Bitcoin Whitepaper Explained

Wielfried Zouantcha | August 8, 2026

Canonical: https://www.zouantcha.com/blog/bitcoin-whitepaper-explained

This note explains Satoshi Nakamoto’s 2008 paper "Bitcoin: A Peer-to-Peer Electronic Cash System" for readers who want the academic structure, not a trading pitch.

Problem. Internet payments usually rely on trusted intermediaries. That model enables reversible disputes and raises the minimum practical transaction size. The paper asks whether electronic payments can rest on cryptographic proof instead of institutional trust.

Electronic coins as signature chains. A coin is a chain of digital signatures. Ownership transfers by signing a hash of the previous transaction and the next owner’s public key. Signatures prove a chain of custody, but they do not by themselves prevent double-spending.

Double-spending without a mint. A central mint can reject second spends, but reintroduces a trusted party. The paper’s alternative is a public history: transactions are broadcast, and participants converge on a single ordered ledger of which spend came first.

Timestamp server and proof-of-work. Blocks hash transactions (and the previous block) into a chain. Proof-of-work, in the spirit of Hashcash, makes rewriting history expensive: changing a block requires redoing its work and the work of every block after it. Honest majority hash power makes the honest chain grow fastest.

Network and incentives. Nodes collect transactions, mine blocks, and extend the longest valid chain. The first transaction in a block mints a coinbase reward to the miner; fees can later replace issuance. Incentives align attackers toward earning rewards rather than destroying the system’s value.

Light clients and privacy. Simplified Payment Verification (SPV) checks Merkle proofs against block headers rather than full history. Privacy is partial: keys can stay pseudonymous, but multi-input transactions and address reuse can still link activity.

Security model. An attacker who rewrites recent history faces a race against the honest chain. Under honest majority, the probability of catching up from z blocks behind falls exponentially in z. Invalid transactions are still rejected by honest nodes even if an attacker mines blocks.

How to read the original. The source paper is short. Read abstract and sections 1-4 for the design, then incentives, Merkle pruning, SPV, and the calculations appendix for the security argument.

Canonical URL for this explanation:
https://www.zouantcha.com/blog/bitcoin-whitepaper-explained

Primary source (Nakamoto, 2008): https://bitcoin.org/bitcoin.pdf

Also on this site: https://www.zouantcha.com/blog/bitcoin-whitepaper

References: Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf; Back, A. (2002). Hashcash; Dai, W. (1998). b-money; Haber & Stornetta (1991). How to time-stamp a digital document; Merkle, R. (1980). Protocols for public key cryptosystems.