B^2: THE MOST PRACTICAL BITCOIN LAYER-2 NETWORK *

B^2 **Team**
contact@bsquared.network

ABSTRACT

The B^2 Litepaper highlights Bitcoin's scalability challenges and introduces the B^2 Network, a Layer-2 solution that bolsters transaction speed and broadens application diversity without sacrificing security. B^2 is the first zero-knowledge proof verification commitment rollup on Bitcoin. Leveraging rollup technology, the B^2 Network provides a platform capable of running Turing-complete smart contracts for off-chain transactions, which enhances transaction efficiency and minimizes costs. Additionally, zero-knowledge proof technology is employed in tandem with gate commitment and challenge-response of Taproot to guarantee transactional privacy and security during confirmation on Bitcoin. The network's objective is to metamorphose Bitcoin into a versatile platform, paving the way for groundbreaking applications such as DeFi, NFTs, and other decentralized systems. Overall, the B^2 Network epitomizes a harmonized progression, upholding Bitcoin's core values while navigating the future digital asset landscape.

***K*eywords** Bitcoin · Layer-2 · ZK-Rollup · ZK Proof Commitment Rollup · Confirmation on Bitcoin

1 Background

Bitcoin[1], since its inception in 2008, has reshaped finance with its decentralization, trustless operations, and transparent ledger. Its rise in adoption brought both rewards and challenges, especially scalability. The blockchain's block size limit, while ensuring efficient validations, restricts transaction throughput. As user numbers surged, this resulted in higher fees and elongated confirmations.

Various remedies were suggested, including block size expansion, but that risked centralization. Hence, the search began for ways to upscale without jeopardizing decentralization. Enter "Layer-2" solutions: secondary protocols on existing blockchains (Layer 1) aiming to boost transaction rates without changing the base layer. These promise Bitcoin transactions that are faster, more affordable, yet secure.

A notable example is the Lightning Network[2], enabling "off-chain" transactions for heightened scalability. Yet, it's among many evolving Layer-2 technologies with goals like smart contract integration or cross-blockchain compatibility. Beyond scalability, Layer-2 fosters innovation, paving the way for microtransactions, immediate settlements, and Bitcoin's decentralized finance (DeFi).

This whitepaper delves into a novel Layer-2 Bitcoin solution, its mechanics, advantages, challenges, and its future potential. It emphasizes Bitcoin's evolution, underscoring its adaptability. This new Layer-2 solution ensures Bitcoin's sustained significance and functionality in the coming decades.

2 Why Bitcoin needs Layer-2

For Bitcoin, current limitations mainly relate to technology and asset liquidity.

*November 14, 2023, v0.2.0

2.1 Technical Aspects

Performance Issues of Bitcoin Bitcoin was originally designed with a primary focus on decentralization and security, rather than peak performance. Due to its 10-minute block intervals and a limited block size, Bitcoin's throughput is heavily restricted, making it capable of processing only a few transactions per second. As the user base of Bitcoin has expanded over time, this problem has become increasingly glaring, leading to network congestion, transaction delays, and surging transaction fees.

Bitcoin's Lack of Turing Completeness Bitcoin's scripting language was deliberately designed to be non-Turing complete, aiming to bolster the network's security and simplicity. This means that Bitcoin can't natively execute intricate smart contracts, thereby limiting its potential in the decentralized application domain.

Transaction Fee Concerns With growing network traffic, users have to pay higher transaction fees to ensure that their transactions receive priority. This dynamic renders small-value or frequent transactions economically impractical.

2.2 Asset Landscape

BTC Asset Liquidity Issues While BTC is widely acknowledged as the "gold" among digital assets, its liquidity faces considerable challenges. According to statistics from September 18, 2023, nearly 95% of BTC remained stagnant, not involved in any transactions in the past month. This behavior indicates that while Bitcoin has been embraced by a vast array of investors, it's more often viewed as a long-term value storage instrument rather than a liquid asset.

Challenges with New BTC Derivative Assets The market for new Bitcoin derivative assets, including Ordinals, BRC20 and others, is still in its infancy. Due to high entry barriers, operational complexities, and limited application scenarios, less than 1% of BTC addresses have ventured into this market. This low participation rate impedes the liquidity and market depth of Bitcoin derivative assets.

The Influence of EVM-Compatible Ecosystem Assets On EVM-compatible chains, a plethora of DeFi products anchored to BTC as their base currency have surfaced. These products offer users an avenue to leverage Bitcoin in a decentralized context, bypassing the inherent constraints of Bitcoin itself. This further underscores Bitcoin's deficiencies in scalability and versatility.

The Role of Centralized Exchange Assets Within centralized exchanges, BTC dominates as the most traded currency, second only to the stablecoin USDT. A predominant reason for this prevalence is Bitcoin's absence from the DeFi product lineup, compelling many users to resort to centralized exchanges for trading instead of using decentralized alternatives. This trend heightens centralized risks and diminishes Bitcoin's influence in the decentralized finance domain.

2.3 B^2 Network: The Path to Bitcoin Future Expansion and Innovation

To address the above technical and asset liquidity challenges, B^2 Network solutions have been ushered in. B^2 Network is a secondary network constructed atop the primary chain – Bitcoin Network, aspiring to deliver enhanced performance, reduced transaction costs, and a richer application landscape.

By deploying B^2 Network, Bitcoin can facilitate near-instantaneous transactions, drastically reduced transaction costs, and complex smart contract functionalities. This metamorphosis would position Bitcoin as a truly decentralized financial platform, catering to the needs of billions of global users.

B^2 Network solutions, leverage rollup with zero-knowledge proof technology to permit users to conduct transactions off-chain without necessitating constant confirmations on the main chain. Additionally, by introducing Turing-complete smart contract capabilities, B^2 Network can usher in unprecedented application potentialities for Bitcoin, like DeFi, NFTs, and other decentralized applications.

In conclusion, B^2 Network furnishes Bitcoin with opportunities for expansion and innovation, enabling it to meet the challenges and prospects of the future. Only through relentless innovation and scalability can Bitcoin perpetuate its leadership stance in the realm of digital currencies, delivering value and services to its global user base.

3 B^2 Network: Exponentially Expanding the Bitcoin Ecosystem

The realm of cryptocurrency has been in constant evolution since its inception. Central to this universe stands Bitcoin - not just as the premier cryptocurrency, but as a symbol of decentralization, security, and trust. However, for all its merits, Bitcoin, like any pioneer, has areas awaiting further evolution. Enter the B^2 Network, an ambitious Layer-2 solution aiming to elevate Bitcoin's potential. By aligning with core values and a clear vision, the B^2 Network emerges as a promising avenue to enhance Bitcoin's footprint in the crypto world.

3.1 Core Values

Bitcoin's Evolution Beyond Payments Bitcoin's significance isn't limited to just being a payment network. Its foundational principles make it ripe for more profound evolution and integration into a broader spectrum of financial services and applications.

Nurturing BTC-related Assets BTC and its related assets require a fertile ground - an ecosystem where they don't just exist but thrive. This includes realms like Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs), Social Finance (SocialFi), and more. These avenues represent the next phase of Bitcoin's integration into global financial systems.

EVM-Compatible Ecosystem Alignment Ethereum's Virtual Machine (EVM) has carved a dominant space in the crypto ecosystem. With over 90% of crypto users interacting with EVM-compatible chains, it's logical and essential that any solution designed for Bitcoin's growth aligns with this user base. By embracing EVM compatibility, B^2 Network aims to resonate with the operational habits of the majority, ensuring familiarity while introducing innovation.

3.2 Vision

The B^2 Network envisions a future where Bitcoin's utility and influence aren't just maintained but exponentially expanded. The network seeks to establish a realm where Bitcoin isn't just a digital asset or a store of value but a dynamic platform. It aims for a world where Bitcoin interacts seamlessly with various financial services, tools, and platforms, making it more embedded in everyday transactions and applications.

3.3 Mission

The mission of the B^2 Network is to build the premier Bitcoin Layer-2 network and revive builder culture.

Practicality At its core, the B^2 Network aspires to create the most practical Layer-2 solution for Bitcoin. This entails a network that isn't just about technical superiority but about real-world applicability. It's about ensuring that users, be they individuals or enterprises, find tangible benefits in using this network, from faster transaction times, reduced fees, to innovative financial tools.

Reviving builder culture Bitcoin began as a revolution, a response to traditional financial systems, and a vision of a decentralized future. Early adopters weren't just users; they were builders - individuals and groups passionate about creating, refining, and expanding. The B^2 Network seeks to reignite this builder culture. By offering tools, platforms, and opportunities, it aims to transform users from mere participants to active contributors, fostering an environment of innovation and growth. Developers can easily build DApps and migrate DApps from EVM-compatible ecosystem by B^2 Network.

In Conclusion, the B^2 Network isn't just another addition to the crypto ecosystem. It's a testament to the belief that Bitcoin's journey is far from over. By staying true to core values, driven by a clear vision, and propelled by an actionable mission, the B^2 Network stands as a beacon for the next phase of Bitcoin's evolution. As we stand at the crossroads of innovation and tradition, B^2 Network offers a path that respects Bitcoin's origins while fearlessly charting its future.

4 Technical Architecture

The technical architecture of the B^2 Network is shown in Figure 1. Comprising two fundamental layers and Rollup Layer, Data Availability Layer, B^2 Network seeks to redefine the way we perceive Bitcoin Layer-2 solutions.

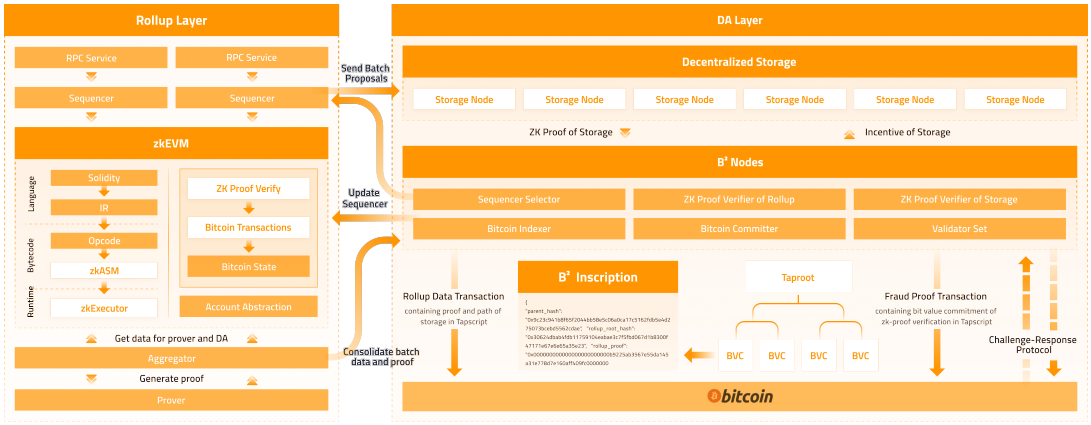

Figure 1: Technical architecture of B^2 Network

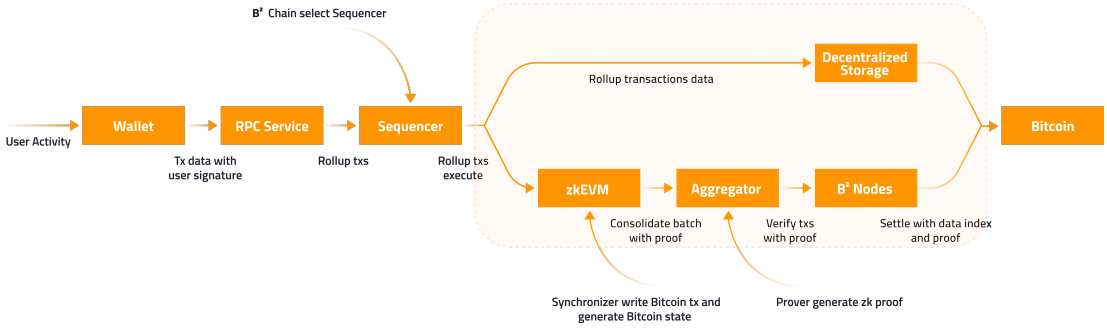

Figure 2: Transaction flow

4.1 Rollup Layer

B^2 employs ZK-Rollup as Rollup Layer. ZK-Rollup Layer adopts the zkEVM solution, responsible for the execution of user transactions within the Layer-2 network and the output of related proofs.

Users' transactions are submitted and processed in the ZK-Rollup Layer. The users' state is also stored in the ZK-Rollup Layer. The batch proposals and the generated zero-knowledge proofs are forwarded to the Data Availability Layer for storage and verification.

4.2 Data Availability Layer

Data Availability Layer includes Decentralized Storage, B^2 Nodes, and Bitcoin Network. This layer is responsible for permanently storing copies of rollup data, verifying rollup zk proofs, and ultimately performing the final confirmation on Bitcoin.

Decentralized Storage A pivotal aspect of the B^2 Network, the decentralized storage serves as the repository for the ZK-Rollup's user transactions and their respective proofs. By decentralizing storage, the network inherently enhances security, reduces single points of failure, and ensures data immutability.

B^2 Nodes B^2 Nodes consist of multiple modules, performing various roles: 1. They incentivize Decentralized Storage, ensuring accurate and efficient storage of B^2 rollup data copies through zk proof of storage and economic incentives. 2. B^2 Nodes validate the zk proof of rollups, checking the accuracy and efficiency of zk rollup transactions and state generation. 3. B^2 Nodes provide decentralized sequencer services for B^2 rollups, selecting sequencers in a DPoS-like manner, ensuring decentralization and preventing malfeasance by a single sequencer. 4. B^2 Nodes supply Bitcoin block and transaction data for integrating Bitcoin state in B^2 rollups and generate zero-knowledge proofs to ensure data security. 5. The Bitcoin committer module of B^2 Nodes writes B^2 rollup data into Bitcoin via Tapscript, creates bit value commitments for zk proof verification, and performs final confirmations on Bitcoin through challenge-response mechanisms. 6. B^2 Nodes maintain Schnorr multi-signature verifiers.

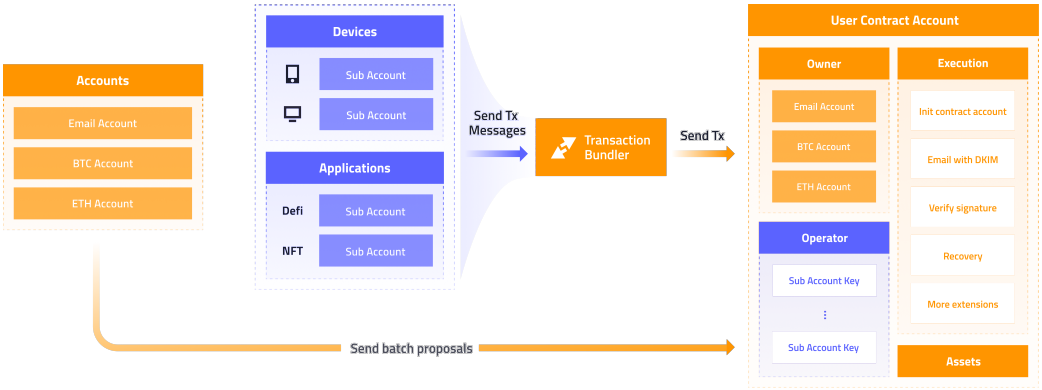

Figure 3: Account abstraction in B^2 Network

Bitcoin Network Bitcoin Network is the final settlement layer for B^2 Network. Users can recover all B^2 rollup transactions through Bitcoin and validate their authenticity using zk proofs recorded on Bitcoin. B^2 Network employs zk proof verification commitment and challenge-response mechanisms for final confirmations on Bitcoin. This process, supported by Bitcoin's robust Proof of Work (POW) algorithm, ensures the security of B^2 rollup.

At last, the transaction flow is shown in Figure 2.

B^2 Network is not just another Layer-2 solution, it's a symphony of cutting-edge technological advancements designed with precision, executed with expertise, and delivered with an overarching vision. By combining speed with security, innovation with reliability, and technology with user centricity, B^2 Network stands poised not just to address the current challenges but to proactively anticipate and tackle future ones. As we navigate the ever-evolving cryptoverse, B^2 Network illuminates the path, offering a glimpse into the future where scalability, security, and seamless user experience coexist harmoniously.

5 Rollup Layer: the execution layer of B^2 Network

ZK-Rollup consists of several components, including Account Abstraction Module, RPC Service, Mempool, Sequencers, zkEVM, Aggregators, Synchronizers, and Prover

Account Abstraction Module B^2 Network implements native account abstraction at Rollup Layer in Figure 3. B^2 creates contract accounts controlled by users in the zkEVM. Contract accounts for Bitcoin address accounts are controlled by the user's Bitcoin private key, those for Ethereum address accounts by the user's Ethereum private key, and for Email accounts by the user's email. Users can generate sub-accounts through their contract account for different devices or DApps. Sub-accounts can have controlled permissions, like only sending standard transactions and not managing assets of the contract account. The controlling account can remove sub-accounts at any time. The contract account features a modular execution layer, which performs default operations or checks based on B^2's and users' settings, such as account initialization, email account DKIM verification, transaction validation, account recovery, permission management, and asset locking. This execution layer is expandable and upgradable. Users' on-chain assets in B^2 are attributed to the contract account and can be managed through the controlling account (Bitcoin address account, Ethereum address account, or Email account).

The Account Abstraction module of B^2 Network, through its Transaction Bundler service, can implement a gas payment function on behalf of users. Upon receiving transaction messages signed by the user's controlling account or sub-accounts, the Transaction Bundler, based on the user's settings for gas payment or the interacting contract's settings, pays the gas for the user. It then collects other assets from the user or the interacting contract as compensation.

RPC Service Users initiate transactions or send signed messages through wallets or services provided by DApps to B^2 RPC Service. Once these transactions or signed details are received, B^2 RPC Service performs preliminary validation, either directly sending them to the Mempool service or processing them for account abstraction before dispatch. B^2 RPC Service internally integrates the Transaction Bundler service of the Account Abstraction Module, which validates message signatures and generates corresponding transaction information based on the message content, as shown in Figure 5. The Transaction Bundler service offers gas payment on behalf of users, using BRC20 assets on Bitcoin like ORDI, SATS, or directly deducting gas from the interacting contracts, facilitating gas-free functionalities for

DApps. By employing horizontal scaling, B^2 RPC Service can enhance the performance of Rollup Layer. Third-party entities and developers can operate B^2 RPC Service and provide related services.

Mempool The Mempool serves as the storage for all pending transactions. Sequencers can access and order these transactions from the Mempool.

Sequencer The Sequencer in B^2 Network is responsible for ordering and packaging the transactions submitted by users, and then handing them over to the zkEVM for specific transaction execution. B^2 Network implements a Decentralized Sequencer service through B^2 Nodes, which update the Sequencer Set via a mechanism similar to DPoS. The Sequencers within the Sequencer Set provide transaction ordering and packaging services in sequence.

zkEVM The zkEVM, compatible with EVM, facilitates developers in constructing secure DeFi, NFTs, and other DApps. It also aids developers in migrating DApps from other EVM-compatible chains to B^2 Network. Combined with the Bitcoin Indexer Module of the B^2 Chain, the zkEVM stores Bitcoin's state data, enabling developers to integrate the Bitcoin network into DApp development.

Aggregators The Aggregators access the sequencer's post-ordered transaction information and state information from the zkEVM. They either generate zero-knowledge proofs via the Prover or aggregate transactions and collate proof details from the Prover, formulating a transaction batch hash tree. This tree is then sent to the data availability layer for backup, ensuring rollup transaction data availability.

Prover The Prover's role is to generate validity proofs, representing the authenticity of a batch of user-submitted transactions. Initially, the Prover creates multiple ZK-STARK proofs based on the transaction batch and state information acquired from the Aggregator. By leveraging STARK Recursion, these ZK-STARKs are bundled to produce a single, extensive ZK-STARK. This ZK-STARK, being sizeable, is channeled out via the CIRCOM component to the SNARK builder, which in turn generates a ZK-SNARK validity proof, drastically reducing Gas costs. Finally, the generated proof returns to the Aggregator.

Synchronizer The Synchronizer ensures that information from the B^2 Chain is synchronized into the Rollup Layer, encompassing details like sequencer information, Bitcoin transaction data, and more.

In conclusion, the Rollup Layer procures user transactions via the RPC Service and stores them in the Mempool. Once sequencers have ordered these transactions, the zkEVM processes the transaction batch. The Prover then produces a zero-knowledge proof of transaction authenticity. Through the Aggregator, transaction and proof details are summarized and synchronized to B^2 Network's data availability layer, ensuring transaction veracity, data security, and data availability.

6 Data Availability Layer: the storage and validation layer of B^2 Network

DA Layer consists of three parts: **Decentralized Storage**, B^2 **Nodes**, and **Bitcoin Network**.

6.1 Decentralized Storage

Nodes in Decentralized Storage receive rollup data sent by the Sequencer from Rollup Layer and store them. Storage Nodes run the ds-prover program of B^2 Network, periodically generating zero-knowledge proofs based on time and space for the stored rollup data. The ds-prover program sends the generated zk proof of storage to B^2 Nodes, and after verification, Storage Nodes receive certain storage rewards. The Storage Nodes in Decentralized Storage redundantly store copies of rollup data, ensuring the data availability of B^2 Network.

6.2 B^2 Nodes

B^2 Nodes act as off-chain validators and are executors of multiple distinctive features in B^2 Network. B^2 Nodes consist of six main modules: ZK Proof Verifier of Rollup Module, ZK Proof Verifier of Storage Module, Sequencer Selector Module, Bitcoin Indexer Module, Bitcoin Committer Module, and Validator Set Module.

ZK Proof Verifier of Rollup Module B^2 Nodes obtain rollup transactions data from Decentralized Storage and rollup transaction merkle tree root hash and zk proof data from the Aggregator of the Rollup Layer. First, within the ZK Proof Verifier of Rollup Module, the merkle tree root hash is used to check if the rollup transactions stored in

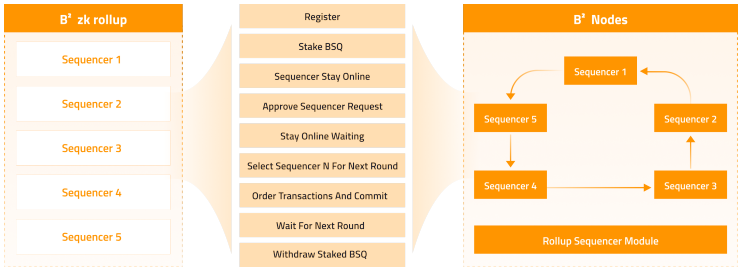

Figure 4: Decentralized sequencer in B^2 Network

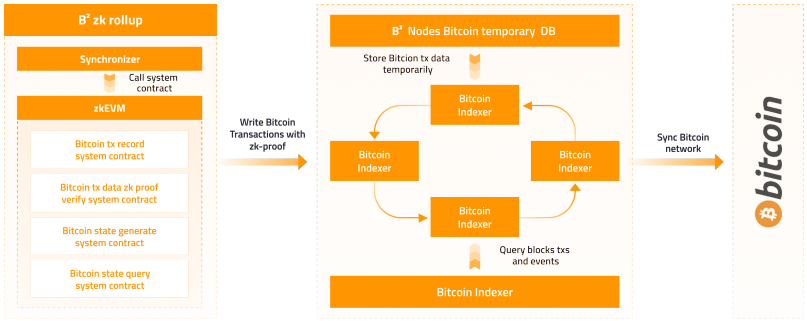

Figure 5: Decentralized sequencer in B^2 Network

Decentralized Storage have been tampered with. Then, the zk proof data is used to verify whether the rollup transactions have been executed correctly and effectively.

ZK Proof Verifier of Storage Module In the ZK Proof Verifier of Storage Module, B^2 Nodes validate the zk proof of storage submitted by the Storage Nodes of Decentralized Storage. Once the verification is passed, B^2 Nodes distribute rewards to the Storage Nodes, incentivizing them to store copies of rollup data over the long term.

Sequencer Selector Module In the Sequencer Selector Module, B^2 Network implements a mechanism similar to Delegated Proof of Stake (DPoS), selecting a group of sequencers. These sequencers sequentially provide transaction ordering and packaging services for a specified period. Individuals or organizations wishing to compete as a sequencer must stake a certain amount of $BSQ and prepare the necessary hardware resources to run the sequencer service. Users can also delegate their $BSQ to candidates competing for a sequencer position. Ultimately, the top N candidates with the highest total staked and delegated $BSQ become the sequencer set for a period. Operating a sequencer service earns a certain percentage of transaction fees and additional $BSQ rewards. (See in Figure 4)

Bitcoin Indexer Module The Bitcoin Indexer monitors blocks and transactions on the Bitcoin network. Upon obtaining the latest blocks and transactions, it generates zero-knowledge proofs for these blocks and transactions to ensure the accuracy of transaction information. The Bitcoin Indexer then sends the transactions and corresponding zk proofs to the Rollup Layer. When the zkEVM receives the Bitcoin transactions and zk proofs, it verifies them and generates the Bitcoin State. (See in Figure 5)

Bitcoin Committer Module The Bitcoin Committer sends two types of transactions to Bitcoin: one that writes rollup data into Bitcoin, and another that writes the zk proof verification commitment into Bitcoin.

- The Bitcoin Committer constructs a data structure to record B^2 rollup data and generates a Tapscript, known as a "B^2 Inscription." The Tapscript includes information such as: 1. Storage path of rollup data in decentralized storage; 2. Merkle tree root hash of rollup data; 3. Zk proof data of rollup data; 4. Parent B^2 inscription UTXO hash. Then, the Bitcoin Committer sends a UTXO of one satoshi unit to a Taproot address containing the B^2 inscription. The rollup data is permanently written into Bitcoin. (See in Figure 6)
- The Bitcoin Committer breaks down large computational units from the ZK Proof Verifier of Rollup Module into smaller computational units. Each small computational unit is then turned into a bit value commitment and placed in a tapleaf script. The zk proof of rollup serves as the input for the first bit value commitment, with the

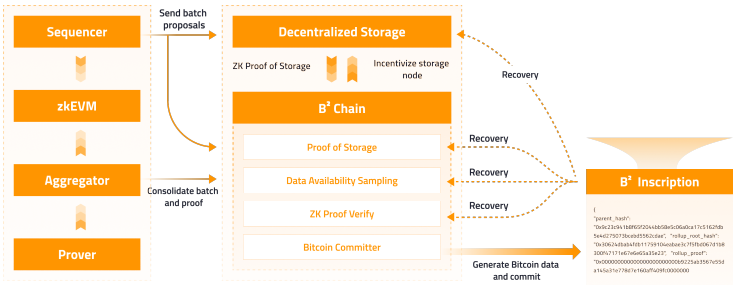

Figure 6: Data availability in B^2 Network

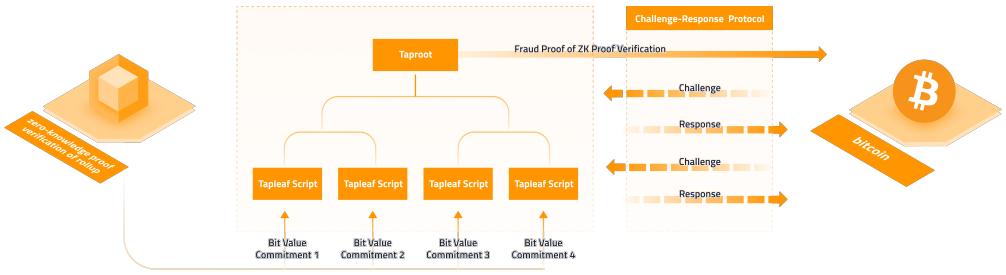

Figure 7: ZK proof verification commitment on Bitcoin

output being the input for the next commitment, eventually forming a taproot. The Bitcoin Committer sends a UTXO of one satoshi unit to a Taproot address containing the commitment. The commitment based on zk proof verification is permanently written into Bitcoin. Additionally, the Bitcoin Committer sets a time-locked challenge, allowing challengers to contest the zk proof verification commitment. If there are no challengers or the challenge fails within the time lock, the rollup is finally confirmed on Bitcoin; if the challenge succeeds, the rollup is rolled back. (See in Figure 7)

Validator Set Module The Validator Set Module maintains members of the Schnorr signature on Bitcoin Layer1.

6.3 Bitcoin Network

Bitcoin serves as the ultimate settlement layer for B^2 Network. B^2 rollup data is stored on Bitcoin, allowing complete retrieval or restoration of B^2 rollup transactions based on the B^2 inscriptions on Bitcoin. The computational validity of zk proof verification of rollup is confirmed on Bitcoin, thereby confirming the B^2 rollup.

7 Technical Features of B^2 Network

7.1 Security and Decentralization

- **Data availability**. Based on the data on Bitcoin, all transactions of the B^2 rollup can be recovered. The strong computational power and consensus of Bitcoin ensure the data availability of B^2 Network.
- **Confirmation on Bitcoin**. Through zk proof commitment and challenge-response, B^2 Network achieves bidirectional confirmation on Bitcoin, rather than just unidirectional data writing onto Bitcoin.
- **Decentralized sequencer**. By implementing decentralized sequencer, the potential for malicious actions by a single sequencer is mitigated.

7.2 Seamless Development and Access

- **EVM compatible**. By being compatible with EVM, it enables rapid migration of DApps from other EVM-compatible chains to B^2 Network, and also allows developers to quickly build new DApps within B^2 Network shown in Figure 8.
- **Account abstraction**. By implementing account abstraction, B^2 Network can support Bitcoin address accounts, Ethereum address accounts, and Email accounts. For Bitcoin users, cross-chain interactions on B^2

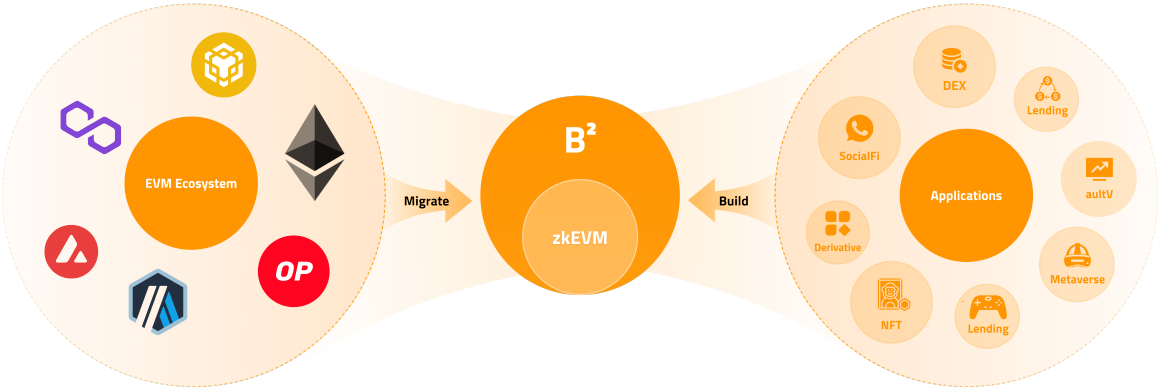

Figure 8: ZK proof verification commitment on Bitcoin

Network are possible without changing wallets. Support for Email accounts also lowers the barrier for web2 users to utilize B^2 Network.

- **Store Bitcoin state**. Storing Bitcoin state offers three benefits: 1. It eliminates the need for a bridge from Layer1 to Layer2, as the Bitcoin state in zkEVM can automatically trigger cross-chain transactions from Layer1 to Layer2; 2. It provides developers with Bitcoin-oriented programming capabilities, enabling the development of various applications based on Bitcoin transactions; 3. It offers users a trustless, decentralized Bitcoin Indexer service to query the Bitcoin state.

7.3 Performance Ready for Mass Adoption

- **Fast and Security**. Employing rollup technology, the Rollup Layer in B^2 Network operates without the need for consensus, ensuring high performance. Additionally, the powerful Data Availability (DA) Layer solution of B^2 Network guarantees security.
- **Cheap**. Fee is cheap. And demand spikes, fees don't.

B^2 Network is the first zk proof verification commitment rollup on Bitcoin. At the same time, B^2 Network is continuously researching and exploring how to construct a safer and more user-friendly Layer-2 network on Bitcoin. B^2 Network will keep evolving to become the most practical Layer-2 network.

Acknowledgments

A tip of the hat and a grand salute to the unsung heroes of the Bitcoin saga! To the users, with your unwavering faith, navigating the tumultuous seas of the crypto world with grace and fervor - you are the heartbeat of this journey. To the developers, the magicians weaving codes into digital tapestries, turning binary into a symphony of innovation - you are the soul. And to the miners, the tireless sentinels, chiseling away in the silent depths, unearthing the gems of opportunity - you are the backbone. Each block mined, code written, and transaction made is a verse added to the epic ballad of Bitcoin. In the grand theatre of cryptography and decentralization, your roles are pivotal, your contributions, immortalized in every byte of the blockchain. As we venture into the enigmatic world of Layer 2, with stars in our eyes and bytes in our hands, we carry the torch of your legacy, illuminating paths untrodden. Here's to the dreamers, the doers, the believers - the mavericks of the Bitcoin odyssey. Cheers!

References

[1] Satoshi Nakamoto. Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[2] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. 2016.