Digital ledger technology-based real estate transaction mechanism and its block size assessment

Nikita Singh* and Manu Vardhan

Department of Computer Science and Engineering,
National Institute of Technology Raipur, India
Email: nikitasinghk@gmail.com
Email: mvardhan.cs@nitrr.ac.in
*Corresponding author

Abstract: Distributed ledger technology (DLT) is set to transform the existing architectural models of financial institutions and government machineries. Although real estate transactions are a major source for the governments to earn revenue, these are plagued with the risk of fraudulent practices. The digital documents are vulnerable to the alteration or any other attacks or can be tampered and ownership of the documents can be changed. The centralised storage involves single point of failure as well as network traffic overhead. The proposed distributed and decentralised blockchain-based architecture provides protection against any intrusive activity which is offset by the majority voting achieved in consensus mechanism for each transaction and verification request. The proposed work provides web interface for user queries and analysis of query search time is carried out.

Keywords: DLT; inter planetary file system; IPFS; leader election; consensus mechanism; peer to peer network.

Reference to this paper should be made as follows: Singh, N. and Vardhan, M. (2019) 'Digital ledger technology-based real estate transaction mechanism and its block size assessment', *Int. J. Blockchains and Cryptocurrencies*, Vol. 1, No. 1, pp.67–84.

Biographical notes: Nikita Singh received her Bachelor's degree in Computer Science and Engineering from the Abdul Kalam Technical University, Lucknow, India in 2015 and MTech in Computer Science and Engineering from the Banasthali University Rajasthan, India in 2018. She is currently pursuing her PhD in Computer Science and Engineering at the National Institute of Technology Raipur, Raipur, India. Her research interests include image processing, computer vision and blockchain technology. She has published over six SCI and Scopus indexed research articles in international conferences and journals.

Manu Vardhan received his PhD degree from the Motilal Nehru National Institute of Technology Allahabad, Allahabad, India in 2013. At present, he is working as an Assistant Professor in the National Institute of Technology Raipur. He has published more than 52 research articles in various SCI and Scopus indexed journals and conferences. His research interest includes distributed computing, service oriented architecture (SOA), and blockchain technology.

1 Introduction

Consistent efforts and research by scores of researchers in evolving a decentralised and highly secure data storage model resulted in blockchain technology. This quest contributed to the evolution of distributed ledger technology (DLT) that is a decentralised and secure approach for storing data blocks that contain vital information or transactions. DLT is a type of database that is based on blockchain and replicated over a peer-to-peer (P2P) network. Instant settlement of transactions is one of the most appealing promise of DLT. Nowadays, various researchers are exploring these novel techniques to use DLT in various applications. Blockchain is an append-only sequential data structure with a unique feature that if a change is made on a single block in the middle of an existing chain, all subsequent blocks gets changed. This is because of the hash field present in every block that is computed from the content of the previous block. This modification is computationally unachievable, and hence, suited for applications that demand immutability. Five major components of a blockchain are cryptography, P2P network, consensus mechanism, ledger or transaction pool and validity rules. The validity rules are implemented as smart contracts.

Important factor that distinguishes blockchains from traditional distributed databases is the ability to operate in a decentralised setting without relying on a trusted third party (Bano et al., 2017). This is possible through the process of consensus. The need for atomic broadcast or consensus protocols in distributed systems originated from the need to provide resilience against failures across multiple nodes holding replicas of any file or database. Thus, one of the major applications where DLT can be useful for society as a whole is for real estate transaction management. The current real estate registry or financial market infrastructure is plagued with issues such as use of fake stamp papers, sale of a single property to more than one buyer or lack of infrastructure for verifying any real estate details before a buyer can transact. The reconciliation or verification process in DLT-based applications is through a consensus mechanism without relying on a central authority. Participants who are also termed as miners can independently verify the transactions and every participant view is consistent with what every other participant. This ensures that all participants have a consistent view of the transaction. This ensures that any improper alteration of the data will be immediately detected and rejected by all other participants.

Various crypto-currencies based on DLT are in operation already. DLT-based applications use blockchain to store the transactions. The blocks in blockchain are immutable due to inclusion of cryptographic hash of each block. Maintenance and security of P2P is provided by various consensus algorithms such as proof-of-work (PoW) (Nakamoto, 2008), proof-of-stake (PoS) (King and Nadal, 2012), proof-of-elapsed time (Ferrer, 2018), etc. These consensus algorithms also provide leader election facilities to all participating nodes when adding any new block. Such kind of decentralised system can be useful for storing and verification of digital documents. DLT can either be a closed chain or open chain.

The very intrinsic nature of blockchain, i.e., immutable records of transactions on distributed ledgers renders itself useful for use by governments. Government offices offer various public schemes and most of these involve finances. Hence, there is need for a system that is efficient, fast, fraud free, tamper proof and trustworthy. Most of these can be offset by moving to DLT. For the application proposed by us, it boils down to closed chain. The stakeholder can look for any real estate by an attribute such as record number or reference number as maintained in the block. A public web interface shall enable to search and request for verification of any real estate. This induces transparency in the system that is detailed in this research work. This research focuses on providing framework for decentralised, P2P and secure infrastructure for handling real estate transactions.

2 Related work

The first blockchain was conceptualised by Nakamoto (2008). It was implemented the following year by Nakamoto as a backbone of the crypto-currency bitcoin, where it serves as the public ledger for all transactions on the network. Through the use of a blockchain, bitcoin became the first digital currency to solve the double spending problem without requiring a trusted authority and this has been the inspiration for many other applications developed later. Bitcoin is a crypto-currency and worldwide payment system. The network is P2P and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a blockchain. It applies proof of work algorithm for consensus. Researchers are exploring applications of blockchain technology in every possible field either financial or non-financial (Underwood, 2016).

Blocks in the blockchain are immutable due to secure hash algorithm also called SHA256 (Eastlake and Jones, 2001). This algorithm generates fixed sized and unique hash string of any input. Eastlake and Jones in the document titled, ‘US Secure Hash Algorithm 1 (SHA1)’, describes SHA1 as a signature that is provided to a text or a data file. For the message or a text of any arbitrarily length, this algorithm produces an output which is fixed size in length and serves as the message digest for that input file. The message digests may later be used as an input to any kind of digital signature algorithm. The author also specifies how, signing the message digest rather than the text or the message itself helps improve the efficiency. This is so because the message digest is smaller in size than the actual message itself. The same hash algorithm may then be used to verify the original message that was sent. The paper also describes the basic binary operations, functions and constants, and binary padding techniques that have been used. The author points out that the binary padding technique is used so as to make the input padded text a multiple of 512, as SHA1 computes the text in the multiples of 512. The author also specifies two different methods for the computation of the message digest, one using message padding and the other using the array implementation using 80 32-bit words. Both these methods produce the same message digest. The paper also demonstrates a C code implementation of the SHA1.

Lemieux (2016) proposes a detailed survey on scope of the blockchain technology in securing digital documents. Proof of existence (PoE) is one of the first non-financial applications of a blockchain. This blockchain application allows users to anonymously and securely store a cryptographic digest of a file linked to the time at which the user submitted the file. This was the first online service to allow a user to publicly prove they possessed a certain file or data without revealing the data or their identity in a completely trustworthy manner. PoE utilises the bitcoin blockchain to ensure that the file’s hash is permanently stored in an immutable data structure without the need for a central time-stamping authority. Po.et (2018) is an organisation that is working on a project focused on providing PoE of digital assets on the top of bitcoin blockchain. It extends the time stamping and hashing features pioneered by PoE to enable new commercial applications by including additional metadata and discoverability. It allows original file to be discoverable. It also allows a user to generate an immutable ownership certificate of digital documents, track and license assets on the web, discover new assets and verify the authenticity of discovered assets.

Herbert and Litchfield (2015) propose novel application of the blockchain for validation of the software licenses. This proposed application helps in preserving privacy policy of the software. Litchfield and Herbert (2018) later extend their work and propose cross platform software license validation. Management and security of the blockchain is carried out by the consensus algorithms such as PoW, PoS, etc. These algorithms control the operations on the blockchain. Many researchers are also working on alternative approaches to these algorithms and its optimisation.

Batubara et al. (2018) systematically review relevant blockchain technology findings for the adoption of applications based on blockchain in e-government platforms that foster the transactions to occur in a more auditable, persistent and decentralised manner. Several technological aspects such as scalability, security, flexibility, anonymity, interoperability, and organisation readiness are also discussed in detail. The paper provides an insight to the state of art in research and the prime challenges faced in the mainstream adoption of the blockchain technology in the financial and the non-financial sectors. Several bibliographic databases are used to find relevant material and the research articles. These include the ScienceDirect, Scopus, and the Springer link. The paper also identifies the application domain in which most of the blockchain research has been carried out. The research findings as provided by the authors also indicate that most of the articles deliver only a theoretical view rather than a practical or an empirical approach. The author states that the need of the hour is to develop blockchain technological standards in accordance with the requirements of the government and public sector infrastructure.

Mathew and Md (2018) propose blockchain as an upcoming technology that can be put to use for global fintech industries across the world. They further state that all the online transactions generally have some intermediary which could be untrustworthy at times. Blockchain eliminates the need of any intermediary between the users who are involved in the transactions. They claim that blockchain and DLT can eliminate many of the existing inefficiencies in the global capital markets. The authors are of the view that DLT can replace the centralised consensus process. Smart contract facilitate users to generate business applications that can be deployed on distributed nodes.

Guo and Liang (2016) in their paper describe how blockchain technology is the combination of several other existing computer technologies namely, distributed data storage, peer to peer systems, distributed consensus mechanism, and encryption algorithms. The paper discusses how major banking giants such as Morgan Stanley, and Goldman Sachs, have started to formulate transaction settlement system based on the blockchain technology. They discuss how the blockchain technology can revolutionise the existing banking industry by focusing on easy cross-border payments and point to point funds transfer. Describing in detail the external and internal issues pertaining to the banking sector, the authors outline how blockchain could help curb non-performing loans and help improve loan quality by providing easy access to information. Point to point transfer of payment help in eliminating the intermediary firms from the picture as they further complicate the payment, clearing, and settlement process. The paper discusses the efficiency problems related to the blockchain which would decrease the efficiency of the blockchain when nodes in the system increase. The paper also talks about the blockchain regulation. Governments of various countries like the USA, India, Russia do not approve of blockchain regulation as it would curb the freedom of innovation. However, the authors view on regulation is that rules on blockchain need to be formulated as decentralisation dilutes the concept of regulation, thus blockchain regulation is extremely important.

Gervais et al. (2016) present a novel approach that discusses the performance and security guarantees that the blockchain technology provides based on the proof of work consensus algorithm. The paper discusses the unfavourable aspects of the blockchain technology such as the double spending problem, selfish mining, while at the same time, taking into consideration the real-time problems that persists in the network. Problem such as the variable block size, block creation time, mechanism for information propagation are considered and their security and performance are monitored using the proposed framework.

According to the ICT facts and figures 2017 report, 42.9% of households in developing countries have internet access driven by affordability and cheaper smartphones (Kshetri and Voas, 2018). They argue that blockchain has a much higher potential for the people of the developing world rather than the developed world. This is because of the inherent capability of the blockchain that makes it less susceptible to rules and regulations, law of the land and their enforcement. It further adds that according to a 2011 UN report, corruption in land transactions has its roots in more than 61 countries. It points out that around 90% of land is undocumented or unregistered in rural Africa. They emphasise how blockchain might mitigate inefficiency, fraud, and gross misallocations of resources so as to help refugees and displaced persons.

Karan et al. (2018) are of the view that various corporate entities and banks maintain large data centres that consume millions of watts of energy thus contributing to increased carbon emission. They are of the view that financial institutions whether private or government worldwide are trying hard to reduce the payment, clearing and settlement cycles of various transaction. This is intended to eliminate operational inefficiencies and reduce risks, thus, making it robust. The authors also propose need for persistent miners for verifying any new block to be added to a blockchain. They are of the view that these miners can be considered as super nodes that shall be persistent and fault tolerant. DLT-based e-stamp procurement system (Singh and Vardhan, 2018) has been proposed and its efficacy has been discussed in terms of authenticity of the stamp paper being used for real estate transactions.

The blockchain technology needs to support not only the peer-peer network but also support publish subscribe system. Mallick and Kushwaha (2012) proposed publish subscribe system that is able to deliver the notification to the subscriber with content delivery capabilities.

Hence, there is need of an architecture that is based on blockchain technology with support for user queries. This research focuses on providing framework for decentralised and secure P2P infrastructure for handling real estate registration documents along with interface for verification of document originality. Major objectives achieved in the proposed research are:

1 proposing a P2P for e-registry

2 verification of real estate details before it can be sold

3 recording transaction for real estate purchase or sale

4 efficient consensus mechanism before adding any block to existing blockchain

5 web interface for verification of real estate registered deed

6 assessing optimal block size based on the characteristics of application deployment.

3 Proposed digital ledger technology-based real estate transaction mechanism

Architecture used in this research is based on the content addressed file system (Benet, 2014). Thus, the proposed digital ledger technology-based secure real estate transaction mechanism is implemented on content addressed inter planetary file system (IPFS). Each node in the P2P network is IPFS node which has a unique IPFS address and is connected to other IPFS nodes of the system. These nodes can perform role of a miner. The bootstrap server stores information about IPFS nodes that are part of the network. Any authorised node that can either be miner or non-miner can join the network by registering with bootstrap server. Bootstrap server maintains list of active and inactive nodes in the network. Before joining, an authorised node obtains list of active peers from bootstrap server.

In every country, there exist many regional/zonal/registry offices where people visit for buying or selling any real estate. These regional offices report to zonal offices structured in a well defined hierarchy. All these offices are part of the P2P network. Every regional office may have more than one node that performs the function of miner. Also, regional offices can involve private miners because these private entities deploy high end computational hardware in lieu of certain incentive paid to them by the regional offices. The P2P system connects all regional/zonal registrar offices to form the common closed blockchain. These are the authorised entities that are responsible for carrying out the transactions. To manage this blockchain, nodes/miners at registrar office are provided with a capability to verify transactions and mine new blocks consisting transaction details to be added to the existing blockchain. The registry offices are overburdened with different types of queries and land record verification requests. In order to cater to public at large, each regional office also deploys a web server. This web server is connected to the regional miners that are capable of verifying authenticity of owner of the record, real estate type and other such queries. The sequence of interactions between buyer/seller, bank, registrar office, miner and blockchain is illustrated in Figure 1.

To ensure the security of the blockchain, each authorised personnel must have a pair of private and public key. Private key is kept secret and the public key is distributed to the all peers in the networks. The nodes in the e-registry network are regional nodes (can be more than one) because each region in the country has its office for registration of the properties. Hence, a regional database needs to be setup for each region in this network. To enhance the efficiency of the consensus mechanism all miners are categorised into different category. Thus, the entire proposed architecture is formed by two set of entities namely government and private.

3.1 Implementation of proposed P2P swarm network architecture

The proposed digital ledger technology-based secure real estate transaction system is swarm based on P2P network that is implemented on IPFS (Benet, 2014). Every regional office has certain nodes that interact with public and accept details for real estate transactions termed as PTnode and certain nodes act as miner termed as Mnode or both the roles handled by one single node termed as PTMnode based on the computational capabilities of the node. For lightly loaded scenarios, PTnode can also carry out mining operations but during heavy loads, Mnodes are the suitable choice as these nodes only perform the mining operation.

Figure 1 Sequence of events for DLT-based real estate transaction

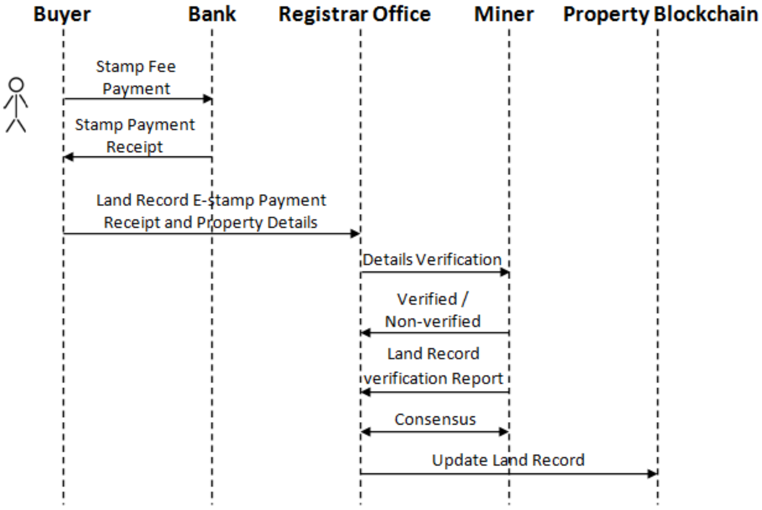
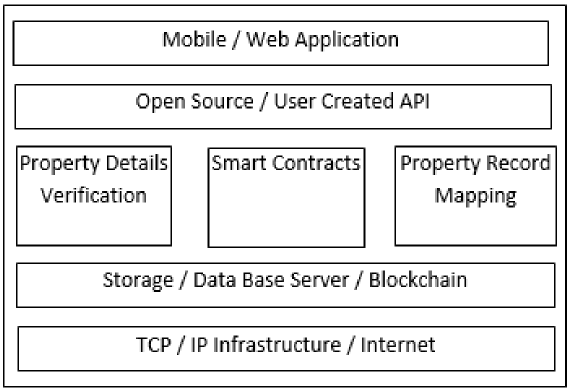


Figure 2 Application stack of miner (IPFS node)


Mobile / Web Application
Open Source / User Created API
Property Details Verification
Smart Contracts
Property Record Mapping
Storage / Data Base Server / Blockchain
TCP / IP Infrastructure / Internet

The real estate transaction process starts by paying for the property transaction fee either by physical stamp paper or e-stamp. Now, all the property details, the concerned records and stamp payment details are submitted at the registrar office. These detailed steps are illustrated in Figure 1. The complete application stack of any miner node is illustrated in Figure 2. Smart contracts are the software codes that can be deployed for verifying any detail pertaining to any real estate transaction and raise alarm.

To join the network, any authorised node at the outset obtains the list of the active nodes in the network and connects with these active nodes. A P2P network of all constituent nodes is composed of some regional nodes that are PTnode, Mnode or PTMnode. Each Mnode or PTMnode has a regional database and web server. The regional database is used to store the details of the digital registry documents local to the region. The regional database stores the real estate transaction details in JavaScript object notation (JSON) file format as illustrated in Figure 3.

Figure 3 Real estate transaction details in JSON file

```
{"index":75,"timestamp":"Wed Oct 31 17:00:52 IST 2018","transactions":

[{"sellerId":{"panDetails":"66655784","aadharNo":"66655784"},"buyerId":
{"panDeails":"66655784","aadharNo":"66655784"},"landDescription":
{"length": 66655784,"width":66655784,"address":"66655784"},"price":66655784},

{"sellerId":{"panDetails":"35152106","aadharNo":"35152106"},"buyerId":
{"panDetails":"35152106","aadharNo":"35152106"},"landDescription":
{"length":35152106, "width":35152106,"address":"35152106"},"price":35152106},

{"sellerId":{"panDetails":"87010329","aadharNo":"87010329"},"buyerId":
{"panDetails":"87010329","aadharNo":"87010329"},"landDescription":
{"length":87010329, "width":87010329,"address":"87010329"},"price":87010329}
```

Since the proposed system is a peer to peer system, nodes can join and leave arbitrarily. Among other reasons for this is that different regions/zones/states or provinces observe different holidays or timings for carrying out registry. This could also be due to unavoidable circumstances. Hence, mechanism of node joining and leaving is discussed in subsequent sub-section.

3.2 *Handling the churn in the network*

Any node that wishes to join the network needs to connect with bootstrap server. The bootstrap server will return the list of IPFS nodes and their IPFS address that are active in the network. Bootstrap server also updates its active user list by adding the requester node id and IPFS address. The new node has to connect with all the active nodes to become the part of this network.

Bootstrap server periodically updates the list of active swarm nodes by sending Is_active signals to all nodes in swarm. Those nodes that are active in the network reply to the Is_active signal. Based on this reply, bootstrap server updates its active and non-active nodes list.

3.3 *Attributes of transaction stored in the block and its structure*

The major entities of the blockchain management are:

1 attributes of transaction stored in the block

2 structure of the block.

These issues are discussed in subsequent sections.

In order to create unique blockchain, structure of the block must be defined. The block contains entries of the transaction. Each real estate transaction has certain number of defined fields. These fields include transaction id, details of the real estate, details of the seller and the details of the buyer. To ensure that these details are immutable, SHA256 cryptographic algorithm is used to obtain the hash of digital document, which is also stored in the block. Figure 4 shows the structure of attributes of a single transaction.

Figure 4 Attributes of real estate transactions

Real estate details
Transaction ID
Seller PAN
Seller UID
Buyer PAN
Buyer UID
Real estate ID
Real estate description
Real estate details
Real estate address
Hash of real estate registry
Digital signature of official

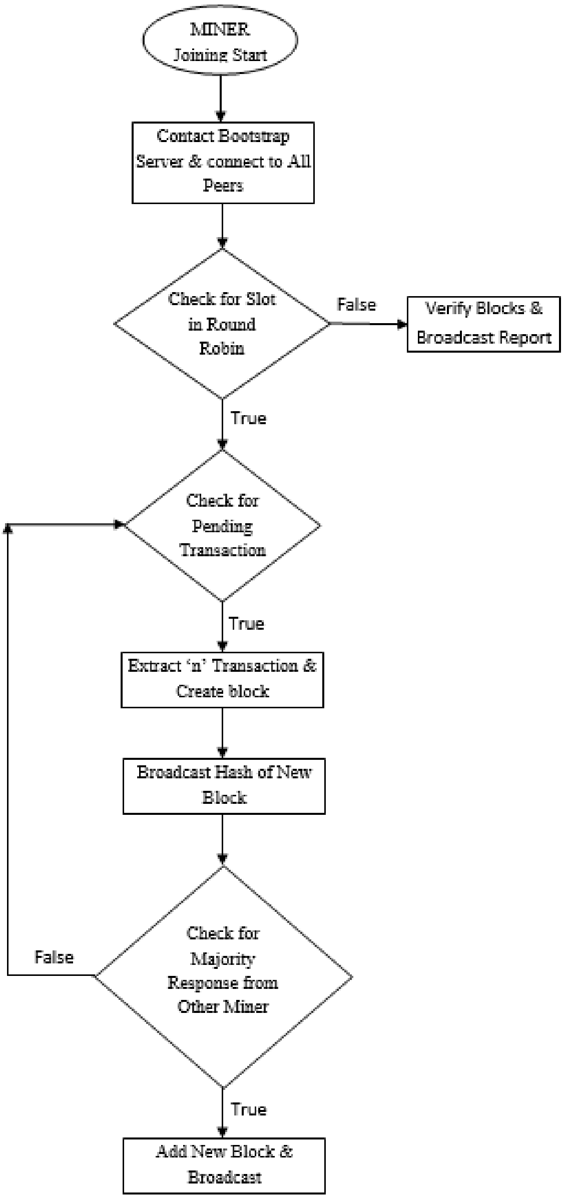
In order to perform any real estate transactions, entries shown in Figure 4 are required. This is the function of the registrar office. Each block in the blockchain can store any number of real estate real estate transaction records. The same is illustrated in Figure 5. The size of the block decides the time when the details are available for view. The smaller the block size, the lesser the time required. Smaller block sizes impose certain penalty on performance of the proposed system such as frequency of blocks being broadcast and fee for the miners. The structure of the block is shown in Figure 5.

Figure 5 Structure of block of proposed blockchain

Previous block hash
Transaction1
Transaction2
.
.
.
Transaction'n'
Digital signature of miner

In the proposed system, only relevant buyer/seller details and real estate details are stored in the blockchain. Any user who wishes to access details of a property first places query with the web interface of the miner. When the user receives the reply, the transaction_id is known. Using this transaction_id, any user can get access to copy of digital registry.

Figure 6 Flowchart of miner process


MINER
Joining Start
Contact Bootstrap Server & connect to All Peers
Check for Slot in Round Robin
False
Verify Blocks & Broadcast Report
True
Check for Pending Transaction
True
Extract 'n' Transaction & Create block
Broadcast Hash of New Block
Check for Majority Response from Other Miner
False
True
Add New Block & Broadcast

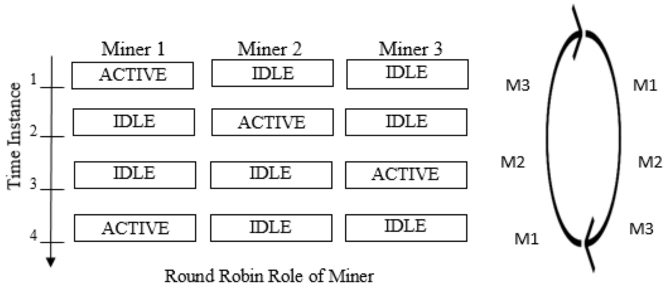
3.4 *Responsibilities of miner*

A miner is responsible for ensuring the integrity of the blockchain and security of the proposed transaction mechanism. When any miner node wishes to be part of the system, it contacts the bootstrap server. As soon as it receives the node id, the miner node synchronises its blockchain. During this process, this miner obtains the blockchain from its peers and updates its blockchain before it starts mining new blocks. The miner either waits for its time slice to mine newly created blocks or verifies the transactions in the newly created block that is broadcast from some other miner as illustrated in Figure 6. While waiting for its time slice, miner waits for new block and verifies the transactions and broadcast its vote to the network.

3.5 Consensus mechanism

A consensus mechanism is a process in computer science that is used to achieve agreement on a single data value among distributed systems. Consensus algorithms are designed to achieve reliability in a network involving multiple unreliable nodes. Examples of consensus algorithms include PoW, PoS among others. PoW is the most popular among these but has slow throughput and it is slowly killing the planet courtesy huge amount of electricity needed to run the PoW algorithm to solve hard useless puzzles in order to create new blocks. This paper proposes a system for the government organisation; hence, it is a closed blockchain. However, consensus must be there in order to verify the authenticity of newly created blocks and transactions in these blocks. To ensure the security of the blockchain, each authorised personnel from each regional office must have a pair of private and public key. Private key must be secret to the personnel and public key of the personnel must be distributed to the all peers in the networks. Whenever a transaction related to the registry of the real estate is performed in a regional office, the authorised personnel must sign the transaction with its digital signature generated by its private key. All other nodes can verify the authenticity of the transaction (document) by using the public key of the signature authority. The majority of the votes about the transaction will decide the authenticity of transaction. The authorised personnel must be responsible for any fraudulent activity in the blockchain that records all the real estate transactions.

Figure 7 Illustration of leader election with time slicing



Time Instance	Miner 1	Miner 2	Miner 3
1	ACTIVE	IDLE	IDLE
2	IDLE	ACTIVE	IDLE
3	IDLE	IDLE	ACTIVE
4	ACTIVE	IDLE	IDLE

As proposed earlier, any DLT-based (Mills et al., 2016) system must use some leader election and consensus mechanism in order to maintain single blockchain. In leader election, the all nodes in the P2P swarm elect a leader. This leader is responsible for verifying each transaction in the newly created block. All other nodes will achieve consensus on newly created block voting. The management of the time slicing between the miner nodes is the responsibility of the bootstrap server that allocates the time slice according to the number of active miners. For sake of illustration, only three miners are shown as active in Figure 7. Validating a blockchain involves checking if data of any transaction or other blocks are tampered by validating hash of previous block and previous hash in the present block. It also invalidates chain which is duplicated. After consensus process, the miner updates its blockchain.

3.6 Proposed time slice-based fair leader election algorithm

PoW algorithm has many limitations such slow throughput and high power consumption, etc. Hence, this research proposes an efficient leader election algorithm. The proposed blockchain network is a peer-peer system where creation of any block or joining and churning of nodes is inevitable. Real estate transaction that get completed are first placed in transaction pool. Later, certain number of transaction are selected based on the time stamp to form one block. Verification of the transactions that exist in any newly created block is critical to the existence of any blockchain. The nodes responsible for mining operations owned by the Government Office may not have enough capability to process transactions and simultaneously mine newly created block. Hence, Mnodes or sometimes PTMnodes mine the newly created block. The Mnodes get paid for each mined block. In order to avoid contention among the Mnodes, fair leader election is proposed so that each Mnode get equal chance to mine newly created blocks. The algorithm allocates equal time to all the different miners for creation of the blocks while one node is creating blocks all other remaining miners must achieve the consensus for the authenticity and originality of the newly created block. The proposed leader election algorithm with time slicing is illustrated in Figure 7. Consensus is based on the majority vote received for the block from other PTnode, PTMnode and Mnode.

4 Workflow of the proposed system

In the previous section, we have discussed about the architecture of the proposed system. The roles and responsibilities of the various entities involved in the proposed system have also been elaborated. In this section, the overall workflow of the proposed system is presented.

The workflow of proposed approach consists of three major phases. In the first phase, digital copy of the registry is generated. During this process, any personal at the registrar office shall collect details from the seller and the buyer for the real estate transaction to be executed. This includes the details of the seller and buyer along with the details of the real estate being bought or sold. In second phase, the real estate transaction is generated along with necessary details as shown previously in Figure 4. A smart contract can be deployed in order to verify these details before generating digital registry or invoking block creation. During the last phase, digital registry gets created that is stored in any database server. This paper proposes a regional database that should also be replicated in order to increase the availability. Figure 8 illustrates the working of the proposed system.

As real estate transactions take place in the registrar office, transaction file gets created. Each transaction stores attributes as illustrated in Figure 4. This file is created in JSON format in the proposed system. This is illustrated in Figure 3. Hence, new transactions get added in the transaction pool. When sufficient number of transactions is available in transaction pool, the miner creates a new block. Number of transaction being stored in a block dictates the efficacy of the system being deployed. This is because, not all the user has same internet bandwidth. Further, people at remote location may wish to query the authenticity of any real estate record before making a buying decision as discussed in the next subsection. Hence, optimal size makes the system work well for different users/offices spread across the country. This impact is illustrated in the next section detailing performance and result. Figure 9 illustrates various states of the transaction, which is committed if verified else dropped.

Figure 8 Working of the proposed system

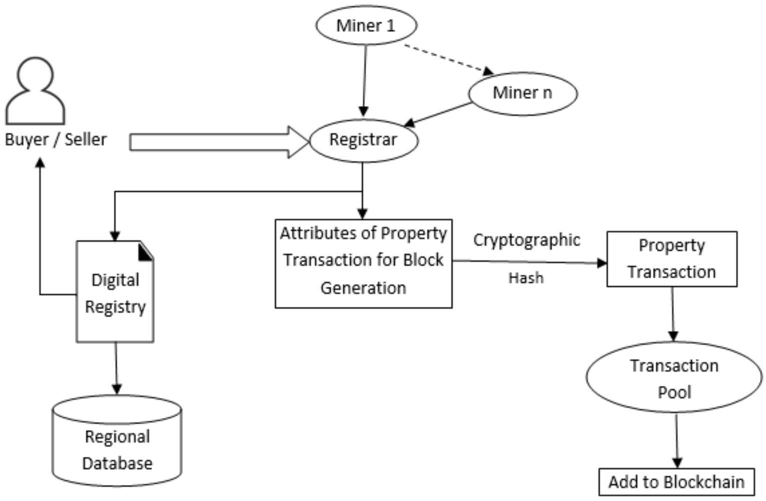
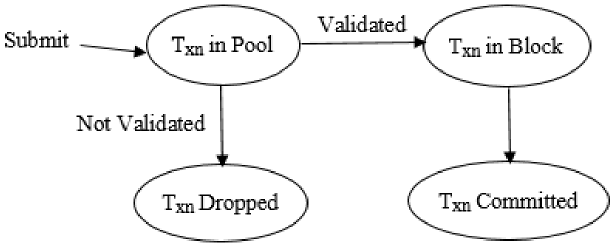


Figure 9 States of transaction



4.1 Role of web interface

A key entity in any system is the ease of use of any application for various types of users. This dictates the usability and versatility of the system. There still exists huge number of countries where internet connectivity is in few kilobytes. Even in country like India, there are large number of remote town and cities who have very weak connectivity. In such scenarios, generally people visit various registrar offices for enquiry of the property. In order to prevent this and enable remote facility, this work also proposes a web interface facility for the public at large. This interface is intended to ascertain the authenticity of any land record that is queried by the user. The miner at each regional office serves as interface between user and blockchain. The web interface accepts the query from user and miner searches for the details in the blockchain. The response is returned to the end user via web interface. The interaction between web interface and web server is based on the web service. The efficient web service discovery system (Mallick et al., 2011) is one of the ways to design the search process. The time required to search for any property record is presented in the next section. If details are found as satisfactory, the user can access the digital registry.

5 Performance and results

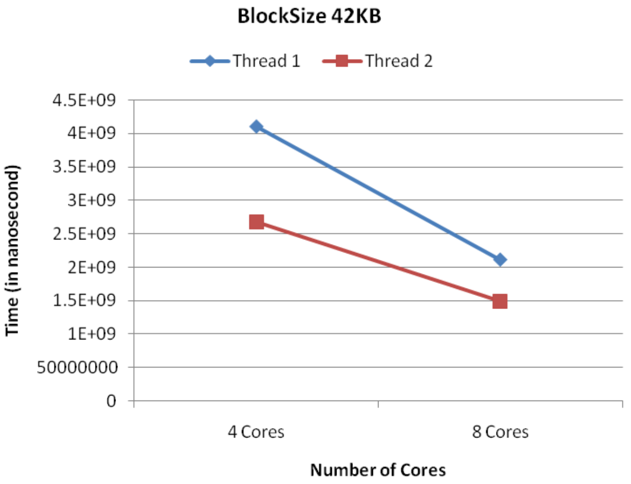
This experimental setup consisted of three number of Intel core i7 4790 3.60 GHz quad/octa core CPU, with 16-GB 1600 MHz DDR3 RAM. All these three machines are connected through a 1 Gbps network. One of the machines is used by the user for requesting or submitting the transactions at the Real Estate Registrar Office. The other two nodes are official miner nodes that also perform the search operation given any query by the seller/buyer.

A vital question is about the number of transactions that should be stored in a block. This translates to block size. If very few transactions are stored, block size is smaller and the transactions are frequently mined by the miner. New real estate transaction records are available to public very quickly but this increases the amount of packets being broadcast among the stakeholders. For larger block size, more transactions can be placed in a block.

Table 1 Transaction search time (ns) for 42 KB block

Block size – 42 KB		
Thread	*4 cores*	*8 cores*
1	4108737210	2107434588
2	2681300195	1482616838

Figure 10 Query time with 42 KB block size (see online version for colours)



In order to address the issue of block size, the proposed system is implemented in java and transactions stored in JSON file format. The proposed results have been obtained by creating a blockchain with 1,200 blocks. Three different block sizes are created in order to assess the impact of blocksize on the queried transaction search time. In the first case blockchain consisted of 42 KB block size and for the other it is 422 KB and 844 KB. For 42 KB block size, 200 transactions are stored in one block and for 422 KB block size, 2,000 transactions are stored in one block. This experiment is again repeated for 844 KB block size. All the three different scenarios have been implemented with two numbers of threads. Independent results have been obtained for quad core and octa core machine. The values listed in Table 1, 2 and 3 are averaged over multiple measurements. All the time recorded is in nano seconds.

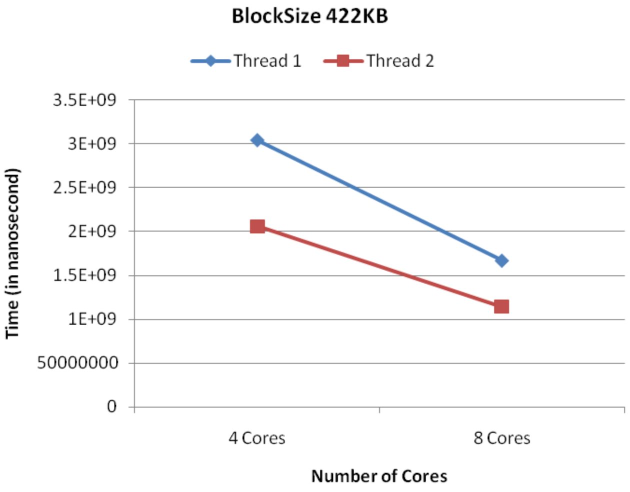
Different queries are invoked for transactions that reside in the last of few blocks in the blockchain, for the transactions that were placed around the mid of the block chain and lastly for transactions that resided in the first few blocks of the blockchain. The results are averaged for multiple readings obtained in order to deal with outliers. As is evident from data in Table 1 and Figure 10, query time with single threaded application for 42 KB block size is 4.1 sec on a quad core machine and 2.7 sec on an octa core machine. This is a reduction of about 65%.

Table 2 Transaction search time (ns) for 422 KB block

Block size – 422 KB		
Thread	*4 cores*	*8 cores*
1	3043104002	1671605772
2	2058415429	1143006781

Observing data in Table 2 and Figure 11, query time with 422 KB block size is 2.7 sec on a quad core machine and 1.9 sec on an octa core machine. This again is a reduction of about 70%. This establishes that a bigger block size reduces the time required to research for any transaction in the blockchain.

Figure 11 Query time with 422 KB block size (see online version for colours)

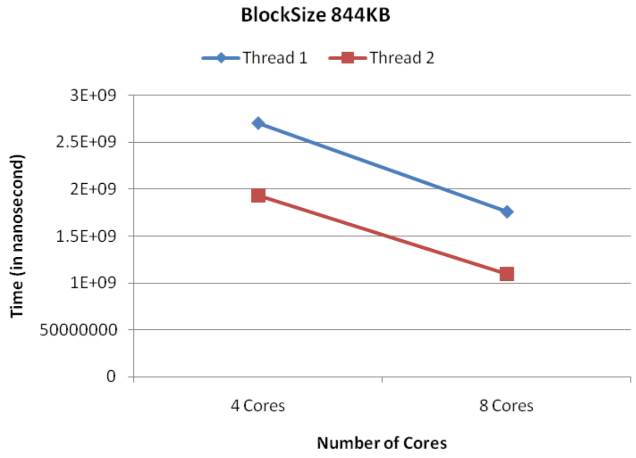


The experiment is further repeated with 844 KB block size, since bitcoin has worked with 1 MB of block size for long. The search for a transaction is further reduced as evident from Figure 12. This bodes well for the users at remote location with low bandwidth internet connection to receive the query results faster, thus compensating for slow network connections.

Table 3 Transaction search time (ns) for 844 KB block

Block size – 844 KB		
Thread	*4 cores*	*8 cores*
1	2701829572	1755724448
2	1929778208	1091624611

Figure 12 Query time with 844 KB block size (see online version for colours)



Hence, depending upon the nation or the territory, where this application is proposed to be deployed, it is a matter of need and requirement as to what should be the block size. If huge number of transactions is taking place in a given time and the time taken by miners for verification of this transaction is more than the tolerable limit, the block size should be smaller. Else one should go for larger block size if the hardware infrastructure deploying and running the application is robust enough.

6 Conclusions

Although real estate transactions are a major source for the governments to earn revenue, these are plagued with the risk of fraudulent practices. The digital documents are vulnerable to the alteration or any other attacks. The real estate records can be tampered and ownership of the property can be changed. The proposed distributed and decentralised architecture provides protection against any such intrusive activity which is offset by the majority voting achieved in consensus mechanism for each transaction and verification request. It has been observed that when the block size is increased from 42 KB to 422 KB, i.e., increased by ten times, the time required to process the user query is reduced by 65–70%. If huge number of transactions takes place in a given time and the time taken by miners for verification of these transactions is more than the tolerable limit, the block size should be smaller. Else one should go for larger block size if the hardware infrastructure deploying and running the application is robust enough.

References

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S. and Danezis, G. (2017) *Consensus in the Age of Blockchains*, arXiv preprint arXiv:1711.03936.

Batubara, F.R., Ubacht, J. and Janssen, M. (2018) 'Challenges of blockchain technology adoption for e-government: a systematic literature review', in *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, ACM, May, p.76.

Benet, J. (2014) *IPFS-Content Addressed, Versioned, P2P File System*, arXiv preprint arXiv:1407.3561.

Eastlake 3rd, D. and Jones, P. (2001) *US Secure Hash Algorithm 1 (SHA1)*, RFC 3174, September, DOI: 10.17487/RFC3174, https://www.rfc-editor.org/info/rfc3174.

Ferrer, E.C. (2018) 'The blockchain: a new framework for robotic swarm systems', in *Proceedings of the Future Technologies Conference*, Springer, Cham, November, pp.1037–1058.

Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H. and Capkun, S. (2016) 'On the security and performance of proof of work blockchains', in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, October, pp.3–16.

Guo, Y. and Liang, C. (2016) 'Blockchain application and outlook in the banking industry', *Financial Innovation*, Vol. 2, No. 1, p.24.

Herbert, J. and Litchfield, A. (2015) 'A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology', *In Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015)*, January, Vol. 27, p.30.

Karan, S., Nikita, S. and Kushwaha, D.S. (2018) 'An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain', *2018 International Conference on Computing, Power and Communication Technologies*, India, pp.168–172.

King, S. and Nadal, S. (2012) *Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, self-published paper, 19 August.

Kshetri, N. and Voas, J. (2018) 'Blockchain in developing countries', *IT Professional*, Vol. 20, No. 2, pp.11–14.

Lemieux, V.L. (2016) 'Trusting records: is blockchain technology the answer?', *Records Management Journal*, Vol. 26, No. 2, pp.110–139.

Litchfield, A. and Herbert, J. (2018) 'ReSOLV: applying cryptocurrency blockchain methods to enable global cross-platform software license validation', *Cryptography*, Vol. 2, No. 2, p.10.

Mallick, S. and Kushwaha, D.S. (2012) 'an efficient publish-subscribe protocol for collaborative content delivery-ex-PUSH', in *2012 International Symposium on Cloud and Services Computing (ISCOS)*, IEEE, December, pp.152–156.

Mallick, S., Pandey, R., Neupane, S., Mishra, S. and Kushwaha, D.S. (2011) 'Simplifying web service discovery & validating service composition', in *2011 IEEE World Congress on Services (SERVICES)*, IEEE, July, pp.288–294.

Mathew, S.A. and Md, A.Q. (2018) 'Evaluation of blockchain in capital market use-cases', *International Journal of Web Portals (IJWP)*, Vol. 10, No. 1, pp.54–76.

Mills, D.C. and Wang, K., Malone, B., Ravi, A., Marquardt, J., Badev, A.I., Brezinski, T., Fahy, L., Liao, K., Kargenian, V., Ellithorpe, M., Ng, W. and Baird, M. (2016) *Distributed Ledger Technology in Payments, Clearing, and Settlement*, December, FEDS Working Paper No. 2016-095.

Nakamoto, S. (2008) *Bitcoin: A Peer-to Peer Electronic Cash System* [online] https://bitcoin.org/bitcoin.pdf (accessed 31 March 2015).

Po.et (2018) *Proof of Existence on the Top of Bitcoin Blockchain* [online] https://www.po.et (accessed 13 November 2018).

Singh, N. and Vardhan, M. (2018) 'Blockchain based e-stamp procurement system with efficient consensus mechanism and fast parallel search', *J. Mech. Contin. Math. Sci.*, Vol. 13, No. 4, pp.73–89.

Underwood, S. (2016) 'Blockchain beyond bitcoin', *Communications of the ACM*, Vol. 59, No. 1, pp.15–17.