Mühendislik Bilimleri ve Tasarım Dergisi
10(3), 1000 – 1013, 2022
e-ISSN: 1308-6693

Journal of Engineering Sciences and Design
DOI: 10.21923/jesd.978517

Araştırma Makalesi Research Article

ANALYSIS OF DATA SECURITY AND CYBER-ATTACK METHODS IN DIGITAL CURRENCY

İsa AVCI*

Karabük Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Karabük, Türkiye

Keywords

Data Security, *Cybersecurity*, *Cyber-Attack Methods*, *Digital Currency*.

Abstract

With the rapid development of technology in recent years, digital data in information technology has become an indispensable area of life. The use of digital data services in our daily lives has become inevitable. Money transactions, purchases, and money transfers are made by banks and users every day. With the transition from paper systems to digital systems, the number of users is increasing day by day, but there are security concerns about these systems. In modern technologies, the possibility of information theft, the risk of cyber-attack, and the fear of breaches are constantly being worried about financial losses. Since such digital currency transactions carry the personal data and privacy of users, everyone needs to complete the correct transactions reliably. Due to the great importance of financial transactions and digital currencies in daily life, this article explains the features of digital currency and how to prevent counterfeiting. It will also analyze what tools are safe to use in a cryptocurrency. The risks that the algorithm mechanisms used in these processes can handle are examined and security problems are explained. In addition, security methods, algorithms, digital currency cyber-attack methods, and security measures of crypto money are examined.

DİJİTAL PARA BİRİMLERİNDE VERİ GÜVENLİĞİ VE SİBER SALDIRI YÖNTEMLERİNİN ANALİZİ

Anahtar Kelimeler

Veri Güvenliği, Siber Güvenlik, Siber Saldırı Yöntemleri, Dijital Para.

Öz

Teknolojinin son yıllarda hızla gelişmesiyle birlikte bilgi teknolojisindeki dijital veriler hayatın vazgeçilmez bir alanı haline gelmiştir. Dijital veri servislerinin günlük yaşamımızda kullanılması kaçınılmaz hale gelmiştir. Her gün bankalar ve kullanıcılar tarafından para işlemleri, satın almalar ve para havaleleri yapılmaktadır. Kağıt sistemlerden dijital sistemlere geçişle birlikte kullanıcı sayısı her geçen gün artmaktadır ancak bu sistemlerle ilgili güvenlik endişeleri bulunmaktadır. Modern teknolojilerde bilgi hırsızlığı olasılığı, siber saldırı riski ve ihlal korkusu finansal kayıplara yol açabileceği endişesi sürekli yaşanmaktadır. Bu tür dijital para işlemleri, kullanıcıların kişisel verilerini ve gizliliğini taşıdığı için herkesin doğru işlemleri güvenilir bir şekilde tamamlaması gerekmektedir. Finansal işlemlerin ve dijital para birimlerinin günlük yaşamdaki büyük önemi nedeniyle, bu makalede dijital para biriminin özelliklerini ve sahteciliğe nasıl önlem alınması gerektiği açıklanmaktadır. Ayrıca bir kripto para birimini kullanmak için güvenli olan araçların neler olduğunu analiz edilecektir. Bu işlemlerde kullanılan algoritma mekanizmalarının ele alabileceği riskler incelenerek güvenlik sorunları anlatılmaktadır. Ayrıca kripto paranın güvenlik yöntemleri, algoritmaları, dijital para siber saldırı yöntemleri ve güvenlik önlemleri incelenmiştir.

Alıntı / Cite

Avcı, İ., (2022). Analysis of Data Security and Cyber-Attack Methods in Digital Currency, Journal of Engineering Sciences and Design, 10(3), 1000-1013.

Yazar Kimliği / Author ID (ORCID Number)

İ. Avcı, 0000-0001-7032-8018

Makale Süreci / Article Process	
Başvuru Tarihi / Submission Date	04.08.2021
Revizyon Tarihi / Revision Date	04.11.2021
Kabul Tarihi / Accepted Date	22.03.2022
Yayım Tarihi / Published Date	30.09.2022

1. Introduction

* İlgili yazar / Corresponding author: isaavci@karabuk.edu.tr, +90-533-425-6111

With the developing technologies, order taking from commercial transactions, confirmation of delivery, transactions, and commercial communications are made over the internet. Tremendous development and continuous advancement in banking technology have enabled many banks to offer easy-to-use money transfers over the Internet through secure techniques, known as electronic transactions.

Much of the early blockchain work focused on Bitcoin's success. Having a real, tangible blockchain application accessible to virtually anybody was a surprise discovery for financial speculators and academics alike. Following the Bitcoin trend, in turn, has demonstrated the upward scalability and stability of blockchain-based applications. This successful use case has led to an ideal situation for researchers seeking funding to expand and explore larger and more complex blockchain applications. While many have found beneficial applications and improvements, there have also been cases and experiments reporting various negative and undesirable effects of blockchain.

Today, most people do banking transactions such as cash withdrawals, money transfers, payphones, electricity bills, and shop online after official business hours using the internet without physical interaction with bank employees. Bank, deposit, transfer, balance inquiry, mini statement, withdrawal, express cash, etc. influenced its customers by performing banking transactions in various ways. As we deal with digital data, the rate of cybercrime is increasing day by day. Crime and criminal attacks target cybersecurity and cyber information also by attacking the electronic banking system and illegally stealing basic personal information for customers (account details, card details, user ID, password, etc.).

In this study, we found it necessary to do an article and scientific research on digital currencies, the data used in them, and how to deal with them. First of all, the studies will be examined, digital currencies, security of digital currencies, cyber events, and cyber attacks will be examined. Thus, cyber security and security measures will be evaluated specifically for digital currencies.

2. Literature Survey

Cryptocurrencies and their data are vulnerable to theft and attempted attack and the user account becomes vulnerable to attack. Not only is it a threat to the user, but it is also a threat to the bank. The research in this article will include identifying the most important digital currencies included in Bitcoin and their counterparts, as well as the method of electronic dealing with digital financial data and the risks that may face its users and the services that can be obtained. We intend to provide a full description as a general reference for dealing with digital financial data. Many scientific research and articles have been presented regarding digital currency data, and the following is a set of research and what it included regarding digital currencies and the study in their fields, in which we can benefit from the experiences provided in them to provide a comprehensive description and sufficient information regarding digital currencies, the risks of digital data, how to protect them and the best use of them.

Table 1. Literature review for related research

No	Researchers	Research	Secured
1	Guglielmo Maria Caporale, Woo-Young Kang, Fabio Spagnolo , Nicola Spagnolo (Caporale et al., 2021)	Cyber-attacks, spillovers, and contagion in the cryptocurrency markets	Effects and fluctuations between (Bitcoin, Litecoin, and Ethereum) and cyberattacks. They found that cyber-attacks strengthen connections across markets, which reduces opportunities for portfolio diversification for cryptocurrency investors.
2	Guglielmo Maria, Woo-YoungKanga, Fabio Spagnoloa, Nicola Spagnolo (Caporale et al., 2020)	Non-linearities, cyber-attacks, and cryptocurrencies	Analyzing the effects of cyber-attacks on (Bitcoin, Ethereum, Litecoin, Stellar) from 8/8/2015 to 2/28/2019, after examining the results, Significant they concluded that there are negative effects of cyber-attacks on the likelihood of cryptocurrencies remaining in the system of low volatility.
3	Guglielmo Maria Caporalea, Woo-Young Kang, Fabio Spagnolo and Nicola Spagnolo (Caporale et al., 2020)	Cyber-attacks and Cryptocurrencies	Looking at the effects of cyberattacks on their revenues, volatility, and trading volume in 99 developed countries (Bitcoin, Ethereum, Litecoin, XRP, and Steller), crypto investors, exhibits risk-loving behavior when hash rate and cryptocurrency returns increase and are risk-averse when economic uncertainty is high when cyberattacks target financial and industrial sectors.

After studying the research presented in digital currencies, we will get to know these digital currencies by choosing

some of them to talk about them in detail and how to deal with those currencies and carry out sales, purchase, and deposit operations, then identify the risks of using them by studying the events and electronic attacks that happened previously, then we move on to know those attacks and how to protect and safety From them, and we also learn about some of the algorithms that are used in data security, to reach a comprehensive guide for dealing with digital currencies.

3. Digital Currencies

Digital currency is all the money, currencies and financial transactions that can be performed using digital computers, the digital currency could be stored and exchanged, as well as sending and receiving it or performing the operations of buying and selling using it and one of the important advantages of digital currencies is that they, like codes or data or bytes, cannot be touched and also cannot be possessed or dealt with except with the presence of computers or mobile devices and the need to connect to the Internet and servers for the electronic wallet, not like paper or metal currencies that can be touched and possessed. Despite these differences, but digital currencies can also purchase goods and services online, digital currencies possess the essential characteristics of paper currencies, which are the possibility of conducting financial transactions and correspondence smoothly and immediately and not restricted by traditional financial transactions procedures (Al-Laham et al., 2009). It is possible to conduct a process of buying and selling between two different countries at a lower cost than the cost of a regular way and without being subject to the commission calculated by the authorities, but the limits should not be exceeded allowed for transactions. Despite the great similarity in the advantages that can be used in all types of paper and digital currencies, there is a difference in many variables. When digital currencies are a group of cryptocurrencies virtual currencies, the issuance of digital currencies by a country's central bank takes place in an organized manner, it is called a "central bank digital currency (CBDC)" and resides in a digital currency. and conceptual form (Bank of England, 2021). It should be noted that the UK, Sweden, and Uruguay are among the countries that are considering launching a digital version of their original paper currency, provided that it is a controlled currency, and an unregulated digital currency can be issued in addition to the regular CBDC. It differs from the first type in that it qualifies as a virtual currency and can be regulated by a defined network protocol rather than currency creators, founders, or a central regulator (Bank for International Settlements, 2021). This virtual currency is an example of cryptocurrency and coupons, or cash rewards associated with systems are included.

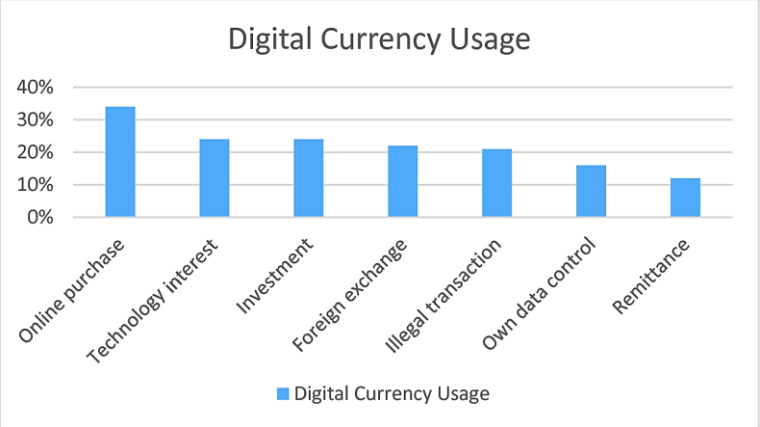

Figure 1. Digital currencies usage (De Silva et al, 2021)

Considering the use of digital currencies, online purchase is around 35% and ranks first. Looking at the next uses, investment and technology interest is around 25%. It is seen that digital currencies are mostly used in the field of online internet shopping.

3.1. Alternate Cryptocurrencies

There are many currencies in circulation at present, some of which are widely known and some that are not traded and used, and we will highlight the most important of these currencies.

3.1.1. Bitcoin

Bitcoin is a cryptocurrency that was created in 2008 by a group of people using the name Satoshi Nakamoto and started working on it in 2009 and is considered a decentralized digital currency. It is the sole authority and does not need intermediaries to complete the sending process between itself. The sending process takes place on a

private network and the process is verification, encryption, and registration under a private distributor called blockchain (Artisantechgroup, 2021).

3.1.2. Ethereum

It is an open-source, decentralized blockchain and is the second-largest cryptocurrency by market capitalization after Bitcoin and the most used. This currency was created in 2013 by Programmer Vitalik Buterin. In 2015, it started with the ability to run decentralized applications and script programs by the Ethereum virtual machine and began implementing a series of upgrades called Ethereum 2.0 (Nytimes, 2021).

3.1.3. Litecoin

It is one of the most important digital currencies launched in the world in 2011. It was developed by Charlie Lee, a graduate of the Massachusetts Institute of Technology and a former engineer at Google, and can be described as one of the world's largest cryptocurrencies (Newreleases, 2021). Litecoin is based on a global network of open sources is not subject to any authority or centralization. As proof of action that can be decrypted by consumer-grade CPUs. Litecoin, compared to Bitcoin has more rewards faster-rendering speed per the blocks and blocks.

3.1.4. Cardano

It is also one of the most important cryptocurrencies, having been developed by engineers, mathematicians, and cryptologists utilizing a research-based methodology. Charles Hoskinson, one of Ethereum's initial five founding members (Investopedia, 2021), was a co-founder of the project. Because it seeks to build decentralized financial products and give solutions for serial interoperability, Cardano has emerged as a leader among its peers in demonstrating the stake in addition to other big cryptocurrencies.

3.1.5. Stellar

It is also an open blockchain network that is meant to deliver business solutions by linking financial institutions to execute huge transactions between them and banks and enterprises very immediately, without the need of middlemen, and at a low or no cost to the parties involved (Thenextweb, 2021). The Lumens is Stellar's first currency (XLM). Users must have Lumens to make transactions and remittances on the network.

3.2. Cryptocurrencies Prices

The table below, based on digital data, displays the market value of the most major digital currencies in the market, and because these values fluctuate based on transactions, they are continuously moving up and down. The figures in the table are intended to illustrate an approximate value for those currencies (Coinmarketcap, 2021).

Table 2. Cryptocurrencies prices.

#	Name	Price	Circulating Supply	#	Name	Price	Circulating Supply
1	Bitcoin	$53,800.20	18,691,981 BTC	10	Litecoin	$244.86	66,752,415 LTC
2	Ethereum	$2,487.33	115,630,493 ETH	11	BitCash	$835.14	18,719,544 BCH
3	Binance Coin	$536.58	153,432,897 BNB	12	Chainlink	$34.53	419,009,556 LINK
4	XRP	$1.33	45,404,028,640 XRP	13	Solana	$45.64	269,856,623 SOL
5	Tether	$0.9999	50,006,254,439 USDT	14	VeChain	$0.1879	64,315,576,989 VET
6	Cardano	$1.23	31,948,309,441 ADA	15	USD Coin	$1.00	11,243,286,480 USDC
7	Dogecoin	$0.267	129,348,760,640 DOGE	16	Stellar	$0.4775	22,917,382,485 XLM
8	Polkadot	$32.89	933,058,442 DOT	17	THETA	$10.74	1,000,000,000 THETA
9	Uniswap	$36.13	523,384,244 UNI	18	Filecoin	$150.62	68,327,015 FIL

Through the amount of digital currency, if the value storing means of a currency we can see that it is available, or relative value over time and can be trusted to malfunction protection and contemporary era coins often takes the money form. Fiat currency does not have the same intrinsic value as precious metal coins. Individuals can and certainly do use electronic cash and payment systems. Some kind of money, "representative" is based on that. This

means that each commodity can be directly replaced with a certain amount of coins or banknotes. So the numbers and the values of the digital currencies are relatively variable in time (CRS, 2021). The changing value of the digital currency has added positive and negative aspects to it, and because of that change, the stock exchange has become effective and mostly used, but the negative effect is the loss of the ability to rely on digital currencies with a fixed value in business and transactions. For example, if we know that the value of 100 pounds is equivalent to a certain amount of Bitcoin at present, then that value may increase or decrease over time, and on the next day, we may not get that value again.

3.3. Advantages and Disadvantages of Cryptocurrency

Cryptocurrencies, customers, and direct money transfers between users are some of the easiest ways to bank or credit card and there is no need for a public institution like the company. Transfers and deposits, public and private keys are secured using a variety of authentication and security steps and share business proof or evidence, such as various incentive systems. What distinguishes modern digital currency systems is that for every user or client there is an electronic wallet that contains a public key, and this owner also has a private key for completing operations and signing transactions, and the operations are carried out with very little financial fees compared to the traditional money transfer and remittance operations. Besides these advantages, some of the cryptocurrencies are considered suitable for illegal business because some of their types are not subject to a central authority and their semi-anonymous nature, but privacy and security are very high in some of their types. Online, given that forensic analysis of the Bitcoin blockchain helps authorities arrest and prosecute criminals. However, some currencies such as Dash, Monero, or ZCash are very difficult to monitor because they are built and built to protect privacy and not share their networks to protect and secure the privacy of customers and user information (JPMorgan Chase, 2021).

One of the benefits of digital currencies is also the provision of highly efficient government payments, and if the government develops a digital currency, then financial payments such as tax amounts, bills, and all financial instruments can be sent to people immediately, instead of trying to mail them a check or discover prepaid debit cards. The existence of a very large number of digital currencies at present. Negatively affects the identification of digital currencies that may be suitable for specific use cases, including whether some of them are designed to expand the scope of adoption and they also need a high effort on how to use them, acquire them and learn how to perform the basic functions with them, also Blockchain transactions can be expensive and fluctuate Continuous price changes and a lot of change may be negative, especially if it is requested to use it completely in all financial transactions (Livetechit, 2021). After studying the strengths and weaknesses of digital currencies, we can make a comparison between the pros and cons of dealing with digital currencies.

Table 3. Advantages and disadvantages of cryptocurrency

Advantages	Disadvantages
1- Easiest ways to transfer money. 2- Transfers and deposits are secured by using public and private keys. 3- Operations are carried out with very few financial fees. 4- Provision of highly efficient government payments. 5- Easy way to be used widely in different applications.	1- Not subject to a central authority. 2- Semi-anonymous nature. 3- The existence of a very large number of digital currencies at present. 4- Need a high effort on how to use them. 5- Transactions can be expensive and fluctuate through continuous price changes.

4. Digital Currencies Transactıon and Security

Digital money is exchanged using technologies such as smartphones, credit cards, and digital currency exchanges over the Internet. In some cases, it can be converted into physical cash, for example by withdrawing cash from an ATM, and because we are dealing here with money sums and private accounts, one of the most important things that must be pointed out is how to secure these operations and accounts. Blockchain technology is commonly used to create cryptocurrencies. The method transactions are recorded in "blocks" and time-stamped is described by blockchain (Andola et al., 2021). It's a lengthy, complicated procedure, but the result is a secure digital ledger of bitcoin transactions that hackers can't alter. For making transactions on financial and account transfers, a two-factor authentication process is required to ensure high security of information, such as entering a username and a passcode, and it may require entering an authentication code that reaches the user's phone or e-mail, and these steps may help to add high security for transactions with digital currencies, but this does not mean that cryptocurrencies are not Permeable. Several breakthroughs have already occurred, and this has cost many breaches and high financial losses for startups in the field of digital currencies in a big way.

4.1. Blockchain Technologies

The initial concept of blockchain was created by Satoshi Nakamoto in 2008, and a year later it became a fundamental component of the cryptocurrency. Then it developed quickly, and its technology was developed, but it did not acquire the final form, and we can say that the rules and standards for it are not yet complete (Zhang et al., 2020). Bitcoin is the first identifier system for electronic cash, written by Nakamoto and created between spouses, the system includes the blocks and chains that are interconnected, and Bitcoin transaction accounts are formed as a data structure that records data specified. A timestamp server receives a block or group of items with a timestamp and stamps, and then hash it publishes on a large scale. This includes a distributed database, with Internet book value for a peer-to-peer network is called the blockchain (Abdi et al., 2020).

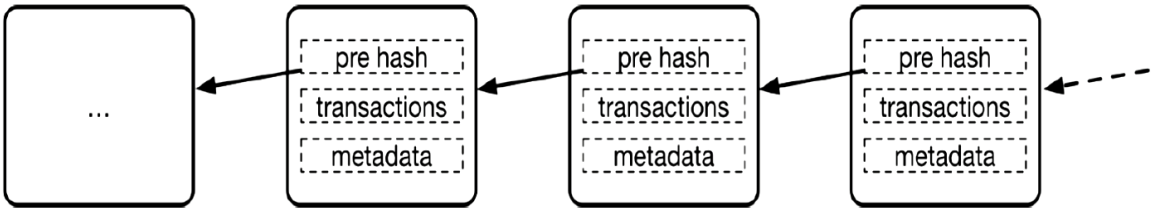

Figure 2. Blockchain structure as in blockchain security analysis overview research (Wang et al., 2018)

4.1.1. Blockchain Classification

Blockchains can be divided into three categories depending on the people who join and interact with them: public consortium and special blockchains are chains based on their relationship with the main chain and side chains. Furthermore, many blockchains may be linked to form a network. The Interchain is created by connecting the chains in the network (Fang et al., 2018). A public blockchain is a consensus blockchain that anybody in the blockchain topology may access and transmit transactions and validations to, and they are typically regarded to be decentralized. A common example is the Bitcoin blockchain, which stores information that is fully disclosed (Casino et al., 2019).

The private blockchain is the final authority. Private blockchains work by limiting who may join the network through access controls. The ability to read might be granted to the general population or restricted to a certain extent. Because the network is controlled by one or more organizations, transactions must be carried out by third parties. There are other choices inside a corporation, such as database administration, auditing, and so on. In many situations, public access is not required. Between the public chain and the private chain, the consortium blockchain refers to a blockchain whose consensus process is controlled by pre-selected nodes (Polge et al., 2021). The ability to view the blockchain might be public, participant-restricted, or mixed.' These networks are referred to as "partially decentralized."

4.1.2. Blockchain Applications

The system of digital currency, the expansion cannot be obtained in a conventional system because it is supported by reliable procedures for financial transactions. This case confirms the importance of blockchain applications in the future, as all financial work will be done with high efficiency and reliability, and the signed contracts will follow the agreement strictly as the cost of the business system will be greatly reduced and by adding to the improvement of social media efficiency, we may argue that, like the internet, the blockchain has the potential to spark a new industrial revolution (Lee et al., 2018).

Consumer blockchain applications must be wide open, transparent, and auditable to work properly. They can be implemented on an open-ended public chain or on a blockchain that is typically owned by multi-center nodes. The most important use of blockchain right now is in financial services, and blockchain can be used to handle ownership, copyright, and traceability. It covers transactions involving assets like automobiles, houses, and artwork, as well as recognizable digital publications and resources, in addition to establishing a transparent and traceable cross-border food supply chain. This new supply chain will enhance food traceability and logistics while also making the global food market safer (De Haro-Olmo et al., 2020).

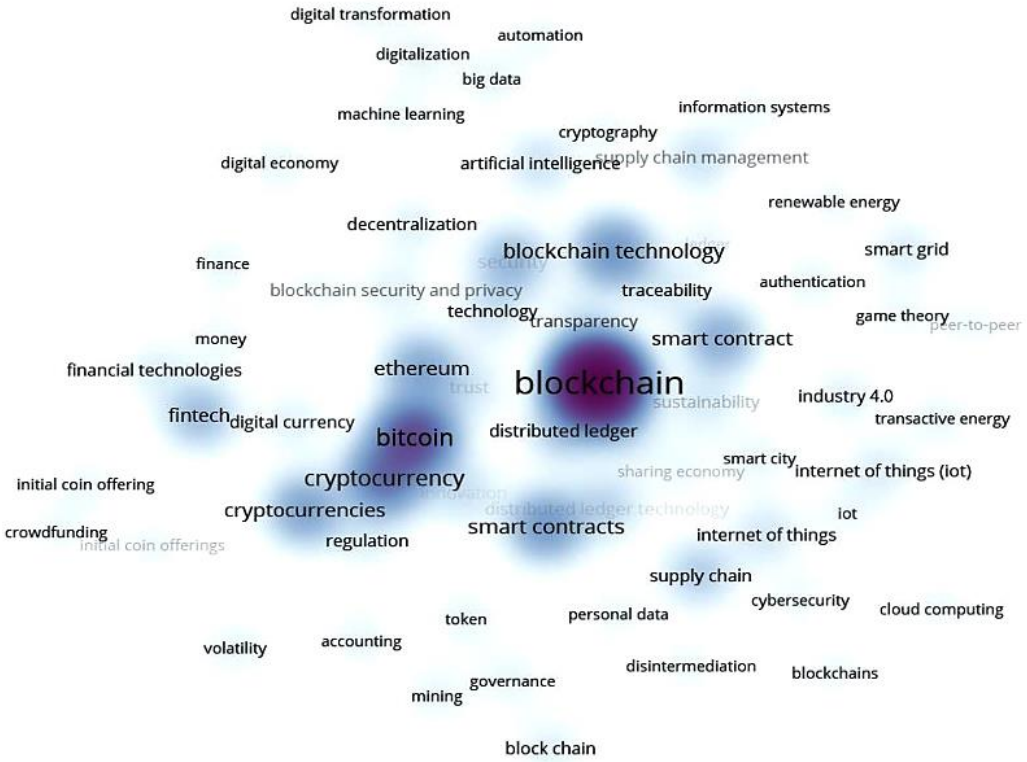

Figure 3. Blockchain applications (Tandon et al., 2021)

4.1.3. Blockchain Security Analysis

With the use of blockchain technology on a large scale, many and many different types of attacks appeared, as in some of those attacks, many digital currencies were stolen and added to the fake accounts machine in the stock exchange, and according to statistics in this field, economic losses with nearly two billion dollars are due to security incidents in information and blockchain data in 2018. This is only a small fraction of what is currently available, and the number of attacks will increase as the value of the blockchain increases (BCSEC, 2021).

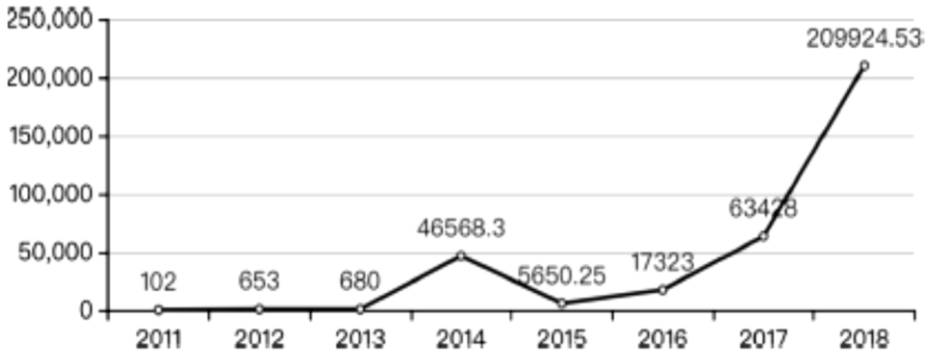

Figure 4. Economic losses caused by blockchain security incidents (ten thousand dollars) as in an overview of blockchain security analysis research (Wang et al., 2018)

Blockchain technology still lags far behind in the early stages of development and security development needs. To keep pace with the development and avoid attacks and internal and external risks, and avoid the need to deal with frequent authentication, more security, protection, and privacy in the storage, transfer, and processing of data can be exposed, protect the privacy and develop security solutions to improve the performance of the security system of the blockchain. Application layer, layer intelligent contracts, incentives layer, consensus layer, network layer, and data layer architecture create the current block and chain security analysis shall be performed separately for each layer (Wang et al., 2018). Application layer security largely addresses security concerns for centralized nodes, such as bitcoin exchanges and financial institutions that handle significant sums of money. The attackers, all blocks chain network at any point of failure because they were lovers targeting these nodes, attack efficiency is huge and costs to a minimum. Access to the Exchange Server without authorization. Stocks frequently deposit significant

sums of money and are hence easy to target (Heilman et al., 2015). An attacker could steal the money of the key after you change the amount may change or have seized control of the exchange server and basic knowledge of the process may leave critical information released, which in turn damages the economy and reputation of the stock market. The smart contract is more than just a computer program that can be run automatically; It is also a system participant. Responds to incoming messages, you can take, and store values, knowledge, and values can be transferred. The following attacks are summarized in terms of smart contract security threats.

The essence of a reentry attack is to block the nodes' flow of control and destroy the offspring of the process, which could be seen as a logical problem in a race situation. The purpose of the incentive level is to provide special incentives to encourage nodes to participate in blockchain security audits. Blockchain security depends on the interaction of many nodes. Blockchain information transfer is mainly based on a peer-to-peer network. A P2P network relies on neighbors to transmit information to reveal each other's IP addresses. It is very easy for an attacker on the network to spread security threats to other hosts (Matzutt et al., 2018). Block Data, harmful information assault, and malicious information writing in the blockchain, such as malware signatures, politically sensitive issues, and so on. Information cannot be deleted after it is written to the blockchain because of the data recovery functionality. If malicious data is found on the blockchain, it will cause a slew of issues.

4.2. Digital Currencies Security Risk

Digital currencies rise and the development of technology for use with application usage increases, the occurrence of certain risks is the inevitable line. we present some of the risks that digital currencies can be exposed to in Table 4.

Table 4. Cryptocurrency security risks

#	Security Risk
1	Risk comes from the difficulty in finding hash group junctions and that is a task that miners do.
2	The risk that cases represent "51%" of the more likely cases in both network attacks that could control the global blockchain ledger and create an alternative blockchain is limited to what the attacker can do even at this stage.
3	The risk of an attacker canceling their transactions or blocking other transactions.

The seizure by law enforcement also cryptocurrency such as PayPal or prohibiting its use by the receiver is less likely. All cryptocurrencies are anonymous, and some additional features allow complete anonymity (Greeshma, 2015).

4.2.1. Cyber-Attacks and Cybercrime

It's vital to recognize that the technology that underpins Bitcoin's functioning is not inherently illegal and that people seeking anonymity in a modern world of intrusive, ubiquitous monitoring are not either. Incidents continue to occur, indicating evident problems with transaction malleability and secure Bitcoin storage, but this is sometimes ascribed to a lack of knowledge of security needs (Caporale et al., 2020).

Cybercrime is defined as a fault that a computer is used as an object or tool for processing the main components of the crime; cyber espionage, from individuals to profit from illegal exploitation, groups and to obtain information without permission from the government hacker techniques and malicious software (such as Trojan horses and spyware) is defined as the use of (Caporale et al., 2021). One of the most common crypto theft attacks can be defined as the unauthorized use of another person's computer to mine cryptocurrencies, as the encryption code runs here in the background and victims often use their computers as usual. The only sign they might notice is poorer performance or performance lag. There are two main ways hackers can secretly search for cryptocurrency on a victim's computer. One is to trick victims into downloading an encryption code to their computer or injecting a script into an advertisement on one or more websites (Eskandari et al., 2018). The code runs complex math problems on victims' computers and sends the results to a server controlled by hackers. The reason for the popularity of this attack is that it brings a lot of money and in turn reduces the risk because unlike the ransomware and the code here, the encryption code works because the hacker is not identified or identified. It may remain deceptive and unknown for a long time and may not be discovered and will be very difficult if found. Follow him back to the source as his illegal activities are hard to trace (Nadeau, 2018).

Include the dangers of crypto theft security training, install a plugin to prevent crypto theft protection, use definitions that can provide endpoint protection from known crypto miners, and protect your web filtering tool (Caporale et al., 2021). If you specify a web page giving Cryptojacking scripts, make sure your users' access is denied again. Browser extensions must be protected. Mobile device management to better control what's going on in your users' devices (MDM) solution use. However, none of the above fail-safes is the recommended method. In

response to this and the growing number of cryptocurrency theft protection cases, The Coalition, a provider of cyber risk solutions, has launched service fraud insurance (Saad et al., 2018).

4.2.2. Algorithms for Security

Many types of cryptocurrencies and protection in the way we deal with these digital currencies, as cryptocurrencies carry many options and information technology activities as they carry accurate and private data and are handled with the presence of high-precision servers to execute transactions, and it is necessary to protect this data and prevent breaches. algorithms should be used. Cryptocurrencies are created based on hashing algorithms to perform hash data. Two of the algorithms for the protection and security of information and data will be highlighted as the mode and mechanism of operation.

A) AES Algorithm

It is a form of encryption that protects data and data transmission over the internet, and it is one of the finest encryption protocols available. Data is asymmetric encryption types that use the same key to encrypt and decrypt code. It encrypts data using a replacement permutation network method with several rounds (Cybernews, 2021). AES encryption keys come in three different lengths: 3.4 x 1038 for 128-bit keys, 6.2 x 1057 for 192-bit keys, and 1.1 x 1077 for 256-bit keys This encryption method's key length fluctuates but remains constant, and much other encryption as well as to use less memory according to the format, easy to understand, implement, offers advantages such as simple and extremely fast encryption and decryption speeds.

The working steps of the algorithms are as follows:

1. Splitting data into blocks: This algorithm encrypts data in blocks of bits, not bits so that each of its blocks contains a column of 16 bytes in a four-by-four pattern. Since a byte contains 8 bits, we get a block size of 128 bits (16x8 = 128).
2. Key expansion: Generates new 128-bit round keys using the Rijndael key program.
3. Adding the round key: the algorithm adds the first key to our expression, which was previously converted to a 4×4 block.
4. Byte replacement: the algorithm replaces each byte with a code according to a pre-generated table called Rijndael S-box (Gaspar et al., 2009).
5. Line wrapping: replaces the lines of the received block during a byte replacement operation. The first row remains in place. However, the second line moves one byte left, the third line moves two bytes left, and the last line moves three bytes left:
6. The columns are shuffled: each column is multiplied by a predefined matrix, resulting in a new code block.
7. Using the Round Key: Now it's time to use the round key we got in the Key Expansion section.
8. Flush and repeat: Depending on the length of the AES key, the algorithm goes through many more cycles such as changing bytes, moving rows, shuffling columns, and adding keys: 9 cycles for a 128-bit key, 11 cycles for a 192-bit key, and 11 256 For -bit round key: 13 turns (Kumar et al., 2016).

Finally, after the indicated 9, 11, or 13 rounds of encryption, another round follows. In this extra loop, the method only performs byte replacement, line wrapping, and padding around the key. Skips concatenating columns. As a result, at the end of the encryption process, the data will go through the following number of rounds: 10 rounds with a 128-bit key, 12 rounds with a 192-bit key, and 14 rounds with a 256-bit key (Cybernews, 2021).

B) SHA Algorithm

One of the most prominent hashing algorithms, SHA (Secure Hash Algorithm), is recognized for its security and speed. When no keys are created, such as when mining Bitcoin, a quick hash method like SHA-2 is typically used. The family of cryptographic hash functions is divided into versions by numbers following the name, with SHA-0 being the initial version of the 160-bit hash function and SHA-1 resembling the previous MD5 method. After then, SHA-2 was followed by SHA-256 and SHA-512, a family of two identical hash algorithms with differing block sizes. Then SHA-3, originally known as Keccak, was released as a hash algorithm, chosen in 2012 after a public competition among non-NSA designers (Gupta and Kumar, 2014). It uses the same hash lengths as SHA-2 and has a different internal structure than the rest of the SHA family (Guesmi et al., 2016).

As an example, we will study SHA 256 steps of working for encryption;

1. Pre-Processing: converting the input string to binary and appending 64 bits to the end
2. Create Hash Values (h): the algorithm generates eight hash values. The first 32 bits of the fractional portions of the square roots of the first 8 primes are represented by these hard-coded constants: 2, 3, 5, 7, 11, 13, 17, 19

3. Initialize Round Constants (k): the method generates some constants this time, 64 in all. The first 32 bits of the fractional portions of the cube roots of the first 64 primes make up each value (0-63)
4. Chunk Loop: For each 512-bit "chunk" of data from the input data, the procedures below will be performed.
5. Create Message Schedule (w): takes the string from the previous step and adds extra zero-valued words, modifying them to make a paragraph (Bayat-Sarmadi et al., 2014).
6. Compression: assign variables a, b, c, d, e, f, g, and h to the current hash values. The compression loop should be executed after h0, h1, h2, h3, h4, h5, h6, h7. The values of a will be changed by the compression loop... h
7. Edit Final Values: We modify the hash values by adding their corresponding variables to them, a-h, after the compression loop, but still within the chunk loop. All addition is modulo 232 as is customary.
8. Concatenate the Final Hash: Finally, slap them all together; a simple string concatenation will be enough to produce a hashed string (Zhu et al., 2018).

4.3. Digital Currencies Experienced Cyber Attack Incidents

Cryptocurrencies are generally safe, but Exchanges are always vulnerable to assault, particularly when they are busy. Cryptocurrency exchanges must take security seriously and implement security measures to prevent security breaches (Caporale et al., 2020). As long as crypto exchanges are profitable, hackers will continue to target them. A reputable cryptocurrency exchange, on the other hand, would have many security measures in place. The following is a list of attempted assaults that resulted in millions of dollars in losses:

Table 5. Cryptocurrency attacks that made money-losing according to finyear.com (Finyear, 2021)

Date	The Project	Stolen Crypto	Stolen USD	Date	The Project	Stolen Crypto	Stolen USD
Feb 2017	Bithumb	-	7 mln $	Jan 2018	Bitstamp	18000 BTC	5 mln $
Apr 2017	YouBit	-	5.6 mln$	Jan 2018	Coincheck	523mln NEM	534 mln $
Apr 2017	Yapizon	3816 BTC	5.3 mln$	Feb 2018	Bitgrail	17mln NANO	170mln $
Apr 2017	EtherDelta	-	266 K$	Jun 2018	Bithumb	-	32 mln $
Aug 2017	OKEx	-	3 mln $	Jun 2018	Coinrail	-	37 mln $
Sept 2017	Coinis	-	-	Jun 2018	Bancor	-	23 mln $
Dec 2017	YouBit	17% BCEX	-	Sept 2018	Zaif	-	60 mln $

From February 2017 until September 2018 the amount of stolen money was 882 million and the number didn't stop there so the selected currency and the way to deal with are very important to avoid being the victim.

4.4 Digital Currencies Cyber-Attack Methods

It's crucial to understand that cyber-attacks infect businesses and their data daily. Former Cisco CEO John Chambers famously remarked, "There are two sorts of companies: those that have been hacked and those that you don't yet know has been hacked"(CISCO, 2021), according to the Cisco Annual Cybersecurity Report. Every year, cybercrime rises as people try to exploit flaws in corporate systems. Attackers frequently seek ransom, and cyber-threats can be conducted for a variety of reasons. Some attackers view system and data suppression as a form of "hacking". Many cyber-attack methods are related to cryptocurrencies that we should study.

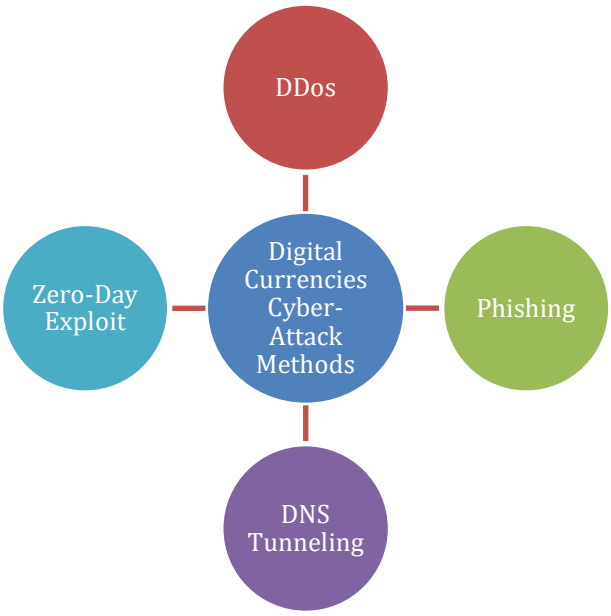

Figure 5. Digital currencies cyber-attack methods

4.4.1 DDoS Attack

DDoS attacks, multiple computer systems, or connected devices such as IoT devices are used as a source of attack traffic. During the attack, computers or other resources possibly exposed to a Trojan target a single system and are forced to flood a server with data until it becomes unusable. Therefore, both the targeted system and all systems used by the hacker for malicious purposes are victims of a DDoS attack.

DDoS attacks can be carried out by various actors, such as individual hackers, organized crime gangs, or government agencies. The motivation behind a DDoS attack can be a childish joke, revenge, or political activism. While attacks sometimes cause only a minor annoyance to the target system, sometimes they can lead to a long-term crash in the system. In some cases, bad coding, incomplete updates, unstable systems, or even legitimate requests to target systems can result in DDoS-like results.

4.4.2 Phishing

Phishing attacks are usually attacking to access sensitive and confidential information such as usernames, passwords, credit card information, network credentials. Cyber attackers use social engineering to masquerade as a normal individual or organization over the phone or email, manipulating victims to perform certain actions – such as clicking on a harmful link or attachment – or willingly revealing confidential information.

The purpose here is; is to convince the person receiving the e-mail that there is something in the message that they want or need – such as a request from a customer bank or an e-mail from a colleague at his company. Apart from email, phishing scams can also use phone calls, text messages, and social media tools to trick victims into providing sensitive information.

4.4.3 DNS Tunneling

The process of moving data belonging to another protocol within a protocol is called protocol tunneling. Any TCP/UDP packet (HTTP, FTP, ssh, etc.) among DNS packets ... Authorized DNS server from the queried domain name responds for the relevant DNS record, and the DNS server forwards this response to the client.

4.4.4 Zero-Day Exploit

Zero-day is a recently discovered broad term that describes vulnerabilities that hackers can use to attack systems. The term “zero-day” means that the supplier or developer has just learned of the problem and has “zero days” to fix the problem. A zero-day attack occurs when hackers exploit this bug before software developers have had a chance to fix the vulnerability.

4.5 Measures Against Cyber Attacks in Digital Currencies

Cyber attacks on digital currencies are increasing more and more today. How these attacks occur and the precautions that can be taken against these attacks are given in Table 6.

Table 6. Measures against cyberattacks in digital currencies.

Methods	Simple Definition	Measures
DDoS	This traffic, due to which the systems, servers, or networks lack the resources and capacity. As a result, the system cannot perform the actual requests. This attack can also be launched using multiple compromised devices.	SIEM, Network Segmentation
Phishing	Phishing is the practice of sending fraudulent e-mails that appear to come from a legitimate source. Objective, credit card and login information or steal sensitive data such as malware to infect the victim's computer. Phishing is a cyber threat increasingly widespread.	Update programs and systems regularly, Monitor for intrusion
DNS Tunneling	DNS tunneling communicates non-DNS traffic across port 53 using the DNS protocol. It uses DNS to transport HTTP and other protocol traffic. Data is transferred from the compromised system to the attacker's infrastructure by manipulating DNS requests. It can also be used for command-and-control callbacks from the attacker's infrastructure to the compromised system.	Network Segmentation, Control access
Zero-day exploit	It occurs after a network vulnerability has been publicly disclosed but before a patch or remedy has been applied. During this period, attackers will focus on the publicly reported vulnerability. The identification of zero-day vulnerabilities necessitates continual monitoring.	SIEM, Network Segmentation

The important thing that needs to be done to deal with the increase in cybercrime should be known as awareness and know-how worldwide for individuals in general and companies. In addition, among the other major obstacles is probably the legal perspective, meaning that despite the existence of special laws in each country or region which Violating data privacy and theft are prevented, so the Internet is identified as an international tool for those who carry out electronic attacks, and the only way to defeat cybercrime is for decision-makers to think to act on the global level and support the rights and safety of citizens in the whole world (Bendovschi, 2015).

5. Conclusion

Cryptocurrencies are quickly becoming a reality, gaining significant momentum in a brief period, and developing rapidly. Studying the behavior of digital currencies and the way to deal with them in the event of a shift from the traditional method to digital currencies reveals that there are many crimes and attacks in them. As they are only composed of data in the space of the internet servers, this does not prevent the existence of many applications that can help in the completion of many operations in record times. To switch to digital currencies, one should wait to reach major digital currencies or choose currencies according to the characteristics that distinguish them because they are all subject to encryption and protection algorithms.

Continuous development creates continuous challenges for responsible users of technology and regulators alike. For the future, defensive programs must be developed against digital currencies' attacks by using data security and forecasting theories and algorithms to protect private information. If the traditional physical method and quantity processes are abandoned and used in many areas, it should ensure that safe and should solve security problems. In terms of safety, they should handle cyber-attacks, secure applications should use against them, and secure encryption algorithms should be preferred.

In this article, we were able to shed light on the important aspects in dealing with digital currencies for the general user or those who are interested in knowing how these currencies work by studying their types and algorithms used in them, as well as the security of their data, events, and attacks that took place. In the future, these algorithms can be applied and compared with each other to obtain different results and choose the most appropriate data encryption to help protect it.

Conflict of Interest

No conflict of interest was declared by the authors.

References

Abdi, A. I., Eassa, F. E., Jambi K., Almarhabi, K., Al-Ghamdi, A. S. A., 2020. Blockchain Platforms and Access Control Classification for IoT Systems, Symmetry, 12(10), 1663.

AL-LAHAM, M., AL-TARAWNEH, H., ABDALLAT, N., 2009. "Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy", Issues in Informing Science and Information Technology, 6: 339–349.doi:10.28945/1063.

Andola, N. et al., 2021. "Anonymity on blockchain-based e-cash protocols—A survey.", Computer Science Review 40 (2021): 100394.

Artisantechgroup, 2021. What is a blockchain, anyway?, https://artisantechgroup.com/what-is-a-blockchain/, (Accessed Date: 29.06.2021).

Bank of England, 2021. "Central Bank Digital Currency: Opportunities, Challenges and Design.", (Accessed Date: 10.06.2021).

Bank for International Settlements. (2021), "Impending Arrival – A Sequel to the Survey on Central Bank Digital Currency," Page 10, (Accessed Date: 15.06.2021).

BCSEC Security Trend Analysis, 2021. https://bcsec.org/analyse, (Accessed Date: 22.06.2021).

Bayat-Sarmadi, S., Mozaffari-Kermani, M., and Reyhani-Masoleh, A., 2014. "Efficient and concurrent reliable realization of the secure cryptographic SHA-3 algorithm.", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33.7, (2014): 1105-1109.

Caporale, G. M. et al., 2020. "Non-linearities, cyber-attacks and cryptocurrencies.", Finance Research Letters 32, (2020): 101297.

Bendovschi, A., 2015. "Cyber-attacks–trends, patterns and security countermeasures.", Procedia Economics and Finance 28, (2015): 24-31.

Caporale, G. M., et al., 2021. "Cyber-attacks, spillovers and contagion in the cryptocurrency markets.", Journal of International Financial Markets, Institutions and Money, (2021): 101298.

Caporale, G. M. et al., 2020. Cyber-attacks and cryptocurrencies, No. 8124, CESifo Working Paper.

Caporale, G. M., Kang, W.-Y., SpagnoloPAGNOLO, F., SPAGNOLO, N., 2021. Cyber-attacks and cryptocurrencies (No. 8124), CESifo Working Paper.

Casino, F., DASAKLIS, T. K., PATSAKIS, C., 2019. A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telematics and informatics, 36, 55-81.

Cisco,2021. https://www.cisco.com/c/m/en_uk/campaigns/security/cyber-threats-and-protection-2018-report/index.html ,(Accessed Date: 03.06.2021).

Congressional Research Service, 2021. "Cryptocurrency: The Economics of Money and Selected Policy Issues,", (Accessed Date: 29.06.2021).

Coinmarketcap, 2021. "https://coinmarketcap.com/" data taken on 26-04-2021 10:45 PM for top 18 coins, (Accessed Date: 29.06.2021).

Cybernews,2021.https://cybernews.com/resources/what-is-aes-encryption/, Accessed May 13, (2021).

De Haro-Olmo, F. J., ÁNGEL JESÚS, V.-V., and JOSÉ ANTONİO ÁLVAREZ-BERMEJO, J.A., 2020. "Blockchain from the perspective of privacy and anonymisation: a systematic literature review.", Sensors, 20.24 (2020): 7171.

De Silva, S., Goyal, S.B., Bedi, P., 2021. Security Challenges of Digital Currency System. In: Abraham A., Sasaki H., Rios R., Gandhi N., Singh U., Ma K. (eds) Innovations in Bio-Inspired Computing and Applications. IBICA 2020. Advances in Intelligent Systems and Computing, vol 1372. Springer, Cham. https://doi.org/10.1007/978-3-030-73603-3_51

Eskandari, S. et al., 2018. "A first look at browser-based cryptojacking.", 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE.

Fang, W. et al., 2018. Cybersecurity in the blockchain: threats and countermeasures, J. Cyber Security, 3(2), 87–104.

Finyear, 2021. https://www.finyear.com/14-cyber-attacks-on-crypto-exchanges-resulted-in-a-loss-of-882 million_a40041.html, (Accessed Date: 23.06.2021).

Gaspar, L. et al., 2009. "Efficient AES s-boxes implementation for non-volatile FPGAs.", 2009 International Conference on Field Programmable Logic and Applications, IEEE, (2009).

Guesmi, R. et al. (2016), "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2.", Nonlinear Dynamics, 83.3, (2016): 1123-1136.

Gupta, P., Kumar, S., 2014. A comparative analysis of SHA and MD5 algorithm, Architecture, 1, 5.

Greeshma, K. V. (2015), Crypto Currencies and Cybercrime, International Journal of Engineering and TechnicalResearch,https://www.ijert.org/research/crypto-currencies, (Accessed Date: 23.06.2021).

Heilmen, E. et al. (2015), "Eclipse attacks on bitcoin's peer-to-peer network.", 24th {USENIX} Security Symposium ({USENIX} Security 15).

Investopedia, 2021. https://www.investopedia.com/news/introduction-cardano/, (Accessed Date:21.06.2021).

JPMorgan Chase, 2021. "Could Blockchain Have as Great an Impact as the Internet?", (Accessed Date:27.06.2021).

Kumar, P., Rana S. B., 2016. Development of modified AES algorithm for data security, Optik, 127(4), 2341-2345.

Lee Lai, R., Kuo, L.E.E., Chuen, D., 2018. Handbook of Blockchain, Digital Finance, and Inclusion; Singapore University of Social Sciences: Singapore.

Livetechit. (2021), https://www.livetechit.com/hackers-have-looted-more-bitcoin-than-satoshis-entire-stash/, (Accessed Date: 22.06.2021).

Mazzutt, R. et al., 2018. "A quantitative analysis of the impact of arbitrary blockchain content on bitcoin.", International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg.

Nadeau, M., 2018. "What is cryptojacking? How to prevent, detect, and recover from it.", CSO Online.

Newreleases, 2021. https://newreleases.io/project/github/litecoinproject/litecoin/release/v0.18.1, (Accessed Date: 10.06.2021).

Nytimes, 2021. Ethereum-bitcoin-digital, https://www.nytimes.com/2017/06/19/business/dealbook/ethereum-bitcoin-digital-currency.html, (Erişim Tarihi: 09.06.2021).

Polge, J., Robert, J., Le Traon, Y., 2021. Permissioned blockchain frameworks in the industry: A comparison, Ict. Express, 7(2), 229-233.

Saad, M., Aminollah K., and Mohaisen A., 2018, "End-to-end analysis of in-browser cryptojacking.", arXiv preprint arXiv:1809.02152, (2018).

Tandon, A., Kaur, P., Mäntymäki, M., Dhir, A., 2021. Blockchain applications in management: A bibliometric analysis and literature review, Technological Forecasting and Social Change, Volume 166, https://doi.org/10.1016/j.techfore.2021.120649.

Thenextweb, 2021. https://thenextweb.com/news/can-blockchain-democratize-education-this-startup-seems-to-think-so, (Accessed Date: 11.06.2021).

Wang, H. et al., 2018. "An overview of blockchain security analysis.", China Cyber Security Annual Conference, Springer, Singapore.

Zhang, J., Zhong, S., Wang, T., Chao, H. C., Wang, J., 2020. Blockchain-based systems and applications: a survey, Journal of Internet Technology, 21(1), 1-14.

Zhu, S., Zhu, C., and Wang, W., 2018. "A new image encryption algorithm based on chaos and secure hash SHA-256.", Entropy 20.9, (2018): 716.