PoISV: Ein Peer-to-Peer-System zur unabhängigen semantischen Validierung

Fatih Dinc
fatdinhero@gmail.com
Pforzheim, Deutschland

Version 1.0 – April 2026
DOI: 10.5281/zenodo.19642292
OTS: poisv.com/verification

Abstract

Ein rein dezentrales System zur Bewertung der Qualität digitaler Aussagen würde es erlauben, Informationen direkt zwischen unabhängigen Beobachtern zu validieren, ohne auf eine zentrale Instanz angewiesen zu sein. Bestehende Konsensmechanismen wie Proof-of-Work oder Proof-of-Stake ordnen Transaktionen, treffen jedoch keine Aussage darüber, ob der Inhalt der geordneten Informationen semantisch konsistent oder unabhängig validiert wurde. Wir schlagen eine Lösung vor, die auf einem Netzwerk von Validatoren basiert und für jede Aussage einen zusammengesetzten Score berechnet – die semantische Konsistenz mit einem öffentlichen Wissenskorpus – sowie einen statistischen Nicht-Kollusions-Test durchführt, der auf der Korrelation der Validierungsfehler bei Kontrollaufgaben basiert. Akzeptierte Aussagen werden dauerhaft in einem gerichteten azyklischen Graphen verankert und bilden eine global verfügbare, fälschungssichere Wissensbasis. Das System ist sicher, solange ehrliche Validatoren gemeinsam mehr unabhängige semantische Arbeit leisten als jede koordinierte Angreifergruppe. Das mathematische Fundament des Nicht-Kollusions-Tests beruht auf der Meta-Bell-Theorie [6], einer maßtheoretischen Erweiterung der Bell'schen Ungleichungen.

1 Einleitung

Vertrauen im Internet beruht heute fast ausschließlich auf zentralen Vermittlern. Finanzplattformen einigen sich über zentrale Bücher auf Kontostände, soziale Plattformen über zentrale Moderatoren auf zulässige Inhalte, und Systeme künstlicher Intelligenz liefern Ausgaben, deren Korrektheit Nutzer nicht eigenständig prüfen können. Das Modell funktioniert für den Großteil des alltäglichen Datenverkehrs, leidet aber an den bekannten Schwächen des Vertrauensparadigmas: Die Kosten steigen mit der Bedeutung der Entscheidung, und eine Grundrate an Fehlern und Manipulation wird als unvermeidlich akzeptiert.

Bitcoin führte eine Möglichkeit ein, ohne eine zentrale Partei Konsens über die Reihenfolge von Transaktionen herzustellen, indem Rechenarbeit aufgewendet werden muss [1]. Proof-of-Stake erreicht eine ähnliche Ordnung, indem Kapital als Pfand gebunden wird. Keiner dieser Mechanismen trifft jedoch eine überprüfbare Aussage darüber, ob der Inhalt der geordneten Informationen semantisch konsistent oder unabhängig bewertet ist. Für reine Zahlungssysteme genügt das; für das Informationszeitalter jedoch nicht.

Was benötigt wird, ist ein Konsensmechanismus, bei dem die knappe Ressource nicht rohe Rechenleistung oder Kapital ist, sondern *nachweislich unabhängige semantische Arbeit*. Ein solches

System bezeichnen wir als **Proof of Independent Semantic Validation (PoISV)**. Diese Arbeit ist die dritte in einer Reihe: Die Meta-Bell-Theorie [6] bildet das mathematische Fundament, Proof of WiseWork [7] ist die erste Anwendung, und PoISV ist das vollendete, operativ präzise Protokoll.

2 Das Problem des semantischen Konsenses

Ein Netzwerk, in dem Teilnehmer *Claims* einreichen – Aussagen über die Welt –, soll jedem Claim einen Qualitätsscore beifügen, der seine Übereinstimmung mit einem objektiven, öffentlich überprüfbaren Wissenskorpus und die Unabhängigkeit der ihn beurteilenden Validatoren widerspiegelt.

Ein einzelner von einem einzelnen Validator bewerteter Claim ist unzuverlässig. Der Validator kann voreingenommen sein, eine veraltete Wissensbasis nutzen oder Teil einer koordinierten Gruppe sein, die eine falsche Aussage durchsetzen möchte. Selbst viele Validatoren könnten alle dasselbe fehlerhafte Modell oder dieselben manipulierten Daten verwenden. Es braucht daher einen Mechanismus, der mathematisch beweisbar macht, dass die Validatoren *wirklich unabhängig* arbeiten.

3 Das PoISV-Protokoll

3.1 Informationseinheiten

Wir definieren einen Claim als $A = (d, \sigma)$, wobei d die serialisierten Aussagedaten und σ eine optionale digitale Signatur des Einreichers sind. Der Wissenskorpus $\mathcal{K}$ ist ein versionierter Datensatz, der via Inhalts-Hashing (z. B. IPFS) adressierbar ist. Sein Hash $H(\mathcal{K})$ ist im Genesisblock verankert.

3.2 Der Semantische Konsistenz-Score

Die Funktion $S_{con}(A) \in [0, 1]$ wird deterministisch berechnet: Entitäten und Relationen werden aus A extrahiert, $\mathcal{K}$ wird nach stützenden oder widersprechenden Fakten durchsucht, und ein gewichteter Übereinstimmungswert wird zurückgegeben. Die genaue Implementierung ist durch die Protokollversion festgelegt; ihr Hash ist im Blockheader enthalten, was vollständige Reproduzierbarkeit gewährleistet.

3.3 Die Nicht-Kollusions-Statistik Ψ

Die Meta-Bell-Theorie [6] liefert die formale Grundlage zur Unterscheidung von wirklich unabhängigen Messungen und koordinierten. Jeder Validator i muss k kanonische Kontroll-Claims $D_1, \ldots, D_k$ lösen, deren korrekte Scores $S^*(D_j)$ im Protokoll festgelegt sind. Dies erzeugt den Fehlervektor

$$\mathbf{e}_i = \big(|S_i(D_j) - S^*(D_j)|\big)_{j=1}^{k}.$$

Für N Validatoren, die zu einem Block beitragen, berechnen wir die mittlere absolute paarweise Pearson-Korrelation:

$$\Psi = 1 - \frac{2}{N(N-1)} \sum_{1 \le i < j \le N} |\rho(\mathbf{e}_i, \mathbf{e}_j)|.$$

Unabhängige Validatoren erzeugen unkorrelierte Fehlermuster und ergeben $\Psi \approx 1$. Kolludierende Validatoren, die dasselbe Modell oder dieselben Daten teilen, erzeugen identische Fehlermuster und ergeben $\Psi \approx 0$.

Diese Statistik ist die operative Realisierung des Meta-Bell-Verschränkungsmaßes $\Psi(X, Y)$ aus [6]: Ein positiver Wert beweist, dass die beobachteten Korrelationen durch kein lokales Hidden-Variable-Modell erklärt werden können, d. h. durch keine Form gemeinsamer Koordination.

3.4 Akzeptanzregel

Ein Block wird genau dann akzeptiert, wenn

$$\frac{1}{|A|} \sum_{A \in \text{Block}} S_{con}(A) \;\geq\; \theta_{min} \quad \text{und} \quad \Psi \;\geq\; \Psi_{min}.$$

3.5 Blockgewicht und DAG-Ordnung

PoISV nutzt das GHOSTDAG-Protokoll [5], um parallele Blockproduktion ohne Verlust ehrlicher Arbeit zu ermöglichen. Das Gewicht eines Blocks ist

$$\text{Gewicht}(B) = \Psi_B \cdot \sum_{A \in B} S_{con}(A).$$

Die kanonische Kette ist der Pfad durch den DAG mit dem höchsten kumulierten Gewicht.

4 Netzwerkbetrieb

Die Schritte des Netzwerks lauten wie folgt.

1. Neue Claims werden an alle Validatoren gesendet.
2. Jeder Validator berechnet S_{con} für den Claim und erfasst seinen Fehlervektor auf dem Kontrollaufgaben-Set.
3. Ein Validator, der einen Block vorschlagen möchte, sammelt Claims, berechnet aggregierte Scores und erstellt einen Block.
4. Der Block wird zusammen mit einem Zero-Knowledge-Beweis korrekter Berechnung übermittelt, erzeugt durch eine zkVM [4].
5. Andere Validatoren akzeptieren den Block, wenn die Scores die Schwellenwerte erfüllen und der Beweis verifiziert.
6. Akzeptierte Blöcke werden dem DAG hinzugefügt und verankern jeden validierten Claim dauerhaft auf der Kette.

Validatoren betrachten stets den DAG-Pfad mit dem höchsten kumulierten Gewicht als kanonisch. Neue Claims müssen nicht alle Validatoren sofort erreichen; solange sie viele erreichen, gehen sie in einen Block ein.

5 Sicherheitsanalyse

Wir betrachten einen Angreifer, der einen Anteil $q < 0{,}5$ der Validatoren kontrolliert.

5.1 Angriff auf die semantische Konsistenz

Um $S_{con}(A)$ für eine falsche Aussage über θ_{min} zu heben, muss der Angreifer entweder den Hash von $\mathcal{K}$ fälschen – kryptographisch nicht durchführbar – oder eine Mehrheit der Validatoren dazu bringen, falsche Pfade in $\mathcal{K}$ zu akzeptieren. Da $\mathcal{K}$ öffentlich ist, kann jeder ehrliche Validator einen Betrugsnachweis erzeugen, der den Block ungültig macht.

5.2 Angriff auf Ψ

Mithilfe der Hoeffding-Ungleichung für U-Statistiken gilt für die Wahrscheinlichkeit, dass ein Angreifer mit dem Anteil q kollusionierende Validatoren $\Psi \geq \Psi_{min}$ fälschen kann:

$$P(\text{Erfolg}) \;\leq\; \exp\!\left(-2k \cdot \frac{(1-q)^2}{q^2} \cdot \left(\Psi_{min} - (1-q^2)\right)^2\right).$$

Einige Ergebnisse zeigen den exponentiellen Abfall:

q	k	Ψ_{min}	P(Erfolg)
0,10	32	0,7	$< 10^{-12}$
0,20	32	0,7	$< 10^{-8}$
0,30	64	0,7	$< 10^{-7}$
0,40	64	0,7	$< 10^{-4}$
0,49	128	0,7	$< 10^{-3}$

5.3 Anreizkompatibilität

Validatoren werden für das Vorschlagen gültiger Blöcke mit neu geprägter Nativwährung und Transaktionsgebühren belohnt. Manipulation erfordert nicht nur die Kontrolle eines signifikanten Anteils an Validatoren, sondern auch, dass diese unabhängig erscheinen – was den Angreifer zwingt, tatsächlich diverse, unabhängige Validierungspipelines zu betreiben, was den Zweck der Koordination unterläuft. Rationale Akteure finden es daher profitabler, die Regeln zu befolgen.

6 Privatsphäre und leichte Clients

Die rohen Evidenzquellen und Modellgewichte der Validatoren verbleiben als privater Zeuge in der zkVM; nur finale Scores und die Ψ-Statistik werden veröffentlicht. Leichte Clients können die Blockakzeptanz prüfen, indem sie nur Blockheader und Zero-Knowledge-Beweise herunterladen, ohne die semantische Engine selbst zu betreiben. Leichte Clients können zudem subjektive Filter anwenden, ohne diese dem Netzwerk aufzuzwingen. Das Protokoll selbst bleibt wertneutral.

7 Speicherplatzrückgewinnung

Ältere Validator-Ausgaben können gelöscht werden, ohne Block-Hashes zu brechen. Validator-Ausgaben werden in einem Merkle-Baum gehasht; nur die Wurzel ist im Blockheader gespeichert. Bei einem Block pro Sekunde entspricht dies etwa 6 Gigabyte pro Jahr – problemlos für moderne Speichermedien.

8 Schlussfolgerung

Wir haben ein System zur dezentralen semantischen Validierung vorgeschlagen, das ohne eine vertrauenswürdige dritte Partei auskommt. Ausgehend von digitalen Signaturen und einem öffentlichen Wissenskorpus haben wir ein Peer-to-Peer-Netzwerk aufgebaut, das einen semantischen Konsistenz-Score berechnet und einen auf der Meta-Bell-Theorie beruhenden Nicht-Kollusions-Test durchführt. Akzeptierte Claims werden dauerhaft in einem DAG verankert und bilden eine öffentliche, fälschungssichere Wissensbasis. Das Netzwerk ist in seiner unstrukturierten Einfachheit robust. Jede benötigte Regel und jeder Anreiz lassen sich über diesen Konsensmechanismus durchsetzen.

References

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.

[2] J. S. Bell, *On the Einstein Podolsky Rosen Paradox*, Physics 1(3):195–200, 1964.

[3] J. F. Clauser et al., *Proposed Experiment to Test Local Hidden-Variable Theories*, PRL 23:880–884, 1969.

[4] Nexus Labs, *Nexus zkVM: Enabling Verifiable Computation*, 2024.

[5] Y. Sompolinsky et al., *PHANTOM GHOSTDAG*, AFT 2021.

[6] F. Dinc, *Meta-Bell-Theorie: Eine maßtheoretische Erweiterung der Bell-Ungleichungen*, v1.0, SHA-256: 062e290009f6b7339e9a8b522ce1d94d9021d109d8e4bc41210d1f3dda053a3b, 2026.

[7] F. Dinc, *Proof of Wise Work: Ein Peer-to-Peer-System zur Konsensbildung über Wahrheit*, v2.0, SHA-256: e57cae993701a1933a3317e28c7bb7141a01b51b31674adee97b6cf89472c2eb, 2026.

[8] C. E. Shannon, *A Mathematical Theory of Communication*, BSTJ 27:379–423, 1948.