Blockchain in Cryptocurrency & its Use In Economy: A Review

*Mohammad Suhail[1], Dr. Bhavya Alankar[2], Dr. Harleen Kaur[3]
[1] Department of Computer Science and Engineering
Jamia Hamdard University, New Delhi India, 110062
[1*]sohailnizamkhan0@gamil.com
[2] Department of Computer Science and Engineering
Jamia Hamdard University, New Delhi India, 110062[2]
[2]balankar@jamiahamdard.ac.in
[3] Department of Computer Science and Engineering
Jamia Hamdard University, New Delhi India, 110062
[3]harleen@jamiahamdard.ac.in

Abstract:
The popularity of Bitcoin and other well-known cryptocurrencies has increased over the past several years. This cryptocurrency, which is widely recognized as both a sort of digital cash and actual money, is purchased and sold over the blockchain system.The blockchain technology used to use cryptocurrencies is being questioned by the financial sector, political stakeholders, and individual investors. The sector has been dramatically disrupted by cryptocurrencies since the introduction of bitcoin in 2009. Future currencies that might displace the ones used today include cryptocurrencies. Users have become interested in interest, while many of them are uninformed of the potential, obstacles, and problems it may present in the future. Hidden knowledge is still scarce and expanding. By offering a crucial framework and viewpoint for the users and the education industry. This essay will examine the possibilities of cryptocurrencies, including their technological security, low transaction costs, and huge financial profits, in order to offer crucial advice and consumer perspectives. The main topics of this article include laws and regulations, excessive power use, accidents and explosions, and network attacks. This essay will meticulously investigate the operation of cryptocurrencies and some of their possible applications

Keywords:
Cryptocurrency, Financial Activity, Blockchain technology, cryptocurrency mines, Investments, Cryptocurrency online trading, Cash flow, How to create cryptography.

1.Introduction

The economic and technical fields have advanced significantly in recent years. One of the most amazing technological advancements in the field of economics is the creation of cryptocurrencies, or virtual money, in the internet environment. As the global economy grows increasingly internationally linked, there is a growing need for financial transactions that are quicker, more comfortable, and more safe. As a result, we need a safe and practical payment method for bank customers. A payment system is a set of procedures for the transfer of funds through national and international value-added transactions between individuals and financial institutions. The Bank of Indonesia categorizes payment system instruments into two groups: financial and non-financial, in its capacity as a payment system officer. For instance, payment mechanisms are so constrained that they are unable to meet the needs of the general public.

A cryptocurrency is a type of digital or virtual currency that employs encryption and mapping to protect it, making it almost impossible to copy or forge. Blockchain technology, a distributed ledger that is compelled onto a separate computer network, powers the majority of cryptocurrencies. Because hidden money frequently aren't issued by a centralized entity, they are shielded from government action and spending. Cryptocurrencies are digital or virtual currency supported by a cryptographic technology. Without the assistance of affiliates from other parties, they allow secure online transactions. Sharp curve encryption, public and private key pairings, and

hashing operations are just a few of the encryption techniques and protocols that are referred to as "crypto" in this context.

Cryptocurrencies may be mined or purchased on exchanges that deal in them. Cryptocurrency transactions are not supported by all eCommerce platforms. Truth be told, not even the most well-known cryptocurrencies like Bitcoin are used for commerce. But as the number of cryptocurrencies has grown, so has their acceptance as trading tools. They are occasionally used for border transfers as well.
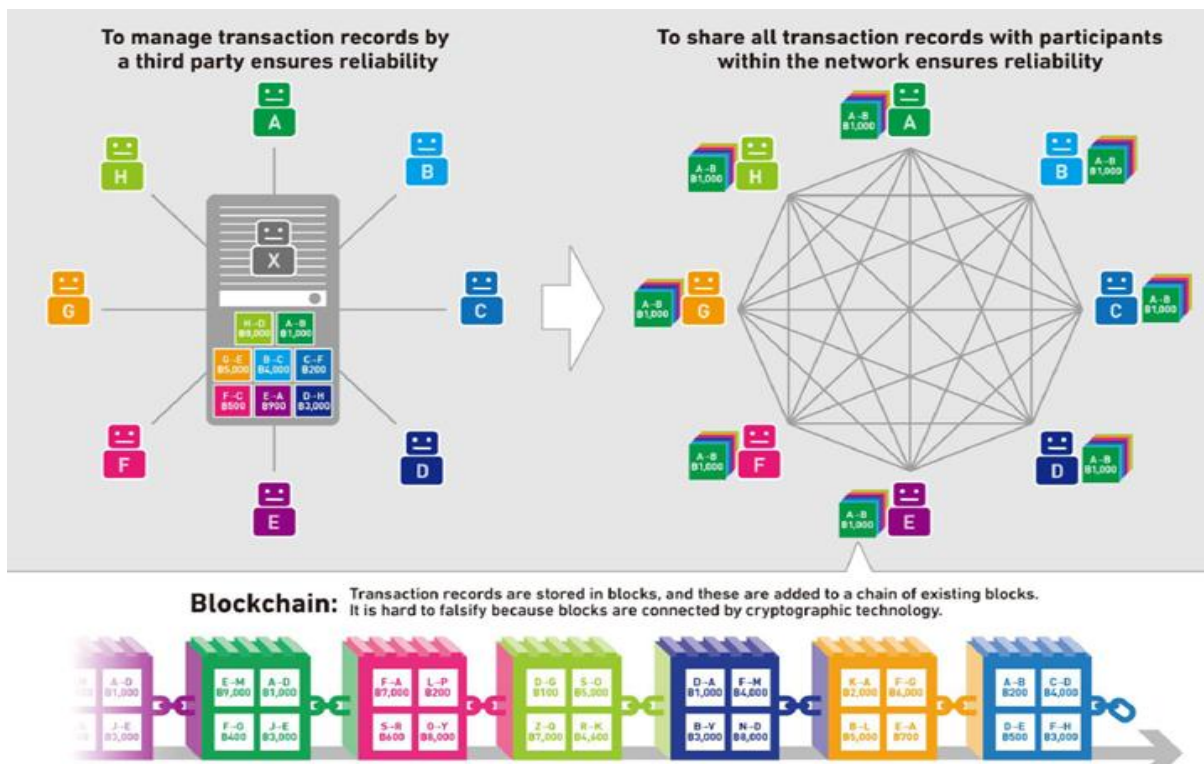
The adoption and use of Bitcoin and other cryptocurrencies depend on blockchain technology. A blockchain is simply a network of interconnected blocks or an electronic book, as its name suggests. Each block contains a set of transactions that have been confirmed by all users of the network. Building transaction histories is difficult since each node must confirm each newly created block before it can be verified.

Bitcoin is a well-liked and valuable cryptocurrency. In 2008, Satoshi Nakamoto, a mysterious creator, released a white paper presenting it to the general world. There are currently thousands of coins accessible.

2. Latest Literature Reviews:

Blockchain is a platform for data management and commerce that was first developed utilizing the virtual currency Bitcoin. Since the initial introduction of the concept in 2008, fascination with Blockchain technology has increased. The main characteristics of this technology are what have sparked interest in it., which enable security, privacy, and data integrity independent of any third-party institution that supervises transactions. offers fascinating research opportunities, especially in light of the challenges and limitations given by technology. Blockchain is a platform for social networking that protects the accuracy of transaction data. The technology that makes use of Bitcoin is more known[1]

A public activity log called Blockchain is a component of the Bitcoin global electronic cash system. One of the most important features of Bitcoin is the maintenance of a monetary value independent of any group or political authorities. The Bitcoin network has a growing quantity of users and transactions[2]. Furthermore, exchange markets frequently see conversions to traditional


Blockchain: Transaction records are stored in blocks, and these are added to a chain of existing blocks. It is hard to falsify because blocks are connected by cryptographic technology.

currencies like KRW, EUR, and USD. As a result, many businesses have shown interest in Bitcoin, the most popular digital money based on Blockchain technology.[3].

The public-key infrastructural (PKI) technique is used by Bitcoin.[4]. Then, The current block is connected to a prior block that was written. On the "nodes," or disk storage, of users, all blocks are preserved, which also houses information on all previous transactions. All nodes keep track of every Bitcoin transaction and confirm that new transactions made using older blocks are accurate[5]. Nodes are rewarded for confirming that transactions are correct. This tactic is known as mining, Moreover, Proof-of-Work, is among the core concepts behind the Blockchain system, underpins it[6]. Once all of the verifications are successful, a consensus is formed. Each block is connected to the others and aligned with a single continuous chain. These blocks reflect the Bitcoin social networking site on the Blockchain[7].

An separate Bitcoin management system called Blockchain was created to allow for cashouts to other Bitcoin users. This process can make it possible to create a public record of every Bitcoin transaction ever made without using an unrelated party[8].The benefit of Cryptocurrency is that once data has been approved by all nodes, it cannot be modified or withdrawn from the public registry. Because of this, blockchain is recognized for its data security and integrity features. There are further uses for blockchain technology. Peer-to-peer data exchange and digital contracts using cloud services, for instance, may both be developed. the validity of other services and apps using it, the resilience of the blockchain process, and the quality of the data[9].

The blockchain technology also has acknowledged limitations and technical issues. You may learn more about blockchain technology and its limitations in the future by reading the following list of seven technological hurdles and constraints[10]:

• **Input:**The potential troublesome transactions per second (tps) on the Bitcoin network has increased to 7. This is enhanced by the processing networks for VISA (2,000 tps) and Twitter (5,000 tps). When Blockchain transactions reach a certain level reaches the same levels, Blockchain network emigration must be addressed.[11].

• **Delay:**One transaction may be processed in around ten minutes, which is long enough to provide Bitcoin block protection. Because the cost of the defense must be larger than the cost of the assault, effective security involves a lot of time on the defensive. The effect of several productive investments is a double expense[12].Bitcoin prevents revenue duplication by securing each transaction uploaded to the blockchain and guaranteeing that inputs have never been used before[13]. As a result, delays are turning into a major problem for blockchain. It need to be feasible to fast authenticate and block while maintaining security. The ability to accomplish tasks quickly, like those in VISA, is a key advantage over Blockchain. As a result, delays are turning into a major problem for blockchain. It need to be feasible to fast authenticate and block while maintaining security. When compared to Blockchain, activities like those in VISA may be accomplished in a matter of seconds[14].

• Size and bandwidth: The Blockchain for the Bitcoin network presently consumes more than 50,000MB (February 2016). Once the result hits Blockchain has the potential to expand by 214PB annually at VISA levels. The Bitcoin community believes that a single transaction ought to be 1MB in size and created every 10 minutes[15]. The number of transactions that may be executed is therefore capped at 500 sales on average every block. Size and bandwidth concerns need to be fixed if more transactions must be processed via blockchain.[16]
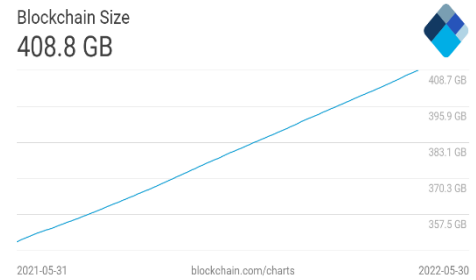
• Waste resources: An tremendous amount of energy ($ 15 million per day) is squandered during bitcoin mining. Waste from the Proof-of-Work endeavor is Bitcoin[17].

• Version: Another problem arises when chains are separated for administrative or transformational reasons[18].
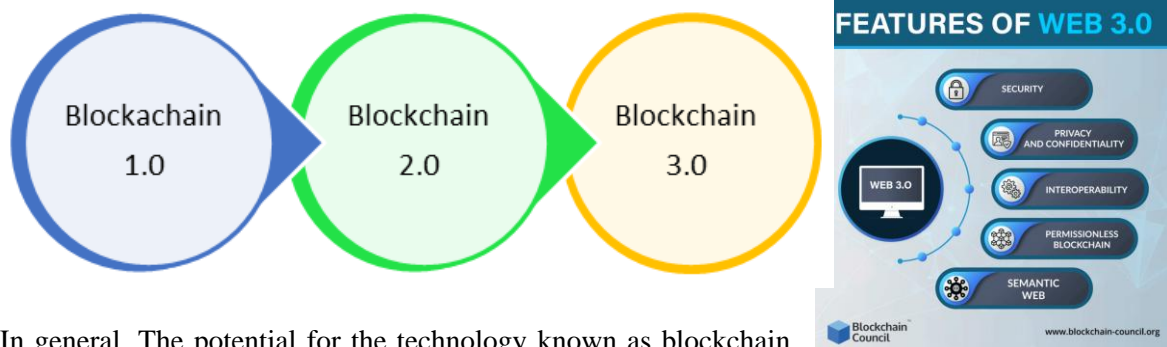
In general, The potential for the technology known as blockchain to transform how daily transactions are carried out. Blockchain technology may be used in a variety of industries where various types of transactions are done, not just in the realm of cryptocurrency[19]. Despite the fact that there are already technical problems and barriers with blockchain, future research in the area of blockchain applications is quite promising. An assortment of exciting issues and questions are presented by the characteristics of anonymity, data integrity, and security, which call for careful examination and solution. In order to satisfy future needs, scalability issues also need to be addressed. It is crucial to compile all pertinent studies in order to recognize and comprehend the present state of research underway on blockchain. It is still possible to observe in Blockchain which problems and inquiries have received solutions in addition to the ones that have not.

3. Technology Used:

Blockchain technology is a method that keeps track of all network transactions in a digital ledger. The term "blockchain" describes a sequence of data made up of each activity, which is referred to as a "block." This is the basic idea underlying blockchain technology, despite the fact that there are several explanations accessible online[20].
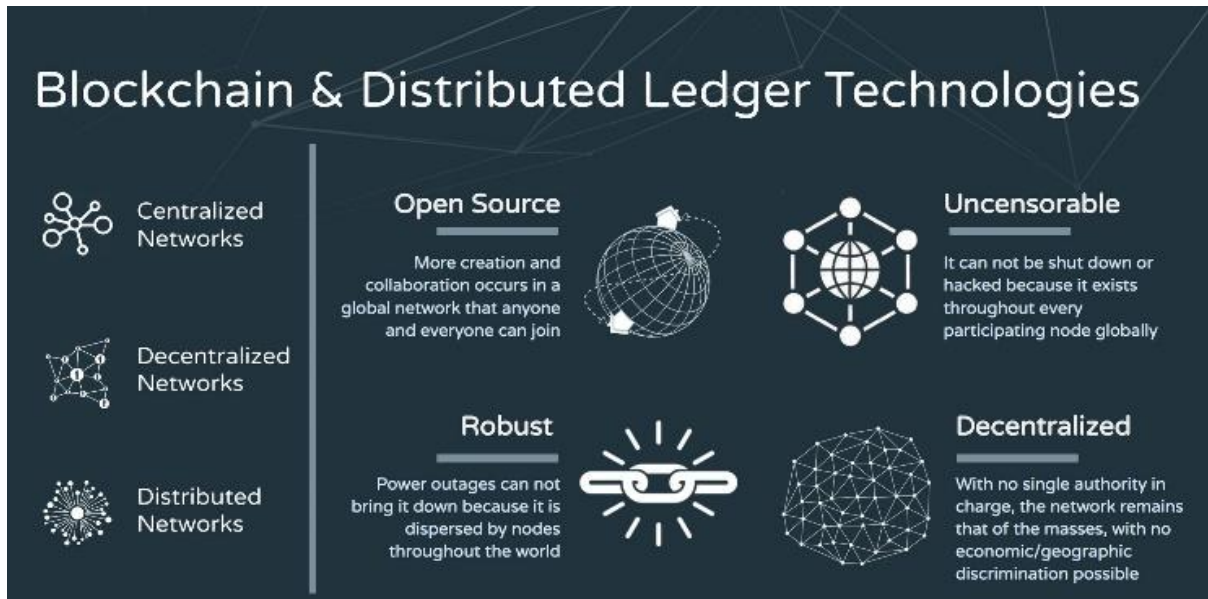
The blockchain technology used in cryptocurrency:
Blockchain technology is based on a principle that is not new, despite the fact that it may only appear to be one idea. There are other networks that function in a way that is comparable to blockchain.Furthermore, it's important to understand that blockchain technology was created in 1991, even if it wasn't publicly available as a part of the Bitcoin platform until 2008. As a result, it is focused only on Bitcoin and not all cryptocurrencies[21].
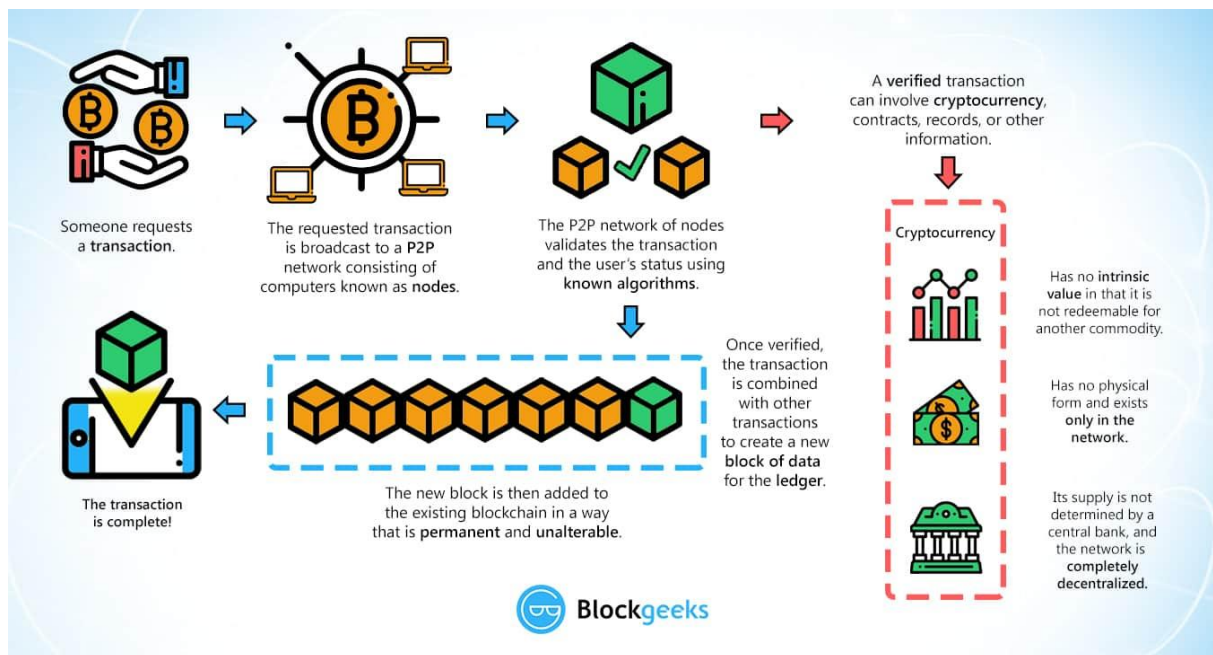
. Accessible: The blockchain is linked to a virtual world, as opposed to conventional systems where you need the approval of regulatory organizations, like a bank, meaning that anybody may use technology to conduct commerce. It bursts more frequently than other peer networks because of its accessibility.
The blockchain is moreover always available. As a result, cryptocurrency traders and investors may profit without having to worry about time constraints.
. Affordability: Additionally, compared to traditional networks, transaction fees on blockchain social networks are lower. This is because there are several stages to the technique.
. Secure: When a blockchain transaction record is created, a unique key is also created. To update or change anything in that particular record, you need a signature that is relevant to your job. In

other words, every document or file has a password. This particular blockchain feature reduces the possibility of interference.

. Default: It is typical for all parties to accept a set of rules, occasionally referred to as a contract, in order to prevent misuse. It takes a lot longer to set up even with the help of modern technology, even if it offers everyone involved a sense of security. Blockchain technology, which makes it possible to immediately create and implement smart contracts, takes this concept to a whole new level.

. Accuracy: Even if this wasn't the case when it was first introduced, blockchain technology does not involve people. A computer network validates every job request that is posted in a public place. As a result, there is little possibility for human error, leading to reliable records of what is being done[22].

. Anonymity: Despite the fact that every transaction on the blockchain reveals the wallet addresses of all parties involved, the owners of each wallet address are unknown. Because the wallet address is visible, there is some exposure, but there is also some anonymity because the wallet address hides the owner's identity.

How does blockchain technology work?

Although blockchain technology may seem to function in strange ways, its architecture and design are actually far more straightforward than you would think. Here is an illustration of how it functions:

.A request to purchase or sell cryptocurrencies is made by each individual.

.The request is received by the "nodes" of a computer network.

.When an application joins a blockchain, thousands of computers will compete for the chance to authenticate what is being done. In reality, this is how cryptocurrency miners work [23].

.In exchange for their work, or more particularly the accounting tools they used during the whole verification

process, the computer or miner, also known as a blockchain, who successfully completes and validates the operation gets compensated with bitcoin.

. Following transaction validation, it will be added to a previous crypto operation's chain and added to the blockchain.
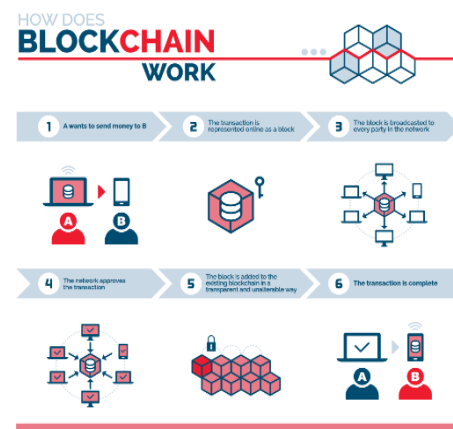
4.BlockChain Process in Cryptocurrency:

Simple startups:

The blockchain idea was first presented in 1991 as part of a research effort, years before its first big debut, which happened in 2009 in the case of Bitcoin. Since then, a variety of anonymous currencies, financial apps (DeFi), static tokens (NFTs), and smart contracts have been developed, further increasing the usage of blockchain technology.

.Each action is documented as a separate "block" of data.

Each block has connections to the ones that came before and after it. To guarantee accurate time and order of events and to prevent any one block from being changed or put in between the other two, blocks are securely linked to one another. The activity is connected to a distributed layout system called a non-volatile series. The whole blockchain is guaranteed by the pre-block authentication of each succeeding block. The blockchain becomes impervious to interruption as a result, offering you the crucial power of consistency[24].

. Dual-use issues with cryptocurrencies and the necessity for a blockchain

In earlier attempts to create a cryptocurrency, such as Nick Szabo's BitGold, double spending was a concern. When a user attempts to use the same cryptocurrency twice, double duplication happens. The blockchain totally solves the issue of double-spending with a flexible, adaptable manual.[25].

## POSSIBLE BLOCKCHAIN NETWORK TYPES:

1.Open Blockchain:

Everybody may use these blockchains. This issue exists in the blockchains used for cryptocurrencies like Solana, Ethereum, and others. Public blockchains require a significant amount of processing power [26].

2. Private blockchains:
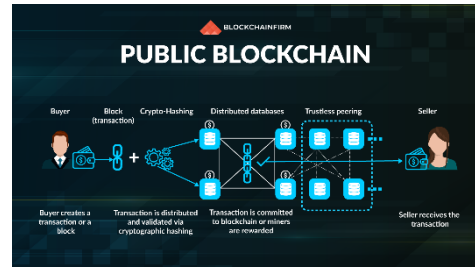
These blockchains are accessible to everyone. This issue exists in the blockchains used for cryptocurrencies like Solana, Ethereum, and others. Public blockchains require a significant amount of processing power[27].
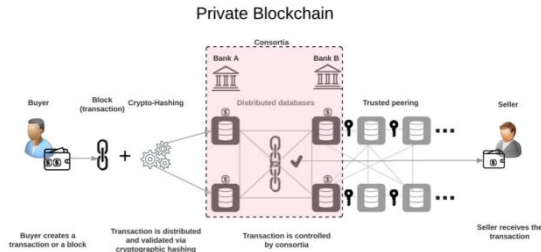
3. Approved Blockchain:

When creating a private blockchain, businesses usually build an approved blockchain network. This limits who can use the network and how much they may be charged. Prior to participating, participants must get an invitation or authorization[28].

4. Consortium Blockchain:

Storage on blockchains may be distributed across several businesses. Who is permitted to submit transactions or access data is within the jurisdiction of these entities. Participants who are interested must ask permission and get authorisation.[29].
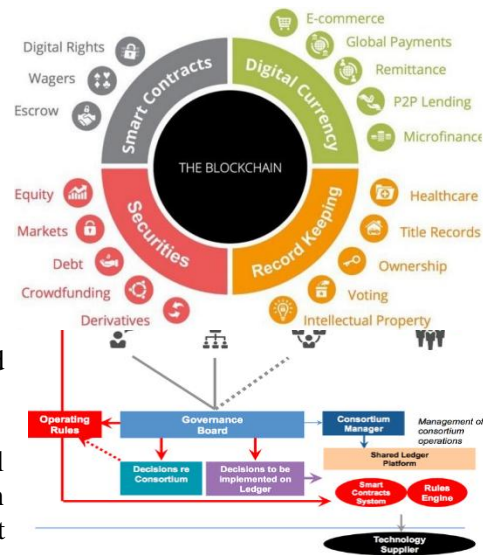
Benefits of Cryptocurrency:

Bitcoin transfers from peer to peer have minimal transaction costs and do not require a central server. In state-allocated systems, conversion costs are also not assessed. Quick payments are made, and fraud risk is not taken into account. Blockchain-based transactions are transparent, anonymous, and irrevocable.Additionally, cryptocurrency offers unrestricted access to anybody in the globe, free from interference from any central authority[30].

A few advantages of blockchain technology:

1.Medium-sized financial systems are simple to use but have constraints.. It is possible to have problems like disparities and bad budgeting. Customers may eventually suffer as a result of all of this.The system is incredibly trustworthy and safe thanks to blockchain technology. Blockchain technology is the business development tool of the future. Every dollar invested in these collaborative technologies will see a reasonable return since they might improve business processes and increase confidence[31].
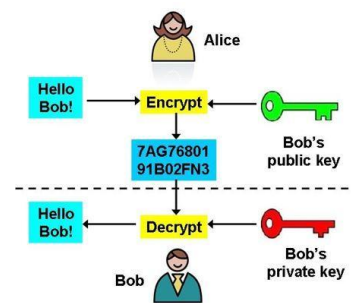
2.Blockchain follows national boundaries, and individuals, not centralized groups like the government, are in charge of making choices. Currently, the financial system is governed by centralized authorities, who must be trusted and whose rules must be followed by everyone. However, these crucial elements may be used; we see several examples of the financial industry acting unethically in order to generate money.

3.All transactions are transparent and anonymous thanks to blockchain technology. Therefore, there is no exploitation at all. Furthermore, because Blockchain transaction history is still dispersed all over a computer chain, there cannot be a single point of failure. By employing cryptographic hashing to encrypt the data and maintain the integrity of the blockchain, blockchain technology prevents data tampering.

Users have total control over transactions using cryptocurrency's blockchain technology and don't have to worry about them being blocked or handled incorrectly by any centralized body of power. Consequently, blockchain technology will grow more effective as more companies and people adopt it[32].
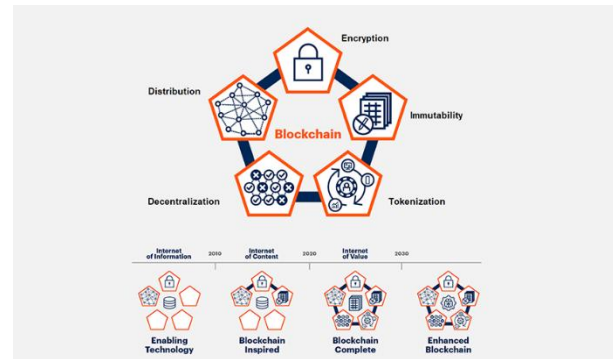
5. Challenges and Future Work:

Having Centralized Systems Can Be Difficult:

Everyone utilized intermediary resources prior to the creation of Bitcoin and BitTorrent. In centralized systems, all data are kept in one location, and only that data center should be used. Google is a good illustration of this kind of a structure.

When we conduct a search for something on Google, the server processes our request and provides the relevant data. Another illustration is the financial institutions who are in charge of all our disposable funds and have us to get in touch with them or visit them anytime we need to submit a payment[33].

Intermediate systems are easily attacked by hackers. If software development is necessary in the central data center, the entire process should be put on hold. All internal data would be at danger if a data centerwere to sustain intentional harm. If the medium-sized business collapses, nobody will have access to the data until it returns to life.

Structure of peer-to-peer networks:

All nodes in a peer-to-peer network that supports blockchain are connected to one another. A main node is any computer that takes information, processes it, and outputs the outcome.

The peer-to-peer network is most typically utilized with flow. When employing a client-server strategy, the download process should ideally slow down and be entirely dependent on the server. However, with a system that works via peer-to-peer, there are still enough of peers for us to obtain files from regardless of whether one network isn't functioning properly. Additionally, the concept of fusing peer-to-peer networks with payment systems marks an important turning point within the financial sector.
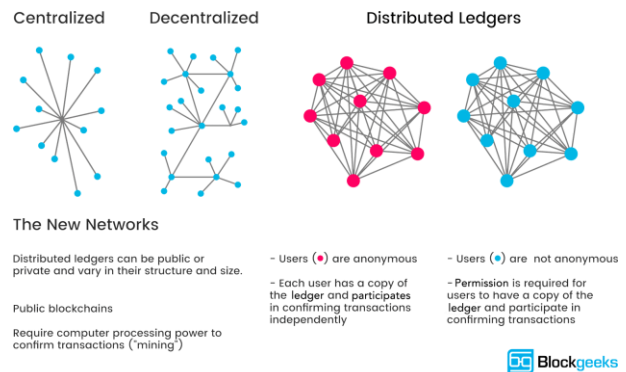
Cryptocurrencies employ the same nodes and network technology, and there is no central authority. The Proof of Work consensus algorithm, utilized by cryptocurrencies like Ethereum and Bitcoin, accords equal privileges to all nodes. However, their level of participation and activity may vary. The network uses the law of gossip to inform its neighbors when a transaction takes place. Until the complete location is made public, speculations and information continue to spread.

The architecture of this system has the drawback of not being highly quantitative. Next-generation currencies have a leader-based consensus technique to overcome this, in which nodes choose leader notes (also known as Supernodes).Supernodes are in charge of the network's overall viability and compatibility. Although these cryptocurrencies are quick, not many people utilize them. Cardano, among Neo's account, and EOS are further examples[34].

What is the Consensus approach to Blockchain?

In a geographically dispersed network like Blockchain, the consensus mechanism refers to the methods that assist technology in achieving trust, confidence, agreement, and security. The blockchain and cryptocurrency technologies work thanks to two different types of consensus. These two sorts of techniques are Proof of Service (PoW) and Proof of Proof (PoS). The PoS-compliant approach is especially used for cryptocurrencies like Bitcoin or Litecoin, however this device is more energy-efficient and has a longer processing time. PoS is a low-cost, low-power substitute for PoW with equivalent applications in the blockchain sector.

6. Conclusion:

Blockchain technology's application to Cryptocurrencies have the power to change a number of sectors. Through geographic clustering and cryptographic hashing, it creates a clear and unchangeable history for digital assets. Blockchain technology and cryptocurrency are interconnected. The independence of cryptocurrencies from any one central entity or individual is their strongest attribute.

The use of blockchain technology in Bitcoin has increased dramatically since it was first introduced in 2008. Bitcoin transactions are peer-to-peer because to the cheap transaction fees. In basic financial systems, several weaknesses and constraints are easy to take advantage of. Blockchain technology enhances the system's reliability and security.

With its safe, global, and trustless methods of value exchange, this invention has completely changed the financial environment and opened the door for future advancements in decentralized financial services and digital assets. With applications across many industries, blockchain's influence goes beyond cryptocurrencies, highlighting its potential to fundamentally alter how we store, move, and organize information as well as possessions in the digital age.

7. References:
References

[1] Huaqun Guo and Xingjie Yu, "A survey on blockchain technology and its security," *Science direct,* June 2022.

[2] ADAM HAYES, JEFREDA R. BROWN and SUZANNE KVILHAUG, "Investopedia," June 24 2022. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp.

[3] Jesse Yli-Huumo and Deokyoon Ko, "Where Is Current Research on Blockchain Technology?—A Systematic Review," *PLoS One,* 2016.

[4] T. Contributo, "Data security and privacy," 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/public-key.

[5] Simplilearn, "Simplilearn - Online Certification Training Course Provider," 13 july Jul 13, 2022. [Online]. Available: https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology.

[6] FranCasinoa, Thomas K.Dasaklis and bConstantinosPatsakisa, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics,* March 2019.

[7] S. Kaur and Sheetal Chaturvedi, "Blockchain Techniques for Internet of Things Security," *hindawi,* 2021 .

[8] Marco Iansiti and Karim R. Lakhani, "The Truth About Blockchain," january-february January–February 2017. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain.

[9] M. K. Pratt, "Top 10 benefits of blockchain technology for business," *digital transformation,* 02 june 2021.

[10] M. Brown, "Digital transformation," *challenges with blockchain adoption and how to avoid them,* 27 May 2021.

[11] S. S. Bagga, "Report of Blockcahin," SCRIBD, RAJASTHAN, (2017-2018).

[12] Jesse Yli-Huumo, Deokyoon Ko and Sujin Choi, "Where Is Current Research on Blockchain Technology?," *PLoS One,* 2016 Oct 3.

[13] Jesse Yli-Huumo and Sooyong Park, "Where Is Current Research on Blockchain Technology?," *PLoS One ,* 2016 Oct 3.

[14] K. L., "The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed," *TDS ,* Jan 30, 2019.

[15] Gurinder Singh, Vikas Garg and Pooja Tiwari, "Introduction to Blockchain Technology," *RESEARCH GATE,* April 2021.

[16] K. L., "The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed," *TDS (Towards Data Science),* Jan 30, 2019.

[17] John Schmidt and Farran powell, "forbesAdvisor," forbes, 18 May 2022. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/bitcoins-energy-usage-explained/.

[18] Bojana Koteska and Anastas Mishev, "Blockchain Implementation Quality Challenges: A Literature Review," *RESEARCHGATE,* September 2017.

[19] K. Little, "What Is Blockchain and How Does It Work?," *NEXTADVISOR,* May 3, 2022.

[20] N. Darlington, "blockgeeks," Navigation, 25th November 2021. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/.

[21] Simplilearn, "What is Blockchain Technology? How Does Blockchain Work?," 2022.

[22] Marco Iansiti and Karim R. Lakhani, *The Truth About Blockchain,* HARVARD BUSINESS REVIEW, January–February 2017.

[23] Z. Church, "Mitsloan," 25 May 2017. [Online]. Available: https://mitsloan.mit.edu/ideas-made-to-matter/blockchain-explained.

[24] R. Sheldon, "WhatIs.com," 09 August 2021. [Online]. Available: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology.

[25] S. Saurel, "medium.com," 08 November 2019. [Online]. Available: https://medium.com/the-capital/how-does-blockchain-bitcoin-protect-itself-against-the-double-spending-problem-d49ad76a0e92.

[26] A. Chaturvedi, "Business Today," 05 May 2022. [Online]. Available: https://www.businesstoday.in/crypto/story/what-is-blockchain-how-is-it-used-in-cryptocurrency-332411-2022-05-05.

[27] FranCasino, Thomas K.Dasaklis and ConstantinosPatsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *sciencedirect,* March 2019.

[28] J. FRANKENFIELD, "investopedia," 24 january 2022. [Online]. Available: https://www.investopedia.com/terms/p/permissioned-blockchains.asp.

[29] Ajay Kumar Shrestha, Julita Vassileva and Ralph Deters, "A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives," *Frontiers,* 22 October 2020.

[30] S. Arora, "simplilearn," 19 july 2022. [Online]. Available: https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-cryptocurrency.

[31] D. Tapscott and Alex Tapscott, "Harvard Business Review Home," 10 May 2016. [Online]. Available: https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services.

[32] Prof. Dr. Robby HOUBEN and Alexander SNYERS, "Cryptocurrencies and blockchain," europarl, 2018.

[33] 101blockchains, "101blockchains," 29 May 2021. [Online]. Available: https://101blockchains.com/decentralized-vs-centralized/.

[34] A. Ohri, "jigsawacademy," 05 january 2021. [Online]. Available: https://www.jigsawacademy.com/blogs/product-management/peer-to-peer-architecture/.