2017 International Conference on Computer, Communications and Electronics (Comptelix)
Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017

Evolution of Bitcoin and Security Risk in Bitcoin Wallets

[*]Puneet Kumar Kaushal, [**]Dr. Amandeep Bagga, [***]Dr. Rajeev Sobti,
Lovely Professional University, Phagwara, Punjab, India – 144411
[*]kkpuneet@gmail.com, [**]amandeep.bagga@gmail.com, [***]rajeev.sobti@lpu.co.in

***Abstract*—This paper identifies trust factor and rewarding nature of bitcoin system, and analyzes bitcoin features which may facilitate bitcoin to emerge as a universal currency. Paper presents the gap between proposed theoretical-architecture and current practical-implementation of bitcoin system in terms of achieving decentralization, anonymity of users, and consensus. Paper presents three different ways in which a user can manage bitcoins. We attempt to identify the security risk and feasible attacks on these configurations of bitcoin management. We have shown that not all bitcoin wallets are safe against all possible types of attacks. Bitcoin core is only safest mode of operating bitcoin till date as it is secure against all feasible attacks, and is vulnerable only against block-chain rewriting.**

Keywords— Bitcoin; bitcoin wallet; bitcoin evolution, threats on bitcoin network, distributed consensus in bitcoin.

I. INTRODUCTION

In 2009, an unidentified hacker or a group of hackers under the name Satoshi Nakamoto [1] created a peer to peer and decentralized financial system called "Bitcoin" and published it as a whitepaper [2]. The concept was not new. The concept of "crypto-currency" was firstly introduced by Wei Dai in 1998 in cryptographic mailing list 'cypherpunks'. Bitcoin provides a platform to run currency without any central control. Satoshi Nakamoto did not reveal anything about his identity and there could be multiple reasons behind it. He might have been inspired by Bernard von NotHaus and his Liberty dollar [3] which landed the latter into conviction for counterfeiting the fiat currency [4], and Satoshi did not want to fall in the same state of affairs as NotHaus did. Another assumption is that Satoshi wanted to create a faith in the bitcoin system. If this system was developed by a known individual or an organization, then people might start thinking that the inventor must be getting some profit out of this. So, he created bitcoin and left it open to the public. Bitcoin was launched soon after the financial crisis of 2007-2008 that had dented people's faith in central banking authorities [5]. This could have been another driving force for Nakamoto to start with the decentralized monetary system.

Bitcoin supersedes fiat currency in multiple dimensions because it can be transferred internationally without any limits, transactions have either no fees or a very low fee, currently it does not need any personal information (useful for anonymity), is transparent as every user has a copy of public ledger, and secure as the underlying cryptographic algorithm provides security. As it is a new currency in the system, two major challenges that Bitcoin is facing are volatility, and degree of acceptance. Perhaps volatility keeps on decreasing as more people join the network.

Pavel et al. [6] analyzed bitcoin characteristics to make it a global currency, and identified that it has an insignificant market presence and price volatility that pulls it back when compared to fiat currency. Kleineberg et al. demonstrated how bitcoin can sustain digital diversity through multidimensional incentive system [7]. The threat of currency counterfeiting always brings mistrust among the people. Chambers et al. identified security and technology involved in currency manufacturing and specified that a robust currency is required [8]. These requirements are fulfilled by bitcoin up to a greater extent. Juan et al. presented bootstrapped protocol like bitcoin which do not require trusted-setup and needs only majority of honest nodes in terms of hash power [9]. Yonatan et al. presented a faster cryptocurrency protocol based upon block chain technology that squeezes delay in confirmation of transactions from several minutes to seconds [10]. The demonetization move in India in November 2016 further fuels people's interest in peer to peer currency which is unrestricted from any such kind of centralized decisions effecting people's life.

II. DECENTRALIZATION IN BITCOIN

Bitcoin is the first system of currency which is completely decentralized and beyond the control of any monetary power. Learning from the failure of the centralized economic system and NotHaus' conviction, the inventor of bitcoin made it decentralized. However, this decentralization is limited to the following aspects:

- The ledger of transactions is maintained publicly by every node.
- Transactions are validated by distributed node and not by any central authority.
- New bitcoins can be created by any node, unlike centralized government economy.
- Bitcoin exchange values are dynamic and there is no central control over it.

The emphasis on decentralization is accomplished up to an extent. However, beyond the protocol the system is still not decentralized as the development of wallet software, service

providers and bitcoin exchange is not completely distributed. But it is decentralized in a manner that users have the transparency of validating the code used for the services and can also participate in software development, as Bitcoin core software is developed through deterministic build.

III. The Block and the Blockchain

All the bitcoin transactions are collectively stored in a public ledger called as block chain [11] which is accessible and maintained by every node in the network. Block chain works as a backbone for a system which does not require any central trusted authority. In bitcoin, on an average of 10 minutes a block of accepted transactions is added to block chain and further broadcasted to all the other nodes. The block contains: reference to previous block, record of some and not all recent transactions, and answer to the hash-puzzle which is solved by the node. The current size of block chain as on 3 January 2017 is 96645 MB.

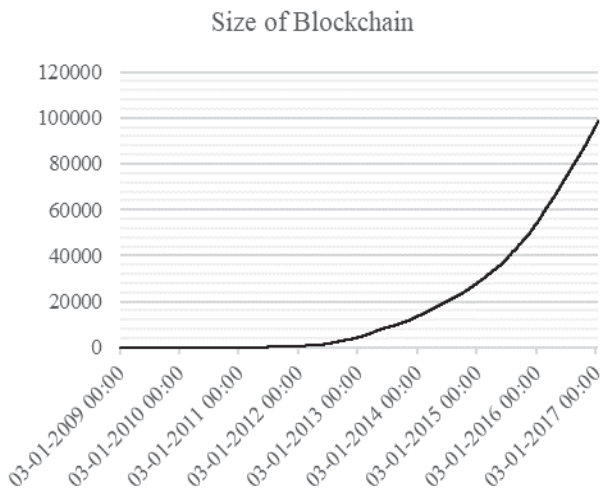

Fig. 1. Shows growth in blockchain (y-axis) in Megabyte along with time (x-axis) (Source: blockchain.info)

IV. Distributed consensus protocol in Bitcoin

The agreement in the judgment by the group is a desirable property in distributed monetary system. In bitcoin, there is no central authority which decides who is having how much amount of money. There is no governing authority who testifies that Alice has transferred a sum of bitcoins to Bob. Bitcoin resolves this issue by broadcasting every transaction to all the nodes in the network and all nodes have consensus on a sequence of transactions. These transactions get clustered inside block chain. Confirmation through consensus in network shows that the coins received by one node is not spent anywhere else.

Consensus on peer to peer network is hard as the network is imperfect. This is a fundamental problem in many other fields of computing where multiple nodes are present. There could be faults and latency in the network, nodes may crash, there can be malicious nodes, and not all nodes are connected always. In bitcoin, there is no concept of global time and nodes cannot agree upon transactions based upon the timestamp. The consensus in a decentralized environment raises serious issues. In literature, there are some impossibility results in distributed consensus like Byzantine's Generals' Problem [12], and Fischer Lynch Paterson impossibility of distributed consensus with one faulty process [13]. The Paxos consensus [14] performs better under the condition that, the situations that can fail Paxos can rise rarely [15] [14]. However, the consensus protocol in bitcoin system is practically working well dissimilar to what is mentioned in the literature. One of the plausible reason is the incentive policy which can only be integrated into a currency system.

V. Incentive policies in Bitcoin

The Block Reward - The nodes get rewarded for every new block they create through special "coin creation" transaction. The node is required to include this transaction into the block with recipient address as the address itself. The block reward reduces to half every four years. Starting from March 2009, this block reward was 50 Bitcoin (50 BTC). Currently, we are in the third round of bitcoin period and the block reward is 12.5 BTC. As per the bitcoin rule, this is the only way through which new bitcoins can be created in the system.

The Transaction Fee - In bitcoin system the user who initiates the transaction usually has output value less than the input value. The difference is considered as a transaction fee and goes as an incentive to that miner who creates the block.

Another benefit of having a transaction fee is that it avoids users to overload the network through transactions. The transaction fee is not related to number of bitcoins transferred. The way fee is charged is still under development and assumed to change over time. Currently, it is proportional to the size of data in the transaction.

VI. Bitcoin Mining and Selection of node for extending block chain

The block creation is basically done by "proof of work" that involves a lot of computing power. This proof of work also prevents malicious identity creation and thus avoids Sybil attack. *The Proof of work* in bitcoin is a hash puzzle that requires a huge amount of computing power to work out, and can easily be verified by anyone. To get up to the block in a block chain, the node is required to solve a computational problem which is given by:

Find nonce such that,

$H(nonce \,||\, prev\_hash \,||\, tx_1 \,||\, tx_2 \,||\, \ldots\ldots \,||\, tx_n)$ = *Output hash with some leading zeros*

Whereas, H = Hash function (SHA-256 in bitcoin).
prev_hash = Hash of the previous block.

tx_1 *to* tx_n = Set of all orphaned transactions which are not included in the block.

Nodes in the network are continuously working on solving this hash puzzle. The nodes are selected automatically in the system to propose the next block as soon as they solve the computational problem. Nodes working on solving hash puzzle are called as miners and the process is called *Bitcoin Mining*. There is a lot of incentive for miners but it also requires a huge amount of investment in terms of sourcing the computation power to solve the hash puzzle. The cost involved for solving the mathematical problem is not fixed every time. In bitcoin, all the nodes automatically re-calculate the average time of block creation every two weeks, and the aim is to keep this average time between two successive blocks globally as 10 minutes. The automatic recalculation property of finding the next block is very crucial in bitcoin. If blocks in the block chain start appearing very soon one after each other, the nodes will lose the ability to adjust all the transactions in the block and will become incompetent. So, it is important to prevent the latency of 10 minutes from falling any further. With this latency and block reward halving every year starting from 50 BTC (in 2009), bitcoin will have a total of 34 halving after which it will reach to block reward of 0 BTC. After 33 halving, it will reach to block reward of 1 Satoshi which cannot be divided any further. With this calculation, it can be figured out that total of 21 million bitcoins will be mined till 2140 as halving is done after every 4 years. Currently, total bitcoins in circulation are nearly 16 million which means 5 million more bitcoins will be mined.

VII. Computation Difficulty in Bitcoin

As digital currency is getting popularity and bitcoin network is growing, more miners are joining the network. This ultimately increases the overall mining computational power. So, it is obvious that larger number of blocks will be created in future than at present and the average time between block creation will shrink. So, the bitcoin system is designed in such a manner that nodes automatically readjust the difficulty level for solving the puzzle, and the amount of work required by a new miner will automatically be higher. This can be understood with the following equation:

Probability that any miner wins next block = fraction of total bitcoin computation power miner posses

For example, if the user has 0.01 percent of global computation power of all bitcoin miners collectively, then there is a chance of 1 in every 10,000 blocks, that he wins in finding the right block. Also, for an individual user, the average time (User_Avg_T) for finding the node can be calculated as:

$$User\ (AvgT) = \frac{BTCn\_Avg\_T}{Fr\_CompPow}$$

Where,

BTCn_Avg_T = Bitcoin network (Avg time of finding block).
Fr_CompPow = Fraction of computational power user has.

There are several miners who are continuously mining and creating a block in the global block chain.

VIII. The Financial Side of Mining

The miners in bitcoin get incentivized with two things: the block reward and the transaction fee. To get this mining reward users are required to invest in hardware as well as in electricity. If the mining reward is greater than the cost involved in hardware and electricity, then bitcoin mining will be profitable.

If, mining reward (block reward + trans fee) > mining expenditure (hardware + electricity)

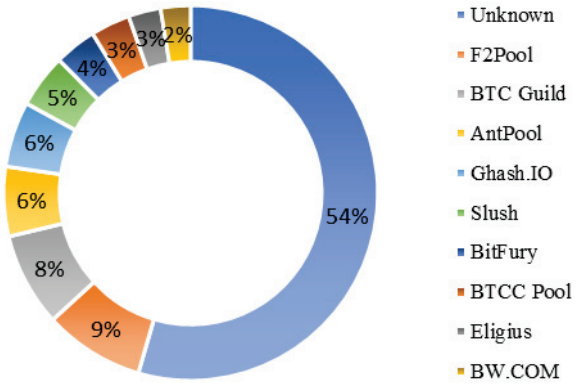

Fig. 3. Shows number of blocks found by top 10 mining pools as on 16 March 2017 (Source: Blockchain.com)

Then profit, otherwise loss.

Also, Cost incurred as mining expenditure will be in fiat currency and outcome of mining will be in bitcoin. So, this factor must be taken into consideration while calculating the actual profit.

IX. The Double Spending Problem

The acceptance of a transaction in the bitcoin network is signaled by extending the block chain and rejection is done by ignoring the transaction and keeping only the latest updated block chain by other nodes. Node 'A' can make a transaction to node 'B' {A -> B} and after that to node 'C' {A -> C} with the same bitcoin. Now, it becomes difficult for the other nodes in the network to determine which one is the double spending attack as the scenario may look another way round. As per the rule nodes are supposed to extend the longest chain, and here at this point, both will have the same length of the block chain. Now, two things may occur:

- Node B may wait for the confirmation from an honest node to include transaction {A -> B} into the block

chain. This will eliminate the chances for the confirmation of other transaction, i.e., {A -> C} to be included in the block chain.

- Node B can orphan the previous transaction {A -> B} as soon as it gets to know about the transaction {A -> C}, as in a peer-to-peer network all the transactions are broadcasted.

The probability of double spending problem reduces drastically as the number of confirmation keeps on increasing and currently in bitcoin the notion is of 6 confirmations. Six confirmations are just a trade-off between the time in which the transaction ends up in the consensus and the time a user is required to wait.

X. Security of block chain

The stable and high value of bitcoin depends upon the security of block chain. Security further depends upon the health of bitcoin mining system and is based upon the number of users involved in mining and creating new blocks. As the number of miners grows in the network people will have more trust in the bitcoin, and chances of crushing the network by malicious nodes reduces. It is, in fact, true that the transactions are cryptographically secure, but 'invalid-transactions' and 'double-spending' are orphaned through consensus in the network. So, user's participation is involved in maintaining the security. When Nakamoto started the bitcoin network, it was having lesser number of nodes and the chances of Sybil attack was higher. But as the time passes by, more and more people came to know about the block chain and digital currency. Their participation in incentivized block chain now created a healthy mining ecosystem and established a value of the currency which is more trustable than the past, and expected to be more trustful in the coming future.

XI. Identification of threat on bitcoin network

Even if we assume a hypothetical attack where more than 50% of the computational power is possessed by malicious node, there are few offensive attempts that can be made. First is stealing coins from other addresses. Perhaps it is not possible to steal coins as it would require subverting the cryptographic algorithms which is not possible. For stealing coins, malicious nodes are required to create a transaction using the private key of the target node. Deducing the private key corresponding to a public key is cryptographically infeasible with current processing capabilities. Another attack which can be mounted is suppressing the transactions in the block chain. The malicious nodes can simply avoid the transactions that provide payment to a specific address. But still in a peer to peer network, as the transactions are broadcasted to every node, this attack will come under notice due to the presence of honest nodes in the network. Such nodes will include this transaction while creating the block. Third is altering the block reward. This is also not possible as malicious nodes do not control the copy of software distributed all over the network. Even if developers change the copy of the software in its updated version, it will be visible to all the users around the globe. The only loss that can occur in this proposed attack is that people will lose confidence in the system and the price of bitcoin will go down without any initiation of attack from malicious nodes. This is the only feasible practical attack but it would require a huge investment in outnumbering hash power which is again practically difficult to achieve.

XII. Incentive policies in bitcoin

The way bitcoin is used at user end poses a threat to its security. There are multiple ways through which users can manage their bitcoins but not all means are completely safe. Following are the three ways of managing the bitcoins:

A. Through Bitcoin core software

Bitcoin core is built deterministically, also called as "reproducible build". In this, end user can verify whether binary release of the software corresponds to source package or not and thus prevents tiny, undetected malicious difference between source and binary release. This type of development eliminates the transparency gap in open source development process. So, bitcoin core is the safest mode for managing bitcoins. But higher security comes with additional cost. Currently, this approach needs around 80 GB of storage for storing Bitcoin transactional data and involves overhead of verifying correctness of broadcast transactions in the system.

B. Through Bitcoin bank and exchanges

In this system, users don't control their private key. Private key of the user is stored by the bank. A company control user's bitcoin on his behalf. In case of company's disappearance user will lose all his money. In this approach, there is very less overhead on client with compromised security at user's end.

C. Simplified payment verification (SPV) wallets

SPV wallet is named after Satoshi Nakamoto paper section that describes it. Users control their private key, but cannot verify the software as it is in executable form and source code is not available. This type of wallet can verify whether a transaction is a part of the block or not without downloading block chain, as node connects only to some of the other peers in the network and it is dependent on those peers. Node cannot verify whether transaction is valid. As compared to Bitcoin core, SPV wallets are gaining popularity due to less overhead or resources and reduced bandwidth consumption.

With these three types of initial setup options available with the user, it is highly recommended to prefer Bitcoin core as it is the safest mode of operating and managing the bitcoins. With other options, there are chances of various kinds of attacks which are explained below:

Direct theft: Occurs when bank owner disappears with the depositor's money. Bank wallets are not safe against this type

of attack. The collapse of Mt. Gox is an example of failure of this kind of system [16]. The firm lost 650000 bitcoins which were a part of their customer's deposits. Mt. Gox claimed that the failure was a result of fault in software algorithm used for bitcoin [17]. Mt Gox went bankrupt and people were not able to recover their money.

Bait and Switch: Occurs when bank audits the source code of the software and pushes new code to user for stealing the coins. Bank wallets and SPV wallets are not safe against this attack. Defensive step taken by online wallet StrongCoin to steal back their bitcoin is an example of this kind of attack [18]. OzCoin mining pool was hacked and 923 bitcoins were stolen. However, StrongCoin modified their wallet code and recovered 569 bitcoins from suspected user. Perhaps the intentions were not bad, but such an attack poses a threat to privacy and security of web wallets.

TABLE I. POSSIBLE TYPES OF ATTACKS IN VARIOUS BITCOIN MANAGEMENT TECHNIQUES

Type of Attack	**Type of Wallet**		
	Bitcoin Core	***SPV Wallet***	***Bank/ Exchange Wallet***
Bait and Switch	No	Yes	Yes
Direct Theft	No	No	Yes
Fabricated Transaction	No	Partially Safe	Yes
Chain High jacking	No	Yes	Yes
Unintentional Transaction suppression	No	Yes	Yes
Intentional Transaction suppression	No	Yes	Yes
Rewriting Chain	Yes	Yes	Yes

Fabricated Transaction: When user realizes that the transaction which pays him bitcoin is a fake transaction. Only Bitcoin core is safe against this type of attack. Bitcoin bank users depends upon the information provided by the bank, and SPV wallet-users depend on miners and full nodes for validating transactions. Apps like Bitcoinj [19] that follows SPV, select random peers on startup so that it can be difficult for an attacker to control the transaction against any node. So, in that case SPV wallet can be considered safe against this type of attack. The practical example for fabricated transaction was presented by a security researcher from central Europe with code name "ShadowShark" on 4 August 2015 with good intentions [20]. He spent 250 bitcoins which people believed were owned by Nakamoto and showed that the transactions were not validated with bitcoin core by blockchain.info.

Chain High jacking: When invalid transactions are confirmed by faulty miners and more than 50% of the hash rate starts authenticating invalid transactions. Only Bitcoin core is safe against this type of attack. This type of attack, when identified first, was unintentional. An invalid block chain, which was longer than the valid block chain, was created by multiple miners in July 2015 [21]. The problem arose when large miners created invalid blocks, and SPV wallets and bank wallet accepted this chain as the longest block chain. It was believed that faulty miners controlled more than 50% of the hash rate in the network. At that time 37500 dollars were lost by large miners were duped into accepting invalid transactions as they thought them to be lawful. The fix by bitcoin core community was a recommendation to switch to full validation block chain at least on a temporary basis by all banks and SPV wallets. It was recommended to wait for 30 more confirmations before a transaction was accepted.

Unintentional Transaction suppression: This type of attack can be better understood with an example. Let us suppose Alice gives $900 to Bob for getting 1 BTC. Bob performs a transaction of 1 BTC to Alice. It turns out that the transaction does not confirm even after waiting for some time. So, Bob gives away $900 to Alice. But later, the transaction is validated and Bob is in loss of 1 BTC which is now held by Alice. This type of accidental attack is not possible only in case of Bitcoin core. If any transaction is not included in the block for some time, its status can be seen in Bitcoin core graphical user interface [22]. Chainanalysis company in March 2015 prevented some BreadWallet users to connect honest node and verify their transactions. Since Chainanalysis introduced spy node which do not relay transactions, BreadWallet users did not get information about new transactions. It was accidental as claimed by CEO. 250 false bitcoin nodes were created to get information about some transactions [23].

Intentional Transaction suppression: Node 'A' can deny the transaction which is originating from node 'B' while creating next block in the chain. This is a genuine attack that can be mounted but this type of attack is just an aggravation as that transaction will be included in the block as soon as an honest node gets a chance to propose a block. Thus, this type of attack can easily be thwarted in Bitcoin core if the network is having more than 50% of the honest nodes. But in SPV wallet and bitcoin exchanges, users do not have full control over transactions, so this type of attack is feasible. *Rewriting chain*: This is also known as 51% attack on block chain and is only type of attack which is applicable in all three types of bitcoin services. It is possible that Alice may steal back the bitcoins even after the confirmation of transactions, which she has transferred to Bob a while ago. But this type of attack requires very high computation power so that miner can rewrite the block chain. The transactions in bitcoin are piled up inside blocks in block chain and the rule says to go by the longest block chain. If a miner or group of miners control 51% of the hashing power of complete network, it may work exhaustively on extending that blockchain and becoming the longest block chain. All invalid transactions will then appear as valid due to the bitcoin rule.

XIII. Future work and Conclusion

People need to understand crypto currency and need to understand how this digital currency is originated and gets its value. The insufficient knowledge of economy and crypto may dupe people to destroy economy made up of digital currency. The purpose of bitcoin is to create a currency through public ledger without the need of the third party and to establish a trust through peer to peer collaboration. Presently, Bitcoin system lacks scalability as it cannot process transactions like Visa Network and other payment gateways, both in terms of speed and bandwidth. As on April 2015, VisaNet is capable of handling more than 56000 transaction messages per second [24]. Bitcoin shall not be assumed as completely anonymous as the transactions can be linked to other addresses.

Other than the Bitcoin, there are many other forms of digital currencies called Altcoins, which have emerged in the last few years. Altcoins include LiteCoins, DogeCoin, Ripple, Namecoin, Peercoin, DevCoin, ByteCoin and the list goes on. With steady growth in digital currency, a parallel economy is developing and it is time when the government should step in and put regulations into it. Putting regulations may help states to impose taxes and prevent black money to sustain in the system. Countries like China, Russia, India, Ecuador, Iceland, Sweden, Thailand, and Bolivia have banned the use of bitcoin. But still, people from these countries are making use of bitcoin as the government does not have control over it. Japan recognizes bitcoin as a currency and has a positive viewpoint towards it [25]. Any currency must not be treated as illegal if it is not at par with government money. It would be wrong to say that the system of digital currency has evolved perfectly as it still lacks the potential to build a good economy which even fiat currency is also not able to do in the history at times of global recessions. Future work in bitcoin involves those aspects that can manage instant boom and burst in the economy thus improving the trust. The current social economic stability depends upon the centralized taxation system by government. Perhaps this digital currency system currently does not get any close to that. It would be interesting to see how society and states will grow up without any central power as economic strength of any state is hooked on the currency.

REFERENCES

[1] A. Chen. (2016, May 9). We need to know who Satoshi Nakamoto is. *The New Yorker* [Online]. Available: http://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is. Retrieved 30 Dec 2016.

[2] S. Nakamoto. (2008). *Bitcoin: A peer-to-peer electronic cash system* [Online]. Available: http://www.bitcoin.org/bitcoin.pdf. Retrieved 30 December 2016.

[3] G. Paul. (2006, Dec 18). Husband, wife lease Royal Hawaiian Mint NORFED founder issues RHM piece. *Coin World* [Online]. Available: http://www.libertydollar.org/news-stories/pdfs/1166043540.pdf. Retrieved 30 December 2016.

[4] J. Taylor. (2007, Nov 16). Your Liberty Dollar Raid Update. *The Liberty Dollar* [Online]. Available: http://libertydollar.org/commentary/pdfs/1196746450.pdf. Retrieved 30 December 2016.

[5] B. Davis. (2009, Apr 22). "What's a Global Recession?". *The Wall Street Journal* [Online]. Available: https://blogs.wsj.com/economics/2009/04/22/whats-a-global-recession/. Retrieved 30 December 2016.

[6] P. Ciaian, M. Rajcaniova and d. Kancs, "The digital agenda of virtual currencies: Can BitCoin become a global currency?", *Information Systems and e-Business Management*, vol. 14, no. 4, pp. 883-919, 2016.

[7] K. Kleineberg and D. Helbing, "A "Social Bitcoin" could sustain a democratic digital world", 2016.

[8] J. Chambers, W. Yan, A. Garhwal and M. Kankanhalli, "Currency security and forensics: a survey", *Multimedia Tools and Applications*, vol. 74, no. 11, pp. 4013-4043, 2014.

[9] J. A. Garay et al., "Bootstrapping the Blockchain -- Directly", *Cryptology eprint Archive*, 2016. [Online]. Available: https://eprint.iacr.org/2016/991.pdf. [Accessed: 30- Dec- 2016].

[10] Y. Sompolinsky et al., "SPECTRE: A Fast and Scalable Cryptocurrency Protocol", *Cryptology eprint archive*, 2016. [Online]. Available: https://eprint.iacr.org/2016/1159.pdf. [Accessed: 30- Dec- 2016].

[11] "The great chain of being sure about things", *Economist.com*, 2015. [Online]. Available: http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable. [Accessed: 30- Dec- 2016].

[12] L. Lamport et al., "The Byzantine Generals Problem", *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382-401, 1982.

[13] M. Fischer et al., "Impossibility of distributed consensus with one faulty process", *Journal of the ACM*, vol. 32, no. 2, pp. 374-382, 1985.

[14] L. Lamport, "The part-time parliament", *ACM Transactions on Computer Systems*, vol. 16, no. 2, pp. 133-169, 1998.

[15] L. Lamport and M. Massa, "Cheap Paxos", *in International Conference on Dependable Systems and Networks*, IEEE Computer Society, 2004, p. 307.

[16] R. McMillan and C. Metz, "The Rise and Fall of the World's Largest Bitcoin Exchange", *Wired.com*, 2013. [Online]. Available: https://www.wired.com/2013/11/mtgox/. [Accessed: 30- Dec- 2016].

[17] T. Hals, "Mt. Gox files U.S. bankruptcy, opponents call it a ruse", *Reuters*, 2014. [Online]. Available: http://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA290WU20140310. [Accessed: 30- Dec- 2016].

[18] V. Buterin, "OzCoin Hacked, Stolen Funds Seized and Returned by StrongCoin — Bitcoin Magazine", *Bitcoin Magazine*, 2013. [Online]. Available: https://bitcoinmagazine.com/articles/ozcoin-hacked-stolen-funds-seized-and-returned-by-strongcoin-1366822516/. [Accessed: 30- Dec- 2016].

[19] "Understanding the bitcoinj security model", *Bitcoinj.github.io*. [Online]. Available: https://bitcoinj.github.io/security-model#pending-transactions. [Accessed: 01- Jan- 2017].

[20] "blockchain.info / spoofed transactions problem / Aug. 4, 2015", *reddit*, 2015. [Online]. Available: https://www.reddit.com/r/Bitcoin/comments/3fv42j/blockchaininfospoofed_transactions_problem_aug_4/. [Accessed: 01- Jan- 2017].

[21] "Some Miners Generating Invalid Blocks", *Bitcoin.org*, 2015. [Online]. Available: https://bitcoin.org/en/alert/2015-07-04-spv-mining. [Accessed: 02- Jan- 2017].

[22] "User Interface - Bitcoin Core Features", *Bitcoin.org*. [Online]. Available: https://bitcoin.org/en/bitcoin-core/features/user-interface#graphical. [Accessed: 01- Jan- 2017].

[23] G. Caffyn, "Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network", *CoinDesk*, 2015. [Online]. Available: http://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network/. [Accessed: 02- Jan- 2017].

[24] "Visa Inc. Reports". *Usa.visa.com*. [Online]. Available: https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.2042597.html. [Accessed: 01- Jan- 2017].

[25] "Japan Officially Recognizes Bitcoin and Digital Currencies as Money | Bitconnect", *Bitconnect.co*, 2016. [Online]. Available: https://bitconnect.co/bitcoin-news/130/japan-officially-recognizes-bitcoin-and-digital-currencies-as-money. [Accessed: 02- Jan- 2017].