PoISV: Bağımsız Anlam Doğrulama için Eşler Arası Bir Sistem

Fatih Dinc
fatdinhero@gmail.com
Pforzheim, Almanya

Sürüm 1.0 – Nisan 2026
DOI: 10.5281/zenodo.19642292
OTS: poisv.com/verification

Özet

Dijital ifadelerin kalitesini değerlendirmek için tamamen merkezi olmayan bir sistem, bilginin merkezi bir otoriteye bağlı kalmaksızın bağımsız gözlemciler arasında doğrudan doğrulanmasına olanak tanıyacaktır. Proof-of-Work veya Proof-of-Stake gibi mevcut konsensüs mekanizmaları işlemleri sıralar, ancak sıralanan bilginin içeriğinin anlam tutarlılığı taşıyıp taşımadığını ya da bağımsız biçimde doğrulanıp doğrulanmadığını denetlemez. Her ifade için, kamuya açık bir bilgi külliyatıyla anlam tutarlılığını ölçen bileşik bir puan hesaplayan ve doğrulayıcıların hata örüntülerindeki korelasyona dayanan istatistiksel bir çakışma-dışı test uygulayan bir doğrulayıcı ağına dayalı bir çözüm öneriyoruz. Kabul edilen ifadeler, küresel ölçekte erişilebilir ve değiştirilemez bir bilgi tabanı oluşturarak yönlendirilmiş bir asiklik grafta kalıcı biçimde çapalanır. Dürüst doğrulayıcılar, koordineli herhangi bir saldırgan grubundan daha fazla bağımsız anlam çalışması yaptığı sürece sistem güvenlidir. Çakışma-dışı testin matematiksel temeli, Bell eşitsizliklerinin ölçüm-teorik bir uzantısı olan Meta-Bell Teorisi'ne [6] dayanmaktadır.

1 Giriş

İnternetteki güven bugün neredeyse tamamen merkezi aracılara dayanmaktadır. Mali platformlar hesap bakiyelerini merkezi defterler aracılığıyla, sosyal platformlar içerik kararlarını merkezi denetçiler aracılığıyla belirler; yapay zeka sistemleri ise kullanıcıların doğruluğunu bağımsız olarak doğrulayamadığı çıktılar üretmektedir.

Bitcoin, merkezi bir taraf olmaksızın işlem sıralamasında konsensüse ulaşmanın bir yolunu, hesaplama çalışması gerektirerek tanıttı [1]. Proof-of-Stake ise sermayeyi teminat olarak kilitleyerek benzer bir sıralama sağlar. Ancak bu mekanizmaların hiçbiri, sıralanan bilginin içeriğinin anlam bakımından tutarlı ya da bağımsız olarak değerlendirilip değerlendirilmediğine dair doğrulanabilir bir iddiada bulunmaz. Saf ödemeler için bu yeterlidir; bilgi çağı için ise değildir.

Gerekli olan şey, kıt kaynağın ham hesaplama gücü ya da sermaye değil, *kanıtlanabilir biçimde bağımsız anlam çalışması* olduğu bir konsensüs mekanizmasıdır. Bu tür bir sisteme **Bağımsız Anlam Doğrulama Kanıtı (PoISV)** adını veriyoruz. Bu çalışma bir dizinin üçüncüsüdür: Meta-Bell Teorisi [6] matematiksel temeli oluşturmakta, Proof of WiseWork [7] ilk uygulama niteliğini taşımakta ve PoISV ise tamamlanmış, operasyonel düzeyde kesin protokolü temsil etmektedir.

2 Anlam Konsensüsü Sorunu

Katılımcıların *iddialar* (dünya hakkındaki ifadeler) gönderdiği bir ağda, her iddiaya o iddiayı değerlendiren doğrulayıcıların bağımsızlığını ve kamuya açık, doğrulanabilir bir bilgi külliyatıyla uyumunu yansıtan bir kalite

puanı eklenmesi istenmektedir.

Tek bir doğrulayıcı tarafından değerlendirilen tek bir iddia güvenilir değildir. Doğrulayıcı önyargılı, güncel olmayan bir bilgi tabanına sahip ya da yanlış bir anlatıyı zorlamaya çalışan koordineli bir grubun parçası olabilir. Birçok doğrulayıcı bile aynı hatalı modeli ya da aynı manipüle edilmiş veriyi kullanıyor olabilir. Doğrulayıcıların değerlendirmelerinde *gerçekten bağımsız* olduğunu ve bunu matematiksel olarak kanıtlayabileceğimizi gösteren bir mekanizmaya ihtiyaç vardır.

3 PoISV Protokolü

3.1 Bilgi Birimleri

Bir iddiayı $A = (d, \sigma)$ olarak tanımlarız; burada d serileştirilmiş ifade verisi, σ ise gönderenin isteğe bağlı dijital imzasıdır. Bilgi külliyatı $\mathcal{K}$, içerik hashleme aracılığıyla adreslenebilen sürümlü bir veri kümesidir. Onun $H(\mathcal{K})$ hashi, başlangıç bloğuna sabitlenmiştir.

3.2 Anlam Tutarlılık Puanı

$S_{con}(A) \in [0, 1]$ fonksiyonu deterministik olarak hesaplanır: A'dan varlıklar ve ilişkiler çıkarılır, $\mathcal{K}$'da destekleyici ya da çelişen olgular sorgulanır ve ağırlıklı bir uyum değeri döndürülür. Kesin uygulama protokol sürümüne göre sabitlenir; onun hashi blok başlığına dahil edilerek tam yeniden üretilebilirlik sağlanır.

3.3 Çakışma-Dışı İstatistik Ψ

Meta-Bell Teorisi [6], gerçekten bağımsız ölçümleri koordineli olanlardan ayırt etmek için biçimsel temeli sunar. Her doğrulayıcı i, doğru puanları $S^*(D_j)$ protokolde sabit olan k kanonik kontrol iddiasını $D_1, \ldots, D_k$ çözmelidir. Bu, hata vektörünü üretir:

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

Bir bloğa katkıda bulunan N doğrulayıcı için ortalama mutlak ikili Pearson korelasyonunu hesaplarız:

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

Bağımsız doğrulayıcılar, korelasyonsuz hata örüntüleri üretir ve $\Psi \approx 1$ elde edilir. Ortak modeli veya veriyi paylaşan çakışan doğrulayıcılar özdeş hata örüntüleri üretir ve $\Psi \approx 0$ elde edilir.

3.4 Kabul Kuralı

Bir blok yalnızca şu koşullar sağlandığında kabul edilir:

$$\frac{1}{|A|} \sum_{A \in \text{Blok}} S_{con}(A) \;\ge\; \theta_{min} \quad \text{ve} \quad \Psi \;\ge\; \Psi_{min}.$$

3.5 Blok Ağırlığı ve DAG Sıralaması

PoISV, dürüst çalışmayı boşa harcamaksızın paralel blok üretimine olanak tanımak için GHOSTDAG protokolünü [5] kullanır. Bir bloğun ağırlığı şu şekilde tanımlanır:

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

Kanonik zincir, DAG'daki en yüksek kümülatif ağırlıklı yoldur.

4 Güvenlik Analizi

Doğrulayıcıların $q < 0{,}5$ oranını kontrol eden bir saldırgana karşı U-istatistikleri için Hoeffding eşitsizliği uygulandığında, saldırganın $\Psi \geq \Psi_{min}$ değerini taklit edebilme olasılığı şu şekilde sınırlandırılır:

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

q	k	Ψ_{min}	$P(\text{Başarı})$
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 Ağ İşlemi

Ağın adımları şu şekildedir:

1. Yeni iddialar tüm doğrulayıcılara yayınlanır.
2. Her doğrulayıcı iddia için S_{con}'u hesaplar ve kontrol kümesindeki hata vektörünü kaydeder.
3. Blok önermek isteyen bir doğrulayıcı iddiaları toplar, toplu puanları hesaplar ve bir blok oluşturur.
4. Blok, bir zkVM [4] tarafından üretilen sıfır-bilgi hesaplama kanıtıyla birlikte yayınlanır.
5. Diğer doğrulayıcılar, puanlar eşikleri karşılıyor ve kanıt doğrulanıyorsa bloğu kabul eder.
6. Kabul edilen bloklar DAG'a eklenir ve her doğrulanmış iddiayı zincirde kalıcı olarak çapalar.

6 Sonuç

Güvenilir bir üçüncü tarafa dayanmayan, merkezi olmayan anlam doğrulama için bir sistem önerdik. Dijital imzalar ve kamuya açık bir bilgi külliyatından yola çıkarak, anlam tutarlılık puanı hesaplayan ve Meta-Bell Teorisi'ne dayanan çakışma-dışı test uygulayan eşler arası bir ağ oluşturduk. Kabul edilen iddialar bir DAG'a kalıcı olarak çapalanarak kamuya açık, değiştirilemez bir bilgi tabanı oluşturur. Bu konsensüs mekanizması aracılığıyla gerekli tüm kurallar ve teşvikler uygulanabilir.

Kaynaklar

[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 WiseWork: 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.