Bitcoin v0.2: Revelation Edition

A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto

Abstract

A purely peer-to-peer version of electronic cash allows online payments to be sent directly from one party to another without reliance on trust, intermediaries, or institutional authority. Digital signatures provide a foundation of ownership, but the system's strength depends on preventing double-spending without a trusted third party.

Bitcoin v0.2: Revelation Edition refines the original design by emphasizing consensus as *revelation through computation*. Transactions are timestamped by hashing them into an ever-growing chain of proof-of-work, forming an immutable historical record. This chain cannot be altered without redoing the accumulated work, making history economically expensive to rewrite.

The longest chain represents not merely chronological order, but collective agreement expressed through time and energy. As long as the majority of computational power is controlled by honest nodes, the network continues to reveal the correct sequence of events and outpaces any attacker.

The network requires minimal structure. Messages are broadcast on a best-effort basis. Nodes may leave and rejoin freely, accepting the chain with the most accumulated proof-of-work as the revealed truth of what occurred while they were absent.

1. Revelation

In traditional systems, truth is declared by authority.
In Bitcoin, truth is revealed by work.

Commerce on the Internet has relied on trusted intermediaries to establish what happened, who owns what, and which transactions are final. This reliance introduces reversibility, mediation costs, surveillance, and systemic fragility.

Bitcoin replaces institutional trust with cryptographic revelation. Events are not declared final by decree, but by the accumulation of irreversible computational effort. Time is transformed into weight. History becomes measurable.

What is revealed is not identity, but order.

2. Transactions as Immutable Witness

An electronic coin is a chain of digital signatures. Each transaction witnesses the previous one by signing its hash and transferring ownership forward. The chain of signatures forms a verifiable lineage that cannot be forged without possession of the corresponding private keys.

The problem is not validation, but uniqueness. Without a global view, the same coin could be spent more than once.

To reveal which transaction occurred first, all transactions must be publicly announced and a single history must emerge from decentralized agreement. The earliest transaction, once buried beneath sufficient proof-of-work, becomes the only one that matters. Later attempts are rendered irrelevant by revelation through consensus.

3. The Timestamp Revelation

The system introduces a distributed timestamp server. Transactions are grouped into blocks, hashed, and broadcast. Each block includes the hash of the previous block, forming an unbroken chain.

This chain is a ledger of time.

Once revealed, a timestamped event cannot be altered without redoing all subsequent work. Each new block reinforces the truth of all blocks before it.

4. Proof-of-Work: Time Made Physical

Proof-of-work converts time and energy into consensus.

Nodes compete to find a nonce that produces a block hash meeting a difficulty target. The cost of producing this proof is high; the cost of verifying it is trivial. This asymmetry ensures that honesty dominates deception.

Proof-of-work replaces identity-based voting with energy-based voting. One unit of work equals one unit of voice. The longest chain represents the greatest revealed commitment of resources.

Difficulty adjusts automatically to preserve a consistent rhythm of revelation, independent of hardware improvements or changes in participation.

5. Network of Unnamed Witnesses

The network operates without hierarchy or identity:

- Transactions are broadcast.
- Nodes assemble blocks.
- Nodes compete to reveal the next proof-of-work.
- Valid blocks are broadcast and accepted.
- Nodes extend the chain with the most accumulated work.

Temporary disagreement resolves naturally. When competing histories arise, the chain with the greatest accumulated proof-of-work reveals itself as truth.

Nodes that fall behind may rejoin at any time, accepting the revealed history without negotiation or trust.

6. Incentive: Reward for Revelation

The first transaction in each block reveals new coins into existence. This reward incentivizes participation and distributes currency without authority.

As issuance declines, transaction fees sustain the system. Eventually, revelation is funded entirely by those who use it.

A rational attacker finds honesty more profitable than deception. To undermine the system is to undermine the value of one's own revealed wealth.

7. Forgetting Without Losing Truth

Old transaction data may be discarded once buried beneath sufficient proof-of-work. Merkle trees allow blocks to retain their integrity while shedding historical detail.

Only block headers, the skeleton of time, must remain. Revelation is preserved even as memory is pruned.

8. Lightweight Revelation

Users may verify payments without witnessing everything. By holding only block headers and Merkle proofs, a user can confirm that a transaction has been revealed and accepted by the network.

Each additional block deepens certainty. Revelation compounds.

9. Value as Flow

Transactions may combine and split value freely. Inputs merge past revelations; outputs project new ones. Change returns naturally to the sender.

There is no need to reconstruct the entire past. The present state, derived from revealed history, is sufficient.

10. Privacy Through Absence

Identities are never revealed, only cryptographic keys. Transactions are public, but ownership remains pseudonymous.

Each transaction may use a new key, breaking narrative continuity. What is revealed is that value moved, not who moved it.

11. Probability and Inevitability

An attacker racing against the honest chain faces exponentially diminishing odds. Each confirmed block deepens the revealed truth.

Time favors honesty. Probability converges toward certainty.

12. Conclusion: Revelation Without Authority

Bitcoin v0.2: Revelation Edition describes a system where truth emerges from computation, not control.

No rulers.
No identities.
No permissions.

Only time, energy, and mathematics.

History is not written.
It is revealed.