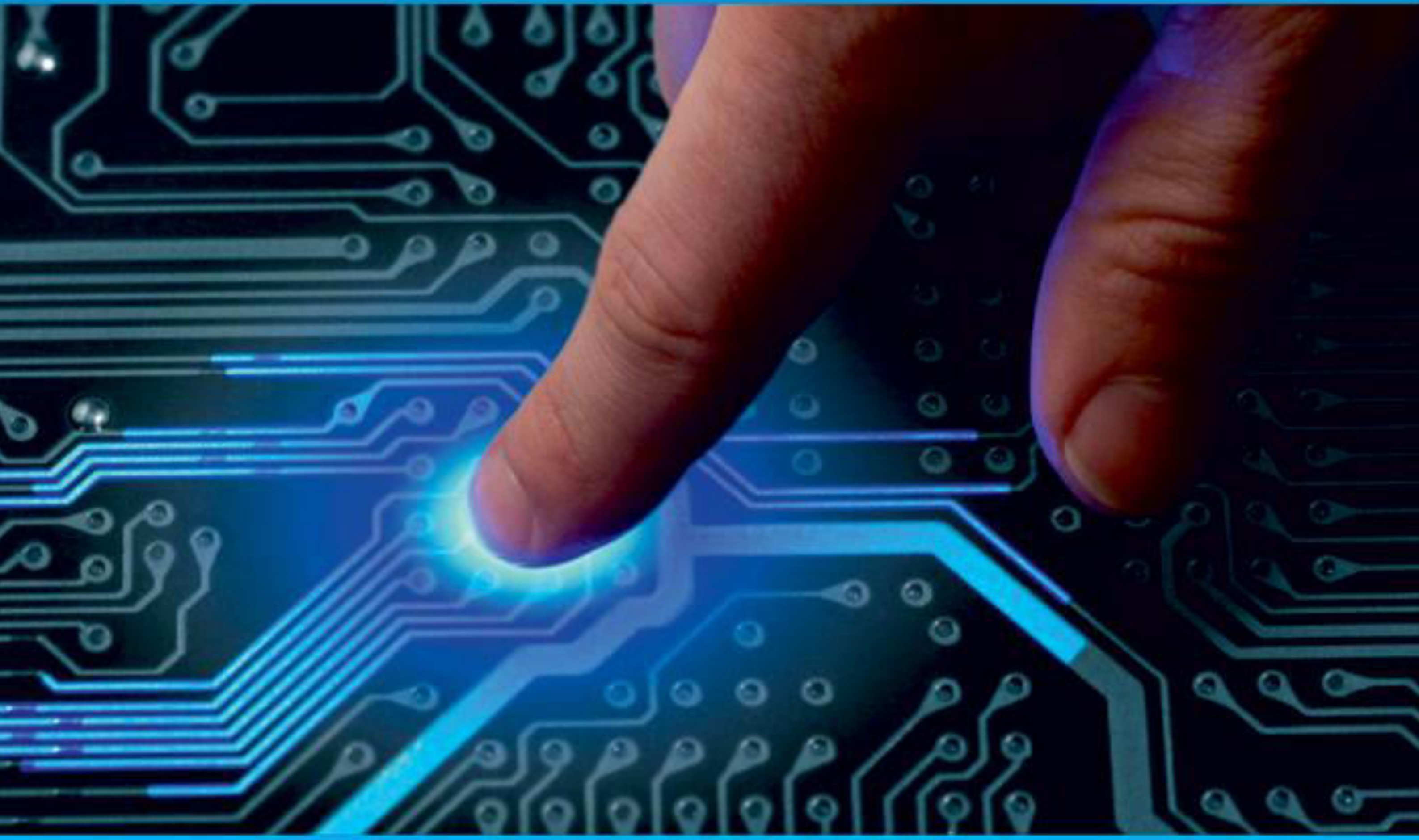
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 7, July 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 7, July 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1107073 |

Privacy-Centric Approach for a Blockchain-Based Stock Exchange Platform

Sourav Dishri, Prof. K Sharath

PG Student, Master of Computer Applications, Bangalore Institute of Technology, Bangalore, India

Assistant Professor, Department of Master of Computer Applications, Bangalore Institute of Technology, Bangalore, India

ABSTRACT: In this research, we provide a privacy-preserving architecture for a distributed stock exchange platform, one that protects the privacy of individual investors by keeping their accounts and trades unlinked. In order to fulfil these privacy needs, the proposed framework (i) uses specialised data generalisation and distortion techniques to conceal the unique account identifier (NIN) and balance information, and (ii) prevents trading transactions from being traced back to their original investors by making the NIN and balance k-anonymous, meaning that k accounts belonging to different investors share the same balance. Furthermore, the anonymization procedure is repeated at regular time intervals (every trading session) to guarantee long-term unlinkability. The suggested system includes capabilities for traceability and non-repudiation in addition to anonymity and unlinkability. The simulation studies on a variety of sized and kinds of markets verify the efficiency of the proposed framework in obtaining complete k-anonymity. Furthermore, we perform many tests with varying degrees of anonymity k to evaluate the impact of the proposed privacy algorithms on the trade execution time. We evaluate our proposed platform by looking at how quickly trades are executed in comparison to a standard stock exchange built on a blockchain that does not protect user privacy. Even under the worst-case circumstances, the findings obtained reveal a reasonable increase in execution time.

KEYWORDS: NIN, Privacy, Stock, Investors, Trade

I. INTRODUCTION

The expansion and maturation of the stock market significantly affect the economic development of any nation. The estimated $70 trillion value of the stock market's worldwide market capitalization is a reflection of the massive scale of the financial transactions and investments made to purchase shares and other securities on the stock market. When investors are assured of a level playing field, they are more likely to participate in the stock market, and when there is a strong financial regulator in place, the market is more likely to function as intended. According to the guidelines set out by regulators, insider knowledge should not be shared with the public during trade. For instance, the well-known stock market manipulation tactic known as front-running may be triggered by the disclosure of investor identifying information. In this kind of assault, the aggressor has access to valuable market data on future trades and transactions before anybody else. Similarly, other investors might gain from the possible price movement of traded shares if they know the names behind significant buy or sell orders and trade either before or after such orders. Because of this, the identities of investors are often treated as private and secret by stock market authorities. According to, and, investing anonymously offers a controlled environment for fair trade and prevents the investor's identity from being traced.

II. LITERATURE SURVEY

The stock market's expansion affects a nation's economy [1]. The worldwide stock exchange market capitalisation was estimated at $70 trillion in 2016, reflecting the huge financial transactions and investments made to acquire shares and other securities [2]. The level of assured fairness that attracts investors and the presence of a well-established financial regulator to define market rules and enforce them are key elements in stock market stability. The regulators prohibit trading using sensitive information that might disrupt the market and manipulate prices [3]. For instance, revealing investor identities might lead to front-running [4]. In such an assault, certain firms may get premium market knowledge about impending transactions and deals. By knowing the names behind big buy or sell orders, other investors might arrange to trade before or after such orders to profit from the share price change. Most stock market authorities consider investors' identities secret and sensitive. [5] and [6] state that anonymous trading protects investors' identities and offers a fair trading structure.

Problem Statement:

Since blockchain replicates data between participants, privacy is not guaranteed. Data distortion-based and data encryption-based blockchain privacy solutions have been suggested. We outline and describe each category's primary approaches below.

Data distortion

Data distortion obscures sensitive information like user identities and geographical locations, providing anonymity. This method hides a buyer/seller transaction without changing its structure or execution in trading. Mixing and generalisation distortion methods do this.

Cryptocurrency transactions are mixed for secrecy. Mixing transactions let users transfer digital currencies between addresses without a direct relationship. Mixing may be centralised or decentralised to anonymize currency. Centralised mixing requires users to submit their coins to a mixing service address, which then delivers the mixed coins to each user's output address. However, relying on a third party to mix renders the system susceptible to a single point of failure and may pose serious privacy concerns if the third party is corrupted or hostile. As seen in, the anonymity provided by centralised mixing increases with the size of the addresses pool. CoinMixer mixes transactions in one to six hours. MixCoin needs each transaction's input-output mappings. If the mixing server is hacked, such data may jeopardise security.

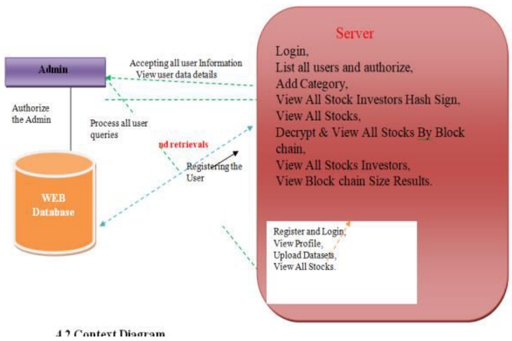


Fig 1.Proposed Flow

III. PROPOSED METHODOLOGY

Determine a decentralised blockchain-based stock exchange platform's privacy requirements.
Create a distortion method that hides the investor's NIN and balance.
Repeated anonymization before trading sessions ensures long-term unlinkability.
Authorised entities may trace investors' anonymous accounts to their original accounts.
Compare execution time with and without the decentralised stock market platform's privacy-preserving architecture to determine the overhead.

Advantages

Investors' trading account data is never shared under the proposed structure. Stock market privacy is ensuring that each submitted trading transaction is unlinkable to its trader's genuine account (NIN, balance) during and after a trading session.

[9] proposes a permission blockchain network with trustworthy members for decentralisation. Permission blockchain secures the ledger to recognised users.

IV. MODEL

Server

Service Providers must login using authentic user names and passwords in this module. After login, he may login, list users, and authorise. Add Category, View All Stock Investors Hash Sign, View All Stocks, Decrypt & View All Stocks By Block Chain, View Investors, View Block Chain Size Results.

Authorise Users

This module lets the admin see all registered users. The admin can see the user's name, email, address, and authorise them.

End User

This module has n users. Register before using. The database stores user data after registration. After registration, he must login using an authorised username and password. After login, user may see profile, upload datasets, and view all stocks.

V. CONCLUSION

This study presents a privacy-preserving system that fulfils block chain-based stock exchange platform privacy criteria. Keeping accounts k-anonymous protects investors' NIN and balance. Repeated NIN and balance anonymity does this. Balances are divided and dispersed to new anonymous accounts to guarantee at least k accounts have the same amount. Each trading session repeats this procedure for long-term unlinkability. We allow block chain ledger modifications with new anonymous accounts for permitted businesses like CSD.We created a non-interactive protocol between investors and authorised companies to generate anonymous accounts without communication overhead. The architecture provides tractability and non-repudiation for trade transactions by having the authorised entity update the ledger. We ran many tests with varied market sizes, anonymity levels, and investor balance distributions to test the framework's privacy performance. The solution's efficiency showed 100% anonymity with acceptable transaction execution time overhead.

REFERENCES

1. "Relation between economic growth and stock market development," Afr. J. Bus. Manage., vol. 4, no. 16, pp. 3473_3479, 2010. [1] M. S. Nazir, M. M. Nawaz, and U. J. Gilani.
2. Stock markets' contributions to economic expansion and long-term prosperity are discussed in [2]. Retrieved on January 21, 2021. [Online].
3. Accessible at: https://unctad.org/system/_les/of_cial-document/WFE_UNCTAD_2017_en.pdf
4. "Privacy-protected blockchain system," in Proc. 20th IEEE Int. Conf. Mobile Data Manage. (MDM), June 2019, pp. 457_461. [3] P. Zhong, Q. Zhong, H. Mi, S. Zhang, and Y. Xiang.
5. [4] C. Chaturvedula, N. P. Bang, N. Rastogi, and S. Kumar, "Price manipulation, front running, and bulk trades: Evidence from India," Emerg. Markets Rev., volume 23, issue 6, pages 26–45, June 2015.
6. "Why do traders choose to trade anonymously?" [5] C. Comerton-Forde, T. J. Putni2, and K. M. Tang. August 2011 issue of the Journal of Financial Quantitative Analysis, pages 1025-1049.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING