

An Analytical Study of Blockchain Technology

Dr. M. Kayalvizhi ^{#1}, U. Abhinaya ^{#2}

^{#1} Assistant Professor, Department of Information Technology, Sri Krishna Adithya college of arts and Science

^{#2} B.Sc IT Student, Department of Information Technology, Sri Krishna Adithya college of arts and Science

¹kayalvizhim@skacas.ac.in, ²abhinayaa0910@gmail.com

Abstract— Blockchain and cryptocurrencies are these big new things that change how we do digital stuff. They make systems that are spread out, easy to see through, and pretty safe without anyone in the middle controlling it all. I mean, blockchain is basically like a shared record book that keeps track of every deal or transaction forever, using some kind of code tricks and ways for everyone to agree on what's real. It gets rid of needing banks or companies to oversee everything. One main way people use it is with cryptocurrencies, you know, like digital money that lets you send cash directly to someone else. That makes things faster, safer, and you can trust it more, at least that's what it seems like. But it's not just about money. Blockchain pops up in all sorts of places, like with smart devices in the Internet of Things, or in hospitals for health records, finance stuff, tracking supplies in chains, cloud services, even how governments run things. It's kind of everywhere now. Still, there are problems with it. For one, it doesn't scale up well when too many people try to use it at once. Plus, it uses a ton of energy, which is not great for the planet. And getting different blockchains to work together is tricky, plus rules from governments are all over the place, not clear yet. Security is another worry, like attacks on the agreement process, bugs in those smart contracts, or losing control of your keys. This paper looks at the basics of blockchain, how the crypto side works under the hood with math and codes, the algorithms that make consensus happen, and some real examples out there. It also goes into the threats and ways to fight them back. Current trends in research are pushing to make it better, faster, more secure, so more people adopt it. I think with more tech improvements and solid ways to handle security, blockchain could really shake up how we build digital systems in industries like these. But it's not all figured out yet, some parts feel messy. *Abstract*

Keywords— *Blockchain, Cryptocurrency, Consensus Mechanisms, Cryptography, Smart Contracts, Security.*

(key words)

I. INTRODUCTION

Blockchain is based on a decentralized, unchangeable database that makes it simpler to record assets and keep track of transactions in a corporate network. An asset may be tangible or intangible. On a blockchain network, virtually anything of value may be stored and traded, reducing risk and improving efficiency for all users. Generally, a blockchain is a digital ledger of transactions that are being recorded. It is decentralized and is not controlled by any individual, group, or company [1]. As a structured technology, blockchain can be very difficult to change without the approval of the people who use it. Blockchain stores data as a decentralized ledger. Participants in this network can read, write, and verify transactions. Transactions cannot be modified or deleted. To support and secure the blockchain system, digital signatures, hash functions, and other cryptographic functions are used. These primitives ensure that transactions recorded in the ledger are integrity-protected and authenticated. This technology is called blockchain because new blocks are linked to older ones to form a chain. The first appearance of this term was a publication written by S.

Haber and W.S. Stornetta in 1991 [2]. In general, blockchain technology is credited to Satoshi Nakamoto, who developed the theory and implemented the technology in 2008 and 2009, respectively in the cryptocurrency Bitcoin, the most well-known blockchain application. Blockchain technology in recent years has attracted significant attention from academics and industries because of its advanced features. It can be applied to a variety of applications beyond cryptocurrencies. Blockchain technology has become a leading technology of internet interaction systems, including the Internet of Things (IoT) [3]. Our motivation in this paper is to inform and assist someone to become familiar with blockchain technology and its security issues, particularly for those who carry out transactions using blockchain technology and for researchers interested in developing blockchain technology and evaluating its security issues. To search publications and information on the Internet, the first step is to identify keywords such as blockchain, consensus algorithm, cryptography, cryptocurrency, and blockchain security. A second approach is to review papers that have been published in top conferences and journals that deal with blockchain. In this

paper, we provide the following main contributions:

- A detailed survey was conducted on blockchain technology.
- A systematic survey of Blockchain applications is conducted in this paper. 10 application areas are considered.
- Security and privacy issues were also addressed. Therefore, we encourage further efforts to survey and develop blockchain technology for widespread adoption. The rest of this paper consists of the following sections: In Section II, we provide an overview of the history of blockchain technology. A typical consensus algorithm used in the blockchain is described in Section III. In Section IV, we focused on blockchain applications. In Section V, we summarize the technical risks, attacks, and challenges of security in this area, and in Section VI, we conclude this paper.

II. EVOLUTION OF BLOCKCHAIN TECHNOLOGIES

Chaums PhD thesis from 1982 was kind of the first one to talk about something like a blockchain protocol. Then there was this paper by Haber and Stornetta in 1991, it was called How to Time-Stamp a Digital Document, and they went into how to cryptographically time stamp digital stuff [3]. I think that laid some groundwork.

Bit Gold came up in 1998 from Nick Szabo, he was trying to make this decentralized virtual currency early on. Even if it never really got built, people say its the basis for what Satoshi Nakamoto did with bitcoin later [4]. That connection seems pretty key.

Satoshi Nakamoto in 2008 is when modern blockchain really kicked off, I guess. He came up with this idea for direct payments online between people, no middleman needed. Instead of trusting someone, it used cryptographic proofs for the payments [5]. That paper changed things.

Ethereum showed up in 2013, bringing blockchain for smart contracts on a decentralized setup. Developers could build markets or handle transactions and funds based on code, all without intermediaries. Unlike Bitcoin which is more about currency, Ethereum lets companies make new apps that

go beyond money [6]. It feels like that opened up a lot.

The Ethereum platform launched in 2015, so now blockchain could handle loans and contracts too. Smart contracts are these algorithms that make sure actions happen between parties. Because its faster and safer, Ethereum got really popular quick. It lets different projects communicate through untrusted apps on its chain, leading to this Ethereum 2.0 idea [7].

Hyperledger got announced by the Linux Foundation in 2015, its open source for building blockchains. Aimed at enterprise stuff, different from Bitcoin or Ethereum. Blockchain draws interest for anonymity, but privacy is the bigger draw, I think. Like in the next section, there are applications in all sorts of industries.

Fig. 1 sums up the history of blockchain tech. Bitcoin and Ethereum are public since anyone can join. Hyperledger is private, permissioned, they check participants first.

Table I shows differences between Hyperledger and Ethereum, the two main ones.

Table.I

Comparison of Ethereum and Hyperledger

Parameter	Ethereum	Hyperledger
Purpose	Execution of smart contracts and decentralized applications	Enterprise-oriented blockchain framework
Network Type	Public blockchain	Private (permissioned) blockchain
Confidentiality	Transparent and open	Restricted to authorized participants
Governance	Ethereum developer community	Linux Foundation

Participation Model	Permissionless	Permissioned
Smart Contract Support	Supported	Supported using chaincode
Programming Languages	Solidity	Java, JavaScript, Go, etc.
Consensus Mechanism	PoW, PoS, and related mechanisms	Configurable consensus mechanisms
Transaction Speed	Relatively low	High
Application Domain	Public applications	Private and enterprise applications

the details yet. The stages' part stands out more to me right now.

B. MORE COMPONENTS OF BLOCKCHAIN

Node: A party involved in storing and processing blockchain information.

Ledger: A distributed, unalterable record accessible by all nodes

Hash Function: Maintains data integrity and security

Consensus Mechanism: Technique for reaching agreement on validity of blocks

Peer to Peer Network: It allows communication to take place among nodes

Cryptography: Protects transactions and user

Table.II

Layer-wise Comparison of Bitcoin, Ethereum, and Hyperledger Fabric

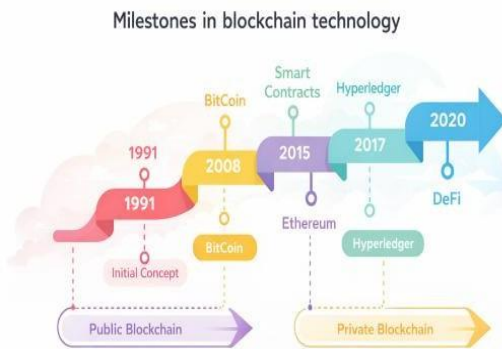


Fig. 3. Milestones in blockchain technology.

A. BLOCKCHAIN COMPONENTS

Blockchain stuff can be broken down into layers, I guess five main ones like application, network, contract, consensus, and data. That's from Table II or something. Melanie Swan talks about how it's gone through stages, the first being blockchain 1.0 with Bitcoin as the example. Then there's the second stage, blockchain 2.0, which is Ethereum.

Even with all these different ways to do it, the basic setup seems similar across them.

You have things like Bitcoin, Ethereum, Hyperledger, and so on in that category [8]. It feels like the layers help make sense of how they all fit together, but I'm not totally sure on

Layer	Bitcoin	Ethereum	Hyperledger Fabric
Application	Digital currency	DApps & smart contracts	Enterprise applications
Network	P2P over TCP	P2P over TCP	Permissioned (gRPC/HTTP)
Contract	Bitcoin Script	Solidity	Chaincode (Java/Go/JS)
Consensus	PoW	PoW / PoS	PBFT / SBFT
Data	Merkle Tree	Merkle Patricia Tree	Merkle Bucket Tree

"Consensus mechanisms: These are primarily the key part of the con Also known as sensus layer. At the contract layer, smart contracts are involved. There are numerous protocols available for data transfer and verification that are being utilized, such included in the network layer. Furthermore, it is relevant that in that it is a peer-to-peer network and the

blockchain is a prime example of lack a central node, but all linked by a planar topology[9]. It is possible to conduct business between any pair of nodes. A node in this network is free to join or leave at any time. A node in this network is free to join or leave at any time such as Bitcoin, Ethereum, and Hyperledger

C. Consensus Algorithms

Among many of the desirable characteristics of blockchain, with technology, it is now possible to determine the veracity of anonymous users when they enter transactions into the ledger. This is done by verifying each transaction for legality before the addition of the transaction to a block is allowed. Consensus algorithms are used to determine whether new blocks are added to the blockchain. This would help in gaining trust between parties using blockchain. System and to store transactions. Therefore, consensus algorithms are the backbone of all blockchain transactions in general.

Each participant has to follow a consensus protocol. There has been several consensus mechanisms that have been developed for blockchains.

This includes Proof of State, Delegated Proof of State, Proof of Work, Proof of Elapsed Time, Directed Acyclic Graph, and so on. Most commonly seen algorithms will be considered in Table III. Proof of Work (PoW): The goal of this algorithm is to determine a problem which has to be solved by guessing. Point being, PoW takes enormous amounts of electricity and thus, it is not practical to implement in real time and is rarely employed.

Proof of Stake (PoS): It stands at the second position in popularity as a consensus algorithm, while it requires fewer computations than PoW. It eliminates the problem of time and energy losses that PoW has been facing with. The consensus algorithm replaces the current method of reaching consensus in a distributed system instead of solving a Proof-of-Work. First cryptocurrency was Black Coin which use a PoS [12].

Proof of Elapsed Time (PoET): This is a consensus algorithm. It acts as an incentive for blockchain networks to help them keep the process more efficient. by avoiding overuse of resources and high-energy endowment. consumption. PoET resembles the proof of work method. PoW method but with less power consumption, since it is able to allow the processor to switch to other tasks after a certain period of time and, hence, less consumption of energy, which raises efficiency [13].

Byzantine Fault Tolerance (BFT): It is targeted at solving problems where there are untrusted parties, but they need reach a consensus. PBFT is designed to enhance BFT. Considering PBFT, within the case hostile nodes represent less than thirty percent of all nodes, then the state of the blockchain will be agreed upon. Agreed upon by all participants. Blockchain systems are more secure it becomes very complex when many nodes are involved. Presently, Hyperledger Fabric is based on PBFT [14].

Direct Acyclic Graph (DAG): It contains vertices and edges, with which it differs from various consensus algorithms. By vertices of the, there are represented transactions structure. A block is not referred to in this algorithm, nor do Transactions can be added using a mining process. Each transaction is built upon the previous one rather than being grouped into a block. Various applications of DAG technology can be found in fields requiring high speed and no fees Connected devices are integral parts of everyday life: like the Internet of Things - IoT [15].

D .Blockchain Cryptography

Blockchains offer confidential and secure transactions. anonymous parties. This could include a trust developed through cryptography, thereby eliminating the need for centralized institutions. By employing cryptography, blockchain information is made End on the ledger. Building blocks of cryptography are used in blockchain technology as follows: Public Key Cryptography: Designed to create digital sign and encrypt data.

Zero-Knowledge Proof: Prove that you know a secret without disclosing the same.

Hash Functions: A mathematical function that generates a fixed-size string of characters for any given input. generates pseudo-random numbers.

1. Public-key cryptography makes it possible to prove that a transaction by: to have been created by the right user by this method. Employing a

With the use of a private key, a user is able to sign a message (so-called digital signature. Digital Signatures in Hyperledger & Ethereum transactions ensure verification of authenticity from the sender .And that information has not been amended since it was signed. The algorithm, ECDSA in full is widely used to generate a combined set of private and public keys.

2.Zero-knowledge proof mainly refers to when Users request to transfer funds to other users. At the end For the blockchain to verify a transaction, it must confirm that the participant of the transaction who is transferring funds has enough to complete it.

3.Hash functions: Hash Functions: Hash functions form The unique configurations of the blockchain make it vital technology. There are five properties of a hash function that are essential to cryptography[18]:Fixed size: it can take any input using the hash function, and This will create the output of a fixed size. To provide digital Whereas signatures take blocks of information and use hash functions to reduce them to a fixed-size message digest, Messages.

Preimage resistance: It should not be feasible to determine an input from any given set of inputs challenging in generating a hash result. However, the reverse Engineering the original input is mathematically impossible based on the hash output. The only way to achieve the same A result is to randomly choose data that should be entered into the hash algorithm.

2nd preimage resistance: It is a resistance to get a second input such that provides the same hash result is impossible given an input and the hash result of it. Collision resistance: No two different hash inputs can produce the same output. produced

from two different inputs. Big change: A completely different hash output will be produced if any single bit is changed in the input.

III. APPLICATIONS OF BLOCKCHAIN

As reported in the survey, blockchain technology has applications in cryptocurrency, Internet of Things (IoT), finance system, healthcare, security and privacy, advertising, copyright protection, society applications, energy, mobile applications, Defense, digital records, supply chain, digital ownership management, automotive, intrusion detection, agricultural sector, voting, identity management, education, law and enforcement, property title registration systems, asset tracking systems and so on [19]. An practical example of the spiraling applications of blockchain can be shown in Figure 2.

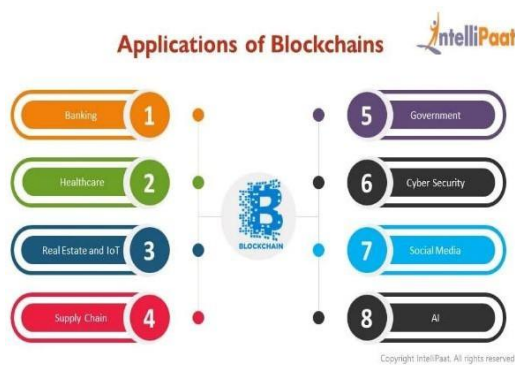


Fig. 2. Application of blockchain

Applications of Blockchain Technology:

Cryptocurrencies & Digital Payments: Bitcoin, Ethereum, and other Cryptocurrencies. Facilitates peer-to-peer transaction without an intermediary.

Supply Chain Management: Tracing products from producer to consumer
 Reads: Ensures transparency and prevents counterfeits.

Financial Services and Banking: Cross-border payments, remittances, and settlements . Smart contracts for automated lending and insurance .Reduces dependence upon central authority figures.

Healthcare & Medical Records: Patient date transmission between hospitalsand clinics securely .Immutable audit trails for medical histories . Protects confidentiality and prevents errors.

Internet of Things (IoT): Encryption of communication and data transfer among devices. Reduces risk of Hacking in Connected Devices

IV. BLOCKCHAIN NETWORK SECURITY: THREATS AND MEASURES

A. THREATS :

Blockchains are distributed, so it makes sense to carry out studying the security issues. In this section, we shall discuss the security threats posed by this technology. In order to gain a clear understanding of the security of blockchain, to always essential to first understand the differences between the private and public blockchain security, especially data access capabilities, as we have pointed out earlier. "The following are the most important issues related to" blockchains [30]

Sybil Attack: In the Sybil attack, multiple bogus or illegitimate nodes are created by hackers. Using the nodes, it will be able to gain the majority's agreement and interrupt Transactions.

Endpoint vulnerabilities: An important consideration in the "Security of blockchain is the vulnerability of endpoints. Elec" electronic devices such as mobile phones and computers that are used to communicate with the blockchain network. Watching the behave identification of users and targeting their devices will enable hackers to steal the user's key. Maybe this is among the most visible security issues related to the technology of blockchain.

51% Attack: In 51% attack, the attacker is either a user or "The institution controls half of the hash rate and holds keys for the entire system". The transactions can be manipulated by the hackers and prevent them from being confirmed. They'll even reverse "all decisions previously made by this president transactions that are already completed, resulting in twice spent.

Phishing attacks: These are phishing attacks that are intended for the theft of user credentials. An email will be sent to the owner of the wallet key that looks to be genuine. A false hyperlink is linked to email requiring entry of login details from a user. It is accessed by the gaining access to the user's credentials and personal data, there could be damage caused to the user and the blockchain network as a whole.

Routing Attacks: In this type of attack, usually unaware of the threat, since the transmission of data and the conduct of operations remains business as usual. There is a possible danger is that such attacks could disclose sensitive information or gen charge revenue illegally without the user's consent. There is a critical hoc reliance on the movement in real time of enormous amounts of Data extracted from: "A Billion-Screen World information within a blockchain application and network. Because the anonymity of an account, the hackers may be able to intercept information transmitted to internet service providers by using it.

B. MEASURES:

So far, to secure blockchain applications, security must be considered at all layers, including permission management through several security measures [20]. The following are Some of the Security measures of blockchain include:

Blockchain governance: Identifying how existing or means that as organizations or users either join or leave the network, the programs using TCP/IP make the adjustments. preventing mechanisms against malicious actors, errors, securing data, and resolve disputes between parties.

Data security: Although data compression is generally considered to be the best way to find out what information Some data, such as medical records, should be kept on-chain ;additional privacy measures should be implemented in order to hash data, cloud storage, and data in motion.

Security of a blockchain network: Blockchain is a distributed network, so nodes should be able to adjust dynamically .Distributed system which involves network connections from various enable various stakeholders from other than one organization to share information. All these factors have the potential to introduce security exploits or defects. Governance, consequently, involves examination of security protocols for users [21].

Security Applications: This involves blockchain application security are weak points and should be guarded with effective User Identification and Endpoint Security. For private blockchains, where permissions and utilization are strictly used and/or granted to authorized participants may require different levels of authorization that might change over time.

Smart Contracts: Security-issue smart contracts include set of coded rules within the blockchain, triggered by a set of Programmed conditions. This presents another point of vulnerability since it is their reliability that determines whether the operation and the results are reliable.

IV. CONCLUSION

In recent years, the field of blockchain technology has attracted a lot of attention because of its very advanced characters characteristics of decentralization, autonomy, integrity, immutability verification, and fault tolerance .,“The first and foremost concern will be addressing security issues,” originating from different types of blockchain networks. Furthermore, consensus protocol like PoW based on blockchain has some demerits. Thus, the creation “of a consensus algorithm that is more efficient” will happen because cheaper blockchain networks. This survey intro presents an overall view of what blockchain technology. A brief A historical background of blockchain technology was discussed, followed by a comparison of the commonly used consensus algorithms . There has been discussed at length the topic of public key cryptography and hash functions used in

the blockchains are applicable in security, identification, as well as non- repudiation reasons. it offers extensive details on the comparison between some of the cryptocurrencies that were used in the blockchain. Additionally, we note that on various categories of top security risks associated with blockchain technology. Finally, through this effort, we also hope that they will gain a greater understanding of blockchains technology. In addition, we hope that more attention will be given by individuals to the safety of the blockchain.

REFERENCES

- [1] Kumar, S., Kumar, A., and Verma, V. (2019). A survey paper on blockchain technology, challenges and opportunities. *Int. J. Comput. Trends Technol.(IJCTT)*, 67(4), 16. ISO 690
- [2] Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document (pp. 437-455). Springer Berlin Heidelberg.
- [3] Zheng, Z., Xie, S., Dai, H. N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, 14(4), 352-375. ISO 690
- [4] R. Sharma, Bit gold, Investopedia, 2021. Available online: R. Sharma, Bit gold, Investopedia, 2021. Available online: <https://www.investopedia.com/terms/b/bit-gold.asp>.
- [5] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>, October 2008.
- [6] Vujić, D., Jagodić, D., & Randić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th international symposium infotech- jahorina (infotech)* (pp. 1-6). IEEE.
- [7] A. Groetsema, A. Groetsema, N. Sahdev, N. Salami, R. Schwentker, F. Cioanca, *Blockchain for Business: an Introduction to Hyperledger Technologies*, The Linux Foundation, 2019
- [8] Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, 8(2), 23-29. ISO 690
- [9] Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In *Journal of Physics: Conference Series* (Vol. 1168, No. 3, p. 032077). IOP Publishing.
- [10] Chaudhry, N., and Yousaf, M. M. (2018, December). Consensus algorithms in blockchain: comparative analysis, challenges and opportunities. In *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 54-63). IEEE. ISO 690
- [11] Nguyen, G. T., and Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information processing systems*, 14(1), 101-128. ISO 690
- [11] Nguyen, G. T., and Kim, K. (2018). A survey about consensus algorithms used in blockchain.

- Journal of Information processing systems, 14(1), 101-128. ISO 690
- [12] Saad, S. M. S., & Radzi, R. Z. R.M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, 10(2).
- [13] J. Frankenfield, Proof of Elapsed Time (PoET) (Cryp tocurrency), Invest, October 16, 2020. Available online: <https://www.investopedia.com/terms/p/proof-elapse>
- [14] Zhang, Z., Zhu, D., & Fan, W. (2020, December). Qpbft: practical byzantine fault tolerance consensus algorithm based on quantified-role. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 991- 997). IEEE. ISO 690
- [15] Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. *arXiv preprint arXiv:2001.07091*. ISO 690
- [16] Khan, S.N., Loukil, F., Ghedira- Guegan, C. et al. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Netw. Appl.* 14, 2901–2925 (2021).
- [17] R. Santos, K. Bennett, E. Lee, *Blockchain: Understanding its Uses and Implications*, The Linux Foundation, 2021. Available online: <https://www.edx.org/course/blockchain-understanding-its-uses-and-implications>.
- [18] R. Santos, K. Bennett, E. Lee, *Blockchain: Understanding its Uses and Implications*, The Linux Foundation, 2021. Available online: <https://www.edx.org/course/blockchain-understanding-its-uses-and-implications>.
- [19] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., and Rehmani, M. H. (2018). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, 21(2), 1676-1717.
- [20] Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. *Blockchain: Research and Applications*, 3(2), 100067.
- [21] D. Wang, J. Zhao and Y. Wang, "A Survey on Privacy Protection of Blockchain: The Technology and Application," in *IEEE Access*, vol. 8, pp. 108766-108781, 2020, doi: 10.1109/ACCESS.2020.2994294.

