Blockchain-based digitization of land record through trust value-based consensus algorithm

Amrendra Singh Yadav [1] · Dharmender Singh Kushwaha [1]

Abstract

The real estate markets currently hold and contribute a fair share of any country's gross domestic product. In real estate transactions, stamp duties produce income that adds to the government funds. However, the transactions in real estate may be subjected to forgery through fraudulent papers or activities. Many reforms have been proposed but distributed ledger technology offers solution to most of these issues. A traditional proof-of-work consensus causes an overhead of a large number of message exchanges, which takes a much longer time. This leads to an increased number of utilized blocks for storing transactions, and the required computational power is enormous. This article proposes a blockchain-based system for digitizing transactions in real estate that mitigates the possibility of falsifying documents and other fraudulent activities. The article also proposes a consensus algorithm, which reduces overhead transmissions by around 50% for multicasting nodes. The proposed consensus approach has been compared with five prominent approaches: proof-of-work, proof-of-stake, delegated-proof-of-stake, load-balanced, and a trust-based approach. The comparative assessment deduces that the proposed consensus process is faster than the compared approaches. The overhead of message exchange communication decreases by up to 50.30% compared to the traditional proof-of-work approach.

Keywords Peer-to-peer · Blockchain · InterPlanetary file system (IPFS) · Consensus algorithm · Trust value · Property transaction · Distributed ledger technology

1 Introduction

The Gross Domestic Product (GDP) levels in any country depend on contribution from different sectors. Out of these sectors, contribution of the real estate industry is enormous. In India, real estate accounts for 5% of the total GDP [1]. Transaction in real estate involves the transfer of ownership of any property, house, or apartment, which is done through a registry. However, the existing land record maintenance

system suffers from many flaws. Different departments manage multiple land records, and there is no uniform system to manage these land records. These flaws often raise disputes over land ownership.

Worldwide, governments are encouraging digital documentation and digital transactions to bring transparency into the e-governance system. Technologies do improve the efficiency and performance of the system, but there exist various challenges. The digital documents are vulnerable to alteration and various network attacks. Since, digital documents can be tampered hence, the ownership of the documents can be changed. Other challenges include storage, availability, and scalability of these documents. Organizations need to provide secure storage for digital document, and access to authorized users must be monitored. Centralized storage introduces a single point of failure and increases network traffic.

The land registration process in India is fragile and tedious. It comprises various procedures to be done manually and requires multiple authorizations at various levels. The registration process is also prone to human errors or typographical mistakes, such as inaccurate data, the unclear title of the property, fake/forgery property records, verification/search issues

---

✉ Amrendra Singh Yadav
  yadavamrendrasingh@gmail.com

  Dharmender Singh Kushwaha
  dsk@mnnit.ac.in

[1] Department of Computer Science and Engineering, Motilal Nehru National Institute of Technology Allahabad, Prayagraj, Uttar Pradesh, India

due to physical documents, multiple registries on one land, and Benami (unnamed) transactions.

Digital India Land Records Modernization Programme (DILRMP) created a new and effective land records management system in 2014 specifically, complete, up-to-date, and open property registration of the belongings real-time, accurate land records are a prerequisite for a titling scheme [2]. Many states successfully implemented the land records digitization system and computerized property registration offices. However, these computerized systems operate independently, and there is a lack of a dependable ecosystem for managing transactions and maintaining records.

The country's current land records are ambiguous, poorly administered, and often do not represent ground truth. The government faces significant difficulties in maintaining and making available information on land records. Additionally, India's new legal framework does not guarantee land possession. Land records information is updated and maintained at all district and village level by various departments. The data between these departments are not usually synchronized, which results to various inconsistencies and mismatch of documents with ground positions. Poor control of land transaction processes and record-keeping affects the management of land market in any country [3].

The main issue with the existing framework is lack of co-ordination among multiple agencies (land record, survey, court, bank, and registration department). Other issues involve improper management of old cadastral records, inadequate usage of IT Systems, costly methods of surveys, ample prospects for fraud, and corruption. Several of these crucial problems can be resolved by new technologies such as Distributed Ledger Technology (DLT), a path-breaking technology capable of resolving land record-keeping challenges.

1.1 Distributed ledger technology and blockchain

DLT is the decentralized and secure approach for overcoming most of the issues, as enunciated in current research. DLT uses distinct cryptographic techniques to preserve decentralized, tamper-proof, and stable transaction records. DLT can bring much-needed radical changes in several welfare operations that the government conducts to benefit the underprivileged in our country. Now a days, digital governance as a service is becoming de facto standard. The same is becoming true with the real estate market growing exponentially to fuel the growth of country economy. This has led to an increase in the frequencies of property transactions that comes with the risk of fraudulent practices; thus, forcing society to demand safe and transparent transactions and enhanced efficiency and accountability [4].

Blockchain comprises nodes in a distributed network utilizing digital ledger technology to store records of transactions among peers. The technology is immutable, cryptographically secure, and implemented through the Internet. The ledger can only be appended, if a consensus is developed to update it. The verification of land records updation involves third parties that can be eliminated for property transfer transactions utilizing blockchain. This, in turn, leads the consumers to have greater confidence in blockchain for safe land transactions and build digital trust. The blockchain-based system allows quick decision-making due to its transparency and integration. The significant aspects of security in blockchain are as follows:

1. The access to records is on-demand.
2. The blocks are a collection of secure transactions.
3. The blocks form a chain with links (to the previous one) using a cryptographic hash.
4. Have an irrefutable unique digital signature.
5. Records are free from duplicity, corruption, and mutability.
6. Records are decentralized and regulated without human discretion.
7. Chronologically set records could not be updated.

This article proposes a blockchain-based solution that eliminates manual processes for the land registration process. It provides a single-window registration service. The proposed solution focuses on providing a decentralized and stable Peer-to-Peer (P2P) framework for managing real estate land registration and an interface for verifying document originality. The suggested approach is based on a hybrid blockchain and is purposely structured such that any client can see the registration issued by the registration office. Any change will be updated in registration, only after a consensus is achieved through a trust-based consensus approach.

1.2 Motivation

Land ownership is one of the most pressing issues confronting India's states, partly due to the lack of an end-to-end emphatic land records management system. Land ownership is such a crucial issue that almost all financial institutions rely heavily on land-based properties as collateral security. Due to the uncertainty surrounding ownership claims, it becomes more difficult for financial institutions to function properly, hampering the nation's growth. Due to low maintenance and a lack of coordination across agencies, we often discover gaps, obsolete data, and data out of sync in land records. These inconsistencies are at the heart of the ownership dispute, as establishing ownership requires many years of records. Various schemes have been implemented in modernizing land records to move away from presumptive property titles to a clearer and conclusive land ownership over the last three decades. The digitalization of paper-based land records, on the other hand, adds redundancy, concurrency, consistency, and database system characteristics. The blockchain is a robust solution to

3542

Peer-to-Peer Netw. Appl. (2021) 14:3540–3558

these issues. Blockchain technology in land registries can solve many issues that come with traditional centralized title recording. Combining the immutable representation of possession transfer with the resulting decentralization of control, collaborative, multi-sided, 'trustless systems' can be built. This article proposes a blockchain-based land registration system framework.

- The existing approaches to consensus are computationally expensive and very demanding to the system and network. Therefore, an efficient consensus mechanism based on trust value is required.
- Frauds relating to property documents and evasion of stamp duties force us to examine, propose and develop a blockchain based e-stamping framework to ensure that verification of e-stamp or transfer tax documents are secure and tamper-proof. This e-governance application shall also increase the revenue collected by the government.
- To support constrained devices that can access e-governance applications, one must establish an optimal block size in blockchain as it is directly associated with the network bandwidth's performance.
- To achieve the goal of exploring the possible mechanism by which blockchain-based decentralized and efficient e-governance framework.

1.3 Organization of the paper

This article is organized as follows: section 2 briefs the leading research relevant to the suggested approach. Section 3 presents the proposed work and is divided into five subsections. The network architecture for the e-registry framework is elaborated under Section 3.1. The stamp-procurement and stamp-duty payment method is explained in section 3.2. Section 3.3 presents the verification of land, its possession, and payment of the registration fee. Section 3.4 proposes the generation of record-keeping and ownership records, followed by section 3.5, which proposes a consensus algorithm for leaders' election. Sections 4 delivers comparative results and analyze them for the betterment of the proposed approach. Finally, section 5 concludes this article.

2 Literature review

Nakamoto [4] suggested the first blockchain-based cryptocurrency called Bitcoin. Barclays is the first industry to implement blockchain technology for its enterprise [5]. InsurChain [6] is the first blockchain technology for the insurance ecosystem. A few studies have also been done for the Strength, Weakness, Opportunities, and Threats (SWOT) analysis of blockchain technology. SWOT Matrix (SWOTM) is a formal planning tool for analyzing different blockchains. Murthy et al. [7] utilized SWOTM to perform an in-depth study of blockchain technologies and their advantages and challenges. The authors discussed the technologies that make up the blockchain and different forms of blockchain, the evolution of blockchain from technology convergence, blockchain functions, its benefits, and challenges.

There is a high probability of Byzantine failures with the consensus algorithm of the blockchain. Consensus structures like Proof-of-Work (PoW) [4] and Proof-of-Stake (PoS) [8] address this issue. The PoW deals with the Byzantine general problem by puzzling the miners. The miners must solve the puzzle to be elected leaders and mine the block. When a majority of miners vote, i.e., 51%, the new block is added to the blockchain. However, in PoS, the highest stakeholder miner can mine the new block, while the remaining miners seek new blocks to obtain. Daming et al. [9] analyzed blockchain's vulnerability to intrusions and inferred that blockchain technology is more stable and reliable. Singh et al. [10] also suggested a distributed and decentralized blockchain-based architecture that secures intrusive activities for each transaction by allowing consensus for approval through the majority votes.

Numerous blockchain-based applications have been proposed in the last decade. Yadav et al. [11, 12] proposed a trust-based consensus mechanism they have suggested a land registry management system to improve and secure land registry data. Singh & Vardhan [10] have proposed DLT based real estate transaction mechanism that emphasizes on keeping the block size smaller for faster operations. Further authors in [13, 14] propose that if blockchain based e-governance applications have to cater to people living in remote areas with little Internet connectivity, then one has to compute optimal block size for increasing the efficacy of the real estate transaction mechanism. Cocco et al. [15] discussed sustainable development and the blockchain's potential as a banking technology, taking into account the Bitcoin framework. Santander [16] initiated the use of blockchain technology for real-time trading in Spain. Schwartz et al. [17] proposed a Ripple protocol consensus mechanism for decentralized and distributed payment systems.

Blockchain technology has also been employed in various new technologies. Singh et al. [18] introduced a wallet transaction framework based on blockchain for the inter-bank transfer of wallet money. Singh and Vardhan [19] suggested an e-stamp procurement method based on DLT, which addresses its usefulness regarding the stamp paper's validity for real estate transactions. Yadav et al. [20] suggested a land registry management system framework that provides an efficient round-robin-based consensus mechanism. Singh and Vardhan [21] proposed a blockchain-based decentralized and stable P2P infrastructure to handle e-stamp and property registration systems utilizing IoT-based devices. Singh et al. [22, 23] proposed a blockchain-based concept of e-cheques

for cheque settlement through an online banking system. The authors utilized e-cheque to address issues like double-spending and counterfeiting. Yadav and Kushwaha [24] proposed a query optimization in blockchain based land registry system reduces the searching time of land record.

Esposito et al. [25] suggested a smart city managing infrastructure, multiple infrastructures owned by a given company. The author discusses the blockchain-based authorization and authentication of smart city decentralized eco framework system. Ouaguid et al. [26] introduced an Android application that is based on a blockchain framework. This aims to provide transparency, reliability, availability in the term of without resorting to a central processing unit judged of trust. The author has proposed a wallet-based financial transaction and provides trust-based security. Li et al. [27] suggested security on smart city applications based on cloud computing environment framework. Tewari and Gupta [28] discussed a lightweight authentication protocol to ensure DDOS attacks, tracking, and replay. The author also reduces the cost of communication and storage data. Shi et al. [29] suggested a trust-based methodology that provides data consistency, non-reputation, authenticity, and data traceability. The author has proposed a decentralized framework based on the AAA scheme data accessing technique, blockchain account address, access control, and authentication of stored data on the blockchain. Liang et al. [30] have proposed a decentralized trusted crowdsourcing mechanism for smart cities based on the blockchain-based framework. Feng et al. [31] implemented a blockchain-based data-sharing model that is both safe and efficient. The author addresses a security auditing system that utilizes a smart contract, public-key cryptography, and a distributed ledger. Zhang et al. [32] have proposed an intelligent decision-making system to improve data evolution and processing.

The consensus mechanism used in various blockchains can be classified based on different characteristics and functionalities. These can either be incentivized or non-incentivized consensus, meaning that the nodes are either rewarded for participating in the consensus process or not. Two of the most popular consensus methods are the PoW [4], PoS [8] consensus mechanism.

PoW is an incentivized consensus method where nodes are rewarded for creating new blocks and adding them to the chain. Miners must solve a cryptographic puzzle to connect the block to the blockchain in this case. The miners are provided with incentives when the puzzle is solved and therefore make use of high-end, computationally expensive devices to be the first to solve the puzzle. In this way, every block helps validate the next subsequent block, resulting in the blockchain.

However, the main drawback of the PoW approach is that the energy consumption required to generate hash power for solving the puzzle is very high. PoW also leads to centralized mining pools as miners join their resources to increase their chance of creating a new block. Further, the algorithm is inherently altruistic as it rewards miners for correct block addition but does not penalize a misbehaving miner node.

PoS is another kind of consensus algorithm that works on the idea that nodes who wish to participate in the consensus process must invest some stake in the network. This stake acts as a guarantee that the nodes will not cause harm to the system. PoS leaves a lesser carbon footprint and is lesser computationally expensive as compared to PoW. However, it results in the problem of "rich getting richer, meaning nodes with a larger stake in the system can exert greater influence. It also threatens the blockchain system's decentralized nature since stakeholding creates a monopoly in the system where participants have control and make authoritative decisions.

Delegated-Proof-of-Stake (DPoS) [33] typically aids in implementing the original PoS consensus model with increased pace, which raises security concerns. Inside blockchain, it is also referred to as democracy since different coin holders vote for block producers' delegation. Furthermore, in contrast to PoW, DPoS typically helps in providing much faster processing-based transactions. However, DPoS has a variety of flaws, including less decentralization and various forms of security problems. In terms of DPoS a delegate is elected to vote on behalf of other users. As a result, the voters hold the power. The voted witnesses can be excluded from power if they underperform or mislead their constituents, and a new delegate can be elected. The delegates' privileges are allocated to the people who chose them. Just a few users have access to the validation process. The delegates, who have the duty and authority to validate blockchains, may misuse their power because the system allows users to select individuals to represent them. The presence of cartels in the system renders the system vulnerable to attacks and makes blockchains less decentralized.

As mentioned above, in the existing consensus approaches, most of the time is spent in solving the cryptographic hashes or requires some form of stake in the system. The consensus process causes an overhead of a large number of message exchanges and dangers of monopoly.

The load-balanced [21] & trust-based [23] approach maintains each minor status table, including node ID, CPU load, computational resources, CPU load status, and other miners' trust values. Later, the miners' trust value is updated based on each block's final consensus and the historical correctness of the transactions carried out by the miners.

The literature review's research gap establishes the need for a blockchain-based framework to implement efficient, quick, fraud-free, tamper-proof, and trustworthy property transactions. Existing approaches consume too much time for transactions and do not provide a proper framework for the land registry process. The involved consensus approaches exchange a lot of messages, thus increasing the overhead of transactions. This article proposes an efficient and fast consensus mechanism and a blockchain-based land registry system that works effectively with minimal messages.

3544

Peer-to-Peer Netw. Appl. (2021) 14:3540–3558

3 Proposed blockchain-based e-registry system

The idea of a novel land record management system for handling land registries has been proposed. The proposal has been described in five subsections. The network architecture for the detailed e-registry transaction structure is explained in subsection 3.1. Any seller or the buyer would buy or sell the properties through the e-stamp papers provided by the e-registry facility of the proposed e-portal system, as demonstrated in subsection 3.2. The system creates an e-register to store the transactions. Blockchain technology is being used to implement the proposed system. All land registry offices willing to adopt the proposed system should adhere to a blockchain-based platform and utilize the proposed e-registry facility. The registry office verifies the possession of the land, and payment of the registration fee, as discussed in subsection 3.3. Blockchain technology generates blocks for land ownership records, which is elaborated in subsection 3.4. The proposed blockchain technology utilizes a novel proposed consensus algorithm for leaders' elections, illustrated in subsection 3.5.

3.1 Underlying network architecture for the proposed system

The existing land registration process includes various activities, such as stamp paper acquisition, calculation of land registration fees, record-keeping of ownership transfer, etc. These activities are carried out in the authorized registration offices of the district. The proposed framework transforms this approach into a blockchain-based application. The network entities involved in the proposed system are numerous registration offices of different districts, which have the validator installed on their machines. These validator nodes will form a common P2P network and all the validator nodes in other regions. The registration offices also replicate their web server as per the requirement of the blockchain. Some professional miners are also employed who possess cutting-edge state-of-the-art hardware resources. All these entities are connected to a distributed cloud server. The underlying network is configured to enforce this blockchain-based proposal for smooth functioning via registration offices. The network architecture of the proposed e-registry framework is shown in Fig. 1.

The IPFS platform enables developers to share content-addressable data and allows for mining policies and consensus approaches. In the IPFS network, each validator node has an individual/unique address. An IPFS node connects to several other approved peers (nodes) in the network via a bootstrap server. The IPFS bootstrap server lists active peers from which the IPFS daemon knows about the other network's other peers.

Stamp duty and land transaction registration fees differ in each state of the country. The regional registry office (Sub-Registrar Officer (SRO) and Registrar Officer (RO)) verifies the land transaction on a multilevel verification basis. Both regional validators (miners) are linked using the P2P network in the proposed system and contain a complete copy of the blockchain. The framework may have intra-district (within a district) or inter-district (among various districts) validators connected over an InterPlanetary File System (IPFS) network. The IPFS network is decentralized, swarm-based P2P, i.e., a swarm node does not communicate with a centralized server but instead communicates with all peers belonging to the same network.

The Government Land Registry Office (GLRO), verify the land transaction at multilevel by both registrar and sub-registrar offices. The first SRO verifies all documents submitted, including land map plans, proofs of identification, and witnesses id. Once the paper has been checked, the SRO forwards it to the registrar's office. The registrar authenticates the document and checks it for formal specifications such as specifying the parties' and witnesses' signatures and the deed's format. After verifying the land, the buyer/seller, and witnesses, the registrar's office issues the buyer's registered deed.

The regional office's primary responsibility in regions is the generation of e-registry documents. The area is made up of numerous registry offices and nodes that are linked via a web server. An area is associated with a web server that stores the regional database of land records. Registry office miners are participants of the GLRO. They can be listed as "Highly Trusted Registry Office Miners (HTROM) or Low Trusted Registry Office Miners (LTROM)." The APM nodes perform essential functions, which include mining and transaction validation. APM enables registry offices to do things more and scale because of the APM miner employee's substantial computational resources. It reduces ROM overhead costs, as the regional miner is controlled by the government, which is already overburdened with deed registration and other routine operations.

Clients request the transaction (buy/sell) by sending the details. The validator validates the transaction and adds it to the transaction pool. The leader miner generates a block after a sufficient number of transactions have been added to the transaction pool. It is the leader's responsibility to mine the new blocks; hence, consensus needs to be achieved on the newly created block. Once a block is created, the transactions in the block need to be verified before it becomes part of the blockchain. The block is assigned to the miners' leader, who has contributed the most to the mining process to earn it. Consensus mechanism verifies the block's transactions. The newly generated transaction block is then subjected to consensus. Finally, the blockchain is updated with the agreed-upon block. The responsibility for maintaining the blockchain, mining the block, validating and verifying transactions, and responding to land verification requests lies with the validator nodes.

The registration office's web servers will connect end-users to the proposed framework for general land/property information
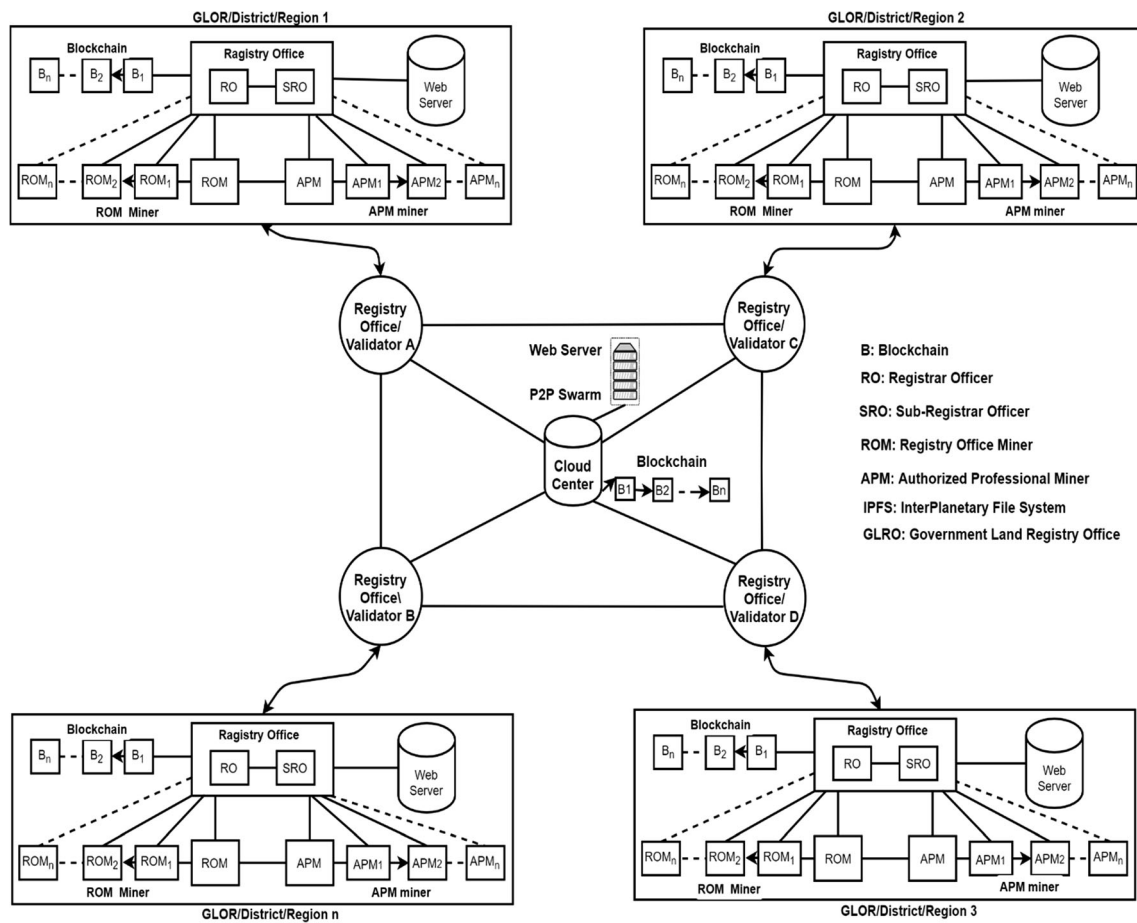
Fig. 1 Network architecture of the proposed e-registry framework

inquiry. The proposed e-registry transaction framework is planned to be entirely controlled by the Government of India. The government will monitor the blockchain network, mining policies, and consensus process in this way. Thus, the proposed framework gives the government complete control of all the organizations involved in registry transactions. The government will eventually have complete control over the documents contained in the blockchain.

All validation nodes from all regions are linked and maintain the shared blockchain with the P2P swarm network. The process of land registration needs to be digitized after developing the proposed network model. The land registration process requires, in general, the following essential steps:

i.   Stamp procurement and stamp duty payments.
ii. Verification of land and possession and payment of a registration fee.
iii. Data keeping and document creation for ownership.

The proposed architecture is structured to keep policies the same and safely digitize and automate only the processes. The complete transaction process is explained in the following subsection.

3.2 Proposed stamp-procurement and stamp-duty payment process

In India, ownership updates primarily occur through sales transactions carried out through property registration. This registry document is evidence of the property's sale and helps to hold land records. A stamp procurement system has been suggested in this article to promote e-stamp procurement. The proposed e-stamp procurement system aims to digitize the purchase of stamp documents as e-documents. Organizations that are allowed to sell the e-stamp connect with a blockchain network across the e-stamp sales and procurement system. Figure 2 demonstrates the method of e-stamp procurement for stamp-duty payments using blockchain technology.

- Using an e-stamp calculator, the buyer calculates the stamp duty and pays the stamp duty through the Stockholding Corporation of India Limited (SCIL) or any other registered agency's e-stamping system [34].
- After raising the challenge (fraud relating to property documents, stamp duplicacy, stamp verification, and evasion of stamp duties) through the registry office, the buyer

3546

Peer-to-Peer Netw. Appl. (2021) 14:3540–3558

Fig. 2 Stamp-procurement and
stamp-duty payment process

Fig. 2 Stamp-procurement and stamp-duty payment process
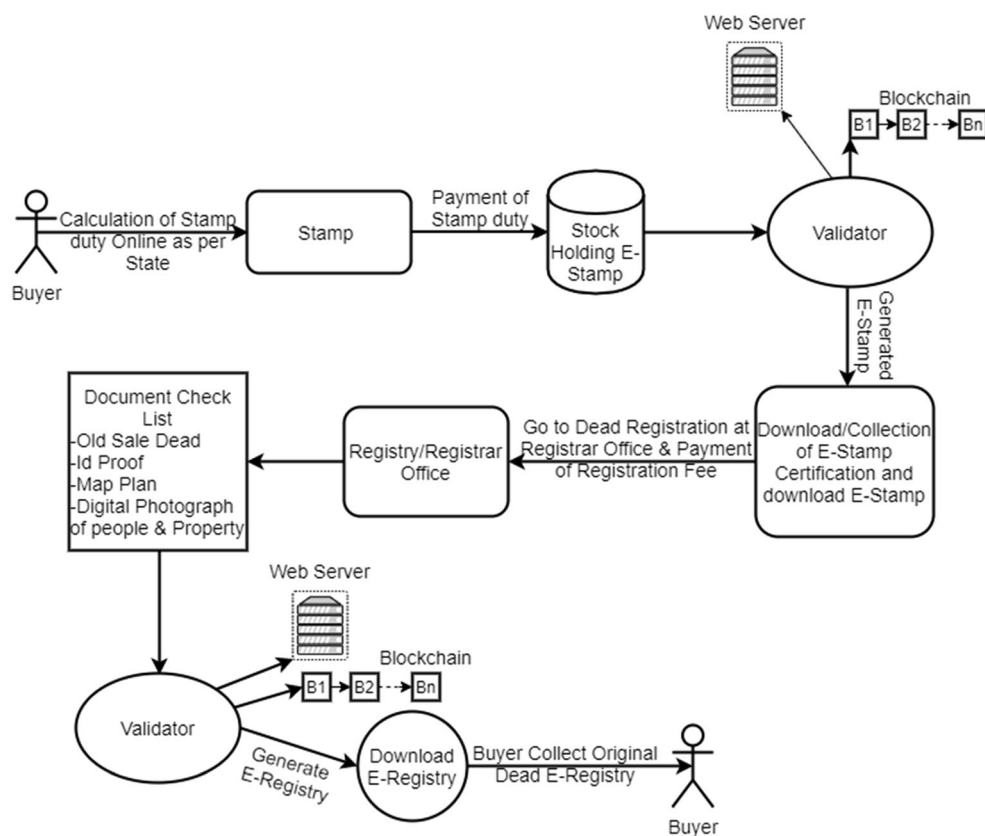
measures the stamp duty and pays electronically or through bank deposits treasuries & accounts department.

- The validator validates the stamp fee payment and produces the e-stamp, and the buyer obtains an e-stamp certification.
- After obtaining proof of payment of the registration fee, the buyer submits it online to the registration office.
- The registry office verifies all documents submitted, including the old property sales deed, identity proof, map plan, digital image, property, etc.
- Validators create e-registry, and a new block in the blockchain is added. The buyer retrieves the final registry document/record.

The validator validates the transaction, and the blockchain ledger is added with a new block of data. The blockchain ledger stores the e-stamp certificate.

3.3 Land and ownership verification and payment of registration face

The buyer/seller system's proposed transaction mechanism is elaborated in this section. The workflow of requests for an e-registry generation is illustrated in Fig. 3 where the registry office validates the land information via the registrar validator.

The verification of land ownership and transfer is done using blockchain technology. The validator verifies the application, approves the digital hash registry and the seller/buyer's signature, and finally approves the transaction. The validator sends the verification report to the office of the registrar. The registrar's office then generates the transaction for e-registry. The seller/buyer downloads concerned documents via a web portal e-registry. The transaction pools for the e-registry transactions are queued at registry offices are managed. The registry offices append the transaction block to the blockchain after a consensus process. The step-wise details of the e-registry transaction process via the proposed system are as follows:

- A pair of private and public keys are issued to all the sellers/buyers. All the transactions are signed digitally using the private key of the seller/buyer to generate the e-registry.
- Both buyers/sellers use the public key to verify the e-registry by the validators. The e-registry generated has a unique number printed on it.
- The validator verifies the seller/buyer's digital signature during the authentication of this newly created e-registry.
- The transaction is added to the transaction pool after verifying the digital signature, and the validated e-registry is generated later.

Fig. 3 Transaction process of buyer/seller
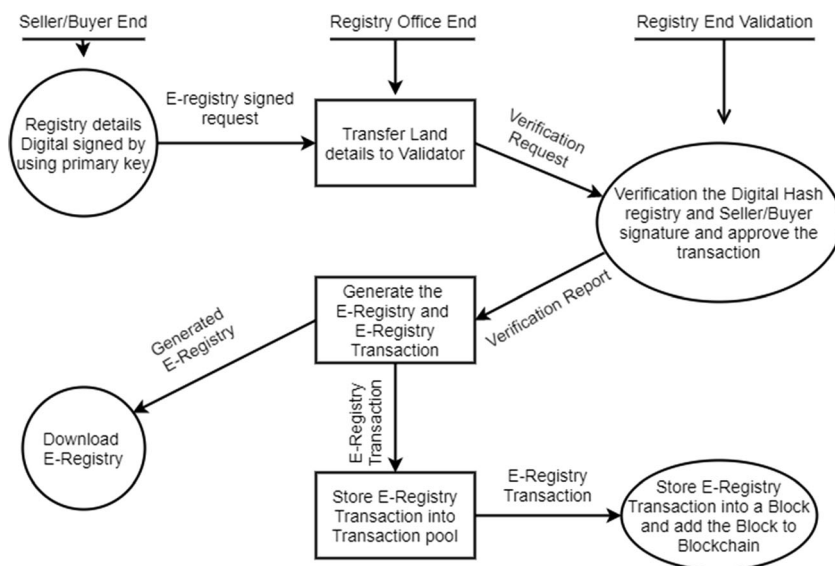
- The registry office portal now enables e-registry to be accessed by the seller/buyer. A validator stores the collection of these checked transactions in a block.
- This validated e-registry should be registered as a transaction on the blockchain until all validated e-registries provided by various entities can be cleared.

3.4 Record-keeping and ownership document generation

For developing a unique blockchain, the block structure must be defined. All of the transaction's essential entries should be placed within the block. The different attributes of land registry transactions are illustrated in Fig. 4. These attributes include details of the property, transaction ID, details of the buyer, and the seller's details. In the context of transactions, the data transmitted by the seller/buyer is processed. A block is generated by the leader validator and sent to the other validators. The process of leader selection among validators has been explained in section 3.5.2. After the validator's review process is complete, the consensus process is used to achieve a final consensus. Depending on the outcome, whether consensus is achieved or not, the block is either added to the blockchain or discarded. The SHA256 cryptographic algorithm is used to obtain the digital document hash and store it in the concerned block. The required acronyms and its corresponding description used in the article has been briefly illustrated in Table 1.

The set ER contains all the attributes of the E-Registry, as defined below:

$$ER = \{\Omega_H, \psi, \psi_L, \mu_A, \gamma_{ES}, \gamma_{ID}, \gamma_{SD}, \lambda_H, \sigma_{DS}, \alpha, \alpha_I, \alpha_{FN}, \alpha_A, \alpha_C, \alpha_S, \alpha_{PC}, \beta, \beta_I, \beta_{FN}, \beta_A, \beta_C, \beta_S, \beta_{PC}\}$$

The set ER is secured through the buyer's digital signature, computed using the SHA256 algorithm.

$HashER = SHA256(ER)$

The seller signs with its private key the set ER and its hash. $DS\alpha pr$ and $DS\beta pu$ represent the seller's private and public keys, respectively. Using the ERDS algorithm, the digital signature is obtained as:

Digital signature = ECDS ($DS\alpha pr$, Hash_ER, ER)

Internal miners check the same after the digital signature has been obtained. A copy of the e-registry is generated and given to the buyer. The hash generated by e-registry is also documented in the transaction on the server-side. The e-registry created is represented by an 'R' file, and this file's hash is computed as:

Hash_R = SHA256(R)

Hence, the complete transaction is represented by set TX as:

TX = {ER, Hash_ER, digital signature, Hash_R}

This transaction is added to the global transaction pool and is then included in the block during the mining process.

3548

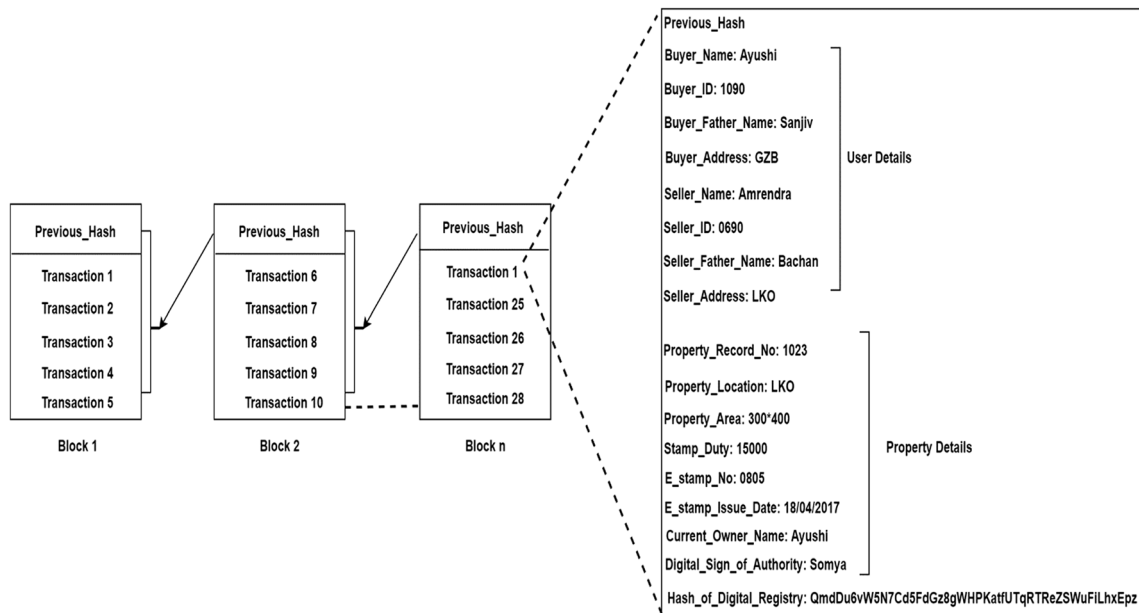Peer-to-Peer Netw. Appl. (2021) 14:3540–3558

Fig. 4 Block record transaction for buying/selling registry

3.5 Proposed trust value-based consensus approach (TrVCA)

Distributed systems rely on a process that produces a single value through consensus. Several reliability algorithms have been suggested to improve the overall network performance when there are problems with unavailable nodes. Examples of consensus algorithms include PoW, PoS, DPoS, etc. A consensus must be achieved before adding a new block into the blockchain. This article proposes a consensus mechanism, named Trust-Value based Consensus Approach (TrVCA), that applies multicasting to minimize network load and allow consensus on a more significant number of transactions quickly. The proposed method of consensus decreases the effort to add and make a new block secure and synchronized.

Synchronizing the general ledger of transactions over the network ensures that the ledger blocks are only updated when the corresponding participants approve the transactions, which is an essential activity. It can become part of the blockchain only for valid transactions. Validation is done only when a node in the network offers a guaranteed transaction ordering mechanism and validates the transaction block. In the blockchain, adding a block is performed by the network miners. When any buyer/seller requests a transaction, the information relating to their identity and the property must be requested. Finally, the Leader Miner (LM) generates and broadcasts a block to all the network nodes. The leader chooses some nodes to participate in the validation process, and these nodes, as mentioned in the following sub-section, are called Validator Miners (VM).

Inside the blockchain, the validator is accountable for verifying transactions. Each VM verifies the transaction by

searching and sending the LM's response to its respective blockchain. In the proposed property transaction system, two types of miners are involved. The first type is Authorized

Table 1 Acronyms and symbols description

Acronym/Symbol	Description
Ω_H	Previous_Block_Hash
ψ	Record Number of Property
ψ_L	Location of Property
μ_A	Area of Property
γ_{ES}	Serial number of E-Stamp
γ_{ID}	Issue Date of E-Stamp
γ_{SD}	Stamp_Duty
λ_H	Digital Registry Hash
σ_{Ds}	Authority for Digital Signature
α	Seller_Name
α_I	Seller_ID
α_{FN}	Seller_Father_Name
α_A	Seller_Address
α_C	Seller_City
α_S	Seller_State
α_{PC}	Seller_Postel code
β	Buyer_Name
β_I	Buyer_ID
β_{FN}	Buyer_Father_Name
β_A	Buyer_Address
β_C	Buyer_City
β_S	Buyer_State
β_{PC}	Buyer_Postel code

Professional Miners (APM), who invest in cutting-edge infra-structure at these farms and provide services to their proper-ties. The Registry Office Miners (ROM) are the second type of miners, which are nodes of registry offices.

3.5.1 Trust value computation through proposed approach

This proposed e-registry would use two distinct miner types: one from the registry office and another from an Authorized Professional Miner (APM). There are HTROM and LTROM are registry office miners. The second APM framework in-vests in state-of-the-art infrastructure and provides services to allow investors to cash in their returns. When a miner joins the InterPlanetary File System network for the first time, they are given a fixed Trust Value (TV) (30 is our proposed mech-anism). The ROM is divided into two categories by the trust value table: HTROM and LTROM are two different miners types. The process of trust value computation begins simulta-neously at each node by obtaining the final consensus. The trust value is determined by the accuracy of the verification response time of a newly created block. Below is a description of the trust value computation mechanism (We have set the initial trust value to 30 and the maximum threshold to 120 as mentioned in algorithm 1).

```
Algorithm 1:  Computation of Trust Value Mechanism
 1:  Input: Final_consensus_result (consensus result of verified block), CM (Consensus Minor)
 2:  Output: Trust_value (updated trust value of each CM)
 3:  Procedure: Trust_computation()
 4:      for each CM
 5:          if CM is new
 6:              CM.trust_value=30 // initializing trust value of CM while if newly joined
 7:          if CM.response == final_consensus_result
 8:              if CM.trust_value < 0
 9:                  CM.trust_value=0
10:              else if CM.trust_value > 0 and CM.trust_value < 120
11:                  CM.trust_value += 3
12:              else if CM.trust_value == 120  // 120 highest threshold value
13:                  No change in trust_value of consensus_minor
14:              end if
15:          else
16:              CM.trust_value -= 12 // Consensus Minor response is invalid
17:          end if
18:          if CM.response_time < 30 // if response time is less than 30 ms
19:              CM.trust_value += 2
20:      end for
21:  End procedure
```

Miners/nodes with a trust value of less than 20 are consid-ered less trustworthy. These miners will be not be permitted to take part in the consensus process. After each new block is created, the trust value table is updated. Based on the new block's correct or incorrect verification and response time, the trust value is incremented or decremented. The same is depicted in Table 2.

3.5.2 Selection of leader miner

The block mining process needs to be synchronized to pre-serve blockchain consistency. The leader election process holds responsibility, of maintaining continuity in the blockchain by synchronizing the mining method. The leader

Table 2 Miner status table of trust value

S. No.	HTROM		LTROM		APM	
	PEER ID	TV	PEER ID	TV	PEER ID	TV
1	N	35	K	18	O	50
2	V	65	T	13	S	56
3	X	52	M	14	Z	59
4	L	74	Y	18	P	63

election mechanism for miner, select miners from several miners for each block's mining phase, as discussed in algo-rithm 2. The new block is mined by this leading miner and sent to all miners for the transaction validation process. Only 50% of HTROM nodes and 50% of APM nodes for a fixed time slot will pick a leader. These nodes are known as nodes of the validator. In this method, LTROMs are not picked. APMs receive incentives from the registry offices for the cre-ation of a new block. A block specification needs to be checked after building a block before being added to the cur-rent blockchain. Verification is performed by the validator nodes, followed by voting for that block.

The miner's leader and consensus receiving votes are ob-tained. The bootstrap server for the proposed system main-tains a list of all active miners. The bootstrap server is then used to allocate mining slots to miners. Any validator of this registry office assumes the proposer's function when transac-tions occur in any registry office, generating the block during its time slot. Also, some miners participate in the process of consensus.

1. A block is created by fetching a certain number of trans-actions from a pool of transactions.
2. This block is broadcast to the entire network's peers.
3. 50% of HTROM nodes and 50% of APM nodes are selected.
4. A multicast consensus signal is sent to the consensus validator.
5. The peer waits until the consensus validator sends a con-sensus validation report.
6. The D_i's from the consensus validation report are added. (D_i's = consensus validation signal)

   a. If the sum is not equal to the "Consensus Validation Report," then waiting for the consensus validation report (V_{RB}) continues.
   b. If the sum is equal to the "Consensus Validation Report," then V_{RB}'s are compared to find the major-ity value out of them. (MejV_{RB} = Majority of valida-tion report)
7. The selected V_{RB} checks whether it is valid or not. (V_{RB} = Validation Report)

3550

Peer-to-Peer Netw. Appl. (2021) 14:3540–3558

a. If V_{RB} is valid, then the block is added to the ledger.

b. If V_{RB} is not valid, then the block is discarded.

8. Trust is updated based on the validation report.

9. Peers are notified about the transaction.

Algorithm 2: Leader Validator Selection

1: **Input**: *SetOfTransactions, ConsensusValidationReport*
2: **Procedure:** Leader_Validator _Selection(node_id)
3: *Block = generateBlock(SetOfTransaction);*
4: *broadcastBlock();*
5: *selectMiner();*
6: *sendConsensusSignal();*
7: *ConsensusValidationReport = getValidationReport();*
8:   ***if*** *(sum(D_i) == ConsensusValidationReport) then*
9:     *MejV_{RB} = majority(ConsensusValidationReport);*
10:   ***else*** *Goto 5;*
11:   ***end if;***
12:   ***If*** *(valid(MejV_{RB})) then*
13:     *addBlock();*
14:   ***else*** *discardBlock();*
15:   ***end if;***
16:   *updateTrustValue();*
17:   *notifyPeers();*
18: ***End procedure***

3.5.3 Selection of consensus validator

To mine and add a block to the blockchain using the existing consensus mechanism - PoW - requires a significant amount of computational power and time. We also suggested a consensus TV based agreement structure in place of a hash power strategy instead of the PoW. This new proposed algorithm minimization reduces block addition time and uses fewer message exchanges than the current proof-of-work. Each node retains its TV, which is modified regularly. The trust value table displays both the peer ID and the peer's TV.

Here, Leader Miner (LM) randomly selects 50% of HTROMs and 50% APMs for the consensus process. Consensus Miner (CM) refers to the nodes that have been chosen. Each CM broadcasts its vote and peer id to the network's nodes. After receiving the final consensus result, all nodes will change the trust values for each consensus miner in the table. The final consensus outcome is determined by measuring majority vote. If the block is validated, LM incorporates it into its current blockchain. Additionally, LM broadcasts the block's hash to all nodes. Subsequently, as discussed in algorithm 3, all other nodes may also connect the block to their respective blockchains.

B – Broadcasted Block C – Consensus Signal

1. Using digital signatures, the broadcast block and the consensus signal are verified.

2. A report on the validity is produced.

3. V_{RB} are transmitted to any network peer.

4. The summation of D_i's is achieved when the consensus validation report is received.

5. This number is compared with the "Validation of Consensus Report."

a. If the amount is not equivalent to the "Validation of Consensus Report," then the consensus validation report continues to wait.

b. If the number is equal to the "Validation of Consensus Report," V_{RB} is compared to finding the majority value out of them.

6. The selected V_{RB} tested whether or not it was correct.

a. The block is added to the ledger if V_{RB} is valid.

b. If V_{RB} is not valid, then it discards the block.

7. Based on the validation report, the trust value is updated.

8. For the next block, step 1.

Algorithm 3: Consensus Validator Selection

1: **Input:** *Block*
2: **Procedure:** *Consensus_Validator_Selection*
3: *validateBlock(Block);*
4: V_{RB} = *generateValidityReport();*
5: *broadcast(V_{RB});*
6: *ConsensusValidationReport = getValidationReport();*
7:   ***if*** *(sum(D_i) == ConsensusValidationReport) then*
8:     *MejV_{RB} = majority (ConsensusValidationReport);*
9:   ***else*** *Goto 4;*
10:   ***end if;***
11:   ***if*** *(valid (MejV_{RB})) then*
12:     *addBlock();*
13:   ***else*** *discardBlock();*
14:   ***end if;***
15: *updateTrustValue();*
16: *Goto 1;*
17: ***End procedure***

3.5.4 Consensus of remaining nodes

The remaining nodes again perform the leader selection process to select a new LM. The LM accesses a specific transaction pool to create a new block. This block is broadcasted to other nodes of the validator, as discussed in algorithm 4. The LM stores the block in the temporary buffer and waits for the block to be checked by the remaining validator report. The validators, including the consensus agents, request and store the newly created block in the proposer's temporary buffer. All validators are now awaiting the vote of the nodes participating in the consensus process. Each validator maintains a status table of validator nodes. Thus, the consensus agents can be established by any validator waiting for consensus.

1. When the broadcasted block and the consensus validation report are received, the summation of D_i's is done.

2. This sum is compared with the "Consensus validation Report."

a. If the sum is not equal to the "Consensus Validation Report," then waiting for the consensus validation report continues.

b. If the sum is equal to the "Consensus Validation Report," then V_{RB} are compared to find the majority value out of them.

3. The selected V_{RB} has checked whether it is valid.

a. If V_{RB} is valid, then the block is added to the ledger.
b. If V_{RB} is not valid, then the block is discarded.

4. Trust value is updated based on the validation report.

5. Step 1 for the next block.

Algorithm 4: Consensus of Remaining Nodes

1: **Input**: *Block*
2: **Procedure:** Consensus among Remaining Nodes
3: *ConsensusValidationReport = getValidationReport();*
4:   **if** *(sum(D$_i$) == ConsensusValidationReport) then*
5:     *MejV$_{RB}$ = majority(ConsensusValidationReport);*
6:   **else** *Goto 1;*
7:   **end if;**
8:   **if** *(valid(MejV$_{RB}$)) then*
9:     *addBlock();*
10:   **else** *discardBlock();*
11:   **end if;**
12: *updateTrustValue();*
13: *Goto 1;*
14: **End procedure**

3.5.5 Selection of validator node

The buyer/seller generates the transaction for the land registry. The buyer/seller's node broadcasts the request for selecting validator nodes, which is based on the majority of votes received by all nodes corresponding to the trust value of miners. The validator nodes select a leader based on the consensus mechanism. The remaining nodes again select a new leader and wait for the validation process to be completed in validator nodes. After the validation is done, the remaining nodes update their table as per the trust value of validator nodes. All nodes in the blockchain network are sent a proposal to add the transaction block as per the request generated by the seller/buyer. All peer nodes run the validator leader module, which is used to determine if a block should be added to the blockchain-based on its validity, as discussed in algorithm 5.

1. The user node broadcasts the transaction in the network.

2. The validator leader creates a block (B) from a pool of transactions and broadcasts the network's block. It also sends consensus signals to nodes responsible for arriving at a consensus.

3. The consensus nodes generate a V_{RB} and broadcast it in the network to every peer.

4. Each peer on getting the broadcasted block and V_{RB} calculates a majority based on TV.

5. The ledger has now been updated, and the user has been notified of the transaction.

The validator nodes verify the block's validity by using their replica of the regional database to decide if the seller owns the property. If the seller does not own the land, then the transaction is invalid. If the seller owns the land, then only the land can be sold. Now the response to the block proposal is sent in the form of votes to the leader node. The nodes then append the validated block in their blockchain.

Algorithm 5: Validator Node

1: **Input**: *Transaction*
2: **Procedure:** Validator_Node
3: *User.broadcastTxn();*
4: *validateLeader.createBlock();*
5: *validateLeader.broadcastBock();*
6: *consensusPeer.generateValidityReport();*
7: *consensusPeer.broadcast(V$_{RB}$);*
8: *Peer.updateTrustValue();*
9: *validatorNode.notifyUser();*
10: **End procedure**

---

4 Comparative analysis of performance

The proposed Trust-Value-based Consensus Approach's (TrVCA) performance is computed in terms of validity and robustness. The proposed land registry management system has been implemented in the InterPlanetary File System (IPFS) installed on a Windows 10 machine. We have implemented a decentralized framework by adopting various hardware and software tools, as summarized in Table 3.

The efficiency of the system is determined by varying the number of miners. Each miner's ability to traverse blocks in search of buyer/seller information is restricted. Already, several blocks have been added to the blockchain. Moreover, each miner makes a new transaction to ensure that they traverse a predetermined number of blocks. The number of miners is then increased, and the execution time is measured in message exchanges or seconds. The TrVCA's performance is compared to that of other approaches using the following two parameters:

1. Number of Message Exchange (NME),
2. Execution time

4.1 Comparison based on total number of messages exchanged (TNME)

The performance of the proposed TrVCA is measured in terms of the number of messages required to achieve consensus. The comparison could only be done with the PoW approach as other approaches had a non-deterministic process that would change for various scenarios. Table 4 illustrates overall messages needed to achieve consensus using the Proof-of-Work and method proposed TrVCA. Assume there are 'N' nodes in a network. All 'N' nodes participate in the consensus in the Proof-of-Work approach, and each

3552

Peer-to-Peer Netw. Appl. (2021) 14:3540–3558

Table 3 Hardware and software specification

Server Specification	
Hardware	• CPU: Intel® Core™ i7–7700 CPU @ 3.60GHz 3.60 GHz
	• RAM: 8.00 GB
Software version (including tool and standards)	• Operating system: Windows
	• IPFS 0.5.0
	• C language
	• GCC compiler 10.2
	• 1 GbE Data Rate Per Port
	• Storage: 4*150 GB
Application	• Land registry management system
Implementation Parameters	
Block size	• 8 MB
Block hash size	• 256 – bit
Nodes	• 10, 20, 30, 50, 100, 150, 200, 250, 300, 350, 400, 500, 600, 700, 800, 900, and 1000 (Numbers of Nodes over exchange massages)

broadcasts its vote to all 'N-1' nodes after verification. Therefore Proof-of-Work requires a total N*(N-1) exchange of messages. Because fewer 'M' nodes are chosen to participate in the consensus process, the proposed approach TrVCA necessitates lower message exchange rates. M*(N-1) messages are exchanged as a result of this method. Among all these nodes N, let N1, N2, and N3 are the total number of miners in the group of LTROM, HTROM, and APM. Let C1, C2, and C3 be selected nodes for the consensus process from N1, N2, and N3. The total consensus agent selected from the C1 group is defined as (N1*50)/100, for the C2 group, it is

defined as (N2*50)/100, and for the C3 group it is defined as (N3*0)/100. Because the proposed mechanism prevents nodes from the LTROM category from participating in the consensus process, the number of miners in group C3 is zero. As a result, the required Total Number of Messages Exchange (TNME) for the proposed algorithm TrVCA is:

$$TNME = (C1 + C2)*(N-1)$$

The TNME needed for final consensus by the TrVCA and PoW is shown in Table 4. After mining, the number of miners

Table 4 Analysis of the proposed and PoW algorithm in terms of message exchanges

S. No.	N	N1	C1	N2	C2	TNME (PoW)	TNME (TrVCA)	Message Reduction (%)
1	10	5	4	2	2	90	54	**60**
2	20	9	6	4	5	380	209	**55**
3	30	14	8	6	10	870	522	**60**
4	50	22	12	11	16	2450	1372	**56**
5	100	45	25	22	30	9900	5445	**55**
6	150	67	38	33	35	22,350	10,877	**48.7**
7	200	90	53	44	48	39,800	20,099	**50.5**
8	250	111	65	55	58	62,250	30,627	**49.2**
9	300	134	76	66	69	89,700	43,355	**48.3**
10	350	156	91	77	85	122,150	61,424	**50.3**
11	400	158	105	80	96	159,600	80,199	**50.2**
12	500	170	119	88	114	249,500	116,267	**46.6**
13	600	185	142	96	135	359,400	165,923	**46.2**
14	700	197	161	107	154	489,300	220,185	**45**
15	800	210	188	118	178	639,200	292,434	**45.7**
16	900	222	201	128	196	809,100	356,903	**44.1**
17	1000	234	225	137	218	999,000	442,557	**44.3**

Bold entries indicate the best results

Fig. 5 Message flow of PoW and proposed approach

M: Miner
CM: Consensus miner
LM: Leader miner

TrVCA

PoW
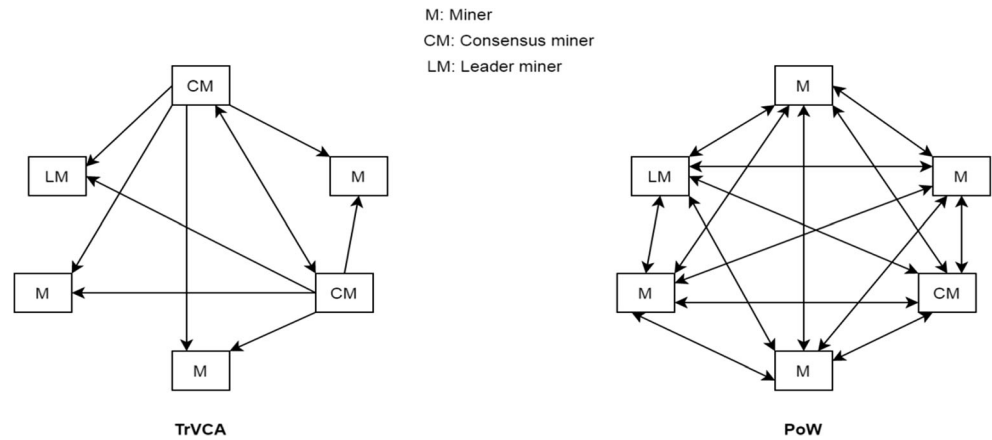
is varied from 10 to 1000 and the total number of messages exchanges is registered. These tabulating outcomes from various simulations show the total number of message entries and the sum of message reduction achieved by the proposed approach TrVCA.

Compared to the conventional PoW approach, the proposed TrVCA approach needs an average of 50.30% message exchange per consensus mechanism. The message flow is depicted in Fig. 5 for both approaches. The left figure, depicts the message flow inside the TrVCA following block verification. One node/miner is designated as the Leader Miner (LM), and a few miners are designated as Consensus Miners (CM). Only CMs are responsible for responding to all nodes. The right-hand side of the figure depicts the message flow in the PoW approach, in which all miners communicate with one another. The statistic does not include the leader's initial messages to all nodes since the messages' total number is identical

in both approaches. The figure demonstrates that the TrVCA needs significantly fewer message exchanges than PoW.

Figure 6 represents the comparison between the PoW and the TrVCA. The performance of the TrVCA is much better than PoW in terms of message exchanges. TrVCA's performance improvement is because it utilizes fewer nodes based on their previous performance in the network's consensus process.

4.2 Comparison based on execution time

The proposed approach's implementation time could be compared to that of conventional methods such as PoW, PoS, and DPoS. The comparative results have been shown in subsection 4.2.1. TrVCA could also be compared with the existing state-of-the-art approaches to measure its performance improvement, as discussed in subsection 4.2.2. In these two

Fig. 6 Message exchange vs. number of nodes

3554

Peer-to-Peer Netw. Appl. (2021) 14:3540–3558
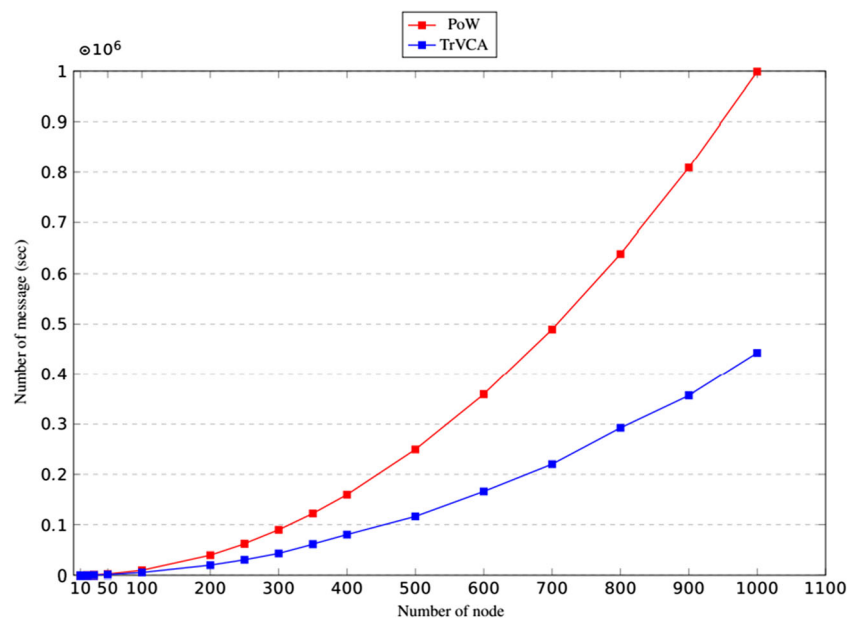
Table 5 Execution time of PoW, PoS, DPoS, and TrVCA in seconds

S. No.	No. of Node (N)	PoW	PoS	DPoS	TrVCA
1	10	129.8	106.2	88.3	**57.1**
2	20	186.2	149.6	125.6	**80.4**
3	30	207.6	183.4	153.2	**93.4**
4	50	296.4	225.3	198.7	**114.5**
5	100	358.2	283.7	252.4	**149.6**
6	150	416.6	319.6	297.6	**184.3**
7	200	476.9	376.3	341.3	**223.6**
8	250	537.3	408.4	383.6	**265.1**
9	300	601.6	458.7	433.2	**303.7**
10	350	663.7	505.3	477.4	**348.2**
11	400	725.1	553.5	525.5	**388.6**
12	500	784.9	604.8	576.9	**431.4**
13	600	848.6	652.7	624.8	**470.6**
14	700	906.5	703.5	674	**512.5**
15	800	970.7	757.7	724.8	**555.1**
16	900	1033.2	809.3	773.6	**596.8**
17	1000	1093.8	858.6	824.8	**639.3**

Bold entries indicate the best results

sections, the execution time to reach consensus on the same block for the TrVCA, conventional approaches, and state-of-the-art approaches is recorded.

4.2.1 Comparison with traditional approaches

Table 5 compares the traditional methods - PoW, PoS, and DPoS - to TrVCA in experiment execution time. The execution times of the PoW, PoS, DPoS, and TrVCA are shown in
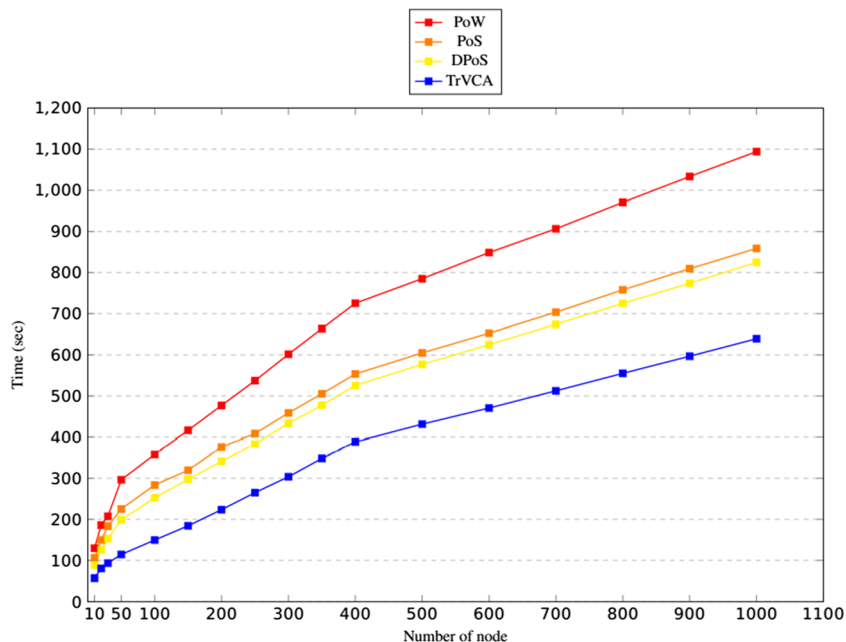
Table 5. The node count is increased from 10 to 1000, and the execution time is recorded. The table contains the results of various simulations used to determine the execution time.

Figure 7 depicts a graphical representation of the number of nodes ranging from 10 to 1000. The proposed consensus algorithm - TrVCA - performs better than the PoW, PoS, and DPoS consensus algorithms. The result shows that the proposed approach-TrVCA reduces execution time by 52.88%, 68.04%, and 72.42%, respectively, compared to PoW, PoS, and DPoS approaches. The proposed consensus algorithm - TrVCA - performs better than the existing approach.

4.2.2 Comparison with the state-of-art approaches

There are two main state-of-the-art techniques utilized for various blockchain applications, which have been described next. A load-aware consensus approach for land registration was proposed by Singh and Vardhan [19] in 2018. Based on the number of transaction requests processed, they proposed classifying the government registry office miners into heavily loaded and lightly loaded.

Singh et al. [21] suggested a trust-based consensus approach. The number of transaction requests classified the miner as either heavily or lightly loaded. 50% of lightly loaded miners and 50% of APM use the method as a load-based consensus miner.

All the approaches need about the same amount of message exchange, as they take up to 50% of consensus miners. The benefit of the proposed approach - TrVCA over the load-balanced approach is the effective load status table, which takes less time to obtain and update the miner's status.

Fig. 7 Number of node Vs. time (Seconds)

Table 6 Execution time of TrVCA and state-of-the-art approaches (in seconds)

| Sr. No	No. of node (N)	Load balanced approach [18]	Trust-based approach [24]	TrVCA
1	10	67.2	30.2	**19.5**
2	20	95.7	30.8	**20.2**
3	30	105.9	31.3	**20**
4	50	129.5	32	**20.2**
5	100	176.9	33	**22**
6	150	224.5	32.8	**21.9**
7	200	274.3	32	**21.2**
8	250	323.2	32.4	**21.3**
9	300	373.1	31	**19.8**
10	350	424.3	31.9	**21.1**
11	400	476.2	32.5	**21**
12	500	581.4	32	**20.2**
13	600	687.8	32.5	**21.4**
14	700	796.9	33.4	**21.1**
15	800	909.6	31.4	**20**
16	900	1023.5	32.2	**19.3**
17	1000	1139.2	32	**19.9**

Bold entries indicate the best results

TrVCA updates a miner status table for faster selection of LM, which is not available for the trust-based approach.

Table 6 compares the existing state-of-the-art approaches with TrVCA based on the execution time. Table 6 illustrated the execution time of the load-balanced approach, trust-based approach, and TrVCA. The number of miners is increased from 10 to 1000, and the execution time is reported. The table shows the results of different experiments used to calculate the execution time.

Figure 8 depicts a graphical illustration of the comparison of TrVCA to current state-of-the-art approaches. The number

Fig. 8 Comparison of load-balanced, trust-based mechanism and TrVCA in seconds

3556

Peer-to-Peer Netw. Appl. (2021) 14:3540–3558
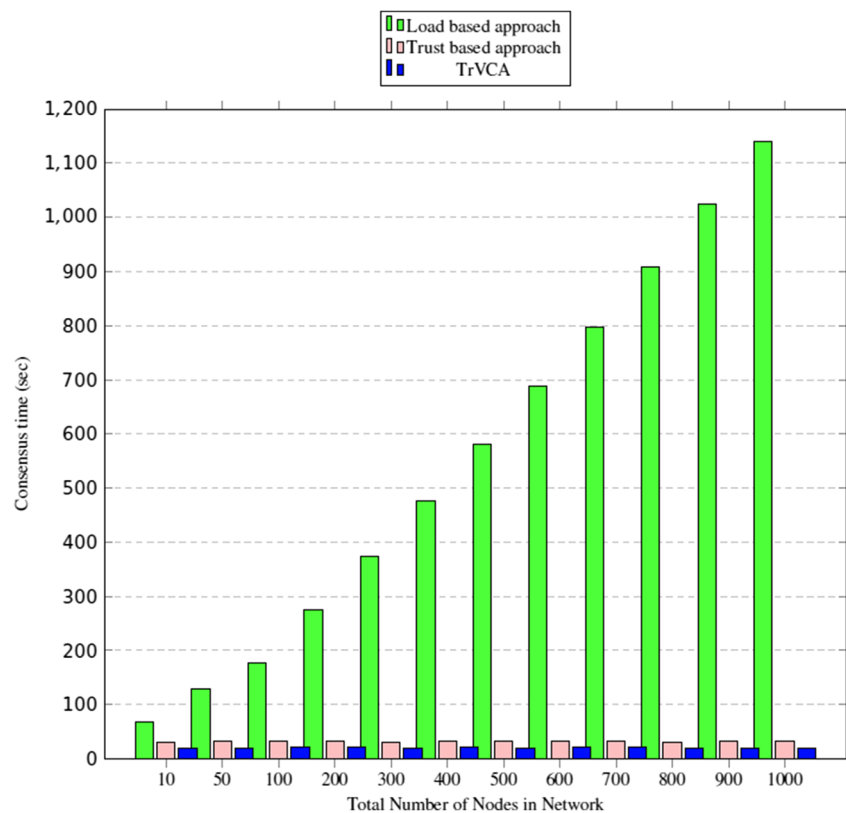
Table 7 Comparison and performance analysis of PoW, PoS, DPoS, Load-based, Trust-based, and proposed TrVCA Approach

Consensus mechanism	PoW	PoS	DPoS	Load-based	Trust-based	Proposed TrVCA
Energy consumption	High	Moderate	Moderate	Less Energy than DPoS	Less Energy than Load Balanced	Low Energy than Trust-based
Advanced hardware	Required	Not required	DPoS is even more energy-efficient than PoS and uses less hardware.	Not required	Not required	Not required
Centralization	Decentralized	Partially	Decentralized than POS and POW protocols	Decentralized	Decentralized	Decentralized
Double spending attack	Theoretically possible	Difficult	Not	Not	Not	Not
Scalability	Not scalable	Scalable	Scalable	Scalable	Scalable	Scalable
Security	With 51% hash power, an attack is feasible, which is impractical in the real world.	Removes 51% attack threat	51% attack can be organized easily because the power of the network is in a few hands	Based on Load and CPU	Based on CPU load & trust based	Based on the Trust value of the miner
Fault Tolerance	50% hashing rate	50% hashing rate	Witnesses could create cartels and again take control of the network	Not	Not	Not
Permission Needed	No	No	Yes	Hybrid Approach	Hybrid Approach	Hybrid Approach

of nodes vary between 10 and 1000. The findings show that the proposed approach - TrVCA - decreases execution time by 64.43% compared to the load-based approach and by 4.48% compared to the trust-based mechanism. The proposed consensus algorithm - TrVCA - outperforms the state-of-the-art algorithms.

Table 7 illustrates the comparative analysis of PoW, PoS, DPoS, load-balanced, trust-based, and proposed TrVCA. Here, we can see all the benefits of the proposed algorithm over the existing algorithms.

5 Conclusion

A blockchain-based framework has been proposed for managing the transactions of real estate. The proposed structure is designed to address the shortcomings of the existing land registry system. All aspects of property transactions can be mapped to the proposed blockchain-based framework. A consensus algorithm has also been proposed to reduce overhead transmissions by about 50% for multicasting nodes. The proposed approach has been established as faster and more efficient than traditional approaches, such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated-Proof-of-Stake (DPoS). The proposed approach also proves it self-superior to the existing state-of-the-art approaches, such as load-balanced and trust-based approaches. Since the proposed algorithm TrVCA has reduced the exchanged message overhead by 50% approximately. Hence, it reduces the execution time by 52.88%, 68.04%, and 72.42% while comparing it with the existing benchmark algorithms PoW, PoS, and DPoS, respectively. Also, the proposed approach TrVCA has reduced the execution time by 64.43% and 4.48% as compared to the load-based approach and the trust-based approach.

The future work includes reducing the blockchain overhead by extending a sidechain to store all related data connected to blocks. Further sidechain will also reduce the time required to access the data from the sidechain, that can be measured and used for the efficiency of searching any registry document. This is the module that we intend to work on.

References

1. Invest India Business Immunity Platform, https://www.investindia.gov.in/. Accessed 14 Oct 2020
2. DILRMP: Digital India Land Records Modernization Programme (2008) Government of India. http://dilrmp.nic.in. Accessed 10 Aug 2020

3. Thakur V, Doja MN, Dwivedi YK, Ahmad T, Khadanga G (2020) Land records on blockchain for implementation of land titling in India. Int J Inf Manag 52:101940

4. Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Available: https://bitcoin.org/bitcoin.pdf. Accessed 20 Jul 2020

5. Barclays I Barclays says conducts first blockchain-based tradefinance deal. https://reut.rs/2AQEG9w. Accessed 15 July 2020

6. Insurchain: Insurchain: a decentralized insurance blockchain eco-system. https://github.com/InsurChain/whitepaper/blob/master/en/whitepaper-en.md. Accessed 10 July 2020

7. Niranjana murthy M, Nithya B, Jagannatha S (2019) Analysis of blockchain technology: pros, cons and swot. Cluster. Computing 22(6):14743–14757

8. King S, Nadal S (2012) Ppcoin: peer-to-peer crypto-currency with proof-of-stake. Self-published paper

9. Li D, Cai Z, Deng L, Yao X, Wang HH (2019a) Information security model of block chain based on intrusion sensing in the IOT environment. Clust Comput 22(1):451–468

10. Singh N, Vardhan M (2019a) Digital ledger technology-based real estate transaction mechanism and its block size assessment. International Journal of Blockchains and Cryptocurrencies 1(1):67–84

11. Singh YA, Singh KD Digitization of land record through blockchain-based consensus algorithm. IETE Technical Review. https://doi.org/10.1080/02564602.2021.1908859

12. Yadav AS, Agrawal S, Kushwaha DS (2021a) Distributed ledger technology-based land transaction system with trusted nodes consensus mechanism. Journal of King Saud University-Computer and Information Sciences

13. Singh N, Vardhan M (2020) Computing optimal block size for blockchain based applications with contradictory objectives. Procedia Comput Sci 171:1389–1398

14. Singh N, Vardhan M (2021) Multi-objective optimization of block size based on CPU power and network bandwidth for blockchain applications. Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems. Springer, Singapore, 2021

15. Cocco L, Pinna A, Marchesi M (2017) Banking on blockchain: costs savings thanks to the blockchain technology. Future Internet 9(3):25

16. Santander Santander launches the first real-time trades in Spain using we trade, a blockchain platform that helps companies go international. https://bit.ly/2Fw2pj7. Accessed 01 Oct 2020

17. Schwartz D, Youngs N, Britto A et al (2014) The ripple protocol consensus algorithm. Ripple Labs Inc White Paper 5

18. Singh K, Singh N, Kushwaha D (2018) An interoperable and secure E-wallet architecture based on digital ledger technology using blockchain. International conference on computing, power and communication technologies (GUCON) (978-1-5386- 4491-1/18)

19. Singh N, Vardhan M (2018) Blockchain based E-stamp procure-ment system with efficient consensus mechanism and fast parallel search. J Mech Contin Math Sci 13(4):73–89

20. Yadav AS, Shikha S, Gupta S, Kushwaha DS (2021b) The efficient consensus algorithm for land record management system. In IOP Conference Series: Materials Science and Engineering, vol 1022, no 1, pp 012090. IOP Publishing

21. Singh N, Vardhan M (2019c) Distributed ledger technology-based property transaction system with support for IoT devices. International Journal of Cloud Applications and Computing (IJCAC) 9(2):60–78

22. Singh N, Vardhan M (2019d) Blockchain based e-Cheque clearing framework. Scalable Computing: Practice and Experience 20(3):511–526

23. Singh N, Kumar T, Vardhan M (2020) Blockchain-based e-cheque clearing framework with trust-based consensus mechanism. Clust Comput:1–15

24. Yadav AS, Kushwaha DS (2021) Query optimization in a blockchain-based land registry management system. Journal homepage: http://iietaorg/journals/isi, 26(1): 13–21

25. Esposito C, Ficco M, Gupta BB (2021) Blockchain-based authen-tication and authorization for smart city applications. Inf Process Manag 58(2):102468

26. Ouaguid A, Abghour N, Ouzzif M (2018) A novel security frame-work for managing android permissions using blockchain technol-ogy. International Journal of Cloud Applications and Computing (IJCAC) 8(1):55–79

27. Li D, Deng L, Gupta BB, Wang H, Choi C (2019b) A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. Inf Sci 479:432–447

28. Tewari A, Gupta BB (2017) Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. J Supercomput 73(3):1085–1102

29. Shi N, Liang T, Li W, Qi X, Keping Y (2020) A blockchain-empowered AAA scheme in the large-scale HetNet. Digit Commun Netw

30. Tan, Liang, Huan Xiao, Keping Yu, Moayad Aloqaily, and Yaser Jararweh. "A blockchain-empowered crowdsourcing system for 5G-enabled smart cities." Comput Stand Interfaces 76 (2021): 103517

31. Feng C, Yu K, Bashir AK, Al-Otaibi YD, Lu Y, Chen S, Zhang D (2021) Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach. IEEE Network 35(1):130–137

32. Zhang J, Yu K, Zheng W, Qi X, Paul AK (2021) 3D reconstruction for motion blurred images using deep learning-based intelligent systems. CMC-Computers Materials & Continua 66(2):2087–2104

33. Yang F, Zhou W, Wu QQ, Long R, Xiong NN, Zhou M (2019) Delegated proof of stake with downgrade: a secure and efficient blockchain consensus algorithm with downgrade mechanism. IEEE Access 7:118541–118555

34. Stock Holding Corporation of India Limited, https://www.shcilestamp.com. Accessed 23 Aug 2020

Amrendra Singh Yadav obtain-ed his obtained B.Tech degree in Information Technology from Uttar Pradesh Technical University Lucknow, India in 2012 and M.Tech degree in Computer Science and Engineering from Madan Mohan Malaviyan University of Technology, Gorakhpur (U.P), India in 2014. Now he is currently a PhD student in the Department of CSE, Motilal Nehru National Institute of Technology Allahabad, India. His research in-terest includes Blockchain Technology and network optimization. He has published more than 15 research articles in various SCI and Scopus indexed journals and conferences.

3558

Peer-to-Peer Netw. Appl. (2021) 14:3540–3558

Dharmender Singh Kushwaha received the B.E in computer engineering from University of Pune, India in 1990. He received the M.Tech and PhD in computer science and engineering from Motilal Nehru National Institute of Technology Allahabad, Allahabad, India in 2007. He was recipient of Gold medal for his masters. Since 2018 he is working as Professor with Department of Computer Science and Engineering, Motilal Nehru National Institute of Technology Allahabad, India. His research interest includes: Distributed systems, service-oriented architecture, software engineering, data structure, image Processing and Blockchain Technology. Contribution in the current study, he stressed on the need for research that helps national security, outline of the proposed system along with its applicability, and mentor and supervision of the proposed work.