MAIN PAGE

Counos Coins

Do your transaction secure and fast

Counos Coins Subtitle

Based on Blockchain technology we made a new way that can be used to pay your financial purchase safe, fast and anonymously in any place and any time.

Conous Coin Introduction

Counos Coin was developed for use by everyone and everywhere in the world. Counos Coin provides the freedom in the financial operation by the safety transaction over the world and their own Exchange companies and Agents. From the basics of Money to the modern electronic currency which is independent of any monetary system and any banks Counos Coin introduces the no limit world without banks and determination of the user of the currency by specific country (Euro in Europe, Dolar in the USA). Imagine you can travel anywhere just with your electronic wallet. Use it for peer-to-peer transactions, sending and receiving the counos coin anywhere and pay in every shop almost for free. That is the world Counos coin is creating.

How does IT work?

Cryptocurrency is a digital currency which formed on top of the blockchain technology and based on its decentralized structure, record all transaction by a hash of its transaction details and store if on all nodes in the network.Counos Coins is a cryptocurrency like BitCoin. It has about 21 million coins in its network, and until now more than16.800.000 coins minded and about 4.200.000 coins left. You may join our system to make it more secure, get an award for mining and do your transaction, safe and quickly. For more information (link to whitepaper)

DOWNLOAD the CounosWallet

By using one of our services, you may receive, transfer or store Counos coins by CounosWallet.

Our software will create a unique address and wallet for yourself Concept. By asking your business partner wallet address, you can send your coin's balance to Your BP. You can receive, transfer or store all your coins safetly and fast ever possible. The software is compatible with other coins so don't be worry you don't need to have more than one wallet. To get our wallet is as easy as to download any application and free. *Download for mobile and desktop (hide link to application)*

Counos Coin network

We create our cryptocurrency based on Blockchain technology

Your BP may sell

Coins to our Representatives and load his/her bank accounts. Counos GmbH will Guarantee to redeem of coins.

As a decentralized network, all nodes will maintain a copy of all transaction history, and a full ledger will be copied and secured to each node.

We follow concepts and rules Bitcoin define for sending and receiving coins.

If you have a question about Counos-Coin, feel free contact us.

Rigiweg 2

CH-6354 Vitznau

Switzerland

Tel:  +41 445869796

Fax: +41 442742029

Cell: +41 789040995

www.counos.io

WHITEPAPER

Overview

A purely peer-to-peer version of an electronic payment method would allow online payments to be sent from one party directly to another without going through any financial institution. Digital signatures are part of the solution, but the main benefits are lost if a trusted third party continues to be required to prevent double spending.

We suggest a solution to the double-spending problem by using a peer-to-peer network. The network timestamps transactions by hashing them into a continuous chain of hash-based proof of work, creating a record that cannot be changed without recreating the proof-of-work. The most extended chain not only serves as proof of the sequence of witnessed events but also as proof that it comes from the largest pool of CPU power.

As long as the majority of CPU power is controlled by nodes that do not cooperate to attack the network, they will generate the most extended chain and be faster than the attackers. The network itself requires only a minimal structure. Messages are transmitted on a best-effort basis, and the nodes can arbitrarily leave and re-enter the network, accepting the longest proof-of-work chain as proof of what happened while they were away.

As much important as safety is how fast you will receive or transfer your coins. Counos coin platform garantee that transaction will be done in up to 10 minutes from or to any place in the world.

1.Introduction

It has become apparent that Internet commerce is now almost entirely based on the fact that financial institutions serve as trusted third parties to process electronic payments. While this system works well enough for most transactions, it still suffers from the weaknesses of a model based on trust. Entirely irreversible transactions are not possible, as financial institutions cannot avoid mediating in disputes. The cost of the broker increases the value of the transaction, raising the minimum size of feasible transactions and eliminating the possibility of small opportunity transactions. Greater harm is also caused by the elimination of the chance of making irreversible payments for irreversible services. The option to undo transactions increases the necessary trust. Traders need to be suspicious of their customers and ask them for more information than they would otherwise require. A certain amount of fraud is accepted as unavoidable. These costs and financial uncertainties can be avoided by personal contact and the use of physical currency, but there is no mechanism for making payments over a communication channel without a trusted party.

What is needed is an electronic payment system based on cryptographic evidence rather than trust, allowing two willing parties to conduct transactions directly with one another without the need for a trusted third party.

Transactions that are computationally impossible to revoke would protect sellers from fraud, and standardized trust mechanisms could be easily implemented Transactions that are computationally impossible to revoke would protect sellers from fraud, and standardized trust mechanisms could be easily implemented to protect buyers. In this paper, we propose a solution to the double-dispensing problem that generates computational evidence of the chronological order of transactions using a distributed peer-to-peer timestamp server. The system is secure as long as the honest nodes control more CPU power than any cooperating group of attacking nodes.

2. Transaction

We define an electronic coin (Counos coin) as a chain of digital signatures. Each owner transfers the coin to the next one by digitally signing a hash of the previous transaction and the next owner's public key and appending it to the end of the coin. The recipient of the payment can verify the signatures to verify the chain of owners. The problem, of course, is that the payee cannot verify that one of the owners has not duplicated the coin.

One standard solution is to introduce a central, trustworthy instance, or mint, that checks each transaction for double-spending. After each transaction, the Coin must be returned to the Mint for a new Coin to issue, and only Coins issued directly from the Mint can be trusted to have not been duplicated. The problem with this solution is that the fate of the entire monetary system depends on the company running the mint and that transaction has to go through it like a bank. We need a way to assure the payee that the previous owners did not sign previous

transactions. For our purposes, the first transaction is the one that counts, so we do not have to worry about later multiple-issue attempts. The only way to confirm the absence of a transaction is to know all transactions.

In the mint-based model, the Mint knew all the transactions and could decide which ones arrived first. To do this without a trusted party, transactions must be made public [1], and we need a system whereby subscribers agree on a single history of the order in which they arrived. The payee requires proof that at the time of each transaction, the majority of the nodes of the network agree that they have received them first.

3. Timestamp server

The solution we have proposed starts with a timestamp server. A timestamp server works by taking the hash of a block of time-stamped records and publishing the hash widely, such as in a newspaper or a Usenet post [2-5].

The timestamp proves that the data existed at this point, obviously, otherwise, there would be no hash of them. Each timestamp contains the previous timestamp in its hash and forms a chain where each additional timestamp strengthens the previous timestamps.

4. Transactions Are Confirmed In Record Time

On the bitcoin platform, transactions are confirmed in an average of 10 minutes. To further ascertain that these transactions cannot be reversed, users are advised to wait till more blocks are added to the chain. This takes an average of one hour. Whereas on the Counos platform, transaction confirmation time takes around 2min 30secs. Therefore, time-sensitive transactions can be made using the Counos platform

5. It Is a Decentralized Network

Like bitcoin, Counos boasts of a system that is not owned or controlled by an entity. Therefore, transactions made on the platform are not controlled by any central figure. This system guarantee users that transaction fees are immensely reduced. Also, transactions can be made anywhere in the world at any time.

6. Counos Coin System Is a Deflationary Coin

There two major types of cryptocurrencies.

- Inflationary coins: these are coins that the reward for mining increases over time. Therefore, the supply of the coins increases until it reaches its maximum supply. This type of coin generally tends to lose value
- Deflationary coins: the reward for mining this type of coins reduces over time. Hence, the scarcity of such coins increases its value.

The maximum supply of Counos is 21 million coins, and there is about 16,800,000 Counos coin already in circulation and 4,800,000 is available for mining. Hence, Counos coin will be reaching it max supply soon. And when this happens, the odds that it will lose it value is greatly reduced.

Other tokens in the platform are Counos cash, Counos gold, and Counos silver. These tokens are tailored for specific purposes, Counos cash is a premined token that guarantees a fixed and regulated price. Counos gold and Counos silver are engineered to mimics the price trends of gold and silver respectively.

7. Proof-of-Work

To implement a peer-to-peer distributed timestamping server, we need to use a proof-of-work system, similar to the Adam Back hash system [6], instead of the newspapers or Usenet posts. The proof-of-work involves finding a value where, when it is hashed, such as through Script –an algorithm which uses SHA-256 with extra work-, the hash begins with a count of zero bits. The average work required is exponential to the number of zero bits needed and can be verified by the execution of a single hash.

For our timestamp network, we implement the proof-of-work by raising a nonce in the block until a value is found that gives the hash of the block the necessary zero bits. After the CPU has put in enough work to do the proof-of-work, the block cannot be changed without running the job again. Since later blocks are chained to it, the work to improve the block would involve recreating all subsequent blocks. The proof-of-work also solves the problem of determining the majority in majority voting. If the majority was based on one vote per IP address, it could be infiltrated by anyone who can reserve many IPs. Proof-of-work is one vote per CPU.

The majority vote is represented by the most extended chain in which the largest proof-of-work effort was invested. If a majority of CPU power is controlled by honest nodes, the reliable chain will grow fastest, and all competing chains will depend. To change a past block, an attacker would have to recreate the proof-of-work of the block as well as all subsequent blocks, and then catch up with and overtake the honest nodes. We will demonstrate later that the more blocks that follow, the less a slower attacker can catch up, the more exponentially it decreases.

To compensate for increasing hardware performance and time-varying interest in operating a working node, the proof-of-work difficulty is determined by a moving average, which is an average number of blocks per hour. If they are generated too fast, the difficulty increases.

8. Network

The steps to operate the network are as follows:

1. New transactions are broadcast to all nodes.

2. Each node collects the late transactions in a block.

3. Each node is working to find hard proof of work for its block.

4. When a node detects evidence of work, it sends out the block to all nodes.

5. The nodes accept the block only if all transactions in it are valid and not already issued.

6. The nodes express their acceptance of the block by working to create the next block in the chain, using the hash of the current block as the previous hash.

Knots always assume that the longest chain is the correct one and are working to extend it. If two nodes simultaneously transmit different versions of the next block, some nodes might receive one or

the other version first. In this case, they work on the first one who received them but save the other branch in case it gets longer.

The tie is broken when the next proof of work is found, and a branch gets longer; the nodes that worked on the other branch will then switch to the longer one. The broadcasting of new transactions does not necessarily have to reach every node. As long as they reach many nodes, sooner or later they will be taken up in one block. Block emissions are also tolerant of lost messages. If a node does not receive a block, it will request it as soon as it receives the next block and recognizes that it is missing one.

9. Incentives

By convention, the first transaction in a block is a special transaction that gets a new coin owned by the creator of the block. This gives new nodes an incentive to support the network and provides a way to get coins into circulation for the first time because there is no central instance issuing them. The constant

addition of a constant number of new coins is analogous to gold miners who spend resources to bring more gold into circulation. In our case, it's CPU time and electricity spent. The incentives can also be promoted by transaction fees.

If the initial value of the transaction is less than its input value, the difference corresponds to a transaction fee added to the value of the stimulus of the block containing the transaction. Once a predetermined number of coins have been put into circulation, the incentives can be completely transferred to transaction fees and thus completely free from inflation. The incentives can help to motivate knots to stay honest.

If a greedy attacker is capable of delivering more CPU power than any honest node, he would have to choose whether to use that power to cheat people by stealing his payments back or using them for new coins to create.

He should find it more profitable to abide by the rules - rules that can provide him with more new coins than any other together - rather than undermine the system and thus the validity of his wealth.

10. Win back storage space

Once the last transaction of a coin has been buried under sufficient blocks, the user transactions can be deleted beforehand to save storage space. To do this without breaking the hash of the block, the transactions are hashed in a Merkle tree [7] [2] [5], and only the root has been included in the hash of the block. Old blocks can then be compressed by cropping branches of the tree. The internal hashes do not need to be saved. A block header without transactions requires about 80 bytes. Assuming that blocks are generated every five minutes, 80 bytes * 12 * 24 * 365 = 8.4 MB per year. With computer systems typically sold with 2GB of RAM

per year (as of 2008) and Moore's Law, which currently anticipates growth of 1.2GB, disk space should not be a problem, even if the block headers need to be kept in memory.