Trillion

TEEs in Web3

Powering Rollups, Consensus, and Real-World Exchange Infrastructure

From hardware isolation to verifiable DeFi — where trusted execution meets blockchain.

PROF. GIOVANNI MAZZEO
CHIEF SCIENTIST @ TRILLION
ASSOCIATE PROFESSOR @ UNIVERSITY OF NAPLES 'PARTHNOPE'

Talk Roadmap

01

The Trilemma Trap & DEX Challenges

The security-scalability-decentralization tradeoffs

02

TEEs in Web3: Usage Patterns

Rollups, sequencers, provers, consensus, confidential smart contract

03

The Trillion DEX Architecture

Verifiable execution, TEE Chain, ZK assurance layer

04

PoTE: Proof of Trusted Execution

A new consensus paradigm for deterministic finality

05

Investor & Customer Concerns

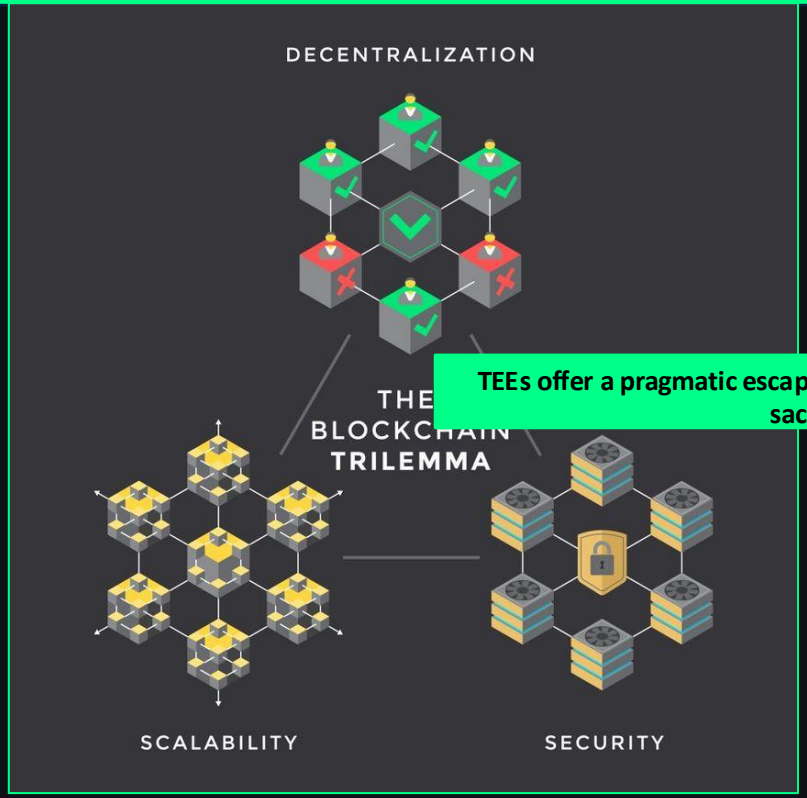
What risks matter and why hardware trust isn't enough

06

Mitigations: Defense-in-Depth

Multi-vendor diversity · Platform Ownership Assurance · ZK backstop

The Blockchain Trilemma Trap



The trilemma suggests that a blockchain can only optimize for **two out of the three** at the same time — improving one often weakens another.

TEEs offer a pragmatic escape hatch — hardware-enforced trust without sacrificing throughput

Real-World Tradeoffs

PoW (Bitcoin) / PoS (Ethereum)

12s slots, slow finality

Alternative Consensus Protocols

Delegated Proof of Stake (DPoS), Proof of Authority, Hybrid models
Often improve scalability but may reduce decentralization.

Optimistic Rollups

Correctness verified after the fact — 7-day dispute windows

ZK Rollups

Strong guarantees, but proving overhead limits real-time trading

Based/Native Rollups

Rollups solutions where certain functions are delegated to the L1 chain

DEXs and the Trilemma Trap

High-performance DEXs inevitably move execution off-chain

Off-chain execution ⇒ implicit trust in operators

Risks:

- MEV & unfair ordering
- Selective censorship
- Opaque execution policies

Sequencers, matchers, engines become centralized points

Users regain speed but lose verifiability

Performance gains often reintroduce Web2-style trust assumptions

Where TEEs Are Being Deployed Across the Web3 Stack

TEE-Secured Rollups

TEE-Enhanced Consensus Protocols

TEE-Secured AI Agents & Coprocessors

Confidential Smart Contracts

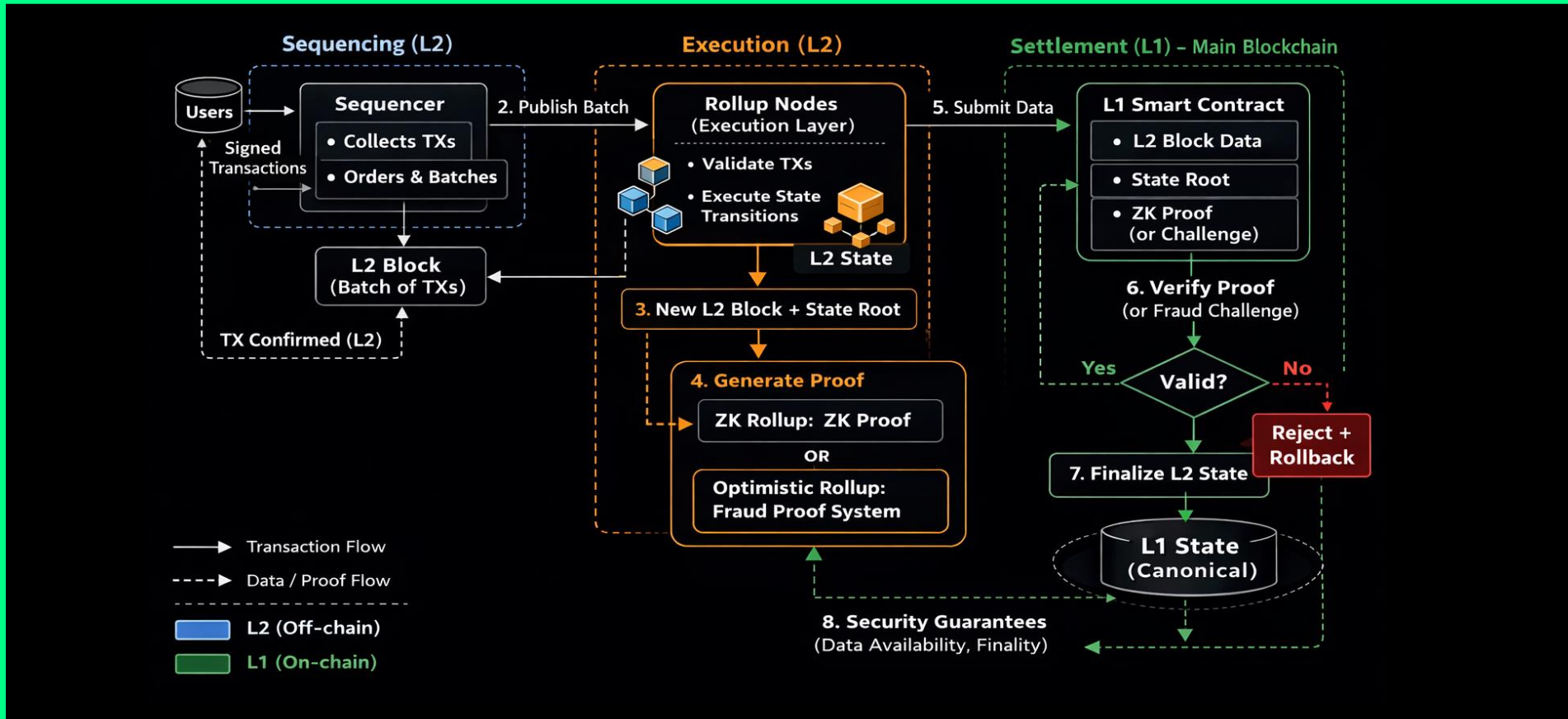
All share that the Attestation Verification is usually made On-Chain

Decentralized Oracle Networks

Key Management & MPC Wallets

Cross-Chain Bridges & Interoperability

Rollups Architecture



TEEs for Enhancing Trust in Rollups

TEE Sequencer

Ordering inside enclave. Non-reorderable batch commitment before execution.

- **Astria**
- **Espresso**
- **Rollup-Boost (Flashbots)**

TEE Execution Engine

STF runs inside attested enclave. Correctness enforced at runtime, not inferred after.

- **Obscuro / TEN Protocol**
- **Automata Network**
- **Phala / Phat Contracts**

TEE-Assisted Proving

TEE accelerates ZK proof generation with integrity guarantees on the prover.

- **Risc Zero / Boundless**
- **Marlin / Oyster**

Consensus Protocols

Proof of Work

Bitcoin

Security via computation

Proof of Stake

Ethereum

Security via capital stake

BFT-style PoS

Tendermint · HotStuff

Deterministic single-round finality

PoS + Proof of History

Solana

High throughput via verifiable clock

Scalability Limitations

- Block propagation & network latency bottleneck throughput at every node
- Global state replication: all validators process every transaction
- Solana pushes TPS but demands high-spec validator hardware
- Decentralization ↔ throughput is a hard trade-off, not an engineering detail

Cost Constraints

PoW	Energy + ASIC hardware costs. Security = wasteful spend.
PoS	Capital lock-up + slashing risk. Opportunity cost on staked assets.
Solana	Lower tx fees, but higher validator hardware requirements.
All L1s	Fee spikes under congestion — degraded UX at peak load.

TEE-Enhanced Consensus Protocols

Gen 1 — TEE for Leader Election

TEE generates verifiable randomness or attests useful computation to replace PoW. Single-vendor SGX. Probabilistic fork-based finality preserved.

Market Solutions / Research

- Proof of Luck (SGX)
- Proof of Useful Work (SGX)
- Early Hyperledger TEE proposals

⚠ Single-vendor trust · Probabilistic finality · No multi-vendor diversity

Gen 2 — TEE-Assisted BFT

TEE Prevents equivocation (a node lying by sending different votes). Ensures nodes follow protocol rules. Reduces communication overhead

Market Solutions / Research

- DAMYSUS (HotStuff + Checker/Accumulator)
- Achilles (rollback-resilient TEE BFT)
- SplitBFT (compartmentalized PBFT)
- Engraft (Raft+SGX → BFT semantics)

⚠ Retains multi-round voting · Single vendor (SGX) · Optimizes BFT but doesn't replace it

Gen 3 — Attested Deterministic Execution

Consensus replaced by hardware-attested deterministic execution. Cross-vendor quorum as safety primitive. Fork-free single-round finality. No replica voting.

Market Solutions / Research

- PoTE / Trillion (multi-vendor quorum)

⚠ Requires k-of-n vendor availability

The Verifiable Trillion DEX

Trillion's Answer: Enforce correctness at execution time — not after the fact — enabling "Instant Finality"

1

TEE-based Sequencing

- Transactions are ordered deterministically
- Sequencers run in attested enclaves
- Ordered inputs are signed and broadcast

2

Deterministic Execution in TEEs

- Matching, risk, and liquidation run inside enclaves
- Execution is bound to the ordered input stream
- Outputs include cryptographic attestations

3

PoTE Consensus & Finalization

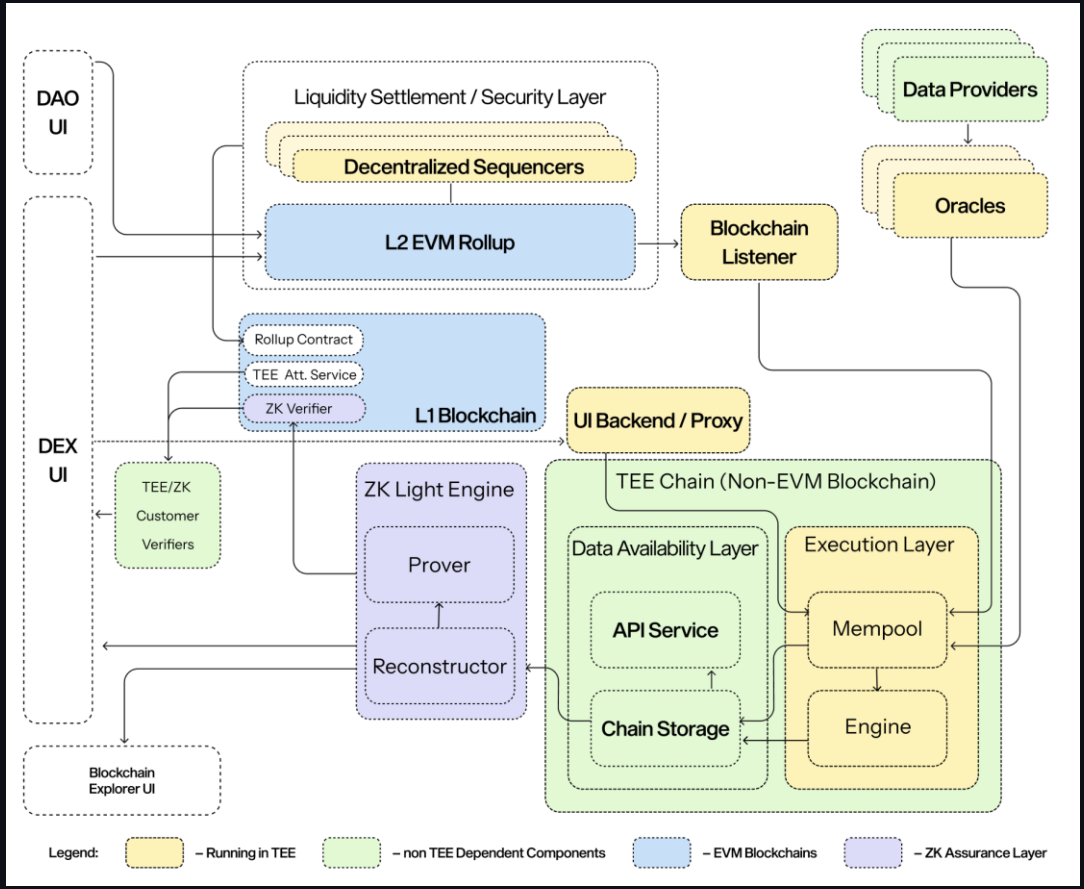
- PoTE validators verify enclave attestations
- Consensus is reached on valid state transitions
- Finalized outputs are committed for settlement in a TEE-based rollup

4

Defense-in-Depth

- Multi-vendor diversity
- Dual Attestation
- ZK fallback

Trillion Architecture



PoTE: Proof of Trusted Execution — A New Consensus Paradigm

Core Idea

Replace replicated re-execution and multi-round voting with verifiable deterministic execution.

1. **Unique Proposer Selected**
2. **TEE Executes Canonical Program C**
   Deterministic STF inside enclave. Block produced with code measurement.
3. **Proposer generates a Proposer Certificate (PC)**
   Attestation q_p binds $(hC, H(Bt), t)$. Enclave signature σ_p over block.
4. **Validators Re-Attest (not re-execute)**
   Each validator verifies block and attaches own vendor attestation.
5. **Quorum Certificate (k-of-n vendors)**
   Block final once at least k attestations are verified. Fork-free. No voting rounds.

Testbed Results (Azure: TDX + SEV)

< 150ms
Block commit latency (up to 225 validators)

>100,000
TPS with 2k tx/block @ 100ms execution

Investors & Customers Do Care About TEE Risks

Key investor question: Does the system fail safely when TEE assumptions are violated?

Hardware Vulnerabilities

· Foreshadow, Plundervolt, WeSee — side-channels that leak enclave secrets

· TEE.fail (2026): DDR5 memory bus interposition extracts keys from TDX, SEV-SNP, SGX

· Physical access → secrets extractable in non-approved environments

Vendor Monoculture

· Single-vendor TEE = single point of trust and failure

· Vendor compromise/collusion could undermine entire system

Attestation Gaps

· Standard remote attestation proves WHAT code runs — not WHERE it runs

· No proof a TEE is in an approved data center with physical security

Mitigation 1: Multi-Vendor TEE Diversity

Threat: A 0-day in vendor v* enables arbitrary manipulation of enclave outputs or extraction of attestation keys

Rotated Primary Executor

One vendor is primary per epoch (block/batch). Selection is unpredictable (derived from prior blocks or randomness beacon). Vendor v* can't ensure it's always primary.

Temporal Containment

Compromised epoch produces incorrect C't. Non-primary replicas from other vendors recompute off critical path and detect divergence — triggering dispute escalation.

Customer Vendor Policies

Customers can specify which vendors they accept for their execution. Verifier enforces vendor constraints per-customer.

Dynamic Vendor Exclusion

Governance or automated detectors can exclude vendor V from primary rotation upon exploit/vulnerability disclosure. Scoped exclusion (firmware range, enclave measurement family).

Mitigation 2: Platform Ownership Assurance (POA)

Threat: Standard TEE attestation proves WHAT code runs — not WHERE. Relay/proxy attacks, tee.fail-style physical extraction outside approved facilities.

Dual Attestation Evidence Bundle E = { Q_TEE, Q_PO, nonce, meta }

Q_TEE — Code Integrity Attestation

- TEE vendor proves enclave/CVM identity
- Measured launch state: correct code is running
- Standard remote attestation (Intel TDX, AMD SEV, etc.)

AND

Q_PO — Platform Ownership Attestation

- Cloud provider / hardware manufacturer root
- vTPM-backed: platform belongs to approved domain D
- Intel Platform Ownership Endorsements (POE/PIID)

Mitigation 3: ZK-Verified Execution Backstop

Worst case: Attacker fully compromises TEE fast-path (multi-vendor compromise OR broken verification roots) — can forge C't and attestations

ZK Statement per epoch t:

```
StateRoot_t+1  =  F( StateRoot_t,  Inputs_t,  Rules_t )
```

Lifecycle

1. **TEE Fast Path Executes**

   Low-latency execution. Trade confirmations available immediately (subject to policy).

2. **Prover Generates ZK Proof (async)**

   Prover proves StateRoot_t+1 = F(pre, inputs, rules).

3. **On-Chain ZK Verifier**

   Proof recorded and verified on-chain

4. **Settlement Gated on ZK**

   Withdrawals/irreversible actions require ZK-finalized checkpoint ($t \leq t^*$)

Defense-in-Depth: Security Layer Summary

L1	**Multi-Vendor TEE Diversity** Threat: Vendor 0-day / monoculture	Rotated primaries · temporal containment · asynchronous dispute · dynamic exclusion
L2	**Platform Ownership Assurance** Threat: Physical attack / relay-proxy	Dual attestation · identity/challenge/time binding · approved deployment domain D enforced
L3	**Decentralized On-Chain Attestation** Threat: Vendor attestation service outage / centralization	Quote verification on-chain · governance-controlled allowlists · rapid revocation without operator
L4	**ZK-Gated Settlement** Threat: Full TEE compromise / broken trust	STARK proofs for settlement-critical actions · hardware-independent · no trusted setup

Thank You

Contact At **giovanni@trillion.xyz**

Website **trillion.xyz**