A Self-Trading and Authenticated Roaming Scheme Based on Blockchain for Smart Grids

Xiaohan Hao, Wei Ren, *Member, IEEE*, Kim-Kwang Raymond Choo, *Senior Member, IEEE*, and Neal N. Xiong, *Senior Member, IEEE*

***Abstract*—The increasing volume of user and household data and number of smart meters compound the challenge of ensuring efficiency and privacy protection of electricity trading in existing smart grids. Therefore, to minimize the cost and latency in electricity trading, in this article, we design a new architecture for smart meters that can support transactions (using a blockchain-based wallet) and initiate transmission switch instructions (using smart contacts). Specifically, our approach comprises a decentralized peer-to-peer electricity trading scheme to enable automated electricity transmission (using smart contract instead of some centralized entity), and our blockchain-based anonymous authentication scheme to facilitate fast and privacy-aware roaming, in order to achieve privacy protection. We demonstrate that our proposed scheme is secure under the universally composable framework.**

***Index Terms*—Authentication, fair protocol, privacy protection, smart contract, smart grid.**

I. Introduction

In THE foreseeable future of smart grids, more participants will be involved in electricity trading and transmission. This is not surprising since the number of smart meters is also increasing rapidly [1]. There are, however, security and privacy considerations in the deployment of smart grids [2]. For example, approximately 230 000 customers were reportedly without power due to successful phishing email attacks against utility companies in Ukraine, and the failure of a smart grid was reported in Utah due to denial-of-service attacks [3]. In addition to cybersecurity threats, there are performance considerations. This necessitates the design of efficient and secure approaches to facilitate electricity trading.

There is a trend of moving away from third-party reliance to avoid limitations, such as single point of failure attacks and collusion attacks. Hence, there have been attempts to utilize blockchain to achieve privacy protection in electricity trading [4], [5], but there are a number of challenges associated with such blockchain-based approaches (e.g., optimization, fairness, and enhanced security in electricity trading). We also need to consider having in place mechanism that will allow users to report misbehavior or malicious activities, and for utility companies to impose penalty for misbehavior or malicious activities.

To address the aforementioned challenges, we propose a self-trading and authenticated roaming scheme based on blockchain for smart grids, designed to achieve automated, secure, and fair electricity trading and transmission. We claim our novel smart meters can be implemented in an integrated client, which can fast change the payment switcher and electricity control switcher to implement automatic trading. To resist some possible single point of failure attacks and collusion attacks, we design a decentralized peer-to-peer (P2P) electricity trading scheme without the existence of untrustworthy third parties. Besides, our scheme also meet the requirement with privacy protection through anonymous and roaming authentication. The contributions of this article are as follows.

1) We propose a new architecture for smart meters that can support *in situ* transactions by blockchain wallet and initiate transmission switch instructions by smart contacts. The electricity trading and electricity transmission thus can be implemented in an integrated client.
2) We propose a decentralized P2P electricity trading scheme that can enable automatically electricity transmission by smart contract after corresponding payments via blockchain are confirmed.

Manuscript received July 8, 2021; accepted October 3, 2021. Date of publication October 14, 2021; date of current version February 18, 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61972366, in part by the Provincial Key Research and Development Program of Hubei under Grant 2020BAB105, in part by the Foundation of Henan Key Laboratory of Network Cryptography Technology under Grant LNCT2020-A01, in part by the Foundation of Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences under Grant KFKT2019-003, and in part by the Foundation of State Key Laboratory of Public Big Data under Grant PBD2021- 02, Grant 2019BDKFJJ003, and Grant 2019BDKFJJ011. The work of Kim-Kwang Raymond Choo was supported only by the Cloud Technology Endowed Professorship. Paper no. TII-21-2868. *(Corresponding author: Wei Ren.)*

Xiaohan Hao is with the School of Computer Science, China University of Geosciences, Wuhan 430074, China (e-mail: xhhao@cug.edu.cn).

Wei Ren is with the School of Computer Science, China University of Geosciences, Wuhan 430074, China, with the Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China, and also with the Key Laboratory of Network Assessment Technology, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China (e-mail: weirencs@cug.edu.cn).

Kim-Kwang Raymond Choo is with the Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: raymond.choo@fulbrightmail.org).

Neal N. Xiong is with the Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK 74464 USA (e-mail: xiongnaixue@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3119963.

Digital Object Identifier 10.1109/TII.2021.3119963

3) We propose a blockchain-based anonymous authentication scheme for fast and privacy-aware roaming that can guarantee the protection of privacy, such as personal accounts and geographical positions.

The rest of this article is organized as follows. Section II gives an overview of the relevant previous work. In Section III, we present our system model and security requirements. Section IV illustrates the proposal and implementation of our scheme. In Section V, we evaluate the security and performance of our scheme. Finally, Section VI concludes this article.

II. Related Works

Traditional electricity trading schemes usually rely on a trusted third party, which may leak participants' information. To tackle the security and privacy challenges in smart grid, Wang *et al.* [6] utilized inner product encryption to imply a secure framework for sharing data in smart grid. To improve the security of trading, some other decentralized schemes have been proposed. A privacy protection and data aggregation scheme was proposed by Guan *et al.* [7]; Aggarwal *et al.* [8] proposed an electricity trading scheme between electric vehicles, charging stations, and utility centers; and Aitzhan and Svetinovic [9] utilized blockchain technology, multisignatures, and anonymous encrypted messaging streams to improve the security of transaction. Luo *et al.* [4] proposed a distributed electricity trading system to promote P2P trading among sellers and purchasers. To improve the self-sufficiency and photovoltaic consumption, Liu *et al.* [10] proposed a hybrid cyberphysical P2P energy sharing framework, which combines P2P physical system with client-server cybersystem. Besides, Kang *et al.* [5] proposed a local P2P power transaction model for local sellers and purchasers between electric vehicles in smart grid. To reduce the dependence on trusted third parties, Li *et al.* [11] utilized blockchain serves as a secure, tamper-proof distributed ledger to IoT devices, and each individual device can be assigned a unique ID and recorded on the blockchain.

With the number of devices in smart grid increasing rapidly, the efficiency may be greatly reduced. Since blockchain has the characteristics of immutability and traceability, there have been attempts to design blockchain-based solutions to achieve enhanced security and improved efficiency of electricity trading in IoT [12]–[15]. Lee [16] proposed a practical example to illustrate how blockchain-based ID as a service works as an identity and authentication management infrastructure for mobile telecommunication companies. Lin *et al.* [17] designed a cryptographic membership authentication scheme to support blockchain-based identity management systems, which binds a digital identity object to its real-world entity and allow singers use trapdoor hash function to effectively update certificates. Ao *et al.* [18] proposed an identity authentication scheme based on blockchain and identity-based cryptography (IBC), where the decentralized private key generator is implemented by deploying smart contracts in Ethereum blockchain. Wang *et al.* [19] proposed an identity signature scheme by security mediator (MED), which can revoke entity to solve the problem of instant identity revocation in IBC authentication system. To avoid information leakage when power company employees access the power system through mobile terminals and solve the authority dependence in traditional authentication process, Huang and Chen [20] proposed a blockchain-based power mobile terminal identity authentication mechanism, and Dang *et al.* [21] proposed a multidimensional identity authentication mechanism for power maintenance personnel based on blockchain, including a cross-domain authentication model composed of multiple distributed independent domains and a blockchain network.

Identity authentication and privacy protection are two important security issues in some industrial applications. Blockchain can ensure the correctness and nontampering of data in consensus mechanism, and avoid spreading wrong traffic information that may lead to misleading driving routes and traffic accidents. Thus, Malik *et al.* [22] proposed a blockchain-based vehicle network authentication and revocation framework, which can not only reduce the reliance on trusted organization authentication, but also quickly update the status of revoked vehicles in the shared blockchain ledger. Yang *et al.* [23] proposed a proof-of-event consensus concept applicable to vehicular networks and introduced a two-phase transaction on blockchain, which can send warning messages in appropriate regions and time periods.

Although there are a lot of research works in smart meters, the previous work also have some items need to be improved, such as cannot meet the requirement of fairness and security of authentication and electricity trading at the same time. We also compare our scheme with some related references, which is shown in Table I. Besides, most of the previous work was partially decentralized rather than completely avoiding the existence of third parties, thus some potential attacks may still exist. It is worth to note that the efficiency also needs to be improved to adapt to the limited resources of some edge devices. Therefore, this article propose a self-trading and authenticated roaming scheme based on blockchain for smart grid, which can fast automatic switch to complete automatic state change and improve the efficiency of trading on the premise of ensuring security.

III. System Model and Security Requirements

A. System Model

In our scheme, there are six entities: electricity participants, single-pole double-throw switchers (STDTSs), smart meters, smart contracts, blockchain wallets, and blockchain.

1) Electricity Participants: Electricity participants are including electricity seller and electricity purchasers. We assume that the seller wants to sell his redundant electricity to neighbors who need it. There are three states for each electricity participants: purchasing electricity, selling electricity, and being idle (there is no need to trade), and participants can show there states through their own smart meters. Before electricity trading, in order to ensure the identity of traders, the process of identity authentication needs to be performed.

2) Single-Pole Double-Throw Switchers: SPDTSs are special switchers that have three gears, that is, they are placed in the left, middle, and right by smart contracts to trigger three different operations: purchasing electricity, selling electricity, and being idle. It is worth to note that SPDTSs are controlled by smart

TABLE I
SCHEMES COMPARISON

	Kumari [24]	Mengelkamp [25]	Garg [26]	Zhang [27]	Aggarwal [28]	Our scheme
Fairness	×	✓	×	×	×	✓
Authentication	×	×	✓	✓	✓	✓
Privacy Protection	✓	Minimum level	✓	✓	✓	✓
Resist Attacks	✓	×	✓	✓	×	✓
pricing strategy	×	✓	Not mentioned	×	×	✓
Data authenticity	×	Not mentioned	×	✓	×	✓
Data integrity	✓	Not mentioned	×	✓	×	✓

contracts, according to the value of controlled account in smart meters.

3) Smart Meters: A smart meter is including two parts: blockchain wallet to pay money and SPDTSs to show the current state. According to the transaction cost, the SPDTSs are controlled by smart contract automatically to initiate transmission switch instructions and execute different operations.

4) Smart Contracts: Smart contracts can read the value of control accounts and then control SPDTSs to trigger corresponding behaviors autonomously, which can avoid the existence of trusted third parties to improve the security and efficiency of our scheme.

5) Blockchain Wallets: Blockchain wallets serve as blockchain clients, that is, when an electricity purchaser initiate a transaction, he will take part of the money out of blockchain wallet and give it to smart contract. On the contrary, after selling electricity, the electricity seller can put the money into his wallet for storage.

6) Blockchain: Blockchain as an account to record the identity of participants. Some traditional authentication models have semihonest third party, such as certificate authority, so there may exist single point of failure threats, which leads to the leakage of participants' privacy. We utilize the decentralization of blockchain to improve the security of our scheme. Besides, the immutable and traceability of blockchain can ensure the authenticity of the identity.

B. Security Requirements

At present, most authentication and trading processes rely on trusted third parties, which are susceptible to some potential attacks, such as single point of failure attacks and collusion attacks. In addition, with the increase of the number of electricity participants, the efficiency of centralized management cannot meet the demand of timely electricity supply. Therefore, to tackle aforementioned challenges, our main goal is designing a secure, autonomous, and efficient scheme that can resist various types of attacks and protect the participants' privacy. According to the previous research work, our scheme needs to meet the detailed following main requirements.

1) *Fairness:* We assume the seller and purchases are honest and inquisitive. After terminating transactions normally, the purchaser can get electricity, and the seller cannot refuse to supply electricity. Once one party has dishonest behavior, he will be punished.
2) *Autonomy and efficiency:* Since the existence of trusted third parties may lead to a series of threats, low efficiency, and unable to meet scalability of electricity trading. The autonomy and efficiency are also important security requirement for trading and authentication. Besides, since some edge devices in smart grids are resource-limited, thus the storage cost and responding time need to be reduced as small as possible.
3) *Payment-based and anonymous authentication:* Payment-based authentication means electricity participants can complete identity authentication after payment, which can improve the efficiency of authentication. Besides, electricity participants may worry about the exposure of their personal identity information or geographic location, so the anonymous is also an important requirement for authentication to protect participants' privacy.
4) *Privacy protection:* In the process of electricity trading, it is inevitable that they need to exchange or update some information that may divulge their personal privacy, such as their personal accounts and electric vehicle charging locations. This threat may leads to some participants reluctant to join in this trading and transmission process. Thus, privacy protection is also an indispensable security requirement when ensure the trading can be successfully completed.
5) *Attack resistance:* There are some potential threats in electricity trading and transmission. On the one hand, some potential attacks may from internal participants, such as a dishonest seller refuse to supply electricity or purchaser refuse to pay money. On the other hand, we assume that there is a probabilistic polynomial-time (PPT) attacker who attempts to intercept the normal trading and authentication process or sniff some transaction data, such as man-in-the-middle attacks, reply attacks, and eavesdropping attacks. Therefore, a secure trading scheme should resist these potential attacks.

IV. PROPOSED SCHEME

In this section, we will detail our proposed scheme from three parts: system framework, the process of identity authentication, and the process of controlling SPDTSs through smart contract. Key notations are described in Table II.

A. System Framework

Our proposed system is designed for smart grid environment. In the process of electricity trading, we design a new smart meter that can support *in situ* transactions by blockchain wallet and initiate transmission switch instructions by smart contacts. In order to ensure the security and improve the efficiency of electricity trading and electricity transmission, we propose a

TABLE II
NOTATION

A_a	Payment account A
A_b	Payment account B
C_a	Control switcher variable of account A
C_b	Control switcher variable of account B
C_B	Challenge Number
p	Electricity price per hour
P	Total amount of electricity
n	The quantity of electricity trading
M	The payment which the purchaser should pay for seller
U	The participants current power generation
V	The participants current power consumption
AP	The current average price in neighboring market
PK_A	The public key of participant A

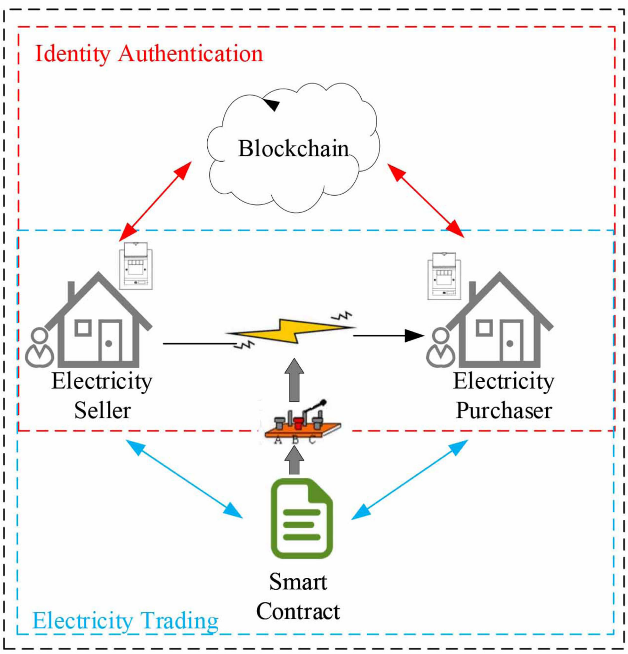


Fig. 1. System framework.

blockchain-based anonymous authentication scheme for fast and privacy-aware roaming.

In order to facilitate electricity trading, we design a novel smart meter that can be installed in every household. Specifically, there are two important parts in this smart meter, one is a blockchain wallet and the other is a SPDTS. Besides, we also set two types of account of electricity participants, that is, payment account and control account. According to the transaction cost of the blockchain, smart contract can read the value of control account and place the SPDTSs in corresponding gear to execute different operations and compete a two-way electricity trading (purchasing and selling electricity). After reading the value of control accounts, smart contracts can control the gear of SPDTSs to trigger different actions according to the value. It is worth to note that the identity authentication should be executed before electricity transmission.

As shown in Fig. 1, we will next elaborate our scheme through a top–down approach for describing electricity trading in smart grids: the main components of smart meters, the process of identity authentication, the process of controlling SPDTSs through smart contract, and the settlement process.

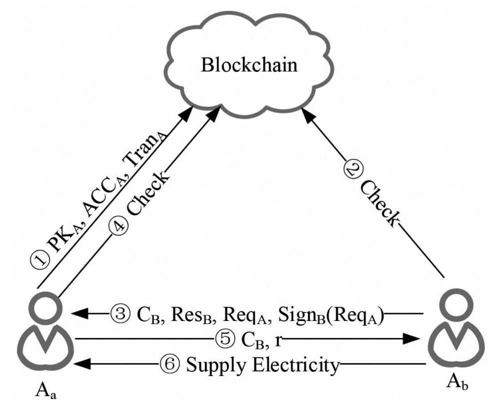


Fig. 2. System framework—identity authentication.

B. Main Components of Smart Meters

We design a new smart meter that includes two types of accounts to support *in situ* transactions by blockchain wallet and an SPDTS controlled by smart contacts. A_a and A_b are payment accounts who ask to trade electricity. We assume that A_b is a electricity seller with redundant electricity, which can be sold and A_a desires to buy electricity from A_b as an electricity purchaser. In order to control the electricity trading more convenient and protect participants' privacy, we assume C_a and C_b are corresponding control accounts. In addition, we set three value of control accounts: -1, 0, and 1. If the value is 1, it means that this account has redundant electricity, which can be sold; if the value is 0, it means that there is no need to initiate a transaction at present; if this value is -1, it means that the current account needs to buy electricity. After reading, the value of the SPDTS can be placed by smart contacts to different gear and initiate corresponding transmission switch instructions.

C. Process of Identity Authentication

In order to authenticate purchaser's identity, we set three labels, including Req_A, Res_B, and r

$$\mathrm{Req}_A = \; < \mathrm{PK}_A, \mathrm{ACC}_A, \mathrm{Tran}_A, \mathrm{Timestamp} >$$

$$\mathrm{Res}_B = \; < \mathrm{PK}_B, \mathrm{ACC}_B >$$

$$r = \mathrm{sign}_A(C_B, \mathrm{Req}_A, \mathrm{Req}_B, \mathrm{Sign}_B(\mathrm{Req}_A)).$$

Among them, ACC means the hash value of participants public key. That is, $\mathrm{ACC}_A = \mathrm{Hash}(\mathrm{PK}_A)$ and $\mathrm{ACC}_B = \mathrm{Hash}(\mathrm{PK}_B)$.

The specific steps are shown in Fig. 2 and the corresponding description is as follows.

1) A_a pays total amount of electricity P to smart contract, which can form a $\mathrm{Tran}_A =< A_a, A_b, P >$.
2) A_a broadcasts and uploads $\mathrm{PK}_A, \mathrm{ACC}_A$, and Tran_A on blockchain.
3) A_b verify these values, including the following.
   a) $\mathrm{ACC}_A \; \epsilon$ Blockchain?
   b) $\mathrm{Hash}(\mathrm{PK}_A) = \mathrm{ACC}_A$?
4) A_b sends $\mathrm{Res}_B, \mathrm{Req}_A, \mathrm{Sign}_B(\mathrm{Req}_A)$ to A_a.
5) A_a checks the following.

Algorithm 1: The Process of Identity Authentication.

Input: deposit of Alice *DepositA*, deposit of Bob *DepositB*, Token, *TimeStart*
Output: result of the transaction $Result_{Trans}$
if C_a = *-1 and* C_b = *1* **then**
  A_b sets the amount of *DepositA*, *DepositB* and *p*;
  A_a sends *DepositA* and P to smart contract, *TimeStart* = now;
  n = P / p;
  if *The amount of DepositA is right* **then**
    TimeCurr = now;
    if $TimeCurr - TimeStart \le n$ **then**
      A_a calculates ACC_A = Hash(PK_A) and $Tran_A$ = <A_a, A_b, P> ;
      A_a uploads PK_A, ACC_A and $Tran_A$ on blockchain;
      A_b verify the identity of A_a;
      if $ACC_A \epsilon Blockchain$ **then**
        if *Hash*(PK_A) = ACC_A **then**
          A_b calculates $Req_A =< PK_A, ACC_A, Tran_A, Timestamp >$ and $Res_B =< PK_B, ACC_B >$;
          A_b sends Res_B, $Req_A, Sign_B(Req_A)$ to A_a;
          A_a verify the identity of A_b;
          if $ACC_B \epsilon Blockchain$ **then**
            if *Hash*(PK_B) = ACC_B **then**
              if $Sign_B(Req_A)$ = *true* **then**
                A_a calculates r = $sign_A(C_B, Req_A, Req_B, Sign_B(Req_A)$;
                A_b checks whether *r* is valid and broadcasts *r*, Res_B and Req_A;
                A_b supplies electricity to A_a;
Return $Result_{Trans}$ = True;
else
  Return $Result_{Trans}$ = False;

a) ACC$_B \epsilon$Blockchain?
b) Hash(PK$_B$) = ACC$_B$?
c) Is Sign$_B$(Req$_A$) valid?

6) A_a sends C_B and *r* to A_b.
7) A_b checks whether *r* is valid and broadcasts *r*, Res$_B$, and Req$_A$.
8) A_b supplies electricity to A_a.

The specific algorithm of smart contract processing is shown in Algorithm 1.

D. Process of Controlling SPDTSs Through Smart Contract

In this section, we will elaborate the process of controlling SPDTSs through smart contracts, as shown in Fig. 3, and the specific algorithm is shown in Algorithm 2. According to the cost of blockchain transaction, electricity participants set the value of their current-controlled account. When smart contract finds that there are two nearby control accounts with the value of 1 and -1 at the same time, it means that there are two participants who can conduct electricity trading. Next, smart contracts initiate transmission switch instructions in different gears to execute different operations.

Algorithm 2: Controlling Switcher through Smart Contract.

Input: P, p, *TimeStart*
Output: C_a, C_b
$C_a = C_b = 0$;
A_a initiates a transaction request and pay P to smart contract;
The smart contract sets $C_a = -1$;
TimeCurr=now;
A_b calculates n = P / *p*;
if TimeCurr $-$ TimeStart $\le n$ **then**
  The smart contract sets $C_b = 1$;
Return C_a, C_b;

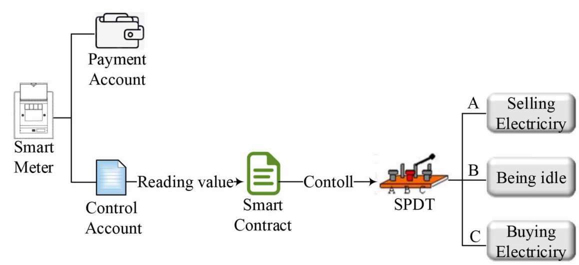


Fig. 3. Process of controlling switcher through smart contract.

E. Pricing Strategy and Settlement Process

Except the security, another main issue should be solved in electricity trading is the pricing strategy. In order to optimize the consumer electricity consumption patterns, the strategy of electricity pricing should be based on the consumption of participants and their neighbors, to encourage participants to use power off-peak. Srinivasan *et al.* [29] proposed a dynamic pricing strategy based on game theory and tested their method in Singapore. However, there are also existing some potential threatens, such as participants' electricity information needs to be transmitted to a center control, which brings some challenges during in real-time applications, such as data processing and transmission. In this article, the price of electricity should be decided by participants according to their own electricity situation and the current average price, instead of depending on the third party. First, smart contract calculates the average price of the current regional neighbor electricity market, named *AP* (average price), which is updated every 24 h. Since the calculation process is relatively simple, smart contract just calculate the average price of current neighboring electricity market, so the consumptions of calculation are not be very large. Next, participants can make accurate pricing by themselves according to their own electricity and current average transaction price

$$p = \mathrm{AP} - k * (U - V).$$

Among them, U is current power generation, V is current power consumption, k is a proportional coefficient, such as 0.8, and AP is the current average price in the neighboring market, that is, the current 24-h average transaction price is calculated in the ledger. It may bring some threatens if someone can connect participants with their electricity usage by observing their transaction price, according to the peak and through periods of the electricity consumption. However, as for participants, these information may not except to be leaked to others. Therefore, in order to protect the participants' privacy, it is worth to note that the record on ledger should be the smart meter manufacturer number instead of participants real identity.

After the electricity price is determined, how much the purchaser should pay for the seller can be calculated according to the current purchase quantity and price, that is, $M = p * n$. As for the purchaser, the corresponding number will be reduced, which can be reflected in the blockchain wallet. On the contrary, the number of seller blockchain wallet will be increased.

V. Security Analysis and Industrial Applications

A. Security Analysis

In this section, we will evaluate our solution from security perspective.

1) Fairness: If assuming all participants are honest, the best situation is that after completing electricity trading and transmission, the seller receives the payment and the purchaser gets the corresponding electricity. However, in our real life, some malicious behaviors may exist, such as the seller does not supply electricity after receiving the purchaser's money. Thus, our scheme claims that both seller and purchaser should pay the deposit to smart contracts before electricity trading starts. Once one party is found to be cheating, the deposit will be deducted and this participant will be blacklisted, then reducing his reputation value, which will affect future transactions.

2) Privacy Protection: Our scheme uses smart contract to control SPDTSs by reading the value of control accounts C_a and C_b, so as to trigger different operations (selling or buying electricity or not trading), instead of trading directly through the payment account A_a and A_b. By this way, the participants' privacy, such as personal accounts and geographical positions, can be protected. Our scheme can also achieve blockchain-based anonymous authentication scheme for fast and privacy-aware roaming of participants, that is, no one can know the real identity of the purchaser except seller. In the process of pricing strategy and settlement, the participants' identity is replaced by the vendor number of the smart meter. Therefore, our scheme can guarantee the protection of privacy efficiently.

3) Traceability and Authenticity: Our scheme adopts smart contract, which can avoid the existence of semihonest third parties during the process of electricity trading and identity authentication, and we also utilize a decentralized P2P electricity trading scheme that can enable automatically electricity transmission by smart contract, so it meets the requirement with traceability and authenticity.

4) Avoid Single Point of Failure and Collusion Attacks: Traditional identity authentication and electricity trading usually rely on some untrusted third parties, so there may exist single point of failure and collusion attacks, which leads to the leakage of participants' privacy. The single point of failure means as long as the third parties are occupied, the whole systems will be paralyzed. Collusion attack means that several participants can infer the privacy of another participant without authorization. Our proposed blockchain-based identity authentication can avoid a single point of failure by avoiding the existence of semihonest third parties.

5) Prevent Man-in-the-Middle Attacks: In the identity authentication process, we assume that there is an attacker named C trying to interfere with this process. On the one hand, if C generates a $\text{Res}_C =< \text{PK}_C, \text{ACC}_C >$ to replace Res_B and $\text{Sign}_C(\text{Req}_A)$, then sends Res_C and $\text{Sign}_C(\text{Req}_A)$ to purchaser A_a. It is easy for A_A to find this value is different from PK_B and ACC_B on the blockchain, thus A_A can refuse to continue next authentication steps. On the other hand, if C generates a $r' = \text{sign}_C(C_B, \text{Req}_A, \text{Req}_B, \text{Sign}_B(\text{Req}_A)$ and sends this value with C_B to A_b, since A_b knows PK_A and if A_b cannot use PK_A to verify this signature, it means r is wrong, so he can stop the authentication. Thus, with combining the public key system and digital signature, our scheme can prevent man-in-the-middle attacks efficiently.

6) Prevent Reply Attacks: Our scheme can resist reply attacks since the existence of timestamp during the electricity identity authentication process. The timestamp can be set according to the current time and embedded to value of Req_A to avoid some attackers resend the authentication messages. After receiving the value of r, if the participants find the value is not valid or the timestamp is not equal to the value of correct time, he/she can judge there may be some issues with this message.

In addition, we also compare our scheme with the other two schemes from five perspectives: privacy protection, decentralized, autonomy, identity authentication, and fairness. After comparison, we can conclude that our system meet all aforementioned conditions, whereas other schemes can only meet parts of them. Therefore, our system has good applicability and feasibility. The specific results are shown in Table III.

We also implement a universally composable (UC) security model and analyze the security of our identity authentication and verification protocols. First, the framework of UC was proposed by Canettig [30] in 1999. They defined three models: the real-life model, the ideal model, and the hybrid model. The comparison of these three models is shown in Table IV. Based on the theory of UC, we propose two ideal functionality F_{Auth} and F_{BL}. F_{Auth} implement the process of authentication scheme and F_{BL} implement the verification process in blockchain. In addition, we also design a protocol π_{Auth} to implement the authentication process. The implementation process of the authentication is similar to the steps mentioned in Section IV, the difference is that in our π_{Auth}, the external environment machine Z can provide protocol input and obtain all output during protocols' interaction.

We define the purchasers as $\{A_i \mid i = 1, 2, \ldots\}$, the sellers as $\{B_j \mid j = 1, 2, \ldots\}$, the dummy purchasers as $\{A'_i \mid i = 1, 2, \ldots\}$, and the dummy sellers as $\{B_j \mid j = 1, 2, \ldots\}$. Attacker S attempts to interfere with the transaction process.

The description of F_{Auth} is as follows.

TABLE III
SCHEMES COMPARISON

	Privacy Protection	Decentralized	Autonomy	Identity Authentication	Fairness
Our scheme	✓	✓	✓	✓	✓
Luo [4]	✓	✓	×	×	×
Kang [5]	✓	✓	✓	×	×

TABLE IV
MODELS COMPARISON

	The real-life model	The ideal model	The hybrid model
Component	The real-life protocol π The real-life participants P The real-life attackers A	A trusted third party that cannot be compromised-Ideal Functionality F The dummy participants P' The ideal attacker S	The real-life protocol π Ideal Functionality F The dummy participants P' The real-life attackers A The ideal attacker S
participants can communicate with each other	✓	×	✓

1) After receiving (active, trading) from Z, F_{Auth} sets the transaction tags of all traders to *trading*, when finding there exits, there are two control accounts at the same time as -1 and 1, respectively, then sends (initiate, A_i) and (initiate, B_j) to F_{BL}, and ignoring future A_i and B_j.
2) After receiving (initiate, trading, A_i) from A_i, F_{Auth} generates unique transaction identifier *req* = <PK$_A$, ACC$_A$, Tran$_A$, Timestamp>, then records (initiate, req, A_i) and sends it to S.
3) After receiving (initiate, trading, B_j) from B_j, if B_j is captured, F_{Auth} ignores this message; otherwise, F_{Auth} generates unique transaction identifier *res* = <PK$_B$, ACC$_B$>, then records (initiate, res, B_j) and sends it to S.
4) After receiving (initiate, res, B_j) and (initiate, req, A_i) from S, F_{Auth} replacing these two records to (trading, A_i, B_j, Timestamp), then sending (verify, A_i, B_j, Timestamp) to F_{BL}, if the checking result is true, B_j using F = {K, ● } to generate a random number C and sends (accept, C, Sign$_B$(req)) to S; otherwise, return false.
5) After receiving [accept, C, res, req, Sign$_B$(req)] from S, F_{Auth} sends (verify, Sign$_B$(req), res, req) to F_{BL}, if the checking result is true, A_i generates r = Sign$_A$ = $(C, \text{req}, \text{res}, \text{Sign}_B(\text{req}))$, then sends (accept, C, r) to S; otherwise, return false.

The description of F_{BL} is as follows.

1) After receiving (verify, A_i, B_j, Timestamp) from F_{Auth}, F_{BL} verifies whether ACC$_A\epsilon$Blockchain and whether Hash(PK$_A$) = ACC$_A$, if the aforementioned results are true, F_{BL} sets (accept, A_i, B_j, Timestamp) to S; otherwise, return false.
2) After receiving (verify, Sign$_B$(req), res, req) from F_{Auth}, F_{BL} verifies whether ACC$_B\epsilon$Blockchain, Hash(PK$_B$) = ACC$_B$ and whether Sign$_B$(Req$_A$) is valid, if the results are true, F_{BL} sets (accept, res, req) to S; otherwise, return false.

Theorem 1: If we assume that the smart contracts are safe, F = {K, ● } is an anticollision pseudorandom function and hash function is unidirectional, under the F_{BL} model, π_{Auth} can implement the ideal function F_{Auth} safely.

Proof:

Construction of simulator S: First, we conduct a simulator S, which is an ideal authentication attacker and it can call the external environment machine Z to simulate every action performed by a virtual real-life protocol as well get all information that the real-life attacker A can acquire. Specifically, if in a real-life protocol, A captures the real-life participant A_i or B_j, then S captures the dummy participants A_i' and B_j'. After the captured dummy participants A_i' or B_j' receives the message m from Z, S lets Z send m to A_i or B_j. Similarly, after A_i or B_j outputs message m to Z, S asks A_i' or B_j' to send message m to Z.

Operation of simulator S:

1) After receiving (initiate, req, A_i) from F_{Auth}, S generates a new req and sends (initiate, req, A_i) to A, and returns the feedback information to F_{Auth}.
2) After receiving (initiate, res, B_j) from F_{Auth}, if B_j is captured, S ignores this message; otherwise, S generates a new res and sends (initiate, res, B_j) to A, and return the feedback information to F_{Auth}.
3) After receiving (accept, C, Sign$_B$(req)) from B_j, if there is a record (trading, A_i, B_j, Timestamp), S Sign$_B$(req) and sends (accept, C, Sign$_B$(req)) to F_{Auth}.
4) After receiving (accept, C, r) from A_i, S generates a new r and sends (accept, C, r) to F_{Auth} F_{Auth}.
5) After receiving (accept, A_i, B_j, Timestamp) from F_{BL}, S sends it to A and verifies whether ACC$_A\epsilon$Blockchain and whether Hash(PK$_A$) = ACC$_A$, if the aforementioned results are true, S sets a new (accept, A_i, B_j, Timestamp) to F_{Auth}; otherwise, return false.
6) After receiving (accept, res, req) from F_{BL}, S sends it to A and verifies whether ACC$_B\epsilon$Blockchain, Hash(PK$_B$) = ACC$_B$ and whether Sign$_B$(Req$_A$) is valid, if the results are true, S a new sets (accept, res, req) to S; otherwise, return false.

Proof of Indistinguishability: Next, we prove the indistinguishability between the ideal protocol (simulated protocol) and

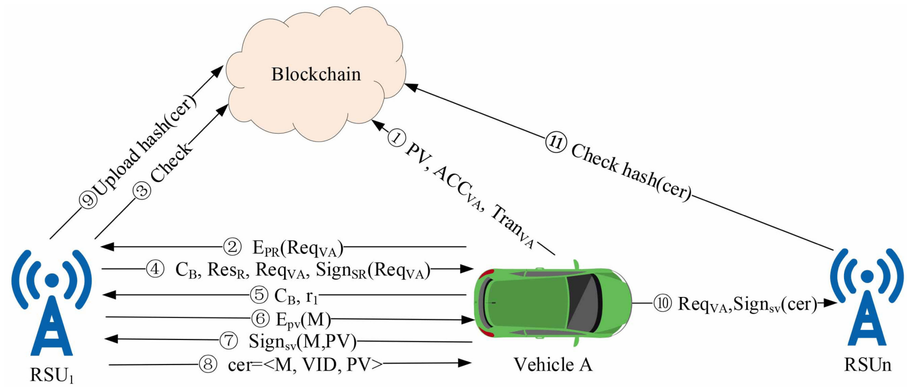


Fig. 4. Industrial applications.

the real-life protocol. We assume that there is a Z,' which can distinguish the interaction between S and simulation protocol π_{Auth} and the interaction between A and simulation protocol F_{Auth} in F_{BL}—hybrid model, that is, S can distinguish F_{Auth} and π_{Auth}. In other words, req, res, r, and ACC are distinguishable, which are calculated by hash function and random function F. Only Z can construct a PPT algorithm, which can distinguish random functions from random functions, and find a collision of hash functions. This violates the hypothesis of our theorem, so this hypothesis does not hold, and the ideal protocol and the real-life protocol are indistinguishable.

Through the aforementioned analysis, we believe that our scheme satisfies UC security, which means that our scheme can still guarantee security when executing parallel with other protocols.

B. Industrial Applications

As shown in Fig. 4, the proposed blockchain-based anonymous authentication scheme can also be applied for authentication of autonomous vehicles, as well as for unmanned aerial vehicle (UAV) autopilot certification. In vehicular ad hoc networks, all messages are forwarded anonymously, which brings up a problem—how to ensure the authenticity of the information? In addition, the communication messages usually contain the participants' personal information, such as personal accounts, geographic location, license plate number, etc. Therefore, identity authentication and privacy protection are two important issues in autonomous vehicles. Besides, how to prevent internal vehicles from spreading false information is also an important issue. Thus, we propose a blockchain-based anonymous authentication scheme for fast and privacy-aware roaming, which can be used for vehicle authentication to tackle aforementioned challenges. Due to the traceability, anonymity, and nontamperability of blockchain, applying our scheme in autonomous vehicles can not only resist single point of failure and collusion attacks by avoiding the existence of semihonest third party, but also can implement one-way authentication through blockchain to protect the participants' privacy, such as the location of electric charging point. As for the efficiency of authentication, since the whole scheme can enable automatically identity authentication by smart contract, our scheme is more efficient than most programs, which requires the participation of a third party.

TABLE V
NOTATION IN INDUSTRIAL APPLICATIONS

C_B	Challenge
VID	ID of vehicle A
PR	The public key of RSU_1
SR	The private key of RSU_1
PV	The public key of vehicle A
SV	The private key of vehicle A

There are many Nodes = <PK, PV, ACC>in the organization management, which can be the monthly fee paid on the 1st of each month or the annual fee on New Year's day. We assume that A is an automatic driving vehicle. While driving in current field, A can request services from rate-sensor units RSUs) in this fields. More specificity, there are three parties, including A, RSU_1, and RSU_n. A is a vehicle that requests authentication, RSU_1 is one of multiple RSUs in this field, and RSU_n represents other RSUs in this field, $n = 2, 3, 4, \ldots$, which can support services for A. After paying *Fee*, a blockchain-based identity authentication starts. Next, we will describe how our scheme can be performed. Table V lists the notations used in autonomous vehicles' identity authentication.

The process of identity certification is as follows.

1) A uploads $\text{PV}, \text{ACC}_{\text{VA}} = \text{Hash}(\text{PV}), \text{Tran}_{\text{VA}} = <\text{PV}, \text{SV}, \text{ACC}_{\text{VA}}>$ on blockchain.
2) A calculates $\text{Req}_{\text{VA}} = <\text{PK}_{\text{VA}}, \text{ACC}_{\text{VA}}, \text{Tran}_{\text{VA}}, \text{Timestamp}>$ and sends $E_{\text{PR}}(\text{Req}_{\text{VA}})$ to RSU_1 to trigger the progress of identity authentication.
3) RSU_1 uses SR to decrypt $E_{\text{PR}}(\text{Req}_{\text{VA}})$ and gets Req_{VA}, then check this value on blockchain.
4) After successful verification, RSU_1 calculates $\text{Res}_R = <\text{PK}_{\text{PR}}, \text{ACC}_R>$and $\text{Sign}_{\text{SR}}(\text{Req}_A)$, then sends C_B, $\text{Res}_R, \text{Req}_{\text{VA}}, \text{Sign}_{\text{SR}}(\text{Req}_{\text{m}})$ to A.
5) After verifying the signature, A calculates $r_1 = \text{sign}_{\text{VA}}(C_B, \text{Req}_{\text{VA}}, \text{Req}_R, \text{Sign}_{\text{SR}}(\text{Req}_{\text{VA}})$ and then sends C_B and r_1 to RSU_1.

Until this step, RSU_1 can determine the identity of A. Next, in order to achieve the goal of one party authentication and multiparty service, that is, once a certain RSU is authenticated, the car only needs to show the certificate when passing through other RSUs in the current field, and there is no need to conduct identity authentication again. The process of issuing certificates is as follows.

1) RSU_1 use *PV* to encrypt a random number and sends the $E_{\mathrm{PV}}(M)$ to A.
2) A uses *SV* to decrypt the received value and gets *M*, then A generates $\mathrm{Sign}_{\mathrm{SV}}(M, \mathrm{PV})$ and send it to RSU_1.
3) RSU_1 generates cer $=< M, \mathrm{VID}, \mathrm{PV} >$ and sends this certificate to A.
4) RSU_1 calculates hash(cer) and uploads it on blockchain, which can be used to verify the authenticity of cer for other RSUs.
5) When A passes by RSU_n and wants to get the corresponding service, such as traffic information, A sends $\mathrm{Req}_{\mathrm{VA}}$ and $\mathrm{Sign}_{\mathrm{SV}}(\mathrm{cer})$ to RSU_n.
6) RSU_n uses *PV* to get cer and check hash(cer) on blockchain.

VI. Conclusion

In this article, we proposed a self-trading and authenticated roaming scheme based on blockchain for smart grid. We implemented our scheme by designing a smart meter, including a blockchain wallet and an SPDTS. The scheme we proposed ensured that electricity participants can authenticate and trading autonomously. We also proposed a blockchain-based anonymous authentication scheme for fast and privacy-aware roaming that can guarantee the protection of privacy. Through the security analysis based on UC security framework, we proved the feasibility and efficiency of our scheme. Besides, we also proposed that our scheme can also be applied for authentication of autonomous vehicles and UAV autopilot certification. In the future work, we will first consider adding real testing to prove the performance and feasibility of our scheme, then we will consider the forecasting of electricity trading on the premise of protect privacy, such as predicting the best time to purchase energy by analyzing participants' electricity consumption behavior. In addition, we also consider adding the function of anomaly detection to our scheme in the suture research.

References

[1] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3125–3148, May 2019.

[2] K. Li *et al.*, "A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid," *Comput. Secur.*, vol. 103, 2021, Art. no. 102189. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102189

[3] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for cybersecurity in smart grid: A comprehensive survey," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 3–19, Jan. 2021.

[4] F. Luo, Z. Y. Dong, G. Liang, J. Murata, and Z. Xu, "A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4097–4108, Sep. 2019.

[5] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[6] Y. Wang *et al.*, "SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain and smart contract," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7688–7699, Nov. 2021.

[7] Z. Guan *et al.*, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[8] S. Aggarwal, N. Kumar, and P. Gope, "An efficient blockchain-based authentication scheme for energy-trading in V2G networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6971–6980, Oct. 2021.

[9] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.

[10] N. Liu *et al.*, "Online energy sharing for nanogrid clusters: A Lyapunov optimization approach," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4624–4636, Sep. 2018.

[11] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *Proc. 27th Int. Conf. Comput. Commun. Netw.*, 2018, pp. 1–6, doi: 10.1109/ICCCN.2018.8487449.

[12] J. Wang, L. Wu, K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 1984–1992, Mar. 2020.

[13] Z. Cui *et al.*, "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Trans. Serv. Comput.*, vol. 13, no. 2, pp. 241–251, Mar./Apr. 2020.

[14] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *Proc. IEEE/ACS 15th Int. Conf. Comput. Syst. Appl.*, 2018, pp. 1–8.

[15] M. T. Hammi *et al.*, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, 2018. [Online]. Available: https://doi.org/10.1016/j.cose.2018.06.004

[16] J. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018.

[17] C. Lin, D. He, X. Huang, M. K. Khan, and K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," *IEEE Access*, vol. 6, pp. 28203–28212, 2018.

[18] W. Ao, S. Fu, C. Zhang, Y. Huang, and F. Xia, "A secure identity authentication scheme based on blockchain and identity-based cryptography," in *Proc. IEEE 2nd Int. Conf. Comput. Commun. Eng. Technol.*, 2019, pp. 90–95.

[19] J. S. Wang and S. Li Wei, "Identity-based cross-domain authentication by blockchain via PKI environment," in *Blockchain Technology and Application*, X. H. Si, Y. Jin, J. Sun Zhu, L. Zhu, X. Song, and Z. Lu, Eds. Singapore: Springer, 2020, pp. 131–144.

[20] H. Huang and X. Chen, "Power mobile terminal identity authentication mechanism based on blockchain," in *Proc. Int. Wireless Commun. Mobile Comput.*, 2020, pp. 195–198, doi: 10.1109/IWCMC48107.2020.9148258.

[21] F. Dang, F. Gao, H. Liang, and Y. Sun, "Multi-dimensional identity authentication mechanism for power maintenance personnel based on blockchain," in *Proc. Int. Wireless Commun. Mobile Comput.*, 2020, pp. 215–219, doi: 10.1109/IWCMC48107.2020.9148178.

[22] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur., Privacy Comput. Commun./ 12th IEEE Int. Conf. Big Data Sci. Eng.*, 2018, pp. 674–679.

[23] Y. Yang, L. Chou, C. Tseng, F. Tseng, and C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[24] A. Kumari, R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "When blockchain meets smart grid: Secure energy trading in demand response management," *IEEE Netw.*, vol. 34, no. 5, pp. 299–305, Sep./Oct. 2020.

[25] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.- Res. Develop.*, vol. 33, no. 1, pp. 207–214, 2018.

[26] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, and J. J. Rodrigues, "An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment," in *Proc. IEEE Int. Conf. Commun. Workshops*, 2019, pp. 1–6.

[27] S. Zhang, J. Rong, and B. Wang, "A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain," *Int. J. Elect. Power Energy Syst.*, vol. 121, 2020, Art. no. 106140.

[28] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, and N. Kumar, "EnergyChain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem," in *Proc. 1st ACM MobiHoc Workshop Netw. Cybersecurity Smart Cities*, 2018, pp. 1–6.

[29] D. Srinivasan *et al.*, "Game-theory based dynamic pricing strategies for demand side management in smart grids," *Energy*, vol. 126, pp. 132–143, 2017. [Online]. Available: https://doi.org/10.1016/j.energy.2016.11.142

[30] R. Canettig, "Security and composition of multiparty cryptographic protocols," *J. Cryptol.*, vol. 13, no. 1, pp. 143–202, 2000, doi: 10.1007/s001459910006.

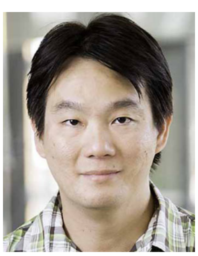
Xiaohan Hao received the bachelor's degree in engineering information security from the China University of Geosciences, Wuhan, China, in 2020.

Since 2020, she has been a Student with the School of Computer Science, China University of Geosciences, China University of Geosciences. Her research interests include blockchain and Internet of Things security.

Wei Ren (Member, IEEE) received the Ph.D. degree in computer science from the Huazhong University of Science and Technology, Wuhan, China, in 2006.

Since 2014, he has been a Full Professor with the School of Computer Science, China University of Geosciences, Wuhan. From 2009 to 2013, he was an Associate Professor with the School of Computer Science, China University of Geosciences. He was with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, USA, in 2007 and 2008; the School of Computer Science, University of Nevada Las Vegas, Las Vegas, NV, USA, in 2006 and 2007; and the Department of Computer Science, The Hong Kong University of Science and Technology, Hong Kong, in 2004 and 2005. He has authored or coauthored more than 100 refereed papers, one monograph, and four textbooks.

Prof. Ren was a recipient of 20 patents and five innovation awards. He is a Distinguished Member of the China Computer Federation.



Kim-Kwang Raymond Choo (Senior Member, IEEE) received the Ph.D. degree in information security from the Queensland University of Technology, Brisbane, QLD, Australia, in 2006.

He currently holds the Cloud Technology Endowed Professorship with The University of Texas at San Antonio (UTSA), San Antonio, TX, USA.

Dr. Choo is the founding Co-Editor-in-Chief of ACM Distributed Ledger Technologies: Research and Practice, and the founding Chair of the IEEE Technology and Engineering Management Society's Technical Committee on Blockchain and Distributed Ledger Technologies. He currently serves as the Department Editor of IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, the Associate Editor of IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, and IEEE TRANSACTIONS ON BIG DATA, and the Technical Editor of IEEE NETWORK MAGAZINE. He is an ACM Distinguished Speaker and IEEE Computer Society Distinguished Visitor (2021–2023), and included in Web of Science's Highly Cited Researcher in the field of Cross-Field—2020. He was the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, the Outstanding Associate Editor of 2018 for IEEE ACCESS, the British Computer Society's 2019 Wilkes Award Runner-Up, the 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, the Fulbright Scholarship in 2009, the 2008 Australia Day Achievement Medallion, and the British Computer Society's Wilkes Award in 2008. He was also the recipient of Best Paper Awards from IEEE SYSTEMS JOURNAL in 2021, *IEEE Consumer Electronics Magazine* for 2020, *Journal of Network and Computer Applications* for 2020, *EURASIP Journal on Wireless Communications and Networking* in 2019, IEEE TrustCom 2018, and ESORICS 2015; the Korea Information Processing Society's *Journal of Information Processing Systems* Outstanding Research Award (Most-Cited Paper) for 2020 and Survey Paper Award (Gold) in 2019; the IEEE Blockchain 2019 Outstanding Paper Award; and Best Student Paper Awards from Inscrypt 2019 and ACISP 2005.

Neal N. Xiong (Senior Member, IEEE) received the Ph.D. degree in sensor system engineering from Wuhan University, Wuhan, China, in 2007, and the Ph.D. degree in dependable communication networks from the Japan Advanced Institute of Science and Technology, Nomi, Japan, in 2008.

He is currently an Associate Professor (6th year) with the Department of Mathematics and Computer Science, Northeastern State University, Tahlequah, OK, USA. Before he attended Northeastern State University, he was with Georgia State University, Atlanta, GA, USA; Wentworth Institute of Technology, Boston, MA, USA; and Colorado Technical University, Colorado Springs, CO, USA (a Full Professor for about five years) for about ten years. He has authored or coauthored more than 200 international journal papers and more than 100 international conference papers. Some of his works were published in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS (JSAC), IEEE or ACM Transactions, ACM Sigcomm Workshop, IEEE INFOCOM, ICDCS, and IPDPS. His research interests include cloud computing, security and dependability, parallel and distributed computing, networks, and optimization theory.

Dr. Xiong is a General Chair, Program Chair, Publicity Chair, Program Committee Member, and Organizing Committee Member of more than 100 international conferences, and a reviewer of about 100 international journals, including IEEE JSAC, IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS (Park: A/B/C), IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON MOBILE COMPUTING, and IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS. He is serving as an Editor-in-Chief, Associate Editor, or Editor Member for more than ten international journals (including an Associate Editor for IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, an Associate Editor for the IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, an Associate Editor for *Information Science*, an Editor-in-Chief for the *Journal of Internet Technology*, and an Editor-in-Chief for the *Journal of Parallel & Cloud Computing* (PCC)), and a Guest Editor for more than ten international journals, including *Sensor Journal*, *Wireless Networks*, and *Mobile Networks and Applications*. He was the recipient of the Best Paper Award in the 10th IEEE International Conference on High Performance Computing and Communications in 2008 and the Best Student Paper Award in the 28th North American Fuzzy Information Processing Society Annual Conference in 2009.