International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Surveying the Landscape: An In-Depth Analysis of Blockchain Technologies

**B. Ch. V. Ajay Babu[1], R. Jyoshana[2], K. Teresa[3]**

[1,2,3]Student, Computer Science Engineering, KL University

**Abstact:**
Blockchain technology has emerged as a transformative force with far-reaching implications across various industries. This survey paper endeavors to provide a comprehensive analysis of the current landscape of blockchain technologies. Delving into the intricate details of decentralized ledgers, consensus mechanisms, and smart contracts, our exploration aims to offer readers a nuanced understanding of the multifaceted world of blockchain. The survey encompasses an examination of key applications, challenges, and emerging trends, providing insights into the diverse use cases and potential future developments. Through an in-depth analysis, this paper is all about blockchain.

**Keywords:** Blockchain technology, Consensus Mechanisms, Smart Contracts, Decentralized Ledgers, Emerging Trends, Multifaceted blockchain, Blockchain Uses

## 1. Introduction:

The groundbreaking technology known as blockchain has attracted a lot of attention from a variety of businesses due to its potential to completely change how traditional record-keeping and trust systems operate. Fundamentally, a blockchain is a distributed, decentralized record that permits safe, open, and impenetrable transactions without requiring a central authority.

A chain of blocks, each containing a list of transactions, is the core idea of blockchain technology. An unchangeable and sequential record of transactions is produced by connecting these blocks using cryptographic hashes. Because it is decentralized, there is no single entity that can control the entire blockchain, which improves security and lowers the possibility of fraud.

a) Contribution to survey: Our work mainly contributes comparative study of consensus algorithms and Blockchain frameworks that are currently in use. In one paper, security threats and future possibilities are discussed. A lot of survey articles have been published recently that try to assess the Blockchain technology with a particular focus and in different levels of detail. Nevertheless, according to the analysis of the literature, no study has combined a discussion of consensus algorithms, security concerns, and in-depth details of several Blockchain iterations into a single survey report. We are driven to make a contribution with this in-depth analysis of Blockchain evolutions, architecture, consensus, and security in this article because of this lack of comprehensiveness.

b) Organization of survey: The survey is structured as follows: First, it covers background concepts to help readers better comprehend the main ideas of this article; then, it explores the properties of blockchain. This paper also focuses on the problems and difficulties with blockchain technology. Explains in detail the development and varieties of Blockchain technology. We examine current Blockchain Cryptocurrency systems and components, as well as smart contracts and Blockchain

applications in general. A thorough examination of current research developments and unresolved questions around blockchain security. This is in line with the open research questions that the literature evaluation revealed.

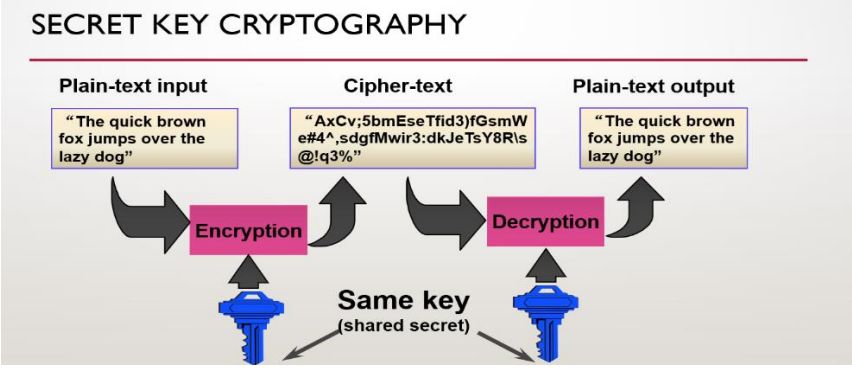
## 2. Background:

**Crypto System:** A cryptographic system's architecture consists of a number of parts and ideas intended to guarantee the authenticity, confidentiality, and integrity of data. Crypto System involves cryptography, Hash Function, Digital Signatures, Elliptic curves etc.

**Cryptography:** The activity and study of methods for protecting information and communication from adversaries is known as cryptography. Information is transformed using mathematical methods to render it unintelligible to unauthorized users. Ensuring information's confidentiality, integrity, authenticity, and occasionally non-repudiation are the main goals of cryptography.

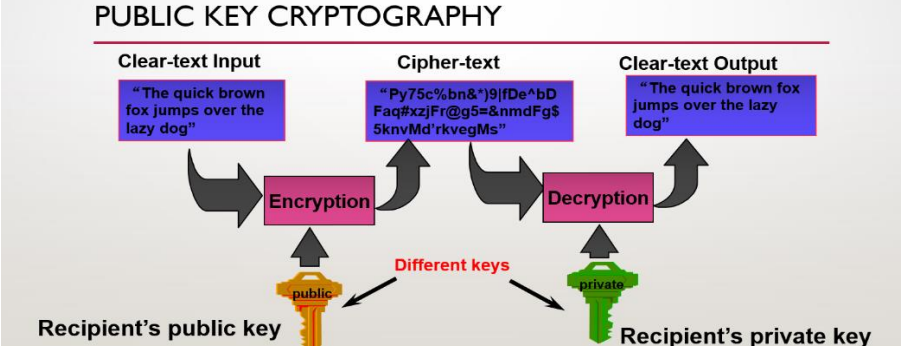
1. **Symmetric Cryptography:** The cryptographic technique known as symmetric-key cryptography or secret-key cryptography, uses a single secret key for both ciphertext decoding and plaintext encryption. With this method, the system's security depends on the communication parties maintaining the confidentiality of a shared secret key. Because symmetric cryptography is quick and effective, it can be used in many different contexts.

**Figure-1: Symmetric/Secret Cryptography**




2. **Asymmetric Cryptography:** Asymmetric key cryptography, commonly referred to as public key cryptography, is a cryptographic technique that employs a public key and a private key as a pair for secure communication. In asymmetric cryptography, the keys serve distinct functions as opposed to symmetric cryptography, which uses the same key for both encryption and decryption. The encryption process uses the public key, while the decryption process uses the private key. This technique addresses some of the major distribution issues with symmetric cryptography while also adding extra security.

**Figure-2: Asymmetric/Public Key Cryptography**



**Hashing:** The process of hashing is transforming input data, often known as a message or plaintext, into a fixed-length character string, usually a hexadecimal integer. The hash value or hash code is the result of this procedure. Due to the rapid and deterministic nature of hash functions, the same input will always result in the same hash output. Among the hashing properties are fixed output, irreversibility, determinism, and efficiency. The most widely used hash algorithm is SHA-256.

1. **SHA-256:** It belongs to the family of cryptographic hash algorithms known as SHA-2. The National Institute of Standards and Technology (NIST) published it in 2001 after the National Security Agency (NSA) designed it. Many different cryptographic systems and security applications employ SHA-256.Although SHA-256 is frequently used and regarded as secure, it's vital to remember that the world of cryptographic algorithms is always changing. With the increasing processing power over time, earlier hash algorithms could be more vulnerable to specific kinds of attacks. As a result, it's wise to keep up with developments in cryptographic research and, if required, switch to more secure algorithms on the advice of professionals.

**Digital Signatures:** A digital message, document, or transaction can have its origin, identity, and integrity verified using a digital signature, which is a cryptographic technique. It has the same function as a stamped seal or handwritten signature, but it's digital. To accomplish their objectives, digital signatures employ public-key cryptography, also referred to as asymmetric-key cryptography.

Working of Digital Signatures:

1. **Key Pair Generation**: A private key and matching public key are created by the entity seeking to create a digital signature. While the public key is distributed freely, the private key is kept secret and known only to the owner.
2. **Signing the Message**: The owner of the private key applies a mathematical operation to the message or document in order to create a digital signature. The result of this operation—usually a hash function—is the hash value, which is a fixed-length string of characters.
3. **Encrypting the Hash**: The digital signature is then created by encrypting the hash value using the private key. The encrypted hash cannot be simply copied or forged because it is specific to the message and private key used.
4. **Verification**: The encrypted hash can be decrypted by anyone with the public key, allowing them to validate the digital signature. They can then create a new hash value on the original message using the same hash function. The signature is legitimate if the newly generated hash and the decrypted hash match.

**Elliptic Curves**: The public-key cryptography system known as Elliptic Curve Cryptography (ECC) is founded on the study of elliptic curves over finite fields. Compared to other public-key cryptosystems, it offers strong security with comparatively shorter key lengths, which makes it especially suitable for resource-constrained environments like mobile devices and the Internet of Things (IoT). Digital signatures and secure communication protocols are just two of the many uses for ECC. ECC is widely used in many security protocols, such as secure messaging protocols, TLS/SSL for secure web communication, and cryptographic applications on devices with limited resources. However, since improper use or implementation flaws can affect a system's overall security, it is imperative to ensure the appropriate and secure implementation of ECC.

**Blockchain:** A blockchain is a distributed, decentralised digital ledger that securely and openly records transactions across several computers. The technology's structure—a chain of blocks, each containing a list of transactions—is where the term "blockchain" originates. In addition to being the foundation of cryptocurrencies like Bitcoin, this technology is being used in numerous other sectors to create transparent and impenetrable record-keeping systems.

Key features of blockchain:

1. **Decentralisation:** A blockchain runs on a peer-to-peer network of computers, or nodes, as opposed to conventional centralised databases. Because every node has a copy of the whole blockchain, decentralisation and resilience are encouraged.
2. **Blocks**: A sequence of blocks is created by grouping transactions into blocks and using a cryptographic hash to link each block to the one before it. The chronological sequence and integrity of the transactions are guaranteed by this linking.
3. **Consensus mechanism**: Nodes in a blockchain network have to concur on whether a transaction is valid and when to add it to the ledger. To reach consensus among nodes, a variety of consensus techniques are employed, including Proof of Work (PoW) and Proof of Stake (PoS).
4. **Cryptographic Hashing**: To ensure the integrity of the data in each block, cryptographic hash functions are employed. A traceable and secure record would be created if the data in a block were to change, as this would change its hash.
5. **Transparent and Immutable**: All network participants can see and access transactions on a blockchain. A block is almost impossible to remove or change once it is added to the chain, making the record unchangeable and impenetrable.
6. **Cryptocurrencies**: The most well-known use of blockchain technology is in digital currencies such as Ethereum and Bitcoin. The decentralisation and integrity of these virtual currencies are guaranteed by blockchain.
7. **Smart Contracts**: These self-executing contracts have their terms encoded directly into the code. They eliminate the need for middlemen by automatically enforcing and carrying out the terms of an agreement when certain requirements are satisfied.
8. **Permissioned vs. Permissionless Blockchains**: Anyone can join a permissionless blockchain and approve transactions, such as Bitcoin. Permissioned blockchains limit access to a predefined group of users, usually within an organisation or consortium.
9. **Mining and Nodes**: The process of adding transactions to the blockchain and validating them is called mining. In certain blockchain networks, miners receive rewards for their efforts, and nodes—computers connected to the network—participate in the consensus process.

**Properties of Blockchain:**

1. **Decentralization**: Decentralisation is the dispersion of control and decision-making power throughout the network as opposed to its concentration in a single central authority.
2. **Transparency**: In the context of blockchain, transparency pertains to the transaction data's availability and openness to all network users. Each participant can validate transactions and has a copy of the complete blockchain.
3. **Immutability**: Immutability refers to the inability of data (transactions) to be changed or removed from the blockchain once they have been added. The transaction history log is unchangeable and untouchable.

4. **Traceability**: The term "traceability" describes the blockchain's capacity to track the beginning and development of a particular asset or transaction. A chain of ownership is created by connecting each transaction to its predecessor.
5. **Anonymity**: In the context of blockchain, anonymity refers to user privacy. Blockchain transactions are transparent, but instead of using real names, participants' identities are frequently represented by cryptographic addresses.

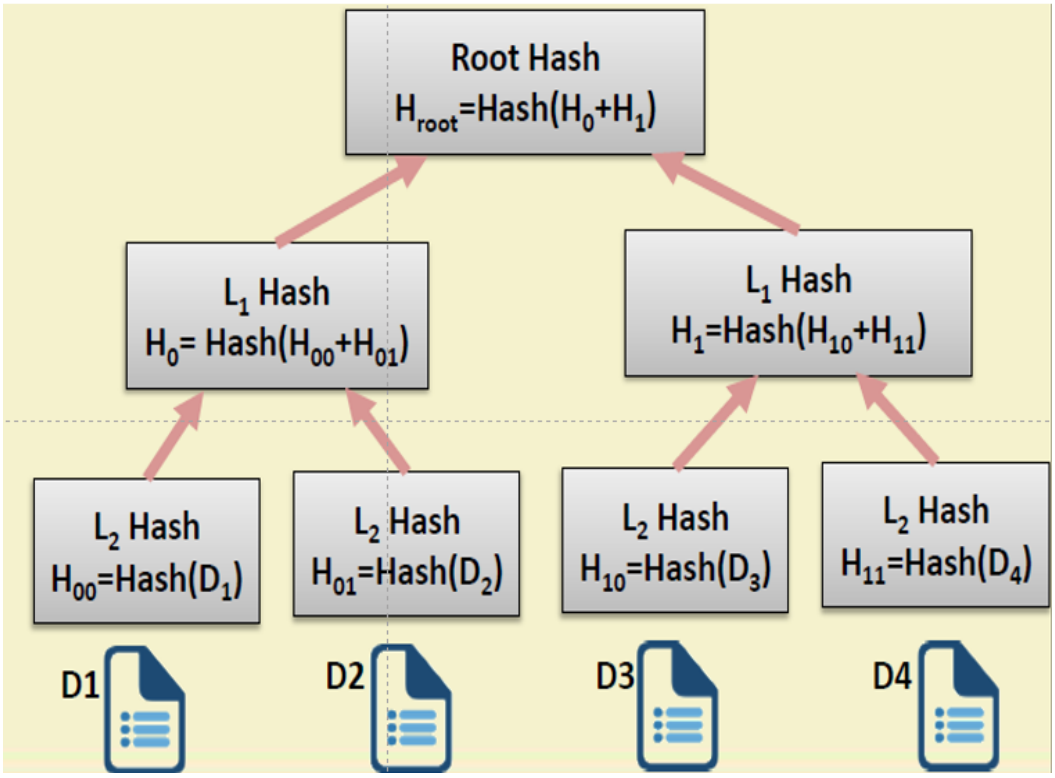
**Merkle Tree Structure:** In computer science and cryptography, a Merkle tree, sometimes referred to as a hash tree, is a data structure that is used to quickly confirm the integrity of big data sets. A Merkle Tree, so named for Ralph Merkle, who patented the idea in 1979, is especially helpful in file systems and blockchain technology.

The following components make up the Merkle Tree Structure:

1. **Leaf Nodes:** The data to be included in the Merkle Tree is separated into fixed-size blocks known as "leaf nodes." A file in a file system or a transaction in a blockchain are two examples of the distinct pieces of data that each leaf node represents.
2. **Hashing Pairs:** After the leaf nodes are paired, each pair's hash value is determined. The leaf nodes inherit their parents from the resulting hash values. In cases where the number of leaf nodes is odd, a pair is formed by duplicating the final node.
3. **Parent Nodes:** To create a new level of parent nodes, the procedure is repeated using the previous level's hash values. This process keeps going until there's just one hash value left, which is referred to as the "root hash" or "Merkle root."
4. **Merkle Root:** The entire set of data is represented by a single hash value, known as the Merkle root. No matter how tiny the alteration to the original data, the Merkle root will be entirely different. As a result, the Merkle root serves as a succinct and effective summary of the dataset's integrity.
5. **Verification:** Merely calculate the hash values as you follow the path from the leaf node holding the data to the root to confirm the integrity of a particular piece of data. The data is deemed to be unaltered if the computed root hash corresponds to the recognised Merkle root.

Merkle Tree offers numerous benefits, including compact representation, parallel processing, and efficient verification. Blockchain technology makes extensive use of Merkle Trees to guarantee the integrity of transactions within a block. The Merkle root is contained in the block header, and each transaction is represented as a leaf node. This eliminates the need to download and process the complete block and enables anyone to quickly and effectively confirm the accuracy of the transactions within a block.

Figure-3: Hash Tree Example



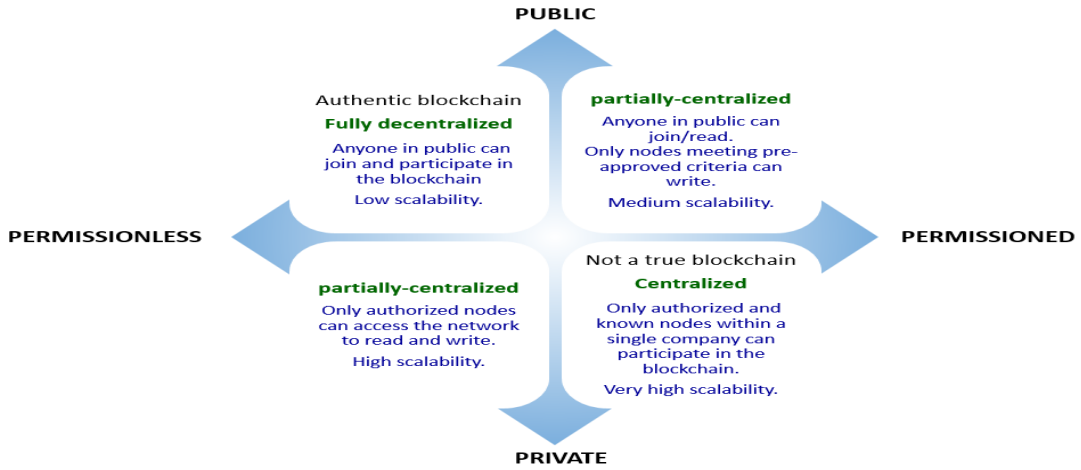

**Structure of Block:** In a blockchain, a block's structure usually consists of a number of uniform parts that come together to create a coherent and safe data unit. Although the precise arrangement may differ slightly based on the blockchain platform, the fundamental components are typically included. A block in a blockchain comprises:

1. **Header:** The header of a block is an essential component that holds metadata and details about the block. The Merkle tree root, version number, timestamp, nounce, and previous block hash are all contained in it.
   A. Version Number: The blockchain protocol's version represented by a number.
   B. Merkle Root: The block's transactional Merkle Tree's root hash. In an efficient manner, this hash represents each transaction in the block.
   C. Timestamp: The block's creation date as indicated by the timestamp.
   D. Nonce: A 32-bit or greater number that miners modify to satisfy the difficulty requirement and, consequently, solve the proof-of-work conundrum.
   E. Previous Block Hash: The blockchain's previous block's cryptographic hash. As a result, a chain of blocks is created, guaranteeing the blockchain's chronological order and integrity.
2. **Transaction Data:** A collection of transactions typically makes up the actual data that is kept in the block. Transactions include sender, recipient, amount, and other pertinent information. The block header contains the Merkle Tree root hash of these transactions.
3. **Block Size Limit:** Depending on the blockchain protocol, there is frequently a limit on the size of a block. This cap guarantees that the blockchain can be effectively distributed and validated by network users while also assisting in keeping each block's size manageable.
4. **Block Reward**: Miners who successfully add a block to the blockchain are rewarded in a number of blockchain networks. Newly created cryptocurrency and user-paid transaction fees are usually included in this reward.

**Types of Blockchain:** There are now many different kinds of blockchains because of the way blockchain technology has developed to meet different needs and use cases. Public and private blockchains are the two primary types; hybrid and consortium blockchains are also recognised. Four categories of blockchain exist:

1. **Public Blockchain**: Anyone can join, validate transactions, and establish a node on a public blockchain, which is an open, decentralised network. They are usually connected to cryptocurrencies and are permissionless. Example: Litecoin, Ethereum, and Bitcoin.
2. **Private Blockchain:** Private blockchains are not accessible to the general public and are limited to a particular set of participants. Businesses, associations, or consortiums frequently use them for internal work or joint ventures with reliable parties. Example: JPMorgan's Quorum, Hyperledger Fabric, and Corda (R3).
3. **Consortium Blockchain**: Consortium Blockchains represent a compromise between public and private blockchain technologies. They entail several groups or organisations cooperating in a consortium to share authority over the blockchain network. Members of the consortium have predefined rights. Example: R3 Corda consortium and B3i.
4. **Hybrid Blockchain**: Hybrid Blockchain incorporate aspects from both private and public blockchains. They permit some portions of the blockchain to be private and others to be public. Flexibility in terms of control and transparency may result from this. Examples are Komodo and Dragon-chain.

**Figure-4: Types of Blockchain**




**Consensus in Blockchain:** The process by which nodes in a decentralised network concur on the blockchain's current state is referred to as consensus in the context of blockchains. It is a crucial component of blockchain technology since it guarantees that everyone using the network comes to the same conclusion about the sequence and legitimacy of transactions. Maintaining the distributed ledger's security and integrity requires consensus.

Advantages of consensus use:

1. **Immutability and Tamper Resistance**: The blockchain's immutability is a result of consensus processes. It is computationally impractical to change a block once it has been added to the chain by a consensus process because doing so would necessitate changing every block that comes after it. The integrity of the transactions that are recorded is guaranteed by this tamper-resistant feature.
2. **Avoiding Double Spending**: Users can conduct transactions in a blockchain network without depending on a central authority. A cryptocurrency or digital asset cannot be spent twice (double-

spending) thanks to the consensus process. To stop fraud, all nodes concur on the legitimacy of transactions and their sequence.

3. **Decentralisation**: A fundamental tenet of blockchain technology is decentralisation. Decentralised decision-making is made possible by consensus mechanisms, which do away with the requirement for a central authority to approve transactions. Because there isn't a single point of failure, the network is more resilient and secure.
4. **Censorship Resistance**: Blockchain networks are resistant to censorship in part because of consensus processes. It is challenging to restrict or ban particular transactions because there isn't a single party in charge of the validation process. This is especially crucial in systems where inclusivity and openness are valued.
5. **Preserving Consistency**: Consensus makes sure that every node in the network sees the blockchain in the same way. The integrity of the entire system would be jeopardised if there were differences in the validity or order of transactions between nodes. The distributed ledger is reconciled and synchronised by consensus mechanisms.
6. **Strengthening Trust**: By offering a clear and agreed-upon procedure for validating and appending transactions to the blockchain, consensus mechanisms strengthen participant trust. The consensus protocols' cryptographic structure and the associated financial incentives foster trust.
7. **Scalability and Performance:** A blockchain network's scalability and performance are influenced by consensus processes. While some mechanisms prioritise energy efficiency, others are built to handle a higher transaction throughput. The consensus decision may have an effect on the system's overall effectiveness.

Blockchain networks require consensus in order to function because it provides the essential security, decentralisation, and trust mechanisms. Numerous consensus algorithms, each with unique advantages and disadvantages, are used by different blockchain platforms. These algorithms include Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and others. The particular objectives and specifications of the blockchain network determine the consensus method to be used.

**Consensus Mechanism**: A collection of guidelines or procedures known as a consensus mechanism allows users of a decentralised network to concur on the current state of a shared ledger. Consensus procedures are essential in the context of blockchain technology to bring nodes' understanding of the sequence and validity of transactions to a common understanding. They are essential to preserving the distributed ledger's dependability, security, and integrity. Various consensus mechanisms, each with its own set of guidelines and features, are used by different blockchain platforms.

1. **Proof of Work (PoW):** In this game, players, referred to as miners, compete to solve challenging math problems. If the solution provided by the first miner to solve the puzzle is accepted by the network, the block is appended to the blockchain. This is a computationally intensive process that uses a lot of resources.
2. **Proof of Stake (PoS):** Depending on how much cryptocurrency a validator is willing to "stake" collateral, they are selected to add new blocks and approve transactions. The stakes determine the probability of being selected.
3. **Delegated Proof of Stake (DpoS):** A small group of reliable delegates are chosen by token holders through a voting process, and these delegates are in charge of validating transactions and building new blocks. This improves scalability by lowering the number of participants in the consensus process.

4. **Proof of Authority (PoA):** Validators are nodes whose identity and authority are acknowledged. They are usually well-known entities, which adds a degree of centralization but improves the efficiency and speed of transactions.
5. **Proof of Space (PoSpace):** Users demonstrate that a specific quantity of disc space has been allotted to the network. The premise behind this consensus process is that users who have more space available to them will be more likely to be selected to add new blocks.
6. **Proof of Burn (PoB):** By "burning" or destroying a specific quantity of cryptocurrency, users show their dedication to the network. This is frequently used as an initial distribution method and demonstrates a willingness to contribute to the security of the network.

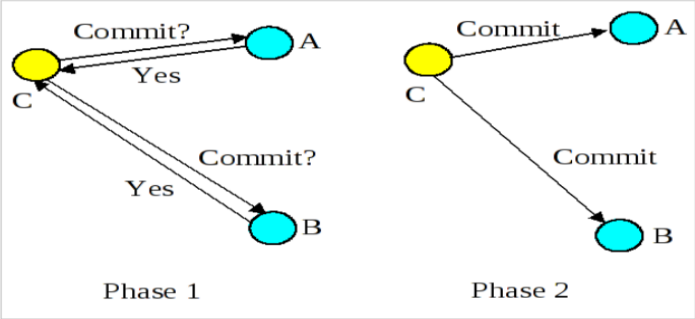
**Miners and Mining:**

**Miners:** For many blockchain networks, especially those that employ Proof of Work (PoW) as their consensus mechanism, miners are essential to their operation and security. Miners are responsible for Transaction validation, Block creation, Block rewards, Security and Consensus mechanism in the blockchain.

**Mining:** Miners, or participants in blockchains, compete to add new blocks to the blockchain through a process known as mining.

1. **Two Phase Commit:** Two-Phase Commit protocol is intended to guarantee that all nodes come to a consensus regarding whether to commit or abort a transaction. This protocol has no direct connection to the blockchain mining process, despite being utilised in some distributed databases and systems.

**Figure-5: 2P Commit**




a) Phase of Voting (Prepare Phase): All participating nodes receive a message from the coordinator node asking if they are prepared to commit the transaction. Each participant votes "yes" or "no" in response.
b) Phase of Decision (Commit or Abort): The coordinator chooses whether to commit the transaction or not based on the votes that were cast. In the event that every voter cast a "yes," the coordinator notifies every node of the commit. An abort message is sent by the coordinator if any participant cast a "no" vote.

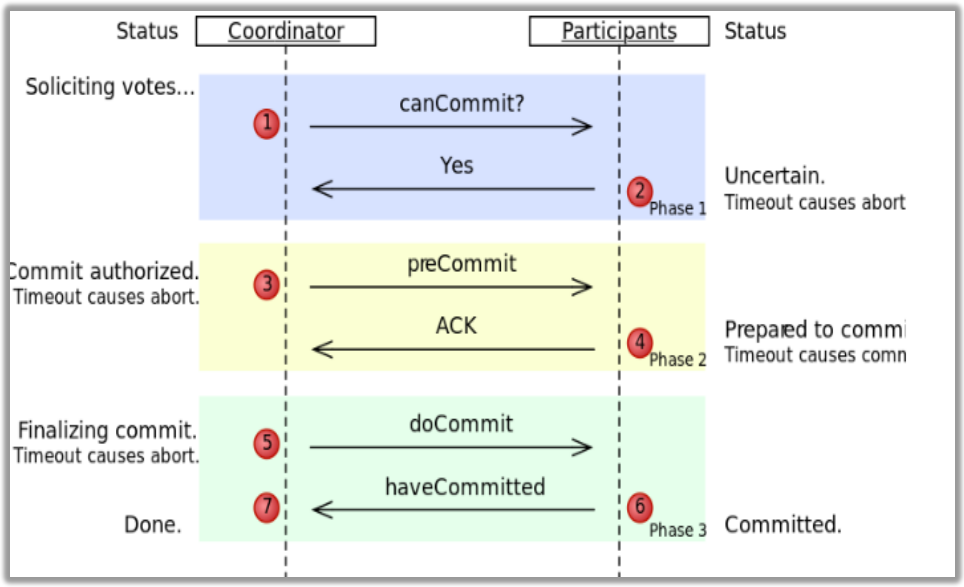
2. **Three Phase Commit:** An expansion of the Two-Phase Commit (2PC) protocol, the Three-Phase Commit (3PC) protocol was created to handle some restrictions and possible blocking scenarios that may arise in distributed systems. The 3PC protocol is used, like 2PC, to synchronise distributed nodes in deciding whether to commit or cancel a transaction.
   a) Pre-Commit Phase:The coordinator node asks all participating nodes via a "CanCommit" message if they are prepared to commit the transaction, much like in the Prepare Phase of 2PC. The

coordinator is aware that at least one participant is not ready to commit if they receive a "No" vote from a participant node or if there is a timeout.

b) Pre-Abort Phase (PreAbort): The coordinator advances to the "PreAbort" phase if every participant votes "Yes" in the first phase. If at any point during this phase the participants' decision changes, the coordinator can advise them to abort.This extra stage was added to address the possibility that a voter may have voted "Yes" at first but later run into a problem that keeps them from committing.

c) Commit or Abort Phase (DoCommit): The coordinator notifies all participants to commit the transaction in a "DoCommit" message if no problems are reported during the "PreAbort" phase.The transaction is committed if a participant gets a "DoCommit" message. The transaction is cancelled if a participant gets a "PreAbort" message or if something goes wrong.

**Figure-6: 3P Commit**




**Smart Contracts in Blockchain:** Self-executing contracts, or smart contracts, have the terms of the contract directly encoded into the code. Because they are blockchain-based, they can execute predetermined conditions automatically and without reliance. A fundamental component of blockchain technology, smart contracts were initially made available by Ethereum, a decentralised platform for creating decentralised applications (DApps). Smart contracts are essential to the development of blockchain technology because they make it possible to create decentralised applications that are executed automatically and without trust. They are an effective tool for many industries looking to streamline procedures and lessen dependency on middlemen because of their adaptability and transparency.
Even with all of their benefits, smart contracts are not perfect. The “oracle problem” prevents them from accessing external data, and the blockchain network’s computational capacity limits how they can operate.

**Double spending using Blockchain:** In digital currency systems, including blockchain-based cryptocurrencies, double spending is a possible problem. It alludes to the possibility that a user will use the same amount of money more than once, thereby producing a conflicting or duplicate record of a transaction. Since it is far simpler to copy and duplicate digital information than physical currency, this issue is especially difficult in digital systems.

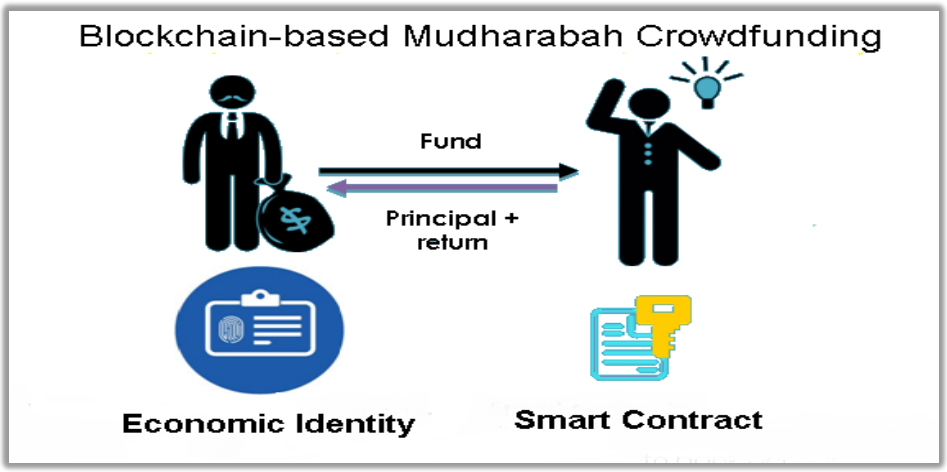
1. Conventional Digital Systems: By taking advantage of the delay between the start of a transaction and its confirmation, a user may try to spend the same digital currency unit twice in a centralised digital payment system (such as traditional online banking).
2. Blockchain System: Consensus procedures are used in a decentralised blockchain system to avoid double spending. A distributed ledger is used by blockchain networks, like Bitcoin, and it is kept up to date by a network of nodes, or computers. Blocks are created by transactions, and a consensus process is used to add these blocks to the chain.

Although the risk of double spending is effectively reduced by blockchain technology, it is important to take into account the particular consensus mechanism and security features of the blockchain network in question. Consensus mechanisms in various forms may be used by different blockchains to protect their networks from possible attacks and double spending.

**Crowd Funding in Blockchain:** Traditional crowdfunding models have been transformed by blockchain technology, which offers improved efficiency, security, and transparency. Often called "crowdfunding on the blockchain" or "tokenized crowdfunding," blockchain-based crowdfunding uses smart contracts and the blockchain to enable fundraising campaigns. Notable blockchain-based crowdfunding platforms include Ethereum-based ICOs and STOs, as well as Kickstarter, which uses blockchain technology for crowdfunding campaigns.

With blockchain-based crowdfunding, project creators can now connect with a global pool of contributors through more effective, transparent, and inclusive mechanisms that offer a new paradigm for fundraising. Potential participants should, nevertheless, proceed with caution, carry out careful due diligence, and be informed about the legal and regulatory environment surrounding blockchain crowdfunding in their country.

**Figure-7: Crowd Funding Example**




**3. Literacy Survey:**

We created a excel sheet regarding our survey from different papers.

Link to view our survey: Our Research Review.xlsx

The paper "A Survey of Blockchain Security Issues and Challenges." researches a number of topics, including the idea behind blockchain technology, how it can be used, and the difficulties and security concerns that come with it. They stressed the need for governments to pass laws governing this technology in their conclusion. [1]

"Bitcoin: A Peer-to-Peer Electronic Cash System" uses a proof-of-work mechanism and peer-to-peer network to keep a public ledger of transactions updated. If honest nodes control most of the CPU power, then an attacker would quickly find it computationally impractical to alter this ledger. Nakamoto also suggested a trustless electronic transaction system. [2]

H. R. Usha, Manjunath R. Kounte, Shreevani Dnai, and V. M. Harshini concentrated their efforts on "Health Record Management through Blockchain Technology." They began by talking about each person's responsibility for their own health and the traditional ways of keeping medical records in hard copy or book format. Next, the group presented the idea of blockchain and its technological uses. They also put in place smart contracts, which are pieces of self-executing code that start working as soon as both parties accept a predefined set of rules. Automated tasks like record creation, validation, and invocation are managed by the smart contracts. [3]

Important topics including Blockchain Architecture, Consensus Algorithms, and Blockchain Applications were covered in the paper "Blockchain Technology: A Literature Survey." The conclusion drawn from their research is that Bitcoin is a widely recognised and accepted example of a decentralised online currency. A distributed database called Blockchain records all transactions made on the Bitcoin network and keeps an unchangeable, unhackable ledger of all transactional data. Similar to traditional bank ledgers, this technology makes it easier to create and share digital ledgers. [4]

In "Smart Farming using Blockchain", a system using sensors and the Internet of Things (IoT) that incorporates Raspberry Pi. This system was made to keep an eye on a variety of factors, such as pH levels in agricultural settings, temperature, humidity, and soil moisture as well as fire incidents. Data collection from the field-deployed sensors was greatly aided by the Internet of Things, with the Raspberry Pi acting as the central hub. Following data collection, real-time insights into the monitored parameters were presented on an LCD screen. The researchers concluded by recommending the use of blockchain technology to improve data management and security in the context of smart farming. [5]

The principal aim of the paper titled "Smart Farming: Securing Farmers using Blockchain Technology and IoT" was to address issues related to crop diseases, quality control, and the wider food supply chain. The team concluded by highlighting the efficacy of their model, which combined blockchain technology for safe data transactions and storage with Internet of Things devices for real-time monitoring. The objective of this comprehensive strategy was to augment traceability, mitigate occurrences of food fraud, and ultimately elevate general transparency in the agricultural supply chain. [6]

In a study on the constraints of blockchain technology, Ambika V.M. and DS Rao concentrated on how the technology might be used in smart cities. Permission access, properties, and drawbacks were among the topics covered in the research. High energy consumption, the necessity of striking a balance between node quantity and cost, and difficulties modifying current infrastructure were also highlighted. The study offers insightful information about the real-world difficulties associated with deploying blockchain in smart city settings. [7]

Mehdi Benchoufi and team, led by Philippe Ravaud, researched using Blockchain to enhance clinical research quality, addressing challenges like reproducibility, data sharing, privacy, and patient enrollment. They concluded that Blockchain offers a significant opportunity by providing a transparent, verifiable methodology. Through defined core metadata, it ensures clinical trial integrity, incorporating transparency and algorithmic verification to an extent. [8]

The study "Mobile Payment Using Blockchain Security" used a secondary methodology, compiling information from reliable sources. Using Ethereum as a private network for strong security, they unveiled a safe mobile payment system with PIN code authentication and encrypted transactions. [9]
The paper "Modern Blockchain-Platforms: Advantages and Prospects" explores the revolutionary potential of blockchain technology, emphasising how it affects both the advancement of economic models and technological innovation. A review of current blockchain-related literature and platforms is part of the research methodology. The analysis concludes that current blockchain platforms face challenges in ensuring transaction volume, speed, and security, which hinders their widespread adoption. [10]
Project titled "E-Voting Using Blockchain with Biometric Authentication" is in order to solve problems with Electronic Voting Machines (EVMs), such as fraud and time-consuming procedures, the paper suggests a blockchain-based solution. In an effort to improve vote authenticity, the Election Commission of India has introduced the Voter Verifiable Paper Audit Trail (VVPAT). The paper highlights the security concerns related to the proposed software-based voting system transition and supports its adoption. [11]

## 4.Conclusion:

Finally, our survey has explored the wide field of blockchain technologies and offered a comprehensive overview of the decentralised space. This investigation has illuminated the complex structure of blockchain, covering everything from the fundamental ideas of distributed ledgers to the complexities of consensus processes and smart contracts. By carefully dissecting applications from a variety of industries, we have seen firsthand how revolutionary blockchain technology can be in upending established paradigms.
According to our survey, there are obstacles on this journey of transformation. To overcome obstacles posed by security worries, scalability problems, and regulatory considerations, the community must work together. Moreover, blockchain technology's dynamic nature necessitates constant innovation and adaptation.
Following this analysis, our survey is a fundamental resource for scholars, professionals, and enthusiasts. We sincerely hope that this thorough overview will stimulate more investigation, intelligent conversation, and direction for future research projects in the exciting and constantly changing field of blockchain technologies.

## 5. Acknowledgment:

First and foremost, we would like to sincerely thank **Ramaiah Challa** sir for all of his help, advice, and insightful criticism during our research. Sincere gratitude is extended to the community and our academic colleagues for all of their help, inspiration & information sharing during the course of the research project. Their advice, knowledge, and perspectives have greatly influenced the concepts in this paper, and I sincerely appreciate what they have done for me academically.

## 6. References:

1. Iuon-Chang Lin, Tzu-Chun. “A Survey of Blockchain Security Issues and Challenges”. IJNS, 2017 http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf
2. Sathosi. “Bitcoin: A Peer-to-Peer Electronic Cash System”. 2009 https://www.researchgate.net/publication/228640975

3. Harshini, Sreevani, Usha, Manjunath. “Health Record management Through Blockchain Technology”. ICOEI, 2019. https://ieeexplore.ieee.org/document/8862594/authors
4. Ibrar Ahmed, Shilpi, Amjad. “Blockchain Technology a Literature Survey”. IJRTE, 2018. **https://www.irjet.net/archives/V5/i10/IRJET-V5I10284.pdf**
5. Jemima, Ezhilarasi. “Smart Farming using Block Chain”. IJRTE, 2020. https://www.irjet.net/archives/V7/i10/IRJET-V7I1048.pdf
6. Praveen, Ali Shaik, Sampath, Tanupriya Choudhury. “Smart Farming: Securing Farmers Using Block Chain Technology and IOT”. Blockchain Applications in IoT Ecosystem, 2021. https://www.researchgate.net/publication/352377264
7. Ammbika, D.S Rao. “Limitations of Blockchain Technology with its Application”. IJRTE, 2019. https://www.ijrte.org/wp-content/uploads/papers/v8i2S11/B14590982S1119.pdf
8. Benchoufi, Ravaud. “Blockchain Technology for improving Clinical Research Quality”. 2017. https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z
9. Obaid, Aqel. “Mobile Payment using Blockchain Technology”. 2021. https://www.researchgate.net/publication/352165809_Mobile_Payment_Using_Blockchain_Security
10. Dr. Ruslan Dolzhenko. “Modern Blockchain Platforms: Advantages and prospects”. https://www.academia.edu/40480923
11. Suralkar, Sanjay, Sumit, Mayur, Mohith. “E-Voting Using Blockchain With Biometric Authentication”. 2019. http://ijrar.com/upload_issue/ijrar_issue_20543302
12. Pingshui, Jianwen, Qinjuan. “Privacy Data Protection in Social Networks Based on Blockchain”. ISSN, IJRES. https://www.ijres.org/papers/Volume-10/Issue-12/1012375379
13. Manuel, Theodoor, Engin Kirda, Christopher. "An overview of tools and methods for automated dynamic malware analysis ". ACM Surveys, March (2008). https://dl.acm.org/doi/10.1145/2089125.2089126
14. Ankush, Sumith. “Artificial Intelligence Enabled Cyber Security”. IEEE,2021. https://ieeexplore.ieee.org/document/9609376
15. Sayeed Sajal. “Artificial Intelligence in Cyber Security”. IEEE, 2023 https://ieeexplore.ieee.org/document/10152034
16. Nouhaila, Hanine, Soriano Flores, Daniel Gavilanes & Imran Asraf. “Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends from Bibliometric Analysis”. IEEE, 2023.https://ieeexplore.ieee.org/document/10192385
17. Al-Issa, Ottom, Tamrawi. “Issues with eHealth Cloud Security: An Overview”. Hindawi. 2019 https://www.hindawi.com/journals/jhe/2019/7516035/
18. Yang Xin, Zhi Liu, Yanmiao Li, Gao, Haixai Hou. “Machine & Deep Learning Methods in Cybersecurity”, IEEE, 2018 https://ieeexplore.ieee.org/document/8359287
19. Iqbal H.Sarker. “Prospects for the Future and Present of Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity”. Sept,2022, Springer https://rdcu.be/drlPH
20. Javed, Rajabi (2019). “IoT botnet traffic classification using a multi-layer perceptron artificial neural network.” Proceedings of the future technologies conference, Springerhttps://www.researchgate.net/publication/336497038
21. **Remya, Ahmad. “**Privacy and Security in Cloud-Based Electronic Health Records**”. MDPI, 2021.**https://www.mdpi.com/2073-8994/13/5/742

22. Qadir, Mujeeb-U-Rahman, Rehmani, M.H, Pathan A.S.K., Imran M.A , Hussain, Rana, Luo. “”.Editorial for Special Section: Health Informatics in Developing Countries IEEE,2017.https://ieeexplore.ieee.org/abstract/document/8262687