The Emergence of Cryptocurrencies

Herman Dhak

APSC 201 Section 204

April 1, 2014

ABSTRACT

The purpose of this report is to provide general information on the topic of cryptocurrencies with an emphasis on the original prototype, the Bitcoin. As the internet becomes an increasingly dominant force in our everyday lives, more and more elements crucial to the function of our society are being transferred over to this massive network, including our finances. It is this shift to an open source network like the internet that provided the framework for a decentralized, peer-to-peer payment system like the Bitcoin protocol that exists today. In this report we will cover the history and usage of Bitcoins, how they are generated, the security issues involved with their use, as well as how they compare to modern fiat currencies.

The material contained in this document was obtained from a combination of online resources and academic journals. Additionally, our team consulted with an expert on the topic who had also completed a similar, but more in depth research project on Bitcoins. Based on our findings, we have determined that the technology that is currently in place to operate the bitcoin system is too complex for the general population to use effectively and securely. However, with a growing number of investors and constant improvements to the network, it is possible that cryptocurrencies like the Bitcoin could become mainstream forms of payment in the future.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

GLOSSARY AND ACRONYMS

Note: Words that are bolded in the text will be defined here.

51% attack: A theoretical attack attack in which a single entity with the majority of the Bitcoin network's computing power attempts to invalidate or rewrite transactions.

Bitcoin (BTC): The first cryptocurrency, created by Satoshi Nakamoto in 2008.

Bitcoin exchange: A trading site where bitcoins can be exchanged for fiat currencies or other cryptocurrencies.

Block: A record in the blockchain which contains three pieces of information: a reference to the previous block, the list of unconfirmed transactions at that point in time, and a random number guess.

Blockchain: A database that contains the public record of all bitcoin transactions in chronological order. On average, every 10 minutes a new block is appended to the blockchain.

BTC: The common unit of Bitcoin currency, similar to USD for United States Dollars.

Cryptocurrency: A peer-to-peer, decentralized, digital currency whose implementation relies on the principles of cryptography.

Cryptography: A branch of mathematics that studies the creation of mathematical proofs to provide high levels of security.

Deflation: A decrease in the general price level of goods and services that occurs when the inflation rate falls below zero percent.

Double spending: When a malicious user tries send the same bitcoins to different recipients at the same time.

ECDSA: Elliptic Curve Digital Signature Algorithm, a mathematical algorithm that uses elliptic curve cryptography to generate digital signatures.

Encryption: The act of encoding messages or information so that only authorized parties may intelligibly make sense of the information.

Hashing rate: A unit of measurement of the processing power of the Bitcoin network.

Inflation: An increase in the general price level of goods and services that occurs in an economy over time.

Market capitalization: The total value of the circulating units of a given stock or currency.

Mining: The process of generating new bitcoins by performing mathematical calculations to confirm transactions in the Bitcoin network.

Mt. Gox: Magic the Gathering online exchange, a popular Bitcoin exchange based in Tokyo, Japan whose systems were compromised and suspended in early 2014.

Nodes: A computer system that is connected to the Bitcoin network.

Peer to peer: Systems that work as an organized collective by allowing each individual to interact directly with others.

Public key: The address which people use to send you bitcoins; it is essentially a username for the Bitcoin network.

Private key: A secret key which authorizes a client to spend the bitcoins belonging to the corresponding public key.

Satoshi Nakamoto: The pseudonym used by the entity responsible for the creation of the Bitcoin network.

SHA-256: Secure Hash Algorithm 256, a cryptographic function that takes an arbitrary message as input and generates a 40 digit number as output.

Signature: The mathematical mechanism used to prove ownership of bitcoins, without the need to see the private key.

Source code: A collection of computer instructions written in a programming language that forms the blueprint of any computer program.

Wallet: A computer program that acts as the equivalent of a physical wallet, it can be used to send and receive bitcoins.

1.0 INTRODUCTION

This document examines the recent development of **cryptocurrencies**, with an emphasis on the most popular type, the **Bitcoin**. As background for your reading of this report, we have included (1) a brief description of the project, (2) the scope of our activities during the study, and (3) an overview of the report format.

1.1 Project Description

At the beginning of the winter term we were informed that we would be assigned a group report on a topic of our choice, as long as it was relevant to our undergraduate program. Alexander suggested we look into the subject of cryptocurrencies. As this was a topic we all had little knowledge about but were very interested in, we decided to make it the subject of our formal report. As outlined in our proposal, we have conducted research and assembled a report on four main topics relevant to our study of cryptocurrencies.

1.2 Scope of Activities

This project involved conducting outside research as well as speaking to an expert that was knowledgeable of our topic. Specifically, the project scope involved:

- Compiling a list of credible sources of information
- Completing research on our subject using the aforementioned reference material
- Finding and interviewing a professional with knowledge of our topic
- Developing conclusions and recommendations that were based on the research completed

1.3 Report Format

To fulfill the report’s purpose for investigating the topic of cryptocurrencies, this report includes these main sections:

- Section 1: Introduction
- Section 2: History and Usage
- Section 3: Cryptocurrency Generation
- Section 4: Security and Anonymity in the Bitcoin Network
- Section 5: Cryptocurrency vs. Modern Fiat Currency
- Section 6: Conclusion

Appendices at the end of the text contain a summary of our interview with an expert on this material, as well as a mechanism description for the blockchain.

2.0 HISTORY AND USAGE OF BITCOIN

The world’s first cryptocurrency known as Bitcoin was developed to address many of the shortcomings of traditional currency. Since its debut in 2008, Bitcoin has experienced a dramatic increase in both value and usage, most likely due to its unique nature. Its popularity has also invoked the development of other types of cryptocurrencies.

2.1 THE INCEPTION OF BITCOIN

The idea of cryptocurrency was conceived in 2008 by an entity known as **Satoshi Nakomoto** (Satoshi, 2008). To this day, it is unknown whether Satoshi is an individual or a group of individuals. In the paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System“, Satoshi discusses the idea of applying the principles of **cryptography** to design a decentralized, secure economic system (Satoshi, 2008). Ultimately, the goal of this system, known as Bitcoin, is to provide a medium through which two parties can transact directly between each other without the need of a third party, such as a bank, to process said transaction. This lack of a third party reduces processing fees for merchants and consumers, and additionally, through the intense mathematical nature of how Bitcoin works, all payments are irreversible. As it is a true **peer-to-peer** system, it is solely maintained and managed by the computational power of the users who actively use it (Satoshi, 2008).

2.2 THE SPREAD OF BITCOIN

The Bitcoin network went live on January 3, 2009. Initially, the currency’s value was set by Bitcoin’s creators to 1308 Bitcoin (BTC) per $1 USD (David, 2014). Since then, the value of a bitcoin has risen drastically to around $459 USD per Bitcoin as of March 31, 2014 (Stats, 2014). As Bitcoin started to gain more public exposure over the next few years individuals began investing into it like a stock, hence this sudden change in price (Bradbury, 2013). Figure 1 below demonstrates the volatility of the price of a Bitcoin versus the US Dollar from 2012 to 2014. The current **market capitalization** of Bitcoin is $7.7 billion (Stats, 2014).

Currently, Bitcoin is mostly accepted by online merchants, however various retail stores are now starting to offer the option to pay with Bitcoin as well (David, 2014). The increased awareness of Bitcoin has been accompanied by a larger number of daily transactions each year. Figure 2 shows that around 63,000 daily transactions occurred with Bitcoin in March 2014. Five years earlier in 2009, there were a mere 100 daily transactions on average.

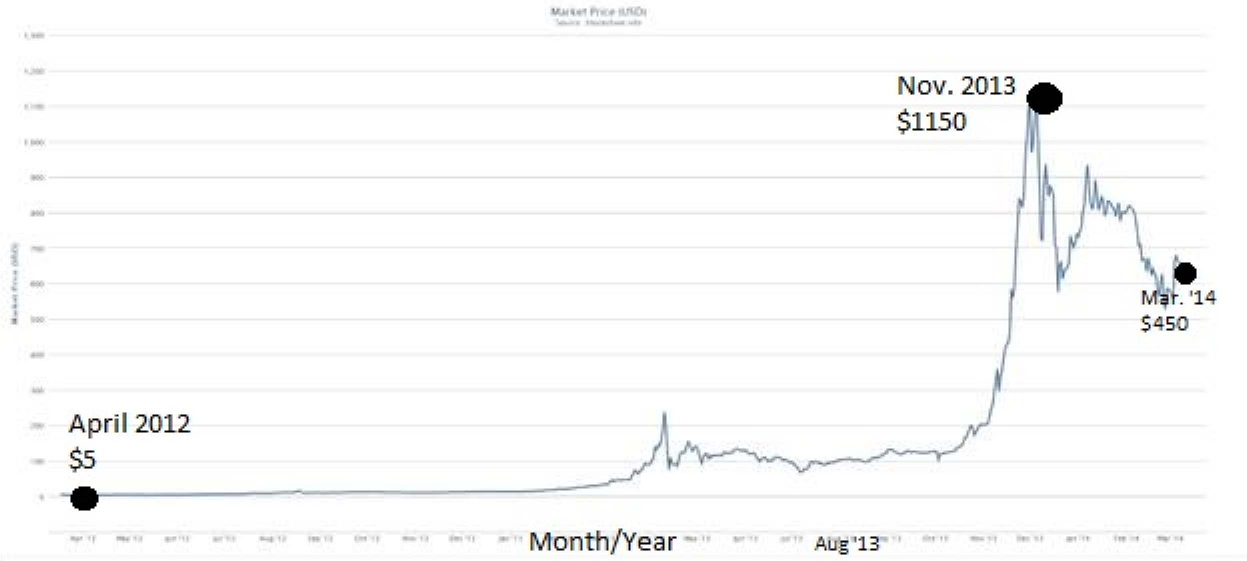

Figure 1: Chart of Bitcoin Market Price (USD) (image courtesy of blockchain.info)

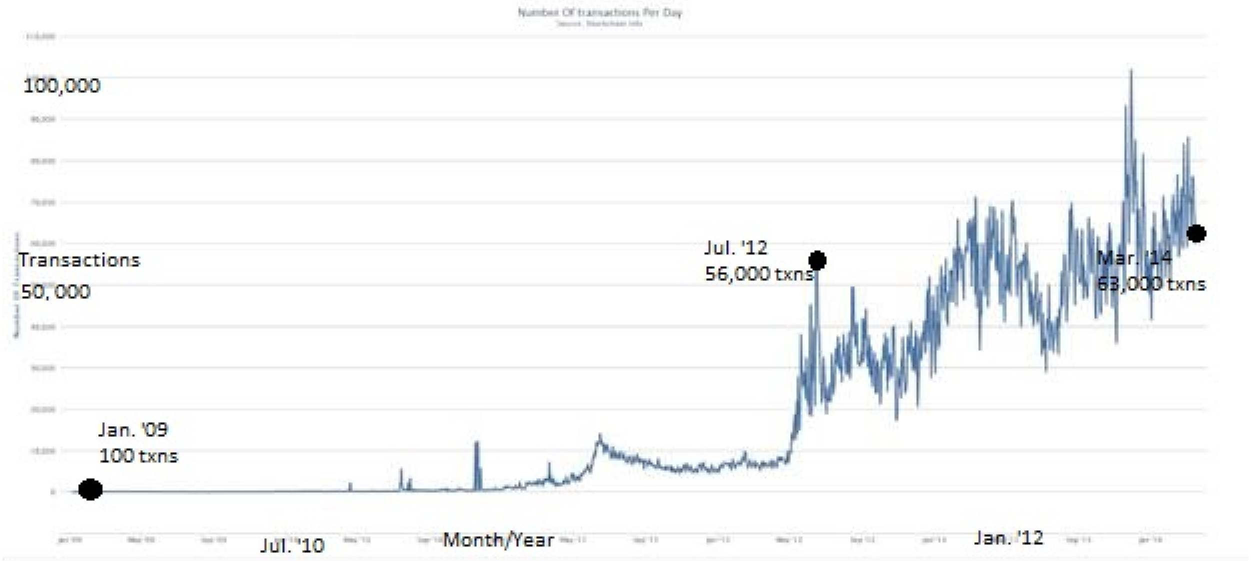

Figure 2: Chart of the Number of Bitcoin Transaction per Day(image courtesy of blockchain.info)

2.3 OTHER CRYPTOCURRENCIES

The **source code** for the Bitcoin protocol is available online for anyone to view or modify. This has led to software developers inventing other types of cryptocurrencies. Each one has its own unique implementation which differentiates it from the others. However, this report will not cover those in detail as they are all variations of the original Bitcoin protocol. A few other types of cryptocurrencies being traded include Litecoin, Namecoin, and Feathercoin (Berson, 2013). As Bitcoin is the original cryptocurrency, it has received the most media attention and thus it is currently the most widely traded. This may change in a few years as these systems evolve into a single, more secure and accessible next-generation cryptocurrency.

3.0 CRYPTOCURRENCY GENERATION

Bitcoin generation is the introduction of new bitcoins into the system through the process of solving **blocks**. This section will focus on the mechanisms behind Bitcoin ownership, generation and spending, as well as touch on how the last two processes are intertwined.

3.1 PRIVATE STORAGE AND NETWORK STORAGE

On the user's storage device with their **wallet** file, they will have multiple wallet addresses which are references to the **public keys** on the network (Hobson, 2013, p. 42). Also stored in the wallet file are the **private keys** used to authorize a transaction, which are only available to the user. To spend **BTC** in transactions you must verify that you are the true public address where the money was sent. A **function** which takes the message and private key as input produces a **signature** which is used to verify you have the private key, without actually seeing it. This signature is used again along with the message to verify that you are the owner of the public key (See Figure 3).

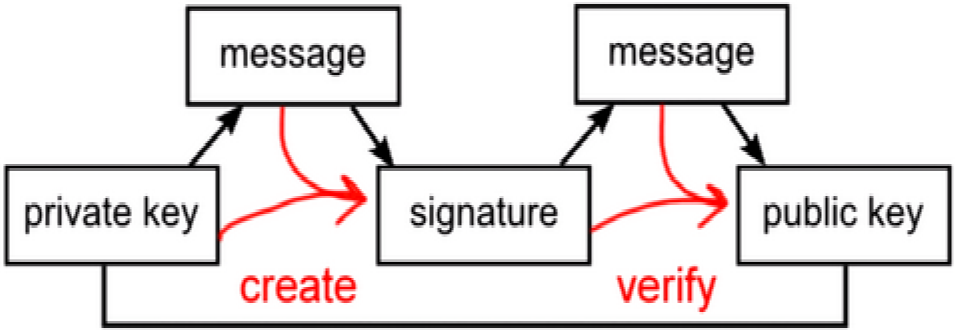

Figure 3: Bitcoin Private Key Verification (image courtesy of CuriousInventor)

Users have full control of their wallet file, and should the file get lost or deleted, the references to the coins stored on the peer-to-peer network are lost as well, effectively making them unspendable (Surowiecki, 2011).

The amount of bitcoins each person owns is stored online in a ledger known as the transaction chain. This ledger keeps a record of each person's received and spent transactions. The total number of bitcoins in an account is the amount of received transactions minus the spent transactions. For example, If John wants to send 10 BTC to Bill, John must reference other transactions where he received 10 or more BTC; the reference transactions are know as inputs (Driscoll, 2013). Other computers on the network will verify that the transaction information is correct. Once a transaction has been used as an input, it is considered spent, and cannot be used again. To protect against spending inputs multiple times, it is important that there is a system which allows the order of transactions to be recorded, this system is known as the **blockchain** (Satoshi, 2008).

3.2 BLOCK REWARDS

Fresh bitcoins are created by the network in a process called **mining.** Mining consists of spending computational power to introduce new bitcoins into the system. The **nodes** on the Bitcoin network are awarded new bitcoins each time they solve a complex computational problem. The network automatically calculates and assigns a level of difficulty for these problems so that on average a new block is solved every 10 minutes. Once the solution to the block is found, the node which solved the block submits their solution to the network. When a block is completed it gives a reward to the miners who helped find it, based off of their **hashing rate** (Berson, 2013, p. 32). The current block reward for the pool is 25 BTC. The reward is halved every four years, so eventually no new bitcoins will be added to the system.

3.3 THE BLOCKCHAIN

The sole purpose of solving blocks isn't only to introduce new bitcoins into the system. Each block contains the list of all unconfirmed BTC transactions, a reference to the previous block, and the random guess from the user to guess the solution to the block (Satoshi, 2008). The computational problem depends on each of the previous blocks, and thus the calculation is impossible to know before the previous block has been found and published. Additionally, new blocks are added to the end of the blockchain. Therefore the blockchain also serves as a ledger of all transactions, and the order in which they happened (See Figure 4). The purpose of the chain is to prevent **double spending**, verifying that a bitcoin transaction has not occurred more than once (Betancourt, 2013).

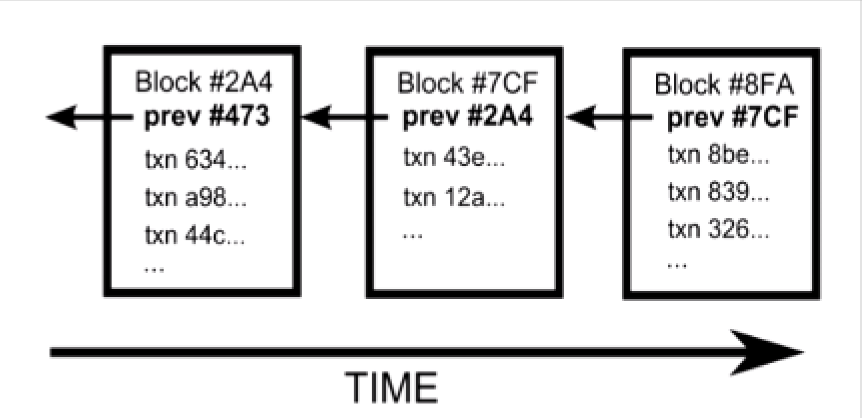

Figure 4: The Blockchain (image courtesy of CuriousInventor)

4.0 SECURITY AND ANONYMITY IN THE BITCOIN SYSTEM

Bitcoin relies heavily upon public key cryptography to maintain the security of its system and transactions. In doing so, the system has embedded the strength and rigor of mathematics itself into maintaining the security of the infrastructure.

4.1 SECURITY OF THE BITCOIN PROTOCOL

The system utilizes military grade modern cryptography such as the **SHA-256** and **ECDSA** to generate public and private keys for Bitcoin users, along with signatures used to verify ownership of keys (Yang, 2011). By operating on a decentralized peer-to-peer system, the amount of information that each user needs to provide in order to conduct a transaction is reduced. In a transaction, only the public key is used to receive input references, and could potentially be used to identify the user. It is possible for a user to generate a new public key for each and every transaction they conduct, minimizing the probability of identification (Betancourt, 2013). Bitcoin users thus enjoy a significant degree of anonymity, although transactions on the Bitcoin network are by no means untraceable.

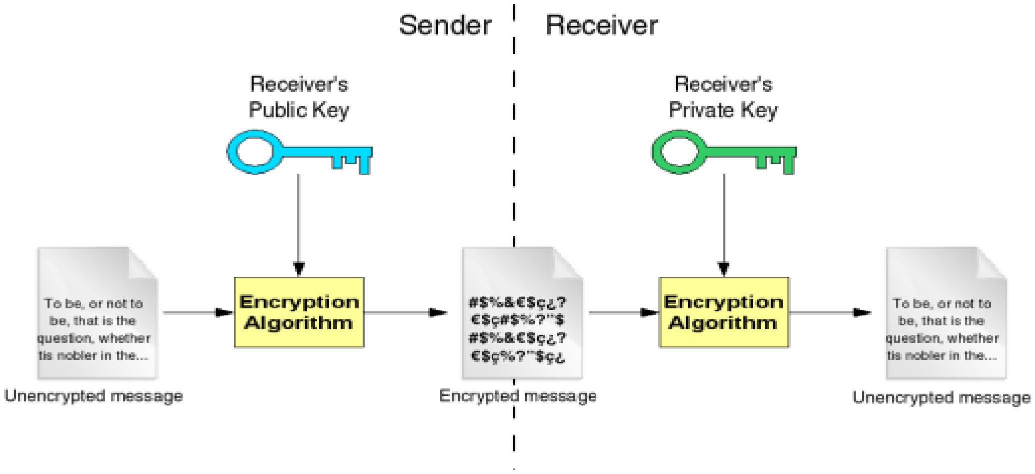

Figure 5: Public/private key pair encryption (image courtesy of University of Chicago)

4.2 NETWORK SECURITY RISKS

With deep roots in cryptography, the premise of Bitcoin's design was to protect against malicious attempts at manipulating the system. However, it is by no means impenetrable, as numerous weaknesses exist within it. Whenever two or more blocks are solved simultaneously, forks in the blockchain are created as differing copies of the blockchain are broadcasted to the network. The fork that forms the longest blockchain is recognised as the legitimate blockchain by the network. Theoretically, a malicious user with an exceptional amount of computing power could nullify transactions by solving and broadcasting a longer blockchain to the network (Bradbury, 2013). This is known as a **51% attack,** as it is postulated that this sort of attack requires at least 51% of the Bitcoin network's total computing power if it is to have a reasonable chance of succeeding (Weaknesses, 2013). In reality, the vast amount of computing resources that would be necessary to compete against the entirety of the Bitcoin network diminishes the feasibility of such an attack.

4.3 CLIENT-SIDE SECURITY RISKS

An unfortunate flaw of Bitcoin originates from the sheer complexity of the system. Bitcoin was designed with the assumption of a technically knowledgeable user-base and thus users of lesser technical inclination are more vulnerable to theft and fraud (Hobson, 2013, p. 43). By default, information stored in a user's Bitcoin wallet is unencrypted allowing both private and public keys associated with the wallet to be easily extracted (Weaknesses, 2013). Such an issue is easily resolved by encrypting the wallet with a simple password, but it depends entirely upon the user to recognise the need for such a precaution.

4.4 THIRD-PARTY SECURITY RISKS

Cryptocurrency exchanges, such as the infamous **Mt. Gox**, present another critical point of vulnerability in end-user security. Unlike the Bitcoin system, cryptocurrency exchanges are centralized businesses subjected to anti-money laundering laws that often require users to formally identify themselves through official documentation (Hobson, 2013, p. 44). Since these organizations operate independently of the Bitcoin Foundation, malicious users may exploit vulnerabilities present in these exchanges to bypass the security of the Bitcoin protocol. Should these exchanges be compromised, both the identities and assets of their clients would be susceptible to theft.

Figure 6: Logo of Mt. Gox exchange (image courtesy of Mt. Gox)

5.0 CRYPTOCURRENCIES VERSUS MODERN FIAT CURRENCIES

One of the key differences between cryptocurrencies and modern **fiat currencies** lies in who controls their production and regulation. While fiat currencies are backed by a central governing body, cryptocurrencies fall outside the control of the state and consequentially are not generally government regulated. However, in recent years some countries such as China and Taiwan have placed prohibitions on the trading of Bitcoins, while others like Thailand and Russia have gone so far as to ban their use entirely (Komnenic, 2014).

5.1 PRODUCTION AND REGULATION

As discussed in an earlier section, the production or "mining" of bitcoins is essentially the transformation of the immaterial labor of computers into a tradable form of currency. This mirrors past commodity-based fiat currencies that attempted to "preserve labour in an exchangeable form" (Betancourt, 2013) and is similar to the common practice of paying monetary wages for human labour.

Like fiat currencies, bitcoin production is subject to stringent regulations, both to prevent new coins from entering the system too rapidly, as well as to ensure the total number of bitcoins produced does not exceed 21 million. In order to achieve this, there are two main methods currently in place, the first being that the number of new bitcoins awarded for every block of transactions completed will be halved every four years (Betancourt, 2013). Secondly, as mentioned in an earlier section, the difficulty of the computational problems solved during the mining process is constantly adjusted to keep the block completion time at approximately ten minutes. This procedure in turn directly controls the rate of bitcoin production.

It is also important to note that due to the aforementioned imposed maximum on Bitcoin production, the cryptocurrency will some day be unable to experience **inflation** and **deflation** like fiat currencies, or at least not in the same manner. While fiat money is not a limited in how much can ever be printed, once the maximum Bitcoin count is reached its production will be permanently halted. However, because the currency is digital there is no physical limit in how many times it can be subdivided. Therefore, should the value of Bitcoin increase too much, the currency could be split into smaller units accordingly so that access to Bitcoin wasn't limited to only those who could afford an entire coin (Graham, 2014). One such subunit currently in existence is the Satoshi, which is equal to 0.00000001 Bitcoin ("Units", 2013).

5.2 SECURITY AND PRIVACY

As a form of peer-to-peer payment where a user's bitcoins can only be "stored" in a unique wallet address, Bitcoin moves away from the use of centralized financial service providers like banks and online payment systems such as Paypal that are so essential to the use of fiat currencies (Hobson, 2013). An advantage of this is it allows owners to have full control over their assets, as well as avoids having personal information regarding their spending habits monitored by a third party (Hobson, 2013). However, this also results in the bearer being solely responsible for ensuring the security of his or her Bitcoins. Without proper knowledge of how the system operates, there is risk of users’ personal identities being linked to their transactions on the block chain, or even having their bitcoins stolen if they accidentally share their wallet addresses. In short, the Bitcoin system allots users more control over their funds, but fiat currencies are still considerably simpler to use in that they requires far less technical knowledge.

6.0 CONCLUSION

We first investigated the origins of cryptocurrencies along with their current market value, followed by an explanation of the technology involved in their generation and management. This included an overview of how the block chain serves as both a record of all transactions and as a means to produce new bitcoins through the mining process. We have also listed the security measures currently in place to protect Bitcoin users and the network from potential hackers, as well as examined potential weaknesses within the system that have yet to be addressed. Finally we compared cryptocurrencies to modern fiat currencies with emphasis on their production, regulation and security.

Although cryptocurrencies are still a relatively new to the global scene, considering the current net worth of Bitcoin alone it is clear there is potential for these digital currencies to become an internationally recognized, mainstream form of payment in the future. However, in order for this to happen, the system on which they operate must first improve its security as well as reduce the technical complexity tied to its use. Doing so will allow it to strongly compete swith the already well established fiat currency systems currently in place.

REFERENCES

Berson, S. A. (2013). Virtual money: Some basic rules for using 'bitcoin. *ABA Journal, 99*(7), 32.

Betancourt, M. (2013). Bitcoin. *Ctheory, Theory Behind The Codes*. Retrieved from http://www.ctheory.net/articles.aspx?id=724

Bradbury, D. (2013). The problem with bitcoin. *Computer Fraud & Security, 2013*(11), 5. doi:10.1016/S1361-3723(13)70101-5

Brezo, Felix. Bringas, Pablo G. (2012). Issues and Risks Associated with Cryptocurrencies Such as Bitcoin. *The Second International Conference on Social Eco-Informatics,* 12 , 20-26.

Driscoll, S. [CuriousInventor]. (2013, July 14). *How Bitcoin Works Under the Hood* [Video File]. Retrieved from https://www.youtube.com/watch?v=Lx9zgZCMqXE

Graham S. (2013). *Bitcoin*. Toronto: Rogers Publishing Limited, 21(2).

Graham, R. (2014, February 19). If anything, Bitcoin is inflationary. Retrieved from http://blog.erratasec.com/2014/02/if-anything-bitcoin-is-inflationary.html#.Uzp7

Hobson, D. (2013). What is bitcoin? *XRDS: Crossroads, the ACM Magazine for Students, 20*(1), 40-44. doi:10.1145/2510124

Karstens-Smith, G. (2014). 'Cryptocurrency' users can fill virtual wallet at toronto's first bitcoin ATM: New machine 'an easy way' to introduce complex digital payment system to the masses. *Toronto Star*, pp. B.1.

Komnenic, A. (2014, January 7). As Bitcoin became more popular, these countries became more suspicious. Retrieved from http://www.mining.com/these-countries-are-the-most-uneasy-about-bitcoin-87882/

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

ShaikShakeel, A. Madhusoodhnan, N. Biju, V. (2013). A Survey on Crypto Currencies. Retrieved from http://searchdl.org/public/conference/2013/AETACS/131.pdf

Stats. (2014) In *Blockchain.* Retrieved from http://blockchain.info/stats

Surowiecki, J. (2011). *Cryptocurrency*. Cambridge: Technology Review, Inc.

Weaknesses. (2013) In *Bitcoinwiki*. Retrieved from https://en.bitcoin.it/wiki/Weaknesses

Units. (2013) In *Bitcoinwiki*. Retrieved from https://en.bitcoin.it/wiki/Weaknesses

Yang, E. (2011, June 3). The Cryptography of Bitcoin. *Inside 206-105*. Retrieved from http://blog.ezyang.com/2011/06/the-cryptography-of-bitcoin/

Yermack, D.. (2014). *Bitcoin economics*. Cambridge: Technology Review, Inc.

APPENDIX:

MECHANISM DESCRIPTION OF THE BLOCKCHAIN

1.0 INTRODUCTION

The blockchain is the tool which orders all bitcoin transactions chronologically. Each block contains a reference to the previous block, and this is where the ordering is derived. A block is created by organizing all **unconfirmed transactions** into the block and broadcasting the result to the network. The block's publisher must also solve a problem, randomized by the SHA-256 hashing function. The problem's difficulty can be altered, and there is a BTC reward for the computers which contributed to finding the block.

2.0 PART-BY-PART DESCRIPTION

Now the individual mechanisms of the blockchain will be described.

2.1 INDIVIDUAL BLOCK

Each block contains: a reference to the previous block, the list of all unconfirmed transactions, and a random number guess (See Figure Below). A transfer of BTC will remain unconfirmed from the time it's created to when the next block is solved. The block is plugged into the hashing function to find the solution.

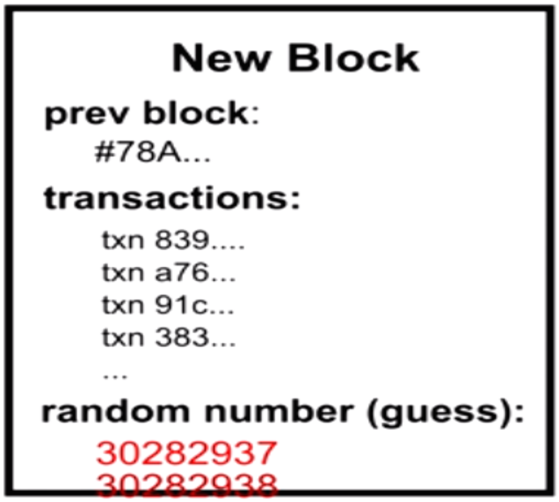

Figure 7: Abstraction of a block (image courtesy of CuriousInventor)

2.2 SHA-256 HASHING FUNCTION

The entire text of the block, along with the random guess is used as an input for the SHA-256 hashing function. If the output of the function is below a certain value, the solution is correct. Changing a single digit in the block changes the results of the output drastically; this way the solution the guess at the end of each block is effectively random.

2.3 NETWORK DIFFICULTY AND REWARD

The difficulty of each block depends on the probability of receiving the solution to the block with each guess. The difficulty of the solution is automatically changed so that on average, a new block is created every 10 minutes. A 25 BTC reward is given to the miners in each pool based off of the amount on hashes they contributed to finding the solution. The reward itself is halved every four years.

3.0 CONCLUSION

The purpose of a the block-chain is to order all bitcoin transactions. Transactions are confirmed once the next block is found. Each block contains: a reference to the previous block, a list of unconfirmed transactions, and a random guess. The block is plugged into the SHA-256 hashing function to find the solution. The miners who solved the block are rewarded with BTC based upon the amount of work they did.

INTERVIEW WITH AN EXPERT

To validate the data in our report, our team interviewed Nick, a 4th year undergraduate computer engineering student at UBC. Nick lead a team of other senior undergraduate students on a research project in which they analyzed the security mechanisms implemented by the Bitcoin network. This project was conducted under the guidance of Dr. Konstantine Besznosov, a professor at UBC who specializes in cryptography. Nick and his team presented their findings in a formal report. Due to the nature of their project, much of our discussion with Nick centered around Bitcoin security.

Some of the major points made by Nick included:

- It is unlikely for the overall Bitcoin network to be compromised by malicious users because that would require controlling at least 51% of it which is nearly impossible.
- Users should ensure they are well-informed of potential security breaches when creating local Bitcoin wallets on their computers in order to keep their Bitcoins secure.
- Since there are numbers such as timestamps tied to your Bitcoin transactions, you are not completely anonymous on the Bitcoin network.
- To improve Bitcoin, software developers should continue to watch out for malicious attacks on the Bitcoin network and adjust the security measures in place to prevent future attacks.

Ultimately, the conclusion drawn by Nick was that the security of any system is only as secure as the amount of effort one is willing to exert to make it secure. He had no strong opinions on whether Bitcoin would become the world’s main type of currency in the future.

Outside of this project, Nick does not actively trade bitcoins.