Blockchain Technology, Its Applications and Open Research Challenges

Rajesh Kumar Kaushal¹, Naveen Kumar² and Surya Narayan Panda³
¹,²,³Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Corresponding author Email: naveen.sharma@chitkara.edu.in

Abstract. Blockchain is a technology that operates on distributed peer-to-peer network and is widely adopted by large number of organizations due to its attractive features such as highly secured, transparent, traceable, low transaction fee, no need of central authority and confidentiality. There are lot of confusions and myths regarding the blockchain technology as it is emerging technology and too complex in nature. This paper is aimed at revealing blockchain technology in depth along with its applications and open research challenges. The past published literature was reviewed to achieve the objectives. The study found that apart from cryptocurrency, blockchain is also suitable for other applications such as smart cities, supply chain, healthcare, smart transportation and authenticating IoT (Internet of Things) devices. This study is also disclosing various open research challenges such as scalability issues, huge power consumption and delay in completing transactions. This paper is also sharing the mitigation approaches and the future of blockchain with smart contracts.

Keywords: Blockchain, Crypto-Currency, Blockchain Challenges, Smart Contracts

1. Introduction
Blockchain technology was first introduced by Satoshi Nakamoto in November, 2008. The idea was to make transactions electronically without any central authority at low transaction fee [1]. In a typical banking environment, central agencies implement concurrency control mechanism to avoid double-spending but this approach is suffering from issues like single point of failure, high transaction fee, trust issues and prone to malicious attacks [2]. In spite of the absence of central authority, the blockchain architecture is efficiently designed to maintain security, confidentiality and traceability [3][4].

In its inception, this technology was used to exchange bitcoins over the network. Bitcoin is not the only cryptocurrency based on blockchain. In fact, several cryptocurrencies are using blockchain at backend such as Ethereum, Ripple, Litecoin, Neo, Stellar and Monero. Due to its usability, now it is also being used in several other applications such as smart cities, retail, healthcare, smart transportation and authenticating IoT (Internet of Things) devices [5][6]. IoT devices are widely adopted for automation[7][8] and blockchain can prevent unauthorized access to such devices.

The blockchain technology comprises of several complex concepts such as decentralized peer-to-peer network, the concept of mining, cryptographic puzzle, nonce, merkle root and consensus algorithms which makes it difficult to conceive for the novices. This paper is aimed at revealing the blockchain technology by explaining these complex concepts in depth along with its applications and open research challenges. Additionally, this paper is also discussing the concept of smart contracts which is the key application and future of blockchain.

The rest of the paper is organized as follows: section 2 is explaining the present state of art, objectives of this paper are listed in the section 3, methodology to achieve the objectives is described in the section 4, blockchain mining process is explained in the section 5, blockchain applications and smart concepts
are showcased in the section 6 followed by open research challenges in the section 7. The paper is concluded with discussion and conclusion in the section 8.

2. Literature Review
Blockchain is a secure and decentralized ledger build upon hashing algorithms as well as public and private key cryptography[9]. It implements security by introducing SHA256 hashing algorithm designed by NSA (National Security Agency) [10]. Deterministic and irreversible are the two key properties of SHA256. It is deterministic in the sense that it always produces the same hash for same inputs. These hashes are irreversible as it is impossible to predict the original input from a given hash. Moreover, SHA256 always produce hashes of 64 hexadecimal letters regardless of the input size. In fact, blockchain wallet address is a SHA256 hash and considered as a public key. This public key needs to be shared on the network to make transactions. The private key must be kept secret and needed so that only the intended user can get the amount. The blockchain hashes may differ from protocol to protocol. For example, Bitcoin generated hashes differs from Ethereum hashes.

Blockchain can be public or private. The public blockchain can be joined by anyone, all that is needed is Internet connection and a computing device. Opposite to public blockchain, only authorized people, organizations and financial institutions can join private blockchain. Such systems are also called permissioned blockchain and based on the trust whereas public or permission less blockchain works in trustless environment. The private blockchain is prone to security threats as only few permissioned nodes are part of the network and if someone could manage to control these few nodes then transactions can be altered [11]. Hybrid blockchains are also getting popularity as it gives the flexibility to shuffle blockchain role from decentralized to centralized as and when required[11][12].

Miners, buyers and sellers are involved in the blockchain ecosystem. A transaction is initiated either by a seller or a buyer. The miners are responsible for validating the transactions [13]. In reality, a chain of block is maintained on blockchain where every single block holds approximate 2000 transactions and miners are responsible for mining these blocks. The first block of this chain is called a genesis block and all succeeding blocks are linked with the previous blocks by a hash key and thus ensure traceability and non-repudiation [14]. Nobody can deny his/her role in the transaction due to non-repudiation (digitally signed transactions). Miners are rewarded with certain amount for every successfully mined block. In case of Bitcoin, the rewarded amount is 12.5 Bitcoins [3].

Miners compete with each other to mine a block and this operation requires huge electricity consumption [15]. The mining difficulty is increasing day by day and as a result improved computational units such as GPU (Graphics Processing Unit) and ASICs (Application Specific Integrated Circuit) are required and demands huge investments. As a result, the small miners have started working in pools and such pools are called mining pools. Every miner in a pool works on a specific range of nonce (32-bit editable field in a block) to find the target hash and rewards are equally distributed among the pool miners on successfully mining a block.

Despite of its popularity, blockchain technology is suffering from few issues such as ever growing demand for computational speed, huge electricity consumption and slow transaction rate [1][6]. The lack of understanding and talent is another major issue which is proving as a huge hindrance in blockchain adoption. The rest of the paper explains the complete mining process along with the reasons for huge electricity consumption and slow transaction rate. This paper is concluded with a discussion on various blockchain applications and smart contracts.

3. Objectives
This study is aimed at achieving the following objectives. The responses to these objectives will certainly contribute in blockchain awareness and its adoption rate.

- Disclosing blockchain ecosystem.
- Identifying key blockchain applications.
- Identifying the open research challenges.
4. Methodology
This study reviewed relevant published studies of last four years to explore the complete ecosystem of blockchain and its key terms such as decentralized peer-to-peer network, the concept of mining, cryptographic puzzle, nonce, difficulty target, merkle root and consensus algorithms. The popular databases like Science-Direct and Google Scholar was used to review the articles. Only those studies were reviewed where blockchain ecosystem, its applications and open research challenges were discussed.

5. Blockchain Ecosystem
The end users can initiate transactions in the blockchain ecosystem after creating a wallet. These transactions are kept on the mempool until picked and mined by the miners. Mempool is a memory block available on every single node on the network. A fee is associated with these transactions and the miners pick high fee transactions from the mempool to put them on the block. A single block can accommodate approximate 2000 transactions. The blockchain ecosystem is depicted in the Figure 1.

![Blockchain ecosystem](image)

Figure 1. Blockchain ecosystem

Each block has a block number, protocol version, timestamp, hash of a previous block, nonce, difficulty target, transactions and merkle root. Hash of a previous block is required to link all the blocks to form a chain. Transaction field hold transaction details and merkle root is the cumulative hash of these transactions. The timestamp filed keeps record of the exact time when the block was mined. The nonce and difficulty target are the most important fields and vital for the mining. The difficulty target is a hash with some leading zeros. These leading zeros are set by the protocol and more number of leading zeros make it more difficult to mine. At present, in October 2020, the difficulty target is nineteen leading zeros.

To successfully mine a block, the miners must find a nonce value (an editable field in the block) which then combined with the other fields to produce a cumulative hash and must below the target difficulty. This is actually the cryptographic puzzle. To achieve this million and billions of iterations are required as the only way to find the correct nonce is brute force technique. These efforts are well known as Proof-of-Work (PoW). Thereafter, the verified mined block is broadcasted on the blockchain network to get the consensus. This is accomplished with consensus algorithm. Different protocol may use different consensus algorithms. Bitcoin protocol use Proof-of-Work consensus algorithm. At least 51% nodes must verify and agree to add the newly mined block on the blockchain.

Complex cryptographic puzzle and slow consensus algorithm is the primary cause of huge electricity consumption and slow transaction rate. On average, every block in bitcoin is mined in approximately 10 minutes.

6. Blockchain Applications and Smart Contracts
Originally, blockchain was designed for cryptocurrencies but with the advent of smart contracts it is being used in wide range of applications [16]. A smart contract is a self-executing piece of code that executes when certain conditions are met and then contract is stored as a block on the blockchain [17][18]. Smart contract is really a smart way of making applications immutable and transparent. Smart contracts are immutable and transparent due to the fact that they are written on blockchain and thus inheriting its key features.
The idea of smart contract eliminates middlemen and saves time and money, prevents paper work and physical presence, less prone to mistakes and establish a highly secure environment and also eliminates the need of lawyers. For example, if two parties are willing to buy and sell a property then they need a middle man, physical appearance of all the parties, need to spend lot of time and money and paper work. Still there are chances of frauds in such environment. Smart contracts eliminate all these issues by making contracts automatically on blockchain network when certain conditions are met. These advantages are absent in the traditional contracts.

All blockchain protocols do not support the concept of smart contracts. The most popular blockchain protocols that offer smart contracts are Ethereum and Neo. Table 1 explains the key differences between smart contracts and traditional contracts. Due to smart contracts, the blockchain is widely used and adopted worldwide. As a result, healthcare industry, real estate market, insurance sector, online voting, supply chain, online public donations, authenticating IoT devices, online vehicle leasing, will management and online gambling/lottery are the key applications of blockchain. Table 2 demonstrates some of the key applications areas of blockchain along with the description.

| Table 1. Benefits of smart contracts over traditional contracts |
|--------------------------|--------------------------|--------------------------|
| Parameter                | Traditional Contracts    | Smart Contracts          |
| 1. Time                  | One or more days         | One or more minutes      |
| 2. Require Middlemen     | Yes                      | No                       |
| 3. Cost                  | Expensive                | Inexpensive              |
| 4. Physical Presence     | Yes                      | No                       |
| 5. Paper Work            | Yes                      | No                       |
| 6. Need of Lawyer        | Yes                      | May not be required      |
| 7. Prone to Mistakes     | Yes, due to human engagement | No, due to smart code |
| 8. Security              | Not secure due to centralized. | Secure due to decentralized. |

| Table 2. Blockchain Applications |
|-----------------------------------|
| Application Area                  | Description                                           |
| 1. Healthcare Industry            | To keep patient medical records securely on distributed network |
| 2. Buying and Selling Property    | Buying property without middlemen and physical appearance will make the process fast and inexpensive |
| 3. Insurance                      | To process claims faster and prevent faulty claims      |
| 4. Voting                         | Prevents massive election expenditures and restrict voting scams |
| 5. Supply Chain                   | To make a transparent environment for the customers and to track middle suppliers |
| 6. Donations                      | To track the sources of transactions and to avoid their misusages. |
| 7. Authenticating IoT devices     | IoT devices can be authenticated with SHA256 hash.      |
| 8. Vehicle leasing/Sales          | Taking vehicles on lease or selling them without middlemen |
| 9. Wills Management               | Keeping wills on distributed network securely can prevent fault claims and misusages |
| 10. Online Gambling/Lottery       | To prevent frauds in online gambling/lottery by making the whole process transparent. |
7. Open Research Challenges and Mitigation Approaches

Despite of its popularity, the blockchain technology is still suffering from few issues and can be considered as open research challenges for the researchers [19][20]. These research challenges are listed below.

- To prevent huge electricity consumption and make it eco-friendly.
- There is a need to improve transaction speed by improving the consensus algorithm.
- There is need to tackle scalability issue as the process of mining blocks is getting slower with the growing network.
- Low adoption of blockchain technology due to lack of awareness and expertise.

To mitigate these issues, improved consensus algorithm and Proof-of-Work mechanism is required that too without compromising with its key features such as security, transparency, traceability and distributed public ledger. Moreover, the improved consensus algorithm should be light enough to work on GPU (Graphics Processing Unit) rather than ASIC (Application Specific Integrated Circuit). This is a threefold solution as it can reduce electricity consumption, improve transaction speed and avoid scalability issues. As far as the low adoption of blockchain technology is concerned, it can only be resolved by training and awareness programs.

8. Discussion and Conclusion

The blockchain is a revolutionary technology which is going to transform the way of managing assets digitally and securely on a distributed network. The centralized systems are prone to scams, hacking attempts, data lost and poor transparency [2]. To mitigate these issues, the blockchain offers a decentralized peer-to-peer network and keeps data in the form of blocks on multiple nodes. The records on blockchain ecosystem are immutable and publicly available by keeping user identity confidential. On the other hand, Smart contracts have opened the doors for other areas such as healthcare industry, insurance sector, supply chain management, public donations, asset registration, authenticating IoT devices, online gambling or lottery and many more. Smart contracts work on top of blockchain and save time, eliminate middlemen, inexpensive, prevents paper work, does not requires physical appearance, avoid human mistakes, maintain transparency, highly secure and prevent frauds [21].

At present, there are certain issues with blockchain technology like high power consumption, slow transaction speed, low adoption rate and professionals and government regulations. As a result, only few organizations are utilizing its strength. There is a need of improved light weight consensus algorithm to overcome with issues like high power consumption and low transaction speed. It is suggested to use computer animation based models with effective design principles for the awareness purposes [22][23] which would certainly motivate industries to adopt this technology. Due to its significant advantages, it is expected that blockchain technology is the future.

References

[1] H. Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, “Blockchain for the IoT and industrial IoT: A review,” Internet of Things, vol. 10, p. 100081, 2020.
[2] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, “iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments,” Softw. Pract. Exp., vol. 47, no. 9, pp. 1275–1296, 2017.
[3] M. Andoni et al., “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” Renew. Sustain. Energy Rev., vol. 100, pp. 143–174, 2019.
[4] J. Mattila, C. Naucler, R. Stahl, M. Tikkanen, A. BAdenlid, and others, “Industrial blockchain platforms: An exercise in use case development in the energy industry,” 2016.
[5] S. K. Singh, S. Rathore, and J. H. Park, “Blockchain intelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence,” Futur. Gener. Comput. Syst., vol. 110, pp. 721–743, 2020.
[6] J. Lin, Z. Shen, A. Zhang, and Y. Chai, “Blockchain and IoT based food traceability for smart agriculture,” in Proceedings of the 3rd International Conference on Crowd Science and Engineering, 2018, pp. 1–6.
[7] N. Kumar, S. Panda, P. Pradhan, and R. Kaushal, “IoT Based Hybrid System for Patient Monitoring and Medication,” *EAI Endorsed Trans. Pervasive Heal. Technol.*, vol. 5, no. 19, 2019.

[8] N. Kumar, S. N. Panda, P. Pradhan, and R. Kaushal, “IoT Based E-Critical Care Unit for Patients In-Transit,” *Indian J. Public Heal. Res. Dev.*, vol. 10, no. 3, pp. 46–50, 2019.

[9] C. Walsh, P. O’Reilly, R. Gleasure, J. McAvoy, and K. O’Leary, “Understanding manager resistance to blockchain systems,” *Eur. Manag. J.*, 2020.

[10] B. Bhushan, P. Sinha, K. M. Sagayam, and A. J., “Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions,” *Comput. Electr. Eng.*, p. 106897, 2020.

[11] Wikipedia contributors, “Blockchain,” 2020. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Blockchain&oldid=986448687. [Accessed: 01-Nov-2020].

[12] Z. Li, H. Wu, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, “A hybrid blockchain ledger for supply chain visibility,” in *2018 17th International Symposium on Parallel and Distributed Computing (ISPDC)*, 2018, pp. 118–125.

[13] N. Kumar and S. Aggarwal, “Core components of blockchain☆☆Introduction to blockchain.,” Elsevier, 2020.

[14] S. Cherukupally, “Blockchain technology: Theory and practice,” Elsevier, 2020.

[15] P. K. Sharma, N. Kumar, and J. H. Park, “Blockchain Technology Toward Green IoT: Opportunities and Challenges,” *IEEE Netw.*, 2020.

[16] D. D. F. Maesa and P. Mori, “Blockchain 3.0 applications survey,” *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, 2020.

[17] Z. Zheng et al., “An overview on smart contracts: Challenges, advances and platforms,” *Futur. Gener. Comput. Syst.*, vol. 105, pp. 475–491, 2020.

[18] C. Sillaber and B. Waltl, “Life cycle of smart contracts in blockchain ecosystems,” *Datenschutz und Datensicherheit-DuD*, vol. 41, no. 8, pp. 497–500, 2017.

[19] Y. Zhou, Y. S. Soh, H. S. Loh, and K. F. Yuen, “The key challenges and critical success factors of blockchain implementation: Policy implications for Singapore’s maritime industry,” *Mar. Policy*, p. 104265, 2020.

[20] M. Torky and A. E. Hassanein, “Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges,” *Comput. Electron. Agric.*, p. 105476, 2020.

[21] R. Koulu, “Blockchains and online dispute resolution: smart contracts as an alternative to enforcement,” *SCRIPTed*, vol. 13, p. 40, 2016.

[22] R. K. Kaushal and S. N. Panda, “A Meta Analysis on Effective Conditions to Offer Animation Based Teaching Style.,” *Malaysian J. Learn. Instr.*, vol. 16, no. 1, pp. 129–153, 2019.

[23] R. Kaushal, S. N. Panda, and N. Kumar, “Proposing Effective Framework for Animation Based Learning Environment for Engineering Students,” *J. Eng. Educ. Transform.*, 2020.