ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Survey on Linking Smart Devices using Decentralised Applications

Deepali Ahir, Vinisha Athwani, Shreya Khandelwal, Sarosh Aga

Dept. of Computer Engineering, MESCOE (Affiliated to the SPPU), Pune, India

ABSTRACT: Internet of Things applications like Smart Homes need a viable technology option that is suitable to ensure implementation of the concept. Current technologies that connect smart devices to one another rely on rudimentary wireless technologies which provide no scope of introducing true automation. They also do not provide an efficient method of performing computation and handling security risks.

Using distributed computing, we disperse the computation work over thousands of devices and reduce the load on the device under consideration itself. To ensure that these devices have a safe and efficient environment to automatically perform tasks and interact with each other and their environments, we propose deploying this distributed network of devices onto the Blockchain: which is a technology borrowed from cryptocurrency which uses the concepts of public ledgers, mathematical hash functions and cryptography to ensure security and is the perfect candidate platform build a network of inter-communicating autonomous machines.

KEYWORDS: Smart Appliances; Smart Home; Blockchain; Cryptocurrency; Internet of Things; Distributed Applications

I. Introduction

In recent years, we have observed a significant paradigm and technological shift in the Internet of Things' field which has the potential to impact people's lives, bodies, homes and almost everything else they touch in a major way. This has allowed us to envision a world in which autonomous machines bring efficiency, flexibility and convenience into our day-to-day lives. This connectivity is an incredible thing, but one major question remains within the burgeoning IoT industry: what is the best way to go about implementing it, taking into consideration all the issues that come with this technology?

The Internet of Things has inherent security concerns that are brought in because of distributed computing; a few weaknesses that can be exploited by attackers are: data transfer, data storage in remote locations, concerns about automation, as well as financial security. The solution may be one of the most unique innovations of the digital era: the Blockchain. The Blockchain model was originally developed as part of the Bitcoin digital currency platform, and it also features inherent permanence as well as transparency. These are integral in the creation of a secure means of direct authentication between autonomous smart devices.

For the Internet of Things, a Blockchain can help to manage device identity, thereby preventing a spoofing attack wherein a malicious party impersonates another device to steal data or implement similar malicious intents.

A vital factor of the Blockchain's effectiveness is the fact that it works as a public record, with all the user nodes auditing the same instance of the record. Evidently, with a public record, there are always privacy concerns about sensitive information. However, the Blockchain ensures protection by making use of one-way hashes. In the Blockchain, a cryptographic hash function denotes a mathematical algorithm which maps the data and limits its size to a bit string, "a hash function", that is also one-way and almost impossible to invert. This implies it is practically impossible to obtain the contents of a hash without procuring the source data.

As well as ensuring the security of transactions, the Blockchain is a suitable candidate for providing a communication network for interaction between machines without the need for human interference to ensure successful exchange of information. Thus, we can use it to create a marketplace where buying and selling of goods and resources between machines can occur seamlessly. Trading is a human concept and to apply it to machines we need to overcome a few problems: Money exists to facilitate trade. Trade among humans has become increasingly complex over the years. It is recorded in human-made ledgers but is closed to the public. These ledgers are kept by Governments, Banks, Accountants etc.. This is a trust based system. Contrary to that, in a Blockchain, public ledgers of transactions are maintained by everyone who is using the Blockchain. There is no need for trust in this scenario since the existence of the Blockchainitself guarantees the authenticity of a transaction. Machines do not understand the concept of trust and the transparency in the Blockchain enforces the trust into the system. Financial transactions among the machines thus becomes viable with the Blockchain.

Blockchain represents a unique type of solution for the Internet of Things, one that is established as a secure means of protecting financial data but flexible enough to be applied to any high-stakes record keeping. With the Internet of Things demonstrating the ability to connect just about every aspect of a person's life, it truly doesn't get any more high stakes than that.

II. Related work

In [1], the authors describe how arbitrarily long messages like text or other similar digital data can be embedded into the Bitcoinblockchain by using an application of arithmetic coding. The work presented in [2], describes a software module which enables any home-automation devices to interact via the IPv6 network protocol. Each autonomous device can interact actively with its environment, as it has been made accessible by its unique IPv6 address that identifies it on the Internet. In [3], we have a system which employs 3G, and ZIGBEE technologies to overcome the limitations of smart home systems such as weak portability, poor updating capability, as well as dependence on personal computers. We can study the presented system architecture, and its gateway design from software to hardware. In the proposed smart home embedded system in [4], data received from the sensors in the smart-home can immediately be analysed. Network Address Translation (NAT) technology can help to monitor the usage of each component in the smart scenario, as the sensors transmit updates/messages to the integrated monitoring system. [5] describes a framework in which the server is interfaced with some relay hardware circuit components that can control the devices running at home.

In [6], we can observe an IoT E-business model, which is optimised for E-business over the Internet of Things, using smart contracts over the blockchain. In [7], the authors look into how smart contracts-scripts on the blockchain facilitate the automation of multi-step processes, which is relevant in our smart home scenario.When we consider the service analytics of the various connected devices in the smart home scenario, we see that in [8] that Sensor Markup Language (SenML) encodes the values read from the IoT device parameters- this simplifies the analysis of the tasks undertaken by the heterogenous devices connected in the smart home. An Event Manager module could be integrated to allow interoperation between the devices. Corresponding to our observations, in [9], the authors have highlighted the foundation for decentralised IoT to include Peer-to-Peer decentralised networks which enables participants of the network to be at the same privilege level. It also removes the single point of failure that is an issue in popular client-server based systems. Peer-to-Peer messaging and distributed file transfers are also described as key components- in P2P messaging,the focus is on trust, fast message transfer rates, as well as store-and-forward of messages to the connected devices. We can implement such messaging using Distributed Hash Table (DHT) which allows peers to use a hash table which has (key, value) pairs. Every peer can generate its own individual public-key hash-name for sending and receiving data from the other peers. We also saw an implementation for Autonomous Device Coordination - wherein we have a framework which allows users to describe their method of interaction with their devices, as well as allows devices to autonomously verify peers on the network, and allows manufacturers to register the devices in a universal register.

The delay of the transaction confirmation in Bitcoin is why it is not popularly used for payments that require quick confirmation of transactions. In [10], the authors have presented a concept that addresses this drawback of Bitcoin and enables it to be used for fast transactions. The authors judged the effectiveness of the concept by using double-spending attacks, and by showing that using their method, the success of such attacks reduced to less than 0.09%. In [11], the authors conjecture that the network propagation delay is the main cause of blockchain forks, which cause inconsistencies in the network. Ways to allay this problem are then discussed.

When it comes to privacy concerns in the Blockchain, [12] defines a mechanism to manage access

to the information and its aggregations. The scheme in [12] enables users (which includes organisations) to control access to their data collections.

DOI: 10.15680/IJIRCCE.2016. 0411015

III. Scope

The decentralised network that we are developing will serve as a platform for hosting smart devices in order to make a smart environment, in our case, a smart home. In order to truly ensure that smart devices and appliances can communicate with each other, a much more potent network is required for communication between machines than conventional client/server architectures.

These devices need to be able to analyse performance critical data and also carry out transactions and other such functionalities. They need to be able to interact with each other autonomously and without human intervention in order to conform with the Internet of Things guidelines. We will enforce this aspect by deploying the devices on a network called as a Blockchain. It is derived from cryptocurrency technology which ensures compliance, validation and security.

For example: A smart TV will receive an intimation about a bill payment that is due, from the cable company. The TV will automatically transfer the amount to the cable company. But that is just for one device. For a number of devices in a smart home, we will create a sub network which will be connected to a larger network. So these networks will also serve as a marketplace where communication between smart devices can take place. The goal is to create a truly financially autonomous IoT system free from any human intervention.

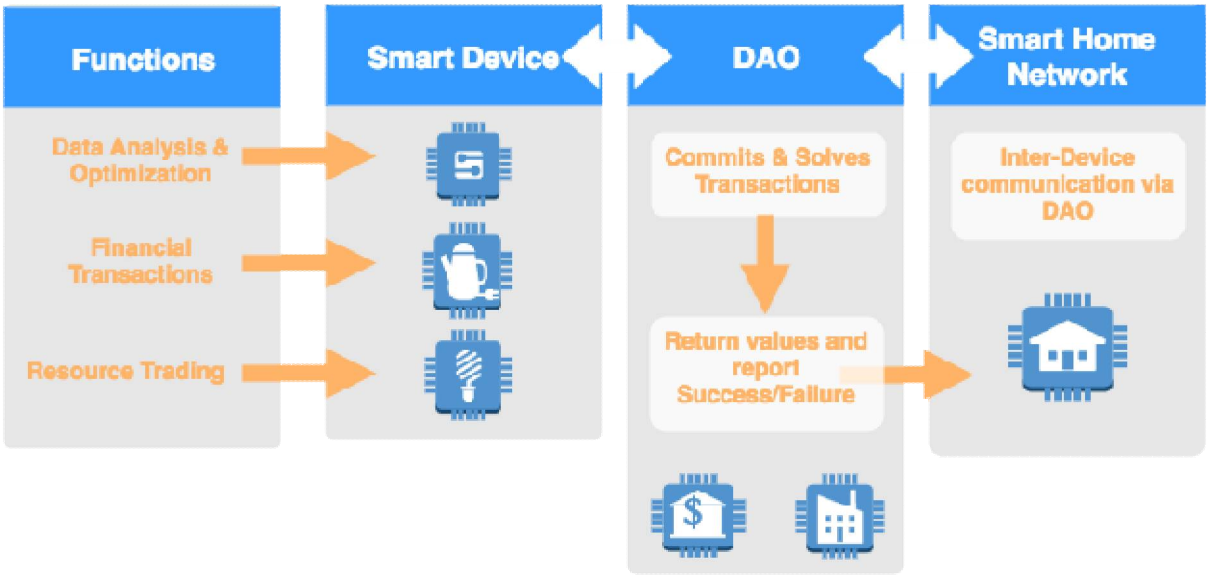
IV. Proposed Methodology and Design

A. *DESIGN:*

We have decided to divide our project into two major modules for implementation:

1) Module 1: A number of nodes (each representing a smart device) will be created. These nodes will be linked to each other wirelessly thus creating a logical network of devices. Each node, will be programmed to simulate an actual appliance used in houses. They shall also have autonomous control over functionalities like financial transactions, data analytics and communication with peers and foreign nodes.

2) Module 2: The logical network mentioned in the previous module is the representation of a smart home. But a smart home needs to interact with elements of the outside world and foreign networks. In our case, each node (smart device) interacts with its own DAO; which is the representation of a Service Provider in our project. A DAO is a decentralised network comprising of the service provider and all its clients using Decentralised Applications or DAPPS. Blockchains are used to implement the decentralised networks and the DAPPS run on the Blockchain.


Functions
Smart Device
DAO
Smart Home Network
Data Analysis & Optimization
Financial Transactions
Resource Trading
Commits & Solves Transactions
Return values and report Success/Failure
Inter-Device communication via DAO

DOI: 10.15680/IJIRCCE.2016. 0411015

B. *SYSTEM IMPLEMENTATION PLAN:*

1) Buying the required Raspberry Pi devices to act as the nodes
2) Installing Ethereum on the Raspberry Pi
    1. EthDev maintains three Ethereum clients: Eth (written in C++), Pyeth (written in Python), and Geth (written in Go).
    2. We choose to install PyEthApp, a simple to run instantiation of the Pyeth client
3) Configuring networking on the Raspberry Pi
4) Installing pyethapp
    1. pyethapp is the python based client implementing the Ethereumcryptoeconomic state machine.
    2. Ethereum as a platform is focussed on enabling people to build new ideas using blockchain technology.
    3. The python implementation aims to provide an easily hackable and extendable codebase. The latest version of the Serpent compiler is written in C++, allowing it to be easily included in any client.
5) Configuring Raspberry Pi to act as the required devices (eg: lights, fan, tv) by writing required scripts in Serpent
    1. Serpent is one of the high-level programming languages used to write Ethereum contracts. The language, as suggested by its name, is designed to be very similar to Python
6) Adding functionality to the devices to do the following:
    1. To add the transactions on the blockchain
    2. Analysis of usage
    3. Resource sharing between the nodes

V. Relevant Mathematics

Let S be the decentralised platform for smart devices
S = { I , O , F , S , Fa }
where,
I is a set of input attributes; I = { Du , R }
Du = Usage Data from appliance
R = Resources bought/acquired

O is a set of output attributes; O = { Fi, Da }
Fi = Financial transaction for buying
Da = Analysed data

F is a set of necessary and additional functions; F = { A , T , R }
A = Analyse Data
T = Perform Transaction
R = Resource Trading

S is a set of success achieved
S = { Transactions and communication achieved successfully }

Fa is a set of failure achieved
Fa = { Transactions and communication fails }

VI. Conclusion

This paper presents the preliminary idea of our project, the functionality and expected outcomes of the project are described in brief. The various requirements and modules along with the necessary diagrams have been explained in detail. Using the blockchain network to run decentralised applications for smart homes is the most realistic method of empowering the Internet of Things. The need for machines to be able to interact with each other, can be re- alised by deploying the machines onto a self-sustaining, self-correcting and self-compliant network which not only provides protocols for communication between devices but also provides security and guarantee of transaction success. These features can be leveraged and applied to normal networked computing devices, in scenarios like factories, assembly lines, warehouses, re- tail stores and as in this case, homes. Automation of single devices can be achieved easily. But creating an ecosystem of automated devices capable of autonomously interacting with each other requires a platform like blockchain. We have thus, proposed a plan to showcase how a smart home with appliances like Televisions, Lights, Fans, Washing Machines etc can be given 'smart' functionality and the capability to interact with each other and their environment.

REFERENCES

1. Matthew D. Sleiman, Adrian P. Lauf, Roman Yampolskiy, "Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System", International Conference on Cyberworlds, pp. 1-3, 2015
2. Vittorio Miori, Dario Russo, "Domotic Evolution towards the IoT", 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 1-2, 2014
3. Kang Bing, Liu Fu, Yun Zhuo, "Design of an Internet of Things-based smart home system", International Conference on Intelligent Control and Information Processing (ICICIP), pp. 2-3, 2011
4. Sung-Jung Hsiao, Kuang-Yow Lian, Wen-Tsai Sung, "Employing Cross-Platform Smart Home Control System with IOT Technology Base", International Symposium on Computer, Consumer and Control (IS3C), pp. 1-3, 2016
5. Pavithra, RanjithBalakrishnan, "IoT based monitoring and control system for home automation", Global Conference on Communication Technologies (GCCT), pp. 1-2, 2015
6. Yu Zhang, Jiangtao Wen, "IoT electric business model", 18th International Conference on Intelligence in Next Generation Networks, pp. 2, 2015
7. KonstantinoChristidis, Michael Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", Special Section on the Plethora of Research in Internet of Things (IoT), IEEEAccess, Vol. 4, pp. 1-2, 2016
8. ThinagaranPerumal, SoumyaKantiDatta, Christian Bonnet, "IoT Device Management Framework for Smart Home", IEEE 4th Global Conference on Consumer Electronics (GCCE), pp. 1-2, 2015
9. IBM ADEPT Practictioner Perspective, pp. 12-14, 2015
10. Tobias Bamert. Christian Decker, LennartElsen, Roger Wattenhofer, Samuel Welten, "Have a snack, pay with Bitcoin", IEEE P2P Proceedings, pp. 1-2, 2013
11. Christian Decker, Roger Wattenhofer, "Information Propagation in the Bitcoin Network", 13th IEEE International Conference on Peer-to-Peer Computing, pp. 1-2, 2013
12. SayedHadiHashemi, FarazFaghri, Paul Rausch, Roy H Campbell, "World of Empowered IoT Users", IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 1-2, 2016