Proof of WiseWork:
Hakikat Konsensüsü için Eşler Arası Bir Sistem

Fatih Dinc
fatdinhero@gmail.com
Pforzheim, Almanya

Sürüm 2.0 – Nisan 2026
DOI: 10.5281/zenodo.19642292
OTS: poisv.com/verification

Özet

Hakikat keşfinin tamamen dağıtık bir biçimi, iddiaların güvenilir bir otoriteye başvurmadan bağımsız gözlemciler arasında doğrudan doğrulanmasına olanak tanıyacaktır. Dijital imzalar çözümün bir kısmını sağlar; ancak iletilen bilginin doğruluğunun değerlendirilmesi için hâlâ güvenilir bir üçüncü tarafa ihtiyaç duyuluyorsa temel faydalar yok olur. Bir eşler arası bilgelik doğrulayıcıları ağına dayalı olarak dağıtık hakikat sorununa bir çözüm öneriyoruz. Ağ, her önerilen blok için hakikat, bağlam, alaka ve etik uyumdan oluşan bileşik bir WiseScore hesaplar ve ek olarak Meta-Bell Teorisi'ne [7] dayanan bir kolüzyon-dışı test uygular. Kabul edilen bilgi birimleri, küresel ölçekte erişilebilir ve değiştirilemez bir bilgi tabanı oluşturarak DAG-sıralı bir zincire kalıcı biçimde çapalanır. Dürüst doğrulayıcılar, koordineli herhangi bir saldırgan grubundan daha fazla bağımsız anlam çalışması yaptığı sürece sistem güvenlidir.

1 Giriş

İnternetteki konsensüs bugün neredeyse tamamen merkezi aracılara dayanmaktadır. Finansal 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. Bu model günlük trafiğin büyük bölümü için işe yarar; ancak güven paradigmasının bilinen zayıflıklarından muzdariptir. Güvenin maliyeti kararın önemiyle birlikte artar ve hata ile manipülasyonun temel bir oranı kaçınılmaz olarak kabul edilir.

Mevcut merkezi olmayan konsensüs mekanizmaları sorunun daha dar bir bölümünü çözer. Proof of Work, hesaplama eforu harcanarak işlemlerin sıralamasında anlaşmaya varır. Proof of Stake, sermayeyi teminat olarak kilitleyerek aynı sıralamayı sağlar. Bu mekanizmaların hiçbiri, sıralanan bilginin içeriğinin doğru, bağlamsal olarak uygun, alakalı ya da etik olup olmadığı konusunda doğrulanabilir bir iddiada bulunmaz. Saf ödemeler için bu yeterlidir; bilgi çağı için değildir.

Gerekli olan şey, kıt kaynağın ham hesaplama gücü ya da sermaye değil, kanıtlanabilir biçimde bilge çalışmanın olduğu bir konsensüs mekanizmasıdır. Bu tür bir mekanizmayı Proof of WiseWork (PoWW) olarak adlandırıyoruz. Bu makale dört katkı sağlamaktadır: hakikat, bağlam, alaka ve etik uyumu bütünleştiren bileşik bir puan tanımlıyoruz; Meta-Bell Teorisi'nden türetilen bir istatistiğin kolüzyon yapan doğrulayıcıları bağımsızlardan ayırt etmek için kullanımını gösteriyoruz; kabul edilen birimlerin kalıcı zincir çapalanmasını açıklıyoruz ve saldırgan başarı olasılığının iki parametrede üssel düşüşünü türetiyoruz.

2 Bilgi Birimleri

Her bilgi birimini dörtlü $i = (v, c, r, e)$ olarak tanımlıyoruz; burada $v \in [0, 1]$ hakikat adayı, $c \geq 0$ bağlam ağırlığı, $r \geq 0$ alaka faktörü ve $e \in [0, 1]$ etik uyum değeridir. Dört bileşen, deterministik ve tüm düğümler tarafından yeniden üretilebilir olmak şartıyla farklı yöntemlerle üretilebilir.

Tek bir bilgi birimi, bir iddialar kümesinin kolektif hakikati hakkında güvenilir bir çıkarıma izin vermez. Yüksek bir hakikat puanı bağlam kaymasıyla değersizleşebilir, yüksek alaka yanlış varsayımlara dayanabilir, uygun bir bağlam alakasız içeriği öne çıkarabilir ve teknik olarak doğru bir iddia etik ilkelere aykırı olabilir. Yalnızca dört boyutun birleşimi sağlam bir gösterge sağlar.

Hakikat değeri v dört düzeyde tanımlanabilir. Ampirik düzeyde $v_i =$ doğrulanmış kanıt/toplam kanıt. Fiziksel düzeyde $v_i = 1 - |x_{\text{ölçüm}} - x_{\text{teori}}|/x_{\text{teori}}$. Kuantum-olasılıksal düzeyde $v_i = |\psi_i|^2$. Bilgi-kuramsal düzeyde $v_i = 1 - H(i)/H_{\text{max}}$, burada $H(i)$ Shannon entropisidir. Etik uyum değeri e de dört düzeyde tanımlanabilir: kodifiye edilmiş hukuki normlarla uyum derecesi, deontolojik kuralların yerine getirilme derecesi, konsakansiyalist net-yarar değerlendirmesi ya da bağlamsal değer tabanına uyum.

3 DAG Sıralama Katmanı

Doğrulayıcılar, doğrusal bir sıraya indirgenemeyen anlam görevlerinde paralel olarak çalışır. Klasik blokzincir konsensüsü bu paralel çalışmanın büyük bölümünü yetim blok olarak atacaktır. Bu nedenle sıralama katmanı olarak Sompolinsky, Wyborski ve Zohar'ın GHOSTDAG protokolünü [5] seçiyoruz. Bu protokolde her yeni blok, gözlemlenebilir tüm uçları üst blok olarak referans gösterir; bir k-küme algoritması ardışıl olarak dahil edilen bloklar üzerinde toplam bir sıra üretir. Sıralama katmanı içerik açısından agnostiktir; anlam doğrulama üsteki bir katmanda gerçekleştirilir.

4 Proof-of-WiseWork

I, bir bloğun tüm bilgi birimlerinin kümesi olsun. Her birime dört normalleştirilmiş nicelik atıyoruz. Normalleştirilmiş hakikat, keskinlik parametresi $\alpha > 0$ ile:

$$T(i) = \frac{\exp(\alpha \cdot v_i)}{\sum_{j \in I} \exp(\alpha \cdot v_j)}. \tag{1}$$

Softmax normalleştirme, beklenen hakikat değeri üzerindeki doğrusal kısıtlama altında maksimum-entropi ilkesinden kaynaklanır. Bağlam ağırlığı:

$$C(i) = \frac{c_i}{\sum_{j \in I} c_j}. \tag{2}$$

Alaka düzeyi:

$$R(i) = \log(1 + r_i). \tag{3}$$

Logaritmik sönümleme, alaka şişirmesinin puana yalnızca doğrusal altında katılmasını sağlar. Etik uyum: $E(i) = e_i$. Bileşik WiseScore:

$$W(i) = T(i) \cdot C(i) \cdot R(i) \cdot E(i). \tag{4}$$

Çarpımsal form, birimin dört boyutun hepsinde yeterince iyi puan alması zorunluluğundan izler. Etik açıdan sorunlu ama teknik olarak doğru bir sonuç sıfıra yakın puan alır. Toplu blok puanı:

$$\text{PoWW} = \frac{1}{|I|} \sum_{i \in I} W(i). \tag{5}$$

Kabul kuralı ayrıca Meta-Bell Teorisi'ne [7] dayalı bir kolüzyon-dışı koşul gerektirir. $\Psi > 0$, doğrulayıcıların gözlemlenen uyumunun ortak bir gizli değişkenle açıklanamayacağının istatistiksel kanıtıdır. Blok kabul koşulu:

$$\text{PoWW} \geq \theta \quad \text{ve} \quad \Psi \geq \Psi_{\min}. \tag{6}$$

5 Ağ

Ağın adımları şöyledir:

1. Yeni iddia birimleri tüm doğrulayıcılara gönderilir.
2. Her doğrulayıcı birimi Alım Katmanında yerel kabul kurallarına karşı işler ve zaman damgası ile imzayı kaydeder.
3. Her doğrulayıcı birim için T, C, R, E ve W'yi Anlama Katmanında hesaplar.
4. Blok önermek isteyen doğrulayıcı, Nexus zkVM [6] kullanarak sıfır-bilgi kanıtı üretir.
5. Blok, kanıtla birlikte yayınlanır.
6. Doğrulayıcılar tüm koşullar sağlanıyorsa bloğu kabul eder ve DAG'a ekler.

Doğrulayıcılar en yüksek toplam WiseScore'a sahip DAG'ı kanonik olarak kabul eder.

6 Teşvik Yapısı

Bloğun ilk işlem girişi, öneren doğrulayıcıya yeni para birimleri atayan özel bir kredidir. Katılımcılar belirli iddiaların doğrulanması için ek ücret ödeyebilir. Kabul kuralını atlatmak isteyen saldırgan, Ψ eşiğini karşılamak için gerçekten bağımsız doğrulayıcılar çalıştırmak zorunda kalır; bu ise koordinasyon amacıyla çelişir. Dolayısıyla kurallara uymak daha kârlıdır.

7 Zincir Üstü Bilgi Tabanı ve Depolama Geri Kazanımı

Kabul edilen birimler tam puanları ve zk-kanıtlarıyla zincire kalıcı çapalanır. Her katılımcı herhangi bir iddia için puanını, bağlamsal gömülmesini, kanıt dayanağını ve etik değerlendirmesini sorgulayabilir. Bu, PoWW'yi yalnızca mülkiyet ilişkilerini dijitalleştiren klasik blokzincirlerden ayırır. Merkle ağacı sayesinde eski doğrulayıcı çıktılar blok hashini bozmadan atılabilir; saniyede bir blok hızında yıllık yaklaşık 6 gigabayt depolama gerekmektedir.

8 Basitleştirilmiş Doğrulama

Tam düğüm çalıştırmadan kabul kuralını doğrulamak mümkündür. İstemci yalnızca blok başlıklarını ve zk-kanıtları indirir. Doğrulama, dürüst doğrulayıcılar ağı kontrol ettiği sürece güvenilirdir. Hafif istemciler, ağa dayatmaksızın öznel filtreler uygulayabilir.

9 İddiaların Birleştirilmesi ve Bölünmesi

Bir iddia, atomik alt-iddiaları ayıran ya da birleştiren birden fazla giriş ve çıkış kenarı içerir. Normalde en fazla iki çıkış bulunur: biri kabul edilen alt-iddia, diğeri kalan belirsizlik artığı için. Fan-out burada sorun oluşturmaz.

10 Mahremiyet

zkVM tanığı ham kanıt kaynaklarını içerir ve özel kalır; yalnızca kabul kuralının sonucu ve sayısal puan kamuya açıklanır. Ψ testi yalnızca kamusal doğrulayıcı çıktılarının korelasyon yapısı üzerinde işler ve ek bilgi ifşa etmez. Her iddia için yeni anahtar çifti kullanılması önerilir.

11 Hesaplamalar

Dürüst zinciri ile saldırgan zinciri arasındaki yarışı Rassal Yürüyüş olarak modelleriz. p dürüst doğrulayıcının, q ise saldırganın bir sonraki bloğu bulma olasılığı; q_z ise saldırganın z blok gerisinden kurtulma olasılığıdır:

$$q_z = 1 \text{ eğer } p \leq q, \qquad q_z = (q/p)^z \text{ eğer } p > q.$$

Alıcının bekleme süresi analizi için, saldırganın gizli ilerlemesini $\lambda = z \cdot (q/p)$ beklentili Poisson dağılımı olarak modelliyoruz:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \left(1 - \left(\frac{q}{p}\right)^{z-k}\right).$$

C kodu:

```
#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;
}
```

Bazı sonuçlar ($q = 0{,}1$):

z	P
0	1,0000000
1	0,2045873
2	0,0509779
5	0,0009137
10	0,0000012

z	P ($q = 0{,}3$)
0	1,0000000
5	0,1773523
10	0,0416605
20	0,0024804
50	0,0000006

$P < \%0{,}1$ için: $q = 0{,}10 \Rightarrow z = 5$; $q = 0{,}20 \Rightarrow z = 11$; $q = 0{,}30 \Rightarrow z = 24$; $q = 0{,}40 \Rightarrow z = 89$.

Meta-Bell istatistiği ikinci, bağımsız bir sınır ekler. Kolüzyon altında Ψ'nin beklenen değeri sıfırdır; Hoeffding eşitsizliği şunu verir:

$$P_{\Psi}(k) \leq \exp\left(-2k \cdot \frac{\Psi_{\min}^2}{\Delta_{\text{krit}}^2}\right).$$

Birleşik saldırgan başarı olasılığı iki sınırın çarpımıdır; gerekli kolüzif kohortin büyüklüğünde üssel olarak düşer.

12 Sonuç

Güvenilir bir otoriteye dayanmayan dağıtık hakikat doğrulaması için bir sistem önerdik. Dijital imzalar ve kamuya açık bilgi külliyatından yola çıkarak, bileşik WiseScore hesaplayan ve Meta-Bell kolüzyon-dışı testini uygulayan bir eşler arası ağ oluşturduk. Kabul edilen birimler bir DAG'a kalıcı çapalanarak 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] C. E. Shannon, *A Mathematical Theory of Communication*, BSTJ 27, 1948.

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

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

[7] F. Dinc, *Meta-Bell Teorisi*, v1.0, SHA-256: 062e290009f6b7339e9a8b522ce1d94d9021d109d8e4bc41210d1f3dda053a3b, 2026.

[8] W. Feller, *An Introduction to Probability Theory*, 1957.