International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(1), pp.185-189
DOI: http://dx.doi.org/10.21172/1.91.28
e-ISSN:2278-621X

ANALYSIS ON CRYPTO-CURRENCY

Shipra Saraswat[1], Vishal Singh Chauhan[2] & Neetu Faujdar[3]

Abstract- From history, people have used commodity currency (i.e. commodity currency consists of objects that have value in themselves as well as value in their use as money). Fiat currency is the most dominant form of money. Now, comes the currency that is neither fiat currency nor commodity money. It is a new development that is growing at a very unpredicted rate. Using crypto-currencies like Bit coin can reduce your transaction fees but miners (Persons who are involved in completing a transaction) are compensated by their own Bit-coin network. Everyone has access to it and all the Bit coins are protected by unique encryption technique. Meanwhile a big and exciting open-source community has presents and organized several changes and extensions. So here in our paper we will have a concise yet comprehensive knowledge of what crypto-currency is.

Keywords-Crypto Currency, Stake Proof, Bit coin, Government Regulations, Public Perception

1. INTRODUCTION

Crypto currency is a digital currency that practices encryption methods and are essentially used to control the age group of units of currency and confirm the transfer of funds and also working autonomously of a Central Bank. Crypto currencies are a subset of alternative currencies, or basically of all digital currencies. The market of the crypto-currency has shown growth at an unpredictable rate that too in a very short lifespan. After the release of the first crypto-currency, Bit coin, in January 2009, more than 710 crypto currencies had been made that are available for trade in the online markets as of 11 July 2016. Out of which only 26 of them have shown a good growth rate. Investigation on this field is still scarce. Most of the researches are mainly focused on Bit coin rather than the crypto-currency industry. This paper tries to give a short yet complete information of this trade with a complete knowledge of the first decentralized currency, Bit coin.

The paper consists the detailed experimental analysis of crypto-currency. Following are the key points of the authors of this paper:

1. Complete overview of this industry.
2. Bit coin, the first decentralized currency.
3. Network Security Protocols used by different crypto- currencies.
4. Factors that affects the growth of crypto-currencies.
5. Public perceptions for crypto-currencies.

A note on sources: Because the crypto-currency industry is still young and factors that impact it are turning on a daily basis, few comprehensive or fully updated academic sources exist on the topic. While academic work was of course consulted for this project, the majority of the information that informs this paper was derived from White Papers or synthesized using raw data.

2. INDUSTRY OVERVIEW

Although the idea of digital forex commenced within the past due Nineteen Eighties, Bitcoin that released in 2009 by means of a developer Satoshi Nakamoto, is the first successful decentralized cryptocurrency [1]. In quick, a cryptocurrency is a virtual coinage device that functions similar to a ordinary foreign money, allowing users to offer virtual payment for their items and offerings free of a valuable trusted authority. Cryptocurrencies ordinarily depends at the transmission of digital facts, via using cryptographic techniques to make sure legitimate, specific transactions. Bitcoin took the virtual coin market one step beforehand, decentralizing the foreign money and making it free from hierarchical energy structures. Alternatively, individuals and corporations transact with the coin electronically on a peer-to-peer network. It stuck extensive interest starting in 2011, and various other coins post-Bitcoin – quickly appeared. Lite coin became launched for the duration of the give up months of 2011, gaining modest achievement and playing the best cryptocurrency market cap after Bitcoin until it became overtaken by using Ripple on October 4th, 2014 . Litecoin changed Bitcoin's protocol, increasing transaction speed with the idea that it might be more suitable for every day transactions. Ripple, launched in 2013, delivered an entirely unique version to that utilized by Bitcoin and currently keeps the second one highest market capitalization of about $255 million (April 22) . Any other wonderful coin in the evolutionary chain of cryptocurrency, Peercoin, employs a innovative technological improvement to at ease and maintain its coinage[2] . Peercoin merges the PoW technology utilized by Bitcoin and Litecoin alongside its very own mechanism, proof-of-stake (PoS), to employ a hybrid network protection mechanism. More recently

[1] *Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India*
[2] *Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India*
[3] *Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India*

Unshars/NuBits have emerged, delivered in August 2014, which rely upon a dual forex version almost completely divorced from the unmarried foreign money version used by previous cash .

On the while this paper was written, the cryptocurrency business comprised of over 550 coins with various user bases and change volumes. due to high volatility, the marketplace capitalization of the cryptocurrency enterprise adjustments dramatically, but is anticipated at the time of this paper to be just over $3.5 billion, with Bitcoin representing about 88% of the marketplace cap[3].

2.1 The Beginning Was Bitcoin-

Bitcoin is an open source, peer-to-peer digital currency first proposed in the 2008 white paper published under the name of Satoshi Nakamoto. Takemoto 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 . Also, the presence of a trusted intermediary shows growth 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 or no transaction fees, low latency (time taken to make a complete transaction), and pseudoanonymity[4].

A bitcoin, and each next cryptocurrency, is just a sequence of virtual signatures in which every proprietor transfers the coin to the following by digitally signing a hash of the previous transaction and the general public key of the next proprietor and adding these to the end of the coin in order that possession can dynamically be programmed into the coin this is done so that every current proprietor can be recognized. In addition, these lines of pc code are stored in a program called a pockets on personal difficult drives and/or through online wallets like Coinbase[5]. Like cash or commodities, bitcoins may be misplaced, stolen or destroyed. One British guy became well-known for throwing out his difficult power, and with it his wallet containing over 7,000 BTC, which had a marketplace cost of approximately $7 million at the time [6]. The outstanding Bitcoin exchange, Mt. Gox, had almost $350 million worth of bitcoin stolen in February 2014, forcing the change to declare financial disaster and highlighting security troubles inside the cryptocurrency world .

Bitcoins can handiest be despatched or acquired through logging the transaction on the public ledger, also called the blockchain. Bitcoins lack intrinsic fee; as a substitute, Bitcoin's fee is only a function of deliver and demand [8]. Unlike paper fiat cash that derives cost from a government, Bitcoin is neither created with the aid of, nor backed by using, any authorities. Bitcoin protocol seeks to resolve the double

spending hassle (essentially, spending the identical coin more than as soon as) inherent in non-coins price structures ensuing inside the need for a relied on 0.33 birthday celebration (which includes a bank or credit score card company) to verify the integrity of the transaction. Double-spending occurs whilst an asset is duplicated, and for that reason may be spent a couple of instances. This trouble does no longer exist in bodily currencies, in view that transactions contain converting possessionof assets[7]. However, a virtual record has the capacity to be copied. The safety of cryptocurrency, however, and its capacity to guard in opposition to such digital copying, is inherent in its blockchain or public ledger structures. Those structures preserve data of ownership and transaction timestamps, eliminating the possibility of virtual copying and, therefore, double-spending. The mechanism used to at ease the network is mentioned deeply in phase 2. in the case of Bitcoin, a transaction is handiest complete and added to the blockchain as soon as a required amount of computational electricity is used if you want to satisfy the proof-of-paintings (discussed in phase 2.1). The transaction at this point is taken into consideration complete, and possession of the coin has been sincerely transferred, without fear of double-spending, due to the fact the whole community will become informed of which wallet the coin currently resides in.

2.2 Competing Cryptocurrencies-

According to en.Wikipedia.org, there more than 710 distinct crypto currencies are written in this study. Despite of many cryptocurrencies in the market Bitcoin has still maintained its position at the top of this industry. Also, all the other currencies uses bitcoins for their transactions i.e many exchanges gives option to their customers to invest in other cryptocurrencies by Bitcoin.

2.3 Protocol Of Network Security-

Perhaps Bitcoin's supreme industrial accomplishment (and the most significant of every other crypto coin) is building a peerto-peer business system that trusts on cryptographic proof rather than trust . However, replacing a central authority presents a unique problem with a solution that is not obvious. First, the coin needs to be able to change ownership. Transactions are recorded by combining the digital signatures of each party and a timestamp, so that the transaction date is recorded[8]. This new code represents the coin and its path through the network. This code is then broadcasted to all nodes (computers connected to and running the cryptocurrency network software) on the network. However, it is necessary that the majority of the nodes agree on transactions that have occurred, otherwise double-spending and denial-of-service (DoS) attacks can occur. The mechanism used to reach consensus among nodes puts integrity in the system by verifying that the transaction is indeed legitimate. Hence, transactions are verified, and the system made secure, by implementing certain mechanisms that make it too costly to violate the integrity of the system. Larry Ren, developer of Reddcoin, notes.The underlying principle of such a mechanism is the necessity of expending resources when confirming transactions

2.3.1 Proof-Of-Work

First proposed through Cynthia Dwork and Moni Naor in 1993, A evidence-of-work (PoW) is a chunk of facts which is luxurious to supply in order to satisfy positive requirements however is trivial to confirm. That is, PoW enhances an monetary value to achieve a given purpose. Inside the situation of cryptocurrencies, dealings are not careful authenticated until a certain quantity of electricity has been expended. Most different coins that use the PoW mechanism are direct copies of, or are very just like, Bitcoin's protocol. The following section will consciousness on how the mechanism is applied by means of Bitcoin [9]. In proof of work it has to verify certain requirements as well as others should also satisfy those requirements. It is just verification of the transactions and once verified the person that helped in execution of the transaction i.e miners is rewarded with some new Bitcoins. It was first introduced in Bitcoin but as the number of cryptocurrencies kept on increasing a numbers of new algorithms came in the market that were proposed to be better.

In the Bitcoin procedure, all dealings all through a certain term are gathered into something called a block. This block is then broadcasted to all the nodes currently related to the Bitcoin network. Bitcoin uses the Hashcash PoW mechanism, first proposed by way of Adam lower back in 1997. beneath this mechanism, in order to agree upon a set of broadcasted transactions, every node basically takes the block and begins including a bit of facts to the block identified as a nonce, such that the (block+nonce), when placed right into a confusing algorithm, has a hash that encounters positive necessities - in this case, it starts offevolved with a certain variety of zeros. as a consequence, every node tries to resolve a difficult mathematical calculation, the outcome of which can be without problems established through computing a unmarried hash. The Bitcoin protocol requires that nodes use the SHA256 hashing feature . Once a node reveals a approach to the trouble, the PoW necessities are considered happy, and the brand new (block+nonce+hash) is added to the blockchain and broadcasted to all nodes. Because best one block may be validated at a time, the possibility a node will solve for the ideal hash will increase proportionally with the amount of CPU electricity expended. Consequently, the sources consumed on this example are energy and time, which can be indeed scarce.

2.3.2 Stake Proof

An opportunity to the PoW device is the proof-of-Stake (PoS) apparatus. In its place of including on computational strength as its scarce useful resource, the aid that the

network safety depends on is possession of the coin itself – proof-of-stake way a form of evidence-of-possession – which is also scarce. Consequently, in order to confirm a transaction and obtain the coin praise (whether new cash or transaction prices), a miner need to personal a few coin himself. In addition, the opportunity that he prospers in generating a novel block is a characteristic of the quantity of money he possesses, not of computational asset. Therefore, there are very little strength expenses in this transaction. Further, so one can undermine the integrity of the device, one might should own extra than 50% of the coin currently being staked, in which case violating the coin security could be very pricey . Normally, charge takes the shape of a hobby on the quantity of coin staked to affirm the transaction . In reality, maximum natural PoS cash have turned out to be fraudulent, as the creator frequently offers himself the majority of the cash.

2.3.3 Hybrid Pow/Pos

A hybrid PoW/PoS unit uses the PoW mechanism in the starting of the coin minting process and distribution. That is, PoW allows the network to give out new coins to miners. However, by time, the PoS mechanism phases out the PoW mechanism, creating a long-term energy efficient cryptocurrency. Sunny King and Scott Nadal, in their white paper PPCoin: Peer-to-Peer Crypto-Currency with Proof-ofStake, are the primary advise and then implement such a cross PoW/PoS system. In this hybrid-design, block generation, instead of relying on one CPU per vote, relies on a concept of coinage . Coinage is roughly the amount of coin owned multiplied by the life of ownership by the current owner of the coin. Block generation thus goes to the block with the most coinage. Further, coins are minted according to one percent per coin-year consumed, which functions as an interest rate for staking coin . The main advantage, however, is that this system does not rely on high-energy consumption in the long run. Hence, the design is costcompetitive to that which relies on PoW and avoids the distribution problem inherent in Pos [10].

3. FACTORS THAT AFFECT GROWTH

Fact that the fraction of the cryptocurrency has increased in the last half decade, its path has been turbulent. Many of the people argued the performance of anarchic cryptocurrency underwhelming in comparison to the hype it stirred when it publicly emerged in 2009. This section will address two of the main factors that have affected the growth of the cryptocurrency industry and will continue to influence its development and integration into the broader financial scheme well into the future: international government regulatory attempts, and ambivalent public perception in moving toward its wider adoption.

3.1 Government Regulations

While the expanding cryptocurrency market has the potential to revolutionize the way money is exchanged, its introduction into global venues is fraught with challenges and potential pitfalls. Because virtual currencies are not universally recognized as official means of paying for goods and services, developing standardized systems for their use is critical. For the currencies to be sustainable, their legal status must be established. Controlling systems are burgeoning, with numerous methods being taken by different governments. Present regulatory actions are in their infancy and endure to change with the rapidly increasing industry. Regulations will offer greater legitimacy to a currency struggling to gain mass acceptance. They will standardize elements of the market and minimize at least some of the volatility. While governments are testing an amalgam of regulatory steps, their end goal is the same: to limit fraud, protect consumers, respect economic sanctions, and institute viable taxation methods. A brief feature of current crypto currency procedure in numerous states will proposal clarity and a wide impression of existing regulation attempts. Because of the infancy of virtual money, offered data is in flux and subject to normal change [11]. The United States takes a permissive, slightly neutral stance on crypto currencies. The current challenge faced by regulators is expanding existing laws to allow for the unique aspects and challenges of the virtual currency world. For taxation purposes, virtual currencies are handled as property rather than as currency, and transactions are subject to the same taxation norms as other types of property[12]. Even the FINCEN (Financial Crimes Enforcement Network) has taken steps to clarify the transaction attempts using crypto currencies. But these currencies should follow the government requirements . Now, California has added cryptocurrency movement than any extra state, and has been proactive in including digital moneys into current monetary agendas. In January of 2015, cryptocurrency increased legal position in California, important to estimates that other states would monitor suit. New York has also taken note of the evolving market, presently in the final stages of establishing its own adjusting context. Australia, whose citizen’s account for roughly 7% of Bitcoin users, has not formally adopted regulations for virtual currency, but has established a system of taxation for the coinage. Trading done in the form of cryptocurrency is subject to the country’s preexisting tax rules relating to goods and services. While the Australian government has been clear that Bitcoin is not a legally recognized universal means of exchange and form of payment by the laws of Australia or the laws of any other country, it has provided space for the cryptocurrency to comfortably exist. Canada is the most powerful and developed system which has a strict regulations having to implement a tax on virtual currencies. Due to this system has consists minimum risks, minimum terrorist funding. The Canada bank’s showed their willingness to start the market of virtual currency but currently they needs the investors rather than money[13].

Russia hasn’t showed any good interest in the emergence of these industries. The Bank of Russia shared concerns that the currency could facilitate money-laundering attempts, it means to transport money to terrorist groups[14]. Moreover, the bank agrees that this market has violates federal laws of central bank. The trend concerning restriction is reflected in other countries. Vietnam has firmly cautioned its citizens on the use of cryptocurrencies. While there is no regulation specifically relating to virtual currency usage, the Bank of Vietnam has warned that Vietnam does not consider virtual currency to be a legitimate form of currency. Transactions utilizing forms of cryptocurrency are not covered by legal protections.

4. PUBLIC PERCEPTION

The growth in this industry has evolved only because of the interest as well as the acceptance of the users in this. without interest it would not have been possible for the bit coin itself to evolve. Yes, this industry is difficult to understand and hence requires a massive amount of education. People investing in these industry without proper knowledge and guidance may also get trapped. The industry has showed a massive growth in the last few years that does not means it turns only to profits of its investors. But yes because of the large number of users and large number of transactions face to fall in this rarely [15]. So, this section represents all the positive and the negative factors corresponding to the public perception.

Slowly, through news stories and pioneering individuals championing its virtues, crypto currency is gaining a presence in the global market. However, despite the recent surge in media coverage, crypto currencies are still widely unknown by the general public[16]. Coincenter.com has conducted a monthly survey for the past eight months, tracking American public sentiment towards Bit coin. Since Bit coin is by far the most prominent of the crypto currencies, much can be inferred about attitudes towards crypto currency as a whole. April’s results indicate that the average person is still largely unaware of Bit coin’s existence. Only 4.5% of those surveyed had ever used the currency. This statistic, coupled with survey results indicating skepticism regarding Bit coin’s usefulness today, forms an underwhelming picture.

5. CONCLUSION

This industry of crypt currency is moving towards another level of success. Despite of many hindrances being getting shutting down by the government it has shown a very resilient behavior towards its growth. Also this industry has shown growth not only in the section of its price but also have shown a dramatic expansion in the number of coins that are currently in circulation

6. REFERENCES

[1] Crypto-Currency Market Capitalizations. [Online]. http://coinmarketcap.com/

[2] Satoshi Nakamoto. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. https://bitcoin.org/bitcoin.pdf

[3] J. Barkatullah, T. Hanke, R. Iyengar, R. Lewelling and J. O'Connor, Goldstrike 1: Cointerra's first generation cryptocurrency processor for bitcoin mining machines, 2014 IEEE Hot Chips 26 Symposium (HCS), Cupertino, CA, 2014, pp. 116. doi: 10.1109/HOTCHIPS.2014.7478824

[4] P. Monamo, V. Marivate and B. Twala, Unsupervised learning for robust Bitcoin fraud detection, 2016 Information Security for South Africa (ISSA), Johannesburg, 2016, pp. 129134. doi: 10.1109/ISSA.2016.7802939

[5] N. T. Courtois, P. Emirdag and D. A. Nagy, Could Bitcoin transactions be 100x faster?, 2014 11th International Conference on Security and Cryptography (SECRYPT), Vienna, 2014, pp. 1-6

[6] J. Li and T. Wolf, A one-way proof-of-work protocol to protect controllers in software-defined networks, IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), Santa Clara, CA, pp. 123124, 2016.

[7] R. Dennis, G. Owenson and B. Aziz, A Temporal Blockchain: A Formal Analysis, International Conference on Collaboration Technologies and Systems (CTS), Orlando, FL, , pp. 430-43, 2016.

[8] A. Ekblaw, C. Barabas, J. Harvey-Buschel and A. Lippman, Bitcoin and the Myth of Decentralization: Sociotechnical Proposals for Restoring Network Integrity, 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), Augsburg, pp. 1823, 2016.

[9] Blockchain info. Online Source.

[10] Christian Decker and Roger Wattenhofer Information propagation in the bitcoin network, 13-th IEEE International Conference on Peer-to-Peer Computing, 2013.

[11] K. Christidis M. Devetsikiotis Blockchains and smart contracts for the internet of things, IEEE, vol. 4, pp. 22922303, 2016.

[12] M. Shoaib M. Ilyas M. S. H. Khiyal "Official digital currency" ,Proc. 8th Int. Conf on Digital Information Management (ICDIM‘ 2013), pp. 346-352.

[13] CoinMarketCap, May 25 2014 [online] Available: http://coinmarketcap.com!all.html.

[14] A. LaFrance ,Why Bitcoin Needs More Women,Feb 28 2014 [online] Available: http://www.popsci.com!blog-networklladybits/why-bitcoin-needs-more-women.

[15] B. Carson ,Such Dogecoin. Much Validity. How one altcoin may have turned into cryptocurrency's best marketing tool, may 4 2014 [online] Available: https:llgigaom.com!2014/05/04/such-dogecoin-much-validity-how-one-altcoin-may-have-turned-into-cryptocurrencys-best-marketing-tool.

[16] D. Morris,Inside the world of national cryptocurrencies, April 9 2014 [online] Available: http://finance.fortune.cnn.com!2014/04/09/national-cryptocurrency.

[17] S. Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" 2008.