International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Research Paper on Blockchain Technology

Mr. Mayur Dayanand Kamble (Dept of MCA)
Guide: Assistant Professor Ms. Dipali Bhusari
(Dept of MCA), Trinity Academy of Engineering,
Pune, India

ABSTRACT:

Blockchain is a Peer to Peer software technology that protects the integrity of a digital piece of information. It was invented to create the alternative currency Bitcoin but may be used for other cryptocurrencies, online signature services, voting systems and many other applications. In this video we explain how it works and what makes it special.
Everyone uses paper money. When you get a 10 dollar bill you trust that it's not fake. If instead someone sent you an email saying "here's 10 dollars" you probably wouldn't trust it. But when we "transfer money", use an ATM or pay with a deposit card that's pretty much exactly what we do. We're sending money in a digital message.
To make sure no one's cheating or sending money they don't have, these "messages" go through a few trusted banks that keep a record of everything. They know how much money everyone has and deduct it properly for every transaction.
Now But this has become expensive when there is a millions of transactions around towards the world every minute. The Economist estimates that banks charged us more than 1.7 trillion dollars to process these payments in 2014. That's about 2% of the entire world economy! With blockchain we can save a lot of this cost because it lets us send money just like sending an email.
Alternately sending a lot of payment information through a few servers, blockchain uses thousands of personal computers on the internet. All transactions are copied and cross checked between every computer in a system wide accounting book called the ledger, which becomes very safe at scale.
Blockchain doesn't just allow us to create safe money online, it lets us protect any piece of digital information. This could be online Identity cards, voter ballots, contracts and many other "legal instruments", bringing bureaucracy into the 21st century.

1. INTRODUCTION:

A blockchain is just one type of distributed ledger, not all distributed ledgers necessarily employ blocks or chain transactions. The blockchain is an indestructible digital ledger for keeping track of economic transactions which can be programmed to maintain financial transactions but virtually everything that has value." Don & Alex Tapscott, authors Blockchain Revolution 2016. A blockchain (originally two-words: blockchain) is a continuously growing list of digital records in packages (called blocks) linked and secured using cryptography. A blockchain is a chain of chronological blocks. A block is an aggregated set of data that is collected and processed to fit inside it through a process called mining. When a new block is formed, it will contain a hash of the previous block, so that blocks can be a chronologically ordered chain from the first block ever generated in the entire blockchain (also called the Genesis Block) to the newly formed block. This process is repeated to grow and maintain the network. Any financial institution or government does not control this decentralized ledger. Companies such as messaging apps, critical infrastructure security, ride-sharing, cloud storage, etc. control blockchain technology.

BLOCKCHAIN APPLICATIONS:

Blockchain technology offers the potential to impact a wide range of industries. The most promising applications exist where transferring value or assets between parties is cumbersome, expensive, and requires one or more centralized organizations.

a) Financial Services :

Several stock exchanges are piloting a blockchain platform that enables the issuance and transfer of private securities. Additionally, multiple groups of banks are considering use cases for trade finance, cross-border payments, and other banking processes.

b) Consumer and Industrial Products:

Companies in the consumer and industrial industries are exploring blockchain to digitize and track the origins and history of transactions in various commodities[9].

c) Life Sciences and Health Care:

Healthcare organizations are exploring blockchain to secure the integrity of electronic medical records, medical billing, claims, and other records[10].

d) Public Sector:

Governments are exploring blockchain to support asset registries such as land and corporate shares.

e) Energy and Recourses: Ethereum is used to establish smart-grid technology, as tradable digital assets among consumers. Since all businesses track information and face the challenge of reconciling data with counterparties, blockchain technology has the potential to be relevant to everyone[11].

There are concerning how blockchain will impact the audit and assurance profession, including the speed with which it will do so. Blockchain is already impacting CPA auditors of those organizations using blockchain to record transactions. However, in the immediate future, blockchain technology will not replace financial reporting and financial statement auditing. Audited financial statements are a cornerstone of the business and play a key role in debt and equity financing, participation in capital markets, mergers and acquisitions, regulatory compliance, and the effective and efficient functioning of capital markets. Financial statements reflect management assertions.

Furthermore, An independent audit of financial statements enhances the trust for the effective functioning of the capital markets system. Any erosion of this trust may damage an entity's reputation, stock price, shareholder value, penalties, or loss of assets. Users of financial statements expect CPA auditors to perform an independent audit of the financial statements using their professional skepticism. CPA auditors conclude whether they have obtained reasonable assurance that the financial statements of an entity are due to fraud or error. Blockchains are unlikely to replace these judgments by a financial statement auditor.

However, CPA auditors need to monitor developments in blockchain technology because it will impact their clients' information technology systems. CPA auditors need to be conversant with the basics of blockchain technology and work with experts to audit the complex technical risks associated with blockchains[12].

In addition, CPA auditors should be aware of opportunities to leverage their clients' adoption of blockchain technology to improve data gathering during the audit. They should also consider whether blockchain technology will allow them to create automated audit routines[13].

The auditing profession must embrace and "lean in" to the opportunities and challenges of widespread blockchain adoption. CPA auditors are encouraged to monitor developments.

3. BASIC FEATURES OF BLOCKCHAINS:

Understanding how a blockchain works from a technical point of view, is valuable only to the extent of developing or troubleshooting one. To cohesively grasp the potential to apply blockchain technology, you must also understand the characteristics of a blockchain. It is important to note that not all characteristics listed below will apply to all blockchains[15].

The above presentation provides the necessary background to identify key characteristics and principles of blockchains. These are the following:

a) Privacy: Blockchains store no personal information and use private/ public encryption to authenticate users undertaking transactions. Mining blockchains to obtain personal information that could be sold to third parties for a profit is not feasible

b) Transparency: All blockchain metadata and information are available to all nodes and users in real-time. It is not possible to hide or redact blockchain information.51 Distributed transparency is thus feasible.

c) Pseudo-anonymity: Nodes and users do not need to provide names or personal details to be part of the network. However, full anonymity is not achieved as linking users to network activity is feasible and can thus lead to revealing their identities.

d) Integrity: This works in two ways. First, data integrity: This is also called immutability. Second, user integrity: metadata about the transactions undertaken by a node end user are recorded on the blockchain and can be linked to the user undertaking them. Users fool the network or try to complete an invalid transaction[19].

e) Security: The use of blockchains requires cryptographic tools and public/private keys by all participants, being nodes or end users

f) Distributed trust and governance: The blockchain successfully bypasses the need for a trusted central authority. Instead, trust is spread across the network. The same goes for governance mechanisms where, in principle, different types of users and nodes have the same 'political' leverage.

g) Sustainability: Built-in economic incentives provide a clear path for network economic sustainability.

a) **Open source**: Software required to use blockchains is freely available to all, including cryptographic tools. Furthermore, users with adequate capacities can actually help enhance and refine blockchain technologies, in addition to catching bugs. This can also facilitate the spread of blockchain innovations.

4. BLOCKCHAIN LIMITATIONS:

As an emerging technology, blockchains face limitations that might prevent widespread adoption in the financial sector and other areas. These can be summarized as follows:

a) Scalability: today, the Bitcoin blockchain can only add a new block of transactions every ten minutes or so. This translates into a low volume of transactions per second (less than five), a far cry from the volumes reported by traditional transactional networks[21].

b) Block size: The above is the small block size defined by the original Bitcoin source code. The maximum size for each block is one megabyte which can accommodate 2,200 transactions. Increasing block size is currently under discussion but a final decision has been reached[22].

c) High costs: Miner nodes use sophisticated and expensive hardware to run proof-of-work algorithms. Consequently, only certain nodes in the network can effectively compete in this process, even though in theory all nodes have the software required to mine the network. Nakamoto's notion of "one-CPUonevote" is no more as hardware and electricity costs prevent most nodes.

d) Cryptography: The use of cryptographic tools is still and the average Internet user cannot be expected to embrace its use in the short term.

e) Complexity: Blockchain technologies appear almost incomprehensible to the average person and the tech speaking around does not help. Only a selected few understand the technology.

f) Environmental impact: A by-product of the above is also proof of work's inefficiency in terms of energy resources. Some estimates on energy consumption suggest that, by Spring 2017, Bitcoin was comparable to that of 280,000 US households per year.

g) Bandwidth: Full nodes that want to be active in the network must have access to the right Internet bandwidth. Slow, unreliable connections are not welcome, especially when the current size of the blockchain is over 120 Gigabytes[24].

h) Centralization: Mining is now centralized with a few nodes controlling a large share. 55 Figure 6 below depicts market shares of the top miner nodes or companies. Note that the top five companies alone control over percent of the market.

i) Usability: Blockchain technology requires public and private keys by end users and nodes. While existing wallet software has come a long way, losing private keys is still a serious risk. None of the existing solutions are physical theft and only a few can protect users from malware.

j)Immutability as liability: If the blockchain is hacked or the software code has a bug that allows a particular exploit, its immutability can become a liability. This was the case for example with the Ethereum hack of last year where one rogue node was over 64 million dollars.

The blockchain technology ecosystem is proactive and working to address some of these limitations. The fact that the code is open source is critical here. On the other hand, changes to both the code and blockchain operations can only be accomplished by either consensus or if a majority of nodes agree on a way forward.

5. CONCLUSIONS :

The Blockchain technology is now one of the useful and versatile concern for our world, Due to the large facilities in most of the systems in the different industries, but in spite of everything it is new and it`s major implementation is little studied issue on practice. Todays Blockchain technology promises us the bright future for information technology without the fraud and any deception. due to the some benefits of the Blockchain technology. The challenges of the Blockchain are large, but the results of the Blockchain using have a greater preponderance than disadvantages. It is necessary to keep exploring the Blockchain development and application in the different areas for the nearest future, because this new technology can help to solve many difficult problems, which are disturbing and preventing correctly systems work. We have discussed in this paper basic features of blockchain technology and security issues of blockchains.

REFERENCES:

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] Shuai Wang , Jing Wang, Xiao Wang , Member, IEEE, TianyuQiu, Yong Yuan , Senior Member, IEEE,LiweiOuyang, YuanyuanGuo, and Blockchain Powered Parallel Healthcare Systems Based on the ACP Approach2329-924Xc 2018 IEEE.

[5] . ZainabAlhadhrami, Salma Alghfeli, Mariam Alghfeli, Introducing Blockchainsfor Healthcare2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA).

[6] K. Malasri, L. Wang. Design and Implementation of Secure Wireless Mote Based Medical Sensor Network. Sensors 9: 6273-6297,
2009A. Azeta, D. O. A. Iboroma, V. I. Azeta, E. O. Igbekele, D. O. Fatinikun, and E. Ekpunobi, “Implementing a medical record system with biometrics authentication in e-health,” in 2017 IEEE AFRICON, Sept 2017, pp. 979–983.

[7] P. Belsis and G. Pantziou. A k-anonymity privacy-preserving approach in wireless medical monitoring environments. Journal Personal and Ubiquitous Computing, 18(1): 61-74, 2014.

[8] B. Jana and J. Poray, "A performance analysis on elliptic curve cryptography in network security," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-7.doi:10.1109/ICCECE.2016.8009587

[9] 11. S. Mitra, B. Jana, and J. Poray, "A novel scheme to detect and remove black hole attack in cognitive radio vehicular ad hoc networks(CR-VANETs)," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-5. doi: 10.1109/ICCECE.2016.8009589

[1] 12. B. Jana, S. Mitra and J. Poray, "An analysis of security threats and countermeasures in VANET," 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, 2016, pp. 1-6. doi: 10.1109/ICCECE.2016.8009588

[2] 13. S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, 2017, pp. 1-7. doi:10.1109/OPTRONIX.2017.8350006

[3] 14. B. Jana, J. Poray, T. Mandal and M. Kule, "A multilevel encryption technique in cloud security," 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), Nagpur, 2017, pp. 220- 224. doi: 10.1109/CSNT.2017.8418541

[4] 15. Jana B., Poray J. (2018) A Hybrid Task Scheduling Approach Based on Genetic Algorithm and Particle Swarm Optimization Technique in Cloud Environment. In: Bhateja V., Coello Coello C., Satapathy S., Pattnaik P. (eds) Intelligent Engineering Informatics. Advances in Intelligent Systems and Computing, vol 695. Springer, Singapore

[5] 16. Jana B., Chakraborty M., Mandal T. (2019) A Task Scheduling Technique Based on Particle Swarm Optimization Algorithm in a Cloud Environment. In: Ray K., Sharma T., Rawat S., Saini R., Bandyopadhyay A. (eds) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol 742. Springer, Singapore

[6] 17. Jana, Bappaditya and Chakraborty, Moumita and Mandal, Tamoghna and Kule, Malay, An Overview on Security Issues in Modern Cryptographic Techniques (May 4, 2018). Proceedings of the 3rd International Conference on Internet of Things and Connected
Technologies (ICIoTCT), 2018 held at Malaviya National Institute of Technology, Jaipur (India) on March 26-27, 2018. Available at SSRN: https://ssrn.com/abstract=3173527 or http://d x.doi.org/10.2139/ssrn.3173527

[7] 18. Jana B., Poray J. (2016) VANET: OVERVIEW, SECURITY ISSUES AND CHALLENGES, International Journal of Engineering Research-Online, Vol-4, Issue-2, Pages-451-459, http://www.ijoer.in

[8] 19. M Chakraborty B. Jana, T. Mandal, and M. Kule, " A Performance Analysis of RSA Scheme Using Artificial Neural Network " 2018 9th International Conference on Computing, Communication and Networking Technologies (ICT)), Bengaluru, 2018, DOI:
10.1109/ICCCNT.2018.8494032

[9] 20. Mandal, Tamoghna and Jana, Bappaditya and Mitra, Saptarshi and Poray, Jayanta, A Study on Risk Assessment in Information Security (October 5, 2018). Available at SSRN: https://ssrn.com/abstract=3261593 or http://dx.doi. org/10.2139/ssrn.3261593

[10] 21. M Chakraborty B. Jana, T. Mandal, and M. Kule, " A Performance Analysis of RSA Scheme Using Artificial Neural Network " 2018 9th International Conference on Computing, Communication and Networking Technologies (ICT)), Bengaluru, 2018, DOI:
10.1109/ICCCNT.2018.8494032

[11] 22. M. Chakraborty, B. Jana, T. Mandal and M. Kule, "A Performance Analysis of RSA Scheme Using Artificial Neural Network," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore, 2018, pp. 1-5. doi:10.1109/ICCCNT.2018.8494032

[12] 23. S. Mitra, B. Jana, and J. Poray, "Implementation of a Novel Security Technique Using Triple DES in Cashless Transaction," 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), Kolkata, India, 2017, pp. 1-6. doi: a10.1109/ICCECE.2017.8526233

[13] Iuon-Chang L., Tzu-Chun L., 2017, " A Survey of Blockchain Security Issues and Challenges ", available : http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns2017-v19-n5- p653-659.pdf

[14] Dusko K., 2018, " Impact of Blockchain Technology Platform in Changing the Financial Sector and Other Industries " , available:http://repec.mnje.com/mje/2018/v14- n01/mje_2018_v14-n01-a18.pdf

[15] Roger W., Christian D., Conrad B., 2017, " Scalable Funding of Blockchain Micropayment Channel Networks ", available : http://drops.dagstuhl.de/opus/volltexte/2017/7363/ pdf/dagrep_v007_i003_p099_s17132.pdf

[16] George C ., 2017, " Bitcoin – A Brief Analysis of the Advantages and Disadvantages ", available : http://www.globeco.ro/wpcontent/uploads/vol/split/vol_5_no_2/geo_2017_vol5_ no2_art_008.pdf

[17] Atul K., Arpit G., 2017, " BLOCKCHAIN: An analysis on next-generation internet ", available : http://dx.doi.org/10.26483/ijarcs.v8i8.4769