A Project Report On

BLOCKCHAIN STOCK BROKERAGE SYSTEM

Submitted in partial fulfillment of the requirement for the 8^{th} semester

Bachelor of Engineering

in

Computer Science and Engineering

DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078

Submitted By

Mohammed Adnan 1DS19CS089

Mohammed Arham 1DS19CS090

Mohammed Faisal 1DS19CS091

Mudassir Ahmed 1DS19CS093

Under the guidance of

Prof. Chaitra S P
Asst Professor, CSE , DSCE

Mr. Yashwanth
Alumni, CSE , DSCE

2022 - 2023

Department of Computer Science and Engineering

DAYANANDA SAGAR COLLEGE OF ENGINEERING

Bangalore - 560078

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Dayananda Sagar College of Engineering

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078

Department of Computer Science & Engineering

CERTIFICATE

This is to certify that the project entitled **Blockchain Stock Brokerage System** is a bonafide work carried out by **Mohammed Adnan [1DS19CS089]**, **Mohammed Arham [1DS19CS090], Mohammed Faisal [1DS19CS091]** and **Mudassir Ahmed [1DS19CS093]** in partial fulfillment of 8th semester, Bachelor of Engineering in Computer Science and Engineering under Visvesvaraya Technological University, Belgaum during the year 2022-23.

Prof. Chaitra S P	**Dr. Ramesh Babu D R**	**Dr. B G Prasad**
(Internal Guide)	Vice Principal & HOD	Principal
Asst Prof. CSE, DSCE	CSE, DSCE	DSCE
Signature:.....	Signature:.....	Signature:.....

Name of the Examiners:	Signature with date:
1.....	.....
2.....	.....

Acknowledgement

We are pleased to have successfully completed the project **Blockchain Stock Brokerage System**. We thoroughly enjoyed the process of working on this project and gained a lot of knowledge doing so.

We would like to take this opportunity to express our gratitude to **Dr. B G Prasad**, Principal of DSCE, for permitting us to utilize all the necessary facilities of the institution.

We also thank our respected Vice Principal, HOD of Computer Science & Engineering, DSCE, Bangalore, **Dr. Ramesh Babu D R**, for his support and encouragement throughout the process.

We are immensely grateful to our respected and learned guide, **Prof. Chaitra S P**, Assistant Professor CSE, DSCE and our co-guide **Mr. Yashwanth**, Alumni, CSE, DSCE for their valuable help and guidance. We are indebted to them for their invaluable guidance throughout the process and their useful inputs at all stages of the process.

We also thank all the faculty and support staff of Department of Computer Science, DSCE. Without their support over the years, this work would not have been possible.

Lastly, we would like to express our deep appreciation towards our classmates and our family for providing us with constant moral support and encouragement. They have stood by us in the most difficult of times.

Mohammed Adnan 1DS19CS089
Mohammed Arham 1DS19CS090
Mohammed Faisal 1DS19CS091
Mudassir Ahmed 1DS19CS093

Blockchain Stock Brokerage System

Mohammed Adnan, Mohammed Arham, Mohammed Faisal, Mudassir Ahmed

Abstract

The stock market faces challenges of insider trading and front running, where privileged information is misused and an unfair advantage is gained. Blockchain technology offers a solution by ensuring transparent transactions and eliminating intermediaries. With blockchain, transaction information becomes public, preventing tampering.

Smart contracts replace intermediaries, mitigating risks of front running and insider trading. Decentralized transactions face similar challenges, such as sandwich attacks, which can be prevented by combining blockchain with encryption algorithms.

A consensus signature mechanism requires all participants to verify transactions, preventing front running. Miners in the Proof-of-Work network also have limited access to transaction data, enhancing security. Implementing blockchain technology resolves these issues, promoting transparency, fairness, and security in the stock market.

Contents

1 Introduction

1.1 The Problem

The stock market and decentralized exchanges face significant challenges, including front-running, insider trading, and sandwich attacks. Insider trading occurs when employees exploit non-public information for personal gain, violating ethical and legal boundaries. Front-running involves individuals with special privileges gaining advance knowledge of transactions, giving them an unfair advantage over other traders. Sandwich attacks, on the other hand, combine front-running and back-running tactics in decentralized exchanges, enabling attackers to manipulate transactions for personal profit.

These issues have far-reaching consequences, leading to the misuse of information and detrimentally impacting the trading experience for the masses. The exploitation of insider information and front-running disrupts the level playing field, eroding trust and fairness within the stock market. Similarly, sandwich attacks introduce additional vulnerabilities in decentralized exchanges, compromising the integrity of transactions and further disadvantaging traders.

To address these pressing concerns, it is crucial to implement effective measures and safeguards. This may involve leveraging blockchain technology to enhance transparency and security. By utilizing blockchain, transaction information can be made public while maintaining tamper-proof integrity. Implementing stringent regulations and comprehensive monitoring systems can also help detect and prevent insider trading and front-running. Additionally, employing advanced encryption algorithms and consensus mechanisms can bolster the security of decentralized exchanges, mitigating the risk of sandwich attacks and ensuring a safer trading environment for all participants.

1.2 Real World Application

The project was designed to solve a real problem and be applied in the real world. Bringing the stock market onto the blockchain can have several real-world applications and benefits. Some potential applications of such a project include:

1. Increased Transparency: By leveraging blockchain technology, the stock market can become more transparent and auditable. Every transaction and ownership transfer can be recorded on the blockchain, providing a secure and immutable ledger of all activities. This enhanced transparency can help prevent fraudulent activities, promote trust among market participants, and enable regulators to effectively monitor and enforce compliance.

2. Efficient Settlements: The traditional stock market settlement process can be time-consuming and involve multiple intermediaries. By utilizing blockchain, the settlement process can be streamlined, reducing the need for intermediaries and automating various tasks. This can lead to faster and more efficient settlements, minimizing counterparty risks and reducing costs associated with the settlement process.

3. Accessibility and Global Reach: Blockchain-based stock markets can potentially enhance accessibility for investors worldwide. The decentralized nature of blockchain allows for seamless cross-border transactions, eliminating the barriers associated with traditional stock exchanges. This opens up investment opportunities for a broader range of individuals and enables participation in global markets without the need for intermediaries.

4. Fractional Ownership and Tokenization: Blockchain can enable the tokenization of stocks, allowing for fractional ownership and the ability to trade smaller units of shares. This can make investing more accessible to a wider range of investors, including those with limited capital. Tokenization also introduces the potential for new trading models and innovative financial products, expanding the scope of investment opportunities.

1.3 Organization of Project Report

2 Problem Statement and Proposed Solution

2.1 Problem Statement

To avoid illegal activities such as front-running and insider trading by eliminating the broker/middleman completely in the present-day stock exchange system.

2.2 Existing Systems

The existing stock brokerage system is a comprehensive infrastructure that facilitates the buying and selling of stocks and securities in financial markets. Brokerage firms serve as intermediaries, providing trading platforms and executing trades on behalf of investors. These platforms offer real-time market data, order placement functionality, and account management features. Brokerage firms establish connectivity with stock exchanges and other trading venues to access liquidity and execute trades. Compliance with regulatory requirements ensures fair and transparent markets. The clearing and settlement process verifies trade details, transfers ownership of securities and funds, and involves central clearinghouses and custodian banks. Investor services include investment advice, research reports, portfolio management tools, and access to IPOs and other investment opportunities. In summary, the existing stock brokerage system comprises brokerage

firms, trading platforms, regulatory bodies, and investor services, enabling investors to participate in stock markets and manage their portfolios.

2.3 Proposed Solution

Blockchain technology can be used as a game-changing solution for stock exchanges, offering benefits such as the elimination of intermediaries through smart contracts. This will result in faster transaction settlements and addresses concerns surrounding front-running and insider trading. The decentralized and immutable nature of blockchain will ensure tamper-proof transactions. However, to tackle the issue of front-running, a mechanism will be needed to handle the viewing of public data by miners. Threshold encryption can be used as a solution that hides transaction information until it is signed by all participants, preventing front-running and the associated sandwich attacks. Overall, blockchain technology can be used in stock exchanges for enhancing security, efficiency, and transparency in trading operations.

2.3.1 Blockchain Infrastructure

Develop a private or permissioned blockchain network specifically designed for the stock exchange. This network should have high transaction throughput, scalability, and robust security features to handle the trading volume and protect sensitive financial data.

2.3.2 Tokenization of Securities

Enable the tokenization of securities on the blockchain. Convert traditional stocks and other securities into digital tokens that represent ownership. This process involves linking each token to the underlying asset and ensuring compliance with relevant regulations governing securities issuance.

2.3.3 Smart Contracts

Utilize smart contracts to automate the execution of trades, settlement, and clearing processes. Smart contracts are self-executing agreements coded on the blockchain, enabling transparent and tamper-proof transactions. These contracts can define the rules for trade execution, share transfers, dividend payments, and other aspects of securities trading.

2.3.4 Order Matching and Trading

Implement an order matching engine on the blockchain network to facilitate the matching of buy and sell orders. This engine should consider factors such as price, quantity, and time priority to ensure fair and efficient order execution. Once matched, the smart contracts can automatically execute the trades.

2.3.5 Clearing and Settlement

Streamline the clearing and settlement process by leveraging blockchain's distributed ledger capabilities. The blockchain maintains a transparent and immutable record of all transactions, simplifying the reconciliation and verification process. Settlement can be facilitated through smart contracts, automatically transferring ownership of digital securities and facilitating the transfer of funds.

2.3.6 Regulatory Compliance

Ensure compliance with relevant securities regulations and KYC/AML (Know Your Customer/Anti-Money Laundering) requirements. Implement necessary protocols and mechanisms to verify the identity of participants, track transaction history, and provide necessary reporting capabilities to regulatory authorities.

2.3.7 Investor Protection and Governance

Establish robust governance mechanisms to protect investor interests and maintain market integrity. This includes implementing mechanisms for dispute resolution, market surveillance, and regulatory oversight.

2.3.8 Market Access and Interfaces

Develop user-friendly interfaces, including trading platforms and mobile applications, to allow investors and market participants to access and interact with the stock exchange. These interfaces should provide real-time market data, order placement, portfolio management tools, and other features to enhance the trading experience.

2.3.9 Collaboration with Market Participants

Collaborate with brokerage firms, custodians, and other market participants to ensure interoperability and seamless integration of existing systems with the blockchain-based stock exchange. This collaboration can facilitate the transition and adoption of the new system.

2.3.10 Continuous Improvement and Innovation

Embrace ongoing research and development to enhance the efficiency, scalability, and security of the blockchain-based stock exchange. Stay updated with emerging technologies, such as interoperability protocols and privacy-enhancing solutions, to further optimize the trading experience.

2.4 Threshold Encryption

Threshold encryption is a cryptography technique that allows for secure communication and transaction execution in a network while providing confidentiality and preventing certain types of attacks, such as sandwich attacks and front-running. It can be broken down into the following key components.

2.4.1 Transaction Information Hiding

Threshold encryption enables the concealment of transaction information from network participants before its execution. When a transaction is created, it is encrypted using a cryptographic scheme that requires the participation of multiple network nodes to decrypt the information. This means that individual nodes in the network do not have access to the plaintext transaction details.

2.4.2 Decryption with Participant Consensus

To decrypt the transaction and access the plaintext information, all participants in the network must sign the transaction. Each participant holds a specific decryption key or share of a key that is necessary to collectively decrypt the encrypted transaction. Only when all participants have signed the transaction, combining their respective shares, can the encrypted information be decrypted and the transaction details revealed.

2.4.3 Prevention of Sandwich Attacks

Sandwich attacks are a type of attack where an attacker tries to interpose or manipulate a transaction between the sender and the receiver by extracting sensitive information or altering the transaction details. With threshold encryption, the encrypted transaction prevents nodes from directly accessing the information, significantly reducing the risk of sandwich attacks. The requirement for all participants to sign the transaction ensures that any attempted modification or manipulation would be detected, as the transaction would not receive the necessary signatures from all participants.

2.4.4 Restricted Pre-Execution Permissions

In threshold encryption, network nodes have limited permissions to view transaction information before its execution. Since the transaction is encrypted, individual nodes can only see encrypted data that they are unable to decipher without the collective participation of all network participants. This restricted pre-execution access ensures that nodes cannot gain early insight into the transaction details or exploit the information for malicious purposes, further preventing front-running attacks.

2.4.5 Front-Running Prevention

Front-running is a type of attack where a malicious actor observes pending transactions in a network and attempts to execute their own transaction ahead of others to gain unfair advantages, such as manipulating prices or order execution. By hiding the transaction information through encryption and limiting pre-execution access, threshold encryption effectively mitigates front-running attacks. The encrypted transaction ensures that participants cannot ascertain the content of a transaction until it is executed and the necessary signatures are obtained from all participants, preventing any attempts to front-run.

2.5 System Requirements

Hardware:

- Processor: A multi-core processor with a clock speed of at least 2.5 GHz or higher.
- Memory: A minimum of 8 GB RAM is recommended, although more may be required for larger-scale DApps.
- Storage: Sufficient storage space for storing the blockchain data and the DApp's files. Solid-state drives (SSDs) are preferable for faster read/write operations.

Operating System:

- Most blockchain platforms support multiple operating systems, including Windows, macOS, and Linux. Choose an operating system that is compatible with the blockchain platform you plan to use.

Blockchain Platform:

- Select a blockchain platform suitable for building a decentralized stock exchange DApp, such as Ethereum, EOS, or Stellar. Each platform has its own specific system requirements, so refer to the documentation of the chosen platform for detailed information.

Network Connectivity:

- A stable internet connection with sufficient bandwidth is necessary for interacting with the blockchain network and exchanging data with other network participants.

Development Tools and Frameworks:

- Depending on the programming language and framework you choose for developing the DApp, ensure that your system meets the requirements for those development tools. For example, if you're developing on Ethereum using Solidity, you would need the appropriate version of the Solidity compiler.

Security Considerations:

- Running a DApp for a decentralized stock exchange involves handling sensitive financial transactions and user data. It's crucial to prioritize security measures, including firewalls, encryption protocols, secure coding practices, and regular updates of software and libraries, to protect against potential vulnerabilities and attacks.

3 Literature Survey

In this literature survey, we aim to delve into the existing body of knowledge regarding blockchain-based stock markets. We will investigate key concepts related to blockchain technology, the functioning of traditional stock markets, and the potential benefits that blockchain can offer to revolutionize the stock market ecosystem. Furthermore, we will explore the challenges and obstacles faced in implementing blockchain solutions in stock markets, including scalability, interoperability, regulatory considerations, and user adoption.

3.1 An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

Authors: Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang

The authors give us a brief overview of the blockchain architecture, its characteristics, and the challenges. The characteristics of blockchain include decentralization, persistency, anonymity, and auditability. The challenges faced in a blockchain network include scalability, privacy leakage, and selfish mining. The author also explains how consensus is achieved in blockchain using certain consensus protocols such as proof of work and proof of stake.

3.2 A Critical Review of Blockchain and Its Current Applications

Authors: Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee

This paper gives us a brief overview of the fundamentals of blockchain and its applications. It gives us an insight into the decentralized ledger and the process of mining. Mining refers to the process of adding new blocks into a blockchain network. It uses heavy resources and makes

difficult for hackers to hack into the network. Mining can be implemented using consensus mechanisms such as proof of work and proof of stake. Blockchain can be widely used in applications such as financial transactions, healthcare, business and industries, and various other domains.

3.3 A Survey of Blockchain Applications in Different Domains

Authors: Wubing Chen, Zhiying Xu, Shuyu Shi, Yang Zhao, Jun Zhao

This paper gives us information about the various applications of blockchain technology. One of the main applications of blockchain is cryptocurrency. Blockchain is majorly used in the financial sector, especially in the field of cryptocurrencies such as Bitcoin. The most famous cryptocurrencies include Bitcoin and Ethereum. The advantage of cryptocurrencies is that they make cross-border payments fast and efficient without the intervention of a central authority. Blockchain is also majorly used in other sectors such as healthcare, advertising, insurance, copyright protection, energy domains, and society applications.

3.4 A Survey on Blockchain Technology and its Proposed Solutions

Authors: Dharmin Dave, Shalin Parikh, Reema Patela, Nishant Doshi

The author explains why blockchain technology sometimes can cause problems such as scaling up, Interoperability, replacement of databases. These problems are very critical and need to be addressed while developing a blockchain application, and the survey on these problems prevents these issues in our application.

3.5 A Survey on Security and Privacy Issues of Blockchain Technology

Authors: Tam T. Huynh, Thuc D. Nguyen, Hanh Tan

The author gives insight into the security issues that arise in a blockchain network. The most usual attacks on a blockchain network originate from unfaithful nodes that aim to control the generation of blocks in the chain. The most common attack is the 51% attack, which can solve a hash puzzle in proof of work and create a new block on the chain. Another common attack is the double spending attack, in which an unfaithful node spends the same coin in one or more transactions. A rare form of attack is a selfish mining attack, in which an unfaithful node publishes private blocks to a network to create the longest valid chain. Eclipse attack is a form of attack wherein peers of the network are isolated from the victims and can launch other types of attacks.

3.6 A Survey on the Security of Blockchain Systems

Authors: Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen

The author explains blockchain propagation and synchronization. Advertising-based propagation is a method derived from Bitcoin protocols in which when a node 'A' receives information about a block, 'A' sends a message to its peers. Another type of propagation is send-headers propagation. For example, when a node 'B' receives information about a block, it will send send-headers message to node 'A'. There is another type of push propagation method called unsolicited propagation. In this type of propagation, there is no INV message or send-headers message. This type of propagation was basically designed to further improve the speed of block propagation. The last type of propagation method is relay network propagation in which all the miners share a single transaction pool, and all of the transactions have a global ID, which reduces the block size and hence reduces the network load, ultimately improving the propagation speed.

3.7 An Overview of Smart Contract and Use Cases in Blockchain Technology

Authors: Bhabendu Kumar Mohanta, Soumyashree S Panda, Debasish Jena

The authors explain the concept and the structure of a smart contract. A smart contract is a computer program that is self-verifying, self-executing, and tamper-free. The combination of blockchain and smart contracts provides us flexibility to develop, design, and implement real-world problems in the least amount of time without the involvement of a third party. The authors also shed light on the use cases of smart contracts. Some of the use cases of smart contracts include supply chain, Internet of Things, healthcare system, digital rights management, insurance, financial system, and real estate.

3.8 Blockchain Smart Contracts: Applications, Challenges, and Future Trends

Authors: Shafaq Naheed Khan, Faiza Loukil, Chirine Ghedira-Guegan, Elhadj Benkhelifa, Anoud Bani-Hani

The authors explain the platforms used to implement smart contracts. The first platform is Bitcoin, which is a public blockchain platform used to process the digital currency called Bitcoin. Another platform, NXT, runs on a proof of stake protocol and requires the selection of smart contracts that are currently living. Ethereum was the first blockchain product platform to implement smart contracts. It also supports advanced and customizable smart contracts. EVM or Ethereum Virtual Machine is the runtime engine for smart contracts, and every miner in the network implements the EVM and executes the instructions. DApps can also be implemented using Ethereum's programming language known as Solidity.

3.9 Ethereum: A Secure Decentralized Generalized Transaction Ledger

Author: Dr. Gavin Wood

Dr. Gavin Wood gives a brief about the blockchain paradigm and its mathematical aspects, specifically of an Ethereum network. A transaction on the blockchain is the same as a state transition, and each transaction creates a valid arc between two states. A valid state transition is represented by A = Y(A(t), T) where Y is the transition function. Y combined with A is more powerful than any existing comparable systems. The author also gives us the units of Ethereum currency.

3.10 Distributed Ledger Technology Review and Decentralized Applications Development Guidelines

Authors: Claudia Antal, Tudor Cioara, Ionut Anghel, Marcel Antal, Ioan Salomie

In this paper, the author emphasizes the architecture of blockchain applications, which can be understood using a 3-tier architecture.

The first tier is the PN tier, also known as the protocol and network tier. This layer consists of technology for creating a peer-to-peer network, ledger replication, and consensus-based validation.

The second tier is the scalability tier (S-Tier) that runs parallelly with a DLT network and addresses the issues raised by the PN tier.

The third tier is the interoperability tier, which is built upon the previous two tiers. It addresses the integration and interoperability of multiple system deployments and DLT applications.

4 Architecture and System Design

The overview of the system is represented in .... It shows the modules involved in stock exchange system i.e

- Stock Trader
- Ethereum Blockchain Platform
- Smart Contract
- Stock Exchange System

4.1 Design Overview

4.1.1 Sequence Flow Diagram

- The stock trader prepares the transaction data and publishes the transaction to the smart contract API.
- The smart contract applies threshold encryption on the received transaction to make the transaction data secure.
- The transaction is broadcasted to all the nodes in the blockchain network and the transaction is mined.
- The new event gets recorded in the blockchain network and the success of the event is notified to the stock trader.

- The stock exchange system polls for the events arriving from the blockchain network to settle the transaction.
- Once the event arrives at the stock exchange system, the event is handled, and the transaction is settled by the system.
- The stock exchange system then publishes back the successful transaction to the blockchain network.
- The transaction is then broadcasted again to all the nodes in the blockchain network, and the transaction is mined.
- Finally, the success of the event is notified to the stock exchange system.