LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI 10.5195/LEDGER.2025.425

Achieving Greater Decentralization with Atomic Ownership Blockchains: Open Review

Zhuo Liu*†

Reviewers: Reviewer A, Reviewer B, Reviewer C

Abstract. The final version of the paper "Achieving Greater Decentralization with Atomic Ownership Blockchains" can be found in Ledger Vol. 10 (2025) 136-153, DOI 10.5195/LEDGER.2025.425. There were three reviewers involved in the review process, none of whom has requested to waive their anonymity at present, and are thus listed as Reviewers A, B, and C. After initial review by Reviewers A, B, and C, the submission was returned to the authors with feedback (1A). The author resubmitted their work and responded to reviewer comments (1B). The editor determined that the revisions and responses were sufficient and the paper was accepted for publication, thus ending the peer review process.

1A. First Round of Review

Reviewer A

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Yes, incremental contribution(s)

Please briefly explain why you think the paper makes or does not make a novel contribution.

The paper presents a genuinely original idea by introducing Atomic Ownership Blockchains (AOB), where each asset has its own mini blockchain controlled by a single owner but visible to everyone. This setup avoids traditional consensus methods like proof-of-work and instead uses broadcast timing to resolve conflicts. It's a fresh take on tackling blockchain's scalability and decentralization issues. As far as I know, this approach hasn't been explored in the existing research, so it does make a novel contribution. That said, the concept is still theoretical and would need more formal modeling and real-world testing to prove its viability.

* Z. Liu (liuzhuo2011@gmail.com) is an independent researcher from Beijing, China.
† 1J9swFhj76E7D1hoacusEA5wBK6ypVSUHL

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Important references are missing

Please assess the article's level of academic rigor.

Unsatisfactory (better than poor but a long way from excellent)

Please assess the article's quality of presentation.

Unsatisfactory (better than poor but a long way from excellent)

How does the quality of this paper compare to other papers in this field?

The paper has some value but it can easily be replaced by better scholarship in the field.

Please provide your free-form review for the author in this section.

This paper introduces a genuinely creative and unconventional idea—representing each digital asset as its own private blockchain (AOB). It's an ambitious attempt to rethink decentralization and scalability from first principles, and I appreciate the out-of-the-box thinking here. The design tackles real limitations in existing blockchain systems, especially the over-reliance on consensus mechanisms and miner incentives.

That said, the paper still feels quite early-stage. The arguments rely heavily on analogies (e.g., burning banknotes) rather than formal definitions or structured analysis. There's no real modeling, no simulations, and no clear comparison to other existing ideas like DAGs, UTXOs, rollups, or account abstraction. It also assumes ideal network conditions (constant uptime, synchronized nodes), which doesn't align with real-world deployment challenges.

The fork resolution mechanism based on broadcast timing seems optimistic—it assumes consistent network connectivity and predictable delays, which may not hold in practice. A more robust treatment of adversarial behavior and network partitions would make this much stronger. Right now, it's unclear how resilient the system is when nodes are offline or operating under inconsistent latency.

It's great that there's a demo and open-source code provided. That's a good step toward grounding the concept. Still, the paper would benefit from a short walkthrough explaining what's actually implemented, what's mocked or conceptual, and how the prototype maps to the core claims.

To move this forward, I'd suggest:

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

Adding a formal description of how AOBs work—pseudocode, diagrams, or protocols would help.

Being clearer about assumptions (e.g., how forks are detected or resolved across unsynced nodes).

Citing and comparing to relevant literature to situate this idea in context.

Rewriting parts to make the exposition tighter and avoid redundancy.

The idea is worth exploring—but right now it reads more like a concept proposal than a finished academic contribution. With more structure, clarity, and technical depth, it could become a much stronger paper.

Reviewer B

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

No

Please briefly explain why you think the paper makes or does not make a novel contribution.

It has been explained in my comments to the authors.

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Important references are missing

Please assess the article's level of academic rigor.

Unsatisfactory (better than poor but a long way from excellent)

Please assess the article's quality of presentation.

Good (not excellent but a long way from poor)

How does the quality of this paper compare to other papers in this field?

This is a good or average paper.

Please provide your free-form review for the author in this section.

The paper presents AOB as a breakthrough in blockchain technology, yet it fails to

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

provide a well-defined security model, or a clear economic framework. The author must address the following critical gaps before AOB can be considered a serious alternative to existing decentralized ledger technologies:

(a) There is no benchmarking against existing blockchain solutions, making it impossible to assess whether AOB genuinely offers improvements in scalability or decentralization.

(b) The proposal does not address potential exploits such as ownership fraud, malicious node behaviors, or blockchain hijacking through private key compromises.

(c) The conflict resolution method—relying on broadcast timing to determine the "valid" chain—assumes that all nodes have reliable network conditions, which is unrealistic in a decentralized setting. This approach is highly susceptible to network latency, malicious time manipulation, and partitioning attacks.

(d) AOB's economic incentives are vague, raising concerns about the system's long-term viability. The paper fails to explain how miners, validators, or users would be incentivized to participate. Without clear incentives, blockchain networks risk low adoption or centralization over time.

(e) The paper describes Bitcoin's centralization issues but ignores existing improvements in blockchain technology. While PoW centralization problems are acknowledged, the paper does not compare AOB to alternative models such as Proof-of-Stake (PoS), sharding (Ethereum 2.0), or Directed Acyclic Graphs (IOTA, Avalanche). A few corroborative studies (e.g., https://doi.org/10.1145/3658644.3690198, etc.) should also be discussed in this regard to affirm the statistical reliability of the principles behind considering these key observation points as the significant highlights of this study.

(f) The writing style is overly technical in some sections but lacks clarity in others. Some terms, such as "microscopic blockchain," are introduced without sufficient definition or context. There is excessive use of blockchain jargon without proper breakdowns, making it difficult for non-expert readers to follow.

(g) The proposed Speedy Channel mechanism is described as an off-chain scaling solution but does not offer any improvements over existing models like the Lightning Network. How does AOB's Speedy Channel differ in terms of efficiency, transaction finality, or security? Without differentiation, this feature appears redundant. In the Introduction section, therefore, please elaborate on the significance of these concepts in current research fields related to machine learning based engineering surveying objectives, especially towards creating sustainable public health surveillance infrastructure (with a brief discussion of certain attributable studies, for instance: https://doi.org/10.48048/tis.2024.8528, etc.).

(h) The claim that AOB achieves "true decentralization" is highly debatable. If each blockchain is privately controlled, how does this prevent asset concentration in a few hands? The idea that AOB eliminates the need for consensus could inadvertently introduce

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

new risks, such as reliance on a single entity per blockchain, making it less decentralized in practical terms.

Reviewer C

Does this paper represent a novel contribution to cryptocurrency or blockchain scholarship?

Not sure

Please briefly explain why you think the paper makes or does not make a novel contribution.

Lack of True Novelty or Substantiation: 1. Similar to NFT Concepts 2. Unproven Security Assumptions 3. No Empirical Validation

Is the research framed within its scholarly context and does the paper cite appropriate prior works?

Yes

Please assess the article's level of academic rigor.

Poor (terms are poorly defined, the use of jargon is widespread, proofs/derivations are flawed or absent [if necessary], arguments contain significant logical holes, etc.)

Please assess the article's quality of presentation.

Poor (the purpose of the paper is unclear, the prose is awkward and significant grammatical errors exists, the reader is bogged down in technical details and the main ideas remain elusive).

How does the quality of this paper compare to other papers in this field?

The paper has some value but it can easily be replaced by better scholarship in the field.

Please provide your free-form review for the author in this section.

1. Poor Formatting and Lack of Visual Aids

The paper does not adhere to standard academic formatting. There are no clear section divisions, tables, or figures to make the content more digestible. No charts, diagrams, or illustrations are provided to explain complex concepts, which makes understanding the proposed system challenging.

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

2. Lack of Proper Editing

The writing contains grammatical errors and unclear sentence structures, making it difficult to follow. The text is repetitive in multiple places, leading to redundancy rather than clarity.

3. Logical Issues in the Argumentation

3.1 Flawed Decentralization Assumption:

The paper claims that each user maintaining a private blockchain enhances decentralization. However, if the ownership and operation of blockchains are individualistic, it raises concerns about fragmentation rather than true decentralization. The lack of a consensus mechanism could lead to disputes in ownership verification and coordination between these micro-blockchains.

3.2 Security Model Is Unconvincing:

The paper argues that eliminating voting and using time-based verification enhances security. However, this approach does not account for real-world network latencies, Sybil attacks, and malicious actors who may manipulate the timing of block propagation. The assumption that all forks can be resolved by time order lacks strong cryptographic or game-theoretic validation.

1B. Author's Responses

Addressing Common Concerns

Several important concerns were raised by multiple reviewers, which I prioritized in my revision:

1. Insufficient Security Analysis and Unrealistic Network Assumptions

Supplementary Explanation

For the mechanism that selects forks by comparing block broadcast timing, the following clarification is necessary:

The fork selection results do not require strict network-wide consensus. Each node can reach different conclusions independently. A node's fork selection serves only as its own determination without influencing others' decisions, and there is no need to communicate this conclusion to other nodes. Malicious nodes cannot affect other nodes' judgments by transmitting incorrect information (Sybil attacks). AOB eliminates any voting or implicit

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

voting behaviors, thus removing the requirement for a low-latency synchronous network. Since each blockchain represents only a single atomic unit, as long as the proportion of disagreements between nodes remains sufficiently small, the impact on system operation is negligible. AOB ensures that attacks are economically disadvantageous by identifying and penalizing attackers, thereby preventing forks from occurring on a large scale.

The receiver is the direct victim of a fork. If the receiver's accepted fork differs from that of most nodes, it will affect their ability to spend this blockchain banknote in the future. For other nodes, this risk is much smaller since they may never receive this forked blockchain, and having a divergent recognition of the fork would also hinder their reception of this blockchain. Therefore, the receiver bears direct responsibility for security and has reason to ensure payment safety through sufficient waiting periods. Longer waiting periods enhance security, and the $4t_0$ waiting duration—derived from the network-wide broadcast time t_0—ensures security reaches a satisfactory level, comparable to waiting for six block confirmations after a Bitcoin transaction is recorded on the blockchain. The network-wide broadcast time is estimated by receivers themselves, who may choose to wait longer for greater security confidence. Similarly, receivers can prevent network partitioning by increasing waiting times and testing the network. If a receiver's measures are insufficient, they will bear the primary risk.

Maliciously manipulating broadcast time is difficult to achieve. Since all blocks are distributed via broadcast, and each user deploys multiple nodes across different network domains, unless an attacker can control all nodes, they cannot cause some nodes to receive a later-broadcast block before an earlier-broadcast block when the broadcast time difference exceeds t_0.

The only new network security requirement AOB introduces is for nodes to remain online long-term. Users can easily fulfill this by deploying monitoring nodes on network servers. This requirement is not strict—a user's offline status only creates difficulty for the user in selecting forks that occurred during their offline period, potentially causing some inconvenience when receiving these blockchains in the future, without disrupting other users.

Network parameters:

- $N = 10^{11}$ nodes
- 500 random connections per node
- 95% connection availability
- Transmission delay $\tau \sim U(20\text{ ms}, 1000\text{ ms})$
- Effective degree $k_{eff} = 500 \times 0.95 = 475$

We define t_0 as the time for a message to reach 99.99% of nodes with 99.99% probability. For a random network with N nodes and effective degree k_{eff}, the average distance (in hops) between nodes can be estimated using:

$d \approx \log(N) / \log(k_{eff}) \approx 11 / \log(475) \approx 4.1$ hops

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

To ensure 99.99% reliability, we add additional hops as a safety margin:

- For 99% coverage: d + 1 hops
- For 99.99% coverage: d + 3 hops

Therefore, critical path length ≈ 4.1 + 3 ≈ 7 hops.

With transmission delays summed across these 7 hops, and accounting for the upper tail of the delay distribution, t_0 is estimated to be approximately 7 seconds.

The maximum reception time difference between any two nodes for the same message is t_0.

Therefore, when a receiver gets messages A and B at times Ta and Tb, where $Tb > Ta + 4t_0$, we can determine that:

1. Any other node will receive message A no later than $Ta + t_0$
2. Any other node will receive message B no earlier than $Tb - t_0$

Since $Tb > Ta + 4t_0$, we can establish that: $Tb - t_0 > Ta + 3t_0$

This means any node will receive message B at least $3t_0$ after receiving message A, ensuring a minimum interval of $2t_0$ between receiving the two messages. Given that t_0 is calculated with 99.99% confidence, the probability that any node will receive messages A and B with an interval exceeding $2t_0$ is greater than 99.98% (99.99% × 99.99%).

2. Lack of Formal Definitions and Structured Analysis

Formal Definitions are added into the paper in section 2.5.

3. Lack of Comparison to Existing Technologies

Response:

Key Differences with DAG:

DAG relies on a consensus mechanism, formed through the free expression of all participants, to counter double-spending attacks, which inevitably introduces the risk of a 51% attack. In contrast, AOB nodes independently assess the legitimacy of forks based on their own observations, without relying on the opinions of other nodes. This ensures security even when the number of malicious nodes or their controlled resources exceeds half.

Key Differences with UTXO (added into the paper):

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

AOB banknotes have fixed denominations, while UTXO values can change during transactions.

AOB banknotes have longer lifespans compared to UTXOs, which are frequently spent and replaced by new UTXOs.

AOB operations are simpler than UTXO operations. There is no need for splitting or consolidating banknotes, unlike UTXOs which require these operations.

Key Differences with rollups and sharding (Ethereum 2.0):

Rollups and sharding are Layer 2 scaling solutions designed to enhance scalability. However, their security and decentralization are constrained by the capabilities of Layer 1, making them less robust than AOB in these aspects.

With account abstraction:

AOB does not yet include features corresponding to account abstraction. Given the associated risks, development in the area of smart contracts is proceeding cautiously. The current priority is to enhance the core functionalities related to currency and commodity transactions.

4. Formatting and Clarity Issues

Response:

I adopted standard academic formatting with clear section hierarchies, add diagrams to illustrate key concepts and processes, added definitions of terms and conducted comprehensive editing for grammar and clarity.

5. Claims About Decentralization and Economic Incentives

Response:

Decentralization: The industry widely regards Proof-of-Work (PoW) public blockchains as the gold standard for decentralization. PoS or other public blockchains are not better. AOB builds on Bitcoin's fully decentralized characteristics while further eliminating miners, achieving complete node equality. Most notably, users can independently execute payments without requiring third-party approval, marking a significant advancement in decentralization.

Economic Incentives: AOB precisely aligns user actions with their consequences, operating without miners or dedicated validators, as reflected in the following mechanisms:

1. Perpetrators of double-spending attacks will face penalties.

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

2. Recipients act as the implementers of security measures and bear the primary risk, autonomously determining the desired level of security.

3. If a node does not remain online, it may struggle to select the correct fork if an attack occurs.

In summary, when a user's actions deviate from the guidelines, they typically cause significant trouble or losses for themselves while having minimal impact on others.

Now I will address each reviewer's specific concerns:

Response to Reviewer A

Beyond the common concerns addressed above, I have addressed Reviewer A's specific points as follows:

Concern: Lack of clarity about the demo implementation

"The paper would benefit from a short walkthrough explaining what's actually implemented."

Response:

Description of the Open-Source Code

The code provides the core functionality used in the AOB demo page, including the creation and transfer of each blockchain, but excludes network protocols. In handling double-spending attacks, the system penalizes attackers. Due to the broadcast time being set to 0, demo nodes can more easily identify the order of fork broadcasts compared to real nodes and reject later-broadcast forks.

The URL of the demo page is updated.

Response to Reviewer B

Beyond the common concerns addressed above, I have addressed Reviewer B's specific points as follows:

Concern: Speedy Channel differentiation

"The proposed Speedy Channel mechanism does not offer any improvements over existing models like the Lightning Network."

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

Response:

The value of Speedy Channel lies in porting the Lightning Network to AOB. While each Speedy Channel can support multiple users, surpassing the capabilities of the Lightning Network, this is not its primary focus. Due to AOB's distinct structure compared to conventional blockchains, existing Layer 2 technologies may require significant redesign to be compatible with AOB.

Concern: Public health surveillance infrastructure

"Please elaborate on the significance of these concepts in current research fields related to machine learning based engineering surveying objectives, especially towards creating sustainable public health surveillance infrastructure."

Response:

AOB does not include elements related to this aspect.

Concern: "The claim that AOB achieves "true decentralization" is highly debatable. If each blockchain is privately controlled, how does this prevent asset concentration in a few hands? The idea that AOB eliminates the need for consensus could inadvertently introduce new risks, such as reliance on a single entity per blockchain, making it less decentralized in practical terms."

The goal of decentralization is to ensure equal rights for all, not to achieve wealth equality.

Each blockchain has an owner, but when viewed as a whole, the multi-chain system allows participants to freely transfer their blockchains to others, thereby achieving a high degree of decentralization.

Response to Reviewer C

Beyond the common concerns addressed above, I have addressed Reviewer C's specific points as follows:

Concern: "The paper claims that each user maintaining a private blockchain enhances decentralization. However, if the ownership and operation of blockchains are individualistic, it raises concerns about fragmentation rather than true decentralization. The lack of a consensus mechanism could lead to disputes in ownership verification and coordination between these micro-blockchains."

Response:

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425

When the owner of a blockchain adds a block, the owner can include declarations of decisions, limited to those within the scope of their ownership rights. For example, the owner can declare in a block that the blockchain banknote is transferred to another person, but cannot demand that someone else transfer a banknote to them or increase the value of their banknote from $10 to $100. This approach prevents data conflicts between blockchains, enabling true decentralization.

ISSN 2379-5980 (online)
associated article DOI
10.5195/LEDGER.2025.425