

# Babylon: A model for a decentralized Stock Exchange

Abdul Malik<sup>1</sup>, Ujjwal Sharma<sup>1</sup>

<sup>1</sup>Department of Computer Science and Engineering, IIIT, Noida Campus, India

**Abstract**—After the rise of the internet in the 90's, the technology sector became dependent on the web in a major way. All the applications that were dependent on the internet soon realized that they have lost their autonomy and are on the mercy of a centralized architecture that is prone to security breaches. With the advent of Blockchain and its potential to disrupt long established centralized systems, the tech industry is set for a new revolution. Blockchain has already shown a deep impact on how we transact and keep record of money and finances. Its potential to simplify stock trading in a global market is the focus of this paper. The biggest hurdles that the present day stock trading faces are cumbersome regulations, time consuming processes, role of intermediaries and a serious lack of trust between parties involved. Through this paper, we explore a decentralized model based on Blockchain, named Babylon that can solve all the above mentioned hurdles and substantially simplify settlement of stocks. This paper attempts to portray the potential upgrades if we transfer the existing architecture to the model proposed and at the same time does a comparative study of the proposed model with existing work in this domain, highlighting the improved efficiency achieved by the proof of concept that is being proposed.

**Index Terms**—Blockchain, Stock Exchange, Decentralized Stocks, Babylon, Blockchain Applications, Cryptocurrency.

## I. INTRODUCTION

The origins of stocks and stock markets dates back to 11th century France, where businessmen traded debts on brokerage. It picked up momentum in 13th century when merchants from Venice started trading government securities. Since then, stock trade has evolved and changed drastically. Today, the largest of economies revolve around stock exchanges where everyday assets worth millions are traded. A stock exchange in essence is a central authority that mediates between brokers, stock traders and investors in trading securities in form of stocks, bonds and other financial instruments. In addition, traditional stock exchanges act as facilities for issuing and redeeming such financial instruments including the payment of dividends. In the recent decades the stock market has moved away from over the counter trading(though it still exists) and has become excessively dependent on computerized systems to handle the huge number of transactions effectively and within the constraints of time. Even though these computerized systems claim to be secure and a lot of focus is on ensuring the authenticity of the transaction, these systems are still highly susceptible to tampering as they serve as central and singular points of failure, which if compromised can lead to disaster. To ensure this does not happen stock exchanges spend lavishly to maintain and secure their operations, which in turn lead to high transaction fees borne by the buyers and sellers on

the market. This drives the cost of trading for the buyer and seller but ensures that the transaction is authentic. However, a cost benefit analysis of the existing system illustrates that the drawbacks of having a central authority far outweigh the benefits. This cost benefit analysis and the drawbacks are discussed in the subsections that follow.

### A. Existing Architecture

The two most important parties in a stock market are buyers and sellers. These parties trade in previously issued shares which are offered by one investor and another investor buys them. This nature of the stock trading wherein the shares are previously issued means that this trading does not have any direct impact on the company being traded. The investor willing to buy places a order to buy at the current price or a limit order to buy if the stock falls to a certain price. In the traditional system the process begins when an investor signs up with a broker. Then the investor lets the broker know, what he wants to buy or sell. The broker then relays the order to the trading desks. Upon which the trader of the trading desk present at the stock exchange fills out the physical form for the purchase. Upon successful transaction the confirmation works its way back to the customer through the same channel. The existing Stock market architecture is reliant on central establishments like the Exchange, Clearing House, Settlement System or Centralized Repository. This process is very time consuming and costs are quite high. The intersection of the traditional model with the internet substantially reduced the time and costs involved but the involvement of the broker and a physical stock exchange or a central authority remain. In the internet architecture you place the buy request or sell request directly from your computers or mobiles but the processing still happens via a broker.

### B. Drawbacks of Traditional Stock Market

The traditional stock markets are strewn with issues of centralized architectures. In such markets central components gather all the data and register them at one central server. In such a scenario where the network over which transactions are happening is owned by a central third party, the network can become easy target for attackers and since the server is a single point of failure, this system is susceptible to even more damage. Also, having a central authority managing every transaction in the system provides for the authority to control and set the prices for processing transactions and other fees as they see fit. Furthermore, the existing system is heavily

dependent on intermediaries also called brokers in the market lingo who act on the behalf of the client in exchange of a fee. This fee and unnecessary involvement can be removed through the use of our proposed system. Another major issue with the traditional system are the long processing times and long settlement delays that essentially destroy the dynamic nature of the stock markets and a completely electronic system can significantly reduce this waiting time and we may be able to achieve the settlements of stocks in near real time. In a nutshell, introducing Blockchain will solve the major issues faced by the stock markets like Insider Trading, Third party involvement, Price control of transaction fees and in some cases of the stocks and the problem of non transparent trading algorithms.

### C. Introduction to Blockchain

The blockchain technology is an upcoming field and promises solutions that will change the way we interact with the internet and the web. Chriss Dannen compares the revolution of the blockchain technologies with the one brought by Ted Nelson through the HTTP concept in 1965[1]. Although still a topic of research and a long way from being perfect, blockchain technologies, are already being employed by lots of companies and startups for ground breaking ventures.

In 2016 over 120 blockchain projects were 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]. A blockchain based solution offers many improvements and upgrades from the traditional implementation paradigms. For starters, it eliminates the need of a middleman. It does so through Smart Contracts, that enforce the rules on the chain. Secondly, the blockchain i.e a hashed linked list of blocks allows for easy tracking of the currency and state updates that happen in the chain. Also, since the records are public and replicated this provides great transparency. Furthermore, the blockchain platform provides high security through consensus, public key cryptography and tamper proof recording. The immutability or the idea that the transactions cannot be modified is a characteristic achieved by the enforcement of the consensus algorithms together with the linked data structure. 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]. Other solutions aim to decentralize the Demand Response programs 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 company that develops electronic locks manageable through blockchain tokens. The authors of [7] 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 [8] 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. In [8] 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. Several startups have started developing solutions in the context of decentralized asset tracking applications using blockchain. Fluent is another startup that aims to provide supply chain services regarding financial solutions. 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.

### D. Proposed Methodology

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 [8] that provide the possibility of developing smart contracts are: NXT [1], Side Chains [5], Hyperledger, and Ethereum[1]. 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:

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

The Stock Market 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. 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 the figure below. diagram here.png diagram here.png

Insert diagram here.png

## II. PROPOSED FRAMEWORK

Whenever a company decides to go public and raise funds by selling shares, it liquidates a fraction of its stake, decides the opening value for each share and makes a “genesis” transaction regarding the shares on the Blockchain, sending the decided amount of shares both from and to the company’s identity. This serves as a announcement to all miners and spectators about the company’s newly-updated status.

Now that the trading has commenced, people may buy shares from the company at the value set by the company. Once enough shares have been sold by the company, the company gradually loses almost complete control over the valuation of it’s stock as it becomes possibly to both buy from and sell to third parties. Thus, the value of the company’s stock is now primarily dependant on supply-demand which in turn is dependant on a couple other factors, like the turnover of the company and the general performance of the company in the markets.

In order to raise more funds, the company may choose to liquidate more stake and sell more shares, further losing absolute control over company matters. Also, the company may decide to mass-purchase it’s own stock in order to regain control over company matters as well as the valuation of it’s own stock. All transactions regarding the trade of stock are recorded on the said blockchain and mimic any other form of transfer/transaction on a model blockchain.

The core difference between the model Blockchain employed in contemporary cryptocurrencies is that instead of transfer of a single commodity from Alice to Bob (BTC or ETH, for example), there instead is an exchange of commodities (for example, the exchange of X amount of shares in company Y for Z ETH). Therefore, instead of the transaction being signed by the sender, it has to be signed by both parties involved and consequently, the miner now has to verify both signatures in order to validate the transaction. Since there is no new cryptocurrency involved in the functioning of this network (the creation of a new method of payment/exchange defeats the core idea behind the model), there is no inherent incentive to the miner since no new block will grant them a fixed amount of remuneration. Therefore, like most other non-traditional Blockchain applications, this one will also rely heavily on charging transaction fees from both parties involved in each transaction. This is not a very unreasonable demand since the current system also relies heavily on brokerage as well as maintenance charges and that when implemented optimally, this model will cut down transaction fees substantially. The model also allows one or both of the parties to incentivize certain transactions by offering higher than usual fees.

### A. Forthcoming

The proposed model brings two great systems together in order to strengthen both and create a more robust, secure final structure. The stock exchange is a very important institution in modern capitalistic economies. This is because it serves a very important function. While allowing people from different walks of life and physical location to diversify their assets and “make their money work for them”, the stock exchange

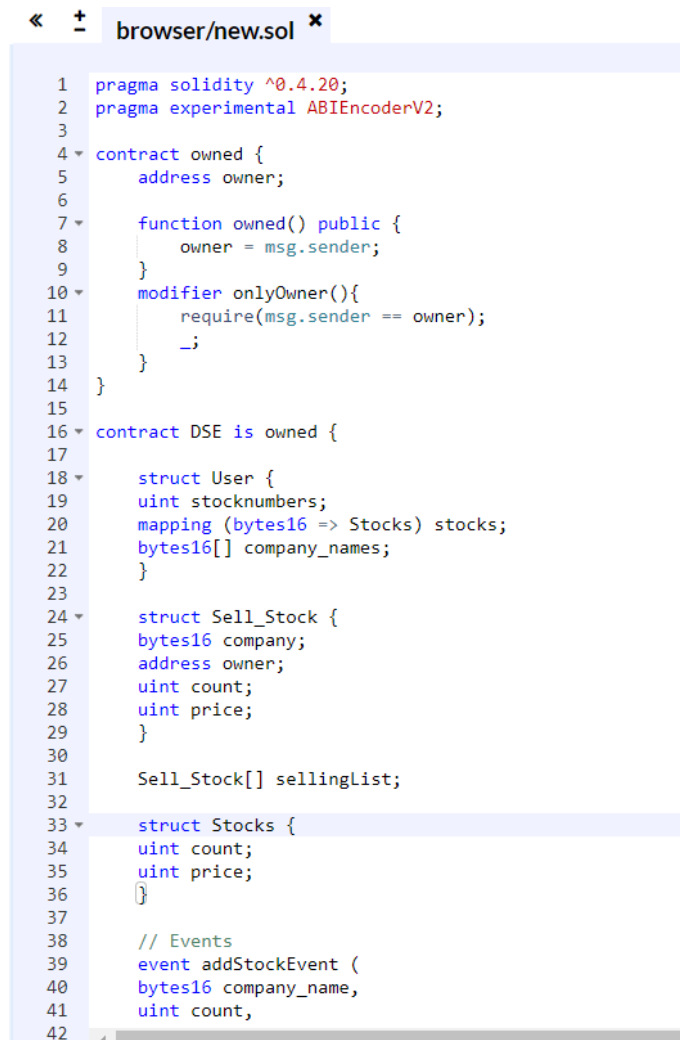
enables major players in the market – huge multi-billion-dollar corporations and smaller innovative start-ups riding the wave of exponential growth alike to get funding without losing a lot of stake in their company. This keeps assets as liquid as possible and avoids the economy from entering a slowdown as people hoard more and more resources, converting their savings into immovable assets. This system is further strengthened manifold by the proposed blockchain-based model by making the stock market more accessible to common public, driving down transaction fees and lowering the fence for smaller players to thrive in the modern investing scenario. It makes the stock market even more accessible by removing the need for specialized knowledge and equipment, making the act of investing as trivial as pressing a button on your mobile phone as well as opening up the stock market to people living in more remote areas where such options may or may not be available to the general public.

While we have discussed how the blockchain-based model substantially improves the status-quo in the modern stock markets, it also serves a huge blow to one of the biggest problems in the current cryptocurrency ecosystem – holding of tokens, or as it is affectionately called – hodling. According to some of the creators and founding fathers of the cryptocurrency revolution, one of the biggest challenges modern cryptocurrencies face these days is the problem of people holding on to tokens (eg: BTC, ETH) like immovable assets and not freely spending them like you would freely spend a normal currency. One of the biggest reasons for this is a very circular problem of unstable and fickle exchange rates. Most cryptocurrencies have very volatile exchange rates that will be substantially stabilized once they are used more freely like any other fiat currency, but spending them while the status-quo continues presents before one what is called the "thousand dollar socks" problem. Namely – if you bought a pair of socks using a couple of ETH today (while the value is a few dollars) and the value skyrockets overnight, preferably before your pair of socks are delivered to your residence, did you spend a thousand dollars for a pair of socks?

This problem might be completely eradicated by this model since people will have something better to hold on to – securities. Also, the companies who raise money in the form of cryptocurrencies will put them to good use and the market will be stabilized and strengthened substantially.

## B. Working

We are working on a prototype to implement the above said blockchain. A private blockchain network has been configured using the Ethereum core and contract on solidity. The Stock-Market contract (figure below) 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.



```

1  pragma solidity ^0.4.20;
2  pragma experimental ABIEncoderV2;
3
4  contract owned {
5      address owner;
6
7      function owned() public {
8          owner = msg.sender;
9      }
10     modifier onlyOwner(){
11         require(msg.sender == owner);
12         _;
13     }
14 }
15
16 contract DSE is owned {
17
18     struct User {
19         uint stocknumbers;
20         mapping (bytes16 => Stocks) stocks;
21         bytes16[] company_names;
22     }
23
24     struct Sell_Stock {
25         bytes16 company;
26         address owner;
27         uint count;
28         uint price;
29     }
30
31     Sell_Stock[] sellingList;
32
33     struct Stocks {
34         uint count;
35         uint price;
36     }
37
38     // Events
39     event addStockEvent (
40         bytes16 company_name,
41         uint count,
42

```

The web app makes use of GANACHE to create a private Ethereum blockchain for us to run tests, execute commands, and inspect state while controlling how the chain operates. It gives us the ability to perform all actions that we would on the main chain without the cost. We also use this to test our smart contracts during development. It provides convenient tools such as advanced mining controls and a built-in block explorer. We also use TRUFFLE as a developer environment, testing framework and asset pipeline for blockchains. It allows us to spin up smart contract projects and provides us with a project structure, files, and directories that make deployment and testing much easier (or else we would have to configure these ourselves). As a developer, we use Truffle project that lays out the structure of our project. For testing the code, we need a blockchain to do so. For which we use Ganache to be this blockchain. We use truffle migrate (which automatically runs truffle compile for us), to deploy the contracts with the data you provided in the migration files. Designing tools used during implementation are as under:

- 1) Framework : Truffle
- 2) Server Environment : NodeJS
- 3) Smart Contract Language : Solidity
- 4) Library : Web3.js
- 5) Ethereum Blockchain Simulator : Ganache-cli

### III. COMPARISON WITH EXISTING RESEARCH

content to be added

### IV. SCOPE FOR FUTURE WORK

content to be added

### V. CONCLUSION

In this paper, we propose a decentralized solution for the Stock 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 is being implemented in Ethereum to validate and test the proposed architecture. The blockchain based solution has a clear advantage of providing lower fees. As future improvements we propose to study the integration of international market exchanges and working on a more efficient data structure for providing the system with a scalability of millions of transactions per second, while at the same time reducing the fees close to zero.

### 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] 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.
- [6] 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
- [7] 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
- [8] 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>