A Traceable Smart Grid Trading System under Blockchain

1st Ming-Te Chen*, 2nd Chu Xuan Liang†, 3rd Chia Chu Chen‡
Computer Science and Information Engineering
National Chin-Yi University Technology
Taichung 41170, Taiwan
*mtchen@ncut.edu.tw; †s4A817016@student.ncut.edu.tw; ‡croussrm@gmail.com

2020 International Symposium on Computer, Consumer and Control (IS3C) | 978-1-7281-9362-5/20/$31.00 ©2020 IEEE | DOI: 10.1109/IS3C50286.2020.00104

***Abstract*— In recently years, the traditional bi-directional smart grid system helps users to save energy such as electricity and also could perform the energy trading with other users in the same grid. However, it also requires a trusted third party to help gird users to maintain the transaction to be fair. If there are some users to deny a transaction in the grid, how the trusted third party is able to trace the real identity is the serious problem to be handle currently.**

As a result, we proposed a traceable smart grid trading system with smart contract in the peer-to peer(p2p) network. We also combine the smart contract into our scheme and adopt the token-based way to make transaction to be fair in case of unexpected problems happened such as the transaction failure.

***Keywords*—smart grids, smart contract, energy trading**

I. Introduction

A smart grid was a platform that each user on this grid could also perform the energy trading with the others. As time goes by, the smart grid ability also to be enlarge such as user identity verification, energy storage, and payment flow exchange. user on this grid could be a energy buyer or a energy producer.

Energy producers could store self energy to the platform and post trading on the platform and other energy buyers could deal with energy producers through the posted announcement on the platform. However, there is a centralized system to be the trusted third party to handle each transaction flow and keeps the transaction process log in the traditional smart grid architecture. From above architecture, we think that a centralized system existence could also bring some problems such as the single point of failure, user privacy disclosure and fair transaction.

In one hand, smart contract is an application of blockchain and it was first proposed by ethereum (ETH)[2]. It is not only a wallet address recorded on this network or a contract address for peer client to use, but also peer client can view this contract and use the content written on the contract. When peer clients execute the contract respectively, they will share all information with other peer clients(miners) and other miners also perform the check on this shared information.

When this information is accepted by most miners,it will be written into the ledger on the same blockchain. Therefore, smart contract could be used to carry out the most important transaction processes. Peer clients can make transaction with other peers or exchange products securely by using smart contract which is decentralized and without the need for a trusted third party.

As a result, we proposed our scheme that it could combine the blockchain with smart contract into the smart grid system and also design the scheme under the identity based encryption scheme. In this scheme, we discussed getting rid of the centralised system for smart grid trading in a two-way transaction process by using blockchain and smart contracts. The proposed smart grid trading system is able to handle energy trading without third-party constraints and also make energy transaction more reliable.

The rest of the paper organized in the following manner. II will introduce the referenced technology and papers, III will show core system technology and IV shows how to convert energy to contract, verify communication and trade energy in the proposed scheme.

II. Related Work

Recently, the blockchain technology is studied in energy trading because of its advantages of decentralization, anonymity and trust of the ledger distribution. For example, Z. Li and J. Kang [8] propopsed a banking system that is added to the smart grid to increase the utilization rate of the electricity network. W. Hou and L. Guo[6] further analyzed the advantages and disadvantages of their method and proposed how to increase the utilization rate of the energy trading network while reducing the energy transaction load of the trusted third parties. The system proposed by [1] which is a token based energy trading system using P2SH and multi-signature to complete the transaction. Kang et al.[7] proposed a peer-to-peer electricity trading system on the smart grid or the vehicle-to-grid (V2G) system[10] which tried to solve the energy problem of electric vehicles.

There are some previous studies trying to remove trusted third-party agents from the smart grid system. In order to achieve true decentralization, such as (SPB)-based framework[4], once the producer is unable to meet the needs energy demand within a predetermined period of time, the corresponding expired transaction will be considered invalid. In addition, the system provided by Aitzhan and Svetinovic[1] which they adopt the P2SH tripartite signature method with a decentralized arbitrator to intervene in the transaction process.

978-1-7281-9362-5/20/$31.00 ©2020 IEEE
DOI 10.1109/IS3C50286.2020.00104

This proposed paper will focus on the combination of smart contract[3] [9] to increase constraints in energy transactions with the smart grid and adopt the concept[5] protection of mutual verification in order to provide effective protection to peer clients and tracing when it is necessary.

III. Core System Components

This section will introduce our system components and give all symbol definition in Table I in the followings.

A. Blockchain

Blockchain technology is a distributed ledger with advantages of decentralization, anonymity protection and trust of the ledger distribution. The distributed ledger records each transaction in a verifiable and permanent way which is the underlying fabric for Bitcoin. In addition, each user adopts the random number to be their identity. By the way, each user has to generate its own signature before each transaction start. Finally, each transaction will be written to the ledger when it is accepted after verifying by each miners in the blockchain.

B. Smart Contract

the smart contract is an application of blockchain in the recently years. It was first proposed by ETH and it is not only the wallet address that is recorded on this network,but also a contract address of each miner. Each peer client could view and execute the content written on the contract. When each peer executes the contract, it will upload all information into p2p network for other miners to check. When this request is accepted by most miners, it will be written into the public ledger of the blockchain.

IV. The Proposed Scheme

In the proposed scheme, each energy will be converted into tokens and stored in smart contract to reduce the energy consumption and save time consumption in the energy transmission. There are some phases of the proposed scheme in the following steps.

$$txAddr_i = hash(pubK_i) \tag{1}$$

$$msgAddr_i = hash(pubK_i \| priK_i) \tag{2}$$

A. Setup Phase

In this phase, we assume that there exists a PKG that it could generate the public key and private key for each user in the smart grid. First, the PKG generates the following parameters.

- It selects elliptic curve E over the G_q and base point P.
- It calculates $SK_{PKG} = s \in_R Z_p$ and computes $PK_{PKG} = s \cdot P \in E$.
- It sets up the hash, encrypt, and decrypt functions as the system parameter.

Then publishes $(E, P, PK_{PKG}, hash, encrypt, decrypt)$.

TABLE I: Used notation and description.

Notation	**Description**
p	the large prime of the field Z_p
q	the prime order of $\mathbf{G}$
ID_i	real identity of user $i$in the smart grid
PKG	the public key generation center
$pubK_i$	PKG issued public key for user i
$priK_i$	PKG issued private key for user i
$txAddr_i$	wallet address of user i
$msgAddr_i$	message address of user i
$msgAddr_{DSO}$	message address of DSO
$hash$	one way hash function that it maps from $\mathbf{G} \to \{0, 1\}$
$Hash$	one way hash function that it maps from $\mathbf{G} \to \{0, 1\}$
E	Elliptic Curve on the $\mathbf{G}_q$
P	elliptic curve base point on E
$\|$	concat binary symbol
$Permit_i$	permit signature of user i
$sign_i$	signature of user i
PK_{PKG}	public key of PKG or DSO
SK_{PKG}	secret key of PKG or DSO
$encrypt(M, pubK_i)$	asymmetric encrypting function with the input message M with the public key $pubK_i$ of the user i.
$decrypt(C, priK_i)$	asymmetric decrypting function on input C with private key $priK_i$ of the user i.
$sym - encrypt(M, K_i)$	symmetric encrypting function with the input message M with the public key K_i of the user i.
$sym - decrypt(C, K_i)$	symmetric decrypting function on input C with private key K_i of the user i.
$K^n_{i,j}$	secret session between a user i and a user j in the n-th session
γ_i	a random number chosen from Z_p of a user i.
κ_i	a secret value computed from the hashed value of user i's identity.
α_i	a encrypting result from identity of a user i by using DSO's public key .

B. PKG Issued Key Phase

In this phase, each peer has to obtain a private key and identity from the public key generator(PKG) before they begin the transaction. PKG checks the identity of each user and use (3), (5), and (4) to issue the $(ID_i, pubK_i, priK_i)$ as the user i's identity, public key and private key, respectively. ID_i is a unique identity of the $user_i$ and $pubK_i$ is a final public key that it combines user i's identity inside with hash protection and $priK_i$ is a private key which could prove the validity of the certificate. These tokens could be used to verify the legitimacy of the user. Moreover, PKG could use PK_i^{pub} to track the user when accident are occurred.

$$\alpha_i = encrypt(ID_i, PK_{DSO}) \tag{3}$$

$$priK_i = \kappa_i = s \cdot hash(ID_i || \alpha_i) \tag{4}$$

$$pubK_i = priK_i \cdot P \in E \tag{5}$$

C. Energy Injecting Phase

In this section, we show that a token-based energy trading system which it allows peer-to-peer energy trading. We assumed that there are energy node in the smart grid network that it could obtain enough electricity for self-sufficiency. Some nodes could even sell electricity to another nodes and earn profit from another nodes.

Through smart contract, each peer could trade energy between each peer without a trusted third party. We assume that Bob is a energy producer that he attempts to sell the energy to other peer. Then he must exchange his tokens with the Distribution System Operator (DSO) in the following steps. Here we assumed that the DSO is an temper-proof device that it receives the signature from each peer and generates the final contract and return it to the corresponding peer.

1) First, Bob generates his wallet address $txAddr_B$ (1), message address $msgAddr_B$ (2) and signature $sign_B = Bob.sign(PK_{DSO})$
2) Then, Bob also forwards ($Energy_B$, $pubK_B$, $sign_B$, $txAddr_B$, $msgAddr_B$) to DSO
3) When DSO has received these data from Bob, it generates the final contract only if the signature $sign_B$ and other values are valid.
4) After DSO verified the signature $sign_B$ successfully, it will send a request to p2p network for generating the contract of Bob. Let the Bob's contract as the C_{addr_B}.
5) Then, DSO generate a signature $sign_D = DSO.sign(C_{addr_B})$ and initial the contract to the blockchain.
6) Finally, DSO also stores Bob contacting information ($pubK_B$, $txAddr_B$, $msgAddr_B$) to the contract and send contract address back.

In this time, Bob could broadcast (C_{addr_B}, $pubK_B$, $txAddr_B$, $msgAddr_B$) and waits for the transaction request when he has announced the information to the blockchain. Through the smart contract, each peer could trade energy without a trusted third party involving. If there is some disputed happened, then we could provide user information to cooperate with the DSO and judge to find out who the criminal is in our journal version. Not only the our method provided a way to finish each transaction, but also the system could achieve the undeniable property. Because the final result is recorded in the public ledger with corresponding signature inside.

D. Messaging Handshake

In this section, we assumed that Alice is a buyer that she sends a message to Bob through the message address to negotiate the energy price. When she decides to buy energy with Bob, they have to create the session key before start streaming to protect the following message from the attackers. Before generating the session key first, they both obtain their contact respectively.

1) Alice generate $priK_A = \kappa_A \in_R Z_p$ and secret $\gamma_A = R(\cdot)$ and calculate $pubK_A = priK_A \cdot P = \kappa_A \cdot P \in E$.
2) Then she could obtain $pubK_B$ from contract and computes $K_{A,B}$(6)
3) Before she sends request, Alice has to encrypt message first in the following. $C_A = encrypt(\gamma_A, pubK_B)$
4) Alice send $(pubK_A, C_A, hash(C_A))$ to Bob. When Bob receives $(pubK_A, C_A, hash(C_A))$ from Alice, he could perform the public key authentication with the contract of Alice. If the $pubK_A$ is valid, he could decrypt C_A and compute the session key $K_{A,B}$.
5) Then, Bob also performs the same generate a new key pair ($\gamma_B = R(\cdot)$, $pubK_B = \kappa_B \cdot P \in E$) and encrypt message $C_B = encrypt(\gamma_B, pubK_A)$ with the hashed value $hash(C_B)$ on cipher-text C_B. Then he forwards $(pubK_B, C_B, hash(C_B))$ to the Alice.
6) Finally, Alice could also decrypt to obtain secret message γ_B if above $pubK_B$ is valid.

Finally, when Alice and Bob has received their own shared secret random number from each other, they could compute the session key for late usage in the following step.

$$K_{A,B} = Hash(\kappa_A \cdot pubK_B || \gamma_A \cdot \gamma_B) \tag{6}$$

$$K_{B,A} = Hash(\kappa_B \cdot pubK_A || \gamma_B \cdot \gamma_A) \tag{7}$$

E. Message Communication Phase

In the messaging phase, Both Alice and Bob have to change their secret value in a period of time with the following steps:

1) Message originator Alice generates a random key pair ($\gamma_A^n \in_R Z_p, pubK_A^n = \kappa_A^n \cdot P \in E$) and encrypts message $C_A^n = sym-encrypt(\gamma_A^n, K_{A,B}^{n-1})$. Then, Alice forwards the message C_A to Bob.
2) When Bob has received this cipher-text C_A^n, he could use $K_{B,A}$ to get the $(pubK_A^n)$.
3) Then, Bob calculates new secret key $K_{B,A}^n$ and encrypts message $C_B^n = sym - encrypt(\gamma_B^n, K_{B,A}^{n-1})$
4) After Alice receives message C_B^n, she could calculate $K_{A,B}^n$ for later message transferring usage.

F. Transaction

After both they had finished above session key generation, Bob signs the information containing the contract address, $pubK_A$ and final both decided energy price to generate the $Permit_B$ (8) signature for transaction.

$$Permit_B = Bob.sign(C_{addr_B} \| pubK_A) \tag{8}$$

Alice can review the contract and use this signature as a parameter template which it can replace the owner. Before executing function of this contract, the contract will check this permit signature and send request to the p2p network. When miners has verified the validity of the request, the result will be written on the public ledger.

G. Exchange Owner Phase

When Alice attempts to exchange owner of smart contract, it has to request a signature $Permit_B$ from the current owner Bob and generate a new signature $sign_A = Alice.sign(C_{addr_B})$. Then, she could use these two signature as parameters to call the method in flowing steps:

1) Alice forwards multiple variables ($pubK_A$, $Permit_B$, $sign_A$) to the contract.
2) Then, this contract will accept request only if the signature $sign_A$ and $Permit_B$ are verified successful, respectively.
3) When Bob has accepted this contract with peer Alice, the contract stores ($msgAddr_A$, $txAddr_A$, $sign_A$) and change owner public key to $pubK_A$.

V. Functional Analysis

A. Undeniable Property

Blockchain is a public ledger system which has anonymity protection, decentralization. It is almost impracticable for users to modify transaction records recorded to the ledger in one half. Attackers does not have negligible probability to modify each block record on the blockchain. Since the characteristics of the blockchain and signature of our proposed scheme, all the transactions and communications on the energy system could not deny.

B. Trackable Property

In our proposed scheme, we embedded the user's identity into the personal private key. If there is user which she/he pretends to attack the transaction record in the blockchain. In this time, PKG could providei its own private key s to find out the identity from this malicious user's private key $priK_i = s \cdot hash(ID_i || \alpha_i)$ with the identity ID_i and the random number α_i to the judge. Then, the judge could make the final decision with the help of PKG and DSO to find out who the user is.

VI. Conclusion

This paper combines the smart contract in the smart grid network and remove reliable third parties from the activities. In addition, we also design the session key under Diffie-Hellman mechanism and keeps the forward security. Besides, we assumed that the DSO is an offline device that if there is a dispute happened, it will be recalled to provide some user's information about the transaction to reduce the communication cost.

References

[1] N. Z. Aitzhan and D. Svetinovic. "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams". In: *IEEE Transactions on Dependable and Secure Computing* 15.5 (2018), pp. 840–852.

[2] V. Buterin. "Ethereum white paper". In: (2014). URL: https://github.com/ethereum/wiki/wiki/White-Paper.

[3] P. Dai et al. "Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform". In: (2017).

[4] A. Dorri et al. "SPB: A Secure Private Blockchain-Based Solution for Distributed Energy Trading". In: *IEEE Communications Magazine* 57.7 (2019), pp. 120–126.

[5] F. Ozguner F. Alanazi S. Al-Shareeda. "An efficient CPPA scheme for intelligent transportation networks". In: *Pervasive and Mobile Computing* 59 (2019).

[6] W. Hou, L. Guo, and Z. Ning. "Local Electricity Storage for Blockchain-Based Energy Trading in Industrial Internet of Things". In: *IEEE Transactions on Industrial Informatics* 15.6 (2019), pp. 3610–3619.

[7] J. Kang et al. "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains". In: *IEEE Transactions on Industrial Informatics* 13.6 (2017), pp. 3154–3164.

[8] Z. Li et al. "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things". In: *IEEE Transactions on Industrial Informatics* 14.8 (2018), pp. 3690–3700.

[9] N. Szabo. "The idea of smart contracts". In: (1997). URL: https://nakamotoinstitute.org/the-idea-of-smart-contracts/.

[10] Z. Zhou et al. "Secure and Efficient Vehicle-to-Grid Energy Trading in Cyber Physical Systems: Integration of Blockchain and Edge Computing". In: *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50.1 (2020), pp. 43–57.