International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Block Chain for Securing Internet of Things

Astha Kumari[1], Sayed Sohail[2], Ritwik Giri[3]

[1, 2, 3]Department of Information Science and Engineering, P E S Institute of Technology, Bangalore-560100, Karnataka, India

Abstract: ***More than a billion intelligent, connected devices already comprise today's "Internet of Things". IoT is bringing more and more things into the digital fold every day, which will likely make IoT a multitrillion dollar industry in the near future. However the rapid evolution of IoT market has caused an urgent need for secure IoT model. In this paper we discuss the current architecture of IoT which is based on centralized model and its inability to provide security to IoT devices. We simultaneously propose architecture of IoT ecosystem based on Block chain model. A Block chain is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them on to a single sheet of paper). Each block is then 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions. This decentralized implementation coupled with encryption can provide us the missing link to settle scalability, privacy, reliability and security concerns in the Internet of Things.***

Keywords: Block Chain, IoT, Centralized Model, Blocks, Decentralized Model, Miners, Ethereum Virtual Machine(EVM), Public Key Cryptography

1. Introduction

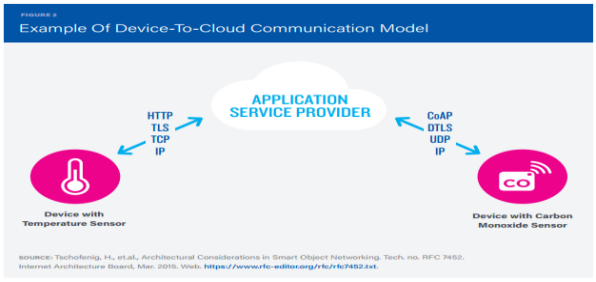
Block Chains are open, distributed ledger that can record transactions efficiently between two parties in a verifiable and permanent way[1]. Having high Byzantine fault tolerance, Block chains have interactive consistency, and can be used to achieve Decentralized consensus i.e. Shifting authority and credibility of a transaction to decentralized virtual networks. Block Chain grows as a set of ordered records called blocks. Each block holds a timestamp (keeping track of creation of blocks), link to previous block and valid transactions, hashed and encoded into Merkle Tree. Block Chains are resistant to modification of data (once recorded), and can't be altered retroactively.Despite of being peer to peer and distributed timestamping server Block Chains are still autonomous, where stigmergy approach is followed i.e. allowing to create leaders without orders. Each miner in a Block Chain, has a copy of block chain, hence data quality is maintained by massive database replication and computational trust (generation of trusted authorities using cryptography).Mining validates transactions, add them to block they are creating and then broadcast to other miners. Using a safe decentralized mechanism like this in technology like Internet of Things which is server/client paradigm, will definitely reduce the security and cost problems faced at present.Being persistent and secure Block Chain is all set to rewrite IoT architecture.

2. Current IoT Models and Demerits

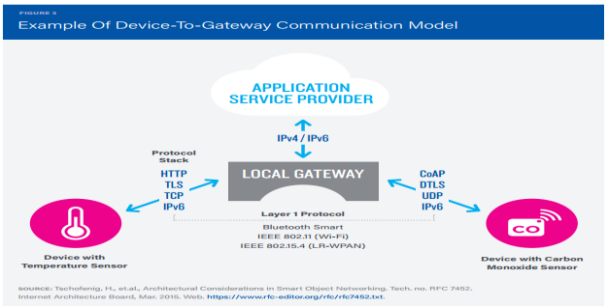
The current IoT ecosystems rely on centralized, brokered communication models like Device to Device Communication, Device to Cloud Communication, Device to gateway model, Back End sharing model.

Device to Device Communication model, where two or more devices that are directly connected, communicate among one another, rather through an intermediary application server.

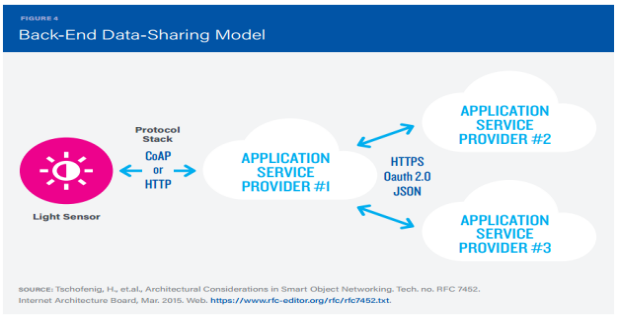
Device to Cloud Communication model, the IoT device connects directly to an Internet cloud service to exchange data and control message traffic.



In Device to Gateway model, application software operating on a local gateway device, acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation.



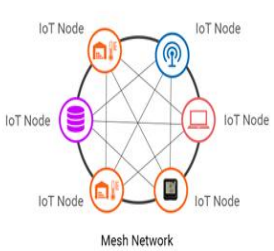
Back-end Data Sharing Model, refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources.



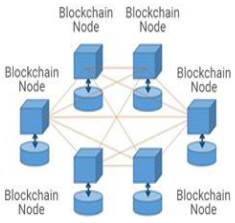
Above discussed models are prone to security and cost concerns. Cost for implementing IoT architecture is generally high and is prohibitive for individuals. Here is where block chain comes into picture.

3. Why Block Chain with IoT?

Both IoT and Block Chain technology are disruptive by nature. IoT being one of the hot trend right now, is highly insecure, one instance of that can be seen in distributed denial of service (DDoS) attack 2016, which affected millions of internet addresses. To overcome this, we can use a highly decentralized public mechanism i.e. block chain model. Block Chain ticks all the boxes for IoT and especially for individual inventor, this will open up massive free market opportunities. Block Chains are so secure that they can even be run on non- trusted computers. Block Chain is the missing link to settle privacy and reliability concerns in the internet of things. It can be the silver bullet needed by the IoT industry. The ledger is tamper-proof and cannot be manipulated by malicious actors because it doesn't exist in single location. Block Chain makes peer to peer messaging possible and has already proved its worth in financial industry. Next we will discuss the model architecture



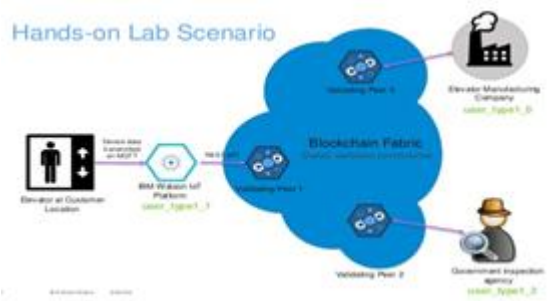
Mesh Network



Distributed Blockchain

4. Architecture

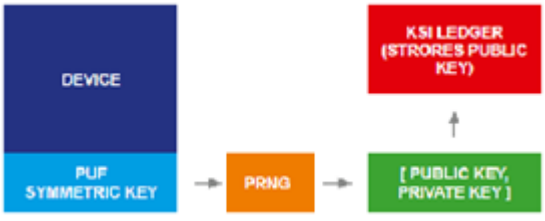
Once an IoT device enters Block Chain network, it can issue smart contracts or can be operated on smart contracts. Ethereum, open source for block chain, which provides Turing-Complete virtual machine i.e. Ethereum Virtual Machine[3] (EVM) can be used to make smart contracts. All the devices (blocks) can see blocks and the respective transactions, but not the actual information, which is protected by public key cryptography. Being decentralized, all the miners in network must reach a consensus to accept transactions rather than a single participant controlling everything (centralization). On addition, a transactions are also validated, i.e. Users come to consensus as what to accept. This is suitable for recording events and to provide data provenance. Then, after transactions are approved, they are bundled in a block, which gets sent to all the miners in the network. Miners, in turn validate the new block. Each block is then hashed with the reference of the previous block making it an iterative process, which confirms integrity of the previous block all the way to genesis block. Highest scoring version of Database is stored in the miners always. Within block chain, the computation is carried out redundantly rather than in a traditional segregated and parallel manner. Following figure shows working of IBM WATSON platform (which integrates block chain and IoT).



A new level of security and governance for customers to deploy IoT devices can be represented using combination of Block Chain and Physical Unclonable Function (PUF).PUF Technology can be used to authenticate a device and registering that device with ownership information on a Block chain ledger, the provenance and integrity of every piece of data generated can be cryptographically proven and can be linked back to an authenticated device with an end to end chain of custody.Most commonly used authentication approaches are based on online trust anchors/trusted third parties whereas a PUF based solution provides an offline method with a tamper resistant ID and resiliency. The shift from a user-centric world to a device-centric one can be aided by PUF technology via enabling:

- Trusted Discovery/Enrollment – To secure registration of the IoT device
- Trusted Interaction – That Authenticates and integrates communication amongst the IoT devices in the network

Using a Block chain to store data that has been secured with PUF derived keys and attributes provides an immutable assurance that data has not been tampered with, in addition to providing traceability and transparent auditing capabilities. PUFs use device unique random patterns to differentiate chipsfrom each other. PUFsare designed to be impossible to duplicate, clone or predict.



5. Applications

IoT technologies have quickly become one of the early adapters of block chain technology. By leveraging the block chain, IoT solutions can enable secure, trust less messaging between devices in an IoT network. IoT block chain can be used in Supply Chain[2], which will ensure proper access control for data which is shared among different participants in a supply chain. Another prominent application can be auto

motive sector, where Block chains are being used to provide real-time information and to execute transactions among key business partners. Under home automation, huge number of sensors are used, IoT block chain can secure devices and data collected from them.

6. Acknowledgment

We would like to acknowledge our teaching faculty and our parents for their support toward this project without which this project wouldn't have been possible.

References

[1] Wikipedia Block Chain
[2] https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/index.html
[3] http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html.