RIKEZA WHITEPAPER

RIKEZA (RIK): A decentralized crypto asset driven by a high-performance blockchain.

Abstract

RIKEZA (RIK) is a decentralized, peer-to-peer (P2P) digital asset and payment network supported by an open-source blockchain protocol that enables instant, near-zero cost transfer to anyone in the world. It is a modern alternative to Bitcoin for mass adoption and aims to evolve as a foundation of a new, global digital crypto-based economic system with greater community participation.Derived from the principles of distributed ledger technology, members of this system may securely transfer, transact, accumulate and trade RIKEZA (RIK) for the benefit of themselves and the entire community. Rikeza works on POA protocol rather than POS or POW which makes it faster and more efficient.

NEXT GENERATION SMART CONTRACTS AND DECENTRALIZED APPLICATION PLATFORM

Development of Bitcoin in 2009 by Satoshi Nakamoto has often been hailed as a revolutionary development in money and currency, being the first example of a digital asset which simultaneously has no backing or "intrinsic value" and no centralized issuer or controller.The currency was introduced as an open-source software project and quickly gained popularity as a new form of decentralized currency that operates without intermediaries or government control. In 2010, the first Bitcoin transaction for a tangible item took place, and since then, Bitcoin has become a major player in the world of digital currencies, inspiring the development of numerous other cryptocurrencies and blockchain-based technologies. The underlying technology of Bitcoin is called blockchain, which is a decentralized and distributed ledger that records transactions across a network of computers. The blockchain is maintained by a network of nodes, which validate and add new transactions to the chain. The technology is designed to be secure and tamper-proof, as it uses cryptographic algorithms to ensure that once data is entered into the blockchain, it cannot be altered or deleted. Each block in the blockchain contains a cryptographic hash of the previous block, creating a chain that links all blocks together. This ensures that the entire history of all transactions on the blockchain is transparent and publicly available, providing an unalterable record of all transactions. This makes blockchain an attractive technology for a variety of applications, including financial transactions, supply chain management, and secure data storage.Blockchain technology has numerous potential uses beyond its original application as the underlying technology for cryptocurrencies like Bitcoin. Its decentralized, secure, and transparent nature make it ideal for various industries and applications that require a secure and tamper-proof method of record-

keeping. This includes financial services, such as cross-border payments, remittances, and settlement systems. In the supply chain management industry, blockchain can be used to improve transparency and traceability of goods as they move through the supply chain. It can also be used in voting systems, as it provides a secure and transparent method for recording and counting votes. Additionally, blockchain technology has the potential to revolutionize the way personal identity and medical records are managed, providing a secure and tamper-proof method for storing and sharing sensitive information. These are just a few of the many potential uses of blockchain technology, which is still in its early stages of development and is likely to lead to the creation of many new and innovative applications in the coming years.

Rikeza intends to provide a blockchain with an in-built fully fledged programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code.

INTRODUCTION OF BITCOIN

Bitcoin uses blockchain technology to maintain a public ledger of all transactions, providing a secure and tamper-proof record of all transfers. Unlike traditional currencies, Bitcoin has a finite supply, with only 21 million bitcoins ever to be produced. Bitcoin has gained popularity and recognition as a new form of currency and has inspired the development of numerous other cryptocurrencies. Despite some initial skepticism and concerns about its use, Bitcoin has become a major player in the world of digital currencies, with millions of people around the world using it for transactions, investment, and as a store of value. Bitcoin are digital assets whose owenership is recorded on an electronic ledger that is updated almost simultaneously on about 10,000 independently operated computers around the world that are connected with each other. This ledger is called bitcoin's blockchain. Transactions that record transfer of owenership of those coins are created and validated according to a protocol i.e a list of rules. The protocol is implemented by software-an app- that participants run on their computers. The machines running the apps are called 'nodes of the network'. Each node independently validates all pending transactions wherever they arise, and updates it's own record of the ledger with validated blocks of confirmed transactions. Specialist nodes, called miners, bundle together valid transactions into blocks and distribute those blocks to nodes across the network. Every Bitcoin transaction is recorded and shared publicly in plain text on Bitcoin's blockchain.

HOW DOES BITCOIN WORK?

Bitcoin works on a decentralized and distributed network of computers, using cryptography to secure and validate transactions. When a user wants to make a transaction, they broadcast a request to the network, which is verified by network nodes through a consensus mechanism. Once a transaction is verified, it is added to a block, along with other transactions, forming a block in the blockchain. The block is then added to the existing blockchain through a process called mining, where specialized computers compete to solve a cryptographic puzzle and the first to do so is rewarded with new bitcoins and the transaction fees for the block. This process ensures that all transactions are verified and added to the blockchain in a secure and tamper-proof manner. The decentralized nature of the network ensures that there is no central authority controlling the currency, making it a truly peer-to-peer system. The transparency of the blockchain allows for all transactions to be publicly auditable, providing a secure and transparent record of all transfers.

The Bitcoin blockchain is managed by software running on computers that communicate with each other forming a network. The most commonly used software is called 'Bitcoin core' and source code to this software is published on GitHub .This software contains a full range of functionalities needed for the network to exist.

The objective behind Bitcoin was to create an electronic payment system that cannot be censored,and to allow anyone the ability to send payments directly from one party to another without going through a 'financial institution'. Bitcoin works on proof-of-work protocol.The mechanism behind proof-of-work was a breakthrough in the space because it simultaneously solved two problems. First, it provided a simple and moderately effective consensus algorithm, allowing nodes in the network to collectively agree on a set of canonical updates to the state of the Bitcoin ledger. Second, it provided a mechanism for allowing free entry into the consensus process, solving the political problem of deciding who gets to influence the consensus, while simultaneously preventing sybil attacks. It does this by substituting a formal barrier to participation, such as the requirement to be registered as a unique entity on a particular list, with an economic barrier - the weight of a single node in the consensus voting process is directly proportional to the computing power that the node brings. Since then, an alternative approach has been proposed called proof-of-stake, calculating the weight of a node as being proportional to its currency holdings and not computational resources; the discussion of the relative merits of the two approaches is beyond the scope of this paper but it should be noted that both approaches can be used to serve as the backbone of a cryptocurrency.

WHY RIKEZA?

Decentralized apps are being proposed in large numbers, but the current blockchain ecosystem is not prepared to match the demands of end user applications with mass adoption. Slow block confirmations, high transaction fees, low scalability and poor user experience are some of the roadblocks for the mass adoption of blockchain applications.

DESIGN PRINCIPLE OF RIKEZA

Parallel blockchain into the RIK ecosystem is created which runs side by side to provide different services. The new parallel chain will be called " RIK smart chain" while the existing mainet will be named " Ethereum chain".

Here are the design principles of RIK:

.Ethereum Compatibility: The first practical and widely-used Smart Contract platform is Ethereum. To take advantage of the relatively mature applications and community, RIK chooses to be compatible with the existing Ethereum mainnet. This means most of the dApps, ecosystem components, and toolings will work with RIK and require zero or minimum changes; RIK node will require similar (or a bit higher) hardware specification and skills to run and operate. The implementation should leave room for RIK to catch up with further Ethereum upgrades.

.Native Cross-Chain Communication: RIK will be implemented with native support for cross-chain communication among the two blockchains. The communication protocol should be bi-directional, decentralized, and trustless. It will concentrate on moving digital assets between RIK, i.e., RIK2, RIK22 tokens, and eventually, other RIK tokens introduced later. The protocol should care for the minimum of other items stored in the state of the blockchains, with only a few exceptions.

Consensus and Validator Quorum

Based on the above design principles, the consensus protocol of RIK is to fulfill the following goals:

- Blocking time should be shorter than Ethereum network, e.g. 3 seconds or even shorter.
- It requires limited time to confirm the finality of transactions, e.g. around 5 seconds level or shorter.
- There is no inflation of native token: RIK, the block reward is collected from transaction fees, and it will be paid in RIK.

- It is compatible with Ethereum system as much as possible.
- It allows modern proof-of-authority blockchain network governance.

Proof of Authority

Although Proof-of-Work (PoW) has been recognized as a practical mechanism to implement a decentralized network, it is not friendly to the environment and also requires a large size of participants to maintain the security.

Ethereum and some other blockchain networks, such as MATIC Bor, TOMO Chain , GO Chain, xDAI, do use proof-of-authority (POA) or its variants in different scenarios, including both testnet and mainnet. PoA provides some defense to 51% attack, with improved efficiency and tolerance to certain levels of Byzantine players (malicious or hacked). It serves as an easy choice to pick as the fundamentals.

Meanwhile, the PoA protocol is most criticized for being not as decentralized as PoW, as the validators, i.e. the nodes that take turns to produce blocks, have all the authorities and are prone to corruption and security attacks. Other blockchains, such as EOS and Lisk both, introduce different types of Delegated proof-of-stake to allow the token holders to vote and elect the validator set. It increases the decentralization and favors community governance.

RIK here proposes to combine DPoS and PoA for consensus, so that:

- Blocks are produced by a limited set of validators
- Validators take turns to produce blocks in a PoA manner, similar to " Ethereum's Clique" consensus design
- Validator set are elected in and out based on a staking based governance.

VALIDATOR QUORAM

In the genesis stage, a few trusted nodes will run as the initial Validator Set. After the blocking starts, anyone can compete to join as candidates to elect as a validator. The staking status decides the top 21 most staked nodes to be the next validator set, and such an election will repeat every 24 hours.

While producing further blocks, the existing RIK validators check whether there is a validator set update message relayed onto RIK periodically. If there is, they will update the validator set after an epoch period, i.e. a predefined number of blocking time. For example, if RIK produces a block every 5 seconds, and the epoch period is 240 blocks, then the current validator set will check and update the validator set for the next epoch in 1200 seconds (20 minutes).

SECURITY AND FINALITY

Given there are more than ½*N+1 validators are honest, PoA based networks usually work securely and properly. However, there are still cases where certain amount Byzantine validators may still manage to attack the network, e.g. through the "Clone Attack".To secure as much as Ethereum, RIK users are encouraged to wait until receiving blocks sealed by more than ⅔*N+1

different validators. In that way, the RIK can be trusted at a similar security level to BC and can tolerate less than ⅓*N Byzantine validators.

With 21 validators, if the block time is 3 seconds, the ⅔*N+1 different validator seals will need a time period of (⅔*21+1)*5 = 45 seconds. Any critical applications for RIK may have to wait for ⅔*N+1 to ensure a relatively secure finality. However, besides such arrangement, RIK does introduce Slashing logic to penalize Byzantine validators for double signing or inavailability, which will be covered in the “Staking and Governance” section later. This Slashing logic will expose the malicious validators in a very short time and make the “Clone Attack” very hard or extremely non-beneficial to execute. With this enhancement, ½*N+1 or even fewer blocks are enough as confirmation for most transactions.

REWARD

All the RIK validators in the current validator set will be rewarded with transaction fees in RIK. As RIK is not an inflationary token, there will be no mining rewards like Bitcoin and Ethereum network generate, and the gas fee is the major reward for validators. As RIK is also utility tokens with other use cases, delegators and validators will still enjoy other benefits of holding RIK.

The reward for validators is the fees collected from transactions in each block. Some parts of the gas fee will also be rewarded to relayers for Cross-Chain communication. Please refer to the "Relayers" section below.

TOKEN ECONOMY

RIK share the same token universe for RIK and RIK2 tokens. This defines:

- The same token can circulate on both networks, and flow between them bi-directionally via a cross-chain communication mechanism.
- The total circulation of the same token should be managed across the two networks, i.e. the total effective supply of a token should be the sum of the token’s total effective supply on both RIK and BC.
- The tokens can be initially created on RIK in a similar format as ERC20 token standard, or on BC as a RIK2, then created on the other. There are native ways on both networks to link the two and secure the total supply of the token.

NATIVE TOKEN

RIK will run on RIK in the same way as ETH runs on Ethereum so that it remains as “native token” for RIK . This means Rikeza DEX, RIK will be also used to:

- pay “fees“ to deploy smart contracts on RIK
- perform cross-chain operations, such as transfer token assets across RIK

OTHER TOKENS

One of the key features of Rikza is its support for a variety of different tokens, which can be used to represent different assets, from traditional financial instruments like stocks and bonds, to more unconventional assets like virtual real estate and collectibles.

Here are some of the most notable tokens that are supported by Rikza blockchain:

1.Utility Tokens: These tokens are used to access specific services or products within the Rikza ecosystem. For example, a token might be required to access a particular decentralized application (dApp) or to participate in a decentralized voting process.

2.Security Tokens: These tokens represent ownership in a company or asset, and typically provide the holder with certain rights, such as the ability to receive dividends or vote on important matters.

3.Stablecoins: These are digital assets designed to maintain a stable value, even in volatile market conditions. This makes them ideal for use as a medium of exchange, as they can be used to store and transfer value without being impacted by fluctuations in the value of other cryptocurrencies.

4.Asset-Backed Tokens: These tokens are backed by real-world assets, such as commodities, real estate, or even artwork. By tokenizing these assets, Rikza makes it possible to trade and manage them in a decentralized and secure manner.

5.Non-Fungible Tokens (NFTs): These are unique, one-of-a-kind tokens that represent a specific asset or piece of digital content. NFTs are becoming increasingly popular as a way to represent and trade everything from digital art and collectibles to virtual real estate.

TOKEN BINDING

RIK2 tokens will be extended to host a new attribute to associate the token with a RIK RIK2E token contract, called “Binder”, and this process of association is called “Token Binding”.

Token Binding can happen at any time after RIK2 and RIK2E are ready. The token owners of either RIK2 or RIK2E don’t need to bother about the Binding, until before they really want to use the tokens on different scenarios. Issuers can either create RIK2 first or RIK2E first, and they can be bound at a later time. Of course, it is encouraged for all the issuers of RIK2 and RIK2E to set the Binding up early after the issuance.

A typical procedure to bind the RIK2 and RIK2E will be like the below:

- Ensure both the RIK2 token and the RIK2E token both exist on each blockchain, with the same total supply. RIK2E should have 3 more methods than typical ERC20 token standard:
    - symbol(): get token symbol
    - decimals(): get the number of the token decimal digits

    - owner(): get RIK2E contract owner's address**.** This value should be initialized in the RIK2E contract constructor so that the further binding action can verify whether the action is from the RIK2E owner.
- Decide the initial circulation on both blockchains. Suppose the total supply is *S*, and the expected initial circulating supply on RIK is *K*, then the owner should lock S-K tokens to a system controlled address on RIK.
- Equivalently, *K* tokens is locked in the special contract on RIK, which handles major binding functions and is named as TokenHub. The issuer of the RIK2E token should lock the *K* amount of that token into TokenHub, resulting in *S-K* tokens to circulate on RIK. Thus the total circulation across 2 blockchains remains as *S*.
- The issuer of RIK2 token sends the bind transaction on RIK. Once the transaction is executed successfully after proper verification:
    - It transfers *S-K* tokens to a system-controlled address on RIK.
    - A cross-chain bind request package will be created, waiting for Relayers to relay.
- RIK Relayers will relay the cross-chain bind request package into TokenHub on RIK, and the corresponding request and information will be stored into the contract.
- The contract owner and only the owner can run a special method of TokenHub contract, Approve Bind, to verify the binding request to mark it as a success. It will confirm:
    - the token has not been bound;
    - the binding is for the proper symbol, with proper total supply and decimal information;
    - the proper lock are done on both networks;
- Once the Approve Bind method has succeeded, TokenHub will mark the two tokens are bounded and share the same circulation on RIK, and the status will be propagated back to RIK. After this final confirmation, the RIK2E contract address and decimals will be written onto the RIK2 token as a new attribute on RIK, and the tokens can be transferred across the two blockchains bidirectionally. If the ApproveBind fails, the failure event will also be propagated back to RIK to release the locked tokens, and the above steps can be re-tried later.

CROSS CHAIN TRANSFER AND COMMUNICATION

Cross-chain communication is the key foundation to allow the community to take advantage of the dual chain structure:

- users are free to create any tokenization, financial products, and digital assets on RIK
- the items on RIK can be manually and programmingly traded and circulated in a stable, high throughput, lighting fast and friendly environment of blockchain
- users can operate these in one UI and tooling ecosystem.

CROSS CHAIN TRANSFER

The cross-chain transfer is the key communication between the two blockchains. Essentially the logic is:

- the transfer-out blockchain will lock the amount from source owner addresses into a system controlled address/contracts;
- the transfer-in blockchain will unlock the amount from the system controlled address/contracts and send it to target addresses.

The cross-chain transfer package message should allow the RIK Relayers to verify:

- Enough amount of token assets are removed from the source address and locked into a system controlled addresses/contracts on the source blockchain. And this can be confirmed on the target blockchain.
- Proper amounts of token assets are released from a system controlled addresses/contracts and allocated into target addresses on the target blockchain. If this fails, it can be confirmed on source blockchain, so that the locked token can be released back (may deduct fees).
- The sum of the total circulation of the token assets across the 2 blockchains are not changed after this transfer action completes, no matter if the transfer succeeds or not.

CROSS-CHAIN USER EXPERIENCE

Ideally, users expect to use two parallel chains in the same way as they use one single chain. It requires more aggregated transaction types to be added onto the cross-chain communication to enable this, which will add great complexity, tight coupling, and maintenance burden. Here RIK only implement the basic operations to enable the value flow in the initial launch and leave most of the user experience work to client side UI, such as wallets. E.g. a great wallet may allow users to sell a token directly from RIK onto a DEX order book, in a secure way.

CROSS-CHAIN CONTRACT EVENT

Cross-Chain Contract Event (CCCE) is designed to allow a smart contract to trigger cross-chain transactions, directly through the contract code. This becomes possible based on:

- Standard system contracts can be provided to serve operations callable by general smart contracts;
- Standard events can be emitted by the standard contracts;
- Oracle Relayers can capture the standard events, and trigger the corresponding cross-chain operations;
- Dedicated, code-managed address (account) can be created on Blockchain and accessed by the contracts on the RIK, here it is named as **“Contract Address on Blockchain”** .

There are some details for the Trade Out:

- both can have a limit price (absolute or relative) for the trade;

- the end result will be written as cross-chain packages to relay back to RIK;
- cross-chain communication fees may be charged from the asset transferred back to RIK;
- RIK contract maintains a mirror of the balance and outstanding orders on CAoB. No matter what error happens during the Trade Out, the final status will be propagated back to the originating contract and clear its internal state.

With the above features, it simply adds the cross-chain transfer and exchange functions with high liquidity onto all the smart contracts on RIK. It will greatly add the application scenarios on Smart Contract and dApps, and make 1 chain +1 chain > 2 chains.

REWARDING

Both the validator update and reward distribution happen every day around UTC 00:00. This is to save the cost of frequent staking updates and block reward distribution. This cost can be significant, as the blocking reward is collected on RIK and distributed on Blockchain to RIK validators and delegator.

A deliberate delay is introduced here to make sure the distribution is fair:

- The blocking reward will not be sent to validator right away, instead, they will be distributed and accumulated on a contract;
- Upon receiving the validator set update into RIK, it will trigger a few cross-chain transfers to transfer the reward to custody addresses on the corresponding validators. The custody addresses are owned by the system so that the reward cannot be spent until the promised distribution to delegators happens.
- In order to make the synchronization simpler and allocate time to accommodate slashing, the reward for N day will be only distributed in N+2 days. After the delegators get the reward, the left will be transferred to validators' own reward addresses.

SLASHING

Slashing is part of the on-chain governance, to ensure the malicious or negative behaviors are punished. RIK slash can be submitted by anyone. The transaction submission requires 'Slash evidence' and cost fees but also brings a larger reward when it is successful.

So far there are two slashable cases.

Double Sign

It is quite a serious error and very likely deliberate offense when a validator signs more than one block with the same height and parent block. The reference protocol implementation should already have logic to prevent this, so only the malicious code can trigger this. When Double Sign happens, the validator should be removed from the Validator set right away.

Anyone can submit a slash request on blockchain with the evidence of Double Sign of RIK, which should contain the 2 block headers with the same height and parent block, sealed by the offending validator. Upon receiving the evidence, if the blockchain verifies it to be valid:

- The validator will be removed from validator set by an instance RIK validator set update Cross-Chain update;

- A predefined amount of RIK would be slashed from the self-delegated
- RIK of the validator; Both validator and its delegators will not receive the staking rewards.
- Part of the slashed RIK will allocate to the submitter’s address, which is a reward and larger than the cost of submitting slash request transaction
- The rest of the slashed RIK will allocate to the other validators’ custody addresses, and distributed to all delegators in the same way as blocking reward.

Governance Parameters

There are many system parameters to control the behavior of the RIK, e.g. slash amount, cross-chain transfer fees. All these parameters will be determined by RIK Validator Set together through a proposal-vote process based on their staking. Such the process will be carried on BC, and the new parameter values will be picked up by corresponding system contracts via a cross-chain communication.

RELAYERS

Relayers are responsible to submit Cross-Chain Communication Packages between the two blockchains. Due to the heterogeneous parallel chain structure, two different types of Relayers are created.

RIK RELAYERS

Relayers for Blockchain to RIK communication referred to as “**RIK Relayers**”, or just simply “Relayers”. Relayer is a standalone process that can be run by anyone, and anywhere, except that Relayers must register themselves onto RIK and deposit a certain refundable amount of RIK. Only relaying requests from the registered Relayers will be accepted by RIK.

The package they relay will be verified by the on-chain light client on RIK. The successful relay needs to pass enough verification and costs gas fees on RIK, and thus there should be incentive reward to encourage the community to run Relayers.

Incentives

There are two major communication types:

- Users triggered Operations, such as token bind or cross chain transfer. Users must pay additional fee to as relayer reward. The reward will be shared with the relayers who sync the referenced blockchain headers. Besides, the reward won't be paid the relayers' accounts directly. A reward distribution mechanism will be brought in to avoid monopolization.
- System Synchronization, such as delivering refund packages, special blockchain header synchronization,RIK staking package. System reward contract will pay reward to relayers' accounts directly.

If some Relayers have faster networks and better hardware, they can monopolize all the package relaying and leave no reward to others. Thus fewer participants will join for relaying, which encourages centralization and harms the efficiency and security of the network. Ideally,

due to the decentralization and dynamic re-election of RIK validators, one Relayer can hardly be always the first to relay every message. But in order to avoid the monopolization further, the rewarding economy is also specially designed to minimize such chance:

- The reward for Relayers will be only distributed in batches, and one batch will cover a number of successful relayed packages.
- The reward a Relayer can get from a batch distribution is not linearly in proportion to their number of successful relayed packages. Instead, except the first a few relays, the more a Relayer relays during a batch period, the less reward it will collect.

What is Proof-of-Authority

Proof of Authority (PoA) is a consensus algorithm used in blockchain networks. It was first introduced in 2017 by Gavin Wood, co-founder of Ethereum and founder of Parity Technologies. The idea behind PoA is to address some of the drawbacks of the Proof of Work (PoW) consensus algorithm, such as its high energy consumption.

In a PoA system, validators are selected based on their identity and reputation, rather than their computational power. These validators are known as "authorities," and they are responsible for validating transactions and creating new blocks.

One of the earliest implementations of PoA was the Kovan testnet, which was launched in March 2017. Since then, PoA has been used in various blockchain projects, including POA Network, Ethermint, and xDai Chain.

AUTHORITY ROUND (AuRa)

In a PoA system, a group of trusted validators known as "authorities" are responsible for validating transactions and creating new blocks. The authority round is the process by which these validators take turns proposing and validating blocks in a predetermined order, similar to a round-robin system.

During each authority round, a single validator is designated as the block proposer, and they are responsible for creating the next block in the chain. The other validators then verify the proposed block and add it to their copy of the blockchain if it is valid.

The authority round mechanism in PoA helps to ensure that the blockchain remains secure and prevents any single validator from having too much power or control over the network. This makes PoA a popular consensus algorithm for private or permissioned blockchain networks, where trust is already established among participants.

In contrast, the PoW consensus algorithm relies on miners solving complex mathematical puzzles to validate transactions and create new blocks, with the first miner to solve the puzzle being rewarded with cryptocurrency. There is no authority round in PoW, as miners compete to create the next block rather than taking turns.

POA NETWORK

VALIDATORS

Validators in a proof of authority (PoA) network are responsible for verifying and validating transactions on the blockchain. In PoA, the validators are typically a group of pre-approved nodes, often referred to as "authorities," that are selected based on their reputation, identity, or stake in the network.

Validators in a PoA network do not compete to solve complex mathematical problems like in proof of work (PoW) systems, but instead take turns adding blocks to the blockchain. The authority that is selected to add the next block is chosen through a round-robin process or a similar method.

Since validators in PoA networks are selected based on their reputation, identity, or stake, they are expected to be more reliable and efficient than validators in PoW systems. Validators in PoA networks are also typically responsible for maintaining the network and ensuring its security, which includes monitoring for potential attacks or malicious behavior.

ECONOMY

In a proof of authority (PoA) network, the economy is typically structured around a native cryptocurrency that is used to incentivize validators and maintain the network. Validators in PoA networks are often rewarded in the form of transaction fees or newly minted tokens, which they receive for adding new blocks to the blockchain. These rewards can help incentivize validators to maintain the network and perform their duties.

Since PoA networks typically have a limited number of validators, the cost of maintaining the network can be lower than in proof of work (PoW) or proof of stake (PoS) systems. This can make it easier for users to participate in the network and reduce the barrier to entry.

However, the economy of a PoA network can also be vulnerable to centralization, as the authority nodes are typically selected based on their reputation, identity, or stake in the network. If a single entity or a small group of entities control a majority of the authority nodes, they may be able to manipulate the network for their own benefit, potentially leading to censorship or other issues.

Overall, the economy of a PoA network is designed to incentivize validators to maintain the network and ensure its stability and security, but it is important to carefully consider the potential risks and vulnerabilities associated with centralization.

TOKENOMICS OF RIKEZA

	Particulars	**Percentage**	**Coin**	**Distribution**
	Total Coin	100%	10,000,000,000	
1	Holding	90%	9000,000,000	This fund will be held by the Smart Contract, as soon as the products are launched, the coins will continue to be released.
2.	Public sale	0.5%	50,000,000	On multiple exchanges.
3.	Research & Development	1%	100,000,000	The aim of this fund is to support the development of idea and systematically upgrade Rikeza Blockchain.
4	Team	1%	100,000,000	This fund will be locked for next ONE year and then in every quarter funds will be released for next TEN years.
5.	Future products	2%	200,000,000	This fund will be used for next generation apps like Dapps, NFT, Metaverse, Smart Contracts, Education, Banking services and much more.
6.	Staking	2.5%	250,000,000	Staking reward will be announced.
7.	Marketing & Ops	2%	200,000,000	This fund will be used for marketing, community mgmt, promotional activites, referral/airdrops, rewards and prize pools etc.
8.	Treasury & Reserve	1%	100,000,000	Funds will be used in supporting Rikeza Blockchain roadmap for the long term and will be eventually covering unexpected expense that might come up related to platform operations, stability, security and growth.