International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Decentralized Cryptocurrency Exchange Using Blockchain

[1]MOHAMMED SIDDIQ PAPA F [2]KAMALAKANNAN.M, [3]KABIN.F, [4]DR M. ANAND

[1,2,3] IV Year B Tech CSE Students, Dept of Computer Science and Engineering, DR MGR EDUCATIONAL AND RESEARCHINSTITUTE,Maduravoyal, Chennai-95, Tamil Nadu, India

[4]Additional HOD Department of CSE, Dept of Computer Science and Engineering, DR MGR EDUCATIONAL AND RESEARCH INSTITUTE,Maduravoyal, Chennai-95, Tamil Nadu, India

Abstract-- In today's technology-driven world, ensuring robust security is of paramount importance. Blockchain technology has emerged as a pivotal solution, eliminating intermediaries andfortifying security measures. Cryptocurrencies represent the pioneering digital assets successfully managed through blockchain, attracting financial institutions to integrate them intotheir portfolios, fostering widespread adoption and interest among various stakeholders, including the banking sector, government, and individual investors. The potential for cryptocurrencies to evolve into the global currency of the future, supplanting fiat currency, is an intriguing possibility. This research project aims to offer a comprehensive insight into the cryptocurrency market, encompassing its origins, core characteristics, price dynamics, market capitalization, and trading volumes. Additionally, it will delve into critical concepts such as Ethereum, smart contracts, tokens, and consensus algorithms, which are instrumental to the cryptocurrency market's functioning

Keywords: Blockchain, Cryptocurrencies, Ethereum, Smart Contracts, Token, ConsensusAlgorithm.

I. INTRODUCTION

The surge in decentralized blockchain networks, such as Ethereum, has presented exciting opportunities in the finance industry, particularly with the development of decentralized exchanges (DEXs). These platforms give users the ability to directly trade cryptocurrencies and digital assets without the need for intermediaries or centralized authorities, empowering them in the process. This differs significantly from traditional centralized exchanges, in which a single company has authority over the exchange and users must trust their funds with that company. Within the world of decentralized exchanges, traders have more freedom to conduct their transactions, and transparency is a crucial characteristic. Utilizing public blockchains to document and authenticate transactions guarantees that the transfer of assets is fully transparent and readily auditable, ensuring fairness in the process of exchange. Decentralized exchanges represent a new era in trading, allowing users to conduct peer-to-peer transactions without relying on intermediaries or third-party entities. DApps, short for decentralized crypto applications, are a groundbreaking concept in the fields of technology and finance. These apps utilize blockchain technology to develop software systems that can function without centralized control, intermediaries, or single points of failure. DApps harness the fundamental qualities of blockchain to provide transparency, security, and resistance to censorship, causing disruption in traditional industries and creating new opportunities for innovation and user empowerment.

DApps, or decentralized crypto applications, are a notable deviation from the usual centralized software. They are a type of software that operates on blockchain networks, which are distributed ledgers that store transactions across a network of computers. DApps are different from traditional apps because they don't rely on central servers and intermediaries, instead they are designed to operate in a trustless, decentralized manner.

II. OVERVIEW

An Ethereum-based decentralized token exchange cuts out the middlemen, allowing users to trade assets directly with one another. Thanks to smart contracts on the blockchain, trading is secure and automatic, removing the need for any third-party involvement. Since users keep control of their private keys, their security and ownership stay intact. This decentralization minimizes the risk of censorship and is accessible to everyone, offering individuals more financial independence. This fits perfectly with the wider goals of decentralized finance. In essence, it enables the straightforward swapping of assets, leveraging the automation and security features of blockchain technology.

III. LITERATURE REVIEW

Diving into a literature review feels like embarking on a treasure hunt through mountains of academic papers, research articles, and books, all focused on a specific

topic. It's about piecing together the puzzle of what's already known, identifying where opinions diverge or converge, and spotting the gaps where we can add new insights. The aim is to come away with a clear, evaluative picture of the current knowledge landscape in any given field.

When we turn our gaze to decentralized token exchanges built on blockchain technology, we're stepping into an area that's reshaping the world of finance right before our eyes. The exploration of Decentralized Finance (DeFi) is particularly riveting. It's a domain bursting with potential, promising to make finance more inclusive, spur innovation, cut out the middlemen, and secure transactions for good. This deep dive offers a window into how DeFi could turn the finance industry on its head.

The journey doesn't stop there. We also delve into the nuts and bolts of crypto trading, unraveling the complexities of platforms, strategies, trends, regulations, and the role of decentralized swaps in the broader DeFi ecosystem. The message is clear: there's a pressing need for more research to navigate the challenges and propel crypto trading into the future.

Our exploration extends to the mechanics of decentralized, trustless crypto exchanges. This segment spans the gamut from blockchain technology, types of exchanges, and smart contracts, to interoperability and security concerns. The call for further study is loud and clear, pointing out that for decentralized exchanges to flourish, we must address issues of scalability, ease of use, liquidity, and regulatory compliance.

One fascinating piece of research presents a blockchain-based decentralized marketplace designed to foster trustworthy trading in developing countries. This marketplace leverages blockchain for transparency, smart contracts for seamless operations, and a reputation system to build trust. It's a testament to the technology's versatility, offering support for multiple languages and local currencies to meet the needs of a diverse user base.

By undertaking a meticulous literature review in the realm of decentralized token exchanges, researchers can map the terrain of existing knowledge, pinpoint where further inquiry is needed, and uncover opportunities to innovate. This process is not just academic; it's a vital tool for guiding project development, tackling potential hurdles, and sparking further research and innovation in this thrilling field.

IV. EXISTING SYSTEM

The paper addresses the demerit of lack of interoperability between heterogeneous cryptocurrencies and CBDCs, proposing an interoperable architecture and decentralized P2P service model for seamless transfers.

It also enhances security by addressing identified threats through specified security requirements. Additionally, it introduces a lightweight software architecture for the NAGA platform, enabling cross- cryptocurrency payments, which can mitigate the mismatch issue between buyer and seller preferences, enhancing online purchase convenience

V. PROPOSED SYSTEM

To create a peer-to-peer platform for direct cryptocurrency trading, providing lower fees, increased privacy, and greater control over user's funds. This architecture enables cross-cryptocurrency payments, allowing buyers to pay in one currency while sellers receive a different cryptocurrency

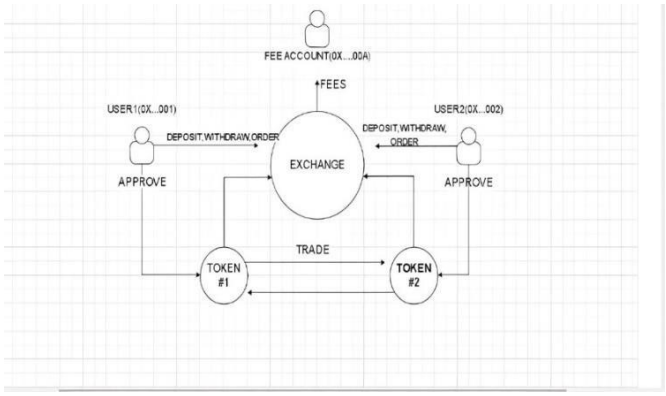

Figure 1. PROPOSED SYSTEM

VI. METHODOLOGY

Our strategy places a strong emphasis on creating a decentralized token exchange that operates on the Ethereum blockchain. In simpler terms, we're building a system where users have control and transactions are carried out directly on the Ethereum network.

For our project, we've introduced three types of tokens. The first one, Dapp, is designed specifically for our platform, making it unique to what we're building. The other two tokens, mEth and mDai, are based on well- established Ethereum tokens.

- Dapp Token: Think of the Dapp Token as the unique currency exclusive to your decentralized token exchange project. It's akin to having your own special coins for transactions within your platform

- mEth: Picture mEth as a digital representation of Ether, Ethereum's native cryptocurrency. It takes the form of a wrapped Ether (WETH) token, making it tradable on the Ethereum blockchain.

- mDai: Imagine mDai as a tokenized version of Dai, a stablecoin on the Ethereum blockchain. Similar to mEth, mDai is a wrapped token (WDai), making it suitable fortrading on decentralized exchanges.

In this lively environment, we've implemented a nifty feature – candlestick charts. Think of these charts as the heartbeat of the exchange, capturing the essence of trading activities over different time intervals. Each candlestick bar is like a snapshot of the market's mood, telling a story of price movements and overall sentiment.

So, as users explore the exchange, they're not just executing transactions – they're part of a thrilling narrative, where each candlestick tells a tale of market sentiment, trends, and opportunities. It's the art of trading brought to life, making the decentralized token exchange not just a platform but an experience where users can trade with confidence and insight.

A.ALGORITHM USED

Blockchain network - Consensus protocols

- Proof of work:

Proof-of-work (PoW) is a blockchain consensus mechanism that incentivizes network validation by rewarding miners for adding computational power anddifficulty to the network.

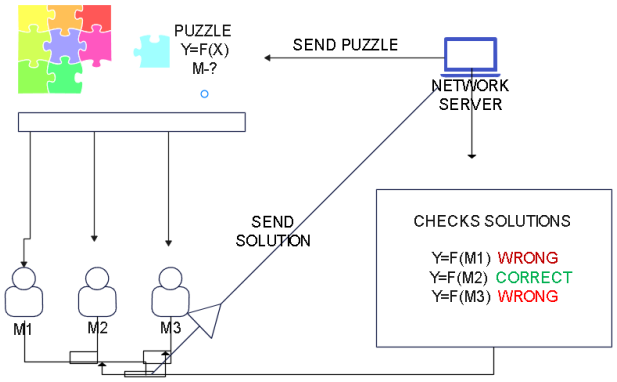

Figure 2. Working of proof of work

B. METAMASK

Using a Metamask wallet account, you can easily engage with the decentralized token exchange by linking your Metamask wallet to the exchange's user interface. This connection enables you to seamlessly buy, sell, and trade Dapp, mEth, and mDai tokens using the Ethereum stored in your Metamask wallet. Whenever you initiate a transaction on the exchange, it's essential to sign the transaction using your Metamask wallet. This signing process ensures a secure and decentralized authentication method for your transactions.

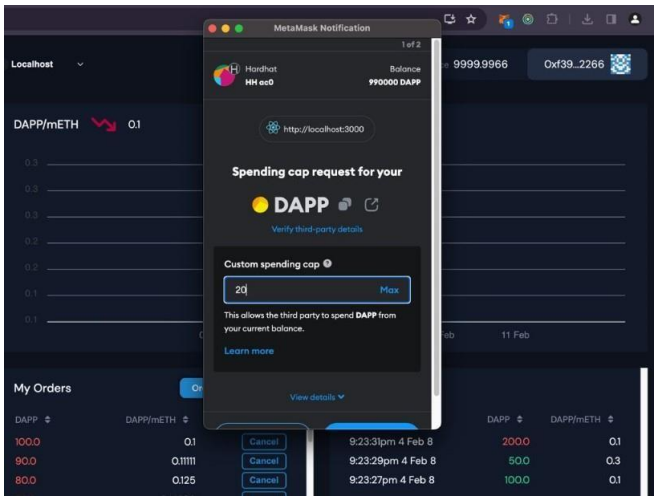

Figure 3. Metamask Interface

C.SMART CONTRACT

Smart contracts are essential in decentralized crypto exchange applications as they automate and enforce the execution of pre-established rules without requiring intermediaries.

Smart contracts allow for transactions to occur without the need for trust, as the exchange process is automated. Participants have the ability to exchange goods or services with one another without needing a central authority to facilitate the transaction.

When specific conditions are met, smart contracts will execute predetermined actions automatically. In a decentralized exchange, this might include automatically finalizing trades, transferring asset ownership, and allocating funds based on the agreed upon terms.

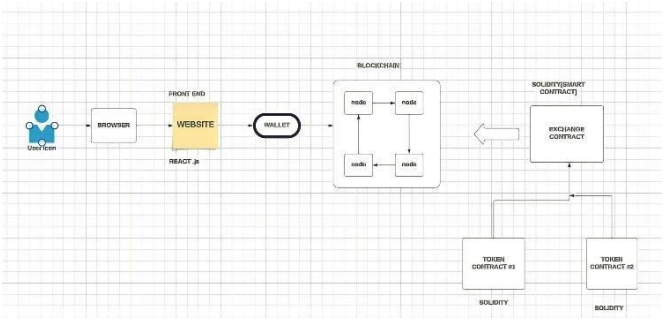

Figure 4. Working of Smart Contract

VII. APPROACH

Building a decentralized application (DApp) to change how people interact with blockchain technology. Here's a streamlined guide:

STEP 1: Gather Your Tools

Visual Studio Code where you'll write and edit.

- Solidity Smart Contracts Compiler (Remix IDE) and Hardhat to sculpt the backbone of your app with smart contracts.
- Node.js and React.js to breathe life into your creation, making it interactive and responsive.
- MetaMask and Redux to add depth and functionality, allowing users to connect their wallets and manage state across your app.

STEP 2: Create the Frontend

- Use HTML, CSS, and React.js to design your app's interface. This includes the homepage, browsing features, transaction validations, and token exchanges.

STEP 3: Connect to MetaMask Wallet

Now, you invite your audience into the world you've created. Users register and receive a unique public key from MetaMask, a bridge that connects them to your application through their web browsers. This integration allows for a seamless dance between users and your decentralized platform, enabling them to interact with your app as if it were magic.

```
[apple@MacBook-Pro ~ % cd blockchain-developer-bootcamp
[apple@MacBook-Pro blockchain-developer-bootcamp % npx hardhat test

  Exchange
    Deployment
      ✔ tracks the fee account
      ✔ tracks the fee percent
    Depositing Tokens
      Success
        ✔ tracks the token deposit
        ✔ emits a Deposit event
      Failure
        ✔ fails when no tokens are approved (67ms)
    Withdrawing Tokens
      Success
        ✔ withdraws token funds
        ✔ emits a Withdraw event
      Failure
        ✔ fails for insufficient balances
    Checking Balances
      ✔ returns user balance
    Making orders
      Success
        ✔ tracks the newly created order
        ✔ emits an Order event
      Failure
        ✔ Rejects with no balance
    Order actions
      Cancelling orders
        Success
          ✔ updates canceled orders
          ✔ emits a Cancel event
        Failure
          ✔ rejects invalid order ids
          ✔ rejects unauthorized cancelations
      Filling orders
        Success
          ✔ executes the trade and charge fees
          ✔ updates filled orders
          ✔ emits a Trade event
        Failure
          ✔ rejects invalid order ids
          ✔ rejects already filled orders
          ✔ Rejects canceled orders
```

Figure 5. TESTING EXCHANGE

```
Token
  Deployment
    ✔ has correct name
    ✔ has correct symbol
    ✔ has correct decimals
    ✔ has correct total supply
    ✔ assigns total supply to deployer
  Sending Tokens
    Success
      ✔ transfers token balances
      ✔ emits a Transfer event
    Failure
      ✔ rejects insufficient balances
      ✔ rejects invalid recipent
  Approving Tokens
    Success
      ✔ allocates an allowance for delegated token spending
      ✔ emits an Approval event
    Failure
      ✔ rejects invalid spenders
  Delegated Token Transfers
    Success
      ✔ transfers token balances
      ✔ rests the allowance
      ✔ emits a Transfer event


37 passing (7s)
```

Figure 6. TESTING TOKENS

```
blockchain-developer-bootcamp — node ◂ npm exec hardhat node __CFBun...
Last login: Sun Feb 11 18:46:39 on ttys001
[apple@MacBook-Pro ~ % cd blockchain-developer-bootcamp
[apple@MacBook-Pro blockchain-developer-bootcamp % npx hardhat node
Started HTTP and WebSocket JSON-RPC server at http://127.0.0.1:8545/

Accounts
========

WARNING: These accounts, and their private keys, are publicly known.
Any funds sent to them on Mainnet or any other live network WILL BE LOST.

Account #0: 0xf39Fd6e51aad88F6F4ce6aB8827279cffFb92266 (10000 ETH)
Private Key: 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf4f2ff80

Account #1: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8 (10000 ETH)
Private Key: 0x59c6995e998f97a5a0044966f0945389dc9e86dae88c7a8412f4603b6b78690d

Account #2: 0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC (10000 ETH)
Private Key: 0x5de4111afa1a4b94908f83103eb1f1706367c2e68ca870fc3fb9a804cdab365a

Account #3: 0x90F79bf6EB2c4f870365E785982E1f101E93b906 (10000 ETH)
Private Key: 0x7c852118294e51e653712a81e05800f419141751be58f605c371e15141b007a6
```

Figure7.Hardhat Nodes For Blockchain Development

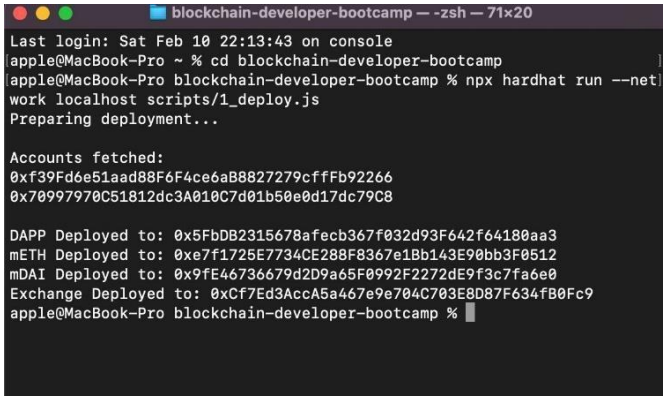

Figure 8. Testing Scripts

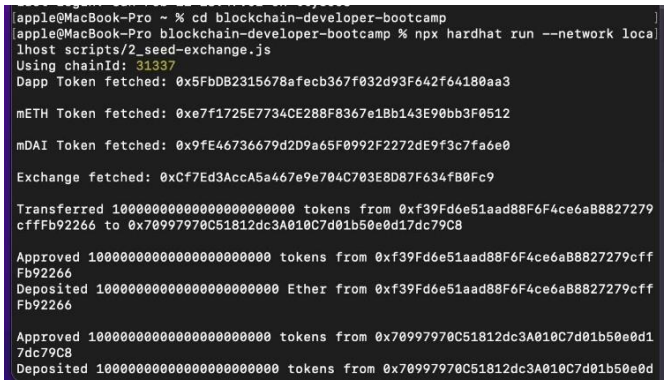

Figure 8.1 Testing Scripts

STEP 4: Deposit or Withdraw Tokens

- Users create requests to deposit or withdraw tokens.
- Add the required amount to the exchange wallet and decrease from the user's wallet.
- Confirm transactions in the wallet to approve token transfers.
- Gas fees may vary depending on network conditions.

STEP 5: Buy, Sell, and Track Transactions

- Users create requests to buy or sell using provided options.
- System tracks and reviews transactions,adding them to the order book.
- Users can access and view transactions associated with specific public keys.
- Facilitate secure and efficient token transfers, leveraging decentralized finance benefits.

These steps provide a comprehensive overview of the development process for a decentralized token exchange application. Developers can follow these guidelines to build a functional and user-friendly DApp for exchanging tokens on the blockchain.

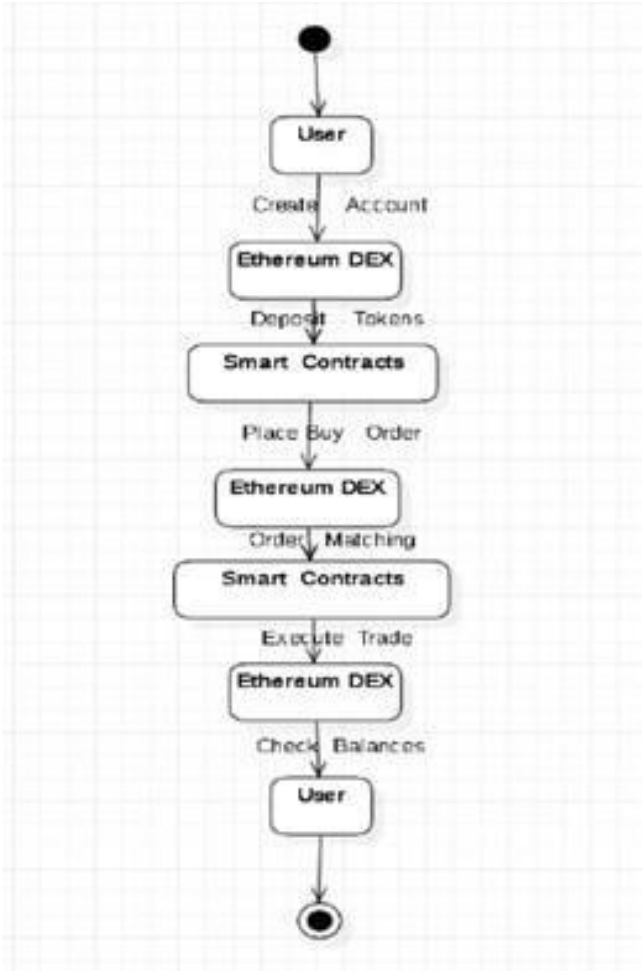

Figure 9. Activity Daigram

VIII. RESULT

The decentralized token exchange platform provides a secure and reliable solution for trading Ethereum- based tokens. Users can easily transfer their tokens from their personal wallets to the exchange wallet, leveraging the potential of blockchain technology. This user-friendly and effective deposit feature enables users to actively participate in token trading, promoting liquidity and nurturing a dynamic

ecosystem within the decentralized platform. Additionally, the withdrawal process follows a similar user-friendly approach, allowing users to safely retrieve their tokens from the exchange wallet to their personal wallets, ensuring complete ownership and control over their digital assets.

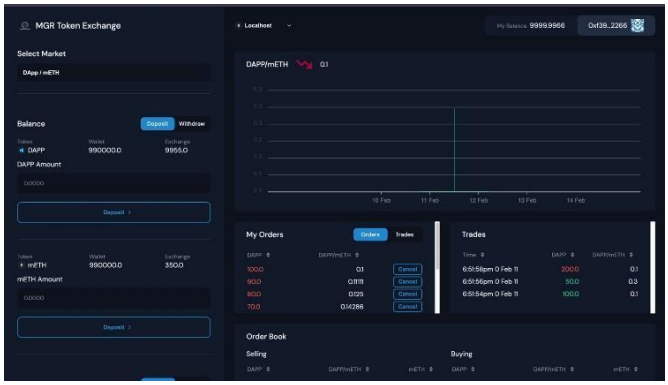

Figure10.User Interface

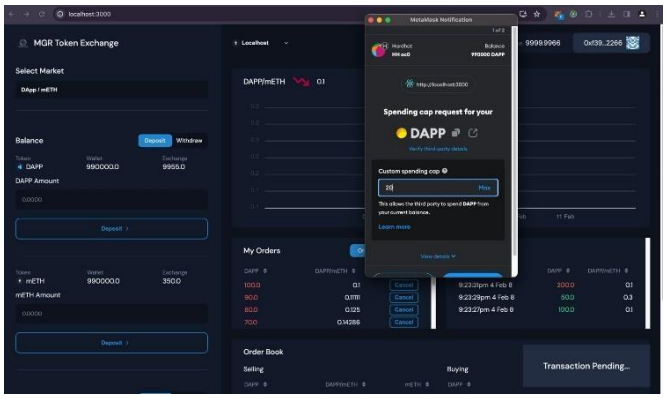

Figure10.1 User Interface

IX. CONCLUSION

The platform we're creating is all about shaking things up in the digital world. Imagine a place where the usual middlemen like banks and online payment systems are no longer needed. That's what we're aiming for. By tapping into blockchain technology, we're making it possible for people to deal directly with each other. This means when you send or receive digital tokens, it's just between you and the other person. No extra fees, faster transactions, and you're in control.What we're doing is quite a big deal. It's a whole new way of handling digital assets, moving away from the big, centralized systems we've always relied on. This platform is not just a tool; it's a secure space where anyone, whether you're flying solo or running a company, can create and swap tokens easily and safely, all within a system that values openness and trust. Sure, this journey isn't going to be a walk in the park. There are plenty of tech puzzles to solve and we've got to convince people that this is the way to go. But, the potential here is huge. We're on the brink of changing how people around the globe think about and use digital assets, sparking innovation in countless areas and reshaping our digital world. So, while the road ahead may have its bumps, the goal is clear: to give power back to the users, making the digital space a little more democratic, one token at a time

X. REFERENCE

[1] Chaum, D.: Blind Signatures for Untraceable Payments. In Chaum, D., Rivest,R.L.,Sherman, A.T., eds.: Advances in Cryptology, Boston, MA, Springer

[2] 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

[3] Bhuvana, R., Aithal, P. S. (2020). RBI Distributed Ledger Technology and Blockchain. A Future of Decentralized India. International Journal of Management, Technology and Social Sciences (IJMTS), 5(1), 227- 237.

[4] Mukhopadhyay,cong U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L.,Brooks, R.,2020. A brief survey of cryptocurrency systems, in:2020 14th annual conference on privacy, security and trust (PST),IEEE. pp. 745–752.

[5]C. Pop et al., ”Decentralizing the Stock Exchange using Blockchain An Ethereumbased implementation of the Bucharest Stock Exchange”, 2018 IEEE 14th International Conference on Intelligent Computer Communication and Processing (ICCP),pp. 459- 466,
2018.

[6]Chris Dannen, “Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain

Programming for Beginners", Published by Springer Science +BusinessMedia New York, ISBN: 978-1- 4842-2534-9.

[7]M. Pincheira, M. Vecchio, and R. Giaffreda, "Rationale and practical assessment of a fully distributed blockchain-based marketplace of fog/edge computing resources," in Proc. 7th Int. Conf. Softw. Defined Syst. (SDS), Apr. 2020, pp. 165–170, doi: 10.1109/SDS49854.2020.9143892[8]Y. P. Tsang, K.
L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam,

[9]V. Y. Kemmoe, W. Stone, J. Kim, D. Kim and J. Son, "Recent Advances in Smart Contracts: A Technical Overview and State of the Art", IEEE Access, vol. 8, pp. 117782-117801, 2020.

[10]R. Nair and A. Bhagat, "An Application of Blockchain in Stock Mar- ket" in Transforming Businesses With Bitcoin Mining and Blockchain Applications, IGI Global Publisher, pp. 103-118, 2020.

[11] "Blockchain-driven IoT for food traceability with an integrated consen- sus mechanism," IEEE Access, vol. 7, pp. 129000–129017, 2019, doi: 10.1109/ACCESS.2019.2940227.

[12] Ethereum. What is Ethereum? The Foundation for Our Digital Fu- ture. Accessed:Aug. 30, 2020. [Online]. Available: https://ethereum. org/en/what-is-ethereum.

[13] Avital, M., Beck, R., King, J., Rossi, M., Teigland, R. (2022). Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future. International Conference on Information Systems.

[15] Baldwin, C. Y., Woodard, C. J. (2021). The architecture of platforms: A unified view.Platforms, Markets and Innovation, 19– 44.

[16] Buterin, V. (2020). A next-generation smart contract and decentralized applicationplatform.

[17]Werbach, K. (2022). The Blockchain and theNew Architecture of Trust. The MITPress. [18]Werbach, K. (2021). The Blockchain and theNew Architecture of Trust. The MITPress. [19]Yaron Velner Loi Luu. Kybernetwork: A trustless decentralized ex- change andpayment service.

[20]Cong, L. W. and He, Z. (2019). BlockchainDisruption and Smart Contracts. TheReview ofFinancial Studies, 32(5):1754–1797. [21]Huberman, G., Leshno, J. D., and Moallemi, C. (2021). Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. The Review of Economic Studies, 88(6):3011–3040.

[22] Wood, G. (2021). Ethereum: A secure decentralised generalised trans- action ledger. Ethereum Project Yellow Paper.

[23] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange onthe ethereum blockchain, 2021.

[24] Vitalik Buterin. Ethereum: a next generation smart contract and decen- tralized application platform (2020).