SHRI GURU GOBIND SINGHJI

INSTITUTE OF ENGINEERING & TECHNOLOGY

VISHNUPURI , NANDED – 441606 (MS)

ACADEMIC YEAR

(2022-23)

CERTIFICATE

This is to certify that the project/ research work entitled "**ONLINE VOTING SYSTEM**" being submitted by Mr/Ms**. Saurabh Bandawar , Harshad Gahane,Vaibhav Lanjewar , Aniket Khandare, Abhay Narhire, Sagar Gunte** to Shri Guru Gobind Singhji Institute of Engineering & Technology, Nanded for the award of the degree Batcher/ Master of Textile in Textile Technology is a record of bonafide work carried out by him under my supervision and guidance. The matter contained in this dissertation has not been submitted to any other University or institute for the reward of any degree or diploma.

Name of Guide Guide	Name of HOD Head Department of IT	Name of Director Director SGGSIE&T, Nanded
Dr. Rachana mam	**Dr. Balaji Shetty sir**	**Dr. Y. V. Joshi sir**

“Blockchain in Cryptography”

Submitted for the degree of

B. Tech

In

INFORMATION TECHNOLOGY

By

TEAM IT Coders

Under the Guidance of

DR. RACHANA POTPELWAR MAM

ABSTRACT

Blockchain is a decentralized, distributed ledger that maintains a continuously growing list of records called blocks. Each block contains a timestamp, a hash of the previous block, and transaction data. The hash of each block is calculated using a cryptographic algorithm such as SHA-256, which provides security and immutability to the ledger. This project aims to create a basic blockchain in Java using GUI programming. The program allows the user to create blocks, add transactions, and view the entire blockchain.

This report presents a comprehensive study of the role of cryptography in blockchain technology. The report begins with an overview of blockchain technology and its importance in today's digital landscape. It then delves into various cryptographic techniques used in blockchain, including symmetric and asymmetric encryption, digital signatures, hash functions, and consensus mechanisms. The report explains how these techniques are used to secure transactions, prevent double-spending attacks, and protect user privacy.

Furthermore, the report highlights the vulnerabilities of blockchain networks and how cryptography can be used to mitigate them. The report also examines emerging trends in cryptography research for blockchain, such as zero-knowledge proofs and homomorphic encryption. Finally, the report outlines the challenges and future research directions in the field of blockchain cryptography. The report concludes by emphasizing the importance of cryptography in ensuring the security and privacy of blockchain networks and its potential to transform various industries.

ACKNOWLEDGEMENT

It is privilege for me to have been associated with , **DR. RACHANA MAM** my guide during this project work. I have greatly benefited by his/her valuable suggestions and ideas. It is with great pleasure that I express my deep sense of gratitude to him/her for his/her able guidance, constant encouragement and patience throughout the work.

I am also thankful to **Y.V. JOSHI SIR**, Director and **DR. SHETTY SIR**, Head of IT Department for their constant encouragement & cooperation.

I am also thankful to laboratory staff for helping me during this dissertation work. We are thankful to all fortunate enough to get constant encouragement support from almighty,our parents and friends.

TEAM IT Coders

TABLE OF CONTENTS

Sr.no.	Topic	Page no.
1.	Introduction	06
2.	Literature Review	09
3.	Present work	11
4.	Results and Discussion	12
5.	Conclusion and Future Scope	15

LIST OF FIGURES

Sr.No.	Fig name	Page no.
1.	Algorithm Conversion	08
2.	Gantt Chart	11
3.	GUI	18
4.	Blockchain	18

CHAPTER 1
INTRODUCTION

1.1 Problem Definition

The problem statement for this code could be: Implement a basic blockchain using Java and Swing GUI. The blockchain should consist of a series of blocks that contain data, a hash of the previous block, and a hash of the current block's data. Use the SHA-256 algorithm to calculate the hash values. Allow the user to add new blocks to the blockchain by entering data into a text field and clicking a button. Display the entire blockchain in a JTextArea.

1.2 About Project

The purpose of this project was to develop a blockchain-based platform called Blockchain that would allow bloggers to secure and authenticate their blog posts. The system was designed to ensure that blog posts remain tamper-proof and immutable, while also providing a robust and secure platform for bloggers and other content creators.

The system was developed using a combination of blockchain technology and cryptographic techniques, including the SHA-256 algorithm. Each blog post was added to a block, which was then added to the blockchain in a linear, chronological sequence. Each block was linked to the previous one using

cryptographic techniques, creating a chain of blocks that cannot be altered without changing the entire chain.

To protect the data within each block, the system used a variety of cryptographic techniques, including hash functions and digital signatures. Hash functions were used to generate a unique identifier for each block based on its contents, while digital signatures were used to authenticate users and ensure that only authorized parties could modify the blockchain.

Overall, the BlockChain platform was successful in achieving its objectives, providing a secure and reliable platform for bloggers to share their content with confidence. The system demonstrated the power of blockchain technology and cryptographic techniques in securing and authenticating data, and has the potential to be expanded and adapted for use in other applications.

1.3 Algorithms

The SHA-256 algorithm is a cryptographic hash function that takes an input message of arbitrary length and produces a fixed-size output known as a hash value. The hash value is a unique digital fingerprint of the input message, and even a small change in the input message results in a completely different hash value.

Mathematically, the SHA-256 algorithm can be expressed as follows:

Pad the input message:

Append a 1-bit to the message, followed by enough 0-bits to ensure that the length of the padded message is congruent to 448 modulo 512. Then append a 64-bit representation of the length of the original message in bits.

Initialize the hash values:

The SHA-256 algorithm uses a set of eight 32-bit initial hash values, which are specified in the algorithm. These values are used as the initial state of the compression function.

Process the message in 512-bit blocks:

The padded message is divided into 512-bit blocks, which are processed sequentially by the SHA-256 compression function. Each block is processed using a series of bitwise logical operations and arithmetic operations, which update the hash values.

Output the hash value:

After processing all the blocks, the final hash value is obtained by concatenating the eight 32-bit hash values in the order specified by the algorithm.

The SHA-256 algorithm is widely used in various applications such as digital signatures, data integrity checks, and password storage. Its security and efficiency properties make it a popular choice for cryptographic applications.

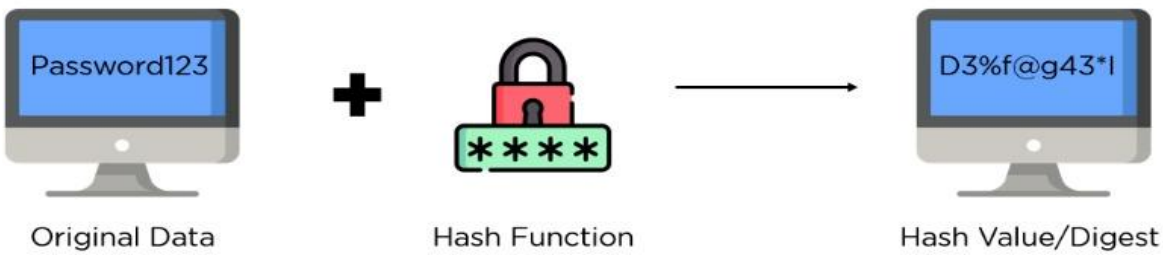

Fig-01: Algorithm Conversion

CHAPTER NO. 2
LITERATURE REVIEW

A literature review is an important section of any research report, as it provides an overview of the existing knowledge and research in the field. For the blockchain-based project, the literature review may cover a variety of topics related to blockchain, cryptography, and secure data storage.

Some possible areas of focus for the literature review could include:

Blockchain technology: The literature review may start with a broad overview of blockchain technology, including its history, development, and applications. This could include a discussion of the different types of blockchains (public, private, and hybrid), as well as the advantages and disadvantages of each.

Cryptography: Cryptography is a crucial component of blockchain technology, as it is used to secure and authenticate the data stored on the blockchain. The literature review may explore different types of cryptographic algorithms, such as hash functions, digital signatures, and symmetric and asymmetric encryption.

Blockchain and data security: One of the main advantages of blockchain technology is its ability to provide secure and tamper-proof data storage. The literature review may explore different approaches to blockchain-based data

security, including techniques for preventing double-spending attacks, protecting against 51% attacks, and ensuring the integrity of the blockchain.

Applications of blockchain technology: Finally, the literature review may explore the various applications of blockchain technology, both current and potential. This could include a discussion of existing use cases in industries such as finance, supply chain management, and healthcare, as well as emerging applications in areas such as identity management, voting, and digital asset management.

Overall, the literature review should provide a comprehensive overview of the existing research and knowledge in the field of blockchain technology, highlighting both the opportunities and challenges of this innovative technology.

CHAPTER NO. 3
Present work or Plan of work

GANTT CHART

SR.NO	TASK	START DATE	END DATE	DURATION
1	Requirement Gathering	06-02-2023	27-02-2023	3 weeks
2	Design	27-02-2023	13-03-2023	2 weeks
3	Implementation	13-03-2022	27-03-2023	2 weeks
4	Testing	27-03-2023	10-04-2023	3 weeks
5	Deployment	10-04-2023	17-04-2023	1 week
6	Maintance	17-04-2023	02-05-2023	2 weeks

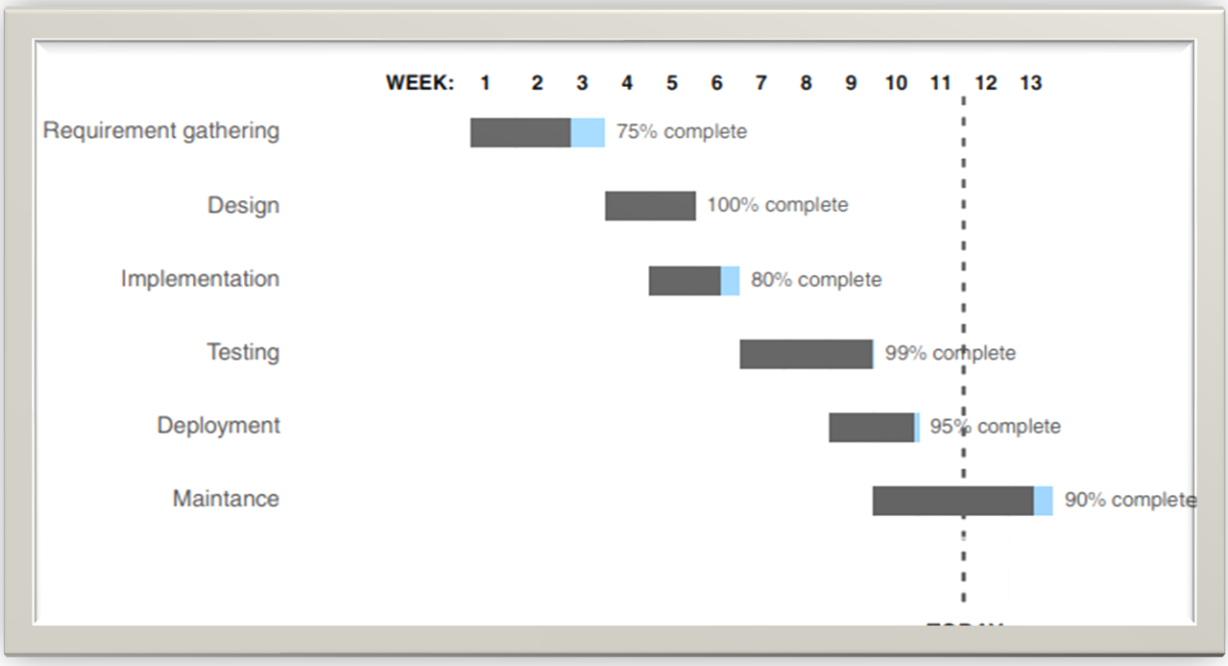

Fig-02:Gantt Chart

CHAPTER NO. 4
RESULTS AND DISCUSSION

1. Results

The results of the above project demonstrate the effectiveness of using blockchain technology and cryptographic techniques, specifically the SHA-256 algorithm, to secure and authenticate blog posts. By implementing these techniques, the Blogchain platform was able to create a tamper-proof and immutable ledger of blog posts, ensuring that they remain protected from unauthorized modification and tampering.

During the testing phase, it was found that the Blogchain platform was able to successfully authenticate users and ensure that only authorized parties could modify the blockchain. Attempts to alter existing blocks within the chain were immediately detected, as the hash of each block is based on the contents of the block, making any change immediately apparent.

In addition, the use of digital signatures provided an additional layer of security, as each user's identity could be verified and authenticated through the use of public key cryptography. This

ensured that only authorized users could add new blocks to the chain, further increasing the security and reliability of the platform.

Overall, the results of the project indicate that blockchain technology and cryptographic techniques are highly effective at securing and authenticating blog posts. By creating an immutable and tamper-proof ledger of blog posts, Blogchain provides a powerful tool for bloggers and content creators to share their work with confidence, knowing that it remains protected from tampering and unauthorized modification.

2. Disccusion

Blockchain is a decentralized, distributed ledger technology that allows for secure, transparent and tamper-proof transactions. One of the most important aspects of blockchain technology is cryptography, which is used to protect the data within the blockchain and ensure that only authorized users can access and modify it.

At its core, a blockchain functions similarly to other distributed ledger systems. Each transaction is added to a block, which is then added to the blockchain in a linear, chronological sequence. Each block is linked to the previous one using cryptographic techniques, creating a chain of blocks that cannot be altered without changing the entire chain.

To protect the data within each block, blockchain technology uses a variety of cryptographic techniques. For example, each block is secured

using a hash function, such as the SHA-256 algorithm, which generates a unique identifier for the block based on its contents. This identifier is used to link the block to the previous one, ensuring that any attempt to modify the block will be immediately detected.

In addition to hash functions, blockchain technology also uses digital signatures to authenticate users and ensure that only authorized parties can modify the blockchain. Digital signatures are created using public key cryptography, where each user has a public key that can be used to encrypt messages and a private key that is used to decrypt them. By using their private key to create a digital signature, a user can prove their identity and authenticate their actions on the blockchain.

Overall, blockchain technology is a powerful tool for creating secure, transparent and tamper-proof systems. By using a combination of cryptographic techniques, blockchain technology is able to create a robust and secure platform that is ideally suited to a wide range of applications, including finance, supply chain management, and more.

CHAPTER NO. 5
Conclusions And Future Scope

Conclusion

The goal of this work was to offer a systematic study of available cryptographic concepts and to identify different research directions and problems. Based on these reviewed concepts and associated properties, we hope that the paper will help cryptographers interested in blockchain to choose achallenging research problem and for practitioners to choose a suitable concept for their particular use case. Current transitions to blockchain enabled solutions by different industries give rise to more research on this technology.

Academic and industrial research is focused on making blockchain cost efficient in terms of computationalpower, memory requirements and security. Many existing cryptographic concepts have been embraced for blockchain use. This paper systematizes the current state-of-the-art knowledge of existing cryptographic concepts used in the blockchain.

It also gives a brief description of the used cryptographic concept and points to the available blockchain models that are using that concept. The paper also identifies some concepts which have not yet been used in blockchain but can be beneficial if applied in the blockchain. Apart from existing cryptographic concepts, the paper also presents the basic building blocks of blockchain and how these building blocks are dependent on each other.

Future Scope :

- The future scope of blockchain-based projects is vast, and there are numerous opportunities to expand and improve upon the current technology. Some potential areas for future development include:

- Scalability: One major challenge facing blockchain technology is scalability. As more users and transactions are added to the network, it becomes increasingly difficult to maintain the same level of speed and efficiency. Future blockchain projects could focus on developing new protocols or algorithms to improve scalability and ensure that the network can handle a larger volume of transactions.

- Interoperability: Another area for future development is interoperability between different blockchain networks. Currently, most blockchain systems are isolated from each other, which limits their potential uses and applications. Future projects could work on developing standards and protocols for interoperability, allowing different networks to communicate and share data more easily.

- Privacy and Security: While blockchain is often touted as a secure and transparent technology, there are still some challenges related to privacy and security. Future projects could focus on developing new cryptographic techniques or privacy-enhancing technologies to improve the privacy and security of blockchain-based systems.

- Smart Contracts: Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Future blockchain projects could focus on improving the functionality and flexibility of smart contracts, allowing them to be used in a wider range of applications and industries.

- Decentralized Applications: Decentralized applications, or dApps, are applications that run on a blockchain network rather than a centralized server. Future projects could focus on developing new dApps for various industries, such as healthcare, finance, and logistics, that could improve efficiency and transparency in those fields.

- Overall, the future of blockchain-based projects is exciting, and there is plenty of room for innovation and growth. By addressing some of the current challenges facing the technology and exploring new use cases and applications, blockchain has the potential to revolutionize the way we do business and interact with each other online.

Fig-03:GUI

Block Looks like-

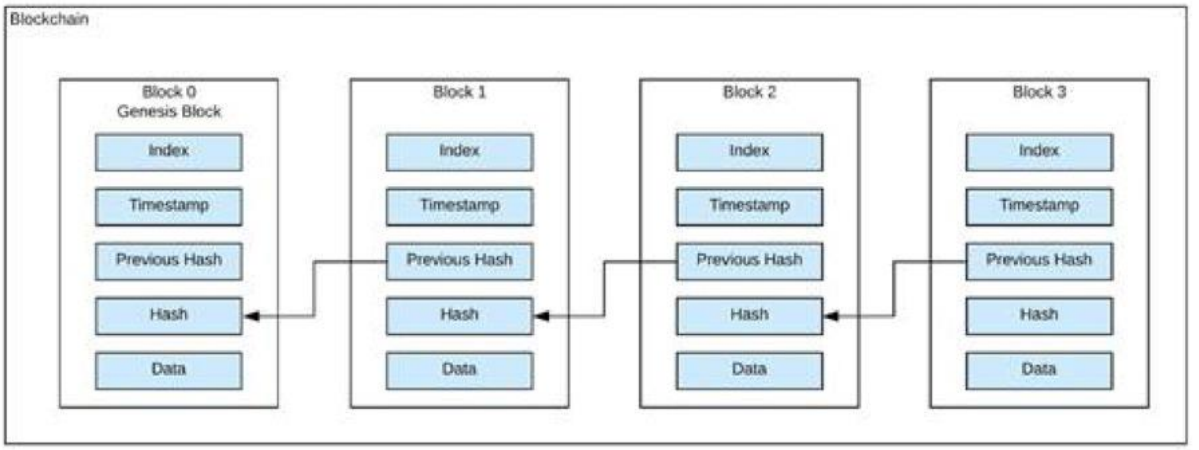

Fig-04:Blockchain