Blockchain: The future of the transaction process

Dillon Ward - *G00326756* - Dillonward2017@gmail.com

Abstract—In the context of Cryptocurrencies, Blockchain is a dynamic data structure that contains information about all of the transactions that have taken place. Blockchain can be thought of as a giant global ledger that records the beginning and end point of each transaction made using Cryptocurrencies. Among the various Cryptocurrencies, I will focus on Bitcoin and how it works in the Blockchain. In this literature review, I will discuss in detail what Blockchain is, how it works, and why it is the future of all transactions all while making physical money redundant. I will also be discussing some of the downsides to Blockchain, such as privacy and transaction times and the solutions to these defects.

Index Terms—Blockchain, Bitcoin, Cryptocurrency, Mining, Security, Privacy.

1 Introduction

WITHIN the past few years, Blockchain has become an ever-growing innovation that has changed the way, according to [1], an estimated 2.9 - 5.8 million unique users make online transactions using digital currency. Blockchain is a dynamic data structure that contains information of all the most recent transactions that have taken place using digital currencies. There are a wide range of digital currencies that are used on the Blockchain, that are collectively known as "Cryptocurrencies".

Currently, Cryptocurrencies are the biggest applicants of the Blockchain data structure, Bitcoin being the biggest to date. In this literature review I will cover in detail what Blockchain is, security measures taken, and the transaction process or adding a new Block to the Blockchain. I will also go over some security and privacy issues that are potential setbacks for the future of Blockchain.

2 Blockchain

2.1 What is Blockchain?

A Blockchain is a large distributed decentralized database of records or a public global ledger of all transactions that have taken place using Cryptocurrencies, and is shared among participating parties – anyone can access the ledger and participate in the executions of transactions. Blockchain stores data about transactions from different Blocks on the chain.

Each transaction that is added to the Blockchain can be added by anyone, and once it is added it cannot be erased. In order to ensure consistency on the Blockchain, users must assume trust with other users. Whenever a digital transaction is executed, it is grouped into a cryptographically protected *Block* along with other transactions that have recently occured and is broadcast along a network, continuously updating digital records of who owns what. Each *Block* that is validated is then timestamped and added to the Blockchain in chronological order.

Blockchain also works on a peer-to-peer basis, making the need for traditional financial intermediaries obsolete. All transactions are done directly from one user to another, and are added to a *Block* which are later added to the Blockchain.

2.2 Blocks

As described in [2], a Block on the Blockchain can be thought of as the current part of a Blockchain that contains recent transactions that have been made. Once these transactions are completed, the Block is added to the Blockchain. As soon as a Block is completed, a new Block is generated in its place. By default, a new Block is generated every 10 minutes. To add another Block to the Blockchain, first a user must solve a Hashing algorithm that is generated by other Blocks on the network. Once the hashing algorithm is solved, the Block is then added to the Blockchain and data is broadcast to other blocks on the network, verifying that a transaction has been made. Users that are willing to use up processing power in order to solve these Hashing algorithms to add these transactions to the Blockchain are what's known as *Miners*.

2.3 Mining

As stated in [3], users can volunteer to verify and add new transactions to Blocks. Users lend their processing power to complete Hashing algorithms to add transactions to Blocks. The newest valid Block of transactions is then confirmed by all users and is appended to the Blockchain. The user who created this Block is then rewarded with some of the Cryptocurrency they are mining.

2.4 Reception

Although the overall reception of Cyptocurrency and Blockchain technology has been positive, some countries believe these advancements pose a serious threat. As stated in [4], just 2 weeks after a Bank in Russia hinted that Cryptocurrency exchanges would be banned, Russian president Vladimir Putin released five presidential orders that all relate to the regulation of Cryptocurrencies and the associated Blockchain technology. Instead of using emerging

Cryptocurrencies, Russia have announced their interest in creating their own Cryptocurrency which will be controlled and taxed by the state.

Although some countries see Cryptocurrencies as a threat, many European countries have welcomed Blockchain with open arms. Denmark has been an advocate for 100% digital currency, while Arnhem in The Netherlands has dubbed itself 'Bitcoin City' with over 100 merchants accepting Bitcoin as a payment method.

3 Security

3.1 Privacy

Since Blockchain is a global ledger, all transaction data is visible to other Blocks on the chain – other Blocks can see executed transactions. As stated in [5], all the transactions on Blockchain are accessible for viewing by anyone of the public without any restrictions by one's government, the users are in control of Blockchain. An alternative to this problem, as proposed in [6], is *Data Ownership* – users can have full control over their own data on the Blockchain, allowing them to hide or show whatever information they like. The user should also know what kind of information third parties are collecting on their transactions, while maintaining some level of encapsulation to protect their data.

3.2 Identification

In order to identify individual users on the Blockchain, each user has their own individual *Blockchain Wallet* that contains 2 keys – the *Public* and *Private* key.

3.2.1 Wallet

A Cryptocurrency Wallet is a virtual wallet that stores the public and private keys that are used to execute transactions such as receive or send Cryptocurrencies. The Cryptocurrency Wallet is encrypted and automatically backed up to servers. In order to ensure security, as stated in [7], another level of security is added to these wallets by encrypting them twice. Cryptocurrency wallets can also be accessed from any device.

3.2.2 Private Key

A Private Key is a randomly generated key that is held privately by each user. Each user on the Blockchain knows their own Private Key, and should keep it protected if they don't want to compromise the security of their wallet and risk losing their Cryptocurrencies. The Private Key is used for each transaction on the Blockchain that a user has made and is used to confirm that the transaction has come from the user.

3.2.3 Public Key

A public key is a key that is used to ensure that the user is the owner of an address that can receive funds. The Public Key is visible to the Public, and is mathematically derived from the user's Private Key, meaning the Private Key is put through a Mathematic Hashing Algorithm to generate the Public Key. Though it may seem that you can reverse the key to gain access to the Private Key, the algorithm used ensures that while it is very easy to generate a Public Key, it is difficult to reverse the key. As stated in [8], "the algorithm involves converting the Private Key to a binary representation, identifying the bits in this binary representation that have a value of 1, and summing an exponentially multiplied generator variable to arrive at the final public key".

3.3 Timestamping

Timestamping is the process of keeping track of the creation and modification time of a document. On the Blockchain, it has become possible to securely timestamp information in a tamper-proof manner. Essentially, hashed data can be incorporated into transactions on the Blockchainm which can serve as secure proof of the exact time at which a document existed or if said document was tampered or modified. This proof is due to a huge amount of computation performed after the hash is submitted to the Blockchain.

If the Timestamp were ever to be tampered with, it would break the integrity of the entire digital currency it is applied to, and would devalue the currency to zero.

4 Transactions

4.1 Transactions Protocols

There are currently two transaction protocols that Blockchain networks can mine Cryptocurrencies: Proof-of-work which allows miners to validate transactions by solving mathematical problems, and Proof-of-stake which allows miners to validate block transactions according to how many coins they currently hold. These protocols are used to deal with double-spending of Cryptocurrencies.

4.1.1 What is Double Spending?

As stated in [9], "double spending, or spending a currency token more than once, is the main security problem that digital currencies have to deal with". Double spending is an attack where a user spends the same digital token in more than one transaction. Other problems can arise from double spending such as inflation. The two transaction protocols are designed to handle and deal with double spending.

4.1.2 Proof-of-work

Proof-of-work is a protocol in which Blocks generate Hashing Algorithms (in the case of Bitcoin, **SHA-256**) which are generally very time consuming and process heavy algorithms to produce, but can be solved relatively quick by other Blocks. As transactions are executed, more algorithms are generated to be solved – generally, ever 10 minutes.

The continuous growth of the Blockchain is one of the downsides of using proof-of-work. As the Blockchain grows more and more, more algorithms are produced, meaning more need to be solved leaving long periods of time to execute and finalize transactions. An alternative to using proof-of-work is **Proof-of-stake**.

4.1.3 Proof-of-stake

Proof-of-stake is a proposed alternative to Proof-of-work. Proof-of-stake states that a user can mine or validate Block

transactions depending on how many coins the user currently has. This means that the more of a particular Cryptocurrency a user has, the more influence the user has over verifying transactions; thus, giving them more mining power. Essentially, rather than letting users solve Hashing Algorithms to verify transactions, they can attribute mining power to the proportion of coins currently held by the miner.

In using Proof-of-stake, rather than delegating energy and processing power to executing transactions, a user can verify transactions that is reflective of their ownership stake. This method of handling transactions is significantly faster. Currently, Nxt is using Proof-of-stake. Additionally, Krypton, a Proof-of-work network, was recently hacked and announced that it would be transferring over to Proof-of-stake.

4.2 Transaction Time

Since the Blockchain is a continuously growing distributed system that distributes its data along a network, transactions can take a long time. One of the initial goal of Cryptocurrencies in making financial intermediaries redundant was that transactions were to be almost instantaneous, all while removing tradition fees for transferring money. Although these were part of the initial appeal to using Cryptocurrencies, the rate at which the Blockchain grew was unprecedented, namely because of the current Proof-of-work protocol that some networks use.

Since there can be a number of other Blocks generating proof-of-work confirmation algorithms, which take time to generate, the transaction process can be drawn out. Currently, it takes from *60 - 80 minutes* for 6 transactions of a Block to be confirmed. Generally, larger transactions take the longest.

Another problem that arises with the transaction delay when it comes to replication and distribution of transactions. Since Blockchain uses replication to keep all transaction entries consistent, it takes a long time for the transaction to be sent to other Blocks on the network. Transaction times are probably one of the biggest downsides of Blockchain to date.

5 Conclusion

Currently, Blockchain, though it does have many advantages thus there are millions of people currently trading on it, is not perfect. The main drawbacks from using Blockchain are the issues with **Privacy** and **Transaction time**.

If Blockchain is supposed to let the users and traders be in control of it, I believe said users should have control over what kind of information companies or other third parties can see on the public global ledger. Anonymity is essential to many people using the Blockchain, and I believe that letting the users choose what others can and cannot see will draw more people to it and give more control to traders, though it may be a deterrent for others.

Secondly, is the issue of Transaction Times and the current time it takes for users to send or receive Cryptocurrencies. I believe the issue of Transaction Times for users is a huge drawback, and may lead many people to use traditional financial intermediaries purely for convenience.

Although it may have these setbacks, I believe that it is only a matter of time before most of our current financial transactions are made on the Blockchain. Blockchain is still an emerging technology, and only within the past couple of years has it gotten mainstream attention. As I previously stated, with places like Denmark or the Netherlands being advocates of trading with Bitcoin, and there even being Bitcoin ATMs in Sweden, I believe it is only a matter of time before currency becomes completely digital.

Blockchain has gradually been seeping into the Business world too, though many companies still feel that Blockchain will fall eventually, whereas others have themselves began investing into Cryptocurrencies.

In its current state, it can fundamentally change the way we currently trade in Business, or even change the way we now trade with Cryptocurrencies if governing bodies step in to regulate it or Businesses such as IBM create their own.

Currently, there is a Blockchain research institution that is trying to push Business to adopt the Blockchain-based business model, to which I say it is only a matter of time.

References

[1] G. Hileman and M. Rauchs, *"Global Cryptocurrency Benchmarking Study"*, p. 10, 2017.

[2] *"Know more about Blockchain: Overview, Technology, Application Areas and Use Cases - Lets Talk Payments"*, Lets Talk Payments, 2017. [Online]. Available: https://letstalkpayments.com/an-overview-of-blockchain-technology/. [Accessed: Nov- 2017].

[3] L. Wang and Y. Liu, *"Exploring Miner Evolution in Bitcoin Network"*, p. 3, 2015

[4] K. Hanley, *"Putin Orders Regulation of Cryptocurrencies and Blockchain"*, Digital Journal, 2017. [Online]. Available: http://www.digitaljournal.com/tech-and-science/technology/putin-orders-regulation-of-cryptocurrencies-and-blockchain/article/506007. [Accessed: Nov- 2017]

[5] V. Buterin, *"Privacy on the Blockchain"*, Ethereum Blog, 2017. [Online] Available: https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/. [Accessed: Nov- 2017]

[6] G. Zyskind, O. Nathan, and A. . Pentland, *Decentralizing privacy: Using blockchain to protect personal data*, May 2015, p. 2.

[7] *"How Your Wallet Works - My Wallet"*, Blockchain.info, 2017. [Online]. Available: https://blockchain.info/wallet/how-it-works. [Accessed: Nov- 2017].

[8] L. Di, *"Why Do I Need a Public and Private Key on the Blockchain?"*, Medium, 2017. [Online]. Available: https://blog.wetrust.io/why-do-i-need-a-public-and-private-key-on-the-blockchain-c2ea74a69e76. [Accessed: Nov- 2017].

[9] C. Perez-Sol'a, S. Delgado-Segura, G. Navarro-Arribas, J. Herrera-Joancomarti, *"Double-spending Prevention for Bitcoin zero-confirmation transactions"*, p. 1, 2017.