Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 1708–1715

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

Securing Land Registration using Blockchain

Krishnapriya S, Greeshma Sarath

Department Of Computer Science And Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, India

Abstract

The current land registration process involves a lot of vulnerabilities and people uses it to cheat the common people and the government. This paper discusses about a secure land registry implemented using blockchain which works on the basis of majority consensus. By implementing the land registry in blockchain, the security issue is resolved to a great extent. The hash value calculated for each block will be unique as it is linked to the hash of the previous block. The algorithm that is used for hashing is SHA256. Along with SHA256, Proof Of Work(PoW) algorithm is also used which makes the information related to each transaction more secure. Message digest that is generated for each block is of fixed size and each hash represents a complete set of transaction within a given block. The proposed land registry blockchain network consists of 12 nodes which calculates the proof of work. Nodes are responsible for verifying a transaction, mining a new block and adding the new block to the blockchain. A total of 200 land transactions are recorded using the blockchain methodology which offers a tamper proof and updated version of land registry. Elliptic curve cryptographic algorithm is used for signature generation which is used for verifying whether the transaction is signed by the owner or not. Merkle tree is used for linking the transactions using hash and in turn reduces the disk usage. The proposed implementation of land registry using blockchain thus offers a 99% reduction in manual effort spent in record keeping.

Keywords: Blockchain; PoW; Hash; Merkle Tree

1. Introduction

Land registration involves collection of details like ownership and size of the property. Currently the entire process of land registry maintenance is too tedious since it involves safekeeping of large volumes of registers in written form. The main issue with the above-mentioned method of land registry maintenance is that any future reference that needs to be taken from these hard copies will involve too much labour. This process is time consuming. Current system is not secure since majority of the process is not transparent, system is slow, and selling a property more than once

* Corresponding author.
E-mail address: kpriya1994@gmail.com

10.1016/j.procs.2020.04.183

needs to be recorded accurately. Several approaches have been made to automate the land registry data maintenance by eliminating the process of keeping bookish records. This is initially done by storing the data in huge databases. But such a method is not efficient in terms of data security as the data contents are breached easily as data tampering can happen in case of poorly maintained databases.

Blockchain is a distributed ledger technology that keeps historical record of all transactions that have taken place across a peer-to-peer network [5]. Implementing land registry using blockchain helps in avoiding fraudulent activities thereby making the system more secure. Since it is difficult to duplicate the blockchain, implementing land registry using this technology helps in avoiding any illegal activities involved in land transactions. Contracts and ownership details are maintained in a decentralized method. It is easier to track the data transaction from the block chain implementation as it eliminates the need for physical intervention and thus improves the overall security for users of the system. Blockchain provides an opportunity to establish a strong system for digital identity. Using blockchain, each block in the network represents the data involved in a land transaction which includes details like property id, property number, owner details, transaction amount, mode of payment and last transaction details such as amount that has been paid for that transaction. By the proper use of encryption methodologies like SHA256 algorithm we can ensure data protection as well as systematic arrangement of data collected.

Implementation of applications using blockchain guarantees the quality of digital data that is being used. Privacy issues like data security breach and identity theft in digital domain are well addressed[7]. Present day technology uses password-based approach for accessing confidential information. Method of storage of data in insecure systems is also not reliable. The authentication schemes followed by blockchain based applications are based on stringent identity verification based on public key cryptography. Cryptographic method of hashing in blockchain checks whether the concerned transaction performed is related to the private key involved. Existing automated versions of land registries have their databases accessible to both commercial units and general public which ensures better documentation of transaction details. The local terrestrial maps and images of the areas under transaction are also maintained under these databases to ensure better surveillance of areas under sale. Elliptic cryptographic curve algorithm is used in this work for producing the signature for each block creating a pair of public private key. By using private key, hash of the transaction is signed thus making the transaction more secure. Merkle root is also calculated in such a way that it reduces the disk space, verifies and validates the transaction and is used for liking the blocks using the root hashes, so that additional validity for the blockchain can be given. Merkle root hash calculation is done by integrating the transaction from individual unit to a root unit so that the root contains the hash of entire blockchain. This merkle root hash is also included in land block so that the hash generation will be based on data like merkle root, elliptic cryptographic algorithm and land details which makes the transaction data more secure.PoW algorithm used in the blockchain helps in decentralizing the events. What the poof of work algorithm does is that when a new transaction occurs, it will first broadcast the transaction to every node in the network. Each node will calculate the PoW. One who found the PoW announces to other nodes in the network and will add that transaction to the block [6]. Difficulty factor is a parameter in PoW which helps to reduce the time for the creation of a new block, so that attacker cannot create or duplicate a block within this time. Always the longest growing chain is taken as the genuine chain.

Each block in the blockchain has a unique identification number and no manual correction or any type data tampering within the block is possible. Once a transaction is completed, it is added to the chain of blocks and if two owners have the same property it is managed with the block chain in a good and secure manner. Blockchain based land registration has the potential to increase liquidity, mitigate risk, and reduce costs, all of which would make property investment an even more attractive prospect. Currently, registration officers and other third party people who get involved in a land transaction deal often tend to make monetary benefits from the clients who are planning to sell the property. The offline method of initiating a land transaction often leads to issues like double spending. Blockchain helps mitigate the interference from third parties by offering a secure platform by means of transaction timestamp, stored within the block.

By implementing land registry using block chain we are addressing some of the challenges involved in data collection and storage, data confidentiality, authenticity of ownership details regarding source of money. It also incorporates the details regarding the funds provided by the financial institutions and the customers involved in land transactions like banker details and insurance providers. Details regarding the quantity of land purchased by a person or an enterprise is incorporated in to the block chain. It also includes representation of previous transaction details, information regarding financial institutions, protection of collected data, fault tolerance without data loss and details about how to

represent previous attributes. Maintaining land registry records is a tedious task. The process of referring back to all the transactions made from a land registry ledger is again a time consuming process. The illegal practices prominent in our society puts the integrity of data stored in the blockchain network under question. These issues have served as a source of motivation to innovate the land record maintenance.

This paper is organised as following. Section 2 describes about Related Works. Section 3 describes about Proposed solution which discusses about system architecture that has been adopted along with the proposed algorithm. Results are discussed in Section 4 and conclusions are drawn in Section 5.

2. Related works

In health field, medical history of each patient must be treated with utmost confidentiality. Blockchain technology is used as a distributed approach to provide security for the medical reports of patients. Security is implemented in a three phased manner which includes authentication, encryption[8] and data retrieval. Quantum cryptography and Advanced Encryption Standard (AES) encryption are used for ensuring a secure transaction for end users. Data retrieval is realized using SHA algorithm [1].

Financial institutions have also started adopting blockchain technology to avoid issues of network attackers and security based issues faced in online transactions. Digital currency called bitcoin ensures a peer to peer distributed and decentralised of payment scheme. Such a network offers added advantages of immutability, reduced charges imposed by third parties and faster transactions. Confirmation of an electronic payment is based on cryptographic proof and no third party is involved which offers a reliable payment platform. Issue of double spending is also avoided by means of distributed timestamp server which generated the computational proof of transaction in chronological order. Users can validate their identity by means of digital signature. Private key will be used by each user to perform a transaction while other nodes will check for the authenticity of the payment by checking the public key of the user. If an attacker wants to interfere with a transaction block, PoW of all previous blocks and all blocks after it must be redone along with suppressing the work of honest nodes. This cannot be done without the consensus of entire network and hence attacking a blockchain network becomes a tedious task [2].

When it comes to buying and selling properties, intermediate brokerage charges incurred in a huge sum. It is a wastage both in terms of time and cost. Blockchain based smart contracts ensures events being tracked in a sequential manner and an online ledger will be maintained for the same. Evarium system is a digital model for real estate investment which offers investors better cost reduction and greater profit sharing for commercial property trades. Smart contracts is a programming language based contract whose information is maintained mainly by means of service oriented cloud computing facilities. But developing smart contracts in the present evarium system is highly challenging as it requires a large set of cross dependant smart contracts that must not yield concurrency conflicts. Another problem is the issue of high distribution which is not addressed in the present work [3].

A blockchain based approach to collate and share academic data pertaining to students between universities and industries has been implemented in EDuCTX. Credits earned by students will be updated in a chronological order with latest education being updated in the new block created. Registered higher educational institutes act as nodes in the network who have the access to grant credits to each student after successful completion of their course work. PoW is implemented in EDuCTX using ARK blockchain platform. Language problems and admininstrative barriers faced by international students pursuing course in any foreign university is reduced to a great extent by means of the available data pool stored and shared in a secure manner. Once a student grants permission for an institute or potential employers to view their academic data, selection procedure can be completed with less hassle [4].

3. Proposed solution

The main objective behind the implementation of land registration using block chain is to secure the land transaction from attacker and to easily maintain records. Proposed solution also keeps a track of double spending which deals with scenarios related to the same land being sold multiple times to other clients. Since very less documentation and record keeping effort is required, the time required for performing a land transaction is also less.

The hierarchy involved in organisations involving land based transactions is shown in Fig. 1, which includes one main registration office and associated sub-register offices. Main registration office is linked to the sub-register offices

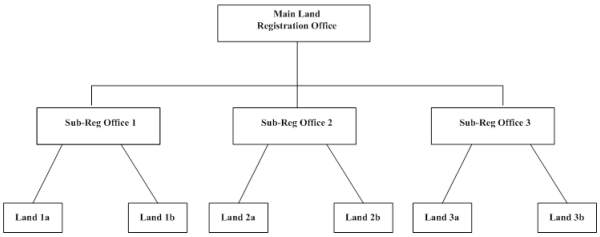

Fig. 1. Main Registration Office

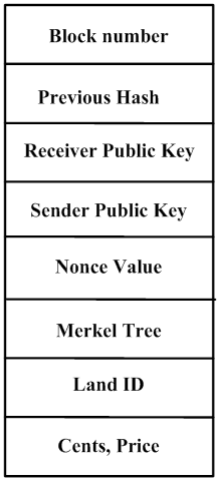

Fig. 2. Single Land Block

by using previous hash. Main registration office holds data related to original quantity of land present before sale while sub-register offices have data regarding amount of land which has undergone transaction and the remaining land that is available after a particular deal. Users having multiple lands in multiple states are also kept track off in the chain who are also linked with their respective land. Thereby it forms a chain of users with basic transaction related details like the previous and present owner of the property, actual price and selling price of the property along with property size.

The network is a single main chain, which has multiple blocks linked using hash. Each transaction is verified using Merkle tree. Fig. 2 shows the parameters available within a block associated with an individual user. Parameters at the input and output are used to track our transactions. Input is the point from which all transactions are derived and output is the defined as to whom we are selling the land.

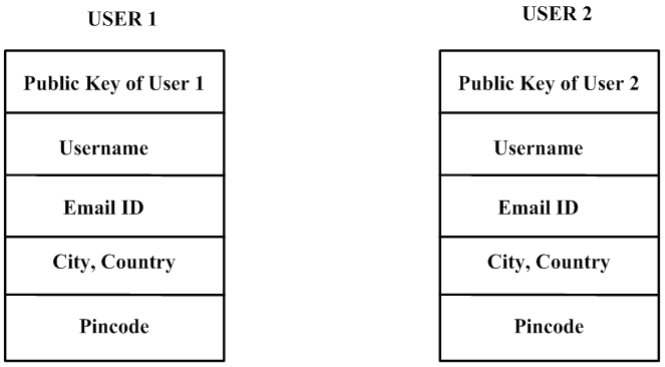

Fig. 3. Overall architecture for forming multiple chain

Fig. 3 shows the block level details pertaining to multiple users. Public key of each user will be available throughout the network in a distributed manner. Private key will be used by individuals to login to their platform so as to decide on how much land must be put to sale and how much money must be transferred to the customers involved.During a transaction, public key will be send throughout the network for consensus while the private key ensures that the user involved will be able to perform the transaction in a secure manner.

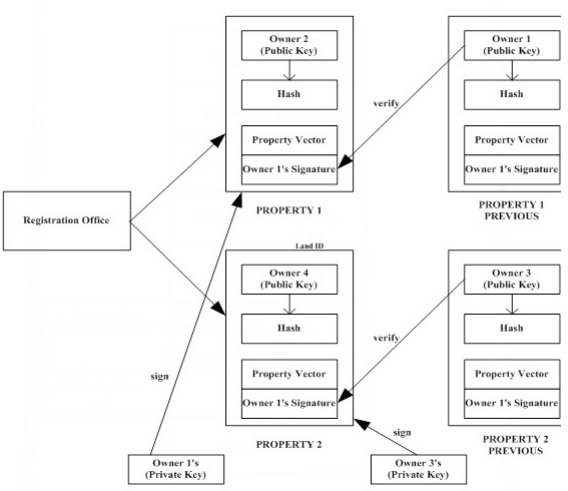

Fig. 4. Land Transaction

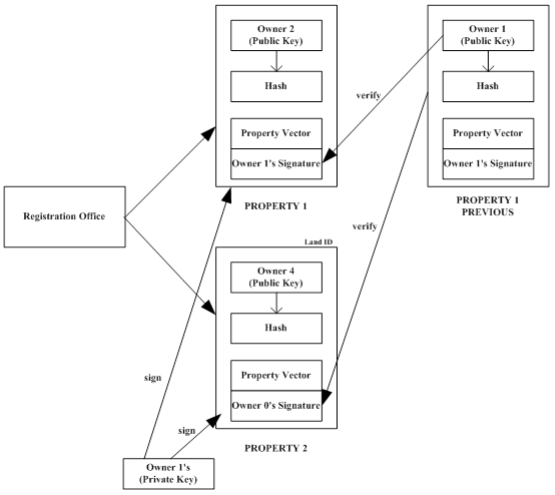

Fig. 5. Splitting of Land

Fig. 4 shows a land transaction that takes place between two users in a blockchain environment. The public key associated with the seller block will be available to the buyer in order to validate the authenticity of the transaction. Private key will be used by individual users to access their data within individual blocks which cannot be accessed by any other person. Fig. 5 shows the case in which only a certain portion of land needs to be sold off. The remaining property details remains intact within the user block which ensures reliability. In case of a property which is having more than one owner, transaction happens only when consensus from all the owners are collected. This avoids unnecessary hassle during a land deal.

Algorithm 1 Algorithm to sell and split land

```
function SendLandAlgorithm(senderPrvtKey, landid, cents, receiverPubKey, price)
    inputs = get all transaction pointing to the old land from the blockchain
    Find the specific land from the blockchain
    oldLand = getLand(landid,chain)
    create new Transaction t( PrvtKeySender, PubKeyreceiver,newland, oldland, inputs)
    sign the Transaction using the eliptic curve Algorithm for ed25519
      st = EdDSA(t,SenderPvtKey)
    check to see if the transaction was signed by the owner of the land itself.
    distribute the signed land for verification to the entire network
    if (st==signed by owner of land) then
        assert(verifyTranction(t.signature, land.owners)
    else
        return False
    end if
    if (user have land to sell) then
        newland=split(oldland,cents)
        compute hash for new land
        add land to blockchain by poW(newLand,3)
    end if
end function
```

Transferring and splitting of land is done by signing the land by the sender and broadcasting to entire blocks using Edwards-curve Digital Signature algorithm. To confirm that the transaction is signed by the owner itself, the public key

is distributed to the entire network which ensures its authenticity. To split a land, availability of property is checked for the concerned user. If available, based on PoW, new block will be created for the transaction by deducting the required land from the oldLand variable.

Algorithm 2 Algorithm for Proof Of Work

```
1: function ProofOfWork(block, difficulty)
2:     difficulty factor is 3 zeros in hash value)
3:     n = difficulty
4:     while (hash(block) != n) do
         1. increment nonce value by 1
         2. recompute hash
5:         repeat step 4
6:     end while
7:     Otherwise return the block with nonce value
8: end function
```

Second algorithm shows the PoW that is implemented in land registration process. It takes a block and computes its hash until it matches a specific condition. Here the predefined condition is that hash should start with three zeros. PoW is like a mathematical puzzle which tries to solve a condition based on difficulty factor. The nonce value is a random value which will change every time. More the difficulty factor, more secure the network. Algorithm checks whether hash of the block matches the difficulty factor. If not, the nonce value will be incremented in each iteration and the computed nonce value will be returned.

Algorithm 3 Algorithm to add new peer

```
1: function AddPeer(port)
2:     try to connect to a instance on the given port
3:     if (connection == TRUE) then
         add connection to peer list
4:         return True
5:     else
6:         return False
7:     end if
8: end function
```

Third algorithm shown is about adding the peer and establishing the communication. The network will be trying to connect to the instance of a given port. If connection is true it will be added to the peer list. Otherwise false connection will be reported. Other two algorithms are to process the message in which every block will get a copy of the latest chain.

Algorithm 4 shows how to transfer data to a node once a secure connection is established to a port. Broadcasting of message occurs throughout the network which ensures that attackers does not intrude in our system. Algorithm 5 shows how to process the data based on event type. Depending upon which chain is the longest, copy of that particular chain will be distributed to the network. The longest chain will be requested and will be checked for its validity. All the transactions are secured with a hash value and SHA256 algorithm is used for encryption purpose. By using this algorithm the hash value of the particular block is calculated and these values are used for linking blocks to make the list of blocks as chain.

Algorithm 4 Algorithm to transfer data to nodes

Input the eventtype indicating what event it is, message a JSON string representing the contents.

```
function BROADCASTMSG(eventtype, message)
    try to connect to a instance on the given port
    if (connection == TRUE) then
        for (for all peer in the peerlist) do
      send (eventype,msg) to the peer
        end for
    else
        return False
```

Algorithm 5 Algorithm to process message

1: Algorithm processmessage(eventtype, message)
2: if the eventtype is connection check to see if connected node has a larger chain if so broadcast(REQUESTCHAIN, null) to connected peer
3: if the eventype is REQUESTCHAIN Create a JSON representation of the blockchain and transmit it to the peer as broadcast(CHAIN, JSON data)
4: if the eventtype is CHAIN convert JSON data to object and check to see if the given chain is valid if the given chain is valid. Then replace the existing chain with new chain
5: if if the eventtype is BLOCK download the given block and check to see if all transactions in it are valid by checking the signature against the private publickey
6: else return false
=0

4. Results

Table 1 shows the comparison between the features implemented in the present work with the previous ones. This work shows a better advantage in terms of security features included and cryptographic schemes used when matched against its predecessors.

Table 1. Comparison of implemented blockchain features.

Works compared	PoW	SHA256	Elliptic Curve Cryptography	Merkle Tree
[3]	Yes	No	No	No
[4]	Yes	Yes	No	Yes
[5]	Yes	No	No	No
[6]	Yes	Yes	No	No
[This work]	Yes	Yes	Yes	Yes

Analysis is done to check the land transaction using blockchain technology in which using an invalid signature using we are trying to transfer the land from main account to a dummy account. A total of 12 nodes are present in the blockchain network with 200 valid transactions Port number and a trial output is created for the attacker node to run. With an Edwards-curve Digital Signature algorithm, private and public key pair is generated, showing that we are attempting for the attack. Block with signature is transferred to network with private key of the attacker and once this private key reaches every node, it verifies public keys of all other nodes and failure occurs as a result of PoW algorithm. Therefore every time an attacker tries to add a new block to blockchain it will lead to a failed scenario.

5. Conclusion

Land registration is implemented using blockchain which offers a more secure platform compared to its predecessors. A total of 200 transactions were performed which included 12 nodes. For the land transaction to be secure, an algorithm called SHA256 is used which helps to create a unique hash for each block. Once the hash value of a transaction is obtained it is not possible to obtain the original message. To retrieve the original message, trial and error or brute force methods are the only way. PoW algorithm is used to verify a transaction, mine the block, distribute the mined block to every node, and add the block to block chain. User information is stored in a trusted third party server which is signed by elliptic curve cryptographic algorithm. Advantages of this algorithm are high speed, independence of the random number generator and high performance. By using a user public key, it is possible to list all the land details under that user. Registration office page is also listed which contains all the details of users and the properties he sold and bought. By using difficulty level we have checked whether mining is happening in a secure manner. Merkle tree is used for validity and linking of the chain and to reduce the disk space. Proper testing is also done with multiple nodes which ensures a 99% reduction in manual effort spent in record keeping.

References

[1] Christo, Mary Subaja and Sarathy, Partha and Priyanka, C and Kumari, Raj and others. (2019) "An Efficient Data Security in Medical Report using Block Chain Technology." *2019 International Conference on Communication and Signal Processing (ICCSP). IEEE, 2017*. 0606–0610.

[2] Nakamoto, Satoshi and others. (2008) "Bitcoin: A peer-to-peer electronic cash system." *Citeseer*.

[3] Norta, Alex, Chad Fernandez, and Stefan Hickmott. (2018) "On Blockchain Application: Hyperledger Fabric and Ethereum." *Commercial Property Tokenizing With Smart Contracts." 2018 International Joint Conference on Neural Networks (IJCNN). IEEE, 2018.*

[4] Turkanovic, Muhamed, Marko Hölbl, Kristjan Košič, Marjan Heričko, and Aida Kamišalić. (2019) "EduCTX: A blockchain-based higher education credit platform." *IEEE access 6*. 5112–5127.

[5] Sajana P, M. Sindhu, and M Sethumadhavan. (2018) "On Blockchain Application: Hyperledger Fabric and Ethereum." *International Journal of Pure and Applied Mathematics* **118** (18): 2965–2970.

[6] Sankar, Lakshmi Siva, M. Sindhu, and M. Sethumadhavan. (2017) "Survey of consensus protocols on blockchain applications." *4th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2017*.

[7] Greeshma Sarath and S.H, M. Lal, "Privacy Preservation and Content Protection in Location Based Queries", in Proceedings of the 2015 Eighth International Conference on Contemporary Computing (IC3), Washington, DC, USA, 2015

[8] B. Venugopal and Greeshma Sarath, "A Novel Approach for Preserving Numerical Ordering in Encrypted Data", in 2016 International Conference on Information Technology (ICIT), Bhubaneswar, India, 2016