# Migrating Bitcoin to AOB for Enhanced Security: A Theoretical Framework and Pathway Exploration

**Author:** Liu Zhuo

**Date:** Sep 26, 2025

## Abstract

**Despite Bitcoin's tremendous success as a peer-to-peer electronic cash system, its reliance on Proof-of-Work (PoW) consensus mechanism presents profound and inherent security vulnerabilities. The essence of PoW is a computational power gamble rather than a pursuit of truth, enabling a "malicious" branch with superior hash power to defeat a "righteous" branch. The recent 51% attack on the mainstream privacy blockchain Monero in August 2025[1] has once again highlighted the real-world threat of this theoretical risk. This paper provides an in-depth analysis of the fragility of PoW consensus mechanisms when confronted with computational hegemony, flawed economic models, and inherent randomness. In response, this paper proposes a revolutionary solution: migrating Bitcoin to the theoretical framework of Atomic Ownership Blockchains (AOB). AOB consists of independent micro-blockchains corresponding to each atomic asset, employing broadcast temporal ordering as implicit consensus, aiming to elevate the security foundation from the economic level to the cryptographic level. This paper not only discusses the core architecture of AOB and its inherent limitations but also explores smooth migration pathways without requiring hard forks. Ultimately, we emphasize that any such migration requires rigorous empirical validation and propose specific simulation testing plans to explore the feasibility of Bitcoin's future evolution.**

## 1. Introduction: Limitations of Bitcoin's Foundational Model

**Since its inception in 2009, Bitcoin has not only pioneered the era of cryptocurrencies but also demonstrated to the world the feasibility of decentralized, censorship-resistant networks for value storage and transfer. At its**

**core lies Satoshi Nakamoto's original Proof-of-Work (PoW) consensus mechanism [1]. However, in-depth scrutiny of this cornerstone reveals serious flaws in its decentralization claims. The essence of PoW is less a consensus process pursuing truth than a gambling competition of computational power.**

**Bitcoin's initial concept envisioned individuals mining with personal computers, where "computational voting" retained some legitimacy. However, the emergence of ASIC miners and specialized mining pools completely disrupted this balance, rapidly concentrating hash power in the hands of a few entities. Unlike Bitcoin's single, monolithic public chain implicitly controlled by computational oligarchs, AOB proposes an "atomic" design aimed at structurally returning to the origins of decentralization. This paper aims to analyze the inherent flaws of PoW and explore a potential direction for Bitcoin's future evolution based on the theoretical framework of the AOB whitepaper [3].**

## 2. Inherent Vulnerabilities of Proof-of-Work: A Profound Security Crisis

**Bitcoin's security model is built upon a series of sophisticated yet fragile assumptions. Once these assumptions are broken, the system's risks become fully exposed.**

### 2.1. The Persistent Threat of 51% Attacks: From Theory to Reality

**The 51% attack is a fundamental, inherent vulnerability of the PoW mechanism. Estimates suggest that launching a one-hour attack on Bitcoin through hash power rental markets (such as NiceHash) costs significantly less than purchasing mining equipment, making this threat no longer distant [4]. The recent attack on Monero[1], along with historical successful attacks on Ethereum Classic (ETC) and Bitcoin Gold (BTG) [5], eloquently demonstrates that 51% attacks are persistent, real threats. The Monero incident is particularly alarming, highlighting that even in 2025, the fundamental flaws of PoW remain present and highly threatening. This validates how prescient the AOB whitepaper's criticism of Bitcoin's "might over right" principle was [3, p. 1]. Unlike PoW, Proof-of-Stake (PoS), while reducing energy consumption, faces different security challenges such as "stake centralization" and "long-range attacks" [6], indicating that consensus security remains a core challenge for the entire field.[15]**

## 2.2. The Double Fallacy of Economic Security

**A common defense argues that the cost of attacking Bitcoin far exceeds potential gains, providing no economic incentive for attackers. However, this constitutes a double fallacy of economic security.**

**First, Bitcoin cannot guarantee absolute security even at the purely economic level, as it cannot completely prevent attackers from profiting. Attackers need not purchase expensive mining equipment; they can rent sufficient hash power through rental markets (such as NiceHash) for short-term attacks. After a successful attack, if not widely publicized, it's difficult to confirm as an attack and won't cause price collapse. Through large deposits, trades, and withdrawals targeting major exchanges, followed by using rented hash power to reverse the original deposit transactions, attackers can potentially achieve profitable "double spending." Additionally, attackers can heavily short Bitcoin in derivatives markets, profiting from market panic induced by the attack itself far exceeding attack costs. As long as "double spend profits + short profits > hash power rental costs," an economically motivated attack becomes entirely feasible.[2].**

**Second, even assuming attacks cannot be profitable, the entire security model still relies on the fragile assumption of "rational economic actors." It completely ignores diverse non-economic attack motivations in the real world:**

- **Ideological or political motivations**: Nations or organizations seeking to destroy a decentralized monetary system
- **Destructive or hacking behavior**: Purely for creating chaos or demonstrating technical prowess
- **Revenge or extortion**: Retaliatory actions against specific individuals, companies, or entire communities
- **Irrational behavior**: Actions unpredictable through economic logic

Therefore, a robust security system must be built on strong, deterministic defense mechanisms rather than hoping attackers are economically rational and that such rational calculations always conclude against attacking[16].

## 2.3. Miners' Public Power vs. Users' Private Rights

**In the Bitcoin network, users' "private rights" to freely dispose of their property**

**must rely on miners exercising the "public power" of recording transactions. This dependency itself contradicts the "trustless" principle, exposing users to potential transaction censorship or interference by miners.**

### 2.4. Sustained Attacks and Blockchain Monopolization

**Attackers gaining superior hash power need not profit only through single double-spend attacks. They can exclude blocks added by other miners by only adding blocks after their own blocks, pushing others' hash power out of the network, then purchase idle mining equipment at low prices to further increase their hash power proportion. When possessing sufficient hash power, they can withdraw some computational power while maintaining advantage, reducing electricity consumption for greater profits. Upon detecting new hash power joining, they immediately increase computational power to exclude new participants, thus monopolizing a public chain.**

### 2.5. Community Consensus Is Not the Correct Direction

**As with previous attack incidents, the blockchain technology community engaged in security discussions following the Monero attack, often concluding with introducing community voting mechanisms. This is not feasible. If communities determine fork choices, cryptocurrency decentralization becomes meaningless. Moreover, community voting itself faces Sybil attack threats.**

## 3. A Superior Security Paradigm: Atomic Ownership Blockchains (AOB)

**The true value of blockchain technology lies in elevating the security foundation from the economic level to the cryptographic level. AOB is designed precisely for this purpose.**

### 3.1. Core Concept: Each Blockchain as a Banknote

**AOB completely abandons the single macro-ledger determined by computational competition. In AOB, the system comprises countless "atomic objects," where each object (e.g., a digital banknote of specific denomination) is itself an**

**independent, micro-blockchain. Each blockchain can only be extended by its owner, with ownership transferred through block migration.**

## 3.2. Implicit Consensus and Attack Model Transformation

**AOB does not rely on computational voting but employs "implicit consensus" based on network broadcast timing: the first block universally received by network nodes is considered valid. Its reliability can be quantified through the $t_o$ model proposed in the AOB whitepaper. $t_o$ is defined as the time required for a message to reach 99.99% of nodes. In a hypothetical global network with $10^{11}$ nodes, each having 475 effective connections, $t_o$ is estimated at approximately 7 seconds [3, p. 6]. This means that in most cases, the network can achieve extremely high-probability consensus on block ordering within seconds. This design does not "completely eliminate" attacks but transforms the attack model from "computational advantage" to "network layer advantage," with the latter being more difficult to achieve.**

## 3.3. From Economic Deterrence to Deterministic Punishment

**AOB's architecture significantly mitigates 51% attack feasibility, with security centered on:**

1. **Computational power irrelevance**: A block's validity depends solely on signatures and broadcast order, unrelated to hash power

2. **Inevitable punishment for malicious behavior**: Double-spend attempts provide undeniable cryptographic evidence, resulting in automatic blacklisting of malicious accounts by protocol rules

3. **Risk isolation**: This concept is key to AOB's security model. As stated in the AOB whitepaper [3, p. 8], even in extremely rare network partition events, a successful double-spend attack affects only that single "atomic object" (one "banknote"). The system's remainder and all other users' assets remain completely unaffected. Problems are confined to the microscopic level without triggering systemic collapse.

## 3.4. Limitations and Challenges

**As a theoretical framework, AOB faces its own challenges. Its security model**

**heavily depends on nodes maintaining long-term online presence to accurately record and verify transaction broadcast order. In extreme network splitting scenarios, potential inflation issues caused by forks also require more comprehensive economic models for constraint.**

# 4. The Path to Smooth Migration: Solutions Without Hard Forks

**Migrating Bitcoin to AOB through mandatory hard forks would fracture the community with extremely high risks. A smoother migration path must be voluntary, gradual, and risk-controllable.**

## 4.1. Ideal Path: Trustless Bidirectional "Atomic Binding"

**This represents an ideally decentralized solution that proceeds in two logical stages rather than a single step, clearly demonstrating the evolutionary path from present to future.**

**Stage One: Unidirectional Anchoring (Peg-In)**

**This stage utilizes Bitcoin's existing protocol without any modifications, achieving trustless unidirectional asset migration.**

1. **Banknote Creation**: Users create a new "banknote" on the AOB network, denominated at the desired Bitcoin amount (e.g., 1 BTC), generating a unique, globally identifiable banknote ID

2. **Cryptographic Destruction**: Users transfer the same amount (1 BTC) from their Bitcoin wallet to a universally recognized "black hole address" derived through a standard, public, deterministic algorithm from that AOB banknote ID. Since no one possesses the private key for this address, this Bitcoin is permanently and publicly verifiably removed from circulation

3. **Banknote Activation**: After this "destruction" transaction receives sufficient confirmations on the Bitcoin blockchain (e.g., 100 blocks) to ensure finality, users record this transaction's UTXO information in the first block of the AOB banknote. This step completes banknote "activation," proving it has adequate, genuine Bitcoin value backing

The initial stage's challenge lies in its unidirectionality—redemption is impossible under Bitcoin's current mechanisms. This may cause AOB-BTC market value to decouple from native BTC. However, this unidirectionality is not a permanent theoretical dead-end but a limitation of current Bitcoin protocol capabilities, laying groundwork for the second stage's ultimate solution.

**Stage Two: Bidirectional Redemption via Miner-Validated State Proof (Peg-Out)**

**This represents the ultimate vision for achieving free asset flow, requiring a significant Bitcoin protocol upgrade (e.g., through a soft fork) to empower miners to validate and enforce the state of an external AOB chain. The process is envisioned as follows:**

1. **Banknote Destruction and Redemption Proposal:** The current owner of an AOB-BTC banknote initiates the peg-out by adding a final "destruction block" to their specific micro-blockchain. Based on the unique ID of this block, a corresponding temporary UTXO (`temp-UTXO`) is generated and broadcast to the Bitcoin network as a redemption proposal.

2. **Miner Verification and On-Chain Anchoring:** Upon receiving the `temp-UTXO`, upgraded Bitcoin miners perform a crucial validation role. They must fetch and verify the entire history of the associated AOB banknote to confirm the legitimacy of the owner who initiated the destruction. If a miner concurs with the ownership proof, they construct a new Bitcoin block that includes the original UTXO from the peg-in stage, the new `temp-UTXO`, and the full data of the AOB banknote chain. This effectively treats the entire AOB chain as a comprehensive proof-of-ownership, linking the locked funds to the redemption request on the main chain.

3. **Probabilistic Finality through Miner Voting:** Recognizing that AOB chains may have forks, the protocol introduces a voting mechanism to resolve ownership disputes. For a `temp-UTXO` to become valid, it must undergo a confirmation period of `n` blocks. During this period, other miners can signal their dissent if they disagree with the validity of the anchored AOB chain. After `n` blocks, if the dissent rate remains below a predetermined threshold `R`, the `temp-UTXO` is activated and becomes a standard, spendable UTXO, allowing the Bitcoin to circulate freely again.

4. **Conflict Resolution:** In the event that a competing `temp-UTXO` (originating from a fork of the same AOB banknote) is broadcast, the protocol enforces a rule that no single Bitcoin block can validate both. The `temp-UTXO` that first successfully completes the `n`-block voting period with a dissent rate below `R` achieves finality. Supporters of the conflicting `temp-UTXO` could theoretically fork the Bitcoin chain, but

the longest-chain rule would ultimately serve as the final arbiter, ensuring only one redemption path succeeds.

This mechanism transforms the redemption process into a decentralized validation and voting system. It conceptually builds upon existing sidechain proposals by leveraging Bitcoin's security infrastructure to adjudicate the state of external assets. The approach is directly inspired by Drivechains (BIP 300) [17], which also proposes using miner consensus to validate peg-out transactions. However, our model extends this concept by requiring miners to validate the entire state history of an AOB banknote, rather than just a single withdrawal transaction. Furthermore, the probabilistic finality model, which relies on an n-block confirmation period and a dissent threshold (R), is logically analogous to the challenge periods found in Optimistic Rollups [18], where a state transition is accepted if it remains unchallenged. This design aims to provide a robust and trustless pathway for bidirectional asset flow, addressing security limitations present in earlier SPV-based proposals [19].

### 4.2. Migration Risks and Challenges

**This path faces enormous obstacles. First, the Bitcoin community maintains extremely conservative attitudes toward any protocol changes, making soft fork upgrades politically difficult—Bitcoin's multi-year intense controversy and community division surrounding SegWit upgrade serves as the best evidence. Second, AOB's atomization characteristics may encounter technical challenges when handling Bitcoin's complex UTXO model. Additionally, if Bitcoin undergoes forks before migration occurs, risks remain for migrated amounts.**

## 5. Conclusion: Call for Specific Next-Step Research

**Proof-of-Work is a great invention, but its security model based on computational hegemony and economic assumptions contains ineradicable hidden dangers. Atomic Ownership Blockchains (AOB) provide a distinctly different, inspiring theoretical framework.**

**However, it must be emphasized that AOB remains a theoretical construct. This paper's purpose is not to assert AOB as the only answer but to use its theoretical framework to deeply analyze existing system inadequacies. Therefore, we call for a specific, executable next-step research plan: We recommend immediately beginning development of an AOB prototype simulator.** Such a simulator would allow rigorous testing of core assumptions, particularly validating the effectiveness of

the $t_0$ model proposed in the AOB whitepaper [3, p. 6] under real-world network latency data. Only through such rigorous scientific validation can we determine whether AOB or similar innovative solutions can truly lead Bitcoin toward a more secure, more decentralized future.

## References


**[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf**

**[2] Leshno, J. D., Pass, R., & Shi, E. *On the Viability of Open-Source Financial Rails: Economic Security of Permissionless Consensus*. https://eprint.iacr.org/2023/1516.pdf**

**[3] Liu, Z. (2025). *Achieving True Decentralization: The Atomic Ownership Blockchains Technology*. Ledger. https://doi.org/10.5195/ledger.2025.425 (In Press). Preprint available at: https://doi.org/10.5281/zenodo.12236674**

**[4] Crypto51.app. (2025). *Cost of a 51% Attack on Various PoW Blockchains*. https://www.crypto51.app/**

**[5] Sayeed, S., & Marco-Gisbert, H. (2019). "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack" - https://www.mdpi.com/2076-3417/9/9/1788**

**[6] Deirmentzoglou, E., et al. (2019). A Survey on Long Range Attacks for Proof of Stake Protocols. IEEE Access, 7, 28712-28725. https://doi.org/10.1109/ACCESS.2019.2901858**

**[7] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2019). *Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack*. Applied Sciences, 9(9), 1788. https://doi.org/10.3390/app9091788**

**[8] Shanaev, S., Shuraeva, A., Vasenin, M., & Kuznetsov, M. (2019). *Cryptocurrency Value and 51% Attacks: Evidence from Event Studies*. Journal of Alternative Investments, 22(3), 65-77. https://www.pm-research.com/content/iijaltinv/22/3/65**

**[9] Xu, G., Bai, H., Xing, J., Luo, T., Xiong, N. N., Cheng, X., ... & Zheng, X. (2020). *SG-PBFT: A secure and highly efficient distributed blockchain PBFT consensus algorithm for intelligent Internet of vehicles*. Journal of Parallel and Distributed Computing, 145, 1-14. https://www.sciencedirect.com/science/article/abs/pii/S0743731522000363**

**[10] Auer, R., & Böhme, R. (2020). *The technology of retail central bank digital currency*. BIS Quarterly Review, March, 85-100. Bank for International Settlements Working Paper No. 765. https://www.bis.org/publ/qtrpdf/r_qt2003j.htm**

**[11] Pass, R., Seeman, L., & Shelat, A. (2017). *Analysis of the blockchain protocol in asynchronous networks*. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 643-673). Springer. https://doi.org/10.1007/978-3-319-56614-6_22**

**[12] Gazi, P., Kiayias, A., & Russell, A. (2018). *Stake-bleeding attacks on proof-of-stake blockchains*. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 85-92). IEEE. https://doi.org/10.1109/CVCBT.2018.00015**

**[13] Vasek, M., Thornton, M., & Moore, T. (2014). *Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem*. In International conference on financial cryptography and data security (pp. 57-71). Springer. https://tylermoore.utulsa.edu/bitcoin14ddos.pdf**

**[14] Kamps, J., & Kleinberg, B. (2018). *To the moon: defining and detecting cryptocurrency pump-and-dumps*. Crime Science, 7(1), 1-18. https://link.springer.com/article/10.1186/s40163-018-0093-5**

**[15] Amin, M. R. "51% ATTACKS ON BLOCKCHAIN: A SOLUTION ARCHITECTURE FOR BLOCKCHAIN TO SECURE IOT WITH PROOF OF WORK" - https://www.researchgate.net/publication/351993636_51_ATTACKS_ON_BLOCKCHAIN_A_SOLUTION_ARCHITECTURE_FOR_BLOCKCHAIN_TO_SECURE_IOT_WITH_PROOF_OF_WORK**

**[16]Budish, E. "Trust at Scale: The Economic Limits of Cryptocurrencies and Blockchains" - https://bfi.uchicago.edu/wp-content/uploads/2022/06/BFI_WP_2022-83-1.pdf**

**[17] Sztorc, P. (2017). *Drivechain - The Simple Two Way Peg*. Retrieved from http://www.drivechain.info/paper/drivechain.pdf**

**[18] Buterin, V. (2021). *An Incomplete Guide to Rollups*. Retrieved from https://vitalik.ca/general/2021/01/05/rollup.html**

**[19] Back, A., et al. (2014). *Enabling Blockchain Innovations with Pegged Sidechains*. Retrieved from https://www.blockstream.com/sidechains.pdf**

**---**

**Footnote**

[1] **Refers to the hash power attack conducted by the Qubic project on Monero in August 2025, described as a "stress test" to demonstrate the boundaries of decentralization and PoW vulnerabilities through economic incentives like triple mining rewards, leading to chain reorganizations. Related information can be found in reports from OKX dated August 2025 and Bitget dated August 21, 2025.**