Blockchain and Cryptocurrencies

Thesis in the field of production and manufacturing Management for the degree in Engineering Management

Author: Khilola Kurbanova
Student ID: 289295

Supervisor: Elisa Ughetto

Date: March 18, 2024

Acknowledgment

Although the completion of this thesis will bring my academic career to an end, I hope that this lifelong path of knowledge and wisdom endures. I am delighted that the Department of Industrial Management and Production Engineering (DIGEP) at Politecnico Di Torino has stood by me in achieving my goals simultaneously improving my managerial and analytical skills.

I would like to express appreciation to my supervisor, Professoressa Elisa Ughetto, for her tremendous guidance during the thesis writing process and for making this work possible. I want to express my gratitude to my parents and friends for their unbending support and drive every step of my life.

List of Contents

Acknowledgment....2

Abstract....4

1. Introduction....5

2. Blockchain Technology....7

3. Literature Review....11

4. Blockchain: Key features....15

4.1 Multi-Currency Payment Processor....16

4.2 Variations across Bitcoin ledgers and Systems....16

4.3 Gambling using Unregulated Cryptographic Currencies....17

4.4 Underground Marketplaces....17

4.5 The Innovation Sector....17

4.6 Utilization of Energy....18

4.7 Tax Evasion and Assessment....18

5. Research Methodology....21

5.1 Qualitative and Quantitative Research....21

5.2 Data Collection Methods....22

6. Blockchain and GDPR....24

6.1 Review the implications of crypto assets....26

6.2 The Tax implications of virtual currency....28

7. The Conclusions and the Future Work....29

References....31

Abstract

Blockchain is a cutting-edge technology that enables individuals to enter transactions on a distributed, digital ledger that is decentralized and operates independently of a central authority. The blockchain revolution has produced many important byproducts, the most notable of which is Bitcoin. Some refer to this technology as "the trust machine [1]."

Cryptocurrencies is not just a means for compensating and transferring funds. The technology involved, blockchain, has an even greater impact due to its potential for use outside of the financial sector. Both favorable and unfavorable consequences have been felt by financial markets and businesses because of tokenization and its adoption. The objective of this research is to illustrate how cryptocurrency affects management.

Although blockchain technology had been around for a long time, it only gained popularity with the introduction of Bitcoin. Technology is divided into three variants based on areas exterior than markets and the world of finance, smart contracts, and digital currencies. This technology diminishes the possibility of counterfeiting and hacking by using intricate algorithms and networked computers.

Valuable assets can also be tokenized and traded through companies like PayPal and eBay. Blockchain is also popular for its record-keeping capabilities. The information is freely available to the general audience. However, people's privacy and anonymity are also prioritized. A qualitative research approach was used. This was accomplished by researching and assessing previous material on cryptocurrencies and their overall economic impact.

The advantages and disadvantages of employing digital assets had been taken into consideration to figure out its economic feasibility. It was found that asset tokenization and virtual currency improve security, perform in conjunction with payment methods, and contribute to enterprise transparency. Additionally, there are also drawbacks, such as an increased chance of fraud and unlawful transactions [2].

Subjects: the digital ledger, the website payments, virtual currencies, security

1. Introduction

Blockchain technology and cryptocurrencies have the potential to overhaul numerous kinds of fields involving supply chain management, healthcare, and fiscal affairs.

Although cryptocurrencies provide a digital medium of exchange that eliminates the need for middlemen like banks, blockchain technology offers a safe, decentralized method of recording and confirming transactions. Understanding the effects of cryptocurrencies and blockchain technology on various sectors of the economy is critical as their popularity and use grow.

The unique qualities of Blockchain, Due to the widely scattered and decentralized ledger that keeps track of transactions, crypto-currencies have since become widely used as a method of online payment. Blockchain is the most effective means to manage cryptocurrencies because of its key characteristics, which include decentralized agreement, privacy, accounting records that are scattered and shared, autonomy, and immutability. Like all alternative forms of payment, blockchain-based systems and cryptocurrencies are vulnerable to vulnerabilities. [3].

A blockchain is a decentralized, open-source database used to record network transactions. Transactions are stored in an immutable block including all the transaction's data. Any essential transaction or knowledge can be registered and transferred throughout the network.

Blockchain eliminates earlier methods of transaction recording that were centralized, ineffectual, costly, and repetitious. Bitcoin, a decentralized peer-to-peer digital currency, is frequently described in terms of blockchain technology.

Figure 1-Blockchain network [4]

This research project uses a public poll to study Actual application scenarios for bitcoins and their investment conceivable. To gain a better understanding of the perceived security threats and investment opportunities associated with cryptocurrencies, a sample of 100 Professionals via academic achievement are given a questionnaire pertaining to digital coins, its applications that is feasible anxieties, and perceived risks.

According to a review of the responses, customers are cautious about adopting cryptocurrencies as a form of online payment owing to alleged security threats. The extensively cited vulnerabilities stemming from cryptocurrencies are somewhat time-jacking, 51% robberies, double spending, selfish mining, and attacks on digital currencies.

By implementing pertinent resolution techniques, the issues can be fixed. The major root cause of blockchain technology misuse has been deemed to be the shortage of homogeneous worldwide conventions and governance. This emphasizes the need for the international community to unite in a bid to put in place codes of conduct that will stop the digital currency's technology being maliciously abused.

2. Blockchain Technology

Blockchain is a technology that utilizes a dispersed data framework for monitoring electronic currencies without necessitating a centralized control system.

In other words, they comprehend anything about each other. Reliability is a prerequisite in all dealings. [5]

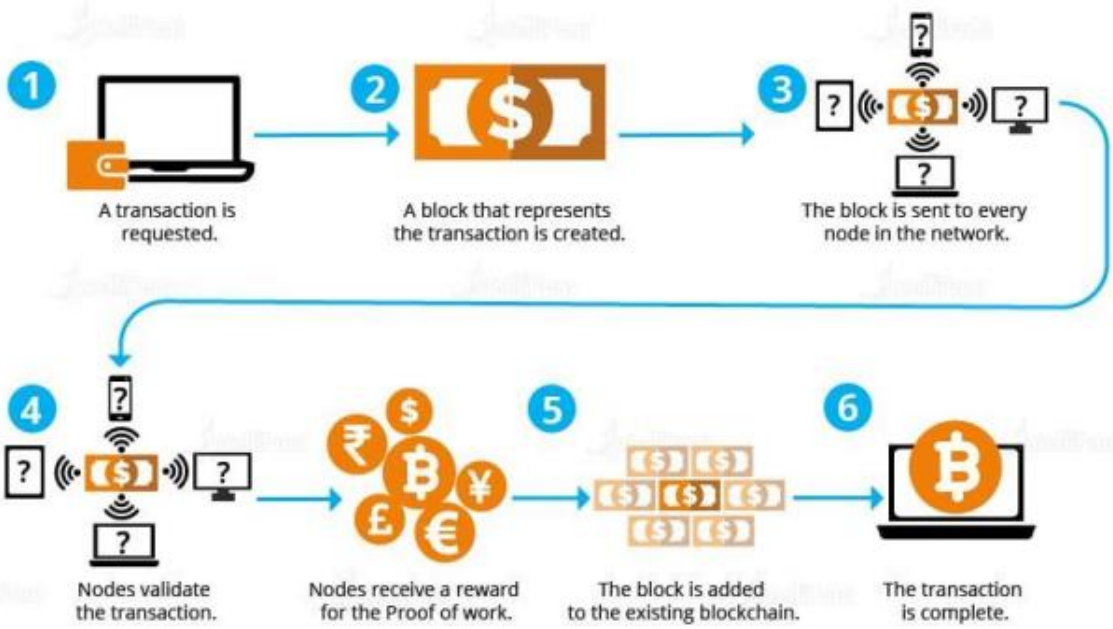

Figure 2 How Blockchain works (Intelli Path) [6]

The blockchain architecture, which was first built for the cryptocurrency Bitcoin, sprang from a preference for avoiding (government-guaranteed) funds and bank-controlled transactions, as well as the attendant expenses.

The primary difficulty associated with any electronic money system is the potential danger of overspending. Electronic money is merely information. One may hypothetically spend it twice. Blockchain solves the Dual allocate issue due to the lack of an electronic backup account or other forms of authority. [7]

Cryptocurrency monitors and verifies operations via a distributed hierarchy of hubs which deliberate on the order where transactions occur. As consequently, the provider's protocol assures every single operation is distinct. Once a significant number of miners concur that all current expenditures are unique (which implies they weren't previously spent twice), they are considered by encryption wrapped into an encrypted block. Every newly formed block is

attached to formerly secured blocks, generating a web of acknowledged memory that preserves a recognized trail of each transaction.

How successful is blockchain technology?

Agreements, operations, and corresponding archives are deeply embedded in our financial, judicial, and governmental structures. Organizations safeguard resources and set limits upon companies and individuals alike. Certain facts are critical to our distinct identity and serve as the foundation for agent trust.

These essential tools are about to transform their current state of centralization and restriction to the borders of individual companies. In the digital age, the method we govern and sustain managerial oversight as needs change. Resources are becoming more dispersed and integrated. Speed is also vital because traditional methods are no longer sustainable with the rapidity of digital transactions.

The bitcoin network gadgets appear to possess the prospective to treatment this threshold obstacle. the decentralized ledger innovations developed via the emergence of digital currencies. Despite individuals simulated coins have endured generated, it is the underneath innovation, the bitcoin blockchain, the fact that encompasses sparked the desire of innovators and shareholders. The digital currencies are a dispersed record that can swiftly and accurately capture and confirm agreements within two groups. The accounting record can also be set up to carry out deals naturally, that is an essential characteristic of the The World Wide Web of devices. Nevertheless, greater on that the in an alternate item. [8]

The data visualization illustrates how the blockchain functions, covering the basic processes. Many blockchain primers and posters concentrate on cryptography, obtaining to convey to novices how "unanimous agreement computations," "encrypted activities," and electronic signatures occur.

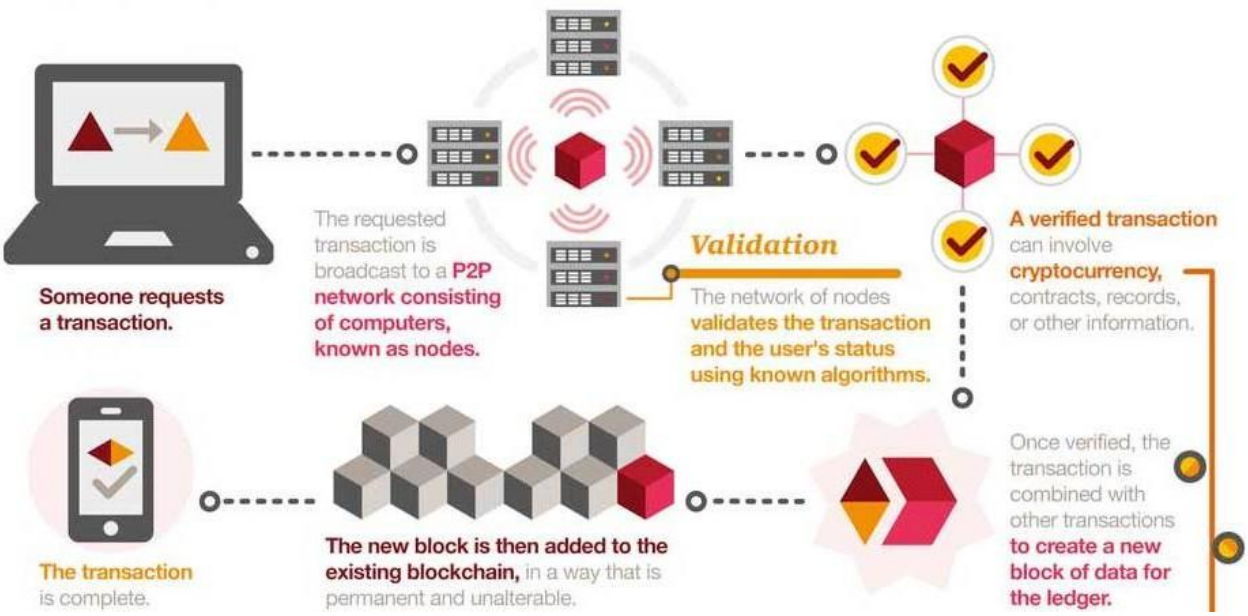

Figure 3- Working of Blockchain technology (Digital vidya) [9]

Bitcoin is a decentralised system of unverified counterparties that holds information about transactions on a common record. Individuals in a Blockchain execute transactions using computers referred to as miners. Every record in an electronic ledger alludes to the preceding one and comprises facts, a unique encode, and the hash of the previous block. The hash algorithm is a computation that derives a unique value of a given piece of text. The hash approach retains the authenticity of a single transaction and the Blockchain, although proof-of-work is additionally employed to avert corruption and increase security. Evidence of work (also called PoW is an option for establishing evidence that can be costly for one to verify but straightforward for others to affirm.

Hackers need to resolve a wireless technology or mathematical puzzle to qualify for those using the network to acknowledge their block as valid. PoW calculations and establishing a new chain to a transaction take approximately ten moments per block (Tania 2018). Any individual may utilize the public key to send an encrypted message to the beneficiary's account. Only the wallet's owner, who possesses the secret key to the wallet, has control over the transaction. A blockchain includes of three fundamental innovations: (1) encrypted private key digital signatures, (2) a network of nodes with a common database, as well as (3) a reward to handle peer-to-peer transactions and preserving documents. Authentication on the digital currency blockchain is assigned via an intersection of simultaneous private and public cryptographic keys [4]. The simultaneous use of these keys generates a powerful electronic

signature, implying strong ownership. Miners conduct agreements, financial transactions form blocks, which are subsequently transmitted to all nodes. The branches validate the block utilizing PoW while inserting the record to the blockchain and altering the ledger. In Ethereum, for example, an exchange may initiate a deal, which might involve the establishment of an additional record (Hu et al., 2017). The proprietor offers a confidential key, which can be regarded as a digitized signature for every interaction. This signature is verified using an examination with publicly accessible keys. The private key is impossible to lost since it is the sole evidence of title that any Bitcoin organization will permit. Once confirmed, this transaction is significant on the blockchain. The primary method of proving these exchanges is using a digging excavator, frequently known as 'Bitcoin mining'.

An excavator creates digital money by solving complex riddles to create blockchains and 'opening' virtual currency for recompense as bitcoins (Monetary Violations Authorization Organization, 2013). Digital currencies provide an immediate strategy for transactions, thereby relieving the go-between. The dispersed capacity is useful in charge of setting aside funds for cash movements, particularly settlements. These monetary forms provide for superior asset advancement without the loss of pay as installments to intermediaries or charges. Furthermore, cryptographic forms of money can perceive any computerized data as a resource, giving safeguarded innovation a more significant title. Every resource in a computerized wallet, also known as an 'e-wallet', records an exchange history.

3. Literature Review

E-commerce is a digital transaction and business-to-business mechanism. E-commerce is widely used around the world, and modern technology has dramatically improved its convenience, security, and sophistication. Cash withdrawal substitutes for online shopping encompass credit/debit PayPal payments, automatic debit payments, digital money transfers, digital wallet payments, chipped card settlements, and digital currency payments. Because both blockchain technology and cryptocurrencies are emerging industries, they can be utilized in a broad range of circumstances. [5]

Crypto is a sort of digital or virtual currency that has been encrypted utilizing cryptography. Peers redistribute it via an autonomous public ledger known as Bitcoin. The first coin was designated as Bitcoin.

Blockchain blocks are used to solve problems in a wide range of sectors. Decentralization and rigidity are two of blockchain's most important properties. Instead of storing data in a single ledger, it tries to decentralize operations so that they can be shared by all parties. It enables the establishment of a peer-to-peer networking network without the involvement of third parties. Without a third party, the process is more efficient and less expensive. Another noteworthy feature is immutability, which claims that once a contract has been formed between two or more parties or individuals, it cannot be changed. If we need to alter it, a new contract will be established and communicated over the entire network.

Because of its decentralized structure, verification will continue to be performed by other machines in the future. As a result, users enjoy exceptional security and confidence.

Blockchain technology has the potential to greatly improve efficiency in sectors that presently require costly intermediation, such as financial services. However, any implementation will be fraught with difficulty. Blockchain technology is being researched by regulators and decision-makers, notably the Committee on Payments and Market Infrastructures. They are thinking about both potential challenges and applications.

Blockchain technology can improve transparency while also decentralizing obstacles. Given its rapid adoption by the technical community, blockchain is well-positioned to be a core component, regardless of whether the future of the Internet comprises artificial intelligence, virtual reality, the semantic web, or something else entirely.

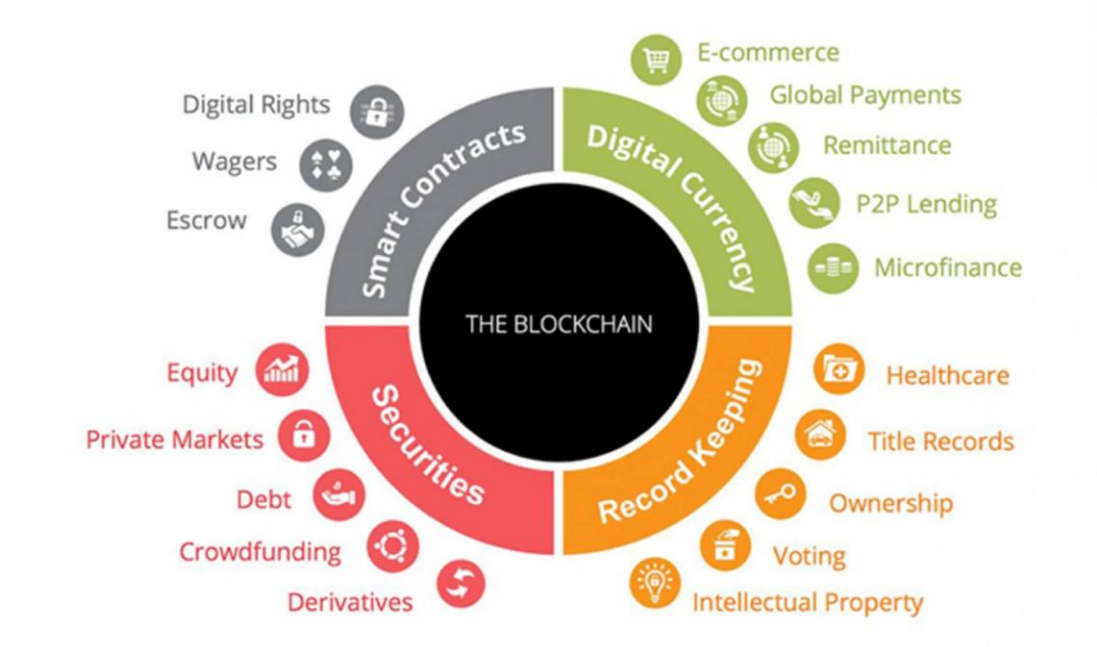

Figure 4 Sectors that use blockchain.

This section discusses background research, potential Blockchain security vulnerabilities, and alternate solutions.

Online Payment Processing in E-Commerce

During a web-based arrangement, the customer and vendor can investigate data, evaluate costs place purchases, handle settlements, and problem-solving warnings. Nearly every one of the above actions entail a high degree of authority, assurances, and confidentiality. [5] Rather than handling transactions via the internet directly, merchant websites generally employ payment gateways. Transaction pathways also known as transaction enablers, negotiate collaborations with financial institutions that handle electronic payments on behalf of their commercial accounts. the launch of PayPal, Google Purchasing, and Authorize.Net provides are among the most used e-commerce platforms worldwide (Acosta 2008). Throughout transaction execution, data involving the end user and the vendor's web ought to be encrypted.

Blockchains are used to create and store digital or virtual currency, such as cryptocurrencies. Cryptography and algorithms for encryption are used to generate, manage, and validate financial transactions. It is decentralized since neither a bank, nor the government enforces or supervises it. Peercoin, Dash, Litecoin, Ethereum, and Bitcoin are the most well-known cryptocurrencies.

Sellers gain from cryptocurrency since it is risk free, has low transaction fees, and provides identity protection. However, they are unstable because to shifting fees and their deficiency of an economic understanding.

Blockchain-based solutions and virtual currencies

Bitcoins encompass multiple types of electronic currency that are used in a range of applications, including finance and internet shopping. Blockchain serves as the basis for the core database that records Bitcoin transactions. This section discusses the principles of bitcoin, including its structure, primary elements, guiding philosophy, and distinctions from traditional systems. Cryptocurrency is a sort of digital cash that was successfully encoded using encryption. This is shared across colleagues via a decentralized records known as Blockchain. [5] Online exchanges allow you to trade cryptocurrencies for conventional currency. The conversion rates of the the globe's foremost currencies, comprising the American currency, the British penny, and euro, all of which fluctuate.

A distributed ledger is a central repository storing every single bitcoin transaction and movement, as well as property information. Every device in the cryptocurrency's programming network is managed by an association of individuals referred to as miners, and each node maintains exact duplicates of the Blockchain. Miners use cryptographic techniques to collect details of transactions, validate them, then generate new blocks. The blocks are perpetual and are inserted to the digital ledger once they are created. Every cryptocurrency owner possesses an encrypted key that they can use to exchange currencies and validate their identity (Jaag & Bach 2016). A digital ledger is a shared database that records every effective bitcoin exchange within an online system. Each block consists of numerous transactions. The original chunk is referred to as the "the formation." According to Nofer et al. (2017), each block includes transactions: [10]

The blockchain system contains several network nodes, each with its own localized version of the publicly available ledger. To form a digital ledger, networks link to other ones and establish an agreement. Consensus building is the technique used to reach this agreement. The phrase "distributed ledger" refers to the notion that whenever an item is strengthened, it appears throughout the register of each server. Once an invoice record is submitted to the Internet of Things, it is unable to be modified or deleted. Immutability is the name given to this feature.

The ability to conduct operations in the digital ledger is classified into two distinct categories: permission frameworks and authorization-less frameworks. Under a permissioned the digital ledger, transactions can only be completed by registered users. In an unrestricted environment, anyone can conduct transactions.

They can only use their data for operations ("Cloud computing Customer Design for Blockchain technology"). The technology behind distributed ledgers enables the bitcoin network to continue operating regardless of why a specific node break. As as a consequence, the network functions more consistently. The Blockchain architecture eliminates intermediaries, which improves data security. [11]

4. Blockchain: Key features

Bitcoin's fundamental components and its underpinning technology demonstrate that it does not utilize just one method, but rather an amalgamation of encryption, mathematical concepts, algorithms, and financial models, as well as a conjunction of interpersonal networks and the use of distributed consensus algorithms, resulting in absorbed multi-field establishment of infrastructure. According to Lin and Liao (2017), blockchain technology is primarily composed on the following basic elements: [6]

Distributed - Bitcoin doesn't involve a centrally located node; instead, information is able to seize, stored, and altered in an autonomous way.

- Visible recordings and chunks maintain the bitcoin network's integrity.
- The overwhelming majority of distributed ledgers are open source and are accessible.
- Individuals may examine records in public as well as develop any application utilizing Blockchain technologies.
- Independence - Consensus updates networks autonomously, reducing the need for user interaction. All of it, rather than a single individual, is entrusted with secure data transfer and upgrades.
- Records are immutable, meaning they cannot be modified unless more than 51% of nodes are controlled concurrently.
- Anonymity - Only Blockchain addresses are required for data transfer and transactions, allowing for privacy.
- Blockchain technology utilizes cloud computing systems. They allow us to use enormous quantities of storage space and can provide flexible and scalable processing resources for data analysis.
- A wallet securely stores user credentials such as ids, passwords, certificates, and encryption keys.

4.1 Multi-Currency Payment Processor

Bitcoin Payment Portal is a modular transaction network that lets clients initiate and receive payments in a variety of cryptocurrencies. The payment gateway lowers the number of parties involved in a transaction. It also plans to promote the use of digital currencies. Bitcoin payments made via such digital payment platforms are considerably more safe and less vulnerable to fraudulent transactions. Cryptocurrencies also allow for low-cost international trade in a variety of currencies among vendors, resellers, organizations, and clients. Aside from money transfers, certain centered around blockchain technology payment gateways, like Eroscion, offer an entire ecosystem. Payment gateways can also assist with the development of smart contracts. Eros currency also offers an in-chat payment function and free collaborative bulk transactions. [7]

These Blockchain payment gateways, such as Eros Coin, accept over 500 different forms of cryptocurrency. The gateway also provides convenience, speed, and cost savings. Payments to anywhere in the world are handled in 15 to 20 seconds, compared to 3 to 4 days for a regular payment gateway. The infrastructure for accepting multiple cryptocurrencies reduces the need for separate apps (Pauw 2017).

4.2 Variations across Bitcoin ledgers and Systems

Within a conventional banking system, for example, a merchant-bank record the transaction payment information in both the bank's and the merchant's databases. The issue at hand revolves around if the digital currency' contents are similar or distinct. Traditional databases can be classified into numerous types, including SQL databases, key-value retail outlets, tabular files, spreadsheets, and network stores. The records could be pooled at just one place or scattered across numerous sites and linked by a computer network. The blockchain concept is like a replicated database design. A networked database separates large information retrieval jobs and divides them into several fewer of them. A user is unaware of the information storage network topology or its propagation over many separate nodes. [7].

A distributed ledger system will refuse an exchange from a particular node when its balance was previously depleted by an additional node. This is one of the notable distinctions among systems and digital currencies.

A further unique trait of digital currencies is their ability to generate self-executing agreements. Every node may complete several challenging assignments to add an item to the the Digital Currency, while they also serve as autonomous computers throughout the system. Databases that are conventional serve as record-keeping sites rather than electronic agreements (Peters & Panayi, 2015).

4.3 Gambling using Unregulated Cryptographic Currencies

The growing popularity of digital currencies and monetary innovation brings with it connected threats posing issues concerning their feasibility and prospective participation into the economic framework, particularly regarding the lack of any pertinent standards. [12]

4.4 Underground Marketplaces

Fernandez (2012) demonstrates the way that online simulating activities or various sensible internet-based entertainment locations, such as Universe of Warcraft, have been linked to criminal activity, such as illegal tax evasion. These phases are used to conceal crimes perpetrated on the internet, costing an estimated $500 million. They mimic a financial structure intended to conceal illicit activities such as tax evasion, drug trafficking, and pornographic material involving kids (Brezo and Bringas, 2013; Bryans, 2014). As digital money payments move closer to replacing traditional fiat monetary forms, the average value of the shadow economy will almost certainly rise. This corresponds mostly since payments have evolved into extraordinarily challenging to nail through to the bitcoin holder. [12]

4.5 The Innovation Sector

As the popularity of cryptographic forms of money grows, the consequences flow over into other ventures. To mine cryptographic forms of money and create blockchains, realistic handling units (GPUs) such as realistic cards and other power-escalated figuring innovations are required. Nonetheless, as diggers plan to establish server farms, interest in The innovation has led to a cost boom for Processors. The sale of components at least doubles the recommended retail price generates a bootleg trade in the acquisition and exchange of computing and mining components (Mearian, 2018). Because NVIDIA's a graphics processor vendor, wants to sell to players compared to excavators, blockchain development is stifled because each new blockchain requires more processing power.

4.6 Utilization of Energy

The inventiveness required in generating and constructing blockchains is enormous: the Bitcoin network's construction itself utilizes roughly the same energy as Austria. According to Dichotomist, the entire Bitcoin organization utilizes 73 terawatt-hours (73 million megawatt-long stretches) of electrical power,4 while the platform's usage has been put at 15.92 terawatt-hours, a figure that is similar to the Dominican Republic's consumption.5. This raises a problem. Due to the fact that when cryptographic forms of money become more commonly recognized and expenses reach $50,000, the accompanying energy usage may climb 10,000. Indeed, as bitcoin mining innovation improves, as monetary requirements increase, usage of energy may escalate to the point where excavators might turn unproductive (Hern, 2018). This could be a major concern for centers of authority in every nation, and it may prove impractical if an unfathomable network emerges.

4.7 Tax Evasion and Assessment

At a larger scale, countries like the United States of America, Germany, and Chinese were probably the initial nations to initiate steps regarding encrypted forms of payment. Germany considered placing a levy on digital money as a capital resource once it was recognized in 2013/14. Even lately, the German financial institution has invested in bitcoin. Six Likewise, in the Chinese mainland, in response to growing concerns about innovation, the state-owned bureau has implemented steps to rein in cryptographic forms of money by limiting their underlying currency contributions (van Steenis). With the increasing use of cryptographic forms of money as transaction mechanisms, fraud in the payment of taxes has emerged as a major concern for governments around the world. [8]

Marian (2013) underlines two crucial features of these monetary forms that operate through unlawful transactions. To begin, there certainly is no limit to the number of wallets that clients may possess, enabling them to exchange while not giving any identifiable details regarding the owner. Furthermore, with regard to the concept of monetary standards, clients refrain from using monetary facilitators. Despite the swift increase of cryptographic forms of money, state-run administrations in countries such as Germany and China have attempted to regulate them by levying fees and enforcing boycotts on the offering of initial coin offerings (ICOs) (Wildau, 2017). The United States of America must try to address this problem by incorporating these

monetary standards into the regulations for cash communication companies, particularly Segments 1960 and 5313 of the U.S.

Marian (2013) emphasizes two key characteristics of these monetary forms that operate through illegal transactions. To begin with, there is no limit to the number of wallets that clients can maintain, allowing them to exchange without disclosing any information about the owner. Second, according to the concept of monetary standards, clients do not rely on monetary intermediaries. Given the rapid development of cryptographic forms of money, state-run administrations in Germany and China have sought to control them by imposing assessments and boycotts on initial coin offerings (ICOs) (Wildau, 2017). The US government must take measures to address this situation by incorporating these monetary standards into the laws for cash communicating companies, particularly Segments 1960 and 5313 of the U.S.

Without proper guidelines, digital currencies, and their ability to function as expense safe houses might completely undermine authorities' efforts to reduce tax evasion (Marian, 2013; Grinberg, 2012). The Unfamiliar Records Assessment Consistency Act is one such US initiative that was drafted in 2010 and began to be gradually implemented in 2014. It compels unknown monetary foundations ... notify a few the United States national client through the Fiscal Service (Marian, 2013).

Within January of 2018, Steven Mnuchin, the Depository's Administrator, indicated that the Monetary Solidity Monitoring Board was going to tackle the developing digital financial system and develop requirements to prevent the creation of a computerized Swiss record elective. He also indicated that his major purpose aimed to avoid illegal transactions from taking place using these financial standards (Nelson, 2018). In August 2017, the Canadian Protections Executives released a statement suggesting that digital currencies may be subject to Canadian Protections regulations. In any case, the head of the Canadian National Bank described digital currencies as 'basically theoretical' in January 2018. [11]

Canada has joined a preventative mandate as a member of the North American Protection Directors Association, whose delegates believe digital forms of money to be extremely dangerous. Given the acceleration of positive thinking shown in Ethereum and Wave, among other digital forms of money, the European National Bank has also elevated digital forms of money on its priority list. A few board participants, particularly Yves Merch, have expressed

alert about the flood, asserting that such 'extremely risky resources' have a huge mental and social impact, analogous to a race for unheard-of wealth, but with almost no true resource support (Megaw, 2018).

5. Research Methodology

The systematic plan for conducting research is outlined in the research methodology. It explains Where the data set, measurements, and inspection interact to meet the investigation's objectives. The next subsection outlines the research process, including the data sources, methods to gather data, along with information analysis techniques. This study sheds light on the use of bitcoins in online retail online payments.

5.1 Qualitative and Quantitative Research

The A questionnaire is going to be used to gather public comment about their understanding of digital currencies, the associated confidentiality and security risks, and their impression of bitcoins as an investment option. The reactions are quantified to figure out if bitcoins are preferred primarily a safe method of payment and financial option.

5.1.1. Qualitative Approach

The qualitative evidence are papers, phrases, and tones gathered through people or reading. Throughout this study, bitcoin clients' responses are completely digits regardless of text-based information acquired. Additionally, supplemental research is carried out upon predetermined themes involving Bitcoin safety issues and Blockchain innovation usage. precisely an outcome, the subjective approach of gathering info was skipped over in the current research. Nevertheless, supplemental evidence is subjectively assessed to support and rebut individual responses, along with react to investigations concerns on safety concerns and abuse of the distributed ledger system. [13]

5.1.2. Quantitative Method

Quantum information is made up of quantifiable items, amounts, and metrics that are expressed quantitatively. The responses to the questionnaire are recorded quantitatively. These reactions are assessed in light of current research, yielding applicable perspectives and conclusions. The idea of the investigation seeks to discover patterns concerning the issues that Bitcoin users face, whether they are new or seasoned. [14]

5.2 Data Collection Methods

It is an organized manner of gathering data regarding the subjects in order to respond to specific inquiries from studies. The acquisition of information is divided into two distinct groups: firsthand information and secondhand information. First data are distinctive because they were collected spanning the preliminary time. [7]

Core data is collected by instruments like polls, forms, phone calls, email messages, and oral interviews, in which feedback from participants are captured, categorized, then assessed. Supplementary data is obtained from already accessible sources that include newspapers, magazines, online platforms, and more ("Data Collection" 2017). This study requires an accumulation of data from both primary as well as secondary sources.

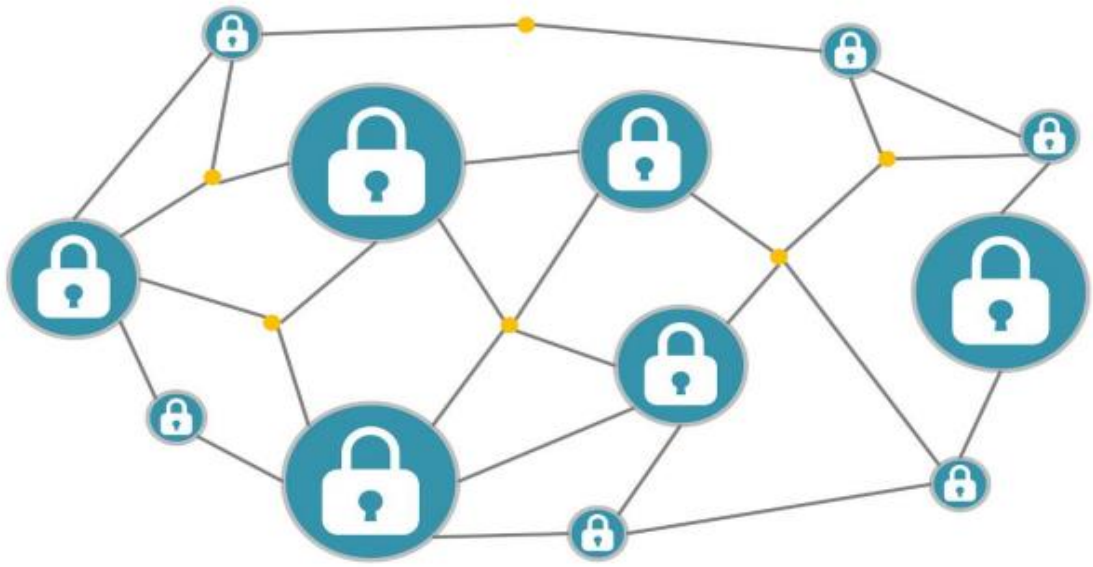

Figure 5- Data Encrypted [15]

Initial collection of information can be either qualitative or quantitative in nature. Quantitative techniques are based on computations with closed-ended questions as inputs. Qualitative research methods concentrate on non-quantifiable factors such as syllable and feelings rather than mathematical computations ("Data Collection" 2017). This study's data gathering approach relies on a sealed-ended survey with numerical responses.
The questionnaire will also enable respondents to provide qualitative input. As a result, research techniques that are qualitative as well as quantitative are going to be utilized in the current research. [16]

In addition to the questionnaire, this research project gathers secondary data from literary works, publications, newspapers, and various additional sources. The material includes suggestions to utilize Bitcoin providing a virtual payment medium, as well as solutions to security issues related with Blockchain transactions and attacks. Literature on expanding the use of The uses of Blockchain technology as a form of payment medium, hazards and opportunities for platforms that rely on the system, as well as techniques for preventing Blockchain misconduct are also discussed.

6. Blockchain and GDPR

The European Association's Overall Information Security Guideline (GDPR) is a piece of policy designed to protect the personal information of EU residents. It went into effect on May 25, 2018, And it rendered it illegal against businesses to possess personal information on individuals who reside in the EU unless they are approached to have it eliminated. However, the indestructibility of digital currencies implies that it's extremely difficult to meet those standards. Essentially, given that information is permanently erased off digital currencies and is freely available to everyone who has permission to the ledger.

Figure 6 -Blockchain and GDPR [17]

Both have been designed as the best course of action when major organizations as well as institutions cannot be relied upon to refrain from abusing their authority or acquiring data. As a result, the two are not necessarily antagonistic. The use of Blockchain can also be viewed as a helpful resource in information security operations. The key to making blockchains conform to GDPR resides in innovation and the development of a blockchain version with an immutable nature but the ability to forget information. There is a noticeable difference between open and private blockchains, particularly in terms of responsibility. Because no one has formal authority across distributed ledgers, platforms are not recommended for use to store private data. [14]

Regardless, private, or permissioned blockchains have a few options. Conventional information bases use the Make Read-Update-Erase paradigm for tasks, together with the typical capabilities that we expect from an information base architecture. Some GDPR-

compliant blockchains have been proposed, and they typically use a Make Recover Add Consume approach. It implies that it is tough to refresh and wipe information, but you may attach and consume individual bits of information. What is the distinction where the consumer part is generally intriguing from a GDPR perspective? Between consuming and deleting information? One method to decipher consumer conduct is to look at it as discarding encryption. [18]

keys making it impossible to unscramble the actual information published in the blockchain. Thus, the information remains in the blockchain, but it is, in practice, unsuited for reading because no one possesses the unscrambling key. This approach is sometimes referred to as cryptographic information erasure, which implies that the information remains on the communicated chain but cannot be deciphered and exploited. Another method for The development of GDPR-compliant platforms involves the usage of referred to as intermediary chains instead of main chains. This implies because this information is kept in an external data set and then linked to the blockchain via a combination of private and public keystrokes for encryption.

The above method of preserving data is also beneficial for a variety of purposes, as it prevents the blockchain from growing to such a large size with each block. In contrast to actual information, each block contains connections to information. As a result, it is not recommended to retain individual data on the actual chain.

The effects of GDPR have not yet been determined, and the degree and severity of the penalties have not been publicly tested at this time.

6.1 Review the implications of crypto assets

There are numerous review options for businesses that have either purchased or created cryptocurrency assets for their operations. In this section of the discourse, we will investigate the review's impact on how such resources are treated in the accounting report. This has significant implications for both internal and external inspections within the company. As part of this discussion, we would expressly focus on the impact of considering these resources on the monetary record for external reviewers. Nonetheless, some of the conclusions reached here may have a basis for the interior examiners. [19]

The primary implications for outside examiners are connected to assessing the value of these resources after some time. We accept that examiners must use extra caution when determining whether the valuations of crypto assets recorded on the balance sheet are accurate considering the necessary concealed assumptions. In addition, there are several evaluation ideas on the obviousness and thus the conclusion of these kinds of resources. In general, we believe that valuation for crypto assets may be a significant risk due to the multiple assumptions and judgments involved. Presence and fulfillment can also be extremely risky affirmations because the underlying data used to determine if resources exist is extremely emotive and hence susceptible to critical predisposition by executives.

As part of the legal review, external evaluators must provide reasonable confirmation that the financial reports are free of material misquotations. To properly evaluate crypto assets, assessors must understand the inherent and control risks associated with these records and organize their evaluation strategies accordingly. As previously stated, there are numerous suggestions regarding the culmination and valuation affirmations of cryptocurrency assets. That is, organizations and their outside reviewers would have significant difficulty determining the right value of these resources over time. For the sake of reducing the risk of errors, companies would most likely want to implement appropriate internal controls to prevent material errors. [20]

For crypto assets, similar controls would entail a higher level of multistage surveys of the assumptions used in the assessment of the benefits of these resources.

Furthermore, supplementary controls would be in place to ensure that the valuations of these

resources were accurate. Nonetheless, it is unlikely that these restrictions will be effective given the large number of judgments made during the valuation step. Based on this and our fundamental hypothetical assessment of the bookkeeping treatment for crypto assets, we believe that the control probability is high to medium. To the extent that the location risk, we trust that to ensure location risk is reasonably low, the examiners need to design more, and additionally, perform incredibly effective review strategies to ensure that the overall risk of material error is reduced to an acceptable level. To do this and reduce the risk to an acceptable level, reviewers may need to incorporate large costs for third-party valuation specialists after some time. However, over time, their contributions would raise the review's overall cost. As a result, there are numerous cost ideas for outside examiners to consider when considering bringing in a new client or continuing with review administrations for current clients.

6.2 The Tax implications of virtual currency

It's exciting to watch how the Internal Revenue Service (IRS) will tax and track digital currency compliance. On the 25th of March 2014, the IRS published Notice 2014-21. in which it investigated sixteen cases and sought clarification on critical problems, providing some guidance on how individuals should regard the transaction or trade of cryptocurrency. According to it, cryptographic money (such as Bitcoins, Litecoin, and others) is "property," hence The identical tax regulations that govern property purchases are also applicable to purchases involving digital currencies.

According to Inward Income Guideline Segment 1.1001-1, "the addition or misfortune understood from the transformation of property into cash, or from the trading of property for other property that differs physically either in kind or in degree, is treated as pay or then again as misfortune supported." The amount recognized from a deal or other exchange of property is the sum of any cash received as well as the honest evaluation of any property (other than cash) received" (U.S. Depository, 2018). Furthermore, any property held for exactly one year or less is considered traditional pay and will be paid at the highest individual rate. [21]

Finally, each time a citizen withdraws cryptographic money, it is considered a transaction or exchange. As each is considered a separate transaction, in the unlikely event that a citizen exchanges, sells, or buys a thousand unique items, there will be 1,000 opportunities. The inventor believes that cryptographic money should be classified as "property" under Internal Revenue Code (IRC) Section 317(a) (I.R.C., 1986a) and other substantial areas. The basis for this viewpoint is that cryptographic money is not supported by any sovereign government and is insufficient in all other respects.

Prior to the part of President Trump approved the legislation known as the Tax Cuts and Jobs Act (TCJA) on December 22, 2017, citizens could treat the deal or trade of cryptographic money as a resource that met all the standards for charge deferral under IRC Area 1031(a). This deferral allowed the citizen to postpone accepting the expense gain or loss until a later time. In essence, according to the previous rule, the citizen may have accepted this increment from now until eternity (I.R.C., 1986b). If a citizen exchanged one digital money for another, it would be considered a 1031 resource. The TCJA revamped IRC 1031, now allowing residents to concede gain or loss on business resources that are considered as real.

7. The Conclusions and the Future Work

Blockchain has grown into a method of electronic payment throughout the course of time from its humble beginnings as digital tokens. The current article examined one facet of its usage: online retailers' payment. Transaction with bitcoin, like ordinary payment via the internet, presents difficulties, among which significant of which are safety issues. The main security risks were identified and investigated in the peer-reviewed review. [9] Remedies regarding privacy issues have been investigated employing publications and presented provided study results.

The research employed a survey on digital currency to assess whether individuals are eager to use them as well as why they are unwilling. The findings revealed that people's unwillingness to accept cryptocurrencies for applications is primarily due to security concerns and the fact that digital currencies are not legal tender. A centralized worldwide regulatory authority is needed to address Blockchain technology abuses. The introduction of global authority is going to alleviate worries that bitcoins are not accepted as currency. People's investments in cryptocurrencies are hampered by the fear of illegitimacy, and a central governance mechanism will assist to alleviate these anxieties and attract investment. [21]

The study used a cryptocurrency questionnaire to determine how eager people are to use them and why they are unwilling to do so. The findings revealed Safety issues and the fact that electronic currencies are not officially recognized currencies Are the primary reasons why individuals are hesitant to use cryptocurrencies for apps. A centralized worldwide regulatory authority is the solution to abuses of blockchain technology. The existence of universal governance will allay concerns about cryptocurrencies not being legal tender. People's investments in cryptocurrencies are hampered by the fear of illegitimacy, and a central governance mechanism will assist in alleviating these anxieties and attract investment. [18]

The responses cited security concerns for the top factor for users' hesitation to utilize digital currencies when a form of payment. Remedies are constantly established, so enacting suitable solutions is going to alleviate this situation.

A different field of study deals with how bitcoins have an uncertain the years to come, that is influenced by the views of individuals of them as a viable investment. The concept of investing

wasn't received properly with the respondents. Respondents cited safety issues and the fact that virtual money is not recognized as currency as the primary justifications for refusing to invest in digital currencies. [5]

Safety concerns have been addressed previously within this chapter. Appropriate regulations as well as global legislation are going to turn bitcoins into a trustworthy and reliable currency that individuals are going to be reluctant to spend.

References

[1] I. Papers, "EconPapers," 2008-05. [Online]. Available: https://econpapers.repec.org/RePEc:ess:wpaper:id:1471.

[2] P. Luca, "Cryptocurrencies and tokenization of assets: the managerial implications of a new financial reality," 21-Apr-2022. [Online]. Available: http://hdl.handle.net/11144/5416.

[3] Pkamau, "Course Hero," Mt. Kenya University , [Online]. Available: https://www.coursehero.com/file/206686609/Blockchain-technology-is-a-decentralized-and-distributed-ledger-system-that-allows-multiple-parties/.

[4] [Online]. Available: https://www.businessworldit.com/blockchain-cryptocurrency/blockchain-in-finance/.

[5] L. R. Z. M. C. G. O. B. W. J. Dinh TTA, "Untangling blockchain: a data processing view of blockchain system," *IEEE Trans Knowl Data Eng,* no. https://doi.org/10.1109/Tkde.2017.2781227, 2018.

[6] [Online]. Available: https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/.

[7] S. A. Ron D, "Quantitative analysis of the full bitcoin transaction graph," in *international conference on financial cryptography and data security*, 2013.

[8] L. L. C. W. Z. D. Liang J, "Targeted addresses identification for bitcoin with network representation," in *In: 17th IEEE int. conf. Intell. Secur. Inf.*, Shanghai, China, 2019.

[9] D. K. Sahu, "Introduction to Blockchain," 2022. [Online]. Available: https://www.digitalvidya.com/blog/introduction-to-blockchain/.

[10] B. J. F. E. M. A. G. S. Narayanan A, "Bitcoin and cryptocurrency technologies: a comprehensive introduction," in *Princeton University Press*, 2016.

[11] "Blockchains: The great chain of being sure about things," The economist, 31 oct 2015.

[12] H.-H. R. S.-H. L. a. X.-J. J. Xiao Fan Liu, "Characterizing key agents in the cryptocurrency economy through blockchain transaction analysis," *EPJ Data science,* p. 13, 2021.

[13] D. G. C. J. W. D. B. C. R. T. L. C. Weber M, "Anti-money laundering in bitcoin: experimenting with graph convolutional networks for financial forensics.," *Cornell University,* p. 7 pages, 2019.

[14] M. W. Y. I. S. N. A. A. Z. Aurangzeb, " Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage," Energy Reports 11 , 2493, 2024.

[15] D. Kingori, "How To Boost Cyber Security with the Blockchain," 2019. [Online]. Available: https://www.paymentsjournal.com/howboost-cyber-security-with-the-blockchain/.

[16] M. P. O. T. Toyoda K, "A novel methodology for hyip operators' bitcoin addresses identification," *IEEE conference,* 2019.

[17] A. Pery, "The Tension between GDPR and Blockchain," 2019. [Online]. Available: https://www.abbyy.com/blog/the-tension-between-gdpr-and-blockchain/.

[18] C. Adams, "Online Payment Process, E-Business technologies," 2018. [Online]. Available: https://www.investinBlockchain.com/cryptocurrency-forks..

[19] D. W. Wadho and A. Ellahi, "DSpace RepositoryCorruption, Tax Evasion and Economic Development in Economies With Hierarchial Tax," 2019-02. [Online]. Available: http://hdl.handle.net/123456789/17132.

[20] K. S. N. Adewole, "Application of cryptocurrencies using Blockchain for e-commerce online payment.," *Blockchain for Cybersecurity and Privacy: Architectures, Challenges and Applications, C&C Press, Taylor & Francis Group, pp. 263-306,* 2019.

[21] K. Kwang, Blockchain for cybersecurity, NW: CRC publisher, 2020.

[22] A. K. Singh and . Q. Sidharth, "A systematic survey on security concerns in cryptocurrencies: State-of-the-art and perspectives," *Science Direct,* p. 60, Feb 2022.

[23] C. R. Garg, "IMPORTANCE OF E-COMMERCE PAYMENT SYSTEM," ISSN: 2349-5677 , April 2016.

[24] A. B. M. S. B. Akhtar, "Blockchain based auditable access control for business processes with event driven policies.," 2024.