Nakamoto: A Mobile‑Native, ZK‑Verified Monetary Network

White Paper — Version 1.0

Date: 2025-08-09

This document presents the Nakamoto protocol: a modern, Bitcoin-inspired Layer-1 designed for phones, secured by validity proofs and data-availability sampling, with a fixed 21 million supply and two-year halvings.

Abstract

Nakamoto is a minimal, sound-money blockchain for a mobile world. It preserves the monetary discipline of Bitcoin—fixed cap of 21 million coins and a deterministic halving schedule—while adopting modern cryptography and networks to achieve fast finality, low fees, and energy-light participation.

The protocol combines a rotating, staked validator set for block proposal with two cryptographic assurances: (1) zk-validity proofs for every block, so clients need not re-execute transactions; and (2) data-availability sampling (DAS) performed by a global crowd of smartphones.

Economic finality is granted only when the block has both BFT commit signatures from validators and a quorum of randomized mobile attestations certifying proof correctness and data availability.

The result is a payments-focused Layer-1 that anyone can help secure from a phone, without mining hardware, while maintaining simplicity comparable to Bitcoin's base layer.

1. Motivation

Bitcoin demonstrated that open monetary systems can be credibly neutral and resilient. It also revealed practical challenges: proof-of-work centralizes around specialized hardware, confirmation latency is minutes, and verifying from resource-constrained devices is costly over time.

Meanwhile, cryptography and networking advanced: succinct zero-knowledge proofs allow fast client verification; BFT protocols offer deterministic finality; mobile networks and processors matured; data-availability sampling provides scalable assurance against withholding.

Nakamoto asks: if a disciplined monetary network were designed today, for billions of phones, how simple and verifiable could it be—without sacrificing decentralization or security assumptions?

2. Design Principles

• Monetary discipline: fixed 21,000,000 supply; halving every two years by height.

• Minimal L1: payments only, plus native staking operations; no general-purpose smart contracts.

• Phone-first security: anyone can verify and contribute from a smartphone; rewards exist for verification and availability work.

• Validity over work: correctness enforced by zk-proofs; safety is cryptographic, not probabilistic hashpower.

• Availability by the crowd: data withholding is detectable via sampling by many independent devices.

• Decentralization in practice: avoid specialized hardware and excessive operator complexity.

• Ossification path: parameters are adjustable early on, but the protocol tends toward stability.

3. System Overview

Nakamoto is a UTXO-based Layer-1 with 10-second target blocks and typical finality under 20 seconds.
A small validator set (64–128) proposes blocks and signs BFT quorum certificates. Each block includes a zk-validity proof attesting to the correctness of state transitions: transaction signatures, UTXO spends and creates, fee burn, and issuance per the halving schedule.
In parallel, smartphones verify the proof and perform DAS over the erasure-coded block payload. The protocol recognizes a block as economically final when both conditions hold: (a) ≥2/3 validator signatures on the header; and (b) a randomized mobile committee reaches a super-majority of positive attestations for proof correctness and data availability.
No general smart contracts are supported at L1; staking actions are protocol opcodes.
Expressivity belongs to higher layers that can inherit Nakamoto's proofs and availability guarantees.

4. Monetary Policy

• Maximum supply: 21,000,000 units.

• Block subsidy: starts at 50 units (in base-subdivisions) and halves every two years. Halvings are height-based.

• Fees: a base fee is burned; users may add an optional tip to the proposer. The base fee adjusts toward a target block fullness, stabilizing fees.

- Distribution: the network avoids hardware races by rewarding verification work (mobile attestations) and validator participation instead of mining. An ecosystem fund (single-digit percent within the cap) vests linearly and is transparent.

5. Transaction Model

Nakamoto uses a conservative UTXO model with standard pay-to-public-key-hash style outputs and Schnorr signatures (BIP-340) over secp256k1.

Transactions are simple: inputs reference existing UTXOs; outputs create new ones; fees are the residual. A small set of protocol-native staking operations—bond, unbond, delegate, slash—allow users to participate in consensus without introducing a general virtual machine.

This model keeps client logic compact, proofs small, and surface area for consensus bugs minimal.

6. Consensus and Finality

Validators post stake to join the candidate set. For each epoch, a verifiable random function (VRF) selects an active set (e.g., 96 validators). Blocks proceed through a HotStuff-style BFT pipeline (propose, prevote, precommit), producing a quorum certificate (QC) when ≥2/3 signatures attest the header.

Economic finality for users adds a second, crowd-sourced requirement: the mobile Proof-of-Verification (PoV) quorum (Section 7) must confirm validity and availability.

This dual condition—cryptographic validity with BFT safety and mass availability attestations—yields deterministic, fast confirmations without proof-of-work energy expenditure.

7. Proof- of- Verification (PoV) by Smartphones

To democratize participation, Nakamoto turns verification into a first-class, rewarded activity. For each block, a randomized committee of smartphones is derived from a VRF beacon. Any device holding a winning ticket may earn rewards by:

1) Verifying the zk-proof in milliseconds;
2) Sampling k random chunks from the erasure-coded block data; and
3) Broadcasting a signed attestation summarizing proof correctness and chunk availability.

A block becomes economically final after a super-majority of the scheduled PoV committee attests positively and the validator QC exists. Attestation rewards—paid from issuance and fees—flow to devices proportionally to valid participation.

This replaces “who has the biggest miner?” with “who verifies honestly?” and scales with the number of phones, not the number of specialized rigs.

8. Data Availability Sampling (DAS)

Each block's payload is erasure-coded into n chunks such that any m suffice to reconstruct. The header commits to the Merkle root of chunk hashes.

Phones independently request random chunks from multiple peers. Under mild assumptions on peer diversity, withholding is detected with high probability if the proposer fails to publish data. The BFT layer refuses to finalize when PoV sampling indicates insufficient availability; proposers that attempt withholding are penalized.

DAS shifts availability guarantees from a few archival nodes to a broad crowd, aligning with mobile reality and keeping verification lightweight.

9. Zero- Knowledge Validity Proofs

Every block carries a succinct proof attesting that applying the contained transactions to the previous state yields the new state and respects protocol rules: UTXO conservation, signature validity, fee burn, and subsidy schedule.

The MVP uses a SNARK system with small proofs and fast verification on phones; a STARK-based path can be added later to remove trusted setup. Circuits are intentionally narrow and stable to enable early ossification.

The proof eliminates entire classes of consensus faults: even a colluding validator majority cannot create an invalid block that clients will accept, since invalid state transitions fail verification on end-user devices.

10. Networking and Mobile Reality

The peer-to-peer layer uses modern transports (e.g., QUIC) and relays to traverse NAT. Gossip is topic-based: blocks, transactions, attestations, and data chunks.

Mobile clients are stateless: they track headers, proofs, and minimal UTXO witnesses. They sync quickly from cold start without downloading historical bodies.

Low-power modes batch verifications, prefer Wi-Fi, and degrade sampling frequency when battery is low, preserving device usability while maintaining network security at population scale.

11. Security Model

Assumptions:

- Standard cryptographic assumptions for Schnorr signatures, hash functions, and the SNARK system in use.
- Less than one-third of the validator voting power is Byzantine within a finality round.
- A randomized, Sybil-resistant subset of phones participates in PoV each block (enforced via VRF gating, rate limits, and optional small bonding).

Threats and Mitigations:

- Invalid blocks: blocked by zk-verification on every client.

- Data withholding: detected by DAS; BFT withholds finality; proposers penalized.
- Committee Sybil: randomized tickets + per-device caps; optional small bond for attesters.
- Network eclipse: relays, diverse peers, and peer-scoring reduce isolation risk.
- Key compromise on mobile: hardware-backed keys and rate-limited signing.

By splitting safety between validator BFT and mass phone attestations, Nakamoto resists both small cartel capture and data availability failures.

12. Incentives and Fairness

Nakamoto avoids hardware-based barriers to entry. Rewards accrue to two roles:

- Validators: stake, propose, vote; earn a share of the block reward and tips.
- Attesters: verify and sample; earn rewards proportional to valid attestations.

Fees are predictable due to a simple base-fee mechanism with burn. The monetary policy is transparent and front-loaded via two-year halvings, echoing early Bitcoin while reaching steady state sooner. Over time, reliance shifts from issuance to fees, aligning incentives with actual network use.

13. Governance and Upgrade Path

Protocol changes are rare and conservative. Early parameters (e.g., committee size, sampling rate) may be tuned via on-chain proposals subject to long timelocks and super-majority thresholds.

Consensus or cryptographic upgrades require staged releases, public review, and explicit activation windows. The long-term goal is ossification: a stable base layer whose rules change only with overwhelming consensus and ample notice.

14. Related Work and Positioning

Nakamoto is inspired by Bitcoin’s monetary minimalism and by advances in succinct proofs and BFT consensus. It differs from proof-of-work chains by eliminating hash-based leader election, and from smart-contract platforms by deliberately limiting base-layer expressivity to keep verification cheap and secure on phones.

Its novelty lies in elevating **verification**—not only validation by validators, but real end-user verification and availability sampling—to a rewarded, consensus-relevant role.

15. Limitations and Future Work

- Trusted setup (if SNARK): mitigated by multi-party ceremonies; a STARK path is on the roadmap.

- Mobile background constraints: OS limitations may restrict continuous participation; batching and push-based wakeups alleviate this.

- Expressivity: absence of general smart contracts at L1 shifts complexity to L2s; standardized bridges and proof aggregation for L2s are part of future work.

- Prover decentralization: initial centralized provers give way to a marketplace where independent operators compete to generate proofs under open verifiable APIs.

16. Conclusion

Nakamoto proposes a monetary network for the age of smartphones: simple like Bitcoin where it matters, modern where it counts.
Validity proofs make correctness cheap to check. Data-availability sampling spreads assurance across a global crowd. A modest validator set provides liveness and ordering without specialized hardware races.
With a fixed 21 million supply and two-year halvings, Nakamoto keeps the social contract that made Bitcoin credible, while delivering faster finality, lower fees, and broader participation. The network's guiding idea is straightforward: in a decentralized system, the more people who can verify, the stronger it becomes.

Acknowledgments

We acknowledge the foundational work of Satoshi Nakamoto, as well as the communities advancing zero-knowledge proofs, data-availability sampling, and BFT consensus. This paper stands on their shoulders.

References

- Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
- Byzantine Fault Tolerance and HotStuff literature
- Succinct zero-knowledge proof systems (SNARKs and STARKs)
- Data Availability Sampling research
- VRFs and randomness beacons

Figures & Diagrams

The following diagrams illustrate key aspects of the Nakamoto protocol. These are placeholders—final versions should be rendered with professional diagramming tools (e.g., draw.io, Figma) and embedded as images in the PDF/print version.

Figure 1: High-Level System Architecture

Description: Shows validator set, smartphone PoV participants, prover infrastructure, peer-to-peer network overlay.

Figure 2: Block Structure

Description: Annotated diagram of the block header and body, including zk-proof, DA commitment, UTXO delta root, and attestation root.

Figure 3: Proof-of-Verification Workflow

Description: Sequence diagram from block proposal → zk verification by phones → DAS sampling → attestation → economic finality.

Formal Probability Model for Data Availability Sampling

Let n = total number of erasure-coded chunks per block, m = minimum chunks required to reconstruct (m < n), and k = number of chunks sampled by each device.

If the proposer withholds h chunks, the probability that a single device detects withholding is:

P_detect_single = 1 - C(n-h, k) / C(n, k)

Assuming independent sampling by c devices, the probability that withholding is undetected by all devices is:

P_fail = (1 - P_detect_single)^c

For example, with n=256, m=128, k=50, h=40 (15.6% withheld), and c=500 devices, P_fail ≈ 1.2 × 10^-55 — effectively zero.

Economic Model Overview

Let R_total be the per-block reward (subsidy + fee share pool). The split is:

R_validators = α * R_total

R_attesters = β * R_total

R_ecosystem = γ * R_total

where α = 0.50, β = 0.40, γ = 0.10.

Validator yield per epoch:

Y_validator = (R_validators / N_active) * (blocks_epoch / stake_amount)

Attester yield per epoch:

Y_attester = (R_attesters / C_committee) * (valid_attestations / max_attestations)

Here N_active = active validator count, C_committee = committee size per block.

Over time, as subsidy S(h) decays (S0 halving every 2 years), fees F(h) must rise to maintain similar yields:

R_total(h) = S(h) + F(h)

Simulations suggest with modest on-chain activity (~2 TPS average), fees can sustain rewards post-halving schedule without inflationary tail.

Deployment Path

Phase 0 – Spec Finalization: Publish white paper, finalize protocol constants, run public design review.
Phase 1 – Devnet: Centralized prover, limited validator set, faucet, block explorer.
Phase 2 – Testnet: Public validator onboarding, incentivized PoV rewards, chaos testing for DAS withholding detection.
Phase 3 – Mainnet Beta: Fully decentralized validator set, multi-prover support, rewards live.
Phase 4 – Mainnet 1.0: Governance timelocks activated, parameters stabilized, circuit freeze for zk-proofs.

Illustrative Diagrams (Embedded)

Figure 1: High-Level System Architecture

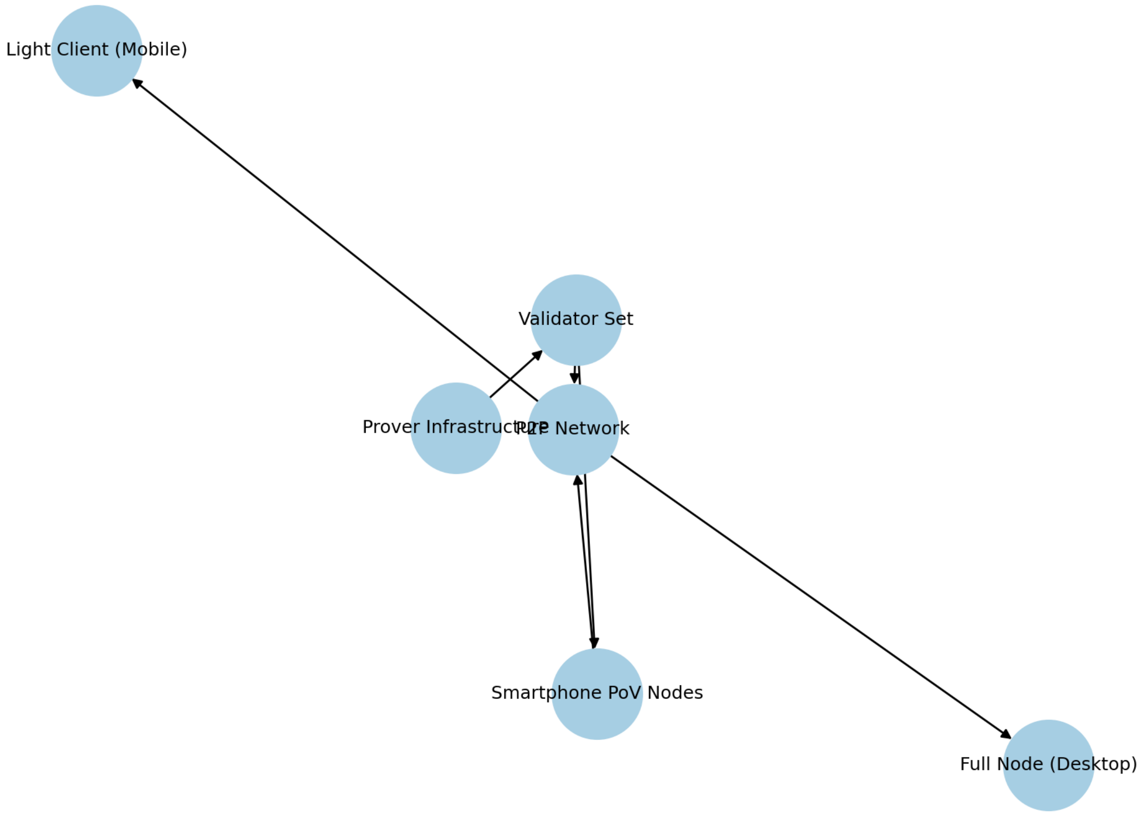


Figure 2: Block Structure

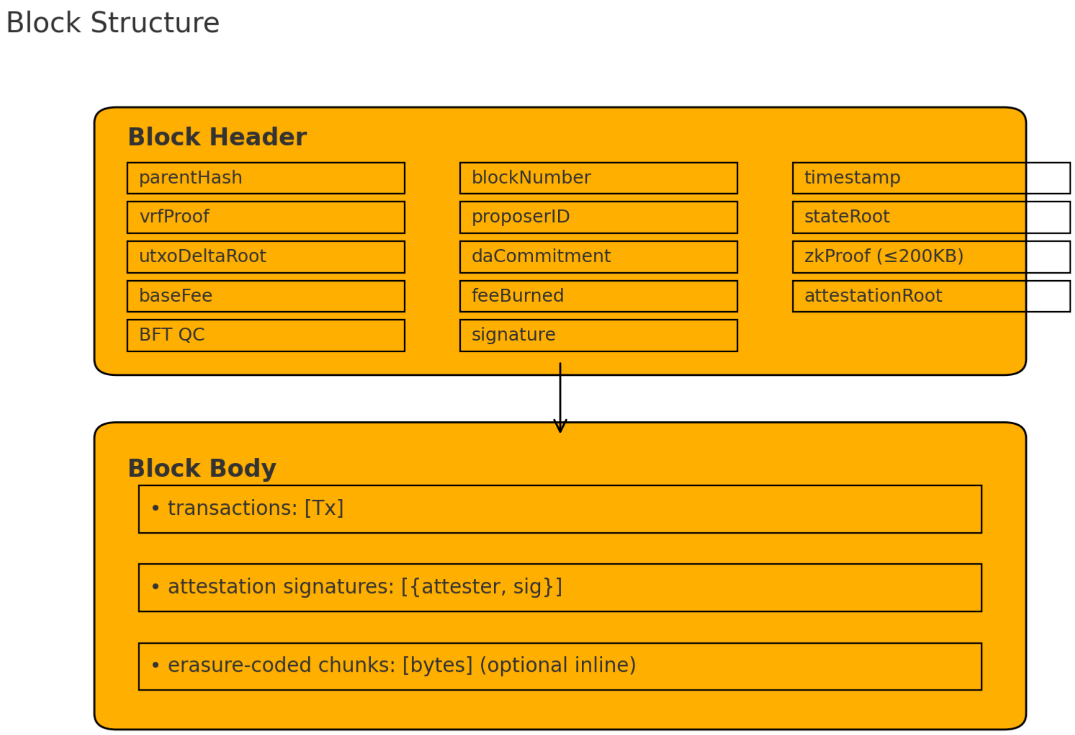
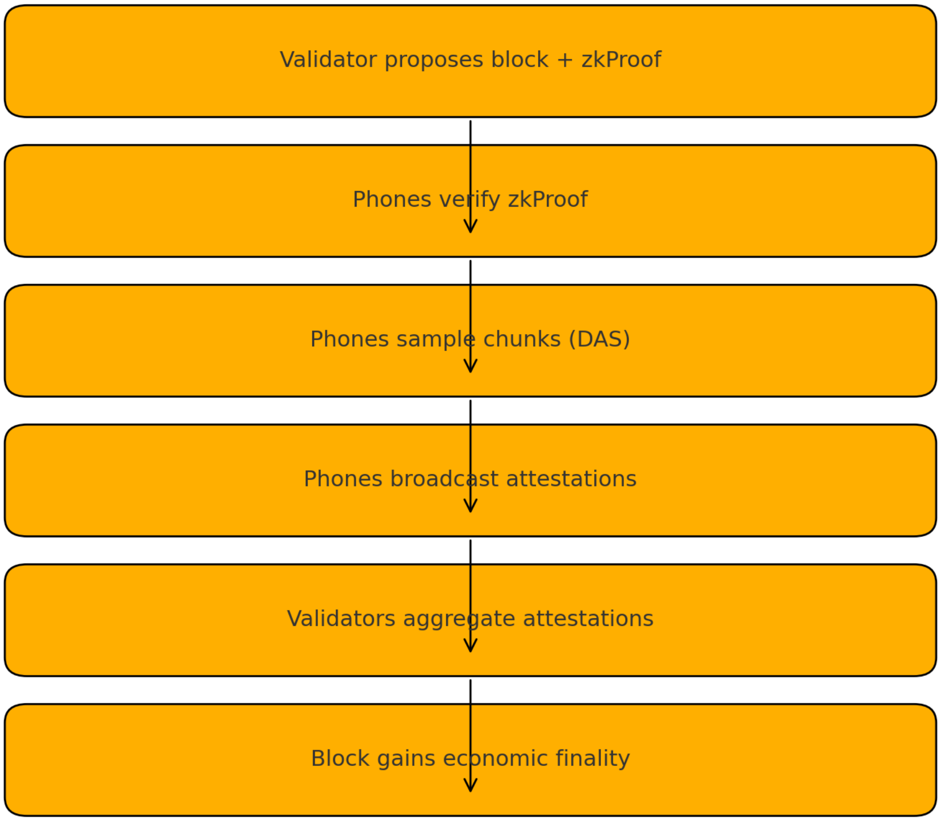


Figure 3: Proof-of-Verification Workflow

Proof-of-Verification (PoV) Workflow


Validator proposes block + zkProof
Phones verify zkProof
Phones sample chunks (DAS)
Phones broadcast attestations
Validators aggregate attestations
Block gains economic finality