Government document distribution and storage using Blockchain

Aashish Nandakumar
CSE Dept.
RNS institute of technology (Aff. VTU)
Bangalore, India
aashishnkumar@gmail.com

Dr Kiran P
Prof and HoD, CSE Dept.
RNS institute of technology (Aff. VTU)
Bangalore, India
kiranpmys@gmail.com

***Abstract*—Incorporating the storage and transfer of formal papers using blockchain technology into daily living is the concept behind this survey research. In order to create a simpler method of exchanging and storing data, this article combines the advantages of blockchain technology and cloud computing technology. The safe and transparent storage and transmission of official documents is made possible by blockchain technology. While the implementation of smart contracts can automate procedures and boost efficiency, the decentralised and tamper-proof characteristics of blockchain technology improve security. This article gives a general introduction of the blockchain technology's architecture, models, and use cases for storing and transferring official documents. Blockchain technology has the potential to radically change how governmental agencies handle and manage sensitive information, but it is essential that these organisations carry out thorough research and testing as well as ensure they are in compliance with all relevant laws and regulations.**

***Index Terms*—Blockchain, BaaS, Cloud computing, Government documents, RSA algorithm.**

I. Introduction

The best way to understand blockchain technology is to use the example of bitcoin. The Byzantine General's problem [1], which refers to the difficulty of reaching consensus in a distributed network when there are participants who are unreliable or at fault, was addressed in 2008 by Satoshi Nakamoto, an anonymous author. Satoshi Nakamoto's work and the network he created from it, namely Bitcoin, allowed value to be transferred at a greater distance [2]. One of the most intriguing issues in science and technology right now is blockchain. Its use has quickly spread beyond economic sectors to a number of other sectors, including government, public welfare, security, and academia. Blockchain is a distributed network or database network that incorporates multi-point maintenance and cryptographic concepts. Additionally, it offers us a wide range of benefits, such as data non-tampering, security, and information scalability and transparency [3]. The integrity and security of government papers, which include sensitive information, are of the highest significance. Blockchain technology is poised to enhance security, transparency, scalability, and efficiency while also enabling the storing and transmission of government documents. Digital identities, land registry systems, voting systems, notary services, tax systems, healthcare records, environment management records, and many more things are possible thanks to technology.

Additionally, the decentralised nature of blockchain technology allows for increased transparency and audibility as all transactions and activities on a blockchain based system are recorded and can be easily audited. Blockchain technology can enable the creation of tamper-proof records of government documents, which can improve the security of sensitive information and reduce the risk of fraud and corruption. The objective of this survey study is to examine the potential benefits and challenges of using blockchain technology in the storage and transfer of government documents in addition to the current condition of this technology and expected future improvements. A variety of proof-of-concepts and pilot projects have been created to examine the viability of using blockchain to distribute and store official documents. For managing land records, the government of Andhra Pradesh, India, has been testing a blockchain-based platform[4]. Similar to this, West Virginia's government in the US has been experimenting with using blockchain to facilitate election voting[5].

II. Blockchain Architecture Analysis

A. Achitecture

A block is the fundamental building block of a blockchain, where transactions take place. The word "block chain" refers to the way in which individual blocks are linked together using a particular cryptographic hashing technique. Because these networks of blocks are unchangeable and a single alteration to one of them would cause the entire blockchain to collapse, blockchain is regarded as a secure, decentralised, and non-sovereign network. Every blockchain relies on some sort of widely used consensus method, including: proof of stake and proof of work. When a transaction has to be validated and new blocks need to be created, a miner (the person who creates blocks in proof of work) must solve a challenging mathematical problem. In proof-of-stake, however, a validator—who is not a miner—is picked based on the quantity of tokens they currently own.

The notion of public blockchain, where the transaction history is made available to the public, applies to the entire section. On the other hand, private blockchains are managed by a central organisation, and only authorised authorities are

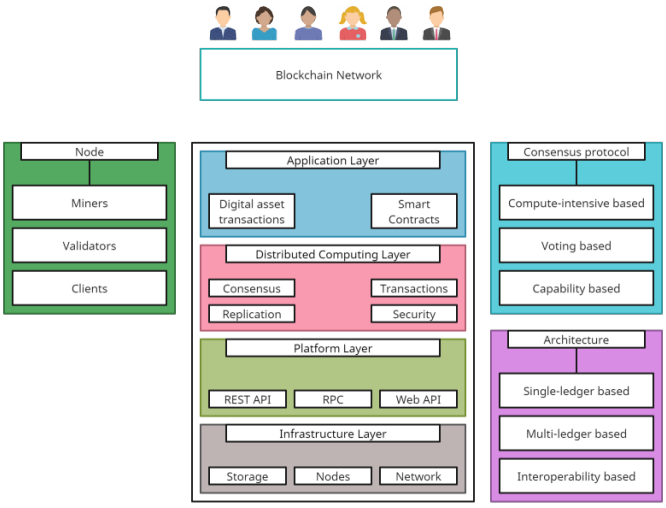

Fig. 1. Blockchain network.

allowed to operate on and use them. In these blockchains, a centralised algorithm serves as the consensus mechanism. This network is mostly utilised in environments with high security and compliance. Any blockchain network's fundamental component that ensures the network continues to operate normally is its consensus procedures. To maintain the efficient and reliable operation of the blockchain ecosystem, a collection of rules, laws, and algorithms is housed by the blockchain. This is known as the consensus mechanism[3]. The deployment of blockchain technology as well as smart contracts has eliminated the need for a central mediator by enabling the creation of new kinds of markets that incorporate the fundamental concepts of supply and demand, secure transactions, and a variety of rules and regulations across the blockchain[10].

B. Components

The blockchain network's architecture is made up of many different parts, some of which are crucial:

- Network: A collection of nodes that interact with one another to verify transactions and build new blocks.
- Consensus mechanisms: This is how the network decides what the state of the blockchain is.
- Smart contracts: In order to automate processes and enforce regulations on the blockchain, smart contracts, self-executing contracts with conditions of agreement inscribed into them in the form of code—are employed.
- Cryptography: Blockchain integrity is guaranteed and the network is secured via cryptography.
- Storage: Blockchain maintains a decentralised ledger of all network transactions, making the information transparent and impervious to manipulation.
- APIs: Application Programming Interfaces provide data access and interaction between blockchain and external applications.

C. Concerns with this architecture

The problems encompass:

- Scalability - A blockchain network is only capable of supporting a finite number of transactions, and at times of high traffic, gas prices and transaction fees will be extremely high, making it impractical for the general public to use. To address this issue, many solutions have been proposed, one of which is to deal with transactions on a derived secondary network rather than the main network, which results in lower traffic and fees. One such application includes Lightning network.
- Regulatory issues - Since the blocks on the blockchain are not generated at random, there must be rules to handle this. One such regulation is the design and use of smart contracts, which handle the blockchain's transaction process.
- Interoperability - Since not all data transfer will occur on a single blockchain, there must be certain standards and protocols in place to enable easy information exchange between several blockchains.

III. Blockchain Security Administration

These use cases are sufficient to draw targets for both internal and external attackers to exploit the network's vulnerabilities. Blockchain tries its best to fend off attackers by replicating its code executions and databases, but there is still no shortage of attacks. Procedures based on distributed ledger technology are not just concepts written on paper; they are used in real-time working environments to track finance and the marketplace. Exploiters attack the consensus processes, flaws in smart contracts, programming languages, or weaknesses in the blockchain network itself, as found by cryptographers and computer scientists. Professionals wishing to deploy security measures against these assaults must have a comprehensive awareness of the current and prospective threats as well as how to do so. A thorough analysis of attacks launched against permissioned blockchains is conducted to address this issue, A collection of threat indicators for automated attack detection based on backup and log data has been developed [6] after analysis of the research's data. In order to prepare for these implementations, The following is a list of a threat model:

- Actors: We create models of the many people who may pose a danger to a blockchain network, such as malevolent insiders or outside attackers.
- Vulnerabilities - These make a blockchain network more susceptible by giving attackers methods to undermine its security, integrity, and availability.
- Malicious intent - Security experts may create internal or external threats with malicious intent to test a certain feature of the blockchain network.

Things to keep in mind: these processes are initially used on permissioned blockchains like the "hyper ledger fabric" so that we can test, evaluate, and fix issues in that network before applying the same techniques to permissionless blockchains, where anybody may join the network.

IV. Blockchain as a Service (BaaS)

The ideal fusion of the blockchain network and cloud network is blockchain as a service (BaaS) [7]. Users are able to take full use of all the benefits and leverages offered by both the cloud and the blockchain network; information and data can be kept on the cloud and easily moved to and retrieved from the blockchain; this is the finest feature addition to implement our issue. The Baas developers oversee all significant and required activities to maintain the network's infrastructure and accessibility. All official papers may be kept in the cloud, and anybody with the proper authorization may access that data and information via the blockchain network. Microsoft and IBM are only two firms that have previously released their BaaS systems and received favourable feedback. BaaS enables businesses to fully benefit from blockchain technology without having to commit money up front to create and maintain the network and infrastructure. A safe and decentralised platform for the dissemination and storage of government documents can be offered by BaaS in this regard. The adoption of blockchain technology guarantees that the papers are immutable, trackable, and auditable. Because blockchain is decentralised, the documents are kept in a dispersed network of nodes, increasing security and making it more challenging for other parties to access the data. BaaS further enables a faster and more effective method for sending and preserving official papers. This can boost accountability and transparency while lowering the cost and time of manual processes. The distribution of documents upon fulfilment of specific circumstances and requirements is one operation that may be automated with the help of smart contracts on the blockchain. In general, the adoption of BaaS can provide a secure, efficient, and open solution for the distribution and storage of important government documents.

V. Blockchain implementation of the RSA algorithm

A. Overview

Government data and documents are stored and transferred under the control of centralised agencies, which are occasionally unreliable and at fault. These agencies are also vulnerable to network attacks, which could compromise the sensitive information contained in those documents. This method is also expensive and time-consuming. All of these issues may be resolved by using blockchain, and by using the RSA method, we can improve the security, economy, and effectiveness of our document transmission system. The widely-used public-key cryptography technique RSA may be used with blockchain technology to give further protection to the storage and circulation of official documents.

To secure the transmission of sensitive information (such as government documents), the RSA algorithm can be implemented onto the blockchain. Using this algorithm, a set of public and private keys can be created, with the public key being used to encrypt the data and the private key being used to decrypt it. Government papers may be securely sent and saved into the blockchain by using the RSA algorithm, guaranteeing that only authorised personnel have access to the data.

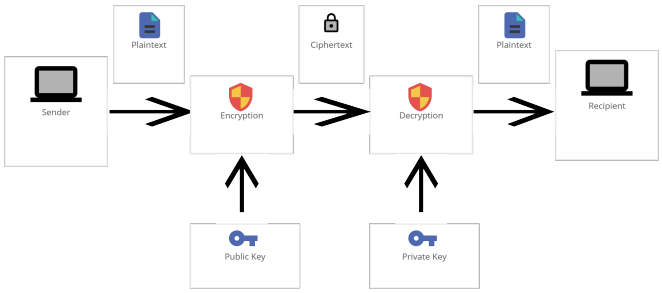

Fig. 2. Overview of RSA algorithm.

The blockchain's decentralised structure adds an extra degree of security since data is spread over a network of nodes, making it more difficult for outsiders to access it. Additionally, the RSA algorithm improves the efficiency of document distribution and storage. The implementation of Smart Contracts on the blockchain, for instance, can automate the distribution of official documents to authorised people in accordance with the fulfilment of the predetermined condition, such as the conclusion of a background check. In general, the application of the RSA algorithm onto the blockchain in the context of the distribution and storage of sensitive government documents can offer a safe, effective, and transparent solution.

B. Implementation

By creating public and private keys offline and storing them in various databases prior to the beginning of the encryption and decryption process, a technique known as the Offline RSA - key generator[8], we may speed up the preexisting implementation speed of RSA. We can mix blockchain and cloud computing technologies (as discussed in topic IV). When a user wants to access the papers in the cloud, the asymmetric cryptosystem RSA is put into use. The government can upload the documents to the cloud, which will be a public cloud (available to all public). The public and private cryptographic keys are first generated by the user.

The blockchain network stores the private key for querying purposes and sends the authorizer (in this case, smart contracts used by the government to authorise legitimate public keys) the public key. The authorizer then uses the public key to encrypt the documents and transfer them to a particular node on the blockchain. The user will be able to access this using the private keys used to decrypt the message and obtain the necessary document. The following procedures can be used to implement the RSA algorithm:

- Document Encryption: Before being put on the blockchain, the official papers can be encrypted using the RSA technique. Information is encrypted throughout the encryption process using a public key, which can only be unlocked with the associated private key. This guarantees

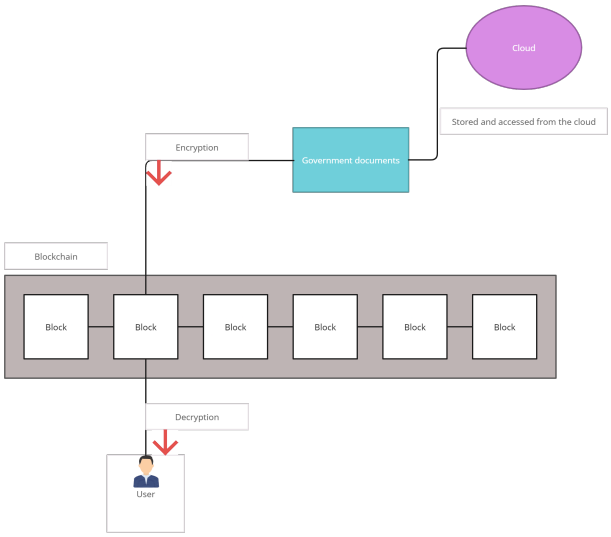

Fig. 3. Overview of RSA algorithm.

that sensitive information is only accessible to those who are authorised.

- Safe key management: The RSA algorithm may be used to handle the encryption and decryption keys for official documents in a secure manner. Authorized persons can safely keep the private keys, and the public keys can be made accessible on the blockchain.
- Automated Document Distribution: To automate the release of official documents to designated persons, the RSA method can be implemented on the blockchain and used in conjunction with smart contracts. For instance, a smart contract may be set up to only give someone access to an encrypted document once they have passed background checks or met other requirements.
- Transparency and audibility: By combining blockchain technology with the RSA algorithm, it is possible to create a tamper-proof log of who has accessed which government papers when. This might improve the process of distributing and storing documents' accountability and openness.

Set methods have been put in place to handle the private and public keys, which are time-critical sensitive information whose relevance will decrease after a certain amount of time[9]. For the dissemination and storage of important government data, the coupling of the RSA algorithm onto the blockchain offers improved security and effectiveness, making it a worthwhile option.

VI. Conclusion

The majority of cryptocurrencies are powered by blockchain technology, which is a decentralised network implementation that enables transparent and secure record keeping. However, blockchain technology has many potential uses that go well beyond just cryptocurrencies. Government documents may be stored and transferred using this cutting-edge technology, which offers several advantages including improved security, transparency, and efficiency. The way government organisations manage and share sensitive information may be completely changed if this technology is used to store and send papers. Utilizing smart contracts, which may automate the process and minimise the need for manual involvement, can also boost efficiency. However, before fully integrating blockchain technology into everyday life, government organisations must take into account the difficulties and restrictions of doing so. They also need to stay up to date on the most recent advancements in the relevant fields and conduct in-depth research and testing.

Acknowledgment

I want to thank the computer science department for helping me choose a subject and for its advice.

References

[1] "Bullish case for bitcoin", (learn.saylor.org). https://learn.saylor.org/mod/page/view.php?id=30719
[2] Shenyi Huang - "Academics records verification platform based on blockchain technology", Second High school attached to Beijing Normal university - International Division, Beijing, 100192, China. DOI: 10.1109/ICCSMT51754.2020.00048
[3] Yang Cheng, Han Shaoqin - "Research on blockchain technology in cryptographic exploration", state Grid Blockchain Technology(Beijing)Co.,Ltd 100192, China DOI: 10.1109/ICBASE51474.2020.00033
[4] "Indian state to implement blockchain for land records", https://www.ledgerinsights.com/indian-blockchain-land-records-registry-andhra-pradesh/
[5] "Blockchain Voting Comes to America: West Virginia's Voatz Experiment", https://www.nasdaq.com/articles/blockchain-voting-comes-america-west-virginias-voatz-experiment-2018-10-04
[6] Benedikt Putz, Gunther Pernul - "Detecting Blockchan Security Threats", Chair of inforamtion Systems, University of Regensburg, Regensburg, Germany. DOI: 10.1109/Blockchain50366.2020.00046
[7] Weilin zheng, zibin zheng, xiangpin chen, kemian dai, peishan li, and renefei chen - "NutBass: A blockchain-as-a-service Platform", DOI: 10.1109/ACCESS.2017.DO
[8] Sami A. Nagar and Saad Alshamma - "High Speed Implementation of RSA Algorithm with Modified Keys Exchange " Faculty of Electronic Engineering, Sudan University of Science and Technology, Khartoum, Sudan 978-1-4673-1658-3/12/31.00 ©2012 IEEE
[9] Wei-Jr Lai National Taiwan University, Chih-Wen Hsueh National Taiwan University , Ja-Ling Wu National Taiwan University -"A Fully Decentralized Time-Lock Encryption System on Blockchain " DOI 10.1109/Blockchain.2019.00047
[10] Sobhan Latifi, Yunpeng Zhang, Liang-Chieh Cheng - "Blochchain-based Real Estate market: one method for applying Blockchain technology in Commercial Real Estate Market", College of Technology University of Houston, U.S.A, Shahid Beheshti university of Tehran, Iran. DOI 10.1109/Blockchain.2019.00002