Security And Privacy Issues Of Block-Chain Technology

Amal Hassan M.Alsuhaimi , Sabah M.Alzahrani

Abstract: Block-chain is getting popular and it is one of the most common topics that can be considered. it has also changed the lifestyles of many people in certain fields, because of the impact on businesses and combines. Blockchain ensures more reliable and appropriate resources and it is very crucial to keep in mind that the security and privacy have some obstacles as any technology in this fields. The spectrum of blockchain applications is very extended into different areas in banking, health, automotive, the Internet of Things (IoT) etc. Many studies concentrate on using the block-chain data model in different implementations. In this paper we try to describe block-chain technology by discussing its model of a data protection and privacy perspective with different consensus algorithms, as well as issues and opportunities in block-chains.

Keywords : Block-chain, Security, Privacy, Group signature, Zero-knowledge.

1 INTRODUCTION

The internet has recently witnessed the unveiling of numerous important bottom-up implementations that solve issues in a supportive and transmitted process that have become ubiquitous and well-known by any of these public and non-profit programmers, The bitcoin cryptocurrency and the origins of blockchain technologies behind it are conne cted toone topic that is growing with surprising frequency. bitcoin technology is continually changing. it is vulnerable by some illness humans and contradictory requirements for its implementation. while the amount of bitcoin excitement for cryptocurrency in Europe block-chain is declining as the technology advancement below the reverse is true there is a rising interest in technology block-chain in different industries banking and government organizations.[2] some thesis gives a comprehensive literature analysis of block-chain-based on the goal of applications across various realms is to analyses the existing state and implementations of block-chain technology and to show how unique features of block-chain technology. In this analysis, we introduce a comprehensive Category of block-chain we also refer to the limitations contained in the applicable liter ary works. Especially the restrictions that block-chain technology introduce and how these restrictions spawning through various markets and sectors on the basis across different sectors such as the healthcare, IoT, privacy and data protection supply chain industry[3]

1. Locating Studies

A comprehensive literature review was conducted during January 2018 without timeline constraints to answer our primary research issue and the findings were Afterwards, revised Throughout April 2018 Scopus was used as the primary science source that searched for the word block-chain in the names of all posts there were also additional searches using the cited works of the related papers snowball effect electronic searches have also established related grey research, comprising unauthorized research conducted b y public administration bodies or private entities. we assessed the first 200 hits from google in order to classify the reported grey literature during the quest alternative words for block-chain and application were used more grey research especially Agency findings or strategy briefs from the agencies representing both private and publics ector entities resulted in the hand-search reference list in some reports. In Fig 1,
a flowchart of the applied approach is shown. Furthermore, Multiple refining features of scopus have been commonly used Multiple refactorings of the findings in the sense of particular papers scan of relevant documents etc. the full paper was collected and analyzed for importance when the abstract of a given analysis was not-available in full text all potentially applicable articles have been retrieved [4].

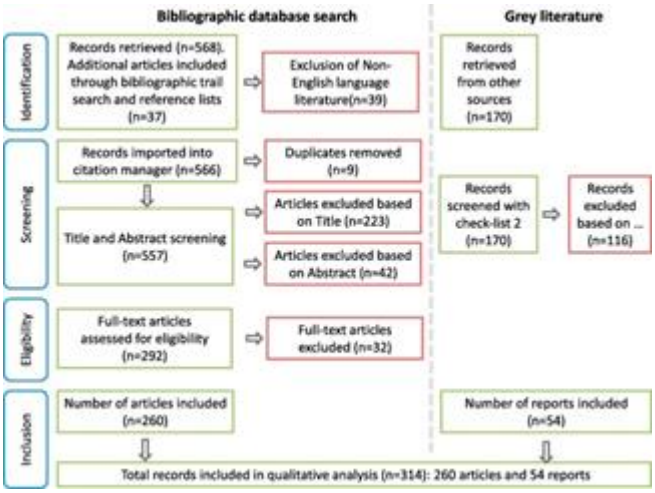

***Fig.* 1**. *Flowchart of the search strategy.*

1.1. Study selection and evaluation

The authors evaluated independently, on the basis of a collection of predefined exclusion and inclusion criteria, the eligibility of the retrieved literature, such exclusion requirements language subject area and text type restrictions were used prior to the bibliographic managers presentation of the literature the abstracts of both academic articles and introductory portions of grey literature were analyzed initially reports satisfying one of the conditions for exclusion. Excluded and ordered by Full-text explanation for omission analysis was also subsequently carried out and several supplementary publications detailing the reasons for omission were omitted from the report any ambiguity with regard to the relevance of the papers. they were focused on the technological aspects of the design of block-chain technologies and or block-chain [5].

1.2. Analysis and synthesis

A qualitative analysis software (MAXQDA11) has been implemented into both publications and studies meeting the inclusion criteria, and data on emerging topics has been analysed. The authors separately conducted the thematic material analysis. The three coded section groups (the The consensus level was around 75 percent)Then all papers were compared, decided on and presented in a single collection of subjects [6]. Understanding for basics of Block-chain Developmentit has more of crucial components: You should be familiar with the following terms:

- **Block-chain**

The block-chain is an incorruptible block-chain where each block contains value data that is validated not by any central authority, but by all nodes throughout the network. every block includes its hash value in the chain and the one of the previous block, which serves as a unique fingerprint so that no data stored in it can be manipulated. It is never possible to erase or change the information stored on the block-chain[7].

- **Decentralized**

a block-chain is decentralised, because it is not held in one location and does not have a core. Instead, the data contained in the block-chain is distributed, or nodes, over several different computers. Because no one individual has control over the data, users communicate directly with each other without a third party 's involvement.[8]

- **Decentralized Consensus**

A block-chain is a peer-to - peer decentralised system that has no central authority to govern the sharing of information. While no central administrator 's presence keeps the system devoid of corruption, the following questions arise[9]:
1. In the block-chain, how is a decision made?

2. Why is a transaction applied to the block chain?

A central authority or a board of decision-makers takes all the necessary decisions in a normal centralised model. But in the case of the block-chain, it is not feasible since it has no chief.
"In order to make decisions, the members of a block-chain network need to come to consensus through" consensus mechanisms. We will explore in depth some of the relevant consensus algorithms.

- **Smart-Contracts**

The building blocks for block-chain based applications are smart contracts. Contractual regulation of transactions between two or more participants is the principle behind smart agreements. Instead of a central authority, it can be programmatically checked using the block-chain. Smart agreements also allow users to retain ownership by providing regulated disclosure of data.[10]

- **Mining**

The process of adding transactions to the distributed ledger is known as mining. This primarily involves making a hash of a block that cannot be forged. As a consequence, without having a central structure, it preserves the dignity of the whole system. The users who use the computing resources to mine for blocks are miners. It's not enough to learn the fundamentals of decentralised technology, before moving to block-chain growth, there's a lot to understand. Let 's discuss some of the concepts for any block-chain enthusiast that are popular but relevant.[5]

- **Node**

What is a node in a network of block-chains?
Let 's start by describing what a node in a block-chain is. In general, a node is any participant in the network of a coin. There are various styles, but each of them shares one particular characteristic-in order to host or simply link to one, you will need special hardware. Block-chain technology, one of the main features that made it so appealing to the general public, is decentralised by nature. It is based on the concepts of a network called P2P (Peer to Peer). There are no dedicated servers on most networks, not a single authority, but a consensus among users. Becoming a member of a certain crypto coin community is not only exciting but also a responsibility, since they are all vital to the protection and credibility of the network. For instance, take Bitcoin. You have two types of nodes. Full nodes that store a block-chain copy and thus guarantee by validating data the protection and correctness of the data on the block-chain.[11] The second form is a lightweight node, with each participating user connecting to a full node in order to synchronise with the network's current state and be able to participate. There are two major types of nodes in a nutshell: complete nodes and light nodes. Clients that supply wallet functions are another word for representing nodes. Full ones include a national copy of the background of the block-chain, including all blocks produced. All wallets that download only the headers of blocks and save hard drive space for users are light nodes or SPV (Simple Payment Verification) nodes. Let us discuss in depth the various sub-kinds.[12]

2. Types Of Block-Chain Nodes

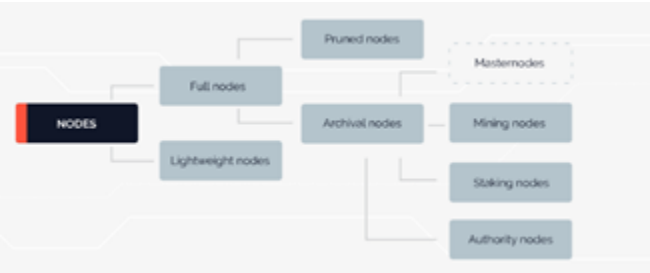

Fig.2 *Types of Block-chain Nodes*

2.1 Full Nodes

In a decentralised network, Complete Nodes function as a server. Their key tasks include the preservation of consensus and transaction verification between other nodes. They also store a block-chain copy, thus being more stable and allowing custom features such as instant sending and private transactions to be allowed. Full nodes are the ones that vote on proposals when making choices about the future of a network. It gets skipped if more than 51 percent of them do not agree with the idea. This can lead to a hard fork in certain situations in which the group cannot agree on a certain

change and instead go their separate ways, producing two chains.[13]

2.2 Pruned Full Node

One type is the complete node that is pruned. The particular feature here is that it starts downloading blocks from the beginning and deletes the oldest ones once it hits the set limit, keeping only their headers and location in the chain. if you set a size limit of 550 MB, you'll store all the latest blocks that can fit into that hard drive space, but you'd first have to go through the entire block-chain to verify all the previous blocks in order to get to that state. Pruned nodes are considered to be complete nodes and can thus validate transactions and engage in consensus as well.[14]

3.2 Archival Full Node

When talking about full nodes, archival complete nodes are what most individuals refer to. They imagine a server that in its database hosts the entire block-chain. Their primary role is to build consensus and verify blocks, as I already discussed with you above. One of the discrepancies between pruned and archival nodes is the amount of hard drive space on your server or PC that they take up. It is possible to split archival nodes into a few subtypes: those that can add blocks to the block-chain and those that cannot.[15]

3. Block-chain applications

Embodied by the Bitcoin network, the large-scale digital currency system functions independently over the entire duration, thereby enabling internationally reliable real-time transactions that can be integrated into the conventional financial system. This is triggered by endless imagination for future block-chain implementations.We assume that there are four punch applications in the block-chain[16]:

3.1 Darknet and black-market payments

This application had an issue. If they don't trust each other and don't want anyone to find out who they are, how are pseudonymous buyers and darknet sellers at opposite ends of the globe going to make transfers?Bitcoin arrived as he approached. It is international, needs no confidence, is pseudonymous and is invulnerable to state intervention (for the most part). Darknet such as The Silk Road, Alpha Bay and their predecessors launched Bitcoin as the unofficial currency. In reality, Bitcoin is used mostly for innocuous motives , but the darknet gives a great deal to it.
A degree of promotion of all cryptocurrencies is require, which doesn't provide them with much protection. Darknet introduced Bitcoin
to the first wave of customers and miners and the world breath ed life.Bitcoin was the first currency in this position [17, 18].

3.2 Digital gold

gold as a metal is not quite beneficial . Less than ten percent of all gold mined It is used for some production or industrial uses. In spite of this, people have acknowledged that gold is highly useful, And why then? If we chuck out the basic causes for why gold attracts individuals, it has some decent financial characteristics. It is hard to have gold, and new reserves are not often found. Thus, supply demand is comparatively poor. Glod still does not diminish or scratch, so, produced gold will therefore continue for sale. It contributes to the decreased market uncertainty as a safe way of investing, which makes it appealing. Moreover, every market or government entity does not have a gold monopoly, Therefore, its highs and lows are not dependent on any one place. People converged on gold as Schelling's point for these and other reasons, for a dynamic form to conserve. Gold serves as protection against global financial disruptions, being such a constant method of investing. Amid markets' highs and lows. gold conduct is independent. Therefore, over the last few years, gold has represented us as a part of the world of savings spread internationally. It is useful because we both agree to use it in many ways .[19]

3.3 (macro and micro) the Payments.

Since their users need ideal key management for cryptocurrencies, block chains do not solve the peer-to-peer payment issues. maybe everyday Darknet clients will take the time to understand the subtleties of technology and take the chance. But more than theoretical protection is required for blockchains to function in a mass market, actual functional security is required. Money should be convenient to use such that something is not misinterpreted and risked by the ordinary citizen in the street. Many people are far below this degree of professional competency now. Cryptocurrencies would not be ideal for a market peer-to-peer payment system until this arises or we can come up with a high level of abstraction. Conversely, in several markets, the versatility of traditional payments is making great strides forward. Standard financial technologies are evolving quickly enough to easily circumvent the block-chain on this front in the relatively near future.[20]

3.4 Tokenizing process

The financial system of the new age is founded upon tokenization, which is used by billions of people every day. It is a mechanism that is by which tokens representing these values replace values. making it easier and safer to exchange them. It may seem distant, but tokenization affects our lives fundamentally and can change whole sectors.If not for tokenization, shopping for goods online will be a much riskier venture. secret data on credit cards, it is transformed into a cryptographic token used by banks to complete the transfer, which is worthless for hackers. Since it is simpler and more reliable, businesses issue digital replacements for stocks and other shares instead of paper. Due to the strength of the block-chain, though people still use tokens on a regular basis (most do not consider this), the true tokenization potential is only now exposed. Block-chain helps you to tokenize a wide range of real assets and organizations securely and effectively, Providing new benefits and applications to a wide variety of markets, such as fashion or health. In fact, tokenization using the block-chain made it possible to fully new trading and fundraising tool-a security token-to be developed. In several areas, the block-chain technology has been used, including financial services, credit and ownership management, market management, cloud computing, content created by users, etc. because of its decentralization, removing confidence, tamper resistance, safety and reliability characteristics. In these cases, Block-chain either addresses the problems of many trust parties in the transaction or decreasing the transaction expense. [21]

4. Block-chain Technology In The Future
7 Predictions For 2020 : [22]

4.1 Failure among most block-chain startups
We saw a growth in block-chain begin funding last year. As all new technology, though, and its application, the block chain is already young, so it does not meet investor standards. As an outcome, it is expected that many block-chains begin are ultimately a waste of time and resources. Not right origins of block-chain implementation will lead to unsuccessful innovations, reckless decisions, Rejection of this revolutionary technology and even utter internal rejection. Block-chain technology will certainly impact all aspects of business in the future, but this is a slow phase that takes time and maturity. Gartner expects most conventional organizations to monitor on block chain technologies, but no action will be planned, waiting for additional explanations of the top implementations for block-chain technology.The reasoning is that for block-chain implementation, traditional firms need more transformation than newly appeared businesses. In Gartner's opinion, only 10 percent of traditional companies will make a dramatic change in blockchain technology by 2023.

4.2 Economy and Finance Will Lead Block-chain Application
The banking and finance sectors, unlike other conventional firms, do not need to implement a radical transition to their block-chain technology implementation processes. Since the cryptocurrency has been effectively implemented, financial institutions are starting to take block-chain use for conventional banking operations seriously.In 2016, for example, in Germany, ReiseBank AG completed instant payments on a cross-border basis between two of its customers using block-chain technologies in around 20 seconds. 77 percent of financial institutions are expected to implement blockchain technology as part of an in-production system or mechanism by2020, according to a new PWC survey. Since the block-chain idea is basic, it would offer substantial savings for banks. Block-chain software will make Banks can minimize excessive complexity, perform faster transactions at lower prices, and increase confidentiality. One of Gartner's block-chain estimates is that with the use of block-chain-centered cryptocurrencies by2020, the banking sector will benefit from $1 billion in market valuation.In addition, block-chain can be used to launch fresh cryptocurrencies that monetary policy can control or affect. Banks want the comparative benefit of stand-alone cryptocurrencies to be minimized and thereby have further control on their financial markets. In addition, at the end of 2020, the Australian Stock Exchange aims to use a modern blockchain-based technology to regulate the financial market in Australia.[23]

4.3 Global Cryptocurrencies are going to appear
The advantages of block-chain-derived currencies would eventually have to be accepted by governments. Governments expressed their skepticism about the practical application of cryptocurrencies as Bitcoin grew. However, When Bitcoin is a consumable currency that no country could manage, they had to think about it. While Bitcoin exchanges are still blocked by some countries such as China, we should expect policymakers to finally recognize the block-chain-based money in 2018 because of its future public and potential operational benefits. By 2022, Gartner estimates that a national cryptocurrency will be issued by at least five nations.[24]

4.4 Integration of the block-chain into government departments
The concept of a public ledger is very enticing to government officials who have to contend with very high data volumes. In fact, each user has its own independent database, so they have to continuously request information from one another about residents. However, it can enhance the operation of those organizations by incorporating block-chain technologies for successful data processing. By 2022, more than a billion users will have any data about them stored on a block-chain, according to Gartner , but they may not be aware of it.[25]

4.5 Block-chain Experts Will Be in High Demand
While the block-chain is at the top of its popularity, there is a shortage of block-chain experts in the job market. An increasingly growing demand for individuals with "block-chain" skills has recently been documented by Upwork, an online freelance directory. There are a small number of block-chain developers as the technology is new.It will serve you well if you join the industry and acquire some skills in block-chain technology. However, due to a lack of funding, there is a possibility that a block-chain start-up that employed you might have to shut down soon. Still, in order to work for a block-chain project, many individuals would choose to leave their current employment. Thus, one of the block-chain developments for 2020 would also be a strong demand for professional block-chain developers.[26]

4.6 Law Integration into Smart Contracts
In relation to cryptocurrencies, another easy option, such as "smart contracts." helps us from block-chain technology. Auto execution as conditions are met is the central concept of smart contracts. For example, selling goods after receiving payment. However other terms of contracts may also be governed automatically. Thus, AIG Industries is now launching a block-chain scheme that allows complicated insurance policies to be created.It should also be recalled that intelligent contracts are autonomous and that they are not governed by any authority. But what are the parties doing in the event of some dispute? Usually, participants in Intelligent contracts expect to be governed by laws, but what if there is a dispute between groups from separate countries? The rule of law can also be applied in smart contracts for the settlement of any conflicts between the parties in the near future. [28]

II. CONCLUSION
Block-chain technology is a new instrument for organizations with future applications, allowing encrypted transactions without the need for a central authority. Solutions focused on technology. Electronic cash systems with the distribution of a global ledger containing all transactions were the first implementations. These transactions are encrypted with cryptographic hashes, and asymmetric-key pairs are used to sign and verify transactions. The use of block-chain technology is still in its early phases, but it is focused on cryptographic concepts that are commonly understood and sound. A block-chain relies on existing network, cryptographic, and recordkeeping technologies, as detailed in this publication, but uses them in a new way. Updates or

improvements to earlier transactions and blocks.

This abstraction of software allows for Working data updates, thus offering a complete background of changes. For such organizations. These are attractive characteristics. These could be deal breakers for others that hinder the adoption of block-chain technology. Block-chain technology is still new and block-chain technology should be handled by companies like they would any other technical solution at their disposal — use it only in suitable circumstances. Block-chain can revolutionize organization operations in many sectors in the future, but it takes time and commitment to introduce it. In the near term we should assume policymakers to completely accept block-chain benefits and start using them to strengthen financial and public services. Although some start-ups in the block chain will struggle, more insight and information about how to use this technology would be provided to individuals. Block-chain will allow individuals to learn new skills, while conventional organizations will have to reinvent their systems entirely.[29]

III. REFERENCES

[1] Narayanan, A., et al., Bitcoin and cryptocurrency technologies: a comprehensive introduction. 2016: Princeton University Press.

[2] Bitcoin, N.S., Bitcoin: A peer-to-peer electronic cash system. 2008.

[3] Casino, F., T.K. Dasaklis, and C. Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 2019. 36: p. 55-81.

[4] Yu, Y., et al., Blockchain-based solutions to security and privacy issues in the Internet of Things. IEEE Wireless Communications, 2018. 25(6): p. 12-18.

[5] Li, D., et al., Information security model of block chain based on intrusion sensing in the IoT environment. Cluster computing, 2019. 22(1): p. 451-468.

[6] Zhao, G., et al., Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. Computers in Industry, 2019. 109: p. 83-99.

[7] Nicholson, J., The library as a facilitator: how bitcoin and block chain technology can aid developing nations. The Serials Librarian, 2017. 73(3-4): p. 357-364.

[8] Kuo, T.-T., et al., EX pectation P ropagation LO gistic RE g R ession on permissioned block CHAIN (ExplorerChain): decentralized online healthcare/genomics predictive model learning. Journal of the American Medical Informatics Association, 2020. 27(5): p. 747-756.

[9] Nofer, M., et al., Blockchain. Business & Information Systems Engineering, 2017. 59(3): p. 183-187.

[10] Smith, S.B., Method and system to use a block chain infrastructure and Smart Contracts to monetize data transactions involving changes to data included into a data supply chain. 2015, Google Patents.

[11] Arora, A. and S.K. Yadav. Block chain based security mechanism for internet of vehicles (IoV). in Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT). 2018.

[12] Nesarani, A., R. Ramar, and S. Pandian, An efficient approach for rice prediction from authenticated Block chain node using machine learning technique. Environmental Technology & Innovation, 2020. 20: p. 101064.

[13] He, S., et al., Decentralizing IoT management systems using blockchain for censorship resistance. IEEE Transactions on Industrial Informatics, 2019. 16(1): p. 715-727.

[14] Reddy, S., securePrune: Secure block pruning in UTXO based blockchains using Accumulators. arXiv preprint arXiv:2010.05448, 2020.

[15] Banavathu Mounika, P., V.L. Narayana, and G.V. Lakshmi, USE OF BLOCK CHAIN TECHNOLOGY IN PROVIDING SECURITY DURING DATA SHARING. Journal of Critical Reviews, 2020. 7(6): p. 338-343.

[16] Oh, S. and C. Lee, Block chain application technology to improve reliability of real estate market. Journal of Society for e-Business Studies, 2017. 22(1).

[17] Buxton, J. and T. Bingham, The rise and challenge of dark net drug markets. Policy brief, 2015. 7: p. 1-24.

[18] Oksiiuk, O. and I. Dmyrieva. Security and privacy issues of blockchain technology. in 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). 2020. IEEE.

[19] Mougayar, W., The business blockchain: promise, practice, and application of the next Internet technology. 2016: John Wiley & Sons.

[20] Sikorski, J.J., J. Haughton, and M. Kraft, Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied energy, 2017. 195: p. 234-246.

[21] Liu, P.T.S. Medical record system using blockchain, big data and tokenization. in International conference on information and communications security. 2016. Springer.

[22] Niu, X. and Z. Li. Research on Supply Chain Management Based on Blockchain Technology. in Journal of Physics: Conference Series. 2019. IOP Publishing.

[23] Foroglou, G. and A.-L. Tsilidou. Further applications of the blockchain. in 12th student conference on managerial science and technology. 2015.

[24] Girasa, R., Regulation of cryptocurrencies and blockchain technologies: national and international perspectives. 2018: Springer.

[25] Liu, W., et al. Advanced block-chain architecture for e-health systems. in 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom). 2017. IEEE.

[26] Lee, J.-H. and M. Pilkington, How the blockchain revolution will reshape the consumer electronics industry [future directions]. IEEE Consumer Electronics Magazine, 2017. 6(3): p. 19-23.

[27] Cao, B., et al., When Internet of Things meets blockchain: Challenges in distributed consensus. IEEE Network, 2019. 33(6): p. 133-139.

[28] Governatori, G., et al., On legal contracts, imperative and declarative smart contracts, and blockchain systems. Artificial Intelligence and Law, 2018. 26(4): p. 377-409.

[29] Ozdemir, A.I., I.M. Ar, and I. Erol, Assessment of blockchain applications in travel and tourism industry. Quality & Quantity, 2019: p. 1-15.