IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Applications of Blockchain Technology in Government Sector: Survey

E-Government

[1]Asharani A. Patil, [2]S. S. Sannakki, [3]V. S. Rajpurohit, [4] Prakash K. Sonwalkar

[1]Student, [2]Associate Professor, [3]Head of the Department (HOD), [4]Associate Professor
[1,2,3] Department of Computer Science &Eng
[4] Department of Computer Science
[1,2,3] KLS Gogte Institute of Technology, Belagavi, Karnataka, India
[4] Jain College of Engineering and Research, Belagavi, Karnataka, India

Abstract : The blockchain serves as the foundational technology utilized by cryptocurrency developers, including Bitcoin, to facilitate the seamless exchange of digital assets among participants without the need for a centralized intermediary, typically provided by governments. Over time, Blockchain has undergone significant evolution, transforming into a versatile solution for storing and processing data in an exceptionally decentralized and impregnable manner. Other than cryptocurrency, blockchain technology finds versatile use in various sectors such as financial and social services, healthcare facilities, risk management, and many others. This paper presents the study of the Utilization of Blockchain Technology in Government Services and discusses challenges.

***IndexTerms* - blockchain technology, e-government,**

I. Introduction

INTRODUCTION

A blockchain is an innovative technology that links multiple blocks of information in a decentralized, traceable, and immutable manner. Unlike conventional approaches, it enables the direct exchange of digital assets between peers, bypassing the requirement for intermediaries [1]. In 2008, Satoshi Nakamoto created the blockchain as a decentralized public ledger designed for recording Bitcoin cryptocurrency transactions. Since its inception, the blockchain has witnessed tremendous growth in the capital market. Essentially, the blockchain contains a chain of blocks, securely storing all verified transactions using a publicly accessible ledger. The chain's growth is perpetual, with the continuous addition of new blocks. Each block securely preserves the hashed data of every transaction, along with the hash of the previous block, thereby creating a ledger known as the blockchain. This ledger empowers a user community to collaboratively document transactions, assuring their unalterable status once incorporated into the blockchain [2].

Blockchain technology holds the capacity to revolutionize government services, fostering greater efficiency, security, speed, and trustworthiness within government bodies. Through the implementation of blockchain-based digital government, the decentralized system becomes apparent in every public interaction. Through blockchain-based digital government, citizens can experience seamless interactions with various government services. Whether it's for identity verification, voting, or accessing public records[2]. Blockchains have become a prominent topic in global news, with their widespread adoption across diverse domains as decentralized solutions for fraud-resistant computing, all without relying on a trusted central authority.

This survey paper primarily focuses on providing an overview of blockchain technology and its architecture, characteristics, as well as its applications in government services. It also addresses the challenges linked to the implementation of this technology. The key contributions of this research encompass a concise summary of the benefits that blockchain technology offers to the government sector. Moreover, this study delves into the obstacles faced during the integration of this technology. The subsequent sections of this survey paper are organized in the following manner.

Section II offers an overview of blockchain architecture and its Overview. Section III presents various blockchain technology for government sectors. Section IV introduces several challenges encountered in blockchain technology. Finally, Section V offers the conclusion of the paper.

OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND ARCHITECTURE

Blockchain architecture is a revolutionary framework designed to establish a decentralized ledger for safeguarding digital data. By leveraging cryptographic techniques, this groundbreaking innovation ensures the integrity and immutability of all records. Essentially, a blockchain constitutes an ever-expanding series of interconnected records, or blocks, forming a secure and transparent network [3]. The fundamental contrast between a blockchain and a conventional database resides in their data storage methods. Unlike typical databases that store raw data directly, encrypted data is interlinked within blocks in a blockchain. While transactions within a blockchain are represented as cryptographic strings, the true value of the data arises from the secure and sequential interconnection of these blocks. This interdependence guarantees the credibility, immutability, and transparency of data, establishing the blockchain as a robust and trusted system with diverse applications [2] [11].

A block is comprised of two main components: the block header and the block body. The header includes a hash value and a hash reference that directs to the hash of the preceding block, creating a chain between blocks. This initial block is called as the Genesis block and holds a constant value, being the first block in any Blockchain. Since there is no block before it, the previous hash is hardcoded as '0'. Subsequent blocks in the Blockchain store all the data, with each block's hash reference pointing to the hash value of the Genesis block in the "previous hash" section. This interconnected structure forms the foundation of the Blockchain system. Hashing is a process of converting input data, regardless of its length, into a fixed-size string through a designated algorithm. In the case of Bitcoin uses SHA 256 and Ethereum uses Keccak-256 algorithms respectively. This hashing mechanism plays a crucial role in ensuring data integrity, security, and the linkage of blocks in the blockchain network.

Digital signatures are exceptionally difficult to forge due to their foundation in number theory. In the realm of "public key cryptography," users possess a unique pair of keys—a public key and a private key. The public key is openly shared, while the private key is kept confidential. This cryptographic method employs encryption techniques to ensure robust security and safeguard sensitive key information, making it highly reliable for authenticating and verifying digital signatures. Digital signatures play a crucial role as a foundational element in blockchains, primarily serving to authenticate transactions. When users initiate transactions, they need to demonstrate to each node within the system that they possess the authorization to spend the designated funds, while simultaneously preventing any unauthorized access by other users. This procedure engages each node within the network in the validation of the submitted transaction. It entails cross-referencing the efforts undertaken by all nodes to attain a unanimous agreement on the precise status of the blockchain. This resilient verification mechanism employed by blockchains guarantees the comprehensive security and unswerving integrity of the entire network.

2.1 Types of Blockchain

2.1.1 Public Blockchain: This blockchain is publicly accessible, meaning it is open to anyone without any ownership restrictions. The system operates in a decentralized manner and allows users to input and access data freely.

2.1.2 Private Blockchain: Unlike the fully public blockchain, these blockchains are not as decentralized since only specific nodes are granted permission to participate in the validation process. This selective approach enhances security compared to other blockchain types. These blockchains operate within a closed network, providing access only to authorized users.

2.1.3 Hybrid Blockchain: It is a fusion of private and public elements, with certain segments under the control of specific organizations, Meanwhile, other components are made accessible as a public blockchain. This integration involves both permission-based and permissionless systems. Smart contracts facilitate entry to the blockchain, providing users with a secure and efficient means to access information and interact with the network.

2.1.4 Consortium Blockchain: This innovative approach caters to the unique requirements of the organization. Also called a Federated Blockchain, it not only validates transactions but also serves as an initiator and receiver of transactions. By combining public and private elements, this blockchain solution effectively addresses the organization's needs in a creative and adaptable manner.

2.2 Characteristics Of Blockchain

2.2.1 Data immutability

It is a fundamental and crucial aspect of the blockchain system, ensuring that data remains unaltered and free from corruption. This is achieved by distributing a copy of the ledger to each and every node in the network. As a result, any attempt to modify the data requires unanimous agreement from all nodes, creating a robust and secure environment. This process fosters a high level of transparency and security throughout the blockchain network.

2.2.2 Decentralization

It is a defining characteristic of the blockchain, ensuring that no single entity, group, or government holds control over this technology. Instead, a network of nodes collaboratively manages the entire transaction process. The decentralized nature of the blockchain network makes it less susceptible to failure. The distributed structure increases the cost for hackers attempting to attack the system, reducing the likelihood of failure. Moreover, the absence of third-party involvement eliminates additional risks in the system, enhancing its overall security and reliability.

2.2.3 Secure

Every record in the blockchain is encrypted individually, providing additional security to the entire process within the blockchain network. The absence of a central authority ensures that one cannot simply add, update, or delete data on the network arbitrarily. Every piece of information on the blockchain is cryptographically hashed, giving each data element a unique identity on the network. Each block within the chain contains its unique hash as well as the hash of the preceding block. As a result, the blocks are cryptographically interconnected, making any attempt to alter the data practically impossible since it would require changing all the hash IDs, which is an infeasible task.

2.2.4. Anonymity

Interacting with the blockchain network is facilitated through randomly generated addresses [43]. In the realm of the Blockchain network, an individual can hold numerous addresses, affording them the ability to shield their identity from disclosure. As the system functions in a decentralized fashion, there exists no central entity overseeing or recording users' personal particulars. Consequently, Blockchain extends a degree of anonymity by operating within an environment built on trust lessness.

BLOCKCHAIN FOR GOVERNMENT SERVICES

3.1 Healthcare :

In the Government Sector, blockchain offers numerous advantages that can enhance various processes. Distributed ledger technology can revolutionize health services, particularly through the implementation of blockchain solutions. One of its key applications lies in the traceability of drugs and efficient management of patient data. The pharmaceutical industry faces a significant challenge in the form of drug counterfeiting, which can be effectively addressed using blockchain[1][5].

Ensuring the integrity of patient data remains a critical concern within the healthcare industry. Each patient's unique physical variability requires personalized treatment strategies, necessitating access to comprehensive medical histories. However, the sensitive nature of medical data demands a secure and confidential sharing platform. The current system of bookkeeping medical records falls short in terms of privacy and interoperability [7].

A permissioned blockchain-based framework called "Med Chain," proposed by B Shen et al., utilizes Hyperledger Fabric to grant patients complete control over their medical records. This distributed storage platform empowers patients to share access to their health information with doctors and health centers securely. Deloitte's publication in 2016 highlights the opportunities for healthcare through blockchain-based solutions. Smart contracts facilitate interoperability within the healthcare system by eliminating intermediaries, resulting in reduced additional costs and increased system resilience. These developments promise to transform the healthcare industry, enhancing patient care and data management [5][7].

Blockchain technology has emerged as a paradigm for e-Healthcare systems. By adopting Hyperledger blockchain architecture, data storage security in health information systems can be significantly enhanced. This approach ensures the achievement of security goals such as confidentiality, integrity, and availability, safeguarding sensitive health data, and enabling secure sharing among authorized entities [6].

3.2 E-Voting:

Blockchain technology strengthens the resilience of the voting process by employing an immutable vote storage mechanism, effectively minimizing the risk of vote tampering and preserving the authenticity of elections. Several countries, including Germany, Russia, Estonia, and Switzerland, have embraced this technology, integrating it into their e-voting systems [8]. The adoption of electronic voting (e-voting) holds the promise of revolutionizing the conventional paper ballot-based voting system, creating a more inclusive and accessible platform. This transformation opens the door for a broader segment of the population to actively engage in the exercise of their civil rights during elections [1][5].

Electronic voting (e-voting) has demonstrated successful implementation in various elections, either as a complement or an alternative to in-person voting, marking a significant step towards more convenient and efficient democratic participation. When dealing with smart systems, especially in sectors like healthcare and industries, a permissioned blockchain is commonly employed to safeguard data privacy at different levels. However, within the sphere of e-voting systems, a permissionless blockchain is important to prevent interference and manipulation, ensuring a free and fair election process for modern democratic systems [9].

The implementation of an E-Voting system can be accomplished using the solidity language on the Ethereum platform, where Ethereum Blockchain handles the storage of individual ballots and vote records. Users are granted the authorization to cast their votes, making the process transparent and tamper-resistant [8][9]. By adopting this strategy, the integrity and security of the electoral process are guaranteed, all the while maintaining the core tenets of democracy within the digital era [1][8][9].

3.3 Smart City:

Smart cities have the potential to introduce inventive solutions, fostering increased citizen engagement and closer collaboration with local governments. Operating through digital technologies and diverse methodologies, these urban centers aim to amplify residents' quality of life while optimizing the efficiency of municipal services. At the heart of this advancement, the Internet of Things (IoT) plays a pivotal role, in amassing and analyzing data, facilitating direct interaction with urban infrastructure, and enabling real-time monitoring of assets and community progress. This data-centric approach empowers smart cities to refine operational efficacy and preemptively tackle potential challenges, thereby nurturing a more sustainable and responsive urban milieu for inhabitants. Furthermore, the integration of blockchain technology within smart cities could usher in enhanced governance by restoring control of personal data to individuals, eradicating intermediaries' dominance over such sensitive information [1][9][10].

The blockchain provides the potential for data encryption, security, and traceability, ensuring anonymity while transmitting data. Additionally, it optimizes the interconnection of all services available in the Smart City, granting access to real-time data on various aspects, including mobility (vehicle usage, routes taken, etc.), energy consumption, waste management, and more.

Vivekanandan et al. introduced a blockchain-based authentication protocol to address the issue of single-point failures in IoT devices used in smart city applications. Instead of relying on a registration center authority (RAC), their protocol utilizes private blockchain technology for IoT device registration. Singh et al. conducted an extensive analysis of the requisites for establishing a sustainable smart city. Figure 8 illustrates their requirements for a blockchain-and-artificial-intelligence-based sustainable smart city [1].

To prioritize security in smart cities using blockchain, we can use Docker, an open-source and secure containerization software platform. Docker is specifically designed for creating, deploying, and managing virtualized applications. Compared to traditional virtualization methods using virtual machines, containers offer a superior alternative, ensuring a lightweight and straightforward execution environment. This architecture comprises three key layers: the perception layer, the data processing layer, and the blockchain layer. The perception layer is dedicated to aggregating data from diverse origins, while the data processing layer undertakes the responsibility of dissecting and handling the compiled data. In parallel, the blockchain layer operates as a secure and indelible ledger, serving as the repository for vital information. By implementing this architecture, smart cities can enhance their security measures and create a robust and reliable infrastructure for efficient and secure operations [10]. The Blockchain has proven to be a valuable tool in enhancing security for smart grids and smart cities. With its ability to provide a more controlled governance system, personal data is no longer in the hands of intermediaries, ensuring greater protection for individuals.

3.4 Education:

During the year 2021, there is a notable upswing in the incorporation of blockchain technology for educational research. A multitude of inventive applications leveraging blockchain has been formulated to amplify the administration of academic credentials within educational frameworks [1]. Especially within the context of developing nations, the constraint of limited financial resources presents a substantial impediment to accessing higher education. A considerable number of exceptionally gifted students find themselves constrained from completing their studies due to parental unemployment and broader economic adversities encountered by their respective nations. This predicament consequently hinders these students from realizing their full potential.

To address this issue and enable students to pursue higher education and reach their maximum potential, many governments have taken the initiative to offer student loans. These loans aim to bridge the financial gap and provide deserving students with the means to acquire higher education. Through such measures, governments aspire to unlock the untapped potential of these students, thereby contributing to both their personal growth and the advancement of their nations.

The government, through the education ministry, facilitates student loans, which students are required to repay, along with accrued interest, once they enter the workforce. Historically, governments have been the exclusive backers of these loans. However, the advent of global challenges like the COVID-19 pandemic and the Russia-Ukraine conflict has triggered a worldwide economic downturn. As a consequence, government expenditures have escalated. To alleviate the government's financial burden and curtail spending, we propose a transformative approach to revamp the student loan system by leveraging blockchain technology and crowdsourcing. This endeavor introduces a decentralized loan platform, powered by blockchain and crowdsourced funding, designed to reshape the landscape of student loans. In this innovative framework, investors will be invited to participate, furnishing funds for higher education students.

Within this platform, eligible students are allowed to apply for loans from investors, facilitated through registered financial institutions. Subsequently, these students will gradually repay the loans, along with accrued interest, upon their entry into the workforce. The envisioned platform carries multifaceted benefits: students gain access to the necessary funds for their education, investors earn interest on their contributions, and governments can redirect the resources previously allocated to student loan programs toward alternative avenues [4].

These examples highlight the diverse potential applications of blockchain technology in various government sectors, offering opportunities to enhance efficiency, accountability, and citizen services. However, it's important to keep in mind that the adoption of blockchain in government requires careful consideration of technical, legal, and regulatory aspects, along with addressing potential challenges and risks.

CHALLENGES OF BLOCKCHAIN TECHNOLOGY

4.1 Privacy and Security

Blockchain is recognized for its ability to offer security and privacy to sensitive personal data during user transactions, establishing it as a primary platform for blockchain technology. However, the absence of interoperability bestows blockchain developers with the flexibility to code using diverse programming platforms. Despite this, these networks remain separate and incapable of seamless interaction with one another.

In terms of security, decentralized blockchains exhibit a higher vulnerability to 51% of attacks compared to their centralized counterparts. Consequently, concerns have arisen among cryptocurrency investors regarding the safety of their assets stored within decentralized chains. The mechanics of 51% attacks exploit a vulnerability inherent in decentralized systems, wherein a user gains control over a chain by commanding more than 51% of the processing power. This susceptibility predominantly affects networks utilizing the proof-of-work (PoW) consensus standard. Permissionless blockchain systems characterized by lower participation rates are particularly susceptible to this type of attack. Cryptocurrencies such as Bitcoin Cash ABC (BCHA), Bitcoin Cash (BCH), and Ethereum Classic have been at the receiving end of these attacks.

4.2 Interoperability

Blockchain projects, even though they operate using the same technology, often exist in isolation from one another. Achieving interoperability within the realm of blockchain involves facilitating smooth data exchange between distinct blockchains, erasing the boundaries that typically constrain such interactions. This endeavor proves to be a formidable task, as it seeks to enable effective data exchange across these blockchain networks.

The 2018 report by Deloitte reveals a widespread interest across various industries in embracing blockchain technology. Nonetheless, a notable challenge emerges the absence of a universally accepted protocol enabling seamless collaboration and integration among these industries. This absence, referred to as a lack of interoperability, casts a negative influence on the advancement of the blockchain sector. Consequently, rather than presenting distinct practical remedies tailored to diverse business models, the primary driving force for blockchain technology remains centered around cryptocurrencies.

4.3 Efficient Storage Management

Within blockchain technology, data storage is achieved by utilizing available unused disk space within a localized network. This localized infrastructure offers a viable solution to various obstacles associated with centralized systems and serves as a compelling alternative to conventional centralized cloud storage. However, it's important to note that within the blockchain context, the accumulation of substantial data volumes can result in diminished performance. Consequently, effective storage management within blockchain-based healthcare systems introduces a significant scalability hurdle.

4.4 Scalability

Lately, researchers have been diligently addressing scalability challenges associated with the network's replica count, alongside performance concerns including throughput (transactions processed per second) and latency (time required to add a block of transactions to the blockchain). However, augmenting the number of replicas can adversely impact throughput and latency, as it necessitates the network to manage an escalated volume of message exchange and processing.

While protocols like Proof of Work (PoW) hold the promise of scalability, they grapple with compromised throughput and elevated latency. This predicament arises from the resources expended in solving cryptographic puzzles to facilitate the publication and appending of a block to the chain.

II. CONCLUSION

This paper explores the potential and advantages of integrating blockchain technology into Government Services, employing a comprehensive comparative survey approach. The discussion encompasses not only the potentials and benefits but also delves into system architecture, various types of blockchain, and the obstacles posed by achieving consensus. Nonetheless, a landscape of unresolved issues remains, necessitating further research and in-depth analysis. This will aid in the development of more viable and efficient industrial applications that can optimally harness blockchain's capabilities, thus aligning with overarching objectives. The presented survey aims in order to provide a valuable roadmap for a deeper comprehension of diverse blockchain consensus mechanisms and their application domains. It also catalyzes the exploration of potential research avenues, fostering promising advancements in related fields.

REFERENCES

[1] Farhana A Sunny , Petr Hajek , Michal M, Mohammad Z Abedin, Md. Shahriare Satu, Md. Iftekharul A Efat, And Md. Jahidul Islam. "Systematic Review of Blockchain Applications", IEEE Access, vol. 7, pp. 117138-117144, 2019, DOI:10.1109/ACCESS.2019.2936094

[2] Varun Malik, Ruchi Mittal, Dinesh M, Bayapa R Narapureddy, S. B. Goyal, R. John Martin, Karthik Srinivasan, And Amit Mittal, "Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based Frameworks". IEEE Access, vol.11, 14 July 2023, DOI:10.1109/ACCESS.2023.3293529

[3] Shinya Haga And Kazumasa Omote, "Blockchain-Based Autonomous Notarization System Using National eID Card", IEEE Access, vol.10, pp. 87477- 87479, August 2022, DOI:10.1109/ACCESS.2022.3199744

[4] Kwame O Asamoah, Adjei P Darko, Collins O Antwi, Seth L Kodjiku, Esther Stacy E. B. Aggrey, Qing Wang, And Jia Zhua, " Blockchain-Based Crowdsourcing Loan Platform for Funding Higher Education in Developing Countries", IEEE Access, vol. 11, 14 March 2023. DO I:10.1109/ACCESS.2023.3252917

[5] Ahmed Afif Monrat, Olov Schelén, And Karl Andersson," A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities", IEEE Access, vol.7, September 4, 2019. DOI:10.1109/ACCESS.2019.2936094

[6] Richard Mnyawi, Cleverence Komb, Anael Sam, and Devotha Nyambo, "Blockchain-based Data Storage Security Architecture for e-Health Care Systems: A Case of Government of Tanzania Hospital Management Information System", IJCSNS International Journal of Computer Science and Network Security, VOL.22 No.3, March 2022

[7] Sadia Ramzan, Aqsa Aqdus, Vinayakumar Ravi, Deepika Koundal, Rashid Amin, and Mohammed A. Al Ghamdi, "Healthcare Applications Using Blockchain Technology: Motivations and Challenges". IEEE Transactions On Engineering Management, 2022.

[8] Maria-Victoria Vladucu, Ziqian Dong, Jorge Medina, And Roberto Rojas-Cessa, "E-Voting Meets Blockchain: A Survey", IEEE Access, vol.11, March 2023. DOI: 10.1109/ACCESS.2023.3253682

[9] Geetanjali R, Razi Iqbal, Omer Waqar, And Ali Kashif Bashir, "on the Design and Implementation of a Blockchain-Enabled E-Voting Application Within IoT-Oriented Smart Cities", IEEE Access, Special Section On Blockchain Technology: Principles And Applications, vol.9, 2021. DOI:10.1109/ACCESS.2021.3061411

[10] Abla El Bekkali, Mohamed Essaaidi, And Mohammed Boulmalf, "A Blockchain-Based Architecture and Framework for Cybersecurity Smart Cities", IEEE Access, vol.11, July 2023. DOI: 10.1109/ACCESS.2023.3296482

[11] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE, 2017, DOI 10.1109/BigDataCongress.2017.85