Received 26 December 2019; revised 23 January 2020; accepted 31 January 2020. Date of publication 26 February 2020; date of current version 9 March 2020.

Digital Object Identifier 10.1109/OJCOMS.2020.2972742

A Sidechain-Based Decentralized Authentication Scheme via Optimized Two-Way Peg Protocol for Smart Community

MIN LI[1] (Student Member, IEEE), HELEN TANG[2] (Senior Member, IEEE), AHMED REFAEY HUSSEIN[1,3] (Senior Member, IEEE), AND XIANBIN WANG[1] (Fellow, IEEE)

[1]Electrical and Computer Engineering Department, Western University, London, ON N6A 3K7, Canada
[2]Centre for Security Science, Defence Research and Development Canada, Ottawa, ON, Canada
[3]Electrical and Computer Engineering Department, Manhattan College, Riverdale, NY 10471, USA

CORRESPONDING AUTHOR: X. Wang (e-mail: xianbin.wang@uwo.ca)

ABSTRACT In this work, we propose a novel sidechain structure via an optimized two-way peg protocol for device authentication in the smart community in order to overcome the limitations of existing approaches. The proposed scheme uses private side blockchains to distribute and manage the local registration and authentication processes, in addition to a local mainchain block to circulate the information record with other smart systems. More importantly, we propose the optimized two-way peg protocol in the proposed sidechain system in order to prevent the worthless information injection attack during the authentication information sharing procedure between the main chain and side blockchains. The optimized two-way peg protocol supervises the availability of the required information by dynamically evaluating the trustworthiness of each smart device. The evaluation is based on numerous criteria, such as the authentication method, previous authentication information sharing history, and local authentication results. Consequently, the simulation results prove the superiority of the proposed scheme in terms of reducing authentication time, improving information management efficiency and decreasing storage consumption as compared to existing works, and the applicability and feasibility of the optimized two-way peg protocol have been approved. It is noteworthy that the proposed sidechain-based method shows its superiority in reducing the cost of authentication time compared with the blockchain-based method when using blockchain structure. The reflected savings are 33.33%, 34.29%, and 36.36% when in comparison to the conventional authentication process without applying any additional method, the authentication process using the proposed sidechain based method, and the authentication process using the blockchain based method, respectively.

INDEX TERMS Smart community, blockchain, information sharing, device authentication, sidechain, two-way peg protocol.

I. INTRODUCTION

WITH the exponential growth of the Internet of Things (IoTs), it is expected to comprise 18 billion connected smart devices by 2022 [1]. In fact, with this rapid expansion, new security challenges have emerged. Precisely, in the new generation of IoT's Edge-Devices (EDs), the authentication process for each device is vital for protecting the security of personal data of each user [2]. Otherwise, it will result in numerous potential security risks such as information stealing, data tampering, and identity usurpation [3].

A smart community is a virtual environment composed of different IoT systems, such as smart homes, smart health, and smart public buildings [4]. Personal data are collected and processed in each system by smart devices, and then get shared among the community in order to improve community safety, home security, healthcare quality,

and emergency response abilities [5], [6]. However, both the device authentication process in each smart system and the information-sharing process within sub-systems are the major obstacles for privacy protection in the smart community due to imperfect mechanisms and the resource-constrained nature of IoT devices [7]. Indeed there is a wide range of attacks threatening the smart community. Whereas the main focus in this work on the authentication, the interested reader can refer to [8] for more details on the security attacks.

Current device authentication approaches still follow the centralized model and suffer from numerous challenges when they are applied in a smart community, such as poor authentication efficiency, inflexible authentication approaches, and an insecure information sharing service [6], [9], [10]. Although decentralized smart community models were proposed to prevent the shortcomings caused by centralized models, lacking inside consensus mechanism among internal decentralized service providers will lead to malicious attacks, and further threaten the data security [11].

By reaching a decentralized consensus mechanism at each smart system, a blockchain-based method has been viewed as a promising solution for solving these issues [12]. Through establishing a blockchain at each gateway in smart systems, the method distributively manages the local device authentication process and realizes the authentication information sharing function among smart systems. However, the blockchain-based method still has several limitations and challenges, which are summarized as follows:

- *Poor local device authentication efficiency:* Each smart system still relies on the gateway device to handle the device authentication process. With the number of IoT devices increasing, the burden of the gateway will increase significantly and the system will undergo bottleneck communications and large processing latencies, which limit the system Quality of Service (QoS) performance [13], [14]. Moreover, the blockchain-based method enormously increases the complexity of searching authentication information by sharing authentication information of the whole community with each system, and it could limit the authentication efficiency at the gateway device.
- *Large storage burden:* Since all the blockchain entities share the same authentication information from the community, the gateway device of each smart system not only needs to save information from its own system but also the information from rest of smart systems in the community. The requirement of the blockchain-based method for storage capacity could exceed the capacity limit of the constrained IoT gateway device [15].
- *Insecure information sharing mechanism:* It is normal in the smart community to have some IoT devices with mobility features, such as drones and community service robots [16]. In this case, the authentication information should be allowed to be shared with other sub-systems. The blockchain-based method involves a shared decentralized database to realize this function. However, if the target device has already been attacked to become a malicious one, sharing its authentication information with other systems will threaten the information security of other systems by giving the direct writing and reading authorities to the malicious device.

Sidechain, as an expended technology of blockchain, can provide a decentralized peer-to-peer platform to maintain the saved data while securely transferring key information between different systems [17]. In this paper, we propose a novel sidechain structure with an optimized two-way peg protocol for device authentication in the smart community in order to overcome the above-mentioned challenges caused by a blockchain-based method. The proposed model utilizes a public mainchain as a reference chain to keep a local device information record, and private side blockchains to manage the local device authentication process in each system. We also come up with the optimized two-way peg protocol for sidechain system. The optimized two-way peg protocol guarantees a secured information sharing procedure between the mainchain and side blockchains by dynamically evaluating the trustworthy of the target device. Both PoW consensus mechanism and Simplified Payment Verification (SPV) proof have been reached as for blocks generation and efficient information tracking purposes [18], [19].

The contribution of this paper is twofold. Firstly, we propose an optimized sidechain structure for device authentication in the IoT smart community. Instead of downloading and updating the entire mainchain after each block generation process as traditional sidechain technology, the proposed structure saves a reference mainchain block at local memory and use SPV proof to prove the existence of the information. The proposed structure consumes less storage consumption and gets more efficient when searching for the target information. Secondly, in order to protect the smart community from the worthless information injection attack and ensure the normal operation of sidechain technology in the IoT environment, an optimized two-way peg protocol has been proposed based on dynamically analyzing the trust value of the target device.

The rest of this paper is organized as follows. Section II briefly introduces the technical details of the sidechain technology and gives an overview of related works. In Section III, the proposed decentralized sidechain-based authentication scheme with an optimized two-way peg protocol is demonstrated. In Section IV, the simulation results are presented. Finally, the paper is concluded in Section V.

II. RELATED WORK

A. SIDECHAIN TECHNOLOGY

Sidechain was firstly defined for enabling bitcoin and other cryptocurrencies to transfer money among multiple blockchains [18]. The structure of sidechain consists of a mainchain with multiple side blockchains, as shown in Fig. 1. Both mainchain and side blockchains flow the basic structure of blockchain technology, including the block structure, PoW consensus mechanism, and new block generation procedure.

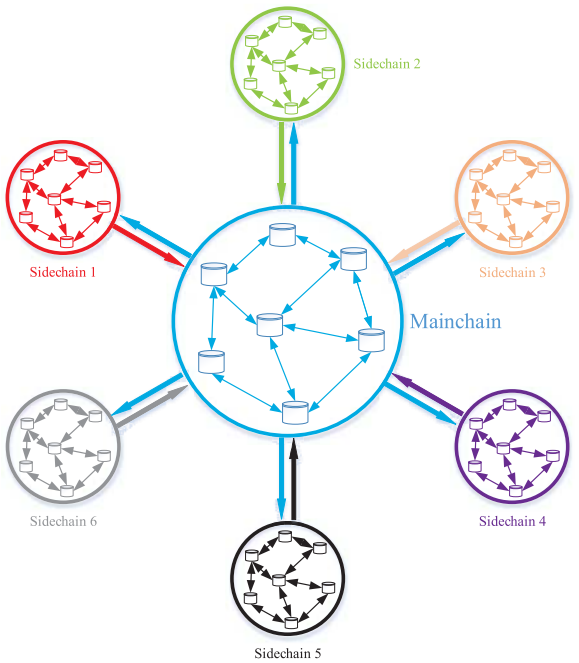

FIGURE 1. Structure of sidechain technology.

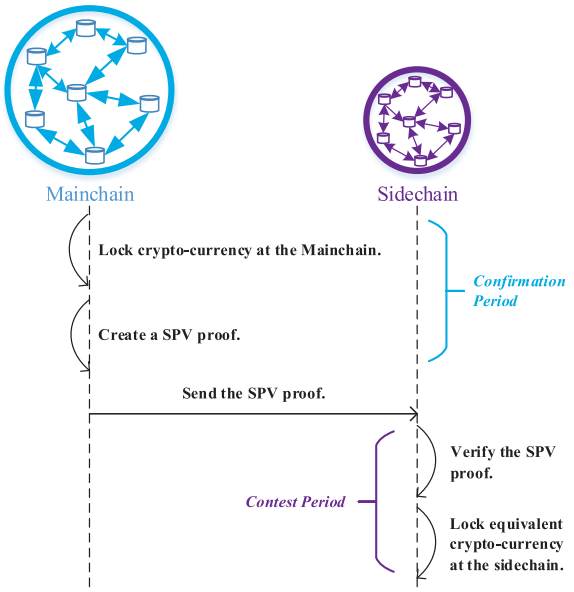

FIGURE 2. Procedure of the two-way peg protocol in sidechain technology.

In order to share information among mainchain and side blockchains, a two-way peg protocol has been applied [20]. The main functions of sidechain are allowing the key information to transfer from one chain to others, and reducing the burden of the mainchain, which help the system to gain both agility and freedom of using multiple networks [21].

B. SPV PROOF AND TWO-WAY PEG PROTOCOL

Simplified Payment Verification (SPV) proof has been reached at both sides to prove that the required crypto-currency has been locked at a certain address [22]. Since the SPV proof only requires to download the block headers instead of the whole blockchain, it can provide an efficient tracking service in the sidechain systems [18].

Fig. 2 presents the traditional two-way peg protocol when mainchain needs to transfer crypto-currencies to a side blockchain. The coins of the mainchain will be firstly locked in a specific address and an SPV proof will be generated. The proof will then be sent to the side blockchain and got verified. Based on the verification result, the corresponding crypto-currencies will be decided to unlock in the side blockchain. To synchronize these two chains, two waiting periods are defined, which are Confirmation Period and Contest Period [18].

It should be noted that there is a certain risk in sidechain technology that side blockchains keep sharing worthless information with the mainchain in order to disturb system operation. This attack will cause a constant increase in the system load, while the existing two-way peg cannot detect this attack [18]. If a mining node of side blockchain has been compromised and performed worthless information injection attack by uploading authentication information of malicious devices to the mainchain system, the security of the smart community will be seriously affected. Therefore, an optimized two-way peg protocol with information evaluation scheme is strongly needed in order to apply sidechain technology into the smart community scenario.

C. RELATED SOLUTIONS

The typical smart community structure is usually composed of several smart sub-systems that provide direct interaction with users by IoT end devices. In these sub-systems, gateways are usually responsible for the local device authentication processes. However, the bottleneck communication could be caused when the number of IoT devices increases. The central information sharing sever usually has high computational powers to handle all the information from the smart community, and then it shows high efficiency in processing the data exchange and data analysis. However, the traditional centralized model could make the system under the risk of one-point failure [9]. If the center has been compromised, the security of personal data is threatened.

A blockchain-based method proposed in [12] has been viewed as an alternative solution for solving these issues. By establishing the blockchain at the gateway level in each smart system, the proposed method distributively manages device authentication and realize the information sharing purpose. However, the local device authentication in each sub smart system is still centrally managed by gateway, and a full blockchain is required to download at the gateway for information sharing, which seriously affects the system security and management efficiency. Moreover, the centralized nature of gateway has a risk of one-point failure, which limits its application in the smart community due to the stringent QoS requirement [23].

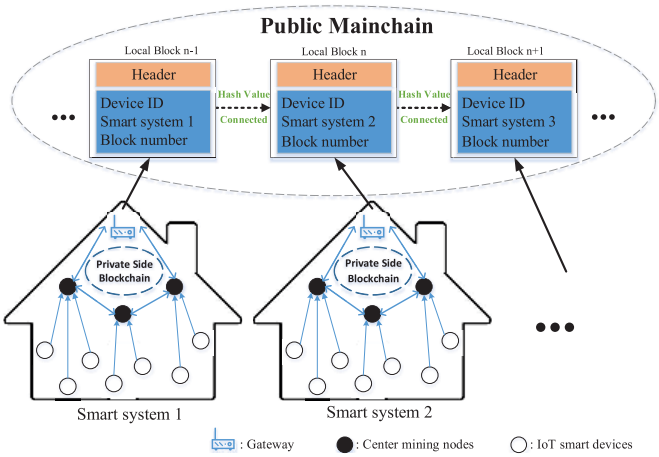

FIGURE 3. Proposed sidechain-based authentication model.

A sidechain-based routing protection scheme was proposed in order to improve the resistance abilities for the Garlic Routing and Onion Routing frameworks to privacy attacks [24]. With the proposed Garlic Onion Routing technique, the sidechain protected the routing process from inaccurate information uploading and data tampering. However, for the sidechain protocol, the proposed work still followed the traditional two-way peg protocol and it has long communication delay, which is not appropriate for routing privacy protection.

III. SIDECHAIN-BASED AUTHENTICATION SCHEME WITH OPTIMIZED TWO-WAY PEG PROTOCOL

Fig. 3 presents the proposed sidechain-based authentication model in a smart community, which is composed of a public blockchain as a mainchain and private blockchains as side blockchains [25], [26]. To illustrate the model, we use two smart home cases to represent the IoT smart systems. In each smart system, central mining nodes are chosen among local smart devices based on their computational abilities and locations. The private blockchain is built among the central mining nodes and gateway in order to securely manage the authentication processes with the distributed PoW consensus mechanism. Among all the gateways in this smart community, a public mainchain is employed to securely manage the authentication information sharing process by implementing the optimized two-way peg protocol. In order to reduce the storage consumption at the gateway level, each mainchain block will only be saved at local gateway after the verification process without updating an entire mainchain.

A. LOCAL AUTHENTICATION PROCEDURE AT PRIVATE SIDE BLOCK-CHAINS

1) REGISTRATION PROCESS

When a new IoT device is firstly added to a smart system, the device should be registered by the corresponding private side blockchain in this system.

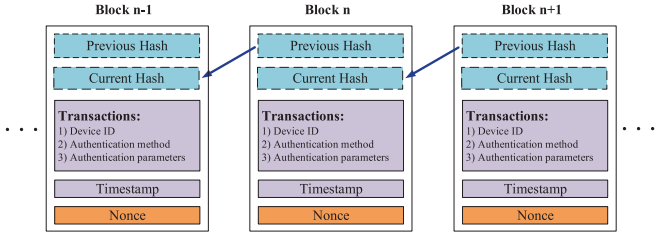

FIGURE 4. Structure and content of the private side blockchain.

Firstly, the device sends its ID to the gateway, and its ID will be searched in the public mainchain to see if it is newly registered. If there is previous authentication information existed in other smart systems, the gateway will send a request to the public mainchain for the authentication information sharing process. Otherwise, the local registration process will start.

The local registration process is achieved by creating a new block into the private side blockchain. As shown in Fig. 4, the block consists of the header information (previous hash and current hash, timestamp and nonce value) and transactions. By adopting the PoW consensus mechanism, the authentication information of a device will be distributively saved as three transactions into the block, which contains the following components: (1) device ID; (2) authentication method; (3) corresponding authentication keys or parameters. The authentication method can be various based on the devices' computational powers and usage scenarios. Except for the device ID for the tracking purpose, all transactions are encrypted by using Secure Hash Algorithm (SHA) 256 with the device's private key [23].

When a new device has been successfully registered, the devices ID and its block number will be uploaded along with the corresponding smart system ID to the public mainchain to form a reference records for the authentication information sharing procedure.

2) AUTHENTICATION PROCESS

When a smart device wants to establish a communication session within the smart system for data uploading or downloading after the registration process, the authentication process will be required.

Fig. 5 displays the procedure of the proposed authentication process. First, a request that contains the device's ID and authentication parameters will be sent to the nearest central mining node. Secondly, the central mining node downloads the corresponding block from the private side blockchain relying on the device ID. Then, after decrypting the block with the public key of the device, the central mining node will compare the decrypted authentication parameters with the received parameters. Finally, a response will be sent to the device to inform whether it is successfully authenticated.

Since the device authentication process is achieved at the nearest central mining node instead of the gateway device, the communication burden of the gateway has been

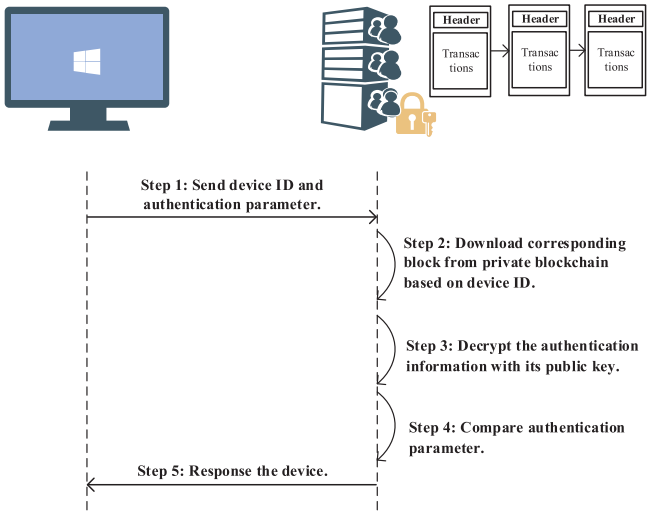

FIGURE 5. Procedure of the proposed authentication process at private side blockchain.

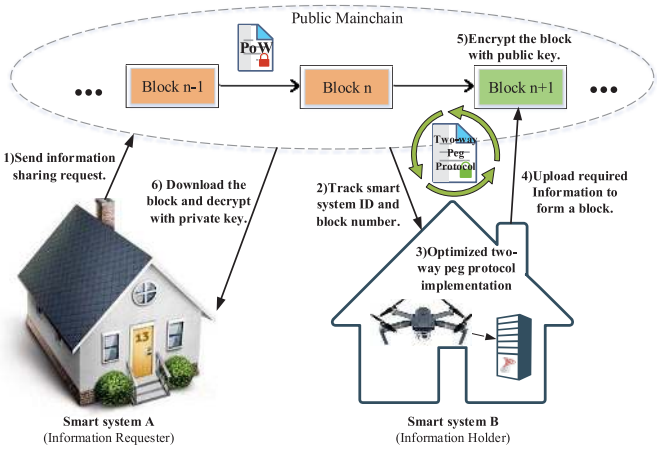

FIGURE 6. Model of authentication information sharing at the public mainchain. Both PoW consensus mechanism and the proposed optimized two-way peg protocol have been applied for safe operation of the proposed sidechain-based smart community system.

significantly decreased. In general, the blockchain framework adopts a zero-trust architecture by authenticating and verifying a nodes for every transaction. Therefore, it can address the potential lateral threat model often found in such environments.

B. AUTHENTICATION INFORMATION SHARING AT PUBLIC MAINCHAIN

The IoT device with mobility features can move from one smart system to another system, such as drones and community service robots. If this device requires to get access to the data in the new system, it should be authenticated by the system. However, if there is no previous authentication information block existed in the system (side blockchains), the device would be required to repeatedly register in the new system, which will cost large amounts of energy and time. Therefore, authentication information should be able to be shared within a smart community.

Although a device can be successfully registered by one system, it still has a risk of being compromised later on to become a malicious device, and its authentication information can no longer be used by other systems. The original two-way peg protocol is designed to defend the financial sidechain systems from a unique business attack which is a double-spending attack, but it cannot prevent the risk in our presented scenario. Thus, we propose an optimized two-way peg protocol to guarantee the trustworthy of the shared information in the information sharing procedure by dynamically calculating the trust value of the target device. Fig. 6 demonstrates the procedure of the proposed authentication information sharing procedure guaranteed by the optimized two-way peg protocol. The procedure mainly consists of the 4 steps as follows:

1) INFORMATION SOURCE TRACKING

When an IoT device firstly registers in a smart system, the corresponding gateway will send a tracking request along with the device ID to the mainchain in order to check if there is previous authentication information of this device. When the public mainchain receives the request from the information requester (smart system A), the corresponding block that contains the information resources (including smart system ID and block number) will be tracked based on the device ID.

2) SPV PROOF COLLECTION

For those smart systems with the required information, an SPV proof (device ID, device ID list, block header list) is required to send to smart system A in order to prove the existence of the target information without downloading the full chain. Then, the gateway of smart system A will do the SPV verification. However, offloading the SPV verification task to a single node (gateway) is a security concern for the smart system since a malicious gateway could deceive the system by responding with adulterated outcomes. Therefore, the local center mining nodes will be required to handle the verification voting process with the local gateway. Only more than half of them successfully verify the SPV proof will the result be proved.

3) TRUSTWORTHY EVALUATION

Based on the SPV proofs, the current trust value of this device will be calculated and get compared with the trust threshold of the smart system A. Only when the gateway provides the positive result will the information be shared with the information requester. Otherwise, the device will be reported to be manually registered in order to protect the security of the smart community.

For the trust value calculation rule, we mainly consider three aspects a device: authentication method evaluation,

information sharing history evaluation, and authentication process evaluation. We set the whole range of trust value in [0-1], and each IoT smart system can have different acceptance threshold to filtrate the untrustworthy devices.

T_{meth} represents the trust value for using different authentication methods. The harder the authentication method is, the higher T_{meth} it gets. The reason is that we assume the harder authentication method can provide a higher security performance, and we set that each device can pick one authentication method depending on its computational powers and its usage scenario. For example, we set 0.4 for using PSK authentication method and 0.5 for using certificates authentication method [27], [28].

The following two equations express the calculation process for information sharing history evaluation and authentication process evaluation [29]:

$$T_{sharing} = \frac{\alpha_i}{N_{sys} * M_{thre}} \sum_{i=1}^{N_{use}} T_{thre}, \tag{1}$$

where $T_{sharing}(i)$ is the trust value of information sharing for this device. N_{sys} is the total number of IoT smart systems in this smart community. M_{thre} is the average trust threshold of the whole smart community. N_{use} is the number of smart systems that currently have the authentication information of this device. T_{thre} is the corresponding trust threshold of the smart system. α_i is decay factor.

$$T_{authen} = \beta \sum_{j=1}^{N_{succ}} T_{thre} - \gamma \sum_{k=1}^{N_{unsucc}} T_{thre}, \tag{2}$$

where $T_{authen}(i)$ is the trust value of authentication process for this device. N_{succ} is the total number of successful authentication process in the smart community, and N_{unsucc} is the total number of unsuccessful authentication process in this smart community. T_{thre} is the corresponding trust threshold of each smart system. Both β and γ are weight factors.

By combining these three trust value components, the trustworthy of a device can be dynamically calculated as in equation (3) [30].

$$T_d = \lambda * T_{meth} + \mu * T_{sharing} + \nu * T_{authen}, \tag{3}$$

where T_{meth}, $T_{sharing}$ and T_{authen} are in [0-1]. λ, μ and ν are weight factors, and $\lambda + \mu + \nu = 1$.

4) INFORMATION SHARING PROCEDURE

When the trust value of this device meets the threshold of the smart system requester, the required authentication information will be allowed to get shared. The decrypted required information will be uploaded to the public mainchain from the nearest information holder (smart system B) to form a new block by using the PoW consensus mechanism. Then, the information will be encrypted with the public key of smart system A by using Elliptic Curve Cryptography (ECC), so that only the information requester with its own private key can read and download the content of the block [32]. It should be noted that the optimized two-way peg protocol presented in this paper could also be employed in other sidechain-based IoT systems to ensure the trustworthy of the required information.

The logic of the proposed authentication sharing procedure has been summarized in Algorithm 1, and the notations used in Algorithm 1 have been listed in Table 1.

TABLE 1. Notations used in Algorithm 1.

Notation	Description
N_{Sys}	Number of smart systems
SPV_i	SPV proof
N_{SPV}	Number of SPV proofs received
T_{meth}	Trust value of authentication method
$T_{thre}(i)$	Trust threshold of the smart system
$N_{succ}(i)$	Total number of successful authentication
$N_{unsucc}(i)$	Total number of unsuccessful authentication
Encr_{Info}	The target message after encryption
Tar_{info}	The message that required to be shared
$\text{Key}_{pub}(A)$	The public key of smart system A
$\text{Key}_{pri}(A)$	The private key of smart system A

TABLE 2. Environment features of authentication process.

CPU Processor	Operating System	CPU Max Speed	Computing Environment
x64	64-bit Microsoft Windows 10	2.6 GHz	Matlab

IV. SIMULATION EXPERIMENT AND RESULT ANALYSIS

In this section, we evaluate the proposed sidechain-based device authentication scheme in terms of the authentication time consumption, the optimized two-way peg protocol performance, information management efficiency and storage consumption.

A. PERFORMANCE ANALYSIS OF THE AUTHENTICATION TIME CONSUMPTION RESULTS

As previously mentioned in Section I, a blockchain-based method has been proposed to distributively manage the local authentication process and information sharing process [12]. The authentication information has been viewed as a transaction saved in the blockchain and can be shared within the community. However, this structure increases the burden of gateways by treating them as central devices to handle the local authentication procedure and saving authentication information from other systems. In this experiment, we compare the proposed sidechain-based method with the blockchain-based method and conventional authentication without any additional method in terms of authentication time consumption. We simulate the device authentication process between a gateway that hosts the blockchain/sidechain and a smart device in MATLAB. Table 2 describes the environment features of the simulation.

We test the authentication time consumption by comparing these three methods: (1) the conventional authentication

Algorithm 1 Pseudo Code of Authentication Information Sharing Procedure at Public Mainchain

***Information Tracking and SPV Proof Collection*:**

if system A requests authentication information sharing **then**
  System A uploads device ID to mainchain
end if
for $i = 1;\ i < N_{\text{Sys}};\ i++$ **do**
  Search device ID in side blockchain
  if device ID existed **then**
    Create SPV_i and reply
  else
    Discard
  end if
end for

***Trustworthy Evaluation*:**

for $i = 1;\ i < N_{\text{SPV}};\ i++$ **do**
  Get(T_{meth})
  Get($T_{thre}(i)$)
  Get($N_{succ}(i)$, and $N_{unsucc}(i)$)
end for
$T_{shar} \leftarrow \frac{\alpha_j}{N_{sys} \cdot M_{thre}} \sum_{j=1}^{N_{use}} T_{thre}$
$T_{authen} \leftarrow \beta \sum_{j=1}^{N_{succ}} T_{thre} - \gamma \sum_{k=1}^{N_{unsucc}} T_{thre}$
$T_d \leftarrow \lambda \cdot T_{meth} + \mu \cdot T_{shar} + \nu \cdot T_{authen}$

***Information Sharing Procedure*:**

if $(T_d > T_{thre}(A))$ **then**
  $\text{Encr}_{Info} \leftarrow ECC(\text{Tar}_{info}, \text{Key}_{pub}(A))$
  Create a mainchain block with Encr_{Info}
  System A download the block from mainchain
  $\text{Tar}_{Info} \leftarrow ECC(\text{Encr}_{Info}, \text{Key}_{pri}(A))$
else
  Require to register manually
end if
end algorithm

process without applying any additional method; (2) the authentication process with using the proposed sidechain-based method; (3) the authentication process with using the blockchain-based method. We use PSK as the authentication method for this experiment. The experimental results are averaged over 30 runs.

1) AUTHENTICATION TIME CONSUMPTION AGAINST PSK CHARACTER LENGTHS

For the first test, we evaluate the effect of PSK character lengths to authentication time consumption. We simulate a smart community with 10 smart systems and each system has 10 smart devices. Fig. 7 presents the authentication time comparison results of using three abovementioned methods with different PSK character lengths. Although the conventional method without any additional method realizes the lowest authentication time among three methods, it has the lowest functionality and security enhancement performance.

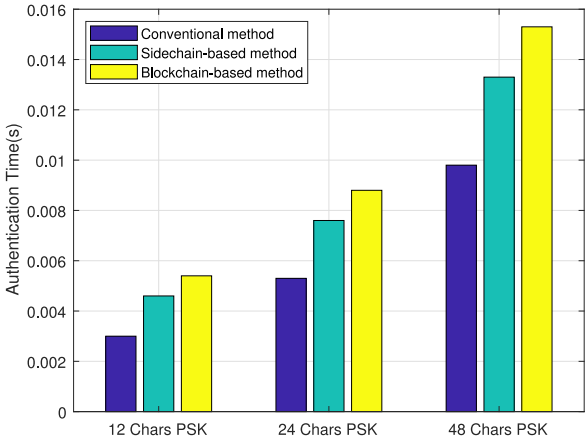

FIGURE 7. Authentication time comparison among the conventional method, the proposed sidechain-based method and the blockchain-based method.

For 12 chars PSK, the authentication time for the blockchain-based method is 0.0054 seconds, and 0.0046 seconds for the proposed sidechain-based method. With increasing the number of characters in PSK, the average authentication times for the conventional method, the proposed sidechain-based method and blockchain-based method are respectively 1) 0.0053 seconds, 0.0076 seconds and 0.0088 seconds when PSK has 24 characters; 2) 0.0098 seconds, 0.0133 seconds and 0.0153 seconds when PSK has 24 characters.

As we can observe from that the proposed sidechain-based method shows its superiority in reducing authentication time compared with the blockchain-based method, with saving 33.33%, 34.29% and 36.36% of the additional cost on authentication time caused by using blockchain structure for these three cases. As the character length of PSK increases, the proposed sidechain-based method shows more advantages in decreasing authentication time compared with the method in [12]. The reason is that the complexity of searching the target device ID in the block has increased with the number of PSK increases. With using the proposed sidechain, the offload of public mainchain could be noticeably reduced compared with the existing blockchain-based method.

2) AUTHENTICATION TIME CONSUMPTION AGAINST BLOCKCHAIN PARAMETERS

Considering the position of the block that owns the authentication parameters and the blockchain length may induce an additional time cost, we focus on analyzing the influence of blockchain parameters to the authentication time results in the second test.

We simulate the blockchain/sidechain with 100 blocks and 200 blocks, and use 12 chars PSK as the authentication method for this experiment. We compare three block positions for each block length scenario: (1) the authentication parameters are in the first block of the blockchain, presented as B_F; (2) the authentication parameters are in the middle block of the blockchain, presented as B_M; and

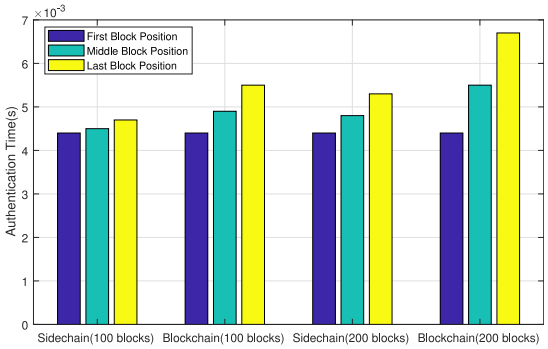

FIGURE 8. Authentication time comparison of three block positions with different blockchain lengths.

(3) the authentication parameters are in the last block of the blockchain, B_E.

Fig. 8 exhibits the authentication time comparison results of three abovementioned block positions with different blockchain lengths. For the 100 block length scenario, the authentication times for the blockchain-based model are 0.0044 seconds, 0.0049 seconds and 0.0055 seconds, respectively for the scenarios B_F, B_M and B_E. Whereas, the authentication times for the proposed sidechain model are 0.0044 seconds, 0.0045 seconds and 0.0047, respectively for these three block positions. It can be concluded that the proposed sidechain-based authentication model could decrease the additional implementation time caused by block positions compared with the existing blockchain-based authentication model. Take B_E for 100 blocks as an example, it decreases 0.0008 seconds. which is 14.55% of the time consumption of the blockchain-based model. For the 200 block length scenario. the authentication time for the blockchain-based model is 0.0044 seconds, 0.0055 seconds and 0.0067 seconds for these three positions, while 0.0044 seconds, 0.0048 seconds and 0.0053 seconds for the sidechain-based model. Therefore, as the number of block increase, the proposed sidechain model show its benefit in reducing the complexity of information searching compared with blockchain model.

B. PERFORMANCE ANALYSIS OF THE PROPOSED OPTIMIZED TWO-WAY PEG PROTOCOL

In this subsection, we evaluate the proposed optimized two-way peg protocol in the simulated sidechain system. We simulate a smart community with 100 smart systems and record the trust value of smart devices with different malicious behavior percentage. In fact, the networking aspects of are beyond the scope of this paper, however, the interested reader can refer to [31]. The parameter configurations for testing the optimized two-way peg protocol are listed in Table 3. All the experimental results are averaged over 30 runs.

We use the certificates method as the authentication method to show the performance of the proposed protocol. In this experiment, we test the performance of the

TABLE 3. Parameter configurations for testing the proposed trust scheme.

	Number of Smart Systems (N_{sys})	Acceptance Trust Threshold (T_{thre})	Registered Systems (N_{succ})
Systems with Low Trust Threshold	60	[0.30-0.50]	10
Systems with High Trust Threshold	40	[0.50-0.70]	5

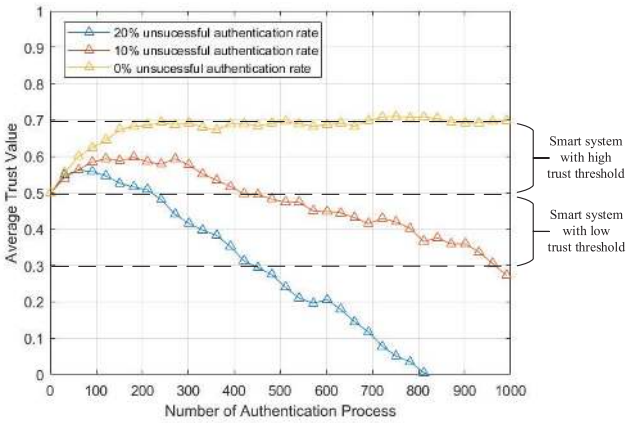

FIGURE 9. Performance evaluation for optimized two-way peg protocol with using certificates as the authentication method.

trust evaluation scheme with three malicious levels: 20% unsuccessful authentication rate, 10% unsuccessful authentication rate and 0% unsuccessful authentication. As shown in Fig. 9, the device with 0% unsuccessful authentication rate continuously gains trust values by its successful behaviors, and its average trust value increases steadily and slowly. Its authentication information can be allowed to be shared with other smart systems through the public main-chain as long as it can provide the proof that its trust value is higher than the trust threshold of a target smart system. As previously mentioned, the trust value of this device with no malicious behavior approximately stays 0.70, which can meet the requirements of most smart systems with a high trust threshold ([0.50-0.70]) and all the smart systems with low trust threshold ([0.30-0.50]). On the contrary, for the devices with 10% unsuccessful authentication rate, its trust value will decline continuously. After 412^{nd} authentication, its authentication information can no longer be shared in the smart systems with a high trust threshold. Then, after 964^{th} authentication, its information will not be allowed to be shared in the smart community. For the devices with 20% unsuccessful authentication rate, its trust value will decline sharply. Its authentication information cannot be shared with smart systems with a high trust threshold at 221^{st} authentication. After 438^{th} authentication, its information will not be allowed to be shared in the smart community.

When the trust value is less than the threshold of the target IoT system, the authentication information cannot be shared with other smart systems in order to protect the information security of the community.

TABLE 4. Parameter configurations for analyzing information management efficiency.

CPU Frequencies of Each Gateway	CPU Frequencies of Each Central Mining Nodes	Cycles per Byte	Block Size for Side Blockchain	Block Size for Mainchain
[2GHZ, 2.8GHZ]	[1GHZ, 2GHZ]	100	248	108

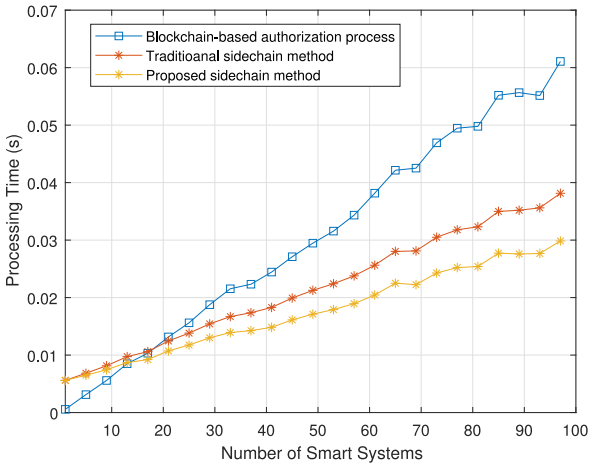

FIGURE 10. Information management efficiency comparison between the proposed sidechain-based method, traditional sidechain method and existing blockchain-based method.

C. PERFORMANCE ANALYSIS OF THE INFORMATION MANAGEMENT EFFICIENCY

Due to the low computational power of constrained IoT smart devices, one of the most important requirements for the proposed sidechain-based authentication method is to decrease the computational overhead caused by managing the authentication information at the gateway side. Thus, this subsection mainly demonstrates the comparison results between the proposed sidechain-based method, the traditional sidechain method and the blockchain-based method mentioned in terms of information management efficiency.

Since gateways and other IoT devices have different computational powers processing the transactions, we set different CPU frequencies for them in order to evaluate the authorization and authentication time [33]. As shown in Table 4, we assume that the block sizes for private side blockchain and public mainchain are respectively 248 bytes and 108 bytes. The CPU frequency for IoT center mining nodes and gateways are between [1GHz, 2GHz] and [2GHz, 2.8GHz], respectively.

Fig. 10 presents the information management efficiency comparison between the proposed sidechain-based method, the traditional sidechain method, and the existing blockchain-based method. We use the processing time consumption during the device registration phase as the criterion for this experiment. As we can observe from Fig. 10 that both sidechain methods have higher time consumption compared with the blockchain method when the number of smart systems in the IoT smart community is lower than 16. The reason is that the authorization time of the sidechain-based method consists of two folds: time for creating one local block in private side blockchain for saving the local authorization information and time for uploading a reference block to the public mainchain for sharing purpose. Thus, when the number of smart systems is low, the processing time for the proposed method would be high than the blockchain-based method, which only needs to store one blockchain in each gateway. However, with the number of smart systems increasing, the sidechain methods show their superiority in decreasing implementation costs. For instance, they save more than 37.33% and 49.12% respectively of processing time compared with the blockchain-based method when the number of smart systems reaches 100. Therefore, compared to the existing methods, our method could enhance information management efficiency at a constrained IoT community.

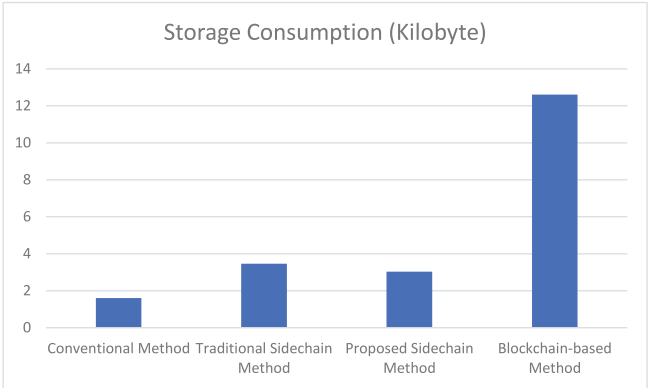

FIGURE 11. Storage consumption comparison between conventional method, blockchain-based method, traditional sidechain and proposed sidechain method.

D. STORAGE CONSUMPTION COMPARISON

Unlike the traditional sidechain structure, the public mainchain proposed in this paper is viewed as a reference database, and it requires the gateway to save simplified information blocks at local memory. Whereas, both the blockchain-based method and traditional sidechain method are required to update the full chain after each new block verification. In this subsection, we compare the storage consumption at the gateway side among the conventional method, blockchain-based method, traditional sidechain, and proposed sidechain method.

In this experiment, we consider a smart community with 5 smart systems and each system has 10 IoT devices. As mentioned in Section III, a local sidechain block contains device ID, authentication method and authentication parameters as transactions. The first two transactions (device ID and authentication method) are both 8 bytes. For the authentication parameters, we take certificate-based authentication as an example. As mentioned in [34], the average message size for the certificate-based authentication parameter is 148 bytes. Based on the quantitative data listed about the size for block component in Table 5, the storage sizes required for the conventional method, blockchain-based method, traditional sidechain, and proposed sidechain method are respectively 1.60 KB, 12.61 KB, 3.45 KB, and

TABLE 5. Memory size for each block component of a blockchain.

Blockchain Component	Size (bytes)
Previous Block Hash	32
Transaction	36
Time stamp	4
Nonce	4
Current Block Hash	32
Rest of a Block (Transaction Counter, Difficult Target)	12
Block Counter	4

3.03 KB. The proposed sidechain method only takes 24.02% of the memory space that the blockchain-based method has required, and it is 87.82% of the memory space that the traditional sidechain method has required.

V. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we proposed a novel sidechain-based decentralized authentication scheme via an optimized two-way peg protocol for the smart community. By applying an optimized mainchain and private side blockchains, the local device authentication process can be effectively handled and secured authentication information sharing procedure could be achieved. The optimized two-way peg protocol was identified to dynamically monitor the trustworthy of the target smart device to ensure the security of the smart community during the information sharing procedure. Simulation results demonstrated that the proposed scheme could significantly reduce the authentication time by comparing it with the existing blockchain-based method. Furthermore, the proposed optimized two-way peg protocol was also measured with different malicious authentication cases, and its practicability and feasibility in evaluating the trustworthy of each smart device have been confirmed. Moreover, compared with the blockchain-based authentication method and traditional sidechain method, the proposed sidechain-based scheme has improved the information management efficiency and reduced the storage burden at the gateway level. In terms of networks and assets, sidechain solutions create their own set of issues. Therefore, there exist potential directions worth exploring in sidechains on both the network and assets level. To begin, on the network level, multiple independent unsynchronized blockchains support transfers between one another. These blockchains must support transaction scripts which are later invalidated by a reorganization proof. This method requires the automatic detection of misbehavior by a software that can produce and publish such proofs. Furthermore, On the assets level, it is no longer as simple as a "one chain, one asset" law; numerous assets are erratically supported by individual chains, even those that did not exist when the chain was first created. To safeguard the transfer process, each asset is marked with the chain it was transferred from, ensuring they can be unwound accurately.

REFERENCES

[1] "IoT security—Protecting the networked society," Ericsson, Stockholm, Sweden, White paper, Jun. 2017.

[2] M. S. Mahamud, M. S. R. Zishan, S. I. Ahmad, A. R. Rahman, M. Hasan, and M. L. Rahman, "Domicile—An IoT based smart home automation system," in *Proc. Int. Conf. Robot., Elect. Signal Process. Tech. (ICREST)*, 2019, pp. 493–497.

[3] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019.

[4] K. Aurangzeb, S. Aslam, H. Herodotou, M. Alhussein, and S. I. Haider, "Towards electricity cost alleviation by integrating RERs in a smart community: A case study," in *Proc. 23rd Int. Conf. Electron.*, Palanga, Lithuania, 2019, pp. 1–6.

[5] A. Sallam, A. Refaey, and A. Shami, "Securing smart home networks with software-defined perimeter," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Tangier, Morocco, 2019, pp. 1989–1993.

[6] S. Mahmud, S. Ahmed, and K. Shikder, "A smart home automation and metering system using Internet of Things (IoT)," in *Proc. Int. Conf. Robot. Elect. Signal Process. Tech. (ICREST)*, 2019, pp. 451–454.

[7] P. Hao, X. Wang, and W. Shen, "A collaborative PHY-aided technique for end-to-end IoT device authentication," *IEEE Access*, vol. 6, pp. 42279–42293, 2018.

[8] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1441–1454, 3rd Quart., 2015.

[9] B. Kuang, A. Fu, S. Yu, G. Yang, M. Su, and Y. Zhang, "ESDRA: An efficient and secure distributed remote attestation scheme for IoT swarms," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8372–8383, Oct. 2019.

[10] Y. Wang and K. M. Khan, "Matrix barcode based secure authentication without trusting third party," *IT Prof.*, vol. 21, no. 3, pp. 41–48, May/Jun. 2019.

[11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[12] A. Fayad, B. Hammi, and R. Khatoun, "An adaptive authentication and authorization scheme for IoT's gateways: A blockchain based approach," in *Proc. 3rd Int. Conf. Security Smart Cities Ind. Control Syst. Commun. (SSIC)*, 2018, pp. 1–7.

[13] M. AbuNaser and A. A. Alkhatib, "Advanced survey of blockchain for the Internet of Things smart home," in *Proc. IEEE Jordan Int. Joint Conf. Elect. Eng. Inf. Technol. (JEEIT)*, 2019, pp. 58–62.

[14] A. Banerjee, F. Sufyanf, M. S. Nayel, and S. Sagar, "Centralized framework for controlling heterogeneous appliances in a smart home environment," in *Proc. Int. Conf. Inf. Comput. Technol. (ICICT)*, 2018, pp. 78–82.

[15] H. Mei, Z. Gao, Z. Guo, M. Zhao, and J. Yang, "Storage mechanism optimization in blockchain system based on residual number system," *IEEE Access*, vol. 7, pp. 114539–114546, 2019.

[16] H. Nishi, "Information and communication platform for providing smart community services: System implementation and use case in Saitama city," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Lyon, France, 2018, pp. 1375–1380.

[17] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K.-K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102471.

[18] A. Back *et al.* *Enabling Blockchain Innovations With Pegged Sidechains*. Accessed: 2014. [Online]. Available: https://www.blockstream.com/sidechains.pdf

[19] A. Refaey, K. Hammad, S. Magierowski, and E. Hossain, "A blockchain policy and charging control framework for roaming in cellular networks" *IEEE Netw.*, early access. Available: https://arxiv.org/abs/1906.06350, doi: 10.1109/MNET.001.1900336.

[20] F. X. Olleros and M. Zhegu, *Research Handbook on Digital Transformations*. Northampton, MA, USA: Edward Elgar Publ., 2016, pp. 1–6.

[21] R. Casado-Vara, P. Chamoso, F. De la Prieta, J. Prieto, and J. M. Corchado, "Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management," *Inf. Fusion*, vol. 49, pp. 227–239, Jan. 2019.

[22] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, Rep., 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[23] M. Li, H. Tang, and X. Wang, "Mitigating routing misbehavior using blockchain-based distributed reputation management system for IoT networks," in *Proc. IEEE Int. Conf. Commun. Workshop (ICC)*, 2019, pp. 1–6.
[24] R. M. Parizi, S. Homayoun, A. Yazdinejad, A. Dehghantanha, and K. R. Choo, "Integrating privacy enhancing techniques into blockchains using sidechains," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, 2019, pp. 1–4.
[25] N.-Y. Lee, J. Yang, M. M. H. Onik, and C.-S. Kim, "Modifiable public blockchains using truncated hashing and sidechains," *IEEE Access*, vol. 7, pp. 173571–173582, 2019.
[26] M. De Ree, G. Mantas, A. Radwan, S. Mumtaz, J. Rodriguez, and I. E. Otung, "Key management for beyond 5G mobile small cells: A survey," *IEEE Access*, vol. 7, pp. 59200–59236, 2019.
[27] J. Zhang, X. Huang, W. Wang, and Y. Yue, "Unbalancing pairing-free identity-based authenticated key exchange protocols for disaster scenarios," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 878–890, Feb. 2019.
[28] D. Kim and J. Lee, "Efficient and secure device clustering for networked home domains," *IEEE Trans. Consum. Electron.*, vol. 65, no. 2, pp. 224–232, May 2019.
[29] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," *J. Future Gen. Comput. Syst.*, vol. 86, pp. 740–749, Sep. 2018.
[30] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei, and F. Yang, "A security authentication method based on trust evaluation in VANETs," *J. Wireless Commun. Netw.*, vol. 59, Mar. 2015, pp. 1–8.
[31] T. Neudecker and H. Hartenstein, "Network layer aspects of permissionless blockchains," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 838–857, 1st Quart., 2019.
[32] H. Wang, D. He, and Y. Ji, "Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography," *Future Gen. Comput. Syst.*, to be published.
[33] M. Qin, L. Chen, N. Zhao, Y. Chen, F. R. Yu, and G. Wei, "Power-constrained edge computing with maximum processing capacity for IoT networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4330–4343, Jun. 2018.
[34] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 11, pp. 4136–4144, Nov. 2007.

MIN LI (Student Member, IEEE) received the bachelor's degree in automation from the Beijing University of Posts and Telecommunications, China, in 2016, and the M.E.Sc. degree from the Department of Electrical and Computer Engineering, University of Western Ontario, Canada. His research interests include blockchain systems under practical network constraint, IoT distributed security management, and IoT smart home applications.

HELEN TANG (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Carleton University in 2005. She is the Portfolio Manager of cyber electromagnetics with the Center for Security Science, Defence Research and Development Canada, Ottawa. From 1999 to 2005, she worked in several research and development organizations in Canada and the United States, including Alcatel-Lucent, Mentor Graphics, and Communications Research Center Canada. From 2005 to 2015, she was a Defence Scientist with DRDC, Ottawa. She has been involved in many projects related to cyber security. She is also an Adjunct Professor with the Department of System and Computer Engineering, Carleton University, where she is the Supervisor of several graduate students. She was a recipient of the Outstanding Contribution Award at DRDC Ottawa in 2009 and 2016, the Best Paper Award at IEEE/IFIP TrustCom 2009, and the Outstanding Leadership Award at IEEE/IFIP TrustCom 2010.

AHMED REFAEY HUSSEIN (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from Alexandria University, Egypt, in 2003 and 2005, respectively, and the Ph.D. degree from Laval University, Quebec, Canada in 2011. He was a System/Core Network Engineer leading a team of junior engineers and technicians in the telecom field with the three prominent companies of Fujitsu, Vodafone, and Alcatel-Lucent. He was a Senior Embedded Systems Architect with the Research and Development Group, Mircom Technologies Ltd. from 2013 to 2016; a Postdoctoral Fellow with the ECE Department, Western University from 2012 to 2013; and a Professional Researcher with the LRTS Lab, Laval University in the field of wireless communications hardware implementations from 2007 to 2011. He is an Assistant Professor with Manhattan College and an Adjunct Research Professor with Western University. He has authored and coauthored more than 40 technical papers, one patent granted, and three patent applications addressing his research activities. He has served a number of roles for journals, including the Guest Editor for *Mathematical Problems in Engineering Journal* and an Associate Editor for the *Canadian Journal of Electrical and Computer Engineering*, as well as different roles for IEEE journals and transactions. He is currently an active member of the IEEE and regularly participates in organizing committees and major IEEE conferences (as a TPC Chair and Symposium Chair).

XIANBIN WANG (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001. He was with the Communications Research Centre Canada (CRC) as a Research Scientist/Senior Research Scientist from July 2002 to December 2007. He is a Professor and the Tier 1 Canada Research Chair with Western University, Canada. From January 2001 to July 2002, he was a System Designer with STMicroelectronics. He has over 400 peer-reviewed journal and conference papers, in addition to 30 granted and pending patents and several standard contributions. His current research interests include 5G and beyond, Internet of Things, communications security, machine learning, and intelligent communications. He has received many awards and recognitions, including the Canada Research Chair, the CRC President's Excellence Award, the Canadian Federal Government Public Service Award, the Ontario Early Researcher Award, and six IEEE Best Paper Awards. He was involved in many IEEE conferences, including GLOBECOM, ICC, VTC, PIMRC, WCNC, and CWIT, in different roles, such as the Symposium Chair, the Tutorial Instructor, the Track Chair, the Session Chair, and a TPC Co-Chair. He is currently serving as the Chair of ComSoc SPCE Technical Committee. He currently serves as an Editor/Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON BROADCASTING, and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He was also an Associate Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2007 and 2011, and IEEE WIRELESS COMMUNICATIONS LETTERS from 2011 and 2016. He is a fellow of the Canadian Academy of Engineering, the Engineering Institute of Canada, and an IEEE Distinguished Lecturer.