JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A LITERATURE SURVEY ON BLOCKCHAIN CYBER SECURITY DESIGN

[1]Hiral Rathod, [2]Sunil Kapadia, [3]Tejas Patel

[1]Assistant Professor, [2]Head of Blockchain Innovation at Inferenz, [3]Assistant Professor
[1]Department of Computer Science and Engineering,
[1]Government Engineering College, Patan, Gujarat,India

Abstract : The problem of block chain cyber security is discussed in this survey study. Block chain cyber security is essential in today's generation[08]. Many studies on block chain cyber security have been done in the past quarter. This research article discusses block chain cyber security improvement. Discussing blockchain technology cybersecurity. Block chain technology, derived from the Merkle Tree, would be a decentralised digital record that secures data transfers. Its decentralisation eliminates the need for these central authority to manage it. This article presents an overview of block chain technology. This study first clarifies the basics of Blockchain Technologies. This research study surveys algorithms presented in numerous block chains. Block chain, the backbone of Bitcoin, has lately gotten a lot of Block chain is really an irreversible data storage technique that may be used to store value in anything. Nevertheless, becoming a human concept, block chain technology has drawbacks such as sustainability, privacy, and non-technical customer. Furthermore, this study effort has discussed current technological advancements.

Index Terms **- Cyber Threat Intelligence (CTI), Distributed Ledger Technology (DLT), Directed Acyclic Graph (DAG), Cyber Security Information Exchange (CYBEX),etc.**

I. INTRODUCTION

In many approaches, block chain technology addresses the problems of security and privacy. To begin, new blocks are always kept in a linear as well as chronological order. That is, they are always appended to the block chain's "terminus." Whenever users examine at the Bitcoin blockchain network, you'll see that each block has a location upon on chain known as a "altitude." This block's height has achieved 656,197 units as of November 2020 [11].

It's also very hard to return and modify the content of a block until it has been put to the end of the block chain unless such majority of people agree to do so. This is due to the fact that each block includes its own hash, as well as the hash of the block before it and the previously stated time stamp. If that information is edited in any way, the hash code changes as well Here's why that's important to security.

Fig 1. Block chain technology accounts [30].

Let's say a hacker wants to alter the block chain and steal Bitcoin from everyone else. If they were to alter their own single copy, it would no longer align with everyone else's copy. When everyone else cross-references their copies against each other, they would see this one copy stand out and that hacker's version of the chain would be cast away as illegitimate.

It is almost hard to counter with such a hack, since the hacker would need to both possess and modify 51% of the block chain copies simultaneously in order for their new copy into becoming the majority copy, which means that the agreed-upon chain would

become the majority copy. Such an assault would also require a massive amount of money and resources, since they would have to rewrite all of the blocks due to the various time stamps but also hash codes.

We are on the verge of the so-called "4th industrial revolution" in this study effort. The fourth industrial revolution will combine numerous technologies, building on the third, which utilised electronics and computer technology to automate many production processes. Artificial intelligence, IoT, and blockchain technology are just a few of the technologies that have the potential to radically transform the world as we know it from this study.

1.1 BASIC IMPLEMENTATION

Block chain claims to be a distributed ledger, with each network node acting as a separate node in a peer-to-peer network, where there is no central authority supervising the process. Block chain is, as the name implies, an ordered chain of blocks where each block contains batches of transactions. A block is made up of a header and a body containing transactions, and therefore, a block is essentially a structure comprising a header and body. Timestamped and signed blocks serve as proof of their origin. Every block in the chain carries a cryptographic hash of the previous block in the chain. This enables one block to reference the preceding block in the chain, and a reference is always built into the head of each block (while ensuring the immutability of that previous block). the genesis block is the very first block from which a block chain is constructed (Figure 1.2) [03].

Fig 2. Block chain as a chain of blocks[05].

It should be noted again that a block chain is a type of Distributed Ledger Technology (DLT) with a series of specific features. By DLT, In this research work mean any type of technology that makes use of a distributed ledger and, therefore, not all DLTs are blockchains. As an example, new generation technologies, such as IOTA[18], or Hashgraph[], are based on DLT different from the blockchain, being named blockless technologies, which are out of the scope of this document[16].

1.2 BLOCK CHAIN AS A SECURE LEDGER

Once block chain technology has been used, the following considerations take precedence:

Block chain ledger is immutable since it is based on unalterable data. Every transaction in a block is cryptographically signed by its sender, every block in the block chain is cryptographically signed by its miner, and every block includes a hash of the immediately previous block. Changing a single transaction in the block chain will require altering all future blocks in the chain, resolving the consensus problem, and achieving 51% of network support. Because of the hashing characteristics and the processing and electrical resources needed, achieving this objective is very near to impossible. The block chain is tamper-resistant, and the greatest virtue of the block chain is its integrity.

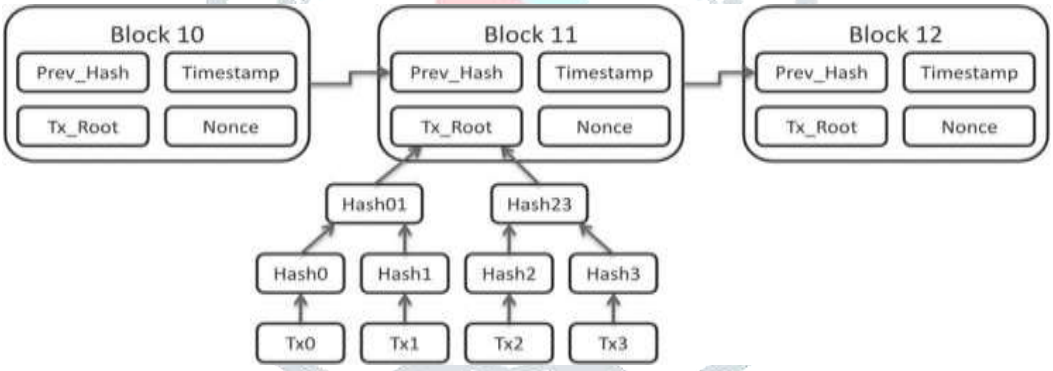

Fig 3 Merkle Trees[07]

While hash chains aren't directly addressed in the text, Merkle trees are an important use of hashing in block chain technologies that were not previously discussed. A Merkle tree creates a single, unique fingerprint for all transactions in a block, enabling verification that the transactions in the block have not been modified. Below In this study, one of these Merkle trees may be found (Figure 3).

Here this research work can see above that each leaf in the Merkle tree is a hash of transactional data, and each sub-hash from this data is hashed. This procedure is then repeated recursively on these smaller hashes to create the Merkle tree. Block transactions, as well as the state of the ledger after the execution of all ledger transactions, use Merkle trees.In terms of availability, the distributed character of blockchain network makes it highly available. In addition, transactions on public blockchain networks usually involve a cost to the sender equivalent to their processing and storage consumption. This cost results in a reward for the miner of the block containing the transaction. Furthermore, it protects against Denial of Service (DoS) attacks, since an attack involves a cost proportional to the resources consumed for a potential attacker. For example, in Ethereum MainNet, this cost is reflected in the concept of gas. Gas represents the computational and storage cost of the transaction[09].

1.3. BLOCKCHAIN FOR BACKUP AND RECOVERY

One of the most innovative applications of blockchain technologies is to use it by secure storage and recovery systems. A Backup & recovery system usually has the following features:

Continuous/Automatic data backup: It ensures that the changes you make to your files are simultaneously copied to the storage location. This lets you recover even the most recent changes in case of data loss, thus lowering your recovery point objective.

- **Incremental backup:** This is a type of backup where only the changes are copied, not the full file. This reduces the time taken for copying data and does not slow down your work.
- **Instant recovery:** This feature allows a backup snapshot to run temporarily on secondary storage to reduce the downtime of an application.
- **Data deduplication:** It eliminates duplicate data record blocks while data is transferred to the backup storage location. This reduces the network load and the storage space you require.

- Error-free copy: Data backup software features also ensure that the data copied from a source and stored at the backup server are the same and do not mismatch nor contain errors.

Historically, backup and recovery procedures were applied mainly to general-purpose devices in the enterprise environment. The number of incidents grows daily, and the consequences are increasingly alarming as, for example, security holes in IP cameras, DDOS attacks generated from the Mirai botnet known as Dyn Attack or event take control of a vehicle. Due to these problems, Backup & Recovery systems are being extended to cover these devices too[20,24].

1.3.1 GENERAL-PURPOSE DEVICES

From the point of view of general-purpose systems, the main challenge that blockchain is expected to solve is the control data from tampering attacks; directly related to the integrity of the data.

In this research work could find proprietary solutions that offer blockchain backup services at an enterprise level, see. This solution provides mechanisms to ensure that legal documents existed on certain dates or to certificate authenticity of medical records[12].

1.3.2 IOT DEVICES

Most existing solutions for firmware upgrades depend on the client-server model in which the manufacturer delegates the firmware distribution process to the suppliers of its products. The central client-server architecture has the drawback to be a Single Point of Failure (SPoF), and in case the server is not available IoT devices cannot access resources (updates). There are two approaches: manual and automatic[27].

1.4 DISTRIBUTED FILE SYSTEM (DFS)

In this research work find use cases such as the previous ones that require a distributed storage it is necessary to resolve where to store the files and who can access them. Block chain technology does not offer storage solutions and it is not a recommended practice to store files in the block chain. A possible solution is the use of distributed storage systems, like the decentralized P2P file storage systems. When using this kind of storage, files are divided into pieces that are replicated in different peers. A peer requiring access to an archive collects pieces of this archive, which is partially located in several peers at a time. The performance is similar to that of the P2P BitTorrent network and files are indexed by their hash or fingerprint.

1.5 INTRODUCING THE CONTENT DELIVERY NETWORKS

The distributed nature of blockchain allows these services to be decentralized. The characteristics obtained are common to both approaches, of which the most important and their counterpart are listed below.

- The load on each individual server is lowered, but the number of servers of the system is increased.
- The network traffic is distributed, but the information needs to be synchronized.
- The latency is diminished, and the bandwidth increased, in exchange for a higher maintenance cost.

In short, the use of CDNs adds some advantages, but it also increases the complexity of the architecture. There are several aspects that are affected by the need for offering copy mirrors and closer access to the client. The original server must have substitutes to ensure the high availability of the service. On the other hand, it is necessary to ensure the consistency of the data served. As there are a number of geographically distributed machines, which theoretically have the same information at all times, synchronization problems may arise.

Additionally, there must be a constant internal routing service to find all nodes in the network, to synchronize information internally and to provide better customer service externally. Furthermore, all these mechanisms are based on a record of user accesses and server use that improves the quality of service but generates an additional cost in computing and storage[12].

II. LITERATURE SURVEY

Giannoutakis (2020, November) Recent increases in Internet of Things (IoT) devices have resulted in smart ecosystems, such as smart houses, being vulnerable to hackers. For traditional security approaches, also acknowledge the necessity of protecting private data and personal security while these applications are being deployed, but their centralised nature, along with the limited computational capabilities of smart home gateways, mean that these approaches are not highly efficient. The last accomplishments made with regard to block chain technology provided platforms where such decentralised architectures may be put to use for cyber security protection measures. In this project, a block chain framework is made available to the smart home industries in order to assist with the cyber security systems that regulate such installations. The two concentrate on user and device immutability. It offers secure, dynamic, and immutable gateway and IoT device management and banned harmful IP administration through the suggested approach. A genuine smart home setting has implemented the framework, and these results show that it is applicable and efficient [1].

Neisse, R., et al (2020) The development of appropriate technical methods for a trustworthy and interoperable exchange of cybersecurity information is required in order to implement an EU cybersecurity certification system. To help meet the current EU cybersecurity legislation's requirements, this study proposed a blockchain-based platform for inter-chain interoperability. In this way, several blockchain implementations may be done on a national level, while problems pertaining to scalability and performance originate from using a single ledger. Authors idea seeks to build an EU-based system to help improve cyber-security awareness while allowing firms in multiple Member States to have a trust-based level of assurance about the rules governing data sharing encoded into the smart contracts and inside the data itself. This is the first time that authors proposal is aiming to effectively manage the cyber security information sharing across the stakeholders. While the deployment of such a platform represents authors ongoing work in this area, the further development of authors proposed platform is necessary in order to examine both technical and governance aspects of possible EU-level deployment [2].

S. Badsha, et al (2020, January) By using cybersecurity information sharing, everyone may benefit from new and undiscovered dangers. One of the key platforms that has played an essential role in the implementation of a proactive cyber defence system is the Cybersecurity Information Exchange (CYBEX). They're centralised, therefore they could completely fail if something happens to

them. Additionally, despite sharing private information, it lacks the method of giving the right to question organisations such as corporations, governments, and other entities the ability to regulate who has access to the shared sensitive information. In other words, non-repudiation of the system does not exist. This means that if someone tries to deny what they have shared, then there will be no method to monitor or confirm their claims, thus the record must be kept to counter false denials. In this research work using block chain-based privacy preserving cyber security information sharing, where the organization is able to assign finer-grain access control using delegating which organization can have access to its cyber security information while also using proxy re-encryption and attribute-based encryption (BloCyNfo-Share). The results of this study effort indicate that the model is private and efficient[3].

Riesco et al. study (2020) Although a potentially helpful method for enhancing overall security, cyber threat intelligence sharing may be difficult to do, since many participants are hesitant to give their information and prefer to consume only voluntary-based solutions. Doing this undermines the goal of sharing knowledge. Similarly, governments mandate reporting events that have the potential to have a significant effect on people and the society as a whole. Otherwise, operators may face penalties for failing to report them on time. Both obligations and penalties often discourage people from sharing information freely. What is required will simply be repeated and reported, and what is not needed will be ignored. In this study, a paradigm shift is proposed that encourages everyone engaged, from the top to the bottom, to communicate important information quickly. It will help to increase the use of Dynamic Risk Management frameworks while also supporting the existence and implementation of such frameworks. diverse participants will have varied motivations to share, invest, and consume threat and risk information, based on their various responsibilities (producers, consumers, investors, donors and owner). authors approach draws on common standards like Structured Threat Information Exchange (STIX) and W3C Semantic Web standards to help organization identify strategies, methods, and processes associated with behavioural threat intelligence patterns. In addition, Proposing an Ethereum Block chain Smart contract Marketplace and establishing a standard CTI token as a digital asset with a potential value in the market are part of this study. Simulations and an experimental were conducted to illustrate the advantages and incentives of the system, but also to help the design team have a better understanding of its possible limitations such as storage and transaction costs[4].

Professor Strang, et al (2020) in this study, in this effort, academic ideology for teaching block chain was examined The researchers that conducted this study investigated several strategies that professors use to teach information technology courses, including block chain and IoT, in order to summarize the literature review. After going through authors colleagues' experiences, we expanded on how professors and instructors at the university level are teaching and developing block chain for business and computer science fields. In this chapter, researchers sought to discover whether higher education requires strong cyber security. Authors tackled the issues of why it is critical for institutions of higher education to implement cyber security, and spoke about the philosophies the schools are using in management science and computer science teaching. This research discovered that contemporary cyber security higher education is heavily dependent on block chain technology. A conceptual typology was also suggested in this study for helping to synthesis university researchers' knowledge on teaching block chain, both of which were found in the examined literature and authors own experience. Using authors conceptual approach, leaders and administrators may develop and offer cyber security and risk management degrees at various levels. In this study, risk management at universities in developing countries was conceptually synthesised into a typology. in this study, in this effort, academic ideology for teaching blockchain was examined The underlying block chain technology has risen into popularity since Bitcoin's creation in 2008. Based on the literature and authors experiences, authors created a conceptual typology that synthesises the justification for teaching blockchain at universities. This model may be used by anybody who is in a position to shape university programmes, as well as those who are interested in deciding on which courses to take while obtaining a degree. This chapter will add to the comprehension of the existing risk management approaches used by businesses when dealing with blockchain technology. While this chapter will be helpful to instructors and students alike, it will also provide in-depth knowledge on how to mitigate the cybersecurity risks posed by the blockchain technology[5].

Abdulkader (2019, June) This article presents lightweight BC cybersecurity for IoT settings. Because the size of the BCH and its incorporation of both public and local transactions as well as a separate local BCH for transactions depending on the IoT device requester differentiate it from other currencies, LBC is distinct among competing currencies. According to authors understanding, this is the first work to establish the distinct BC system by dividing transactions depending on who is making the request. The idea of LBC may be used to adopted for different purposes. terminology including Proof of Work (PoW), Proof of Stake (PoS), mining, minor, and its algorithms is essential to significantly slow down the formation time of the Bitcoin Core (BC)[7].

III.TYPES OF BLOCKCHAINS

Block chain technologies can be divided into three broad categories. These distinctions are important for understanding the role of people in the system and how the system operates in the context in which it is applied.

A. PUBLIC BLOCK CHAINS

Public block chains [15],emphasize transparency and participation. The consensus of transactions is “decentralized,” in that anyone can participate in validating transactions on the network, and the software code is publicly available or “open-source.” Examples include Bitcoin and Ethereum.

The key attribute of public block chain networks is that they pursue decentralization through cryptoeconomics, to ensure cooperation in a distributed network. In this case, decentralization refers to the characteristic of having no political center of control and no architectural central point-of-failure in the design of the software system (Buterin, 2017). The degree to which a block chain is decentralized depends on design of the consensus algorithm, issuance of cryptoeconomic incentives, ownership of cryptographic “private keys,” and governance of the network. Governance considerations include who can develop the software code, who can participate in the consensus mechanism, and who can take part in communal governance activities to maintain the network[26].

B. Private Block chains

Private block [17],chains mean that membership to participate in validating transactions on the network is restricted to only include parties that are approved by a central administrator. Thus, private block chains are centralized and operate more closely to a traditional database, than a complex, macrosocial coordination system. Transaction data is most often kept private. Private block chains often employ a "Proof-of-Authority" (PoA) consensus approach (Peng et al., 2020). Private block chains are often adopted in internal, business secure environments, such as access, authentication, and record keeping[22].

Fig 4. Private Block chains[22]

C. Consortium Block chains

Consortium block chains are comprised of known participants that are preapproved by a central authority to participate in consensus in a block chain network. This "semi-permissioned" approach allows for a network to be distributed, or partly decentralized, while allowing for a degree of control over a network. Transaction data may be kept private. Consortium block chains can reach consensus via PoW, PoS, PoA, or others, such as delegated proof-of-stake, and more.

Fig 5. Consortium Block chains

D. Hybrid block chain

How it works. Sometimes, organizations will want the best of both worlds, and they'll use hybrid block chain, a type of block chain technology that combines elements of both private and public block chain. It lets organizations set up a private, permission-based system alongside a public permissionless system, allowing them to control who can access specific data stored in the block chain, and what data will be opened up publicly.

Fig 6. Hybrid block chain

Typically, transactions and records in a hybrid block chain are not made public but can be verified when needed, such as by allowing access through a smart contract. Confidential information is kept inside the network but is still verifiable. Even though a private entity may own the hybrid block chain, it cannot alter transactions.

E. Consortium block chain

The fourth type of block chain, consortium block chain, also known as a federated block chain, is similar to a hybrid block chain in that it has private and public block chain features. But it's different in that multiple organizational members collaborate on a decentralized network. Essentially, a consortium block chain is a private block chain with limited access to a particular group, eliminating the risks that come with just one entity controlling the network on a private block chain[13].

Fig 7. Consortium block chain

In a consortium block chain, the consensus procedures are controlled by preset nodes. It has a validator node that initiates, receives and validates transactions. Member nodes can receive or initiate transactions.

IV. CHARACTERISTICS OF BLOCK CHAIN

In summary, block chain has following key characteristics:

DECENTRALIZATION. In standard centralized group action systems, every group action must be valid through the central trustworthy agency (e.g., the central bank), inevitably ensuing to the value and therefore the performance bottlenecks at the central servers. Distinction to the centralized mode, third party is not any longer required in block chain. Accord algorithms in block chain are accustomed maintain information consistency in distributed network.

PERSISTENCY. Transactions are often valid quickly and invalid transactions wouldn't be admitted by honest miners. It's nearly not possible to delete or rollback transactions once they're enclosed within the block chain. Blocks that contain invalid transactions may well be discovered directly.

ANONYMITY. Every user will act with the block chain with a generated address, that doesn't reveal the $64000 identity of the user. Note that block chain cannot guarantee the proper privacy preservation thanks to the intrinsic constraint .

AUDITABILITY. Bitcoin block chain stores knowledge regarding user balances supported the unexpended dealings Output (UTXO) model: Any dealings must ask some previous unexpended transactions. Once this dealing is recorded into the block chain, the state of these referred unexpended transactions switch from unexpended to spent. Therefore, transactions may well be simply verified and tracked[28],[29]

1. Block chain for health care industry

In today's life patient doesnt like to reveal there treatment details to outsider. In this case patient can use this technology to keep secure all information from others. This block chain can be used as a website, or mobile app. Each and every user in a block chain has two keys. Public key and private key. By using this only who can make a transaction. For example there two person Alice and Bob. Alice want to send some secure data to bob. So that Alice sign a digital signature by using here private key. That means private key is always act like as a password. Then shew will hash the data by using here public key and generate an address. Then bob validate the digital signature. If it is validated they will make a transaction. So by using these type of security methods, potions information can be protected from others[10].

2. Electronic medical records.

Patients can handle electronic medical records by using the block chain technology. Most of the health cares institution should not allow patient to access their medical data. Patients are becoming disappointed about the privacy of their medical records. This all can be avoided by block chain. In handling electronic medical records, block chain should deal with different frame work for managing the authentication, confidentiality, and accountability. It is mainly used when handling the sensitive data. Online electronic records in block chain will operated as decentralized application. In centralized environment all application should be done at one location. But in decentralized environment application should be done in different location. Electronic medical records should affect some challenges and limitations. This system will face some important challenges during the implementation of personally controlled system. That is this personally controlled records would replace provider or hospital records. Some segment of the personally controlled records would be downloaded in to the institutional record to tribute the existing data[25],[26].

3. Blockchain to protect personal data

Today there is recent increase in reported incident of security problem in users personal data. Because of this there is a third party control over the data, who will collect all personal information. Block chain can eliminate this third party and can transfer directly between two parties. The amount of data recently increasing in our world. Facebook, is the largest online social network, collected 300 petabytes of personal data. Personal data or sensitive data should not be secure in the hand of third parties. They are tried to attack and misuse. Block chain helps users that not required to trust any third party. Block chain recognizes the users as the owners of their personal data. Block chain should have its own rules and regulation. It is known as smart contract. Before starting a transaction the gateway keeper should create some rules and will written as a contract. It will make a peer to peer communication. Bitcoin has demonstrated in financial space that is trusted and computing is possible in decentralized network. Block chain is mainly proposed to handle the bitcoin, it is a digital currency.

Fig 8. Block chain to protect personal data

4. Bitcoin

Bitcoin is a digital currency, created and held electronically. It is operated as a decentralized application. That directly control the transfer of digital currency. Value of bitcoin increasing in recent year. Bitcoin sets out to solve the distributed tracking and validation of transactions is one ot its main problem. It will keep the full history of transaction. Block chain is mainly developed to transact this digital currency. If the user wants the recent history, then who can filtering it. Before making a transaction the rules and regulations of this will be written as a contract form known as smart contract. Transaction is only possible between two persons, before making it sender side should enter a digital sign. The transaction is validated by this digital sign. If this sign is validated transaction is proceed, that means botco in should transacted[12],[23].

v. CONCLUSION

In reseach work discuss about the domain improvement of block chain cyber defense throughout this survey study. The results explained in chapter on comparative analysis are of critical importance. While conducting this research, users will notice that architecture block chain information security has the main issue when it comes to the overall improvement of block chain information technology. Furthermore, because of prevalence of software reliability problems in the design block chain, almost all of the cyber security for the block chain is distributed there. An area enhancement of block chain cyber security is needed in the future. Improving all of these issues will have a big effect on healthcare. Focus on developing an area optimization of the block chain's cyber security in the future. Block chain is a disruptive technology that has revolutionized the Internet for everyone. Block chain has showed promise for being the best option when individuals are handling value-sensitive goods in the digital age. This article provides a basic introduction to block chain technology for those new to the subject. They've additionally discussed its applicability and the problems it confronts in that study. The main goal of this article is to offer a ready-made solution for understanding the functioning of block chain technologies.

REFERENCES

1. Giannoutakis, Konstantinos M., et al. "A blockchain solution for enhancing cybersecurity defence of IoT." 2020 IEEE International Conference on Blockchain (Blockchain). IEEE, 2020.
2. Neisse, Ricardo, et al. "An interledger blockchain platform for cross-border management of cybersecurity information." IEEE Internet Computing 24.3 (2020): 19-29.
3. Badsha, Shahriar, Iman Vakilinia, and Shamik Sengupta. "Blocynfo-share: Blockchain based cybersecurity information sharing with fine grained access control." 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2020.
4. Riesco, Raúl, Xavier Larriva-Novo, and Víctor A. Villagrá. "Cybersecurity threat intelligence knowledge exchange based on blockchain." Telecommunication Systems 73.2 (2020): 259-288.
5. Strang, Kenneth David, Ferdinand Che, and Narasimha Rao Vajjhala. "Ideologies and Issues for Teaching Blockchain Cybersecurity in Management and Computer Science." Innovations in Cybersecurity Education. Springer, Cham, 2020. 109-126.

6. Neisse, Ricardo, et al. "Toward a blockchain-based platform to manage cybersecurity certification of IoT devices." 2019 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2019.
7. Abdulkader, Omar, et al. "A lightweight blockchain based cybersecurity for IoT environments." 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom). IEEE, 2019.
8. Serrano, Will. "The blockchain random neural network in cybersecurity and the Internet of Things." IFIP International Conference on Artificial Intelligence Applications and Innovations. Springer, Cham, 2019.
9. Ejaz, Waleed, and Alagan Anpalagan. "Blockchain technology for security and privacy in Internet of Things." Internet of Things for Smart Cities. Springer, Cham, 2019. 47-55.
10. McGhin, Thomas, et al. "Blockchain in healthcare applications: Research challenges and opportunities." Journal of Network and Computer Applications 135 (2019): 62-75.
11. Kotilevets, I. D., et al. "Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions." IFAC-PapersOnLine 51.30 (2018): 693-696.
12. Mora, Olga B., et al. "A Use Case in Cybersecurity based in Blockchain to deal with the security and privacy of citizens and Smart Cities Cyberinfrastructures." 2018 IEEE International Smart Cities Conference (ISC2). IEEE, 2018.
13. Xu, Quanqing, et al. "Blockchain-based decentralized content trust for docker images." Multimedia Tools and Applications 77.14 (2018): 18223-18248.
14. Maurya, Sweta, Shilpi Sharma, and Pranay Yadav. "Internet of Things based Air Pollution Penetrating System using GSM and GPRS." 2018 International Conference on Advanced Computation and Telecommunication (ICACAT). IEEE, 2018.
15. Alexopoulos, Nikolaos, et al. "Towards blockchain-based collaborative intrusion detection systems." International Conference on Critical Information Infrastructures Security. Springer, Cham, 2017.
16. Aste, Tomaso, Paolo Tasca, and Tiziana Di Matteo. "Blockchain technologies: The foreseeable impact on society and industry." computer 50.9 (2017): 18-28.
17. Dinh, Tien Tuan Anh, et al. "Blockbench: A framework for analyzing private blockchains." Proceedings of the 2017 ACM International Conference on Management of Data. 2017.
18. Li, Cheng, and Liang-Jie Zhang. "A blockchain based new secure multi-layer network model for internet of things." 2017 IEEE International congress on Internet of Things (ICIOT). IEEE, 2017.
19. Moinet, Axel, Benoît Darties, and Jean-Luc Baril. "Blockchain based trust & authentication for decentralized sensor networks." arXiv preprint arXiv:1706.01730 (2017).
20. Singh, Sachchidanand, and Nirmala Singh. "Blockchain: Future of financial and cyber security." 2016 2nd international conference on contemporary computing and informatics (IC3I). IEEE, 2016.
21. Kosba, Ahmed, et al. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." 2016 IEEE symposium on security and privacy (SP). IEEE, 2016.
22. Noyes, Charles. "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning." arXiv preprint arXiv:1601.01405 (2016).
23. Tschorsch, Florian, and Björn Scheuermann. "Bitcoin and beyond: A technical survey on decentralized digital currencies." IEEE Communications Surveys & Tutorials 18.3 (2016): 2084-2123.
24. Sharples, Mike, and John Domingue. "The blockchain and kudos: A distributed system for educational record, reputation and reward." European conference on technology enhanced learning. Springer, Cham, 2016.
25. Peters, Gareth, Efstathios Panayi, and Ariane Chapelle. "Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective." Journal of Financial Perspectives 3.3 (2015).
26. Foroglou, George, and Anna-Lali Tsilidou. "Further applications of the blockchain." 12th student conference on managerial science and technology. 2015.
27. Zhang, Yu, and Jiangtao Wen. "An IoT electric business model based on the protocol of bitcoin." 2015 18th international conference on intelligence in next generation networks. IEEE, 2015.
28. Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." International workshop on open problems in network security. Springer, Cham, 2015.
29. Vasin, Pavel. "Blackcoin's proof-of-stake protocol v2." URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf 71 (2014).
30. Eyal, Ittay, and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable." International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2014.