BITCOIN

A Seminar Report

Submitted By

Shantanu Kumar Singh

In partial fulfilment for the award of the degree of

Bachelor of Technology

IN

Computer Science & Engineering

At

Integral University, Lucknow

Kursi Road Lucknow-226026, Uttar Pradesh

Phone: 0522-2890812, 2890730, 3296117, 6451039

2015 - 2016

A Seminar Report

On

By: Shantanu Kumar Singh

CSE-4, Final Year

1200112202

ABSTRACT

Bitcoin is a decentralized electronic cash system using peer-to-peer networking to enable payments between parties without relying on mutual trust. It was first described in a paper by Satoshi Nakamoto (widely presumed to be a pseudonym) in 2008. Payments are made in bitcoins (BTC's), which are digital coins issued and transferred by the Bitcoin network. The data of all these transactions, after being validated with a proof-of-work system, is collected into what is called the block chain. Participants begin using bitcoin by first acquiring a program called a Bitcoin wallet and one or more Bitcoin addresses. Bitcoin addresses are used for receiving bitcoins. Even though Bitcoin is considered to be an experimental payment system, it is already deployed on a large scale (in the sense that the current value of all the coins issued so far exceeds 4,673,522,976 USD) and attracts a lot of media attention. Its proponents claim that it is the first truly global currency which does not discriminate its users based on citizenship or location, it is always running with no holidays, it is easy to secure with very low usage fees, it has no charge backs, etc. On the other hand, its detractors claim that it is widely misused to buy illegal items and to launder large sums of money, and that it is too easy to steal bitcoins from wallets via cyber-attacks.

The concept has grown since its shadowy introduction in 2009, and bitcoin values have fluctuated from as low as US$2.95 to nearly $1,200 per bitcoin. To date, over 14.78 million bitcoins exist, with a rough aggregated valuation of around $4.6B in Nov'15. The wallet contains nothing more than a regularly updated file, listing all bitcoin transactions ever made. The public and private key combinations permit a degree of privacy among those who exchange bitcoins.

The Researchers have proposed a system for electronic transactions without relying on trust. They started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, they proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power.

TABLE OF CONTENTS

CERTIFICATE

This is to certify that Shantanu Kumar Singh, student of B.Tech. C.S.E Fourth Year has presented a seminar on the topic **"BITCOIN"** as a final year seminar during the session 2015-2016.

This seminar report is submitted in the partial fulfilment of the requirement for the award of the degree of B.TECH. in Computer Science & Engineering from Integral University.

Mohammadi Akheela Khanum
(Associate Professor)

Ms. Saima Rehman
(Assistant Professor)

Mrs. Dr. Kavita Agarwal
(Head of Department)

ACKNOWLEDGEMENT

There is always a sense of gratitude which people express towards others for their help and supervision in achieving the goals. This formal piece of acknowledgement is an attempt to express the feeling of gratitude towards people who helped me in successfully completing my presentation.

I would like to express my deep gratitude to Mohammadi Akheela Khanum and Ms. Saima Rehman, my seminar coordinators for their constant co-operation. They were always there with competent guidance and valuable suggestions throughout the pursuance of this presentation.

I would also like to appreciate all the respondents and group members whose responses and coordination were of utmost importance for the presentation and who helped me a lot in collecting necessary information.

Above all no words can express my feelings to my parents, friends and all those people who supported me during my seminar.

Shantanu Kumar Singh

1200112202

Chapter 1

BITCOIN

Bitcoin uses peer-to-peer technology to operate with no central authority or banks; managing transactions and the issuing of bitcoins is carried out collectively by the network. Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part. Bitcoin is a network that enables a new payment system and a completely digital money.

1.1 Introduction

Bitcoin is a peer-to-peer payment system introduced as open source software in 2009 by developer Satoshi Nakamoto. The digital currency created and used in the system is also called bitcoin and is alternatively referred to as a virtual currency, electronic money, or cryptocurrency. The bitcoin system is not controlled by a single entity, like a central bank, which has led the US Treasury to call bitcoin a decentralized currency. Economists generally agree that it does not meet the definition of money

Bitcoins are created as a reward for payment processing work in which users who offer their computing power verify and record payments into a public ledger. Called mining, individuals engage in this activity in exchange for transaction fees and newly minted bitcoins. Besides mining, bitcoins can be obtained in exchange for other currencies, products, and services. Users can buy, send, and receive bitcoins electronically for a nominal fee using wallet software on a personal computer, mobile device, or a web application.

1.2 History

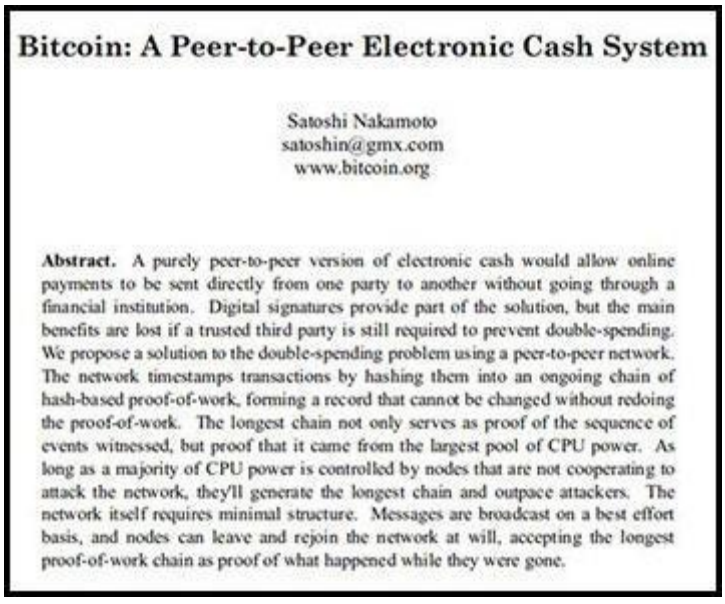
Bitcoin was first mentioned in a 2008 paper published under the name Satoshi Nakamoto. In 2009, an exploit in an early bitcoin client was found that allowed large numbers of bitcoins to be created. The price of bitcoins has fluctuated wildly since its inception, going through various cycles of appreciation and depreciation, which have been referred to by some as bubbles and busts. In 2011, the value of one bitcoin rapidly rose from about US$0.30 to US$32 before returning to US$2.

In the latter half of 2012 and during the 2012-2013 Cypriot Financial Crisis, the bitcoin price began to rise, reaching a peak of US$266 on 10 April 2013, before crashing to around US$50. In the end of 2013, the cost of one bitcoin rose to the all-round peak of US$1135, but fell to the price of US$693 three days later.

Some mainstream websites began accepting bitcoins c. 2013. WordPress started in November 2012 followed by OKCupid in April 2013, TigerDirect in January 2014, andOverstock.com that same month. Certain non-profit or advocacy groups such as the Electronic Frontier Foundation allow bitcoin donations. (Although this organization subsequently stopped accepting bitcoin.)

October 31, 2008 The white paper is published.

Nakamoto published a design paper through *metzdowd.com* cryptography mailing list that describes the Bitcoin currency and solves the problem of double spending so as to prevent the currency from being copied.



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1.3 Creation of Bitcoin

Bitcoin is the first implementation of a concept called "crypto-currency", which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi left the project in late 2010 without revealing much about himself. The community has since grown exponentially with many developers working on Bitcoin.

Satoshi's anonymity often raised unjustified concerns, many of which are linked to misunderstanding of the open-source nature of Bitcoin. The Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software. Just like current developers, Satoshi's influence was limited to the changes he made being adopted by others and therefore he did not control Bitcoin. As such, the identity of Bitcoin's inventor is probably as relevant today as the identity of the person who invented paper.

1.4 Mining

Bitcoin mining is the processing of transactions in the digital currency system, in which the records of current Bitcoin transactions, known as a blocks, are added to the record of past transactions, known as the block chain.

A Bitcoin is defined by the digitally signed record of its transactions, starting with its creation. The block is an encrypted hash proof of work, created in a compute-intensive process. Miners use software that accesses their processing capacity to solve transaction-related algorithms . In return, they are awarded a certain number of Bitcoins per block. The block chain prevents attempts to spend a Bitcoin more than once -- otherwise the digital currency could be counterfeited by copy and paste.

Originally, Bitcoin mining was conducted on the CPUs of individual computers, with more cores and greater speed resulting in more profitability. After that, the system became dominated by multi-graphics card systems, then field-programmable gate arrays (FPGAs) and finally application-specific integrated circuits (ASICs), in the attempt to find more hashes with less electrical power usage.

Due to this constant escalation, it has become hard for prospective new miners to start. This adjustable difficulty is an intentional mechanism created to prevent inflation. To get around that problem, individuals often work in mining pools.

Bitcoin generally started with individuals and small organizations mining. At that time, start-up could be enabled by a single high-end gaming system. Now, however, larger mining organizations might spend tens of thousands on one high-performance, specialized computer.

In the malware world, one of the more prevalent current threats is mining botnet infections, in which user systems mine for Bitcoin without the owners' knowledge and funds are channelled to the botnet master.

1.5 Bitcoin Mining Hardwares:

BITCOIN MINING BY THE GH

300 GH BITCOIN MINING CARD

1 TH BITCOIN MINER

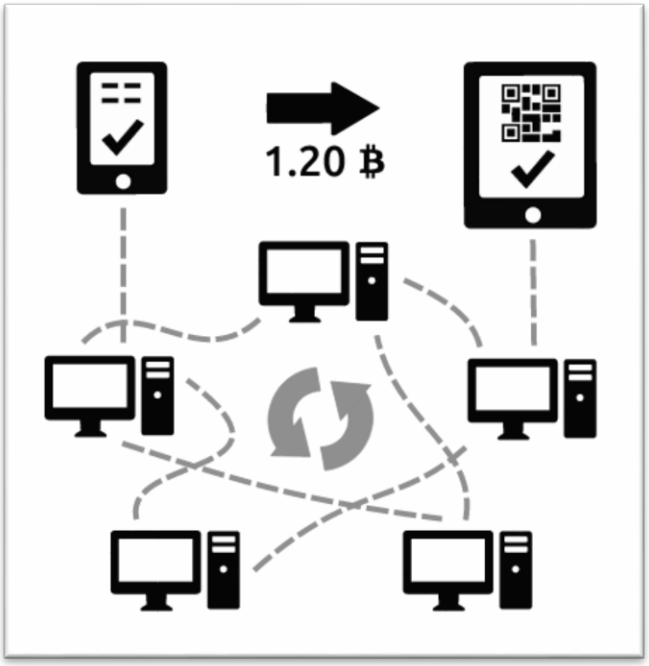
Chapter 2

WORKING OF BITCOIN

2.1 Introduction

The basics for a new user-

As a new user, you can get started with Bitcoin without understanding the technical details. Once you have installed a Bitcoin wallet on your computer or mobile phone, it will generate your first Bitcoin address and you can create more whenever you need one. You can disclose your addresses to your friends so that they can pay you or vice versa. In fact, this is pretty similar to how email works, except that Bitcoin addresses should only be used once.



2.2 Balances - Block Chain:

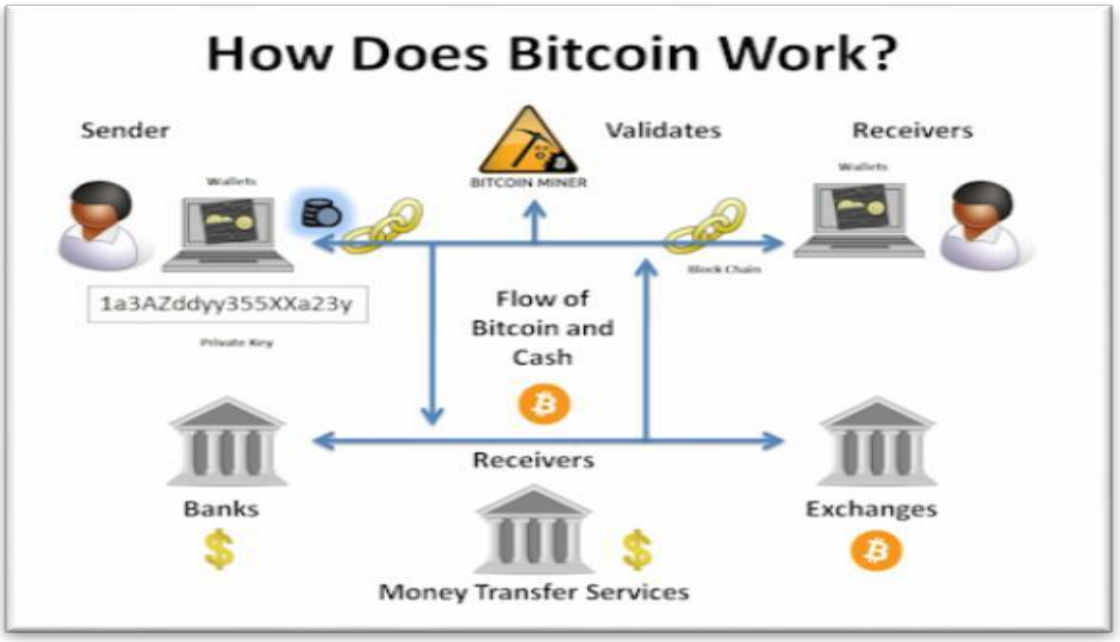
The block chain is a **shared public ledger** on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.

2.3 Transactions - Private Keys:

A transaction is **a transfer of value between Bitcoin wallets** that gets included in the block chain. Bitcoin wallets keep a secret piece of data called a *private key* or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The *signature* also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast between users and usually begin to be confirmed by the network in the following 10 minutes, through a process called *mining*.

2.4 Processing – Mining:

Mining is a **distributed consensus system** that is used to *confirm* waiting transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a *block* that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks. 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 control what is included in the block chain or replace parts of the block chain to roll back their own spends.



Chapter 3

PAYMENT METHOD

3.1 Using Bitcoin as an Individual

Install the official Bitcoin client on your computer. To get started using Bitcoin, whether you want to set it up on your phone or online, you'll need to download the client and visit the main Bitcoin page to set up your account on the computer. The client is suitable for Mac, Windows, and Linux.

Set up your wallet:

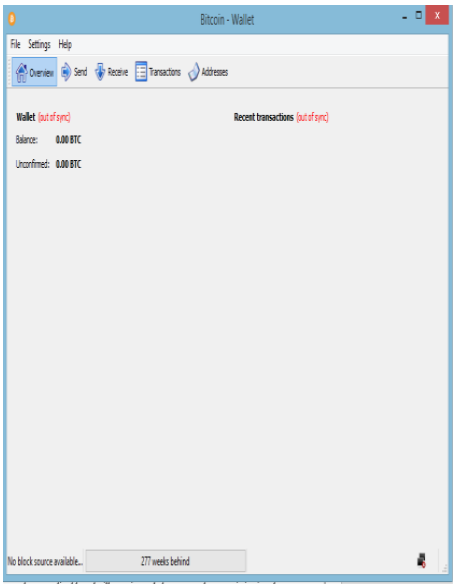
Like regular money, you've got to have a place to keep your digital money. Wallets are basically programs that sort and track your digital currency via your account settings. There are a variety of options available, depending on your intentions for using Bitcoin.

Software wallets don't run on a third-party service after download. These wallets are operated from your computer, where you'll have to run a local blockchain to keep your transactions anonymous. This is the wallet for which the Bitcoin was originally conceived. Software wallets include:

- BitcoinQT
- Armory
- Multibit
- Copay

Software Wallets

For PC

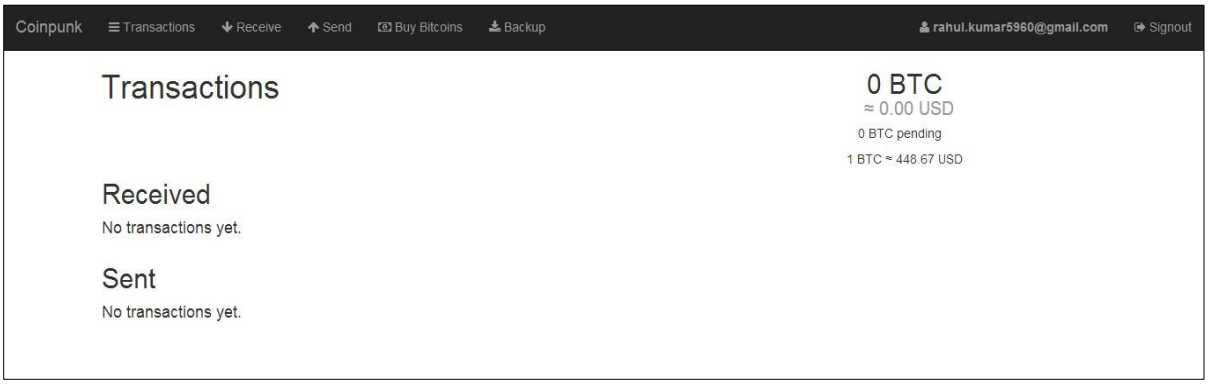


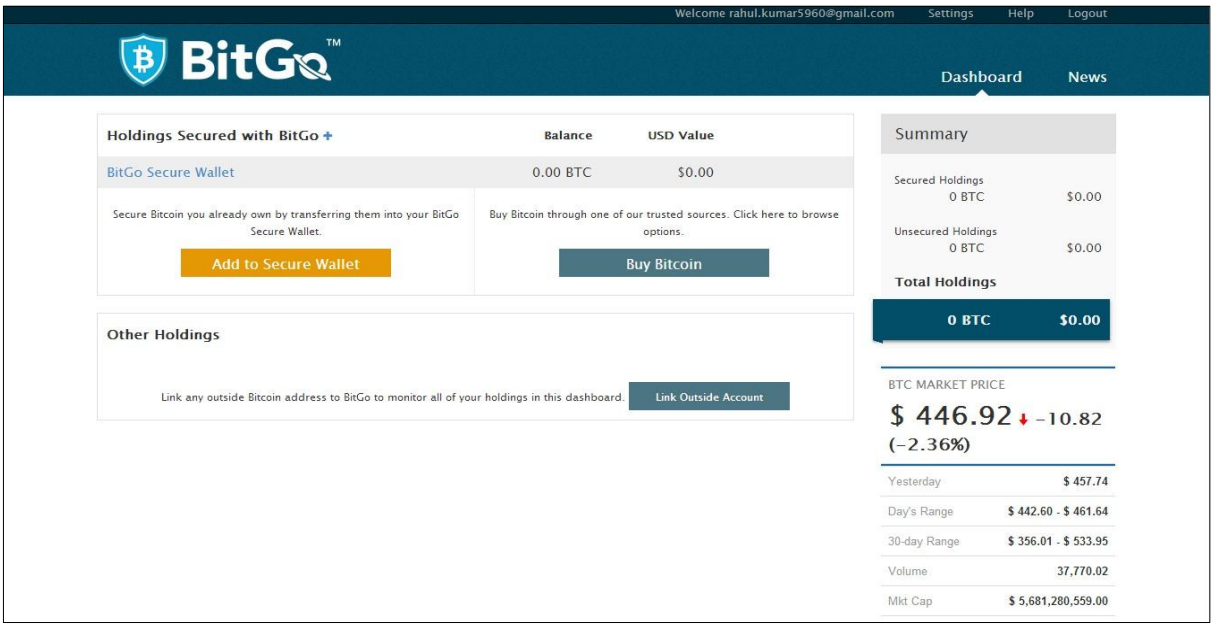
For Mobile

Web wallets are always available online, making them probably the most convenient and user-friendly. All you need to do is set up an account and log in. They are, however, potentially somewhat less secure than hardware wallets, though each of these is also compatible with most Mobile phone providers. Web wallet options include:

- Blockchain
- Coinbase
- Coinjar
- Coinpunk
- BitGo

Web Wallets


Coinpunk
Transactions
Receive
Send
Buy Bitcoins
Backup
rahul.kumar5960@gmail.com
Signout
Transactions
0 BTC
≈ 0.00 USD
0 BTC pending
1 BTC ≈ 448.67 USD
Received
No transactions yet.
Sent
No transactions yet.


Welcome rahul.kumar5960@gmail.com
Settings
Help
Logout
BitGo
Dashboard
News
Holdings Secured with BitGo
Balance
USD Value
BitGo Secure Wallet
0.00 BTC
$0.00
Secure Bitcoin you already own by transferring them into your BitGo Secure Wallet.
Add to Secure Wallet
Buy Bitcoin through one of our trusted sources. Click here to browse options.
Buy Bitcoin
Other Holdings
Link any outside Bitcoin address to BitGo to monitor all of your holdings in this dashboard.
Link Outside Account
Summary
Secured Holdings
0 BTC
$0.00
Unsecured Holdings
0 BTC
$0.00
Total Holdings
0 BTC
$0.00
BTC MARKET PRICE
$ 446.92 -10.82
(-2.36%)
Yesterday
$ 457.74
Day's Range
$ 442.60 - $ 461.64
30-day Range
$ 356.01 - $ 533.95
Volume
37,770.02
Mkt Cap
$ 5,681,280,559.00

Get some Bitcoin:

Now that you've got everything set up, great, but how do you get bit coins to spend? There are several options available to grow your wallet and acquire more Bitcoin to spend. While the system is somewhat unpredictable and still experimental, they seem to be appreciating in value, making Bitcoins a unique opportunity. You can earn Bitcoin in several ways.

- **To purchase Bitcoin**, it's helpful to visit a database of Bitcoin marketplaces, likethis one. You'll simply complete a transaction at most marketplaces, in which your currency in converted into Bitcoin. You can also convert cash into Bitcoin using a similar process.

- **To mine Bitcoin** you can download and run a miner like CGMiner on a custom CPU that can theoretically turn a profit without doing much of anything at all. While you used to be able to do this on your home desktop, it's not much of a practical possibility anymore. You'll spend more on electricity keeping the computer running than you will turning a profit.

- **To trade Bitcoin**, look for other people participating in Bitcoin interested in transactions. You can find them at trading sites. In addition, if you sell goods or services, consider offering Bitcoin as a method for accepting payment.

Secure your wallet:

Now that you've actually got some coins in your purse, you want to make sure they're protected. Unfortunately, older Bitcoin clients won't encrypt the wallet.dat file, which means that anyone who can access it could theoretically swipe your Bitcoin. The good news is you can secure your wallet to ensure that this won't happen.[2]

- If you want, you can run a file encryption program.
- Click the menu option “Settings” -> “Encrypt Wallet”.
- It's also a good idea to try and keep two different wallets, one account for daily use and making transactions and a separate savings account, offline, where you might consider storing the bulk of your Bitcoin.

3.2 Using Bitcoin as a Merchant:

Learn how to accept Bitcoin:

Follow the basic steps of setting up a secure wallet and preparing for transactions as you would for an individual account, and then explore your payment processing options to make your business Bitcoin-friendly. There are a variety of Bitcoin services designed for vendors to facilitate transactions and work alongside businesses to make Bitcoin use simple and safe. Some have small transaction fees associated with them, while others are free. [3]

- Blockchain is free and semi-complex, but requires no account or set-up.
- Coinbox is basically the Bitcoin equivalent of Square, a mobile app that lots of small businesses use to process card payments quickly and affordably.
- BitPagos is an international service that processes both Bitcoin and credit card transactions.

Understand the Bitcoin rate and accommodate for it:

Lots of Bitcoin providers will automatically translate Bitcoin into your local currency for you, though for others this will be a necessary step, extending the length of some transactions. You need to be able to translate the price into the sliding scale of the Bitcoin quickly and effectively at your place of business. Given the unpredictable fluctuations of the value of the Bitcoin, and the length of time (sometimes up to 10 minutes) for a single payment to be confirmed, transactions in person can be a dodgy proposition at times.

Advertise your business as a Bitcoin merchant:

Given that people all over have the same interest in participating in Bitcoin exchanges, it's a great idea to advertise your business as being Bitcoin friendly. Work it into any advertising materials and register with Bitcoin databases online to attract customers.

Exercise caution:

Bitcoin is innovative, exciting, and full of possibilities. It's also experimental and volatile. It's important to know that Bitcoin payments are irreversible. So, if you get scammed by someone trying to exploit Double Payment loopholes, it'll be impossible to get your money back. Try to work a series of safeguard protocols into every Bitcoin transaction. Keep in mind the following concerns if you're going to start accepting Bitcoin at your place of business, especially in terms of what client to use for transactions:

- How are the funds converted? How are they received?
- How is the exchange rate calculated?
- How fast are payments approved?
- What risk is associated with the exchange?
- Are there any fees involved?

Confirm all payments:

Bitcoin transactions--even "instant" ones--are delayed by a few seconds, and can take up to 10 minutes to process completely. During that transaction period, it would be easy for a merchant to give a customer the "ok" during a window in which the transaction could still be reversed. Bitcoin itself recommends that merchants complete up to 6 separate confirmations or more on larger transactions to reduce the possibility of taking a hit.

Chapter 4

ADVANTAGES OF BITCOIN

- **Payment freedom -** It is possible to send and receive any amount of money instantly anywhere in the world at any time. No bank holidays. No borders. No imposed limits. Bitcoin allows its users to be in full control of their money.

- **Very low fees** - Bitcoin payments are currently processed with either no fees or extremely small fees. Users may include fees with transactions to receive priority processing, which results in faster confirmation of transactions by the network. Additionally, merchant processors exist to assist merchants in processing transactions, converting bitcoins to fiat currency and depositing funds directly into merchants' bank accounts daily. As these services are based on Bitcoin, they can be offered for much lower fees than with PayPal or credit card networks.

- **Fewer risks for merchants** - Bitcoin transactions are secure, irreversible, and do not contain customers' sensitive or personal information. This protects merchants from losses caused by fraud or fraudulent chargebacks, and there is no need for PCI compliance. Merchants can easily expand to new markets where either credit cards are not available or fraud rates are unacceptably high. The net results are lower fees, larger markets, and fewer administrative costs.

- **Security and control -** Bitcoin users are in full control of their transactions; it is impossible for merchants to force unwanted or unnoticed charges as can happen with other payment methods. Bitcoin payments can be made without personal information tied to the transaction. This offers strong protection against identity theft. Bitcoin users can also protect their money with backup and encryption.

- **Transparent and neutral** - All information concerning the Bitcoin money supply itself is readily available on the block chain for anybody to verify and use in real-time. No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent and predictable.

Chapter 5

DISADVANTES OF BITCOIN

- **Degree of acceptance** - Many people are still unaware of Bitcoin. Every day, more businesses accept bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects.

- **Volatility** - The total value of bitcoins in circulation and the number of businesses using Bitcoin are still very small compared to what they could be. Therefore, relatively small events, trades, or business activities can significantly affect the price. In theory, this volatility will decrease as Bitcoin markets and the technology matures. Never before has the world seen a start-up currency, so it is truly difficult (and exciting) to imagine how it will play out.

- **Ongoing development** - Bitcoin software is still in beta with many incomplete features in active development. New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. Some of these are still not ready for everyone. Most Bitcoin businesses are new and still offer no insurance. In general, Bitcoin is still in the process of maturing.

Chapter 6

ECONOMY OF BITCOIN

6.1 Classification as Money

Bitcoin is often referred to as a currency, but it does not conform to the definition of money. Economists agree that to qualify as money, something must be a store of value, amedium of exchange, and a unit of account. Bitcoin conforms to only one of these three criteria. It is used as a medium of exchange. (About 1,000 brick and mortarbusinesses were willing to accept payment in bitcoins as of November 2013 in addition to more than 35,000 online merchants.) The bitcoin market currently suffers fromvolatility, limiting the ability of bitcoins to act as a stable store of value, and it is not commonly used as a unit of account. Where people are allowed to buy with bitcoins, prices are not denominated in bitcoins. The People's Bank of China has stated that bitcoin "is fundamentally not a currency".

6.2 Price Volatility

Bitcoin has an extremely volatile exchange rate. According to Mark T. Williams of Boston University, its volatility is over seven times that of gold and over eight times that of theS&P 500. The Bitcoin Foundation contends that high volatility is due to insufficient liquidity while a Forbes journalist claims that it is related to the uncertainty of its long-termvalue. Volatility has little effect on the utility of bitcoin as a payment processing system.

6.3 Alternative to National Currencies

Some in countries with problem plagued national currencies may use bitcoins to protect their savings against inflation or the possibility that governments could confiscate savings accounts. Bitcoins are used by some Argentinians as an alternative to the official currency, which is stymied by inflation and strict capital controls. It's been suggested that during the 2012–2013 Cypriot financial crisis bitcoin purchases rose due to fears that savings accounts would be confiscated or taxed.

6.4 Speculative Bubble

Bitcoin has been labelled a speculative bubble by many including Former Federal Reserve Chairman Alan Greenspan and economist John Quiggin. Two lead software developers of bitcoin, Gavin Andresen and Mike Hearn, have warned that bubbles may occur. Nobel Laureate Robert Shiller said that bitcoin "exhibited many of the characteristics of a speculative bubble." Others reject the label and see bitcoin's quick rise in price as nothing more than normal economic forces at work.

6.5 As Investment

One way of investing in bitcoins is to buy and hold them as a long-term, high-risk investment. FINRA, a United States self-regulatory organization, warns that investing in bitcoins carries significant risks. The European Banking Authority warns that the risks of investment go beyond a potential fall in the value of bitcoins. Bitcoins may be of limited value to unsophisticated investors. Risk hasn't deterred some such as the Winklevoss twins, who made a US$1.5 million personal investment and attempted to launch a bitcoin ETF. Other investors, like Peter Thiel's Founders Fund, which invested US$3 million, don't purchase bitcoins themselves instead funding bitcoin infrastructure like companies that provide payment systems to merchants, exchanges, and wallet services, etc. Investors also invest in bitcoin mining.

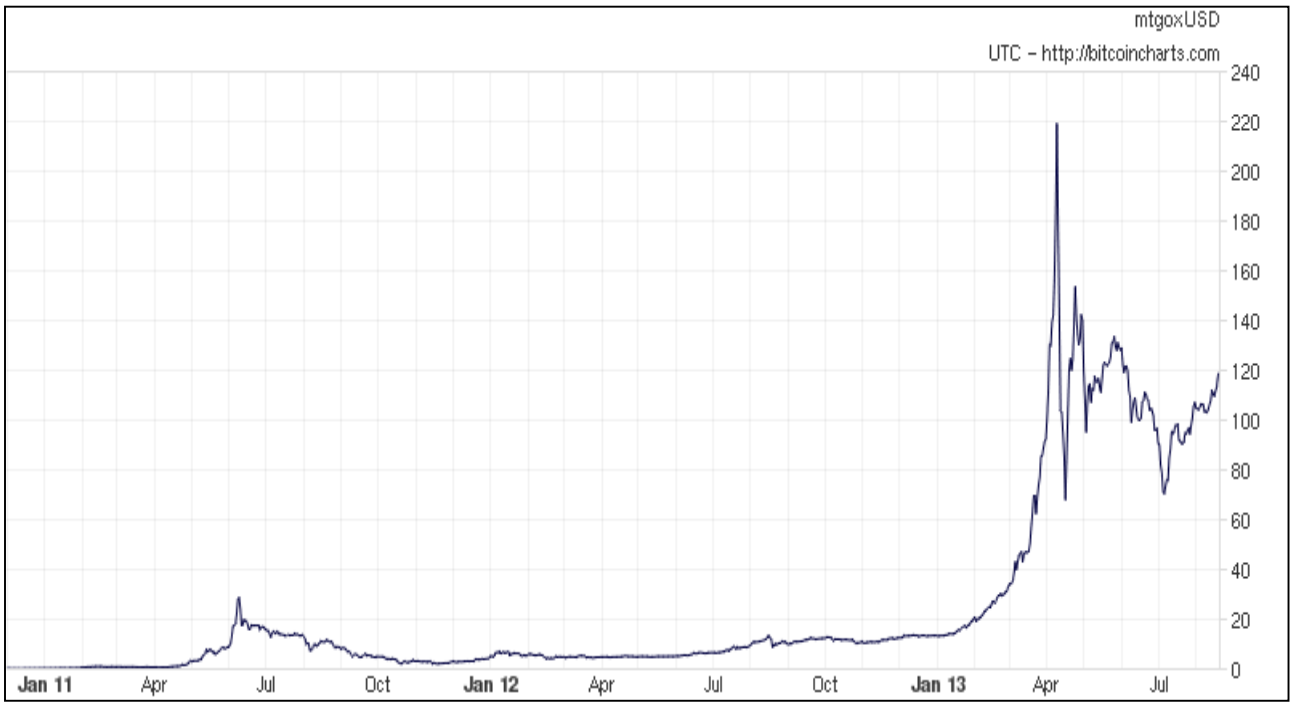
6.6 Money Supply

Growth of the bitcoin money supply is predefined by the bitcoin protocol, and in this way inflation is kept in check. Currently there are over twelve million bitcoins in circulation with an approximate creation rate of 25 every ten minutes. The total supply is capped at an arbitrary limit of 21 million, and every four years the creation rate is halved. This means new bitcoins will continue to be released for more than a hundred years.

6.7 Value Forecasts

Financial journalists and analysts, economists, and investors have attempted to predict the possible future value of bitcoin. Economist John Quiggin stated, "bitcoins will attain their true value of zero sooner or later, but it is impossible to say when." In 2013, Bank of America FX and Rate Strategist David Woo forecast a maximum fair value per bitcoin of $1,300. Bitcoin investor Cameron Winklevoss stated in 2013 that the "[s]mall bull case scenario for bitcoin is... 40,000 USD a coin". In late 2013, finance professor Mark Williams forecast a bitcoin would be worth less than ten US dollars by July 2014.

Bitcoin Price, 2011 to 2013:



Chapter 7

SECURITY

There are two main ways the blockchain ledger can be corrupted to steal bitcoins: by fraudulently adding to or modifying it. The bitcoin system protects the blockchain against both using a combination of digital signatures and cryptographic hashes.

7.1 The Addition Attack and Digital Signatures

Payers and payees are identified in the blockchain by their public cryptographic keys: most bitcoin transfers are from one public key to a different public key. (Actually, hashes of these keys are used in the blockchain, and are called "bitcoin addresses".) In principle, an attacker Eve could steal money from Alice and Bob by simply adding transactions to the blockchain ledger like *Alice pays Eve 100 bitcoins*, *Bob pays Eve 100 bitcoins*, and so on, using of course these people's bitcoin addresses instead of their names. The bitcoin protocol prevents this kind of theft by requiring every transfer to be digitally signed with the payer's private key; only signed transfers can be added to the blockchain ledger. Since Eve cannot forge Alice's signature, Eve cannot defraud Alice by adding an entry to the blockchain equivalent to *Alice pays Eve 100 bitcoins*. At the same time, anyone can verify Alice's signature using her public key, and therefore that she has authorized any transaction in the blockchain where she is the payer.

7.2 The Modification Attack and Mining

The other principal way to steal bitcoins would be to modify blockchain ledger entries. Eve could buy something from Alice, like a sofa, by adding a signed entry to the blockchain ledger equivalent to *Eve pays Alice 100 bitcoins*. Later, after receiving the sofa, Eve could modify that blockchain ledger entry to read instead: *Eve pays Alice 1 bitcoin*, or even delete the entry. Digital signatures cannot prevent against this attack: Eve can simply sign her entry again after modifying it.

To prevent against modification attacks, the bitcoin system first requires entries be added to the blockchain not one at a time, but in groups or *blocks*. More importantly, each block must be accompanied by a cryptographic hash of three things: the hash of the previous block, the block itself, and a number called a *nonce*. A hash of only the first two items will, like any cryptographic hash, always have a fixed number of bits (e.g. 256 for SHA-256). The nonce is a number which, when included, yields a hash with a specified number of leading zero bits.

Because cryptographic hashes are essentially random, in the sense that their output cannot be predicted from their inputs, there is only one known way to find the nonce: to try out integers one after the other, e.g. 1, then 2, then 3, and so on. This process is called mining. The larger the number of leading zeros, the longer on average it will take to find a requisite nonce. The bitcoin system constantly adjusts the number of leading zeros so that the average time to find a nonce is about ten minutes. That way, as computer hardware gets faster over the years, the bitcoin protocol will simply require more leading zero bits to make mining always last about ten minutes.

This system prevents modification attacks in part because an attacker has to recalculate all the hashes of the blocks after the modified one. In the example above, if Eve wants to change *100 bitcoins* to *1 bitcon*, she will not only have to recompute the hash of the block that transaction is in, but of all the blocks that come after it; she will have to recreate the chain of blocks. She can do this, but it will take her time, about ten minutes on average per block. However, during that time the network will continue to add blocks, and it will do so much faster than Eve alone can mine. Eve would have to recalculate all the blocks before the network could add a new one, or at least catch up with or overtake the network's miners. To do this, she would have to have roughly as much computing power as much of the existing bitcoin miners combined. This would be very expensive and, if the bitcoin network is large enough, likely infeasible. Furthermore, because of financial incentives to mine described below, it will make more financial sense for Eve to devote her resources to normal bitcoin mining instead. Thus the system protects against fraudulent blockchain modifications by making them expensive and, if the attacker is rational, unappealing because they make less financial sense than becoming a miner. The more miners there are, the more expensive and less feasible such attacks become, making the whole system even more secure.

7.3 Double-Spending

Bitcoin system is based on an innovative solution of a problem common to all digital currency and payment schemes: that of so-called double-spending. With paper money or physical coins, when the payer transfers money to the payee, the payer cannot keep a copy of that dollar bill or coin. With digital money, which is just a computer file, this is not the case, and the payer could in principle spend the same money again and again, copying the file over and over. With bitcoin, when Eve offers to pay Alice some bitcoins, Alice can always first check the blockchain ledger to verify that Eve actually owns that many bitcoins. Of course, Eve could try to pay many people simultaneously; but bitcoin can defend against that. If Eve offers to pay Alice some bitcoins in exchange for goods, Alice can stipulate that she will not deliver the goods until Eve's payment to Alice appears in the blockchain, which typically involves waiting about ten minutes.

7.4 Type of Attacks:

- **Race attack**

If the transaction has no confirmations, shops and services which accept payment can be exposed to a so-called *race attack*. For example, two transactions are created for the same funds to be sent to different shops/services. System rules ensure that only one of those transactions can be added to the block chain.

Shops can take numerous precautions to reduce this type of attack. It is always good to consider whether you should accept transactions without any confirmation.

- **Finney attack**

Another type of attack. Shops or services which accept transactions without any confirmation are affected. A *Finney attack* is an attack which requires the participation of a minerto premine a block sending the money to be defrauded back to the fraudster. The risk of such an attack cannot be reduced to nothing regardless of the preventative measures taken by shops or services, but it does require the participation of a miner and an ideal combination of contributing factors. It is no mean feat, the miner risks a potential loss of the block reward. Just as with the other type of attack, the shop or service must seriously consider its politics concerning transactions without any confirmation.

- **Vector76 attack**

Also called an *attack with confirmation*, this is a combination of the 2 aforementioned attacks which gives the perpetrator the ability to spend funds twice simply with a confirmation.

- **Brute force attack**

This attack is possible even if the shop or service is expecting several transaction confirmations. It requires the attacker to be in possession of relatively high-performance hardware (hash frequency).

The perpetrator sends a transaction to the shop paying for a product/service and at the same time continues looking for a connection in the block chain (block chain fork) which recognizes this transaction. After a certain number of confirmations, the shop sends the product. If the perpetrator has found more than n blocks at this point, he breaks his block chain fork and regains his money, but if the perpetrator has not succeeded in doing this, the attack can be deemed a failure and the funds are sent to the shop, as should be the case.

The success of this attack depends on the speed (hash frequency) of the attacker and the number of confirmations for the shop/service. For example, if the attacker possesses 10% of the calculation power of the bitcoin network and the shop expects 6 confirmations for a successful transaction, the probability of success of such an attack will be 0.1%.

- **> 50% attack**

If the perpetrator controls more than 50% of the bitcoin network power, the probability of success of the aforementioned attack will be 100%. By virtue of the fact that the perpetrator can generate blocks more often than the other part of the network, he can create his own block chain until it becomes longer than the “integral” part of the network.

Chapter 8

CONCLUSION

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending.

To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power.

The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

REFERENCES

- https://bitcoin.org/en/
- http://en.wikipedia.org/wiki/Bitcoin#History
- http://whatis.techtarget.com/definition/Bitcoin-mining
- https://products.butterflylabs.com/
- https://bitcoin.org/en/faq#what-are-the-advantages-of-bitcoin
- https://bitcoin.org/en/faq#what-are-the-disadvantages-of-bitcoin
- http://en.wikipedia.org/wiki/Bitcoin#Economics
- http://en.wikipedia.org/wiki/Bitcoin#Security


ACCEPTED HERE