POSSCHAIN WHITEPAPER

CONTENTS IN TABLE

INTRODUCTION 2
BLOCKCHAIN GENERATIONS 2
OVERVIEW 3
NETWORKING 3
USING AI ON THE NETWORK 4
RANDOMNESS SOLUTIONS 4
ABOUT THE CONSENSUS MECHANISM 6
CONSENSUS ROLES 8
INCENTIVE MECHANISM 8
SHARDING 9
STATE SHARDING 9
MICRO CHAINS AND MACRO CHAINS 10
PROCESS QUEUE ENGINE 11
ALPHA LAYER 11
UPGRADABILITY FEATURE 12
THE POSS TOKEN 12
COMMUNITY-SUPPORTED MANAGEMENT 12
VIRTUAL MACHINE 12
POSSARENA FRAMEWORK 13
POSSAPP TESTNET 14
TEAM AND COMMUNITY 14
ACKNOWLEDGMENT 14
SUMMARY 15
CONCLUSION 15
DISCLAIMER 16

INTRODUCTION

Technology has allowed the world to unlock extensions of talent that previous generations could not even dream of. However, vehicles that are now a part of our daily lives are controlled by many technology giants. Monopolizing an unethical industry, Big Tech is selling its users' information. People want their privacy back.

Blockchain promises the most in protecting user privacy. The distributed nature and various forms of encryption on the blockchain allow users to interact securely through a fair and private system. Although the potential of blockchain is clear, the technology is in its infancy. Before mainstreaming, blockchain technology needs to overcome several hurdles: sustainability, interoperability, and efficiency—each limit both the scalability and functionality of blockchain technology. For example, if all blockchains cannot communicate with each other due to a lack of interoperability, blockchain technology is not truly decentralized.

If the lack of interoperability in blockchains is resolved, will the information flow cause backlogs due to low throughput? Will scaling blockchain technology have a negative environmental impact that eclipses the benefits?

The development team at Posschain has pushed the outer limits of blockchain innovation to come up with a solution. Posschain transcends all existing forms of blockchain technology, bringing the industry mainstream by addressing scalability, interoperability, sustainability, and usability. “Tech giants control our daily lives. People want their privacy back!”

BLOCKCHAIN GENERATIONS

Each successive generation of blockchain technology has delivered exponential growth. The first-generation pioneer Bitcoin gave us the first digital currency to be traded without a third party. First-generation chains provide security and immutable transactions and lay a solid foundation for innovation. Recent headlines highlight the potential environmental impact of proof-of-work (PoW) models and the lack of scaling and communication capability.

Ethereum, Neo, and Tron are entering the scene as examples of second-generation blockchains. The tremendous growth of decentralized finance (Defi) is almost entirely due to Ethereum. Second-generation blockchains expanded functionality and allowed the running of multiple decentralized applications (dApps) and token projects using smart contracts. Although similar to the first generation in terms of limitations, smart contracts provided more user options and applications. However, in practice, the framework of work (PoW) raises concerns about high energy consumption and associated trading fees.

The industry is now laser-focused on third generations of blockchains. For example, Cardano, Polkadot, and Cosmos attempt to address the limitations of cross-chain communication, scalability, and sustainability. Commonly utilized in third-generation chains, Proof of Stake (PoS) scales faster as processing is divided amongst the network, providing energy-efficient transaction solutions. Delegated proof of stake (DPoS), a consensus algorithm designed for technology governance, protects third-generation blockchains from centralization and malicious usage. Interoperability, the ability to communicate with other chains, is another primary target. Providing complete interoperability and scalability within an eco-friendly manner is the primary goal of the third generation and beyond.

OVERVIEW

Posschain is a next-generation blockchain protocol that allows all legacy, current, and future blockchains to scale and communicate with each other seamlessly. Through sharding, interoperability, and centralized AI consensus protocol, Posschain opens up many possibilities in the blockchain space.

After extensive research, the Posschain development team has designed and built an enterprise-grade blockchain platform solution that combines the best features of each existing blockchain. Posschain paves the way for blockchain and distributed technology by simplifying the use and development of blockchains and addressing common issues such as blockchain interoperability, scalability, and sustainability.

Posschain provides advantages over existing and legacy blockchains, such as sharding, simple blockchain creation and implementation, cross-chain capabilities, and high transaction throughput.

NETWORKING

Current blockchain technology suffers from confirmation latency, the time between transaction issuance and network confirmation. Advancing existing consensus protocols will only result in slightly lower delays. The propagation delay of messages through the underlying peer-to-peer network is at the root of the blockchain's confirmation delay.

Transaction nodes used to discover each other within a network need to change to resolve latency issues. For most blockchain ecosystems in the market, common node discovery is random. This approach raises concerns as it neglects geographical distance between nodes, differences in bandwidth, hash power, and computational capabilities.

Posschain created a decentralized neighbor selection protocol that constantly tries to develop optimal peer connections to reduce confirmation latency. The protocol achieves this by continually analyzing and learning how nodes interact with their neighbors.

The hard-coded topologies that users can find on the standard blockchain often require extensive tuning to optimize performance within the blockchain. Posschain's self-learning algorithm quickly locates the best topology for any network. Posschain's Neighbor Selection Protocol uses the right balance of discovery and exploitation by learning how nodes in a network communicate with each other. Through exploitation, the protocol pairs nodes with neighbors, ensuring good connectivity during block announcement times. The protocol finds potential candidate peers that will better connect with the existing node through research. Through this usage and discovery process, the protocol focuses on the most suitable topology for the network, which reduces the overall latency.

Posschain's protocol is attractive for the following reasons:

- Light.
- The ability to choose the best neighbors or compatible with personal interests.
- Robust against hostile actions: A Posschain peer does not need all the details about the prospective neighbor to decide whether to connect or not.
- Encourages peers to transfer blocks immediately.
- Naturally adaptable to varying hash rates.

USING AI ON THE NETWORK

Posschain includes an AI model at the heart of the blockchain. This AI model helps the network reach consensus effectively and reduces the overall byzantine error of the network. These speeds up the network's batch processing times and keeps the network running under attacks or flags.

Posschain's AI model coordinates the various roles of each node in the network. The nodes are arranged in a hierarchy based on a trust rating system. The higher the node reaches the order, the higher the degree of trust. A higher degree of confidence provides access to vital roles in the network. A node's trust rating can be adversely affected and then dropped if the node mishandles a transaction. This mainly includes disrupting or slowing down the network or creating an incorrect trade.

It takes about six months for a node to reach a 99.9% confidence rating. If a node's collective trust rating is lowered, it moves down the trust hierarchy and is assigned a less critical role in the network. Once a node's trust has been reduced, it will take time to reach its full potential again.

It takes about six months for a node to reach a 99.9% confidence rating. If a node's collective trust rating is lowered, it moves down the trust hierarchy and is assigned a less critical role in the network. Once a node's trust has been reduced, it will take time to reach its full potential again.

AI randomly selects nodes to test and collate information. This phase identifies terrible nodes. Selected nodes are listed as inactive during testing. Reactivation occurs when the chosen nodes pass all tests successfully or achieve a degree of confidence above or equal to the threshold set by the network administrators. These tests include:

- Behavioral controls using AI and Machine Learning
- Data integrity checks
- Hardware speed controls
- Network speed checks
- Security controls

Following the testing phase, the results of the node form part of the factors that determine the degree of confidence of the node. Other factors include reputation in the network and time active on the web.

RANDOMNESS SOLUTIONS

Randomness plays a pretty important role in the blockchain ecosystem, especially in every blockchain. It affects the difficulty in mining functionality of PoW blockchains and periodically selects validators on a PoS blockchain.

It isn’t easy to achieve randomness on a blockchain. When trying to attain on-chain randomness, a standard developer error occurs when the randomization process includes quantities such as future block hashes, block difficulty, or timestamps. This makes the process open to manipulation by miners. Miners can potentially notice how choices affect the randomness generated on the chain. This makes it easy for attackers to visualize how different inputs affect the outcome of a random number generator. Attackers can take advantage of this and potentially skew the result of the pseudo-random generator.

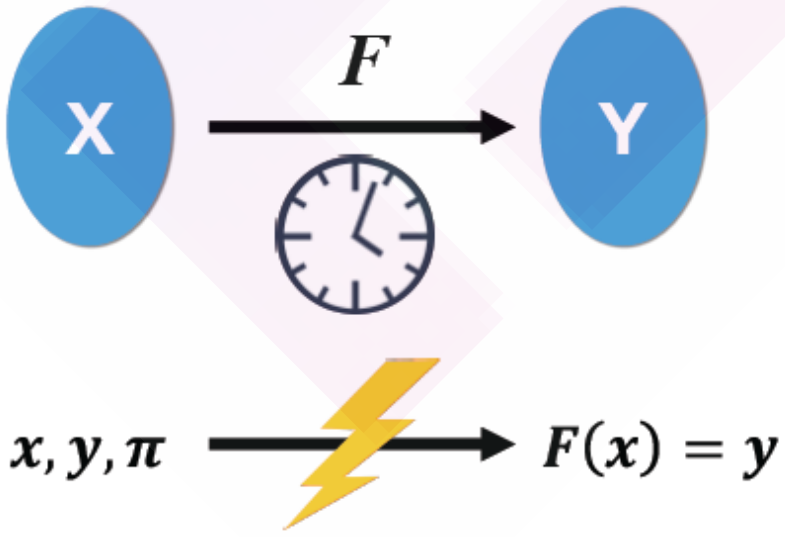
Many solutions have been proposed to solve randomness in blockchain ecosystems. Two unique solutions are verifiable delay functions (VDFs) and verifiable random functions (VRFs). VDFs are functions that require moderately sequential computation to evaluate but are verified very quickly for accuracy once solved.

VDFs have time delays applied to the output of a pseudo-random generator, preventing malicious actors from affecting the generator's output because all inputs are terminated before users can complete the computation of the VDF. In retrospect, VDFs are a computationally cheaper alternative to the PoW mining puzzle tailored specifically for PoS blockchains.

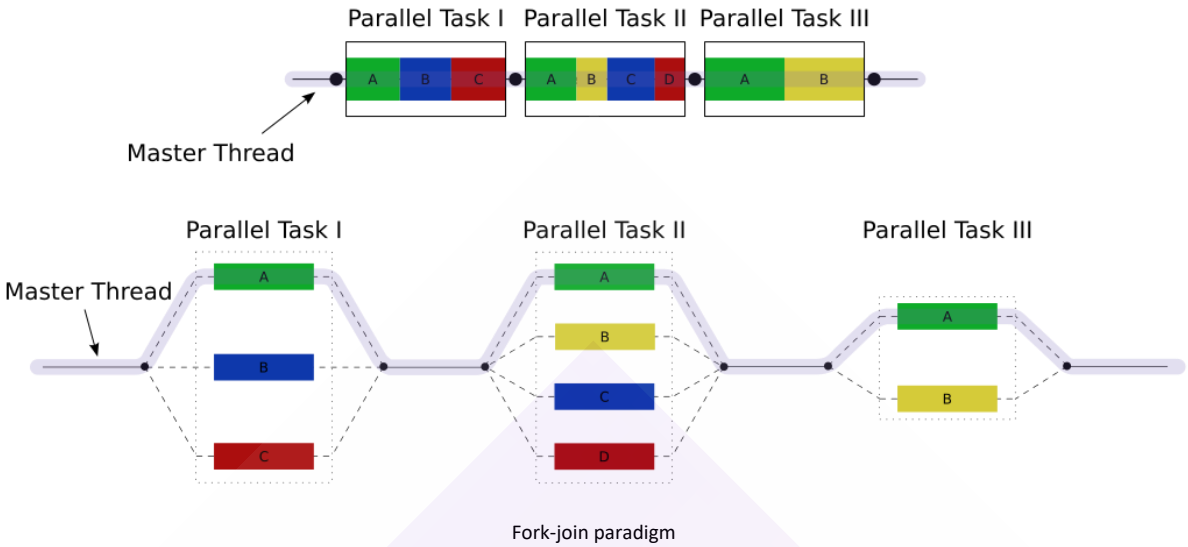
VRF is the public key version of the keyed cryptographic hash. Only the owner of the private key can calculate the soup, but anyone with the corresponding public key can verify the correctness of the hash. VRFs are helpful when trying to avoid enumeration within hash-based structures and, like any other type of function, it takes input and produces an output. This output contains a random number and proof that the node executing the function correctly generated the lucky number. The process takes the defined input and performs mathematical operations to produce the output. This is easily verified by anyone who challenges the validity of the production. A VRF includes the following security features: reliable uniqueness, complete collision resistance, and full pseudo-randomness.

VRF consists of time slots called slots. These slots are technically called periods in the Posschain blockchain. Each validator in the network "rolls a dice" in each slot by executing the VRF. VRF takes a secret key, a period randomness value, and a slot number as input.

When a node calls the function, the node's result - the random number - is compared to a threshold defined by the protocol. If the value is less than the threshold, the validator responsible for the output becomes a suitable block generation candidate for that slot. The validator then tries to create a block with the obtained proof and the resulting random number and send it to the network.



Evaluator and verifier attached.



Fork-join paradigm

As a result, the purpose of VDF is to make a big difference between the computation time of the validation function and the computation time of the evaluation function. In this paper, an example function constructed from the permutation polynomial is presented as follows.

Candidate permutation polynomial. We consider the following polynomial of Guralnick and Muller [37] over $\mathbb{F}_{p^m}$:

$$\frac{(x^s - ax - a) \cdot (x^s - ax + a)^s + ((x^s - ax + a)^2 + 4a^2x)^{(s+1)/2}}{2x^s} \tag{5.1}$$

Equation 5 VDF candidate function

ABOUT THE CONSENSUS MECHANISM

The consensus mechanism determines how quickly and securely validators on the blockchain will reach consensus on the next block. Proof of Work (PoW), the first successful implementation of a consensus mechanism within a blockchain, was used in Bitcoin. In PoW, all network participants rush to solve a complex mathematical puzzle to get a chance to add their blocks to the network and win associated rewards.

The second application of a consensus mechanism gaining traction in the blockchain space is Proof of Stake (PoS). In PoS, participating validators receive rewards on the network based on the amount of the network's native cryptocurrency they stake or lock in a wallet for a given period.

Another consensus mechanism, Practical Byzantine Fault Tolerance (PBFT), has been researched and developed for over two decades. PBFT is an ideal consensus mechanism for institutional consortia, such as blockchains, where all members are only partially trusted.

Consensus rounds in PBFT involve a node chosen as the leader. In contrast, the other nodes are each validator and can be divided into the preparatory and completion phases.

The leader broadcasts his proposal for a new block to other validators, who then post their votes on the proposal to the rest of the network. For messages to be broadcast continuously, each node in the network must count each vote.

When more than 2f + 1 consistent votes are seen, and the total number of validators plus the leader is 3f + 1 (f = number of malicious validators), the preparation phase is complete. Similar vote-counting is used during the commitment phase, where consensus is formed when 2f+1 consistent votes are seen.

A disadvantage of the PBFT consensus mechanism occurs when the network becomes extremely slow when it reaches a validator threshold and loses its ability to scale. This is due to the number of messages that each authenticator in the network must send and receive from each node.

To address the scalability issue of PBFT, the Accelerated Practical Byzantine Fault Tolerance (APBFT) consensus mechanism is inspired by best practices, including Posschain, HotStuff, and Harmony's consensus protocol (FBFT) to create a consensus mechanism by reducing communication complexity within standard PBFT implementations. Developed the tool. Rather than publishing the votes for each verifier, the leader conducts a multi-signature signing process to collect the votes of all verifiers. Now every node doesn't need to take and count each of the voices of the remaining validators in the network; it just accepts one multi-signature.

A deeper dive into Posschain's enhanced APBFT consensus mechanism reveals the two algorithms responsible for selecting the node to be the leader and the remaining validator nodes in each segment within the network. The primary algorithm used to choose the leader and validator nodes in a shard is a random function such as VRF. The VRF function will output the new leader for the fragment in a generation in each new era. Suppose the primary random function cannot extract a set of candidate leader and validator nodes. In that case, a secondary algorithm is called in the selection process to ensure that the epoch in a given shard has a set assigned to it.

Posschain's APBFT consensus includes the following steps:

1. The leader broadcasts the block header he formulated to all validators. Simultaneously, the leader publishes the block’s content with the erasure coding, called the "announcement" stage.
2. Validators check the validity of the block header. If valid, they sign the block header with a Boneh-Lynn-Shacham (BLS) signature and send the signature back to the leader.
3. When the leader receives 2f H 1 valid signatures from the validators, it collects them into a BLS multi-signature. The leader publishes the batch multi-signature and a bitmap showing which validators signed it. This step forms the “preparation” phase with the second step.
4. Verifiers check that the multi-signature has at least 2f H1 signers, verify transactions in the block content broadcast from the leader in Step One, sign the message received from Step Three, and send it back to the leader.
5. The leader then waits for at least 2f H1 valid signatures in step four, combines them into a BLS multi-signature, and creates a bitmap that logs all the signers. Finally, the leader commits and publishes the new block with all multiple signatures and bitmaps added for all validators to commit. The fifth and fourth steps make up the "commitment" phase.

CONSENSUS ROLES

- Validators: Validators are nodes on the Posschain blockchain that validate, process, and attest transactions on the blockchain. Through its democratic consensus mechanism, validators are voted for by community members that have voting rights.
- Defenders: A node type attests to the validity of blocks as they are formed and submitted to the chains. A Defender fishes out for any illegal partnerships formed by malicious actors on the network and is rewarded for their work.
- Nominators: Members who hold tokens on the chain nominate staking members as validators for transactions. Nominators receive a part of the reward that their nominated validators receive for their work in successfully assigning validators.

INCENTIVE MECHANISM

A distributed system relies on nodes in the network to provide security. Nodes are responsible for keeping accurate records of all transactions within the web and acting in a way that does not challenge the network's consensus. As an additional measure to ensure that the nodes are working correctly, nodes are encouraged by the network to maintain security and report malicious or misbehaving nodes to put the safety of the network at risk.

A standard attack on the PoS blockchain is called a long-range attack. These attacks exploit blocks in PoS blockchains that rely on signatures, not computer-intensive computations like PoW. Hackers can steal keys from a trusted validator, using it much later to create a simulated version of the original blockchain. Since these blocks are signed with trusted private keys, new nodes cannot decrypt between the actual and simulated blockchain.

These private keys are obtained in one of two ways. The keys were either stolen due to a security breach in the validator, or the keys were purchased from a no longer used. The Posschain network fights attacks by incentivizing nodes. Incentive models depend on the consensus protocol and may differ slightly on each blockchain.

In Proof of Stake, validators are rewarded for verifying and validating blocks with correct transactions. The distribution of rewards for validating a block depends on the number of votes a node cast for the league. The distribution of mining transactions within the block is also distributed similarly. If a node confirms or confirms a block of wrong transactions, its stake is cut. If a node reports a dishonest node to the network, it receives rewards in cryptocurrency deducted from the illegal node's stake. This encourages nodes to act within the network's consensus rules and report dishonest nodes.

The Posschain ecosystem uses the same incentive system to secure the blockchain across all nodes. Posschain's incentive model combined with the AI-based consensus protocol creates a highly secure blockchain ecosystem.

SHARDING

Currently, blockchains face a triad. No existing blockchain provides decentralization, security, and scalability simultaneously.

Heterogeneous sharding, a potential secure scaling solution, is the ability to run multiple shards, each with specific parameters such as transaction fees and block header sizes, without affecting the performance of other bits. Fragmentation significantly reduces the latency of a blockchain by dividing the transaction processing workload into smaller chunks called shards. This allows for parallel processing of transactions, which increases the throughput of a blockchain.

Although sharding allows for faster throughput within blockchains, there are some issues with the security and validity of shard data before blockchain can be considered a viable option for scaling.

Potential issues of blockchain sharding include verifying the state of a blockchain and the potential security risk of reducing nodes due to the total nodes being scattered among the shards. Low throughput in inter-part operations also needs a solution.

Posschain's heterogeneous fragmentation model offers a safe way to tailor each fragment to a specific use case. It also solves the high latency and low throughput of cross-shard transactions using a two-stage commit protocol. Posschain 's fragmentation model also addresses the lack of validity and security of fragment data using erasure codes and polynomial coded fragmentation.

STATE SHARDING

The current low transaction volume of blockchain technology has resulted in the blockchain community seeking methods to increase the technology's transaction processing capabilities. One approach is sharding, splitting the total computational work of the leading blockchain into multiple smaller blockchains. This dramatically increases the throughput of a blockchain by allowing transactions to be processed in parallel on various shards. One aspect of sharding found in the Posschain Blockchain is State sharding. In-state sharding, each bit maintains its blockchain and state database. Validators on each shard do not need to verify the entire global state of the network but rather 1/N of the worldwide state (N=number of bits present in the network). The eventual atomicity of cross-shard transactions guarantees that double spending cannot occur and ensures states' consistency between shards. Atomicity refers to the integrity of the entire blockchain, not just one blockchain component.

Selections of validator nodes are performed on the main blockchain after a certain number of periods have passed on the Posschain Blockchain. A period is a predetermined period during which the verification committees of the parts remain unchanged. The result of the selection is written in the last block of the epoch on the main blockchain. Once this is complete, the leading blockchain enters the new era with the newly elected verification committee and all the pieces. The new shard State of the main Posschain Blockchain is then written to the new block of each shard, creating the last partnership of the period for that shard.

The Posschain network uses crosslinks to facilitate communication between the main Posschain blockchain and various parts. A crosslink can be a block hash, block number, period, etc. It contains data corresponding to block signatures and block identification. When a new block is confirmed in a shard chain, the corresponding crosslink is created and sent to the main Posschain Blockchain for validation. After the mainchain has verified the signature of the crosslink and that it comes from the shard's canonical chain, the verified crosslink is added to the new block of the leading blockchain to confirm the shard chain's block canonical permanently. Without corresponding crosslinks verified and added to the main chain, the network considers broken chain blocks invalid.

Posschain implements State sharding to process transactions in parallel, thus significantly increasing the transaction throughput of the Posschain Blockchain compared to current blockchain technology.

MICRO CHAINS AND MACRO CHAINS

The main Posschain Blockchain consists of several parts classified in two ways: Micro Chains and Macro Chains.

As the foundation of the Posschain platform, Micro Chain controls and coordinates the entire network and is responsible for security, consensus, and monitoring. Verifiers on the Posschain Blockchain stake the native cryptocurrency on the Micro Chain. Since the primary responsibility of the Micro Chain is to coordinate the network, it has minimal functionality to enable it to fulfill its obligations.

One of the primary responsibilities of Micro Chain is to secure the network. Including the block header from each piece, the chain helps strengthen the security and consistency of the various states of the pieces that make up the network. After a new block is linked to a shard chain, the block header is sent to the Micro Chain. Micro Chain then checks the validity of the block header as follows:

1. Verifying the previous block’s hash already processed in the Micro Chain.
2. Verifying who signed the multi-signature of the block to ensure the authenticity of the verifier for this piece.

The committed block headers on the Micro Chain are then broadcast to the network. After broadcasting, each shard adds the block headers to its internal chain that follows the current block headers of all other bits in the network. These internal chains validate transactions on other bits.

Adding the block headers of fragment chains to the Micro Chain provides the following benefits:

1. The difficulty of attacking a single shard increases as attackers must corrupt both the shard chain and the Digest Chain to convince the other shards that an alternative block is valid.
2. Reduced network cost associated with publishing block headers between shards.

Other notable jobs are delegated to Multiple Chains with different applications and features. Macro Chains, which are multiple chains operating simultaneously, can be an instance of an existing blockchain or independent blockchains with their use cases and tokens. Macro Chain is a blockchain that processes and validates its transactions and stores its state.

While relatively independent, each multi-chain communicates with other ecosystem parts through cross-part communication. Cross shard communication breaks the barrier between shards in a shard-based blockchain, allowing each bit in the ecosystem to expand its functionality. This is accomplished in one of three ways:

1. Relying on the main chain facilitates communication between parts, also known as central chain-oriented communication.
2. The use of a client-driven cross-shard processing mechanism, also known as client-driven communication, in which messages between shards are collected and sent by clients of the ecosystem.
3. Messages sent between shards by nodes in the bit without external assistance, also known as shard-based communication.

Client-oriented communication places an unnecessary burden on the clients of the network. Resource-intensive, main-chain-oriented communication includes limitations when network traffic and transaction activity increase. Therefore, Posschain implements piece-oriented communication. The advantages far outweigh the disadvantages, especially when compared to the other two cross-piece communication methods. Using erasure codes to encode messages, Posschain reduces the overall communication cost in the network by using a network-level broadcast in fragment-oriented communication. This ensures the robustness of the cross-shard communication on the Posschain Blockchain.

PROCESS QUEUE ENGINE

Transactions are queued on the blockchain in the transaction queue engine. More specifically, validators take raw trades and process or verify them. Traditionally, validators on the blockchain handle all unprocessed transactions (within the boundaries of the structured network) and verify them with each new verification cycle. Recent unprocessed transactions added to the queue are processed in the following validation cycle.

Research into optimizing the transaction queue and reducing the average transaction processing time shows that specifying a minimum number of raw transactions in the line before starting the next validation cycle optimizes the approach. Alongside the fragmentation and parallel processing of transactions, Posschain has reduced the average blockchain transaction confirmation time by optimizing the transaction queue engine and configuring a minimum threshold within the network before the next verification cycle begins.

ALPHA LAYER

As blockchain adoption increased, the throughput of existing blockchain technology could not keep up with the increasing volume. Research and development of potential solutions are currently being explored in the blockchain ecosystem. Blockchain scaling solutions are divided into different tiers, mainly tier 1 and tier 2. Tier 1 scaling refers to modifying the blockchain itself to increase scalability. Changing the blockchain directly is complex.

Layer 2 scaling refers to increasing the throughput of a blockchain by refreshing the physical blockchain and enabling off-chain transaction processing. Authenticated messages sent between users transacting off-chain accomplish this. These authenticated messages pass through an external medium to the physical blockchain's first layer but depend on it. The leading blockchain is only invoked to resolve disputes. The consensus algorithm determines the security and non-surveillance features of the second layer. When classifying layer two scalability solutions, there are three classifications: protocols, commit-chains, and channels.

Protocols are vital components of blockchain technology and allow secure and reliable information sharing between cryptocurrency networks. They are basic rules that define how data can be shared between computing systems.

Commitment chains leverage an untrusted, non-custodial operator to facilitate communication between transacting parties. The operator commits to the status of user account balances by sending periodic updates to the main blockchain.

The channel, which is a mechanism, provides a particular layer for communication. This allows subsets of members to create a separate ledger for their transactions. Posschain's Alpha layer combines all three of these Layer 2 methodologies to develop a unique scalability layer used to scale any blockchain.

UPGRADABILITY FEATURE

Software development has come a long way since the 90s, especially when looking at the upgradeability aspect of the software. These apps on our phones are updated seamlessly while we sleep.

But that is not the case for blockchain development teams and blockchain software. Up until this point, blockchains could only be upgraded after forking. What forking requires is to create a new version of the blockchain. As you can imagine, this is a grueling and lengthy process. Especially if it was just a few minor upgrades, it was clear that the blockchain industry needed a way to upgrade blockchains seamlessly, to have a surge of apps on our phones. This is where forkless upgrades come in.

A forkless upgrade is a future-proof concept that enables a blockchain to be upgraded without forking. Inspired by the Substrate framework, the Posschain blockchain includes a fork-free upgrade feature made possible by Posschain's on-chain governance system, allowing agile blockchain development and improvement.

THE POSS TOKEN

Unique to the Posschain platform, the POSS token allows users to transact with others on the blockchain and pay all service fees in the ecosystem. The token can be used for governance, betting, transactions, smart contracts, and validator rewards on the platform.

COMMUNITY-SUPPORTED MANAGEMENT

Early blockchains did not have formal management procedures. Individual stakeholders were powerless to propose or veto protocol changes unless they knew the right people.

VIRTUAL MACHINE

A virtual machine acts as a layer between the execution software and the execution machine. It also allows multiple applications to run independently of each other. A great example of a virtual machine in the blockchain ecosystem is the Ethereum Virtual Machine (EVM). EVM is not only a decentralized currency like Bitcoin or Ethereum but also a distributed state machine that can create decentralized applications using smart contracts. The EVM updates the states of the applications built on it each time a new block is created. The EVM is executed as a stack machine with a depth of 1,024 items. Each element is a 256-bit word chosen for ease of use with 256-bit encryption such as Keccak-256 hashes or secp256k1 signatures.

In the virtual machine's Posschain instruction set, opcodes are commands used to execute specific tasks. In total, there are 140 transaction codes that together complete EVM touring. Given enough resources, it can calculate almost anything. Since each opcode is one byte in size, there can only be a maximum of 256 opcodes. All of these opcodes can be divided into the following categories:

1. Stack manipulating opcode
2. Arithmetic/comparison/bit opcode
3. Environmental transaction code
4. The opcode that manages the memory
5. Transaction code manipulating storage
6. Operation code related to the program counter
7. Stopping transaction codes

The virtual machine uses bytecodes to encode opcodes to store these opcodes efficiently.

The Posschain network contains the EVM-inspired virtual machine. Using EVM as a blueprint, Posschain has created a virtual machine that overcomes the limitations found in EVM to enable the scalable and sustainable development of decentralized applications.

POSSARENA FRAMEWORK

Building a private blockchain can be quite complex and takes unnecessary time.

Posschain's Possarena framework simplifies blockchain creation, allowing developers to focus on optimizing blockchains for specific use cases. Being modular, the framework enables the user to implement ready-made, fully customizable components or modules such as networking and consensus to suit user needs.

Possarena comes with various tools that streamline the blockchain development process and allow simple implementation of custom business logic. Developers can effortlessly combine the off-the-shelf components offered by the Possarena framework with their custom-developed features to create the desired enterprise-grade blockchain.

Besides the ready-made components and modules available in the Possarena framework, developers can use several development engines that open up additional customization and functionality, such as consensus algorithm selection or a custom cryptographic hash function. Developers can leverage Possarena's State, Tokenizer, Consensus, and Cryptography Engines.

Possarena's ecosystem, a state-of-the-art peer-to-peer networking platform called libp2p, uses a modular system of protocols, features, and libraries to develop peer-to-peer networking applications.

Integration with blockchains inside and outside the Posschain ecosystem is also possible, with Possarena's native blockchain connectivity capabilities such as cross-chain communication, collaboration, and shared security.

Cross-blockchain data transmission can be securely isolated using a TPPL and P2P communication and routing inspired by the Invisible Internet Project (I2P). A universal layer applied to every Posschain linked chain, TPPL adds an extra layer of security and privacy when transacting on a blockchain.

Developed using Rust, Haskell, C++, and Golang, Posschain and Possarena provide optimal implementation and protection. Being the most advanced programming languages on the market, these programming languages offer fast speeds and solid performance. Web Assembly (Wasm), a super-performance virtual environment that allows code written in multiple languages to be run on the web at near-native speed, provides a platform for Possarena's runtime architecture.

POSSAPP TESTNET

Possapp Testnet is the experimental playground blockchain for Posschain. Developers can test blockchain applications and integrate them with all existing services Posschain offers without interrupting Mainnet's operations. Additionally, it includes a tap and a block explorer, so developers can go through unlimited testing of their apps and easily track transactions within their apps during the testing phase.

Community members who feel Posschain's native cryptocurrency of the network maintain and manage the Possapp Testnet. It also functions as an independent blockchain. Integrating with the test net, developers can explore Posschain technology limits in real-world applications before deploying to the Posschain Mainnet.

TEAM AND COMMUNITY

Posschain is centered around the community. The Posschain native token (POSS) allows users to vote for management and developer teams within the platform. Funding for the project comes from contributions by the Posschain community. The community will vote on any proposed changes to the blockchain or platform and create a user-centric blockchain.

The Posschain team shares a passion for blockchain technology. It is open to collaborating with other blockchain projects. We will hold webinars and conferences for these other projects, creating a larger developer community and sharing our know-how. By integrating and collaborating with different platforms and tokens, project teams can benefit from the support of the broader community of followers that Posschain plans to build.

Posschain aims not only to address the current limitations of blockchain technology through its hybrid software solution but also to make a lasting contribution to the blockchain ecosystem by growing the global blockchain community.

Posschain truly believes in a peer-to-peer community. Active participation in the community takes place through hosted events, grants, and collaborations. For Posschain, we aim to create a genuinely community-centric platform by instilling a community-first behavior within the team's Posschain beliefs.

ACKNOWLEDGMENT

This work is the cumulative effort of multiple people on the Posschain team. It would not have been possible without the help, comments, and reviews from our developers, advisors, community collaborators, and valued founders.

Posschain received service and analyses from the Posschain engineering and marketing team during the writing process, valuable feedback from emails, WeChat groups, Telegram groups, and our online conferences.

Posschain thanks all our advisors and collaborators for their valuable conversations.

SUMMARY

Posschain helps the world regain its privacy and provides a platform for users to interact in a secure and fair system. Sustainability, interoperability, and enhanced throughput met their match. It aimed to demonstrate that it will develop a scalable blockchain with functionality that bypasses current limitations, all within the framework of an environmentally sound system.

Posschain offers a solution at every blockchain development level. The Posschain network reduces confirmation latency by using pivot chains, multiple chains, and bridges. The use of AI in the network helps the blockchain reach consensus and improves security.

VRF and VDF, Unique APBFT consensus mechanism, and state sharing help achieve Neutral randomness while increasing scalability and throughput. Optimized transaction queue engine and virtual machine allow speed and multiple applications to run independently.

Alpha Layer uses three models to create a unique infrastructure that scales to any blockchain, and the Possarena framework simplifies blockchain creation for developers.

CONCLUSION

Posschain's team of professionals from various academic disciplines has conducted extensive research to develop a philosophical understanding of the human psyche to understand the technical limitations blockchain technology faces and explore some of the objections people have to blockchain technology. As a result, Posschain has created a roadmap that provides sustainability, interoperability, and improved efficiency. Posschain aims to prove that it will develop a scalable blockchain with functionality that bypasses existing limitations, all within the framework of an environmentally sound system.

This Cryptographic Object Resource Engine powered by the POSS token will provide the foundation for the future of blockchain technology, allowing all blockchains, past, and present, to scale and communicate seamlessly. At Posschain, we are proud to announce that we have answered all the questions that underpin our research and present it in the Posschain blockchain ecosystem, a simplified, secure, and scalable solution.

For future updates and frequently asked questions, please visit posschain.com.

Join our Telegram group at t.me/posschain to keep up to date with our progress.

DISCLAIMER

The purpose of the following whitepaper is a technical overview. It is not intended to be a comprehensive or final design. Non-critical aspects are not covered.

This article is for discussion purposes only and does not contain investment advice of any kind. In addition, an offer to sell shares or securities does not constitute a request to purchase such shares or securities. None of the inside information is intended to influence any investment decision and should not be the basis for any investment decision. An investment advisor should only give tax or legal advice for any security investment. Posschain encourages readers to seek appropriate and independent professional advice to inform themselves about their investments' legal requirements and tax implications, both within Posschain and within the blockchain industry. Investments should only be made with the assistance of an independent financial advisor in the context of their nationals or country of residence and businesses to purchase, hold or trade in Posschain Token (POSS) or any other token. Please note that this White Paper does not constitute an offer to sell or a solicitation for an offer to purchase for anyone whose participation in a token sale may be illegal. Those who are banned from participating should not participate. Please consult your attorney or accountant to determine whether it is legal for you to join in this coin sale. This document should not be construed as intended to create an investment contract.

This White Paper may be revised so that the newest edition always appears on our website. For each revision cycle, we will provide notes on what has changed and the rationale for the change. Updated versions of the White Paper (as indicated by consecutive edition numbers) may contain information that may override, clarify, or contradict previous versions; In this case, the latest version should be considered the most accurate and up-to-date. Therefore, versions available outside the Posschain website may contain outdated or inaccurate information.

The most current whitepaper version can be found online at: posschain.com.