INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

ISSN

Impact Factor: 7.488

Blockchain with Smart Contract for Internet of Things

Bagule Akshayvilas[1], Dr Shyam Gupta[2]

PG Student, Siddhant College of Engineering, MH, India[1]

Associate Professor, Department of Computer Engineering, Siddhant College of Engineering MH, India[2]

ABSTRACT: Blockchain has widely exploded due to distributed peer-to-peer networks, which allows nontrusting users to interact with each other without having any intermediate owner or administrator. The transaction in the peer-to-peer networks by two nontrusting users can be done in a verifiable manner with the help of blockchain itself. To automate the process of any blockchain application various scripts are written which reside on blockchain and are called as Smart Contracts. Combination of blockchain with internet of things would result in a great Application inclusion, application would be secured from its core with many cryptographic algorithms instead providing external security factors. Certain modifications or issues should also be considered before deploying blockchain with internet of things, these will help in digitizing many applications with security and reducing faults and time complexity avoiding third party intermediate. Conclusion is that blockchain and internet of things combination can cause a great transformation and advancements in various industrial sectors with new and efficient business models.

KEYWORDS: Blockchain, Smart contracts, internet of things, digitization, security inclusion, distributed systems.

I. INTRODUCTION

Recently Blockchain has attracted stakeholder from wide range of industrial sectors from finance departments to healthcare, utility sectors, government sectors, real estate, etc. With combining existing applications with blockchain technology they will become more secure and often decentralized in nature, without need of central authority carrying out same certainty was not possible easily, but with the blockchain it has become very easy and reliable. Blockchain provides trustless networks as the parties can make transactions even though they don't trust each other, the absence of central trusty or authority increases the transactions time making the transact more reliable and scalable. The key characteristics of blockchain is that it makes heavy use of cryptography algorithms with makes it unbreakable in terms of security, avoiding central authority increases reconciliation between the parties making the transactions.

Automated scripts called smart contracts which resides on blockchain are used to manage the heavy and distributed workflow of the applications, logical functions are written in smart contract to ensure blockchain to process accordingly. Blockchain was introduced to solve the double spending problem with the digital money or electronic cash, blockchain has the distributed data structure which it replicates and shares among the other network members. On the other side, smart contact executes automatically between the networks to handle the newly integrated concepts. Detailed information should be gathered to integrate blockchain with internet of things. Here the focus is to make paper/receipt free transactions based on the blockchain technology.

II. RELATED WORK

A. How blockchain works with smart contracts

Existing technologies has to maintain central authority or trusty administrator for avoiding double spending problem that is to keep track of every transactions between two parties and no transactions are made between two parties who don't trust each other in any scenario, but with the explosion of blockchain technology each and every sector based on continuous transactions can enable blockchain into existing applications ensuring the high level security and avoiding double spending problem, central authority and maintaining trustless networks. Blockchain is nothing but the collections of blocks, each block is identified as block hash or cryptographic hash which maintains the hash of the before block along with timestamp.

Smart contracts are the scripts that are used to integrate application level logic on the networks, smart contracts reside on blockchain and are executed automatically accordingly. They are responsible to manage the distributed and heavy networks.
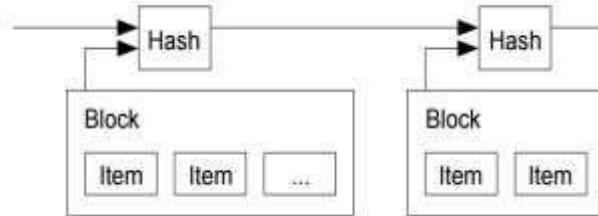

Fig.1. Block hash with information of other hash.

B. How Reliability of blockchain with internet of things

Existing centralized model for internet of things has highly maintenance cost where a small update in the device has to reach the millions of users even to them who have been long discontinued with the devices. From the users side the updates requires large amount of time and the central device has to send it to every device connected in network. Here the central device is in continuous work until all updates are done, but manufacturer now a days realized that blockchain could really solve this problem by its decentralized nature. With the blockchain integration the central authority has to take part just for the few device updates and onwards this device will share the firmware or software updates within the other devices in the network which will reduce central device workload and making the updates more scalable and secure with the help of in build blockchain cryptography.

III. METHODOLOGY

Blockchain with smart contracts can be very useful in Internet of things to avoid the high cost and make it more scalable in terms of efficiency and security. Designing of paperless carparking or any other applications which requires receipts, paper bills can be avoided using this technology. The existing system for the car parking has the receipt which the party will get during the entrance time and has to keep it safely until they exit the parking area, and at the time of parking specific amount for the parking is taken along with the receipt. The amount of paper used is very large and resources are used to maintain the receipt and bills for the process. Blockchain can be used to avoid the same problem and making the application decentralized.
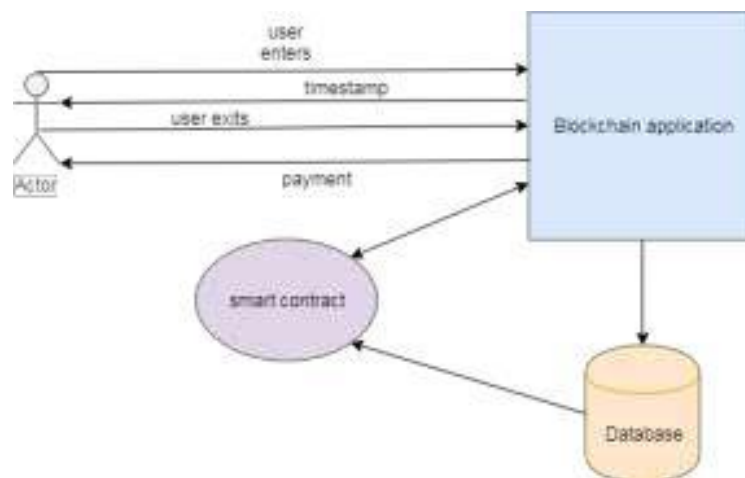

Fig.2. Block diagram of proposed system

Here the proposed application will have an application based on blockchain will which generate a unique cryptographic hash when user registers with the application and that block hash will be used for the payment of the car parking, the user when entering the parking has to initiate the application so the time of the parking will be started and when he is going to exit again he has to initiate the application which will calculate the total bill with respect to time and is submitted to the central authority without any third party vendor.

In this scenario when the user initiates the application while he is exiting from the parking the smart contract is triggered and the amount according to time is calculated and user is asked to pay the amount through tokens or any respective currency. The user will be provided with the QR code, when scanned the central owner address will be shown and user can transfer the amount to respective address. Here if the user is x and the central owner is y we can conclude how the process will be executed.

Our mobile application will act as the node or device which will be synced with the blockchain or block hashes.

A. Mathematical algorithm

- X enters.

- Timestamp is recorded as t1.

  - X about to exit.

- Timestamp is recorded as t2
  - Smart contract S is initiated.

  - t1 –t2 is calculated.

  - Amount is generated based on t value

  - User has to scan the QR code of Y.

  - Y unique address will be shown.

  - Payment is done.

  - Y exits.

Here we can show all the transactions in the applications where all the users will have the transparency about the last transactions done.

The central owner will be provided with the administrator panel where he can login and export all the transactions, can change the per hour rates of the parking, vehicle based rates can be applied, etc.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

Before analyzing the results of our system, we will just review how existing system works and what modifications we have done to make it more scalable and secure. The existing system is receipt/paper based system where the user has to keep the receipt until he exits the car parking zone, and at the time of exit the amount is to be paid by showing the receipt. This workflow lead to wastage of paper to large extent and also increases the resources to handle the process, whereas the solution is not generic in terms of technical terms. In our proposed system we have excluded the resources and use of paper making the system eco-friendly. The transactions are also very secured and decentralized because of use of the blockchain technology.

This combination of blockchain with internet of things using smart contracts is not specific to some applications but can be used in wide range of areas where the security and resources can be reduced to large extent providing more secure networks along with decentralized nature. Here we are proposing this to ensure that many applications depending on internet of things can be integrated with blockchain to make it more secure and scalable. The key features our application is that it is robust, secured and transparent compare to existing application.

V. CONCLUSION

The proposed system demonstrates that combination of blockchains and Internet of things are very powerful. Blockchain gives us trusty distributed peer-to-peer network systems and ensures the security in the trustless networks and with auditable manner. Smart contract allows to process multi-step complex logical entities along with blockchain.

IoT devices are directly connected with the physical world, hence combining these all technologies together will automate the whole process along with cryptographic verifiability as well as significant time and cost savings. The integration of the blockchain with IoT domain will result in extremely advanced transformations in various industrial sectors bringing new business models improvising the existing systems

REFERENCES

[1] J. Kelly and A. Williams. (2016). Forty Big Banks Test Blockchain-Based Bond Trading System.

[2] I. Kar. (2016). Estonian Citizens Will Soon Have the World's Most Hack-Proof Health-Care Records. [Online].

[3] W. Suberg. (2015). Factom's Latest Partnership Takes on US Health- care.

[4] S. Lacey. (2016). The Energy Blockchain: How Bitcoin Could be a Catalyst for the Distributed Grid.

[5] D. Oparah. (2016). 3 Ways That the Blockchain Will Change the Real Estate Market.

[6] A. Mizrahi. (2015). A Blockchain-Based Property Ownership Recording System.

[7] M. Walport, ''Distributed ledger technology: beyond block chain,'' U.K. Government Office Sci., London, U.K., Tech. Rep.,Jan. 2016.

[8] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[9] Double-Spending—BitcoinWiKi, accessed on Mar. 15, 2016.

[10] T. Swanson, ''Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems,'' Tech. Rep., Apr. 2015.

[11] M. Castro and B. Liskov, ''Practical Byzantine fault tolerance,'' in Proc. OSDI, vol. 99. 1999, pp. 173–186.

[12] L. Lamport, R. Shostak, and M. Pease, ''The Byzantine generals problem,'' ACM Trans. Program. Lang. Syst., vol. 4, no. 3, pp. 382–401, Jul. 1982.

[13] C. Cachin, R. Guerraoui, and L. Rodrigues, Introduction to Reliable and Secure Distributed Programming. New York, NY, USA: Springer, 2011.

[14] Hyperledger/Fabric: Blockchain Fabric Incubator Code, accessed on Mar. 15, 2016.

[15]   D. Ongaro and J. Ousterhout, ''In search of an understandablecon- sensus algorithm,'' in Proc. USENIX Conf. USENIX Annu. Tech. Conf. (USENIX ATC), Berkeley, CA, USA, 2014, pp. 305–320.

[16]   Juno: Smart Contracts Running on a BFT Hardened Raft, accessed on Mar. 15, 2016.

[17]   Blockchain App Development Simplified—Tendermint, accessed on Mar. 15, 2016.

[18]   D. Schwartz, N. Youngs, and A. Britto, ''The ripple protocol consensus algorithm,'' Ripple Labs, Inc., San Francisco, CA, USA, Tech. Rep., 2014.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING