International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 12, Number 12 (2019), pp. 2133-2137
© International Research Publication House. http://www.irphouse.com

An Outlook in Blockchain Technology- Architecture, Applications and Challenges

Dr. Aarthy C[1] & Dr. Aishwarya N[2]

Assistant Professor
Christ (Deemed to be) University, Bengaluru, India.

Abstract:

Blockchain is mechanism which stores and exchange data in a peer-peer network serving as an immutable ledger allowing transactions to take place in decentralized method which neglects the role of intermediaries. The technology reduces greater complexity by combining three key features; security, decentralization and transparency. This paper is an attempt explaining the concepts, structure, applications and challenges the technology has. The paper introduces blockchain taxonomy, reviews applications and discussed technical challenges and way of handling these challenges. Blockchain technology is springing up with promising applications in various fields and the authors have explored about three emerging field of blockchain say; Education, Government and Healthcare. Finally the paper concludes by stating other emerging fields of applications where further research can be explored.

Keywords: Block chain, categories, scalability, performance, applications.

INTRODUCTION

Block Chain is a public ledger storing all transactions in chain of blocks which continuously grows when new blocks are added to it. This technology is supported by integrating other core technology like hash, digital signature and consensus mechanism. Bitcoin is the famous application in block chain but the concept can be applied beyond crypto currencies (Z.Zheng et al., 2018). Block chain is considered to be the most promising technology of future with widespread application in areas like IOT (Zhang and Wen, 2015), smart contracts (Kosba et al., 2016), public services (Akins et al., 2013), security services (Noyes, 2016), healthcare and education (Beck et al., 2017). World economic system depends on individuals and organizations rely on each other to create records like financial, hospital and educational records. These repositories which are created by third party are vulnerable to theft or failure in storage systems thusthe blockchain technology acts as a digital guard mitigating unbiased and incorruptible data. (Naerland et al., 2017).The following section of the paper discuss about the types, characteristics, architecture, application, challenges of blockchain.

At present there are three types of blockchain as: Public, Consortium and Private. The categorization is done based on the factors like modification, network nodes, acceptance of nodes, validation and authorization as depicted in below table.

Table 1: Categorization of Blockchain

FACTORS	PUBLIC BLOCKCHAIN	CONSORTIUM BLOCKCHAIN	PRIVATE BLOCKCHAIN
Modification	Blocks are validated one on another and modification is not possible	Blocks are validated one on another and modification is not possible	Blocks are validated by an authority and can be modified.
Network Nodes	Nodes Chosen automatically	Nodes chosen automatically	Nodes selected by authority
Acceptance	Any new participants can be added to network	Consensus algorithm plays a role in accepting new nodes	Central authority accepts new nodes.
Validation	Participants have rights to validate the blocks	Validation is possible based on predefined rules	Validation is by central authority
Readability	Participants can read data in blocks	Limited to certain nodes	Limited to central authority

The block chain technology works on basic four characteristics such as decentralization, persistency, anonymity and auditability. Decentralization, the key feature of block chain is that it does not require any third party validation; instead consensus algorithms are used to maintain data consistency. Persistency is the act of miners validating invalid transaction at a faster rate because it's difficult to rollback transactions once they are included in the block. Anonymity is user interacting with the blockchain with a generated address without revealing identity of the user which becomes sometimes a threat to privacy. Auditability is the process of validating and tracing out the transactions iteratively in any node of the network with the help of timestamp.

Though the blockchain has great potential for the future internet system, it has two primary challenges: Security (major attacks, selfish mining, anonymity and privacy) and Performance issues (Scalability and availability) (Gao et al., 2018). Technical challenges like scalability arises like in, bitcoin is restricted to 7 transactions per second, which is not capable of dealing with high frequency trading. When the

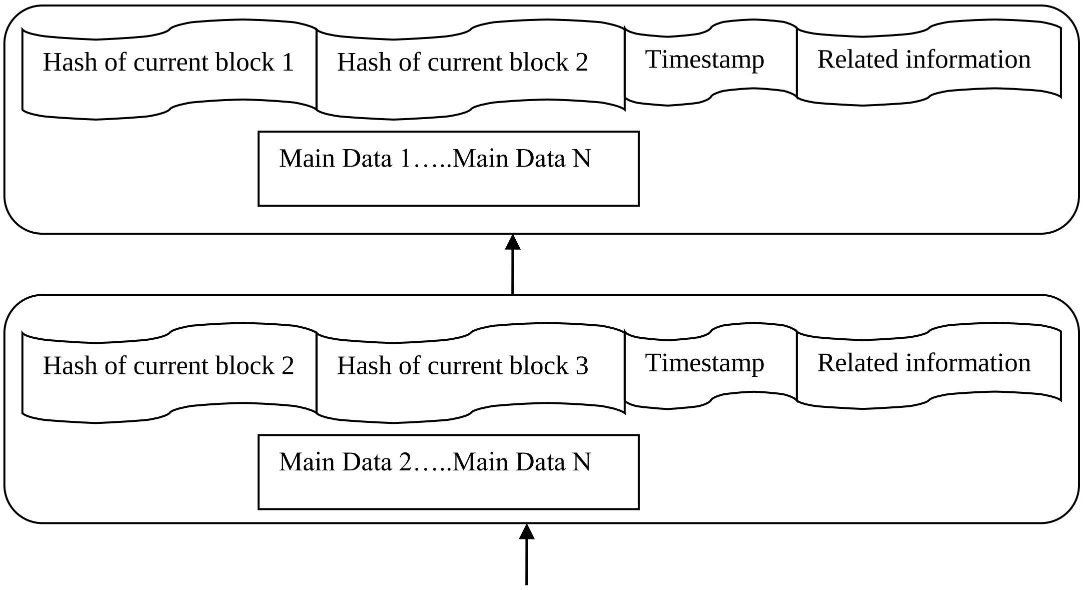

Figure 1. Architecture of Blockchain

block size increases the storage space increase and network propagation decreases leading to trade-off between block size and security. It is evident that miners can earn good revenue than the fair share by using selfish mining strategy (Eyal and Sirer, 2014; Zeng et al., 2018) which is a technique of hiding mined blocks eventually hinders blockchain development. The data leakage happens when users make records through public and private key (Biryukov et al., 2014) and also there is possibility of tracking user's real IP address. The two distinct algorithm of block chain Proof of Stake (PoS) and Proof of Work (PoW) also face certain issues like usage of too much electricity.

The structure of blockchain contains main data, hash of previous block, hash of current block, timestamp and related information. The structure of blockchain is depicted in Fig.1

The main data here denote the transaction that takes place like banking records or contract records or medical records or IOT records. Each block has set of transactions or new records as well as the hash value of previous block (Gao et al., 2018). The blockchain uses Merkle Tree to generate hash value which will be recorded in block header i.e. current block. Time stamp is the amount of taken to generate a block. Related information refers to Nonce values, signature or other data defined by user (Lin and Liao, 2017).

APPLICATION OF BLOCKCHAIN IN VARIOUS SECTORS

Education

Blockchain is predominantly used in online education system these days. Online education system is an internet based teaching method for course delivery and quicker learning through recent technologies (Sun and Wang, 2018).Online education platforms are being immensely popular in the current trend, as they provide new courses with facilitators from all over the world. Propounded in the US, content providers such as EdX, Coursera and Udemy are gaining attention among Indian learners. Even the SWAYAM platform initiated from the government of India provides certification courses on various disciplines from experienced IIT and IIM professors. In such case, there is a growing demand for issuing, storing and sharing students' academic certificates and transcripts via this platform (Ali et.al., 2019). This acts as a digital wallet for the students who can see and control whom they share information with. However, the current forms of online education model have got many disadvantages in terms of privacy and flexibility (Sun and Wang, 2018). The learning process and results are under a constant threat as learning happens in an open centralized platform. Students' knowledge and their intellectual capacity are at risk and there is no mechanism to fully transfer learning resources and materials. Hence, to make the process more trustable, it becomes essential to build a distributed and credible data storage tool to store the students' learning process and share data in public and make it easier to be downloaded by the employer (Sun and Wang, 2018).

There are blockchain based applications which evaluate students' professional skills based on their learning. Apart from this security in the form data protection, privacy and integration to education models are considered to be the most important application of blockchain in education sector which ensures prevention of degree fraud to a greater extent. There are also researches focusing on blockchain based application which reduces the education cost of the students' fraternity (Ali et.al.,2019). This technology can detect and prevent paper fraud, fake certification and other destructive activities in the education sector. It also benefits in the way of encouraging knowledge management within an institution and promotes further research and development. Overall, blockchain in education sector can be used to build a balance between the learning in the class and outcomes of the process (Chen et.al., 2018).

Government

Governments across the world in the last decade are focusing on moving to e-government platform and are using digital tools to support their infrastructure and increase their efficiency. Given the amount of data each government handles, it's not surprising to see that many of them have chosen distributed ledger technology. Since blockchain technology is extremely good at creating trust among the users in terms of data and processes, its applications are tried and tested upon various platforms. This technology offers data integrity, transparency, fraud prevention, manipulation avoidance, corruption reduction and also builds trust, security and privacy. In 2017, 117 initiatives have been taken by 26 countries in blockchain technology. Among which, governments such as EU, USA, UAE, China, Russia and India have rigorously initiated projects to implement blockchain technology across industries (Lyons et.al., 2019). The major themes which these government addresses are digital identity, payments and supply chain and provenance (Hardjono, 2017). Apart from this, smart cities, digital currencies, vaccination tracking, student grants and loans tracking, payroll tax collection and validation of education and professional qualifications are the other areas of interest. Contract and vendor management is one area which allows complete transparency of government expenditures. To avoid ballot-rigging and to conduct smooth elections, governments are planning to use digital voting mechanism enabled by blockchain technology to ensure accuracy and error free counting (Observatory of Public sector innovation blockchain report, 2018). Smart contracts technology can be utilized to track social security benefits, international aids, and anticipatory payments. Land registry programs can also be handled via blockchain technology to record real estate and property related transactions.

Some of the examples of government led blockchain projects include China's social security funds management system initiative in 2016, mortgage valuations on blockchain in 2016, Blockchain based asset custody system in 2016 and Blockchain city project in 2016. Also, Chinese government leads the world in blockchain standardized certification, where companies like Lenovo, aelf and Alipay are some of them to receive it (prnewswire,2019). Dubai Government has initiated Smart Dubai program to focus on government efficiency, global leadership and industry creation by leveraging the recent technologies such as Artificial Intelligence, Internet of Things and Blockchain. Similarly they have begun documents management system in 2018, Blockchain based digital passport initiative in 2017 and Blockchain based real-time information on shipments in 2017.Estonia's eID system in 2018, e-health system, and e-residency program are initiated and trail runs are being are carried out. Russia has begun document management program, and blockchain based health pilot program in 2017. Singapore's Project Ubin and cross border interbank initiative aims at building banking innovation and industry leadership. Sweden's smart contract technology for land registry was initiated in 2018. USA introduced Pilot project for secure exchange of personal health data online in 2016, as well as Blockchain based birth certificates in 2017 and making smart contracts legal in Arizona in 2017 (Jun, 2018). In July 2018, UK's FSA developed blockchain based meat tracking platform to ensure compliance in the food sector (Jun 2018) .Denmark's Vehicle wallet partnership program between the payment service provider and the Danish Administrative office acted as a great supply chain management tool to reduce risks involved with the buyers and the suppliers as well as in collecting taxes (Observatory of Public sector innovation blockchain report, 2018). .

Overall, smart cities can be built using blockchain technologies implemented in the areas of commerce and investment; municipal and health affairs; education, health; utilities such as asset management; safety and justice; labour and social development; communication and information; environment and agriculture ; and tourism and antiques (Synergy report, 2019). It can be understood that blockchain technology will act as a great instrument for social innovation and uplift of the government activities in terms of efficiency, effectiveness and innovation. Bitcoin based blockchain transactions can be done four times per second and ethereum based transactions can be done nine times per second (Jun, 2018), this improves the speed of smart contracts and achieves greater performance in processing.

Healthcare

The present healthcare industry is tormented by numerous inefficiencies, red-tapeism, errors and administrative costs. A decentralized and distributed digital ledger like Blockchain could have widespread applications in healthcare industry. Some of them include drug counterfeiting (BlockchainPulse, 2018), clinical trials (Mackay et.al., 2019), patient data management, Billing and processing claims (Yaeger et.al., 2019), electronic medical records (Agbo et.al., 2019), health data analytics (Agbo et.al., 2019) and dental industry. The problem with fake drug is that it isn't original and also differs from the original product in terms of quality and quantity. The patients who take these fake drugs can suffer in innumerable ways by experiencing the disease pain as well as the side-effects of the fake drug. Blockchain can be used to solve this problem by offering the security in drug traceability. When a drug is produced, a hash will be created containing the relevant information of the drug and then on, each transaction will be added to the digital ledger from the supplier to distributor to customer. This is beneficial to companies' too in terms of tracking down their product in case of a problem. Clinical trials have huge financial investment with very less data management. It is possible for any individual to tamper the data to stop the advancement of a particular clinical trial. Blockchain can provide proof of existence of any document and provide authenticity and tracking to user who has handled the data (Mackay et.al., 2019).

Data ownership and privacy is another area where blockchain application would revolutionize the way the industry operates. There are concerns between a doctor and the patient in terms of who owns and controls the data. Smart contracts can be implemented to simplify the process of data consent and also the patient has the knowledge of what data of them is been handled by the hospital management (Vaziraniet.al., 2019).Similarly, patient data from IoT wearable’s can be regulated via smart contracts to adopt further treatment. Blockchain in healthcare industry garnered much attention in 2017 when Initial Coin Offerings (ICO) were sold by the health care companies, from then on there have been ups and downs for crypto currency prices as well as in the ICO. Some of the startups such as Guard time, Gem Health, Cyph, MedRec, and Blockchain Health are working in this area.

Challenges

Though blockchain has enormous potential there are still challenges with respect to security and performance issues. The security depends on the hardware, software and protocols implemented for its function. Scalability, Privacy leakage and Selfish mining are the three major challenges related to blockchain. Scalability arises with the increasing number of transactions and each node should be validated for the data stored on it. There exist a restriction with respect to block size and the time interval used to generate a new block since the blockchain can process only 7 transactions per second. Storage optimization and redesigning of blockchain solution was proposed to address scalability issue, where in former method network removes old transaction records (Bruce, 2014) and later method is to de-couple conventional block into two parts namely key block (leader election) and micro block (store transaction) (Eyal. I et al., 2016). The privacy of transaction can be preserved through public and private key but still there is no guarantee of transactional privacy since the public key exhibits balances and transactions (Meiklejohn S et al., 2013 and Kosba et al., 2016). To improve the anonymity of blockchain, Mixing and Anonymous techniques were proposed. Mixing is the act of providing security by transfer of funds from multiple input addresses to multiple output address. Anonymous is usage of zero-knowledge proof where transaction amount and values of coins held by users are hidden (Zeng et al., 2017). Selfish mining is a strategy where miners keep their mined blocks without revealing and the private branch will be revealed to public only when it’s longer than public. The honest miners tend to waste their resources and time while selfish miners are building their private branch without competitors generating more revenue. This can be put an end by the concept Zero block proposed by Solat and Butucaru (2016): where each block is generated and accepted by network with a limited time interval so that they can’t gain more than its expected reward.

However attractive and appealing is a recent technology like Blockchain, it has its own share of disadvantages in utilization and implementation which worries the users associated with it. Security is still questioned as an important topic in blockchain, as it can be considered as an advantage and if not implemented properly can lead to data hacking and other malicious activities. Having the blind trust on the blockchain developers, the companies, lawmakers and the law enforcement questions the trade-off between security and performance. As with any technology, the cost of building and running the system from scratch will be expensive for both governments as well as private entities; as long as the benefits outrun the expense - implementing this technology would be worthwhile. Overall, the immaturity of the technology itself is considered as a serious challenge given the amount of hype this technology receives. Nevertheless, it is still common for any new technology to be criticized for its features. However, the potential for blockchain is still unexploited and could have applications in various fields that work on bureaucracy and storage.

CONCLUSION

Blockchain has its potential in transforming traditional system to enhance their performance with its key features. In this paper we have given an outline about blockchain including its architecture, key features application in emerging areas, challenges faced and few methods to solve these concerns. Blockchain can be applied in areas of Big Data, IoT, Edge computing, cloud computing, artificial intelligence, smart contracts, medical informatics, supplychain, education, finance and business solutions. This technology is still in the budding stage but widely implemented in many real-world applications and gives future direction of research towards in-depth investigation in the field of above mentioned.

REFERENCES

[1] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future, *Trends, 2017 IEEE 6th International Congress on Big Data*, 557-564.

[2] Zhang, Y.L., & Wen, J. (2015). An IoT Electric Business Model Based on the Protocol of Bitcoin. *18th International Conference on Intelligence in Next Generation Networks*, 184-191.

[3] Kosba, Ahmed & Miller, Andrew & Shi, Elaine & Wen, Zikai & Papamanthou, Charalampos. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, *IEEE Symposium on Security and Privacy*, San Jose, USA, 2016.839-858.

[4] Akins, B. W., Chapman, J. L., & Gordon, J. M. (2015). A Whole New World: Income Tax Considerations of the Bitcoin Economy. *Pittsburgh Tax Review*, 12(1), 24–56.

[5] Noyes, C. (2016). BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning. *ArXiv*, abs/1601.01405.

[6] Beck, Roman & Müller-Bloch, Christoph. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers as Incumbent Organization. *2017 Hawaii International Conference on System Sciences*.10.24251/HICSS.2017.653.

[7] Nærland, Kristoffer & Müller-Bloch, Christoph & Beck, Roman & Palmund, Søren. (2017). Blockchain to Rule the Waves – Nascent Design Principles for Reducing Risk and Uncertainty in Decentralized

Environments. International conference on information systems, Seoul.

[8] Gao, W., Hatcher, W.G., & Yu, W. (2018). A Survey of Blockchain: Techniques, Applications, and Challenges. *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 1-11.

[9] Eyal, I., & Sirer, E. G. (2014). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. *Financial Cryptography and Data Security Lecture Notes in Computer Science*, 436-454. doi: 10.1007/978-3-662-45472-5_28

[10] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services. 14 (4), 352-375.

[11] Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of Clients in Bitcoin P2P Network. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,* New York, 15-29.

[12] Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *IJ Network Security*, 19(5), 653-659.

[13] Agbo, C. C., Mahmoud, Q. H., &Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare (Basel, Switzerland)*, *7*(2), 56. doi:10.3390/healthcare7020056

[14] Ali Alammary ,SamahAlhazmi, MarwahAlmasri and SairaGillani, Blockchain-based application in education: A systematic review, *Applied sciences*, 2019, 1-18

[15] Carter and Ubacht, Challenges of Blockchain Technology Adoption for e-government: A Systematic Literature review, *Blockchain application in government*, 2018, 1-9

[16] *Chinese Government Leads the World in Blockchain Standardized Certification,* prnewswire, https://www.prnewswire.com/news-releases/chinese-government-leads-the-world-in-blockchain-standardized-certification-300888136.html accessed on 27.9.19.

[17] Constantin, Uses cases for blockchain tech in healthcare, *Blockchain Pulse: IBM Blockchain blog*, 2018.

[18] Guang Chen, Bing Xu ,Manli Lu and Nian-Shing Chen, Exploring Blockchain technology and its potential applications for education, *Smart learning environments- Springer Open*, 2018

[19] Mackey, Kuo and et.al, 'Fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare, *BMC Medicine*, 17(1), 68. Doi: 10.1186/s12916-019-1296-7

[20] MyungSan Jun, Blockchain government - a next form of infrastructure for the twenty-first century, *Jun Journal of Open Innovation: Technology, Market, and Complexity*, (2018) 4:7

[21] Report on Blockchain and its use in the Public sector, Observatory of Public sector innovation June 20, 2018

[22] Report on blockchain in government, future synergy, 2019

[23] Sun and Wang (2018), Application of Blockchain Technology in Online Education, International Journal of Emerging Technologies in Learning,*, vol 13, No 10, 252-259*

[24] *Thomas Hardjono, A report on the impact of Blockchain for government, MIT Connection science, 2017, 4-40*

[25] Tom Lyons, LudovicCourcelas, Ken Timsit,*Blockchain in Europe: Scalability, interoperability and sustainability,*The European Union Blockchain Observatory and Forum*, 2019, 1-29*

[26] Tom Macaulay, How governments around the world are using blockchain, Computer world, 19 September 2019

[27] Vazirani, A. A., O'Donoghue, O., Brindley, D., &Meinert, E. (2019). Implementing Blockchains for Efficient Health Care: Systematic Review. *Journal of medical Internet research*, *21*(2), e12439. doi:10.2196/12439

[28] Yaeger, K., Martini, M., Rasouli, J., & Costa, A. (2019). Emerging Blockchain Technology Solutions for Modern Healthcare Infrastructure. *Journal of Scientific Innovation in Medicine*, *2*(1), 1. DOI: http://doi.org/10.29024/jsim.7.

[29] J. Bruce.(2014). The mini blockchain scheme. Online Available: http://cryptonite.info/files/mbc-schemerev3.pdf.

[30] I.Eyal, A.E.Gencer,E.G.Sirer, R. Van Renesse (2016). Bitcoining: A scalable blockchain protocol. *13 USENIX Symposiums on Networked Systems Design and Implementation (NSDI 16),NY*, 1304-1316.

[31] S. Meiklejohn, M,Pomarole, G.Jordan, K.Levchenko, d.McCoy, G.M Voelker and S.Savage. (2013). A fistful of bitcoins: characterizing payments among men with no names. *2013 Conference on Internet Measurement Conference (IMC 13), NY.*

[32] S.Solat and M.Potop-Butucaru. (2016). Zeroblock: Timestamp-free prevention of block-withholding attack in Bitcoin. UPMC University of Paris, Technical Report.