JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOKKCRYPT: BLOCKCHAIN AND CRYPTOGRAPHY BASED COMMUNICATION SYSTEM

Dikshant Bhagat
Department Of IT,
G H Raisoni College Of Engineering & Management, Pune
dikshant.bhagat.it@ghrcem.raisoni .net
Pune,India

Aftab Shaikh
Department Of IT,
G H Raisoni College Of Engineering & Management, Pune
Aftab.shaikh.it@ghrcem.raisoni.net
Pune, India

Abhi Dadhaniya
Department Of IT,
G H Raisoni College Of Engineering & Management, Pune
abhi.dadhaniya.it@ghrcem.raisoni.net
Pune, India

Chhaya Nayak
Department Of IT,
G H Raisoni College Of Engineering & Management, Pune
chhaya.nayak@raisoni.net
Pune, India

Abstract : This is a document that is a review report on research conducted and the project is made in the domain of Information Technology to have a system for secure communication to prevent threats and vulnerabilities caused by attackers and intruders. Thus, this report proposes the results and solutions of the limited implementation of the various techniques that are introduced in the project. Also, the implementation of the project gives a practical idea of How the entire system works and what effective changes can be made to modify the overall project. Lastly, this paper states an overview of the observations of the authors to help further optimizing in the mentioned domain to achieve utility at better efficiency for a safer road.

Keywords: Decentralization, Security, Blockchain, Cryptography.

Introduction

As we all know, traditional chat applications are centralized, i.e., all data is stored on a centralized server. So, the main problem with this structure is that if the central server fails, the entire network collapses. For example, the WhatsApp server stores all data on a central server, if this server is destroyed, user data may be lost or even user information stored on the server may be leaked. To overcome this problem, our project uses a decentralized application approach. In our application, all user data is stored on a block that is connected to other blocks forming a chain. It is essentially a peer to-peer network. Also, data that is stored in a block is almost impossible to see as very secure encryption and hashing functions (256 bits) are used. Also, if a hacker tries to make changes to the information in a block, he will have to make changes to all copies of that block on the entire blockchain network and it can be completely impossible.

Security is a significant factor in an open system and cryptography plays an important role in this area. Cryptography is old and made sure of the information system is an open system. Be that as it may, the goal of cryptography is not exclusively used for classification, but in addition to providing measures of various issues: data trustworthiness, verification, and non-repudiation. Cryptography is defined as encapsulation and finishing techniques that allow important information and data to be sent in a protected environment so that the main individual is ready to restore this information as a conscious recipient. Cryptography is a systematic technique and procedure to hide data and information through the communication channel. Hiding data from strangers is a craft. Like step-by-step innovations exceed the need for data security the communication channel is greatly expanded. Encryption is defined as a systematic process of change from the plain text of the message to the encrypted text. The encryption process needs any programmed encryption algorithm and key to change the plain text of the message to cipher r [3]. Encryption of the cryptography system is done at the sender of the message lateral. Encrypting the message on the sender's side before sending it to the receiver. Decryption is the reverse systematic procedure of encryption. Transforms encrypted ciphertext into a message plain text. Perform the decryption procedure in the cryptographic system on the receiver side. The decryption Algorithm Process requires several steps– a decryption algorithm and a key. Cryptography is broadly isolated into two classes that rely on each other on the key; which is characterized as used leads change unique book to coded content: - Asymmetric key encryption and symmetric key encryption. Symmetric key encryption uses a similar key for decryption and encryption processes. This system is basic yet pioneering but key circulation is a major issue that should be addressed. While asymmetric encryption uses keys two mathematically related keys: a public key and a private key for encryption. The public key is accessible to everyone except for data once encrypted any client's public key must be decrypted with that particular client's private key as either sender or receiver.

RELATED WORK

2.1 GOALS & OBJECTIVES

BlokkCrypt is a secure communication system that helps to provide security over cyber threats. The major goal is to create a system that advances and secures communication intruders with the help of blockchain and cryptography. Blockchain and Cryptography could be a system's cornerstone to potentially reduce threats caused by intruders or attackers. The system's function is to decrease threats and provide more safety while communicating through BlokkCrypt: a secure Communication system.

2.2 MOTIVATION

An energetic inspiration to make a system that manages communication over a network to be secure and reliable with the help of advanced technologies. It should be part of an overall effective communication strategy for businesses, firms, organizations, and people. With proper communication, the system plan includes all aspects of handling messages, including storage, retrieval, backups, and security. The Inspiration comes from making a system that organizes important data(messages) and provide a secure connection. These fast moves of consideration are caught to encourage the execution of the standard undertaking of this system.

2.3 EXISTING SYSTEM

The systems we currently use have a unified approach to resource sharing and communication. Here, all the data is stored on a unified server. This may lead to loss of data if the server fails. Also, there are countless fake pieces of information and product published on social networking without any known root transgressor (like on WhatsApp, hike). The information shared can be hacked which is stored on the unified server.

2.4 ADVANTAGES

Our approach removes central authorities (CAs) and uses the public blockchain as a distributed ledger of identity and associated public keys. We use blockchain to store public keys, digital signatures, and partner information.

Once the smart contract code is published, it works exactly as programmed. This is one of the main advantages of the platform, the code always interacts as promised, it cannot be faked and it never crashes. The system is trustworthy, transparent, and traceable.

Confidentiality: Once the communication channel between users is secured, peer-to-peer encryption can be set up between endpoints, and only authorized users can access the exchanged messages.

Message integrity and authentication: Blockchain checks signature validity before storage. Another person cannot change/modify the signed contract or change the exchanged messages during the network transit. Each user has a certificate kept on the blockchain. The smart contract checks the certificate and proves the identity of the users. All messages exchanged are signed with private keys associated with the public key on the certificates using the ECDSA algorithm.

Fidelity: It is impossible to shut down all the computers contributing in the blockchain at the same time. As a result, this database is always online and never stops in succession.

Scalability: Cryptography makes the transaction irretrievable giving the pledge that all users can rely on the precision of the digital ledger. It allows boundless connections to be recorded securely in the network.

Non-repudiation: The digital signature provides the non- repudiation service to guard against any denial of a message passed by the sender.

2.4 LIMITATIONS

Blockchains execute smart contracts sequentially, which negatively impacts blockchain performance. As the number of smart contracts grows, the blockchain becomes unscalable. In practice, it is impossible to modify an existing contract registered on a blockchain. Therefore, special care must be taken during the drafting stage of these contracts to avoid future disappointments.

3. PROPOSED SYSTEM

3.1 SYSTEM ARCHITECTURE

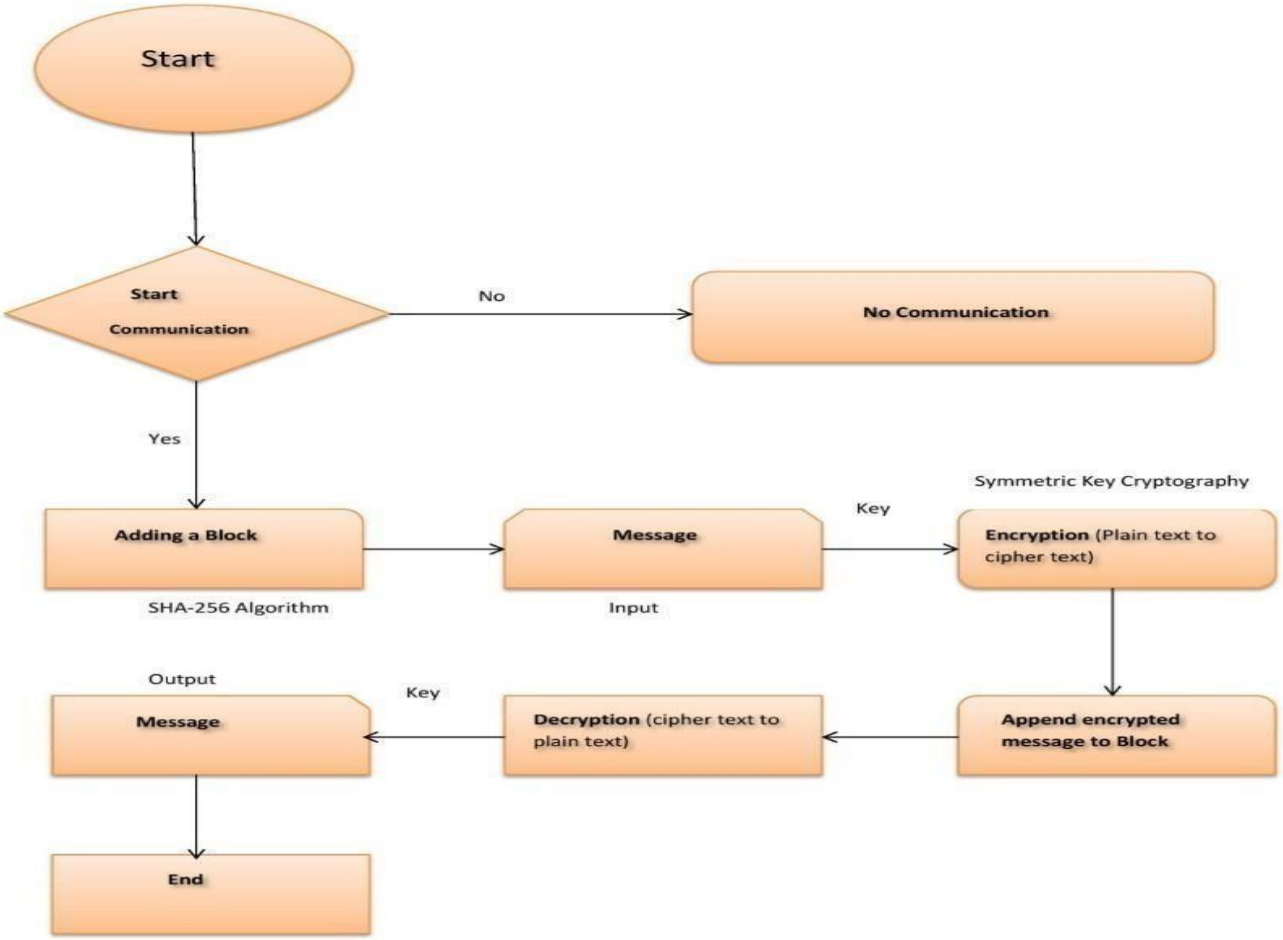

fig 1.1 system architecture of blokkcrypt

3.2 ALGORITHMS USED

A cryptographic hash is a type of ‘signature’ for a text or a data file. SHA-256 generates a nearly unique 256-bit (32-byte) signature for a text.

SHA-256 is one of the successor hash functions as well as the strongest hash function which is available. The SHA-256 code is not much more complex than the SHA-1 code and has not yet been compromised in any way. The 256-bit key makes it a good companion feature to AES. It is well-defined in the National Institute of Standards and Technology (NIST) standard 'FIPS 180- 4'. NIST also provides several test vectors to verify the correctness of the implementation.

Where is SHA 256 used?

We can use SHA 256 in conditions where we need the following: • Data integrity protection

When we communicate online, we assume the response is coming from the person we think it is. How true is this assumption? Well, if the communication is not sufficiently encrypted, a cybercriminal can easily intercept it and impersonate the other party.

SHA 256 ensures data integrity so both parties can be sure that the communication is coming from the person they think it is. The recipient's device creates a hash of the original message and compares it to the hash value sent by the sender. If both hash values are the same, the message was not tampered with in transit.

• Verification of digital signatures

A digital signature is a way of signing digital documents, code, or software that the recipient or user verifies. This way, they will know if you created or signed the document or file, or if the item in question was created or modified by someone else.

But all of this would mean nothing without verification, which is where SHA-256 comes in. Hashing ensures that the digital signature has not been altered since it was signed. The receiving system runs a hashing algorithm on its end and uses the public key to decrypt the message. If it matches, then it knows the data is unchanged and trustworthy. • Verification of blockchain transactions

You may be surprised to learn that SHA-256 is also used in some popular blockchain applications, notably the cryptocurrency Bitcoin. Block headers are integral to blockchains because they help "chain" one block of transactions to the next in a certain order. The SHA-256 hash helps ensure that no previous blocks are changed without changing the new block's header. Examples of where you will find SHA 256 in usage

SHA 256 is one of the most reliable algorithms for authenticating and verifying the integrity of messages. It is used with many different authentications and encryption protocols and processes, including:

SSL/TLS — Secure socket layer (SSL) and transport layer security (TLS) are encryption protocols that maintain the integrity and confidentiality of data in transit.

SSH — The Secure Shell (SSH) protocol creates a secure channel between two devices to transfer data.

IPsec — Internet Protocol Security (IPsec) is a set of protocols designed to secure data transmission between different IP S/MIME — Secure/Multipurpose Internet Mail Extensions (S/MIME) is an algorithm for securing the integrity and confidentiality of e-mails.

Blockchain — In the blockchain, previous hash values are used to calculate the hash value of the current block.

3.4 UML DIAGRAM

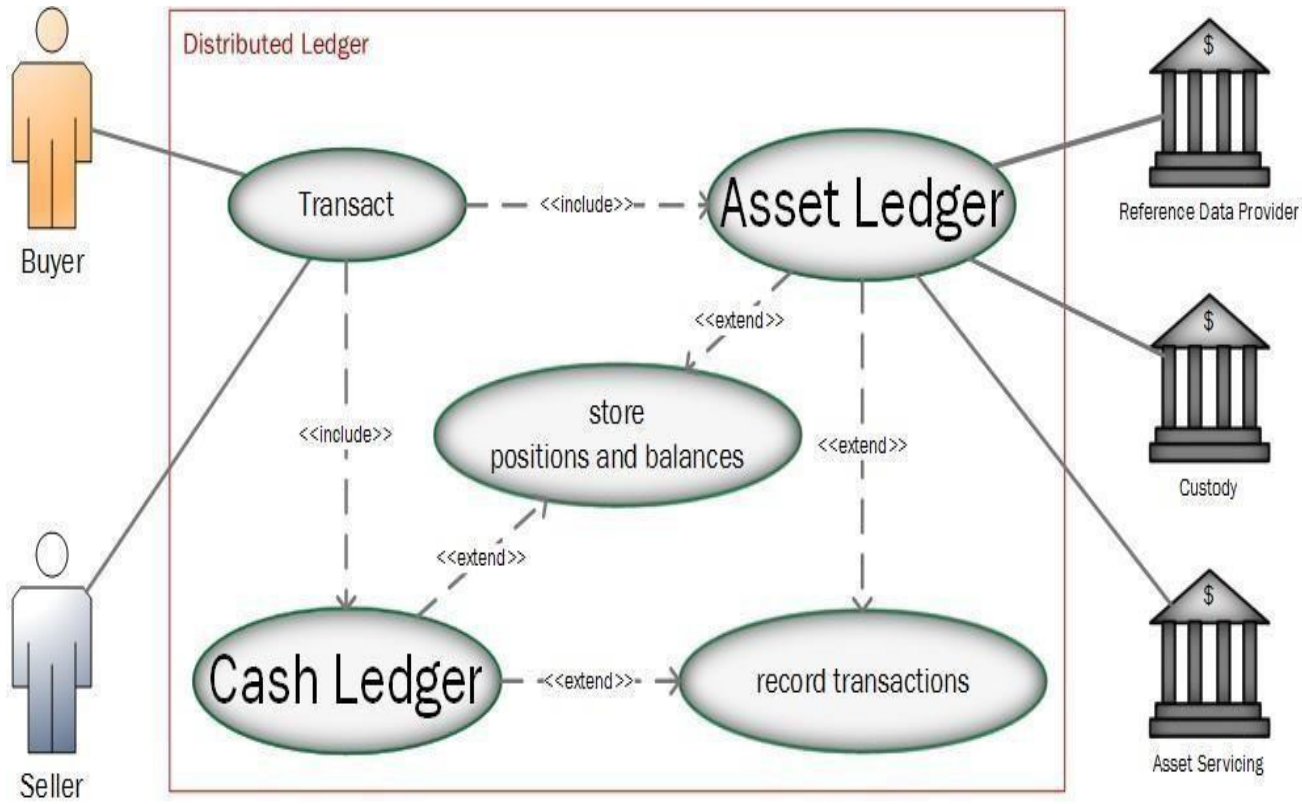

Fig 1.2 uml diagram

4. CONCLUSION

Blockchain technology has been the key focus area of development for all multinational companies and also a huge number of start-ups are emerging in this technology in the past few years. This study introduces the main applications of cryptography in the blockchain and analyses existing problems. Firstly, starting from the blockchain infrastructure, blockchain technology is simplified. Secondly, cryptography technology is introduced to elaborate the blockchain. Finally, the existing security problems in the blockchain are examined. It shows that digital encryption technology runs through the blockchain system and is the central technology of the blockchain system. The Communication system as messages will go through the cryptography and blockchain process for complex security.

1. FUTURE SCOPE

I. Finance: -

Blockchain, when incorporated into financial transactions, provides amazing results. That helps in saving money and time required for processing and verifying transactions. It works on a distributed database that facilitates operations and ensures strict security. Thus, it is consistently used to track financial properties and the government is now looking at them to explore a range of options.

II. Cloud Storage: -

Because data on a centralized server is usually exposed to data loss or hacking. This is where Blockchain comes in and makes cloud storage comparably stronger and more secure.

III. Supply Chain Management: -

Blockchain technology helps document a transaction as an eternal distributed record and therefore oversees transactions more transparently. In addition, it helps in tracking costs, employment, and releases at every point in the supply chain.

IV. Cyber Security: -

Blockchain technology reduces the chances of data attacks because it verifies data and encrypts it using cryptographic technology. Thus, this technology is hugely used in the field of cyber security. 5. Advertising: -

Blockchain provides a solution for supply chain transparency and gaining trust in a distrustful environment. So, it allows the right organizations to succeed by reducing the number of bad players and cheaters. That is why more and more advertising companies are now exploring blockchain to improve their business.

6. Prediction: -

Currently, global distributed prediction markets are being created with online platforms, and Blockchain technology is effectively changing research methodology and techniques for consulting and forecasting.

ACKNOWLEDGEMENT

We would like to thank Dr. Poonam Gupta, our Head of Department (IT), and Prof. Chhaya Nayak for her support and guidance in completing our project BlokkCrypt: Blockchain and Cryptography-based communication system. I would like to take this opportunity to express my gratitude to all of my group members Aftab Shaikh, and Abhi Dadhaniya. [3] The project would not have been successful without their cooperation and input.

REFERENCES

[1] Prof. Shivaji Vasekar, Akash Adhav, Anirudha Adekar, Kshitij Kanake, Shubham Gondhali (2022). Survey paper on Communication Systems using blockchain and cryptography. https://doi.org/10.22214/ijraset.2022.42442.

[2] DR. R. K. Gupta. A review paper on the concept of cryptography and cryptographic hash function. (2020) ISSN 2515-8260

[3] Obamehinti Adeolu Seun1, Touraj Khodadadi2, Sellappan Palaniappan3(2020) Blockchain Technology for managing LandTitlesinNigeria.https://www.researchgate.net/publication/360683789_blockchain_paper

[4] Abdalbasit Mohammed. (2019) Research Paper on Cryptography. 10.1109/ISDFS.2019.8757514

[5] Thomas Kitsantas, Evangelos Chytis. (2019) A review of Blockchain Technology and its Applications in the Business Environment.

[6] Chhaya Nayak "Performance of various algorithms used in cryptography", IJMIE Volume 2, Issue 7 June 2012.