MAZZE

MAZZE WHITEPAPER

Abstract

In this whitepaper, we explore the economic and technological aspects of the Mazze blockchain, a high-performance, high-throughput Proof-of-Work system. It differentiates itself from traditional blockchains like Bitcoin and Ethereum by introducing parallel block processing, enhancing performance limits. The paper analyzes Mazze's economic viability, its impact on blockchain's performance, and the effect of storage costs on user behavior in this decentralized environment. It aims to provide a detailed understanding of the critical parameters that shape the ecosystem's design and user incentives.

Legal Notice

This document and the information contained herein are provided for informational purposes only and are not intended to serve as legal, financial, business, or tax advice. Individuals or entities considering participation in any activity related to the content of this document are encouraged to seek guidance from their own professional advisors. The Mazze project, its project team members, and any third-party service providers expressly disclaim any liability for direct or indirect losses or damages that may result from the use of information contained in this whitepaper, related materials, or any associated websites, such as [https://www.mazze.io]. No guarantees or warranties are offered by Mazze or its team, and any representations or undertakings to any person or entity are expressly disclaimed.

Statements made in this whitepaper or during public communications, including press releases and oral statements by Mazze or its team, may contain forward-looking information regarding market conditions, business strategies, financial health, and risk management. Such statements are inherently subject to risks and uncertainties, and actual outcomes or results may differ materially from those projected. Information provided is valid as of its publication date, and there is no commitment from Mazze or its team to update any forward-looking statements.

Participation in Mazze project and any token distribution is subject to inherent risks. These include potential technical issues with the project's technology, the possibility of decreased interest or adoption by stakeholders or the broader community, and no guaranteed market valuation for the tokens.

This document does not constitute a prospectus of any sort nor should any content herein be considered as a solicitation for investment. The whitepaper is a technical description of Mazze blockchain's functionality and the deployment of its platform. It is intended solely to present Mazze project and details about MAZZE token. Redistribution of this document without written permission from Mazze team is prohibited. This document and the information it contains are not to be sent or addressed, in whole or in part, directly or indirectly, to persons in countries where such distribution is restricted.

Mazze makes no representations, warranties, or guarantees regarding the completeness, accuracy, or reliability of any information, facts, or opinions contained in this document. The founders, advisors, partners, directors, employees, and agents of Mazze and itself cannot be held liable for any reliance on the content of this document.

The information provided in this whitepaper is subject to change without notice. It may not be exhaustive of all information that Mazze represents and does not imply any elements of a contractual relationship. This whitepaper may be modified at any time to provide more detailed information.

This document and the information contained herein may not be sent or addressed, in whole or in part, directly or indirectly, to any person in jurisdictions where such distribution is restricted or where it would constitute a violation of applicable law.

This Legal Notice is intended to provide potential participants and stakeholders with a clear understanding of the terms, risks, and legal considerations associated with Mazze project. It is crucial that all parties read and understand this notice before participating in any related activities.

1. Introduction

1.1. Purpose and Vision

Mazze's purpose and vision are centered on establishing a decentralized blockchain platform that integrates robust security and absolute transparency. This innovative platform is designed to facilitate a sustainable approach to high-volume transactions, a notable achievement for a PoW (Proof of Work) chain. The essence of Mazze lies in its commitment to reducing environmental impact, a critical concern in contemporary blockchain technology. Key to its vision is the support of DeFi (Decentralized Finance), a transformative sector in the financial industry. Mazze's architecture is tailored to empower the creation and proliferation of DApps (Decentralized Applications) across a diverse range of sectors, including finance, healthcare, and education. These applications are poised to revolutionize how services are delivered and accessed in these fields, offering unprecedented levels of efficiency, security, and user control. The strategic focus of Mazze on these sectors demonstrates its commitment to not only advancing blockchain technology but also addressing real-world challenges and opportunities. By leveraging cutting-edge cryptographic techniques and innovative consensus mechanisms, Mazze aims to optimize transaction speed and reliability while ensuring scalability and network resilience. The platform's design emphasizes user-centricity, ensuring that both technical and non-technical users can engage effectively with its ecosystem. Furthermore, Mazze's approach to governance and legal compliance illustrates a deep understanding of the regulatory landscape, ensuring that the platform aligns with global standards and practices. This comprehensive approach positions Mazze as a pioneering force in the blockchain domain, with a clear trajectory towards shaping the future of decentralized technologies and their applications in critical sectors of the economy.

1.2. Blockchain Type

Mazze is a public blockchain network, characterized by its permissionless nature, ensuring full decentralization without any central oversight. This architecture fosters a high degree of trust and security, which is crucial for applications demanding transparency and immutability. Its design integrates a state-of-the-art consensus mechanism, which combines Proof of Work (PoW) with a unique Directed Acyclic Graph (DAG) structure, enhancing scalability and transaction throughput. This hybrid model enables parallel processing of blocks, a significant improvement over the serial block processing in traditional PoW systems. The DAG architecture also addresses scalability issues common in PoW networks, while the reward distribution mechanism promotes a diversified miner network, reinforcing network integrity. Advanced cryptographic techniques, such as robust hashing algorithms and digital signature standards, fortify the security of transactions, maintaining their integrity and authenticity. Mazze's architecture, inclusive of a layered design optimizing scalability and security, supports high-speed transactions and smart contract execution.

Mazze's blockchain employs a hash tree structure for efficient and secure transaction storage, optimized for quick verification and retrieval, capable of supporting large-scale and complex transactional needs. This structure, combined with strategies for data pruning and state management, ensures the scalability and robustness of the network. The comprehensive design of Mazze, from its consensus mechanism to its architecture and data structure, positions it as a pioneering platform suitable for a wide array of applications, from high-volume transactions to complex smart contract executions, thereby establishing it as a leader in the blockchain domain.

1.3. Consensus Mechanism

Mazze's consensus model, which merges Proof of Work (PoW) with a Directed Acyclic Graph (DAG) structure, forms the foundation for the introduction of the "Weighted Graph Ledger (WGL)". This new solution builds on the scalability and security advancements of Mazze, integrating a unique block weight system and a DAG-based ledger structure to further revolutionize blockchain technology. WGL's hybrid approach addresses the inherent scalability-security trade-off prevalent in traditional blockchains and offers a robust defense against liveness attacks.

Weighted Graph Ledger (WGL) synergizes with the DAG architecture of Mazze, introducing a novel block weight system alongside the DAG-based ledger. This integration enhances both scalability and transaction throughput, mitigating the limitations of conventional PoW systems.

Key Components:

A. Weighted Ledger Selection Rule (WLSR):

- WLSR, building on Mazze's dynamic, parallel block processing methodology, implements a block weighting system where blocks carry weights of 0, 1, or X (e.g., X=1000).
- The network hosts normal and special blocks, with normal blocks consistently weighing 1 and special blocks weighing either X or 0, based on mining difficulty.
- This mechanism aligns with Mazze's approach by promoting throughput in normal conditions and enhancing security during attacks through the generation of more special blocks.

B. DAG-Embedded Tree Structure (DETS):

- DETS leverages Mazze's DAG architecture, embedding it within a tree-like structure.
- This structure allows each block to have a single parent and reference multiple predecessors, enhancing ledger security and throughput.
- DETS complements Mazze's multiple chains of blocks, facilitating efficient data integration and concurrent block processing.

Consensus Process:

- Blocks in WGL are produced rapidly, up to 1 per second, benefiting from Mazze's efficient DAG structure and the WLSR.
- The nature of the blocks is determined by the network, echoing Mazze’s dynamic approach to block processing.

- WGL uses WLSR for selecting the pivot chain within DETS, an advancement of Mazze's parallel processing model.
- This selection, coupled with reference edges, orders transactions linearly, maintaining consistency and preventing double-spending.

```python
def calculate_block_weight(block, X=1000):
    if block.is_special():
        # Special blocks have a weight of X or 0 based on difficulty
        return X if block.meets_difficulty_threshold() else 0
    else:
        # Normal blocks always have a weight of 1
        return 1

# Example block objects
block_normal = Block(type="normal")
block_special = Block(type="special", difficulty="high")

# Calculating weights
weight_normal = calculate_block_weight(block_normal)
weight_special = calculate_block_weight(block_special)

print(f"Normal Block Weight: {weight_normal}")
print(f"Special Block Weight: {weight_special}")
```

Example of Block Weight Calculation

Benefits:

- Scalability: Enhanced by the rapid block generation and efficient ledger structure, building upon Mazze's scalability improvements.
- Security: Further fortified against various threats, including liveness attacks, complementing Mazze's advanced cryptographic techniques.
- Decentralization: WGL maintains decentralization by integrating all concurrent blocks, aligning with Mazze's ethos of a distributed network.

Implementation Use Cases:

- Suitable for high-throughput, secure cryptocurrency transactions, building on Mazze’s enhanced scalability.
- Ideal for enterprise blockchain solutions requiring both scalability and robust security.
- Supports decentralized applications (dApps) demanding a resilient and efficient blockchain infrastructure, leveraging Mazze's groundbreaking model.

2. Foundation and Core Concepts

2.1. Cornerstones of the Existing Blockchain World

The blockchain ecosystem, a revolutionary technology that has reshaped the digital landscape, is underpinned by several fundamental concepts. Initially conceptualized for digital currencies like Bitcoin, blockchain technology has evolved far beyond its initial use case. Its core principles of decentralization, transparency, and immutability have been instrumental in its widespread adoption across various industries.

Decentralization stands as a cornerstone, shifting power from centralized authorities to distributed networks. This paradigm shift ensures that no single entity has complete control over the network, enhancing security and fostering trust among users. The underlying technology of distributed ledger ensures that each participant has access to a shared ledger, an immutable record of transactions, enhancing transparency and auditability.

Immutability, another key feature, ensures that once data is recorded on the blockchain, it cannot be altered retroactively. This aspect is vital for ensuring the integrity of data, a crucial factor in sectors like finance, healthcare, and supply chain management.

Smart contracts, self-executing contracts with the terms of the agreement directly written into code, have expanded blockchain's applicability. They automate processes and transactions, reducing the need for intermediaries and enhancing efficiency.

Consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), are critical for maintaining the integrity and security of the blockchain. They ensure that all transactions are validated and agreed upon by network participants, mitigating the risk of fraudulent activities.

Interoperability and scalability are ongoing challenges in the blockchain world. Solutions like sidechains and layer-two protocols are being developed to enhance the ability of different blockchain networks to communicate and scale effectively.

Lastly, the role of cryptocurrency in blockchain cannot be overlooked. Cryptocurrencies not only facilitate transactions on the blockchain but also incentivize participants, playing a crucial role in maintaining and securing the network.

2.2. Consensus Protocol

Blockchain technology, at its core, relies on consensus protocols to validate transactions and secure the network. These protocols are fundamental to the integrity and functionality of blockchain systems. In the case of Mazze, a high-performance blockchain network, the decision to implement PoW as its consensus mechanism is rooted in a desire to balance ecological impact with network security and fairness in miner rewards.

Consensus protocols serve as the backbone of blockchain networks. They are responsible for achieving agreement on the network's state among distributed nodes, a critical requirement for maintaining the decentralized and tamper-proof nature of blockchains.

Proof of Work (PoW), the original consensus mechanism utilized by Bitcoin, requires miners to solve complex mathematical problems to validate transactions and mine new blocks. This process, known as mining, necessitates significant computational power, making PoW networks secure but energy-intensive.

Proof of Stake (PoS), in contrast, selects validators based on the number of tokens they hold and are willing to "stake" as collateral. This method is less energy-intensive but tends to favor wealthier participants, potentially leading to centralization.

Mazze's choice of PoW is underpinned by the belief that it offers a more democratized and fair means of participating in the network. Unlike PoS, which could potentially privilege wealth over contribution, PoW rewards miners based on their computational contributions, aligning rewards more closely with effort and investment in the network's security. Furthermore, Mazze addresses the environmental concerns traditionally associated with PoW through innovations in energy-efficient mining and parallel block processing.

2.3. Data Structure

The blockchain architecture of Mazze features a hash tree data structure, which plays a pivotal role in the secure and efficient storage of transaction data. This choice of data structure is instrumental in achieving an optimized balance between rapid verification processes and the facilitation of complex and large-scale transaction management. Within this framework, each block on the chain houses multiple transactions, with each transaction being uniquely identifiable through its own hash value. This structuring allows for enhanced data integrity and security.

Further refining its architectural efficiency, the Mazze blockchain incorporates advanced strategies for data pruning and state management. These strategies are designed to address the critical need for scalability within the blockchain environment. The data pruning methodology particularly focuses on the removal of redundant or obsolete data, thereby streamlining the storage requirements and enhancing the overall performance of the system. In conjunction with this, the state management aspect of the system ensures that the blockchain can effectively handle the dynamic changes in state that occur as a result of the continuous addition of new blocks and transactions. This holistic approach to data structure and management positions Mazze as a robust platform capable of supporting complex, large-scale transactional ecosystems, while maintaining the high-security standards and efficiency required in modern blockchain applications.

2.4. Cryptography and Security

Mazze employs cutting-edge cryptographic techniques to ensure top-tier security within its blockchain infrastructure, incorporating SHA-256 for hashing purposes. This robust algorithm is pivotal in generating unique, irreversible hash values, safeguarding data integrity and thwarting unauthorized data tampering. Additionally, the implementation of multi-signature wallets adds a layer of security, requiring multiple parties to authorize a transaction, thus reducing the risk of fraud or single points of failure. The two-factor authentication further fortifies user accounts against unauthorized access, adding an essential security layer.

The architecture of Mazze is conscientiously designed to be impervious to prevalent blockchain vulnerabilities. It effectively counters the risks associated with 51% attacks, where an entity gains majority control of the network's hashing power, posing a threat to the network's integrity. By leveraging advanced design principles and security protocols, Mazze minimizes the feasibility of such attacks, ensuring a decentralized and secure network.

Moreover, the system is fortified against double-spending, a significant concern in digital transactions where the same digital token could be spent more than once. Mazze's underlying technology and consensus mechanisms are engineered to detect and prevent such fraudulent activities, thereby preserving the sanctity of the transactional process.

Sybil attacks, wherein a single entity creates multiple fake identities to gain a disproportionate influence over the network, are also effectively thwarted. Mazze's security framework incorporates mechanisms to identify and mitigate such attempts, ensuring the network's democratic and equitable operation.

3. Mazze Insights

Mazze is a Proof-of-Work (PoW) blockchain network, markedly distinct from predecessors like Bitcoin and Ethereum, primarily due to its parallel block and transaction processing capabilities. This unique approach culminates in a singular, linear chain, deviating from the sequential block processing norm in existing networks. This paper scrutinizes the economic and security advantages of Mazze, particularly in thwarting double-spending attacks.

A critical innovation of Mazze lies in its handling of smart contract storage costs. Unlike Ethereum, where users incur costs only at the contract's initial addition, Mazze implements ongoing maintenance fees. This model economically motivates users towards judicious resource utilization.

The essence of blockchain technology as a secure medium for economic value transfer and programmatic state/storage execution without intermediaries is a delicate balance of several elements. The native token in Mazze, like in other PoW networks, serves multiple functions: a medium of exchange, a unit of account, and potentially a store of value, providing long-term incentives for network engagement. This paper further explores the role of native tokens in network adoption and utilization.

Mazze introduces a novel PoW network with a Turing-complete smart contract language and a Directed Acyclic Graph (DAG) structure for parallel block processing. This architecture significantly enhances transaction throughput and reduces confirmation times.

To address space congestion, Mazze requires users to bond tokens for storage space, with interest payments on these tokens directed to miners. Mazze also revamps the mining reward system, moving away from the winner-takes-all approach to a more cooperative and fair model.

Mazze's account-based framework incorporates Solidity, mirroring the smart contract programming language used in Ethereum, to ease the transition of smart contracts from Ethereum to Mazze. This adoption of Solidity capitalizes on its compatibility with the Ethereum Virtual Machine (EVM), thereby boosting the security and performance of smart contract execution within the Mazze ecosystem. In Mazze, transactions are designed to either initiate financial transfers or to deploy and execute smart contract code. Reflecting key attributes of Ethereum, Mazze integrates an efficient storage system and improved consensus mechanisms, enhancing transaction processing speed and reducing latency. Additionally, drawing from Ethereum's approach, Mazze's security model is structured to guard against a broad array of cyber threats, ensuring the network's reliability and continuous stability.

The Mazze consensus algorithm introduces a cutting-edge approach in blockchain technology by adopting the Weighted Graph Ledger (WGL) framework. This innovative system combines advanced consensus mechanisms and DAG-based ledger structures, offering enhanced security, scalability, and resilience against various types of attacks, notably liveness attacks.

Theoretical results show Mazze's capability to process around 40,000 transactions per second, a huge improvement over Ethereum and Bitcoin. The network is designed to maintain a consistent block generation rate, promising a substantial increase in daily block generation.

4. Smart Contracts

Mazze's smart contract platform distinguishes itself by integrating Solidity as its primary programming language, a strategic choice to enhance the migration of decentralized applications (dApps) from other blockchains like Ethereum. Solidity's alignment with Ethereum Virtual Machine (EVM) compatibility, coupled with its maturity in smart contract development, makes it an ideal language for developing secure, efficient, and interoperable smart contracts. This decision also allows for a seamless transition for developers familiar with EVM-compatible environments. The platform's architecture, designed to support EVM compatibility, ensures versatility and adaptability in blockchain application development. Additionally, Mazze's unique domain-specific language, tailored specifically for blockchain applications and optimized for EVM compatibility, further simplifies and streamlines the development process.

Integrating a robust testing and auditing framework, the platform ensures the reliability and security of contracts deployed on the Ethereum network. This framework includes advanced tools for static and dynamic analysis, formal verification techniques, and comprehensive simulation environments to rigorously test smart contracts under various conditions, ensuring EVM compatibility. Such an environment is vital for identifying potential vulnerabilities and ensuring code integrity before deployment.

Mazze's approach represents a significant advancement in smart contract technology, providing a highly secure and developer-friendly platform that is fully compatible with the Ethereum ecosystem. This is crucial for fostering innovation and trust in blockchain applications across various industries. By leveraging Solidity's capabilities and focusing on a rigorous testing regime that emphasizes EVM compatibility, Mazze sets a new standard for smart contract development in terms of security, efficiency, interoperability, and scalability.

5. Tokenomics and Financial Structure

Mazze introduces a novel Proof-of-Work (PoW) network that incorporates a fully functional smart contract language akin to Ethereum's. A standout feature of the Mazze network is its use of a Directed Acyclic Graph (DAG) structure for processing parallel blocks. This architectural choice leads to reduced confirmation times and a substantial increase in transaction throughput, marking a significant leap in performance capabilities.

To mitigate the issue of space congestion, the Mazze network has implemented a system where users must bond native tokens to secure storage space. This approach inherently discourages unnecessary space occupation, as it involves paying interest on these bonded tokens. Interestingly, this interest payment is redirected to miners, not users, providing a sustained income source for miners. To combat the issue of fairness in mining, Mazze has restructured the block reward system, moving away from the conventional winner-takes-all model. In Mazze, miners are compensated for every block they generate, with certain penalties in place to ensure adherence to the consensus protocol. This system penalizes competing blocks to deter selfish mining, promoting cooperation among miners and enhancing the network's stability and security.

Mazze operates on a model similar to Ethereum, leveraging the Ethereum Virtual Machine (EVM) for its core functionalities. In this model, regular accounts are linked to balances, and smart contract functionality is achieved through state transitions that are transaction-based. Embracing Ethereum's established approach, Mazze relies on Solidity and the EVM, facilitating a seamless integration of smart contract practices and principles from Ethereum's ecosystem.

In Mazze, transactions serve two primary purposes: to initiate payments or to deploy/execute smart contract code. Each block consists of a list of transactions, which are verified by the miner responsible for proposing that block. Nodes in the network maintain a pool of verified transactions that have yet to be included in blocks. Miners engage in a competitive process to incorporate these transactions into new blocks. Unlike Bitcoin's Proof-of-Work (PoW) system, Mazze uses Ethereum's consensus mechanism, which enhances efficiency and security. Additionally, Mazze inherits Ethereum's dynamic adjustment of difficulties to maintain a steady rate of block generation. Each node in the network keeps a local state, which is updated with each new block received.

The Mazze consensus algorithm utilizes a unique Directed Acyclic Graph (DAG) structure as part of the Weighted Graph Ledger (WGL), a novel development in blockchain technology. This algorithm enhances traditional blockchain approaches by integrating a block weight system into a DAG-based ledger, addressing the scalability-security trade-off and providing a robust defense against liveness attacks. The blockchain's structure, known as the DAG-Embedded Tree Structure (DETS), incorporates a DAG within a tree-like framework. In this structure, each block has a single parent but can reference multiple preceding blocks, capturing the temporal relationships between them. This design allows for efficient integration of concurrent blocks, thereby improving both the security and throughput of the blockchain system.

Blocks within this system are interconnected uniquely: they are either normal or special, with normal blocks consistently weighing 1 and special blocks weighing either 0 or a significantly large value, like 1000, based on their mining difficulty. This dual-block system ensures optimal throughput in normal conditions and heightened security during attacks. The Weighted Ledger Selection Rule (WLSR), a modified heaviest chain rule, dynamically weights blocks and guides the selection of the pivot chain within DETS. This pivot chain, along with reference edges, orders transactions linearly, enabling efficient execution and preventing double-spending.

WGL's block generation is rapid, up to one block per second, thanks to the efficient DAG structure and WLSR. This rapid production, combined with the strategic selection of the pivot chain, significantly enhances the scalability and security of the system. Blocks are produced without predefined types; the network assigns types based on historical ledger structure and mining difficulty. The design of WGL makes it suitable for high-throughput cryptocurrency transactions, scalable enterprise blockchain solutions, and decentralized applications requiring robust infrastructure.

In theory Mazze will have the ability to process around 40,000 transactions per second for straightforward payment transactions, which is much higher than Ethereum and Bitcoin, offering at least a hundredfold increase in throughput.

This remarkable improvement is attributed to the DETS structure and the consensus algorithm, enabling a faster block generation rate, no discarded forks, and more efficient utilization of block space. Based on its technical specifications, the main network of Mazze is designed to operate with a consistent block generation rate of one block per second. Consequently, this results in a daily block generation of 60 × 60 × 24, totaling 86,400 blocks each day.

Next we will be examining the intricate architecture of proof-of-work (PoW) blockchains, which necessitates careful crafting to ensure the establishment of proper incentives for user participation and prudent resource consumption. It is vital for miners to be incentivized to maintain network security, just as it is crucial for users and developers to be engaged with blockchain services. We delve into the Mazze blockchain, which stands out due to its high throughput PoW capabilities, and assess how its design is engineered to nurture economically viable incentives that encourage positive social conduct. Our exploration includes an analysis of Mazze's potential for miner revenue and network security, emphasizing the influence of user behavior and key policy variables such as block rewards and interest rates. Furthermore, we will explore how the economic structure of Mazze positions it as an evolution in the landscape of traditional PoW blockchains. It should be noted that while our focus is on the expected economic outcomes based on the network's design, the actual behavior of users in practice is subject to variability.

5.1. Guidelines for Tokens

On the Mazze network, there is a distinctive native token known as *MAZZE*. Each MAZZE is comprised of 1,000,000,000,000,000,000 (10^{18}) smaller units called *Mazzy*. The way transactions are conducted on Mazze parallels the Ethereum network, positioning MAZZE in a role comparable to Ethereum's Ether. This means users conduct transactions by determining a gas limit and setting a gas price, with the latter being expressed in MAZZE.

5.1.1. Rules for Distributing Initial (Genesis) Tokens

The starting quantity of tokens is set at 5 billion (5,000,000,000). Upon the launch of the main network, all these tokens will be initially locked and subsequently released in a phased manner, with distributions occurring on a monthly basis. The allocation of these initial tokens will be divided among the following groups:

5.1.2. Allocation of Storage Resources

A crucial element of the reward structure within the Mazze network is the concept of bonded storage. To deploy a smart contract on the Mazze network, users are required to allocate a certain number of tokens to establish bonded storage. Notably, the interest payments generated by these tokens in bonded storage are consistently distributed to the miners, rather than to the individuals who have locked up those tokens.

As a result, these interest payments effectively create a transfer of value from those using the network's storage space to those responsible for maintaining the network.

The deposit required for securing storage resources on the network is denominated in the native MAZZE token: specifically, 0.5 MAZZE per 1 kB of storage. The procedure operates as follows: A user, such as a decentralized application (dApp) developer, commits a certain amount of tokens as a lockup. When this user utilizes network resources (for instance, by deploying a dApp or storing data generated through dApp execution), the corresponding amount of tokens is deducted from the locked amount and transferred to bonded storage. The interest generated by these bonded storage tokens is then allocated to the miners. For users to retrieve their tokens from bonded storage, they must first release the equivalent amount of storage space they are occupying.

5.1.3. Rewards for Mining Activities

Maintainers of the Mazze network derive their earnings from three primary sources: fees paid by users for transactions, rewards for mining blocks, and interest income generated from users who "rent" space on the blockchain.

User Fees: Users are required to pay miners for executing transactions and altering the state of the blockchain. The fees collected from these transactions are allocated proportionally to the binary base factors of blocks.

Block Rewards: In line with typical Proof-of-Work (PoW) network practices, the mining of a block on the Mazze network yields a reward in the form of newly created coins. This process expands the monetary base, leading to inflation. This inflation rate, driven by block rewards, is represented as r_b. It's important to note that, setting aside any market-induced price fluctuations, these coin-based rewards essentially represent a redistribution of wealth from all existing MAZZE holders to the miner who successfully mines a block.

The initial base block reward is set at 14 MAZZE per block, corresponding to an inflation rate r_b of 8.83%. This base reward is fixed for the first four years. Subsequently, it decreases quarterly by a factor of 0.958, effectively halving approximately every four years, until it reaches a minimum of 3.5 MAZZE per block.

The decentralized network determines block rewards deterministically, but there isn't a predefined quantity of coins awarded to a miner for successfully mining a block. Instead, blocks are grouped into 'epochs,' and rewards are calculated and distributed for each epoch. The protocol assigns a 'weight' to each block based on its features in the directed acyclic graph, essentially gauging its significance in the parallel arranged chain. The reward is then based on this weight.

Storage Interest: When tokens are bonded for storage purposes, the interest generated on these tokens is allocated to miners. Similar to block rewards, the total interest accrued from bonded storage is distributed proportionally, based on the base reward received for each block.

While the intricacies of block rewards can be complex, the fundamental principle remains consistent with other public Proof-of-Work networks: miners contribute computational power, and the more power they provide, the higher their likelihood of winning a block and, by extension, the greater their potential income.

The following section will introduce a calibrated model outlining user adoption and inflation, aiming to offer insights into the projected revenues from mining activities.

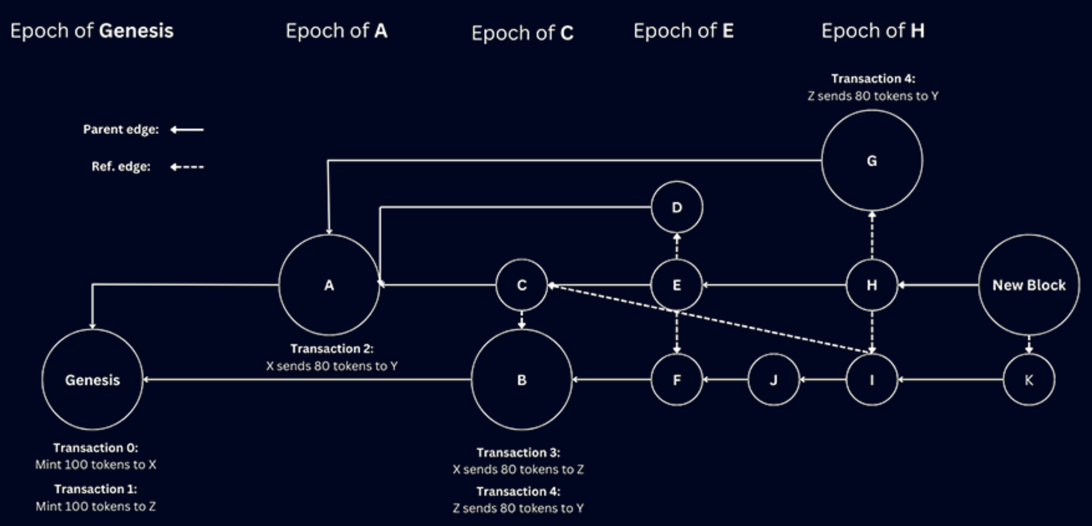


Figure 1: DAG-Embedded Tree Structure (DETS) structure in Mazze

Outlier Penalty Ratio in Mazze: This concept involves adjusting the mining reward of a block based on an Outlier penalty ratio. We establish the penalty ratio for a specific block, referred to as block ***b***, in Mazze's framework.

$$max\left\{0,1-\left(\frac{|Outlier(b)|}{100}\right)^2\right\}$$

The term Outlier(***b***) represents the set of blocks that are neither part of the past sub-graph (those reachable through parent or reference edges from b) nor part of the future sub-graph (those reachable to b through parent or reference edges) of block b. For instance, in Figure 1, Outlier(***F***) comprises blocks A, C, D, and G. The Outlier for a block can expand; however, in this context, Outlier(***b***) only includes blocks within 10 epochs of block ***b***'s epoch. We simplify our explanation by not including difficulty adjustment in this formula, assuming constant difficulty.

The base reward for a new block represents the highest possible reward for its generator. A portion of this reward is deducted for each Outlier block of the new block, potentially reducing the reward to zero. This reward structure is designed to incentivize miners to adhere to the honest behavior outlined in the consensus protocol.

The incentive mechanism in Mazze encourages miners to reference as many blocks as possible to reduce the occurrence of Outlier blocks caused by unreferenced blocks. Additionally, it motivates miners to quickly disseminate new blocks, minimizing Outlier blocks that arise from network delays. This approach contrasts with Bitcoin's longest chain rule, where the winner takes all. In Mazze, every block earns a reward, and miners collaborating with each other can effectively reduce the Outlier, enhancing security against selfish mining attacks that exploit Bitcoin's mining structure.

In our model, we simplify by assuming the Outlier is non-existent, implying that miners reference all preceding blocks accurately without errors.

5.1.4. Evolution of the Mazze Rate

The freely traded MAZZE tokens' market price, influenced by the permissionless nature of Mazze's network, is beyond the control of Mazze. While speculation is inevitable, it is anticipated that the token's price will ultimately reflect the demand for Mazze's services. We present a formal model to illustrate the relationship between service usage and token price.

The MAZZE price primarily depends on two factors: the system's inherent inflation and the token's market price externally. This is similar to covered interest parity, an economic principle explaining fluctuations in exchange rates. In our model, p_0 represents the current fiat price of MAZZE, p_1 the future price (specifically, the 1-year forward rate), $r_c + r_b$ the real interest rate in Mazze (comprising both block rewards and storage interest payments), and r the compounded-average real interest rate in the fiat economy, considering a range of major fiat currencies.

$$p1 = p0 \times \frac{1 + r}{1 + r_c + r_b}$$

Put simply, if Mazze offers an interest rate higher than what fiat markets provide, it is expected that the price of MAZZE will naturally decline over time.

5.2. Calibrated Model for Miner Rewards

5.2.1. Overview

A critical aspect for the functioning of a Proof-of-Work (PoW) network is the willingness of miners to invest resources into mining activities in return for compensation. The security of such a network is intrinsically linked to the computational power that miners contribute. Given that procuring computational power is expensive, providing adequate compensation to miners is essential to maintain their participation and, by extension, the security of the blockchain. In this section, we describe our methodology for calculating the expected revenue for miners participating in this system. Our model is calibrated based on our technical specifications and insights from the Ethereum blockchain project, due to its comparable features.

Miners in Mazze earn their income from three main sources: block rewards, user fees, and interest from tokens deposited by users as bonds for storing data on the blockchain.

Block rewards, which consist of newly created tokens, increase Mazze's monetary base. Disregarding any changes in the price of Mazze tokens, an enlargement of the monetary base devalues each Mazze token. Therefore, block rewards essentially constitute a transfer of value from the holders of the native token (who in return receive services like enhanced security and ledger consistency) to the miners.

We believe the most effective way to consider block rewards is through the lens of the annual inflation rate they induce. This interaction between block rewards and block inflation will be comprehensively explored in the following subsection.

User fees are contingent on the actual usage of the blockchain. To estimate these fees, we first need to construct a model predicting user adoption, which is addressed in Subsection 5.2.3. Subsequently, in Subsection 5.2.4., we will calculate the corresponding fee revenue. Likewise, interest payments contribute to the increase of the monetary base. Additionally, the amount of interest paid to miners is influenced by the volume of storage space users opt to utilize; we create a model for this in Subsection 5.2.5. and then calculate the interest payments to miners in Subsection 5.2.6.

In Subsection 5.2.7., we integrate all these elements to ascertain the total revenue miners can expect. We believe the most effective way to consider block rewards is through the lens of the annual inflation rate they induce. This interaction between block rewards and block inflation will be comprehensively explored in the following subsection. The final part of this chapter, presented in Subsection 5.2.8, involves simulating this revenue under various parameters.

To aid in understanding, all notations used in this section are summarized in Table I.

Table I: Results of Non-Linear Least Squares Regression for Ethereum's User Adoption Rate Using Logistic Curve-Fitting

Symbol	Meaning
G	genesis tokens, 5B
D	number of seconds in a day, 60 × 60 × 24
d	days since main-net launch
B	block reward
$b(d)$	block rewards per day, defined in equation (1)
rb	annual inflation rate from block rewards
$u(d)$	user uptake rate ∈ (0, 1); estimated from Ethereum data using equation
u^{ETH}	estimated user uptake rate using Ethereum as a benchmark, described in equation
$u^{fast}(d)$, $u^{slow}(d)$	user uptake rates, modelled based on Ethereum but one where shift in growth occurs faster and another where it occurs slower; defined in equations (4) and (5)
$T(d)$	transactions on day d; computed as u(d) × D × 40,000 (maximum theoretical throughput)
F	average transaction fee paid in fiat-equivalent terms
$F(d)$	total transaction fees paid to miners on day d, defined in equation
α	fraction of tokens that an average user locks up to receive interest payments
r_c	annual rate of inflation created by interest payments in the Mazze blockchain
R	daily interest rate for compound transactions; derived in equation
$\gamma(d)$	fraction of gas used by computations that are not plain token transactions;
β	system required fraction of tokens that need to be put in bonded storage for occupying space.

I(d)	interest income from bonded tokens for miners; defined in equation
p(0)	price of MAZZE on day on mainnet launch
p(d)	inflation adjusted price on day d
G(d)	number of coins outstanding on day d; it is genesis plus interest tokens plus block reward tokens, described in equation
m(d)	total revenue for miners on day d, derived in equation
$\bar{m}(d)$	total miner revenue averaged over 1 year

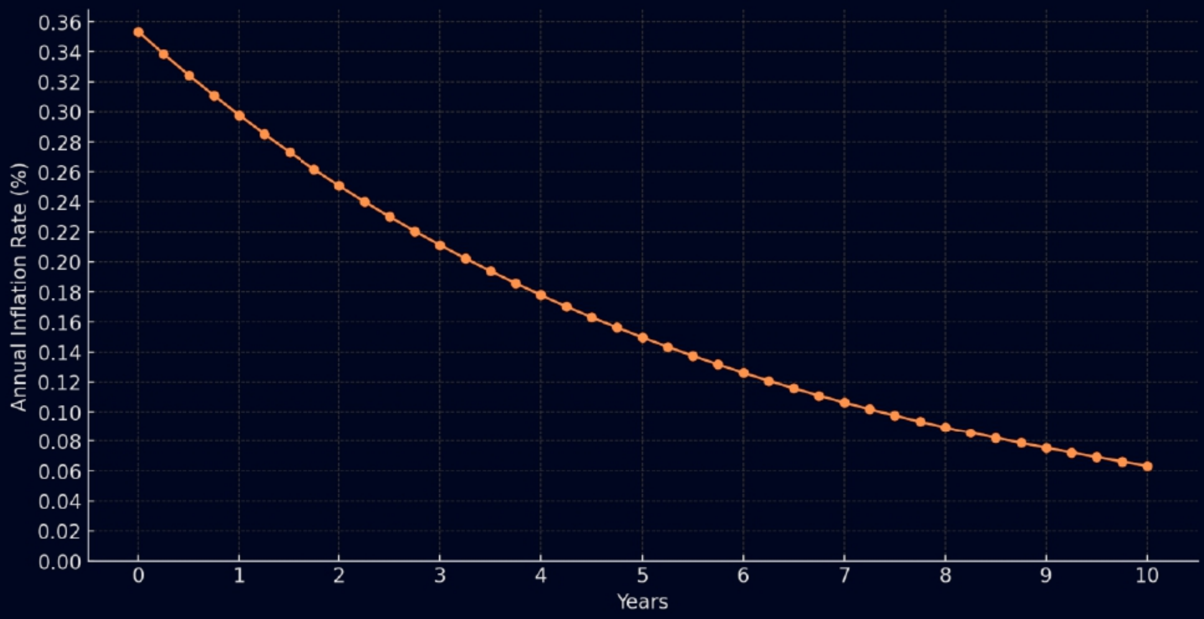
5.2.2. Miner Block Rewards

Miners are compensated per block mined, with the reward amount varying depending on the block's position in relation to the main chain and its Outlier. For the purpose of our calibration, we focus not on the individual block reward but rather on the total daily block reward amount.

As per the technical specifications, the network generates one block every second, equating to 60 × 60 × 24 = D new blocks daily. Assuming a steady mining rate, this results in D × 365 blocks mined annually. If B represents the number of new tokens minted as block rewards for miners, then B × D × 365 new tokens need to be issued each year as block rewards. These block rewards expand the monetary base, leading to inflation. Essentially, by setting a block reward rate, the system can directly control the inflation rate caused by the minting of new blocks. This inflation represents a wealth transfer from token holders to miners. By adjusting the block reward rate, Mazze aims to manage the amount of wealth redistribution within a given year. Mazze's goal is to establish the block reward based on a targeted annual inflation rate of $r_b \in (0, 1)$. Therefore, to meet a specific target value r_b, the block reward must be determined accordingly.

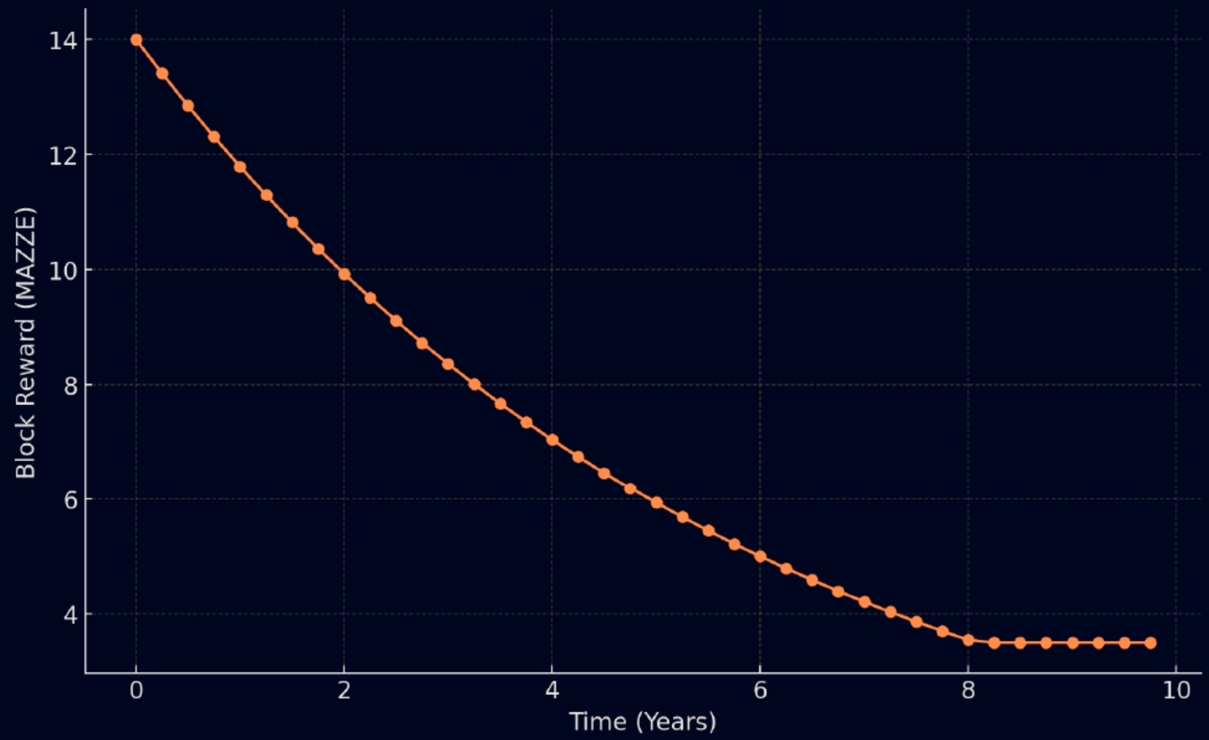
$$B \cdot D \cdot 365 \equiv G \cdot r_b \Leftrightarrow B = \frac{Grb}{365D}$$

It's important to note that in Mazze, blocks are generated continuously and can sometimes be empty if there are no valid transactions. Consequently, the total block rewards given out on any particular day, represented as b(d), will vary accordingly: $b(d) = \frac{2G \cdot rb}{365}$



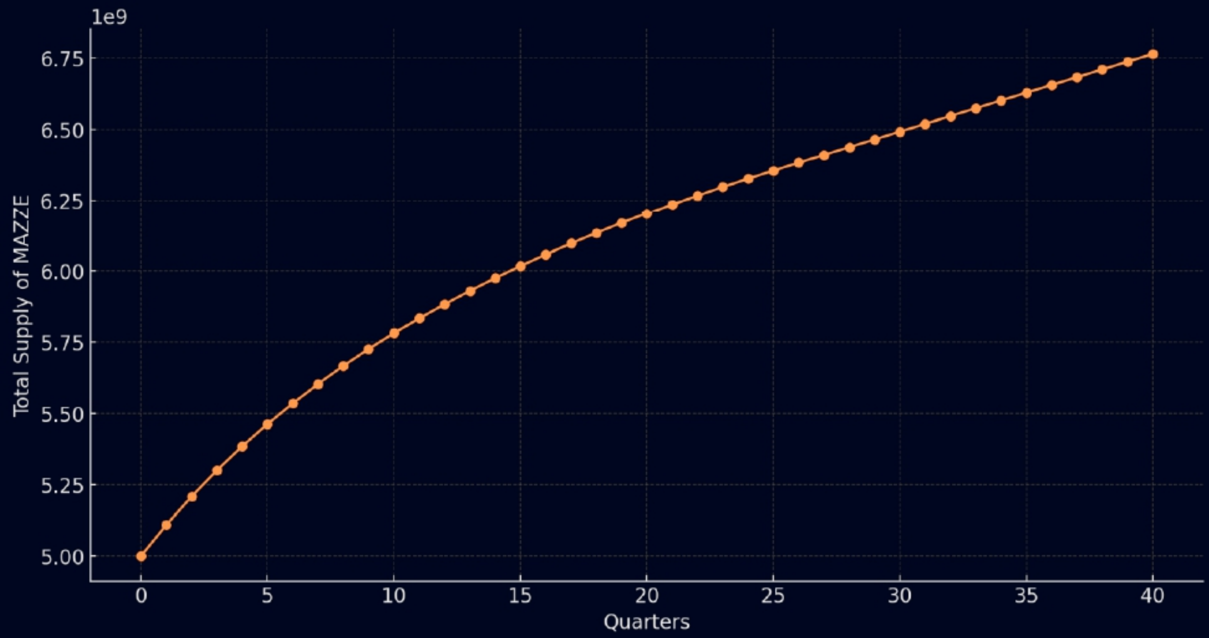
Annual Inflation Rate (First 10 Years)

Annual Inflation Rate chart depicts the annual inflation rate of MAZZE over the first 10 years. Starting at an initial rate of 8.836%, the inflation rate decreases quarterly by a factor of 0.958. The decline is steady, reflecting the protocol's design to reduce the rate of new MAZZE entering the system, a mechanism akin to Bitcoin's halving. This gradual reduction in inflation is intended to bolster the token's value over time, making it less prone to the devaluation that can occur with higher inflation rates. By the end of the 10-year period, the inflation rate approaches a much lower level, signifying a transition to a more stable token economy.



Block Reward Decline (First 10 Years)

The Block Reward Decline chart showcases the decreasing amount of MAZZE awarded per block over a decade. The initial block reward of 14 MAZZE is subjected to a quarterly decrement, resulting in a halving effect approximately every four years. The reward diminishes until it plateaus at the predetermined minimum of 3.5 MAZZE per block. This planned decrease in block rewards aligns with the cryptocurrency's deflationary policy, aiming to create scarcity and potentially increase the token's value as the reward for mining new blocks diminishes.



Total Supply of MAZZE (First 10 Years)

Total Supply of MAZZE chart provides a comprehensive view of the total supply growth of MAZZE tokens over a period of 10 years, segmented by quarters. With a starting point of 5 billion genesis tokens, the supply increases with each new block, considering the inflation rate and decreasing block rewards. The curve's upward trend demonstrates a predictable yet declining growth rate, as influenced by the protocol's deflationary strategy. This strategy is often employed in cryptocurrencies to ensure long-term sustainability and value retention by controlling the rate of new token creation.

5.2.3. User Uptake

The level of user engagement with the network is crucial as it influences the demand for transactions and computations, the fees users pay, and the storage rent miners receive. We will delve into these aspects in later subsections, but our current focus is on developing a model for user adoption.

Typically, the adoption of new technologies follows an S-shaped curve, characterized by a gradual increase in usage at the beginning, followed by a rapid surge in activity. A prime example of this can be seen in the adoption of the Ethereum network.

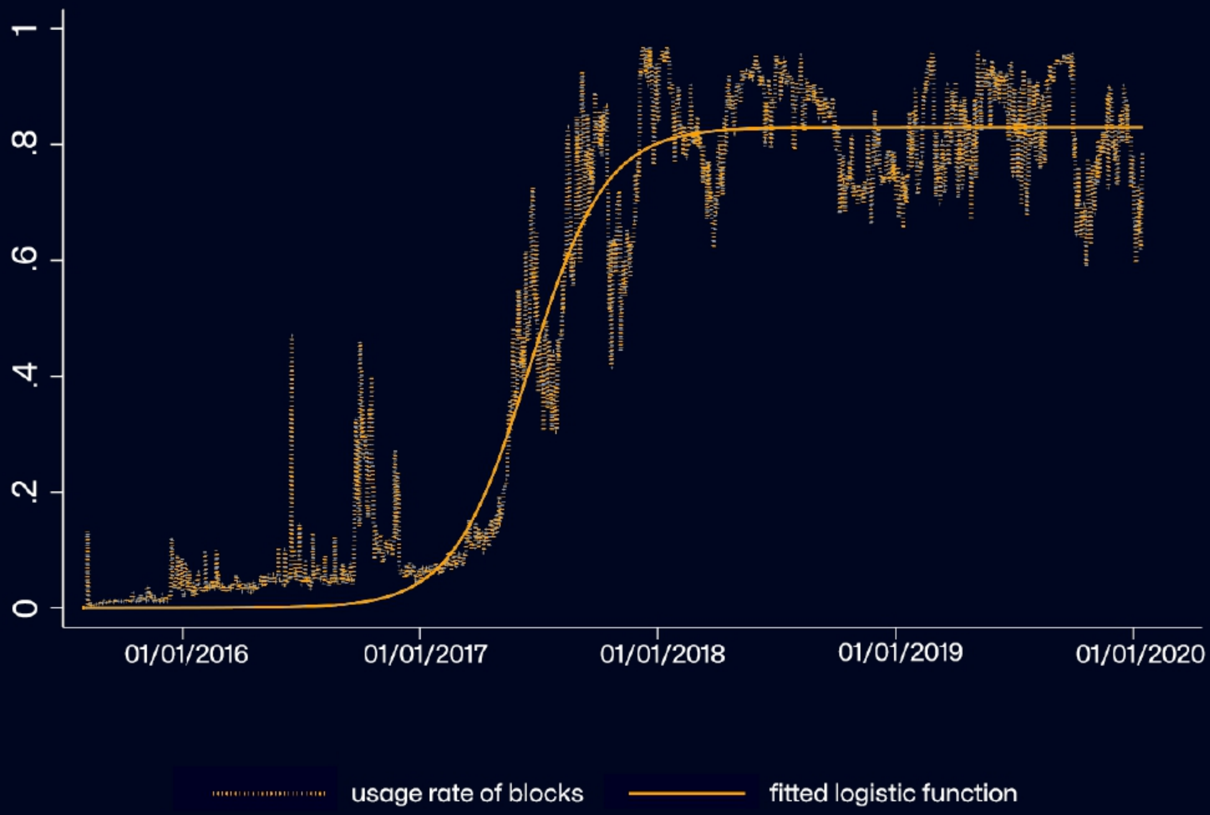


Figure 2

Figure 2 illustrates this trend by **showing the** average daily usage of the gas limit on the Ethereum network, with data sourced from https://etherscan.io/charts

Since Mazze is a novel technology, it's logical to anticipate that its adoption will exhibit an S-shaped curve, similar to other successful technologies. Given the similarities between Mazze and Ethereum, we will utilize the historical adoption data of Ethereum as a basis to project a plausible adoption rate for Mazze.

To begin, we model Ethereum's user adoption rate using a parametric function. There are several ways to represent an S-shaped or sigmoid curve, with one common approach being the logistic function. This function takes the following form:

$$Y = \frac{\xi 0}{1 + \mathrm{e} - \xi 1 \cdot (X - X0)},$$

In the mentioned equation, Y represents the uptake rate at a given time X, ξ_0 is the maximum achievable uptake rate, ξ_1 denotes the growth rate, and X_0 is the time point at which the curve reaches 50% of its maximum value (technically, this is the point on the horizontal axis corresponding to the midpoint of the sigmoid curve). The results of our estimation are displayed in Table II, and Figure 2 also includes the fitted function.

Although it's theoretically possible for blocks to be filled to 100% of the gas limit, our estimate for ξ_0 suggests that the Ethereum blockchain's actual usage rate currently peaks at around 84%. There are several potential reasons for this. One possibility is that miners may be colluding to exclude transactions with lower transaction fees. Another explanation could be that the 84% rate represents a practical, day-to-day technological limit for miners, taking into account the time required for validating transactions and submitting them. Lastly, a graph of daily transactions would have a similar shape. We note that there is an upper bound in transactions because the total amount of gas per block is limited. It's feasible that when the network experiences congestion, users might refrain from initiating new transactions.

Due to prolonged delays, users may choose not to submit transactions to the chain, potentially creating an inherent upper limit on the demand for transaction processing (as seen in the size of the mempool).

According to data from https://bitinfocharts.com/ethereum, transaction fees consistently make up less than 3% of the miners' revenue per block. This suggests that miners might not prioritize fully utilizing the available block space.

Moving forward, our user adoption model, represented as u(d) and ranging from 0 to 1, will be based on the standardized estimates previously established. On any given day d, it is expected that a fraction u(d) of Mazze's total capacity will be in use. The aim is for Mazze to reach a transaction throughput of 40,000 transactions per second.

Given that there are 86,400 seconds in a day, the total number of transactions on day *d* would be $u(d) \times 40{,}000 \times 86{,}400$. We can derive the following:

$$u^{\mathrm{ETH}}(d) = \frac{0.83}{1 + e{-0.017\cdot(\mathrm{d}-690)}}$$

According to our model, it is projected that Mazze will reach 50% of its network capacity in 718 days and attain 70% capacity in 793 days, which is roughly two years.

It's important to note that the actual rate of Mazze's adoption could differ from the modeled predictions, especially in terms of the time it takes to achieve certain levels of adoption. Factors such as ecosystem investments and the development of decentralized applications (dApps) could accelerate this process. The compatibility of Mazze's smart contract platform with Solidity, a primary programming language for Ethereum smart contracts, facilitates easier adoption for many existing blockchain dApp developers from the Ethereum community. This ease of transition contrasts with Ethereum's initial phase, where there was a smaller pool of developers skilled in Solidity. Consequently, a more rapid user uptake for Mazze compared to Ethereum is a reasonable expectation.

In fine-tuning our model, we consider two variations. The first involves shifting the adoption curve 180 days to the right, indicating a delay in adoption by a quarter. The second adjustment shifts the curve 180 days to the left, suggesting an acceleration of adoption by a quarter. Formally, these shifts represent an increase or decrease in the X_0 parameter to 870 and 510 calendar days, respectively, leading to the following adjustments:

$$u^{\text{fast}}(d) = \frac{0.83}{1 + e{-0.017\cdot(\mathrm{d}-510)}}$$

$$u^{\text{slow}}(d) = \frac{0.83}{1 + e{-0.017\cdot(\mathrm{d}-870)}}$$

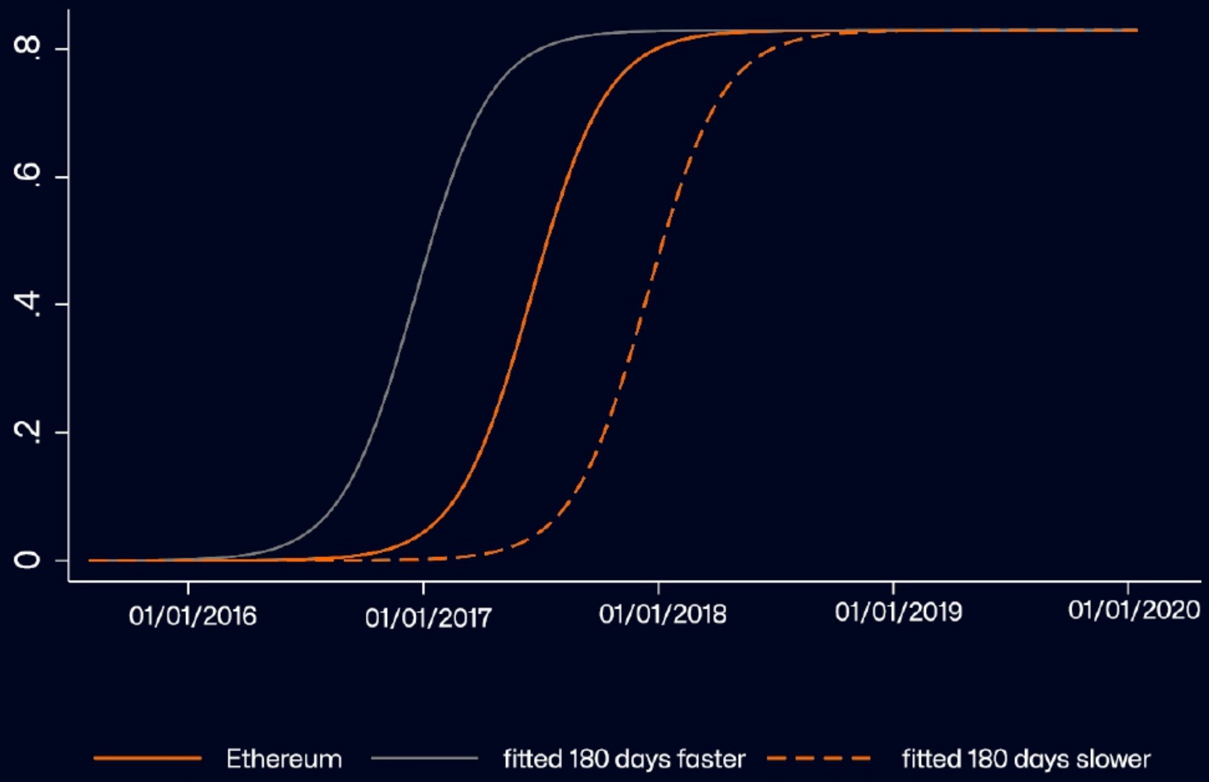


Figure 3: Illustration of the Three Calibrated Adoption Rate Scenarios

Figure 3 depicts three distinct models of adoption rates, identified as *fast* ($u^{\text{fast}}(d)$), based on Ethereum's historical data ($u^{\text{ETH}}(d)$), and slow ($u^{\text{slow}}(d)$).

When operating at full capacity, Mazze has the capability to process 4,000 transactions per second. Assuming a long-term adoption rate of $u(d)$ = 80%, this equates to an expected utilization of 3,200 transactions per second. Given an adoption rate of $u(d)$, the average number of transactions processed daily is calculated as follows:

$$T(d) = u(d) \cdot 4,000D = u(d) \cdot 345.6 \times 10^6$$

We use Ethereum's data to estimate the fractional usage of maximum capacity, and anticipate that Mazze's actual adoption rate may surpass these initial estimates. Our rationale is based on several observations: Firstly, Ethereum often operates at full capacity, as indicated in Figure 2 and by its consistently populated mempool of unconfirmed transactions. This constant full capacity of Ethereum somewhat discourages developers from launching new dApps, particularly those aimed at enterprise-scale applications. In contrast, Mazze’s higher transaction throughput alleviates concerns about delays in transaction confirmations. Furthermore, Mazze's compatibility with Solidity means developers have a minimal learning curve. These factors collectively are likely to lead to a quicker adoption of Mazze compared to Ethereum.

5.2.4. User Fees

Users incur costs for the computational resources they consume, commonly referred to as gas. Blockchain capacity is often measured in transactions per second, where a standard transaction is defined as the transfer of the native token from one address to another. Such transactions require a predetermined amount of gas; for instance, on Ethereum, this is 21,000 gas. Following this standard, we equate user fees to the charges incurred for these simple address-to-address transfers.

We base our calculations on the assumption that users pay an average transaction fee denoted by f. Consequently, the average daily fees, represented as a function of the day $F(d)$, are calculated using the following formula:

$$F(d) := \underbrace{f}_{\text{average daily fee}} \times \underbrace{T(d)}_{\text{number of transactions on day } d} = F \cdot u(d) \cdot 4,000 \cdot D$$

The table provided below showcases various scenarios of annual fee income generated for miners on the Mazze Network. These scenarios are based on the network operating "at capacity" and consider different average fee levels denoted by f.

average	per day	annual
$0.001	$276,480	$88,300,800
$0.005	$1,382,400	$441,504,000
$0.010	$2,764,800	$883,008,000
$0.020	$5,529,600	$1,766,016,000
$0.050	$13,824,000	$4,415,040,000

Assuming Mazze operates at a similar block-usage rate as Ethereum, the total fee income from user fees alone would match Ethereum's combined revenue (from both fees and block rewards) if users are prepared to pay an average of $0.01 per transaction. Even with a moderate level of user willingness to pay fees, the annual income could be significant. For context, the median transaction fee on the Ethereum blockchain during January–February 2020 ranged between $0.08 and $0.15.

Comparing these figures with traditional retail payment networks provides further insight. For instance, credit card transactions, involving entities like Visa or Mastercard and processing banks, usually incur charges between 1%-

3% of the transaction value. Typically, any transaction over $2.5 attracts a minimum fee of $0.05. On another front, FinTech companies like Square charge a flat fee of 2.75% per transaction. Similarly, other platforms that charge a flat per-transaction fee often impose at least $0.15 on users.

5.2.5. Transactions vs. Computations

Until now, we've used the term 'transactions' interchangeably with the use of the underlying network. However, it's important to recognize that a blockchain like Mazze is capable of more than just processing transactions. To illustrate this distinction, refer to Figure 4. In this figure, the solid black line represents the daily number of transactions on the Ethereum blockchain, while the gray line shows the percentile of Gas used specifically for these transactions.

Formally, we derive this line as follows. We obtain from etherscan.io/chart the data series for daily transactions and daily Gas used. A simple transfer of ETH transaction requires 21,000 Gas, and we therefore obtain the non-transaction Gas amount by subtracting the number of transactions times 21,000 from the total gas.

As demonstrated in the figure, over time, the proportion of basic token transactions relative to overall blockchain activity has been decreasing.

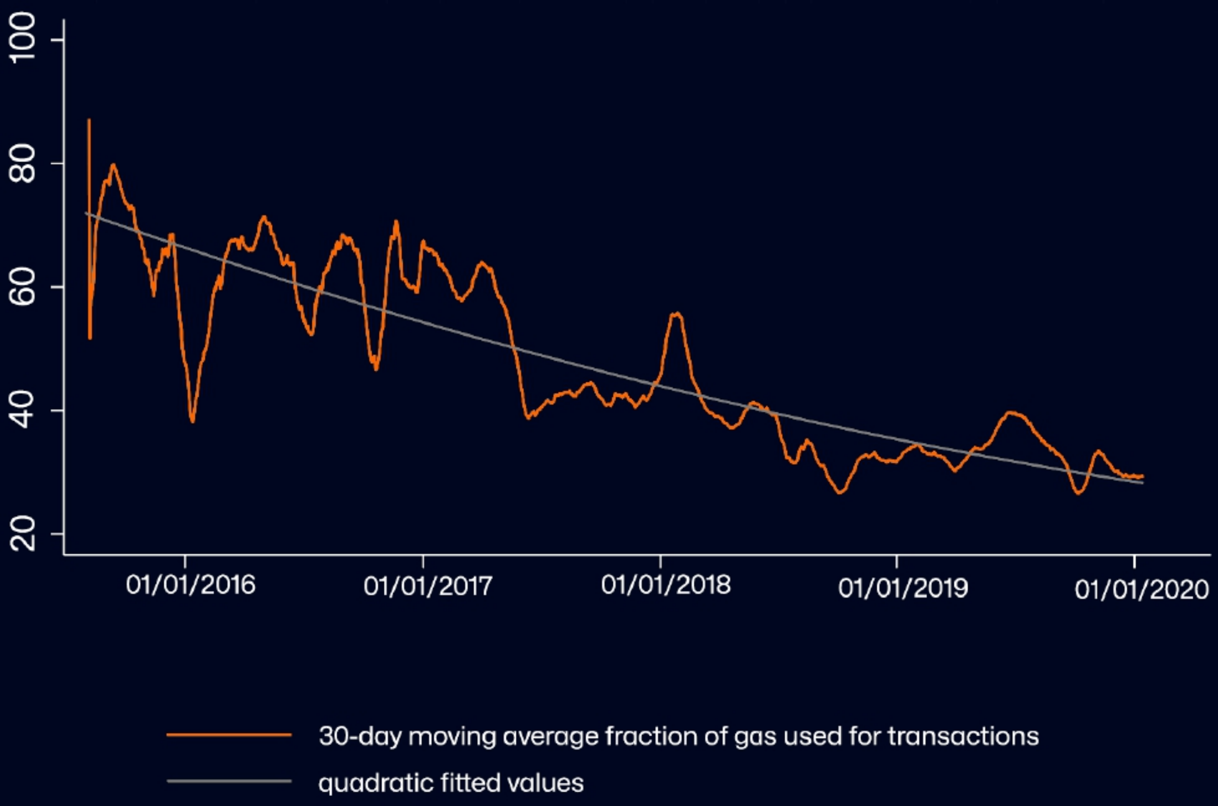


Figure 4: Comparison of Transactions and Computational Activities

In estimating the expected patterns of blockchain activity on the Mazze network, we use the Ethereum blockchain's activities as a reference. Specifically, we conduct a regression for a quadratic fit to analyze the rate of non-transactional gas usage. The equation for this regression is:

$$\%\ \textit{non-transaction gas} = \alpha + \beta_1 \cdot d + \beta_2 \cdot d^2 + \epsilon$$

where *d* represents the number of days since the launch of the mainnet. The aim is to quantify the percentage of non-transactional gas usage within the range ∈ [0, 100].

To refine our analysis, we consider not only the raw rate, which tends to be quite volatile at the start of the dataset, but also the 30-day moving average of the proportion of non-transactional gas used. This approach provides a more stable and representative view of the non-transactional activities on the blockchain. The analysis yields results that are quite consistent. It's notable that the coefficient estimated for the quadratic term, β_2, is quite small, approximately 7.05×10^{-6}, which is attributable to the scale of the variable it's associated with.

Up to this point in the subsection, our focus has been on the use of gas for purposes other than transactions. Moving forward, it's necessary to establish how much interest miners earn for storing smart contract code. We've been assessing miner income in relation to transactions since user fees are charged per transaction, and a block can only contain a certain number of transactions. However, a more intuitive approach might be to base this assessment on gas usage. To maintain consistency in our analysis, we will convert the fraction of non-transactional gas into equivalent hypothetical transactions. Then, we will base the interest payments on these hypothetical transactions. Specifically, we define $\gamma(d)$ as the fraction of gas usage not related to standard MAZZE remittance transactions:

$$\gamma(d) := 1-(72 - 0.04 \cdot d + 7.05 \cdot 10^{-6} \cdot d^2)/100 = -0.0000000007(d-2,837)^2+.85$$

Consequently, for $T(d)$ transactions on day d, we categorize $(1-\gamma(d))\cdot T(d)$ as basic coin transfers and $\gamma(d) \cdot T(d)$ as transactions involving smart contract executions needing blockchain data storage.

5.2.6. Interest Payments to Miners

Users storing data like smart contract code on the chain must deposit a specific number of tokens into bonded storage. These tokens generate interest paid to miners, not to the token depositors. For model calibration, it's assumed users decide daily about keeping tokens in bonded storage, implying total transactions accurately mirror the scale of interest payments. This approach probably underestimates the interest revenue for miners. The model presumes the required tokens for bonded storage are proportional to the contract's gas usage or the number of actual transactions, as each necessitates gas. Therefore, for x transactions, users must deposit $\beta\cdot x$ tokens in bonded storage, and on day d, it's $\gamma(d)\cdot T(d)$ transactions that necessitate this token deposition.

The total necessary amount is calculated as $\beta \cdot \gamma(d) \cdot T(d)$. It's determined that the daily interest received by miners from these bonded tokens, is given by:

$$I(d) := \beta \times \gamma(d) \cdot T(d) \times R$$

5.2.7. Total Miner Revenue

In summary, the overall revenue for miners, denoted as m(d), is composed of the block reward, interest income from bonded tokens, and user fees:

$$m(d) = p(d) \cdot b(d) + p(d) \cdot I(d) + F(d) = p(d) \cdot \frac{Grb}{365} + p(d) \cdot \beta \times \gamma(d) \cdot T(d) \times R + f \cdot T(d)$$

In the following subsection, we will use simulations to demonstrate potential revenue levels using realistic parameters for our model.

5.2.8. Calibration of Miner Revenue

Before examining the calibration outcomes for Mazze miner revenue, it was insightful to review the past earnings of Ethereum miners when it operated under a proof of work system. Approximately 6,500 blocks were produced daily, yielding around 13,500 ETH, which amounted to nearly $30M USD in average daily block rewards (based on early 2020 ETH prices). For Ethereum, transaction fees paid by users contributed minimally to the miners' income. In contrast, user fees were anticipated to have a greater impact on Mazze's revenue due to its higher throughput capacity. Initially, however, transaction volume might have been low as the network was building its user base. Therefore, in our calibration, we considered miner income over extended periods. Calculations of average yearly incomes were presented in intervals of 91 days.

$$m(d) = \frac{1}{365} \sum_{d'=i \cdot 91+\mathrm{d}}^{(i+4) \cdot 91+\mathrm{d}} m(d'), \quad i = 0, \dots, 7.$$

We employ four different average transaction fee scenarios, denoted as f, with values {.005, .01, .02, .08}. The highest fee, \$0.08, is akin to the lower median fee observed on Ethereum in early 2020, as previously mentioned. For the rate of network adoption, we consider three standard rates: $u^{\text{fast}}(d)$, $u^{\text{ETH}}(d)$, and $u^{\text{slow}}(d)$, as outlined in Subsection C. Regarding the requirement for bonded storage, we apply a rate of β = 2%. This implies that if a user utilizes blockchain space equivalent to that used by one virtual-machine opcode transaction, they must allocate 2/100 of a Mazze token to bonded storage.

In the following analysis, we do not presume any market-driven price increases, except in instances where it is specifically mentioned.

Initially, we graphically represent the three elements of miner revenue: block rewards, interest income, and user fees. Figure 5 displays these daily revenue components. In these illustrations, we assume an annual interest rate of r_c = 4%, and an average transaction fee of \$.01.

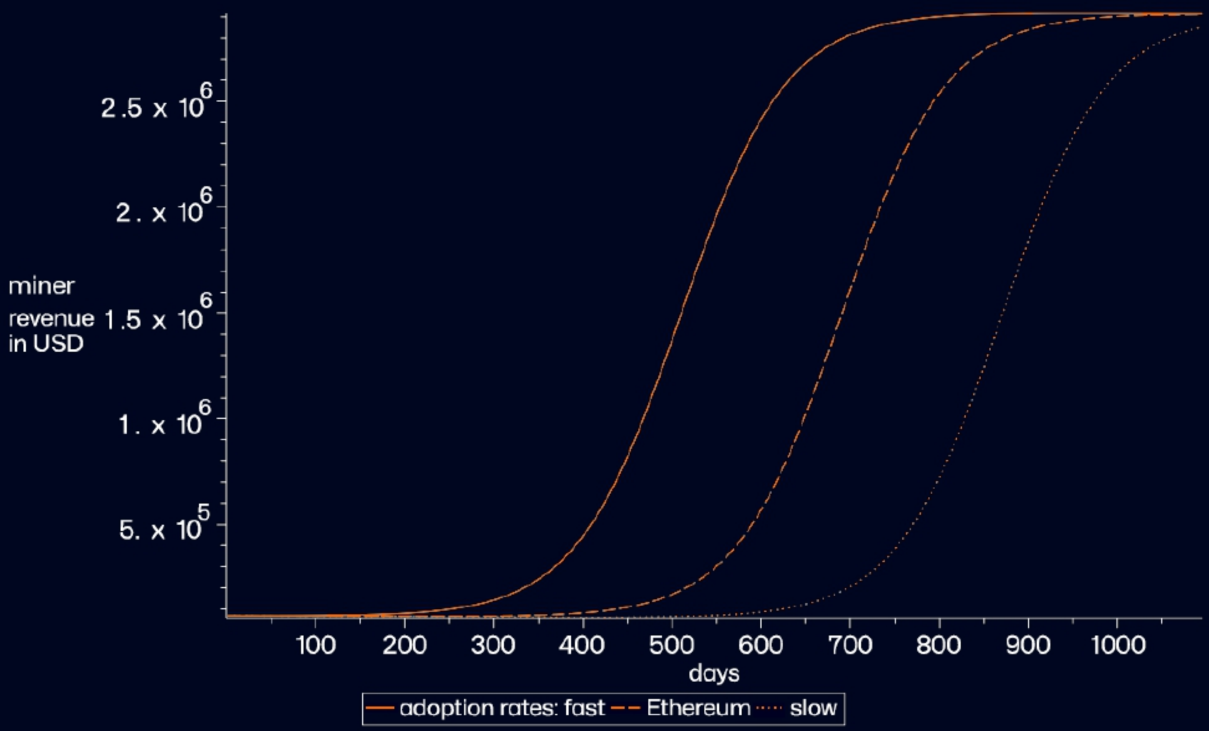


Figure 5: Miner Revenue Trends Based on Adoption Rate

In Figure 5, the dollar value of block rewards decreases due to the price drop caused by inflation. It's important to note that the quantity of tokens awarded per block is considered constant in this interval. For the other two panels, the annual block inflation rate is set at r_b=5%. Interest income increases alongside blockchain activity, yet remains relatively small in total. In contrast, revenue from user fees is illustrated, with the vertical axis values indicating that these fees are likely to be significantly higher than either interest income or block reward income, except just after the mainnet launch.

By merging these three elements, Figure 5 illustrates the projected daily miner revenue $m(d)$ over a three-year period post-mainnet launch, under three different user adoption speed scenarios. This projection assumes an annual block inflation rate of r_b = 5%, annual interest payments of r_c = 4%, and average transaction fees of $.01.

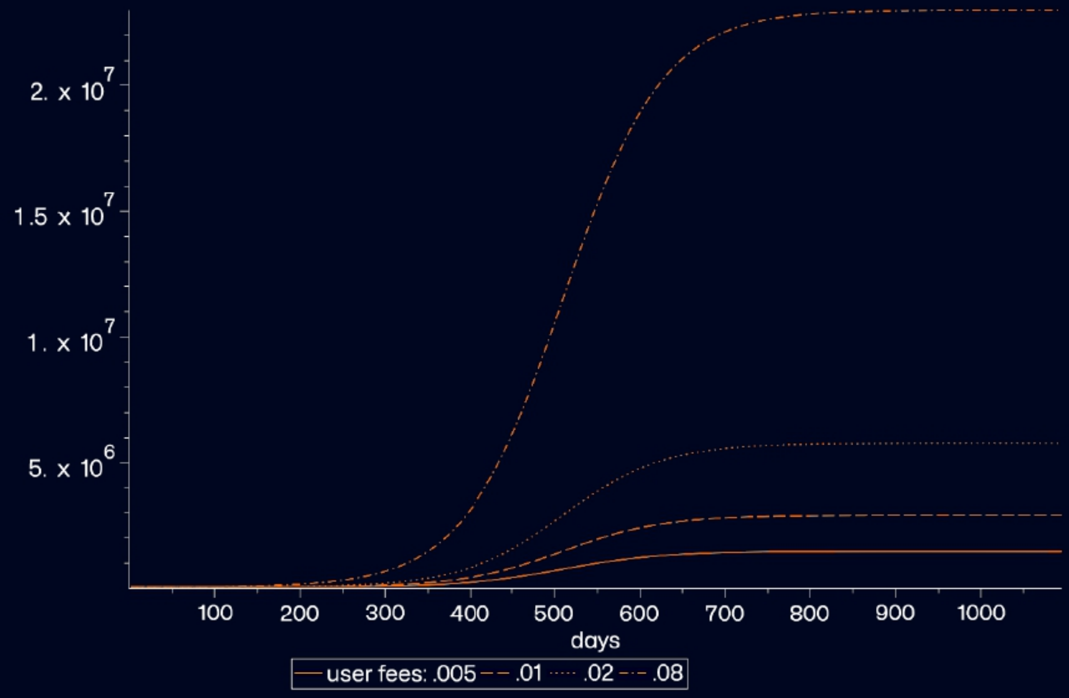


Figure 6: Miner Revenue Trends Based on Average Transaction Fees

Figure 6 presents a time series of expected daily miner revenues, considering four different average transaction fee scenarios. When Mazze operates at full capacity, even with modest fees of $0.02, the miner revenue is anticipated to be around $2.5M. This projection is based on a block inflation rate of 5%, interest payments of 4%, and adoption rates similar to Ethereum. This upward trend is indicative of Mazze's robust economic design, which seems to promise a sustainable and lucrative future for miners. The data underscores Mazze's potential to achieve high scalability and financial viability, with revenue trends that are likely to attract and retain miners, a fundamental aspect for the security and growth of the network.

Mazze presents a groundbreaking advance in blockchain technology, showcasing a unique blend of high throughput, enhanced security, and economic incentives that promote fair participation and stability. With its innovative use of a Directed Acyclic Graph structure, rapid block generation, and a reimagined tokenomics model, Mazze stands poised to redefine the landscape of Proof-of-Work blockchains. Its alignment with Ethereum's established practices further strengthens its potential for widespread adoption, offering a robust and scalable infrastructure for a wide range of applications. As we continue to explore the economic dynamics of this novel platform, it becomes increasingly clear that Mazze not only addresses the limitations of existing blockchain systems but also opens new avenues for growth and innovation in the digital economy.

6. Data Privacy and ZK Proofs Integration

In Phase D of the Mazze project, we will focus on enhancing data privacy and confidentiality. This phase includes the integration of advanced privacy features, notably Zero-Knowledge (ZK) Proofs. ZK Proofs are a cryptographic method that allows for transaction validation without exposing the transaction data, maintaining a high level of confidentiality. This approach is in line with the foundational principles of blockchain technology, which emphasize transparency and security, while addressing the increasing need for privacy in transactions

6.1. Introduction to Zero-Knowledge Proofs

6.1.1. Brief Explanation of ZK Proofs

Zero-Knowledge Proofs (ZK proofs) represent a paradigm shift in the realm of cryptographic protocols, enabling the validation of data authenticity without revealing the data itself. Fundamentally, a ZK proof is a method by which one party, the prover, can prove to another party, the verifier, that a certain statement is true without conveying any information apart from the veracity of the statement.

The essence of ZK proofs lies in their ability to uphold two critical properties: soundness and completeness. Soundness ensures that if the prover is dishonest, they cannot falsely convince the verifier of the truth of a statement. Completeness guarantees that a truthful prover can always validate the truth to an honest verifier. Additionally, the zero-knowledge aspect means that no additional information is disclosed, preserving data confidentiality.

In the context of blockchain, ZK proofs can be implemented in various forms, such as ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) and ZK-STARKs (Zero-Knowledge Scalable Transparent Argument of Knowledge). These implementations differ in their computational requirements, proof sizes, and the need (or lack thereof) for a trusted setup.

6.1.2. Importance of ZK Proofs in Blockchain Technology

The integration of ZK proofs into blockchain technology heralds a new era of privacy and scalability. Traditional blockchain systems, while decentralized and secure, often struggle with privacy concerns and scalability issues. Every transaction and its details are visible on the ledger, posing privacy risks. Moreover, the growing size of the blockchain and the need for every node to process every transaction can lead to scalability bottlenecks.

ZK proofs address these challenges by enabling transactions to be validated without revealing their contents. This feature not only enhances user privacy but also paves the way for more efficient processing of transactions. By validating the correctness of transactions without needing to reveal their full details, ZK proofs can significantly reduce the amount of data that needs to be transmitted and stored on the blockchain, leading to enhanced scalability.

6.1.3. Overview of How ZK Proofs Will Enhance MAZZE

The MAZZE blockchain, being a PoW system utilizing a DAG structure, stands to gain substantially from the integration of ZK proofs. The DAG architecture already offers advantages in terms of scalability and reduced transaction times compared to traditional blockchains. The addition of ZK proofs will further augment these benefits.

In MAZZE, ZK proofs will primarily enhance two aspects: privacy and efficiency. On the privacy front, MAZZE users will be able to execute transactions and interact with smart contracts without revealing sensitive information. This is particularly advantageous for use cases that require confidentiality, such as secure voting systems, confidential transactions, and private smart contract interactions.

From an efficiency standpoint, ZK proofs can reduce the computational load on the network. Since transactions can be verified without needing full exposure of their data, the amount of information that needs to be propagated across the network is minimized. This leads to faster transaction processing times and reduces the storage requirements for nodes, thus addressing some of the inherent limitations of PoW systems.

Moreover, the implementation of ZK proofs in MAZZE is expected to foster a more diverse ecosystem of decentralized applications (dApps). Developers will be able to build applications that leverage the privacy-preserving features of ZK proofs, opening up possibilities for innovative use cases that were previously constrained by privacy concerns.

The introduction of ZK proofs into the MAZZE blockchain is a strategic advancement that aligns with the overarching goals of enhanced privacy and improved scalability. This integration will not only benefit MAZZE users and developers but will also position MAZZE as a forward-thinking blockchain platform at the forefront of technological innovation in the digital ledger space.

6.2. ZK-Proof Types

ZK proofs come in various types, each with unique characteristics and use cases. ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) are known for their efficiency and small proof size but require a trusted setup, making them popular in blockchain applications like Zcash. ZK-STARKs (Zero-Knowledge Scalable Transparent Argument of Knowledge) offer similar benefits without the need for a trusted setup and are quantum-resistant, thus providing enhanced security. Bulletproofs, another variant, eliminate the need for a trusted setup and are particularly efficient when batching multiple proofs, although they have larger proof sizes and longer verification times than SNARKs. Each of these types represents a different approach to achieving zero-knowledge, balancing factors like computational efficiency, proof size, and security assumptions, making them suitable for diverse applications in digital privacy and secure communication.

Criteria	ZK-SNARKs	ZK-STARKs	Bulletproofs
Setup Requirement	Trusted Setup	No Trusted Setup	No Trusted Setup
Proof Size	Very Small	Larger than SNARKs	Smaller than STARKs, larger than SNARKs
Computation Time	Very Fast	Fast	Slower than SNARKs and STARKs
Quantum Resistance	No	Yes	No
Trust Assumptions	High	Low	Low
Scalability	Moderate	High	Moderate
Use Cases	Private transactions, Blockchain scalability	Private transactions, Quantum-resistant applications	Confidential transactions, Range proofs

This table provides a concise overview of the key differences between ZK-SNARKs, ZK-STARKs, and Bulletproofs, highlighting aspects such as setup requirements, proof sizes, computation times, resistance to quantum computing, trust assumptions, scalability, and typical use cases.

6.2.1. Detailed Explanation of ZK-STARKs

Zero-Knowledge Scalable Transparent Argument of Knowledge (ZK-STARKs) is an advanced cryptographic protocol that provides a way to prove the validity of a computation without revealing any additional information. They are a breakthrough in the field of zero-knowledge proofs due to their unique properties.

ZK-STARKs are built upon the concept of polynomial commitments, where computations are represented as polynomials. The prover demonstrates that they know a polynomial that satisfies certain conditions (corresponding to the computation or transaction in question) without revealing the polynomial itself. This is achieved through a series of interactive or non-interactive cryptographic protocols.

6.2.2. The Meaning of 'STARK' in ZK-STARK

'STARK' in ZK-STARK stands for Scalable, Transparent, Argument of Knowledge:

Scalable: They can handle complex computations and large datasets efficiently. Scalability is achieved through the use of FRI (Fast Reed-Solomon Interactive Oracle Proofs) protocol, enabling the compression of computational proofs regardless of their size.

Transparent: Unlike ZK-SNARKs, ZK-STARKs do not require a trusted setup. The absence of a trusted setup removes certain security risks and makes the system more robust against potential vulnerabilities.

Argument of Knowledge: This aspect ensures that the prover possesses explicit knowledge of the proof, rather than merely having a probabilistic assurance of its truth.

6.2.3. Why we chose ZK-STARKs

MAZZE’s blockchain architecture presents specific challenges and requirements that make ZK-STARKs an ideal choice. MAZZE's DAG structure, known for its potential in high transaction throughput, aligns well with the scalability offered by ZK-STARKs. The scalability feature of ZK-STARKs means that as MAZZE grows and processes more complex transactions and smart contracts, the ZK proofs will not become a bottleneck.

As a future-proofing strategy, MAZZE's adoption of ZK-STARKs is strategic due to their quantum resistance. Unlike ZK-SNARKs, which rely on elliptic curve cryptography potentially vulnerable to quantum attacks, ZK-STARKs use hash-based cryptography, making them more secure against quantum computing threats. The absence of a trusted setup in ZK-STARKs eliminates the risk of hidden vulnerabilities associated with the setup phase. This transparency is crucial for MAZZE, aiming to maintain a high-security standard and trust within its community.

Implementing ZK-STARKs in a blockchain supporting EVM and Solidity requires thoughtful integration. The computation model of ZK-STARKs is conducive to representing and verifying complex computations, which is essential for smart contracts written in Solidity. This compatibility ensures that existing smart contracts on MAZZE can benefit from the enhanced privacy and security without significant modifications.

ZK-STARKs, due to their non-reliance on complex cryptographic assumptions and minimal energy requirements for proof generation, align well with the sustainability goals of MAZZE. In a PoW system, where energy efficiency is often a concern, ZK-STARKs offer a way to add functionality without significantly increasing the energy footprint.

6.3. Understanding the Functioning of ZK-STARKs

In ZK-SNARKs, the "prover" performs a computation and generates a proof, demonstrating that they know certain information (like a secret key) or have performed a specific computation correctly, without revealing the details of the information or the computation.

```
def generate_proof(computation, input_data, secret):
    """
    Generate a ZK-STARK proof for a given computation.

    :param computation: The computation or transaction to be proven.
    :param input_data: Public input data for the computation.
    :param secret: Secret data or witness that proves the computation is correct.
    :return: A proof object.
    """
    # Step 1: Represent the computation as a polynomial
    polynomial = convert_computation_to_polynomial(computation, input_data, secret)

    # Step 2: Use FRI protocol to create a commitment to the polynomial
    commitment = FRI_commit(polynomial)

    # Step 3: Generate a proof that the polynomial satisfies the computation
    proof = generate_polynomial_proof(polynomial, commitment)

    return proof
```

This proof is then sent to the "verifier", who can quickly and efficiently check the validity of the proof without learning anything about the secret information. The "succinct" nature of ZK-SNARKs means that the proofs are small in size and quick to verify, making them particularly useful for applications where efficiency and privacy are paramount, such as in blockchain transactions. The process involves complex mathematical techniques, including the use of elliptic curve pairings and cryptographic hash functions, to construct a secure and efficient proof system.

```
def verify_proof(computation, input_data, proof):
    """
    Verify a ZK-STARK proof.

    :param computation: The computation or transaction to be verified.
    :param input_data: Public input data for the computation.
    :param proof: The proof object to be verified.
    :return: True if the proof is valid, False otherwise.
    """
    # Step 1: Check the proof against the committed polynomial
    is_valid = verify_polynomial_proof(computation, input_data, proof)

    return is_valid

# Example usage
computation = "some_complex_computation"
input_data = "public_input_data"
secret = "secret_witness_data"

# Generate a proof
proof = generate_proof(computation, input_data, secret)

# Verify the proof
is_proof_valid = verify_proof(computation, input_data, proof)
print("Proof valid:", is_proof_valid)
```

Thus, ZK-SNARKs provide an elegant solution for maintaining confidentiality and integrity in digital interactions, notably enhancing security in decentralized environments like blockchains.

6.4. Technical Implementation of ZK Proofs in MAZZE

The integration of ZK Proofs into the MAZZE blockchain, which operates on a Proof of Work (PoW) mechanism and employs a Directed Acyclic Graph (DAG) architecture, presents a unique set of technical challenges. This integration aims to enhance privacy and efficiency without compromising the existing strengths of the blockchain. This subchapter delves into the technical specifics of embedding ZK Proofs into MAZZE's architecture, focusing on its PoW and DAG structure, modifications to the Ethereum Virtual Machine (EVM) and Solidity smart contracts, and handling data privacy and transaction validation.

6.4.1. Integration with MAZZE's Architecture

The first step involves embedding ZK Proofs within the PoW consensus mechanism and DAG framework. In a typical PoW system, miners solve complex mathematical problems to validate transactions and create new blocks. Integrating ZK Proofs requires these miners to also validate ZK Proof-based transactions. This integration ensures that transactions remain private while still being verifiable by the network.

The DAG architecture of MAZZE, known for its ability to handle a higher throughput of transactions compared to traditional blockchain structures, poses an additional layer of complexity. The integration here involves ensuring that the DAG can effectively handle the additional data and computational requirements of ZK Proofs. This might necessitate optimizing the DAG algorithm to efficiently process and order ZK Proof transactions, ensuring they are consistent with the network's overall state.

6.4.2. Modifications to the EVM and Solidity Smart Contracts

The next critical aspect is the modification of the EVM and Solidity smart contracts to support ZK Proofs. Since Solidity is the language used for writing smart contracts in MAZZE, it is imperative to develop new libraries and tools within the Solidity framework that can generate and verify ZK Proofs. This involves creating functions that allow smart contracts to interact with ZK Proof protocols, enabling them to execute private transactions and maintain confidentiality of sensitive data.

For instance, a Solidity smart contract could be designed to use ZK Proofs for verifying a user's credentials without revealing the actual credentials. Implementing these features requires deep integration with the EVM, ensuring that it can process and execute these enhanced smart contracts efficiently.

6.4.3. Handling Data Privacy and Transaction Validation

The implementation of ZK Proofs significantly enhances data privacy on the MAZZE blockchain. By allowing transaction validation without revealing the actual transaction data, ZK Proofs ensure that sensitive information is not exposed on the public ledger. Additionally, transaction validation mechanisms must be adapted to accommodate ZK Proofs. Validators in the MAZZE network would need to be equipped with the tools and knowledge to verify ZK Proof transactions. This might involve updating the node software across the network and providing extensive training and documentation to the network participants.

The technical implementation of ZK Proofs in the MAZZE blockchain is a multifaceted endeavor. It necessitates a careful balance between enhancing privacy and maintaining the integrity and efficiency of the blockchain. This integration not only positions MAZZE at the forefront of blockchain innovation but also sets a new standard for privacy and security in the blockchain domain.

7. Performance Metrics and Optimization

The significance of monitoring and enhancing performance metrics, also known as Critical Performance Indicators (CPIs), cannot be overstated. These metrics are essential for evaluating the efficiency, speed, and overall health of a blockchain network. They serve as vital tools for identifying areas needing improvement, ensuring the blockchain operates at optimal levels, and maintaining user trust and engagement. Effective optimization of these indicators is crucial for the success and sustainability of any blockchain initiative.

The Mazze project, a Layer 1 blockchain utilizing PoW and DAG for achieving high throughput and low finality times, emphasizes performance metrics and optimization through continuous monitoring and adjustment of Key Performance Indicators (KPIs). These KPIs include transaction throughput, block time, network latency, and node health. The initiative ensures efficient and reliable network performance by leveraging real-time data to optimize these metrics, crucial for the blockchain's scalability, security, and user experience.

To elaborate, in the context of Mazze, the implementation of sophisticated monitoring systems is critical for the proactive identification and resolution of network inefficiencies. This involves a multifaceted approach, where each KPI is not only tracked but also analyzed in the context of overall network performance. For instance, transaction throughput is continuously monitored to ensure the network meets its target of 100,000 transactions per second (TPS). Any deviations are promptly addressed by adjusting network parameters or deploying additional resources.

Similarly, block time and network latency are closely scrutinized to maintain the blockchain's promise of 1-second finality. The health of individual nodes is also a priority, as it directly impacts the robustness and decentralization of the network. Advanced diagnostic tools and predictive analytics are employed to anticipate potential issues, ensuring swift remedial actions are taken to sustain optimal network health.

Moreover, Mazze's emphasis on optimization extends beyond mere reactive measures. The project invests in research and development to continually enhance its underlying algorithms and data structures. This includes refining its DAG architecture and consensus mechanisms, as well as exploring innovative cryptographic techniques and efficiency improvements in its PoW protocol.

The overarching goal for Mazze is not just to maintain but to elevate the standards of blockchain performance. By focusing on KPIs as the cornerstone of its optimization strategy, Mazze aims to set a new benchmark in blockchain efficiency, reliability, and user satisfaction. The commitment to continuous improvement, driven by precise and actionable data, reflects Mazze's dedication to being at the forefront of blockchain innovation.

8. Interoperability with Existing Systems

In Phase D of Mazze's development, interoperability emerges as a strategic imperative, vital for realizing the platform's vision of a unified digital ecosystem. This phase focuses on integrating Mazze with a diverse range of digital and blockchain systems, underscoring the platform's commitment to universal applicability and ease of use. The technical architecture facilitating this interoperability is founded on robust APIs, adaptive protocols, and standardized data exchange mechanisms, ensuring a seamless, efficient bridge between Mazze and external systems.

This cross-platform integration is poised to enhance the utility and adoption of blockchain technology across multiple sectors. In finance, for example, Mazze's interoperability could enable more streamlined transactions and improved security protocols. In healthcare, it could facilitate secure and efficient patient data management across various platforms. Similarly, in education, interoperability with Mazze could revolutionize the management of educational credentials and records, making them more accessible and verifiable.

However, implementing such a comprehensive interoperability strategy is not without its challenges. These include technical hurdles related to compatibility with legacy systems, ensuring data privacy and security during cross-platform exchanges, and maintaining operational efficiency. Mazze addresses these challenges through a combination of cutting-edge technological solutions, strategic partnerships, and continuous innovation.

Looking ahead, the successful implementation of interoperability in Phase D is expected to significantly impact the blockchain domain. It will not only enhance the functionality and appeal of the Mazze platform but also contribute to the broader adoption and maturation of blockchain technology. This step is seen as a milestone in creating a more interconnected, efficient, and user-friendly digital landscape, paving the way for new opportunities and innovations in the blockchain space.

9. User Interface and Experience

9.1. Community and Stakeholder Engagement

Engaging the community and stakeholders is a crucial element in the realm of blockchain projects, significantly contributing to their development and creative advancement. This engagement, far from being a mere formality, is the lifeblood that nourishes the ecosystem, ensuring its relevance and sustainability. For Mazze, this principle is not only acknowledged but actively pursued as a core strategy. The commitment to engaging with its community is evident in its approach of providing regular updates, establishing open forums for feedback, and implementing incentivization programs for active contributors. This strategy is further exemplified by the collaboration with Zealy, a multifaceted platform in the crypto and blockchain space.

Zealy's role in enhancing Mazze's community engagement is multilayered. By gamifying the process of community interaction, Zealy transforms passive community members into active contributors. This is achieved through a system of quests and rewards, which not only incentivizes participation but also fosters a sense of belonging and investment in the project's success. For Mazze, leveraging Zealy's capabilities means tapping into a rich vein of organic growth, enhancing social media engagement, and gaining valuable insights into community behavior. This is crucial in a landscape where understanding and responding to community needs and trends is vital for success.

Prior to Mazze's public sale, a strategic move is made to host a competition on Zealy, signaling a deep understanding of the value of community engagement in the pre-launch phase. This competition is not just a one-off event but part of a series of ongoing contests designed to maintain engagement and interest over time. These contests serve multiple purposes: they keep the community active and involved, provide Mazze with continuous feedback and ideas, and help to attract new members to the community.

For blockchain projects and crypto investors alike, Zealy serves as a bridge. Projects gain tools for growth and engagement, while investors find a platform for discovering new DeFi projects and unique investment opportunities. This duality of purpose aligns perfectly with Mazze's objectives of growth, transparency, and community involvement. The gamified approach and incentivization model of Zealy are not just gimmicks but strategic tools that Mazze employs to foster a robust and dynamic community.

9.2. User Interface and Experience

The user interface and experience design of Mazze is an exemplar of cutting-edge software engineering, crafted to provide an optimal balance between intuitiveness for beginners and comprehensive functionality for advanced users. Anchored in the principles of human-computer interaction, the interface simplifies complex blockchain operations through a meticulously organized layout, offering a clear, linear navigation path and minimizing cognitive load. This is further augmented by a robust suite of educational resources and interactive tutorials, tailored to demystify blockchain technology and foster user empowerment.

Customization features are intricately woven into the fabric of the platform, offering a plethora of adjustable settings that cater to individual user preferences. These settings encompass a wide array, including aesthetic choices like themes and color schemes, functional elements like dashboard layouts and data visualization tools, and accessibility options to ensure inclusivity for all users. For the more technically inclined, Mazze offers an advanced suite of analytical tools, real-time data tracking, and API integrations, enabling a high degree of control and customization over their blockchain interactions.

Additionally, the platform integrates user feedback mechanisms and adapts dynamically to evolving user behaviors, ensuring a continuously improving and user-centric experience. Security and privacy are also paramount, with the interface incorporating state-of-the-art encryption and data protection measures. In essence, Mazze's interface stands as a paragon of user experience design, seamlessly marrying simplicity with sophistication, and making blockchain technology accessible and manageable for a diverse user base.

9.3. Feedback Mechanisms and User Involvement

Incorporating feedback mechanisms and fostering user involvement are pivotal elements in blockchain projects, where the intricate balance of technical precision and user-centric design is vital. For Mazze, this approach is not just theoretical but a practical, ongoing process. The platform is envisaged as a dynamic ecosystem, continuously evolving through user interaction and feedback. This is not limited to mere suggestions; rather, it encompasses a comprehensive feedback loop, where user inputs are systematically analyzed and incorporated into the development cycle. Specialized channels on Discord serve as the nerve center for this interaction, where users can open tickets to address specific issues or propose enhancements. These channels are more than just support lines; they are interactive forums where ideas are exchanged, issues are debated, and solutions are crowdsourced. The user feedback is not just passively received but actively sought, with regular polls, AMAs (Ask Me Anything sessions), and focused discussion threads to gauge user sentiment and preferences. This feedback then translates into tangible platform enhancements, be it in the user interface, transaction processing mechanisms, or security protocols. The technical team at Mazze leverages this user feedback to fine-tune the platform, ensuring that it not only meets but anticipates user needs. The incorporation of advanced analytics tools aids in deciphering patterns and trends from user interactions, enabling the team to proactively address potential issues and innovate. User experience on Mazze is not a static feature but a dynamic attribute, continuously refined through a symbiotic process involving user feedback and technical innovation. This approach ensures that Mazze remains at the forefront of blockchain technology, offering a user-friendly, secure, and efficient platform that resonates with its user base. The integration of user feedback into the development lifecycle is a testament to Mazze's commitment to user-centric design, setting it apart in the ever-evolving landscape of blockchain technology.

10. Security and Compliance

10.1. Decentralization Level

Decentralization in blockchain projects is a pivotal aspect that significantly impacts their security, efficiency, and overall network health. In the case of Mazze, achieving an optimal level of decentralization is a core objective, strategically designed to enhance network security and operational efficiency. By meticulously balancing decentralization, Mazze aims to optimize network performance while averting central points of failure or control. This delicate equilibrium is achieved through innovative architectural decisions and the integration of advanced consensus mechanisms.

In line with this vision, the Mazze team plans to introduce a unique approach to token distribution and network participation. A key strategy involves the creation of a wrapped version of its native token on a popular blockchain, which will be made available through a public sale. This initiative allows users to acquire these tokens easily, which can later be converted to the native currency via a bridge. Such a design is ingeniously crafted to mitigate the risks of token concentration among early miners, especially during the initial phases when mining difficulty is relatively lower.

The genesis block of Mazze will play a critical role in this process. By generating these wrapped tokens in the genesis block, the platform ensures a more equitable and decentralized distribution of tokens from the outset. This approach is a proactive measure against potential centralization issues that often plague new blockchain networks, where early miners or participants could disproportionately influence the network.

Moreover, the implementation of a wrapped token on a well-established blockchain serves multiple purposes. It not only facilitates wider accessibility and liquidity for Mazze's tokens but also leverages the security and stability of the underlying blockchain. This strategic move demonstrates Mazze's commitment to building a robust and decentralized ecosystem, where network security, user accessibility, and efficient performance are harmoniously balanced.

The underlying technology that facilitates this token bridge and wrapped token system is a testament to Mazze's innovative spirit. By employing state-of-the-art cryptographic methods and smart contract functionalities, the platform ensures a secure and seamless conversion process for its users. This technological prowess extends to the platform's overall architecture, where scalability and interoperability are key considerations, ensuring that Mazze remains adaptable and responsive to the evolving demands of the blockchain landscape.

Mazze's approach to decentralization is a comprehensive and forward-thinking strategy that encapsulates the essence of blockchain technology. By balancing decentralization with performance, introducing innovative token distribution methods, and leveraging advanced technologies, Mazze is set to establish a new paradigm in blockchain network design, where decentralization is not just a feature but a foundational principle driving its growth and success.

10.2. Bug Bounty Programs and Security Audits

The importance of Bug Bounty Programs and Security Audits in blockchain projects cannot be overstated, as they are essential in identifying and mitigating vulnerabilities in a technology that heavily relies on security and trust. For Mazze, a pioneering blockchain platform, these aspects are paramount. The project plans to implement a comprehensive Bug Bounty Program, actively engaging the community and cybersecurity experts to identify and report potential security flaws. This initiative not only harnesses the collective intelligence and vigilance of the community but also instills a sense of shared responsibility for the platform's security.

Complementing this, Mazze will conduct regular, exhaustive security audits by esteemed external firms, an initiative crucial for maintaining the highest standards of security integrity. These audits will scrutinize every facet of the blockchain's architecture, from its consensus mechanisms and smart contract protocols to its data encryption methods, ensuring that any potential security breach is identified and rectified promptly.

In Q4 2024, Mazze is set to organize a landmark event, the "MAZZE Hackathlon." This event will not be just a mere competition; it will be an incubator of innovation and a testament to Mazze's commitment to security. The Hackathlon will invite developers, coders, and cybersecurity experts from around the globe to stress-test Mazze's blockchain infrastructure. Participants will be encouraged to uncover vulnerabilities, propose optimizations, and develop innovative security solutions. The event will feature various categories of challenges, ranging from smart contract security to network resilience, and will offer substantial rewards for significant contributions and breakthroughs.

The MAZZE Hackathlon is envisioned as more than a competition; it is a festival of blockchain technology where knowledge sharing, workshops, and keynote speeches by leading figures in blockchain and cybersecurity will take place. It aims to foster a community around security research, encourage the exchange of ideas and techniques, and solidify Mazze’s position as a secure and innovative blockchain platform.

Moreover, the findings and advancements from the Hackathlon will be integrated into Mazze’s continuous development cycle, ensuring that the platform not only stays ahead of potential security threats but also evolves with the cutting-edge of blockchain security technology. This event will also serve as a platform for Mazze to showcase its robustness and commitment to transparency and security to its users and stakeholders.

Through these initiatives – the Bug Bounty Program, regular security audits, and the MAZZE Hackathlon – Mazze is setting a new standard in the blockchain industry's efforts to secure and safeguard its platforms. This holistic approach to security, encompassing community engagement, expert collaboration, and real-world testing, underscores Mazze's dedication to creating a resilient and trustworthy blockchain ecosystem.

10.3. Upgrade and Fork Management

In managing upgrades and forks, Mazze's blockchain ecosystem adopts a meticulous and structured approach that prioritizes community consensus and transparent decision-making. This is crucial in a blockchain environment where network changes, including both hard and soft forks, profoundly affect integrity, trust, and functionality. The process involves a comprehensive governance system, ensuring thorough evaluation and agreement on major network changes from diverse stakeholders like developers, miners, and users. This strategy, rooted in advanced technology and strong community involvement, aims to maintain network stability and adaptability, aligning with Mazze's vision of a user-centric, decentralized blockchain.

The fork management policy is designed to prioritize network stability and continuity. In the dynamic and often unpredictable landscape of blockchain technology, forks - whether planned or unplanned - can present both opportunities and challenges. Our approach is to mitigate risks associated with forks, such as chain splits or community division, by fostering a culture of open dialogue, thorough impact analysis, and consensus-building. For instance, in the event of a hard fork, our framework includes comprehensive guidelines to ensure a smooth transition, minimizing disruption to network operations and maintaining user confidence.

In addition to the governance aspect, our approach to upgrade and fork management is heavily reliant on cutting-edge technological solutions. This includes the deployment of advanced monitoring and alert systems to track network performance and detect anomalies indicative of potential forks.

Furthermore, we leverage automated testing environments to rigorously evaluate the effects of proposed upgrades or forks, thereby ensuring compatibility and performance optimization across various network scenarios.

The underlying principle of our upgrade and fork management strategy is to align with Mazze's overarching vision of a decentralized, efficient, and user-centric blockchain. By embedding these values into our governance and technological frameworks, we aim to facilitate a resilient and adaptable network, capable of evolving in response to both internal developments and external market forces. This proactive and inclusive approach not only reinforces network stability but also engenders a strong sense of community and shared purpose among all participants in the Mazze ecosystem.

The Mazze blockchain's approach to upgrade and fork management is a balanced amalgamation of community-driven governance, technological innovation, and adherence to the fundamental principles of decentralization and transparency. This strategy not only safeguards the network's stability and performance but also ensures that it remains at the forefront of blockchain evolution, responsive to the needs and aspirations of its diverse user base.

11. Marketing and Community Outreach

11.1. Marketing and Outreach

Strategic marketing and outreach are pivotal for the successful launch and adoption of innovative platforms like Mazze. As Mazze transitions from its foundational phases to more public and expansive stages, our marketing endeavors will intensify in collaboration with a specialized firm. This partnership aims to strategically spotlight Mazze's unique attributes, such as its sustainable Proof of Work (PoW) model and scalability solutions. Emphasis on marketing will notably increase during Phase B and Phase C of our development roadmap.

Our multi-faceted marketing approach will incorporate comprehensive digital marketing campaigns, leveraging SEO, social media, and content marketing to reach a broad audience. The emphasis will be on elucidating Mazze's groundbreaking features to both potential users and developers, thereby fostering a robust user base and developer community. Moreover, active participation in blockchain events and conferences will play a crucial role in our outreach strategy, providing us with platforms to engage with industry leaders, influencers, and potential collaborators. This direct engagement will be instrumental in building a strong brand presence and establishing Mazze as a leader in the blockchain space.

Simultaneously, partnerships with key industry players and influencers will be pursued to enhance our visibility and credibility. These collaborations will not only amplify our marketing messages but also provide valuable networking opportunities, facilitating Mazze's integration into broader blockchain and fintech ecosystems. This phase of intensified marketing and outreach is designed to propel Mazze to the forefront of blockchain innovation, securing its position as a trailblazer in the industry.

11.2. Partnerships and Collaborations

Acknowledging the essential role of partnerships and collaborations is paramount in the dynamic world of blockchain ventures. These alliances act as crucial conduits, bringing in new insights, resources, and expertise.

For Mazze, strategic alliances with other blockchain entities and key industry players are not just beneficial but essential. These collaborations are meticulously designed to enhance technological capabilities, propel adoption rates, and pioneer new use cases. A primary objective is to forge as many meaningful partnerships in the blockchain realm as possible. While Mazze is actively engaged in various discussions to forge these alliances, the details of such partnerships are strategically withheld until they materialize. This approach is adopted to mitigate speculative noise and focus on the substantive progress of the collaborations. Imagining further, Mazze's partnerships could involve joint ventures in developing cutting-edge decentralized applications, co-creating blockchain infrastructure improvements, or integrating interoperable solutions for cross-chain functionality. These collaborations might extend beyond mere technical enhancements, encompassing initiatives like joint marketing campaigns, collaborative research and development projects, and shared educational programs to uplift the entire blockchain community. Mazze's vision of partnerships transcends typical business collaborations, aiming instead to establish a synergistic ecosystem where each entity, while maintaining its unique identity and expertise, contributes to a larger, cohesive blockchain narrative. This strategy not only enhances Mazze's technological prowess but also solidifies its position as a visionary and collaborative leader in the blockchain sector.

12. Education and Support

12.1. Documentation and Training

The Mazze platform, at the forefront of blockchain technology, prioritizes the dissemination of knowledge and skill development. It establishes an innovative framework for documentation and training, specifically targeting developers and users involved in blockchain applications. This approach is not only instrumental in enhancing the proficiency and efficiency of its user base but also serves as a cornerstone in advancing the broader blockchain community's capabilities and understanding.

A central aspect of this effort is the establishment of a Developer Hub, a dedicated virtual space where developers can access in-depth technical guides, extensive API documentation, and best practices tailored to blockchain development. The Hub is designed as a dynamic, interactive portal, featuring a mix of written materials, video tutorials, and live webinars. Advanced topics such as smart contract optimization, security best practices, and efficient resource utilization on the blockchain are thoroughly covered, with a particular emphasis on Solidity programming and Zero-Knowledge (ZK) proof implementations.

Furthermore, the Developer Hub will host a collaborative environment, encouraging peer-to-peer learning and community-driven project development. Interactive forums and real-time chat channels will facilitate knowledge sharing and problem-solving among developers. Regular hackathons and coding challenges are planned to spur innovation and practical application of blockchain technology within the Mazze ecosystem.

These initiatives are complemented by a series of hands-on workshops and training sessions, designed to cater to various proficiency levels, from beginners to advanced developers.

The comprehensive approach of Mazze in documentation and training reflects its commitment to empowering its users and fostering a robust developer community. By providing these resources, Mazze not only enhances the user and developer experience but also contributes to the advancement of blockchain technology as a whole.

12.2. Continuous Learning and Adaptation

The importance of continuous learning and adaptation in blockchain projects is paramount, particularly in an industry characterized by rapid technological advancements and shifting market dynamics. For Mazze, this philosophy is not just a guiding principle but a core operational strategy. The team is committed to an agile methodology that emphasizes perpetual learning, ensuring the platform remains at the cutting edge of blockchain technology. This approach involves constant monitoring of the blockchain landscape, identifying emerging trends and technologies that could potentially enhance the platform's functionality and user experience.

Key to this strategy is the implementation of a robust research and development (R&D) framework, dedicated to exploring new blockchain protocols, cryptographic methods, and consensus mechanisms. This ensures that Mazze not only adapts to the current technological environment but also anticipates future developments, positioning itself as a leader in innovation. The team's expertise in various blockchain domains, including smart contracts, decentralized finance (DeFi), and tokenomics, is continuously expanded through targeted training programs, workshops, and collaborations with industry leaders and academic institutions.

The agile framework extends to the development process itself, where feedback loops and iterative design play a critical role. User feedback, market analysis, and internal evaluations are integral to this process, enabling the Mazze team to rapidly prototype, test, and deploy new features and improvements. This agility allows Mazze to respond effectively to both opportunities and challenges within the blockchain space, ensuring its offerings remain relevant and competitive.

The Mazze platform's architecture is designed with modularity and scalability in mind, allowing seamless integration of new technologies and features without disrupting existing services. This flexibility is critical in a landscape where technological obsolescence is a constant threat. By fostering a culture of innovation and continuous improvement, Mazze not only enhances its technological prowess but also strengthens its market position.

Continuous learning and adaptation are not just strategies for Mazze; they are the lifeblood of the project. By embracing change and seeking innovation, Mazze is poised to not only navigate the complexities of the blockchain world but also shape its future, delivering a platform that is both technologically advanced and attuned to the needs of its users. The Mazze team will commit to continuous learning and adaptation to stay abreast of market trends and technological advancements. This agile approach will allow the project to evolve and remain competitive in the dynamic blockchain landscape.

13. Development and Future Roadmap

13.1. Roadmap

Phase A: Ideation and Conceptualization (Early 2023)

- Concept Development: Formulate the initial idea of Mazze blockchain, focusing on creating a PoW blockchain with minimal environmental impact and high transaction throughput. Define the vision and long-term goals.
- Whitepaper Drafting: Write a comprehensive whitepaper detailing the Mazze blockchain concept, technology, tokenomics, and long-term vision. This document serves as a foundational piece for potential investors, partners, and early adopters.
- Technical Documentation: Begin creating detailed technical documentation, outlining the proposed architecture, consensus mechanism, and the role of DAG in enhancing scalability and efficiency.
- Branding and Initial Marketing:
- Brand Identity: Develop a strong brand identity for Mazze blockchain, including logo design, messaging, and overall visual theme.
- Marketing Plan: Outline an initial marketing plan to increase visibility and attract early adopters. This might include digital marketing campaigns, participation in blockchain events, and content marketing strategies.

- Build an online presence through a project website, social media channels, and participation in blockchain forums and communities.
- Initial Community Outreach: Start building a community around the Mazze blockchain. Engage with potential users and developers through blockchain forums, social media, and crypto-focused events.

Phase B: Community Building and Initial Token Launch (Q1 2024)

- Wrapped MAZZE Token Creation: Develop MAZZE as a wrapped token on a popular blockchain (e.g., Ethereum) to facilitate early fundraising and market presence. This will involve smart contract development for token wrapping and deploying these contracts on the chosen blockchain.
- Community Engagement Initiatives: Launch community-building efforts through social media, forums, and crypto communities. This includes AMAs and contests (Zealy).
- Public sale: Conduct a strategic, controlled release of wrapped MAZZE tokens in a public sale, designed to maximize liquidity and establish a robust market presence.
- Devnet Launch: Establish a development network (devnet) for internal testing of Mazze blockchain. This network will be instrumental in testing the PoW consensus mechanism, transaction processing, and overall network stability.
- Recruitment of Node Operators: Begin recruitment and vetting of node operators worldwide to ensure a decentralized and robust network.

- Smart Contract Development: Initiate development of smart contracts in Solidity for later deployment on the mainnet. This includes building a robust smart contract framework that can support various DApps.

Phase C: Mainnet Launch and Token Migration (Q4 2024)

- Mainnet Launch: Officially launch the Mazze blockchain's mainnet. This will involve extensive testing and security audits prior to the launch to ensure network integrity and security.
- Bridge Development for Token Swap: Develop a bridge for swapping wrapped MAZZE tokens with native MAZZE coins. This bridge will facilitate the secure transfer of assets between the original blockchain and Mazze blockchain.
- Token Swap Event: Conduct a token swap event where investors and token holders can exchange their wrapped MAZZE tokens for native MAZZE coins.
- Smart Contract Integration: Deploy smart contracts on the mainnet, allowing developers to create and launch DApps on Mazze blockchain.
- Developer Toolkit Release: Provide comprehensive documentation, SDKs, and APIs to encourage developers to build on Mazze blockchain.
- Ecosystem Partnerships: Establish partnerships with fintech firms, healthcare providers, and educational institutions for DApp development.

Phase D: Ongoing Development and Scalability Enhancements (Q2 2025 onwards)

- Decentralized Finance (DeFi) Integration: Focus on integrating DeFi capabilities, enabling services like decentralized exchanges (DEXs), lending platforms, and yield farming on Mazze blockchain.
- Advanced Privacy Features: Implement advanced privacy features, such as Zero-Knowledge Proofs, to enhance transactional privacy.
- Cross-Chain functionality: Develop and implement cross-chain interoperability features, allowing seamless asset transfers and communication between the Mazze blockchain and other blockchain networks.
- Continuous Network Optimization: Regular updates and optimizations to the network based on performance analytics and community feedback.
- Global Compliance and Localization: Adapt the platform to meet international regulations and standards, with multilingual support for global accessibility.
- Sustainability Initiatives: Focus on incorporating sustainable practices in mining and overall network operations, aligning with the environmental goals of Mazze blockchain.

13.2. Monitoring and Analytics

A key step in Mazze's development plan is adding monitoring and analytics features. These are still being refined and are expected to enhance the network's efficiency when they're ready.This initiative involves the implementation of state-of-the-art monitoring tools, engineered for real-time surveillance of pivotal network performance indicators including transaction throughput, block generation times, and overall network health. These tools are not mere passive observers; rather, they serve as a nerve center for the network, continuously harvesting data which then feeds into an advanced analytics engine. This engine employs cutting-edge data analysis techniques, leveraging both traditional statistical methods and modern AI-driven insights, to distill vast amounts of raw data into actionable intelligence.

The primary objective of these analytics is to inform and guide a continuous iterative process of network optimization and adaptation. By closely examining patterns and trends in network performance, the Mazze team can make data-driven decisions to fine-tune network parameters, enhance protocol efficiency, and preemptively identify and address potential bottlenecks or vulnerabilities. This dynamic and proactive approach to network management is expected to be a cornerstone in the quest for achieving and maintaining high scalability, robust security, and optimal performance in the face of an ever-evolving digital landscape. The anticipated result is a blockchain network that not only meets the current demands of its users but is also well-prepared to adapt and thrive amid future technological shifts and challenges.

13.3. Token Liquidity Strategy

The Mazze liquidity strategy is meticulously designed to ensure robust market presence and accessibility for its native token, MAZZE. Initially, the focus will be on launching a wrapped version of the MAZZE token on a widely-recognized and established blockchain platform. This strategic move enables us to leverage the existing infrastructure and user base of the platform, thus facilitating immediate liquidity and market penetration.

Following the creation of the wrapped MAZZE token, we will initiate a token sale aimed at generating essential funding for ongoing development and operational needs of the Mazze. This sale is not only a financial endeavor but also a vital step in community building and fostering early adopters' engagement.

Concurrently, we plan to list the wrapped MAZZE token on prominent decentralized exchanges (DEXs), such as Uniswap. This listing will provide traders with easy access to the token, ensuring liquidity and enabling price discovery in a decentralized environment. Furthermore, the integration with DEXs plays a crucial role in upholding the decentralized ethos of the blockchain community.

In parallel, we will pursue listings on several leading centralized exchanges (CEXs). These listings will expand our reach to a broader investor base, providing additional liquidity and trading options. Centralized exchanges will also offer more exposure to the mainstream market, which is essential for wider adoption.

Post-mainnet launch, we will collaborate closely with these exchanges to facilitate a seamless token swap campaign. This campaign will allow holders of the wrapped MAZZE tokens to exchange them for the native MAZZE coins. The exchanges will play a pivotal role in this process, ensuring a smooth and secure transition for token holders.

This multi-faceted liquidity strategy is crafted to ensure that the Mazze maintains a strong and stable market presence throughout its development phases, ultimately enhancing the overall value and utility of the MAZZE token within the blockchain ecosystem.

13.4. Use Case

Understanding and developing effective use cases are critical in blockchain projects, as they provide a tangible framework for how the technology can solve real-world problems. Mazze, a versatile blockchain platform, illustrates this principle by introducing a range of innovative use cases that transcend traditional boundaries.

In the financial sector, Mazze could revolutionize cross-border transactions, offering a secure and transparent system that drastically reduces processing times and fees. Imagine a scenario where small businesses effortlessly engage in international trade, unhindered by the complexities and costs of current banking systems. Similarly, in the healthcare industry, Mazze's robust encryption and privacy features could transform patient data management. Hospitals and clinics could securely store and share sensitive medical records, ensuring patient confidentiality while enhancing accessibility and efficiency.

Education is another domain ripe for disruption. Mazze could enable the creation of immutable and verifiable academic credentials, combating the prevalent issue of qualification fraud. Universities could issue blockchain-based certificates, ensuring authenticity and ease of verification for employers. Additionally, in the realm of supply chain management, Mazze's transparent and unalterable ledger could be employed to track the journey of products from manufacturing to delivery, significantly enhancing trust and accountability in the process.

One of the most promising applications lies in the development of decentralized voting systems. Mazze could facilitate secure, transparent, and tamper-proof digital voting platforms, thereby fostering more democratic and reliable electoral processes. This would not only increase voter participation but also restore trust in the electoral systems.

In each of these scenarios, the underlying strength of Mazze - its high transaction throughput, robust security mechanisms, and user-friendly interface - comes to the fore. The platform's flexibility allows for the tailoring of blockchain solutions to specific industry needs, showcasing the vast potential of this technology. Mazze's innovative approach in leveraging blockchain technology demonstrates its capacity to not only revolutionize various sectors but also to pave the way for new, unexplored applications.

14. Outlook

The Mazze blockchain project distinguishes itself in the sector through its unique combination of Proof of Work (PoW) and Directed Acyclic Graph (DAG) technologies, ensuring exceptional scalability and transaction speeds. Utilizing Solidity for advanced smart contract functionalities, it supports a wide array of decentralized applications (dApps) across various domains, with a notable emphasis on Ethereum Virtual Machine (EVM) compatibility. This compatibility ensures seamless integration with the established Ethereum ecosystem, broadening the scope for interoperability with existing dApps and smart contracts. Key achievements include exceeding initial performance goals, fostering a dynamic community, and innovating in concurrent block processing. These accomplishments reflect a deep commitment to developing a top-tier blockchain solution. Future plans include enhancing decentralized finance (DeFi) features, increasing interoperability, particularly with EVM-compatible chains, and integrating advanced privacy measures like Zero-Knowledge Proofs. Prioritizing ongoing network performance and user experience improvements, this platform addresses critical scalability and security issues in the blockchain ecosystem, setting new standards in blockchain efficiency and promoting wider adoption across industries. Recognizing challenges like network security and regulatory compliance, the strategy focuses on continual innovation, community engagement, and adherence to international norms. Stakeholder and community involvement is crucial for further development and success in transforming the blockchain landscape. This platform represents a driving force in the digital realm, with a steadfast focus on innovation, security, and scalability, shaping the future of blockchain technology.