# A Survey on Blockchain Applications and their Security Challenges

**B.Vaidehi[1], S.Rajeashwari [2], Dr.K.Arunesh[3]**

*[1]Department of Computer Science, Sri.S.Ramasamy Naidu Memorial College, Sattur, Tamil Nadu*
*[2]Research Scholar, Sri.S.Ramasamy Naidu Memorial College,Sattur, Tamil Nadu*
*[3]Department of Computer Science, Sri.S.Ramasamy Naidu Memorial College,Sattur, Tamil Nadu*

## ABSTRACT

*Blockchain has received massive attention recently due to its characteristics of enhanced security, decentralization, improved traceability tamper-proof, and transparency. Many banks, Internet companies, car manufacturers, and even governments worldwide have incorporated or started considering blockchain to improve the security, scalability, and efficiency of their services. However, there is a significant concern about blockchain's performance, since blockchain back-and-forth its performance in a completely distributed feature, which enlarges its security. The blockchain concept provided an essential part of this decentralization together with hash-based proof-of-work, public-key cryptography, and peer-to-peer network. In this article, the widespread blockchain technology for academic research has been analyzed. And, the challenges of implementing Block chain and privacy security issues have been also discussed.*

***Keywords -Blockchain, Decentralization, Cryptocurrency, Blockchain concepts, Blockchain applications.***

## I. INTRODUCTION

In recent years, blockchain technology has attracted computer scientists and experts from diverse sectors, including finance, real estate, healthcare, and transitive energy. A blockchain is an increasingly long list of records (known as blocks) that are linked using cryptography. Each block contains a cryptographic hash from the preceding block, a timestamp, and transaction data that is represented as a Merkle tree. A blockchain is well known for the functionality of immutable data.

It is an open and distributed ledger running over a peer-to-peer (P2P) network that can manage transactions for multiple entities efficiently without a middleman and in a verifiable and traceable way.

Blockchain technology is the most popular in recent years because of its decentralized, peer-to-peer transaction and immutable properties. It is a digital ledger, which available to all the users present in the network.

The Bitcoin plan has powered other apps [3] [2] and blockchains that are discernible by the open and are widely used by cryptocurrencies. Blockchain is considered a kind of staggered rail [6]. Private Blockchains have been proposed for commerce utilize but Computerworld called thepromotion of such privatized blockchains without appropriate security demonstrate "wind oil".[7] In any case, others have contended that permissions blockchains, in the case carefully planned, may be more decentralized and thus more secure in hone than authorization fewer ones.[4][8]

In modern industry, digital information flows from one end to the other end of an unreliable transmission channel. Here, confidentiality and confidentiality can be a major preoccupation. Blockchain innovation provides safe peer-to-peer communication. In Blockchain innovation exchange is freely accessible for perusing, but none can adjust the exchange once it is recorded. Extensive writing research has been done and it has been found that Blockchain is used in many valuable application areas. Creators [7] indicate Blockchain may be a probabilistic state machine and is not useful where finality decisions are required. Currently, Blockchain innovation is one of the main applicants to investigate areas, but it needs specialized points of interest to form a highly updated in almost every area. The investigative articles are classified in the astute application. This paper, moreover clarified issues related to the usage of totally different applications of Blockchain innovation.

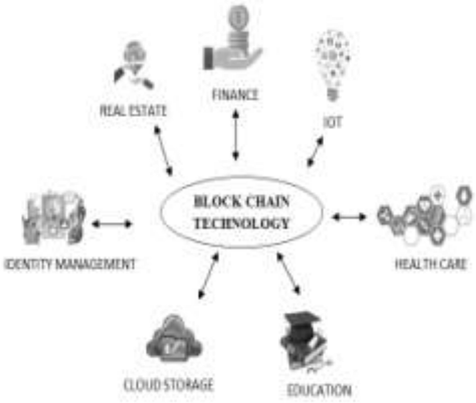
## II. SCIENTIFIC BACKGROUND

Blockchain innovation is decentralized and peer-to-peer communication. It is additionally freely accessible like a computerized record. It can be connected to put away information or exchange in a trusted environment without the third party sodalities. At first, the Blockchain keyword is opted to amass the papers from five specialized databases; they are IEEE Xplore, ScienceDirect, ACM Advanced Library, Web of Science, Inderscience. Within the first stage 751 investigate articles have been considered. We eliminate 526 articles after perusing the unique. Within the moment stage, we considered full paper and once more perform a few disposals. The last 153 articles are culled from the study. Out of 153 articles, integrate up to 106 numbers articles are applied predicated and 20 numbers papers are predicated on security aegis. These five databases sufficiently cover Blockchain innovation and give a wide visual perception of subsisting inquire about.

## III. APPLICATIONS OF BLOCKCHAIN TECHNOLOGY

Blockchain was originally introduced to control Bitcoin but now evolved for different applications.

### *A. Health Care*



Patients and healthcare Information need to be maintained with high security. Patients should be able to access and manage their health information anywhere in the world securely. Blockchain technology plays a vital role in solving most of the challenging issues like accessing and sharing patient medical records, medical data management, and safe retrieval of the massive amount of personal health data, which in turn, improve the quality of treatment and improve health outcomes. Blockchain has many applications in healthcare such as mobile health applications, remote monitoring systems, sharing and storing of electronic medical records, clinical trial data, and insurance information storage.

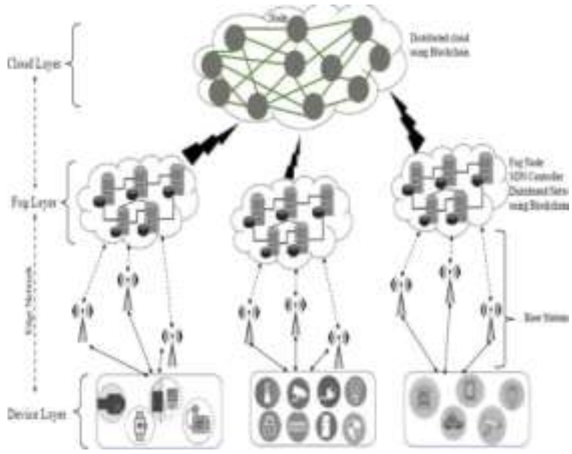
### *B. Education*

In today's world, education is considered a basic necessity of life. Traditional school-centered classroom learning is slowly changing with the advancement of cloud computing and the globalization of the learning environment. The increasing digitization of higher education needs authenticity and safely keeping accurate records. Blockchaintechnologies has a role in ensuring identity, privacy, security of students' data and maintain a consistent and transparent ledger for safe storage of information, decentralized open data, and academic data control. Such technology will increase students' flexibility to store their lifelong learning data and more control over their learning data. The blockchain improves the capacity of educational institutions to empower modern learning structures, online learning, mobile learning, and distributed learning for more students. Job driven education is another scope for blockchain technology implementation

### *C. Cloud Storage*

Nowadays Data is a valuable resource because it guides people to make decisions in most human activities. Cloud computing is a well-defined technology to store, manage, and process data using a network of remote servers with many advantages like the availability of the data across the globe, flexibility with a highly automated process, and easy scalability.

Blockchain integration with cloud computing, making our data more safe and secure with more storage flexibility, and at the same time, it keeps the validated data. By integrating blockchain with cloud computing, there will be many advantages in usability, trust, security, scalability, data management.



### *D. Finance*

Financial services industry witnesses millions of transactions every day where it has been facing many challenges for a long time for its security, transparency, and efficiency. Now, the financial services industry is moving towards blockchain adoption, which is highly promising and can solve many challenges faced by the industry and make financial services more secure and efficient. Blockchain creates a distributed public ledger with a secured communication protocol and robust verification method to improve our existing financial services in such a way to makes it is secure and easily accessible.

### *E.* Identity Management

Identity management has always been a challenge because; misuse of identity has been occurring nowadays. In many places, the person requires government-authorized personal identity like an Aadhar card, Passport, Pan Card to identify them. The existing method is not secure because of Identity theft and lack of control. Blockchain technology has emerged as one of the secure ways to store the Identity of individuals, which makes data more reliable and secure. It also prevents the loss of data and protects from unauthorized access.

### *F. IoT*

Internet of things (IoT) and the advancement in electronic home appliances have been changed the human work-life culture. IoT connects people, devices, and products by using sensors to incorporate and share the data from the different devices. Security of Internet of Things (IoT) devices is still unaddressed. Blockchain offers a compact solution for IoT devices to enhance security and bring transparency. Blockchain provides a scalable and decentralized environment to IoT devices, which gives strong protection against data tampering and reduces inefficiencies.

### *G. Real Estate*

Real estate has been primarily concerned with world economic assets and transaction activity. Real estate transactions are often conducted as face-to-face engagements. Blockchain introduces new ways to trade real estate with many benefits like digitalizes many steps of purchasing a property, providing secure and virtual solutions, and storing information about an asset on a ledger, instantly available to any party anywhere on the network. This will increase the transparency of the real estate market at the same time will give only true information about contractors, which will increase the reliability of transactions and reduce the risks of fraud to a minimum. Using this technology, real estate transactions will be faster, safer, and cheaper. As a result, the blockchain can be considered one of the most significant financial innovations that can make revolutionary changes in the real estate sector

## IV. SECURITY OF BLOCKCHAIN TECHNOLOGY

Blockchain conception derived from bitcoin cryptocurrency emerged as an inspiriting technology for peers to optically discern transaction, information integrity, and conspicuous storage in decentralized circumventions. The numerous threat and assail of Blockchain technology subsist in numerous programs a few are double-spending, privacy leakage, private key safety, mining assault, balanced attack. The security and privacy quandary of Blockchain is likewise addressed with the avail of the extraordinary researcher, in this section; some of the academic paintings already carried out are mentioned in brief.

The cryptographic primitives [10], privacy, and anonymity on the Blockchain are some of the key issues all through hashing the transaction. One-of-kind cryptographic set of rules are utilized all through mining procedure, [11] in comparison and proposed bitcoin and Ethereum consensus algorithms. Authors in [12] investigated the merits of utilizing open allotted ledgers (ODLs), for securing acceptance as true with management for authentication. The records integrity [13] can be realized thru a transaction, authentication of Blockchain properties which minimizes the threats and ascertain data integrity. Authors in [14] proposed the concept and model of certain verifier evidence of assets for bitcoin alternate and constructed the first concrete scheme to realize the designated verifier proof of paraphernalia for bitcoin trade with the avail of the utilization of elliptic curve cryptography. Public key infrastructure predicated framework integration with coin disbursed PKI scheme used to better security [15]. Cybersecurity and protective privacy [16] is every other critical trouble in Blockchain implementation. In the work proposed in [17], a novel trust-primarily predicated solution had been proposed to model efficacious cooperative content importing in cellular environments predicated on D2Dproximity communications. Some software is afflicted by sundry assaults like double-spend attacks [18] and Code predicated plenary attacks, double-spending, dust transactions [19]. Those assailants need to be addressed. The resilience of the Bitcoin atmosphere the unequivocalness of the Blockchain in utilization, the propagation, and verification of transaction blocks [20]. Authors in [21] seasoned-posed a framework present PoW-predicated exhaustively deployments in integration to PoW. Blockchain editions can be instantiated with distinct parameters, and objectively evaluate the tradeoffs between their overall performance and safety provisions. Ownership of the statistics engendered through the network becomes more and more crucial in times of ever-developing facilities to accumulate and analyze statistics of individuals. In mild of those challenges, authors show Blockchain technology can enable privatives by betokens of providing an odometer fraud aversion machine [22]. The application records mileage and GPS information of motors and secures that at the Blockchain, which vigorously obstructs odometer fraud. On-line attacks like ransomware [23] withal are wanted to be addressed, in some software wherein network architecture addresses the net. The software infrastructure ought to be safe from alfresco accessibility otherwise ransomware attacks can possible. Any other type of easement is Byzantine-fault tolerant [24] authoritatively mandating accommodation for the Hyperledger material Blockchain platform the utilization of the BFT-perspicacious replication library deal with the security and privatives trouble. Authors in [25] perceive situations underneath which Blockchain structures fail to ascertain consensus and gift a reproducible execution of an Ethereum personal chain. Authors in the article [26] defined the numerous adversaries, which can manage expeditiously shrewd settlement to get gain. The work in [27] discussed, evaluate and analyze the safety provisions of Bitcoin and its underlying Blockchain correctly shooting these days suggested assaults and threats inside the contrivance. The evaluation of the document describes and examines some of the countermeasures to discover threats at the contrivance some of that have already been incorporated in the machine. Authors in[28] presented the at ease utilization of drones as on-demand nodes for inter-accommodation operability between more than one company by way of exploiting the functions of the Blockchain.

E-trade, innovation, or some other consequences if now not handled well. Authors in [29] make use of the decentralization, Ionian, and audibility of the Blockchain suggest a Blockchain-predicated consummately personal privacy aegis mechanism, which uses online taxi-hailing because of the application scenario.

## V. CONCLUSION

Blockchain is the peer-to-peer (P2P) decentralized transaction and publicly to be had digital ledger, given that 2008 bitcoin and Blockchain are the two maximum crucial technology in facts machine. Blockchain can be acclimated to several applications to carry out a transaction in a trustful environment without the 0.33 element. In these survey paintings, initially explicate studies technique has been mentioned followed with the avail of the architecture and running precept of the Blockchain. Next twelve applications vicinity in which Blockchain technology seems promising to resolve the subsisting centralized system in a decentralized way withal numerous aegis troubles are addressed. A number of the maximum traumatic utility regions like the cyber world of things (IoT), Healthcare, and so forth have been identified. The from the have an optical canvassing of it was found that some work being done in the duration of privacy and safety issues but masses of the amendment want to be executed. Blockchain generation has numerous gains like decentralized, publicly available transaction, openness, and cozy, but there's still some research that needs to be executed like network, scalability, and mining technique of Blockchain system.

## REFERENCES

[1] P. Treleaven, R.G. Brown, D. Yang, Blockchain technology in finance, Computer 50 (9) (2017) 14–17.

[2] T. Aste, P. Tasca, T. Di Matteo, Blockchain technologies: the foreseeable impact on society and industry, Computer 50 (9) (2017) 18–28.

[3] Eyal, Blockchain technology: transforming libertarian cryptocurrency dreams to finance and banking realities, Computer 50 (9) (2017) 38–49.

[4] C. Khan, A. Lewis, E. Rutland, C. Wan, K. Rutter, C. Thompson, A distributed-ledger consortium model for collaborative innovation, Computer 50 (9) (2017) 29–37.

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

[6] M. Moser, R. Bohme, D. Breuker, An inquiry into money laundering tools in the Bitcoin ecosystem, in Proceedings of the eCrime Researchers Summit (CRS), 2013, IEEE, 2013, pp. 1–14.

[7] J.A. Dev, Bitcoin mining acceleration and performance quantification, in Proceedings of the 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE, 2014, pp. 1–6.

[8] Beikverdi, J. Song, Trend of centralization in Bitcoin's distributed network, in Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), IEEE, 2015, pp. 1–6.

[9] G. Di Battista, V. Di Donato, M. Patrignani, M. Pizzonia, V. Roselli, R. Tamassia, Bitconeview: visualization of flows in the Bitcoin transaction graph, in Proceedings of the 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), IEEE, 2015, pp. 1–8.

[10] D.A. Wijaya, Extending asset management system functionality in Bitcoin platform, in Proceedings of the 2016 International Conference on Computer, Control, Informatics and its Applications (IC3INA), IEEE, 2016, pp. 97–101.

[11] K. Saito, H. Yamada, What's so different about blockchain? Blockchain is a probabilistic state machine, in Distributed Computing Systems Workshops (ICDCSW), 2016 IEEE 36th International Conference on, IEEE, 2016, pp. 168–175.

[12] H. Halpin, M. Piekarska, Introduction to security and privacy on the blockchain, in Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2017, pp. 1–3.

[13] V. Gramoli, From blockchain consensus back to Byzantine consensus, Fut. Gen. Comput. Syst. (2017), doi:10.1016/j.future.2017.09.023.

[14] N. Alexopoulos, J. Daubert, M. Mühlhäuser, S.M. Habib, Beyond the hype: on using blockchains in trust management for authentication, in: Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, IEEE, 2017, pp. 546–553.

[15] Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, L. Yalansky, Ensuring data integrity using blockchain technology, in Proceedings of the 2017 20th Conference of Open Innovations Association (FRUCT), IEEE, 2017, pp. 534–539.

[16] H. Wang, D. He, Y. Ji, Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography, Fut. Gen. Comput. Syst. (2017), doi:10.1016/j.future.2017.06.028.

[17] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, W. Shi, Coin: A decentralized PKI mitigating MitM attacks, Fut. Gen. Comput. Syst. (2017), doi:10.1016/j. future.2017.08.025.

[18] N. Kshetri, Blockchain’s roles in strengthening cybersecurity and protecting privacy, Telecommun. Policy 41 (10) (2017) 1027–1038.

[19] L. Militano, A. Orsino, G. Araniti, M. Nitti, L. Atzori, A. Iera, Trust-based and social-aware coalition formation game for multihop data uploading in 5g systems, Comput. Netw. 111 (2016) 141–151.

[20] C. Pinzón, C. Rocha, Double-spend attack models with time advantage for Bitcoin, Electr. Notes Theor. Comput. Sci. 329 (2016) 79–103.

[21] D. Bradbury, The problem with Bitcoin, Comput. Fraud Secure. 2013 (11) (2013) 5–8.

[22] S. Feld, M. Schönfeld, M. Werner, Analyzing the deployment of Bitcoin’s p2p network under an AS-level perspective, Proceed. Comput. Sci. 32 (2014) 1121–1126.

[23] Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 3–16.

[24] M. Chanson, A. Bogner, F. Wortmann, E. Fleisch, Blockchain as a privacy enabler: an odometer fraud prevention system, in Proceedings of the 2017 ACM International Joint Conference on Pervasive and

Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers, ACM, 2017, pp. 13–16.

[25] N. Kshetri, J. Voas, Do crypto-currencies fuel ransomware? IT Prof. 19 (5) (2017) 11–15.

[26] J. Sousa, A. Bassani, M. Vukolic, A Byzantine fault-tolerant ordering service for the hyper ledger fabric blockchain platform, in 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, 2018, pp. 51–58.

[27] C. Natoli, V. Gramoli, The blockchain anomaly, in Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applica-

[28] C. Natoli, V. Gramoli, The blockchain anomaly, in Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applica-

[29] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 254–269.

[30] G. Karame, On the security and scalability of Bitcoin's blockchain, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 1861–1862.

[31] V. Sharma, I. You, G. Kul, Socializing drones for inter-service operability in ultra-dense wireless networks using blockchain, in Proceedings of the 2017 international workshop on managing insider security threats, ACM, 2017, pp. 81–84.

[32] N. Zhang, S. Zhong, L. Tian, Using blockchain to protect personal privacy in the scenario of online taxi-hailing, International Journal of Computers, Communications & Control 12 (6) (2017).