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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

A Study on Blockchains and Bitcoin - A Blockchain based Cryptocurrency

Rijul Luman,

Student, MS - Computer Science, Sacramento State University, CA, USA

ABSTRACT: A purely peer-to-peer version of electronic cash allows online payments to be sent directly from one party to another without going through a financial institution. Digital signatures along with blockchain technology provide a solution without requiring a trusted third-party. Here, we shall discuss how bitcoin works and some other applications of the blockchain technology.

KEYWORDS: Blockchain, Bitcoin, Cryptocurrency**.**

I. INTRODUCTION

A **blockchain** is basically a chain of blocks where each block must contain the cryptographic hash of the previous block. Hence, in order to change any one of the blocks we need to modify all the proceeding blocks in order to remain valid; since change to a block will change its hash, which in-turn will change all the consequent block hashes. Blockchain are generally decentralized and use a consensus algorithm to decide which node created the next block and provide trust to the blockchain.

Bitcoin uses Proof-of-Work as a consensus method to decide which node mines (creates) the next block. This node picks up top paying transactions from the transaction broadcasts it received from the network, and adds them into this newly created block. He then has to prove that he put in certain effort in creating the block by finding a suitable nonce for the block, which generates the block hash value below a certain threshold value. For this the miner must rehash the same block with a different nonce again and again till he finds a nonce that works. This process takes a lot of computation power and time. The goal of this, is to keep the block generation time around 10 minutes. The threshold representing a valid hash is increased or decreased every 2016 blocks proportional to the computational power change in the network.

II. BITCOIN: LITERATURE SURVEY

The author Satoshi Nakamoto, argues that buying and selling goods over the internet relies on financial institutions acting as 3rd parties to process financial transactions. These processes are therefore based upon the 2 parties trusting a 3rd party to process their transaction, and as a 3rd party must be "trusted" there is always room for a transaction to be reversed. Before Bitcoin, there was no way to make a non-reversible payment online for a non-reversible service as there is with cash in the physical world. To overcome this problem, Satoshi introduced an electronic payment system based on cryptography.
The "Methodology" section of the paper is spilt into the following sections that outline the concept of Bitcoin:

(1) Transactions
The definition of a Bitcoin is a "chain of digital signatures" that can be passed from one person to another using an electronic signature (hash). During this process, the sender passing the Bitcoin onwards, electronically signs the

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

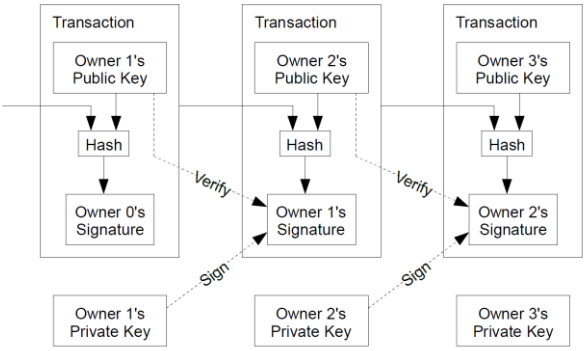
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

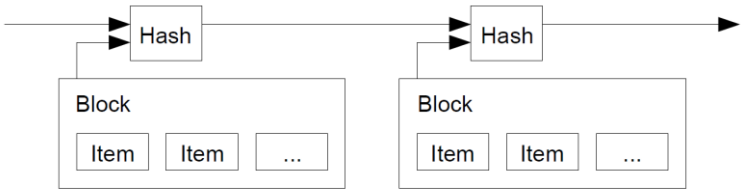
Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

pervious transactions of the Bitcoin and the public key of the recipient they are sending the Bitcoin to. Bitcoin overcomes the double spending problem by using timestamps to ensure that whenever a Bitcoin is passed on, a duplicate copy of that coin cannot be double spent (fraud). If a coin is sent to two recipients, the coins will have different time stamps and hence the second coin sent will be automatically rejected by the system.
The Bitcoin system processes every transaction and "publicly announces" whenever a transaction takes place. This ensures that the system, along with its users, moderate the chain of transactions (blockchain) to ensure fraudulent activity does not take place. Using this method of moderating transactions ensures that a 3rd party is not needed, and the Bitcoin system is truly decentralized.



(2) Timestamp Server
The timestamp server is a simple piece of software that is used to digitally timestamp data. The server takes a small section of the transaction data (the hash) and timestamps it. This time stamped hash is then made publicly available for everyone to see. The existence of this time stamped hash therefore proves that the transaction exists and is therefore valid.



(3) Proof-of-Work
To implement a time stamp server across a network of computers (nodes), bitcoin uses a proof-of-work system. Proof-of-work requires proof that a specified amount work was performed by the system. In terms of Bitcoin, a specific mathematical problem has to be solved by a computer is as follows:
The hash value of the generated block needs to start with a certain number of 0 bits. The number of bits is determined by the network difficulty. As the processing power of the network goes on increasing, the time required to generate 2016 blocks reduces. We calculate the time difference between the time to mine last 2016 blocks and the expected time to mine 2016 blocks (10 mins * 2016 = approximately 2 weeks). The number of 0 bits is adjusted accordingly to get the block generation time closer to 10 mins. Similarly, if it takes more than 2 weeks to generate 2016 blocks, the difficulty is reduced.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

(4) Network
New transactions are "publicly announce" to all nodes >> each node puts all new transactions into a block >> each node works on solving the proof-of-work (explained above) for its own block >> when a lucky node solves the puzzle for its block, it informs all other nodes >> nodes accept the solved block if ALL transactions are valid and there are no issues of double spending >> nodes move onto next block in chain >> This process then repeats in a loop. Nodes always consider the longest chain to be correct. If two nodes send two versions of the block at the same time, these blocks will be processed based on their time stamp. The longest chain will win. If a node is switched off and subsequently does not receive a block, the rest of the nodes will continue without it and the node that missed out will be updated when it connects to the network later.

(5) Incentive
Conventionally, the first transaction in a block creates a new coin which is owned by the person (node) who created that particular block. This incentivizes people to use their computers (nodes) and connect to the Bitcoin network to help process Bitcoin transactions. This is where the term Bitcoin mining originates. Transaction fees also act as incentives.

(6) Reclaiming Disk Space
Old transactions can be discarded after a set amount of time to save disk space, the root (a trace) of the discarded transaction will remain so the Blockchain remains intact.

(7) Simplified Payment Verification
Payments can be verified without running the full network on a node. If a user has a copy of the longest Blockchain and block hash's, they can verify a payment. This is done by querying the network of nodes and matching a transaction to its time-stamp.

(8) Combining & Splitting Value
Processing coins individually is possible; however, it is inefficient to make a separate transaction for every cent in a transfer. The value of coins can therefore be split and/or recombined. This allows a large coin to be split into multiple parts before being passed on, or smaller coins to be combined and make a larger amount.

(9) Privacy
Although transactions are publicly declared, the public keys that identify individuals are anonymous, and hence the identities of the sender and receiver cannot be determined by the public. It is publicly declared that an amount of money is moving from point A to B, however no identifiable information is openly distributed.

(10) Calculations
There is a higher probability that an honest node will find a block before a fraudulent node. It is therefore unlikely that the fraudulent node will catch up with the honest node when making a fraudulent Blockchain. The odds are not in the favor of the fraudulent node unless they simply get lucky or own 51% of the networks processing power. This is important when increasing the size of the Blockchain as the nodes identify the longest Blockchain as being the correct chain.

III. PROPOSED APPLICATIONS OF BLOCKCHAINS

Financial Applications of blockchain technology

(1) Stock Market: The current process of trading stocks in existing exchanges is inefficient and slow due to involvement of multiple 3rd parties. We can implement a smart contract that manages share trading over a blockchain.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

These smart contracts facilitate, verify or enforce the negotiation of contract and eliminate the need for a physical document. This eliminates the need for an intermediary, such as broker, exchange or bank.

(2) Insurance: Any property (physical or digital such as real estate, automobiles, physical assets, laptops, other valuables) can potentially be registered in blockchain and the ownership, transaction history can be validated by anyone. This information can be verified by the insurance companies using simple APIs (Application programming interface).

Non-Financial Applications of blockchain technology

(1) Notary Public: Verifying authenticity of the document can be done using blockchain and eliminates the need for centralized authority. The document certification service helps in Proof of Ownership (who authored it), Proof of Existence (at a certain time) and Proof of Integrity (not tampered) of the documents. Since it is counterfeit-proof and can be verified by independent third parties these services are legally binding. It also eliminates the need for expensive notarization fees and ineffective ways of transferring documents.

(2) Applications in the Music Industry: The process by which music royalties are determined has always been convoluted one, but the rise of the Internet has made it even more complex giving rise to the demand of transparency in the royalty payments to the artists and songwriters. This is where the blockchain can play a role by maintaining a comprehensive, accurate distributed database of music rights ownership information in a public ledger. In addition to rights ownership information, the royalty split for each work, as determined by "smart contracts" could be added to the database. The "smart contracts" would define relationships between different stakeholders (addresses) and automate their interactions.

(3) Decentralized proof of existence of documents: Validating the existence or the possession of signed documents is very important in any legal solution. The traditional document validation models rely on central authorities for storing and validating the documents, which present some obvious security challenges. These models become even more difficult as the documents become older. The blockchain technology provides an alternative model to proof-of-existence and possession of legal documents. By leveraging the blockchain, a user can simply store the signature and timestamp associated with a legal document in the blockchain and validate it anytime using native blockchain mechanisms.

(4) Decentralized Storage: Cloud file storage solutions such as Dropbox, Google Drive or One Drive are growing in popularity to store documents, photos, video and music files. Despite their popularity, cloud file storage solutions typically face challenges in areas such as security, privacy and data control. The major issue is that one has no choice but to trust a third party with one's confidential files. Here, bitcoin based micropayments serve as both an incentive and payment while a separate blockchain is used as a datastore for file metadata.

(5) Decentralized IoT: The Internet of Things is increasingly becoming popular technology in both the consumer and the enterprise space. A vast majority of IoT platforms are based on a centralized model in which as broker or hub controls the interaction between devices. However, this approach has become impractical for many scenarios in which devices need to exchange data between themselves autonomously. The blockchain serves as the general ledger, keeping a trusted record of all the messages exchanged between smart devices in a decentralized IoT topology.

IV. RISKS IN ADOPTATION

(1) Behavior change: With updates in technology, changing the behavior of an existing blockchain difficult.
(2) Scaling: We need a copy of the entire blockchain in-order to derive information from it.
(3) Quantum Computing: The basis of Blockchain technology relies on the very fact that 8 it is mathematically impossible for a single party to game the system due to lack of needed compute power. But with the advent of Quantum

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Computers (in future), the cryptographic keys may be easy enough to crack through sheer brute force approach within a reasonable time. This will bring the whole system to its knee.

(4) Government Regulations and Fraudulent Activities: The anonymity provided by the blockchain can be used for money laundering and other illegal activities, hence the government will pass restrictions and regulations on blockchains sooner-or-later.

V. CONCLUSIONS

Satoshi concludes their work by drawing attention to the key features of this paper:

1. A system for electronic transactions without relying on 3rd party for trust
2. Digital signatures provide strong controls over ownership and double-spending is prevented
3. A peer-to-peer network using proof-of-work is used to create a public log which is impractical for attackers to change, provided honest nodes are in control of the system
4. Nodes work with little coordination, they do not need to be identified since messages are not ever sent to a single location
5. Nodes can leave and rejoin the network at any time, provided they update their Blockchain upon re-entering the network
6. Rules and incentives can be enforced using a voting system

To conclude, Blockchain is the technology backbone of Bitcoin. The distributed ledger functionality coupled with security of Blockchain, makes it very attractive technology to solve the current Financial as well as non-financial business problems. There is enormous interest in Blockchain based business applications and hence numerous Start-ups working on them. The adoption definitely faces strong headwind as described before. Thus, the authors envision Blockchain to go through slow adoption due to the risks associated. Most of the Startups will fail with few winners. We should be seeing significant adoption in a decade or two.

REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf
[2] Sutardja Center for Entrepreneurship & Technology Technical Report, "Blockchain Technology, beyond Bitcoin", http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
[3] https://steemit.com/trending/bitcoin
[4] Rijul Luman, https://www.youtube.com/watch?v=ueM-vMdR8Ws