REGIUS MARK

www.regiusmark.io
contact@regiusmark.io
July 10, 2019

White Paper

Ticker symbol: MARK

Our mission is to bring utility to precious metals in an innovative blockchain solution — Enter the Golden Age.

DISCLAIMER OF LIABILITY

The purpose of this White Paper is to present Regius Mark to potential coin holders and network operators. The information provided in this document may not be exhaustive, and it will not imply any elements of a contractual relationship. Its sole purpose is to provide relevant and reasonable information to potential coin holders who wish to mint or purchase Regius Mark while it is available on the open market.

Nothing in this White Paper shall be deemed to constitute a prospectus of any sort or a solicitation for investment, nor does it in any way pertain to an offering or a solicitation of an offer to buy any securities in any jurisdiction. This document is not composed in accordance with, and is not subject to, laws or regulations of any jurisdiction, which are designed to protect investors.

Regius Mark is not a security, and has not been registered under the Securities Act, the securities laws of any state of the United States or the securities laws of any country, including the securities laws of any jurisdiction in which a potential coin holder is a resident.

Regius Mark is not intended for sale or use in any jurisdiction where sale or use of the coin may be prohibited.

Regius Mark confers no other rights in any form, including but not limited to any ownership, distribution (including but not limited to profit), redemption, liquidation, proprietary (including all forms of intellectual property), or other financial or legal rights, other than those specifically described in the White Paper.

Note: This document is a work in progress and will be continuously updated as necessary.

Contents

1 Introduction

Cryptocurrencies such as Bitcoin have been successful examples in creating a distributed network that users could trust, and many of these currencies have experienced a tremendous increase in value, regardless of having no backing. It has marked a significant beginning to the digital currency world that users can trust, becoming what many have called "digital gold".

Currency markets are volatile where our token will be backed by physical gold providing stability and minimizing risk. The blockchain provides a means to secure funds digitally without weighing you down. Our technology is designed to be eco-friendly and easy to use for the average consumer.

Decentralized networks have good intentions but we see it leads to issues such as scalability, performance, and inability to upgrade the software easily. Our centralized network allows us to scale, optimize for performance, and easily upgrade the system.

The Regius Mark blockchain will contain one virtual asset with the name of MARK (gold). These virtual assets will be backed by physical gold, ensuring a stable market, rather than a volatile market.

2 Current Issues

There are a variety of issues in the financial system and existing cryptocurrencies that prevent wide-scale adoption by the user and merchants. There are risks involved for the merchant and the consumer.

The common risk is a consequence of the volatile nature of the cryptocurrency markets. This volatility is notably caused by tokens that have no intrinsic value, relying on the trust and faith of its users to bring value. The volatility helped drive new technologies that are increasingly sophisticated for the merchants and users alike. However, both have to account for the ever-changing landscape of the token values. By physically stabilizing our token to gold, we get the benefits of the gold standard.

When blockchains are under heavy load, the fees become expensive. The underlying technology is not designed to scale. Modern advances and research into algorithms allow us to create new technologies designed to be scalable for the world.

The technology is still too difficult to use for the consumer and business owner alike. There's a problem when merchants have to use third-party payment processors to accept payments on the blockchain and users have to decide which wallet to use and learn how it works. We aim to have an intuitive wallet with native multi-signature support for consumers and SDKs designed to interact with the blockchain made available for merchants. The current lack of DX and UX is a hindrance to global adoption.

Consumers want the cheapest fees when making transactions. Tech-savvy crypto users will hold a wide portfolio of tokens and decide which blockchain is the most cost effective to create a transaction. A novice will be forced to struggle with the expensive fees and time-to-time even the tech-savvy will have to as well.

The Proof-of-Work algorithm is a dinosaur in the modern era of computer science. A Bitcoin specialist has determined it takes over an estimated 2.5 gigawatts of electricity to mine. We are phasing out these expensive algorithms and replacing them with an eco-friendly system that is designed to scale and confirm transactions quickly. The efficiency is essential to enable a positive experience for the merchant and consumer.

3 Technology

We have seen blockchains provide a secure tamper-resistant database. Operations performed are deterministic allowing for the history to be verified. Any client will be able to synchronize the blockchain to validate past transactions as well as confirm the validity of future transactions.

3.1 Centralized

Being backed by physical assets requires a strong authority to strive properly. These assets may be handled by third-party brokers which present a proof of ownership to the network authorities. The authority will have permission to mint new tokens and store the associated documents including the distribution of these tokens.

3.2 Smart Contract VM

The virtual machine is used to execute smart contract bytecode. In Regius Mark, a stack machine is used with a forth-like scripting language. The bytecode supports a minimal set of opcodes required for financial services without adding unnecessary functionality to accomplish our goal. The opcodes used must be deterministic based on the current state of the blockchain.

3.3 Wallet

Wallets have been increasingly becoming easier to use by the user for basic transactions. However, these interfaces are too simple for the power user. Our interface will be versatile to the varying scenarios from simple tasks to the complex. Performing complex tasks by the power user should be as straight forward as the novice sending a transaction.

The wallet experience and interface must be simple and intuitive for all users. Multi-signature wallets will be supported out of the box. A friend system can be used to create new wallets and sign a multi-signature transaction with the click of a few buttons. This system can also be used by merchants to accept payments and allow users to track who owns the address they sent the funds.

For our expert users, advanced options and script builders will be available. The UI will be simple yet feature rich to avoid hindering expert users and ease new users getting into advanced smart contracts.

3.4 Security

Blockchains inherently need to be a fortress. All transactions are signed to prove the authenticity of the owner to perform an action on the blockchain. Regius Mark will support multi-signature wallets and smart contracts where higher levels of security are necessary.

The centralized nature does not diminish the security of our infrastructure. The blockchain can be synchronized across the world in real time providing durability and tamper resistance as blockchain history cannot be rewritten. The master node will be using a multi-signature cold storage wallet and separate keys only for block production.

3.5 Transparency

Blockchains are naturally sequential and contain all the necessary data that pertains to the system. This allows us to easily distribute the block log without worrying about additional metadata. Any node operators will be able to synchronize the log and be able to remain in sync as new blocks arrive.

3.6 Minting

Blocks will be produced through a process called minting every three seconds. This process can only occur by use of a master node. The Regius Mark team will be the only master node on the network.

Unlike traditional cryptocurrencies with block rewards, Regius Mark does not partake in the creation of tokens unless explicitly created by a master node during minting a new block. This is a necessary step to ensure that we never overcommit circulating tokens, in this way we never exceed our physical asset reserves.

Minting transactions will contain data pertaining to a NI 43–101 report or any other document providing proof of ownership of physical gold.

3.7 Fees

Transaction fee costs start with a minimum fee. For every additional transaction accepted within the block window, the minimum fee is exponentially multiplied by the number of transactions accepted from the applicable address. The fee costs will reset back to the minimum fee after the block window is reset. The block window is reset when transactions are halted on the address for a period of time.

In addition to the address fee mentioned in the above paragraph, there is an associated "global" network fee. The network fee works in the same way as the address based fee and protects the network from flooding via multiple addresses. The global fee is dynamically adjusted based on network usage.

This quickly gets expensive for an attacker attempting to Denial-of-Service (DoS) the network, but allows flexibility for a normal user when waiting for the block window to reset back to the minimum fee is not an option.

Our fees will remain low because of our dynamic fee model allowing us to adjust costs based on network usage. Any fees collected will be rewarded to the network operators.

Sample based on transferring funds with a minimum fee of 0.0050 coins with a 1.5000 multiplier:

Fees	Block Height
0.0050	10
0.0075	11
0.0112	12
0.0050 ← block window reset →	20
Total Fees	0.0287

3.8 Message Signing

A signature is used to confirm the authenticity of the owner or owners of a particular message or document. Blocks produced by the minter and transactions created by the user are signed using the *Ed25519*[1] algorithm.

Ed25519 is a modern signing algorithm, it provides a similar protection level to NIST P-256 and has fast verification times with small signatures. This particular algorithm is capable of even faster batch verification using the Pippenger's method or the Bos-Coster method for scalar multiplication as mentioned in the Ed25519 paper.

Ed25519 has fewer attack vectors, such as resistance to side-channel attacks and attacks from poor random number generator implementations. While non-deterministic algorithms can suffer from hardware fault attacks, it is extremely difficult to successfully execute. Even with a server running without ECC memory the attack isn't practical in any way over the internet.

3.9 Scaling

Scalability can be achieved through vertical or horizontal machine deployment. Vertically scaling the hardware is easy to maintain, but the costs may become infeasible as hardware requirements increase to process the influx of transactions being added to the network. We will use horizontal deployment through different types of nodes that serve a specific function to spread the workload across multiple machines.

The majority of processing power required will be for transaction validation. We will use validator nodes to validate transactions being broadcasted to the network. The master node relies on the correctness of the validator to ensure that bad transactions cannot be added to the blockchain state.

3.9.1 Security

Each validator will contain an Ed25519 key utilized as an identity. The master node will send a challenge that the validator must sign to prove the machine is trusted. The link between the nodes must use the latest version of TLS to prevent any man in the middle or replay attacks.

External Links

- https://regiusmark.io
- https://github.com/RegiusMark

References

[1] J. Bernstein Daniel, Duif Niels, Lange Tanja, Schwabe Peter, and Yang Bo-Yin. *High-speed high-security signatures*. 2011. URL: http://ed25519.cr.yp.to/ed25519-20110926.pdf.