Research Article

Enhancing the Security using Blockchain-Based Privacy-Preserving Framework for Stock Exchange Platform

Rohith Davuluri
Dept. of CSE
QIS College of Engineering & Technology
Ongole-523001, India

Preetham Roy Patibandla
Dept. of CSE
QIS College of Engineering & Technology
Ongole-523001, India

Adithya Kalastri
Dept. of CSE
QIS College of Engineering & Technology
Ongole-523001, India

Supriya Kommu
Dept. of CSE
QIS College of Engineering & Technology
Ongole-523001, India

Suguna Sri Andukuri
Dept. of CSE
QIS College of Engineering & Technology
Ongole-523001, India

Sheema.Sk
Asst. Professor, Dept. of CSE
QIS College of Engineering & Technology
Ongole-523001, India

Abstract— **This article introduces a privacy-preserving architecture for a distributed stock exchange platform, which keeps investors' accounts and trades private and untraceable. 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. In addition, the anonymization procedure is carried out on a periodic basis (after each trading session) to provide permanent anonymity. The suggested framework includes not only anonymity and unlinkability but also traceability and non-repudiation. 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 undertake a number of 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.**

I. INTRODUCTION

There is a strong correlation between the health of a country's economy and its stock market . As a result of the massive scale of the financial transactions and investments made to purchase shares and other securities provided on the stock market, the worldwide market capitalization of the stock exchange . 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 smoothly. Regulators prohibit the dissemination of material nonpublic information during trade due to concerns that it might disrupt the market and lead to manipulative pricing . For instance, the well-known stock market manipulation assault front-running may be triggered by the disclosure of information relating to investor identification. In such an assault, certain companies may gain an advantage by gaining access to sensitive market data about future deals and trades. 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 , anonymous trading offers a controlled environment for fair trade and prevents the investor's identity from being traced.

For a more trustworthy, open, and distributed financial system that doesn't depend on middlemen, block chain technology has just been developed . New decentralised stock exchange platforms have been designed in recent years to address inefficiencies in the traditional stock market, such as the market's reliance on a single point of failure, the lengthy time required for financial settlements, and the lack of transparency afforded to investors. However, the security of investors' personal information and account balances has not been taken into account by the aforementioned initiatives. While there has been significant effort put into addressing privacy problems in block chain-based solutions via the use of data distortion and encryption methods, these solutions are not tailored to the anonymity, unlinkability, traceability, and non-repudiation needs of the stock market.

For systems like the stock market, where sensitive information like investors' names must be kept private, block chain's data replication among various participants is a need. Investors on the stock market platform are identified by their NIN and their cash or share balance. The NIN is being used to place orders on the platform, where they will be matched with other orders and eventually result in transactions. The investor's identity must be concealed so that other parties are unable to determine who placed an order or received a particular deal. In light of the aforesaid privacy concerns, we present in this research a privacy-preserving block chain-based stock market platform that employs data distortion and encryption to shield investor information. Under the proposed system, each trader is assigned a unique set of anonymous accounts for usage during that session's trading alone. The initial investment sum is likewise divided up and distributed across the newly formed anonymous accounts. A data distortion approach based on the k-anonymity model is used to guarantee unlinkability and prevent an attacker from tracing and attaching the several anonymous accounts to the original investor's account. If there are k accounts in the market, then each anonymous account must have a balance of at least k1. To make matters worse, the distortion approach is redone at the start of each new trading session, making it much more difficult for an attacker to construct trade patterns from the anonymous accounts and deduce beneficial information throughout the transaction. The proposed architecture also enables auditing of transactions by permitted organisations through the tracking of anonymous accounts back to their rightful owners.

II. RELATED WORKS

Mexchange: A Ring Signature and Stealth Address-Based Blockchain-Based Framework for Confidential Health Data Exchange

By "health information exchange" (HIE), we mean the coordinated administration of patients' health records and their safe, encrypted transmission between various providers. HIE helps to elevate the standard of healthcare and streamlines administrative processes. Because of these benefits, many involved in healthcare have pushed for the use of HIE. However, barriers to HIE's wider adoption include concerns about security, privacy, and expense. Blockchain-based HIE has been proposed in recent research as a means of addressing security and privacy concerns. The privacy concerns raised by studying blockchain transaction senders and recipients have so far been ignored in previous blockchain-based HIE research. To circumvent this privacy problem, we propose mexchange, a new blockchain-based privacypreserving HIE. Mexchange does this by masking the identities of both the sender and the recipient in the transaction. We propose a blockchain-based HIE that makes use of smart contracts and a workflow that incorporates ring signature and stealth address. The mexchange private Ethereum network and its software components are explained. We conduct a quantitative analysis of mexchange by monitoring the latency and throughput of transactions. Furthermore, we conduct a qualitative analysis of mexchange in accordance with the standards established by the Office of the National Coordinator for Health Information Technology (ONC). In addition, we use STRIDE to predict potential threats. Finally, we examine the differences between mexchange and Ancile, fhirchain, the Integrating the Healthcare Enterprise XDS, and medrec. By addressing concerns about patient privacy and data security, the mexchange facilitates the adoption of blockchain-based HIE systems.

A Multi-Level Blockchain Security and Privacy Infrastructure for Cluster-Based vanetcomposed of A. F. M. Suaib Akhter1, Mohiuddin Ahmed2, A. F.

M. Shahen Shah3, Adnan Anwar4,* and Ahmet Zengin

There is a need for better security and privacy preserving authentication method, yet studies have shown that Cluster-based Medium Access Control (CB-MAC) protocols are effective in managing and controlling Vehicular Ad hoc Networks (vanets). To this purpose, we propose a multi-tiered, blockchain-based authentication scheme that protects users' anonymity. The document gives a detailed account of how authentication centres were established, how automobiles were registered, and how keys were generated. In the proposed architecture, all vehicle data is stored in a global authentication centre (GAC), while each vehicle cluster's local authentication centre (LAC) maintains a blockchain for fast data transfer. To address the problems with the existing MAC protocols, we also propose a new control packet format based on the IEEE 802.11 standards. Additionally, the safety and non-safety of message transmission is taken into account throughout the cluster creation, membership, cluster-head selection, merging, and departing operations. High-speed 5G internet is used for all blockchain-related communication, and all data is encrypted before transmission using the RSA-1024 digital signature process to ensure privacy and security. Our proof of concept takes into account many virtual machines and implements the authentication scheme. Using extensive trials, we demonstrate that our technique significantly outperforms the state-of-the-art solutions in terms of both time and space. Furthermore, the suggested transmission protocols have been shown to provide better results than the standard MAC and benchmark approaches in terms of throughput, latency, and packet dropping rate in numerical studies.

Cryptography and Privacy-Preserving Smart Contracts on the Blockchain: Hawk Charalampos Papamanthou, Zikai Wen, Elaine Shi, Ahmed Kosba, Andrew Miller, University of Maryland, and Ahmed Kosba, Cornell University

A new kind of "smart contract" built on top of cryptocurrency blockchains eliminates the need for third parties in transactions between parties who don't trust each other. The distributed ledger makes sure that the right people get paid when contracts become broken or cancelled. However, existing technologies do not protect user data during transactions. The blockchain publicly displays all transactions, including the transfer of funds between anonymous parties and the total amount exchanged. We introduce Hawk, a distributed smart contract platform that protects the privacy of financial transactions by not recording them in the clear on the blockchain. Our compiler automatically generates an efficient cryptographic protocol where contractual parties interact with the blockchain, using cryptographic primitives like zero-knowledge proofs, so that a Hawk programmer can write a private smart contract in an intuitive manner without having to implement cryptography. Because of this, we are the first to explicitly describe and reason about the security of our protocols using the blockchain paradigm of cryptography. There is value in the formal modelling on its own. We recommend that developers using blockchain technology for their applications follow this formal approach.

III. SYSTEM ANALYSIS

Given that data are copied between multiple participants, blockchain is not designed to offer any kind of privacy protection for its users. Several methods have been presented in order to maintain privacy in blockchain, and these solutions may be broken down into two primary categories: (i) techniques that are based on data distortion, and (ii) approaches that are based on data encryption [10]. Following this, we will present an overview of each area and explore the primary methods that fall under each of those categories.

Data Distortion

[10], [11] Data distortion is a method that offers anonymity by making it difficult to correlate certain sensitive information, such as geographical locations and user identities, to the users' real data. This approach is used to protect users' privacy. This method is used in the context of trade, and its goal is to conceal the identity of a buyer or seller in a transaction without changing the structure of the transaction or impacting how it is carried out [10], [12]. In order to accomplish this objective, a number of different types of distortion, such as mixing and generalisation methods, are used [13].

In order to improve the level of secrecy afforded by bitcoin transactions, mixing strategies have been implemented. Users are able to shift digital currency from one user address to another through mixing transactions since there is no direct relationship between the addresses. To protect users' privacy when transacting in cryptocurrency, mixing may be carried out either via a centralised or decentralised service. When using centralised mixing [10], a third party is responsible for doing the mixing. This is done by asking users to submit their coins to a mixing service address, which then delivers the mixed coins received to a variety of output addresses [14]. However, since the mixing must be performed by a third party, the system is susceptible to having a single point of failure, which may lead to significant privacy concerns if the third party is breached or behaves maliciously [15], [16]. Also, according to research done in [13], the level of anonymity that may be obtained by centralised mixing is related to the size of the addresses pool. This means that the more addresses there are in the pool, the better the mixing service will be able to conceal its users' identities. Coinmixer [17] is a service that mixes coins and needs, on average, anything from one to six hours to finish mixing transactions. Mixcoin [18] is another service that may be used, but using it needs you to have access to the actual mappings that exist between each transaction's input and output addresses. If the mixing server is hacked, the storage of such information on the server might pose major problems with data security.

The Encryption of Data

Encryption is an additional method that may be used in a blockchain network environment in order to maintain the confidentiality of transaction data [10, 11]. secret ring signature [5, 9], [3], secret transaction [13], Zero-Knowledge Proofs [20], and homomorphic encryption [10] are some of the encryption-based approaches that are utilised in blockchain to provide privacy.

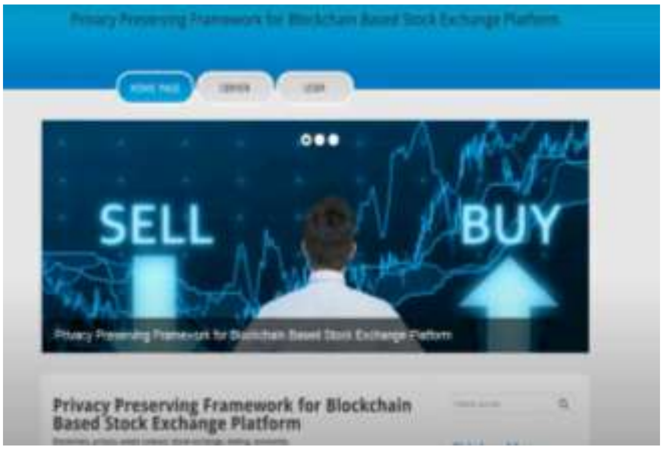
The process of signing a transaction by a group of participants is referred to as confidential ring signature [20]. During this procedure, a verifier is unable to establish which member of the group is responsible for producing the signature on the transaction. To put it another way, the public key that generates the transaction is masked among the other public keys that are part of the same group. When a group is formed, it is done so in such a manner that all of its members share the same amount of bitcoin and help safeguard the member who is really sending the transaction [19]. This method has a significant benefit over the mixing technique in that the owner of the public key may create the transaction on their own without having to depend on any third parties. This results in increased anonymity and protection from prying eyes.

The most significant drawback, on the other hand, is that in order to create a group signature for a transaction in order to deliver a certain quantity of coins, there should exist other users that share the same amount of coins. However, this is not always guaranteed to be the case. Because there is no group manager to assign new members to the group, revoke group membership, or handle disputes, another drawback is that it is not feasible to identify the signer of a transaction in the event that there is a disagreement [12]. This is because there is no one to take on the function of administering these responsibilities. Monero employs a methodology that is conceptually similar to this one [6]. Monero is a decentralised cryptocurrency that hides the transaction value as well as the addresses of both the senders and the recipients. This is done to ensure that users' privacy and anonymity are protected

IV. METHODOLOGY

Examine and specify the criteria for a decentralised blockchain-based stock exchange platform's required level of privacy protection. Create an innovative distortion approach with the goal of concealing the unique identity (NIN) of the investor as well as their balance. Achieve unlinkability over the long term by carrying out repeated anonymization procedures just before the beginning of each trading session. Make it possible for authorised organisations to trace investors' transactions and connect their anonymous accounts to their primary accounts using the tracing capabilities. Examine the extra burden by contrasting the amount of time required to carry out an operation with and without the privacy-protecting framework provided by the decentralised stock exchange platform.

. Fig 1 Home Page


SELL
BUY
Privacy Preserving Framework for Blockchain Based Stock Exchange Platform
Privacy Preserving Framework for Blockchain Based Stock Exchange Platform

V. RESULTS AND DISCUSSION

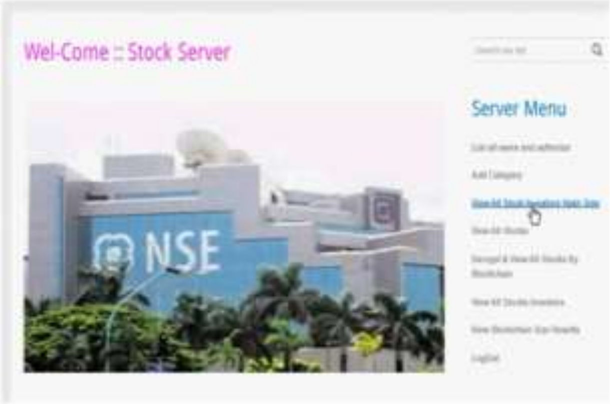


Fig 2 : Server Page

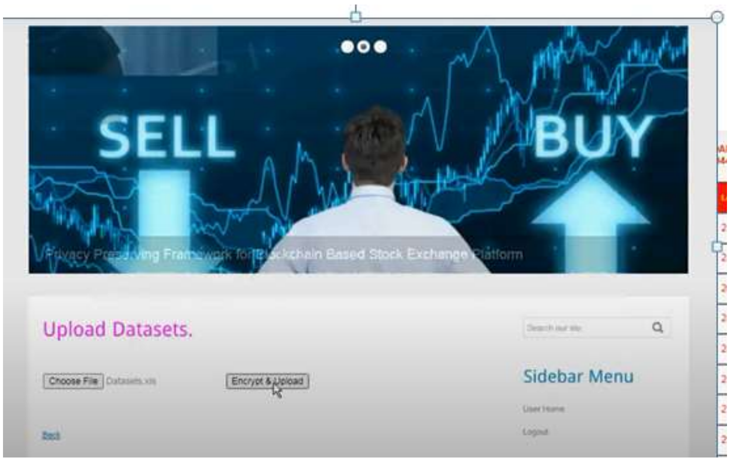
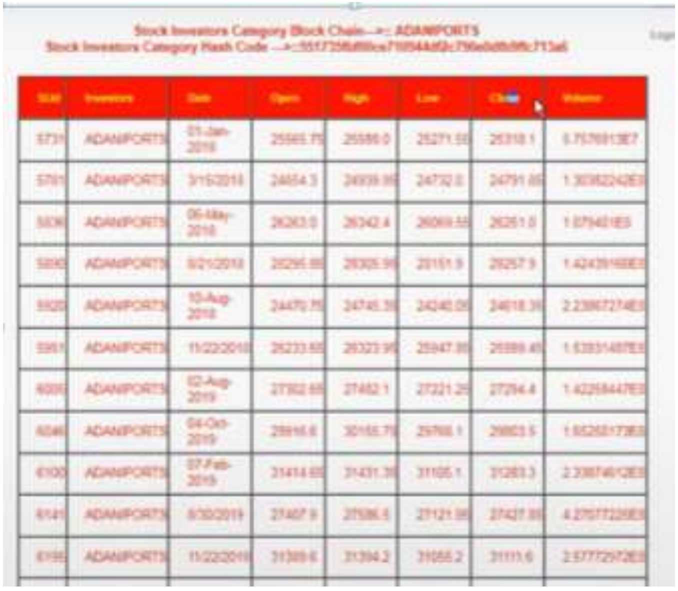


Fig 3: Upload Dataset



Stock Investors Category Block Chain--->:: ADANIPORTS
Stock Investors Category Hash Code --->::5517256[illegible]

SId	Investors	Date	Open	High	Low	Close	Volume
5731	ADANIPORTS	01-Jan-2018	25565.75	25586.0	25271.55	25318.1	5.757691387
5781	ADANIPORTS	3/15/2018	24654.3	24939.95	24732.0	24791.65	1.3036224E8
5836	ADANIPORTS	06-May-2018	26263.0	26342.4	26069.55	26251.0	1.0794E8
5890	ADANIPORTS	8/21/2018	26296.85	26305.95	26151.5	26257.5	1.4243916E8
5920	ADANIPORTS	10-Aug-2018	24470.75	24745.35	24240.05	24618.35	2.2386727E8
5961	ADANIPORTS	11/22/2018	26233.65	26323.95	25947.35	25999.45	1.6393148E8
6005	ADANIPORTS	02-Aug-2019	27302.65	27482.1	27221.25	27294.4	1.4225844E8
6046	ADANIPORTS	04-Oct-2019	29916.6	30155.75	29766.1	29803.5	1.6526173E8
6100	ADANIPORTS	07-Feb-2019	31414.65	31431.35	31105.1	31283.3	2.3387461E8
6141	ADANIPORTS	8/30/2019	27407.9	27536.5	27121.95	27427.85	4.2707722E8
6195	ADANIPORTS	11/22/2019	31389.6	31394.2	31055.2	31111.6	2.5777297E8

Fig 4: Stock Investors

VI. CONCLUSION

The privacy needs of a blockchain-based stock exchange platform have been addressed in this research via the presentation of a privacy-preserving architecture. By making sure every account is k-anonymous, this framework protects the confidentiality of investors' account information (NIN) and balances. Repeatedly concealing the NIN and the account amount does this. In order to guarantee that at least k accounts have the same amount, we construct new anonymous accounts and divide and distribute the funds from the existing anonymous accounts among them. Every time a new trading session begins, the procedure starts over again to guarantee permanent delinkability. New, anonymous accounts used only by sanctioned parties (like CSD) are allowed to be added to the block chain ledger.In order to avoid any communication costs associated with creating anonymous accounts, we created a non-interactive protocol between investors and the authorised businesses. The suggested architecture guarantees tractability and non-repudiation features for trade transactions by depending on the authorised entity to update the ledger. We performed many tests with varying market sizes, anonymity levels, and investor balance distributions to verify the efficacy of the proposed framework in ensuring the needed privacy. The results proved the effectiveness of the method, showing that full anonymity can be maintained at the cost of a tolerable increase in transaction processing times.

REFERENCES

[1] M. S. Nazir, M. M. Nawaz, and U. J. Gilani. Stock markets' contributions to economic expansion and long-term prosperity are discussed in

[2]. As of the 21st of January, 2021. [Online]. The full report may be seen at: "Privacy-protected blockchain system," Mobile Data Manage. (MDM),

[3] P. Zhong, Q. Zhong, H. Mi, S. Zhang, and Y. Xiang.

[4] C. Chaturvedula, N. P. Bang, N. Rastogi, and S. Kumar, "Price manipulation, front running, and bulk trades: Evidence from India," Emerg. Markets Rev.

[5.] Why Traders Prefer Anonymity, by C. Comerton-Forde, T. J. Putni2, and K. M. Tang

[6]. "Market manipulation as a security challenge," 2019 arxiv:1903.12458, V. Mavroudis.

[7]. "Blockchain access privacy: Challenges and directions," R. Henry, A. Herzberg, and A. Kate.

[8] "Decentralising the stock exchange using blockchain an ethereum-based implementation of the bucharest stock exchange," in Proc.

[9]. C. Pop, C. Pop, A. Marcel, A. Vesa, T. Petrican, T. Cioara, I. Anghel, and I. Salomie.

[10]. Consortium blockchain-based decentralised stock exchange platform. H. Al-Shaibani, N. Lasla, and M. Abdallah.

[11]. "RZKPB: A privacy-preserving blockchain-based fair transaction technique for sharing economy," by B. Li and Y. Wang, in Proc.

[12]. C"FPPB: A fast and privacy-preserving method based on the permissioned blockchain for fair transactions in sharing economy," [13]. B. Li, Y. Wang, P. Shi, H. Chen, and L. Cheng, Proc. 17th IEEE Int. Conf. Trust, Secur. Big Data Sci. Eng. (trustcom/bigdatase),

[14]. "A privacy-preserving Ecommerce system based on the blockchain technology,"

[15] "An examination of bitcoin laundry services," by T. De Balthasar and J. Hernandez-Castro.

[16] "Anonymity for bitcoin from safe escrow address.

[17] "Towards anonymous, unlinkable, and con_dential transactions in blockchain," by K. Singh, N. Heulot, and E. B. Hamida.

[18] Coinmixer. Until 2021. [Online]. J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. Kroll, and E. Felten.

[19] Sybil-Resistant Mixing for Bitcoin, by Gregory Bissias, Andrew Ozik, Brian Levine, and Mario Liberatore (2019).

[20] Secure and anonymous decentralised bitcoin mixing, Future Gener. Comput. Syst., vol. 80, pp. 448_466, March 2018; J. H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, and K. Wehrle.

[21] Coinjoin. Until 2021. [Online]. To access, visit https://coinjoin.io/en.

[22] "Anonymous coinjoin transactions with arbitrary values," in Proc.

[23] "coinparty: Secure multi-party mixing of bitcoins," by J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle,

[24] "Ef_cient k-anonymization using clustering algorithms," by J.-W. Byun, A. Kamra, E. Bertino, and N. Li,

[25] X. He, H. Chen, Y. Chen, Y. Dong, P. Wang, and Z. Huang, "Clusteringbased k-anonymity.".