CredaCash – The Perfection of the Zero Knowledge Proof ™

Creda Software, Inc.

Abstract

CredaCash™ is a next generation cryptocurrency that is fast, scalable, and completely private. It achieves high-speed and complete privacy using an advanced implementation of zero knowledge proofs, and offers breakthrough features such as completely private multi-party escrow transactions and completely private cross-chain swaps. CredaCash is designed to meet the current and future needs of a digital economy, and is one of the most exciting and significant cryptocurrency releases since the introduction of Bitcoin. This paper describes the design and vision for CredaCash, its current status, and plans for an upcoming "ICX".

CredaCash Features

Crytocurrencies and blockchains have exploded in value since their introduction, while an ideal solution has yet to be found. CredaCash addresses a number of important features:

- Fast – CredaCash transactions are confirmed in seconds.
- Final – CredaCash transactions are final and irrevocable after one confirmation.
- Private – CredaCash transactions are completely private, including the transaction amounts and the sources and destinations of funds.
- Fungible – CredaCash tokens are effectively indistinguishable and have no "history" linking them to prior transactions.
- Low-cost – CredaCash transactions can be processed with minimal fees.
- Efficient – The CredaCash network requires as few resources as possible.

- Scalable – The CredaCash network scales to hundreds of transactions per second, and may someday scale to thousands.
- Non-custodial – CredaCash users have control over their own assets.
- Secure – Non-custodial assets have both benefits and drawbacks and very few cryptocurrencies have addressed the drawbacks. CredaCash provides tools to keep assets secure, recover assets if a wallet is lost, and ensure agents or heirs can receive assets if necessary.
- Decentralized – CredaCash depends on voluntary consensus with no control by a central authority.
- Censorship resistant – The CredaCash network is resistant to being censored, blocked or shut down by a corrupt or oppressive authority.

CredaCash Architecture

CredaCash primarily consists of two software programs: a network node server and a wallet. A user may run both programs on a single computer or on different computers. A user can also run only the wallet, and use it to connect to a public or private network node server.

The CredaCash Network Node Server

The network node server forms the backbone of a peer-to-peer network that broadcasts transactions and blocks to all other nodes. It also has the ability to act as a witness node to cooperatively create the blockchain, and it has a transaction server interface that can provide the information required by user wallets to send and receive transactions. Network nodes can connect to each other directly for high-speed operation, or over the Tor network for increased security and privacy.

The CredaCash Wallet

The wallet tracks user funds, receives incoming transactions, and creates and sends outgoing transactions. The wallet has a Remote Procedure Call (RPC) interface that implements a subset of the commands in the Bitcoin core wallet. It accepts Bitcoin RPC commands and turns them into completely private CredaCash transactions. The goal is to allow merchants and exchanges to connect existing backend systems to the CredaCash wallet and obtain the benefits of fast, final and completely private CredaCash transactions with minimal effort. The wallet can also be run interactively from the console, and it is fully multi-threaded to handle multiple simultaneous clients and requests. Mobile devices such as smartphones can access the wallet's RPC interface via the Tor network for increased privacy and security. The wallet uses the node server's transaction interface to obtain the information it needs to send and receive transactions, and can connect to a node server either directly, or over the Tor network.

The CredaCash Blockchain

The CredaCash blockchain uses permissioned witnesses for speed and security. The witnesses receive transactions from the relay network, assemble them into digitally-signed blocks, and broadcast the blocks to the network. The only function this fulfills is to place transactions in a sequential order, so that if two transactions attempt to spend the same token, only the first will succeed. Unlike Bitcoin, the protocol used by CredaCash ensures that the blockchain only advances forward and cannot revert. Any attempt by the witnesses to revert the blockchain would be rejected by the other network participants. All nodes on the network therefore work together to ensure the witnesses operate correctly.

In the future, the CredaCash project will implement as Proof-of-Stake protocol that allows all users to create and witness new blocks, and receiving mining rewards. This protocol has already been created and tested in a simulation environment, and like the current protocol, it is fast, final, secure, robust and resilient. Additional development is

needed to turn it into a fully functional Proof-of-Stake protocol that can operate with a privacy-preserving currency.

The CredaCash project also does not believe “one size fits all” when it comes to blockchains. The project envisions a future where thousands of blockchains all operate simultaneously and exchange transactions with each other similar to routing data on the internet. This would make it possible for any person or organization to set up their own public or private blockchain, with transactions seamlessly routed across a vast internet of multiple blockchains. It would provide massive scalability, as well as an ability to choose the best consensus protocol for each application.

CredaCash Zero Knowledge Proofs

One of the key technologies in CredaCash is a fast, efficient and powerful zero knowledge proof engine. The CredaCash zero knowledge proof uses zk-SNARK’s to create completely private transactions that keep the transaction amounts and the sources and destinations of funds completely private. It also prevents transactions from being linked, which results in tokens having no “history” and being completely fungible.

CredaCash’s zero knowledge proof also supports the following breakthrough features:

- Completely private tokenized assets. Up to 18,400,000,000,000,000,000 = 2^64 different tokenized assets can be created, with up to 340,000,000,000,000,000,000,000,000,000,000,000,000 = 2^128 total units of each asset, in fractional amounts down to 0.00000000000000000000000000000001 = 1E-31 of a unit. This is an unprecedented capacity and precision, and is designed to accommodate a wide variety of assets for the indefinite future. A single transaction can include multiple assets with both the asset identifiers and amounts kept completely private. This makes it impossible for someone who is not a party to a transaction to determine whether the transaction includes currency, assets, or some

combination, and in what amounts. This feature would allow digital or tokenized assets to be created on the CredaCash blockchain and traded through completely private transactions.

- Completely private escrow transactions. CredaCash supports completely private three party escrow transactions where a buyer and seller can settle an escrow transaction if they both agree, or either party can enlist the assistance of an escrow agent. These transactions are completely private and indistinguishable from non-escrow transactions. This would allow the creation of completely private escrow-mediated exchanges and marketplaces based on the CredaCash blockchain.

- Completely private on-chain swaps. CredaCash supports completely private swap transactions (also known as atomic swaps) where one asset is traded for another in linked transactions. These transactions are completely private and indistinguishable from other transactions, and the linkage between the transactions is private as well. This would allow the creation of completely private securities and commodities exchanges based on the CredaCash blockchain.

- Completely private cross-chain swaps. Significantly, CredaCash also supports completely private cross-chain swap transactions. For example, Bitcoin on the Bitcoin blockchain can be exchanged for CredaCash on the CredaCash blockchain in two linked transactions. These transactions are private as well: the transaction on the Bitcoin blockchain would appear to be one half of a swap transaction, but there would be no visible second half because the CredaCash transaction would be completely private and would contain no identifier linking it to the Bitcoin transaction. This would allow the creation of completely private peer-to-peer cross-chain currency exchanges that use the CredaCash blockchain as the medium of exchange.

- Multiple asset pools. More than one asset pool can be created on a single blockchain, allowing the possibility of different transaction processing rules for assets in each pool. One potential use would be to audit the total currency on the blockchain by requiring all assets to be moved from one pool to another in transactions that publicly publish the asset identifiers and amounts.

- Multiple hierarchical secrets, which include:

    - A master secret, if provided, that can be used to recover assets if the other secrets are lost. The intention is for the master secret to be written on paper and stored offline where it can be kept safe and retrieved only if needed.

    - Up to 7 spend secrets that can be used in "M of N" multi-secret transactions.

    - Up to 7 trust secrets that can be used in "S of T" multi-secret transactions. The trust secrets can be used as an alternate set of spend secrets in specialized transactions such as swaps. They can also be stored offline or provided to attorneys or heirs to administer assets if the owner is unable, or if the spend secrets have been lost. Transactions that use trust secrets are indistinguishable from transactions that use spend secrets, which keeps the use of the trust secrets completely private.

    - A monitor secret that allows transaction spends and receives to be monitored, but does not allow spend transactions to be created. The monitor secret may also be used to block unauthorized transactions and freeze assets if the spend secrets have been compromised.

    - A receive secret that allows incoming transactions to be processed, but does not allow spend transactions to be created or monitored. For

increased security, the receive secret can be used on an e-commerce server that is only allowed to receive transactions.

- Restricted output addresses that restrict the destinations to which a token may be sent. Restricted addresses are completely private, and tokens with restricted output addresses are indistinguishable from other tokens. This feature is used in completely private escrow transactions.

- Token lock times that prevent a token from being spent until a predetermined time in the future. The token can be subject to different lock times depending on whether the spend secrets or trust secrets are used to spend the token. This feature is used in completely private swap transactions.

- Token spend delay times that delay the effect of a token spent attempt, allowing the token spend to be cancelled or superseded by a more privileged transaction. The token can be subject to different delay times depending on whether the spend secrets or trust secrets are used to spend the token. Delayed token spends are not completely private because the delay time must be publicly published and enforced by the blockchain.

- Acceptance-required destinations. Destinations may be created that require transactions sent to that destination to be accepted before they become effective. These transactions are not completely private because the acceptance of the transaction must be enforced by the blockchain.

- External spend scripts. Tokens can be created that require external spend scripts, which in the future may be used for smart contracts or other applications.

Not all of the above features are currently supported by the wallet, but are all available to external scripts using a JSON API. Features that require enforcement by the blockchain are also not yet fully supported. The CredaCash project hopes these features are fully implemented by the wallet and blockchain in the future.

The CredaCash project has also developed a method for creating private "smart contracts". The project hopes this technology might someday be available to blockchain applications that require privacy-preserving smart contracts.

It is important to note that unlike most projects that use zk-SNARKs for privacy, CredaCash shares no code with Zcash. CredaCash's implementation of zero knowledge proofs was created and released to the public in 2015, before the Zcash project was even announced. CredaCash has never used the multi-party computation scheme that was recently found to cause a currency counterfeiting vulnerability in Zcash, since the CredaCash project considered this too experimental. CredaCash also uses none of the mathematics in the latest version of Zcash which it again considers too experimental and insufficiently tested. CredaCash has a much more conservative design philosophy and relies only on code and techniques that are as proven by time as possible. The zero knowledge proof engine in CredaCash is between 7 and 4 years old, and no vulnerabilities have been found. Despite this, CredaCash's zero knowledge proof implementation is very efficient and remains approximately five times faster than Zcash's latest release. CredaCash intends to continue this conservative design philosophy in order to ensure the most reliable blockchain and cryptocurrency possible.

CredaCash Vision and Future Plans

The CredaCash project strongly believes in freedom of choice. Consensus is a process determined by the voluntary participation of each user. Ultimately, users will choose the technology that works best for them.

The vision for CredaCash is to be the best possible medium of exchange: fast, easy and inexpensive to store, transport, authenticate, convey and keep private; resistant to damage, decay, loss, theft and extortion; completely fungible; impossible or impractical to counterfeit; readily available and widely accepted in exchange for goods and services that are part of everyday life.

Most of these attributes come from technology, and the technology developed for CredaCash provides a sound foundation, including its fast, scalable blockchain and the privacy of its zero knowledge proof. The rest—to be readily available and widely accepted—has to come from users.

Starting in June 2019, the CredaCash currency will be minted with 80% going to a non-profit Foundation. A portion of this currency will be presold to fund ongoing development, and the remainder auctioned in an "ICX" to fund the Foundation. The user community will be invited to participate in the currency mint and receive some portion. Information on the currency mint and Foundation ICX will be announced on the project website and newsletter.

Free and Open Source Licensing

"Free software" is software that respects users' freedom and community. As stated by the Free Software Foundation, "free software is a matter of liberty, not price", in particular, the freedom to "run, copy, distribute, study, change and improve the software". Some Free and Open Source licenses, such as the GNU General Public License, are "copyleft" licenses. They allow a program to be modified, and they impose a requirement that any modifications must be released under the same license.

The CredaCash software will have a similar Free and Open Source license, with a primary focus on the freedom to use the CredaCash currency. More specifically, the license will allow the CredaCash software to be run, copied, distributed and modified for any purpose. It will allow new assets, blockchains and networks to be created, existing blockchains to be forked, new features to be added and new consensus rules selected or implemented as desired. There will be no requirement that modified versions of the software be released open source—users may elect to release their modified versions open source, or keep them proprietary—however, there will be a requirement that any modified versions continue to support the CredaCash currency on a non-discriminatory basis. The goal of this license will be to ensure that the freedom to

use the CredaCash currency will be passed on and preserved for all holders of the currency, no matter when they acquire it. The specific details and language of the license will be published prior to the Foundation “ICX”.

Conclusion

CredaCash is fast, final, completely private, and offers a combination of advanced features currently not available in any other cryptocurrency, such as completely private multi-party escrow transactions and completely private cross-chain swaps. It is designed to meet the current and future needs of a digital economy. The initial release is planned for June 2019.

More information is available at the project website: **https://CredaCash.com**