International Journal of Engineering & Technology, 7 (4.25) (2018) 262-266

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

The Emergence in Mining Technology of Digital Gold: Ambiguity Surrounded in the Bitcoin System

Abhishek Gupta[1], Biswajit Das[2], Bhubaneswari Bisoyi[3]

[1]Research Scholar, KIIT University, Bhubaneswar, India. email: abhishek7422@gmail.com
[2]Professor, School of Management, KIIT University, Bhubaneswar, India. email: biswajit@ksom.ac.in
[3]Assistant Professor, Sri Sri University, Bhubaneswar, India. email: bhubaneswari.bisoyi@gmail.com

Abstract

This article is based on the revolutionary development in the year 2008 by Satoshi Nakamoto was of a *"Peer to peer Electronic cash system".* The purpose of this paper is to analyze research surrounding the anonymity of online transactions using cryptocurrencies and report on the feasibility that does not have a regulatory body. This article takes the wheel around the journey of an unknown secondary invention which emerged as the digital gold across the globe and works as the digital barter system, a stepping stone towards the cashless world. The success wing of the invention was the decentralized mechanism to operate a digital cash system that restricts and checks double payment. Unlike in centralized server system, in the decentralised network, every nod in the network ensures and achieves absolute consensus. Crypto-currencies being unique and volatile are the most talked, researched, observed topic of the past few years. It is no less than an ocean of opportunities which works differently for different set of people. Crypto currencies functionalities and trade revolve around the internet based global markets. The design of the paper follows on from the approach taken by Reid and Harrigan, 2013 in determining whether the transactions made need to be detected and should have an option of rectifying the errors after knowing the peer or the location of the dealer or investor. By doing so, this research tests the interest of the investor and how much an individual will rely on such online mining of currency. Additionally, this will create an atmosphere which can extradite fraudulent or illegitimate transactions.

Keywords: *Bitcoin, Crypto currency, Digital Currency, Ethereum, Litecoin.*

1. Introduction

Crypto-currencies being a major global advancement which is known to most of the people is still not understood and adopted by many big players in the market. The volatility and vulnerability associated with the endless growth opportunities provided by crypto-currencies have made it the most researched topic for every department may it be scientists, banks or government regulatory or big IT companies or consultants [1], [4], [5].

Crypto-currencies work on an absolute consensus model. Every peer in a decentralized network maintains a complete record of every single small or big transaction. Such records being cross-checked and updated with other peers tend to validate and restricts double spending. The result is that there would be an immediate shutdown or breakdown if any single node failed to agree with other nodes on the network i.e they do not achieve consensus[4],[5],[6]. These transactions gain security with the use of cryptography which also controls the creation of additional coins/tokens of different currencies. Crypto-currencies often called as virtual currencies have emerged as digital currencies or alternative currencies. Bitcoin, which emerged as the first and till date most popular crypto-currency, uses decentralized control. The technology adopted by bitcoin for the recording of transactions in the ledger is called Blockchain. It maintains records in chronological order when achieves consensus. The distributed ledger enables to perform decentralized control over the use of bitcoins. Cryptocurrency wing has more than 1000 members in its family and has derived similarity from the parent cryptocurrencies i.e. Bitcoin being the first in the family.

2. Mining

Cryptocurrency is all about confirmation. Till the transactions are not confirmed they can be altered and forged at any given point of time. And once the transactions are confirmed there are irreversible. Even the minor who can confirm the transactions cannot reverse them. Only minors can confirm transactions in the blockchain[10],[13],[14]. They are the members of the general public who validate and record transactions with the use of their computers. They play the vital role to ensure security integrity and consensus of balance across each peer on the network. The system would shut down in no time if numerous peers are created and transactions are forged. Since everyone can be a minor and there is a lack of central authority to delegate such task, there emerged a need for a system to prevent and control abuse of transactions[8], [9], [23]. Henceforth, miners need to have a specialized hardware installed on their computers to qualify for mining. Mining can also be done through various exchanges and services. Mining is a very tricky task to perform but very easy to verify. They ought to find a hash being a product of a cryptographic function that connects the successor and predecessor block. Bitcoin uses a secure hash function SHA-256 for mining coins[23,26,29].

In Bitcoin mining, a lottery system is used to reward the miner to add a block to the blockchain based on some probability. Such miner acts as a trusted third party to confirm the transactions. Each winner of the lottery system receives a certain amount of bitcoins as a reward which also includes transaction fees. This motivates miners to add more number of blocks to blockchain to multiply their rewards[18,19].

3. Crypto currency Market – An Overview

Currently, Cryptocurrencies are traded in 4046 markets. The Cryptocurrency market is growing at a tremendous speed, where its market capitalization is expected to reach around 110 Billion. The top trading cryptocurrencies are Bitcoin, Ethereum, Ripple, Litecoin, and Monero. These currencies are widely accepted and also traded as an alternative to physical currencies. These currencies are traded across the globe in 24*7 exchanges. No exchanges are made through legal channels or platforms; still, they see high volumes of trading[30,32,33].

These exchanges allow to mix and trade among various other currencies, intra/ inter cryptocurrency, which can be easily bought, sold or traded. The most unique feature of exchanges is it offers the widely traded currencies [26]. They may differ in their trading numbers, bid-ask proportions. The trading charges depend on the location or from which part of the world it is being traded. One of the crucial aspects lies in the format of the market it is being traded in. It does not have an organized market or regulatory body, where Government plays its role. So the Crypto-currencies hold the current market value as deemed by the market & is converted into local currency [35]. Hence, being unregulated, there are no authorities and no legal framework protecting the value. It is also believed that if Cryptocurrency is also regulated like fiat Currencies, that it may lose its charm & value. Keeping belief in such transactions and currency is a major challenge along with cyber risks[15].

3.1 Properties

Transactional properties

1.) Irreversible: Cryptography doesn't allow reversal of the transaction. Not even the First man i.e. the President of the United States is also not allowed to diverge or alter the transaction. The Criteria to deal with it is with utmost sincerity. If any transaction is wrongly posted it does not allow reconciling the transactions like in Bank or any other financial institutions [7].

2.) Pseudonymous: Real-world identities have no link between the transactions or operational address. 30 characters which are placed in a random chain like structure are delivered to the address. If one tries than can find the transactional flow stats but cannot identify the real address of the dealers [14].

3.) Fast and global: Transactions are immediately shown in the order chart without taking much time. These transactions allow you to be part of the massive global network. It gives the ease to transact with either a person next door or million miles away.

4.) Secure: The backbone of cryptography is the use of public and private key to encrypt and decrypt data. Cryptocurrencies are put to the world with public keys and are kept secured with the respective private key of the owner of coins.

5.) No Central Authority: Either this is a drawback or a merit. There is no Authorized body or organization from where one has to take approval to start the crypto-currency transactions. One simply needs to download the app and start buying & selling of crypto-currencies.

4. Bitcoin

Among the entire industry of cryptocurrency Bitcoin is first and till date most popular. It is often called the digital gold amongst all. It functions and operates by a computer program called blockchain [32], [33], [39].

The blockchain is a set of codes and instructions and has a separate decentralized ledger system. Every cryptocurrency has its own blockchain to record each and every transaction. The figure.1 explains the dealer (A) setup a Bitcoin account and in doing so provides identifying data to exchange and enables the ability to transact with other users. These programs are independent and even the creators of such programs cannot control them. Bitcoins are installed on multimillion networks across the globe. They need to achieve consensus on changes in the blockchain network. Being an open source network anyone who satisfy specific conditions can edit modify and improve the program but however cannot control it.

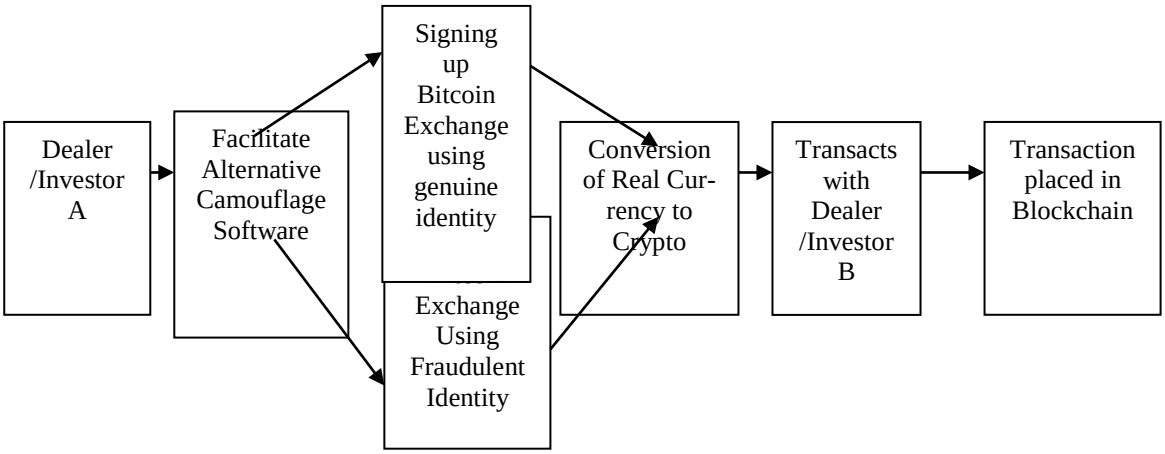

Figure 1: Example of a Bitcoin transaction , Source [23]

Therefore to achieve consensus is utmost important in the decentralised network. Each peer on the network must be in confirmation with others to achieve consensus.

4.1 Bitcoin and Bitcoin Cash

Despite the massive success rate of Bitcoin, its low scalability is a true concern. Its core problem is scalability and slow verification process. Bitcoin works with the latest technology of ledger recording i.e. blockchain and being decentralized allows it to be democratic in its operations. However, the technology it works on is slow to a great extent. Each transaction in the bitcoin blockchain takes nearly 10 minutes to process. With the ever-increasing network of its users, the waiting time will further increase to an unacceptable rate. Therefore, to make the transactions faster either the data to be verified can be squeezed or the blocks storing and processing the data can be magnified [22], [25], [28].

Bitcoin Cash was created as a solution to scalability problem of Bitcoin. It came as an answer to the stretched discussions to scale Bitcoin to more users. Bitcoin Cash has increased the Block size limit which thereby supporting high scalability.

The Bitcoins block size is at one megabyte that allows 250000 transactions per day. Whereas, Bitcoin Cash block size is 8 megabyte that allows processing of two million transactions each day. Bitcoin Cash offers low fees and speedy rate of transaction thereby giving a challenge to the massive network and infrastructure of

Bitcoin which sets back due to higher fees and long waiting time. The development or alteration of Bitcoin Cash was quite simple due to the same codes shared by Bitcoin [27], [28].

4.2 Solutions to Achieve Scalability

Sidechains and State channels are two solutions associated with blockchain technology that helps to work on scalability issues. As the name suggests Sidechains are additional blockchains that are attached to the main blockchain with the use of a two-way peg. It works as a bridge through which assets can be transferred between two blockchains. Once created, they become permanent and never close down. Another solution to poor scalability is the use of state channels that help participants to interact off a blockchain without a significant increase in the risk of exposure [19]. The privacy is better in case of these as compared to sidechains as all the transactions take over the state channels except the opening and closing transactions. However, sidechains availability is better as they are available even when participants involved are absent. It updates through state channels and confirms transactions once agreed between parties and make the implementation process faster and convenient [35,39].

5. Ethereum

The rising star who holds the second place in the legacy of cryptocurrencies is the Ethereum. It was first described by young and enthusiastic 19-year-old programmer Vitalik Buterin in the year 2013. Ethereum has its own blockchain which not only validates its set of transactions and balances but it also processes complex contracts and programs. A group of smart contracts can be written on ethereum blockchain. Ethereum can be used to create applications for numerous services. Every centralized service can be converted into decentralized service with the help of ethereum. Ethereum can also build Decentralised Autonomous Organisation (DAO) [27, 29, 32]. It can be owned by everyone who has the token which gives the voting rights and builds the programming code for industries as per their requirement to replace/alter the set of traditional rules. It helps to eliminate the need for central processing and control. However, after the hack of DAO emerged different child of Ethereum among which Ethereum Classic is most popular. Therefore Ethereum in itself can be said to be a family of cryptocurrencies [35,37]. Ethereum is young in the family of cryptocurrencies being launched in 2015 yet has seen the highs and lows of prices to a great extent. Started with $10 per coin and hitting $1400 in January 2018 and then a downfall by $1000 and currently sailing at around $450, Ethereum has seen it all. The total value of all the ether coins in circulation as of February 2018 was $88 billion against the $143 billion value of all the Bitcoins [20].

6. Ethereum and Bitcoin

The popularity of young Ethereum can be credited to its continuous comparison with Bitcoin, the first virtual currency. Ethereum allows faster transaction time i.e. the block time taken by it is around 15 seconds which is much faster when compared to Bitcoins block time of 10 minutes. They also differ in their respective programming language. Ethereum uses Turning complete and Bitcoin uses stack-based language. The basic build of Ethereum uses ethash and Bitcoin uses secure hash algorithm SHA-256. However, both work on the technology of Blockchain but differ in their respective purpose. Ethereum is much more than a currency as it allows third-party transactions to enable developers to build and run distributed applications. Also, its network is used by start-ups to raise money with initial coin offerings that exchange ether and/or other currencies to access services [12],[14],[19].

7. Litecoin

Often called the digital silver, Litecoin was one of the first crypto-currencies after Bitcoin. As the name suggests Lite coin was far lighter in its coding format and gave emergence to several other cryptocurrencies with the same codings such as Dogecoin or Feathercoin. Its functionality is much faster than bitcoin and has a large amount of tokens with new mining algorithms. While Litecoin failed to find a real use case and lost its second place after bitcoin, it is still actively developed and traded and is hoarded as a backup if Bitcoin fails [15], [17], [20].

8. Cryptojacking

Recently there has been a shift in cybercrime from ransom ware to crypto-jacking. Crypto-jacking is more attractive for hackers because of rewarding money involved as against the minimal risk. Crypto-jacking is the latest cyber security threat as there is an alarming increase in the attacks by approximately 8500% in the year 2017 as presented below in Figure 2 [31].

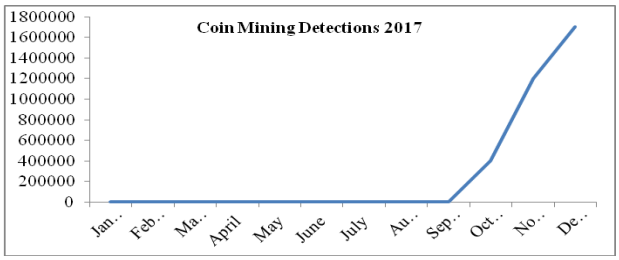

Figure 2: Coin mining in the year 2017, Source [31]

9. Operation of Cryptojacking

Under cryptojacking, victim's computer power is secretively used by web attackers to mine cryptocurrencies. Cryptojacking often called as coin-mining neither involves installation of any kind of software program in targeted computer nor steals or destroys any kind of data or information. It simply hijacks the computing device to perform the mining and updating of varied cryptocurrencies. This results in generation of new coins and fees for undertaking mining process which is deposited in the hackers wallet and the cost related to computing is seldom borne by victims account [22], [28], [32].

Also, cryptojacking can be done by using web browsers that often uses Java Script which runs in almost every webpage. As the targeted computer's hardware is exploited for computing it faces frequent slow down or shut down during processing.

9.1 Prevent Against Cryptojacking

•The initial signs of cryptojacking are similar to that of phishing. Getting trained about these signals might help when technical support fails [23].

•Cryptojacking scripts often take a seat through webpages, therefore effective means of ad-blocking can restrict such crime to an extent [25].

•Installation of anti-viruses to provide end-point protection from coin minors which enables the detection of coin mining. However the constant change and updating in techniques are real challenge for validity of such anti viruses.

•Blocking the users from accessing webpages that support or deliver cryptojacking scripts.

•Adopt a mobile device management (MDM) solution to monitor and control Bring Your Own Device (BYOD) policies. They often help larger enterprises to manage apps and extensions on users devices and prevent unethical coin mining at user desk [40].

•Look for initial signs of cryptojacking such as slow processing, frequent shut downs, over heating of system.
•Enterprises with network monitoring solutions can find it helpful and easier to detect cryptojacking as they tend to review complete web traffic.

10. Conclusion

Cryptocurrencies have taken a step forward on how traditional financial system operates. In no time it has become the global financial alternative. The volatility associated with these currencies has yet a bigger portion of the untapped market. There is high risk in trading these currencies as the prices tend to get extremely volatile, that attract a wide range of speculators as well. Due to the new technologies, it is yet not well understood by many big players in the market. After it gains the required faith and addresses security concerns, its market size will multiply the number of times. If it fails to achieve the trust then they might see a decline. There are 1000s varieties of cryptocurrency as of now, however, the most popular ones can together transform the economic and financial reforms. We are here yet to see a lot of advancements and achievements in the whole new world of cryptocurrencies that will shift the global financial landscape [24], [39].

As the emerging cryptocurrencies and blockchain technology has rigorously tapped the global marketplace; organizations that adopt themselves to the changing scenario of financial culture may gain the advantage of early risers. Also, those who leverage these innovative technologies shall encounter an increase in regulatory intervention in upcoming years.

However, market is witnessing a short supply of personnel for leadership roles to adopt and ensure compliance of emerging rules, regulations and legislations. In the era of global professional market challenges are difficult to address due to ever changing technologies and geographic ramifications. Therefore with limited human capital available on latest technologies, talent will migrate to early adopting markets, nations and organisations where their skills are valued and are allowed autonomy to an extent in operations. Major global consulting firms, private equity investors and venture capital investors shall prefer to hire talent from adjacent markets instead of untested personnel from less regulated markets.

Digital currencies are yet not stable enough to keep as long term assets. Current economic system and some internal challenges related to technology and security are major challenges for crypto currencies. In order to replace completely the existing currency system, these digital currencies first need to address some substantial and core challenges.

References

[1] Ajtai, M. (1996), "Generating hard instances of lattice problems", Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of computing, ACM, Philadelphia, PA, pp. 99-108.

[2] Bisoyi, B. and Das, B. (2017). Organic Farming: A Sustainable Environmental Ingenuity for Biotechnological Intervention towards a Green World. International Journal of Innovative Research in Science, Engineering and Technology, 6(9), pp.179-186

[3] Bisoyi, B. and Das, B. (2015). Adapting green technology for optimal deployment of renewable energy resources and green power for future sustainability, Indian Journal of Science & Technology, 8 (28), pp.1-6.

[4] Bisoyi, B. and Das, B. (2015). Necessitate green environment for sustainable computing" published in Advances in Intelligent Systems and Computing, Advances in Intelligent Systems and Computing, Volume: 380, pp. 514-524.

[5] Bisoyi, B. and Das, B. (2018). Green technology for attaining environmental safety and sustainable development, International Journal of Mechanical Engineering and Technology (IJMET) Volume 9, Issue 3, March 2018, pp. 1087 – 1094

[6] Bisoyi, B. and Das, B.(2015). Development in the Field Of Technology for Cooperative Problem Solving Utilizing Nonconventional Energy Resources in India &Future Trend, International Journal of Scientific Research And Management, 3(1), pp.2321-3418.

[7] Bank, European Central. (2015). Virtual currency schemes– a further analysis. Frankfurt, Germany: European Central Bank.

[8] Bradshaw, D. (2015). NYU Stern broadens impact of Bitcoin expertise. Financial Times.

[9] BTCManager. (2016, 10 15). Ethereum continues to be exploited. Retrieved from BTC Manager: https://btcmanager.com/news/tech/ethereum-continues-to-beexploited-another-hard-fork/

[10] Buterin, V. (2013), "A next generation smart contract and decentralized application platform", available at: www.theblockchain.com/docs/Ethereum-white-paper-a-nextgeneration-smart-contract-and-decentralized-application-platform-vitalik buterin.pdf [Google Scholar]

[11] Buterin, V. (2016a), "Critical update re: DAO vulnerability", available at: https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/ Buterin, V. (2016b), "Hard fork completed", available at: https://blog.ethereum.org/2016/07/20/hard-fork-completed/

[12] Caffyn, G. (2015, August 21). What is the Bitcoin Block Size Debate and Why Does it Matter? Retrieved from Coindesk:http://www.coindesk.com/what-is-the-bitcoinblock-size-debate-and-whydoes-it-matter/

[13] Chen, A. B. (n.d.). Bitcoin: Technical Background and Data Analysis. Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board, Washington, D.C.

[14] S. Rohini, M. Sharanya, A. Vidhya, S. Viji and P. Poornima. "Proximity Coupled Microstrip Antenna for Bluetooth, WIMAX and WLAN Applications ." International Journal of Communication and Computer Technologies 5 (2017), 48-52.

[15] Damgård, I. and Jurik, M. (2001), "A generalisation, a simplification and some applications of paillier probabilistic public-key system", in Kim, K. (Ed.), Public Key Cryptography, Lecture Notes in Computer Science, Springer, Berlin, Vol. 1992, doi: https://doi.org/10.1007/3-540-44586-2_9. [Crossref], [Google Scholar]

[16] Delmolino, K., Arnett, M., Kosba, A., Miller, A. and Shi, E. (2015), "Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab", available at: https://eprint.iacr.org/2015/460.pdf

[17] Diaz, C. D. (2015, December 17). Who controls Ethereum? The relationship between Ethereum and ConsenSys:a mystery that matters. Retrieved from Medium.com:https://medium.com/@celeduc/who-controls ethereum94fcb4aa3a50#.xodo2v329

[18] Douceur, J.R. (2002), "The Sybil attack", Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS-2002), Lecture Notes in Computer Science, Springer-Verlag, Berlin, Vol. 2429, pp. 251-260.

[19] Ethereum, F. (2016), "Introduction to smart contracts", available at: https://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html

[20] Eyal, I. and Sirer, E.G. (2014), "It's time for a hard bitcoin fork", available at: http://hackingdistributed.com/p/2014/06/13/in-ghash-bitcoin-trusts/

[21] Fischer, M.J., Lynch, N.A. and Paterson, M.S. (1983), "Impossibility of distributed consensus with one faulty process", Proceedings of the 2nd ACM SIGACT645 SIGMOD Symposium on Principles of Database Systems, Association of Computing Machinery, New York, NY.

[22] Gentry, C. (2009), "A fully homomorphic encryption scheme", Ph.D. dissertation thesis, Standford University, Standford.

[23] Gentry, C., Sahai, A. and Waters, B. (2013), "Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based", Cryptology ePrint Archive, Report 2013/340.

[24] Dahiya, V. A Survey on Educational Data Mining.

[25] Gervais, A., Karame, G.O., Wst, K., Glykantzis, V., Ritzdorf, H. and Capkun, S. (2016), "On the security and performance of proof of work blockchains", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS-2016), Association of Computing Machinery, New York, NY, pp. 3-16.

[26] Goodin, D. (2014), "Bitcoin security guarantee shattered by anonymous miner with 51% network power", available at:

https://arstechnica.com/security/2014/06/bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/
[27] Gupta, M. (2017), Blockchain for Dummies, IBM Limited Edition, John Wiley and Sons, Hoboken, NJ, available at: https://public.dhe.ibm.com/common/ssi/ecm/xi/en/xim12354usen/
[28] Hayes, A. (2015). What factors give cryptocurrencies their value: An empirical analysis. New York: The New School for Social Research.
[29] Hyperledger, F. (2017), "Hyperledger: Linux foundation projects", available at: www.hyperledger.org/
[30] Margaret Harwood-Jones (2016), Blockchain and T2S: A potential disruptor, Beyond Borders Report, SCB https://www.sc.com/BeyondBorders/blockchain-mass-adoption/
[31] McGrath, R. (2016, July 21). Cryptocurrency Governance Processes: A Master Class. Retrieved from Robert McGrath's Blog: https://robertmcgrath.wordpress.com/2016/07/21/cryptocurrencygovernance- processesa-master-class/
[32] Nakamoto, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.
[33] Reid, F. and Harrigan, M. (2013), "An analysis of the anonymity in the Bitcoin system", in Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N. and Pentland, A. (Eds), Security and Privacy in Social Networks, Springer, New York, NY.
[34] Sid Kalla and Matt Chwierut (2017, Jan 8), 2016- Year Blockchain ICO's disrupted Venture Capital, Coindesk Report. https://www.coindesk.com/2016-ico-blockchainreplace-traditional-vc/
[35] Stallings, W. and Brown, L. (2015), Computer Security: Principles and Practice, 3rd ed., Pearson Education, London.
[36] Szabo, N. (1997), "Formalizing and securing relationships on public networks", First Monday, Vol. 2 No. 9Todd, P. (2016, June 21). Will The Cryptocurrency Industry Figure Out Governance? Retrieved from Velocity Blog:http://blog.velocity.technology/cryptocurrencygovernance/
[37] Velner, Y., Teutsch, J. and and Luu, L. (2017), "Smart contracts make bitcoin mining pools vulnerable", available at: https://eprint.iacr.org/2017/230.pdf Walch, A. (2017), "Should public blockchains serve as financial market infrastructures?", Handbook of Digital Banking and Internet Finance, Elsevier, Amsterdam, Vol. 2, available at: https://ssrn.com/abstract=2879239
[38] Wood, G. (2016), "Ethereum: a secure decentralised generalised transaction ledger", available at: http://gavwood.com/paper.pdf
[39] Wüst, K. and Gervais, A. (2016), "Ethereum eclipse attacks", ETH Library, available at: http://e-collection.library.ethz.ch/eserv/eth:49728/709eth-49728-01.pdf
[40] Yarvin, C., Monk, P., Dyudin, A. and Pasco, R. (2016), "Urbit: a solid-state interpreter", available at: www.urbit.org
[41] Yermack, D. (2013). Is Bitcoin a Real Currency? New York: New York University Stern School of Business.