Journal of Modern Computing and Engineering Research
JMCER
Volume 2024, p. 34-43
https://jmcer.org

Identifying the Impacts of Majority Cyberattack on Distributed Ledger and Blockchain

Najla B. Aldabagh[1], Yasir A. Hamza[1] and Nashwan S. Ali[1]

[1,2,3]Dept. of Computer Science, College of Computer Science and Mathematics, University of Mosul, 41002 Mosul, Iraq

[1]najlabadie@uomosul.edu.iq, [2]yasir.23csp57@student.uomosul.edu.iq, [3]nashwan.23csp56@student.uomosul.edu.iq

Received: April 1, 2024 *Revised: June 2, 2024* *Accepted: June 13, 2024*

Abstract

During the last decade, the financial sector has transformed into digital platform by digitizing all their financial services. As a result of this transformation, a new term "Fintech" has appeared that means combining finance and technology together. In addition, a new type of currency, which called cryptocurrencies such as Bitcoin, has become popular for using as an alternative to physical currencies. Using such currencies in financial transactions and working in unsecure and open accessed environment like internet may be led to several problems and threats related to security objectives of participated parties in such transactions. Therefore, blockchain that based on DLT is best approach for securing the financial transactions. In despite of these features of DLT, it has exposed to different types of cyberattacks. In this study, the most well-known majority or 51% cyberattack on DLT has been carefully investigated. According to results of the study, this cyberattack impacts the security objectives for the transactions of parties that are participated on the blockchain network such as (privacy, data integrity, system integrity, availability, authenticity, authorization and accountability). In addition, the adversary is able to apply 51% cyberattack successfully even if has computational power less than 50.

Keywords: *51% cyberattack, blockchain, distributed ledger technology, Impact, Majority cyberattack*

1 Introduction

Recently, the rapidly development and the new technologies have made the financial sector able to involved all these potentials for digitizing their financial services. In addition, this transformation is based on merging two terms together 'finance' and 'technology'. For this reason, sometimes these two terms can be referred as 'Fintech' (Krause S. K. et.al., 2017). Fintech is used to describe any company or innovation that used the new technologies for improving the financial services. Fintech can be emerged via all stages of the financial processes such financial infrastructures, payments, lending, investment, insurance, and venture financing.

Furthermore, blockchain and distributed ledger technology (DLT) have been shown rapidly growth as future technology especially in financial sector (Lemieux, V.L., 2017). DLT has built itself like an umbrella to create multiparty systems that work in decentralized environment without any operator or authority even if these parties may be malicious or unreliable (Rauchs, M. et al., 2018).

In contrast, blockchain is frequently defined as a subset of the DLT general framework that employed a specific data structure such as chain of blocks of data connected with hashed links. DLT, which is the blockchain can be considered a best example for it, has gained more attraction for financial sector (Priem, R., 2020). Therefore, DLT has become an authenticated approach that used for cryptocurrencies trading, like Bitcoins (Krause S. K. et.al., 2017 and Priem, R., 2020). DLT is based on validating the transactions among individual users without requiring a central authority. Consequently, DLT have obtained several applications in securities markets, cross-border payments, and collateral registries (Krause S. K. et.al., 2017). DLT applications are not bounded for using in the financial

Corresponding author: najlabadie@uomosul.edu.iq P-ISSN: 2960-141X E-ISSN: 2958-0021

sectors only, they can be used for facilitating the digital identification products such as (ID cards, birth, death, and marriage records) or to construct tamper proving, records of decentralized flow for materials via a supplier chain by employing trusted stakeholders in order to authorize movements and flow. In addition, DLT has several advantages over the traditional centralized ledgers and shared ledgers. There advantages can be summarized as decentralized, better transparency and auditability, reduced cost, provide high speed and efficiency, and programmability and automatability (Krause S. K. et.al., 2017). While DLT has offered significant features in terms of security such as tamper resistance, fault tolerance, and better availability, it has several vulnerabilities related to cyberattacks (Gojka, E.E. et al., 2021).

This study provides an identifying the impacts of majority cyberattack on distributed ledger and blockchain. Consequently, the contributions can be summarized as follows:

Permissionless DLT is more threaten than permissioned DLT in term of related security concerns.

51% cyberattack has higher impacts on the security objectives and these can be considered as threats on the transactions of parties that are participated on blockchain network includes (privacy, data integrity, system integrity, availability, authenticity, authorization, and accountability).

The adversary can apply such cyberattack even if has computational power less than 50.

In this study, DLT has been reviewed based on the application domains, types of DLT, key points of this technology, and the benefits of using DLT in financial sector. In addition, the most critical cyberattack called 51% has been clarified based on its effectivity on DLT and blockchain. Also, the other cyberattacks that have same strategies of 51% cyberattack have been identified. The remainder sections of this paper are organized as follows. In Section II, DLT extensively is clarified. Blockchain is explained at the Section III. In Section IV, 51% cyberattack carefully is demonstrated in order to identify its threats of DLT and as well as blockchain. The final section is represented the findings of this study and addressed the future work followed by references.

2 DLT

There are a lot of definitions for DLT. According to (Krause S. K. et.al., 2017), DLT can be defined as a novel approach for registering and data sharing via several data stores or ledgers. Therefore, this approach allows different parties to be registered, participated, and synchronized their data and transactions via a distributed network.

In addition, DLT provides a significant supporting for several Peer-to-peer (P2P) networks that works on the internet such as data sharing, email, and other multimedia files. P2P is a type of network that divided tasks or loading between peers. Therefore, such network not required to has a data center like (server) rather than each peer has equal privileges in order to participate in transaction (Kadam, S., 2018). Also, peers have their own processing power, storage space, and network bandwidth which can be sharable among other participated parities on network.

However, using P2P network without centralized ledgers could be a big problem for transferring asset among individual parties. For this reason, transferring asset over internet has still a major problem in past decades because of each transferred asset must be identified by its actual owner and ensuring that the same asset cannot transferred several times like (double spending). Fig. 1 shows the difference between DLT and centralized ledgers.

To overcame such problem, DLT is used a blockchain that represents storing and transmitting data in special package named blocks (Krause S. K. et.al., 2017 and Rauchs, M. et al.,2018). These blocks are connected among them by a digital chain. DLT provides several key attributes for data sharing among distributed network such as scalability, validity, interoperability, security, and fees (Khan, M.D. et al., 2022).

Scalability: In DLT environment, there are several transactions have occurred at each second. This situation is required the system to be able for handling the load according to the increased number of participated

parities in distributed network. Consequently, DLT must be scalable and adaptable with transactions per second (TPS) which either to be constant or increased continuously (Khan, M.D. et al., 2022 and Soltani, R.et al,2022).

Validity: In distributed ledgers, the concept of centralization not found rather than each party work independently and can be able to exchange data with each other. Therefore, such case does not provide the trusting among multiple parties. DLT must be provide a trusting mechanism in system in order to perform tamper proving for each transaction. As a result of that, DLT validation offers for each transaction immutability and auditability.

Interoperability: In DLT environment, each party connect to P2P network with its own machine. These machines can be either heterogonous or homogenous according to their (operating system, machine architecture, network protocols, and user applications). For these reasons, DLT must provide a standard platform that can be worked with different machines (Krause S. K. et.al., 2017 and Khan, M.D. et al., 2022).

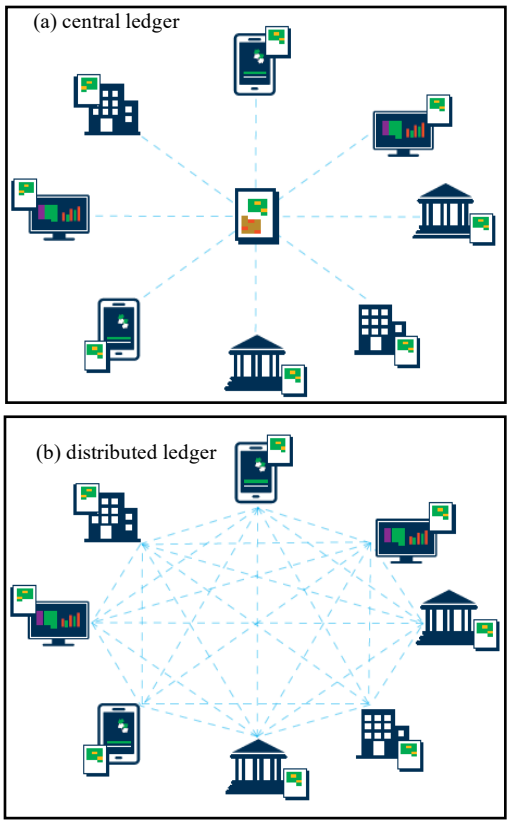

Figure 1: Difference between DLT and centralized ledger. (Krause S. K. et.al., 2017)

Security: Data security can be considered as a major requirement for any system works on untrusted environment like internet. DLT must provide higher security for participated parties in distributed network in order to protect and prevent any cyberattacks (Krause S. K. et.al, 2017, Gojka, E.E. et al., 2021 and Khan, M.D. et al., 2022). As mentioned before, in this study the security concerns of DLT is reviewed carefully especially in terms of cyberattacks.

Fees: The fees of participating in P2P Network for data exchanging among parties are normally attached according to DLT. The reason for that, the transaction validation required powerful computers for solving more complex mathematical problems. In addition, some fees can be dependent on network status at the time, the volume of sent and received data, and the consumed energy during the transaction. The relationship between fees and mentioned factors is reversely (Rauchs, M. et al., 2018, Gojka, E.E. et al., 2021and Khan, M.D. et al., 2022).

There are two types of DLT, the first one is open or permissionless and the second is permissioned (Krause S. K. et.al., 2017 and Wang, C. et al, 2022). The essential differences between these two types can be explained according to using in cryptocurrencies transactions. Bitcoin and Ethereum can be considered as fully permissionless blockchains because of any party on the network able to join or leave at any time without requiring to be preapproved or checking by any party. Therefore, the party is just needed to connect with the network and then add its transaction on the ledger which consist of a computer with special software. In this case, the transaction not needed to central owner and the copies of ledger are distributed to all parties that participated on network. Fig. 1. (b) illustrates the permissionless DLT.

In permissioned DLT as depicted in Fig. 2, the parties are chosen by someone called owner or administrator of ledger. This owner controls the access to network and specifies the rules of ledger. Therefore, the permissioned DLT can be solved many concerns of regulators and governments that related to permissionless DLT like

identification of network members, whom to authorize and regulate, and legitimated owner of the ledger.

Permissioned DLT is differed from permissionless by authorizing bounded numbers of parties that able to engaging in the decision making. Consequently, the roles of participated parties give the impression of being delegated rather than elected.

However, permissionless DLT are more complicated in term of governance due to it provides higher level of decentralization. Therefore, the permissionless DLT should be offering better negotiation and polling approaches for the participated parties for accessing consensus (Anthony Jnr, B., 2023). In fact, there is graduated spectrum for openness and decentralized degrees of DLT started from public permissionless blockchains like Bitcoin and end in private permissioned blockchains.

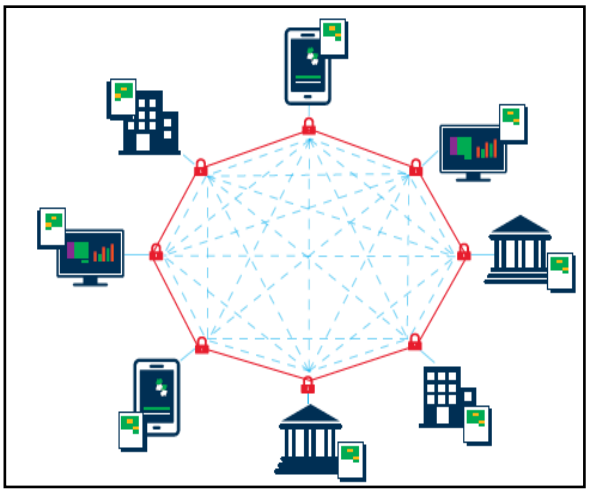

Figure 2: Permissioned DLT (Krause S. K. et.al, 2017)

In addition, each platform differs from others in its specified features. Thus, several companies use a hybrid method by building the permissioned DLT network on the permissionless blockchain infrastructure and restricting roles of the parties on DLT network according to open access. Table 1. illustrates the differences between permissionless and permissioned DLT according to different criteria.

Table 1. Differences between permissionless and permissioned DLT

Criterion	*Permissionless DLT*	*Permissioned DLT*
Central Administrating	Fully decentralized	Decentralized with some external administration
Access	Anyone can be joined	Just selected parties can be joined
Trusting Level	Parties not required to trust each other	Higher level of trusting among parties
Openness	DLT is open and transparent among all parties	DLT can be have different degrees of open and transparent
Security	Security via wide distribution in large-scale network	Security via controlling access to DLT in small-scale network
Speed	Transaction is slower with restricting volume of transaction	Transaction is faster with higher volume of transaction
Consensus	Difficulty for proving transaction and need to provide consensus	Easy in proving transaction and provide different mechanisms of consensus
Identity	Parties are anonymous or used nicknames	Each party must be authenticated by administrator
Asset Type	Just for cryptocurrencies	Any asset
Legitimated Ownership	Lack to identifying the legitimated ownership	Ownership precisely should be legal and administrator is legitimated entity
Example	Bitcoin, Ethereum	Hyperledger Fabric

3 Blockchain

In 2008, Satoshi Nakamoto had proposed a new system of electronic cash based on purely P2P network that allow parties for online payment without requiring to central financial institution (Nakamoto, S., 2008). This system is known as Bitcoin. The proposed system has significant features such as (transaction without trusting parties, proofing of work for transaction, and parties able to leave and reconnect network as desired). In addition, it has solved the big problem of digital money innovation especially double spending problem. This problem has been solved by adopting a new technique called blockchain. The blockchain is best example for employing DLT (Deshpande, A. et al, 2017). Therefore, DLT is most important innovation for digital currencies.

Blockchain can be described as block that consisting a number of consecutive chains as shown in Fig. 3. Each block is attached to its prior block along of chain (Nicolas, K. et al., 2020). In addition, each block can be identified according to four attributes (size of block, header of block, transaction, and transaction counter).

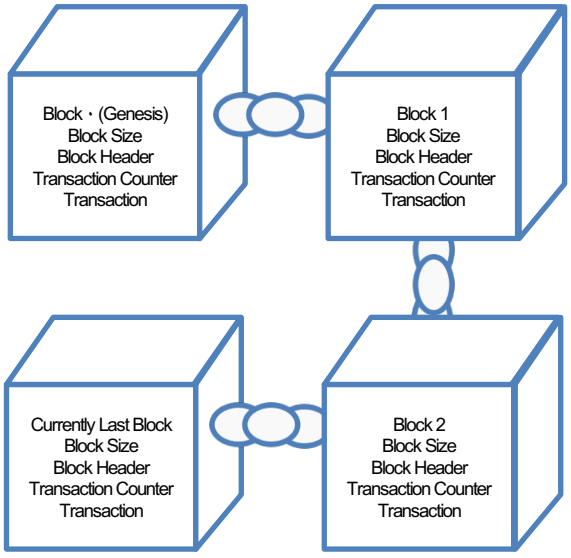

Figure 3: The blockchain

The size of block has four bytes in order to store the entire block. The header of block has size eighty bytes that used to hold the ciphered unique hash for each block. Each transaction has a counter of varying size started from one to nine bytes that refers to the number of relating transactions. The block also stores information about transaction that have size of according to the size of transaction. All blocks are appended into public database in successive order to generate a chain. As mentioned before, blockchain uses P2P network that enable the parties to participate their transactions around world.

4 Cyberattacks on DLT

As mentioned before, DLT offers solutions for security concerns that related to financial sectors. Despite these features, DLT is subjected to cyberattacks that can be applied by adversaries based on some vulnerabilities. In this section of paper, the most well-known 51% cyberattack on DLT is investigated carefully and then analysed in order to summarize all its concerns.

In order to achieve the main objective of this study, several papers that recently published regarded to 51% cyberattack on DLT and as well as blockchain has been collected. Then, this cyberattack is precisely described for identifying its strength and weakness points. In addition, this study aims to clarify major problems and other cyberattacks that are related 51% cyberattack. In other words, 51% cyberattack can be described as starting point for applying other cyberattacks such as (selfish mining, n-confirmation, and double spending) because these cyberattacks work with strategies similar to 51% cyberattack (Sayeed, S. and Marco-Gisbert, H., 2019, Nicolas, K., Wang, Y. and Giakos, G.C., 2019) For these reasons, 51% cyberattack can be considered as the most threaten on DLT as well as blockchain.

4.1. 51% Cyberattack

It can be defined as a cyberattack that targeted the consensus algorithm, that is commonly used proof of work (PoW) algorithm, of DLT application. In this cyberattack, the adversary seeks to obtain either a majority control over the participated nodes or more than half percent of overall computational power in the network (Sayeed, S. and Marco-Gisbert, H., 2019, König, L., Unger et al, 2020). In this case, the adversary

has a permission to disrupted the consensus algorithm and able to refuse any valid blocks. Therefore, these blocks unable to add to the chain (Saad, M. et al, 2020). In addition, the adversary be able to add any malicious content to the chain that involved in transaction. Consequently, 51% cyberattack has another name called consensus hijacking.

In case of one or more than one adversary lunches the 51% cyberattack, they are able to, i) denying the verification of other blocks or transactions that related to trustworthy parities (thus making their blocks or transactions invalid). ii) allowing double spending during the controlling time on the network by reversing the transactions, iii) forking the main blockchain and dividing the network, iv) denying other parties (even the miners) form obtaining any blocks during that period of time (Saad, M. et al, 2020 and Aponte-Novoa, F.A. et al,2021). Therefore, the adversary with more than 50% computational power or hash rate has higher priority over other parities and able to append his/her blocks to blockchain network with higher probability. This situation is based on concept of race conditions.

4.2. Working Mechanism of 51% cyberattack

The 51% cyberattack can be precisely clarified according to the following scenario: consider the adversary has more than 51% computational power of the network and executes a transaction *Tx* with the receiver. Also, he synchronously able generate another deceptive double-spent transaction *Ty* using the same transaction of parent in order to cheating the receiver. On the other side, the receiver waits for n confirmations before releasing the asset to the party who responsible for mining a new block called miner (Saad, M. et al, 2020, Dasgupta, D., Shrein, J.M. and Gupta, K.D., 2019).

The *n confirmations* stand for *n* subsequent blocks which have been mined during executing transaction *Tx* by the network. During this operation, the adversary preserves these mining blocks in the end of transaction *Ty* as well as with double-spent and aims for forking the blockchain after he obtains the asset form the receiver. As a result of chain forking, the adversary has ability to invalidate the transaction *Tx* that belongs to the chain before forking and substitute it with his own chain that hold the transaction Ty with double spent as shown in Fig. 4

To apply 51% cyberattack in efficient manner, the adversary requires to release a lengthy chain with valid *PoW* in order to switch the network into his forked version (Dasgupta, D., Shrein, J.M. and Gupta, K.D., 2019). Therefore, the success of adversary for obtaining his computational power *h* and the number of confirmation *n* depends on the fraction of the total computational power of network.

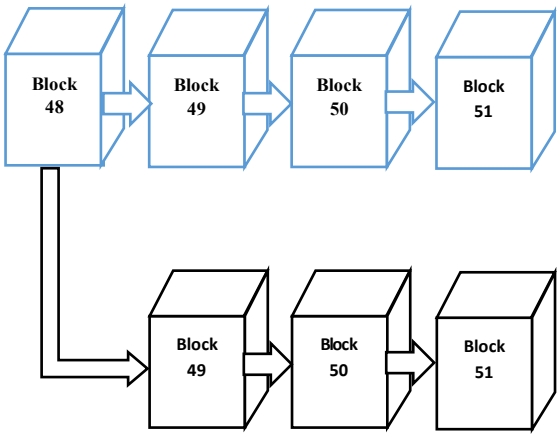

Figure 4: Forking chain, the blue blocks belong to trustworthy parties or miners and they added their blocks into the public blockchain. while, the black blocks added by adversary to its private blockchain and not broadcasting them to the public blockchain.

In order to calculate the probability *P(s)* success of the adversary, suppose g to be computational power of the adversary and h is the remaining computational power of the network, where $g + h = 1$. The probability of success *P(s)* can be determined according to the following formula (Saad, M. et al, 2020):

$$P(s) = \begin{cases} 1 & if\ g > h \\ (\frac{g}{h})^n & if\ g < h \end{cases} \quad (1)$$

According to the above formula, when the value of g more than 50 that means the adversary is able to apply

cyberattack successfully. In case of the value of g less than *50*, the number of blocks play a significant role for increasing the chance of adversary to apply successful cyberattack. Based on the results that obtained from "(1)", when the number of blocks equal to *zero* and the value of *g* equal to *49*, the adversary can be applied cyberattack successfully.

The relationship between the value of g (when less than *50*) and the value of n are inverse relationship. Fig. 5. Illustrates the *P(s)* values according to different values of *g* and *n*.

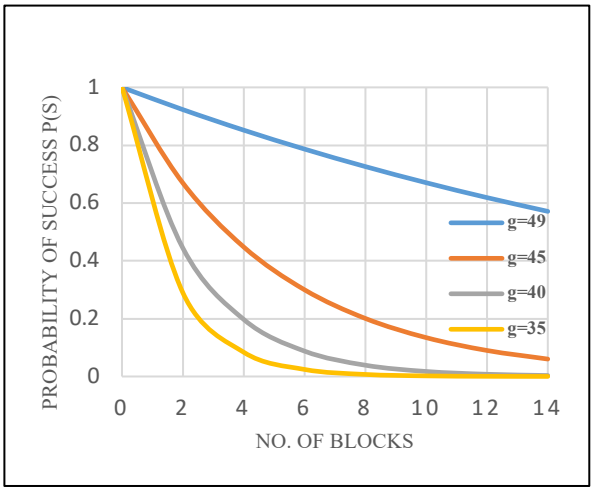

Figure 5. The values of P(s) according to different values of ($g < 50$) and n.

4.3. Impacts of 51% cyberattack

Every cyberattacks have impacts on the three key objectives of security (confidentiality, integrity, and availability). These three objectives are often referred to as the CIA triad (Stallings W., 2020, Hamza, Y.A. and Abduallah, W.M., 2020). Aforementioned cyberattack, it represents the most critical and dangerous cyberattack on DLT and as well as blockchain.

Consequently, the impacts of such cyberattack on the CIA have been clarified precisely in order to identify its threats on DLT based applications. In case of 51% cyberattack applied on cryptocurrencies, it able the adversary to perform malicious activities such as double spending, fully domination on the market price of targeted cryptocurrency, rejecting blocks of trustworthy parties, restricting valid transactions, and controlling the strategies of mining (Sayeed, S. and Marco-Gisbert, H., 2019). In May 2018, 51% cyberattack has been applied on the altcoin Bitcoin Gold and able the adversary to fork it from the main Bitcoin chain. Therefore, this cyberattack led to enable the adversary from stealing $18 million worth of Bitcoin gold (Binance Academy, 2023).

As mentioned before, there are two types of DLT (permissioned and permissionless). In permissioned DLT, the threat of 51% cyberattack mainly depends on the administrator of ledger that controls the transactions of parties on the network. Accordingly, the administrator of ledger can be considered as insider threat (König, L., Unger et al, 2020). While, in permissionless DLT that is based on consensus algorithm for proofing the transactions among different parties (trustworthy and adversary), may be more threaten than permissioned DLT. Therefore, 51% cyberattack heavily impacts permissionless DLT.

Based on the impacts of 51% cyberattack on DLT, the security objectives can be violated as follows: the term confidentiality stands for two concepts (data confidentiality and privacy) (Stallings W., 2022). Therefore, 51% cyberattack trespasses the privacy of trustworthy parties that are participated in transactions over blockchain network. The second term is integrity and includes two types are data integrity and system integrity. When the adversary lunches 51% cyberattack on blockchain network, both the data integrity and system integrity are violated. The integrity of blocks that holds transactions of parties in blockchain network are altered by adversary due to double spending or modifying the market price of cryptocurrency. While the integrity of blockchain system is manipulated in case of the adversary able to be controlling the strategies of mining.

In addition, the ability of adversary to fork the blockchain network is considered as system integrity violation. The last objective of security is availability. Restricting the valid transactions of trustworthy parties and building a private chain are examples for disrupting and denying accessibility the blockchain network. As an

extension to *CIA triad*, there are three additional security objectives that often referred as triple *AAA* (authenticity, authorization, and accountability). The authenticity of blockchain network can be breached, when trustworthy parties unable to proofing their transactions during the consensus algorithm applied in permissionless blockchain network. Authorization is affected in case of the adversary able to gain access to unauthorized resources of blockchain network without any permissions from trustworthy parties. Finally, when the adversary able to fork the blockchain network and build his own private chain without informing the trustworthy parties. Thus, the blockchain network unable to perform accountability requirement and cannot trace its operations.

The previous discussion to impacts of 51% cyberattack on blockchain according to security objectives can be summarized in table. Consequently, Table 2. illustrates each security objective separately and in case of the cyberattack has affected it, then the impact will be assigned by true sign otherwise, the false sign will be used.

Table 2. Impacts of 51% cyberattack according to security objectives

Security Objective	Impact
Data Confidentiality	×
Privacy	√
Data Integrity	√
System Integrity	√
Availability	√
Authorization	√
Authenticity	√
Accountability	√

5 Conclusions

In this paper, DLT has been reviewed according to its usage in the financial sector. Therefore, DLT provides important features for managing and securing the transactions of any assets over unsecured environment like internet. In addition, cryptocurrencies become widely used as an alternative to physical currencies. For these reasons, DLT and as well as blockchain are best framework for exchanging cryptocurrencies in distributed P2P network.

In P2P network, DLT can be configured in two types (permissioned and permissionless). Permissioned DLT has less security problems because of it depends on administrator of ledger that controls the transactions among parties on the network. Therefore, the administrator of ledger can be only considered as insider threat of permissioned DLT. In contrast, permissionless DLT is used widely than permissioned DLT especially in cryptocurrencies. Therefore, it can

be more threaten than permissioned DLT. Finally, the most critical cyberattack that known as 51% has been touched in order to explain its effectivity on DLT and blockchain.

According to the results, 51% cyberattack has higher impacts on the security objectives that known as CIA triad. These impacts are represented as threats on the transactions of parties that are participated on blockchain network includes (privacy, data integrity, system integrity, availability, authenticity, authorization, and accountability). In addition, the probabilities of success for applying such cyberattack has been calculated according to computational power less than *50*. Based on results, the adversary can apply such cyberattack even if has computational power less than *50*. The limitations of this study are not suggested any solution or countermeasure for security problems related to 51% cyberattack. In addition, the study is not used any special case study for different types of cryptocurrencies such as (Bitcoin or Ethereum). Finally, the study represents a short survey paper rather than well-known extensive survey paper. Therefore, these limitations can be considered for future works. Also, providing one or more countermeasures that defeated such attack will be considered as a main objective in future studies.

References

Anthony Jnr, B., 2023. A developed distributed ledger technology architectural layer framework for decentralized governance implementation in virtual enterprise. Information Systems and e-Business

Management, 21(3), pp.437-470. https://doi.org/10.1007/s10257-023-00634-2

Aponte-Novoa, F.A., Orozco, A.L.S., Villanueva-Polanco, R. and Wightman, P., 2021. The 51% attack on blockchains: A mining behavior study. IEEE access, 9, pp.140549-140564. 10.1109/ACCESS.2021.3119291

Binance Academy, 51% Attack, Accessed: Nov. 11, 2023.Available:https://academy.binance.com/en/glossary/51-percent-attack

Dasgupta, D., Shrein, J.M. and Gupta, K.D., 2019. A survey of blockchain from security perspective. Journal of Banking and Financial Technology, 3, pp.1-17. https://doi.org/10.1007/s42786-018-00002-6

Deshpande, A., Stewart, K., Lepetit, L. and Gunashekar, S., 2017. Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. Overview report The British Standards Institution (BSI), 40, p.40.

Gojka, E.E., Kannengießer, N., Sturm, B., Bartsch, J. and Sunyaev, A., 2021. Security in distributed ledger technology: An analysis of vulnerabilities and attack vectors. In Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3 (pp. 722-742). Springer International Publishing. https://doi.org/10.1007/978-3-030-80129-8_50

Hamza, Y.A. and Abduallah, W.M., 2020, April. A Secured Method of Reversible Data Hiding. In 2020 International Conference on Computer Science and Software Engineering (CSASE) (pp. 61-66). IEEE. DOI: 10.1109/CSASE48920.2020.9142098

Kadam, S., 2018, March. Review of distributed ledgers: The technological advances behind cryptocurrency. In International Conference Advances in Computer Technology and Management (ICACTM).

Khan, M.D., Schaefer, D. and Milisavljevic-Syed, J., 2022. A review of distributed ledger technologies in the machine economy: challenges and opportunities in industry and research. Procedia CIRP, 107, pp.1168-1173. https://doi.org/10.1016/j.procir.2022.05.126

König, L., Unger, S., Kieseberg, P., Tjoa, S. and Blockchains, J.R.C., 2020. The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks. J. Internet Serv. Inf. Secur., 10(3), pp.110-127.

Lemieux, V.L., 2017, November. Blockchain and distributed ledgers as trusted recordkeeping systems. In Future technologies conference (FTC) (Vol. 2017).

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system.

Nicolas, K., Wang, Y. and Giakos, G.C., 2019, September. Comprehensive overview of selfish mining and double spending attack countermeasures. In 2019 IEEE 40th Sarnoff Symposium (pp. 1-6). IEEE.

Nicolas, K., Wang, Y., Giakos, G.C., Wei, B. and Shen, H., 2020. Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach. IEEE Access, 9, pp.3838-3857. DOI: 10.1109/ACCESS.2020.3047365

Priem, R., 2020. Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications. Financial Innovation, 6(1), p.11. https://doi.org/10.1186/s40854-019-0169-6

Rauchs, M., Glidden, A., Gordon, B., Pieters, G.C., Recanatini, M., Rostand, F., Vagneur, K. and Zhang, B.Z., 2018. Distributed ledger technology systems: A conceptual framework. Available at SSRN3230013. http://dx.doi.org/10.2139/ssrn.3230013

S. K. Krause, K. Solvej, H. Natarajan, H. L. Gradstein, “Distributed Ledger Technology (DLT) and blockchain,” (English). FinTech note, no.1 Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. and Mohaisen, D., 2020. Exploring

the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), pp.1977-2008.

Sayeed, S. and Marco-Gisbert, H., 2019. Assessing blockchain consensus and security mechanisms against the 51% attack. Applied sciences, 9(9), p.1788.

Soltani, R., Zaman, M., Joshi, R. and Sampalli, S., 2022. Distributed ledger technologies and their applications: A review. Applied Sciences, 12(15), p.7898. https://doi.org/10.3390/app12157898

Stallings W., "Cryptography and Network Security: Principles and Practice," Global Edition, 8th edition, Published by Pearson, 2022.

Wang, C., Dohler, M., López, D., Forbes, R., Steiff, S., Faisal, T., Backia, M., Liu, Q. and Arribas, I., 2022. An Introduction of Permissioned Distributed Ledger (PDL). ETSI White Paper, (48),pp.1-12. etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf

Biography

Najla Badie Al-Dabagh received her B.Sc. degree in computer science from Mosul University, Iraq in 1988, M.Sc. degree in Computer Science in Data Security from Technology University, Iraq in 1995 and Ph.D. degree in Network Security from Mosul University, Iraq in 2006. Currently she is an Associate Professor at the department of Computer Science, College of Computer Science and Mathematics, Mosul University. Her research interests include cryptography, honeypot and intrusion detection, IoT security, network security, and AI.

Yasir Ahmed Hamza is an Associate Professor at Duhok Polytechnic University, Duhok, Iraq. He earned his Master degree in Computer Science from Anadolu University, Turkey in 2008. Currently, he is studying PhD at department of Computer Science - Mosul University. His research interests in the fields of Cybersecurity, Cryptography, and Information Hiding Techniques. He has presented and published several papers in local and international journals.

Nashwan Salih Ali is a programmer at department of IT, directorate of education in Nineveh. He recived his Master degree in Computer Science from Jamia Hamdard University, India in 2012. Currently, he is studying PhD at department of Computer Science - Mosul University. His research interests in the fields of Wireless Sensor Network, AI, and Cybersecurity.