

Hybrid Auction system bridging centralized efficiency and decentralized trust

Mrs.Ariyamala.V, Assistant professor, Department of Computer Science and Engineering,Rajalakshmi Engineering College,
veerariya2016@gmail.com.

Selvendran.K, Ragul Karthik.G.U, Sashi Kumar.B, Department of Computer Science and engineering,Rajalakshmi Engineering College,
selvendranks@gmail.com, ragul262003@gmail.com,
bsashikumar2002@gmail.com,

I. ABSTRACT

Blockchain technology has undergone significant evolution, originally conceived as a decentralized currency and later incorporating advanced features such as smart contracts, leading to the emergence of Web 3.0. Traditional E-auction systems, primarily hosted on centralized servers with inherent trust and privacy challenges, have prompted the development of innovative solutions. This paper introduces a secure online bidding system that leverages blockchain technology, specifically implemented using the Truffle framework with the Ethereum blockchain. In this hybrid system, the integration of both decentralized and centralized components becomes pivotal. Blockchain technology, renowned for decentralized storage and resistance to fraudulent activities, addresses the inherent flaws of centralized data storage in E- auction systems. The permanence and tamper-proof nature of blockchain records ensure the immutability of every action taken by bidders and sellers. Furthermore, the implementation of smart contracts automates payment processes, mitigating the risk of fraud. However, this secure online bidding system adopts a hybrid approach by incorporating certain centralized components, such as Firebase. This integration enhances the overall functionality of the system while retaining the benefits of decentralization. Transactions remain verifiable by all users, fostering trust and transparency within the auction system. The hybrid model, marrying the strengths of both decentralized and centralized systems, presents a robust solution to the trust and security challenges posed by traditional E-auction systems.

Keywords— *Blockchain, Ethereum, Decentralized storage, Auction, Smart contract*

II. INTRODUCTION

The E-auction system has two main categories, the first category is known as the English auction in which the previous highest bid value for the particular item is publically visible whereas other bidders bid for a higher value than the previous. At the end of the auction, the highest bidder wins. The second category is known as sealed bid auction, where every bidder bids without knowing the highest bid or the other's bid. At the end of the auction bidder who bid the highest value wins.

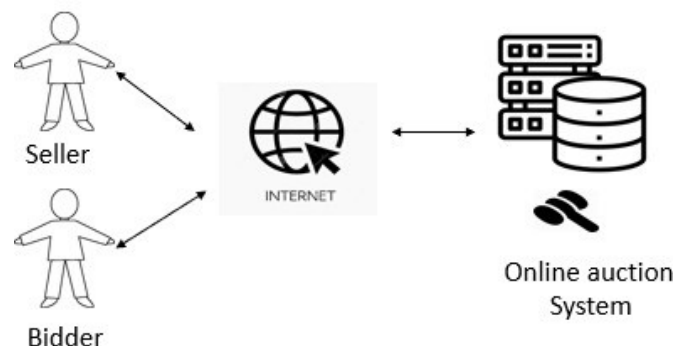


Fig 1 Traditional auction system

Fig 1 depicts the traditional auction system, where a 3rd party auction host provides a platform for sellers and bidders to post their products. There are some flaws in this system. A 3rd party is needed to manage all the information between the seller and bidder. Personal information and data stored in the server may cause privacy leakage

In this proposed system, we are going to design and implement an auction system using blockchain. For this, the Truffle framework with Ganache (personal Ethereum blockchain) will be used.

The proposed system aims to create a web-based application where users can create an account, allowing them to list items for auction. All users, except the item owner, have the opportunity to place bids on these items. The price of the item increases automatically each time a bidder places a bid. Once the auction time for the item expires, the highest bidder is declared the winner of the auction.

Every action made by the bidders and sellers is permanently recorded in the blocks, including details related to the item and information related to the bidders' bids. At the end of the auction, the highest bidder is automatically declared the purchaser, and ownership of the item is transferred to the winner.

To facilitate user authentication and interaction, we integrated centralized services such as Firebase for user authentication and for storing/retrieving information regarding items and bidder information. We provide payment information and functionality through the Ethereum blockchain. Additionally, we leverage MetaMask with secure wallet management capabilities to manage user accounts. This hybrid approach combines the reliability of the blockchain with the user-friendliness of centralized services while also reducing unnecessary transaction costs.

III. RELATED WORK

A. Traditional Bidding System

One of the first e-auction systems concerning security was initially proposed by [1]. This paper primarily focused on the implementation of a distributed auction system. The author discusses how they implemented validation and prevention measures against malicious users.

Various other authors have proposed their ideas on implementing auction system protocols and signature methods [2][3][4], to provide secrecy for bid information and ensure validation against tampering.

Additionally, authors such as [5][6] have suggested involving a trusted third party to achieve fairness, a process that can be verified by both the seller and the bidder parties. At the bid-winning stage, the winning bidder is jointly decided by the third party and the auctioneer.

B. Blockchain and distributed ledger

Blockchains are containers of data records linked together. Each block has a timestamp and the hash value of the previous block, along with transaction data. The primary purpose of this data storage technique, where data is stored in blocks and linked, is to ensure that once data is stored in a block, it can never be changed.[7]

A distributed ledger as shown in Fig 2 is a data store with multiple copies of the data chain running across a network, all synchronized with each other. Since all nodes have the same replica running, there is no possibility of a single node modifying the data, making this technology highly secure.

Consensus algorithms are used by distributed ledgers to agree upon the current state of the chain. Every time a new block is added to the chain, every ledger validates the block and agrees to add it to the chain on all nodes.

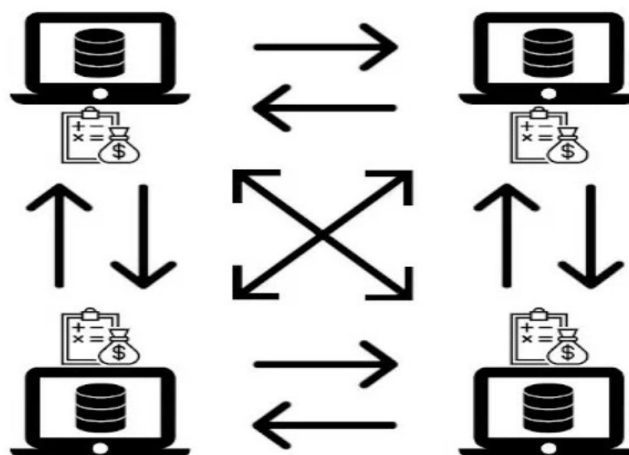


Fig 2 Distributed ledger

C. Smart Contract

A smart contract is a program deployed on a blockchain as a transaction, which runs when a certain predefined condition is met. These contracts help eliminate the need for an intermediary to oversee program execution. Smart contracts are digital and resemble real-time contracts. Once a contract is in place, no one can modify or cancel it [8].

Smart contracts have a variety of use cases, which include implementation in the supply chain sector for greater transparency, reliability, and trustworthiness without third-party involvement. Additionally, using smart contract technology can automate tasks in healthcare systems and maintain the privacy of patients. Traditionally, insurance systems take longer to process, and sometimes the insurance party may modify the policy in favor of the insurance company. Smart contracts can help mitigate these trust issues [9].

Even though smart contracts seem to be ideal, it comes with some of the downsides. The immutable nature of the contract once deployed can cause unfixable bugs and exceptions. Smart contract programs need to be rigorously tested and then deployed. Smart contracts operate based on predefined rules. If circumstances change or parties want to amend the contract, it can be challenging to do so without creating an entirely new contract.

D. Limitations in the Existing Auction Systems using Blockchain

- a) **Costs for Large Datasets:** In existing auction systems leveraging Blockchain technology, a notable limitation revolves around the costs incurred when dealing with large datasets. Specifically, storing comprehensive item information, which may include images and detailed descriptions, on the blockchain results in substantial expenses. These costs primarily stem from transaction fees linked to the volume of data stored in each transaction on the Blockchain.
- b) **Time to Retrieve Data from the Blockchain:** Another critical limitation in existing auction systems utilizing Blockchain pertains to the time required to retrieve data from the blockchain. This challenge becomes more pronounced as the size of the blockchain grows over time. The process of traversing the entire blockchain to retrieve specific data introduces delays, impacting the efficiency of querying and data retrieval operations.

IV. HYBRID AUCTION SYSTEM BRIDGING FIREBASE AND BLOCKCHAIN

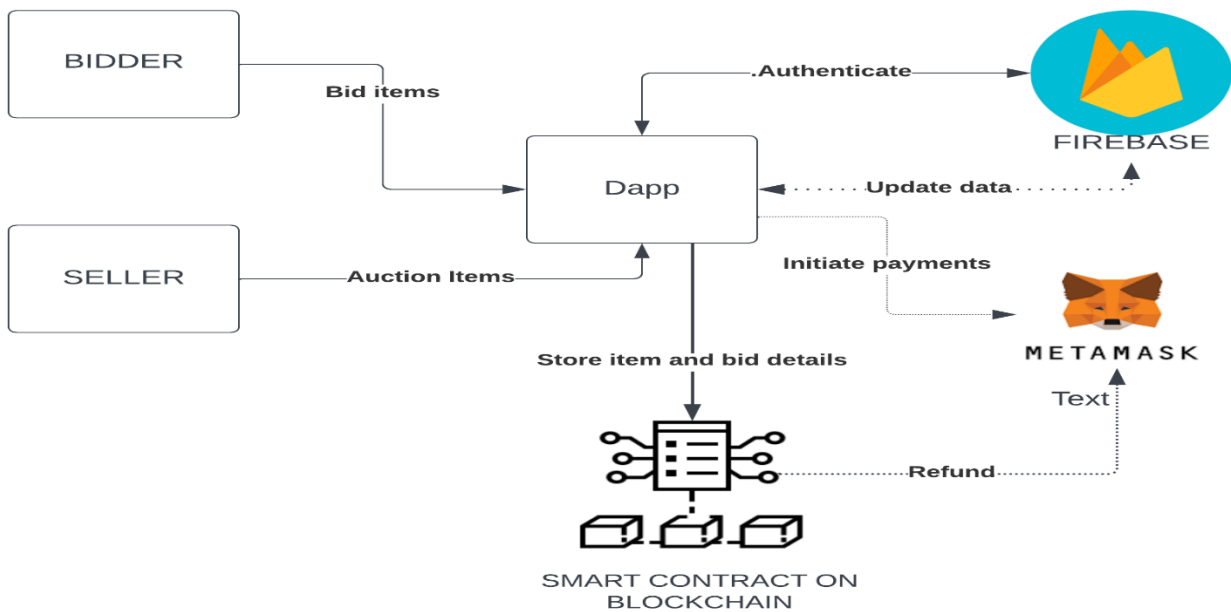


Fig 3 Hybrid Auction system bridging centralized efficiency and decentralized trust

A.Novelty

Our project introduces a groundbreaking approach to online auctions by implementing a secure and efficient hybrid system. Unlike traditional methods that store all information in the blockchain, leading to cost and retrieval time limitations, our solution leverages the strengths of both blockchain technology and Firebase, optimizing performance and cost-effectiveness.

1) Blockchain Core Functionality: When a seller initiates an auction by listing an item, only essential information crucial for the blockchain's backend functionality is stored and processed within the blockchain. This ensures that the core auction processes, such as bidding and payment, operate seamlessly without unnecessary data burden.

2) Firebase for Additional Data: Non-essential data, such as item images and detailed descriptions, is intelligently stored in Firebase, a centralized service. This strategic off-chain storage in Firebase minimizes storage costs on the blockchain, addressing the financial challenges associated with large datasets.

3) Authentication and Information Management: Firebase plays a key role in providing robust authentication services and efficient information management for our decentralized application (dApp). User registration, login authentication, and personalized dashboard functionalities are seamlessly handled by Firebase, enhancing the overall user experience.

4) Real-time Data Retrieval and Display: To optimize the user interface, Firebase is utilized for the retrieval and display of non-core data. This includes fetching images, item descriptions, and other details necessary for rendering the website. By avoiding direct blockchain queries for non-essential data, we significantly reduce retrieval time and associated costs.

5) Data Integrity Check: Ensuring the safety and integrity of data stored in Firebase is paramount. When an item is created, the blockchain generates and stores the hash value of the complete item information. During each website load, the system dynamically recalculates the hash values for existing items and compares them with the already stored hash in the blockchain. Any discrepancies indicate potential tampering, triggering immediate corrective actions.

B.Objectives

- 1)Enhance
Transparency
- 2)Improve Security
- 3)Eliminate Centralized Control on payment
- 4)Foster Trust
- 5)User-Friendly Interface

C.Technologies used

1. React:

In our project, React is the frontend framework of choice. We use it to build the user interface (UI) of our web- based auction application. React allows us to create dynamic and responsive UI components, such as item listings, bid buttons, and user dashboards. It also facilitates seamless interaction with the backend and blockchain for tasks like bidding and displaying auction details.

2. Firebase:

Firebase is employed for user authentication and real-time data management in our project. Sellers and bidders can create accounts, log in securely, and access personalized dashboards. Firebase's real-time database enables us to update auction information instantly, ensuring that users receive live updates on bidding activity and auction results.

3. Truffle:

Truffle is pivotal for developing and deploying our Ethereum smart contracts. Auction items are managed by smart contract which also manages the bidding process, tracks bids, and determines winners. Truffle simplifies the development workflow by providing tools to write, compile, and test these smart contracts efficiently.

4. Ganache:

Ganache serves as our local Ethereum blockchain during development. It allows us to test and debug smart contracts without incurring real gas fees or interacting with the live Ethereum network. Ganache's blockchain simulation ensures that our smart contracts function as expected before deploying them to the main net.

5. MetaMask:

MetaMask is a crucial component for users participating in auctions. It acts as a bridge between their web browsers and the Ethereum blockchain. Users can install MetaMask to create Ethereum wallets, manage their funds, and place bids securely. MetaMask also handles transaction signing and approval, ensuring a seamless bidding experience

D. Project workflow

- 2)Registration phase
- 2)Item auctioning
- Phase3)Bidding
- Phase
- 4)Winner declaration phase

D.1 Registration Phase

In the first step of the auction system, which is followed by all users, there is a registration phase where new users are required to enter their details. These details include:

- username
- mail address
- password

This registration process follows standard authentication procedures that all users must adhere to. The user details are securely managed by the Firebase Authentication Cloud service [10][11][12](Fig 4), a leading backend service provider. Every user has the independence to either auction items or place bids. However, it's important to note that sellers are not allowed to bid on their own auctioned items. All users must log in with their credentials to participate in auctions or place bids.



Identifier ↓	Providers	Created ↓	Signed In	User UID
seller@gmail.com		Aug 31, 2023	Sep 2, 2023	Q3r38QstAdRnsy2yZsZPNR46FBf1
bidder@gmail.com		Aug 31, 2023	Sep 2, 2023	q5Fc9kzrSRcEtdaipWu62AgO4es2

Fig 4 user authentication details stored in Firebase

D.2 Item auctioning Phase

Every user can auction an item as well as participate in bidding. In the item auctioning phase, the seller needs to provide the following details regarding the item to be auctioned:

- Item name
- Item description
- Item image
- Item starting price
- Item auction duration

Once the user enters these details and clicks on "place item," they are prompted to use the MetaMask extension installed in their browser. He/She must choose the account from which the transaction needs to be processed. Every seller has to pay the required amount of gas fees each time they place an item for auction.

After the successful transaction via MetaMask, all the details related to the item are stored in the chain and managed by the smart contract. Additionally, a replica of the item's details is stored in Firebase. This hybrid approach ensures both the immutability of the blockchain and the efficiency and speed of data retrieval from Firebase[13][14], which is essential for displaying the real-time status of the item on the web interface.

Algorithm : Seller provides the details of the item to be auctioned

Input Parameters:

itemName: Name of the item.

durationInMinutes: Auction duration.

Function Steps:

1. Retrieve item index using `getItemIndex`.
 2. Create new `Item` with seller as `msg.sender`.
 3. Set item details and calculate end time.
 4. Push new item to `items` and add end time to `expirationTimestamps`.
-

D.3 Bidding Phase

A user can bid on multiple items until the auction for each item expires. The auction system operates on an incremental approach, and every user must place bids higher than the previous highest bid made by other users. The previous bid price made by the user for a specific item is also displayed.

The incremental approach follows the standard auction increment formula:

Minimum Bid Increment = Current Highest Bid × Bid Increment Percentage

In our case, we fix:

Bid Percentage = 10%

When a person clicks on the bid button for a specific item, they are prompted to use the Metamask wallet. The bidder must choose a valid account for the transaction. The bidder needs to pay the bid price in ethers along with additional gas fees for the transaction. The bidding process for the item continues until the expiration date. The bidder information along with the user's highest bid is recorded in both Firebase(Fig 5) and the smart contract corresponding to the item bid.

```
▼ bidders
  bidder1@gmail.com: 66550
  bidder2@gmail.com: 60500
  bidder@gmail.com: 55000
  createdAt: September 28, 2023 at 9:24:40 AM UTC+5:30
  curPrice: 66550
  curWinner: "bidder1@gmail.com"
  desc: "One of the rarest man crafted pen with the purest of gold"
  duration: 1695880480080
  email: "seller@gmail.com"
  imgUrl: "https://firebasestorage.googleapis.com/v0/b/onlineauction-83b82.appspot.com/o/download.jpeg?alt=media&token=87dbb5cd-5de0-47b1-abc3-dc087532d76b"
  title: "Golden pen"
```

Fig 5, item details stored in Firebase

Algorithm : Bidder places bid on the auctioned item

Input Parameters:

itemName: Name of the item.

Function Steps:

1. Retrieve item index using getItemIndex
if auction is active and bidder != seller **then**
 2. Update bidder's bid amount in bidAmounts
End
 - if** new bidAmount > current highest bid **then**
 3. update highest bidder and bid amount.
End
 4. Add the bidder to the list if not already present.
-

D.4 Winner declaration Phase

After the end of the period for the auctioned item. The phase undergoes two sub-phases.

1)**Winner Notification Phase:** The Firebase stores data about the auctioned item, including the start and end dates. The React front end keeps track of this information and displays a countdown. When the countdown reaches zero, React displays the winner based on the "curWinner" and the bid price based on the "curPrice" fields stored in Firebase.

2)**Fund Credit and Refund Phase:** As previously mentioned, an exact copy of the item is stored in both Firebase and the blockchain network. The smart contract operates independently without the need for the front end. At the end of the auction time for a specific item, it performs two processes:

- **Crediting the Auctioneer:** When the auction for an item concludes, and the winner is declared, the highest bid amount from the winning bidder is transferred to the auctioneer.
- **Refunding the Bidders:** For all bidders other than the highest bidder, who placed bids on the item, their money is refunded to their respective MetaMask accounts, which they used for bidding.

Algorithm : End the auction by crediting the seller and refunding the bidders

Input Parameters: None

Function Steps:

```
for (items[itemIndex])
    2. Verify that the auction is active (items[itemIndex].active).
    3. Set the auction status to inactive (items[itemIndex].active = false)
    for (items[itemIndex].bidders)
        if (bidder != highestBidder) then
            4. payable(items[itemIndex].seller).transfer(items[itemIndex].highestBid)
            5. Get the bid amount of the bidder (items[itemIndex].bidAmounts[recipient])
            6. Transfer the bid amount back to the bidder (payable(recipient).transfer(refundAmount))
        End
    End
End
```

B. Smart contract modules

Below mentioned are the smart contract functions in the deployed contract in the Ethereum blockchain which handles the decentralized payment.

- `createItem()`: This function allows a user to create a new auction item. It takes the item name and the duration of the auction in minutes as parameters and initializes the auction.
- `placeBid()`: Users can place bids on auction items with this function. It takes the item name as a parameter and checks that the auction is active and that the user is not the seller. If the bid is higher than the current highest bid, it updates the highest bidder and highest bid amount.
- `Refund()`: This internal function refunds a specific bidder for a particular item. It transfers the bid amount back to the recipient.
- `endAuction()`: This internal function is used to end an auction for a specific item. It checks if the auction is active, ends it, and transfers the highest bid amount to the seller. It also refunds other bidders who didn't win the auction.
- `checkExpiredItems()`: This function checks if any auction items have expired and ends them if necessary. It iterates through the list of items and ends the auction for any item where the auction end time has passed.

V. RESULT

Finally we have implemented the secure auction system which upholds the following key features of our proposed system.

Function Name	Transaction Gas	Low Transaction Fee (USD)	Market Transaction Fee (USD)	Aggressive Transaction Fee (USD)
Deployment	382649	14.69	15.38	15.66
CreateItem	39433	1.48	1.55	1.58
placeBid	31633	1.19	1.24	1.26
checkExpiredItems (internally executing *endAuction *refund)	15944	0.60	0.62	0.63
getBidders	0	0	0	0
getHighestBidderAndAmount	0	0	0	0
Total	469659	17.96	18.79	19.13

Auto-Refund Mechanism

Our e-auction system incorporates an automatic refund mechanism to enhance fairness and trust among participants. If a bidder does not win an auction, the system automatically refunds their bid amount. This feature not only promotes a secure and transparent auction process but also ensures that users are confident in participating without the fear of losing their funds.

Hybrid Data Storage Approach

To optimize data storage and minimize unnecessary gas fees, our system employs a hybrid approach. Complete information about auction items, such as item images and descriptions, is stored in a centralized database. The blockchain retains essential information and references to the off-chain data, ensuring data integrity while significantly reducing the cost of storing large volumes of data on the blockchain. This approach is particularly beneficial as the Ethereum network's gas fees can be substantial, with approximately 0.032 ETH per 1 KB of data. Our hybrid model efficiently balances data storage costs and system performance, creating a practical and cost-effective solution for users and the platform alike.

Independence from Centralized Systems

One of the standout features of our e-auction system is its independence from centralized systems. The blockchain operates autonomously and does not rely on external centralized databases. This means that even if changes or disruptions occur in the centralized system, the e-auction platform remains fully functional. Users can participate in auctions with confidence, knowing that their transactions and auction results are not subject to external system fluctuations, providing a robust and reliable experience.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have presented the implementation of a hybrid secure auction system by combining a DApp with a centralized database, such as Firebase, and a smart contract on the Ethereum blockchain for decentralized payments. This approach offers efficient data management, alleviating the issue of high gas fees on the Ethereum blockchain for storing extensive item information. Moreover, it ensures independence from centralized systems, providing robustness and security against data breaches or disruptions in the central infrastructure.

To further enhance the security of this project, the next step for improvement involves implementing a technique to identify any modifications in the central database. One potential solution is to store the hash value of the item details in the blockchain. Each time the DApp retrieves data from the central database (Firebase), the DApp cross-verifies the hash value of the retrieved data with the hash stored in the blockchain for the corresponding item.

VII. REFERENCES

- [1] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," in *IEEE Transactions on Software Engineering*, vol. 22, no. 5, pp. 302-312, May 1996.
- [2] Shengke Zeng, Shaoquan Jiang, Zhiguang Qin. An efficient conditionally anonymous ring signature in the random oracle model. *Theoretical Computer Science* 461 (2012): 106–114.
- [3] Hongwei Li. Ring signature and signcryption scheme design and research of [D]. Xihua University. 2011.
- [4] Y. Komano, K. Ohta, A. Shimbo, S. Kawamura. Toward the fair anonymous signatures: deniable ring signatures. *The Crypto- graphers' Track at the RSA Conference 2006*, in: LNCS, vol. 3860, Springer, Heidelberg, 2006, pp. 174-191
- [5] C. C. Wu, C. C. Chang, I. C. Lin. New sealed-bid electronic auction with fairness, security and efficiency. *Journal of Computer Science and Technology*, 2008, 23 (2): 253-264.
- [6] M. J. Li, J. S. T. Juan, J. H. C. Tsai. Practical electronic auction scheme with strong anonymity and bidding privacy, *Information Sciences* 181 (2011) 2576- 2586.
- [7] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.
- [8] Macrinici, D., Cartoceanu, C., & Gao, S. Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics*, 35(8), 2337–23, 2018.
- [9] B. K. Mohanta, S. S. Panda and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2018, pp. 1-4, doi: 10.1109/ICCCNT.2018.8494045.
- [10] L. H. Pramono and Y. K. Yana Javista, "Firebase Authentication Cloud Service for RESTful API Security on Employee Presence System," 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2021, pp. 1-6, doi: 10.1109/ISRITI54043.2021.9702776.
- [11] "Allocating Resources in Cloud using Auction Mechanism". *International Journal of Innovative Technology and Exploring Engineering*, January 2020, ISSN: 0193-4120 Page No. 5399 – 5401.
- [12] "An Online Auction Frame Work for Dynamic Resource Provisioning In Cloud Computing" *International Journal of Advanced Science and Technology (IJAST)* Vol. 29 No. 9s (2020): Vol. 29 No. 9s (2020) Special Issue
- [13] E. Şafak, A. F. Mendi and T. Erol, "Hybrid Database Design Combination of Blockchain And Central Database," 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2019, pp. 1-5, doi: 10.1109/ISMSIT.2019.8932763.
- [14] Kumar, P., Swetha, S., & Sundari, M. (2023). Secured Web-based Alumni Network and Information Systems. In 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1427- 1434). IEEE.
- [15] Kotobi, K., & Bilén, S. G. (2018). Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access. *IEEE Vehicular Technology Magazine*, 13(1), 32–39. <https://doi.org/10.1109/mvt.2017.2740458>