Journal of Computing Research and Innovation (JCRINN) Vol. 6 No. 2 (2021) (pp165-172)
https://jcrinn.com : eISSN: 2600-8793

Review on the Advantages and Disadvantages of Cryptocurrency Attacks

Nornajihah Rusli[1]*, Mohamad Fadli Zolkipli [2]
[1,2] School of Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia

*Corresponding author: * nornajihah_rusli@soc.uum.edu.my*
Received Date: 10 May 2021
Accepted Date: 21 August 2021
Published Date: 1 September 2021

HIGHLIGHTS

- Cryptocurrency attacks by hackers through dark websites, Tor browsers and others.
- The value of digital currency is increasing.
- Databases are used to store and record transactions.
- Blockchain technology uses unique personalized keywords.
- No government intervention in blockchain.

ABSTRACT

The advantages and disadvantages of blockchain technology in cryptocurrency attacks will be explained in this article. Digital currency has been widely used around the world. The soaring value of digital currencies has also led to an increase in the use of cryptocurrency. Cryptocurrency is a form of payment that can be exchanged online for goods and services. The increasingly popular use of cryptocurrency around the world is causing criminals, and hackers are starting to attack cryptocurrency on an ongoing basis. With the advent of blockchain technology, it managed to save the digital currency system with the availability of a decentralized database. Each block has many transactions, and for new transactions will be recorded and added to a decentralized database with a cryptographic signature that does not change making it difficult for abuse and theft. The authors have examined the strengths and weaknesses of the blockchain in cryptocurrency attacks. As a result, the authors support that this blockchain technology can help deal with cryptocurrency attacks that occur.

Keywords: *advantages and disadvantages, cryptocurrency, cryptocurrency attacks, technology blockchain*

INTRODUCTION

Cryptocurrency is a digital payment system for authenticating transactions that does not depend on banks. In other words, cryptocurrency is a peer-to-peer system that allows users regardless of who they are, anywhere to send and receive payments (Judmayer, Tsabary, Stifter, Eyal, Zamyatin, Gazi, Meiklejohn & Weippl, 2021). This digital payment system does not rely on banks to authorize the transaction process. Cryptocurrency is only created through a complex computer process or called mining, where high -powered computers are capable of solving difficult mathematical problems. Once this cryptocurrency is mined, the blockchain will record or add information into a decentralized database to record transactions (Investopedia, 2021). Blockchain is a system of recording information that is impossible and difficult to modify, hack and cheat the system. Basically, a blockchain is a book of transactions that is duplicated and distributed to the

blockchain through an entire network of computer systems. Every new transaction on the blockchain will be recorded and added to the decentralized database.

As the value of cryptocurrency increases in value and its use becomes more widespread even internationally, there are attempts to exploit it illegally through money laundering, breach of restrictions, and cryptography is also on the rise. Moreover, Cryptojacking is the unauthorized use of a person's computer to mine cryptocurrency (Strebko & Romanos, 2018; Roket It, 2021). Often, phishing emails that contain links or attachments often allow hackers to install a piece of code directly on a user's computer without them realizing it. In 2018, there were 51% of attacks occurring against two cryptocurrency networks namely ZenCash and Bitcoin Gold. In the attacks, the total costs for both crypto covered $ 550,000 and $ 18 million (Lite Forex, 2018).

To prevent these attacks from continuing, blockchain technology is used to prevent hacking of digital currency systems. Blockchain technology is an open database that stores all transaction data records on several computers in a worldwide peer-to-peer network (Sarmah, 2018). A database is a center for collecting information or transaction data stored in a computer system. Any information, or data, in the database is arranged in tables to facilitate the retrieval and filtering of information.

However, each technology has its advantages and disadvantages. Therefore, the authors have examined the advantages and disadvantages of blockchain technology in cryptocurrency attacks. Among its advantages are a reliable distributed system, no government interface, increased security & financial efficiency, better stability, and instant payment with cost reduction. The disadvantages of this technology are private keys, 51% attacks, difficult data modification, large energy consumption, and illegal activity.

The use of cryptocurrency system is higher than cash in Malaysia. The use of cryptocurrency systems can be seen when shopping malls, hotels and restaurants use these systems to make payments and transactions. Even convenience stores, and eateries on the shoulder of the road also use cryptocurrency systems to make payments. This is because, most users already have their own e-wallet and prefer to use it. However, some consumers are worried about saving money in this digital money system. Therefore, everyone should know that there is blockchain technology that protects this digital money system from being hacked by hackers. Users should also be aware of the strengths and weaknesses of this blockchain technology in protecting digital currency.

LITERATURE REVIEW

a) Advantages of Technology Blockchain

i. Security

The security of blockchain technology is highly guaranteed. This is because, a unique identity is given when each individual enters a blockchain network to make a link to his or her account. This is to ensure that the account owner himself is doing the transaction. Besides that, the technology has blockchain encryption, causing hackers to have difficulty interfering with traditional chain provisioning.

ii. Banking the Unbanked

Blockchain and bitcoin users are made up of anyone regardless of ethnicity, background, culture, gender to use this technology. According to the world bank, nearly 2 billion people from the adult category do not have a bank account or a way to keep their money or property (Lite Forex, 2018). Although most people live in developing countries and have stable economies, they are still completely dependent on cash.

For those who do not have a bank account, it is likely that they received the money physically and chose to keep the cash in a hidden place such as in their residence or residence. Moreover, for more people who choose to use technologies such as Bitcoin, Litecoin or other cryptocurrencies to store their money and wealth. This is because this option is easier to store and hide money and wealth than to hide it under a mattress or in a residence.

Moreover, blockchain is looking for ways and ideas to further improve its technology. In the future this technology can not only be used as a place to store money or wealth, but can also be used for property rights, keeping medical records, permanent assets, and various other contracts.

iii. Secure Transactions

In transactions, the use of cryptocurrency is safer and easier to use. This is because every transaction made will be recorders, and the blockchain network will verify its authenticity. There are thousands of computers used to verify purchase details correctly on the blockchain. Upon completion of the transaction confirmation and it will be added a block. Each block in blockchain technology has a unique hash. Further, if the information on a block is updated or changed, the hash code of that block will change (Arnason, 2015). However, the hash code on the block will remain. Therefore, information about the blockchain is difficult to change without notification.

iv. Transparency

Most blockchain technologies are software openly so that everyone can see their code. Auditors have the ability to review cryptocurrency security. Also, the rules of the bitcoin code and how it is updated, there is no real authority. Therefore, anyone can provide suggestions on changes or improvements to this blockchain system. This suggests that if the majority of users agree the new code version with its improvements is the best and worth it then bitcoin will be updated.

b) Disadvantages of Technology Blockchain

i. Technology cost

Generally, for all users, blockchain is a technology that can save users money when making transaction payments, and its technology is free. Transaction verification by using large sums of money for calculations performed by bitcoin or a “proof of work” system. However, the bitcoin network uses millions of computers almost like the one used by Denmark every year. Assuming the cost of electricity used is around $ 0.03 ~ $ 0.05 per kilowatt-hour, around $ 5,000 ~ $ 7,000 per coin is used to cover the cost of mining (Lite Forex, 2018).

A As a result, there is an increase in the total cost of electricity when using this technology to validate transactions. This is because, in order to make their time and energy more valuable, miners will add blocks to the bitcoin blockchain. Although blockchain does not use cryptocurrency, miners must be paid or given other incentives to validate transactions.

ii. Extremely Volatile

Blockchain technology that defines cryptocurrencies. One example is the price of Bitcoin which fluctuates differently every day. Behind this instability is decentralized blockchain technology and virtual currency is a new character for the market. This means that companies, governments, and other groups that adopt or do not use it will inevitably influence the volatility of cryptocurrencies. This causes people to be confused as to whether they want to invest in Bitcoin or invest in another cryptocurrency.

The Advantages and Disadvantage of Blockchain

The use of cryptocurrency has been widely used across the country. There are many industries and businesses that use this cryptocurrency to facilitate them in payment transactions. However, not all industries, businesses and consumers know the advantages and disadvantages of cryptocurrency.

a) The Advantages of Blockchain

i. Trusted Distributed Systems

Previously, transaction processes used traditional methods that had intermediaries party such as banks, credit cards, or other services (Binance Academy, 2020; Redbytes, 2020). This transaction method has additional charges in the form of transaction fees. This additional transaction fee will be charged each time the user processes a transaction. However, with the advent of blockchain technology, every transaction made is open or free or there is no additional charge.

In addition, blockchain technology has distributed network nodes to authenticate each stage of the transaction and replace intermediary requirements. This authentication process will confirm all types of transactions throughout the transaction performed by the user (Sarmah, 2018). Thus, the blockchain has never experienced a failure to monitor in terms of transaction aspects. If intermediaries are not used, then it will reduce the risk of depending on one organization and also reduce costs.

ii. No Government Interface

Blockchain technology is able to manage key systems operated by existing governments more effectively. This technology is able to create, store, and forward transaction-related information even per transaction and at all times. Therefore, governments or financial institutions have no control over virtual currencies that use blockchain technology. Government intervention often causes the devaluation of various currencies and a good example is the recent Zimbabwe dollar (Redbytes, 2020).

Moreover, regardless of country and currency, one of the main problems, when governments interfere with currency a lot, they end up with inflation or hyperinflation by printing too many currencies in a short time (Redbytes, 2020). With the existence of blockchain technology as a decentralized online ledger, it is impossible for governments to intervene and take action against cryptocurrency.

iii. Improved Security & Financial Efficiency

Processing by blockchain technology is faster and easier to gain trust compared to traditional procedures. Blockchain that there is no third-party intervention leading to greater financial efficiency (Redbytes, 2020).

By using this technology, it will allow users to enjoy the process of money transactions, time savings, and without additional charges.

As such, users will rely entirely on the blockchain as they do not rely on one organization for their entire transaction process. In addition, the system will offer information to users related to several open networks and even one server as in traditional transaction systems. Therefore, this blockchain technology will prevent the occurrence of hacking from cybercrime as the transaction is publicly distributed.

iv. Improved Stability

The company now relies entirely on this system which has higher retention in its services (Redbytes, 2020). Once data is registered and stored in a digital ledger, it is difficult to remove or alter that data. This is enough to prove that a great enough technology is used by to store property data, financial records, and other data (Binance Academy, 2020; 101 Blockchains, 2021). Therefore, ledgers that track and record changes are permanently distributed publicly until an audit trail is required.

In addition, data stored on the Blockchain can only be viewed and accessed by persons with authorized access. The precision and paperless system allows for more transparency throughout the transaction process. This suggests that stable blockchain technology can make the process easier.

Companies that use this technology to prevent and avoid fraudulent behaviors that can be committed by its employees (Binance Academy, 2020). Blockchain is able to ensure that all records of transactions performed by the company are secure and stable. With the use of this technology, employees will find it more difficult to hide suspicious transactions.

v. Instant Payments at Reduced Costs

The transactions done via Blockchain is rapid but at a reduced overall cost (Redbytes, 2020). The traditional processes in the transaction process are replaced by simpler methods with single Blockchain record keeping. The payment process can be completed easily and reliably without third party intervention. Through the blockchain technology, documentation that processes in detail is eliminated and transactions are performed with the least number of errors. Cryptocurrency helps in streamlining the process faster and reducing costs.

b) Disadvantages of Blockchain

i. Private Key

Blockchain technology uses asymmetric or better known as public key cryptography (Kiktenko, Kudinov & Fedorow, 2019). this asymmetry is used is to assign cryptocurrency units or other blockchain data to user ownership (Binance Academy, 2020; Caporale, Kang, Spagnolo & Spagnolo, 2020). Each blockchain usage has an individual personal keyword. Although the blockchain address is shared with individuals who can access it via a private key and the private key must be kept confidential to prevent misuse. If the user loses his private key, the process will be a failure, the money will be lost, and the user will not be able to do anything about it (Binance Academy, 2020; Redbytes, 2020; Azret, Sergey & Rasul, 2020).

ii. 51% Attack Costs

Blockchain technology is protected by a consensus algorithm to be a highly efficient Proof of Work (Binance Academy, 2020; 101 Blockchains, 2021). There are several possible attacks taking place on blockchain technology networks and those attacks have resulted in 51% of them being a large total cost up to hundreds of thousands as shown in figure 2. If an entity is able to address more than 50% of the network, it is highly likely that the attack will be attacked, intentionally disrupting the network by altering or excluding transaction order.

Although in theory, the blockchain has never been attacked up to 51% (Lite Forex, 2018). However, as the network gets bigger, security increases and miners will not dare to invest large sums of money.

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$113.24 B	SHA-256	34,061 PH/s	*$469,115*	1%
Ethereum	ETH	$50.34 B	Ethash	217 TH/s	*$371,492*	3%
Bitcoin Cash	BCH	$14.97 B	SHA-256	5,468 PH/s	*$75,308*	9%
Litecoin	LTC	$5.62 B	Scrypt	295 TH/s	*$54,421*	7%
Dash	DASH	$2.15 B	X11	1 PH/s	*$8,666*	48%
Monero	XMR	$2.05 B	CryptoNightV7	360 MH/s	*$15,130*	21%
Ethereum Classic	ETC	$1.42 B	Ethash	8 TH/s	*$13,604*	92%
Zcash	ZEC	$821.14 M	Equihash	573 MH/s	*$56,676*	8%
Bytecoin	BCN	$814.01 M	CryptoNight	432 MH/s	*$919*	99%
Bitcoin Gold	BTG	$580.09 M	Equihash	27 MH/s	$2,636	180%

Figure 2: Show a list of coins and the theoretical cost of a 51% attack on each network (Lite Forex, 2018).

iii. Difficult Data Modification

In blockchain technology, to add or change data that has been recorded is very difficult. This is because, the data modification process requires rewriting the code and performing an extensive process (Redbytes, 2020). Too high stability is likely to affect the system. Therefore, the record is irreversible and its modification process is required. Moreover, to change data or code will cause one network to be abandoned and a new one to be used.

iv. Large Energy Consumption

Users need to go through a consensus process, to ensure that every transaction made is valid. This suggests the consensus process requires more effort to form each node (Lite Forex, 2018). In addition, all nodes must communicate back and forth to ensure that the transaction is valid. The use of concession algorithms as proof of work that requires more computational power to increase overall power consumption.

v. Invalid Activity

Confidentiality of blockchain technology networks in protecting users from hacking and maintaining privacy. In addition, it can also be used as a place of trade and illegal activities in this network. For example, in February 2011 to October 2013, there were illegal transactions, and online websites, yet they were successfully shut down by the Federal Bureau of Investigation (FBI) (Lite Forex, 2018).

Moreover, the shady website allows users to browse it freely and is undetectable by onion routers (Tor browser). In addition, the site is used for illegal purchases directly in Bitcoin, Litecoin or other cryptocurrencies. Blockchain technology can also be seen as pros and cons. This is because, the account can be accessed by anyone, but criminals can also make transactions more easily (Dragomiretskiy, 2018).

CONCLUSION

In conclusion, cryptocurrency is a digital payment system for authenticating transactions that does not depend on banks. The increasing use of cryptocurrency around the world has resulted in attacks on cryptocurrency. However, the advent of blockchain technology is able to prevent cryptocurrency from being attacked and hacked by criminals, hackers, and scammer. Each block in the blockchain contains a number of transactions, and each transaction is recorded and added to a decentralized database. Therefore, users also need to know the advantages and disadvantages of blockchain technology in preventing attacks on this cryptocurrency. By knowing the advantages and disadvantages of this blockchain, users will be more confident to use it.

ACKNOWLEDGMENTS

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

REFERENCES

101 Blockchains. (2021). Ultimate Guide to Pros and Cons of Blockchain Retrieved February 02, 2021, 2021, from https://101blockchains.com/disadvantages-of-blockchain/

Arnason, S. L. (2015). Cryptocurrency and Bitcoin: A Possible Foundation of Future Currency why it has Value, what is its History and its Future Outlook, 2015.

Azret A., Sergey D., & Rasul A. (2020). Analysis of DDoS Attacks on Bitcoin Cryptocurrency Payment System. Revista Espcios, 2020.

Binance Academy. (2020). Blockchain Advantages and Disadvantages. Retrieved October 09, 2020, 2020, from https://academy.binance.com/en/articles/positives-and-negatives-of-blockchain

Dragomiretskiy, S. (2018). The Influence of DDoS Attacks on Cryptocurrency Exchamges. *International Journal of Network Security & Its Applications (IJNSA)*, 2018.

Guglielmo Maria Caporale, Woo-Young Kang, Fabio Spagnolo, & Nicola Spagnolo. (2020). Cyber-Attacks, Cryptocurriences, & Cyber Security. *Munich Society for the Promotion of Economic Research*, 2020.

Investpedia. (2020). Blockchain Explained Retrieved from November 17, 2020, 2020, from https://www.investopedia.com/terms/b/blockchain.asp

Judmayer, A., Tsabary, I., Stifter, N., Eyat, I., Zamyatin, A., Gazi, P., Meiklejohn, S. & Weippl E. (2021). Pay-To-Win: Incentive Attacks on Proof-of-Work Cryptocurrencies. 2021.

Kiktenko, E.O, Kudinov, M.A. & Fedorow, A.K. (2019).Detecting Brute-Force Attacks on Cryptocurrency Wallets. *International Conference on Business Information Systems*, 2019.

Lite Forex. (2018). Cryptocurrency Attacks: Types of Vulnerabilities, Risks and Results. Retrieved January 15, 2018, 2018, from https://www.liteforex.com/blog/for-investors/eight-fears-of-a-beginner-investor-and-how-to-overcome-them/

Redbytes. (2020). Advantages and Disadvantages of Blockchain Technology. Retrieved November 05, 2020, 2020, from https://www.redbytes.in/advantages-and-disadvantages-of-blockchain-technology/

Rocket It. (2021). Protecting Your Pot of Gold | Tips for Securing Cryptocurrency. Retrieved March 16, 2021, 2021, from https://rocketit.com/cryptocurrency-security-cryptojacking/

Sarmah, S.S. (2018). Understanding Blockchain Technology. Computer Science and Engineering, 2018, 23-29.

Strebko, J. & Romanos, A. (2018). The Advantages and Disadvantages of the Blockchain Technology. IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018.