International Journal of Financial Management (IJFM)
ISSN(P): 2319-491X; ISSN(E): 2319-4928
Vol. 8, Issue 1, Dec Jan 2019, 1-6

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

BLOCK CHAIN SYSTEM FOR DATA MANAGEMENT

Anoukh. N

School of Distance Education, University of Kerala, Thiruvananthapuram, Kerala, India

ABSTRACT

A blockchain system is a new form of data management. Its working consists in creating "blocks" of data that record every bitcoin activities that have been done from the launch of bitcoin. This systems ensure traceability and security of every transaction, making any hacking attempt impossible. Calculating every new "block" requires a huge amount of processing resources, and so it is the role of the "mining" system. The mining system is the system in charge of generating the blockchain's blocks, and at the same time creating (mining) new units of bitcoin. Bitcoin is limited in its amount with a maximum of 21 million units, that are progressively released in its system through mining and estimated being all released by 2033. The process idea is the following: some bitcoin users are also bitcoin miners: they allocated their computers/servers to feed the processing system of block-chain that is creating the blocks. In exchange for furnishing their personal devices' processing capacities, the miners get a reward in bitcoin that is added to their personal bitcoin wallet. This system provides to the Bitcoin system boththe required processing resources to aliment blockchain and the progressive production (or release) of bitcoin units. The present paper gives an overview of cryptography enabled financial products like crypto-currencies, Bitcoin and the Blockchain system for its accounting

KEYWORDS: *Cryptography, Bitcoin, Crypto Currency, Block Chain*

Article History

Received: *26 Sep 2018* **|** ***Revised:*** *21 Nov 2018* **|** ***Accepted:*** *30 Nov 2018*

Block Chain System for Data Management

Anoukh.N, SDE (2014-16), University of Kerala

INTRODUCTION

Cryptography allows to build purely decentralized systems and networks where zero trusts is needed, the possibility of fraud and malicious manipulation is reduced, and so are the mediation fees. Digital currencies are gaining grip in the financial landscape all over the world. The academic community, especially economics and computer science is also attentive on its development. This paper tries to give light on the basics of digital currency, network map based on co-authorship and co-occurrence of keywords from the web of science database. Considered as a compliment to emerging market currencies, digital currencies have inbuilt features which can revamp the financial landscapes. The cryptocurrency market has evolved erratically and at unprecedented speed over the course of its short lifespan. Since the release of the pioneer anarchic cryptocurrency, Bitcoin, to the public in January 2009, more than 550 cryptocurrencies have been developed, the majority with only a modicum of success.

As the concept of 'Blockchain' draws its implication in the context of bitcoin system it is important to explain the emergence of cryptocurrencies. Cryptocurrency is a subset of digital currency which uses cryptography (conversion of plain text into cipher text using encryption while sending and then converting it back to plain text at receiving end using decryption) to secure its transaction. It is a virtual currency with decentralized control and hence no mediators like the bank. Bitcoin is a cryptocurrency and worldwide payment system. It is the first decentralized digital currency. Its conception is peer-to-peer and transactions take place between users directly, without an intermediary. Thus, bitcoin is a type of cryptocurrency. Just as in the case of paper currency, types are US dollars, Indian rupees, etc. Bitcoin is often confused with cryptocurrency, as it is the first and foremost and the most popular cryptocurrency. Other types of cryptocurrencies are Ethereum, Ripple, Litecoin, altcoins, etc. These are used for trading, exchange, investment etc. Although the concept of electronic currency dates back to the late 1980s, Bitcoin, launched in 2009 by pseudonymous (and still unidentified) developer Satoshi Nakamoto, is the first successful decentralized cryptocurrency. In short, a cryptocurrency is a virtual coinage system that functions much like a standard currency, enabling users to provide virtual payment for goods and services free of a central trusted authority.

Cryptocurrencies rely on the transmission of digital information, utilizing cryptographic methods to ensure legitimate, unique transactions. Bitcoin took the digital coin market one step further, decentralizing the currency and freeing it from hierarchical power structures. Instead, individuals and businesses transact with the coin electronically on a peer-to-peer network. It caught wide attention beginning in 2011, and various altcoins – a general name for all other cryptocurrencies post-Bitcoin – soon appeared.

Litecoin was released in the fall of 2011, gaining modest success and enjoying the highest cryptocurrency market cap after Bitcoin until it was overtaken by Ripple on October 4th, 2014.

Bitcoin is an open source, peer-to-peer digital currency first proposed in a 2008 white paper published under the name of Satoshi Nakamoto. Nakamoto begins his paper by stating that "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weakness of the trust based model" Further, the existence of a trusted intermediary increases transaction costs, "cutting off the possibility for small casual transactions." Additionally, the trusted intermediaries are pressured to gather as much information about the parties as possible in order to control transaction costs. Hence, Nakamoto sought to create a coin that completely removed any trusted central authority and replace trust with cryptographic proof. This system would have the added benefits of having low transaction fees, low latency (time to make transactions), and pseudo-anonymity.

A bitcoin, and every subsequent cryptocurrency, is merely "a chain of digital signatures" where "Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin" so that ownership can dynamically be programmed into the coin. Further these lines of computer code are stored in a program called a "wallet" on personal hard drives and/or via online wallets like Coinbase. Like cash or commodities, bitcoins can be lost, stolen or destroyed. One British man became famous for throwing out his hard drive and with it his wallet containing over 7,000 BTC, which had a market value of approximately $7 million at the time.The prominent Bitcoin exchange, Mt. Gox, had nearly $350 million worth of bitcoin stolen in February 2014, forcing the exchange to declare bankruptcy and highlighting security issues within the cryptocurrency world.

Bitcoins can only be sent or received by logging the transaction on the public ledger, also known as the "blockchain." Bitcoins lack intrinsic value; rather, Bitcoin's value is purely a function of supply and demand. Unlike paper "fiat currency" that derives value from a government, Bitcoin is neither created by nor backed by any government. Bitcoin protocol seeks to solve the double-spending problem (essentially, spending the same coin more than once) inherent in non-cash payment systems resulting in the need for a trusted third party (such as a bank or credit card company) to verify the integrity of the transaction. Double-spending occurs when an asset is duplicated, and thus can be spent multiple times. This problem does not exist in physical currencies since transactions involve changing possession of the property. However, a digital file has the potential to be copied. The security of cryptocurrency, however, and its ability to safeguard against such digital copying, is inherent in its blockchain or public ledger systems. These systems keep records of ownership and transaction timestamps, eliminating the possibility of digital copying and, thus, double-spending. In the case of Bitcoin, a transaction is only complete and added to the blockchain once a required amount of computational power is used so as to satisfy the proof-of-work. The transaction at this point is considered complete, and ownership of the coin has been absolutely transferred, without fear of double-spending, because the entire network becomes informed of which wallet the coin currently resides in.

Bitcoinintroduced to the public on January 3rd, 2009, but traded for less than a dollar until February 2011. Bitcoin reached an all-time high of $1151/coin on December 4th, 2013, and has since steadily declined. Despite this decline, it is apparent that daily trading volume has held steady for the past year. Further, the number of unique transactions, including and excluding popular addresses, is increasing steadily, despite a sliding price. Litecoin modified Bitcoin's protocol, increasing transaction speed with the idea that it would be more appropriate for day-to-day transactions. Ripple, launched in 2013, introduced an entirely unique model to that used by Bitcoin and currently maintains the second highest market capitalization of approximately $255 million (April 22). Another notable coin in the evolutionary chain of cryptocurrency, Peercoin, employs a revolutionary technological development to secure and sustain its coinage. Peercoin merges the PoW technology used by Bitcoin and Litecoin along with its own mechanism, proof-of-stake (PoS), to employ a hybrid network security mechanism. More recently NuShares/NuBits have emerged, introduced in August 2014, which rely on a dual currency model almost entirely divorced from the single currency model used by previous coins.

One of the most important aspects of Bitcoin consists of its status of decentralized currency. The system is based on a peer-to-peer formation that has no authority to watch over. This implies various specific behavior for the Bitcoin system that does not occur in traditional payment systems and currency management. Bitcoin is generated by its own users, and not any authority, thanks to the mining system that in consequence limits inflation for the currency. It is not possible to accelerate neither slow down the pace of generation of new units since it is defined by the algorithm. It has for consequence the pure and simple impossibility of manipulation of a number of bitcoins circulating.

As a digital currency, Bitcoin is accessible through internet platforms, instanta-neously and all-over the world. It does not require intermediaries and allows instant and cheaper trades between Bitcoin users. Bouri, Elie: "On the return-volatility relationship in the Bitcoin market around the price crash of 2013" examined the relation between price returns and volatility changes in the Bitcoin market using a daily database denominated in US dollar. The results for the entire period provide no evidence of an asymmetric return-volatility relation in the Bitcoin market. The authors test if there is a difference in the return-volatility relation before and after the price crash of 2013 and show a significant inverse relation between past shocks and volatility before the crash and no significant relation after. This finding shows that, prior to the price crash of December 2013, positive shocks increased the conditional volatility more than negative shocks. This

inverted asymmetric reaction of Bitcoin to positive and negative shocks is contrary to what one observes in equities. As leverage effect and volatility feedback do not adequately explain this reaction, the authors propose the safe-haven effect (Baur, Asymmetric volatility in the gold market, 2012). They highlight the benefits of adding Bitcoin to a US equity portfolio, especially in the pre-crash period. Robustness analyses show, among others, a negative relationship between the US implied volatility index (VIX) and Bitcoin volatility. Those additional analyses further support the findings and provide useful information for economic actors who are interested in adding Bitcoin to their equity portfolios or are curious about the capabilities of Bitcoin as a financial asset. Bitcoin can be used as a hedge against the American dollar in the short-term. Bitcoin thereby possesses some of the same hedging abilities as gold and can be included in the variety of tools available to market analysts to hedge market specific risk.

The peer-to-peer format creates a relatively anonymous system, where users are only registered with personal bitcoin wallet keys. Their identity does not appear in the blocks and no institution can access it. Only the wallet reference, the current amount in this wallet and the amount transferred from a wallet to another appear in the blocks that are accessible for all.

It has no real economy guarantee (no concrete value of any kind nor any government or institution support), its value is only determined by supply and demand. There is no possibility of action on the value of the bitcoin, making it very volatile and subject to strong appreciation and depreciation, while traditional currencies benefit from the action of central banks that limit their currencies' volatility. This is a fertile soil for speculators on foreign markets.

CONCLUSIONS

The vision of an Internet of Things (IOT), in which every physical object can become part of the Internet, is almost 25 years old. Historically we have been surrounded by various organizations, financial institutions, or government agencies that have been based on centralized systems. This was for a good reason. Any kind of information or resources possessed by these entities needed to be administrated by some certain authority that was trustworthy and credible. These entities usually, due to the centralized character of the system, represent a single point of access. Given this, they are necessarily exposed to the conceivable risk of corruption, manipulation, censorship, or technical failures. Centralized systems thus inherently retain their weaknesses. On the other hand, for a long time creation of decentralized systems had been technologically infeasible. This is because such a system inherently lacks any kind of hierarchy, and thus also the authority that supervises the whole system, and provides its trustworthiness. However, nowadays we have technologies available that eliminate the need for trust in such systems by state of the art mathematical algorithms. This, in its consequences, may foster trade across the world since it allows trading people that don´t need to trust each other, and who would not have done it otherwise. Moreover, since a majority of organizations are defined by a set of various contracts, and all these can be made smart and automated, the utilization of the blockchain may bring far-reaching consequences in the field of economics and governance. All crypto-technology is underpinned by the two main ideas: Public Key Cryptography and the blockchain. The first one – public key cryptography – is a sophisticated math concept that allows an individual to encode a virtual good that can only be decoded by the intended recipient. Even the sender cannot decode it once the good has been encoded. In this concept, there are two numbers deployed: a private key and a public key. The second idea is the blockchain which can be described as a special form of the ledger that keeps track of evidence who holds what, and that is extremely hard to be deceitfully modified. Also, one of the important properties of the blockchain is its pseudo-anonymity. The present paper elaborates on emerging developments namely Cryptocurrencies, Bitcoin and Blockchain and related

issues.

REFERENCES

1. *Ryan Farell, An Analysis of Crypto Currency Industry, University of Pennsylvania Research Sclolar*
2. *Dávid Stancel 'Economic Consequences of Crypto Currencies and Associated Decentrlised Systems'Batchelor Thesis pp. 95–298. url*
3. *Worner,¨ Dominic, Thomas von Bomhard, Marc Roschlin,¨ and Felix Wort-mann (2014). "Look Twice: Uncover Hidden Information in Room Climate Sensor Data." In: International Conference on the Internet of Things (IOT). Cambridge, MA, pp. 25–30*
4. *Worner,¨ Dominic, Thomas Von Bomhard, Yan-Peter Schreier, and Dominik Bilgeri (2016). "The Bitcoin Ecosystem: Disruption Beyond Financial Ser-vices?" In: European Conference on Information Systems (ECIS). Istanbul, Turkey Wikipedia.org*