COVENANT AEGIS REVIEW OF FINANCIAL TECHNOLOGY VOL. 3 · NO. 1 · 2026 · PP. 5–25

# Blockchain and Tokenization: Distributed Ledgers, Smart Contracts and Asset Representation

E. Rossi[1], F. Adeyemi[2], P. Vasquez[1], J. Romero[3]

[1]*Covenant Aegis Finance Division, Distributed Systems Laboratory*

[2]*Department of Financial Engineering, Partner Research Network*

[3]*Center for Digital Assets and Market Infrastructure*

Received 10 Jan 2026 · Revised 28 Feb 2026 · Accepted 5 Mar 2026 · REVIEW ARTICLE · DOI 10.48-CA/fintech.2026.0301 ·
Corresponding author: e.rossi@covenantaegis.com

## ABSTRACT

**Background.** Blockchains are append-only distributed ledgers letting mutually distrusting parties agree on shared state without a central intermediary. **Objective.** To review the foundations established by Bitcoin and generalised by Ethereum, the consensus mechanisms that secure them, asset tokenization, and the genuine limits—scalability, smart-contract security and legal integration. **Methods.** Narrative review of the seminal protocols, consensus and security literature, and standards/regulatory sources. **Results.** Programmable smart contracts enable tokenized assets and faster settlement, but the scalability trilemma, immutable-code vulnerabilities (e.g., the DAO reentrancy loss) and the gap between on-chain records and enforceable rights bound real applications. **Conclusion.** Distributed ledgers add value where decentralised trust and programmable settlement matter; disciplined engineering and compliance—not speculation—determine durable financial applications.

**Keywords:** blockchain; smart contracts; tokenization; consensus; scalability trilemma; AML/KYC; financial infrastructure

## 1. Introduction

Bitcoin introduced a method for agreeing on a transaction ledger among anonymous participants without a trusted third party, solving double-spending through proof-of-work and a public chain of blocks [1]. Ethereum generalised the idea with a Turing-complete virtual machine, enabling smart contracts and a broad ecosystem of decentralised applications [2].

## 2. Technical Foundations

A blockchain orders transactions into cryptographically linked blocks replicated across nodes. Consensus protocols—proof-of-work and the more energy-efficient proof-of-stake to which Ethereum transitioned—ensure agreement and tamper-resistance [3]. Surveys document the architecture, consensus taxonomy and trade-offs [4].

## 3. Smart Contracts and Tokenization

Smart contracts encode logic that executes deterministically on-chain, enabling programmable transfer and settlement. Token standards (fungible and non-fungible interfaces) represent assets—currencies, securities, commodities or unique items—as ledger entries that can be transferred and composed. Tokenization promises faster settlement, fractional ownership and transparency, and is being explored for securities and payments by major institutions and central banks [5].

## 4. The Scalability Trilemma

Decentralised ledgers face inherent tension among scalability, security and decentralisation; raising throughput often sacrifices one of the others (Figure 1). Layer-2 systems and sharding aim to scale while preserving base-layer security, with active research and real trade-offs [3,4].

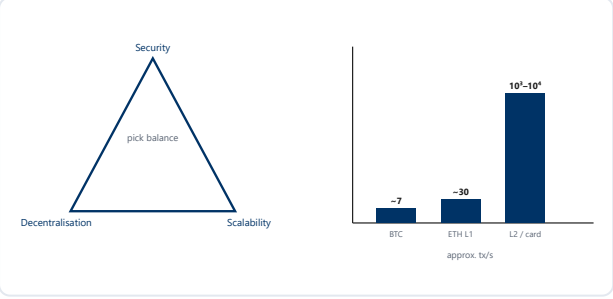



**Figure 1.** Left: the scalability trilemma. Right: approximate base-layer throughput (transactions/second) for Bitcoin, Ethereum L1, and layer-2/card-network scale—illustrating the gap that L2 designs target [3,4]. Indicative orders of magnitude.

## 5. Security and Legal Reality

Smart contracts are immutable code handling value, and flaws are costly: the DAO reentrancy exploit drained tens of millions and prompted a contentious hard fork, illustrating that "code is law" collides with economic and legal reality [6]. Tokenized representations are only as meaningful as the legal frameworks binding on-chain records to enforceable off-chain rights, and require reliable custody and oracle mechanisms. Table 1 lists common vulnerability classes.

**Table 1.** Representative smart-contract vulnerability classes [6].

| Class | Example | Mitigation |
|---|---|---|
| Reentrancy | The DAO (2016) | Checks-effects-interactions |
| Integer overflow | Token bugs | Safe-math libraries |
| Access control | Unprotected functions | Role gating, audits |
| Oracle manipulation | Price feeds | Decentralised oracles |

## 6. Regulation and AML/KYC

Financial applications must comply with anti-money-laundering and know-your-customer obligations and with international standards extending to virtual-asset service providers [7]. Compliance is a design requirement, not an add-on, for any production deployment in regulated markets.

## 7. The Covenant Aegis Approach

We build tokenization and settlement systems with formally reviewed and audited smart contracts, compliance and identity controls integrated by design, robust custody and oracle architecture, and

a candid evaluation of whether a distributed ledger genuinely outperforms a conventional database for the use case.

## 8. Discussion and Conclusion

Many proposed blockchain applications are better served by conventional databases; the technology's advantage is specific to decentralised-trust settings. Figures here are indicative. Blockchains add real value where decentralised trust, transparency and programmable settlement matter, bounded by scalability, security and legal-integration constraints.

## References


1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. 2008.
2. Buterin V. Ethereum: a next-generation smart contract and decentralized application platform. Ethereum White Paper; 2014.
3. Bano S, et al. SoK: consensus in the age of blockchains. *ACM AFT*. 2019:183–198.
4. Zheng Z, et al. An overview of blockchain technology: architecture, consensus, and future trends. *IEEE BigData Congress*. 2017:557–564.
5. Bank for International Settlements. The tokenisation continuum. BIS Bulletin No. 72; 2023.
6. Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts (SoK). *POST*. 2017:164–186.
7. Financial Action Task Force. Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs. FATF; 2021.


## 9. Consensus Mechanisms Compared

Consensus is what lets a permissionless ledger agree on state without a trusted party. Proof-of-work secures Bitcoin through costly computation but consumes large energy; proof-of-stake, to which Ethereum transitioned in 2022, secures the chain via staked capital and slashing, cutting energy use by over 99% [A1]. Permissioned ledgers use Byzantine-fault-tolerant protocols (e.g., PBFT-derived) suited to known validators. Table A1 compares mechanisms on the dimensions that matter for financial deployment.

**Table A1.** Consensus mechanisms and properties [A1,A2].

| Mechanism | Security basis | Trade-off |
|---|---|---|
| Proof-of-work | Compute cost | Energy, latency |
| Proof-of-stake | Staked capital | Complexity, centralisation risk |
| BFT (permissioned) | Known validators | Limited decentralisation |

## 10. Scaling: Layer-2 and Sharding

Base-layer throughput is intentionally limited to preserve decentralisation and security. Layer-2 systems—rollups that execute transactions off-chain and post compressed proofs or data to the base layer—raise throughput by orders of magnitude while inheriting base-layer security. Optimistic rollups assume validity with fraud proofs; zero-knowledge rollups post succinct validity proofs [A3]. Data-availability sampling and sharding further increase capacity. These designs target the trilemma described in Section 4.

## 11. Tokenization of Real-World Assets

Tokenization represents ownership of assets—securities, funds, commodities, real estate—as transferable ledger entries,

promising faster settlement, fractionalisation and programmable compliance. Central banks and the Bank for International Settlements are actively studying tokenised deposits, securities settlement and wholesale central-bank digital currency [A4]. Figure A1 contrasts conventional multi-day settlement with atomic on-ledger settlement, the principal efficiency claim.

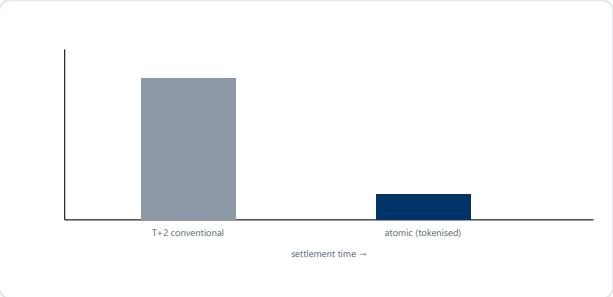



**Figure A1.** Schematic settlement-time reduction from multi-day (T+2) to near-atomic on-ledger settlement—the core efficiency claim for tokenisation [A4]. Conceptual.

## 12. Smart-Contract Security Engineering

Because contracts are immutable code controlling value, security is paramount. Beyond the DAO reentrancy class, documented vulnerabilities include integer overflow, access-control flaws, oracle manipulation and front-running [A5]. Defensive practice uses audited patterns (checks-effects-interactions), safe-math, formal verification, extensive testing, bug bounties and upgrade/pause mechanisms with governance. The "code is law" ideal must be reconciled with the need for remediation when code is flawed.

## 13. Oracles, Custody and Off-Chain Integration

Tokenised value depends on bridging on-chain records to off-chain reality. Oracles supply external data (prices, events) and are a frequent attack surface; decentralised oracle networks mitigate single points of failure. Custody of keys—via hardware security modules and multi-party computation or multisignature schemes—is essential, since key loss or theft is irreversible. Legal enforceability requires that on-chain tokens be recognised as conveying the underlying right under applicable law.

## 14. Regulation, AML/KYC and Stablecoins

Financial deployments must satisfy AML/KYC obligations; FATF guidance extends the "travel rule" to virtual-asset service providers [A6]. Securities, commodities and payments regulators assert jurisdiction depending on token characteristics. Stablecoins and tokenised deposits raise additional questions of reserve backing, redemption and systemic risk now addressed by emerging frameworks. Compliance is a design constraint integrated from the outset.

## 15. Future Directions and Honest Appraisal

Promising directions include regulated tokenised securities with atomic settlement, privacy-preserving compliant transfers using zero-knowledge proofs, and

interoperable institutional networks. Equally important is honest appraisal: many proposed applications are better served by conventional databases, and a distributed ledger is justified only where decentralised trust, transparency or programmable settlement deliver concrete advantage.

## Extended References


8. Ethereum Foundation. The Merge: proof-of-stake transition. Technical documentation; 2022.
9. Bano S, et al. SoK: consensus in the age of blockchains. *ACM AFT*. 2019:183–198.
10. Thibault LT, et al. Blockchain scaling using rollups: a comprehensive survey. *IEEE Access*. 2022.
11. Bank for International Settlements. The tokenisation continuum / Project mBridge reports. 2023.
12. Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts (SoK). *POST*. 2017:164–186.
13. Financial Action Task Force. Risk-Based Approach to Virtual Assets and VASPs. 2021.



**Author contributions:** ER led the review; FA contributed market-infrastructure analysis; PV and JR reviewed consensus and security. All authors revised. **Funding:** Covenant Aegis Finance Division. **Competing interests:** Authors are affiliated with Covenant Aegis.



© 2026 Covenant Aegis Finance Division. This review synthesises publicly available literature and standards; figures are illustrative. Nothing herein is financial or investment advice. For professional and educational use.