2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET – SIP)

2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP) | 979-8-3503-4842-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICETET-SIP58143.2023.10151573

Review based on Blockchain and Financial Transactions related to Cryptocurrencies across Globe

Dr. S.V. Sonekar
Department of Computer Science and Engineering
J D College of Engineering and Management
Nagpur, India
srikantsonekar@gmail.com

Saikiran Bejjaniwar
Department of Information Technology
J D College of Engineering and Management
Nagpur, India
saibejjani@icloud.com

Shejal Dandekar
Department of Information Technology
J D College of Engineering and Management
Nagpur, India
shejaldandekar2002@gmail.com

Sarthak Pal
Department of Information Technology
J D College of Engineering and Management
Nagpur, India
sarthakpal3210@gmail.com

Pratik Karwade
Department of Information Technology
J D College of Engineering and Management
Nagpur, India
karwadepratik11@gmail.com

***Abstract*—Blockchain is one of the most interesting and exciting field of technology today it provides a decentralized network for anyone who is willing to store data on it as blockchain is relatively new there is still experiments going on it to reveal its true potential. One of the applications of blockchain which has gone incredibly popular is cryptocurrency and also blockchain payment system. In today's blockchain payment system there are few components which are required for a successful transaction such as nodes, ledger, wallet, nonce and hash. Payment gateways are one of the first blockchain application that provide a decentralized way to do transactions we will also discuss some of the ledger applications of blockchain. We carefully selected the most recent research papers in this review paper. We will be reviewing various research paper and they take on blockchain technology.**

Keywords—Blockchain, cryptocurrency, Bitcoin, smart-contract, decentralized

I. INTRODUCTION

Any software in the world can be categorized into two systems first being a centralized system and second being a decentralized system. [1] Centralized system uses client/ server active there are multiple nodes that are connected to a central server, this is commonly used network architecture as it is easy to secure and service the server. Decentralized system are the types of system that has been gaining a lot of popularity because of various cryptocurrencies such a Bitcoin, Ethereum, Litecoin etc.

In a decentralized system every node on every computer makes its own decision and the final output of the system is calculated upon the aggregate of all the individual node, every node of the decentralized system have a copy of all the past transactions in it so that means even if you change the log of transaction you have to individually change every node within the system [2]. Its advantages are more transparency throughout the system also secure database management. As this paper focuses on blockchain technology we will be exploring several research papers on blockchain technology and its applications the very first major commercial use of blockchain technology was Bitcoin created by a guy using the alias name of Satoshi Nakamoto, He created Bitcoin as a decentralized way of transaction. Bitcoin has no physical bank or even a currency all its value and worth is only in digital format. The reason why Bitcoin was so successful was because of its decentralized nature as it provides transparency to all its users which provides a sense of security and reliability to them. Aside from cryptocurrencies blockchain also has a variety of applications to them it's current potential is limitless.

II. LITERATURE SURVEY

There was a thorough discussion of 25 research publications that are linked to blockchain applications. The papers were carefully selected from the internet database, Google Scholar, based on how well they could be used in actual situations. The Research papers are searched by using keywords like "blockchain", "cryptocurrencies, “Bitcoin”, “smart contract” and “decentralized” which produced roughly (31,000 approx.) results, 25 paper works were selected for classification. Since the unknown developer Satoshi Nakamoto originally published the blockchain technology in 2008, there are undoubtedly a lot more articles on the topic. It is also important to note that blockchain has captured the attention of academics since it offers the chance to collectively create and maintain transactions distributed ledger in the network.

[3], [4], [5], [6] and [7]: - These 5 Research papers entitles that Healthcare is one industry where blockchain technology has enormous potential since it can help integrate fragmented systems, improve the quality of electronic medical data, and take a more patient-centric approach to healthcare systems. Blockchain technology makes it possible to have a distributed, decentralized ecosystem without the need for a centralized power. Transactions are secure and reliable because of the application of cryptographic concepts. Blockchain technology has dominated several industries in recent years largely because cryptocurrencies are so well-liked. Blockchain technology makes it possible to have a distributed, decentralized ecosystem without the need for a centralized power.

[8] and [9]: - Blockchain offers new possibilities for developing new types of digital services. When studying, the topic is still emerging. It primarily focuses on technical and legal issues rather than exploiting them. A source of

979-8-3503-4842-2/23/$31.00 ©2023 IEEE

blockchain technology for proposing designs for new electronic voting systems that can be used in Elections for local or national councils. Blockchain-based systems are secure, reliable, and anonymous. It helps increase voter numbers and increase people's trust in government.

[10] Shreekanth M Prabhu, Natarajan Subramanyam, Ms Krishnan, P Shreya, Ms Sachidananda "Decentralized Digital Currency System using Merkle Hash Tree" arXiv preprint arXiv:2205.03259, 2022: - This Paper entitles a Decentralized Digital Currency System(DDCS) that makes use of Merkle hash tree as an authenticated data structure. The framework of this DDCS uses Ledger-less, distributed, peer-to-peer Architecture. The money utilized in this system, called " δ-Money " is designed to replace actual physical money and includes built-in security characteristics that compete with those of cryptocurrencies.

[11], [12], [13], [14], [15], [17] and [18]: - These 7 Research Papers entitles how blockchain is must choice, domain or new technology to be implement in the financial sector. Although, Blockchain cannot be used for the transaction of a physical currency. It is used for the transaction of cryptocurrencies across globe. Initially, cryptocurrencies (digital money) used blockchain technology as its open transaction ledger. Beyond cryptocurrencies, however, blockchain technology has lately been taken into consideration for a wide range of additional applications because to its unique combination of decentralization, security, transparency, and anti-tampering features. Such characteristics are especially helpful for a range of significant problems encountered in the financial sector. Therefore, by changing how various financial services are provided, blockchain technology has the ability to completely transform the financial sector. In this article, we present a list of five different financial industry use cases that the application of blockchain technology is predicted to fundamentally alter.

[4] and [7]: - These paper entitles why India should go for digital payments instead of physical money transaction. This action was taken in order to make India a cashless economy, get rid of black money in India, ensure equitable tax collection for undeclared cash, and a host of other goals. Millions of Indians now use digital payments to pay for everything from regular energy bills to shopping. This Research paper [4] focuses on online transaction systems that leverage blockchain technology and its characteristics, specifically distributed databases, and talks about Advanced Encryption Standard (AES), and Secure Hash Algorithm 256 (SHA-256) to be used in the blockchain based payment system. As a result, a more dependable and secure model for a blockchain-based digital payment wallet service has been created.

[5]: - This paper offers a unified energy trading and payment settlement model (UBETA) that connects three different types of energy markets. It is based on a permissioned blockchain. The Istanbul Byzantine Fault Tolerance (IBFT) consensus algorithm and the Hyperledger Besu business Ethereum Blockchain form the foundation of the UBETA system. We used particular performance measures (read/write transaction latency, read/write transaction throughput, and fail rate) to compare the performance of the proposed IBFT-based system with three existing systems (Ethereum Clique, Ethereum Proof of Work, and Hyperledger Fabric's Raft).

III. Applications of Blockchain

This Paper entitles some of the major few areas of interest were blockchain can be implement because of its decentralized, censorship resistance, immutability, Trust lessness and Transparent nature in order to make the system more efficient and faster.

A. Finance and Business

One of the major commercially successful application of blockchain is cryptocurrency. The earliest form of cryptocurrency is Bitcoin. Bitcoin is a decentralized currency which doesn't have any physical form in the world [4][2], it does not belong to any banks or institution. Similar to bitcoin Ethereum is also one of the most successful cryptocurrencies which makes use of smart contracts [9].Table 1 represents current existing cryptocurrency system.

From the Fig. 1 given, we can identify each leaf node as a transaction of each block present in the system[6]. Each transaction has its own Hash (A Hash is a numeric value that a hashed block header which is used to identify individual block in a blockchain based system), and it is very difficult to

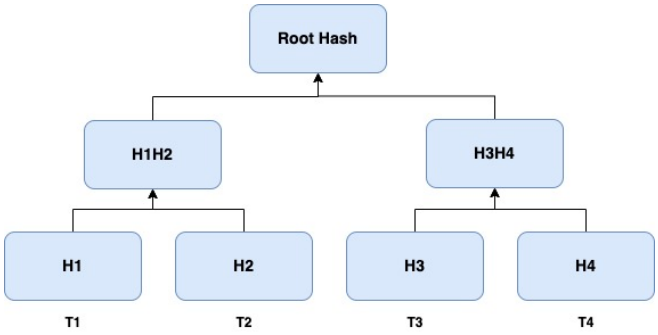

Fig.1 Merkle Hast tree

TABLE I Current existing cryptocurrencies

Cryptocurrency	Year	Hash Function	Mining Method
Bitcoin	2008	SHA-256	Find all possible nonce values by computing proof of work and other users agree and verify the proof.
Litecoin	2011	Scrypt	Similar to Bitcoin (proof of work)
Peercoin	2012	SHA-256d	proof of work and proof of stake
Primecoin	2013	Cunningham Chain	proof of work
Ripple	2014	EC digital signature	consensus system
Ethereum	2014	Ethash	proof of work
Permacoin	2014	Floating digital signature	proof of retrievability
Blackcoin	2014	Scrypt	proof of stake
Auroracoin	2014	Scrypt	proof of work
Darkcoin	2014	X11	proof of work

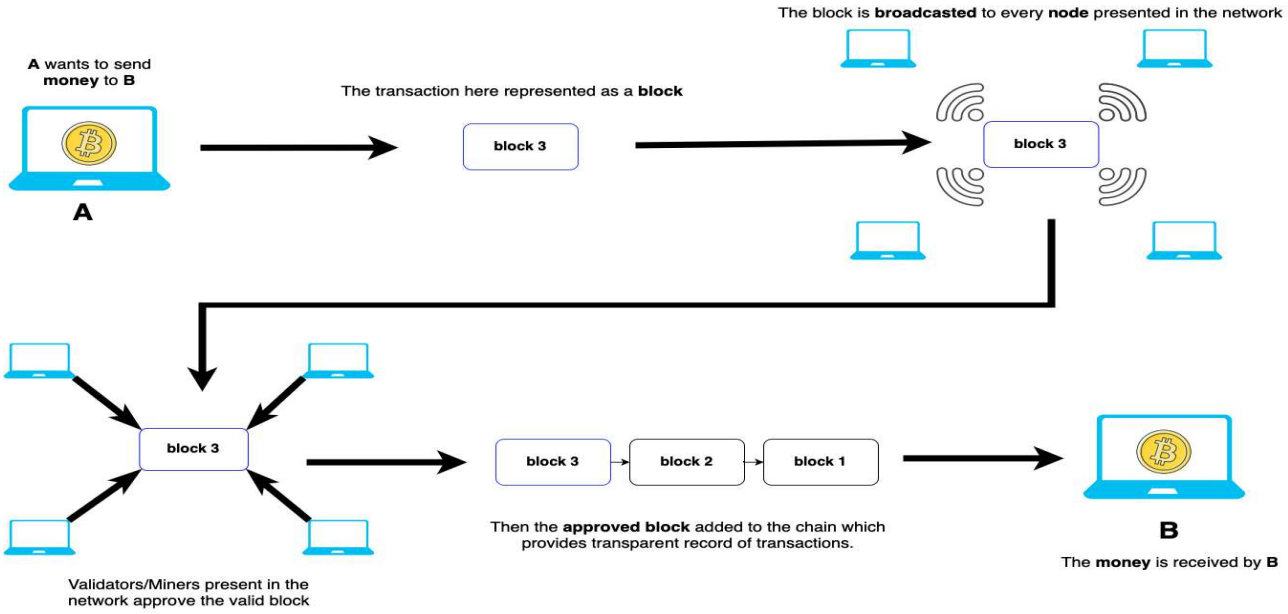

Fig.2 Generalized block diagram of a Blockchain based payment system.

track them because there are so many transactions inside a block and There are so many block present in the system so it can become very difficult to track them all and to manage them all. So here is Merkle Tree arrive to solve these issues.

Merkle Hash Tree is an important part of decentralized digital currency system based on blockchain. Merkle Hash Tree is an authentic data structure which makes use of hash functions. The principle of Merkle Hash is that it predicated on the notion that the signer and the verifier can share the tree's root in a secure and reliable manner to ensure that there is no malicious attack should not happen in the middle of the transaction and in order to check consistency of each data block. Only the nodes that are engaged in the authentication path of the data block under consideration have their hashes transmitted by a signer. The Merkle tree offers the benefits of holding lot of objects (for example hash of any transaction) all one needs to remember the root hash. From the research paper [7]. We have found out that in their system they used one operation called O (log n) – where n is the height of the hash tree it can determine whether a block is a member of tree or not.

The Fig. 2 give us a brief idea of how Blockchain payment system works. Suppose there are two peoples A and B who wants to do an online Bitcoin transaction through a Blockchain based payment system. So here in the system each transaction is represented as a block. So, for the new transaction there is going to be an addition of new block in the system. To do the transaction, here the new block is going to broadcast to each and every node present in the system. A node is one of the computes or we could say validators that runs the blockchain's software to verify and preserve the whole history of transactions on the network and also maintains the allocations of new node that can be easily distinguished from other nodes in the network by being given a special identification by each one. With the availability of smart contracts, it creates an if-then condition which means that if the new block is valid then it can only be added in the system otherwise the transaction will be failed or the block should have majority vote. So, when the new block is requested to be added in the system, the validators or nodes present in the system approved the block if it's valid according to them. Then the block is added in the system and the money (Bitcoin) moves from Person A to Person B. And hence, the transaction completes with full security and with minimum charges.

B. Healthcare

Due to Blockchains Decentralized nature, hospitals can share and manage medical history in the form of Electronic Medical Record (EMR) data which allows automatic updating and sharing of medical information of patients and can predict future disease based on their symptoms. Enables all the health care[1], researchers, doctors and institutions to share all the information regarding any patient securely which can be only accessed by authorized users. Sharing all the data will benefit the patients remained asleep as all the doctors will be able to give correct treatment based on their medical history[1]. A good communication between different healthcare professionals involved in the care of the same patient can help prevent errors, make it easier to diagnose patients, and provide them with individualized treatment.

C. Voting System

Blockchains immutable nature makes it useful for voting system as with traditional Voting system there are high chances of security threats such as error, malicious manipulation and alteration of votes, malware attacks, etc. [10] In traditional voting system, we cannot verify if our vote is registered to desired candidate or not. Implementation of blockchain in Voting System can make the voting process more secure, reliable, transparent and immutable. In blockchain every vote is stored as a transaction and it gives a receipt (form of a Transaction Id) and you can use it to track whether your vote is secured or not. From the Fig. 3 we get a brief idea about how the blockchain based Voting system works. If a Voter wants to vote through a blockchain based Voting System. So, there are some authentications which will happen because of the smart contract [10] available in the system which provides an If-then condition which means that if all the condition satisfies then the new Vote will be

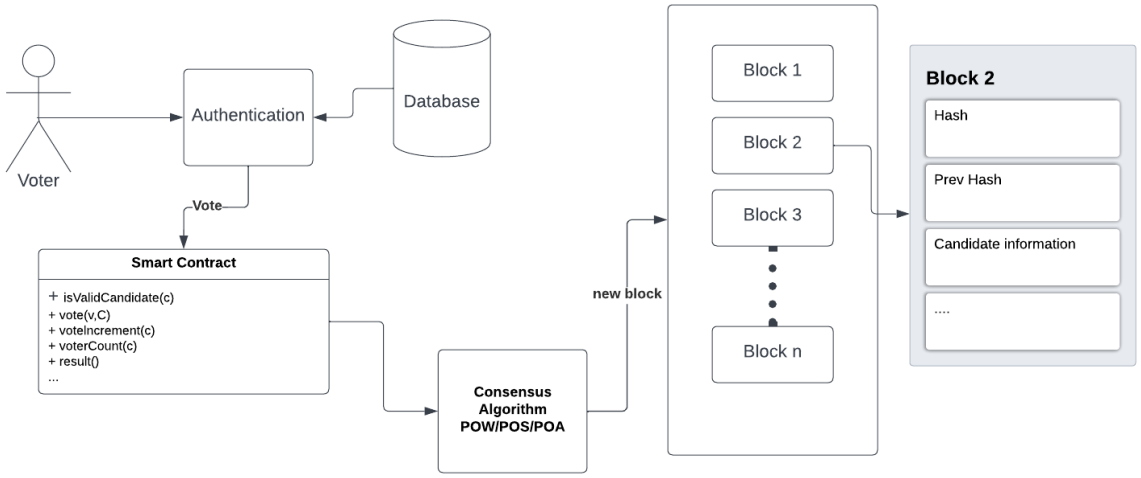

Fig.3 System architecture of Electronic Voting System.

casted. So, there are several layers to authentication first it checks

whether the voter is a valid candidate or not it checks their nationality, age, voter ID and other important information and then it decides whether to allow the person to vote or not, then as the person is voting, it increments the total vote count by one then it counts the total amount of vote and then it shows the result.

All this processing is dictated by consensus algorithm which adds all the information in the form of a new block which is then connected to the main block.

TABLE II SUMMARIZES THE BLOCKCHAIN APPLICATION AND SHOWS BLOCKCHAIN ADAPTATION EXAMPLES IN REAL LIFE.

Sr. No.	Application	Description	Examples
1	Government	Helps to provide government operation in secure, transparent and efficient way.	Dubai Blockchain Strategy, Switzerland CryptoValley
2	Energy management	Helps to organize the energy operations such as generation, distributions and selling between parties.	lo3energy, Sun Contract
3	Supply chain management	Blockchain achieves management of supply chain transactions in a decentralized, and secure way.	Fluent, Everledger, Skuchain, Provenance
4	Human Resources	Managing hiring employees in a company	Colony.io, Chrono.tech
5	Health care	Stores and shares sensitive data and medical records	Gem , Tierion
6	Financial and banking	Blockchain technology al- lows the parties to make financial and money transferring in different locations	ABRA, Barclays
7	Online music	Provides ways to music artists to collect their sell- ing money directly from their fans with no need to give a large percentage of sales to music distribution companies	Mycelia , Ujo Music
8	Retail	Decentralized blockchain retail utilities connect buyers and sellers without a third party which making purchasing operation easy, reliable, and fast.	OpenBazaar , OB1
9	Online storage	Helps to reduce attack that are associated with online and cloud storage and cancel the central provider services.	Online Data Storage
10	Forecasting	Provides away for prediction that is different from the traditional way in forecasting	Augur

IV. APPLIED ALGORITHM

All entities in a decentralized network must agree on transactions on the network, verify blockchain validity, and determine if this is the case.

Whether to add to the blockchain and which block to add next is also determined. In Bitcoin, a decentralized network lacks centralization and trust between network entities, requiring all entities to agree on transaction history. The challenge here is how all these entities agree on the correct state of the data set and how they all come to consensus. There are different implementations of consensus mechanisms for consensus algorithms used in different blockchain applications, and they differ in various terms such as decentralization. This section summarizes current consensus algorithms used in Blockchain Technology.

A. Proof of Work

This consensus algorithm will be used to select miners for the next generation block. Bitcoin uses this Proof of Work consensus algorithm. The core idea behind this algorithm is to solve complex mathematical puzzles and provide

solutions in an easy way. This mathematical puzzle requires a lot of computing power, so the node that solves the puzzle as soon as possible will mine the next block.

B. *Proof of stake*

This is the most popular alternative to PoW. Ethereum has moved from PoW to PoS consensus. Rather than investing in expensive hardware to solve complex puzzles, in this type of consensus algorithm, validators invest in the system's coins by locking a portion of them as stake. After that, all validators start validating blocks. Validators place bets and validate blocks when they find blocks that they believe can be added to the chain. Based on the blocks actually added to the blockchain, all validators will receive a reward proportional to their wager, and their wager will increase accordingly. Ultimately, validators are selected to generate new blocks based on their financial stake in the network. Thus, PoS encourages validators to reach consensus through its mechanism of incentives.

C. *Proof of Activity*

A Proof of Activity consensus algorithm has been proposed. This is a hybrid approach that includes Proof of Work and Proof of Stake. Starting with Proof of Work, where minors can mine blank templates without transactions, moving to Proof of Stake. There, validators select blocks to sign and rewards are distributed to proof-of-work miners and stakers.

These are some of the most important consensus algorithms.

V. Conclusion

The stated research papers provide insights for the current blockchain research areas and its applications in the real world. The number of research articles has been comprehensively culled from various online databases.

From the research, we conclude that Blockchain is a relatively new technology that is not yet universal in all industries, but it is slowly gaining momentum. Several industries are continually looking for new ways to use blockchain technology, which has been available around us a decade ago, to implement and support this technology in their operations. There is also an increasing need for the data protection, access, transparency, and integrity that blockchain can offer as the amount of digital data used in our lives increase. Once blockchain becomes mainstream, it could become a powerful data democratizer that will encourage transparency and ethical business tactics. Also, the world's blockchain applications are on the rise, resulting in faster transactions, greater transparency and security, and lower costs.

The benefits of blockchain technology are its quickness, dependability, and openness. To add a transaction to the blockchain, consensus is necessary. The security of financial transactions, potential criminal activities, legal obstacles, and financial hazards are some difficulties. Although it cannot address every issue, blockchain is a promising technology when implemented properly. So, for individuals who are thinking about incorporating a blockchain into their system or application, doing so could be a positive step.

Although blockchain technology is still relatively new and not widely used in various industries, the assessment reveals that it is gaining traction. A wide range of sectors are investigating how to leverage blockchain technology to enhance operations and handle issues with data protection, access, transparency, and integrity. While blockchain has advantages like speed, durability, and openness, it is not a cure-all and can come with concerns in the areas of money, law, and security. But, as its uses grow, blockchain has the potential to become a formidable data democratizer that promotes openness and moral corporate practices. This will lead to speedier transactions, more transparency and security, and cheaper prices. Blockchain may therefore be a promising technology in the future if properly applied.

References

[1] E. Chukwu and L. Garg, “A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations,” in IEEE Access, vol. 8, pp. 21196-21214, 2020, doi: 10.1109/ACCESS.2020.2969881.Judmayer, Aljosha et.al.

[2] Christian Jaag & Christian Bach, “Blockchain Technology and Cryptocurrencies: Opportunities for Postal Financial Services,” Part of the Topics in Regulatory Economics and Policy book series (TREP) pp 205–221.

[3] Kuldeep Hule, Arjun Dashrath, Ashwin Gupta, “Self-Mining Blockchain Mobile Unified Payment Interface” 2021 International Conference on Computing, Communication and Green Engineering (CCGE), 1-7, 2021.

[4] KS Thakre, Gargi Kulkarni, Prajwal Sameer Deshmukh, “Digital India Digital Economy Using Blockchain Technology,” Blockchain for Smart Systems, 123-153, 2022.

[5] Juhar Abdella, Zahir Tari, Adnan Anwar, Abdun Mahmood, Fengling Han “An architecture and performance evaluation of blockchain-based peer-to-peer energy trading,” IEEE Transactions on Smart Grid 12 (4), 3364-3378, 2021.

[6] Shreekanth M Prabhu, Natarajan Subramanyam, Ms Krishnan, P Shreya, Ms Sachidananda, “Decentralized Digital Currency System using Merkle Hash Trees.” arXiv preprint arXiv:2205.03259, 2022.

[7] Dr. Ranjith P.V., Dr. Swati Kulkarni, Dr. Aparna Varma, “A Literature Study Of Consumer Perception towards Digital Payment Mode in India,” Psychology and Education (2021) 58(1): 3304-3319.

[8] Geetanjali Sharma and Jai Deep Pandey, “Transaction processing time in Unified payment interface (UPI) using M|M|1 queuing model,” International Journal of Advanced Research in Engineering and Technology (IJARET)4Volume 12, Issue 5, May 2021, pp. 220-227, Article ID: IJARET_12_05_020.

[9] Zhang, L, Xie, Y, Zheng, Y, Xue, W, Zheng, X, Xu, X, “The challenges and countermeasures of blockchain in finance and economics,” Syst Res Behav Sci. 2020; 37 691–698. https://doi.org/10.1002/sres.2710

[10] U. Jafar, M. J. A. Aziz, and Z. Shukur, “Blockchain for Electronic Voting System—Review and Open Research Challenges,” vol. 21, no. 17, p. 5874, Aug. 2021, doi: 10.3390/s21175874.

[11] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," in IEEE Access, vol. 7, pp. 45201-45218, 2019, doi: 10.1109/ACCESS.2019.2908780.

[12] V. J. Morkunas, J. Paschen, and E. Boon, ‘‘How blockchain technologies impact your business model,’’ Bus. Horizons, vol. 62, no. 3, pp. 295–306, May 2019.

[13] M. W. L. Moreira, J. J. P. C. Rodrigues, V. Korotaev, J. Al-Muhtadi, and N. Kumar, ‘‘A comprehensive review on smart decision support systems for health care,’’ IEEE Syst. J., vol. 13, no. 3, pp. 3536–3545, Sep. 2019.

[14] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Danie, and B. Amaba, ‘‘Blockchain technology innovations,’’ in Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON), Jun. 2017, pp. 137–141

[15] R. Guo, H. Shi, Q. Zhao, and D. Zheng, ‘‘Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,’’ IEEE Access, vol. 6, pp. 11676–11686, 2018.

[16] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar, ‘‘BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications,’’ IEEE Trans. Netw. Sci. Eng., early access, Dec. 25, 2019.

[17] H. R. Hasan and K. Salah, ‘‘Proof of delivery of digital assets using blockchain and smart contracts,’’ IEEE Access, vol. 6, pp. 65439–65448, 2018.

[18] S. Krishnamurty, ‘‘Blockchain for business,’’ Wilmott, vol. 2018, no. 96, pp. 18–19, 2018.

[19] J. Vora et al., ‘‘BHEEM: A blockchain-based framework for securing electronic health records,’’ in Proc. IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 2018, pp. 1–6.

[20] Randall, D., Goel, P. and Abujamra, R., 2017. Blockchain applications and use cases in health information technology. Journal of Health & Medical Informatics, 8(3), pp.1-17

[21] Abraham, Ittai, and Dahlia Malkhi. "The blockchain consensus layer and BFT." Bulletin of EATCS 3.123 (2017).

[22] Coleman L. Smart contracts: 12 use cases for business and beyond. Retrieved December. 2016;23:2018.

[23] Pilkington, Marc. "Blockchain technology: principles and applications." Research handbook on digital transformations. Edward Elgar Publishing, 2016. 225-253.

[24] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz and S. Kot, "Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review," in IEEE Access, vol. 10, pp. 122679-122695, 2022, doi: 10.1109/ACCESS.2022.3223370.

[25] Kamilaris, Andreas, Agusti Fonts, and Francesc X. Prenafeta-Boldú. "The rise of blockchain technology in agriculture and food supply chains." Trends in Food Science & Technology 91 (2019): 640-652.