Pareme: The Proof Of Work Blockchain

Alejandro Ochoa
www.pareme.org

Abstract. Pareme is a lightweight proof-of-work blockchain that secures externally submitted hashes to create a shared hash rate environment. Each block contains up to 10 user chosen hashes and proof-of-work metadata, totaling 85-373 bytes. The chain has no native tokens, public keys, private keys, or block ownership, reducing complexity and storage demands. This design separates proof-of-work from application logic, allowing blockchain and non-blockchain systems to anchor data without maintaining their own mining ecosystems. Miners embed hashes for a fee paid by users, enabling systems to leverage collective hash power for security. Potential applications include merge mining, document authenticity, timestamped records, and ideology voting. By consolidating hash power, Pareme provides a generalized security layer that strengthens all connected systems while remaining efficient for miners and nodes.

Introduction

Pareme is a proof-of-work blockchain designed to store and secure user-submitted hashes. Each block contains up to 10 hashes chosen by a miner or user, alongside minimal proof-of-work metadata. This eliminates the need for native tokens, public keys, private keys, or block ownership. Users pay miners to embed hashes, enabling systems to anchor data without running their own chains. The design prioritizes simplicity and efficiency, reducing storage and bandwidth demands for nodes and miners.

Proof-of-work systems face challenges that fragment their security. New blockchains split hash power by requiring dedicated miners, weakening existing chains. Arbitrary data embedded in chains like Bitcoin bloats their storage, serving no purpose for their primary function. Merge mining and transaction fees attempt to address these issues, but they introduce complexity and misalignment of incentives. These inefficiencies highlight the need for a new approach to proof-of-work security.

Existing blockchains often become accidental parent chains when users embed hashes for external systems. This practice leverages the chain's hash power but adds unnecessary data, increasing storage and processing costs. A dedicated parent chain can address this by providing a lightweight location for hashes. Such a chain would consolidate hash power, offering security to any system without requiring it to maintain its own mining ecosystem.

Pareme aims to unify proof-of-work security across diverse applications. By acting as a shared parent chain, it allows blockchain and non-blockchain systems to anchor data with minimal overhead. Miners focus on a single chain, increasing hash power and resilience. This vision reduces vulnerabilities in individual systems, strengthens decentralization, and enables new use cases for proof-of-work verification.

Problems

Isolated Hash Power

Proof-of-work blockchains suffer from isolated hash power. Each new chain requires its own miners, pulling computational resources from existing systems. This fragmentation reduces security for all chains, as hash power spreads thinly across competing ecosystems. New chains struggle to attract miners unless they offer significant rewards, which often leads to centralization around a few dominant players. The result is a landscape of vulnerable systems, each maintaining its own mining infrastructure with limited collective strength.

Accidental “Parent” Chains

Many blockchains become accidental parent chains when users embed hashes for external systems. These chains, designed for specific purposes like cryptocurrencies, attract users seeking their high hash power for security. External systems submit hashes through transaction metadata or merge mining, relying on the parent chain’s proof-of-work. This practice forces chains to process data unrelated to their primary function, straining miners and nodes. The added complexity undermines efficiency, as chains were not built to serve as generalized security layers.

Fragmented Mining Ecosystems

Mining ecosystems remain fragmented due to competition and misaligned incentives. Merge mining allows miners to embed hashes from child chains into a parent chain, claiming rewards from multiple systems. However, miners must support the parent chain’s ecosystem, even when child chains offer higher rewards for their hashes. Miners evaluate external systems to select the most profitable hashes to embed, but the parent chain’s requirements force ongoing participation in its system, regardless of reward disparities. This constraint discourages miners from freely pursuing optimal incentives across child systems.

Hardware and Algorithm Barriers

Hardware and algorithm barriers further complicate proof-of-work systems. Different chains use distinct hashing algorithms, requiring specialized ASICs for each. Miners cannot easily switch between chains to pursue higher rewards, as new hardware investments are costly. This rigidity locks hash power into specific ecosystems, limiting flexibility and innovation. A chain that standardizes proof-of-work without native rewards or algorithm diversity could address these barriers, enabling broader participation.

Existing Solutions

Embedding Data on PoW Chains & Merge Mining

Users embed hashes onto existing proof-of-work chains to leverage their security. For example, Bitcoin stores arbitrary data in transaction metadata for purposes like timestamping documents. Systems without native rewards pay miners fees to include these hashes. Merge mining offers another approach, where miners embed a child chain’s hash into a parent chain, securing both with one proof-of-work puzzle. This allows smaller chains to share hash power with larger ones, increasing their security without dedicated miners.

Limitations

These solutions have significant limitations. Embedding arbitrary data bloats chains, increasing storage and bandwidth demands for nodes and miners. The data serves no purpose for the chain’s primary function, yet remains permanently stored. Merge mining requires miners to participate in the parent chain’s ecosystem, even when child chains offer higher rewards. This misalignment of incentives restricts miners’ flexibility to pursue optimal rewards. Both approaches add complexity, as chains handle data or protocols unrelated to their design, reducing efficiency and scalability.

Pareme’s Solution - A Generalized PoW Parent Chain

Separated Proof-Of-Work

Pareme separates proof-of-work from application-specific logic by creating a dedicated blockchain that stores only user-submitted hashes. Unlike cryptocurrencies that combine proof-of-work with transactions or smart contracts, Pareme exists solely as a security layer. Multiple chains and systems can anchor their data to Pareme, leveraging its hash power without maintaining their own mining ecosystems. This separation reduces complexity and allows diverse systems to share a common proof-of-work infrastructure.

Hash Rate Sharing

Hash rate sharing enables chains with their own miners and rewards to join Pareme’s ecosystem. Miners from different chains can work on Pareme simultaneously, embedding hashes for their respective systems. This consolidates hash power, increasing security for all connected systems. Miners process a single proof-of-work puzzle for Pareme, which secures their chosen hash, eliminating the need to split computational resources across isolated chains.

Generalized Parent Chain

Pareme acts as a simplified parent chain with a lightweight block structure. Each block contains ~200 bytes compared to >1MB blocks for other blockchains, including proof-of-work metadata and up to 10 content hashes. This design generalizes the role of a parent chain, focusing solely on securing hashes. The minimal data size ensures low storage and bandwidth demands, as parent chains are the only systems all miners in an ecosystem must run, while child systems remain optional, necessitating an efficient parent chain design. Pareme has no native tokens, rewards, or block ownership, as its purpose is to serve child systems. Blockchain child systems embed block hashes through merge mining, while non-blockchain systems use Pareme for verification, timestamping, or authenticity proofs. Miners receive rewards from child systems, aligning incentives with the systems they choose to support.

A Theoretical Overview

Security and Decentralization

Collective Hash Power Defense

Pareme’s security relies on collective hash power defense. Miners from multiple child systems contribute to a single proof-of-work chain, pooling their computational resources. This aggregated hash power strengthens every system anchoring data to Pareme. Unlike isolated chains, where security depends on individual miner bases, Pareme’s shared ecosystem ensures that all connected systems benefit from the total computational effort. Nodes verify blocks with minimal overhead, maintaining integrity across the network.

Attacks on Pareme target child systems, as Pareme itself offers no native rewards. A malicious actor seeking to manipulate a child chain’s hashes, such as through a 51% attack, must control the majority of Pareme’s hash power. This is significantly harder than attacking a standalone child chain, as Pareme’s hash power includes contributions from all miners across its ecosystem. The absence of rewards on Pareme removes incentives for attacking the chain directly, shifting the focus to child systems. The high computational cost of dominating Pareme’s collective hash power protects connected systems from censorship or manipulation.

Comparison to Existing Systems

Bitcoin’s Data Bloat
Bitcoin serves as an accidental parent chain when users embed hashes for external systems. Designed for monetary transactions, it stores arbitrary data in transaction metadata, such as timestamps or document hashes. This data, unrelated to Bitcoin’s payment system, increases block sizes, often reaching multiple megabytes. As a parent chain, Bitcoin processes these hashes inefficiently, as miners and nodes must handle transaction data alongside external content, leading to higher storage and bandwidth demands compared to a dedicated parent chain.

Ethereum’s Complexity
Ethereum also functions as a parent chain for systems anchoring hashes, but its complexity hinders efficiency. Built for smart contracts and decentralized applications, Ethereum’s blocks contain program state and transaction data, adding significant overhead. When used as a parent chain, it requires miners to process this unrelated data to secure external hashes. This burdens nodes with large storage requirements and slows verification, making Ethereum less effective for lightweight hash anchoring compared to a specialized chain.

Pareme’s Advantage
Pareme’s lightweight advantage stems from its design as a dedicated parent chain. Each block contains only ~200 bytes. Unlike Bitcoin’s megabyte-scale blocks or Ethereum’s state-heavy structure, Pareme minimizes storage and bandwidth demands. Miners and nodes process only the data necessary for hash security, enabling efficient operation. This focus makes Pareme a more effective parent chain for systems seeking proof-of-work security without extraneous overhead.

Alleviating Pressure
Pareme alleviates pressure on other chains by providing a specialized parent chain for hash anchoring. Bitcoin and Ethereum, when used as parent chains, accumulate data that strains their ecosystems, as they were not designed for this role. Pareme offers a lightweight alternative, allowing external systems to embed hashes without bloating existing chains. By redirecting hash-anchoring activities to Pareme, it reduces the operational burden on Bitcoin and Ethereum, enabling them to focus on their primary functions while Pareme handles proof-of-work security.

Theoretical Implications

Unified Security Model
Proof-of-work serves as a defense system for cyber applications, analogous to physical defense outsourcing. In early human societies, individuals defended themselves independently, limiting their ability to specialize. Modern systems outsource defense to police, militaries, and agencies protecting land, air, water, and space, freeing individuals to focus on productive tasks. Cyberspace lacks such a unified defense layer, forcing applications to implement their own security against threats like hackers, DDoS attacks, and bots. Pareme introduces a proof-of-work parent chain that outsources defense for digital systems. By pooling hash power, it provides collective security, allowing applications to specialize without maintaining individual proof-of-work ecosystems.

Pareme establishes a unified security model through this outsourced defense. Applications anchor hashes to Pareme, leveraging its aggregated hash power instead of building separate mining networks. This outsourcing of verification enables systems to prove data integrity, authenticity, or existence without computational overhead. Blockchain and non-blockchain systems benefit equally, as Pareme’s lightweight structure supports diverse use cases. The shared proof-of-work layer reduces the need for redundant security mechanisms, creating a standardized approach to protecting digital assets.

Outsourcing Defense

By outsourcing defense, Pareme reduces vulnerabilities in individual systems and strengthens decentralization. Standalone chains or applications with limited hash power are susceptible to attacks, as their security depends on small miner bases. Pareme's collective hash power shields connected systems, making attacks like hash manipulation computationally expensive. The absence of native rewards and block ownership encourages a diverse miner base, as no central incentives drive consolidation.

Use Cases

Merge Mining for Blockchain Child Systems
Merge mining for blockchain child systems allows cryptocurrencies to outsource their proof-of-work security to Pareme. Miners embed a child chain's block hash into a Pareme block, validating both chains with a single proof-of-work puzzle. This enables smaller chains to leverage Pareme's aggregated hash power without maintaining dedicated miners. The child chain provides rewards, while Pareme remains lightweight, reducing costs and increasing security for participants.

Access Control for Third Party Systems
Access control for third-party systems uses Pareme to verify user credentials. Systems require users to embed a hash of their credentials on Pareme, proving authenticity through proof-of-work. This mechanism defends against bots, as each connection attempt requires a verified hash. The provable cost of embedding hashes makes this approach practical for applications needing secure, decentralized access control.

Timestamped Records
Timestamped records enable users to prove a file's existence at a specific time. A user hashes a file, such as a contract or artwork, and mines it into a Pareme block, or pays a miner to do so. The block's timestamp and hash serve as a tamper-proof record, publicly verifiable on the blockchain. This use case supports legal, creative, or archival applications requiring proof of prior existence. This can be generalized as "proof-of-existence".

Decentralized Signaling
Decentralized signaling enables communities to coordinate through Pareme. Users mine hashes representing proposals, preferences, or endorsements, such as support for a protocol upgrade. Observers analyze hash frequency to identify dominant signals, facilitating consensus without centralized control. This use case supports governance and decision-making in decentralized systems.

Ideology Voting
Ideology voting allows users to embed hashes representing sets of principles or beliefs. Users mine a hash of a document outlining their views, such as economic or social policies, into Pareme. Observers tally blocks to gauge support for different ideologies, tracking shifts over time by comparing recent and historical blocks. This creates a decentralized, transparent record of global sentiment.

Content Verification
Content verification uses Pareme to validate the integrity of digital content. A creator of a document mines the hash of the content, such as a dataset or media file, and shares the hash as well as the document. Verifiers check the hash against Pareme's blockchain to confirm it has been unaltered. This approach supports applications where trust in content integrity is critical, such as scientific research or journalism.

Document Favorability
Document voting leverages Pareme to resolve disputes over document versions. Users mine a hash of the document they consider authentic/favorable into a Pareme block. Observers count blocks containing each hash to determine the most trusted version. This method allows communities to signal consensus on documents, like religious scriptures and/or their translations, by embedding their hashes, providing a transparent record of trust.

A Technical Overview

Pareme is a compact blockchain, distinct from those supporting currency or smart contracts. Each block carries 85-373 bytes:

- **Proof Of Work Data**
  - Height: 4 bytes
  - Timestamp: 8 bytes
  - Previous Block Hash: 32 bytes
  - Difficulty: 4 bytes
  - Nonce: 4 bytes
  - Payload Size: 1 byte

- **Payload**
  - Content Hashes: 32 bytes each (10 max)

Blocks target 10-second intervals, resulting in approximately 3 million blocks per year, or roughly 11.8 GB (high end) of data per decade.

Proof of Work & Difficulty Adjustment
A block's validity is determined by its difficulty value, adjusted every 2,016 blocks. A miner constructs a potential block with their chosen data, hashes it, and compares the result to the current difficulty. If the hash exceeds the difficulty, the nonce is altered, and the process repeats until a valid hash is found.

The difficulty is calculated as:

$$\text{New Difficulty} = (\text{Old Difficulty}) \times (\text{Ratio})$$

Where:

$$\text{Ratio} = \frac{\text{Average Time of Last 2016 Blocks}}{\text{Target Block Time (10 seconds)}}$$

With:

$$0.25 \leq \text{Ratio} \leq 4$$

Additional verification steps include:

- **Height and Previous Block Checks:** These ensure the referenced previous block is valid and the height value has incremented by exactly 1.

- **Timestamp Checks**: Ensures timestamp integrity, accounting for global time zones and propagation delays, with limits on future or past deviations.

Full Nodes & Pruning
Pareme's small blocks impose minimal storage demands. However, users may opt for a pruned version of the chain, where older blocks are discarded. Since each block references its predecessor, extremely old blocks are not required to verify new ones. At minimum, a node needs the last 2,016 blocks (< ~750 KB) to confirm a new block's difficulty and perform other verification steps.

While pruning is viable, retaining the full historical chain offers advantages. Certain use cases, detailed later, may require analyzing the frequency or existence of a specific hash across the entire chain. Nodes interested in such applications would thus benefit from maintaining the complete record. For basic verification and mining, however, a pruned node suffices.

Conclusion

Developers and miners should adopt Pareme to strengthen their systems. Miners can embed hashes for child systems, earning rewards without splitting hash power across chains. Systems can integrate Pareme to outsource proof-of-work, reducing operational costs and vulnerabilities. Nodes benefit from low resource requirements, enabling broad participation. Technical communities are encouraged to explore Pareme's open design, contributing to its protocol and use cases to refine its role as a parent chain.

Pareme envisions a secure, decentralized ecosystem where proof-of-work defends cyberspace.