A Modified Hybrid Blockchain Framework for Secured Data Transaction

P Bhanupriya*, Sabitha Gauni, K Kalimuthu, and C T Manimegalai
SRM Institute of Science and Technology, Chennai, Tamil Nadu, India
Email: *bp1869@srmist.edu.in

Abstract. Blockchain has recently become an essential tool which enables sensitive cloud services without the need for central confidence. For example, several different cryptocurrencies were permitted with public blockchains. Unfortunately, confidential details may be exposed on current public blockchain and smart contracts implemented there. Whilst some continuous work is under way to resolve these insecure knowledge leakage problems using advanced cryptography, they need major improvements on current and common Blockchain technology such as Ethereum and are typically costly in computing. On the other hand, blockchain applications were proposed to allow the data exchange among the pre accepted nodes/participants to be more efficient and privacy-preserving. While private blockchains respond to certain challenges of privacy by allowing only the particular community of participants to view sensitive data, they do not allow public transparency for communications because businesses are accepted by a known number of users also cannot be freely viewed. One natural problem is whether we should use public and private Blockchain networks in order to allow effective, improve privacy and accountable applications in view of these findings? In this work, we try in connection with digital auctions to face this challenge. In specific, we provide a newly designed blockchain architecture combined with private and open blockchains which enables sensitive offers to be opened up on a secluded blockchain so solitary the merchant can study the offers, and none of others. We also use shared blockchains to report the public sale winner and to make transfers responsible. Moreover, we demonstrate how we can promote sincere activity among auction participants by using intelligent contracts on public blockchains. Our detailed analytical findings suggest that it's more cost effective compared to pure public auction implementations based on blockchain.

Keywords: Secured Data Transaction; Blockchain; privacy-preserving; cloud; cryptocurrencies

1. Introduction
Blockchain applications have recently been extended to several significant topics, from crypt coins to cryptographic keys. Cryptocurrencies arose as the early crucial use of the blockchain technologies by eliminating the need for the central-based trust firm for financial transactions. Two separate blockchains have emerged as blockchains technology has evolved: public/permission-free blockchains, besides private/permission blockchains. Community blockchains inform any contributor of all transactions and of the blockchain data held. Although this is beneficial in some applications, such as cryptocurrency, in applications such as healthcare that protect data protection, it poses major challenges.

A variety of solutions have recently been discovered which aim to resolve these data security issues using advanced encryption techniques [1]. These implementations are either too costly in order to
enable the general implementation of smart agreements [2] or require major modifications in fundamental blockchains such as Ethereum [1]. Around the similar time, private blockchains, including Hyper Ledger Material [3] have been built in order for developers to be able to use more effectively and privacy-saving methods for screening applications. For example, a private blockchain to enhance exchange management may be generated by multifunctional entities participating in a global trade transaction. A secluded blockchain in this case may enable quicker care (e.g., mining need, etc and greater confidentiality (i.e., only the contributing gatherings can see the potentially delicate data). These secluded blockchains sadly do not permit public transparency. For eg, no trades and/or relevant currency fluctuations can be shown to the public. The lack of public transparency for certain proposals may be a concern. Public transparency, for example, may improve public interest and likely minimise bribery and nepotism by way of essential government contract bids. Ideally, solutions to safeguard the privacy of individuals and allow public transparency without major blockchain changes are required.

In this article, we aim to tackle some of the above-mentioned problems by merging pub licences with private blockchains to allow for improved anonymity and accountable Auctions. Our implementation uses common cryptographic methods in the public blockchain to preserve information on accountability while restricting the volume of information revealed in sensitive terms. The protected discovery of an auction winner is used of private smart contracts based on blockchain, and, eventually, public smart agreements grounded on blockchain have been used to declare an auction winner and sanction someone who attempts to cheat.

As far as we are aware, this is the primary project to merge community besides private blockchains to allow confidentiality and accountable auctions. We are offering a modern hybrid Blockchain Architecture for auction site work, which will summarise the major contributions. The suggested architecture prohibits the provision of confidential offer information and provides for the actual auction results to be accountable to the public. We empirically prove that the suggested hybrid architecture makes the auction of a pure public blockchain-based public auction more computerised efficient and less costly (i.e. reduced gas usage on a public blockchain such as Ethereum). We demonstrate that the approach provided only provides the person run the auction with potentially confidential bid information. In return, this eliminates the loss of private knowledge. We also prove that any dishonest group can be prosecuted with public intelligent treaties on a monetary basis.

2. Related Work

Study that integrates encryption primitives into a decentralized directory has been considerably carried out. The blockchain was also analysed and redesigned to ensure that transactions were safe and committed more efficiently. A significant effort is also made to build multifunctional applications. In this section, we explain the ideas we have proposed and address how our system design meets some excellent problems and helps make the blockchain simpler and safer for auctioning. The addition of encryption in intelligent contracts is a potential way of protecting anonymity, which is a means of sharing data between different parties. The Hawk [2] article, which explores a blockchain paradigm of steganography besides transactional anonymity, implements privacy that safeguards intelligent contracts. To achieve this purpose, it uses zero awareness proof. However, it is incompetent since, whenever a business is created, it must pass finished the cryptanalytic primitives which in the real world take far longer.

With the aid of homogeneous encoding to safeguard the authenticity of "secluded" operations, Ma et al build non-interactive zero-knowledge (NIZK) evidence [4]. These proofs aim to mask some transaction balance and payment number by making NIZK proofs created with efficiency of time, but to the detriment of longer proofs. Zkledger [5] is another means of protecting participants' personal data by using cryptographic methods to conduct an accurate audit with rolling caches. This removes the need for an investigator who can view any transactions from a third party.

Zero cash [6] is a framework that encourages the use of nil information facts by the Bitcoin network in maintaining the transaction's safety. In comparison, our protocol and generic encoding
strategies used in current blockchains are powerful and simple. Instead of such efforts, another network that guarantees anonymity, security and high-quality smart contracts, the newly proposed Ekiden[1]. It deals with the problem of anonymity and low performance of current blockchain books by integrating their personalised trustworthy execution environment (TEE) with Intel's SGX architecture.

The detail that it depends seriously on a TEE which is an obstruction exposes it to a host of vectors of attacks. One such attack is that an assailant cans effectively furnace blockages and disables legitimate dealings when the TEE and blockchain have gotten out of synch. Recently, off-chain measurement has emerged as a direct way to increase community blockchains performance. For instance, a bitcoin flashlight system [7] tries in the public leader to solve the problem of reported delays by launching a system of payment system channels or off-blockchain business channels. It deals with the security issues associated with off-chain dealings by means of a new confusion to permit meltability besides public transmission in the case of a disco operative time clock’s member. Xinfin [8] emphases on the construction of a mixture blockchain using the quorum architecture of Ethereum which creates secluded channels across the community blockchain. They push the minimum blockchain to boost transaction performance and build a low-weight consumer who communicates with the system natively. The Xinfin architecture is therefore a concern because it places tremendous trust in third parties, such as the system boss, the clever agreement director besides the manager of the administration.

Enigma suggests a common solution to the problems of privacy [9]. It makes transfers across the network from peer to peer while privately owned records. To maintain the network access, identity and event logger to a tamperproof link, an external blockchain is used. The system's correctness and justice were proven by the deposits, responsibilities and incentivised activities. Users may exchange their personal information using cryptography through this framework. In Strain [10], secure reselling was considered. How-ever they use zero awareness proofs to preserve the privacy of auction with enhanced performance, comparable to earlier studies. They strive to be successful using a poor adversary paradigm with low blockchain latency. The Ethereum simulated machine used on a mix of private besides public organization is a perfect case where dispersed parties must compete in the process of bidding for an object.

3. Proposed System

Our suggested hybrid auction mechanism involves two blockchains – a private one besides a public one besides three forms of auctioning performers as shown in Figure 1. A player consists of an auctioneer, numerous auctioneers and electors who vote in case of suspicion of a contractual infringement. The auctioneer is hosting the proprietary blockchain. The auctioneer is either the intermediary or a link between the private and the public. The auctioneer shall post to the public chain the details of the privately owned auction. The members of the auction will still enter as voters in the event that any individual of the scheme is accused of breaching it. The voters also confirm if the public chain details the auctioneer has released is accurate. In the sense of this referendum, alleged cheaters should be disciplined and sincere conduct promoted.

The smart contract is implemented using a device parameter, which induces no delay. For starters, we assume prefunded accounts to circumvent interruptions caused by withdrawal when a public sale is launched. The dilemma is often set to actual low values, so that transactions can be deduced more easily. The personal and the social blockchains are attached to the two chains by a module. The sockets establish a link between the chains to essentially build a connection layer between the two chains.

The bitcoin key is a blockchain that's almost enabled which ensures that no trustworthy third parties or a member-ship service provider will enter the blockchain? The auctioneer is nevertheless an individual that will allow a candidate to enter the scheme. The decision is taken with the approval of all parties on the private chain. If the decision has been taken and the proposal accepted it is possible to change the admission control policy on the secluded chain by passing information on the system.
connection to the prospective contributor and to enable the participant to communicate with the system. These data are used to access the network by the active user. While in the network, the newcomer can begin offering through the private chain with the Smart Auction Contract.

Any player in the structure interacts both with the personal and the public networks. Each actor keeps a different chain account because the chains are both exclusive. So there will be two accounts for each player. The public blockchain account address cannot be configured and is automatically produced when the explanation is created. In a secluded blockchain, though the auctioneer who initialises the chain will default on the account address. For saving several account addresses referring to the same actor, a confusion table in the form of the key-value pair is rummage-sale. The participants who affirmed their interest in the auction must first be aware of the auctioneer in order to update the hash table with participant information and addresses. Whenever the member chooses to quit the scheme, the hash table entry with the required address will be removed and the participant will essentially not communicate with the intelligent contracts on the two networks. In command to allow our infrastructure – the sale contract, the Public Announce agreement, and the System agreement – there are three smart contracts in place [11].

The contract is executed by the auctioneer on the bitcoin cloud. The blockchain public housing is two intelligent contracts and Congress-Factory. The former is used to disclose their respective auction deals to the first and second highest off errors [12]. Lastly, a convention is created in cases of an infringement. Both parties must always settle on a declared winner of the auction. If not, then the System is used to establish a convention. This begins with a voting process between the competitors to validate that such parameters are valid. Validating the findings displayed by the auctioneer is carried out using different approaches. One of them is to track the principles of loyalty. The participants sell the products in the form of promises to ensure the auction is safe. The System tracks all deals in the form of obligations during the bidding process. The Congress-Factory shall be immediately reviewed if a violation is detected and required to give its details to the vendor. Confirming that the auctioneer committed an infringement, the System validates it with the evidence it possesses.

To be part of the hybrid chain, the individual participants deposit ether into the System. The accuser needs to apply a deposit to System in order to report a violation of the hybrid network. System only starts a congress deal for voting purposes until a fee is paid. The explanation for this is that if the alleged violation is false the accuser’s money will be shared between the System and the convicted party. It discourages misrepresentations and advocates true news. If the violation mentioned is valid then the accused in System owes all the money to all the other competitors and the violator needs to forfeit his or her rank as an auctioneer and is deleted from the scheme until he/she deposits more money into the System.

Each participant carries out a wrapped bid auction with the aid of disconnected conversion. In the form of promises, participants make deals, but a temporary timer runs background continuously to set the overall limit to the period of time reserved for the object being auctioned. When the timer is running out the auction sees this as a form of completion of the auction and starts a public blockchain process for publicizing the winner. The auction begins a "Revelation Phase" which enquires the participants about the values and random numbers that are used to produce the obligations to state the champion in the community blockchain. The auctioneer shall verify if the values used for commitments conform to the commitments produced. After accuracy has been checked, the winner shall be declared, otherwise the auctioneer shall be penalised. The bidding process consists of two main phases: the commit stage and the disclosure phase.
Applications and disclosures are transmitted by the auctioneer by a private chain to each participant. When any person receives the email, he or she will choose to send an auction and participate. Each participant uses the adapted one-way variation bit pledge procedure for protection and privacy purposes to encompass their offer into a hash value. Because of its immutability, this hash value is registered in the public chain. When the auctioneer finishes the auction stage and begins the disclosure process, the auctioneer must give an invitational disclosure to the auctioneer over the secluded chain, with the valuation and the random number employed. After a process of revelation, the auctioneer will recover all promises from the public directory made by any party and will immediately search and sanction those involved who have not submitted their disclosure or have forwarded fraudulent disclosures using both private besides community intelligent agreements. The champion (top buyer) is later announced over the public chain, and the additional maximum auction-goer of the auction.

4. Results and discussions
As shown in Figure 2 public chain cost for both personal and open blockchains, The Virtual Machine Ethereum is used. The private blockchain is built on the Amazon Web Services (AWS) Online Computing Cloud instance in a virtual private over multiple hosts. For nodes to explore each other, Port 30303 is revealed. The public blockchain is Ropsten [13]. A JSON-format genesis file is written for a private blockchain[15]. This file is a custom genesis file containing information on the gas cap, chain id, complexity, nonce and most notably, pre-funded balance account ids. The genesis block is the first block to be generated with this genesis state file in the blockchain or block 0.
The gas cap is the largest quantity of gas to be used by any secluded chain operation. This is set to a in height value, a normal 2100000, such that the auction doesn't get restricted so the value transacted will ultimately be huge if the gas cap is set too small. This is the standard 2100000. The dilemma is set at a low level, so as to prevent spending time coming up for transactions to be undermined.

The goalmouth is to render private chain estimates as easily as possible by eliminating any delays induced by transaction mining. For initial bidding, each participant's address will be pre-financed with 100,000 petrol. 1,000,000 petrol is delivered to the auctioneer. The auctioneer supplies 50,000 gas for initial operations for each new member who joins the private chain. The user is forced to become a miner after he has entered the scheme. Via a JavaScript web platform, the participants create commitments offline[14].

The participants then submit the obligations to the auctioneer using the web3 programme. The web3 programme calls on the method for a locked bid in the public sale contract used in the secluded chain. The party of miners is only for block formation participants. Each participant must become a private chain coal miner. Each contributor can have their explanation address constructed to be a coal miner in the secluded chain such that each participant behaves as a miner. Since, however the private chain does not have real "ethers," any participant does not have an opportunity to become a resource mine, which would drain their computing resources. Furthermore, as a competitor joins the private chain, it lacks ample gas to engage in the bidding. It has first to develop a miner besides it begins collecting enough gas after a significant period of time to engage in a deal. Thus, we set the system
form in the system as the amount of Ether required for participation in transactions is prefunded by each participant. On acceptance of the private chain, each participant shall become a miner. Since the fallouts shown, we container conclude that the hybrid blockchain auction system is much quicker and cheaper than the entire public auction system based on blockchain. The number of transactions verified in time for the composite chain vs. the whole civic chain has also been analysed. For each public chain transaction, 50-60 transactions on the hybrid chain are verified. This means that the time has been significantly shortened by at least 2000% and productivity improved by 5000%. In this scenario, we neglect the smart contract, as the contracts are implemented in both architectures and will illustrate the same degree of efficiency and gas usage. The offers of participants have been registered during the revealing process.

The first bid for each participant is higher, but subsequent bids are constant. The system database is updated with the details of the current bidder, which requires a public address of the applicant, if a new bidder is introduced to the system. In case of additional proposals by the same tendered, because information of the tenderer is already contained in the scheme, the contract status does not modification with new data other than the amount of the tender promise. The higher the number of accusers the more gas it is required to complete the violation decision as the other player (participant / auctioneer) believes that any auctioneer would violate. When an auction expires, a new Congress deal may be produced if a member discovers a violation. If the Figure 3 shows only one participant suspects a violation, it takes 1.02e+06 steam. If more than one contributor assumes a violation, each Congress agreement's gas rises linearly. If, 10 accusers suspect an infringement, the total gas used for a single infringement decision increase.

5. Conclusion
Data security becomes an important problem, provided that blockchain technology gains importance as a distributed storage facility. Present research is being carried out in this field with respect to sophisticated computer-intensive cryptography. We deliver novel hybrid architecture, allowing improved privacy accountable auctions where confidential offers are opened for payment and transparency in a private blockchain and public blockchains. A broad spectrum of uses, including auctions for digital asset interactions, the exchange of PII, real time data recording and notarization, can be used for the hybrid blockchain architecture. Payment transfers can be performed on the public chain for digital asset trades and the sale of digital possessions on the secluded cable, allowing private owning and exchange information on individual assets. The PII can also be shared using our hybrid solution. Public de-tails such as first, last, race etc can be exchanged with institutions like Govt. Public-chain officials though private information can be exchanged via the private-sector chain, such as Social Security Number (SSN), address in addition passport number. As the hybrid blockchain is stored in the PII receiver, mixing the private specifics of the network with public chain particulars which be checked in contradiction of the official foundation, besides the sender's account is penalised for the implementation of transparency if there is a failure. The hybrid blockchain can likewise be used as solicitor facility with authorized leaflets signed besides submitted through the private chain through the 'trusted' addresses besides the public chain for payment / approval.

References
[1] S. Ma, Y. Deng, D. He, J. Zhang, and X. Xie, “An efficient nizk scheme for privacy-preserving transactions over account-model blockchain,” in Cryptology ePrint Archive, Report 2017/1239, 2017. https://eprint.iacr.org/2017/1239.
[2] N. Narula, W. Vasquez, and M. Virza, “zkledger: Privacy-preserving auditing for distributed ledgers,” in 15th USENIX Symposium on Net-worked Systems Design and Implementation (NSDI 18), USENIX Association, 2018.
[3] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and
[4] M. Virza, “Zerocash: Decentralized anonymous payments from bitcoin,” in IEEE Symposium on Security and Privacy, 2014.

[5] J. Poon and T. Dryja, “The bitcoin lightning network: Scalable off-chain instant payments.” http://lightning.network/lightning-network-paper.pdf, 2015.

[6] X. organization, “The xdc protocol technical whitepaper.” www.xinfin.org, 2017.

[7] G. Zyskind, O. Nathan, and A. Pentland, “Enigma: Decentralized computation platform with guaranteed privacy.” www.enigma.co.

[8] E.-O. Blass and F. Kerschbaum, “Strain: A secure auction for blockchains,” in European Symposium on Research in Computer Security, pages 87–110. Springer, 2018.

[9] Harsh Desai, Kevin Liu, Murat Kantarcioglu and Lalana Kagal, “Adjudicating violations in data sharing agreements using smart contracts,” in The 1st IEEE International Conference on Blockchain (Blockchain-2018), 2018.

[10] D. Lucking-Reiley, “Vickrey auctions in practice: From nineteenth-century philately to twenty-first-century e-commerce,” Journal of Economic Perspectives—Volume 14, Number 3—Summer 2000—Pages 183–192, 2000.

[11] “Ropstentestnet pow chain.” https://github.com/ethereum/ropsten, 2018. [Online].

[12] O. Goldreich, “Foundations of cryptography.” Vol 1, Vol 2, 2004.

[13] “Node.js.” https://nodejs.org/en/, 2018. [Online].

[14] “Go-ethereum.” https://github.com/ethereum/go-ethereum, 2018. [On-line].

[15] “Truffle.” https://github.com/trufflesuite/truffle, 2018. [Online].