Maiscoin A Privacy-Centric Crypto-Currency

Abstract. A cryptocurrency based on Bitcoin, the work of Satoshi Nakamoto, with various improvements such as a twotier incentivized network, known as the Masternode network. Included are other improvements such as Darksend, for increasing fungibility and InstantX which allows instant transaction confirmation without a centralized authority.

Introduction

- Mais Coin has the support of Mais Bank
- The MaisCoin professional team joins the Mais Bank team to make a successful Dream Team.
- Mais Bank is a pioneer in offering new financial products based on cryptocurrencies.

  The first are in the Cryptocurrency Maiscoin:

  1. Deposit at 12 months with a high monthly return. Minimum capital is 10,000 USD. in mais coins

  2. Deposit to 90 days. From 5,000 usd. in mais coins

  3. Deposit to 30 days. Minimum investment of 3,000 usd. in mais coins

  4. 60-day equity deposit with daily yield and weekly collection. Minimum amount of 1,000 usd. in mais coins

  The characteristics of the deposits are:

  - the yields are guaranteed for the contracted period and are published on the website of https://www.maiscoin.space
  - investment is in MaisCoin
  - income payments are made in MaisCoin
  - the Mais coins can be changed in https://beta.wavesplatform.com/ and in the exchange that already counts maiscoin.space website

- We are currently developing a own crypto processor that will see the light within the next 6 months
- We finance innovative and profitable projects presented by entrepreneurs.

- To the businesses and companies that want to adopt maiscoin as a way of billing solution for their products and services we offer an attractive and profitable proposal.

- Individuals who want to serve as https://beta.wavesplatform.com agents who promote our product portfolio are offered a very interesting incentive plan.

- For investors in cryptocurrency, maiscoin is a financial asset with an extraordinary possibility of growth in short-term value that makes it exceptional.

- To the issuers of other cryptocurrencies we offer the possibility of developing new financial products based on them. We are open to mutually beneficial arrangements.

Technical details

MaisCoin (MSC) is a privacy-centric digital currency with instant transactions. It is based on the Bitcoin software, but it has a two tier network that improves it. Maiscoin allows you to remain anonymous while you make transactions, similar to cash.

With Bitcoin, transactions are published to the blockchain and you can prove who made them or to whom, but with MaisCoin the anonymization technology makes it impossible to trace them. This is important because the blockchain is accessible to anyone with an internet connection – a significant drawback for those don't wish their transaction history and balances to be publicly available.

MaisCoin does this through a mixing protocol utilizing an innovative waves decentralized network of servers called Masternodes, avoiding the need for a trusted third party that could compromise the integrity of the system.

MaisCoin transactions are almost instantly confirmed by the Masternodes network. This is a great improvement on Bitcoin's system, where confirmations take much longer because all the work is done by the miners.

- X11 hashing algorithm: 11 rounds of scientific hashing functions (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo)
- CPU/GPU/ASIC mining
- Block generation: 1 minute
- 7.14% decrease in the number of coins generated per year
- Decentralized Waves Masternode Network

- Superior Transaction Anonymity using PrivateSend
- Two-tier network using masternodes to form the second tier
- Instant transactions (InstantSend) made possible by the masternode network
- Decentralized Governance By Blockchain allows masternode owners to vote on budget proposals and decisions that affect Dash. Budget proposals fund Dash development and come directly from block rewards, i.e. Dash development is self-funded by its own blockchain.

X11

X11 is a widely used hashing algorithm created by Dash core developer Evan Duffield. X11's chained hashing algorithm utilizes a sequence of eleven scientific hashing algorithms for the proof-of-work. This is so that the processing distribution is fair and coins will be distributed in much the same way Bitcoin's were originally. X11 was intended to make ASICs much more difficult to create, thus giving the currency plenty of time to develop before mining centralization became a threat. This approach was largely successful; as of early 2016, ASICs for X11 now exist and comprise a significant portion of the network hashrate, but have not resulted in the level of centralization present in Bitcoin.
X11 is the name of the chained proof-of-work (PoW) algorithm that was introduced in Dash (launched January 2014 as "Xcoin"). It was partially inspired by the chained-hashing approach of Quark, adding further "depth" and complexity by increasing the number of hashes, yet it differs from Quark in that the rounds of hashes are determined a priori instead of having some hashes being randomly picked.

The X11 algorithm uses multiple rounds of 11 different hashes (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo), thus making it one of the safest and more sophisticated cryptographic hashes in use by modern cryptocurrencies.
The name X11 is not related to the open source GUI server that provides a graphical interface to unix/linux users.

Advantages of X11
Increased confidence and safety for currencies
The increased complexity and sophistication of the chained algorithm provides enhanced levels of security and less uncertainty for a digital currency, compared to single-hash PoW solutions that are not protected against security risks like SPOF (Single Point Of Failure). For example, a possible but not probable computing breakthrough that "breaks" the SHA256 hash could jeopardize the entire Bitcoin network until the network shifts through a hard fork to another cryptographic hash.

In the event of a similar computing breakthrough, a digital currency using the X11 PoW would continue to function securely unless all 11 hashes were broken simultaneously. Even if some of the 11 hashes were to prove unreliable, there would be adequate warning for a currency using X11 to take measures and replace the problematic hashes with other more reliable hashing algorithms.

Given the speculative nature of digital currencies and their inherent uncertainties as a new field, the X11 algorithm can provide increased confidence for its users and potential investors that single-hash approaches cannot. Chained hashing solutions, like X11, provide increased safety and longevity for store of wealth purposes, investment diversification and hedging against risks associated with single-hash currencies plagued by SPOF (Single Point Of Failure).

Evan Duffield, the creator of Dash and X11 chained-hash, has wrote on several occasions that X11 was integrated into Dash not with the intention to prevent ASIC manufacturers from creating ASICs for X11 in the future, but rather to provide a similar migratory path that Bitcoin had (CPUs, GPUs, ASICs).

Masternode Protocol

The Masternodes are propagated around the network using a series of protocol extensions including a Masternode announce message and Masternode ping message. These two messages are all that's needed to make a node active on the network, beyond these there are other messages for executing a proof-of-service request, Darksend and InstantX.

Masternodes are originally formed by sending 10000 Maiscoin to a specific address in a wallet that will "activate" the node making it capable of being propagated across the network. A secondary private key is created that is used for signing all further messages. The latter key allows the wallet to be completely locked when running in a standalone mode.

A cold mode is made possible by utilizing the secondary private key on two separate machines. The primary "hot" client signs the 10000 Maiscoin input including the secondary signing private key in the message. Soon after the "cold" client sees a message including its secondary key and activates as a Masternode. This allows the "hot" client to be deactivated (client turned off) and leaves no possibility of an attacker gaining access to the 10000 Maiscoin by gaining access to the Masternode after activation.

Upon starting a Masternode sends a "Masternode Announce" message to the network, containing:

Message: (10K Maiscoin Input, Reachable IP Address, Signature, Signature Time, 1K MaisCoin Public Key, Secondary Public Key, Donation Public Key, Donation Percentage)
Every 15 minutes thereafter, a ping message is sent proving the node is still alive.

Message: (10K Maiscoin Input, Signature (using secondary key), Signature Time, Stop?)
After a time-to-live has expired the network will remove an inactive node from the network, causing the node to not be used by clients or paid. Nodes can also ping the network constantly, but if they do not have their ports open, they will eventually be flagged as inactive and not be paid.

References

https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf