Trust Access Authentication in Vehicular Network Based on Blockchain

Shaoyong Guo[1,*], Xing Hu[1], Ziqiang Zhou[2], Xinyan Wang[3], Feng Qi[1], Lifang Gao[4]

[1] State Key Laboratory of Networking and Switching Technology, BUPT, Beijing 100876, China
[2] State Grid Zhejiang Electric Power Co., Ltd. Institute of Electric Power Science, Zhejiang 310007, China
[3] State Grid Henan Electric Power Company Information and Communication Company, Henan 450052, China
[4] State Grid Hebei Electric Power Company, Information and Communication Company, Hebei 050022, China
* The corresponding author, email: syguo@bupt.edu.cn

Abstract: Data sharing and privacy securing present extensive opportunities and challenges in vehicular network. This paper introduces `trust access authentication scheme' as a mechanism to achieve real-time monitoring and promote collaborative sharing for vehicles. Blockchain, which can provide secure authentication and protected privacy, is a crucial technology. However, traditional cloud computing performs poorly in supplying low-latency and fast-response services for moving vehicles. In this situation, edge computing enabled Blockchain network appeals to be a promising method, where moving vehicles can access storage or computing resource and get authenticated from Blockchain edge nodes directly. In this paper, a hierarchical architecture is proposed consist of vehicular network layer, Blockchain edge layer and Blockchain network layer. Through a authentication mechanism adopting digital signature algorithm, it achieves trusted authentication and ensures valid verification. Moreover, a caching scheme based on many-to-many matching is proposed to minimize average delivery delay of vehicles. Simulation results prove that the proposed caching scheme has a better performance than existing schemes based on centralized model or edge caching strategy in terms of hit ratio and average delay.

Keywords: blockchain; vehicular network; edge computing; authentication mechanism; many-to-many matching

Received: Oct. 17, 2018
Revised: Mar. 25, 2019
Editor: Min Lei

I. INTRODUCTION

With the development of Industrial Internet of Things (IIoT) technologies in vehicular network, data sharing among different vehicles becomes necessary, which brings serious threats to data integrity and privacy security. A trust access authentication network is in urgent need to achieve real-time monitoring and promote collaborative sharing. As a popular technology applied to IIoT scenarios, Blockchain is paid increasing attention to provide secure authentication and protected privacy for vehicles. First proposed by Satoshi Nakamoto, it consists transaction blocks that can be verified and confirmed without centralized authentications [1], [2].

Existing works have been studied to apply Blockchain to various scenerios of IIoT. In [3], it proposed a reputation system based on Blockchain for data credibility assessment. Authors in [4] designed a prototype proving

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

that a Blockchain based on-demand insurance system can be realized for vehicles. [5] introduced an autonomous negotiation selecting the most convenient electric vehicle charging station according to Blockchain.

However, the centralized model cannot cover all vehicles for they are usually mobile and geographically distributed. Moreover, data stream generated by innumerable cars causes heavy burden for core network. To improve efficiency of data processing, many novel schemes have also been proposed. Authors in [6], [7] considered parking vehicles as storage resource to enhance capacity, at the cost of increasing probability of revealing owners' privacy. [8], [9] improved network efficiency through Network Function Virtualization and a novel resource allocation algorithm. In [10], it established a hierarchical VEC offloading framework in cloud-based vehicular network. Nevertheless, long delivery latency and poor real-time monitoring are still issues to be solved.

Therefore, an edge computing enabled Blockchain network is introduced to improve real-time response and edge security. Edge computing is a new computing model whose nodes distribute geographically [11], [12]. By allowing smart cars to access and utilize storage and computing resource from edge nodes, the system promote deployment of Blockchain in peer-to-peer networks. It enables direct authentication between vehicles and edge nodes, reduces load in Blockchain network, and achieves information sharing among Blockchain edge nodes.

Researchers consider to establish distributed trust framework through combining edge computing and Blockchain. [13] proposed a novel mobile edge computing enabled wireless blockchain framework, where the computation-intensive mining tasks can be offloaded to nearby edge nodes. Authors in [14] established a blockchain-based distributed cloud architecture with software defined network (SDN). It could provide low-cost, secure and on-demand access to the most competitive computing infrastructure based on fog computing, but authors ignored mobility of vehicles. In [15], it analyzed the advantages of facilitating blockchain applications in future mobile IoT system without specific applications.

These articles mentioned above have dedicated to solve trust access problems, while they ignore mobility and high standard for low-latency services in vehicular networks. In this paper, we establish a distributed trust access authentication system for vehicular network, where a hierarchical architecture is constructed combining Blockchain network and edge computing, to support collaborative sharing and valid authentication. Blockchain network is adopted as the underlying architecture for recording device information and protecting privacy. And edge computing enables to lower delivery latency and improve response. Additionally, an authentication mechanism according to digital signature algorithm is designed to ensure data security and privacy protection. Furthermore, a caching scheme according to many-to-many matching is proposed, aiming to minimize vehicle latency in delivering. Main contributions of this paper can be summarized as follows:

- A hierarchical architecture including vehicular network layer, Blockchain edge layer and Blockchain network layer is established. It achieves trust access for vehicles and collaborative sharing among different vehicular network. Therefore, it enhances network capability, lowers delivery latency and improves authentication speed.
- An authentication mechanism based on Blockchain is designed, achieving trust access authenticating and reliable verifying for vehicles. Considering frequent connections among nodes and vehicles, a digital signature algorithm is applied to prevent links from being attacked.
- An edge caching scheme according to many-to-many matching is proposed. Through optimizing caching strategy dynamically, it can minimize average delay and promote collaborative sharing performance.

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

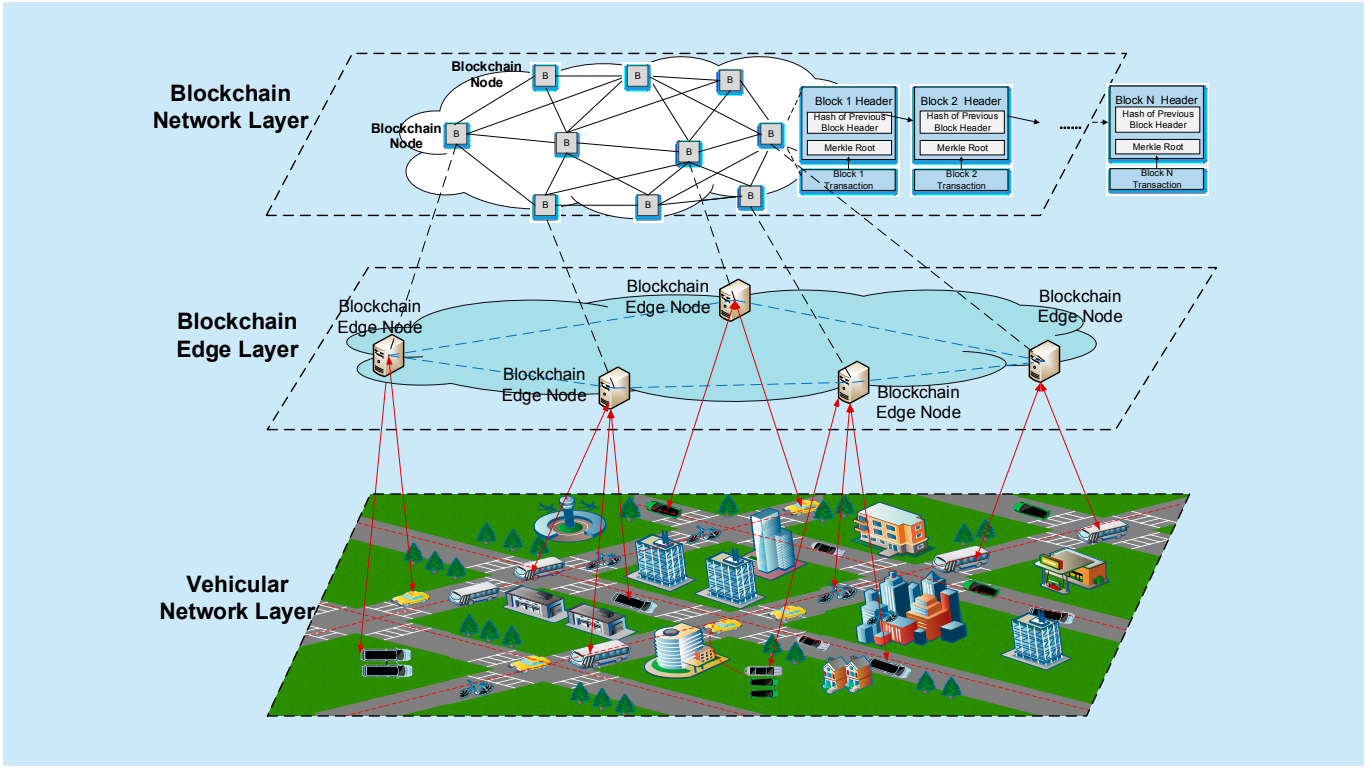

Fig. 1. *System architecture.*

II. System Model

In this section, we demonstrate a broad overview of our proposed architecture and introduce authentication process for a vehicle to register in blockchain network through edge nodes.

2.1 Block hierarchical architecture

Different from previous studies which applied Blockchain in IIoT scenario adopting cloud model [16], [17], we establish a three-layer architecture combining edge computing to realize trust access and handle long transmission delay. As shown in figure 1, it consists of vehicular network layer, Blockchain edge layer, and Blockchain network layer. Function of each layer is described as follows:

- **Vehicular Network Layer:** As the widespread use of IIoT technologies in vehicular network, smart vehicles are equipped with many sensors that collect data and transfer it to other layer. It gets crucial for them to achieve secure communication and protected privacy as they lack access control mechanism and encryption. Moreover, long communication latency in Blockchain network is also unbearable for a car moving with high speed.
- **Blockchain Edge Layer:** Blockchain edge nodes can synchronize and update device information based on vehicle activity as a Blockchain network client. They register vehicles in Blockchain and create smart contract after obtaining authority from vehicles. Furthermore, information sharing through channels between edge nodes helps to reduce delivery latency for vehicles and relieve traffic jam in the Blockchain network.
- **Blockchain Network Layer:** Blockchain network provides a decentralized service of storing device information and creating smart contract. It's a distributed ledger which can orderly store and record device information and transaction. Each recorder in the ledger acts as a time constraint and a unique cryptographic signature.

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

2.2 Delivery model

In the system, distribution of edge nodes follows PPP ... Poisson Point Process (PPP) with intensity of λ_B, and λ_B represents the initial number of nodes per square kilometers [18]. Their set is denoted as $B = \{B_1, B_2, \cdots, B_N\}$. Set of M vehicles is $V = \{V_1, V_2, \cdots, V_M\}$, which deploys randomly in the area.

A dedicated frequency band of bandwidth W_i is allocated to the downlink channels from the Blockchain network to B_i. For collaborative sharing among edge nodes is crucial to improve edge security and edge process, vehicles can also get requested data from nearby nodes having cached its information via connected node. On case that none of nodes cache the device information, the vehicle need to obtain response from the Blockchain network. For the sake of simplify, we think Blockchain network supplies a fixed download rate of R_0. As core network is usually located far from devices in the edge, it's believed that R_0 is lower than download rate supported by connected nodes.

To show connections between edge nodes and vehicles, a location matrix is defined by $\mathbf{L}_{i,j} = \left[l_{i,j} \right]_{N \times M}$, where

$$l_{i,j} = \begin{cases} 1, \text{ if } V_j \text{ is within coverage of } B_i \\ 0, \text{ otherwise} \end{cases}.$$

Due to limited caching capacity, B_i requires to determine whether to cache device information of V_j. A caching matrix is defined as $\mathbf{C}_{i,j} = \left[c_{i,j} \right]_{N \times M}$, where

$$c_{i,j} = \begin{cases} 1, \text{ if information of } V_j \text{ is cached in } B_i \\ 0, \text{ otherwise} \end{cases}.$$

III. Blockchain Based Authentication Mechanism

To supply trust access authenticating for vehicles and guarantee valid verification and confirmation among edge nodes and moving vehicles, an authentication mechanism based on Blockchain is designed as follows.

3.1 Trust access authentication

Figure 2 demonstrates the process for a vehicle to get authenticated in the Blockchain network. Firstly, the vehicle information and privacy policy will be uploaded to Blockchain edge nodes from the vehicle and then be delivered to Blockchain. Then the Blockchain network generates a block and invokes transactions to store device information and associated privacy. A unique ID and a pair of keys shall be distributed to the vehicle. After authorized by the vehicle, Blockchain creates a smart contract for it.

A smart contract is scripts stored on the Blockchain with a unique address. It executes independently and automatically in a prescribed manner on every node in the network, according to the data that was included in the triggering transaction [19]. By sending transaction to the address, trusted nodes in the system can access to the smart contract and invoke its function, which enables direct authentication for registered vehicles without revealing device privacy.

To achieve user control over Blockchain network, a pair of private key and public key will be distributed to vehicles. The private key shall be kept confidentially to sign or modify the transactions. The public key of vehicles can be delivered to edge nodes, allowing them to download device information with permission. Thus when moving vehicles enter coverage of different edge nodes, they can delivery public keys to nodes and get authenticated directly.

Blockchain based vehicular network ensures the valid authentication, integrity and nonrepudiation in device registering through smart contracts, asymmetric cryptography mechanism and so on. It allows us to have a distributed peer-to-peer network where non-trusting vehicles can interact with each other without a trusted intermediary, in a verifiable manner. In this way, we realize trust access authenticating for vehicles and shorten certificating latency in moving.

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

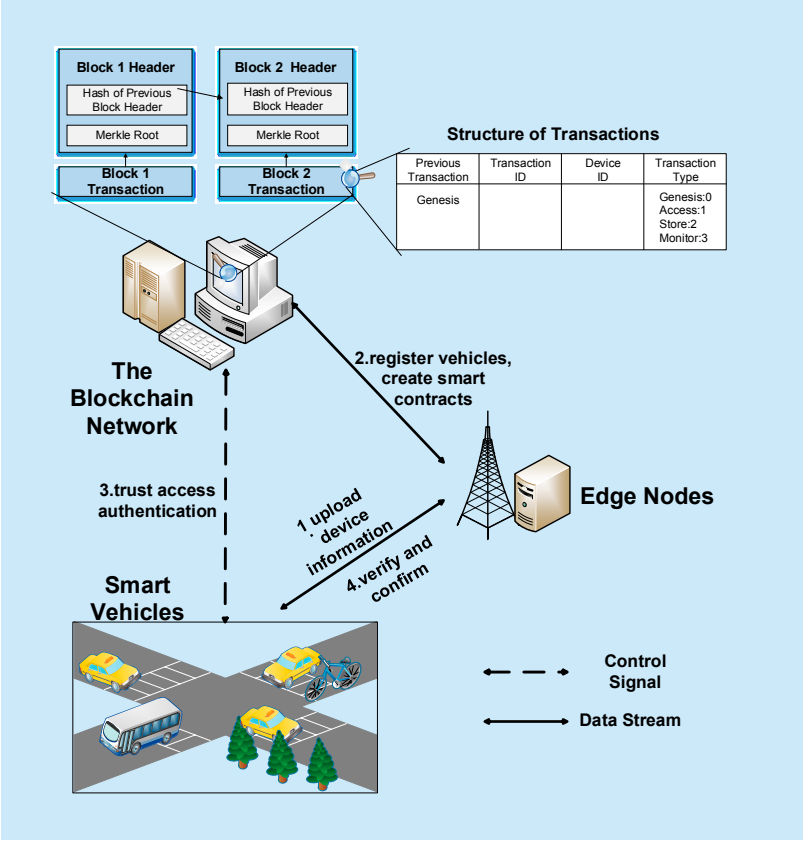

Fig. 2. *Overview of the Blockchain based vehicular network.*

3.2 Verification and confirmation according to digital signature algorithm

Vehicles should be verified by edge nodes and receive confirmation before getting accessed to them when entering coverage of new nodes. In the communication process, applying digital signature algorithm is necessary to prevent messages being attacked and tampered, for frequent contacts between edge nodes and vehicles are lacked of monitoring measurement. A typical digital signature algorithm used in Blockchain is Elliptic Curve Digital signature algorithm (ECDSA) based on Elliptic Curve Discrete Logarithm Problem (ECDLP) [20].

Let E/E_p denote a plane curve E over a prime finite field E_p, including all the points satisfying $y = x^3 + ax + b$ with the discriminant of the Weierstrass equation $\Delta = 4a^3 + 27b^2 \neq 0$. All point on E and infinity point O form a cyclic group G. Scalar multiplication can be computed as: $tP = P + P + \cdots + P(t\ times)$, where P is a generator of G with order n. In ECDLP, given G with prime order n, a generator P of G and aP, it is computationally infeasible to derive a. Therefore, ECDSA can guarantee security based of the intractability of ECDLP. Assume that G_1 and G_2 are cyclic group with the same prime order q, where G_1 is an additive cyclic group and G_2 is a multiplicative cyclic group. Define $e: G_1 \times G_1 \to G_2$, and a formulation can be written:

$$e(aP, bQ) = e(P, Q)^{ab}, \forall a, b \in Z_q^*, \forall P, Q \in G_1, \tag{1}$$

The algorithm can be devided in 4 steps as follows:

3.2.1 Setup

Blockchain edge nodes choose a number $s \in Z_q^*$ as master private key and computes master public key $PK_{BE} = s \cdot P$. Two secure hash functions are chosen: $H_1: \{0,1\}^* \times G_1 \to Z_q^*$, $H_2: \{0,1\}^* \times G_1 \times G_1 \to Z_q^*$. $\{s, PK_{BE}, H_1, H_2\}$ will be broadcast in the system as public parameters.

3.2.2 Abstract

After registering in the Blockchain network for V_j, B_i assigns the private key to the vehicle, achieving user controlling on privacy policy.

Given public parameters and V_j's ID ID_j, B_i selects a random number $r_j \in Z_q^*$ and calculates following formulations:

$$R_j = r_j \cdot P, \tag{2}$$

$$h_j = H_1(ID_j, R_j, PK_{BE}), \tag{3}$$

$$u_j = r_j + h_j \cdot s \bmod q. \tag{4}$$

Then (R_j, v_j) is transmitted to V_j as the private key from B_i. V_j can validate the private key through checking whether the following equation is hold:

$$u_j \cdot P = R_j + H_1(ID_j, R_j, PK_{BE}) \cdot P. \tag{5}$$

When the equation is satisfied, V_j can confirm reliability of the node private key received from B_i.

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

3.2.3 Sign

In communicating with edge nodes, V_j shall sign a message m with public parameters.

It selects a random number $x_j \in Z_q^*$ as the private key and computes public key, $PK_j = x_j \cdot P$.

According to ECDSA, we have:

$$X_j = H_2\left(ID_j, PK_j, R_j, PK_{BE}, m\right), \quad (6)$$

$$v_j = \left(X_j \cdot u_j + x_j\right) \bmod q. \quad (7)$$

Therefore, V_j's signature for the message m is $\left(m, PK_j, u_j\right)$.

3.2.4 Verify

Upon receivng signature $\left(m, PK_j, u_j\right)$ from V_j, B_i verifies the validity of messages through an examing equation:

$$v_j \cdot P = PK_j + H_2\left(ID_j, R_j, PK_{BE}\right) \cdot P. \quad (8)$$

If and only if the equation is proved to be true, will B_i accept the signature and open access to the vehicle.

To sum up, the digital signature algorithm plays an important role in verifying and confirming, ensuring data integrity, accessibility and security in transmitting between edge nodes and vehicles.

IV. Caching Scheme Based on Many-to-Many Matching Algorithm

In this section, a caching scheme based on many-to-many matching algorithm is put forward. It can adjust resource allocating strategy of caching capacity dynamically as vehicles' location changes, satisfying their demand for low-latency and fast-response service.

4.1 Caching model

According to [22], the arrival rates of vehicles follows Poisson distribution with parameter λ, and their duration time follows an exponential distribution having expected value μ. Define $\eta = \lambda / \mu$. Let $M_{\max}$ represent maximal number that Blockchain edge nodes can support. Then probability of k vehicles' coming can be calculated as:

$$pro_k = \frac{\eta^k}{k!} \cdot pro_0 = \frac{\eta^k}{k!} \cdot \frac{1}{\sum_{k=0}^{M_{\max}} \left(\eta^k / k\right)}. \quad (9)$$

Based on eq. (9), expected number of vehicles in the whole system can be calculated as follows::

$$M = \sum_{k=0}^{M_{\max}} k \cdot pro_k, \quad (10)$$

Assume that data size of device information for V_j is da_j, and size of required data is s_j. Caching capacity of B_i is denoted by Cap_i. Define P_i as transmission power of B_i, and σ_j^2 as noise power of V_j. According to [21], path-loss between B_i and V_j can be modeled as $d_{i,j}^{-\alpha}$, where $d_{i,j}$ is distance between them, and α is path-loss exponent. $f_{i,j}$ represents coefficient of Rayleigh fading between B_i and V_j. To eliminate interference among channels distributed from Blockchain edge nodes to devices, all the downlink channels are independent and identically distributed. When B_i covers V_j, transmission rate between them can be calculated based on signal to interference plus noise ratio [18]:

$$R_{i,j} = W_i \log\left(1 + \frac{f_{i,j}^2 \cdot d_{i,j}^{-\alpha} \cdot P_i}{\sum_{k \in V/i} f_{k,j}^2 \cdot d_{k,j}^{-\alpha} \cdot P_k + \sigma_j^2}\right), \quad (11)$$

where $\sum_{k \in V/i} f_{k,j}^2 \cdot d_{k,j}^{-\alpha} \cdot P_k$ represents the total interference caused by other nodes to V_j except B_i.

To evaluate performance of the caching scheme, hit ratio is used to denote probability that edge node caches information of covered vehicles. Hit ratio of B_i can be calculated as:

$$hit_i = \frac{\sum_j c_{i,j} \cdot l_{i,j}}{\sum_j l_{i,j}}. \quad (12)$$

Hence total hit ratio for edge nodes is:

$$Hit = \frac{\sum_i hit_i \cdot \sum_j l_{i,j}}{M} = \frac{\sum_i \sum_j c_{i,j} \cdot l_{i,j}}{M}, \quad (13)$$

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

4.2 Delivery latency for vehicles

When a vehicle expects to obtain response from higher layer, it has three options with different delivery latency. We give analysis of all choices in next parts.

4.2.1 Latency to connected edge nodes

V_j is able to download data from B_i directly if it is coverd by B_i and finds device information in the node. In other words, $l_{i,j} \cdot c_{i,j} = 1$. According to (11), latency for vehicles obtaining information from connected nodes is:

$$t_{i,j} = \frac{s_j}{R_{i,j}}. \tag{14}$$

4.2.2 Latency to nearby edge nodes

If information of V_j is not available in connetcted node B_i, V_j can fetch information from B_k through B_i. Distance between them is expressed as $D_{i,k}$. Let $B_{i,k}$ be average bandwidth on the path, and transmission delay from B_k to B_i is:

$$t_{B_i,B_k} = \frac{s_j}{B_{i,k}} \cdot D_{i,k}. \tag{15}$$

Given weight factor $\beta_{i,j}$ related to network core congestion, transmission latency from nearby node B_k to V_j according to (14)-(15) is:

$$\begin{aligned} t_{k,j} &= \beta_{i,j} \cdot \left(t_{i,j} + del_{B_i,B_k} \right) \\ &= \beta_{i,j} \cdot \left[\frac{s_j}{R_{i,j}} + \frac{s_j}{B_{i,k}} \cdot D_{i,k} \right]. \end{aligned} \tag{16}$$

4.2.3 Latency to the BlockChain network

If no edge nodes cache device information, V_j has to submit requests to the Blockchain network. For simplification, the Blockchain network is regarded as the $(N+1)_{th}$ edge node, which can be denoted by B_{N+1}. Given transmission rate R_0 and weight factor γ, delay from Blockchain network to V_j can be calculated as:

$$t_{N+1,j} = \gamma \cdot \left(\frac{s_j}{R_0} \right). \tag{17}$$

Above all, transmission delay that V_j need to fetch data from higher layer is:

$$T_j = \sum_i c_{i,j} \cdot t_{i,j}. \tag{18}$$

To minimize average latency, the optimization problem can be formulated as:

$$\begin{aligned} &\text{minimize } T(C) = \frac{1}{M} \sum_j T_j, \\ &s.t. \begin{cases} \sum_j c_{i,j} \cdot da_j \le Cap_i, \forall B_i \in B, \forall V_j \in V, \\ \sum_i l_{i,j} = 1, \\ C, L \in \{0,1\}^{N \times M}. \end{cases} \end{aligned} \tag{19}$$

Obviously, Total caching size shouldn't exceed capacity of storage space of Blockchain edge nodes. The optimization problem is an integer programming problem, which is NP-hard. We intend to solve it with many-to-many matching.

4.3 Algorithm based on many-to-many matching

In this part, a many-to-many matching is proposed to solve optimizing problem. According to [23], Blockchain edge nodes and vehicles are two set of players in the matching, which are individually rational. Based on delivery delay and caching size, a utility function is defined to represent system cost if B_i determines to allocate caching capacity to V_j:

$$f^i(j) = t_{i,j} + \rho \cdot da_j, \forall i \in \mathbf{B}, \forall j \in \mathbf{V}, \tag{20}$$

where ρ is the weight factor for caching resource. Specially, when i equals to $N+1$, the vehicle intends to cache terminal information in Blockchain network. Lower costs mean that edge nodes can provide low-latency service for vehicles with small storage size. Observing the utility function over each vehicle, B_i has a preference list on all vehicles, represented by $\Phi^i = \left\{ \phi_1^i, \phi_2^i, \cdots, \phi_M^i \right\}$. Vehicles with high preferences can get priority in resource allocating of caching capacity. As node prefers to choose vehicle with lower expenses, we set,

$$\phi_j^i = -f^i(j), \forall i \in \mathbf{B}, \forall j \in \mathbf{V}. \tag{21}$$

Furthermore, each vehicle has different preference over edge nodes and Blockchain network. Therefore, a preference list is set, de-

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

noted by $\Psi^j = \left\{\psi_1^j, \psi_2^j, \cdots, \psi_N^j, \psi_{N+1}^j\right\}$, where

$$\psi_i^j = -f^i(j), \forall i \in \mathbf{B}, \forall j \in \mathbf{V}. \quad (22)$$

On the basis of preference lists, a many-to-many matching algorithm between BEs (Blockchain edge nodes and Blockchain network) and vehicles is designed as algorithm 1 described. After initializing, the preference lists of BEs and vehicles, i.e., Φ^i and Ψ^j, are constructed, and their pointers move to the most preferred objects in the lists. At each round vehicles which have not been responded in past rounds will move pointer to preferred BE and submit requests. Observing behaviors of vehicles, each BE chooses its most preferred vehicle in the preference list until all caching capacity has been allocated. At the end of each round, if vehicle is accepted by BE, pointer of its preference list remains unchanged and the caching matrix is updated. Otherwise, the pointer of rejected vehicle will move to the next BE in list. In next round, the vehicle requests for caching space to the new BE. The matching repeats in circulations till all vehicle information have been cached in suitable BEs. And the caching matrix $\mathbf{C}_{i,j}$ shows the optimizing results. Based on the matching algorithm, we can calculate the minimum average delivery latency $T(\mathbf{C})$.

Lemma 1. *Following the algorithm 1, the caching optimization will ultimately converge and achieve a stable matching result.*

Proof. For each vehicle in the matching algorithm, the pointer of the vehicle's preference list moves in one direction. It chooses the most preferred BE to cache device information firstly, aiming to obtain minimizing delay. If its request is rejected by the BE, the pointer moves to the suboptimal BE. Above processes repeat until one BE meets demand of the vehicle. In this way, the vehicle cannot achieve a lower latency through moving the pointer back.

Therefore, when the pointer of each vehicle moves to the end of preference list, it has evaluated all BEs and has chosen one. In other words, it cannot gain higher utility by unilaterally changing caching location and submitting request for other BEs. Furthermore, through multi-rounds of matching algorithm, each BE has traversed all vehicles and has distributed caching capacity in an optimized way. According to [20], when two preference list in the matching market is substitutable, a pairwise stable matching always exists. Above all, the caching optimization will ultimately converge and achieve a stable matching result.

Algorithm 1. Many-to-many matching algorithm for caching problem.

Initialize matrixs $\mathbf{L}_{i,j} = \left[l_{i,j}\right]_{N\times M}$, $\mathbf{C}_{i,j} = \left[c_{i,j}\right]_{N\times M}$.
for B_i **do**
    Construct a preference list on vehicles based on (21);
    One pointer is set as the indicator pointing at the vehicle with highest value in preference list;
end for
for V_j **do**
    Construct the preference list on all BEs according to (22);
    One pointer is set pointing at the largest item in the list;
end for
Set $flag_j, \forall j \in V$, to show whether the vehicle has been chosen by BEs in last round, but discarded in current round. Initially, $flag_j = 0$;
while the pointers of all BEs have not scanned all vehicles **do**
    for V_j whose information have not been cached **do**
        if $flag_j = 0$
            The pointer keeps current position in the preference list of V_j;
        else
            The pointer moves to the next position in the preference list of V_j;
        end if
        The vehicle submits requests to pointed BE with required caching size;
    end for
    for B_i **do**
        if the available caching capacity of B_i exceeds the requirement space of vehicles **then**
            B_i allocates caching space to the most preferred vehicle whose pointer points to B_i. Set $c_{i,j} = 1$;
        else
            B_i rejects the request of V_j. Set $flag_j = 1$;
        end if
    end for
end while
Calculate $T(\mathbf{C})$ according to (19);

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

V. Simulation Results and Analysis

5.1 Security analysis

CIA triad is basically guidelines which are set for information security in an organization, known as confidentiality, integrity, and availability [24]. Confidentiality makes sure that only the authorized user is able to read the message. Integrity guarantees the message is correct and trustworthy in transmitting, and availability means that the data is accessible to authorized users only. In this article, the Blockchain network achieves confidentiality via smart contracts and asymmetric encryptions. To ensure data integrity, the digital signature algorithm adopted in authentication mechanism is designed, protecting communication among edge nodes and vehicles in open environment. In order to increase availability, vehicles are protected from unauthorized requests. Edge nodes cannot access to vehicle information and privacy without public key distributed from the vehicle. Moreover, the caching scheme improves data sharing among platforms on the basis of getting authority from vehicles. Therefore, minimizing latency has no impact on vehicle availability. In summary, the Blockchain based vehicular network makes improvements in CIA triad.

5.2 Simulation performance

In this section, we evaluate performance of our proposed system with simulator in Matlab. In simulation model, capacity of edge nodes is 1 GB, and size of device information ranges from 10 MB to 50 MB. Vehicles gain data from nodes with size of 1 MB. Transmission rate between nodes is 15 Mbps. For simplify, all the BEs have the same transmission power P and channel fading coefficients. The arrival of mobile terminals is decided by Poisson distribution with parameter λ, and departure time follows exponentially distribution with index μ. Parameters used in the simulation is list as Table. 1 shows.

Table I. *Simulation parameters.*

Parameters[Symbols]	Value[Units]
Path loss exponent, α	4
Transmission power, P	2
Noise power, σ_j^2	10^{-10}
Number of BEs, N	2:2:8 /km^2
Number of vehicles, M	50:50:500/km^2
Bandwidth, W	10^7Hz
Size of vehicle information, da_j	[10,50] MB
Size of requested data, s_j	1 MB
Caching capacity of BEs, B	15 Mbps
Vehicle's arrival interval, λ^{-1}	10:2:28
Vehicle's depature interval, μ^{-1}	300:10:390

To better evaluate the proposed caching scheme in this article, we study different mechanism that vehicles gain informtion from higher layer in vehicular network as below:

- Blockchain network based scheme (BCBS): vehicles can authenticate and fetch information from the Blockchain network directly.
- Least recently arrived based scheme (LRBS): information of the vehicle which arrived the node earliest will be removed from caching space, and Blockchain edge node replaces it with newly coming device information.
- Many-to-many matching algorithm based system (MMBS): according to our proposed scheme, edge nodes can verify vehicles and allocate caching capacity to them dynamically and efficiently.

In simulation, experiments are conducted with different parameters changing, i.e., total number of vehicless, intensity of edge nodes in the network and caching capacity of nodes, to perform proposed scheme by comparison with BCBS and LRBS in terms of average delivery delay and hit ratio.

Figure 3 shows changes of hit ratio and average delivery delay versus total number of vehicles under 3 situations. Hit ratio of BCBS always equals to 1 for all terminal's information are cached in Blockchain network. Following rising amount of terminal, values of hit ratio in BPBS and LRBS are close to 1 and decline gradually. When it comes to average delivery delay, values of 3 curves rise with

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

mobile terminals increasing. Among them BCBS has the biggest latency, since fetching data from Blochchain network for terminals goes through the longest transmission distance. Under BPBS and LRBE, their changes of curves are similar when there are a few vehicles in network. With terminal amount increasing, BPBS has a lower latency and higher hit ratio than LRBS. Reasons are that though vehicle's demand for caching capacity surpasses available space of nodes, BPBS can allocate caching capacity efficiently and dynamically by considering terminal number and caching size to minimum average delay.

Figure 4 represents influence of arrival interval λ^{-1}. When λ^{-1} gets greater, average delivery delay decreases. High arrival rate means vehicles staying in this area are fewer. Thus a larger proporation of vehicles can cache information in nodes with lower latency. It's observed that LRBS may has a better performance than BPBS for it caches terminal information in connected node with priority. And BCBS undertakes the largest delay.

In figure 5, average delivery delay decreases in pace with μ^{-1} getting larger. When departure interval increases, more cars are left in this area, causing caching burden to edge nodes or Blockchain network. Moreover, delivery latency will get higher. Increasing speed of curves also becomes faster. Among three schemes, BPBS has the smallest average delay benefited from collaborative sharing among nodes.

Finally, we examine performance of proposed scheme with different average caching capacity of Blockchain edge nodes when number of nodes varies within this area.

Figure 6 shows changes of hit ratio with different average caching capacity of edge nodes when number of nodes varies. When caching space increases ranging from 400 MB to 2400 MB, a larger proportion of mobile terminals' information which can be cached in nodes arises. For the node can meet demands of more requested vehicles. Moreover, as node intensity rising, hit ratio can also get higher

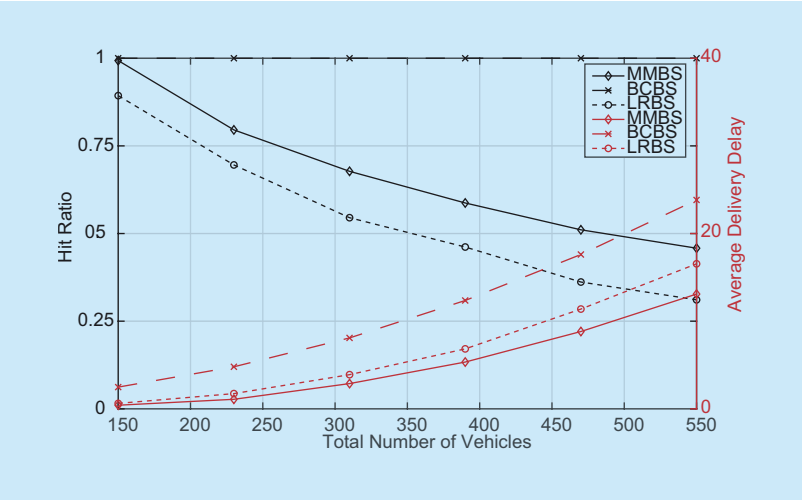

Fig. 3. *Hit ratio and aveage delivery delay with different total number of vehicles.*

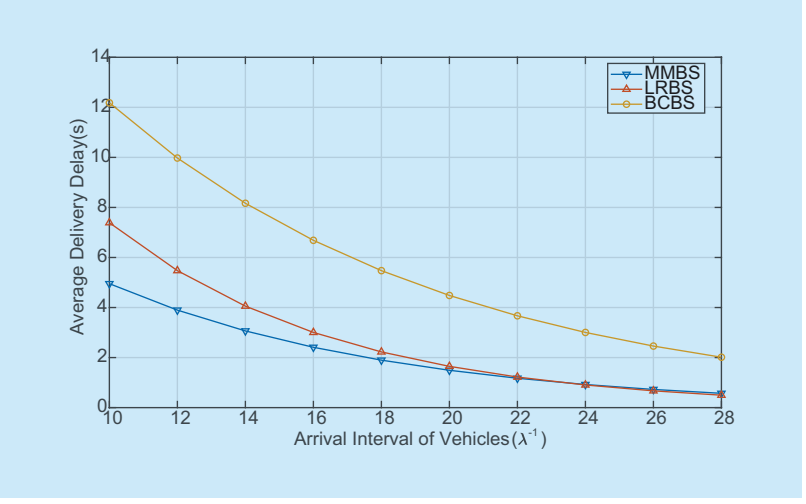

Fig. 4. *Average delivery delay with different arrival interval of vehicles.*

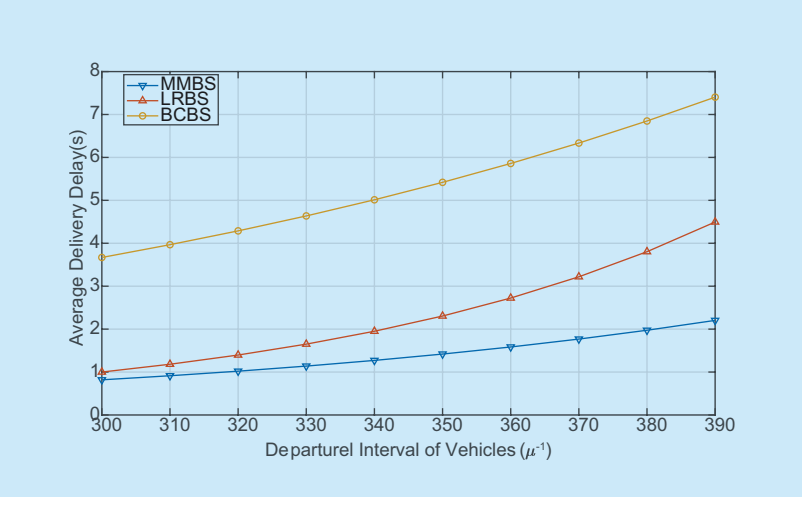

Fig. 5. *Average delivery delay with different departure interval of vehicles.*

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

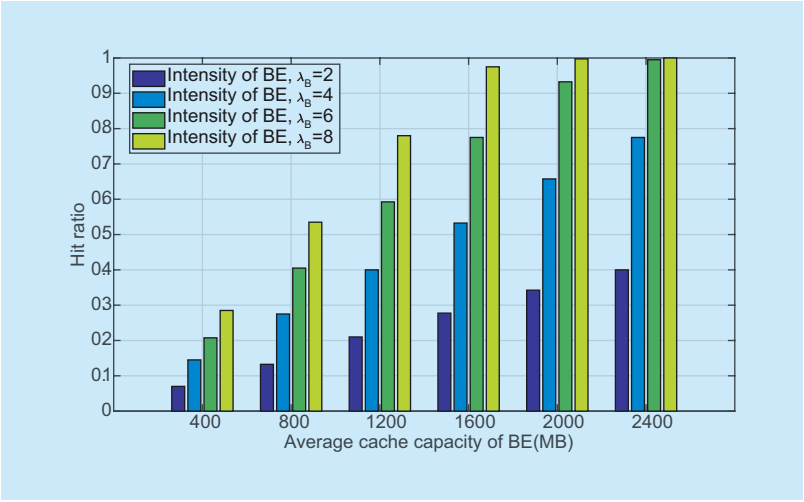

Fig. 6. *Hit ratio with different cache capacity of Blockchain edge nodes.*

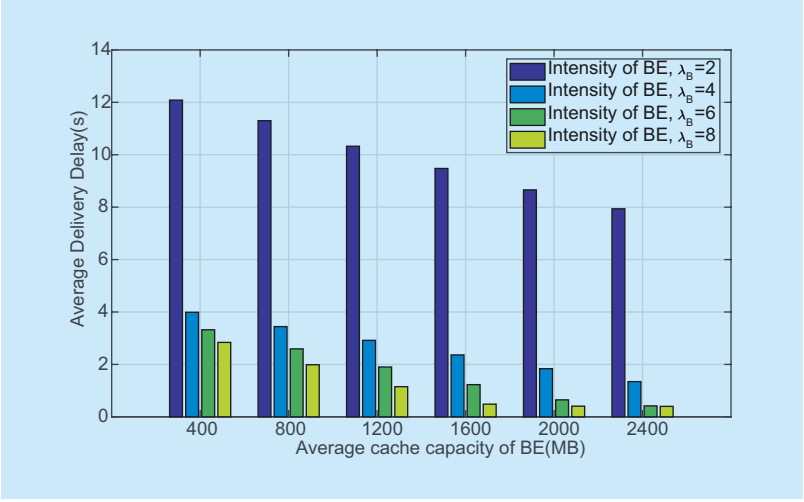

Fig. 7. *Average delivery delay with different cache capacity of Blockchain edge nodes.*

until it comes near to 1. With more edge nodes deployed in system, the system caching capacity can be enhanced to supply low-latency services for vehicles. Additionly, collaborative sharing between nodes will occure more frequently.

On the contrary, average delivery delay declines constantly when caching capacity or amount of nodes increase as figure 7 shows. If caching capacity improves, vehicles can cache device information in connected edge node and fetch authority from it directly. By this way, transmission latency is reduced and utimately keeps unchanged when all vehicles can cache information in connected nodes.

VI. Conclusion and Future Work}

To achieve fast authentication for vehicles and collaborative sharing among vehicular networks, a distributed trust access authentication system is proposed based on Blockchain network and edge computing in this article. Therefore, a hierarchical architecture is established consist of vehicular network layer, Blockchain edge layer and Blockchain network layer. Additionally, an authentication mechanism ensures data confidentiality, integrity and accessibility in communicating between vehicles and edge nodes, relying on the Blockchain network and digital signature algorithm. Furthermore, to avoid heavy burden for Blockchain network and optimize transmission latency, we propose a caching scheme based on many-to-many matching algorithm which can realize cooperation between nodes and adjust caching strategy efficiently by taking vehicle amounts and network caching condition into account. Simulation results prove that the proposed caching scheme has a higher hit ratio and lower delivery latency than other caching schemes on the basis of security.

In future work, we will apply this mechanism to various scenarios of IIoT to promote cooperation among IIoT platforms, and further optimize performance and accessibility.

Acknowledgment

This work was support by Research on Key Technologies of Dynamically Secure Identity Authentication and Risk Control of Power Business in the Science and Technology Project of State Grid Electric Power Company (No. 5204XA19003F) and National Natural Science Foundation of China (Grant No. 601702048).

References

[1] Zhaofeng M, , Weihua H, Wei B, et al."A Master-Slave Blockchain Paradigm and Application in Digital Rights Management." [J] *China Communications*, vol.15, no.8, 2018, pp.174-188.

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

[2] Nakamoto S. "Bitcoin: a peer-to-peer electronic cash system [Online]," available: https://bitcoin.org/bitcoin.pdf, 2009.
[3] Yang Z, Zheng K, Yang K, et al. "A blockchain-based reputation system for data credibility assessment in vehicular networks[C]." IEEE, *International Symposium on Personal, Indoor, and Mobile Radio Communications*, IEEE, 2018, pp. 1-5.
[4] Lamberti F, Gatteschi V, Demartini C, et al. "Blockchains Can Work for Car Insurance: Using Smart Contracts and Sensors to Provide On-Demand Coverage[J]." *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, 2018, pp. 72-81.
[5] M. P, Kos A, and Sedlar U. "Blockchain Based Autonomous Selection of Electric Vehicle Charging Station[C]." *International Conference on Identification, Information and Knowledge in the Internet of Things*, IEEE, 2018, pp. 217-222.
[6] Zhou S, Hui Y, Xu Q, et al. "An Edge Caching Scheme to Distribute Content in Vehicular Networks[J]." *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, 2018, pp. 5346-5356.
[7] Guiyang L, Quan Y, Haibo Z, et al. "Cooperative Vehicular Content Distribution in Edge Computing Assisted 5G-VANET." [J] *China Communications*, vol.15, no.7,2018, pp.1-17.
[8] Xuxia Z, Ying W, Xuesong Q. "Service Function Chain Orchestration across Multiple Clouds." [J] *China Communications*, vol.15, no.10, 2018, pp.99-116.
[9] Pan Z, Lei F, Peng Y, et al. "A Fairness Resource Allocation Algorithm for Coverage and Capacity Optimization in Wireless Self-Organized Network. [J] *China Communications*, vol.15, no.11, 2018, pp.10-24.
[10] Zhang K, Mao Y, Leng S, et al. "Optimal delay constrained offloading for vehicular edge computing networks[C]." *IEEE International Conference on Communications*, IEEE, 2017, pp. 21-25.
[11] Feng W, Sixuan C, Weixia Z. "A greedy algorithm for task offloading in Mobile Edge Computing system." [J] *China Communications*, vol.15, no.11, 2018, pp.149-157.
[12] Ahmet Cihat Baktir, Atay Ozgovde, and Cem Ersoy. "How Can Edge Computing Benefit from Software-Defined Networking: A Survey, Use Cases and Future Directions." *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, 2017, pp. 2359-2391.
[13] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung and M. Song, "Computation Offloading and Content Caching in Wireless Blockchain Networks With Mobile Edge Computing," in IEEE Transactions on Vehicular Technology, vol. 67, no. 11, 2018, pp. 11008-11021.
[14] P. K. Sharma, M. Chen and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," in IEEE Access, vol. 6, 2018, pp. 115-124.
[15] Z. Xiong, Y. Zhang, D. Niyato, P. Wang and Z. Han, "When Mobile Blockchain Meets Edge Computing," in IEEE Communications Magazine, vol. 56, no. 8, 2018, pp. 33-39.
[16] F. Lombardi, L. Aniello, S. De Angelis, et al, "A Blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, 2018, pp. 1-6.
[17] Biswas K, Muthukkumarasamy V. "Securing Smart Cities Using Blockchain Technology[C]." *2016 IEEE 18th International Conference on High Performance Computing and Communications*, IEEE, 2016.
[18] Dhillon H S, Ganti R K, Baccelli F, et al. "Modeling and Analysis of K-Tier Downlink Heterogeneous Cellular Networks[J]." *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 3, 2018, pp. 550-560.
[19] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts forthe Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016.
[20] Jin H, He D, Chen J. "An Identity Based Digital Signature from ECDSA[C]" *Second International Workshop on Education Technology and Computer Science*, IEEE, 2010, pp. 627-630.
[21] H.-S. Jo, Y. J. Sang, P. Xia, et al. "Heterogeneous cellular networks with flexible cell association: A comprehensive downlink SINR analysis," *IEEE Trans. Wireless Communication*, vol. 11, no. 10, 2012, pp. 3484-3495.
[22] Gu L, Zeng D, Guo S, et al. "Leverage parking terminals in a two-tier data center[C]." Wireless Communications and NETWORKING Conference. IEEE, 2013, pp. 4665-4670.
[23] Echenique, Federico and Oviedo, Jorge, A Theory of Stability in Many-to-Many Matching Markets (October 2004). Caltech SS Working Paper No. 1185. Available at SSRN: https://ssrn.com/abstract=691443 or http://dx.doi.org/10.2139/ssrn.691443.
[24] Varshney G, Gupta H. "A security framework for IOT devices against wireless threats[C]". *International Conference on Telecommunication and Networks*, 2017, pp. 1-6.

Biographies

Shaoyong Guo, is with the department of State Key Laboratory of Networking and Switching Technology, and received Ph.D. degree at Beijing University of Posts and Telecommunication. His main contribution about Blockchain and IoT is taking the lead to declare ITU- standard: Decentralized IoT communication architecture based on Information Centric Networking and Blockchain in ITU-T

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.

SG20 2018 and undertake State Grid project Application Research of Blockchain Technology in Energy Internet. Email: syguo@bupt.edu.cn.

Xing Hu, was born in Hunan, China, in 1997. She received B.Eng. degree at Beijing University of Posts and Telecommunication. And she is currently pursuing her MA.Sc. degree in the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications. Her main research interest lies in edge computing and Blockchain. Email: xinghu@bupt.edu.cn.

Ziqiang Zhou, graduated at Institute of Energy and Environment, Southeast University, Nanjing. He works at State Grid Zhejiang Electric Power Co., Ltd. Institute of Electric Power Science. His current research interests include blockchain, artificial intelligence, and power system. Email: jx_zzq@sina.com.

Xinyan Wang, received the B.Eng.Degree in communication engineering from Huazhong University of Science and Technology. She works at the State Grid Henan Electric Power Company Information and Communication Company. Her current research interests include information and communication technology, electrical engineering automation. Main results: the practice of grid enterprise information operation and maintenance mode in the context of cloud computing; Dynamic Secure Sharing of Cloud Aduit Data Based on Blockchain Technology. Email: pinzhe0326@163.com.

Feng Qi, is a Professor of Beijing University of Posts and Telecommunications, engaged in scientific research, teaching, and standardization research in information and communications. His research interests include communications software, network management, and business intelligence. He has won 2 National Science and Technology Progress Awards. He has also written more than 10 ITU-T international standards and Industry Standards. Served as vice chairman of the ITU-T Study Group 4 and Study Group 12.

Lifang Gao, graduated at Harbin Institute of Technology and received her master degree at North China Electric Power University. She works at State Grid Hebei Electric Company, Information and Communication Company. Her main researches is in the information system operation and maintenance. Email: manyupiaoling@126.com.

Authorized licensed use limited to: SHANDONG UNIVERSITY. Downloaded on May 03,2020 at 05:39:00 UTC from IEEE Xplore. Restrictions apply.