A Survey on Blockchain and Cryptocurrency based Systems

Atharva Deshmukh[1], Hariket Sukesh Kumar[2], Pratap Pawar[3], Amit Kumar Tyagi[4][0000-0003-2657-8700]
[1] Department of Computer Engineering, Terna Engineering College, Mumbai
[2]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India.
[4]Department of Fashion Technology, National Institute of Fashion Technology, New Delhi, Delhi India
atharva1525@gmail.com, shethhariket@gmail.com, iampratappawar@gmail.com, amitkrtyagi025@gmail.com

Abstract - With the increasing pace of life, more and more people are getting interested in various projects, facilities, services and gadgets. One of the most popular and in trend system in the world right now is the blockchain and cryptocurrency system. Every person who has technology at his service is interested in blockchain. They provide with an interesting medium of transaction as it does not have a single powerful source. Cryptocurrencies have made a name for themselves as essential financial software platforms. It is based on a dataset from a decentralised information ledger, with mining playing a crucial role. Through mining, past transaction data is added to the Chain, or decentralized ledger, allowing users to securely agree on each action. Block chain has existed since Santoshi Nakamoto attempted to use it as a restricted ledger for bitcoin, a most popular and successful cryptocurrency, in 2008. It must not be equated to other technology, such as the internet. Blockchain is proud of the fact that it gives its users with a high level of pleasure and a strong sense of trust. There seem to be substantial blockchain deployments in numerous areas of a country, including education ventures, supply chain management systems, and agriculture ventures. Blockchain technology has completely changed the field of cryptocurrency. This paper will explore on the topics such as security in blockchain activities in cryptocurrency, fraudulent activities possible in blockchains, cyberattacks, etc. This paper seeks to identify the threats to blockchain technology in cryptocurrency and find countermeasures to overcome those threats. Top cited articles would be reviewed in this paper accompanied by detailed analysis a to come up on a conclusion. In this paper, strengths and threats of cryptocurrency and their emergence in the internet-connected financial payments in the futuristic economic world will be discussed.

Keywords: Blockchain, Distributed Ledger Systems, Cryptocurrency, Smart Era.

1. Introduction

Blockchain technology is attracting the attention of people and government organisations across the world. It has the ability to significantly modify how citizen records are maintained, enabling improved information management and quicker data exchange, much like a shared ledger that is absolutely safe and available as more than simply many clones continuously altered in real time. Above all, that innovation, by allowing certification of specific acts or conformity to formal standards without such engagement of a centrally controlled admin or an external independent party [1], foretells the Government's and government workers' inevitable exit from the area. Cryptocurrencies like Bitcoin, that are non-fiat, unregulated online payment systems work outside of the traditional finance industry, are also having an impact on the shifting landscape. Despite the reality that Bitcoin was designed as a payment system and a form of asset storage, it is unlikely that banking system currencies would be replaced given the volatility of Bitcoin's market price. The rigidity of the proof-of-work-based, fixed Bitcoin supply schedule is what causes the instability. The blockchain, on which Bitcoin's fundamental protocol is based, symbolises a development capable of transforming investment instruments and arousing existing financial, public, and safety regulations and policies, despite the fact that Bitcoin has drawn a lot of attention for its position in illicit behaviour such as financing terrorism, money laundering, the trafficking of firearms, tax avoidance, and digital ransomware. [2].

The rise of misunderstanding about the use of technology, the benefits and challenges it presents, has coincided with the new wave of blockchain and cryptocurrency systems. There is a lot of speculation regarding which coin or system will succeed. Due to its varied functions that are applicable worldwide, this has an impact not only on the business sector, but also on the rest of the globe. These modern technologies pose a threat to well-established business structures, eliciting a great deal of criticism, concern, and a sense of being in unfamiliar territory [3]. Enthusiasts also have a tendency to exaggerate this information, focusing on short-term goals and situations in order to inflate the value of the blockchain and cryptocurrency systems. Overestimating short-term rewards while underestimating long-term benefits is a common problem. They fail to consider market demand, existing frictions, and the societal consequences. Border control, government identity, insurance, shipping, real estate, advertising, waste management, energy, tourism, and a variety of other challenges can all be solved using

blockchain technology. It is made up of numerous algorithms that are kept in the ledger and are used to detect faults. This even identifies the block in which the problem occurred. Several nations, namely Estonia, has experimented with blockchain in a range of fields and therefore have discovered positive outcomes that have aided its development [4]. Other important feature is anytime an issue arises, it leaves behind a footprint, that decreases the work required to locate the block where the problem happened. As a result of this aspect, the process becomes decentralised. Cryptocurrencies based on blockchains are becoming a new form of money in the last few years. Instead of depending on centralized authorities like the bank to manage money, cryptocurrencies depend on mathematical design and complex cryptographic protocols. Since most cryptocurrencies are fully decentralized, no individual or organization can keep track of or prevent the transfer of funds. Cryptocurrencies grew from just being an idea and model to being a worldwide prodigy with millions of individuals and organizations investing in them [5].

Bitcoin, the first cryptocurrency, became popular because it was being controlled by a decentralized network and can avoid double-spending. Currently, Bitcoin is the leading cryptocurrency having 51% (as of June 2021) of total market share among 5000 altcoins. Blockchain is like a linked list as it doesn't keep data in a huge continuous ledger, but splits the data into nodes known as blocks. Each block contains several elements which contain the block header and its transactions [6]. The transactions in a block account for almost all of the data, while the block header contains a timestamp, hash of the previous block, Merkle root hash, and other such essential metadata. What makes blockchain different from a linked list is that in a blockchain the hash of the previous block, also known as a reference, is cryptographically enciphered hence tamper-evident, and new data can only be added in the form of new blocks which will be linked with previous blocks of data [7]. The main technology behind Cryptocurrency is Blockchain, a shared and immutable ledger. The key elements of blockchain include hashing for security and immutability, peer-to-peer (P2P) networks for transaction verification, data structures for storing and managing the transactions, smart contracts for corporate bond transfers, consensus protocols for decentralization and avoiding double-spending issues [8]. and incentive mechanisms for secure transactions. But cryptocurrencies still being in their early stages, create a lack of trust among many stakeholders.

The most common misbelief about cryptocurrencies is that are anonymous. Most cryptocurrencies are pseudonymous, which means that the real identities of people are represented by addresses, so the two can be connected through data analysis. But some cryptocurrencies follow certain approaches for making it difficult to trace the transactions and link addresses on the blockchain to real-world identities or follow more advanced concepts, which allows transactions to be completely private even on public blockchains [9].

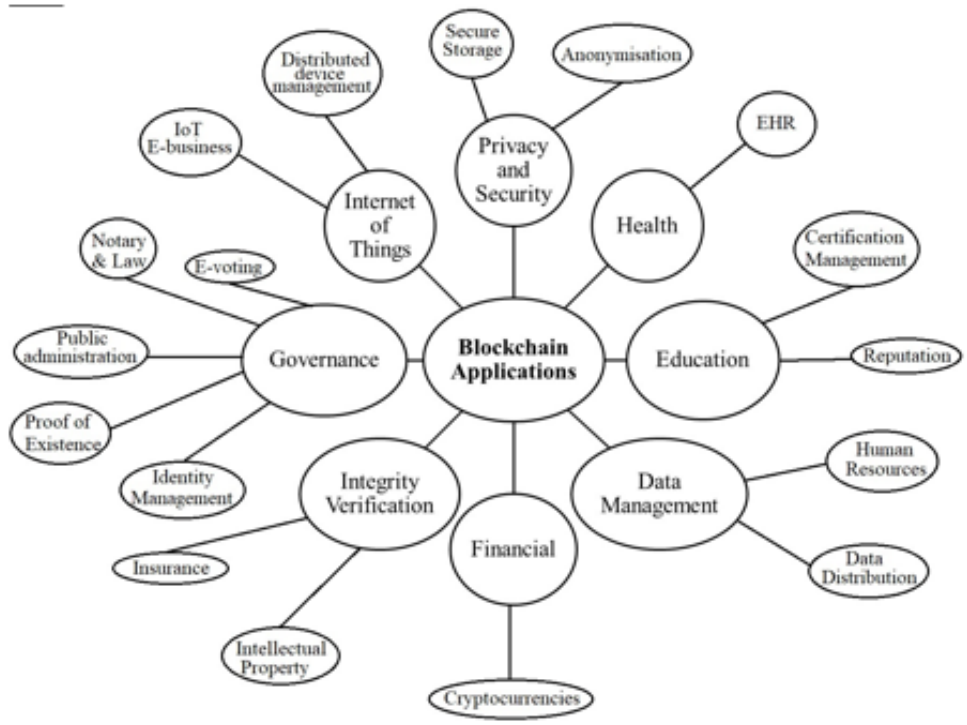

Figure 1: Applications of blockchain technology in various sectors.

Figure 1 depicts the applications of blockchain technology in various sectors. Blockchain technology is one of the many recent revolutions in the tech sector. It is considered to be the new way of living in the near future. With its applications in most walks of life, it is seen as a revolution to the old methods. The history of blockchain technology goes way back in 1991. It was first defined by two researchers, namely, Stuart Haber and W. Scott Stornetta who desired to make a system where blocks of information could be stored along with their timestamp which could not be manipulated. But it was nearly after two decades that this technology gained popularity. Blockchain technology found its first use in cryptocurrency in 2009. This was the year when blockchain technology was seen to have its first real-life application. In 2009, the cryptocurrency, 'Bitcoin', was invented which proved to be a revelation [10]. After that, many more cryptocurrencies were introduced and is believed that it may be the next method for money related transactions. In IoT it is used in security purposes, trusted exchanges, etc. While in healthcare blockchain technology finds its use in security and data sharing solution. In public services it is used in e-voting, propriety registration, and so on. In finance, blockchain technology is seen to have its use in running digital currencies i.e., the cryptocurrency. Bitcoin, Ethereum [11].

As an organization of this work, this article discusses security and how to address it by implementing blockchain technology. The majority of blockchain security applications are seen in critical information systems, such as financial databases. In this paper, we have discussed about Merits and Demerits of using Blockchain in section 2. In the next section 3, we discuss about the implementation of Blockchain in different sectors like education, healthcare, etc. Then in section 4, we discuss about cryptocurrency systems. We also discuss Consensus Algorithms in blockchain technology in section 5. Then in next section 6, we discuss about different crypto assets in detail. In section 7, we also discuss about threats to Cryptocurrency and Blockchain. Section 8 includes few countermeasures for these mitigated threats. This paper covers the explanation of link between blockchain and cryptocurrency in section 9. Section 10 explains future work for future researchers. In the last, section 11 concludes this work in brief.

2. Merits and Demerits of using Blockchain

Let's take a look at some of the Merits and Demerits of blockchain technology in today's applications.

2.1 Advantages of using Blockchain

Cryptocurrencies, the digital currency or the virtual currency, demand is being increasing over a decade without the effect of inflation is the best advantage for the investors to bring their money into the world of digital currency without having the fear of inflation due to National government rules and regulations and international disputes. This design of cryptocurrencies to have a limited number of coins for a particular cryptocurrency has fulfilled to remain strong for any international crises or inflation of country currencies. Investors in stock market also need to change their investments form one stock to [12] another or one market to another based upon the decisions of government bodies which are can't be predicted by a common man as better as big investors. One example which says that the cryptocurrencies stayed strong is the situation when whole world is under pandemic due to COVID-19, Cryptocurrencies didn't comprise to affect its value even there is a decrease in the investments in the stock market or an increase in the value of ornaments like gold due to heavy investments in the commodities. It is due to the advantage of digital currency by not restricting itself to some Government bodies or having abundant coins for a particular Cryptocurrency so that the value can be decreased as wanted [13]. Due to these advantages and much more investments in of the Cryptocurrencies with high returns can bring a lot of attention of other small and big investors to invest and thus by increasing the value by increasing the demand of Cryptocurrencies

2.1.1 Protection from Payment Fraud

The best way used by the fraudsters in this digital system is by paying the same coin to two different people by giving two different transaction recipients and this cause of fraud online transaction can easily be found in today's banking system. When it comes to digital currency, the system used here to note the transactions is block Chain technology where a block is to be implemented in the chain of blocks where the details of transaction is noted which is accessible to many users without revealing the confidential information of both buyer as well as seller and not encouraging any fraudster to make double payments for the same coin [14]. Block Chain technology is considered as one of the highest security technologies available and Bitcoin (one of the Cryptocurrency) is the first to use this technology after it was outlined. However, other studies claim that if fraudsters have a significant stake in the proof of work hash power, they can take over the block chain's security mechanism. Hash power is a term used to describe the capacity to manage computing power. A typical burn-through force of 10 minutes includes the hash power. By retaining a higher percentage of the interest in the verification of labour, fraudsters can double spending on a comparable square by silently setting up the block chain branches in advance before alerting the chain organisation. Theoretically, big scale extortion should be possible if fraudsters can control a

certain level of hash power. The Bit coin's factorial arbitrary walk calculation states that a fraudster may spend twice as much if they have control of 51% of the processing power. In this analysis, it was found that the hash strength, rather than the potential for many fake identities, is all that triple transaction verification depends on. By validating alternate tactics rather than depending solely on hash power, this has made sure that the problem of fraudsters being able to control a bigger amount of the hash rate is undermined. The assumption is that controlling the majority's personality is far harder than controlling the majority's hash power. Using digital currency to make payments is more easy and secure than doing it with credit cards.

Cryptographic money has a lot of reduced handling charges with the secured exchange it provides [15], despite the fact that it is still understudied. The validation of customers and dealers is an important part of moving digital money. Fraudsters will be unable to create a new trade or postpone any discount exchange due to the verification between the two players. In contrast to MasterCard, this manufacturing has existed and will continue to exist as a result of its component. The cardholder, trader, vendor bank, Visa organisation, giving bank, and specialised co-op are all involved in the Visa exchange innovation. The conversation is more complicated than it appears in any single exchange. Before an exchange can be completed, it must first go through this load of components. In any of these steps, fraudsters and opportunities for supplying false information might arise. Despite the fact that specific precautions have been made to reduce MasterCard fraud, the architecture is less robust when compared to block chain. The framework used by charge card innovation is still not as secure as the encryption used by digital currency innovation [16]. The intricacy just exists in the hub and numerical riddle that will be addressed by the mining system. Other than that, the block chain innovation gives helpful capacities to all clients. It is probably not going to go before to tumultuous framework predicated on irreversibility and flexibility. The archives of advanced archives on the web and ID are very much safeguarded inside the block chain framework for the present and the not-so-distant future.

2.1.2 Potential for high returns

Cryptocurrencies are being a unique asset for the investors due to its features and ability to provide more returns to its investors. Bitcoin, being the first digital currency facilitated about 1000-10000 percentage of profit to its investors from what they have invested during its early days of introduction. Due to extra feature of Bitcoin generation becoming halve of its usual generation when more transactions occur and limited amount of Bitcoin i.e., 21 million coins and also the belief of people that it would be the future currency, people began to invest in it to gain the high returns in the future [17]. The utilization of cryptographic money is basically similar to the utilization of fiat cash or by utilizing Mastercard’s in buying genuine products from retailers. Aside from that, Bitcoin can be utilized for more extensive purposes.

2.1.3 Fast and Inexpensive

Sending any amount of money only takes a few seconds. Regardless of the total or the goal. The cost is either negligible or non-existent when done in bitcoins. Any nation in the world may send bitcoins abroad. Bitcoin has no geographical limitations, much like the Internet and email [18]. This makes Bitcoin the only genuinely worldwide money, together with the guarantee that its customers' freedoms are safeguarded. The main advantage that participants in the exchange market in bitcoin receive is the capacity to pay in instalments. They are unrestricted in their ability to send bitcoin transactions at any time and from any location [19].

2.2 Disadvantages of using Blockchain

Here are few disadvantages of blockchain (during implementation in real word applications):

2.2.1 Volatility and high risk of loss

Bitcoin costs are amazingly unstable, increasing and falling at a quick rate. Theorists need to benefit from it, however real financial backers consider it to be too hazardous, so nobody puts resources into Bitcoins. One of the main disadvantages of putting resources into Bitcoin is the absence of administrative oversight [20]. Digital currency laws and charges vary from one country to another and are frequently equivocal or quarrelsome. An absence of guidelines, sadly, can prompt misrepresentation and scams. If a hard drive fails or an infection contaminates data, and the wallets document is compromised, bitcoins are practically "gone." No method exists to get it back. These coins will continue to be stuck in the scheme forever. A wealthy Bitcoin financial supporter may go quickly and irreparably bankrupt as a result of this. Coins from the financial supporter will likewise always be stranded [21].

2.2.2 New System and investor Protection

Even though it is said to have high security for the information about buyer and seller but as it is a new system which was brought recently without certified by anyone, it should also think in the way of misuse. The Bitcoin system might have bugs that still can't seem to be found. Since this is a generally new plan, in case Bitcoins were broadly executed and a bug was found, it may bring about colossal abundance for the exploiter to the detriment of the Bitcoin economy [22]. There is no overseeing body responsible for bitcoin's usefulness.

2.2.3 Black Market Activity

The fast development in digital currencies and the secrecy that they give clients has made impressive administrative difficulties, remembering the utilization of digital currencies for unlawful exchange (medications, hacks and burglaries, illicit porn, even homicide for-recruit), potential to support launder cash, psychological oppression, and keep away from capital controls [23]. There is almost no doubt that cryptographic forms of money, like as bitcoin, have aided the establishment of 'darknet' online commercial hubs where illegal labour and items are transacted by providing a sophisticated and secretive payment system. The recent FBI seizure of more than $4 million in bitcoin from one such business hub, dubbed "Silk Street," provides some insight into the scope of the problem.

2.3 History of Blockchain

Figure 2 describes the history of blockchain technology in cryptocurrency over the years. Stuart Haber and W Scott Stornetta first presented it in 1991. By 1998, computer scientist Nick Szabo was working on 'Bit Gold,' a decentralised digital money. A team led by Satoshi Nakamoto published a white paper in 2008 proposing a blockchain paradigm, then in 2009, the famous ‘Bitcoin’ cryptocurrency was introduced by Satoshi Nakamoto and team. In 2014, another cryptocurrency, Ethereum came into the picture. It introduced computer programs which represented financial instruments such as bonds which were known as smart contracts [24].

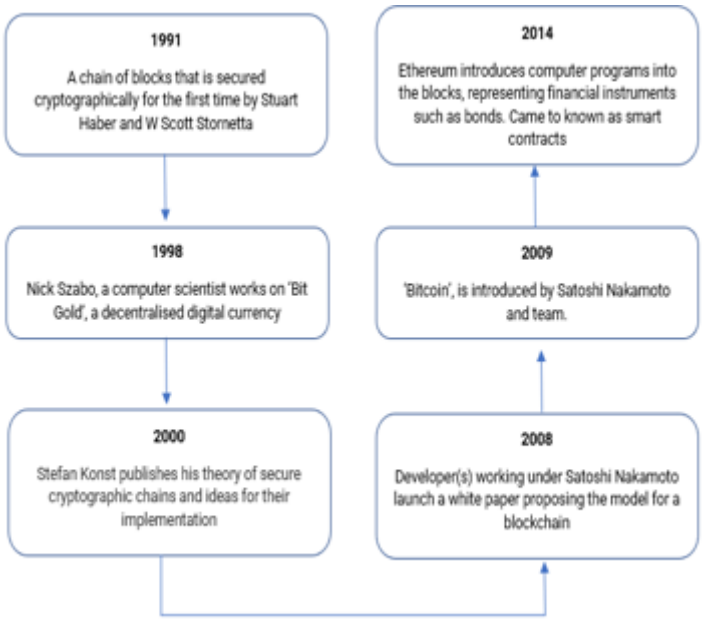

Figure 2: History of blockchain

2.4 Mechanism

Blockchain is a chain containing blocks of immutable data. Each block is connected two the previous block through cryptography. It contains information of the previous block such as timestamp, transaction data and proof-of-work signature. There are certain steps to add a block into the chain. Firstly, a transaction has to be made in the network. Next, the details regarding the transaction must be approved by the participant who is referred to as 'Miner' in this case. The data is then placed in the block when the miner has confirmed the transaction. Finally, the block is added to the ledger using cryptographic procedures that include the prior block's timestamp. Once the block is added into the network, it is made public. Figure 3 represents the same set of procedure as mentioned above [25].

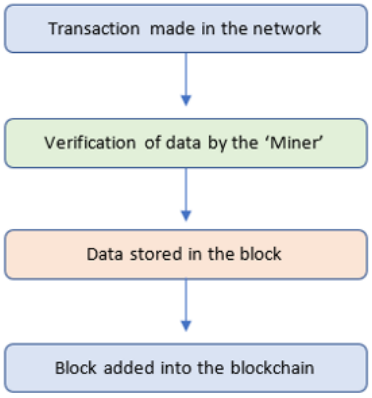

Figure 3: Creation of Blocks in blockchain

2.5 Types of Major Cryptocurrencies

Below are some of the major blockchains

2.5.1 Bitcoin

Bitcoin is a decentralized cryptocurrency. It was introduced in 2009 by Santoshi Nakamoto. It is not managed by a bank or a single administrator. It operates on a peer-to-peer (P2P) network, which eliminates the need for third-party intervention in the transaction. The transactions are verified through network nodes and are stored in the form of blocks in a chain called the blockchain. Bitcoin has also been criticised for its use of bitcoins in illegal transactions. Also, the large amount of electricity used to mine a Bitcoin is one of the reasons for Bitcoin coming under scrutiny around the world [26]

2.5.2 Ethereum

Ethereum is a decentralized, open-source, and disseminated registering stage that empowers the production of brilliant agreements and decentralized applications, otherwise called Dapps. Keen agreements are PC conventions that work with, confirm, or implement the arrangement and execution of some kind of understanding. For example, a brilliant agreement could be utilized to address a lawful agreement imitating the rationale of legally binding provisions or a monetary agreement determining liabilities of the partners and mechanized progressions of significant worth [27].

2.6 Structure of Blockchain

The Blockchain is a collection of blocks that are back-linked together and include events that may be recorded as flat files or kept in conventional databases. Each block in the chain refers to the one before it, and the blocks are connected back-to-back. The first block ever created serves as the basis of the Blockchain, which is commonly represented as a series of layers of transactions [28]. The blockchain is the primary invention that underlies Bitcoin, which is recognised as first decentralised crypto-electronic money. The initial request for payment made in Bitcoin by its future owner initiates the transaction. Every time Bitcoin is supported, a computer hashed sign is used to transmit funds. Each coin has a unique location that serves as its identifier, and every

transaction on the Blockchain is essentially an exchange of bitcoin, starting with one place before moving on to the next [29].
A Blockchain trade takes place between two parties, and it begins if one of the complex parties informs the other about the rules governing the transaction. The citizen Blockchain record will be updated with the current status of the organization's most recent blocks after the exchange has been reviewed and approved, along with all of the organization's customers [30]. Through the use of a public distributed journal and crypto algorithm components that guarantee accepted purchases won't be removed after confirmation, this decentralised structure, along with the cryptography employed, guarantees that the almost no declared payment could be changed or wiped away. It also contributes to the development of trust among parties. A most recent square, known to as one of the "parents," is referenced in each square. There is a header for each square that contains the family's hash information. Users may link each square to its parent using the hash sequence, creating a chain that goes all the way back to the first square that was produced, also known as the "beginning square." A square may have several kids although it only uses a single parent [31]. Each child can be traced all the way back to the very same square and has the same preceding block hash as its parent.

2.7 Properties of Blockchain

Blockchain is a new way to store data that offers a number of appealing properties as follows.

2.7.1 P2P Transmission

Each block in a blockchain is called as a ‘node’. Nodes are interconnected to each other through cryptographic means. Miners can share or transmit data among nodes [32-34].

2.7.2Timestamped Blocks

Blocks are stored as nodes. They are stored along with the time when they have been created.

2.7.3 Immutable Records

Data is stored in the blocks or nodes. The data stored in a node remains completely safe as once the data is entered in the node, the data is immutable i.e., cannot be altered or modified. This is because each node or block contains hashed value of the information from the previous block and a timestamp.

2.7.4 Validation

On the creation of a block or node, the information needs to be verified by other participants or blocks in a blockchain. This is called mining.

2.7.5 Computational Logic

Blockchains include computational logic. Users can introduce algorithms and procedures known as smart contracts. These smart contracts can be executed automatically while transmitting the data.

2.7.6 Encrypted Data Transmission

Data of a 'Miner' is stored securely in a block or node through data encryption. The data is encrypted by the sender's 'Public key' and decrypted by the receiver's 'Private Key'.

2.7.7 Shared Database

Blockchain technology is implemented using shared databases which are distributed all over the network. Participants or 'Miners' in a network are required to agree on the true state of the database. There is no single party controller.

2.7.8 Disintermediation

Blockchain is implemented over a wide range of networks. The network uses a mechanism called as proof-of-work consensus. Proof of work (PoW) depicts a framework that requires a not-immaterial however doable measure of exertion to dissuade paltry or noxious employments of processing power, for example, sending spam messages or dispatching disavowal of administration assaults. This does not require any third-party involvement. Therefore, the dependence on any third-party gets completely removed [35]. As the popularity and usage of the Internet are increasing day-by-day and on the other hand, Cryptocurrency (also called virtual currency) is increasing its popularity and drawing a lot of attention from the public, investors, businessmen and entrepreneurs. As it is becoming more popular with the advantage of not having any trade regularity, people began to invest their savings in cryptocurrencies for high returns. Bitcoin is the first digital currency/virtual currency, which came into existence without having the middleman like banks where personal data is to be revealed for any transaction to be made or done either from the buyer or seller side, thus making others to know the part of assets owned by an individual [36]. As many of the cryptocurrencies are using blockchain technology which among the most advanced surveillance equipment with sophisticated technology that is most efficient for online transactions by preventing fraudsters from using the same money for many people, preserving users' sensitive information, and removing intermediate bodies. The value of the cryptocurrencies is usually due to the limited number of coins for a particular cryptocurrency and demand by the investors. In the case of Bitcoin, the anonymous group created some advanced mathematical and computer engineering puzzles or problems which need to be solved to use the non-useable bitcoins and this process of solving and creating the newer bitcoins is said be to mining, which is usually done with a high server and some advanced software.

So, the difficulty of the puzzles goes on increasing as the non-useable bitcoins goes on decreasing, thus creating the demand in the market which usually raises the value of the currency [37]. From Fig1, it can be observed clearly that the demand and interest in investing money in cryptocurrencies are drastically increasing from the day of its origin. Cryptocurrencies are widely experiencing fast user acceptance across the world and it will be an important subject to be learned by everyone as it can transform the whole system of exchanging money. Being in the world of the internet which brings the world to such a small place with fast transferring of information, Cryptocurrencies will definitely show their rise than present as one end of the world can easily influence the other parts of the world.

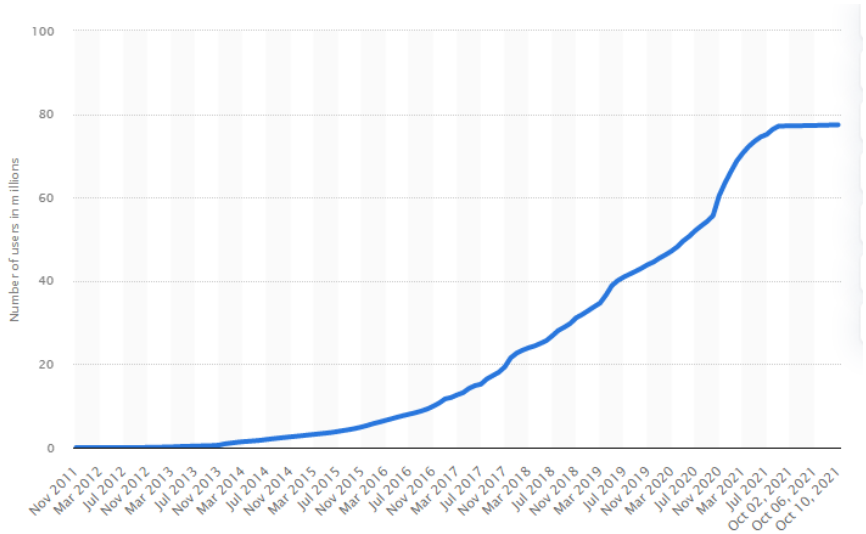

Figure 4: blockchain wallet users worldwide from 2011 to 2021

Note that Figure 4. Here the x-axis depicts the time period, while the y-axis depicts the quantity in millions. Hence, in summary, Blockchain is a new and effective way to store information, execute transactions, etc. But, the security and privacy of blockchains are always at the centre of the debate when using blockchain-based cryptocurrency. There is a misbelief that cryptocurrencies are an anonymous means of payment. The blockchain is a public, fully transparent ledger, so anybody can browse the data of a blockchain using a block explorer and see which addresses transferred how much amount of money and at what time. Blockchain Technology is one of the latest revolutions around the globe which is expected to have a great impact and lead to significant changes in everything, especially in the ways of business. It is a new technology of storing data which prevents the data to be stolen, tinkered with or hacked. It is a technology where data is stored as a chain of blocks and allows users to communicate with each other through a secure gateway. Although it ensures a secure gateway, as a new technology it has some threats too. This research paper would be a review of many cited papers that talk about the threats to the usage of blockchain technology in cryptocurrency.

Cryptocurrency developed and emerged as one of the financial tools about thirteen years back. As there are no barriers like exchange rates when transferred from country to country, they are going to become the leading payment gateway. Bitcoin is the first and most popular cryptocurrency which was introduced by the mysterious and pseudonymous Satoshi Nakamoto has shown its emergence as the digital currency which could replace the long-lasting financial payment systems. Though it can't change the traditional exchange of money, can emerge as the best payment gateway where a global transaction occurs. As cryptocurrency is a decentralized digital currency which is not physical like paper money and due to the increase in technology which is easily accessible to each and every person to promote digital payments with no exchange rates can easily emerge as a leading gateway. Though it is good to know the advantages of cryptocurrency, it is also having some disadvantages of investing and using cryptocurrency.

3. Implementation of Blockchain in Different Systems

Now we discuss different uses and implementations of the blockchain technology systems in various industries [38-40]:

Educational Sector: Blockchain is a technology that can assist students with their academics. Challenges reduced by blockchain are as follows:

i. It has the potential to arise in the formation of an environment that is based on open-source software. This can provide a way for a student to store all of the data needed during his or her course of study, as well as provide an air of validity for carrying fewer books.

ii. It can also establish an environment in which students' personal databases can be modified and then stored. The blockchain gives institutions access to data, and the data that is altered is a lot more exact, so any changes don't have to be as time-consuming.

iii. The issue that the schools/universities face is the increasing number of incidences of fraud and unauthorised diplomas supplied to pupils. The main goal of blockchain technology is to get to a point where every block is a proven block so that any fraud can be detected.
iv. One significant feature of such a technology in the educational context would be that it assigns every student a distinct id, that aids students in syncing up their findings and may easily settle possible project misunderstandings among students. The ability to see the grades in real time can be a huge benefit.

Agricultural Sector: Blockchain has an impact on the convenience of agricultural products for farm kinds of materials, farmers, loans, farmer financing, as well as many other things. Blockchain technology is based on four considerations–

i. Consensus: It conveys information about the dispersed trust, which may be gleaned from how farmers trust the government to protect their fundamental rights.
ii. Safety: This discusses the part of the product export and import, as well as the safety of the farmer's data.
iii. Provenance: This refers to the process of tracing an event's origins. In the event that a farmer-to-farmer transaction occurs. Some intermediaries may use fictitious data to defraud farmers for financial gain. Farmers benefit from blockchain because it helps them build trust.
iv. Trust: The trust factor increases as there is no single supreme force to rule or use unfair methods to dominate.

Healthcare sector Blockchain: There are many different business models used in the healthcare sector. Several organisations are presently developing the Proof of State (PoS) perspective for a wide range of stakeholders [41]. Blockchain technology is thus, in some ways, harmful. The most discussed technology of the decade is blockchain. In addition to numerous contractual obligations for health-care technologies, there is a significant chance that blockchain technology will be employed in the digitalization of pharmaceutical chains. There are 3 methods that blockchain can help change healthcare:

a) An electrical chip which can be used to help with the adoption of blockchain in each and every area of health care appears to be one possible use case for the technology. a) Records saved on the chip: Lists of all patients might be built using electro records at any given moment. Due to the fact that they are updated after each hospital visit by a patient, health files can be cumbersome.
b) Records kept on a chip: One plausible use for blockchain technology is to create a chip that may be used to help all areas achieve healthcare reform. Databases containing data on all individuals at any given time may be created using electro records. Due to the fact that they are updated after each hospital visit by a patient, health files can be cumbersome.
c) Supply chains - The pharma sector adheres to the highest requirements for stability, security, and safety. For instance, supply chain management might be openly scrutinised, reducing human error and delays while simultaneously controlling prices and labour. Even a waste in missions is tracked at all times, and some logistical solutions are followed. While physical items are being transported and being recorded permanently on the blockchain, a solution may be presented to the nodes and it might be a workable choice.
d) Genetic industry - In a billion-dollar business, companies like Enc and Nebula genomics employ blockchain to reliably and securely transfer genomic data. This company makes extensive use of blockchain due to the security it provides and the fact that data is delivered to users without the use of a middleman. They have excellent marketing, and they must safeguard that marketing in order to protect their market [42]. There are numerous use cases that can be generated pertaining to the health-care business
    i. A situation in which the patient has the last say - Every patient has access to their medical information, but they are not allowed to change them. They do, however, have the option of limiting access to certain hospitals.
    ii. Such innovation must be in a tabulated form, which means all information should be preserved in tables, charts, or other statistical forms.
    iii. It can provide a variety of options for employers - This can be advantageous in situations when employers are needed.

Such innovation has the capacity to produce a disruptive environment if it does not match the user's demands. Consider the instance of a patient who has an immediate need to obtain information in order to offer it for any other purpose. However, because this technology prevents the patient from receiving each of the data from the hospital, the patient may feel burdened and his or her requirements may not be met.

3.1 Security and Privacy Concerns

Cryptocurrencies face some serious security concerns and risks, due to which it faces dramatic price drops many times. These concerns can be destructive to any cryptocurrency. Some of such concerns are briefly described below.

3.1.1 Double Spending

Double-spending is a process in which the same single unit of a cryptocurrency can be spent more than once. It occurs when a cryptocurrency is stolen by altering or damaging the blockchain network. The transaction could be erased or a copy of the transaction would be sent by the hacker to make it look authorized. Most commonly, the hacker will send numerous packets to the network for reversing a transaction, which will make it looks like it never happened [43].

3.1.2 Vulnerable Wallets

A wallet should protect our money and privacy, but cryptocurrency wallets are very vulnerable to hacking attacks and theft. Using malware, the wallet can be prevented from communicating with the PC, hence breaching the security. This affects the privacy of its users, and their transactions can now easily be redirected to different accounts.

3.1.3 Cyber-Attacks

A disastrous cyber-attack on not only blockchain but also cryptocurrency exchanges is one of the major concerns of its users. There have been major attacks on exchanges before, which resulted in the loss of people's money as well as the downfall of cryptocurrency value. In 2014, the Mt. Gox heist took place, in which the hackers went away with 850,000 [44] bitcoins which is equivalent to USD 47.03 billion as of October 2021. Distributed Denial of Service (DDoS) attacks is also a threat to cryptocurrency exchanges. There have been many such heists, which is why people don't trust the security of blockchain-based cryptocurrency.

3.1.4 Sybil Attack

In a Sybil Attack, numerous fake identities are created and controlled by a single entity to manipulate a peer-to-peer network Various fake nodes gather around a node so that it can't connect to the other nodes on the network, which then prevents the user from sending or receiving information to the blockchain.

3.1.5 Selfish Mining

Due to the proof-of-work consensus mechanism, certain cryptocurrencies can be threatened by the selfish mining of the major mining pools. Crypto mining is the process in which transactions of cryptocurrency are verified and confirmed, with miners earning cryptocurrencies in return for their computational effort [45]. For selfish mining, greedy miners and hide their generated blocks from the main blockchain, and later reveal them to earn more revenue. With this combined with the Sybil attack, miners can invalidate transactions on the network with their power.

3.1.6 percent Attacks

A 51 percent attack is an attack by a group of miners controlling the majority of the blockchain's computing power. The attackers can reverse transactions that were completed resulting in double-spending or can prevent new transactions from getting confirmed. In 2018, hackers pulled off more than $18 million worth of Bitcoin Gold through a 51 percent Attack [46].

3.2 Security and Privacy Requirements

In blockchains, the usage of private keys and public keys is a critical part of privacy. To safeguard transactions between users, blockchain systems employ asymmetric cryptography. Each user has both a public key and private key in these systems. These keys are cryptographically connected random numbers strings.

3.2.1 Integrity of Data

Blockchains must be designed for data integrity otherwise, the data will be vulnerable or completely non-functional. The blockchain should be used to collect and manage precise, authentic, and timely data, so it is useful to the users.

3.2.2 Tamper-resistant Data

The data in a blockchain should be able to resist any type of damage. The data which is stored on the blocks of the blockchain cannot be modified anyhow.

3.2.3 Preventing Double-spending

Double spending means when a particular unit of currency is spent more than once. For transactions performed with a decentralized blockchain-based cryptocurrency, the blockchain should have strong security measures to prevent the double-spending of a coin.

3.2.4 Anonymous User Identities

If the user data is shared with various financial institutions, then the user's identity may get disclosed. Also, in a transaction, the two users might be unwilling to disclose their real identities to each other [47]. So, the blockchain must have strong security and privacy methods to make user identity anonymous or at the very least pseudonymous.

3.2.5 Transaction Unlikability

If all the transactions of a user could be linked then, the user's identity and other information can be deduced. So, the blockchain should have security measures to provide unlikability of transactions.

3.2.6 Transaction Confidentiality

The blockchain must have security measures such that the user's data couldn't be accessed or disclosed without his or her permission, even under unexpected failures [48].

3.2.7 DDoS Attack Resistant

A Distributed Denial of Service (DDoS) attack is a malicious attempt to flood the internet traffic of a network or server and to take advantage of its security vulnerabilities. A heavy DDoS attack could be used to knock off a blockchain network, so the blockchain should have security measures to prevent or tackle it.

3.2.8 51% Attack Resistant

Malicious miners can conspire and launch various security and privacy attacks like illegal transfer of cryptocurrency or reversing transactions. So, the blockchain should have security measures to prevent or tackle it.

3.3 Privacy and Security Techniques

There are various techniques a blockchain system uses or can use to achieve or enhance its privacy and security.

3.3.1 Change Addresses

A cryptocurrency transaction needs at least one input and output. The existing funds used for sending a transaction are called input, and when the funds are received it's called output. When a user gives an input fund more than the transaction cost, the remaining funds (or the change) are sent back to the user as a change but to a newly generated Change Address. But if the input fund is exactly equal to the transaction cost, then a change address is not needed. Most of the wallets generate change addresses automatically creating a transaction. Change address makes it difficult to track the user's transaction history, hence improving privacy.

3.3.2 Coin Mixing

In Coin Mixing, several input coins, in a mixing pool, are combined and then sent to their receivers' addresses. This makes tracking the transactions more difficult. Coin mixers are software companies serving as a middleman between parties looking to send and receive cryptocurrencies. If a user wants a transaction to be untraceable, he will send a particular number of coins to the coin mixer, who will then combine it with many other transactions of the same currency, and then redistributing it to the receiving addresses [49]. A fee is charged for the mixing

services by coin mixers. Coin mixing increases the level of privacy than regular transactions, but addresses can be linked by observing the amounts of coins in a mixing pool, and many mixing services are centralized.

3.3.3 Ring Signatures

A ring signature is a digital signature that can be created by any member of a group, and each member has their own keys. So, it is not possible to determine which group member created the signature. To sign a message, a member of the group has to use his secret key as well as the public keys of others in the group. The public keys of the group are used to validate that person signing the message is a member of the group, but it is not possible to figure out who signed the message from the group [50]. Ring Signatures are great for private transactions, but if the secret key of a person is compromised, any of his signed messages can be modified.

3.3.4 Homomorphic Encryption

Homomorphic encryption allows users to perform computations on encrypted data, so decrypting the data is not needed. The decrypted form of the computed results will be the same as the result of the same operations performed on the unencrypted data. Homomorphic encryption is used to ensure that the data stored on the blockchain is encrypted. The homomorphic encryption technique is used to preserve privacy and to allow access to the encrypted data over public blockchain for validation. But homomorphic encryption requires a special client-server application to work functionally [51].

3.3.5 Zero-Knowledge Proofs (zk-Proofs)

Zero-knowledge proof lets someone prove the truth regarding something to the verifier without revealing any additional information. In blockchain-based cryptocurrency, the Zero-Knowledge Proofs are used for private transactions. The sender will have to create a proof, without revealing any of the actual transaction data, that the transaction will be considered valid by a verifying node. This allows the identities of both the parties and the amount to be private [52]. Zero-Knowledge Proofs does not require any complicated encryption methods, increases the privacy of users, strengthens the security of information but a tremendous amount of computing power is needed, and if the user forgets their information, all the data is associated with it will be lost.

4. Cryptocurrency Systems

Investors, speculators, the general public, and regulators are all still fascinated by cryptocurrencies. Concerns about legal and regulatory evasion, significant price swings, and claims that the cryptocurrency market is a fad with no underlying value have all sparked recent public conversations regarding cryptocurrencies. These worries have sparked calls for stricter laws, if not outright bans. The use of cryptocurrencies (ICOs) to finance start-up projects, the categorization of cryptocurrencies as payment, commodities markets, or something entirely different, the advancement of credit contracts and cryptocurrency derivatives, and the issuance of cryptocurrency transactions by the fed reserve utilising cryptocurrency innovations are some of the other issues. These debates frequently produce more power as compared to light. There is still a lack of well-established scientific understanding concerning cryptocurrency markets and their influence on economies, businesses, and individuals. The goal of this unique study in the Journal of Industry and Commercial Economy [53] is to help close that gap. The special issue's collection of articles presents six multiple viewpoints on cryptocurrencies, authored through both conventional and behavioural viewpoints and covering both financial and larger problems of cryptocurrencies' link to socio-economic growth and sustainability.

The legitimacy of every cryptocurrency's coin is confirmed through a blockchain. A cryptocurrency is a constantly changing group of linked, encrypted documents, or "blocks." Each block typically includes transaction information, a timestamp, and a hashed reference to the block before it. Blockchains are resistant to data alteration by design. The description calls for "an accessible, decentralised network that may reliably and persistently store transactions." Managing a bitcoin as a distributed ledger is often done through a peer network that uses a system for verifying new blocks. The network majority's participation is required since it is impossible to modify the data in any one block without also changing the data in all subsequent blocks. A computer that is connected to a public blockchain is referred to as a node in the cryptocurrency realm. The node assists to the network of the relevant cryptocurrency by relaying transactions, validating transactions, and storing an identical copy of the ledger. Each network computer (node), when it comes to transaction rehashing, has an identical copy of the ledger of the cryptocurrency it supports. When a transaction happens, the node that made it employs cryptography to simulcast transaction details to other nodes all through the network, guaranteeing that the activity (and all other transactions) is known.

Node owners include volunteers, those maintained by the entity or group responsible for developing the bitcoin blockchain network technology, and those persuaded to host a node in exchange for financial gain [54]. Because the bitcoins in a wallet is linked to one and more unique keys instead of to specific people, Bitcoin is more anonymous than cash (or "addresses"). Owners of bitcoin are therefore anonymous, despite the fact that all transactions are recorded on the blockchain. In spite of this, exchanges regularly find themselves required by law to collect personal information from their users.

The mortgage lender is required by law to reimburse the owner of the asset if their management system has a weakness, including a security breach that causes theft or loss or refuses to carried out a transfer instruction. In the case of cryptocurrencies, the supporting software is responsible for conducting transactions as well as verifying ownership. There is no requirement to employ a "trusted third party." This system, meanwhile, necessitates the existence of a complete history record of prior cryptocurrency transfers that dates each coin holding back to its inception. A "blockchain," a mechanism for connecting records ("blocks"), is the foundation of this historical record. Each new structure in the "chain" of digital data contains details about previous blocks. Consensus is reached all through the whole bitcoin network to accept a new block, ensuring that each user sees the same transaction history.

5. Consensus Algorithms

Blockchain, being a distributed decentralized network with no central authority present to validate and verify the transactions, is considered to be secure only because of the consensus protocols, a core part of Blockchain networks. A consensus mechanism refers to methods used to achieve agreement, trust, and security across a decentralized blockchain network. These consensus protocols help all the nodes in the network to verify the transactions.

5.1 Proof of Work (PoW)

In 2008 Satoshi Nakamoto applied the Proof of Work algorithm in the Bitcoin whitepaper. Proof of Work algorithm is a technique used by many cryptocurrencies. Once all the nodes are brought in an agreement, the transactions will get validated and the new block will be forged on the blockchain.

In the Proof of Work consensus algorithm, miners solve a complex computational problem to create and add new blocks in the blockchain. The verification and organization of transactions in a block, and introducing the newly mined block to the blockchain network needs much less time and energy than solving the ‘complex computational problems’, required to add the new block in the blockchain. When a miner successfully solves the ‘complex computational problem’, the nodes broadcast the block to the blockchain, and the miner receives some of the cryptocurrency as a reward. Although proof of work is an efficient mechanism, it has some disadvantages, like it increases the chance of 51% attacks, finding the correct solution to the ‘complex computational problems’ is very time-consuming, and money and electricity consumption is too high [55].

5.2 Byzantine Fault Tolerance in Practice (pBFT)

The practical Byzantine Fault Tolerance mechanism's goal is to improve features of Byzantine Fault Tolerance on a blockchain. BFT (Byzantine Fault Tolerance) is a method that allows a network to achieve an agreement despite the existence of hostile or malfunctioning nodes. The goal of a BFT technique is to reduce the impact of malfunctioning nodes by using collaborative decision-making. There are two forms of defective node failures: fail-stop and arbitrarily defined failure. The node fails and ceases functioning in the fail-stop failing, whereas the node fails to appear a result or delivers an inaccurate result in the random node failure [56]. One node in a practical Byzantine Fault Tolerant enabled blockchain is set as the primary node and others as secondary nodes. A practical Byzantine Fault Tolerant system functions if the number of malicious or faulty nodes are lesser than or equal to one-third (or 34%) of all the nodes in the system. Although the practical Byzantine Fault Tolerant mechanisms are energy and time-efficient, there are a few limitations to it as it is open to Sybil attack, and it does not scale well.

5.3 Proof of Stake (PoS)

In 2012 the Proof of Stake was first used for a cryptocurrency named Peercoin. The Proof of Stake mechanism states that the mining power is directly dependent on the number of coins staked. Proof of Stake is one of the most common alternatives to Proof of Work. Proof of Stake mechanism requires users to stake their coins to become a validator in the network rather than buying expensive hardware or wasting resources to mine. Validators are randomly chosen to propose new blocks, and validate proposed blocks when they are not chosen. Validators get rewarded for doing so but validating malicious blocks will result in losing stakes.

Although being energy and money efficient, the Proof of Stake has some disadvantages such as, a staked coin can't be sold until the staking period is over, the staking reward much is lesser than the mining reward, the users holding a large number of coins can have a huge influence on the mechanism, and this mechanism is still in its early stage and the privacy and security of Proof of Stake are not proven to be even as good as that of Proof of Work [57].

5.4 Proof of Burn (PoB)

Proof of Burn, first proposed by Iain Stewart in 2012 is an algorithm in which a miner uses a virtual rig to burn (permanently erase) their coins. The more coins they burn the better virtual mining rig they get. So, Proof of burn is Proof of Work without the high energy consumption. For burning the coins, they are sent to a verifiably spendable address. Miners are allowed to burn the coins as specified and get rewarded with tokens of that particular cryptocurrency [58]. The Proof of Burn mechanism uses the burning of cryptocurrency coins periodically to increase the mining power. The value of burnt coins reduces with every newly mined block, to keep miners regularly engaged. The Proof of Burn mechanism is more sustainable as the power consumptions are very low, the expensive mining hardware isn't needed, which can make the miners stay dedicated to it for long. But the verification process is slow, and its efficiency and security are yet to be confirmed on larger scales.

5.5 Proof of Capacity (PoC)

The Proof of Capacity algorithm enables mining by using the hard drive space. In Proof of Capacity, a list of possible solutions is stored on the hard drive of the mining device. The number of possible solution values increases if the available space in the hard drive is more, which increases the more chances of getting the correct solution, hence increasing the chances to win the mining reward. The Proof of Capacity mechanism has two steps: plotting, and mining. In plotting, through repeated hashing of data, all the possible nonce values are listed and stored in the hard drive. In mining, a miner calculates a scoop number. For each nonce in the hard drive, the process is repeated to calculate its deadline. Then the miner chooses the one with the minimum deadline. A deadline is the amount of time that has to be passed after the creation of a block, for a miner to create a new block. A miner can create a block and gets the block reward if no one else has created a block within that time [59]. Proof of Capacity uses just a hard drive, it is more efficient than Proof of Work and Proof of Stake mechanisms, and expensive hardware is not needed. But Proof of Capacity is still new and not adopted by many, and hackers can take advantage of it using malware.

6. Crypto Assets: An Introduction

Cryptocurrencies are a subset of a larger class of financial instruments called as "digital currencies," which allow peer-to-peer supply and distribution transfers without requiring third parties to validate transactions. What sets bitcoin apart from several other digital assets? Whether they should be given with the sole intention of relocating or if they'd been given for other purposes will determine this. The discrepancies observed in regulatory modifications studies within the broad category of cryptocurrency transactions, differentiating two additional sub-categories of digital currencies, are in addition to cryptocurrencies [60]:

i. Cryptocurrencies: an asset built on the blockchain that may be exchanged or transferred between network users and is used as payment, but has no other capabilities.
ii. Crypto securities: a network asset with the possibility for further payments in the future, such a share of profits.
iii. A bitcoin asset that can be exchanged for or utilised to get accessibility to pre-defined goods or services is known as a cryptocurrency utility asset.
iv. A significant turning point in the development of cryptocurrencies and other crypto assets was the emergence of bitcoin exchanges, where anybody can establish an account and exchange virtual currencies against each other and versus fiat money.

Publications using the terms 'Cryptocurrencies' and 'Bitcoin' in the title, abstract, or keywords that are listed in the Scopus database. The graph depicts the number of articles in the Scopus database that had the terms "cryptocurrency" or "Bitcoin" in the title, abstract, or keywords as of August 10, 2019. The category Economics, Econometrics, and Finance is represented by the subsample ECON [62], whereas Business, Management, and Accounting is represented by the subsample BUS. Both an investment and a type of payment may be made using cryptocurrencies. Glaser et al. demonstrate that the main reason for buying cryptocurrencies is high risk investing, at least in the context of Bitcoin. Brokers are enabling a larger variety of investors to participate in speculative investments by making financial instruments like ETNs (Exchange Traded Notes) and CFDs (Derivative Products) that replicate Bitcoin's price performance available. In light of this, it becomes sense to consider cryptocurrencies as capital intermediates.

Some Interesting Statistics:

One way for understanding the differences and similarities between cryptocurrencies and much more standard finance assets is to estimate associations recognized for traditional assets [63]. They discover that while the amount of Bitcoin trades has no impact on the return, it has a positive impact on return volatility. These statistics support the idea that bitcoin markets and traditional financial assets are regulated by analogous features, despite the fact that their main focus is on market attention.

6.1 On point accuracy of the Chain

The whole blockchain is managed by a set of computers instead of humans which leads to a very minimal fraction of error. Transactions in the blockchain are supervised by a network of computers which almost negates the possibility of human error. Even if there are computational errors, the errors are copied in only one of the blockchains and the rest remain as it is. If that error was to spread in the rest of the blockchains, it would need at least 51% of the error to creep up in all of the blockchains which is nearly impossible for large blockchains such as Bitcoin blockchain.

6.2 Cost Reductions

Since the involvement of banks and personal firms is not there in transactions related to blockchain, the third-party costs get saved while making transactions in a blockchain.

6.3 Decentralization

One of the most important advantages of blockchain technology is that it is decentralized. It means that the data in a blockchain is not stored in one chain or database rather the chain of data is copied into many more chains and shared across various networks. This means that if data gets hampered in any one of the chains, the whole database does not get corrupted. This gives blockchains protection against potential hackers as even if they alter data in a block, it won't get reflected in other chains and therefore the chance of hacking the data remains very low.

6.4 Efficient Transactions

Since blockchains are not controlled by banks or firms, they run 24 hours a day, 7 days a week and 365 days a year. Banks usually work for 5 days or 6 days a week which may lead to inefficient transactions sometime. Therefore, blockchains provide a very efficient gateway for transactions.

6.5 Transparency

This means that the code that is written to run the blockchains can be easily viewed by users and therefore the whole process of transactions remains transparent to them. Monitoring bodies can thus ensure the safety of transactions. Also, blockchains accept suggestions from people on how to improve the working of cryptocurrencies and blockchains [64].

7. Threats to Cryptocurrency and Blockchain

Blockchain is another breakthrough, and attacks are emerging that most clients are unaware of. Many attacks till now have targeted the Bitcoin Blockchain, which is the first Blockchain application to involve money and, if compromised**, might result in monetary gain**. The Blockchain framework exclusively perceives the lengthiest chain as authentic. Accordingly, it is near unthinkable for an assailant to come out with a fake exchange since it has not just needed to make a square by settling a numerical issue, yet additionally needs to contend numerically with the genuine hubs to make all succeeding squares with the goal for it to cause different hubs in the organization to acknowledge its exchange as the authentic one. Since all exchanges in the organization are cryptographically associated, this assignment goes to be extremely intense and essentially unthinkable [65].

7.1 Quantum Computing

The Blockchain technology is based on the notion that due to computer limitations, it is theoretically not possible for an individual to edit or mess with it. Nevertheless, given quantum computing's growth and the potentially immense computational power it offers, the secret may become simple enough to break in a reasonable period of time. It would be disastrous for the Blockchain system as a whole, rendering it useless.

7.2 Anomality Attack

Blockchain—specifically, the Bitcoin Blockchain—is widely regarded as an anonymous platform where customers may receive and send money without having to reveal their identities. Bitcoin addresses are associated with an alias rather than a specific person. Notwithstanding, this nom de plume be connected to individuals utilizing different means, and when that happens, the assailant will actually want to discover all exchanges connected to the individual from the very first moment. A facilitated wallet, as well as online services which can track what IPs a customer visits, might be an easy means of revealing the client's persona. Client information is stored in providers, and wallets data bases can be handed to the government when requested and the necessary administrative process is completed.

7.3 A Distributed Denial of Service (DDoS) attack

DDoS assaults are the same old thing, but with the increment of the utilization of data innovation in all parts of life, late assaults are becoming serious, muddled, and incessant. This makes them a standard issue to organizations too as to customers. The assortment of gadgets distantly controllable by applications is growing extraordinarily and the quantity of IoT gadgets is relied upon to rapidly surpass 20billion connected gadgets before the finish of 2020. A large portion of the associated gadgets are ill suited and not outfitted with wellbeing and safety efforts to stay away from vindictive just as ill-advised use (reference); They could be recorded in this way and used to guide DDoS attacks. Apart from DDoS attacks against Bitcoin cash trading exchanges, Blockchain IoT devices are the most persistent target.

7.4 Scams with Bitcoin

Bitcoin has attracted a growing number of people who are looking for a quick and easy way to get cash. Since Bitcoin is another innovation, trick methods are arising and are not completely perceived, which assists programmer with marking benefit of the excited and ineffectively educated clients.

7.5 Scams in Mining Scams

Almost every mining company that sells equipment or provides cloud services ends up being a fraud. Customers are generally promised cloud mining services or equipment, but nothing is delivered. These con artists offered to supply mining gear or cloud mining services, took victims' money, and never delivered on their claims.

7.6 Scams involving Wallets

These are phoney administrations masquerading as online Bitcoin wallets. Deceitful wallet administrations function in the identical way as genuine wallet administrations do, with the exception that they seize the victim's Bitcoin when it arrives at a certain edge. The most popular tactics were identified as Easy Coin, Onion Wallet, and Bitcoinwallet.in [66].

8. Countermeasures for Threats to Blockchain

Blockchain systems do have threats during the implementation process or after the implementation process as mentioned above. Here are few countermeasures for threats to Blockchain.

8.1 Refrain from Spending Double

The exchange rate discrepancy and mining security procedures in Bitcoin offer an indisputable layer of safety against double spending [67]. It is achieved by following a straightforward rule that permits the majority of unspent proceeds from earlier exchanges to be contributed to a successive return, and that the proposition for interactions is determined by one's chronological order in the blockchain, which is preserved using reliable cryptography techniques. This boils down to timestamping and calculating circulating agreements. The most

effective but simple technique to avoid double spending is to wait for a distinct number of confirmations before delivering labour and goods to the payee. Specifically, when the number of affirmations increases, the likelihood of a successful twofold go through decreases.

8.2 Securing Wallets

The term "cold wallet" was used to describe a manual procedure for wallet insurance. A cold wallet is another record that stores the client's wealth of an amount. This method employs two PCs (the second PC must be disconnected from the Internet), and another private key is generated using Bitcoin wallet programming. The abundant money is sent from this new wallet using a client's private key [68]. Creators in guarantee that if the PC isn't associated with the Internet, the programmers won't become acquainted with the keys, thus the wallet security can be accomplished.

8.3. Defence against Distributed Denial of Service (DDoS) Attacks

To mitigate DDoS attacks, a Proof of Activity (PoA) Protocol was created, which is effective against a DDoS attack that might be launched by sending a large number of bogus blocks across the organisation. Each square header in PoA is assigned a sepulchre value, which is stored by the client that records the primary exchange. These clients are referred to as "partners" in the company, and they are expected, to be honest. If there are significant partners involved with the square, any further hoarding of trades is done. The capacity of sepulchre esteem is arbitrary, and more exchanges are stored if the chain has more stake customers connected to it. If the chain is longer, the level of trust among various companions rises, and more excavators are drawn to the network. Because all of the organization's hubs are managed by partners, an opponent will no longer be able to place a malicious square or exchange.

Another option for preventing DDoS attacks is to monitor network traffic on a regular basis with tools like Tor or any other client-defined web administration. Using AI approaches like SVM and bunching, we can figure out which parts of the company are sick. As a result, that portion can be kept out of the organisation until it is rectified. Other possible DDoS defence approaches include: I arranging the organisation so that vengeful packages and requests from unnecessary ports are avoided, and (ii) implementing an outsider DoS insurance scheme that carefully filters the organise and recognises variations in the example [69].

9. Blockchain and Cryptocurrency Link

One event in the cryptocurrency industry is use of Bitcoin's basic source code to create alternative cryptocurrencies, or alt-coins, having characteristics that diverge slightly from those of Bitcoin. Though some of these "forks" have indeed been shady attempts to profit from speculating, others are obviously intended to fix problems that the designers see with Bitcoin and usually incorporate criticisms of the Bitcoin paradigm. Others use less exacting mining techniques or have made an effort to deliberately create a unique culture around their currency, like Dogecoin [70], that has a hilarious non-competitive culture. Despite these modifications, cryptocurrencies are now frequently associated with the values of the free market. They have been specifically linked to the extreme individualism of conservative libertarianism. The components of cryptocurrency, but at the other hand, may enable non-hierarchical identity and peer-to-peer collaboration inside a communitarian network structure, which appeals to people to a more left-wing libertarian leaning. Therefore, there are emerging initiatives to develop digital currencies that could be used as a means of exchange for explicitly cooperative and collaborative enterprises that function outside of the logic of conventional market processes. Modern technology (Blockchain) Although there are several ideological arguments around cryptocurrencies, the majority of interested parties consider the fundamental idea of a decentralised ledger kept by a community of nodes to be crucial. The use of a blockchain ledger for reasons other than logging financial transactions has prompted interest in blockchain 2.0 efforts as a result of this.

A blockchain may be compared to a database that is accumulated over the years by a network of users who all use the same programme and are subject to the restrictions and regulations set out by the foundation programme. A blockchain is built up of data fragments that are progressively "chained" together, as the name suggests. It resembles a spreadsheet that expands as additional columns are added to the blockchain over time. A blockchain record is created and maintained as long as the software is in use. As a consequence, unlike a central database dominated by a single organization, it continues to function even if certain participants leave. It creates a permanent record that is impossible for any one party to change. The structure of the resulting blockchain also changes whenever the code of the underlying software used by participants is altered, enabling the creation of blockchain database that hold a lot of information, including title deeds, contracts, shares, vote totals, and even character ratings. All three firms are developing systems that will enable individuals and microbusinesses to use

blockchain technology: Ethereum [71], Related party, and Blockstream25. For instance, Provenance is a start-up that uses Ethereum technology to provide a high transparency record of information from the global supply chain of businesses.

The front of the scene is experiment with smart contracts, which are little packets containing code—or screenplays may be kept on a blockchain and also that users may interact with to do basic tasks. This smart-contract is designed to use data from meteorological organisations and then, after a predetermined period of time, unlock bitcoins from escrow and send them to a farmer in need of rain protection. This blockchain-based weather derivatives contract was created. Simple building-block contracts can be used to form larger multi or multi-function organisations that some people refer to as "decentralised autonomous organisations" (DAOs). Even if strong multi-stage algorithms are controlled by a distributed network of computers rather than a single top management, such DAOs are challenging to comprehend and seem to many people to belong in the realm of science fiction.

10. Future Scope

It is verifiable that the rise of digital money will assume a huge part on the planet's financial texture. Because digital money has not yet reached maturity in terms of time, further research into its innovation, potential, and risk should be considered to ensure that the possibilities are not merely a coincidence. The security convention ought to be better, if not the same than the ordinary brought together financial framework in ensuring the client's financial resources [72]. Client security necessitates a significant contribution from stakeholders in this new business, thus the blockchain innovation's certainty and confidence will allow it to become the norm for clients while conducting daily transactions over the internet. In evidence of stake strategy, an individual necessity to approve the coins that they own and the sum had. The individual requirements to make an exchange of their coins that they ship off their record as an award with the data of predefined rate [73]. The evidence of stake looks like a pool like plan that give the same opportunity for all diggers. Furthermore, a cross-breed method that includes combined verification of labour and confirmation of stake has been presented, with a portion of the verification of work being compensated to all dynamic hubs and the stake determining the ticket gained to all wagers. In PoA, the movement term alludes to dynamic clients that keep up with the full internet-based hub furthermore, the one that ought to be compensated. Oppositely, in evidence of stake, disconnected clients can in any case gather the coins over the long run what's more, this can prompt twofold expenditure of a similar square. PoA provides much improved security for dealing with future threats to cryptographic money. It has more additional space, and the arrangement correspondence allows for less penalty. Furthermore, PoA has minimal exchange costs, consumes less energy, and the organization's geography may be made to work. In this way, PoA elective serve as a superior stage for digital money because of its capacity to fight of twofold spending and in particular the expense in procuring the digital money contrasted with confirmation of work [74]. The market has been plunged with some new digital currencies that had effectively made it into the market and there are many actually holding back to be delivered. There have been many arising monetary standards that are testing and contending Bitcoin in term of its cost and market capitalization. The model does recreation on the market where the monetary forms are exchanged. With the approval of the record holders, any monetary types can be traded among themselves. It was also discovered that Bitcoin may be swapped for other money, suggesting that the highly justified Bitcoin may be substituted through other exciting coins with superior features in the future. As a result, considering factors like as security, return on investment, and cheap mining costs can help determine which one of the new and emerging sophisticated coins will supersede Bitcoin in the near future. One of them is to improve the outcome of the work confirmation by reusing it. By remunerating other clients from the established handled issue, an all-around given customer can reuse this outcome as an asset in handling any numerical riddle. Another concept is to convert the electrical energy produced through the mining technology into warm energy [75]. This is recognised in cold-climate countries, where the substantially high heat energy liberated by solving the numerical puzzle may be used to heat private homes and other family duties that require heat energy.

Moreover this, Digital money looks to have passed the stage where new innovations are met with scepticism. Even engine vehicles were surprised by this phenomenon. Bitcoin has started to establish a specialised marketplace for itself, which may either help bring virtual currencies closer to the mainstream or be its main weakness. Virtual payment methods are still in its infancy, so it's hard to predict if they'll ever become a really popular presence in international business. The Financial world is creating new features and fixing existing issues in an effort to establish the money as a standard. Different forms of virtual currency have evolved, each with a little different appeal from Bitcoin but seemingly equal importance. It's feasible that crypto money may have a significant impact, and Bitcoin will be essential to the survival of such monetary standards. The growth of bitcoin exchanges across Europe and Latin America suggests that the currency has real legitimacy. When it came to Bitcoin as well as other digital forms of payment, there are a tonne of other factors to consider. The financial ramifications of Bitcoin's effect on traditional fiat cash execution as well as the ramifications for

nations that are starting to adopt government cryptographic types of money should be carefully examined. Although this needs much more financial and marketing study to ascertain, digital money's ability to carry out minute exchanges may allow it to cover a financial vacuum that based one's monetary types are unable to fill. These are modified instalments that occur when a certain event occurs. Predetermined instalment contracts are often accomplished by an organization's whole bookkeeping branch, making this an incredibly exciting subject of extra improvement. Finally, electronic currency is a product of using encryption to create a computerised asset.

11. Conclusion

The conclusion this paper comes to is that blockchain and cryptocurrency systems are the most versatile and in demand technology in the world right now. They are useful in so many various industries and for various purposes as it as pros and benefits which the normal facilities cannot offer. But even with this, there are some disadvantages as there are with a new technology. It is still in the developing phase and will only help more and more as it improves. Educational, Agricultural and Health industries all use blockchain system for better transaction related services. The demerits are that there is no single head so everybody has power and it might be difficult to manage someday. Their fundamental principle is based on blockchain and that is what helps the system to work efficiently. The security and anonymity of blockchains have generated a great deal of attention as a result of several large institutions and organisations investing in blockchain-based cryptocurrencies. The trust that users have in the privacy and security of blockchain-based cryptocurrencies may be increased or built up by having a thorough understanding of the security and privacy features and methods of blockchain. The future growth of blockchain-based cryptocurrencies is thought to depend on adopting and developing the techniques stated above, such as consensus algorithms, mixing, etc. Above that, the users can and should use strong passwords, two-factor authentication, VPN, encrypted emails, etc. to protect their privacy. Blockchain is incredibly praised and supported for its decentralised architecture and distributed nature. However, a few studies on the blockchain region unit are protected by Bitcoin. However, blockchain is being used in a variety of sectors well outside of Bitcoin. With its main characteristics of decentralisation, persistency, secrecy, and auditability, the blockchain has demonstrated its promise for modernising outdated commerce. For upcoming scholars, this study thoroughly examines the depth of a comprehensive evaluation of blockchain technology.

Conflict of Intertest

The authors have declared that they do not have any conflict of interest regarding publication of this work.

References

[1] Belchior, Rafael, et al. "A survey on blockchain interoperability: Past, present, and future trends." *ACM Computing Surveys (CSUR)* 54.8 (2021): 1-41.

[2] A. Deshmukh, N. Sreenath, A. K. Tyagi and U. V. Eswara Abhichandan, "Blockchain Enabled Cyber Security: A Comprehensive Survey," 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, pp. 1-6, doi: 10.1109/ICCCI54379.2022.9740843.

[3] Hewa, Tharaka Mawanane, et al. "Survey on blockchain based smart contracts: Technical aspects and future research." *IEEE Access* (2021).

[4] Zuo, Yanjun. "Making smart manufacturing smarter–a survey on blockchain technology in Industry 4.0." *Enterprise Information Systems* 15.10 (2021): 1323-1353.

[5] Alharbi, Mekhled, and Farookh Khadeer Hussain. "Blockchain-Based Identity Management for Personal Data: A Survey." *International Conference on Broadband and Wireless Computing, Communication and Applications*. Springer, Cham, 2021.

[6] Gimenez-Aguilar, Mar, et al. "Achieving cybersecurity in blockchain-based systems: A survey." *Future Generation Computer Systems* (2021).

[7] Liu, Chao, et al. "A survey on blockchain-enabled smart grids: Advances, applications and challenges." *IET Smart Cities* 3.2 (2021): 56-78.

[8] Dorsala, Mallikarjun Reddy, V. N. Sastry, and Sudhakar Chapram. "Blockchain-based solutions for cloud computing: A survey." *Journal of Network and Computer Applications* 196 (2021): 103246.

[9] Peng, Li, et al. "Privacy preservation in permissionless blockchain: A survey." *Digital Communications and Networks* 7.3 (2021): 295-307.

[10] Bhushan, Bharat, et al. "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions." *Computers & Electrical Engineering* 90 (2021): 106897.

[11] Bornholdt, Stefan, and Kim Sneppen. "Do Bitcoins make the world go round? On the dynamics of competing crypto-currencies." *arXiv preprint arXiv:1403.6378* (2014).
[12] Cocco, Luisanna, Giulio Concas, and Michele Marchesi. "Using an artificial financial market for studying a cryptocurrency market." *Journal of Economic Interaction and Coordination* 12.2 (2017): 345-365.
[13] Becker, Jörg, et al. "Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency." *The economics of information security and privacy*. Springer, Berlin, Heidelberg, 2013. 135-156.
[14] Hofman, A. "The Dawn of the National Currency–An Exploration of Country-Based Cryptocurrencies." *Retrieved from Bitcoin Magazine Website: https://bitcoinmagazine. com/articles/dawnnational-currency-exploration-country-based-cryptocurrencies-1394146138* (2014).
[15] Hileman, Garrick. "State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass." *Retrieved from Coindesk Website: http://www. coindesk. com/state-of-bitcoin-blockchain-2016* (2016).
[16] Doshi, Saloni S., and Sub Commerce. "A Study of Opinions on Future of Crypto Currency in India."
[17] Bentov, Iddo, et al. "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y." *ACM SIGMETRICS Performance Evaluation Review* 42.3 (2014): 34-37.
[18] Vranken, Harald. "Sustainability of bitcoin and blockchains." *Current opinion in environmental sustainability* 28 (2017): 1-9.
[19] Shi, N. "A new proof-of-work mechanism for bitcoin. Financ. Innov. 2, 31 (2016)."
[20] Böhme, Rainer, et al. "Bitcoin: Economics, technology, and governance." *Journal of economic Perspectives* 29.2 (2015): 213-38.
[21] Bouri, Elie, et al. "Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions." *Finance Research Letters* 23 (2017): 87-95.
[22] Dos Santos, Renato P. "On the philosophy of Bitcoin/Blockchain technology: is it a chaotic, complex system?" *Metaphilosophy* 48.5 (2017): 620-633.
[23] Van Alstyne, Marshall. "Why Bitcoin has value." *Communications of the ACM* 57.5 (2014): 30-32.
[24] Khatwani, S. "Explaining Hash Rate or Hash Power In Cryptocurrencies." *CoinSutra. https://coinsutra. com/hash-rate-or-hash-power/ (accessed 13 September, 2018)* (2018).
[25] FAUZI, Muhammad Ashraf, Norazha PAIMAN, and Zarina OTHMAN. "Bitcoin and cryptocurrency: Challenges, opportunities and future works." *The Journal of Asian Finance, Economics, and Business* 7.8 (2020): 695-704.
[26] DeVries, Peter D. "An analysis of cryptocurrency, bitcoin, and the future." *International Journal of Business Management and Commerce* 1.2 (2016): 1-9.
[27] Salcedo, Eduardo, and Manjul Gupta. "The effects of individual-level espoused national cultural values on the willingness to use Bitcoin-like blockchain currencies." *International Journal of Information Management* 60 (2021): 102388.
[28] Wang, Zeli, et al. "Ethereum smart contract security research: survey and future research opportunities." *Frontiers of Computer Science* 15.2 (2021): 1-18.
[29] Alofi, Akram, et al. "Selecting Miners within Blockchain-based Systems Using Evolutionary Algorithms for Energy Optimisation." *arXiv preprint arXiv:2106.11916* (2021).
[30] Dibaei, Mahdi, et al. "Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: a survey." *IEEE Transactions on Intelligent Transportation Systems* (2021).
[31] Frikha, Tarek, et al. "Healthcare and fitness data management using the iot-based blockchain platform." *Journal of Healthcare Engineering* 2021 (2021).
[32] Fu, Xiang, Huaimin Wang, and Peichang Shi. "A survey of Blockchain consensus algorithms: Mechanism, design and applications." *Science China Information Sciences* 64.2 (2021): 1-15.
[33] Khan, Shafaq Naheed, et al. "Blockchain smart contracts: Applications, challenges, and future trends." *Peer-to-peer Networking and Applications* (2021): 1-25.
[34] Sanka, Abdurrashid Ibrahim, et al. "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research." *Computer Communications* (2021).
[35] Bouraga, Sarah. "A taxonomy of blockchain consensus protocols: A survey and classification framework." *Expert Systems with Applications* 168 (2021): 114384.
[36] Ahmad, Raja Wasim, et al. "The role of blockchain technology in telehealth and telemedicine." *International Journal of Medical Informatics* (2021): 104399.
[37] Yue, Kaifeng, et al. "A Survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective." *IEEE Communications Surveys & Tutorials* 23.4 (2021): 2191-2217.
[38] Dwivedi, Sanjeev Kumar, et al. "Blockchain-based internet of things and industrial IoT: a comprehensive survey." *Security and Communication Networks* 2021 (2021).
[39] Hakak, Saqib, et al. "Recent advances in blockchain technology: A survey on applications and challenges." *International Journal of Ad Hoc and Ubiquitous Computing* 38.1-3 (2021): 82-100.

[40] Mezquita, Yeray, et al. "Cryptocurrencies and Price Prediction: A Survey." *International Congress on Blockchain and Applications*. Springer, Cham, 2021.
[41] Berdik, David, et al. "A survey on blockchain for information systems management and security." *Information Processing & Management* 58.1 (2021): 102397.
[42] Hewa, Tharaka, Mika Ylianttila, and Madhusanka Liyanage. "Survey on blockchain based smart contracts: Applications, opportunities and challenges." *Journal of Network and Computer Applications* 177 (2021): 102857.
[43] Latif, Shahid, et al. "Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions." *Transactions on Emerging Telecommunications Technologies* 32.11 (2021): e4337.
[44] Bodziony, Norbert, et al. "Blockchain-Based Address Alias System." *Journal of Theoretical and Applied Electronic Commerce Research* 16.5 (2021): 1280-1296.
[45] Huang, Huawei, et al. "A survey of state-of-the-art on blockchains: Theories, modelings, and tools." *ACM Computing Surveys (CSUR)* 54.2 (2021): 1-42.
[46] Walsh, Clara, et al. "Understanding manager resistance to blockchain systems." *European Management Journal* 39.3 (2021): 353-365.
[47] Dabbagh, Mohammad, et al. "A survey of empirical performance evaluation of permissioned blockchain platforms: Challenges and opportunities." *computers & security* 100 (2021): 102078.
[48] Kumar, Rajesh, and Rewa Sharma. "Leveraging blockchain for ensuring trust in IoT: A survey." *Journal of King Saud University-Computer and Information Sciences* (2021).
[49] Gomathi, S., et al. "A survey on applications and security issues of blockchain technology in business sectors." *Materials Today: Proceedings* (2021).
[50] Jang, Hyeji, and Sung H. Han. "User experience framework for understanding user experience in blockchain services." *International Journal of Human-Computer Studies* 158 (2022): 102733.
[51] Guggenberger, Tobias, et al. "A structured overview of attacks on blockchain systems." *Proceedings of the Pacific Asia Conference on Information Systems (PACIS)*. 2021.
[52] Sookhak, Mehdi, et al. "Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues." *Journal of Network and Computer Applications* 178 (2021): 102950.
[53] El Sobky, Wageda I., Sherif Hamdy Gomaa, and Ashraf Y. Hassan. "A Survey of Blockchain from the Viewpoints of Applications, Challenges and Chances."
[54] Tran, Quang Nhat, et al. "A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture." *IEEE Open Journal of the Computer Society* 2 (2021): 72-84.
[55] Nerurkar, Pranav, et al. "Dissecting bitcoin blockchain: Empirical analysis of bitcoin network (2009–2020)." *Journal of Network and Computer Applications* 177 (2021): 102940.
[56] Ahmad, Raja Wasim, et al. "Blockchain for aerospace and defense: Opportunities and open research challenges." *Computers & Industrial Engineering* 151 (2021): 106982.
[57] Gupta, Rajesh, Aparna Kumari, and Sudeep Tanwar. "A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles." *Transactions on Emerging Telecommunications Technologies* 32.6 (2021): e4009.
[58] Kahyaoğlu, Sezer Bozkus, and Tamer Aksoy. "Survey on blockchain based accounting and finance algorithms using bibliometric approach." *21st Century Approaches to Management and Accounting Research* (2021).
[59] Johar, Sumaira, et al. "Research and applied perspective to blockchain technology: A comprehensive survey." *Applied Sciences* 11.14 (2021): 6252.
[60] Shankar, C. Gowri. "A SURVEY ON BLOCKCHAIN APPLICATIONS." *INFORMATION TECHNOLOGY IN INDUSTRY* 9.3 (2021): 635-639.
[61] Werner, Flynn, et al. "Blockchain adoption from an interorganizational systems perspective–a mixed-methods approach." *Information Systems Management* 38.2 (2021): 135-150.
[62] Kshetri, Naresh, Chandra Sekhar Bhusal, and Devendra Chapagain. "BCT-AA: A survey of Blockchain Technology-based Applications in context with Agribusiness." *Available at SSRN 3834004* (2021).
[63] Pal, Om, et al. "Key management for blockchain technology." *ICT Express* 7.1 (2021): 76-80.
[64] AlMendah, Ohood M. "A Survey of Blockchain and E-governance applications: Security and Privacy issues." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.10 (2021): 3117-3125.
[65] Steinmetz, Fred, et al. "Ownership, uses and perceptions of cryptocurrency: Results from a population survey." *Technological Forecasting and Social Change* 173 (2021): 121073.
[66] Nguyen, Tri, Risto Katila, and Tuan Nguyen Gia. "A Novel Internet-of-Drones and Blockchain-based System Architecture for Search and Rescue." *2021 IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*. IEEE, 2021.

[67] Anand, M. Vivek, and S. Vijayalakshmi. "A Survey on Blockchain Adaptability in IoT Environments." *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. IEEE, 2021.
[68] Shinde, Rucha, et al. "Blockchain for securing ai applications and open innovations." *Journal of Open Innovation: Technology, Market, and Complexity* 7.3 (2021): 189.
[69] Wang, Gang, and Mark Nixon. "Intertrust: Towards an efficient blockchain interoperability architecture with trusted services." *Cryptology ePrint Archive* (2021).
[70] Khan, Dodo, Low Tang Jung, and Manzoor Ahmed Hashmani. "Systematic Literature Review of Challenges in Blockchain Scalability." *Applied Sciences* 11.20 (2021): 9372.
[71] Bhutta, Muhammad Nasir Mumtaz, et al. "A Survey on Blockchain Technology: Evolution, Architecture and Security." *IEEE Access* 9 (2021): 61048-61073.
[72] Kaur, Sivleen, et al. "A Research Survey on Applications of Consensus Protocols in Blockchain." *Security and Communication Networks* 2021 (2021).
[73] Al-asmari, Aisha M., Rahaf I. Aloufi, and Youseef Alotaibi. "A Review of Concepts, Advantages and Pitfalls of Healthcare Applications in Blockchain Technology." *International Journal of Computer Science & Network Security* 21.5 (2021): 199-210.
[74] De Campos, Mário Gabriel Santos, et al. "Towards a Blockchain-Based Multi-UAV Surveillance System." *Frontiers in Robotics and AI* 8 (2021).
[75] Liu, Xiao Fan, et al. "Knowledge discovery in cryptocurrency transactions: a survey." *IEEE Access* 9 (2021): 37229-37254.