Security Analysis of Bitcoin

Dibyojyoti Mukherjee, Jaswant Katragadda, Yashwanth Gazula

Department of Electronics and Computer Engineering, Volgenau School of Engineering
George Mason University
Fairfax, VA USA
dmukher2@.gmu.edu, jkatraga@gmu.edu, ygazula@gmu.edu

Abstract: **In recent years many cryptocurrencies have come into existence. The most prominent among them is Bitcoin. It has emerged as the first decentralized, peer-to-peer, digital currency. Bitcoin is the decentralized payment system that is based on proof-of-work. Potential security threat, and also the uniqueness, of Bitcoin over the internet lie within the peer-to-peer transactions over the Internet. This paper presents an exploratory security analysis of Bitcoin.**

I. INTRODUCTION

Bitcoin is an electronic currency, which was introduced in 2009 as open source software. The software uses its own units for payments, which coincidentally is also termed Bitcoin. Bitcoin is also a protocol which is why it provides very fast peer-to-peer transactions and with that payments which does not incur very high transaction fees. There is no central repository as the payments are made peer to peer and this is why Bitcoin has been termed as a decentralized virtual currency by the US Treasury.

The value of Bitcoin, as digital currency, comes from mathematical algorithm behind it and its limited supply. Security of Bitcoin is based on the strength of the cryptographic algorithm and not on the safe storage of data in databases.

The Bitcoin system uses a public record book, which keeps all the financial transactions. This is done without the help of several intermediate computer servers, which run the Bitcoin software. So truly this is a decentralized system. The record book, which keeps the information about the transactions, are known as the Block Chains. The maintaining of these block chains is called mining and the people in charge of the maintenance are awarded newly created Bitcoins and waivers of transaction fees. The security of this decentralized system is done through the use of a combination of digital signatures and cryptographic hashes.

Similar to any currency, a transaction involves moving some set of currency from a location to another location. Transaction of Bitcoins does not take place between the individuals, rather between the addresses on the network. All of these transactions happen in public; however, with the human identity they're difficult to link up [1]. Thus, maintaining pseudo-anonymity is accomplished by the various security measures involved in, storing of these Bitcoins in associated Bitcoin wallets apart from mining.

II. CRYPTOCURRENCY

Cryptocurrency is a special form of digital currency and essentially a digital medium of exchange. The most significant difference of cryptocurrency with traditional Dollars and Euros is that the acceleration of the production of money is not controlled by any entity; Rate of production is publicly known and defined.

An open source project named Bitcoin was conceived in January 2009 by a pseudonymous researcher going by the name Satoshi Nakamoto. This project was created based on the principle proof-of-work that there is a secured transaction being processed on a decentralized peer-to-peer network without the need for a central clearinghouse. Since then, several cryptocurrencies have attempted at such a decentralized digital currency ecosystem, like Namecoin, Litecoin, Peercoin, and Freicoin.

Cryptocurrencies have slowly received attention from media and public over the past couple of years, Due to rapid price rise of Bitcoin in April 2013, interest has rapidly increased. Figure A [2]

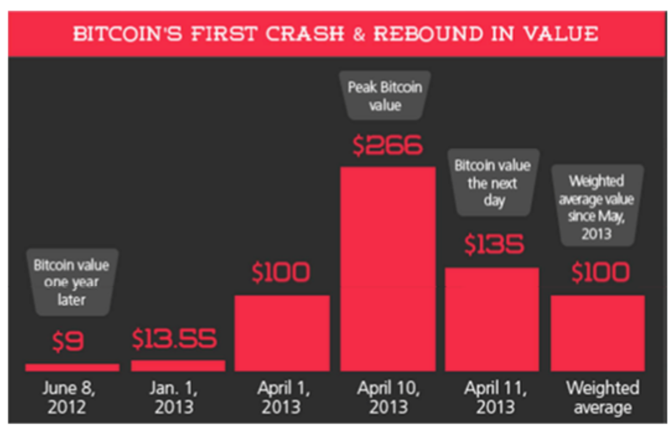

Figure A

III. BITCOIN

A. History

Before Bitcoin, there was no reliable way to transfer digital cash among people without any central mediator. Central mediator such as PayPal will be able to track transactions by maintaining account ledger, but it wasn't clear how group of strangers who do not trust each other could accomplish same transactions dependably. In 2008, Bitcoin's inventor, known pseudonymously as Satoshi Nakamoto, solved the problem. His breakthrough made it possible for digital currency to exist without relying on a central authority. He proposed concept in his paper "Bitcoin: A Peer-to-Peer Electronic Cash System."[4] Since it is an open-source project the software was improved and maintained by hundreds of volunteers till today. In January 2009, the first bitcoins were distributed using early Bitcoin software [3], and since then transactions have been running smoothly. Slowly but securely, an increasing number of people started using Bitcoin, and what began as an experiment is now a multi-billion dollar economy, which processes hundreds of thousands of transactions per day.

B. Cryptography behind Bitcoin

Bitcoin relies on cryptography for functioning; hence it is referred to as cryptocurrency. In Bitcoin, hash functions and digital signatures are used for authorizing transactions with digital signatures and verifying the validity of the transaction history. Figure B [4], below, shows how transaction protocol actually works.

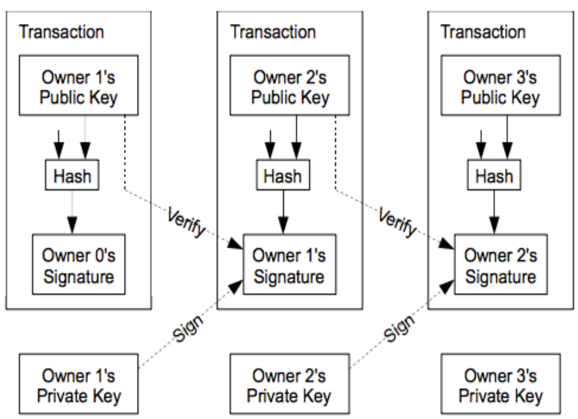

Figure B

Bitcoin transaction is a chain of digital signatures. Every owner signs the hash of previous transaction and public key of the person to whom he is sending, and attaches this signature to the coin. So every Bitcoin transactions contains information about number of bitcoins transferred, the address to which they are transferred, transaction fee and the digital signature. If the signature is missing or doesn't match the public key, nodes on the Bitcoin network will consider the transaction invalid and will not add it to the blockchain. Bitcoin depends on the blockchain being widely distributed among the nodes in the network. Each block in the blockchain contains a list of transactions and a hash of the transactions in the previous block in the chain. Hence, it's impossible to alter just one transaction in a block in the middle without causing a mismatch between the expected block hash and the hash recorded in the next block. This verification provides an efficient way for a single node to check whether transactions in its copy of the blockchain have been tampered with. Rather than checking every transaction in the entire transaction history, a node can simply check whether the hash of each block matches the recorded hash of subsequent blocks. Instead of sharing a public key, users share a Bitcoin address, which is a cryptographic hash of a public key. In fact, the public key is hashed twice using two different cryptographic hash functions to create a Bitcoin address. This extra protection ensures that no amount of analysis of a Bitcoin address can reveal the underlying private key. This process is explained in figure C [5] below.

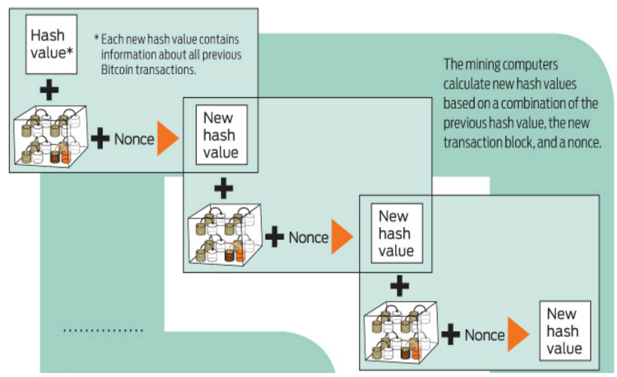

Figure C

C. Bitcoin Mining

Bitcoins are created through Bitcoin mining using miner's computational power. Mining is the process by which new Bitcoin transactions are added to the block-chain, or the public ledger. By adding a new block of transactions to the blockchain, the miner who added the block is rewarded with newly minted bitcoins (as well as old bitcoins in the form of transaction fees). The number of new bitcoins being mined from each block is diminishing slowly over time and will continue to do so until all 21 million bitcoins have been excavated.

By the year 2140, every Bitcoin will have been extracted and will be in circulation. Because protecting the Bitcoin network requires effort, time, and money, anyone willing to do this work would merit a monetary incentive. Therefore, Satoshi's strategy of using bitcoins as an incentive for miners acted as a decentralized mechanism for giving away new coins and created a community dedicated to protecting the network through the mining process. Because Bitcoin was intended to be a currency with a finite supply, miners can't generate new bitcoins forever. Satoshi chose a scheme in which bitcoins would be distributed over a century at a rate that is reduced by half approximately every four years until the total number eventually reaches 21 million.

The below figure D [6] shows the bitcoins those will be awarded to miners over time are reduced. A solved block (i.e., a block that will be accepted by others as part of the blockchain and the one the miner is paid for) occurs when the double SHA256 hash of the block header results in a number that is less than some predetermined threshold, known as the difficulty target. If the result is greater than the target, the block remains unsolved. When this happens, the miner must try a different nonce, which is contained in the header and hence affects the hash. Because cryptographic hash functions produce completely new outputs when the input is changed by even the tiniest amount, changing the nonce value results in a totally new hash for the entire block header. By repeatedly changing the nonce value, eventually a hash output will be found that is less than the target. Typically, a miner simply increments the nonce by 1 in this search until a successful nonce value is found. When a working nonce is found, the block is solved. The difficulty is adjusted every time the blockchain grows by 2,016 blocks, which happens approximately every two weeks (2,016 × 10 minutes = 14 days). If it takes less than two weeks to mine 2,016 blocks, the difficulty is increased, but if it takes longer than two weeks, the difficulty is decreased.

During the first five years, the mining difficulty in Bitcoin increased from 1 to over 50 billion. At this difficulty, an ordinary personal computer (tablet, laptop, etc.) would be lucky to solve one block every 3.5 million years! This difficulty corresponds to a network hash rate that is ~360,000,000,000 MH/s, or 360 petahash/s (PH/s). All of the world's conventional supercomputers combined would hash at a rate less than 1 PH/s.

D. Mining Pool

A mining pool is a collection of miners who combine computational resources and then split the block reward. From the network's perspective, a mining pool is a single mining node, but hundreds or perhaps thousands of individual miners are calculating hashes within that node. A mining pool solves blocks more often than an individual miner; therefore, the miners' income is more frequent. When the block reward is divided among the miners, it is usually allocated proportionally based on the number of hashes a miner contributed. Because it is difficult to know exactly how many hashes an individual contributed, the typical measurement of contribution is in the form of calculated shares.

Although the exact details vary between mining pools, a miner earns a share when she calculates a hash output that is less than a much easier-to-reach target than the real target. As a result, it might take individual miner years before he would find a hash less than the real target but only a few minutes to find a hash less than the pool's share target. The number of shares accumulated by a miner represents how much of the pool's hashing power that miner contributed.

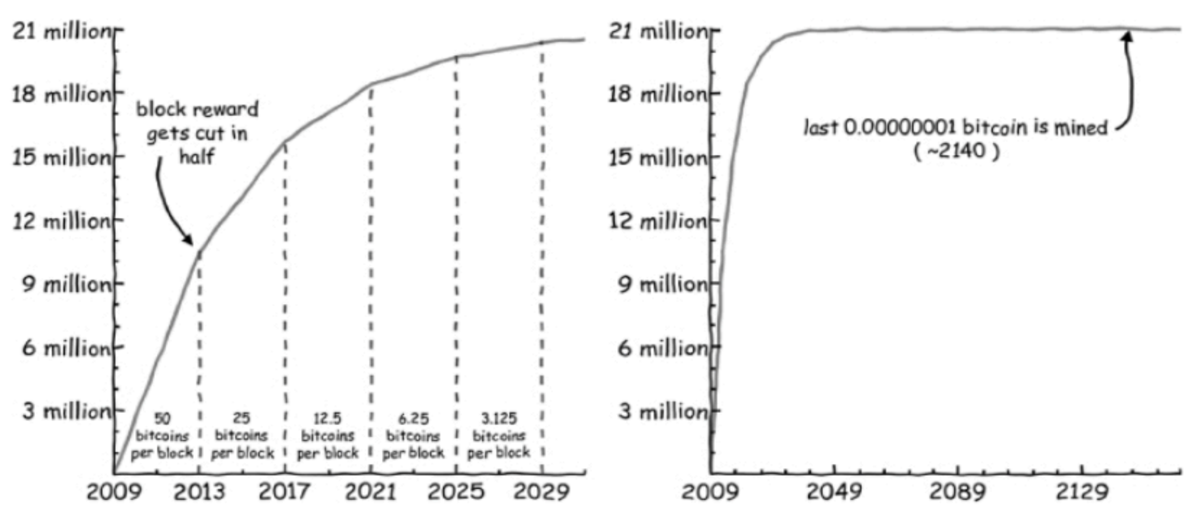

Figure D

IV. HARDWARE ACCELERATORS FOR MINING

In the beginning the only way to mine Bitcoins was mining with the CPU. This is how the Bitcoin network started by mining this way via the original Satoshi client. Since the network difficulty level is so high nowadays this method is no longer viable. By this method, without making a single coin it might take years together to mine.

Soon more efficient technique for mining Bitcoin was discovered i.e. by using high-end graphic cards. GPU (Graphical Processing Unit) mining was found from the developments done in CPU mining. Some of the GPU's parallel nature increased the power of Bitcoin mining by 50X to 100X [7] by using far less power per unit of work.

The Bitcoin mining world progressed up the technology food chain to field programmable array (FPGA) as with the CPU to GPU transition. By the launch of Butterfly Labs 'Single' landscape of Bitcoin mining hardware gave way to specially manufactured hardware dedicated to Bitcoin mining. Although FPGA did not see the increase in the mining speed of 50X to 100X as in the case of CPU to GPU transition but the benefit was found in the ease of use and the power efficiency. Power consumed by a 600MH/s graphic card was 400W4, whereas power consumed by FPGA mining device that provide hash rate of 826MH/s was found to be 80W. FPGA miners made concentrated mining farms possible for the first time.

Application Specific Integrated Circuits (ASIC) has taken over completely in the present era. Design of ASIC chip is done specifically to do one thing only. To do other tasks it cannot be repurposed unlike FPGA's. ASIC chip designed to mine coins is only used in mining Bitcoins. An offset of 100X [7] times increase is observed in hashing power due to inflexibility of ASIC, with reducing the power consumption when compared to previous technologies. When disruptive technology is concerned ASIC is the "end of the line". GPU's have replaced CPU's. FPGA's replaced GPU's. Finally ASIC in turn replaced all the previous technologies. Now or even in the immediate future no other technologies can replace ASIC's. These ASIC products can see stepwise refinement and hence increase in the efficiency.

Bitcoin ASICs are optimized to calculate SHA256 hashes. Today, practically all Bitcoin mining is done with ASIC-based hardware. Further increases in speed and efficiency are being achieved continually by designing the chips with smaller and smaller features (from 130 nm to 65 nm to 28 nm features, and so on). Consequently, more calculations can be made per unit of area.

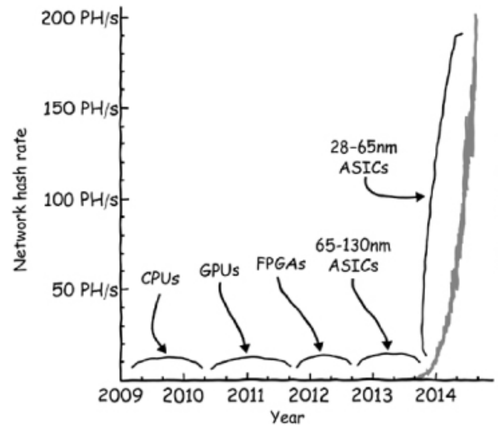

Figure E

The above figure E [6] uses a traditional linear scale for the y-axis, in which the enormous computing power of ASIC miners in 2013 dwarfs all previous methods of mining making it possible to see the progress in computing power on the network more clearly, progressing from CPU, to GPU, to FPGA, and finally ASIC mining.

V. COMPARISON OF BITCOIN WITH SIMILAR PEER-TO-PEER MODEL SYSTEMS

A. Litecoin

Litecoin is a crypto-currency which was created with the sole motivation of improving upon the existing gold standard of crypto-currency i.e. Bitcoin. Former Google employee Charles Lee invented Litecoin in October 2011. The motivation behind coming up with an all new mining system was to improve upon the existing structure of Bitcoin which has given rise to a hardware race for better and efficient mining.

Litecoin relies on an algorithm, which could repel the rapidly escalating hardware race. The key difference between Bitcoin and Litecoin is the algorithm, which they utilize to perform mining. Bitcoin employs SHA-256 algorithm which a power intensive algorithm where lots of hardware are needed for the calculations that are performed during mining. Litecoin uses the S-Crypt algorithm. The S-Crypt algorithm takes in the SHA-256 algorithm but the amount of calculations performed are much more serialized than those in Bitcoin. The S-Crypt algorithm employed in Litecoin favors the use of high speed RAM than processing power of the GPU's alone. Since Litecoin puts more reliance on RAM calculations and since RAM is the most expensive component the investors can use less resources and time for mining Litecoin. The total hashing rate of the Bitcoin network is over 20000 Terra Hashes per second whereas Litecoin is just 95462 Mega Hashes per second.
The time difference in generating a block is also massive. It takes 2.5 minutes to generate a Litecoin block whereas a bitcoin block takes 10 minutes. The transaction times in Litecoin are also four times faster than those of Bitcoin.

Bitcoin cannot match this right now because the code employed in the Bitcoin network where everybody is mining has to be significantly upgraded.

Litecoin is affordable to many people as an investment because each LTC is around 3.5$ whereas BTC is almost 377$. Also, since Litecoin mining is faster, there is the possibility of more rewards and hence increased earnings for the miners [8].

There are a few constraints to Litecoin, which is yet to be overcome. The price of a Litecoin is always tied to Bitcoins because it cannot be directly bought with US dollars or other currencies. So the fate of Litecoin is tied to Bitcoin partly. Also, the other disadvantage that Litecoin faces is that Bitcoin has more momentum and support from the mining community. Hence more resources are put into Bitcoin than Litecoin. There seems to be hope in the horizon for Litecoin since the coin limit of Litecoin is much higher than Bitcoin, which in theory should help future proof Litecoin [9][10].

B. Ripple

Ripple is a payment system which is built upon an open source Internet protocol, consensus ledger and native currency called ripples (XRP). It is the third largest crypto-currency based on market capitalization after Bitcoin and Lite-coin. Ripple employs the same algorithm that Bitcoin employs and it provides multi-signature support just like Bitcoin. Ripple transactions cannot be reversed after they have been processed and they have been made in such a manner by Ripple Labs that they are counterfeit proof. Ripple transactions occur by a transfer of debt (IOU). There is a huge advantage of Ripple over Bitcoin and i.e. they have developed a solution for the double spend problem that plagues Bitcoin. The term that ripple miners have coined for the solution is Consensus.

Consensus is explained below. There is the concept of an agreement room. If a person enters the room he/she has to agree with all the members of the room already present. The person can create their own room if he/she is not in agreement with all the preexisting members. People who are honest try to enter the biggest room with the maximum number of people in it. The members always agree on the present state of the system. This is implemented as a hash tree which is just one 256-bit number.

When a transaction is performed the miner enters the big room and displays the transaction. All the other members check the transaction against their ledger. If there presents no conflict in transactions and everybody is satisfied with the validity of the transaction, then it is included in the set of transactions. If there is a disagreement then an avalanche process is utilized where the majority of votes determine the validity of the transaction. Once the transaction terms are set upon, the transactions are applied and every member calculates the next ledger, which is under a set of rules. All the members sign it and after that they publish the signatures and then the whole world can see which transactions the process of consensus has accepted.

So to solve the double spend problem, the members of the room agree on an order for the two transactions. If all the members of the group agree which transaction should be performed first, then the problem is solved [10]. The reaction to ripple as a crypto-currency has been polarizing. Even though Ripple allows the use of any electronic value holder, many in the community harp on the fact that XRP (Ripple coins) are mined beforehand by Ripple Labs and the owners retained 45% of the coins. So this holdback by the owners is the reason many people from the crypto-currency community consider Ripple as a scam. But the supporters of Ripple are quick to point out that their strategy is the same as any company that has gone public while retaining most of the shares.

Ripple remains the third largest crypto-currency after Bitcoin and Litecoin. Even though Bitcoin as a currency took a huge hit in 2013 due to the scams, it remains a better choice among the coin mining community thus maintaining its comfortable lead over Ripple [11].

C. Mintchip

Mintchip is the brainchild of The Royal Canadian Mint, which decided to jump into the digital currency world after witnessing the success of Bitcoin. Mintchip is meant to offer the benefits of electronic currency, which has the support of the Canadian Dollar. As advertised by the Canadian Government, Mintchip offers secure transactions like Bitcoin and it also seemingly solves the double spending problem. Mintchip is very similar to Bitcoin because it shares the core algorithms, which run both of these peer-to-peer systems.

The security model employed by Mintchip is very similar to Bitcoin. Here the payment transaction is done by sending a message from the sender's Mintchip to the receiver. The message contains the receiver's unique ID and a digital signature generated from the sender's chip. The problem arises when questions are raised about how the system prevents double spending. The core of Mintchip is an IC, which stores the electronic value and helps with transferring the value from one chip to another. The chip uses tamper resistant trusted hardware. The Canadian government has refused to divulge more details about how double spending is avoided. So it has not been verified whether double spending is truly stopped by using Mintchip.

Another bone of contention between Bitcoin and Mintchip is that Bitcoin is a decentralized cryptocurrency whereas Mintchip is centralized and is controlled by the Royal Canadian Mint. The system does get many things right and the Canadian Government are certainly heading towards the right direction with Mintchip. Like Bitcoin, Mintchip makes do with no transaction fees, ease of use and also the digital signature model, which Bitcoin employs, for payment verification [12].

Two years after its inception in 2012, the Canadian Government pulled the plug on Mintchip in the early months of 2014 and the government is in the process of selling off its digital currency program. The government declined to give any reasons why they put an abrupt halt on the Mintchip program and they issued a statement in their 2014 budget that they have moved on with their plan to solidify the current payment system and put more emphasis on cracking down on digital currencies which are used in money laundering and criminal activities [13].

VI. VULNERABILITIES

A. Double Spending

Double Spending is a possible way to cheat in a transaction. A user attempts two transactions almost simultaneously by transferring a quantity of Bitcoins to one person and transferring the same exact Bitcoins to another. This splits the block chain. Transactions must be verified six times over and the correct block chain will win the split. The existing solution for double-spending attack is block-chain, which lets the user know what tractions count and can be trusted. But, a better solution for preventing this attack is to have a timestamp server. A timestamp server works by taking a hash of a block of item to be timestamped and widely publishing the hash. Timestamp proves that the data must have existed at the time. The below figure F [14] shows block chain structure with timestamp.

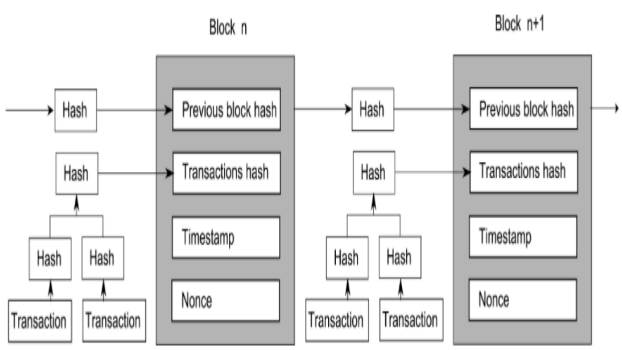

Figure F

B. Brute Force Attack

Brute Force Attack is nothing but an exhaustive key search. In a theoretical manner, a brute force attack can be used against any data, which has been encrypted. This kind of attacks can be used when all other options have been employed to exploit the weaknesses of the encryption system. Brute force attack checks all possible keys, or passwords that it can get its hand on until the correct key or password has been found [15].

In theory, Brute Force attacks can be applied on Bitcoin. Brute Force attacks can be used to attack keys, which were generated by wrongly configured random number generators. Also it can be employed towards poorly chosen brain wallets, which are nothing but repositories of the passwords of a network system.

Every Bitcoin private key is meant for exactly one Bitcoin public address. The algorithm used for the generation of the private keys is Elliptic Curve Digital Signature Algorithm (ECDSA). So in order to obtain the keys the brute force attack has to be applied to the ECDSA. That requires operations in the magnitude of 2^256 (since the private key is 256 bits). If we consider in terms of magnitude, brute forcing 50 bits would cost $1000 of CPU time. So it's a waste of time and resources trying to brute force a Bitcoin private key. This is the reason why Brute force attacks are not computationally feasible.

C. Finney Attack

The Finney attack has been named after the person who discovered this attack. His name is Hal Finney and he is the first person to receive a Bitcoin transaction. The Finney attack is a variant of the double spending attack. A Finney attack works only if the merchant who is involved in the trading accepts unconfirmed transactions. It can also work when the trader waits for few seconds to ensure that everyone in the network agrees that he has indeed paid. Also the Finney attack can only happen when the attacker is mining and is keeping control of the contents of the block.

The hacker who is employing this technique makes two transactions-one acknowledging the person he is trying to rip off and one crediting himself. The hacker doesn't use the first transaction and goes ahead with the mining of the second block. This takes a certain amount of time and the moment he is successful, he uses the stored first transaction to purchase the good he wanted. Then he frees the pre-mined block. This ensures that the former transaction is invalidated even when it shows up in the block table.

Finney attacks are performed in groups because it is rather difficult to conduct this attack alone because mining a block by oneself requires a lot of resources. The best thing about this attack is that it is virtually undetectable until the entire process has been executed and it is too late for the trader. The only solution that is available for this kind of attack is to make at least one confirmation per transaction before sending out the goods and repeating this process for each and every transaction.

The most recent case of a Finney attack was against a gaming website called Satoshi Dice where some illegal miners were using this technique to siphon money from them. The miners created a block where they credited themselves. Then the miners sent another transaction to Satoshi Dice that would let them earn more money than the reward for each block. If they lost the released that block and got their money back and if they won they would discard the block and keep the winnings. Once Satoshi Dice got to know of this attack, they switched over to processing bets with 1 or more confirmations, which remains the only way to block a Finney attack [16].

VII. CONCLUSION

In this paper we wanted to explain the working and security concepts of Bitcoin by briefly going through the protocols that are implemented in its each and every category. We have compared Bitcoin with similar peer-to-peer model systems like Litecoin, Ripple and Mintchip. Also Bitcoin's major vulnerabilities such as Double-spending attack, Brute force attack and Finney attack have been discussed with possible solutions to overcome those weaknesses. Bitcoin's full potential has not been completely analyzed yet. But, the true future of Bitcoin is evident: The technology of the distributed asset ledger combined with an incentive-producing currency is certain to remain with us for all time.

VIII. REFERENCES

[1] Peck, M, "Bitcoin: The Cryptoanarchists' Answer to Cash". Retrieved April, 2014 Available: http://spectrum.ieee.org/computing/software/bitcoin-thecryptoanarchists-answer-to-cash

[2] Steadman, I , %22Wary of Bitcoin? A guide to some other cryptocurrencies%22. Retrieved April,2014 http://arstechnica.com/business/2013/05/wary-of-Bitcoin-a-guide-tosome-other-

[3] Internet: http://en.wikipedia.org/wiki/Bitcoin#wallets [Dec. 6, 2014]

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." Internet: https://bitcoin.org/bitcoin.pdf

[5] Internet: http://visual.ly/bitcoin-infographic [May. 24, 2012]

[6] Conrad Barski and Chris Wilmer, "Bitcoin for the Befuddled", USA: No Starch Press, 2013

[7] Internet: https://www.weusecoins.com/en/mining-guide, [2014]

[8] Internet: 'http://www.coindesk.com/information/comparing-litecoin-bitcoin/' [Apr. 2, 2014]

[9] Danny Vega, Internet: 'http://heavy.com/tech/2013/12/bitcoin-vs-litecoin-peercoin-ripple-namecoin/' [Dec. 2, 2013]

[10] Jason D. O'Grady Internet: 'http://www.zdnet.com/article/a-crypto-currency-primer-bitcoin-vs-litecoin/' [Dec. 14, 2013]

[11] Pieter Wuille, Internet: 'http://bitcoin.stackexchange.com/questions/7549/what-is-ripple-and-how-does-it-compare-to-bitcoin'

[12] Vitalik Buterin, Internet: 'http://bitcoinmagazine.com/776/the-mintchip-the-canadian-governments-answer-to-bitcoin/' [Apr. 5, 2012]

[13] David George-Cosh, Internet: 'http://blogs.wsj.com/canadarealtime/2014/04/04/canada-puts-halt-to-mintchip-plans-could-sell-digital-currency-program/' [Apr. 4, 2014]

[14] Jan Klusacek, "Trusted Timestamp in Cryptocurrency Blockchain" Internet: http://www.feec.vutbr.cz/EEICT/2014/sbornik/03doktorskeprojekty/01elektronikaakomunikace/03-xklusa00@stud.feec.vutbr.cz.pdf, [2014]

[15] Internet: 'http://en.wikipedia.org/wiki/Brute-force_attack' [Nov. 25, 2014]

[16] ThePiachu Internet: 'http://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack' [Oct. 3, 2012]