Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 4573-4582

Blockchain Enabled Smart Contract For Stock Exchange

T Shanmuigapriya[1], S Sasirekha[2], I Joe Louis Paul[3], R Sowmya[4]
[1]Dr. T Shanmuigapriya , Associate Professor, Department of Information Technology, Sri Siva Subramaniya College of Engineering
[2] Dr S Sasirekha, Associate Professor, Department of Information Technology, Sri Siva Subramaniya College of Engineering
[3]Dr. I Joe Louis Paul, Associate Professor, Department of Information Technology, Sri Siva Subramaniya College of Engineering
[4]Ms.R.Sowmya, Alumni , Department of Information Technology, Sri Siva Subramaniya College of Engineering

ABSTRACT

The structure of the traditional stock market consists of collaboration of various individuals, organizations and several intermediaries namely brokers and traders. In the Indian Stock market, an investor can participate in the trading process only through stock brokers. Stock broker firms charge these investors for the services provided. Each party manages its own system and collaborates with others to facilitate trading on the stock exchange platform. The buy and sell orders go through different parties before settlement. The execution of post-trade settlements takes several days. Involvements of several intermediaries lead to shortcomings such as single point failure, brokerage charges, weak transparency and longer time for posttrade settlements. Blockchain technology is a distributed ledger technology that allows peer to peer transactions eliminating third parties. In this project, we use a blockchain-based architecture to implement the stock trading process. Our architecture uses a private blockchain network to create consortium networks leveraging few participants in the traditional stock market as the validating nodes. The stock trading logic is implemented in a smart contract that is deployed on the private blockchain network. Since the new platform does not introduce significant changes to the stock exchange trading logic and does not eliminate any of the major traditional parties from the system, our proposal promotes efficient adoption and deployment of decentralized stock exchange platforms.

Index Terms—Blockchain, Decentralised, Stock Exchange

1. INTRODUCTION

The stock market can be defined as, “an aggregation of buying and selling offers corresponding to an asset” [9]. The asset can be in the form of shares, bonds or other securities of a company. The person who trades in the stock market is calledan investor. The investor must open a demat account with the Securities Exchange Board of India (SEBI) which manages the investor’s trading accounts and personal data. Due to market regulations, investors cannot directly place orders into thesystem and need to go through third parties namely, stock brokers. The StockExchange (SE) entity is responsible for matching the entered buy and sell orders. SEBI is responsible for formulating the rules and

regulations to be followed by the participating entities and also monitoring the stock exchange platform. Every investor in the stock market relies on brokers for making a transaction in the stock market. A broker may be a firm or an individual who generally acts as an intermediary between the investor and securities exchange. This is because securities exchange accepts orders from brokers who are a member of that exchange. The main functionality of security exchange involves the regulation and approval of laws in stock exchange, handling brokers and inspecting accounts of listed companies.

Stock brokers generally buy and sell stocks on behalf of the investor and charge a service fee for that. This is called commission. Once a trade is complete the transaction should be approved, records of ownership should be changed, securities should be transferred and then the amount should be settled. This is called post-trade-processing which takes 2- 4 days to settle. With the help of blockchain technology theneed for brokers can be removed and the time for post trade processing can be reduced.The entire stock market process can be decentralized, could be made transparent, secure and immutable. To perform trade on their behalf, investors sign a document called Power of Attorney(POA). Here the investors give limited permission to the broker so that the brokers can be given authorization to handle the investor's shares. It is not mandatory that all the investors should sign power of attorney. But generally most of the investors sign this because it is more advantageous for online trading. There is a high risk that this POA can be misused. Since personal information about the investor is disclosed to the broker, there is a chance of risk of data breach. Blockchain adds transparency, immutability and slective share of information to the entities involved with the help of smart contracts. Besides that, the time for post trade settlement for a transaction is also reduced with the help of blockchain technology. Whereas in the traditional architecture, even after a successful transaction, the investor has to wait for the cash to be credited because of increased time of the settlement period.

II.LITERATURE REVIEW

Blockchain technology can be used to implement the stock market structure. Blockchain can be defined as a "network of computers", all of which must approve a transaction that has taken place before it is recorded, in a 'chain' of computer code, called blocks. The details of the transaction are recorded in a public ledger that is common for all the nodes in the network. Each block consists of a unique block identification number, hash value of the transaction and the hash value of the previous block. Transactions in blockchain are broadcasted in the network and are validated by a process known as mining that is performed byspecial nodes in the network known as miner nodes or validator nodes. Validator nodes are responsible for adding new blocks to the chain once a block becomes full. All of these blocks are immutable i.e. a block cannot be changed once created. This feature provides a high level of security. In order to keep track of all transactions, blockchain ledger is used in a network where participants have access to the same ledger replicating the transactions among all peer nodes in that network. This replication ensures that the overall system built on blockchain can resume if multiple participating nodes failed to connect to the network. The nodes in the network use addresses known as public keys to be distinguished by, and hence, defined roles, privacy, and anonymity can be efficiently maintained [4]. Validator nodes rely on the fact that all transactions in the network are duplicated across all nodes involved. Therefore, "Distributed

Consensus" needs to be achieved, meaning that an agreement on the validity of the blockchain is achieved by all nodes involved and they all share the same version of the Blockchain.

According to [6], implementation of blockchain in the financial sector focuses on four main areas, which are improving the transaction processing time, having sustainability for banking and financial transactions, improving financial data privacy and security, and automating financial contracts. Current banking transactions rely on centralised database that takes several days to complete the trade settlements. Blockchain has the potential to solve this problem by automating the trade settlements through a single account structure that will be used for settlements as well as speeding up the transfers. Financial data security and privacy are main concerns in the traditional system due to the centralised storage system used. In [7], the authors point out the stability and security blockchain can provide in the financial sector. Blockchain can prevent data breaches and help to maintain privacy not only in trade transactions but also personal data. Blockchain addresses these issues by decentralizing the data and ensuring they are securely stored in the participating nodes, which add high complexity to unauthorized attempts to alter or access the stored data. Each participant is authorized to perform changes according to the role assigned while maintaining anonymity on transactions performed. In [8], the authors suggest that smart contracts can be used for specifying the rules and regulations of a transaction as it eliminates any third parties in the transaction. The authors highlight that the security features in smart contracts enable secure transactions between two parties involved.

The Block chain based framework is not a one size fits all solution. Sin Kuang Lo et al. [1] has developed a suitability evaluation framework based on metrics like need for MultiParty, Trusted Authority, Centralized Operation, Data Transparency vs Confidentiality, Data Integrity, Immutability, Speed of computation. The author has applied for several applications including stock exchange. Al-Shaibani et al [2] addressed single point of failure in centralized stock exchange platforms, they introduced a permissioned blockchain-based decentralized stock exchange platform. The authors also simulated the behaviour of various participating entities and measured the efficiency in terms of throughput and delay. However the results of the uncontrolled real time environment may not resemble the behavior of the real time environment. In [3], the authors discuss the limitations of the traditional stock market and propose a solution to implement the trading platform on Blockchain. Their research objective is to showcase how transaction fees can be reduced if blockchain technology is used as a trading platform instead of the traditional stock exchange platform. Our project differs from [3] as follows First, we are using a consortium blockchain network in which all participants are known and trusted, and there is no form of cryptocurrency fees that will be used to pay the miners in the network. Second, our main objective is to optimize the performance of the decentralized system rather than reducing the fees, as we measure the throughput and latency to ensure our implementation meets the required level of the stock market platform. Also, our consensus algorithm is based on Proof of Authority (PoA). It provides better performance in terms of execution time and power efficiency in comparison with the public network consensus algorithms such as Proof of Work (PoW) used by the decentralized Bucharest stock exchange.

With respect to the consensus algorithm, in a permissioned blockchain network all the participants are known and trusted entities. According to [5], PoA is an algorithm that attracted a lot of attention due to its offered performance resulting fromlighter exchanged messages. It operates in rounds where

several nodes are elected, with one of them acting as a mining leader charged with the task of proposing the new block and eventually reaching consensus. In [10], the author argues that RAFT consensus is easy to understand and implement, which makes it efficient to use when building applications and systems. It works by having a set timer for all authorized nodes, which can validate new blocks in “terms” that can be seen as rounds that get repeated over time.

II. DECENTRALIZED STOCK EXCHANGE PLATFORM

The proposed architecture is a decentralized stock exchange platform that is based on a consortium blockchain network, where, few of the entities in the traditional platform are leveraged as the validators of the network.

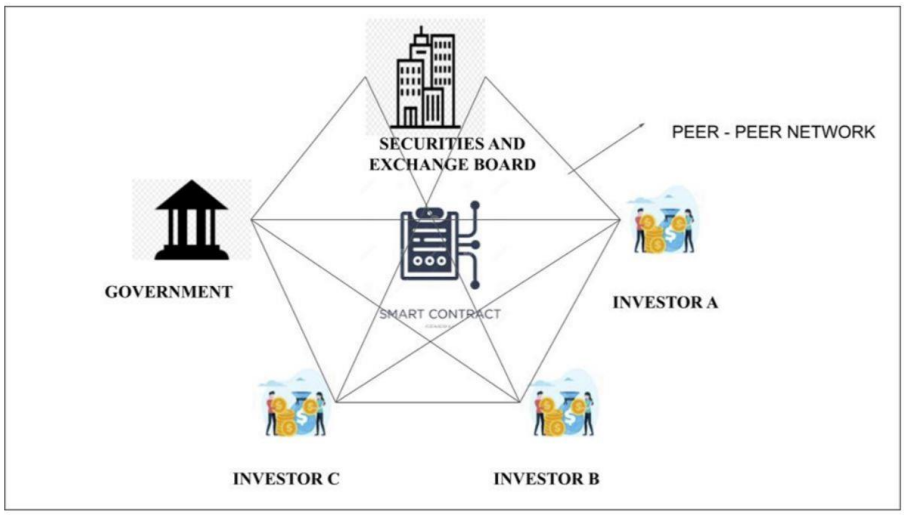

Fig. 1. Decentralized Stock Exchange Platform

As shown in Figure1, the proposed architecture consists of consortium blockchain network. The participating entities of which are a smart contract, SEBI, Government and investors. The consortium blockchain facilitates transactions between the different participating entities, and manages the stock exchange smart contract that handles the stock trading logic. A permissioned blockchain is selected as the entities are all known, and also because the private version of blockchain is more effective in terms of transaction throughput and latency. The consortium network is composed of a set of authorized participants (validators) which are the SEBI, Government and Stock Exchange Contract(SE). Each of them has specific roles and responsibilities as per the traditional stock exchange platform. The SE defines all the trading logic as well as the different functions that can be performed by the participating entities, such as, creating new investors, assigning shares to investors, etc. Each participating entity has a private key along with the associated address and public key that are used for authentication. Therefore, the smart contract ensures that each entity is only allowed to trigger functions according to its associated privileges. Table I summaries the StockExchange smart contract functionalities and the entities authorized to execute each of them. The detailed description of the role of each of the participating entities is as follows:

- Government is responsible for verifying the identity of the investors as to whom they claim as. The primary test condition involves checking if the investor is a valid citizen of the country.

- SEBI is responsible for various duties that includes creating and deploying the smart contract, adding investors to the system, assigning unique trade account numbers to investors, adding and maintaining a list of public limited companies, assigning shares to investors as well as starting the stock market.

- Investor is responsible for placing buy/sell orders in the order book, viewing the shares currently owned.

- StockExchange Contract is responsible for carrying out the trade process by matching the buy and sell queues. It includes the authorisation rules to carry out transaction in block chain.

StockExchange Smart Contract : The smart contract includes the business logic and authorization roles of each entity in the network. The smart contract manages buy and sell orders in separate queues. The smart contract handles only limit order type. It generates respective trades whenever a buy order offers a price that is equal to or more than the sell order's price. The different steps in trading process are detailed as follows:

Functionalities	Entities			
	SEBI	SE	Government	Investor
Create/maintain smart contract	Yes	No	No	No
Create/maintain list of investors	Yes	No	No	No
Verify Investors	No	No	Yes	No
Create/maintain list of companies	Yes	No	No	No
Buy/Sell Shares	No	No	No	Yes
Assign Shares	Yes	No	No	No
Generate trades	No	Yes	No	No
Transfer shares	No	Yes	No	No
View owned Shares	No	No	No	Yes

TABLE I

STOCKEXCHANGE SMART CONTRACT FUNCTIONALITIES ANDAUTHORIZATIONS

1. When an investor places a sell order into the sell queue, the ownership of the investor for that particular share is verified. If the investor tries to sell shares that are not owned by him/her, the transaction fails.

2. The buyer places the order specifying the maximum price that he/she is willing to bid for the share.

3. The seller places the order specifying the minimum price that he/she is willing to sell the share for.
4. Let BQ denote the buy queue and Bp denote the maximum price of a particular share whose quantity is given as Bq in the buy order.
5. Let SQ denote the sell queue and Sp denote the minimum price of a particular share whose quantity is given as Sq in the sell order.
6. The orders in the buy queue are sorted in the ascending order of the price and descending order of the quantity.
7. When BpSp and Bq=Sq the orders are said to be matched and trade is generated.
8. When the trade is generated the ownership of the said share is transferred from the seller to the buyer.
9. The current price of the share is updated to the new buying price of the share.

Figure 2 shows the sequence diagram between the participating entities and the smart contact, including all the steps required before generating trades and matching buy/sell orders. The detail description is as follows:

1) SEBI defines the list of companies in the stock market along with their shares. The function "addCompany" is used for this purpose.
2) SEBI adds the investor into the system using the "addInvestor" function. The investor profile is verified by the government before added to the Investor management module.
3) SEBI assigns the investor a unique new investor account number "NIN" using the "addNIN" function.
4) SEBI assigns shares to the investors in the system using the "assignShares" function.
5) The investor places buy/sell orders in the order management module using the corresponding "buyShares" and "sellShares" function.
6) SEBI initiates the market by calling the "doMatch" function which matches the orders in buy and sell queues. On successful matching the ownership of the shares are transferred accordingly.
7) In case of no match the order is deleted from the queue.

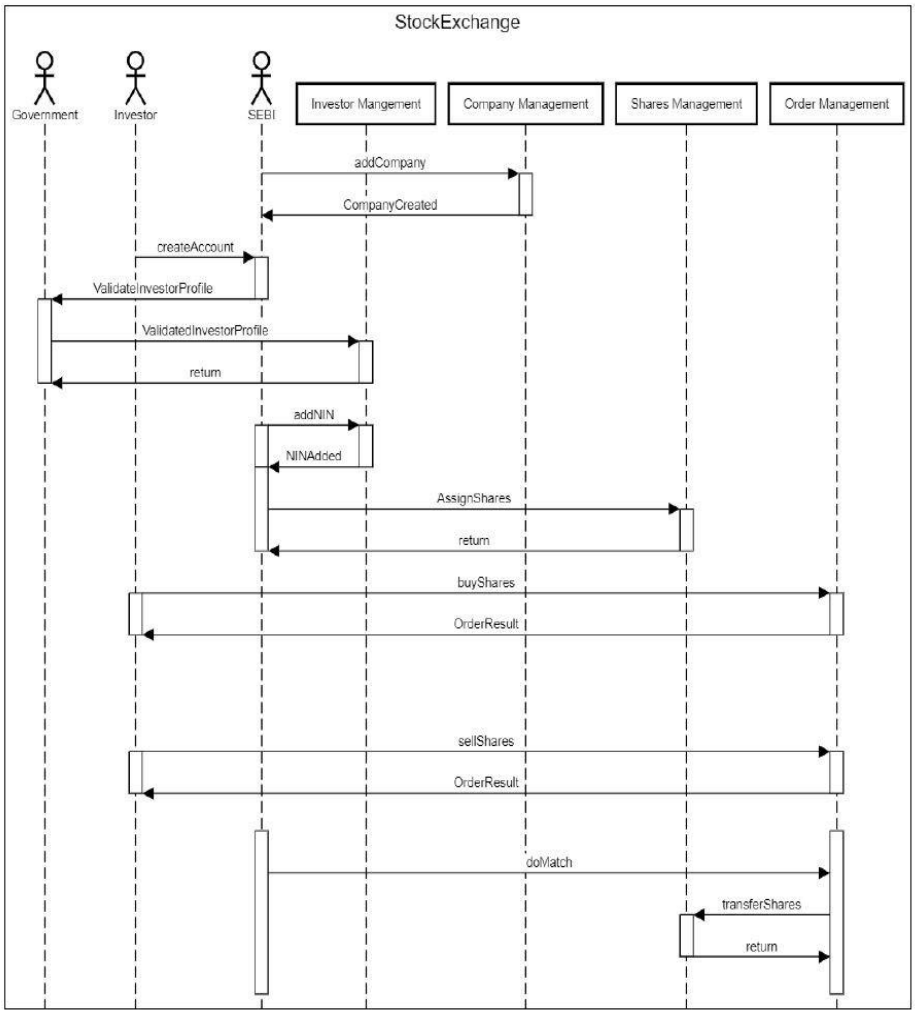

Fig. 2. Sequence diagram of the system

III. SECURITY AND SYSTEM EFFICIENCY ANALYSIS

The proposed blockchain-based stock architecture has the following security and system efficiency:

1) Transparency: the level of transparency provided by using blockchain guarantees that all transactions and data maintained by the system are visible to the authorized participants and cannot be manipulated. However, any change requires consensus and commitment from all network participants before it gets validated. In contrast, the traditional stock exchange suffers from insufficient transparency level as each party has its system and can hide or manipulate the data before sharing it with other participants.

2) Reduced brokerage interference: in the trading process. In the traditional structure, investors required stock brokers to participate in the trading process. This leads to brokerage commissions and breaching of personal as well as trading data to a third party. Although SEBI monitors the activities of stock brokers regularly, it takes longer time for SEBI to identify the discrepancies if any committed by the brokers.

3) High availability: the proposed architecture addresses the single point of failure by ensuring high availability through decentralizing the data across multiple participants. The smart contract can still be executed even if some nodes were disconnected from the network. Contrary to the traditional stock market, if any of the system participants is unavailable, the whole market is affected.

4) Network efficiency: in the stock exchange, the quality of network connectivity has a critical impact on investors' profits. For instance, an order sent by an investor through his/her associated broker can be delayed by the network if the broker has connectivity issues, or it is physically located far from the SE. Orders that were entered later by other brokers, with better network connectivity or located physically closer to the SE, will be executed first. This results in a financial loss to the investor despite entering the order first and can cause a lack of fairness and trust in the overall platform. The blockchain network provides better connection utilization between the different participants since nodes are distributed in different physical locations. The node physically located closest to the users interacting with the smart contract will receive the transactions and broadcast them to the remaining nodes in the network.

5) Flexible configuration: the proposed architecture provides more flexibility and scalability in comparison with the traditional stock exchange platform when it comes to adjusting the functionalities and introducing new changes to the trading logic. The smart contract is shared in the network without requiring participants to make changes in the hardware and storage, which makes it much easier to adopt.

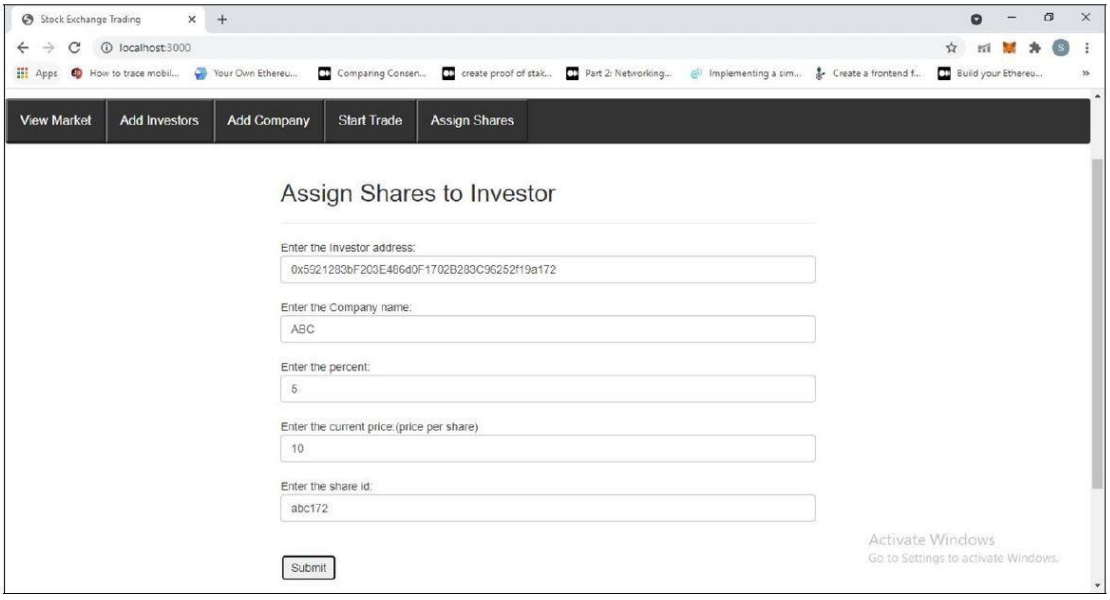

Fig. 3. SEBI Assigns Share to Investor

A. Result Discussion

The web pages contain different functionalities depending on the role of the current user. There are three major roles in the system, such as SEBI, Government, Investor. The government entity can add a citizen into the system and view the stock market and the events that happen in the market. Government can approve and add users to the block chain portal by verifying the user's valid identity

proof. The SEBI entity can add an investor to the system, assign shares to the investors, view the market, it's events and start the market for the day. Figure 3 shows SEBI assigning shares to the investor. The user will be able to buy share directly or will be able to give their preferred share amount. Snapshot shared in Fig 5 demonstrates the user opting to buy share directly from the Investor. The balance amount and transaction details can be seen with the help of the metamask wallet added to the browser. Any transaction confirmed here is also reflected in the block chain. Since there are no brokers involved, the time at which the transaction happens is very quick compared to the traditional stock market, where it may take a day or two. Moreover the charges paid for the block chain transaction in terms of gas is very less compared to the commission amount paid to the broker. The trading can also be programmed by the user, where the buyer can mention their preferred amount and whenever the seller's preference matches with that of the buyer the transaction is initiated. Fig 5 demonstrates the sales and transfer of ownership.

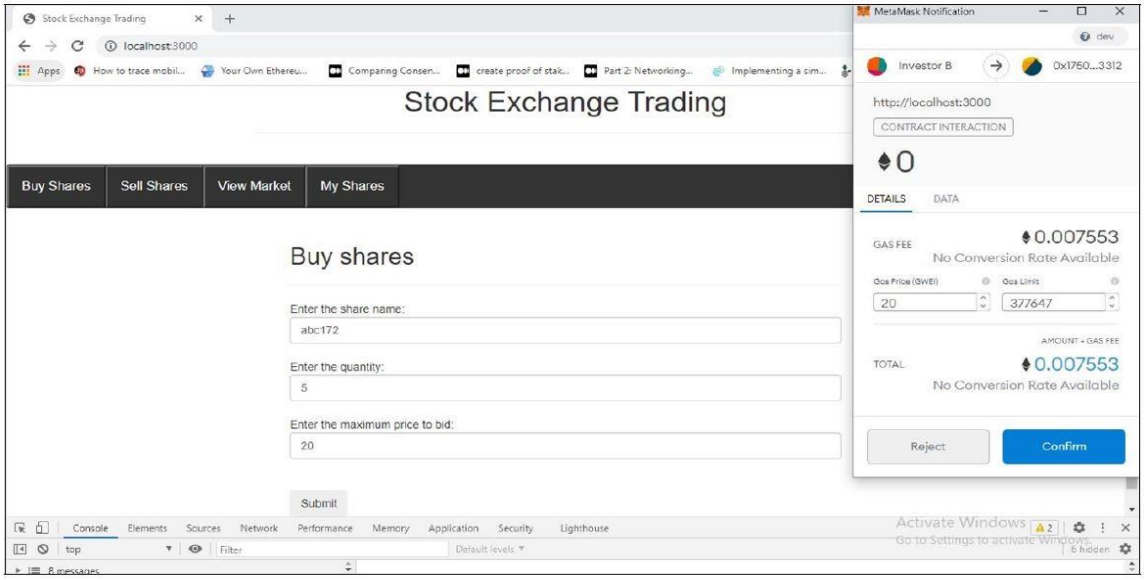

Fig.4 . Investor – Buy Shares Interface

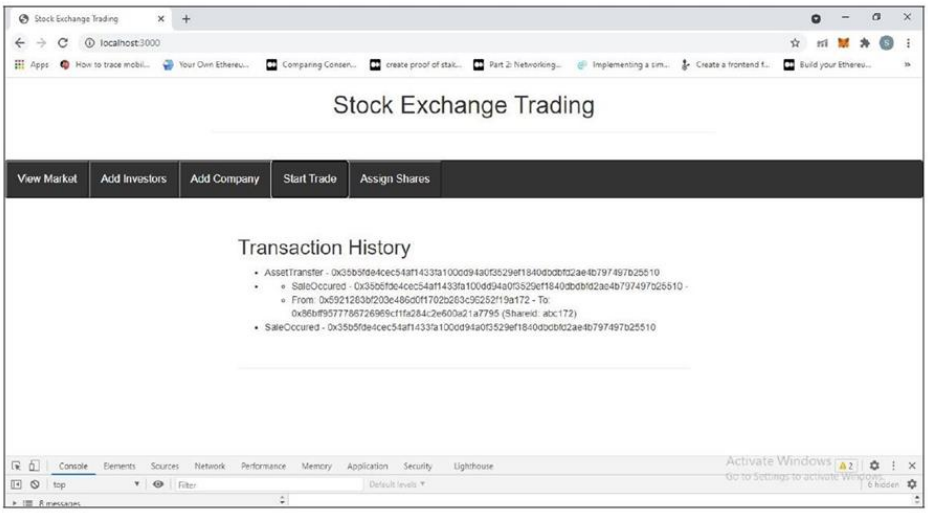

Fig. 5 . Page indicating the sale generated and transfer of share

IV. CONCLUSION

The proposed blockchain-based architecture for stock market implementation is based on Ethereum smart contract that is implemented on the consortium based permissioned blockchain network. The new architecture leverages entities in the existing trading structure to act as validators. This new architecture addresses the limitations of the traditional stock exchange platform such as the single point of failure in the participating systems by replicating the data and smart contract across all participating nodes, the complexity and inefficiency of the data management which our solution solves by providing a shared ledger that can be easily updated and maintained, the limited level of transparency since now all transactions can be seen, the limited daily time to access the platform's data as now it is easier to monitor the blockchain and access it throughout the day, and offering a faster financial and cash settlement time instead of the three days needed after the trading session. The future work will also cover further enhancements in the proposed smart contract. For instance, the possible introduction of new changes to the already deployed smart contract without causing disturbance to the overall stock exchange platform.

REFERENCES

[1] Sin Kuang Lo, Xiwei Xu, Yin Kia Chiam, and Qinghua Lu. Evaluating suitability of applying blockchain. In *2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS)*, pages 158–161. IEEE, 2017.

[2] Hamed Al-Shaibani, NoureddineLasla, and Mohamed Abdallah. Consortium blockchain-based decentralized stock exchange platform. *IEEE Access*, 8:123711–123725, 2020.

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

[4] A. Dorri, S. S. Kanhere and R. Jurdak, "Towards an optimized BlockChain for IoT", Proc. 2nd Int. Conf. Internet-of-Things Design Implement., pp. 173-178, Apr. 2017.

[5] S. D. Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri and V. Sassone, "Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain", Proc. Italian Conf. Cyber Secur., pp. 11, Jan. 2018.

[6] J. Jaoude and R. Saade, "Blockchain applications—Usage in different domains", IEEE Access, vol. 7, pp. 45372-45373, 2019.

[7] Q. K. Nguyen, "Blockchain–A financial technology for future sustainable development", Proc. 3rd Int. Conf. Green Technol. Sustain. Develop. (GTSD), pp. 51-54, Nov. 2016.

[8] Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. Wang, "Blockchain- Enabled Smart Contracts: Architecture, Applications, and Future Trends," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[9] V. V. Bhandarkar, A. A. Bhandarkar and A. Shiva, "Digital stocks using blockchain technology the possible future of stocks?", Int. J. Manage., vol. 10, no. 3, pp. 44-49, Jun. 2019.

[10] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm", Proc. USENIX Conf. USENIX Annu. Tech. Conf. (USENIX ATC), pp. 305-320, 2014