

BLOCKCHAIN TECHNOLOGY: AN OVERVIEW OF RECENT APPLICATIONS.

Peace Ayegba

Department of Computer
Science, Landmark University,
Omu-Aran, Nigeria
ayegba.peace@lmu.edu.ng

Adebayo Omotosho

Department of Computer
Science, Landmark University,
Omu-Aran, Nigeria
bayotosho@gmail.com

ABSTRACT

Blockchain has attracted attention in recent years particularly as the innovative technology behind popular cryptocurrencies such as Bitcoin and Ethereum. Blockchain is a distributed database which offers new ways for developing decentralized and secure systems. It has been adopted in several fields due to inherent characteristics such as transparency, immutability and efficiency, however the use of blockchain technology still faces some challenges particularly in its implementation. This paper provides an overview of the most current state of the art blockchain applications, the benefits of blockchain utilization across various sectors and outlines some challenges faced in its deployment. This study gives an informed study on open research topics in blockchain technologies and future research directions.

Keywords: Blockchain, Cryptocurrency, Decentralized, Applications.

1. INTRODUCTION

Blockchain, though in its early stages, is now widely used as a result of several benefits including decentralization, fault-tolerance, resilience, persistency, anonymity and auditability. Blockchain is a system that uses popular cryptographic algorithms that enhance the integrity, security and privacy of personal information and serves as an intervention that authenticates entities participating in a transaction. With inherent properties such as timestamping, traceability and data provenance, blockchain has been effectively used for Cloud computing (Park and Park, 2017), Internet of things (Ejaz and Anpalagan, 2019; Ferrag et al., 2018), and Smart homes (Biswas and Muthukkumarasamy, 2016). Hence, blockchain technology has potentials to become the new engine of growth in our digital world where the internet is required for conducting major daily activities like sharing personal data and life events, conducting online commercial and financial transactions. The adoption of blockchain can revolutionize the operating modes of commerce, industry, and education, as well as promoting the rapid development of a knowledge-based economy on a global scale. It gained popularity with the introduction of Bitcoin which first came to light in 2008 when a paper titled, *Bitcoin: a peer to peer electronic cash system*, was introduced by Satoshi Nakamoto (Satoshi, 2008). The major concepts described in this paper were the use of a consensus model where computers in an unreliable network can reach an agreement introduced by (Lamport, 1998) and the use of an electronic ledger for digitally signing documents such that the documents are not easily tampered with, highlighted by (Narayanan et al., 2016). Blockchain is the backbone technology of *BitCoin*, digital cryptocurrency. Cryptocurrency refers to all networks and mediums of exchange that uses cryptography to secure transactions, compared to other systems where the transactions are channeled through a centralized trusted entity (Crosby et al., 2016). Bitcoin has been predicted by financial industries to reach a 20 billion dollars market value in 2020 (Park and Park, 2017). As highlighted by (Swan, 2015), the development process of blockchain applications is categorized into three distinct stages, blockchain 1.0, 2.0 and 3.0. Blockchain 1.0 brought about the innovative cryptocurrencies used as a peer-to-peer cash payment system while Blockchain 2.0 presented the utilization of more advanced blockchain applications than basic money transactions, for example, smart contracts, stocks, securities, loans, investments and smart properties. Blockchain 3.0 involved the development of blockchain applications beyond cryptocurrencies and digital payments as well as financial markets, for example, in the government, health, science, literature, culture, and art sector. Blockchain technology is the foundation of modern cryptocurrencies and relies heavily on cryptographic functions. Currently, blockchain has applications in various financial services such as digital assets, remittance and online payment, internet of things, smart contracts and other security services. More recently, smart contracts are used as blockchain technologies for digitizing and automating the execution of business workflows such as agreements and contracts where consensus mechanisms are required for its proper execution (Governatori et al., 2018). This study therefore aims to present an overview of blockchain technology, the existing applications and current issues faced by blockchain systems in order to understand its future directions.

2. LITERATURE REVIEW

A recapitulation of some of the documented works in literature shows blockchain has been used extensively in different sectors. Numerous applications of blockchain technology have been singularly implemented or combined with other applications. Some of the positive contributions of blockchain in the financial sector, such as smart contracts, tracking and shipping of containers as well as other cross border money transfers for modern organizations were highlighted by (Beck et al., 2017). A summary on blockchain implementations and other digital ledger techniques already existing, showed the benefits of blockchain beyond cryptocurrency. In applying blockchain to cryptocurrency, an extra layer of security is provided, and the technological fundamentals of blockchain revolve around transactions which are triggered by participants, and blocks (Miraz and Ali, 2018). Zheng et al., (2018) compared different consensus algorithms and their technical challenges faced while implementing blockchain. Scalability, particularly for cryptocurrencies was the major technical issue discussed as a tradeoff between the block-size and security is required and difficult to achieve. The study showed that the proof of work and proof of stake consensus algorithms were more suitable for public blockchain while tender-mint, ripple, delegated proof of work and practical byzantine fault tolerance are more suited for private and consortium blockchain. The authors recommended the standardization of the blockchain testing phase and a combination of bigdata analytics and blockchain to address privacy leakages and selfish mining. Novo, (2018) combined the development of an IOT architecture with blockchain technology. The decentralized architecture for managing IOT devices based on blockchain technology, arbitrates roles and permissions in IOT systems. Some advantages of the proposed architecture listed include, concurrency, lightweight, scalability, transparency, mobility, and accessibility for IOT systems. The system ensures issues associated with managing numerous IOT devices are combated. The evaluation of the prototype showed the system was effective and highly flexible in managing IOT devices. Vujicic et al., (2018) further discussed blockchains and cryptocurrencies with emphasis on bitcoin cash, bitcoin gold and Ethereum. Bitcoin cash deals with the 1mb block-size limitation on bitcoins by allowing for 8mb block-size which leads to faster confirmation times. Bitcoin gold is also a hard fork of bitcoin, but the proof of work algorithm used is Equihash not the SHA-256 used in the regular bitcoin cryptocurrency. However, Ethereum was introduced to support all types of computation and transaction states which a major limitation in bitcoin is, that is, for every transaction in the list, a new state is created based on previous states. Ethereum is therefore suitable for issuing tokens which are needed in smart contracts. Kramer (2019) revealed the need for more awareness of blockchain as over 83% of 53 business professionals had never heard of blockchain technology in the survey conducted.

3. BLOCKCHAIN ARCHITECTURE

The technical framework of the blockchain architecture is shown in figure 1. First, data is stored in units of blocks which are connected in a chained structure. Depending on the specific rules of the blockchain in question, the current block is closed, and a new block is created once a certain number of transactions has been recorded or some other criteria has been met. Consecutive blocks are connected in chronological order to form a chained data structure thereby forming a *blockchain*. All user nodes participate in the validation, storage and maintenance of data. At least, more than half of the participants or users in a blockchain system must approve the new block which is then broadcasted to other user nodes and an agreement/synchronization is reached. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions. The use of a consensus algorithm allows most validators of network come to an agreement on the state of a ledger (Swanson, 2015). In this manner, new transactions are not consequently added to the ledger. Instead, the transaction procedure guarantees that these exchanges are put away in a block for a specific time, for instance, 10 mins in the network, before being moved to the ledger. After some time, the data in the blockchain becomes permanent.

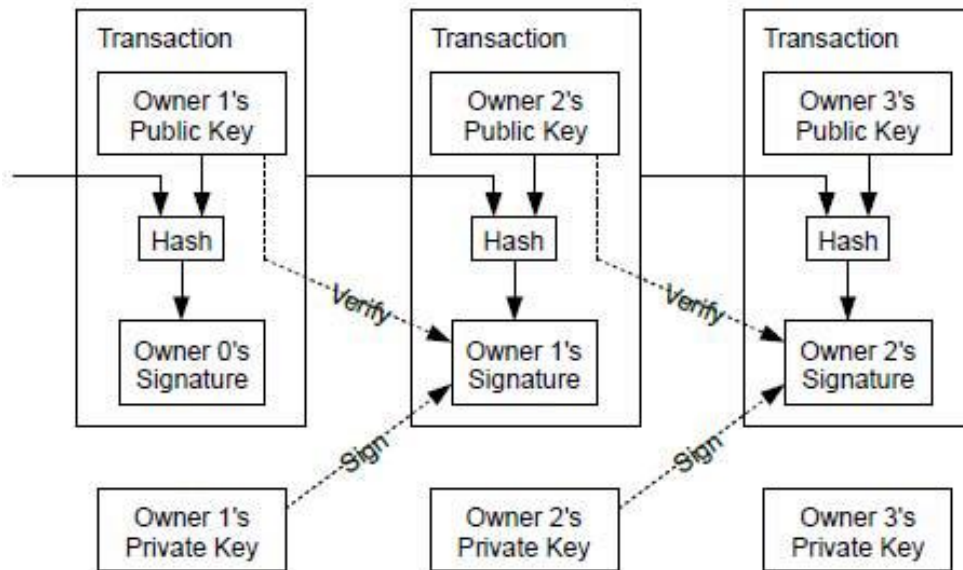


Fig 1. Blockchain technical framework (Satoshi, 2008).

3.1 Cryptocurrencies

Cryptocurrency is an advanced digital payment method that utilizes encryption (cryptography) to create money and to confirm transactions. Cryptocurrencies take advantage of blockchain technologies allowing for a decentralized, straightforward and immutable nature of making payments. The most significant component of a cryptocurrency is that it isn't constrained by any authority. This features of blockchain makes cryptocurrencies hypothetically insusceptible to government monitoring, control or obstruction. Cryptocurrencies can be sent legitimately between two parties who make use of private and public keys. These transactions are possible with very minimal expense fees, enabling clients to avoid the precarious charges charged by regular financial institutions. Popular cryptocurrencies include, Bitcoin, Ethereum, Dogecoin, Zcash, Bitcoin Gold, and Monero. A cryptocurrency like Bitcoin comprises of a network of peers. Each peer has a record of the total history of all transactions thus ensuring the record remains valid. Bitcoin is one of the primary digital currency that utilizes distributed technology to encourage instant payments.

3.2 Smart Contracts

A smart contract is an understanding between two individuals in form of computer codes. They keep running on the blockchain, so they are put away in a public database and are immutable. The transactions that occur in a smart agreement are consequently processed by the blockchain, which means they can be sent naturally without an outsider and these transactions occur only when the conditions in the agreement are met. One of the major advantages in the use of blockchain for smart contract is the exclusion of intermediaries as it is a decentralized system and there is no need to middlemen which reduces cost, saves time and avoids conflict. Tonelli et al., (2019) designed a microservice system based on Blockchain smart contracts. Microservice architectures are small services deployed independently for specific purposes. The authors implement a microservice system based on blockchain smart contracts for improved transparency and immutability. The smart contracts, written in solidity programming language is executed on an Ethereum virtual machine. A case study was used to show the successful mapping of the microservice paradigm to a smart contract. This system provides a new way in which blockchain and microservices can be used for online services and in developing applications particularly using a blockchain oriented software engineering approach (BOSE). Smart contracts promote ledger feedbacks in transferring money and receiving the product or service. Figure 2 gives a detailed workflow of how smart contracts work.

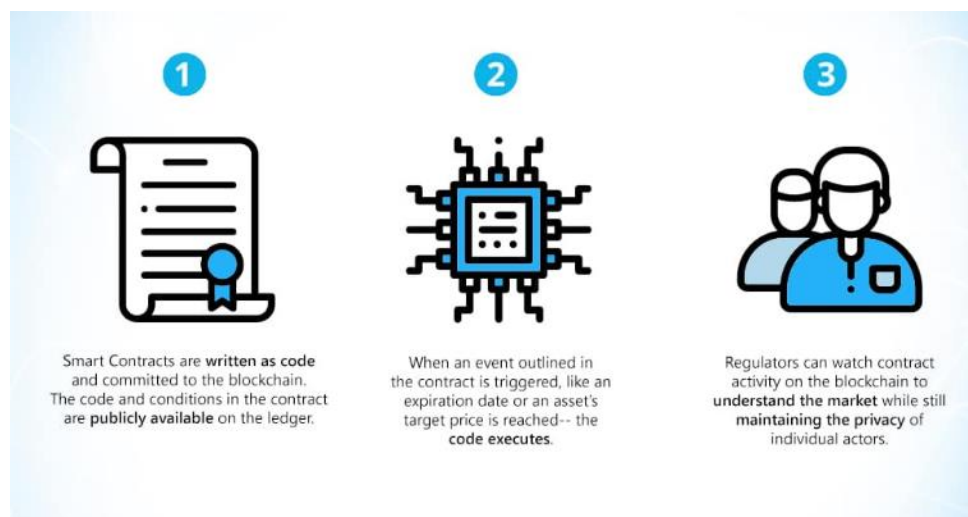


Figure 2. Smart contracts (Ameer, 2016).

4. Blockchain Applications

Following the new development and worldwide use of blockchain, blockchain related research has also become increasingly popular. However, considering the development from its application layer, blockchain is still in its exploratory stage. By adequately ensuring the validity and uniqueness of transactions, blockchain has turned into the specialized core for cryptocurrency, resource management, credit control, and gradually more researchers are investigating its application in finance, proffering health services, education, energy distribution and management as well as real estate services.

4.1 Blockchain in Finance

The emergency of blockchain systems such as Bitcoin (Satoshi, 2008) and Hyperledger (hyperledger, 2015) has brought tremendous impacts in rendering financial and business services. Real world business cases such as the collateralization of financial commodities and the clearing and settlement of financial assets could leverage the use of blockchain in reducing costs and risks. Morini(2016) showed that a business model based on distributed consensus would be useful for financial markets. Also, conventional financial institutions can employ the use of cryptocurrency and blockchain technology for extending postal operations. Furthermore, Jaag et al. (2016) highlighted the opportunities offered by blockchain technology for postal operations showing that post-coins (a form of bitcoin) could be issued by postal operators, and since the postal operators are viewed as a trusted authority by the public, post-coins would become popularly used to simplify their operations. This also details the diverse business opportunities that blockchain technology offers in postal services, device and supply chain management. In financial technology, blockchain has been shown to improve risk management. Pilkington (2016) presented an innovative risk-management framework, whereby blockchain technology was used to analyze investment risks. Individuals who make investments often hold securities through chains of curators and therefore face the risks of failures. With the use of blockchain, investments and subsequent insurances can be chosen rapidly rather than undergoing a long term deliberation. Micheler and von der Heyde (2016) additionally developed another framework combined with blockchain to diminish custody risk while achieving a similar degree of transaction safety. Blockchain-based smart contracts empower a decentralized autonomous association (DAO) to take part in broad business-work collaborations.

4.2 Blockchain in Agriculture

Two important and highly relevant areas for blockchain application, are in agriculture and food supply chain. The transactions that occur in agriculture and food supply chains are often related, since the results of farming quite often are utilized as contributions to large multi-national supply chain, where the purchaser is generally the last customer (Maslova, 2017). More than 1,300 clients and more than 1.6 million tons of grain was executed over a bitcoin cloud-based framework which resulted in an expanded benefit of over \$360 million dollars. This was started by AgriDigital and the achievement of AgriDigital prompted the potential utilization of blockchain innovation in the farming and supply chain networks. The goal of AgriDigital was to develop trusted and proficient agricultural supply chains by using blockchain innovation (AgriDigital, 2017). (Lee et al., 2016) saw that agricultural supply chains often face issues of decreased trust, distances in shipping, complexities and prolonged processing times. Blockchain serves as a productive intervention in the dire requirement for improved traceability of food as regards its security and transparency. To improve the traceability in value chains, a decentralized ledger associates inputs, suppliers, producers, purchasers, controllers that are far separated, who are under various projects, various principles (arrangements) and use various applications. Some major companies such as Walmart and Kroger constitute examples of the

first companies to combine the use of blockchain in their supply chains (CB Insights, 2017). Issues such as data integrity, tampering and a single point of failure are common to a centralized agri-food supply chain system. A blockchain based decentralized system called *AgriblockIoT* was therefore proposed by (Caro et al., 2018) as a result of its inherent properties such as fault tolerance, immutability and transparency. A *from farm to fork use-case*, that is, from agricultural production to consumption use-case, was used to test the feasibility of the solution along the food supply chain. The performance of the solution using Ethereum was compared to the performance while using Hyperledger sawtooth, and results showed the sawtooth showed better performance based on CPU load and latency. However, Ethereum was shown to be better suited when there is a larger number of participants in a network.

4.3 Blockchain in Healthcare

Blockchain technology also allows for the development of several potential applications in health care. Although blockchain remains in its early stages of advancement, numerous health bodies have proposed healthcare interventions such that health data and records are operated efficiently and with transparency. Guardtime, a Netherlands-based information security firm, made a blockchain-based system to secure their patient personal information (Mettler, 2016). Each individual in the community was given a smartcard, which connected their Electronic health records (EHR) information with their blockchain-based identity. An update in the health record was then allocated a hash and enlisted in the blockchain. This methodology guarantees that information inside the record contains a changeless audit trail and that records can't be altered without appropriate access rights. Also, any update in the healthcare database, similar to scheduling an appointment, is allotted a period stamp and then cryptographically marked in a block. MedRec, another EHR venture, offered a decentralized way to deal with overseeing permissions, approvals and sharing health data between healthcare facilities (Azaria et al., 2016). The utilization of blockchain with this application enabled patients to have determine the type of information accessed and who can access their healthcare information. These consents can be shared on a blockchain to ensure information sharing for clinical and research use is done in a computerized manner, even though the real healthcare data are not eventually stored in the blockchain. While the authorizations, data storage locations, and audit trails are stored in the blockchain, all healthcare data stays in EHR platform and requires extra programming to enable genuine interoperability. The major challenge faced by regular EMR systems is the lack of coordinated management of health records, issues in data sharing and retrieval. The proposed system therefore addresses fragmentation, delayed access to patient records, system interoperability and patient agency. Medical personnel were incorporated into the network as miners who secure and sustain the network and get mining rewards in form of access to aggregate anonymized data. The patient records are logged as smart contracts on an Ethereum blockchain. Medrec is shown to be suitable for large scale management of health records with improved flexibility, granularity, integrity and data sharing. The MedRec system has been evaluated and validated as a proof of concept for health and drug information, and thus, biomedical and results research may altogether take advantage of the use of blockchain in providing fast, secure access to research data across borders (Azaria et al., 2016). In spite of the fact that putting away the whole health record inside the blockchain could be imagined as a potential use case for health care, a few potential challenges have been recognized, such as the issues regarding security, compliance with health regulations, and the technical challenges in data storage and distribution. Along these lines, most momentary recommendations have concentrated on validating patient information, reviewing audit trails, and access control. More recent uses of blockchain for internet of things are in internet of healthcare things, internet of things in 5G period, internet of vehicles and internet of device things. Other challenges faced in using blockchain for healthcare is the transparency of highly sensitive patient information, the threat of 51% attack and long transaction times which hampers scalability of blockchain applications. To mitigate these issues, (Kuo et al., 2017) recommend the careful design of blockchain health applications, encrypting sensitive information on the network, storing only verified transactions in the blockchain repository to improve speed and scalability or a BigchainDB and the use of a virtual private network to reduce a 51% attack.

4.4 Blockchain in E-Government

Blockchain allows for more efficient and reliable distribution of public and government services by providing transparency and accessibility of these services, enabling the development of information sharing and individual credit systems (digital identity systems) for citizens Hou (2017). By endorsing and utilizing blockchain technology, the government can strengthen their authority and credibility with the public thus enhancing trust and openness. Hjalmarsson et al., (2018) proposed the design of an e-voting system based on blockchain. The e-voting system contains the election process, that is, the roles in the system, the agreements, and voting transactions in a smart contract as a permissioned blockchain infrastructure. The major roles defined involved the election administrator and the voter only. For the voting phase to occur, each voter gets a transaction ID for their votes, place a vote on the official election site after an authentication phase and the vote is counted. The proposed voting system ensures the voters information is unanimous and untraceable which makes the system flexible and secure. However, some difficulties faced in applying blockchain to e-government includes the cost of implementation, the long term storage and preservation of citizen records, the grave consequences of security breaches in blockchain applications and management and sustainability of the platform.

4.5 Blockchain in Energy Management

The key technologies in blockchain such as consensus mechanisms, encryption algorithms, smart contracts, and distributed data storage are seen to be particularly useful for the construction and development of the Energy Internet. Wu and Tran, (2018) suggested the use of blockchain to solve the problem of control and management of distributed sustainable energy forms for Energy internet and smart grids. Energy internet encompasses sustainable energy and network technologies to mitigate the problems of decentralized geographical distribution, low management and utilization rates, data transparency among stakeholders, inefficient administrative processes, high complexities around energy efficiency market and high energy conversion costs, which reduces the use of new energy for large scale deployments and industrialization. The different applications of blockchain for energy internet is shown in figure 3. Experts have affirmed the promising application of blockchain technology in the energy sector particularly for peer-to-peer energy trading and electric vehicle charging and sharing (Omezzine and Schleich, 2019). The blockchain promises to create a system whereby energy prosumers from the commercial sector or private homes can trade electricity without the interference of a central authority. With the continuous growth of electric vehicles, blockchain promises to provide an adequate, publicly available charging infrastructure that tackles the “lack of range” challenge, by enabling individuals to make their private EV charging stations available for public use for a fee.

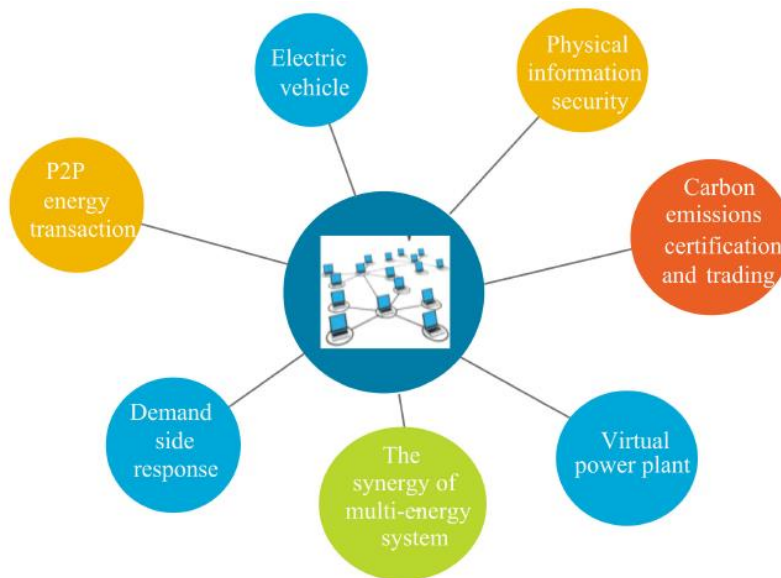


Figure 3. Blockchain in energy internet (Wu and Tran, 2018)

5. Opem Issues

Although blockchain has undergone several innovative advancements, the technology still has some intrinsic security challenges. Some security issues related with the utilization of blockchain for cybersecurity was presented by (Zheng et al., 2017). Blockchain has enhanced trust with its use of complex cryptographic and numerical computations. Other significant benefits in the use of blockchain for security includes privacy security, disaster recovery and providing a tamper proof network. In banking and financial institutions, blockchain encourages cross border transactions, in healthcare, blockchain has been used to store and share patient records and blockchain has been broadly applied in developing smart grids for energy management. Some potential challenges related with using cryptographic calculations in blockchain are the challenges in private key administration and backdoor attacks. To combat these issues, detailed attention must be paid to the innovation testing phase for blockchain, verifying business flows and a standard for blockchain security must be developed and met. Ferrag et al., (2018) compared state-of-the-art advancements in blockchain security and provided open research issues and future headways for blockchain technologies. A major restriction is the constraints of block size which limits the use of blockchain on a large scale. The consensus mechanism of blockchain depends on most nodes being genuine to run and maintain the network. When at least one node controls over 51% computing complexity of the entire framework, combined the nodes can dispatch an assault to alter the contents in the block and cause disruptions, for example, a DDoS attack. Blockchain platforms often stores a total duplicate of all information in the users' side and this gives an attacker an alternative in accessing the user's data unauthorized. Hackers also could likewise use different methods, for example, data mining and correlation investigation in accessing significant data associated with blockchain applications or network structure and user's information which lead to destructive outcomes. Another issue is the potential dangers of cryptographic algorithms utilized.

The use of private keys also contributes to the security risks in blockchain. Existing blockchain applications utilize private keys to affirm a client's identity and complete payments in a transaction. This shows that the vital condition for untampered and immutable information, is the security of private key. In contrast to conventional applications that use public key cryptography, users in a blockchain network oversee their own private keys, which implies that a private key is created and managed by the user not an outsider. If a client loses his private key, it will be difficult to gain access to his digital assets on the blockchain. Blockchain applies several cryptographic algorithms, for example, ECC and RSA in the development of applications. Backdoor intrusions and security vulnerabilities may be found in the algorithms themselves or while implementing the applications. However, with the recent development of quantum computers, Blockchain faces higher risks as quantum computers are capable of cracking asymmetric encryption algorithms within seconds and these algorithms are the backbone of blockchain architectures. Several issues in security management and anonymity are evident in distributed systems and mechanisms. Distributed systems often cause independent and frequent data spread in blockchain use cases. However, blockchain emphasizes data storage in a distributed way and keeps a full duplicate of information at every user's side. Hence, when another transaction is being added to a block, every one of the data duplicates is updated synchronously. Blockchain ascertains the hash value of a party's public key to identify unique users. However, this technique for privacy security, makes it difficult to check and follow a user's identity in the event of an attack.

6. CONCLUSION

Blockchain has undoubtedly become a hot topic in recent years and it has been applied in several fields. Although, blockchain is characterized as being decentralized, transparent, immutable and a secure way for transactions, it still faces major security challenges. Recent studies have focused on enhancing blockchain security, but some challenges still exist. Blockchain is still in its early stages of design and implementation, therefore further research is necessary for its full-scale deployment. In this study, we have provided an overview of blockchain technology, its current applications, and open problems and issues associated with its deployment. While the benefits and advantages of blockchain have been highlighted, we need to be aware of possible future trends and security limitations associated with blockchain technology.

7. REFERENCES

1. Park, J., & Park, J. (2017). Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, 9(8), 164.
2. Ejaz, W., & Anpalagan, A. (2019). Blockchain Technology for Security and Privacy in Internet of Things. In *Internet of Things for Smart Cities* (pp. 47-55). Springer, Cham.
3. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal*, 6(2), 2188-2204.
4. Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)* (pp. 1392-1393). IEEE.
5. Satoshi, N. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, Available at <https://bitcoin.org/bitcoin.pdf> Accessed 28/7/2019.
6. Lamport, L. (1998). The part-time parliament. *ACM Transactions on Computer Systems (TOCS)*, 16(2), 133-169.
7. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.
8. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10), 71.
9. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. "O'Reilly Media, Inc."
10. Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, 26(4), 377-409.
11. Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain Technology in Business and Information Systems Research. *Business and Information Systems Engineering*, 59(6), 381-384.
12. Miraz, M. H., & Ali, M. (2018). Applications of Blockchain Technology beyond Cryptocurrency. *Annals of Emerging Technologies in Computing (AETiC)*, 2(1).
13. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352-375.
14. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184-1195.
15. Vujičić, D., Jagodić, D., & Randić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1-6). IEEE.
16. Kramer, M. (2019). An Overview of Blockchain Technology Based on a Study of Public Awareness. *Global Journal of Business Research*, 13(1), 83-91.

17. Swanson, T. (2015). Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. *Report, available online, Apr.*
18. Tonelli, R., Lunesu, M. I., Pinna, A., Taibi, D., & Marchesi, M. (2019, February). Implementing a microservices system with blockchain smart contracts. In 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE) (pp. 22-31). IEEE.
19. Ameer, Rosic. (2016). Smart Contracts: The Blockchain Technology That Will Replace Lawyers. Available at: <https://blockgeeks.com/guides/smart-contracts/>. [Accessed 29/08/2019].
20. Hyperledger (2015). Hyperledger Business Blockchain Technologies. Available at: <https://www.hyperledger.org/>. Accessed 27/7/2019.
21. Morini, M. (2016). From 'Blockchain hype' to a real business case for Financial Markets. Available at SSRN 2760184.
22. Jaag, C., Moyano, J. P., & Trinkner, U. (2016). Postal strategies in a digital age. In *The future of the postal sector in a digital world* (pp. 103-120). Springer, Cham.
23. Pilkington, M. (2016). Blockchain technology: principles and applications. *Research handbook on digital transformations*, 225.
24. Micheler, E., & von der Heyde, L. (2016). Holding, clearing and settling securities through blockchain technology creating an efficient system by empowering asset owners. Available at SSRN 2786972.
25. Maslova, A. (2017). Growing the Garden: How to Use Blockchain in Agriculture. *Cointelegraph*, November, 2.
26. Agridigital (2017). Building a blockchain for agri-supply chains. Available at: <https://www.agridigital.io/reports/blockchain-pilot-report>. Accessed 29/10/2019
27. Lee, K., James, J. I., Ejeta, T. G., & Kim, H. J. (2016). Electronic voting service using block-chain. *Journal of Digital Forensics, Security and Law*, 11(2), 8.
28. C. B. Insights (2017). Blockchain investment trends in review. CB Insights. Available at: <https://www.cbinsights.com/research/report/blockchain-trends-opportunities>. Accessed 29/10/2019.
29. Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018, May). Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany) (pp. 1-4). IEEE.
30. Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. In *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)* (pp. 1-3). IEEE.
31. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)* (pp. 25-30). IEEE.
32. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 1211-1220.
33. Hou, H. (2017, July). The application of blockchain technology in E-government in China. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-4). IEEE.
34. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983-986). IEEE.
35. Wu, J., & Tran, N. (2018). Application of blockchain technology in sustainable energy systems: An overview. *Sustainability*, 10(9), 3067.
36. Omezzine, F. & Schleich, J. (2019, March 5). The future of blockchain according to experts in the energy sector. *The conversation*. Available at: <http://theconversation.com/the-future-of-blockchain-according-to-experts-in-the-energy-sector-111780> Accessed 28/10/2019.
37. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.