LITECOINX

A Peer-to-Peer Cryptocurrency with Anonymous Blockchain Transactions

Intro

LitecoinX is a free open source peer-to-peer electronic currency system that is completely decentralized, without the need for a central server or trusted parties. Users hold the crypto keys to their own money and transact directly with each other, with the help of a P2P network to check for double-spending. The blockchain is a Proof of Work via mining X11 Algorithm.

Abstract

LitecoinX is a privacy centric cryptographic currency based on Satoshi Nakomoto's Bitcoin. A peer-to-peer version of electronic transaction would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of mining power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

X11 ALGORITHM

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 THE X11 ALGORITHM

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).

DIGISHIELD IN LITECOINX

MAINTAINING A 45 SECOND BLOCK SOLUTION

DigiShield re-targets a coin’s difficulty between every block, in LitecoinX every 45 seconds. DigiShield re-targets a coin’s difficulty to protect against multi-pools and an over-inflation of easily mined coins

DigiShield was created after seeing the threat that multi-pools pose to a crypto currency when they start mining a coin at a very low difficulty in relation to their net pool hash. This allows many coins to be quickly and easily mined before the difficulty increases. Once the difficulty increases the multi-pool leaves a coin, dumps the coins on the market, and then leaves the dedicated existing miners with a very high difficulty and very few new coins to be mined. This leads to a drop in price and frustration among the committed community members & miners of the affected coin. DigiShield protects against this threat and helps ensure greater confidence in any coin that implements it by allowing the difficulty to rise and fall almost perfectly in sync with increases or decreases in the net hash of a coin. The secret to DigiShield is an asymmetrical approach to difficulty re-targeting. With DigiShield, the difficulty is allowed to decrease in larger movements than it is allowed to increase from block to block. This keeps a blockchain from getting "stuck" i.e., not finding the next block for several hours following a major drop in the net hash of coin. It is all a balancing act. You need to allow the difficulty to increase enough between blocks to catch up to a sudden spike in net hash, but not enough to accidentally send the difficulty sky high when two miners get lucky and find blocks back to back. The same thing occurs with difficulty decreases. Since it takes much longer to find the next block, you need to allow it to drop quicker than it increases. In summary DigiShield is a balanced asymmetrical approach to difficulty re-targeting.

MINING LITECOINX

Generate your own LitecoinX Coin and store your funds securely, anonymously, and permanently. LitecoinX Coin is mined by contributing processing power to secure the LitecoinX Coin network. Miners receive rewards proportional to their computing power. Once the coins are mined, they can be sent and received by anyone anywhere in the world. Mining is the method used to generate LitecoinX Coin. Miners use the processing power of their CPUs (Central Processing Units) or GPUs (Graphical Processing Units) or ASICs (Application Specific Integrated Circuit devices) to secure and process LitecoinX Coin transactions. Finding a solution to a block rewards the miner who found it so that they have an incentive to process more transactions. Originally designed for CPU mining all you need to mine for LitecoinX Coin is a computer and an Internet connection, but the

difficulty level of finding solutions increases with time, so specialized equipment is most commonly used. GPU mining resources will increase difficulty and with this increase and the release of ASIC devices will become standard equipment for high difficulty mining. ASIC devices for the X11 algorithm is the most efficient way to generate LitecoinX Coin currently.

PROOF-OF-WORK

For our timestamp in the LitecoinX network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it. The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

SUMMARY

We believe that blockchain and crypto currencies are the payment method of the future. Trading plays a major role in creating awareness about crypto in whole world. So trading plays an important part in making the whole world aware about crypto currencies. We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly

becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism. . LitecoinX wants to offer an easy to use interface to all users and also being the safest, fastest and secure platform. LitecoinX Coin will make trading profitable and offers its participation in the crypto currency world by Mining or Buying LitecoinX. Individuals will have the opportunity to participate in our long-term growth and success. LitecoinX is a powerful engine of a cryptocurrency, running smooth and fast, at a good pace in its blockchain and escalating to its 84 Million in coin growth potential with upcoming expanding wealth opportunities.

Reference:

 X11 is a widely used hashing algorithm created by Dash core developer Evan Duffield. 2014 DigiShield by DigiByte.