Decentralising Stock Exchange Using Blockchain

Amaldev P J[#1], Gokulkrishna S[*2], Mohammed Salman[#3], Prof. Elizabeth Issac[*4]

[#1, *2, #3]*Department of Computer Science and Engineering*
Mar Athanasius College of Engineering, Kothamangalam, Kerala, India
[*4]*Professor, Department of Computer Science and Engineering*
Mar Athanasius College of Engineering, Kothamangalam, Kerala, India

Abstract *-The traditional stock market posses lot of shortcomings such as high transaction fees, centralized system susceptible to attacks and lack of openness regarding the market actions and algorithms, Moreover,lack of awareness among stock sector among common people is also an issue. We propose an innovative architecture using blockchain to develop a decentralized stock exchange and 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 through consensus algorithm as well as it provides a stock prediction system which allows all kinds of people to know about the trend . 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.*

Keywords — *Stock exchange, Blockchain, Distributed ledger, Smart contract, Ethereum.*

INTRODUCTION

Challenges at Stock Market

The stock market is actually a measure of the health of the economy as well as a reflection of the future, which is highly sensitive. There always lies huge opportunities and problems in the market. Though it brings profit for many, investing in stock has always been a risky factor. The participants must be more alert and familiar about what is happening in the stock market for a successful investment. Transparency and trust are the major factors that are required in a stock trading market.

Here are some of the common challenges faced by the stock market. Involvement of intermediaries increases operational risks and costs more. This also slows down the settlement process .The existing stock market is centralized and the process is not transparent. The participants fail to have direct dealing over Financial burden which is one of the common problems in stock markets. The process may involve a lot of intermediary and needs more financial transactions.

The major issue lies in security. The investors doesn't know whether they will get their stock value or not. Trust on third party is required in stock trading. It is not easy to earn trust of investors.

Blockchain Applications at Stock Market

Implementing blockchain with smart contract will eliminate the need of a third party as the transactions, rules, regulations and everything in the stock market will be induced in smart contract. This will reduce operational risks to a great extent Companies can issue tokens which can be built in-house, using blockchain. These tokens will have smart contract to automate the performance as per the functions defined at the time of its designing. Features like permissions to users , potential to drive promotions, transaction features and much more are embedded in smart contract to provide a wider applicability than the general stock on a stock exchange. When integrating tokens in the stock market, the market is not limited to investors alone, but also wide open to the token holders. This will help an enterprise to make huge capital for business.
Time required to set up a token on blockchain, excluding ICO and marketing process is much lesser than the time consumed in stock exchange. Also, the present stock market involves more middleman and thus transactions become complex and take at least 3 days to complete an exchange. Blockchain can eliminate this complexity and consume less time for an exchange. Besides time, trading on blockchain is faster than traditional stock trading. This is because of the features which are built on smart contracts and as new innovations come, it creates faster protocols that eliminate the speed limitations.
Blockchain creates a decentralized database which is highly safe and has the ability to store complete information about the token holder and history of transactions, which is missing in the current stock market system.

LITERATURE REVIEW

Blockchain

The concept of blockchain was proposed by Satoshi Nakamoto in 2008. Blockchain can be explained as a growing list of records called blocks. Each block in a blockchain contains a cryptographic hash of the previous block, data and a timestamp. The data in blockchain is tamper proof. It is an open distributed ledger that records data in a permanent and verifiable way. Blockchain is managed by apeer-to-peer network adhering to a protocol for internode communication and validating new blocks. Once the data is recorded in a block, it can't be altered without alteration of all successive blocks in the blockchain, which requires permission of the network majority. Blockchain can be used in digital identity, tokenization, financial, markets, inter-organizational data management and many more.

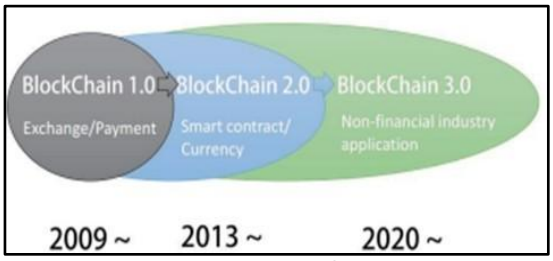

Fig. 1 : Development of blockchain

Blockchain is an online ledger that lends decentralized and transparent data sharing. Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the blocks then form a blockchain with timestamps. The whole procedure is open to the public, transparent, and secure.

Ethereum

Ethereum is software running on a network of computers that ensures that data and small computer programs called smart contracts are replicated and processed on all the computers on the network, without a central coordinator. The vision is to create an unstoppable censorship-resistant self-sustaining decentralised world computer.

It extends the blockchain concepts from Bitcoin which validates, stores, and replicates transaction data on many computers around the world (hence the term 'distributed ledger'). Ethereum takes this one step further, and also runs computer code equivalently on many computers around the world.

What Bitcoin does for distributed data storage, Ethereum does for distributed data storage plus computations. The small computer programs being run are called smart contracts, and the contracts are run by participants on their machines using a sort of operating system called a "Ethereum Virtual Machine".

Smart Contract

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 that provide the possibility of developing smart contracts are: NXT , Side Chains , Hyperledger, and Ethereum. 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.

DESIGN

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. 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.

Proposed Design

Here we present 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.

Automation of post-trade events

Applying blockchain and smart contracts to post-trade activities can eliminate the need for intermediaries, reduce counter-parties and operational risk, while providing the infrastructure for faster trade settlement.

Mechanism for fairness and transparency

If implemented, blockchain can act as an online automated surveillance system for each transaction. A blockchain-based exchange can have inbuilt characteristics to track, block and report illegitimate attempt made by anyone on the network, and can provide a robust platform to implement the security policy and standards.

Lower transaction costs

Blockchain transactions are faster, as trade confirmations are done through smart contracts by peers instead of any intermediary. As the intermediaries in the system get minimised, costs associated with them, like trades record keeping, audits and trade verifications also get eliminated or reduced.

Higher liquidity

Blockchain can reduce the inefficiencies through automation, which also leads to reduction in cost and thus lowering entry barriers resulting into increased market base. For people, who could not access the markets due to cost barriers will be able to participate, ultimately increasing liquidity and investment.

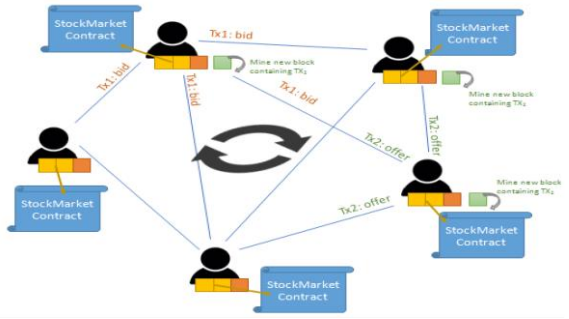

Fig 2 : Architecture

1) To model the Decentralized Exchange Platform, We develop a smart contract, the Stock Market contract that acts like an enhanced order book.

2) The Stock Market contract which is deployed on chain has wledge 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.

3) 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. Once the order transaction is gossiped among the peers, the integrity of the order is checked in the platform before its further next execution.

4) 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.

5) 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.

6) 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.

7) 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.

8) Once issued, these marketplace actions will be registered and replicated in future blocks across all the nodes in the network as presented in Fig 2.

9) 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 Stock Market Contract is replicated across all the nodes in the 10) 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 Stock Market 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.

STOCK MARKET PREDICTION USING MACHINE LEARNING

Machine learning can be used in order to predict the stock market. With the onset of recent advancements in machine learning applications, the field has been evolving to utilize non-deterministic solutions to learn what is going on in order to make more accurate predictions. The schematic diagram is given below:

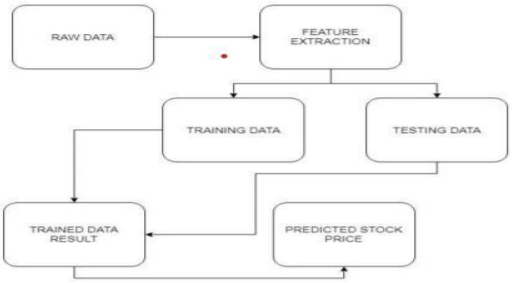

Fig 3 : Prediction

STEP 1. CHOOSING THE DATA : One of the most important steps in machine learning and predictive modeling is gathering good data, performing the appropriate cleaning steps and realizing the limitations. This step involves the selection of attributes for the prediction. An example is provided in the following figure

	1	2	3	4	5	6	7
1	Date	Open	High	Low	Close	Adj Close	Volume
2	11/11/13	88.519997	89.559998	88.410004	89.230003	85.394432	1151800
3	11/12/13	88.779999	89.309998	88.349998	89.25	85.413544	1102700
4	11/13/13	89.07	89.650002	88.519997	89.639999	85.786797	743000
5	11/14/13	89.470001	90.75	89.400002	90.300003	86.418427	1068800

Fig 4 : Table

STEP 2.CHOOSING THE MODEL : The next step is to choose a model. I We will use a neural network to perform a regression function. A regression will spit out a numerical value on a continuous scale, compared to a model that may be used for classification efforts, which would yield a categorical output. In this project, we are trying to predict the price of a stock on any given day .To build our model we are going to use Tensor Flow… well, a simplified module called TFANN which stands for "Tensor Flow Artificial Neural Network." In order to do this, we are going to use Google Colab.

STEP 3. TRAINING THE MODEL: We will split this dataset into 60% train, 20% validation, and 20% test. The model will be trained using the train set, model hyperparameters will be tuned using the validation set, and finally the performance of the model will be reported using the test set. In the moving average method, the predicted value will be the mean of the previous N values. In our context, this means we set

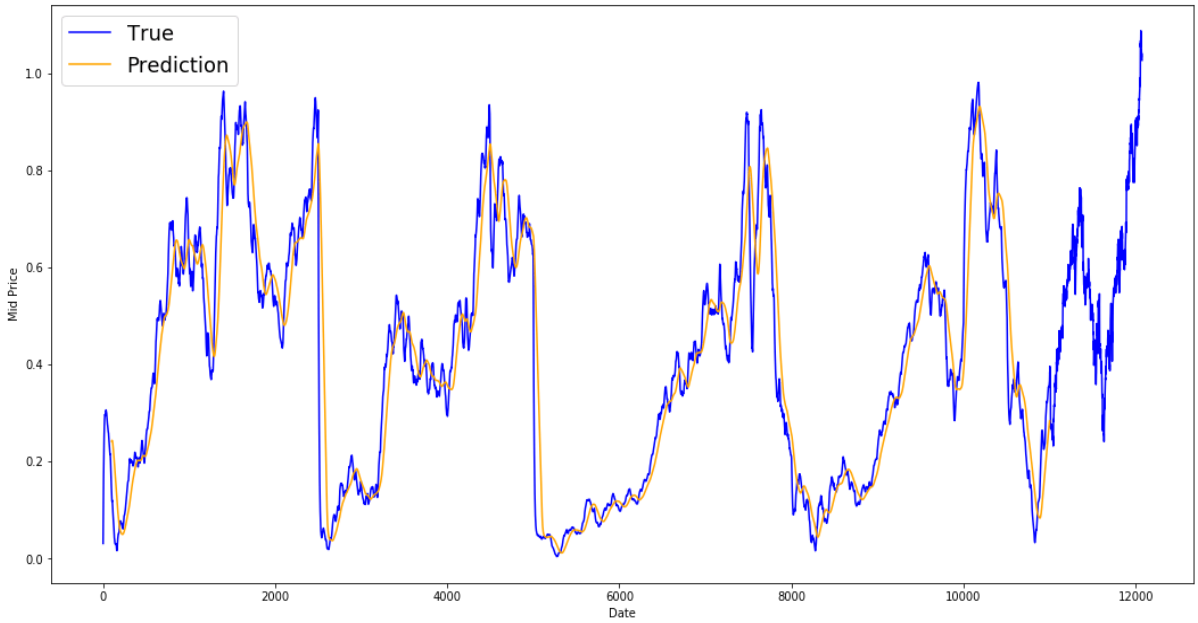

Fig 5: Prediction graph

the current adjusted closing price as the mean of the adjusted closing price of the previous N days. The hyperparameter N needs to be tuned. Other method is linear regression

method. Linear regression is a linear approach to modeling the relationship between a dependent variable and one or more independent variables. The way we are going to use linear regression here is that we will fit a linear regression model to the previous N values, and use this model to predict the value on the current day

The validation and the testing datasets can be used to check the consistency of the model and is used to validate the model

The Mean Squared Error (MSE) can be calculated by taking the Squared Error between the true value at one step ahead and the predicted value and averaging it over all the predictions.

Standard Average

First we will try to predict the future stock market prices (for example, x_{t+1}) as an average of the previously observed stock market prices within a fixed size window (for example, x_{t-N}, ..., x_t) .The normal averaging works in following way:

$$x_{t+1} = 1/N \sum_{i=t-N}^{t} x_i$$

In this method,t+1 is the average value of all the stock prices you observed within a window of t to t-N .

The output in this method is given below:

Exponential Moving Average(EMA)

In the exponential moving average method, you calculate

$x_{t+1} = EMA_t = \gamma \times EMA_{t-1} + (1-\gamma)\, x_t$ where $EMA_0 = 0$ and EMA is the exponential moving average value you maintain over time.

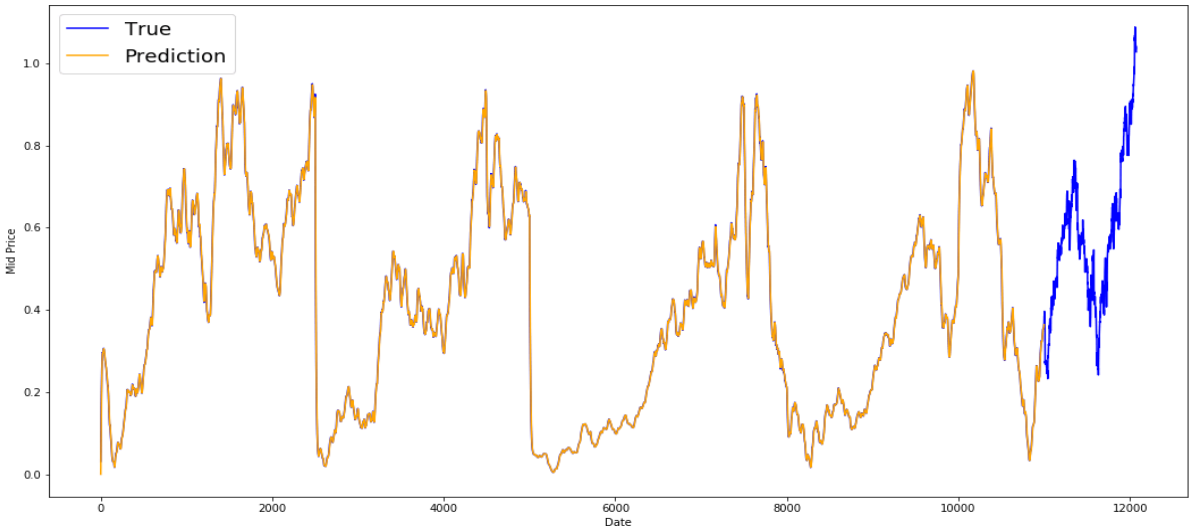

Fig 6: Prediction graph

The above equation basically calculates the exponential moving average from t+1 time step and uses that as the one step ahead prediction. γ decides what the contribution of the most recent prediction is to the EMA. For example, γ=0.1 gets only 10% of the current value into the EMA. Because you take only a very small fraction of the most recent, it allows to preserve much older values you saw very early in the average. The diagram is given below

CONCLUSION

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

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] Trans Active Grid, Available at http://transactivegrid.net/

[6] Solar Coin, 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.itBlockchain + 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