Journal of Research Administration
Society of Research Administrators International

A STUDY ON EMERGENCE AND FUTURE OF BLOCKCHAIN TECHNOLOGY

Ashish Kumar Singh
(Research scholar) Mahatma Gandhi Kashi Vidyapith University, Varanasi, Uttar Pradesh.

Rajat Jaiswal
(Research scholar) Mahatma Gandhi Kashi Vidyapith University, Varanasi, Uttar Pradesh.

***Corresponding Author: -** Ashish Kumar Singh
*(Research scholar) Mahatma Gandhi Kashi Vidyapith University, Varanasi, Uttar Pradesh.

Abstract

In the era of digitalization, businesses have emerged with the lots of futuristic technologies that make communications easier and faster. This white paper depicts the ubiquitous nature of Peer-toPeer communication i.e., Blockchain. It has several positives and applications in various fields such as digital currency, banking and financial services, logistic, personal identity security etc. Blockchain works on consensus algorithms, once entered information can never be erased. Blockchain has manifold benefits such as decentralization, persistency, anonymity and auditability. Lime light of the paper is to figure out how far the roots of modern technology Blockchain has strengthen and the possible future possibilities.

Keywords: Blockchain, Digital Currency, Consensus Algorithms.

Introduction

Blockchain is a technology based on an immutable ledger, also known as triple entry accounting. In his paper, Trevor I. Kiviat discussed triple entry accounting, claiming that "Blockchain technology enables secure electronic transactions without a centralized ledger or double spending."Instead of a centralized ledger, it makes a collective accounting by distributing a shared (that is, decentralized) public ledger—a complete record of all past transactions on the network. This ledger is the Blockchain. When two parties wish to engage in a transaction, they must broadcast it to the entire network, effectively asking network participants to determine its authenticity.

The 21st century has witnessed remarkable technological strides that help make economic transition efficient and effective as well. Nakamoto [2008] proposed the first generation of the Blockchain and introduced the first decentralized crypto-currency, Bitcoin. Wide-ranging arguments about the benefits of decentralization, disintermediation, anonymity, and censorship resistance in this context have been sparked by the use of digital currencies. Recent times have seen the emergence of Blockchain applications that go well beyond their initial application domains in virtual currency. For example, they are currently crucial in industries like crowdsourcing, prediction markets, registration, and even gambling. Second-generation Blockchain technologies enable computation on a network, where, for example, payments are made conditional on the state of some internal or external variables, in addition to the execution of simple transactions.

Second-generation Blockchain technology has far-reaching applications. The applications do not appear overnight; they have evolved and been conceptualized over the course of more than three decades. The concept was brought down to reality by Satoshi Nakamoto in 2008 and introduced Bitcoin as an electronic peer-to-peer cash system. In the year 2014, Blockchain technology got a big push and separated from bitcoins and entered second-generation applications in financial, nonfinancial, and governance fields.

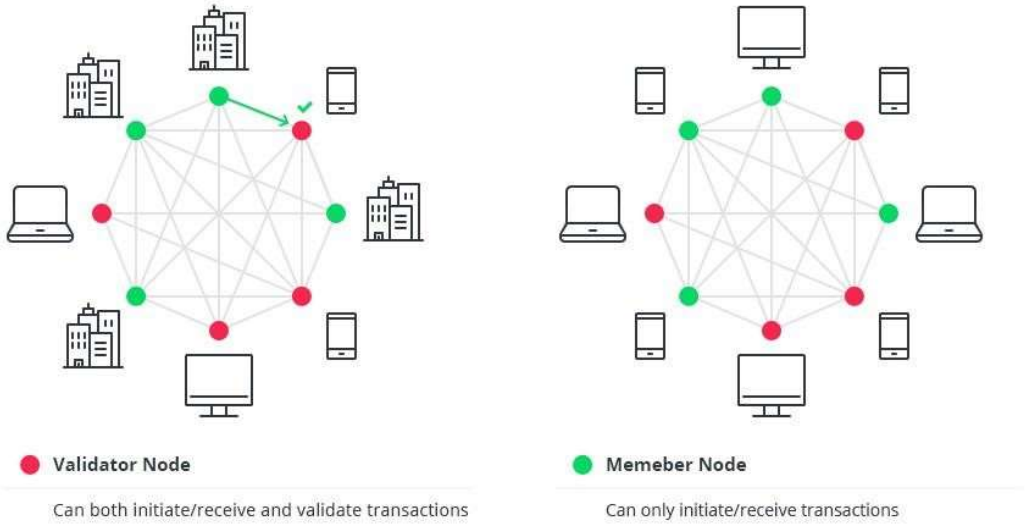

Validator Node
Can both initiate/receive and validate transactions
Memeber Node
Can only initiate/receive transactions

Figure 1: Nodes connected in Blockchain

Categories of Blockchain

- *Permissionless Blockchains*, allow anybody to participate in the verification process without prior authorization; users can contribute their computing power in exchange for a financial reward most often. Sectors using consortium Blockchains are Banks and Clearing houses, Food tracking and Research.
- *Permissioned Blockchains* where the verification nodes are selected by the central authority or consortium. Real estates and retail sectors are often using this type of Blockchain.
- *Public Blockchains* are trustable and anyone can read and submit transactions into the Blockchain. It is open and transparent and van be used in fundraising and voting.
- *Private Blockchains* or restricted Blockchain which is controlled by the single entity. It is centralized and works at high speed. Examples of private Blockchains are internal voting, asset ownership and supply chain management.

Blockchain emergence

The peer-to-peer technology i.e., Blockchain is a technology which was awaken just a decade ago. The idea was first conceived by Stuart Haber and W. Scott Stornetta in 1991. They first thought of cryptographically secured chain of blocks (*cryptography is the study of secure communications techniques that allows only the sender and intended recipient of a message to view its contents*). The term is derived from the Greek word kryptos, which means hidden. In 1998, the famous scientist Nicholas Szabo sprouted the idea of 'bit gold' a decentralized digital currency. The emerging technology was on its incubation stage in the late 20th century. At the onset of 21st century Stefan konst publishes his theory of cryptographic secured chains, plus idea for implementation.

All the basics that required to bring into the existence, the Blockchain technology was conceptualized and merged by Pseudonym Satoshi Nakamoto and released a white paper establishing the model for a Blockchain in 2008. The year 2009 was the year first time ever Nakamoto implements the first Blockchain the public ledger for transactions made using bitcoin. The transactions of bitcoin undergo without the need for a central bank. All the above mentioned belongs to the first generation of Blockchain or say Blockchain 1:0. The efforts made by Satoshi Nakamoto are immutable in developing Blockchain. In the year, 2014, Blockchain 2.0 is born, referring to application beyond the currency. Blockchain technology was separated from the currency after exploring the potential of Blockchain for other financial and interorganizational transactions.

We can simply say bitcoin belongs to first generation Blockchain. Ethereum and Ripple are the famous example of second generation Blockchains. Ethereum distributes a currency called ether, but also allows for the storage and operation of computer code, allowing for smart contracts, and it is the second largest Blockchain after bitcoin on the other hand Ripple is a real-time gross settlement system, currency exchange and remittance network, based on public ledger.

The summary of the evolution of Blockchain technology is given in Table. 1

S. No.	**Year of Publishing**	**Description**
1.	**2008**	A pseudonymous person or group with the name Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System".
2.	**2009**	Founder Satoshi Nakamoto and computer scientist Hal Finney execute the first successful Bitcoin transaction.
3.	**2010**	Laszlo Hanycez, a Florida-based programmer, purchases two Papa John's pizzas with Bitcoin. A transfer of 10,000 BTCs, worth $60 at the time, was made by Hanycez. Bitcoin's market cap is now over $1 million
4.	**2011**	Bitcoin equals 1 USD, making it the world's most valuable cryptocurrency. Several organizations, including Wikileaks and the

		Electronic Frontier Foundation, have started accepting Bitcoin donations.
5.	**2012**	There is widespread media coverage of Blockchain and cryptocurrency, including in television shows such as The Good Wife, bringing
		Blockchain into the mainstream. The Bitcoin Magazine was launched by Vitalik Buterin, a pioneering Bitcoin developer.
6.	**2013**	The Bitcoin market cap has exceeded $1 billion. There was a first-time rise in Bitcoin's price to $100/BTC. The Ethereum Project paper is published, suggesting Blockchain has other uses besides Bitcoin (such as smart contracts)
7.	**2014**	A variety of companies accept Bitcoin as a payment method, including Zynga, The D Las Vegas Hotel, and Overstock.com. In an Initial Coin Offering (ICO), Buterin's Ethereum Project raises over $18 million in Bitcoin and opens up new avenues for Blockchain development. Over 200 Blockchain firms form the R3 group to explore new uses of Blockchain. PayPal announces a Bitcoin integration. The first-ever NFT is minted.
8.	**2015**	It is estimated that more than 100,000 merchants accept Bitcoin. A partnership between NASDAQ and San Francisco-based Blockchain company Chain is intended to test the technology for trading shares in private companies.
9.	**2016**	IBM announced a Blockchain strategy for cloud-based business solutions. Several government agencies recognize the legitimacy of Blockchain and crypto currencies in Japan.
10.	**2017**	The price of Bitcoin reaches $1000/BTC for the first time. Crypto currencies have a market cap of $150 billion. Despite Wall Street's distrust of Blockchain, JP Morgan CEO Jamie Dimon said he believes in this technology. As of 19,783.21/BTC, Bitcoin has reached its all-time high. A Blockchain-powered government has been announced for Dubai by 2020.
11.	**2018**	Facebook committed to creating a Blockchain group and hinted at creating a cryptocurrency itself. Large banks such as Citi and Barclays have signed up to use IBM's Blockchain-based banking platform.
12.	**2019**	President Ji Xinping embraces Blockchain as the Chinese central bank announces its crypto currency. Twitter CEO Jack Dorsey announced Square would hire Blockchain engineers as part of its cryptocurrency plans. Bakkt is a digital wallet company that offers crypto trading on the New York Stock Exchange (NYSE).

13.	**2020**	It is estimated that BTC will reach $30,000 by the end of 2020. From now on, Bitcoin and other cryptocurrencies will be bought, sold, and held by PayPal users. Having launched its central bank digital currency aptly called the Sand Dollar, the Bahamas became the first country in the world to do so. As part of the fight against COVID-19, Blockchain technology plays a key role in securely storing the data of medical researchers and patients
14.	**2021**	For the first time, Bitcoin has reached a market value of more than $1 trillion. Increasing popularity for Web3 implementation. The El Salvadorian government has adopted Bitcoin as a legal tender for the first time. The first car manufacturer to accept Bitcoin as a method of payment for automobiles, Tesla buys $1.5 billion in BTC. As Blockchain technology advances, mainstream interest is drawn to the Metaverse, a virtual environment incorporating Blockchain technology.
15.	**2022**	A $2 trillion market value loss occurs due to economic inflation and rising interest rates. Google forms an Enterprise Digital Assets Team to serve customers on Blockchain-based platforms. In the UK, the government has proposed safeguards for stablecoin holders. Blockchain technologies and NFTs are banned in the popular video game Minecraft.

Working of Blockchain Technology

For two willing parties to complete an online transaction over the Internet using Bitcoin, cryptographic proof is used in place of the third party’s faith. An electronic signature safeguards each transaction. Each transaction is digitally signed using the sender’s “private key” and sent to the recipient’s “public key.” The “private key” must be proven to be the rightful owner before money can be spent. Using the sender’s “public key,” the entity receiving the digital currency authenticates the digital signature on the transaction, proving possession of the associated “private key.”

In 1998, the famous scientist Nicholas Szabo sprouted the idea of "bit gold," a decentralised digital currency. The emerging technology was in its incubation stage in the late 20th century. Stefan Konst published his theory of cryptographic secured chains, along with implementation ideas, at the turn of the century.Every transaction in the Bitcoin network is broadcast to every node before being verified and then added to a public ledger. Every transaction should be verified for validity before being recorded in a distributed ledger. For validation, we should check that "the spender owns the cryptocurrency and digital signature verification on the transaction." and "spender should have sufficient cryptocurrency in his/her account".

Concensus Algorithm

Blockchain is a decentralized distributed ledger that offers security, privacy, anonymity and immutability notwithstanding the absence of a Central authority to confirm and validate the transactions every Blockchain transaction is megarads [A unit of radiation equivalent to one million rads] being fully secure and verifiable. All possible only because of omnipresence of the Consensus protocol, this is soul of any Blockchain network.

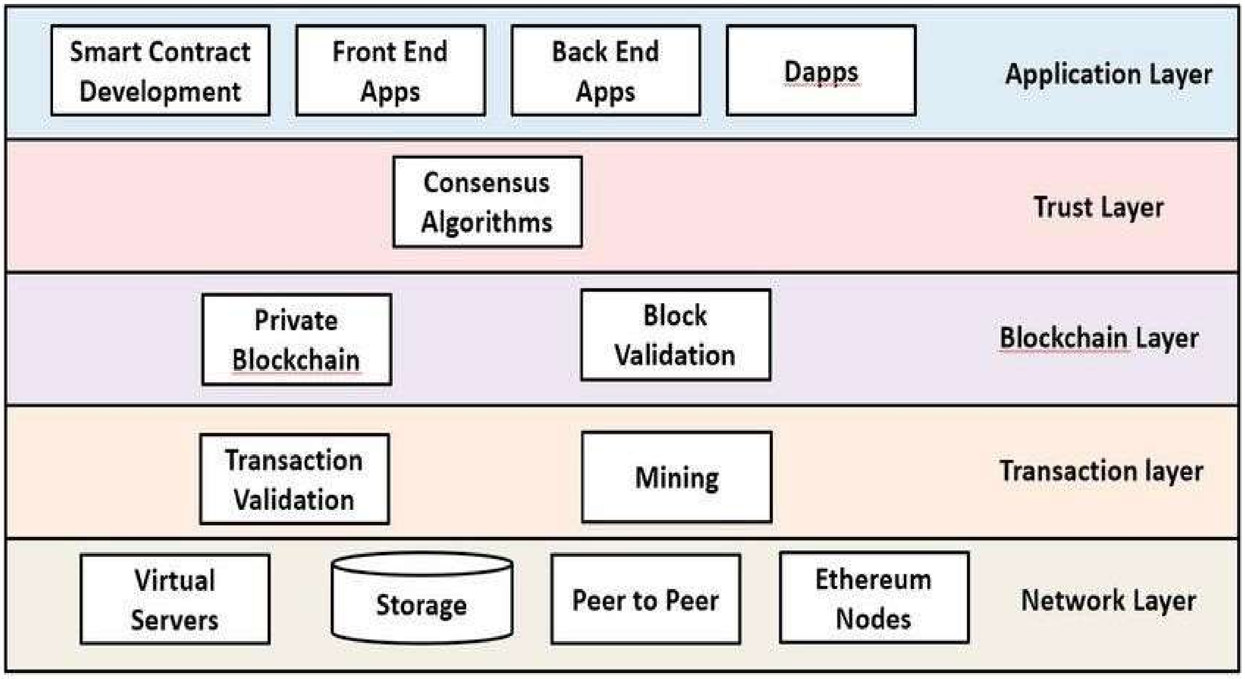


Figure 3: Working Layers of Blockchain

Consensus algorithm is a procedure of the Blockchain through which all the peers network reach a Common agreement about the present state of the distributed ledger."

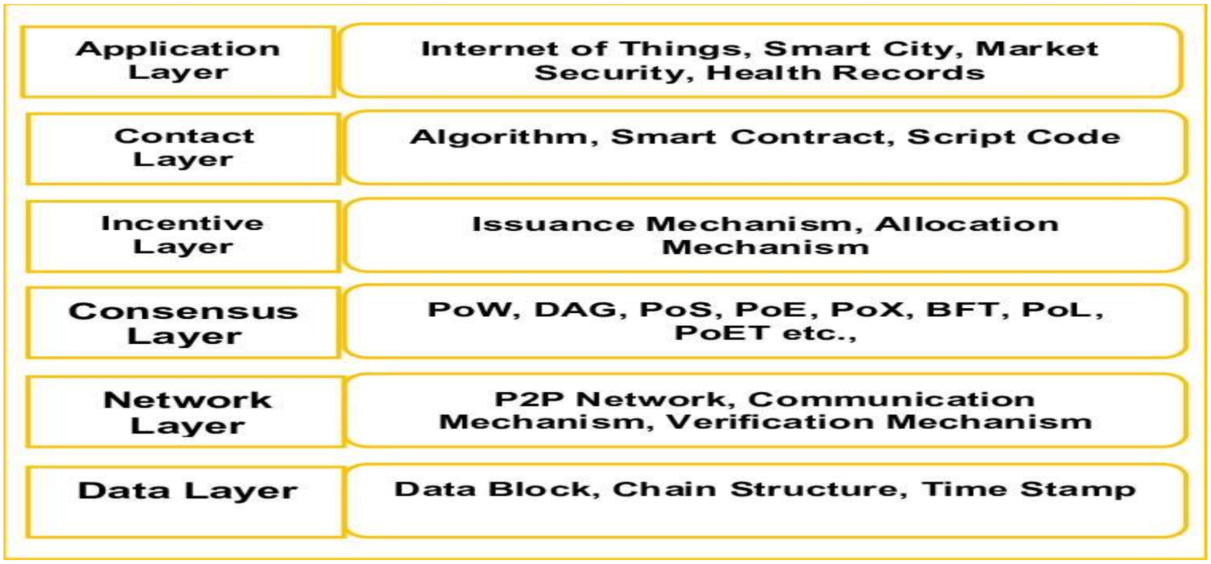
1. **PROOF OF WORK:** To choose a miner for the following block generation, this consensus algorithm is employed. This PoW (PROOF OF WORK) consensus algorithm is used by Bitcoin. The main goal of this algorithm is to quickly and readily provide a solution to a challenging mathematical conundrum. The node that completes this mathematical challenge as quickly as feasible wins the right to mine the following block because it demands a lot of computational power.

2. **Practical Byzantine Fault Tolerance:** A replication algorithm to accept byzantine errors is known as practical byzantine fault tolerance (PBFT) (Miguel and Barbara, 1999). Using the Hyperledger Fabric since PBFT could handle up to 1/3 malevolent byzantine replication, it was chosen as the consensus algorithm. A round determines a fresh block. A primary would be chosen in every round in accordance with certain regulations. Also, it is in charge of directing

the transaction. Three phases, pre-preparation, preparation, and commitment, might be used to describe the entire process.

3. **Proof of Stake (PoS):** This is the most typical substitute for PoW. In Ethereum, the consensus has changed from PoW to PoS. In this kind of consensus algorithm, validators invest in the system's coins by securing part of their own coins as stakes rather than spending money on expensive hardware to solve a challenging puzzle. All validators will then begin validating the blocks. If a validator finds a block that they believe can be added to the chain, they will validate it by placing a wager on it. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets, and their stake increase accordingly. A validator is ultimately selected to create a new block based on its financial investment in the network. As a result, PoS motivate validators to agree through an incentive system.

4. **Delegated Proof of Stake (DPoS):** Another Proof of Stake consensus algorithm is this one. The cornerstone for this particular consensus process is the voting delegation. Other users are given the users' votes by the users. The rewards will be given to the users who delegated to that particular vote by whichever user mines the block next.



Application Layer	Internet of Things, Smart City, Market Security, Health Records
Contact Layer	Algorithm, Smart Contract, Script Code
Incentive Layer	Issuance Mechanism, Allocation Mechanism
Consensus Layer	PoW, DAG, PoS, PoE, PoX, BFT, PoL, PoET etc.,
Network Layer	P2P Network, Communication Mechanism, Verification Mechanism
Data Layer	Data Block, Chain Structure, Time Stamp

Figure 4: Depicting Consensus Layer

5. **Proof of Burn (PoB):** Using PoB, validators "burn" coins by sending them to an address from which they are unrecoverable rather than spending money on pricey hardware equipment. Validators gain the right to mine on the network based on a random selection procedure by sending the coins to an unreachable address. Burning coins here entails a long-term commitment on the part of validators in exchange for a temporary loss. Miners may burn either the native money of the Blockchain application or the currency of an alternative chain, such as bitcoin, depending on how the PoB is implemented. Their chances of getting chosen to mine

the upcoming block increase as they burn more money. PoB is an intriguing substitute for PoW, however the protocol still uses resources inefficiently. The idea that mining power merely goes to those who are prepared to spend more money is also contested.

6. **Proof of Capacity:** Their chances of getting chosen to mine the upcoming block increase as they burn more money. PoB is an intriguing substitute for PoW, however the protocol still uses resources inefficiently. The idea that mining power merely goes to those who are prepared to spend more money is also contested.

7. **Proof of Elapsed Time (PoET):** One of the most ethical consensus algorithms is PoET, which only uses ethical criteria to determine the next block. In Blockchain networks with permissions, it is commonly employed. Every validator on the network has an equal opportunity to construct their own block using this process. To do this, every node waits for a different length of time, adding evidence of their delay to the block. The built blocks are broadcast to the network for review by other users. The validator with the lowest timer value in the proof portion wins. The winning validator node's block is added to the Blockchain. Other safeguards in the algorithm prevent nodes from consistently winning the election and from producing the smallest timer value.

Other consensus algorithms include Leased Proof of Stake, Proof of Activity, Proof of Weight, Proof of Importance, and others. So, it is crucial to carefully select one in accordance with the needs of the business network, as Blockchain networks cannot operate as intended without the consensus algorithms to confirm each and every transaction that is being committed.

Applications of Blockchain

The consensus and security are two of the Blockchain technology's highly recommended properties. Here, we list a few common uses for Blockchain technology. We roughly divide the Blockchain's applications into the financial, IoT, public, and social services, reputation system, security, and privacy sectors.

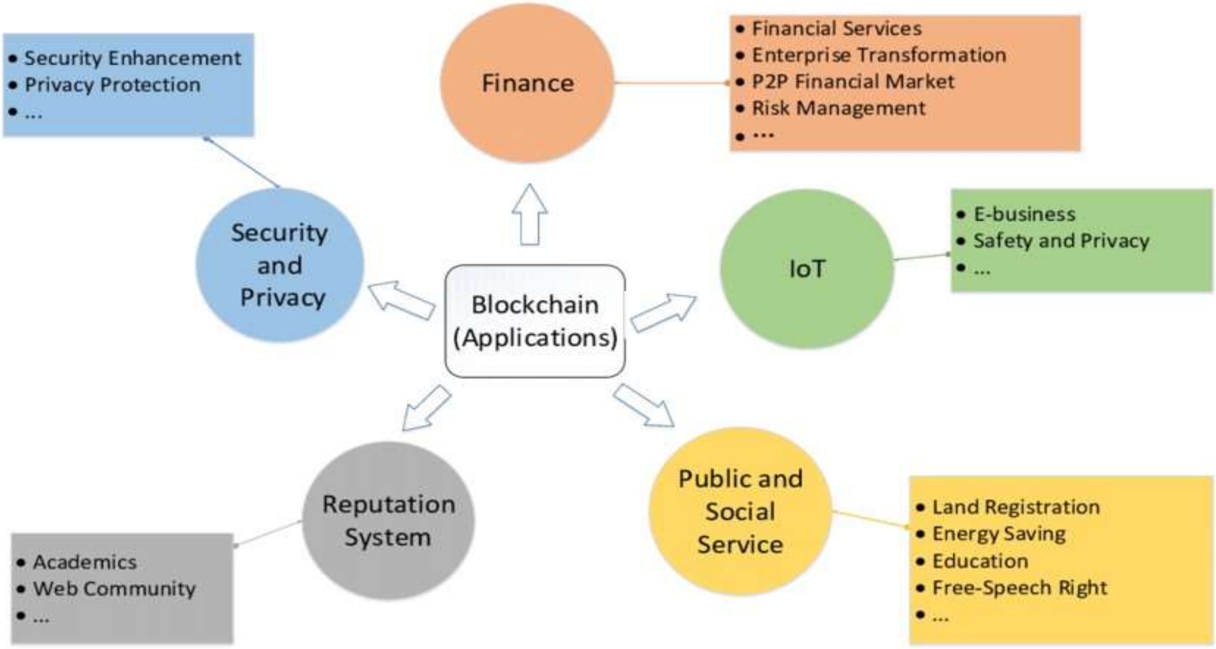


Figure 5: Representative application domains of Blockchain

Financial Application

1. **Private Securities:** A corporation must spend a lot of money to go public. To underwrite the transaction and entice investors, a bank syndicate is required. The secondary market for corporate shares is listed on stock exchanges so that it may operate safely and trades can be settled and cleared quickly. Theoretically, businesses may now offer shares directly through the Blockchain. The secondary market that is built on top of the Blockchain is where these shares can subsequently be bought and traded. These are a few examples: NASDAQ Private Equity, Medici, Block stream, Coin setter Augur, Bit share.

2. **Insurance:** Blockchain can be used to register assets that can be uniquely identifiable by one or more IDs that are challenging to copy or destroy. This can be used to trace the history of transactions as well as confirm who owns an asset. Every item (physical or digital, including real estate, cars, tangible goods, laptops, and other valuables) may be recorded in Blockchain, and the ownership and transaction history may be verified by anybody, particularly insurance.

Non-Financial Applications

1. **Public Notary:** Blockchain technology can be used to validate the document's legitimacy, doing away with the requirement for a centralized authority. The document certification service aids in proving the documents' Ownership (the person who created it), Existence (at a specific moment), and Integrity (that they haven't been tampered with). These services are enforceable under law because they are impervious to forgery and are verifiable by unaffiliated third parties. The confidentiality of the document and those seeking certification

is ensured by using Blockchain for notarization. The notary time stamping is raised to a new level by publishing proof of publication using cryptographic hashes of files into a block chain. Additionally, it does away with the necessity for exorbitant notarial costs and inefficient document transfer methods.

2. **Applications of Blockchain in the Music Industry:** Due to the expansion of the Internet and the availability of numerous streaming services online, the music industry has undergone significant upheaval in the past ten years. Everyone in the music business is being impacted by it, including musicians, labels, publishers, composers, and streaming services. The method for calculating music royalties has always been complicated, but as the Internet has grown in popularity, it has become even more so, leading to calls for greater transparency in the royalties that musicians and songwriters are required to pay. Here’s where the Blockchain can help by keeping a complete, accurate distributed database of ownership data for music rights in a public ledger. The database could be expanded to include information on rights ownership as well as the royalty distribution for each work as determined by "smart contracts."

3. **Decentralized proof of existence of documents:** In any legal settlement, proving the custody or presence of signed documents is crucial. The traditional forms of document validation rely on central authorities to store and validate the papers, which obviously poses certain security risks. As the papers age, these models get harder and harder. The Blockchain technology offers an alternative to the models of document possession and existence evidence. A user can easily record the signature and timestamp associated with a legal document in the Blockchain and validate it whenever they want using native Blockchain techniques by utilizing the Blockchain.

(Proof of Existence is a simple service that allows one to anonymously and securely store online proof of existence of any document. This service simply stores the cryptographic digest of the file, linked to the time in which a user submits his/her document. It is to be noted here that cryptographic digest or fingerprint--not the actual document- is stored in Blockchain, so user need not be worried about the privacy aspect. This allows then a user to later certify the existence of a document that existed at a certain time. The major advantages of this service are security and privacy that allows a user to give decentralized proof of the document that can’t be modified by a third party. The existence of the document is validated using Blockchain that does not depend on a single centralized entity. Proof of Existence web service is available at https://proofofexistence.com/)

4. **Decentralized Storage:** A growing number of people are using cloud file storage services like Dropbox, Google Drive, or One Drive to store their documents, images, videos, and music. While being widely used, cloud file storage systems frequently encounter issues with data control, privacy, and security. The main problem has to entrust a third party with one's

private documents. Storage is a peer-to-peer distributed cloud storage infrastructure built on Blockchain that enables users to transfer and share data without depending on a third-party data provider. In exchange for bitcoin-based micropayments, this enables individuals to share their idle internet bandwidth and unused disc space on their own computer devices with those wishing to store huge files. The majority of conventional data failures and outages are eliminated when there is no central control, which also vastly improves security, privacy, and data control. The challenge system used by the Story platform provides an incentive for users to interact with the network properly. This enables the Story platform to periodically cryptographically verify the availability and integrity of a file and provide direct rewards to people who maintain it.

5. **Decentralized IoT:** Both in the consumer and business markets, IoT technology is gaining popularity. The great majority of IoT platforms have a centralized model in which a hub or broker manages communication between devices. This strategy has shown to be unworkable in many situations when devices must communicate with one another on their own. The development of decentralized IoT platforms has been prompted by this particular demand. The development of decentralized IoT systems, such as secure and reliable data interchange and record keeping, is made possible by Blockchain technology. A decentralized IoT topology is used in this architecture and the Blockchain acts as the general ledger, maintaining a trusted record of all communications sent and received between smart devices.

A technology called ADEPT (Autonomous Decentralized Peer To Peer Telemetry), created by IBM in collaboration with Samsung, combines aspects of the decentralized Internet of Things' underlying architecture to create a dispersed network of devices (IOT). The platform of ADEPT makes use of the three protocols BitTorrent (for file sharing), Ethereum (for smart contracts), and TeleHash (for peer-to-peer messaging).

6. **Blockchain based Anti-Counterfeit Solutions**: One of the major problems in contemporary commerce is counterfeiting. That is one of the largest problems the world of digital commerce is currently facing. Current solutions rely on a third-party trustworthy entity, which creates a logical friction between businesses and customers. The decentralized implementation and security features of Blockchain technology offer an alternative to the current anti-counterfeiting systems. One may imagine a situation where brands, retailers, and marketplaces are a part of a Blockchain network with nodes holding data to verify the items' legitimacy. With the use of this technology, supply chain participants may verify the authenticity of branded goods without depending on a single authority.

7. **Internet Application**: Namecoin is a decentralized, censorship-resistant Domain Name System (DNS) that uses an alternative Blockchain technology (with minor modifications). The governments and major businesses that now control the DNS servers might misuse their

influence to restrict, hijack, or spy on your Internet usage. Since the DNS, or phonebook, of the Internet is kept in a decentralized fashion and any user may have the same phone book data on their computer thanks to the usage of Blockchain technology. For the centralized distribution and maintenance of digital certificates, public key infrastructure (PKI) technology is frequently utilized. To validate a digital signature, every device must have the Certification Authority's (CA) root certificate. Scalability is a problem for PKI despite their extensive use and incredible success. This is due to their reliance on a CA. With Keyless Security Infrastructure, the properties of the Blockchain can assist alleviate some of the shortcomings of the PKI (KSI). By utilizing cryptographic hash functions, KSI enables verification to rely only on the safety of hash functions and the presence of a Blockchain.

8. **Digital identity**: Passports, E-Residency, Birth certificates, wedding certificates, online account login are the following areas can apply Blockchain technology for Identity applications.

9. **Supply chain communications and proof of provenance:** If a company could proactively provide digitally permanent, auditable records that show stakeholders the state of the product at each value.

10. **Smart Contracts:** The digitized contracts entered in Blockchain are legally bound and smart because they are automated and self-execute. Second generation Blockchain applications, such as digitalizing asset ownership, intellectual property, and smart contracts, have attracted a growing amount of industry interest. The latter use case is particularly intriguing because it allows for the encoding of contract rules in computer code that can then be replicated and performed throughout the nodes of the Blockchain. Such a contract may be self-enforcing, observing outside inputs from reliable sources and settling in accordance with its terms.

11. **Digital voting:** With the help of Blockchain, a voter can verify and it was successfully transmitted to the rest of the world. As the data is immutable and distributed among each node the verification becomes ease and effective.

12. **Medical Services:** The newly developed Blockchain technology and its prospective effects on the financial and healthcare sectors. Due to the sensitive nature of data collecting and management, the Blockchain technology offers a decentralized network and is seen to have enormous potential for usage in the financial and healthcare sectors. The evaluation sought to define the current state of Blockchain in financial services and healthcare, as well as its current implementations in these sectors. Blockchain technology offers new models for electronic medical records and financial payments, helping to replace paper-based and manual transaction processing in financial services and healthcare.

Future Applications

1. **Artificial intelligence**: Current advancements in Blockchain technology are opening up new possibilities for applications of artificial intelligence (AI) (Omohundro, 2014). Several Blockchain difficulties may be helped by AI technologies. As an illustration, an oracle is always accountable for assessing if the contract's requirements have been met. This oracle is typically a reliable outside source. An intelligent oracle could be created using AI technology. It just learns from the outside and trains itself; it is not under the control of any party. In such case, there wouldn't be any disputes in the smart contract, and it may advance in intelligence. AI, on the other hand, is already influencing our life. Blockchain technology and smart contracts may be able to limit bad behavior by AI products.

2. **Big data analytics**: Big data and Blockchain could work nicely together. Here, the combination has been roughly divided into two categories: data management and data analytics. In terms of data management, as Blockchain is distributed and safe, it might be utilized to store crucial data. Blockchain might guarantee the data's originality as well. For instance, if Blockchain technology is utilized to store patient health information, the data cannot be altered and is difficult to steal. Blockchain transactions may be used for big data analytics when it comes to data analysis. User trading trends, for instance, might be retrieved. Through the study, users can anticipate the trading habits of possible partners.

3. **Smart contract:** A computerized transaction protocol known as a "smart contract" is used to carry out a contract's terms (Szabo, 1997). This idea has long been floated, and now Blockchain technology can bring it to life. The smart contract is a piece of code that can be automatically executed by miners in Blockchain technology. There are now more and more platforms for developing smart contracts. Developing and smart contracts may be able to accomplish increasing features. IoT and banking services are just two potential applications for Blockchain technology (Christidis and Devetsikiotis, 2016). (Peters and Panayi, 2015). Development and evaluation are the two categories into which we divide research on smart contracts. Smart contract platform development or smart contract development are two possible options.On the Ethereum (Wood, 2014) Blockchain, several smart contracts are currently in use. In terms of platform development, a number of smart contract development platforms are emerging, including Hawk (Kosba et al., 2016) and Ethereum (Wood, 2014). Code analysis and performance evaluation are examples of evaluation. Smart contract flaws could result in catastrophic losses. For instance, the DAO smart contracts over $60 million in funds were stolen as a result of the recursive call flaw (Jentzsch, 2016). Analysis of smart contract attacks is therefore crucial. The performance of smart contracts, on the other hand, is equally crucial to smart contracts. A growing number of smart contract-based apps would be used as Blockchain technology advanced swiftly. Businesses must take application performance into account.

4. **Put an end to the centralization trend:** A decentralized system is how Blockchain is intended. The mining pool is becoming increasingly centralized, though. The top 5 mining pools collectively control more than 51% of the network's total hash power as of this writing. A selfish mining technique (Eyal and Sirer, 2014) also shown that pools with more than 25% of the total computer capacity might earn more money than a fair share. The selfish pool would draw logical miners, and eventually, it might easily have more than 51% of the entire power. As the Blockchain is not designed to benefit a select few organizations, solutions for this issue should be put forth.

5. **Blockchain testing:** Subsequently, many Blockchain types have emerged, and as of this writing, lists over 700 cryptocurrencies. Yet, some developers may exaggerate their Blockchain performance in order to draw investors drawn by the promise of enormous profits. Also, consumers must know which Blockchain best suits their needs when integrating Blockchain into their businesses. In order to test several Blockchains, a framework for Blockchain testing must be in place. Testing for Blockchains may be divided into two stages: standardization and testing. All criteria must be created and approved during the standardization process. After a Blockchain is created, it may be evaluated against the predetermined standards to determine whether it really functions as well as its creators promise. Regarding the testing process, certain criteria need to be used while doing Blockchain testing. For instance, a user in charge of an online retail business is concerned about the throughput of the Blockchain, so the examination must test the capacity for a Blockchain block as well as the average time it takes from the user sending a transaction to the transaction being packed into the Blockchain.

Conclusions and Findings

The purpose of this paper is to highlight a few recent developments in the field of Blockchain technologies. The development of second-generation Blockchain technologies is then explained in depth in a number of ground-breaking new areas, including central bank treasury ledgers, retail and investment bank ledgers, trading, settlement, and clearing processes, and multi-signature escrow services. Blockchain has strengthened its technical jargon in economic transition. Blockchain has emerged as a decentralized consensus, security, transparency, etc. are some of its qualities that we advocate. Consensus makes Blockchains incredibly safe. These days, security is everyone's top concern, and Blockchain fully ensures it. A Blockchain network is virtually impossible to hack since it requires breaking into thousands of connected machines. The benefits of Blockchain features for society are numerous. Blockchain can aid society in eradicating many ills, including corruption, because it is transparent. Due to the transparency feature, no single party can alter the transaction history since if it tries to do so, it will be reflected throughout all Blockchain systems. Final words each Blockchain has a unique set of advantages, and there is no simple answer to the dilemma of choosing which Blockchain to employ.

References

1. Peters, Gareth W. & Panayi, Efstathios (2015).*Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money on,* page 7
2. Nakamoto, Satoshi. (2008). Bitcoin: A peer-to-peer electronic cash system.
3. Wood, Gavin. (2014). *Ethereum: A secure decentralized generalized transaction ledger.*
4. P.S.G. Aruna Sri, (2018). A study on Blockchain technology. *International Journal of Engineering & Technology.*
5. Forsstrom, Stefan. (2018). *Blockchain Research Report.*
6. P. Franco, (2014). Understanding Bitcoin: Cryptography, engineering and economics. *John Wiley & Sons.*
7. TREVOR I. KIVIAT "BEYOND BITCOIN: ISSUES IN REGULATING BLOCKCHAIN TRANSACTIONS" at 578 in *DUKE LAW JOURNAL*
8. Crosby,Michael, Nachiappan, Pattanayak,Pradhan & Verma, Sanjeev.(2015). Blockchain Technology Beyond Bitcoin .*Sutardja Center for Entrepreneurship & Technology Technical Report*
9. NAKAMOTO, supra note 31, at 8.
10. Di, Z., Wang, G., Jia, L., & Chen, Z. (2018). Blockchain challenges and opportunities: a survey. *Int. J. Web and Grid Services*, Vol. 14, No. 4, 2
11. Castro, Miguel & Liskov, Barbara .(1999, February). Practical Byzantine Fault Tolerance. *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, USA
12. Aithal, P.S. & Aithal, Architha.(2021).Blockchain Technology - Current Status and Future Research Opportunities in Various Areas of Healthcare Industry. *International Journal of Health Sciences and Pharmacy* ISSN: 2581-6411, Vol. 5, No. 1
13. Harvey, C.R.(2014).*Bitcoin Myths and Facts*. https://www.semanticscholar.org/paper/Bitcoin Myths-and-Facts-Harvey/992342c42002b5952df16f8236b1c80072135496
14. Hayes, A.(2019).*The socio-technological lives of bitcoin.* Theory Cult. Soc., 36, 49–72. [CrossRef]
15. Rose, C. (2015).The evolution of digital currencies: Bitcoin, a cryptocurrency causing a monetary revolution. *Int. Bus. Econ. Res. J*, 14, 617–622. [CrossRef]
16. Jeong, S.(2022).*The Bitcoin Protocol as Law, and the Politics of a Stateless Currency*. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124
17. Di, Z., Wang, G., Jia, L., & Chen, Z. (2022, September). Bitcoin transactions as a graph. *IET Blockchain*, *2*(3–4), 57–66. https://doi.org/10.1049/blc2.12016
18. Szabo, N. (1997) The Idea of Smart Contracts
19. Peters, G.W. and Panayi, E. (2015) 'Understanding modern banking ledgers through Blockchain technologies: Future of transaction processing and smart contracts on the internet of money', *Social Science Research Network*.

20. Christidis, K. and Devetsikiotis, M. (2016) ‘Blockchains and smart contracts for the internet of things’, *IEEE Access*, Vol. 4, pp.2292–2303.
21. Wood, G. (2014) Ethereum: A Secure Decentralised Generalised Transaction Ledger, Ethereum *Project Yellow Paper*.
22. Jentzsch, C. (2016) The History of the DAO and Lessons Learned.
23. Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C. (2016) ‘Hawk: the Blockchain model of cryptography and privacy-preserving smart contracts’, *Proceedings of IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, pp.839–858.
24. Omohundro, S. (2014) ‘Cryptocurrencies, smart contracts, and artificial intelligence’, AI Matters, Vol. 1, No. 2, pp.19–21.
25. DuPont, Q.(2019).Cryptocurrencies and Blockchains. *John Wiley& Sons: Hoboken, NJ, USA*
26. French, L.A.(2022).The Effects of Blockchain on Supply Chain Trust: A Thesis Presented in Partial of the Requirements for the Master of Supply Chain Management. *Massey University, Palmerston North, New Zealand. Ph.D. Thesis, Massey University, Palmerston North, New Zealand*
27. Burniske, C.; White, A.(2017). *Bitcoin: Ringing the Bell for a New Asset Class.*
28. Mougayar, W. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology; *John Wiley & Sons: Hoboken*, NJ, USA, 2016.
29. Notaro, A. 2022. *All that is solid melts in the Ethereum: The brave new (art) world of NFTs*. *J.Vis. Art Pract.,* 1–24 . [CrossRef]
30. KiliÇarslan, S.K.(2023).*Bitcoin Özel˙Inde Kripto paralarin Edinilmi¸s mallara katilma rejiminde tasfiyesi sorunu. Kırıkkale Hukuk Mecmuası*, 3, 1–27.
31. Strilets, B.(2022).*Current state and prospects for the legal regulation of cryptocurrencies in the European Union*. 70–76. [CrossRef]
32. Ramadoss, R.(2022).*Blockchain technology: An overview*. 41, 6–12. [CrossRef]
33. Eyal, I. and Sirer, E.G. (2014) ‘Majority is not enough: Bitcoin mining is vulnerable’, Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, pp.436–454
34. Hocao glu, M.; Habbal, A .(2022).*NFT-based model to manage educational assets in Metaverse*.
35. Trimborn, S.; Peng, H.; Chen, Y.(2022).*Influencer Detection Meets Network AutoRegression– Influential Regions in the Bitcoin Blockchain.*
36. *https://proofofexistence.com/*
37. *www.kaspersky.com*
38. *https://www.icaew.com/technical/technology/Blockchain-and-cryptoassets/Blockchainarticles/what-is-Blockchain/history*
39. *https://www.ft.com/content/eb1f8256-7b4b-11e5-a1fe-567b37f80b64#axzz3qe4rV5dH*
40. *https://www.geeksforgeeks.org/consensus-algorithms-in-Blockchain/*
41. *https://www.researchgate.net/figure/Blockchain-layered-architecture-31-Proposed-SystemModel-Ethereum-Private-Blockchain_fig3_340700069*

42. *https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/*