Significance of Blockchain in the functioning of Crypto-currency

Akash Kumar Bhagat, Assistant Professor

Department of Computer Science Eng., Arka Jain University, Jamshedpur, Jharkhand, India

Email Id-akash.b@arkajainuniversity.ac.in

ABSTRACT: ***Blockchain creates interesting research subjects from a technical perspective since it offers security, privacy, and data integrity without a third-party organization managing transactions. Blockchain is a decentralized transaction and data management system that was first developed for the Bitcoin crypto currency and is now utilized by a wide range of businesses. We will emphasize the applications and contributions of blockchain technology in finance in general, as well as areas where the technology may have a greater effect on payment systems, in this article. The authors examine the successful applications of blockchain technology in various financial areas, including crypto-currency, in addition to giving a thorough study of blockchain technology and crypto-currency. The authors carefully analyze a technical research on bitcoin price behavior. Crypto currency, which is the first successful application of blockchain technology, may fuel a money transfer network.***

KEYWORDS: Bitcoin, Blockchain, Crypto-Currency, Network, Transactions.

1. INTRODUCTION

People and corporations commonly use a third-party agency to regulate their currency transactions. In order to execute a digital payment or currency transfer, a bank or credit card issuer must serve as a middleman. An additional fee is charged by a bank or credit card provider for a transaction. Other fields such as video games, music and software are also affected by this process [1]. All data and information are handled and maintained by an independent third-party entity, rather than by the two major parties engaged in the transaction. To overcome this problem, blockchain technology has been created and is currently being used. In order to establish a decentralised environment where no third party controls the transactions and data, blockchain technology was developed as a solution[2].

Block-chain is a distributed database that maintains an ever-expanding list of data entries that are verified by the nodes that participate in the network. In a public ledger, every transaction is recorded. Decentralized blockchain technology eliminates the need for a third-party intermediary. All nodes in the blockchain network have access to information about every transaction that has ever taken place. Transparency is enhanced by this feature, as opposed to centralised transactions that involve a third party. Due to the anonymity of the nodes in Blockchain, it is more secure for other nodes to verify transactions. When Blockchain technology was initially used in Bitcoin, it was a game-changer. Participants may purchase and sell things with digital money thanks to the decentralised ecosystem provided by it[3].

1.1 Overview Of Blockchain Technology:

Decentralized currencies, self-executing contracts (smart contracts), and intelligent assets that can be controlled via the Internet are all possible with blockchain technology (smart property). Decentralized (autonomous) organisations that may function across a network of computers without any human involvement are also possible using blockchain. With these uses, some have drawn comparisons between Blockchain and Internet, predicting that it would help displace centralised authority in the fields of communications, economic transactions, and even politics or law.

Without a centralised authority to ensure that the data was not tampered with, it was impossible to coordinate individual actions over the Internet prior to the creation of the blockchain. Without a central authority to verify that this specific transaction was neither fraudulent nor invalid, a collection of unconnected persons could not affirm that an event had taken place. Unanimity was thought to be impossible in the case where there was no central clearinghouse for the scattered collection of individuals. This problem can be solved using a probabilistic method using a blockchain.20 Through the use of computationally intensive mathematical problems, it makes information passing through a network of computers more transparent and verifiable. If an attacker does not control a majority of the network's processing capacity, it will be more difficult for them to damage a shared database with false information. 21 Decentralized transactions may be coordinated without having to rely on a trusted third party to validate and clear all transactions, because blockchain protocols

ensure that transactions on a blockchain are legitimate and never recorded to the common repository more than once[4].

1.2 Emerging Uses Of Blockchain Technology:

Cryptographic tokens that might represent property or ownership interest in future services have been created by software developers who have swiftly grasped the possibilities of blockchain technology. Decentralized domain name management systems (DNS) and censorship-resistant digital voting platforms are also being developed with it. 32 For this reason, the technology is becoming recognised as a means to facilitate machine-to machine connections that will soon arise from the Internet of Things' Internet-enabled objects. 33 This is because the blockchain combines digital currency, smart contracts, and distributed data storage to create whole new decentralised organisations (such as autonomous decentralised organisations) that utilise source code to design a governance structure for their companies.

1.3 Digital Currencies and Global Payment Systems:

Digital currencies such as Bitcoin were one of the first implementations of blockchain technology. From the anonymous organisation or individual known only as Satoshi Nakamoto, this book was published in 2009[5]. This digital money, unlike the US dollar, does not depend on any bank or government. As Nakamoto explains, the system is "totally decentralised, with no central server or trusted parties, because everything is based on crypto evidence instead of trust".

From the moment it was first introduced, Bitcoin has captivated the interest of the globe. However, Bitcoin is utilised for more than simply speculative purposes nowadays. A whole new payment system is powered by it, allowing for frictionless transfers of cash throughout the world. A bitcoin transaction may be transmitted around the globe in less than seven minutes, compared to days for conventional payment methods such as Western Union. Only an Internet connection and a computer or mobile device are required.

Crypto-currencies like Bitcoin have been gaining popularity rapidly, and they have the potential to be the first breakthrough applications that rely on blockchain technology. They notes that these digital currencies have the ability to boost international trade, support financial inclusion and alter the way we spend money, save money and do business in ways we haven't completely grasped as of yet." There is a potential for faster and cheaper bank transfers, the expansion of banking and e-commerce operations to third-world nations, and a significant reduction in merchant fraud if this technology is implemented.45

1.4 Ethereum:

A blockchain-based virtual machine and Cloud 2.0 platform, Ethereum has stateful user-created digital contracts that may be executed in real time. The engineers are working on a system that will allow for the exchange of complicated contracts, which will be available in the future. As users become more sophisticated in their interactions, they will be able to enter into digital contracts using a distributed ledger architecture. Crypto-economy is being extended beyond virtual currency transactions with Ethereum, which provides a strong technological and legal foundation for the development of a nexus of digital contracts related to all sectors of life (for example, wage payment or marriage).

1.5 Distributed and Secure Data Stores:

A decentralised, encrypted database, blockchains are also beginning to influence the way we communicate and exchange data online because of their decentralised nature. Additionally, they are increasingly regarded as a means to promote machine-to-machine connections for Internet enabled devices. Blockchain technology eliminates the need to route conversations and data through a centralised system or internet platform (like Gmail for e-mails or Dropbox for the exchange of digital files). Parties can save and retrieve communications without the danger of government intrusion using decentralised, encrypted communication protocols59 and a blockchain. 60 The same technology also enables for the decentralised and safe sharing of data. Publication and distribution of information over hundreds of thousands of computers (encrypted if required) makes censorship nearly impossible. People are encouraged to use their spare hard drive space by using anonymous, decentralised cloud storage solutions that employ blockchain technology and other peer-to-peer technologies. A number of technical problems and constraints associated with blockchain technology have been discovered. In the future, blockchain technology will face seven technological problems and limitations:

1.5.1. Through-put:

The Bitcoin network's maximum throughput is presently 7tps (transactions per second). VISA (2,000tps) and Twitter are two other transaction processing networks (5,000tps). In order to maintain the same level of transaction frequency, the blockchain network's throughput must be increased.

1.5.2. Latency:

Currently, it takes about 10 minutes to complete a transaction in order to ensure the security of a Bitcoin transaction block. Because double spending assaults are costly, more time must be spent on a block to achieve efficiency. As a result, latency is now a major problem in the blockchain world. As long as security is maintained, it should be possible to create a block and confirm the transaction in a few seconds. To execute a transaction with VISA, for example, it takes only a few moments.

1.5.3. Size and bandwidth:

Bitcoin's blockchains are over 50,000MB in size at now (February 2016). 214PB per year might be added to the blockchain if throughput reaches VISA levels. It is assumed by the Bitcoin community that one block is 1MB in size with one block being generated every 10 minutes. It follows thus that transactions are limited in quantity (on average, 500 per block). To increase the number of transactions that the blockchain can handle, the size and bandwidth concerns must be addressed first.

1.5.4. Security:

The present Blockchain is vulnerable to a 51 percent assault because of the way it is designed. The bulk of the network's mining hash-rate would be under the control of a single organisation, allowing it to influence Blockchain. Additional security research is required to solve this problem.

1.5.5. Resources that have been wasted:

Bitcoin wastes mining in the billions of dollars a day. Crypto-currency's Proof-of-Work effort is to blame for wasting Bitcoin's resources. A miner's Bitcoin holdings are used to compare resources while using Proof-of-Stake. When someone holds 1 percent of bitcoin, they may mine 1 percent of the blocks that prove their stake. In order to improve the efficiency of mining in Blockchain, the problem of wasted resources must be addressed and resolved.

1.5.6. User-friendliness:

The Bitcoin API for creating services is not very user-friendly. For Blockchain, a more developer-friendly API is required. REST APIs are a good example of this.

It's all there, versioning, hard forks, and numerous chains of code 51 percent attacks are more likely to occur in chains with a small number of nodes. When chains are separated for administrative or versioning purposes, another difficulty arises.

1.6 Decentralized (Autonomous) Organization:

As a result, Michael Jensen and William Meckling's notion that entities are nothing more than a collection of contracts and connections is now a reality. As the world's first decentralised public ledger, Bitcoin has grown in popularity since 2013-2014. Despite the fact that mainstream adoption is still a long way off, the success of Bitcoin may be attributed to the underlying technology known as the blockchain. An electronic public ledger platform that is shared by all participants through the Internet or another distributed network of computers. As a general rule, blockchain is designed to eliminate the requirement for a trusted third party to ensure transactions, with the noteworthy exception of token-free applications this will go through five of the most essential characteristics of public ledgers in the following paragraphs.

However, even while Blockchain appears to be a good option for conducting transactions using crypto-currencies, it still has certain technological problems and limits that need to be explored and dealt with in the future. To avoid assaults and efforts to disrupt transactions in Blockchain, high integrity of transactions and security, as well as privacy of nodes, are required. Aside from that, verifying transactions in the Blockchain needs a lot of computing power. What subjects have already been investigated and handled in Blockchain, as well as what are the current major problems and limits that require additional study, are crucial to recognise and understand. A thorough mapping study approach [2] was used in order to find relevant Blockchain-related articles. A well-designed procedure was used to scan scientific databases in the systematic mapping investigation. Researchers and practitioners will be able to discover prospective study areas and issues for future research thanks to the map of existing research on Blockchain.

1.7 Challenges Faced By Blockchain Technology

Almost everyone would agree that the blockchain technology has the ability to fundamentally alter society, and notably banking and economics, in the near term. On its road to becoming a key ecosystem for the global financial network, this cutting-edge technology must overcome a number of challenges. Numerous reasons hinder crypto-currencies and blockchain technology from becoming a global standard for financial transactions, despite its many benefits. In the absence of rules, users are concerned. Legal status as a means of making a long-term payment system Standardizing market components and reducing volatility will be achieved through legislation.

The use of crypto-currencies in money laundering and financial crimes, as well as its usage by the black market, is another significant concern connected to the absence of laws[6]. Block chain's innovative technology makes it a popular alternative to conventional systems for money transfers and record keeping, but it is still at risk of being attacked by hackers. All recent crypto-currency-related hacking instances did not use blockchain technology, but rather digital currency exchanges. Crypto-currency's network security has never been hacked by hackers. Each exchange is responsible for implementing and maintaining the security protocol used at digital currency exchanges. However, these hacking stories have a detrimental impact on users' and prospective users' perspectives. There's no doubt about it, but news about hacking incidents at exchanges has generated a bad image of crypto-currencies and blockchain that has yet to be overcome.

1.8 Public Ledgers under Criticism that is Toward Hybrid Solutions:

Technological advances have always provided a means of shifting power from central authority to the populace. A few centuries ago, early mechanical advances permitted individuals to track their own time in the same manner that massive and expensive clock towers were a testament to the concentration of power in the hands of a minority. Traditional banking's basic concepts are at odds with the blockchain. An accountant's propensity is to consolidate all payment, transaction, and loan information in a computer system. This is what a banker's job is all about: keeping money and money information. It's possible that blockchain technology will be a game changer for the financial sector as a whole. Reviewing possible applications that might increase the efficiency of financial organisations while reducing their costs

Here, we examine the benefits and drawbacks of this emerging decentralised tech, arguing that its widespread adoption will lead to the expansion of a new subset of law, which we call Lex-Cryptographia: rules administered through self-executing smart contracts and decentralised organisations. Due to the widespread use of blockchain technology, governments and big multinational businesses may lose the capacity to control and affect the behaviour of disparate individuals using conventional methods. This means that there will be a growing need for a better understanding of how to govern blockchain technology and how to guide the formation and deployment of these new decentralised organisations in ways that have not previously been examined under existing legal theory.

1.9 Growth Of Blockchain:

Our lives have improved dramatically as a result of technological advancements. Its ease, transparency, correctness, and efficiency in terms of time and cost make blockchain a revolutionary technology that can transform the world for the better. In addition to the recent advancements in the world of finance, there has been a significant leap forward in technology. Some commentators compare the potential effect of blockchain technology to the worldwide connectedness and ease that the internet offered us. It's important to note that this comparison does not exaggerate the potential of blockchain technology for the future of humanity. Neither the improvement in our quality of life nor the fast growth of contemporary technology are coincidental events.

Finance industry applications of blockchain technology and crypto-currencies that are networked by blockchain technology have shown success in the operation of payments and money transfers, especially. For this unique technology to grow, there is still a lot of opportunity remaining. Due to its speed, very low cost, transparency, security and ease, the worldwide money transfer industry is the perfect place for blockchain technology to be applied.

An increase in the number of successful use cases and testimonials as well as suitable legal reforms are required for blockchain adoption in finance to continue to expand. In presenting an in-depth analysis of the contributions blockchain technology has made and will continue to make in the field of financial services in this paper A special focus was on comprehending the major crypto-currencies and their uses, along with proof of Ripple's use and prospective applications in cross-border money transfer markets provides a thorough review of empirical research that address the features and price fluctuations of crypto-currency marketplaces.

Despite the fact that the hype around blockchain is currently high, it's expected to hit a plateau in the next 5 to 10 years. As a result, this technology appears to be descending towards the Disillusionment Valley. We predict a shift in maturity from 5 to 10 years to 2 to 5 years as a result of the extensive use of the Blockchain across a wide variety of applications outside crypto-currencies. If extensively embraced by e-governance applications for identity management, asset ownership transfer of valuable commodities, healthcare, and other commercial purposes, as well as financial inclusion, blockchain has the potential to empower individuals in poor nations. What happens in the future is, of course, highly dependent on national political decisions.

Main goal of this article is to recognise the advantages and present problems of utilising crypto-currencies for diverse purposes. It has implications for a general audience that wants a basic but critical grasp of crypto-currencies and blockchain technology. In recent months, volatility in major crypto-currency prices appears to have stabilised. Longer time-series, including recent less volatile pricing data, allow for a more thorough study of crypto-currency features (e.g., speculative vs. non-speculative, bubble vs. non-bubble) using longer time-series including the recent less volatile pricing data[7]. All parties involved in the transfer of funds - including banks - must be able to trust each other. Instead of trust, blockchain technology uses mathematically defined and mechanically enforced rules to replace a system that was previously dependent on it. In the global payments business, auditors, legal professionals, payment processors, brokers, and so on supply a variety of contingent services. Is there any way to use distributed consensus processes to convey value transparently and securely without expensive proof-of-work methods[8]. It is possible to generate an accurate record using a completely decentralised distributed ledger and anonymous validators (proof-of-work techniques). A distributed consensus ledger with known validators and the capacity to penalise individuals who do not follow protocol, on the other hand, would perform better. Swanson demonstrates that the second scenario reduces the requirement for interpersonal trust much more than the first.

There are numerous flaws in immutable public ledgers, according to Buterin[9]. Reversibility is desirable in some instances, such as land registrations, when government-uncontrollable records run the danger of not being recognised at all. Because the government may enter the game through a public ledger with smart contracts, Buterin acknowledges that this conclusion is nuanced but not undermined. As a second point, crypto-economics has extensively researched the concept of an anonymous 51 percent assault that results from miners working together to take control of a public decentralised network. In the case of known validators, the pitfall is eliminated. Third, public ledgers have greater transaction costs, but private blockchains, with their smaller number of high-processing nodes, allow for more cost-effective transactions to be handled by them.

A blockchain-based digital economy, according to Underwood, may totally restructure the digital economy. The first and initial issue of blockchain use is ensuring and sustaining trust. Because BC is a large networked time stamping system, it may also be used to gather chronological and sequence information about transactions. In order to keep track of its private securities transactions, NASDAQ relies on Linq Blockchain[10]. Financial settlement services such as post-trade issues and swaps are being implemented by the Depository Trust & Clearing Corporation in conjunction. Additionally, regulators are attracted to British Columbia's capacity to provide real-time, secure, confidential, and traceable monitoring of transactional data in real time

2. DISCUSSION

Crypto-currencies such as Bitcoin and Ethereum have the potential to change our societies in profound ways. In order to avoid utopian aspirations and the traps of technocratic thinking and predestination, the risks and advantages of its prospective uses must, nevertheless, be carefully balanced. Allowing the decentralisation of government services through permissioned blockchains is both practical and desired, since it can improve the efficiency of government services. In contrast, the dangers and downsides of decentralisation of governance through open, distributed blockchains, such as Bitcoin, outweigh the benefits

In addition to a large number of third parties and successful companies offering intermediation services, fully distributed blockchain ecosystems are characterised by severe information and power imbalances between developers and consumers. Concentration of power in the hands of key engineers and a lack of openness in decision making due to all of these reasons, existing distributed networks' egalitarian character is called into doubt, rendering some blockchain proponents' hopes unrealistic. It turns out that the concept of a blockchain-based authority is misleading, since authority is actually more subtle.

There are hence reasons to question the role of the blockchain-based governance as a great facilitator of individual power, in an absolute sense. Due to the prominent role of markets and the speculative verification

methods of fully distributed blockchains, the promise of empowering individuals is likely to remain unfulfilled. Yet another nefarious development may be hidden behind the process of devaluing public institutions, giving precedence to economics over politics, and transforming citizens into customers with the promise of more freedom and efficiency, as well as greater equality. In fact, this type of power transfer has been going on for decades, in many forms, with tremendous social and economic costs attached to it.

3. CONCLUSION

Most techno-libertarians believe that the blockchain's ability to establish consensus between participants on a wide scale is particularly important since they believe that centralised vertical authority is harmful to individual powers. It's not uncommon for them to espouse a utopian vision of a non-hierarchical, non-coercive society controlled by algorithm-based consensus, in which individuals may freely interact. A variety of additional ICT clichés have arisen in recent decades, such as "the myth of a better government" and "the idea of a savvy and empowered customer." Briefly, we'll look at reasons why blockchain governance doesn't solve either the political problem of compulsion, or the social problem of hierarchical organisations.

The fact that overthrowing the State and absorbing its functions is a profitable business cannot be overlooked when evaluating the risks and benefits of blockchain applications. While the blockchain was originally created to eliminate the need for a third party in transactions, stakeholders now involved in blockchain governance play the classical role. in which the state is replaced in some or all of its functions by a third party; even worse, these agents may deliberately pursue a divide and imperia strategy between civil society and the state in order to undermine traditional democratic order, modify existing power balances, and gain dominance in society. As global civil society explores new political and social dimensions, the challenge will be to integrate disruptive technology like blockchain with citizens' rights, equality, social cohesion, inclusion and public sector protection. A mature and multidisciplinary endeavour by all disciplines of human knowledge, with special attention to political theory, humanities, and social sciences, is required to better assess risks, advantages, and consequences of new technology.

REFERENCES

[1] F. Alfonita, “Prevalence of Crypto-currencies: A Critical Review of Their Functioning and Impact on Indian Economy,” *Comput. Ind. Eng.*, 2018.

[2] M. Milutinović, “Cryptocurrency,” *Ekonomika*, 2018, doi: 10.5937/ekonomika1801105m.

[3] S. Volosovych and Y. Baraniuk, “Tax control of cryptocurrency transactions in Ukraine,” *Banks Bank Syst.*, 2018, doi: 10.21511/bbs.13(2).2018.08.

[4] G. Hileman and M. Rauchs, “2017 Global Cryptocurrency Benchmarking Study,” *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.2965436.

[5] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system, October 2008,” *Cited on*, 2008.

[6] A. I. Joy, “THE FUTURE OF CRYPTO-CURRENCY IN THE ABSENCE OF REGULATION, SOCIAL AND LEGAL IMPACT,” *PEOPLE Int. J. Soc. Sci.*, 2018, doi: 10.20319/pijss.2018.41.555570.

[7] D. Maxwell, C. Speed, and D. Campbell, “‘Effing’ the ineffable: Opening up understandings of the blockchain,” 2015. doi: 10.1145/2783446.2783593.

[8] T. Swanson, “Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Work,” *World Agric.*, 2015.

[9] V. Buterin, “A next-generation smart contract and decentralized application platform,” *Etherum*, 2014.

[10] S. K. Lo, X. Xu, Y. K. Chiam, and Q. Lu, “Evaluating Suitability of Applying Blockchain,” 2018. doi: 10.1109/ICECCS.2017.26.