BLOCKCHAIN TECHNOLOGY

MAMATHA LOGANATH.

Department of Computer Science and Engineering, RNSIT
Bangalore, Karnataka, India

Email:

mamatha200114@gmail.com

NANDITA R P.

Department of Computer Science and Engineering, RNSIT
Bangalore, Karnataka, India

Email:

nandikavya24@gmail.com

Abstract—"EVERYTHING WILL BE TOKENIZED AND CONNECTED BY BLOCKCHAIN ONE DAY"
-FRED EHRSAM

Blockchains have received a lot of attention recently since they provide localized approaches to the creation and management of value. Blockchains are currently talked concerning within the news worldwide. Several banks, web companies, automotive manufacturers, and even governments worldwide have incorporated or started considering blockchains as localized approaches to fraud-resistant computing while not a trusty authority. A blockchain could be a distributed, append only log of time-stamped records that's cryptographically protected against tampering and revision to improve the security, scalability, and potency of their services. This paper provides a survey of blockchain applications in numerous areas. These areas embrace cryptocurrency, healthcare, advertising, insurance, copyright protection, energy, and social applications. Our work provides a timely outline for individuals and organizations curious about blockchains. This survey envision to encourage a lot of blockchain applications.

KEYWORDS: Blockchain, decentralized IoT, security, digital ledger, consensus algorithm, PoW, PoS

I. INTRODUCTION

Blockchain is an information recording system that makes it difficult or impossible to modify, hack, or defraud the system. A blockchain is essentially a digital record of transactions that are duplicated and distributed across the entire network of computer systems on the blockchain. Blockchain is a technology that securely manages ever-growing lists of data and transaction records. Blockchain relies on established cryptographic techniques so that every participant in a network can interact to store, exchange and display information. No centralized authority, Instead, the transaction logs are stored and distributed across the network. The entries are provided with the date and time. Interactions with the blockchain medium are made known to all participants and must be verified by the network before adding the information. This allows less trust in the collaboration between the participants on the network, while keeping an immutable audit trail of all interactions: for security reasons, users can only update the block they have access to, and those updates are replicated across the network. Many people still confuse blockchain with bitcoin, but they are not the same. Bitcoin is an application that uses blockchain technology. Blockchain offers many advantages such as decentralization, persistence, anonymity and verifiability.

II. OVERVIEW OF BLOCKCHAIN

In principle, a blockchain should be considered as a distributed append-only time stamped data structure. Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can verifiably interact with each without the need for a trusted authority. To achieve this one can consider blockchain as a set of interconnected mechanisms which provide specific features to the infrastructure, as illustrated in figure 1. At the lowest level of this infrastructure, we have the signed transactions between peers. These transactions denote an agreement between two participants, which may involve the transfer of physical or digital assets, the completion of a task, etc. At least one participant signs this transaction, and it is disseminated to its neighbors. Typically, any entity which connects to the blockchain is called a node. However, nodes that verify all the blockchain rules are called full nodes. These nodes group the transactions into blocks and they are responsible to determine whether the transactions are valid, and should be kept in the blockchain, and which are not. A valid transaction means, for instance, that Jack received one bitcoin from Bob. However, Bob may have tried to transfer the bitcoin, as it is a digital asset, to Carol. Therefore, nodes must reach to an agreement on which transactions must be

kept in the blockchain to guarantee that there will be no corrupt branches and divergences.

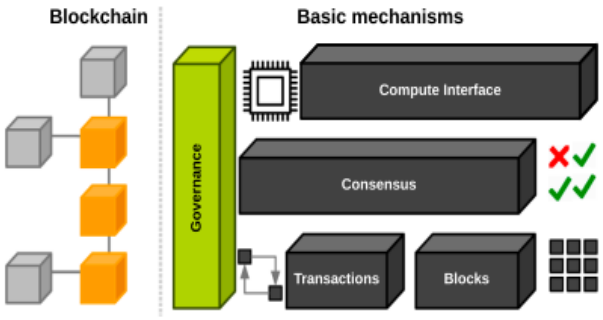

Figure 1*.An overview of blockchain architecture*

III. THE THEORY OF BLOCKCHAIN

Blockchain technology is not using one single technique but contains Cryptography, mathematics, Algorithm and economic model, combining peer-to-peer networks and using distributed consensus algorithm to solve traditional distributed database synchronization problem. [1, 2, 3]

The following six key elements of blockchain are:

A. Decentralized:

Blockchain doesn't have to rely on centralized node anymore, the data can be recorded, stored and updated distributively.

B. Anonymity:

Blockchain technologies solve the trust problem between node to node, so data transfer can be anonymous, only person's blockchain address need to know.

C. Autonomy:

The blockchain solely works according to the rules which are defined by its members. There is no central-authority for the defined rules.

D.Automation :

Manual processes that are generally guided by the legal contracts can be automated with a self-executing type of computer program called as smart contract. A smart contract is a component of a blockchain-based system which can automatically enforce stakeholder-agreed rules and process steps. Once launched, smart contracts are completely autonomous; when the conditions of contracts are met, pre-specified and agreed actions occur automatically.

E.Security:

There are various ways which proves a blockchain is more secure than other record-keeping systems. Transactions must be agreed upon before they are recorded into the system. Once a transaction is approved, it is encrypted and then linked to the previous transaction. This, along with the fact that information is stored across the network of computers instead on a single server, makes it very difficult for hackers to compromise the transactional data. In any industry where the protection of sensitive data is crucial — financial services, government, healthcare — blockchain has an opportunity to change how the critical information is shared by helping to prevent frauds and unauthorized activity.

F. Transparency :

The data's record by blockchain system is transparent to each node, it is also transparent on update of data that is why blockchain can be trusted. Changes to public blockchains are publicly viewable by all parties creating transparency, and all transactions are unchangeable.

IV.TYPES OF BLOCKCHAIN ARCHITECTURE

A. Public Blockchain

Public blockchain is an unrestricted and unlicensed distributed ledger system. Anyone with Internet access can enter the blockchain platform, become an authorized node and become a part of the blockchain network. Part of the public blockchain is authorized to access current and previous records, view transactions or perform proof of work on incoming blocks and perform mining. Most of the time, public blockchains are used to mine and exchange cryptocurrencies. The most common public blockchains are Bitcoin and Litecoin blockchains. As long as users strictly abide by security rules and practices, public blockchains are basically safe. However, this is only dangerous if the participant has sincerely failed to comply with the security agreement.

B. Private Blockchain

A private blockchain is an authorization or a restrictive blockchain that only runs on a closed network. Private blockchains are generally used in an organization or company where only selected members are participants in a blockchain network. Therefore, private blockchains have a similar use to public blockchain but have a small and restrictive network. Private
Blockchain networks are implemented for voting, supply chain management, digital identity, asset ownership
Some of the examples are Multichain and Hyperledger projects (Fabric, Sawtooth), Corda.

C. Consortium Blockchain

A consortium blockchain is a semi-decentralized type where more than one organization manages a blockchain network. This is contrary to what we saw in a private blockchain, which is managed by only a single organization. More than one organization can act as a node in this type of blockchain and exchange information or do mining. Consortium blockchains are typically used by *banks, government organizations*, etc.
Examples of consortium blockchain are; Energy Web Foundation, R3.

D. Hybrid Blockchain

Hybrid blockchain is a combination of private and public blockchains. It uses the properties of two types of blockchains, so you can have either a privilege-based private system or a non-privileged public system. Through such a hybrid network, users can control who has access to data stored on the blockchain. Only selected parts of the data or blockchain data sets can be released, and the rest will be handled confidentially in a private network. The hybrid blockchain system is very flexible, so users can easily connect a private blockchain with multiple public blockchains. Transactions on private hybrid blockchain networks are usually verified on that network. However, users can also share it for review on a public blockchain. Public blockchain Increases the hashing and uses more nodes for verification. This increases the security and transparency of the blockchain network. An example of a hybrid blockchain is Dragonchain.

V.BLOCKCHAIN PARTICIPANTS

Blockchain participants include:

- Blockchain user
- Blockchain regulator
- Blockchain developer
- Blockchain network operator
- Certificate authority
- Traditional processing platform
- Traditional data resources

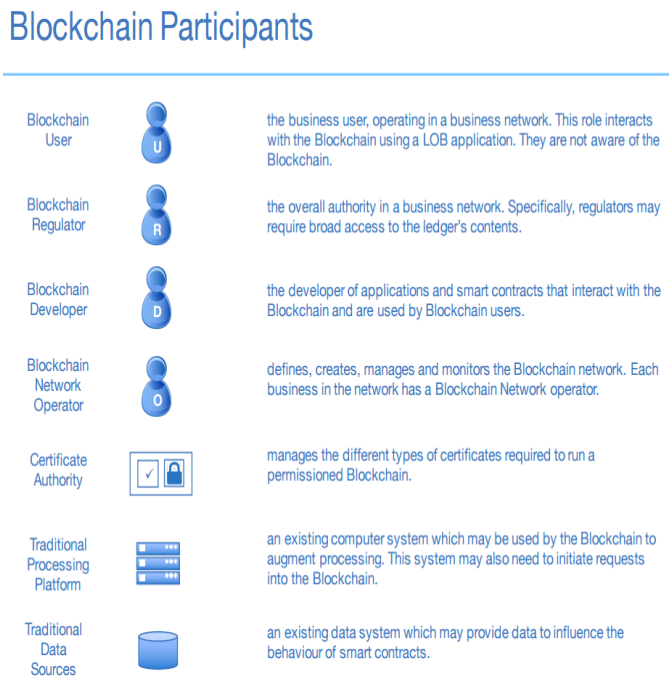

Figure 2. Blockchain participants

VI.BLOCKCHAIN COMPONENTS

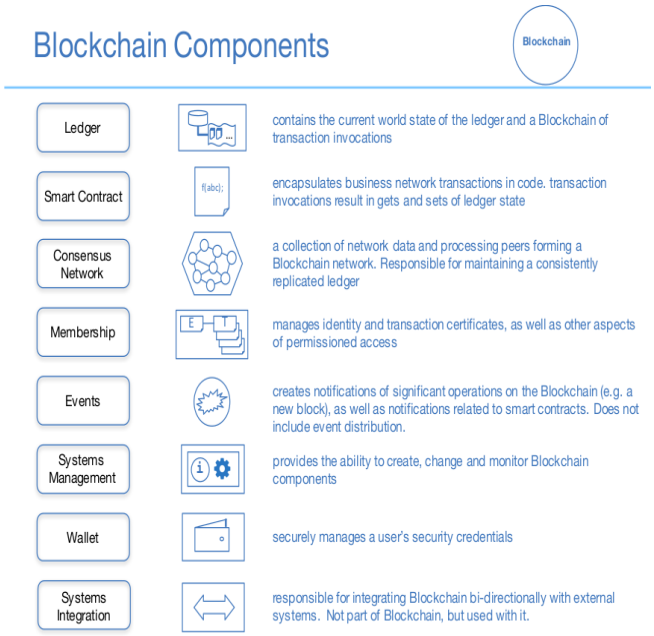

Figure 3. Blockchain components

- Ledger
- Smart contract
- Consensus network
- Membership
- Events
- System management
- Wallet
- System integration

VII.CONSENSUS ALGORITHMS

A consensus algorithm [4] is like Bitcoin's PoW (Proof-of-Work), which requires miners to solve complex cryptographic mathematical puzzles for which they get rewarded with certain amount of Bit coins. It is important to understand that each block which is added to the network must follow a set of consensus rules.

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger [5].

A. Proof of Work (Pow)

This consensus algorithm is used to select miners for the next generation of blocks. Bitcoin uses this PoW consensus algorithm. The main idea of the algorithm is to solve a complex mathematical problem and find a solution easily. The power and the ensuing knot to solve the problem as quickly as possible destroys the next obstacle.

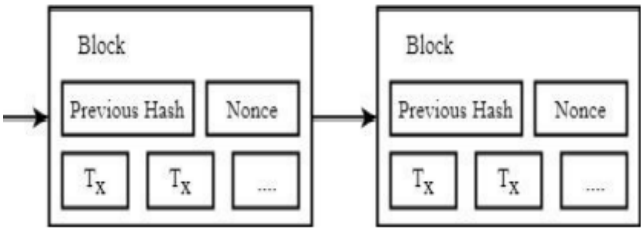

Figure 4. (PoW) Proof of Work

In Figure 4, A nonce is an abbreviation for "number only used once," which is a number added to a hashed block in a blockchain that, when rehashed, meets the difficulty level restrictions. The nonce is the number that blockchain miners are solving for. The hash number connects new block to the last block in the valid blockchain.

B. Proof of Stake (PoS)

PoS replaces PoW. Ethereum uses PoS consensus. This is not to invest in costly hardware to solve complex problems, but to invest in system coins and prevent certain coins as bets. They found blocks that they thought could be linked together. According to the actual blocks added to the blockchain, all validators will receive corresponding rewards based on the increase in their participation. Finally, validator is selected generate new block based on their economy class. Block networks based on their economic participation. Therefore, PoS will reward verifiers through a consensus incentive mechanism. When the miner has more coins, the mining tool has more choices. In figure 5, Kernel input is the initial coin stake input that has to pass hash protocols.

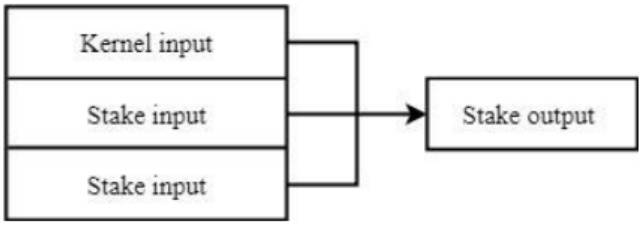

Figure 5.Structure of PoS Transaction

PoS uses less equipment as well as the electricity cost is less. The below graph gives the comparison between Pow and PoS.

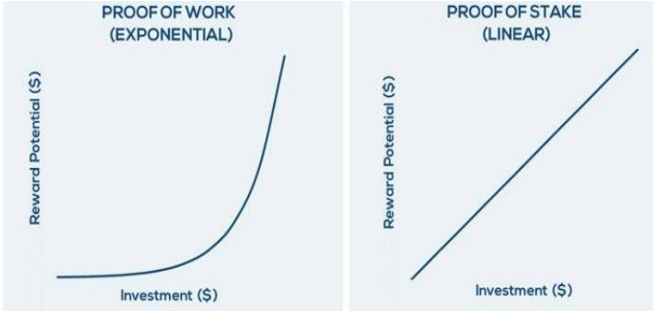

Figure 6. Comparison between PoW and PoS

VIII. Blockchain Technology Platforms

	BITCOIN	ETHEREUM	HYPERLEDGER	R3 CORDA
Verification	Proof of work Data format: Merkle tree (20 txs per sec)	Proof of work Data format: Patricia tree	Consensus based – Modular & Extensible	Consensus with Financial sector as focus area
Permission State	Permissionless with basic contracts	Permissionless with smart contracts (e.g. solidity)	Permissioned with smart contracts (e.g. Golang, Java)	Permissioned with Smart contracts (Kotlin, Java) Smart Legal prose
Distributed	Distributed system with all accounts equal access	Distributed system with all accounts equal access	Distributed system with role-based restricted access	Microledgers semi-distributed systems with restricted access
Block creators	External account	External Account, Contract account	Multiple roles such as Validator or Transactor	Multiple roles including Notary
Cryptocurrency	Bitcoin currency	Ether or other tokens via smart contract	No currency (chaincode tokens if required)	No currency

Figure 7: Table: Blockchain Technology Platforms

IX. Benefits of Blockchain Technology

A.Enhanced security

Data is sensitive and important, and blockchain can greatly change the way of displaying critical information. By creating an immutable record and encrypting it from beginning to end, blockchain helps prevent fraud and unauthorized activities. The blockchain is implemented by anonymizing personal data and using permissions to prevent access. This information is stored on a computer network instead of a single server, which makes it difficult for hackers to view the data.

B. Great Transparency

Without blockchain, every organization has to hold a separate database. Since blockchain makes use of a disbursed ledger, transactions and information are recorded identically in multiple locations. All community individuals with permission get admission to see the identical statistics on the identical time, imparting complete transparency. All transactions are immutability recorded, and are time- and date-stamped. This permits participants to view the whole records of a transaction and sincerely removes any possibility for fraud.

C. Instant Traceability

The blockchain adds an audit trail to record the source of each step of the asset. This can help provide evidence in industries where consumers are concerned about environmental or human rights issues related to products, or in industries where counterfeiting and fraud exist. Raw data can be shared directly with customers. Traceability data can

also reveal weaknesses in any chain where goods might sit on a loading dock awaiting transit.

D. Increased efficiency and speed

Traditional processes that require many paper documents are time-consuming, prone to human error, and often require third-party mediation. By optimizing these processes using blockchain, transactions can be executed faster and more efficiently. Documentation can be stored on blockchain with transaction details without the need of eliminating the paper. There is no need to reconcile multiple lenders, so clearing and settlement can be completed faster.

E. Automation

We can even use smart contracts to automate transactions, thereby increasing transaction efficiency and further speeding up the process. After the specified conditions are met, the next step of the transaction or process will be automatically activated. Smart contracts reduce human intervention and reliance on third parties to verify that terms of a contract have been met. We can even use smart contracts to automate transactions, thereby increasing transaction efficiency and further speeding up the process. After the specified conditions are met, the next step of the transaction or process will be automatically activated. Ensure compliance with contract terms. For example, in insurance, a claim can be filed after the customer has provided all the documents required to submit the claim which is automatically calculated and paid. [11]

X. Challenges of Blockchain Technology

Some of the major challenges faced by Blockchain technology is listed below:

a) Scalability:

As the quantity of exchanges will increase gradually, the block chain seems to be overwhelming. Bitcoin blockchain has now passed one hundred GB of storage [12]. To approve the trade, all transactions ought to be stored. In addition, because of the authentic block length containment and the intervening time used to create every other block, the Bitcoin blockchain can simplest procedure approximately 7 transactions according to second, which can't satisfy the want to put together a large quantity of exchanges in a non-stop layout. Meanwhile, because the block restrict is low, limitless tiny exchanges may be behind schedule as miners are willing in the direction of the ones exchanges with a heavy trade charge. Be that as it may, expansive block length could purpose blockchain branches to go back from spreading velocity. So the trouble of scalability may be very intense.

b) Interoperability/Compatibility:

Interoperability is the potential to unreservedly proportion records crosswise over block chain frameworks [13]. In a totally interoperable condition, if a consumer from every other block chain directs you a piece for your blockchain, you may have the potential to effortlessly peruse, fathom, and cooperate with or react to it with moderate exertion. Tasks that want to execute interoperability of their framework assume to make a platform so one can empower specific different block chains to speak about successfully with one every other, without the requirement for an out of doors delegate.

c) Reliability/Adaptability:

Adaptability and adequacy of the innovation are executed via reducing the weight at the EON stage [14]. The decentralized device accepts the primary potential related to security. Right now, the much less essential information, for example, symbols and pictures, are deposited with outside carrier providers. This layout takes into attention an extensive scope of alternatives to be actualized, that are exhibited at the "Solutions" page.

d) Privacy leakage:

The blockchain is specially susceptible to transactional privateness leakage because of the truth that the information and balances of all public keys are seen to all of us within side the community. The proposed answers for conducting anonymity in blockchains may be substantially categorized into blending answer and nameless answer. Mixing is a carrier that gives anonymity with the aid of using moving property from numerous information promises to diverse yield addresses. Anonymous is a carrier which unlinks the fee origins for a transaction to save transaction graph evaluation as mentioned in [15].

e) Selfish mining:

Selfish mining is every other venture confronted with the aid of using blockchain. A block is at risk of dishonest if a small part of hashing energy is used. In egocentric mining, the miners hold the mined blocks without broadcasting to the community and create a personal department which receives broadcast simplest after positive necessities are met. In this case, sincere miners waste quite a few time and sources whilst the personal chain is mined with the aid of using egocentric miners.

XI. Applications of Blockchain Technology

A. Governance

Governments throughout years are entrusted with managing and holding official records of both citizens and enterprises. Blockchain-enabled applications can change the way governments at local or state level operate by disintermediating transactions and record keeping. The accountability, automation, and safety that blockchain offers for handling public records could eventually obstruct corruption and make government services more efficient. In particular, blockchain could serve as a secure communication platform for integrating physical, social, and business infrastructures in a smart city context (Ibba et al., 2017; Jaffe et al., 2017; Biswas and Muthukkumarasamy, 2016; Sharma et al., 2017). Blockchain governance aims at providing the same services that are offered by the state and its corresponding public authorities in a decentralized and efficient way while maintaining the same validity. Examples of such services include registration or legal documents, attestation, identification, marriage contracts, taxes and voting (Swan, 2015).[10]

B. Healthcare sector

Blockchain technology could play a pivotal role in the healthcare industry with several applications in areas like public healthcare management, longitudinal healthcare records, automated health claims adjudication, online patient access, sharing patients' medical data, user-oriented medical research, drug counterfeiting, clinical trial, and precision medicine. A blockchain system for (Electronic Health Record) EHRs could be seen as a protocol through which users may access and maintain their health data that simultaneously guarantees security and privacy.[10]

C. Business Applications

Blockchain has become a significant source of disruptive innovations in business management through improving, optimizing, and automating business processes (Tapscott and Tapscott, 2017; Bogner et al., 2016; Ying et al., 2018). Many e-business models based on IoT and blockchain are emerging. One example can be found in Zhang and Wen (2015) where authors propose a business model in which transactions between devices are performed using SCs on a blockchain-based distributed database.[10]

D. Copyright Protection

The development of the Internet have been accompanied by copyright issues regularly. From peer-to-peer file-sharing services, such as photographs on the Web, copyrights have not always been respected [16]. From the perspective of a file holder, copyrights are often ignored or under some attacks. Therefore, unauthorized (also illegal) file-sharing and use of copyrighted content remains a significant problem. Now, blockchain technology has brought some light to this issue. Blockchain is a decentralized, distributed digital ledger of records [17]. Considering that a file is duplicated thousands of times across the network, this network is designed to regularly update and reconcile all the copies so that all records are consistent. No single computer or organization is responsible for the blockchain. The property of no central storage location makes it almost impossible to manipulate or corrupt.[9]

E. Cryptocurrency

One of the most active areas of the blockchain is in the financial sector, especially in the field of cryptocurrency. Since the advent of the first carrier bitcoin in the blockchain [18], various cryptocurrencies have emerged. In addition to being used in the field of cryptocurrencies, the blockchain is increasingly being used in financial services, including stock exchanges, cross-border payments, repurchase agreements, and digital identities. Utilizing the nature of the blockchain's distributed transaction ledger, the Bank of England Santander [19] used the technology provided by the payment protocol and exchange network based on Ripple to transfer payments in real time through a mobile application. [9]

XII. Future of Blockchain Technology

The early adopters are financial services other sectors will definitely adopt this technology. The integration of Blockchain with AI will make Blockchain more secure and platform user-friendly. Career opportunities in this domain are growing to increase at an alarming rate. Integration with new-age technology like IoT will help in building secure infrastructure. Enterprise Blockchain will continue to mature and develop, leading to high job prospects and good pay. [7]

XIII .Conclusion

Blockchain have received much interest worldwide. Blockchain, also known as distributed ledger technology, is a digital database managed by several different computers rather than a single central server. The different computers are called nodes and are all randomly connected. It's a magazine that is practically difficult to produce. It is extremely considerate and authoritative for its decentralized setup and peer-to-peer identity. However, Bitcoin protects numerous types of research related to the blockchain. Remembering that blockchain and bitcoin are not a similar object. In this article, we have examined the general concepts of blockchain technology, which consists of basic definitions, functions, key concepts, advantages, limitations and consensus algorithms, as well as security challenges and future work. In the future, like any new innovation, blockchain is an originally disruptive term and could eventually help improve a superior biological community that embraces both the old and old method. Innovative invention.

XIV. REFERENCES

[1] J.Garay, A. Kiayias, and N. Leonardos, The Bitcoin Backbone Protocol: Analysis and Applications, pp. 281–310, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[2] A.Gervais, G. O. Karame, V. Capkun, and S. Capkun, ―Is bitcoin a decentralized currency?,‖ IEEE Security Privacy, vol. 12, pp. 54–60, May 2014

[3] S.Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Feb. 24, 2013. (http://bitcoin.org/ bitcoin.pdf).

[4] Li, Lun, Jiqiang Liu, Lichen Cheng, ShuoQiu, Wei Wang, Xiangliang Zhang, and Zonghua Zhang. "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles." (2018).

[5] https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/#:~:text=A%20consensus%20algorithm%20is%20a,state%20of%20the%20distributed%20ledger.

[6] Deepak Sukheja,Prteek Sharma,Sachin Chirgaiya "Blockchain Technology: A Comprehensive Survey".

[7] https://www.blockchain-council.org/blockchain/5-key-challenges-for-blockchain-adoption-in-2020/

[8] Sandeep Kumar,Abhay Kumar,Vanita Verma, "A Survey Paper On Blockchain Technology, Challenges and Opportunities". International Journal of Computer Trends and Technology (IJCTT) - Volume 67 Issue 4 – April 2019

[9] Wubing Chen, Zhiying Xu, Shuyu Shi, Yang Zhao, Jun Zhao,"A Survey of Blockchain Applications in Different Domains".

[10] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis,"A systematic literature review of blockchain-based applications: Current status, classification and open issues"

[11] https://www.ibm.com/topics/benefits-of-blockchain#:~:text=Blockchain%20increases%20trust%2C%20security%2C%20transparency,cost%20savings%20with%20new%20efficiencies.

[12] Aste, Tomaso, Paolo Tasca, and Tiziana Di Matteo. "Blockchain technologies: The foreseeable impact on society and industry." computer 50, no. 9 (2017): 18-28.

[13] Kshetri, Nir, and Jeffrey Voas. "Blockchain-Enabled E-Voting." IEEE Software 35, no. 4 (2018): 95-99.

[14] Kotobi, Khashayar, and Sven G. Bilen. "Secure Blockchains for Dynamic Spectrum Access: A Decentralized Database in Moving Cognitive Radio Networks Enhances Security and User Access." IEEE Vehicular Technology Magazine 13, no. 1 (2018): 32-39.

[15] Z.Zheng, S. Xie, H. Dai, X. Chen and H. Wang, An overview of blockchain technology:Architecture, consensus, and future trends, in Big Data (BigData Congress), 2017 IEEEInternational Congress on, IEEE, 2017, 557–564.

[16] https://abovethelaw.com/2018/02/how-blockchain-just-may-transform-online-copyright-pr

[17] https://www.diyphotography.net/blockchain-copyright-protection-a-viable-solution-to-prove-ownership-of-creative-works/

[18] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Whitepaper, 2009.

[19] Santander becomes first UK bank to introduce blockchain technology for international payments with the launch of a new app https://www.santander.com/csgs/Satellite?appID=santander.wc.CFWCSancomQP01&c=GSNoticia&canal=CSCORP&cid=1278712674240&empr=CFWCSancomQP01&leng=en_GB&pagename=CFWCSancomQP01%2FGSNoticia%2FCFQP01_GSNoticiaDetalleMultimedia_PT18