International Journal of Engineering &Technology, 7 (3.12) (2018) 296-299

International Journal of Engineering & Technology

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

Research paper

Survey on Surging Technology: Cryptocurrency

Swathi Singh[1], Suguna R[2], Divya Satish[3], Ranjith Kumar MV[4]

[1]Research Scholar, [2, 3]Professor, [4]Assistant Professor
[1,2,3,4]Department of Computer Science and Engineering, [1,3]SKR Engineering College, Chennai, India,
[2]Vel Tech Rangarajan Dr.Sagunthala Institute of Science and Technology, Chennai, India
[4]SRM Institute of Science and Technology, Kattankulathur, Chennai.
**Corresponding Author Email: [1]vk.swathisingh@gmail.com*

Abstract

The paper gives an insight on cryptography within digital money used in electronic commerce. The combination of digital currencies with cryptography is named as *cryptocurrencies* or *cryptocoins*. Though this technique came into existence years ago, it is bound to have a great future due to its flexibility and very less or nil transaction costs. The concept of cryptocurrency is not new in digital world and is already gaining subtle importance in electronic commerce market. This technology can bring down various risks that may have occurred in usage of physical currencies. The transaction of cryptocurrencies are protected with strong cryptographic hash functions that ensure the safe sending and receiving of assets within the transaction chain or blockchain in a Peer-to-Peer network. The paper discusses the merits and demerits of this technology with a wide range of applications that use cryptocurrency.

Index Terms: *Blockchain, Cryptocurrency.*

1. Introduction

The concept of cryptocurrency alias cyber currency or virtual currency came into existence by 2009. This was the period when electronic commerce was already growing vast with electronic payment and POS systems to enhance feasibility. An engineer named Satoshi Nakamoto introduced the very first usable cryptocurrency in the form of Bitcoin [1]. Later then, many other cryptocurrencies were introduced with underlying Bitcoin protocol. However, none of them gained popularity as Bitcoin. This cryptocurrency holds a decent position in electronic commerce market competing with other cryptocurrencies despite of less advancement over the existing protocol.
The earlier versions of electronic cash or digital money used trust-based model for spending money through a protocol that can be easily hacked or broken. The replacement of trust-based model led to the concept of cryptocurrency that involves a secure payment system implemented in peer-to-peer environment without an intermediary[4,6,7,9,15]. The removal of an intermediary for authenticating transactions resulted in very low transactions costs.

2. Bitcoin

The first cryptocurrency that came into existence was Bitcoin published in 2008 and implemented as open-source software in 2009 by a Japanese engineer named Satoshi Nakamoto. The speculations on identity of Satoshi Nakamoto had been high since the invention. Few people denote this name as a team of developers while others consider it as a pseudonym of an

unidentified software developer.

However, the first implementation of Bitcoin protocol routed many other cryptocurrencies to exist. Bitcoin is a self-regulatory system that is not supported by government or any organization. It does not have a central authority and hence is a decentralized payment system that enables transactions between two parties restricting the need of a third party or an intermediary to authenticate the transactions [8]. The transactions take place in peer-to-peer environment and trusted nodes in the peer network verify these transactions.
The transactions that take place within this payment system are recorded in a public ledger called Blockchain. The identity of the users sending or receiving electronic cash is anonymous.

A. Blockchain

The transactions within the Bitcoin payment system are recorded in a Blockchain. It is similar to a public ledger. All the transactions are held publically but none of the user's identity is revealed. In this way the property of anonymity is maintained throughout the transaction. For a better understanding of blockchain concept, consider a person *X* sending *Y* amount of electronic cash or bitcoins to person *Z* [11]. The blockchain records transaction details of *Y* amount only. It doesn't reveal the name or other details of the payee and the payer. In simpler terms, blockchain can be denoted as a database of bitcoins.

B. Cryptocurrency Mining

Mining of cryptocurrencies are done on a computer, capable of generating 'n' cryptographic hashes per second for every unique bitcoin transaction. The computers mining bitcoins are powerful and their processing units consume a lot of resources.
The use of more resources ensures effective and secured

cryptocurrency mining[17].
The complexity of mining increases with the increase in supply of bitcoins. The estimated supply of bitcoins is 21 million. At present, more than 13 million bitcoins are in circulation each comprising market value upto 4,58,621.27 in Indian Rupees.

C. Technical Background

The bitcoin system uses SHA – 256 cryptographic algorithm or system to provide security within the blockchain. Each bitcoin is a combination of private keys and public address. The private or secret keys are stored in a virtual wallet or bitcoin wallet and can range from 32-bit to 51-bit. The range of secret keys is dynamic [17]. These keys can be a combination of alphabets and numbers. The key size varies depending on the complexity of the algorithm. The public address is also named as bitcoin address and is a unique identifier for every bitcoin owner. The mean block time is about 10 minutes[17].

3. Cryptocurrency Classification

The existing virtual currencies or cryptocurrencies can be classified as the original cryptocoins bitcoins and altcoins. The similarity between these two classifications is the use of common protocol or similar technology but with varying versions[24]. The classification differs by means of key generation, blockchain size, number of cryptocoins to be mined for a user or the use of security prototype depending on the severity of usage. The cryptocurrencies that are created or mined, by default, use a part or whole of bitcoin protocol with certain amendments [2].
Many cryptocoins exist with bitcoin being the predominantly original cryptocoin. All other cryptocurrencies are named as altcoins or alternative cryptocoins. The altcoins include but are not limited to the following - Litecoin, Feathercoin, Zerocoin, Namecoin, Blackcoin, Dogecoin, Ethereum, Mastercoin, Peercoin, Potcoin, Primecoin, Bytecoin, Huntercoin, Darkcoin, Zetacoin, Novacoin, Digitalcoin, Stablecoin, Quarkcoin etc [16,22].

A. Underlying Mechanization

The cryptocoins are an assembly of hash algorithms and timestamping mechanism. Every cryptocurrency has its own set of embedded algorithms over a common or uncommon protocol. Few hash algorithms that can be listed are SHA – 256 algorithm, Scrypt algorithm, Cryptonight or a combination of any of these to form a stronger set of automated cryptocoins [2]. The mean block time is about 10 minutes. The total hashing rate of the bitcoin network is over 20,000 terra hashes per second. The time stamping strategies that are dedicated towards mining these virtual currencies include Proof-Of-Work, Proof-Of-Stake or Consensus methods. The first paper on cryptocurrency introduced the use of SHA – 256 hash algorithm with Proof-Of-Work time stamping strategy [22].
The bitcoin exactly follows the combination of these two mechanisms and is estimated to mine atleast 21 million bitcoins. The fear of depleting bitcoins has ultimately led to amendments of the existing protocol to create various altcoins
that can replace the bitcoins [3].
Comparatively, the fundamental cryptocoin continues to rule the virtual, automated world with its capability to override double-spending attack and protect the blockchain from being hacked [5]. The fraudulent attacks can be prevented to a larger extent by implementing a complex and strong hash algorithm. It can also be stated as heart of the bitcoin protocol [22].

B. Mining Pools

The mining of cryptocoins is done through mining pools. A mining pool can be defined as a set or group of dedicated volunteers meant only for mining cryptocurrencies and are usually independent of time or power [7,10]. A single computer could take minimum of 24 hours to mine a single bitcoin. Such an outcome may result in over-consumption of energy, power or money. The mining pools strive to combine the power consumption of systems owned by various individuals such as to produce and mine more cryptocoins using comparatively less resources[26,27].
The mining pools ensure the availability of bitcoins and other altcoins at customer's discretion. The volunteers involved in pooling procedure are rewarded considerably after every transaction. The payments are small but steady ensuring lump sum payment elimination and fair pay.

4. Altcoins

The altcoins can be considered as the enhancement of bitcoin in terms of security, mining speed and availability. Various altcoins exist and all of them might not be listed here. Many altcoins were a failure but few of them managed to gain limelight and succeeded their predecessor by means of different technical parameters. The highlight of these altcoins is they are very cheap compared to that of the original cryptocoin – bitcoin. There are many such cryptocoins that cost less than a dollar and provide enhanced security, reliability and availability.

A. Litecoin

The second most successful cryptocurrency is the Litecoin. Former Google engineer, Charles Lee, introduced it in October 2011 [25]. It is also named as the memory-intensive cryptocoin. The total number of cryptocoins that can be mined is estimated to be 84 million. It can also be mentioned as cheaper version of bitcoins. The major difference between litecoin and bitcoin is the use of hash algorithm. The bitcoin used SHA – 256 hash algorithm whereas the Litecoin uses Scyrpt hash algorithm to enable faster yet secured mining mechanism. The algorithm benefits the altcoin to provide a mean block time of 2.5 minutes. These cryptocoins were the first to launch a successful Scrypt-based cryptocurrency strategy. The algorithm favours large amounts of high-speed RAM, rather than raw processing power alone. It features faster transaction confirmation times and improved storage efficiency. The total hashing rate of the Litecoin network is over 95,642 mega hashes per second. With substantial industry support, trade volume and liquidity, Litecoin is a proven medium of commerce complementary to Bitcoin.
Litecoin can handle a higher volume of transactions owing to its faster block generation. The faster block time of litecoin minimizes the risk of double spending attacks. The current value of Litecoin is approximately $3.91.

B. Peercoin

The next cryptocurrency conscripted after Litecoin was Peercoin. The protocol of this cryptocoin was much simpler yet secure from previous versions. It was introduced in August 2012. It is limited to 80 transactions per second and 6.9 million transactions per day. Unlike bitcoins, it uses the Proof-Of-Stake strategy. The notable advantages of this cryptocurrency include faster, efficient mining and usage of lesser computing power comparatively. It has a centralized system of checkpointing that prevents the cryptocoin from major vulnerable attacks. The transaction fee of Peercoin is fixed at 0.01 PPC per transaction to prevent heavy transaction volume. The maximum cryptocoins that can be mined cannot be estimated (preferably more than bitcoins) and hence it is sometimes called as an inflationary currency[27].

C. Namecoin

The next preeminent advancement after Peercoin was the Namecoin. It was introduced in April 2011. This was not

considered as a full-fledged cryptocurrency but was designed to form as an alternative Domain Name System (DNS). This was exclusively done for the .bit domain that was not under the control of Internet Corporation of Assigned names and Numbers, (ICANN) like other top-level domains. One of the primary advantages of this concept is that it is difficult for governments, corporations, and criminals to compromise the system[14].
The recipients invest in .bit domain for the exchange of Namecoins. Later, these domains are affixed in the blockchain. The blockchain records the transactions and updates the amount of namecoins assigned to recipients.

D. Primecoin

The Primecoin in accordance to its name involves the use of prime numbers. It was introduced in July 2013. The mining process excludes the process of mathematical hash solving. The mining technique forms new and larger prime numbers thereby increasing the security of the blockchain. The proof of work protocol would require Primecoin miners to find long chains of prime numbers.
The process of generating and processing significantly large prime numbers is done by the Cunningham chains or bi-twin chains. The working rule behind a Cunningham chain of the first kind is that each prime in the chain must be one less than twice the previous. The bi-twin chains are chains of pairs of twin primes, or primes that are two units apart from each other, with the average of each pair being twice the average of the previous pair. Primecoin protocol processes payment transactions approximately ten times faster than bitcoin network.

E. Quarkcoin

The Quarkcoins were introduced in July 2013. The protocol used here is similar to that of Peercoin and hence can also be considered as inflationary cryptocurrency. Quarkcoin protocol differs from Bitcoin in three key ways namely its proof of work algorithm, its block interval and its distribution model.
The total number of cryptocoins cannot be estimated here. The distribution model in Bitcoin is an exponential decay model. The most critical part of the mining process lies in the fact that it merges many hashing algorithm techniques together to form a powerful mining strategy. It uses upto six different types of hash algorithms with nine rounds of strong encryption. The six algorithms namely BLAKE, Blue Midnight Wish, Groestl, JH, Skein and Keccak [23] are implemented in series. The block interval time is about 30 seconds.

F. Novacoin

Novacoins were launched in February 2013. The hash algorithm used here was Scrypt. However, the mining strategy involved Proof-of-Work and Proof-of-Stake method to achieve secured cryptocoins. This cryptocurrency used hybrid mining method. The maximum supply of Novacoins is restricted to 2 billion. The overall system is more complex that that of other digital currencies protocol. It requires *Centralized Checkpointing* to avoid several issues.

G. Feather coin

Feather coins are predominantly derived from Litecoin protocol. It was introduced in April 2013 and achieved maximum of 200 cryptocoins per block[13]. The most enchanting part of this cryptocurrency lies in the fact that it can protect its integrity and security against 51% of various network-based attacks. The security measure that protects this cryptocoin from reversing cryptocurrency transactions and multiple spending is called as Advanced Checkpointing.

H. Ripple

Ripple is the only cryptocurrency that does not follow bitcoin protocol. It was formulated in July 2013. It is both an open payment network and a digital currency developed by OpenCoin organization. It is the only network that facilitates the seamless transfer of any form of physical or digital currency[27]. The transactions across Ripple network ensure no waiting period for block confirmations within the distributed environment. The cryptocoins are the Ripples that are mined across the payment network. Apart from transaction logs and digital wallet balances it enables trading of cryptocurrencies in the public domain. Major benefits include expedited transactions and increased stability.

I. Elastic Coin

The term Elastic Coin was released this year 2016. The founder of this cryptocurrency is Lionel Keys. This protocol uses customized Proof-of-Work functions. It is the latest advancement in the world of digital currencies and it allows the users to wrap arbitrary computational tasks with self-programmed Proof-of-Work. The processing is carried out in peer-to-peer environment by dedicated miners. The elastic coin is considered to be the largest computation cluster available open source to the users of digital currency[12,18,19].
There are as many as 740 cryptocurrencies approximately in existence. Not every cryptocoin is successful and its foundation purely relies on the blockchain technology, hash algorithm, time stamping techniques and mining strategies. Many cryptocurrencies use Application Specific Integrated Chip (ASIC) mining and exploit the efficiency of technology. The below figure gives an insight of basic cryptocurrency system. However, it is to be noted that the first protocol of bitcoin was based on the below process. The digital wallet is the standard storage area of cryptocoins. Every wallet is unique entity and it stores the balance bitcoins of every cryptocoin user. The bitcoin address and private or secret key size may vary depending on the complexity of the protocol and number of cryptocoins to be mined. Every consecutive digital wallet is encrypted and verifies the holder's identity.

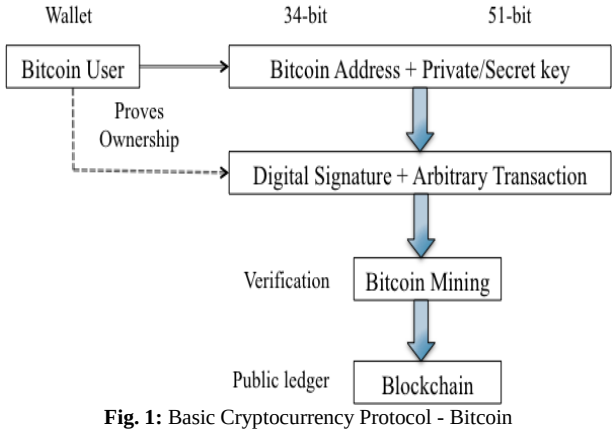

Fig. 1: Basic Cryptocurrency Protocol - Bitcoin

5. Darknet Markets

A darknet market is a collection of online deceptive markets that involves in numerous fraudulent activities. The activities can be as small as stealing a cryptocoin or as large as money laundering for terrorist based transactions. These cryptomarkets exist specifically to trade illegal drugs, forged confidential documents, complete details of victim's credit or debit card and cyber weapons such as hacking tools[20,21,23].
The darknet markets operate via darknets such as Tor and Invisible Internet Project (I2P). The Tor Project was highlighted for providing anonymous transaction whereas the Invisible Internet Project facilitated anonymous chatting, blogging and file transfers.

The first and most popular darknet market was found on a website named *Silk Road*. The website was highly anonymous without any third-party intervention leading to an increase in illegal transactions for drugs, pharmaceuticals, forged documents etc between the seller and the end customer.

The presence of darknet markets poses a major threat towards regulation of cryptocurrencies by the legal body. This is one of the biggest challenges faced by cryptocoins. Hackers or intruders can exploit the anonymity feature easily for illegal trading purposes.

The below table gives an overview of cryptocurrencies discussed in this paper. The table gives a description of few cryptocoins that gained subtle significance, the year they came into existence, the thriving technology used for cryptocoin mining and their market value.

Table 1: Overview of Cryptocoins

Cryptocoin	Established Year	Technology Used	Market Price (As per [9])
Bitcoin	2008	SHA-256	$418.00
Litecoin	2011	Scrypt	$3.23
Peercoin	2012	SHA-256	$0.449506
Namecoin	2011	SHA-256	$0.446100
Primecoin	2013	Proof-of- work	$0.086824
Quarkcoin	2013	SHA-2	$0.004332
Novacoin	2013	Scryot	$0.8513
Feathercoin	2013	Scrypt	$0.010101
Ripple	2013	Non-Proof-of-work	$0.007418
Elasticcoin	2016	Proof-of-work	$0.00146

6. Conclusion

The high volatile nature of cryptocurrencies is a matter of concern for investors that share the capital. The dwindling frequency of investment differs for each country. If their existence reduces the costs and intervention of third parties then it is also prone to complete loss due to strong malware and data loss. Various improvements can now be observed with each of them possessing their own advantage.

The concept of cryptocurrency was introduced to eliminate the need of third party for evaluating the transactions within two different entities. The protocol is customized to handle small and large transactions with frequent updation in public ledger called the blockchain. Every cryptocurrency is designed to deliver the similar output but with different approach. The difference is categorized by means of usage in various fields.

The virtual currencies are an alternative to physical currencies. Unlike, physical currencies, the handling risk can be reduced to minimal. Unpredicted phenomena such as theft or physical damage are one of the main reasons leading to a better and self-sustained alternative solution named cryptocurrencies. The most dominating cryptocurrency of this decade remains the classic Bitcoin that has paved way for existence of other cryptocoins. The market value of Bitcoin as per Table I is much higher than any other existing cryptocurrency. However, a new technology is fairly becoming one of the best rivals Bitcoin ever had called the Ethereum[24]. The value of Ethereum has increased 1000% within a span of three months due to cheaper exchange of virtual currencies and ability to create secured online markets. The major challenges that exist for cryptocurrencies includes the maintenance of digital wallet secured with password or pin, the hardware and software resources maintenance, continuous power supply wherever pool mining required, high volatility, fear of malware or data loss, physical damage of computer system etc.

References

[1] Satoshi Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System", https://bitcoin.org

[2] Bastiaan Quast, "Bitcoin and Cryptocurrencies: Or How Inflation Will Come About in Cybermoney", February 2014, 20th International Conference on Computational Engineering, Geneva.

[3] Decker C., Wattenhofer R., "Information propagation in the Bitcoin network", IEEE International Conference on Peer-to-Peer Computing, 2013, Zurich.

[4] Neil Gandal., Hanna Halaburda., "Competition in the Cryptocurrency Market", September 2014, Currency Department, Bank of Canada, Ontario.

[5] Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto, "Is Bitcoin the Only Cryptocurrency in the Town?", February 2014, Institute of Economic research, Hitsubashi University.

[6] Alex Heid, Analysis of the Cryptocurrency Marketplace, http://www.HackMiami.org

[7] Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography and Data Security, pages 436-454. Springer, 2014.

[8] https://en.wikipedia.org/wiki/Cryptocurrency

[9] https://coinmarketcap.com/

[10] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19, 2012.

[11] Reid, F., Harrigan M.: An Analysis of Anonymity in the Bitcoin System, arXiv:1107.4524v2 [physics.soc-ph] 7 May 2012.

[12] Holz, T., Steiner, M., Dahl, F., Biersack, E., Freiling, F.C.. Measurements and mitigation of peer-to-peer-based botnets: A case study onstorm worm. Proceedings of the USENIX Workshop on Large-Scale Exploits and Emergent Threats 2008.

[13] Stock, B., Gobel, J., Engelberth, M., Freiling, F.C., Holz, T.. Walowdac-analysis of a peer-to-peer botnet. In: Proceedings of the European Conference on Computer Network Defense (EC2ND). 2009.

[14] Rossow, C., Andriesse, D., Werner, T., Stone-Gross, B., Plohmann, D., Dietrich, C.J., et al. P2PWNED: modeling and evaluating the resilience of peer-to-peer botnets. In: Proceedings of the 34th IEEE Symposium on Security and Privacy (S&P). 2013.

[15] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., et al. A fistful of bitcoins: Characterizing payments among men with no names. In: Proceedings of the Internet Measurement Conference. 2013.

[16] Karame, G.O., Androulaki, E., Capkun, S.. Double-spending fast payments in bitcoin. In: Proceedings of the 2012 ACM conference on Computer and Communications Security. 2012.

[17] Ron, D., Shamir, A.. Quantitative analysis of the full bitcoin transaction graph. IACR Cryptology ePrint Archive 2012.

[18] Ober, M., Katzenbeisser, S., Hamacher, K.. Structure and anonymity of the bitcoin transaction graph. Future Internet 2013.

[19] Litke, P., Stewart, J.: Cryptocurrency-stealing malware landscape (2014) [Online, Retrieved March, 2014].

[20] Bamert, T., Decker, C., Elsen, L., Wattenhofer, R., Welten, S.: Have a Snack, Pay with Bitcoins. In: 13th IEEE International Conference on Peer-to-Peer Computing (P2P), Trento, Italy. (2013).

[21] Boehm, F., Pesch, P.: Bitcoin: A First Legal Analysis - with Reference to German and American Law. In: Workshop on Bitcoin Research. (2014).

[22] Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] ACM SIGMETRICS Performance Evaluation Review, 42(3):34-37, 2014.

[23] https://bitcoinmagazine.com/articles/quarkcoin-noble-intentions-wrong-approach-1387343686

[24] G. Wood. Ethereum: A secure decentralized generalised transaction ledger. Ethereum Project Yellow Paper, 2014.

[25] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A fistful of Bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference, IMC '13, pages 127-140, 2013.

[26] http://www.coindesk.com/information/comparing-litecoin-bitcoin/

[27] Kumar, M.V.R., Bhalaji, N. & Singh, S. "An augmented approach for pseudo-free groups in smart cyber-physical system" Cluster Comput (2018). https://doi.org/10.1007/s10586-018-2353-2.