Ren *et al. EURASIP Journal on Wireless Communications and Networking* (2020) 2020:152
https://doi.org/10.1186/s13638-020-01762-w

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A novel authentication scheme based on edge computing for blockchain-based distributed energy trading system

Yan Ren[1], Qiuxia Zhao[1], Haipeng Guan[1] and Zhiqiang Lin[2*]

*Correspondence:
linzhiqiang0824@163.com
[2]School of Mathematics and Information Science, Guangzhou University, 510006 Guangzhou, China
Full list of author information is available at the end of the article

Abstract

Distributed energy trading system is a new business model of energy industry. Applying blockchain technology, energy supply contracts can be communicated directly between producers and consumers. However, blockchain is without any identity authentication and legitimate user identities are possibly forged if there is not any user identity authentication procedure in a trading system. In this paper, we design an authentication scheme for blockchain-based energy trading systems by using edge computing, including journalizing processes, registration, and identity authentication. In our scheme, each node has computing power, which can ensure the meter data can be processed locally or on the edge. In addition, the correctness and security analysis of the scheme are also given in this paper. The analysis shows that our scheme is unforgeability and can protect users' privacy.

Keywords: Edge computing, Blockchain, Authentication scheme, Energy trading system, Consensus

1 Introduction

1.1 Background and motivation

Blockchain is a shared distributed ledger that records transactions in a public or private peer-to-peer network. The ledger is distributed to all member nodes in the network, and the history of asset transactions occurring between peer nodes in the network is permanently recorded in the block. As the core technology of distributed ledger technology (DLT) system, blockchain is considered to have broad application prospects in many fields such as finance, Internet of Things, commercial trade, credit reporting, and asset management [1].

As a new generation of energy supply mode, distributed energy system is a powerful supplement to centralized energy supply system. A distributed trading system should be designed to adapt multiple energy suppliers and consumers. Blockchain technology can be applied to construct a distributed energy trading system. Actually, there are many researches on blockchain-based energy trading systems [2–10]. The literature [2] conducted a preliminary economic evaluation of the market mechanism of blockchain

application in the local energy market. In [3], the author compares the business model and characteristics of P2P power transaction and emphasizes the sustainable development of P2P ICUE 2018 green energy. In [4], the author demonstrated a blockchain implementation that can be used for energy auctions in the campus environment. The authors discuss the components of the microgrid energy market related to the Brooklyn microgrid project in [5]. The authors discuss business models that ensure transparency for energy consumers in [6]. Blockchain technology has also realized several other energy-related applications, such as the use of blockchain in island microgrids to identify energy losses [7] and the application supporting emissions trading [8]. In [9], the authors review the way blockchain technology works in the context of the Internet of Things (IoT). A secure energy trading system was proposed in [10].

In addition, many enterprise projects are also focused on the application of blockchain technology in the field of energy [11–20], such as the PowerLedger project which provides a peer-to-peer marketplace for renewable energy [11]. Its white paper [12] continues to discuss system architecture and ecosystems. The Brooklyn Microgrid Project developed by New York startup LO3 Energy [13] is dedicated to creating a blockchain-based P2P trading system that delivers electricity to hospitals, shelters, and community centers when needed. Dajie project in [14] provides a blockchain-based platform that allows P2P energy exchange, redeems carbon credits for consumers, and pays for energy companies' energy and services. The Shared Charging Project [15] provides a solution for charging electric vehicles on an open network developed on the Ethereum blockchain [16], which provides seamless access to charging poles in different countries. NRGcoin project [17] provides incentives for the production of green energy. The concept is similar to the solar coin project [18], where one of the solar coins represents 1 MWh of solar power. The solar exchange program [19] allows individuals to purchase or lease solar battery by using bitcoin or local currency. An electronic project initiated by the UK in the literature [20], which runs on Ethereum, provides a flexible block-based trading platform that supports electricity, natural gas, and community energy. Enerchain project [21] focuses on the use of blockchain technology for P2P transactions in the wholesale energy market.

However, many security issues such as identity authentication, the realization of consensus mechanism, and privacy protection are not mentioned in these systems. This paper focus on the identity authentication of users for the blockchain-based energy trading systems.

1.2 Related work

Currently, there are some blockchain-based identity authentication schemes [22–27]. These researches can be divided into two categories. One is based on government platforms. The goal is to create a blockchain-based world or national identity registration system and provide some government services [22–25]. Another one is for companies; its aim is to complete the identity registration authentication services with blockchain [26, 27]. Moreover, several blockchain-based authentication schemes for smart grid were proposed over the last several years [28–31]. A blockchain identity management system based on public identities ledger is discussed in [32]. Unfortunately, among these schemes, the important node is the smart grid. They only considered how to complete the certification for smart grid. In the general energy trading system, there is no smart

grid, and more participants are users. We focus on how to implement user identity authentication in such a system.

Edge computing is a way of processing data that is physically close to where the data is generated. Edge computing is relative to cloud computing. There is much literature on the application of edge computing [33–47]. In an edge computing-based blockchain system, each device needs to pay a certain amount of deposit. Each device is a node, a witness, a trusted oracle, and a judge with clear rewards and punishments. No one even needs to participate. People just need to enjoy a credible society, and the rest is done by the marginal computing block chain.

1.3 Our contribution

In order to solve the problem of identity authentication in blockchain-based energy trading system, we design an edge computing-based authentication scheme for blockchain-based distributed energy trading systems (ECAS-BDETS), which includes three processes named as journalizing, registration, and identity authentication. Our scheme can ensure unforgeability and privacy. In addition, the correctness and security analysis of the scheme are also given in this paper. The main contributions of this paper include:

1. In the process of journalizing, we use the proof of stake (PoS) plus credit score to complete the bookkeeper selection. To avoid regional managers with more transactions which tend to get higher credit score, we randomly select one of the regional managers with honor values greater than or equal to k each time.
2. In the process of user registration, we ensure that the user's identity cannot be forged by processing and storing the user identity information in the block chain based on the tag and Merkle tree principle.
3. In the process of identity authentication, the user's identification is realized by using digital signature technology and time stamp.

1.4 Organization of this paper

The rest of the paper is organized as follows. Preliminaries are given in Section 2. In Section 3, we formally define the framework and security requite for blockchain-based authentication scheme for energy trading system. The proposed scheme is presented in Section 4. An example of our scheme will be presented in Section 5. We analyze the security of the proposed scheme and compare it with other related schemes in Section 6. In Section 7, our scheme is compared with some existing schemes in terms of function. Finally, conclusions and future work are given in Section 8.

2 Preliminaries

In this section, we briefly introduce some knowledge of Merkle tree and signature, which are necessary for the subsequent development.

2.1 Merkle tree

Merkle Tree, also known as a "Hash Tree," as the name implies, is a tree that stores hash values. A leave node of a Merkle tree is attached the hash value for a data block. A non-leaf node is attached the cryptographic hash of its corresponding child nodes.

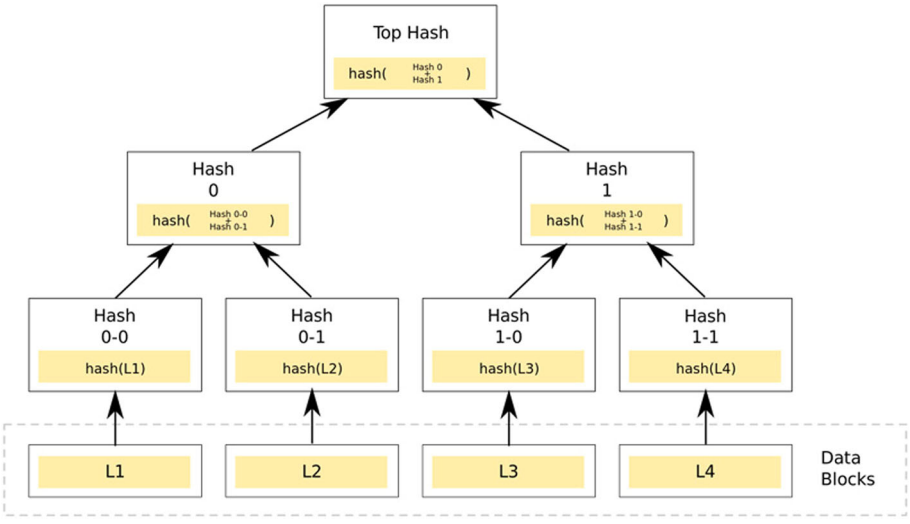

Fig. 1 An example of a Merkle Tree. The working mechanism of Merkle tree

Figure 1 presents a simple example of a Merkle Tree. Let $D = \{L_1, L_2, L_3, L_4\}$ to denote the set of data. In the leaf nodes, $Hash(ij) = H(L_k)$, where $i, j \in \{0, 1\}, k \in \{1, 2, 3, 4\}$, H is a hash function. In the nodes inside, each of H_0 and H_1 has a left child denoted by $(i, 0)$ and a right child denoted by $(i, 1)$. A hash value, which is computed by $H(i) = H(Hash(i0), Hash(i1))$ is stored by each internal node. Top Hash denotes the root node. It stores a hash value computed by $H(H(0), H(1))$.

2.2 Signature scheme

Digital signature is a digital string that can only be generated by the sender of the information and cannot be forged by others. This digital string is also an effective proof of the authenticity of the information sent by the sender. It is based on public key cryptography and can be used for identification. In general, a digital signature scheme is a tuple of three probabilistic polynomial time (PPT) algorithms $Sig = (Sig.Gen, Sig.Sign, Sig.Vrf)$ such that:

- SIG.Gen: $Sig.Gen(1^{\lambda})$ takes in a security parameter and outputs a verification key vk and a signing key sk.
- SIG.Sign: $Sig.Sign(sk, m)$ takes in a signing key sk and a message m and outputs a signature σ on message m under signing key sk.
- SIG.Vrf: $Sig.Vrf(vk, m, \sigma)$ takes in a verification key vk, a message m, and a signature σ and outputs 1 if the signature is valid and 0 otherwise.

A complete digital signature should include the following three mechanisms:

- The signer cannot deny his signature after signing.
- Others cannot forge a signature.
- If the parties dispute the authenticity of the signature, the validity of signature can be verified by a fair arbitrator.

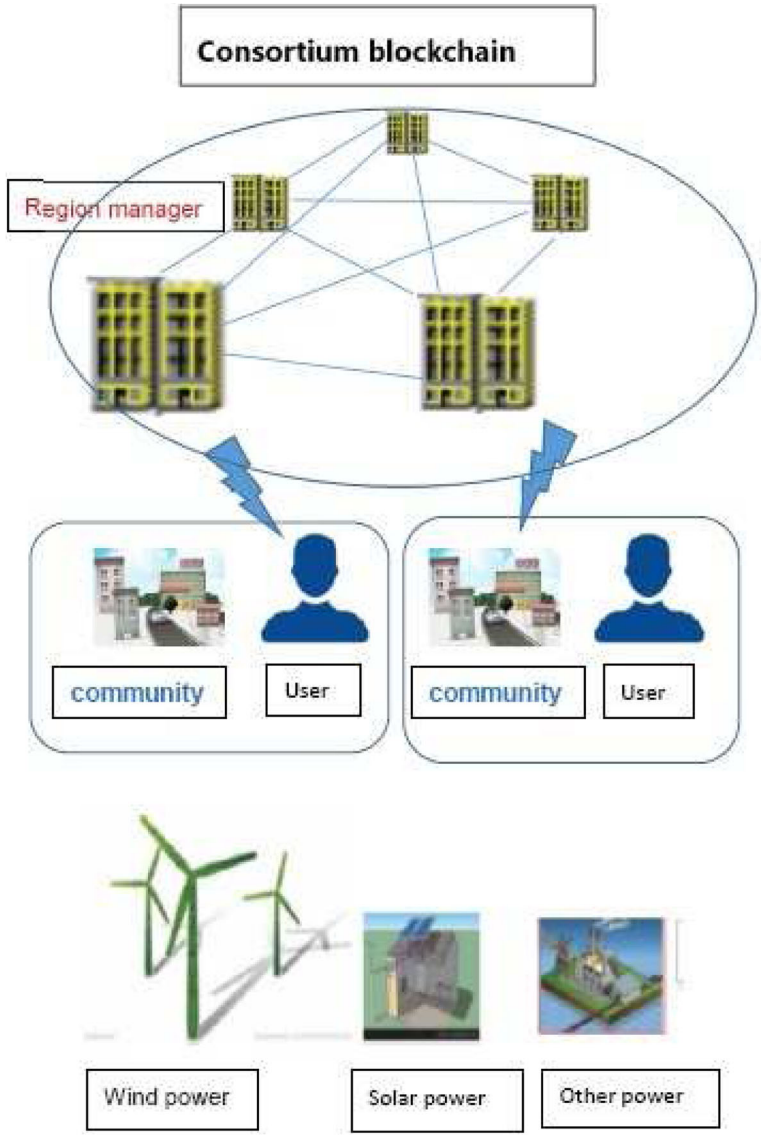

Fig. 2 The system structure. The system of our scheme consists regional manager, the communities and users

3 Security model

3.1 The system structure

The system of our scheme consists of two parts, i.e., regional manager and the communities and users. Figure 2 shows the system structure.

The regional manager, conducted as the energy management center of a certain region, is responsible for the management and transaction information of the blockchain. It completes the registration of new users and the identity authentication of users in the process of transaction and can trade with other regional managers according to the electricity consumption in the region.

Communities and users can send transaction requests to the regional manager, including buy, sell, and so on, depending on their situation. Because the community and the user have the same functional needs, we treat the community as a user in our system.

3.2 Security requirement

In ECAS-BDETS, we assume the user and the regional manager are semi-honest. It means that they will run the protocol honestly, but they will collect information from other users maliciously for forged identity. According to the requirements of the identity authentication scheme, we present security goals for a blockchain-based energy trading system.

- *Correctness.* We require that the identity authentication process is correct. Namely, if both of the user and the regional manager follow the proposed protocol, the identity authentication can be verified.
- *Unforgeability.* In our scheme, the identity of a legitimate user will not be forged. A forged identity will not pass verification.
- *Privacy.* User identity information will be hidden. The identity of the user in our scheme is replaced by the value of the root node of a Merkle tree. Neither the regional manager nor other users will know the true identity of the user.

Remark 1 *Because the semi-honest model is more common in actual production and life, it is necessary to consider the semi-honest opponent alone, so we choose the semi-honest model.*

Remark 2 *The participants in the semi-honest model follow the execution of the protocol, but preserve the intermediate computed state of the protocol.*

4 Our construction

ECAS-BDETS consists of two parts: one is the regional manager, anthrone is user. Both the regional manager and the user are considered nodes. We assume that every regional manager has a key pair (Pk_M, Sk_M) and the user has a key pair (Pk_i, Sk_i). Three operating steps namely, process of journalizing, the user registration, and identity authentication are described as follows.

4.1 Process of journalizing

In the accounting process, the consensus mechanism is the most important. In bitcoin, the proof of work (PoW) and the proof of stake (PoS) are used for gaining the right to account. Since our scheme is based on edge calculations, we regard the participants in the blockchain as nodes and use the credit score to obtain the accounting permission. In order to avoid some people have more opportunities to get higher credit score, we randomly select one of the nodes with honor values greater than or equal to k each time.

1. The initial credit score for each transportation is n. In the first round of voting, because the credit score is the same, each node randomly selects a node as the accounting node, and the one with the most votes will be the bookkeeper.
2. If there is a transaction, in the end of every transaction, both parties give each other a score s according to each other's performance in this activity. The score range is $[-\beta, \beta]$.
3. Node generates the signature $Sign(s, t)$ for the credit score and sends the signature to bookkeeper, where t is the current time.

4. Bookholder receives the signature; he first checks if the signature is valid. If it is valid, he broadcasts the credit score computed below in the blockchain.

$$C = \alpha * n + (1 - \alpha) * s,$$

where n is the credit score before this transaction, s is the score in the current accounting period and α is a number with range $[0, 1]$, representing a weight value.

Remark 3 *This value can be adjusted as needed. If you think the previous credit is more important, you can take a larger value. If you think the current credit score is more important, you can take a smaller value.*

4.2 User registration

Firstly, a new user should choose a manager which she belongs to and sends the registration request to the regional manager. The regional manager helps her register with her identification through an interactive protocol. The sketch of the protocol as shown in Fig. 3 and detail described as follows.

- User
  User O does the following:
  1. O generates a tag $Tag = tag(name, sk)$ for her name by using her private key.
  2. Then, she encrypts the detailed identity information (i.e. tag, address, email address, phone no.) with the manager's public key, obtained
  $$\phi_1 = E_{PK_M(Tag,address,emaiaddress,phoneNO.)}.$$
  3. Next, O computes the signature $Sig(Tag, t_r)$, where t_r is the current time.
  4. Finally, O sends the ϕ_1 and the signature Sig to the manager M.
- Regional manager
  The regional manager (M) does the flowing while receiving the request:
  1. M decrypts the ϕ_1 and obtains the user's information including:
  $$\{Tag, address, emaiaddress, phoneNO.\}.$$
  2. Then, M checks if t_r and the signature Sig are valid.

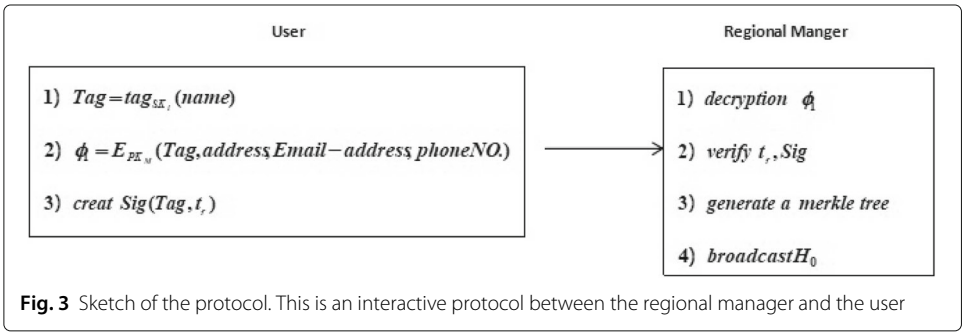

Fig. 3 Sketch of the protocol. This is an interactive protocol between the regional manager and the user

3. If all are valid, M generates a Merkle tree for user's information as shown below

$$
\begin{aligned}
H_{11} &= H(tag(name)),\\
H_{12} &= H(address),\\
H_{21} &= H(emailaddress),\\
H_{22} &= H(phoneNO.),\\
H_1 &= H(H_{11}, H_{12}),\\
H_2 &= H(H_{21}, H_{22}),\\
H_0 &= H(H_1, H_2).
\end{aligned}
$$

4. Finally, M broadcasts the H_0 in the blockchain.

The user's registration process is shown in Fig. 4.

Remark 4 *In order to protect the privacy of user, we hide the user's name by using Tag. The user generates a Tag for her name by using her private key.*

Remark 5 *There are many details information of the user. For the sake of simplicity, we have only selected four parameters Tag, address, emaiaddress, phoneNO.. The case of multiple parameters can be obtained in the same way.*

Remark 6 *For the sake of simplicity, we only generated tag for name to hide user's name information. In fact, one can create tags for any information to be hidden.*

4.3 Identity authentication process

When a transaction is made between the user and the region manager, the region manager first authenticates the user's identity. To this end, we construct the following protocol. The main idea is shown in Fig. 5.

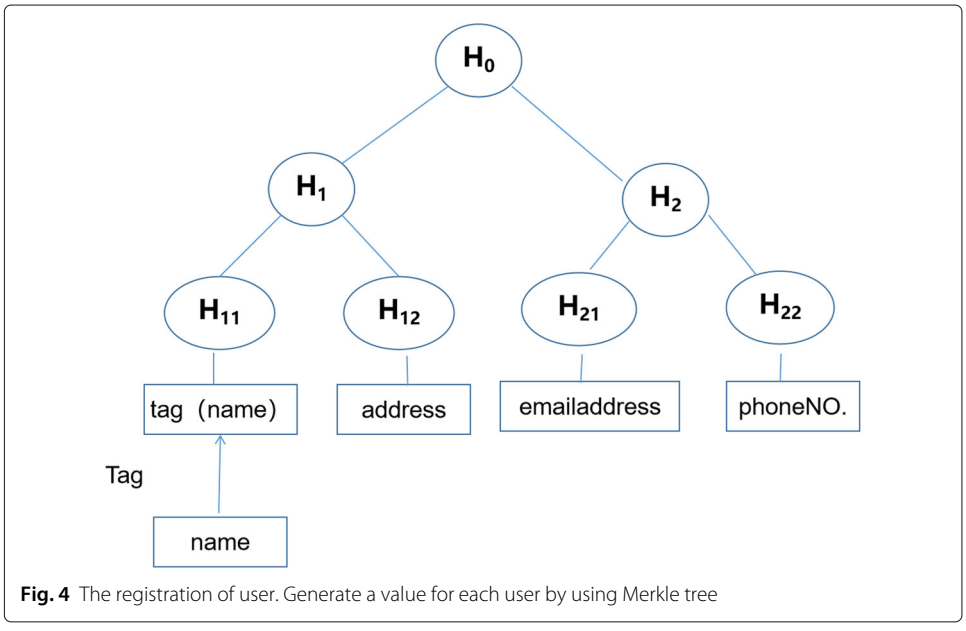

Fig. 4 The registration of user. Generate a value for each user by using Merkle tree

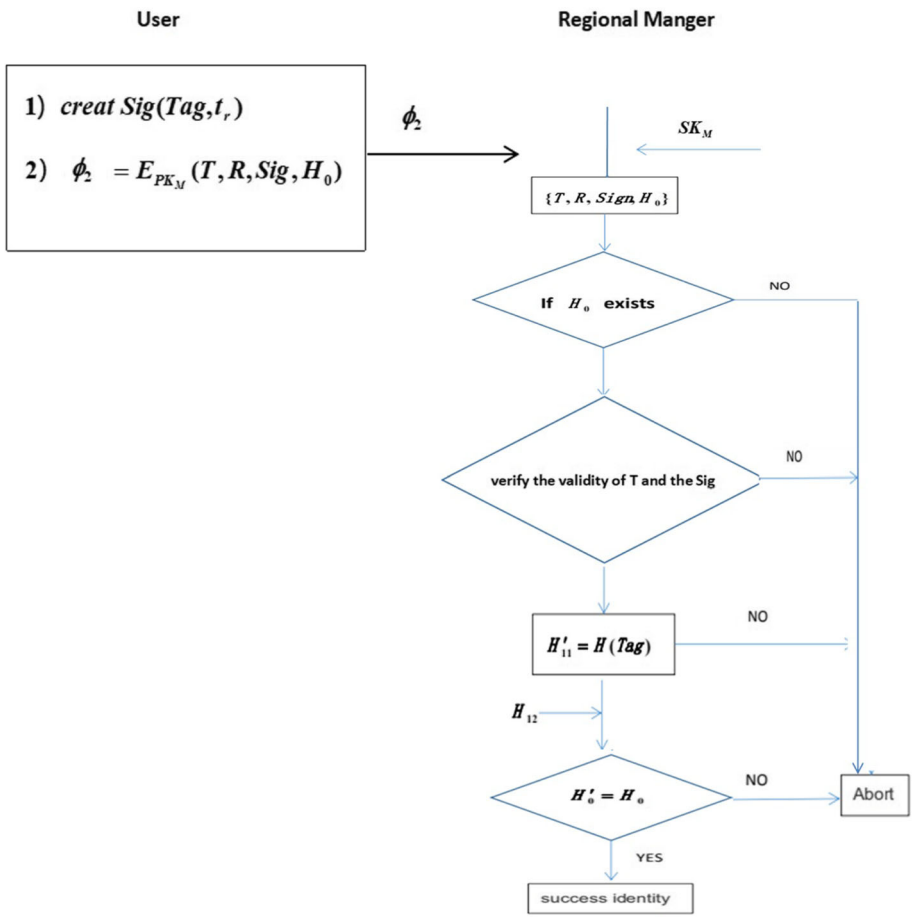

Fig. 5 The authentication of user. The regional manager completes the user's identity authentication through a series of calculations

- User
  1. O generates the signature $Sig(Tag, t_r)$, where t_r is the current time.
  2. Then, O computes the ciphertext $\phi_2(T, R, Sig, H_0)$ using the public key of the manager in which the transaction is done, where T is the time stamp and R is the current request.
  3. Finally, O sends the ϕ_2 to M.
- Manager
  When the manager received the request, M firstly decrypts the ϕ_2 and obtains the information:

  $$\{T, R, Sig, H_0\}.$$

  Then,
  1. M makes a query for the existence of H_0.
  2. If H_0 exists, M continues to check if T and the Sig are valid.

3. Next, M computes $H'_{11} = H(Tag)$ and checks if the equations hold

$$\begin{aligned} &H'_{11} = H_{11}, \\ &H_1 = H(H_{11}, H_{12}), \\ &H'_0 = H(H_1, H_2), \\ &H'_0 = H_0. \end{aligned}$$

If all valid, user authentication is verified. The transaction can be done with this user.

5 An example

Any secure encryption and signature scheme, such as identity-based, attribute-based, lattice-based, and encoding-based signature schemes, can be used in our authentication scheme. We take the encryption and signature scheme based on elliptic curve based on discrete logarithm as an example to illustrate the workflow of our scheme.

5.1 Key generation algorithm

Let G be the generator of the elliptic curve. The key pairs are generated for users and managers as follows:

1. Randomly selects $k \in [1, N]$.
2. Calculate

$$K = kG.$$

The public key is K, and the private key is k.

Assume that user O has the public/private key pair (k_O, K_O) and manager M has the bookkeeping authority and has the public/private key pair (k_M, K_M). The details of user registration and identity authentication process are as follows.

5.2 User registration

- User
  1. Compute

$$Tag = k_o H_1(name).$$

  2. Calculate

$$\phi_1 = (rG, (Tag, address, emaiaddress, phoneNO.) + rK_M),$$

  where $r \in Z_q$ is random number.
  3. Generate

$$\begin{aligned} &R = r'G, \\ &S = r' + H(Tag)k_O, \end{aligned}$$

  where $r' \in Z_q$ is random number. Then, $Sig = (R, S)$.
  4. Finally, O sends the ϕ_1 and the signature Sig to the manager M.
- Regional manager The regional manager (M) does the flowing while receiving the request:

1. M decrypts the ϕ_1 and obtains the user's information through the following algorithm:

   $$(Tag, address, emaiaddress, phoneNO.) + rK_M - k_M rG,$$

   Then, it obtains the user's information including

   $$\{Tag, address, emaiaddress, phoneNO.\}.$$

2. Then, M checks if t_r and the signature Sig are valid through the following equation.

   $$SG = (R + H(Tag))K_O.$$

3. If the equation holds, the signature is valid, then M generates a Merkle tree for user's information as shown below:

   $$\begin{aligned}
   &H_{11} = H(tag(name)),\\
   &H_{12} = H(address),\\
   &H_{21} = H(emailaddress),\\
   &H_{22} = H(phoneNO.),\\
   &H_1 = H(H_{11}, H_{12}),\\
   &H_2 = H(H_{21}, H_{22}),\\
   &H_0 = H(H_1, H_2).
   \end{aligned}$$

4. Finally, M broadcasts the H_0 in the blockchain.

5.3 Identity authentication process

- User

  1. Generates the signature

     $$\begin{aligned}
     &R' = r_2 G,\\
     &S' = r_2 + H(Tag, t)k_O,
     \end{aligned}$$

     where $r_2 \in Z_q$ is random number and t is the current time.
  2. Computes

     $$\phi_2 = (r_3 G, (T, R, Sig, H_0) + r_3 K_M),$$

     where $r_3 \in Z_q$ is random number, T is the time stamp, and R is the current request.
  3. Finally, O sends the ϕ_2 to M.

- Manager

  When the manager received the request, M firstly decrypts the ϕ_2

  $$(T, R, Sig, H_0) + r_3 K_M - k_M r_3 G,$$

  and obtains the informations:

  $$\{T, R, Sig, H_0\}.$$

  Then,

  1. M makes a query for the existence of H_0.

2. If H_0 exists, M continues to check if T and the *Sig* are valid through the following equation.

$$S'G = (R' + H(Tag, t))K_O.$$

If the equation holds, the signature is valid.

3. Next, M computes $H'_{11} = H(Tag)$ and checks if the equations hold

$$\begin{aligned} &H'_{11} = H_{11}, \\ &H_1 = H(H_{11}, H_{12}), \\ &H'_0 = H(H_1, H_2), \\ &H'_0 = H_0. \end{aligned}$$

If all are valid, user authentication is verified. The transaction can be done with this user.

6 Correctness and security analysis

According to the security model introduced in Section 3, correctness and security proofs will be given in this section.

6.1 Correctness analysis

Theorem 1 *The identity authentication process is correct. It means that legitimate users must be able to pass the verification, that is, the following equation*

$$\begin{aligned} &H'_{11} = H_{11}, \\ &H_1 = H(H_{11}, H_{12}), \\ &H'_0 = H(H_1, H_2), \\ &H'_0 = H_0. \end{aligned}$$

holds.

Proof If the user is legitimate, he/she has the correct private key which is used to generate *Tag*. The tag can be verified.

Then,

$$H'_{11} = H(Tag) = H_{11}$$

holds.

So,

$$\begin{aligned} &H_1 = H(H'_{11}, H_{12}) = H(H_{11}, H_{12}), \\ &H'_0 = H(H_1, H_2) = H_0. \end{aligned}$$

□

6.2 Security analysis

Theorem 2 *The proposed scheme is secure against forgery.*

Proof Suppose that an adversary C can attack the proposed scheme with advantage ϵ; it means that a malicious user can forge a legitimate identity and pass the verify; then, we can construct an algorithm F by C to solve the hard problem in which the signature scheme depends on.

- **User registration process**

  - *TagQuery*
    Assume that C can make query on Tag, F maintains the list L_{Tag} to store the answers.
    When C makes a query on Tag, F checks if the query can found in the list L_{Tag}; if yes, return the answer to C; otherwise, F returns the random value.
  - *SignQuery*
    C also makes signature query on Tag. F can simulate the signature.
    Then, the adversary can output a forged signature σ^* on Tag^*.
  - Finally, F can solve the hard problem that the signature schemes depend on.

- **Identity authentication process**
  We consider it in two cases.

  - *The adversary C can forge a signature* This is similar to the user registration process. If the adversary can output a forged signature σ^* on Tag^*. Then, F can solve the hard problem that the signature schemes depend on.
  - *The adversary C can forge a Hash value*
    It is well known that hash functions are collision resistant. So, no adversary can forge the H_0 unless the hash function can be solved.

□

Theorem 3 *The proposed scheme can realize the privacy protection of user identity.*

Proof In our scheme, the user's name is hidden in the *Tag*. Everyone only knows the tag, but they do not know the user's true identity. If the adversary C can obtain the name of the user, it means that the encryption scheme has been breached. That is impossible since the user generates a *Tag* for her name by using her private key.

Therefore, our scheme can protect the privacy of our users. □

7 Results and discussion

In terms of function, our scheme is compared with some existing schemes. The authors used a variety of patterns that provide authentication only in a centralized manner in [28–31], and third parties are used in a variety of applications. In our scheme, we use blockchain technology to provide authentication and can used for all engine trading systems. Also, our scheme is independent of third party and is a peer-to-peer network. The brief summary of this comparison is given in Table 1.

Remark 7 *In Table 1, tech. and app. mean the technique used and the application scenario of these schemes, respectively.*

Table 1 Function compare

Schemes	Tech.	Forger	Third part	Anonymity	App.
Our	Blockchain	Yes	No	Yes	Engine trading
[28]	Attribute-based	No	Yes	Yes	Smart gird
[29]	Pairing-based	Yes	Yes	No	Smart gird
[30]	ID	Yes	Yes	No	Smart gird
[31]	Hash	No	Yes	No	Smart gird

8 Conclusion and future work

In this paper, we proposed a general authentication scheme to solve the problem of identity authentication in blockchain-based energy trading system. The digital signature technology, time stamp, and Merkle tree are used to ensure that the identity of legitimate users cannot be forged in our scheme. Moreover, to avoid regional managers with more transactions which tend to get higher credit score, we use the proof of stake (PoS) plus credit score to complete the bookkeeper selection and randomly select one of the managers with honor values greater than or equal to k each time in the process of journalizing. In future work, we will continue to study the application of the scheme in other areas.

Abbreviations

DLT: Distributed ledger technology; P2P: Peer-to-peer; IoT: Internet of Things; PoW: Proof of work; Pos: Proof of stake

Acknowledgements

The authors thank the person who provided meticulous and valuable suggestions for improving the paper.

Authors' contributions

YR and ZI proposed the main idea. YR is the main writer of this paper. QZ and HG analyzed the results and discussed the function compare. ZL is the corresponding author of this paper. All authors read and approved the final manuscript.

Funding

This work was supported by the Higher Education Technology Innovation Projects Foundation of Shanxi (Grant No.2019L0860), the National Natural Science Foundation of Shanxi (Grant No.201601D021014), the National Natural Science Foundation of China (Grant No. 61702124), and the Subject Research Projects Foundation of Key Laboratory of Information Security Technology of Guangdong (Grant No. GDXXAQ2016-05)

Availability of data and materials

Data sharing is not applicable to this article as no datasets are generated or analyzed during the current study.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Mathematics and Information Technology, Yuncheng University, 044000 Yuncheng, China. [2]School of Mathematics and Information Science, Guangzhou University, 510006 Guangzhou, China.

Received: 1 April 2020 Accepted: 6 July 2020
Published online: 20 July 2020

References

1. S. Nakamoto, et al., *Bitcoin: a peer-to-peer electronic cash system*. (Working Paper, 2008). https://bitcoin.org/bitcoin.pdf
2. E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, C. Weinhardt, A blockchain-based smart grid: towards sustainable local energy markets. Comput. Sci.-Res. Dev. **33**(1-2), 207–214 (2018)
3. C. Park, T. Yong, Comparative review and discussion on P2P electricity trading. Energy Procedia. **128**, 3–9 (2017)
4. A. Hahn, R. Singh, C.-C. Liu, S. Chen, in *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Smart contract-based campus demonstration of decentralized transactive energy auctions (IEEE, 2017), pp. 1–5
5. E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, C. Weinhardt, Designing microgrid energy markets: a case study: The brooklyn microgrid. Appl. Energy. **210**, 870–880 (2018)
6. J. Hwang, M.-i. Choi, T. Lee, S. Jeon, S. Kim, S. Park, S. Park, Energy prosumer business model using blockchain system to ensure transparency and safety. Energy Procedia. **141**, 194–198 (2017)
7. E. R. Sanseverino, M. L. Di Silvestre, P. Gallo, G. Zizzo, M. Ippolito, in *2017 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)*, The blockchain in microgrids for transacting energy and attributing losses (IEEE, 2017), pp. 925–930
8. K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, M. Kraft, Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. Appl. Energy. **209**, 8–19 (2018)
9. K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the Internet of Things. IEEE Access. **4**, 2292–2303 (2016)
10. Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium blockchain for secure energy trading in industrial Internet of Things. IEEE Trans. Ind. Inform. **14**(8), 3690–3700 (2017)
11. PowerLedger (2018). https://powerledger.io/. Accessed April 2019
12. PowerLedger whitepaper online (2018). https://powerledger.io/media/Power-Ledger-Whitepaper-v8.pdf. Accessed April 2019
13. Brooklyn Microgrid online (2018). http://www.brooklynmicro-grid.com. Accessed Jan 2019
14. DAJIE online (2017). https://www.dajie.eu. Accessed May 2019

15. Shareandcharge online (2018). https://shareandcharge.com/. Accessed May 2019
16. Ethereum blockchain app platform online (2018). https://www.ethereum.org. Accessed May 2019
17. NRGcoin Smart Contract for green energy online (2018). http://nrgcoin.org. Accessed Feb 2019
18. Solar Coin online (2017). https://solarcoin.org. Accessed Mar 2019
19. The Silicon Based Economy - financing solar cells with Bitcoin online (2017). https://thesunexchange.com/silicon-based-economy-financingsolar-cells-bitcoin. Accessed June 2018
20. Electron project online (2017). http://www.electron.org.uk. Accessed Mar 2019
21. M. Merz, Enerchain project overview and key insights. Hamburg: PONTON. https://ponton.de/downloads/enerchain/EnerchainKeyInsights_2018-03-29_final.pdf. Zugegriffen am. **1**, 2019 (2018)
22. Bitnation (2018). https://bitnation.co. Accessed Mar 2019
23. ConsenSys (2018). https://consensys.net. Accessed Mar 2019
24. Hyperledger (2018). https://www.hyperledger.org/community/projects. Accessed Mar 2019
25. Future of identity (2018). http://www.futureofidentity.org. Accessed Mar 2019
26. R. Jones, Becoming a virtual Estonian (2016). http://www.bbc.com/news/technology-36276673. Accessed Mar 2018
27. E-Estonia (2018). https://e-estonia.com/e-residents/about. Accessed Oct 2019
28. R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, J. J. Rodrigues, SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment. IEEE Trans. Ind. Inform. **14**(6), 2629–2640 (2018)
29. L. F. Roman, P. R. Gondim, J. Lloret, Pairing-based authentication protocol for V2G networks in smart grid. Ad Hoc Netw. **90**, 101745 (2019)
30. D. Ghosh, C. Li, C. Yang, A lightweight authentication protocol in smart grid. IJ Netw. Secur. **20**(3), 414–422 (2018)
31. P. Gope, B. Sikdar, Privacy-aware authenticated key agreement scheme for secure smart grid communication. IEEE Trans. Smart Grid. **10**(4), 3953–3962 (2018)
32. S. Muftic, Blockchain identity management system based on public identities ledger (2017). US Patent 9,635,000
33. H. Liu, H. Kou, C. Yan, L. Qi, Link prediction in paper citation network to construct paper correlation graph. EURASIP J. Wirel. Commun. Netw. **2019**(1), 1–12 (2019)
34. Y. Huang, Y. Chai, Y. Liu, J. Shen, Architecture of next-generation e-commerce platform. Tsinghua Sci. Technol. **24**(1), 18–29 (2018)
35. G. Li, S. Peng, C. Wang, J. Niu, Y. Yuan, An energy-efficient data collection scheme using denoising autoencoder in wireless sensor networks. Tsinghua Sci. Technol. **24**(1), 86–96 (2018)
36. A. Ramlatchan, M. Yang, Q. Liu, M. Li, J. Wang, Y. Li, A survey of matrix completion methods for recommendation systems. Big Data Min. Analytics. **1**(4), 308–323 (2018)
37. L. Liu, X. Chen, Z. Lu, L. Wang, X. Wen, Mobile-edge computing framework with data compression for wireless network in energy internet. Tsinghua Sci. Tech. **24**(3), 271–280 (2019)
38. W. Zhong, X. Yin, X. Zhang, S. Li, W. Dou, R. Wang, L. Qi, Multi dimensional quality driven service recommendation with privacy preservation in mobile edge environment. Comput. Commun. **2020** (2020). https://doi.org/10.1016/j.comcom.2020.04.018
39. X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, W. Dou, Become: blockchain-enabled computation offloading for IoT in mobile edge computing. IEEE Trans. Ind. Inform. **16**(6), 4187–4195 (2019)
40. C. Zhou, A. Li, A. Hou, Z. Zhang, Z. Zhang, F. Wang, Modeling methodology for early warning of chronic heart failure based on real medical big data. Expert Syst. Appl. (2020). https://doi.org/10.1016/j.eswa.2020.113361
41. C. Zhang, M. Yang, J. Lv, W. Yang, An improved hybrid collaborative filtering algorithm based on tags and time factor. Big Data Min. Analytics. **1**(2), 128–136 (2018)
42. L. Qi, W. Dou, Y. Zhou, J. Yu, C. Hu, A context-aware service evaluation approach over big data for cloud application. IEEE Trans. Cloud Comput. (2015). https://doi.org/10.1109/TCC.2015.2511764
43. X. Chi, C. Yan, H. Wang, W. Rafique, L. Qi, Amplified LSH-based recommender systems with privacy protection. Concurr. Comput. Pract. Experience (2020). https://doi.org/10.1002/CPE.5681
44. L. Qi, W. Dou, W. Wang, G. Li, H. Yu, S. Wan, Dynamic mobile crowdsourcing selection for electricity load forecasting. IEEE Access. **6**, 46926–46937 (2018)
45. Y. Liu, S. Wang, M. S. Khan, J. He, A novel deep hybrid recommender system based on auto-encoder with neural collaborative filtering. Big Data Min. Analytics. **1**(3), 211–221 (2018)
46. Li. Jianxin, T. Cai, K. Deng, X. Wang, T. Sellis, F. Xia, Community-diversified influence maximization in social networks. Information systems. Inf. Syst. **92**, 1–12 (2020)
47. Y. Chen, N. Zhang, Y. Zhang, X. Chen, W. Wu, X. S. Shen, Energy efficient dynamic offloading in mobile edge computing for Internet of Things. IEEE (2019). https://doi.org/10.1109/TCC.2019.2898657

Publisher's Note