Layer Edge: Bitcoin's First Optimistic Rollup

*

Layer Edge Team
info@layeredge.io

***Abstract*—Layer Edge is poised to redefine the blockchain landscape by harmonizing the unparalleled security and decentralization attributes of Bitcoin with the dynamic smart contract functionality and composability of Ethereum. We introduce a layer 2 solution that achieves full Ethereum Virtual Machine (EVM) equivalence, enabling a wide array of decentralized finance (DeFi) applications and smart contract capabilities that were previously unattainable on Bitcoin's network. Aimed at being the fastest, most cost-effective, and user-friendly blockchain, Layer Edge is designed to attract a broad spectrum of developers and users, fostering a new era of blockchain innovation. Our staking mechanism is set to create unprecedented liquidity, enhancing network efficiency and scalability while ensuring seamless and secure interoperability across various blockchain networks. Layer Edge stands at the forefront of blockchain evolution, offering a robust solution that combines the best of Bitcoin and Ethereum in a single, cohesive ecosystem.**

I. Introduction

Welcome to the Layer Edge white paper, a comprehensive document that outlines our vision, technology, and the groundbreaking approach we are taking to bridge the best aspects of Bitcoin and Ethereum. Layer Edge is not just layer 2; it's a paradigm shift in how we perceive and interact with blockchain technology.

Bitcoin, the progenitor of the cryptocurrency revolution, has set the standard for decentralized financial systems with its robust blockchain technology. However, its inherent limitations, such as constrained block sizes and slower transaction speeds, have sparked a quest for innovative solutions that can unlock its full potential as a decentralized global currency. Concurrently, Ethereum has redefined the blockchain landscape by introducing a Turing-complete programming language, fostering an ecosystem brimming with decentralized applications that test the limits of its scalability.

While Ethereum envisions a future of EVM-compatible chains stacked to enhance scalability, with its parent chain as the ultimate settlement layer, it grapples with its own set of challenges, including centralization concerns and scalability bottlenecks. In this dynamic landscape, the quest for a foundational layer that combines the security and decentralization of Bitcoin with the flexibility and scalability of Ethereum is more pressing than ever.

Layer Edge emerges as a groundbreaking solution in this context, offering a layer 2 protocol that leverages Bitcoin's unmatched security and Ethereum's smart contract versatility. Unlike existing layer 2 solutions, which often involve trade-offs in terms of decentralization or scalability, Layer Edge is designed to offer the best of both worlds, enabling rapid, cost-effective, and scalable applications without compromising on decentralization.

Our approach diverges from traditional models by eschewing the UTXO model of Bitcoin in favor of an account-based model akin to Ethereum's, facilitating seamless integration with Ethereum's rich ecosystem of applications and smart contracts. Layer Edge nodes will operate in tandem with Bitcoin core, ensuring a robust and decentralized network that is both fast and user-friendly.

At Layer Edge, we are not just building a bridge between Bitcoin and Ethereum; we are crafting a new paradigm for blockchain technology, one that promises to enhance liquidity, foster innovation, and expand the horizons of what decentralized systems can achieve. This white paper delves into the architecture of Layer Edge, exploring how our unique solution stands to revolutionize the blockchain space by providing a versatile, scalable, and secure Layer 2 for the next generation of decentralized applications.

II. Philosophy

The landscape of blockchain technology is in a constant state of evolution, with Layer Edge standing at the forefront of this transformative journey. Our philosophy is rooted in the belief that the true potential of Bitcoin's security and Ethereum's flexibility can be unlocked through a harmonious integration, leading to a blockchain ecosystem that is not only robust and decentralized but also scalable and user-friendly.

A. Layer Edge: Bridging Bitcoin and Ethereum

At the heart of Layer Edge's philosophy is the vision to transcend traditional blockchain boundaries by creating a second-layer solution that seamlessly blends the strengths of Bitcoin and Ethereum. Unlike conventional Layer 2 solutions that often operate within the limitations of their parent chains, Layer Edge redefines this narrative by establishing a Layer 2 where Bitcoin's unparalleled security and Ethereum's

Archived copy · cryp2nova.com

dynamic smart contract capabilities coalesce, fostering a new realm of possibilities for decentralized applications and financial instruments.

B. Asset-Driven Innovation

Layer Edge adopts an asset-driven approach, emphasizing the active role of Bitcoin within our ecosystem. Our layer 2 is not just a passive layer atop Bitcoin; it is an active participant, leveraging Bitcoin's liquidity and security to enhance network efficiency and scalability. This approach not only amplifies the value of Bitcoin within our ecosystem but also opens up new avenues for BTC/BRC20 holders to engage with and benefit from the burgeoning world of decentralized finance.

C. Interoperability and EVM Compatibility

Understanding the pivotal role of interoperability in the future of blockchain, Layer Edge is designed to be fully EVM-compatible, ensuring seamless interaction with Ethereum's vast ecosystem of applications and services. This compatibility extends the utility of Bitcoin, enabling it to participate in a wider range of decentralized applications and financial products, thereby enriching its use cases and value proposition.

D. Activating Bitcoin in the DeFi Ecosystem

Layer Edge recognizes the conservative nature of Bitcoin holders regarding asset mobility. Our layer 2 is designed to mobilize Bitcoin, transforming it from a static asset into a dynamic participant in the DeFi space. By providing secure and efficient mechanisms for Bitcoin holders to engage with DeFi, Layer Edge not only enhances the liquidity and utility of Bitcoin but also opens up new opportunities for yield generation and financial innovation.

E. Summary

In conclusion, Layer Edge embodies a forward-thinking philosophy that seeks to unify the best aspects of Bitcoin and Ethereum, creating a blockchain ecosystem that is secure, scalable, and synergistic. Our commitment to asset-driven innovation, interoperability, transparency, and the active mobilization of Bitcoin paves the way for a new era in blockchain technology, where the possibilities are as limitless as the potential of the decentralized world we are building.

III. Design Choices

Layer Edge's architectural choices are meticulously crafted to address the blockchain ecosystem's critical challenges, merging Bitcoin's robust security and Ethereum's advanced smart contract capabilities. This section delineates the strategic decisions underpinning Layer Edge's design, reflecting a deep engagement with the core technological confrontations in the blockchain landscape.

A. Decentralization and Security: Opting for Bitcoin's Foundation

1) - Choice of Base Layer: Selecting Bitcoin as the foundational layer underscores a commitment to unparalleled security and decentralization, acknowledging Bitcoin's proven resilience against external pressures and its role as a benchmark in the blockchain domain.

2) - Implications: This choice ensures that Layer Edge inherits Bitcoin's robust security framework, providing a solid foundation for building advanced functionalities on top.

B. Smart Contract Integration: Leveraging Ethereum's Ecosystem

1) - EVM Compatibility: Ensuring full compatibility with the Ethereum Virtual Machine (EVM) allows Layer Edge to tap into Ethereum's mature ecosystem, offering developers a familiar and rich environment for dApp creation.

2) - Rationale: This decision aligns with the industry's recognition of Solidity and the EVM's proven track record, ensuring that Layer Edge benefits from an established developer base and a wealth of existing applications.

C. Consensus Mechanism: Evolving from Bitcoin's Proof of Work to Optimistic Rollup

1) Optimistic Rollup: Layer Edge is built on Arbitrum stack and uses Optimistic Rollup. This is aimed at enhancing the platform's scalability and efficiency while significantly reducing transaction costs. By adopting Optimistic rollup, Layer Edge will enable faster transaction throughput and lower latency, all while maintaining a high level of security and decentralization.

2) Bitcoin as a Security Layer: In this next phase, Layer Edge intends to use Bitcoin not just as a reference for security practices but as an active security layer. The integration of Optimistic Rollup will allow Layer Edge to leverage the security and immutability of Bitcoin's blockchain, further fortifying its network against potential threats and ensuring the integrity of its transactions.

3) Outcome: The adoption of Optimistic Rollup signifies Layer Edge's commitment to innovation and scalability, preparing the platform for a future where it can support a higher volume of transactions and diverse applications. This strategic evolution from Proof of Work to Optimistic Rollup reflects Layer Edge's forward-thinking approach, ensuring that it remains at the forefront of blockchain technology while continuing to benefit from the security and reliability of Bitcoin's network.

CRYP2NOVA

Archived copy · cryp2nova.com

D. Summary

Layer Edge's design choices are a strategic amalgamation of Bitcoin's and Ethereum's best features, aimed at propelling the blockchain ecosystem forward. These choices reflect a nuanced understanding of the blockchain landscape's challenges and opportunities, positioning Layer Edge as a pioneering Layer 2 that bridges the gap between security, scalability, and functionality.

IV. Optimistic Rollup Architecture

Layer Edge is set to revolutionize Bitcoin's scalability by implementing an innovative layer 2 scaling solution, utilizing optimistic roll-up technology, a concept more commonly associated with Ethereum. This approach allows for off-chain transaction execution while ensuring data availability through a Hybrid DA system, thereby significantly boosting Bitcoin's transaction capacity without compromising its security. In the following sections, we will delve into the architecture, functionality, and advantages of Layer Edge, demonstrating its seamless integration with Bitcoin via BitVM, all while preserving the network's foundational consensus rules.

A. Overview

Layer Edge introduces an innovative layer 2 protocol designed to enhance Bitcoin's transaction throughput without compromising its core principles. By processing transactions off-chain and only interacting with the Bitcoin blockchain for finality and security checks, Layer Edge significantly alleviates the load on the main chain.

B. Components

1) Off-chain Ethereum Virtual Machine (EVM): The off-chain VM, an EVM-equivalent engine, is the heart of Layer Edge's transaction processing. It is a separate computational environment where transactions are executed and state changes occur independently of the Bitcoin blockchain. This VM is designed to be efficient and scalable, capable of handling a high volume of transactions that would otherwise burden the Bitcoin network.

a) Execution Environment: The VM provides a secure and isolated environment for executing transactions, ensuring they are processed accurately and efficiently.

b) State Management: It maintains a separate state for Layer Edge, tracking account balances, smart contract states, and other relevant data.

2) Data Availability Layer: Layer Edge employs a Hybrid DA mechanism to ensure the availability of off-chain transaction data without bloating the Bitcoin blockchain.

a) Decentralized Storage: Utilizes Layer Edge Hybrid DA to store transaction data, ensuring it is accessible for validation and auditability.

b) Data Compression: Before storage, data is compressed to minimize its footprint, enhancing efficiency and reducing costs.

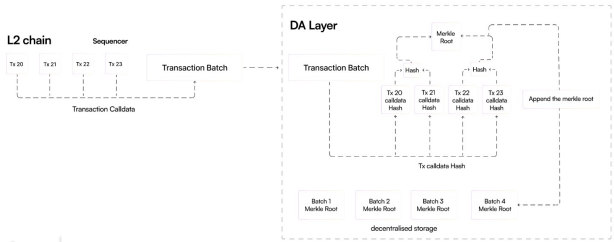


Fig. 1. Data Availability Layer

3) On-chain Contracts and BitVM: Layer Edge's interaction with the Bitcoin blockchain is facilitated through BitVM, which allows for the execution of complex contracts without altering Bitcoin's consensus rules.

a) BitVM Integration: BitVM serves as the bridge between Layer Edge and Bitcoin, verifying the correctness of off-chain computations and enabling the execution of fraud proofs.

b) On-chain Contracts: These contracts, executed via BitVM, manage the submission of batched transaction summaries, handle disputes, and ensure the integrity of the rollup.

C. Operation

1) Transaction Processing: Layer Edge processes transactions in batches, significantly increasing throughput.

a) Transaction Aggregation: Transactions are collected and executed in the off-chain VM, where they are aggregated into batches for efficient processing. Transactions $T_1, T_2, ..., T_n$ are collected and executed in the off-chain VM, where they are aggregated into batches for efficient processing. A batch B can be represented as:

$$B = T_1, T_2, ..., T_n \tag{1}$$

b) Batch Processing: Each batch of transactions is processed collectively, allowing Layer Edge to spread the computational and storage costs over many transactions, thus reducing the overall cost per transaction. The state transition function f applied to the state root and a transaction updates the state root as follows:

$$S_n = f(...f(f(S_0, T_1), T_2)..., T_n) \tag{2}$$

Archived copy · cryp2nova.com

where S_0 is the initial state root, and S_n is the new state root after processing the batch.

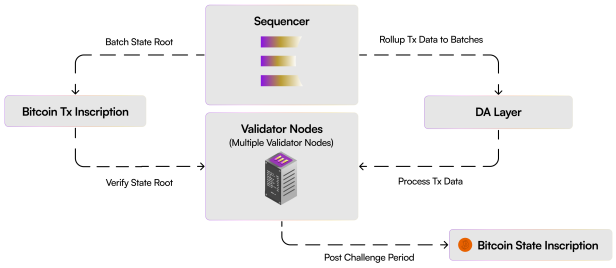


Fig. 2. Optimistic Rollup Architecture

2) Data Posting and Compression: After processing, the results are efficiently stored and summarized for the Bitcoin blockchain.

a) Data Compression: Transaction data is compressed using advanced algorithms to reduce its size before being stored in the decentralized DA layer.

b) Batch Summarization: A summary of each batch, including state changes and transaction outcomes, is generated and posted to the Bitcoin blockchain via BitVM. This includes the submission of the new state root S_n and the batch B to the blockchain:

$$Submit(B, S_n) \tag{3}$$

3) Fraud Proofs: Layer Edge utilizes a challenge period during which the correctness of the batched transactions can be disputed.

a) Challenge Window: After a batch is posted, there is a predefined period during which any observer can submit a fraud proof if they detect inconsistencies. This is represented as:

$$C(S_{i-1}, T_i, S_i) \tag{4}$$

where C is the challenge function, and S_{i-1}, T_i, and S_i represent the state before the transaction, the transaction itself, and the state after the transaction, respectively.

b) Fraud Proof Execution: If a challenge is made, BitVM facilitates the execution of the fraud proof on the Bitcoin blockchain, ensuring any disputes are resolved transparently and securely.

D. Benefits

1) Scalability: Layer Edge significantly enhances Bitcoin's transaction capacity by offloading the bulk of transaction processing from the main chain.

a) High Throughput: By batching transactions and processing them off-chain, Layer Edge can handle a much higher volume of transactions than the Bitcoin network alone.

b) Reduced Block Space Usage: The rollup only posts compressed batch summaries to the Bitcoin blockchain, conservatively using block space.

2) Security: Layer Edge leverages the underlying security of Bitcoin while introducing additional mechanisms to safeguard its rollup layer.

a) Inheritance of Bitcoin's Security: By anchoring its finality and dispute resolution on the Bitcoin blockchain, Layer Edge benefits from the same level of security that protects Bitcoin.

b) Enhanced Security Measure: The use of Hybrid DA for data availability and BitVM for fraud proofs adds layers of security, ensuring the integrity and reliability of the rollup.

3) Cost Efficiency: The rollup model significantly reduces the cost per transaction by distributing the costs of batch processing and data storage across many transactions.

a) Economies of Scale: Batching transactions allows Layer Edge to spread the costs of computation and data storage across multiple transactions, reducing the cost per transaction.

b) Optimized Data Storage: Using hybrid DA and data compression minimizes the costs associated with data availability, further enhancing cost efficiency.

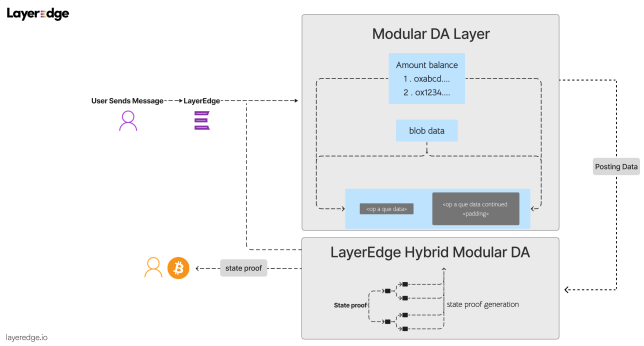
E. Summary

Layer Edge represents a significant step forward in the scalability and efficiency of Bitcoin. By leveraging optimistic rollup technology, hybrid DA, and BitVM, Layer Edge offers a scalable, secure, and cost-effective solution for Bitcoin transactions, paving the way for broader adoption and more innovative applications on the Bitcoin network.

V. Hybrid Data Availability Layer

We plan to utilize Data Availability (DA) Layer, such as Avail or Celestia, to store the actual block data and store it's state root on Bitcoin. This provides a scalable and efficient way to store the large amounts of data required for the blockchain, without being constrained by the limitations of the Bitcoin network.

Archived copy · cryp2nova.com



A. Bitcoin Integration

While the block data is stored on the separate DA Layer, the we plan to post the state root of each block onto the Bitcoin blockchain. This serves as a reliable verification mechanism, as the state root acts as a cryptographic commitment to the entire block data.

By posting the state root to Bitcoin, we can leverage Bitcoin's robust security and decentralization to provide a trustless way for users to verify the integrity of the data stored on the DA Layer.

B. Rapid Finality

One of the key benefits of the Hybrid DA Layer approach is the significant increase in block time and finality. While Bitcoin has a block time of 10 minutes, the project's Hybrid DA Layer is designed to have block times of 12-20 seconds.

This rapid finality provides several advantages:

1) Efficiency: : Faster block times allow the network to process transactions and execute smart contracts more efficiently, improving the overall user experience.

2) 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.

3) 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.

C. Modular Approach

Initially, we planned to create a custom hybrid DA solution specifically for its use case of an Optimistic Rollup on Bitcoin. However, the team recognized that Data Availability would likely become a bottleneck for most Rollups built on Bitcoin, as they would all be constrained by using only Bitcoin as the DA layer.

To address this, we decided to make its hybrid DA layer a modular solution. This allows the project to offer its DA layer as a service that other Rollup projects can utilize, rather than forcing them to rely solely on Bitcoin for their DA needs.

By taking this modular approach, we can provide a more flexible and scalable DA solution that can be adopted by a wider range of Rollup implementations on Bitcoin. This helps to address the potential scalability challenges faced by the broader Bitcoin Rollup ecosystem.

VI. Conclusions

In conclusion, Layer Edge stands as a transformative force in the blockchain domain, ingeniously merging Bitcoin's security and decentralization with Ethereum's smart contract versatility and scalability. Our white paper has delineated Layer Edge's innovative approach, showcasing a Layer 2 solution that not only enhances Bitcoin's functionality but also opens new avenues for DeFi and blockchain applications. By integrating a fully EVM-compatible environment, Layer Edge provides a fertile ground for developers and users, fostering a new wave of innovation and utility in the blockchain space.

Our design choices, rooted in a deep understanding of blockchain's core challenges, strategically combine the best of Bitcoin and Ethereum, ensuring robust security, scalability, and user-centricity. Layer Edge's protocol, with its advanced features and commitment to energy efficiency, sets a new standard for blockchain interactions, offering a seamless and cost-effective experience.

Looking ahead, Layer Edge's adoption of optimistic rollup architecture signifies a pivotal leap towards unprecedented scalability and efficiency for Bitcoin, reinforcing our vision of a more accessible, versatile, and interconnected blockchain ecosystem. As we move forward, Layer Edge remains committed to pushing the boundaries of blockchain technology, driving innovation, and shaping a future where the full potential of Bitcoin is realized, creating a more decentralized, secure, and inclusive digital world.

Acknowledgment

We express our heartfelt gratitude to the Bitcoin and Ethereum communities for their foundational work and continuous innovation, which have inspired and informed the development of Layer Edge. Special thanks to the dedicated developers, engineers, validators, and network participants whose expertise and commitment are vital to our progress. We also acknowledge the invaluable insights from the academic and research community, as well as the support and feedback from our early adopters and community members. Together, we are pushing the boundaries of blockchain technology, and we are deeply thankful for the collective effort that has made Layer Edge a reality.

References

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, URL: https://bitcoin.org/bitcoin.pdf-(17.07. 2019), 2008.
[2] Robin Linus, BitVM: Compute Anything on Bitcoin, URL: https://bitvm.org/bitvm.pdf-(12.12. 2023).

Archived copy · cryp2nova.com