BITCOIN : AN OVERVIEW

by

Mangala Gowri

School of Computer Science
McGill University, Montréal

Monday, December 17th 2014

TOPICS IN COMPUTER SCIENCE : PROJECT

Abstract

This report explores the world of Bitcoin - a virtual currency that is very popular right now in the digital world. First, we take a look at its history and underlying philosophy. Next, we discuss the workings of Bitcoin along with its strength and weaknesses. We also look into Bitcoin's use in the Deep Web and attempt to shed light on the debate common in the digital community about how anonymous Bitcoin really is. Finally, we discuss some practical considerations that need to be taken into account if Bitcoin is to become the money of the future.

Table of Contents

Appendices

Chapter 1
Introduction

There are a number of sentiments among the public regarding Bitcoin and other crypto currencies. It is not uncommon to hear "Bitcoin is a big snub to financially inept governments and corrupt banks. Bitcoin is a scam, a ponzi scheme, a bubble. Bitcoin is the future of money. Bitcoin has no future." All these statements reflect the confusion that is prevalent about the public about Bitcoin. To truly understand which of these statements is truly correct, we must look deeper into the fundamentals of Bitcoin and understand how it works, its inherent weakness and strengths.

1.1 History of Bitcoin

In November 2008, a paper was published by Satoshi Nakamoto titled "Bitcoin: A Peer-to-Peer Electronic Cash System" [Nak08]. This paper proposes the formation of a peer-to-peer network for a new cryptocurrency. The bitcoin network came into existence in November 2009 when the first bitcoins were mined by Satoshi Nakamoto. Since then, the bitcoin network has grown and spread all over the world making it one of the most famous online currencies. It recently reached a market cap of $1 billion.

1.2 Digital Currencies

Bitcoin is a form of digital currency that has no physical existence but can be used to interact with the real world and buy physical goods. Transactions with these types of currencies is instantaneous and borderless. For any digital currency to be widely adopted, it must satisfy at least two basic properties:

1.2.1 Central authority to keep track of transactions

If multiple people are to use digital currencies, a central managing authority is needed to keep track of the transactions. Consider Paypal which is a popular digital currency. In order for Paypal payments to be processes, a central Paypal exchange exists which acts as a middleman between the buyer and the seller. It verifies the identities of both the parties, checks if the amount of money involved is correct or not ie. if the buyer actually has the requires money or not, and then validates the transaction. Credit cards also work in the same way. In this case, the central authority is a bank. Without this kind of an authority, a currency would fall into chaos and cheating would become common. Bitcoin does not have a central authority to validate its transactions but instead uses a peer-to-peer network to achieve the same purpose. We shall explain the details in the next section.

1.2.2 Provide safeguards against double spending

A digital currency is in the end, a string of zeros and ones. What is to prevent one user to copy the currency and use it over and over again? This problem is called "double spending". This once again points back to the need for a central authority to prevent this kind of incident. We shall see in the next section how bitcoin solves this problem.

Chapter 2
Structure of Bitcoin

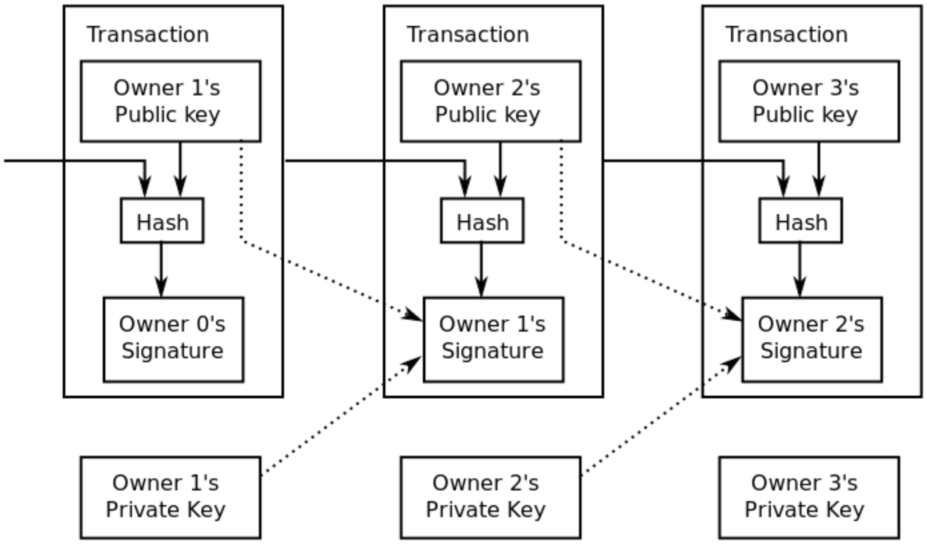
Among digital currencies, bitcoin falls into the category of cryptocurrency. A key feature of cryptocurrencies is a decentralized network to approve transactions which makes them different from other currencies that require a central authority. Cryptocurrencies make use of peer-to-peer networking and cryptography to achieve this purpose.

2.1 Making everyone the bank

To solve the first problem of not having a central bank, bitcoin makes all the peers that are in its network the bank. All the peers verify and validate each other's transactions. The central concept of bitcoin is the publicly available ledger also called a "block chain" that keeps track of all the bitcoin transactions and helps to validate them. The block chain contains all the details of transfership of the money from the day it was created (called the genesis block) to the most recent transaction. The block chain itself is distributed. Multiple copies exist of the block chain which are then synchronized thus making it possible for the peers to verify them independently.

2.2 A Bitcoin Transaction

A bitcoin transaction is of the form "I, Alice want to send Y bitcoins to Bob". This message is published onto the block chain. Multiple peers now verify the validity of the transaction and if it is valid, validate it and add it to a block of accepted transactions. Every hour, around six blocks of accepted transactions are added to the block chain. Once a block is published, everyone in the network now knows that the transaction has taken place. The transaction once published cannot be reversed ie., once Alice sends money to Bob, the money cannot be claimed back. A typical transaction in bitcoin looks like this:



Looking at the transaction message more carefully, we see that Owner1 uses his private key to sign the transaction and generate a hash which he then passes on to Owner2. Owner2 then uses his public key to verify the ownership of the transaction. Thus, a chain of ownership for each bitcoin is maintained. By this process, we have ensured that transactions can be verified and validated without the need for a central authority. If a private key is lost, all the bitcoins associated with that key is also lost and cannot be recovered. There is a case of a man of a man losing his harddrive contataining his private key and thereby losing $7.5 Million worth of bitcoins [Her13].

2.3 Bitcoin Mining

A bitcoin transaction on the network does not get added to the block chain (which contains accepted transactions) until it is verified and included in a block by a process called "mining". In order to motivate peers to validate transactions, new bitcoins are issued to them as a reward. Mining serves two main purposes:

1. Mining creates new bitcoins. This is similar to minting money in the real world.

2. It helps to verify the transactions involving bitcoins

2.4 Problem of Double Spending

What happens if Alice has a bitcoin and tries to double spend with it with two people at the same time? Lets say Alice controls two machines that immediately verify and publish her two transactions to the block chain. Once published, they cannot be reversed. So how do we solve this problem?

This problem can be solved by using a concept known as proof of work. This concept relies on two main ideas:

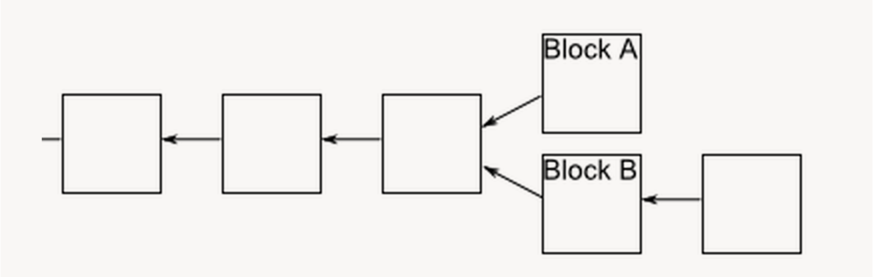
1. Make it computationally costly to verify transactions in a block.

2. Reward people for validating the transactions.

The benefit of making it costly to validate transactions now means that validation does not depend on the amount of network identities that a person has but depends on the amount of computational power that he has. With a small modification, we can make it such that a cheater would need enormous computing power to validate her transactions thus making it impractical.

Suppose a miner has to validate Block B that contains a list of transactions t. He has to find a nonce (a number) and append it to the list of transactions t. When this is passed to the SHA-256 hash function and hashed, the output should begin with a large number of zeroes. The difficulty of the puzzle can be altered by requiring a larger number of trailing zeros. What makes this so difficult is that if the input changes even a little, the output from the hash function changes completely. So, if we want 10 trailing zeroes before our hash, we will have to try $16^{10} \approx 10^{12}$ different combinations before producing the correct nonce.

Under this scenario, let us look at the issue of double spending again where Alice is trying to double spend her bitcoin. She sends one of her transactions to one set of miners and the other to another set of miners hoping to get both of them validated simultaneously. Lets call it Block A and Block B (containing Alice's transactions). The miners who received Block A first will continue working on it while miners who received Block B will work on validating it. This creates a fork in the block chain.



Now, suppose miners working on fork B mine a block first. As soon as miners working on fork A hear this news, they will immediately abandon work on fork A and switch to fork B. So, the fork A will be abandoned at it can be ignored. In this way, only one of Alice's transactions will be accepted. In real life, a transaction in Bitcoin is not considered accepted until:

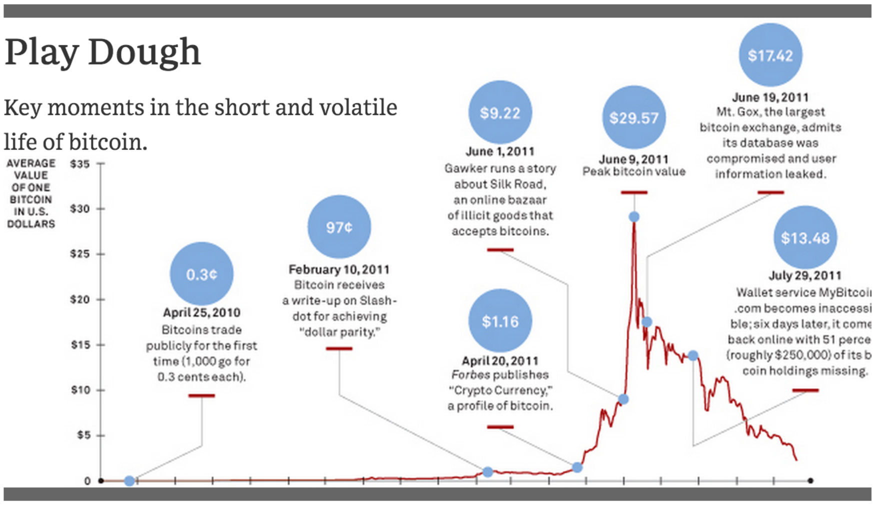
1. It is part of the longest fork.

2. At Least 5 blocks follow it in the longest fork.

Under these conditions, unless Alice is able to solve the proof-of-work as fast as everyone else (controlling fifty percent of the network's computing power), one of the fork will become shorter and get abandoned. Thus double spending is avoided in the Bitcoin protocol.

Chapter 3
Bitcoin's Use in the Deep Web

Bitcoin has been largely unregulated till now. This has given free reign to the black market community and the underground network to use bitcoins for their shady deals. Unlike cash, bitcoin gives them the comfort of doing illegal activities without moving from their home. And unlike other methods of payment like banks and credit cards, bitcoin is anonymous in that the ownership of bitcoin cannot be directly traced back to a real person. This led to bitcoin being very appealing to criminals. Bitcoins have been used in drug deals, money laundering schemes and gambling. Bitcoin is also used for legitimate purposes with many merchants and online stores accepting the currency as payment. The diagram below shows briefly the events in the bitcoin world up to now.



3.1 Is Bitcoin really anonymous?

The protocol behind bitcoin is designed to be a transparent system with the blockchain recording every transaction. Even though the transactions are known and the chain of ownership is known, the identity of the person possessing the bitcoin is not obvious. This has led people to argue that bitcoin is in fact "pseudonymous" - meaning "false name", which allows people to use a disguised identity. Though there are various steps that a user can take to be careful, using bitcoin for illicit purchases is a bad idea even if the chain is anonymous. Jeff Garzik, a bitcoin core developer said, "Attempting major illicit transactions with bitcoin, given existing statistical analysis techniques deployed in the field by law enforcement, is pretty damned dumb." What are these statistical analysis techniques that are being used to trace bitcoin transactions?

3.2 How to get started with bitcoins?

Users can get new bitcoins by mining (validating transactions on the block chain). But this activity requires a lot of computing power. So users usually join a mining pool like "Deep-bit" where they are paid proportionately according to the computing power they contribute [dee14]. The other option is to buy bitcoins by exchanging bitcoins for real money. There are bitcoin exchanges where one can perform these transactions. Some popular bitcoin exchanges are Mtgox [mtg14]. Currently, one bitcoin costs about $357.95. Once a user has the bitcoins, he stores them in a "wallet". A wallet is a software that stores the digital credentials for your bitcoin holdings and allows you to spend them. Bitcoin-Qt [qt14] also called Satoshi Client was the first bitcoin wallet to be developed. One the user has the bitcoins in his wallet he can start spending them on goods and services.

Chapter 4
De-anonymizing Bitcoin

Due to bitcoin's use in the black market for illicit activities, several attempts have have been undertaken both by law enforcement agencies and computer science researchers to de-anonymize the network. In this context, the aim is not to de-anonymize all Bitcoin users, but rather to identify common patterns of use. By using a passive analysis of a publicly available dataset, the limits of anonymity when using Bitcoin are demonstrated. Let's look at the latest developments towards this end.

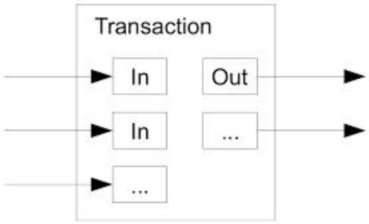
4.1 By Law Enforcement Agencies

The first legal issue occurred in May 2013 when bitcoins belonging to Mt.Gox were seized by the federal authorities in the US for violating money transfer regulations [Dil13]. Then in October 2013, Silk Road a drug market website was taken down by the FBI [Far13]. Silk Road was a notorious website that dealt in drugs, fake IDs, ordered hits etc. Soon after this incident, Silk Road 2.0 became available backed by the former administrators of Silk Road. It too was shut down by the authorities. In February 2014, 744,000 bitcoins were stolen from Mt.Gox one of the largest bitcoin exchanges. The thief's identity still remains unknown.

4.2 Research on the Bitcoin Network

4.2.1 Using Multi-input transactions

Multi-input transactions can be used to trace bitcoin activity back to a user. This approach was adopted by Androulaki, Elli, et al. Multi [AKR+13]. A Multi-Input transaction is one where multiple bitcoins have to be spent in order to procure a product.



1. User u has 2 BTC that have value 10B(BTC1) and 20B(BTC2)

2. He wants to buy something for 25B from BTC(Dest)

3. Bitcoin clients choose a set of BTCs from u’s wallet and perform a multi-input transaction. ie. transaction from multiple BTCs.

4. So, if we look at the block chain and observe a multi input transaction from multiple BTCs, they are from same user. (Different users cannot participate in a single transaction). So now we know that BTC1 and BTC2 are the same user.

Using this approach, they were able to cluster 1,632,648 unique addresses into 1,069,699 addresses. To obtain further refinement, the researchers used the concept of “change” from bitcoin transactions which is as follows:

1. To collect the change 5B, a "shadow" address is created for u. This BTC(Shadow) is created internally by bitcoin and is never reused.

2. So, we examine the output to a transaction. If one of the address is something that has never occurred in the chain before, we know it is a shadow address.

3. Therefore the transaction will be form BTC1+BTC2 -> BTC(Shadow) ,BTC(Dest)

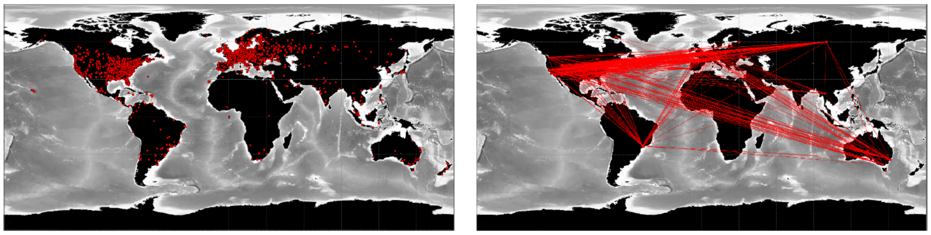
So, now we know that BTC1, BTC2 and BTC(Shadow) are the same user. Using this second heuristic, they were able to further cluster the 1,069,699 address into 693,051 addresses. This represents grouping approximately 58% of bitcoin addresses with an average of 11.5 address per user.

4.2.2 Using voluntarily disclosed information

In another paper, researches made use of voluntarily disclosed information to track down users [RH13].

Bitcoin Faucet

Bitcoin Faucet is a website where users can donate Bitcoins that will be redistributed to other users after breaking them into smaller pieces. To prevent fraud, Bitcoin Faucet publishes a list of recent donations along with the IP addresses of the donors. Researchers mined this list and used it in their network analysis. The public keys that were generated from here were searched in the block chain. From there, the researchers were able to put together a map of geolocated IP addresses belonging to users who receive bitcoins over a period of one week. They also put together a map of users who are linked by a path (a path between two nodes exists if a transaction has occurred between the two nodes). The path does not include the transaction to the Bitcoin Faucet.



(a)

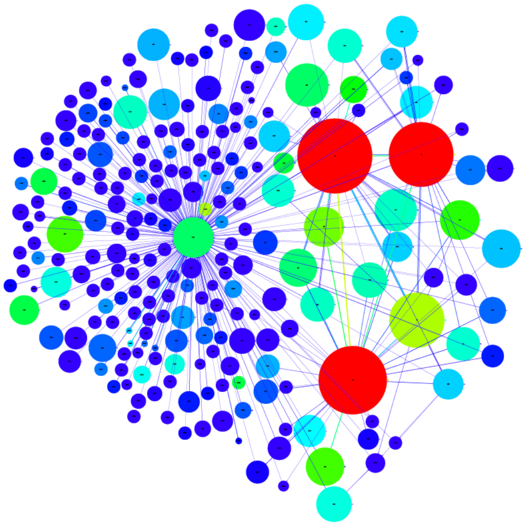
(b)

Bitcoin Forums

Many users post their experiences on numerous bitcoin forums. Sometimes, they also reveal their public key along with their comments. Public keys in Bitcoin start with the digit one and are thirty three characters in length. These can be indexed by a search engine. The researchers collected all such publicly listed public keys. They were also able to scrape public keys of users from twitter. By observing the usage of these public keys in the block chain and then obtaining the user details from the public forums, de-anonymization of users is possible.

Egocentric Analysis and Visualization

WikiLeaks publicly announced that they were accepting anonymous donations via bitcoins. They also published their public key for the users to be able to send donations. The researchers used network visualization and analysis tools to investigate the flow of bitcoins to and from WikiLeaks's public key. They were able to put together this graph representing a sub-network of all users who had contributed to WikiLeaks:



Determining Users using addresses of Bitcoin Exchanges

If we have identified a Bitcoin Exchange by obtaining their private keys, we can obtain a list of almost all users who have exchanged money and bought bitcoins through that exchange. The exchange is the point of origin of the bitcoin. A new public key never seen before in the block chain originates at this point. Starting from the exchange, the users found the shortest path to a user where the bitcoin went. By combining other publicly disclosed information, they were able to trace the flow of the bitcoin and pinpoint it to a user. Bitcoin exchanges collect a user's real name and email address before exchanging real money for bitcoins. So,if a law enforcement agency subpoenas the exchange, the user's identity along with his complete transaction history will be available to the authorities.

Chapter 5
How to be anonymous while using Bitcoin?

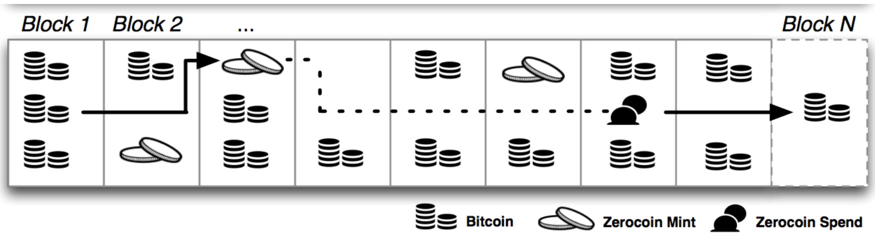
Although Bitcoin stores all the transactions in a public ledger accessible to everyone, it is not always easy to trace the ownership back to a real person. Also, there are steps one can take to prevent being detected by the network analysis techniques. As long as protocol level anonymity is built around Bitcoin, there are several workarounds that one can follow to hide one's true identity. Any user not taking proactive steps to conceal himself is at a high risk of being found.

5.1 Be careful of Bitcoin Exchanges

While buying Bitcoins, do not buy them from MtGox, Coinbase or other exchanges that need your bank account and ask you for your name. Instead, one can mine them from a Bitcoin pool like Eligius (no accounts/email necessary, they only ask for a bitcoin address) [eli]. Doing so covers one weak point of Bitcoin in that the identity of the owner at the point of origin of the coin is protected.

5.2 Zerocoin

After getting the Bitcoins, before spending them, one can pass them through several intermediate services to mask their point of origin. One such service is Zerocoin [MGGR13]. Zerocoin is a distributed e-cash scheme that aims to keep Bitcoin anonymous by using cryptographic techniques. A user takes his Bitcoins and converts them into Zerocoins. This takes the Bitcoins out of the public ledger. Payments can now be made via Zerocoins to other users, and split and merge Zerocoins in any way that preserves its total value. By reconverting Zerocoins to Bitcoins, a new private-public key pair is generated thus breaking the link in the block chain.



5.3 For the Paranoid User

5.3.1 Anonymous Hardware and Software

For users who are serious about protecting their identity, it is necessary to use anonymous hardware. One can buy a cheap laptop and remove its hard drive. It is important that one does not connect it to the home wifi that can be traced back to him. For the next step, the user can download a Linux LiveCD to connect to the TOR network /citeparanoid.

5.3.2 Create an anonymous wallet

Do not use any eWallet to store your Bitcoins. Apart from being insecure, some of the wallets themselves are fraud or ponzi schemes to steal user's Bitcoins. Instead, use a service like BitAddress [bit] that can be used to generate Bitcoin addresses offline. Also, the addresses and private key pair generated allows one to spend and receive Bitcoins without running any other external software.

5.3.3 Funding the anonymous wallet

This step refers to filling one's wallet with Bitcoins and is arguably the most difficult step. One must take extra care not buy Bitcoins from banks or Bitcoin Exchanges as they are easy to trace. Instead, one can exchange cash for Bitcoins from cash transaction networks like ZipZap [zip] that do not verify the buyer's identity. One can provide a fake email address for the purchase.

5.3.4 Spending your Bitcoins

Before spending the Bitcoins you have, you should send the funds through a mixing service that mixes one's Bitcoins with others to confuse anyone following the trail [mix]. However, an important point to note here that the mixing services are not always trustworthy and may steal your money. Instead one can use services such as Zerocoin(as mentioned above) to do the mixing. Also, these mixing wallets should not be created using the TOR network as the TOR exit node may be monitored. In a yet to be published paper researchers from Cornell University argue that the TOR network is susceptible to man-in-the-middle attacks thus affecting Bitcoin's privacy as well [BP14].

Chapter 6
Practical Considerations of Using Bitcoin

Bitcoins are used widely in today's world. A lot of online e-commerce sites accept bitcoins. Bitcoins are also being increasingly accepted in bars and restaurants, hotels and other physical stores. Below are some of the current scenarios involving Bitcoin.

6.1 Facilitation of e-commerce

6.1.1 Traditional e-commerce

In a traditional environment, customers do not care about centralization and anonymity. In order for a currency to be widely used by all segments of the population, it has to be stable and reliable. Bitcoin has an ill reputation for being highly volatile with prices fluctuating from $100 to $1240 almost 10x changes in price versus the U.S dollar in a short period of time. Since there is no central institution handling the currency, it is highly susceptible to bad press and variance in perception of Bitcoin's value [Bar14]. More importantly, Bitcoin has no inbuilt anti-fraud capabilities. By making transfers irreversible, it offers almost no protection to legitimate buyers or sellers. Cases of fraud involving Bitcoins are not uncommon. Due to these reasons, it is unlikely that Bitcoin can become the de facto money of the internet and replace credit card companies and other payment gateways like Paypal.

6.1.2 Micropayments

Micropayments refer to very small payments for digital goods. The payments can be as small as 10 cents. Traditionally, there have been no efficient means to handle these kinds of payments as the transaction fees involved is too high. Bitcoin is a good competitor in this space due to its very low transaction fees. There exist services on the internet where you can tip very small amounts or "microdonate" to websites and businesses using Bitcoin [Bar14].

6.1.3 Virtual World and Game related Commerce

Individuals also use digital money to buy game related items such as digital clothing in Second Life or crops in Farmville [far]. At the end of 2010, around USD $30 million transacted in Second Life was in the form of Linden Dollars(another virtual currency) [Lin10]. As this indicates, virtual and game related markets are huge sources of revenue for vendors. Where digital currencies have not created a foothold in traditional e-commerce, they flourish in virtual e-commerce. Bitcoin has the potential to become the standard in this area. It increases trust as now the game company would not be issuing and inflating the currency as Bitcoin exists independently of any game.

6.2 Points of Failure of Bitcoin

6.2.1 External Threats

Improper Use of Discretionary Authority

As of now, Bitcoin is unregulated by any central authority leading to its wide price fluctuation. In the future if a consortium of developers or any external authority is established to control Bitcoin's problems, it may lead to erosion of confidence from Bitcoin even if the changes are performed with good intentions.

Competing Currency

As of now, many competitors to Bitcoins exist Namecoin, Litecoin, Zerocoin etc. They could lead to reduction of value of Bitcoin.

Government Crackdown

With Bitcoin generating a lot of bad press due its use in illicit activities, there is steady pressure from the government on it. This could lead to crisis in conficence towards the currency.

Legal Issues

One major factor impeding Bitcoin's use is that consumers and businesses are unsure of its exact legal standing. Traditionally, only the central government authority can issue and mint money. Existing online financial systems like credit cards and Paypal use this money. With the introduction of a new currency, it is unclear where it stands leading to Bitcoin being in the legal grey area. Unless this is resolved, a majority of businesses may be unwilling to adopt Bitcoin on a large scale.

6.2.2 Technology Failures

Anonymity Failure

Bitcoin is popular because it is considered to be anonymous by the general public. Increasingly, statistical techniques are being used to de anonymize the Bitcoin network and users. Such exposure could lead to the erosion of confidence in Bitcoin.

Theft

Bitcoins can be lost or stolen. Cases of huge thefts involving Bitcoins are common. 744,000 bitcoins were stolen from Mt.Gox in 2014. Such incidents are detrimental to the widespread adoption of Bitcoin.

Denial of Service

The Bitcoin network is susceptible to a denial of service attack. An attacker with significant computing power can flood the network and cause disruption of services. Obtaining the necessary computing power for this kind of attack is expensive but possible. It has been speculated that interested parties may include the government wishing to shut down Bitcoins or a huge group of hackers.

Bibliography

[AKR+13] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating user privacy in bitcoin. In *Financial Cryptography and Data Security*, pages 34–51. Springer, 2013.

[Bar14] Jonathan Todd Barker. Why is bitcoin's value so volatile? 2014.

[bit] Is bitaddress.org safe?

[BP14] Alex Biryukov and Ivan Pustogarov. Bitcoin over tor isn't a good idea. *arXiv preprint arXiv:1410.6079*, 2014.

[dee14] Deepbit:bitcoin mining pool. 2014.

[Dil13] Romain Dillet. Feds seize assets from mt. gox's dwolla account, accuse it of violating money transfer regulations. 2013.

[eli] Eligius.

[far] Farmville.

[Far13] Greg Farrell. Fbi snags silk road boss with own methods. 2013.

[Her13] Alex Hern. Missing: hard drive containing bitcoins worth £4m in newport landfill site. *Guardian*, 2013.

[Lin10] Nelson Linden. The second life economy in q4 2010. 2010.

[MGGR13] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013, pages 397–411. IEEE.

[mix] Mixing service.

[mtg14] Mt.gox. 2014.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1(2012):28, 2008.

[qt14] Bitcoin-qt. 2014.

[RH13] Fergal Reid and Martin Harrigan. *An analysis of anonymity in the bitcoin system*. Springer, 2013.

[zip] Zipzap.