Blockchain Development, Architecture, Prospects, Applications, Difficulties, and Future Directions

KA Hossain, Ph.D.

DOI: 10.31364/SCIRJ/v11.i10.2023.P1023970
http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

Abstract: A blockchain is a distributed database or ledger that is shared amongst a computer network's nodes. In an effort to address the 2008 European financial crisis, Satoshi Nakamoto suggested using blockchain technology for Bitcoin. Numerous more applications as well as cryptocurrencies like Bitcoin are supported by this technology. Satoshi introduced Bitcoin as a new form of payment that uses a blockchain—a cryptographically secure chain of interconnected data blocks—to do away with central authorities like central banks. This method was initially applied to cryptocurrencies, with Bitcoin demonstrating its viability. These days, blockchain technology has numerous uses, some of which are covered in this paper. Ether, like with many other cryptocurrencies, is built on top of blockchain technology. The current market capitalization of cryptocurrencies is $2.79 trillion, which is equal to the eighth largest economy in the world. Every day, 30,000 postings on social media about Bitcoin are put online. This translates to 1500 posts every hour or 30 posts every minute. Blockchain technology has limitations and difficulties that prevent its complete acceptance in some domains, despite its promise, prospects, strength, and success. This article discusses these issues. The goal of this thorough study is to analyze how blockchain technology is used in different application contexts and to assess its prospects, difficulties, features, and future directions.

Key words: AI, NFTs, P2P, DLT, blockchain, bitcoin, Ethereum, Cryptocurrency

Introduction: A blockchain is a series of blocks that each contain a unique piece of information. As a result, a blockchain is a file or ledger that is always expanding and permanently storing the history of every transaction.[1]This process proceeds in a methodical, absolute, and safe manner. A new block is created each time an informational block is finished being stored.[2]The scientists Stuart Haber and W. conducted research in 1991. Blockchain technology is introduced by Scott Stornetta. These scientists were looking for a workable computational method to time-stamped digital documents, preventing them from being tampered with or incorrectly dated. Thus, using cryptography, the two scientists worked together to create a system. The time-stamped documents in that system is kept in a Chain of Blocks.[3] Stefan Konst released his theory of cryptographic protected chains along with implementation ideas in 2000. Following that, in 2008, Satoshi Nakamoto introduced the idea of "Distributed Blockchain" as a "Peer to Peer Electronic Cash System" in his white paper. He made changes to the Merkle Tree architecture to produce a more secure system that includes a safe history of data exchange.[4] Actually, 2014 is regarded as the year that blockchain technology turned a corner, separating itself from money to create Blockchain 2.0.[5] Financial institutions and other sectors began refocusing their attention from digital currency to the advancement of blockchain technology.[6] Japan acknowledged Bitcoin as a legitimate currency in 2017. 2018 was the tenth anniversary of Bitcoin, which was first released by Block.one as the EOS blockchain operating system, intended to facilitate commercial decentralized applications.[7] The value of bitcoin kept declining, and at the end of the year, it was only worth $3,800.[8] Digital media giants such as Facebook, Twitter, and Google have outlawed cryptocurrency advertisements. Once more, over a million Ethereum network transactions occurred daily in 2019. Amazon declared that their managed Blockchain solution on AWS is now generally accessible.[9]Ethereum's consensus process has changed from Proof of Work (PoW) to Proof of Stake (PoS). The PoS-enabled Beacon Chain and the original Ethereummainnet combined. It currently exists as a single chain.[10] The energy usage of Ethereum has decreased by nearly 99.9%.[11,12] In 2020, the market value of cryptocurrencies worldwide was estimated to be around $1000 million. With a 30% compound annual growth rate, the cryptocurrency market is predicted to reach $5,190,62 million by 2026. According to reasonable estimations, the size of the global cryptocurrency market in 2020 will be $1500 million. At a CAGR of 11.2%, it is projected to reach $1,758 million by 2027. Dogecoin experienced a sharp increase in value in 2021 due to remarks expressing its immense potential. Elon Musk, the CEO of Tesla, earned $5.35 in January 2022.

Blockchain can alternatively be defined as a series of blocks that together hold some specified information.[13]This is a chronological, safe, and unchangeable process. A new block is created every time a block of data is finished being stored.[14] Blockchain, a distributed ledger technology (DLT), is a collection of records with sequential time stamps. This decentralization technology has developed into a potent, verifiable methodology for building confidence between entities that lack trust. Blockchain-enabled edge intelligence is an

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

emerging technology for the Internet of Things (IoT), driven by the recent advancements in artificial intelligence (AI) and multi-access edge computing (MEC).[15] By 2030, Europe hopes to see $500 billion invested in blockchain projects. Industry and research communities have long predicted that blockchain technology will be challenging to use but crucial for managing, controlling, and most importantly, securing IoT devices. When it comes to offering workable security solutions for current difficult IoT security issues, blockchain technology can be a crucial enabler.[16]IoT devices are weak and unable to defend themselves in the modern world. The primary causes of this are the limited resources in Internet of Things devices, the lack of mature standards, and the inability to design, develop, and implement secure hardware and software. The diversity of resources in IoT is also impeding efforts to define a strong worldwide strategy for protecting the IoT layers. Blockchain technology has the potential to fix this. Many security flaws and privacy issues arise from the present IoT systems' absence of intrinsic security measures. A distributed, decentralized technology like blockchain proves to be a workable answer in this regard.[17]

By facilitating decentralized record keeping and making data accessible as needed, blockchain technology has the potential to fundamentally alter the way healthcare is administered. Additionally, with the aid of this technology, medical professionals will be able to quickly and thoroughly learn about patient cases, allowing for speedier treatment times and fewer waiting periods between the collection and interpretation of data.[18] Researchers have found numerous applications of blockchain in various business, industry, services, technology, and innovative sectors, including finance, management, defense, automotive, stock exchange, IoT, voting, public and social services, reputation system, healthcare, education, energy, agriculture, law enforcement, asset tracking, insurance, cyber-security, advertising, security and privacy, digital record, etc. Additionally, due to its immutable qualities, blockchain can also prevent the circulation of fraudulent drugs and treatments. Nonetheless, there are two main advantages to integrating blockchain with services computing: first, it may be able to address some of the major issues facing services computing, and second, it may encourage the growth of blockchain technology. Today, there are many new issues brought about by the growth of services computing. Blockchain has limitations in a few areas, including security, privacy, and scalability, despite its strengths. Numerous advantages of blockchain technology include decentralization, persistency, auditability, and anonymity.[19] Blockchain has a wide range of applications, including cryptocurrencies, risk management, financial services, Internet of Things, public and social services, artificial intelligence, healthcare, and industrial. There is a fairly thorough evaluation and study on the blockchain technology from both a technological and application standpoint, even though many studies concentrate on implementing the technology in different application aspects.

All committed transactions are recorded in a series of blocks that make up blockchain, which may be thought of as a public ledger. When fresh blocks are added to this chain, it keeps growing. By combining multiple fundamental technologies, including distributed consensus mechanisms, digital signatures, and cryptographic hashes, blockchain technology may operate in a decentralized setting. A transaction can happen in a decentralized way using blockchain technology. Blockchain can therefore significantly reduce costs and increase efficiency. Globally, blockchain technology is becoming more and more popular among businesses and nations. Blockchain is currently revolutionizing a number of industries, including AI, IoT, finance, healthcare, supply chain, insurance, and registry. To take advantage of the benefits of blockchain technology, many businesses integrate it with their systems. The author has attempted to provide a thorough overview and analysis of blockchain technology in this paper, highlighting its origins, history, architecture, potential, prospects, applications, uses, obstacles, and future. This research employs an analytical approach, utilizing primary and secondary data, to assess the advancement, potential, and obstacles of Blockchain technology, as well as its future prospects. Industry, services, health, banking, finance, management, and other advanced technical industries will benefit from the study's findings.

Blockchain's Background and History

One kind of distributed ledger technology is blockchain technology (DLT). A distributed ledger functions as a digital data recorder, sharer, and synchronizer. A network of computers shares and replicates this database. The information or entries in the ledger can be updated by network participants. It functions without requiring a centralized authority. Blockchain arranges data into immutable blocks that are joined together. Blockchain makes use of cryptographic hashing and decentralization. This contributes to the unchangeable and transparent history of any digital item. But in his 1982 dissertation, "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups,[21] " David Chaum[20] initially proposed a blockchain-like protocol. Stuart Haber[22] and W. Scott Stornetta[23]detailed their subsequent work on a cryptographically protected chain of blocks in 1991. Stornetta Scott. Their goal was to put in place a system that would prevent tampering with document timestamps.[24] WhenMerkle trees were added to the architecture in 1992 by Haber, Stornetta, and Dave Bayer[25], it became more efficient because several document certificates could be gathered into a single block.[26] Since 1995[27], their document certificate hashes under the name Surety have been published in The New York Times every week. In 2008[28], a person or group of persons going by the name of Satoshi Nakamoto came up with the idea for the first decentralized blockchain.[29] By timestamping blocks without needing them to be signed by a third party and adding a difficulty

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

parameter to control the pace at which new blocks are added to the chain,[30]Nakamoto made significant improvements to the system. The next year, Nakamoto put the design into practice as a fundamental part of the cryptocurrency bitcoin, where it acts as the network's public ledger for all transactions.[31]

The size of the bitcoinblockchain file, which contains a history of every transaction made on the network, surpassed 20 GB in August 2014.[32]The size of the bitcoinblockchain increased from 50 GB to 100 GB between January 2016 and January 2017. In January 2015, it had grown to around 30 GB. By early 2020, the size of the ledger had surpassed 200 GB.[33] Although block and chain were used separately in Satoshi Nakamoto's original paper, they eventually became popularized as a single word, blockchain, by 2016.[34] According to Accenture, the diffusion of innovations theory applied to financial services indicates that blockchains reached the early adopters' phase in 2016 with a 13.5% adoption rate.[35,36] In 2016, the Chamber of Digital Commerce organized industry trade groups to form the Global Blockchain Forum.[37] According to a May 2018[38] Gartner survey, only 1% of CIOs said their organizations were adopting blockchain technology, and only 8% said they were "planning or [looking at] active experimentation with blockchain" in the near future.[39] According to a 2019 Gartner report, 5% of CIOs thought blockchain technology would "change the game" for their company.[40]

According to Nakamoto, the writing of the Bitcoin code started in 2007.[41] He or a colleague registered bitcoin.org as a domain name and set up a website at that address on August 18, 2008.[42] Entitled "Bitcoin is a Peer-to-Peer Electronic Cash System"[43]Nakamoto published a white paper on October 31 on the metzdowd.com cryptography mailing group.[44] In order to start the network, Nakamoto published version 0.1 of the Bitcoin software on SourceForge on January 9, 2009. This block, known as block number 0[45], carried a reward of 50 bitcoins.[46]The statement "the Times 03/Jan/2009 Chancellor on brink of second bailout for banks" is embedded in the coinbase transaction for this block. It references a headline from the UK newspaper The Times that was published on the same day.[47] This note has been read as a mocking reference to the supposed instability brought about by fractional-reserve banking as well as a timestamp.[48] Nakamoto worked on the Bitcoin program with other engineers until the middle of 2010, personally making all changes to the source code.[49] After that, he stopped being officially involved in the project, handed Gavin Andresen ownership over the source code repository and network alert key,[50] and moved a number of associated domains to other well-known members of the bitcoin community.[51]Nakamoto is the owner of between 750,000 and 1,100,000 bitcoin. When Bitcoin reached its peak value of more than US$68,000 in November 2021, he would have become the 15th richest person in the world with a net worth of up to US$73 billion.[52]

A cryptocurrency, often known as a crypto, is a type of digital currency[53] that operates independently of a central bank or government and is intended to be used as a medium of trade over a computer network.[54] It is a decentralized system for verifying that the parties to a transaction have the money they claim to have, eliminating the need for traditional intermediaries, such as banks, when funds are being transferred between two entities.[55] Individual coin ownership records are stored in a digital ledger, which is a computerized database using strong cryptography to secure transaction records, control the creation of additional coins, and verify the transfer of coin ownership.[56.57]Despite their name, cryptocurrencies are not considered to be currencies in the traditional sense, and while varying treatments have been applied to them, including classification as commodities, securities, and currencies, cryptocurrencies are generally viewed as a distinct asset class in practice.[58,59] Cryptocurrency does not exist in physical form (like paper money) and is typically not issued by a central authority.[60]Cryptocurrencies typically use decentralized control as opposed to a central bank digital currency (CBDC).[61] When implemented with decentralized control, each cryptocurrency works through distributed ledger technology, typically a blockchain that serves as a public financial transaction database.[62]

A company that lets clients swap cryptocurrencies or digital currencies for other assets, including traditional fiat money or other digital currencies, is known as a cryptocurrency exchange, or digital currency exchange (DCE). Usually, a user's personal cryptocurrency wallet can receive cryptocurrency transfers via cryptocurrency exchanges. While some digital currencies are backed by real-world commodities like gold, others can transform their balances into anonymous prepaid cards that can be used to withdraw money from ATMs all around the world.[63] The people who create digital currencies are usually not associated with the exchange that allows trading in the currency.[64] To recap, a cryptocurrency wallet is a hardware, software, or service that keeps track of the public and/or private keys used in cryptocurrency transactions.[65]Again, a cryptocurrency wallet is a device,[66] physical medium,[67] program or a service which stores the public and/or private keys[68] for cryptocurrency transactions. A cryptocurrency wallet typically has the ability to encrypt and/or sign data in addition to its primary purpose of storing keys.[69]Bitcoin was first introduced in 2008 and was based on the principles described by Satoshi Nakamoto in the paper "Bitcoinasa Peer-to-Peer Electronic Cash System".[70] The project was marketed as an electronic payment system that relies on cryptographic proof rather than trust. Additionally, it discussed the use of cryptographic proof to confirm and log transactions on a blockchain.[71] Vulnerabilities in wallets might be either known or undiscovered. Vulnerabilities can be introduced by a side-channel attack or a supply chain assault. In extreme circumstances, it is possible to hack a machine that is not connected to any network.[72] The first cryptocurrency was called Bitcoin, and it was first made

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

available as open-source software in 2009.[73] More than 25,000 other cryptocurrencies were available in the market as of June 2023, with over 40 of them having a market capitalization of $1 billion or more.[74]

An Overview of Cryptocurrency and Its Historical Development

The symbol for bitcoin is ₿, and it is a type of decentralized digital money.[75] The currency codes for bitcoin are BTC and XBT.[76] Network nodes use cryptography to verify transactions, and the records are stored in a publicly accessible distributed ledger known as a blockchain.[77] The term "bitcoin" was defined in a white paper published on October 31, 2008;[81] it is a compound of the words bit and coin.[82] According to the Library of Congress, as of November 2021, nine countries have fully banned the use of bitcoin, and a further forty-two have implicitly banned it.[83] In contrast, a few governments have used bitcoin in some capacity.[84] The cryptography was invented in 2008 by an unknown entity under the name Satoshi Nakamoto.[78] The currency began use in 2009.[79] For instance, El Salvador has made Bitcoin legal tender, yet few businesses actually utilize it.[80] Iran has used bitcoin to get around political sanctions, and Ukraine has accepted bitcoin donations to fund its resistance to a Russian invasion in 2022. At least eight Nobel Memorial Prize winners in Economic Sciences have called bitcoin an economic bubble[85], and its effects on the environment are significant.[86] As a result of the computational difficulty of its proof-of-work algorithm, mining bitcoins has increased electricity consumption, which has contributed to climate change.[87] The University of Cambridge estimates that since its launch, bitcoins have released 200 million tonnes of carbon dioxide,[88] or approximately 0.04% of all carbon dioxide released since 2009.[89]

Figure 1: The world's most popular cryptocurrencies[91] and the cryptocurrency revolution[90]

You may divide one bitcoin to eight decimal points.[92] The lowest division of bitcoin, called after its creator, the satoshi (sat), represents 1⁄100000000 (one hundred millionth) bitcoin.[93] One mBTC is equivalent to 100,000 satoshis. The millibitcoin (mBTC), which is equivalent to 1⁄1000 bitcoin, is the unit of measurement for smaller amounts of the cryptocurrency.[94] A public ledger called the bitcoin blockchain keeps track of all bitcoin transactions.[95] It is implemented as a series of blocks, each of which has a cryptographic hash of the one before it, all the way up to the chain's genesis block.[96] The blockchain is maintained by a network of nodes that communicate and run bitcoin software.[97] Transactions of the type payer X pays Y bitcoins to payee Z are broadcast to this network via easily accessible software applications. Network nodes have the ability to verify transactions, append them to their ledger copy, and subsequently disseminate these ledger additions to more nodes.[98] Every network node has a copy of the blockchain on hand to enable independent verification of the ownership chain. Without the need for central management, a new block—a collection of approved transactions—is generated, uploaded to the blockchain, and promptly disseminated to every node at irregular intervals that average around every ten minutes. In order to avoid double-spending, this enables bitcoin software to track when a specific bitcoin was spent.[99] As a digital ledger, bitcoins are only possible because of the blockchain; they are represented by the unspent outputs of transactions. In contrast, a traditional ledger records the transfers of real banknotes or promissory notes that exist independently of it.[100] With a blockchain explorer, one may look at specific blocks, public addresses, and transactions inside blocks.[101]

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

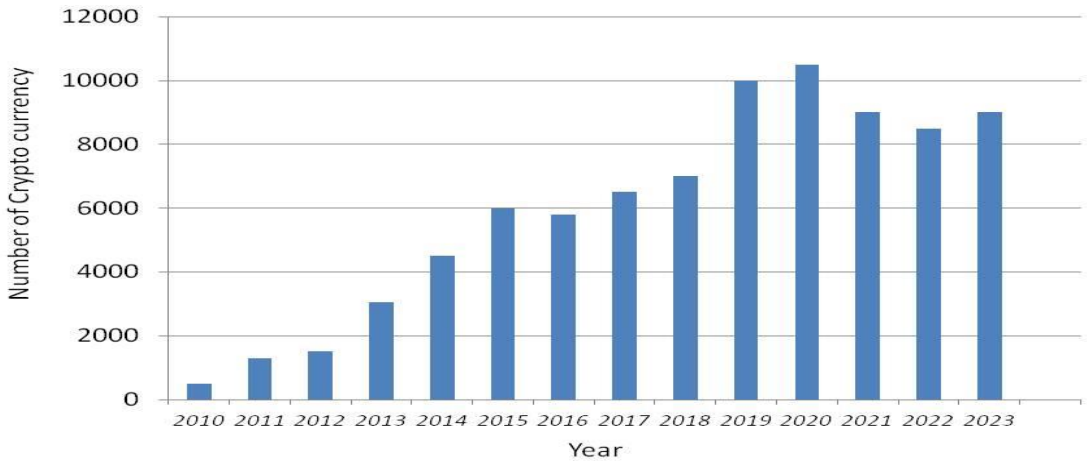

Figure 2: The total number of cryptocurrencies from 2013 to 2023[102]

A scripting language akin to Forth is used to define transactions. A transaction consists of one or more inputs and one or more outputs. When a user transmits bitcoins, they specify each address in an output along with the quantity of bitcoin being transferred to each address. Every input must make reference to a prior, unspent output in the blockchain to avoid double spending.[103] In a cash transaction, using several inputs is equivalent to using multiple coins. Users are able to transmit bitcoins to numerous recipients in a single transaction since transactions can have multiple outputs. Similar to a monetary transaction, more coins may be utilized as inputs than are intended for payments. Any input satoshis that are not taken into account in the transaction outputs become the transaction fee.[104] In this scenario, an additional output is needed to give the payer their change back. Miners can select which transactions to process and give priority to those that pay larger fees, even though transaction costs are optional. Instead of selecting transactions solely on the basis of the total amount paid as a charge, miners may also consider the cost in relation to the size of their storage. The standard unit of measurement for these fees is satoshis per byte (sat/b). The number of inputs needed to construct a transaction and the number of outputs determine its size. The size of blockchain blocks was initially restricted to 32 megabytes. In 2010, Satoshi Nakamoto imposed a one megabyte block size limit.[105] This eventually caused issues with transaction processing, including a rise in transaction costs and a delay in transaction processing.[106] According to Andreas Antonopoulos, the Lightning Network can be scaled, and he has called it a second-layer routing network.[107]

Bitcoin addresses are linked to bitcoins in the blockchain. The process of creating a bitcoin address only involves selecting a random valid private key and quickly computing the matching bitcoin address.[108] However, the opposite—calculating the private key associated with a certain bitcoin address—is essentially impossible. Users can disclose or publicly display a bitcoin address without jeopardizing the private key associated with it. Furthermore, it is quite improbable that someone will compute a key pair that is currently in use and has funds because there are so many legitimate private keys.[109] It is not possible to compromise a private key by brute force due to the large number of valid private keys. The owner of the bitcoin must have the associated private key and digitally sign the transaction in order to spend their bitcoins.[110] The public key is used by the network to validate the signature; the private key is never disclosed.[111] The bitcoin network will not accept any other proof of ownership if the private key is lost, rendering the coins useless and essentially lost. For instance, a user reported losing ₿7,500, or US$7.5 million at the time, in 2013 after inadvertently discarding a hard disk that held his private key.[112] It is estimated that 20% of all bitcoins have been lost; at July 2018 pricing, these bitcoins would have been worth almost US$20 billion.[113] The private key must be kept secret in order to guarantee the security of bitcoins. If the private key is discovered by a third party, such as through a data breach, the third party may utilize it to steal any bitcoins that are linked to it.[114] Nonetheless, around ₿980,000 has been pilfered from cryptocurrency exchanges as of December 2017.[115] In terms of ownership distribution, 98.51% of all bitcoins ever produced are owned by 9.62% of bitcoin addresses as of December 28, 2022.[116] The exchanges that hold their bitcoin in cold storage are believed to be the owners of the largest of these addresses.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

Mining is a type of record-keeping that makes advantage of computer processing power.[117] By continuously collecting recently broadcast transactions into a block, which is subsequently broadcast to the network and validated by recipient nodes, miners maintain the consistency, completeness, and immutability of the blockchain. The name of the blockchain comes from the fact that every block links to the preceding block through the use of a SHA-256 cryptographic hash.[118] A proof-of-work (PoW) is a requirement for a new block to be approved by the rest of the network.[119] This Proof of Work (PoW) is simple for any node in the network to verify, but it takes a lot of time to generate. Miners must find a number called a nonce (which is a number used only once) such that when the block content is hashed along with the nonce, the result is numerically smaller than the network's difficulty target.[120] Before a result turns out to be smaller than the difficulty target, miners must try a large number of various nonce values (typically the sequence of tested values is the ascending natural numbers: 0, 1, 2, 3, 4, 5...). Block hashes have a lot of leading zeros since the difficulty goal is much smaller than a regular SHA-256 hash.[121]

This difficulty target allows you to modify how much work is required to generate a block. Nodes deterministically modify the difficulty target based on the recent pace of block generation every 2,016 blocks (about 14 days given roughly 10 minutes per block), aiming to maintain the average time interval between new blocks at ten minutes.[122] The technology automatically adjusts to the total mining power on the network in this way.[123] To generate a block hash smaller than the difficulty target as of April 2022, an average of 122 sextillion (122 thousand billion billion) attempts are required.[124] These kinds of computations are very costly and require specialist gear.[125] Because an attacker must change every block after another for changes to one block to be approved, the proof-of-work system and block chaining make blockchain modifications exceedingly difficult.[126] Since new blocks are constantly being created, the difficulty of changing an older block grows over time, as does the number of subsequent blocks (also known as confirmations of the given block)[127] . To lessen the variation in miner income, the great majority of mining power is gathered into mining pools.[128] It could take a number of years for independent miners to mine a single block of transactions and get paid. Every time a miner in a mining pool creates a block, they are all compensated. The amount of money each miner donated to the pool is reflected in this payout.[129]

The remaining members of the network permit the successful miner who discovers a new block every ten minutes to keep all transaction fees from the transactions they included in the block[130] as well as a fixed reward of freshly created bitcoins.[131] As of May 11, 2020, this reward is ₿6.25 in newly created bitcoins per block.[132] In order to be eligible for this reward, the miner must include a unique transaction known as a coinbase into the block.[133] This is how all bitcoins were created; according to the bitcoin protocol, the reward for adding a block will decrease by half every 210,000 blocks, or roughly every four years, until ₿21 million are produced.[134] By the year 2140, the last bitcoin will be created. Following that, a profitable miner would only receive transaction fees.[135] Since bitcoin is decentralized, it lacks a central authority.[136] The network is peer-to-peer, lacking central servers.[137] The ledger is distributed and accessible to anybody with a computer.[138] The ledger is managed by a group of equally privileged miners rather than a single administrator. Most people can become miners, albeit not everyone from every nation can. Competition keeps the ledger updated. It is unknown which miner will produce a new block until it is added to the ledger. Bitcoin is issued in a decentralized manner. They are given out as a prize for starting a new block.[139] Anyone can open a new bitcoin address, which is the equivalent of a bank account in bitcoin, and send transactions to the network without requiring permission[140]; the network only needs to verify that the transactions are valid from authorized nations.[141]

Conversely, a "trend towards centralization" has been noted by numerous experts. While bitcoin can be sent directly between users, intermediaries are very frequently utilized in practice.[142] Because transactions on the network are verified by miners, decentralization of the network requires that no single miner[143,144] or mining pool obtains 51% of the hashing power. If they did, they could double-spend coins, prevent certain transactions from being verified, and prevent other miners from earning money. As a result, bitcoin miners join large mining pools to minimize income variance.[145] Just six mining pools possessed 75% of the world's bitcoin hashing power as of 2013.[146] When mining pool Ghash.io attained 51% hashing power in 2014, serious concerns over the network's security were raised. In order to protect the interests of the entire network, the pool has voluntarily limited its hashing power to 39.99% and asked other pools to follow suit.[147] Around 2017, 90% of transactions and over 70% of hashing power came from China[148] , according to researchers. Other aspects of the ecosystem, such as online wallets, simplified payment verification (SPV) clients, and client software maintenance, are also "controlled by a small set of entities."[149]

Because bitcoin is pseudonymous, money is linked to bitcoin addresses rather than actual people or organizations.[150] All transactions on the blockchain are visible to everyone, but the owners of bitcoin addresses are not made publicly known. Furthermore, transactions can be traced back to specific individuals by cross-referencing publicly available transaction data with publicly available information about the owners of certain addresses.[151] Moreover, exchanges that sell bitcoins for fiat money may be legally obligated to gather

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

personal data.[152] A new bitcoin address can be created for every transaction to increase financial privacy.[153] Although the Bitcoin network treats all bitcoins equally, establishing a minimum degree of fungibility, users and apps are allowed to violate this rule. For example, wallets and related software treat all bitcoins in an identical manner; they are not differentiated from one another. However, because every bitcoin transaction history is recorded and made publicly accessible in the blockchain ledger, chain analysis users may choose not to accept bitcoins from questionable transactions.[154] For instance, in 2012, Mt. Gox blocked the accounts of users who deposited bitcoins that were known to have recently been stolen.[155]

A wallet is a device that holds the data needed to exchange bitcoins. Although wallets are sometimes referred to as locations to hold or store bitcoins, because of the architecture of the system, bitcoins and the blockchain transaction record are inseparable.[156] A better definition of a wallet would be anything that "stores the digital credentials for your bitcoin holdings" and makes them accessible for use. Public-key cryptography, which is used by Bitcoin, generates two cryptographic keys: a public key and a private key.[157] These keys are what a wallet essentially consists of. Satoshi Nakamoto released the first wallet program, simply known as Bitcoin, as open-source software in 2009.[158] After version 0.9 was released, the software bundle was renamed Bitcoin Core to differentiate it from the underlying network.[159] Bitcoin Core is arguably the most well-known implementation or client.[160] There are several forks of Bitcoin Core, including Parity Bitcoin, Bitcoin XT, and Bitcoin Unlimited.[161,162]

Hackers target wallet software because it offers a lucrative opportunity to steal bitcoins.[163] The process of keeping private keys offline at all times[164] by generating them on a device that is not connected to the internet is known as "cold storage."[165] There are several ways to store the credentials required to spend bitcoins offline, ranging from specialized hardware wallets to straightforward paper printouts of the private key.[166] A computer add-on that verifies transactions at the user's request is called a hardware wallet.[167] With the exception of transactions that have already been signed and are therefore irreversible, these devices store private keys, perform internal encryption and signing, and do not exchange any sensitive data with the host computer. Even PCs that can be infected with malware cannot access or steal private keys from hardware wallets since they never reveal them.[168] When creating a hardware wallet, the user creates a passcode. Because hardware wallets are impenetrable, the passcode is required in order to retrieve any funds.[169] A key pair that is generated on a computer without an internet connection is used to construct a paper wallet; the private key is printed or written on the paper, and it is then deleted from the computer.[170] After that, the paper wallet can be kept for eventual retrieval in a secure physical location. Physical wallets can also be in the form of metal token coins that have a security hologram engraved in a recess on the back that allows access to the private key.[171] When the security hologram is taken out of the token, it self-destructs, indicating that someone has access to the secret key.[172] Coins with stored face value as high as ₿1,000 have been struck in gold.[173] The British Museum's coin collection[174] includes four specimens from the earliest series of funded bitcoin tokens; one is currently on display in the museum's money gallery.[175,176] Originally, these tokens were struck in brass and other base metals, but later used precious metals as bitcoin grew in value and popularity.

On August 18, 2008, the domain name bitcoin.org was registered.[177] A link to a document titled Bitcoinas a Peer-to-Peer Electronic Cash System, written by Satoshi Nakamoto, was sent to a cryptography email group on October 31, 2008.[178] In January 2009, Nakamoto published the open-source code for the Bitcoin software.[179] It is still unclear who Nakamoto is.[180] Following initial proof-of-concept transactions, illicit marketplaces like Silk Road were among the primary bitcoin users. [181] In its thirty months of operation, which started in February 2011, Silk Road only took bitcoins as payment, transferring ₿9.9 million, or roughly US$214 million.[182] According to University of Cambridge research, there were between 2.9 and 5.8 million distinct users of cryptocurrency wallets in 2017[183] ; the majority of these individuals used bitcoin. YouTube banned videos pertaining to bitcoin and other cryptocurrencies in December 2019, but later decided they had "made the wrong call" and reinstated the content.[184] The Canadian cryptocurrency exchange QuadrigaFintech Solutions collapsed in February 2019, leaving almost $200 million unaccounted for.[185] The price had recovered to $13,000 by June 2019.[186] Elon Musk added the handle Bitcoin to his Twitter profile on January 19, 2021, tweeting, "in retrospect, it was inevitable," which caused the price to spike briefly to US$37,299 in just one hour.[187] On January 25, 2021, Microstrategy announced that it was still buying bitcoin, with holdings of ₿70,784 worth $2.38 billion as of that date.[188] In September 2021, El Salvador legalized bitcoin alongside the US dollar.[189] On April 27, 2022, the Central African Republic legalized bitcoin.[191,192] Investors also engage in bitcoin mining.[192] In three years (Q1 2012 – Q1 2015), bitcoin businesses raised about $1 billion in funding, according to a 2015 analysis by Paolo Tasca.[193] As of September 30, 2014, Mark T. Williams claims that the volatility of bitcoin is seven times higher than that of gold, eight times higher than that of the S&P 500, and eighteen times more than that of the US currency.[194]

Bitcoin is a digital asset intended to function as a currency in peer-to-peer transactions.[195] The Economist stated in January 2015 that three characteristics of bitcoins make them valuable as a medium of exchange: they are "hard to earn, limited in supply, and easy to verify."[196] However, some researchers argue that as of 2015, bitcoin is more of a payment system than a medium of exchange.[197] Between 2.9 million and 5.8 million unique individuals used a cryptocurrency wallet in 2017, the majority of them for bitcoin,

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

according to research from the University of Cambridge.[198] Since 2013, when there were between 300,000 and 1.3 million users, the number of users has increased dramatically.[199] As of 2018, the vast majority of bitcoin transactions happened on cryptocurrency exchanges rather than with merchants.[200] Bitcoins can be purchased on these exchanges.[201] The precise number of bitcoin millionaires is unknown because a single person can own multiple bitcoin wallets. François R. Velde, Senior Economist at the Chicago Fed, has called bitcoin "an elegant solution to the problem of creating a digital currency." 9,272 bitcoin wallets with more than $1 million worth of bitcoins were recorded in 2017, according to bitinfocharts.com.[202] Major corporations including SpaceX[203], Tesla[204], and MicroStrategy[205] have made investments in bitcoin as a store of value. Since 2014, federal elections in the US have permitted the use of cryptocurrencies for political campaign contributions. Moreover, a number of US states have either explicitly permitted or prohibited the use of cryptocurrencies in state-level elections.[206] The Democratic governor of Colorado, Jared Polis, accepted bitcoin and other cryptocurrencies as official campaign funds in 2022.[207] At least eight Nobel Memorial Prize in Economic Sciences laureates have called bitcoin and other cryptocurrencies an economic bubble, including Robert Shiller[208], Joseph Stiglitz[209], and Richard Thaler[210]. Columnist and economist Paul Krugman has called bitcoin "a bubble wrapped in techno-mysticism inside a cocoon of libertarian ideology."[211] Economist NourielRoubini of New York University has referred to bitcoin as the "mother of all bubbles,"[212] while James Heckman of the University of Chicago has likened it to the tulip mania of the 17th century.[213] Another recipient of the prize, Robert Shiller, contends.[214]

Category	**Double-Entry**	**Bitcoin (POW Accounting)**
Greed Effect	Fraud, other aggressive accounting practices	Under the correct conditions, deters motivation for fraudsters and encourages actors to play by the rules
Audit	Audited historically	Audited in real time
Audit Quality	Reasonable Assurance	Absolute Assurance
Accounting + Audit Dependence	Human processional judgment + software	Largely software driven
Unit of Account	Fiat / Crypto denomination of choice	bitcoin
Accuracy	Pre-audit, accuracy depends on quality of financial statement control design and execution	Accuracy depends on users running compatible client versions, non-buggy code, and a majority of hashrate being honest
Fraud Cost	Cheap	Expensive
Determining intent (Fraud or Honest Mistake)	Difficult	Easy, and obvious
Fraud Detection	After the fact	Immediate
Network Effect Upside	Average - can run double entry accounting with your own local currency (including Bitcoin)	Very Strong - need to use the network incentive token (i.e. bitcoin) to access available assurances
Accounting Dependence	Run independently – fraud in Company A largely does not affect Company B	Run independently – but fraud within the accounting system causes large disruption for all stakeholders

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

Ledger	Private	Public
Redundancy	Low- ledger stored by a few parties at most	High - ledger stored by a large amount of parties
Ledger Entry Rights	Closed - only company employees allowed to make entries	Open - anyone can create entries
Entries	Subject to change	Immutable
Entry Finality (Timing)	Delayed- post annual audit	After x amount of blocks that makes it infeasible to rewrite ledger history
Scalability	High	Low

Table 1: Bitcoin as a decentralized accounting revolution platform[215]

Data on Various Cryptocurrencies, Owner Nations, and Industry Outlook

Globally, there are 84.02 million cryptocurrency wallets as of August 2022. Compared to 2015, when there were just 3.16 million cryptocurrency wallets worldwide, this number has significantly increased. Based on trading volumes, traffic, liquidity, and exchange rates, Binance, Coinbase Exchange, FTX, Kraken, and KuCoin are the top five cryptocurrency exchanges. Crypto exchanges are exempt from registration requirements with a unified authority because of the nature of cryptocurrency and the lack of legislation around it in most countries. It is nearly impossible to determine the precise number of cryptocurrency exchanges worldwide due to its lax restrictions. On the other hand, the current estimate of 504 exchanges is approximately. Of these interactions, around half are monitored and the other half are just getting started. But the first decentralized cryptocurrency was Bitcoin, which was developed in 2009 by an unidentified developer under the pseudonym Satoshi Nakamoto.[216] As of February 2023, Bitcoin (BTC) is the most valuable cryptocurrency on the market, with a market capitalization of about $457 billion. In actuality, since 2010, the price of Bitcoin has grown by more than 46,449,400%. Nonetheless, the price of Bitcoin peaked in 2010 at $0.09, and it currently costs more than $23,000. Numerous market observers forecast that the price of Bitcoin would hit $100,000. Bitcoin is owned by 65% of all crypto users. As of February 2023, the most well-liked cryptocurrencies outside Bitcoin are Tether USD, Ethereum, BNB, and USD Coin. The market capitalization of these other cryptocurrencies is far smaller than that of Bitcoin; for example, Ethereum's market capitalization is only $200 billion, whereas Bitcoin's is $457.16 billion.

A cryptocurrency's popularity can be determined by a variety of factors, including how often it trades, how many people own it, and how many transactions it is used for. However, market capitalization is the most widely used metric. By dividing the total number of coins in circulation by the price of each coin, we can determine the capitalisation of a cryptocurrency. As a matter of fact, many people believe that Bitcoin is the original cryptocurrency. The only cryptocurrency that most people are aware of is this one because it has been around for the longest and has a strong enough brand awareness. While some technology existed before, Bitcoin was created in the fall of 2008. However, Ethereum is seen as the prototype for a second-generation cryptocurrency, and since its launch in early 2016, its market capitalization has maintained it as the second cryptocurrency. In a technical sense, Ethereum is the network and Ether is the currency. Its usage of smart contracts is what makes it famous. Its blockchain is utilized by over 3,000 dApps and other cryptocurrencies. Ethereum operates as a nonprofit. Technically speaking, it is not a deflationary currency like Bitcoin, even if several adjustments have been made to eliminate the chance of there ever being too much ether. Its security and scalability issues have drawn criticism. The network's transaction costs have skyrocketed recently. Similar to Bitcoin, it requires a lot of energy. More energy is used in a single Ethereum transaction than in a week in the average US household. One Ethereum transaction has the same carbon footprint as 141,000 Visa transactions, which makes comparisons simpler. In addition, it moves more slowly than more recent cryptocurrencies. 13 transactions may be processed on the blockchain in a second, and confirmations take roughly five minutes. Table 3 below displays the breakdown of the top five cryptocurrencies by market capitalization as of February 2023. Figure 3 below displays the top 15 cryptocurrencies by market capitalization as of January 2022.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

Cryptocurrency	2023 Market Cap
Bitcoin	$457.16 billion
Ethereum	$202.46 billion
Tether	$70.97 billion
BNB	$47.77 billion
USD Coin	$42.46 billion

Table 2: Market capitalization of the top five cryptocurrencies[217]

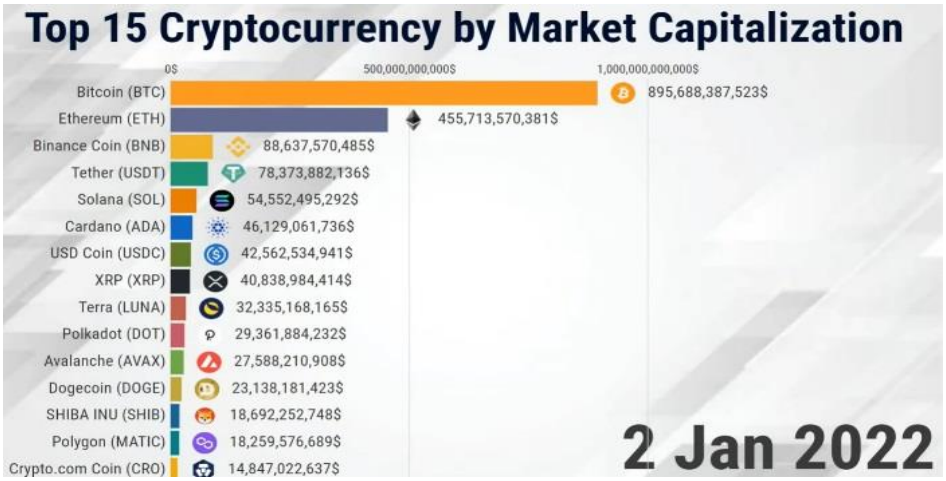

Figure 3: Market capitalization of the top 15 most valuable cryptocurrencies[218]

By 2023, there will be 420 million cryptocurrency users worldwide. Over the past several years, there has been a remarkable increase in the use of cryptocurrencies. Globally, the number of bitcoin users increased by 190% between 2018 and 2020. Just in the last year, the industry's growth rate has continued to increase.[219] With 27.67% of the population owning bitcoin as of 2023, the United Arab Emirates is the nation with the highest percentage of cryptocurrency owners. Vietnam is the nation with the highest percentage of bitcoin ownership (26% of the population). The Philippines, where 13% of the population uses cryptocurrency, the United States, where 13.22% of the population owns cryptocurrency, and India, where 11.5% of the population owns cryptocurrency, come next. India leads the world in the overall number of cryptocurrency owners, at 157.6 billion as of 2023.[220] With 44.3 million crypto owners, the United States is the nation with the second-highest number of crypto owners. The United States has the most cryptocurrency ATMs, with 17,436 running ones as of 2021. Other top countries for cryptocurrency ownership are Vietnam, with 25.9 million owners, China, with 19.9 million owners, and Brazil, with 17.8 million owners.[221] By a wide margin, the United States has the most cryptocurrency ATMs worldwide.[222] Furthermore, the United Kingdom has 200 ATMs, Austria has 157 ATMs, Spain has 138 ATMs, Canada has 1,464 ATMs, and Austria has 157 ATMs. The amount of bitcoin ATMs in the US is increasing at an exponential rate compared to the rest of the world.[223] Figure 4 below displays the number of cryptocurrency owners by country worldwide. The trend of cryptocurrency ownership as a comparative percentage of users across various nations is displayed in figure 5 below.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

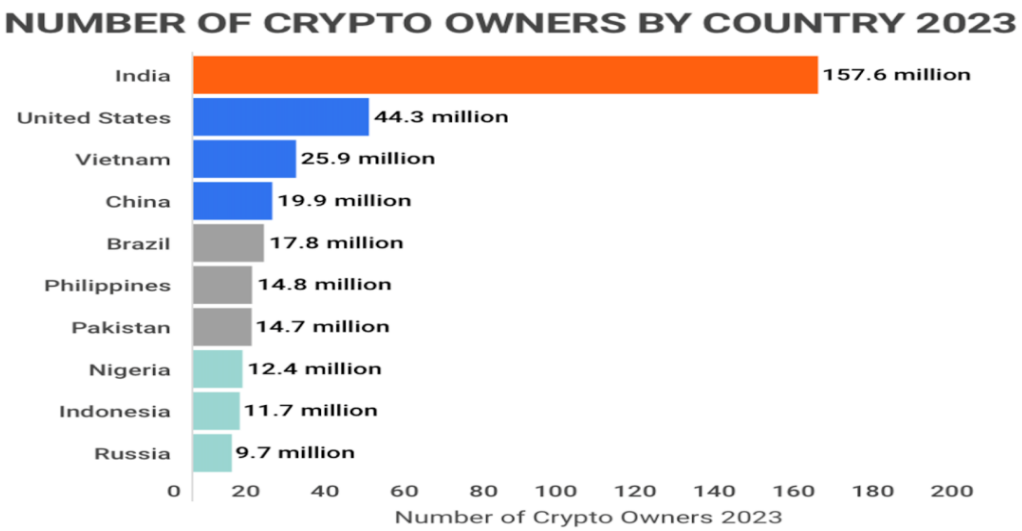

Figure 4: Global cryptocurrency ownership numbers by nation[224]

According to the analysis, the worldwide cryptocurrency market is expected to expand at a compound annual growth rate (CAGR) of 56.4% between 2019 and 2025. The report on cryptocurrency market is a thorough analysis and presentation of drivers, restraints, opportunities, demand factors, market size, forecasts, and trends in the global cryptocurrency market over the period of 2017 to 2025. The study covers the analysis of the leading geographies such as North America, Europe, Asia-Pacific, and RoW. In addition, the paper presents the results of both primary and secondary research collectively.[225]A compound annual growth rate (CAGR) of 68.4% is projected for the worldwide blockchain technology industry by 2026. However, since 2016, the number of cryptocurrency wallets globally has increased at a rate of 1,271.97%. Globally, there were 5.78 million cryptocurrency wallets in January 2016 and 84.02 million as of August 2022.[226] On the other hand, it is anticipated that adoption rates will rise with cryptocurrencies.[227] However, it's also anticipated that there will be more restrictions pertaining to cryptocurrencies in the near future. The market for cryptocurrency wallets was projected to be worth USD 8.42 billion in 2022, and from 2023 to 2030, it is projected to expand at a compound annual growth rate (CAGR) of 24.8%.[228] The market's primary growth engine is the extensive acceptance of cryptocurrencies as a real asset class. The need for safe and convenient storage solutions has grown as institutional and individual investors alike are becoming more aware of cryptocurrencies. The creation and use of cryptocurrency wallets have increased globally as a result of this awareness. The increased understanding of cybersecurity's crucial significance in the cryptocurrency field is another important factor.[229] People's concerns over the security of their investments are growing as a result of the increasing value of digital assets.[230]

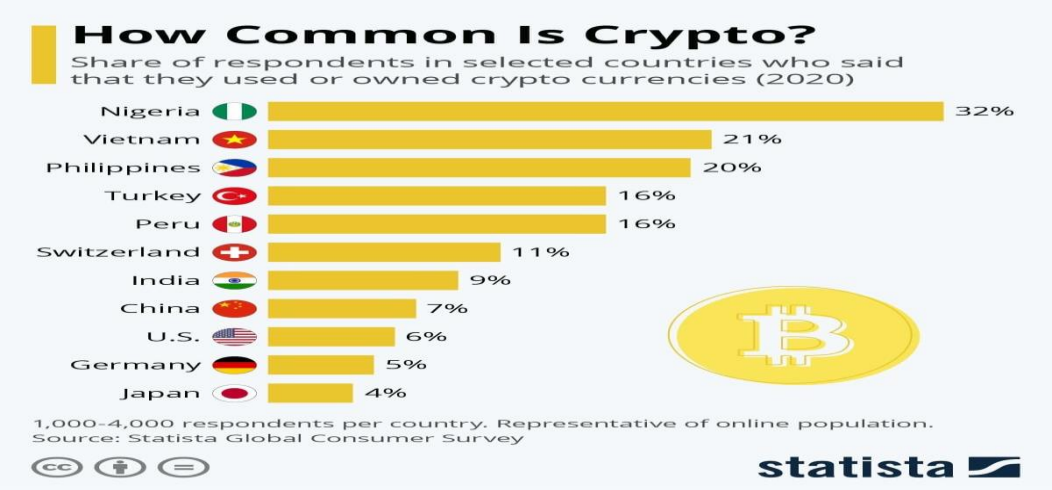

Figure 5: Trends in cryptocurrency ownership as a comparable percentage of users across several nations[231]

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

Crypto wallets are a strong substitute for centralized exchanges that are subject to hacking and cyberattacks since they offer a private and secure way to store cryptocurrency. The need for reliable crypto wallet solutions is anticipated to grow as cybersecurity threats change. The Decentralized Finance (DeFi) ecosystem's explosive growth is another factor propelling the cryptocurrency wallet business. Smart contracts are the foundation of DeFi platforms, and in order for users to engage with these decentralized apps efficiently, they need cryptocurrency wallets.[232] The need for cryptocurrency wallets that work well with DeFi's lending, borrowing, and trading platforms has increased dramatically as a result of the platform's popularity. Furthermore, the market has been significantly impacted by the spread of Non-fungible Tokens (NFTs).[233] Crypto wallet growth is also being aided by the worldwide remittance sector. Because cryptocurrencies are more efficient and less expensive than traditional financial institutions, they are being utilized for international money transfers on a growing basis. The use of cryptocurrency wallets, which allow users to transfer and receive digital currencies across borders with lower fees and quicker processing times, is essential to the success of these transactions.[234] Top cryptocurrencies other than bitcoin include Tron (TRX), Polygon (MATIC), Cardano (ADA), Solana (SOL), Dogecoin (DOGE), Ethereum (ETH), Tether (USDT), XRP, Binance Coin (BNB), USD Coin (USDC), and so on.[235]

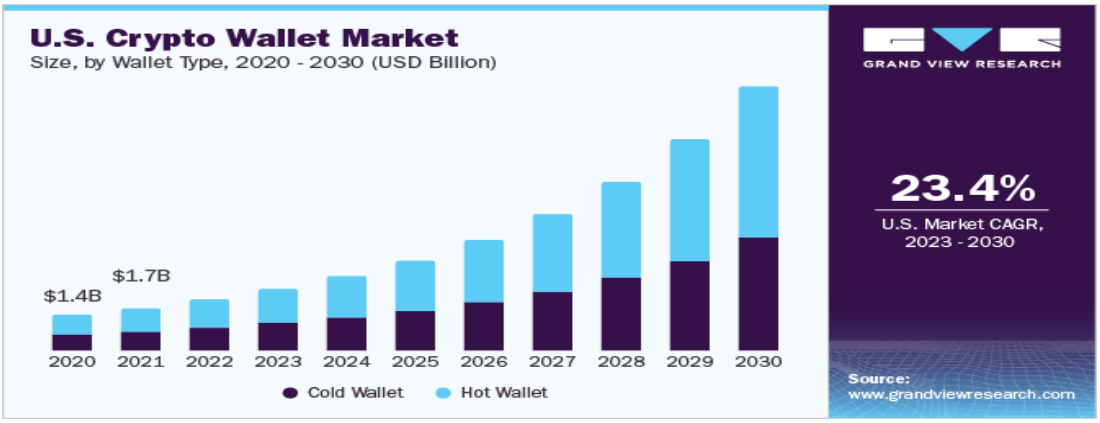

Figure 6: American cryptocurrency wallet market forecast[236]

Furthermore, changes in regulations are reshaping the cryptocurrency wallet business. Governments and regulatory agencies are starting to set rules and specifications for cryptocurrency wallet suppliers in an effort to improve security protocols and reduce risks associated with illegal activities such as fraud and money laundering. It is now essential for wallet providers to abide by these rules in order to win over consumers' trust. The market is notably constrained by the intricate and sophisticated nature of cryptocurrencies and blockchain technology.[237] For many prospective users, it might be frightening to understand the nuances of maintaining wallet security, public addresses, and private keys. Newcomers may be deterred from utilizing cryptocurrency wallets and the cryptocurrency environment by this intricacy.[238] Wallet providers and the industry at large need to put an emphasis on user education and user-friendly design in order to get through this barrier. Wallets must to be created with user-friendly interfaces, unambiguous instructions, and strong customer service to assist users in configuring and utilizing their wallets safely. The most well-known cryptocurrency, bitcoin, saw a 500% increase in value in just six months in 2020.[239] The longest bull market in the history of the bitcoin market is still ongoing. The increased use of cryptocurrencies during the pandemic can be linked to a number of factors, including digitization, rising internet penetration, quick technical advancements, and dwindling faith in established financial institutions. During the COVID19 pandemic, people's demand for cryptocurrencies increased, which is encouraging for the market's expansion.

One way to characterize the crypto wallet market is as highly fragmented. To maintain their dominant position in the market and obtain a competitive edge, key players are putting numerous strategic initiatives into practice, including product launches, mergers and acquisitions, partnerships, collaborations, and geographic expansions.[240] Major players are growing their offers to include cryptocurrency assets like Non-Fungible Tokens (NFTs) by utilizing advancements in blockchain technology. The expansion of the industry is anticipated to be fueled by the technological innovations spearheaded by leading companies in the market. With cutting-edge features, players are concentrating on introducing new services to gain a greater share of the market's clientele.[241] Ledger, for example, announced a strategic relationship with PayPal in August 2023, which was a significant step toward the simplification of cryptocurrency transactions. An official statement stated that the integration of PayPal's Ledger Live software will enable authenticated citizens of the United States to easily purchase cryptocurrencies like bitcoin, ether, bitcoincash, and litecoin through ledger live, eliminating the requirement for additional verification steps.[242] A few well-known companies in the worldwide

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

cryptocurrency wallet industry are Ledger SAS, BlockFi Inc., Exodus Movement, Inc., ZenGo Ltd., Coinbase worldwide, Inc., BitGo, Binance, BitPay, SatoshiLabss.r.o. (Trezor), etc.[243]

Examining data from over 61,000 global crypto users, this analysis is the first of its kind to focus on retail consumers globally and sheds light on the motives, habits, and preferences of this rapidly expanding audience. The results show that 97% of users have almost universal confidence in cryptocurrency. More than half (52%) view cryptocurrency investing as a source of income rather than a pastime, and 15% of users view it as their main source of income. As for the top three reasons people invest in cryptocurrency, they are: Short-term trading opportunities (31%), mistrust of the current financial system (38%), and owning cryptocurrency as part of a long-term investment strategy (55%).[244]The global retail cryptocurrency market is expanding. With the expanding accessibility of cryptocurrencies through various channels such as Paypal, LocalBitcoins, Binance, Grayscale, and others, it is crucial to comprehend the prevailing user profiles and their preferences. Apart from anecdotal evidence, a systematic study exploring the motives, habits, and preferences of these expanding worldwide audiences has not been conducted.[245]

The market for blockchain technology related to bitcoin was projected to reach $50 billion by 2026. In the financial sector, blockchain technology is worth 60% of its overall value. Every day, 30,000 social media postings on bitcoin are shared online. This translates to 1500 posts every hour, or 30 posts every minute. By February 2022, Tether will have a $109 billion volume, making it one of the largest Crypto assets. By 2025, Ethereum will see roughly 10 million bitcoin transactions every day. In Q3 of 2021, Ethereum—Bitcoin's main rival—had the most daily cryptocurrency transactions. Bitcoin transactions per day indicate that it only reached about 660K, which is about four times less than Ethereum. With 2.4 million bitcoin transactions as of January 2022, ETH continues to lead the pack, while bitcoin completed at least 500K transactions. By March 2030, there will be 14 million new instances of cryptomalware. In 2020, the entire value of the world's cryptocurrency market was estimated to be $1 billion. With a 30% compound annual growth rate, the cryptocurrency market is predicted to reach $5,190,62 million by 2026. According to reasonable estimations, the size of the global cryptocurrency market in 2020 will be $1500 million. It is projected to increase at a CAGR of 11.2% to $1,758 million by 2027. From March 2021 to February 2022, the value of the entire cryptocurrency market is probably going to rise by over 1800%.[246] However, figure 7 below summarizes and illustrates the reasons for the widespread use and enormous popularity of cryptocurrencies.

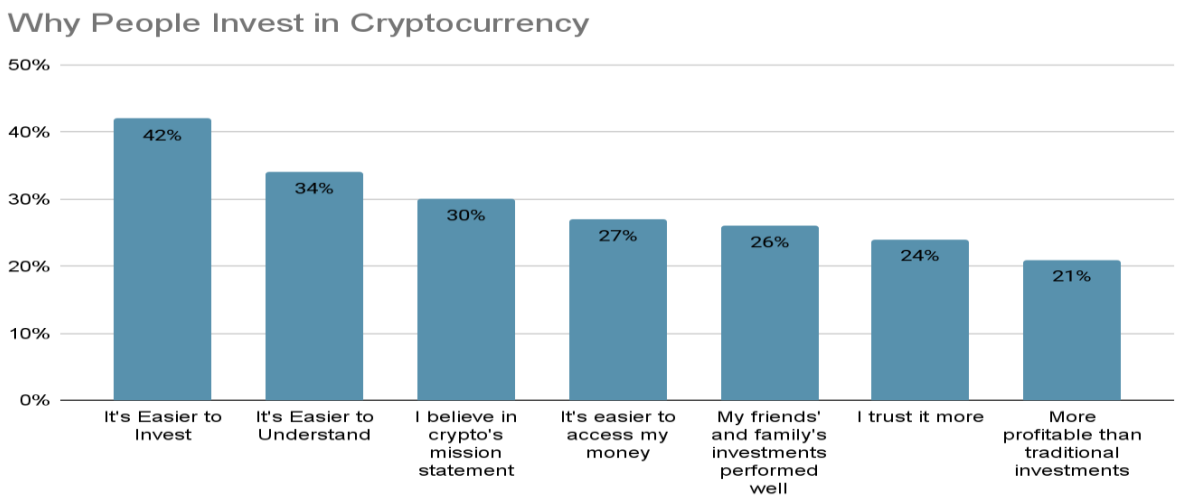

Figure 7: Key justifications for the present population's use of cryptocurrencies[247]

Key Features and Diverse Cryptocurrency Statistics

The current market capitalization of cryptocurrencies is $2.79 trillion, which is equal to the eighth largest economy in the world. 730 cryptocurrency spot exchanges are located throughout the world. By February 2022, Tether will have a $109 billion volume, making it one of the largest Crypto assets. The attorney general of New York, who had previously opposed the cryptocurrency, has now stated that it may not be as stable as it has claimed because the US dollar did not fully support it. Every day, 30,000 postings on social media about Bitcoin are put online. This translates to 1500 posts every hour or 30 posts every minute. Bitcoin only received about 660K transactions each day, which is about four times less than Ethereum. Now, in Q3 of 2021, Ethereum—the main rival of Bitcoin—had the most daily cryptocurrency transactions. By 2025, Ethereum will see roughly 10 million bitcoin transactions every day. With 2.4 million bitcoin transactions as of January 2022, ETH continues to lead the pack, while Bitcoin completed at least 500K transactions.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

By March 2030, there will be 14 million new instances of crypto-malware. In 2020, the entire value of the world's cryptocurrency market was estimated to be $1 billion. With a 30% compound annual growth rate, the cryptocurrency market is predicted to reach $5,190,62 million by 2026. According to reasonable estimations, the size of the global cryptocurrency market in 2020 will be $1500 million. It is projected to increase at a CAGR of 11.2% to $1,758 million by 2027. From March 2021 to February 2022, the value of the entire cryptocurrency market is probably going to rise by over 1800%. By 2026, the market for bitcoin blockchain technology was projected to grow to $50 billion. In the financial sector, blockchain technology is worth 60% of its overall value.[248]

Bitcoin is the most widely used cryptocurrency in the USA, making about 72% of all transactions. Since 2018, when barely 3% of people worldwide owned bitcoin, the number of cryptocurrency users in the UK has surged by 600%. The largest number of Google searches for “cryptocurrency” is made in Nigeria. In the UK, 79% of cryptocurrency owners have made Bitcoin investments. Of all the regions, Africa has the smallest cryptocurrency economy, with $8 billion going into the blockchain and 8.1 billion going out. With almost 90% of all volume traded (above $20,000 worth of cryptocurrency), professional traders control the majority of the East Asian cryptocurrency market. By 2030, $500 billion in blockchain funding is what Europe hopes to see. As of January 2022, the Middle East only accounted for 15% of the global cryptocurrency market, with Turkey leading the way in terms of transactions. By early 2025, there will be more than 2000 business blockchain projects underway in the US. G20 nations claimed 85% of all cryptocurrency exchanges in 2013, but by 2021, just 30% of G20 transactions were made. According to data, as of January 2022, the G20 countries with the highest number of cryptocurrency exchanges were Hong Kong (27), Singapore (47), the US (40), and the UK (70). Once more, the countries with the fewest exchanges were Mexico (5 exchanges), Argentina (4 exchanges), Indonesia (3 exchanges), and Russia (2 exchanges).

The blockchain market had a valuation of only $3.2 billion in 2020. That amount will rise to $5 billion in 2021, and an additional $7 million is anticipated the following year. Eighty percent of initial coin offers (ICOs) that were made public in 2021 were frauds intended to trick people or raise money for vital cryptocurrency initiatives. In 2021, the crypto market saw a $150 billion loss. As of Q4 2021, Bitcoin's market capitalization stood at $1100 billion. It experienced its largest growth since its founding in Q12022, with $500 billion in growth. The global blockchain industry is expected to grow at a compound annual growth rate (CAGR) of 5% from 2022 to 2027, reaching a projected value of $30 billion by 2025. By 2026, investors are expected to invest up to $40 billion in blockchain technology. The global market for digital currency is expected to reach a value of over $1200 million by 2027, according to forecasts. That represents a nearly 5% compound annual growth rate for cryptocurrencies like Dogecoin, Litecoin, Ethereum, Ripple, and others. By January 2030, the growth of cryptocurrencies is probably going to be 5000% more than it was in 2021.

Because of the oversupply of miners, mining bitcoin is currently more difficult than it was in the past. Because of this, mining cryptocurrency is costly and yields a small profit. Each year, the energy used in bitcoin mining can power more than 10 million households. Whether we buy or rent, the costs of the rig will be our responsibility. Additionally, its user will have to split the block with other pool miners, whose fees range from $2000 to $6000. In 2021, miners will only receive 5 Bitcoin every block, or roughly $30,000. From their high in 2009, the bitcoin block rewards had decreased the previous year. With a daily payment of just $10, or 0.0085ETH, Ether's blockchain reward is now less than it has ever been as of January 2022. You could formerly get five Ethereum from cryptocurrency mining, but that amount dropped to three in 2017. The percentage of people using the digital currency Bitcoin Network is at a record 96%. Cryptocurrency statistics show that the number of validators increases by 10% per week. The annual cost of electricity for mining Bitcoin is $4,466,697,344. In China, where coal power accounts for almost 66% of electrical production, 72% of Bitcoin mining takes place. Emissions from bitcoin alone could raise the world average temperature above +2°C. Ten minutes will be needed for the verification of each transaction within a block. This implies that 6.25 Bitcoins will be issued and added to the overall cryptocurrency market every ten minutes.

The cryptocurrency market has grown significantly over the past several years, but there are still a lot of security risks. Every day, hundreds of cybercrimes involving bitcoins are committed. At the time of its inception, crypto-jacking accounted for about 5% of the entire Monero cryptocurrency in circulation.[249] The majority of its resources were devoted to mining Monero. Based on the current market value of Monero, theft has cost us roughly $65 million in Monero. The amount of crypto-crime that occurs will increase by over 600% by 2030. The estimated cost of cybercrime occurrences in 2030 is close to $5 trillion, an 800% increase from roughly $600 billion in 2018. $2.9 billion was made in 2019 using a Ponzi scheme that went by the name PlusToken. WoToken scammed cryptocurrency investors out of $1.1 billion in 2020. The Squid game in 2021 will be the same. With 2% of all transactions, cryptocurrency transactions to unauthorized accounts are most common in Latin America. Major cryptocurrency frauds, hacks, and thefts came to $3 billion in 2021. 2020 saw the transfer of $3.5 billion to Bitcoin wallets linked to illegal activity. In 2021, the total amount of bitcoin theft worldwide was $600 million, a notable rise over the $500 million recorded in the 2020s. The countries with the least amount of ransomware threats in 2021 were Ireland, the UK, France, Germany, Denmark, Netherlands, Finland, and Norway, where just 0.01% of mining equipment experienced them each month. The yearly increase in ransomware crimes is 500%. This was

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

primarily due to work-from-home policies that were inspired by COVID-19 creating vulnerabilities for businesses. According to a study, two hacker gangs have been implicated in over 60% of all cryptocurrency thefts that have been reported, totaling over $1 billion. About half of all crypto thefts worth over $1 billion USD were said to have been committed by two groups of hackers. According to a research, the initial design and creation of 50–70% of initial coin offerings (ICOs) were done fraudulently.

By 2021, there will be roughly 1000 new coins available each day. Approximately 88% of the entire cryptocurrency market value is comprised of the top 10 cryptocurrencies with the greatest market capitalization. (Bitcoin, Ethereum, Ripple, Tether, Bitcoin Cash, Bitcoin SV, Litecoin, Binance Coin, EOS, and Tezos). As of Q1 2022, there are an estimated 300 million identity-verified cryptocurrency users worldwide. Nigeria leads the way with the highest percentage of people who indicated that they used or owned cryptocurrencies at 31.9%. Vietnam comes in second with 21.1%, the Philippines with 19.8%, and South Africa with 17.8%. Sixty-sixty-three percent of US investors have not invested in cryptocurrency and are not interested in doing so; only 7% say they have plans to do so. Fifty-five percent of 18 to 35-year-olds in the US are more likely to buy Bitcoin in the next five years, while forty-sixteen percent of adults between 36 and 44 want to invest and thirty-sixty-to-54-year-olds want to do the same. Males make up 88% of Ethereum traders and 85% of Bitcoin traders. With a 24-hour volume of $90 billion as of November 29, 2021, Tether (USDT) is the largest cryptocurrency in the world. With $60 billion, Bitcoin is ranked second, and Ethereum (ETH) is ranked third with $25 billion. As of January 2022, there were 28,000 Bitcoin Automated Teller Machines (ATMs). The number of Bitcoin transactions per day almost hit 600,000 during the second quarter of 2021. Ethereum's (ETH) value as of December 15, 2021 is equal to $1,809.07. As of December 1, 2021, Ethereum's (ETH) market capitalization was over $225 billion. Based on 24-hour volume, Binance has grown to be the largest cryptocurrency exchange. Hydax Exchange is in second place with $12.19 billion, followed by HBTC with $14.44 billion. On January 1, 2022, Litecoin's market capitalization was $16 billion. In 2021, Dogecoin experienced a sharp increase in value due to comments expressing its immense potential. Elon Musk, the CEO of Tesla, earned $5.35 in January 2022.

Consensus algorithms, architecture, and the history of blockchain

Cryptocurrency has garnered significant interest from academia and industry. Although Bitcoin is one of the most well-known blockchain applications, blockchain technology has many uses outside of cryptocurrencies.[250] Blockchain was first proposed in 2008 and implemented in 2009,[251] and Bitcoin, which is frequently referred to as the first cryptocurrency, has seen tremendous success in the capital market.[252] Blockchain technology is applicable to a number of financial services, including digital assets, remittance, and online payments, since it enables transactions to be completed without the need for a bank or other middleman.[253] The next generation of Internet interaction systems, including smart contracts[254], public services[255], the Internet of Things (IoT)[256], reputation systems[257], and security services[258], are also looking to blockchain as one of their most promising technologies. Although blockchain technology has a lot of potential for building the Internet infrastructure of the future, it is now confronting several technical difficulties. To begin with, scalability is a major worry. Currently, a Bitcoin block can only be one megabyte in size, and a block is mined roughly every 10 minutes. As a result, high frequency trading cannot be handled by the Bitcoin network, which is limited to 7 transactions per second. Larger blocks, however, require more storage space and propagate through the network more slowly. Users will want to maintain such a big blockchain, which will eventually lead to centralization. As a result, balancing block size and security has grown difficult. Second, it has been demonstrated that miners can use self-serving mining strategies to make more money than is reasonable.[259] For future financial gain, miners conceal the blocks they have already mined. Hence, branches may occur frequently, impeding the advancement of blockchain technology. Therefore, some fixes for this issue must be proposed. Furthermore, it has been demonstrated that privacy leaks in blockchain technology can occur even in situations where users merely use their public and private keys to complete transactions.[260] Even the user's actual IP address can be traced. Furthermore, there are a number of significant issues with the consensus methods used today, such as proof of stake and proof of work. For instance, proof of work consumes excessive amounts of electricity, but the proof of stake consensus process may give rise to the phenomena of the affluent getting richer. Swift resolution of these issues is crucial for the advancement of blockchain technology.

Blockchain Structure

Similar to a traditional public ledger, a blockchain is a series of blocks that together contain a complete list of transaction records.[261] Figure 8 shows an illustration of a blockchain. By means of a reference, which is simply the parent block's hash value, each block refers to the block that came right before it. It's important to remember that hashes of uncle blocks—children of the block's ancestors—will likewise be kept on the Ethereum network.[262] A blockchain's genesis block, which is the first block without a parent block, is known as such. The block structure, digital signature process, essential features of the blockchain, taxonomy of the

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

blockchain, etc. are then introduced. As seen in Figure 9 below, a block is made up of the block header and the block content. Block version, parent block hash, merkle tree root hash, timestamp, nBits, nonce, etc. are specifically included in the block header. Transactions and a transaction counter make up the block body. The block size and the size of each transaction determine the maximum number of transactions that can be contained in a block.

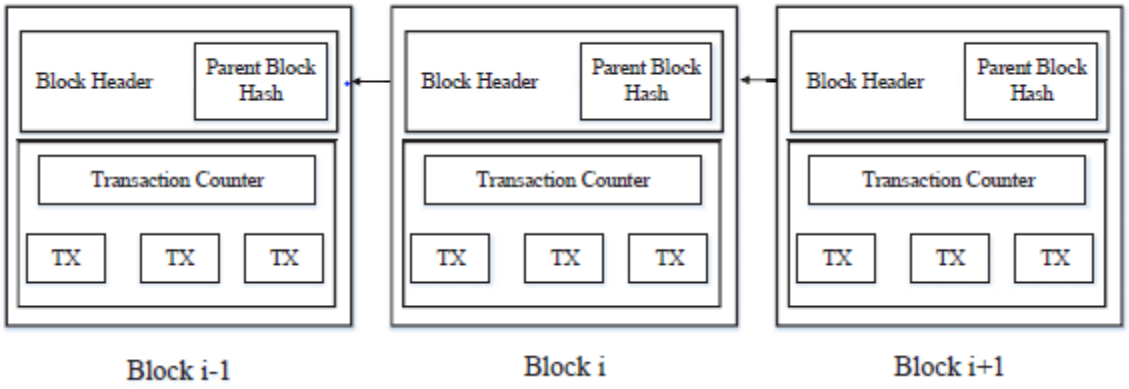

Figure 8: A blockchain sample that is made up of an ongoing series of blocks[263]

Blockchain verifies transaction authentication by an asymmetric cryptography technique.[264] An unreliable environment is where asymmetric cryptography-based digital signatures are utilized. Every user possesses a set of both private and public keys. The transactions are signed using the private key. Public keys, which are visible to all network users, are used to access the digitally signed transactions that are dispersed throughout the whole network. An illustration of a digital signature utilized in blockchain technology is provided in Figure 10. There are two stages to a typical digital signature: the signing phase and the verification phase. Again, let's use Figure 10 as an illustration. Ross, the user, first creates a hash value from the transaction before attempting to sign it. Then, he uses her private key to encrypt this hash value, and he gives Rachel, another user, the encrypted hash along with the original material. Using Ross's public key and the hash value obtained from the incoming data using the same hash function, Rachel compares the decrypted hash to confirm the received transaction. Elliptic curve digital signature algorithm (ECDSA) is one of the common digital signature algorithms used in blockchains.[265]

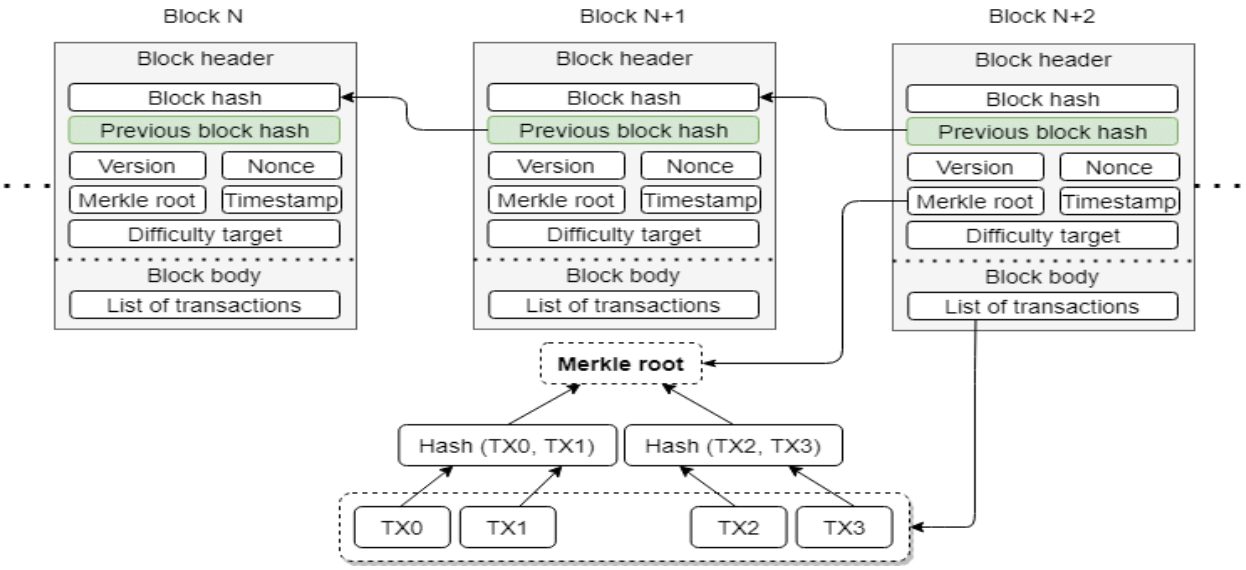

Figure 9: Block structure and blockchain[266]

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

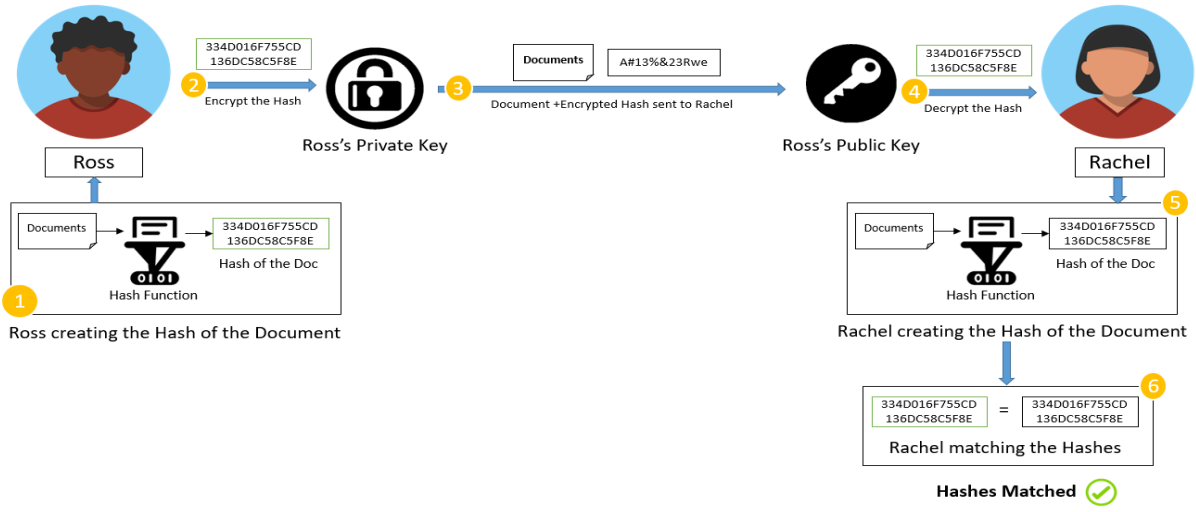

Figure 10: An illustration of a blockchain-based digital signature[267]

Important features of blockchain

One kind of technology that incorporates ledger distribution is called blockchain. The transactions in this ledger are referred to as blocks. Because these blocks are connected in a fashion that updates with each transaction, the system is referred to as a blockchain. It is also hard to change or amend any records due to the cryptography utilized. Blokchain is actually not the same as bitcoin, nor does it just power cryptocurrencies—rather, it powers smart contracts, fraud detection, healthcare, and other industries. We also examined the key components of cryptocurrency, including its single source of truth, decentralization, and immutability of data.[268] Key elements of blockchain technology are enumerated below.

- Dispersal of power. Conventional centralized transaction systems necessitate the validation of every transaction by a central trusted agency, such as the central bank. This leads to inevitable expenses and performance bottlenecks at the central servers. On the other hand, peer-to-peer (P2P) transactions within the blockchain network do not require central agency authentication. Blockchain can help alleviate performance constraints at the central server and drastically lower server costs (both development and operating costs). Because blockchain technology is decentralized, it is not governed by a single entity, a governing body, or a group of people. Instead, the entire transaction is managed by a collection of nodes.

- Unchangeability. It refers to something that is unchangeable. One of the key characteristics of blockchain technology that contributes to its longevity as an everlasting, unchangeable network is this.

- Continuedness. It is nearly impossible to tamper with because every transaction that spreads over the network must be verified and recorded in blocks that are dispersed throughout the whole network. Every broadcasted block will also undergo transaction verification and validation by other nodes. So any deception will be noticed simply.

- Anonymity. It is true that every transaction is transparent and open to the public, but the actual persons are kept anonymous through the addresses. If someone were to transfer a certain amount of money, for instance, the recipient would be aware that the sender is associated with a bitcoin address but would not be aware of the address itself. There are various reasons for this - one of them is privacy. Each user can communicate with the blockchain network with a created address. Further, a user will generate multiple addresses to avoid identity disclosure. There is no longer any central party keeping users' private information. This approach preserves a certain amount of privacy on the transactions contained in the blockchain. Note that blockchain cannot ensure the perfect privacy preservation due to the intrinsic constraint.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

- Auditability. Since each of the transactions on the blockchain is confirmed and recorded with a timestamp, users can simply verify and trace the previous records through accessing any node in the distributed network. In Bitcoin blockchain, each transaction can be tracked to prior transactions repeatedly. It improves the traceability and the transparency of the data recorded in the blockchain.

- Transparency. Every transaction, be it tangible or non-physical, can be traced from the start to the finish with blockchain. For a transaction to be accepted and recorded on the blockchain, all the participants or nodes must agree to follow the same rules.

- Single source of truth. In a blockchain, there is only one source of truth, the distributed ledger. So, to know who owns something, or to examine a particular transaction, you just need to go to one spot.

Characteristics	Public Blockchain	Private Blockchain	Consortium Blockchain
Permission Read	Public Class	Could be public or restricted	May be public or restricted
Determination of Consensus	All miners	Only one organization	Designated set of nodes
Efficiency	Low	High	High
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Centralized	No	Yes	Partial
Consensus	Permission less	Permissioned	Permissioned

Table 3: Comparisons between Private, Public and Consortium Blockchain[269]

Nomenclature of blockchain systems

Current blockchain systems can be loosely divided into three types: public blockchain, private blockchain and consortium blockchain.[270] We compare these three versions of blockchain from different perspectives. Again, as public blockchain is open to the globe, it can attract numerous users. Communities are also very active. Many public blockchains emerge day by day. As for consortium blockchain, it may be applied to numerous business applications. Currently Hyperledger is developing business consortium blockchain frameworks. Ethereum also has provided tools for building consortium blockchains.[271] As for private blockchain, there are still many companies implementing it for efficiency and auditability.

- Consensus determination. In public blockchain, each node can take part in the consensus process. And only a selected set of nodes are responsible for validating the block in consortium blockchain. As for private chain, it is fully controlled by one organization who can determine the final consensus.

- Read permission. Transactions in a public blockchain are visible to the public while the read permission depends on a private blockchain or a consortium blockchain. The consortium or the organization can decide whether the stored information is public or restricted.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

- Unchangeability. Since transactions are stored in different nodes in the distributed network, so it is nearly impossible to tamper the public blockchain. However, if the majority of the consortium or the dominant organization wants to tamper the blockchain, the consortium blockchain or private blockchain can be reversed or tampered.

- Efficiency. It takes plenty of time to propagate transactions and blocks as there are a large number of nodes on public blockchain network. Taking network safety into consideration, restrictions on public blockchain will be much more strict. As a result, transaction throughput is limited and the latency is high. With fewer validators, consortium blockchain and private blockchain can be more efficient.

- Centralized. The main difference among the three types of blockchains is that public blockchain is decentralized, consortium blockchain is partially centralized and private blockchain is fully centralized as it is controlled by a single group.

- Consensus process. Everyone in the world can join the consensus process of the public blockchain. Different from public blockchain, both consortium blockchain and private blockchain are permissioned. One node needs to be certificated to join the consensus process in consortium or private blockchain.

Consensus Algorithms

In blockchain, how to reach consensus among the untrustworthy nodes is a transformation of the Byzantine Generals (BG) Problem.[273] In BG problem, a group of generals who command a portion of Byzantine army circle the city. The attack would fail if only part of the generals attack the city. Generals need to communicate to reach an agreement on whether attack or not. However, there might be traitors in generals. Traitor can send different decisions to different generals. This is a trustless environment. How to reach a consensus in such an environment is a challenge. It is also a challenge for blockchain as the blockchain network is distributed. In blockchain, there is no central node that ensures ledgers on distributed nodes are all the same. Nodes need not trust other nodes. Thus, some protocols are needed to ensure that ledgers in different nodes are consistent. There are several common approaches to reach consensus in blockchain and that has been given below.

- **PoW** (Proof of work) is a consensus strategy used in Bitcoin network.[274] POW requires a complicated computational process in the authentication. In POW, each node of the network is calculating a hash value of the constantly changing block header. The consensus requires that the calculated value must be equal to or smaller than a certain given value. In the decentralized network, all participants have to calculate the hash value continuously by using different nonces until the target is reached. When one node obtains the relevant value, all other nodes must mutually confirm the correctness of the value. After that, transactions in the new block will be validated in case of frauds. Then, the collection of transactions used for the calculations is approved to be the authenticated result, which is denoted by a new block in the blockchain.

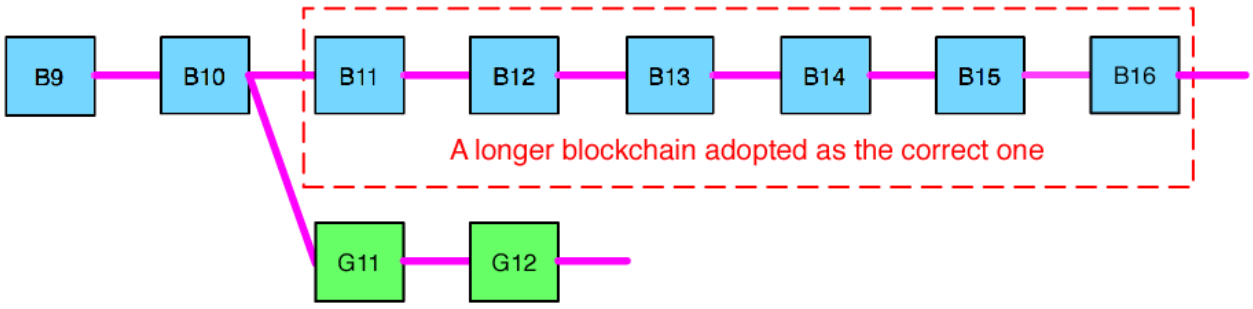

Figure 11: Example of a scenario of blockchain branches[275]

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

The nodes that calculate the hashes are called miners and the POW procedure is called mining. Since the calculation of the authentication is a time consuming process, an incentive mechanism (e.g., granting a small portion of Bitcoins to the miner) is also proposed.[276] In the decentralized network, valid blocks might be generated simultaneously when multiple nodes find the suitable nonce nearly at the same time. As a result, branches (or forks) may be generated as shown in Figure 11. The longer branch will be admitted as the main chain while the shorter one will be deserted. However, it is unlikely that two competing forks will generate next block simultaneously. In POW protocol, a chain that becomes longer thereafter is judged as the authentic one. Take Figure 11 as an example again. Consider two forks created by simultaneously validated blocks B11 and G11. Miners work on both the forks and add the newly generated block to one of them. When a new block (say B12) is added to block B11, the miners working on fork G11-G12 will switch to B12. Block G12 in the fork G11-G12 becomes an orphan block since it is no longer increased. Generally, after a certain number of new blocks are appended to the blockchain, it is nearly impossible to reverse the blockchain to tamper the transactions. In Bitcoin blockchain, when approximately six blocks are generated, the relevant blockchain is considered to be the authentic one (e.g., the chain of blocks B11, B12, B13, B14, B15 and B16 in Figure 11). Block interval depends on different parameter setting. Bitcoin block is generated about every 10 minutes while Ethereum block is generated about every 17 seconds. Miners have to do a lot of computer calculations in PoW, yet these works waste too much resources. To mitigate the loss, some PoW protocols in which works can have some sideapplications have been designed. For example, Primecoin[277] searches for special prime number chains which can be used for mathematical research. Instead of burning electricity for mining the POW block, proof of burn asks miners to send their coins to addresses where they cannot be redeemed.[278] By burning coins, miners get chances for mining blocks and they don't need powerful hardwares as POW.

Layers	**Main Technologies**		
Consensus Mechanism	Proof of Work (PoW)	Proof of Stake (PoS)	Delegated Proof of Stake (DPoS)
Security Mechanism	Asymmetric Encryption Algorithm	Hashing Algorithm	-
Storage Mechanism	Block-Chain Data Structure	-	-
Communication Mechanism	P2P	-	-

Table 4: The Technical Architecture of Blockchain[279]

- **PoS** (Proof of stake) is an energy-saving alternative to POW. Instead of demanding users to find a nonce in an unlimited space, POS requires people to prove the ownership of the amount of currency because it is believed that people with more currencies will be less likely to attack the network. Since the selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. In particular, Blackcoin[280] uses randomization to predict the next generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peercoin[281] favors coin age based selection. In Peercoin, older and larger sets of coins have a greater probability of mining the next block. Compared with PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many blockchains adopt PoW at the beginning and transform to PoS gradually. For instance, Ethereum is planing to move from Ethash (a kind of PoW)[282] to Casper (a kind of PoS)[283]. To combine the benefits of POW and POS, proof of activity is proposed. In proof of activity, a mined block needs to be signed by N miners to be valid.[284] In that way, if some owner of 50% of all coins exists, he cannot control creation of new blocks on his own. Sometimes stake can be other things, for example, in proof of capacity, miners have to allocate large hard drive space to mine the block.[285]

- **PBFT** (Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults.[286] Hyperledger Fabric utilizes the PBFT as its consensus algorithm since PBFT can handle up to 1/3 malicious byzantine replicas.[287] A new block is determined in a round. In each round, a primary will be selected according to some rules. And it is responsible for ordering the transaction. The whole process can be divided into three phase: pre-prepared, prepared and commit. In each phase, a node will enter next phase if it has received votes from over 2/3 of all nodes. So PBFT requires that every node is known to the network. Like PBFT, Stellar Consensus Protocol (SCP) is also a Byzantine agreement protocol. There is no hashing procedure in PBFT.[288] In PBFT, each node has to query other nodes while SCP gives participants the right to choose which

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

set of other participants to believe. Based on PBFT, Antshares has implemented their dBFT (delegated byzantine fault tolerance).[289] In dBFT, some professional nodes are voted to record the transactions instead of all nodes.

- **DPOS** (Delegated proof of stake). Similar to POS, miners get their priority to generate the blocks according to their stake. The major difference between POS and DPOS is that POS is a direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate a block. With significantly fewer nodes to validate the block, the block can be confirmed quickly, making the transactions confirmed quickly. Meanwhile, the parameters of the network such as block size and block intervals can be tuned. Additionally, users do not to need worry about the dishonest delegates because the delegates can be voted out easily. DPOS has already been implemented, and is the backbone of Bitshares.[290]

Property	**POW**	**POS**	**PBFT**
Identity management of nodes	Without permission	Without permission	With permission
Energy saving	No	partial	yes
Power tolerated	<25% computing power	<51% stake	<33,3% Defective replicas
Example	Bitcoin	Ethereum	Hyperledger

Table 5: Comparison between some consensus algorithms[291]

- **Ripple.** It is a consensus algorithm that utilizes collectively-trusted subnetworks within the larger network.[292] In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds. In contrast to that PBFT nodes have to ask every node in the network, each Ripple server has a Unique Node List (UNL) to query. UNL is important to the server. When determining whether to put a transaction into the ledger, the server will query the nodes in UNL. If the received agreements have reached 80%, the transaction will be packed into the ledger. For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20%.

- **Tendermint** is a byzantine consensus algorithm.[293] A new block is determined in a round. A proposer will be selected to broadcast an unconfirmed block in this round. So all nodes need to be known for proposer selection. It can be divided into three steps: 1) Prevote step. Validators choose whether to broadcast a prevote for the proposed block. 2) Precommit step. If the node has received more than 2/3 of prevotes on the proposed block, it broadcasts a precommit for that block. If the node has received over 2/3 of precommits, it enters the commit step. 3) Commit step. The node validates the block and broadcasts a commit for that block. if the node has received 2/3 of the commits, it accepts the block. The process is quite similar to PBFT, but Tendermint nodes have to lock their coins to become validators. Once a validator is found to be dishonest, it will be punished.

Different consensus algorithms have different advantages and disadvantages. However, different consensus algorithms use the following properties have been given below.[294]

- Node identity management. PBFT needs to know the identity of each miner in order to select a primary in every round while Tendermint needs to know the validators in order to select a proposer in each round. For PoW, PoS, DPOS and Ripple, nodes can join the network freely.

- Energy saving. In PoW, miners hash the block header continuously to reach the target value. As a result, the amount of electricity required to process has reached an immense scale. As for PoS and DPOS, miners still have to hash the block

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

header to search the target value but the work has been largely reduced as the search space is designed to be limited. As for PBFT, Ripple and Tendermint, there is no mining in consensus process. So it saves energy greatly.

- Tolerated power of adversary. Generally 51% of hash power is regarded as the threshold for one to gain control of the network. But selfish mining strategy in PoW systems can help miners to gain more revenue by only 25% of the hashing power.[295] PBFT and Tendermint is designed to handle up to 1/3 faulty nodes. Ripple is proved to maintain correctness if the faulty nodes in a UNL is less than 20%.

- Example. Bitcoin is based on PoW while Peercoin is a new peer-to-peer PoScryptocurrency. Further, Hyperledger Fabric utilizes PBFT to reach consensus. Bitshares, a smart contract platform, adopts DPOS as their consensus algorithm. Ripple implements the Ripple protocol while Tendermint devises the Tendermint protocol.

- PBFT and Tendermint are permissioned protocols. Node identities are expected to be known to the whole network, so they might be used in commercial mode rather than public. PoW and PoS are suitable for public blockchain. Consortium or private blockchain might has preference for PBFT, Tendermint, DPOS and Ripple.

Advances on consensus algorithms

A good consensus algorithm means efficiency, safty and convenience. Current common consensus algorithms still have many shortages. New consensus algorithms are devised aiming to solve some specific problems of blockchain. The main idea of PeerCensus[296] is to decouple block creation and transaction confirmation so that the consensus speed can be significantly increased. Besides, Kraft proposed a new consensus method to ensure that a block is generated in a relatively stable speed.[297] It is known that high blocks generation rate compromise Bitcoin's security. So the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection rule is proposed to solve this problem. Instead of the longest branch scheme,[298] GHOST weights the branches and miners can choose the better one to follow. Recently some researchers have proposed a new consensus algorithm for peer-to-peer blockchain systems where anyone who provides non-interactive proofs of retrievability for the past state snapshots is agreed to generate the block. In such a protocol, miners only have to store old block headers instead of full blocks.

Blockchain Potential

Blockchain technology isn't just ordinary hype that people will forget after a few days, rather it's here to stay. All the blockchain's important features are making a whole another level of impact on the web. It's infused with all sorts of new techs. However, blockchain is giving rise to a lot of controversies still if people can utilize the ideology behind all benefits of blockchain they can make a brighter and shinier future for everyone.[299] In fact, Blockchain is going to change the world. Blockchain features and versatile capabilities are truly making changes in every aspect of life around the world. Blockchain has enough potential to benefits financial institutions. Blockchain technology has the potential to result in a radically different competitive future for the financial services industry.[300] This technology emphasis and accelerate other technologies. Blockchain has huge potential and are very much useful technology in 21st century due to following capability and facilities.

- **Less Failure:** Everything in the blockchain is fully organized, and as it doesn't depend on human calculations it's highly fault-tolerant. So, accidental failures of this system are not a usual output.
- **User Control**: With decentralization, users now have control over their properties. They don't have to rely on any third party to maintain their assets. All of them can do it simultaneously by themselves.[301]
- **Less Prone to Breakdown:** As decentralized is one of the key features of blockchain technology, it can survive any malicious attack. This is because attacking the system is more expensive for hackers and not an easy solution. So, it's less likely to break down.
- **No Third-Party**: Decentralized nature of the technology makes it a system that doesn't rely on third-party companies; No third-party, no added risk.
- **Zero Scams:** As the system runs on algorithms, there is no chance for people to scam you out of anything. No one can utilize blockchain for their personal gains.[302]
- **Transparency:** The decentralized nature of technology creates a transparent profile of every participant. Every change on the blockchain is viewable and makes it more concrete.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

- **Authentic Nature:** This nature of the system makes it a unique kind of system for every kind of person. And hackers will have a hard time cracking it.
- **Extremely secure**: It's extremely secure because it offers a special disguise known as Cryptography.[303] Blockchain has emerged as one of the most innovative application models with capabilities for integrating consensus mechanisms, distributed data storage, digital encryption technology, peer-to-peer transmission, and other computing technologies. It has provided an effective platform for secure and decentralized information exchange. As a matter of fact, digital encryption technologies are the core elements of blockchain technology, thereby drawing attention towards blockchain cryptography. The assurance of security for user information and transaction data is a mandatory condition for encouraging the popularity of blockchain.[304] Cryptography lays another layer of protection for users. Cryptography is a rather complex mathematical algorithm that acts as a firewall for attacks.
- **Hashed cryptographically**: Hashing is quite complex and it's impossible to alter or reverse it. No one can take a public key and come up with a private key. Also, a single change in the input could lead to a completely different ID, so small changes aren't a luxury in the system. If someone wants to corrupt the network he/she would have to alter every data stored on every node in the network. There could be millions and millions of people, where everyone has the same copy of the ledger. Accessing and hacking millions of computers is next to impossible and costly. That's why it's one of the best blockchain features. As it's too hard to bypass, we won't have to worry about hackers taking all our digital assets from us. Every piece of information on the blockchain is hashed cryptographically. In simple terms, the information on the network hides the true nature of the data.[305] For this process, any input data gets through a mathematical algorithm that produces a different kind of value, but the length is always fixed.
- **Distributed Ledger**. As we know that, a public ledger will provide information about a transaction and the participant. It's all out in the open, nowhere to hide. The case for private or federated blockchain is a bit different. But still, in those cases, many people can see what really goes on in the ledger. That's because the ledger on the network is maintained by all other users on the system. This distributed computational power across the computers to ensure a better outcome. The result will always be a higher efficient ledger system that can take on the traditional ones.[306]
- **Irreversible Hashing.** This technology is quite complex, and it's impossible to alter or reverse it. No one can take a public key and come up with a private key. Also, a single change in the input could lead to a completely different ID, so small changes aren't a luxury in the system.[307]

Prospect and Multipurpose Uses of Blockchain Technology

Blockchain is the latest 'disruptive innovation' that has caught scholars' attention. It is the underlying technology for Bitcoin and other digital currencies. Stakeholders like developers, entrepreneurs, and technology enthusiasts claim blockchain has the potential to reconfigure the contemporary economic, legal, political and cultural landscape. Skeptics claim the concept and its applications remain ambiguous and uncertain. Business scholars began publishing studies on the emergence and impact of blockchain, bitcoin, and related projects in 2014.[308] Blockchain is an emerging and potentially disruptive technology that business scholars have recently begun investigating. The first and most famous blockchain application is Bitcoin. Its anonymous inventor, Satoshi Nakamoto released it in 2009 during the global financial crisis. Their goal was to create a new kind of digital currency that was decentralized and removed the control of governments, banks, and other traditional financial institutions. Blockchain is a decentralized, digital ledger that facilitates peer-to-peer value transfers of all sorts, from digital currency to physical commodities and land titles, without the need for an intermediary such as banks, accountants, or lawyers.[309] Blockchain technology is at the heart of many exciting prospects aimed at improving efficiency, transparency, and security, across all sorts of business and social transactions. Since its creation, Bitcoin and a host of alternative cryptocurrencies, known as 'alt coins,' has captured public attention as a source of fascination, skepticism, and debate for economists and financial experts. Some of the earliest media coverage characterized cryptocurrencies as evil due to their association with nefarious commerce on the dark web like, illicit weapons and drugs and since they often escape public record or regulation. [310] Soon after other journalists hailed cryptocurrencies as a solution to the pressing problems of the current economy, such as poverty, debt, and hyperinflation. More broadly, stakeholders like developers, entrepreneurs, and technology enthusiasts claim blockchain has the potential to reconfigure the contemporary economic, legal, political, social landscape.[311]

The technology is simple yet powerful - literally a chain of blocks of information, each verified by a distributed network of nodes. To conceptualize the rapid development of blockchain technologies, organizes the different types of blockchain activity into three categories. Blockchain 1.0 is currency, as in digital payment systems and cryptocurrencies. Blockchain 2.0 is contracts, as in the more sophisticated value transfers of stocks, bonds, loans, mortgages and titles via smart contracts. Blockchain 3.0 is applications beyond finance, as in government, health, science, arts and culture. Recent research has explored blockchain's potential to help citizens reclaim control of their personal data, make the insurance industry more transparent, manage supply chains, manage employee benefits, transform electronic health records, etc.[312] Over the past decade, the emergence of blockchain has sparked myriad initiatives

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

to re-imagine, and in some cases begin to disrupt, financial systems through cryptocurrencies. These types of changes can have far reaching effects on companies and industries because they disrupt information systems and social relations. The field of information management is particularly concerned with the various technologies and activities that influence changes in patterns of behaviour in customers, people, and organizations. Blockchain enthusiasts claim that the technology will have a significant effect on precisely these processes and a host of others such as AI, ML and IoT.

Scholars of technology and society have shown that innovations do not consist solely of new technical devices, but also of new social and organizational arrangements. In the earliest stages of blockchain scholarship, business scholars explore its instrumental value for achieving new levels of corporate efficiency and profitability. Again, business scholars tend to be early movers or early adopters. They tend to investigate emerging phenomenon like the Internet, social media, big data, and now blockchain, to understand their role in organizational change. Like the Internet, blockchain is projected to be the cornerstone of new types of business and social interaction. It is already affecting these, through its decentralized architecture, trustless and permissionless systems, smart contracts, as well as data, privacy, and information management. According to its some advocates, blockchain is a prime example of a 'disruptive innovation'. Disruptive technologies, like the Internet, are rarely 'positive' or 'negative,' but productive of and produced in contexts of social change.The Internet enabled communication and social relations to spread globally at a reach and speed never before seen in human history. It changed how we understand time and space, both expanding and intensifying human relations and organizations. The Internet connected us and helped create a global village.

Blockchain is changing the nature of social relations and organizations in the global village. Blockchain is changing the interactive effect of human relations by facilitating trustless technologies such as the smart contract. A smart contract removes the need to build trust between individuals and organizations through intermediaries like lawyers and social activities like meetings where actors get to know one another. Smart contracts build the transactional relationship of a contract into technical code that is executed automatically. Business scholars strive to understand what new social and economic forms will be produced by actors developing blockchain technologies and applications. However, scholars have investigated blockchain as a disruptive innovation for an array of civic arenas including e-voting, degree verification, and land registries. Scholars have started to publish systematic reviews of blockchain research in a number of fields. For example, adoption of blockchain platforms in health care as well as technical perspective, focused on topics such as security, performance, data integrity, privacy, and scalability of blockchain practices. From those studies also highlighted a gap in scholarship and the need for further blockchain research in other domains including business. This gap needs to be filled up. There is a need for research on the social, economic, and ethical dimensions of blockchain adoption and diffusion. Technical-focused systematic review of relevant research work by analyzing important business processes can also shape up with the help of blockchain. Successful uses of blockchain and its prospect in different sector have been described below.

- Nowadays, the interest in the IoT is rising considerably with the development of information communication which sanctions persistent, direct and automated Machine-to-Machine (M2M) interaction or Cyber-Physical Systems (CPSs).[313] The IoT system endeavours to implement a logic which is based on computer programs to an ecosystem of things or devices, which then can be controlled or monitored by a centralized engine (typically based on cloud computing). Entities or devices in IoT are provided with a digital description in the physical world. This digital 'wrapper' authorizes communication with Information and Communications Technology (ICT) entities which are present on a private, public, hybrid cloud, on a Local Area Network (LAN), or at the ends of Wide Area Network (WAN). IoT applications are categorized into two broad areas. The first class includes various types of sensing applications, such as traffic monitoring, power administration, Intelligent Transportation Systems (ITSs), smart cities, crowdsensing, industrial automation, etc. Whereas, the second class deals with data analytics rather than the physical aspects and characteristics of the sensors themselves. These applications refer to the elementary renovation of business processes that are linked to marketable functions such as insurance, banking, organizational processes, healthcare provision enhancement, etc. Considering the broadening scope of IoT implementation, security and safety of the network becomes a critical aspect of the IoT system, especially under constrained resources in terms of power, storage and controlled nodes proficiency. Furthermore, limited capability of operating systems, vendor-specific application installations, deployment in uncontrolled open environment and limited computational capability of the end nodes are several other factors that contribute to this vulnerability of IoT systems.

Owing to these challenges, it is necessary to rethink and fundamentally restructure the IoT systems. Nowadays, blockchain has emerged as the most suitable candidate technology that promises to support a distributed and secure ecosystem for the IoT. Blockchain has received enormous attention from various industries including finance, agriculture, logistics and insurance. Owing

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

to its ability to digitise transactions efficiently, it contributes towards making several processes faster, leaner and more transparent. Blockchain can be described as a chain of cryptographically linked timestamped blocks that operates as a distributed ledger whose data is shared among its peers. Therefore, blockchain is capable of solving the security issues associated with the traditional IoT systems by leveraging a distributed and secure environment. Due to its decentralized, immutable, auditable and fault tolerant features, several researchers are making efforts to eliminate the need for a central trusted authority and leverage blockchain to support decentralized IoT communications. The advantages associated with a blockchain based IoT systems are manifolds. It can easily mitigate single point of failure, promotes fault tolerance capabilities and enables end-to-end communications without involvement of a centralized server. Again, participants in a blockchain network can verify data integrity as well as the sender's identity. Furthermore, the tamper proof data storage capability of blockchain enables to leverage secure software updates to IoT devices. Additionally, blockchain stores the data and event logs in an immutable manner thereby guaranteeing traceability and accountability.

In recent research, numerous researchers have tried to exploit the benefits of integrating blockchain with the IoT in varied application scenarios. Several survey articles focussed on reviewing these solutions in varied degree of dept and scope. Huckle et al. (2016) highlighted the benefits of integrating blockchain technology and IoT for shared economy applications.[314] Similarly, Christidis et al. (2016) highlighted the role of smart contracts and blockchain for IoT systems.[315] However, these works did not provide a detailed description of the security improvements in IoT using blockchain technology and the challenges associated with this integration. In another work, Zheng et al. (2018) comprehensively surveyed blockchain technology in various application and technological perspectives. The work highlighted the architecture, consensus schemes, applications and challenges related to blockchain.[316] Alladi et al. (2019) attempted to review existing blockchain applications in Industrial Internet of Things (IIoT) settings and highlighted the associated industry specific challenges. However, the work failed to highlight the approaches, security benefits and challenges associated with the integration of blockchain and IoT.[317] Alotaibi et al. (Alotaibi, 2019) attempts to survey the recent blockchain-based advances to overcome the cyber security challenges in IoT but does not throw enough light on background, transaction process, consensus algorithms and the application areas of blockchain technology.[318] In another work, Li et al. (2020) investigated various types of security threats and attacks related to blockchain systems.[319] Similarly, Mohanta et al. (2020) highlighted the IoT architecture along with its enabling technology and presented an in-depth description of various security issues within the IoT system. However, these works did not highlight the security benefits associated with the integration of IoT and blockchain technology.[320] In another work, Sengupta et al.(2020) presented a detailed description of security attacks in IIoT along with the proposed countermeasures and highlighted the importance of blockchain technology towards addressing the related issues.[321] However, the work was not fully successful to explore various aspects of blockchain technology including the transaction process, consensus mechanisms and challenges associated with integrating blockchain technology and IoT.

IoT finds huge range of applications in our day-to-day life and the internal composition of these applications includes the interaction of end-devices and networking technologies. Heterogeneity and decentralization are two key features of IoT. Given its large structure and extensively large piles of data to be analysed, decentralization property is crucial. Data is gathered, analysed and recorded in a decentralized approach by the IoT devices. IoT is optimizing and transforming physical procedures to convert them into the elements of the digital era. In this process, piles of information are being created that are providing knowledge and insights at unthinkable levels. This data helps to improve the quality of life through the digitalization of facilities in every major sector. The implementation of IoT integrated with Cloud Computing has proved to be instrumental.[322] Similarly, blockchain has the potential to solve many IoTproblems.Developers and researchers around the world are innovating ingenious ways to integrate blockchain in IoT systems.[323] These use cases focus on taking benefits from the inherent features of blockchain such as immutability, fault tolerance, capability to run smart contracts, cryptographic security, decentralized control, data integrity and authentication. It is evident that some of the applications use patented blockchains developed for their particular a model or a scheme.As we know that, blockchain is a powerful technology, it is still under development several obstacles are faced in the adoption of blockchain for IoT systems irrespective of its innumerable advantages. Majority of these challenges arise due to the utilization of blockchain technology in systems that have limited capabilities in terms of resources, scalability and privacy preservation.[324] The exponential rise in adoption of IoT led to the emergence of numerous security vulnerabilities ranging from attacks on data to attacks on devices. The current IoT devices are insecure and impotent of defending themselves majorly due to its resource constrained nature, immature standards, poor interoperability and absence of secure software and hardware design, deployment and development. This has drawn huge attention from the research community and numerous efforts have been carried out so far and will be continue.

- Cryptocurrencies such as Bitcoin, SETLcoin, Ether, Solar Coin, or Liberty Reserve exist since 2009.[325] Because of their decentralized control, they are often considered a threat or alternative to the conventional centralized banking system.[326]

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

While the technological consequence of some such currencies, especially of Bitcoin,[327] has drawn great interest, so far there is little discussion about the overall area of cryptocurrencies and very little academic work addressing its ethical meaning.[328] The promise hinges on the fact that blockchain or distributed ledger technologies (DLT) can redefine digital trust and can remove middlemen producing a new paradigm of management that might potentially disrupt established systems of governance.[329] The disruptive nature lies on the potential of replacing top-down control with consensus and also in the underlying philosophy of distributed consensus, open source, transparency and community based decision-making.[330] According to the research institute of the Finnish economy,[331] these characteristics could instigate further societal changes and implications. According to a recent Gartner assessment, blockchain technologies have already past the top of exaggerated expectations in the hype cycle and are anticipated to be 2–5 years from broad implementation.[332]

- Attribute-based encryption (ABE) allows users to encrypt and decode data based on attributes. It realizes fine-grained access control and can successfully handle the one-to-many encryption and decryption problem in open cloud application.[333] Linear secret sharing scheme (LSSS) is the common access structure with a matrix on the characteristics in ABE schemes, which may depict AND, OR, threshold operations, etc. However, LSSS access structure does not portray the complex and dynamic access policy of attributes, such as the convoluted linkage of different attributes and the generation of dynamic attributes.[334] It greatly hinders the expansion of the practical application of ABE. Besides, there exists another difficulty; attribute authority (AA) in classic ABE has a concentration of power and readily suffers from single-point failure or privacy leakage for being attacked or corrupted. Blockchain is a decentralized, tamper-free, traceable, and multi-party distributed database technology. Consortium blockchain (CB) is a partially centralized blockchain, whose openness lies between the public blockchain and the private blockchain.[335] The CB technology strengthened the authority and reliability of AA by openly recording AA's attribute key distributions in CB transactions.[336]

- It is conceivable to design an effective cooperation method for secure cloud file sharing combining blockchain and attribute-based encryption (ABE). Blockchain enables us to establish access control as a smart contract between data owner and users.[337] Each data owner establishes its own smart contract where in a data user can request to access a certain file by registering a transaction.[338] In response transaction, the data owner sends the appropriate credential to the user so enabling her/him to decrypt the desired file on the cloud storage. This technique is decentralized, fault tolerant and guarded against denial-of-service (DoS) assaults.[339] The cipher-key, which is used for file encryption, is embedded inside a set of coefficients of a polynomial so-called access polynomial.[340] It is a metadata that is connected to the encrypted file in the cloud storage. By using the credential receiving in response transaction and access polynomial, the data user can recover the cipher-key. In order to maintain user anonymity and enforce their own access policies to the file, the data owner employs the ABE technique in response transactions. By altering the access polynomial coefficients, this technique facilitates quick revocation of user access without requiring additional communication with users whose access has not been canceled. This approach can be secure in terms of participant authentication and credential information confidentiality.[341]

- It is challenging for patients to actually take ownership of their electronic health records (EHRs) in medical situations facilitated by edge clouds. However, it is simple for medical professionals to alter hospital data in order to reject inaccurate treatment records, which makes it challenging to defend patients' rights. An attribute-based encryption security strategy for EHRs paired with a blockchain to safeguard EHRs in edge cloud environments can be developed to enhance patient control over EHRs. A confidential encryption technique is used to communicate treatment information, such as treatment time, treatment doctor, and additional information, in a scheme where the agreement procedure between the hospital and the patient is finished before the ABE stage.[342] The integrity of the data is ensured by keeping the submitted encrypted data on the blockchain as transaction records, which makes the traceability of EHR creation easier. The outsourced ciphertext policy's ABE scheme regulates access to EHRs, and fine-grained attribute revocation can be used to guarantee the ciphertext's security.[343] This algorithm along with other algorithms undergo experimental testing, and a satisfactory result is obtained by comparing the computational delay of each role and the computational cost of each step of the algorithms.[344]

- Because blockchain may resolve the issue of information asymmetry and allow users who do not trust one another to cooperate without the involvement of third-party intermediaries, it has been widely employed in many sectors. The majority of existing blockchain access control solutions use attribute-based encryption instead of attribute authorization, which has the drawback that the authority is overworked and needs to be completely reliable.[345] By enhancing the current blockchain privacy protection technique, a useful blockchain access control strategy based on multi-authority attribute-based encryption can be created.[346] The blockchain is utilized for autonomous identity management in order to finalize the process of

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

initializing user identification and issuing attribute certificates.[347] The reputation proof consensus process is employed in the selection of attribute authorities. Keys are generated via the distributed key generation protocol, and the linear secret sharing mechanism is enhanced. The private data that has to be uploaded to the blockchain is encrypted and access controlled using the hierarchical relationship of the access structure.[348]

- Distributed ledgers, or blockchains, are a new technology that has attracted a lot of attention from the academic community, national governments, energy supply companies, entrepreneurs, and technology developers. Blockchain technology is seen by many sources with these backgrounds as having the potential to be highly innovative and beneficial. Blockchains, especially when paired with smart contracts, promise to provide transparent, safe, and impenetrable platforms that can facilitate creative business solutions. Energy systems will require substantial investment to meet aggressive emission reduction targets. An estimated €200 billion would need to be invested annually in generation, networks, and energy efficiency improvements in the EU alone in order to make the transition to a more secure and sustainable energy system.[349] By 2030, the US will need to upgrade its power networks, spending $2 trillion.[350] In order to reduce the necessary investment, energy systems must implement smart management and control measures.[351] These are difficult jobs since energy systems are becoming more complex, dynamic, decentralized, and "multi-agent," meaning there are more actors and alternative courses of action. The need for sophisticated data exchanges and communication between various power network components is growing, which makes central administration and operation more difficult. It takes local distributed control and management strategies to meet these tendencies toward digitalization and decentralization.[352] The main goal of distributed ledger technologies, or DLTs, is to eliminate central management in order to enable distributed transactions. Blockchains may therefore be able to assist in resolving the issues that decentralized energy systems are facing.
- Blockchains are distributed and shared ledgers or data structures that hold digital transactions securely without the need for a central authority. What's more, blockchains enable smart contracts in peer-to-peer (P2P) networks to be automatically executed.[353] Alternatively, they can be thought of as databases that let several users to concurrently edit the ledger, potentially producing different chain versions. Rather of having a single trusted center manage the ledger, every network participant has a copy of the chain of records and uses consensus to decide if the ledger is still legitimate. Research on the precise process of reaching consensus is still continuing, and it may vary depending on the needs of various application areas. Blockchain networks are robust and safe because cryptography links new transactions to older ones. Transparency and reliable, tamper-proof records are provided by the ability for any network member to verify the validity of transactions. The energy industry is just beginning to realize the promise of blockchain technology, as evidenced by the growing number of startups, pilots, trials, and research initiatives. According to a German Energy Agency poll of decision-makers in the energy sector, close to 20% of respondents think blockchain technology would revolutionize the way energy suppliers operate.[354] Seventy executives from the energy industry, including utility companies, energy providers, network operators, generators, and aggregators, provided their opinions for the poll. Over 50% of survey respondents have already started working on blockchain-related innovations. Numerous energy utility businesses are interested in learning more about distributed ledger technologies (DLT) and how they might help with sustainability and the low-carbon transition.[355] Furthermore, as digital assets that can be traded across borders, blockchain or distributed ledger technologies can undoubtedly benefit energy system operations, markets, and consumers.[356,357] Senior consultancy and commercial reports from Deloitte and PWC indicate that blockchains have the potential to drastically disrupt energy-related products and commodities. In addition to providing disintermediation, transparency, and tamper-proof transactions, blockchains most critically offer innovative ways to enable consumers and small-scale renewable energy producers to participate more actively in the energy market and profit from their assets.[358] Blockchain technology has made it possible to apply sharing economies to the energy sector, which has caused a number of authors to discuss new market models and the democratization of energy.[359] Blockchain innovation in the energy sector is now being pursued by numerous research and commercial organizations. Since the field of blockchain research and development is developing quickly, a study of this emerging technology is necessary to advance knowledge, contribute to the body of information on blockchains, and realize their potential.[360]

Applications of Blockchain

Applications of blockchain technology are numerous and varied. We provide an overview of a number of common blockchain applications in this section.[361] The uses of blockchain technology are broadly divided into several categories, including finance, management, defense, automotive, stock exchange, Internet of Things, voting, public and social services, reputation management, healthcare, education, energy, agriculture, law enforcement, asset tracking, insurance, cyber-security, advertising, security and

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

privacy, and digital records. Numerous typical blockchain application domains are depicted in Figure 6 below. Figure 12 below depicts an application domain for blockchain technology.

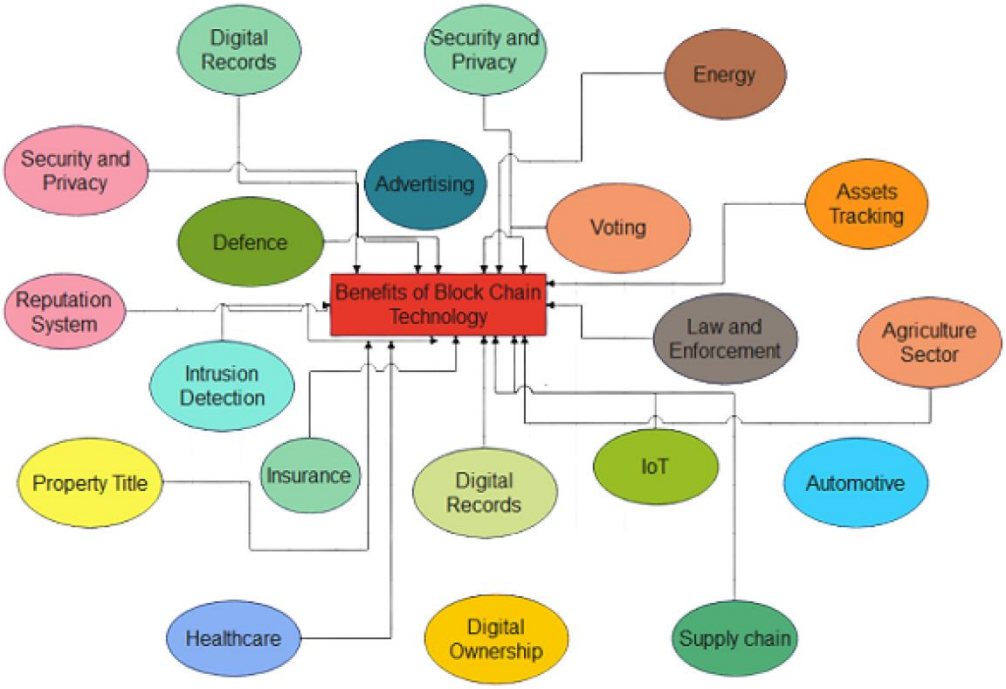

Figure 12: Blockchain technology application domains[362]

Monetary

- **Banking and related Services.** Traditional financial and business services have been greatly impacted by the emergence of blockchain platforms like Bitcoin. According to Peters et al. blockchain technology has the potential to upend the financial industry.[363] Blockchain technology has numerous applications, such as financial asset clearing and settlement. Additionally, Morini et al. demonstrated that there are actual business scenarios that can use blockchain to lower costs and risks,[364] such as the collateralization of financial derivatives. Big software businesses have also been very interested in blockchain, and companies like IBM[366] and Microsoft Azure[365] are starting to offer Blockchain-as-a-Service.

- **Business Conversion.** Blockchain can assist traditional firms in seamlessly completing their enterprise transformation, in addition to the advancement of financial and business services. Take postal operators (POs) as an example. Blockchain and cryptocurrency technology can assist traditional postal operators (POs), who currently serve as a basic middleman between customers and merchants, in expanding their activities to include the supply of new financial and non-financial services. Jaag and Bach examined how blockchain technology might benefit POs and asserted that each PO could create their own postcoin, a Bitcoincolored coin.[367] With their extensive retail network, POs can swiftly gain traction as the public views them as reliable authorities. Furthermore, it has been demonstrated that blockchain technology presents POs with commercial prospects in supply chain management, identity services, and device management.

- **P2P Lending Platform.** Blockchain technology can contribute to the safe and dependable development of P2P lending markets. Noyes investigated the creation of a P2P financial MPC (Multiparty computing) market by fusing peer-to-peer techniques and multiparty computing protocols.[368] Offloading computing chores to a network of anonymous peer-processors is possible with the blockchain-based MPC market.

- **Risk supervision**. Financial technology (FinTech) relies heavily on risk management frameworks, which can now function more effectively when integrated with blockchain technology. Pilkington offered a unique framework for risk management that analyzes investment risk in the Luxembourgish situation using blockchain technology. [369] Today's investors who hold

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

their shares through a chain of custodians run the danger of experiencing any one of these issues. Investments and collateral can be chosen rapidly with blockchain's assistance rather than requiring careful thought. According to Micheler and Heyde, a novel system can achieve the same level of transactional safety while lowering custody risk when it is integrated with blockchain.[370] Additionally, decentralized autonomous organizations (DAO) can collaborate on commercial projects thanks to blockchain-based smart contracts. A highly reliable DAO-GaaS conflict model was put out to protect consistency rules caused by business semantics.[371]

The Internet of Things

One of the most exciting information and communication technologies (ICT) to emerge recently is the Internet of Things (IoT).[372] It is suggested that the Internet of Things (IoT) connects things, also known as smart items, to the network and offers users a range of services.[373] The Maritime Industry, smart homes, e-health, smart grids, and logistic management using Radio-Frequency Identification (RFID) technology are some of the common killer applications of IoT. Blockchain technology may help the Internet of Things industry.

- **eCommerce.** Currently, there are various IoT e-business models that enable smart property transactions based on smart contracts and blockchain technology. Distributed Autonomous Corporations (DAC) are used as a decentralized transaction entity in these schemes. Without the involvement of a third party, people share sensor data and swap DACs for currencies.

- **Security and seclusion.** Another significant issue with the IoT sector is the protection of privacy and safety. Blockchain technology can also aid in enhancing IoT application privacy. A mechanism exists for commissioning different IoT devices into a cloud environment while maintaining anonymity.

- Numerous architectural solutions have been put out to assist devices in demonstrating their manufacturing provenance without the need for third-party authentication, and they are permitted to register anonymously. IBM announced their proof of concept for Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT), a system that creates a dispersed network of devices by utilizing blockchain technology. Home appliances will be able to recognize malfunctions and automatically download software upgrades thanks to ADEPT.

Social and Public Services

Blockchain technology is widely applicable to social and public services.

- Registration of Land. Land registration [65] is one of the common uses of blockchain technology in public services. It allows land information, including its physical condition and associated rights, to be registered and made public on blockchains. Additionally, any land-related transactions, such a land transfer or the creation of a mortgage, can be tracked and managed on blockchains, which enhances the effectiveness of public services.

- Conserving energy. Blockchains can also be applied to renewable energy. The solarcoin was proposed by Gogerty and Zitoli [36] in an effort to promote the use of renewable energy sources. Specifically, solarcoin is a type of virtual money that rewards solar energy providers. As long as you have produced solar energy, the solarcoin foundation may award you with solarcoins in addition to the standard method of obtaining coins through mining.

- instruction. The original purpose of blockchain technology was to facilitate trustless monetary transactions. However, blockchain technology may be used in the online education sector if we consider the process of teaching and learning to be the currency. Blockchain learning was suggested in [30]. Teachers can pack and insert blocks into a blockchain to facilitate blockchain learning, and learning objectives can be viewed as currencies.

- Freedom of Speech. Furthermore, DNS and identity management on the Internet can be secured with blockchain technology. One experimental open-source technology that enhances decentralization, security, privacy, censorship resistance, and speed of DNS and identities is Namecoin. By strengthening the internet's resistance to censorship, it safeguards the right to free speech online.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

- Additional social events. Other governmental services like income taxation, patent administration, and marriage registration can also be implemented with blockchain technology.[374] Mobile devices with digital signatures embedded may take the role of seals that must be attached to papers submitted to administrative departments in the future public services connected with blockchain technology. Large amounts of paperwork can be saved in this method.

Reputation Management

One key indicator of how much the community trusts you is your reputation. People view you as more trustworthy the better your reputation is. A person's reputation can be assessed based on their prior dealings and relationships with the community. The number of instances of fabricating personal reputation records is on the rise. For instance, in order to build a solid reputation in e-commerce, numerous service providers enlist a large number of fictitious consumers. Perhaps blockchain can help with this issue.

- **Scholars**. Among academics, reputation is significant. A distributed system built on blockchain can be utilized for reputation and academic records. An initial award of educational reputation money will be issued to each institution and intellectual worker. An organization may give a staff member an award by transferring part of their reputation records to them. All reputation changes are clearly detectable since blockchain records transactions.

- **Online community**. It's critical to be able to judge a member's reputation inside an online group. It is conceivable to create a blockchain-based reputation model that customers may use to sign a voucher indicating their satisfaction with the service and desire to provide positive comments. In order to deter a Sybil attack, a service provider must withhold an additional percentage of the money once the voucher is signed as a voting fee from the network.
- Reputation of a service provider is determined by voting fee amount. It is possible to create a novel reputation system that works well across several networks. To store the single dimension reputation value (0 or 1) from the completed transactions, they specifically constructed a second blockchain. Use file sharing as an illustration. A file is sent from entity A to entity B. After getting the file, B sends a transaction that includes the score, the file's hash, and B's private key in order to confirm B's identity. Subsequently, the miners get in touch with A and B to verify that the transaction proceeds without any issues. Reputation records are practically hard to manipulate with because transactions are maintained on blockchain.

Privacy and Security

These days, a variety of mobile services and gadgets are widely used, and this has made them vulnerable to rogue nodes. Many anti-malware filters have been developed, using pattern matching techniques that keep and update virus patterns on a central server, to detect suspicious files. Nevertheless, malevolent attackers can potentially exploit these centralized countermeasures. Blockchain technology may be used to enhance distributed network security. BitAV is an effective anti-malware ecosystem that can spread virus patterns on blockchain. BitAV can improve the fault tolerance in this way. BitAV can increase fault reliability, accelerate scanning, and make a system less vulnerable to deliberate denial-of-service assaults. Utilizing blockchain technology can also increase the security infrastructure's dependability. For instance, malicious attacks or hardware and software defects can frequently lead to a single point of failure in traditional public key infrastructures (PKIs). Blockchain technology can be utilized to build a privacy-aware PKI and increase the dependability of traditional PKIs at the same time.[375] However, privacy protection is crucial for a variety of IoT devices. These days, our sensitive data is being collected by numerous social network providers and mobile services, on top of the growing danger that malware will access our personal information. For instance, since its founding, Facebook has gathered more than 300 petabytes of personal data. Typically, the gathered information is kept on service providers' central servers, which are vulnerable to malicious attacks. Blockchain technology has promise for enhancing sensitive data security and privacy. A decentralized system for managing personal data that guarantees data ownership to the user can be created. Blockchain is used to implement such a system. Fine-grained access control, data ownership, transparency, and auditability, among other privacy-related concerns, can all be addressed by this approach.

Medical Care

These days, securely accessing, storing, integrating, and exchanging health records are a difficulty for both patients and healthcare professionals. Patients should be able to securely exchange their health records with any healthcare provider, control their records from anywhere in the world, and keep track of their medical history. Patients' direct access to data and a stronger infrastructure for data exchange should better position the healthcare system to handle public health risks when a severe illness outbreak, like COVID-19, breaks out. The privacy, security, and full ecosystem interoperability needs are not fully addressed by the technologies now in use

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

in the healthcare sector. Perhaps the best solution is blockchain. Blockchain technology can be extremely important in resolving some of the most important and difficult problems the healthcare sector is currently facing.[376]

Quick Settlement in Several Services and the Main System

Conventional banking methods move slowly. After all agreements have been completed, processing a transaction might occasionally take days. It is also highly susceptible to corruption. In comparison to conventional banking institutions, blockchain technology provides speedier settlement. This allows for comparatively speedier money transfers, ultimately saving a great deal of time for the user. Features of blockchain assist international workers understand its significance and make their lives easier. A lot of people leave their family behind and relocate abroad in quest of a better life and employment. However, it takes a long time and could be deadly in an emergency to send money to their families who live abroad. They may easily use the current, much faster blockchain technology to transmit money to their loved ones. Smart contract systems are guaranteed by blockchain. This may make it possible to conclude contracts of any kind more quickly. Even now, this remains one of the greatest advantages of blockchain features. Additionally, by eliminating the middleman, users can send money in a faster, safer, and more secure manner for a relatively small charge. Blockchain will influence and control global trade in this way in the future. On the other hand, under certain situations, the network cannot handle an excessive number of users, making a quicker settlement impractical. Nevertheless, the situation is becoming better every day, so a better answer to this problem should be apparent shortly.

Decentralization of the Production and Service Systems

The way that blockchain technology operates differs slightly from that of a standard financial institution. It uses a group of nodes to guarantee the blockchain's functionalities rather than depending on centralized authorities. A copy of the digital ledger is stored on each node in the system. Any node that wants to contribute a transaction must verify its legitimacy. It is entered into the ledger if the majority finds it to be legitimate. As a result, it becomes more transparent and impervious to corruption. It follows that no one can add any transaction blocks to the ledger without the approval of the majority of nodes. The fact that no one can simply go back and alter transaction blocks once they are added to the ledger really supports the list of essential blockchain features. As a result, it cannot be updated, deleted, or edited by any user on the network. Because the network is decentralized, there is no central body in charge of it or a single person responsible for maintaining its structure. The network is decentralized since it is instead maintained by a collection of nodes. One of the main components of blockchain technology that functions flawlessly is this. Blockchain users are in an easy-to-understand situation. We can access the system straight from the web and keep our assets there because it doesn't require any regulating authority. Anything from cryptocurrency to contracts, papers, and other priceless digital assets can be stored by us. And we'll be able to directly control them with your private key thanks to blockchain technology. It is evident that the decentralized structure is returning control and rights to the general public over their property.

Combating Corruption

As everyone knows, enormous sums of money are compromised annually through our usual methods. Trillions of dollars being spent by many people to shield their companies from outside hacking. But we frequently overlook the internal cybersecurity threats posed by dishonest individuals and institutions of power. We ultimately pay a price for our faith because there is frequently an internal link that allows these attacks to learn about all the security precautions. As you are all aware, banks are becoming less and less trustworthy, and in order to adequately address this problem, the global economy needs a trustless environment. Thus, it is reasonable to expect that blockchain will undoubtedly alter many of these situations in terms of a corruption-free environment. Businesses would be unable to hack into, change, or even steal information from their internal networking system if they began integrating blockchain technology.[377] Public blockchains provide as an excellent illustration of this. It is particularly transparent because all users have access to the transactions on the public blockchain.[378] However, private or federated blockchain may work best for businesses that want to maintain employee transparency and shield confidential data from prying eyes.[379]

Cryptocurrency is gaining traction.

Due to their consistent high returns, cryptocurrencies have emerged as a promising new asset class for investors. It is expected that the cryptocurrency market will continue to grow as more players from various industries express interest in its possibilities. Ten years ago, the only people experimenting with digital currencies were tech-savvy, privacy-conscious individuals who firmly disapproved of centralized financial institutions. You may now trade them on numerous cryptocurrency trading apps, including Binance, Coinbase, Robinhood, and many more.[380] Hardware cryptocurrency wallets are a wonderful way to keep our cryptocurrencies in a safe and secure manner. They have safe designs and integrated functions that make them perfect for holding big volumes of cryptocurrencies. They provide extra functions like NFT storage, DeFi, cryptocurrency transactions, etc. Therefore, a hardware cryptocurrency wallet is the best choice for us if we're seeking for a safe and secure means to store our cryptocurrency holdings. There are a lot of hardware wallets on the market, and choosing the right crypto hardware for our storage needs might be difficult.[381] A Bitcoin wallet is a

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

hardware or software application that allows you to store cryptocurrency assets such as bitcoins. Bitcoin can only be kept digitally in a crypto wallet, in contrast to Fiat Currencies like USD ($), which can be used as real currency in our wallets or digitally in our bank accounts. A Bitcoin wallet is quick, safe, and simple to use. When it comes to selecting the best Bitcoin wallet app, there are many of options available. But making the appropriate choice can be a daunting challenge.[382]

Blockchain's Problems and Solutions

The integration of blockchain with services computing primarily shows merits in two aspects: blockchain can potentially address key challenges of services computing, and services computing can also promote blockchain development.[383] These recent advances in blockchain technology bring opportunities to address the challenges of services computing because of its built-in encryption as well as digital signature schemes, decentralization feature, and intrinsic incentive mechanisms. Today, there are several issues brought about by the expansion of services computing. These challenges include:

(1) Risks to security and privacy: service providers frequently gather and keep customers' private-sensitive data without their knowledge or consent. Without the consent of the customers, the private information may be misused or inadvertently revealed to third parties. Data centers are also vulnerable to malicious assaults (such as DDoS attacks or hackers) and SPFs, among other security flaws.[385]

(2) Information Silo: Due to challenges in information exchange and reciprocal activities among various systems, diverse information systems inside a company or across multiple business sectors have resulted in the establishment of dozens of information silos. Information silos invariably result in higher communication costs and worse service quality since appropriate service recommendations are frequently predicated on data analysis of past records that are now dispersed among several locations or silos.[386]

(3) Pricing and incentive concerns: The intricacies around pricing have impeded the progress of services ecosystems. For instance, when it was discovered that self-centered developers were abusing the free APIs to generate revenue, LinkedIn was forced to switch to using premium APIs. Initially, the majority of its APIs were made available without charge. The developers' excitement might be diminished by the premium services, though. Furthermore, new price and incentive mechanisms have been developed as a result of growing application scenarios like crowdsourcing collaboration and M2M service selling.[387]

The emergence of blockchain technologies in recent times presents prospects for surmounting the aforementioned obstacles in services computing. Blockchain was first intended to support virtual currencies like Ethereum and Bitcoin. But thanks to recent developments in cryptography, distributed systems, consensus algorithms, and smart contracts, blockchain has developed into a reliable and decentralized platform that can support a wide range of applications, including IoT, supply chain, finance, healthcare, and energy. Blockchain technology has the ability to address the following issues with services computing.

(1) To improve system security and protect data privacy, the built-in encryption and digital signature systems of blockchain can be integrated with additional security countermeasures like access control and authentication. For instance, access control and data encryption built on top of blockchain technology can significantly lower the likelihood of privacy breaches and data exploitation.[388]

(2) Blockchain decentralization can aid in reducing security risks and weaknesses like DDoS assaults and SPFs. Additionally, smart contract auto-execution can assist in firmware updates to help reduce security flaws. [389]

(3) The pricing and incentive issues in services computing may be resolved by intrinsic incentive schemes. The automatic execution of smart contracts, for instance, allows developers to be compensated with a particular amount of digital currency for contributing codes or reporting defects.[390] As a result, services computing's drawbacks can be solved by integrating blockchain technology with services computing. [391,392,393]

Blockchain data analysis has uses in both commercial and scientific domains. One open-source software platform for blockchain analysis is called BlockSci.[394] BlockSci's support for various blockchains and analytical tasks is flexible. Compared to using general-purpose graph databases, it is orders of magnitude faster since it combines an analytical, in-memory database.[395] The design of blockchain software BlockSci is presented, along with four analyses that highlight its potential and provide insight into the economics, security, and privacy of cryptocurrencies.[396] There are two well-defined and opinionated factions in the bitcoin space: believers and nonbelievers. This is rapidly changing, though. In fact, consumers' demand for access to Bitcoin and other cryptocurrency-related products is growing, according to financial services companies, and the capital markets are also dealing with a wide range of changes related to cryptocurrencies. Other groups are considering whether and how to become involved as the space develops. It can be difficult to define the area or even comprehend the strategic reasoning behind integrating a cryptocurrency into a company given the dynamic nature of the market, the changing legal and regulatory landscape, and the extreme volatility of crypto assets. The aforementioned pertains particularly to directors and executives who might lack adequate knowledge about cryptocurrencies, their constraints, or the underlying technology. Additionally, they may not be familiar with the regulatory, risk, accounting, data security,

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

and tax aspects that come with handling a novel asset class or service provision.[397] Nonetheless blockchain is a young technology that faces a number of difficulties. Let's review and discuss the three common challenges that are listed below.

Reliability

The blockchain gets heavier every day as the volume of transactions rises. The Bitcoin blockchain currently has more storage than 100 GB. To validate a transaction, every transaction must be saved. Furthermore, the Bitcoin blockchain can only handle about 7 transactions per second because of the initial limitations on block size and the time interval required to construct a new block. This means that it is unable to meet the demand for processing millions of transactions in real-time. Since miners prioritize transactions with high transaction fees, many minor transactions may be delayed due to the very small capacity of blocks. Large block sizes, however, will cause blockchain branches and slow down the rate of propagation. Scalability is therefore a difficult problem. Numerous initiatives have been put out to solve the blockchain's scalability issue, and they fall into two categories:

- **Blockchain storage optimization**. Bruce J. developed a unique cryptocurrency system to address the issue of the bulky blockchain.[398] The new scheme involves the network removing outdated transaction records and using an account tree database to store the balance of all non-empty addresses. Nodes can verify a transaction's validity without having to record every transaction in this way. In addition, a lightweight client can assist in resolving this issue. A brand-new scheme called VerSum was put up to offer an additional means of permitting lightweight clients to exist.[399] Lightweight clients can outsource costly computations over big inputs with VerSum. By comparing findings from several servers, it makes sure that the computation result is accurate.
- **Revamping The Blockchain**. The Next Generation of Bitcoin has proposed itself.[400] Bitcoin-NG's primary goal is to split the traditional block into two sections: a microblock for transaction storing and a key block for leader elections. The goal among miners is to become the leader. The leader is in charge of creating microblocks up to the arrival of a new leader. Additionally, Bitcoin-NG continued to use the heaviest (longest) chain technique, in which microblocks are ignored and only important blocks are counted. The trade-off between block size and network security has been addressed, and blockchain is reconstructed in this way.

Privacy Violation

Because users only utilize created addresses—rather than their actual identities—to complete transactions, blockchain is thought to be extremely secure. In the event that information leaks, users can also generate multiple addresses.[401] This reference, however, demonstrates that [402] blockchain cannot ensure transactional privacy because all transaction values and balances for each public key are available to the public. Furthermore, a recent study [16] has demonstrated that information about a user can be obtained by linking their Bitcoin transactions. Furthermore, Biryukov et al.[403] described a way to connect user pseudonyms to IP addresses even in situations where users are protected by firewalls or Network Address Translation (NAT). Each client in this reference has a unique identity based on the nodes it connects to. On the other hand, one can learn to use this collection to determine a transaction's origin. Various techniques have been suggested to enhance the anonymity of blockchain, broadly classified into two categories:

- **Blending.** Users' addresses in blockchain are pseudonymous.[405] Because many users interact with the same address on a regular basis, it is still possible to connect addresses to users' true identities. A type of service called"mixing service" transfers money from several input addresses to numerous output addresses while maintaining anonymity. For instance, user Ross, whose address is A, wishes to give money to Rachel, whose address is B. Ross and Rachel's relationship in figure 10 may become clear if Ross transacts directly with input address A and output address B. Ross can then transfer money to someone else, like Carol, who is a reliable middleman. Carol can then send money to Ross using a variety of inputs, outputs, etc. The output addresses also include Rachel's address B. Thus, it gets more difficult to disclose Ross and Rachel's relationship. But the middleman can be dishonest and purposefully divulge Ross and Rachel's personal information. It's also feasible that Carol moves Ross's money from Rachel's address to her own. Mixcoin offers a straightforward way to stay away from dishonest behavior.[406] The intermediary uses its private key to encrypt the requirements of users, including the amount of payments and the transfer date. Anybody can then confirm that the middleman cheated if they did not transmit the money. Theft is still identified but not stopped, though. To guard against theft, Coinjoin relies on a central mixing server to swap output addresses.[407] CoinShuffle, which was influenced by Coinjoin, use decryption mixnets for address shuffling.[408]

- **Not named.** Zero-knowledge proof is employed in Zerocoin. In order to prevent transaction graph analyses, the origin of a payment is separated from the transaction in order for miners to verify that the currencies belong to a list of valid coins instead of needing to validate a transaction using a digital signature.[409] However it still displays the amount and destination of

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

payments. Zerocash has suggested a solution to this issue. Zerocash leverages Succinct Noninteractive Arguments of Knowledge (zk-SNARKs), which are knowledge-based concise arguments.[410] Both transaction amounts and user-held coin values are kept secret.

Idle Mining

Blockchain is vulnerable to collusive, self-serving miner attacks. Most people believe that nodes possessing more than 51% processing power have the ability to undo transactions on the blockchain. Recent studies, however, demonstrate that nodes with less than 51% power are still hazardous. Specifically, Eyal and Sirer demonstrated how the network is susceptible to attacks even when a negligible amount of hashing power is utilized for deception.[411] Under the selfish mining approach, miners keep their blocks they have mined private and only release the private branch to the public once certain conditions are met. All miners will be able to access the private branch because it is longer than the current public chain. Sincere miners are squandering their resources on a pointless branch prior to the private blockchain publishing, while avaricious miners are mining their own chain unopposed. Thus, self-centered miners typically make more money. The selfish pool will draw in rational miners, and the selfish can swiftly surpass 51% power. Numerous more attacks have been presented to demonstrate the vulnerabilities of blockchain technology, based on selfish mining. Miners can increase their profit in persistent mining by non-trivially combining network-level eclipse assaults with mining attacks.[412] One of the obstinate tactics used by miners to continue mining blocks even when the private chain is abandoned is trail-stubbornness. However, in certain instances, it can yield increases of 13% when compared to a counterpart that does not have obstacles. This reference demonstrates that,[413] in contrast to straightforward selfish mining, there exist selfish mining tactics that generate more profits and are advantageous for smaller miners. However, the benefits are negligible. Moreover, it demonstrates that selfish mining can still be profitable for attackers possessing less than 25% of the processing power. Heilman proposed a unique method for discerning miners to select the branch they should follow in an effort to address the issue of self-centered mining.[414] Sincere miners will choose more new blocks with random beacons and timestamps. It is susceptible to fake timestamps, though. ZeroBlock expands on the basic concept, which states that every block must be generated and approved by the network within a set amount of time.[415] Selfish miners in ZeroBlock are unable to get greater rewards than what is anticipated.

Blockchain's Prospects for the Future and Next Steps

Numerous advantages of blockchain technology include decentralization, persistency, auditability, and anonymity. While many studies concentrate on applying blockchain technology in different contexts, there isn't a thorough analysis of blockchain technology from both a technological and application standpoint.[416,417] Blockchain technology is now a hot topic for research and a viable technical choice for many companies and industrial groups. Blockchain can provide organizations new options and benefits through increased efficiency, lower costs, improved integrity and transparency, better security, and improved traceability because of its distributed, decentralized, and trustless nature. Although the finance and banking industries have benefited most from blockchain technology, other industries are also experimenting with and proposing uses for it.[418] Blockchain technology is becoming more and more popular worldwide, with corporations and nations all over the world adopting it. Currently, blockchain is bringing about a transformation in a number of industries, including IoT, finance, healthcare, supply chain, insurance, and registry. To take advantage of the benefits of blockchain technology, many businesses integrate it with their systems. Blockchain has several issues with security, privacy, scalability, and other areas despite its advantages. Before blockchain technologies are widely adopted, a number of challenges need to be resolved. Scalability and cost considerations while preserving the desired security and decentralization characteristics are a major concern. Other new concerns include user privacy, anonymity, and blockchain governance, which frequently deviates from established procedures used by businesses and governments.[419] Numerous industry white papers and analyses, mostly from reputable consulting firms, have detailed the continuous development efforts in the blockchain and energy domains.[420] Blockchain has demonstrated its potential in both academia and industry. We address potential future paths concerning five domains: large data analytics, smart contracts, blockchain testing to counteract the trend toward centralization, artificial intelligence, and big data.

Currently, approximately 700 cryptocurrencies are covered in this reference, and many blockchain types have been emerging recently.[421] But some developers might exaggerate their blockchain performance in order to draw in investors attracted by the enormous profit. Furthermore, customers need to know which blockchain meets their needs in order to integrate blockchain into their businesses. Thus, in order to test several blockchains, a blockchain testing system must be established. Testing for blockchain can be divided into two stages: testing and standardization. Every criterion needs to be created and approved during the standardization step. As soon as a blockchain is created, it can be verified using established standards to see if it functions as the creators have claimed. In terms of the testing stage, certain criteria must be used when doing blockchain testing. The throughput of the blockchain is important to a user running an online retail store, for instance, thus the investigation must evaluate the capacity of a blockchain block, the average time it takes for a transaction to be sent by a user and then packed into the blockchain, and other related factors. Blockchain systems are intended to be decentralized. Miners are becoming more concentrated within the mining pool, though. As of right

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

moment, the combined hash power of the top 5 mining pools on the Bitcoin network exceeds 51%.[422] Furthermore, pools with more than 25% of the overall processing capacity can earn more money than they should due to selfish mining strategies. The self-centered pool will draw rational miners, and eventually it will be able to hold more than 51% of the total power. Since the blockchain isn't meant to benefit a select few companies, some solutions to this issue ought to be put out.

Big data and blockchain can work nicely together. Here, the combination was loosely divided into two categories: data analytics and data management. In terms of data management, blockchain's distributed and secure nature makes it suitable for storing vital data. Blockchain can also guarantee the authenticity of the data. Blockchain technology, for instance, makes it difficult to steal confidential information about patients and prevents tampering with the data. Blockchain transactions have the potential to be utilized for big data analytics. Trading patterns among users, for instance, might be retrieved. With the analysis, users may forecast the trading tendencies of possible partners. A computerized transaction protocol that carries out a contract's terms is called a smart contract.[423] This idea has been around for a while, and blockchain technology can now make it a reality. A smart contract on a blockchain is a piece of code that miners can run autonomously. These days, there are an increasing number of platforms for developing smart contracts, and smart contracts are capable of ever-more functions. Applications for blockchain include banking services and the Internet of Things.[424] We divide the study on smart contracts into two categories: development and assessment. Development can take the form of creating smart contract platforms or smart contract development itself. The Ethereum blockchain is now hosting a large number of smart contracts.[425] In terms of platform development, a number of platforms, such as Ethereum and Hawk, are developing smart contract development.[426] Code analysis and performance assessment are examples of evaluation. Smart contract bugs have the potential to cause terrible harm. For example, the DAO smart contract has over 60 million dollars stolen from it due to the recursive call flaw. This highlights the criticality of smart contract attack analysis.[427] However, the performance of smart contracts is also a critical component of smart contracts. There will be an increasing number of smart contract-based apps used as blockchain technology advances swiftly. Businesses must assess how well an application performs.

Blockchain technology advancements in recent times are opening up new possibilities for AI applications.[428] A lot of the blockchain's problems can be resolved with AI technologies. For example, the determination of whether the contract condition is satisfied always rests with a disclosure. This oracle is typically a reliable third party. AI techniques could be used to create a smart oracle. It simply trains itself by learning from the outside world and is not governed by any group. That way, disputes in smart contracts won't arise, and smart contracts will be able to get smarter. However, AI is already influencing our daily lives. Smart contracts and blockchain technology can be used to limit the wrongdoings of AI goods. Laws drafted in smart contracts, for example, can aid in limiting the wrongdoings of autonomous vehicles. Blockchain technology is currently one of the most well-liked technological developments worldwide. Due to its immutability and decentralization, blockchain technology is already being used by a large number of companies, services, and industries. According to Statista, expenditures on blockchain technology are expected to approach 19 billion dollars by 2024. Future technological advancements and various businesses will benefit from this technology, which will also alter our surroundings.[429] Numerous innovative applications of Blockchain have been developed, and many more will follow, with the potential to transform the world. Below is a summary of those.

- Blockchain technology makes transaction processing cheaper and faster. Additionally, it enables trusted members to agree on the database's current state.[430]

- Cryptocurrency apps are the most well-known use case or use of blockchain technology. Blockchain is the foundation for several thousand cryptocurrencies worldwide, including Ethereum and Bitcoin. A blockchain is used to exchange and authenticate the thousands of coins.

- Blockchain technology could revolutionize how people make payments for goods and services. It has the potential to alter our commercial and financial practices. Blockchain has the potential to alter the world in a lot of ways.[431]

- Nowadays, a lot of companies have begun to accept payments in bitcoin. Even yet, a lot of customers find bitcoin trading to be difficult.[432] This idea will probably alter as new cryptocurrencies are introduced. More virtual currencies like Bitcoin, Ethereum, and many others might be introduced. In the near future, this would lead to a greater adoption of cryptocurrencies.

- On a blockchain, smart contracts are self-executing scripts or programs. They implement the conditions of a contract between parties. Smart contracts facilitate the simplification of procedures that are dispersed throughout many ERP systems and

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

databases. Smart contracts built on blockchains benefit organizations in a variety of ways. They can assist in carrying out transfer pricing agreements between subsidiaries and determining loan eligibility. Business and service processes can operate more quickly and accurately when smart contracts are used. Additionally, it can lower expenses and eliminate the need for middlemen or third-party mediators.

- Blockchain technology may eventually enable us to pay with cryptocurrencies for our cars. It might also enable tokenized ownership, which would let us to recover some of that payment. We won't have to get in touch with a salesman or credit dealer in the future. In a few minutes, everything would be completed in accordance with our cryptocurrency wallet.

- Businesses can use blockchain technology to address problems related to traceability, partner privacy, and real-time data access. They will be able to keep track of supply chain updates more effectively. Additionally, it can aid in improving the supply chain's visibility and security. Blockchain would also make it possible for companies and customers to see how goods performed in terms of quality control as they traveled from their point of origin to their final destination. Walmart now sets up food tracking systems using blockchain technology. It can set up an automated system to handle payments and invoices for its third-party freight carriers thanks to technology.

- Anyone would be able to swap money more quickly and securely with blockchain. Blockchain has some advantages in the financial and banking sectors.[434] For example, enhanced security, increased openness, reduced expenses, quicker payments, etc. In the near future, it will be used more in numerous service sectors.

- Blockchain technology has the potential to significantly improve and streamline energy transactions between producers and consumers. Utility corporations may lose control of the energy sector if blockchain technology is used. Customers would have more authority over their energy sources as a result. The user would be able to sell any extra energy they produce to their neighbors. Additionally, it would enable the sale of goods to other network users via automated smart contracts. In the near future, such sales and purchases will be made possible via Blockchain technology.

- Blockchain technology can aid in the healthcare system's paper trail removal. It would make it possible to improve the accessibility and accuracy of patient medical histories.[435] The patient's permanent blockchain record will list all of their allergies, diseases, and lifestyle choices. This would improve the ability of medical professionals to identify and manage health issues. Blockchain could be used by healthcare professionals to share data with one another. Blockchain might also aid in a few other areas, such as tracking the hospital supply chain, increasing medicine safety, placing protection against fake medications, lowering health insurance rates, etc. It would also decrease redundancies, speed up diagnostics, and secure patient privacy.[436]

- Blockchain technology can assist you in safeguarding your possessions, including your land, cars, and other property. It produces an unquestionable record of who owns our possessions. We will have to transfer or obtain a title when we purchase or sell assets. The titles can be stored on Blockchain's network. This will provide a clear picture of the ownership and transfer of the asset.[437]

- Voters must visit the polls in order to cast their ballots today. Digital voting with immutability can become a reality with the aid of blockchain technology. It can let voters cast their ballots, authenticate themselves, and log in to a computer or mobile device. Thus, the use of Blockchain technology in voting would make it easier, faster, and more safe in the future.[438]

- IoT stands for the Internet of Physical Objects. Through the internet, these IoT devices gather and share data with other linked systems and devices. Cyberattacks are common on these devices. The data generated by Internet of Things devices can be accessed by hackers. Blockchain can assist in resolving these problems. Blockchain encryption can make altering already-existing data records very impossible. It stores data and adds another layer. This prevents unauthorized users from connecting to the network.[439]

- The idea of wealth is evolving quickly in the post-pandemic world, along with society. Wealth can be defined as money, real estate, and generational financial security in traditional financial circles that rely on fiat currency, however cryptocurrency expands on this idea.[440] In the future, blockchain will be more crucial to overcoming obstacles in the event of a pandemic or other disaster.

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

- While traditional kinds of wealth can also be generated through blockchain-powered cryptocurrency initiatives, the technology also makes new forms of wealth possible, such as privacy, decentralization, and personal safety from governmental and third-party interference. When used properly, blockchain gives riches a new meaning in a society where values have changed due to the recent health crisis. The technology is also poised to become a disruptive force in a variety of businesses.[441]

- The uses for blockchain, a peer-to-peer distributed digital database of time-stamped transactions, are essentially endless. Data indicates that technology has the potential to transform digital property, business structures, lending, security, and consumerism.[442] Furthermore, these are only the very beginnings of its more extensive powers. The fundamental idea behind cryptocurrencies backed by blockchain technology is to use digital finance to shift power away from central banks, using technology as a weapon against governments and banks that have centralized authority.

- A distributed ledger of digital records, known as blockchain, is available to any computer running the same protocol. It finds a solution to the trust establishment issue in a distributed system. Blockchain technology establishes a distributed storage system for timestamped documents, ensuring that no third party may alter the data or timestamp without being detected. In order to do away with the necessity for a central authority or middleman to handle or authenticate transactions, distributed ledgers are decentralized. Because Blockchain is a decentralized database, it can handle any kind of register, whether it be public or private, and implement various applications such as identity and property verification, transaction tracking, and tracking of any digital occurrences. Due to the sensitive data involved and the vital nature of these systems, security is a major concern for both clients and developers.

- Because these could result in implementation flaws and security difficulties, researchers at the Cybersecurity Lab look into general blockchains' limitations and issues, including complexity, network size and speed, human error, inevitable security flows, and lack of standards and regulations. The cybersecurity lab is leading the way in detecting and addressing the most prevalent security problems in Blockchain-based applications, including consensus, scalability, privacy leaks, and transaction speed, to mention a few. Additionally, we are looking for new blockchain application situations and building secure and effective solutions to these issues.[443]

- Naturally, blockchain marketplaces are more secure than regular ones. Because of the nature of the public ledger, all data on the blockchain is completely encrypted and secure, making it impossible for a single person to alter the data. This makes the technology perfect for use by entrepreneurs. Gamers and cryptocurrency go hand in hand, as seen by the several times greater quantities of users trading cryptocurrencies than non-gamers. Cryptocurrency and gaming go hand in hand, and blockchain businesses like Gameflip have introduced their own coins to further cement this relationship. The FLIP token from Gameflips was designed specifically to scale peer-to-peer video game goods trade, purchasing, and selling.

- With privacy and security as its top priorities, eCash was created by Bitcoin's "fallen angel" and one of the ecosystem's biggest innovators, AmaurySechet. Sechet left the world's most well-known cryptocurrency to create Bitcoin ABC, hoping to make the coin far more useful than its predecessor.[444] eCash, which was developed utilizing the ground-breaking Avalanche blockchain, is based on a consensus algorithm that permits immediate transactions, upgrades without forks, and improved security. eCash'sblockchain leverages the public's mistrust of centralized authorities and privacy concerns by introducing a decentralized governance protocol that is both technically sound and politically sound. This approach protects the privacy of its users while utilizing an adaptive blockchain.[445]

- Due to the burden of an antiquated and unstable financial environment, people have developed to value privacy and authenticity. Blockchain is a leading alternative to bring about the necessary changes in accordance with social awareness. Blockchain technology is probably going to play a major role in how we address these new societal issues and redefine what it means to be wealthy in the brave new world of digital finance as we transition from the epidemic period to the "new normal."

- Blockchain technology's ability to foster trust, security, and transparency can have a profound impact on tax compliance and collection. Enabling various parties to confirm each stage of the procedure. Blockchain technology has the potential to drastically increase tax collecting efficiency while cutting expenses.[446] Blockchain technology might be used by governments in every nation to create intelligent taxation schemes for residents and businesses.[447]

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

- Applications for blockchain-based patient care include social networks and data preservation platforms, medical research systems, mobile health and telemedicine, health information exchanges and remote monitoring systems, and medical information systems. These blockchain-based health applications will increase access to information for healthcare providers, empower patients, and improve the use of patient data for future medical research. Blockchain technology has the potential to significantly improve health information technology (HIT) by guaranteeing patient privacy and security, promoting interoperability across disparate HIT systems, and raising the standard of care. Health information technology (HIT) developers will face obstacles when utilizing blockchain technology, such as security and privacy flaws, user aversion, expensive implementation and processing power requirements, ineffective consensus algorithms, and difficulties integrating blockchain with current HIT.[448]

- In under ten years, blockchain has gained widespread recognition, mostly through its association with Bitcoin, the world's inaugural decentralized cryptocurrency. Conventional money transfers across borders are frequently costly, time-consuming, and difficult. By eliminating middlemen like banks, blockchain technology can be utilized to expedite a variety of financial transactions at a lower cost and faster pace. With blockchain, money may be moved directly and securely for incredibly minimal fees when compared to traditional banking systems. Coins based on blockchain technology are also extremely difficult—some might even say impossible—to counterfeit.[449]

- Blockchain technology can be used to bring transparency to all business and governance processes to a whole new level. Since every data block is connected to the blockchain by default, any tampering of one block would simultaneously affect all other blocks and notify all relevant parties. For instance, utilizing blockchain technology to record property rights would guarantee that owners can rely on the legitimacy and durability of their title documents. We can think of this technology as a universally secured public record fortress that is practically impenetrable by hackers.[450]

Customers can make peer-to-peer (P2P) payments with cryptocurrencies more quickly and affordably than with traditional money services companies, and they don't require personal information. Although some people still accept cryptocurrencies as a form of payment, price volatility and the possibility of making speculative bets drive people to trade cryptocurrencies rather than use them to pay for products and services. Because of their almost instantaneous settlement, cryptocurrencies provide businesses and merchants with low transaction fees, reduced volatility risk, and the elimination of chargebacks—a credit card provider's demand that a retailer make good on the loss of a fraudulent or disputed transaction. But in addition to upending the established payment system, the blockchain public ledger technology—which powers cryptocurrencies—has the ability to affect a vast range of transactions. These consist of stocks, bonds, and other financial assets for which digital records are kept and for which transaction verification is still now required from a reliable third party. Actually, the major players in the bitcoin market will determine how quickly it develops. These players will probably expand their legitimacy in bursts during what are known as "credentializing moments." In order for the market to advance to the next stage of its development toward widespread acceptance and steady growth, all five of the major players in the market—tech developers, investors, financial institutions, and regulators—will be essential going forward.[451]

Blockchains are utilized in many contexts than just cryptocurrency systems, where they are essential for maintaining a safe, decentralized record of transactions. Blockchains can be used in any industry to make data immutable—that is, incapable of being altered.[452] According to PwC's Time for Trust analysis, by 2030, blockchain jobs would rank second in terms of employment benefits globally, behind almost 40 million jobs. It's possible that even people who don't know much about blockchain technology have heard of it, usually in connection with cryptocurrencies like Bitcoin. However, blockchains are used for more than just virtual currency.[453] These are stand-alone technologies with diverse uses. Blockchain technology has already been effectively applied in the healthcare sector and is being used in the automobile business to record vehicle histories in order to prevent seller fraud. No one will be able to falsify information about the mileage or upkeep of the car if all of this data is safely kept on the blockchain. Indeed, looking at it from today's perspective, blockchain has a ton of promise, and in the future, blockchain engineers will be in high demand by almost every industry. The younger generation can become successful professionals in the future by learning about blockchain technology and its applications in modern technology. On the other hand, data is digitally structured and assembled into clusters or blocks using blockchains. There is a limited amount of storage for each block. Once that threshold is met, the block closes and links to the previous one using cryptography to create a chain. Cryptography creates an unchangeable timestamp when one block is linked to another. This continuous record validates the accuracy of sensitive data, including transactions.[454]

In summary

Blockchain facilitates the creation of a P2P decentralized database. This implies that the database won't be under the control of a single entity. A public record of who owns what and who transacts what with whom is essentially what blockchain is. It offers a

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

productive method of collaborating with multiple partners without requiring mutual confidence. Blockchain technology, also known as Distributed Ledger Technology (DLT), allows financial organizations to control governance surrounding data sharing. Furthermore, blockchain's decentralized ledgers cannot be altered. This implies that records cannot be later altered or amended. Every transaction is kept on the network as historical data. It can handle a ledger of records that is appended only and will be subsequently added to the chain. As a result, sharing information between many parties is made simpler and safer when client information and transaction records are kept on a decentralized network. The emergence of Blockchain technologies has set off a revolution that is currently going strong and altering many facets of our society. Not only is this technology the foundation of well-known cryptocurrencies like Bitcoin, but it also has great promise for use in a wide range of other contexts and facets of contemporary life. It also sparked the development of novel techniques like smart contracts, a very promising technology that has the potential to greatly expand the use of blockchain technology.

From a technological and application standpoint, blockchain technology will be valuable and functional. The underlying technology of several digital cryptocurrencies is called blockchain. Blockchain is a distributed, decentralized network of blocks used to store data with digital signatures. Blockchain technology has applications beyond bitcoin, including risk management, healthcare facilities, financial and social services, and more. Numerous studies concentrate on the potential that blockchain offers across a range of application fields. Blockchain technology has countless applications. It has the enormous potential to significantly alter international business practices. Blockchain contributes to cost savings, increased productivity, and transparency. It offers answers to the problems that many sectors encounter. By increasing enterprises' productivity and profitability, it is enhancing international trade. Blockchain technology is developing quickly, and the years ahead appear to be promising. Blockchain technology can be viewed as a sort of next-generation software for business process improvement from a business standpoint. Blockchain and other collaborative technologies promise to drastically reduce the "cost of trust" in business transactions between companies, which makes them potentially much more profitable per unit of investment than most conventional internal investments. Financial institutions and service providers are investigating how blockchain technology could revolutionize a range of industries, including insurance and clearing and settlement. First, let's review money is no object as an introduction to cryptocurrencies. However, there are certain drawbacks, such scalability and data privacy. As a result, for blockchain to be fully adopted by different industries, the market as a whole must comprehend how it will work against the existing infrastructure.

Blockchain is highly regarded and supported due to its peer-to-peer architecture and decentralized structure. Nevertheless, Bitcoin obscures a lot of blockchain research. Blockchain, however, has far wider applications than just Bitcoin. With its primary features—decentralization, persistency, anonymity, transparency, safety, smart contracts, auditability, and increased transaction security and tamper proof—blockchain has demonstrated its potential to revolutionize traditional industries. The blockchain has complete organization and is very fault-tolerant because it doesn't rely on human computations. Therefore, unintentional system failures are rarely a typical result. Blockchain guarantees transfers while granting users authority over their properties. They can take care of their assets without depending on someone else. They can all do it at the same time on their own. There is no possibility for someone to con us out of anything because the system is based on algorithms. Blockchain prevents anyone from using it for their own benefit. Each participant's profile is made accessible. The blockchain makes all changes visible and more tangible. Blockchain technology is so safe and secure that it creates a system that is suitable for all types of users. And it will be difficult for hackers to break through. However, because smart contract languages still have a lot of flaws and limitations, it is now difficult to implement many creative applications. This calls for further research on smart contracts and other issue solving techniques in the future. As the market develops with more technical innovation, research and analysis are required to determine how players in the market—such as investors, technology suppliers, engineers, academic institutions, and financial institutions—will be impacted. While blockchain technology isn't a panacea for every issue pertaining to businesses and services, it is an excellent fit for a lot of them.

About Author

Hossain KA, PhD is the former Head of Dept NAME, MIST; and professor/researcher/Examiner of BUET, Dhaka, Bangladesh. Email: kahossain756@gmail.com

References

[1]Oberhaus Daniel, (27 August 2018), "The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995", www.vice.com, accessed on 21 Sep 2023

[2] https://www.geeksforgeeks.org/history-of-blockchain/,accessed on 21 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[3] Anthony Cuthbertson, (July 21, 2014), "Bitcoin Breakthrough as Chamber of Digital Commerce Opens in US", International Business Times UK,accessed on 21 Sep 2023

[4] Song Shaoxu, et al, (May 2021), "Cleaning timestamps with temporal constraints", The VLDB Journal, 30 (3): 425–446, doi:10.1007/s00778-020-00641-6, ISSN 1066-8888,accessed on 21 Sep 2023

[5] Block 0 – Bitcoin Block Explorer", Archived from the original on 15 October 2013,accessed on 21 Sep 2023

[6] Pagliery Jose, (2014), Bitcoin: And the Future of Money. Triumph Books, ISBN 9781629370361, Archived from the original on 21 January 2018, accessed on 21 Sep 2023

[7] https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A52186,accessed on 21 Sep 2023

[8] Bosker Bianca, (16 April 2013), "Gavin Andresen, Bitcoin Architect: Meet The Man Bringing You Bitcoin (And Getting Paid In It)", HuffPostTech, Archived from the original on 3 August 2016,accessed on 21 Sep 2023

[9] Badea Liana, et al, (2021), "The Economic and Environmental Impact of Bitcoin", IEEE Access, 9: 48091–48104, doi:10.1109/ACCESS.2021.3068636, ISSN 2169-3536,accessed on 21 Sep 2023

[10] Huang Jon,et al, (3 September 2021), "Bitcoin Uses More Electricity Than Many Countries, How Is That Possible?", The New York Times, ISSN 0362-4331,accessed on 21 Sep 2023

[11] Messina, Irene (31 August 2023). "Bitcoin electricity consumption: an improved assessment - News &insight". Cambridge Judge Business School,accessed on 21 Sep 2023

[12] https://www.javatpoint.com/history-of-blockchain,accessed on 21 Sep 2023

[13] Oberhaus, Daniel (27 August 2018). "The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995". www.vice.com, accessed on 19 Sep 2023

[14] https://www.geeksforgeeks.org/history-of-blockchain/, accessed on 19 Sep 2023

[15] https://www.mdpi.com/1999-5903/13/2/48,accessed on 22 Sep 2023

[16] https://www.sciencedirect.com/science/article/abs/pii/S0167739X17315765,accessed on 21 Sep 2023

[17] https://www.sciencedirect.com/science/article/abs/pii/S1084804521000758,accessed on 22 Sep 2023

[18] https://www.nasdaq.com/solutions/nasdaq-100?channel=Advertising&source=Marketing,

[19] https://www.sciencedirect.com/science/article/abs/pii/S0268401219306024,accessed on 22 Sep 2023

[20] Bambysheva Nina, "Satoshi & Company: The 10 Most Important Scientific White Papers In Development Of Cryptocurrencies". Forbes, accessed on 22 Sep 2023

[21] Sherman, Alan T.,et al, (January 2019), "On the Origins and Variations of Blockchain Technologies", IEEE Security Privacy, 17 (1): 72–77, arXiv:1810.06130, doi:10.1109/MSEC.2019.2893730. ISSN 1558-4046, accessed on 22 Sep 2023

[22] Haber Stuart, et al, (1991-01-01), "How to time-stamp a digital document", Journal of Cryptology, 3 (2): 99–111, doi: 10.1007/BF00196791. ISSN 1432-1378, accessed on 22 Sep 2023

[23] "The World's Oldest Blockchain Has Been Hiding in the New York Times Since 1995". www.vice.com, 27 August 2018, accessed on 22 Sep 2023

[24] Claudia Maria Bauzer Medeiros (19 September 2009), ADVANCED GEOGRAPHIC INFORMATION SYSTEMS -Volume I.EOLSSPublications.p. 59. ISBN 978-1-905839-91-9, accessed on 22 Sep 2023

[25]Nijenhuis Albert et al, (1978), Combinatorial Algorithms, Computer Science and Applied Mathematics (2nd ed.), New York-London: Academic Press, ISBN 0125192606, accessed on 22 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[26] Bayer, Dave; Haber, Stuart; Stornetta, W. Scott (March 1992). "Improving the Efficiency and Reliability of Digital Time-Stamping". Sequences II. pp. 329–334, CiteSeerX 10.1.1.71.4891, doi: 10.1007/978-1-4613-9323-8_24. ISBN 978-1-4613-9325-2, accessed on 22 Sep 2023

[27] "The New York Times", Encyclopædia Britannica, Archived from the original on April 26, 2015, accessed on 22 Sep 2023

[28] Kharif, Olga (23 April 2019). "John McAfee Vows to Unmask Crypto's Satoshi Nakamoto, Then Backs Off". Bloomberg, accessed on 22 Sep 2023

[29] http://www.hashcash.org/papers/hashcash.pdf, accessed on 22 Sep 2023

[30] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton, New Jersey: Princeton University Press. ISBN 978-0-691-17169-2, accessed on 22 Sep 2023

[31] "Blockchains: The great chain of being sure about things", The Economist. 31 October 2015. Archived from the original on 3 July 2016.Retrieved 18 June 2016, The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency, accessed on 22 Sep 2023

[32] Nian, Lam Pak, et al, (2015),"A Light Touch of Regulation for Virtual Currencies", In Chuen, David LEE Kuo (ed.), Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. Academic Press, p. 319. ISBN 978-0-12-802351-8, accessed on 22 Sep 2023

[33] https://www.blockchain.com/explorer/charts/blocks-size?scale=1&timespan=all&showDataPoints=true,

[34] Johnsen, Maria (12 May 2020). Blockchain in Digital Marketing: A New Paradigm of Trust. Maria Johnsen, ISBN 979-8-6448-7308-1, accessed on 24 Sep 2023

[35] Stone, Diane, (January 2000), "Non-governmental policy transfer: the strategies of independent policy institutes", Governance. 13 (1): 45–70. doi:10.1111/0952-1895.00123, accessed on 24 Sep 2023

[36] "The future of blockchain in 8 charts", Raconteur, 27 June 2016, Archived from the original on 2 December 2016, accessed on 24 Sep 2023

[37] Staff, (October 16, 2014), "Chamber of Digital Commerce Receives IRS Recognition", Politics & Government Week, Archived from the original on December 2, 2019, accessed on 24 Sep 2023

[38] "Gartner, Inc., 2022 Annual Report (Form 10-K), U.S. Securities and Exchange Commission, 16 February 2023, accessed on 24 Sep 2023

[39] Silverstein, Jake (February 18, 2015). "Behind the Relaunch of the New York Times Magazine", The New York Times, ISSN 0362-4331. Archived from the original on May 3, 2021, accessed on 24 Sep 2023

[40] "The New York Times Company – Redesigned T Magazine Franchise to Launch in 2013", investors.nytco.com, Archived from the original on February 2, 2017, accessed on 24 Sep 2023

[41] Wallace Benjamin, (23 November 2011), "The Rise and Fall of Bitcoin". Wired.Vol. 19, no. 12, ISSN 1059-1028,

[42] https://www.whois.com/whois/bitcoin.org, accessed on 24 Sep 2023

43 Antonopoulos Andreas, M. (2014), Mastering Bitcoin: Unlocking Digital Crypto-Currencies, O'Reilly Media. ISBN 978-1-4493-7404-4, accessed on 24 Sep 2023

[44] Economist Staff, (31 October 2015), "Blockchains: The great chain of being sure about things". The Economist, Archived from the original on 3 July 2016, accessed on 24 Sep 2023

[45] https://bitcoincharts.com/charts/mtgoxUSD#rg60zczsg2013-03-12zeg2013-03-15ztgSzm1g10zm2g25zv, accessed on 24 Sep 2023

[46] https://www.blockexplorer.com/l/en-US/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f, accessed on 24 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[47] https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h, accessed on 24 Sep 2023

[48] https://books.google.com.bd/books?id=_-wuBAAAQBAJ&redir_esc=y, accessed on 24 Sep 2023

[49] https://www.huffpost.com/entry/gavin-andresen-bitcoin_n_3093316, accessed on 24 Sep 2023

[50] Rodriguez, Salvador (6 March 2014), "Dorian Satoshi Nakamoto chased by reporters, denies founding Bitcoin", Los Angeles Times. Archived from the original on 6 March 2014,

[51] Leah McGrath Goodman (6 March 2014). "The Face BehindBitcoin", Newsweek, Archived from the original on 8 March 2014, accessed on 25 Sep 2023

[52] "Bitcoin creator is now the 15th richest person in the world", The Independent, 15 November 2021. Retrieved 1 December 2021, accessed on 25 Sep 2023

[53] Benchoff Brian, (2018-04-23), "What Does 'Crypto' Actually Mean?", Hackaday, Archived from the original on 2018-04-26, accessed on 25 Sep 2023

[54] Milutinović, Monia (2018), "Cryptocurrency". Ekonomika, 64 (1): 105–122. doi:10.5937/ekonomika1801105M. ISSN 0350-137X. Archived from the original on 16 April 2022, accessed on 25 Sep 2023

[55] Yaffe-Bellany, David (15 September 2022). "Crypto's Long-Awaited 'Merge' Reaches the Finish Line", The New York Times. Archived from the original on 16 September 2022, accessed on 25 Sep 2023

[56] Andy Greenberg, (20 April 2011), "Crypto Currency", Forbes, Archived from the original on 31 August 2014, accessed on 25 Sep 2023

[57]PolansekTom, (2 May 2016), "CME, ICE prepare pricing data that could boost bitcoin". Reuters. Archived from the original on 23 April 2022, accessed on 25 Sep 2023

[58] "Bitcoin not a currency says Japan government", BBC News. 7 March 2014, Archived from the original on 25 January 2022, accessed on 25 Sep 2023

[59] https://www.reuters.com/article/us-crypto-currencies-idUSKBN20Q0LK, accessed on 25 Sep 2023

[60] Brown, Aaron (7 November 2017), "Are Cryptocurrencies an Asset Class? Yes and No", www.bloomberg.com, Archived from the original on 1 April 2022, accessed on 25 Sep 2023

[61] Allison, Ian (8 September 2015). "If Banks Want Benefits of Blockchains, They Must Go Permissionless", International Business Times, Archived from the original on 12 September 2015, accessed on 25 Sep 2023

[62]MatteoD'Agnolo, "All you need to know about Bitcoin", timesofindia-economictimes, Archived from the original on 26 October 2015, accessed on 24 Sep 2023

[63] "Substantiation – Money laundering in digital currencies (Unclassified)", Money Laundering in Digital Currencies, National Drug Intelligence Center, US Department of Justice, June 2008. Archived from the original on 14 April 2022, accessed on 25 Sep 2023

[64] Byrnes William H., et al, (2 October 2013), Money Laundering, Asset Forfeiture and Recovery and Compliance – A Global Guide, LexisNexis, p. 2802, ISBN 978-0-327-17084-6, accessed on 25 Sep 2023

[65]SoodAditya K, et al, (2013), "Cybercrime: Dissecting the State of Underground Enterprise", IEEE Internet Computing.IEEE Computer Society, 17 (1): 60–68. doi:10.1109/MIC.2012.61

[66]https://finance.yahoo.com/news/send-bitcoin-hardware-wallet-140141385.html?, accessed on 25 Sep 2023

[67] Divine, John (1 February 2019). "What's the Best Bitcoin Wallet?", U.S. News & World Report, accessed on 25 Sep 2023

[68] Newman, Lily Hay (2017-11-05), "How to Keep Your Bitcoin Safe and Secure", Wired, ISSN 1059-1028, accessed on 25 Sep 2023

[69]Baloian Artiom, (2021-12-18), "How to Generate Public and Private Keys for the Blockchain", Medium, accessed on 25 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[70] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF), accessed on 25 Sep 2023

[71] "What are blockchain and cryptocurrency?",Blockchain and Cryptocurrency: International Legal and Regulatory Challenges, Bloomsbury Professional, 2022, accessed on 25 Sep 2023

[72] https://cyber.bgu.ac.il/advanced-cyber/airgap, accessed on 25 Sep 2023

[73] Law, Laurie; Sabett, Susan; Solinas, Jerry (11 January 1997). "How to Make a Mint: The Cryptography of Anonymous Electronic Cash", The American University Law Review, 46 (4), Archived from the original on 12 January 2018, accessed on 25 Sep 2023

[74] "Cryptocurrencies: What Are They?", Schwab Brokerage, Archived from the original on 14 September 2023, accessed on 25 Sep 2023

[75] Al-Laham, et al, (2009), "Development of Electronic Money and Its Impact on the Central Bank Role and Monetary Policy" (PDF), Issues in Informing Science and Information Technology, 6: 339–349. doi:10.28945/1063, accessed on 25 Sep 2023

[76] Mick, Jason (12 June 2011). "Cracking the Bitcoin: Digging Into a $131M USD Virtual Currency". Daily Tech. Archived from the original on 20 January 2013, accessed on 25 Sep 2023

[77] https://www.bankofengland.co.uk/explainers/how-is-money-created, accessed on 25 Sep 2023

[78] https://www.economist.com/the-economist-explains/2015/11/02/who-is-satoshi-nakamoto, accessed on 25 Sep 2023

[79] Davis Joshua, (10 October 2011), "The Crypto-Currency: Bitcoin and its mysterious inventor", The New Yorker, Archived from the original on 1 November 2014, accessed on 25 Sep 2023

[80] https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/, accessed on 25 Sep 2023

[81] Vigna Paul, et al, (2015), The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order (1 ed.), New York: St. Martin's Press. ISBN 978-1-250-06563-6, accessed on 25 Sep 2023

[82] "Oxford Dictionaries API", Oxford University Press, Archived from the original on 22 October 2013, accessed on 25 Sep 2023

[83] https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf, accessed on 25 Sep 2023

[84] https://www.bostonglobe.com/2022/07/08/opinion/nayib-bukeles-failed-bitcoin-experiment-el-salvador/, accessed on 25 Sep 2023

[85] Wolff-Mann, Ethan (27 April 2018). "'Only good for drug dealers': More Nobel prize winners snub bitcoin", Yahoo Finance, Archived from the original on 12 June 2018, accessed on 25 Sep 2023

[86] Jones, Benjamin A.; Goodkind, Andrew L.; Berrens, Robert P. (29 September 2022). "Economic estimation of Bitcoin mining's climate damages demonstrates closer resemblance to digital crude than digital gold", Scientific Reports. 12 (12): 14512, accessed on 25 Sep 2023

[87] Huang, Jon; O'Neill, Claire; Tabuchi, Hiroko (3 September 2021), "Bitcoin Uses More Electricity Than Many Countries, How Is That Possible?", The New York Times, ISSN 0362-4331, accessed on 25 Sep 2023

[88] https://www.newscientist.com/article/2339629-bitcoin-has-emitted-200-million-tonnes-of-co2-since-its-launch/,

[89] https://www.iea.org/reports/global-energy-review-2021/co2-emissions,

[90] https://www.weetechsolution.com/blog/cryptocurrency-a-big-revolution, accessed on 26 Sep 2023

[91] https://economictimes.indiatimes.com/markets/cryptocurrency/top-crypto-prices-today-bitcoin-regains-usd-20000-levels-ethereum-still-below-usd-1500/articleshow/94280726.cms?from=mdr, accessed on 26 Sep 2023

[92] Antonopoulos, Andreas M, (2014), Mastering Bitcoin: Unlocking Digital Crypto-Currencies.O'Reilly Media. ISBN 978-1-4493-7404-4, accessed on 26 Sep 2023

[93] https://www.unicode.org/versions/Unicode10.0.0/, accessed on 26 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[94] Katie Pisa, et al, (9 July 2014), "Bitcoin your way to a double espresso", cnn.com, CNN, Archived from the original on 18 June 2015, accessed on 26 Sep 2023

[95] https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things, accessed on 26 Sep 2023

[96] Lucks Stefan, (2004), "Design Principles for Iterated Hash Functions", Cryptology ePrint Archive, Report 2004/253, accessed on 26 Sep 2023

[97] Rainer Böhme, et al, (2015), "Bitcoin: Economics, Technology, and Governance", Journal of Economic Perspectives, 29 (2): 213–238, accessed on 26 Sep 2023

[98] Sparkes, Matthew (9 June 2014), "The coming digital anarchy", The Daily Telegraph, London, Archived from the original on 23 January 2015, accessed on 26 Sep 2023

[99] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174, accessed on 26 Sep 2023

[100] https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/,

[101] https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8301.pdf,

[102] https://www.statista.com/statistics/863917/number-crypto-coins-tokens/, accessed on 26 Sep 2023

[103] Joshua A., et al, (11–12 June 2013), "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries" (PDF), The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Archived (PDF) from the original on 9 May 2016, accessed on 26 Sep 2023

[104] Economist Staff, (31 October 2015), "Blockchains: The great chain of being sure about things", The Economist. Archived from the original on 3 July 2016, accessed on 26 Sep 2023

[105] Satoshi Nakamoto, (17 November 2008), "Re: Bitcoin P2P e-cash paper 2008-11-17 16:33:04 UTC", Satoshi Nakamoto Institute, Archived from the original on 7 December 2016, accessed on 26 Sep 2023

[106] https://www.technologyreview.com/2015/05/19/168128/leaderless-bitcoin-struggles-to-make-its-most-crucial-decision/, accessed on 26 Sep 2023

[107] https://www.youtube.com/watch?v=sE7998qfjgk, accessed on 26 Sep 2023

[108] Nakamoto Satoshi, (24 May 2009), "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF), Archived (PDF) from the original on 20 March 2014, accessed on 26 Sep 2023

[109] Wallace Benjamin, (23 November 2011, "The Rise and Fall of Bitcoin", Wired. Archived from the original on 31 October 2013, accessed on 26 Sep 2023

[110] https://en.wikipedia.org/wiki/Elliptic-curve_cryptography, accessed on 26 Sep 2023

[111] R. Shirey (August 2007). Internet Security Glossary, Version 2. Network Working Group. doi:10.17487/RFC494, accessed on 26 Sep 2023

[112] "Man Throws Away 7,500 Bitcoins, Now Worth $7.5 Million", CBS DC, 29 November 2013. Archived from the original on 15 January 2014, accessed on 26 Sep 2023

[113] Krause, Elliott (5 July 2018). "A Fifth of All Bitcoin Is Missing. These Crypto Hunters Can Help". The Wall Street Journal, Archived from the original on 9 July 2018, accessed on 26 Sep 2023

[114]effries Adrianne, (19 December 2013), "How to steal Bitcoin in three easy steps", The Verge, Archived from the original on 27 July 2019, accessed on 26 Sep 2023

[115] Harney Alexandra, et al, (16 November 2017), "Twice burned – How Mt. Gox'sbitcoin customers could lose again". Reuters. Archived from the original on 29 August 2019, accessed on 26 Sep 2023

[116] https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html, accessed on 26 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[117] Wescott, Bob (2013), The Every Computer Performance Book, CreateSpace, ISBN 978-1482657753, accessed on 26 Sep 2023

[118]Aumasson, Jean-Philippe (6 November 2017). Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press. ISBN 978-1-59327-826-7, accessed on 26 Sep 2023

[119] https://ieeexplore.ieee.org/document/9170774, accessed on 26 Sep 2023

[120]Rogaway P., et al, (2004), "Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance", In Roy, B.; Mier, W. (eds.). Fast Software Encryption: 11th International Workshop, FSE 2004, Vol. 3017, Lecture Notes in Computer Science: Springer. pp. 371–388, ISBN 3-540-22171-9, accessed on 27 Sep 2023

[121] Lafore, Robert W. (1987), Microsoft C: programming for the IBM, H.W. Sams, p. 294, ISBN 9780672225154,

[122] https://www.intel.com/content/www/us/en/developer/technical-library/overview.html, accessed on 27 Sep 2023

[123] Wallace Benjamin, (23 November 2011), "The Rise and Fall of Bitcoin", Wired, Archived from the original on 31 October 2013, accessed on 27 Sep 2023

[124] "Difficulty History" (The ratio of all hashes over valid hashes is D x 4,295,032,833, where D is the published "Difficulty" figure.). Blockchain.info. Archived from the original on 8 April 2015, accessed on 27 Sep 2023

[125] "Bitcoin boom benefiting TSMC: report", Taipei Times, 4 January 2014, accessed on 27 Sep 2023

[126] Hampton, Nikolai (5 September 2016). "Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin". Computerworld.IDG. Archived from the original on 6 September 2016, accessed on 27 Sep 2023

[127] Nakamoto, Satoshi (24 May 2009). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF), Archived (PDF) from the original on 20 March 2014, accessed on 27 Sep 2023

[128]EyalIttay, (2017), "The Miner's Dilemma" (PDF), Cornell University, Archived (PDF) from the original on 2017-08-09, accessed on 27 Sep 2023

[129] Biggs John, (8 April 2013), "How To Mine Bitcoins". Techcrunch, Archived from the original on 6 July 2017,

[130] Woods Nick, (2021), Bitcoin for Beginners: An Introduction to Bitcoin, Blockchain and Cryptocurrency, Publishing Forte, Chapter 4, Section 2, ISBN 9781954937000, accessed on 27 Sep 2023

[131] Ashlee Vance, (14 November 2013), "2014 Outlook: Bitcoin Mining Chips, a High-Tech Arms Race", BusinessWeek, Archived from the original on 21 November 2013, accessed on 27 Sep 2023

[132] Browne Ryan, (11 May 2020), "Bitcoin investors are bracing for a key technical event — here's what you need to know". CNBC, accessed on 27 Sep 2023

[133] Nakamoto Satoshi, (31 October 2008), "Bitcoin P2P e-cash paper", Archived from the original on 28 December 2012, accessed on 27 Sep 2023

[134] https://bitcoin.org/bitcoin.pdf, accessed on 27 Sep 2023

[135] Ritchie S. King, et al, (17 December 2013), "By reading this article, you're mining bitcoins", qz.com, Atlantic Media Co., Archived from the original on 17 December 2013, accessed on 27 Sep 2023

[136] https://www.fincen.gov/sites/default/files/2016-08/20131118.pdf, accessed on 27 Sep 2023

[137] https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency, accessed on 27 Sep 2023

[138] Meola Andrew, (5 October 2017), "How distributed ledger technology will change the way the world works", Business Insider. Archived from the original on 27 April 2018, accessed on 27 Sep 2023

[139] https://web.archive.org/web/20131121225123/http://www.businessweek.com/articles/2013-11-14/2014-outlook-bitcoin-mining-chips-a-high-tech-arms-race, accessed on 27 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[140]Penenberg Adam, (2013), "The Bitcoin Crypto-Currency Mystery Reopened", Fast Company. Archived from the original on 6 October 2013, accessed on 27 Sep 2023

[141] https://ijeecs.iaescore.com/index.php/IJEECS/article/view/15610, accessed on 27 Sep 2023

[142] https://www.wsj.com/market-data/quotes/fx/BTCUSD/historical-prices, accessed on 27 Sep 2023

[143] https://www.cftc.gov/dea/futures/financial_lf.htm, accessed on 27 Sep 2023

[144] https://www.nasdaq.com/articles/bitcoin-prices-remain-below-600-amid-bearish-chart-signals-2014-08-05, accessed on 27 Sep 2023

[145] Zaki, Myret (14 January 2021). "Bitcoin: The Derivative Bomb", The Market (in German), Archived from the original on 15 January 2021, accessed on 27 Sep 2023

[146] Gervais Arthur, et al, (2016), "Is Bitcoin a Decentralized Currency?",InfoQ.InfoQ& IEEE Computer Society, Archived from the original on 10 October 2016, accessed on 29 Sep 2023

[147] Wilhelm Alex, (2017), "Popular Bitcoin Mining Pool Promises To Restrict Its Compute Power To Prevent Feared '51%' Fiasco", TechCrunch. Archived from the original on 5 December 2017, accessed on 28 Sep 2023

[148] Chan Edwin, (9 April 2019), "China Plans to Ban Cryptocurrency Mining in Renewed Clampdown", Bloomberg.com, Archived from the original on 18 December 2019, accessed on 28 Sep 2023

[149] Ben Rooney, (29 November 2013), "Bitcoin worth almost as much as gold", CNN, Archived from the original on 26 October 2014, accessed on 28 Sep 2023

[150] https://web.archive.org/web/20200810062846/https://www.lexico.com/definition/pseudonym, accessed on 28 Sep 2023

[151]Simonite Tom, (5 September 2013), "Mapping the Bitcoin Economy Could Reveal Users' Identities", MIT Technology Review, accessed on 27 Sep 2023

[152] Lee Timothy, (21 August 2013), "Five surprising facts about Bitcoin", The Washington Post, Archived from the original on 12 October 2013, accessed on 27 Sep 2023

[153] McMillan Robert, (6 June 2013), "How Bitcoin lets you spy on careless companies", Wired UK. Conde Nast. Archived from the original on 9 February 2014, accessed on 27 Sep 2023

[154] https://river.com/learn/terms/t/taint/, accessed on 27 Sep 2023

[155]MöserMalte, et al, (2013), An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem (PDF), 2013 APWG eCrime Researchers Summit, IEEE, ISBN 978-1-4799-1158-5. Archived (PDF) from the original on 26 June 2018, accessed on 27 Sep 2023

[156] Adam Serwer, et al, (10 April 2013), "Bitcoin, Explained". motherjones.com. Mother Jones, Archived from the original on 27 April 2014, accessed on 27 Sep 2023

[157] https://www.economist.com/technology-quarterly/2013/11/28/bitcoin-under-pressure, accessed on 27 Sep 2023

[158]SkudnovRostislav, (2012), Bitcoin Clients (PDF) (Bachelor's Thesis), Turku University of Applied Sciences, Archived (PDF) from the original on 18 January 2014, accessed on 29 Sep 2023

[159] https://bitcoin.org/en/release/v0.9.0, accessed on 28 Sep 2023

[160] Metz, Cade (19 August 2015). "The Bitcoin Schism Shows the Genius of Open Source", Wired, Condé Nast. Archived from the original on 30 June 2016, accessed on 28 Sep 2023

[161] Vigna, Paul (17 January 2016). "Is Bitcoin Breaking Up?", The Wall Street Journal, Archived from the original on 20 August 2016, accessed on 28 Sep 2023

[162] Allison, Ian (28 April 2017). "Ethereum co-founder Dr Gavin Wood and company release Parity Bitcoin", International Business Times, Archived from the original on 28 April 2017, accessed on 28 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[163] Jeffries, Adrianne (19 December 2013), "How to steal Bitcoin in three easy steps", The Verge, Archived from the original on 27 July 2019, accessed on 28 Sep 2023

[164] Roberts Daniel, (15 December 2017), "How to send bitcoin to a hardware wallet", Yahoo Finance, Archived from the original on 17 February 2018, accessed on 28 Sep 2023

[165]BarskiConrad,e al, (2015), Bitcoin for the Befuddled. No Starch Press. ISBN 978-1-59327-573-0, accessed on 28 Sep 2023

[166] Martindale, Jon (16 March 2018). "Who owns all the Bitcoin? A few billionaire whales in a small pond", Digital Trends, Archived from the original on 30 June 2019, accessed on 28 Sep 2023

[167]BeikverdiA.,et al, (2015), Trend of centralization in Bitcoin's distributed network, accessed on 28 Sep 2023

[168] Staff, Verge (13 December 2013). "Casascius, maker of shiny physical bitcoins, shut down by Treasury Department", The Verge, Archived from the original on 10 January 2014, accessed on 28 Sep 2023

[169]ArapinisMyrto, et al, (2019), A Formal Treatment of Hardware Wallets (PDF) (Technical report), University of Edinburgh, IOHK, accessed on 28 Sep 2023

[170] Martindale Jon, (16 March 2018), "Who owns all the Bitcoin? A few billionaire whales in a small pond", Digital Trends, Archived from the original on 30 June 2019, Retrieved 1 July 2019, accessed on 28 Sep 2023

[171] Ahonen Elias, et al, (2016), Encyclopedia of Physical Bitcoins and Crypto-Currencies, Elias Ahonen, ISBN 978-0-9950-8990-7, accessed on 28 Sep 2023

[172] Mack, Eric (25 October 2011). "Are physical Bitcoins legal?", CNET, Archived from the original on 26 June 2019, accessed on 29 Sep 2023

[173] French, Sally (9 February 2017). "Here's proof that this bitcoin crash is far from the worst the cryptocurrency has seen", Market Watch, Archived from the original on 3 July 2018, accessed on 29 Sep 2023

[174] https://www.britishmuseum.org/collection/object/C_2012-4040-4, accessed on 29 Sep 2023

[175] Finley, Klint (31 October 2018). "After 10 Years, Bitcoin Has Changed Everything—And Nothing". Wired, Archived from the original on 5 November 2018, accessed on 29 Sep 2023

[176] Bustillos, Maria (1 April 2013), "The Bitcoin Boom", The New Yorker, Archived from the original on 2 July 2018, accessed on 29 Sep 2023

[177] Bernard, Zoë (2 December 2017). "Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator", Business Insider, Archived from the original on 15 June 2018, accessed on 29 Sep 2023

[178] Finley, Klint (31 October 2018). "After 10 Years, Bitcoin Has Changed Everything—And Nothing", Wired, Archived from the original on 5 November 2018, accessed on 29 Sep 2023

[179] Nakamoto, Satoshi (3 January 2009), "Bitcoin", Archived from the original on 21 July 2017, accessed on 29 Sep 2023

[180] Nakamoto, Satoshi (9 January 2009). "Bitcoin v0.1 released". Archived from the original on 26 March 2014, accessed on 29 Sep 2023

[181] Bustillos, Maria (2 April 2013), "The Bitcoin Boom", The New Yorker, Condé Nast. Archived from the original on 27 July 2014, accessed on 29 Sep 2023

[182] Ostroff, Caitlin; Pérez, Santiago (9 June 2021). "El Salvador Becomes First Country to Approve Bitcoin as Legal Tender", Wall Street Journal, ISSN 0099-9660, accessed on 29 Sep 2023

[183] https://bitcoincore.org/en/2016/01/26/segwit-benefits/, accessed on 29 Sep 2023

[184] "YouTube admits error over Bitcoin video purge", bbc.com, BBC, 28 December 2019. Archived from the original on 28 December 2019, accessed on 29 Sep 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[185] Alexander, Doug (4 February 2019). "Crypto CEO Dies Holding Only Passwords That Can Unlock Millions in Customer Coins", bloomberg.com, Bloomberg, Archived from the original on 16 December 2019, accessed on 29 Sep 2023

[186] del Castillo, Michael (19 March 2020). "Bitcoin's Magic Is Fading, And That's A Good Thing". Forbes.com. Archived from the original on 20 March 2020, accessed on 29 Sep 2023

[187] Ryan Browne (29 January 2021). "Bitcoin spikes 20% after Elon Musk adds #bitcoin to his Twitter bio". CNBC, accessed on 29 Sep 2023

[188] Will Daniel (26 January 2021). "Crypto miner Marathon Patent Group pours $150 million into bitcoin as the token pulls back from record highs". Business Insider, accessed on 29 Sep 2023

[189] https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/,

[190] https://www.bbc.com/news/world-africa-61248809,

[191] "Bitcoin Declared Legal Currency in Central African Republic", Bloomberg.com. 28 April 2022,

[192] https://www.redherring.com/finance/coinseed-raises-7-5m-invests-5m-in-bitcoin-mining-hardware-investment-round-up/, accessed on 30 Sep 2023

[193] Tasca, Paolo (7 September 2015). "Digital Currencies: Principles, Trends, Opportunities, and Risks". SSRN 2657598, accessed on 30 Sep 2023

[194] Williams Mark T., (21 October 2014), "Virtual Currencies – Bitcoin Risk" (PDF), World Bank Conference Washington DC, Boston University, Archived (PDF) from the original on 11 November 2014, accessed on 30 Sep 2023

[195] "Monetarists Anonymous", The Economist, The Economist Newspaper Limited, 29 September 2012. Archived from the original on 20 October 2013, accessed on 30 Sep 2023

[196] "The magic of mining", The Economist, 13 January 2015, Archived from the original on 12 January 2015, accessed on 30 Sep 2023

[197] Kent Peter, et al, (2022), Bitcoinfor Dummies, John Wiley & Sons, p. 102, ISBN 978-1-119-60213-2, accessed on 30 Sep 2023

[198] Divine, John (1 February 2019). "What's the Best Bitcoin Wallet?". U.S. News & World Report, accessed on 30 Sep 2023

[199] https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-global-cryptocurrency-benchmarking-study.pdf, accessed on 30 Sep 2023

[200] Murphy, Hannah (8 June 2018). "Who really owns bitcoin now?", Financial Times, Archived from the original on 10 June 2018, accessed on 30 Sep 2023

[201] Byrnes William H., et al, (2 October 2013), Money Laundering, Asset Forfeiture and Recovery and Compliance – A Global Guide, LexisNexis, p. 2802, ISBN 978-0-327-17084-6, accessed on 30 Sep 2023

[202] "Top 100 Richest Bitcoin Addresses and Bitcoin distribution", bitinfocharts.com, Archived from the original on 15 October 2017, accessed on 30 Sep 2023

[203] https://www.wsj.com/tech/behind-the-curtain-of-elon-musks-secretive-spacex-revenue-growth-and-rising-costs-2c828e2b, accessed on 30 Sep 2023

[204] https://www.wsj.com/livecoverage/tesla-earnings-q2-2022-elon-musk-live/card/tesla-sells-75-of-its-bitcoin-purchases-tgkMdMf1EHDvdniqHu8S, accessed on 30 Sep 2023

[205] https://www.forbes.com/sites/emilymason/2023/08/01/microstrategy-adds-to-its-bitcoin-stash-in-q2-crypto-aids-results/?sh=145a817e16b9, accessed on 30 Sep 2023

[206] https://www.govtech.com/budget-finance/states-split-on-cryptocurrencys-place-in-political-races,

[207] Ibid

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[208] Shiller Robert, (1 March 2014), "In Search of a Stable Electronic Currency", The New York Times, Archived from the original on 24 October 2014, accessed on 01 Oct 2023

[209] "Jersey approve Bitcoin fund launch on island", BBC News. 10 July 2014, Archived from the original on 10 July 2014, accessed on 01 Oct 2023

[210] https://econews.pt/2018/01/22/economics-nobel-prize-winner-richard-thaler-the-market-that-looks-most-like-a-bubble-to-me-is-bitcoin-and-its-brethren/, accessed on 01 Oct 2023

[211] Krugman Paul, (29 January 2018), "Bubble, Bubble, Fraud and Trouble", The New York Times, Archived from the original on 4 June 2018, accessed on 01 Oct 2023

[212] https://www.theguardian.com/technology/2018/feb/02/bitcoin-biggest-bubble-in-history-says-economist-who-predicted-2008-crash,

[213] Wolff-Mann Ethan, (27 April 2018), 'Only good for drug dealers': More Nobel prize winners snub bitcoin, Yahoo Finance, Archived from the original on 12 June 2018, accessed on 01 Oct 2023

[214] "Don't Call Bitcoin a Bubble. It's an Epidemic - Bloomberg". Bloomberg News. Archived from the original on 10 June 2021, accessed on 01 Oct 2023

[215] https://financebrief.org/india/98765431/, accessed on 01 Oct 2023

[216] https://www.zippia.com/developer-jobs/jobs/, accessed on 01 Oct 2023

[217] https://www.guru99.com/cryptocurrency-statistics.html, accessed on 04 Oct 2023

[218] https://www.whitecoatinvestor.com/most-popular-cryptocurrencies/, accessed on 05 Oct 2023

[219] https://coinmarketcap.com/all/views/all/, accessed on 01 Oct 2023

[220] https://www.fool.com/the-ascent/cryptocurrency/articles/6-crypto-trend-predictions-for-2022/, accessed on 01 Oct 2023

[221] https://www.moneycontrol.com/news/business/cryptocurrency/cryptocurrency-prices-today-bitcoin-marginally-up-global-market-cap-increases-7896061.html, accessed on 01 Oct 2023

[222] https://financesonline.com/number-of-blockchain-wallet-users/#, accessed on 01 Oct 2023

[223] https://www.forbes.com/sites/niallmccarthy/2021/07/07/which-countries-have-the-most-crypto-atms-infographic/?sh=34027d973577, accessed on 01 Oct 2023

[224] https://www.zippia.com/advice/cryptocurrency-statistics/, accessed on 01 Oct 2023

[225] https://www.prnewswire.com/news-releases/global-cryptocurrency-market-is-expected-to-grow-with-a-cagr-of-56-4-over-the-forecast-period-from-2019-2025--301028084.html, accessed on 2 Oct 2023

[226] https://www.binance.com/en/blog/all/binance-research-releases-firstever-global-report-on-crypto-user-motivations-behaviors-and-preferences-421499824684901545, accessed on 2 Oct 2023

[227] Ibid

[228] Messina, Irene (31 August 2023), "Bitcoin electricity consumption: an improved assessment - News & insight", Cambridge Judge Business School, accessed on 2 Oct 2023

[229] https://www.grandviewresearch.com/industry-analysis/cyber-security-market, accessed on 2 Oct 2023

[230] https://triple-a.io/crypto-ownership-data/, accessed on 2 Oct 2023

[231] https://thesmallbusinessblog.net/crypto-statistics/?__cf_chl_tk=o1R.1TOzX5bulvsx1gGAxn0S09zV5BUeRTCtvZgAjwY-1696823365-0-gaNycGzNCfs, accessed on 03 Oct 2023

[232] https://www.grandviewresearch.com/industry-analysis/smart-contracts-market-report, accessed on 3 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[233] https://www.statista.com/statistics/806453/price-of-ethereum/, accessed on 3 Oct 2023

[234] https://www.cnbc.com/2021/08/30/cryptocurrency-has-a-big-gender-problem.html, accessed on 3 Oct 2023

[235] https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/, accessed on 2 Oct 2023

[236] https://www.grandviewresearch.com/industry-analysis/crypto-wallet-market-report, accessed on 2 Oct 2023

[237] https://www.grandviewresearch.com/industry-analysis/blockchain-technology-market, accessed on 2 Oct 2023

[238] https://www.pewresearch.org/short-reads/2021/11/11/16-of-americans-say-they-have-ever-invested-in-traded-or-used-cryptocurrency/, accessed on 2 Oct 2023

[239] https://www.globenewswire.com/news-release/2021/12/16/2353499/28124/en/Global-Blockchain-Market-Report-2021-Market-Size-is-Projected-to-Grow-from-4-9-Billion-in-2021-to-67-4-Billion-by-2026-at-a-CAGR-of-68-4.html, accessed on 2 Oct 2023

[240] https://coinmarketcap.com/rankings/exchanges/, accessed on 2 Oct 2023

[241] https://www.statista.com/statistics/1337097/crypto-ownership-usa-age-gender/#, accessed on 3 Oct 2023

[242] https://www.statista.com/statistics/1343499/average-number-of-bitcoin-transactions/, accessed on 3 Oct 2023

[243] https://www.zippia.com/advice/cryptocurrency-statistics/, accessed on 3 Oct 2023

[244] https://www.financemagnates.com/cryptocurrency/education-centre/exploring-the-surging-interest-of-retail-investors-in-cryptocurrency-in-2023/, accessed on 3 Oct 2023

[245] https://www.binance.com/en/research/analysis/global-crypto-user-index-2021, accessed on 3 Oct 2023

[246] https://www.guru99.com/cryptocurrency-statistics.html, accessed on 4 Oct 2023

[247] https://www.forbes.com/uk/advisor/investing/cryptocurrency/cryptocurrency-statistics/, accessed on 03 Oct 2023

[248] https://www.guru99.com/cryptocurrency-statistics.html, accessed on 5 Oct 2023

[249] https://www.guru99.com/how-to-mine-monero.html, accessed on 5 Oct 2023

[250] State of blockchain q1 2016: Blockchain funding overtakes bitcoin (2016), http: //www.coindesk.com/state-of-blockchain-q1-2016/, accessed on 5 Oct 2023

[251] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008), https:// bitcoin.org/bitcoin.pdf, accessed on 5 Oct 2023

[252]Foroglou, G., Tsilidou, A.L., (2015), Further applications of the blockchain, https://www.researchgate.net/publication/276304843_Further_applications_of_the_blockchain, accessed on 5 Oct 2023

[253] Peters, G.W., Panayi, E., Chapelle, A.: Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective (2015), http://dx. doi.org/10.2139/ssrn.2646618, accessed on 5 Oct 2023

[254]Kosba, A., Miller, A., Shi, E., Wen, Z., (2016), Papamanthou, C.: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of IEEE Symposium on Security and Privacy (SP). pp. 839–858. San Jose, CA, USA, accessed on 5 Oct 2023

[255] Akins, B.W., Chapman, J.L., Gordon, J.M., (2013), A whole new world: Income tax considerations of the bitcoin economy https://ssrn.com/abstract= 2394738, accessed on 5 Oct 2023

[256] Zhang Y., et al, (2015), Aniot electric business model based on the protocol of bitcoin. In: Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN). pp. 184–191. Paris, France, accessed on 5 Oct 2023

[257] Sharples, M., Domingue, J., (2015), Theblockchain and kudos: A distributed system for educational record, reputation and reward. In: Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015). pp. 490–496. Lyon, France, accessed on 5 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[258] Noyes C., (2016), Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning. arXiv preprint arXiv:1601.01405, accessed on 5 Oct 2023

[259] Eyal, I., Sirer, E.G., (2014), Majority is not enough: Bitcoin mining is vulnerable. In: Proceedings of International Conference on Financial Cryptography and Data Security. pp. 436–454. Berlin, Heidelberg, accessed on 5 Oct 2023

[260] Biryukov, A., et al, (2014), Deanonymisation of clients in bitcoin p2p network, In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 15–29. New York, NY, USA, accessed on 5 Oct 2023

[261] LeeKuoChuen, D. (ed.), (2015), Handbook of Digital Currency. Elsevier, 1 edn. http://EconPapers.repec.org/RePEc:eee:monogr: 9780128021170, accessed on 6 Oct 2023

[262] Buterin, V., (2014), A next-generation smart contract and decentralized application platform. white paper, available at: https://scholar.google.com/scholar?q=Buterin,+V.,+(2014),+A+next-generation+smart+contract+and+decentralized+application+platform.+white+paper&hl=en&as_sdt=0&as_vis=1&oi=scholart, accessed on 6 Oct 2023

[263] https://www.researchgate.net/figure/An-example-of-blockchain-which-consists-of-a-continuous-sequence-of-blocks_fig1_331425517, accessed on 6 Oct 2023

[264] NRI: (2015), Survey on blockchain technologies and related services, Tech. rep, 2015

[265] Johnson D., et al, (2001), The elliptic curve digital signature algorithm (ecdsa), International Journal of Information Security 1(1), 36–63, accessed on 6 Oct 2023

[266] https://www.researchgate.net/figure/Blockchain-and-block-structure_fig1_351730117, accessed on 6 Oct 2023

[267] https://www.shiksha.com/online-courses/articles/digital-signing-in-blockchain/, accessed on 6 Oct 2023

[268] https://www.educative.io/answers/what-are-the-characteristics-of-blockchain, accessed on 6 Oct 2023

[269] https://www.researchgate.net/figure/Comparisons-between-Private-Public-and-Consortium-Blockchain_tbl1_337904696, accessed on 6 Oct 2023

[270] Buterin, V.: On public and private blockchains (2015), https://blog. ethereum.org/2015/08/07/on-public-and-private-blockchains/, accessed on 9 Oct 2023

[271] Hyperledger project (2015), https://www.hyperledger.org/, accessed on 9 Oct 2023

[272] Consortium chain development, https://github.com/ethereum/wiki/ wiki/Consortium-Chain-Development, accessed on 9 Oct 2023

[273] Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem, ACM Transactions on Programming Languages and Systems (TOPLAS) 4(3), 382–401 (1982), accessed on 9 Oct 2023

[274] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008), https:// bitcoin.org/bitcoin.pdf, accessed on 9 Oct 2023

[275] https://www.semanticscholar.org/paper/Blockchain-challenges-and-opportunities%3A-a-survey-Zheng-Xie/305edd92f237f8e0c583a809504dcec7e204d632/figure/5, accessed on 9 Oct 2023

[276] Ibid

[277] King S.: Primecoin: Cryptocurrency with prime number proof-of-work. July 7th (2013), accessed on 9 Oct 2023

[278] P4Titan: Slimcoin a peer-to-peer crypto-currency with proof-of-burn (2014), accessed on 9 Oct 2023

[279] https://www.researchgate.net/figure/The-Technical-Architecture-of-Blockchain-Drawn-by-the-author_tbl1_369611598, accessed on 9 Oct 2023

[280] Vasin, P.: Blackcoin¡¯s proof-of-stake protocol v2 (2014), https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper.pdf, accessed on 9 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[281] King S., Nadal, S.: Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. SelfPublished Paper, August 19 (2012), accessed on 9 Oct 2023

[282] Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper (2014), accessed on 9 Oct 2023

[283] Zamfir, V.: Introducing casper ¡°the friendly ghost¡±. Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casper-friendly-ghost (2015), accessed on 9 Oct 2023

[284] Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M.: Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Performance Evaluation Review 42(3), 34–37 (2014), accessed on 9 Oct 2023

[285]Burstcoin: burstcoin (2014), https://bitcointalk.org/index.php? topic=731923.0, accessed on 9 Oct 2023

[286] Miguel, C., Barbara, L.: Practical byzantine fault tolerance. In: Proceedings of the Third Symposium on Operating Systems Design and Implementation. vol. 99, pp. 173–186. New Orleans, USA (1999), accessed on 9 Oct 2023

[287] Hyperledger project (2015), https://www.hyperledger.org/, accessed on 9 Oct 2023

[288]Mazieres, D.: The stellar consensus protocol: A federated model for internet-level consensus. Stellar Development Foundation (2015), accessed on 9 Oct 2023

[289]Antshares digital assets for everyone (2016), https://www.antshares.org, accessed on 9 Oct 2023

[290]Bitshares - your share in the decentralized exchange, https://bitshares.org/, accessed on 9 Oct 2023

[291] https://www.researchgate.net/figure/Comparison-between-some-consensus-algorithms_tbl1_330626077, accessed on 9 Oct 2023

[292] Schwartz D., et al, (2014), The ripple protocol consensus algorithm. Ripple Labs Inc White Paper 5 (2014), accessed on 9 Oct 2023

[293] Kwon, J. (2014), Tendermint: Consensus without mining, URL http://tendermint.com/docs/tendermint v04, pdf (2014), accessed on 9 Oct 2023

[294]Vukoli´c, M.: The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: International Workshop on Open Problems in Network Security. pp. 112–125. Zurich, Switzerland (2015), http://dx.doi.org/10.1007/ 978-3-319-39028-4_9, accessed on 9 Oct 2023

[295] Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: Proceedings of International Conference on Financial Cryptography and Data Security. pp. 436–454. Berlin, Heidelberg (2014), accessed on 9 Oct 2023

[296] Decker C., et al, (2016), Bitcoin meets strong consistency. In: Proceedings of the 17th International Conference on Distributed Computing and Networking (ICDCN), p. 13. ACM, Singapore, Singapore (2016), accessed on 9 Oct 2023

[297] Kraft, D.: Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications 9(2), 397–413 (2016), accessed on 9 Oct 2023

[298]Sompolinsky, Y., Zohar, A.: Accelerating bitcoin's transaction processing. fast money grows on trees, not chains. IACR Cryptology ePrint Archive 2013(881) (2013), accessed on 9 Oct 2023

[299] https://www.pwc.com/us/en/industries/financial-services/library/cryptocurrency-questions.html, accessed on 10 Oct 2023

[300] https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html#, accessed on 10 Oct 2023

[301] https://101blockchains.com/decentralization-in-blockchain/, accessed on 10 Oct 2023

[302] https://www.strategy-business.com/article/A-Strategists-Guide-to-Blockchain, accessed on 10 Oct 2023

[303] https://101blockchains.com/blockchain-cryptography/, accessed on 10 Oct 2023

[304] https://www.pwc.com/us/en/industries/financial-services/library/cryptocurrency-evolution.html, accessed on 10 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[305]https://viewpoint.pwc.com/dt/us/en/pwc/podcasts/podcasts_US/Cryptocurrency_Digital_asset_Whats_the_accounting.html, accessed on 10 Oct 2023

[306] https://www.pwc.com/gx/en/about/new-ventures/crypto-center.html, accessed on 10 Oct 2023

[307] https://101blockchains.com/course/blockchain-implementation-and-strategy/, accessed on 10 Oct 2023

[308] Barkatullah, J., et al, (2015), Goldstrike 1: CoinTerra's first-generation cryptocurrency mining processor for Bitcoin. IEEE micro, 35(2), 68–76, accessed on 10 Oct 2023

[309] Böhme R., et al, (2015), Bitcoin: Economics, technology and governance, Journal of Economic Perspectives, 29(2), 213–238. doi:10.1257/jep.29.2.213, accessed on 10 Oct 2023

[310] https://www.sciencedirect.com/science/article/abs/pii/S0040162523002093, accessed on 10 Oct 2023

[311] https://www.sciencedirect.com/science/article/abs/pii/S0925527319300507, accessed on 10 Oct 2023

[312] http://tesi.luiss.it/28102/1/218631_RUSSO_ELENA.pdf, accessed on 10 Oct 2023

[313] https://www.sciencedirect.com/science/article/abs/pii/S1084804517301455, accessed on 10 Oct 2023

[314] https://www.sciencedirect.com/science/article/pii/S1877050916322190, accessed on 10 Oct 2023

[315] https://ieeexplore.ieee.org/abstract/document/7467408, accessed on 10 Oct 2023

[316]ZibinZheng, (20180, Blockchain challenges and opportunities: a survey, International Journal of Web and Grid ServicesVol. 14, No. 4, accessed on 10 Oct 2023

[317] https://ieeexplore.ieee.org/abstract/document/8917991], accessed on 11 Oct 2023

[318] https://ieeexplore.ieee.org/abstract/document/8795541, accessed on 11 Oct 2023

[319] https://www.sciencedirect.com/science/article/abs/pii/S0167739X17318332, accessed on 11 Oct 2023

[320] https://www.sciencedirect.com/science/article/abs/pii/S2542660520300603, accessed on 11 Oct 2023

[321] https://www.sciencedirect.com/science/article/abs/pii/S1084804519303418, accessed on 11 Oct 2023

[322] https://www.sciencedirect.com/science/article/abs/pii/S2210670717310685, accessed on 11 Oct 2023

[323] https://www.sciencedirect.com/science/article/abs/pii/S0167739X17320095, accessed on 11 Oct 2023

[324] https://www.sciencedirect.com/science/article/pii/S1877050918308809, accessed on 11 Oct 2023

[325] Davis, Joshua. "The Crypto-Currency: Bitcoin and its mysterious inventor", The New Yorker, Archived from the original on 18 September 2013, accessed on 11 Oct 2023

[326] "Satoshi's posts to Cryptography mailing list", Mail-archive.com, Archived from the original on 3 January 2013, accessed on 11 Oct 2023

[327] Davis, Joshua (10 October 2011). "The Crypto-Currency: Bitcoin and its mysterious inventor", The New Yorker, Archived from the original on 1 November 2014, accessed on 11 Oct 2023

[328] Angel, J. J., & McCabe, D., (2014), The ethics of payments: Paper, plastic, or Bitcoin? Journal of Business Ethics, 1, 1–9, accessed on 11 Oct 2023

[329]Konashevych O. Advantages and current issues of blockchain use in microgrids, (2016), available at: https://ssrn.com/abstract=2662660, accessed on 11 Oct 2023

[330]Walport M. Distributed ledger technology: beyond blockchain., (2016), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, accessed on 11 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[331] Mattila J. The blockchain phenomenon-the disruptive potential of distributed consensus architectures, (2016), http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf, accessed on 11 Oct 2023

[332] Gartner, Gartner identifies three megatrends that will drive digital business into the next decade, (2017), available at: https://www.gartner.com/newsroom/id/3784363, accessed on 11 Oct 2023

[333] Sahai A, et al, (2005), Fuzzy identity-based encryption, Advances in Cryptology, EUROCRYPT, 3494:457–473, accessed on 11 Oct 2023

[334] Wan Z, et al, (2012) HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Transactions on Information Forensics & Security 7(2):743–754, accessed on 11 Oct 2023

[335] Waters B, (2011), Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. Public Key Cryptography 6571:53–70, accessed on 11 Oct 2023

[336] https://link.springer.com/article/10.1007/s12243-023-00949-8, accessed on 11 Oct 2023

[337] Zhu, Y., et al, (2016), Security architecture and key technologies of blockchain, J. Inf. Secur, Res. 2(12), 1090–1097, accessed on 11 Oct 2023

[338] Sahai A., et al, (2005), Fuzzy identity-based encryption, In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg, accessed on 11 Oct 2023

[339] https://www.sciencedirect.com/science/article/abs/pii/S0016003221005561, accessed on 11 Oct 2023

[340] https://www.sciencedirect.com/science/article/abs/pii/S1570870515001936, accessed on 11 Oct 2023

[341] https://www.sciencedirect.com/science/article/abs/pii/S0920548923000260, accessed on 11 Oct 2023

[342] https://ieeexplore.ieee.org/abstract/document/9841022, accessed on 11 Oct 2023

[343] Su, J.S., et al, (2011), Attribute-based encryption schemes, J. Softw, 22(6), 1299–1315, accessed on 11 Oct 2023

[344] Yu Jiang et al, (2022), Attribute-Based Encryption with Blockchain Protection Scheme for Electronic Health Records, IEEE Transactions on Network and Service Management, Volume: 19, Issue: 4, December 2022, accessed on 11 Oct 2023

[345] Chase, M., (2007), Multi-authority attribute based encryption. In: Vadhan, S.P. (eds.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg, accessed on 11 Oct 2023

[346] Ma, Z., (202), Research on Distributed Authentication and Access Control Based on Blockchain. Chongqing University of Posts and Telecommunications, accessed on 11 Oct 2023

[347] He, P., Yu, G., Zhang, Y., Bao, Y, (2017), Survey on blockchain technology and its application prospect. Comput. Sci. 44(04), 1–7+15, accessed on 11 Oct 2023

[348] https://link.springer.com/chapter/10.1007/978-981-19-5209-8_8, accessed on 11 Oct 2023

[349] Energy Union Package, A framework strategy for a resilient energy union with a forward-looking climate change policy, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?Uri=COM%3A2015%3A80%3AFIN, accessed on 11 Oct 2023

[350] Bronski P, et al., (2015), The economics of load defection: How grid-connected solar-plus-battery systems will compete with traditional electric service-why it matters, and possible paths forward. 〈https://www.rmi.org/wp-content/uploads/2017/04/2015-05_RMI-TheEconomicsOfLoadDefection-FullReport-1.pdf, accessed on 11 Oct 2023

[351] Office of Gas and Electricity Markets (Ofgem). Transition to smart meters, available at: https://www.ofgem.gov.uk/gas/retail-market/metering/transition-smart-meters, accessed on 11 Oct 2023

[352] Ahsan U, et al, (2017), Distributed big data management in smart grid. In: WirelOptCommun Conference (WOCC) 2017, IEEE, 2017, pp. 1–6, accessed on 11 Oct 2023

[353] Swan M., (2015), Blockchain: Blueprint for a new economy. O'Reilly Media Inc., accessed on 11 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[354]https://shop.dena.de/fileadmin/denashop/media/Downloads_Dateien/esd/9165_Blockchain_in_der_Energiewende_englisch.pdf, accessed on 11 Oct 2023

[355] Mattila J, et al., (2016), Industrial blockchain platforms: An exercise in use case development in the energy industry. 〈 https://www.etla.fi/julkaisut/industrial-blockchain-platforms-an-exercise-in-use-case-development-in-the-energy-industry/, accessed on 11 Oct 2023

[356] Grewal-Carr V, , (2016), Blockchain enigma paradox opportunity. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf, accessed on 11 Oct 2023

[357] PwC global power & utilities, Blockchain - an opportunity for energy producers and consumers?, (2016), available at: https://www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf, accessed on 11 Oct 2023

[358] Ernst & Young, Overview of blockchain for energy and commodity trading, (2017), availableat: http://www.ey.com/Publication/vwLUAssets/ey-overview-of-blockchain-for-energy-and-commodity-trading/FILE/ey-overview-of-blockchain-for-energy-and-commodity-trading.pdf, accessed on 11 Oct 2023

[359]Mylrea M. et al., (2017), Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. In: Proceedings of the Resilience Week (RWS) 2017, IEEE, 2017, pp. 18–23, accessed on 11 Oct 2023

[360] Utility Week, Electron reveals blockchain energy platform, (2017), http://utilityweek.co.uk/news/Electron-reveals-blockchain-energy-platform/, accessed on 11 Oct 2023

[361] https://www.researchgate.net/figure/Application-domains-of-Blockchain-technology_fig4_348559366, accessed on 11 Oct 2023

[362] https://www.mdpi.com/1999-5903/14/11/341, accessed on 11 Oct 2023

[363] Peters, G.W., Panayi, E.: Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Social Science Research Network (2015), accessed on 11 Oct 2023

[364] Morini, M.: From'blockchainhype'to a real business case for financial markets. Social Science Research Network (2016), accessed on 11 Oct 2023

[365] Microsoft azure: Blockchain as a service (2016), https://azure.microsoft. com/en-us/solutions/blockchain/.

[366]Ibmblockchain (2016), http://www.ibm.com/blockchain/, accessed on 11 Oct 2023

[367]Jaag, C., Bach, C., et al.: Blockchain technology and cryptocurrencies: Opportunities for postal financial services. Tech. rep. (2016), accessed on 11 Oct 2023

[368] Noyes, C.: Efficient blockchain-driven multiparty computation markets at scale. Tech. rep. (2016), https://www.overleaf.com/articles/ blockchain-multiparty-computation-markets-at-scale/ mwjgmsyybxvw/viewer.pdf, accessed on 11 Oct 2023

[369] Pilkington M., (2016), Does the fintech industry need a new risk management philosophy? ablockchain typology for digital currencies and e-money services in luxembourg. Social Science Research Network (2016), accessed on 11 Oct 2023

[370]Micheler, E., von der Heyde, L.: Holding, clearing and settling securities through blockchain technology creating an efficient system by empowering asset owners. Social Science Research Network (2016), accessed on 11 Oct 2023

[371] Norta, A., Othman, A.B., Taveter, K.: Conflict-resolution lifecycles for governed decentralized autonomous organization collaboration. In: Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society: Challenges in Eurasia. pp. 244–257. ACM (2015), accessed on 11 Oct 2023

[372] Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer Networks 54(15), 2787 – 2805 (2010), accessed on 11 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[373]Miorandi, D., Sicari, S., Pellegrini, F.D., Chlamtac, I.: Internet of things: Vision, applications and research challenges. Ad Hoc Networks 10(7), 1497 – 1516 (2012), accessed on 12 Oct 2023

[374] Akins, B.W., Chapman, J.L., Gordon, J.M.: A whole new world: Income tax considerations of the bitcoin economy (2013), https://ssrn.com/abstract= 2394738, accessed on 12 Oct 2023

[375] Axon, L.: Privacy-awareness in blockchain-based PKI. Cdt technical paper series (2015), accessed on 12 Oct 2023

[376] https://www.tandfonline.com/doi/abs/10.1080/20479700.2020.1843887, accessed on 12 Oct 2023

[377] https://101blockchains.com/implement-blockchain/, accessed on 12 Oct 2023

[378] https://101blockchains.com/public-blockchain/, accessed on 12 Oct 2023

[379] https://101blockchains.com/federated-blockchain/, accessed on 12 Oct 2023

[380] https://www.guru99.com/cryptocurrency-trading-apps.html, accessed on 12 Oct 2023

[381] https://www.guru99.com/best-hardware-wallet-crypto.html, accessed on 12 Oct 2023

[382] https://www.guru99.com/best-bitcoin-wallets.html, accessed on 12 Oct 2023

[383]https://arxiv.org/abs/2303.14438, accessed on 12 Oct 2023

[383] https://arxiv.org/abs/2303.14438, accessed on 12 Oct 2023

[384] https://www.sciencedirect.com/science/article/abs/pii/S0743731520304196, accessed on 12 Oct 2023

[385] https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sfw2.12118, accessed on 12 Oct 2023

[386] https://www.sciencedirect.com/science/article/abs/pii/S0377221721007177, accessed on 12 Oct 2023

[387] https://www.sciencedirect.com/science/article/abs/pii/S0958394717301036, accessed on 12 Oct 2023

[388] https://www.sciencedirect.com/science/article/abs/pii/S0743731523001004, accessed on 12 Oct 2023

[389] https://www.sciencedirect.com/science/article/abs/pii/S0020025518309174, accessed on 12 Oct 2023

[390] https://www.sciencedirect.com/science/article/abs/pii/S2095495619307417, accessed on 12 Oct 2023

[391] https://www.sciencedirect.com/science/article/abs/pii/S0045790618332750, accessed on 12 Oct 2023

[392] https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/sfw2.12118, accessed on 12 Oct 2023

[393] https://dl.acm.org/doi/abs/10.1145/963770.963772, accessed on 12 Oct 2023

[394] https://www.usenix.org/conference/usenixsecurity20/presentation/kalodner, accessed on 12 Oct 2023

[395] Li, X., Zheng, Z., Dai, H.-N.: When services computing meets blockchain: challenges and opportunities. J. Parallel Distr. Comput. 150, 1–14 (2021), https://doi.org/10.1016/j.jpdc.2020.12.003, accessed on 12 Oct 2023

[396] Chen, L., et al.: An enhanced qos prediction approach for service selection. In: Services Computing (SCC), 2011 IEEE International Conference on. IEEE, pp. 727–728 (2011), accessed on 13 Oct 2023

[397] https://www.pwc.com/us/en/industries/financial-services/library/cryptocurrency-questions.html, accessed on 12 Oct 2023

[398] Bruce, J.: The mini-blockchain scheme (July 2014), http://cryptonite. info/files/mbc-scheme-rev3.pdf, accessed on 12 Oct 2023

[399] Van den Hooff, J., Kaashoek, M.F., Zeldovich, N.: Versum: Verifiable computations over large public logs. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 1304–1316. New York, NY, USA (2014), accessed on 12 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[400] Eyal, I., Gencer, A.E., Sirer, E.G., Van Renesse, R.: Bitcoin-ng: A scalable blockchain protocol. In: Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16). pp. 45–59. Santa Clara, CA, USA (2016), accessed on 12 Oct 2023

[401] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: Characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13). New York, NY, USA (2013), accessed on 12 Oct 2023

[402]Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of IEEE Symposium on Security and Privacy (SP). pp. 839–858. San Jose, CA, USA (2016), accessed on 12 Oct 2023

[403] Biryukov, A., Khovratovich, D., Pustogarov, I.: Deanonymisation of clients in bitcoin p2p network. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 15–29. New York, NY, USA (2014), accessed on 12 Oct 2023

[404] Ibid

[405]Möser, M.: Anonymity of bitcoin transactions: An analysis of mixing services. In: Proceedings of MünsterBitcoin Conference. pp. 17–18. Münster, Germany (2013), accessed on 12 Oct 2023

[406] Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: Anonymity for bitcoin with accountable mixes. In: Proceedings of International Conference on Financial Cryptography and Data Security. pp. 486–504. Berlin, Heidelberg (2014), accessed on 12 Oct 2023

[407] Maxwell, G.: Coinjoin: Bitcoin privacy for the real world. In: Post on Bitcoin Forum (2013), accessed on 12 Oct 2023

[408] Ruffing T., (2014), Moreno-Sanchez, P., Kate, A.: Coinshuffle: Practical decentralized coin mixing for bitcoin. In: Proceedings of European Symposium on Research in Computer Security. pp. 345–364. Cham (2014), accessed on 12 Oct 2023

[409] Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous distributed ecash from bitcoin. In: Proceedings of IEEE Symposium Security and Privacy (SP). pp. 397–411. Berkeley, CA, USA (2013), accessed on 12 Oct 2023

[410] Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: Proceedings of 2014 IEEE Symposium on Security and Privacy (SP). pp. 459–474. San Jose, CA, USA (2014), accessed on 12 Oct 2023

[411] Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: Proceedings of International Conference on Financial Cryptography and Data Security. pp. 436–454. Berlin, Heidelberg (2014), accessed on 12 Oct 2023

[412] Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In: Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 305–320. Saarbrucken, Germany (2016), accessed on 12 Oct 2023

[413]Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. arXiv preprint arXiv:1507.06183 (2015), accessed on 12 Oct 2023

[414] Billah, S.: One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner (2015), accessed on 12 Oct 2023

[415] Solat, S., Potop-Butucaru, M.: ZeroBlock: Timestamp-Free Prevention of BlockWithholding Attack in Bitcoin. Technical report, Sorbonne Universites, UPMC University of Paris 6 (May 2016), https://hal.archives-ouvertes.fr/ hal-01310088, accessed on 13 Oct 2023

[416] https://www.inderscienceonline.com/doi/abs/10.1504/IJWGS.2018.095647, accessed on 13 Oct 2023

[417] https://ieeexplore.ieee.org/abstract/document/8805074, accessed on 13 Oct 2023

[418] https://scholarworks.lib.csusb.edu/jitim/vol29/iss4/4/?fbclid=IwAR1eP2D_mZLt70rFGdE-0GCZXnhuFQGGo8b48j8lHzi9m5ynEV3mzYifuXg, accessed on 13 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[419] European Commission, European SmartGrids Technology Platform: Vision and strategy for Europe's electricity networks of the future, available at: https://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf, accessed on 13 Oct 2023

[420] US Department of Energy. Smart grid system report, available at:https://www.smartgrid.gov/files/systems_report.pdf, accessed on 13 Oct 2023

[421] Crypto-currency market capitalizations (2017), https://coinmarketcap.com, accessed on 13 Oct 2023

[422] The biggest mining pools, https://bitcoinworldwide.com/mining/ pools/, accessed on 13 Oct 2023

[423] Szabo, N.: The idea of smart contracts (1997), accessed on 13 Oct 2023

[424] Peters, G.W., Panayi, E.: Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. Social Science Research Network (2015), accessed on 13 Oct 2023

[425] Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper (2014), accessed on 13 Oct 2023

[426]Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of IEEE Symposium on Security and Privacy (SP). pp. 839–858. San Jose, CA, USA (2016), accessed on 13 Oct 2023

[427] Jentzsch, C.: The history of the dao and lessons learned (2016), https://blog, slock.it/the-history-of-the-dao-and-lessons-learned-d06740, accessed on 13 Oct 2023

[428] Omohundro, S., (2014), Cryptocurrencies, smart contracts, and artificial intelligence, AI Matters 1(2), 19–21 (Dec 2014), http://doi.acm.org/10.1145/2685328, 2685334, accessed on 13 Oct 2023

[429] https://www.shiksha.com/online-courses/articles/how-blockchain-technology-can-change-the-world-around-you/, accessed on 13 Oct 2023

[430] https://www.shiksha.com/online-courses/emerging-technologies-courses-certification-training-ct127, accessed on 13 Oct 2023

[431] https://www.shiksha.com/online-courses/what-is-blockchain-st561, accessed on 13 Oct 2023

[432] https://www.shiksha.com/online-courses/what-is-cryptocurrencies-st561-tg1365, accessed on 13 Oct 2023

[433] https://www.shiksha.com/online-courses/what-is-supply-chain-management-st627-tg341, accessed on 13 Oct 2023

[434] https://www.shiksha.com/online-courses/articles/blockchain-in-banking-how-blockchain-can-revolutionize-banking-around-the-world/, accessed on 13 Oct 2023

[435] https://www.shiksha.com/online-courses/what-is-healthcare-ct47, accessed on 13 Oct 2023

[436] https://medium.datadriveninvestor.com/how-blockchain-technology-will-change-the-world-e1d915b4394f, accessed on 13 Oct 2023

[437] https://www.shiksha.com/online-courses/articles/structure-of-a-block-in-blockchain/, accessed on 13 Oct 2023

[438] https://www.linkedin.com/pulse/how-blockchain-technology-change-world-ashutosh-sahni, accessed on 13 Oct 2023

[439] https://www.shiksha.com/online-courses/what-is-internet-of-things-st563, accessed on 13 Oct 2023

[440] https://www.nasdaq.com/articles/how-blockchain-will-change-the-way-we-work-play-and-stay-healthy-in-the-future-2021-08-26, accessed on 13 Oct 2023

[441] https://www.nasdaq.com/articles/mindfulness-industry-to-embrace-crypto-and-blockchains-potential-2021-08-17, accessed on 13 Oct 2023

[442] https://cri-lab.net/security-in-blockchain-applications/, accessed on 13 Oct 2023

[443] https://www.inderscienceonline.com/doi/abs/10.1504/IJWGS.2018.095647, accessed on 13 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970

[444] https://www.nasdaq.com/articles/bitcoins-blockchain-is-the-timechain-lets-call-it-that-2021-08-14, accessed on 13 Oct 2023

[445] https://www.computerweekly.com/news/252494451/Most-British-people-dont-trust-government-with-personal-data, accessed on 13 Oct 2023

[446] https://www.microsoft.com/en-us/industry/blog/government/2019/04/16/could-blockchain-become-governments-best-ally-in-driving-tax-compliance/, accessed on 13 Oct 2023

[447] https://www.bocasay.com/5-ways-blockchain-will-transform-the-world/, accessed on 13 Oct 2023

[448] https://www.jmir.org/2020/7/e18619/, accessed on 13 Oct 2023

[449] https://www.researchgate.net/profile/Shaikh-Abdul-Hannan/publication/372746680, accessed on 13 Oct 2023

[450] https://ieeexplore.ieee.org/abstract/document/9463842, accessed on 13 Oct 2023

[451] https://www.pwc.com/us/en/industries/financial-services/library/cryptocurrency-evolution.html, accessed on 13 Oct 2023

[452] https://www.investopedia.com/terms/b/blockchain.asp, accessed on 13 Oct 2023

[453] https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency, accessed on 13 Oct 2023

[454] https://www.coursera.org/articles/blockchain-developer, accessed on 13 Oct 2023

http://dx.doi.org/10.31364/SCIRJ/v11.i10.2023.P1023970