2015

moneta

Electronic Cash System

WHITEPAPER

- What is MONETA?
- Technology and Economics Overview.
- Distributed trust.
- Blockchain Technology.
- Network.
- Decentralisation.
- Double spend solution.
- Conclusion

WHAT IS MONETA?

MONETA uses an innovative technology, design and economic model to maximize both security and the long-term value of the decentralized cryptocurrency.

GLOBAL DECENTRALIZED CURRENCY BASED ON BLOCKCHAIN TECHNOLOGY.

-A decentralized cryptocurrency designed for online transactions.

-easy and useful for regular consumers

-developing tangible utility over traditional currencies by creating platforms for online transactions.

The MONETA network aims to process a block every seconds, rather than Bitcoin's 10 minutes, which its developers claim allows for faster transaction confirmation.

Advantages can include greater resistance to a double spending attack over the same period as Bitcoin.

MONETA is new digital currency that enables instant payments to anyone, anywhere in the world.

MONETA uses peer-to-peer technology to operate with no central authority: managing transactions and

issuing money are carried out collectively by the network.

MONETA Core is the name of open source software which enables the use of this currency.

Technology and Economics Overview.

MONETA was created by an experienced team of entrepreneurs and technologists that previously founded multiple companies with millions of users in the music, gaming and shopping sectors - hundreds of millions of users in total.

- Support and development of integrations in social sphere (online stores and payments, ATM, markets etc.)

How it use (buy, sell and use in life)

- No tax, no bank.

- online wallet, software and awards for system usage.

- Proof of work.

- Fast transactions without reference placement.

Distributed trust.

In traditional models, trust is deposited in an authority or entity which controls all the relevant information. In MONETA, conversely, there is no such authority; rather, information is managed by the users as a whole. In this way, whenever more than half of the users of the system are honest, the “rules” set out by the system cannot be broken by any dishonest users.

By convention, until the limit of OUR MONET is reached, when a miner builds a new block they are rewarded with a predefined amount of bitcoins. In this way all the nodes have an incentive to support the network, and a way of creating and distributing cash is defined, which is necessary given that there is no central authority minting new money. These incentives can also be provided through fees for the verification of transactions, such that the user who creates a valid block receives as a payment a part of the money involved in the verified transaction.

Blockchain Technology.

A block chain or blockchain is a distributed database that maintains a continuously growing list of data records that are hardened against tampering and revision, even by operators of the data store's nodes.

A blockchain is a public ledger of all MONETA transactions that have ever been executed. It is constantly growing as 'completed' blocks are added to it with a new set of recordings. The blocks are added to the blockchain in a linear, chronological order.

- The core advantages of the block chain architecture include the following:
- The ability for a large number of nodes to converge on a single consensus of the most up-to-date version of a large data set such as a ledger, even when the nodes are run anonymously, have poor connectivity with one another, and whose operators could be dishonest.
- The ability for any node that is well-connected to other nodes to determine, with a reasonable level of certainty, whether a transaction does or does not exist in the confirmed data set.
- The ability for any node that creates a transaction to, after a certain period of confirmation time, determine with a reasonable level of certainty whether the transaction is valid, able to take place, and become final (i.e. that there were no conflicting transactions confirmed into the blockchain elsewhere that would make the transaction invalid, such as the same currency units "double-spent" somewhere else).
- A prohibitively high cost to attempt to rewrite or alter any transaction history.
- An automated form of resolution that ensures that conflicting transactions (such as two or more attempts to spend the same balance in different places) never become part of the confirmed data set.

A blockchain implementation consists of two kinds of records: transactions and blocks. Transactions are the actual data to be stored in the blockchain, and blocks are

records that confirm when and in what sequence certain transactions became journaled as a part of the block chain database. Transactions are created by participants using the system in the normal course of business (in the case of cryptocurrencies, a transaction is created anytime someone sends cryptocurrency to another), and blocks are created by users known as "miners" who use specialized software or equipment designed specifically to create blocks.

Users of the system create transactions which are loosely passed around from node to node on a best-effort basis. The definition of what constitutes a valid transaction is based on the system implementing the block chain. In most cryptocurrency applications, a valid transaction is one that is properly digitally signed, spends currency units from a known valid wallet, and meets various other requirements such as including a sufficient miner "fee" and/or a certain time elapsed since the currency units were previously involved in a transaction.

Meanwhile, miners attempt to create blocks that confirm and incorporate those transactions into the blockchain. In a cryptocurrency system such as bitcoin, miners are incentivized to create blocks in order to collect two types of rewards: a pre-defined per-block award, and fees offered within the transactions themselves, payable to any miner who successfully confirms the transaction.

Network.

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.

2) Each node collects new transactions into a block.

3) Each node works on finding a difficult proof-of-work for its block.

4) When a node finds a proof-of-work, it broadcasts the block to all nodes.

5) Nodes accept the block only if all transactions in it are valid and not already spent.

6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one. New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

Decentralisation.

Every node in a decentralized cryptocurrency has a complete or partial copy of the block chain. This avoids the need to have a centralized database that other systems, such as PayPal , require. Whereas a conventional ledger records the transfers of actual bills or promissory notes that exist apart from it, the block chain is the only place that bitcoins can be said to exist in the form of unspent outputs of transactions.

Transactions of the form payer X sends Y currency to payee Z are broadcast to this network using software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes.

Double spend solution.

Cryptocurrencies use various timestamping schemes, such as proof-of-work, to avoid the need for a trusted third party to timestamp transactions added to the block chain. This avoids anyone easily double-spending the currency.

Conclusion.

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.i

For more information, as well as an immediately useable, binary version of the MONETA software, see

Web:	http://moneta.io
Twitter:	https://twitter.com/moneta_io - follow the last news
Facebook:	https://www.facebook.com/io.moneta
Google+:	https://plus.google.com/+MonetaIo