IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13354

Distributed e-Tendering System using Escrow-Account

Sri Venkat Chennu[1], Aneesh Gonu[2], Kiran Manukonda[3], Babu Naik Mudavath[4]

CSE (IoT, Cyber Security including Blockchain Technology), VVIT, Guntur, India[1]

CSE (IoT, Cyber Security including Blockchain Technology), VVIT, Guntur, India[2]

CSE (IoT, Cyber Security including Blockchain Technology), VVIT, Guntur, India[3]

CSE (IoT, Cyber Security including Blockchain Technology), VVIT, Guntur, India[4]

Abstract: The process of tendering is generally utilized by governments and businesses to source goods or services from manufacturers or service providers. Nonetheless, with e-tendering being the most commonly employed procurement method, there exist various security concerns. Blockchain technology offers a potential solution to address these security issues by emphasizing information decentralization and incorporating robust encryption within an immutable block-based framework for managing transactions. This article delves into the utilization of smart contracts (built on ethereum blockchain) in developing a decentralized e-tendering system. The paper is segmented into four key phases:
1.Tender Creation and Publication 2.Bid Submission 3.Bid Evaluation and Negotiation 4.Bid Selection .

Diverse algorithms are harnessed to execute each step. The security and transparency challenges are assessed and juxtaposed against the existing tendering process. The primary objective of this study is to establish an impartial, transparent, and publicly accessible tendering model. At the end of the bid selection we will add an Escrow account between two parties , where authorized work will be done between them . both parties can review their work . This will results in trust between two parties.

Keywords: Blockchain, Fair and Open Tendering Scheme, Smart Contract, E-Tender.

I. INTRODUCTION

Current E-Tendering systems are not ‘fair and open' meaning, that information is not shared with all stakeholders (Right to Information[1]). The information is released on ‘as they please’ basis, for example, - when a company is selected as a winner of a contract, other companies that bid on the same tender are not notified of why their bid was rejected and why a particular company was selected as a winner.

A company can get information related to it but it is a tedious process of getting this data. Even though auditing these documents is possible, evaluating the documents needs time. Apart from not being transparent, security is also a major issue for these portals, leading to fraud and manipulation of data stored in a centralized database [2],[3].If a hacker gets hold of this centralized database, bids can be leaked to competitors leading to major financial and strategic losses for a business [4]. Blockchain technology can be used to solve these security implications as it heavily focuses on the decentralization of information and is secured by encryption integrated with undeniable block-based architecture for transaction management. Hence, Blockchain and Smart Contract can be used as a transparent, decentralized and secured tendering framework that will facilitate bidders' oversight on portal functions and observe all the activities carried out by the tender portal. At the end of creation of bid there will be another smart contract at the end where it will increase the trust between two parties . This will improves the working or trust . Hence it will provides the security , transparent , trust among two parties .

II. BLOCKCHAIN CONCEPTS

A. Blockchain Explained:
Blockchain is based on the concept of decentralization [5]. In this case, the distributed database employs the concept of full replication i.e. each node has a full copy of a blockchain [6].

Whenever the blockchain needs to be updated because of a transaction, a process called mining takes place [5],[7]. A block consists of many transactions. A consensus protocol is used, andthe mined block is broadcasted to all other nodes

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

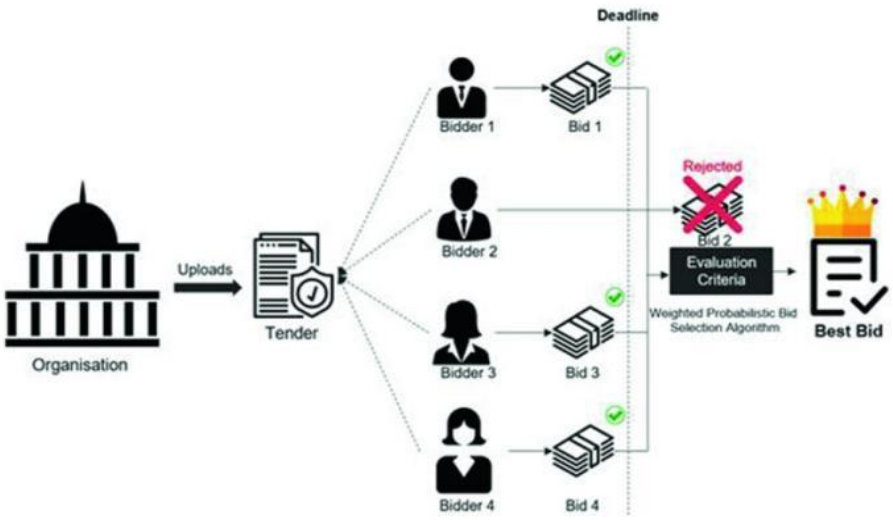
DOI: 10.17148/IJARCCE.2024.13354

[8]. These blocks will have a cryptographic hash in the header that relates to the previous block in the chain. If a block is manipulated, the hash associated with this block changes, and as a result, all the proceeding blocks should be re-mined which is not possible. In this manner, blockchain employs the property of immutability. How the blockchain is implemented and what consensus protocol is the core of blockchain can hold the information[10].

B. Smart Contracts:

Smart contracts are immutable as they are part of the blockchain,which is itself immutable. Hence, the agreement between thetwo parties cannot be changed once a smart contract is created with this agreement clauses[11]. Here Smart contracts will improves the trust between two parties . And each smart contract will have a definite role and they execute automatically once they are executed in the background.

III. SYSTEM DESIGN



A request for proposal is generated by the tendering entity, outlining details such as the description, bidding timeframe, etc. The tendering firm also submits documents like its financial statement and a certificate from RoC (Registrar of Companies) for potential bidders to assess the credibility and risk of default from the tendering firm before proceeding with their bids.

- The specifications of the tender are defined, including the demands and the criteria for evaluating bids.
- Once the tender particulars are settled and documents are submitted, the tender is transformed into a smart contract on the blockchain. The documents are securely stored in a database and accessible only to interested bidders.

1. Bidder Registration Process

The bidder enrolls asynchronously with the system, gaining access to all available tenders along with their details.

- The bidder then identifies a suitable tender to bid on.
- The bidder is furnished with the requirements of the tender and details of the tendering organization.

2. Bidding Process

The bidder places a bid on the tender by presenting a quote and quotation clauses. The bids are encrypted twice - first with the bidder's unique key and then with the tender's public key (blockchain address). Additionally, the bidder proves its credibility by providing its financial statement and RoC license, encrypted with the same key as before. Bidding is only allowed during the specified period, with no extensions once the deadline lapses.

3. Bid Evaluation

After the deadline, the tendering entity evaluates all bids by decrypting them with the bidder's key.

- The bid undergoes an assessment, scrutinizing the credibility and capacity of the bidding company based on the provided documents. The tendering entity can either accept or reject the bid.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13354

4. Negotiation Phase

The tendering entity may choose to negotiate with the bidder, sending necessary updates for consideration. Upon agreement, the bid is modified and resubmitted for review. Like the bidding process, negotiation transactions are encrypted for security.

5. Bid Selection and Transparency

The tendering entity selects the winning bid as the most favorable. All bid and negotiation details are shared with all bidders to ensure transparency.

6. Escrow Account Creation

Once the winning bid is chosen, a smart contract establishes an escrow account between both parties to foster trust. The bidder showcases their work to the organizer as proof of completion, receiving payment to carry out the paper smoothly. This will results in working of paper in a smooth way.

IV. METHODOLOGY

A. Tender Creation and Publishing

Algorithm: creating the tender

Procedure: createTender(tenderTitle,bidO,bidC,description,adress)

```
tdr ← new Tender()
tdr.manager ← \_address
tdr.title ← \_tenderTitle
tdr.description ← \_description
tdr.bid\_open ← \_bidO
tdr.bid\_close ← \_bidC
tenders.add(tdr)
```

The tender smart contract is created using a factory contract thattakes all the information required for creating a tender. The bidO corresponds to bid opening date and bidC corresponds to bid closing date. The documents are links to encrypted documents on the server. These documents include a balance sheet of the tendering organization and a certificate from RoC (Registrar of Companies). These documents are encrypted usingthe same key through which bids are encrypted. Once the deadline for the bids (bidC) passes, the bidder sends thesymmetric key for decryption to the tendering organization.

B. Bidding on Tender

Algorithm: Placing a Bid

procedure Bid(_adress,_quote,_quoteClass,_documents)

```
companyAdd ← \_address
quoteAmount ← \_quote
quoteClause ← \_quoteClause
documents ← \_documents
bidStatus ← “pending”
procedure
placeBid(\_adress,\_quote.\_quoteClass,\_documents)
placeBid(\_address,\_quote,\_quoteClause,\_documents)
greatStart ← now > bidO
lessEnd ← now < bidC
notComplete ← tenderComplete == false
notBidLimit ← bidders[\_address]==false
if greatStart and lessEnd and notComplete and notBidLimit then
bidders[\_address] = true
biddersCount++
bids.add(bid)
```

Initially, when the bid is created it is pending. After the bids are closed, the tendering organization can either choose to approve, reject or negotiate with the bidder.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13354

The bid is first validated for four conditions before it is placed:

1. It is checked whether the bid is placed after the bid openingdate.
2. It is checked whether the bid is placed before the bid closingdate.
3. It is checked whether the tender is not complete.
4. It is checked whether the bidder has already placed the bid once.

If any of these conditions are violated, the bid is rejected or else the bid is created using the details provided including company documents.

C. Bid Evaluation and Negotiation

Algorithm: Bid Evaluation and Negotiation

procedure approveBid(index)
bids[index].bidStatus ← "approved"
bids[index].bidStatus ← "rejected"
procedure initNegotiation(index)
bids[index].bidStatus ← "negotiating"

procedure
updateBidToNegotiate(index,_quote,_quoteClause,_address) validIden←bids[index].companyAddress==_address
greatEnd ←now > bidC
negotiating←bids[index].bidStatus=="negotiatin"notComplete ←tenderComplete == false
if validIden and greatEnd and negotiating and notComplete then
bids[index].quoteAmount ← _quote
bids[index].quoteClause ← _quoteClause

If the bid is approved by the tendering organization by evaluating the documents given by the bidding organization, the tendering organization can choose to negotiate with the bidder. The bidder can then update their bid to suit the requirements of the tendering organization. These transactions that happen during a negotiation between the bidder and the tendering organization are also encrypted using the symmetric key used before during bid placing.

The bid is updated if it satisfies the following conditions:
1. The sender of the update transaction is the same as one who placed the bid in the first place.
2. The bidC (bid closing) deadline has passed. The bidder cannot update the bid before the bid closing date.
3. The bid is in the negotiation state.
4. It is also checked whether the tender is complete or not. If thetender is complete then this request is rejected else the contract proceeds with the update request.

D. Winner Selection and Publishing Bids to Bidders

Algorithm: Select Winner and Publishing Bids

procedure selectWinner(index)
if now > bidC then
winningCompany ← bids[index].companyAdd
finalTenderAmount ← bids[index].quoteAmount
finalTenderClause ← bids[index].quoteClause
complete ← true
procedure getWinningDetails()
if now > bidC and complete then
return(finalTenderAmount,finalTenderClause,winnin gCompany)

procedure releaseBids()
if complete then
return bids

Once the negotiation phase has passed, the tendering organization has to select a winner to close the tender. It does this by calling the select winner procedure of the tender contract.This selectWinner function is restricted to the manager who is the one that created the tender smart contract on the blockchain. Hence, only the tendering organization can call this function.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13354

The selectWinner procedure checks if the bidC (bid closing) deadline has passed. It then updates the winning details by setting the winner's adders to the company address of the bidder.The final tender amount and the final tender clauses are also set using the data from the winning bid. The complete status is also set to true.

Once the tender is complete, any bidder can get the winner details consisting of quotation amount and clauses of the winning bid. The bidders can compare this information with their bids to evaluate where they lacked and what had gone wrong. The bidders can also demand all the transactions (Bids) that the tender has accepted to date. Hence, making the process of bidding and winner selection highly transparent and secure.

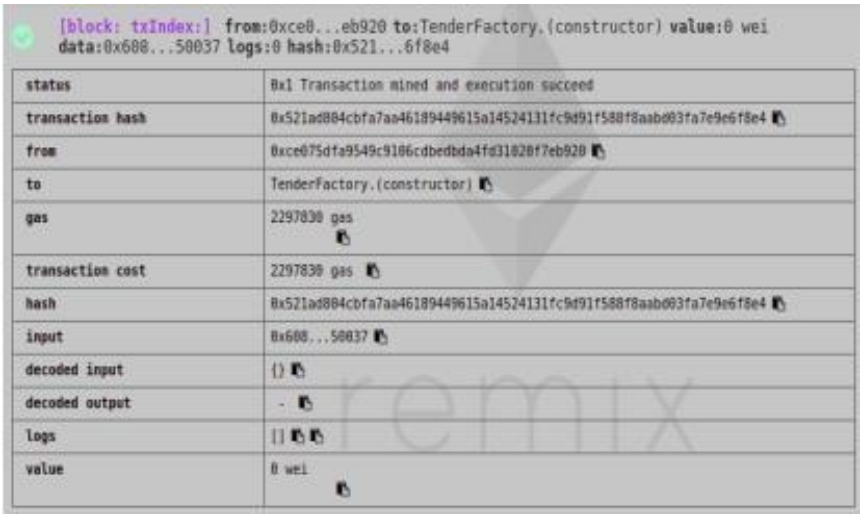
E. Escrow Account

After assigning bid to the bidder now the smart contract work at background and automatically it adds an escrow account between two parties this will result the trust between two parties , it will result smooth working of paper".

V. RESULTS

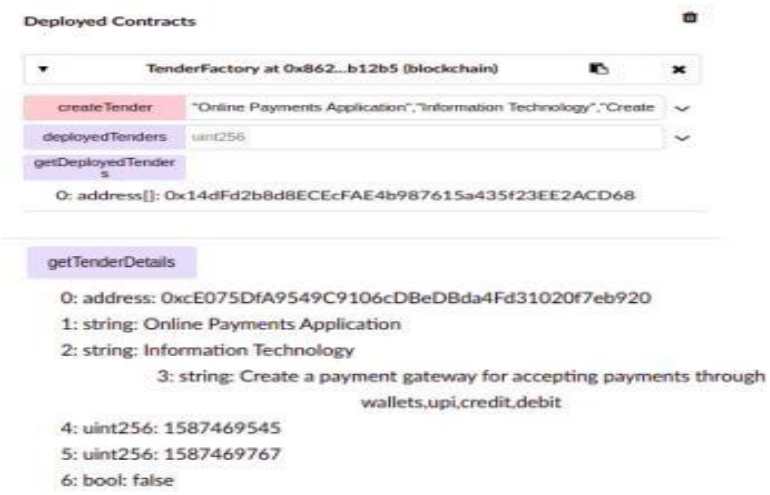
The Smart Contracts came into existence on the Rinkeby Ethereum test network through the utilization of web3.js and metamask.

1. Establishing CreateTenderFactory



The transaction noted in the table above represents the action taken on the blockchain for CreateTenderFactory.

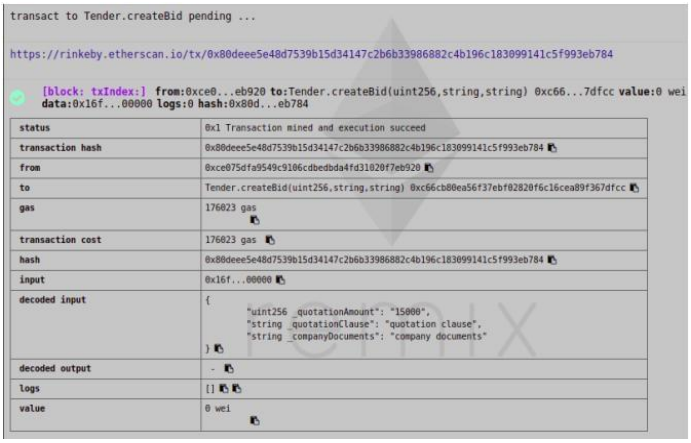
2. CreateTender Process



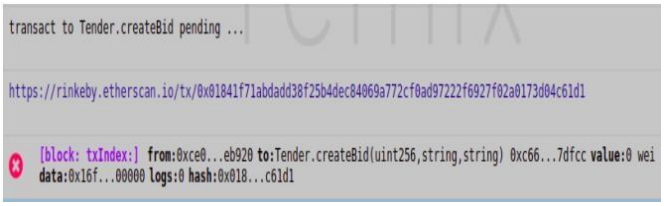
International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024
DOI: 10.17148/IJARCCE.2024.13354

An example tender got initiated utilizing the Tender Factory Smart Contract. The mentioned address 0x14dFd2b8d8ECEcFAE4b987615a435f23EE2ACD68 corresponds to the Tender named "Online Payments System." The initial uint256 signifies the bidO (bid opening) time inUNIX time, while the subsequent uint256 pertains to bidC (bid closing) time.

3. Initiating CreateBid

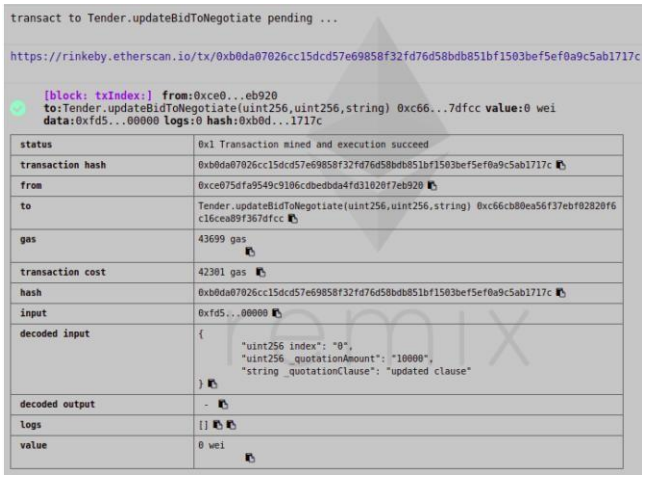


The transaction depicted in the table signifies the process executed on the blockchain for CreateBid.
By furnishing three parameters –
a)quotationAmount
b)quoatation clause
c)documents ,the bids gets generated.



The visual above portrays an unsuccessful transaction wherethe bidder endeavored to submit a bid post the bidC time.

4. Upgrading Bid to Negotiation Stage



The transaction record displayed captures the action carried out on the blockchain for UpdateBidToNegotiate. The tender initiator validated the bid and dispatched a notification along with comments to the relevant bidder for negotiation. The bidder responds with an updated quotation amount and quotation clause.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024

DOI: 10.17148/IJARCCE.2024.13354

5. Selection of Winning Bid

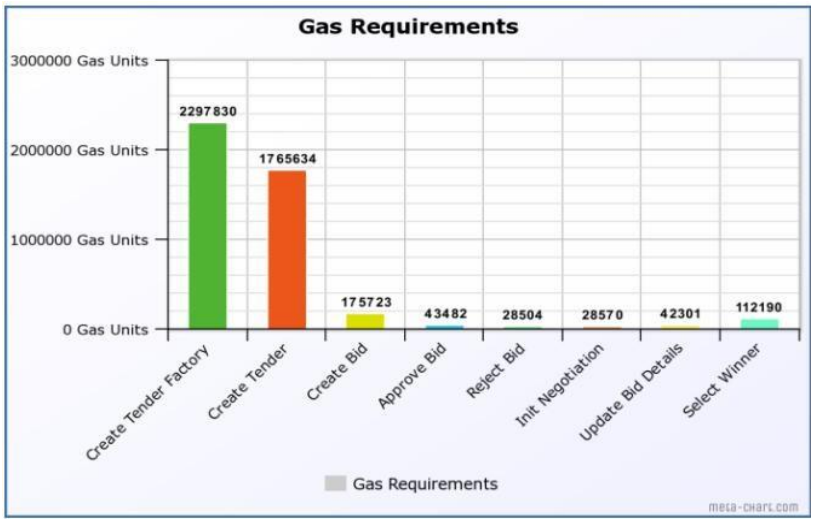
After Negotiation, the bid indicated above was chosen as the winner. Information concerning the winner can get accessed by all participating organizations involved in the tendering process.Additionally, all submitted and negotiated bids were made accessible to the participating entities.

Examination of Security and Gas Requirements Analyzing the security and transparency delivered by a Blockchain-centric tendering system

- The bids placed by organizations remain concealed from other bidders until the tender outcome is revealed.
- The blockchain network should uphold its security to prevent bidders from altering another organization's bid.
- The tendering entity lacks the authority to alter the tender prerequisites once the tender is live as such modifications could be biased towards a specific organization.
- The tendering organization remains uninformed about the bids until the deadline elapses.
- Because the bids are encrypted, miners on the block cannotintroduce any security risks into the system.
- The implemented Tender Smart Contract was rolled out onthe rinkeby test network of the ethereum blockchain leveraging metamask(A crypto wallet & gateway to blockchain apps) and web3.js library. For stakeholders to initiate a Tender Smart Contract, a distinct Smart Contract known as the Tender.

VI. GAS REQUIREMENTS: THE COMPLEXITY EXPLAINED

It refers to the complexity the function and is directly proportional to the complexity of transaction to the blockchain. If the gas used goes beyond the gas limit, the transaction is reverted! It is also related to the transaction fee. The higher the gas requirements are, the higher is the transactional fee to be paid.



The above bar-graph displays the gas requirements of the various sub-processes of the system. The createTenderFactory has the highest gas requirements, and the rejectBid has the lowest gas requirements? Which somewhat justifies the complexity of these processes! The gas value that was used was 1 GWEI aka Shannon, approximately 0.000000001 ether. The gas value corresponds to the amount the stakeholder is willingto pay per unit of gas required... The transaction fee is calculated by taking the product of gas requirements and the gasvalue. The above graph also shows the complexity of the various functions as complexity and gas requirements are directly proportional.

Keep in mind that understanding gas requirements is essential for navigating blockchain transactions smoothly!

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2024
DOI: 10.17148/IJARCCE.2024.13354

VII. CONCLUSION AND FUTURE WORK

When it comes to applications such as tender portals, where transparency, trust, and security are of foremost importance!!! traditional technologies and design patterns cannot be used as they put a threat to these requirements. As discussed earlier, there are many security requirements for a tendering framework that cannot be solved using just by using a centralized tender portal for creating and bidding on the contracts. The security requirements!!! and openness required from this type of application can only be solved by using fair, open, decentralizedtechnology such as Blockchain and Smart Contracts. In this paper, how such a system can be designed by mentioning various processes involved and their basic implementation and gas requirements of the tender smart contract is discussed. There are two further research directions, which are as follows - The Smart Contract can be made more secure by using more complex cryptographic algorithms for example. SHA-256 to encrypt its confidential contents. The use of blockchain is explored further in other government services. I hope that as a reader you can see the clear importanceof blockchain technology and its relevance in modern applications!!!!!!!! As always, the future holds many exciting possibilities when it comes to technology and innovation.

REFERENCES

[1]. "Efficient approach for Tendering by introducing Blockchain to maintain Security and Reliability." 2018 4th International Conference on Computing Communication and Automation (ICCCA). IEEE, 2018.
[2]. Pal, Om, and Surendra Singh. "Blockchain Technology and Its Applications in E-Governance Services."
[3]. Betts, Martin, et al. "Towards secure and legal e-tendering." Journal of Information Technology in Construction 11 (2006): 89- 102.
[4]. Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE international congress on big data (BigData congress). IEEE, 2017.
[5]. Pilkington, Marc. "Blockchain technology: principles and applications." Research handbook on digital transformations. Edward Elgar Publishing, 2016.
[6]. Wang, Wenbo, et al. "A survey on consensus mechanisms and mining strategy management in blockchain networks." IEEE Access 7 (2019): 22328-22370.
[7]. Cachin, Christian, and Marko Vukolić. "Blockchain consensus protocols in the wild." arXiv preprint arXiv:1707.01873 (2017).