ESKENAS WHITE PAPER

Abstract

A fully private cryptocurrency and shielded blockchain deriving from the Komodo ecosystem. Eskenas solves Zcash's "fungibility problem" through the elimination of transaction functionality to transparent addresses in its blockchain, making private usage "fool-proof". This feature results in a fully shielded user coin base in Eskenas. By consistently utilizing zk-SNARKs technology, Eskenas leaves no usable metadata of user's transactions on its blockchain. All outgoing transactions other than mining block rewards and notary transactions are sent into shielded Sapling addresses maximizing the efficiency and speed of its chain. Eskenas utilizes the consensus algorithm Equihash proof-of-work originating from Zcash, with an added security layer of delayed proof-of-work from Komodo which provides a higher than BTC-grade level of security to the Eskenas blockchain. The future of private decentralized payments is here.

Table of Contents

The Eskenas Code

Mission Statement

The mission of Eskenas is to maintain people's financial privacy in a system dominated by transparent transactions, to ensure their financial freedom.

Value propositions

- All Eskenas transactions are private by default.

This alleviates the fungibility problems that many cryptocurrencies with optional privacy introduce into their protocol. This complete privacy protocol provides users with more assurance that no authorities are able to claim that user's funds are "tainted" due to previous transactions, now and in the future.

- Eskenas is fully decentralized

There is no third party handles your funds at any time. All transactions are private and validated with Eskenas blockchain meaning no third party is involved in the validation process. Private transactions are confirmed and processed by Eskenas code and its blockchain.

- Eskenas allows for secure and quick transfer of value

Eskenas uses delayed Proof-of-Work (dPoW) mechanism which makes it harder to crack and temper. The fee usage is very inexpensive for customers and vendors. Moreover, it is impossible for fraudulent chargebacks, no erroneous fund verification periods, and transactions are validated and secured within minutes. These characteristics can save customers and vendors around the globe billions of dollars by eliminating facilitation fees.

- Eskenas uses the strongest privacy protocol

The highly advanced and respected privacy protocol zk-SNARKs doesn't require the data from your transaction to be viewable on the public ledgers. This is considered by many prominent developers to be one of the strongest methods of hiding your financial data on the blockchain.

Why focus on privacy?

Crypto offers advantages to users and businesses, but this shouldn't come at the cost of financial privacy. Today's FIAT currencies are already making a mass exodus towards digital systems (Japparova en Rupeika-Apoga 2017). Crypto has shown to offer numerous advantages for business such as costsavings in fees and transaction speed. In our opinion, users deserve privacy in those transactions.

Why do you need to reveal your wealth to others?

Financial privacy may therefore be needed by all parties that want to accept cryptocurrency such as vendors, distributors, merchants, purchasers, suppliers, service providers and customers. Businesses can assure their clients and themselves that both parties to the transaction will receive the best combination of privacy, speed and cost-savings through using Pirate.

The Team

Being a truly decentralized cryptocurrency, Eskenas welcomes developers and contributors of all skillsets. Many contributors have provided services to the growth and development of Eskenas since its infancy, whether it be coding, marketing, development of partnerships or various other aspects. Developers are working in a coherent team fashion to bring in knowledge and experience from all parts of the crypto-sphere. With our diverse group, there is always a person with the knowledge of how to complete a needed task, or someone with a connection to someone who can. Eskenas has completed many first time accomplishments in the cryptocurrency industry when it comes to privacy protection (see Roadmap) and Eskenas will continue to work with third parties on innovative techniques to facilitate stronger privacy for all.

Introduction

Cryptocurrencies

Since the release of the famous whitepaper written by Satoshi Nakamoto in 2008 (Nakamoto 2008), Bitcoin has grown into a multi-billion dollar market cap digital asset. A number of alternative cryptocurrencies have spawned since then attempting to fill the void of a plethora of use-cases, with their own respective communities. Using cryptocurrencies as a means of payment is one of the most popular use-cases and also the main purpose for which Satoshi wrote the whitepaper. The goal of Bitcoin is to enable every person to transfer value anywhere in the world at any time instantly using an internet connection in a peer-to-peer, trustless fashion. Bitcoin utilizes a distributed ledger to facilitate and record transactions of which the truthfulness is determined through the consensus algorithm Proof-of-Work (PoW).

Privacy

One large concern about the usage of this technology is the ability of observers to analyze your spending behavior and wealth status (Moser 2013). This greatly compromises the financial privacy of the user. A number of cryptocurrency protocols have been developed that seek to improve on the privacy aspects of Bitcoin. The most notable protocols that have been developed thus far are CryptoNote (Van Saberhagen 2013) and Zerocash (Sasson et al. 2014). The first protocol utilizes Ring Confidential Signatures while the latter uses zero-knowledge proofs to obfuscate transactions and account balances, more in detail on that later. Both protocols have their advantages and disadvantages. This whitepaper addresses how Eskenas attempts to improve on the privacy aspects of current decentralized payment protocols.

Main drawbacks illustrated of current decentralized payment protocols

Monero Ring CT Signatures scheme

Monero, a fork of Bytecoin based on the CryptoNote protocol, utilizes a Ring Signature scheme in their transactions combined with stealth addresses, random one-time addresses for every transaction on behalf of the recipient. Ring signatures make it increasingly difficult to trace back the sender depending on the ring size. However, this leaves the ability of parties to analyze the available data with sophisticated analytic tools right now and in the future.

Due to its use of ring signatures, analysis of Monero's blockchain is difficult. The difficulty of finding the correct sender is increasingly difficult with bigger ring sizes. The ring size is the total number of possible signers including yours, which in turn determines the complexity and difficulty of finding the "real output". A higher ring size number thus provides a higher level of privacy than a lower number.

The fundamental problem of coin mixing methods though is that transaction data is not being hidden through encryption. RingCT is a system of disassociation where information is still visible in the blockchain. Mind that a vulnerability might be discovered at some point in the future which allows traceability since Monero's blockchain provides a record of every transaction that has taken place.

Zcash's shielded addresses implementation and spend types

Zcash, an implementation of the decentralized anonymous payment scheme Zerocash, adds a shielded payment scheme secured by zero-knowledge succinct non-interactive arguments of knowledge (zkSNARKs) to the existing transparent payment scheme used by Bitcoin (Hopwood et al. 2016). The usage of shielded or non-shielded payments is free to choose by the user. The percentage of shielded transactions is assumed to rise as Zcash's recent implementation of "Sapling" makes processing shielded transactions only a fraction more computationally intensive than non-shielded transactions (Bowe 2017). Unfortunately, the relative high percentage of non-shielded transactions and balances impairs the fungibility of the coins, as it is possible to link transactions during "private" payment activity and thus possibly relate them to coin mixing. This is especially the case when conducting a "round-trip transaction", meaning sending the exact number of coins from a transparent (t-addr) to a shielded address (z-addr) and back to another transparent address (Quesnelle 2017). This situation is referred as the "fungibility problem".

Zcash users are given the ability to conduct 4 different types of transactions in the current Zcash protocol. Being able to send from public to shielded address and vice versa greatly puts the fungibility of the coins at risk. It is possible to identify coin mixing patterns among the different types of transactions when users send coins back to transparent addresses, such as the case in "roundtrip transactions", as this behavior has been shown to exhibit high linkability (Quesnelle 2017).

The performance upgrades of Sapling unfortunately come at a privacy cost as Sapling transactions reveal more metadata than the "old" legacy JoinSplit operations. Sapling transactions show the number of inputs and outputs used. This functionality increases the options to differentiate between transaction types, analyze transaction data and possibly identify behavior related to mixing.

To reduce or eliminate this risk it is important to either reduce the usage of transparent addresses or simply disable it from the beginning in a new blockchain such as Eskenas.

Our Approach

Eskenas aims to improve substantially upon the privacy and security features of Monero and fix the "fungibility problem" of Zcash. Eskenas does this by means of only accepting "Sapling" shielded transactions (z-tx), apart from mining rewards and notarizations, as explained in the dPoW section. Additionally, Eskenas is secured through the delayed Proof-of-Work mechanism making its privacy and security features currently unmatched in the blockchain industry compared to existing privacy coins.

Eskenas: Privacy, fungibility and security

Komodo – Zcash fork – zk-SNARKs

Eskenas is an asset chain part of the Komodo platform ecosystem. The Komodo project focuses on empowering blockchain entrepreneurs and the average cryptocurrency user with freedom and ease of use through blockchain technology (Lee 2018). Komodo began as a fork of the popular privacy coin, Zcash. The Zcash project itself is a fork of Bitcoin. Thus, all the features designed by Satoshi Nakamoto in the Bitcoin protocol are also available in Komodo. As such, Komodo retains the same inherent privacy features as Zcash. Among these features are the Zcash parameters and zk-SNARKs technology. Zk-SNARKsis one of the most powerful forms of blockchain privacy in existence, as the provided privacy is effectively permanent.

Komodo Asset chains

An Asset chain is an independently created blockchain that inherits all of Komodo's features like BarterDEX compatibility, Zero Knowledge Privacy and delayed Proof-of-Work. but also has numerous custom specifications such as custom coin supply and custom RPC-port. Other examples of Komodo asset chains include ChainZilla (ZILLA), DEX, Equalizer (EQL), KMDice, Monaize (MNZ), PUNGO, REVS, SuperNET, Utrum and ZEX.

Forced z-transactions

“fungibility problem” is resolved by disabling the process of sending to visible addresses. This eliminates the existence of transactions from shielded balances to transparent balances which are often the root cause of decreased fungibility.

Delayed Proof-of-Work: Maximum security and flexibility

What is delayed Proof-of-Work?

Delayed Proof-of-Work stems from Komodo and provides a unique and innovative form of security which is as strong as the network it attaches to, yet does not require the cost to run that network. Delayed Proof-of-Work is a solution that utilizes multiple existing methods into a single hybrid consensus system that is as energy efficient as Proof-of-Stake (PoS), while being secured by Litecoin's Proof-of-Work. Users who build independent blockchains in the Komodo ecosystem can choose to have a block-hash, serving as a "snapshot" of their own blockchain inserted into the Komodo main chain. In this manner, the records of the asset chain are indirectly included in the block-hash of Komodo that is pushed onto the blockchain of one of the strongest networks (Litecoin).

What are the mechanics behind delayed Proof-of-Work?

The Komodo security service is performed by notary nodes which are needed to record block-hashes onto the Litecoin blockchain, referred to as notarization. Notarization entails the creation of a group signed Litecoin transaction containing the most recent block-hash of Komodo, signed by an unknown combination of 33 of 64 notary nodes. Block-hashes of Eskenas are inserted in the Komodo blockchain in a timely fashion as well using the same method. In this manner, even a single surviving copy of the Komodo main chain will allow the entire ecosystem of asset chains to overwrite and overrule any of an attacker's attempted changes. The notary nodes pay the Litecoin transaction fee for notarizing the Komodo blockchain. The Litecoin transaction fee costs for notary nodes is compensated for by block rewards and transaction fees of the Komodo blockchain going towards notary nodes. It is therefore expected that the financial interests of the stakeholders is to be voting for notary nodes that the stakeholders are comfortable with. 64 largely distributed notary nodes are up for election and are expected to be an optimal representation of a decentralized ecosystem making any type of 51% attack highly improbable.

Therefore, to carry an attack on Eskenas the attacker would need to destroy:

- all existing copies of the Eskenas;
- all copies of the Komodo main chain;
- the PoW security network (Litecoin) into which the Komodo blockchain notarized data is inserted.

Furthermore, notary nodes have the freedom to switch the notarization process to another PoW network if a shift in hash rates between the large blockchains occurs in the future. Delayed Proof-of-Work provides Eskenas with a higher than Bitcoin-level security, while avoiding the excessive financial and eco-unfriendly costs. Through dPoW´s flexibility it offers a more flexible and adaptive nature than Bitcoin itself.

Examples of attacks on blockchains

There are a number of examples which highlight the need for a mechanism like delayed Proof-of-Work:

In April 2018, a bug in the retargeting mechanism of the algorithms of Vergecurrency (XVG) was exploited by means of a 51% attack. Using spoofed timestamps, the need for a different algorithm each block was circumvented. The hackers were able to submit blocks to the chain at a mining speed of 1 block per second, effectively denying 99% of the legitimate pools' blocks and causing them to lose money (Ocminer 2018a). During May 2018 the same attack happened but with a different approach: hackers sent one block with Scrypt algorithm containing a spoofed timestamp followed by a block with Lyra2re algorithm containing a spoofed timestamp and by repeating that process and thus lowering the difficulty, the hackers were able to mine several blocks per minute (Ocminer 2018b).

On May 16 2018, Bitcoin Gold was attacked by an unknown actor who managed to steal over 388,000 BTG from cryptocurrency exchanges, the coins were worth 17.5 million dollars during the attack (Roberts 2018).

NiceHash currently offers more than enough hash power for rent to attack a number of small to midcap cryptocurrencies. The term "Nicehashable" has been coined for the ability to rent hash to attack a coin and sites have already popped up to showcase the hacking opportunities (EXAKING 2018).

Technical characteristics

Eskenas has these technical characteristics and features:

- Mining algorithm: Equihash Proof-of-Work
- Delayed Proof-of-Work
- Block-time: 60 seconds
- Transaction fee: 0.0001 ESK
- Transaction signing under seconds Transactions per second: 50–80 TPS
- Send to up to 100 addresses in a single transaction
- Tx sizes of +- 2000 bytes with a max. of 200 kB
- Memory usage of only 40 MB (Raspberry Pi) Block size of 4 MB maximum
- Viewing keys which offer the ability to see all sent transactions of an assigned address
- Ability to generate "endless" number of "Lite" wallets

Road Map

2021 December:

- First Block Mined
- Z Address Mining Pools
- Z Address Only Exchange Capabilities Initiated
- Full Node Wallet
- Onboarding Referral Program
- Website Updated

2022 January:

- Lite Wallet
- Android Wallet
- Gift Card Project

Eskenas Guide

Official Website
https://eskenascoin.com/

References

Jl777c. 2016. “Delayed Proof of Work (dPoW) Whitepaper”. Github. 2016. https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-(dPoW)- Whitepaper.

Nakamoto, Satoshi. 2008. “Bitcoin: A peer-to-peer electronic cash system”. Working Paper.

Ocminer. 2018a. “Network Attack on XVG / VERGE”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.0.

Roberts, Jeff John. 2018. “Bitcoin Spinoff Hacked in Rare ‘51% Attack’”. FORTUNE. 2018. http://fortune.com/2018/05/29/bitcoin-gold-hack/.

EXAKING. 2018. “PoW 51% Attack Cost”. 2018. https://www.exaking.com/51.

Quesnelle, Jeffrey. 2017. “On the linkability of Zcash transactions”. arXiv preprint arXiv:1712.01210.

Hopwood, Daira, Sean Bowe, Taylor Hornby, en Nathan Wilcox. 2016. “Zcash protocol specification”

Bowe, S. 2017. “Cultivating Sapling: Faster zk-SNARKs--Zcash Blog”. Zcash Blog.

Lee, James. 2018. “Komodo: An Advanced Blockchain Technology, Focused on Freedom.” Komodo. 2018.

Japparova, Irina, en Ramona Rupeika-Apoga. 2017. “Banking Business Models of the Digital Future: The Case of Latvia”. European Research Studies 20 (3A). Professor El Thalassinos: 846.