A Study on Blockchain Technology

Dr.M.Moorthy[1], Mrs.C.Radha[2], Mr.S.Nithyananth[3]
[1]*Professor, Muthayammal Engineering College*
[2,3]*Associate Professor, Muthayammal Engineering College*

***Abstract*—Blockchain is undoubtedly a revolutionary technology that is making a great impact on modern society due to its transparency, decentralization, and security properties. Blockchain has gained considerable attention due to its very first application of Crypto currencies e.g., Bitcoin. In the near future, Blockchain technology is determined to transform the way we live, interact, and perform businesses. Unlike other Blockchain surveys focusing on its applications, challenges, characteristics, or security, we present a comprehensive survey of Blockchain technology's features, architecture, development frameworks, and scalability issues. We also present a comparative analysis of frameworks, use cases, technologies involved and other things. Finally, this paper elaborates on key future directions and use cases, which could be explored by researchers to make further advances in this field.**

***Index Terms*—Blockchain, Bitcoins, P2P Networks, Smart contracts, Blockchain use cases, and Blockchain platform.s**

I. INTRODUCTION

The concept of secured chain of blocks is not a new idea. It was presented by Stuart Haber et al. in 1991 as a means to digitally timestamp electronic documents to protect against tampering [2]–[4]. However, it gained popularity in the recent years when used in Blockchain technology to store transactions of a crypto currency called ‘‘Bitcoin’’ [1].

The Blockchain 1.0 technology is associated with Crypto currencies, especially Bitcoin. Bitcoin uses Blockchain as a way to solve the long-existing problems of double spending of digital cash and processing of digital transactions in a decentralized way without the need of any trusted third party.

The Blockchain 2.0 is associated with Smart Contracts. The new key concepts are Smart Contracts, small computer programs that "live" in the blockchain. They are free computer programs that execute automatically and check conditions defined earlier like facilitation, verification, or enforcement. It is used as a replacement for traditional contracts.

The Blockchain 3.0 is associated with Dapps. DApps is an abbreviation of decentralized application. It has its backend code running on a decentralized peer-to-peer network. A DApp can have frontend Blockchain example code and user interfaces written in any language that can make a call to its backend, like a traditional App.

In a layman term, Blockchain is defined as the chain of digital blocks connected and associated with each other as an open distributed ledger. Initially, it was used to store only transactions of digital currencies, but later it started to use in other applications beyond currency and payments [5]. There are also different types of Blockchains based on their usage and distinct attributes viz., Public blockchains, Private blockchains and Consortium blockchains. Public blockchains are truly decentralized and allow anyone to join the network and engage in managing them. While in private blockchains only invited people from a single organization can join the network and manage them. The consortium Blockchain also called ‘‘Federated Blockchain’’ is between public and private Blockchain, in terms of permissions and management. Invited people from multiple organizations are allowed to join this Blockchain.

This paper is organized as different sections containing the core details of blockchain technology which every researcher should know, from section-1: Blockchain up to section-18: Future of Blockchain including blockchain's applications, use cases and platforms.

II. BLOCK CHAIN

It is a digital ledger that stores transaction details. These records are stored in containers called blocks. These blocks are linked to each other and are secured using cryptography.

A. Features

- Available for anyone to access
- Data can be added but cannot be altered

- To add data, a mathematical puzzle has to be solved
- This solution has to be approved by everyone in the network
- No central authority has control over the information
- Privacy is protected by cryptography

III. BITCOIN

It is a digital currency that uses cryptography to limit how much of it exists at a time. It is also used to verify transfer of assets and secure financial transactions. It uses blockchain technology.

A. Features

- Uses blockchain technology
- Identities can be anonymous
- Payments are secured by cryptography
- Transferring assets is costlier with that currency
- Transferring assets is faster as compared to flat currencies
- They do not work under a central authority

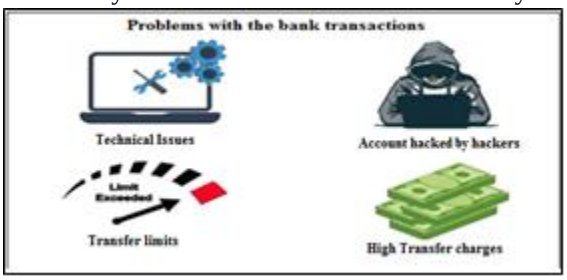

Figure-1: Problems with the bank transactions

As shown in Figure-1, the problems with the bank transactions are Technical issues, Accounts might have been hacked by hackers, Limits for transfer of amounts, and high transfer charges are there.

IV. NEED FOR BLOCKCHAIN

Here are some reasons why Blockchain technology has become so popular.

Resilience: Blockchains is often replicated architecture. The chain is still operated by most nodes in the event of a massive attack against the system.

Time reduction: In the financial industry, blockchain can play a vital role by allowing the quicker settlement of trades as it does not need a lengthy process of verification, settlement, and clearance because a single version of agreed-upon data of the shared ledger is available between all stack holders.

Reliability: Blockchain certifies and verifies the identities of the interested parties. This removes double records, reduces rates, and accelerates transactions.

Unchangeable transactions: By registering transactions in chronological order, Blockchain certifies the inalterability of all operations, which means when any new block has been added to the chain of ledgers; it cannot be removed or modified.

Fraud prevention: The concepts of shared information and consensus prevent possible losses due to fraud or embezzlement. In logistics-based industries, blockchain as a monitoring mechanism act to reduce costs.

Security: Attacking a traditional database is the bringing down of a specific target. With the help of Distributed Ledger Technology, each party holds a copy of the original chain, so the system remains operative, even a large number of other nodes fall.

Transparency: Changes to public blockchains are publicly viewable to everyone. This offers greater transparency, and all transactions are immutable.

Collaboration – Allows parties to transact directly with each other without the need for mediating third parties.

Decentralized: There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated and all valid transactions are added one by one.

V. SAMPLE BLOCKCHAIN

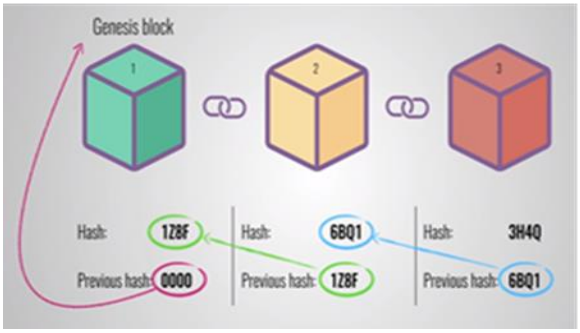

Figure-2: Sample blockchain [6]

In Figure-2, there are three blocks in the blockchain and they are serially numbered from 1 to 3.

Every block in the blockchain has its unique hash and previous hash. The previous hash of block-3 is hash of block-2 and for block-2 it is the hash of block-1. But for block-1, the previous hash is '0000' which is called genesis block.

VI. BLOCKCHAIN 4 MAJOR FEATURES

1. Public distributed ledger: It is a collection of digital data which is shared, synchronized and replicated across the world, across multiple sites, countries and institutions.
2. Hash encryption: Each user has their own public and private key. The public key is used to uniquely identify the user. The private key gives the user access to everything in the account. The sender's message is passed through a hash function. The output of hash is passed through a signature algorithm with user's private key. The user's digital signature is obtained.
3. Proof of work: It is a competition among people around the world, who want to add a block to the blockchain. Finding the nonce value is the mathematical puzzle that miners need to solve. It is the process of finding the appropriate nonce that helps generate a hash value that satisfies certain predefined conditions. The first one to find that nonce value is rewarded for it.
4. Mining: It is the process of a miner being rewarded with 12.5 bitcoins for being the first one to find the nonce. This by extension adds that block to the blockchain.

VII. CORE COMPONENTS OF BLOCK CHAIN

Node: User or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)

Transaction: smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain

Block: A data structure used for keeping a set of transactions which is distributed to all nodes in the network

Chain: A sequence of blocks in a specific order

Miners: Specific nodes which perform the block verification process before adding anything to the blockchain structure

Consensus (consensus protocol): A set of rules and arrangements to carry out blockchain operations

Any new record or transaction within the blockchain implies the building of a new block. Each record is then proven and digitally signed to ensure its genuineness. Before this block is added to the network, it should be verified by the majority of nodes in the system.

VIII. THREE TECHNOLOGIES USED IN BLOCKCHAIN

1. Private Key cryptography: Blockchain uses this to secure identities and hash functions to make the blockchain immutable
2. P2P Network: P2P machines on the network help in maintaining the consistency of the distributed ledger. Double-spending can be avoided using this [12].
3. Blockchain program: It is to implement the blockchain technology.

IX. BLOCKCHAIN VERSIONS

Blockchain 1.0: Currency

The implementation of DLT (distributed ledger technology) led to its first and obvious application: crypto currencies. This allows financial transactions based on blockchain technology. It is used in currency and payments. Bitcoin is the most prominent example in this segment.

Blockchain 2.0: Smart Contracts

The new key concepts are Smart Contracts, small computer programs that “live” in the blockchain. They are free computer programs that execute automatically and check conditions defined earlier like facilitation, verification, or enforcement. It is used as a replacement for traditional contracts.

Blockchain 3.0: DApps:

DApps is an abbreviation of decentralized application. It has its backend code running on a decentralized peer-to-peer network. A DApp can have frontend Blockchain example code and user interfaces written in any language that can make a call to its backend, like a traditional App.

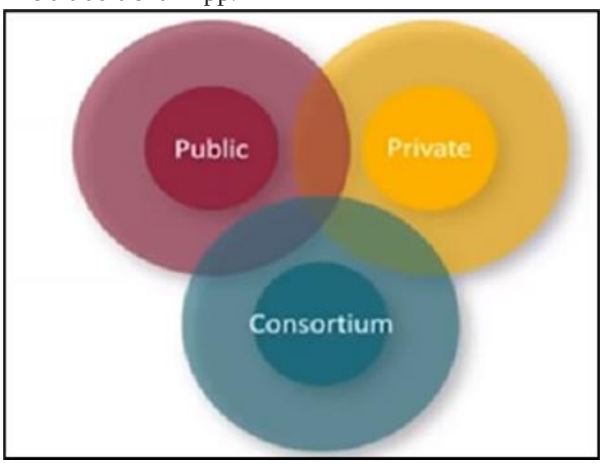

Figure-3: Types of blockchain

X. TYPES OF BLOCKCHAINS

There are three types of blockchains as shown by figure-3.

Public: Public blockchains have ledgers visible to everyone on the internet and anyone can verify and add a block of transactions to the block chain.

Private: Private blockchains allow only specific people in the organization to verify and add transaction blocks but everyone on the internet is generally allowed to view.

Consortium: In this type of blockchain, only a group of organizations can verify and add transactions but the ledger can open or restrict to select groups.

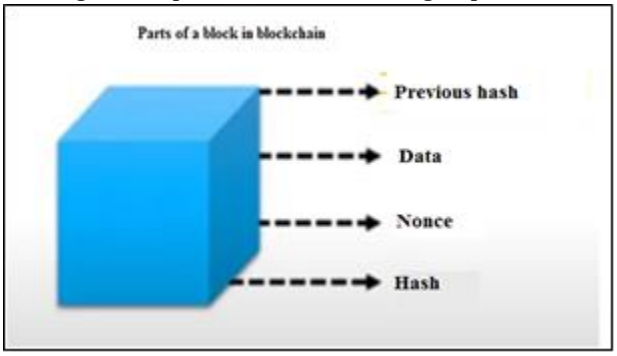

Figure-4: Parts of a block in blockchain

XII. BLOCK IN BLOCKCHAIN

A block is the smallest unit of blockchain which records all the transactions. It has the following four fields as shown in Figure-4.

- Previous hash: It holds the hash value of the previous block. For block 1, it is '0000' and called as genesis block.
- Data: It contains details of several transactions which are stored in this field.
- Nonce: In proof of work, nonce is a random value which is used to vary the output of the hash value.
- Hash: It is the resultant hash value obtained from passing the previous hash, data and nonce through the SHA-256 algorithm.

XIII. STEPS IN BLOCKCHAIN FLOW DIAGRAM

1. Someone requests a transaction
2. The transaction is broadcast to the P2P network
3. The network of nodes validate the transaction
4. Once verified, the transaction become a part of new block for the ledger
5. The new block is then added to the existing blockchain
6. The transaction is complete

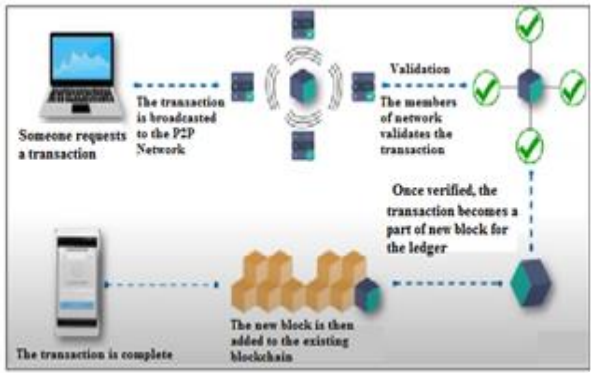

Figure-5: Blockchain flow diagram

A. Advantages of Blockchain

1. Trustless: The blockchain is immutable and automates trusted transactions between counterparties who do not need to know each other. Transactions are only executed when programmed conditions are met by both parties.
2. Unstoppable: Once the conditions programmed into a blockchain protocol are met, an initiated transaction cannot be undone, changed, or stopped. It's going to execute and nothing – no bank, government, or third party – can stop it.
3. Immutable: Records on a blockchain cannot be changed or tampered with – Bitcoin has never been hacked. A new block of transactions is only added after a complex mathematical problem is solved and verified by a consensus mechanism. Each new block has a unique cryptographic key resulting from the previous block's information and key being added into a formula.
4. Decentralized: No single entity maintains the network. Unlike centralized banks, decisions on the blockchain are made via consensus. Decentralization is essential because it ensures people can easily access and build on the platform, and there are multiple points of failure.
5. Lower Cost: In the traditional finance system, you pay third parties like banks to process transactions. The blockchain eliminates these intermediaries and reduces fees, with some systems returning fees to miners and stakers.
6. Peer-to-Peer: Cryptocurrencies like Bitcoin, let you send money directly to anyone, anywhere in

the world, without an intermediary like a bank charging transaction or handling fees.

7. Transparent: Public blockchains are open-source software, so anyone can access them to view transactions and their source code. They can even use the code to build new applications and suggest improvements to the code. Suggestions are accepted or rejected via consensus.
8. Universal Banking: 2 Billion people globally do not have a bank account. Because anyone can access the blockchain to store money, it's a great way to bank the unbanked and protect against theft that can happen due to holding cash in physical locations.

B. Disadvantages of Blockchain

1. Environmental Impact

Blockchain networks like Bitcoin use a lot of electricity to validate transactions, leading to environmental concerns.

2. Personal Responsibility

One of blockchains and crypto currencies' most significant advantages is also its biggest weakness. When you invest in public open-source blockchains by mining or buying crypto currencies and store it in your crypto currency wallet (your wallet is like your bank account, except only you can access it and have the passwords), only you control your money.

3. Growing Pains

Even though public blockchains remain more efficient than traditional banking systems, decentralization comes at the cost of scalability.

4. False Narratives

Some crypto currencies are undoubtedly used in unlawful activity. The most famous example is Silk Road: people laundered money and bought drugs on the platform using Bitcoin.

XIV: SCALABILITY PROBLEMS AND SOLUTIONS

Scalability problems are the main thing restraining the excitement around blockchain technology. With increasing popularity of crypto currencies, transactions have increased considerably over the years. While it was manageable when the number of transactions was less, as they have more popular a host of issues have come up.

It is because of the following two reasons:

The time taken to put a transaction in the block and time taken to reach a consensus.

Solutions:

The lightening network: It does not require every individual transaction to be recorded on the blockchain.

Segwit: It is exclusive to bitcoins and means that all the signature of each and every transaction will move from main chain to the side chain[11].

Block size increase: With increasing transactions particularly in Bitcoins and Ethereum, the possible solution is to increase the block size to accommodate more transactions.

Sharding: It separates the blockchain data in several sets, and storing only one of these sets.

XV: APPLICATIONS OF BLOCKCHAIN

1. Insurance: Utilizing blockchain, insurance companies can eliminate forgery and prevent false claims.
2. Accounting: Blockchain virtually maintains a record of accurate financial information by protecting the data from tampering.
3. Travel: To ease the verification of documents.
4. Music: To stop music piracy and to compensate artists for purchased songs.
5. Cybersecurity: Data integrity can be guaranteed. There cannot be a single point of failure.
6. Human Resources: Verification of identity of employee, history, etc. Payment and benefit process validation.
7. Walmart: Due to blockchain's decentralized system, the company is able to protect its data from hacking and data alteration.
8 British airways: With blockchain, flight data from various sources are merged together and help passengers receive accurate information.
9. Maersk: With blockchain, the company is able to provide an efficient, transparent and secure service in global trade.
10. Brilliant earth: In order to track and trace the provenance of gemstones, Brilliant Earth uses blockchain.

XVI: BLOCKCHAIN USE CASES

Blockchain Technology is used widely in the different sectors as given in the following table.

Sector	Usage
Markets	• Billing, monitoring and Data Transfer • Quota management in the Supply Chain Network
Government Sector	• Transnational personalized governance services • Voting, propositions P2P bond, • Digitization of documents/ contracts and proof of ownership for transfers • Registry & Identify • Tele-attorney service • IP registration and exchange • Tax receipts Notary service and document registry
IOT	• Agricultural & drone sensor networks • Smart home networks • Integrated smartcity. • Smart home sensors • Self-driving car • Personalized robots, robotic component • Personalized drones • Digital Assistants
Health	• Data management • Universal EMR Health databanks • QS Data Commons • Big health data stream analytics • Digital health wallet Smart property • Health Token • Personal development contracts
Science & Art	• Supercomputing • Crowd analysis • P2P resources • Digital mind fit services
Finance & Accounting	• Digital Currency Payment • Payments & Remittance • Decartelized Capital markets using a network of the computer on the Blockchain • Inter-divisional accounting • Clearing & Trading & Derivatives • Bookkeeping

Table-1: Blockchain use cases

XVII: TOP BLOCKCHAIN PLATFORMS

S.No	Name of the Platform	Description
1	XDC Network	A ready enterprise-grade hybrid blockchain for finance and global trading, XDC Network combines the features of public and private blockchains via cross-chain smart contracts. XDC is a decentralized and liquid network leveraging interoperability. It powers digitization and tokenization with instant regulation of trade transactions, increasing efficiency and minimizing dependency on complicated FX infrastructures.
2	Tezos	Founded by Arthur Breitman and Kathleen Breitman, Tezos is designed to offer the safety and code correctness needed for digital assets and high-value use cases. It is a decentralized blockchain platform that is self-governing.
3	Hyperledger Fabric	Hyperledger Fabric is proposed as a foundation for building apps or solutions with a modular architecture. It allows components, including membership services and consensus, to be plug-and-play. It has a wide range of modular and versatile design that meets various industrial use cases.
4	Hyperledger Sawtooth	Hyperledger Sawtooth provides a modular and flexible architecture that separates the core system from the application domain. Therefore, smart contracts can imply the business rules for applications without understanding the underlying design of the core system. It supports different consensus algorithms, including Proof of Elapsed Time (PoET) and Practical Byzantine Fault Tolerance (PBFT).
5	Stellar	Stellar is an open blockchain network that allows the storing and moving of money. It facilitates you to create, trade, and send digital representations of all forms of money, for example, dollars, bitcoin, pesos, and a lot more.
6	EOS	EOS is a blockchain platform designed to develop scalable and secure dApps. It provides dApps' hosting, smart contracts capability, decentralized storage of enterprise solutions to solve

		the scalability issues faced by Ethereum and Bitcoin.
7	Corda	Corda is an open-source blockchain platform that allows businesses to transact directly and in strict privacy with smart contracts. It reduces record-keeping and transaction costs by streamlining business processes.
8	Klaytn	Klaytn is a worldwide public blockchain platform created by Ground X, the South Korean social media company Kakao's blockchain subsidiary. Klaytn, a blockchain developed by Kakao, was built with modular network architecture, making it an interesting business blockchain option. Its modular network architecture makes it easy for enterprises to create and run service-oriented blockchains based on the Klaytn architecture.
9	Tron	Tron is a decentralized blockchain platform that aims to develop a decentralized web. Like Ethereum, Tron allows dApp developers to create and leverage complete protocols via smart contracts on the blockchain. The Tron platform can handle 2000 transactions per second, which put it on par as compared to major payment processors like Paypal. It has zero transaction fees.
10	Hedera Hashpraph	Hedera Hashgraph Platform is a lightning secure, fair, and fast platform that does not require computing a heavy proof of work algorithm. It allows developers to develop new innovative and scalable decentralized applications.
11	Ethereum	Ethereum is one of the leading blockchain platforms that have a native crypto currency called ETH or Ether. Developers use Ethereum to build new applications related to financial apps, decentralized markets, games, crypto currency wallets, and more. They have the largest community with core protocol developers, cypherpunks, crypto-economic researchers, and mining organizations. It aims to eliminate internet third parties who save data and track financial instruments.

Table-2: Top blockchain platforms [9]

XVIII: FUTURE OF BLOCKCHAIN

Blockchain has a great potential to revolutionize the way of doing businesses and making payments across the world without consideration of geographical boundaries and trusted intermediaries. The business and research community has shown incredible interest in adopting Blockchain technology in the last decade. The following are the points to denote future of blockchain.

- Increased adoption among organizations
- A need for blockchain regulations
- Removing the negative speculations surrounding blockchain
- An increase in job opportunities for skilled personnel

XIX.CONCLUSION

To conclude, Blockchain is the technology backbone of Bitcoin. The distributed ledger functionality coupled with security of BlockChain, makes it very attractive technology to solve the current financial as well as non-financial business problems [10].

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability. Blockchain is a transformational technology, which provides a basis to develop distributed and secure applications for all industries beyond the monetary markets. Due to its vast and rapid applications development, it is envisaged that Blockchain will do for trusted transactions what the internet did for communications. This paper has provided a perspective to describe the Blockchain architectures in relation to crypto currencies, smart contracts and other applications. This could help to pave the way for researchers to carry out their researches in the Blockchain field.

REFERENCE

[1] R. Schollmeier, ''A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications,'' in Proc. 1st Int.

Conf. Peer to Peer Computer., Linkoping, Sweden, 2001, pp. 101–102.
[2] J. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Indianapolis, IN, USA; Wiley, 2008.
[3] B. Schneier, Applied Cryptography, Protocols, Algorithms and Source Code in C, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.
[4] L. Lamport, ‘‘Password authentication with insecure communication,’’ Commun. ACM, vol. 24, no. 11, pp. 770–772, Nov. 1981.