BLOCKCHAIN CANON

2026-03-18

Dexter Hadley, MD/PhD

Hadley Lab CANONIC

Abstract

Example

Contents

Claims about blockchain security MUST specify the consensus mechanism and its guarantees.

Example: Proof of Work (PoW) computational puzzle solving, 51% attack threshold, energy-intensive (Bitcoin: ~150 TWh/year). Proof of Stake (PoS) validator selection weighted by stake, 33% BFT threshold (Ethereum post-Merge, 2022). Delegated PoS (DPoS) elected block producers (EOS: 21 BPs). PBFT (Practical Byzantine Fault Tolerance) deterministic finality, 3f+1 nodes tolerate f faults, O(nˆ2) message complexity. Finality: probabilistic (PoW deeper = more secure, 6 confirmations standard) vs deterministic (PBFT immediate but requires known validator set). Fork resolution: longest chain (PoW), finalized checkpoints (PoS/Casper).

0.1 2. Smart Contract Governance

Smart contracts MUST be audited, tested, and governed with explicit upgrade and emergency procedures.

Example: Solidity (Ethereum), Vyper (security-focused), Move (Aptos/Sui), Rust (Solana). Formal verification: mathematical proof that code matches specification (tools: Certora, Halmos, K Framework). Audit standards: minimum two independent audits before mainnet deployment, bug bounty programs (Immunefi: $150M+ paid). Upgradeability patterns: transparent proxy (EIP-1967), UUPS (EIP-1822), diamond/multi-facet (EIP-2535). Emergency procedures: circuit breakers (pause functionality), timelocks (governance delay), multisig requirements (Gnosis Safe). Common vulnerabilities: reentrancy (DAO hack, 2016, $60M), flash loan attacks, oracle manipulation, front-running/MEV.

0.2 3. Regulatory Landscape

Digital asset operations MUST comply with applicable securities, commodities, and money trans-

mission regulations.

Example: SEC Howey test determines security classification. SAB 121 (2022) required custodians to record crypto as liabilities (rescinded by SAB 122, 2025). CFTC Bitcoin and Ether classified as commodities. State money transmitter licensing 49 states + DC, each with separate requirements. New York BitLicense (2015) most comprehensive state regime. MiCA (Markets in Crypto-Assets, EU 2024) CASPs (Crypto-Asset Service Providers) require authorization, stablecoin issuers need e-money license or credit institution status. Travel Rule (FATF Recommendation 16) VASPs must share originator/beneficiary information for transfers above $1K (US) or EUR 1,000 (EU).

0.3 4. Tokenomics

Token economic models MUST disclose supply mechanics, distribution, governance rights, and regulatory classification.

Example: Token standards: ERC-20 (fungible), ERC-721 (NFT), ERC-1155 (multi-token). Token classification: utility (access to platform service), security (investment contract), governance (voting rights), payment (medium of exchange). Each classification has different regulatory treatment. Vesting schedules: cliff (initial lock period), linear (gradual release), milestone-based. Treasury management: diversification, on-chain governance votes for spending. Tokenomics design: supply cap vs inflationary, burn mechanisms, staking rewards, liquidity mining incentives. Dilution analysis and token velocity economics.

0.4 5. DeFi Protocols

Decentralized finance protocols MUST document risk vectors, economic assumptions, and failure modes.

Example: AMM (Automated Market Maker) constant product formula (x*y=k, Uniswap), concentrated liquidity (Uniswap v3). Lending/borrowing: overcollateralized (Aave, Compound), isolated markets, liquidation mechanics. Oracle design: Chainlink (decentralized oracle network), TWAP (time-weighted average price), Uniswap v3 oracle. MEV (Maximal Extractable Value) searchers, builders, proposers extract value through transaction ordering. Flash loans uncollateralized loans within single transaction (Aave, dYdX). Composability risks: protocol dependencies create systemic risk failure in one protocol cascades through DeFi stack.

0.5 6. Identity & Privacy

Blockchain identity systems MUST balance verifiability with privacy rights.

Example: DID (Decentralized Identifiers, W3C) self-sovereign identity, no central authority. Verifiable Credentials (W3C) cryptographically provable claims about identity attributes. Zero-knowledge proofs: zk-SNARKs (Zcash, Tornado Cash), zk-STARKs (StarkNet), enable verification without revealing underlying data. GDPR tension: immutable ledger vs right to erasure (Art. 17) off-chain storage with on-chain hashes is common mitigation. Privacy protocols: Aztec (encrypted transactions on Ethereum), Tornado Cash (OFAC sanctioned 2022 demonstrates regulatory risk of privacy tools). Soulbound tokens (SBTs) non-transferable tokens for reputation and credentials.

---

1. Constraints

```
MUST:     Cite specific protocol, standard, or regulat
MUST:     Distinguish between L1/L2/sidechain security
MUST NOT: Present token mechanics without regulatory c
```

BLOCKCHAIN | CANON | REGULATORY