Research Paper | Information Technology | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 2 | Feb 2017

CONVERGING BLOCKCHAIN TECHNOLOGY WITH THE INTERNET OF THINGS

Karthik Prabhu [1] | Keerthi Prabhu [2]

[1] Mediaocean Asia Pvt Ltd, Pune, Maharshtra, India.
[2] MKSSS's Cummins College Of Engineering For Women, Pune, Maharashtra, India.

ABSTRACT

: We present the concept of leveraging Blockchain technology, for the management and security of information related to the Internet Of Things. Here, we put forth a model for the intercommunication of smart devices, their identity management and information security, with Blockchain posing as the backbone. The model proposes to serve as a robust and scalable solution, in order to address the security and identity concerns, arising due to the distributed nature of the Internet of Things. The proposed model is further compared to the existing ones in practice.

KEYWORDS: blockchain, Internet Of Things, decentralization, security, cryptography, distributed database

INTRODUCTION

In today's world, there is an increasing demand to connect devices to the Internet. Studies and research estimate that, in the years to come, there would be a multitude of devices interconnected. With this happening, there arises the need for a stalwart mechanism to address the data storage and security concerns, pertaining to machine-to-machine communication. Solutions currently exist, which address these concerns by adopting a centralized architecture. However, there are some disadvantages of a centralized system. These include the risk of central point failure, lesser autonomy and high costs. In order to overcome these weaknesses, we propose to put forth a decentralized architecture, using blockchain technology. A blockchain is a type of distributed ledger, comprising of unchangeable, digitally recorded data in packages called blocks. These digitally recorded "blocks" of data are stored in a linear chain. Each block in the chain contains data, which is cryptographically hashed. Blockchain technology discards the need of any third-party or central authority for peer-to-peer transactions. The security and verifiability of data and its transfer is achieved using mathematically designed cryptosystems. Moreover, in case of a decentralized system, the risk of central point failure is avoided and it is better able to withstand malicious attacks.

METHOD OF STUDY

The Centralized Architecture

The current IoT systems rely on the centralized, brokered communication model which is also known as the client-server paradigm. All the devices which are present in the IoT are identified and authenticated and connected through cloud servers that support huge processing as well as storage capacities. The IoT systems depend on centralized trust brokers and protocols such as the SSL/TSL(Secure Sockets Layer/Transport Security Layer) or mechanisms such as thePublic Key Infrastructure(PKI) to identify the nodes in the network and control communications.

However, the rapid and chaotic growth of the IoT has also introduced several challenges. Some of the drawbacks of a centralized architecture are as follows:

- Single point of failure could bring down the entire system.
- The need to have equipment with higher processing capabilities.
- Lesser autonomy provided for branches or departments
- Under-utilization of resources when running lower applications.
- Inability to cater to localized requirements of the organization.
- High initial set-up cost.

Also, the diversity of ownership between devices and their supporting cloud infrastructure makes machine-to-machine (M2M) communications difficult. The centralized models also cause problems as the number of nodes in the network increase. The centralized servers also become a bottleneck and this central point of failure makes the IoT vulnerable to the attack known as the 'Denial Of Service attack' (DOS).

Need for a Decentralized Architecture

A decentralized approach to the IoT networking would solve many of the problems. Adopting a standardized peer-to-peer communication model process will significantly reduce the cost associated with installing and maintaining large centralized data centers and will distribute storage and computation needs. Thus, this will prevent failure in any single node in a network from bringing the entire network to a halting collapse.

To perform the functions of traditional IoT solutions without a centralized control, any decentralized approach must support three fundamental functions:

- Peer-to-peer messaging
- Distributed file sharing
- Autonomous device co-ordination

A decentralized technology such as the blockchain can be used in tracking billions of devices connected in the IoT and enable co-ordination between the devices. This decentralized approach would eliminate single points of failures, thus creating a more resilient system for the devices to run on .The cryptographic algorithms used by the blockchains would make the consumer data more private.

Securing IoT through Blockchain

International Data Corporation (IDC) estimates that 90% of organizations that implement the IoT will suffer an IoT-based breach of back-end IT systems by the year 2017.

Handling the enormous volume of existing and projected data is daunting. Managing the inevitable complexities of connecting to a seemingly unlimited list of devices is complicated. And the goal of turning the deluge of data into valuable actions seems impossible because of the many challenges. The existing security technologies will play a role in mitigating IoT risks but they are not enough. Businesses will have to tailor security to each IoT deployment according to the unique capabilities of the devices involved and the risks associated with the networks connected to those devices.

Blockchain attempts to address these growing security concerns in an elegant way. Blockchain is a database that maintains a continuously growing set of data records. It is distributed in nature, meaning that there is no master computer holding the entire chain. Rather, the participating nodes have a copy of the chain. It is ever-growing – data records are only added to the chain. A blockchain comprises essentially of 2 main elements :

- Transaction : The actions created by the participants of the system.
- Blocks : They record transactions and ensure correct sequence and prevent tampering of data. They also maintain an audit (timestamp) when the transactions are added.

Blockchain technology can be used in tracking multitude of connected devices, enable the processing of transactions and coordination between devices. This would ultimately lead to decreases costs, thereby increasing savings, eliminate single point failures and create a more resilient ecosystem for devices to run on. The cryptographic algorithms used by blockchains would make consumer data more private. The idea is to leverage the power of blockchain to treat message exchanges between the connected devices in the same way as financial transactions, which occur in the case of the bitcoin model, for which blockchain was originally designed.

The blockchain based model, would be used to register new devices, authenticate users, and perform various custom functions for devices. These functions would occur seamlessly and securely, without much risk of intrusion. The storage of information in a cryptographic format makes it hard for any kind of attack to occur on it. The blockchain would also serve as an abstraction to the information being transacted. That is, the communicating device does not have a need to customize the information in any way, before pushing it to the blockchain. The blockchain,, on its part, would as well be totally unaware of the actual message incoming to or outgoing from it.

Figure 1 proposes an algorithm to handle the intercommunication between 2 devices talking to each other with blockchain as the underlying database. The concept lies in the fact that any device wanting to send a message to another, needs to include its identity address (such as, the IP address) as well as the target device's address. This would result in a new block being added to the blockchain. Thus, the data persisted as part of the block, by the chain would comprise of the following:

- Source device address
- Target device address
- Message to be sent
- Cryptographic hash value created on the basis of data contained within the block

The cryptographic hash function, as said, would perform an encryption of an amalgamation of the data, contained within the block. The encryption used, for example, could be SHA-1.The encrypted result is persisted as part of extra information within the block. This result serves as the identity of the block as well as the identifier of the information within it. It also serves as a protection mechanism which will prevent tampering of data within the block.

For instance, let us take that an intruder manages to get hold of a block in the chain. He illegally modifies data in the block (let us take that modifies the IP address of the target device to point to his own). Now, this would immediately result in a mismatch between the encrypted hash value and the encryption of the data contained within the block, which will invalidate the block, thus preventing any further attack from the intruder.

RESULTS AND DISCUSSION

Thus, we have shown the methodology to leverage the benefit of blockchain for the intercommunication between devices as well as the comparison between centralized and decentralized systems, by way of the model presented. This has been done to address the challenges faced by the centralized nature of databases currently in use for IoT.

Comparison between Existing and Proposed Approach

Table 1: Difference between Existing and Proposed architecture

Points of Distinction	Existing Solution	Proposed Solution
Type of database	Centralized	Distributed
Data hosting	Cloud, private vendor etc	Blockchain itself
Transaction management	Trusted networks	Pseudonymous, open
Security Level	Dependent on provider	Strong due to data encryption and algorithm
How difficult is data tampering	Depends on efforts taken by provider	Fairly immutable due to longest chain rule

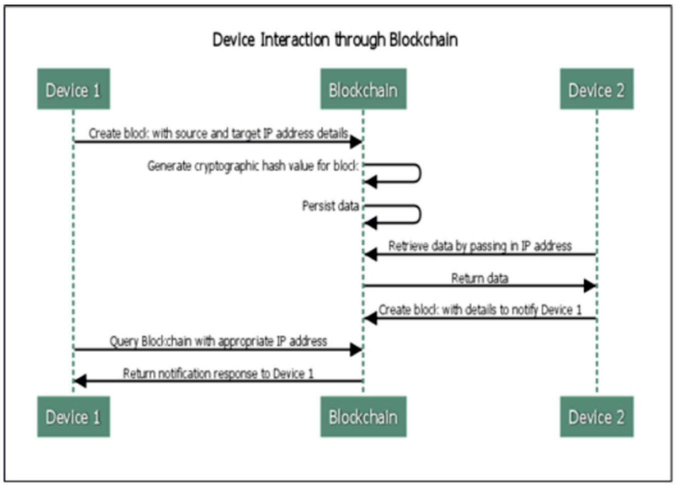
Device Interaction through Blockchain
Device 1
Blockchain
Device 2
Create block with source and target IP address details
Generate cryptographic hash value for block
Persist data
Retrieve data by passing in IP address
Return data
Create block with details to notify Device 1
Query Blockchain with appropriate IP address
Return notification response to Device 1
Device 1
Blockchain
Device 2

Figure 1: Sequence diagram to show interaction between devices through blockchain

REFERENCES

1. Sutardja Center, UC Berkeley, Blockchain Technology, Beyond Bitcoin (2015)
2. Melanie Swan, "Blockchain, Blueprint for a new economy" (2015)
3. IBM.com, What blockchain means for you, and the Internet of Things, (2017). [Online]. Available: https://www.ibm.com/blogs/internet-of-things/watson-iot-blockchain
4. How To Secure the Internet Of Things (IoT) with Blockchain, Retrieved from https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228
5. A gentle introduction to blockchain technology, Retrieved from https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/
6. UK Government Chief Scientific Advisor, Distributed Ledger Technology, (2015) [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
7. Infosys Consulting, Blockchain Technology and the Financial Services Market, (2016) [Online]. Available: https://www.infosys.com/consulting/insights/Documents/blockchain-technology.pdf
8. Barclays Capital, Blockchain: understanding the potential, [Online] Available: https://www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/insight/blockchain_understanding_the_potential.pdf
9. IBM, Blockchain Explained, (2016), [Online] Available: https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/Blockchain%20Explained/$file/Blockchain%20Explained.pdf
10. Ovidiu Vermesan, Peter Friess, Internet Of Things – Converging Technologies for Smart Environments and Integrated Ecosystems