Proof of Time: A Peer-to-Peer Electronic Cash System Based on Time

Alejandro Montana alejandromontana@tutamail.com

Version 2.0 — December 2025

Abstract

A purely peer-to-peer version of electronic cash where consensus is based on time, not capital. The main problem with existing systems is that influence is proportional to money: in Proof of Work — to ASIC purchases, in Proof of Stake — to token holdings. We propose a system where the only resource that matters is time. Time cannot be bought, accelerated, or transferred. Run a node for 180 days — gain maximum influence. Your capital is irrelevant.

1. Introduction

Commerce on the Internet has evolved from trusted third parties to trustless consensus. Bitcoin solved the double-spending problem through Proof of Work. Ethereum added programmability through Proof of Stake. Both systems share a fundamental flaw: influence is bought with money.

In PoW, those who can afford more ASICs control the network. In PoS, those who hold more tokens control the network. The promise of decentralization collapses into plutocracy.

We need a system where: - Influence cannot be purchased - Entry barrier is zero - Attack cost scales with time, not money

The solution is Proof of Time.

2. Time as Consensus

2.1 The Problem with Capital-Based Consensus

```
PoW:  Influence = f(Money → Hardware → Electricity)
PoS:  Influence = f(Money → Tokens)
PoT:  Influence = f(Time)
```

Time is the only resource distributed equally to all humans. One second for a billionaire equals one second for anyone else.

2.2 Verifiable Delay Functions

A Verifiable Delay Function (VDF) is a function that: 1. Requires sequential computation (cannot be parallelized) 2. Produces a proof that can be quickly verified 3. Has deterministic output

We use Wesolowski VDF:

```
y = x^(2^T) mod N
π = x^⌊2^T/l⌋ mod N

where:
  T = number of iterations (time parameter)
  N = RSA modulus (2048-bit)
  l = hash-derived prime
```

Verification: `y = π^l · x^r mod N` where `r = 2^T mod l`

VDF guarantees that T sequential squarings were performed. No amount of money can speed this up — only time.

---

3. Dual-Layer Architecture

3.1 Layer 1: Proof of History (PoH)

Fast transaction layer. Sequential SHA-256 chain:

```
H(n) = SHA256(H(n-1) || data || timestamp)
```

- 1 hash per slot
- Transactions embedded in hash chain
- Provides ordering without consensus

3.2 Layer 2: Proof of Time (PoT)

Finality layer. VDF checkpoints every 600 seconds:

```
Checkpoint(n) = VDF(H(last_slot), T=1,000,000)
```

- Cannot be reverted after VDF completion
- 10-minute finality (like Bitcoin, but deterministic)
- Checkpoint = irreversible anchor

---

4. Leader Selection

4.1 ECVRF

Leader is selected via Elliptic Curve Verifiable Random Function:

```
(β, π) = VRF_prove(sk, seed)
VRF_verify(pk, seed, β, π) → {0, 1}
```

Where: - `seed` = previous checkpoint hash - `β` = pseudo-random output - `π` = proof of correct computation

4.2 Selection Probability

```
P(node_i) = Adonis(i) / Σ Adonis(all)

Selected if: β < P(node_i) × 2^256
```

The Adonis score determines selection probability.

---

5. The Six Dimensions of Adonis

Node weight is computed from six dimensions, each measuring a different aspect of node contribution.

5.1 Formula

```
Adonis(i) = Σ(w_d × score_d) for d ∈ {TIME, INTEGRITY, STORAGE, GEOGRAPHY, RELIABILITY, STAKE}
```

5.2 Dimensions

#	Dimension	Domain	Weight	Saturation
1	**TIME**	Uptime	35%	180 days
2	**INTEGRITY**	Behavior	22%	No violations
3	**STORAGE**	Data	15%	100% chain history
4	**GEOGRAPHY**	Location	12%	Country + city diversity
5	**RELIABILITY**	Performance	8%	99.9% response rate

#	Dimension	Domain	Weight	Saturation
6	**STAKE**	Collateral	8%	Optional

5.3 TIME — 35%

```
score_time = min(uptime_seconds / 15,552,000, 1.0)
```

15,552,000 seconds = 180 days. After 180 days, newcomer equals veteran.

TIME is the primary dimension. Without time commitment, nothing else matters.

5.4 INTEGRITY — 22%

Behavioral score. Positive actions increase, violations decrease:

Event	Change
BLOCK_PRODUCED	+0.05
BLOCK_VALIDATED	+0.02
BLOCK_INVALID	−0.15
EQUIVOCATION	−1.0 + 180-day quarantine

Double protection: score reduction AND time penalty.

5.5 STORAGE — 15%

```
score_storage = min(stored_blocks / total_blocks, 1.0)
```

Full nodes store complete history. Light nodes get proportional score.

5.6 GEOGRAPHY — 12%

Incentivizes global distribution:

```
country_score = 0.6 × (1 / (1 + log10(nodes_in_country))) + 0.4 ×
(countries / 50)
city_score = 0.7 × (1 / (1 + log10(nodes_in_city))) + 0.3 ×
(cities / 100)
geography = 0.6 × country_score + 0.4 × city_score
```

First node from new country: +0.25 bonus. First node from new city: +0.15 bonus.

Fewer nodes in your location = higher score. Incentivizes global distribution.

5.7 RELIABILITY — 8%

```
score_reliability = successful_responses / total_requests
```

Measures node availability and response quality over time.

5.8 STAKE — 8%

Optional collateral for enhanced trust. Not required for basic participation. Provides additional weight for nodes willing to put tokens at risk.

---

6. DAG Structure

6.1 Block References

Each block references 1–8 parent blocks:

```
Block {
  parents: [hash_1, hash_2, ..., hash_k]  // k ∈ [1, 8]
  transactions: [...]
  vrf_proof: π
  timestamp: t
}
```

6.2 PHANTOM-PoT Ordering

Blocks are ordered by: 1. VDF checkpoint anchors 2. Topological sort within checkpoint window 3. Tie-breaking via block hash

Horizontal scaling: more parents = higher throughput.

---

7. Economics

7.1 Unit

```
1 Ɉ (Jot) = 1 second of time
```

7.2 Emission

Parameter	Value
Total supply	1,260,000,000 Ɉ
Block time	10 minutes
Initial reward	50 Ɉ per block
Halving	Every 210,000 blocks (~4 years)
Full emission	~132 years

Same curve as Bitcoin. Predictable, deflationary.

---

8. Privacy Tiers

Tier	Hidden	Size	Fee Multiplier
T0	Nothing	250 B	1×
T1	Receiver (stealth address)	400 B	2×
T2	+ Amount (Pedersen commitment)	1.2 KB	5×
T3	+ Sender (ring signature)	2.5 KB	10×

Privacy is optional. User chooses transparency vs. anonymity.

---

9. Attack Analysis

9.1 Sybil Attack

Creating N fake nodes: - Each needs 180 days to reach TIME saturation - No shortcut. N nodes = N × 180 days

```
Attack cost = N × 180 days
```

9.2 51% Attack

To control 51% of Adonis weight: - Need 51% of TIME-weighted nodes - With 1000 existing nodes at 180 days: need 1020 nodes running 180 days

```
Cost = 1020 × 180 = 183,600 node-days
```

Compare: - Bitcoin 51% attack: ~$20B in hardware - Ethereum 51% attack: ~$10B in stake - **Proof of Time 51% attack: N × 180 days (cannot be bought)**

9.3 Long-Range Attack

VDF checkpoints are irreversible. Rewriting history requires: 1. Recomputing all VDFs from fork point 2. Each VDF takes real time 3. Honest chain always ahead

Not feasible.

---

10. Comparison

Property	Bitcoin	Ethereum	Proof of Time
Consensus	PoW	PoS	VDF + Time
Influence	Money→ASIC	Money→Stake	Time only
Entry cost	High	Medium	**Zero**
Energy	Massive	Low	Minimal

Property	Bitcoin	Ethereum	Proof of Time
51% attack cost	$20B	$10B	N × 180 days
Finality	Probabilistic	~15 min	10 min (deterministic)

11. Pantheon Architecture

The protocol is organized into 12 modules, each named after a Greek deity:

#	God	Domain	Description
1	**Chronos**	Time	VDF, temporal proofs
2	**Adonis**	Reputation	6-dimension trust
3	**Hermes**	Network	P2P, Noise Protocol
4	**Hades**	Storage	SQLite, DAG
5	**Athena**	Consensus	VRF leader selection
6	**Prometheus**	Crypto	Ed25519, ECVRF
7	**Mnemosyne**	Memory	Mempool, cache
8	**Plutus**	Wallet	UTXO, keys
9	**Nyx**	Privacy	Ring signatures
10	**Themis**	Validation	Transaction rules
11	**Iris**	API	RPC, WebSocket
12	**Ananke**	Governance	Protocol upgrades

12. Conclusion

We have proposed a system for electronic transactions that does not rely on capital for consensus. Time is the only resource that cannot be bought, accelerated, or transferred.

The network self-organizes through the Six Dimensions of Adonis: - **TIME** ensures long-term commitment - **INTEGRITY** removes bad actors - **STORAGE** maintains data availability - **GEOGRAPHY** enforces global distribution - **RELIABILITY** rewards performance - **STAKE** provides optional collateral

The result is a system where: - Everyone starts equal - Influence is earned, not bought - Attacks require time, not money - Decentralization is incentivized, not just promised

In time, we are all equal.

References

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
2. Wesolowski, B. (2019). Efficient Verifiable Delay Functions.
3. Boneh, D., et al. (2018). Verifiable Delay Functions.
4. Sompolinsky, Y., Zohar, A. (2015). PHANTOM: A Scalable BlockDAG Protocol.
5. Micali, S., Rabin, M., Vadhan, S. (1999). Verifiable Random Functions.

Ɉ