Blockchain Architecture to Support Recent Trends in Technology

Pankaj Kumar Singh[1], Rahul Biswas[2], Anirban Bhar[3], Shyamapriya Chatterjee[4]

[1,2] *B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*
[3,4] *Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*

ABSTRACT

The blockchain technology that served as Bitcoin's model has recently attracted a lot of interest. A decentralized ledger that is immutable, the blockchain enables transactions to be recorded. Applications based on blockchain are emerging in many industries, including financial services, reputation management, Internet of Things (IoT), etc. But there are still a lot of difficulties with blockchain technology to be solved, including issues with scalability and security. This study provides a thorough understanding of blockchain technology. After providing a brief overview of blockchain architecture, we contrast a few common consensus methods used by various blockchains. Additionally, recent advancements and technological problems are briefly listed. The future must be blockchain. To maximize the advantages of blockchain systems, technological choices must be made at the design phase. The review gives guidance to the new blockchain research and the proposed unique framework enables a structured technique for resolving key technical design decisions for optimizing the benefits of blockchain systems in project management.

Keywords: - *Blockchain Technology, Decentralization, Consensus methods, Design phase.*

1. INTRODUCTION

The basic definition of Blockchain is a knowledge system that preserves transactional records while promoting decentralization, security, and transparency. You can alternatively conceive of it as a collection of records kept in different kinds of blocks that are not under the control of a single authority. A distributed ledger known as a blockchain may be open to use by anyone on the network. Once data is stored on a blockchain, it is very challenging to alter or change it. On a blockchain, each agreement is protected by a digital signature that attests to its validity. The data saved on the blockchain is tamper-proof and unchangeable because of the use of encryption and digital signatures. Blockchain technology enables the network's participants to reach consensus, often known as an agreement. Every piece of information kept on a blockchain is digitally recorded and has a shared history that is made available to all network users. This eliminates the possibility of any fraudulent activity or transaction repetition without the need for a third party. To further understand blockchain, imagine that you're looking for a way to send some money to a friend who lives somewhere else. A bank or a payment transfer service like PayPal or Paytm are two common options that you can typically employ. With this option, the transaction is processed by third parties, resulting in a further deduction from your funds as a transfer fee. Additionally, in situations like these, you cannot be certain that your money is secure because a hacker could interrupt the network and take your money. It was the customer who suffered in both scenarios. Blockchain might be useful in this situation. In these situations, using a blockchain to transfer money instead of a bank makes the process considerably simpler and more secure. there is no additional cost because you process the funds directly, doing away with the need for a third party. Additionally, as the blockchain database is decentralized and not restricted to a particular location, all information and records stored there are both public and decentralized. No danger of data tampering by a hacker exists because the knowledge isn't kept in a single location.

2. LITERATURE REVIEW

The term "cryptocurrency" has recently gained popularity in both business and academics. Bitcoin has been one of the most successful cryptocurrencies, with its capital market surpassing $10 billion in 2016 [1]. The key technology used to develop Bitcoin is blockchain, which was first proposed in 2008 and implemented in 2009 [2]. With a specially built data storage structure, transactions in the Bitcoin network could occur without the involvement of a third party. All committed transactions are recorded in a list of blocks on the blockchain, which might be thought of as a public ledger. This chain expands as additional blocks are consistently added to it. For user security and ledger consistency, asymmetric cryptography and distributed consensus algorithms have been used. Decentralization, persistency, anonymity, and auditability are four essential properties of blockchain technology. Blockchain can significantly reduce costs and increase efficiency because to these characteristics.

Blockchain can be utilized in a variety of financial services, including digital assets, remittance, and online payment, because it enables payment to be completed without the use of a bank or other middleman [3], [4]. The Internet of Things (IoT), smart contracts, public services, reputation systems, and security services are just a few additional areas where it can be used. These industries benefit blockchain in a number of ways. Blockchain is firstly unchangeable. Once a transaction is stored in the blockchain, it cannot be altered. Blockchain can be used by companies that need to be highly dependable and honest to draw clients. Additionally, because blockchain is distributed, it can prevent single points of failure. When a smart contract is deployed on a blockchain, miners may automatically carry out the contract's terms.

Although the blockchain technology offers a lot of potential for the development of future Internet services, there are a number of technical difficulties it must overcome. Scalability is a major concern, to start. A block of bitcoin can only be 1 MB in size right now, and one is mined every 10 minutes or so. As a result, the Bitcoin network can only process 7 transactions per second, making it unable to handle high frequency trading. Larger blocks, however, require more storage space and propagate more slowly over the network. As fewer people are willing to maintain such a big blockchain, this will gradually lead to centralization. Therefore, balancing block size and security has proven to be a difficult task. Second, it has been demonstrated that selfish mining tactics can result in miners earning more money than is fair [10]. To generate more money in the future, miners conceal their extracted blocks. In that case, branches might happen frequently, which would slow down the development of the blockchain. Therefore, some remedies must be proposed in order to resolve this issue. Additionally, it has been demonstrated that privacy leaking can occur in blockchain even when users only utilize their public key and private key for transactions [11]. Additionally, there are several significant issues with current consensus techniques like proof of work and proof of stake. For instance, the proof of stake consensus process may reveal the anomaly that the affluent get richer while proof of work wastes excessive amounts of power energy.

Numerous sources, including blogs, wikis, forum postings, codes, conference proceedings, and journal articles, have a wealth of information on blockchain. A technical study on decentralized digital currencies, such as Bitcoin, was conducted by Tschorsch et al. [12]. Our study differs from [12] in that it focuses on blockchain technology rather than virtual currencies. Blockchain was the subject of a technical report from Nomura Research Institute [13]. Unlike [13], our study is focused on cutting-edge blockchain research, encompassing current advancements and emerging developments.

3. BLOCKCHAIN ARCHITECTURE

An open financial ledger or record called a blockchain is where every transaction is verified and approved. A blockchain is intended to function as a decentralized network of millions of computers, or "nodes," as they are usually known. It is a distributed database design in which every node assumes the function of an active network administrator. A blockchain is virtually impossible to hack since there is no centralized information in its architecture. The blockchain architecture supports blocks, which are expanding collections of ordered records. Each block keeps a connection to the preceding block and a timestamp.

Fig -1: Blockchain Networks

The key elements of a blockchain architecture are listed below:
Node: Within the blockchain architecture, a node is a computer (each node has an independent copy of the entire blockchain ledger)
Transaction: A data record that is confirmed by blockchain users and acts as a nearly unchangeable certification of the legitimacy of a financial transaction or contract.
Block: An encrypted data container that houses a native hash code to identify it, a hash code from the block before it in the chain of blocks, and a series of time-stamped transactions.
Chain: An arrangement of building blocks
Miners: The nodes known as miners are responsible for validating blocks before adding them to the network.
Consensus: A set of guidelines and agreements for carrying out blockchain operations is known as a consensus (protocol).

The blockchain architecture provides numerous advantages for businesses. Here are some inherent qualities:
Cryptography: Due to intricate calculations and cryptographic proof between the participants, blockchain transactions are trusted and validated.
Immutability: A blockchain prohibits editing or erasing records.
Provenance: Each transaction's origin may be found on the blockchain ledger.
Decentralization: Access to the complete distributed database is available to every member of the blockchain structure. In contrast to centralized systems, a consensus mechanism controls the network.
Anonymity: Instead of a user ID, every participant in the blockchain network has a created address. This protects user privacy, particularly on a public blockchain.
Transparency: Since entirely rewriting the blockchain network requires a lot of computer power, the blockchain system is unlikely to be harmed.

The three types of block chain architecture are:

3.1 Public blockchain architecture

A public blockchain architecture uses the right protocols and operates on the basis of proof-of-work (PoW) consensus algorithms. Being open-source, a public blockchain doesn't require any authorization. Being open-source, you can define new blocks using their current states. Additionally, you can download a blockchain's source code and examine network transactions.

This enables transactions throughout the network. An open blockchain architecture enables transactions that are transparent but pseudonymous or anonymous. Blockchains for Bitcoin, Ethereum, and Litecoin are open to the public.

3.2 Private blockchain architecture

Information can only be accessed by a certain participant group (of businesses or individuals) in a private blockchain architecture. Organizations create such blockchain systems in an effort to boost overall efficiency or benefit. The participants' shared objectives, as well as the Byzantine fault tolerance (BFT) and proof of stake (PoS) consensus procedures, ensure their dependability.

The primary blockchain protocol and the smart contract layer are separated by a private blockchain architecture. You can access online markets and a programmable transaction area known as a smart contract using a private blockchain.

3.3 Consortium blockchain architecture

Additionally, a public permissioned or consortium blockchain architecture exists. Anyone can connect to and observe the blockchain in this type of blockchain architecture, but a participant can only upload data or join a node with the consent of other participants. Such blockchains are developed by organizations in an effort to boost consumer or societal trust. The same PoS and BFT consensus techniques are used in this case, and they help to achieve reliability.

4. BLOCKCHAIN DECISION FRAMEWORK

Based on the review's results, a decision framework is created. The framework's major goal is to maximize the blockchain's advantages while minimizing its drawbacks for a particular project management application. The proposed framework takes into account the block-alleged chain's qualities and benefits as well as its contributions to project management. The framework takes into account choices regarding decentralization, privacy, flexibility, transparency, efficiency, transaction costs, use of standard programming languages, development of the blockchain platform, market capitalization of the employed cryptocurrency, and the requirement for a potent smart contract engine. The framework specifies the primary application category for project management and takes into account choices made in relation to information management, payments, and contract management.

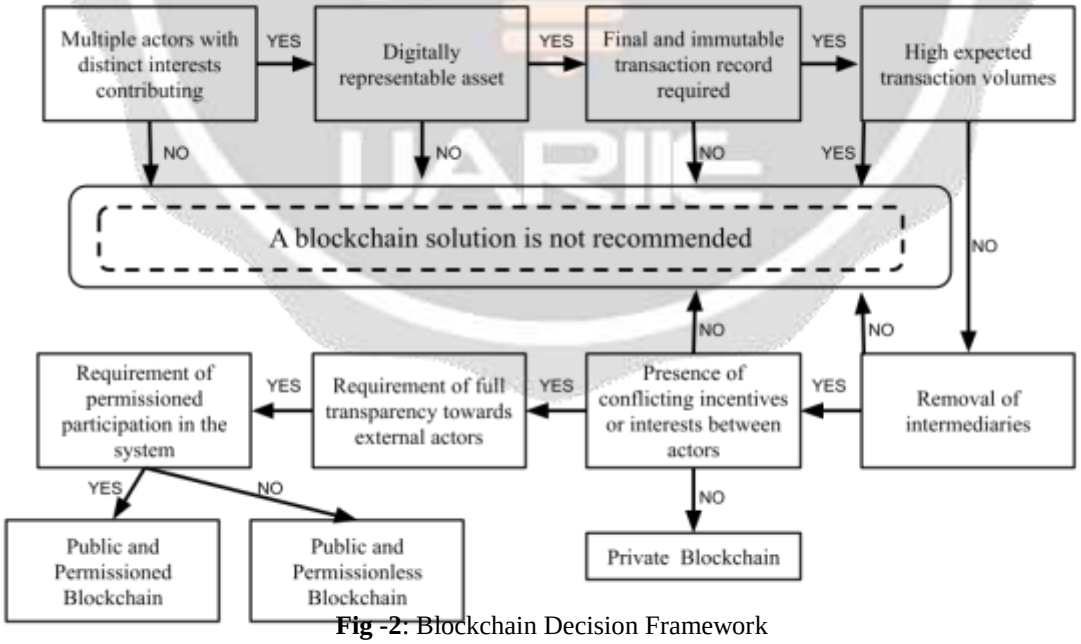

Fig -2: Blockchain Decision Framework

As shown in Fig-2, the framework begins by determining if the application requires cryptocurrency transactions. Payments is the application's primary domain category if cryptocurrency transactions are required. Only public blockchain and hybrid blockchain platforms are taken into account in the payments category because only public

platforms currently support bitcoin transactions. According to the demand for privacy, the first decision is made for the payments category. Hybrid-Ethereum platform is chosen if privacy is required. The second choice in the payments category is related to the magnitude of the transactions if privacy is not necessary. Due to its significant market capitalization of Ether, the Public-Ethereum platform is advised if the application will be used to conduct massive cryptocurrency transactions. A decision is made between the Public-EOSIO (efficiency and low transaction costs) and Public-Ethereum (mature and potent smart contract engine) platforms if the application won't be used to conduct massive transactions.

The framework then takes guaranteed contract condition execution into account. Although private and consortium blockchains can also be used to program smart contracts, only public blockchains can ensure that they are executed because the organization or consortium administering the blockchain can readily change the smart contracts. On public blockchains, on the other hand, smart contracts are guaranteed to be executed and cannot be changed once they are deployed on the blockchain. The primary domain category is considered to be contract management if the application requires guaranteed execution of contract conditions. The privacy need is the first issue to be decided in the contract management category. A hybrid Ethereum platform is advised if the contract management application needs privacy, as this hybrid option might guarantee privacy and smart contract execution. The features of efficiency and cheap transaction costs (Public-EOSIO), or maturity and the necessity for a potent smart contract engine, are chosen if privacy is not necessary (Public-Ethereum).

The principal domain category in the architecture is characterized as information management if the application does not require cryptocurrency transactions or guaranteed fulfilment of contract terms. Based on the degree of decentralization needed for the application, the first choice in the information management category is chosen. Decentralized governance should be chosen if complete decentralization is necessary to ensure transparency, dependability, immutability, traceability, authenticity, and self-execution qualities. The level of privacy is the next choice for an information management application that needs decentralized governance. A hybrid blockchain alternative is included in the proposed framework, allowing for fine-grained control over the decentralization and privacy aspects for a given application. Hybrid-Ethereum platform should be utilized if a portion of the application demands complete decentralization and privacy as well. One can choose between the Public-EOSIO or Public-Ethereum when full decentralization and transparency are desired. Based on the characteristics of consortium platforms, a decision is taken as to whether governance at the consortium level is more appropriate for the information management application. When efficiency and the use of general programming languages are essential, Consortium- Hyperledger should be employed. When a stable platform with a potent smart contract engine is required, Consortium-Ethereum should be chosen. Decentralization may not be preferred in all blockchain applications for information management, so a decision should be made between the Private-Hyperledger and Private-Ethereum platforms.

5. BLOCKCHAIN FUTURE TRENDS

As a result of the efforts of numerous IoT Solution development organizations, there has been a cyclical increase in the number of virtual approaches and technologies that are increasing our level of living today. Blockchain is seen as one of the most cutting-edge technologies with a promising future in this context.
According to experts, the gadget advances cyber-security while also greatly enhancing human activities. It's crucial to first comprehend blockchain in order to properly understand the connected blockchain trends.
A new technology by the name of blockchain is becoming more well-known as the bitcoin market expands. Literally speaking, "blockchain" would be the term. Blockchain differs from conventional databases in that the database cannot be updated or deleted. The foundation of blockchain methodology and technology is the idea of a distributed ledger.

A blockchain's security is ensured via cryptography, which also allows network users with private keys to execute any transactions they want. The network is not at risk of failing because the information won't disappear. It is considered to be quite secure. The data can be recovered and used in numerous situations if necessary.

Global spending on Blockchain infrastructures is anticipated to reach $11.7 billion by 2022. This article will examine the top Blockchain trends for 2022 as well as how various techniques effect Blockchain IoT solutions over time.

5.1 It is simpler to manage and distribute immunizations

By 2022, it is anticipated that blockchain technology would manage and track the efficient supply of vaccinations going straight from manufacturers to patients. This accomplishment will lessen the challenges posed by blockchain currency. The system makes sure that location changes and transportation records are recorded. The IoT blockchain revolution will address issues at every level and guarantee authenticity all the way through.

5.2 National cryptocurrencies are rising in acceptance

All throughout the world, governments must acknowledge the advantages of currencies based on the Blockchain. During the creation of Bitcoin, a number of nations expressed skepticisms on the precise application of cryptocurrencies.

By 2022, the market for Blockchain technology is predicted to generate $20 billion in revenue. We remain optimistic that by 2022, some parts of the world will have fully adopted Blockchain-based currency, despite the fact that some countries, like China, have placed restrictions on bitcoin and other Blockchain transactions.

5.3 Blockchain technology is being adopted by government organizations

Among public servants, the idea of a distributed ledger is gaining ground. They intend to use various Blockchain IoT services as a result by 2022. The databases that each agency has nowadays make it necessary to have up-to-date information on the population. For improved data management, these agencies will certainly use the best Blockchain technologies.

In decentralized digital ledgers, information on people and the area's residents is kept. Additionally, the system can use two-factor authentication and powerful encryption technology to boost security measures and give users control over their data.

5.4 Incorporating NFTs and digital archives into the Blockchain network

Thanks to the development of the NFT marketplace, users can now stake a claim to ownership of a digital asset. Additionally, it is simpler to get more data about a user, which has an immediate impact on the pricing structure of the blockchain sector. Currently, more than 60% of the market value of Blockchain is derived from the financial industry.

NFTs (non-fungible tokens) preserve the artistic legacy and track who owns the automobiles, real estate, and other assets, making it easier to keep track of information about prior owners. The technique is becoming more and more popular, and many people prefer it over the cumbersome, antiquated methods that involve waiting.

5.5 Using blockchain technology to accomplish social and political goals

The usage of Blockchain in social and political activities is one of the most exciting parts of the technology's future predictions. Bitcoin has already shown promise as a potential method for assuring the change of digital rights management, according to current blockchain developments. It can lessen instances of identity theft and aid in supply chain management.

After that is established, 2022 blockchain trends will concentrate on using blockchain capabilities to boost transparency and trust.

5.6 The overall status of the economy is shifting

Recent predictions predict that the adoption of blockchain wallet technology will provide enormous economic growth by 2022. International corporate representatives are certain that Blockchain IoT solutions will help with the renewal and reorganization of their organizations. It paves the stage for a new era to run more smoothly and successfully.

5.7 The use of blockchain technology in the service industry

Several sizable businesses, like Microsoft and Amazon, have already started utilizing Blockchain IoT services. The websites will be made specifically for business owners that are proficient with technology and eventually use it as a service. This means using resources without making an investment in tools, training, or expertise.

Thanks to technological breakthroughs, we can now create entirely decentralized and self-contained systems and objects. In everyday life, ideas are consequently immediately presented and actively developed.

6. CONCLUSIONS

This paper's research and application benefits are dual. The paper first presents a review of the scholarly literature in the field, creates a taxonomy of blockchain application domains, and analyses the blockchain's major contributions to achieved pricing management. In order to maximize the benefits of blockchain applications for project management, the study that supported their discovery then proposes a blockchain call framework. According to the examination of employment situations, blockchain technology has considerable promise for fostering trust, improving communications, lowering disputes and claims, and preventing fraud in project management, particularly in data management and payments. The benefits and attributes of blockchain, however, depend on technological decisions for a particular application.

One of the most cutting-edge virtual technologies in the world, the blockchain IoT solution is gaining traction across a range of industries, including technology, aerospace, automotive, and finance.

In this domain, there have been breakthroughs in the functionality and functioning of international economic systems. Blockchain can help experts think through a variety of challenging problems, despite the fact that the virtual design was previously erroneous.

7. REFERENCES

[1]. “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016.
[2]. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[3]. G. W. Peters, E. Panayi, and A. Chapelle, “Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective,” 2015.
[5]. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in Proceedings of IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
[6]. B. W. Akins, J. L. Chapman, and J. M. Gordon, “A whole new world: Income tax considerations of the bitcoin economy,” 2013.
[7]. Y. Zhang and J. Wen, “An iot electric business model based on the protocol of bitcoin,” in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.
[8]. M. Sharples and J. Domingue, “The blockchain and kudos: A distributed system for educational record, reputation and reward,” in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490–496.
[9]. C. Noyes, “Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning,” arXiv preprint arXiv:1601.01405, 2016.
[10]. I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436– 454.
[11]. A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in bitcoin p2p network,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 2014, pp. 15–29.
[12]. F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Sur- veys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.
[13]. NRI, “Survey on blockchain technologies and related services,” Tech. Rep., 2015.