International Journal of Intelligent Transportation Systems Research (2024) 22:503–517
https://doi.org/10.1007/s13177-024-00414-3

BlockToll: A Hierarchical Blockchain Based Secure Toll Collection System for Intelligent Transportation System

Sukanta Chakraborty[1] · Abhishek Majumder[1]

Received: 12 March 2024 / Revised: 11 July 2024 / Accepted: 24 July 2024 / Published online: 5 August 2024

Abstract

With the increase in urban population more and more vehicles are coming to road. Along with the recent advancement of technology, the transportation system is also getting modernized like other systems. Intelligent Transportation System (ITS) is the modern way of transportation, and toll collection is an integral part of it. Toll collection devices and roadside units are installed in open public areas along the roadside. Therefore, these devices are easily accessible by intruders and are prone to different kinds of attacks. The literature study shows that the current road toll collection systems suffer from various security risks and lack in network features like distributed nature, transparency, and more; hence, the system needs to be updated. Also, a few existing blockchain-based toll collection systems do not keep vehicle trip information private. A secure, back-traceable, and trustworthy uniform mechanism should be adopted to overcome those problems. Blockchain can be one of the solutions for doing so. In this paper, a multilevel blockchain-based toll collection system has been proposed. To keep driver and vehicle information private, the Conditionally Anonymous Ring Signature scheme has been used. For faster performance and to ensure the security of devices at toll plazas, Proof-of-Authority consensus has been implemented. Elliptic Curve digital signature is used to ensure data integrity and faster processing in resource-constrained devices. The main aim of this research is to enhance the security and enable traceability in the existing toll collection system by developing a hierarchical blockchain based system. Simulation results obtained in terms of transaction latency, throughput and gas cost shows that the proposed system is capable to handle toll collection. Experimental result shows the feasibility of implementation in the real world.

Keywords Blockchain · Conditionally anonymous ring signature · Electronic toll collection system · Intelligent transportation systems · Proof of authority

Abbreviations

Abbreviation	Description
ITS	Intelligent Transportation Systems
$CARS$	Conditionally Anonymous Ring Signature
TP	Toll Plaza
STA	State/Regional Transport Authority
NTA	National/Global Transport Authority
$CARS$	Conditionally Anonymous Ring Signature

1 Introduction

The invention of blockchain technology for Bitcoin has decentralized the payment system [1]. The decentralized and distributed computing architecture of blockchain opens the way to redefine finance, economics, and other societal systems [2]. The use of smart contracts in blockchain builds trust among the users of blockchain technology [3]. Blockchain has the advantages of security, scalability, decentralization, trust-building, collective maintenance, and programmability [4]. Nowadays, blockchain technology is used in applications starting from home to healthcare, manufacturing industries, and space. The distributed feature, short transaction settlement time, trust between devices and users, and eliminating intermediaries make blockchain technology very suitable for IoT applications [5]. Kataoka et al. [6] focused on the distribution of trust among IoT devices and service providers. Integration of Software-defined networks (SDN)

✉ Abhishek Majumder
abhi2012@gmail.com

Sukanta Chakraborty
visitsukanta@gmail.com

[1] Department of Computer Science & Engineering, Tripura University, Suryamaninagar, Agartala, Tripura 799022, India

and blockchain has been done to automate the process of IoT services. Using this integration, trust-based device verification is also obtained to prevent attacks. A private (permission) blockchain is used for circulating the service profile and device profile information of TrustList. Encrypting this list before the execution of a transaction is a way to work it on a public blockchain. Novo O. [7] proposed a blockchain architecture for access management in IoT devices where a management hub controls access to blockchain resources. The result of his work shows that blockchain technology can be used for access management in IoT devices. The privacy of vehicle users is an important concern in Intelligent Transportation Systems (ITS). A user may not want his or her road trip to be known by others. Toll collection is one of the most important parts of ITS. Toll generates revenue for the government, which is used to maintain the roads and also a source of income. Previously, toll collection was manual. Later, RFID has been used for the automation of toll collection by several countries. The increased number of vehicles on the road and the openness of toll collection devices make secure toll collection challenging. The open nature of toll devices makes them vulnerable to different kinds of attackers. The information shared between a vehicle and roadside units (RSU), RSUs, and Toll Plazas (TPs) can be altered by an intruder to bypass the toll fee and also may be used for the privacy breach of vehicle users. Private information like trip information of vehicle users needs to be private so that toll controllers or other unauthorized entities are not aware of that. Blockchain can be one of the potential solutions for the above. Review of existing schemes shows that there are research gaps in systems developed for toll collection. Some of them [8, 9] which are using proof of work (POW) introduce high latency and high gas cost. Some other schemes [6, 10] use permission less blockchain which compromises car owner's privacy. In those schemes, toll manager may know travel information of the vehicle user provided during toll payment. Also, some existing works [7, 8, 11] focus on reducing additional transaction fees and traffic distribution. So there is a need to develop such a solution which will provide scalability, low latency and preserve car owner's privacy.In summary, in existing systems, toll manager is aware of trip details of a vehicle which compromises vehicle owner's privacy. Also, existing systems lack the combination of an established blockchain with a high transaction rate while ensuring security of the system. For example, in existing RFID based system, RFID readers reads vehicle number plate and fetches detailed vehicle information and corresponding bank account details from database. So, the toll manager sitting in the toll booth can see personal details of each vehicle passing through the toll plaza and their travel information. The primary objective of this study is to address these security gaps especially ensuring privacy of vehicle user and enhance traceability within the current toll collection system. An effort has also been made for making electronic toll collection systems more reliable. In this paper, a multilevel blockchain-based secure toll collection system named BlockToll has been proposed. While maintaining vehicle user privacy and providing higher security to the toll collection system, by the use of a multilevel blockchain with a ring signature, BlockToll addresses the issues of scalability and information availability. Contributions in this paper are the following:

(1) Here, a privacy-preserving multilevel blockchain-based toll collection system named BlockToll has been proposed.
(2) Conditionally Anonymous Ring Signature (CARS) has been incorporated to keep vehicle trip information private.
(3) A detailed literature survey has been done on the existing toll collection system. Existing works on the security of ITS components have also been presented.
(4) The proposed BlockToll has been implemented and the result has been analyzed. Also, the security analysis of BlockToll has been done.

The organization of the paper is as follows: Section 2 discusses the related works on toll collection system, their security, and shortcomings. Section 3 presents the privacy preservation process in blockchain. The BlockToll framework has been discussed in Section 4. Security analysis has been done in Section 5. In Section 6, experimental setup has been given. Analysis of results have been made in Section 7. Lastly, Section 8 concludes the work and future directions have also been presented.

2 Related Work

For more understanding of existing and ongoing advancements in present toll collection system security, a detailed literature review has been done in this section. The literature review has been divided into two subsections, *Modern ITS system and blockchain in ITS* and *Toll collection using blockchain*.

2.1 Modern ITS System and Blockchain in ITS

There are a large number of sensor devices and controller agents deployed to run distributed and secure operations in ITS [12, 13]. The existing techniques for ITS-based traffic light management systems consider vehicles as honest [14]. Vujic et al. [15] proposed a cooperative traffic management framework for IoT devices in ITS. They focused on two main communication channels of ITS namely, vehicle-to-vehicle communication and vehicle-to-infrastructure communication. The communication between entities in ITS must be secure so that their privacy is ensured. Namane et al. [16] proposed an authentication scheme based on blockchain. It uses fog computing for traffic lights to work in collaboration within a city. Baskar et al. [17] proposed a decentralized system to manage the Internet of Vehicles (IoV) and to control traffic. The decentralized model was developed for small-scale systems by introducing different levels of control. The motivation of the system was that a large-scale system can be divided into efficient smaller and interconnected hierarchical systems. To remove the central authority and to provide scalability, transparency, and decentralization, a blockchain-based solution is proposed by Amiri et al. [18]. But, since a public blockchain is applied, user and control authority data is publicly visible to all the other users. To overcome these kinds of security issues, a secure crowd-sensing-based smart parking system was proposed by Kim and Kim [19]. The system used both public and private blockchains. But in this technique, if the bridge node that connects the private blockchain with the public blockchain gets compromised, the whole system gets exposed to network threats. This node can also cause a single point of failure in the whole system. Therefore, it is necessary to develop a system that will not have a single point of failure and will ensure the security of user and controller data. Nema et al. [20] proposed RSA based encryption and decryption method to secure the communication between RSUs and vehicles on the road. Levels of trust were assigned to nodes to detect and remove malicious nodes. Wen [21] presented an expert system to trace malicious or illegal activities using the information collected by RFID technology. To ensure the security of ITS Yuan and Wang [22] proposed a novel blockchain-based ITS (B2ITS) framework. Li et al. [23] proposed an advertisement dissemination scheme where a vehicle's privacy is achieved using a zero-knowledge proof technique. The zero-knowledge proof technique [24] allows the prover to generate cryptographic proof for the verifier without revealing any private information. The rise of deep learning and neural network significantly improved modern ITS by facilitating traffic management, increasing road safety and performance while reducing maintenance costs. Haghighat et al. in [25] provided a broad view of how deep learning models can be used in ITS. Jiang and Luo [26] reviewed graph based approaches to forecast traffic for a period. Based on the survey, the authors have listed the challenges and provided future research direction for traffic forecasting. Shamsi et al. [27] proposed a deep reinforcement learning based traffic light control algorithm. The system learns policies to facilitate priority of emergency vehicles using real time traffic details. In a very recent survey, Shahrier et al. [28] studied different technologies and their applications in ITS. The authors also listed the future scope of these technologies in ITS and limitations of them. Integration of blockchain in IoT networks can help to construct a scalable ITS system [29]. Kharche et al. in [29] discussed the possible ways of blockchain implementations in transportation system in Indian context. They presented a case study of two most populated and congested cities Delhi and Mumbai in India as well as in the world. Also, they introduced an architecture to integrate IoT and blockchain in ITS. Inter domain communication between devices from different ITS domain arises trust and interoperability issues. To overcome this, Sun et al. [30] proposed a cross-chain communication architecture for ITS. Also, they introduced an inter chain communication for the system. They established their proposed system's feasibility by implementing the system and achieving a read transaction throughput of 2000 transaction per second.

2.2 Toll Collection Using Blockchain in ITS

Like in other application fields, blockchain is now also used in toll collection systems. Tanveer et al. [8] proposed an Ethereum blockchain-based automated road toll collection system. Smart contracts have been used to make toll payments. In the system, the driver has to create a personal account. The blockchain smart contract automatically debits the driver's account whenever the vehicle passes through a toll plaza. In this system, toll manager may see vehicle owner details and trip information which compromises the owner's privacy. Also, permission less blockchain makes the system more open to the blockchain participants. Another work by Soner et al. [31] proposed a blockchain and smart contract based approach for efficient toll collection. In the system, user need to pay for their travelling distance only. Also the system keeps tracks of each toll transaction. Naik et al. [32] introduced a web based toll collection system using blockchain to make toll collection process transparent and secure. The work also contributes to the communication network by simulating 5G network in the modern transportation system. For public sharing of heterogeneous edge devices, Xiao et al. [11] proposed a blockchain-based toll collection system. Before entering into the system, edge nodes need to register the address into the blockchain. The payment channel technique has been deployed to reduce payment transaction overhead. To facilitate the auditability of blockchain records by third party, the system has been made transparent which violates its users privacy. Electronic toll collection from each vehicle in real-time requires a significant amount of time for the vehicles. To overcome this, Ying et al. [9] proposed a blockchain based technique for toll collection from opportunistic vehicle platoons. A temporary platoon member as a leader pays for all vehicles in the platoon and later the account of each member vehicle will be debited through the smart contract. Once the trip ends, platoon members will pay their toll amount back to the platoon leader as recorded in the blockchain. In this scheme vehicle credentials and driving history of all registered vehicle is recorded into the blockchain. RSU is used to differentiate between a single vehicle and a vehicle platoon.

This scheme is limited to platoon of vehicles and inefficient for normal singular vehicles which is common scenario in roads. Didouh et al. provided a blockchain-based technique to prevent spoofing attacks on legitimate nodes in ITS [33]. This solution used received signal strength indication-based technique and Proof-of-Location to determine the legitimacy of an ITS node. Smart contract has been employed to ensure non-repudiation of messages using vehicle GPS location and timestamp. In this system, nearby RSUs and vehicle's on board units are aware of the location of vehicles. Das et al. [10] proposed a blockchain and smart contract based ITS management system where an automated toll collection system was the main objective. Patil et al. [34] and Thosar et al. [35] developed a boothless toll collection system using a private blockchain. To use the system, each vehicle must register using owner information, registration number, and digital identity. To make the system transparent, these works [10, 34, 35] didn't consider the vehicle's privacy. Hence, trip information of a vehicle is available to authorities in the blockchain. Toll collection Techniques mentioned above did not consider the driver's travel information privacy. The travel information of the driver is shared with toll plazas which violates his/her privacy. Moreover, all the ITS devices participate in a single blockchain which will make the blockchain size large. So, a copy of the blockchain cannot be stored in resource-constrained ITS devices. Since the existing schemes consider vehicles as honest nodes, a malicious vehicle can attack these wireless ITS devices to get higher priority to pass through the intersections. In this work, a multilevel blockchain-based secure toll collection system named BlockToll has been proposed. While maintaining driver's privacy and providing higher security to the toll collection system, by the use of a multilevel blockchain, BlockToll addresses the issues of scalability and information availability.

3 Privacy in Blockchain

In this section, the privacy preservation techniques in blockchain have been discussed. Different techniques have been developed to preserve privacy in the blockchain. The two most prevalent techniques are *Zero Knowledge Proof* and *Ring Signature*.

3.1 Zero Knowledge Proof

Zero Knowledge Proof [24] enables a user to communicate information without revealing the information to others. This technology is suitable for user authentication. There must be a prover and one or more verifiers. The prover needs to convince the verifier without disclosing any meaningful information to the verifier.

3.2 Ring Signature

In a ring signature, other users and verifiers know the communicated information but the signer's identity is hidden in a list of public keys. The Ring signature was originally proposed by Shamir et al [36] for hiding the identity of the signer from others in the ring. In this scheme, the signer's identity is preserved in a group of public keys. The ring signature process can be divided into 3 parts, *keyGeneration(), sign() and verify()*.

keyGeneration(): The signer obtains a list of public keys $(K = pk_1, pk_2, ..., pk_n\})$ of selected ring members from the Certification Authority (CA).

sign(): Signer uses list K, his private key(sk), and the message (M) to be signed and generates ring signature ψ.

verify(): Verifier uses ψ, K, M and returns 'True' if the signature is valid else, returns 'False'.

To keep the signer's identity private while also keeping the scope to verify the signer only by certain authorities, Zhang et al. [37] proposed a technique called Conditionally Anonymous Ring Signature. It is the modified version of the ring signature where the signer's identity is hidden from verifiers except for the authoritative node. The authoritative node can trace the identity of the signer when there is an invalid or illegal transaction verified.

4 Proposed Technique

In this section, the proposed BlockToll system architecture has been discussed. The operations performed in the BlockToll system have also been presented. The working of the system has been explained. The different symbols used and their description is presented in Table 1.

4.1 System Architecture

In this subsection, the proposed blockchain-based toll collection system and its components have been discussed. The architecture of BlockToll has been shown in Fig. 1. The secure distributed property of blockchain is utilized in this proposed scheme to overcome the security deficiencies in the current toll collection systems. To maintain the privacy of the vehicle and driver, the CARS scheme has been used. With the use of multilevel blockchain, monitoring of the toll collection system becomes easier for road transport authorities and different malicious activities are fully traceable.

4.1.1 Entities in BlockToll

The proposed architecture consists of five entities namely, Certificate Authority (CA), vehicle, Toll Plaza (TP), State Transport Authority (STA), and National Transport Author-

Table 1 Symbols in the architecture

Symbol	Description
pk_{tp}	Public key of Toll Plaza
sk_{tp}	Private key of Toll Plaza
pk_{auth}	Authoritative node
v_{id}	Vehicle registration number
$\$_{rs}$	Toll charge amount
tp_i	i^{th} Toll Plaza
K	List of public keys
C_{0x}	Smart contract address
k	Security parameter in N, set of natural numbers
p, q	Large prime numbers
g	Generator of prime filed p
Z_p^*, Z_q^*	Prime fields over p, q
x, z, y, w, α	Random numbers
t	Time
TX	Blockchain transaction
$H()$ & h	Hash function & hash value
$H_p(), H_q()$	Collision resistant hash function
a, b, c	Key factors
ψ	Signature

ity (NTA). The architecture of the proposed system is shown in Fig. 1. The functions of different entities of the proposed system are discussed below.

(i) *Certificate Authority (CA):* Private and public keys of the devices in the system is provided by the CA. Before entering into the blockchain, devices in the system need to register into the CA. The CA is assumed to be fully trusted. CA can be the Ministry of Transportation. It is to be noted that the presence of CA is not in conflict with the distributed nature of the system because the CA is required for the system initialization only.

(ii) *Vehicle:* The vehicle is the first and most important entity for which the system is needed. Vehicles going through a toll road communicate with the toll plaza via RSU and fetches the toll fees. The vehicle will have to pay the toll fee.

(iii) *Toll Plaza (TP):* Every toll collection system has a toll controller that calculates toll fees for a vehicle based on its trip information. To do that, TP senses the v_{id} using sensors installed at TP. TP makes a transaction to the blockchain with the vehicle registration number (v_{id}), toll charge amount($\$_{rs}$), and current time ($t$).

(iv) *State Transport Authority (STA):* Each STA is associated with a large number of TPs from different roads within a state or region. There are a large number of STAs in the system. STA is the higher authority in the TP-STA blockchain and has the ability to add or remove a TP in the blockchain. STA gets $\$_{rs}$ for each v_{id} passing by from the TP-STA blockchain. STA uploads the information about the collected toll amount and the vehicle numbers to the STA-NTA blockchain.

(v) *National Transport Authority (NTA):* NTA is the supreme authority in the whole system. All the STA works under the supervision of NTA. The NTA and all STAs make a shared blockchain. NTA can add or remove an STA in the shared STA-NTA blockchain. NTA can easily monitor toll collection throughout the nation.

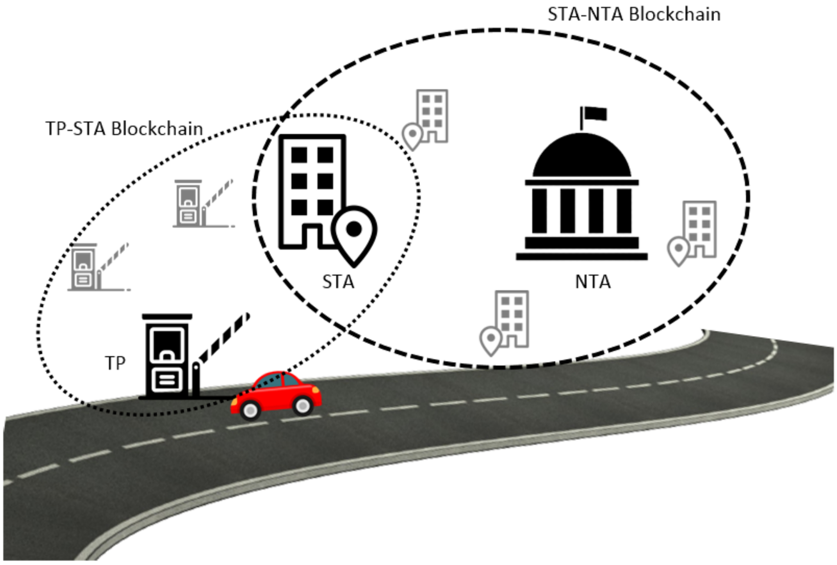


Fig. 1 Proposed BlockToll architecture

4.1.2 Blockchains used in BlockToll

In the proposed scheme, two blockchains are used. Working of these blockchains are,

(i) *TP-STA shared blockchain:* All the TPs within a state or region and the associated STA participate in this shared blockchain. Each TP makes a transaction of v_{id} and $\$_{rs}$ with the current time (t) signed using CARS (Algorithm 1) and encrypted by the public key of STA into the blockchain. STA gets the collected toll information within its service region from this blockchain and verifies each toll transaction using Algorithm 2.

(ii) *STA-NTA shared blockchain:* The NTA and all the STAs nationwide participate in this blockchain. STA makes transactions of the toll information $(\$_{rs}, v_{id}, t)$ received from the TP-STA blockchain for each vehicle into this blockchain encrypted by the public key of NTA and signed by STA using Algorithm 1. NTA verifies (using Algorithm 2) and monitors every transaction made by STAs in this blockchain.

4.2 Operations in BlockToll

The proposed technique consists of four steps: i) System initialization iii) Key generation and user registration iii) TP-STA shared blockchain updation iv) STA-NTA blockchain updation. The overall system working has been shown using flow diagram Fig. 2. Also a flowchart of the system has been provided in Fig. 3. The operations performed in each step are discussed below.

(i) *System initialization:* The CA randomly chooses security parameter k to initialize BlockToll. Let, p and q be two large prime numbers (where, $q > 2^k$) and Z_p^* and Z_q^* are cyclic groups whose elements are $\{1, ..., p-1\}$ and $\{1, ..., q-1\}$. CA chooses generators g and h in Z_p^* with order q. H_p and H_q are two collision resistant hash functions in Z_p and Z_q.

(ii) *Key generation and user registration:* To be a part of the system, each user must obtain a digital certificate from the CA. CA randomly chooses $sk_i \in Z_q^*$ as user i's private key and generates the corresponding public key $pk_i = g^{sk_i} \ mod \ p$. Then CA will issue a digital certificate to the user containing sk_i and pk_i.

(iii) *TP-STA blockchain updation:* Sensors installed at TPs continuously check for vehicles passing through a toll road and if a vehicle is found it immediately informs the associated toll controller with the vehicle identity (v_{id}). After obtaining the v_{id}, TP calculates $\$_{rs}$ and updates the toll charge info for the v_{id}. TP performs a transaction using v_{id} and $\$_{rs}$ with the current time (t) into the shared TP-STA blockchain. The transaction is signed using Algorithm 1. STA checks whether the retrieved transaction block is valid or not by executing the Algorithm 2. Proof-of-Authority (PoA) consensus has been used to create blocks into the blockchain. The consensus is high risk tolerant and provides high transaction processing rate. Furthermore, the PoA con-

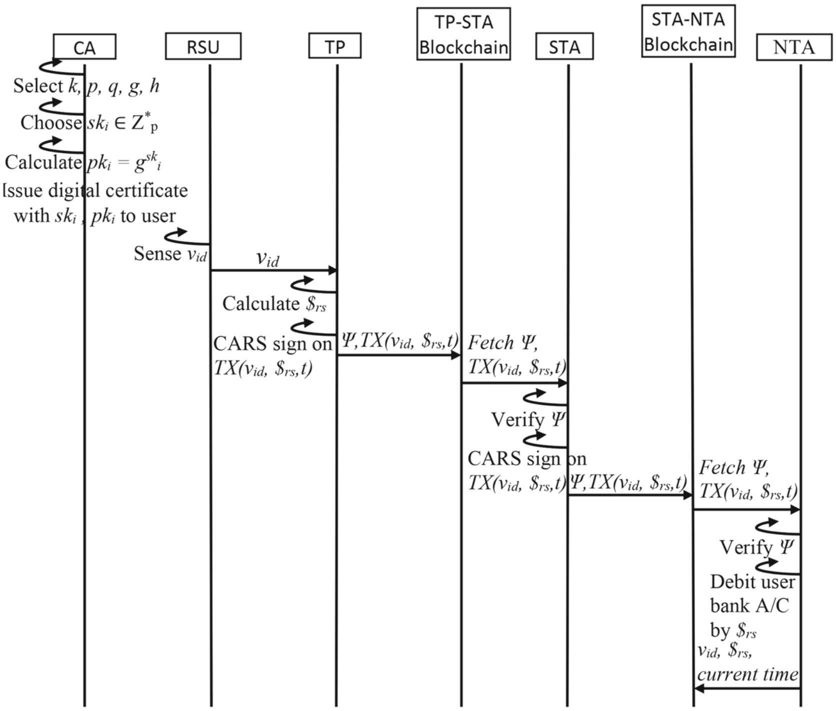

CA
RSU
TP
TP-STA Blockchain
STA
STA-NTA Blockchain
NTA
Select k, p, q, g, h
Choose $sk_i \in Z^*_p$
Calculate $pk_i = g^{sk_i}$
Issue digital certificate with sk_i , pk_i to user
Sense v_{id}
v_{id}
Calculate $\$_{rs}$
CARS sign on $TX(v_{id}, \$_{rs}, t)$
$\Psi, TX(v_{id}, \$_{rs}, t)$
Fetch Ψ, $TX(v_{id}, \$_{rs}, t)$
Verify Ψ
CARS sign on $TX(v_{id}, \$_{rs}, t)$
$\Psi, TX(v_{id}, \$_{rs}, t)$
Fetch Ψ, $TX(v_{id}, \$_{rs}, t)$
Verify Ψ
Debit user bank A/C by $\$_{rs}$
v_{id}, $\$_{rs}$, current time

Fig. 2 Workflow of BlockToll system

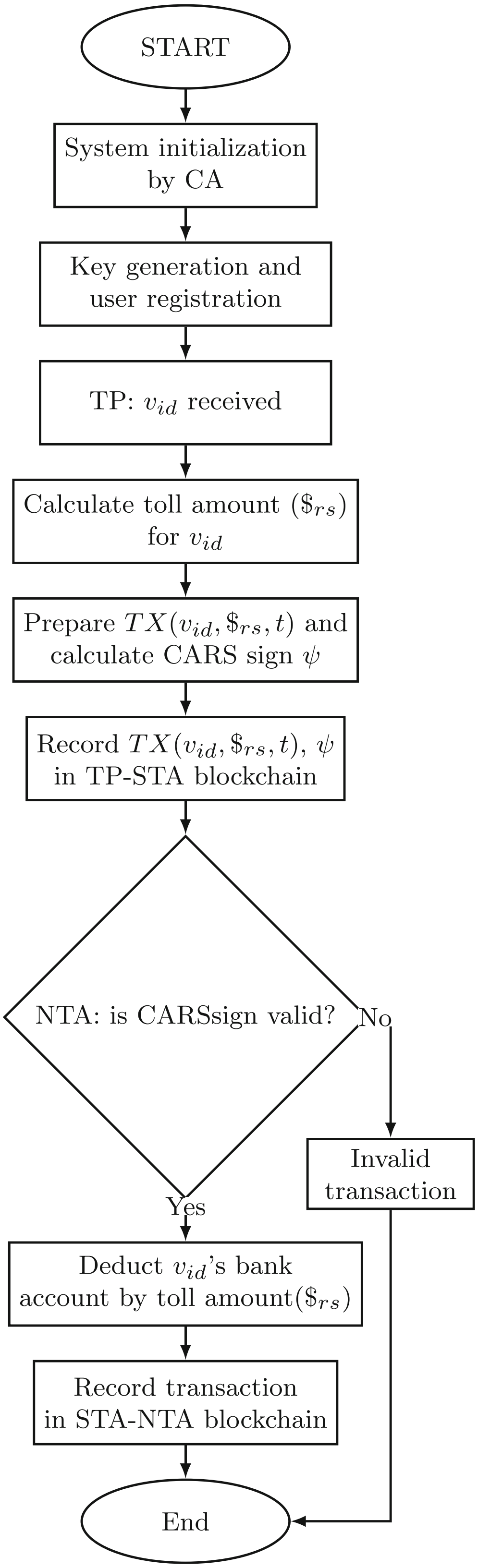

START
System initialization by CA
Key generation and user registration
TP: v_{id} received
Calculate toll amount ($\$_{rs}$) for v_{id}
Prepare $TX(v_{id}, \$_{rs}, t)$ and calculate CARS sign ψ
Record $TX(v_{id}, \$_{rs}, t)$, ψ in TP-STA blockchain
NTA: is CARSsign valid?
No
Yes
Invalid transaction
Deduct v_{id}'s bank account by toll amount($\$_{rs}$)
Record transaction in STA-NTA blockchain
End

Fig. 3 Flowchart of BlockToll system

sensus is computationally inexpensive compared to PoW. Only designated signers can produce new blocks into the network. Signers are selected by a Round-Robin order. No signer is allowed to produce more than a certain number of consecutive blocks. This limit is calculated as $CONSECUTIVE\_BLOCK\_LIMIT = (NUMBER\_OF\_TOTAL\_SIGNERS/2)+1$. Blocks in STA-NTA blockchain are created in same fashion using POA.

(iv) *STA-NTA blockchain updation and toll charge collection:* STA signs each verified toll trip details using CARS. Then it makes a transaction of each trip into TP-STA blockchain. Upon verification of Algorithm 2 these transactions by NTA, it charges the toll amount for v_{id} from the linked bank account and the transaction is recorded into the STA-NTA blockchain.

4.3 Signing a Transaction Using CARS

TP can obtain a public key list from the CA as $K = \{pk_{tp_1}, pk_{tp_2}, ..., pk_{tp_{n-1}}\}$. TP prepares a transaction using the list K, smart contract address C_{0x} and a set of transaction information ($\$_{rs}, v_{id}, t$). The process of signing a transaction, TX by TP is discussed below Algorithm 1.

Algorithm 1 Algorithm for signing TX using CARS.

```
Input: Vehicle registration no($v_{id}$), toll charge($\$_{rs}$), time($t$). Output: A CARS, $\psi$ on $TX$

$a = h^x \ mod \ p$
$b = a^y \ mod \ p$
$c = a^w \ mod \ p$
$\phi = w + yH(TX(v_{id}, \$_{rs}, t)||a, c) \ mod \ p$
$tx = H_p(TX(v_{id}, \$_{rs}, t)||a||b)$
$R = g^\alpha \prod_{i=1,i\neq k}^{n-1} pk_{tp_i}^{\beta_i} \ mod \ p$
for $0 \leq i \leq n\text{-}1$ do
    if $i \neq k$ then
        $\beta_i \leftarrow Z_q$
        $R = R \times pk_{tp_i}^{\beta_i}$
    $i \leftarrow i + 1$
$\beta = H_q(K, tx, R)$
for $0 \leq i \leq n\text{-}1$ do
    if $i \neq k$ then
        $\beta_k = \beta_k - \beta_i$
    $i \leftarrow i + 1$
$\gamma = (\alpha - \beta_k \cdot sk_{tp_k}) \ mod \ q$
$\psi = (\gamma, \beta_0, \beta_1, ..., \beta_{n-1}, a, b, c, \phi)$
return $\psi$
```

Step 1: For a transaction TX to be signed, TP chooses random numbers x, y, and w from Z_q^* to calculate the following as in Eqs. 1, 2 and 3:

$$a = h^x \ mod \ p \tag{1}$$

$$b = a^{y} \ mod \ p \tag{2}$$

$$c = a^{w} \ mod \ p \tag{3}$$

TX is included in the input of hash function H (4) so that attackers cannot sign other transaction TX' using a and b.

$$\phi = w + yH(TX(v_{id}, \$_{rs}, t)||a, c) \ mod \ p \tag{4}$$

Step 2: TP computes message digest (tx) of transaction TX using Eq. 5.

$$tx = H_p(TX(v_{id}, \$_{rs}, t)||a||b) \tag{5}$$

Step 3: Again TP randomly chooses $\alpha, \beta_i \in Z_q(i = 0, 1, ..., n-1; i \neq k)$ to calculate R using Eq. 6 as follows,

$$R = g^{\alpha} \prod_{i=1, i \neq k}^{n-1} pk_{tp_i}^{\beta_i} \ mod \ p \tag{6}$$

$$\beta = H_q(K, tx, R) \tag{7}$$

Step 4: Then, TP produces signature ψ using equation using Eqs. 7, 8, 9 and 10.

$$\beta_k = \beta - \sum_{i=0, i \neq k}^{n-1} \beta_i \ mod \ q \tag{8}$$

$$\gamma = \alpha - \beta_k \cdot sk_{tp_k} \ mod \ q \tag{9}$$

$$\psi = (\gamma, \beta_1, ..., \beta_{n-1}, a, b, c, \phi) \tag{10}$$

4.4 Transaction Verification

$$\sum_{n-1}^{i=0} \beta_i = H_q(K, H_p(TX(v_{id}, \$_{rs}, t)||a||b), g^{\gamma} \prod_{n-1}^{i=0} pk_{tp_i}^{\beta_i}) \ mod \ q \tag{11}$$

After receiving a signed transaction on the blockchain, STA can easily verify signature ψ on TX. To ensure the correctness of key factors, STA first checks whether the condition $a^{\phi} \ mod \ p = cb^{H(TX(v_{id}, \$_{rs}, t)||a, c)} \ mod \ p$ is satisfied or not. On valid key factors, STA verifies the signature using Eq. 11. Algorithm 2 presents the verification process of transactions.

For each valid signature, STA records the transaction into the blockchain otherwise discards the transaction. Similarly, in the STA-NTA blockchain, STA makes transactions signed using CARS, and NTA records valid transactions or discards invalid ones.

Algorithm 2 Algorithm to verify CARS signature.

```
Input: A CARS, $\psi$ on $TX(v_{id}, \$_{rs}, t)$ Return: 0: invalid, 1: valid

$d_1 \Leftarrow a^{\phi} \ mod \ p$
$d_2 \Leftarrow cb^{H(TX(v_{id}, \$_{rs}, t)||a, c)} \ mod \ p$
if $d_1 \neq d_2$ then
    return 0
$tx = H_p(TX(v_{id}, \$_{rs}, t)||a||b)$
$\beta' = \sum_{i=0}^{n-1} \beta_i \ mod \ q$
for $0 \leq i \leq$ n-1 do
    $\beta' = \beta' + \beta_i$
    $i \leftarrow i + 1$
$R \leftarrow 1$
for $0 \leq i \leq$ n-1 do
    $R = R \times pk_{tp_i}^{\beta_i}$
    $i \leftarrow i + 1$
$h' = H_q(K, tx, g^{\gamma} R) \ mod \ q$
if $h' \neq \beta'$ then
    return 0
return 1
```

4.5 Tracing Malicious Signer

If a node has been found with illegal data or misbehavior in transaction ($TX_{illegal}$), the authoritative node (STA in TP-STA blockchain and NTA in STA-NTA blockchain) will execute confirmation protocol to know the source of the transaction. TP_i selects a random $r_1 \in Z_q^*$ and calculates $\tau = a^{r_1} \ mod \ p$.

TP_i chooses another random $\alpha \in Z_q^*$ and calculates $\delta = g^{\tau} pk_{auth}^{\alpha} \ mod \ p$. TP_i sends τ and δ to the authoritative node.

The authoritative node selects $\varepsilon \in Z_q^*$ and sends it to TP_i. Upon receiving ε, TP_i calculates $\kappa = \alpha + y\varepsilon \ mod \ q$ and sends it to the authoritative node.

Authoritative node calculates,

$$\delta = g^{\tau}(pk_{auth})^{\alpha} \ mod \ p \tag{12}$$

and

$$a^{\kappa} = \tau b^{\varepsilon} \ mod \ p \tag{13}$$

Now, if Eqs. 12 and 13 holds, the authoritative node confirms that TP_k has made the transaction $TX_{illegal}$. Similarly, NTA traces illegal transactions in the STA-NTA blockchain.

5 Security Analysis

This section analyzes the security of the proposed BlockToll from different aspects.

5.1 Device Authentication

In BlockToll every device in the system has a private and public key which is obtained from the CA at the time of system setup. So, devices in the system can verify whether the information is coming from authenticated sources or not by validating the signature of the received information using the sender's public key. Also an intruder not having the private keys of legitimate devices cannot steal their identity.

5.2 Data Integrity

Integrity ensures that the information sent is not tampered with in the path from sender to destination. In BlockToll along with the encrypted data, the TP sends its hash too. Hence if the information sent by a TP is modified by an intruder, the hash received will not match with the hash obtained from the decrypted data at receiver's end. So, the integrity of information is maintained in communication between toll devices.

5.3 Confidentiality

In BlockToll since an intruder doesn't know the private keys of devices, an intruder will not be able to retrieve information from encrypted data. By the use of CARS in a private blockchain, the confidentiality of information is maintained. Except for the government authorities vehicle trip information is not known to others.

5.4 Information Availability

In BlockToll, information about all the toll transactions is securely stored in the blockchains. Information is also stored on the higher-layer blockchains. So, if one or few devices in the system is goes down, information is still available in the other devices as well as blockchains. Hence the remaining system can function normally.

5.5 Man-in-Middle Attack

A malicious user may try to modify the data sent by a vehicle. In BlockToll, if the data is changed, the hash of the data received at the receiver's end will not match with the hash sent. Also, malicious users cannot obtain the signature of a vehicle and other blockchain devices because the private key of any device is known to that device only.

5.6 Sybil Attack

An intruder can steal the identity information of a legitimate vehicle and pass through toll plaza which will debit the bank account of the legitimate user in the system [8]. In BlockToll an attempt to use the identity of a vehicle by a malicious user is difficult since the private key of the vehicle is not available publicly.

5.7 Reply Attack

In BlockToll, there is a timestamp with every transaction. If a malicious user wants to carry out a reply attack it has less impact since the toll-collection process on past information is already over. A reply of the same transaction has no meaning in the finished toll process. Any attempt for the reply attack will be unsuccessful.

5.8 Non-repudiation

In BlockToll all transactions in the system are considered valid only after signature verification. Added transactions in a blockchain cannot be modified. The recorders discard records with invalid signatures. STA and NTA has the authority to ensure a valid CARS signer. Since the private key of any device is known to that device only, a record cannot be denied by its signer and hence BlockToll ensures non-repudiation.

5.9 Eclipse Attack

In [8, 9, 33], a malicious vehicle may isolate the toll plaza by which it is passing through to avoid paying toll charge. This may impact the whole system. In BlockToll, isolating an individual node from other nodes doesn't have much impact on the remaining system. The attacker may feed incorrect data to the isolated node. The authoritative node can trace the malicious signer and penalize or ban the node from making transactions in the system. Because of the hierarchical blockchain, the remaining system is secured from the eclipse attack.

5.10 51% Attack

Since other blockchain-based schemes use a single blockchain for the whole system, they are susceptible to 51% attack. In BlockToll multilevel blockchains are used. So, if one blockchain gets compromised, the information is still available in the higher levels of the blockchain.

5.11 Distributed Denial of Service (DDoS)

Models proposed by Xiao et al. [11] and Ying et al. [9] use a single blockchain. If a DDoS attack is conducted the entire system will be affected. Web based toll collection system such as [32] are vulnerable to DDoS attack. In this kind of system, rather than flooding the network with pings or requests, malicious actors can saturate it by initiating spam transactions, which creates network congestion and reduces

Table 2 Security Comparison of BlockToll and baselines (DA: Device Authentication, DI: Data Integrity, CF: Confidentiality, MM: Man-in-middle, NR: Non-repudiation, DP: Driver's Privacy, DDoS: Distributed Denial of Service)

Scheme	DA	DI	CF	MM	Sybil	Reply	NR	Eclipse	51%	DP	DDoS
Tanveer et al. [8]	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗
Xiao et al. [11]	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
Ying et al. [9]	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗
Didouh et al. [33]	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
Das et al. [10]	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗
BlockToll	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

the throughput of legitimate transactions. On the other hand, in BlockToll hierarchical blockchains are used. Therefore, if a DDoS attack is conducted, the attack will be localized to one blockchain only and it will not affect the entire system.

5.12 Privacy in BlockToll

No vehicle user wants their travel information or ownership details to be known by others. To make the toll collection system transparent, works in [8, 9, 11] compromise vehicle owners privacy as well as users trip information. Also, in [31, 32], travel information of vehicle users are recorded in the blockchain for accountability and transparency which compromises vehicle users travel information. Use of CARS in the proposed BlockToll system ensures that trip information of a vehicle is private and not known by others.

A summarized comparison of BlockToll and baselines has been provided in Table 2. From the security analysis, it has been found that BlockToll provides better security compared to baselines.

Security, scalability, information availability, and decentralization are the most important features of a network-based system. In the case of IoT networks, the developed system also needs to be suitable for resource-constrained devices. Existing toll collection schemes do not provide one or more of the above mentioned features. Table 3 shows that BlockToll has all the above-mentioned features.

Scalability of those schemes are limited which use single blockchain. Because if the number of ITS devices are huge, performance of the blockchain will degrade. Proposed scheme is highly scalable because of multiple blockchain. Since, multiple blockchain is used in proposed scheme, if few nodes or one blockchain is down the the information is still available in other blockchain which is not the case for existing schemes. Unlike few existing schemes where parts of the communication between devices is open, in BlockToll, all the communications are made in encrypted form and thus it is more secure. Using a single blockchain will make the chain data size large and hence constrained devices would not be able to store that chain data. Use of multiple small blockchain will keep chain data smaller in BlockToll, which makes BlockToll very suitable for constrained devices.

6 Experimental Setup

This section provides the view of experimental setup for the proposed BlockToll system simulation.

The BlockToll architecture has been simulated and tested on an Intel Xeon E5-1607 3.0GHz workstation running Ubuntu 20.04.2 LTS. The proposed architecture has been developed on top of the Geth private Ethereum blockchain version 1.10.7 stable with the help of truffle blockchain development framework v5.1.60 and Solidity version 0.5.16. Web.js is used to interact with blockchain from the front end. Table 4 summarizes the experimental hardware and software configuration used in the simulation of the proposed system. In the simulation, each entity device runs a Geth private Ethereum blockchain node.

A smart contract containing separate functions for CARS signature, CARS verification, blockchain query, and transfer of assets has been implemented. The example smart con-

Table 3 Comparison of available blockchain-based toll collection schemes with BlockToll

Scheme	Scalability	Info. availability	De/Centralized	Security	For constrained devices
Tanveer et al. [8]	Limited	No	Decentralized	Low	Suitable
Xiao et al. [11]	Limited	No	Decentralized	Low	Suitable
Ying et al. [9]	Limited	No	Decentralized	Yes	Not suitable
Didouh et al. [33]	Limited	Yes	Decentralized	Yes	Suitable
Das et al. [10]	Limited	Yes	Decentralized	Yes	Not suitable
BlockToll	Highly scalable	High	Decentralized	High	Very suitable

Table 4 Experimental configuration information

HW/SW	Description
Machine	Dell precision T3610 workstation
Processor	Intel Xeon CPU E5-1607 3.0 GHZ x4
Memory	28 Gigabyte
HDD	500 Gigabyte
Graphics	NVIDIA GK107GI (Quadro K600)
OS	Ubuntu 20.04.2 LTS x64
Geth version	1.10.7 stable
Node version	10.19.0
Node Package Manager (Npm) version	6.14.4

tract of the caliper benchmark has been replaced by the proposed smart contract and results for the function have been generated in terms of Latency, throughput, and time cost using the caliper benchmark. The maximum number of blockchain nodes simulated in this experiment is 100, which is almost equal to the maximum number of TPs within a state (Rajasthan) in India [38].

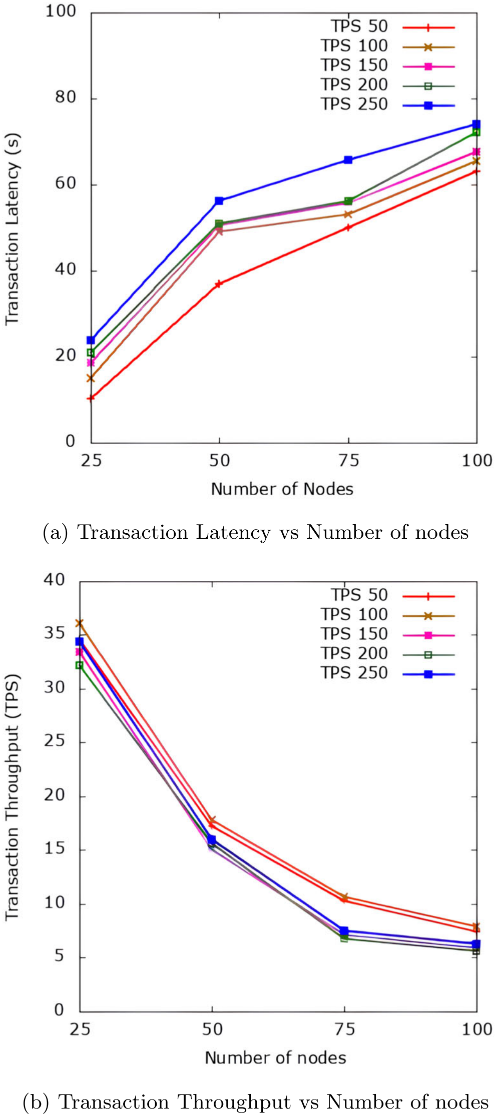
7 Results and Discussion

Results obtained from the simulation based on different parameters has been discussed in this section. Performance analysis has been done to understand the feasibility of the BlockToll system. In simulation of the BlockToll system, five different transaction send rates has been considered in Figs. 4, 5 and 6. Five different lines in Figs. 4 and 5 represent the transaction submission rate of 50, 100, 150, 200 and 250 Transaction per Second (TPS). In Fig. 6 these lines represent for 5, 10, 15, 20 and 25 TPS. In the figures, each value represents the average obtained by running the system ten times.

Transaction latency is the time required to make a transaction and submit the transaction into a block. Figure 4a shows the effect of number of nodes on transaction latency of BlockToll. The figure shows that as the number of nodes increases, the average latency increases. Still, the latency is suitable for deployment in real-world toll-collection devices. Because the increment in latency is neither changing unexpectedly nor growing exponentially.

Transaction throughput in blockchain is the number of transaction completed in a given time frame. It tells how fast a blockchain is. From Fig. 4b it can be observed that, throughput is decreasing when the number of nodes increases. This is because more nodes mean more validators in the network. And more validators mean it takes longer for all the validators to agree on the same block.

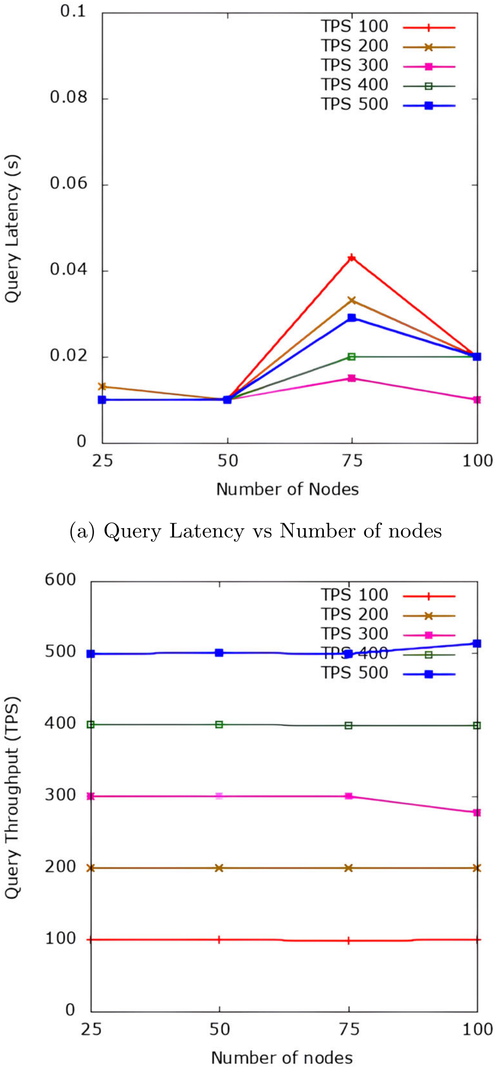
The time between sending a request for accessing the information and receiving the information is known as query latency. On the other hand, query throughput is the number of queries completed successfully within a specific period. A



(a) Transaction Latency vs Number of nodes

(b) Transaction Throughput vs Number of nodes

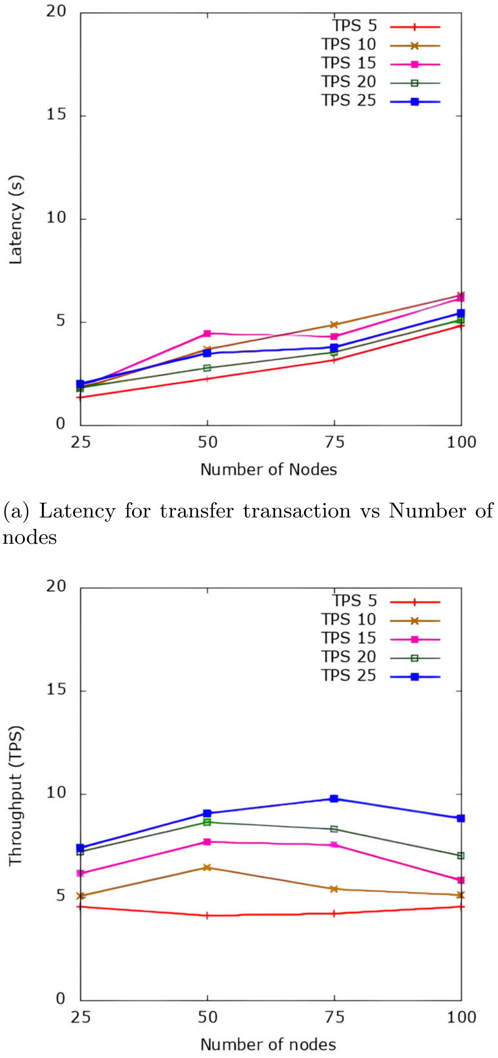
Fig. 4 Transaction latency and throughput vs number of nodes



(a) Query Latency vs Number of nodes

(b) Query Throughput vs Number of nodes

Fig. 5 Query latency and throughput vs number of nodes



(a) Latency for transfer transaction vs Number of nodes

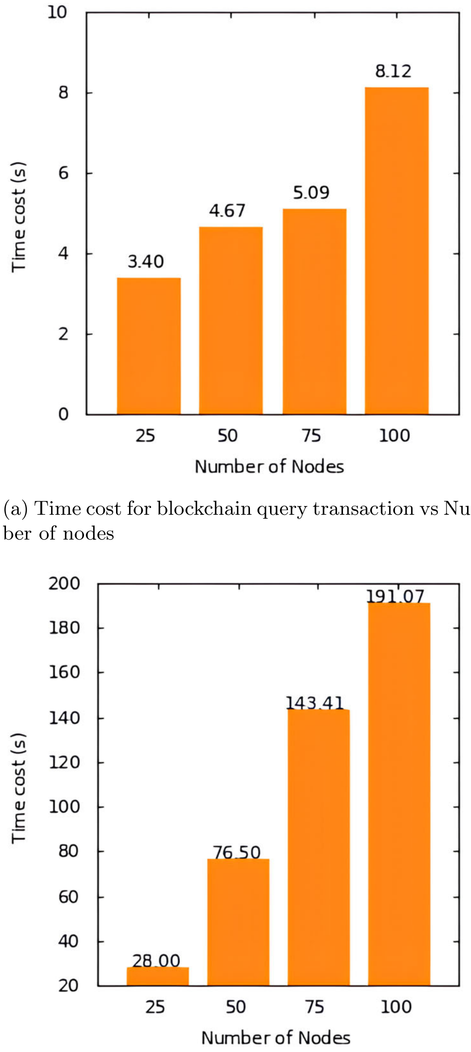
(b) Throughput for transfer transaction vs Number of nodes

Fig. 6 Latency and throughput for transfer transaction vs number of nodes

blockchain query doesn’t change the state of the blockchain but only reads data from the blockchain. It does not require any validation by the network and hence transactions are faster. In Fig. 5a and b, it is clear that number of blockchain nodes do not have much effect on the query latency, as well as query throughput. The throughput for query is very close to the rate of submitted transactions.

Primary looking components of real-world crypto currency blockchain performances are transfer transaction throughput and latency. Throughput of transfer transaction can be defined as the number of successful transfer transactions occurring in a given time frame. Inspired by this, to better analyze the performance of the proposed system, transfer transaction latency and throughput has also been recorded. Figure 6a and b show the effect of number of nodes on latency and throughput for transfer transaction. Unlike a CARS sign or a value store transaction, a transfer transaction modifies two values at two different places, one at the sender wallet and another at the receiver wallet. Here number of submitted transactions is kept lower. Like Fig. 6a, the latency increment is neither unexpected nor growing exponentially in Fig. 6a. As rate of submitted TPS is kept lower here, latency and throughput for transfer transaction are low.

The time taken to complete a fixed number of transactions can be expressed in terms of transaction time cost. The time cost provided in Fig. 7 represents the time required to finish 1000 transactions for varying number of nodes. Figure 7a



(a) Time cost for blockchain query transaction vs Number of nodes

(b) Time cost for CARS sign transactions vs Number of nodes

Fig. 7 Time cost for 1000 transaction vs number of nodes

and b shows the time cost of 1000 blockchain query and CARS sign transactions respectively. As the number of nodes increases, the time cost of both query and sign transaction also increases.

Real world challenge to implement BlockToll is, replacing existing system infrastructure and setting up STA and NTA will incur a good amount of initial investment to the transport department. Adding existing toll data if any available to the newly adopted system will be another challenging task. The primary limitation of the system could be, if the number of toll plazas within an NTA is very less, the authority may not be benefited much. Another limitation is, the system needs an enhancement to support inter-chain operation.

Use of multilevel blockchain has made the system very scalable. The proposed system scalability has been tested by simulating upto 100 blockchain nodes into a level. Interoperability of the proposed system can achieved by creating a bridge node to handle communication in cross-chain. The system will provide financial and managerial benefits to the transport authorities and hence the system will attract authorities to adapt the system. Also, the privacy feature will make the system more adaptable by vehicle users. In future, the system can be expanded to make it suitable for cross-domain and cross-chain in ITS.

8 Conclusion

This work proposes a secure toll collection system named *BlockToll* using hierarchical Blockchain and CARS. Two private blockchains have been created consisting of toll plazas, state authorities, and the national authority to store toll collection records. Ring signature has been used to hide the vehicle's trip information from other blockchain nodes so that no one is aware of the vehicle's travel information other than the government agencies. PoA consensus has been utilized to achieve faster transaction processing and high throughput. Security analysis of BlockToll has been done and compared to the baselines. Various simulation results have been provided to present how transaction latency and transaction throughput changes with the number of nodes. Also, the time cost for queries within blockchains and signing transactions is presented with respect to the number of nodes. The simulation results show the practicality and performance of the proposed scheme. The implementation of the proposed system in real life will make existing toll collection system more secure. Vehicle owner's details and their travel information will remain private. Toll payments received by toll plazas will be verifiable in the system which will increase revenue of transport authorities and governments. In the future, the proposed system will be enhanced in such a way that any deduction of toll amount from a vehicle account will require user confirmation. Also, other blockchains will be used to find if the throughput can be increased while providing at least equivalent or higher security.

Acknowledgements The authors are thankful to Mobile Computing Laboratory, Department of Computer Science & Engineering, Tripura University for providing necessary infrastructure to conduct the work.

Author Contributions The authors have jointly worked to model this problem and confirm contribution to the paper as follows: Writing - original draft, Writing review & editing, Visualization, Simulation, Result analysis was done by SC; Conceptualization, Methodology, Supervi-

sion was done by AM. All authors have read and agreed to the final version of the manuscript.

Funding Not Applicable.

Availability of Data and Materials Not applicable.

Declarations

Competing Interests The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethics Approval and Consent to Participate Not applicable.

Consent for Publication The authors give their consent for publication of the work if accepted for the same.

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Rev. **4**(2), 1–9 (2008)
2. Majeed, U., Khan, L.U., Yaqoob, I., Kazmi, S.A., Salah, K., Hong, C.S.: Blockchain for IoT-based smart cities: recent advances, requirements, and future challenges. J. Netw. Computer Appl. **181**, 103007–103031 (2021)
3. Shin, D.D.: Blockchain: the emerging technology of digital trust. Telematics Inf. **45**, 101278 (2019)
4. Yuan, Y., Wang, F.Y.: Blockchain: the state of the art and future trends. Acta Automatica Sinica **42**(4), 481–494 (2016)
5. Mohanty, S.N., Ramya, K., Rani, S.S., Gupta, D., Shankar, K., Lakshmanaprabu, S., Khanna, A.: An Efficient Lightweight Integrated Blockchain (ELIB) model for IoT security and privacy. Future Generatation Computer Syst. **102**, 1027–1037 (2020)
6. Kataoka, K., Gangwar, S., Podili, P.: Trust list: internet-wide and distributed IoT traffic management using blockchain and SDN. In: Proceedings of 4^{th} IEEE World Forum on Internet of Things (WF-IoT), IEEE, (pp. 296–301) (2018)
7. Novo, O.: Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Int. Things J. **5**(2), 1184–1195 (2018)
8. Tanveer, H., Javaid, N.: Using ethereum blockchain technology for road toll collection on highways [Graduate course major assignment, COMSATS University Islamabad, Pakistan] (2019)
9. Ying, Z., Yi, L., Ma, M.: BEHT: blockchain-based efficient highway toll paradigm for opportunistic autonomous vehicle platoon. Wireless Commun. Mobile Comput. **2020**, 1–13 (2020)
10. Das, D., Banerjee, S., Chatterjee, P., Biswas, M., Biswas, U., Alnumay, W.: Design and development of an intelligent transportation management system using blockchain and smart contracts. Cluster Comput. **25**(3), 1899–1913 (2022)
11. Xiao, B., Fan, X., Gao, S., Cai, W.: EdgeToll: a blockchain-based toll collection system for public sharing of heterogeneous edges. In INFOCOM IEEE Conference on Computer Communications Workshops (pp. 1–6). IEEE (2019)
12. Balasubramaniam, A., Gul, M.J.J., Menon, V.G., Paul, A.: Blockchain for intelligent transport system. IETE Technical Rev. **38**(4), 1–12 (2020)
13. Al-Nasser, F.A., Mahmoud, M.S.: Wireless sensors network application: a decentralized approach for traffic control and management. In: Matin, M.: Wireless Sensor Networks: Technology and Applications (pp. 347–374). IntechOpen (2012)
14. Waters, B., Juels, A., Halderman, J.A., Felten, E.W.: New client puzzle outsourcing techniques for DoS resistance. In: Proceedings of the 11^{th} ACM conference on Computer and communications security (pp. 246-256). ACM (2004)
15. Vujic M., Mandzuka S., Dedic L.: IoT Concept in cooperative traffic management. In: Karabegović I. (eds), New Technologies, Development and Application II (pp. 406–410). Springer (2019)
16. Namane, S., Ahmim, M., Kondoro, A., Dhaou, I.B.: Blockchain-based authentication scheme for collaborative traffic light systems using fog computing. Electronics **12**(2), 431 (2023)
17. Baskar L.D., De Schutter B., Hellendoorn H.: Decentralized traffic control and management with intelligent vehicles. In: Proceedings of the 9^{th} TRAIL Congress 2006 - TRAIL in Motion CD-ROM **1**, 3–16 (2006)
18. Al Amiri, W., Baza, M., Banawan, K., Mahmoud, M., Alasmary, W., Akkaya, K.: Towards secure smart parking system using blockchain technology. In: Proceedings of IEEE 17^{th} Annual Consumer Communications & Networking Conference (CCNC) (pp. 1–2). IEEE (2020)
19. Kim, M., Kim, Y.: Multi-blockchain structure for a crowd sensing-based smart parking system. Future Int. **12**(5), 1–18 (2020)
20. Nema, M., Stalin, S., Tiwari, R.: RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11 p. In: Proceedings of IEEE International Conference on Computer, Communication and Control (IC4) (pp. 1–5). IEEE (2015)
21. Wen, W.: An intelligent traffic management expert system with RFID technology. Expert Syst. Appl. **37**(4), 3024–3035 (2010)
22. Yuan, Y., Wang, F.Y.: Towards blockchain-based intelligent transportation systems. In: Proceeding of IEEE 19^{th} International Conference on Intelligent Transportation Systems (pp. 2663–2668). IEEE (2016)
23. Li, M., Weng, J., Yang, A., Liu, J.N., Lin, X.: Toward blockchain-based fair and anonymous ad dissemination in vehicular networks. IEEE Trans. Vehicular Technol. **68**(11), 11248–11259 (2019)
24. Feige, U., Fiat, A., Shamir, A.: Zero-knowledge proofs of identity. J. Cryptol. **1**(2), 77–94 (1988)
25. Haghighat, A.K., Ravichandra-Mouli, V., Chakraborty, P., Esfandiari, Y., Arabi, S., Sharma, A.: Applications of deep learning in intelligent transportation systems. J. Big Data Analytics Transportation **2**, 115–145 (2020)
26. Jiang, W., Luo, J.: Graph neural network for traffic forecasting: a survey. Expert Syst. Appl. **207**, 117921 (2022)
27. Shamsi, M., Rasouli Kenari, A., Aghamohammadi, R.: Reinforcement learning for traffic light control with emphasis on emergency vehicles. J. Supercomput. **78**(4), 4911–4937 (2022)
28. Shahrier, M., Hasnat, A., Al-Mahmud, J., Huq, A.S., Ahmed, S., Haque, M.K.: Towards intelligent transportation system: a comprehensive review of electronic toll collection systems. IET Intell, Transport Syst (2024)
29. Kharche, A., Badholia, S., Upadhyay, R.K.: Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India. Blockchain: Res. Appl. 100188 (2024)
30. Sun, X., Dou, H., Chen, S., Zhao, H.: A novel block-chain based secure cross-domain interaction approach for intelligent transportation systems. Phys. Commun **63**, 102223 (2024)
31. Soner, S., Litoriya, R., Pandey, P.: Making toll charges collection efficient and trustless: a Blockchain-based approach. In 3^{rd} International Conference on Advances in Computing, Communication Control and Networking (pp. 1533–1538). IEEE (2021)
32. Naik, D.A., Soumya, C.S., Mahadesh, J., Braganza, J.A., Singh, P., Nanda, R.: Revolutionizing transportation infrastructure and communication technology through blockchain and 5G simulation. *In: International Conference on Intelligent and Innovative Tech-*

nologies in Computing, Electrical and Electronics (pp. 1–7). IEEE (2024)

33. Didouh, A., Lopez, A. B., El Hillali, Y., Rivenq, A., Al Faruque, M.A.: Eve, you shall not get access! A cyber-physical blockchain architecture for electronic toll collection security. In: 23^{rd} International Conference on Intelligent Transportation Systems (pp. 1-7). IEEE (2020)
34. Patil, S., Kulkarni, M., Desale, S., Adsul, D., Choudhary, K.: Smart toll booth system using smart contract. In: 2023 IEEE 8^{th} International Conference for Convergence in Technology (pp. 1–6). IEEE (2023)
35. Thosar, K., Singh, H., Chatterjee, S., Ambawade, D.: Blockchain-based Booth-less Tolling System using GPS and Image Processing. In: IEEE World AI IoT Congress (pp. 380–383). IEEE (2023)
36. Rivest, RL., Shamir A., Tauman Y.: How to leak a secret. In: International Conference on the Theory and Application of Cryptology and Information Security (pp 552-565). Springer (2001)
37. Zhang, X., Ye, C.: A novel privacy protection of permissioned blockchains with conditionally anonymous ring signature. Cluster Comput. **25**(2), 1221–1235 (2022)
38. Toll Plazas - At a Glance. National Highways Authority of India. https://tis.nhai.gov.in/tollplazasataglance.aspx? Accessed 2 Feb 2024

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Sukanta Chakraborty received the M.C.A. degree from Indira Gandhi National Open University, New Delhi, India, in 2016, and the M.Tech degree in Computer Science & Engineering from Tripura University, Tripura, India, in 2019 respectively. He is currently Pursuing Ph.D. in Computer Science and Engineering at Tripura University. His main research interests include IoT, Network security, Blockchain, privacy protection and Intelligent Transportation System.

Abhishek Majumder is currently working as Assistant Professor in the Department of Computer Science & Engineering, Tripura University (A Central University). Prior to joining Tripura University he had worked as Assistant Professor in the Department of Information Technology (Currently Department of Computer Science & Engineering, Assam University (A Central University). He had completed his BE, M.Tech and PhD from NIT Agartala, Tezpur University and Assam University respectively. His research interests are Mobile Computing, IoT, AI and Network Security. He has published more than 50 papers in National and International Journals and Conferences. He has also authored many book chapters in books published by reputed publishers. As Principal Investigator/Coordinator he has handled projects funded by Ministry of Electronics and Information Technology, Government of India and AICTE.