Abstract

In recent years, there has been an extraordinary surge in the advancement of GPU computing power, big data analysis, and the Internet of Things (IoT), catalyzing a notable proliferation of artificial intelligence (AI) capabilities. This transformative progression has manifested in the seamless integration of futuristic technologies like facial recognition and voice interaction into our daily lives. This trajectory underscores the profound impact of AI on societal evolution.

Kiiro Chain's overarching vision is firmly anchored in the creation of an infinitely scalable distributed high-performance computing network. This network is poised to emerge as a pivotal cornerstone within the landscape of AI-integrated metaverse technologies. By harnessing the potential of this network, Kiiro Chain aspires to establish itself as a market leader and become the most important computing infrastructure in the era of AI.

Introduction

1.1. Cryptocurrency, Bitcoin and Dash

The main network of Kiirocoin is developed based on Firo. Kiiro is a cryptocurrency aimed at revolutionizing the community by rewarding members through a unique 60% Proof of Stake (PoS) and 20% Proof of Work (PoW) mechanism. Built as a fork of Dash, Firo, Raptoreum leverages the power of the Firopow algorithm and asset-creation capabilities to create a sustainable and versatile community ecosystem. This whitepaper outlines the core principles, technical aspects, and roadmap of Kiirocoin.

Our focus has been directed towards the development of practical applications and services in the realm of artificial intelligence for a diverse range of Internet of Things (IoT) applications. Our objective is to imbue everyday devices with cognitive capabilities, encompassing dialogue, reasoning, and thinking abilities.

During the conceptualization of AI products by enterprises, a notable portion of their budget, typically ranging from 10% to 30%, is allocated for the development of AI computational capabilities. This includes the acquisition and maintenance of high-performance computing hardware. However, this expenditure often places a substantial burden on enterprises, impeding their investments in technological research and development. Thus, the need for an effective solution to alleviate this challenge and enable AI enterprises to navigate the technological evolution more seamlessly arises.

The answer to this challenge is affirmative, and this is where Kiirocoin Chain comes into play. Kiirocoin Chain stands as the world's pioneering and exclusive artificial intelligence platform propelled by blockchain technology, meticulously designed to address this predicament. Through the utilization of the Kiirocoin Chain platform, enterprises operating in the artificial intelligence domain can achieve a

reduction of up to 80% in their hardware expenses. Furthermore, the potential privacy risks associated with data utilization can be prudently circumvented.

1.2. The Need for Kiirocoin

We hold the conviction that the process of asset tokenization will assume a significant role in contemporary society, particularly as it pertains to fostering globalization through secure and privacy-ensured asset transfers. Within this context, specific tangible assets stand to gain from a streamlined and cost-effective conversion into what are referred to as "digital assets." These digital assets can be expeditiously transmitted to any geographical location worldwide within a matter of seconds, and this expediency comes at a mere fraction of the expenses associated with the conventional methods of physical mailing or tangible asset trading.

As this trend of global expansion gains momentum, there arises a corresponding necessity for enhanced user agency and resilience against censorship in the domains of digital asset issuance and governance.

Future Expansion

The dynamic landscape of rapid global progress necessitates a multifaceted and profound transformation. Kiiro stands as a proactive agent of transformation by introducing sustainable products and services that intricately align with the ever-evolving demands of the contemporary market. This adaptability underscores our commitment to not only remain relevant but also to contribute to the advancement of industries and societies.

Our guiding ethos, characterized by the "Go Beyond Next" spirit, epitomizes our dedication to transcending conventional boundaries and exhibiting creative ingenuity that sets us apart. This spirit propels us to approach innovation with a distinctive perspective, consistently venturing beyond established limits. This approach encapsulates our steadfast commitment to surpassing expectations and unlocking new realms of possibility.

Central to our modus operandi is an unwavering emphasis on the well-being of the global community and the planet at large. Our initiatives are meticulously orchestrated to prioritize the paramount interests of humanity and the environment. This ethos resonates across all aspects of our operations.

We have directed our energies toward establishing an ecologically conscious production and distribution ecosystem. The foundation of this endeavor is rooted in environmentally friendly practices that curtail our carbon footprint and resource consumption. This concerted effort resonates not only within our immediate operations but extends its influence across our entire supply chain, fostering sustainability at every juncture.

Ultimately, our actions are imbued with a forward-looking perspective that underscores our commitment to a positive and enduring impact. As we forge ahead, we remain steadfast in our dedication to shaping a future that is not only technologically advanced but also socially responsible and ecologically sustainable. This vision compels us to continually innovate, adapt, and redefine the contours of possibility, ensuring that our contributions stand as beacons of progress in the landscape of global transformation.

Mission

Our mission is to take **"Kiiro Coin to New Heights"** by providing an innovative, user-friendly, one-stop-shop to make a decentralized ecosystem but also to research and make a more precise decision, using a decentralized blockchain platform to give the opportunity to learn and raise funds for their projects to manage and improve their financial security.

- Our goal is to make staking and digital assets as easy as possible for all.
- In digital asset staking, it reduces volatility and generates positive price pressure.
- Operate as a community-focused and community-driven digital asset that is completely decentralized.
- Our goal is to make a blockchain with privacy features to provide a decentralized financial and secure ecosystem to everyone in the world.
- Is to provide the best computing power platform that can be used for AI processing.
- Integrate to eCommerce platform for more exposure and build a use case.

Kiiro Blockchain Privacy Mechanism

Blockchain privacy is kind of a hard task to achieve as you know that one of the purposes of building cryptocurrencies was that all transactions are transparent and coin amounts are public. This is also necessary to validate the state of chain and wallet balances. Kiiro uses Lelantus Spark Mechanism but to understand it we must understand how other privacy coin Mechanism works.

CoinJoin

As used in: Dash, Decred, Bitcoin Cash, Bitcoin mixers

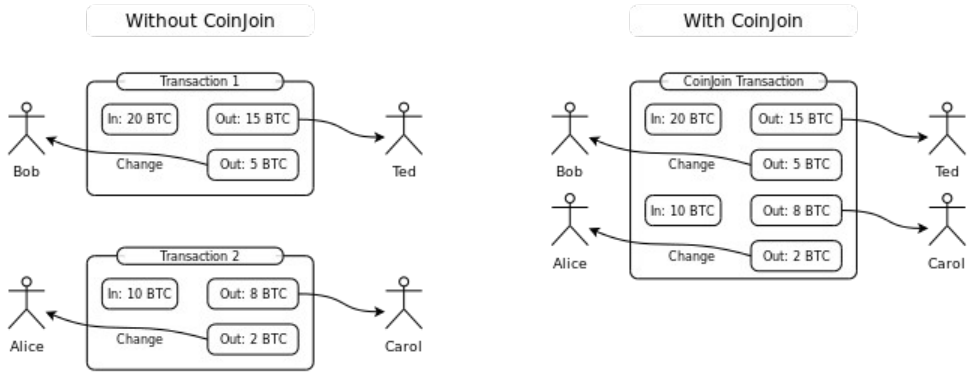
Pros:

- Works on top of most cryptocurrencies without the need for specific consensus rules
- Relatively simple to implement
- Transactions are regular transactions introducing no additional overhead

Cons:

- Amounts are still completely visible
- Anonymity sets are generally low and reliant on the number of mixers

- Coins that are mixed can be ‘flagged’ as going through a coin mixer.
- Needs time for mixes to happen
- Requires mixers to be online
- Difficult to use correctly and cumbersome requiring careful UTXO management
- Increases blockchain bloat with many transactions required to do mixes
- Earlier implementations involve trust in a third party mixer



CryptoNote & Ring Signatures

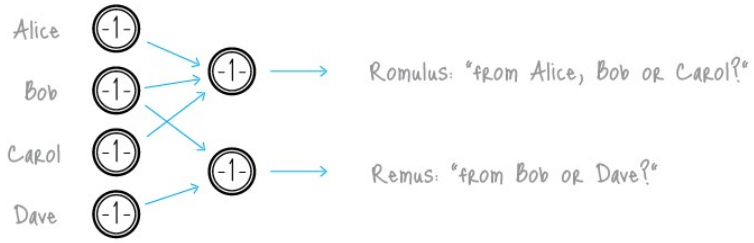
As used in: Monero, Particl, Zano

Pros:

- No need for a mixer and mixing is done automatically
- Can be implemented with privacy on by default
- Anonymity increases as time passes as outputs become the new inputs of new mixes
- Hides transaction amounts when implemented with RingCT
- Well understood cryptography

Cons:

- Does not break transaction links, merely obscures them, hence a ‘decoy’ model.
- Selecting the right decoys can be tricky and incorrect input selection algorithms can lead to loss of privacy
- Low anonymity set per transaction due to practically limited ring sizes



Lelantus Spark

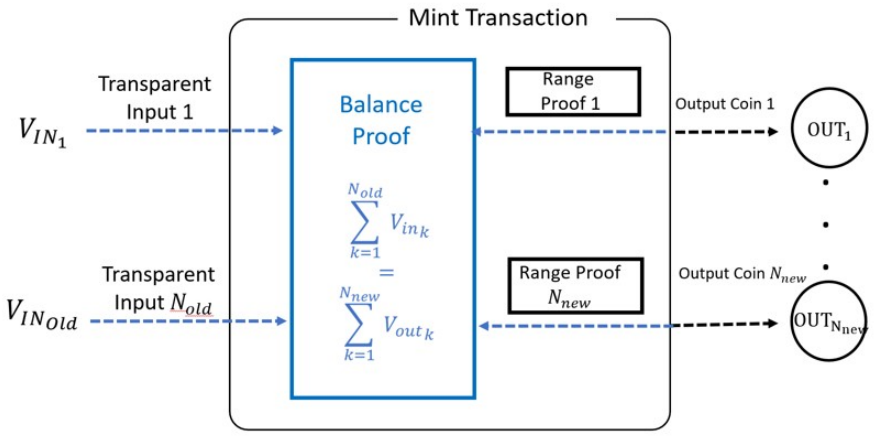
As used in Kiirocoin

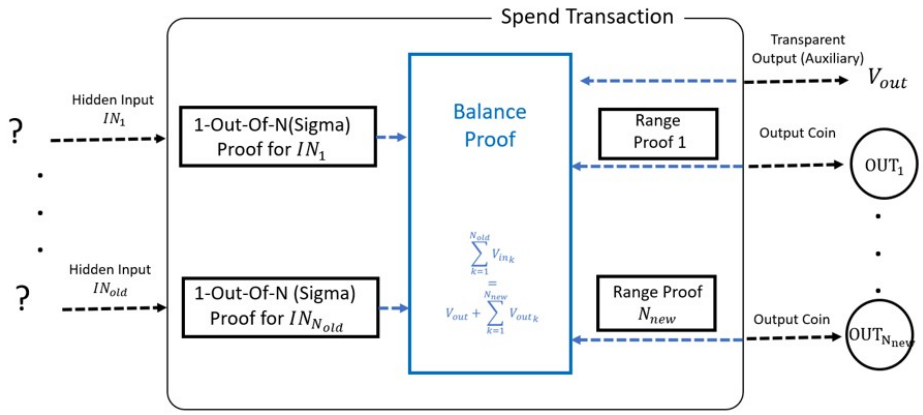
Pros:

- No need for a mixer
- High anonymity sets up to around 65,000.
- Uses well-researched cryptography and only requiring DDH cryptographic assumptions
- Small proof sizes of around ~1.5 kB per proof
- No trusted setup
- Doesn't use fixed denominations
- Can do direct anonymous payments without having to convert to base coin.
- Efficient batch verification
- Full support of stealth addressing, efficient multi/threshold signatures and view key functionality via Spark addresses
- Modular design which allows easier upgrade of components
- Unlike Lelantus v1/v2 a security proof for the balance is available
- Relatively simple cryptographic design compared to circuit-based zero-knowledge proof systems making it easier to implement and less room for error.

Cons:

- Difficult to scale past anonymity sets larger than 100,000 without cryptographic breakthrough, huge optimizations or replacement of underlying Groth-Bootle proofs.
- Verification of proofs are still slower than Groth16 zkSNARKs but are mitigated with efficient batch verification





Spark addresses work similarly to stealth addresses by allowing people to publicly share their address without it being searchable on the blockchain. Spark addresses instead automatically allows senders to generate one-time addresses on behalf of the recipient, which then designates who can spend the funds in the transaction. Additionally, third parties then are unable to easily link the recipient's wallet address to a transaction on the blockchain without the assistance of additional external information.

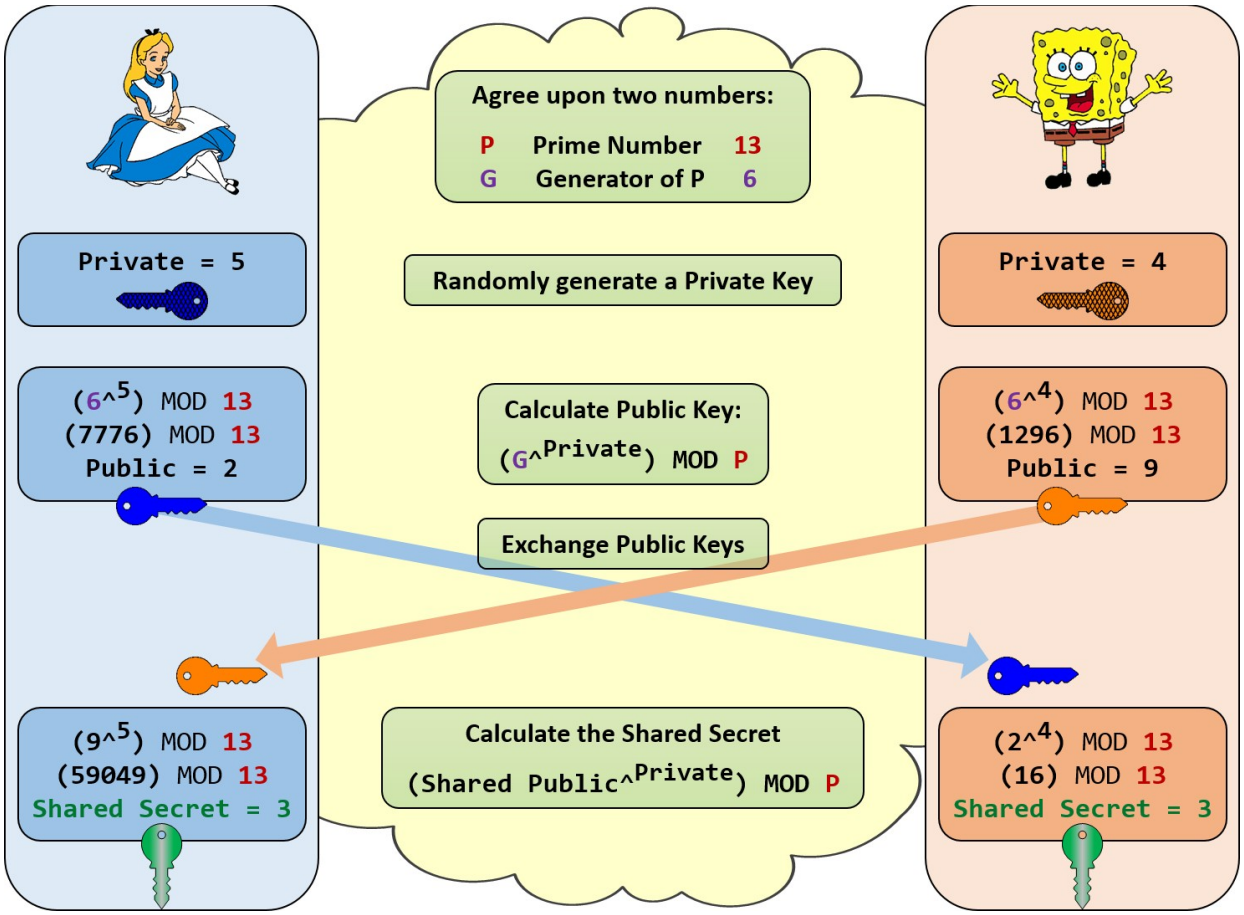
Spark addresses also has full view key support meaning it can track both incoming and outgoing funds should you choose to reveal it. In comparison, Monero's stealth addresses only support incoming view keys making it hard to disclose balances even if you wanted to. Spark addresses also have efficient multi-sig and threshold signature support.

We believe Lelantus Spark represents a holistic balance of high anonymity, simplicity and flexibility and offers a compelling alternative to existing cryptocurrency privacy protocols.

DDH Cryptography & DH Key Exchange Protocol

In the context of cryptography, "DDH" stands for the "Decisional Diffie-Hellman" assumption. It is an important assumption used in some cryptographic protocols, particularly in the field of public key cryptography and key exchange schemes.

The Decisional Diffie-Hellman assumption is related to the Diffie-Hellman (DH) key exchange protocol, which allows two parties to establish a shared secret over an insecure channel. In the classical DH protocol, two parties agree on a large prime number and a primitive root modulo that prime. They each generate a secret private key and compute a public key based on their private key and the agreed-upon values. By exchanging these public keys, they can then compute a shared secret that is known only to them.



The Decisional Diffie-Hellman assumption states that it is computationally infeasible for an attacker to distinguish between the Diffie-Hellman tuple (g, g^a, g^b, g^(ab)), where g is the generator, a and b are random secret integers, and g^x denotes the result of raising g to the power of x.

In simpler terms, the DDH assumption asserts that given the public values g, g^a, and g^b, it is hard to determine whether g^(ab) or some other random value was used for the shared secret computation. If the DDH assumption holds true, it provides a foundation for the security of various cryptographic protocols, such as key exchange, digital signatures, and encryption schemes based on the Diffie-Hellman primitive.

KIIRO uses the Diffie-Hellman-Discrete-Logarithm (DDH) cryptographic algorithm for key exchange. DDH is a key exchange protocol that allows two parties to establish a shared secret over an insecure channel. The shared secret can then be used to encrypt and decrypt messages.

KIIRO uses DDH in its Proof-of-Stake (PoS) consensus mechanism. In PoS, validators stake their KIIRO coins to participate in the consensus process. When a validator is selected to create a block, they must use their private key to sign the block. The signature is then verified using the public key of the validator.

The use of DDH in KIIRO's PoS consensus mechanism helps to secure the network from attack. If an attacker were to try to steal KIIRO coins from a validator, they would need to know the validator's private key. This is very difficult to do, as DDH is a very secure cryptographic algorithm.

In addition to its use in PoS, KIIRO also uses DDH for other purposes, such as message encryption and network authentication. The use of DDH helps to ensure that KIIRO is a secure and reliable cryptocurrency.

Here are some of the advantages of using DDH in KIIRO:

- DDH is a very secure cryptographic algorithm.
- DDH is relatively efficient, making it suitable for use in a cryptocurrency.
- DDH is well-understood and has been widely used in other applications.

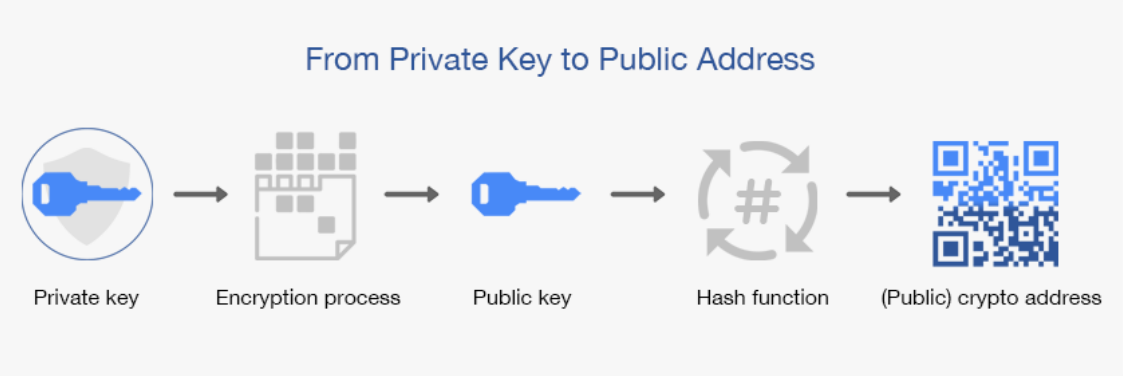
Here are some of the disadvantages of using DDH in KIIRO:

- DDH is a relatively complex cryptographic algorithm.
- DDH is not as widely supported as some other cryptographic algorithms.

Overall, the use of DDH in KIIRO is a good choice for securing the network and ensuring the integrity of transactions.

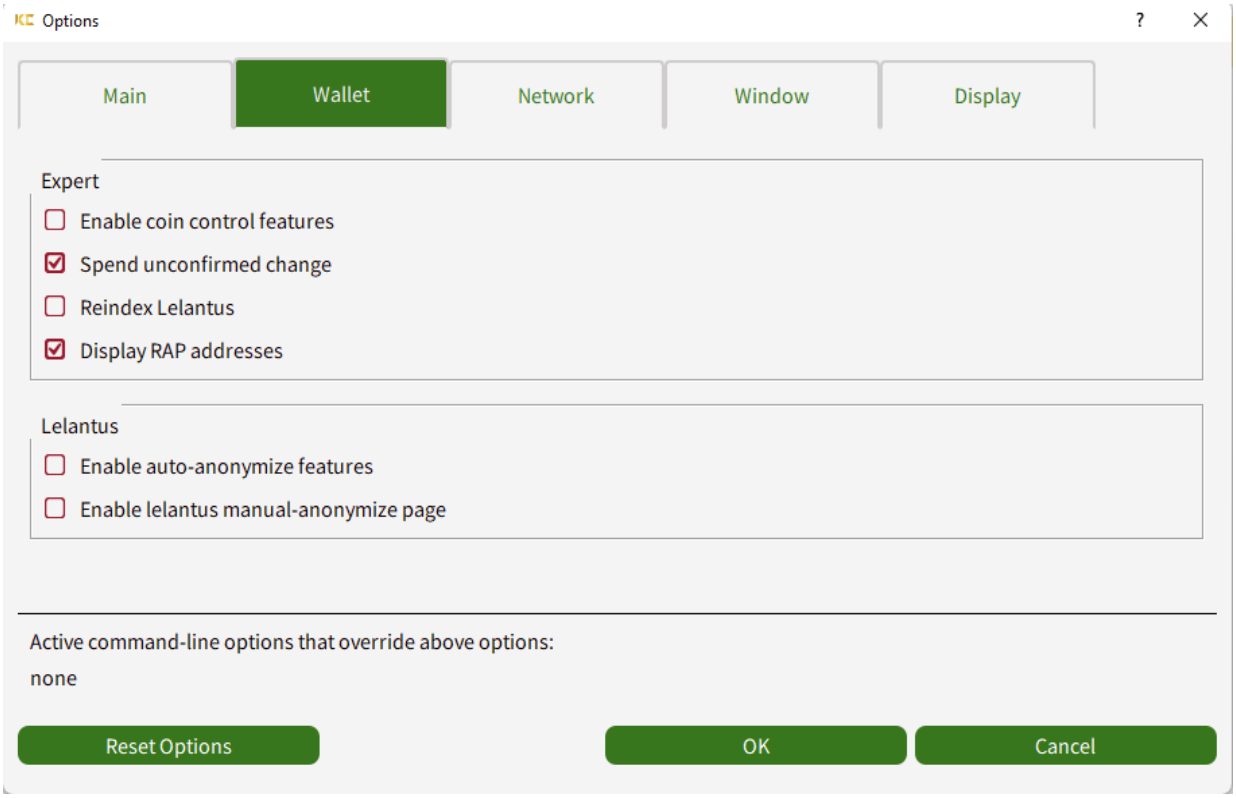
Receiver Address Privacy (RAP)

This unique privacy feature allows you to post your RAP address without compromising on your privacy. It means that you will be able to share your RAP address in the same way as you do share your email address now a days.



Today if we post our Bitcoin or Ethereum address publicly anyone can go to blockchain explorer and look for current balance and all past transactions with it.

By default, you will not find this option in your wallet. In order to activate it you need to first encrypt your Kiiro wallet. On the top left corner click settings >> options >> wallet >> In expert group check “Display RAP Addresses”.



ChainLocks Protects Against 51% Attacks

PoW is an excellent mechanism for ensuring fair distribution especially if mineable using commodity hardware. Anyone can participate in the network and earn a share of the block reward as long as they provide computing power when compared to other distribution mechanisms such as ICOs, pre-sales or even airdrops. It also provides an objective way to evaluate which chain is valid without relying on any external source.

While elegant, PoW isn't perfect and either boils down to being controlled by ASICs, which are by its very nature exclusionary, or being subject to 51% attacks, where hardware can be rented to attack the network as we have seen in past with many coins.

To mount an attack on Kiirocoin blockchain now would require approximately 50% of all masternodes to be taken over to disable ChainLocks and also the necessary hashrate to mount the 51% attack. As masternodes require some amount of collateral backing it, an attacker would also need to acquire significant amounts of coins to attack the network.

Blockchain Scalability

KIIRO presents itself as a cryptocurrency distinguished by its inherent scalability, poised to seamlessly accommodate a substantial volume of transactions without compromising operational efficiency. This characteristic is underpinned by an array of meticulously engineered techniques that collectively elevate the performance of its network, positioning KIIRO as a frontrunner in the domain of high throughput blockchain systems.

The pivotal facet of KIIRO's scalability is a product of its strategic incorporation of a multifaceted approach. The orchestration of these strategies underscores our commitment to ensuring that the cryptocurrency network remains robust and responsive even as transaction demands surge.

1. Batching transactions

KIIRO uses a technique called batching transactions to optimize the performance of its network. This means that multiple transactions can be processed together, which can help to reduce the cost and time of transactions.

For example, if there are 100 transactions that need to be processed, they can be batched together into 10 batches of 10 transactions each. This means that only 10 blocks need to be created, instead of 100 blocks. This can help to reduce the time it takes to process transactions and the amount of data that needs to be stored on the blockchain.

2. High-performance consensus mechanism

KIIRO uses a high-performance consensus mechanism called Proof-of-Stake (PoS). PoS is a more efficient consensus mechanism than Proof-of-Work (PoW), which is used by many other cryptocurrencies. This is because PoS does not require miners to compete to solve complex mathematical problems. Instead, validators are randomly selected to create blocks based on the amount of KIIRO they stake.

This makes PoS more scalable than PoW, as it does not require as much computational power. This means that KIIRO can handle a larger number of transactions without sacrificing performance.

3. Future scalability plans

The KIIRO team is constantly working to improve the scalability of the network. Some of the future scalability plans include:

- **Sharding:** Sharding constitutes a strategic methodology employed to partition the blockchain into more manageable segments referred to as shards. This approach is instrumental in augmenting the network's scalability by facilitating concurrent processing of a greater volume of transactions.

- **Layer 2 solutions:** Layer 2 solutions present a mechanism for enhancing blockchain scalability by relocating a portion of the processing activities off the primary blockchain. This strategic off-chain processing alleviates the strain on the main blockchain, thereby fostering improved overall performance.

Our team is committed to making Kiirocoin a scalable cryptocurrency. They are constantly working to improve the scalability of the network, and they are confident that KIIRO will be able to handle a large number of transactions in the future.

Challenges and Potential Solutions

Adoption and Market Penetration

To gain widespread acceptance, Kiiro needs to address entry barriers comprehensively and present attractive benefits for miners, developers, and other participants in the trading realm. By refining its Proof of Stake system, expanding its ecosystem, and forming strategic partnerships, Kiiro can effectively extend its market presence and position itself as leading cryptocurrency.

In essence, the Kiiro blockchain introduces a new way of integrating blockchain technology with AI applications. Notably featuring a distinct 60% Proof of Stake mechanism, the platform possesses an inherent capability for changing the financial system. As the platform's influence continues to expand, Kiirocoin is poised to bring about significant changes in the ecosystem, offering fresh opportunities and incentives for AI based businesses, developers, and other stakeholders.

Tokenomics of Kiirocoin

The Kiiro tokenomics model is designed to support a balanced and sustainable ecosystem by distributing rewards among miners Proof of Work (PoW), masternodes Proof of Stake (PoS) and developers. The tokenomics model is as follows:

- 60% MasterNodes (PoS)
- 20% Proof of Work (PoW)
- 10% Community Rewards
- 10% Governance Fee

The masternodes mechanism will receive 60% of the rewards, incentivizing small and medium-sized businesses to participate in the Kiiro ecosystem to make the network more secure and earn coins in return.