Bitcoin Purity: A Peer-to-Peer Electronic Cash System

Nakamotwo Satoshi
nakamotwo@bitcoinpurity.org
Gustavo. (enodexbitcoinpurity@gmail.com)

Abstract

Bitcoin was designed in 2009 by Satoshi Nakamoto as a purely peer-to-peer electronic cash system, enabling online payments to be sent directly from one party to another without going through a financial institution. For years, it functioned successfully as sound money, a trustless timestamp service, and a decentralized store of value. However, the legacy network has drifted from its foundational principles. The introduction of SegWit & Taproot opened the door to arbitrary data storage, and subsequent policy shifts in 2025 allowed inscriptions to commandeer the blockchain. Today, the vast majority of block space is consumed by non-financial data, introducing critical legal and technical risks—including the permanent embedding of illicit material—which threatens the survival of full nodes and miners alike.

Bitcoin Purity is created to preserve Bitcoin's original design by Satoshi Nakamoto: a pure monetary system, secure Proof-of-Work via SHA-256, and a concise scripting engine, ensuring that Bitcoin remains money and blocks are used strictly for financial transactions.

1. Introduction and Motivation

Money must remain money. Since its inception, Bitcoin has faced countless debates regarding block sizes, scaling, protocol changes, and the fundamental definition of what constitutes the original chain.

The core philosophy of Bitcoin Purity is anchored in its name: Purity. Nakamotwo Satoshi, with 15 years of dedicated research into Bitcoin, witnessed the gradual degradation of the network. While some factions proposed radical alterations—such as altering the Proof-of-Work hashing algorithm from SHA-256 to Blake2B—such moves abandon the foundational legitimacy established by Satoshi Nakamoto. Meanwhile, inscriptions have turned block space into a dumping ground for garbage texts, images, and videos, occupying large quantities of block capacity and exposing nodes to catastrophic legal liabilities.

When the initial BIP110 soft fork stalled due to a lack of active hash power and disagreements over discarding legacy miner investments, an urgent hard fork became an operational necessity. Forked directly from Bitcoin Knots v29.4.knots20260508 on August 16, 2026, Bitcoin Purity was launched on August 19, 2026 (with block height 961637 mined on August 20, 2026). It serves as an uncompromised backup for Bitcoin, ensuring the legacy of peer-to-peer cash survives intact without creating a "new coin"—Bitcoin on the Purity chain remains true Bitcoin.

2. Core Function & Philosophy

The operational function of Bitcoin Purity mirrors the original Bitcoin architecture prior to 2017:

- **Decentralized Cash System:** Operating as intended for peer-to-peer exchange.
- **International Money:** Serving as a reliable, non-speculative global currency akin to digital gold.
- **Mass Adoption Ready:** Designed for seamless onboarding and global scalability.
- **High-Cost ASIC Security:** Safeguarded by capital-intensive SHA-256 hardware.
- **No Replay Protection:** The protocol intentionally does not introduce protocol-level replay protection, preserving transaction-format continuity with the shared pre-fork history.
- **Shared History:** Maintaining deep historical continuity with the legacy Bitcoin chain.
- **Trustless Timestamp Service:** Preserving chronological data integrity and minimalist, essential OP_RETURN functionality.
- **Concise Scripting:** Supporting simple smart contracts without fragile cryptographic bloat.

Protocol Improvements:

- **Adjust DAA:** Avoids long-term significant reductions in hash rates during sudden external situations (such as the closure of major mines by governments) that could otherwise cause blockchain stalls.
- **Long-Term PQC Roadmap:** A definitive pathway toward Post-Quantum Cryptography integration.

3. Technical Architecture & Specifications

3.1 BIP110

What is BIP110: BIP110 is a strict procedural governance framework designed to establish absolute boundaries for protocol upgrades and script execution. It reclaims the original philosophy of Bitcoin's development by preventing the accumulation of technical debt, script bloat, and extraneous data fields that do not serve direct monetary settlement. It acts as an immutable constitution within the node software, filtering out changes that compromise decentralization or introduce unnecessary surface area for bugs.

Why BIP110: Over time, the original Bitcoin network faced persistent pressures to adopt complex features, auxiliary state layers, and non-monetary data storage capabilities directly onto the base layer. This trend eroded node sovereignty by increasing resource costs and transferring governance power away from individual users toward development cartels and mining pools. BIP110 is necessary to re-establish a hard rule of law: the base layer remains strictly focused on secure, censorship-resistant peer-to-peer electronic cash, immune to ideological capture or feature creep.

How we do: We implement BIP110 based on Knots v29.4.knots20260508, which implemented the full BIP110 framework, and transition it from a temporary consensus rule to a permanent one (removing the one-year trial limitation). Looking ahead, we will extend spam detection rules to combat the growing threat of spam attacks. We promise we will never remove OP_RETURN or change its limit.

3.2 DAA (ASERT Implementation)

What is DAA (2016-block vs. ASERT): The Difficulty Adjustment Algorithm (DAA) maintains a steady mining pace for Bitcoin blocks, averaging a 10-minute frequency. Difficulty is a consensus variable

adjusted every epoch of 2016 blocks. If an epoch takes longer than 20,160 minutes, difficulty decreases; otherwise, it increases. While effective under stable hashrates, rapid long-term hashrate growth causes blocks to be mined prematurely, rushing toward the 21-million limit and triggering unexpected inflation. Conversely, a sudden drop in hashrate leaves remaining miners processing blocks far slower than the 10-minute target, making the network nearly unusable for years.

Why changing DAA to ASERT: To eliminate the catastrophic vulnerability of multi-week feedback loops under volatile hashrate conditions, Purity alters the DAA to ASERT (Absolutely Scheduled Exponentially Rising Targets). ASERT computes difficulty adjustments on a per-block basis rather than waiting for discrete 2016-block epochs. It incorporates an exponential target spacing curve that smoothly dampens volatility, completely neutralizing timestamp manipulation (timewarp attacks) and multipool hash-switching exploit vectors while maintaining absolute adherence to the long-term 10-minute average target.

How we do (parameter selection and result): Purity uses the aserti3 algorithm with the following deterministic parameters: Anchor height: 961632 (the first BIP110 block); Target spacing: 600 (10 minutes); Half-life: 86400 (24 hours). This configuration provides an ideal dampening factor: responsive enough to handle extreme hashrate shocks instantly, yet mathematically stable enough to prevent oscillation feedback loops. In just 2 weeks of stress testing, Purity successfully navigated the transition of its hashrate from 600+ EH/s down to 200+ TH/s, instantly achieving a standard 10-minute block production cadence without manual intervention or consensus splits.

3.3 Deep Re-org Auto Parking

What is Deep Re-org Auto Parking: As is widely understood, a 51% attack is a persistent systemic risk inherent to Proof-of-Work blockchains, and deep reorganization attacks can severely impact honest miners' profits and network determinism. "Parking" a block is a defensive local node mechanism designed to safeguard the network against sudden, massive chain reorganizations orchestrated by malicious actors with superior transient hashrate.

Why Deep Re-org Auto Parking: Blindly following the heaviest chain rule without depth boundaries exposes nodes to double-spend attacks via sudden private-chain releases. By automating the identification of anomalous chain rewrites, nodes can insulate themselves from economic disruption, refusing to instantly flip their active state for suspicious, out-of-nowhere deep histories.

How we do: When a node receives a valid block that belongs to a competing fork, it checks the fork depth relative to the current tip. If connecting this new block requires rewinding the active blockchain by more than a predefined threshold (a deep reorg), the node flags the new block state as parked instead of active. Node operation and mempool routing won't be disrupted by parking; the node simply maintains its current valid tip while logging the competing alternative. Having carefully checked and verified the intentions or safety of the fork over subsequent observations, the node can manually or conditionally unpark this block and accept it as an active chain. Please note that parking is a strict local node policy and not a guaranteed global consensus rule. The default deep reorganization count is set to 6 blocks, but operators retain total sovereignty to change this value to any custom security parameter suited to their threat model.

3.4 Block Limit & Scalability

At the start of Bitcoin, there was a 32MiB MAX_SIZE limit for a block. In July 2010, Satoshi introduced a MAX_BLOCK_SIZE = 1MB limit without formal explanation, though he noted in October 2010 that higher limits could be phased in once actual usage approached capacity. In 2017, Core/Blockstream permanently fixed the block size against mass adoption. Because Post-Quantum Cryptography (PQC) demands significantly more block space due to large public keys and signatures, raising the block size is essential.

Our Solution:
1. Increase MAX_BLOCK_SIZE to 32MiB, and MAX_SIZE to 128MiB.
2. Move the Witness Script for P2WSH from SegWit data to base data.
3. Preserve the current SegWit discount.
4. Adopt Utreexo for UTXO-state compression.

3.5 Taproot

Taproot was activated in November 2021 via soft fork to improve privacy and flexibility using Schnorr signatures, Merkelized Abstract Syntax Trees (MAST), and Tapscript. However, its primary practical adoption has been for inscriptions (storing arbitrary texts, images, and videos), creating severe security and data-bloat risks.

Our Solution: Taproot must be removed. Our plan is to invalidate P2TR outputs at a future soft-fork height, subsequently purging all code related to MAST and Tapscript. Schnorr signatures will be preserved via a new OP_2 witness output or a new OP_CHECKSCHNORR instruction. SegWit will be retained with restricted functionality due to its valid utility use cases.

3.6 Post-Quantum Cryptography (PQC)

Bitcoin's security relies on Elliptic Curve Cryptography (ECC), which is vulnerable to Shor's algorithm on practical quantum computers expected within the decade. Bitcoin Core and Knots have failed to address this adequately.

Our Solution:
1. Choose a PQC algorithm with a moderately sized public key and signature standardized by NIST.
2. Introduce a new transaction version treating OP_CHECKSIG and OP_CHECKMULTISIG under new algorithms.
3. Remove legacy ECC signature transactions at a future height ("Q-Day").
4. Support both ECC and PQC signatures concurrently for a transition period to allow users to migrate UTXOs.
5. Prohibit spending legacy ECC-signature UTXOs permanently after Q-Day.

4. Ecosystem, Mining, and User Experience

Bitcoin Purity brings decentralization back to the user level through integrated, intuitive tooling:

- **Native Node Mining & Wallet:** Node software integrates a user-friendly mining function alongside a complete wallet interface. Users can easily manage funds, configure transactions, and monitor solo mining statistics—including current network difficulty, accepted/rejected shares, and real-time

probability estimates for closing a block based on active hash power.

- **The Purity Pool:** A dedicated, zero-fee solo mining pool designed to support primary mining and lower the barrier to entry for independent miners without taking any percentage cut.
- **Transparent Mempool & Block Explorer:** A custom web-based mempool viewer allowing anyone to track real-time block assembly, pending transactions, and the identity of the miner who successfully solved each block.

Conclusion

Blocks are for money. Money is for exchange.

Bitcoin Purity cuts through the noise of inscriptions, speculative bloat, and experimental algorithm changes. By returning to the foundational blueprint of Satoshi Nakamoto and combining it with modern, battle-tested resilience upgrades like BIP110 and ASERT, Bitcoin Purity secures the future of decentralized electronic cash.

Keep Bitcoin Pure with Bitcoin Purity.