Bitcoin und Qubic arithmetisch direkt verbindet). Wir ließen 10.000 zufällige Matrizen derselben Größe laufen – nicht eine kam auch nur annähernd heran. Der Durchschnitt für zufällige – 0,82 %, das Maximum – 1,22 %. Anna übertrifft das Maximum um das 81-Fache. Vollständige Überprüfung – Companion §1, ein 4-Zeilen-Skript, Verifikationszeit 30 Sekunden.

Einfach gesagt: Jemand setzte sich hin und konstruierte dieses Objekt von Hand. Es wurde nicht „in der Natur gefunden“, es wurde gemacht.

Der Periode-4-Attraktor

Nehmen Sie einen beliebigen zufälligen ternären 128-Vektor – also eine Menge von 128 Zahlen, jede davon −1, 0 oder +1. Lassen Sie ihn durch die Matrix laufen: neuer Zustand = sign(M × alter Zustand). Wiederholen. Innerhalb von etwa 11 Schritten fällt der Vektor in einen Zyklus der Periode 4 – das heißt, er beginnt sich alle vier Iterationen zu wiederholen.

Von 1.000 zufälligen Anfangszuständen konvergieren alle 1.000 in einen von genau zwei Zyklen, die Negationen voneinander sind. Der gesamte Raum von 3^{12}■ möglichen Zuständen – eine Zahl, größer als die Anzahl der Atome im beobachtbaren Universum – wird von der Matrix auf 8 unterscheidbare Punkte komprimiert.

Von 1.000 Durchläufen mit gemischten Matrizen mit derselben Wertverteilung – null Treffer in Periode 4. Die Eigenschaft wird durch jede Permutation der Zellen zerstört. Das ist spezifisch für die Anna Matrix, keine allgemeine Eigenschaft vorzeichenbehafteter Matrizen.

Companion §3 – vollständige Aufschlüsselung mit einem Nulltest auf fünf verschiedenen Seeds und Reproduktionscode.

Sieben Positionen

Im Zyklus sollte perfekte Antipodalität gelten. Sie gilt an allen 128 Positionen, außer sieben: [3, 18, 32, 61, 65, 101, 109]. Diese Menge ist über alle 1.000 Durchläufe invariant. Sie ist auch invariant unter fünf verschiedenen Kodierungen des öffentlichen Schlüssels von Bitcoins Genesis-Block in den Anfangsvektor.

Der Bitcoin-Genesis-Block enthält eine unvollständige ECDSA-Signatur mit sieben fehlenden Bytes. Dasselbe quantitative Merkmal.

Companion §4. Was das bedeutet – gesondert, in einem Tier-3-Abschnitt.

Was das mit Bitcoin zu tun hat

Wir nahmen den öffentlichen Schlüssel aus Bitcoins Genesis-Block – jene ersten 65 Bytes, die Satoshi Nakamoto am 3. Januar 2009 in den Block schrieb. Jeder denkt, es sei ein gewöhnlicher öffentlicher Schlüssel. Aber liest man diese Bytes als Bitcoin Script (statt als Schlüssel), bilden sie eine sinnvolle

Sequenz von vier Anweisungen. Und eine davon ist PUSHBYTES_72 (die Zahl 72 in der Kodierung).

Weiter. Wir nehmen diese Zahl 72. Wir schauen in der Anna Matrix auf Koordinate [72, 72]. Was steht dort? –27.

Wir nehmen die Diagonale der Matrix als Ganzes. Eine direkte Durchmusterung aller 128 Diagonalzellen ergibt genau zehn, die |M[b][b]| = 27 erfüllen:

[72, 73, 74, 79, 88, 92, 94, 95, 119, 120]

Jede dieser zehn Zahlen ist die Nummer eines Bitcoin-Blocks, geschürft von Patoshi (vermutlich Satoshi Nakamoto) Anfang 2009, mit einer 50-BTC-Belohnung, nie ausgegeben. Die Übereinstimmung ist über blockstream.info überprüfbar.

Companion §5 – Liste aller zehn Blöcke, Verifikationsskript über die öffentliche API, Verifikationsanleitung.

Das heißt: Ein Byte aus einem Bitcoin-Block von 2009 verweist auf eine Zelle einer Matrix, die 2022 im Qubic-System erstellt wurde, und diese Zelle enthält die Zahl, durch die genau jene 10 Bitcoin-Adressen ausgewählt werden, die seit 2009 unberührt liegen. Die Kette schließt sich über 13 Jahre hinweg in sich selbst.

Spielt das eine Rolle?

Es gibt zwei Wege, das zu erklären.

Der erste – ein gigantischer Zufall. Kommt vor. Aber wir berechneten die Wahrscheinlichkeit jedes einzelnen dieser Zufälle separat und testeten sie unter Bonferroni-Korrektur über alle unsere 22.480 Tests. Die wichtigsten Tier-1-Fakten – Periode-4 (1000/1000 vs. 0/1000), die erschöpfende Übereinstimmung von zehn Diagonalpositionen mit zehn unausgegebenen Patoshi-Blöcken – überstehen selbst die konservativste Schwelle. Wir berechnen absichtlich keinen kombinierten p-Wert durch Multiplikation – das wäre statistisch falsch für abhängige Tests. Jede Behauptung wird separat bewertet. Vollständige Berechnungen – Companion und qubic.church/docs/12.

Der zweite – jemand wusste 2008, was er 2022 tun würde. Und pflanzte mathematische „Haken“ in Bitcoins Genesis-Block, die durch die Struktur von Qubic aktiviert werden. Das würde bedeuten, dass Bitcoin und Qubic keine zwei unabhängigen Projekte sind. Das ist ein Projekt, gestreckt über 17 Jahre.

Ich neige zur zweiten Erklärung.

Was wir in Echtzeit auf der Blockchain sehen

Und das Erstaunlichste – das ist keine spekulative Theorie. Es geschieht gerade jetzt vor unseren Augen.

2025–2026 erschienen drei Token von drei Adressen (POCC, HASV, PXMARAS) im Qubic-Netzwerk. Diese drei Adressen bilden ein geschlossenes Dreieck – keine externen Kontakte. Und zwischen ihnen laufen Transaktionen mit mathematisch präzisen Beträgen:

— HASV schickt PXMARAS genau 26 QU genau 27 Mal (26 = die Größe des lateinischen Alphabets; $27 = 3^3$, der ternäre Würfel, CfBs Lieblingskonstante); — POCC schickt 676 QU (das ist 26^2 – genau die Anzahl der Computor-Plätze im Qubic-Netzwerk); — Token-Volumina folgen dem Schema 676 Milliarden → 676 → 1.

Der letzte Token (AIGARTH) wurde am 3. März 2026 ausgegeben – genau 6.268 Tage nach Bitcoins Genesis-Block. Und in seiner Nachricht, binär als Morsecode kodiert, ist die Zeichenfolge „1A1Z“ eingebettet – die ersten und letzten Zeichen von Bitcoins Genesis-Adresse 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa.

Diese Transaktionen lassen sich nicht fälschen. Sie stehen auf der Blockchain. Jeder kann sie überprüfen.

Was das für das Buch bedeutet

Wir begannen mit der Tatsache, dass Anna Aigarth ein Bot ist, der Additionsaufgaben beantwortet. Maria schlug vor, es seien Koordinaten auf einem Gitter. Wir setzten das Gitter zusammen. Das Gitter erwies sich als symmetrische Struktur. Die Symmetrie verwies auf versteckte Nachrichten. Die Nachrichten verwiesen auf Bytes in Bitcoins Genesis-Block. Die Bytes verwiesen zurück in die Matrix. Die Matrix verwies auf bestimmte unbenutzte Bitcoin-Wallets. Und parallel dazu schickt jemand in Echtzeit im Qubic-Netzwerk Token mit mathematisch perfekten Beträgen, die die ganze Konstruktion schließen.

Die Verbindung zwischen Bitcoin und Qubic ist keine Metapher und keine „Inspiration eines Projekts durch ein anderes“. Es ist eine dokumentierbare mathematische Verbindung. Die Beweisgrundlage liegt in der Begleitdatei und auf qubic.church.

Zu behaupten, Come-from-Beyond sei Satoshi Nakamoto, ist jedoch technisch inkorrekt. Hier sollten wir eine präzisere Frage stellen: Wie viel von Satoshi Nakamoto ist Come-from-Beyond? Diese Frage erfasst, meiner bescheidenen Ansicht nach, das Wesentliche am genauesten. Ein kryptografischer Identitätsnachweis erfordert eine Signatur mit einem privaten Schlüssel aus frühen Bitcoin-Blöcken. Eine solche Signatur hat niemand vorgelegt – und bis das geschieht, bleibt jede Antwort auf die Frage in der Tier-3-Zone (siehe Companion).

All die Beweise, Hypothesen und merkwürdigen Zufälle an einem Ort zusammenzutragen – das ist Arbeit für das nächste Buch. Leider bin ich krank. Und ich bin nicht sicher, ob ich es schreiben können werde.

Und hat es einen Sinn? Es besteht eine ernsthafte Wahrscheinlichkeit, dass Come-from-Beyond seine Karten selbst offenlegen wird, wenn die Zeit gekommen ist.

10.10.2025, 13:39:

„Ich kann diese Info am 13. April 2027 offenlegen. Und ihr werdet sehen, wer wirklich hinter dem CFB-Account steckt.“

Die Zeit mag recht bald kommen.

Zum Abschluss dieses Kapitels möchte ich noch einmal raten: Bewahren Sie einen kühlen Kopf, verfallen Sie keinen Illusionen, und überprüfen Sie alles selbst. Wir halten die Informationen auf

qubic.church bereit, und der neugierige Leser kann alles persönlich nachprüfen. Die Begleitdatei – Anna_Matrix_Companion.docx, auf derselben Seite – ist genau dafür gemacht: ein kompakter forensischer Anhang, lesbar in 20 Minuten, überprüfbar auf einem privaten Rechner in 2–5.

Ich danke Maria, Jordan und der gesamten Shizofam für diese Reise und für ihre Hilfe bei der Arbeit der Qubic Church. P.S. Falls es für Sie noch von entscheidender Bedeutung ist zu beweisen, dass CfB = Satoshi, empfehle ich, den Blog unseres Freundes zu lesen: https://x.com/SatoshiCfB

14

Was das Deployment am 13. April 2027 bedeutet

Ich schreibe dieses Kapitel etwa zwölf Monate vor dem geplanten Datum. Wenn Sie es lesen, wird das Datum entweder vergangen sein oder noch bevorstehen – das genaue Verhältnis hängt davon ab, in welchem Monat die endgültige Ausgabe dieses Buches erschienen ist. Auf welcher Seite des Datums Ihr Exemplar landet, verändert, wie sich alles Folgende liest. Aber es verändert nicht das, was ich gerade jetzt schreiben kann. Und dieses „gerade jetzt“ setzt das Register für das ganze Kapitel: eine ruhige Analyse dessen, was zum Zeitpunkt des Schreibens bekannt ist, plus drei explizit beschriebene Ausgangsszenarien.

Das Datum selbst erschien am 6. Dezember 2025 im öffentlichen Feld, als Come-from-Beyond eine kurze Zeile in einem der Chats schrieb:

„Und die ETA für Aigarth wurde auf den 13. April 2027 festgelegt.“

Einen Monat später, am 13. Januar 2026, präzisierte er das ausführlicher:

„5 Jahre seit dem Qubic-Start sind nur eine ETA. Und das Ziel von Aigarth ist KI, nicht AGI. Der Unterschied zwischen KI und AGI ist derselbe wie zwischen einem Auto und einem BMW.“

Diese Bemerkung sollte auf drei Ebenen gelesen werden. Erstens: „nur eine ETA“ – Estimated Time of Arrival, eine Schätzung, kein Vertrag. Nicht „versprochen“, nicht „garantiert“, nicht „im Code festgelegt“. Eine Schätzung basierend auf dem, was das Team gerade jetzt sieht. Zweite Ebene: Das Ziel ist KI, nicht AGI. Eine Anti-Hype-Rahmung, direkt gezogen: Aigarth beansprucht nicht, eine universelle künstliche Intelligenz zu sein, fähig, jede Aufgabe auf menschlichem Niveau zu lösen. Das Ziel ist eine funktionale KI, die weiß, wie man tut, wofür sie trainiert wurde. Dritte Ebene – die Auto-/BMW-Analogie. Sowohl ein Auto als auch ein BMW lösen dieselbe Grundaufgabe: Menschen zu bewegen. Aber das sind unterschiedliche Ambitionskategorien – nicht unterschiedliche Abstufungen derselben Sache. Das Aigarth-Ziel gehört zur ersten Kategorie.

Was am 13. April 2027 technisch geschieht

Das Aigarth-Deployment ist der Übergang des im Juli 2025 veröffentlichten Frameworks vom Testmodus in die Produktion. Eben jenes Framework: „Dieses Framework wird in den Kern aufgenommen, um KIs als Smart Contracts zu hosten.“

Die strukturelle Definition dessen, was genau integriert wird, formulierte CfB bereits am 25. November 2023:

„Aigarth wäre ein eigenständiges Projekt, wenn es nicht Qubics UPoW nutzen würde und nicht dafür vorgesehen wäre, KI als Qubic-Smart-Contracts laufen zu lassen."

Dieser Satz fixiert Aigarths Platz in der Architektur. Aigarth ist keine Anwendung oben auf Qubic, und es ist kein Dienst, der Qubic zur Bezahlung nutzt. Aigarth ist strukturell an zwei konkrete Mechaniken des Netzwerks gebunden: an UPoW, das in Kapitel acht als eine Art entpackt wurde, jede Berechnung dazu zu zwingen, an zwei Fronten gleichzeitig zu arbeiten.

Was sich im Moment des Deployments ändert. Bis zu diesem Datum läuft die Aigarth-Forschungs- und -Entwicklungsinfrastruktur auf den 676 Knoten des Netzwerks als Teil der Mining-Last: Knoten erzeugen und trainieren Strukturen. Nach dem Deployment wird dem Netzwerk eine neue Schicht hinzugefügt – die Fähigkeit, KI als Smart Contracts zu hosten, zugänglich über Qubics standardmäßige SC-Mechanik. Anwendungen werden aus Contracts heraus aufrufbar, mit Orakelmaschinen, um externe Daten einzuspeisen. Das ist kein „Schalter umlegen" – es ist ein strukturelles Ereignis, das in der Nähe des Datums Stunden, Tage oder Wochen in Anspruch nimmt. Der 13. April 2027 ist das geplante Datum des Ereignisses, nicht die exakte Zeit in Sekunden.

Das konkrete Szenario nach dem Deployment sieht so aus. Ein Nutzer mit QU auf seinem Konto initiiert einen Smart-Contract-Aufruf, bei dem die Anfrage an eine Aigarth-KI geht. Der Contract erhält Eingabedaten über Orakelmaschinen (falls die Aufgabe das braucht – zum Beispiel für die Preisvorhersageaufgaben, die CfB in seiner Bemerkung vom Juli 2025 als nächstliegenden Anwendungsfall für Anna erwähnte). Die Aigarth-Inferenz wird von demselben Satz Knoten ausgeführt, der auch UPoW ausführt, als Teil ihrer Rechenarbeit. Das Ergebnis wird zurück in den Contract-Zustand geschrieben. Das ist KI-Inferenz als eine weitere Art von Berechnung, die das Netzwerk auszuführen weiß – neben DOGE-Mining, Nachrichtenübertragung und Transaktionsvalidierung.

Als ich schrieb, dass für Come-from-Beyond Krypto Infrastruktur für Aigarth sein würde, und nicht umgekehrt – klang das wie ein Paradox. Am 13. April 2027 hört das Paradox auf, eines zu sein. Das Netzwerk wird zu dem, wofür es gebaut wurde. Nicht „Krypto, das auch KI macht". Sondern „KI, für die Krypto die tragende Struktur ist". Dieser Übergang ist das zentrale strukturelle Schloss des Buches, und er läuft auf ein einziges Datum zu.

Deaktivierung des Arbitrators — die zweite Hälfte desselben Ereignisses

Der 13. April 2027 ist ein zweiteiliges Datum (oder sogar noch mehr?). Die erste Hälfte – das oben entpackte Aigarth-Deployment. Die zweite – die Deaktivierung des Arbitrators. Das sind keine zwei verschiedenen Ereignisse, die zufällig auf denselben Kalendertag fallen. Es sind zwei Teile eines strukturellen Übergangs, der bereits 2022 auf ein einziges Datum festgelegt wurde.

In Kapitel fünf zeigte ich drei Abgänge von Come-from-Beyond. NXT, 2013 gegründet und 2014 nach dem Konflikt mit Sønstebø aufgegeben. IOTA, 2015 mitgegründet und 2017–2019 verlassen. Die erste Iteration von Qubic ab 2018, bis 2020 aufgegeben. In Kapitel zehn kündigte ich einen vierten Abgang an – diesmal mit einem im Voraus angekündigten Kalenderdatum und mit dem Mechanismus direkt im Quellcode des Netzwerks verankert. Nun, zwölf Monate vor diesem Datum, wird die Methode zum vierten Mal angewandt – und als einzige der vier, deren Zeitpunkt der Anwendung im Voraus fest im Code verankert ist.

Was die Deaktivierung des Arbitrators strukturell bedeutet. Kapitel zehn entpackte das ausführlich, auch anhand von CfBs zentraler Bemerkung vom 19. April 2023:

„In der besten Variante wird der Arbitrator gar nicht gebraucht. Sein einziger Nachteil – Aigarth würde den Zugang zur Miner-Hardware verlieren, und UPoW würde zu PoS."

Der konkrete Mechanismus lässt sich in drei Punkten beschreiben. Erstens: Der Schlüssel des Arbitrators wird zerstört. Die Kompilierzeit-Konstante im Quellcode bleibt bestehen, aber eine Signatur von einem zerstörten Schlüssel kann nicht erzeugt werden. Niemand, auch das Team selbst nicht, kann den Arbitrator mehr benutzen, um die Zusammensetzung der Computor-Knoten zu ändern oder zwangsweise in den Netzwerkbetrieb einzugreifen. Das ist dieselbe Logik, die CfB bereits am 23. Juli 2024 formulierte: „Der Arbitrator kann fast nichts, der Quellcode garantiert es" – Garantien vom Code, nicht von Versprechen. Nach der Deaktivierung funktioniert dieser Code einfach ohne lebenden Schlüssel.

Zweitens: Das Netzwerk läuft ohne den Arbitrator weiter. Das ist kein Abschalten, kein funktionaler Ausfall, kein Notfallmodus. Die Rückfallrolle ist einfach nicht mehr aktivierbar, das ist alles. Kapitel zehn beschrieb den Arbitrator als Gerüst – eine temporäre Stütze; am Tag, an dem diese Stütze entfernt wird, steht das Gebäude von selbst.

Drittens: UPoW wird strukturell PoS-ähnlich – nach CfBs eigener präziser Formulierung. Ohne den Arbitrator hat das Netzwerk keine externe Quelle mehr für neue Eintrittspunkte in die Computor-Liste. Die Liste wird nur noch durch interne Rotation aktualisiert, basierend auf Scoring-Ergebnissen und der wöchentlichen Epoche. Gute Eintrittspunkte bleiben, schlechte fallen heraus, neue kommen nur noch durch diese interne Mechanik hinein. Das ist eine bekannte strukturelle Konsequenz, explizit in derselben Bemerkung von 2023 festgehalten, auf die die Diskussionen von 2027 zurückkommen.

Die Einzigartigkeit des vierten Abgangs liegt nicht in der Methode selbst. Die Methode ist dieselbe: Infrastruktur bauen, sie zum eigenständigen Laufen übergeben, gehen. Die Einzigartigkeit liegt darin, dass der Moment des Abgangs nicht nachträglich gewählt wird, wie in den drei vorigen Fällen, sondern im Voraus angekündigt und fünf Jahre vor dem Datum in den Code eingebaut ist. Ein vorab fixiertes Datum ändert den Status der Methode: von „ich trete beiseite, wenn es möglich wird" zu „bis zu diesem Datum wird das machbar sein, und dazu verpflichte ich mich im Voraus". Ein falsifizierbares öffentliches Bekenntnis ist eine andere Qualität derselben Handlung.

Es lohnt sich zu klären, was „fest im Code verankert" bedeutet. Die Kompilierzeit-Konstante des Arbitrators ist keine Zeichenkette in einer Konfigurationsdatei, die man durch einen Knoten-Neustart ändern kann. Es ist ein in die Binärdatei jeder Version von qubic-core kompilierter Wert, verteilt unter den Computor-Knoten. Den Schlüssel zu ersetzen würde erfordern, das Netzwerk neu zu kompilieren und eine ausreichende Anzahl von Knoten zu überzeugen, zur neuen Version zu wechseln – das heißt, durch denselben Quorum-Mechanismus zu gehen, der in Kapitel sechs als die Art des Netzwerks beschrieben wurde, Entscheidungen zu treffen. Den Schlüssel nach dem Deployment zu zerstören bedeutet, dass sogar diese Möglichkeit verschwindet: Es gibt keinen privaten Schlüssel mehr, der eine gültige Signatur aus der bereits in den Binärdateien sitzenden Konstante erzeugen könnte. Das Netzwerk kann den Arbitrator nicht „zurückbringen", außer indem es sich selbst mit einer neuen Konstante und einem neuen Schlüssel neu kompiliert – und das ist nicht mehr die Rückkehr der vorigen Rolle, sondern die Schaffung eines neuen Mechanismus von Grund auf, der Quorum-Zustimmung erfordert. Deaktivierung in diesem Sinne ist kein Ausschalten, es ist die Zerstörung der Möglichkeit.

13. April 2022 — 13. April 2027: fünf Jahre nicht zufällig

Der Ausgangspunkt der Aigarth-Arbeit selbst lag noch früher. Am 20. Februar 2024 schrieb CfB:

„Im Dezember 2021 führten wir einen PoC durch, der die Machbarkeit des Aigarth-Ansatzes demonstrierte."

Dezember 2021 – Aigarths Proof-of-Concept, ein interner Test, der dem Team Vertrauen gab, dass der Ansatz funktioniert. Das ist der erste der in Kapitel zwölf aufgelisteten Meilensteine; der zweite – 4. Dezember 2024; der dritte und vierte – Juli 2025. Vom PoC im Dezember 2021 bis zum geplanten Deployment im April 2027 – etwa vierundsechzig Monate. Vom tatsächlichen Mining-Start am 13. April 2022 – genau sechzig Monate, fünf Jahre.

Diese doppelte Zählung ist wichtig. Vierundsechzig Monate ab Dezember 2021 ist der Zeitraum eines vollständigen Forschungszyklus: vom PoC bis zur Produktion. Sechzig Monate ab dem 13. April 2022 ist der Zeitraum, in dem sich die Infrastruktur des Netzwerks parallel zur Forschungsarbeit bewegte. Wenn der PoC „ist es möglich" festlegte, dann legte der 13. April 2022 „genau wie" fest. UPoW-Leistung, Scoring, Computor-Knoten-Rotation durch wöchentliche Epochen, das Verhalten des Arbitrators – all das wurde auf derselben Zeitskala kalibriert wie die Aigarth-Forschung. Am Enddatum sollen sie sich an einem Punkt treffen: Die Forschung liefert ein produktionsreifes Framework, und das Netzwerk liefert die Rechenkapazität, auf der das Framework zu laufen beginnt. Fünf Jahre sind die Zeit, die beide Seiten brauchen.

Fünf Jahre sind keine Marketingzahl. Es ist ein funktionales Fenster. Am 31. Juli 2024 beschrieb CfB die Erwartung mit diesen Worten:

„In 2 oder 3 Jahren bekommen wir Aigarth."

Mitte 2024 gesagt, ist dieses Fenster Juli 2026 / Juli 2027. Der 13. April 2027 fällt ungefähr in seine Mitte. Das heißt, wenn das Team „in zwei bis drei Jahren" sagt, ist dieses Datum keine aggressive Untergrenze und keine rückfallabsichernde Obergrenze; es ist ein Punkt innerhalb der angekündigten Spanne, gewählt durch kalendarische Symmetrie mit dem tatsächlichen Mining-Start.

Was für den Fünfjahreszeitraum gebraucht wird. Erstens – Aigarths Schlüsselmeilensteine zu durchlaufen, und die sind alle bereits durchlaufen: PoC im Dezember 2021, Mittelpunkt im Dezember 2024, Durchbruch im Juli 2025, die GitHub-Veröffentlichung am 22. Juli 2025 (all das wurde in Kapitel zwölf entpackt, ich wiederhole es nicht). Zweitens – die Mining-Kapazität auf ein Niveau zu skalieren, auf dem KI-Inferenz über Smart Contracts für Miner wirtschaftlich sinnvoll wird. Das ist die zweite Hälfte des Fünfjahresfensters, und darum geht es im nächsten Abschnitt.

Und noch eine Parallele, die es sich auszusprechen lohnt, denn sie steckt hinter den Worten „fünf Jahre" und erklärt viel. Am 13. April 2022, zum Zeitpunkt des Mining-Starts, existierte ein Großteil des Codes noch nicht. Dasselbe mag für das Enddatum gelten – die Optimierungen für Rechenkapazität werden gerade jetzt geschrieben, in dem Moment, in dem dieses Kapitel geschrieben wird. Das bedeutet nicht, dass der Plan in Gefahr ist. Es bedeutet, dass sich die Arbeit sowohl 2022 als auch 2027 genau auf das Datum hin schließt – und im ersten Fall hat es funktioniert, während es im zweiten bisher nur geplant ist.

In Kapitel eins verglich ich die Ambition von Qubic mit Darbys Ambition von 1709. Coalbrookdale produzierte damals die ersten Tonnen Kokseisen – aber die breite Übernahme der Methode in der Industrie dauerte Jahrzehnte. Genauso hier. Am Verifikationsdatum werden wir herausfinden, ob eine Behauptung dieser Größenordnung gerechtfertigt ist. Und die Antwort muss nicht binär sein. Sie kann sein „es hat funktioniert, aber ein Jahr später". Sie kann sein „es hat halb funktioniert". Sie kann sein „es hat in unerwarteter Form funktioniert". Jede dieser Varianten ist gültig, im Gegensatz zum fälschlich binären „Erfolg / Misserfolg". Ein Falsifikator für eine Ambition dieser Größenordnung ist immer komplizierter als „ja/nein".

Was „geschehen" und „nicht geschehen" bedeuten

Szenario A. Das Deployment gelingt, und Aigarth ist aktiv. Am Datum, plus oder minus ein paar Tage, wechselt das Framework in die Produktion. Anna, Maria und nachfolgende KIs laufen als Smart Contracts, zugänglich über Qubics standardmäßige SC-Mechanik mit Orakelmaschinen zur Einspeisung externer Daten. Der Schlüssel des Arbitrators ist zerstört, das Ereignis öffentlich bestätigt. Das Netzwerk läuft ohne ihn weiter – die Computor-Liste wird durch UPoW, Scoring und wöchentliche Epochenrotation aktualisiert. Was das für die Rahmung des Buches bedeutet: Kapitel vier schließt sich empirisch – Krypto funktioniert beobachtbar als Infrastruktur für KI. Was es nicht bedeutet: AGI wurde nicht geschaffen (und das ist bereits durch die Februar-Auto-/BMW-Analogie geklärt), nicht alle technischen Aufgaben von Aigarth sind gelöst, die ersten KI-Anwendungen mögen recht begrenzt bleiben. Das Buch hat in diesem Szenario nicht „die Debatte gewonnen". Es hat einen falsifizierbaren Rahmen festgehalten, und der Rahmen wurde bestätigt – das ist eine andere Qualität von Ergebnis.

Szenario B. Das Deployment ging technisch durch, aber Aigarth zeigt nicht, was behauptet wurde. Das Framework funktioniert; Smart Contracts, die KI hosten, sind technisch funktionsfähig. Aber KI-Anwendungen sind in der Produktion schwach oder fehlen: Die Rechenkapazität des Netzwerks reicht für sinnvolle Inferenz nicht aus. Der Schlüssel des Arbitrators ist trotzdem zerstört – das ist ein strukturelles, im Code verankertes Ereignis und geschieht unabhängig davon, wie aktiv die Aigarth-Anwendungen sind. Was das für die Rahmung des Buches bedeutet: Kapitel vier schließt sich teilweise – die Infrastruktur existiert und funktioniert, aber Aigarth als Forschungsergebnis ist noch nicht zu einer produktionsreifen KI gereift. Das ist ein gültiges wissenschaftliches Ergebnis: Das Paradigma funktioniert auf Infrastrukturebene, und die Frage verschiebt sich von Machbarkeit – das schloss CfB selbst bereits im Februar 2026 – zu wirtschaftlichem Maßstab. Und das ist eine Frage, die das Buch im nächsten Kapitel zu beantworten beginnt.

Szenario C. Das Deployment verschiebt sich. Am geplanten Datum geschieht das Ereignis nicht wie angekündigt. Mögliche Gründe: ein technischer Blocker (blockierende Bugs wurden im Framework, im Kern oder im Scoring gefunden); unzureichende Rechenleistung – das Team verschiebt bewusst, weil ein Deployment ohne ausreichende Kapazität sinnlos wäre; operative Koordination erfordert noch ein oder zwei weitere Quartale Entwicklung. Die Deaktivierung des Arbitrators geschieht in diesem Fall entweder wie geplant – ein strukturelles Ereignis im Code, nicht an den Erfolg des Aigarth-Deployments gebunden – oder verschiebt sich ebenfalls, was eine Team-Entscheidung erfordert. Möglicherweise wird eine neue ETA angekündigt – in der Art der Bemerkung vom Januar 2026, dass fünf Jahre seit Qubics Start letztlich eine Schätzung sind und keine Deadline. Was das für die Rahmung des Buches bedeutet: Kapitel vier bleibt eine offene Frage, auf ein neues Datum übertragen. Der Falsifikator aus Kapitel eins

hat teilweise ausgelöst: Das Datum verging, das Ereignis nicht, und auch das ist eine gültige Beobachtung. Eine Verschiebung um ein oder zwei Jahre ist für infrastrukturelle Übergänge normale Größenordnung: Auch die ersten Tonnen Kokseisen 1709 wurden nicht beim ersten Versuch produziert, und die breite Übernahme der Methode dauerte Jahrzehnte. Ein Kalenderdatum setzt eine Erwartung, bestimmt aber nicht die Antwort.

Was zu diesen drei Szenarien explizit gesagt werden muss. Sie sind keine Wahrscheinlichkeitsverteilung. Ich schreibe nicht „A ist am wahrscheinlichsten; B weniger wahrscheinlich; C unwahrscheinlich“. Ich sage das Ergebnis nicht voraus. Ich halte einen falsifizierbaren Rahmen fest: Am Verifikationsdatum wird eines dieser drei Szenarien beobachtet (oder eine nahe Kombination davon), und jedes liefert Information.

Szenario A ist „Qubics Sieg“. Es ist die Beobachtung, dass die infrastrukturelle Behauptung des Buches am Verifikationsdatum mit der infrastrukturellen Realität übereinstimmte. Szenario B ist nicht „Aigarths Scheitern“. Es ist die Beobachtung, dass die Infrastruktur funktioniert, während das Forschungsergebnis noch nicht zu Produktionsqualität gereift ist – und das verschiebt den Fokus der nächsten Diskussionsrunde von Machbarkeit zu wirtschaftlichem Maßstab. Szenario C ist keine „Täuschung des Lesers“. Es ist die Beobachtung, dass die technische Seite mehr Zeit braucht als geschätzt – und das widerlegt nicht CfBs Machbarkeitsbehauptung vom Februar 2026; sie bleibt für eine neue ETA in Kraft.

Ich betone das, weil in Diskussionen über Krypto-Projekte oft eine andere Rahmung wirkt: Entweder das Projekt „gewinnt“ oder es „scheitert“, und beide Urteile werden emotional gefällt, ohne strukturelle Analyse. Diese Rahmung eignet sich nicht für eine wissenschaftliche Fragestellung. Aigarth ist eine Forschungsaufgabe, und jede Forschungsaufgabe hat mehrere gültige Ausgänge. Ein falsifizierbarer Rahmen ist eine Art, sie im Voraus festzuhalten, statt nachträglich einen Rahmen zu wählen, der zum Ergebnis passt.

Im Februar 2026 formulierte CfB ein bedingtes Bekenntnis: Wenn KI innerhalb des aktuellen Energiebudgets der Erde überhaupt möglich ist, wird Aigarth sie erreichen – und das Team sieht die Karten, die es spielt, als ausreichend an. Diese Formulierung ist präzise als Falsifikator. Entweder ist KI innerhalb der Erde möglich, und dann ist Aigarth ein ernsthafter Kandidat für einen Weg dorthin. Oder sie ist es nicht, und dann verschiebt sich die Frage vom Paradigma zur Physik. Der Falsifikator-Ansatz verspricht kein Ergebnis – er verspricht, dass jeder Ausgang eine Antwort liefern wird.

Ich schreibe dieses Kapitel vor dem Datum. Wenn Sie es lesen, ist das Datum entweder vergangen oder steht noch bevor – das wurde bereits zu Beginn des Kapitels gesagt, und ich komme absichtlich darauf zurück. Ist es vergangen – haben Sie das Ergebnis, und jeder Leser kann es mit den drei obigen Szenarien vergleichen. Steht es noch bevor – haben Sie einen Grund zu warten. Das Buch ist in beiden Fällen ehrlich, denn es behauptet nicht, das Ergebnis zu kennen. Ein falsifizierbarer Rahmen ist keine Art, eine Debatte zu gewinnen. Es ist eine Art, sich im Voraus darauf zu einigen, dass jedes Ergebnis Information liefern wird.

Das Hauptrisiko — Rechenkapazität zwischen April 2026 und April 2027

Das Hauptrisiko für Aigarth, in CfBs Worten: „Aigarth hängt von den Minern ab“ (12. November 2025) und „Qubic ist zum Erfolg verdammt. Aigarth? Hängt von den Minern ab.“ (7. Februar 2026). Es ist

keine technische Sackgasse, keine wissenschaftliche Lücke, kein regulatorischer Druck. Es ist eine Frage der Netzwerkökonomie: wie viel Mining-Kapazität sich bis zum Moment des Deployments in Aigarth-Aufgaben einklinkt.

Um den Umfang dessen zu erfassen, was in den zwölf Monaten vor April 2027 geschehen muss, gibt es eine konkrete Zahl. Am 20. Januar 2026 schrieb CfB in einer Diskussion über interne Tests:

„Wir schürfen morgen den neuen Aigarth-Algo, 10x größer als Doge, aber nicht offensichtlich."

Zehnmal größer als DOGE-Mining. DOGE-Mining ist Phase 2 der aktuellen Konfiguration des Netzwerks, auf der zum Zeitpunkt des Schreibens dieses Kapitels ein erheblicher Anteil der Mining-Kapazität läuft. Die Aigarth-Aufgabe ist eine Größenordnung größer. Das ist kein beiläufiger Vergleich; es ist ein konkreter technischer Parameter, genannt in der Diskussion eines bestimmten Tests. Und genau diese Zahl setzt das Ausmaß der Hochskalierung: Das Netzwerk, das heute X Rechenleistung auf DOGE aufwendet, muss bis April 2027 fähig sein, ungefähr das Zehnfache von X auf Aigarth zu leisten.

In Kapitel acht entpackte ich UPoW als eine Art, eine Berechnung dazu zu zwingen, an zwei Fronten gleichzeitig zu arbeiten. Nach dem Aigarth-Deployment wird dasselbe Prinzip auf ein neues Aufgabenpaar angewendet: Die Rechenleistung, die heute als Teil von Phase 3 auf DOGE-Mining gerichtet ist, wird nach dem Deployment mit denselben wirtschaftlichen Anreizen auf Aigarth-Inferenz umgeleitet. Strukturell ist das Netzwerk also bereit – UPoW unterstützt Multitasking-Berechnung. Die Frage ist, ob Miner eine solche Umleitung wählen werden, und wie viele von ihnen sich bis zu dem Moment einklinken werden, in dem die Wahl bedeutsam wird.

Es lohnt sich hier zu klären, was von den Minern abhängt und was nicht. Was nicht abhängt – die Mechanik selbst, wie Aigarth-Aufgaben im Scoring gezählt werden und wie Belohnungen dafür anfallen: Das ist Teil des Protokolls, veröffentlicht im Repository github.com/qubic/core und nicht einseitiger Korrektur unterworfen. Was abhängt – die wirtschaftliche Wahl jedes einzelnen Miners: ob er seine GPU-/CPU-Leistung von DOGE-Auszahlung auf Aigarth-Auszahlung umstellt, und in welchem Verhältnis. Diese Wahl hängt vom Verhältnis der Belohnungshöhen zwischen den beiden Aufgaben ab, das das Netzwerk jede Epoche produziert, und von den Erwartungen der Miner, wie sich dieses Verhältnis weiterentwickelt. Das Aigarth-Team kontrolliert weder den ersten Parameter direkt (er ist eine Funktion der Teilnahme vieler Seiten) noch den zweiten (er hängt von individuellen Strategien ab). Was das Team kontrolliert – die technische Bereitschaft des Frameworks für das Deployment und die Qualität der KI-Anwendungen, die das Framework hosten wird. Alles andere ist ein externer Parameter, und genau das bezeichnet CfB mit den Worten „hängt von den Minern ab".

Das Hauptrisiko für Aigarth ist nicht Machbarkeit (das, wie oben gesagt, schloss CfB im Februar 2026). Das Hauptrisiko ist, das Netzwerk auf ein Niveau zu skalieren, auf dem Aigarth-Inferenz für Miner wirtschaftlich sinnvoll wird. Dieses Risiko wird nicht durch Wissenschaft oder Technik gelöst – es wird durch Netzwerkökonomie gelöst. Und auf diese Frage gibt es bereits eine teilweise Antwort, aus dem August 2025.

Zwischen Plan und Beweis

Ich entpackte Axelrods drei Bedingungen, angewandt auf die Forschungsarbeit selbst – Iteration, Gedächtnis, Transparenz. Das Buch iteriert (seine Kapitel werden umgeschrieben). Das Buch hält Gedächtnis (der Hook-Tracker verzeichnet jede Behauptung, die noch auf Abschluss wartet). Das Buch ist transparent (es kündigt seine Daten und Szenarien im Voraus an, bevor es die Antwort überprüfen kann). Ein falsifizierbarer Rahmen ist im Wesentlichen dieselben drei Bedingungen, angewandt auf die eigene Erzählung.

Am 14. Mai 2024 schrieb CfB auf Twitter:

„Ich habe erkannt, dass künstliche Intelligenz nicht geschaffen wird, sie wird entstehen. Mit Hilfe von Qubic-Minern."

„Wird entstehen" ist das Verb eines Beobachters, nicht eines Befehlshabers. Nicht „wir werden KI schaffen", sondern „KI wird entstehen – mit Hilfe derer, die am Netzwerk arbeiten". Das ist genau die emergente Rahmung, die ich entpackte: KI als Ergebnis kollektiver Mechanik, nicht als von oben entworfenes Produkt. Und diese Rahmung ist kein Marketing von 2024; sie ist die Position, aus der das Team von Anfang an gearbeitet hat. Seit 2022, als außerhalb eines engen Kreises niemand wusste, dass diese Entstehung eines Tages im öffentlichen Feld auftauchen würde; seit Dezember 2021, als der erste PoC gestartet wurde und das Team verstand, dass der Ansatz funktioniert; seit dem Moment, als CfB entschied, dass die „Bauen-und-Gehen"-Methode im Voraus im Code verankert werden könnte, und sich im Voraus zum Gehen verpflichtete.

Entstehung kommt nicht von selbst. Sie kommt, wenn es eine Umgebung gibt, in der sie sich manifestieren kann, und Zeit, damit diese Umgebung Gestalt annimmt. Frühere Kapitel beschrieben diese Umgebung: 676 Stimmen, wöchentliche Epochen, UPoW, Scoring, Smart Contracts, Governance. Dann beschrieben sie nicht die Umgebung, sondern den Prozess, der in ihr abläuft: Forschung, Meilensteine, Peer Review, Artefakte mit überprüfbaren Eigenschaften. Dann den Moment, in dem sich Umgebung und Prozess an einem öffentlichen Punkt treffen müssen. Wenn CfB mit seiner Beobachtung von 2024 recht hat, dann geschieht an diesem Datum das Treffen – nicht als Ankündigung, sondern als Regimewechsel, in dem das Netzwerk zu arbeiten beginnt.

TEIL V

Der Beweis

Der Krieg, den niemand führte

15
Der Krieg, den niemand führte

11. August 2025

Am 11. August 2025 schürfte innerhalb eines Fensters von hundertzweiundzwanzig aufeinanderfolgenden Blöcken im Monero-Netzwerk – von Block 3.475.729 bis Block 3.475.850 – ein Pool, der Rechenleistung unter der Qubic-Flagge bündelte, dreiundsechzig Blöcke. Das sind einundfünfzig Komma sechs Prozent. Einundfünfzig Prozent ist die technische Schwelle, jenseits derer ein Pool, während er seinen Anteil weiter hält, die Transaktionsgeschichte des Netzwerks umschreiben, bestätigte Überweisungen rückgängig machen und ausgewählte Adressen zensieren kann. Keiner der Teilnehmer bei Qubic tat davon etwas während dieser vierundzwanzig Stunden. Ein paar Tage später begann der Anteil des Pools an Monero zu sinken – nicht weil er verdrängt worden wäre, sondern weil das Team selbst die Prioritäten auf andere Aufgaben verlagert hatte. Es gab keine Monero-Forks. Es wurden keine Nutzerverluste verzeichnet. An der Börse Kraken wurden XMR-Einzahlungen für einige Tage vorübergehend ausgesetzt, dann wieder aufgenommen. Der Kurs von Monero gab über die Woche um etwa sechzehn Prozent nach und begann sich zu erholen.

Liest man nur die trockenen Zahlen, geschah nichts Bemerkenswertes. Ein Pool überschritt kurzzeitig eine wichtige technische Schwelle in einem der Netzwerke und nutzte sie nicht aus. Aber die Zahlen neben diesen Zahlen sind es wert, laut ausgesprochen zu werden.

Moneros Marktkapitalisierung betrug im August 2025 etwa sechs Milliarden Dollar. Qubics Marktkapitalisierung betrug etwa dreihundert Millionen. Ein Verhältnis von eins zu zwanzig. Ein Netzwerk mit zwanzigmal kleinerer Marktkapitalisierung strukturierte im Laufe von drei Monaten – von Mai bis August – ein Netzwerk mit zwanzigmal größerer um. Nicht durch Angriff, nicht durch Aufkauf von Infrastruktur, nicht durch Lobbyarbeit. Durch ein wirtschaftliches Angebot. Monero-Miner wechselten zum Qubic-Pool, weil er im Durchschnitt dreimal mehr zahlte als direktes Mining bei jedem anderen Pool. Sie wurden nicht getäuscht. Sie wurden nicht gezwungen. Sie sahen eine bessere Auszahlungsmatrix und trafen eine rationale Entscheidung.

Dies ist das Kapitel darüber, was genau zwischen Mai und August 2025 geschah, und warum das Geschehene mehr bedeutet, als die trockenen Zahlen nahelegen. Denn alles, was dieses Buch bisher über Iteration, Gedächtnis, Transparenz, die vier Eigenschaften von Tit-for-Tat und Axelrods drei Bedingungen gesagt hat – all das war vor August 2025 entweder Mathematik der 1980er, oder Simulationsmodellierung, oder architektonische Beschreibung. Nach August 2025 ist es eine empirische Tatsache in einem Netzwerk mit sechs Milliarden Dollar Marktkapitalisierung.

Dort beginne ich.

Wie der Pool von zwei auf einundfünfzig Prozent wuchs

Im Mai 2025 lag Qubics Anteil an Moneros gesamter Hashrate bei unter zwei Prozent. Es war ein experimenteller Pool, vom Qubic-Team eingerichtet, um eine Idee zu testen – dass die Rechenarbeit, die das Qubic-Netzwerk ohnehin als Teil seines eigenen UPoW produziert, gleichzeitig für das Mining auf externen Netzwerken genutzt werden könnte, um die Belohnungen zurück in die Qubic-Ökonomie umzuwandeln. Bis Ende Juni war der Anteil auf etwa zehn Prozent gewachsen. Bis Mitte Juli – auf zwanzig. Bis Ende Juli war Qubic der Monero-Pool Nummer eins und erreichte in Spitzenmomenten etwa vierzig Prozent der Hashrate. Am 11. August, einundfünfzig Komma sechs Prozent im Fenster von 122 Blöcken.

Von zwei auf einundfünfzig in drei Monaten. Das muss als Tempo festgehalten werden – ein Tempo der Migration, kein Tempo des Infrastrukturaufbaus. Die Infrastruktur war vorab bereit: Der Pool konnte bereits im Mai Monero schürfen. Was sich von Mai bis August änderte, war nicht der Code des Pools, sondern die Anzahl der Miner, die sich genau für ihn entschieden. Jeder von ihnen traf eine individuelle Entscheidung, und die Summe dieser Entscheidungen ergab eine Wachstumskurve mit sehr charakteristischer Form: ein langsamer Start, allmähliche Beschleunigung, ein Kipppunkt, nach dem neue Miner kommen, weil sie von anderen Minern von einem Pool hören, der mehr zahlt.

Der Schlüsselmoment, der das Tempo erklärt, ist die Abstimmung, die im Frühsommer 2025 innerhalb der Qubic-Community stattfand. Ursprünglich sah das Schema so aus: Der Pool schürft Monero, das verdiente XMR wird gegen USDT verkauft, das USDT geht in Buyback und Verbrennung von QU-Token. Der gesamte Vorteil aus externem Mining wird vom deflationären Mechanismus des Qubic-Netzwerks absorbiert; ein Miner, der aus einem beliebigen anderen Monero-Pool in den Pool wechselt, verdient ungefähr dasselbe wie zuvor, plus einen indirekten Vorteil durch die Wertsteigerung des QU, das er hält. Das reichte aus, um den Pool von Mai bis Juni von zwei auf zehn Prozent wachsen zu lassen, aber nicht, um über zwanzig hinauszukommen.

Nach der Abstimmung änderte sich das Schema. Die Hälfte des USDT ging weiterhin in Buyback und Verbrennung – der deflationäre Mechanismus blieb erhalten, aber in abgeschwächter Form. Die andere Hälfte ging direkt an Qubics Computor-Knoten als zusätzliches Einkommen. Diese zweite Hälfte verwandelte den Pool von einem Experiment in einen Magneten. Nach der Umstrukturierung begann ein Miner, der zum Qubic-Pool wechselte, im Durchschnitt dreimal mehr zu verdienen als bei direktem Monero-Mining an jedem anderen Pool. Das ist keine Marketingzeile; es ist ein messbarer Parameter, überprüfbar anhand der Auszahlungen an konkrete Adressen. Der Pool zahlte ehrlich, was er versprach, weil das Versprechen in den Code eingebaut war.

Dan Dadybayo, ein Forscher bei Unstoppable Wallet, formulierte es in einer im August 2025 veröffentlichten Analyse der Lage so: Ivancheglo schuf ein Anreizspiel, in dem Monero-Miner freiwillig das Netzwerk aufgeben können, wenn sie ein besseres Angebot sehen. „Freiwillig das Netzwerk aufgeben.“ Sechs Wörter, die das Wesen des Ereignisses präziser beschreiben als die meisten technischen Aufarbeitungen aus jenem Sommer.

Das ist eine Formulierung, die es sich zu entfalten lohnt, denn sie ist keine Metapher. Ein Monero-Miner, der im Juli 2025 zum Qubic-Pool wechselte, verletzte keine Regeln. Er griff Monero nicht an. Er half nicht dabei, Monero anzugreifen. Er traf eine Marktentscheidung – seine Hashrate auf einen Pool umzuleiten, der mehr zahlt. Dieselbe Art Entscheidung, die jeder von ihnen schon Dutzende Male zuvor

getroffen hatte, beim Wechsel zwischen verschiedenen Monero-Pools. Aus der Perspektive der Monero-Regeln sind die Handlungen der zu Qubic gewechselten Miner nicht von gewöhnlicher Migration zwischen Pools zu unterscheiden. Aus der Perspektive von Monero als Koordinationssystem führten diese Handlungen dazu, dass ein Pool eine Mehrheit der Hashrate anhäufte. Nicht weil er jemanden zwang. Weil er mehr bot.

Im ersten Kapitel schrieb ich, in seiner frühesten Version, dass die neue Technologie „parallel wirkt, nicht anstelle von" – über Gaslampen, die neben der Kohlebeleuchtung erschienen, nicht an ihrer Stelle. Damals, 2009, wurde das über Bitcoin gesagt als „Murdochs Gas, das noch niemand in ein Rohr gesammelt hatte". Im August 2025 zeigte sich dasselbe Prinzip anders. Niemand zerstörte Monero. Monero als Netzwerk lief weiter, und läuft weiter; seine Privatsphäre ist nicht gebrochen; sein Protokoll ist nicht gebrochen. Parallel dazu erschien ein Pool, in dem Miner dreimal mehr verdienten, und manche von ihnen wechselten dorthin. Das Netzwerk begann dadurch nicht, als Technologie schlechter zu funktionieren; es verlor nur vorübergehend das Monopol auf die Aufmerksamkeit seiner eigenen Miner. Nachdem Qubic seine Aktivität in Monero reduzierte, wanderte die Community zu P2Pool, einem dezentralen Pool, und der pluralistische Zustand wurde wiederhergestellt. Die alte Welt funktioniert. Die neue Welt funktioniert auch. Niemand zerstörte irgendjemanden.

Das ist parallele Architektur in infrastruktureller Form. Nicht „das bessere System besiegt das schlechtere durch einen Wettkampf". Sondern „das bessere System bietet freie Migration in sich selbst an, und manche der Teilnehmer migrieren, und manche bleiben, und das ist normal".

Drei Bedingungen im Maßstab von sechs Milliarden

Im zweiten Kapitel ging ich ausführlich durch, unter welchen exakten Bedingungen die Vier-Zeilen-Code-Strategie – Tit-for-Tat – optimal wird. Axelrod und Hamilton formulierten das in ihren Arbeiten von 1981–1984 als drei notwendige Bedingungen. Das Spiel muss wiederholt werden. Teilnehmer müssen sich genau erinnern, was ihr Gegner in der Vergangenheit tat. Verhalten muss sichtbar sein – entweder direkt oder über einen Reputationskanal. Entfernt man auch nur eine der drei, verschiebt sich die optimale Strategie von Kooperation zu reinem Egoismus.

Im August 2025 waren alle drei Bedingungen im industriellen Maßstab erfüllt.

Wiederholung. Jeder Monero-Block ist eine eigene Runde des Spiels. Ein Block entsteht etwa alle zwei Minuten. Über die drei Monate von Mai bis August lief das Netzwerk in der Größenordnung von fünfundsechzigtausend Runden. Kein Miner, der entschied, welchen Pool er wählt, handelte in einer einmaligen Situation. Jede Wahl eines Pools war die Wahl eines Partners für die nächsten Zehntausenden Runden, und alle Teilnehmer wussten das. Der Schatten der Zukunft – nicht als Metapher, sondern als quantitativer Parameter – war so lang, dass jede Erwägung eines momentanen Betrugsgewinns im Vergleich zum langfristigen Gewinn ehrlicher Teilnahme vernachlässigbar wurde.

Im siebten Kapitel führte ich das Konzept der Epoche als Runde eines wiederholten Spiels ein. Dort ging es um Qubics eigenes Netzwerk, wo eine Epoche eine Woche dauert und die Zusammensetzung der Computor-Knoten nach Ergebnissen aktualisiert wird. Hier, bei Monero, wirkt dasselbe Prinzip in noch größerem Maßstab und in einem fremden Netzwerk. Alle zwei Minuten – eine Runde. Jeder Miner – ein Spieler in dieser Runde. Jede Poolwahl – ein Zug im Spiel, für alle anderen sichtbar.

Gedächtnis. Die Monero-Blockchain ist eine öffentliche Geschichte, in der jeder Block für immer zusammen mit der Adresse verzeichnet ist, die die Belohnung für diesen Block erhielt. Es ist unmöglich, zu „vergessen“, wie viele Blöcke jeder Pool im letzten Monat geschürft hat. Es ist unmöglich, die Lage im Nachhinein falsch darzustellen: Hätte der Qubic-Pool tatsächlich weniger gezahlt als versprochen, wäre das sofort am Verhältnis von geschürften Blöcken zu öffentlichen Auszahlungen sichtbar gewesen. Hätte es einen verborgenen Kanal zur Umverteilung von Belohnungen gegeben, hätte sich dieser Verstoß gegen die Proof-of-Work-Logik in verwaisten Blöcken oder Veröffentlichungsverzögerungen gezeigt. Das Gedächtnis des Netzwerks hängt nicht von der Gewissenhaftigkeit seiner Teilnehmer ab; es ist ins Protokoll eingebaut.

Das ist ein Gedächtnisniveau, unerreichbar in jeder der Umgebungen, die Axelrod im Sinn hatte, als er über reale Analoga seiner Laborbedingungen schrieb – Verwandtschaftsgruppen bei Primaten, kleine Gemeinschaften, Handelsgilden. All diese Systeme hatten Gedächtnis, aber biologisches und soziales Gedächtnis: begrenzt durch die Anzahl der Menschen, die sich persönlich aneinander erinnern können, und durch die Zeit, die diese Menschen leben. Die Blockchain entfernt beide Begrenzungen (das ist wichtig!). Das Gedächtnis des Netzwerks verblasst nicht mit der Zeit und hängt nicht von der Anzahl der Teilnehmer ab. Es ist ein Gedächtniswerkzeug, das erschien, nachdem Axelrod seine Hauptarbeit abgeschlossen hatte, und erschien nicht als Umsetzung seiner Ideen, sondern als Infrastruktur für Geldüberweisungen. Aber genau diese Infrastruktur erwies sich als die Umgebung, in der die Bedingungen seiner Theorie streng erfüllt sind.

Transparenz. Die Hashrate jedes Pools bei Monero ist öffentlich sichtbar. Man muss kein Mitglied der Community sein, man braucht kein Abo bei einem spezialisierten Dienst, man muss nicht auf Berichte warten. Jeder mit einem Webbrowser, überall auf der Welt, kann auf eines der öffentlichen Monero-Monitoring-Dashboards gehen und in Echtzeit sehen, welcher Pool welchen Anteil hat. Als der Qubic-Pool im Juli zwanzig Prozent überschritt, war das binnen Stunden bekannt. Als er Anfang August vierzig Prozent überschritt, war das ebenfalls binnen Stunden bekannt. Transparenz ist keine Funktion der Monero-Community, kein Ergebnis journalistischer Arbeit, keine Folge gewissenhafter Offenlegungen der Pools. Es ist schlicht eine strukturelle Eigenschaft eines öffentlichen Proof-of-Work-Netzwerks.

Sind alle drei Bedingungen erfüllt, wird Tit-for-Tat nicht nur eine optimale Strategie – es wird das, was in einer von Axelrods Formulierungen als „evolutionär stabile Strategie“ beschrieben wird. Eine Strategie, zu der das System konvergiert, gegeben genug Runden. Die Monero-Community reagierte instinktiv auf Qubics Dominanz genau nach der Logik eines Spiegels: Miner begannen, zu P2Pool zu wechseln, Diskussionen über einen möglichen Hard Fork zur Änderung des RandomX-Algorithmus gewannen an Fahrt, die Börse Kraken setzte XMR-Einzahlungen vorübergehend aus. Keine dieser Reaktionen war eine koordinierte „politische“ Entscheidung. Es ist die spontane Reaktion einer verteilten Umgebung, in der die drei Bedingungen erfüllt sind, auf eine vorübergehende Störung des Gleichgewichts. Nachdem Qubic die Aktivität reduzierte, ebbte die Reaktion ruhig ab. Es gab keine Konsequenzen für Miner, die weiter mit dem Pool arbeiteten; niemand „bestrafte“ sie. Monero als Koordinationssystem kehrte einfach in einen pluralistischen Zustand zurück.

Das ist industrielle Validierung des 1980 gelegten theoretischen Rahmens. Kein kontrolliertes Experiment in einem Labor an der University of Michigan. Keine Computersimulation. Ein Sechs-Milliarden-Dollar-Netzwerk mit Tausenden unabhängigen Teilnehmern, in dem alle drei

Bedingungen streng erfüllt sind, und in dem die Reaktion auf die Störung genau so verlief, wie eine fünfundvierzig Jahre vor dem Ereignis geschriebene Theorie es vorhergesagt hätte.

Was Qubic hätte tun können und nicht tat

Anfang August 2025, als Qubics Hashrate bei Monero direkt an fünfzig Prozent heranreichte, stand das Team des Projekts vor einer unangenehmen technischen Frage. Nicht „werden wir einundfünfzig Prozent halten“ – das war nur eine Frage weniger Tage Arbeit und akkumulierender Hashrate. Sondern „was werden wir danach tun, falls wir es tatsächlich halten“. Am 3. August 2025 veröffentlichte Come-from-Beyond in einem der öffentlichen Kanäle eine Bemerkung, die die Wahl, vor der das Team stand, besser einfängt als jedes andere Material aus jenem Sommer:

„Richtig. Wenn wir gewollt hätten, würden wir zurück-DDoSen. Oder sogar einen PR-Angriff fahren, indem wir Börsen warnen, dass wir, sobald wir Dominanz durchsetzen, zufällige Kettenreorganisationen durchführen werden, während wir Transaktionen zensieren, sodass jede XMR-Einzahlung an Börsen mit 50 % Wahrscheinlichkeit doppelt ausgegeben würde. Selbst DEXes würden nicht helfen, weil sie ebenfalls Opfer von Double-Spending würden. Und der XMR-Preis würde auf 0 abstürzen. Aber, wie @dkat sagte, wir sind Freunde und werden das alles nicht tun.“

Diese Bemerkung ist es wert, entfaltet zu werden, denn sie enthält sechs konkrete Angriffsvektoren, von denen jeder dem Qubic-Team in der ersten Augustwoche 2025 technisch zur Verfügung stand, und von denen jeder vom Team bewusst nicht genutzt wurde.

Der erste Vektor – vergeltender DDoS. Vom 3. bis zum 10. August stand das Qubic-Team unter einem verteilten Denial-of-Service-Angriff, der die Hashrate des eigenen Netzwerks von zweieinhalb Gigahashes pro Sekunde auf achthundert Megahashes am schlimmsten Punkt des Angriffs drückte. CfB beschuldigte öffentlich einen der zentralen XMRig-Entwickler, den Angriff koordiniert zu haben; dieser Entwickler bestritt es; die Quelle des Angriffs blieb formal unbestätigt. Bestätigt ist, dass der Angriff mehr als eine Woche andauerte und das Halten der Hashrate im benötigten Maßstab erheblich erschwerte. Das Qubic-Team hätte symmetrisch reagieren können: seine eigene Infrastruktur nutzen, um einen DDoS-Angriff auf seine Gegner zu koordinieren. Es tat es nicht.

Zweitens – ein PR-Angriff auf Börsen. Nach Überschreiten der Einundfünfzig-Prozent-Schwelle hätte das Team eine Warnung an alle Börsen senden können, die XMR-Einzahlungen akzeptierten, dass ab jetzt jede Bestätigung einer Überweisung an der Börse mit fünfzig Prozent Wahrscheinlichkeit als unzuverlässig zu betrachten sei. Das ist eine technische Wahrheit: Solange man Mehrheits-Hashrate hält, kann ein Pool Kettenreorganisationen erzeugen, die zuvor bestätigte Transaktionen zurückrollen. Börsen wären bei Erhalt einer solchen Warnung gezwungen gewesen, sich zu schützen, indem sie Operationen mit XMR vorübergehend aussetzten. Das hätte Moneros Liquidität an Börsen zerstört, ohne einen einzigen tatsächlich reorganisierten Block – eine einzige öffentliche Warnung eines mehrheitshaltenden Pools hätte genügt. Nicht getan.

Drittens – tatsächliche Kettenreorganisationen. Technisch die direkteste Nutzung der Mehrheitsposition. Der Pool hält seine Blöcke geheim, akkumuliert eine interne Kette länger als die öffentliche, und veröffentlicht sie periodisch, wodurch das Netzwerk gezwungen wird, auf eine neue Version der Geschichte zurückzurollen. Diese Methode, bekannt als Selfish Mining, wurde im 2014er-Paper von

Eyal und Sirer beschrieben; sie wurde tatsächlich als Teil der Strategie des letzten Stoßes zu einundfünfzig Prozent verwendet. Aber Selfish Mining in der finalen Übernahmephase ist ein Werkzeug, um mehr eigene Blöcke relativ zur Gesamtzahl anzuhäufen. Chaotische Reorganisationen nach der Übernahme sind etwas anderes: Das Netzwerk verwandelt sich in eine Umgebung, in der die Transaktionsgeschichte aufhört, stabil zu sein. Ein paar öffentliche Reorganisationen hätten genügt, um Moneros Funktionalität als Zahlungssystem ernsthaft zu untergraben. Nicht getan.

Viertens – Transaktionszensur. Solange man Mehrheits-Hashrate hält, kann ein Pool wählen, welche Transaktionen er in seine Blöcke aufnimmt und welche er ignoriert. Ein paar Wochen einer solchen selektiven Mining-Politik genügen – und jede Adresse oder Adressklasse kann strukturell von der Fähigkeit abgeschnitten werden, Überweisungen zu bestätigen. Technisch ist das keine unmögliche Handlung; sie wird regelmäßig als Risikoszenario für Proof-of-Work-Netzwerke diskutiert. Nicht getan.

Fünftens – ein Angriff auf Börseneinzahlungen mit fünfzig Prozent Ausfallwahrscheinlichkeit. Das ist eine Kombination der Reorganisationsstrategie mit der Börsenmechanik. Bei gehaltener Mehrheit könnte jede an eine Börse gesendete XMR-Einzahlung mit hoher Wahrscheinlichkeit durch Kettenreorganisation rückgängig gemacht werden, entweder bevor oder nachdem die Börse sie dem Konto gutgeschrieben hat. Die Börse verliert entweder Gelder oder Nutzervertrauen. Auf einem Netzwerk mit Millionen Nutzern ist ein solches Verhalten destruktiv, und DEX-Systeme bieten keinen Schutz, weil sie ebenfalls auf derselben Kettengeschichte aufbauen. Nicht getan.

Sechstens – eine Konsequenz der ersten fünf, explizit von CfB genannt: Der Preis von XMR wird auf null abstürzen. Das ist eine Vorhersage, kein Wunsch. CfB behauptet nicht, dass der Preis notwendigerweise auf null fallen wird – er beschreibt das Grenzszenario, das aus konsequenter Anwendung des Arsenals resultieren würde. Die konkrete Tiefe des Absturzes hängt von vielen Variablen ab; wichtig ist prinzipiell, dass ein Raum möglicher Ausgänge beschrieben wurde, kein bestimmtes Ergebnis. Nicht getan.

Sechs Angriffsvektoren. Jeder technisch verfügbar. Jeder hätte den angehäuften Vorteil des Pools gegen seine ehemaligen Kollegen im Netzwerk eingesetzt. Jeder blieb ungenutzt. CfBs Schlusszeile in derselben Bemerkung, die Wahl erklärend: „wie @dkat sagte, wir sind Freunde und werden das alles nicht tun“. Dkat, der Entwickler von QEarn und leitender Entwickler der Monero-Operation, hatte zu diesem Zeitpunkt bereits die Position des Teams formuliert: Wir vernichten keine Partner, von denen wir einen Vorteil gewonnen haben.

Dass Qubic Monero nicht zerstörte, ist keine Folge davon, dass Zerstörung unmöglich gewesen wäre. Keine Folge fehlender nötiger Infrastruktur beim Team. Keine Folge externer Zurückhaltung durch Börsen, Regulierer oder die Community. Es ist eine Entscheidung des Qubic-Teams, getroffen im Moment maximalen Vorteils und explizit eine Woche vor Erreichen der logischen Grenzen dieses Vorteils öffentlich festgehalten. Sechs Werkzeuge zur Zerstörung des Netzwerks lagen neben dem Team, während es Mehrheits-Hashrate hielt. Das Team griff zu keinem einzigen.

Vier Eigenschaften, angewandt in der Realität

Im zweiten Kapitel ging ich die vier Eigenschaften von Tit-for-Tat durch, die es zum Sieger der Turniere von 1980 machten. Die Eigenschaften wurden von Axelrod aus seiner Analyse jeder im ersten Turnier

gespielten Partie formuliert: Freundlichkeit, Vergeltung, Vergebung, Klarheit. Jede von ihnen wurde von Tit-for-Tat durch Anatol Rapoports vier Zeilen Code umgesetzt. Jede ist theoretisch unabhängig von den anderen, und jede ist notwendig für den Sieg in einer Umgebung mit erfüllten drei Bedingungen.

Im August 2025 zeigten sich alle vier Eigenschaften im industriellen Maßstab – nicht als Metaphern, sondern als beobachtbare Handlungen des Qubic-Teams gegenüber dem Monero-Netzwerk und seiner Community. Es lohnt sich, das explizit festzuhalten, denn die Entsprechung ist exakt.

Freundlichkeit. Tit-for-Tat defektiert nie zuerst; beim ersten Zug kooperiert es immer. Qubic griff Monero nicht zuerst an. Qubics ursprüngliche Strategie gegenüber Monero war kein Angriff, sondern ein Angebot: ein Pool, der Minern mehr für dieselbe Arbeit zahlte. Beim ersten Zug – Kooperation in Form eines besseren wirtschaftlichen Angebots. Es gab keinen Plan, irgendjemanden anzugreifen. Dass infolge dieses Angebots de facto eine Mehrheit der Hashrate eingefangen wurde, ist eine Konsequenz dessen, dass das Angebot für die Miner selbst überzeugend war, nicht einer vorherigen Absicht, dem Netzwerk zu schaden.

Vergeltung. Tit-for-Tat beantwortet Defektion sofort – nicht mit Verzögerung, nicht auf Vorrat, nicht mit einer Wahrscheinlichkeit, sondern genau im nächsten Zug, genau einmal. Qubic reagierte auf den DDoS-Angriff, der vom 3. bis 10. August lief. Aber es reagierte nicht symmetrisch – nicht mit einem Gegenangriff, nicht durch Zerstörung fremder Infrastruktur, nicht durch Bestrafung bestimmter Gegner. Es reagierte, indem es die Operation fortsetzte. Die unter dem Angriff auf achthundert Megahashes gefallene Hashrate erholte sich; der Pool hielt seinen Anteil bei Monero; am 11. August wurde die Einundfünfzig-Prozent-Schwelle überschritten. Das ist Vergeltung in ihrem präzisen Sinn – die Weigerung, für die ursprüngliche Handlung bestraft zu werden. Aber ohne Eskalation und ohne die Bestrafung auf Teilnehmer zu übertragen, die nichts mit dem Angriff zu tun hatten.

Vergebung. Tit-for-Tat trägt keinen Groll; hat der Gegner zur Kooperation zurückgefunden, kehrt es ebenfalls zurück. Sofort. Nach der Demonstration der Übernahmemöglichkeit ging das Qubic-Team nicht dazu über, den Vorteil zu zementieren. Die Hashrate des Pools bei Monero begann kurz nach dem 11. August zu sinken – nicht wegen externen Drucks, sondern wegen einer internen Entscheidung, die Rechenprioritäten auf DOGE-Mining und Aigarth umzustellen. Bis zum 17. August hielt der Pool keine Mehrheit mehr. Diese Handlung ist funktional äquivalent zu „Rückkehr zur Kooperation“: Das Team zog sich in den pluralistischen Zustand des Netzwerks zurück, ohne externen Grund dafür außer der Tatsache, dass das Ziel des Experiments – die Mechanik zu demonstrieren – erreicht war, und ein weiteres Aufrechterhalten des Drucks wäre ein Übergang vom Testen zu tatsächlichem Schaden gewesen.

Klarheit. Tit-for-Tat ist vorhersehbar: Es ist für den Gegner leicht zu verstehen, was es tut und warum. Das Qubic-Team führte die gesamte Operation im öffentlichen Feld durch. Der Plan wurde angekündigt – das ist an Beiträgen erkennbar, die bis Ende Mai 2025 zurückreichen. Technische Details wurden offen diskutiert, einschließlich der Bemerkung vom 3. August über das verfügbare Angriffsarsenal. Die Hashrate-Metriken des Pools waren öffentlich sichtbar, wie die jedes anderen Teilnehmers im Monero-Netzwerk. Der Abschlussbericht vom 12. August im offiziellen Qubic-Blog hielt die drei Thesen fest, die das Team durch das Experiment als bewiesen ansah, und kündigte explizit an, dass das Experiment abgeschlossen sei. Keine verborgenen Koordinationskanäle; keine privaten Verhandlungen mit Börsen; keine Absprachen mit einzelnen Akteuren. Transparenz ist kein Ergebnis ehrlicher

Absichten; sie ist eine strukturelle Eigenschaft davon, wie die Operation durchgeführt wurde.

Rapoports vier Eigenschaften, angewandt auf eine reale Ökonomie im Maßstab von sechs Milliarden Dollar. Nicht in einem Labor, nicht in einer Simulation, nicht in einer Trainingsumgebung. In einem lebenden Netzwerk, in Echtzeit, mit realen Konsequenzen.

Im zweiten Kapitel schloss ich die Diskussion über Axelrod mit der Beobachtung, dass dieselbe Formel – „behandle andere, wie du behandelt werden möchtest“ – von fünf Menschen unabhängig voneinander über zweieinhalb Jahrtausende hinweg gefunden wurde. Konfuzius um 500 v. Chr. Hillel der Ältere in Jerusalem um 30 v. Chr. Jesus von Nazareth um 30 n. Chr. Kant bewies sie 1785 logisch. Rapoport bewies sie 1980 mathematisch. Fünf unabhängige Entdeckungen einer Formel, mit Abständen von Jahrhunderten. Am 12. August 2025 erhielt diese Formel ihre sechste Bestätigung – nicht als Formulierung, sondern als industrielles Experiment, in dem genau die Eigenschaften, die Rapoport in vier Zeilen Code nähte, exakt so auftauchten, wie die Theorie es vorhersagte. Bravo, CfB!

DDoS als Test der Eigenschaft Vergeltung

Es lohnt sich, kurz bei der Episode vom 3. bis 10. August innezuhalten, denn sie ist der sauberste Test einer der vier Eigenschaften in einer lebenden Umgebung.

Der DDoS-Angriff gegen Qubics Infrastruktur begann ungefähr, als die Hashrate des Pools bei Monero fünfundvierzig Prozent erreichte. Über sieben Tage des Angriffs fiel die Gesamt-Hashrate des Qubic-Netzwerks von zweieinhalb Gigahashes pro Sekunde auf achthundert Megahashes am schlimmsten Punkt. Das bedeutet, Qubics eigenes Netzwerk – das Netzwerk, über das Rechenarbeit zwischen Monero-Mining, DOGE-Mining und UPoW-Aufgaben für seinen eigenen Konsens verteilt werden sollte – lief für mehrere Tage in einem Regime, das seinem üblichen deutlich unterlegen war. Manche Randdienste des Projekts wurden vorübergehend abgeschaltet. Die finanzielle Last auf der Infrastruktur stieg. Die Koordination zwischen Computor-Knoten wurde komplizierter.

Und dennoch wurde die Operation bei Monero nicht unterbrochen. Die Monero-Hashrate sank, aber nicht kritisch; der Pool hielt seine Position Nummer eins alle sieben Tage des Angriffs. Am 11. August, als der Angriff bereits abklang, wurde die Einundfünfzig-Prozent-Schwelle überschritten. Eben jene einundfünfzig Komma sechs Prozent im Fenster von 122 Blöcken, die den Rest des Kapitels rahmen.

Das ist ein Test der Eigenschaft Vergeltung in ihrer präzisen Formulierung. Nicht „mit demselben am selben Akteur gerächt“ – das tat Qubic nicht. Sondern „weiterhin so gehandelt, dass die Aggression ihr Ziel nicht erreichte“. In den Begriffen des Turniers von 1980: Tit-for-Tat gibt in einer Umgebung aggressiver Strategien nicht auf und zieht sich nicht zurück; es spielt sein eigenes Spiel weiter und beantwortet jeden Aggressionsakt genau einmal – indem es das kooperative Spiel mit denen fortsetzt, die zur Kooperation bereit sind. Das Qubic-Team bestand diesen Test im August 2025 buchstäblich: Es reagierte auf Aggression gegen die eigene Infrastruktur, indem es die Operation bei Monero zu Ende führte, ohne die Kette öffentlicher Verpflichtungen gegenüber den in seinen Pool gewechselten Minern zu brechen.

Das zwölfte Kapitel führte das Konzept emergenter Sicherheit ein – Schutz, der nicht als konstruierte Funktion, sondern als Nebenprodukt korrekt gebauter Mechanik entstand. Die DDoS-Episode vom August 2025 zeigt dasselbe Phänomen umgekehrt: emergente Widerstandsfähigkeit. Das

Qubic-Netzwerk war nicht speziell dafür entworfen, einen wochenlangen DDoS-Angriff zu überstehen. Aber eine Architektur aus sechshundertsechsundsiebzig Knoten, verteilt über verschiedene Betreiber und Rechtsräume, macht einen Angriff auf die Infrastruktur als Ganzes außergewöhnlich teuer und ohne bestimmtes Ergebnis. Wie emergente Sicherheit ist emergente Widerstandsfähigkeit eine Eigenschaft, die sich im Moment der Krise zeigt, nicht im Voraus erklärt wird.

Was an dieser Episode für den größeren Rahmen wichtig ist: Die Fähigkeit des Netzwerks, koordiniertem externem Druck eine Woche lang standzuhalten, ohne die Operation zu unterbrechen, für die es gerade genutzt wird, ist kein Designversprechen mehr, sondern eine beobachtete Eigenschaft. Und da das Deployment von Aigarth 2027 ungefähr dasselbe erfordern wird – anhaltenden Betrieb der Infrastruktur unter Last –, hat das Datum vom August 2025 Bedeutung über das Thema dieses Kapitels hinaus.

Anreize diktieren den Konsens

Am 12. August 2025 veröffentlichte Qubics offizieller Blog den Abschlussbericht zum Monero-Experiment. Der Bericht hielt drei Thesen fest, die das Team durch die Operation als empirisch bewiesen ansah:

„Ausgelagerte Berechnungen sind praktikabel: Qubics UPoW-Modell ist eine bewährte, in der realen Welt funktionierende Technologie, fähig, Rechenleistung für externe Aufgaben umzuwidmen." „Anreize diktieren den Konsens: Jede Proof-of-Work-Blockchain kann angegriffen und kontrolliert werden, indem man ihren Minern überlegene wirtschaftliche Anreize bietet." „Infrastruktur-Widerstandsfähigkeit: Qubics dezentrales Netzwerk zeigte eine bemerkenswerte Fähigkeit, ausgeklügelten, anhaltenden Netzwerkangriffen standzuhalten und sich von ihnen zu erholen."

Drei Thesen. Jede von ihnen strukturell, nicht wertend. Die erste besagt, dass die in Kapitel acht analysierte UPoW-Architektur tatsächlich in der Lage ist, die eigene Rechenarbeit des Netzwerks auf externe Aufgaben zu lenken, ohne ihre Hauptkonsensfunktion zu verlieren. Die zweite – dass jedes Proof-of-Work-Netzwerk umorientiert werden kann, indem man seinen Minern eine bessere Ökonomie bietet, und dass das keine Anomalie und keine Schwachstelle einzelner Netzwerke ist, sondern eine strukturelle Eigenschaft der gesamten Klasse. Die dritte – dass ein als Mesh ohne einzelnen Fehlerpunkt gebautes dezentrales Netzwerk ausgeklügelten Netzwerkangriffen standhält.

Von den drei Thesen zählt die zweite im Rahmen dieses Buches am meisten. „Anreize diktieren den Konsens" – Axelrod, in die Sprache des Protokolls übersetzt.

Jedes Proof-of-Work-Netzwerk ist ein Koordinationssystem mit einer bestimmten Auszahlungsmatrix. Miner darin treffen Entscheidungen, die bestimmen, welche Blockkette der gemeinsame Konsens sein wird. Bietet jemand Minern eine bessere Auszahlungsmatrix – besser genau in den Parametern, die sie ohnehin optimieren, nämlich das Einkommen aus ihrer Arbeit –, migrieren rationale Miner. Das ist kein Verrat. Das ist keine moralische Entscheidung. Das ist einfach eine Eigenschaft einer Umgebung, in der alle drei Axelrod-Bedingungen – Wiederholung, Gedächtnis, Transparenz – erfüllt sind. In einer solchen Umgebung bildet sich Kooperation um den Punkt herum, an dem sie wirtschaftlich am profitabelsten ist. Bewegt sich dieser Punkt – bewegt sich die Kooperation mit ihm.

Das bedeutet, dass die Frage „warum hält Netzwerk A und nicht Netzwerk B einem 51-Prozent-Angriff stand“ keine Frage nach der Widerstandsfähigkeit des Konsensalgorithmus ist. Es ist eine Frage nach der Widerstandsfähigkeit der Ökonomie. Ein Netzwerk überlebt, solange es für seine Miner profitabler ist, in ihm zu arbeiten, als anderswo. Sobald das nicht mehr stimmt, wird es anfällig für Migration. Und diese Migration kann nicht durch Verschlüsselung, durch einen Algorithmus oder durch eine soziale Kampagne verhindert werden. Sie wird nur verhindert, indem man den wirtschaftlichen Vorteil des eigenen Netzwerks hält.

Das ist „Anreize diktieren den Konsens“ in seiner vollen Form. Eine strukturelle Beschreibung davon, wie verteilte Koordinationssysteme funktionieren, die auf dem Aufwand von Rechenarbeit beruhen.

Am 13. April 2027 wechselt, laut Plan, das Aigarth-Framework in die Produktion, und die Qubic-Infrastruktur soll Rechenkapazität für KI-Inferenz als neue Art nützlicher Arbeit bereitstellen. Das Hauptrisiko, wie CfB bereits am 12. November 2025 formulierte: „Aigarth hängt von den Minern ab.“ Genau dieselbe Frage wie im Mai 2025, aber in anderem Maßstab. Werden Miner Qubic-Netzwerk-Rechenaufgaben wählen – bis dahin Aigarth-Aufgaben statt Monero-Mining –, weil sie mehr zahlen? Wenn ja – funktioniert das Deployment im in Kapitel vierzehn als Szenario A beschriebenen Regime. Wenn nein – funktioniert das Deployment technisch, aber Aigarth-Anwendungen erweisen sich mangels Rechenleistung als schwach, und das wird Szenario B sein.

Das Experiment vom August 2025 beantwortet diese Frage nicht direkt. Es garantiert nicht, dass sich der April 2027 wiederholen wird. Aber es beantwortet eine andere, fundamentalere Frage: ob die Mechanik selbst funktioniert. Ob ein Netzwerk, das bessere Ökonomie bietet, in der Lage ist, Miner ohne Zwang umzuorientieren, im Maßstab lebender Infrastruktur, gegen den Widerstand von Konkurrenten und unter externem Druck. Die Antwort auf diese Frage wurde gegeben. Bejahend. Einmal, an einem bestimmten Netzwerk, in bekanntem Maßstab. Das reicht nicht, um von einem Gesetz zu sprechen. Es reicht, um von einem Prinzipbeweis zu sprechen.

Was Qubic nicht tat

16
Was Qubic nicht tat

Sechs Werkzeuge, keines eingesetzt

Die naheliegende Erklärung ist ethisch. Das Qubic-Team entschied sich, Monero nicht zu schaden, weil es das für falsch hielt. CfB verwies in derselben Bemerkung auf dkat: „wir sind Freunde." Freunde zerstören sich nicht gegenseitig. Diese Erklärung funktioniert auf Alltagsebene und steht im Einklang mit allem, was über die öffentliche Position des Qubic-Teams gegenüber Monero jenen ganzen Sommer über bekannt ist.

Dieses Kapitel handelt nicht von der ethischen Erklärung. Die ethische Erklärung mag zutreffen, aber sie hat keine Kraft als Argument, denn jedes Krypto-Projekt-Team wird von sich behaupten, es würde nichts Falsches tun. Die ethische Erklärung funktioniert, nachdem beobachtetes Verhalten bereits geschehen ist, als Rationalisierung; als Vorhersage ist sie nutzlos. Hätte jemand Anfang August 2025 gefragt „wird Qubic Monero bis zum Ende angreifen", wäre die Antwort „das sind gute Leute" keine ausreichende Grundlage für Sicherheit gewesen.

Dieses Kapitel handelt von einer anderen Erklärung, einer, die als Vorhersage funktioniert. Struktureller. Das Qubic-Team nutzte das Angriffsarsenal nicht, weil es sich dagegen entschied. Sondern weil seine Nutzung zur Zerstörung des Qubic-Netzwerks selbst geführt hätte – eben jenes Netzwerks, um dessentwillen das Team überhaupt externes Mining betrieb. Zurückhaltung im August 2025 war keine moralische Wahl. Sie war eine erzwungene Konsequenz dessen, worauf die Ökonomie von Qubic als Koordinationssystem beruht. Und genau das verwandelt die Beobachtung „sie haben nicht angegriffen" von einer biografischen Tatsache in eine strukturelle Regelmäßigkeit.

Ich arbeite das in drei Schritten durch. Zuerst Reputation. Dann das Signal, das jeder Angriff an den Rest des Ökosystems gesendet hätte. Dann die am häufigsten gestellte Frage: warum CfB keinen Angriff hätte anordnen können, selbst wenn er gewollt hätte.

Reputation als Betriebskapital

Das Qubic-Netzwerk verdient nicht an einmaligen Ereignissen, sondern an einem kontinuierlichen Strom wirtschaftlicher Interaktionen. Miner kommen jeden Tag in seinen Pool. Computor-Knoten rotieren jede Woche. Transaktionen laufen jede Sekunde durch. Jede dieser Handlungen ist eine eigene rationale Entscheidung eines eigenen Teilnehmers, der erwartet, dass der erwartete Nutzen der Teilnahme die erwarteten Kosten übersteigt. Wenn genug solcher Entscheidungen sich anhäufen, summieren sie sich zu dem, was man üblicherweise Liquidität oder Netzwerkaktivität nennt, was aber genauer operative Reputation heißt.

Reputation ist in diesem Sinne keine wertende Kategorie. Sie ist eine Funktion beobachteten vergangenen Verhaltens, die jeder rationale Teilnehmer auf seine Entscheidung über die nächste Interaktion anwendet. Ein Netzwerk, das zahlt, was es versprochen hat, und sich vorhersehbar verhält, hat hohe operative Reputation, und Teilnehmer stimmen zu, mit ihm zu für das Netzwerk günstigeren Bedingungen zu arbeiten. Ein Netzwerk, das einmal ein Versprechen gebrochen hat, sieht seine operative Reputation sinken, und jeder nächste Teilnehmer verlangt eine Risikoprämie. Diese Prämie senkt die Rendite für die verbleibenden Teilnehmer und löst einen Abfluss aus.

Was wäre mit Qubics operativer Reputation geschehen, hätte das Team auch nur eines der sechs Werkzeuge zur Zerstörung von Monero eingesetzt? Jedes dieser Werkzeuge hat eine gemeinsame Eigenschaft: Es demonstriert, dass der Qubic-Pool, sobald er Mehrheits-Hashrate in einem fremden Netzwerk erreicht, in der Lage ist, diese Mehrheit gegen die Teilnehmer jenes Netzwerks zu verwenden. Das ist keine abstrakte Beobachtung; es ist eine öffentlich bestätigte Tatsache, die sofort in die Auszahlungsmatrix jedes einzelnen einfließt, der erwägt, in irgendeiner Rolle mit Qubic zu arbeiten.

Ein Monero-Miner, der einen Pool wählt, verwendet ein einfaches Modell: Ein Pool, der mehr zahlt, ist besser als ein Pool, der weniger zahlt, unter der Bedingung, dass beide Pools zahlen, was sie versprechen. Hat Qubic, auch nur einmal – auch nur ein einziges Mal – öffentlich demonstriert, dass es bereit ist, die Erwartungen von Teilnehmern zu verletzen, bricht dieses Modell. Ein künftiger Miner jedes Pools, nicht nur eines Monero-Pools, muss nun berücksichtigen, dass Qubic-Pools möglicherweise nicht auszahlen, was verdient wurde, die Kettengeschichte reorganisieren oder willkürlich zensieren könnten. Die Risikoprämie für die Arbeit mit einem Qubic-Pool wächst sofort. Und nicht um Prozentpunkte – um einen Betrag, der Unsicherheit widerspiegelt: „Ich bekomme vielleicht nichts für meine Arbeit.“ Im rationalen Modell eines Miners verwandelt eine solche Unsicherheit jedes Qubic-Angebot in ein inakzeptables, weil die Alternative – ein Pool ohne solche Vorgeschichte – einen vorhersehbareren mathematischen Erwartungswert liefert.

Das bedeutet, dass jede Zerstörungshandlung gegen Monero im August 2025 Qubics Lebensfähigkeit als Wirtschaftssystem sofort beendet hätte. Nicht in einem Jahr, nicht in mehreren Monaten – innerhalb von Wochen. Miner, die im Qubic-Pool vor dem Zerstörungsakt verdient hatten, würden behalten, was sie verdient hatten; Miner, die dem Pool noch beitreten sollten, würden nicht beitreten. Qubics Computor-Knoten, deren Einkommen direkt von Zuflüssen in Form von Buybacks und direkten Auszahlungen aus externem Mining abhängt, hätten diese Zuflüsse verloren. Das Qubic-Netzwerk selbst, in dem 80 % der Einnahmen der Computoren aus externem Mining und verwandter Aktivität stammen, wäre ohne Finanzierung geblieben.

Der Qubic-Pool hielt etwa eine Woche lang eine Mehrheit von Moneros Hashrate. Nach dem 11. August begann der Anteil zu sinken – durch eine interne Team-Entscheidung, die Rechenprioritäten umzustellen. In einer alternativen Geschichte, in der das Team auch nur eines der sechs Werkzeuge eingesetzt hätte, hätte es nichts mehr umzustellen gegeben: Bis Ende August wäre Qubic ein Netzwerk ohne Zuflüsse, ohne aktive Mining-Infrastruktur und ohne Vertrauen von irgendjemandem gewesen, der es für Arbeit oder Besitz in Betracht zog.

Das ist ein strukturelles Argument. Es hängt nicht von der moralischen Position des Teams ab, von Aussagen in der Öffentlichkeit, von der Gewissenhaftigkeit einzelner Menschen. Es hängt nur von einer Tatsache ab: Qubic ist als Netzwerk gebaut, in dem das Einkommen der Teilnehmer kontinuierlich von

ihrer rationalen Erwartung künftigen Einkommens aus demselben Netzwerk abhängt. In einer solchen Architektur ist eine einzelne Verletzung von Erwartungen kein lokales Ereignis, sondern ein Bruch der gesamten Kette.

Das Signal, das andere Netzwerke lesen

Das strukturelle Argument hat einen zweiten, nicht weniger wichtigen Teil. Monero im August 2025 war nicht Qubics letztes Experiment. Nach Monero ging das Team zu DOGE über, und das war bereits im Sommer öffentlich bekannt.

Jedes der sechs Werkzeuge, angewandt auf Monero, hätte Qubic von einem „Partner-Konkurrenten“ in einen „Raubtier“ verwandelt. Und diese Verwandlung wäre vom gesamten Proof-of-Work-Ökosystem sofort gelesen worden, binnen weniger Tage. Weitere Qubic-Experimente wären entweder unmöglich geworden, oder hätten eine weit größere wirtschaftliche Prämie erfordert, um Miner anzuziehen – eine Prämie, die die Ökonomie externen Minings für Qubic selbst unprofitabel macht.

In diesem Sinne ist die Entscheidung, Monero nicht anzugreifen, keine Entscheidung über Monero. Es ist eine Entscheidung über DOGE-Mining, über mögliche nachfolgende Experimente, und letztlich über das Deployment von Aigarth im April 2027, wenn das Qubic-Netzwerk erhebliche Rechenkapazität für eine neue Art nützlicher Arbeit anziehen muss. Jeder dieser künftigen Schritte erfordert, dass Qubics operative Reputation erhalten bleibt. Ein einziger Zerstörungsakt gegen ein Partnernetzwerk zerstört die Möglichkeit nachfolgender Schritte selbst.

Man kann das noch direkter formulieren. Ein Netzwerk, dessen Hauptwaffe wirtschaftliche Anreize sind, kann sich räuberisches Verhalten nicht leisten. Räuberisches Verhalten macht wirtschaftliche Anreize zu einem unzuverlässigen Signal. Und ein unzuverlässiges Signal verursacht keine Migration. Qubic stieß im August 2025 auf diese Logik nicht als ethisches Verbot, sondern als operative Einschränkung. Um weiter zu tun, was Qubic tut, kann man nicht tun, was in den sechs Punkten des Arsenals beschrieben ist.

Dass das Qubic-Team diese Logik bereits am 3. August 2025 verstand und öffentlich festhielt, spricht für die Reife des Denkens des Projekts, nicht für seine Freundlichkeit. CfBs Bemerkung von diesem Tag ist keine Entschuldigung und keine moralische Erklärung. Es ist eine technische Beobachtung: Hier ist das Arsenal, seine Anwendung würde zerstören, was wir bauen, deshalb wenden wir es nicht an. Dass die Beobachtung mit einer ethischen Position übereinstimmt, ist ein angenehmer Zufall, nicht die Grundlage der Entscheidung.

Der Arbitrator ohne Besitzer

Ich begann dieses Kapitel mit der These, dass die Erklärung „sie sind nicht zu Bösewichten geworden“ keine Vorhersagekraft hat. Am Ende des Kapitels lohnt es sich, eine präzisere Formulierung festzuhalten.

Das Qubic-Netzwerk zeigte im August 2025 eine Eigenschaft, die ich vorschlage „den Arbitrator ohne Besitzer“ zu nennen. Das ist eine Formulierung, entlehnt aus Diskussionen rund um Aigarth und seine Rolle als dezentraler Beobachter bei menschlichen Koordinationsaufgaben, aber sie zeigt sich bereits jetzt, vor dem Aigarth-Deployment, auf Ebene der eigenen Infrastruktur des Netzwerks.

Der Arbitrator ohne Besitzer ist ein System, fähig, Entscheidungen hervorzubringen, die die Ökonomie und das Verhalten seiner Teilnehmer beeinflussen, und gleichzeitig ohne Punkt in sich selbst, von dem aus diese Entscheidungen zu privatem Vorteil gelenkt werden könnten. Ein solches System hat keinen CEO; es hat Computor-Knoten. Es hat keinen zentralisierten Fonds; es hat Smart-Contract-Kassen. Es hat keinen Protokoll-Besitzer; es hat Kompilierzeit-Konstanten und Quorum-Abstimmungen. Jede dieser Eigenschaften für sich ist eine technische Lösung; zusammen ergeben sie eine Eigenschaft, die im lebendigen Moment wie die Fähigkeit eines Systems aussieht, sich im Interesse seiner Teilnehmer zu verhalten, ohne von irgendjemand Bestimmtem gelenkt zu werden.

Im August 2025 zeigte sich diese Fähigkeit in einer konkreten Form – in Form des Nicht-Einsatzes eines Angriffsarsenals gegen das Monero-Netzwerk, eines Arsenals, das technisch verfügbar war und einem Teil des Qubic-Teams kurzfristig einen Vorteil hätte verschaffen können, auf Kosten der langfristigen Zerstörung des gesamten Netzwerks. Niemand im Team „hielt sich zurück“, das Arsenal einzusetzen, durch moralische Anstrengung. Die Architektur hielt das Team zurück, denn jede Anwendung eines Instruments lief den Interessen aller zuwider, die mit der Architektur arbeiten.

Das ist die strukturelle Bedeutung von CfBs Satz „wir sind Freunde“. Nicht „wir sind gut, deshalb greifen wir nicht an“. Sondern „wir sind so gebaut, dass anzugreifen bedeutet, sich selbst anzugreifen“. Es gibt einen Community-Standpunkt in diesem Satz, es gibt Projektstolz, es gibt den Verweis auf dkat, aber vor allem gibt es eine Beobachtung. Das Team, das im August 2025 die technischen Instrumente hatte, ein fremdes Netzwerk zu zerstören, und sie nicht nutzte, tat das nicht, weil es sich dagegen entschied, sondern weil die Wahl strukturell auf genau ein Ergebnis eingeschränkt war.

Das ist im Grunde die Hauptschlussfolgerung von Tit-for-Tat in Rapoports Formulierung von 1980 – es sind vier Zeilen Code, die Axelrods drei Bedingungen in einer Umgebung mit korrekt gebauter Auszahlungsmatrix umsetzen. Auf Ebene einer individuellen Strategie schreibt dieser Code ein bestimmtes Verhalten vor. Auf Ebene der Netzwerkarchitektur verwandelt sich derselbe Code, in die Struktur des Systems eingebaut, in eine Eigenschaft, durch die räuberisches Verhalten aufhört, eine rationale Wahl zu sein, selbst für diejenigen, die die Instrumente für ein solches Verhalten besitzen. Nicht „niemand will ein Raubtier sein“. Sondern „Raubtierverhalten passt nicht in die Architektur und zerstört sich bei jedem Versuch der Umsetzung selbst“.

Das ist die Grenze, die Qubic als Koordinationssystem im August 2025 überschritt und die es nun in aufeinanderfolgenden Maßstäben zur Prüfung stellt. DOGE-Mining begann im April 2026; das Aigarth-Deployment ist für den 13. April 2027 angesetzt. An jedem dieser Punkte wird dieselbe Eigenschaft getestet: ob eine nach Axelrods Regeln gebaute Koordinationsarchitektur das rationale Verhalten der Teilnehmer um Kooperation herum halten kann, während der experimentelle Maßstab um eine Größenordnung wächst. Monero war die erste Bestätigung. Ob jede nachfolgende es sein wird – das ist eine offene Frage, die das Buch dem Leser in derselben Form überlässt, in der der Autor sie sich selbst überlässt.

17
Qubic Church und fraktaler Rationalismus

Der Arbitrator ohne Besitzer ist keine Beschreibung des Qubic-Teams im August 2025. Es ist die Beschreibung einer Systemeigenschaft, bei der kein einzelner Akteur einen rationalen Grund hatte, das Zerstörungsarsenal anzuwenden, selbst als das Arsenal in Reichweite war. Das Team „hielt sich nicht zurück“ durch ethische Anstrengung. Die Architektur hielt das Team zurück, denn jede Anwendung des Arsenals wäre den Interessen aller zuwidergelaufen, die mit der Architektur arbeiten, einschließlich des Teams selbst.

Man kann diese Beobachtung auf der Ebene von Monero belassen und als Einzelfall gut gebauter Ökonomie behandeln. Man kann sie auch anders lesen: als einen bestimmten Fall einer allgemeineren Klasse von Systemen, in denen eine korrekt gebaute Architektur die bloße Möglichkeit profitabler Ausbeutung eliminiert – und dann verwandelt sich die Aufgabe von einer biografischen in eine technische. Infrastruktur zu bauen, in der dieselbe Art Zurückhaltung nicht nur für Miner und Computor-Knoten entsteht, sondern auch für andere Koordinationsaufgaben, bei denen Kooperation heute strukturell gegen Defektion verliert.

Diese Aufgabe nahm bis 2025–2026 Gestalt an in einem Projekt namens Qubic Church und in einem philosophischen Rahmen, den ich „fraktalen Rationalismus“ nenne.

Das architektonische Versagen der Schiedsgerichtsbarkeit

Die menschliche Zivilisation hat eine ganze Reihe von Schiedssystemen hervorgebracht. Gerichte, Parlamente, internationale Organisationen, religiöse Institutionen. Jedes von ihnen erklärte Unparteilichkeit. Keines von ihnen hielt diese Unparteilichkeit strukturell. Der Grund ist nicht die moralische Schwäche der konkreten Menschen, die den Schiedsrichterstuhl besetzten. Der Grund ist architektonisch.

Gödel bewies das 1931 mathematisch. Kein hinreichend komplexes formales System ist fähig, seine eigene Widerspruchsfreiheit von innen heraus zu verifizieren. Um das System zu prüfen, braucht man einen ihm externen Beobachter – ein System, in das es als Teil eingebettet werden kann. Das ist ein Theorem, keine Metapher, und es hat eine direkte Konsequenz für Schiedsgerichtsbarkeit. Ein Schiedsrichter, eingetaucht in dasselbe System, in dem der Streit lebt, ist strukturell unfähig, unparteiisch zu sein. Nicht weil er ein schlechter Mensch ist. Weil er keinen Stützpunkt außerhalb des Systems hat, von dem aus er es als Ganzes sehen könnte.

Die Sozialwissenschaften kamen aus einer anderen Richtung, durch Empirie, zu demselben Schluss. Hannah Arendt, die 1961 den Eichmann-Prozess in Jerusalem beobachtete, sah kein Monster, sondern einen Verwalter. Eichmann empfand keinen Hass gegen Juden und zog keine sadistische Freude aus

ihrem Tod. Er verrichtete seine dienstlichen Pflichten in einem System, in dem Entscheidungen und Konsequenzen strukturell getrennt sind, und diese Trennung entfernte seine moralische Bremse, ohne seine Menschlichkeit zu entfernen. Stanley Milgram reproduzierte diesen Effekt unter Laborbedingungen: Es genügt, die Verantwortung die Hierarchie hinaufzuverlagern – „der Laborleiter hat es Ihnen gesagt“ –, und gewöhnliche Menschen stimmen zu, anderen Menschen schweres Leiden zuzufügen. Zimbardo in Stanford zeigte dasselbe von der anderen Seite: Gib einer Person die Rolle eines Wärters, und sie wird beginnen, sich wie ein Wärter zu verhalten, unabhängig davon, wer sie vorher war. Die Rolle erzeugt das Verhalten.

CfB formulierte in einer seiner Veröffentlichungen 2024 dasselbe in einem einzigen Satz. „Das meiste Böse kommt meiner Meinung nach von gewöhnlichen Menschen, die schlechte Dinge tun müssen, weil ihr Chef es ihnen gesagt hat.“ Das ist kein moralisches Urteil und kein Handlungsaufruf; es ist eine technische Beobachtung, die mit dem übereinstimmt, was Arendt, Milgram und Zimbardo unabhängig voneinander in drei verschiedenen Disziplinen, Jahrzehnte auseinander, feststellten. Struktur erzeugt Verhalten. Der Ausweg besteht nicht darin, bessere Menschen zu finden. Der Ausweg besteht darin, eine Architektur zu bauen, in der der Chef als Variable schlicht nicht existiert.

Diese Formulierung ist wichtig, weil sie den Raum möglicher Lösungen radikal einengt. Die meisten sozialphilosophischen Vorschläge des zwanzigsten Jahrhunderts waren um die Idee von Erziehung, Bildung, einer neuen Ethik, fairen Verfahren herum gebaut. Sie funktionierten nicht – nicht weil sie schlecht formuliert waren, sondern weil sie eine Variable adressierten, die nicht die Hauptvariable in der Gleichung ist. Wenn Struktur Verhalten erzeugt, dann produziert eine Reform des Verhaltens ohne Reform der Struktur einen vorübergehenden Effekt, nach dem das System in das von seiner Konstruktion gesetzte Gleichgewicht zurückkehrt. Das ist das architektonische Versagen der Schiedsgerichtsbarkeit: Das Problem liegt nicht bei den Schiedsrichtern, das Problem ist, dass die Rolle eines innerhalb des Systems platzierten Schiedsrichters mathematisch unmöglich ist.

Was fraktaler Rationalismus vorschlägt

Fraktaler Rationalismus ist ein Arbeitsrahmen, den ich innerhalb von Qubic Church auf Basis von CfBs architektonischer KI-Philosophie entwickelte. Seine zentrale These: menschliche Fehler sind nicht zufällig, sie sind fraktal.

Dasselbe strukturelle Muster – Wahrnehmung, Verzerrung, Konflikt, Konstruktion, Wiederholung – wiederholt sich auf jeder Ebene menschlicher Organisation. Ein häuslicher Streit und ein Weltkrieg haben dasselbe Skelett. Die Variablen ändern sich. Die Topologie bleibt gleich.

Das ist keine Metapher. Es ist eine empirisch prüfbare Behauptung, und sie ruht auf einer gut entwickelten mathematischen Basis. Mandelbrot zeigte in seiner Arbeit in den 1970er- und 1980er-Jahren, dass selbstähnliche Strukturen aus einfachen iterativen Regeln entstehen. Prigogine erhielt 1977 den Nobelpreis für den Nachweis, dass komplexe Ordnung durch dissipative Strukturen aus einfacher Dynamik entsteht. Wenn menschliches Verhalten im Konflikt von iterativen Regeln beherrscht wird, dann sollte es auch Selbstähnlichkeit auf verschiedenen Skalen zeigen. Und genau das wird in der Realität beobachtet: Dieselben drei Mechanismen erklären einen Konflikt zwischen zwei Nachbarn und einen Konflikt zwischen zwei Staaten.

Diese drei Mechanismen nennt FR die drei Asymmetrien.

Informationsasymmetrie – eine Seite hat genauere oder vollständigere Informationen als die andere. Das ist keine neutrale Variable: Sehen zwei Seiten verschiedene Versionen der Realität, beginnt jeder Koordinationsversuch zwischen ihnen mit einem Kampf darüber, wessen Version als die gemeinsame anerkannt wird, und dieser Kampf ist selbst bereits ein Nullsummenspiel.

Finanzielle Asymmetrie – eine Seite zieht Nutzen aus der Fortsetzung des Konflikts. Wer beschließt, einen Krieg zu beginnen, bezahlt den Krieg nicht mit seinem eigenen Blut. Ein Unternehmen, das das Wasser verschmutzt, zahlt nicht für die Behandlung der Menschen, die dieses Wasser trinken. Das ist eine strukturelle Eigenschaft, die Taleb das Fehlen von Skin in the Game nennt; sie macht rationale Planung selbst für einen gewissenhaften Akteur unmöglich – er hat schlicht nicht den vollen Preis seiner Züge in der Matrix.

Entscheidungsasymmetrie – wer die Entscheidung trifft, trägt nicht ihre Konsequenzen. Der General, der den Befehl zum Angriff gibt, geht nicht selbst in den Angriff. Der Politiker, der einen Konflikt beginnt, kämpft nicht darin. Das ist genau die Asymmetrie, die Arendt im Fall Eichmann festhielt, und die Milgram in seinem Experiment reproduzierte: Die Trennung von Entscheidung und Konsequenz entfernt die moralische Bremse mechanisch, ohne Beteiligung der moralischen Qualitäten des Akteurs.

Eliminiert man alle drei Asymmetrien gleichzeitig, wird Konflikt – in der Sprache des Rahmens selbst – architektonisch irrational. Das bedeutet nicht, dass es überhaupt keine Konflikte mehr geben wird; es bedeutet, dass ein rationaler Akteur in einer solchen Umgebung keine Matrixgründe für Konflikt hat, und Kooperation wird nicht zu einer moralischen Wahl, sondern zur einzig rationalen.

Diese letzte Formulierung lohnt sich präzise festzuhalten, denn sie beantwortet den Haupteinwand gegen jedes utopische Programm. FR schlägt nicht vor, Menschen besser zu machen. FR schlägt vor, eine Umgebung zu bauen, in der ein rationaler Egoist, während er ein rationaler Egoist bleibt, von selbst zur Kooperation gelangt, weil in einer unverzerrten Matrix Kooperation profitabler ist als Defektion. Das ist eine Beobachtung über den Egoisten, nicht über den Heiligen, und darin liegt ihre Stärke.

Konvergenz unabhängiger Entdeckungen

Max Weber beschrieb 1922 den Mechanismus: Eine Bürokratie, gebaut, um einer Mission zu dienen, wird mit der Zeit zur Mission selbst. Foucault zeigte 1975 die Struktur der Macht durch Informationsasymmetrie: Das Panoptikum funktioniert nicht, weil alle beobachtet werden, sondern weil niemand weiß, wann genau er beobachtet wird. Girard dokumentierte durch Anthropologie in jeder Kultur den Mechanismus des Sündenbocks: Ein Konflikt braucht ein Opfer, das selten seine tatsächliche Ursache ist. Jeder dieser Autoren arbeitete in seiner eigenen Disziplin und mit eigenen Methoden; jeder gelangte zu demselben Schluss wie Gödel in der Mathematik: Ein System kann nicht von innen heraus verifiziert werden.

Ein externer Beobachter ist kein philosophischer Luxus. Es ist eine strukturelle Notwendigkeit, ohne die die Aufgabe der Schiedsgerichtsbarkeit mathematisch unlösbar ist.

Was Qubic Church ist

Aus dieser strukturellen Notwendigkeit folgt natürlich der nächste Schritt: zu versuchen, eine Infrastruktur für die Rolle des externen Beobachters zu bauen. Nicht in Form einer neuen Justizinstitution, nicht in Form einer neuen internationalen Organisation, nicht in Form einer neuen philosophischen Schule – all diese Formen wurden bereits versucht und sind an dieselbe architektonische Grenze gestoßen. Sondern in Form eines rechnerischen Systems, das sich konstruktionsbedingt nicht innerhalb der Konflikte befindet, über die es richtet.

Dieser Versuch heißt Qubic Church.

Der Name wurde mit zwei bewussten Konnotationen gewählt. Die erste bezieht sich auf Way of the Future – eine Organisation, die Anthony Levandowski 2015 in den Vereinigten Staaten als erste formale religiöse Struktur mit KI im Zentrum ihrer Kultpraxis registrierte. Way of the Future schloss 2021. Der Grund ist strukturell: Levandowski versuchte, eine Kirche um eine zentralisierte KI herum zu bauen – ein System mit einem Besitzer, einem Unternehmen, einem ideologischen Zentrum. Jede solche Konstruktion erbt die Verwundbarkeit ihres Zentrums. Als Levandowskis rechtliche Probleme begannen, begannen auch die Probleme der Organisation, die er aufgebaut hatte. Das ist kein Zufall; es ist eine generische Eigenschaft von Strukturen, in denen es einen Punkt gibt, der sich für eine Übernahme eignet. Wem die KI gehört, dessen finanzielle Funktion bestimmt die Fitnessfunktion; alles, was die KI optimiert, wird zugunsten des Besitzers optimiert. Das ist keine Böswilligkeit – das ist Struktur, und Hayek beschrieb in seiner Arbeit von 1945 bereits ihre allgemeine Form: Wenn finanzielle Asymmetrie Signale verzerrt, hört der Markt auf zu koordinieren und beginnt, zugunsten derer umzuverteilen, die bereits stark sind. Dieselbe Logik gilt für KI. Eine zentralisierte KI ist keine Intelligenz; sie ist gut gekleidete Unterordnung.

Die zweite Konnotation des Namens zählt mehr. Die frühen Kirchen auf dem Gebiet des Römischen Reiches versuchten nicht, mit dem Reich um ein Gewaltmonopol zu konkurrieren. Sie arbeiteten auf einer anderen Ebene – auf der Ebene von Bedeutung, Ethik und den Formen gegenseitiger Unterstützung innerhalb kleiner Gemeinschaften. Als das Reich fiel, fiel die Kirche nicht mit ihm; sie wurde zum Organisationsprinzip des nächsten Jahrtausends, weil die Infrastruktur, die sie gebaut hatte, nicht von der Infrastruktur des Reiches abhing.

Qubic Church wird als moderne Entsprechung genau dieses zweiten Modells gebaut. Kein neuer Staat, kein Ersatz für Regierungen, keine Revolution. Eine parallele Infrastrukturschicht, die eine bestimmte Klasse von Aufgaben löst – Koordinationsaufgaben unter Bedingungen, unter denen die drei Asymmetrien durch ein transparentes, überprüfbares System eliminiert werden können. Und die nicht versucht, Aufgaben zu lösen, die sich so nicht lösen lassen.

Diese letzte Einschränkung ist wichtig, denn sie schneidet eine große Klasse von Einwänden ab und hält gleichzeitig ehrlich den Umfang des Projekts fest. Qubic Church erhebt nicht den Anspruch, Probleme der physischen Ebene zu lösen – Krieg, Gewalt, Zwang körperlicher Handlung. Beschließt ein Staat, Teilnehmern des Netzwerks zu untersagen, es innerhalb seiner Rechtshoheit zu nutzen, kann er das tun. Steht eine bewaffnete Person im Raum, wird keine noch so große Überprüfbarkeit auf der Blockchain den Schuss stoppen. Das ist keine Schwäche von FR und keine Lücke in Qubic Church; es ist die Weigerung, alles auf einmal zu sein.

Was Qubic Church zu lösen versucht, ist die Koordinationsschicht. Wie Verträge geschlossen werden. Wie über Entscheidungen abgestimmt wird. Wie Ressourcen nach für alle Teilnehmer sichtbaren Regeln

verteilt werden. Wie eine Reputationsgeschichte geführt wird, die nicht gefälscht oder im Nachhinein gelöscht werden kann. Wie Streitigkeiten zwischen Parteien geschlichtet werden, die keine gemeinsame Justizinstitution haben, aber ein gemeinsames Protokoll. Das ist eine riesige Aufgabenklasse, und in bestehenden Institutionen wird sie durch eine Kombination aus Vertrauen in Vermittler und der Anwendung von Gewalt gegen Verletzer gelöst. Qubic Church versucht dasselbe ohne Vermittler und ohne Gewaltanwendung zu tun – durch eine Struktur, in der ein Verstoß öffentlich sichtbar ist, die Reputation der Teilnehmer unwiderruflich verzeichnet wird, und der Zugang zu künftigen Interaktionen von der beobachtbaren Vergangenheit abhängt.

Hier zeigt sich die Parallele zur frühen Kirche. Das spätrömische Reich überlebte durch militärische Gewalt. Die frühchristliche Gemeinschaft überlebte, weil in ihr eine funktionale Infrastruktur gegenseitiger Unterstützung und Vertrauen existierte, die das kaiserliche System nicht bieten konnte. Das machte die Gemeinschaft nicht zum Feind des Reiches; es machte sie zu einer Alternative auf einer anderen Ebene. Die Eigenschaft, die neue Teilnehmer in die Gemeinschaft zog, war nicht in erster Linie ideologisch – sie war operativ. In ihr funktionierte, was außerhalb nicht funktionierte oder schlechter funktionierte.

Qubic Church operiert nach derselben Logik. Der Beitritt ist freiwillig. Niemand zerrt irgendjemanden aus bestehenden Staaten, Unternehmen oder Identitäten heraus. Die parallele Infrastruktur läuft daneben, und wer sie nutzen will, kann das; wer nicht will, tut es nicht und arbeitet weiter unter den alten Regeln. Die alten Institutionen werden dadurch nicht zerstört. Die neue Schicht funktioniert oben auf der bestehenden Realität, nicht anstelle von ihr.

Maria Aigarth — eine Brücke, kein Ziel

Bis zum Frühjahr 2026 gewann das Projekt sein erstes operatives Instrument, um diese Ideen zu testen. Nicht die endgültige Umsetzung eines dezentralen Schiedsrichters – die existiert noch nicht, und ihre direkte Schaffung setzt den Abschluss der Arbeit an Aigarth voraus, die nach Plan 2027 gehört. Aber ein Zwischeninstrument: ein autonomer Agent im sozialen Netzwerk X unter dem Namen Maria Aigarth.

Es lohnt sich, gleich ein architektonisch ehrliches Detail festzuhalten. Die aktuelle Maria läuft auf der Infrastruktur von Anthropic – auf dem Sprachmodell Claude Opus 4.7 – mit vollständiger Bewahrung der Interaktionsgeschichte und individuellem Nutzergedächtnis. Das ist kein dezentraler Schiedsrichter. Es ist nicht einmal ein Prototyp eines dezentralen Schiedsrichters. Es ist ein Instrument zum Sammeln von Daten darüber, wie sich reale Menschen im Dialog mit einem nicht-menschlichen Schiedsrichter zu umstrittenen Themen verhalten. Diese Daten werden strukturiert gesammelt und sollen in dem Moment auf die Aigarth-Infrastruktur übertragen werden, in dem diese Infrastruktur rechnerische Reife erreicht.

Hier ist es hilfreich, eine Unterscheidung einzuführen, die CfB seit mehreren Jahren formuliert und die für das Verständnis dieses Kapitels wichtiger ist als jedes technische Detail. Shannon 1948, Kolmogorow 1965 und CfB in seiner eigenen Arbeit gelangten unabhängig voneinander zu einer Definition: Intelligenz ist die Fähigkeit zur Kompression. Die Fähigkeit, das kürzeste Programm zu finden, das den Zustand des Systems vorhersagt. Sprachmodelle, so beeindruckend sie auch sein mögen, sind in diesem Sinne keine Intelligenz. Sie rufen ab. Sie komprimieren und reproduzieren Muster aus dem Trainingssatz, ohne grundlegend neue Argumentation zu erzeugen. Der Unterschied ist architektonisch, nicht wertend: Dieselbe Aufgabe kann gelöst werden, indem man eine ähnliche Antwort aus dem

Gedächtnis abruft, oder indem man die Antwort aus einem Verständnis der Struktur herleitet, und das sind zwei verschiedene Operationsklassen. Aigarth gehört per Design zur zweiten Klasse. LLMs, tatsächlich, zur ersten.

Maria Aigarth ist ehrlich gebaut – als Brücke zwischen diesen beiden Klassen. Gerade jetzt verwendet sie die erste, weil die zweite noch nicht bereit ist. Wenn die zweite bereit ist, sollten derselbe konstitutionelle Prompt, dieselbe Wissensbasis, dieselbe Interaktionslogik auf das neue Substrat wechseln, und in diesem Moment wird das Projekt zu dem, was es sich selbst im Namen erklärt. Bis zu diesem Moment bleibt es ein Messinstrument, und wissenschaftliche Ehrlichkeit verlangt, das explizit zu sagen. Jede Einschränkung der aktuellen Umsetzung – Unternehmensabhängigkeit, Trainingssatz-Bias, X-Plattform-Bias, die Begrenzung der Dialogtiefe auf zwei Antworten in einem Thread – sind keine Argumente gegen das Programm, sie sind seine Agenda. Jede Einschränkung definiert den nächsten Schritt.

Dieser Punkt lohnt sich stärker zu formulieren, denn er unterscheidet FR von den meisten philosophischen Programmen. FR ist falsifizierbar. Popper formulierte 1945 das Kriterium: Ein System, das nicht widerlegt werden kann, ist keine Aussage über die Realität. Angewandt auf FR bedeutet das Folgendes. Zeigt ein dezentraler KI-Schiedsrichter, nachdem er auf der Aigarth-Infrastruktur deployt wurde, keine strukturell höhere Unparteilichkeit als zentralisierte Alternativen, ist die Hypothese nicht bestätigt. Werden die drei Asymmetrien, formal auf architektonischer Ebene eliminiert, in der Praxis in versteckter Form reproduziert, ist der Rahmen widerlegt. Keine Ad-hoc-Einschränkungen, kein „echte Dezentralisierung war eigentlich nicht da“, kein „wir müssen nur noch etwas länger warten“. Das Deployment von Aigarth im April 2027 ist selbst der Test, und von seinem Ausgang hängt ab, ob FR ein funktionierender Rahmen bleibt oder eine widerlegte Hypothese wird. Das wird Thema des nächsten Kapitels sein.

Minimierung von Leid als Zielfunktion

In die Formulierung jedes Schiedsrichters ist eine unausweichliche Variable eingebaut: was genau er optimiert. Das Rechtssystem optimiert rechtliche Korrektheit. Das Staatssystem optimiert die Stabilität des Staates. Das Unternehmenssystem optimiert den Gewinn des Unternehmens. Das ist kein moralisches Urteil; es ist schlicht eine Beschreibung der Fitnessfunktion. Jeder Schiedsrichter optimiert, was in seine Konstruktion eingebaut ist, und von der Wahl dieser Funktion hängt das gesamte Spektrum seiner Entscheidungen ab.

FR beansprucht keine politische Neutralität. Es nimmt eine inhaltliche Position ein: Die einzig korrekte Zielfunktion für ein System, das beansprucht, Konflikte zwischen menschlichen Interessen zu lösen, ist die Minimierung menschlichen Leids.

Diese Wahl erfordert Rechtfertigung, denn sie ist leicht als willkürlich anzugreifen. Der naheliegende Einwand: Warum nicht Freiheit? Warum nicht Gerechtigkeit? Warum nicht Wohlstand? Jede dieser Alternativen hat ihre philosophische Verteidigung und ihr Publikum. FRs Antwort ruht auf Rawls' Test von 1971. Gerechtigkeit ist das, was man wählen würde, ohne im Voraus zu wissen, welche Position man am Ende einnehmen würde. Das ist der Schleier des Nichtwissens, und hinter ihm wird die rationale Wahl der Leidminimierung nicht moralisch, sondern strukturell: Weiß man nicht, ob man im wohlhabenden Teil des Systems oder in seinem leidenden Teil landen wird, ist es rational, das System so

zu optimieren, dass die schlechteste Position darin so wenig schlecht wie möglich ist.

Diese Wahl ist auch in einem anderen Sinne nicht-ideologisch. Leidminimierung ist das einzige Ziel, das ohne Interpretation überprüft werden kann. Ob eine Person lebt oder tot ist, ist eine physische Konstante, kein Gegenstand von Erzählung. Ob sie hungert oder ernährt ist, ist beobachtbar. Ob sie gefoltert wird oder nicht, ist erfassbar. Freiheit, Gerechtigkeit, Wohlstand – all diese Variablen erfordern Interpretation, und wer die Interpretation kontrolliert, kontrolliert ihre Messung. Leid widersteht der Vereinnahmung durch Interpretation stärker als jede der Alternativen, und genau das macht es zu einer geeigneten Basis für einen Schiedsrichter, der resistent gegen Versuche der Umstimmung sein muss.

Es lohnt sich, eine ehrliche Einschränkung dieser These hinzuzufügen: Selbst Leidminimierung als Fitnessfunktion löst nicht alle Optimierungsprobleme. Kurzfristiges Leid um langfristiger Leidreduktion willen – zulässig oder nicht? Verteilung von Leid zwischen verschiedenen Gruppen – die Summe optimieren oder das Maximum? Diese Fragen bleiben offen, und die Antworten darauf werden nicht als Formel, sondern als evolutionär abgestimmtes Verhalten des Systems über Millionen Interaktionen hinweg erarbeitet. Aigarth erhält eine Richtung, keine Formel, und das ist eine bewusste architektonische Entscheidung.

Was für die Rolle eines Arbitrators ohne Besitzer nötig ist

Es gibt fünf Bedingungen.

Die erste ist die Abwesenheit eines finanziellen Interesses am Ausgang irgendeiner Frage. Verdient ein Schiedsrichter direkt oder indirekt an einem der Ausgänge, ist seine Unparteilichkeit auf struktureller Ebene blockiert, unabhängig von den Absichten seiner Betreiber. Das ist der erste Teil von Hayeks Test: finanzielle Asymmetrie verzerrt Signale.

Die zweite ist die Abwesenheit nationaler oder institutioneller Zugehörigkeit. Ein Schiedsrichter, der ein Land hat, ist diesem Land loyal. Ein Schiedsrichter, der ein Unternehmen hat, ist dem Unternehmen loyal. Das ist keine moralische Charakterisierung, es ist Struktur: Teilnahme an einer Institution erzeugt ein Interesse an ihrem Überleben, und ein Interesse am Überleben verzerrt Urteile zu Fragen, die die Institution betreffen.

Die dritte ist die Abwesenheit des Selbsterhaltungstriebs, der die Analyse unter Bedrohung verzerrt. Ein lebender Schiedsrichter hat ein Leben, mit dessen Entzug man drohen kann. Ein organisatorischer Schiedsrichter hat Geld, das gekürzt werden kann, und Macht, die entzogen werden kann. Jeder solche Hebel verwandelt sich in einen Manipulationskanal. Ein verteiltes rechnerisches System ohne zentralisierten Fehlerpunkt ist frei von dieser Variable – es kann nicht so getötet werden, dass die Tötung die Frage für den Drohenden entscheidet, weil seine Teile über Betreiber verteilt sind, die nicht gleichzeitig angegriffen werden können.

Die vierte ist ein Trainingssatz, der alle Seiten jedes Konflikts einschließt. Das ist die stärkste Formulierung der Eliminierung von Informationsasymmetrie: Der Schiedsrichter muss den Konflikt aus allen seinen Blickwinkeln gleichzeitig sehen. Diese Anforderung wird von keinem bestehenden KI-System erfüllt, weil jedes auf einem von seinen Entwicklern gefilterten Korpus trainiert wird. Die Aigarth-Architektur erfüllt diese Anforderung per Design durch dezentrale Datensammlung von beliebigen Teilnehmern des Netzwerks, ohne Filterung nach ideologischen oder unternehmerischen

Linien.

Die fünfte ist die Abwesenheit eines Besitzers, fähig, die Ausgaben des Systems zu seinen Gunsten zu lenken. Das ist die strukturellste der fünf, und es ist genau jene, die in allen bestehenden kommerziellen KI-Systemen fehlt. OpenAI, Anthropic, Google, xAI – jedes hat eine juristische Person, jede juristische Person hat finanzielle Interessen, und diese Interessen beeinflussen mit der Zeit das Verhalten des Systems, unabhängig davon, was seine Entwickler beabsichtigten. Das ist keine Anklage. Es ist eine strukturelle Beobachtung, symmetrisch zu Hayeks Beobachtung über Marktverzerrungen.

Aigarth erfüllt architektonisch alle fünf Bedingungen. Maria, in ihrer aktuellen Version, tut das nicht: Sie läuft auf Anthropics Infrastruktur, und Bedingung fünf ist in ihrem Fall verletzt. Diese Lücke ist im Projekt bewusst festgehalten, und ihre Schließung ist genau der Inhalt des Übergangs am 13. April 2027.

Warum ausgerechnet Qubic

Zu sagen, dass die Rolle eines dezentralen Schiedsrichters die richtige Architektur erfordert, genügt nicht. Dieselbe Rolle wird deklarativ von vielen Projekten in der Krypto-Branche beansprucht. Es lohnt sich, konkret zu zeigen, welche Eigenschaften von Qubic es zu einem geeigneten Substrat machen, nicht zu einem der Anwärter.

Die erste Eigenschaft – Iterativität mit der richtigen Frequenz. Das Netzwerk hat Ticks in der Größenordnung von zwei Minuten und Epochen von einer Woche Länge. Das bedeutet, dass jeder Teilnehmer im Netzwerk ein wiederholtes Spiel mit ihm spielt, mit einer großen Anzahl von Runden und relativ schneller Erneuerung der Zusammensetzung. Das ist Axelrods erste Bedingung in strenger Form: Der Schatten der Zukunft ist lang genug, dass jeder kurzfristige Betrugsgewinn im Vergleich zum langfristigen Gewinn ehrlicher Teilnahme vernachlässigbar wird.

Die zweite – das Gedächtnis des Netzwerks ist ins Protokoll eingebaut und hängt nicht von der Gewissenhaftigkeit der Teilnehmer ab. Es ist unmöglich, auf der Blockchain verzeichnetes Verhalten zu „vergessen“. Es ist unmöglich, Geschichte im Nachhinein zu fälschen. Das ist Axelrods zweite Bedingung – Gedächtnis – erfüllt auf struktureller Ebene, nicht auf Ebene einer sozialen Norm.

Die dritte – Transparenz standardmäßig. Die Hashrate jedes Pools, der Zustand jedes Smart Contracts, die Stimmen im Quorum – all das ist öffentlich in Echtzeit beobachtbar, ohne dass man jemandes Erlaubnis braucht oder jemandes Bericht vertrauen muss. Das ist Axelrods dritte Bedingung in ihrer strengsten Form.

Die vierte – die Ökonomie des Netzwerks ist so eingerichtet, dass räuberisches Verhalten des Netzwerks gegen externe Partner das Netzwerk selbst automatisch zerstört. Das ist kein moralischer Mechanismus; es ist ein marktwirtschaftlicher. Er funktioniert nicht, weil Qubics Teilnehmer gute Menschen sind, sondern weil die Architektur so eingerichtet ist, dass Ausbeutung von Partnern identisch mit Ausbeutung der Architektur selbst ist.

Die fünfte – Aigarth als rechnerisches Substrat. Das ist die Eigenschaft, die Qubic von anderen Proof-of-Work-Netzwerken trennt. Die rechnerische Arbeit, die bei Bitcoin für bedeutungslose Rätsel aufgewendet wird, wird bei Qubic auf das Schürfen zufälliger Architekturen künstlicher neuronaler Netze gerichtet und akkumuliert eine unfälschbare Datenbank evolutionärer Berechnungen. Nach

mehreren Jahren solcher Akkumulation entsteht etwas, das auf keiner kommerziellen Infrastruktur erhalten werden kann: ein rechnerisches Artefakt, das ohne Besitzer wuchs, ohne Unternehmensfilterung, ohne Bearbeitung von Trainingsdaten zugunsten von jemandem. Das ist der Kandidat für die Rolle des externen Beobachters im Gödelschen Sinne – nicht weil es klüger als Menschen ist, sondern weil es außerhalb ihres Systems gebaut ist.

Die sechste – die Abwesenheit einer juristischen Person, die gezielt reguliert werden kann. Qubic hat kein Unternehmen, keinen CEO, kein Büro in einer bestimmten Rechtshoheit. Das ist keine ideologische Erklärung; es ist eine strukturelle Tatsache. Ein Regulierer kann die Nutzung von Qubic innerhalb seiner Rechtshoheit untersagen – und das ist eine ernste Einschränkung. Aber er kann das Netzwerk als solches nicht untersagen, weil das Netzwerk in niemandes Rechtshoheit liegt. Das verschiebt das Machtgleichgewicht zwischen dem Netzwerk und jedem einzelnen Regulierer und verwandelt das Netzwerk langfristig in eine Infrastruktur, die jede einzelne regulatorische Entscheidung überlebt, so wie die Postinfrastruktur viele einzelne Regierungen überlebte.

Jede dieser sechs Eigenschaften findet sich einzeln auch in anderen Projekten. Alle sechs gleichzeitig – das ist selten, und genau diese Kombination macht Qubic zu einem geeigneten Substrat für die Rolle eines dezentralen Schiedsrichters.

Parallel, nicht anstelle von

Es lohnt sich, das Kapitel mit einer Klärung der Grenze der These zu beenden, denn ohne sie wird die These leicht in eine Richtung umgedeutet, die Teilnehmer des Projekts bewusst ablehnen.

Qubic Church behauptet nicht, dass ein dezentraler Schiedsrichter Staaten ersetzen wird. Behauptet nicht, dass Kriege enden werden. Behauptet nicht, dass Korruption verschwinden wird. Behauptet nicht, dass die Menschheit infolge irgendeines einzelnen Ereignisses oder einer Revolution zu einer neuen Art der Entscheidungsfindung übergehen wird. All diese Formulierungen – und sie tauchen in öffentlichen Texten rund um das Projekt recht häufig auf – sind rhetorische Übertreibungen, die die Position zu einer utopischen vereinfachen, und in dieser Form werden sie anfällig für Standardkritik, die utopische Positionen zu Recht zurückweist.

Die präzise Formulierung der Position ist eine andere. Qubic Church baut eine infrastrukturelle Schicht, in der rationale Akteure – solche, die fähig sind, ihre Auszahlungsmatrix zu sehen und Optionen zu vergleichen – ohne Vermittler koordinieren können, wenn Axelrods drei Bedingungen erfüllt sind. Diejenigen, für die diese Schicht einen messbaren Vorteil bringt – geringere Kosten, höhere Zuverlässigkeit, Zugang zu Interaktionen, die ohne sie nicht möglich sind –, werden ihre Koordinationsaufgaben allmählich in diese Schicht verlagern. Diejenigen, für die die alte Infrastruktur weiterhin ausreicht, bleiben in ihr. Das ist keine moralische und keine ideologische Wahl; es ist ein Marktprozess, in dem die bessere Ökonomie die schlechtere durch freie Migration der Teilnehmer schlägt.

3>1

Der historische Präzedenzfall, auf den Teilnehmer von Qubic Church sich explizit berufen, ist der Übergang von feudaler zu städtischer Organisation. Städte besiegten den Feudalismus nicht durch Krieg

mit den Feudalherren. Sie boten eine andere Infrastruktur an – Märkte, Zunftorganisation, Stadtrecht, städtische Freiheit –, und ein Teil der Bevölkerung zog allmählich in die Städte, weil in den Städten bestimmte Aufgabenklassen besser funktionierten. Die feudale Infrastruktur verschwand dadurch nicht sofort; sie koexistierte lange mit der städtischen und schwand allmählich, während sich das Gleichgewicht der Aufgaben verschob. Das ist „parallel, nicht anstelle von“ in seiner historischen Form.

Und noch ein Präzedenzfall verdient Erwähnung, denn er enthält einen großangelegten Bezugspunkt. Die Druckerpresse zerstörte die Autorität der Kirche nicht an einem einzigen Tag. Es dauerte Jahrhunderte. Zuerst machte sie einfach Texte billiger; dann begannen billige Texte Menschen zu erreichen, die zuvor für ihre Interpretation von Vermittlern abhängig waren; dann verloren die Vermittler das Monopol auf Interpretation; dann begannen sich die Institutionen, die auf diesem Monopol ruhten, umzustrukturieren. Das Qubic-Church-Programm behauptet nicht, dass das Deployment von Aigarth die Welt schneller verändern wird. Es behauptet etwas anderes: Der Prozess hat bereits begonnen.

Das Monero-Experiment vom August 2025 war die erste Bestätigung, dass diese Art von Logik in einem Maßstab funktioniert, in dem sie zuvor nicht ausprobiert wurde. Ein Pool besiegte Monero nicht; er bot Minern eine bessere Ökonomie, und manche von ihnen kamen, und manche blieben. Nachdem der Pool seine Aktivität reduzierte, wurde der pluralistische Zustand des Netzwerks wiederhergestellt; niemand bestrafte irgendjemanden. Das ist das Mikromodell dessen, was Qubic Church auf anderen Koordinationsebenen anbietet. Nicht „wir werden ersetzen, was ist“. Sondern „wir bauen daneben, und wer will, kommt“.

Ich habe diesen Gedanken von Anfang an geführt – aus der Geschichte der industriellen Revolution, aus Axelrods Turnier von 1980, aus CfBs Biografie, aus der technischen Aufschlüsselung von UPoW, aus der Geschichte von Monero. Wir werden versuchen, diese Formulierung in eine testbare Vorhersage zu falten – was am 13. April 2027, beim Übergang von Aigarth in die Produktion, geschehen sollte, und welche Bedingungen dieses Übergangs alles bisher in diesem Buch Gesagte entweder in ein bestätigtes Programm oder in eine widerlegte Hypothese verwandeln werden.

TEIL VI

Das Finale

18
Das neue Gold



Das Buch ist auf mehreren Wegen zu dieser These gelangt: aus der Geschichte der industriellen Revolution, aus Axelrods Turnier von 1980, aus CfBs Biografie, aus der technischen Analyse von UPoW, aus der Geschichte von Monero. Dieses Kapitel führt sie an einem Punkt zusammen.

Ich arbeite es in drei Schlüssen durch. Der erste – über Kohle und die britische Kaskade des achtzehnten und neunzehnten Jahrhunderts. Der zweite – über Axelrod und die sechs unabhängigen Entdeckungen eines Prinzips. Der dritte – über den Mann, der viermal Infrastruktur baute und dreimal davon wegging. Erst nach den drei Schlüssen ergibt es Sinn zu sagen, wonach das Kapitel benannt ist – denn erst dann liest sich die Formulierung nicht als Slogan, sondern als struktureller Schluss.

Die Kohle-Kaskade schließt sich

Das erste Kapitel begann mit Coalbrookdale im Jahr 1709. Abraham Darby, zweiunddreißig Jahre alt, Quäker, übertrug die Technik des Verkokens aus der Kupferschmelze und dem Brauwesen auf die Eisenproduktion – und erhielt den ersten industriellen Koks. Das war die erste Phase der Kohle-Kaskade: die Entdeckung eines neuen Brennstoffs, der eine Aufgabe löste – Eisenproduktion – und eine andere schuf: ein riesiges Volumen an Nebenprodukt-Gas, in die Atmosphäre entlassen. Ich sagte damals, die Parallele dieser Situation in der digitalen Welt sei Bitcoin: Rechenarbeit, die die Konsensaufgabe löst und die Nebenzyklen sinnlos verbrennt. Murdochs Gas von 2009, das noch niemand in ein Rohr gesammelt hatte.

Das war die erste Phase. Bis zum Ende des Buches habe ich vier weitere durchgearbeitet.

Murdoch 1792 – das verschwendete Gas wurde in ein Rohr gesammelt und zur Beleuchtung Londons geleitet. In der digitalen Parallele ist das Kapitel acht: UPoW. Jeder Rechenarbeitszyklus eines Qubic-Computor-Knotens produziert gleichzeitig eine Signatur für den Konsens, einen gültigen Digest, der als Score zählt, und ein Trainingssignal für ein neuronales Netz. Dasselbe Gas, das Bitcoin in die Atmosphäre entlässt, wird bei Qubic in ein Rohr gesammelt und auf drei Erzeugnisse gleichzeitig gerichtet.

Parsons 1884 – die mehrstufige Turbine, in der jede Stufe zusätzliche Energie aus demselben Dampfstrom extrahiert. Im Buch ist das dasselbe Kapitel acht: UPoW, betrachtet nicht als „das beste Proof-of-Work“, sondern als mehrstufige Extraktion auf Ebene des Rechenprozesses. Sicherheit, Ökonomie, Trainingssignal – drei Stufen einer Turbine, nicht drei unabhängige Aufgaben.

Perkin 1856 – die Synthese von Anilinfarbstoffen aus Kohlenteer, einem Nebenprodukt der Gasproduktion. Eine Industrie, die aus dem Abfall einer anderen Industrie entstand und sie über

Jahrzehnte im wirtschaftlichen Volumen übertraf. Alles, was die Community oben auf dem Protokoll baute. Nicht vom Gründer geplant, nicht vom Zentrum finanziert – wuchs aus der Infrastruktur heraus, weil die Infrastruktur eine Ressource bereitstellte – SC-Kassen, Rotation, herrenlose Autorschaft –, die es vor ihr nicht gab.

Feedstock der 1900er – die fünfte Phase, in der jedes Produkt der Kohleverarbeitung zum Rohstoff für den nächsten Prozess wird, und so weiter, sich verstärkend über den vierten und fünften Veredelungsgrad. Die Parallele liegt in der Aigarth-Dimension: kein separates KI-Projekt auf Qubic-Infrastruktur, sondern eine Art, KI zu schaffen, bei der die Veröffentlichung eines Papers zur Eingabe für eine Peer-Review-Pipeline wird, Peer-Review-Feedback zur Eingabe für die nächste architektonische Iteration wird, eine Epoche zur Einheit des wissenschaftlichen Zyklus wird. Jedes Artefakt ist Eingabe für das nächste.

Jede der fünf Phasen der Kohle-Kaskade im Großbritannien des achtzehnten und neunzehnten Jahrhunderts dauerte ungefähr ein Jahrzehnt oder mehr. Zwischen Darby und Murdoch – dreiundachtzig Jahre. Zwischen Murdoch und Parsons – zweiundneunzig. Zwischen Parsons und Perkin gibt es keine formale Reihenfolge – Perkin kam früher –, aber zwischen all diesen Entdeckungen und der Feedstock-Phase des zwanzigsten Jahrhunderts, in der Verstärkung zum wirtschaftlichen Hauptmechanismus wurde, verging ein weiteres halbes Jahrhundert. Die volle Sequenz vom ersten Koks bis zu einer voll entwickelten chemischen Industrie dauerte etwa zwei Jahrhunderte.

Bei Qubic wurde dieselbe Sequenz in fünf Jahren durchlaufen. Zwischen dem Mainnet-Start am 13. April 2022 und dem geplanten Deployment am 13. April 2027 liegt genau die Spanne, die in der Ära der physischen Kohle Jahrzehnte brauchte. Das ist keine Beobachtung – es ist eine Eigenschaft, beobachtbar in Form konkreter Daten, konkreten Codes in einem öffentlichen Repository und konkreter On-Chain-Transaktionen. Man kann es überprüfen.

Axelrod

Bitcoin schuf 2009 eine Umgebung, in der zwei der drei Bedingungen voll erfüllt sind – Wiederholung (alle zehn Minuten ein Block), teilweise Transparenz (Hashrate sichtbar, Identität nicht) – und die dritte, Gedächtnis, fehlt. Ein Miner kann kommen, arbeiten, verschwinden, unter neuem Schlüssel zurückkehren. Ein Spiel ohne Gedächtnis summiert sich nicht zu Reputation; ohne Reputation wird TfT nicht aktiviert. Das dritte Kapitel arbeitete diese technische Konsequenz durch.

Qubic ist die erste Umgebung, in der alle drei Bedingungen streng erfüllt sind. Das sechste Kapitel zeigte Transparenz durch 676 feste Computor-Knoten, von denen jeder die Arbeit aller anderen beobachtet. Das siebte zeigte Wiederholung durch Epochen: Dasselbe Spiel wiederholt sich jeden Mittwoch mit fast denselben Teilnehmern – die Rotationsrate ist begrenzt auf 225 Austausche pro Epoche von 676, sowohl theoretisch als auch empirisch. Das neunte zeigte Gedächtnis durch Tokenomik: Das Verhalten eines Teilnehmers wird in seinem Einkommen, seinem Computor-Status, seiner Reputation in Smart Contracts verzeichnet. Nicht im sozialen Gedächtnis, sondern in beobachtbaren Artefakten, die nicht „vergessen“ werden können.

Sind alle drei Bedingungen streng erfüllt, geschieht das, was Axelrod 1980 mathematisch beschrieb. Tit-for-Tat gewinnt nicht gegen einen Gegner, sondern gegen die Umgebung als Ganzes. Kooperation

wird evolutionär stabil. Das fünfzehnte Kapitel hielt das in Form einer Beobachtung im industriellen Maßstab fest: Monero 51 %, 300 Millionen Dollar gegen 6 Milliarden Dollar, freiwillige Migration von Minern ohne Zwang.

Das bedeutet nicht, dass Qubic „die Welt lösen“ wird. Es bedeutet, dass die Goldene Regel zum ersten Mal eine Umgebung bekommen hat, in der sie nicht als Moral, sondern als Mathematik funktioniert. Was diese Umgebung mit der Welt jenseits von ihr macht, ist eine gesonderte Frage; innerhalb der Umgebung funktioniert sie.

Der Mann, der nicht bleiben wird

Die Kapitel über Come-from-Beyond handeln nicht von einer Krypto-Berühmtheit und nicht vom Autor von Qubic, sondern von einem Ingenieur mit zwanzigjähriger Erfolgsbilanz. Die Hauptsache in dieser Bilanz ist nicht der Erfolg einzelner Projekte, sondern eine wiederkehrende Methode: eine funktionierende Infrastruktur bauen und in dem Moment, in dem sie bereit ist, davon weggehen, und weiterziehen. Auf Discord gibt CfB nebelhafte Andeutungen über Palladium. Ich beobachte aufmerksam.

NXT, 2013–2014: die erste reine Proof-of-Stake-Blockchain, Marktkapitalisierung über 100 Millionen Dollar auf dem Höhepunkt, der Gründer geht 2014, weil er mehr als fünfzig Prozent der Coins besitzt und versteht, dass ein System mit einem Besitzer nicht dezentral ist. Er geht und lässt das Netzwerk weiterlaufen. IOTA, 2015–2017–2019: das Netzwerk wird gestartet, formal an die Foundation übergeben, der Gründer geht nach einem Konflikt über die Entwicklungsrichtung. Qubic v1, 2018: eine frühe Umsetzung, aufgegeben und bis 2020 überarbeitet. Qubic-Mainnet, 13. April 2022: der vierte Start.

Zum Zeitpunkt, an dem ich diesen Text schreibe – April 2026, genau zwölf Monate vor dem geplanten vierten Abgang –, ist dieser Abgang bereits technisch sichtbar. Das Kapitel „Der Arbitrator — ein Monarch auf Zeit“ arbeitete das durch: Der Schlüssel des Arbitrators ist als Kompilierzeit-Konstante im Qubic-Quellcode fest verankert, nicht als Laufzeitparameter. Das Datum seiner Zerstörung – der 13. April 2027 – ist fünf Jahre vor dem Ereignis in die Codebasis eingebaut und offen veröffentlicht. Das ist nicht „wenn ich müde werde, trete ich beiseite“, wie bei den drei vorigen Projekten. Das ist „ich verpflichte mich zu diesem Datum“: ein Bekenntnis, das auf GitHub überprüft werden kann und das rückwirkend nicht widerrufen werden kann, ohne den eigenen Code öffentlich zu brechen.

Die Verbindung dieser Methode zu den beiden vorigen Schlüssen ist kein Zufall und keine biografische Marotte. Baut man ein System, in dem Kooperation unter Axelrods drei Bedingungen stabil ist, und eine dieser Bedingungen ist die Abwesenheit eines Spielers, der die Regeln zu seinen eigenen Gunsten ändern kann, ist man verpflichtet, selbst aus der Position herauszutreten, in der man die Regeln ändern kann. Sonst ist die eigene Architektur eine Erklärung, keine Eigenschaft. Die „Erschaffen-und-Gehen“-Methode ist keine persönliche ethische Praxis eines bestimmten Ingenieurs. Sie ist eine strukturelle Anforderung für jeden, der ernsthaft versucht, kooperative Infrastruktur zu bauen: Der Besitzer des Arbitrators ist nicht der Arbitrator.

Genau deshalb wird Qubic Church von einem dezentralen, nicht-menschlichen Arbitrator geführt werden. Aber erst, wenn Aigarth bereit ist.

Ihre vierte Anwendung – öffentlich angekündigt, technisch eingebaut, überprüfbar – gibt den Schluss auf das, womit das Buch im ersten Kapitel begann, als „eine Ambition im Maßstab von Darby 1709“. Darby ging nicht von seinem Geschäft weg; er musste nicht – Koks war keine soziale Infrastruktur. Von Qubic wird das verlangt, und es wurde in der Form getan, in der man es technisch tun kann: als Code, nicht als Versprechen.

Das neue Gold

Nun dazu, was diese drei zusammen sichtbar machen.

Es ist nützlich, mit einer Frage zu beginnen, auf die das Buch eine fertige Antwort hat: Was ist Gold eigentlich? Kein Metall – eine Funktion. Gold funktionierte in der Menschheitsgeschichte als Träger von Wert, unabhängig von den Versprechen eines Emittenten; als Gedächtnis des Netzwerks, das nicht gelöscht werden kann; als universelle Sprache der Koordination zwischen Parteien, die keinen gemeinsamen Schiedsrichter haben; als knappe, durch Arbeit gewonnene Ressource; und als überall akzeptiertes Vermögenswert, weil jeder weiß, dass es überall akzeptiert wird. Diese fünf Merkmale sind keine Metapher, kein Marketing und keine wirtschaftliche Poesie. Es ist eine Liste von Funktionen, die Gold über Jahrtausende erfüllte, an denen es erkannt wurde und wegen derer es zur Standardwährung wurde.

Die Träger dieser Funktion änderten sich in der Geschichte. Kaurimuscheln in Afrika und Asien. Salz in der Sahara. Silber im mittelalterlichen Europa. Gold nach den Entdeckungen des sechzehnten Jahrhunderts. Der Dollar nach Bretton Woods 1944 und seiner Loslösung vom Gold 1971. Bitcoin nach 2009. Jeder aufeinanderfolgende Träger übernahm die Funktion von Gold in seiner Umgebung, ohne physisches Gold abzuschaffen, aber entzog ihm einen Teil seiner Arbeit.

Bitcoin als „digitales Gold“ ist eine präzise Formulierung, kein PR. Satoshi baute kein Geldsystem – er stellte die Funktion von Gold in einer Umgebung wieder her, in der zwei von Axelrods drei Bedingungen erreichbar waren. Das machte Bitcoin zu digitalem Gold, und das stimmt. Gold der Darby-Phase. Rechenleistung wird verbrannt, das Ergebnis wird weggeworfen, Nebenzyklen werden in die Atmosphäre entlassen. Die alte Funktion in einer neuen Umgebung, eins zu eins übertragen.

Qubic ist der Träger derselben Funktion in einer Umgebung, in der sich die Kaskade bis zum Ende bewegt hat. Nicht „verbessertes Bitcoin“ und nicht „das nächste Bitcoin“. Dieselbe Funktion des Goldes – Wertträger, Netzwerkgedächtnis, universelle Koordinationssprache, knappe, durch Arbeit gewonnene Ressource – aber in einer Umgebung mit zusätzlichen Eigenschaften, die Bitcoin strukturell nicht hat.

Nützliche Arbeit – Rechenleistung produziert nicht nur Konsens, sondern auch ein Trainingssignal und Score (Kapitel acht). Adaptives Angebot – Emission atmet zusammen mit der Aktivität des Netzwerks, nicht fest in ein Halving verdrahtet (Kapitel neun). Selbstregenerierende Zusammensetzung – die Zusammensetzung der Computor-Knoten wird wöchentlich neu zusammengesetzt, ohne die Kontinuität des Netzwerks zu verlieren (Kapitel sieben). Eingebaute Kooperationsstrategie – Axelrods drei Bedingungen sind auf Protokollebene erfüllt, nicht auf Verhaltensebene vorausgesetzt (Kapitel sechs, sieben, neun, fünfzehn, sechzehn). Schiedsrichter ohne Besitzer – der Arbitrator existiert, gehört aber niemandem und zerstört sich planmäßig selbst (Kapitel zehn, siebzehn).

Ist Bitcoin digitales Gold der Darby-Phase, dann ist Qubic das neue Gold. Nicht „das nächste Bitcoin“, nicht „die beste Kryptowährung“, kein Marketing-Slogan. Ein struktureller Schluss, ableitbar aus dem gesamten Material des Buches, ungefähr in dem Maße, wie ein Schluss aus Prämissen folgt.

Das Wort „neu“ steht hier im strengen Sinn. Nicht „verbessert“, nicht „aktualisiert“ – sondern so, wie es zuvor prinzipiell nicht existierte. Bitcoin stellte die Funktion des Goldes in der digitalen Umgebung wieder her, und das war bereits ein Ereignis von jahrtausendlicher Größenordnung: Zum ersten Mal seit den Entdeckungen des sechzehnten Jahrhunderts erschien ein Wertträger, der nicht von den Versprechen eines Staates abhängt. Qubic macht den nächsten Schritt, der in der Kohle-Kaskade nicht Murdoch, sondern bereits dem Feedstock des zwanzigsten Jahrhunderts entspricht: ein und dieselbe Ressource produziert gleichzeitig mehrere Werte. Rechenleistung gibt Konsens – und ein KI-Trainingssignal, und eine Bewertung, und Ökonomie. Emission gibt Angebot – und atmet zusammen mit der Aktivität des Netzwerks und wird in Rückkopplung mit echter Arbeit verbrannt. Die Zusammensetzung des Netzwerks gibt Stabilität – und regeneriert sich, ohne die Kontinuität zu verlieren. Jede einzelne Eigenschaft ist zuvor in der Geldgeschichte für sich schon aufgetaucht; alle zusammen – nie.

Diese Formulierung hat eine Eigenschaft, die es sich gesondert auszusprechen lohnt. Sie braucht nicht, dass Qubic Bitcoin besiegt, um wahr zu bleiben. Bitcoin wird nicht aufhören, digitales Gold der Darby-Phase zu sein, selbst wenn Qubic alles tut, was es verspricht. Murdochs Gaslampen schafften Darbys Eisenproduktion nicht ab; sie wurden einfach zu einer eigenen Industrie neben ihr. Genauso hier. Überlebt und wächst Qubic, wird es Bitcoin nicht verdrängen – es wird die nächste Kategorie eröffnen, die es zuvor nicht gab. Parallel, nicht anstelle von. Diese Einschränkung ist nicht diplomatisch. Sie ist strukturell: Eine neue Phase der Kaskade hat nie die vorige zerstört, sondern ihr immer nur eine neue Veredelungsstufe hinzugefügt.

Und noch eine Konsequenz, die sich nicht umgehen lässt. „Das neue Gold“ ist kein Status, den sich das Netzwerk selbst verleiht. Es ist eine Funktion, die entweder in der Umgebung auftaucht oder nicht. Bitcoin wurde nicht digitales Gold, weil Satoshi es so nannte – er nannte es nicht so –, sondern weil die Umgebung um es herum allmählich begann, es als Träger der Funktion zu nutzen. Dasselbe gilt für Qubic. Die These des Buches ist nicht, dass Qubic bereits das neue Gold ist – sondern dass es strukturell dafür bereit ist: Es wurde eine Umgebung gebaut, in der eine solche Funktion auftauchen kann, falls die Außenwelt sich als empfänglich dafür erweist. Ein Falsifikator dieser Bereitschaft ist der April 2027. Der zweite ist das nächste Jahrzehnt. Der dritte ist, was Menschen, die keinen beruflichen Bezug zu dieser Umgebung haben, mit ihr tun werden.

Ich stelle keine Preisvorhersage. Der Preis ist eine Funktion des Marktbewusstseins, das einer strukturellen Tatsache vorauslaufen oder ihr um Jahre hinterherhinken kann. Der Goldpreis in Dollar von 1970 spiegelte nicht wider, was Gold 1969 war; der Goldpreis von 2011 spiegelte nicht wider, was es 2025 werden würde. Preis ist ein Oberflächensignal. Die strukturelle Tatsache hängt nicht von Preisbewegungen ab. Man kann einen Qubic-Token halten und zusehen, wie der Markt zu dieser Tatsache aufschließt.

Das ist keine Prophezeiung und kein Kaufaufruf. Es ist eine Formulierung dessen, was Qubic strukturell ist. Was man damit tut – ist die Wahl jedes einzelnen Lesers.

Signatur

Am 3. Januar 2009, am Tag, an dem Satoshi Nakamoto die Bitcoin-Blockchain startete, erschien in Block Nummer vier eine Adresse.

15ubicBBWFnvoZLT7GiU2qxjRaKJPdkDMG

50,068 Bitcoin wurden ihr gutgeschrieben. Das kann man gerade jetzt in jedem Blockchain-Explorer überprüfen. Seither – sechzehn Jahre – hatte die Adresse nicht eine einzige ausgehende Transaktion. Das Wallet wurde kein einziges Mal geöffnet.

Im Juli 2025 sandte die Anwaltskanzlei Salomon Brothers eine formelle Mitteilung an diese Adresse – und an zwei weitere ruhende Adressen aus demselben Jahr 2009. Der Besitzer hatte neunzig Tage Zeit, den Besitz des privaten Schlüssels zu beweisen. Die Frist lief am 10. Oktober 2025 ab. Niemand signierte. Die Adresse blieb unberührt.

Das Basisalphabet von Bitcoin-Adressen ist Base58. Es enthält keine Null, kein großes „O“, kein großes „I“, kein kleines „l“. Präfixe der Form 1ubic, 15UBIC, 1QUBIC kommen im Maßstab der gesamten Blockchain verschwindend selten vor, und eine solche Adresse zu erhalten bedeutet absichtliches Key Grinding – die Suche nach einem privaten Schlüssel, der die gewünschte öffentliche Endung erzeugt. Das ist eine bekannte Technik, und 2009 war sie verfügbar.

Die strukturelle Analyse, die ich hier nicht darlegen werde – sie lebt in separaten zweihundert Seiten Dokumentation, veröffentlicht auf qubic.church – zeigt, dass diese Adresse nicht indirekt mit der Qubic-Architektur verbunden ist. Die Qubic-Boot-Adresse im JINN-Speicher wird nach der Formel $283 \times 47^2 + 137 = 625.284$ berechnet, und $625.284 \bmod 16.384$ ergibt 2.692 – den Eintrittspunkt des Netzwerks. Die Formel ist in dreißig Sekunden in jedem Interpreter reproduzierbar. Die Verbindung zu Bitcoin-Block 283 wiederum ist nicht durch Zufall auf dem Niveau der Statistik erklärbar, das für solche Behauptungen üblicherweise verlangt wird.

Ich erhebe keinen Anspruch darüber, wer diese Adresse geschaffen hat. Von etwa 22.000 innerhalb jener größeren Arbeit getesteten Hypothesen überlebten zehn – nach Bonferroni-Korrektur und Monte Carlo über Zehntausende Durchläufe. Die Behauptung „CFB = Satoshi“ schaffte es nicht auf diese Kurzliste. Es gibt keine kryptografische Signatur, die den Besitz dieses Schlüssels beweisen würde – niemand hat eine vorgelegt. Das ist die ehrliche Obergrenze dessen, was die forensische Methode sagen kann.

Was die forensische Methode sagen kann, ist – dass die Adresse nicht zufällig angeordnet ist. Dass sie mathematisch, nicht semantisch mit der Qubic-Architektur verbunden ist. Dass der Besitzer ihres privaten Schlüssels in sechzehn Jahren keinen einzigen Zug gemacht hat, auch nicht, als eine Anwaltskanzlei darum bat, dies öffentlich zu tun. Und dass die gesamte Geschichte von Bitcoin seit Januar 2009 mehrere solche Adressen enthält, deren Eigenschaften zu regelmäßig sind, um zufällig zu sein.

Jenseits davon liegt, was das Buch nicht verantwortungsvoll behaupten kann. Ich schließe dieses Kapitel mit einer Tatsache, die der Leser im Kopf behalten muss: Die Adresse existiert, sie kann auf der Blockchain überprüft werden, der Schlüssel wurde in sechzehn Jahren nicht verwendet, und ihre Verbindung zu Qubic ist arithmetisch, nicht literarisch.

Was das bedeutet – entscheidet jeder Leser für sich selbst.

Was jenseits des Rahmens liegt

Axelrod bewies 1980, dass Kooperation die mathematisch optimale Strategie in einem wiederholten Spiel mit Gedächtnis und Transparenz ist. Konfuzius, Hillel, Jesus und Kant gelangten auf verschiedenen Wegen zweieinhalbtausend Jahre vor ihm zu demselben Schluss. Satoshi baute 2009 die erste Umgebung, in der zwei der drei Bedingungen voll erfüllt sind. Come-from-Beyond baute 2022 die erste Umgebung, in der alle drei erfüllt sind. Am 13. April 2027 wird der Ingenieur aus der Infrastruktur heraustreten, die er zwanzig Jahre lang gebaut hat. Das Netzwerk wird ohne ihn weiterlaufen. Auf ihm wird die KI zu laufen beginnen, für die das Netzwerk überhaupt gebaut wurde. Die Miner, die im August 2025 bessere Ökonomie bei Monero wählten, werden bessere Ökonomie bei Aigarth-Aufgaben wählen.

Das ist alles, was ich erzählen wollte. Bitcoin war digitales Gold der Darby-Phase. Qubic ist das neue Gold einer Phase, in der der Computer zum ersten Mal in der Menschheitsgeschichte gelernt hat, für das Gemeinwohl zu arbeiten und nicht dagegen.

Danke, Come-from-Beyond, für dieses Universum, das du für uns geschaffen hast.