
BITSDIAMOND
21/02/2018
WHITE PAPER

Content

Summary

Cryptocurrency technology is decentralized by design. It is believed that rigorous truth is a natural byproduct of an open source platform run by the public. The decentralization and automation of systems in which they choose to participate and provides an even playing field as never seen before in history.

As well as the inherently democratic nature of decentralized systems, they offer protection to the participants by providing a safety in numbers hypothesis. This limits the ability of malicious actors to threaten or attack participants in the system due to the number of people involved and the global nature of their relationships.

Another advantage is that they are extremely robust. Once a piece of software has entered the public domain, it becomes impractical and virtually impossible to shut down completely. This enables security to the future of the system and knowledge that if the public deems it valuable it will persist.

INTRODUCTION

Decentralization is the means of disturbing, powers, people or things away from a central location or authority.

Bits Diamond Coin wants no central management and no central point of failure. Bits Diamond Coin can operate as self-sustaining entity. Systems run by specific people, in specific locations, with specific computer systems, are susceptible to government interference, coercion, legal issues and more.

The whitepaper describes open source code, freely distributed, with systems in place that reward and facilitate trust. Users will be free to use and operate the network in the way they think best.

The Bits Diamond Coin covers a lot of the technical details for solving the problems posed by decentralization. Since other papers are describing only one cluster of servers, Bits Diamond Coin mainly is looking at how multiple servers work together and what protections against the core technical obstacles are in place.

The main security method employed to protect the system from malicious activity is forming servers into trusted clusters who transact with each other. Servers which are in the same cluster share multiple layers of security features to stop unwanted transactions occurring.

The Bits Diamond Coin is extremely safe to use and offer an unparalleled level of financial privacy. It has overcome all the core technical obstacles which have arisen when presented with the challenges we have implemented solutions which have been tried and tested in parallel fields of interest rather than attempting to redesign the wheel.

TRANSACTIONS

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transactions and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

The problem of course is the payee can't verify that one of the owners did not double spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be refunded to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the

earliest transaction is the one that counts, so we don't care about later attempts to double spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

NETWORK'S

Bits Diamond Coin has many steps to run the network which are as follows:

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof of work for its block.
- When a node finds a proof of work, it broadcasts the block to all nodes.
- Nodes accept the block only if all transactions in it are valid and not already spent.
- 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 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.

Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges,

where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

About Bits Diamond Coin

Bits Diamond Coin is a peer to peer internet currency that enables instant, neat-zero cost payments to anyone in the world. Bits Diamond Coin is the form of digital money that uses encryption to secure transactions and control the creation of new units.

The plan was to make a form of currency not controlled by government or businesses that you could trade globally with no cost and without having to reveal your identity. It is an open source, global payment network that is fully decentralized without any central authorities.

In Bits Diamond Coin mathematics secures the network and empowers individuals to control their own finances. Bits Diamond Coin features faster transaction confirmation times

and improved storage efficiency than the leading math- based currency.

With Bits Diamond Coin, you can buy goods and services using this currency as you would with dollars or euros. It is used for electronic purchases and transfers in which every single purchase is immediately logged digitally on a transaction. Every transaction in Bits Diamond Coin is 100% transparent giving more safety to the whole process.

Each and every transaction is recorded in the public log and the names of buyers and sellers are never revealed, only their wallet IDs which keeps the transactions private.

Why Bits Diamond Coin

The reason for using Bits Diamond Coin is simple as it is a very fast payment method which is much like the credit card payments that are done instantly. It is very cheap form of currency, as it only has minimal fees or sometimes free. This is a major advantage particularly for small businesses as the typical credit card payments are 2-3% on the transaction.

The plus point of the Bits Diamond Coin is there is no central bank or institution with power over the industry. Bits Diamond Coin is controlled by its community and for good and for bad it is completely decentralized.

Another advantage relies on the security aspects of Bits Diamond Coin. It is 100% owned by you which means that no one can freeze your account or access into your Bits Diamond Coin account. Each transaction is only subject to two pieces of data which is a public key and a private one. Anyone can see the public but your private key is secret. This is all different from the traditional credit and transaction where you need to provide your card number, expiry date and CSV.

Disclaimer

The whitepaper does not provide any type of legally binding contract. Bits Diamond Coin limited does not accept any legal liability arising from the material contained in this whitepaper. Anyone looking to invest in cryptocurrency should seek professional advice regarding tax regulations in their local area.

The material provided here represents our current plans for the cryptocurrency platform. The details may change (including ICO distributed plans) and should not be considered finalized. Bits Diamond Coin co-founders and employees do not offer investment advice under any circumstances. No entity is legally bound or contractually obligated by the transferring of Bits Diamond Coin tokens or flat currency. Contributions from investors should be seen as that, a contribution towards the project.

Bits Diamond Coin limited and all persons associated with the company are in no way arranging, dealing or advising on regulated financial investments.

Conclusion

It is believed that in future government or financial institutions will have no choice but to pass or legalize various crypto-currencies.

Bits Diamond Coin will revolutionize the 21st Century economy and how financial transactions are carried out. In future, we can expect to trade in digital money without having to worry about banks, interest rates, the printing or minting process, and any other fees and processes which have become a general part of today's banking systems.

You don't send any personal information when transacting in Bits Diamond Coin. On the other hand, when dealing with paper money, your account number along with your ID number, social security information, balance, and address are transferred between banks and systems. You can only HOPE that your information remains safe. The transactions pass through a clearing house where several people have access to your most sensitive data. For this reason, approximately 5% of US residents have had their identity stolen at least once in their lives. In a Bits Diamond Coin-driven future, identity theft will be consigned to history.

There are many more benefits of Bits Diamond Coin than can fit into a single article. While it is not the perfect solution to all the worlds' monetary problems, its benefits far outweigh the challenges this currency has to overcome. The convenience and security it offers will mean that more and more individuals, businesses and governments will have little choice but to adopt Bits Diamond Coin in one form or another.