Coin Drop—A Decentralised Exchange Platform

Vanita Jain, Akanshu Raj, Abhishek Tanwar, Mridul Khurana, and Achin Jain

Abstract In today's world, cryptocurrency has seen a boom in users' number, and the numbers are increasing day by day. There are multiple cryptocurrencies, so there must be a platform to provide an exchange of cryptocurrencies. These days, many platforms provide users with the service, but they lack speed and are limited to some cryptocurrencies. Thus, we have proposed and developed a system that will increase the transactions rate by performing it off-chain to increase the transactions' speed and perform exchange between any cryptocurrencies. The proposed system combines the best practices of both the decentralised and centralised exchange platforms.

Keywords Cryptocurrency · Centralised cryptoexchanges · Decentralised exchange · Blockchain · Ethereum · Smart contract

1 Introduction

A cryptocurrency [1] is a form of currency available only virtually and is protected using various cryptography techniques. Researchers and developers proposed it in the early 1980's giving hints of the systems having digital money. Cryptocurrency is a term that refers to a digital asset of a network that does all the money-related work using that cryptocurrency, and the network is distributed across a large number of computers. Thus, the network is considered to have a decentralised structure with no single authority having all the power.

We can also consider cryptocurrencies as the systems that allow users to make online payments securely [2]. These payments are denominated in terms of virtual

V. Jain (✉) · A. Raj · A. Tanwar · M. Khurana · A. Jain
Bharati Vidyapeeth's College of Engineering, New Delhi, India
e-mail: vanita.jain@bharatividyapeeth.edu

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_33

"tokens", which are represented by ledger entries internal to the system. "Crypto" refers to the various encryption algorithms and cryptographic techniques that safeguard these entries, such as elliptical curve encryption, public–private key pairs and hashing functions [3].

In today's world, there are thousands of cryptocurrencies with various functions and specifications. Some of these cryptocurrencies are clones or forks of popular cryptocurrencies like bitcoin and Ethereum, and also, some new currencies are built from scratch. Some popular cryptocurrencies apart from bitcoin [4] and Ether [5] include Litecoin [6], Peercoin, Namecoin [7] and Cardano [8]. The total estimated value of the cryptocurrencies in existence can be around $214 billion [9].

However, there are several risks involved while using cryptocurrencies. The actual value as currency is effective $0, so the only store of value is in other utility for a distributed trustless public append-only ledger [10]. Since the government does not monitor cryptocurrency, this creates a massive security risk as the criminals could use unmonitored money [11]. The private key protects the cryptocurrencies wallet, and once someone gets hold of the private key of the user, he can move the money from one account to another, and since the cryptocurrency is not monitored by the government or any central authority (in the case of decentralised exchange platforms), the owner cannot even file a report [12].

We already know that there are multiple cryptocurrencies globally, then there must be a system to allow trading between these currencies; this leads to the introduction of decentralised exchange platforms. Decentralised exchange (DEX) platforms provide the users of cryptocurrencies with a platform to perform cryptocurrency exchange. It allows users to have direct peer-to-peer cryptocurrency transactions online securely and without the need for any intermediary authority. Some of the famous DEX platforms are AirSwap, Atomex, Bancor and dex.blue [13].

However, these systems have some drawbacks in terms of speed, and they are also limited to the number of cryptocurrencies they can take into consideration in their respective platforms; these issues are discussed later in this paper, and a solution to overcome all those shortcomings is proposed.

The proposed system (coin drop) is comparatively much faster than the already present decentralised systems and can work with almost all kinds of cryptocurrencies available. In Section II of this paper, we have discussed cryptographic networks, their working, and the different types of wallets. In Section III, we have discussed the cryptocurrencies exchange platforms. Section IV discusses the working and architecture of "coin drop". Section V holds the results obtained by comparing various cryptographic exchange platforms against the proposed system. In Section VI, we have concluded the paper.

2 Cryptonetworks and Wallets in Today's World

2.1 Cryptographic Networks

To create a network that uses cryptocurrency for online payments, we need to work with blockchain [14]. This technology can be used to keep track of all the transactions that have taken place ever been in a ledger. Blockchain provides the developers with a way to create a structure of the ledger that is to be stored. It is made sure that the structure is secure. This structure is then shared with the entire network, individual nodes or computer maintaining a ledger copy. When a majority of nodes in the network are in favour of the structure, then only the structure is established in the network. A set of transactions is forged into a new block verified by each node of the network. If the nodes confirm the block, then only the block is added to the chain. Thus, this process makes it almost impossible for the mishappenings of the transaction histories. The main goals of such a network are to allow members of the network to synchronise their view of the system state and then to disseminate peer information to allow peers to reenter the system after a disconnection [15].

One such network is the bitcoin network [16]. Bitcoin is a cryptocurrency created in January 2009 after the housing market crash. Bitcoin follows the ideas that are set out in a whitepaper by the mysterious and pseudonymous Satoshi Nakamoto. Bitcoin uses the blockchain network that keeps balances and maintains a public ledger that everyone has transparent access to; all bitcoin transactions are verified by a massive amount of computing power [17].

2.2 Hot and Cold Wallets

These cryptocurrencies are stored in digital wallets. There are two types of digital wallets: hot wallet and cold wallet [18].

A wallet that is connected to the network is referred to as hot wallet. They are generally easy to set up, access and be given more tokens. Hot wallets can hold any cryptocurrencies. These wallets are mainly for everyday cryptocurrency users. Nevertheless, they are open to hackers and other technical vulnerabilities because they are connected to the Internet. Some examples of hot wallets are Coinbase and Blockchain.info.

Any wallet which is not connected to the cryptographic network is termed as cold wallet. They are more secure than hot wallets, but they do not accept as many cryptocurrencies when compared to hot wallets. Cold wallets are mainly designed devices that are designated physical cryptocurrency storage. One of the main advantages these wallets provide is that we can have our cryptos beside us. They are expensive to buy, while hot wallets are free of cost and easy to access. Some examples of cold storage devices are Trezor and Ledger [19, 20].

3 Cryptocurrency Exchange Platforms

3.1 Centralised Cryptoexchanges

They are trading platforms like the stock market, where a company or a third party has total control over all the transactions made by both parties. In centralised cryptoexchanges [21], the user has to trust the third party because they do not have access to the private keys of exchange account wallets. Trust is the main factor in centralised exchange platforms. All the transactions are controlled by third parties, which could lead to hacks in these platforms or malicious activities by the service providers. Centralised exchange platforms have their system's off-chain. The transactions are not handled by the blockchain, due to which it is prone to security breaches and other attacks on the systems. Today most of the platforms are centralised, which run on high regulatory risk. Some famous CCEs are Binance, Bittrex, Bitfinex, Coinbase and Kraken.

None of the centralised cryptoplatforms is immune to hacks. More than 30 cryptocurrency exchange hacks have occurred in the last nine years, for example, MTGox, BitGrail, and Coincheck. Some government bodies have also banned CCEs in recent years. China, South Korea and Russia are among them. Using CCEs often comes with a large amount of risk, the user has to provide sensitive information about themselves, including bank details, address and govt. issued ID as well [22].

3.2 Decentralised Cryptocurrency Exchanges

Decentralised cryptocurrency exchanges overcome many disadvantages of the centralised structure as it operates on a peer-to-peer marketplace directly on the blockchain. Using this way, the traders do not have to reveal their sensitive information to a third party. Since it works on blockchain, it is less immune to security attacks, unlike centralised cryptoexchanges. Still, most of the platforms have a centralised structure because building decentralised exchange platforms is complicated and too costly. Currently, most of the platforms do not have the liquidity to compete with centralised cryptoexchanges.

Decentralised cryptocurrency exchanges operate on a peer-to-peer network because their nodes are distributed; they experience a lower risk of attacks compared to centralised cryptoexchanges [13]. There is no involvement of a third party in DEX which will have control over all the transactions. They are less prone to security attacks and malicious activities by service providers. In DEX, all the payments use cryptocurrencies. DEX enables users to remain in control of their funds by operating essential functions over the blockchain. It overcomes the centralised structure's main limitation since there is no point of failure in this exchange, making blockchain a powerful technology. There are many through backs and

inefficiencies in a centralised structure, due to which there is an introduction of many semi-decentralised exchanges which are coming into action. These are models that operate between the centralised and decentralised marketplace, which are highly efficient than centralised ones. CCEs lack security, transparency and efficiency, due to which demand for decentralised exchanges has increased. DEX promises two significant advantages: security control and the global marketplace. EtherDelta is one of the oldest projects in this field. It has a simple user interface and basic trading features. It has already gained sufficient attraction in the market. Some of the popular DEX are Wavesdex, Bancor protocol, Kyber Network, EtherDelta and Airswap.

4 Proposed System and Working

We have proposed a system that provides decentralised cryptocurrency exchange facilities using blockchain, which is merged with an interactive, user-friendly interface created using ReactJS. The proposed system is much faster than the traditional methods used and combines the best features from both the centralised and the decentralised exchange platforms. The working of the whole system is explained in great detail. Figure 1 shows the workflow of the system.

The trader interacts with the interface (web app in the diagram). The smart contract that we have to build is deployed on Ethereum blockchain and connected with the front end. For testing purpose, we have deployed a contract on the Rinkeby network and used injected web3 environment.

First of all, the user deposits the quote currency in the wallet provided in the exchange and any other token listed on the exchange. Figure 2 shows the wallet that a user will use.

Coin drop has two types of orders: one is market orders and the other one is limit orders. Market orders are filled immediately, irrespective of the price of the token.

To create a market order, there is a function in the smart contract called createMarketOrder that takes the ticker, amount of the token, and the side of the order book. For selling tokens, we can identify if the seller has enough tokens, but while buying market order, we cannot determine the price at which the market order will be fulfilled because one order can have several trades under it, i.e. market orders can be fulfilled partially as per availability in the order book. It is also checked whether the token for which the order is being created exists or not.

In the case of limit orders, there is a function called createLimitOrder that is used to create a new order in the order book. It takes ticker, amount, price of the token and side to place the order. It is checked that the token exists for which the order is being placed, and the token is not quoted currency. The cost to buy/sell one token is specified and is only filled if matching order is found in the counter order book, i.e. if a user wants to sell tokens using limit order, the order can only be filled if there is a matching order to buy.

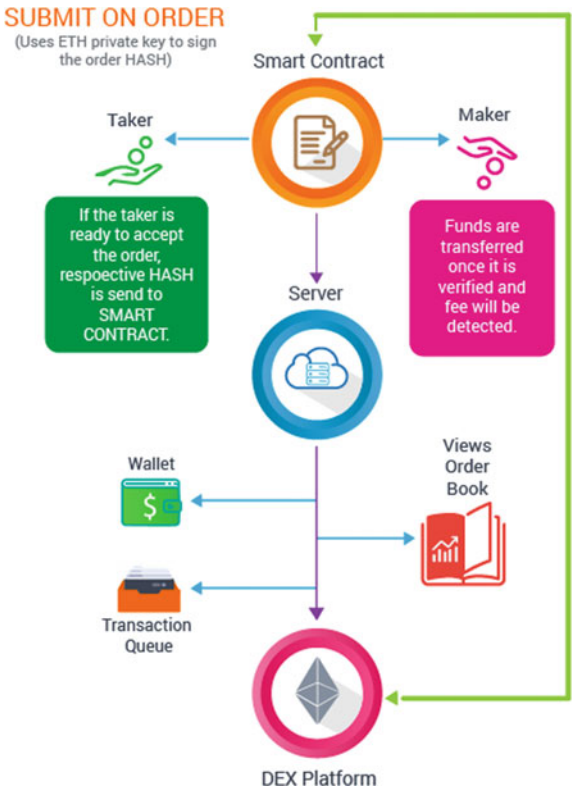

Fig. 1 Flow chart of the system

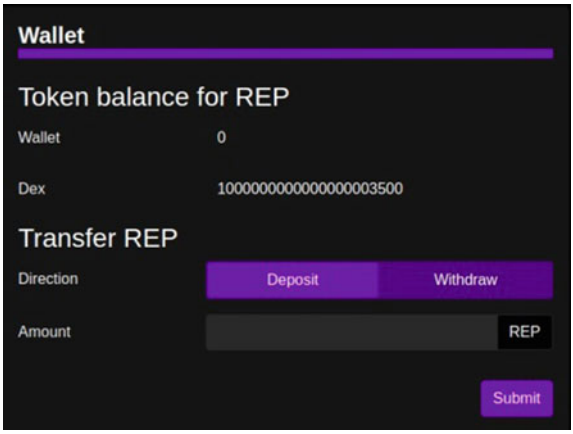

Fig. 2 User wallet in the coin drop

The getOrders function in the smart contract is used to list all the current orders from both sides of the order book, i.e. from the sell-side and buy-side. A getTokens function is used to list all the tokens purchased or sold on the exchange. It returns an array of tokens. The addToken process in the smart contract is used to record a

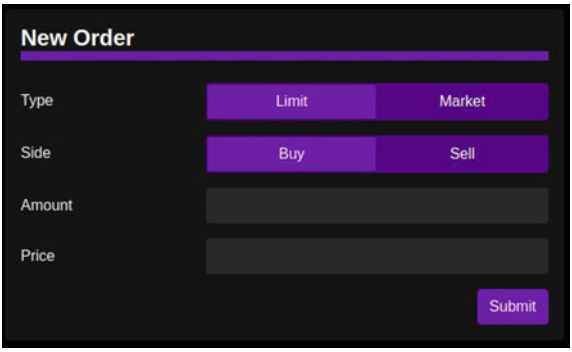

Fig. 3 New order function

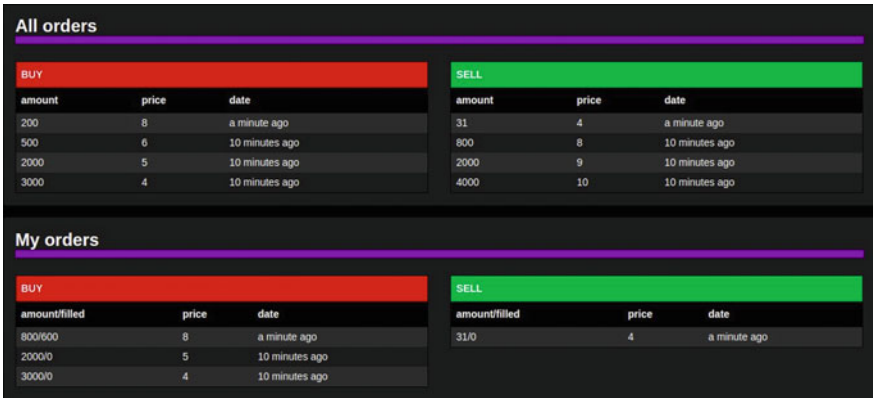

Fig. 4 Orders placed on the coin drop platform

new token on the exchange. It takes token address and ticker (symbol) as an argument. The admin of exchange can only call this function. The Deposit function is used to deposit tokens into the exchange, and the Withdraw function is used to withdraw the tokens from the exchange into external wallets.

DAI token is used as quote currency using which any listed token can be purchased or sold for DAI. DAI is used because it is a stable coin and its value always remains close to $1.

Figure 3 shows the function where a user can place new orders.

Figure 4 shows all the orders placed on the platform by the users worldwide and the orders that a particular user places on the coin drop platform in my orders' section.

Characteristics	Centralized Exchange Platforms	Decentralized Exchange Platforms	Coin Drop (Proposed System)
Control	platform has the most control	User has the most control	User has the most control
Security	Risk of Hackers	No chance of hacking	No chance of hacking
Transaction Fees	Charges fees for using the platform	Charges zero or very minimal fees	Charges zero fees
Type of Transactions	On-Chain	On-chain	Off-chain
Number of Currencies	2-5	2-5	Almost all
Liquidity	High Liquidity	Low Liquidity	High Liquidity
Speed	Executes orders in milliseconds	Can take up to an hour to execute orders	Executes orders in milliseconds

Fig. 5 Comparison of centralised exchange [13–15], decentralised exchange [13, 14, 22] and coin drop

5 Result

From the proposed system stated in the paper, we found that the decentralised platform that is proposed and created has the control in the hands of users and is less prone to attack by the malicious users as compared to the centralised exchanges as the amounts in the personal wallets are comparatively less when compared to the centralised banks. The proposed system aims to take no amount to create or validate a transaction, and the transactions are performed off-chain, which increases the speed of transactions. The proposed system can handle any cryptocurrencies using DAI token, a stable currency form, as an intermediatory currency when exchanging between two currencies. Thus, all these points were taken into consideration, and a comparison of current centralised and decentralised exchange platforms with the system proposed in the paper is shown in Fig. 5.

6 Conclusion

The cryptocurrency users have increased, and so the worth of cryptocurrencies. Many platforms provide cryptoexchanges services, but they have certain limitations, and they work with a few cryptocurrencies. We have developed and proposed a system that increases the cryptographic transactions' speed as they are done in the off-chain. The coin drop system can handle exchange between any cryptocurrencies. Thus, the developed system provides a better approach and takes the right parts of both the centralised and decentralised systems.

References

1. Farell, R.: An analysis of the cryptocurrency industry (2015)
2. Peters, G., Panayi, E., Chapelle, A.: Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective. J. Financ. Perspect. **3**(3) (2015)
3. Bucko, J., Pal'ova, D., Vejacka, M.: Security and trust in ´ cryptocurrencies. In: Central European Conference in Finance and Economics, pp. 14–24 (2015)
4. Bohme, R., Christin, N., Edelman, B., Moore, T.: Bit- ¨ coin: Economics, technology, and governance. J Econ. Perspect. **29**(2), 213–238 (2015)
5. Bouoiyour, J., Selmi, R.: Ether: Bitcoin's competitor or ally? arXiv preprint arXiv:1707.07977 (2017)
6. Reed, J.: Litecoin: an introduction to litecoin cryptocurrency and litecoin mining (2017)
7. Gkillas, K., Bekiros, S., Siriopoulos, C.: Extreme correlation in cryptocurrency markets. Available at SSRN 3180934 (2018)
8. Guides, T.S.: Why cardano ada deserves your attention—cardano cryptocurrency strategy (2018)
9. Wei, W.C.: Liquidity and market efficiency in cryptocurrencies. Econ. Lett. **168**, 21–24 (2018)
10. Liu, Y., Tsyvinski, A., Wu, X.: Common risk factors in cryptocurrency. National Bureau of Economic Research, Technical Report (2019)
11. Barone, R., Masciandaro, D.: Cryptocurrency or usury? Crime and alternative money laundering techniques. Eur. J. Law Econ. **47**(2), 233–254 (2019)
12. Twomey, D., Mann, A.: Fraud and manipulation within cryptocurrency markets. In: Alexander, C., Cumming, D. (eds.) Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation, pp. 205–250 (2020)
13. Lin, L.X.: Deconstructing decentralised exchanges. Stanf J Blockchain Law Policy, **2** (2019)
14. Scott, B.: How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? UNRISD Working Paper, Technical Report (2016)
15. Bashir, I.: Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained. Packt Publishing Ltd (2018)
16. Velde, F., et al.: Bitcoin: A primer (2013)
17. Nakamoto, S.: Bitcoin whitepaper (2008). https://bitcoin.org/bitcoin.pdf (17.07. 2019)
18. Khan, A.G., Zahid, A.H., Hussain, M., Riaz, U.: Security of cryptocurrency using hardware wallet and qr code. In: 2019 International Conference on Innovative Computing (ICIC). IEEE, pp. 1–10 (2019)
19. Das, P., Faust, S., Loss, J.: A formal treatment of deterministic wallets. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 651–668 (2019)
20. Jasem, F.M., Sagheer, A.M., Awad, A.M.: Enhancement of digital signature algorithm in bitcoin wallet. Bull. Electr. Eng. Inf. **10**(1), 449–457 (2021)
21. Bacon, J., Michels, J.D., Millard, C., Singh, J.: Blockchain demystified: a technical and legal introduction to distributed and centralised ledgers. Rich. JL Tech. **25**, 1 (2018)
22. Pop, C., Pop, C., Marcel, A., Vesa, A., Petrican, T., Cioara, T., Anghel, I., Salomie, I.: Decentralizing the stock exchange using blockchain an ethereum-based implementation of the bucharest stock exchange. In: 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing (ICCP). IEEE, pp. 459–466 (2018)