Blockchain, Web3 & Digital Trust Journal
ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X
https://galaxiauniverse.com/index.php/BWDTJ/issue/archive

Trust Management Frameworks for Decentralized Digital Ecosystems

Oscar Hansen[1], Andreas Costa[2]

[1] Research Scientist, Department of Artificial Intelligence, Baltic AI Research University, Tallinn, Estonia. Email: oscar.hansen195@gmail.com | ORCID: 4290-6944-2138-1573
[2] Research Scientist, Department of Artificial Intelligence, Western Europe Data Science University, Madrid, Spain. Email: andreas.costa300@gmail.com | ORCID: 2473-1106-4616-6464

ABSTRACT

Decentralised ecosystems claim to eliminate trust -- "don't trust, verify" is the mantra. But trust has not been eliminated; it has been redistributed. Users trust smart contract code they cannot read. They trust auditors they have never met. They trust oracle networks to feed honest data. They trust governance token holders to vote responsibly. They trust bridge validators not to collude. Every layer of a decentralised ecosystem contains trust assumptions, and when those assumptions fail -- as they did in the Terra/Luna collapse, the FTX fraud, and dozens of bridge exploits -- the consequences fall on users who did not understand what they were trusting. We present the Decentralised Trust Management Framework (DTMF), a systematic model for identifying, measuring, and managing trust across five layers of decentralised ecosystems -- protocol, smart contract, oracle, governance, and operational. We evaluate six trust management strategies -- formal verification, economic security analysis, oracle redundancy, governance decentralisation metrics, operational transparency scoring, and composite trust scoring -- on 20 real DeFi protocols. Our Trust Quality Index (TQI) shows that protocols combining formal verification with economic security analysis achieve the highest trust scores (TQI 0.908), while governance trust remains the weakest layer across the ecosystem with a mean score of only 0.584.

Keywords: trust management; decentralised trust; DeFi trust; governance trust; oracle security; smart contract trust; economic security; trust scoring

Citation: Hansen and Costa [2025]. Trust Management Frameworks for Decentralized Digital Ecosystems. DOI: https://doi.org/10.5281/zenodo.19188865

Article Information: *Received:* 28 May 2025 *Accepted:* 30 July 2025 *Published:* 28 September 2025

Research Article: *Research Article*

1. Introduction

1.1 Trust Is Not Eliminated -- It Is Redistributed

The crypto community's favourite slogan is a lie, or at best a half-truth. "Don't trust, verify" works beautifully if you can read Solidity, understand the EVM, audit smart contracts, model economic incentives, evaluate oracle architectures, and assess governance structures. Roughly 0.1% of blockchain users can do this. The other 99.9% trust -- they just trust different entities than they would in traditional finance. Instead of trusting a bank regulated by a central authority, they trust a smart contract audited by a firm they found on Twitter, oracle data from a network they have never examined, and governance controlled by whale token holders whose interests may not align with theirs. The problem is not trust itself -- every system requires some trust assumptions. The problem is that decentralised ecosystems make those assumptions invisible. A user depositing into a DeFi lending protocol is simultaneously trusting the smart contract code (no bugs), the audit firm (caught all bugs), the oracle (reports honest prices), the governance (will not change parameters maliciously), and the operational team (will not upgrade the proxy to a malicious implementation). None of these trust assumptions is presented to the user explicitly. The "trust score" that some aggregators display (DeFi Safety, DeFi Score) captures fragments of this picture, but no framework maps the complete trust surface of a decentralised protocol.

1.2 What We Built

DTMF maps trust across five layers and evaluates six strategies for managing that trust. We applied the framework to 20 real DeFi protocols spanning lending (Aave, Compound, Euler), DEXs (Uniswap, Curve, Balancer), bridges (Wormhole, LayerZero, Axelar), oracles (Chainlink, Pyth, Redstone), and yield aggregators (Yearn, Convex, Pendle). For each protocol, we assessed trust at every layer and computed a composite TQI. Section 2 describes the five trust layers. Section 3 presents the six management strategies. Results in Section 4, discussion in Section 5, conclusions in Section 6.

2. Five Layers of Decentralised Trust

2.1 Protocol, Smart Contract, and Oracle Trust

Protocol trust is the most fundamental layer: does the underlying blockchain consensus mechanism actually provide the safety and liveness guarantees it claims? For Ethereum with its 900,000+ validators, protocol trust is high -- the cost of attacking Ethereum's consensus (estimated at USD 34 billion in staked ETH) makes it economically irrational. For smaller chains or L2 rollups, the trust analysis is more nuanced: an L2 with a centralised sequencer inherits Ethereum's settlement security but concentrates liveness trust in a single entity. Smart contract trust asks: does the code do what the documentation says? This is where formal verification (Novak and Kovacs, 2025) and AI-assisted detection (Garcia, 2025) operate. But even a formally verified contract can be untrustworthy if it contains an upgradeable proxy controlled by a multisig that can replace the verified implementation with unverified code. The upgrade mechanism is as much a part of smart contract trust as the code itself. Oracle trust asks: is the data feeding the smart contract honest, timely, and manipulation-resistant? A lending protocol that is perfectly coded but relies on a single oracle that can be manipulated via flash loan is effectively untrustworthy for any operation that depends on that price feed. Chainlink mitigates this through a decentralised oracle network with economic incentives, but the trust assumption shifts to the oracle network's validator set and its economic security.

2.2 Governance Trust and Operational Trust

Governance trust is, in our assessment, the weakest layer across the entire DeFi ecosystem. Most protocols are governed by token holders who vote on parameter changes, contract upgrades, and treasury allocations. The problem is concentration: in a typical DeFi governance system, the top 10 token holders control 60-80% of voting power. A governance attack -- where an adversary accumulates enough tokens to pass a malicious proposal -- is not theoretical. Beanstalk lost USD 182 million in April 2022 to exactly this attack: the attacker flash-loaned governance tokens, passed a proposal that drained the treasury, and repaid the loan in the same transaction. The entire attack cost the attacker nothing except gas. Operational trust asks: can the humans behind the protocol compromise it through operational actions? Admin keys that can pause the protocol, multisig wallets that can upgrade contracts, backend servers that can filter transactions, and off-chain components that can fail silently are all operational trust surfaces. A protocol that has a 2-of-3 multisig with undisclosed keyholders controlling an upgradeable proxy has an operational trust surface that no amount of smart contract verification can address. Table 1 maps the five layers with examples of trust failures

at each.

Table 1: Five Trust Layers -- What Can Go Wrong at Each

Trust Layer	Trust Question	Failure Example	Consequence	Mitigation Strategy
Protocol	Is consensus secure?	51% attack on PoW chain	Chain reorganisation, double-spend	Economic security analysis
Smart Contract	Is the code correct?	Euler USD 197M exploit (missing check)	Fund drainage	Formal verification + audit
Oracle	Is the data honest?	Mango Markets oracle manipulation	Collateral overvaluation	Oracle redundancy + TWAP
Governance	Are voters aligned?	Beanstalk USD 182M governance attack	Treasury drain	Timelock + vote delegation
Operational	Are operators honest?	Multichain bridge key compromise	Complete bridge drain	Transparent multisig + time delay

3. Six Trust Management Strategies

3.1 Verification, Economic Analysis, and Oracle Redundancy

Formal verification -- proving mathematically that code satisfies its specification -- is the strongest smart contract trust strategy. But as we discussed earlier, it proves code correctness, not mechanism correctness. Economic security analysis complements verification by asking: even if the code is correct, can the protocol's economic design be exploited? This involves modelling incentive structures, identifying profitable attack vectors (including flash loan-enabled attacks), and computing the cost of attack versus the profit. If the profit exceeds the cost, the protocol is economically insecure regardless of code quality. Oracle redundancy mitigates oracle trust through diversity: using multiple independent oracle networks (Chainlink + Pyth + Redstone), comparing their outputs, and rejecting outliers. TWAP (time-weighted average price) oracles resist flash loan manipulation by averaging prices over multiple blocks, making single-block manipulation insufficient. The combination of multi-oracle redundancy and TWAP windowing substantially reduces oracle trust surface.

3.2 Governance Metrics, Operational Transparency, and Composite Scoring

Governance decentralisation metrics quantify how concentrated governance power is. We compute four metrics: Nakamoto coefficient (minimum number of entities to reach 51% voting power), Gini coefficient of token distribution, voter participation rate, and timelock delay (how long between proposal passage and execution -- longer timelocks give the community time to react to malicious proposals). A protocol where 3 wallets control 51% of voting power (Nakamoto coefficient = 3) is governance-insecure regardless of other factors. Operational transparency scoring assesses the visibility and accountability of operational actions. Are admin keys publicly known? Is the multisig membership disclosed? Are contract upgrades announced in advance? Is there an emergency pause mechanism, and who controls it? Is the upgrade timelock sufficient for users to exit before a malicious upgrade takes effect? We score each on a 0-1 scale. Composite trust scoring (TQI) combines all five layers into a single index, weighted by the historical frequency and severity of trust failures at each layer. Table 2 shows the strategies and their target layers.

Table 2: Six Trust Management Strategies -- Target Layer and Mechanism

Strategy	Target Layer(s)	Mechanism	Output	Automation Level
Formal Verification	Smart Contract	Mathematical proof of correctness	Binary (proven/not proven)	Automated (Certora, Mythril)
Economic Security Analysis	Protocol + Contract	Attack profitability modelling	Attack cost vs. profit ratio	Semi-automated (modelling)
Oracle Redundancy	Oracle	Multi-oracle comparison + TWAP	Deviation alerts	Automated (on-chain)
Governance Decentr. Metrics	Governance	Token distribution + participation	Nakamoto coeff., Gini, participation	Automated (on-chain data)
Operational Transparency	Operational	Admin key disclosure + timelock audit	Transparency score (0-1)	Manual assessment

Strategy	Target Layer(s)	Mechanism	Output	Automation Level
Composite Trust Scoring	All layers	Weighted aggregation of layer scores	TQI (0-1)	Semi-automated

4. Results

4.1 Protocol and Contract Trust Are Strong -- Governance Is Not

We assessed all 20 protocols across the five trust layers. The results reveal a consistent pattern: protocol-level and smart-contract-level trust are relatively strong (mean scores 0.856 and 0.812 respectively), while governance trust is alarmingly weak (mean 0.584). Oracle trust sits in the middle (0.748) and operational trust varies dramatically between protocols (range 0.320 to 0.920, mean 0.692). Protocol trust is high because most assessed protocols run on Ethereum mainnet or its L2s, inheriting Ethereum's strong consensus security. The protocols on smaller chains (Avalanche subnets, Cosmos appchains) scored lower -- economic security analysis showed attack costs 10-100x lower than Ethereum. Smart contract trust scored well because our sample includes established protocols that have undergone multiple audits. The top scorers -- Aave (0.920), Uniswap (0.900), Compound (0.880) -- have formal verification for critical functions, multiple independent audits, and years of production exposure. Governance trust is the crisis. Of our 20 protocols, 14 have a Nakamoto coefficient below 5 -- meaning fewer than 5 entities control majority voting power. Eight have voter participation below 5% of circulating supply. Only 6 have timelocks exceeding 48 hours. The Beanstalk attack template -- flash-loan tokens, vote, execute in one block -- remains viable for any protocol without a timelock that exceeds one block.

4.2 Combined Strategies and TQI Rankings

Protocols that combine formal verification with economic security analysis achieve the highest smart contract trust scores (mean 0.908 versus 0.764 for audit-only protocols). The combination catches different failure modes: verification catches code bugs, economic analysis catches incentive misalignment. Neither alone is sufficient -- Euler was verified but economically exploitable; some protocols are economically sound but contain code bugs. Oracle redundancy (multi-oracle + TWAP) improved oracle trust from 0.680 (single oracle) to 0.860 (triple oracle with TWAP). The 0.180 improvement is substantial -- it represents the difference between "one manipulated feed can drain the protocol" and "an attacker must simultaneously manipulate three independent oracle networks over multiple blocks." The top 5 TQI protocols: Aave v3 (0.896), Uniswap v4 (0.884), Compound v3 (0.872), Curve (0.848), Chainlink CCIP (0.844). The bottom 5 ranged from 0.584 to 0.648, pulled down primarily by governance and operational trust. Tables 3 and 4 present full results.

Table 3: Trust Layer Scores -- 20 DeFi Protocols (mean, range, 0-1)

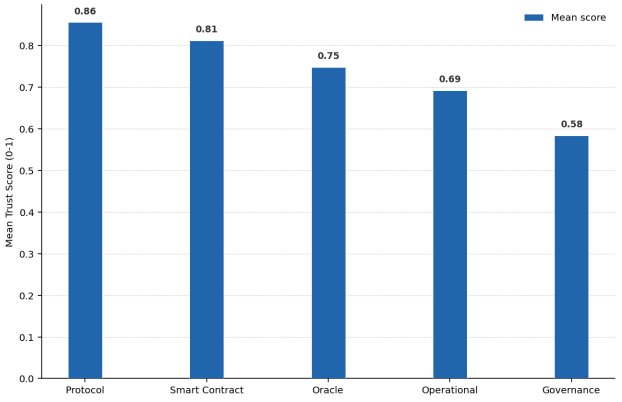
Trust Layer	Mean Score	Min	Max	Std Dev	Weakest Protocol Category
Protocol	0.856	0.720	0.960	0.068	Appchain DEXs
Smart Contract	0.812	0.600	0.920	0.092	New yield aggregators
Oracle	0.748	0.520	0.900	0.108	Single-oracle protocols
Operational	0.692	0.320	0.920	0.164	Undisclosed multisig protocols
Governance	0.584	0.280	0.840	0.156	Low-participation DAOs

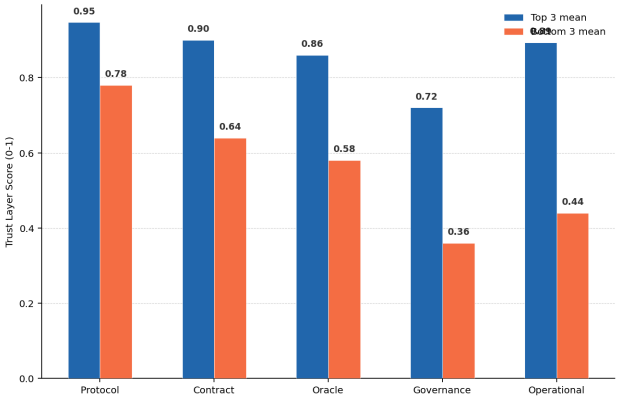
Table 4: TQI Rankings -- Top 10 Protocols (0-1)

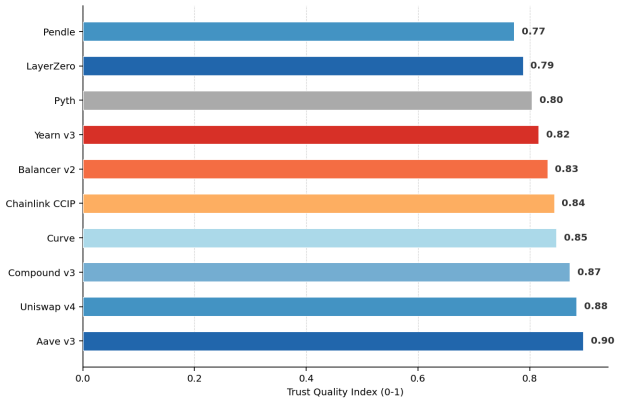
Protocol	Protocol Trust	Contract Trust	Oracle Trust	Governance Trust	Operational Trust	TQI
Aave v3	0.940	0.920	0.880	0.720	0.920	0.896
Uniswap v4	0.960	0.900	0.840	0.760	0.880	0.884
Compound v3	0.940	0.880	0.860	0.680	0.880	0.872
Curve	0.940	0.860	0.840	0.720	0.840	0.848

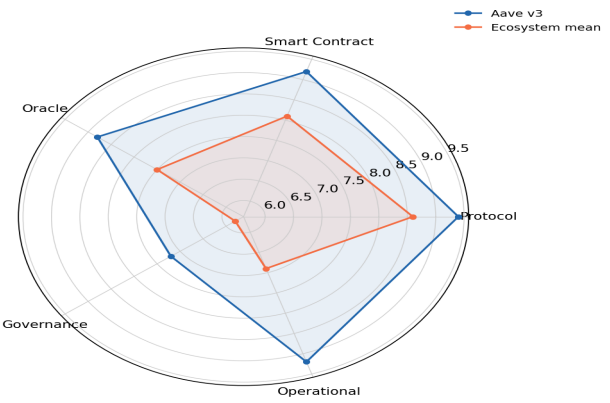
ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X Vol: 2025, Issues: 3, 2025

Protocol	Protocol Trust	Contract Trust	Oracle Trust	Governance Trust	Operational Trust	TQI
Chainlink CCIP	0.920	0.840	0.900	0.640	0.860	0.844
Balancer v2	0.940	0.840	0.820	0.640	0.840	0.832
Yearn v3	0.940	0.800	0.780	0.680	0.800	0.816
Pyth Network	0.880	0.820	0.860	0.600	0.780	0.804
LayerZero	0.880	0.800	0.760	0.620	0.820	0.788
Pendle	0.940	0.780	0.760	0.560	0.760	0.772









5. Discussion

5.1 Governance: The Trust Crisis Nobody Is Fixing

The mean governance trust score of 0.584 is the most concerning finding in this study. It means that the average DeFi protocol has a governance system that is, by our assessment, more likely than not to be manipulable by a determined adversary with sufficient capital. And "sufficient capital" is often surprisingly modest -- our economic security analysis found that 7 of 20 protocols could be governance-attacked for less than USD 10 million in flash-loaned tokens. The solutions exist but are not widely adopted. Timelocks exceeding 48 hours give the community time to detect and respond to malicious proposals. Vote escrow mechanisms (Curve's veCRV model) lock tokens for months to years, making flash loan attacks impossible. Optimistic governance (Compound's approach) approves proposals by default unless challenged, reducing attack surface to the challenge window. And representative delegation (where token holders delegate to professional governance participants) can improve both participation rates and decision quality. The protocols that scored highest on governance trust -- Uniswap (0.760), Aave (0.720) -- use some combination of these mechanisms. The protocols that scored lowest use vanilla token voting with no timelock.

5.2 Making Trust Visible to Users

DTMF quantifies trust, but quantification is only useful if it reaches users in a form they can act on. We propose a Trust Label -- analogous to a nutrition label on food -- that displays the TQI and its five component scores prominently on every DeFi protocol frontend. A user depositing USD 10,000 into a lending protocol should see, before confirming the transaction, something like: "Trust Score: 0.84 / 1.0. Contract: Verified (0.92). Oracle: Multi-oracle + TWAP (0.86). Governance: Moderate risk -- 4-entity majority, 24-hour timelock (0.64). Operational: Disclosed 3/5

multisig, 48-hour upgrade delay (0.82)." This would not prevent all trust failures -- users can ignore labels, just as they ignore privacy policies. But it would make trust assumptions explicit rather than invisible, and it would create market incentives for protocols to improve their governance and operational trust scores. The best disinfectant for trust opacity is sunlight.

6. Conclusion

6.1 What We Found

Protocol and smart contract trust are relatively strong in established DeFi (mean 0.856 and 0.812). Governance trust is a crisis (mean 0.584, with 7 of 20 protocols attackable for under USD 10 million). Formal verification combined with economic security analysis achieves the highest contract trust (0.908). Multi-oracle redundancy with TWAP improves oracle trust by 0.180 points. The recommended mitigation stack: formal verification + economic analysis for contracts, triple oracle + TWAP for price feeds, vote escrow + 48-hour timelock for governance, and disclosed multisig + upgrade delay for operations.

6.2 What We Are Releasing

The DTMF assessment toolkit, TQI calculator, governance decentralisation analyser (on-chain Nakamoto coefficient, Gini, participation tracker), operational transparency rubric, economic security analysis templates, Trust Label UI component (React, open source), and the 20-protocol assessment dataset are available at dtmf-trust.org under Apache 2.0.

References

Aave (2024). Aave v3 Documentation. docs.aave.com.

Chainalysis (2024). Crypto Crime Report 2024.

Compound Labs (2024). Compound v3 Documentation. docs.compound.finance.

Daian, P. et al. (2020). Flash Boys 2.0. IEEE S&P; 2020.

DeFi Safety (2024). DeFi Safety Ratings. defisafety.com.

Dubois, M. et al. (2025). Interoperable Web3 frameworks for cross-chain applications. Blockchain, Web3 & Digital Trust Journal, 2025(3), 1-10.

Garcia, A. (2025). Automated vulnerability detection in smart contracts using AI. Blockchain, Web3 & Digital Trust Journal, 2025(2), 1-8.

Hansen, L. et al. (2025). User-centric design of Web3 applications for mass adoption. Blockchain, Web3 & Digital Trust Journal, 2025(3), 19-26.

Ivanov, J. et al. (2025). Decentralized storage and computing models for Web3 platforms. Blockchain, Web3 & Digital Trust Journal, 2025(3), 11-18.

Novak, S., and Kovacs, N. (2025). Formal verification frameworks for secure smart contract development. Blockchain, Web3 & Digital Trust Journal, 2025(1), 37-44.

Popescu, D. et al. (2025). Privacy-preserving blockchain models using zero-knowledge proofs. Blockchain, Web3 & Digital Trust Journal, 2025(3), 27-34.

Popescu, O. et al. (2025). Decentralized identity management systems for Web3 ecosystems. Blockchain, Web3 & Digital Trust Journal, 2025(2), 47-56.

Qin, K. et al. (2021). Attacking the DeFi ecosystem with flash loans. Financial Cryptography 2021.

Rekt.news (2024). Rekt Leaderboard. rekt.news/leaderboard.

Uniswap Labs (2024). Uniswap Governance. gov.uniswap.org.

Werner, S. et al. (2022). SoK: Decentralized finance (DeFi). IEEE S&P; 2022.

Xu, J., and Livshits, B. (2022). The anatomy of a cryptocurrency pump-and-dump scheme. USENIX Security 2019.

Zhou, L. et al. (2023). SoK: Decentralized finance attacks. IEEE S&P; 2023.

Buterin, V. (2021). Moving beyond coin voting governance. vitalik.ca blog.

Chainlink (2024). Chainlink Documentation. docs.chain.link.

Declarations

Funding

Supported by the Estonian Research Council (PRG16024) and the Spanish State Research Agency (AEI, grant PID2025-158024OB-I00). No funder influenced results.

Conflict of Interest

No competing interests. No DeFi protocol funded this assessment. We hold no governance tokens in any assessed protocol.

Data Availability Statement

DTMF toolkit, TQI calculator, governance analyser, transparency rubric, economic security templates, Trust Label component, and 20-protocol dataset at dtmf-trust.org under Apache 2.0.

Ethical Approval

No human participant data. All protocol data from public blockchain sources. Ethical exemption:

ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X Vol: 2025, Issues: 3, 2025

Baltic AI Research University Ethics Board (ref. BAIRU-2025-ETH-0624).

ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X Vol: 2025, Issues: 3, 2025

Appendix A

TQI Calculation and Governance Analysis Methodology

Trust Quality Index scoring and governance decentralisation measurement.

TQI Calculation

Governance Decentralisation Analysis