International Journal of Applied Sciences and Smart Technologies

Volume 4, Issue 1, pages 1-20

p-ISSN 2655-8564, e-ISSN 2685-9432

Cryptocurrencies Advantages and Disadvantages: A Review

Zaer Qaroush[1], Shadi Zakarneh[1], and Ammar Dawabsheh[1]

[1]*M.Sc. Student, Palestine Technical University- Kadoorei*

Tulkarem, Palestine

[*]*Corresponding Author: zakarnehshadi@gmail.com*

(Received 07-04-2022; Revised 08-05-2022; Accepted 21-05-2022)

Abstract

With the rapid spread of technology in life and the necessary need to increase the speed of payment processes, confidentiality, and privacy, cryptocurrencies appeared. A cryptocurrency is a virtual and intangible currency, in which transactions are made through the internet. These currencies are characterized by decentralization, transparency, and privacy. Because transactions are carried out through a cryptography process and depend on Blockchain technology it is highly protected. Blockchain generally is a distributed ledger or a decentralized database. The Blockchain architecture combines advanced cryptography, consensus mechanisms, and a complex system of incentives. In cryptocurrency, transactions are created, transferred, and verified through an integrated process called mining. Blockchain technology architecture has given cryptocurrencies many advantages and features that increase their strength and distinction from regular financial transactions such as decentralization, confidentiality, anonymity, very low fees, unrestricted by geography, transparency, protection from Inflation, and the peer-to-peer network. The misuse of powerful features in cryptocurrencies and Blockchain technology has led to many disadvantages such as the risks of lack of knowledge, the lack of wide

Volume 4, Issue 1, pages 1-20

p-ISSN 2655-8564, e-ISSN 2685-9432

acceptance, the high risk of investment, its volatile nature, and the inability to return missing payments. This study concentrates on cryptocurrencies in terms of advantages and disadvantages.

Keywords: cryptocurrency, blockchain, mining, miners, wallet, bitcoin

1 Introduction

Since ancient times, mankind has used more than one method of payment in commercial transactions, such as barter, precious metals coins, and then paper money, which is the most widespread to this day. As a result of the development in the technology market especially the internet, the human race is still looking for new methods of payment suitable to the needs and development of technology, the most recent method is cryptocurrencies which were theoretically laid by Chaum in 1983 relying on a fundamental principle not to misuse and accelerate production [1].

A cryptocurrency is a digital asset that uses cryptography to encrypt transactions and monitor the production of additional currency units as a means of exchange. Cryptocurrencies are categorized as virtual currencies and as alternative currencies [2].

Bitcoin is considered one of the most prominent cryptocurrencies, It was founded by a group that uses the pseudonym Satoshi Nakamoto [1][2]. Numerous other cryptocurrencies have been created since then. As a fusion of bitcoin derivatives, they are often referred to as 'altcoins' which are decentralized power. The decentralized control of the distributed ledger function is related to the Bitcoin Blockchain transaction database [2].

Besides users have complete control over their own money, users can even send very small payments like the so-called Satoshi, which is equal to 0.00000001BTC [3].

Bitcoin is “designed by people for people” and The rules are imposed on everyone through one another's mutual distrust [3], it has provided solutions to the double-spending problem and Byzantine Generals Problem, these innovations made the use of cryptocurrencies possible [4].

Previously before the invention of Bitcoin, it was impossible to deal electronically without a trusted third party, for example, PayPal was used as a trusted third party [4].

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

To be sure that the same bitcoin has not been used or spent previously, the Blockchain is used to examine new transactions, it is a peer-to-peer network that carries out the verification process by distributing the work to all users In the network to utilize their computing power to reconcile and maintain the ledger in the Blockchain [4].

Solving the problem of double-spending presents another problem concerning the newly added nodes and the current nodes. As for the new nodes, how to make sure that it has the correct ledger?. As for the current nodes, the problem is how it knows that it is getting correct updates of the ledger?, this problem is known as Byzantine Generals Problem [4].

2 Literature Review

There are over a thousand cryptocurrency specifications as of October 2017; most are identical to and derived from the first centralized cryptocurrency, bitcoin, which was completely implemented. The mines are mutually suspicious parties, and maintain the protection, credibility, and balance of the ledger inside cryptocurrency systems: To verify the timestamp, computers belonging to members of the public are used, and they are later added to the ledge according to a firm time stamp. Most cryptocurrencies are designed to progressively reduce currency supply, Putting a final limit on the total amount of currency that will simulate the precious metals in circulation. For law enforcement agencies, cryptocurrencies in terms of seizing them or keeping them as cash in hand are more difficult than traditional currencies owned by financial companies. The leverage of cryptographic technology results in this difficulty [2].

In 1998 Wei Dai published an anonymous distributed electronic cash system 'b-money'. Shortly afterward, Nick Szabo " invented "bit gold. Which is an electronic currency scheme, including other cryptocurrencies that would follow it which allowed users to complete a proof of work feature with cryptographically put together and published solutions. The work of Dai and Szabo's was followed by Hal Finney, who later developed a reusable proof-of-work currency system [2].

Bitcoin was the first decentralized cryptocurrency developed by Satoshi Nakamoto in 2009. As its proof-of-work scheme, it used SHA-256, a cryptographic hash function. In

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

April 2011, Namecoin was created as an attempt to create a decentralized Domain Name Server (DNS), which would make it very difficult to censor the Internet. Litecoin has launched in October 2011. It was the first popular cryptocurrency using Script instead of SHA-256 as its hash function. The first to use a proof-of-work/proof-of-stake hybrid was Peercoin, another prominent cryptocurrency. IOTA (Distributed Ledger Technology) was the first non-blockchain-based cryptocurrency to use the Tangle instead. While few have been popular, several other cryptocurrencies have been developed, because they brought very little technological innovation [2].

A. Reasons to use Cryptocurrency

Cash payment is characterized as an easy, effective, and fast payment method, but using this method has many disadvantages, including exposure to fraud, loss of money, and costs of managing transactions with financial institutions [5].

Many reasons encourage the trend to use cryptocurrencies, among these reasons are confidentiality and security, to maintain a high degree of security and great confidentiality, cryptocurrencies use encryption methods that use public keys and private keys in transactions and payments, as well as the cryptocurrency transactions carried out easily and quickly. Also due to cost, payment, and money transfer operations are done at the lowest possible cost, as there are no banks or intermediary monetary institutions to transfer funds between the parties [5].

B. Blockchain

Simply the cryptocurrency consist of a public and distributed ledger (distributed database) referred to as Blockchain, which users can use to record their transactions. Blockchain technology is designed to manage cryptocurrencies [6].

Blockchain is a decentralized solution for managing data and transactions. Through this solution, the data is shared and recorded in multiple data stores called a distributed ledger. They are controlled by a network of distributed servers called nodes [7].

In Blockchain, data can only be added and cannot be deleted, the data is in the form of a series of transaction blocks. To protect data and transactions, an encryption method called cryptography is used, and to create data and verify the continuous growth in the data structure, specific mathematical algorithms are used to achieve this [7].

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

Depending on the practical application of the Blockchain, it is divided into two main types:

1- Permissionless Blockchain: there is no central authority to control users or to control joining or preventing anyone from joining the network. a person only needs a computer with the necessary software installed on it and thus he can join and perform the transactions he wants and store them in the decentralized ledger, an identical copy of the ledgers is distributed to all nodes in the network [7].

2- Permissioned Blockchain: for a person to join the network, approval must be made by the network validators based on specific parameters and rules that are determined by the network administrator, who defines validators and rules. The permissioned Blockchain is divided into two subcategories, (a) Private permissioned Blockchain which restricts access on the network to an administrator to update the ledger, and creates, and stores transactions. Also known as enterprise permissioned Blockchain. (b) Public permissioned Blockchain where the network can be accessed and viewed by anyone [7].

C. How the Blockchain works

Blockchain can be likened to a distributed database. Any node of the network nodes (network members) starts in addition to this database when it creates a data block, then the created data block is broadcasted in encrypted form to all network members, and the other network nodes determine the validity of the data based on the predefined validation algorithm, this method called “consensus mechanism”. After the block validation is completed, the blocks are added to the Blockchain, and then the distributed transaction ledger will be updated [8]. See Figure 1.

International Journal of Applied Sciences and Smart Technologies

Volume 4, Issue 1, pages 1-20

p-ISSN 2655-8564, e-ISSN 2685-9432

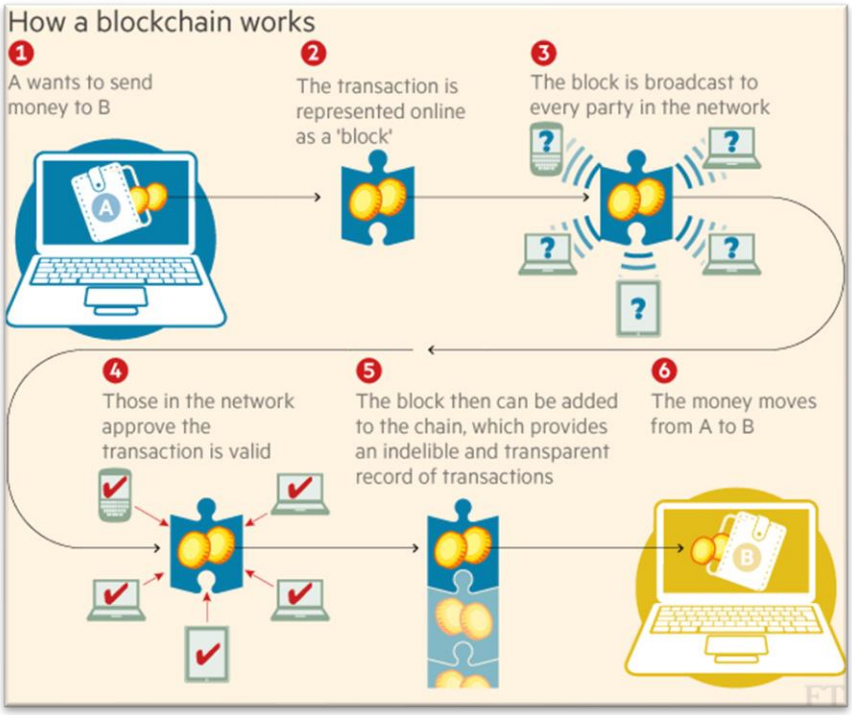

Figure 1. How Blockchain Works [8]

The Blockchain network member has two keys for his transactions public and private keys. The public key will be known to all network members and used as an address on the Blockchain and to validate the sender's identity by verifying the digital signature. The private key is used to create the transaction digital signature. These keys are kept in a digital wallet online or offline [8].

D. Blockchain consensus mechanisms

As the process of validating the added data block is done by a group of Blockchain network nodes in a decentralized manner to ensure its legitimacy, there must be an agreement between the nodes on the method of validation, this is known as the consensus mechanism, which is a predefined encrypted method within certain parameters. It ensures the correct sequence of transactions in the Blockchain. As an example of this in the case of cryptocurrencies, these mechanisms include preventing the problem of double payment [9]. The Blockchain uses a certain consensus

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

mechanism based on the resources required and the expected results. Different types of consensus mechanisms used in Blockchain technology are as follows:

1- Proof of Work (PoW): it is known as mining and the network nodes are the miners. This process needs large-scale computing power to enable miners to solve complex mathematical puzzles. Many cryptocurrencies like bitcoin used this mechanism [10].
2- Proof of Stack (PoS): In this mechanism, who has the priority to produce the next block is determined, this is done through a random process. For the user to be able to produce blocks, he must become a validator, and this is done in several ways, either after the user has locked his token for a certain period, or the validator is chosen based on the Blockchain design. Another way for the user to be a validator is by keeping the coins for the largest time or owning the biggest stack gives a greater opportunity for the user to become a validator. Proof of stack is considered to be more energy efficient than other mechanisms [10].
3- Delegated Proof of Stack (DPoS): In this mechanism, delegates are chosen based on a vote from the users, where the user can share his coins and vote for a specific number of delegates, as the user's share of the coins affects the user's voting weight, more user stack mean larger vote weight. The delegate who gets the most votes has the opportunity to produce new blocks. The delegate rewards are like other Blockchain consensus mechanisms. This mechanism is one of the fastest Blockchain consensus mechanisms [10].
4- Proof of Capacity (PoC): In this mechanism, digital stores are used to store mathematical puzzle solutions. In this mechanism, users who are faster to find solutions get a chance to create a new block. This process is called plotting. In this mechanism, users with higher storage capacity have more chances to produce new blocks [11].
5- Proof of Authority: This mechanism is a modified version of the proof of stack mechanism. In this mechanism, the identities of the validators in the network are on the stack. In this mechanism, the identity is used as a correspondence between the personal identity of the validators and their official documents, to verify their identity. In the mechanism of establishing authority, the nodes that become

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

validators are the only nodes that are authorized to produce new blocks. To secure and protect the Blockchain network, validators whose identity is at stack are incentivized [11].

6- Proof of Activity: This mechanism is a mixture of the Proof of Work mechanism and the Proof of stack mechanism. This mechanism relied on miners and auditors. In this mechanism, the blocks that are generated are simple blocks that contain the mining reward address and header information. Header information is used to define a random group of validators for block signature, in which case the validators with the highest stacks are the ones selected to sign the new block. The miners try to solve the puzzle and claim their reward. When the designated validators sign on, the new block becomes part of the network. The block must be signed by all validators in order not to be ignored. In this mechanism, the network fees generated by the process are distributed between the winning miner and the validators [11].

E. Mining

Mining is an integrated process in which cryptocurrency transactions are created, transmitted, and verified. Ensures a stable, safe, and secure prevalence of currency from payer to recipient. Cryptocurrencies are decentralized and work on a peer-to-peer system, and they are unlike fiat currencies that are controlled and regulated by the central authority. Banks need a huge infrastructure to generate currency and monitor transactions. But the cryptocurrency that uses the mining system overcomes this need, as it is the responsibility of miners or nodes to verify and monitor transactions [12].

When a transaction is made, details of the transaction are broadcast to all network nodes. To form a block the transactions that take place during a specific period are summarized. The system is designed to merge transparency into it, whereby all transactions made are maintained and recorded in blockchain [12].

Miners play a major role in mining, as they verify the property of currency from source to destination. Each transaction contains a previous retail transaction that was performed by and through the owner. The current position is tested for validity and thus

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

validated. Miners prevent double-spending on currency through the verification process [20].

The main objective of mining is to create and issue currencies in the currency economy. After making and verifying the transactions, it is the role of the miners to collect these transactions and include them in the blocks that they are currently solving. Before the blocks are broadcast, they must be resolved and then placed in the blockchain. Solving blocks includes difficult mathematical puzzles to crack and unlock. Miner is allowed to add the block to the ledger only when solving a math puzzle, and as a result, they are awarded a reward [13].

F. Mining Requirements

Cryptocurrencies are mined using special machines for this purpose called a "Mining machine". Mining history starts from the CPU to the currently widely used ASICs. New machines with better efficiency than previously designed machines have been developed as a result of the cyclical growth of mining difficulty [12].

1- During the beginning of mining, the CPU was used efficiently with hash rates lower than or equal to 10 Mbps to mine cryptocurrencies. To deal with mining previously, having a computer with the necessary software installed on it was sufficient. But because of the increasing difficulty of mining, the use of CPUs became insufficient because the hash rates became high and thus we need advanced mining machines. cpuminer was one of the popular CPU mining software [12].

2- Since the CPU mining power did not meet the increasing requirements, the CPU was used with graphic cards for coin mining. Graphics cards contain GPUs, which are used to solve complex polygons and high mathematical functions used in games. Different hash-based algorithms are used by different cryptocurrencies to solve blocks of transactions that require high math; Therefore GPUs are considered an alternative to CPU Mining [12].

   Expanding the hash rate of cryptocurrency through GPUs is the goal of pushing the boundaries of consumer computing in amazing new ways. Despite the benefits of GPU, there are some Limitations:

   - GPUs are more expensive compared to normal CPUs [12].

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

- Each GPU must be connected to a PCI-E 16x or 8x slot, of these, are relatively few on commercial motherboards [12].
- Failure to use all components such as RAM, motherboard, and hard disk in GPU mining leads to an increase in the mining cost [12].
- GPUs require a high additional power of 200-300 watts to mine effectively [12].
- Because GPU takes two slots in a motherboard, it became difficult to connect more than one GPU to a computer to get better performance [12].

3- FPGA (Field Programmable Gate Array): It has the feature to configure after manufacturing because it contains CLB, which is Configurable logical blocks that contain the property of reconfiguring, and also contains RAM and logic gates. Its power consumption is a fifth less than GPUs. It is also good at hash-based algorithms like SHA256 used in Bitcoin transactions [12].

4- ASIC (Application Specific Integrated Circuit): Bitcoin ASICs designed specifically for Bitcoin mining is effective in complex mining mathematical tasks, with high speed and efficiency [12].

G. Wallets

An electronic wallet is a type of electronic card and is used for transactions over the Internet using computers or smartphones. Its utility is the same as a debit or credit card. Cashless transaction technology has seen growth in the past year [15].

To help move away from the monetary economy e-wallets are being used. As a result of all transactions in the economy being calculated in this process, the size of the parallel economy decreases. Widespread in rural areas after the spread in urban areas of the mobile phone wallet. Hence, Wallet Funds see a very bright future very soon. In this section, we will try to study the types of electronic wallets and how to use them and talk about bitcoin as an example [14].

To pay the money the wallets collect private keys to access their Bitcoin address. They appear in various forms, especially for special types of devices. And to avoid

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

placing it on the computer, paper storage can be used. It is important to have a backup copy of your Bitcoin wallet and to secure it [14].

Bitcoin has become a new way of cash, and it is starting to find acceptance among merchants as a method of payment. The mechanism of transactions and the method of creating them became known, and it remained to be known how they were stored? The money is stored in a physical wallet, and Bitcoin is stored in a wallet, but it is a digital wallet [15].

To be precise, Bitcoin is not stored anywhere. Rather, it is the protected digital keys used to access public Bitcoin addresses and sign transactions [15].

There are five main types of wallets [14]:

1. Desktop wallets

   To run a wallet you need to install the original Bitcoin Core client, and you might not even know it. This program allows you to create a Bitcoin address to obtain and transfer virtual currency, collect the private key for that as well as migrate transactions to the network. MultiBit operates on Linux, Mac OSX, and Windows. Hive is an OS X-based wallet with some features, one of which is an app store that has direct contact with bitcoin services. Some desktop wallets are specified to enhance security: Armory falls into this group. DarkWallet - It uses a lightweight browser add-on to deliver services including currency mixing where users' currencies are exchanged for others, to prevent citizens from being tracked [14].

2. Online wallets

   Web-based wallets store private keys on a computer connected to the Internet and access to it is restricted by the user. Due to the availability of these services through the Internet, and their connection to a computer and mobile phone wallets, which causes duplicate addresses between the devices used by you [15].

   - Advantages

   - The time required to complete a transaction is short [16].
   - Storing a small amount of cryptocurrency is recommended [16].

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

- Some digital wallets are used to store and transfer many different cryptocurrencies between them [16].
- TOR network is used for more privacy [16].

- Disadvantages

- There is a third party that fully controls the digital wallet [16].
- When using a digital wallet it is recommended to use a personal computer and it is important to install security software [16].
- Various online fraud operations are a result of a lack of knowledge in information technologies, which exposes users to various frauds [16].

3. Mobile wallets

Using a special application on your smartphone, the wallet can save your private keys to Bitcoin addresses, and thus you can pay directly using the mobile phone. Bitcoin wallet can take advantage of near field communication (NFC), letting you tap a mobile phone versus a reader and pay with Bitcoin without ever having to provide any information [15].

- Advantages

- More useful and easier to use than other types of cryptocurrency wallets [16].
- The possibility of using the TOR network for more privacy [16].
- Provide using a QR code to scan [16].

- Disadvantages

- Because mobiles are not secure devices. The loss of the user's private encryption codes may happen in case the user's mobile was hacked [16].
- Mobile wallets are vulnerable to malware and viruses [16].

4. Hardware wallets

It is in the form of a USB device with a program, and some of it contains a screen, so the user does not need a computer to complete the transaction See Figure 2. It provides user control over the cryptocurrency with the ability to store digital assets for a long time [15].

Volume 4, Issue 1, pages 1-20

p-ISSN 2655-8564, e-ISSN 2685-9432

- Advantages
  - A USB wallet with a display screen is the most secure [16].
  - More secure than other wallets [16].
- Disadvantages
  - Too difficult to buy [15].
  - There are risks of use for beginners so it is not recommended for them [16].

Figure 2. Hardware Wallet [17]

5. Paper wallets

One of the cheapest and most impressive options for keeping your Bitcoins safe is seen in Figure 3. Many websites offer paper Bitcoin wallet services. They will create your Bitcoin address with an image containing the two QR codes: one for the public address which use to receive bitcoins; and the other for the private key, which use to pay the Bitcoins stored at this address. In a paper wallet, private keys are not stored digitally on a computer or mobile device and therefore are not subject to electronic attacks or the risk of hardware failure or loss [15].

- Advantages
  - It is kept in the user's wallet or pocket, and there is no need for a computer connection [16].
- Disadvantages
  - Need more time to complete the transaction [16].

International Journal of Applied Sciences and Smart Technologies

Volume 4, Issue 1, pages 1-20

p-ISSN 2655-8564, e-ISSN 2685-9432

Figure 3. paper wallet [18]

3 Results and Discussion

Based on previous studies and literature reviews, Blockchain is a decentralized database, each member of the network maintains a complete, synchronized, and verified copy of the database that contains all transactions. The Blockchain architecture combines advanced cryptography, distributed consensus mechanisms, and a complex system of incentives and rewards. Blockchain architecture makes it have a group of characteristics including the inability to alter transactions or fraud, and it does not require any trust in the integrity of the participants but it ensures absolute credibility in the system, it is outside of censorship. If two participants want to conduct a transaction between them, it cannot be prevented, and because of the short settlement time, which is close to zero, the speed of the final settlement and its verification leads to faster capital and increased liquidity.

The cryptocurrency is a virtual currency that exists only in electronic form on the Internet. The cryptocurrency was introduced as a digital currency for financial exchange independently of banks or financial institutions. Whereas Blockchain is the technology that underlies cryptocurrencies to conduct, secure, verify, and store transactions, these currencies gain many advantages because of their characteristics of Blockchain.

As the ledger database is distributed over the network, each member of the network has a complete copy of the ledger database. Whereas, the miners are the members of the network where the process of verifying transactions is carried out by miners. Therefore, there is no central authority to control the network and the transactions that take place on it or to individually control the database. This is what distinguishes cryptocurrencies as being decentralized. With the advantage of decentralization, the transaction cannot be prevented or controlled. Therefore, since the user has a cryptocurrency wallet, he can

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

perform any number of transactions and transfers at any time and anywhere without restrictions. Thus, the cryptocurrency has unlimited transactions.

In conducting transactions in cryptocurrencies, there are no high fees. As in the case of purchase, there are very low fees for the crypto process and mining operations. Here, fees in mining operations do not go to a central authority but are distributed to the miners who have verified the reliability and validity of the transaction, and these small fees are exposed to one party of the transaction, which is the buyer. In contrast to banks that impose multiple types of fees for transactions, currency transfers, accounts, and database management. This makes cryptocurrency operations significantly lower in fees and costs compared to banks. Also As a result of the short time of mining operations and the absence of a central authority such as banks to control the transaction and make approvals, this makes the transaction progress very fast, which distinguishes the cryptocurrency by the short time in its transactions.

Since cryptocurrencies are virtual currencies and their transactions take place over the Internet, and because transactions in them are not subject to the control of a central authority, it became possible to conduct transactions between countries and outside borders without any hassles or restrictions. This is what makes cryptocurrency a cross-border currency.

Blockchain stores cryptocurrency transactions in blocks that are recorded in the distributed ledger. In cryptocurrency, each user has a crypto address, and the user can specify whether the crypto address is public or not. If the user sets their crypto address public, then other users will be able to see how much crypto is for that user. If the address is not public, then no one can know the amount of crypto for the user. This adds a transparency advantage to cryptocurrencies.

In cryptocurrencies, the user can create his wallet or any number of wallets without referring to his name, address, or any other real information. This makes anonymity another feature of the cryptocurrency to maintain and protect privacy.

By using the cryptography process, no person can perform any payment transaction from the wallet except by the owner. Cryptocurrencies use cryptography and the use of public and private keys to achieve a high level of security.

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

In cryptocurrencies, transactions are carried out by a large number of distributed servers, which may be in the hundreds or more. As the cryptocurrency has no main server to control and manage transactions. The wallet software installed on users' computers in the network is part of the network. The process of exchanging transactions and payments between two or more members of the cryptocurrency network who are installed the wallet software is done directly so that neither banks nor governments can control the exchange of money in them. Thus cryptocurrency networks form a peer-to-peer network.

Since cryptocurrencies do not follow a central authority nor are they controlled by companies or governments. Cryptocurrencies are limited to use and mining, therefore there is no possibility for any party or authority to change the system or develop inflation in the system.

Accompanied by more and more expansion in the use of technology that adds to the world a lot of advantages and disadvantages that depend on how the technology is used and the purpose of its use. In addition, the use of cryptocurrencies is also expanding as the advantages of their use are accompanied by many disadvantages that depend on some of their characteristics, how they are used, and the goal of their use.

While Blockchain-based cryptocurrency technology is somewhat complex, the user needs to know about it and learn it well before starting to invest in it. The lack of knowledge about it exposes the user to the risks of hackers.

Since cryptocurrencies are still not accepted by many countries, as well as not being accepted until now in many online buying and selling sites. This makes it impractical to use it for everyday buying and selling, making it not widely accepted.

Although the cryptography and anonymity features in cryptocurrencies are considered two of its strong advantages, this gave the possibility to use it in financing illegal business and prohibited activities. In addition to the lack of a central authority to issue and supervise it, there is no legal guarantee in the event of bankruptcy. Thus, there is a high risk of investing in cryptocurrencies. As well as the volatile nature of cryptocurrencies, which increased the fear of people and companies from investing in them. As large volatilities, increase the risk of investing in the cryptocurrency.

Volume 4, Issue 1, pages 1-20
p-ISSN 2655-8564, e-ISSN 2685-9432

In cryptocurrencies, the possibility of recovery is not available, as it is not possible to recover any wrong payment without the consent of the other party only. This increases the risks of using cryptocurrencies and requires more caution and attention before conducting any transaction.

As a result of the characteristics of cryptocurrencies and the features of Blockchain technology, which is the technology on which the cryptocurrency is based, there are many advantages and disadvantages of cryptocurrencies as shown in Table 1.

Table 1. Cryptocurrency advantages and disadvantages

No.	Advantages	Disadvantages
1.	Decentralization	Lack of Knowledge
2.	Unlimited number of transactions	Not widely accepted
3.	Transactions low fees	High risk in investment in cryptocurrency
4.	Fast transaction	Strong Volatility nature
5.	Cross-border currency	Missing payment cannot be recovered
6.	Transparency	
7.	Anonymity and privacy	
8.	High security	
9.	Peer-to-peer network	
10.	No inflation	

4 Conclusion

Cryptocurrency is a virtual currency that depends on cryptography to achieve confidentiality, secrecy, privacy, speed, and low cost of transactions. Blockchain is the cryptocurrency underlying technology. Blockchain technology provides the cryptocurrency with all the abilities to achieve the decentralization mechanism. The Blockchain architecture combines advanced cryptography, distributed consensus mechanisms, and a complex system of incentives and rewards. Cryptocurrency comes to

solve the traditional currency problems to avoid the loss of time, effort, fraud, loss of physical money, and high fees in banking transactions. Cryptocurrencies with their underlying technology (Blockchain) have several advantages and features that increase their strength and distinction from regular currencies and regular financial transactions such as decentralization, high confidentiality, anonymity, speed of transactions, very low fees, unlimited number of transactions, unrestricted by geography and borders, transparency, protection from Inflation, and the peer-to-peer network. While there are these advantages to cryptocurrencies, they have many disadvantages such as the risks of lack of knowledge, the lack of wide acceptance, the high risk of investing in them, their volatile nature, and the inability to return missing payments. It is possible to overcome these disadvantages by raising awareness and training on the use of these currencies on the one hand, and on the other hand, creating regulations and laws that regulate their work and investing in them, which reduces risks, helps spread, and reduces the misuse of their potentials.

References

[1] M. Vejačka, "Basic Aspects of Cryptocurrencies," *Journal of Economy, Business and Financing*, **2**(2), 75-83, 2014.

[2] A. Okhuese, "INTRODUCING CRYPTOCURRENCY," Schemas Group, 11-12, 2016.

[3] C. Rose, "The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution," *International Business & Economics Research Journal*, **14**(4), 617-621, August 2015.

[4] E. D. a. J. Brito, "The New Palgrave Dictionary of Economics," *New Palgrave Dict. Econ.*, March 2020.

[5] M. Badar, S. Shamsi and J. Ahmed, "Blockchain: Concept and Emergence," in *Blockchain Applications for Secure IoT Frameworks: Technologies shaping the future*, Bentham Science, 19, 2020.

[6] B. Scott, "How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?," in *Social and Solidarity Finance: Tensions, Opportunities and Transformative Potential"*, 2016.

[7] P. Mulgund, A. Sharma, A. Srivastava and L. Agrawal, "Beyond Cryptocurrency - More To Blockchain," *Cutter Business Technology Journal*, **32**(11), 8, 2019.

[8] J. Wild, M. Arnold and P. Stafford, "Technology: Banks seek the key to blockchain," Financial Times, November 2015. [Online] Available: https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe 567b37f80b64?segid=0100320#axzz3qK4rCVQP. [Accessed: 04 December 2020].

[9] R. Houben and A. Snyers, *Cryptocurrencies and blockchain*, European Parliament, 103, 2018

[10] A. Nick and L. Hoenig, "Consensus Mechanisms in Blockchain Technology," Lexology, [Online]. Available: https://www.lexology.com/library/detail.aspx?g=e30e7d54-3c7f-4ca0-8a22-478227a9b5ec. [Accessed 02 December 2020].

[11] N. JOSHI, "8 blockchain consensus mechanisms you should know about," Allerin, 23 April 2019. [Online]. Available: https://www.allerin.com/blog/8-blockchain-consensus-mechanisms-you-should-know-about. [Accessed 04 December 2020].

[12] H. Krishnan, S. Saketh and V. Vaibhav, "Cryptocurrency Mining – Transition to Cloud," *International Journal of Advanced Computer Science and Applications (IJACSA)*, **6**(9), 115-124, 2015.

[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[14] B. Pachpande and A. Kamble, "Study of E-wallet Awareness and its Usage in Mumbai," *Journal of Commerce & Management Thought*, **9**(1), 33-45, 2018.

[15] P. Ankalkoti and S. S G, "A Relative Study on Bitcoin Mining," *Imperial Journal of Interdisciplinary Research (IJIR)*, **3**(5), 1757-1761, 2017.

[16] S. Jokić, A. Cvetković, S. Adamović, N. Ristić and P. Spalević, "Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets," *Ekonomika*, **65**(3), 65-75, September 2017.

[17] S. Singh, April 2018. [Online]. Available: https://cryptocurrencynews.com/best-hardware-wallets/.

Volume 4, Issue 1, pages 1-20

p-ISSN 2655-8564, e-ISSN 2685-9432

[18] 30 May 2018. [Online]. Available: https://www.universidadedobitcoin.com.br/o-lancamento-da-paper-wallet-da-cardano-vem-com-recurso-de-armazenamento-offline.

[19] A. Rosic, "Blockchain Consensus: A Simple Explanation Anyone Can Understand," Blockgeeks, [Online]. Available: https://blockgeeks.com/guides/blockchain-consensus/#What_is_the_Byzantine_Generals_Problem. [Accessed 01 December 2020].

[20] Brito, J. & Castillo, A. Bitcoin: A Primer for Policymakers. 2013.