International Journal of Security and Its Applications
Vol. 11, No. 10 (2017) pp.25-34
http://dx.doi.org/10.14257/ijsia.2017.11.10.03

Towards an Ethical Online Payment System through Cryptography and Next Generation Communication Network

Marwa Yousif Hassan[1], Abdi O. Shuriye[2], Momoh Jimoh Eyiomika Salam[3], Aisha Hassan Abdalla[4] and Othman O. Khalifa[5]

[1]Department of Electrical and Computer Engineering
Kulliyah of Engineering
[2]Department of Mechatronic Engineering
[3,4] Department of Electrical and Computer Engineering
IIUM
Kuala Lumpur, Malaysia

Abstract

The internet brings unprecedented connectivity and communications for both social and commercial settings. There have been many businesses that offer their products and services completely online. Nowadays, even the break and mortar businesses use the internet in a way or another to promote their offerings and to reach people and places they would have never thought of reaching them before the internet era. Conventional online payment systems such as credit and debit cards have enabled such a revolutionary way of doing business. However, conventional financial system has been generating catastrophic disasters to the world. The great depression of 1930s, the World War II, the dot com bubble at the beginning of the new century, and the recent financial crisis that has begun on 2008; to name a few. This will persist if we keep trusting the old ways of finance. This paper investigates the relatively new online payment system termed "Bitcoin" which embraces intentionally or unintentionally the principle of Islamic finance such as saving, compared to the conventional financial system of borrowing, lending and "Riba" (interest).

1. Introduction

Real stories of people who have experienced economical tragedies are the best in showing the dark sides of the conventional economy. One of them is the story of Edmund L. Andrews, the New York Times magazine's economic reporter, who has transcribed his personal credit crisis in a book entitled "Busted: Life inside the Great Mortgage Meltdown" during the recent collapse of the mortgage market in the United States which has triggered the global financial crisis. Despite of his economic experience and knowledge, Mr. Edmund was a victim of a lending company that has literally begged him to take a mortgage loan during the housing boom in the US even though he was not qualified to take such a loan, that most of his income went to alimony and child support of a previous marriage at that time. He was getting married again and the offer was so appealing that he could not reject. He took the mortgage, bought the house and got married and life was perfect for a while. When the lending company decided to increase the interest rate, his monthly payment has jumped and as a result he and his family could not even buy life essentials after paying the mortgage. They had to use their credit cards to make ends meet. The debt from mortgage loan and the credit cards had been magnified. After years of stress and defaults, Mr. Edmund had not only lost his wealth, but he had also lost his new marriage [5, 6].

Received (March 13, 2017), Review Result (August 16, 2017), Accepted (September 8, 2017)

ISSN: 1738-9976 IJSIA

2. The Economy of Deception

One of the famous theories that economic policy makers in today's economy extensively use, is the Monetarism Theory. It was developed by Milton Friedman, the Nobel Prize winner of 1976 for his work in its developing. Friedman idea was encapsulated in the equation :(MV= PY), M denotes Money Supply, V for velocity which is a measure of how fast people spend their money, P for price levels, and Y for the real GDP which is a measure for economic growth. According to Friedman, to maintain the GDP at an acceptable level, Money supply should be increased. That can be achieved by governments by means of printing more money; however, governments can control only 20% of the total money supply. The other 80% comes from loans that are made by banks. Also, he assumes the velocity as constant which has proved not to be the case because the speed of how people spend their money is behavioral and not easily controlled, by nature.

According to Friedman and his theory, in order to revive the economy, governments should print money, people should spend it and banks should lend it. However, spending which is driven by the psychology of lenders, borrowers and consumers, is essentially a behavioral phenomenon. Therefore, to revive the economy, Governments need to change mass behavior and convince banks to lend and people to spend, sometimes money that they do not actually own. Using mass media to change mass behavior sometimes involves the use of deception, manipulation and propaganda [1].

3. The Story of Central Banks

A financial crisis had occurred in 1907 after a failed attempt by several New York banks to monopolize the copper market. In addition to being volatile and nervous due to massive losses caused by the 1906 San Francisco earthquake, there was a panicked response in the market triggered by the attempt of cornering the copper market. The crisis made leading private bankers of the day led by J. P. Morgan, the founder of current J. P Morgan financial institution, to act on a saving plan. After the crisis, there had been a consensus among the private bankers that the United States needed a government-sponsored entity with the ability to bail out the private banking system and to lend them unlimited amount of money when needed. That is how the idea of central banking has been found [1].

There had been a general distrust to central banks in the US. That is because there was general and political opposition to the idea of concentrated financial power. In order to get around that problem, the private banks led by representatives of J. P. Morgan and others from Wall Street, organized marketing and educational campaigns in support of the idea. Over the next several years, numerous sponsored research studies and events with prestigious, famous economist and political scientists of the time were conducted, all with a vision to sell the idea of a powerful central bank [1].

The result was a central bank (Federal Reserve) run by the New York banks and addresses their goals. Decades after, in 2008, Citibank, has received the largest bank bailout in history conducted by the U.S. Federal Reserve exactly as intended one hundred years before. Citibank is one of the major New York banks whom its founders had pushed for the establishment of a central bank in America [1].

4. The Global Financial Crisis: What Has Really Happened?

4.1. The American Dream and the Housing Boom

After 9/11, the chairman of US Federal Reserve, Alan Greenspan, worried that the tragedy would cause the already in recession economy to collapse. The economy had already been reeling after the burst of the technology stock bubble. Following the monetarism economic theory, former president Bush urged Americans to spend in order

to boost the country's economy. This concept was more strengthened by a series of interest rate cuts by the Federal Reserve that have created the demand for borrowing and spending in the mortgage sector. Much more Americans were seeking to own new fancy homes to fulfill the American dream of a prosperous and luxurious life style; the dream that turned to be a nightmare in the years to come [2].

4.2. Much More Borrowers

Before the housing boom, there had been long standing rules to document financial condition and credit history of potential borrowers. Mortgage underwriters conducted exhaustive research on their finances. Motivated by the greed to easily cash-in on the housing boom, many banks and non-bank lenders relaxed those rules. The standards borrowers had to meet were lowered so that lenders could monetize large sectors of potential customers with low credits who previously were unable to apply for a mortgage. They have created new types of mortgages that allowed borrowers to get loans they did not afford and triggered a crisis that would have nearly drown the world economy [2].

4.3. Inflating the Subprime Bubble

Mortgages had become huge profit-generators for investment banks, which bought the loans from other banks and non-bank lenders, packaged them together, sliced them up, and sold them as securities [2]. Mortgage-Backed Securities (MBS) are defined as debt obligations that represent claims to the cash flows from pools of mortgage loans, most commonly on residential property [3] and [4]. Investors from around the world had bought mortgage- backed securities unaware that they were toxic and risky investments, miss-led by the highest possible rates of triple -A MBSs given by world class credit rating companies such as Standards & Poor's (S&P) (Figure 1, and 2); who would downgrade millions in mortgage backed securities several years later. In 2007, Standards and Poor's (S&P) admitted its misjudgment [2].

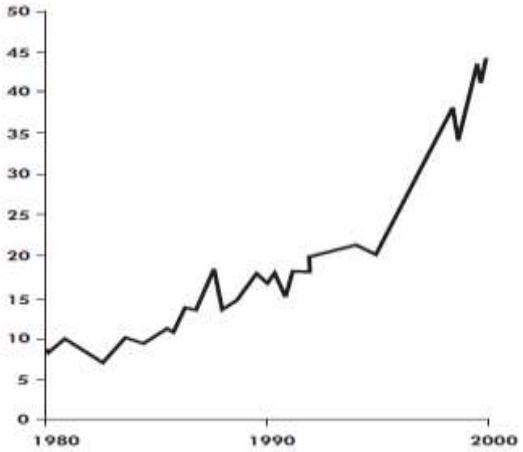


Figure 1. [18]

The graph shows that the stock market (a highly respected US stock index, the S&P 500), has climbed very quickly, and if you had invested in the early 1980s you would have profited very much. This was shown to investors by pension salesmen at the beginning of the millennium.

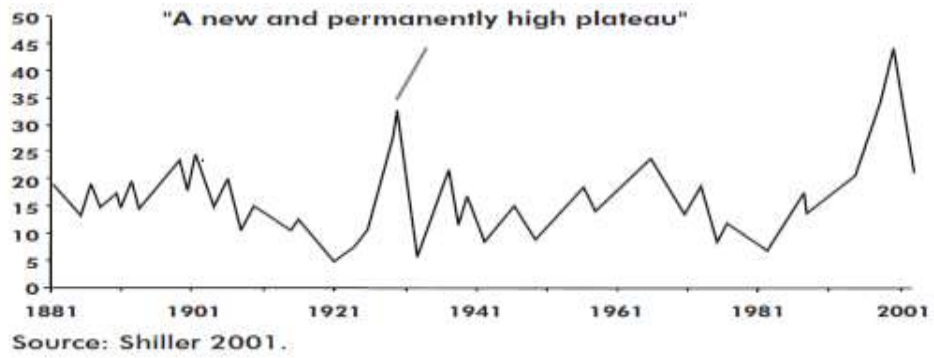


Figure 2. [18]

This graph is the original version of fig. 1 above, however, it spans longer time period from the 1880s to 2001. The graph shows clearly whenever there is a market boom (represented by a high plateau in the graph), the market crashes immediately after it. This has happened in 1930s followed by the great depression, at the year 2000 followed by the burst of the dot com bubble, and also after the housing boom in the US at 2008.

4.4. The Collapse: No One is too big to Fail

Motivated by greed and miss- led by credit rating companies, many banks heavily invested in mortgage- backed securities. As more and more borrowers defaulted, higher interest rates were imposed by lenders, which led to more defaults and foreclosures in a vicious cycle. Many banks were faced by the inevitable fate of bankruptcy despite governmental bailouts. Banks and financial institutions which were considered too big to fail had no choice other than accepting low offers from competitors and buyers. Other banks which were too toxic to be touched had faced their fate of bankruptcy and complete failures. The collapse of big names such as Bear Stearns, Lehman Brothers, and Washington Mutual foreshadowed a global financial crisis that would erupt in the coming weeks and months. Many more well-known companies have collapsed and the world was faced by unpredictable challenges that are still present to the day of this writing.

4.5. Credit Cards: the Time Bomb

As more and more people default on their credit card debt, banks and credit cards issuers inspired by the mortgage- backed securities that have inflated the bubble of subprime, sell credit card debt- backed securities to investors all around the world. These are often pension funds and hedge funds. Securities backed by credit card debt are hundreds of billions of dollars market. This market motivated credit card companies to offer cards to risky borrowers and to allow greater and greater amounts of debt [7, 8, 9].

When we were collecting materials and articles about the financial crisis and the credit cards, we had got many mixed feelings. We felt sympathy for those who have been paralyzed and drown in credit cards debts for all over their lives although they are hard workers and make good living every month. It is the 21st century slavery. It was not understandable to us when we knew the practices of the credit cards companies and the financial sector in order to get easy magnified profits on the expense of ordinary people and against all kinds of ethics and morality. We haven’t accepted the fact that some Muslims who have got the revealed knowledge are involving in such a practice and promoting it, instead of warning others from the unbearable consequences of a war from Allah and his prophet.

5. Other Alternative? The "BITCOIN" Cryptographic System

The main pitfall of a government's controlled economy is the massive financial and manipulation power given to that government. It can devalue the currency of the country it governs on purpose by printing excess money so as to gain competitive advantage over other countries in terms of low cost exports and to create higher employment rates in the expense of inflation in its own country. It also creates deflation and lower employment rates in other countries the thing that may trigger currency wars between nations and may be developed into physical wars so as to protect each country's economic interest as was the case in the World War II [1]. Also, the current financial crisis in the US proved that governments are ready to bailout lobbies of the strong financial sector on the expense of citizens using tax payers' money without a clear return on investment.

Bitcoin is a virtual currency that uses cryptography to control the creation and transfer of money, instead of relying on central authorities. It is a decentralized digital currency that enables payments to be done using peer-to-peer technology with no third party (Figure 3). Transactions and money issuance is carried out and managed by the Bitcoin network. Bitcoins are sent easily through the Internet. It uses public-key cryptography, peer-to-peer networking, and proof-of-work (Figure 5) for payment processing and verifying. Payment transactions are broadcast to the network and included in a ledger-like record called the block chain (Figure 6) so that the included Bitcoins cannot be spent twice. Using these techniques, Bitcoin provides a fast and reliable payment network as is claimed by its users and supporters [13].

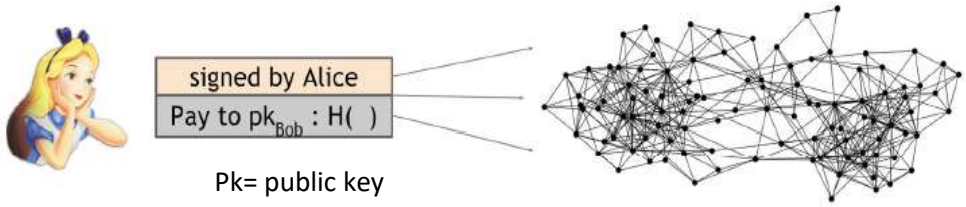
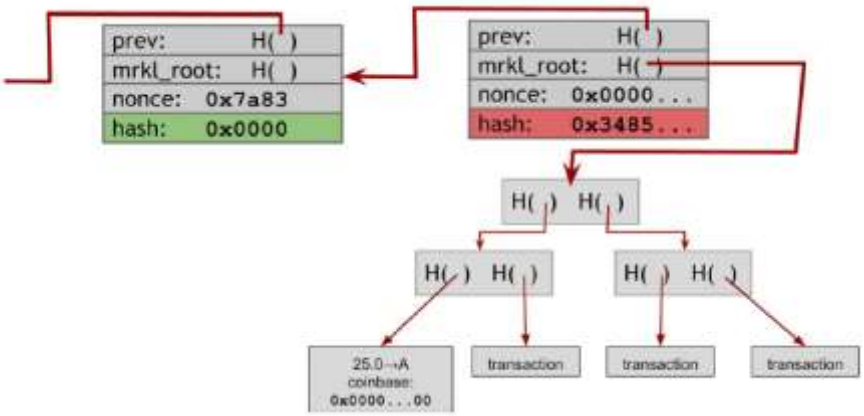


Figure 3. [19, 20]. Bitcoin System is a Peer- to Peer Network that Uses Public Key Cryptography

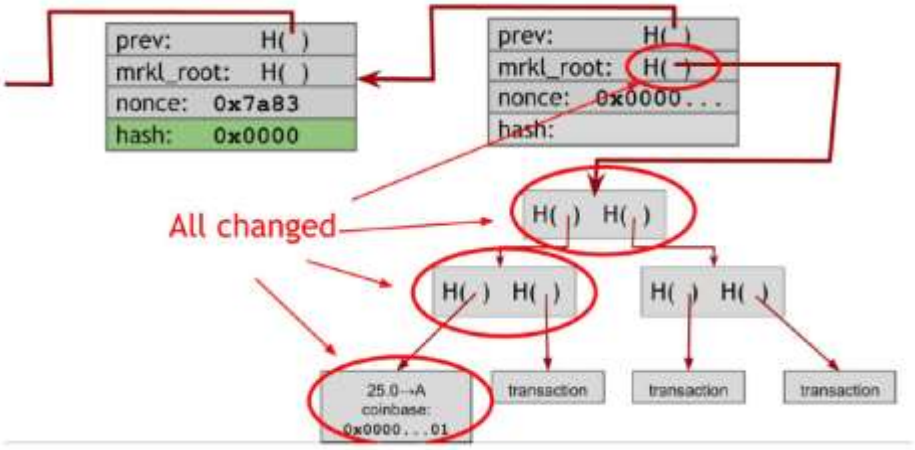
When Alice wants to pay Bob she broadcasts the transaction to the entire Bitcoin network - Public keys here are used as identities to support anonymity which is a central design goal of Bitcoin.

5.1. Securing the Bitcoin System from Attacks By implementing "Public Key Cryptography" and "Proof- Of- Work" Concepts

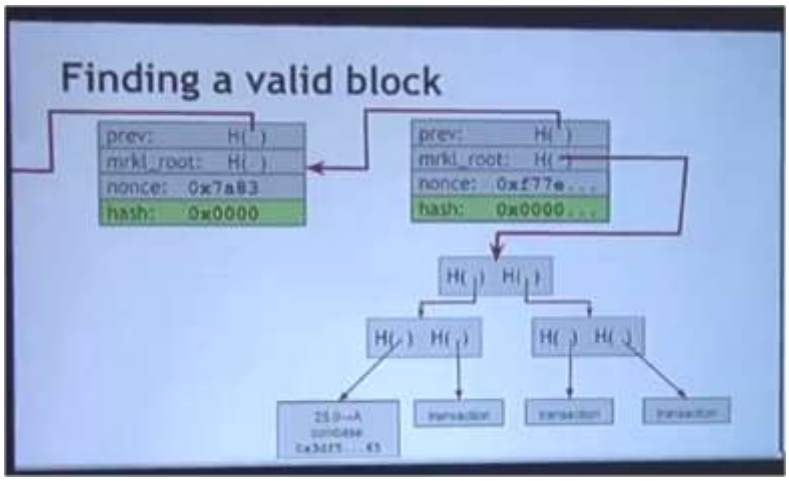
Mining serves the purpose of bringing coins into circulation, and securing and auditing the network. Bitcoins come into circulation from miners who compete to mine valid blocks (Figure 4). The blocks contain transactions which are verified to have come from users authorized to send the coins. This verification is performed using the public key cryptography scheme in which a message's sender generates a "cryptographic key pair", composed of a private key and a public key. He/ she sign the message (Bitcoins in our case) with the private key (which only he/ she knows). It can be verified that the transaction was initiated from a legitimate user that really owns the coins by using the matching public key (which is known to everyone); the public key allows anyone to verify that a message signed with the private key is valid.



a)



b)



c)

Figure 4. [19, 20]. The Mining Process

a) The miner tries a nonce of all 0s to solve a computationally consuming mathematical problem. See figure 5 below, Proof- Of-Work . It does not produce a valid hash output, so the miner would then proceed to try a different nonce.
b) Changing a nonce in the coinbase transaction propagates all the way up the Merkle tree.

c) A valid block is found and included in the block chain. The miner who finds it get incentives in Bitcoin currency around 25 Bitcoins.

The block chain is a distributed record of all the blocks containing all transactions done from the very beginning of Bitcoin to present (Figure 6). The network protects itself from malicious activity by implementing the concept of “Proof- Of- Work” (Figure 5) which is relying on the fact that it takes a certain amount of computing power to mine blocks. Therefore, to create a longer "spoof" chain than the network, which could be confirmed as valid, would require more computing power than the combined network of miners. The Bitcoin system motivates miners to continue to validate transactions and secure the system by automatically rewarding a miner who succeeds in validating a block of transaction with a certain amount of Bitcoins per a valid block (Figure 4) [14, 15, and 16].

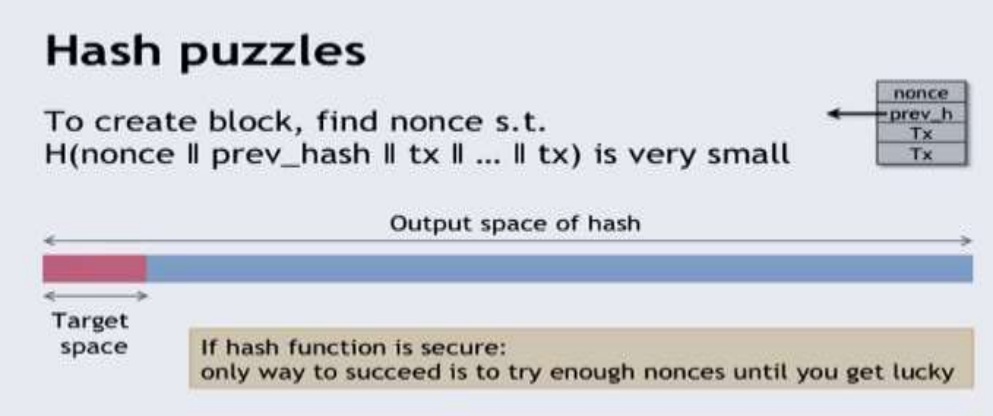


Figure 5. [19, 20]. Proof- Of-Work

It is a way to select nodes in proportion of their computing power. Let nodes to compete for rights to create blocks by solving a moderately hard hash puzzle and reward the achieving node (the miner) in Bitcoin currency.

Key security assumption here, attacks are infeasible if majority of miners weighted by hash power follow the protocol. In other words, mining following the protocol is more rewarding than attacking the network.

5.2. Preventing Inflation, Fraud, and Double Spending

A key characteristic to know about Bitcoin is that there is a limited supply of them ((Figure 7). To prevent inflation, the Bitcoin system is designed so that there will never be more than 21 billion of them. Compare that with other fiat currencies in which excess money can simply be printed by governments making the money that we own worth less. Unless rules changes, with Bitcoin that will not going to take place. Also, by design it is not possible for anyone to block you from sending or receiving Bitcoins or freezing your account (Wallet).

One solution for preventing double spending in the past was one central ledger (in a Bank, or a credit card company) that keep track of who owns what money, and any time Alice paid Bob they just update their ledger. The company or bank that held that ledger has full control over it; they can prevent fraud as well as freeze somebody’s account, sell or give private credit information to others, etc. With Bitcoin, there is no single ledger in one place, rather it is distributed in all the computers around the world that run the Bitcoin software (Figures 3, and 6), but instead of real world identities associated with the transaction, Bitcoin uses strings of numbers and letters as addresses to keep track of those transaction and to ensure the security and privacy of the System’s users at the same time [17].

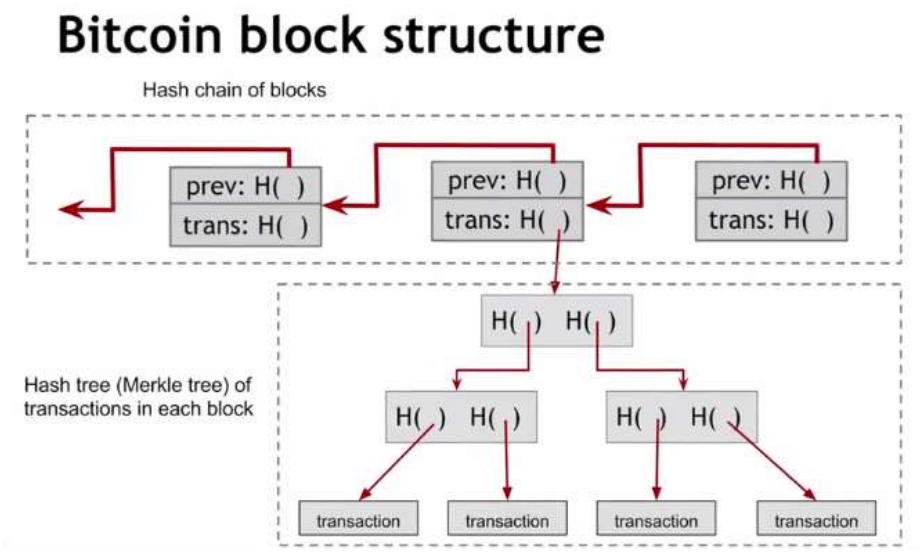


Figure 6. [19, 20]. The Block Chain

A ledger- like record that is (with some simplification) included in each node that runs the Bitcoin software following a "distributed consensus" protocol; each transaction that ever happened is there. Designed this way to prevent double spending without needing a central authority.

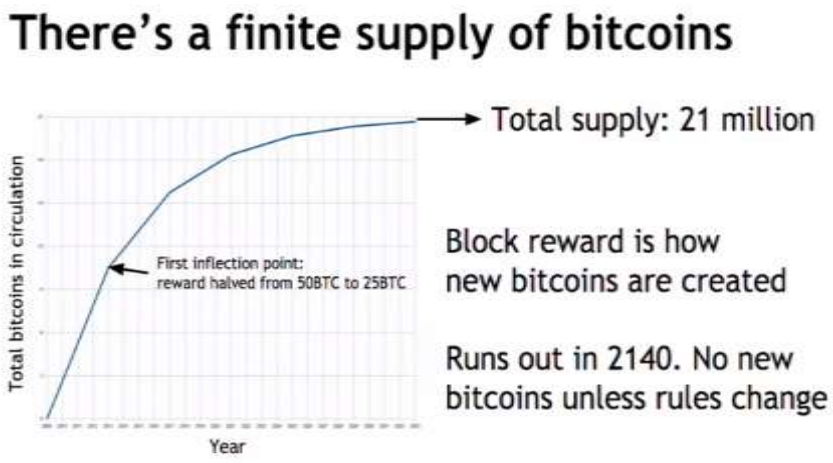


Figure 7 [19, 20]. Preventing Inflation- Finite Supply of Bitcoins

6. Conclusion

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third party to process electronic payments. Some will argue that the system works well enough for most transactions, but it still suffers from the inherent weaknesses of the trust based model [11]. An ethical failure has been observed within the financial industry including banks. In order to obtain easy short- terms profit, banks lent the money for people who could not possibly pay it back. Neither careful background check nor legal and repayment conditions have been studied. That resulted in the collapse of the mortgage market and has been one of the major causes of the recent global financial crisis. Considering banks as a trusted third- party is no more the only option, at least at the online economy. Bitcoin is a virtual currency scheme based on a peer-to-peer network. It does not require a central authority in charge of money supply, nor are financial

institutions involved in the transactions. All these tasks are performed by the users themselves. Its exchange rate with respect to other currencies is determined by supply and demand and several exchange platforms exist [12].

References

[1] J. Rickards, "Currency Wars: The Making of the Next Global Crisis", a book published by the Penguin Group, **(2011)**.
[2] CNBC News Network, "What Happened: Explore the timeline", 5, Sept, 2012, https://www.cnbc.com/id/100001231, last retrieved 12, August, 2017.
[3] Securities Industry and Financial Markets Association (SIFMA), "Investor's Guide: Mortgage-backed securities (MBS) and collateralized mortgage obligations (CMOs)", 2010, https://www.fidelity.com/static/dcle/learning-center/documents/MBS-CMOs.pdf, last retrieved 12, August, 2017.
[4] "US Securities and Exchange Commission, "Mortgage-Backed Securities, https://www.sec.gov/fast-answers/answersmortgagesecuritieshtm.html, last retrieved 12, August, 2017.
[5] E.L. Andrews, "My personal Credit Crisis", The New york times newspaper, 17, May , 2009, http://www.nytimes.com/2009/05/17/magazine/17foreclosure-t.html, last retrieved 12, August, 2017.
[6] D.M. Figart, "Book Review: Busted, Life inside the great mortgage meltdown by Edmund L. Andrews", Journal of Financial Counseling and Planning, https://afcpe.org/assets/pdf/volume_21_issue_1/bookreview_figart.pdf, last retrieved 12, August, 2017, vol. 21, Issue 1, **(2010)**.
[7] J. Silver, "The Next Meltdown: Credit-Card Debt", Bloomberg BusinessWeek, Oct., 8, 2008 https://www.bloomberg.com/news/articles/2008-10-08/the-next-meltdown-credit-card-debt, last retrieved 12, August, 2017.
[8] A. Gomstyn and Abc News Business Unit, "Credit Cards: The Next Financial Crisis", ABC NEWS, July 25, 2008, http://abcnews.go.com/Business/Economy/story?id=5444545, last retrieved 12, August, 2017.
[9] A. Huffington, "The Credit Card Debt Crisis: The Next Economic Domino", HUFFPOST, February 24, 2009, updated May 25, 2011, http://www.huffingtonpost.com/arianna-huffington/the-credit-card-debt-cris_b_169657.html, last retrieved 12, August, 2017.
[10] G. Curtis, "The Financial Crisis and the Collapse of Ethical Behavior", a white paper published by Greycourt & Co. Inc.,2008, http://transformgov.org/en/knowledge_network/documents/kn/document/301680/financial_crisis_and_the_collapse_of_ethical_behavior_white_paper, last retrieved 12, August, 2017.
[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Bitcoin.org, https://bitcoin.org/bitcoin.pdf, last retrieved 12, August, 2017.
[12] European central bank publication, "Virtual currency schemes", October, 2012, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, last retrieved 12, August, 2017.
[13] Bitcoin Wiki, https://en.bitcoin.it/wiki/Main_Page, last retrieved 12, August, 2017.
[14] R. A. Glantz, "Pantera Primer", Pantera Capital, March 11th, 2014, https://cdn.panteracapital.com/wp-content/uploads/43517996c44ec1d3372ed7eb0a6138bd-pantera.primer.03.2014-af.pdf, last retrieved 12, August, 2017.
[15] B. Segendorf, "What is Bitcoin?", Sveriges Riskbank Economic Review, 2014, http://www.riksbank.se/Documents/Rapporter/POV/2014/2014_2/rap_pov_artikel_4_1400918_eng.pdf, last retrieved 12, August, 2017.
[16] M. E. Peck, "The Cryptographic Answer to Cash: How Bitcoin Brought Privacy to Electronic Transactions", IEEE Spectrum, **(2012)**.
[17] R. Ver, "Bitcoin 101 for Businesses", a talk at Bitcoin 2013 conference, Canada, **(2013)**.
[18] T. Harford, "The Undercover Economist", Oxford University Press, **(2006)**.
[19] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies", Draft- February, 2016; available online https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf, **(2016)**.
[20] A. Narayanan, "Bitcoin and Cryptocurrency Technologies", Princeton University, Online course via Coursera https://www.coursera.org/learn/cryptocurrency/home/welcome.

