RESEARCH ARTICLE OPEN ACCESS

A Virtual Energy Trading Platform for Smart Homes

Shruti Hegde [1], Ashwini B V [2], Shylaja Madasu [3]
Department Of Computer Science & Engg
Brindavan College Of Engineering,VTU
Banglore - India

ABSTRACT

Renewable energies are becoming a major source o0f energy for all the applications in our day to day life. Micro grids are used to establish the energy trading platforms. These have helped in introducing a variety of applications and ingenious solutions for effective system maintenance. In this paper we delve deeper and outline the various core components and functions of the smart home tier. Each smart home is equipped with an always online, high resource device, known as ”miner” that is responsible for handling all communication within and external to the home. The miner also preserves a private and secure BC, used for controlling and auditing communications. We show that our proposed Blockchain-based smart home framework is secure by thoroughly analyzing its security with respect to the fundamental security goals of confidentiality, integrity, and availability. This paper proposes a system without the third party intervention using renewable energy installed in micro grids for the smart homes.

Keywords :-- Micro grid,smart home, block chain,smart contract, network security, energy trade

I. INTRODUCTION

IoT is a technology in which numerous devices and persons are connected together through the internet; and exchange vast amount of data and have a high risc of cyber attacks[1]. Smart homes are connected with home appliances ,energy devices all consume less energy. Thus security methods are expensive because of energy consumption and functionality[2]. The Smart Grid provides automated energy network between suppliers and consumers.

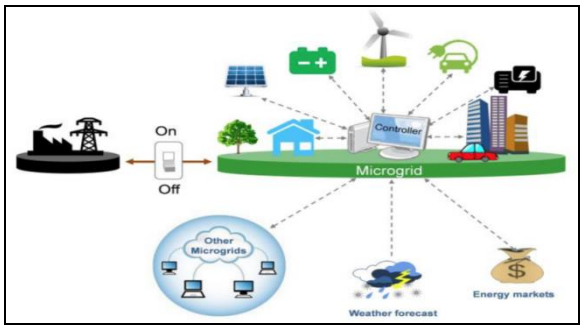

Fig 1. Microgrid on a blockchain

In this paper, secure and automated renewable energy trading within the micro grid using smart in block chain technology is proposed . The micro grid node has two groups: consumer and prosumer. Prosumer is capable of producing renewable energy itself. Each smart home is equipped with an always online, high resource device, known as “miner” that is responsible for handling all communication within and external to the home. The miner also preserves a private and secure BC, used for controlling and auditing communications. We show that our proposed BC-based smart home framework is secure by thoroughly analysing its security with respect to the fundamental security goals of confidentiality, integrity, and availability. Finally, we present simulation results to highlight that the overheads (in terms of traffic, processing time and energy consumption) introduced by our approach are insignificant relative to its security and privacy gains. Each node in smart homes have an ESS which can store energy which is monitored by home miner.

II. PROPERTIES OF BLOCKCHAIN

Block chain records transactions continuously which is known as blocks using hash-based PoW which cannot be changed without doing the Proof of work[5]. Node that records the transactions broadcasts to all the nodes in the network and only few nodes try to solve the PoW or the cryptographic paradox[4] are known as miners.

Every transaction in the block chain requires a valid digital signature which can be generated with digital keys which ensures authentication and non-repudiation. Later the transaction is verified and can never be erased[6].

These blockchains can be divided into two types: public and private block chain. Public block chain,allow any number of nodes without limitations for example includes ethereum [7] or bitcoin[5]. In private block chain, the participant nodes are decided in advance and specific nodes can be added or removed as needed which in turn reduces processing cost and time.

A. *Blockchain as a data structure*

A blockchain is a growing record of data, compiled as virtual blocks. Block chain records transactions continuously which is known as blocks using hash-based PoW which cannot be changed without doing the Proof of work[5]. Node that records the transactions broadcasts to all the nodes in the network and only few nodes try to solve the PoW or the cryptographic paradox[4] are known as miners.

In Bitcoin’s blockchain, the data being recorded is Bitcoin transactions. The structure starts with a single

block, known as the genesis block. As the amount of data recorded on the system increases, more blocks keep getting added. Each block in the sequence is linked to the previous block, going all the way back to the genesis block. This "chain" of blocks is what gives this type of data structure its clever name.

Many word and photo processing applications create stacks of data linked sequentially, so a user can "undo" the most recent state and revert to the previous state.

B. Immutability and tamper detection in blockchain

Data stored in the blockchain is made secure and immutable using cryptography. Every block is referenced by a unique string of characters, generated by a cryptographic hash function. This function can accept any amount of data as inputs and generate a fixed length string as output. This fixed length output is known as a hash. Each block links to the previous block (known as the parent block) by storing the hash of the parent. One of the striking properties of the hash function is that even a small change in the input generates a completely different hash output. Therefore, any changes made to the contents of a block will change the hash of the block. Each block stores the hash of the parent block, going all the way to the genesis block. Hence a data tamper in any block across the blockchain will change the hash of all subsequent blocks. This way an observer can identify tampering at any point on the blockchain, without having to verify contents of each and every block.

Data recorded in blockchain is further made secure by using private/public pairs of digital keys, as we will see in the next section.

C. Data protection in blockchain

Instead of a physical or online account that has to be maintained by a third party (such as a bank), every unit of Bitcoin is stored on the blockchain itself. Users can securely access bitcoins using their private/public key pairs. A consumer can spend or transfer her bitcoins only by using her private keys, while a merchant can receive bitcoins by sharing her public keys with the consumer. Once the transaction has been relayed throughout the internet and included in a block, it is considered permanent. The merchant can then irrefutably claim ownership of those Bitcoins. She can also use her own private keys to spend those Bitcoins and so on.

The blockchain is typically stored and maintained on multiple devices. Thousands of devices worldwide store the Bitcoin blockchain. Thus, the data is protected even if one or more of the devices are compromised by an attack or network issues.

D. Decentralizededger technology

We shall now talk about perhaps the most popular attribute of the blockchain, the decentralized ledger of data. The ledger can be shared among a private group of users connected through the local area network, or with thousands across the internet. A message is relayed on creation of every new block, to ensure that all users have a latest version of the ledger. This feature has applications well beyond digital currencies, as it eliminates the need of a trusted central party to record the information. Areas ripe for disruption through decentralization include stock exchanges, real estate transactions, personal identification and many more.

Since the ledger is stored on multiple storage devices, possibly in different locations, it also protects the system from data loss in case any devices or servers face downtime. Other users can continue accessing and adding information on the blockchain, as long as there is at least one online device that has the latest version of the blockchain. Every transaction in the block chain requires a valid digital signature which can be generated with digital keys which ensures authentication and non-repudiation. Later the transaction is verified and can never be erased[6].

E. Blockchain's solution to double spending

Double spending is quite simply the risk that a user may spend the same units twice. This is akin to sharing a message on Whatsapp (the ubiquitous messaging app) with several contacts. The receivers may not even be aware of how many others got the same message. While this is not a bug (it is in fact a feature) in Whatsapp, it could spell disaster when transferring money or shares. If we could sell the same artwork or apartment to different buyers, that would render those assets effectively worthless. This is the reason we have authorized clearing houses to settle trades in the stock markets.

Bitcoin found an elegant solution by implementing a decentralized ledger and a consensus mechanism, allowing users to vote on valid transactions to be added to the latest block. Once the block has been relayed across the network, anyone can verify if the user actually owns the coins that he/she wishes to spend.

III. ENERGY MANAGEMENT IN BLOCKCHAIN BASED SMART HOME IN THE MICROGRID

A. Blockchain Based Smart Home in the Microgrid.

IoT devices, ESS and home miner in a smart home generate, collect, process, and exchange vast amounts of data that can be used to manage, control and monitor everything that happens in a smart home. As shown in Figure 2, the microgrid, a small-scale grid, is constructed as a private blockchain network. Each node of blockchain is a smart home consisting of IoT devices, energy storage device, home miner and solar

panel only for prosumers that produce renewable energy by itself. Here, smart home miner is a device that centrally processes incoming and outgoing data to and from smart home and implements energy trading by smart contract. And the miner is placed between devices and home gateway. IoT devices are connected via WiFi, so they exchange data with home miner by wireless communication.

The data generated in the smart home is called transactions.

The transactions are added to the block by adding several parameters including device ID, home owner ID, transaction type by the home miner after being authenticated and authorized. The home miner of each smart home collects the transactions not included in the block and works on finding a difficult PoW.

When a home miner is successful in PoW, the block consisting of several transactions is appended to the blockchain and miner broadcasts the block to all home miners. They accept the block only if all transactions in it are valid. After this, the transactions included in the block are never forge or falsified.

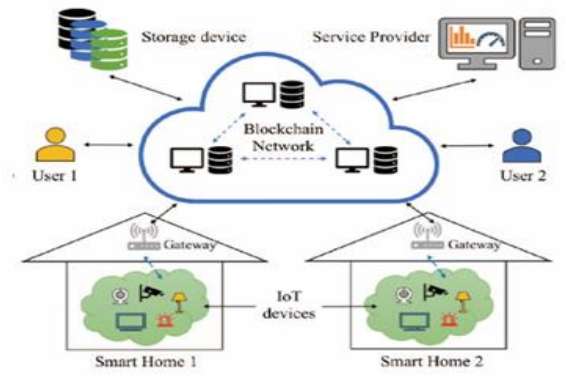

Fig 2: Private Blockchain network for Smart Home

Because this consensus process is achieved within the private block chain, sufficient security is provided and processing cost and time can be reduced.

B. Energy Management

Through ESS, the blockchain based smart home can store energy used in the house. Consumers purchase energy from prosumers that they need to consume and they charge energy to the energy storage device in the house. Prosumers produce renewable energy itself with photovoltaic system and store it in energy storage device to sell energy to consumers. The aforementioned home miner can centrally process data from all devices and ESS and store data in a connected cloud system or data storage. Using stored data, the home miner can know the current state, the operation history, energy usage of each device, energy output and the amount of energy remaining in the energy storage device. Other than that, more information is available and can be used for various applications. However, the proposed energy trading platform only requires information on energy usage of each device and the amount of energy remaining in the energy storage device.

IV. PROPOSED SYSTEM

In the Proposed system ,ENERGY TRADE PROCESS using smart contract has been introduced.In this system the consumer's home miner monitors energy usage and energy remaining in real time. If consumer's home miner determines that the stored energy is in sufficient, it implements energy trading by smart contract with prosumer's home miner and charges the energy storage device with energy. Consumer's home miner and prosumer's home miners are included in private blockchain network.

1) Prosumer must register the smart contract in which the transaction conditions are written to sell the energy. When the PoW is completed, the smart contract is included in the block.

2) Both the consumer and the prosumer set the price and transaction process. When the PoW is completed, contents of price and transaction process is included in the block.

3) If consumer's home miner determines that the amount of energy remaining is not sufficient, it will convey purchase intention to prosumer. And transaction matching begins.

4) If the transaction matching is successful, the energy transaction is completed. Thus the consumer is supplied with energy and the prosumer receives the price. The above process uses ethereum's smart contract based on blockchain technology. Because of data integrity characteristics of blockchain, it is not possible to forge or falsify the information about the energy. In addition, using ethereum's smart contract[8], energy transaction is automatically achieved in real time without the third party intervention.

V. CONCLUSION

This paper mainly focuses on energy management in smart homes that uses block chain systems and propose the use of micro grids a renewable energy trading platform . Here the home miner can manage, control and monitor all the devices which is included in the block of block chain technology which provides security for the data. The transactions are not possible to create because of block chain and smart contract characteristic and is achieved automatically. Hence, it is possible to expand it to more and more nodes and get closer to the micro grid system. A decentralized renewable energy trading platform can be built in full scale for the virtual micro grid.

REFERENCES

[1] S. sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead." Computer Networks, vol. 76, pp. 146-164, 2015.

[2] Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home.", The University of New South Wales, 2017

[3] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang, "Smart Grid – The New and Improved Power Grid: A Survey." IEEE Communications Surveys & tutorials, vol. 14, Dec. 2011, pp 944-980, doi: 10.1009/SURV.2011.101911.00087

[4] S. King, "Primecoin: Cryptocurrency with prime number proof-of- work," July 7th, 2013

[5] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system.", 2008

[6] M. Crosby, Nachiappan, P. Pattanayak, S. Verma and V. Kalyanaraman. (2015). "Blockchain Technology Beyond Bitcoin." Sutardja Center for Entrepreneurship&Technology, http://scet.berkeley.edu/wp-content/uploads/ AIR-2016- Blockchain.pdf (accessed June 20, 2016)

[7] Buterin, Vitalik. "Ethereum White Paper.", 2013 Seyoung Huh, Sangrae Cho, and Soohyung Kim. "Managing IoT Devices using Blockchain Platform." ETRI, 2017