International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V67I4P103
Volume 67 Issue 4, 16-20, April 2019

Original Article

A Survey Paper on Blockchain Technology, Challenges, and Opportunities

Sandeep Kumar[1], Abhay Kumar[2], Vanita Verma[3]

[1]*M.Tech (CS) BIT Mesra, Ranchi, C-DAC Kolkata*
[2,3] *BIT Mesra, Ranchi, Assistant Professor- University Polytechnic*

Abstract *- Blockchain Technology had the most impact on our lifestyles in the last decade. Many people still confuse Blockchain with Bitcoin, but they are not the same. Bitcoin is an application that uses Blockchain technology. However, as a distributed technology, blockchain as a powerful tool can be utilized for immense daily life applications. There is a wide spectrum of blockchain applications ranging from cryptocurrency, risk management, internet of things (IoT), and financial services to public and social services. Blockchain technology has shown considerable adaptability in recent years as various market sectors require integrating its potential into their operations. Blockchain has a lot of benefits, such as decentralization, persistency, anonymity, and auditability. Although several studies focus on the usage of blockchain technology in various application aspects, there is no comprehensive survey on blockchain technology from both the technological and application perspectives. To fill this gap, we conduct a comprehensive survey on blockchain technology, blockchain type, reviews blockchain applications, and technical challenges. Moreover, this paper also points out the future aspect of blockchain technology.*

Keywords *- Blockchain, smart contract, cryptocurrency, IoT, security, digital ledger, consensus algorithm, PoW, PoS.*

I. INTRODUCTION

Although not named as such, blockchain was presented to the world in a whitepaper in 2008, its use in the digital peer-to-peer currency system, Bitcoin. Bitcoin is a form of network protocol, like HTTP or TCP layers which underpin global internet infrastructure and are used every time we browse the World Wide Web. A blockchain is a ledger of digital transactions; it is decentralized and not under the control of any individual, group, or company. Blockchain technology is structured, and it's extremely difficult to change the rules or content without the consensus among the people using it. In the blockchain, newer blocks are linked to the older ones, forming a chain, therefore the term blockchain.

This structure ensures that only the entries can be added to the database; data can never be Changed or removed because changing a single entry in an older block would mean rewriting the entire history of transactions after that block. A blockchain is an unchangeable, shared record of peer-to-peer transactions stored in a digital ledger created from linked transaction blocks. Blockchain is a technology that securely maintains continuously growing lists of data records and transactions. Blockchain relies on established cryptography techniques to allow each participant in a network to interact to store, exchange, and view information. There is no centralized authority; instead of it, transaction records are stored and distributed across the network.

Most importantly, all data entries are stamped with date and time. Interactions with the blockchain medium become known to all participants and require verification by the network before adding the information, enabling trustless collaboration between network participants while recording an unchangeable audit trail of all the interactions. Users can update only the block to which they have access for security purposes, and those updates get replicated across the network.

Bitcoin is the very first application of blockchain, and it's a kind of digital currency based on blockchain. Because of the success of Bitcoin, people now can utilize blockchain technologies in many fields and services, such as financial market, IOT, supply chain, election voting, medical treatment, document handling and tracking in a government office, insurance tracking records, and cybercriminals. We use these tools or services daily; cybercriminals and cybercrime can also be eradicated through this blockchain technology. [15, 16].

This paper will have a quick study about blockchain theory, key features of blockchain technology, consensus algorithm, different application in blockchain, different types of services, and security& privacy issues that we need to overcome.

II. THE THEORY OF BLOCKCHAIN

Blockchain technology is not using one single technique. Still, it contains Cryptography, Mathematics, Algorithm, and an economic model,

combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronization problems. [11, 12, 14].
The following six key elements of blockchain are:

A. Decentralized

Blockchain doesn't have to rely on centralized nodes anymore, and the data can be recorded, stored, and updated distributively.

B. Anonymity

Blockchain technologies solve the trust problem between a node to nodes so that data transfer can be anonymous; only a person's blockchain address needs to know.

C. Autonomy

The blockchain solely works according to the rules defined by its members. There is no central authority for the defined rules.

D. Automation

Manual processes generally guided by the legal contracts can be automated with a self-executing computer program called a smart contract. A smart contract is a component of a blockchain-based system that can automatically enforce stakeholder-agreed rules and process steps. Once launched, smart contracts are completely autonomous; when the conditions of contracts are met, pre-specified and agreed actions occur automatically.

E. Security

Various ways prove a blockchain is more secure than other record-keeping systems. Transactions must be agreed upon before they are recorded into the system. Once a transaction is approved, it is encrypted and linked to the previous transaction. This, along with the fact that information is stored across the network of computers instead of on a single server, makes it very difficult for hackers to compromise the transactional data. In any industry where the protection of sensitive data is crucial — financial services, government, healthcare — blockchain has an opportunity to change how the critical information is shared by helping to prevent fraud and unauthorized activity.

F. Transparency

The data recorded by the blockchain system is transparent to each node; it is also transparent on updating data, which is why blockchain can be trusted. Changes to public blockchains are publicly viewable by all parties creating transparency, and all transactions are unchangeable.

III. CONSENSUS ALGORITHM

The consensus algorithm makes the blockchain network highly secure and decentralized. The consensus function is a mechanism that makes all blockchain nodes agree to the same message, ensures the latest block has been added to the chain correctly, guarantees that the message stored by the node was the same one, and protects from malicious attacks.

A. Proof of Work (PoW)

Producing a proof of work can be a random process. Valid proof of work is generated after a lot of trial and error. Calculating PoW is called mining. Each block has a random value called Nonce in the block header; by changing this nonce value, PoW has to generate a value that makes this block header hash value less than a "Difficulty Target," which has already been set up. Difficulty means how much time it will take at the time when the node is calculating a hash value less than the target value. For a block to be accepted by network participants, miners must complete a proof of work that covers all of the data in the block. [1, 13].

B. Proof of Stake (PoS)

A Proof of Stake method increases protection from a malicious attack on the network.

IV. TYPE OF BLOCKCHAIN ARCHITECTURE

There are different kinds of blockchain architecture, and each of them has a different design and architecture.

A. Public Blockchain

In this type of blockchain, everyone in the network can validate the transaction and take part in attaining consensus. It ensures decentralization by setting up a block of peer-to-peer transactions. Each transaction is associated with the blockchain before it is written to the system. Hence, it can be confirmed and synced with every node in the network. Anybody with a computer and internet connection can be enrolled as a node and provided with the complete blockchain history. It states that everybody can check the transaction and verify it and can also participate in the process of getting consensus. The benefit of the public network is the user's anonymity and the full transparency of the ledger.

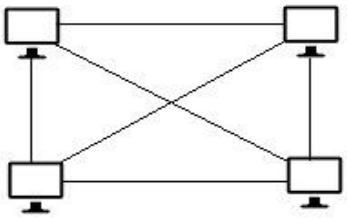

Fig. 1 Public Blockchain

B. Private Blockchain

The node will be restricted, and not every node that can participate in this blockchain has strict authority management on data access. Private blockchains have strict management concerning the

authority of the data access in the network. None of the nodes in the network can participate in the verification and validation of transactions. Instead, a company or organization initiates, verifies, and validates each transaction. This gives a higher efficiency level in the verification and validation of transactions. The benefit of a private blockchain is that a company can select the access rights to individuals and permit a higher level of privacy compared with public blockchains. A private blockchain is pertinent to a traditional and governance model-based business. Using a privately-run version of blockchain can bring the organization into the 21st century. Private blockchains are more prone to acceptability by the private sector or government-based companies. They allow a central authority to be present with a more secure, more efficient, and faster technology.

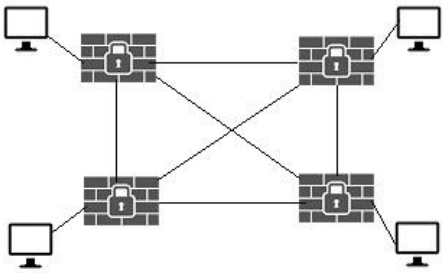

Fig. 2 Private Blockchain

C. Consortium Blockchain

A consortium blockchain is a combination of public and private blockchain and can be interpreted as partly decentralized. These blockchains are open to the public, but not the entire data is available to all the participants. User rights vary, and blocks are validated based on the predefined rules. Consortium blockchains are hence "partly decentralized." Consortium Blockchains are where a preselected set of trusted nodes controls the consensus process. A block is added to the chain after consensus is achieved through the transaction validation by a group from the preselected set of nodes. In a consortium Blockchain, the right to read the blockchain can be public or restricted only to participants. In addition to this, consortium Blockchains are considered partially decentralized, unlike private Blockchains. A consortium blockchain model is more appealing to corporate companies because it is decentralized, unlike private Blockchains.

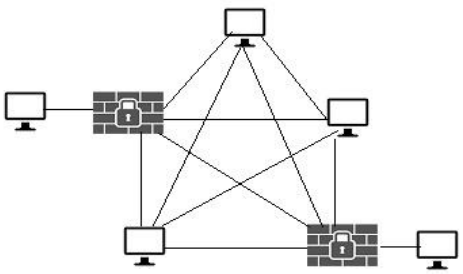

Fig. 3 Consortium Blockchain

V. BLOCKCHAIN APPLICATION

A. Bitcoin

Bitcoin was first introduced by an anonymous person or group under the alias Satoshi Nakamoto in 2008 [2]. Bitcoin uses a Blockchain public ledger to make transactions across a peer-to-peer network.

B. Ripple

The Ripple is a currency exchange, remittance, and real-time gross settlement system (RTGS) [8] that uses ripple protocol across a peer-to-peer network. This decentralized exchange focuses on the banking market.

C. Ethereum

A Next-Generation Smart Contract and Decentralized Application Platform was created by a cryptocurrency researcher and programmer named Vitalik Buterin [23]. It uses a Blockchain-based distributed computing platform with a Turing complete scripting language that enables the processing of smart contracts on the blockchain.

D. Hyperledger

The Hyperledger is a Linux Foundation project that develops Blockchain technologies for business and supports only registered members. Hyperledger is an open-source collaborative effort created to advance cross-industry Blockchain technologies. This is a global collaboration hosted by The Linux Foundation, including leaders in finance, banking, the Internet of Things, supply chains, manufacturing, and technology.

VI. SECURITY AND PRIVACY OF BLOCKCHAIN

Security ideas and principles are listed below:

A. Defense in penetration

This is a strategy that uses numerous corrective measures to protect the data. This data protection principle in multiple layers is more efficient than in a single security layer.

B. Minimum privilege

In this strategy, data access is reduced to the lowest level possible to reinforce an elevated level of security.

C. Manage vulnerabilities

This strategy checks for vulnerabilities and manages them by identifying, authenticating, modifying, and patching.

D. Manage risk

This strategy processes the risks in an environment by identifying, assessing, and controlling risks.

E. Manage patches

We patch the flawed part like code, application, operating system, firmware, etc., by acquiring, testing, and installing patches in this strategy.

Security in blockchain can be defined as the transaction information and data in a block against internal and peripheral, malicious and involuntary threats. This protection involves detecting and preventing threats and appropriate response to threats using security policies, tools, and IT services. Blockchain technology uses various techniques to achieve the security of the transaction of data of a block. Many applications such as bitcoin use encryption technology for data safety, using a combination of private and public keys to encrypt and decrypt data securely. The other most secure blockchain concept is that the longest chain is the authentic one. This removes the security risks due to the 51% majority of attack and fork problems. As the longest chain is ultimately considered authentic, the other attacks become null and void as they are orphaned forks. Privacy is the capability of a single person or a group to seclude themselves or data, therefore, expressing themselves discerningly. Privacy in blockchain means being able to perform any transaction without leaking identification information. At the same time, privacy allows users to remain compliant by discerningly revealing themselves without showcasing their activity to the entire network.[14, 31, 45]

VII. CHALLENGES OF BLOCKCHAIN

A challenge can be defined as an implicit demand for proof. Some of the major challenges currently faced by blockchain technology are listed below.

A. Scalability

With regular volume expansion of blockchain utilization and the flood in the sheer number of exchanges every day, the blockchain is continuously colossal. All transactions are stored in each and every node to get validated. The current transaction should be validated first before the other transactions are validated. The restricted block size and the time interval used to create another block plays an important part in not fulfilling the requirement of processing millions of transactions simultaneously in real-time scenarios. Meanwhile, the size of the blocks in the blockchain may create an issue of transaction delay in the event of a little transaction, as diggers transaction fees, miners would prefer to validate transactions. As referenced in [18], the proposed solutions for the adaptability issue of blockchains can be categorized into two classes: storage optimization and redesigning of blockchains. The database would keep up rest of the non-empty addresses. A customer with lightweight could likewise be utilized as another to fix the versatility issue. In updating, the blockchain can be divided into a key block and a smaller block, with the key block responsible for leader elections and the micro block responsible for transaction storage.

B. Privacy leakage

The blockchain is mainly vulnerable to transactional privacy leakage because the details and balances of all public keys are visible to everyone in the network. The proposed solutions for accomplishing anonymity in blockchains can be classified into mixing and anonymous solutions. Mixing is a service that offers anonymity by transferring assets from numerous info delivered to various yield addresses. Anonymous is a service that unlinks the payment origins to prevent transaction graph analysis, as discussed in [18].

C. Selfish mining

Selfish mining is another challenge faced by blockchain. A block is susceptible to cheating if a small portion of hashing power is used. In selfish mining, the miners keep the mined blocks without broadcasting to the network and create a private branch that gets broadcast only after certain requirements are met. In this case, honest miners waste time and resources while selfish miners mine the private chain.

D. Personal identifiable information

Personal Identifiable Information (PII) is any information that can be used to remove an individual's identity. [17] discusses the PII concerning communication and location privacy.

E. Security

Security can be discussed in terms of confidentiality, integrity, and availability, as discussed in [19]. It is always a challenge in open networks such as public blockchains. Confidentiality is low in distributed systems that imitate information over their network. Integrity is the forte of blockchains, although there exist many challenges. Availability in blockchains is high in terms of readability due to wide replication compared to write availability. The 51% majority attack is more theoretical in a large blockchain network because of these properties.

VIII. CONCLUSION

Blockchain technology is exceedingly recognized and appraised due to its decentralized infrastructure and peer-to-peer nature. There's no doubt that blockchain has been a hot topic in recent years; some problems have already been improved along with new techniques developing on the application side, getting more and more mature and stable. In this paper, we propose a comprehensive survey by initially discussing the structure of blockchains and their major components and characteristics. Then we

endeavor to highlight the security and privacy issues the blockchain technology faces in the different areas of its usage. Finally, the future applications, opportunities, and challenges of blockchain technology are summarized. We plan to investigate blockchains in the future and design and develop some of the architecture in the area of healthcare, election voting, automobile application, IoT, mobile application and cyber security, etc.

REFERENCES

[1] I.Bentov, A. Gabizon, and A. Mizrahi, Cryptocurrencies without proof of work, CoRR, vol. abs/1406.5694, 2014.

[2] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

[3] Lee R and Maeve D, Privacy and Information Sharing, Pew Research Center, 2016

[4] A.Narayanan and J. Clark, Bitcoin's Academic Pedigree, Communications of the ACM Magazine, vol. 60, no 12, Dec. 2017, p 36-45.

[5] RJ Krawiec et al., Blockchain: Opportunities for Health Care, Deloitte Report, Aug. 2016. https://goo.gl/y423dT (Erişim: 1 Şubat 2018).

[6] Guy Zyskind, Oz Nathan and Alex 'Sandy' Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, Security and Privacy Workshops (SPW), 2015 IEEE [02] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

[7] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. International Conference on Open and Big Data (OBD). Vienna, Austria: IEEE; 2016:2530 [08] Satoshi Nakamoto, Bitcoin: A

[8] Hou, The application of blockchain technology in e-government in china, in ICCCN. IEEE, 2017, pp. 1–4

[9] B.E.Dixon and C. M. Cusack, Measuring the value of health information exchange, in Health Information Exchange. Elsevier 2016, pp. 231–248.

[10] J.Richardson, Ethereum vs. Hyperledger, [Online] http://goo.gl/64a3Gg [26] Wall Street Firms to Move Trillions to Blockchains in 2018, IEEE Spectrum, Sept. 2017, [Online] http://goo.gl/bhr3Ck (Erişim: 1 Şubat 2018).

[11] J.Garay, A. Kiayias, and N. Leonardos, The Bitcoin Backbone Protocol: Analysis and Applications, pp. 281–310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[12] A.Gervais, G. O. Karame, V. Capkun, and S. Capkun, Is bitcoin a decentralized currency?, IEEE Security Privacy, vol. 12, pp. 54–60, May 2014.

[13] A.Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, On the security and performance of proof of work blockchains, in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 3–16, New York, NY, USA, 2016.

[14] S.Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Feb. 24, 2013. (http://bitcoin.org/ bitcoin.pdf).

[15] E.U.Opara, O. A. Soluade, Straddling the next cyber frontier: The empirical analysis on network International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017 (DOI: 10.6633/IJNS.201709.19(5).01) 659 security, exploits, and vulnerabilities, International Journal of Electronics and Information Engineering, vol. 3, no. 1, pp. 10–18, 2015.

[16] J.Singh, Cyber-attacks in cloud computing: A case study, International Journal of Electronics and Information Engineering, vol. 1, no. 2, pp. 78–87, 2014

[17] A.S.Elmaghraby and M. M. Losavio, Cyber security challenges in smart cities: Safety, security, and privacy, Journal of Advanced Research, 5 (2014), 491–497.

[18] Z.Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in Big Data (BigData Congress), 2017 IEEEInternational Congress on, IEEE, 2017, 557–564.

[19] J.Mendling, I. Weber, W. V. D. Aalst, J. V. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. D. Ciccio, M. Dumas, S. Dustdar, et al., Blockchains for business process management-challenges and opportunities, ACM Transactions on Management Information Systems (TMIS), 9 (2018), Article No. 4.

[20] F. Gierschner, Bitcoin and beyond.

[21] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems, (2017), URL http://www.sciencedirect.com/science/article/pii/S0167739X17318332.

[22] F.Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, IEEE Communications Surveys & Tutorials, 18 (2016), 2084–2123.

[23] Vitalik Buterin, Ethereum and The Decentralized Future. Future Thinkers Podcast. 2015-04-21. Retrieved 2016-05-13.

[24] Wikipedia, Bitcoin,https://en.wikipedia.org/wiki/Bitcoin.

[25] Ripple, RippleNet, https://ripple.com.