Decentralizing the Stock Exchange using Blockchain

An Ethereum-based implementation of the Bucharest Stock Exchange

Claudia Pop, Cristian Pop, Antal Marcel, Andreea Vesa, Teodor Petrican, Tudor Cioara, Ionut Anghel, Ioan Salomie
Computer Science Department
Technical University of Cluj-Napoca
Cluj-Napoca, Romania
{claudia.pop, cristian.pop, marcel.antal, andreea.vesa, teodor.petrican, tudor.cioara, ionut.anghel, ioan.salomie}@cs.utcluj.ro

***Abstract*— This paper tackles the shortcomings of the traditional centralized stock exchange systems, such as high transaction fees, centralized governance susceptible to attacks and lack of openness regarding the market actions and algorithms, by proposing an innovative architecture using blockchain to develop a decentralized stock exchange and an open continuous market. The proposed blockchain based solution solves the drawbacks of the centralized stock exchange architecture by ensuring the integrity and security of the owner's assets and orders, self-enforcing smart agreements between parties as well as achieving democratic and reliable decisions regarding the execution and settlement of the orders through consensus algorithms. The proposed architecture uses smart contracts to enforce the validation of the owner's rights and the correct execution and settlement of the orders, thus eliminating the need of a central authority that ensures the correctness of the stock exchange process. The solution was validated by implementing a prototype in Ethereum for a subset of rules for the Bucharest Stock Exchange. The experimental results show that the decentralized solution can offer lower transaction fees by replacing the commissions owed to brokers and central authorities with mining fees that are used to compensate the miners for their honest work in keeping the integrity of the system.**

Keywords—stock exchange; blockchain; distributed ledger; smart contract;

I. INTRODUCTION

Since the 17th century when the Dutch East India company was the first listed company on a stock exchange, the world's economy was built around and relies upon stock exchanges where millions of trades are performed every day helping companies raise their value. A stock exchange market is an aggregation of buying and selling offers corresponding to an asset. An asset can represent equities or stocks of companies, bonds, or other securities. People who buy or sell the assets are called investors while the persons who perform the transactions are called brokers or traders.

Modern stock exchanges are highly computerized and can handle vast number of transactions in a short amount of time, assuring the security, execution and authenticity of transactions at a cost of a transaction fee, usually directly proportional with the value of the auction. The traditional stock markets are implemented in a centralized application that gathers all the trading actions. This architecture has many benefits by having a central authority that ensures the authenticity, security and validity of the transactions. However, the centralization has also a lot of drawbacks, such as having a single point of failure, a possible performance bottleneck or susceptibility to attacks. Furthermore, the central authority oversees the fees and there is a lack of transparency of the auctioning process for the trader.

This paper proposes decentralized stock exchange architecture to tackle the shortcomings identified above by using the new and emergent blockchain technology. The potential of the blockchain system can bring benefits to the entire system, by leveraging on full replication and verification by all the nodes in the system regarding the assets owned, the execution of the market orders and the correct settlement between the accounts. Furthermore, the ensured immutability of the ledger brings a valuable advantage with respect to the centralized system. Also, by decentralizing the system, there is no central authority or intermediate needed for placing and executing the orders. To demonstrate that a blockchain based solution can provide a better option regarding the order transaction fees we implement both a centralized and decentralized Ethereum-based prototype [1] for a subset of rules of the Bucharest Stock Exchange (BVB) [24], perform a set of transactions in centralized and decentralized fashion and compare the transaction fees for both approaches.

The rest of the paper is structured as follows: Section II shows related work, Section III presents the centralized stock exchange market architecture, Section IV describes the proposed decentralized stock exchange and a prototype implemented in Ethereum, Section V presents results obtained in a simulated environment, while Section VI concludes the paper.

II. STATE OF THE ART

The blockchain technologies are considered groundbreaking solutions that will change the face of the web as we know it today. Chriss Dannen compares the revolution of the blockchain technologies with the one brought by Ted Nelson through the HTTP concept in 1965[1]. Although even the

978-1-5386-8445-0/18/$31.00 ©2018 IEEE

most robust platforms are still in development and research is done in order to improve different aspects of the blockchain technologies, there are many startups and companies that invest in decentralizing traditional applications.

In 2016 over 120 blockchain projects have been identified by Moody's Investors Service [2], since then countless projects have started and are continuously revolutionizing the traditional systems. Currently, Ethereum is the platform for more than 1600 decentralized applications [3].

There are several benefits that a blockchain based solution brings with respect with a traditional based implementation. Firstly, it eliminates the need of a mediator, through Smart Contracts, which enforce the rules on chain, each side being aware of the consequences of their actions. Secondly, the blockchain data structure (hashed linked list of blocks) allows for easy traceability of the coins and state updates that happen in the chain. Since the records are public and replicated this also provides great transparency so that companies and actions can easily be verified. Even if all the transactions and all the actions are public, the blockchain platform provides high security through consensus, public key cryptography and tamper proof recording. The immutability is a characteristic achieved by the enforcement of the consensus of algorithms together with the linked data structure: the further a block gets in the chain, the more improbable is a successful attack that alters its state, since such an attack would require all the following blocks to be re-mined.

Research is done in order to take the benefits that the distributed ledger brings and apply them to improve the traditional centralized systems in other domains. Besides the well-known regard in the financial domain, many resources were dedicated to finding solutions to decentralize the traditional approaches in domains such as: medical systems, provenance of products, Internet of Things (IoT), electricity grids, copyright management systems, autonomous vehicles, etc.

One of the highest studied domains is the decentralization of the Smart Grids. As in most of the use cases the aim is to provide an alternative to the traditional system by eliminating the mediators of the system (Distribution System Operators, Aggregators). The resulting solutions provide automated systems by integrating smart meters and near real time financial settlement [4], [5], [6], [7], [8]. Other solutions aim to decentralize the Demand Response programs [9], [10] and propose decentralized flexibility market where each client of the grid has the option to participate in democratic and competitive markets leading to more fair prices, driven by the demand and offers instead of being controlled by single authorities.

Another direction of the blockchain research is aiming to study the integration of blockchain advantages in the IoT domain. The authors of [11] perform an analysis of the blockchain in the context of IoT, showing how the distributed ledger mechanism eases the resource sharing process, creates a marketplace of services between devices and helps automating existing workflows. They show a scenario where manufacturers of IoT devices equip them with distributed ledgers and smart contracts. Furthermore, the integration of blockchain with the IoT platform can facilitate the sharing of real-world services and properties, such as the Slock.it [12] company that develops electronic locks manageable through blockchain tokens. The authors of [13] tackle the problem of scalability in the IoT domain by choosing a distributed ledger approach versus the classical client-server architecture prone to multiple failures. Another issue encountered in the IoT domain is the incentive system to stimulate or pay the users. The author of [14] proposes a crypto currency system called *iota*, for addressing the scalability issues of integrating Internet-of-Things. The proposed solution does not rely on a global blockchain, instead it uses a DAG (directed acyclic graph) called a tangle to save and validate transactions. The system uses this graph to approve transactions that reside on a directed path. Algorithms and uses-cases that cope with security problems and attacker's strategies are presented and solved.

A third major research direction regarding blockchain based decentralization is studied in the context of smart manufacturing and asset tracking. As a solution to eliminate centralized manufacturing systems drawbacks, Cognizant [16] proposes blockchain together with IoT. Among the mentioned benefits that can be brought by the blockchain technology are: audit trails, real-time negotiation regarding pricing and delivery time, supply chain traceability on both upstream and downstream directions, data gathering from IoT to establish the quality and performance, and secure intellectual property registration. The same authors consider in [15] that blockchain will be the solution to deliver less expensive and more trustworthy connections between manufacturer chains. Such a solution will provide a way of tracing any product back to the composing raw materials and to their source location. At the same time, tracking services can be provided for any complete future product in case a subcomponent defect is discovered. Furthermore, a blockchain solution will provide support for continuous business modification through smart contracts. In [17] the vision of a future blockchain based manufacturing chain is presented. The physical product has a virtual identity which is mapped to a profile contained in blockchain. The proposed architecture gathers consumers together with producers, manufacturers, distributors and waste management coordinators in order to provide services that help track the asset through its entire lifecycle. Each actor has the right to modify information about the associated virtual asset profiles, and the data access rights changes depending on the actor's role. Several startups have started developing solutions in the context of decentralized asset tracking applications using blockchain. A solution for tracing the origin, the subcomponents and the history of products that are sold in stores has already been developed by [18]. Fluent [19] is another startup that aims to provide supply chain services regarding financial solutions. Blockchain technology also has a big impact on different industries where specialized applications have been developed to provide reliable tracking services regarding: pharmaceutical industry [20], food industry [21], automotive industry [22], [23], etc.

As demonstrated by the current research directions regarding the decentralization of traditional systems, the blockchain has the potential to disrupt many domains. In this context, we propose a solution for the decentralization of the stock exchange system aiming to reduce the transactions fees and aid individuals trade auctions without the need of a broker. Furthermore, a case study for the Bucharest Stock Exchange [24] is presented and a prototype is implemented in Ethereum to validate the transaction fees benefits of using the blockchain based stock exchanges.

III. Traditional Stock Exchange Architecture

The traditional stock markets are implemented in a centralized application that gathers all the trading actions. The instruction of buying or selling an asset on a specified price on the market is called *order* and is most of the time intermediated by the broker. There are different types of orders that can be executed on the stock markets: Limit Orders, Market Orders or Hidden Orders. The Limit Orders gives control to the agent over the price at which that order can be executed. Specifically, the trading action needs to be executed at the price-limit specified or at a better one. That is, for buying a security the price cannot be higher than the price specified, and for selling a security, the price cannot be less than the price specified. The Market Orders on the other hand are not so restrictive, giving the possibility of the order to be executed at the price of the market. A specific case of Limit Orders is the Hidden Orders, which are orders that enter the order book without displaying either the price or the volume of the traded security.

The traditional stock market systems are relying on centralized components: Stock Exchange, Clearing House, Settlement System, and Centralized Repository.

We consider the Bucharest Stock Exchange (BVB) model for implementing a simulator for the Stock Markets. Firstly, we designed and implemented a centralized solution, where the orders are gathered by a central authority and then are executed. The next section will present a decentralized solution, leveraging on the benefits brought by a blockchain-based implementation. In the following sections we will present the BVB-based model considered for implementing the simulators. After that we present the design of the two simulators: centralized stock market, blockchain-based stock market.

A. BVB Stock Exchange Model

We modeled our system according to the BVB specifications considering a sub set of the market rules specified in the official exchange description. The market allows trading different securities, from intangible assets like bonds or different titles to more tangible actual products.

The BVB Stock Exchange presents two types of markets: continuous and auction markets. The **Auction Markets** are organized at discrete moments in time. There are one or two market sessions organized for an auction during which all the requests and offers are published and aggregated in a central registry. At the end of each session, the fixing algorithm is run against the gathered orders and the clearing price is computed as the intersection point between two curves, one representing the requests orders and one representing the offer orders. All the matched the orders are executed at the same price, which is the clearing price. The matched orders are all the offering orders with a lower price than the clearing price and all the demanding orders with the price higher than the clearing price.

In a **Continuous Market** on the other hand, the orders that are published are executed immediately or as soon as their order type permits. However, before opening the continuous market, there are some preparing sessions. In the *Pre-Open Session*, the clients can publish, modify and withdraw orders. This session is created to avoid the volatility created in the first minutes of the market. In this sense, the price is estimated in the pre-open session, but no orders are matched. Next, the *Opening Session* starts the prices and traded volumes are computed based on the orders performed in the previous session. The orders start to be executed and the market transitions to continuous trading stage in the *Open Session*. Similarly, when closing the market, the *Pre-Closed, Closing* and *Closed Sessions* are defined, where the orders are no longer executed but the potential price is computed as an estimation for the next day sessions. For the simulation, we considered the market to be always opened, so that clients are able to enter orders.

The orders submitted for a specific market symbol (security) are gathered in an Order Registrar. At any time, the orders are sorted with respect to their price (highest price for Offers and smallest price for Demands), their quantity and the timestamp. Corresponding to their order type, a trading action can have different availabilities:

- **DAY Order** (Good for the day) – the order can be executed until the day trading session ends.
- **OPEN Order** – the order can be executed or withdrawn for 62 days from the day it was its last updated
- **Good till Date** - the order is valid until the date specified when submitting
- **Fill or Kill (FOK)** – the order must be executed in full when submitted otherwise it is dropped
- **Immediate or Kill (IOC)** – the order can be partially executed when submitted. The volume that is not matched is dropped.

For the current simulation we consider a subset of the official BVB model. In this sense we consider a continuous market type that is opened at the time of simulation. Furthermore, we allow two types of order to be placed on the Open Session: Limit Order and Market Order; giving the possibilities to specify the one of the following availabilities: OPEN, FOK, IOC.

B. Centralized Architecture of the Stock Exchange

The traditional system of the stock exchange markets is developed as a centralized system where one component gathers all the market actions from the agents, as presented in Fig.1. The actions are collected in a central registry of the **Security Exchange Platform**. All the actions are grouped by type (bid, offer) and are ordered by price. Although the mechanisms are described as continuous, the matching is performed at discrete moments in time, driven by the actual buy-sell orders. When conditional actions are registered in the market, they are kept in the order book until the conditions are met (Limit Orders). Market Orders on the other hand, are registered at the market price, which is the price at the top of the order book. These orders are executed instantaneously and do not appear in the order book.

Once the market actions are registered in the Security Exchange Platform the actions are executed according to their conditions. Once the actions are matched, the actual transfer needs to be executed, which means that the real asset (bond, share certificate, etc.) needs to be exchanged for the actual monetary value. For the transfer to happen correctly, the **Clearing House** is responsible to perform all the necessary steps by guaranteeing and recording all the transactions and grouping the activities by member for each trading day. The **Settlement Platform** ensures the actual action of exchanging the goods. In the electronically systems the settlement must be done until a set deadline. In the current systems, stock securities are settled in 3 business days (T+3), while government bonds are settled in one day (T+1) [25]. The more traditional systems, where the exchanged securities were performed in paper format, the settlement could take more, even 5 days. In order make the settlement process faster, the certificates began to be stored and immobilized in a **Central Depository**. At first, the documents were stored in and *book-entry accounting system*, but then the *dematerialization* process begun, and all the securities were processed in electronically formats.

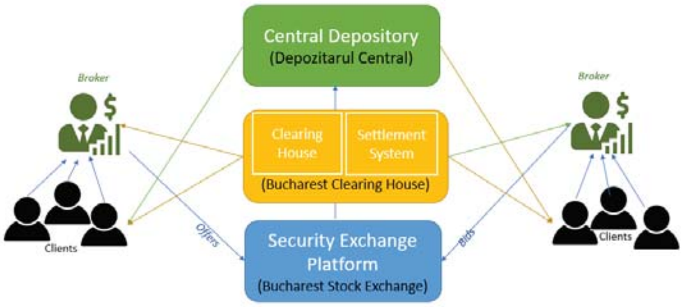


Fig.1. Centralized Architecture of the Stock Exchange

One of the main drawbacks of the current system is that the network is owned and regulated by a central third party. Such a system can easily be the target of attacks and single point of failures, due to its centralized architecture. Furthermore, by having a central third party managing every transaction in the system, it provides an authoritarian system were the fees are dictated by the owner and do not benefit of the lower fees competitiveness that a decentralized system could bring. Furthermore, the current system allows registering new market actions only through intermediates. These intermediaries are the Brokers, which are registered trusted entities that act on behalf of the clients in exchange for a fee. Furthermore, the central authority is also in charge of the matching marketplace algorithms deployed, and these very often lack openness and transparency. Another major drawback is the high processing and settlement time. A completely electronically system should be able to fast track the settlements in near real time.

IV. Decentralized Stock Exchange using Blockchain

This section presents a decentralized solution that aims to provide a solution that tackles all the above-mentioned drawbacks by providing a completely decentralized blockchain based system by providing: global agreement over all the transactions, self-enforced validation through smart contracts, transparency of the algorithms through smart contract code and low transaction fees through competitive peer-to-peer markets.

A smart contract is a piece of code that depicts different business rules that need to be verified and agreed upon. An actual legal contract can thus be represented as a set of instructions. These contracts are registered in the blockchain, similarly with the transactions. They can be triggered in the future by transaction calls, which will determine each node to update its state based on the results obtained after running the smart contract. However, even if the term is “contract” the smart contracts should be seen as agents that can have a state and functionality and can be triggered at any point after its successful deployment. The purpose of smart contracts is to replace the third-party entities from the real world (judges, litigators, escrows, etc.) with a neutral agent that will act according to a predefined set of rules. The specifics of a smart contract depend very much on the framework implementing it. Currently, the most well-known ledgers [17] that provide the possibility of developing smart contracts are: NXT [10], Side Chains [18], Hyperledger, and Ethereum[19]. Out of these, Ethereum is the most mature and advanced in terms of writing smart contracts. It is a distributed ledger system that offers several improvements in term of consensus algorithms and blockchain structure.

To model the **Decentralized Exchange Platform**, we develop a smart contract, the StockMarket contract that acts like an enhanced order book. As states of the smart contract we define the following information:

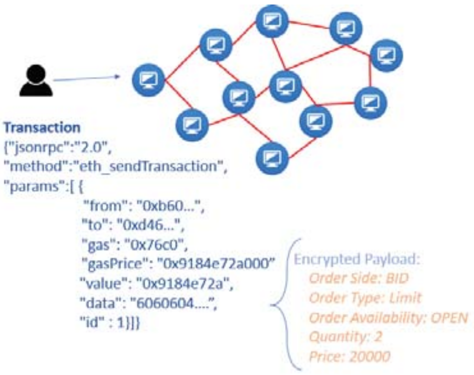
- **symbol -** representing the name of the transacted asset
- **ownedStocks** – a *mapping* between the owner address and the quantity of the assets owned
- **marketPrice –** *uint* representing the price at which the latest action was executed
- **bids –** Order a sorted array of all the sell actions that were registered and not yet executed
- **asks–** Order a sorted array of all the buy actions that were registered and not yet executed

Each Order action is defined by the smart contract as a structure containing information regarding:

- the address of the actor
- the timestamp when the action was registered in the system
- the transacted asset quantity
- the price at which the actor is willing to sell/buy

- the order action side of the order (**OrderSide –**specify the action side: Sell or Buy)
- the order type specifying the condition on prices (**OrderType –** specify the type of orders: Limit or Market)
- the order availability choosing between the allows options (**OrderAvailability –** specify the type of availability: OPEN, FOK or IOC)

Besides this information, each transaction aiming to publish a new order contains a locked amount of money (eth) to be used in case of a settlement.



```
Transaction
{"jsonrpc":"2.0",
"method":"eth_sendTransaction",
"params":[ {
        "from": "0xb60...",
        "to": "0xd46...",
        "gas": "0x76c0",
        "gasPrice": "0x9184e72a000"   Encrypted Payload:
        "value": "0x9184e72a",           Order Side: BID
        "data": "6060604....",           Order Type: Limit
        "id" : 1}]}                      Order Availability: OPEN
                                         Quantity: 2
                                         Price: 20000
```

Fig. 2. Transaction deploying a new Order

The StockMarket contract that is deployed on chain has knowledge about the securities owned by each holder. The mapping between the owner address and quantity of securities owned, acts as a **Decentralized Depository**, keeping track of all the assets, and provides replication of the data across the network. Furthermore, any modification of the depository is governed by consensus between peers, and any kind of attack is unfeasible since the state of the depository is stored in blocks in a tamper proof manner.

The deployment of the order transaction is depicted in Fig. 2. Once the order transaction is gossiped among the peers, the integrity of the order is checked in the platform before its execution. Performing the tasks of a **Decentralized Clearing House**, each node in the network will check the validity of the order by guaranteeing the success of the execution in case of a matching order. For each BUY transaction it is validate whether the sender has locked during the transaction enough money to be able to pay the securities. This is checked with respect to the required quantity and the price, depending on the Order Type (the SELL transaction should have 0 money locked). By locking inside the transaction, the actual amount of money to be spent, the need of an escrow is eliminated. From this point over the money will be locked and controlled by the contract and sent to the seller once the order is executed. Similarly, whenever a SELL transaction is deployed, the network will validate whether the sender owns the quantity of securities that he is willing to sell, by checking the Decentralized Depository entries.

Each seller of the market will issue transactions representing the offer and the proposed quantity and prices. Similarly, the buyers will issue transactions representing the bids containing the quantity and the price they are willing to pay. Once issued, these marketplace actions will be registered and replicated in future blocks across all the nodes in the network as presented in Fig. 3.

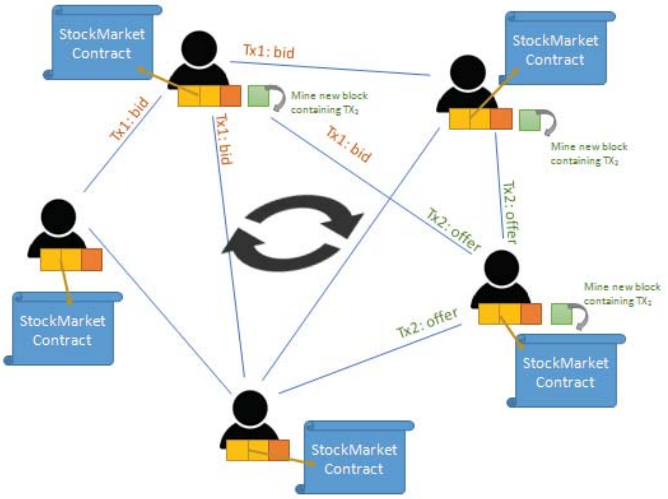


Fig. 3. Transaction deploying a new Order

The consensus mechanisms implemented in the blockchain system, keeps track of all these changes and validate at each point the state updates corresponding to each bid/offer received by the corresponding actor. Since the StockMarket Contract is replicated across all the nodes in the network, the incoming transactions (market actions) contained in a block, are validated by each node in the network in the following way. In order to create a valid block, it must contain together with the transactions also the latest state of the accounts, in our case the StockMarket Contract. The latest states are determined by the miner after applying the sequence of actions represented by the transactions stored in that block. When a miner wins a competition, its block will be propagated to the entire network for verification and acceptance. Each node of the network will receive this newly mined block and will validate the state transitions, by executing all the transactions with respect to the state known from the previous block, and then comparing the results between the block received from the miner and their own computation. The proposed changed state is accepted if and only if the validation is correct, otherwise the block is dropped, and new block proposals are accepted.

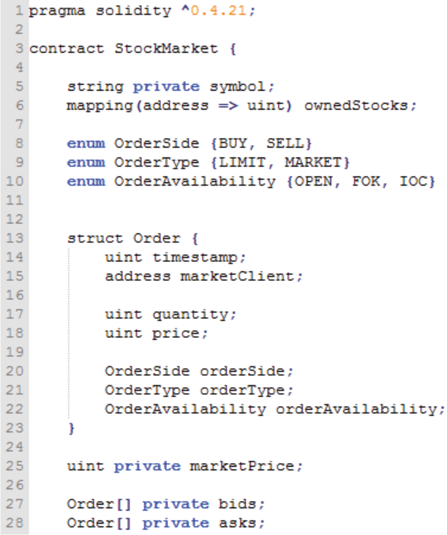
As a result, the system offers a completely replicated and highly reliable decentralized application, where each node is responsible to validate the integrity of the registered actions: assets owned, bids and offers, market price, settled price, etc. The system proposed manages to provide complete decentralization, while at the same time providing a democratic system, where each stakeholder can have transparent access to all the algorithms and actions deployed, and at the same time verifying and validating the integrity of these actions. Moreover, an important improvement of the system is the lower fees that are obtained by eliminating the intermediate agents that are acting on behalf of the clients. These fees are replaced with the mining fees that are necessary to provide the security and the integrity of the system, by rewarding the miners for their honest work.

V. Experiments and Results

We have developed two prototypes to test the feasibility of the decentralized system with respect to the centralized system.

A private blockchain network has been configured using the Ethereum core, on four computers, from which two miners and two regular nodes. The two miners were deployed on two desktop computers, having CPU I5-7600K, 16GB DDR4 RAM memory and GPU nVidia 1050 2GB GDDR5 running Windows 10. The regular nodes were run on two desktop computers having CPU I7-870 and 8GB DDR3 RAM memory, running also Windows 10.

The StockMarket contract (Fig. 4) was deployed and mined in the network. The prototype smart contract has been developed according to the business rules proposed in the decentralized market model.



```
pragma solidity ^0.4.21;

contract StockMarket {

    string private symbol;
    mapping(address => uint) ownedStocks;

    enum OrderSide {BUY, SELL}
    enum OrderType {LIMIT, MARKET}
    enum OrderAvailability {OPEN, FOK, IOC}


    struct Order {
        uint timestamp;
        address marketClient;

        uint quantity;
        uint price;

        OrderSide orderSide;
        OrderType orderType;
        OrderAvailability orderAvailability;
    }

    uint private marketPrice;

    Order[] private bids;
    Order[] private asks;
```

Fig. 4. States defined in the Solidity StockMarket Solidity Contract

Three of the nodes are used to simulate the market clients that are interacting with the smart contract by deploying new orders. The orders are matched correctly in both centralized and decentralized systems. However, the most notable differences between the two systems are the fees that the client needs to pay for deploying their orders.

TABLE I. Orders Deployed In the System

	Client ID	Order Side	Order Availability	Quantity	Action Price (ETH)	Market Price	Gas Used
1	1	SELL	OPEN	2	2.5	0	194866
2	2	BUY	FOK	1	2.3	0	63976
3	2	BUY	FOK	1	2.5	2.5	167741
4	3	BUY	OPEN	1	2.3	2.5	195891
5	2	SELL	FOK	1	2.2	2.3	110624
6	1	SELL	OPEN	10	2.5	2.3	233983
7	2	BUY	IOC	15	2.5	2.5	224654
8	1	SELL	OPEN	5	2.5	2.5	194866
9	3	BUY	IOC	6	2.5	2.5	88712

In the centralized system, the fees paid by the clients are proportional to the money ruled by the client in the past 3 months. A sporadic client of the BVB system is charged with a fee of 0.65% however, the higher the turnover of that client, the more the commission is reduced. The lowest commission charged by the BVB system is 0.30 % of the traded value, which is applied to clients that have run in the previous 3 months more than 375.000 dollars as presented in Table II.

TABLE II. Commissions of the BVB system

Tradeville (BVB commission)		
Orders run in the last 3 months		Commission
< 300 000 RON	< 75.000 $	0.65%
300 000 - 700 000 RON	75 000 - 175 000 $	0.50%
700 000 - 1 500 000 RON	175 000 - 375 000 $	0.40%
> 1 500 000 RON	> 375 000 $	0.30%

On the other hand, in the decentralized system, the fees are not proportional to the traded value, but are computed based on the number of instructions (gas) run for executing the contract code. The mining fees that are paid by the client in order to reward the miner are computed as the product between the price that the client is willing to pay per gas unit and the units of gas consumed for executing the instructions in the contract. When choosing the next transactions to be mined, the miners will maximize their benefits by choosing the transactions that have the largest gas price. As a result, the clients are motivated to choose larger price values per gas unit, in order to ensure that their transactions are mined as soon as possible.

On the Ethereum main network [26], a transaction with the gas price of 1 gwei is ensured to be mined within 30 minutes. However, by increasing the price over 8 gwei per gas unit, the transaction is ensured to be mined in matter of seconds.

The simulation has been run considering three specifications: 4 gwei, 8 gwei and 13 gwei per gas unit. Considering this, the highest fee registered in the system is 1.62 dollars, whereas the BVB fees for the same orders are between 3.52 dollars and 8.67 dollars. The fees in the blockchain system however, are proportional to the number of instructions in the contract

TABLE III. Fees Paid for the Orders Execution

	Gas Price (4 gwei)		Gas Price (13 gwei)		BVB Cost ($)		
	ETH	$	ETH	$	0.65%	0.50%	0.30%
1	0.0007	0.416	0.0025	1.35	8.678	6.675	4.005
2	0.0002	0.136	0.0008	0.44	7.983	6.141	3.685
3	0.0006	0.358	0.0021	1.16	8.678	6.675	4.005
4	0.0007	0.418	0.0025	1.36	7.983	6.141	3.685
5	0.0004	0.236	0.0014	0.77	7.636	5.874	3.524
6	0.0009	0.499	0.0030	1.62	8.678	6.675	4.005
7	0.0008	0.479	0.0029	1.56	8.678	6.675	4.005
8	0.0007	0.416	0.0025	1.35	8.678	6.675	4.005
9	0.0003	0.189	0.0011	0.62	8.678	6.675	4.005

As one can see in Table III one can deploy the same market order (entry 1 and entry 6) and have pay different mining fees. Due to the iterative instructions implemented in the contract, whenever a new order is placed the number of instructions will also increase proportionally with the number of orders contained in the order book. In Fig. 5 the results of a simulation of deploying the same order on different configurations of the order book length. We considered the first order from Table I to be deployed at the gas price of 13 gwei in order to ensure its fastest mining. The fees of the decentralized system are varying for the same order from 1.35 dollars when the order book is empty, to 30 dollars when the order book contains 100 orders. On the centralized system however, the fee remains the same according to the commission category from which the client is a part of.

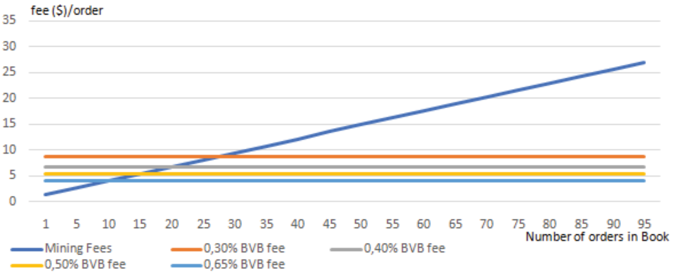


Fig. 5. Variation of fees with respect to the code complexity

The second simulation presented in Fig. 6 aims to evaluate the systems with respect to the variations of the value transacted from 1 ETH to 100 ETH. The price of the ETH at the moment of simulation was considered to be equal 534 dollars. In the simulation setup the order book is filled with 100 orders, thus the fees of the decentralized simulation are constant to 30 dollars no matter the value transacted. However, the centralized system fees are increasing proportionally to the value transacted, reaching the most expensive fee of 330 dollars for a 100 ETH order.

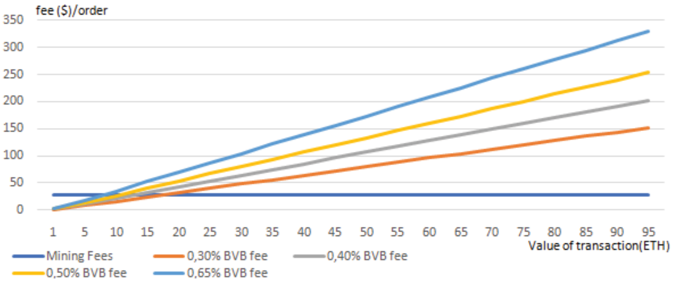


Fig. 6. Variation of fees with respect to the value transacted

As a result of the simulations, we conclude that when transacting in a market with partially filled order books the decentralized system has the clear advantage of being the cheapest option. However, when the order book is increased in size, a sporadic client has the advantage of trading in a centralized system up to 5 ETH (2500 dollars) from which point, the decentralized system becomes more advantageous choice. For a high profile client however, the fees of the centralized system may prove to be more advantageous when trading up to 20 ETH (10000 dollars) per order. But for higher valued trades, the decentralized system is clearly a better option.

VI. CONCLUSIONS

In this paper, we propose a decentralized solution for the BVB Stock Exchange Market to overcome the drawbacks of the centralized architecture and reduce the transaction fees due to the brokers and central authorities. We integrate the stock market elements in a blockchain architecture together with associated smart contracts that ensure self enforcement of the published orders.

A prototype was implemented in Ethereum to validate and test the proposed architecture. The results are promising showing that for partially filled order books, the blockchain based solution has a clear advantage of providing lower fees. Furthermore, for filled order books, the decentralized approach gives better results than the centralized approach only for orders more expensive than 2500 dollars, where the mining fees become smaller than the broker fees. However, for a high-profile client that trades tens of thousands of dollars, the blockchain-based architecture requires far less fees than traditional stock exchanges.

As future improvements we propose to study the integration of state channel for providing the system with a scalability of millions of transactions per second, while at the same time reducing the fees close to zero.

ACKNOWLEDGMENT

This work has been conducted within a research contract between Montran Labs, NY, USA and Technical University of Cluj-Napoca - Distributed Systems Research Laboratory.

REFERENCES

[1] Chris Dannen, “*Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners”,* Published by Springer Science+Business Media New York, ISBN: 978-1-4842-2534-9

[2] Luke Parker, “*Moody's new report identifies 25 top blockchain use cases, from a list of 120”,* Available online at https://bravenewcoin.com/news/moodys-new-report-identifies-25-top-blockchain-use-cases-from-a-list-of-120/

[3] State of the Dapps, https://dapps.ethercasts.com/

[4] M. Mihaylov, S. Jurado, K. Van Moffaert, N. Avellana, A. Nowe, “*NRG-X-Change A Novel Mechanism for Trading of Renewable Energy in Smart Grids”*, in Proceedings of the 3rd International Conference on Smart Grids and Green IT Systems, pp. 101–106, Apr. 2014

[5] TransActive Grid, Available at http://transactivegrid.net/

[6] SolarCoin, Avialable at https://solarcoin.org/en/front-page/

[7] Grid Singularity, Available at https://gridsingularity.com/

[8] Grid+ , Available at https://gridplus.io/

[9] Pop Claudia, Tudor Cioara, Marcel Antal, Ionut Anghel, Ioan Salomie, and Massimo Bertoncini. "Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids." *Sensors* 18, no. 1 (2018): 162.

[10] N. Zhumabekuly Aitzhan , D. Svetinovic,”*Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams”*, IEEE Transactions on Dependable and Secure Computing, Oct 2016

[11] KONSTANTINOS CHRISTIDIS, MICHAEL DEVETSIKIOTIS, “Blockchains and Smart Contracts for the Internet of Things”, SPECIAL SECTION ON THE PLETHORA OF RESEARCH IN INTERNET OF THINGS (IoT) June 2016

[12] Slock.it Blockchain + IoT, Available online at: https://slock.it/faq.md

[13] S. Huh, S. Cho and S. Kim, "*Managing IoT devices using blockchain platform," 2017 19th International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, , pp. 464-467. doi: 10.23919/ICACT.2017.7890132, 2017

[14] Serguei Popov, *"The tangle*", Self-Published 2015

[15] Cognizant, "*How Blockchain Can Slash the Manufacturing "Trust Tax'*"", Available online at https://www.cognizant.com/whitepapers/how-blockchain-can-slash-the-manufacturing-trust-tax-codex2279.pdf

[16] Cognizant*, " Blockchain's Smart Contracts: Driving the Next Wave of Innovation Across Manufacturing Value Chains Smart"*, Available online at https://www.cognizant.com/whitepapers/blockchains-smart-contracts-driving-the-next-wave-of-innovation-across-manufacturing-value-chains-codex2113.pdf

[17] Saveen A. Abeyratne , Radmehr P. Monfared*, " Blockchain ready manufacturing supply chain using distributed ledger"*, International Journal of Research in Engineering and Technology, September 2016

[18] Provenance, Available at https://www.provenance.org/

[19] Fluent, Available online at https://hijro.com/

[20] Blockpharma, Available at http://www.blockpharma.com/

[21] Giulio Prisco, "*Walmart Testing Blockchain Technology for Supply Chain Management*", Available at https://bitcoinmagazine.com/articles/walmart-testing-blockchain-technology-for-supply-chain-management-1482354996/, December 2016

[22] Alicia Naumoff, "*Engine for Blockchain: Toyota Financial Services joins R3*", Available at https://cointelegraph.com/news/engine-for-blockchain-toyota-financial-services-joins-r3, June 2016

[23] Diana Asatryan, "*Blockchain Is Coming to the Auto Industry, and Not Just for Financing*", Available online at http://bankinnovation.net/2017/02/blockchain-is-coming-to-the-auto-industry-and-not-just-for-financing/, February 2017

[24] Bucharest Stock Exchange, Available online at http://www.bvb.ro/

[25] "Execution, Clearing and Settlement", Available online at https://thismatter.com/money/stocks/settlement-and-clearing.htm

[26] Ethereum Gas Station, Available online at https://ethgasstation.info/