HMDA: Secure Anything on Bitcoin

LayerEdge

1st Ayush Gupta
LayerEdge
ayush@layeredge.io

***Abstract*—The Blocksize War marked a significant chapter in Bitcoin's history, ultimately leading to the adoption of smaller block sizes and the development of Layer 2 solutions. Despite the advantages of maintaining decentralization and security, the increasing proliferation of Layer 2 and Layer 1 applications on Bitcoin has led to anticipated data congestion and rising transaction fees. This paper introduces Hybrid Modular Data Availability (HMDA) as a solution to these emerging challenges. HMDA combines the robustness of Bitcoin's Proof of Work (PoW) consensus mechanism with modular data availability frameworks to enhance scalability and security.**

The paper explores the role of Bitcoin timestamping in HMDA, which mitigates long-range attacks and allows for faster unbonding of staked assets. Through the implementation of checkpoints and the recording of block hashes and staking set votes on the Bitcoin blockchain, HMDA ensures data integrity and resilience. This mechanism not only reduces withdrawal timeframes but also provides an additional layer of data integrity verification.

One of the key benefits of HMDA's Hybrid DA Layer approach is the significant reduction in block time and finality, with block times of 12-20 seconds compared to Bitcoin's 10 minutes. This rapid finality provides several advantages, including improved efficiency in transaction processing and smart contract execution, enhanced responsiveness for interactive applications, and better scalability by processing more transactions per unit of time.

If all Layer 1 dApps and Layer 2 solutions posted their data directly on Bitcoin, it would lead to severe data clogging, exacerbating congestion and dramatically increasing transaction fees, making it unsustainable for the network to handle the growing demand. By storing large data on modular data availability solutions and state proofs on the Bitcoin blockchain, HMDA creates a synergistic framework that leverages the strengths of both systems. This dual approach enhances data availability, scalability, and security, making it a robust solution for future blockchain applications. The paper concludes by discussing the potential impact of HMDA on Bitcoin and the broader blockchain ecosystem, highlighting its prospects for wider adoption and its role in advancing blockchain technology.

I. Introduction

A. Background

1) The Blocksize War:

- The Blocksize War was a critical conflict within the Bitcoin community from 2015 to 2017, centered around how to scale the Bitcoin network to accommodate more transactions.
- Proponents of larger blocks argued that increasing the block size limit would allow more transactions to be processed per block, reducing transaction fees and improving network speed.
- Proponents of smaller blocks emphasized maintaining a decentralized network where the majority of nodes could afford to store the full blockchain, ensuring security and robustness.

2) Large Block Size vs. Small Block Size Debate:

- **Large Block Size** Supporters, including some major miners and companies, suggested increasing the block size from 1 MB to up to 8 MB to accommodate more transactions.
- **Small Block Size** Supporters, including many developers and decentralization advocates, argued for keeping the block size at 1 MB and focusing on second-layer solutions like the Lightning Network to handle transaction throughput.

3) Conclusion of the War:

- The debate concluded with the adoption of Segregated Witness (SegWit) in 2017, which effectively increased the the block size limit by changing how transaction data is stored, effectively allowing more transactions to fit into each block without increasing the actual block size limit of 1 MB, and paved the way for the development of the Lightning Network.

B. Current Scenario

1) Rise of Layer 2 and Layer 1 Applications on Bitcoin:

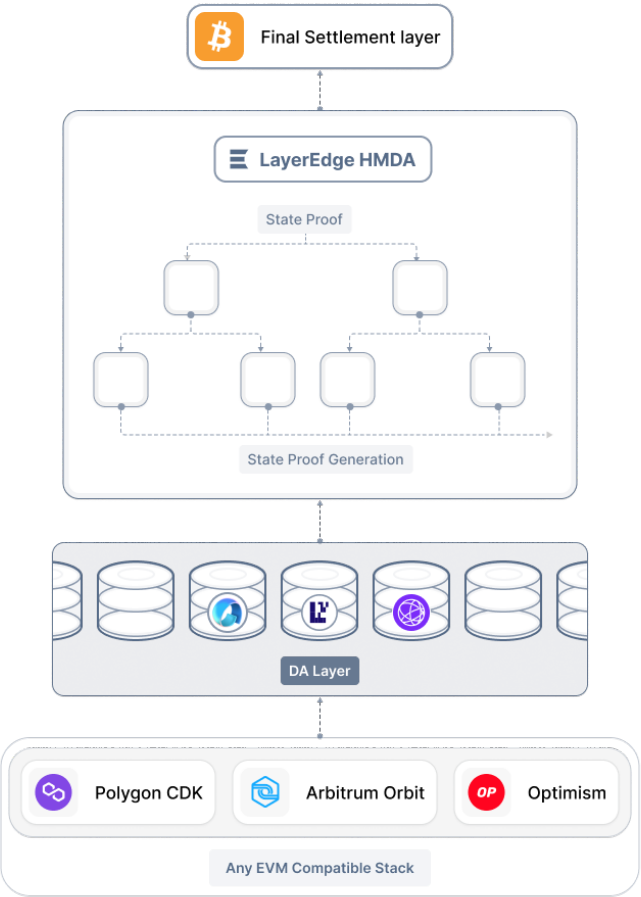
- The integration of Layer 2 solutions (e.g., Lightning Network) and various Layer 1 applications (e.g., sidechains like Liquid and RSK) on Bitcoin has dramatically increased the volume of transactions and data demands on the Bitcoin network.

2) Anticipated Data Congestion and Rising Gas Fees:

- As more applications and users leverage the Bitcoin network, the transaction volume is expected to outpace the capacity of the network, leading to data congestion and skyrocketing transaction fees.

3) Introduction to HMDA as a Solution:

- Hybrid Modular Data Availability (HMDA) emerges as a potential solution to these issues, offering a scalable and secure framework for data availability by integrating Bitcoin's robust security with modular data storage solutions.
- If all Layer 1 decentralized applications (dApps) and Layer 2 solutions post their data directly on Bitcoin, it would lead to severe data clogging, exacerbating congestion and dramatically increasing transaction fees, making it unsustainable for the network to handle the growing demand.



II. Overview of Hybrid Modular Data Availability (HMDA)

A. Definition and Purpose

1) What is HMDA?:

- HMDA is a framework designed to enhance data availability and scalability for blockchain networks. It combines modular data storage solutions with robust security measures, leveraging Bitcoin's immutability.

2) Objectives of HMDA:

- The primary objectives of HMDA are to maintain the security and immutability of Bitcoin while providing a scalable solution for data-heavy applications, addressing the limitations of both small block size and the increasing demand for data throughput.

B. Key Features of HMDA

1) Integration with Bitcoin's Security and Immutability:

- HMDA leverages Bitcoin's Proof of Work (PoW) consensus mechanism to ensure the integrity and resistance to censorship, capitalizing on Bitcoin's established security model.

2) Leveraging Proof of Work (PoW):

- By integrating PoW, HMDA inherits Bitcoin's immutability, making it highly resistant to attacks and ensuring that data stored within the framework is immutable.

3) Efficient Consensus Protocol Resistant to Censorship:

- HMDA employs a consensus protocol designed to be efficient and resistant to censorship, maintaining high levels of security and reliability.

4) Rapid Finality:

- One of the key benefits of the Hybrid DA Layer approach is the significant reduction in block time and finality. While Bitcoin has a block confirmation time of 10 minutes, the project's Hybrid DA Layer is designed to have block times of 12-20 seconds.
- **Efficiency** Faster block confirmation times allow the network to process transactions and execute smart contracts more efficiently, improving the overall user experience.
- **Responsiveness** The quick finality enables more responsive and interactive applications to be built on top of the blockchain, as users don't have to wait as long for their transactions to be confirmed.
- **Scalability** The faster block times help alleviate some of the scalability challenges faced by Bitcoin, as more transactions can be processed per unit of time.

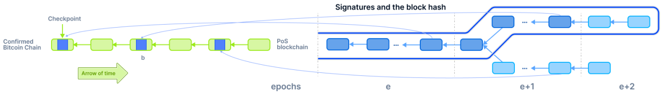
III. Bitcoin Timestamping

A. Importance of Bitcoin Timestamping

1) Long-Range Attacks:

- Blockchain security relies on validators who diligently validate each block, earning incentives or newly minted coins in return. Validators are required to stake a certain amount of cryptocurrency within the blockchain network, which can be slashed in response to dishonest or malicious behavior. Slashing, a penalty mechanism, aims to deter validators from engaging in activities that

could disrupt the blockchain network. Common reasons for slashing include Double-Signing, Liveness Violations, and Byzantine Behavior.
- Long-range attacks occur when a validator violates protocol and engages in malicious activities such as Double-Signing, where a corrupted validator attempts to approve a block multiple times. Another form of attack is altering the transaction history of an older block, known as a long-range attack.
- A critical loophole in this process arises post-unbonding, where validators can manipulate blocks created in the past without facing penalties beyond slashing, which becomes ineffective after the stake is unbounded.



2) *Mitigating Long-Range Attacks:*

- Bitcoin timestamping effectively mitigates long-range attacks by establishing checkpoints that invalidate any forks originating before them, thereby safeguarding the network's history from tampering.
- Honest validators contribute to this security measure by signing the hash of the last Proof of Stake (PoS) block of each epoch and posting both the hash and their signatures to Bitcoin as checkpoints. If an attacker attempts a long-range attack by creating an alternative chain from a distant point in the past, validators can compare this chain against the checkpointed state. This robust mechanism discourages attackers from tampering with historical data, as their attempts would be rejected in favor of the established and checkpointed blockchain state.

B. *Implementation of Checkpoints*

1) *Recording Block Hashes:*

- Checkpoints involve recording block hashes, creating a tamper-proof record of the network's state and ensuring that all participants can verify the integrity of the data.

2) *Invalidation of Forks Before Checkpoints:*

- These checkpoints invalidate any forks that originate before the checkpoint, ensuring the integrity and consistency of the blockchain and preventing malicious actors from rewriting history.

C. *Security Enhancements*

1) *Extra Layer of Data Integrity Verification:*

- Checkpoints provide an additional layer of data integrity verification, ensuring that data stored on the network is accurate and trustworthy, and providing an additional security measure against data tampering.

2) *Restoration of Data Using Full Nodes and Checkpoints:*

- Even in the event of network collapse, data can be restored using full nodes and checkpoints submitted on the Bitcoin blockchain, ensuring that the network can recover and maintain data integrity even under adverse conditions.

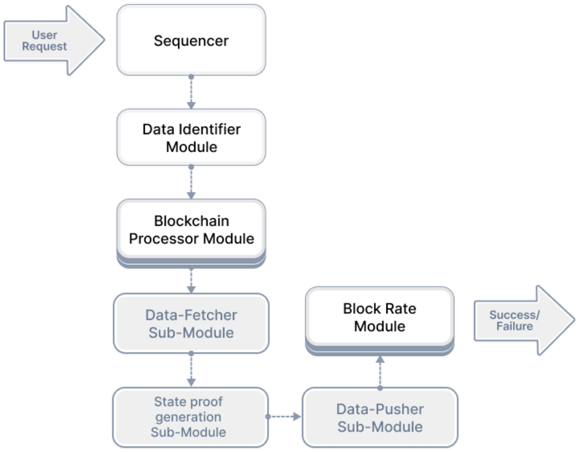
3) *Invalidation of Forks Before Checkpoints:*

- These checkpoints invalidate any forks that originate before the checkpoint, ensuring the integrity and consistency of the blockchain and preventing malicious actors from rewriting history.

IV. Architecture

A. *Sequencers*

- Sequencers play a crucial role in the Hybrid Modular Data Availability (HMDA) framework by generating state proofs and pushing them onto the Bitcoin blockchain using OP_RETURN transactions. The responsibilities of Sequencers include

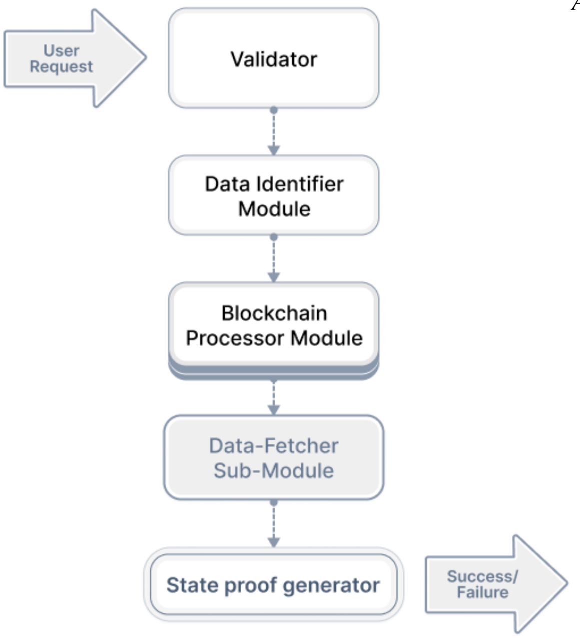


  - **State Proof Generation** Sequencers are responsible for compiling state proofs from Layer 1 decentralized applications (dApps) and Layer 2 solutions.
  - **Data Aggregation** They aggregate transaction data and state updates into a compact format suitable for inclusion in Bitcoin transactions.
  - **OP_RETURN Transaction Submission** Sequencers submit the compiled state proofs as OP_RETURN transactions on the Bitcoin blockchain. These transactions serve as a cryptographic commitment to the current state of the off-chain data.

  - **Timestamping** Utilizing Bitcoin's robust timestamping capabilities, Sequencers ensure that each state proof is securely anchored to the Bitcoin blockchain, providing a verifiable record of the state at a specific time.

B. Validators

- Validators in the HMDA architecture are responsible for verifying the state proofs posted on the Bitcoin blockchain. Their role includes



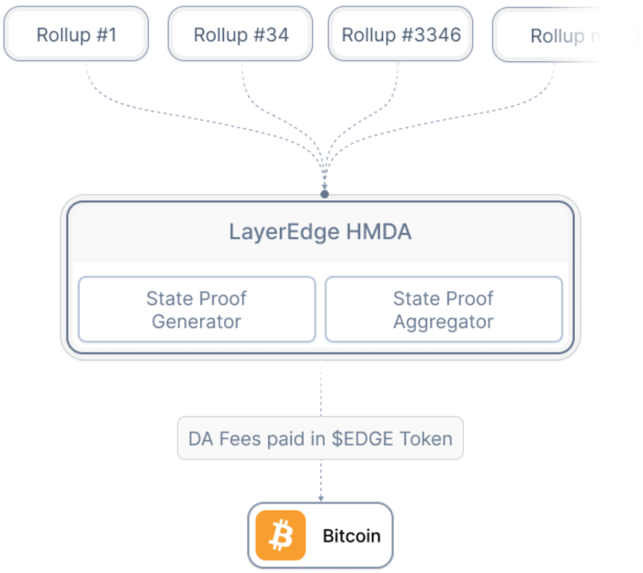
  - **State Proof Verification** Validators independently verify the integrity and correctness of state proofs submitted by Sequencers. This verification ensures that the data and transactions reflected in the state proofs are accurate and consistent.
  - **Consensus Mechanism** Validators participate in a consensus mechanism designed to achieve agreement on the validity of state proofs. This mechanism typically involves cryptographic validation and agreement among a set of distributed validators.
  - **Network Security** By validating state proofs, Validators contribute to the overall security and reliability of the HMDA framework. They help prevent malicious or erroneous data from being accepted as valid, thereby maintaining the integrity of the blockchain network.

- The collaboration between Sequencers and Validators forms a robust data availability layer that leverages Bitcoin's security and immutability while scaling to accommodate high volumes of data from Layer 1 and Layer 2 applications. This architecture ensures that the HMDA framework can handle significant data throughput while maintaining trust and security across the network.

V. Aggregated Proofs: A Cost-Effective Solution for Bitcoin Timestamping

A. Introduction

- In the realm of Bitcoin timestamping, the cost associated with recording state proofs over an extended period can be substantial. Bitcoin generates state proofs by hashing data approximately every 10 minutes through the mining of new blocks. This process, while ensuring the security and integrity of the blockchain, incurs significant expenses. To address this issue, we propose a solution aimed at significantly reducing these costs by employing aggregated proofs.



B. The Cost of Bitcoin Timestamping

- Bitcoin's state proofs are generated every 10 minutes, translating into a considerable financial burden over time. Let's break down the annual expenditure involved in this process.
- Taking into account a average transaction cost of $20

1) Cost Per Hour:

- Blocks per hour = 60 minutes / 10 minutes = 6 Blocks

- Cost per hour = 6 blocks * 20 =120

2) Cost Per Day:

- Blocks per day = 24 hours * 6 blocks = 144 blocks
- Cost per day = 144 blocks * 20 =2,880

3) Cost Per Week:

- Blocks per week = 7 days * 144 blocks = 1,008 blocks
- Cost per week = 1,008 blocks * 20 =20,160

4) Cost Per Month:

- Blocks per month = 30 days * 144 blocks = 4,320 blocks
- Cost per month = 4,320 blocks * 20 =86,400

5) Cost Per Year:

- Blocks per year = 365 days * 144 blocks = 52,560 blocks
- Cost per year = 52,560 blocks * 20 =1,051,200

- As illustrated, the yearly cost for Bitcoin timestamping amounts to a staggering $1,051,200. This calls for a more efficient approach to reduce these expenses.

C. The Proposed Solution Aggregated Proofs

- To mitigate these costs, we propose aggregating data into bundles of 10 and storing these aggregates on the Bitcoin blockchain. This method leverages the principle of aggregated proofs to achieve significant cost reduction.

1) Cost Per Hour:

- Cost per hour = 6 blocks * 20/10 =12

2) Cost Per Day:

- Cost per day = 144 blocks * 20/10 =288

3) Cost Per Week:

- Cost per week = 1,008 blocks * 20/10 =2,016

4) Cost Per Month:

- Cost per month = 4,320 blocks * 20/10 =8,640

5) Cost Per Year:

- Cost per year = 52,560 blocks * 20/10 =105,120

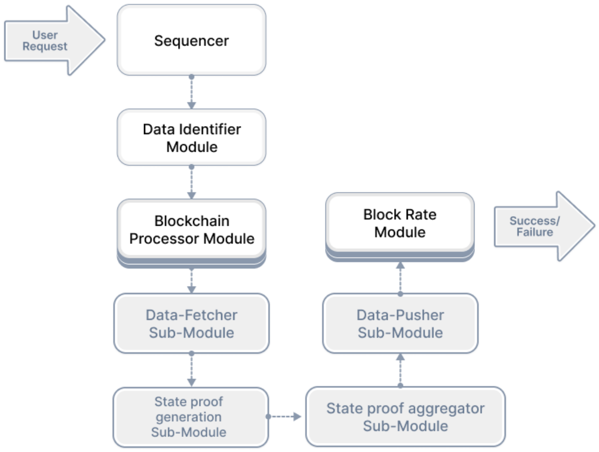
- Despite the significant cost reduction, the implementation of aggregated proofs introduces some challenges, particularly in the validation process. Validators must shift from single to double validations, ensuring both the integrity of aggregated proofs and the accuracy of individual proofs.

D. The Technical Breakdown How It Works

- The proposed solution leverages zero-knowledge proofs (ZKPs) to enhance the efficiency and security of Bitcoin timestamping. Here's a detailed breakdown of the process

1) Creation of Individual Zero-Knowledge Proofs (ZKPs):

- Each piece of data or transaction generates an individual zero-knowledge proof. A ZKP allows one party to prove to another that a statement is true without revealing any information beyond the veracity of the statement itself. In this context, the ZKP verifies the integrity and validity of each transaction without exposing its details.



2) Aggregation of Zero-Knowledge Proofs:

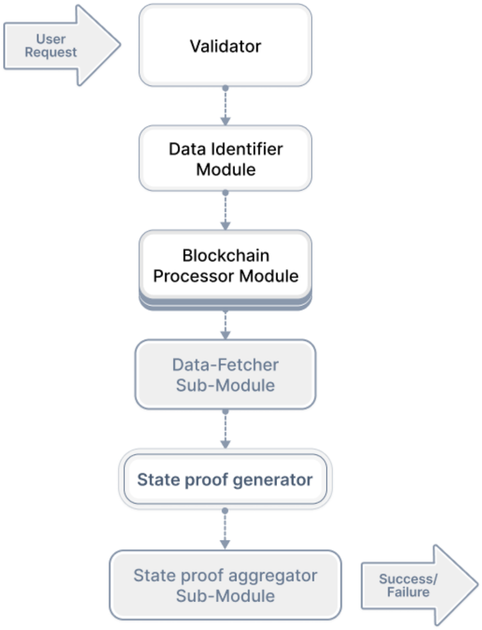
- Once individual ZKPs are created, they are aggregated into a single proof. This aggregated proof represents the combined validity of all included data blocks. The aggregation process ensure the integrity and non-repudiation of the combined proof.

3) Settlement on Bitcoin:

- The aggregated proof is then settled on the Bitcoin. Instead of recording each individual proof, only the aggregated proof is included in a new block. This significantly reduces the number of transactions recorded on the bitcoin, thus lowering the associated costs.

4) Verification of Aggregated Proof Integrity:

- Validators must verify that the aggregated proof accurately represents the data it claims to include. This involves confirming that the provided hash or proof matches the computed value from the included data blocks, ensuring the aggregation process is secure and untampered.



5) *Data Accuracy and Validity:*

- Validators must also confirm the accuracy and validity of each data block within the aggregation. This involves ensuring that each data block doesn't have any data inconsistencies.

E. Role of Zero-Knowledge Proofs

- Aggregated proofs often employ zero-knowledge proofs (ZKPs) to verify data integrity without revealing the underlying data. ZKPs enable validators to confirm that the aggregated data matches the provided hash without inspecting each data block individually. Zero-knowledge proofs add a layer of complexity to data verification, allowing for secure and private validation of aggregated data.

F. Summary

- In summary, the introduction of aggregated proofs in Bitcoin timestamping offers a substantial cost-saving opportunity by consolidating transactions into bundles of 10. This approach reduces annual expenses by over 90%, from $1,051,200 to $105,120. However, it requires validators to adapt to double validations, ensuring both the integrity of aggregated proofs and the accuracy of individual proofs. The use of zero-knowledge proofs further enhances data verification, providing a secure and efficient solution for reducing Bitcoin timestamping costs. The positive impact of adopting aggregated proofs is undeniable, presenting a cost-effective and efficient solution for Bitcoin timestamping while maintaining the integrity and security of the blockchain.

VI. The Benefits of HMDA

A. Combining the Best of Both Worlds

1) *Storing Large Data on Modular DA:*

- **Optimized Storage Efficiency and Scalability**: HMDA allows for the storage of large amounts of data on modular data availability solutions, optimizing storage efficiency and scalability. This ensures that the network can handle high volumes of data without compromising performance.

- **Enhanced Network Performance**: By utilizing modular data availability, HMDA ensures that data storage is both efficient and scalable, enhancing overall network performance and capacity.

2) *Storing State Proofs on Bitcoin:*

- **Integrity and Security**: By storing state proofs on the Bitcoin blockchain, HMDA ensures that the data's integrity and security are maintained. This leverages Bitcoin's immutability and robust security model to protect critical data.

- **Cost Efficiency with Aggregated Proofs**: The introduction of aggregated proofs significantly reduces the cost of storing state proofs on Bitcoin. Aggregated proofs combine multiple state proofs into a single proof, which is then stored on the Bitcoin blockchain. This method reduces the number of transactions recorded, thereby lowering costs by over 90%, from $1,051,200 to $105,120 annually.

B. Guarding Against Long-Range Attacks

1) *Checkpoints and Timestamping Mechanisms:*

- **Robust Protection**: The use of checkpoints and timestamping mechanisms provides robust protection against long-range attacks. This ensures network stability and security by invalidating any forks that originate before the checkpoints.

- **Aggregated Proofs for Enhanced Security**: Aggregated proofs further enhance security by ensuring that state proofs are securely stored and validated. This involves creating individual zero-knowledge proofs for each transaction, aggregating these proofs, and storing the aggregated proof on the Bitcoin blockchain. Validators then ensure the integrity and accuracy of both the aggregated proof and individual transactions.

2) *Enhanced Security and Resilience:*

- **Increased Network Robustness**: These mechanisms enhance the overall security and resilience of the network, making it more robust against potential threats. This ensures that the network can maintain data integrity even under adverse conditions.

- **Zero-Knowledge Proofs for Privacy and Security**: The use of zero-knowledge proofs (ZKPs) within aggregated proofs adds an additional layer of security and privacy. ZKPs enable validators to confirm the integrity of aggregated data without revealing the underlying details, ensuring both security and privacy of the transactions.

VII. Conclusion

A. *Recap of HMDA's Advantages*

1) *Integration with Bitcoin's Security Features:*

- HMDA integrates seamlessly with Bitcoin's security features, leveraging its PoW consensus and immutability to provide a secure and scalable data availability solution.

2) *Cost Reduction through Aggregated Proofs:*

- The implementation of aggregated proofs in Bitcoin timestamping introduces a significant cost-saving opportunity by consolidating transactions into bundles of 10. This method reduces annual expenses by over 90%, from $1,051,200 to $105,120, while maintaining the integrity and security of the blockchain. Aggregated proofs enhance data verification efficiency, making them a valuable addition to HMDA's capabilities.

3) *Efficient and Secure Data Availability:*

- HMDA provides a scalable and secure solution for data availability, addressing the challenges posed by increasing data demands and ensuring that the network can handle high volumes of data without compromising performance.

B. *Future Implications*

1) *Potential Impact on Bitcoin and Blockchain Technology:*

- HMDA has the potential to significantly impact Bitcoin and the broader blockchain ecosystem by providing a scalable and secure data availability solution, paving the way for more complex and data-intensive applications.
- The cost-saving benefits of aggregated proofs can further enhance the economic feasibility of data-intensive blockchain applications, encouraging innovation and adoption within the ecosystem.

2) *Prospects for Wider Adoption of HMDA:*

- The innovative approach of HMDA paves the way for its wider adoption, offering substantial benefits for various blockchain applications and contributing to the overall advancement of blockchain technology.
- By addressing both security and cost-efficiency, HMDA with aggregated proofs can attract a broader range of users and developers, fostering a more robust and versatile blockchain environment.

References

[1] Buterin, V. (2024, May 31). Some reflections on the Bitcoin block size war. https//vitalik.eth.limo/general/2024/05/31/blocksize.html

[2] Nakamoto, S. (2008). Bitcoin A peer-to-peer electronic cash system.

[3] Christian Decker, Rusty Russell, and Olaoluwa Osuntokun. 2018. eltoo A Simple Layer2 Protocol for Bitcoin. https//blockstream.com/eltoo.pdf.

[4] Christian Decker and Roger Wattenhofer. 2015. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In Stabilization, Safety, and Security of Distributed Systems - 17th International Symposium, SSS 2015, Edmonton, AB, Canada, August 18-21, 2015, Proceedings. Springer, 3–18. https //doi.org/10.1007/978-3-319-21741-31

[5] Christoph Egger, Pedro Moreno-Sanchez, and Matteo Maffei. 2019. Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment- Channel Networks. In Proceedings of the 2019 ACM SIGSAC Conference on Com- puter and Communications Security, CCS 2019, London, UK, November 11-15, 2019. ACM, 801–815. https//doi.org/10.1145/3319535.3345666

[6] Mike Hearn. 2013. Micro-payment channels implementation now in bitcoinj. https//bitcointalk.org/index.php?topic=244656.0. Last accessed on September 20, 2023.

[7] Joseph Poon and Thaddeus Dryja. 2016. The Bitcoin Lightning Network Scalable Off-Chain Instant Payments, Version 0.5.9.2. https//lightning.network/lightning- network-paper.pdf. Last accessed on September 20, 2023.

VIII. Glossary

- **Blocksize War** A historical conflict within the Bitcoin community focused on the optimal block size for the Bitcoin blockchain, which concluded with a preference for smaller block sizes and the adoption of Segregated Witness (SegWit).
- **Layer 1 Applications** Decentralized applications (dApps) that run directly on the base layer of a blockchain, such as Bitcoin.
- **Layer 2 Solutions** Secondary chain or protocols built on top of a blockchain to improve its scalability and efficiency, such as the Lightning Network.
- **Data Congestion** The overload of transactions and data on a blockchain, leading to slower processing times and higher fees.
- **Gas Fees** Transaction fees required to process and validate transactions on a blockchain network.
- **Hybrid Modular Data Availability (HMDA)** A framework combining modular data storage solutions with Bitcoin's security features to enhance data availability, scalability, and security for blockchain networks.
- **Proof of Work (PoW)** A consensus mechanism used by Bitcoin that requires network participants (miners) to perform computational work to validate transactions and secure the network.
- **Consensus Protocol** A system used to achieve agreement on a single data value among distributed processes or systems, ensuring data consistency and security.
- **Bitcoin Staking** A process where Bitcoin holders can participate in Proof of Stake (PoS) blockchains by staking their assets to secure the network, eliminating the need for third-party custody services.
- **Proof of Stake (PoS)** A consensus mechanism where validators are chosen to produce blocks based on the

amount of cryptocurrency they hold and are willing to ”stake” as collateral.

- **Extractable One-Time Signatures (EOTS)** Cryptographic signatures that reveal the secret key if duplicated across different blocks, ensuring validator accountability.
- **Bitcoin Timestamping** A method of recording block hashes and staking set votes on the Bitcoin blockchain to create tamper-proof checkpoints, enhancing security against long-range attacks.
- **Checkpoints** Points in the blockchain where data is recorded to prevent forks and ensure network integrity.
- **Long-Range Attacks** Attacks where an adversary attempts to rewrite a blockchain’s history by creating an alternative chain fork, typically after the unbonding period in PoS networks.
- **Rapid Finality** The quick confirmation of transactions in a blockchain network, significantly reducing block times from minutes to seconds.
- **Block Time** The time it takes to generate a new block in a blockchain, which affects transaction confirmation speed.
- **Aggregated Proofs:** A method of combining multiple proofs into a single, compact proof to reduce the cost and data size required for verification on the blockchain.
- **Zero-Knowledge Proofs (ZKPs):** Cryptographic protocols that allow one party to prove to another that a statement is true without revealing any information beyond the validity of the statement.
- **State Proofs:** Cryptographic proofs that confirm the state of data at a given point in time on the blockchain, ensuring its integrity and authenticity.
- **Mining:** The process of using computational power to solve cryptographic puzzles, which in turn validates transactions and adds them to the blockchain, creating new blocks.
- **Validators:** Participants in the blockchain network responsible for verifying and validating transactions and blocks to ensure the network’s security and integrity.
- **Hashing:** The process of converting an input (or ’message’) into a fixed-size string of bytes, typically for the purpose of data verification and integrity.
- **Transaction Costs:** Fees paid by users to have their transactions included in a new block on the blockchain. These costs compensate miners for the computational power used in mining.
- **Data Integrity:** The accuracy and consistency of data over its lifecycle, ensuring that data remains unaltered and trustworthy.
- **Data Block:** A unit of data storage in a blockchain, containing transaction records and a reference to the previous block, forming a chain of blocks.
- **Non-repudiation:** Assurance that someone cannot deny the validity of their digital signature on a document or a message, ensuring the authenticity and integrity of the data.
- **Immutability:** The characteristic of a blockchain that ensures once data has been added to a block and the block is added to the chain, the data cannot be changed or tampered with.