KOMA CHAIN

Technical White Paper

Blockchain solutions for WEB3 application ecosystem

KOMA Foundation
2023·06

Content

Preface

Blockchain is a new type of database software that integrates multiple technologies such as distributed networks, encryption, and smart contracts. It is an important component of the new generation of information technology and a critical technical foundation for the development of the digital economy. Currently, blockchain technology enterprises and ecological application companies face challenges at different levels from technology, talent, and user demand. Specifically, these uncertainties mainly stem from two aspects:

Blockchain technology is still in its early stages of development. While many different blockchains have emerged, a unified platform and standardized technology that meets industry consensus has yet to be developed.

How to combine blockchain technology with existing industries and effectively apply it is still being explored.

Smart contract platforms and cryptocurrencies have drawn high attention from governments and experts in various fields.

However, due to scalability and user experience issues, they have yet to be widely adopted on a large scale. Even in the most widely used smart contract platform, Ethereum, there has not yet been a national or killer level of DApps. In some cases, one or a few specific applications have temporarily captured significant user groups, but high concurrency often results in severe network damage in a short period. Essentially, this means that even the most advanced platform today is not fully prepared for mass adoption.

On the other hand, the few smart contract platforms with higher transaction throughput can only sacrifice decentralization to achieve relatively faster transaction speeds. In addition, many upcoming solutions suggest developing their blockchain and ignore the billions of dollars in market value already created by existing DApps and other projects on platforms like Ethereum. In a sense, these solutions overlook the huge developer community and ecosystem that currently exists on platforms like Ethereum.

A、Introduction to KOMA:

KOMA is dedicated to providing a more comprehensive and complete blockchain solution for the WEB3 application ecosystem, in order to promote technological innovation in the WEB3 field. In the era of WEB3, blockchain technology has become a necessary tool to achieve many attributes, such as decentralization, information security, transparency, traceability, interoperability, and more. However, with the continuous development of blockchain technology, it is necessary not only to consider the core issues such as security, performance, and scalability of blockchain itself, but also to consider more the integration with other technologies and the connection and integration with the real world.

The KOMA blockchain solution aims to provide a more comprehensive and systematic solution to these issues. Starting from security protocol design, security audit, performance optimization, privacy protection, smart contract coding specifications, development tool chains, cross-chain protocols and other aspects, a blockchain solution that can be applied to multiple scenarios and multiple applications has been created. At the same

time, KOMA not only focuses on the technology itself, but also pays attention to user experience, application scenarios, and business models that support the promotion and application of technology while promoting technological innovation in WEB3. Therefore, KOMA's blockchain solution not only emphasizes innovation at the technical level, but also has profound commercial value and social impact.

Since the emergence of Bitcoin and decentralized databases like blockchain, many different protocols have been developed to design such databases. Recently, the idea of using PoS (Proof of Stake) to build such systems has gained significant popularity.

In the initial PoW (Proof of Work) mechanism used by Bitcoin, the voting power used to incentivize participation and ensure security of the system was proportional to the computational power held by participants. In PoS, however, voting power is proportional to the number of tokens (a specific digital currency unique to the system) held by participants. In such a system, a common approach is to periodically appoint a committee of fixed size participants

known as a delegated committee, which is responsible for running consensus and determining which blocks should be added to the blockchain.

This approach to building a blockchain has two important advantages over ordinary PoW systems, such as Bitcoin:

it allows for the operation of one of the classic authorized consensus protocols developed in the past few decades, and

it not only rewards nodes for participation but also punishes malfeasance by cutting down on the guaranteed margin of members who violate rules.

Recently, significant progress has been made in the design of authorized consensus protocols that can serve as the core engine in PoS blockchains. Most of these protocols are designed under a partially synchronous BFT (Byzantine Fault Tolerance) model, which asserts that communication between nodes eventually becomes synchronized, and no more than a given proportion (e.g., 1/3, which is optimal in this model) of the nodes can behave maliciously in any way they choose.

Advanced protocols such as Hotstuff, Tendermint, and Streamlet are close to optimal and achieve the best in terms of bandwidth, final confirmation time, and implementation simplicity. However, some important properties of such blockchain systems are not covered by the classical models, leaving considerable scope for improvement.

One major aspect is that the partitioning of nodes may not accurately reflect their true attitudes. In fact, according to the model, even "honest" nodes that miss several protocol messages due to DDoS attacks or temporary network failure are considered Byzantine nodes. In situations where more than 1/3 of nodes (even just for a few seconds) experience such network issues, the protocol in the classical BFT model cannot guarantee normal operation, which is a practical problem.

On the other hand, aside from occasional offline periods, it can be reasonably assumed that the vast majority of nodes in real-world systems, if not all, follow protocol rules honestly. This is the result of financial incentives for honest participation. In fact, committee

members would do well to ensure their active participation in the consensus protocol because they will be rewarded for honest work and penalized for being offline or not contributing enough to the protocol's progress. In fact, due to the penalty for protocol violations, it is almost impossible for a adversary to attempt an attack that is not guaranteed to succeed, otherwise it may face significant losses. Therefore, except for large-scale coordinated attacks aimed at destroying the entire system, we should always expect almost all nodes to behave honestly.

On this basis, several studies have designed protocols that are secure in the classical sense, while attempting to provide better guarantees in "typical" cases. In this paper, we propose a new protocol, KoMaBFT, which is beneficial for this work. The security of KoMaBFT is still formalized based on a partially synchronous BFT model. Therefore, it achieves security and liveness, especially in the strictest case where one-third of the nodes are Byzantine nodes. However, based on this, KoMaBFT provides the following two functions, making it particularly attractive for practical deployment.

Firstly, during periods of a large number of nodes participating in a honest manner, it allows for higher "confidence" than one-third to achieve block finality. For example, if a block achieves a finalization confidence of 0.8 (which is possible in KoMaBFT), then at least 80% of the nodes need to violate the protocol in order to roll back the block from the chain. This contrasts with the traditional concept of finality, which is relative: a block is either finalized (which means the finalization confidence is one third) or not. The second practical improvement of KoMaBFT is that it implements a flexibility concept similar to those defined in the literature. Nodes participating in KoMaBFT can configure different security trade-offs, allowing for different numbers of Byzantine nodes and crash nodes (which may go offline but are still honest nodes) in the protocol. Flexibility means that despite the configuration differences, all nodes run a single version of the protocol and perform the same operations, and only the finalization decisions depend on the selected parameters. A practical result is that nodes with lower security thresholds may reach finality faster than nodes with higher thresholds, but as long

as the hypotheses of these nodes are met, they will eventually determine the same block and maintain consistency.

Technically, KoMaBFT can be classified as a DAG (Directed Acyclic Graph) protocol, where nodes collectively maintain a common history of protocol messages, forming a directed acyclic graph that represents causal relationship ordering. In design, KoMaBFT is derived from the Ethereum Casper protocol and improved significantly through the use of new finality mechanisms, message creation schedules, and spam prevention mechanisms. We believe that the simplicity of DAG protocol concepts and the superior practical characteristics of the KoMaBFT protocol make it a reliable choice for a proof-of-stake based blockchain consensus engine.

The KOMA CHAIN aims to address scalability and usability issues without affecting decentralization and leveraging existing developer communities and ecosystems. It is an extension solution for existing platforms, providing scalability and excellent user experience for DApps/user features. The KOMA Foundation plans to

provide KOMA wallets, payment APIs and SDKs, products, identity solutions, and other supporting solutions, allowing developers to design, implement, and migrate DApps based on underlying platforms such as Ethereum.

B、KOMA Architecture

2.1、Basic Model

We consider a system with n validators and a fixed set x, where each validator is equipped with a public key known to other nodes. This model fits the scenario of "permissioned blockchain," but by rotating the validator set, the protocol can also be applied to a semi-permissioned scenario. Our model makes the following assumptions:

• (Reliable point-to-point network) We assume that channels do not drop messages and all messages in the protocol are authenticated by the sender's digital signature.

• (Partial synchronous network) There exists a publicly known bound Δ and an unknown global stabilization time (GST), so that

after GST, any message sent by a validator arrives at the recipient within Δ time.

• (Byzantine failures) We assume that f validators out of n are completely controlled by opponents, so they can deviate from the protocol arbitrarily. We have not made any assumptions about the global relationship between f and n, as security and liveliness require different bounds and the latter also interacts with the number of crashed nodes.

• (Crash failures) We assume that c out of n nodes may permanently fail to respond at some point during protocol execution.

2.2、KOMA blockchain main consensus.

In a typical blockchain system, the task of validators is to iteratively reach consensus on a growing chain of transactions received from the external environment. In this process, they package transactions into blocks to form a blockchain, with each block referencing the previous one via a hash value. The first block is the genesis block and is defined as part of the protocol. In

KoMaBFT, due to the validator set either remaining constant or only undergoing extremely controlled changes, certain validators are directly appointed to construct a block within a designated time period. They do this by packaging transactions in their local queue and by considering the hash value of what should be the previous block. As validators may not reference the last constructed block, either intentionally or due to network failures, the set of blocks B forms a tree, with each block having a unique path leading to the root (genesis block G). In this situation, the main objective of the consensus protocol is to select a single branch from this tree. For each block B, all blocks on other branches are referred to as competing blocks, as selecting any one of them would exclude B.

2.3、Challenges in achieving consensus.

Since the initial definition of the partially synchronous model by Dwork, Lynch, and Stockmeyer, a large body of research has been created to optimize various parameters of protocols in this setting. However, much of it has been written under semi-formal assumptions that assume that there exist more than n⁄3 dishonest

nodes before proofs of the protocol's correctness can be established. This assumption originated from the original paper's proof that partial synchronous protocols cannot guarantee both liveness and safety if $n < 3f + 1$. Despite this negative result, additional guarantees of finality can still be provided for long time periods even if dishonest nodes don't deviate from the protocol and actively work to complete blocks. While this may not seem important from a classical security model perspective, we stress that it has significant practical implications – in most blockchain deployments, it can be assumed that most nodes will collaborate actively towards consensus, for the majority of time. Thus, blocks created during these time periods can provide stronger finality guarantees, requiring collusion of more than $n/3$ validators to revoke them.

Flexibility, there is a natural trade-off between finality and liveness once the traditional $n < 3f + 1$ boundary is no longer applicable. The stronger the finality guarantees we need, the more honest validators are required to collaborate to complete blocks with such guarantees. Agreement on a common finality threshold

used by all validators can resolve this trade-off, but this solution has significant limitations.

However, in KoMaBFT, there is no need to reach a common threshold, so each validator can use a different threshold, even multiple ones. Besides eliminating the need for additional consensus on this hyperparameter, an important significance of this feature is that it allows validators to play slightly different roles in the ecosystem - for example, some validators may mainly handle small transactions and carry out finalization, where small latency is more important than very high security (and as will be apparent after the protocol is introduced, reaching higher thresholds typically takes longer time), while others may prioritize security over latency.

2.4、KoMaBFT

We introduce the KoMaBFT protocol - a consensus protocol that implements strong optimistic finality and flexibility, allowing validators to use different confidence thresholds to confirm that a block has been "finalized". Unless some validators actively violate the protocol, the finality of a block can only increase for a given

validator, similar to how the confirmation count of a block continually increases in the PoW scenario. However, unlike PoW, in KoMaBFT, for a given block, the confidence level can be directly interpreted as the number of validators needed to behave badly in order to reverse such a block, which we formalize in the following theorem:

Theorem 1 (Finality): If some honest validator reaches a confidence threshold $t \geq f$ for a given valid block B, no other honest validator will use a confidence threshold t to finalize a block competing with B.

It should be noted that even though survivability cannot be proven for confidence thresholds higher than n/3 due to the aforementioned impossibility result, in practice, the vast majority of validators will not deviate from the protocol for most of the time. At such times, arbitrary high confidence thresholds can be reached, making blocks constructed during these periods almost impossible to roll back.

Next, we provide an upper bound on the number of honest validators needed to continue finalizing blocks with a given confidence threshold. We note that this is consistent with the traditional $n \geq 3f+1$ bound, adding the concept of "crash faults" (denoted by c), which disrupt the consensus process but are not as severe as Byzantine faults.

Theorem 2 (Survival): For every confidence threshold $0 \leq t < n/3$, if $f \leq t$ and $c < n-3t/2$, then for every honest validator, the blockchain consisting of blocks with t confidence will grow infinitely.

C、Constructing the protocol.

In blockchain, we refer to the initial block as the "genesis block," which is considered to be a part of the protocol definition. Except for the genesis block, all other blocks are composed of a reference to its parent block and the content of the block, represented by prev(B). Typically, a block contains a list of transactions and other information. The parent reference in B is implemented by including the hash of prev(B) in B, which ensures

that there are no cycles in the block graph. We also use next(B) to denote the set of all blocks whose parent block is B. We recursively define the height H of a block as follows: the height H(G) of the genesis block G is 0, and for any other block B, H(B) = 1 + H(prev(B)). We say that block B1 is a descendant of block B2 if we can reach B1 by following the parent links starting from B2, and we denote this as B2 ≤ B1 (in particular, H(B2) ≤ H(B1)).

In the KoMaBFT protocol, validators reach consensus on proposed blocks by exchanging messages and validating one of the possible multiple branches in the produced blockchain. In order to capture and propagate knowledge of different validators on existing messages, it adopts a DAG (Directed Acyclic Graph) framework, where each message broadcasted by a validator references some set of messages previously sent by the validator. We refer to such messages broadcasted during normal protocol operation as units, and the references contained therein as references. More formally, each unit includes the following data:

- Sender: the ID of the creator of the unit.

• Citations: a list of hashes containing other units that the creator wants to attest to.

• Block: if this unit is generated by a validator who is specified to produce blocks within a given time, it will be included in the unit.

D、Why choose KOMA?

Decentralized applications (DApps) are being proposed in large numbers, yet the current blockchain ecosystem is not ready to scale to meet the needs of final user applications with large-scale adoption. Furthermore, DApp user experience is very poor and not beneficial for ordinary users. Slow block confirmations, high transaction fees, low scalability, and poor user experience are some of the main obstacles to large-scale adoption of blockchain applications. The following section explains the problems that currently exist in the blockchain ecosystem and how KOMA CHAIN intends to address them. Detailed technical specifications are provided in other sections of the white paper.

4.1 Solving the problem of blockchain network congestion.

Blockchain transactions are typically very slow and have limited throughput. Most PoW (Proof-of-Work) based blockchain protocols have limitations on block size and require a certain amount of time to generate blocks. Additionally, each transaction must wait for multiple block confirmations due to potential chain reorganizations.

PoS (Proof-of-Stake) based blockchains attempt to offset these limitations using staking mechanisms, but the ability to achieve high throughput with PoS comes at the cost of decentralization. These limitations are typically necessary for public blockchains to ensure security and decentralization, where blocks need to propagate through the network and be verified by all nodes to achieve finality.

KOMA CHAIN addresses this issue by using a high-throughput blockchain that is provided by a set of selected block producers and selected by a set of stakers for each checkpoint. It then uses a Proof-of-Stake layer to validate the blocks and periodically publishes proofs (merkle roots) of the blocks generated by the block producers to the Ethereum mainchain. This helps achieve a high

level of decentralization while maintaining extremely fast (<2 seconds) block confirmation times.

4.2 Solving the issue of low transaction throughput in current PoS systems.

Public blockchains must maintain a certain amount of time lag between the production of adjacent blocks to ensure adequate time for block propagation. Additionally, block sizes must be small to ensure blocks are transmitted quickly through the network. This requires that the number of transactions in a specific block be quite limited.

4.3 Providing sidechain scalability.

In theory, the KOMA network has the ability to handle millions of transactions per second using multiple sidechains. Moreover, the mechanism for the first KOMA sidechain has been proven through the first KOMA concept, and new sidechains can be added and scaled to meet the demands of specific protocols (such as newly introduced NFT/SFT protocols or some enterprise independent validation mechanisms).

In the case of smart contract-based blockchains, each block on the blockchain and/or computational state must be validated by multiple nodes. Each node must maintain copies of the state and the block. Although chain scalability increases over time, maintaining and validating the whole blockchain becomes difficult and leads to a decrease in the number of full nodes on public blockchains, resulting in a decentralized risk.

For the KOMA network, the main decentralized layer can choose to store only the KOMA CHAIN blocks from the previous CheckPoint to the next one. All previous transactions/block proofs have been submitted to the main chain. This can achieve an extremely low fidelity of PoS nodes that can run on low-cost, low-storage machines. In the future, KOMA will also introduce mobile PoS verification nodes.

4.4 Multiple Micro-Payment Channels and Cross-Chain Solutions.

Some payment channel solutions have proposed solutions to micro-payment problems. However, the process of using multiple

DApps or users opening and managing channels is complex. Additionally, there are still debates over the speed and convenience of intermediary payments through channels.

As the KOMA CHAIN uses state-based architecture on the Ethereum Virtual Machine (EVM), there is no need to open payment channels between parties. In fact, any valid Ethereum address is also a valid KOMA address. When they want to retrieve payments on the main chain or try to join the KOMA ecosystem, they only need a KOMA wallet.

4.4.1 Solving the Problem of High Transaction Fees in Traditional Blockchain.

As the blockchain ecosystem rapidly develops, more and more new cryptocurrency assets are being created, transferred, and sold, often involving multiple crypto tokens. Additionally, most decentralized applications have their own tokens and economic models. Paying for blockchain services with tokens or conducting any type of transaction requires chain transfers. Each blockchain has a transaction cost (GAS fee).

The fee amount is an important factor for incentivizing validators and preventing certain types of security attacks (such as DoS). However, there is a problem of fee variability due to limited block size (depending on the queue of transactions to be processed). KOMA achieves low-cost transactions by heavily transacting at the block producer layer, ensuring low costs, and then batching proof of highly distributed KOMA blocks using the Merkle root of the block. The main chain (such as Ethereum) uses a decentralized PoS Stakers layer.

4.4.2 Solving the Problem of Poor Usability in Traditional Blockchain.

Compared to their centralized counterparts, user interaction on DApps is often poor. For the power decentralization revolution to be widely adopted, the user experience of DApps must be on par with, if not better than, that of their centralized peers.

4.4.3 The KOMA system architecture includes the following components:

Cross-chain zones refer to a collection of blockchains that run the same type of business. KOMA can name and address this collection of blockchains and their internal resources. Cross-chain operations create partitions between and within partitions, as well as chains within each partition, based on business needs.

Cross-chain routers are service processes used to bridge business systems and blockchains. Multiple cross-chain routers can be interconnected and forward requests to each other. Users can access resources in cross-chain zones by initiating requests to cross-chain routers. Cross-chain stubs are interface implementations that connect to a blockchain and can be loaded by cross-chain routers. Cross-chain routers can configure multiple blockchain adapters to connect to multiple blockchains. Cross-chain routers automatically synchronize the configuration information of blockchain adapters to help users address resources located on other blockchains.

Cross-chain resources refer to data objects that users can access on blockchains, such as smart contracts and digital assets. Similar to the configuration information of blockchain adapters, the

metadata of cross-chain resources is also synchronized between cross-chain routers. Users can address and call resources in cross-chain zones through a unified interface. To meet the future diversified business interconnection needs and typical business characteristics of massive data cross-chain, KOMA has set the following key design goals for network interaction and deployment architecture.

Cross-regional interconnection: As a blockchain application with multiple parties involved, it usually involves multiple service institutions, and the business is deployed in multiple data centers across regions. KOMA designs a secure, reliable, and efficient network architecture for cross-regional scenarios, based on network mechanisms using TCP long connections, heartbeats, automatic reconnections, and encrypted communication technologies to ensure the stability, timeliness, and security of large-scale cross-regional interconnections.

Flexible deployment architecture: Since cross-chain needs usually originate from mature blockchain application projects, the

cross-chain deployment architecture needs to have the ability to be compatible with existing blockchain instances. KOMA adopts a "non-invasive" design. Cross-chain routers are deployed separately from blockchain nodes as independent processes, and can achieve flexible deployment architecture without changing the existing blockchain network architecture. Cross-chain routers use network transmission of cross-chain messages and blockchain messages, combined with automatic network routing function. As long as there are directly or indirectly reachable network links between cross-chain routers, cross-chain interactions can be completed.

Customizable: Cross-chain requirements in real business scenarios are diverse, and the variety of blockchain platforms that need to be integrated is immense. Therefore, customizable and modifiable cross-chain capabilities are indispensable. KOMA's blockchain adapters and cross-chain resources support free customization, enabling users to select different blockchain adapters and cross-chain resources based on the type of blockchain being accessed, system resources, and network conditions.

The KOMA development team is also developing various mobile and web browser integration tools and is a pioneer in this field. It intends to develop an omnipresent mobile/browser application that will serve as a secure interaction layer for blockchain interactions. The KOMA development team will soon release these designs and prototypes.

E、Introduction to KOMA Network

As mentioned briefly above, KOMA CHAIN aims to address the challenges faced by the blockchain ecosystem by building a decentralized platform using an adaptive version of the DAC framework. This provides fast and extremely low-cost transactions with finality on the main chain.

The KOMA development team is also building a product ecosystem, including user-friendly mobile applications, desktop wallets, and browser extensions that will provide seamless experiences for all users. The vision is for users to be able to make

payments, transfer, or store crypto assets without worrying about the complexity of the underlying systems.

5.1 KOMA Network Architecture

As KOMA's core focus is on mass user adoption, a deep understanding of KOMA's technical architecture should begin with the user journey.

When users transmit ETH or ERC20 tokens on the Ethereum network, they must wait for block confirmations, ranging from 14 to 20 seconds. Even then, users must wait for multiple block confirmations to ensure the final outcome of the transaction. Imagine buying a cup of coffee or paying tokens to watch a movie. In each transaction, you not only have to pay high fees but also wait for confirmations.

In addition, during peak load periods, a large number of transactions can congest the Ethereum network, and each transaction increases GAS fees to obtain faster confirmations. KOMA Network is proposed as a solution to overcome these problems.

5.2 KOMA Role Positioning

KOMA Ecosystem Participants

The KOMA ecosystem will involve the following participants:

End-users

DApp Developers: Developers should use KOMA to extend their applications and provide better UI/UX for their end-users.

Stakers: Stakers need to deposit/hold tokens to qualify and play a critical role in KOMA. They validate transactions using a PoS consensus mechanism with over two-thirds and propose a CheckPoint on the Mainchain. Additionally, they select block producers who meet certain criteria to produce blocks on the sidechain.

Block Producers: These are block producers selected by stakers, who, in turn, can produce blocks more quickly. They must provide full Asset Proof (KMC) to be nominated.

5.3 KOMA Consensus

KOMA CheckPoint and Block Producer Layers

KOMA uses a dual proof strategy with the CheckPoint layer and block producers at the block producer layer to achieve faster block times while ensuring high decentralization through the use of the CheckPoint and anti-fraud mechanisms on the Mainchain.

Through this mechanism, KOMA CHAIN achieves high conversion speed while also achieving high decentralization and finality on the Mainchain. In the first version that only used Ethereum as the base chain, the Ethereum root contract effectively enforced solvency and finality through the Header Chain (CheckPoint). The various elements and mechanisms of the system are described below:

CheckPoint Layer

Essentially, anyone can place their KMCs on the root contract and become a Staker of the PoS CheckPoint layer (deployed on the Ethereum chain). This provides a highly decentralized foundation layer for KOMA CHAIN.

Validation Nodes

In the KOMA blockchain layer, there are several Block Producers selected by PoS Stakers on the base layer, who will create KOMA blocks. To achieve faster block generation time, the number of these block generators will be few. This layer is expected to achieve block generation time of approximately 1-2 seconds at extremely low to negligible transaction costs.

In the CheckPoint layer of KOMA CHAIN, based on the PoS mechanism of the KOMA network, for every few blocks on the block layer of the KOMA network, a proposer is selected among stakeholders to propose a CheckPoint on the Mainchain. These CheckPoints are created by the proposer after validating all blocks on the block layer of the KOMA network and generating a Merkle tree of block hashes since the last CheckPoint. The Merkle root is then broadcasted to the Staker network for signature. The evidence is also validated by other stakeholders. If the proposed blocks are valid, they will be approved by providing a signature.

The system requires the approval of stakeholders to propose a "Title Block" to the root contract. Once a CheckPoint is proposed on

the Mainchain, anyone on the Ethereum main chain can challenge the proposed CheckPoint during a specified time period. If no one questions it and the challenge period ends, the CheckPoint is officially listed as a valid CheckPoint on the Mainchain.

In addition to providing finality on the Mainchain, CheckPoint plays a critical role in withdrawals as they contain proof of tokens destruction upon user withdrawal. It enables users to prove their remaining tokens on the root contract using PatriciaMerkle and Title Block proofs. Note that to prove remaining tokens, the header block must be submitted to the root chain through PoS (stakeholders).

Through this mechanism, KOMA CHAIN achieves high transaction speed, high decentralization, and finality on the Mainnet. In the first version of using Ethereum as the base chain, the Ethereum root contract effectively enforced solvency and finality through the Header Chain (CheckPoint).

Selection of Validation Nodes

Block Producers are selected by Stakers in the CheckPoint layer through voting on the Mainchain. Block producers are selected

within a predetermined time interval until the network consensus mechanism is reduced/removed, or if they are unable to participate in block production due to any external issues.

P2P Network

1. KOMA Network will ask for applications from the public to run the Block Producer nodes 2. It will also run 3 Block Producer nodes itself during the seed stage of the network 3. At the epoch, the public stakers will select a total of 5-7 block producer nodes 4. These nodes will be kickstarted with a KOMA Chain N(number of) genesis configuration

Validation Node Application Process

1. The Block Producers have to apply by staking the Block Producer Stake requirement amount in KOMA Tokens on the mainchain 2. The Network will maintain a pool of interested Block Producers (An incentive system for the Block Producer nominees would be devised to keep ample number of Block Producers in the pipeline)Criteria on the basis on which Stakers will decide to vote for a particular nominee Block Producer are as follows:- Uptime history

- Technical specifications - Dynamic scaling capability - Location persity - Other factors under consideration

Selection through Voting upon Completion of Term

1. Voting process is scheduled and completed one week before the completion of one tenure 2. Existing Block Producers can re-appear in the elections 3. Stakers vote for Block Producers from the pool of Nominees

Replacing Block Producer During Current Term

If a block producer is removed or unable to participate in block production during its term, new block producers will be recruited from a temporary pool. An appropriate incentive mechanism will be designed based on the voters' votes to determine the priority/preference list of validation nodes to maintain a healthy validation node pool.

5.4 Multi-Chain Support

The KOMA CHAIN's public CheckPoint layer is designed to support multiple sidechains. In theory, an infinite number of sidechains can operate under a secure and decentralized CheckPoint

layer. Enterprises can connect their private sidechains to the public CheckPoint layer, where they have complete control over their execution environment while retaining transaction immutability, verifiability, and security through the CheckPoint mechanism.

The key factors expected to influence the design of this sharding process are:

1. The scheduling of the scheduling layer to periodically propose CheckPoints for different sidechains.

2. The flow of assets across multiple sidechains.

3. Users will be able to send assets across sidechains using chain IDs and receipts.

4. An intuitive wallet interface will be provided to users to execute cross-chain transactions.

5. API/SDKs will be provided to developers to build programmable interfaces for inter-chain transactions.

6. Asset movement from one chain to another will be managed at the CheckPoint layer and may not require any interaction with the

main chain. Research is currently underway to facilitate faster (possibly instantaneous) sidechain transfers.

5.5 Interoperability

Interoperability and Integration

As outlined in the previous whitepaper, the Ethereum main chain is the first fundamental/main chain incorporated securely into the KOMA CHAIN, using a DAC framework implementation. Additionally, the KOMA network intends to integrate multiple leading smart contract platform cryptocurrencies, such as Bitcoin, to provide a universal platform for users to use/exchange assets across different blockchains.

It can also provide a robust foundation for a large DEX (decentralized exchange) that hosts assets from multiple blockchains. Furthermore, a single platform that hosts assets from multiple blockchains can generate a significant number of new use cases that developers can conceptualize for their future products. This is an exciting exploratory area for the KOMA development team.

Overall, if the problematic EVM state transitions can be effectively identified for verification, it can be challenged and protected through the EVM-in-an-EVM structure.

5.6 Security

Security Measures

To enhance transaction security, KOMA CHAIN also provides fraud evidence on the main chain. This mechanism allows any individual on the main chain to submit details of a transaction they believe to be fraudulent. If the challenge is successful, the interests of all parties involved in the fraud will be reduced, and the challenger will receive significantly reduced funds as a motivation for detecting the fraud. For any party looking to investigate the authenticity of transactions on the KOMA network, this can be considered a high-reward bounty program that is always running.

Basic proof: When necessary, each proof must submit the following corresponding proofs:

1. Merkle proof contained in the transaction: this type of proof is needed to demonstrate that a given transaction is included in the block.

2. Merkle proof contained in the block: this type of proof is needed to demonstrate that the block is included in the given CheckPoint. Blocks need this proof to demonstrate that they correspond to a valid reference hash sequence.

Transaction

Single-level Transaction Proof

// validate ERC20 TX function validateERC20TransferTx(uint256 headerNumber, bytes headerProof, uint256 blockNumber, uint256 blockTime, bytes32 txRoot, bytes32 receiptRoot, bytes path, bytes txBytes, bytes txProof, bytes receiptBytes, bytes receiptProof) public { // validate tx receipt existence }

Nonce Verification

• Checking for transactions with duplicate nonces

• Checking for transactions with missing nonce values (skipping multiple nonces in between) - this is an interactive fraud proof where in case of challenge to such transactions, the block producer must submit missing random number transactions within a given time frame.

• Checking for transactions with non-sequential nonces.

function validateMisMatchedNonce(bytes tx1, bytes tx2) public { // check if both transactions are not the same ... // validate first transaction ... // validate second transaction ... // check if sender is the same in both transactions ... // make sure 2 is included after tx1 ... // check if both nonce values are same or nonce2 < nonce1, just call slasher ... // revert the operation ... }

Verification

• Checking the receive field, event, topic, and data type in a given receipt.

Deposit

• Verify deposit transaction - Verify the deposit transaction on the main chain to see if it matches with the DepositBlock object on the root chain.

• Duplicate deposit transaction - This proof verifies the existence of any duplicate transactions with the same DepositID, and ensures that each DepositID is included only once.

• Verify deposit amount and depositor address.

ERC20 Transfer

• Verify ERC20 transaction data, receipt logs, and values.

• Check if the UTXO-style input in the log receipt matches the UTXO-style output of the most recent transaction receipt in the log receipt.

5.7 Focus on user experience.

The KOMA development team is developing a wallet by implementing the WalletConnect protocol, an open protocol that connects web-based distributed applications to mobile cryptocurrency assets.

This wallet will help users easily interact with DApps and sign transactions while also helping them to keep their private keys

secure on their mobile devices. This is a significant development that will greatly assist in bringing mainstream users to the blockchain.

In addition, the team is also looking for context-specific gas relay abstractions for Ethereum accounts and identities to enable Ethereum signature transactions, which can further increase mainstream adoption.

5.8 KOMA smart contract.

The KOMA smart contract on the main chain provides the core logic for the KOMA network. The contracts include various mechanisms, such as depositing and withdrawing from the main chain to side chains, and vice versa. They also include a priority queue for withdrawals, periodic state commitments from the Validator layer, anti-fraud mechanisms, binding exit challenge logic, and various other components.

5.9 KOMA CHAIN Bridge（Cross-chain, chain bridge.）

The bridger of KOMA Chain is a part of the block producer node, which listens to the RootContract events on the main chain and monitors any token/ETH transfer events occurring on the

RootContract. The cross-chain solution uses KOMA Chain's Dagger tool. Once the bridge detects a deposit on the main chain, it triggers a deposit event on the KOMA Chain and assigns the deposit amount to the user address on the KOMA network.

5.10 KOMA PoS

The CheckPoint mechanism of KOMA Network is a PoS-based layer that has some Stakers who propose CheckPoints to the main chain. The CheckPoint layer will start with approximately 100-150 Stakers. With the emergence of more efficient signature mechanisms on the Ethereum blockchain, KOMA CHAIN will be able to significantly increase the number of Stakers on the CheckPoint layer, which is expected to further improve its decentralization, potentially comparable to leading public blockchains such as Ethereum and Bitcoin.

5.10.1 Block producer layer

At the base layer, KOMA Network has block producer nodes that are selected by Stakers of the PoS layer through voting on each CheckPoint interval.

Block producers accept transactions through KOMAVM, with the creation of a block expected to occur approximately every 1 second. More technical and code-level details of the BlockProducer layer will be added to higher versions of the whitepaper.

5.10.2 KOMA EVM virtual machine

KOMA uses a state machine based on standard EVM, run by the BlockProducer nodes to generate blocks. Using EVM, KOMA CHAIN can build and deploy protocols such as ERC, as well as other protocols like KyberNetwork, ZRX, etc.

The advantage of KOMA Network architecture is that it becomes very easy to port DApps and smart contracts running on the Ethereum blockchain to the KOMA network, since it uses an EVM-compatible state machine. The KOMA development team intends to support generalized state transitions on the KOMA network, providing a smooth foundation for construction.

5.10.3 KOMA Revocation

When an address on the KOMA network submits a revocation request to the network, the corresponding tokens are burned

(revoked) on the KOMA chain, and this transaction is pushed to the KOMA chain. After a designated CheckPoint interval, the PoSCheckPoint layer publishes the CheckPoint to the main chain, which includes a recording (revocation) proof of these tokens on the KOMA chain. Once this CheckPoint is submitted on the main chain, users can claim their revocation tokens.

5.11 DDos Protect

The block producers of the block producer layer running KOMA will monitor the transfer status of assets to identify redundant transactions. They reject any incoming transactions with zero payment amount, thus thwarting any DoS/spam attacks and enabling zero-cost transactions. Despite the very low cost and fees of KMC, persistent DoS attacks on the KOMA network are economically unfeasible due to its high TPS.

KOMA keeps a record of payment transfer events in a data structure similar to UTXO, allowing for effective verification of inputs and outputs. This enables various security measures.

Perform other checks to mitigate spam based on this, including:

- For each input, referenced outputs must exist and not be already spent.
- Check that the sum of input values is less than the sum of output values.
- Verify that the transaction fee is not too low.
- Check for duplicate transactions in the pool with identical outputs.
- Check for duplicate transactions in the pool with identical transaction fees.

5.12 Potential case

The KOMA Foundation is committed to providing a scalable and user-friendly ecosystem for third-party decentralized applications. Governance bodies, like Ethereum and other platform foundations, will promote a variety of base-chain DApps (such as those currently being built on Ethereum, as well as future ones on

NEO and EOS), to build and migrate user-facing applications/transactions onto the KOMA network. It will also grant funding and financial support to third-party application developers to build various use cases on top of the KOMA CHAIN, such as:

5.12.1 Payment

KOMA CHAIN will provide payment APIs and SDKs for DApps, merchants, and users to instantly accept or pay in crypto assets (such as ERC20 tokens, Ethers, ERC721 tokens).

5.12.2 TOKEN Ecosystem

KOMA contracts allow users to pay with any crypto token they prefer, and the recipient will receive payment in their preferred asset. KOMA CHAIN can process transactions through token exchange between encrypted assets across chains.

5.12.3 Liquidity provider

Third parties can use KOMA CHAIN to exchange tokens for any other token while transferring crypto assets by utilizing 0x liquidity pools or other liquidity providers. In the case of fiat currencies, the

KOMA development team plans to collaborate with major national currency liquidity providers.

5.12.4 Decentralized exchange (DEX) and market support.

It is expected that KOMA will have all the features that a trading platform should have - faster and cheaper transactions. KOMA CHAIN is capable of supporting decentralized exchanges, enabling trustless, reliable, and easy cryptocurrency transactions. Decentralized exchanges are the future of digital assets, providing better security and solvency than centralized exchanges.

5.12.5 Loan and Credit Scoring Platform.

KOMA will allow merchant platforms to evaluate the reputation of associated users based on their transaction history. This enables merchants to offer tokens to users on the network when transacting with users who do not have sufficient funds. KOMA CHAIN aims to provide tokenized debt for users using the Dharma protocol.

5.12.6 Digital identity.

Users need a practical and user-friendly interface without requiring MetaMask or a web3-enabled browser. They don't need to understand how Ethereum works behind the scenes.

Decentralized applications need a way to sign transactions but should not have to submit private keys for every DApp on Web browsers or mobile apps. KOMA's development team believes that users must be able to control their private keys without compromising security concerns. KOMA CHAIN will address this issue through Open-Identity system and provide a seamless experience for users.

The system will also offer a way to automatically approve transactions based on criteria chosen by the user. This will drive recurring payments on the KOMA network.

5.12.7 GAME

We envision games to be a significant part of KOMA CHAIN. Game assets represented by NFTs (ERC721) are expected to be bought, sold, and traded heavily on our sidechain. Developers can also choose to save game states on the sidechain, if they wish. With

the NFT marketplace that we will enable, developers and users will have a truly fast, efficient, and secure sidechain to build and play games on.

5.13 Infrastructure

The KOMA development team will adhere to a simple catchphrase - simple and seamless. To this end, the team will build new infrastructure around KOMA CHAIN, including user-friendly wallets for individual users and merchants, a payroll dashboard, payment SDKs, and other open-source tools.

KOMA Dagger Tool

Starting with Dagger, the KOMA development team has already begun building infrastructure for developers. Dagger is a tool or engine that tracks Ethereum accounts and events in real-time.

Developers can use Dagger to track their own smart contracts, accounts, and transactions. They can create custom services or integrate with third-party services through IFTTT or Zapier.

KOMA Wallet

The KOMA development team is working hard to build an easy-to-use plasma wallet mobile application that integrates with WalletConnect to ensure the secure storage of keys, intuitive access to KOMA CHAIN's capabilities, and a seamless mechanism for connecting browser-based DApps with mobile applications. Users can interact with DApps on browsers and future devices while still keeping their keys stored in their mobile wallets.

The KOMA wallet will serve as a ready-made tool for DApp developers, enabling them to allow their users to quickly and efficiently use KOMA's sidechains.

F、KOMA Native Token（KMC)

The KOMA token (KMC) is a primary component of the ecosystem on the KOMA network, intended to serve as the main token on the network. KMC will be issued as a digital token on the KOMA blockchain that conforms to the ERC-20 standard.

KMC is designed as a utility token, serving as a payment and settlement unit between participants interacting within the ecosystem on the KOMA network.

KMC does not represent in any way a share, participation, rights, ownership, or interests in the management body, issuer, associated companies, or any other companies, enterprises, or businesses. The possession of KMC does not give token holders any commitment, fees, dividends, income, profits, or investment returns, and does not constitute securities in Hong Kong or any relevant jurisdiction. Ownership of KMC carries no express or implied rights other than those which may be provided by KOMA CHAIN and/or any other third parties that may use such tokens.

It is expected that KMC will provide economic incentives to encourage participants to contribute to and maintain the ecosystem on the KOMA network. Various functions on the KOMA network require computational resources, such as verifying blocks and issuing evidence, so providers of these services/resources will receive KMC (i.e. "verification rewards" on the KOMA network) for

maintaining the integrity of the network. KMC will be used as the exchange unit to quantify and pay for the cost of consumed computational resources. KMC is an essential part of KOMA, as without KMC, users will not spend resources to participate in activities or provide services for the entire ecosystem on the KOMA network. Only users who actively contribute to maintaining the network will receive token incentives. KOMA CHAIN users and/or KMC holders who are not actively participating will not receive any KMC as a reward.

To participate in the consensus process of the KOMA network, users need to stake KMC as an indication of their commitment to the process. Therefore, KMC will also be used as a deterrent to prevent various illegal activities (such as invalid blocks, illegal verification blocks, or invalid transaction execution), requiring them to place KMC tokens before being authorized to participate in the ecosystem. If violators commit illegal acts, their KMC will be deducted.

G、KMC Legal Statement

7.1 The tokens are non-refundable and cannot be exchanged for cash (or the equivalent of any other virtual currency) or any payment obligation with the management organization, issuer, or any affiliated company.

7.2 The tokens do not represent or grant token holders any rights to the management organization, issuer (or any affiliated company), or their income or assets, including but not limited to the right to receive future dividends, income, ownership or equity, shares or securities, voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licensing), or other financial or legal rights or equivalent rights, or any other form of participation or association with KOMA, the management organization, issuers, and/or their service providers.

7.2.1 The tokens are not intended to represent any rights of a contract for difference or any other contract whose purpose or assumed purpose is to ensure profits or avoid losses.

7.2.2 The tokens are not intended to represent any currency (including cryptocurrency), securities, commodities, bonds, debt instruments, or any other type of financial instrument or investment.

7.2.3 The tokens are not loans provided to the management organization, issuer, or any affiliated company, and are not intended to represent any debt owed by the management organization, issuer or any affiliated company, and there are no profit expectations.

7.2.4 The tokens do not provide token holders with any ownership or other interests in the management organization, issuer, or any affiliated company.

The proceeds raised in the token sale will be held by the issuer (or its subsidiary) after being sold by the agent, and after the token sale, the contributors have no economic or legal rights or beneficial interest in these proceeds or entities. If a secondary market or exchange for KMC does emerge, it will be entirely independent of the governing body, issuer, KMC, and KOMA CHAIN's sales and operations. Neither the governing body nor the issuer will create

such secondary market, and no entity will be deemed as an exchange for KMC.

H、Risk

You acknowledge and agree that there are many risks involved in purchasing KMC, using KMC, and participating in KOMA CHAIN. In the worst-case scenario, this could result in the loss of all or part of the purchased KMC. If you decide to purchase KMC, you expressly acknowledge, accept, and assume the following risks:

8.1 Uncertain regulations and enforcement actions: The regulatory status of KMC and distributed ledger technology is unclear or unresolved in many jurisdictions. The regulation of virtual currency has become a major target of regulatory bodies in all major countries in the world. It is impossible to predict how regulatory bodies will, when or if existing regulations can be applied, or new regulations will be formulated against such technologies and their applications, including KMC and/or KOMA. Regulatory actions may have negative effects on KMC and/or KOMA in various ways. If

regulatory action or changes in laws or regulations make it illegal to operate within that jurisdiction, the foundation, distributors (or their affiliated companies) may cease operations in that jurisdiction or be commercially unwanted to obtain the necessary regulatory approvals for operation within that jurisdiction. A cautious approach will be taken to the sale of KMC after extensive consultation with legal advisors and continuous analysis of the development and legal structure of the virtual currency. Therefore, for the token sale, the sales strategy may be constantly adjusted to minimize related legal risks. For the sale of KMC, a cautious approach will be taken. Therefore, for the token sale, the sales strategy may be constantly adjusted to minimize related legal risks. For the token sale, the foundation and distributors are working with Tzedek Law LLC, a boutique law firm in Hong Kong with a good reputation in the blockchain field.

8.2 Insufficient information disclosure: As of the publication of this paper, KOMA is still in the development phase, and its design concepts, consensus mechanisms, algorithms, codes, as well as

other technical details and parameters may be constantly updated and revised. Although this white paper contains the latest information about the KOMA network, it is not absolutely complete and may still be adjusted and updated from time to time by the KOMA development team. The KOMA development team is not able and is not obligated to inform KMC holders of every detail of the project regarding the development of the KOMA network (including development progress and expected milestones). Therefore, insufficient information disclosure is inevitable and reasonable.

8.3 Competitors: Various types of decentralized applications are rapidly emerging, and industry competition is becoming increasingly fierce. It is possible to establish alternative networks that use the same or similar code and protocols using KMC and/or KOMA and attempt to recreate similar facilities. KOMA network may have to compete with these alternative networks, which may have negative effects on KMC and/or KOMA network.

8.4 Failure to develop: the development of KOMA network may not be executed as planned due to various reasons, including but

not limited to events such as the decline in the prices of any digital assets, virtual currencies or KOMA, unforeseen technological difficulties, and a shortage of development funding.

8.5 Security vulnerabilities: Hackers or other malicious organizations or entities may interfere with KMC and/or KOMA in various ways, including but not limited to malware attacks, denial-of-service attacks, consensus-based attacks, Sybil attacks, smurfing, and deception. Additionally, there is a risk that third-party or Foundation members, distributors, or their affiliates may intentionally or unintentionally introduce weaknesses into the core infrastructure of KMC and/or KOMA, which may have negative effects on KMC or KOMA. Furthermore, the future of cryptography and security innovation is highly unpredictable, and advancements in cryptography or technologies (including but not limited to the development of quantum computing) may pose a risk.

8.6 Other risks: Additionally, the potential risks briefly mentioned above are not exhaustive, and there may be other risks associated with your purchase, holding, and use of KMC (as further

specified in the terms and conditions) that distributors cannot foresee. These risks may further manifest as unforeseen variations or combinations of the above risks. You should conduct comprehensive due diligence on the Foundation, distributors, their affiliates, and the KOMA development team and understand the overall framework, mission, and vision of KOMA before purchasing KMC.

Attachment A：Independence (with no affiliation to stakeholders)

This standard applies to independent members of the Strategic Decision Committee and Advisory Committee.

Members who meet the relevant selection criteria for independence and meet all of the following classification criteria should be considered as "independent members":

The member and their immediate family members do not serve as partners, significant stakeholders, or executives of any stakeholders of the Foundation.

The member and their immediate family members do not hold large amounts of KMC. The KMC holder referred to under this standard should be an important KMC holder.

The member and their immediate family members do not serve as executives of the Foundation.

Immediate family members referred to in the above criteria include spouses, parents, children, siblings, in-laws, children’ s

spouses, stepchildren, siblings' spouses, and any cohabiting individuals (excluding domestic service personnel).

In addition, in assessing independence, the Strategic Decision Committee will also consider other relevant facts and circumstances.

Attachment B：REFERENCES

[1] V. Buterin. A next generation smart contract & decentralized application platform (Ethereum white paper), 2014.

[2] G Wood. Ethereum: A secure decentralised generalised transaction ledger (Ethereum yellow paper), 2014.

[3] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system, 2008.

[4] POA Network. Proof of Authority: consensus model with identity at stake, Medium (https://medium.com/), 2017.

[5] M. Castro and B. Liskov. Practical Byzantine fault tolerance, in the Proceedings of the Third Symposium on Operating Systems and Implementation, 1999.

[6] POS Network. PROOF-OF-STAKE: Proof-of-stake underlies certain consensus mechanisms used by blockchains to achieve distributed consensus., Ethereum (https://ethereum.org/), 2023.