International Journal of Innovative Research in Engineering & Management (IJIREM)
ISSN: 2350-0557, Volume-7, Issue-3, May 2020
www.ijirem.org

Block Chain: Review and Application

Ankur Daksh
Student,
Department of Computer Application,
International Institute for Special Education,
Lucknow, India

Manoj Kumar
Senior Assistant Professor,
Department of Computer Application,
International Institute for Special Education,
Lucknow, India
iisemanoj@gmail.com

ABSTRACT
Blockchain technology has been referred to as a digital currency platform since the emergence of Bitcoin, the primary and the largest of the cryptocurrencies. Formerly, it's used for the decentralization of markets more generally, not exclusively for the decentralization of cash and payments. The decentralized transaction ledger of blockchain might be employed to register, confirm, and send all types of contracts to other parties in the network. During this paper, we thoroughly review state-of-the art blockchain-related applications emerged within the literature. A number of published works were carefully included supported their contributions to the blockchain's body of data.

Keywords
Blockchain, Digital Currency, Smart Contract, Decentralized

1. INTRODUCTION
Introduced by one or more individuals under the pseudonym Satoshi Nakamoto [1], the cryptocurrency Bitcoin and therefore, the underlying blockchain technology (BCT) have created an incredible hype around electronic payment systems using the peer-to-peer paradigm of the web [2, 3]. More generally, BCT provides the infrastructure that permits secure direct exchange useful between participants with none financial intermediary ('internet of value') [4]. Blockchain technology is currently being successfully applied to both financial markets also as quite few non-financial applications. Since the arrival of blockchain many researchers have considered the distributed peer to see model for blockchain as an invention like a external-combustion engine or the web, having the potential to completely alter the planet of commerce and beyond [5]. Meanwhile, blockchain are often seen as a neighborhood of the implementation layer of a distributed software. The info integrity in distributed systems are often achieved and maintained using blockchain [6]. Furthermore, blockchain might be also considered as a purely peer-to-peer system which is formed from the individual nodes during a network.

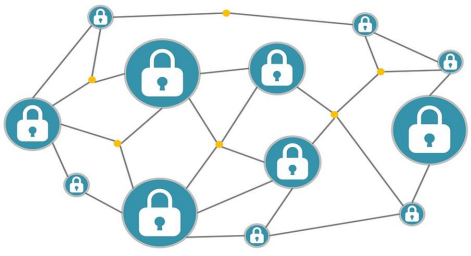

Figure 1: Blockchain[48]

Dishonest and malicious peers become the crucial integrity threat in peer-to-peer systems. The individual nodes attempt to exploit the system for his or her own purposes since unknown peers with unknown reliability and trustworthiness may exist [7]. Thus, these critical problems are needed to be solved by blockchain. Originally, the most area for blockchain is connecting cryptocurrencies with conventional banking and financial institutions. Blockchain technology offers an ovel banking ecosystem thus enabling financial institutions to conduct their financial transactions directly between themselves with none central authorities or intermediaries. Every transaction must be authenticated through the agreement of quite half those participating within the network [8]. This suggests that no participants would be ready to modify any data within the blockchain without the approval of other participants.

1.1 Types of Blockchain[46]
Blockchain is the foundation of the digital cryptocurrency, Bitcoin. It has raised its sheer importance in the digital world by holding its critical character traits of decentralization, immutability, anonymity, and suitability for the e-money transaction process. There are primarily four types of blockchains to be considered.

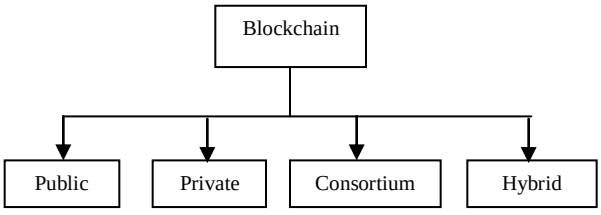

Figure 2: Different types of blockchain and their attributes

1.1.1 Public Blockchain
It is a non-restrictive, permissionless distributed ledger system. It marks the start of the main sorts of blockchains we all know today. Bitcoin, Litecoin and Ethereum are the blockchain platforms that are typical samples of a public blockchain. So, what are public blockchains? As the name suggests, this blockchain is 'for the people, by the people, and of the people.' Anyone having access to the web can become a licensed node by signing in to the blockchain platform. They are then considered a part of the blockchain network. In this blockchain, there's nobody

responsible, and anyone can participate in writing, reading, or auditing the blockchain. These blockchains are open and transparent. In a public blockchain, deciding happens through consensus algorithms like proof-of-work proof of stake. Consensus algorithms refer to a decision-making process for a group, where individuals of that group support the decision that works best for everyone.

- A public blockchain network lets people do the subsequent things.
- Anyone can run nodes and start mining.
- Anyone can review or audit the blockchain employing a blockchain explorer.
- Anyone can engage in transactions.

1.1.2. Private Blockchain

This refers to a closed blockchain network, and this network isn't completely decentralized and distributed sort of a public blockchain. It is the private property of an organization or an individual. Unlike public blockchains, there's an individual who is responsible here and appears after important things like read /write and to whom access must tend to read. Here, consensus or decision-making is achieved on the whims of the central in-charge who will decide whom to give mining rights or will even decide not to give at all. Private blockchains comprise of specific constituent nodes on the network that are given the rights to create, view, and authorize transactions. The blockchains developers will choose the node which will get the transaction rights. The authorizations, permissions, accessibility, and level of security in the hands of the controlling organization. Public blockchains have a small and restrictive network. The blockchain platforms that fall into the private blockchain category are Hyperledger Fabric, Hyperledger Sawtooth, Corda, and Multichain.

In a public blockchain, the subsequent things aren't possible:

- Anyone cannot make transactions on the blockchain.
- Anyone cannot run a node and start mining.
- The blockchain can't be audited or reviewed by a random user or node.

1.1.3. Consortium Blockchain

It is a semi-decentralized sort of blockchain where a blockchain network is managed by quite one organization. It is part public and part private and hence a combination of both public and private blockchains. The split between the public and private nature happens based on the consensus. In a consortium blockchain, only a couple of nodes or users are given the proper to authorize transactions and oversee the consensus process. The division of rights and powers will be different for each individual consortium blockchain. Consortium blockchains are governed by a group and not by a single entity. Some of the typical examples of consortium blockchains are Quorum, Corda, and Hyperledger.

1.1.4. Hybrid Blockchain

It is a mixture of a public and personal blockchain because it combines the features of both because it lets one have a public permission less system and a personal permission system. The nodes or users can control the feature of who gets access to which data on the blockchain. Dragonchain may be a perfect example of a hybrid blockchain. It provides businesses with the flexibility the data that they want to keep public and transparent and the data that they want to keep private. This allows businesses to operate with transparency without having to forego security and privacy. This is then followed by storing the data in the public blockchain without compromising data privacy. It provides flexible control over the blockchain. Hybrid blockchain is used for scalability and decentralization.

2. RELATED WORK

Aishath Muneeza et_al. propose the emergence of innovative digital financial technologies, namely blockchain and crowdfunding, indicates new ways to succeed in the poor and economically vulnerable groups. This paper contributes to the emerging literature on financial technology by presenting the case of crowdfunding in financial inclusion. The rationale behind this inquiry is to demonstrate the relevance of crowdfunding to financial inclusion, and the way might blockchain technology fuel the event of crowdfunding. This paper also constitutes one among the primary attempts to analyse crowdfunding in Malaysia and Shariah-compliant crowdfunding. during this paper, a desk research is conducted where journal articles, books, magazines, newspapers, industry reports published on the topic matter are reviewed critically. To analyse the event of crowdfunding in Malaysia, 6 crowdfunding platforms are examined. the result of this research suggests that crowdfunding may be a viable means to market financial inclusion, and blockchain technology could help mitigate the present issues faced by platform operators [9].

Friðrik Þ. et_al. building associate electronic electoral system voting system legal needs of legislators has been a challenge for an extended time. Distributed ledger technologies is associate exciting technological advancement within the info technology world. Blockchain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to guage the applying of blockchain as service to implement distributed electronic option systems. The paper elicitates the necessities of building electronic voting systems and identifies the legal and technological limitations of mistreatment blockchain as a service for realizing such systems. The paper starts by evaluating a number of the popular blockchain frameworks that provide blockchain as a service. we tend to then propose an ovel electronic voting system based on blockchain that addresses all limitations we tend to discovered. additional usually this paper evaluates the potential of distributed ledger technologies through the outline of a case study, particularly the method of associate election and implementing a blockchain-based application that improves the safety and reduces the value of hosting a nationwide election[10].

Iuon-Chang Lin et al. proposed a replacement scheme for Block chain technology which can bring more reliability and convenient services. This technology isn't one technique but it contains cryptography, mathematics, Algorithm etc. to unravel traditional distributed database synchronize problem. This paper

also specialise in the safety issues and challenges behind the this innovative technique[11].

Gregor Blossey et_al. given the hype round the cryptocurrency Bitcoin, blockchain technology (BCT) has also received considerable attention outside the financial sector. Multiple applications of BCT in supply chain management (SCM) are discussed in business practice and there's increasing interest during this topic within the tutorial community. During this paper, we shall combine these two perspectives on BCT in SCM to summarize a current state of the art and to derive avenues for further research. For this purpose, a comprehensive framework of use case clusters of BCT in SCM is developed consistent with the distinctive features of BCT. The framework is employed to research 53 applications of BCT in SCM which are derived from a scientific literature review and a secondary dataset of blockchain-driven innovations in SCM. We identify five emerging use case clusters of BCT in SCM which clearly extend the scope beyond frequently mentioned applications like product tracking and tracing[12].

3. WORKING OF BLOCKCHAIN[11]

The main operating processes of blockchain area unit as follows:

- The causing node records new knowledge and broad casting to network.
- The receiving node checked the message from those knowledge that it received, if the message was correct then it'll be keep to a block.
- All receiving node within the network execute proof of labor (PoW) or proof of stake (PoS) algorithmic program to the block.
- The block are going to be keep into the chain when death penalty agreement algorithmic program, each node within the network admit this block and can ceaselessly extend the chain base on this block.

3.1 Structure of Blockchain

Generally within the block, it contains main information, hash of previous block, hash of current block, timestamp and alternative info.

Main data: Counting on what service is that this blockchain applicate, for example: group action records, bank clearing records, contract records or IOT information record.

Hash: once a group action dead, it had been hash to a code so broadcast to every node. as a result of it may well be contained thousands of group action records in every node's block, blockchain used Merkle tree perform to come up with to come up with hash worth, that is additionally Merkle tree root. This final hash worth are going to be record in block header (hash of current block), by victimisation Merkle tree perform, information transmission and computing resources are often drastically reduced.

Timestamp: Time of block generated.

Other information: Like signature of the block, time being worth, or alternative information that user define.

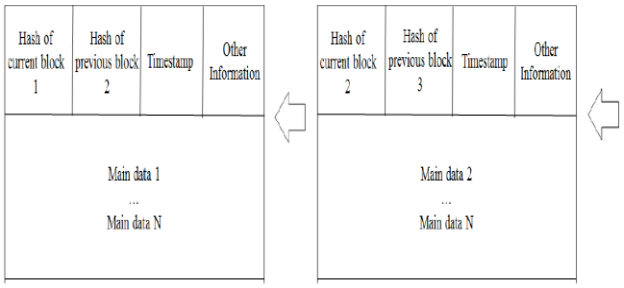

Figure 1: The structure of block chain[11]

3.2 Consensus Algorithm

A network that's receptive everybody and at the same time maintains user's namelessness without doubt raises trust problems relating to the participants. So, to make the trust the participants ought to undergo many accord algorithms like Proof of labor and Proof of Stake.

3.3 Proof of Work (PoW)

A proof of Work may be a piece of information that is difficult (costly or time-consuming) to supply however straight forward for others to verify and that satisfies bound needs. manufacturing a symptom of work is a random method with low likelihood in order that a great deal of trial and error is needed on the average before a legitimate proof of Work is generated. Bitcoin uses the Hashcash proof of Work system. once calculative prisoner, it's referred to as "mining". every block contains a random price referred to as "Nonce" in block header, by ever-changing this present price, prisoner ought to generate {a price|a worth|a price} that produces this block header hash value but but Target" that has already been came upon. Difficulty means that what proportion time it'll take once the node calculative hash price but target price. so as for a block to be accepted by network participants, miners should complete a symptom of work that covers all of the information within the block. The difficulty of this work is adjusted therefore on limit the speed at that new blocks is generated by the network to 1 each ten minutes. thanks to the terribly low likelihood of prospering generation, this makes it unpredictable that employee pc within the network are ready to generate consecutive block [38,44].

3.4 Proof of Stake (PoS)

Because Proof of work methodology can cause a great deal of electricity power and computing power be wasted, Proof of Stake doesn't would like big-ticket computing power. With Proof of Stake, the resource that's compared is that the quantity of Bitcoin a manual laborer holds - somebody holding 1 Chronicles of the Bitcoin will mine 1 Chronicles of the "Proof of Stake blocks" [14]. a symptom of Stake methodology may give redoubled protection from a malicious attack on the network. further protection comes from 2 sources:

1) capital punishment an attack would be far more big-ticket.

2) Reduced incentives for attack. The assailant would want to possess a close to majority of all bitcoin. Therefore, the assailant suffer severely from his own attack.

4. BLOCKCHAIN METHODOLGY[47]

Too often confused with cryptocurrencies, blockchain may be a generic term for methodologies designed for managing data and

operating databases. Somewhat confusingly, a database, platform or system built using blockchain methodology is typically itself called a blockchain.

The principles driving the blockchain methodology are easy to know, but life quickly becomes more complicated and confusing once you check out its mechanics.

Having looked in our previous block at why crypto currencies are only one blockchain application, and searching forward to future blocks during this series where we'll examine specific blockchain applications also as applicable law and regulation, now looks like an honest time to dive into how blockchain works.

4.1 Incorruptible distributive digital ledger

In block 1 we said that blockchain may be a methodology with which to create databases which it's one common distinguishable feature: distribution. In an undistributed database, data is stored in one place such as the server of a document management system, and while one computer updates data, the others are locked out. By contrast with a database built as a blockchain, the knowledge shared (the 'ledger') is stored on each computer on the network (or 'node') and each time the ledger is updated, the update is downloaded to each node. So, all users each have their own identical copy of the ledger, can see any changes while they're being made, and no information gets lost.

4.2 Create, Review, Update And Delete

Traditional databases are based on the 'CRUD' model: create, review, update and delete.

The C is secured through large scale peer-to-peer review: as the ledger is public – between all users who have access to the database – everyone can see the data, and any new piece of data must be verified and accepted by the network before it can actually be created. Any attempt to create false data, or to validate a fraudulent transaction does not withstand digital review: by comparing each other's ledger, honest nodes will instantly spot that their ledgers don't match with the bad or corrupted nodes' ledgers which consequently their ledgers are right and therefore the one that doesn't match the bulk must be wrong.

For that reason, blockchain advocates argue that it's 'incorruptible'.

4.3 Dual Key-Pair System

The R (for review) is secured through a dual key-pair encryption system: only the user who has encrypted the data with his private key can decrypt and review it. Indeed, blockchain works on a dual key-pair system. Every user has both a public and a private key. The public key can be compared to someone's address and the private key to the house key: the public key and the public information it contains is distributed throughout the network (publicly available such as in an address book), whereas the private key is only known to its owner. The public key is linked to the private key, so before transacting on a blockchain database, a user can verify that they are transacting with somebody holding that particular private key. The private key's wont to control which public information a user shows to whom, to encrypt bits of knowledge or sign transactions.

4.4 Encryption

All data is recorded on a blockchain database employing a sort of encryption called 'hashing'. This method turns data, through a basic algorithm [1] , into a sequence of numbers and letters (a 'hash'). This hash is usually an equivalent length no matter the dimensions of the info encrypted. It works in order that an equivalent data will generate an equivalent hash, but a small change within the data will produce a completely different hash. Once information has been hashed, it is impossible to reverse the process, unless one holds the private key which was used to encrypt the particular data in the first place.

5. APPLICATION OF BLOCKCHAIN

Blockchain technologies are often utilized in numerous sets of applications. it's vital to know that Bitcoin isn't equal to blockchain; instead, it's one amongst the foremost flourishing applications of blockchain technology . Bitcoin may be a cryptographic digital currency, that is transacted over an open, public and anonymous blockchain network. The implementations of blockchain technology in different areas are thoroughly discussed. Furthermore, such applications have been categorized into several groups, i.e. financial services, healthcare, business and industry, and other novel applications.

5.1 Financial Service

Blockchain has been wide applied for monetary dealing that is alleged cryptocurrency. Nowadays, cryptocurrencies have appeared as outstanding software package systems. Cryptocurrency has its own currency (coin). Mining is that the method of introducing a brand new block into blockchain. Every node uses blockchain to verify whether or not the coin is legitimate or if it's not spent already. Before the dealing records, square measure appended into blockchain, a bigger variety of participants reaches associate degree agreement. Mining method could be a resource-intensive task, so makes it powerful for associate degree wrongdoer to validate associate degree invalid dealing. every mined-block is verified to visualize if it's whether or not a sound proof of labor [13] or a symbol of stake [14]. The followings square measure the rife steps in cryptocurrency: (i) a generated address (public key) is out there for a user WHO contains a case; (ii) a non-public secret is assigned to the case. it's wont to sign dealing and proving possession; (iii) the money dealer sends coin to the receiver mistreatment given address and sign it mistreatment payer's personal key, and eventually; (iv) the dealing is valid via mining method. Eleven cryptocurrency sytems square measure enclosed in our study, i.e. Bitcoin [1], Litecoin [15], Peercoin [16], Primecoin [13], Ripple [17], Ethereum [18], Permacoin [19], Blackcoin [20], Auroracoin [21], Darkcoin [22], and Namecoin [23].

5.2 Healthcare

Blockchain encompasses a tremendous potential in addressing the ability problems exist within the current aid systems [24]. It may be used as a regular that permits the stakeholders, i.e. aid entities, medical research worker, etc to share electronic health record (EHR) in a very secure manner [25]. Sharing of HER permits North American nation to enhance the standard of treatment [26] and enhance the advice for doctors [27], as an example. However, managing aid knowledge, i.e. acquiring, storing, and analyzing isn't a straightforward task, notably just in case of privacy problems. Aid knowledge mustn't be discovered to different parties that it'd be susceptible to be used fraudulently by malicious users or attackers. So as to induce the higher of these problems, a aid knowledge entry (HDG) supported the blockchain storage platform is projected by [28]. It's a smartphone application which might be wont to manage and management the information sharing simply. The projected system permits users to method the patient knowledge while not

exposing patient privacy. Moreover, a non-public blockchain cloud is employed to hold on {the knowledge |the info |the information} so making certain the medical data cannot be altered by anybody, as well as physicians and patients. The work [29] emphasizes on the planning of a brand new system to rank patient agency, referred to as MedRec. It's a distributed ledger protocol that uses public key cryptography to form blockchain. The blockchain replicas are distributed on every node within the network. just like previous work, blockchain technology is employed as a access management so as to automatise and track bound tasks, i.e. append a brand new record, modification in viewership rights, etc. moreover, sensible contracts on AN Ethereum blockchain [18] is employed to form intelligent illustration of EHR that are hold on in every individual node. later, the applying of pervasive social network (PSN) primarily based aid exploitation blockchain is projected by [30]. PSN permits North American nation to share medical knowledge nonheritable by medical sensors. PSN-based aid system contains 2 main security protocols, i.e. AN authentication protocol between medical sensors and mobile devices in wireless body space network (WBAN) and an EHR knowledge sharing exploitation blockchain in PSN space. every node within the PSN is liable for generating and broadcasting of medical knowledge transactions, i.e. node address and medical sensors. The miners, on the opposite hand, are liable for group action verification and new blockcreation. Lastly, a blockchain-based access management mechanism is projected by [31]. Access management includes identification, authentication, and authorization method. It ascertains a condition of being responsible wherever user access may be copied for what specific action in a very system. The projected system permits users to access EHR from a shared knowledge pools exploitation blockchain after validating their identity and cryptological keys. to attain user's authentication, an identity primarily based authentication is adopted. Additionally, an economical light-weight block format is projected to reinforce the present implementation of blockchain.

5.3 Business and Industry

The emergence of web of Things (IoT) has brought several blessings like delivering AN inter-connection between objects and humans. This motivates authors in [32] [33] to propose AN e-business design that is especially developed for IoT atmosphere. For this purpose, distributed autonomous corporation (DAC) is adopted as AN entity that offers dealings services within the absence of human intervention. The core of the projected system may be dealings mode during which peer to see dealings is performed autonomously, while Bitcoin and IoT coin area unit adopted because the currency and exchange certificate, severally. The authors [34] contemplate the importance of food safety and quality once proposing a agri-food offer chain traceability system victimisation RFID and blockchain technology. Blockchain is adopted for making certain the shared and revealed info is reliable and valid. Moreover, a term 'smart manufacturing' within the era of trade four.0 is additionally extensively mentioned in [35] [36]. Industry 4.0 denotes the pliability of product and services to be shared over the web or alternative networks, i.e. blockchain. With respect to the provision chain management, Industry 4.0 is predicted to realize the circumstance of decentralization and self-regulation. To date, AN extension of cloud computing that is alleged fog computing or edge computing, has been attracted authors to develop a good payment system supported Bitcoin [37]. Fog computing is considered a large-scale, ubiquitous, and suburbanized system that processes any computing tasks.

The projected system is established to boost the normal e-cash system that wants a trusty authority, i.e. bank to come up with payment token. By using the Bitcoin-based payment, the fog users (outsourcers) will directly create dealings to the fog nodes (workers) while not involving third party. The authors argue that the projected system will assure a payment for any completed tasks performed by honest employees no matter the outsourcers is malicious or not.

6. CONCLUSION AND FUTURE WORK

The progressive analysis papers that square measure connected with blockchain technology are reviewed and mentioned. The application of blockchain technology is not restricted solely to the finance business. it's an amazing future in several sectors like offer chain management, digital advertising, statement, cyber security, web of things, networking, etc.

The researchers believe that Blockchain has vast potential in each academe and business. The transaction process, application areas of blockchain also is explained. There are still many open issues that need to be further researched and analyzed to make more workable and effective industrial applications which will fully benefit from the utilization of blockchain and achieve the intended goals. Samples of these open issues include security, privacy, scalability, energy issues, and integration with other systems and, more specifically, with regulatory issues. Future work in this field is required to deal with these issues and shut the gaps for more efficient, scalable and secure blockchain industrial applications. This survey is predicted to function an efficient guideline for further understanding about the tradeoffs regarding different blockchain consensus mechanisms and application areas for exploring potential research directions that may cause exciting outcomes in related areas.

7. ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisors Prof. Manoj Kumar, Senior Assistant Professor of International Institute for Special of Education for providing valuable guidance, comments and suggestions throughout the colloquium.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cashsystem."Availableathttps://bitcoin.org/bitcoin.pdf, retrieved 06/15/2018, 2008.

[2] M. Iansiti and K. R. Lakhani, "The truth about blockchain," Harvard Business Review, vol. 95, no. 1, pp. 118–127, 2017.

[3] C.Mulligan,J.ZhuScott,S.Warren,andJ.Rangaswami, "Blockchain beyond the hype: A practical framework for business leaders." World Economic Forum, Cologny/Geneva, 2018.

[4] D. Tapscott and A. Tapscott, "How blockchain will change organizations," MIT Sloan Management Review, vol. 58, no. 2, pp. 10–13, 2017.

[5] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman. "BlockChain Technology : Beyond Bitcoin".

[6] D. Drescher, "Blockchain basics," Springer, Tech. Rep.

[7] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[8] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation, vol. 2, pp. 6–10, 2016.

[9] Aishath Muneeza, Nur Aishah Arshad, Asma' Tajul Arifin International Centre for Education in Islamic Finance (INCEIF) MalaysiaThe Application of Blockchain Technology in Crowdfunding: Towards Financial Inclusion via Technology 2018.

[10] Blockchain-Based E-Voting System Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson School of Computer Science Reykjavik University, Iceland {fridrik14, gunnlaugur15}@ru.is.

[11] Iuon-Chang Lin1,2 and Tzu-Chun Liao2 "A Survey of Blockchain Security Issues and Challenges"Jan. 12, 2017)

[12] GregorBlossey, BlockchainTechnologyinSupplyChain Management: AnApplicationPerspective 2019.

[13] S. King, "Primecoin: Cryptocurrency with prime number proof-ofwork," *July 7th*, 2013.

[14] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of- stake," *self-published paper, August*, vol. 19, 2012.

[15] C. Lee, "Litecoin," 2011

[16] ——, "Peercoin–secure & sustainable cryptocoin," *Aug-2012 [Online]. Available: https://peercoin. net/whitepaper*.

[17] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, 2014.

[18] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, 2014.

[19] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2014, pp. 475–490.

[20] P. Vasin, "Blackcoins proof-of-stake protocol v2," 2014.

[21]] D. Cawrey, "Auroracoin airdrop: Will iceland embrace a national digital currency," *CoinDesk, March*, vol. 24, 2014.

[22] E. Duffield and K. Hagan, "Darkcoin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proof of work system," *Mar-2014 [Online]. Available:https://www.dash.org/wpcontent/uploads/2014/09/DarkcoinWhitepaper.pdf*,2014 International Conference on Electrical Engineering and Computer Science (ICECOS) 2017

[23] H. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design," in *Workshop on the Economics of Information Security (WEIS)*. Citeseer, 2015.

[24] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. IEEE, 2016, pp. 1–3.

[25] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health IT and health care related research."

[26] B. A. Tama, "Learning to prevent inactive student of Indonesia open university." *Journal of Information Processing Systems*, vol. 11, no. 2, pp. 165–172, 2015.

[27] B. A. Tama and K.-H. Rhee, "Tree-based classifier ensembles for early detection method of diabetes: an exploratory study," *Artificial Intelligence Review*, 2017.

[28]] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[29] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on*. IEEE, 2016, pp. 25–30.

[30] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, 2016.

[31] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[32] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on*. IEEE, 2015, pp. 184–191.

[33] ——, "The IoT electric business model: Using blockchain technology for the internet of things," *Peer-to-Peer Networking and Applications*, pp. 1–12, 2016.

[34] F. Tian, "An agri-food supply chain traceability system for china based on RFID & blockchain technology," in *Service Systems and Service Management (ICSSSM), 2016 13th International Conference on*. IEEE, 2016, pp. 1–6.

[35] E. Hofmann and M. R¨usch, "Industry 4.0 and the current status as well as future prospects on logistics," *Computers in Industry*, vol. 89, pp. 23–34, 2017.

[36] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, 2017.

[37] H. Huang, X. Chen, Q. Wu, X. Huang, and J. Shen, "Bitcoin-based fair payments for outsourcing computations of fog devices," *Future Generation Computer Systems*, 2016.

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

[39] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in IEEE Symposium on Security and Privacy, pp. 104– 121, May 2015.

[40] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," CoRR, vol. abs/1402.1718, 2014.

[41] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," CoRR, vol. abs/1311.0243, 2013.

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

[43] 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.

[44] A. Gervais, G. O. Karame, K. Wu¨st, 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.

[45] Haque, A K M Bahalul & Rahman, Mahbubur. (2020). Blockchain Technology: Methodology, Application and Security Issues. 20. 21-30.

[46] https://www.blockchain-council.org/blockchain/types-of-blockchain-in-the-market-which-one-is-better/

[47] https://humphreys.law/blockchain-methodology/

[48] https://hellofuture.orange.com/en/blockchain-for-consent-management-improved-privacy-and-user-control/

