Blockchain-Empowered Identity Management with a Dual Identity Model for UAVs in 5G Networks

Ren Chen, Hao-Wei Tseng, Jie-Lin Lien, and Wanjiun Liao

Abstract

In this work, we study secure and trusted authentication of unmanned aerial vehicles (UAVs) in 5G networks. Existing centralized UAV identity authentication mechanisms may only be able to verify the identity of the UAV itself or manage pilots, which are far from complete protection of legal access. Some recent works on UAV identity management are based on blockchain technology, in which UAV identities are generated through the blockchain software wallets, so they may be vulnerable to UAV identity forgery. To tackle the challenges described above, we propose an authentication mechanism based on a dual-identity (dual-ID) model for UAVs in 5G networks via a cross-layer design of SIM cards, blockchain, and smart contracts. The proposed self-sovereign UAV identity management procedure will then jointly process the authentications of both the UAV device and its pilot through the blockchain hardware wallets embedded in 5G SIM cards. In this way, a global registry of a unique identifier of each UAV device and each pilot can be ensured, and the identity forgery problem can also be avoided. Due to the limited power and processing capacity of UAV devices and the need of quick response for authentication, we employ 5G and multi-access edge computing (MEC) servers for communication and processing. To validate the proposed solution, a developed proof-of-concept system is tested through the 5G MEC testbed at National Taiwan University to demonstrate the flexibility and usability of UAV authentication.

Introduction

With the coming era of 5G networks, one of the new goals is to flexibly accommodate a large number of Internet of Things (IoT) devices and their applications in the cellular infrastructure to perform their communications. To facilitate the vertical developments of IoT applications, one of the critical issues that needs to be addressed is security, especially identity management and access control for IoT devices. In cellular networks, IoT devices are equipped with Subscriber Identity Module (SIM) cards, which are secure and cost-effective for authentication at the network layer. However, for the IoT platform at the application layer, existing identity management schemes and identity federation standards (e.g., OAuth2.0 and OpenID Connect [1]) are mainly based on a centralized "trusted third party" and only allow the use of weak authentication schemes (e.g., passwords), which are vulnerable to attacks against various IoT devices.

Unmanned aerial vehicles (UAVs) are a special type of IoT devices, which are flexibly maneuverable and remotely administered via wireless channels by individuals or a group of people. In recent years, UAVs have rapidly become popular and widely deployed in military, aviation, civilian, and commercial application domains, such as precision agriculture, cargo delivery, search and rescue, and aerial photography. One of the challenges imposed by UAVs is their illegal flying, invading places such as airports, prisons, and military bases. Malicious UAVs that can be remotely controlled can even exacerbate the problem due to the lack of trusted authentication and UAV identity management. To avoid malicious UAVs, one of the key issues in identity management is ensuring the integrity of UAV identities, including the UAV device and the pilot. To allow a UAV to enter a specific airspace, both the pilot and the UAV device should be authenticated and authorized to enter the airspace. Without proper integrity checks, there may be a risk of forged identity [2] for the UAV device or the pilot, or both.

Some recent work leverages decentralized ledgers and smart contracts in blockchain technology for UAV identity management, especially using a single identity based on blockchain software wallets. However, the single identity mechanism based on blockchain software wallets has the problem of identity integrity. As a result, it is not suitable for secure and trusted authentication for UAVs.

To address the challenges described above, in this work, we study the secure and trusted authentication of UAVs in 5G networks by leveraging the secure SIM card mechanism in cellular IoT and the decentralized ledger service in the blockchain systems. Specifically, we propose a dual-identity (dual-ID) scheme for UAV authentication with a cross-layer design of 5G SIM card, blockchain, and Ethereum smart contract, as shown in Fig. 1. The self-sovereign dual-ID management procedure for secure and trusted authentication in 5G networks will jointly handle the ID verifications of UAV devices and their pilots through blockchain hardware wallets embedded in 5G SIM cards. As a result, the global registry of each UAV (i.e., the device and its pilot) can be ensured, and the identity forgery of the UAV device and its pilot can also be avoided. To validate the proposed solution, a proof-of-concept (PoC) system was implemented and tested

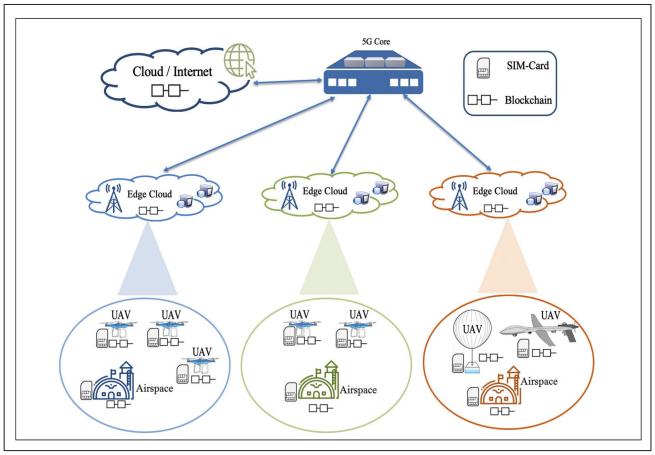

FIGURE 1. The illustration of the proposed blockchain-based dual-ID management in 5G UAV systems.

The authors are with Xiamen University of Technology and National Taiwan University, China.

Digital Object Identifier: 10.1109/IOTM.001.2100137

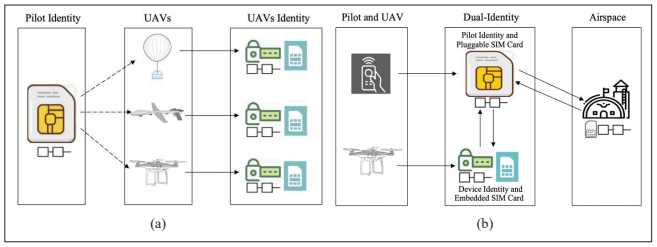

FIGURE 2. Dual-identity management scheme: a) dual-identity relationship; b) dual-ID-based authentication.

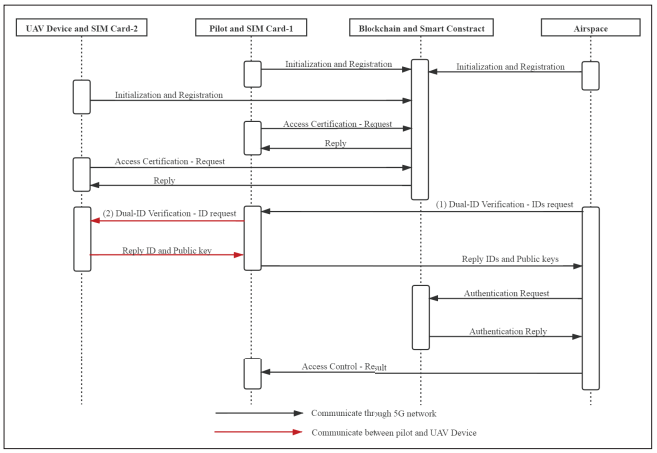

FIGURE 3. The workflow of dual-identity management for UAVs.

to demonstrate the flexibility and usability of UAV applications via the Ethereum private testnet [4] and 5G MEC testbed at National Taiwan University [5].

Blockchain and Identity Management for UAVs

In this section, we first overview the concepts of blockchain, smart contract, and SIM card, and then describe the related work of identity management for UAVs.

Blockchain, Ethereum Smart Contract, and SIM Card

Blockchain, originally introduced by Bitcoin [3], is a peer-to-peer mechanism to achieve decentralized ledgers with immutable and traceable benefits. Blockchain technology includes cybersecurity, crypto-hash, and consensus protocols. How the transactions are created, organized into blocks, mined, verified, and stored on the blockchain are also well defined. Ethereum [4] is another well-known blockchain technology whose goal is to create a general-purpose decentralized computer through smart contracts, allowing various programs to be deployed without downtime, censorship, or fraud. Smart contracts are immutable and executable codes recorded on the blockchain. Once a smart contract is finalized and published on the blockchain, the executable code is immutable and determines the outcome with specific inputs.

For blockchain systems, each account is associated with a key pair (i.e., private key and public key) and a blockchain address, which is determined based on a hash function of the public key stored on the blockchain [3, 4]. The private key used for signature to ensure confidentiality needs to be stored and protected in a secure manner, which is also known as the blockchain wallet. Accounts with lost private keys can no longer be operable. Key pairs can be saved in software (e.g., a web wallet or app wallet) or hardware (dedicated hardware wallets). The security of the software wallet mainly depends on the developer and the usage environment of the wallet, and users need to download and save the private key themselves. Saving private keys in software wallets is vulnerable to traditional attacks (e.g., computer virus, worm, and trojan horse), resulting in private key disclosure. With hardware wallets, however, the private keys are burned in secure hardware (chips) controlled only by the user, making it nearly impossible for hackers to steal the private keys. Generally, hardware wallets are more resistant to attacks than software wallets. In our work, the key pair is stored in two SIM cards that will be used as the hardware blockchain wallets for the UAV, and these two blockchain-wallet-enabled SIM cards also have 5G communication capabilities. In this way, we can well protect blockchain keys and create a globally unique address as the UAV identity, combined with the dual-ID based authentication to avoid forgery of the UAV device and the pilot in 5G networks.

Identity Management for UAVs

Identity management is the process of identifying various entities in the system (e.g., users or devices) and managing access to resources in the system by combining access rights and constraints with established identities [6]. There are very few research works on UAV identity management in 5G networks. UAVs are often regarded as a special kind of IoT device, so the methods of IoT identity management can be applied (e.g., [7]). Reference [8] is a typical approach to address the authorization and authentication problem for constrained devices and ensure that the miniature IoT devices can still maintain the required security level. Chen *et al.* [9] proposed an IoT user-centric identity management framework centered on IoT users built on top of the global identity provider to maintain a global identity space. Different service providers can generate their own local identities based on global identities. Reference [10] proposed a physical unclonable functions-based identification and authentication mechanism with privacy-preserving functions. However, the above-mentioned traditional identity management methods are centralized and may have several security issues.

In [11], some decentralized and semi-decentraliized identity management methods for IoT devices are proposed. In [12], a semi-decentralized identity management framework is proposed, which defines a unique global digital identity to solve the ownership management and identity update problems of IoT devices. Kapitonov *et al.* [13] designed a communication protocol for agents in UAV swarms to make decisions autonomously. Specifically, it employs a decentralized blockchain framework, so this approach only allows user IDs to be identified by locally generated cryptographic keys. Sharma *et al.* [14] utilized UAVs to achieve interoperability between heterogeneous networks to form an ultra-dense wireless network. They then established a trust relationship between the blockchain-based UAVs to reduce network latency and overhead. Secure network access is ensured with public and private keys. The public key helps UAVs identify and authenticate, while the private key helps UAVs access broadcast information from other neighboring UAVs. In summary, existing blockchain-based decentralized and semi-decentralized identity management approaches only use one blockchain address as the identity in the software, and perform a single-pass authentication for identity management. Such a setup would weaken identity management and complicate ownership transfer, thus increasing the risk of identity forgery.

Blockchain-Assisted Authentication with Dual-ID for 5G UAVs

In this work, we design a blockchain-assisted authentication scheme with a dual-ID model for UAV identity management in 5G networks, as shown in Fig. 2. Figure 2a shows the dual-ID relationship; that is, the pluggable pilot identity can control multiple UAVs, but each UAV has only one device identity. Figure 2b shows the dual-ID-based authentication. During this process, both UAV devices and pilots should be authenticated before airspace access certificates are issued. By using the decentralized ledger of the blockchain system, the secure SIM card of the cel-

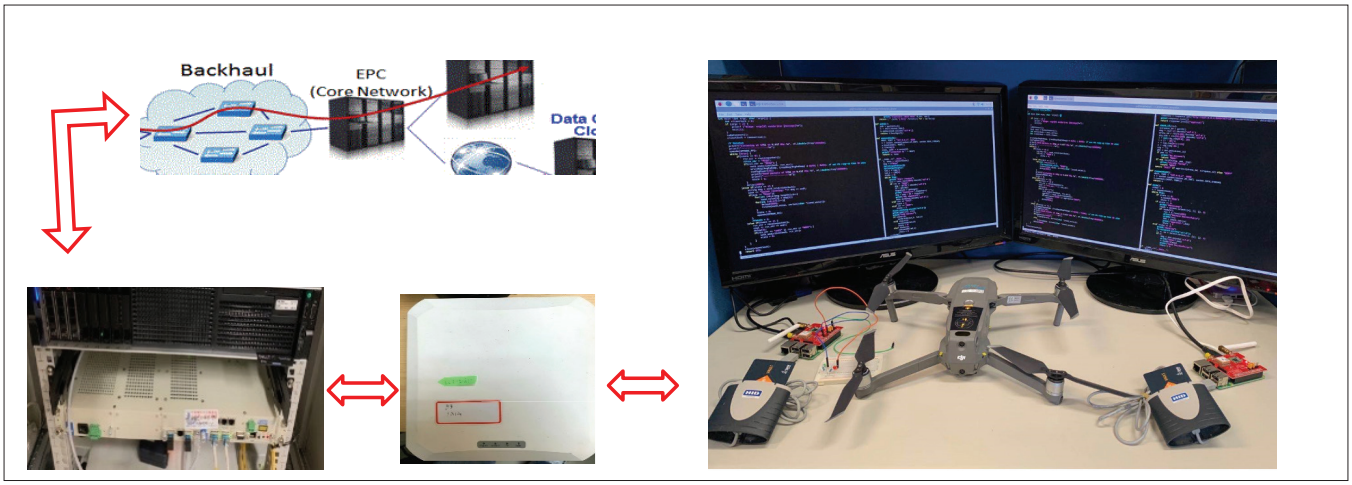

FIG
blockchain, and smart contract.

lular network, and the smart contracts on top, we can establish a global registry that enables authorized and identifiable entities to create UAV device identities and pilot identities. For the dual-ID model, the first ID corresponding to the UAV pilot identity is created by the blockchain public key and stored in a pluggable SIM card. A user who inserts the pluggable SIM card into the UAV device becomes the pilot of the UAV, and the role will remain active until the SIM card is removed. The second ID corresponding to the UAV device ID is created from the blockchain public key stored in the embedded SIM card when the UAV device is manufactured. The UAV device ID is stored in the UAV hardware and remains unchanged after manufacture. With this dual-ID model, since each UAV has two SIM cards, the two identities can be verified. Note that the same blockchain system will only create one identity for the airspace.

For the dual-ID-based authentication scheme, the first step is to verify the ID pair of the UAV device and its pilot by the airspace. The message is then co-signed by the pilot and the UAV device using the private keys stored in the two SIM cards and is sent back to the airspace to complete the authentication process. In this way, the UAV device and its pilot will be jointly authenticated before entering the airspace, avoiding forged identity attacks.

The workflow of our proposed UAV identity management scheme is shown in Fig. 3 and summarized as follows.

Initialization: The system initializes the SIM cards of the UAV device and its pilot to generate the respective key pairs (i.e., public key and private key) and generate their respective blockchain addresses (i.e., their respective IDs) based on their respective public keys. The UAV communicates with the airspace through the associated 5G base station.

Registration: The UAV device and its pilot store their respective public keys and blockchain addresses (ID) on the blockchain. The airspace sets up access contracts (including the fee, access duration, and others) for the authorized UAV device and its pilot, and stores the smart contract on the blockchain.

Access Certification: Before takeoff, the UAV access certification must be issued by executing a smart contract based on the pilot ID and UAV device ID (dual-ID). When dual IDs and the contract are ensured, the UAV can be allowed to enter the requested airspace. The access certification will be stored on the blockchain as a transaction, and the authorization result will be sent back to the UAV.

Dual-ID Verification: Upon detecting that the UAV is approaching the airspace, the airspace will verify its identity integrity as follows. First, the airspace verifies dual IDs through the communication channel between the pilot and the airspace. Then, in response to the pilot's request, the UAV device

Item	Detail
Blockchain system	Ethereum private network and smart contract
Development kits	Raspberry Pi 3+
UAV	DJI Mavic2
SIM card	SIMoMe VAULT[15]
4G/5G module	NTU 5G MEC system -BLT-ISA11[5]

TABLE 1. The main hardware and software of PoC tests.

```
Require: main register address
1:  public struct Pilot {
2:      address pilot,
3:      string pilot_ID,
4:      string pilot_pbk
5:  };
6:  public struct UAVDevice {
7:      address UAVD // UAVDevice
8:      string UAVD_ID
9:      string UAVD_pbk
10: };
11: public struct Airspace {
12:     address airspace
13:     string airspace_ID
14:     string airspace_pbk
15:     uint pos_x
16:     uint pos_y
17: };
18: PolicyControlModifiers {
19:     Is sender = owner;
20:     Is sender_credit > tx_value;
21: }
22: ContractFunctions {
23:     if sender = UAVD_ID then
24:         register_UAVD();
25:     end if
26:     if sender = pilot_ID then
27:         register_pilot();
28:     end if
29:     if sender = airspace_ID then
30:         register_space();
31:     end if
32: }
```

CONTRACT 1. Identity registry contract.

```
Require: main authentication
1:  public mapping(string ID ->UAVD) id2UAVD;
2:  public mapping(string ID -> Pilot) id2Pilot;
3:  public mapping(string ID -> Airspace) id2Airspace;
4:  public mapping(string UAV_ID -> mapping( //
5:  airspace_ID -> boolean)) CertificateUAVD;
6:  public mapping(string pilot_ID ->mapping( //
7:  airspace_ID -> boolean)) CertificatePilot;
8:  PolicyControlModifiews {
9:    Is sender = owner;
10:   Is sender_credit > tx_value;
11: }
12: ContractFunctions {
13:   if sender = UAVD_ID then
14:  Get_Approval(UAVD_ID, pilot_ID, airspace_ID);
15:   end if
16:   if sender = airspace_ID then
17:     Authentication();
18:   end if
19: }
```

CONTRACT 2. Identity authentication contract.

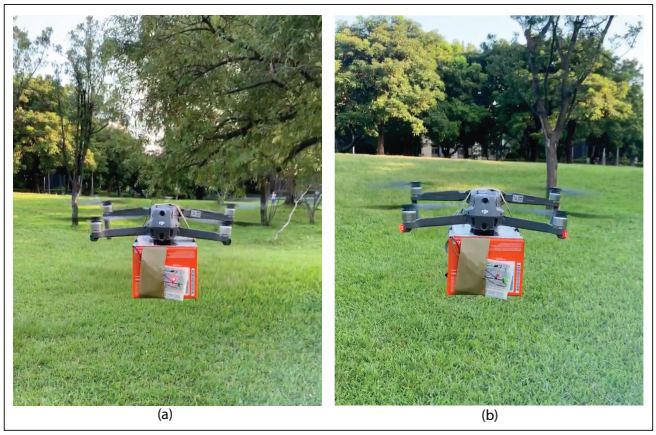

FIGURE 5. The results of two outdoor experiments: a) validation failed; b) validation passed.

sends its identity, public key, and the signed message information in reply to the pilot. Second, after the device responds, the pilot signs the message from the UAV device again. Finally, the pilot sends the dual IDs and the corresponding public keys, and the co-signed message back to the airspace for the authentication procedure described in the next step.

Authentication and Access Control: The airspace uses the two public keys of the UAV (i.e., the device and its pilot) stored on the blockchain to verify signed messages. Only after both the UAV device and its pilot are authenticated will the airspace issue an access certificate with the corresponding signature to the UAV device and its pilot.

POC System Implementation and Result Analysis

To validate the proposed solution, a proof of concept was built and tested via the 5G MEC testbed at National Taiwan University, as shown in Fig. 4. We deploy a server as the airspace and use a drone with two SIM cards as the UAV. Table 1 summarizes the main hardware and software for the PoC system implementation. We first initialize the SIM cards to generate and store blockchain key pairs and addresses by loading our Java applet into the Taysis SIMoME VAULT cards via globalplatformPro, an open source software to interact with the SIM cards. Then we build the Ethereum private testnet [4] on Ubuntu 18.04LTS and deploy the registry and the authentication smart contracts, as shown in the pseudo-codes of Contracts 1 and 2, respectively.

We demonstrate two typical cases, and the results are shown in Fig. 5. The green light in Fig. 5b indicates that the IDs of the pilot and the UAV device are both verified. In contrast, the red light in Fig. 5a shows that at least one ID failed during verification.

Note that in this article, we set the two SIM-card based hardware wallets as blockchain light nodes, and let them only handle blockchain transactions and signatures. Most of the computational burden falls on Ethereum miners, not on these two blockchain light nodes (hardware wallets). Therefore, these two blockchain wallets will not impose an energy burden on UAVs. According to our measurement results, the rated capacity of the two SIM-card-based blockchain hardware wallets is 2.553 Wh, which is only 4.255 percent of the DJI Mavic 2 Intelligent Flight Battery (60 Wh). Therefore, the information and control overhead of integrating the blockchain hardware wallets into each UAV is very small.

Conclusions

In this work, we design a blockchain-empowered authentication mechanism for UAV identity management in 5G networks. Existing UAV identity management work is mainly based on the blockchain software wallet and a single identity to authenticate UAV devices. We propose a dual-ID management method with a cross-layer design of cellular SIM cards, blockchain, and Ethereum smart contracts. By using the SIM card as the blockchain hardware wallet to store the key pair for identity and verification, our dual-ID model is based on two SIM cards per UAV, and conducts the verification for both IDs and their association. In this way, we can prevent identity forgery attacks on the access control of the service. We also implement a proof of concept of the system based on NTU's 5G network testbed, and the results demonstrate that the system is feasible and effective under our proposed UAV ID management framework.

Acknowledgment

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under the grant number of 110-2223-E-002 -004.

References

[1] W. Li, C. J. Mitchell, and T. Chen, "Oauthguard: Protecting User Security and Privacy with oauth 2.0 and openid connect," *5th ACM Wksp. Security Standardisation Research*, London, U.K., Nov., 2019, pp. 35–44.
[2] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain Envisioned UAV Networks: Challenges, Solutions, and Comparisons," *Comp. Commun.*, vol.151, Feb. 2020, pp. 518–38.
[3] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *IEEE Commun. Surveys & Tutorials*, vol. 18, no. 3, Mar. 2016, pp. 2084–2123.
[4] G. Wood, "ETHEREUM: A Secure Decentralised Generalised Transaction Ledger (EIP-150 REVISION)," Oct. 2017; http://gavwood.com/Paper.pdf, accessed Jan. 22, 2021.
[5] Y.-H. Hsu *et al.*, "NTU Smart Edge for Wireless Virtual Reality," *2020 Int'l. Conf. Consumer Electronics*, Taoyuan, Taiwan, Sept. 2020, pp. 375–89.
[6] D. Recordon and D. Reed. "OpenID 2.0: A Platform for Usercentric Identity Management," *2nd ACM Wksp. Digital Identity Management*, VA, Nov. 2006, pp. 11–16.
[7] M. Shen *et al.*, "Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT," *IEEE JSAC*, vol. 38, no.5, May 2020, pp. 942–54.
[8] L. Seitz *et al.*, "Use Cases for Authentication and Authorization in Constrained Environments," RFC 7744, Jan. 2016. DOI 10.17487/RFC7744.
[9] J. Chen, Y. Liu, and Y. Chai. "An Identity Management Framework for Internet of Things," *2015 12th Int'l. Conf. e-Business Engineering*, Beijing, China, Oct. 2015, pp. 360–64.
[10] G. Fragkos *et al.*, "Artificially Intelligent Electronic Money," *IEEE Consumer Electronics Mag.*, vol. 10, no. 4, July 2021, pp. 81–89.
[11] L. Lesavre *et al.*, "Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems," NIST Cybersecurtiy White Paper, Jan. 2020.
[12] A. Sghaier Omar and O. Basir, "Identity Management in IoT Networks Using Blockchain and Smart Contracts," *2018 IEEE Int'.l Conf. Blockchain*, Halifax, NS, Canada, Aug. 2018, pp. 994–1000.
[13] A. Kapitonov *et al.*, "Blockchain-Based Protocol of Autonomous Business Activity for Multi-Agent Systems Consisting of UAVs," *2017 Wksp. Research, Education and Development of Unmanned Aerial Systems*, Linkoping, Sweden, Oct. 2017, pp. 84–89.
[14] V. Sharma, I. You, and G. Kul, "Socializing Drones for Inter-Service Operability in Ultra-Dense Wireless Networks Using Blockchain," 2017 ACM Int'l.

Wksp. Managing Insider Security Threats, New York, NY, 2017, pp. 81–84.
[15] "SIMoMe VAULT"; http://taisys.com/, accessed Feb., 21, 2021.

Biographies

Ren Chen [S] (d03921017@ntu.edu.tw) received his M.S. degree from Chonnam National University, South Korea, in 2009, and he is currently a Ph.D. candidate in the Department of Electrical Engineering, National Taiwan University. He is an assistant professor in the Computer Network Department, Xiamen University of Technology. His research interests include blockchain security, consensus algorithms, and 5G wireless networks.

Hao-Wei Tseng (r08921a14@ntu.edu.tw) received his B.S. degree in mechanical engineering from National Taiwan University in 2019. He is currently pursuing an M.S. degree in the Department of Electrical Engineering, National Taiwan University. His current research interests include blockchain, machine learning, and cryptography.

Jie-Lin Lien (r08942159@ntu.edu.tw) received his B.S. degree in electrical engineering from National Taiwan University in 2019. He is currently pursuing an M.S. degree in the Department of Electrical Engineering, National Taiwan University. His current research interests include blockchain and machine learning for privacy preserving.

Wanjiun Liao [F] (wjliao@ntu.edu.tw) is a Chair Professor of Electrical Engineering at National Taiwan University, Taipei. Her research interests include 5G/6G, AI for networking, blockchain, and IoT. She is an Associate Editor of *IEEE Transactions on Mobile Computing* and is a Senior Editor of the *IEEE Systems Journal*. She has been very active in IEEE and the Communications Society (ComSoc), serving on the IEEE Fellow Committee, the IEEE ComSoc Fellow Evaluation Committee, as an IEEE ComSoc Distinguished Lecturer, IEEE ComSoc Board of Governors Member-at-Large, and IEEE ComSoc Chair of the Distinguished Lecturer Selection Committee.