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, underscoring the profound impact of AI on societal evolution.
RealiChain's overarching vision is anchored in creating a privacy-focused blockchain that not only empowers users with secure transactions but also contributes to environmental sustainability. By integrating a unique feature that rewards users for planting trees and reduces carbon emissions with each transaction, RealiChain aims to become a pivotal cornerstone within the landscape of eco-friendly technologies. Through its innovative approach, RealiChain aspires to establish itself as a leader in both blockchain and environmental responsibility, creating a decentralized ecosystem that nurtures the planet while protecting user privacy.

Introduction

- Cryptocurrency, Bitcoin, and Dash

The main network of RealiChain is developed based on Firo. RealiChain is a cryptocurrency designed to revolutionize community engagement by rewarding members through a distinctive mechanism Built as a fork of Dash, Firo, and Raptoreum, RealiChain leverages the power of the FiroPoW algorithm and asset-creation capabilities to create a sustainable and versatile community ecosystem. Our focus has been on developing practical applications and services that not only enhance privacy but also contribute to environmental sustainability. Each transaction on the RealiChain network helps plant a tree, directly reducing carbon emissions. This unique feature aligns with our objective of creating a blockchain that is not only technologically advanced but also environmentally responsible. During the conceptualization of eco-friendly blockchain solutions, a significant portion of the budget, typically ranging from 10% to 30%, is allocated for the development and maintenance of high-performance computing hardware. This expenditure can place a substantial burden on enterprises, hindering their investments in technological research and development. RealiChain offers an effective solution by integrating green initiatives into the blockchain, allowing AI enterprises to navigate technological evolution more seamlessly while contributing to environmental sustainability. RealiChain stands as a pioneering blockchain platform that marries technological advancement with ecological responsibility, offering enterprises in the AI domain a means to reduce operational costs and environmental impact. Additionally, RealiChain’s privacy features ensure that potential risks associated with data utilization are prudently managed.

- The Need for RealiChain

We believe that the process of asset tokenization will play a significant role in contemporary society, particularly in 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 "digital assets." These digital assets can be transmitted globally within seconds at a fraction of the cost associated with conventional methods of physical mailing or tangible asset trading.

As global expansion gains momentum, there is a corresponding need for enhanced user agency and resilience against censorship in the realms of digital asset issuance and governance. RealiChain addresses this need by providing a decentralized, privacy-focused blockchain platform that also contributes to environmental sustainability.

- Environmental Impact of RealiChain

RealiChain stands out by integrating environmental consciousness into the core of its blockchain technology. Every transaction on the RealiChain network is designed to reduce carbon emissions by contributing to the growth of new trees. This unique approach ensures that as the network expands, its positive impact on the environment also increases, making it an active contributor to global reforestation efforts.

By incorporating a mechanism that rewards users for planting trees, RealiChain not only offsets its carbon footprint but also plays a proactive role in combating climate change. The network's design ensures that with each transaction, a portion of the fees is allocated to environmental projects, such as tree planting and forest conservation. This initiative not only mitigates the environmental impact of blockchain technology but also sets a new standard for sustainability in the cryptocurrency space.

Furthermore, the decentralized nature of RealiChain empowers individuals and businesses to participate in environmental conservation efforts on a global scale. By using RealiChain, participants are not just engaging in secure and private transactions but are also contributing to a greener planet. This makes RealiChain an essential tool for those who are conscious of their ecological footprint and wish to take actionable steps towards a more sustainable future.

RealiChain's commitment to the environment extends beyond its transactions. The network's architecture is designed to minimize energy consumption by optimizing mining processes and promoting the use of renewable energy sources. This energy-efficient approach further reduces the environmental impact associated with traditional blockchain networks, aligning RealiChain with global sustainability goals.

Future Expansion

The dynamic landscape of rapid global progress necessitates a multifaceted and profound transformation. RealiChain is a proactive agent of transformation by introducing sustainable products and services that align with the 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, "Go Beyond Next," epitomizes our dedication to transcending conventional boundaries and exhibiting creative ingenuity that sets us apart. This spirit drives us to approach innovation with a distinctive perspective, consistently venturing beyond established limits. Central to our mission is an unwavering emphasis on the well-being of the global community and the planet. Our initiatives are meticulously orchestrated to prioritize the interests of humanity and the environment.

We have focused our efforts on establishing an ecologically conscious production and distribution ecosystem, rooted in environmentally friendly practices that reduce our carbon footprint. This effort extends across our entire supply chain, fostering sustainability at every juncture. As RealiChain grows, our environmental initiatives will scale in parallel, ensuring that our impact on the planet is always positive.

Our approach includes partnerships with environmental organizations to enhance the effectiveness of our tree-planting initiatives and expand our contribution to global reforestation efforts. By integrating blockchain technology with environmental stewardship, RealiChain aims to lead by example in demonstrating how digital innovation can coexist with and support the natural world.

As we forge ahead, we remain steadfast in our commitment to shaping a future that is technologically advanced, socially responsible, and ecologically sustainable. Our contributions aim to be beacons of progress in the landscape of global transformation, ensuring that RealiChain is not just a leader in privacy and security, but also a champion of environmental sustainability.

Mission

Our mission is to elevate "RealiChain to New Heights" by providing an innovative, user-friendly, decentralized ecosystem that not only prioritizes privacy and security but also actively contributes to environmental sustainability. We aim to empower users by offering a blockchain platform that integrates ecological responsibility with advanced financial technology, allowing users to improve their financial security while making a positive impact on the planet.

- **Community-Driven and Decentralized:** We are committed to operating as a community-focused and community-driven digital asset, ensuring that RealiChain remains completely decentralized and governed by its users.
- **Prioritizing Privacy and Security:** Our mission includes building a blockchain with robust privacy features, providing a secure and decentralized financial ecosystem accessible to everyone globally.
- **Supporting Environmental Sustainability:** We are dedicated to integrating environmental initiatives into our platform, rewarding users for planting trees and contributing to carbon emission reductions with every transaction.
- **Expanding Use Cases and Exposure:** By integrating RealiChain with eCommerce platforms and other industries, we aim to expand its use cases, increase exposure, and create a more versatile and impactful digital asset.

REALI 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. REALI uses Lelantus Spark Mechanism but to understand it we must understand how other privacy coin Mechanism works.

Coinjoin

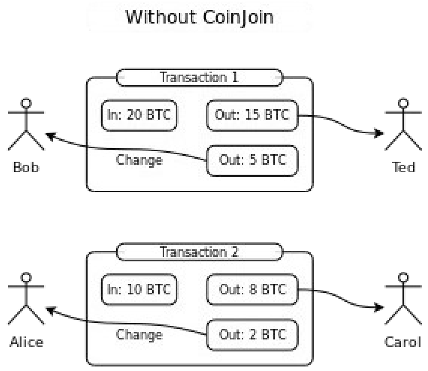
As used in: Dash, Decred, Bitcoin Cash, Bitcoin mixers

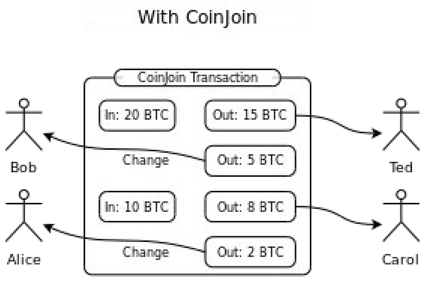
Pros:

- 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

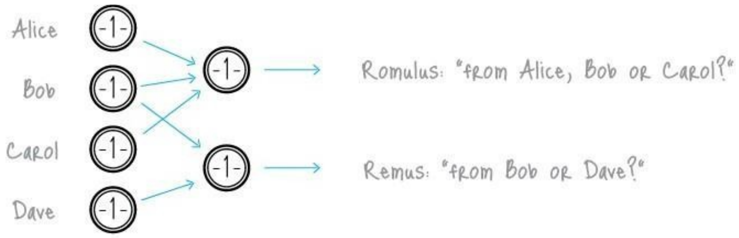
As used in: Monero, Particl, Zano

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


Alice
Bob
Carol
Dave
-1-
-1-
-1-
-1-
-1-
-1-
Romulus: "from Alice, Bob or Carol?"
Remus: "from Bob or Dave?"

Lelantus Spark

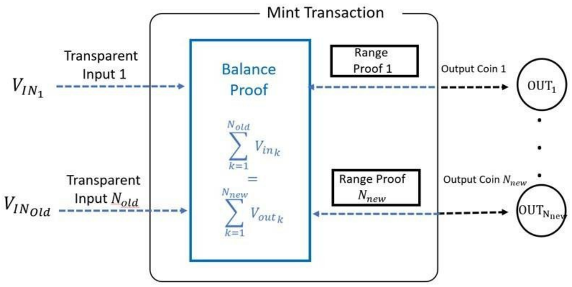
As used in RealiChain

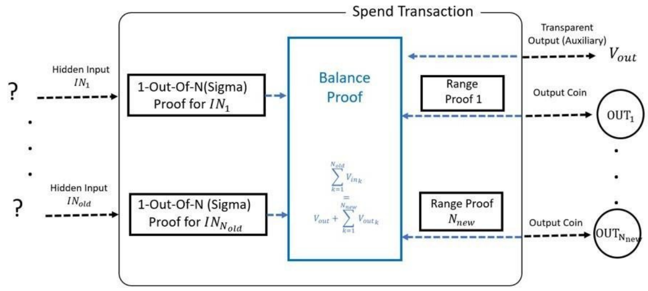
Pros:

- 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




Spend Transaction
?
Hidden Input IN_1
?
Hidden Input IN_{old}
1-Out-Of-N(Sigma) Proof for IN_1
1-Out-Of-N (Sigma) Proof for $IN_{N_{old}}$
Balance Proof
$\sum_{k=1}^{N_{old}} V_{in_k} = V_{out} + \sum_{k=1}^{N_{new}} V_{out_k}$
Range Proof 1
Range Proof N_{new}
Transparent Output (Auxiliary)
V_{out}
Output Coin
OUT_1
Output Coin
$\mathrm{OUT}_{\mathrm{N_{new}}}$

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.

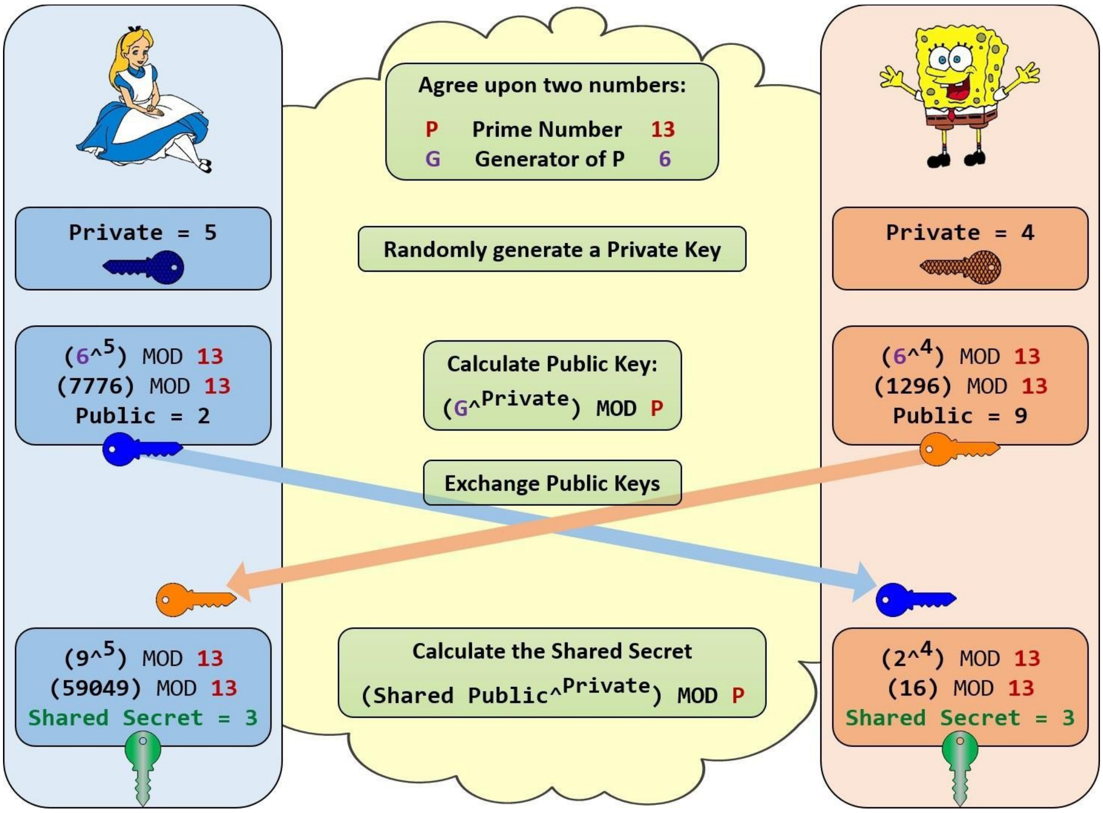
Spark addresses also has full view key support meaning it can track both incoming and outgoing funds should you choose to reveal it. In comparison, Monero's stealth addresses only support incoming view keys making it hard to disclose balances even if you wanted to. Spark addresses also have efficient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

REALI 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.

REALI uses DDH in its Proof-of-Stake (PoS) consensus mechanism. In PoS, validators stake their REALI 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 REALI's PoS consensus mechanism helps to secure the network from attack. If an attacker were to try to steal REALI 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, REALI also uses DDH for other purposes, such as message encryption and network authentication. The use of DDH helps to ensure that REALI is a secure and reliable cryptocurrency.

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

- 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.

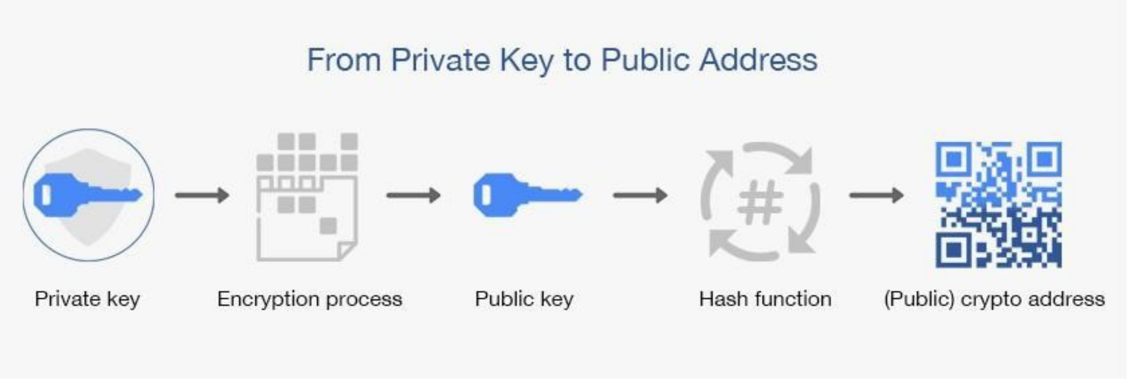
Here are some of the disadvantages of using DDH in REALI:

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

Overall, the use of DDH in REALI 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 REALI 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 REALI 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

REALI 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 REALI as a frontrunner in the domain of high throughput blockchain systems.

The pivotal facet of REALI'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.

Batching transactions

REALI 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.

High-performance consensus mechanism

REALI 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 REALI they stake.

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

Tokenomics of RealiChain

The RealiChain tokenomics model is designed to support a balanced and sustainable ecosystem by distributing rewards and resources across various participants in the network. The distribution model is as follows:

- **8% Team:** Allocated to the team for continued development, maintenance, and innovation within the RealiChain ecosystem.
- **2% Expenses:** Reserved for operational costs, including marketing, partnerships, and other essential expenses necessary for the growth and expansion of RealiChain.
- **37% Masternodes (MNs):** A significant portion dedicated to masternodes, incentivizing network stability and security by rewarding those who contribute to the network's operation.
- **20% Miners:** Allocated to miners who secure the network through Proof of Work (PoW) using the FiroPow algorithm, which is ASIC-resistant and ensures a fair mining process.
- **33% Project:** Reserved for ongoing and future projects, including environmental initiatives such as tree planting and carbon emission reduction efforts. This allocation supports RealiChain's mission to make a positive impact on the environment with every transaction.