Kira Interchain Exchange

Lite Paper, June 2019

Securing The Future of Proof of Stake

Kira is a hyperscale decentralized exchange that enables trustless cross-chain token transfers and trading. Thanks to dual consensus mechanisms of Multi-Bonded Proof of Stake (MBPoS) that provides security and Multi-Bonded Proof of Authority (MBPoA) that delivers speed, users can trade in trustless manner whilst maintaining a user experience that matches or exceeds that of centralized exchanges.

Connections to Internet of Blockchain (IoB) networks such as Cosmos and Polkadot and bridges to foreign public and private ledgers enable Kira users access to a variety of markets previously unreachable in a decentralized manner. Behind the scenes, the Tendermint consensus engine provides fast finality of trades, enabling liquidity providers to reduce risk, tighten spreads and deepen order books.

Stakeholders and operators manage, govern and benefit from all aspects of exchange operations in a fully decentralized fashion, without any privileged participants deriving excessive power or tribute. Efficient operations and ongoing open-source development is incentivised via a novel economic model consisting of multiple self-sustaining positive feedback loops. Kira aims to offer the emerging Proof of Stake (PoS) ecosystem a number of fundamental advances in decentralization that, taken together, will help ensure the future security of all interconnected PoS by delivering uncensorable and unstoppable market access.

Introducing

Table of Contents

Key Failings of Centralized Exchanges

1. Access

Accounts created on centralized exchanges expose users to a multitude of threats, even when employing security best practices such as Two Factor Authentication (2FA). Attack vectors such as SIM Port Hacks, Man in The Middle Attacks (MITM), Man in The Endpoint Attacks (MITE), JWT token hijacking, account recovery attacks, Phishing, Stolen Biometrics, One Time Password generation vulnerabilities and physical attacks on 2FA hardware exhibit far greater levels of risk versus accessing a blockchain network using a hardware wallet.

2. Availability

Even though centralized services can provide high uptime, they are rarely capable of sufficient auto scaling and tend to exhibit stress under high load. Sophisticated trading UIs frequently become unresponsive in the event of major market moves and entirely unavailable during maintenance periods and other unexpected events. Users can be restricted in their ability to place or cancel order or altogether denied the ability to trade or move funds, while market direction rapidly changes, incurring losses for traders that can be every bit damaging as hacks.

3. Custody

When sending funds to a centralized exchange you relinquish custodianship and forfeit the security guarantees of the originating blockchain. Your funds are only as secure as the weakest link in the complex set of business processes that aims to protect them; authorization, internal vulnerabilities, employee affairs, non compliance with local laws and international legal actions can all cause irreversible loss. Even the most trusted custodians rely on a human element which is the most likely source of failure next to a software vulnerabilities and the processes surrounding cold storage and custodianship of funds. In essence, centralized exchanges are a black box of interleaving and potentially fragile human-mediated software processes, wrapped in slick marketing whose security claims are often entirely unverifiable.

4. Transparency

Centralized exchanges are private businesses, and as such, detailed knowledge of operational goings-on is reserved only for insiders. With many of these exchanges domiciled in unregulated privacy jurisdictions and controlled by anonymous owners, there are long standing suspicions within the crypto community of market manipulation, malfeasance and outright fraud. Accusations leveled at these businesses range from wash trading or outright forgery of volume statistics in order to give the appearance of liquidity and to gain market share, to the recent claim that a number of top tier exchanges are discretely operating a fractional reserve system in order to mask solvency issues. Without a truly decentralized alternative that caters to the full range of tokens that users want to trade, customers at centralized exchanges have little choice but to accept this lack of transparency and bear the risks. Given the lessons of MtGox and others, we feel that centralized exchanges are an unnecessary existential threat to the ecosystem, and that the time has come to render them obsolete.

5. Identity

Centralised exchanges make attractive targets for reasons beyond the funds they custody. In particular, exchanges capture, process and retain a wealth of sensitive user data, including private email addresses, trading limits and histories, hashed passwords and a plethora of identity documents used for KYC purposes. We believe that (for crypto-to-crypto trading, at least) users should not be required to expose themselves to threats from hackers, rogue employees and overreaching government agencies. Even incumbent decentralized exchanges are seemingly unable to resist the pressure to enforce KYC and restrict users in certain jurisdictions from participating. Kira, on the other hand, offers a completely decentralized experience, and has no website that users can be blocked from accessing. Because the KiraEx trading interface is delivered trustlessly over the blockchain itself, like Bitcoin, Kira puts itself beyond jurisdiction and enables peer-to-peer exchange in the safest possible manner.

6. Governance

Centralised exchanges, like most private companies, are subject to demands that can skew incentives toward the pursuit of short-term profit. One major consequence of these economic pressures is that our industry is increasingly becoming homogenised and undifferentiated; in particular, centralised exchanges tend to offer the weakest security believed to be acceptable and a trading experience just adequate enough to be competitive. Minor features and novelties are quickly copied, but game-changing innovation is in extremely short supply. Meanwhile, customers are treated to a uniform ‘take it or leave it’ experience across products and are absent from any meaningful dialogue that might lead to industry improvement. At Kira, our belief is that users are not a resource to be mined for transaction fees, but a community of potential partners who (via a fair and inclusive system of governance) can help steer our technical direction and deliver new and corruption resistant forms of market access.

Gateway To The Trustless Economy

Kira aims to establish itself both as a primary settlement layer within the Internet of Blockchains (IoB), and as a focal point for interchain commerce, by providing scalable order-books, OTC and a range of future decentralized finance (DeFi) applications that will be developed by our community and evolved via governance.

Our mission is to support the emerging proof of stake economy in realising its full potential by delivering a gateway for unfettered market access. We believe that all participants should be able to transact free from the whims of gatekeepers who might otherwise govern which projects will (and will not) be permitted to trade. It is this freedom of exchange that is crucial to the security of blockchains operating under proof of stake consensus, and must be protected at all costs.

Kira aims to solve following issues -

- Accessibility
    - Client Side Interchain Availability
    - Secure Access to The Network
- Scalability
    - Market Sharding
    - Interchain Validation and Slashing
- Ownership
    - Governance and Sustainability
    - Verification and Trust

Accessibility

The scalable decentralized applications (dApps) of the future will demand highly reliable gateways to the internet of blockchains that users can depend upon, even in extreme circumstances. Today, the majority of centralized (and even decentralized) exchanges hinge upon the availability of backend services, via which users requests are proxied in order to trade. Not only does this architecture threaten application availability when the system is stressed, attacked, censored or down for maintenance, but it also exposes users to a multitude of threats, even in the presence of security best practices such as multi-factor authentication.

These risks represent the tip of an iceberg of potential hazards that remain largely unaddressed by mainstream centralised and decentralized exchanges alike; even users of popular decentralized exchanges can be surprised to learn that applications they once imagined bulletproof can be rendered useless when key elements of their centralised and closed-source infrastructure become unreachable.

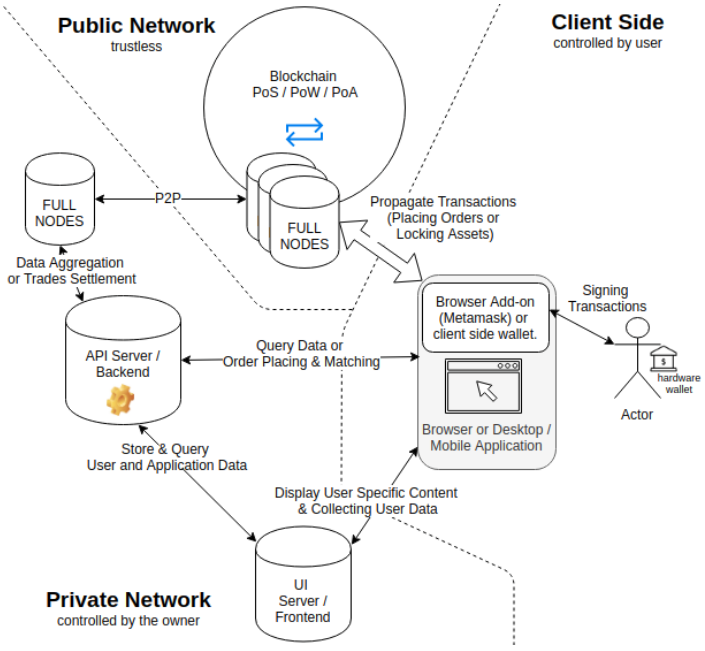
Kira aims to become the world's first exchange to offer direct, client side, access to the interchain economy - all without sacrificing user experience. Our goal is that users should be able to trade even in the event that our statically hosted frontend becomes unreachable. Should this happen, users will seamlessly fallback to a secure copy of the UI that is signed by validators and verified over the blockchain itself. Because users interact directly with the IoB, and sign and propagate transactions using a hardware wallet and a 'lite client', our system is able to offer security guarantees almost as high as the underlying cryptographic and blockchain protocols themselves.

Scalability

Currently most decentralized exchanges rely on a single blockchain or even have to share its chain capacity with other applications in case of generic smart contract chains, which immensely limits their speed and increases costs for the end user. Another limiting factor is the imbalance between how quickly a transaction should be finalized and the level of security (number of trusted validators) actually required to settle it as both of those factors are tightly conjoined with one another.

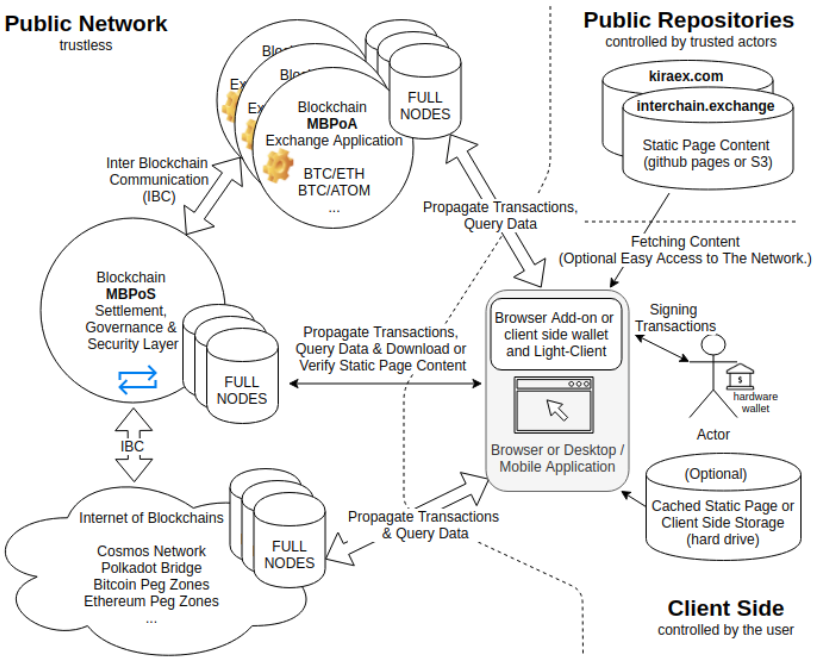
Kira employs a novel hub-spoke architecture in the blockchain space which parallelizes computation of the exchange applications into specialized, independent, interconnected Byzantine Fault Tolerant Proof of Authority consensus side chains, which share the validator set and communicate directly with the Proof of Stake based settlement layer, thus creating a hybrid system of scalable chains, independently processing transactions and matching orders with the optimal, comfortable for users level of security while maintaining speed and user experience available until now only on centralized exchanges.

Traditional Decentralized Exchanges



Requires dynamically hosted backend (by centralized, identifiable party) in order to present page content and often gathers user related data and statistics.

Kira Interchain Exchange



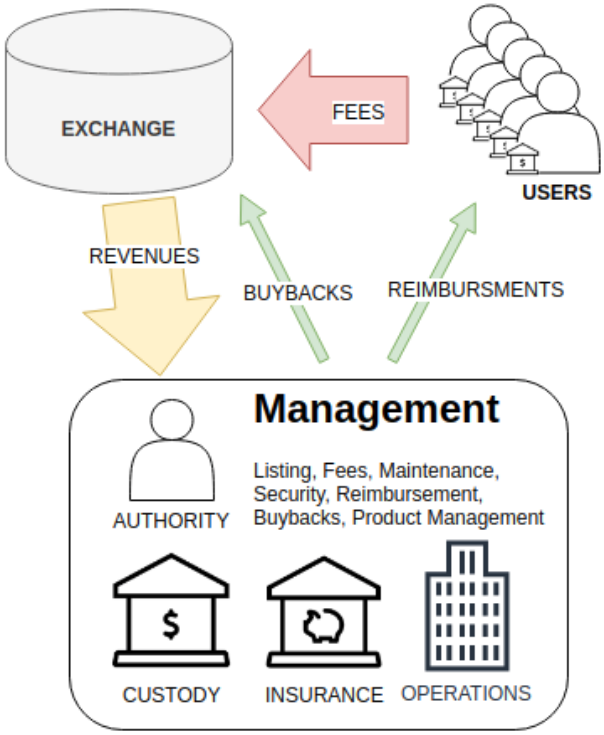
User directly communicates with the Internet of Blockchains and Sharded Exchange Application. Does not require any central authority to allow secure, “user friendly”. access.

Ownership

To date, the management of most exchanges was disjointed from their users and network operators. The listings, withdraws, deposits, exchange and other fees are usually either enforced by the protocol and limit usability of the system or driven by business decisions without a say nor a veto power from the community, that is other than forking away or abandoning the system and using another similarly managed counterparty.

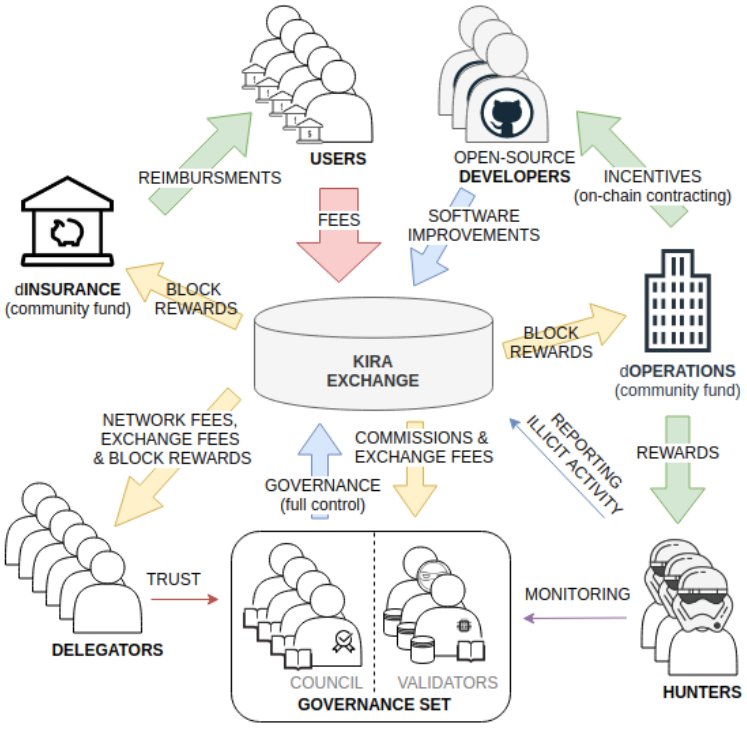
With Kira a transparent consensus of operators, users and elected council members helps not only optimize exchange operations by actively adjusting parameters that steer the economy but also adds a second layer of security in the form of activity monitoring, insurance, and governance managed validator slashing on top of the underlying protocol. Governance set can thus not only control the economy but also help prevent fraud and reimburse users in case of potential application faults, unforeseen events or malicious acts. Finally a governance enables smart slashing which ensures that bonded tokens are safe in case of validator accidental faults that do not threaten the network as well as incentivise an open source development and audits allowing for constant improvement and maintenance of the network.

Traditional Exchanges



Custody of assets and management is fully controlled by the authority that operates the exchange.

Kira Interchain Exchange



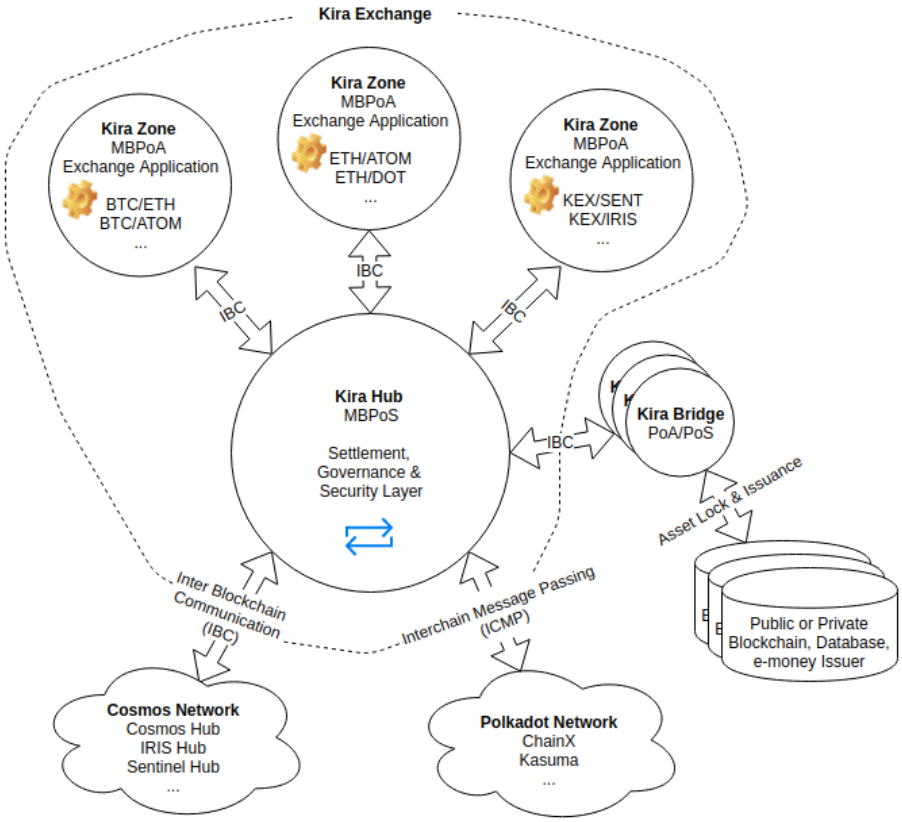
Kira is fully controlled by the governance set consisting of council members and validators with no single entity managing exchange operations.

Exchange Overview

Kira is a Hybrid Consensus Exchange within The Internet of Blockchains

Kira consists of many independent, interconnected shards called zones where various cryptocurrencies can be traded in a fully parallelizable manner to achieve centralized exchange experience and transaction throughput while maintaining decentralized exchange level of asset security, in order for them to remain fully within user custody even if originating from various different blockchains.

While the next generation networks like Cosmos and Polkadot provide access to broad economy of their native ecosystem tokens and legacy cryptocurrencies via the standards like IBC or ICMP - Kira directly bridges to them and offers a trustless exchange of assets between various Internet of Blockchains (IoB)

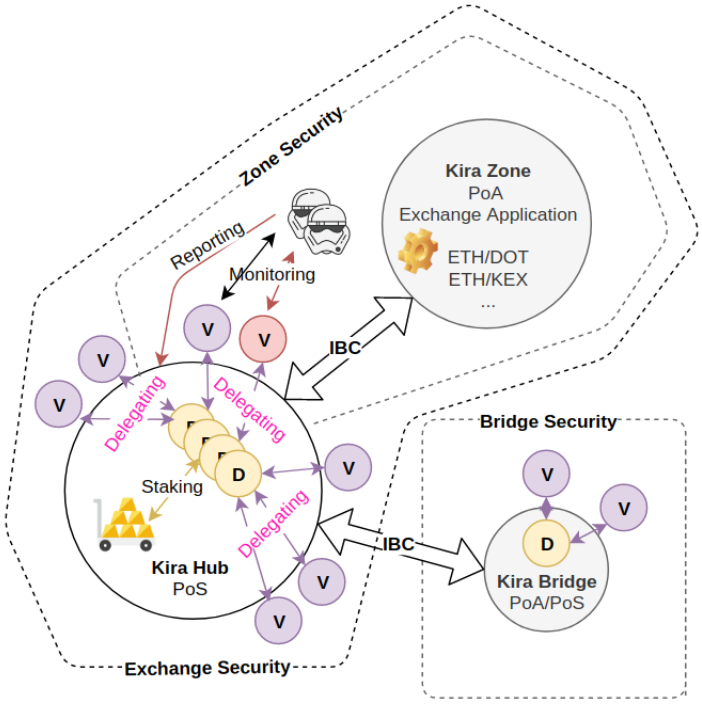


Kira Hub - Is a blockchain application operated under Bizantine Fault Tolerant Multi-Bonded Proof of Stake (BFT MBPoS) consensus engine that provides a governance, token issuance, token incubation and settlement layer for entire exchange, as well as interchain routing.

Kira Zones - Are an independent set of Interchain Slashable Byzantine Fault Tolerant Multi-Bonded Proof of Authority (MBPoA) blockchains operating a specialized parallelizable order books.

Kira Bridges - Secure, independent set of of PoA or PoS blockchains (deployed using Kira toolkit) allowing communication, asset transfer with various non IBC compatible networks, databases and e-money issuers.

Participant Roles



Hub Validator - Is an individual or entity participating in the consensus of the Kira Hub by executing a blockchain application containing the hub logic and by proposing blocks. Hub Validators are elected by the governance set and incentivised through commission fees. Each validator can charge individual commission fees from the revenues that stakeholders of Kira Exchange Tokens (KEX) and other whitelisted tokens generate. Hub validators are a part of the governance set and possess equal voting power.

Zone Validator - Is a Kira Hub Validator participating in the consensus of independent Kira Zones by executing a blockchain application with the exchange logic and proposing blocks. Zone Operators are elected and assigned to particular Zones by the Kira Hub governance system.

Bridge Validator - Is a person or entity participating in the consensus of the Kira Bridges by executing a blockchain application with the bridge logic and proposing blocks as well as observing state and controlling assets on the foreign blockchains or private ledgers. Bridges help custodians or e-money issuers interface their own private networks and quickly gain exposure to the interchain ecosystem. Bridge Validators are independent under PoS/PoA consensus and security constraints of their individual bridge chains.

Delegators - Secure Kira Hub and Bridge Zones by delegating their stakeable assets to Hub and Bridge Validators as well as actively participating in the governance.

Hunters - Secure Kira Exchange by monitoring Zone Validator operations and reporting any inconsistency of the state transitions or suspicious on-chain activity into the Settlement Layer where malicious acts can be stopped and penalized.

Counselors - among hub validators form initially technocratic and later democratic governance set. All governance set members have equal voting power, however counselors as opposed to the validators do not possess veto power over governance proposals.

Summary

Kira's goal is to become the first usable and truly decentralized interchain exchange, fully owned, governed, managed, protected and operated by the community thus becoming not only borderless and unstoppable but also the core of the new Proof of Stake paradigm which requires permissionless market access in order to sustain its growth.

Kira is crafted for the specialized purpose of the asset exchange thus able to handle throughput, which is comparable or even exceeding most of the current centralized exchanges while providing security, surpassing any usable trading platforms known to date by ensuring that users assets never leave their custody and can be traded using a hardware wallet.

Kira is a set of autonomous, parallelizable blockchain applications within internal hub-spoke architecture. By interconnecting with the state of the art internet of blockchain networks like Cosmos or Polkadot as well as maintaining dedicated bridges to other networks and chains of the most importance, Kira's can allow the highest number of assets in the current cryptocurrency space to have a trustless access to the market.