International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Blockchain Based Secure Online Bidding System using Cloud Storage

Kartik Parmar, Jaimin Solanki, Rohan Tondlekar and Keegan Vaz
Computer Engineering Department
St. Francis Institute of Technology
Mumbai, India
Email: kartikprmr4664@student.sfit.ac.in, jaiminsolanki027@student.sfit.ac.in,
tondlekarrohan@student.sfit.ac.in and keegangeorgevaz@student.sfit.ac.in

Under the Guidance of
Ms. Nidhi Gaur
Computer Engineering Department
St. Francis Institute of Technology
Mumbai, India
Email: nidhigaur@sfit.ac.in

***Abstract*—Blockchain Based Secure Online Bidding System intends to create a platform that enables auctioneers to offer physical and digital products for sale online. Blockchain technology has several uses in the present world. Two of these are cloud storage systems powered by blockchain and electronic bidding. The fastest, most secure, and most effective method to construct a bidding system is provided by blockchain technology and cloud storage. To organize and store bids, the system will make use of blockchain technology, eliminating the potential for rigged bids. As a result, the users will experience a fair and transparent system.**

***Index Terms*—Auction, Bidding System, Blockchain, Cloud Storage, Decentralized storage.**

I. Introduction

Blockchain technology is a distributed ledger system that has been designed to allow for the secure and transparent transfer of anything of value. It records transactions in an immutable and verifiable way. Blockchain technology has many use cases in today's world. One of them is an e-auction system. In the present bidding process, there is always a third party involved. There are numerous unstated fees present in the bidding process. The return procedure is also opaque. The proposed system uses Avalanche-based Blockchain with a ReactJS frontend creates a platform with transparency for buyers and auctioneers. The bidding system would allow auctioneers to sell physical as well as virtual assets. Physical assets would be delivered using a delivery chain, whereas soft assets would be transferred over the blockchain.

Other use case of Blockchain would be data storage, which allows people to store their data securely on a decentralized network. Blockchain can be used to create a decentralized, transparent, and secure cloud storage platform that is resistant to any type of hacking or manipulation. A blockchain-based storage system would be more efficient and cheaper than traditional cloud storage because it does not require a central server to store data. This network ensures that no single entity controls or owns your data and also makes sure that everyone's privacy is safeguarded.

Using these two ideologies, a secure and reliable platform is created where users won't need to worry about data theft or any privacy related issues and can experience a smooth transaction without any difficulty.

II. Problem Definition

The traditional bidding system involves auctions being conducted at a physical location. This limits bidders and sellers to a single location. This also forces them to travel with huge pieces of industrial equipment or assets either to or from the auction location. Buyers are bound to bear the extra costs of traveling and attending the auction with no assurity of acquiring the desired bid/asset. Even if the buyer gets the bid he/she has to bear the shipment expense in some cases. Seller's asset is limited to the physical auction market present during the duration of auction. Even sellers are bound to bear the expense of shipping the large equipment for sale with no guarantee that the desired buyer will be at the auction. Traditional Bidding system is not flexible. Traditional bidding systems operate for a limited amount of time. The presence of seller, buyer and auctioneer is necessary for the smooth conduct of auction.If the seller or buyer is not physically present for that duration of auction he/she could not avail the benefits from the system.The online auction system overcomes some of these problems but involves third party risk. Online auction system is centralized and thus is prone to being biased at times. It also creates a threat to users' privacy by revealing their identity in public.

III. Literature Survey

S. K. Shah [1] discusses about creating a bidding system with blockchain using Hyperledger Sawtooth Framework. They used Proof of Elapsed Time (PoET) algorithm in their system. The proposed work aims to create a system that allows clients to connect to the validator network and add selected items or goods to the auction. Other customers can view the various items for sale, connect to our verification network, and bid on each of those items. For each item, after a specified period of time, the highest bidder wins the item and gets the item at the bid price. Thus, the system provides an online her platform with an easy-to-use user interface so that users can buy and sell various commodities. A consensus mechanism is a fault-tolerant mechanism used in computers and blockchain systems to reach a desired agreement about a single data value or state of a network between distributed processes or multi-agent systems. [2] The electronic bidding system aims to determine a comparatively fair and open online trading platform between the demand side (tenderer) and therefore the solution provider (bidder).BCES comprises basic configuration management, contract business deployment, data service processing, system service support, and data visualization. Through the detailed design of a collection of blockchain integration and transformation mechanisms for bidding business, different stakeholders are connected along with the assistance of the alliance blockchain, forming a flat trust management model. The experiments demonstrate that the typical TPS of BCES is stable at around 2600-2800, and therefore the time interval of the blockchain deposit platform is within the appropriate time range of 3s, and therefore the error rate is incredibly low.

P. Manimaran [3] discusses about the challenges faced in the traditional system and how one can overcome them using blockchain like, First, the bidding system requires a centralized intermediary to support communication between bidders and auctioneers. They charge centralized brokerage fees to increase transaction costs. Also, personal details and transaction records stored in databases can lead to invasion of privacy. Second, with sealed envelopes, bidders have no way of guaranteeing that the top bidder will not reveal their bid price. Blockchain is a peer-to-peer access structure, so the points in the structure are mutually trustworthy. Each site can communicate, authenticate, and transfer data securely with other sites. As a result, a decentralized structure can reduce transaction costs by eliminating centralized intermediaries. Second, it utilizes smart contracts to prevent leaks of bid prices from winning bidders. Smart contracts have some rules written in them and cannot be opened before the deadline. Y. -H. Chen [4] showed us how important it is to give authority to the right user using smart contracts. He explained it using an example, for instance, if a bidder unintentionally invokes her Reveal() method and opens all bids. This is accomplished by setting permission evaluations for certain functions, which are then executed without first checking to see if the caller has permission to do so.

[5] Here the resources which are divisible for example, electricity, mobile data, and cloud resources are traded for arbitrary prices. The Divisible double auction enables both buyers and sellers to dynamically submit bids/prices for exchanging resources until convergence is achieved, i.e., at Nash Equilibrium. Then, optimally, resources are allocated from sellers to buyers.Smart contracts are designed to allow distributed agents to exchange divisible resources using digital agreements, and the blockchain-based platform facilitates smart contract execution with strong integrity and availability. Since the secure computation for divisible double auction and smart contract execution are computationally expensive to address all these concerns, they designed a Trusted Execution Environment (TEE) Blockchain hybridized system. The TEE first decrypts the input data with the private key and then launches the auction smart contract code in the enclave (a sandboxed environment). Once the manager in Hybrid receives the final output from the TEE, it will check the correctness. If the output is accepted by the Blockchain via checking the new state, the result will be delivered to all the agents, and the Blockchain will store the new state. Using the Double Auction Mechanism, the best responses of all the buyers/sellers is derived, and finally they converge to a Nash Equilibrium (achieving the optimal allocations) and, accordingly, the winner of the bid is computed.

M. Shah [6] uses the concept of cloud storage and integrates it with blockchain to create a secure, decentralized storage space that would reduce the risks of security breach and would allow efficient utilization of the resources. The system uses AES - 256 bits algorithm to encrypt the uploaded file and then divides it among the peers in the network in a 64KB block using a IPFS(InterPlanetary File System) protocol, which returns a hash value with metadata which is mapped with the user's wallet address and is stored in the blockchain using a smart contract. The hash value contains the file address and the user can access it whenever he wants. The user can then pay for all this cost altogether. The future scope of this system was to apply an adaptive scheduling algorithm with which files can be accessed multiple times by the user as compared to the one which is accessed rarely. This will help to ensure that frequently accessed files are available easily to the user whenever required. V. A. Kanade [7] talks about The inevitable use of IOT devices has created a bloom in the rate at which the data is received per second. It will be difficult to meet the requirements of storing this data in the future if appropriate infrastructure is not developed to meet this fast paced environment and store this data efficiently in the current scenario. Cloud storage proves best to provide a solution to this problem of storing data on the internet rather than on the user's device without having the risk of any physical failure and loss of data. This is one of the major reasons that almost all companies have shifted to cloud storage. The Blockchain based distributed storage model and compensation model focuses on utilizing the unused space on the user's electronic device and allowing it to be shared for storage purposes for other users. The user whose storage is being shared receives compensation for

sharing the space. The basic idea here is to enable users to rent out their unused space using a blockchain registry and benefit from the same. This will also promote the concept of creating a global cloud space. The system built is on a peer to peer network but is decentralized using blockchain technology. Hashing is done on the rental registry, making the system secure and less hackable. The equitable compensation model provides monetary benefits to users lending their unused disk space. The financial settlement is intended to be done using cryptocurrency. The system provides a secure portal between storage contributors and storage buyers. But the problem with this concept is that financial settlement is not instant it requires to go through the sorted financial model and it is restricted to IOT devices.

IV. Proposed Methodology

Blockchain Based Secure Online Bidding System overcomes the problem of traditional bidding systems. It also completely eliminates the third party traditionally involved in the whole process. Smart Contract based participation and validation ensures no biasedness. Rules of auction are set in a smart contract, only those participants who meet its condition can participate in the bidding process. The Buyer's identity is anonymous. Only Buyer's wallet id is public. Blockchain Based Secure Online Bidding System eliminates the hidden charges involved in the traditional bidding process. The smart contract closes the bid as per the program code written in it and computes the winner. The seller and buyer transacts the asset and settlement is done.

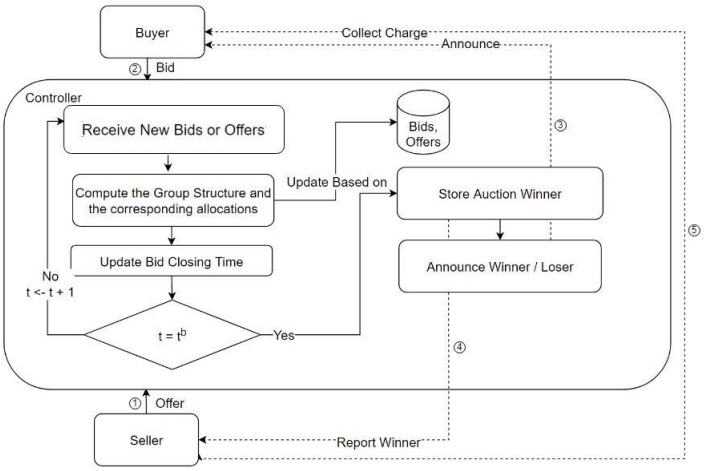

Fig. 1. Block Diagram

From the above figure we can understand that first the seller would create a bid with a base price offer. Later on for a period of time until the bid is live, any bidder can come and bid on the object. The system would receive the new bid, add it to the table compute the group structure with rankings, and lastly update the bid closing time. After the bid has ended, the stored auction winner would be announced to the seller and the respective bidder. The seller can then collect the charges of the bid from the user through the website and the transaction would be completed.

Now, understanding the development of our proposed model

1) Conduct Market Research: Before beginning development,we conducted market research to understand the target audience, their needs, and pain points. Through Literature Survey, we understood the scope of our project as no such project was full fledged deployed in the market.
2) Blockchain Platform: Choose the appropriate blockchain platform based on the requirements of the project. Some popular blockchain platforms are Ethereum, Avalanche, or Binance Smart Chain.We have used Avalanche.
3) Smart Contracts: Developed smart contracts that define the rules for bidding, payment, and item delivery. Including parameters such as starting price, reserve price, auction duration and decision for deciding the winner.
4) Front end: Built a user-friendly front end interface for buyers and sellers. This includes developing the back end components for processing bids and payments.We have used React JS
5) Wallet: Integrate the option for crypto currency payments, allowing users to bid and pay using popular crypto currencies such as Bitcoin, Ethereum, or Meta mask. One can connect through a meta mask account and participate in auctions.
6) Security and Transparency: Used blockchain technology to ensure that all transactions are secure and transparent. This includes implementing measures such as meta mask wallets, encrypted and immutable data storage, and decentralized hosting.
7) Testing and Debugging: Conduct comprehensive testing, including unit testing, integration testing, and user acceptance testing, to identify and fix any issues.
8) Launch the System: After successful testing, deploy the smart contracts and front end React JS components to Avalanche.

V. Results and Analysis

The Auctionify project is an auction management platform built using the Avalanche blockchain and the Drizzle framework. The platform allows users to create and manage auctions for a variety of different items, using the Avalanche network for secure and transparent transactions.

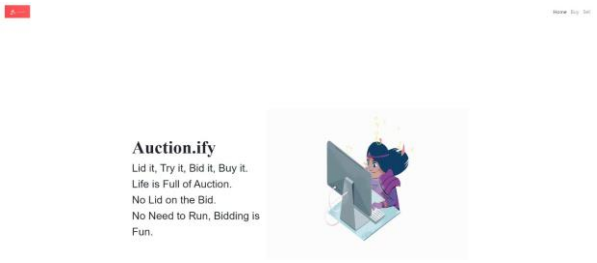

Fig. 2. Home Page

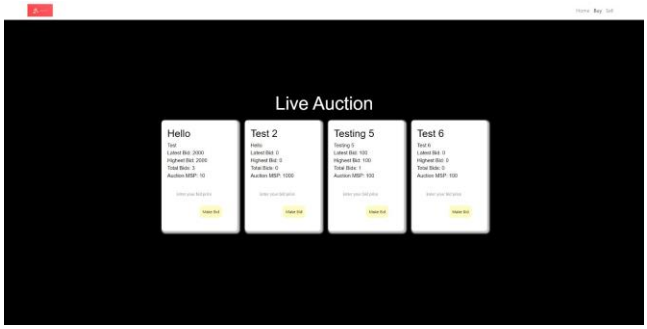

Fig. 3. Items Page

Fig 2, 3 and 4 represents the home page, bid page and seller page of Auctionify. Home Page shows the navigation bar prominently displays two key options: ”Buy Items” and ”Sell Items.” These options are designed to appeal to both buyers and sellers, providing a seamless experience for both parties. Users who wish to browse the items currently being auctioned can simply click on ”Buy Items,” while users who wish to list their own items for auction can click on ”Sell Items.” In addition to the navigation bar, the home page also provides an overview of the auction system, highlighting its key features and benefits. This information is presented in a clear and concise manner, using graphics and bullet points to make it easy for users to understand.

The bid page for the auction system built on blockchain also provides a clear and concise display of the items that are currently being auctioned. Each item is listed along with a clear image, a description, and the current highest bid. The page also shows the time left for each auction, creating a sense of urgency and encouraging potential buyers to act quickly. The current highest bid for each item is prominently displayed, providing a clear indication of the current market value of the item. This information is updated in real-time, ensuring that buyers have the most up-to-date information on the status of the auction.

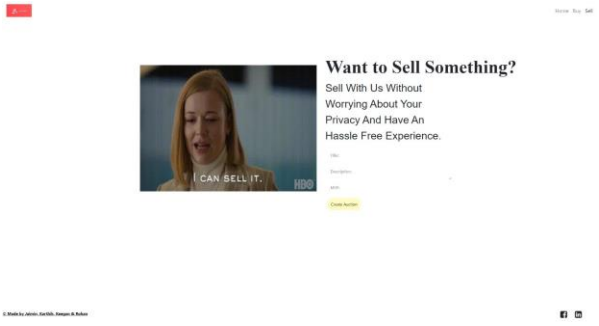

Fig. 4. Seller Page

The sell page is primarily designed to offer a seamless and user-friendly experience for sellers to sell their items through an auction system built on blockchain. It provides an intuitive interface for sellers to set up their auctions, specify the starting price and reserve price, and choose the duration of the auction.

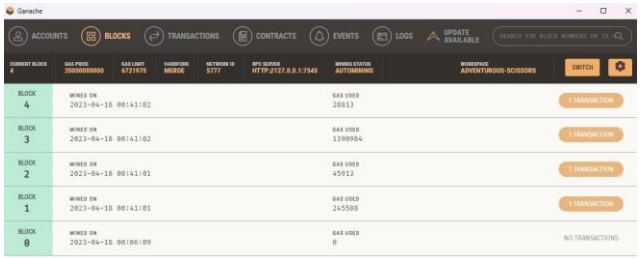

Fig. 5. Block Creation History

Figure 5 shows the Block Creation History. When a transaction is sent to Ganache, it is validated and then added to a new block. The new block contains a reference to the previous block, creating a chain of blocks that make up the blockchain. Each block contains a unique block number, timestamp, hash value, and a set of transactions.

Ganache generates a block every time a transaction is executed on the network. Each block contains a set of transactions that have been executed, along with metadata such as the block number, timestamp, and the address of the miner who generated the block. The block generation history in Auctionify represents a record of all the blocks that have been generated by the Ganache blockchain during the development and testing of the platform. This history provides developers with a detailed record of the network activity, including transactions that have been executed, the order in which they were executed, and the addresses of the accounts involved in each transaction.

Figure 6 shows the Transacion History. The transaction history in Auctionify represents a record of all the transactions that have been executed on the platform. Each transaction contains information such as the sender and recipient addresses, the amount of cryptocurrency transferred, and the timestamp of

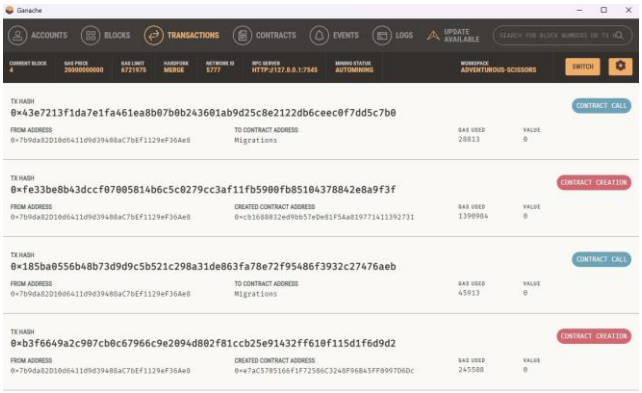

Fig. 6. Successful Transactions

the transaction.

The transaction history is stored on the Avalanche blockchain, which provides a secure and transparent ledger for recording all transaction activity on the platform. This information is accessible to all users of the platform, ensuring that the auction process is transparent and tamper-proof.

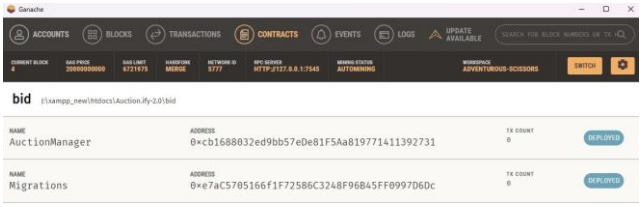

Fig. 7. Contracts Deployed

Figure 7 shows the deployed contracts on Ganache. Smart contracts are used to facilitate the auction process and manage the flow of funds between buyers and sellers. These contracts are deployed on the Avalanche blockchain, which provides a secure and transparent ledger for recording all contract activity.

The deployed contracts in Auctionify consist of a set of smart contracts that are responsible for managing the auction process. These contracts include the Auction Manager contract, which is responsible for creating and managing auctions, and the Auction Bidding contract, which is responsible for handling bids and managing the flow of funds between buyers and sellers.

Each contract contains a set of functions that define its behavior and enable users to interact with it. For example, the Auction Manager contract includes functions for creating new auctions, setting the starting and ending times for each auction, and managing the list of items available for auction.

The Auction Bidding contract includes functions for placing bids on items, transferring funds between buyers and sellers, and managing the finalization and settlement of each auction

The further is the list of features of our system

- Ease of Use: The platform is designed to be user-friendly and intuitive, with a clear and concise interface that allows users to easily create and manage their auctions. The use of the Drizzle framework also makes it easy to integrate with other blockchain-based tools and platforms.
- Security and Transparency: The use of the Avalanche network provides a high level of security and transparency, ensuring that all transactions are secure and immutable. This creates a sense of trust and reliability for both buyers and sellers, and can help to increase participation in the platform.
- Customizability: The platform allows for a high degree of customizability, with users able to set their own auction parameters such as starting price, reserve price, and auction duration. This allows for a wide range of items to be auctioned, and can help to attract a diverse range of buyers and sellers.
- Integration with Cryptocurrencies: The platform supports the use of cryptocurrencies for payment, allowing for fast and efficient transactions without the need for traditional banking institutions. This can be particularly useful for high-value items, where traditional payment methods may be slow or cumbersome.

Analysis of our system is discussed below:

- User Base: While the platform has the potential to attract a wide range of buyers and sellers, initially it would have a relatively small user base. This can limit the number of auctions being conducted on the platform, and may make it less attractive for some users.
- Marketing: The project could benefit from increased marketing and outreach efforts, in order to attract more users and increase participation in the platform. This could include targeted advertising campaigns, partnerships with relevant organizations, and other marketing initiatives.
- Technical Limitations: While the Drizzle framework offers a high degree of flexibility and customizability, it may also have some technical limitations that could impact the scalability and performance of the platform. This could be a potential area for further development and optimization.

VI. Conclusion

The limitations of the traditional bidding system could easily be overcome by our Blockchain based online bidding system. The major advantage of using blockchain is the privacy that users get by simply being identified by his/her wallet id without revealing his/her personal details. Thus, our system is built with the vision of being secure, anonymous, and transparent online using blockchain. The literature review's experiments infer work on optimization of transaction rates. The aim is to create an efficient process such that the transaction time reduces and, eventually, the transaction rate per second increases. Our system will be most suitable for bids

on trending NFTs and such soft assets. The proposed system consumes ether, it needs to be worked on to create a method such that ether consumption is minimal.

VII. Future Scope

In future, we can create an app for this project. Also we can have a collaborative recommendation system implemented in the system allowing users to view frequently visited bids also showcase live bids the user would be interested in. We can also reduce the gas fee that would be cost by the user to place each bid. Few more future scopes for Auction System would be the integration of artificial intelligence (AI) to enhance the user experience and improve the efficiency of the auction process. With the use of AI, Auction System can analyze user data and preferences to provide personalized recommendations to buyers, thereby increasing the chances of successful bids. It can also provide sellers with insights into market trends and pricing, helping them to set optimal reserve prices and maximize their profits. Implementation of cloud storage for storing and sharing multimedia assets related to the auctioned items. By integrating with cloud storage services like Amazon S3 or IPFS, system can allow sellers to upload images, videos, and other media files related to their items for display to potential buyers. This would improve the user experience of the platform, as buyers can view and evaluate the items more effectively.

References

[1] S. K. Shah, A. H.M. and P. Jayarekha, ”Bidding System using Blockchain,” 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), 2020, pp. 1-5, doi: 10.23919/ICOMBI48604.2020.9203438.

[2] X. Li, ”BCES: A BlockChain based Credible E-Bidding System,” 2020 IEEE 6th International Conference on Computer and Communications (ICCC), 2020, pp. 2415-2421, doi: 10.1109/ICCC51575.2020.9345176.

[3] P. Manimaran and R. Dhanalakshmi, ”Blockchain-Based Smart Contract for E-Bidding System,” 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), 2019, pp. 55-59, doi: 10.1109/ICCT46177.2019.8969042.

[4] Y. -H. Chen, S. -H. Chen and I. -C. Lin, ”Blockchain based smart contract for bidding system,” 2018 IEEE International Conference on Applied System Invention (ICASI), 2018, pp. 208-211, doi: 10.1109/ICASI.2018.8394569.

[5] B. Liu, Y. Yang, R. Wang and Y. Hong, ”Poster: Privacy Preserving Divisible Double Auction with A Hybridized TEE-Blockchain System,” 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), 2021, pp. 1144-1145, doi: 10.1109/ICDCS51616.2021.00128.

[6] M. Shah, M. Shaikh, V. Mishra and G. Tuscano, ”Decentralized Cloud Storage Using Blockchain,” 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), 2020, pp. 384-389, doi: 10.1109/ICOEI48184.2020.9143004.

[7] V. A. Kanade, ”A Blockchain-Based Distributed Storage Network to Manage Growing Data Storage Needs,” 2021 3rd International Conference on Signal Processing and Communication (ICPSC), 2021, pp. 365-368, doi: 10.1109/ICSPC51351.2021.9451813.