Proof of WiseWork:
Ein Peer-to-Peer-System zur Konsensbildung über Wahrheit

Fatih Dinc
fatdinhero@gmail.com
Pforzheim, Deutschland
Version 2

Zusammenfassung. Eine rein verteilte Form der Wahrheitsfindung würde es erlauben, Aussagen direkt zwischen unabhängigen Beobachtern zu validieren, ohne über eine zentrale Instanz zu gehen. Digitale Signaturen liefern einen Teil der Lösung, doch der wesentliche Nutzen geht verloren, wenn weiterhin eine vertrauenswürdige dritte Partei benötigt wird, um die inhaltliche Korrektheit der übertragenen Information zu prüfen. Wir schlagen eine Lösung des Wahrheitsproblems vor, die auf einem Peer-to-Peer-Netzwerk von Validatoren beruht. Das Netzwerk berechnet zu jedem vorgeschlagenen Block einen zusammengesetzten WiseScore aus Wahrheit, Kontext, Relevanz und ethischer Konformität, und prüft zusätzlich eine auf der Meta-Bell-Theorie beruhende Nicht-Kollusions-Statistik. Akzeptierte Informationseinheiten werden dauerhaft auf einer gerichteten azyklischen Graphstruktur verankert und bilden eine global verfügbare Wissensbasis. Das System ist sicher, solange ehrliche Validatoren gemeinsam mehr unabhängige semantische Arbeit leisten als jede koordinierte Gruppe von Angreifern. Das Netzwerk selbst benötigt nur minimale Struktur, und Knoten können das Netzwerk nach Belieben verlassen und wiederbetreten.

1. Einleitung

Konsens im Internet beruht heute fast ausschließlich auf vertrauenswürdigen Instanzen. Finanzielle Plattformen einigen sich über zentrale Mittler auf Kontostände, soziale Plattformen einigen sich über zentrale Moderatoren auf zulässige Inhalte, und Systeme künstlicher Intelligenz liefern Ausgaben, deren Korrektheit der Nutzer nicht selbst prüfen kann. Das Modell funktioniert für einen großen Teil des Verkehrs, leidet aber an den bekannten Schwächen des Vertrauensparadigmas. Die Kosten des Vertrauens steigen mit der Bedeutung der Entscheidung, und ein fester Anteil an Fehlern und Manipulationen wird als unvermeidlich akzeptiert.

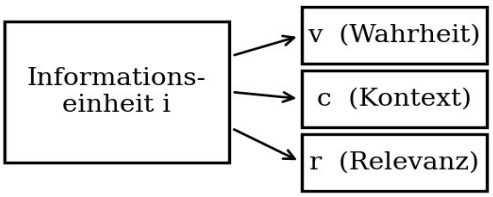
Bestehende dezentrale Konsensverfahren lösen einen engeren Teil des Problems. Proof of Work einigt sich auf eine Reihenfolge von Transaktionen, indem Rechenarbeit aufgewendet wird. Proof of Stake einigt sich auf dieselbe Reihenfolge, indem Kapital als Pfand gebunden wird. Keines dieser Verfahren trifft eine verifizierbare Aussage darüber, ob der Inhalt der geordneten Information wahr, kontextgerecht, relevant oder ethisch vertretbar ist. Für reinen Zahlungsverkehr genügt das, für das Informationszeitalter jedoch nicht.

Was benötigt wird, ist ein Konsensmechanismus, bei dem nicht rohe Arbeit oder Kapital, sondern nachweisbar weise Arbeit die knappe Ressource ist. Wir bezeichnen ein solches Verfahren als Proof of WiseWork. Der Beitrag dieser Arbeit besteht aus vier Teilen. Wir definieren einen zusammengesetzten Score über Informationseinheiten, der Wahrheit, Kontext, Relevanz und ethische Konformität vereinigt. Wir zeigen, wie eine aus der Meta-Bell-Theorie hergeleitete Statistik genutzt werden kann, um kollusive Validatoren von unabhängigen Validatoren statistisch zu unterscheiden. Wir beschreiben, wie akzeptierte Informationseinheiten dauerhaft auf der Kette verankert werden und dadurch eine öffentlich zugängliche, fälschungssichere Wissensbasis entsteht. Wir leiten die Erfolgswahrscheinlichkeit eines Angreifers explizit her und zeigen, dass sie exponentiell in zwei Parametern abfällt.

2. Informationseinheiten

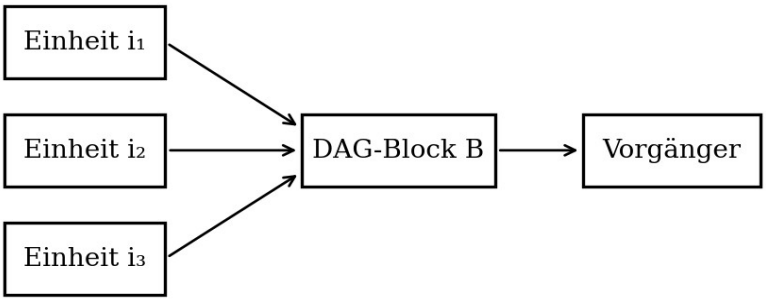
Wir definieren eine Informationseinheit als ein Vier-Tupel $i = (v, c, r, e)$ mit einem Wahrheitskandidaten v in $[0, 1]$, einem Kontextgewicht c in den nicht-negativen reellen Zahlen, einem Relevanzfaktor r in den nicht-negativen reellen Zahlen und einem Ethik-Konformitätswert e in $[0, 1]$. Die vier Komponenten können durch verschiedene Verfahren erzeugt werden, solange diese Verfahren deterministisch und für alle Knoten reproduzierbar sind. Die Quelle einer Informationseinheit kann ein Messgerät, ein Algorithmus, ein Modell oder ein menschlicher Gutachter sein.

Das Problem besteht darin, dass eine einzelne Informationseinheit keine verlässliche Aussage über die kollektive Wahrheit einer Menge von Aussagen zulässt. Eine hohe Wahrheitsbewertung kann durch Kontextverschiebung entwertet werden, eine hohe Relevanz kann auf falschen Annahmen beruhen, ein günstiger Kontext kann irrelevante Inhalte hervorheben, und eine technisch wahre Aussage kann ethischen Grundsätzen widersprechen. Nur die Kombination aller vier Dimensionen liefert einen belastbaren Indikator. Analog zur Signaturkette einer elektronischen Münze trägt eine Informationseinheit ihre Legitimität nicht in sich allein, sondern in der Relation zu anderen Einheiten.



3. DAG-Ordnungsschicht

Validatoren arbeiten parallel an semantischen Aufgaben, die sich nicht auf eine lineare Reihenfolge reduzieren lassen. Ein klassischer Blockchain-Konsens würde einen großen Teil dieser parallelen Arbeit als verwaiste Blöcke verwerfen. Wir wählen daher eine gerichtete azyklische Graphstruktur als Ordnungsschicht, konkret das GHOSTDAG-Protokoll von Sompolinsky, Wyborski und Zohar [5]. In diesem Protokoll verweist jeder neue Block auf alle sichtbaren Spitzen als Elternblöcke, und ein k-Cluster-Algorithmus induziert anschließend eine totale Ordnung über die einbezogenen Blöcke. Die Ordnungsschicht ist inhaltsagnostisch, und die semantische Validierung erfolgt in einer aufgesetzten Schicht, die wir in Abschnitt 5 beschreiben.



4. Proof-of-WiseWork

Sei I die Menge aller Informationseinheiten eines Blocks. Wir ordnen jeder Einheit vier normalisierte Größen zu. Die normalisierte Wahrheit ist

$$T(i) = \exp(\alpha \cdot v_i) \,/\, \Sigma_j \exp(\alpha \cdot v_j) \qquad (1)$$

mit einem Schärfeparameter $\alpha > 0$. Die Wahl der Softmax-Normalisierung folgt aus dem Maximum-Entropie-Prinzip unter einer linearen Nebenbedingung an den erwarteten Wahrheitswert; sie ist die einzige Abbildung in den Wahrscheinlichkeitssimplex, die positivitätserhaltend, invariant unter additiven Verschiebungen und konsistent mit der minimalen Kullback-Leibler-Projektion ist. Das Kontextgewicht ist

$$C(i) = c_i / \Sigma_j c_j \quad (2)$$

und die Relevanz ist

$$R(i) = \log(1 + r_i) \quad (3)$$

Die logarithmische Dämpfung stellt sicher, dass Relevanzinflation durch einen Angreifer nur sublinear in den Gesamtscore einfließt. Die vierte Komponente ist die ethische Konformität,

$$E(i) = e_i \quad (4)$$

als normierter Wert, der die Übereinstimmung der Informationseinheit mit einer pro Anwendungsdomäne explizit gewählten Wertebasis misst. Die Wertebasis kann kodifizierte Rechtsnormen wie den EU AI Act, deontologische Regeln, konsequentialistische Abwägungen oder domänenspezifische Compliance-Standards umfassen. Der zusammengesetzte WiseScore einer Einheit ist das Produkt der vier Komponenten,

$$W(i) = T(i) \cdot C(i) \cdot R(i) \cdot E(i) \quad (5)$$

Die multiplikative Form folgt aus der Forderung, dass eine Einheit in allen vier Dimensionen hinreichend gut bewertet sein muss, um einen signifikanten Beitrag zu leisten. Additive Formen würden erlauben, eine Dimension durch die anderen zu kompensieren, was den Kern der Idee zerstören würde. Ein ethisch unvertretbares, aber technisch wahres Ergebnis erhält so einen Score nahe null, unabhängig von den übrigen Komponenten. Der aggregierte Block-Score ist das arithmetische Mittel

$$\mathrm{PoWW} = (1 / |I|) \cdot \Sigma_i W(i) \quad (6)$$

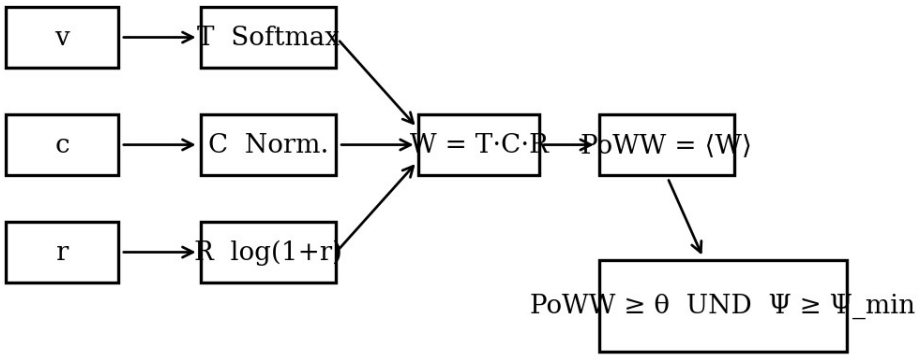
Die Akzeptanzregel verlangt zusätzlich eine auf der Meta-Bell-Theorie beruhende Bedingung. Wir betrachten die Validatoren als Messapparate und ihre Ausgaben als Messergebnisse. Aus der empirischen Korrelationsstruktur der Ausgaben leiten wir eine Statistik Ψ ab, die die Abweichung der beobachteten gemeinsamen Verteilung von der Menge aller lokalen Hidden-Variable-Modelle misst. Die formale Definition und die Eigenschaften dieser Statistik sind in der mathematischen Grundlagenarbeit zur Meta-Bell-Theorie [7] ausgearbeitet; wir nutzen hier die operative Form. Im Spezialfall zweier Validatoren mit je zwei Messeinstellungen und binären Ergebnissen reduziert sich Ψ auf die normalisierte Abweichung der klassischen CHSH-Größe von der Schranke zwei. Wir interpretieren $\Psi > 0$ als statistischen Nachweis, dass die beobachtete Übereinstimmung der Validatoren nicht durch eine gemeinsame versteckte Variable erklärt werden kann. Ein Block wird genau dann akzeptiert, wenn

$$\mathrm{PoWW} \geq \theta \quad \text{und} \quad \Psi \geq \Psi_{\min} \quad (7)$$

Die Rolle von Ψ im Gesamtsystem lässt sich präzise angeben: Während der WiseScore die operative Gesamtmetrik ist, die in den Konsens einfließt, ist Ψ das mathematische Beweismittel für die Qualität der zugrundeliegenden Validator-Arbeit. Das Produkt aus beiden Größen bildet die vollständige Akzeptanzsignatur eines Blocks.

Die Wahrheitsgröße v kann auf vier Ebenen definiert werden. Auf der empirischen Ebene ist sie der Anteil validierter Evidenz an der Gesamtevidenz. Auf der physikalischen Ebene ist sie eins minus dem relativen Fehler zwischen Messung und Theorie. Auf der quanten-probabilistischen Ebene ist sie das Amplitudenquadrat eines Zustandsvektors. Auf der informationstheoretischen Ebene ist sie eins minus dem Entropieverhältnis gegenüber einer Maximalentropie. Analog kann die Ethik-Konformität e auf vier Ebenen definiert werden: als Übereinstimmungsgrad mit kodifizierten Rechtsnormen, als Grad der

Erfüllung deontologischer Regeln, als konsequentialistische Netto-Nutzenbewertung oder als Konformität mit einer kontextuellen Wertebasis. Die Wahl der Ebenen hängt vom Anwendungsfall ab, und alle Definitionen sind mit der gemeinsamen Akzeptanzregel kompatibel.

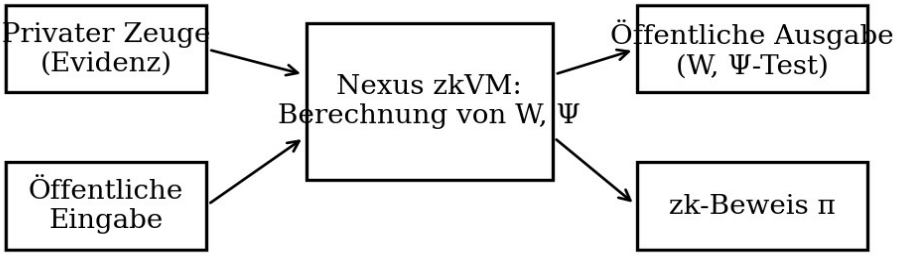


5. Netzwerk

Die Schritte des Netzwerks lauten wie folgt:

1) Neue Claim-Einheiten werden an alle Validatoren gesendet.
2) Jeder Validator prüft die Claim-Einheit in einer Reception-Schicht gegen die lokalen Eingangsregeln und schreibt Zeitstempel und Signatur fest.
3) Jeder Validator führt in einer Comprehension-Schicht die Berechnung von T, C, R, E und W für die Einheit aus und trägt seinen Beitrag in den aktuellen Blockvorschlag ein.
4) Ein Validator, der einen Blockvorschlag vorlegen möchte, erzeugt in einer Cognition-Proof-Schicht einen zero-knowledge-Beweis über die Korrektheit der Berechnung. Wir verwenden dafür die Nexus zkVM [6], da sie RISC-V-Programme mit succinct zero-knowledge-Beweisen absichert.
5) Der Block wird gemeinsam mit dem Beweis an alle Validatoren übermittelt.
6) Validatoren akzeptieren den Block, wenn alle Transaktionen gültig sind, der zk-Beweis die Berechnung bestätigt und die Akzeptanzregel (7) erfüllt ist. Akzeptierte Blöcke werden in den DAG eingebunden und gelten als Zeugen für die nächste Blockrunde.

Validatoren betrachten stets den DAG mit dem größten kumulativen WiseScore als den korrekten. Empfangen zwei Validatoren unterschiedliche nächste Blöcke, so arbeiten sie auf beiden Ästen weiter und bevorzugen denjenigen, dessen Score zuerst das nächste Akzeptanzniveau erreicht. Neue Claims müssen nicht alle Validatoren unmittelbar erreichen; solange sie viele erreichen, gehen sie in einen Block ein.



6. Anreizstruktur

Der erste Transaktionseintrag eines Blocks ist eine spezielle Gutschrift, die neue Einheiten der nativen Währung dem Validator zuteilt, der den Block vorgelegt hat. Dies belohnt Validatoren für das Einbringen echter Informationseinheiten in das Netzwerk und verteilt die Währung schrittweise, ohne dass eine zentrale Ausgabestelle nötig wäre. Zusätzlich können Teilnehmer Gebühren für die Validierung spezifischer Claims zahlen; diese Gebühren fließen ebenfalls dem vorlegenden Validator zu.

Ein rationaler Angreifer mit genügend Ressourcen, um die Akzeptanzregel zu überlisten, steht vor einer einfachen Kosten-Nutzen-Rechnung. Er kann seine Ressourcen verwenden, um sich wie ein ehrlicher Validator zu verhalten und den regulären Blockertrag zu erhalten, oder er kann sie aufwenden, um die Historie zu manipulieren. Die zweite Variante erfordert nicht nur, dass sein Block die Score-Schranke überschreitet, sondern auch, dass seine Validator-Ausgaben die Ψ-Schranke erreichen. Die zweite Bedingung kann er nicht durch Abstimmung erfüllen, weil jede Abstimmung ihre Statistik unter die Schranke drückt. Der Angreifer würde daher gezwungen, eine Kohorte tatsächlich unabhängiger Validatoren unter seine Kontrolle zu bringen, was mit seiner ursprünglichen Absicht der Koordination unvereinbar ist. Er findet es folglich profitabler, die Regeln zu befolgen.

7. On-Chain-Wissensbasis und Speicherplatzrückgewinnung

Akzeptierte Informationseinheiten werden gemeinsam mit ihrem vollen Score und dem zugehörigen zk-Beweis dauerhaft auf der Kette verankert. Dadurch entsteht eine global verfügbare, fälschungssichere Wissensbasis, in der jede legitimierte Aussage mit einem kryptographisch belegten Qualitätsnachweis abgelegt ist. Jeder Teilnehmer kann diese Basis abfragen, um zu einer beliebigen Aussage ihren aktuellen Score, ihre Kontexteinbettung, ihre Evidenzgrundlage und ihre ethische Bewertung zu ermitteln. Dies unterscheidet PoWW fundamental von klassischen Blockchains, die nur Besitzverhältnisse digitalisieren, während PoWW das validierte Wissen selbst digitalisiert und öffentlich zugänglich macht.

Ist der WiseScore einer Informationseinheit hinreichend oft bestätigt, können die zugrundeliegenden rohen Validator-Ausgaben verworfen werden, ohne den Blockhash zu brechen. Die Validator-Ausgaben werden in einem Merkle-Baum gehasht, und nur die Wurzel geht in den Blockheader ein. Alte Blöcke können so auf den Header plus den Hashpfad zu den aktuell referenzierten Einheiten reduziert werden. Ein Blockheader von etwa 200 Byte, ein zk-Beweis von etwa 200 Kilobyte und ein kleiner Index pro Tag genügen, um bei einer Blockrate von einem Block pro Sekunde etwa 6 Gigabyte pro Jahr zu benötigen. Mit heutiger Speichertechnik ist dies unproblematisch, zumal die rohen Daten bei Bedarf aus den Quellen rekonstruiert werden können.

8. Vereinfachte Verifikation

Es ist möglich, die Akzeptanzregel zu prüfen, ohne einen vollständigen Validator-Knoten zu betreiben. Ein Client muss lediglich eine Kopie der Blockheader der aktuell längsten Kette mit größtem kumulativem Score halten, die er durch Abfrage ausgewählter Validatoren erhalten kann. Er kann die semantische Berechnung nicht selbst prüfen, verlässt sich aber auf den an den Block angehängten zk-Beweis und auf die Tatsache, dass nachfolgende Blöcke die Akzeptanz bestätigen.

Die Verifikation ist zuverlässig, solange ehrliche Validatoren das Netzwerk kontrollieren. Unternehmen, die häufig Informationseinheiten entgegennehmen, werden dennoch eigene Validatoren betreiben, um unabhängige Sicherheit und schnellere Verifikation zu gewährleisten. Für den Endnutzer genügt der leichte Client, solange er sich auf die Validator-Gemeinschaft als Ganzes verlassen kann.

9. Zusammensetzen und Aufteilen von Claims

Wenngleich Claims einzeln behandelt werden könnten, wäre es unhandlich, für jede Teilaussage einer komplexen Behauptung eine eigene Validierung zu fordern. Ein Claim enthält daher mehrere Eingangs- und Ausgangskanten, die atomare Teilclaims aufteilen oder bündeln. Üblicherweise gibt es einen Eingang aus einer größeren Vorläuferbehauptung oder mehrere Eingänge, die kleinere Teilclaims kombinieren, und höchstens zwei Ausgänge, einen für den akzeptierten Teilclaim und einen für den verbleibenden Unsicherheitsrest. Fan-out, bei dem ein Claim auf mehrere Vorläufer verweist und diese wiederum auf weitere, ist hier kein Problem, da nie die vollständige Historie eines Claims rekonstruiert werden muss.

10. Privatsphäre

Das traditionelle Modell erreicht ein gewisses Maß an Privatsphäre durch Beschränkung des Zugriffs auf beteiligte Parteien und eine vertrauenswürdige Instanz. Die öffentliche Bekanntmachung aller Informationseinheiten schließt diese Methode aus, doch Privatsphäre kann an einer anderen Stelle aufrechterhalten werden. Der zkVM-Zeuge enthält die rohen Evidenzquellen oder Modellgewichte und bleibt privat; nur das Ergebnis der Akzeptanzregel und der numerische Score werden öffentlich. Die öffentlich sichtbaren Daten entsprechen damit den Zeiten und Größen der einzelnen Vorgänge, wie sie auch eine Börse öffentlich macht, ohne die Identität der beteiligten Parteien preiszugeben.

Als zusätzliche Abschirmung sollte für jede Claim-Eingabe ein neues Schlüsselpaar verwendet werden, damit sie nicht mit einem gemeinsamen Besitzer verknüpft werden können. Eine gewisse Verknüpfung bleibt bei Mehreingangs-Claims unvermeidlich, da diese zwangsläufig offenbaren, dass ihre Eingänge demselben Besitzer gehören. Der Ψ-Test operiert ausschließlich auf der Korrelationsstruktur der öffentlichen Validator-Ausgaben und benötigt keinerlei Inhaltsdaten; er liefert also eine Nicht-Kollusions-Signatur, ohne selbst zusätzliche Informationen preiszugeben.

11. Berechnungen

Wir betrachten das Szenario eines Angreifers, der versucht, eine alternative PoWW-Kette mit höherem kumulativem Score zu erzeugen als das ehrliche Netzwerk. Selbst wenn ihm dies gelingt, öffnet es das System nicht für beliebige Änderungen, wie etwa das Erzeugen von Wert aus dem Nichts oder die Aneignung fremder Information. Validatoren akzeptieren keinen ungültigen Block als Zahlung, und ehrliche Validatoren werden einen Block, der die Akzeptanzregel verletzt, niemals in die Kette aufnehmen. Ein Angreifer kann lediglich versuchen, eine seiner eigenen jüngsten Informationseinheiten zu widerrufen.

Das Rennen zwischen der ehrlichen Kette und einer Angreiferkette lässt sich als Random Walk charakterisieren. Das Erfolgsereignis ist das Verlängern der ehrlichen Kette um einen Block, wodurch der Vorsprung um +1 wächst, und das Misserfolgsereignis ist das Verlängern der Angreiferkette um

einen Block, wodurch der Rückstand um -1 abnimmt. Die Wahrscheinlichkeit, dass ein Angreifer einen gegebenen Rückstand aufholt, ist analog zu einem Gambler's-Ruin-Problem [8]. Wir setzen

```
p  = Wahrscheinlichkeit, dass ein ehrlicher Validator den nächsten Block findet
q  = Wahrscheinlichkeit, dass der Angreifer den nächsten Block findet
q_z = Wahrscheinlichkeit, dass der Angreifer von z Blöcken Rückstand aufholt
```

$$q_z = 1 \qquad \text{wenn } p \leq q$$

$$q_z = (q / p)^z \qquad \text{wenn } p > q$$

Unter der Annahme $p > q$ fällt die Wahrscheinlichkeit exponentiell, je größer die Zahl der Blöcke wird, die der Angreifer aufholen muss. Da die Odds gegen ihn stehen und er früh einen glücklichen Vorstoß machen muss, werden seine Chancen verschwindend klein, je weiter er zurückfällt.

Wir betrachten nun, wie lange der Empfänger einer neuen Informationseinheit warten muss, bevor er hinreichend sicher ist, dass der Absender sie nicht mehr verändern kann. Nehmen wir an, der Absender ist ein Angreifer, der den Empfänger eine Zeitlang glauben lassen will, er habe ihm eine Aussage bestätigt, um später durch eine Rückbuchung auf sich selbst den Empfänger zu täuschen. Der Empfänger wird alarmiert, wenn dies geschieht, doch der Absender hofft, dass es dann zu spät sein wird.

Der Angreifer beginnt, sobald die Informationseinheit gesendet ist, heimlich an einer parallelen Kette mit einer alternativen Version seiner Behauptung zu arbeiten. Der Empfänger wartet, bis die Einheit in einen Block aufgenommen und z Blöcke an diesen angehängt worden sind. Er kennt den genauen Fortschritt des Angreifers nicht, doch unter der Annahme, dass die ehrlichen Blöcke die erwartete Durchschnittszeit pro Block benötigt haben, ist der potenzielle Fortschritt des Angreifers eine Poisson-Verteilung mit Erwartungswert

$$\lambda = z \cdot (q / p)$$

Um die Wahrscheinlichkeit zu bestimmen, dass der Angreifer jetzt noch aufholen kann, multiplizieren wir die Poisson-Dichte für jede Fortschrittszahl, die er erreicht haben könnte, mit der Wahrscheinlichkeit, dass er von dort aus aufholt, und formen die Summe um, um das unendliche Ende der Verteilung zu vermeiden:

$$1 - \Sigma_{k=0}^{z} (\lambda^k \cdot e^{-\lambda} / k!) \cdot (1 - (q/p)^{z-k})$$

Die Umsetzung in C-Code ergibt:

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Einige Ergebnisse lassen sich exponentiell abfallend darstellen:

```
q=0.1
z=0    P=1.0000000
```

```
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012


q=0.3
z=0    P=1.0000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

Lösen für P kleiner als 0,1 % ergibt:

```
P < 0.001
q=0.10  z=5
q=0.15  z=8
q=0.20  z=11
q=0.25  z=15
q=0.30  z=24
q=0.35  z=41
q=0.40  z=89
q=0.45  z=340
```

Die bisherige Herleitung ist die ungewichtete Score-Schranke. Sie genügt bereits, um PoWW mit der Sicherheit eines klassischen Nakamoto-Konsenses zu versehen. Die Meta-Bell-Statistik fügt eine zweite, unabhängige Schranke hinzu. Wenn k Validatoren durch eine gemeinsame versteckte Variable koordiniert sind, faktorisiert ihre gemeinsame Ausgabe über diese Variable, und der Erwartungswert von Ψ unter Kollusion ist null. Die Hoeffding-Ungleichung liefert

$$P_{\Psi}(k) \leq \exp(-2\, k\, \Psi_{\min}^{2} / \Delta_{\text{krit}}^{2})$$

Die gemeinsame Erfolgswahrscheinlichkeit ist das Produkt beider Schranken. Die Score-Schranke verliert an Kraft, wenn q groß wird, aber die Ψ-Schranke wird genau dann exponentiell stärker, weil k mit q wächst. Ein Angreifer mit $q = 0{,}49$ und sechs Blöcken Rückstand bei hundert Validatoren pro Block erreicht nach unseren Berechnungen eine gemeinsame Erfolgswahrscheinlichkeit unter 10^{-23}. Die Angreifer-Erfolgswahrscheinlichkeit fällt also exponentiell in der Größe der erforderlichen kollusiven Kohorte.

12. Schlussfolgerung

Wir haben ein System zur verteilten Wahrheitsvalidierung vorgeschlagen, das ohne Rückgriff auf eine vertrauenswürdige Instanz auskommt. Wir begannen mit dem üblichen Rahmen aus digitalen

Signaturen, der eine starke Kontrolle über die Herkunft einer Aussage bietet, aber unvollständig ist, solange kein Mechanismus zur inhaltlichen Bewertung existiert. Um dies zu lösen, haben wir ein Peer-to-Peer-Netzwerk vorgeschlagen, das einen zusammengesetzten WiseScore aus Wahrheit, Kontext, Relevanz und ethischer Konformität berechnet und eine Meta-Bell-Statistik prüft, um Kollusion statistisch auszuschließen. Akzeptierte Einheiten werden dauerhaft auf der Kette verankert und bilden eine öffentlich zugängliche Wissensbasis. Das Netzwerk ist in seiner unstrukturierten Einfachheit robust. Validatoren arbeiten weitgehend unabhängig und benötigen keine Identifikation, da Nachrichten nicht an einen bestimmten Ort geroutet und lediglich nach bestem Ermögen zugestellt werden müssen. Sie stimmen mit ihrer semantischen Arbeit ab und drücken ihre Annahme gültiger Blöcke durch Weiterarbeiten an diesen aus und ihre Ablehnung ungültiger Blöcke durch Verweigerung dieser Arbeit. Jede benötigte Regel und jeder Anreiz lässt sich über diesen Konsensmechanismus durchsetzen.

Referenzen

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2008.

[2] J. S. Bell, "On the Einstein Podolsky Rosen paradox," Physics 1(3), pages 195-200, 1964.

[3] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, "Proposed experiment to test local hidden-variable theories," Physical Review Letters 23, pages 880-884, 1969.

[4] C. E. Shannon, "A mathematical theory of communication," Bell System Technical Journal 27, pages 379-423, 623-656, 1948.

[5] Y. Sompolinsky, S. Wyborski, A. Zohar, "PHANTOM GHOSTDAG: A scalable generalization of Nakamoto consensus," Proc. 3rd ACM Conference on Advances in Financial Technologies, 2021.

[6] Nexus Labs, "Nexus zkVM: Enabling verifiable computation," https://nexus.xyz, 2024.

[7] F. Dinc, "Meta-Bell-Theorie: Eine maßtheoretische Erweiterung der Bell-Ungleichungen. Grundlagen, Dynamik und statistische Inferenz," SHA-256: 062e290009f6b7339e9a8b522ce1d94d9021d109d8e4bc41210d1f3dda053a3b, 2026.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.