Mετchain

White Paper

The next evolution in metaverse ecosystems: Creating a decentralized portal for Web3 applications and Smart Contracts.

Table of Content

Introduction

Metchain is an innovative platform that seeks to revolutionize the creation and facilitation of metaverse ecosystems. It bridges the gap between the realms of decentralized application (DApp) development and the immersive worlds of gaming and Web3, bringing to life the boundless imagination of developers and users alike.

Metchain's foundation is built upon three pillars: fostering community inspiration, establishing a global network, and providing a blue-chip investment opportunity.

At its core, Metchain operates on a sophisticated three-layered blockchain architecture designed to achieve unparalleled security, scalability, and interoperability.

- The first layer employs the Kheavyhash algorithm's proof-of-work (PoW) consensus mechanism, ensuring robust blockchain functionality and security.
- The second layer introduces a unique proof-of-stake (PoS) mechanism based on non-fungible tokens (NFTs), enabling scalability, network speed, and redundancy.
- The third layer is a groundbreaking development suite that empowers interoperable DApp creation and production.

This innovative platform seamlessly merges the boundless creativity of developers with the aspirations of users, breathing life into the metaverse and unleashing its full potential. Through this comprehensive architecture, Metchain establishes itself as a trailblazer in the realm of decentralized ecosystems, fostering a symbiotic relationship between cutting-edge technology and the limitless possibilities of the metaverse.

Abstract

In 2008, Satoshi Nakamoto created the foundation for distributed ledgers based on blockchains.

This system is an open, anonymous network of nodes or miners that work together to maintain a public ledger of transactions. The ledger is a chain of blocks called a blockchain, and each block contains a collection of new transactions from users.

However, the blockchain created by Satoshi has a significant scalability issue. For Satoshi's longest chain rule, also known as the Bitcoin protocol, to work securely, all trusted nodes must be aware of each other's blocks relatively soon after they are created. To achieve this, the system's throughput is artificially suppressed so that each block propagates completely before the creation of the next.

To distinguish between blocks mined correctly by honest nodes and those produced by non-cooperating nodes who deviated from the mining protocol, PHANTOM solves an

optimization problem over the blockDAG. By making this distinction, PHANTOM provides a solid total order on the blockDAG that is ultimately accepted by all trusted nodes.

To avoid the excessive computation required to implement PHANTOM, we created the effective greedy algorithm GHOSTDAG, which perfectly captures the design of PHANTOM. We offer a formal proof of GHOSTDAG's security, showing that its block ordering is irreversible up to an exponentially insignificant factor with interoperability.

We discuss GHOSTDAG's characteristics and how it compares to other DAG-based protocols. We evaluate GHOSTDAG's performance under real-world conditions and analyze confirmation times obtained from observing the main network.

Problem Statement

The intricate landscapes of the metaverse, Web3, and gaming industries have unveiled significant obstacles in the integration of blockchain technology.

Challenges such as scalability limitations, rising transaction costs, user adoption complexities, and pervasive security vulnerabilities impede the natural evolution of these dynamic sectors.

- Metchain keenly recognizes these hurdles as formidable barriers to widespread blockchain adoption, underscoring the urgent need for a holistic solution to surmount these challenges. The overarching goal is to unlock the untapped potential of decentralized systems, fostering innovation and efficiency within these pivotal industries.

The blockchain industry was founded on proof-of-work (PoW) mechanisms, which enabled the decentralizing ethos of the cryptocurrency sector to take hold. However, it must be acknowledged that despite the PoW sector's energy consumption being comparable to other technology industries, the sector is inherently reliant on energy-intensive technologies, resulting in a substantial environmental cost. Consequently, striking a balance between technological progress and reduced environmental impact has become an imperative endeavor.

While the proof-of-stake (PoS) market segment offers solutions to existing problems, it introduces its own set of complications. Notably, PoS systems may favor large investors, fostering economic centralization and control. Moreover, the prevalent either-or approach to consensus mechanisms in cryptocurrencies results in shortcomings, limiting blockchains in terms of centralization, scalability, and equitable wealth distribution throughout ecosystems.

Finding a balanced solution that addresses these intricacies and advances the blockchain industry sustainability has become a paramount objective.

Solution

Metchain's design takes into account the above issues in the industry by proposing a combination of Proof-of-work (PoW) and Proof-of-stake (PoS) consensus methods. Combining these two methods allows the ecosystem to overcome the downsides of each system while taking advantage of their upsides.

Metchain's commitment to decentralization aligns well with the GPU-based PoW mining community. Recognizing the value of the PoW GPU miner community while also acknowledging the global shift towards sustainability and environmental impact, Metchain adopts and modifies the use of the Kheavyhash algorithm, highlighting its efficiency while still ensuring a strong security framework through PoW.

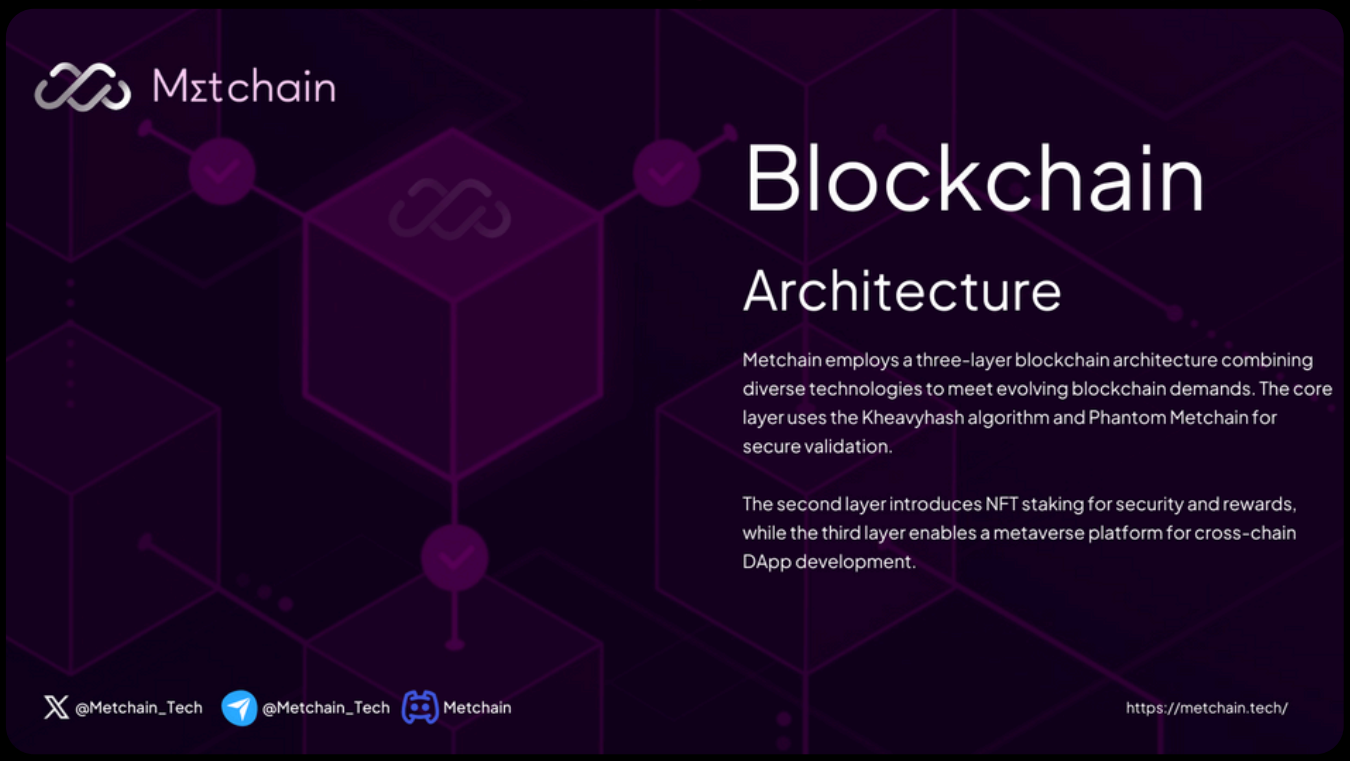
Metchain also recognizes the diverse capacities of investors and aims to provide an inclusive ecosystem that benefits all types of investors, big and small. The scaling solution within Metchain's Layer 2 NFT-based PoS consensus creates a unique combination of important groups and technologies to further these goals.

The tokenomic design takes into account the nuances presented by both consensus methods, such as high global energy prices and typical barriers to entry. Creating a balanced and sustainable tokenomic ecosystem also benefits the main purpose of MET coins, which is for them to be used within Metchain's Layer 3 open-source metaverse platform.

The overall goal is to streamline the integration of blockchain features within the metaverse, Web3, and gaming industries, overcoming existing obstacles. This focus on community engagement, technology, high efficiency, and sustainable tokenomics creates an appealing ecosystem for all parties involved, including end-users, developers, miners, and stakeholders.

Metchain's commitment to tackling these challenges positions it as a serious contender poised to advance the Metaverse industry.

Blockchain Architecture



Metchain uses a three-layer blockchain architecture that brings together different technologies to meet the evolving needs of blockchain.

The core layer uses the Kheavyhash algorithm and the Phantom Metchain block validation system to provide a highly efficient and secure foundation.
The second layer has Metchain's scaling mechanisms. This layer introduces staking of Non-Fungible Tokens (NFTs), where the 500 genesis NFTs act as validator nodes for the blockchain when they are staked. This offers a unique way for people to contribute to the network's security and earn financial rewards.

The third layer will host the creation of the metaverse platform. This is a virtual world created by inspired developers, enabled by connections across different blockchain ecosystems for building decentralized apps (DApps).

Metchain Algorithm

Metchain introduces PHANTOM Metchain, a new blockchain protocol designed to tackle scalability issues found in Satoshi Nakamoto's original Bitcoin protocol. Traditional blockchains rely on the longest-chain rule, but PHANTOM Metchain uses an innovative Directed Acyclic Graph (DAG) structure, allowing blocks to reference multiple predecessors. This architecture, explained in the GHOSTDAG algorithm, provides a total ordering over blocks and transactions, enhancing security and addressing scalability problems.

PHANTOM Metchain also features a unique split hashrate algorithm, categorizing blocks into Mini Metblocks, Mega Metblocks, and MET Metblocks, each with different time intervals. This hierarchical structure optimizes block propagation and strengthens the protocol against 51% attacks.

Metchain enhances traditional Proof-of-Work (PoW) by adding a Proof-of-Stake (PoS) layer for extra security and efficiency.
The Layer 2 blockchain includes an NFT staking system where validators are chosen based on staked MET coins, promoting decentralization. This dual-layer consensus approach reduces transaction times to sub-seconds and maintains low transaction fees of 0.025%

The Metchain V3 Wallet offers advanced security features like timestamp-based address generation and a multi-step private key process, providing additional protection. An Anti-ASIC Mining sub-algorithm dynamically adjusts hashing algorithms to prevent ASIC mining, ensuring a fair environment for GPU miners.

In summary, Metchain presents a comprehensive blockchain solution with PHANTOM Metchain, integrating DAG, PoS, and innovative security measures to redefine scalability, security, and sustainability in the blockchain ecosystem.

PHANTOM Metchain

For the Bitcoin system to be secure, blocks must spread quickly to all network miners. The requirement that each block carry a proof-of-work slows down block generation itself. For the Bitcoin protocol to be secure, block propagation must be faster than the average time it takes the network as a whole to construct the next block. To ensure this property, the Bitcoin protocol limits block creation to once every 10 minutes. Additionally, the block size is constrained to allow for quick transmission.

In this paper, we present PHANTOM METCHAIN, a protocol that generalizes Nakamoto's longest-chain protocol. Unlike Bitcoin, where blocks reference a single predecessor in the chain, forming a tree, PHANTOM blocks reference multiple predecessors, thus forming a Directed Acyclic Graph (DAG), called a blockDAG. Each block can include several hash references to predecessors.

PHANTOM then provides a total ordering over all blocks and transactions and outputs a consistent set of accepted transactions. Unlike the Bitcoin protocol, where blocks that are not on the main chain are discarded, PHANTOM incorporates all blocks in the blockDAG into the ledger. However, keeping in mind the 51% attack, PHANTOM METCHAIN has an added split hash rate algorithm.

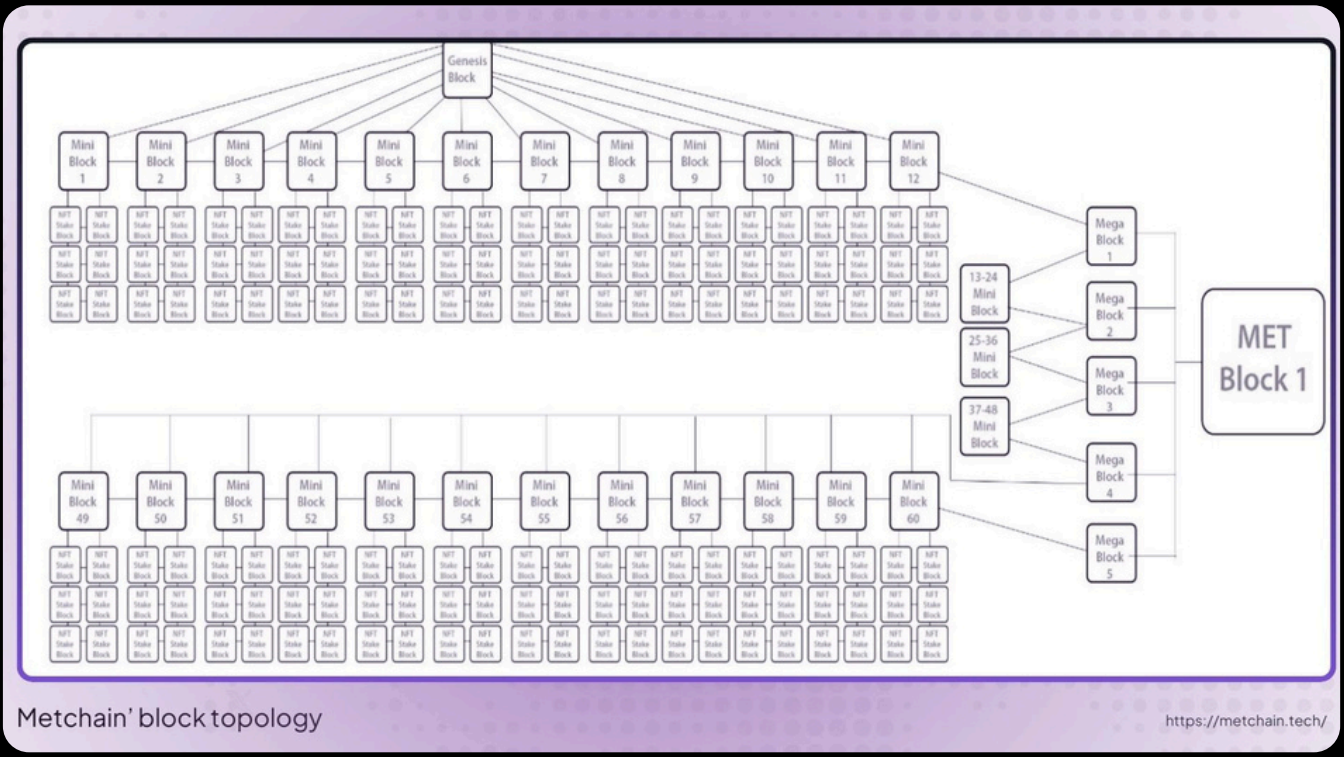
In rough terms, PHANTOM METCHAIN consists of a four-step procedure. This method, the core of the protocol, is used to exclude blocks made by misbehaving nodes and recognizes a set of well-connected blocks using the blockDAG's structure (later referred to as blue blocks). Blocks that are either withheld by their creator for a while or reference only older blocks from the DAG will almost certainly not be included in the set of blue blocks.

Our method encourages blocks inside the chosen cluster and penalizes those outside it to convert the DAG's naturally occurring partial order into a full topological order (i.e., an order that respects the topology). Transactions within a block are arranged according to the order in which they appear in the block as a result of the order over blocks. We go over each transaction in this order iteratively and approve any that are compatible (in terms of the underlying consistency concept) with the previous transactions.

Hash rate split algorithm which splits the hash rate into 3 block types:

1. Mini MetBlock (Interval of 10 Seconds) 6 blocks per minute.
2. Mega Metblock (Interval of 2 Minutes)
3. MET Metblock (Interval of 10 Minutes)

Mini Metblocks generated are reconfirmed after every 2 minutes to form a Mega Metblock, which helps METCHAIN to attain more security over other Proof-Of-Work chains and helps to avoid 51% attacks. As the mining hash rate will be automatically split as per the block time to avoid any false blockchain from being created. The same is followed by the MET Metblock.



Metchain' block topology

https://metchain.tech/

PHANTOM protocol

The PHANTOM assumes that a malicious mining coalition does not hold the majority of the mining power, meaning an attacker has less than 50% of the total mining power. This sets the system's maximum security threshold at 50%, similar to protocols like GHOST and SPECTRE. However, PHANTOM differs from SPECTRE by enforcing strict ordering of blocks and transactions.

This makes PHANTOM suitable for smart contract systems, but it requires a proper ordering of blocks, which impacts the time it takes for nodes to reach consensus. Although PHANTOM is scalable, its consensus time is slower compared to a protocol like SPECTRE that doesn't enforce such strict guarantees.

PHANTOM uses a mining protocol similar to Bitcoin's Proof of Work, where computational puzzles involve finding hashes below a target difficulty. During the mining process, a node examines its view of the blockDAG network and performs the following steps:

Identifies all blocks with 0 in-degree, denoted as B, and computes hashes until it finds a hash $h < D$.
Creates a block b with the hash h, includes B in the block header (creating directed edges to those blocks), and broadcasts b.

PHANTOM uses topological methods to reach consensus, differing from SPECTRE's voting system. The protocol selects a "correct blockchain" within the blockDAG by assembling the total number of legitimate blocks.

This recursive process forces the overall ordering of the transactions contained within the chain. PHANTOM adds these blocks using a greedy approximation algorithm to solve an optimization problem.

Finding the maximum m-cluster subDAG, as shown in the Metchain Block Topology figure, is the first step in the process of identifying the finest, honest blocks. The official issue is described below. Due to the fact that it involves several trade-offs and the fact that the actual network delay is unknown, the task of choosing the best parameter m also poses an interesting problem.

To begin with, the parameter has a direct relationship with the expected propagation delay of the entire network. The fact that this delay is bounded but not explicitly known is due to the partially synchronous model that we work under.

In PHANTOM, a miner refers to all blocks in tips(G), where G is the DAG that the miner observes locally at the time the new block is created, rather than extending a single chain. The miner should publish its new block as soon as it is ready. Together, these two guidelines make up PHANTOM's DAG mining protocol.

The aforementioned DAG mining algorithm specifically indicates that both blocks are added to the blockDAG and used as references by all (honest) miners even if two blocks contain conflicting transactions. The main issue is therefore how to restore the blockDAG's consistency. In our system, this is accomplished by making sure all 12 mini-blocks which are set 10 seconds apart after reaching the mature difficulty point. Each mini-block supports a layer 2 blockchain which creates a staking block every 1.67 seconds, reducing the transaction time and also increasing the security.

These staking blocks point to a Mini Block consisting of a block reward of 0.3 MET, and these then point to the subsequent Mega Block which is created every 2 minutes with a block reward of 3 MET and also points to the same previous hash.

This is then further verified while creating a MET block. All the previously created Mega and Mini blocks in 10 minutes should point to the previous MET Block and the subsequent MEGA block as well, approving those who came before them. By achieving consensus on the sequence of blocks, PHANTOM ensures that there is also agreement on the set of allowed transactions.

In essence, Bitcoin may be viewed as an ordering protocol as well, with the longest chain of blocks' worth of transactions coming before those with the shortest chain. However, the protocol underlying Bitcoin is only known to be secure under low block rates.

Unfortunately, the security analysis of existing blockchains is not as general as ours (e.g., their attacker does not take advantage of providing consulting information to different honest parties), while the analysis of METCHAIN does not carry to the setting of GHOST. This is because the GHOST rule is a natural, albeit radical, reformulation of how each miner determines the main chain. In GHOST, miners adopt blocks in the structure of a tree.

Note that in both Bitcoin and GHOST, one can consider parties collecting all mined blocks in a tree data structure. However, while in Bitcoin the miners would choose the most difficult chain as the main chain, in GHOST, they will determine the chain by greedily following the heaviest observed subtree. This means that for the same subtree, a Bitcoin miner and a GHOST miner may choose a completely different main chain.

Furthermore, it means that the difficulty of the main chain of honest parties does not necessarily increase monotonically (it may decrease at times) and thus a fundamental argument (namely that blockchain monotonically increases) that made the analysis possible, does not hold anymore.

Transactions

MET is the native coin of Metchain, rewarding stakeholders and miners for their contributions. It is a tradable asset within the ecosystem, cross-chain, and exchangeable with other crypto assets on both Metchain and third-party exchanges. Upon the launch of Layer 3's metaverse, MET will also facilitate payments for in DApp goods and services. Transaction fees are set at 0.025% of the transaction volume.

Scalability

To tackle blockchain scalability, Metchain uses a layer 2 POS consensus mechanism with the Genesis NFT collection as validator nodes. While layer 1's POW efficiently processes transactions, POS enhances scalability by reducing the workload from general transactions and micro-transactions in the metaverse. One Metcoin can be divided into over a billion units, ensuring adaptability and scalability regardless of TVL and MET's future valuation.

In layer 3, the metaverse's scalability is achieved by allowing developers from other blockchains to integrate their assets into the Metchain ecosystem. This feature ensures that developers can use their existing tools and expertise across different chains, creating a diverse and scalable ecosystem.

Accessibility

Metchain prioritizes user experience, recognizing the varying levels of blockchain knowledge among users. The platform features intuitive interfaces, comprehensive guides, and tutorials to make blockchain features accessible. Metchain's Layer 3 network enhances accessibility by allowing seamless migration of DApp development tools across chains, fostering a user-friendly environment for widespread participation.

Metchain plans to increase access to the MET coin by establishing a strong presence on global centralized exchanges early on and offering a wide range of trading pairs. Additionally, the development of a Layer 3 decentralized exchange will further enhance ecosystem accessibility, enabling direct asset exchange within the metaverse.

Security is fundamental to Metchain's design. The platform conducts third-party audits of all blockchain components, including smart contracts, to ensure ecosystem integrity.

Metchain Security

Security is at the core of Metchain's design philosophy. The platform maintains high standards by conducting thorough third-party audits on all aspects of its blockchain, including smart contracts and blockchain implementations. This ensures the highest integrity of the entire ecosystem.

Metchain leverages the inherent security features of Proof of Work (PoW) to enhance the network's overall resilience. The Phantom block architecture of Metchain authenticates block validation by creating high-throughput blocks that can be referenced by multiple miners. This ensures the continuation of a true and valid chain.

To strengthen security further, the MET mining pool uses an advanced monitoring algorithm to moderate high fluctuations in hash rate. The mining pool adjusts the network difficulty on a per-block basis, minimizing the impact of these fluctuations. Additionally, the mining pool employs IP bans to prevent bad actors from hijacking the blockchain, such as in 51% attacks.

The web wallet on Metchain utilizes on-chain encryption and block validation for the creation and storage of user assets. This ensures that only validated wallets are maintained. Once validated by the chain, users' assets are securely held on-chain, encrypted, and accessible only by the associated wallet and its seed phrase.

Blockchain validators on Metchain are implemented through staked Genesis NFTs and local nodes. This creates a low-latency blockchain architecture that continuously references the highest true chain and rejects invalid side chains that could be used to attack the blockchain.

Metchain V3 Wallet

MetChain wallets are unique in many ways. Metchain wallet creation uses a bip39 mnemonic seed to generate the wallet but in such a way that it becomes difficult for the user to anticipate the seed.

Each wallet has its own stamp included in the wallet to generate a wallet address locally. Keeping the wallet secure unless the timestamp is the same wallet address won't be created nor can be recovered even with the same seed unless recovered using a private key.

Private key generation also uses multiple processes.

Each seed creates 1 wallet address which are then again combined to a single wallet address making it more secure than ever. The signature verification for the transaction also follows the same steps.

12 + 1 signature must match before the transaction is accepted by any node to be processed. Transaction signature and approval uses Elliptic Curve Digital Signature Algorithm (ECDSA) for all wallet signatures merged as one.

If the transaction gets approved by 12 and rejected by 1 it will reject the transaction as the signature must match the wallet address and its 12 wallets in a single wallet.

Metchain Anti - Asic

Metchain being unique uses an Anti-Asic Mining sub-algorithm. Which includes multiple hashing algorithms. When a certain criterion is met by the integrated mining algorithm it automatically modifies the sub-algorithm. This results in Kheavyhash Asics being unable to provide valid shares. They might be able to connect or stay connected to the blockchain, but all the shares will start being rejected. Keeping it safe for GPU miners.

If the system detects unusual traffic on the node for hashes the algorithm is modified automatically for all nodes after reaching consensus.

All nodes agree to 1 modification in the algorithm, if any node has not come to agreement and has miners connected all the blocks submitted from that node will be counted or marked as orphan blocks but transactions will still be accepted.

Proof-of-Stake (PoS)

It is a revolutionary consensus algorithm that is gaining popularity in the blockchain space. In contrast to traditional Proof-of-Work (PoW) algorithms, PoS relies on validators who are chosen to create new blocks based on the number of tokens they "stake" or lock up as collateral. As the blockchain industry evolves, new and improved versions of PoS algorithms are emerging, promising greater efficiency, scalability, and environmental sustainability.

The Drawbacks of Proof-of-Work

While PoW has been the backbone of several successful blockchain networks, it comes with some significant drawbacks. The most prominent issue is its high energy consumption. Miners must compete to solve complex mathematical puzzles, leading to enormous computational power consumption, which has raised concerns about its impact on the environment.

Additionally, PoW is susceptible to centralization, as it oEen rewards those with access to the most powerful and expensive mining equipment.

This concentration of power can compromise the decentralization and security of the network. This is resolved by adding layer 2 PoS to the blockchain. Metchain has enhanced the security by adding another layer for the consensus, which includes the NFT.

Only the NFT holders will be considered validators and allowed to stake. Layer 2 blockchain PoS above layer 1 blockchain PoW will also reduce the transaction to sub-seconds and create the fastest transactions possible with low transaction fees of 0.025%

The Advantages of New Metchain Proof-of-Stake Algorithm:

1. Energy Efficiency: One of the most significant advantages of new PoS algorithms is their energy efficiency. Since they do not rely on energy-intensive mining processes, the energy consumption is drastically reduced compared to PoW. This makes PoS a more sustainable and eco-friendly op1on for blockchain networks, aligning with global efforts to combat climate change.
2. Scalability: PoS algorithms offer improved scalability, enabling networks to process a higher number of transactions per second. With reduced energy requirements, validators can process transactions more quickly and efficiently, contributing to a smoother user experience.
3. Decentralization: New Metchain Proof-of-Stake Algorithm addresses the centralization concerns of PoW. Validators are chosen based on their stake, incentivizing token holders to participate in securing the network. This democratic approach encourages a broader distribution of power, ensuring the network's resilience and security.
4. Security: PoS algorithms enhance network security by penalizing malicious behavior. Validators are required to lock up their tokens as collateral, which they stand to lose if they act against the network's best interests. This economic incentive promotes honest behavior and discourages aWacks.

Layer 2 Staking

When the block is mined and supplied to the other miners' tree, it also verifies the block for the next few seconds which is achieved through layer 2 authentication. Metchain is one of the first blockchains which supports Layer 1 Mining and Layer 2 Staking.

A unique concept of NFT consensus providing annual yield percents (APY) returns based on rarity and the vesting period. Within the process of NFT staking, The NFT and the staked MET coin amount is locked with the transaction. The balance of MET coins is then transferred to the Metchain Coinbase for the vesting period. When the vesting is completed the NFT is unlocked and staking rewards plus agreed APY are sent to the respective user's wallet. NFT locking and unlocking can only be achieved through Byzantine Fault Tolerance System (BFT).

If the nodes do not agree on the unlocking period and staking user wallet and block hash where they staked, then the nodes will come to force BFT's to check the altered blocks. Any block alter will suspend the node for 3 days unless it's unbanned manually. A node banned through BFT's will be broadcast to all nodes, so it remains banned. This increases the security of the user staked coins and user wallets.

Layer 2 blocks have their own consensus system where the nodes communicate with each other and decide which staked NFT becomes the validator for each block till the next MET Block is generated.

(a) = Mini block
(b) = Mega Block
(c) = MET Block

When (c) block is created, all the nodes confirm and add it. At this point, each node is randomly selected to supply the selected staked NFT validators for all blocks that will be created between every (a) block. There are 6 NFT stacked blocks which are sub-seconds apart and are decided by all the nodes then only the next (a) block can be submitted or accepted. Any block generated before that will be counted as an orphan.

Any transaction in the orphan block is still counted as valid no matter what the block state is but the orphan block must be validated as orphan on all nodes. And the transaction should have been broadcast throughout the node system.

Conclusion of NFT staking

- 15 NFT Staked blocks every (a) Mini Block.
- 12 (a) Mini Block in every Mega Block.
- 5 (b) Mega Block in every MET Block.

1 Met Block consists of 900 NFT staked blocks which must be the same and verified through all the nodes. If these 900 NFT staked blocks do not match BFT's will be forced into action to prevent any attack.

Results

In contrast to METCHAIN, we propose a new analysis framework for blockchain protocols that focuses on trees of blocks. Due to this framework, it can reason about random variables on the participant-created block trees. We can describe notions like a node being d-dominant in our framework, which indicates that the block corresponding to that node would be favored over other sibling nodes by a margin of d based on a particular weight measure. In fact, by demonstrating that Bitcoin and GHOST adhere to the same rule but just for a different weight measure, it allows us to unify the description of both.

We then offer the first formal security proof of the GHOST rule for blockchain systems using our framework. In particular, it is demonstrated that GHOST is a reliable transaction ledger that meets liveness and persistence requirements. The new methodology, which is referred to as the fresh block lemma, which condenses the properties of the resilient transaction ledger into a single lemma, allows us to obtain this result.

We use the abstraction suggested in METCHAIN for our model. In Particular, synchronous communication is assumed in their environment, known as the q-bounded environment, and each party is permitted to q queries to a random oracle.

The network includes an anonymous message diffusion mechanism that ensures that each round's messages are delivered by all sincere parties. At the start of the following round, all messages are delivered. It should be noted that the diffusion mechanism is unreliable, meaning that the attacker may deliver messages to only some of the network participants.

Additionally, the enemy rushes and adapts. Rushing in this situation allows them to view every honest player's message before choosing their own course of action.

Furthermore, they have total control over the sequence in which messages are sent to each player. In terms of computational power, the model assumes that all honest parties have the same amount, whereas the adversary's computational power is inversely proportional to the number of participants it controls.

Since there are n parties altogether, it is presumed that the adversary has power over t of them (honest parties are unaware of any of these conditions). Finding a hash value smaller than a difficulty parameter D results in the discovery of a new block.

The probability that a single hashing query will result in a solution is given by the formula $p=D/2^h$, where h is the hash length. The adversary's total hashing power is equal to pqt, the honest players' total hashing power is f = pq(n-t), and the sum of all hashing power is pqn. The following list includes a number of definitions that will be used frequently.

A round is referred to as: Successful if in this round at least one honest participant computes a solution. If precisely one honest participant computes a solution in this round, it will be considered uniquely successful.
In execution, blocks are called:

- honest, if mined by an honest party.
- adversarial, if mined by the adversary.

Some chain notations: By C^dk we denote the chain that results by dropping the last k blocks of C. We will say that a chain C' extends another chain C if a non-empty prefix of C' is a suffix of C.

In METCHAIN, a lower bound to the probabilities of two events, that a round is successful or that it is uniquely successful (denoted above), was established and denoted by γu = α–α^2. While this bound is sufficient for the setting of small f, here we will need to use a better lower bound to the probability of those events, denoted by γ, and with a value approximately αe^-α

The Ghost Backbone Protocol

The term "Backbone Protocol" was first used to investigate the characteristics of the fundamental Bitcoin protocol in METCHAIN. At this level of abstraction, we are only concerned with the characteristics of the blockchain, not the information contained in the blocks themselves.

The fundamental tenet of the Bitcoin Backbone is that sincere participants receive fresh chains from the network at the beginning of each round and choose the longest valid chain to mine.

At the conclusion of the round, if they discover a new block (by finding a liWle hash), they broadcast their chain. The Ghost protocol can also be expressed at the same level of abstraction.

The Ghost Backbone protocol, as described above, is founded on the idea that blocks that do not become part of the main chain should nevertheless be taken into consideration when deciding which chain to use.

Players maintain a tree of all mined blocks they have received in order to accomplish this, and then they choose which chain to mine using the greedy heaviest observed subtree (Ghost) rule.

Every round, Miners add valid1 blocks sent by other miners to their tree, updating it. Similar to Bitcoin, a block must be a legitimate child of another tree block in order to be added to the tree.

As long as the blocks are valid, the opponent is free to add them anywhere in the tree. miners aTTempt to add one or more blocks to the chains they select, just like in Bitcoin. Finally, a tree of blocks is saved and updated during each round in the main function.

A miner then broadcasts any changes to his tree to all other miners on the network.

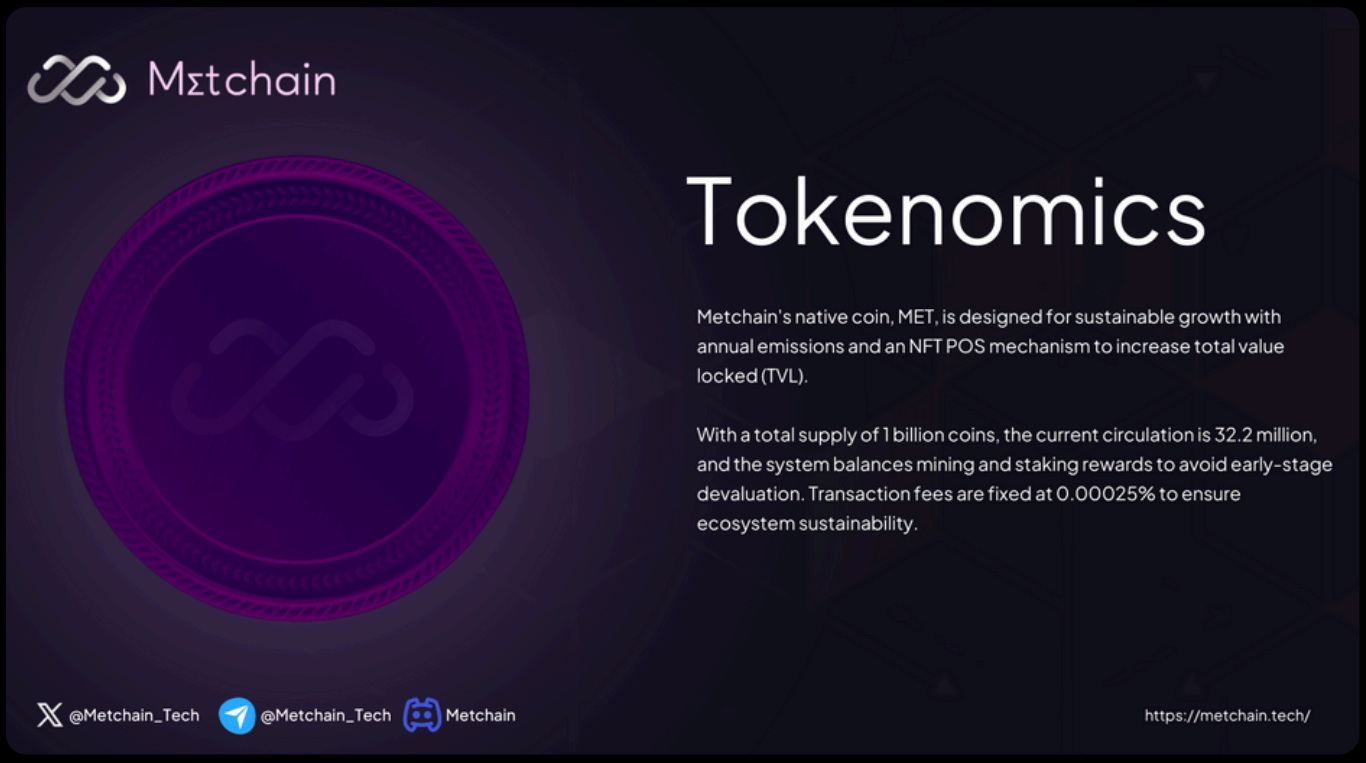
Interoperability

Metchain promotes interoperability through features like Multi-network Validator NFTs and layer 3 networks. These tools allow users to easily move between different networks and platforms within the Metchain ecosystem, providing a seamless experience.

This focus on interoperability positions Metchain as a key enabler of efficient data exchange and collaboration across various blockchain networks.

- Metchain's commitment to smooth integration supports its vision of a unified and interconnected blockchain ecosystem, fostering collaboration and data exchange with simplicity and effectiveness at its core.

Tokenomics



The main asset in Metchain's financial ecosystem is its native coin, [MET]. Designed with a focus on sustainable annual emissions, Metchain aims to avoid the early-stage devaluation common with other new coin releases. As the community grows, the value of MET is expected to appreciate rapidly, bolstered by the NFT POS mechanism, which increases the total value locked (TVL) on the Metchain network.

This approach positions MET as a key driver of the ecosystem's financial growth.

Metchain’s [MET] coin has a total supply of 1 billion coins. Currently, 32.2 million coins (3.2% of the total supply) have been mined and distributed as follows:

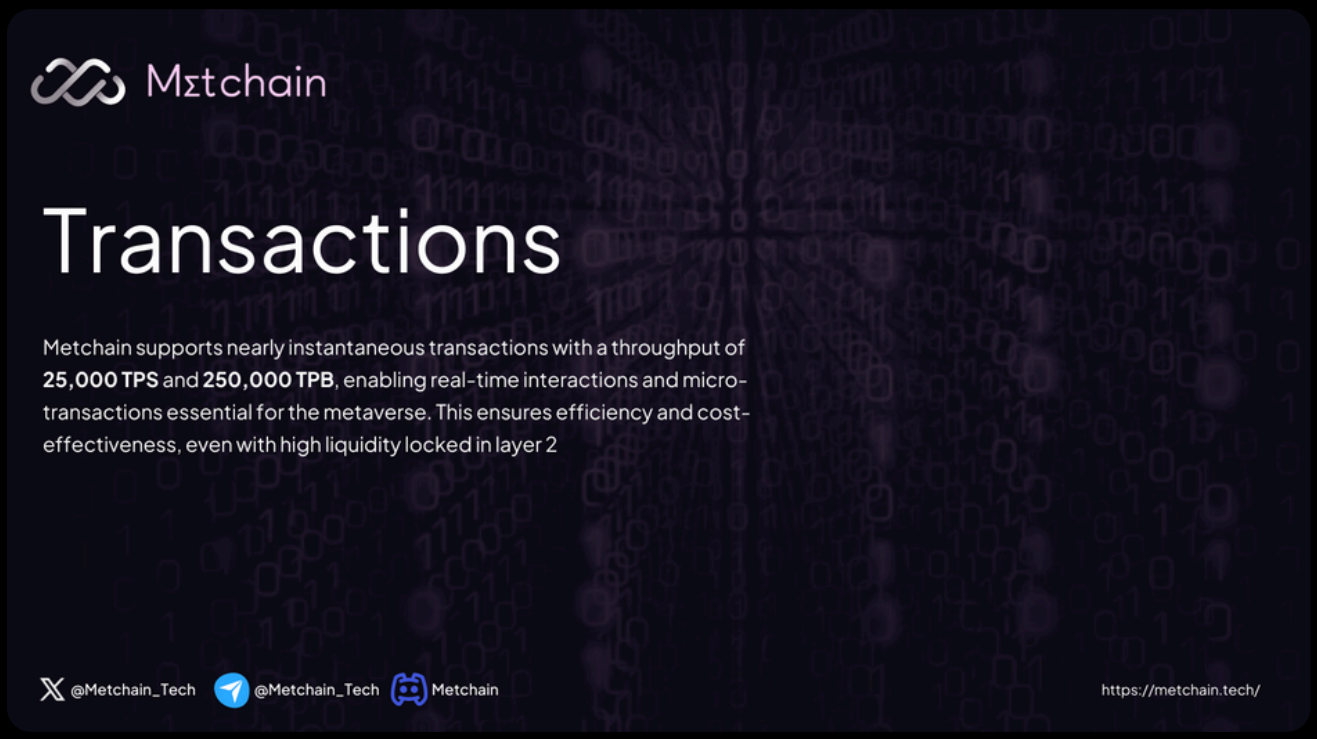
- 1.2% to user holdings
- 1% to the developer fund
- 1% to the exchange and marketing fund

Annual coin emissions include a fixed mining rewards schedule of 4 million coins. The POS mechanism maintains a sustainable variable staking emission based on the annual percentage yield (APY), which ranges from 1% to 11% depending on NFT rarity- total coins reward is based on amount of coins staked.

This dual emission system enables consistent mining and staggered staking emissions, promoting balanced incentives for both miners and stakers. The circulating supply inflation for the first year is projected to be 5.5 million coins, a 17% increase in the current circulating supply, and a 0.55% emission of the maximum supply.

Metchain's financial ecosystem features fixed transaction fees of 0.025% of the transaction volume. Mining emissions are set without a halving schedule to maintain sustainability throughout Metchain's emissions life cycle. Once the emission schedule is complete, miners will be rewarded through network transaction fees to maintain the primary consensus. This fee structure ensures a sustainable and functional ecosystem, accommodating a wide range of transaction sizes, including micro-transactions within the metaverse.

Transactions



Metchain strategically addresses the needs of a growing user base by enabling nearly instantaneous transaction processing. It achieves an impressive throughput of 25,000 transactions per second (TPS) and 250,000 transactions per block (TPB).

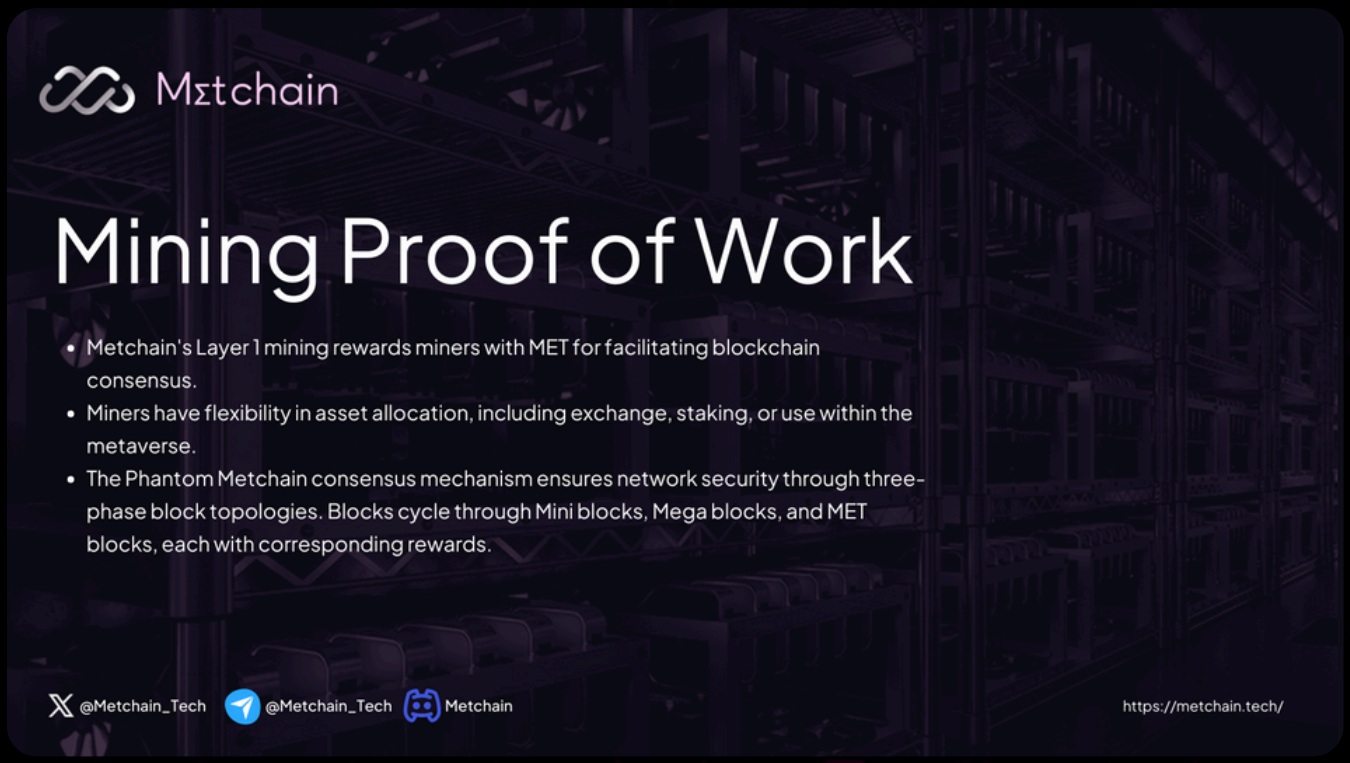
This allows real-time interactions and supports micro-transactions, essential for activities like in-game purchases within the metaverse.

Micro-transactions are crucial for maintaining the ecosystem's efficiency, even with high liquidity locked in layer 2. This ensures the metaverse operates smoothly without liquidity constraints. The overarching goal is to create an ecosystem where transactions are efficient, cost-effective, and capable of supporting diverse real-time interactions.

Fund Allocations

Metchain's treasury funds are allocated as follows: 1% for the development fund, used exclusively for the future development of the blockchain ecosystem, and 1% for marketing and exchange purposes to achieve these specific goals. Transaction fees are used to support the ecosystem and build a treasury balance for future stability and continuity.

Mining Proof of Work



Metchain's Layer 1 mining facilitates primary blockchain consensus, rewarding miners with MET for their work. Miners can choose to exchange, stake, hold, or use their assets within the metaverse. The emissions schedule provides a fixed annual emission of 4 million coins. Metchain's proof of work mining is built on the Phantom Metchain consensus mechanism, utilizing three-phase block topologies for accurate block consensus and enhanced network security.

This mechanism cycles through high-frequency blocks (Mini blocks) for 12 intervals, which are then collated and validated into a Mega block every 13th block. This pattern continues until the 66th block, when all previous blocks are collated into a MET block, restarting the cycle.

The different blocks reward miners as follows:

Block Type	Coin Value	Block Frequency (S)	Block Frequency per cycle
Mini-Block:	0.3 Met	10	60 Blocks per cycle
Mega-Block:	3 Met	120	5 Blocks per cycle
Meti-Block:	15 Met	650	1 Block per cycle

NFT Staking

Holders of MET can stake their coins and Metchain NFTs, enhancing network security and providing sustainable financial returns. Staking involves purchasing one Genesis NFT per stake and maintaining a minimum balance of 15,000 MET coins. Rewards are based on annualized percentage yields (APY) detailed below.

Staking is carried out within the V3 wallet, involving selecting the MET value to stake, choosing the vesting term, and confirming the transaction. Staked MET is transferred to Metchain Coinbase and remains locked until the vesting period ends.

Upon completion, the original balance plus the agreed APY is credited back to the staker's wallet for further use.

APY varies based on NFT rarity and investment period.

Rarity & Term	3 months	6 months	9 months	12 months
Super Rare	2.00%	5.00%	8.00%	11.00%
Rare	1.70%	4.25%	6.80%	9.35%
Less Common	1.30%	3.25%	5.20%	7.15%
Common	1.00%	2.50%	4.00%	5.50%

Community Engagement & Governance

Recognizing the importance of community engagement, Metchain will establish a governance system based on Genesis NFT holders. This allows all NFT holders to vote on crucial ecosystem decisions, shaping its direction collectively. Please note that this system will be fully implemented in Layer 3.

Ecosystem Development

Metchain has successfully developed and integrated Layer 1 and Layer 2, establishing a strong proof-of-work mining consensus followed by proof-of-stake. These layers form the foundation of the ecosystem, enabling blockchain operation and progression.

The next phase involves completing and integrating Layer 3, focusing on the metaverse. This stage aims to reshape decentralized ecosystems. Metchain's upcoming product suite will address challenges like interoperability in the metaverse, web3, and gaming industries.

It will empower developers to seamlessly integrate with other blockchains, facilitating ongoing development and the realization of their metaverse visions.

This innovative suite positions Metchain at the forefront of blockchain ecosystems.

Market Size and Growth Projections

The current market, valued at 51 billion USD, is set for remarkable growth, projected to reach 1.3 trillion USD in a decade (Fact.MR, 2023).

This growth is driven by advancements in hardware and software products and the increasing integration of blockchain technology. Metchain aims to capitalize on this potential, positioning itself to lead industries toward limitless possibilities and a decentralized future. By staying at the forefront of innovation.

Conclusion

Metchain is a pioneering force in the metaverse, Web3, and gaming sectors, leveraging the strengths of Proof-of-Work (PoW) and Proof-of-Stake (PoS) mechanisms to create a synergistic blockchain-based metaverse. This innovative approach addresses industry challenges, providing a foundation of security, sustainability, and scalability for the Metchain ecosystem.

The emissions structure for both PoW and PoS offers multiple entry points into the financial ecosystem, promoting stable tokenomics and asset value appreciation. Community engagement is central to Metchain's vision, with governance vested in Genesis NFT holders, fostering a collaborative and inclusive environment.

Metchain's efforts are focused on fostering the creation and implementation of decentralized applications (DApps) within Layer 3's Metaverse, bridging reality and imagination to deliver a unique user experience.

The evolution of blockchain technology has led to the development of improved PoS algorithms, marking an important step towards a more efficient, scalable, and sustainable future for the industry. As PoS algorithms continue to grow in adoption, blockchain networks are becoming more environmentally friendly, secure, and accessible to a wider audience. With the implementation of PoS algorithms, blockchains are using less energy and computational power compared to PoW mining.

PoS is enabling faster transaction speeds and higher throughput, while also providing more opportunities for people to participate in validating transactions and earn rewards.

By embracing the potential of PoS algorithms, the future of blockchain technology looks promising. Blockchains are becoming more decentralized, interconnected globally, and conscious of their environmental impact. This improved sustainability will allow blockchain to further revolutionize various industries like finance, supply chain, and many others.

As PoS algorithms continue advancing, blockchain networks like Metchain will become even more efficient, scalable, and eco-friendly.

This evolution is paving the way for blockchains to create a decentralized, globally interconnected ecosystem that is equitable and sustainable for the long-term.

The future is bright for this transformative technology, and Metchain is well-positioned to lead the charge in revolutionizing the metaverse, Web3, and gaming industries through its innovative blockchain architecture, community-driven governance, and commitment to sustainability.

Official links and social media

Social media links serve as a bridge between the Metchain team and the community, reinforcing a culture of transparency and open communication. Stay connected with the Metchain team through their social media profiles.

- Website: https://www.metchain.tech
- Block Explorer: https://www.metscan.io
- Metchain wallet: https://metwallet.metchain.tech/vec
- Telegram: https://t.me/Metchainofficial
- Twitter: https://twitter.com/MetChain_tech
- Instagram: https://www.instagram.com/metchain.tech
- Medium: https://medium.com/@Metchain
- LinkedIn: https://www.linkedin.com/company/metachain-tech/about

Algorithm 1

The GHOST backbone protocol, parameterized by the input contribution function I(•) and the reading funcion R(•). xC is the vector of inputs of all blocks in chain C.

1: T GenesisBlock . T is a tree.
2: state <- ε
3: round <- 0
4: while True do
5: Tnew <- update(T , blocks found in Receive())
6: C <-˜ GHOST(Tnew)
7: hstate, xi <- I(state, C˜, round, Input(), Receive())
8: Cnew <- pow(x, C˜)
9: if C 6 ˜ = Cnew or T 6= Tnew then
10: T <- update(Tnew, head(Cnew))
11: Broadcast(head(Cnew))
12: end if
13: round <- round + 1
14: if Input() contains Read then
15: write R(xC) to Output()
16: end if
17: end while

Algorithm 1 Explained

For completeness' sake, we now go over the remaining steps in the GHOST backbone protocol. Funcion update (see Algorithm 4) refers to how the block tree is updated. Funcion pow (see Algorithm 3), which has to do with block mining, is the same as the one described in the Bitcoin Backbone.

Algorithm 2

The GHOST backbone protocol, parameterized by the input contribution function I(•) and the reading funcion R(•). xC is the vector of inputs of all block in chain C.

1: T GenesisBlock . T is a tree.
2: state <- ε
3: round <- 0
4: while True do
5: Tnew <- update(T , blocks found in Receive())
6: C <-˜ GHOST(Tnew)
7: hstate, xi <- I(state, C˜, round, Input(), Receive())
8: Cnew <- pow(x, C˜)
9: if C 6 ˜ = Cnew or T 6= Tnew then
10: T <- update(Tnew, head(Cnew))
11: Broadcast(head(Cnew))
12: end if
13: round <- round + 1
14: if Input() contains Read then
15: write R(xC) to Output()
16: end if
17: end while

Algorithm 2 Explained

For completeness' sake, we now go over the remaining steps in the GHOST backbone protocol. Funcion update (see Algorithm 4) refers to how the block tree is updated. Funcion pow (see Algorithm 3), which has to do with block mining, is the same as the one described in the Bitcoin Backbone.

Algorithm 3

The proof of work function, parameterized by q, D and hash functions H(•), G(•). The input is (x, C).

1: function pow(x, C)
2: if C = ε then . Determine proof of work instance
3: s <- 0
4: else
5: hs 0 , x0 , ctr0 i <- head(C)
6: s <- H(ctr0 , G(s 0 , x0))
7: end if
8: ctr <- 1
9: B <- ε
10: h <- G(s, x)
11: while (ctr ≤ q) do
12: if (H(ctr, h) < D) then
3: B <- hs, x, ctri
14: break
15: end if
16: ctr <- ctr + 1
17: end while
18: C <- CB . Extend chain
19: return C
20: end function

Algorithm 3 Explained

Two essential security characteristics of the Bitcoin backbone protocol; the common prefix and the chain quality property were taken into account in [above and algorithms 2 and 3]. If they remove a few blocks from the tail, the common prefix property assures that two trustworthy participants have the same understanding of the blockchain.

On the other hand, the chain quality feature makes sure that chains from honorable players don't include long stretches of hos1le blocks. These characteristics are defined as predicates over the random variable created by adding the viewpoints of all par- 1es, which is represented by the nota1on view H(.)Π,A,Z (k, q, z)

Algorithm 4

The tree update funcion, parameterized by q, D and hash functions H(•), G(•). The inputs are a block tree T and an array of blocks.

1: funcion update(T,B)
2: foreach hs, x, ctri in T
3: foreach hs 0 , x0 , ctr0 i in B
4: if ((s 0 = H(ctr, G(s, x))) (H(ctr0 , G(x 0 , ctr0)) < D)) then
5: childrenT (hs, x, ctri) = childrenT (hs, x, ctri) U hs 0 , x0 , ctr0 i . Add to the tree.
6: end if
7: return T
8: end function

Algorithm 4 Explained

To make the concepts of persistence and liveness relevant to the manner in which par1es confirm transactions, we slightly modify them. A transaction is ‘stable' in Bitcoin, for instance, if it is at least k blocks deep in the chain and has the parameter k.

On the other hand, for a transaction to be deemed "stable" in GHOST, the subtree rooted at the block containing the transaction must be at least k in size. From this point on, whenever we discuss the longevity or persistence of Bitcoin or GHOST, we'll be referring to the parameterized versions with the corresponding definitions of stability that we just discussed.