Home IoT Authority Control Method Based on DID Auth

Jae-Ho Choi
dept. Knowledge Information Engineering
Ajou University
Suwon, Republic of Korea
cjh7748@ajou.ac.kr

Jun-Hyuk Im
dept. Knowledge Information Engineering
Ajou University
Suwon, Republic of Korea
amigojun@ajou.ac.kr

Hae-Jun Song
dept. Knowledge Information Engineering
Ajou University
Suwon, Republic of Korea
young7135@ajou.ac.kr

Ki-Hyung Kim
dept. Cyber Security
Ajou University
Suwon, Republic of Korea
kkim86@ajou.ac.kr

***Abstract*—The Home IoT device market is expanding rapidly, which has led to the increasing adoption of these devices in the home. However, IoT devices have long been challenged by various vulnerabilities and pose unique security challenges compared to other devices. This paper aims to redefine the process of entering the Home IoT environment by leveraging Decentralized Identifier(DID) authentication, and proposes a comprehensive approach to using Verifiable Credential(VC) and Verifiable Presentation(VP) to control access from outsiders like visitors. Through security analysis, this paper also highlights how these authentication and permission controls address traditional vulnerabilities and provide improved security over traditional IoT authentication methods. The results of this study shed light on the significant impact this methodology can have on the security of the Home IoT environment.**

***Index Terms*—Home IoT, DID, VC·VP, Blockchain, Security, Authentication**

I. Introduction

There are many Home IoT devices at home these days, and the number of households that have them will increase in the future. According to the survey, the global smart home market size will reach $222.9 billion by 2027 and the number of active households will approach approximately 672.6 million [1].

Home IoT systems are getting closer to human life, but there are some security vulnerabilities. IoT devices often use simple patterns or default passwords, and they are lightweight devices or are subject to various attacks such as impersonation and DoS attacks [2] [3]. In addition, the device enables a variety of services, but transmits sensitive information, which can allow an attacker to maliciously access the device, compromising the system or forging information [4].

These vulnerabilities are more likely to occur if a stranger enters the house and accesses a Home IoT device. Excluding intruders, visitors from outside, such as cleaners, babysitters, and caregivers, have become more common than ever. The average housekeeping service expenditure in U.S. was about $160 in 2021, an increase of as much as %35 over 2020 [5]. Visitors may have to use Home IoT devices when doing their works, and most of them will use the devices without any restrictions from homeowners. However, if the homeowner is outside, it is hard to notice whether the visitor is using an IoT device. In other words, if a visitor accesses an IoT device with malicious intent, personal information or data inside the device may be leaked and even damage the entire home. Therefore, in this paper, we present a user's authentication process for Home IoT using DID Auth. And we also proposes a method with VC·VP to prevent indiscriminate access to Home IoT by visitor at home.

The next sections are structured as follows. In Section 2, we describe the relevant techniques needed to control visitors' Home IoT access, and the Section 3 contains a detailed picture and description of the method proposed in the paper. And the Section 4 explains how the method has advantages in protecting vulnerabilities over conventional methods. In the last Section 5, the results and significance of the study are mainly described.

II. Relative Works

A. Home IoT

Smart Home, which enables the connection and use of various Home IoT devices such as TVs and refrigerators in apartments and houses, is on the rise. The main goal of Home IoT devices on the market is to improve the quality of life and maximize convenience at home. With the recent development of information and communication technology and IoT, the role of Home IoT environment continues to be important, and smart Home IoT and network environment are emerging as key elements [6].

Unlike the existing method in which users operate each device separately, the network method of Home IoT can manage devices through gateways inside and outside the home. However, since several devices are centrally configured, they cause serious security vulnerabilities such as malicious access,

data forgery, and tampering [7]. While the demand for Home IoT devices is increasing, there are weaknesses related to user data and privacy, so improving the infrastructure of smart homes is essential.

To solve these problems, we propose a more secure smart home mechanism by taking advantage of the integrity and confidentiality of DID Auth and blockchain.

B. Vulnerabilities in IoT Devices

The proliferation of IoT devices has brought about unprecedented connectivity and convenience. However, these devices also introduce vulnerabilities that pose significant security risks. Even they are low-level devices with limited resources and can perform only a small number of actions, making it difficult to apply advanced security, and they have a wide variety of devices, making it difficult to develop and apply security mechanisms [8]. The following are five typical vulnerabilities that can occur in IoT devices.

1) Dictionary Attack: A Dictionary Attack is a indiscriminate attack in which an intruder attempts to access an IoT system/device by attempting any combination of characters for password authentication. This attack may cause other serious attacks such as DDoS [9].

2) Unauthorized Access: Attackers can gain unauthorized access to IoT systems/devices in a variety of ways, from exploiting hardware/software vulnerabilities to illegal login attempts [10]. This can cause problems with data forgery and system abuse. To prevent such access, a secure credential management system must be implemented. IoT devices are still weak or have basic credentials. There are also fewer attempts to change existing credentials [9].

3) Malicious Code Injection: Malicious Code Injection is a type of physical attack that imparts malicious code to a device through an exposed and unsafe software/hardware interface that exists on the IoT device, thereby damaging the IoT device. This could be a starting point for an attacker to take control of other devices on the same network if one IoT device is hacked [10].

4) DoS(Denial of Service), DDoS(Distributed Denial of Service): IoT devices are becoming targets of attacks that run DoS and DDos. IoT devices targeted by the attack increase the amplification rate of the traffic generated, which overloads the network. IoT devices are particularly vulnerable to this attack because they have low-performance hardware [2] [9] .

5) Social Engineering Attack: Attackers can profile users of IoT devices using their personal information. Attackers can find out the user's password, etc., thereby accessing sensitive data and controlling IoT devices. To prevent this, a stronger authentication system is needed to protect the personal data of users using IoT devices [10].

C. OAuth(Open Authorization) 2.0

The concept of OAuth 2.0 emerged to solve various security vulnerabilities related to existing authentication methods and password management. OAuth is an open protocol that allows clients registered with web services or applications to log in or access data more quickly and securely using authentication information, and that allows them to obtain API rights for applications with a single authentication. OAuth defines a total of four roles: resource owner, resource server, client, and authorization server [11]. These actors establish end-to-end Transport Layer Security(TLS) channels and interact with each other during resource access procedures.

The procedure is summarized as follows: ①The client contacts the resource owner of the resource. ②The resource owner transmits the code to grant access to the client. ③The client delivers the received code to the authorization server. ④The authorization server checks the authorization code and provides a token containing the content provided to the client. ⑤The client passes the token to the resource server. ⑥The resource server provides a protected resource after validating the received token [12].

If OAuth is applied to IoT, it is possible to provide safer services to users who are allowed access, but there is a limitation that requires strong trust in third parties, that is, authentication servers [13].

In order to overcome these limitations, This paper proposes to use the DID Auth method, a peer to peer(P2P) method that excludes third-party intervention, for access to Home IoT devices.

D. Decentralized Identifier(DID), DID Document

1) DID: DID is an identity authentication certification technology that uses decentralized identifiers, and is a technology that is directly issued and managed by individuals, not by institutions or central systems. Since it is used based on the distributed ledger system, it is easy to validate and has advantages in protecting personal information.

As shown in Fig. 1, the format of DID is largely divided into three parts: Scheme, DID Method, DID Method-Specific Identifier. Scheme proves that this address is DID schema. DID Method is a mechanism for managing DID Document related to DID in a distributed ledger or network. And DID Method-Specific Identification is a unique ID used in the DID method [14].

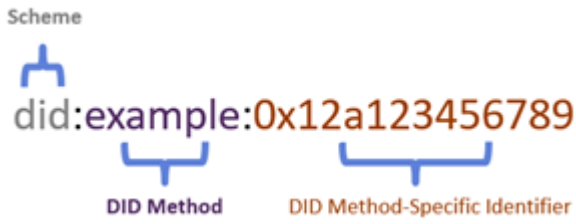

Fig. 1. An Example of DID Structure

2) DID AUTH: The relevant information of the DID is stored in a place called DID Document. As you can see in Fig. 2, The DID Document includes authentication methods for performing DID Auth, and mainly includes '@context', 'id', 'verificationMethod', 'authentication'.

@context defines the basic grammar of DID Document. It contains the url of the predefined context or the context set by

administrator. The id inclueds the DID of the aforementioned subject. The verificationMethon is an authentication information that can prove ownership. Several ownership authentication methods, such as RSA and biometric authentication, are defined along with key values. The authentication item shows a list of verification methods, of which the verification process can be carried out in the way that the user wants or the other party requires [14].

Fig. 2. An Example of DID Document

E. Verifiable Credential(VC), Verifiable Present(VP)

1) VC: Data models of VC are defined as Credential Metadata, Claim(s), and Proof(s), as shown in Table 1.

Credential Metadata defines who issued the VC, the expiration period of the VC, and the method of discarding the VC. In Claim(s), information on the Subject is stored in the order of Subject-Property-Value like a tree structure. Claims can be specified in multiple subjects if necessary. Proof(s) includes values necessary to verify the authenticity of VC, and various encryption techniques such as RSA and biometric authentication are used. The verifier verifies the Proof part to ascertain whether the VC was issued by the issuer specified in the VC [15].

TABLE I
COMPONENTS OF VC

Credential Metadata	Issuer Issuance Date of VC Expiration Date of VC ...
Claim(s)	Information about Property of Subject Save as "Subject – Property – Value"
Proof(s)	Signature of Issuer Generation Date Signature Algorithms ...

2) VP: Data models of VP are composed of Presentation Metadata, Verifiable Credentials(s), and Proof(s).

Presentation Metadata includes data that can be used for VP verification, such as the subject of VP, the type that specifies that it is VP, and the terms of use. The Verifiable Credential(s) includes VC(s). The Subject can select and insert the VC(s) and properties required by the verifier and such selective disclosure can protect personal information. The verifier who receives the VP can clarify the authenticity of the VC by verifying the Issuer through the Proof part included in the VC. The proof is signed by the Subject. The verifier can verify whether the VP is submitted by the subject by ascertaining the signature of the subject submitting the VP. Like VC, various encryption techniques are used [15].

TABLE II
COMPONENTS OF VP

Presentation Metadata	Issuer Issuance Date of VC Expiration Date of VC ...
Verifiable Credential(VC)	| VC 1 |, | VC2 |, | VC 3 |, ...
Proof(s)	Signature of Subject Generation Date Signature Algorithms ...

F. Blockchain

Blockchain first emerged in 2008 based on Bitcoin's ledger and evolved into a computing platform that enables anonymously monitored transaction records on the network [16]. Blockchain cannot be falsified or changed because data is connected to each block in the form of a chain, and it can also prove the integrity of the data. In addition, we are building a reliable network by utilizing blockchain technology jointly managed by network participants [17]. Each block is chained using hash values from the previous block to implement a reliable network form. Each block in the blockchain consists of a header part and a body part. The header portion contains information for connecting to the previous block, and the body portion includes transactions.

III. ACCESS CONTROL METHOD FOR HOME IOT DEVICES

This section provides detailed methods for controlling access to DID Auth-based Home IoT devices.

Before that, we will define the key actors and terms that will appear in this section. The Homeowner is the administrator of the Home IoT device and the resident of the home. The Manufacturer sells Home IoT devices and manage DApp and blockchain. DApp is a platform that allows users to connect with Home IoT and other users to issue and submit credentials called VC and VP. A Visitor is a housekeeper, a repairman, or a relative of the Homeowner, who enters the Homeowner's house when visiting. It is assumed that the Homeowner and the Visitor have agreed to enter in advance.

The first subsection describes the authentication process when Homeowners purchase devices from manufacturers and configure their Home IoT environment for the first time. The second section includes the process of obtaining access to the Home IoT device when a Visitor visits the Homeowner's home.

A. Initial Authentication Method for Homeowner

Fig. 3 shows the process of the Homeowner entering the Home IoT environment for the first time.

①After purchasing a device manufactured by Manufacturer, Homeowner requests registration through DApp managed by Manufacturer. ②The Manufacturer performs conventional authentication to the Homeowner, and Connection takes place when it is completed normally. ③The Manufacturer stores DID Documents of Homeowner, Smart Hub, and other IoT devices in the blockchain ledger. ④The Manufacturer conducts DID Auth with the Home Owner, and at this time, the Manufacture completes authentication by inquiring the DID Document of the Homeowner. ⑤Manufacture delivers the VC to Homeowner, and the transaction of VC issuance are stored in the blockchain ledger. In VC, Credential Metadata, Claim, and Proof are defined as described in Section II. The credentialSubject in the Claim part should include the DID of all devices purchased by Homeowner, including Smart Hub. ⑥Homeowner creates VP, a form that is readable by the Smart Hub. ⑦Homeowner performs DID Auth with one's Smart Hub. At this time, the Smart Hub verifies the DID Document of the Homeowner on the blockchain. ⑧If it is determined to be a normal user, the Smart Hub receives a VP from the Homeowner and Transactions related to VP are stored in the ledger. the Smart Hub inquires the DID Document of the Manufacturer in the blockchain ledger to verify whether it is the right credentials. ⑨When all verification is completed, Smart Hub approves access to Homeowner and Homeowner can communicate with IoT devices using DApp.

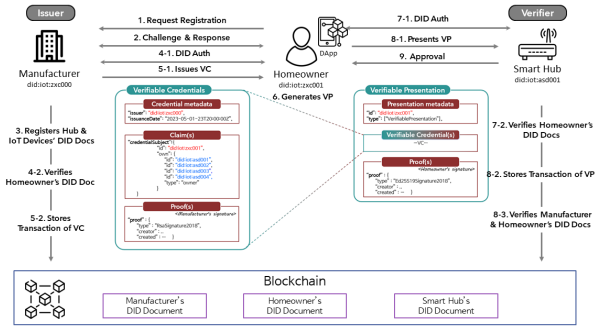

Fig. 3. Initial Authentication Method for Homeowner

B. Method of Controlling Home IoT Access of Visitors

Fig. 4 and 5 show how to control Visitors' Home IoT access.

Fig. 4 includes the process by which the Homeowner sets up Visitor's permission for the Home IoT.

The Visitor's user registration procedure is omitted because it is similar to the Homeowner's procedure described above, except that Visitor does not register DID documents of IoT devices. ①Homeowner and Visitor proceed to the interconnection through DID Auth. At this time, the Homeowner verifies the Visitor's DID Document. ②The visitor asks the Homeowner for credentials to access the home network. ③Upon receiving the request, the Homeowner creates a VC and delivers it to the Visitor. The structure of the VC is similar to that of the VC manufactured by the manufacturer in Fig. 2 However, the VC's credentialSubject created by Homeowner defines only Homeowner's Home IoT devices that Visitor can access. Devices that the Homeowner does not want to allow can be set up for access by not including the DID in the credentialSubject. In addition, the VC contains an expiration date set by the Homeowner, so Visitor cannot use the VC again after the expiration date. VC issuance information is stored in the blockchain.

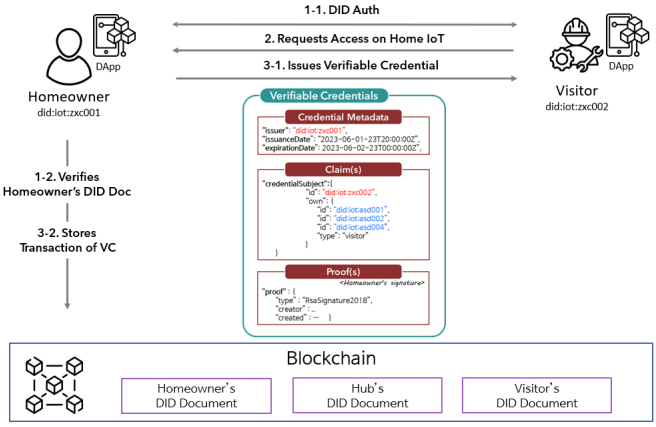

Fig. 4. Visitor's Home IoT Access Acquisition Process

Fig. 5 shows the authentication procedure for the Visitor who received the VC to use the Home IoT devices. ①The Visitor generates a VP with the VC received from the Homeowner. ②The Vistitor conducts DID Auth with the Smart Hub to submit the VP, and the Smart Hub queries the DID Document of the Visitor. ③When the DID of the Visitor is confirmed, the Visitor submits the VP to the Smart Hub, and the Smart Hub verifies the validity of the VP by inquiring the Visitor and Homeowner's DID Document. Transactions about VP are stored in the blockchain. ④After completing the verification process, Smart Hub finally grants Visitor access to Home IoT. However, the Visitor is granted limited authority to control only the devices defined by the Homeowner in the credentialSubject.

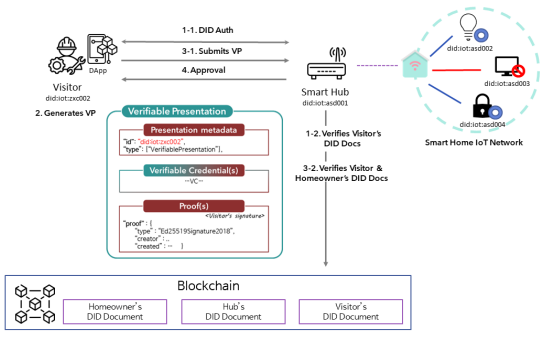

Fig. 5. Visitor's Home IoT Access Authorization Process

IV. Analysis of Vulnerabilities

The DID Auth for Home IoT control proposed in this paper not only provides a higher level of security and protection than traditional authentication methods, but is also more efficient than security response or attack detection technologies that are difficult to apply within IoT devices. The method can mitigate vulnerabilities described in Section 2.

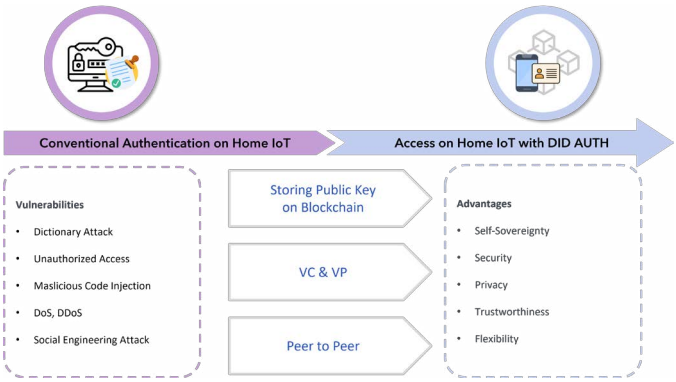

Fig. 6. Comparison of Conventional and DID Auth Methods in Home IoT

a) Dictionary Attack: The Method allows you to use a variety of validation methods within a DID Document, significantly reducing the vulnerability to proactive attacks from conventional password authentication. This approach leverages several verification factors, such as asymmetric keys and biometric recognition, to ensure a higher level of security in the authentication process.

b) Unauthorized Access: By eliminating reliance on centralized authentication systems, this can significantly reduce the risk of hackers stealing user credentials and accessing them without permission. VC·VP also makes it difficult for unauthorized individuals to enter Home IoT systems or devices.

c) Malicious Code Injection: Peer-to-peer authentication with DID and VC·VP can prevent intruders from injecting code into devices without permission and ensure the integrity and reliability of devices and data within Home IoT.

d) DoS, DDoS: The Authentication mechanisms protect the device from unauthorized control or malicious operations, preventing it from being used as part of a network attack.

e) Social Engineering Attack: The method reduces the risk by minimizing reliance on centralized identity stores. and it also decreases the likelihood of attackers exploiting personal data obtained through social engineering tactics through the ability to individually control their identity and selectively share information. Users can share only the information they need, reducing the risk of manipulation or impersonation.

Home IoT permission control methods based on DID Auth can provide strong and secure authentication and permission control, including all of these security advantages.

V. Conclusion

In conclusion, we presents a novel access control method for Home IoT devices using DID authentication. By leveraging DID authentication and VC·VP, this approach enables secure authentication and permission management for external access to Home IoT devices. It offers the ability to set limited authorities for visitors, such as housekeepers, who enter the home.

Compared to existing authentication methods, The utilization of DID authentication and VC·VP enhances security and prevents various cyber attacks, including password theft and forgery and the decentralized ledger provides a safer and more robust authentication key management system.

By allowing homeowners to define customized access privileges for visitors, this access control method offers granular control over the interactions with Home IoT devices. And It ensures that visitors, have access only to the necessary devices while protecting sensitive data from unauthorized access.

The implementation of this method has the potential to significantly improve the security of smart home environments and It is expected to contribute to the advancement of secure and trustworthy smart home environments.

Acknowledgment

This research was supported in part by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2021-0-01835) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation), MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2023-2018-0-01396) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation),Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P00 08703, The Competency Development Program for Industry Specialist), National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT (2021R1F1A1045861) and Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT)(2021-0-00590, Decentralized High Performance Consensus for Large-Scale Blockchains)

References

[1] Statista, “Smart Home – Market Data & Forecast,” December 2022.
[2] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri and G. Baldini, ”Security and privacy issues for an IoT based smart home,” 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2017, pp. 1292-1297.
[3] A. M. Gamundani, A. Phillips and H. N. Muyingi, ”An Overview of Potential Authentication Threats and Attacks on Internet of Things(IoT): A Focus on Smart Home Applications,” 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 50-57.
[4] M. Hossain, S. Noor and R. Hasan, ”HSC-IoT: A Hardware and Software Co-Verification Based Authentication Scheme for Internet of Things,” 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), San Francisco, CA, USA, 2017, pp. 109-116.

[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[6] Lee, Y., Rathore, S., Park, J.H. et al. A blockchain-based smart home gateway architecture for preventing data forgery. Hum. Cent. Comput. Inf. Sci. 10, 9 (2020).
[7] Md. Moniruzzaman, Seyednima Khezr, Abdulsalam Yassine, Rachid Benlamri, Blockchain for smart homes: Review of current trends and research challenges, Computers & Electrical Engineering, Volume 83, 2020.
[8] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, ”A Supervised Intrusion Detection System for Smart Home IoT Devices,” in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042-9053, Oct. 2019.
[9] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar and N. Kumar, ”IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges,” in IEEE Access, vol. 8, pp. 168825-168853, 2020.
[10] T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, ”Consumer IoT: Security Vulnerability Case Studies and Solutions,” in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020.
[11] Dick Hardt, Ed. RFC 6749: The OAuth 2.0 authorization framework. October 2012. http://tools.ietf.org/html/rfc6749.
[12] S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia and G. Bianchi, ”OAuth-IoT: An access control framework for the Internet of Things based on open standards,” 2017 IEEE Symposium on Computers and Communications (ISCC), Heraklion, Greece, 2017.
[13] S. Cirani, M. Picone, P. Gonizzi, L. Veltri and G. Ferrari, ”IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios,” in IEEE Sensors Journal, vol. 15, no. 2, pp. 1224-1234, Feb. 2015.
[14] W3C, “Decentralized Identifiers (DIDs) v1.0,” July 2022. https://www.w3.org/TR/did-core/
[15] W3C, Verifiable Credentials Data Model v1.1,” March 2022. https://www.w3.org/TR/vc-data-model/
[16] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Mar. 2009. https://bitcoin.org/bitcoin.pdf.
[17] Z. Jiao, R. Tian, D. Shang, H. Ding, B. Zhang and C. Li, ”A Bilayer Scalable Nakamoto Consensus Protocol for Blockchain Systems,” in IEEE Network, vol. 36, no. 3, pp. 174-182, May/June 2022.