





Article

Blockchain-Based Automated Market Makers for a Decentralized Stock Exchange

Radhakrishna Dodmane ¹, Raghunandan K. R. ^{1,*}, Krishnaraj Rao N. S. ², Bhavya Kallapu. ³, Surendra Shetty ⁴, Muhammad Aslam ^{5,6,*} and Syeda Fizzah Jilani ⁷

- ¹ Department of Computer Science and Engineering, NMAM Institute of Technology—Affiliated to Nitte (Deemed to be University), Karnataka 574110, India; rkddodmane@gmail.com
 - ² Department of Information Science and Engineering, NMAM Institute of Technology—Affiliated to Nitte (Deemed to be University), Karnataka 574110, India
 - ³ Department of Mathematics, NMAM Institute of Technology—Affiliated to Nitte (Deemed to be University), Karnataka 574110, India; bhavyak@nitte.edu.in
 - ⁴ Department of Master of Computer Applications, NMAM Institute of Technology—Affiliated to Nitte (Deemed to be University), Karnataka 574110, India; hsshetty@nitte.edu.in
 - ⁵ School of Computing, Engineering and Physical Sciences, University of West of Scotland, Paisley PA1 2BE, UK
 - ⁶ Scotland Academy, Wuxi Taihu University, Wuxi 214063, China
 - ⁷ Department of Physics, Physical Sciences Building, Aberystwyth University, Aberystwyth SY23 3BZ, UK; sjf7@aber.ac.uk
- * Correspondence: raghunandan@nitte.edu.in (R.K.R.); muhammad.aslam@uws.ac.uk (M.A.)

Abstract: The advancements in communication speeds have enabled the centralized financial market to be faster and more complex than ever. The speed of the order execution has become exponentially faster when compared to the early days of electronic markets. Though the transaction speed has increased, the underlying architecture or models behind the markets have remained the same. These models come with their own disadvantages. The disadvantages are usually faced by non-institutional or small traders. The bigger players, such as financial institutions, have an advantage over smaller players because of factors such as information asymmetry and access to better infrastructure, which give them an advantage in terms of the speed of execution. This makes the centralized stock market an uneven playing field. This paper discusses the limitations of centralized financial markets, particularly the disadvantage faced by non-institutional or small traders due to information asymmetry and better infrastructure access by financial institutions. The authors propose the usage of blockchain technology and the data highway protocol to create a decentralized stock exchange that can potentially eliminate these disadvantages. The data highway protocol is used to generate new blocks with a flexible finality condition that allows for the consensus mechanism to configure security thresholds more freely. The proposed framework is compared with existing frameworks to confirm its effectiveness and identify areas that require improvement. The evaluation of the proposed approach showed that the improved highway protocol boosted the transaction rate compared to the other two mechanisms (PoS and PoW). Specifically, the transaction rate of the proposed model was found to be 2.2 times higher than that of PoS and 12 times higher than that of the PoW consensus model.

Keywords: centralized financial markets; liquidity; information asymmetry; decentralized finance (DeFi); PoS; PoW



Citation: Dodmane, R.; K. R., R.; N. S., K.R.; Kallapu., B.; Shetty, S.; Aslam, M.; Jilani, S.F. Blockchain-Based Automated Market Makers for a Decentralized Stock Exchange. *Information* **2023**, *14*, 280. <https://doi.org/10.3390/info14050280>

Received: 2 April 2023

Revised: 29 April 2023

Accepted: 2 May 2023

Published: 9 May 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Centralized Stock Exchange is the agency where stocks of public companies are listed and traded. The exchange takes a fee whenever an order is successfully executed. If a trader wants to interact with the exchange, he/she has to go through a broker [1]. The trading process begins with the trader initiating the trade. The trader sends an order to the broker. Once the order has been placed, the broker is responsible for the order's execution.

If the asset being traded is highly liquid, i.e., has high volumes of supply and demand, it is sent directly to the exchange where it will be executed by the order book for the best price [1]. The order book refers to a digital list of buy and sell orders for a specific stock or a financial instrument arranged according to their prices. If the asset being traded is not highly liquid, then the market makers take up the responsibility of executing the trade [2]. A market maker, also called a liquidity provider, is an organization or an independent trader that quotes both a buy and a sell price for a stock held in their inventory, hoping to make a profit on the bid–ask spread. The bid–ask spread is the price difference between an immediate sale (ask) and an immediate purchase (bid) for stocks. Some market makers are called designated market makers as they are hired by the exchange to provide liquidity to one or more assets in the market. The main role of market makers is to roughly add three things to the market:

1. **Liquidity:** This means the availability of buyers and sellers at a given time. An asset being sold in the market is said to be liquid if it can be bought and sold easily without any time delay. Market makers may be appointed to provide liquidity for one or multiple assets depending on the market [3].
2. **Price discovery:** When an asset is being listed in a market, the price of the asset must be decided by someone based on the supply and demand; this responsibility is also taken up by market makers.
3. **Price continuity:** The prices, once discovered, must change continuously in a positive or negative direction based on supply and demand. The prices should not jump from one point to another in a random order. The market makers make sure that the starting price in a given day is not very far off from the previous day's closing price, thus providing price continuity.

Market making in centralized stock exchanges comes with its own disadvantages. The biggest disadvantage of them all is **information asymmetry** [4]. This means that market makers have better access to information such as the following:

- Order flow.
- Supply and demand data of a given asset or stock.
- Origin of trade (information about traders themselves).

Order flow and supply and demand information can be purchased from the brokers by the market makers to understand the direction of the trade being made and use this information to make trades against uninformed traders. The information about the origin of trades and trader information can also be used to trade against uninformed traders. Knowing about the traders will help market makers decide the order size and the time at which the order will be placed. This asymmetry in information can help market makers make profits at the expense of other market participants who do not have access to this information, thus creating a huge disadvantage for the regular traders.

Another major disadvantage that regular participants face is **infrastructure asymmetry**. This means that most market makers have access to faster communication systems, which give them advantages in order execution speeds and early access to orders placed by regular participants.

To create a fair market where all the participants have access to the same opportunities and information, the market must offer the following options to its participants:

1. Anonymity of the trader (optional).
2. Transparency of market orders.
3. Equal access to all market information.
4. Speed of information access and speed of execution should be the same for every participant in the market.

Giving these options to all market participants can, to a certain extent, make sure that the traders are not taken advantage of by the market forces. Currently, these options are hard to implement in the centralized exchange model. These shortcomings of the

centralized stock exchange model have led many market researchers to look for alternate market models to efficiently run the stock market.

This paper proposes a distributed ledger technology that can be used to build a **decentralized stock exchange**, which offers the above-mentioned options to traders, thus leveling the playing field [5]. The primary objectives are to determine the current state of research in this field, evaluate the merits and limitations of the existing methodologies, and identify potential gaps in the research that warrant further exploration. The main contributions of the paper are as follows:

- To give the reader an understanding of how automated market makers work.
- To explore how the technology can be used to build a decentralized stock exchange.
- To discuss the proposed consensus mechanism and decentralized stock exchange.
- To compare different automated market-making formulas.
- To compare centralized exchanges (CEXs) and decentralized exchanges (DEXs).

2. Literature Survey

In this section, we will describe some background knowledge to help readers understand our work.

2.1. Distributed Ledger (Blockchain) Technology [6]

A blockchain is a continuous chain of blocks that holds data in the form of a ledger, which are linked together following certain rules. These blocks contain a hash of the previous block's data, a timestamp, and transaction data. The timestamp proves that the transaction data existed when the block was published. As each block contains information about the previous block, each new additional block added will reinforce the chain, making it harder and harder to change the previous block's data. This is the reason why blockchains are considered tamper proof, as data once recorded cannot be altered without subsequently changing all future blocks. Blockchains are managed by a network of peer-to-peer participants as a publicly distributed ledger, where nodes follow a protocol to communicate and evaluate new blocks. Although blockchain records are immutable, new forks can lead to the creation of new blocks. The adoption of blockchain technology has the potential to significantly improve the quality of accounting information. By increasing the accuracy, transparency, efficiency, security, and auditability, a blockchain can help to ensure that financial information is reliable, trustworthy, and accessible to all stakeholder [7].

Properties of Distributed Ledger

Programmable is the ability of a system to be controlled or modified with code or software [8]. In the context of a blockchain, smart contracts are an example of programmable elements that can be used to automate complex processes and enforce the terms of an agreement. Smart contracts are self-executing programs that serve as an agreement between the buyer and seller that are directly written into lines of code. The code and the agreements are deployed publicly on the blockchain network.

Secure refers to the measures in place to protect against unauthorized access or attacks on a system [8]. In the context of a blockchain, this can include measures such as cryptography and consensus algorithms, which help ensure the ledger's integrity and security. Cryptography is used to secure the contents of blocks on the blockchain and to ensure that transactions cannot be altered once they have been added to the blockchain. Consensus algorithms are used to ensure that all parties agree on the state of the ledger and to prevent unauthorized changes from being made to it.

Anonymous is the ability to use a system without revealing one's identity using a self-sovereign identity that can be achieved using pseudonymous addresses that do not reveal the identity of the user. While the transactions that are associated with a particular pseudonymous address can be seen on the blockchain, the identity of the user behind the address is not revealed.

Unanimous is when all parties in a group or system agree. A consensus is achieved using consensus algorithms, which allow the network to agree on the ledger's state. Different blockchain networks use different consensus algorithms, each with their own trade-offs and characteristics. Some standard consensus algorithms include proof of work (PoW), proof of stake (PoS), and delegated proof of stake (DPoS).

Time-stamped is the inclusion of a timestamp in a record or transaction, which helps to establish the order in which the transactions occurred and to prevent double-spending using a globally agreed upon time source, such as the Coordinated Universal Time (UTC).

Immutable [9] refers to the inability to change or alter the network. The immutability of the blockchain is an important feature that helps to ensure the integrity and security of the ledger. A transaction cannot be altered once it has been recorded on a blockchain. This is achieved using cryptographic techniques, which make it computationally infeasible to alter the contents of a block once it has been appended to the blockchain.

Distributed is the fact that a blockchain ledger is stored and maintained by multiple parties in a network rather than being stored in a central location. This decentralization makes it more difficult for a single actor to alter the ledger, because any changes would have to be made simultaneously across all the copies in the network. The distributed nature of the blockchain is an important feature that helps to ensure the integrity and security of the ledger. It also allows the network to continue functioning even if some nodes are unavailable, since different parties are maintaining multiple copies of the ledger.

The author of paper [10] aims to examine the interrelationships of monetary policy's structural shocks, the real exchange rate, and stock prices. For the security of the transactions on stock exchanges, decentralization, immutability, and a robust consensus mechanism are the main properties of a secure blockchain-based system.

2.2. Decentralized Exchanges

Decentralized exchanges or DEXs are exchanges built on the blockchain using smart contracts [11,12]. It enables the peer-to-peer transfer of digital assets without the use of any intermediary and also offers a slew of other advantages. In DEXs, the users do not handover their funds or assets to any custodians or depositories, as the exchange is taken care of by smart contracts and is non-custodial. These exchanges are either partially or fully governed by a set of contracts.

Smart contracts are automatic contracts stored on blockchains. They are computer programs that run automatically when a certain condition is met or satisfied. They contain a set of instructions, which are usually written in the Solidity programming language if the Ethereum blockchain is being used. Ethereum is a blockchain protocol with smart contract functionality that allows developers to build decentralized applications on top of the blockchain [11]. Smart contracts run on the EVM (Ethereum Virtual Machine). The smart contract system is designed in such a way that it cannot access the network, file system, or any other processes running on the EVM.

DEXs were built as a response to the problems faced by centralized cryptocurrency exchanges, or CEXs, such as susceptibility to external attacks causing the loss of user funds and several other problems faced by centralized exchanges. There are many ways to build a DEX [12]. One way is to use the orderbook format of the CEX. This is performed by building an on-chain order book where every order is recorded on the blockchain; however, this can be very expensive, as every transaction on the blockchain costs money. There are off-chain order books as well, which record the order off-chain and only use the blockchain as a settlement layer. These are not as expensive as on-chain order books, but they do not offer the same amount of security and decentralization as on-chain order books [5].

Both on-chain and off-chain order books perform regularly in markets with high liquidity, but when the assets being traded are not highly liquid, they are not very useful. To solve this problem, some decentralized exchanges have adopted a new technique called automated market makers, or AMMs [13].

AMMs use liquidity pools, which store funds. The traders who are willing to buy or sell a cryptocurrency or a token do so by directly interacting with the pool, which decides the price of the asset using mathematical formulas. This technique works well even when the liquidity of an asset is low. A detailed explanation of AMMs with an example will be given in the next section.

Table 1 draws a comparison between orderbooks and AMMs in decentralized cryptocurrency exchanges. The metrics used to compare the two are some of the general criteria that an exchange has to fulfil.

Table 1. Comparison between centralized and decentralized exchanges.

Type	Trade Execution Speed	Availability during High Liquidity	Availability during Low Liquidity	Types of Orders	Scope for Market Manipulation	Scope for Market Failure
Centralized exchanges using regular market makers	Depends on the Liquidity	Yes	No	Multiple	High	High
Decentralized exchanges using AMM	Immediate	Yes	Yes	Limited	Low	Low

2.3. Automated Market Makers [13]

Earlier versions of decentralized exchanges suffered with low liquidity because it was hard to find an active set of sellers and buyers. AMMs fix the issue by allowing individuals to create or contribute to liquidity pools and offer these individuals incentives to supply these pools with assets. These individuals are called liquidity providers, or LPs, and the incentives they receive are in the form of trading fees when someone uses the pool that they created or contributed to. In liquidity pools, as the amount or reserve of assets in a pool increases, the liquidity of that asset also increases, and trading becomes easier on that exchange. By changing their formulas, liquidity pools can be optimized for different purposes. LPs are given liquidity pool tokens or LP tokens that are proportional to their contribution to the pool, which they can use to claim their share of the fees. The exact mechanics of AMMs vary from exchange to exchange based on the asset being exchanged, but generally, AMMs offer deep liquidity, low transaction fees, and 24/7 availability for as many users as possible. In a regular exchange, only individuals with access to huge capital or large institutions can provide liquidity, but in decentralized exchanges, anyone can become an LP, as long as they meet the requirements of the protocol being used.

This paper aims to give the reader an understanding of how automated market makers work. In the next section, a model for how the technology can be used to build a decentralized stock exchange will be discussed, along with a comparison of different automated market-making formulas. This work uses Uniswap v2's AMM smart contracts as a reference; hence, a brief explanation of those contracts will also be given in the upcoming sections [13]. After the explanation, a brief comparison between CEXs and DEXs will be made.

3. Working of Automated Market Makers (AMMs)

Automated market makers (AMMs) are a type of decentralized exchange (DEX) that uses an algorithm to determine prices and execute trades automatically, without relying on traditional order books. The typical materials and methods used in the operation of an AMM are as follows:

- **Liquidity pools:** An AMM operates through liquidity pools, which are pools of tokens that are locked in smart contracts. These pools are created by users who contribute

an equal value to two different tokens. The ratio of tokens in the pool determines the price of the assets in the pool.

- **Mathematical algorithms:** AMMs use mathematical algorithms to determine the price of assets in the pool. The most common algorithm used in AMMs is the constant product market-maker algorithm, which is also known as the $X \times Y = K$ formula.
- **Trading interface:** AMMs provide a simple trading interface for users to buy and sell tokens in the pool. Users do not need to specify a price or a counterparty for their trades, as the price is determined automatically by the algorithm.
- **Incentives:** To encourage users to contribute liquidity to the pool, AMMs offer incentives in the form of transaction fees and liquidity provider (LP) tokens. LP tokens are given to users who contribute liquidity to the pool, and they represent a share of the pool's total value. LP token holders earn a portion of the transaction fees paid by traders using the AMM.
- **Smart contracts:** All operations on AMMs are executed through smart contracts on a blockchain network. These smart contracts automatically execute trades, adjust prices, and distribute transaction fees and LP tokens to users.

The working of AMMs differs based on the underlying assets being traded. The most popular form of AMMs in decentralized crypto exchanges are the constant function market makers or CFMMs, which will be explained with an example below [13].

3.1. Constant Product Market Makers

This AMM is of the form

$$X \times Y = K$$

where X and Y are assets (tokens) in the pool, both valued relative to each other, and K is their product. While creating the pool, it must have a 50:50 ratio of each asset. Equation (1) must satisfy the following condition:

$$(Rx + (f + \Delta x))(Ry - \Delta y) = K \quad (1)$$

where Rx and Ry are the reserves for assets X and Y and f is the transaction fee. Δx is the amount of X being added to the pool and Δy is the amount of Y being removed from the pool. Trading any amount of either assets will change the reserves in such a way that, when the fee variable is ignored, the product $Rx \times Ry$ remains equal to the constant K . In practice, because of the fee being non-zero during each trade, the constant K keeps increasing [13].

An example for the usage of this formula would be, let $X = 1000$ and $Y = 5000$, which would result in $1000 \times 5000 = 5,000,000$. This would mean that 1000 X tokens are equal to 5000 Y tokens. If a trader wanted to buy 200 X worth of Y tokens, then the process would be as follows:

$$(X + \Delta x) \times (Y - \Delta y) = K \text{ (representation of the trade when fees} = 0)$$

Substituting values in the above equation, we obtain the final equation:

$$1200 \times 4166.666 = 4,999,999.2 \text{ (after solving for } \Delta y, \text{ we achieve } 833.334)$$

From the solution, it can be said that 833.334 Y tokens can be obtained for 200 X tokens, and the final equation will be the new reserve in the pool after the first trade. If the same trade is repeated a second time, the value obtained for Δy will be 595.238. This decrease in the amount of Y tokens obtained by adding the same amount of X tokens occurs because the formula works in such a way that, as the demand for a particular asset increases, the price for the asset will also increase. Hence, if a trader wants to obtain 833.334 Y tokens on the second trade as well, the trader must add more than 200 X tokens into the pool. This also makes sure that the reserve of any one token in the pool does not reach zero, because as the reserve of a token keeps decreasing, the price keeps increasing, making sure that it

becomes harder to bring the reserve of any one asset to zero. If the above-mentioned trade is repeated 45 times, the X token vs. the Y token reserve curve obtained will be as follows:

As seen in Figure 1, the equation forms a hyperbola when plotting for two assets, which gives the property of having continuous liquidity as the prices reach infinity on both sides. The Uniswap v2 protocol uses a constant product market maker in its decentralized exchange [13].

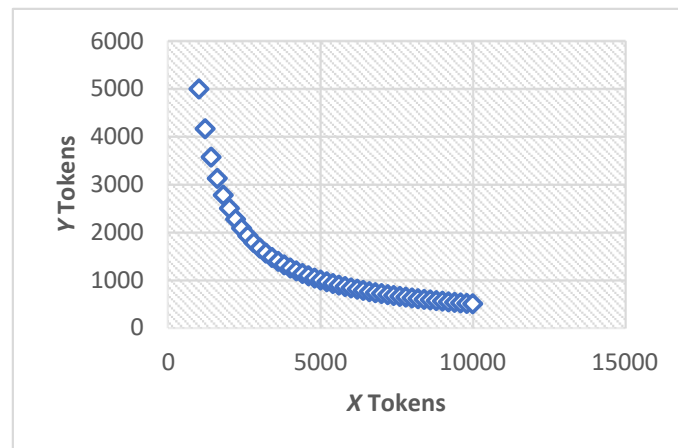


Figure 1. Graph showcasing the property of having continuous liquidity as the prices reach infinity on both sides.

3.2. Constant Sum Market Makers

This formula uses a sum of tokens in the pool instead of a product [14]

$$X + Y = K$$

which satisfies the condition:

$$\sum_{i=1}^n R_i = K$$

where R_i is the reserve of each asset in the pool and K the constant. Any number of assets can be added to the pool depending on the requirement. This formula offers zero slippage but does not offer infinite liquidity; thus, the formula has never been used in any real-world applications [15]. The constant sum function forms a straight line when plotting for two assets.

Figure 2 shows how the formula offers low slippage but not infinite liquidity [10]. This means that the price movement when the trades are made will not be as drastic as other AMMs, but the formula does not guarantee that the reserve of the pool will not fall to zero.

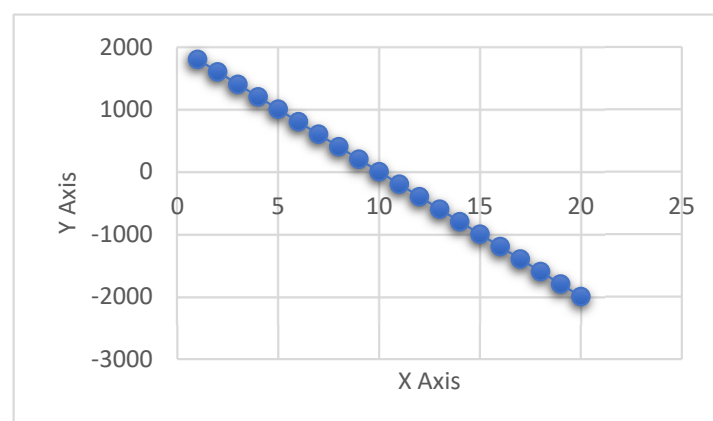


Figure 2. Graph showing low slippage but not infinite liquidity.

3.3. Constant Mean Market Makers

A constant mean market maker is another version of a constant product market maker; it allows for more than two assets to be stored in the pool and also allows for a varying weight of each asset, i.e., a weight ratio other than 50:50 [13]. The equation is of the following form:

$$\prod_{i=1}^n R_i^{w_i} = K \quad (2)$$

R_i represents the reserve of the assets in the pool, w is the weight of each asset, and K is the constant [16]. In a simplified form, the function for a pool of three assets would be shown using Equation (3) as follow:

$$\frac{(X^a \times Y^b \times Z^c)}{3} = K \quad (3)$$

where X , Y , and Z are assets, and a , b , c are their ratios, respectively. In other words, when the fee is considered zero, the constant mean markets ensure that the mean of the reserves remains constant.

Figure 3 shows the bonding curve for an equally weighted portfolio of three assets, formed by the Balancer protocol, which uses a constant mean market maker [13,17].

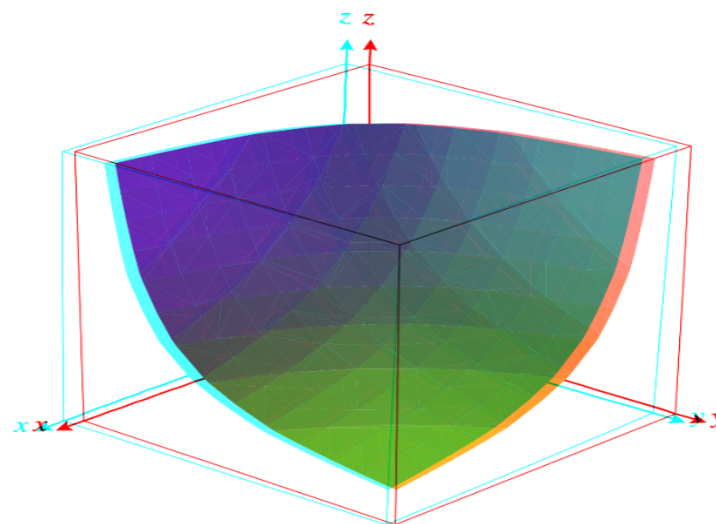


Figure 3. Three-dimensional view of bonding curve for an equally weighted portfolio of three assets.

3.4. Hybrid Constant Function Market Maker

There are several projects that use hybrid functions to achieve desired characteristics based on the properties of the assets being traded. Curve (stable swap) uses a hybrid version of the constant function formula to reduce the amount of slippage in the function [12]. The formula uses a hybrid of a constant product and constant sum:

$$A n^n \cdot \sum x_i + D = A D n^n + \frac{D^{n+1}}{n^n \prod x_i} \quad (4)$$

where x_i represents the reserve for each asset in the pool, the number of assets is n , D is the invariant, and A is the amplification coefficient, which is dynamic, i.e., can be tuned as per the needs of the user. This system behaves like the constant sum function when the pool is balanced and like the constant product function as the pool becomes more imbalanced. The graphical comparison of the hybrid function along with the constant sum and product is shown in Figure 4.

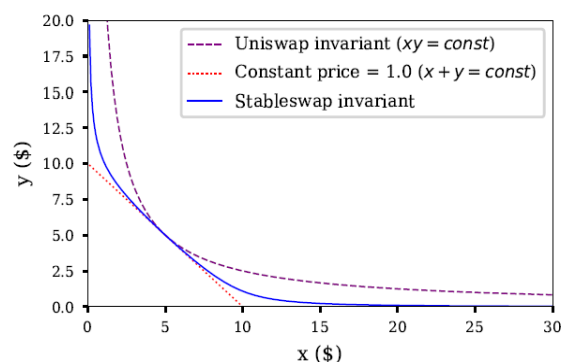


Figure 4. Comparison between constant product, constant sum, and hybrid function (stable swap).

Figure 4 gives a comparison between the constant product, constant sum, and hybrid function (stable swap) [18]. These are some of the AMM formulas that are currently in use by various cryptocurrency exchanges. AMMs use mathematical algorithms to set prices and determine liquidity, which allows for continuous trading and eliminates the need for a central party to match buyers and sellers.

Prediction markets are markets that allow individuals to bet on the likelihood of future events, such as election outcomes, sports events, or even the weather. The prices in these markets can be seen as market forecasts of the likelihood of the events occurring [19].

The combination of AMMs and prediction markets has become increasingly popular in recent years, with several platforms offering decentralized prediction markets powered by AMMs. These platforms allow users to buy and sell shares that represent the outcome of a particular event. The prices of these shares are determined by the market and are updated in real-time as more information becomes available.

One of the benefits of using AMMs in prediction markets is that they provide liquidity, which means that users can easily buy and sell shares without worrying about finding a counterparty. Additionally, AMMs are transparent, which allows users to see how prices are determined and make informed decisions about their trades.

In the next section, the model and the methodology used for building the exchange will be discussed along with an explanation of the technical implementation of the model.

4. The Proposed Consensus Mechanism and Decentralized Stock Exchange

The consensus mechanism for block creation is a critical component of blockchain technology. It is the process by which the nodes in a decentralized network agree on the validity of a new block and add it to the blockchain.

There are several consensus mechanisms, each with their own advantages and disadvantages. The most common ones are as follows: proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS), and byzantine fault tolerance (BFT).

The consensus mechanism used for block creation depends on the specific needs and goals of the blockchain network.

A blockchain-based distributed ledger framework has the potential to address the security and privacy issues in the stock market unit. By creating a distributed ledger, the market-maker applications can be securely stored and accessed by authorized parties while also ensuring data integrity and immutability.

To achieve this, a highway consensus protocol with flexible finality can be developed. This protocol can ensure that transactions are validated and confirmed quickly, while also allowing for flexibility in the finality of transactions. This means that transactions can be considered final after a certain number of confirmations, but they can also be reversed if necessary.

However, it is important to note that implementing a blockchain-based distributed ledger framework requires careful consideration and planning. It is crucial to ensure that the network is secure and scalable, and that all parties involved are aware of the risks and

benefits of using blockchain technology. Proper governance and regulation must also be in place to ensure the integrity of the market and protect investors.

4.1. Highway Consenses Protocol

The highway consensus mechanism presented in the manuscript offers a flexible finality based on threshold conditions for validators to confirm if a given block is valid. This means that the finality of a block can only progress for a particular validator until several validators deliberately violate the protocol, which is similar to the continuously rising number of approvals for a block in a proof-of-work (PoW) scenario [19]. However, the confidence levels for a particular block on the highway can easily be translated into the number of misbehaving validators required to invert such a block.

In the manuscript, the following conditions are defined for block inversion:

1. Single validator attack: A single validator must deliberately violate the protocol to invert the block. This is the minimum number of misbehaving validators required to invert a block [20].
2. Sudden power loss: In case of sudden power loss or system failure, a certain number of validators must be offline or unable to participate in the consensus process to invert the block [20].
3. Byzantine attack: In case of a Byzantine attack, where validators intentionally act maliciously, a certain number of validators must collude to invert the block [20].

By defining these conditions, the confidence level for a particular block can be easily translated into the number of misbehaving validators required to invert such a block. This provides a higher level of security and flexibility in the finality of blocks compared to traditional PoW mechanisms.

The finality condition: Once the genuine validator achieves finality with an assurance threshold for a given legitimate block B , then no genuine validator will ever achieve finality with an assurance threshold t for a block participating with B . In the threshold condition, the assessment results assert that the impossibility to guarantee the liveness of the assurance threshold $\frac{n}{3}$ and greater, in real-time, entails that a greater number of validators will not get away from most of the conditions of the consensus mechanism. In such cases, the assurance threshold can be achieved without finality conditions, which create a new block during these times and are almost impractical to revert. The confidence threshold values are generated through a limit value on the number of genuine validators that guarantee the protocol to select blocks. We consider a limit value that incorporates the conventional $n \geq 3f + 1$ limit value and combines with a notion of crashing faults, which is represented by c . The combination of limits and faults interrupts the consensus process, but not as much as the Byzantine crashing faults model.

The block guarantee condition: For the block guarantee process, every confidence threshold value should be in the range of $0 \leq t < \frac{n}{3}$, when $f \leq t$ and $c < \frac{n-3t}{2}$. The confidence threshold value is used to generate the chain of blocks based on the genuine validator with confidence t values.

The genesis block generation: The genesis block of the blockchain network is represented as G . We need to develop a smart contract that generates a genesis block. Excluding the genesis block, all other blocks are considered valid block B , which indicates to its parent block B . Expect for the parent block, other valid blocks are denoted by $nextB$ and $prevB$. The parent block B is validated through $prevB$, and for $nextB$ block, the parent will be the validating block. Additionally, we consider that the height of genesis block is 0 and donated by $H(G)$. For parent blocks and all other blocks, the height is represented as $H(B) = 1 + H(prevB)$. Consider the following example: we consider that B_1 is the successor of B_2 , and then the height is $H(B_2) \leq H(B_1)$, in this way, the block can reach a parent link.

GHOST-based voting rule for selecting the genesis block: The GHOST (Greedy Heaviest Observed Sub-Tree) rule selects a fork in a decentralized network. The following

rules are concretely used as a virtual voting process in the blockchain network in order to guarantee the genesis block.

The rule for the fork section: A main building block of the blockchain client network is selecting the fork. In this proposed blockchain model, we consider a group of blocks B_n that do not need to create a single chain. These sets of blocks create a tree in order to choose a single tip from the network, which is then selected as the head of the blockchain. In the PoW consensus mechanism, the longest chain of the tree is considered the head because it consumes more energy than the other blocks. In our proposed model, we introduce the GHOST rule for fork selection, which is validated by a set of blocks in the blockchain network. Sometimes, this process is not possible due to absences of additional information of validator blocks. We include the set of blocks B_n with opinions of each validator (V_n). The complete steps of the GHOST rules are described in Algorithm 1.

Algorithm 1: Fork Selection Process Based on GHOST Rule

1. For each block $B \in B_n$.
 2. Calculate the total number of blocks $total(B)$.
 3. For each validators $V \in V_n$ such that the block opinion is $V \geq B$.
 4. Choose B as the genesis block.
 5. Repeat the given rules when B is not a chain in B_n .
 6. Select $B' \in nextB$ with the network chain $totalB$.
 7. Set $B : B'$.
 8. Select the output B as the head.
-

4.2. Proposed Decentralized Stock Exchange

Automated market makers are nothing but a collection of smart contracts with instructions to execute trades. At the time of writing this paper, the most mature blockchain in terms of developers, users, and miners is Ethereum [21]. The model proposed in this paper uses Ethereum as the reference blockchain.

An AMM-based exchange consists mainly of two components. The first component is the asset that has to be traded. A decentralized stock exchange trades securities against a reserve currency. In Ethereum, the token standard that can be used to represent a reserve currency is ERC-20 [22]. The ERC-20 standard covers all the criteria needed to represent a currency. An alternate Ethereum token standard is needed to represent the security or stock token. These tokens require additional functionalities to better represent the underlying asset and to enforce regulations on the asset and the trader or the issuer of that asset. One of the standards that can be used to represent securities in Ethereum is ERC-1400 [23]. The second component is the AMM. The AMM that is used for such an application must either be for a general purpose or must be specific to stocks. Building an AMM specifically to trade stocks is out of the scope of this paper, as it would require more research into the mathematics involved in the game theory of financial markets. In the current work, an existing AMM formula has been used, as it has been tried and tested in the cryptocurrency markets. The AMM used for a decentralized stock exchange should be a general-purpose digital asset exchange tool because a stock or securities represent a fractional ownership or stake in a physical or digital entity. This ownership or stake can have different functionalities based on how it is implemented and what kind of entity will be using it. The stocks are bought or sold on exchanges using currencies that have their own characteristics. This AMM needs to have the capability to swap or exchange assets with fundamentally different natures.

Table 2 shows a comparison between different AMM formulas. The results demonstrate that constant product market makers, or CPMs, offer advantages when checking for different metrics that determine their usefulness as an AMM. CPMs, with some modifications, can be used to exchange digital assets that are independent of their individual values and properties, making them suitable for building an exchange for swapping stock with currencies. The metrics used are explained below.

Table 2. Comparison of different AMM formulas.

Type	Balancing	Slippage	Useful in Exchanging Stocks	Dynamic AMM	Flexibility in Asset Class
Constant product AMM	Yes	Yes	Yes	Yes (newer versions)	High
Constant Sum AMM	No	No	Yes	No	High
Stable swap AMM	Yes	Minimal	No	Yes	Only assets that are equally priced
Constant sum with varying weights AMM	Yes	Yes	Yes (as a portfolio manager)	No	High

Balancing: AMMs must be capable of balancing the reserves of the assets in the pool, making sure that no token in the pool reaches a balance of zero.

Slippage: This can be referred to as the difference between the quoted price and the executed price.

Useful in exchanging stocks: This refers to the capability of AMMs to be able to exchange assets other than cryptocurrencies.

Dynamic AMM: This refers to the capability of AMMs to dynamically adjust weights in their functions, reducing their reliance on arbitrage activities [13].

Number of different types of digital assets that can be traded: This metric is used to represent the capability of the AMM to be able to exchange assets other than cryptocurrencies.

The most used decentralized exchange in terms of trading volume, which uses CPMM, is the Uniswap protocol. It is a decentralized cryptocurrency exchange. It facilitates the exchange of cryptocurrencies and is built on the Ethereum blockchain. The current work uses Uniswap's v2 system of smart contracts. Version 2 is used instead of version 1 because of the usage of the smart contract language solidity, which offers much better support in terms of functionality than version 1 [24]. Another reason why version 2 is better to use as a reference is because the code base is well documented and hence is easier to explain and understand.

The smart contracts of Uniswap v2 are divided into two categories. The first category is the core contracts and the second category is the periphery contracts. This allows Uniswap to separate the core logic from the helper functions. The core logic consists of the logic involved in the creation and working of the exchange. The periphery contracts consist of the extra functionalities needed by the traders other than the exchange logic. In the core contracts, the two main contracts are the factory contract and the core contract.

The **factory contract** is responsible for the creation of new liquidity pools. Each new pool is unique and every pair will have a unique liquidity pool. Each time a user wants to create a new liquidity pool, the factory contract creates a pair contract for that liquidity pool. It is also responsible for setting the fee to the liquidity providers and optionally, to the protocol.

The **pair contract** will house the functions that deal with the pricing logic, which is the logic for the exchange of security tokens with reserve currency tokens. The contract also has functions for minting and burning LP tokens. LP tokens represent the ownership share of the LPs. The contract's mint function takes care of creating and distributing LP tokens. The burn function houses the logic to send the LP tokens back to the liquidity pool to claim the rewards for contributing liquidity.

The above-mentioned core contracts are the main reference contracts used in the current work, as the work only deals with the exchange logic. The proposed model for the decentralized stock exchange will be explained in the next section.

Exchange Model

The two assets that will be traded in the exchange will be the security token and reserve currency. The workings of these assets are as follows.

Figure 5 depicts the creation of liquidity pools for different security tokens. Each pool will have a unique security token and reserve currency with predetermined ratios. The reserve currency will be common to all the pools. When a LP wishes to create a new pool, the factory contract creates a new pair contract for that particular pair.

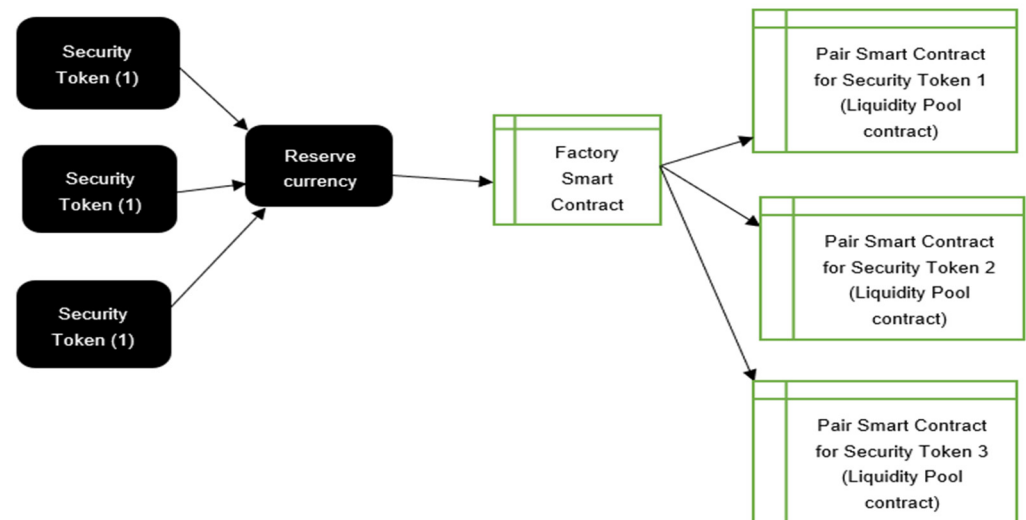


Figure 5. Creation of liquidity pools for different security tokens.

Figure 5 also gives a broad overview of how the process of making exchanges for every pair works. Each of these exchanges will be a market for that asset pair. Whenever an LP wants to give liquidity for a security token, if the liquidity pool does not exist, then the factory smart contract will create the pool, and the proportional amount of LP tokens is given to the liquidity providers, as seen in Figure 6.

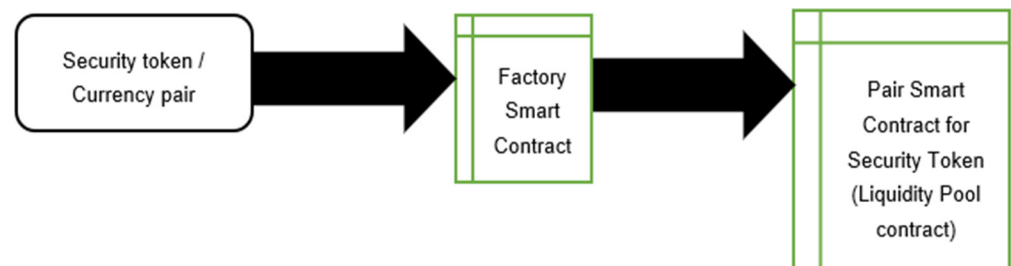


Figure 6. Functionality of tokens contribution to the pool and proportional amount of LP tokens are given to the liquidity providers if liquidity pool does not exist.

Figure 7 shows that when a liquidity pool for a security token/currency pair already exists, tokens are contributed to the pool and the proportional amount of LP tokens is given to the liquidity providers. The factory smart contract contains functionalities for handling the fees that the LPs will earn for creating or contributing to the pool. The fee will be a small percentage of each trade that is executed by the liquidity pool. When a trader wants to trade a particular stock, he/she will interact directly with the liquidity pool that has that stock.



Figure 7. Functionality of tokens contribution to the pool and proportional amount of LP tokens are given to the liquidity providers if liquidity pool exists.

5. Results and Performance Analysis

5.1. Performance Analysis of the Consenses Protocol

This section presents the investigations into the performance of the proposed stock exchange framework in a dynamic and heterogeneous computing environment. The authors conducted numerous tests to evaluate the effectiveness of the proposed methodology using various metrics. Three different blockchain platforms were used in the evaluations to compare their performance.

As a recent and well-established platform, proof of work (PoW) was chosen as the parent source for comparison. Proof of stake (PoS) was also utilized as a benchmark for subsequent high-throughput research deployment on blockchain computing systems. The evaluations were carried out on one of the public test networks, which are typically used for such purposes. The performance of the proposed methodology was evaluated on this along with other blockchain platforms. The authors used various metrics, such as throughput, latency, and scalability, to assess the performance of the different platforms. The results of the evaluations were analyzed and compared to identify the strengths and weaknesses of each platform.

Table 3 describes an evaluation that was conducted to compare the performance of a proposed blockchain framework with existing blockchain techniques, such as PoW and PoS. The evaluation used a virtual environment that mimicked a test network and hardware resources such as an Intel Core i5 CPU, 8 GB of RAM, and 1 TB of storage to ensure a fair comparison.

Table 3. Performance comparison of various consensus mechanisms.

Consensus Algorithm	PoW	PoS	Highway Protocol
Block creation	Block creation	Block creation	Block creation
Security issues	Security issues	Security issues	Security issues
Energy consumption	Very high	High	Low
Transaction per second	7–30	30–175	100–2500
Reliability	High	Low	Low

The evaluation presented in Table 3 compares the effectiveness of the proposed highway protocol with a flexible finality mechanism to the current blockchain consensus mechanisms of PoW and PoS. The results indicate that the proposed approach offers a significant improvement in the transaction processing speed, security, and energy efficiency of these traditional methods.

Specifically, the proposed approach achieved a transaction rate that was 2.2 times higher than PoS and 12 times higher than PoW. This improvement in the transaction rate is attributed to the flexible finality-based consensus mechanism, which enables a more efficient confirmation process and reduces the time required for blocks to be validated and added to the blockchain. Furthermore, the flexible finality condition-based consensus method reduces the energy consumption required to validate blocks and maintain the

blockchain network, which is a significant advantage compared to traditional consensus mechanisms such as PoW.

5.2. Performance Analysis Protocol of Centralized (CEXs) and Decentralized (DEXs) Market Makers

CEXs and DEXs use two completely different infrastructures, making it hard to compare which system is more efficient. The amount of literature analyzing the performance between the two is small in numbers. The paper by Andrea Barbon and Angelo Ranaldo tries to explore some metrics that can help understand these markets better [25]. The researchers have used a unique and representative dataset to analyze the centralized and decentralized cryptocurrency markets.

The researchers have taken trading volume data from three centralized exchanges, namely Binance, Kraken, and Coinbase, and compared them graphically. As shown in Figure 8, the trading data spans from the time period of July 2020 to around January 2021. These centralized exchanges use the Limit Order Book (LOB) mechanism to execute trade orders.

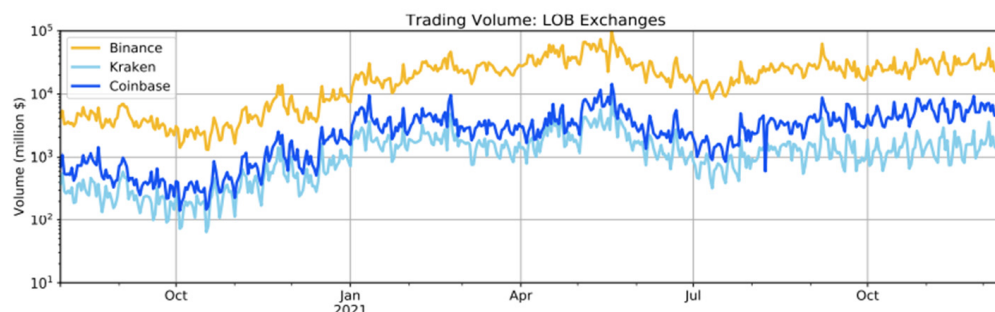


Figure 8. Graph showing the CEXs and DEXs trading data, spanning from the time period of July of 2020 to January of 2021.

Figure 9 shows the comparison made by them between the trading volumes of AMM-based DEXs [25]. The exchanges taken under consideration in the paper are Uniswap, Sushiswap, and Pancakeswap. The time period between when the data was taken is the same as its centralized counterpart. The results obtained when the trading volume between the centralized LOB exchange and the decentralized AMM-based exchange (Uniswap) was compared side by side for the same time period are shown in Figure 10.

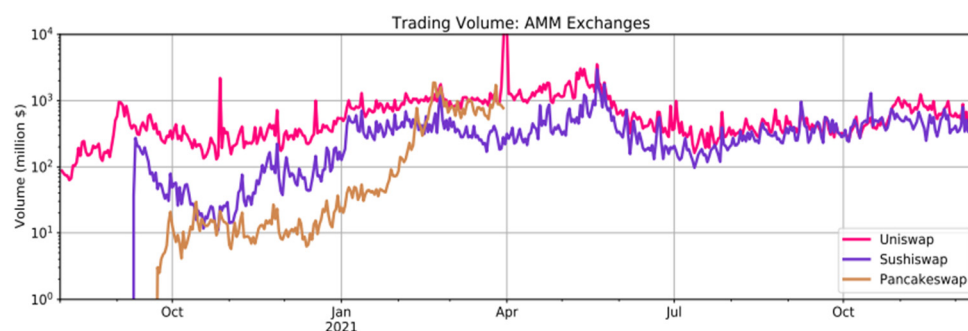


Figure 9. Graph showing the comparisons of trading volumes of CEXs and DEXs.

The results of this paper state that when it comes to overall performance, CEXs performed much better than DEXs, but DEXs also become competitive for transactions above USD 100,000. The paper also highlights how DEXs can give a greater competitive advantage if there is an increase in volume, provided there is a reduction in the blockchain transaction costs. As more and more blockchain systems are moving away from a proof-of-work consensus, this could soon become a possibility.

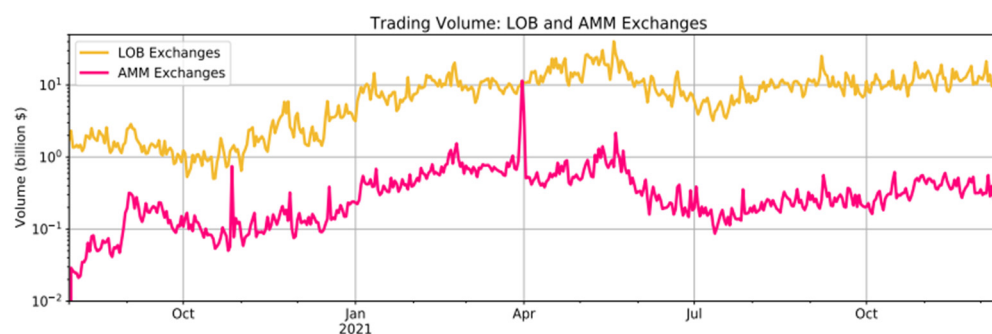


Figure 10. Graph showing the trading volume between centralized LOB exchange and decentralized AMM-based exchange.

6. Discussion

From the existing research, some major advantages of AMMs are described below:

- **Faster exchange:** In regular exchanges, the traders must wait until their offers are accepted by a counterpart for their trade to be executed. If a counter offer is not available, then the trade may not go through. AMMs allow for an exchange to occur immediately as the pools with reserves are readily available for trade, and there is no need to wait for order matching, which makes it perfect for markets with both high and low liquidity.
- **AMMs for price discovery:** AMMs can act as source of price discovery, as the prices shown by AMMs are usually a reflection of the original prices of the asset outside the exchange because of the action of arbitrageurs.
- **Path independence:** In regular exchanges, the path taken while placing the order heavily affects the price at which the asset is bought or sold. This is because some participants who have access to the order sequence use the information against uninformed participants to trade against them.

AMMs are path independent, i.e., the path taken while placing the order is the same for all participants, as there is only one path for placing AMM orders. There is complete transparency of the order sequence, as all the participants can see every transaction that is being made while avoiding the information asymmetry problem. In regular exchanges, the participants strategize their trade sequences based on the current state of the market. In markets using AMMs, knowledge of the state of the exchange will not help, as the only factor deciding the prices is the quantity of the reserve of the asset in the AMM pool.

Along with the advantages, it is also important to look into some of the drawbacks of the technology. At the time that this paper was written, the numbers of AMM system failures recorded was very few, which makes it hard to quantify the exact amount of monetary loss that has occurred because of them. The literature in the area points toward three most prominent drawbacks of AMMs.

- The first major drawback is slippage. This refers to the property of prices to move against a trader's actions as the trader consumes the reserve: the larger the consumption, the greater the slippage. AMM trades sometimes face huge slippage costs, which must be incurred by the traders.
- Another major issue faced by AMMs is impermanent loss. This loss refers to the opportunity cost faced by the LPs when they have their assets locked in the reserves.
- The third biggest hurdle in the adoption of AMMs is the high gas prices charged for transaction settlement by the underlying blockchain consensus mechanisms. Most blockchains use proof-of-work algorithms, which are resource-intensive consensus mechanisms; hence, the higher the number of transactions, the higher the gas fees the participants end up paying.

As the technology has not been completely explored, there may be more unique financial risks than those discussed above. With more research in the area, AMMs could

soon become a strong contender for price discovery mechanisms in other areas as well. The existing performance analytics from the cryptocurrency market can be used to understand AMMs to a certain extent, but there is a strong need for more research on these technologies to understand their use for the exchange of assets such as stocks.

7. Conclusions

Automated market makers (AMMs) have indeed been a significant innovation in the field of market making, and their potential to trade other assets beyond cryptocurrencies is an area of active research. The decentralized nature of blockchain technology has created new opportunities for the decentralization of marketplaces, and the use of consensus mechanisms, such as the highway protocol, can enhance the security and privacy of massive data storage. As a way to demonstrate the high level of scalability and mobility of our framework and reduce traffic overheads, we employed baseline models to assess the security requirements of the new user device. We conducted a performance of our proposed framework to confirm its effectiveness and identify areas that require improvement in subsequent studies. The technology has given investors a sense of security and trust in their transactions. Blending this technology along with traditional financial institutions, such as the stock exchange, would be a huge undertaking, especially because of the lack of regulations and understanding of the technology among the authorities.

The use of AMMs in traditional stocks is still relatively new and has several research implications, including liquidity provision, price discovery, risk management, regulatory implications, and adoption and integration challenges. Further research can help to better understand the potential benefits and drawbacks of using AMMs in traditional stock exchanges and their impact on market efficiency and stability. This work, along with several others, aims to act as a reference for all future developments that happen in this area.

Author Contributions: Conceptualization, R.D.; investigation and methodology, writing—review and editing, R.K.R.; data curation, K.R.N.S.; resources, B.K.; supervision, S.S.; visualization, M.A.; validation, S.F.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work did not receive any funding, directly or indirectly, from any source or agency.

Data Availability Statement: Not applicable.

Acknowledgments: We are grateful to the Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte, for providing the resources for this research. We are thankful to Nitte University for their motivation. We would also like to thank the editor and reviewers for their time and consideration.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jiang, C.; Liang, K.; Chen, H.; Ding, Y. Analyzing market performance via 835 social media: A case study of a banking industry crisis. *Sci. China Inf. Sci.* **2014**, *57*, 1–18.
2. Li, Q.; Chen, Y.; Wang, J.; Chen, Y.; Chen, H. Web Media and Stock Markets: A Survey and Future Directions from a Big Data Perspective. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 381–399. [\[CrossRef\]](#)
3. Yang, Y. The Measure of Liquidity in Futures Market. In Proceedings of the 2006 IEEE International Conference on Management of Innovation and Technology, Singapore, 21–23 June 2006; pp. 320–324. [\[CrossRef\]](#)
4. Kajtazi, M. Information asymmetry in the digital economy. In Proceedings of the 2010 International Conference on Information Society, London, UK, 28–30 June 2010; pp. 135–142. [\[CrossRef\]](#)
5. Dhillon, V.; Metcalf, D.; Hooper, M. *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You*, 1st ed.; Apress: New York, NY, USA, 2017.
6. Soltani, R.; Zaman, M.; Joshi, R.; Sampalli, S. Distributed Ledger Technologies and Their Applications: A Review. *Appl. Sci.* **2022**, *12*, 7898. [\[CrossRef\]](#)
7. Alkafaji, B.K.A.; Dashtbayaz, M.L.; Salehi, M. The Impact of Blockchain on the Quality of Accounting Information: An Iraqi Case Study. *Risks* **2023**, *11*, 58. [\[CrossRef\]](#)
8. Buterin, V. A Next Generation Smart Contract and Decentralized Application Platform. 2013. Available online: www.theblockchain.com/docs/Ethereum-white-paper-a-nextgeneration-smartcontract-anddecentralized-application-platform-vitalik-buterin.pdf (accessed on 1 September 2022).

9. Conte de Leon, D.; Stalick, A.Q.; Jillepalli, A.A.; Haney, M.A.; Sheldon, F.T. Blockchain: Properties and misconceptions. *Asia Pac. J. Innov. Entrep.* **2017**, *11*, 286–300. [CrossRef]
10. Mahdi, S.; Mehdi, B.; Mohammad, A. Structural shocks in monetary policy, exchange rates, and stock prices using SVAR in Iran. *Int. J. Islam. Middle East. Financ. Manag.* **2021**; ahead-of-print. [CrossRef]
11. Zheng, G.; Gao, L.; Huang, L.; Guan, J. *Ethereum Smart Contract Development in Solidity*; Springer: Berlin/Heidelberg, Germany, 2021.
12. Lin, L.X. Deconstructing Decentralized Exchanges. *Stanf. J. Blockchain Law Policy* **2019**, *2*, 58–77.
13. Mohan, V. Automated market makers and decentralized exchanges: A DeFi primer. *Financ. Innov.* **2022**, *8*, 20. [CrossRef]
14. Adams, H.; Zinsmeister, N.; Robinson, D. *Uniswap V2 Core*; Uniswap: New York, NY, USA, 2020.
15. Alex, P.; Tiruvilumala, N. Mixing Constant Sum and Constant Product Market Makers. *arXiv* **2022**, arXiv:2203.12123.
16. Yuliya, G. A Conceptual Framework for Digital-Asset Securities: Tokens and Coins as Debt and Equity. *Md. Law Rev.* **2020**, *80*, 166.
17. Dossa, A.; Ruiz, P.; Vogelsteller, F.; Gosselin, S. Security Token Standard. Available online: <https://github.com/ethereum/eips/issues/1411> (accessed on 23 September 2022).
18. Bahga, A.; Madiseti, V.K. Blockchain Platform for Industrial Internet of Things. *J. Softw. Eng. Appl.* **2016**, *9*, 533–546. [CrossRef]
19. Christian, S.; Bernd, S.; Martin, S. Prediction Market Performance and Market Liquidity: A Comparison of Automated Market Makers. *IEEE Trans. Eng. Manag.* **2013**, *60*, 169–185. Available online: <https://ssrn.com/abstract=2476333> (accessed on 16 January 2023).
20. Abhishek, G.; Mohanta, B.K.; Mohapatra, H.; Al-Turjman, F.; Altrjman, C.; Yadav, A. A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Appl. Sci.* **2023**, *13*, 2604. [CrossRef]
21. Schwarz-Schilling, C.; Neu, J.; Monnot, B.; Asgaonkar, A.; Tas, E.N.; Tse, D. Three Attacks on Proof-of-Stake Ethereum. In *Financial Cryptography and Data Security FC 2022*; Eyal, I., Garay, J., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13411. [CrossRef]
22. Jiao, J.; Lin, S.W.; Sun, J. A Generalized Formal Semantic Framework for Smart Contracts. In *Fundamental Approaches to Software Engineering FASE 2020*; Wehrheim, H., Cabot, J., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2020; Volume 12076. [CrossRef]
23. Zinsmeister, N.; Robinson, D.; Adams, H.; Salem, M.; Chriseth; Jepsen, W. Uniswap v2 Core Contracts. Available online: <https://github.com/Uniswap/v2-core> (accessed on 13 October 2022).
24. Zinsmeister, N.; Salem, M.; Bukov, A.; Adams, H. Uniswap v2 Periphery Contracts. Available online: <https://github.com/Uniswap/v2-periphery> (accessed on 13 October 2022).
25. Sedlmeir, J.; Lautenschlager, J.; Fridgen, G.; Urbach, N. The transparency challenge of blockchain in organizations. *Electron. Mark.* **2022**, *32*, 1779–1794. [CrossRef] [PubMed]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.