ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

Data Integrity of Cryptocurrency

Aditya L Prabhu, Aishwarya U, Chaitra Pradeep, Suresh P

Hewlett Packard Enterprise, Accenture, SAP Labs, Sri Venkateshwara College of Engineering, Bangalore, India

ABSTRACT:A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Secure hashing techniques are used to create the currency and the transaction logs are stored by a technique known as mining. All these modules work in a software wallet, where the transaction can take place and the details are stored. The direct users of these wallets are first-party investors and the disadvantages of the first-party investors are overcome by the use of external servers which maintains the data integrity. Efficient routing has become an important optimization.

KEYWORDS: Cryptocurrency, Mining, Hashing, Bitcoin

I. INTRODUCTION

According to the main word “crypto” which was derived from the Greek word meaning “secret” or “private”, we get words like encryption and decryption, which relates to the encoding of a message when it is transmitted and its decodingwhen received. Cryptocurrency means currency that is private and therefore, it is secure. All details of cryptocurrency are protected by a lengthy and complex code, each of them are unique to the item or the person protecting it.
Taking an example of an investor, the person who is performing the transaction is identified by a one-of–a-kind code. Each “coin” of cryptocurrency itself has its own code as well, depending on what amount is needed for the transaction. Finally, the transaction itself is identified with its unique code. The encryption is done layer by layer which is one of the things that makes cryptocurrency unique, secure and anonymous. All the encryption and concealment is what gives cryptocurrency that name. The industry of cryptocurrency not only has a unique jargon but terms that have synonyms that are used interchangeably. Terms like “digital currency” or “alternative currency” are all additional terms for cryptocurrency.
Following are the details of the paper on how the paper would proceed. Firstly it specifies the details of the generation of cryptocurrency through hashing and storing them in block chains. Secondly, it deals with the managing of log files generated by the transaction known as mining and the working of cryptocurrency and a brief of first-party investors in cryptocurrency and their disadvantages and how the disadvantages can be overcome.

II. CREATION OF CRYPTOCURRENCY

In a recent article from CoinPursuit, it states that the digital currency has been there from around the 1900s, that is the time that internet took over the public world, and people started making online payments and started online shopping. Cryptocurrency wasn’t a hot topic until 2008, when Satoshi outlined the principles and functions of what would be developed and introduced as Bitcoin the following year. One of Bitcoin’s major competitors, Litecoin, used the Bitcoin source code in early 2012, modifying a few key parameters before releasing its own source code. This, in turn, spawned more clones, and one such clone was altcoin.
To create an altcoin, the developers take the Bitcoin source code found in Github, modify the code as it is seen, and it is compiled into the files necessary to generate the block chain and start mining. Once all of the dependencies are built and installed, the next step followed is to clone the source from the ‘git’. Considering one example where, if a user is cloning fooocoin and renames it, regit initializes it, and pushes the initial copy out of Github to make sure git is working:

```
%git clone https://github.com/fooocoin/fooocoin.git
cloning in to fooocoin
 %mv fooocoin barcoin
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

```
%cd barcoinz
%rm -rf .git
%git init
initializing git repository in ~/barcoin
%git add -A *
%git commit -m "first commit coin"
%git remote add origin https://github.com/barcoin/barcoin.git
%git push -u origin master
username for git@github.com: bcoin
password for bcoin@github.com: **********
```

A. *Hashing of Currency*

Bitcoins and their clones (derivatives) depend on a “hash function” which are a complex set of equations that converts a block of data (might contain numbers or letters or both) into a one-way, fixed-size string known as the “hash value.” The initial value of the hash value is called the “message,” while the result is sometimes called the “digest”.

The properties of a good hash value are mentioned below:

1) Hash value must be easily computable
2) With the given hash, it should be infeasible to create a message
3) Without changing the hash, it should be infeasible to modify a message.
4) It should be infeasible to locate two messages that yield the same hash.

In any cryptocurrency or cryptocoin, the origin or creation of new coins and the records of how those coins are traded are logged in what's known as the “block chain.” Each block contains various pieces of information, including a log of recent transactions and a reference to the previous block as shown in Figure 1.

This is implemented by incrementing a value known as “nonce” in the block until a value is found that returns the block's hash the required zero bits. Once the CPU effort has been expended to make it complete the work, the block cannot be modified without redoing the work. As later blocks are chained after it, the work to modify the block would also include redoing all the blocks after it.

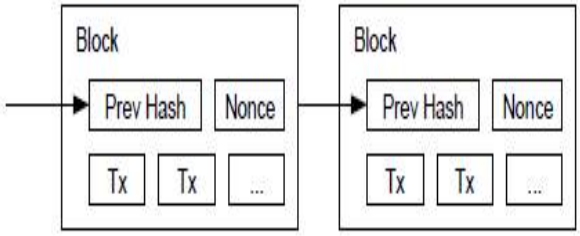

Fig 1. Block chain

For example, Bitcoin’s hash function is an algorithm called SHA-256. An online hash calculator shows that by using SHA-256, the message “a” yields the hash ca978112ca1bhuytfac231b39a23dc4da786eff8147c4e72b9807785afee48bb. Similarly, “ab” yields the hash a63d8014dba891345b30174df2b2a57efbb64f9f09b98f245d1b3192277ece and “abc” yields the hash 0653c7e992d7aad40cb26334568b870e4c154afb346340d02c4577d490dd52d5f9

So if a merchant was looking for hashes that start with 0, we would have just determined that “abc” fulfils those criteria. The system “awards” 100 bitcoins to the computer that finds that solution first.

In a survey, nine or fewer “miners” who worked independently using ordinary computers and Linux, took around five minutes to solve a block. As more people join the network and more clones of Bitcoins are created, this will take a longer time. It will take a lot of time to generate new cryptocoins on their own; that’s when the concepts of “pools” was taken into consideration. With pools, people combine their resources and share the rewards of mining and they make some cryptocoins for themselves.

Eventually, as cryptocurrency gained popularity, special hardware became important. The chips used in thesehardware can calculate the hashes at an order of magnitude much more efficiently than individual consumer-graded computers. Specialized hardware make a huge difference when cracking the SHA-256 hash function. Cryptocoin mining is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

essentially the same concept as password cracking, just with different math applied to different ends which are explained below.

Fig 2. Symbol of Bitcoin

B. *Cryptocurrency Mining*

Mining is the process of aggregating transaction logs to block chain which contains legacy transaction details. The block chain is used so that it can pass the message to the rest of the network that a transaction has taken place. The cryptocurrency nodes use the block chain to distinguish legitimate cryptocurrency transactions from users to attempt to re-use coins that have already been used elsewhere. Independent blocks must contain a proof of work to be termed as valid. This proof of work is validated by other Cryptocurrency nodes when a block is received. For example, Arscoin uses the hash cash proof-of-work function.

The primary purpose of mining is to allow Cryptocurrency nodes to reach a safer, tamper-resistant consensus. Mining is also another procedure used to introduce Cryptocoin or cryptocurrency into the system: Miners are paid for the coins which they create. These both serve the purpose of dispersal of new coins in a decentralized manner as well as encouraging people to provide security for the system.

III. THE WORKING OF CRYPTOCURRENCY

A cryptocurrency wallet is a website or application which is used to store cryptocurrency and is used for making transactions. This wallet generates the first cryptocurrency address and it can be disclosed to anybody trusted for transferring and receiving currency. These addresses should be used only once.

The entire cryptocurrency network relies on the block chain. All confirmed transactions are aggregated in the block chain. This way, cryptocurrency wallets can calculate their spendable balance and new transactions can be validated that is actually owned by the spender, this transaction is a transfer of value between cryptocurrency wallets that get included in the block chain. Cryptocurrency wallets keep a secret and confidential data called a private key, which is used to sign transactions, that provides proof that it has come from the owner of the wallet. The signature prevents the transaction from being altered by anybody else once it has been used. All transactions are published between users and usually begin to be confirmed by the network in a few minutes, through mining. This confirms the waiting transactions by adding them in the block chain. It enforces an order of occurrence in the block chain, safeguards the neutrality of the network, and allows different machines to agree on the state of the system. To be confirmed, transactions must be arranged and packed in a block that follows very strictcryptographic rules that will be verified by the network. These rules do not let legacy blocks to be altered because doing so would make all the following blocks obsolete.

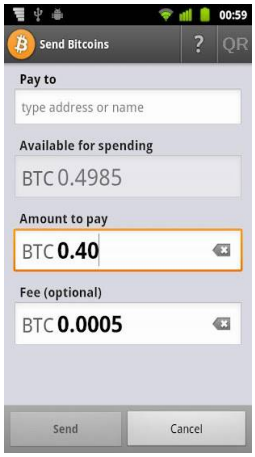

Fig 3. Snapshot of a Bitcoin data wallet

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the block chain. This way, no individuals can handle what is included in the block chain or change or replace parts of the block chain to roll back their own spends. The data integrity and the order of occurrence of the block chain are implemented with cryptography. The following section explains about First-party wallets.

A. *First-Party Investors*

These are wallets can be installed and maintained by the member himself, as opposed to having them stored by a third party. With a first-party wallet, the user has to take charge of the wallet and cannot depend on any source. The wallet can be stored on the user's mobile, tab, laptop or his desktop.

Though this kind of wallet has its own advantages, like it can be maintained by the user itself rather than a third party and the user has full control over the wallet and it is secure from attacks. But there are disadvantages as well. The first disadvantage is that in which ever device the data wallet is installed during the transaction the device must be present with the user because this wallet is stored only in the user's device and is not connected or linked to any external source. The second disadvantage which must be rectified is that, if the wallet is lost, cryptocurrency is lost. In the case of a hard drive crash, or if a virus corrupts the data, which leads to the wallet application is corrupted, cryptocurrency has essentially been lost. There is no way to recover the lost currency. These coins will be forever orphaned in the system and cannot be used for any transaction. This leads to a wealthy cryptocurrency investor to lose all the money within seconds with no way to recover it. The coins that the investor-owned will also be permanently orphaned and can never be retrieved. This is a very big disadvantage when it comes to huge investments by the user.

B. *Protection of the First-Party Investor*

With respect to the disadvantage of the First-Party investor, when it comes to the data being lost due to a system crash or when data gets corrupted, it can be overcome if the wallet is present on an external server. In this case, each user can have a dedicated server for his data wallet and each transaction can occur on the external server.

In this case, the user is the client, and the client communicates with the server and processes the requests such as transactions. The client communicates with a certain set of communication protocols. All client-server protocols operate in the application layer. To formalize the data exchange even further, the server may implement an API script (such as a web service).The API script is an abstraction layer for such resources as databases and custom software.

As it is stored on the external server, the transactions can be shared easily anytime as it's present in the server.

This method maintains security because the data or the currency will be encrypted by the client and decrypted by the server and as the user himself maintains both the wallet and the server. It is not vulnerable to attacks during transactions.

In this case, the hard disk crash or data being corrupted will not affect the user and the currency will not be "lost" and thus, it is secure.

IV. CONCLUSION

We have proposed a system for electronic transactions without relying on trust. The investor has full control of the wallet. There is no chance of the data to be lost, as the wallet is stored on the external server and the data integrity is maintained. The transactions are performed on the server, as well as without any third-party investor being involved. This makes the transaction secure.

REFERENCES

1. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System
2. http://arstechnica.com/business/2014/03/behold-arscoin-our-own-custom-cryptocurrency
3. http://en.wikipedia.org/wiki/Cryptocurrency
4. http://www.coindesk.com/information/how-bitcoin-mining-works
5. http://startbitcoin.com
6. http://en.wikipedia.org/wiki/Bitcoin