Smart Electricity Billing System Using Blockchain Technology

Shafiq Aiman, Suhaidi Hassan, Adib Habbal, Athirah Rosli, and Ahmad Hanis Mohd Shabli
InterNetWorks Research Laboratory, School of Computing,
Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia.
shafiq_aiman@internetworks.my

***Abstract*—Nowadays, many home appliances use electricity to operate. However, prediction of the electricity usage is not easy and accurate. A prepayment scheme provides the better way to forecast domestic electricity usage. Traditionally, the prepayment scheme is based on the centralized server or the standalone embedded machine, but the centralized service is highly vulnerable to security threats and potential attacks. The purpose of this paper is to describe our design of a peer-to-peer token bill system for the domestic electricity distribution. It also describes the trusted information transaction among the Internet-of-Things devices. In addition, we provide a conceptual overview of the blockchain-based Wattcoin payment system. In this system, a wallet is created by using the cryptography technique that generates private key, public key and the wallet address. Then, the transaction is done when the digital signature is used to authenticate every transaction floating in the network. Moreover, this paper illustrates blockchain message protocol for message exchange among devices.**

Index Terms—Distributed Ledger; Prepayment Metering; Ethereum; Smart Contract.

I. Introduction

Nowadays, with the rapid development of technology and social service awareness, the prepayment schemes are widely adopted in the provision of utility services such as electricity, water, and gas. There are huge benefits of using the prepayment scheme for such services on users and as well as suppliers [2]. The monthly usage expenses can be forecasted and the cash flow of the providers can be improved because of the prepayment nature prior to the product being consumed [1]. The prepayment scheme had traditionally been interconnected to the centralized services. As we know, the risks of having centralized system are considerably higher. There are many possible threats that can undermine the centralized system or illegally trespass the system from a distance. In order to prevent any type of threats from compromising our system, we need to make sure all the transaction data is secure and highly trusted.

Besides, the measurement of the electricity consumption still using the old metering method in unit terms of Kilowatt Per-Hour (kW/h), which is based on the power consumption at a certain amount of time. In order to enable the electricity sharing over the existing power grid system, we need to change this type of measurement method into another form of asset that can be transferred among its peers. This type of asset is absolutely referred to the digital assets and moves over the peer-to-peer network. The process of transforming the electrical power to the digital assets is called Tokenization. In this paper, the tokenized asset is called *Wattcoin*. Our Wattcoin can be transferred or controlled by Wattcoin wallet, which is a mobile application that can be installed by users on their smartphone. The Wattcoin usage can be reduced in the electricity meter by having Exhaustion Function. Besides the reduction of the Wattcoins, the Exhaustion Function also gives a real-time electricity usage reading of personal or overall users.

To enhance the overall performance of prepayment system and avoid issues within the present prepayment system, including a single point of failure and fake transaction data, the design of a network prepayment meter reading system, which is fully based on blockchain technology, is described in this paper [1]. The proposed scheme utilizes the blockchain technology to replace the centralised system with the peer-to-peer system. Furthermore, the replacement of the prepaid card with the electronic wallet (i.e., the Wattcoins wallet) in order to replace the usage of card which is not very cost effective and users can buy the resource directly from the store. The blockchain technology itself is really an advanced technology, often referred to as the new-era of intelligent technology. This is due to the fact that blockchain technology combines many advanced technologies such as zero-knowledge proof, consensus algorithm, and state transition system to achieve one of the most secured and trusted platform.

This paper is organized as follows; first, it describes the issues of the centralized service in the prepayment scheme. Next, it discusses the deployment of the blockchain into prepayment scheme. Then, the smart token billing system is designed. Finally, the discussion of the proposed billing system is presented in the last section.

II. Related Works

A. Prepayment Electricity Meter

In a power distribution system, an electricity meter plays an important role to measure the electricity consumption for every single user to be presented to the supplier. In spite of measuring the electricity, there are many issues regarding the "post-paid" electricity meter such as high operational cost. The prepayment electricity meter was introduced to overcome the issues of high operational cost borne by the supplier and to remove over-usage of electricity for the customers.

Most of the prepayment meters must have an Internet connection in order to connect to the centralized services. Vendor normally selects the suitable protocol to adopt this technology such as CoAP, MQTT, MQTT-SN, and Web Socket [3]. But, there are many challenges related to the centralized service such as privacy and trust issues. The privacy issues appear as an uncontrollable massive amount of information about specific meter is shared over the Internet [4]. After the privacy issues were raised, we have seen many prepayment meters were compromised, this will cause the owner of the prepayment meter felt much hesitated to use the prepayment meter.

Then, some other researchers and manufacturers proposed other security schemes for the prepayment meter. Besides security, they also proposed about the energy saving, fault tolerance management and smart metering for the electricity meter [5].

B. Ethereum

Proposed by Vitalik Buterin in 2013, Ethereum is an open blockchain-based decentralized computing platform [7, 8, and 9]. Unlike preceding blockchain inclusive of Bitcoin, Ethereum is able to work as a computer even the performance is slower than usual personal computer since it has approximately 12 seconds to verify a transaction. It also has its own language which includes Solidity and Serpent, we could write and compile a program. Once compiled, it can run on the Ethereum Virtual Machine just like another programming languages. Compiled code gets translated to the assembly code and then to the binary code, which it will be executed on the Ethereum Virtual Machine environment. Ethereum is precise in an experience that it combines computing system with blockchain. It is miles ground-breaking because it gives developers the flexibility to write a code that could run on the blockchain. It can be tough to maliciously manipulate or tamper the code. Users who depend on the written code are almost assured that it will behave as they anticipate it to. Even though attacks together with DAO or computational denial of provider took place lately, it became because of the vulnerabilities of clever contract code or operation code fuel charge no longer vulnerabilities on basics of blockchain or Ethereum itself. Thus, once the device is stabilized and matures, it could become a stronger device.

When the machine is stabilized, it could be utilized in huge tiers of domain. Because of its transparency because people can study it publicly to be had good judgment or code of smart contracts, betting or gambling carrier can be carried out and used. Consequently, there are numerous corporations, industries and people who are searching for their personal use cases of Ethereum [10].

III. MANAGING PREPAYMENT METER WITH ETHEREUM

A. Concept Model, scheme

In order to make proof of concept, only a few devices will be used instead of hundred. Specifically, we will use two smartphones, two Raspberry Pis, and two prepayment meter. For the prepayment meter we will attach the Raspberry Pi to it and then we let the electricity flow throughout the meter while keeping track of electricity usage. Using the Wattcoins Wallet in the smartphone, user can set up the policy and make Wattcoins transaction. For example, the user can set the device to turn on power saving mode when the electricity usage reached 100 KW. When the user deploys new configuration via smartphone, the data will be sent to the Ethereum network and automatically give updates to the new configuration to the prepayment meter. In the meantime, the prepayment meter keeps track of electricity usage and updates it on Ethereum. Thus three different processes are happening simultaneously.

Figure 1 shows the conceptual diagram of the system. The system involves six significance identities: the Wattcoin wallet which is the mobile application or web application that provide the front-end for the Billing system, the Smart Meter which is running the Ethereum Virtual Client that connected to the Ethereum Blockchain Network, Ethereum network that consists of many Ethereum nodes that connected each other, community that represent the people who involved with the system to sell or buy the electricity asset and supplier that represent the organization that provide the electricity.

The user needs to download the Wattcoin wallet application from the trusted source which means the Supplier will host the application to some trusted hub so the user can trust the application and download it, thus he/she will install the application. Then, the Wattocoin wallet application will generate a private and public key and submit the public key to the Ethereum Network. The Ethereum network will receive the public key and generate a wallet address and send it to the user. Once the user received the wallet address from the blockchain network, he/she will install and export the wallet address to the Smart Meter by accessing the front-end of the Smart Meter via web service provided by the devices. When the installation of the smart meter succeeds, it will check for the wallet address whether it has enough balance or not for the meter to supply the electricity to the electrical appliance. If not, the user needs to buy some electricity tokens from the supplier. The smart meter will calculate the electricity usage of every electrical appliance connected to him. So, periodically the smart meter will interact with the Exhaustion Contract in order to deduct the token from the user account and send the token to the supplier account. On the other hand, the user also can buy the token from the community or their neighbor.

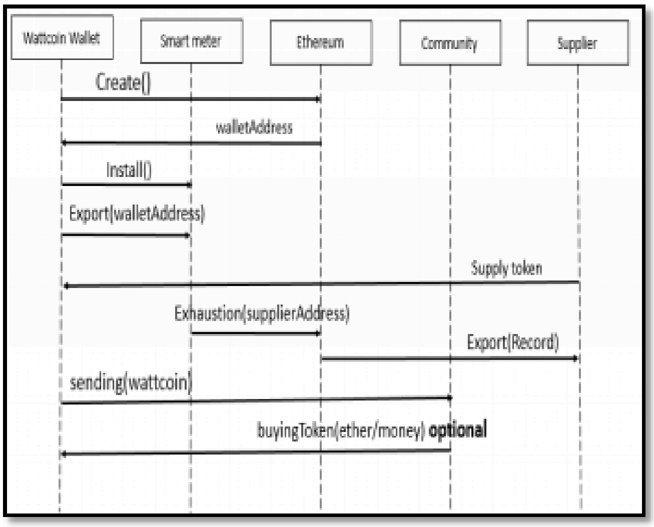


Figure 1 : Concept Diagram

B. Ethereum Model

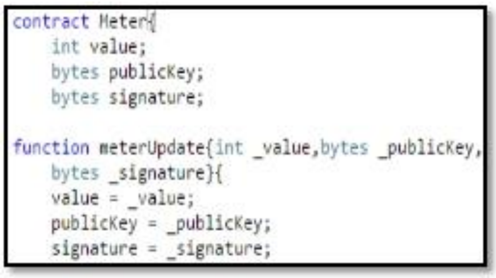
Different from the client-server model, Ethereum is a decentralized computing platform, which means all the blockchain nodes have the same copy of the data. The raspberry pi will act as the Ethereum Virtual Machine and connected to all Ethereum Virtual Machine and all nodes maintaining the same databases. The front-end of the system is stored on smartphone, which Wattcoins Wallet and connected to the Ethereum Virtual Machine via Remote Procedure Code (RPC), Web3, and JavaScript. All transactions are executed and stored via consensus algorithm, which means all the transactions are tamper proof. Besides, blockchain protects the privacy of the user to stay anonymous by implementing pseudonymous. Furthermore, the advantages of this blockchain technologies are to prevent the Denial of Service attack by implementing Proof-of-Work consensus mechanism.

C. Smart Contract

Ethereum is a smart contract enabled blockchain beyond Bitcoin. Nick Szabo was the one who introduced this smart contract in 1994 [11]. The developer writes the smart contract and program on top of the blockchain platform. Furthermore, code can be completely added on the blockchain and with zero single point of failure. There are programming languages consisting of Solidity, Serpent, and LLL in Ethereum. At this point, Solidity is the most widely used language and compiler. This excessive degree language is compiled into byte codes and deployed onto Ethereum. Considering the fact that byte codes are a listing of opcode, Ethereum nodes follow the one's instructions inside the code as soon as the corresponding contract is completed from legitimate account.

For the conducted experiment, two contracts have been built. The first contract is for tracking the value of the meter which is Exhaustion Function. While the second contract is for saving policy values of the meter. In order to verify the account, digital signature and public key were added to the contract. Thus, the attacker cannot simply manipulate the data stored in the smart contract.

Meter Contract: Ahead of a smart contract, meter occasionally saves the electricity that has been used. Precisely, Raspberry Pi holding an Ethereum account acts as a device that monitors meter and sends the value to Ethereum. So, as to show the identity of the sender, it is necessary for the sender to send its public key and signature along with the usage of electricity as shown in Figure 2.

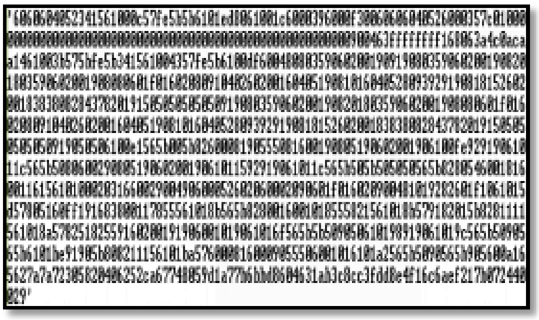


```
contract Meter{
    int value;
    bytes publicKey;
    bytes signature;

function meterUpdate(int _value,bytes _publicKey,
    bytes _signature){
    value = _value;
    publicKey = _publicKey;
    signature = _signature;
```

Figure 2 : Simple example of meter contract

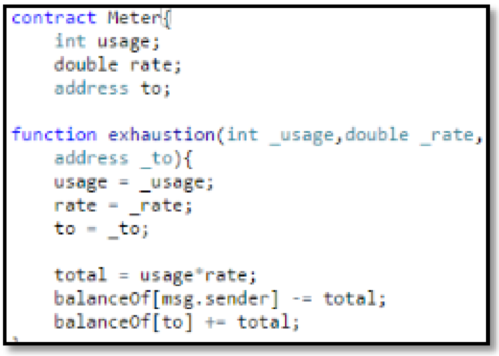
The meter contract is really simple and understandable. The prepayment meter is an Ethereum Virtual Machine that can sign and send the transaction which contains value, public key and signature. Furthermore, each contract contains its own address. Thus, it can identify where the data is sent in order to execute the contract. All the contracts need to be compiled into byte code so it can be executed into Ethereum Virtual Machine. Hence, it will increase the execution time. For instance, the contract can be encoded as in Figure 3.



```
'6060604052341561000c57fe5b5b6101ed8061001c6000396000f30060606040526000357c01000
000000000000000000000000000000000000000000000000000000000900463ffffffff168063a4c0aca
a14610003b575bfe5b341561000435 7fe5b6100df6004808035906020019091908035906020019082
18035906020019080806001f01602080910402602001604051908101604052809392919081815260
0018383808284378201915050505050919080359060200190820180359060200190808060 1f016
02080910402602001604051908101604052809392919081815260200183838082843782019150505
0505050919050506100e1565b005b6026000190555060019080519060200190610 0fe929190610
11c565b5060060029080519060200190610115929190610 11c565b505b50505050565b82805460018160
0011615610100020316600290049060005260206000209060 1f016020900481019282601f10610 15
d57805160ff191683800117855561018b565b82800160010185558215610 18b579182015b8281111
561018a578251825591602001919060010190610 16f565b5b50905061019891906101 9c565b50905
65b6101be91905b808211156101ba576000816000905550600101610 1a2565b5090565b905600a16
5627a7a723058204 06252ca67748059d1a77b6bbd8604631ab3c8cc3fdd8e4f16c6aef217b072440
029'
```

Figure 3 : Example for compiled contract code

Exhaustion Function: Exhaustion Function is one of the mechanisms in the meter that will automatically deduct the Wattcoin in every account based on the rate and usage of the electricity. Then, there is also exhaustion account which is the account of the electricity supplier, so the meter will periodically deduct the user's Wattcoins and sends the Wattcoin to the supplier account. Figure 4 shows the example of the Exhaustion Function in the meter contract.



```
contract Meter{
    int usage;
    double rate;
    address to;

function exhaustion(int _usage,double _rate,
    address _to){
    usage = _usage;
    rate = _rate;
    to = _to;

    total = usage*rate;
    balanceOf[msg.sender] -= total;
    balanceOf[to] += total;
```

Figure 4 : Exhaustion Function in the Meter Contract

D. Wallet Address

Every meter needs to have an address in order to interact with the other meters. The generation of the wallet address is derived from the public key of the meter by using the Elliptic curve digital signature algorithm (ECDSA). The advantage of the ECDSA is the key sized generated is much smaller than RSA by giving the same security level as RSA. In order to generate a private key EDSA only select a number from 1 to secp256k1n number and the private key is stored in the devices and secured by password. After that, it uses the ECDSAPUBKEY function to generate public key. Then, it utilises KECCAK-256 algorithm to derive the public key into a string and it takes the first twenty bytes of the string as an address.

E. Blockchain Gateway Server

To develop a web or mobile application as Wattcoins wallet a gateway interface is needed in order to make the mobile or web application interacts with the blockchain network. The gateway interface must provide a web socket connection, this is because to access an account in the public ledger, a user needs to pass his private key to the gateway server and the channel must be secured. The other advantages of the gateway interface are the mobile devices do not need to download and synchronize their databases with the blockchain public databases. Furthermore, Ethereum does not provide a lightweight client for the Android operating system as well as apple operating system. The mobile devices only communicate with the blockchain gateway interface by using Remote Procedure Call (RPC) protocol.

IV. Discussion

This paper describes the deployment of all the electricity meter contracts on the Ethereum Virtual Machine. Once the meter contracts have been deployed, the supply input is embedded in the Ethereum Virtual Machine in order to trigger all the functions in the meter. Thus all the output from the Ethereum Virtual Machine can be retrieved. Then, the mobile devices will be used to store the front-end user interface that will communicate to the Ethereum Virtual Machine via Jason Remote Procedure Code (JsonRPC) to make Wattcoin transaction between owners of the meter.

Furthermore, even the Ethereum is a trusted platform that can predict some issues that will occur when the system is deployed with the Ethereum. This is due to the issue of Ethereum that does not provide a light client for the Raspberry Pi. It can cause insufficient storage to store transaction data. Thus, larger storage is needed for the Raspberry Pi. Moreover, Ethereum takes 12 seconds time stamp for every transaction and this will cause some problems in the Time Sensitive Networking in the term of Time Synchronization Policies.

V. Conclusion

In this paper, we present an approach to implement the electricity sharing utilizing a blockchain platform by using the existing power distribution system. The smart contract is designed to the make transactions and requests to the Ethereum Virtual Machine. Using Ethereum account, electricity meter periodically sends transaction and the electricity use over the Ethereum platform. Meter owners can also use mobile devices to make electricity sharing between them. Since it is feasible to build such a system, a further study that involves a large scale can be developed for such system to contain multiple meter devices.

References

[1] Q. Ma, C. Duan, X. Ding, T. Qian, and P. Duan, “A design of Network Prepayment Meter Reading System based on ESAM,” in *2012 7th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2012, pp. 686–690

[2] D. San-lei, Y. Jing-feng, W. Fu-sheng, and Q. Hua-kun, “Design of prepayment implementation and its data exchange security protection based on Power Metering Automatic system,” in *2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, 2012, vol. 3, pp. 331–335.

[3] D. H. Mun, M. L. Dinh, and Y. W. Kwon, “An Assessment of Internet of Things Protocols for Resource-Constrained Applications,” in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, 2016, vol. 1, pp. 555–560.

[4] I. I. Atanasov, “Structure of semantic information for prepaid smart metering,” in *2015 12th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS)*, 2015, pp. 293–296.

[5] B. S. Elhassan, E. M. Imam, Y. M. Alsideeq, and S. F. Babikir, “Fault diagnosis using cross-wavelet transform for electricity pre-payment meter,” in *2017 International Conference on Communication, Control, Computing and Electronics Engineering (ICCCCEE)*, 2017, pp. 1–5.

[6] D. Bradbury, “Blockchain’s,” *Engineering Technology*, vol. 11, no. 10, pp. 44–47, Nov. 2016.

[7] V. Buterin and others, Ethereum white paper. 2013.

[8] “Writing a contract | Ethereum Frontier Guide.” [Online]. Available: https://ethereum.gitbooks.io/frontier-guide/content/writing_contract.html. [Accessed: 17-May-2017].

[9] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum Project Yellow Paper*, vol. 151, 2014.

[10] “Thomson Reuters Demos New Ethereum Blockchain Use Cases - CoinDesk.” [Online]. Available: http://www.coindesk.com/thomson-reuters-blockchain-ethereum-devcon2/. [Accessed: 17-May-2017].

[11] N. Szabo, “Formalizing and securing relationships on public networks,” *First Monday*, vol. 2, no. 9, 1997.