Pretzel Layer: Proof-of-play based L2 on Berachain

Bambo
Pretzel
bambo@pretzel.build

Grizz
Pretzel
grizz@pretzel.build

Bclaren
Independent Researcher

Duck
Pretzel
duck@pretzel.build

Abstract

In this paper, we present a novel Layer 2 (L2) scaling solution tailored specifically for the gaming industry: Pretzel. Built on Berachain, Pretzel introduces the groundbreaking concept of Proof-of-Play, a consensus mechanism that rewards players based on their in-game activities, seamlessly integrating decentralized game economies with blockchain technology. By leveraging Berachain's innovative Proof-of-Liquidity model, Pretzel ensures low-latency, high-speed gaming experiences while maintaining the security and decentralization inherent in blockchain systems. Pretzel token (PRET) and BERA, iBGT tokens power the ecosystem, enabling governance, fee payments, and staking mechanisms that align with the interests of both players and developers. Pretzel stands at the forefront of gaming's next revolution, merging gameplay with blockchain in a truly decentralized manner.

1 Introduction

As the gaming industry grows and converges with blockchain technology, new mechanisms are emerging to reshape how players interact with games, and more importantly, how they derive value from their participation. One such innovative model is Proof-of-Play, a novel consensus mechanism tailored specifically for decentralized gaming ecosystems. Pretzel, built on Berachain, leverages Proof-of-Play to reward players for their in-game contributions in a decentralized and transparent manner. This new framework not only incentivizes user engagement but also offers verifiable proof of interaction, allowing for a scalable and secure Layer 2 solution optimized for the demands of modern gaming.

Blockchain gaming has introduced a paradigm shift where players can truly own their in-game assets, tokenize them as non-fungible tokens (NFTs), and trade them on decentralized markets. While these innovations have laid the groundwork for decentralized economies within gaming, Pretzel pushes these boundaries further by integrating Proof-of-Play, a system that verifies and rewards players based on their gaming activity. This is a key evolution from traditional play-to-earn models, providing a more direct and verifiable link between gaming efforts and economic rewards.

Proof-of-Play operates by recording player actions and interactions directly on the blockchain, making these activities tamper-proof and transparent. This level of verifiability opens up a new era in gaming, where player skill, achievements, and in-game contributions are not only recognized but also incentivized through blockchain mechanics. In this ecosystem, players are no longer just participants; they are integral to the network's security and operations. By aligning economic incentives with player engagement, Pretzel aims to create a symbiotic relationship between the gaming experience and the underlying blockchain infrastructure.

At the core of Pretzel's infrastructure lies Berachain, a revolutionary blockchain that utilizes the Proof-of-Liquidity consensus model. In contrast to traditional proof-of-work or proof-of-stake systems, Proof-of-Liquidity optimizes both security and economic efficiency by requiring validators to lock liquidity in the network. This locked liquidity forms the foundation of Berachain's consensus, allowing the network to be secured without the high computational costs associated with proof-of-work, while also providing deeper liquidity for decentralized applications (dApps).

Berachain's architecture, which is designed to be scalable and interoperable, serves as the ideal backbone for Pretzel's Layer 2 gaming solution. The Proof-of-Liquidity model is uniquely aligned with gaming use cases, where liquidity and speed are crucial for the seamless operation of decentralized economies. By building on Berachain, Pretzel ensures that in-game transactions, whether involving assets, rewards, or player interactions, are handled efficiently, with minimal latency and optimal gas costs. This is a critical feature, especially as traditional Layer 1 networks, such as Ethereum, often struggle with congestion and high transaction fees during peak gaming activity.[1]

In this model, validators play a crucial role in the network's operation by staking liquidity to secure the network, validating transactions, and submitting game-related state roots to Berachain. The liquidity that underpins this system is not only used for network security but also powers decentralized finance (DeFi) integrations, offering a fluid connection between gaming and broader blockchain ecosystems. This dynamic approach to securing the network enhances scalability and flexibility, ensuring that Pretzel can handle the unique demands of the gaming industry.

Pretzel's Layer 2 scaling is a direct response to the limitations of existing blockchain architectures when it comes to gaming. High gas fees and slow transaction speeds have long plagued decentralized games, making seamless, real-time interaction between players and the blockchain nearly impossible on traditional networks. By utilizing Berachain's scalable infrastructure, Pretzel delivers a fluid and responsive gaming experience without sacrificing security or decentralization.

The synergy between Proof-of-Play and Proof-of-Liquidity represents a novel approach to gaming and blockchain integration. While Proof-of-Play rewards players for their engagement and activity, Proof-of-Liquidity ensures the network remains secure and liquid, enabling a seamless interaction between gaming mechanics and decentralized finance. Pretzel thus provides a robust and flexible platform for developers and players alike, allowing them to build and participate in decentralized economies that transcend the traditional boundaries of gaming.

2 Architecture

Pretzel's architecture is designed to meet the unique demands of decentralized gaming at scale, leveraging a network of nodes that ensures robust performance, security, and decentralization. The system is built to handle high-throughput, low-latency transactions necessary for gaming applications while ensuring that players and developers experience seamless interactions with the blockchain layer.

2.1 Rollup Design

Pretzel is designed as a Layer 2 (L2) scaling solution using *Arbitrum Orbit* for execution and *Berachain* for settlement. This dual-layer architecture ensures that gaming applications benefit from the high throughput and low latency of Arbitrum's Optimistic Rollup model, while leveraging Berachain's settlement layer for finalizing transactions and ensuring long-term security.

In this design, transactions are grouped into batches by an operator, and Optimistic Proofs are generated to validate the batch's integrity. Once these proofs are validated without any challenges, the state is updated on Berachain's settlement layer, ensuring that transaction finality is achieved.

2.2 Optimistic Rollup Mechanics

The Optimistic Rollup design relies on two key components:

- **Execution on Arbitrum Orbit:** Transactions are executed via Orbit. The batching of transactions and execution logic is optimized for speed and cost-efficiency, ensuring that players experience real-time performance without the bottlenecks typically seen in Layer 1 systems.

- **Settlement on Berachain:** After successful execution on Orbit, the resulting state updates are submitted to Berachain, where final settlement occurs. If no fraud is detected during the challenge period, the updated state is confirmed on Berachain, which acts as the settlement layer for the entire system.[2]

2.3 Data Availability via Celestia

Pretzel ensures that all transaction data is securely stored and available through integration with *Celestia*. This external data availability layer ensures that all game-related state changes processed on Orbit are backed by decentralized, verifiable storage. Celestia's *Data Availability Committee (DAC)* signs each batch of transactions to indicate that the data is stored and can be retrieved in the event of network issues or malicious actions.

By leveraging Celestia for data availability, Pretzel ensures that the critical data required for withdrawal or transaction recovery is always accessible, even if the Layer 2 system becomes unresponsive. This ensures the security of user assets and data, regardless of any disruptions to Arbitrum Orbit.

2.4 Cross-Chain Communication via LayerZero

Pretzel integrates with *LayerZero* to enable cross-chain communication, facilitating the seamless movement of assets and data between Arbitrum Orbit, Berachain, and other blockchain ecosystems. This integration ensures that developers and players can manage assets across different chains without the limitations of traditional bridges.

LayerZero allows Pretzel to provide interoperability between multiple blockchains, ensuring that game assets and user states are transferable across different platforms. This cross-chain capability creates a more dynamic gaming ecosystem where assets are not confined to a single blockchain, enhancing player flexibility and game developer opportunities.

2.5 Node System and Validator Responsibilities

At the core of Pretzel's architecture is a decentralized network of Guardian Nodes, responsible for securing the platform and maintaining data integrity. Guardian Nodes are tasked with monitoring and verifying transactions across the network, ensuring that all in-game actions and state changes are accurately reflected and securely stored on the blockchain.

Node operators within the Pretzel ecosystem must acquire a unique "Node Key," issued as a non-fungible token (NFT), granting them the authority to validate transactions. This Node Key acts as both a license and an identification mechanism within the network, making it a verifiable part of the Pretzel ecosystem.

Guardian Nodes are responsible for endorsing state assertions — validating that the game states submitted by developers are accurate and tamper-proof. Once a Guardian Node successfully validates a state assertion, it is signed off and stored on-chain. If later validated as a legitimate claim by the network, the Guardian Node is rewarded for its participation. Rewards are distributed in the native token of the Pretzel ecosystem, aligning incentives between the node operators and the overall health of the platform.

2.6 Participating in Node Operation

To participate in the node system and earn rewards, prospective node operators must acquire and stake a Node Key. This grants them the right to validate and endorse state assertions on the network. The node operator's responsibilities include consistently monitoring the state of the network and performing validation tasks for both game-related transactions and off-chain state transitions.

Owning a Node Key also involves active participation in the network's security. Operators must ensure that game states are accurate and properly recorded before they are finalized on-chain. If any discrepancies or malicious activity is detected during the validation process, the network can take corrective measures based on the input from Guardian Nodes.

2.7 Assertions and Challenges

The validation of game-related assertions is handled by smart contracts within the Pretzel architecture. For every state assertion made by a game, a "challenger" node can sign off on the assertion's validity using their private key. The smart contract verifies these signatures and, if consensus is reached, the assertion is accepted. If the assertion is disputed, the challenger node's inputs are reviewed, and further validation is performed.

This process ensures that game states and player interactions are accurately represented on the blockchain without any manipulation or fraud. Guardian Nodes are incentivized to monitor the validity of assertions closely, with rewards tied to their ability to maintain the network's accuracy and reliability.

2.8 Security and Scalability

Pretzel's node system ensures both security and scalability, allowing for a large number of transactions to be processed simultaneously. The decentralized nature of the node network provides a robust layer of security, protecting the system from attacks or malicious behavior. Additionally, the modular nature of the node system means that new nodes can be added to the network as required, allowing for seamless scaling as more games and players join the ecosystem.

To further ensure scalability, the system leverages off-chain computation where possible, minimizing the computational load on the blockchain layer. This approach allows Pretzel to handle the intensive resource demands of gaming without sacrificing decentralization or security.

3 Node Keys

The *Node Key* is a unique non-fungible token (NFT) that plays a crucial role in Pretzel's decentralized node architecture. It serves as the authorization and identification for operators running nodes on the Pretzel network. Acquiring a Node Key grants operators the ability to participate in network validation, submit assertions, and earn rewards for their contributions.

To mint a Node Key, users will utilize the official Pretzel Node Key minting platform. The cost of minting a Node Key follows a threshold system, which is subject to adjustment as the number of active Node Keys increases within the network.

3.1 Role of the Node Key in Assertion Validation

The Node Key is essential for submitting state assertions to the network, ensuring that each node participating in the challenge process is authorized and validated. During the assertion process, the network verifies whether the submitter is the legitimate owner of the Node Key or an authorized party. This verification is critical for maintaining the integrity of the network, allowing only authorized nodes to challenge or validate state changes.

Additionally, the Guardian Verifier contract within the system oversees the submission of assertions. Before rewards are distributed to a Node Key holder, the system checks the key's compliance status to ensure that the operator is eligible to receive rewards based on the validity of their submission. This mechanism ensures that all operators adhere to network rules, preventing unauthorized or fraudulent participation.

3.2 Node Key Hardware Requirements

To operate a node on Pretzel's network, certain hardware requirements must be met to ensure optimal performance and security. The minimum recommended specifications are as follows:

- **RAM:** At least 4GB
- **CPU:** At least 2.0 GHz clock speed
- **Processor Architecture:** x86-64 or Apple Arm64
- **Disk Space:** At least 50GB of free disk space
- **Internet Connection:** Stable 500 kbps upload/download speed

As the network evolves, these hardware requirements may change to accommodate future updates or increased system complexity. Operators can run multiple Node Keys on a single machine, optimizing performance and resource usage across the network.

3.3 Rewards and Incentives

Pretzel allocates a portion of its native token supply as rewards for Guardian Node operators who participate in the assertion process. The reward pool is distributed relative to the number of active Node Keys associated with each operator. The more Node Keys an operator has, the larger their share of the reward pool.

Nodes are rewarded each time they successfully participate in an assertion challenge. The assertion challenge process automatically involves Guardian Nodes in validating game state transitions. These validation tasks ensure that game states are recorded accurately and transparently on the blockchain.

The total rewards allocated per assertion challenge can vary but are predictable based on the total number of Node Keys and the overall activity on the network. In addition to assertion rewards, Guardian Nodes receive 25% of all transaction fees generated across the network, further incentivizing active participation and ensuring the long-term security of the Pretzel ecosystem.

3.4 MEV Revenue Distribution

In addition to transaction fees and assertion rewards, Pretzel's architecture incorporates a mechanism to capture and distribute Maximum Extractable Value (MEV) revenue. MEV represents the profit that can be captured by reordering, inserting, or censoring transactions within a block. Given the nature of decentralized networks, MEV plays a significant role in incentivizing validators and node operators.

MEV revenue generated within Pretzel's Layer 2 ecosystem will be distributed among **Node Key** holders and node operators. The distribution model is designed to align incentives between the participants responsible for network validation and the overall security of the system. Node operators who actively participate in transaction ordering and validation will be entitled to a share of the MEV revenue, proportional to the number of Node Keys they hold and the operational uptime of their nodes.

This MEV distribution mechanism further strengthens the economic model of Pretzel, ensuring that validators are adequately compensated not only through transaction fees and assertion rewards but also through the additional revenue streams that MEV provides. This structure incentivizes consistent participation and enhances the security and efficiency of the network, creating a more robust and profitable environment for all participants involved in securing and operating Pretzel nodes.

3.5 Example Reward Calculation

Consider a scenario where the Pretzel network processes 30 million transactions in a given month, with an average fee of 0.4 tokens per transaction. This would result in 12 million tokens in transaction fees for that month. Out of this amount, 25% (or 3 million tokens) is allocated to the reward pool for Guardian Nodes, distributed based on the number of Node Keys they hold.

If a node holds 50 Node Keys out of a total of 12,000 active Node Keys, the node's reward share is calculated as 50/12,000, or 0.4% of the monthly rewards. Based on this calculation, the node would earn approximately 39,777 tokens in that month.

4 Conclusion

Pretzel represents a groundbreaking approach to scaling decentralized gaming ecosystems through the integration of Arbitrum Orbit's efficient execution layer and Berachain's secure settlement layer. By leveraging Optimistic Rollup technology, the architecture enables seamless, low-latency gaming experiences while maintaining the security and scalability necessary for decentralized applications.[3] The Proof-of-Play mechanism aligns user activity with network incentives, ensuring that both players and validators contribute to the ecosystem's stability and growth. Additionally, with data availability ensured through Celestia and cross-chain capabilities provided by LayerZero, Pretzel offers a robust and flexible platform that meets the unique demands of the gaming industry. This multi-layered architecture positions Pretzel as a leading solution for integrating blockchain technology into the future of gaming.

References

[1] Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform. 2014.

[2] Berachain Foundation. Berachain documentation: Proof-of-liquidity and core concepts. `https://docs.berachain.com/`, 2023.

[3] Offchain Labs. Arbitrum nitro whitepaper, 2022.