

SEG2911
FINAL REPORT

**IMPLICATIONS OF BLOCKCHAIN
TECHNOLOGIES ON THE FUTURE**

Prepared for: Riadh Habash, University of Ottawa

Written by: Zarif Shahriar, 8177206

Pasoon Azimi, 8215497

Date: March 17, 2018

TABLE OF CONTENTS

ABSTRACT	1
1. INTRODUCTION	2
2. BACKGROUND INFORMATION 2.1 History of Blockchain Technology 2.2 Understanding Blockchain	2
3. DISCUSSION OF FINDINGS 3.1 Blockchain Usages 3.2 Blockchain on the Future	4 6
4. CONCLUSION	7
5. REFERENCES	8

ABSTRACT

The purpose of this report is to inform engineers and entrepreneurs about the implications of blockchain technologies on the future and give a general understanding of this incredible technology that is growing rapidly.

With its discrete arrival in 2009, blockchain technology was founded after the release of its counterpart Bitcoin, the first cryptocurrency released to the public. From that day, it has exponentially impacted several domains and industries as its incredible potential is being harnessed by researchers, engineers and entrepreneurs around the world.

The technology has several usages already and with much more to come in the future. By harnessing the power of a public and private key encryption system, applications and entrepreneurs can create efficient, low cost and transparent services. These services can range from industries such as remittances, voting, ride sharing and rental applications and many more. With the robust features of the blockchain it is possible to create a distributed world of value where majority of the computational power and energy is no longer wasted but rather distributed for cryptocurrencies and other sources of value instead.

The future of blockchain is bright despite some of the hurdles and obstacles it may face on its path to adoption. However with engineers and industry leaders already hard at work to utilize this powerful and open tool. In the future it will only grow to make data recording, transactions, governments and corporations more transparent, secure and efficient.

1. INTRODUCTION

This report will begin by introducing the *Background Information* surrounding blockchain technologies, including a brief history as well as explaining how it works. It will then continue to explain the implications of blockchain technologies in the *Discussion of Findings* section where it will discuss some of the usages of the blockchain. It will continue to demonstrate some of the future perspectives on blockchain and where it is possibly headed with new technology. The report will conclude summarizing the implications blockchain technology has on the future.

2. BACKGROUND INFORMATION

2.1 History of Blockchain Technology

The birth of blockchain came with the arrival of Bitcoin, a cryptocurrency experiment aiming to create a new form of currency. Bitcoin was released to the open source community in 2009 by Satoshi Nakamoto, an alias used by the creator. On its release, the Bitcoin software allowed the public to both trade and mine Bitcoin. This so called “mining” is the process in which new Bitcoins are created and the transactions that are involved in moving Bitcoins are recorded and verified on the blockchain. (*A Short History of Bitcoin and Cryptocurrency Everyone Should Read*, 2017, p1-p2)

In 2014, as Bitcoin grew its footprint in the market, the realization that blockchain, the underlying technology of Bitcoin could be harnessed and used completely separate from its cryptocurrency counterpart. This blockchain technology could then be used for several different operations. From this, a surge of several different cryptocurrencies arrived on the market after the industry began to understand the power of blockchain. Many of these new cryptos offered solutions in various domains like supply chains, health care, insurance, transportation and many more. As of today nearly 15% of financial institutions are either researching or using blockchain technologies and this number is still growing as the world continues to uncover this phenomenon. (*A Very Brief History Of Blockchain Technology Everyone Should Read*, 2018, p1)

2.2 Understanding Blockchain

Blockchains popularity and intrigue came from its solution to many of the problems involved with transactions today. Blockchain keeps all records of important information and gives access to this information to the public but this information can never be

removed or altered. Everything you need to know is provided thoroughly with full transparency and most importantly its decentralized (not in one specific location) (*A Very Brief History Of Blockchain Technology Everyone Should Read, 2018, para 1*).

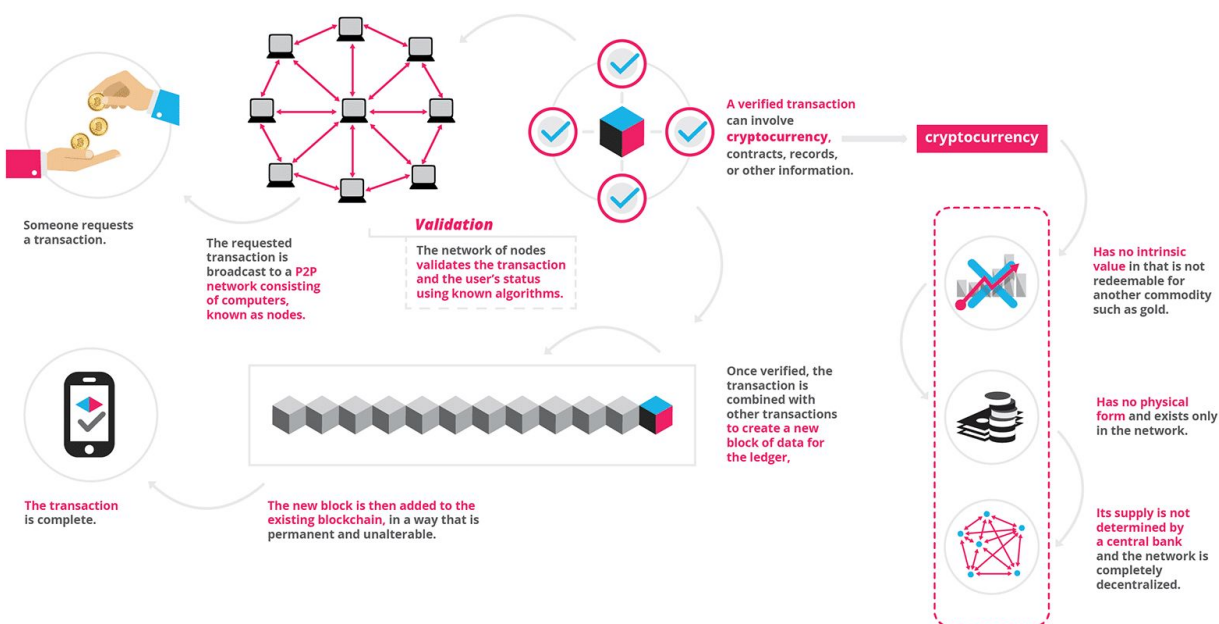


Figure 1: This image explains the blockchain infrastructure and how each piece works together. Source: *What is Blockchain Technology?*, 2017.

In abstract, blockchain is essentially a database that is duplicated thousands of times across a network of computers. This network of computers is designed to then consistently and regularly update this database. Information stored on this database is shared amongst the users, meaning it isn't stored in any one location. This was earlier referred to as a decentralized ledger. This is important because it allows the information recorded by the blockchain to be easily accessible and verifiable by the public. There is no central location, as a result it is being hosted by millions of computers around the world preventing hackers from directly manipulating these records. Everyone interacting with this database sees the newest and recently updated version. As can be seen from figure 1.

The Bitcoin blockchain consistently checks with itself every ten minutes to reconcile every transaction that happened during this interval. Each group of these transactions created during this interval are called “blocks”. The blockchain network is composed of several “nodes”. These nodes are computers that are connected to the blockchain network using a client that both validates and relays transactions. Once connected to the

blockchain network, the node gets a copy of the blockchain. Every node connected to the network is an “administrator” that can join or leave voluntarily. Joining the network provides each node with an incentive at acquiring an amount of cryptocurrency. Each node competes with one another to solve high level computational puzzles which is known as “mining”. This interaction of nodes is what allows transactions to be verified and added to the public ledger. These nodes usually use high level graphics card when participating. (*What is Blockchain Technology?*, 2017)

Blockchain is also renowned for its enhanced security. Being decentralized eliminates several risks but what makes blockchain very interesting is its public and private “keys”. A public key in a blockchain is a very long randomly generated string of numbers and characters which represents the users address in the current blockchain. The private key on the other hand is a password created by the user themselves that allows him/her to get access to their cryptocurrency. This ensures a very high level of security in which information and digital assets can only be lost if the user is not careful. (Blockchain security, 2017)

3. DISCUSSION OF FINDINGS

3.1 Blockchain Usages

The introduction of blockchain technologies allows for incredible innovation in many industries. Having a trusted ledger allows individuals to interact with other entities with complete transparency. This means that entire industries such as remittances, voting, ride sharing and rental applications can be completely redone from the ground up.

Cryptocurrencies and Virtual Money

The most common usage for blockchain is the cryptocurrency market. Cryptocurrency is digital or virtual tokens that are transacted on a certain network. The most popular cryptocurrency is the first one developed called Bitcoin (BTC). Bitcoin runs on the Bitcoin network also known as the Bitcoin blockchain. This blockchain is responsible for all the transactions every single Bitcoin token goes through, the history of each transaction and the location and address (the public key of the owner) of each token. This means that every time someone uses Bitcoin for any transaction, it is recorded and stored permanently. The advantages of using these tokens is primarily speed and security (*Tapscott, 2015, p.32-40*). Using a newer token such as Ripple (XRP) allows cross border payments within seconds on the Ripple Net (Ripples blockchain network). This is extremely useful as it allows financial

institutions to send and request large amounts of money extremely fast as well as remittance payments across the world. Together the advantages of blockchain based currencies are becoming more exciting for governments and investors as it allows for a much more transparent and secure financial systems.

Redefining the Sharing and Ecommerce Economy

Taking a look at what the blockchain can do for individuals starts at the first step of a secure identity. This identity, which can be recognized by the persons public key holds all their information and transactions on the blockchain. In the case of a rental application, one can look at the renters past transactions and determine, using some rating system provided by the blockchain application, the individual's integrity without ever having to meet them similar to AirBNB. This rating goes beyond just the rental application and can determine the users interactions on other applications as necessary. This allows individuals to create and maintain important and secure personas online.

These identities can be government issued similar to SIN numbers in the form of public keys. With these public keys people can easily get access to health care, air travel and other public services without having to worry about paperwork and documentation. The blockchain will handle it all. Since the blockchain is extremely secure with its encryption, it would be safer than current standards (Tapscott, 2015, p.41-43).

With both identification and trust handled, the only thing left for an AirBNB style system is the payment. Fortunately the blockchain has an efficient, secure and transparent solution already with the cryptocurrencies.

Securing Payments with Smart Contracts

When it comes to payments and transactions, the blockchain does even more than just record and verify transactions. With the creation of smart contracts, transactions can now be enforced. This means that if a payment for a room rental is agreed upon, the blockchain will take the payment and place it in escrow until it is time for the payment to be paid. This prevents double purchasing and also prevents fraud by enforcing the transaction on certain contracted terms.

Taking the blockchain version of AirBNB as an example; if a individual holds \$500 USD worth of BTC in their digital wallet and agrees on a room rental for \$200 USD/night for 2 nights then the blockchain will place \$400 USD worth of BTC in a secure vault (the escrow of the smart contract) inaccessible by neither the owner of the room or the renter. For each

night the renter stays in the room the blockchain will automatically deposit the appropriate sum to the owners account. This can be even further broken down into for each hour, each half hour and so on, creating a complete and total value system.

The implications for this are far beyond just room rentals as it ventures into energy costs, gas and heating bills, internet usage and even mobile data plans. Each individual can pay for what they use as they use it creating the next large advantage of blockchain technologies; distributed power and value (*Tapscott, 2015, p.62-65*).

Distributed Power and Value

How often do individuals use 100% of their allocated internet bandwidth, mobile data, computer or mobile CPU? The answer is not often enough. How can blockchain change these services and many others completely? It can do so efficiently with the power of distribution of value. What this means is individuals can rent out their unused bandwidth or other utilities to others around the world in exchange for cryptocurrencies. Since cryptocurrencies are lighting fast and have near 0 transaction costs the exchange will primarily connect people, power and create value.

Imagine a world where the extra 2 or 3 gigabyte of internet data never used will earn its owner value while they sleep. Imagine not having to pay for more energy or gas then their homes need. This is the power of distribution and it affects many industries. In fact, it is because of distribution that the blockchain is possible as described in *Understanding Blockchain Technologies* and the goal of these technologies is to bring this new paradigm to as many industries as possible.

3.2 Future of Blockchain

Blockchain technologies are still very new and its implications are something engineers and industry experts are continuously studying. However there is already new technologies utilizing the basic concepts of Blockchain but are improving it, making it faster, more secure and even more efficient. One such example is Hashgraph, a blockchain technology boosting speeds more than 50,000 times that of the Bitcoin network.

The way Hashgraph works is similar to the blockchain in it being a distributed ledger, however one key difference is that Hashgraph has been able to take advantage of a coveted computer science algorithm called the gossip algorithm. This algorithm allows the network to predict the state of other nodes without actually polling them for their response. Generally speaking this would be impossible since it is not possible to guarantee that each node will

have the same “vote” or status. However with blockchain, the whole purpose is to make sure everyone has the same blocks, making the discovery of Hashgraph worthwhile. Utilizing this gossip algorithm allows the network to be incredibly fast without sacrificing any security (*Demystifying Hashgraph: Benefits and Challenges, 2017*). At the moment, however, the technology is privatized and not open to the public as the blockchain network is. As more interest and applications appear for this new technology it will be quite apparent that many industries will begin to study and utilize this new version of the blockchain.

Hashgraph is just one of the few technologies that are truly taking advantage of what Satoshi Nakamoto created in 2009 and expanding on what can one day truly change the global economics and the way information is stored throughout the world.

As with many new technologies, there will definitely be hurdles and obstacles to overcome before there is mass adoption. One such obstacle is the regulation of cryptocurrencies, a major usage of blockchain. As the technology gets more attention, both governments and private corporations are sure to see the many benefits in this technology.

4. CONCLUSION

Blockchain technology has only begun to show its fruits though it has not ripen. As more industries and entrepreneurs begin to take advantage of the open and powerful technology, society as a whole will benefit. Creating a trustworthy automated ledger will allow for better records, faster communications and secure transactions. Blockchain will free mankind from many shackles and cryptocurrencies will make way for a fairer and more open economy. An economy in which the government and corporations will be forced to be transparent.

In conclusion, the implications for blockchain in the future are many with each bringing to the world a new set of benefits and paradigms. The future is looking bright for this technology and with newer innovations and adoption the light will only get brighter.

5. REFERENCES

Gupta, V. (2017). *A Brief History of Blockchain*. *Harvard Business Review*. Retrieved from: <https://hbr.org/2017/02/a-brief-history-of-blockchain>

Jiya, Y. (2017). *Demystifying Hashgraph: Benefits and Challenges*. Retrieved from: <https://hackernoon.com/demystifying-hashgraph-benefits-and-challenges-d605e5c0cee5>

Marr, B. (2017). *A Short History of Bitcoin and Crypto currency Everyone Should Read*. Forbes. Retrieved from: <https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-Bitcoin-and-crypto-currency-everyone-should-read/#295388113f27>

Marr, B. (2018). *A Very Brief History Of Blockchain Technology Everyone Should Read*. Forbes. Retrieved from: <https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#3e39a6607bc4>

Miles, C. (2017). Blockchain security: What keeps your transaction data safe?. IBM. Retrieved from: <https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/>

Rosic, A. (2017). What is Blockchain Technology? A Step-by-Step Guide For Beginners. Blockgeeks. Retrieved from: <https://blockgeeks.com/guides/what-is-blockchain-technology/>

Tapscott, D, & Tapscott, A (2015). *Blockchain Revolution*. Toronto, Ontario: Penguin Publications.