CredaCash™ – A Next Generation Cryptocurrency

Creda Software, Inc.

Abstract

CredaCash™ is a next generation cryptocurrency with increased speed, privacy, reliability, scalability and efficiency. CredaCash uses "zero knowledge proofs" to keep transactions private, it uses a small set of witnesses to rapidly assemble the blockchain, and it introduces the concept of "indelible" blocks that are permanent and cannot be amended or replaced. CredaCash also supports a transaction API that allows lightweight wallet applications to securely and privately send and receive payments. The result is a cryptocurrency that meets the current and future needs of a digital economy.

Introduction

The first cryptocurrency, Bitcoin, was introduced in 2008. Bitcoin allows divisible units of value called "bitcoins" to be used as payment for goods and services, exchanged for other currencies, and sent to other users worldwide. There are currently over 14 million bitcoins in existence trading at a value near US$400 per bitcoin, for a total "market cap" over US$6 billion.

This paper looks at Bitcoin and some of its limitations, and then introduces a new cryptocurrency called CredaCash that attempts to address these limitations.

Bitcoin

In Bitcoin, transactions transfer value from one or more inputs to one or more outputs. For a transaction to be valid, the sum of the input amounts must be greater than or equal to the sum of the output amounts. The difference between the two is an optional "fee" paid to the "miner" who incorporates the transaction into the blockchain.

An output is represented by an amount and an “address” formed from the hash of a public signing key. An output is spent by using it as an input in a new transaction and digitally signing the new transaction with the output’s signing key. Thus, only the holder of the signing key can spend an output.

In order to allow only valid transaction outputs to be spent, and to prevent a valid output from being spent more than once, transactions are submitted to the network and assembled into blocks by “miners”. The blocks serve as a public ledger of all accepted transactions. An attempt to spend an output that was not recorded in the ledger, or that has already been recorded as spent, is rejected.

For a block to be valid, it must contain a solution to a cryptographic puzzle called a “proof-of-work” that can only be found by trial-and-error. The threshold difficulty of this puzzle is periodically adjusted so that it takes an average of roughly 10 minutes for some miner on the network to produce a new block. That miner is permitted to harvest the “fee” amounts in the included transactions, and create new bitcoins for itself called a “reward”.

Blocks are broadcast to the network and assembled into a sequential blockchain by each individual network node. Each block created by a miner references a single prior block. The sequence of blocks, from one block to each of the prior blocks in order, forms a blockchain. Miners are not however required to build a new block on top of the last block in a blockchain—they can build on any block. They might do so based on their mining strategy (to build all the blocks in a segment of the chain so they gain all of the mining rewards), or because they did not see a later block due to network transmission errors or delays. When multiple competing blocks or chains appear, the network nodes will chose the one with greatest “total difficulty”, which is defined as the difficulty of reproducing all of the puzzle solutions in the chain. That choice is not fixed however—the total difficulty of any chain can be increased by adding more blocks to it. Thus, at times, a node can track one chain as best, and then suddenly switch to a competing

chain when a block is added that makes that chain's total work greater. When a switch is made, all of the blocks in the lesser chain are disregarded, and if that chain included transactions not in the new chain, those transactions suddenly go from a "confirmed" state to an unspendable state. It is believed in the Bitcoin community that the likelihood of a block being suddenly replaced by an alternate block is inversely exponentially proportional to the length of the chain subsequent to that block. To account for the possibility of a new chain suddenly replacing the existing chain, the Bitcoin community recommends waiting for 6 to 100 "confirmation" blocks (from 1 to 17 hours) before accepting a significant payment. That recommendation is based on assumptions that are not guaranteed by the protocol, and it is possible and allowed by the protocol for the behavior of the blockchain to change unpredictably at any time.

Bitcoin Advantages

The primary advantage of Bitcoin over "fiat currency" and the traditional banking system is that it allows units of value to be inexpensively sent anywhere in the world. For example, while a traditional international wire transfer might cost over US$25, a Bitcoin transaction costs only a few cents.

Part (if not all) of this advantage comes from Bitcoin's low overhead. Unlike a traditional bank, the Bitcoin network does not require a large staff to set up accounts, issue statements, handle customer service, investigate disputes, perform chargebacks, etc. In Bitcoin, all transactions are intended to be non-reversible. Some would say this is a disadvantage for payment senders, since they have no mechanism within the Bitcoin network to get their money back if there is a problem. However, if that were a desired feature for a particular transaction, the payment sender could presumably engage a third party to provide these services in the form of escrow, insurance, etc. That would increase the transaction cost, but only for transactions that need it.

Bitcoin Limitations

The biggest limitations of Bitcoin are its slow speed and lack of a definitive point in time that a transaction can be considered confirmed and non-reversible. As mentioned above, the blockchain does not advance in a linear fashion. At any point in time, there can be multiple competing chains, and a sudden switch from one chain to another can occur at any time. That has led the Bitcoin community to recommend waiting for 1 to 17 hours before considering a transaction to be cleared. Even after that wait however, the protocol does not prohibit a switch to a different chain—it is simply believed to be unlikely based on certain assumptions and operating experience. It would be desirable to have a cryptocurrency with a faster confirmation time, and a definite point in time at which a transaction becomes permanent and irrevocable.

Another related potential limitation in Bitcoin is the potential for a "hard fork" or split in the blockchain. A hard fork can occur when network problems or software incompatibility cause some participants to follow one chain while another set of participants follow a different chain. A hard fork has happened at least once before after a software update, and may happen again in the future. The risk to participants is that the resolution of a hard fork can cause transactions to become invalidated days after they appeared to be confirmed. Browsing the historical Bitcoin discussion forums finds many mentions of forks or potential forks and the need for users to be wary of accepting transactions until the issue is resolved. It would be desirable to have a cryptocurrency that is not prone to forks in the blockchain.

Another limitation in Bitcoin is a lack of privacy and the traceability of transactions. In Bitcoin, any person is able to see the details of every transaction: the transaction amounts, the source of funds and the payment addresses. Single-use anonymous payment addresses help provide some level of privacy, and proposals have been made to address this issue outside Bitcoin by pooling and mixing coins. It would be desirable to have a cryptocurrency that offers a higher level of privacy.

A related problem is that every bitcoin in the system has a unique history that can be traced by anyone from its creation to its present owner. That potentially allows users to "blacklist" or discriminate against some coins based on their history, making them more difficult to spend and potentially less valuable. In such a situation, users would have to consider each time they accept a payment whether the particular coins tendered by the payor might at some time become devalued because they do not have a clean history. It is a desirable property in any currency that all valid units are completely fungible and indistinguishable so that once they are lawfully accepted, users do not have to worry about the units' past histories and whether that could devalue their holdings.

A final limitation is efficiency. The Bitcoin network currently pays approximately US$525,000,000 worth of bitcoins to miners each year in rewards for creating new blocks. The majority of that is spent on electricity to create and power the mining hardware, in most cases using carbon-based fuels or energy that could displace carbon fuels. It would be desirable to have a cryptocurrency that were more energy efficient and eco-friendly.

CredaCash

Let's start by discussing the CredaCash system and architecture, then its performance and advantages.

The most important components in the CredaCash network are:

- A relay network that transmits transactions through the network where they are assembled into blocks, and transmits blocks back to the system participants.
- A witness system that assembles transactions into blocks.
- A transaction verification system based on "zero knowledge proofs" that allows transactions to be validated while maintaining privacy.

- Transaction servers that assist lightweight wallet applications to send and receive payments.

Transactions

Like Bitcoin, the CredaCash system consists of transactions that contain one or more inputs and one or more outputs. The outputs from one transaction are used as inputs in a subsequent transaction. A transaction transfers all value from the inputs to the outputs, and after the transaction is processed, the inputs cannot be used again in another transaction. To enforce this, transactions are assembled into a sequential blockchain that serves as public ledger and provides a list of the outputs that can be spent and the outputs that have already been spent.

Relay Network

The relay network is a highly-interconnected peer-to-peer mesh network. For both privacy and security, all communication between nodes occurs over the Tor network using Tor hidden services. Nodes find each other by registering their Tor onion addresses with a randomly chosen directory server, and in return receive a list of randomly chosen peers. Each node then connects to 6 to 12 peer nodes, and they exchange transactions and blocks using an announce-and-request flooding protocol, where each node requests transmission of objects it does not already have.

Witnesses

The witnesses receive transactions from the relay network and assemble them into blocks. The blocks are digitally signed with the witness's signing key. One block builds upon another, forming a blockchain. The witnesses work round-robin, each adding a block to the blockchain in turn. If one or more of the witnesses are offline, they are skipped, as long as a minimum number of witnesses remain operational. If too many witnesses are off-line, the remaining witnesses will pause operation and the

advancement of the blockchain will also pause until one of the missing witnesses resumes operation.

The blocks are sent back across the relay network to the other nodes. When a sufficient number of blocks have been added that "confirm" a block, that block becomes "indelible". At that point, under the rules of the protocol, the block is permanent and will never be replaced by a different block. The transactions within the block are then said to have "cleared", since they are also permanent and nonreversible.

The system is designed to operate correctly in the presence of some number of malfunctioning or even maliciously operating witnesses, as long as at least a majority of the witnesses are operating correctly. In addition, each node on the network validates all blocks before accepting them, and if a block is invalid or signed by a witness out-of-turn, the block is rejected. If the witnesses as a group attempt to create a block that would replace an indelible block, the network nodes will refuse to accept the conflicting block and will halt any further acceptance of blocks and advancement of the blockchain until the issue is resolved. All nodes on the network therefore work together to keep the witnesses "honest" and ensure they operate correctly.

Zero Knowledge Proofs

In the CredaCash transactions, the source of funds, the destination address, and the input and output values are kept private using a "zero knowledge proof". The zero knowledge proof allows the network and any person using the network to verify the validity of a transaction without accessing the private data. The CredaCash zero knowledge proof system is similar to the one proposed for "Zerocash" which to date has not been implemented in a working system. Simplified to its essence, a payment sender commits to a spend_secret and value by publishing a "commitment" in the blockchain, where

commitment = hash(value, hash(spend_secret))

When the recipient wants to spend the payment, he publishes a “serial number” in the blockchain where

serial_number = hash(commitment, spend_secret)

The key to making this work is the zero knowledge proof. The zero knowledge proof connects the serial number with the commitment without publicly revealing the connection. In order to construct the zero knowledge proof, the spender has to provide a spend_secret and value that satisfy the above equations, along with the path of the commitment in a Merkle tree containing all commitments. The zero knowledge proof proves that:

- The commitment path hashes to the global Merkle root, and therefore the commitment belongs to a valid payment.
- The spender knows the spend_secret that corresponds to the commitment, and is therefore authorized to spend the payment.
- The serial number and commitment were created from the same spend_secret, and therefore the serial number belongs to the same payment as the commitment.
- The value used when spending the payment is the same value used to create the payment.
- The sum of all the input values in the transaction equals the sum of all the output values.

The zero knowledge proof allows any node in the network to verify the above conditions hold without revealing the spend_secret, payment value, or Merkle path that the spender input into the proof—the only information another user is able to determine is whether the transaction satisfies the conditions or not; the hidden values used to satisfy the conditions are kept private and not published. Along with verifying the zero knowledge proof, every node on the network also verifies that the serial_number

published in the transaction has not been already spent in an earlier transaction in the blockchain. This prevents a payment from being spent twice. The serial number cannot however be publicly connected to the commitment published in a prior transaction because the two are not published together in the same transaction, and the only information that ties them together, the value and spend_secret, are kept private by the zero knowledge proof and never published.

The Merkle tree containing all commitments and the list of spent serial numbers are large datasets that would potentially grow without bound as transactions are published. To keep the size of the tree manageable, all outputs have to be spent or rolled over into new commitments within 5 years. This allows commitments and serial numbers older than 5 years to be removed from the active datasets. An additional transaction type is contemplated to spend expired commitments, but it would come with a considerably higher processing cost.

While not shown here but discussed further in an accompanying paper, CredaCash also has the ability to allow multi-signature transactions and signature checking scripts, similar in style to Bitcoin.

Transaction Server and Wallet API

In order to create a transaction, a Merkle tree of all commitments must be maintained in order to compute the path from an input commitment to the Merkle root. Even with the expiration of commitments, this is expected to be a larger data structure than many wallet applications will want to maintain. In order to allow lightweight wallets to create transactions, CredaCash provides a transaction server to obtain the necessary information. When a wallet wishes create a transaction, it first contacts a transaction server at a Tor hidden service address and requests the Merkle paths from one or more input commitments to the Merkle root. If the wallet trusts the transaction server to keep its requests private (for example, if the transaction server is run by the user itself, or by

a trusted party), the information returned by the transaction server can immediately be used to construct a transaction.

If the wallet does not trust the transaction server, maintaining complete privacy requires a little more work. In that case, the wallet cannot simply construct a transaction using the Merkle root returned by the transaction server because the server might correlate the Merkle root it provided with the Merkle root published in the transaction, thereby linking the transaction inputs and outputs and partially compromising privacy. To maintain complete privacy, a wallet can request the Merkle path for each commitment one at a time, possibly from different transaction servers and/or at different times in advance of their use. When ready to spend the outputs, the wallet would query the transaction server to obtain only the path inputs that have changed since the earlier queries. Since the changed entries would be toward the root of the tree and span many commitments, the transaction server would be unable to identify the specific commitments the wallet is updating. The wallet then constructs a spend transaction with the updated paths.

After a transaction is constructed, the wallet submits it to a transaction server where it is forwarded throughout the network. If desired, after a short wait, the wallet can query the transaction server again to see if the transaction has cleared, i.e., if it has been entered into an indelible block in the blockchain and is therefore permanent and nonreversible.

Performance

CredaCash had been deployed on the internet in a test network. The time to construct a transaction depends primarily on the speed of the host machine and the number of input serial numbers. Using a single core of an Intel Core i5-520M @ 2.4 GHz (a circa 2010 midrange laptop CPU), the time to generate a zero knowledge proof is roughly 3.8 seconds per input and 0.20 seconds per output.

The time to submit and clear a transaction on the test network is approximately 20 seconds. The primary speed limitations come from the time required to establish Tor connections and the latency across the Tor network of the relays' announce-and-request protocol. With optimization, that time can likely be cut to just several seconds. The eventual goal is to make the blockchain function more like a ticker tape with a constant stream of blocks.

Furthermore, in point-of-sale applications, it is often not necessary to wait for a transaction to clear. If some level of risk is acceptable, transactions can be sent directly from the customer's wallet to the merchant, checked for validity, and then accepted immediately without waiting for them to clear. This would be nearly instantaneous once the transaction is created. To strengthen that process somewhat against double-spend attacks, the merchant could also monitor the network to ensure the transaction does not include an input serial number that is listed in any other transaction being relayed around the network, or, for higher value transactions, the merchant could wait for the transaction to be incorporated into at least one block before proceeding.

CredaCash Advantages

As shown above, CredaCash has several advantages over Bitcoin:

- Speed: CredaCash cuts transaction clearance time from hours to seconds.
- Reliability: CredaCash provides a clear point in time at which a transaction is permanent and irreversible; Bitcoin provides none.
- Privacy: Transaction amounts and the source of funds are kept private.
- Fungibility: All valid CredaCash are identical and completely fungible.

- Low fees: CredaCash shares Bitcoin's advantage of low transaction processing costs.

- Highly scalable: CredaCash can scale to sub-second block times. If the Bitcoin protocol were run at that speed, it would degenerate into chaos.

- No forks: The witness protocol ensures all nodes on the system follow the same blockchain.

- Efficiency: The total electricity used by the CredaCash' witnesses is likely to be measured in the thousands of dollars per year, while Bitcoin miners likely consume over $200 million per year in electricity, with a commensurate impact on the environment.

Conclusion

CredaCash offers a combination of unique features currently not offered by any other cryptocurrency and is well-suited to meet the current and future needs of a digital economy. As of the date of this paper, CredaCash is in technology-preview state, and further information is available at https://CredaCash.com