KADEMLIA

WHITE PAPER

01

Project Introduction

KAD platform chain (KADSEA Chain will be referred to as KAD Chain later) is to build the most convenient public chain platform that integrates high speed, low cost and large capacity. Our vision is to create an ecosystem that is compatible with all Ethereum Virtual Machines (EVM) and provide users with a seamless development and interaction experience. By enabling efficient transaction speeds and low transaction costs, we are committed to making blockchain technology a more accessible and applicable tool to meet the growing digital needs around the world.

Our public chain is not only a chain connecting the digital world, but also a bridge to the Web 3.0 world. It aims to provide users with broader development space and richer innovation possibilities by connecting the real world and the world on the chain. . We strive to break traditional digital boundaries, promote the development of the digital economy, create more value for users, and build a more open, secure, and efficient digital future.

02

Design Principles

KADChain design follows the following principles

01 | Independent blockchain

Technically, KAD is an independent blockchain and not a Layer 2 solution. Most of KAD's basic technologies and business functions are independent, and KAD operations are not affected by any other public chains.

02 | Ethereum compatible

The first practical, widely used smart contract platform was Ethereum. In order to connect with relatively mature applications and communities, KAD chose to be compatible with the existing Ethereum mainnet. This means that most DApps, ecosystem components and tools will be compatible with KAD without modification or only minor changes; KAD nodes only require similar, or slightly higher hardware specifications and operational skills to operate. This implementation should provide room for continued compatibility between KAD and future versions of Ethereum.

03 | Hybrid consensus mechanism KPoS (Hybrid consensus of PoA and PoS)

The consensus based on the hybrid consensus of PoA and PoS is more environmentally friendly and provides a more flexible choice for community governance. It can be expected that this consensus will have better performance than the PoW consensus, that is, the block generation time is short and the transaction processing capacity is high.

04 | Cross-chain

Our public chain is committed to supporting the comprehensive application of cross-chain technology to achieve interoperability and seamless connections between different blockchain networks. By adopting secure cross-chain technology, we are committed to building an open ecosystem, providing users with more choices and flexibility, and promoting the flow of assets and data between different blockchains, thereby enabling wider application scenarios and more Rich functional experience.

05 | community autonomy

Establish an open, inclusive, and democratic community culture, encourage community members to actively participate and contribute, promote the innovation and development of the public chain ecosystem, promote communication and cooperation among community members, and jointly create a prosperous and healthy public chain ecosystem. Through community autonomy, public chain communities can better respond to challenges, seize opportunities, and promote the long-term sustainable development of the public chain ecology.

Hybrid consensus mechanism KPoS (hybrid consensus of PoA and PoS)

The hybrid consensus mechanism KPoS (hybrid consensus of PoA and PoS) is a blockchain consensus algorithm that introduces the concept of trustee (representative) based on proof of stake (POS). The following are some advantages of the KPOS consensus algorithm:

- High performance and fast confirmations: KPOS generally has fast block generation times, typically a few seconds. This results in faster transaction confirmations, increasing the throughput of the entire blockchain network.
- Relatively high degree of decentralization: KPOS allows users to elect representatives to generate blocks and verify transactions. This mechanism can increase the censorship resistance and decentralization of the network to a certain extent through decentralization.

● Low energy consumption: Compared with the proof-of-work (POW) algorithm, KPOS has lower energy consumption. Since only a small group of representatives has the authority to generate blocks, rather than competing to solve mathematical problems, the entire network consumes less electricity.

● Voting rights: In KPOS, users with more rights have more voting rights and can choose the trustee of the network. This encourages users to actively participate in the governance of the network.

● Real-time governance: KPOS can respond to network changes more quickly through real-time election of representatives. If users are dissatisfied with a representative's performance, they can quickly replace it by voting.

● High fault tolerance: KPOS systems are usually highly fault tolerant to failures or malicious behaviors of a small number of representatives. Even if there is a problem with one representative, other representatives can still continue the operation of the network.

● Incentivize trustees to provide stable services: Representatives receive rewards by providing efficient and stable network services. This incentive mechanism helps maintain the stability and security of the network.

03

Validator node quorum

During the genesis block phase of network launch, a number of trusted nodes will operate as the initial set of validators. After the block production begins, anyone can participate as a candidate in the election of validators. The stake pledge status determines that the top 21 nodes with the most stake pledges will become the next set of validators. Such election and elimination are carried out by voting on the Security Council proposal.

KAD is the token for KAD equity pledge.

In order to maintain compatibility with the Ethereum consensus protocol (including upcoming upgrades), the KAD chain adds staking management (see the “Staking and Management” section below). There is a module dedicated to KAD equity staking on the KAD chain. It will accept KAD stakes from KAD holders and calculate the set of nodes with the largest stakes. Every time UTC reaches zero, its validator set is updated.

Before generating new blocks, existing KAD validators regularly check for updates. If so, they will update the validator set after a certain height (i.e. a predefined block interval). For example, if KAD generates a block every 3 seconds and the check period is 200 blocks, then the current validator set will check and update the validator set for the next period in 600 seconds (200 blocks).

04

safety and finality

Considering that more than half of the ½*N+1 validators are honest and trustworthy, PoA-based networks can generally work safely and properly. However, in some cases, Byzantine validators may still manage to attack the network, such as through a "clone attack." In order to ensure the security of the KAD chain, we encourage KAD users to wait until the received block is confirmed by more than ⅔* N+1 different validators. In this way, less than 1/3 N of Byzantine validators can be tolerated.

*For 21 validators, if the block time is 3 seconds, then⅔*N + 1 different validators will take (2/3*21 + 1)*3 =45 seconds to confirm. Any significant application of KAD will probably have to wait ⅔****N+1 to ensure a relatively safe end result. However, in addition to such an arrangement, KAD also introduces a penalty mechanism to penalize Byzantine validators for double-signing or instability, which will be described later in the “Staking and Management” section. This penalty mechanism will expose malicious validators in a very short period of time and make "clone attacks" very difficult to execute or very uneconomical even if executed. Through this penalty mechanism, ½*N + 1 or even fewer blocks are enough to meet the finality of most transactions.

05

safety and finality

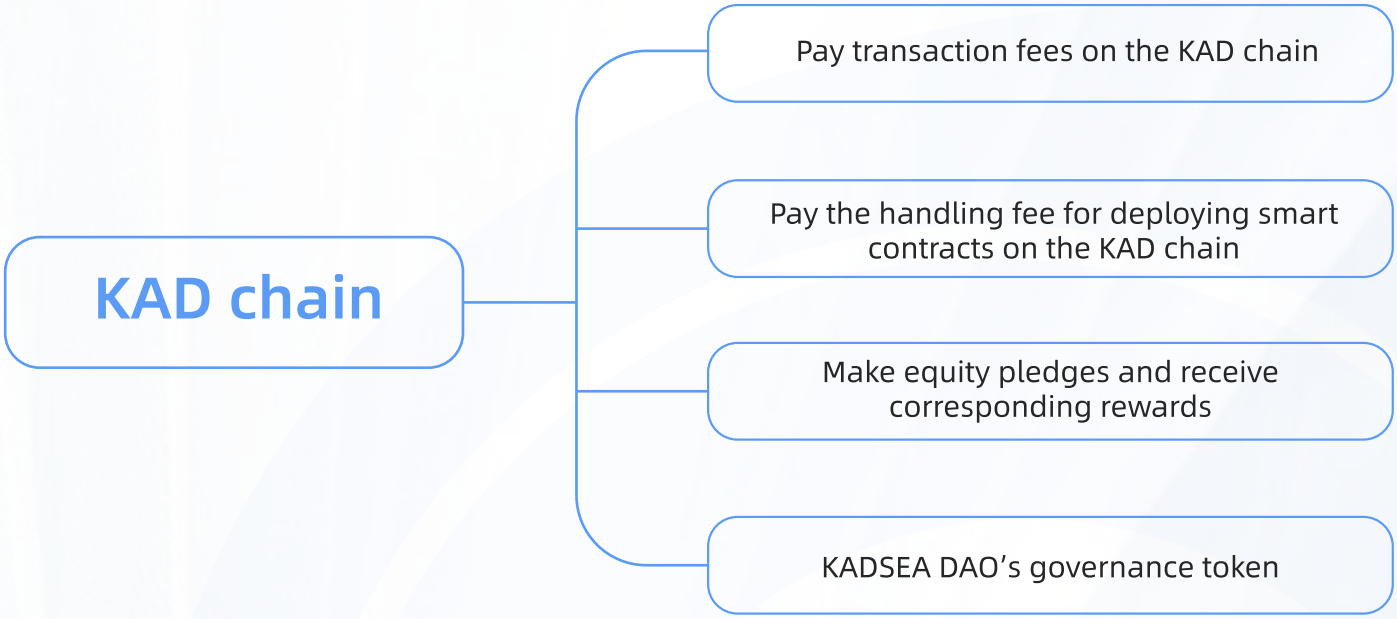
All KAD validators in the current validator set will receive income from the handling fees paid in KAD and the block output KAD. Since KAD is also its governance token, delegators and validators will still receive the other benefits of holding KAD.

The income of the validator is obtained from the handling fees and block rewards collected from the transactions of each block. Validators can decide how much revenue to share with delegators who have pledged KAD to attract more pledged investments. Each validator will take turns generating blocks with the same probability (if they remain 100% online), but the rewards are distributed based on the amount staked by each validator node. Therefore, the size of the pledged assets of each validator may be different, and validators with higher quality may obtain more benefits. Therefore, as long as the validator remains trustworthy (untrusted validators can bring great risks), it is consistent for rational delegators to get rewards for staking on any validator node.

06

Tokenomics

KAD runs on the KAD chain in the same way that ETH runs on Ethereum, so it is the "native token" of the KAD chain. This means that KAD can be used on the KAD chain for:



07

Issued

In the initial stage, 1% of KAD will be put on the market through IEO. Most of the remaining KAD will be used to promote the ecological development of the KAD public chain through mining and foundations. Tokens are distributed as follows:

Allocation	Quantity	Proportion	Describe
Mining output	548 million pieces	54.80%	The monthly growth is 12% of the original base (circulation volume). The monthly growth is 9% of the original base in 6 months. The monthly growth is 7% of the original base in 18 months. The monthly growth is 5% of the original base in 30 months. The monthly growth is 48 months. 3% of the original base while stocks last. Example: In the first month (first stage), the additional issuance ratio is 12%, and the circulation is 10 million. Then the additional issuance of the entire network in the first month = 10 million x 12% = 1.2 million; the additional issuance of the entire network in the second month = 1120 In the first month, 1.2 million is produced every day/30 days. 1.2 million is produced per block/30 days/number of blocks produced on the day is calculated. Circulation calculation: 1 billion - the currency holding power mining is not produced - the following few The number of coins held by each wallet address
public offering	100 million pieces	10%	It is allocated to the initial investors and is dynamically released based on NFT rules.
foundation	300 million pieces	30%	For the operation and development of the KAD Foundation
Technical lock-in	1 million pieces	0.10%	Assigned to the core technical team, it will begin to be unlocked after one year, and 5% will be released every month, and will be released in 20 months.
Operation lock-up	1 million pieces	0.10%	Assigned to the core technical team, it will begin to be unlocked after one year, and 5% will be released every month, and will be released in 20 months.
angel wheel	10 million pieces	1%	allocated to initial investors
Ranking incentives	40 million pieces	4%	allocated to early investors and contributors involved in the project.

08

Other tokens

The KRC20 tokens used by the KAD public chain are native assets that can be quickly traded and confirmed, can be circulated, and can be traded on DEX after being listed. At the same time, since KAD is Ethereum compatible, supporting ERC20 contracts on KAD is called "KRC20". KRC20 "enhances" existing protocols by adding more methods that expose more information, such as token units and precision.

09

Equity pledge and on-chain governance

KPOS realizes decentralized community governance. You can see similar ideas from other networks, notably Cosmos and EOS. Its core logic can be summarized as follows.

- Token holders, including validators, can “lock” their tokens into staking. Token holders can delegate their tokens to any validator or a validator candidate. They can then reselect a different validator or candidate to delegate their tokens to.
- All validator candidates will be ranked by the number of delegated tokens they have received, and the top ones will become the real validators.
- Validators can share block rewards with their delegators.
- Validators may suffer “penalty rates,” which are penalties for their bad behavior, such as double-signing and/or instability.
- There is an “unbinding period” between validators and delegators. When malicious Byzantine behavior is discovered, the tokens remain locked for a certain period of time, and the perpetrators will be punished promptly.

Equity pledge

Ideally, such staking and reward issuance logic should be included in the blockchain and executed automatically when new blocks are produced.

Since the day of design, we have completed KAD's equity pledge logic on the KAD chain:

KAD'S RIGHTS AND INTERESTS PLEDGE LOGIC

1. The staking token is KAD because it is the native token on the blockchain.
2. Record KAD's equity pledge and entrustment behavior on the KAD chain.
3. KAD's validator set is determined by its stake pledge and delegation logic.
4. Reward distribution on the KAD chain occurs when each block is produced.

Verification node (validator)

- Verification nodes are generated by the top 21 nodes in terms of pledge amount and are responsible for creating and verifying blocks.
- Validation nodes earn the trust of voters by providing computing power, network stability, and community participation.
- Verification nodes can obtain handling fees & block rewards.
- You must run a complete verification node and stake at least 3,000 KAD to participate in the verification node election.

Token holders

- Token holders participate in KPoS network mining by holding a certain number of tokens and staking them on verification nodes or participating in candidate node election and staking verification nodes.

- Token staking users can receive handling fees and block rewards.

Punishment rules

OFFLINE PUNISH

If the verification node fails to produce blocks normally or participate in the network consensus within 5 minutes, and it occurs for the first time within a month, 100KAD will be deducted from the verification node as a penalty, 500KAD will be deducted for the second time, 1000KAD will be deducted for the third time, and 2000KAD will be deducted for the 4th time. For example, 5 times, the node will be punished to exit the verification node.

MALICIOUS BEHAVIOR PUNISH

If a node is found to have participated in malicious behavior, such as double spending, attacking other nodes, etc., the system may severely punish it, directly disable the node, and confiscate all verification node pledge tokens.

LOW PERFORMANCE NODE PENALTY

If a node produces blocks slowly and has low efficiency, the verification node will be eliminated directly.

double signature

It is a serious act of evil when a validator intentionally signs multiple blocks of the same height and with the same parent block. Implementations of protocols should already take into account how to prevent this from happening, so only malicious code can trigger this. When a double signature occurs, the validator should be immediately removed from the validator set.

instability

The availability of the KAD chain relies on each validator in the validator set in the KPOS consensus to be able to generate blocks in time when it is their turn to generate blocks. A validator may miss the opportunity to produce a block for a number of reasons, especially due to hardware, software, configuration or network issues. This unstable operation will harm the performance of the network and bring more uncertainty to the system.

KAD has an internal contract that is responsible for recording the blocks missed by each validator. Once this metric exceeds a predefined threshold, a portion of the validator's staked assets will be forfeited. In this way, poorly performing validators will gradually exit because they are punished too many times and will be forced out of the validator status.

Parameter management

There are many system parameters to control the behavior of KAD, such as penalty interest threshold, quantity, etc. All these parameters will be determined by KAD validators through the proposal voting process. This process will take place on the KAD chain.

Bug bounty program

- Reward scope: This bug bounty program applies to all components and related applications of our public chain network, including but not limited to smart contracts, wallet applications, node software, blockchain browsers, etc.

● Reward Levels: Rewards will be assessed based on the severity and scope of the vulnerability. We will provide corresponding rewards according to the following levels:

● Reward amount: The foundation will announce the vulnerability reward amount for this quarter based on project status every quarter. Technicians who report vulnerabilities this quarter will share the rewards based on quantity, severity and other dimensions.

- Reporting method: Security researchers can submit vulnerability reports through our designated vulnerability reporting channels. We encourage the submission of specific reports, including vulnerability description, reproduction steps, vulnerability impact analysis and recommended remediation measures.

- Assessment process: Our security team will evaluate the received vulnerability reports and communicate with the submitter after confirming the validity of the vulnerability to further verify and fix the vulnerability. Once the vulnerability is confirmed and fixed, we will pay the corresponding reward in a timely manner.

Performance

1. Transaction speed: KAD has fast transaction processing capabilities, and its average confirmation time is usually around 3 seconds. This means users can complete transactions quickly and have their validity confirmed within a short period of time.

2. Low cost: KAD's transaction fees are usually low, allowing users to conduct transactions and transfers at a lower cost. One transaction is about 0.000021KAD (ps: the more transactions on the chain, the more GAS fees will increase). This low-cost feature helps promote more transaction activities and asset flows, providing users with a more cost-effective blockchain application experience.

3. High throughput: KAD has high throughput capabilities and can handle a large number of transactions and data transfers simultaneously. This enables KAD to support complex smart contracts and large-scale data processing to meet the needs of different application scenarios.

4. Smart contract compatibility: KAD is compatible with the Ethereum Virtual Machine (EVM), allowing developers to easily migrate their Ethereum smart contracts to run on KAD. This compatibility helps developers build rich and diverse smart contract applications on KAD and expands the application scenarios and functions of the KAD ecosystem.

5. Cross-chain bridging capabilities: KAD has good cross-chain bridging capabilities and can connect different blockchain networks to achieve cross-chain transfer and exchange of assets and data. This capability helps promote the interoperability of KAD with other blockchain networks and expands the application scope and user base of the KAD ecosystem.

Expansion plan

ECOLOGY DIVERSIFICATION

KAD will continue to promote ecological diversification and expand more application scenarios and functional modules. By attracting more developers and project parties to join the KAD ecosystem, and introducing more decentralized applications (DApps) and digital assets, we will provide users with more diverse blockchain application choices.

DEVELOPER SUPPORT

KAD will increase its support for developers and provide more developer tools and resources, including development documents, technical guides, SDKs, etc., to help developers more easily build and deploy KAD-based blockchain applications. At the same time, KAD will actively support and promote more developer community activities and technical exchange activities to promote communication and cooperation among developers.

SAFETY AND STABILITY

KAD will continue to strengthen the security and stability of the network, constantly improve the network's security mechanisms and protective measures, and ensure the security of user assets and data. KAD will strengthen the security audit and monitoring of smart contracts and blockchain nodes, improve the network's attack resistance and fault tolerance, and ensure the stable operation of the network.

CROSS-CHAIN INTEROPERABILITY

KAD will actively promote connections and cooperation with other blockchain networks, establish more cross-chain bridges, promote asset and data interoperability between different blockchain networks, and expand the application scope and user base of the KAD ecosystem. KAD will continue to explore and practice cross-chain technology to improve KAD’s competitive advantages and status in the cross-chain field.

COMMUNITY CONSTRUCTION

KAD will strengthen community building and enhance community participation and cohesion. KAD will strengthen training and guidance for community members, encourage more community members to participate in KAD's governance and decision-making, and jointly promote the development and growth of the KAD ecosystem. At the same time, KAD will actively carry out more community activities and publicity and promotion to enhance KAD's visibility and influence, and expand KAD's user group and user base.

Network congestion solution

1. Improve capacity and throughput: Optimize the architecture and design of the blockchain network and increase the capacity and throughput of the blockchain to support more transactions and data processing. This can be achieved by increasing the block size, optimizing the transaction confirmation mechanism, and introducing sharding technology.

2. Optimize the transaction fee mechanism: Adjust the transaction fee mechanism of the blockchain, set transaction fees reasonably according to the importance and urgency of the transaction, encourage users to choose reasonable transaction fees, and reduce transaction congestion. The transaction fee mechanism can be optimized by dynamically adjusting transaction fees and providing preferential policies for transaction fees.

3. Use distributed storage and computing: Distribute the storage and computing of the blockchain to different nodes and servers to achieve distributed storage and computing and improve the scalability and fault tolerance of the blockchain. Distributed storage and computing can reduce the pressure on a single node and improve the stability and performance of the overall network.

4. Strengthen network security and privacy protection: Strengthen the security protection measures of the blockchain network, including encryption algorithms, identity authentication mechanisms, privacy protection technologies, etc., to prevent malicious attacks and data leaks, and ensure the security and stable operation of the blockchain network.

Application scenarios

The KAD public chain can find a wide range of applications in many different fields. The following are some specific application scenarios:

- Decentralized Finance (DeFi): The KAD public chain provides a framework for building decentralized financial services, such as lending protocols, decentralized exchanges (DEX), stable coins, etc.

- Digital ownership and transactions: Through smart contracts, the EVM public chain can be used to create and trade digital assets, including tokens, artworks, real estate, etc. NFTs (non-fungible tokens) are an important case, and they have significant room for innovation in the fields of digital art and games.

- Supply chain management: The KAD public chain can be used to track transactions and logistics information in the product supply chain to ensure transparency and traceability. Smart contracts can ensure compliance of all parties in the supply chain and reduce fraud and errors.

- Governance and voting: Using smart contracts and token mechanisms, the KAD public chain can be used to implement transparent community governance and voting mechanisms. This mechanism can be used in democratic organizations, corporate governance, and community decision-making.

- Games and virtual worlds: KAD public chain provides developers with a platform to build blockchain-based games and virtual worlds. These applications can leverage smart contracts and cryptoeconomics to create unique gameplay and economic models.

- Authentication and data security: The KAD public chain can be used to build secure authentication systems and data storage solutions. Through the immutability and encryption technology of blockchain, the security and privacy of user data can be ensured.

These are just some examples of KAD public chain applications. In fact, its application fields are very wide, covering many industries such as finance, supply chain, games, social networks, and medical care. With the continuous development of blockchain technology, it is expected that more innovative application scenarios will be implemented on the KAD public chain.