Strategy for Upholding Confidentiality on Blockchain-based Securities Trading Infrastructure

S. Pandikumar, Ravikumar N K

ABSTRACT

This paper proposes a privacy resilient framework for a decentralized stock exchange platform is proposed to provide anonymity and unlinkability of accounts of the investors and the trading activity respectively. The proposed framework addresses these privacy requirements by (i) employing tailored data generalization and distortion methods to anonymize anonymize both the unique account identifier (NIN) and balance information and (ii) unlink the trading transactions from their original investors by making both the NIN and balance k-anonymous; i.e., k accounts held by different investors have the same balance. Additionally, to provide long-term unlinkability, the anonymization is conducted repeatedly at predetermined intervals (each trading session). There are also traceability and non-repudiation elements added to the proposed framework alongside the anonymity and unlinkability properties. The simulation scenarios for different market sizes and types provide assurance that the proposed framework performs very well in delivering full k-anonymity. Additionally, in order to evaluate the overhead that the proposed privacy algorithms add on the trading execution time, we do some experiments using several anonymity levels k and compare the execution time of our proposed platform to a standard blockchain-based stock exchange without privacy. Based on the tests we carry out for the most pessimistic scenarios, our results indicate acceptable overhead in execution time.

Index Terms: Blockchain, Decentralized stock exchange, Privacy preservation, K-anonymity, Data anonymization, Data distortion, Unlinkability, Traceability, Smart contracts, Financial data security.

I. INTRODUCTION

The rapid growth of decentralized finance (DeFi) has opened the opportunity for blockchain stock exchange platforms to offer transparency, immutability, and trustless interactions. Despite offering distinct advantages over traditional, centralized systems, including the properties of transparency, immutability, and trustless interactions, augmenting the positive aspects of decentralized stock exchanges creates another set of problems related to user privacy [1]. In the DeFi public blockchain environment, the public nature of chains can expose sensitive information about investors, such as account identities, account balances, and trading activities. This reduces privacy to the investors, which is part of the core of confidentiality and might scare away institutional and retail investors towards decentralized trading systems [2]. Providing privacy protection may help mitigate these anxieties over user privacy. Ideally, privacy assurances can be built in to decentralized stock markets without deterritorializing important functions such as traceability and accountability. Privacy and traceability and accountability are challenging to realize, however, due to their conflicting nature [3]. Present solutions fall short either by promising ineffective privacy assurances or incurring in prohibitive computation overhead that negatively impacts system performance and scalability. In this paper, we develop a new privacy-protection framework for decentralized SEFs. The new framework offers anonymity and unlikability for investor accounts and trading histories, while retaining requirements such as traceability, and non-repudiation [4]. The mechanism uses a proprietary combination of data generalization and distortion methods to anonymize individual account identifiers (NINs) and balances such that every account is k-anonymous from at least k-1 other accounts.

II. LITERATURE REVIEW

The increasing prominence of financial markets around the world has helped reinforce the overall view that 'finance' is a notable contributor to economic growth. Thus, it is no surprise that the emphasis continues to be on economic growth and stock market development. The stock market, since it is a large support of a country's economy, has an important part to play in the development of the industry and commerce that indirectly, to a fair extent, continues to support the country's economy [5]. This is part of the reason why the industrial organizations, government advisers, and even the nation's central bank have a strong eye of interest on the stock market. The stock market is important not only from an investor's point of view but also from an industry perspective.

The World Federation of Exchanges (WFE) and the United Nations Conference on Trade and Development (UNCTAD) exploratory report examines the role of stock exchanges3 in economic development – and sustainable development, and outlines this in the report. Chapter 1 begins with a description of what a stock exchange looks like presently and what its context looks like to operate in. It then describes the debates in economic theory about stock exchanges and economic development. It states not only the positive effects of stack markets to spur economic growth but also some of the imperfections and common criticisms of markets. The report then describes functionally what an exchange does and provides economic effect[6]. Finally, the report summarizes exchange activity worldwide.

The blockchain uses a decentralized consensus mechanism to keep the books immutably, making the blockchain smart contract system secure. As for the current blockchain systems, all user data are pushed to the blockchain and can be seen by everyone in the blockchain. However, people these days are more and more concerned about personal privacy and therefore, the future blockchain smart contract system will require not only immutability but privacy of the users. In order to realize this goal, in this paper we suggest a privacy-encrypted blockchain system where the data are encrypted during a period we control [7]. User data can still be seen from a historical point of view but our design really has the potential to protect user privacy and impersonators effectively, making it ultimately safer and healthier for the system overall.

Consortium blockchain is being used in Internet of Things (IoT) supply chains for tracking and securing supply chain data, including manufacture, storage and shipping. However, all supply chain data in a consortium blockchain are available for public reading to all involved parties. This raises a wide range of concerns around supply chain data privacy. Some existing attribute-based encryption (ABE) based blockchain systems targeting supply chain data privacy either create new security concerns, or lack the feasibility analysis for IoTs. In this paper, we present a new multiauthority ABE (MA-ABE) based blockchain system to provide data privacy protection for supply chains on IoTs. In particular, we developed a four-way tradeoff optimization system such that the decentralization of the system, its scalability, and storage usage are not adversely impacted by the improved privacy [8].

We evaluate the effects of bulk trade on share prices in India done between 2004 to 2012. In an event study modeling we see the tremendous effects of bulk trades on share prices with cumulative returns being very considerable during the time of trades for both NSE and BSE. Buy trades have considerably positive cumulative abnormal returns meaning buy trades add value to the firm on average. After that, we regress the cumulative average abnormal returns of various windows against the different independent variables. Moreover, the effect of all such variables that we consider are greater in the case of buy trades relative to sell trades.

This article explores the use, determinants, and consequences of anonymous orders in an environment where brokers' identities on the trading screen are voluntarily disclosed. We find that the majority of trading occurs non anonymously, which is inconsistent with earlier literature claiming that liquidity flows to anonymous markets. By selectively using anonymity when it is beneficial, traders reduce their execution costs. Traders select anonymity based on a combination of factors, including order source, order aggressiveness and size, time of day, liquidity, and expected costs of execution [10]. We conclude by explaining the implication of anonymous orders on market quality and speculate on implications on exchange design.

Modern equity exchanges are based on order matching systems and millions of investors use order matching systems on a daily basis. Their operation is highly regulated within the framework of multiple regulatory measures that provide openness and fairness in markets. Even with these measures, however, market manipulation is looming large. In our paper, we concentrate on a type of market manipulation methods that take advantage of factors concealed in the mechanics of the exchange (mechanical arbitrage). This type of device is employed by predator traders who learn more about the makeup of the exchange than other participants in the market [11]. In our opinion, these activities can be severely disrupted by technical answers to the mechanical arbitrage problem. We have identified the threat situation in the first instance, summarized fair markets and their security qualities, and given a few approaches to mitigation. The paradoxes of the historical centralized stock exchange system which are addressed in this published work are low transaction charges, central management attacked and unavailable when needed upon market functions and algorithms, by developing a concept of new architecture of a decentralized stock exchange and open continuous market [12]. It is possible that the proposed blockchain approach can address the weakness of the centralized stock exchange architecture through the provision of integrity and security of the owners assets and orders, self-executing smart contracts between parties and democratic and trusted decisions about the execution / settlement of the orders, through consensus algorithms.

III. PROBLEM STATEMENT

A notable, but difficult to achieve element of building trust, avoiding market manipulation, and expediting the potential of decentralized stock exchange is the principle of investor confidentiality in the context of decentralized finance and securities trading built upon blockchains. The traditional blockchain utility, despite the immediacy and transparency it offers, inevitably exposes account identities, balances, and trading history to the eyes of all financial ecosystem participants. Such public-facing elements undermine isolating characteristics, as malicious stakeholders can discern patterns in trading, as well as correlate trades to individual actors, and/or manipulate confidential financial data.

Existing privacy-protecting solutions such as centralized mixing services and basic encryption provide little balance to the issues of confidentiality, traceability, and the overall efficiency of the system. They may create single points of failure, use a wide variety of computations, or limit the possibility of supervision by regulatory bodies. Failure to explore the opportunity to incorporate decentralized exchanges that promote strong anonymization, unlinkability, and compliance with financial legislation reduces an effective privacy feature across different decentralized exchanges.

To overcome these issues, this project proposes a privacy-resilient framework for a decentralized stock exchange platform that anonymizes sensitive investor data using methods such as k-anonymity, fine-grained data distortion, and frequent re-anonymization. The proposed system is unlinkable across trading sessions and can support regulatory auditing of all authorized users with traceability and non-repudiation, creating a secure and efficient blockchain trading system that is regulatory compliant.

IV. METHODOLOGY

This project will adhere to the following guidelines in order to ensure that investor privacy is preserved without impairing the operational and functional integrity of a decentralized stock exchange. Essentially the framework applies a mixture of data distortion, anonymization and controlled traceability. The framework starts with an in-depth analysis of privacy requirements that are peculiar to trading securities. Investor identifiers such as National Identification Numbers (NINs) and, account balances, in this area are exceedingly secretive, and should not be divulged or attributed to a person without the assistance of the relevant authority. Based on that, this framework is privatizing NIN and balance data as at an always anonymous state, by state-of-the-art data distortion techniques. The means are generalization, where the granularity of the data (e.g., sets of values of balances, rather than values of balances) is bypassed, and random perturbation modifies the values of data to prevent and conceal the buyer/seller relationship, without interfering with the trading logic.

The most important innovation is the introduction of k-anonymity in which account information of individual investors are made indistinguishable with at least k -1 other accounts. It is achieved by clustering accounts of investors with the same range of balances and anonymizing their NINs into non-unique, synthetic identities. To improve unlinkability even more, this anonymization is not only a one-time event, it is done again before each trading session, so that if an attacker were able to correlate information from one session, the same information in the next session would be meaningless. This re-anonymization for each session protects against long-term correlation attacks and provides secure unlinkability over time, because all trades will be exchanged using these anonymized IDs. The actual correlation of original IDs to anonymous IDs is stored in a secure encrypted audit log, which is only accessed by regulatory bodies with approved procedures and rigorous legal guidelines.

The framework will be evaluated for feasibility by deploying the system on a permissioned blockchain, authenticating and trusting all participants (brokers, exchanges, regulators). The blockchain will provide immutable trade logs, and smart contracts will govern the trading rules, which may include privacy restrictions, thus allowing the regulations to be enforced on the blockchain. System capacity will be evaluated through several scenarios including using varying market sizes and levels of k-anonymity. Each of the scenarios will be examined to show the impact of increased k on system memory and execution time. In addition, to validate the privacy guarantees, artificial datasets will be used to simulate multiple attacks against the system (linkage attack, re-identification, and pattern analysis).

The proposals also has a traceability module, that will allow regulated parties to re-identify individuals to reverse anonymization, when freedom of information, or litigation is required in the case of fraud. The system will comply with financial regulations. Overall they will create a singular trading infrastructure that combines privacy, security, and compliance that is practical in the real-world. The system architecture consists of three main blocks: Server, Admin and End User with a Web Database in all cases. Admin provides user authentication and categories, and looks after all stock-related queries; and retrieves and saves data securely from the database. Server performs key functions such as logging in, decrypting stock data over blockchain and managing investor data. End Users can sign up, log in, access their profile, add datasets, and view stock data. This structure allows for secure, controlled, role access to all parts of the trading information.

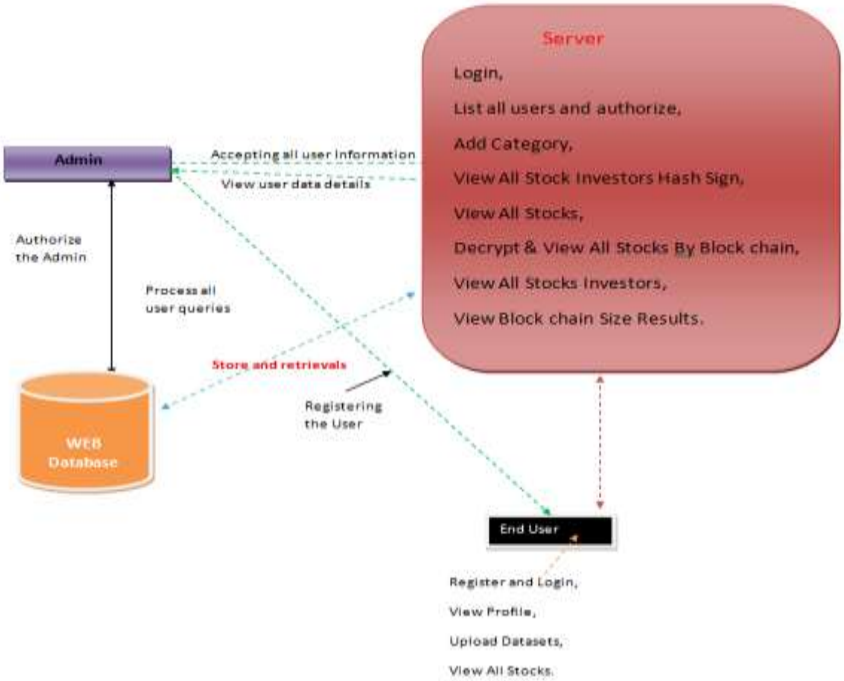

Fig: 1 System Architecture

V. RESULT AND ANALYSIS

By executing the server and user modules, the system effectively offers a secure, systematic, and interactive environment for maintaining stock data and user involvement. The server module maintains control of administrator-level activities for user authorization, category management, verification of stock datasets, and security using blockchain, which ensures data integrity and transparency. At the same time, the user module enables users to maintain their profiles, upload useful stock datasets, and retrieve detailed stock information. The incorporation of blockchain decryption provides additional assurance and trust along with authenticity in the information exchanged throughout the platform. In general, the system enables effective cooperation between administrators and users to secure trustworthy handling of data along with open investor involvement.

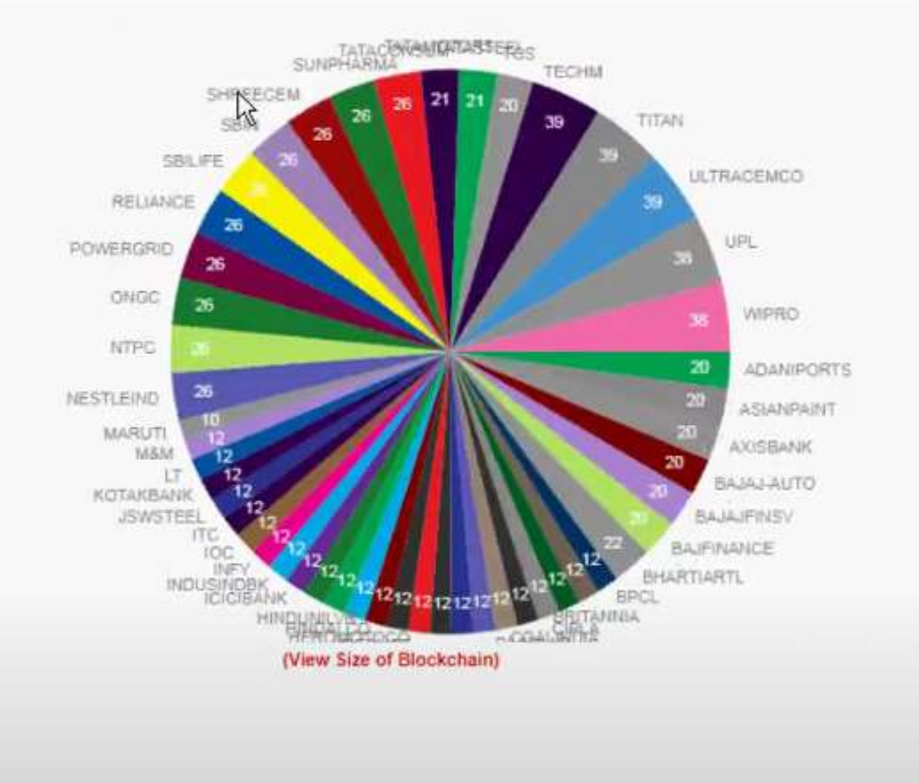

Fig: 2 Result Analysis

VI. CONCLUSION AND FUTURE DIRECTION

Conclusively, the developed system functionally links the user interaction and administrative oversight in a stock data management space. The user's interface utilises blockchain technology to ensure validation, transparency, and integrity of stock data sets. The modular design is based on a secure server-side administrative control and user-based client module to allow data to be processed using user management and protocols around permission. This mutual advantage led to the increased credibility, traceability and effectiveness of stock data analysis and share.

The system may also be extended with AI and ML models to facilitate various predictive analytics, decisions, anomalie detection and automated stock recommendations, Amassing real-time network-sourced data feeds via APIs, and a decentralized identity (DID) solution to facilitate more rigorous levels of authentication and privacy. Additionally, this system improvement will be achieved through interactive data visualizations and dashboards; cross-platform support (mobile and cloud); and automation of smart contracts to facilitate validation, reward, and compliance regimes to enable it to keep on becoming a full-fledged and intelligent and scalable stock data management and analytics platform.

REFERENCES

[1] M. S. Nazir, M. M. Nawaz, and U. J. Gilani, "Relationship between economic growth and stock market development," Afr. J. Bus. Manage., vol. 4, no. 16, pp. 3473–3479, 2010.

[2] The Role of Stock Exchanges in Fostering Economic Growth and Sustainable Developmnt. Accessed: Jan. 2 1, 2021. [Online]. Available: https://unctad.org/system/files/official-document/WFE_UNCTAD_2017_en.pdf

[3] P. Zhong, Q. Zhong, H. Mi, S. Zhang, and Y. Xiang, "Privacy-protected blockchain system," in Proc. 20th IEEE Int. Conf. Mobile Data Manage. (MDM), Jun. 2019, pp. 457–461.

[4] C. Chaturvedula, N. P. Bang, N. Rastogi, and S. Kumar, "Price manipulation, front running and bulk trades: Evidence from India," Emerg. Markets Rev., vol. 23, pp. 26–45, Jun. 2015.

[5] C. Comerton-Forde, T. J. Putniš, and K. M. Tang, "Why do traders choose to trade anonymously?," J. Financial Quant. Anal., vol. 46, no. 4, pp. 1025–1049, Aug. 2011.

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

[7] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," IEEE Security Privacy, vol. 16, no. 4, pp. 38–45, Jul./Aug. 2018.

[8] C. Pop, C. Pop, A. Marcel, A. Vesa, T. Petrican, T. Cioara, I. Anghel, and I. Salomie, "Decentralizing the stock exchange using blockchain an ethereum-based implementation of the bucharest stock exchange," in Proc. IEEE 14th Int. Conf. Intell. Comput. Commun. Process. (ICCP), Sep. 2018, pp. 459–466.

[9] A. Ramiro and R. de Queiroz, ''Cypherpunk,'' Internet Policy Rev., vol. 11, no. 2, pp. 1–14, 2022.

[10] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, ''Blockchain consensus algorithms: A survey,'' 2020, arXiv:2001.07091.

[11] A. Zohar, ''Bitcoin: Under the hood,'' Commun. ACM, vol. 58, no. 9, pp. 104–113, Aug. 2015.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ''An overview of blockchain technology: Architecture, consensus, and future trends,'' in Proc. IEEE Int. Congr. Big Data (BigData Congress), Jun. 2017, pp. 557–564.

[13] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, ''Research on the application of cryptography on the blockchain,'' J. Phys., Conf. Ser., vol. 1168, Feb. 2019, Art. no. 032077.

[14] J. Arya, A. Kumar, A. Singh, T. Mishra, and P. H. J. Chong, ''Blockchain: Basics, applications, challenges and opportunities,'' Jan. 2021, doi: 10.13140/RG.2.2.33899.16160.

[15] V. Buterin. (Nov. 15, 2015). Merkling in Ethereum. Accessed: 2024. [Online]. Available: https://blog.ethereum.org/2015/11/15/merkling-inethereum

[16] H. S. de Ocáriz Borde, ''An overview of trees in blockchain technology: Merkle Trees and Merkle Patricia Tries,'' Feb. 2022.

[17] Bucket Tree—Hyperchain Documentation, Hyperchain, 2024.

[18] S. Gueron, S. Johnson, and J. Walker, ''SHA-512/256,'' in Proc. 8th Int. Conf. Inf. Technology: New Generat., Apr. 2011, pp. 354–358.

[19] NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition Nat. Inst. Standards Technol. (NIST), Oct. 2012.

[20] H. Dobbertin, A. Bosselaers, and B. Preneel, ''RIPEMD-160: A strengthened version of RIPEMD,'' in Proc. Int. Workshop Fast Softw. Encryption, 1996, pp. 71–82.