IoT DEVICE MANAGEMENT USING BLOCKCHAIN

CHRISTY VARGHESE, christyvarghese50@gmail.com
guided by, JISHA JOSE, jisharainbow@gmail.com

Abstract— **The Internet of Things (IoT) is establishing itself as part of the future Internet. One of the technical challenges of having billions of devices deployed worldwide is the ability to manage and synchronize them. In such situations, it is expected that using current model of server-client system may have some limitations and issues while in synchronization. Also security issues such as Denial of Service attack and data forgery are common. To overcome these limitations, building IoT system using blockchain is proposed. Specifically, Ethereum is chosen as the blockchain platform because using its smart contract, Turing-complete code can be written to run on top of Ethereum. A system with minimum number of devices is implemented to showcase the practical application of Ethereum platform to IoT. The proposed system forms a decentralized network offering transparency and security. It also guarantees authentication, synchronization and data integrity.**

Index Terms— IOT-Internet of Things, DoS- Denial of Service, DAO- Decentralized Autonomous Organization, PoW- Proof of Work.

I. INTRODUCTION

1.1 INTERNET OF THINGS

The Internet of Things specifies the vision in which objects become part of the Internet: where every object is exclusively identified, and accessible to the network, its position and status known, where services and intelligence are added to this expanded Internet, combining the digital and physical world into a single one. There is a very large variety of smart IoT devices that are being developed at each layer of IT. Each device has a definite purpose and specific characteristics. But a common aspect is that human is not the centre of the system but a part of it. With the fast-paced increment in the number of users of internet over the past decade has made internet an integral part of life, and IoT is the most recent and developing web innovation. IoT is a growing trend that has been called as the next Industrial Revolution and it will impact the way all businesses, governments, and consumers interact with the physical world. With the rise of IoT, the number and diversity of connected devices is expected to increase exponentially.

1.2 HOW IOT WORKS

An IoT ecosystem consists of web-enabled smart devices that use embedded processors, sensors and communication hardware to gather, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data is either sent to the cloud to be analyzed or analyzed locally. Sometimes, these devices communicate with other related devices and act on the information they get from one another.

The devices do most of the work without human intervention, although people can interact with the devices - for instance, to set them up, give them instructions or access the data. The connectivity, networking and communication protocols used with these web-enabled devices largely depend on the specific IoT applications deployed.

1.3 BENEFITS OF IOT

1. **Communication**: IoT encourages the communication between devices, also very well known as Machine-to-Machine (M2M) communication. Because of this, the physical devices are able to stay connected and hence the total transparency is available with marginal inefficiencies and greater quality.

2. **Automation and Control**: Due to physical objects getting connected and controlled digitally and centrally with wireless infrastructure, there is a large amount of automation and control in the workings. Without human intervention, the machines are able to communicate with each other leading to faster and timely output.

3. **Information**: It is obvious that having more information helps making better decisions. Whether it is mundane decisions as needing to know what to buy at the grocery store or if your company has enough widgets and supplies, knowledge is power and more knowledge is better.

4. **Monitor**: The second most obvious advantage of IoT is monitoring. Knowing the exact quantity of supplies or the air quality in your home, can further provide more information that could not have previously been collected easily. For instance, knowing that you are low on milk or printer ink could save you another trip to the store in the near future. Furthermore, monitoring the expiration of products can and will improve safety.

5. **Time**: As indicated in the previous examples, the amount of time saved because of IoT could be quite large. And in today's modern life, all could use more time.

6. **Money**: The biggest advantage of IoT is saving money. If the price of the tagging and monitoring equipment is less than the amount of money saved, then the Internet of Things will be very widely adopted. IoT fundamentally proves to be very helpful to people in their daily routines by making the appliances communicate to each other in an effective manner thereby saving and conserving energy and cost. Allowing the data to be communicated and shared between devices and then translating it into our required way, it makes our systems efficient.

7. **Automation of daily tasks leads to better monitoring of devices**: The IoT allows you to automate and control the tasks that are done on a daily basis, avoiding human intervention. Machine-to-machine communication helps to maintain transparency in the processes. It also leads to uniformity in the tasks. It can also maintain the quality of service. Necessary action can also be taken in case of emergencies.
8. **Efficient and Saves Time**: The machine-to-machine interaction provides better efficiency, hence; accurate results can be obtained fast. This results in saving valuable time. Instead of repeating the same tasks every day, it enables people to do other creative jobs.
9. **Saves Money**: Optimum utilization of energy and resources can be achieved by adopting this technology and keeping the devices under surveillance. People can be alerted in case of possible bottlenecks, breakdowns, and damages to the system. Hence, they can save money by using this technology.
10. **Better Quality of Life**: All the applications of this technology enables increased comfort, convenience, and better management, thereby improving the quality of life.

II. EXISTING SYSTEM

2.1 EXISTING ARCHITECTURE

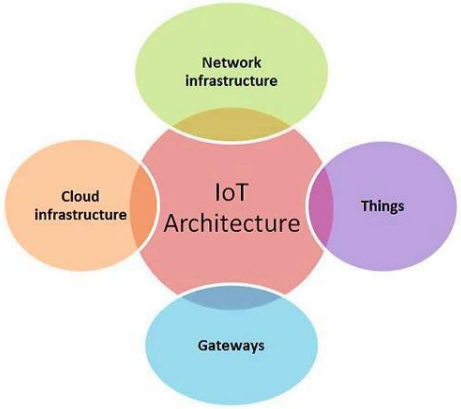

Figure 2.1: IOT- Existing Architecture

IoT architecture can be represented by following four main components:

1. **Things**: uniquely identifiable nodes, primarily sensors that communicate without human interaction using different connectivity methods.

2. **Gateways**: they act as intermediaries between things and the cloud to provide the needed connectivity, security, and manageability.

3. **Network Infrastructure**: set of devices that control and secure data flow (routers, aggregators, gateways, repeaters).

4. **Cloud infrastructure**: pools of virtualized servers and storage that are networked together with computing and analytical capabilities.

III. CHALLENGES FOR IOT SECURITY

a. Centralized architectures like the one used in cloud computing have significantly contributed to the development of IoT. However, regarding data transparency they act as black boxes and network participants do not have a clear vision of where and how the information they provide is going to be used. If the server is vulnerable, then all the relying devices will be in trouble. Also, due to the centralized nature, there is a higher chance for DoS attacks.

b. Authorize and authenticate devices: With so many devices offering potential points of failure within an IoT system, device authentication and authorization is critical for securing IoT systems. Devices must establish their identity before they can access gateways and upstream services and apps. However, there are many IoT devices that fall down when it comes to device authentication, for example, by using weak basic password authentication, or using passwords unchanged from their default values.

c. Secure communication: Once the devices themselves are secured, the next IoT security challenge is to ensure that communication across the network between devices and cloud services or apps is secure. Many IoT devices don't encrypt messages before sending them over the network.

d. Ensure data privacy, synchronization and integrity: It is also important that wherever the data ends up after it has been transmitted across the network, it is stored and processed securely. Implementing data privacy includes redacting or anonymizing sensitive data before it is stored or using data separation to decouple personally identifiable information from IoT data payloads. Data that is no longer required should be disposed of securely, and if data is stored, maintaining compliance with legal and regulatory frameworks is also an important challenge.

Also**,** there are more than hundreds of devices interconnected, it is a hassle to synchronize all of devices. Ensuring data integrity, which may involve employing checksums or digital signatures to ensure data has not been modified.

e. Ensure high availability: As people come to rely more on IoT within our day-to-day lives, IoT developers must consider the availability of IoT data and the web and mobile apps that rely on that data as well as our access to the physical things managed by IoT systems. The potential for disruption as a result of connectivity outages or device failures, or arising as a result of attacks like denial of service attacks, is more than just inconvenience. In some applications, the impact of the lack of availability could mean loss of revenue, damage to equipment, or even loss of life.

For example, in connected cities, IoT infrastructure is responsible for essential services such as traffic control, and in healthcare, IoT devices include pacemakers and insulin pumps. To ensure high availability, IoT devices must be protected against cyber-attacks as well as physical tampering. IoT systems must include redundancy to eliminate single points of failure, and should also be designed to be resilient and fault tolerant, so that they can adapt and recover quickly when problems do arise.

IV. PROPOSED SYSTEM

4.1 BLOCKCHAIN

A blockchain is a distributed database that maintains a continuously growing list of records, called blocks. It's an open distributed ledger that can record transactions between parties efficiently in a verifiable permanent way (no master host that holds the entire chain). Blockchains are secure by design from tampering and revision: once recorded, the data in a block cannot be altered. It offers a decentralized identity management (a user can register in the blockchain all by himself).

Through the use of a peer-to-peer network and a distributed timestamping server, a blockchain database is managed autonomously. A blockchain consists of two types of elements:

Transactions: The actions created by users in the system.

Blocks: Record of valid transactions in the correct sequence that are hashed and encoded to form a chain.

4.1.2 HOW A BLOCKCHAIN NETWORK RUNS

Nodes in the blockchain network form a peer-to-peer network by repeating the following process:

1. Nodes interact with the blockchain network via a pair of private/public keys. They use their private key to digitally sign their own transactions and they are addressable on the network via their public key. Every signed transaction is broadcast by a node that creates the transaction.

2. The transaction is then verified by all nodes in the blockchain network except the node that creates the transaction. In this step, invalid transactions are discarded. It is called verification.

3. Each node collects the transactions that have been validated in a certain time into a block and implements a proof-of-work finding a nonce for its block. When a node finds a nonce, it broadcasts the block to all nodes. This is a process called mining.

4. All nodes select a block broadcasted for the first time and verify that the block contains valid transactions, and references via hash the correct previous block on their chain. If that is the case, add the block to their chain and apply the transactions it contains to update their block chain. If that is not the case, the proposed block is discarded. This marks the end of current mining round.

4.1.3 VERIFICATION

Blockchain technology ensures the elimination of the double-spend problem, with the help of public-key cryptography, whereby each node is assigned a private key a public key shared with all other nodes. When a signed transaction is broadcast by a node that creates the transaction, all receiving nodes verify the transaction by decrypting a signature with a public key of a sending node. If a signature verification result is true, the signed transaction is verified that the sending node is not changed.

4.1.4 PROOF-OF-WORK

Any node in the peer-to-peer network of Blockchain can choose to be a miner. A miner is an entity that is responsible for mining (adding) new blocks to BC by solving a resource-intensive cryptographic puzzle called Proof Of Work (POW) and appending new blocks to Blockchain. When a new transaction occurs, it is broadcasted to the entire network. All miners who receive the new transaction verify it by validating the signatures contained within the transaction. Each miner appends the verified transaction to its own pending block of transactions that are waiting to be mined.

Each block contains a timestamp, a nonce (Proof Of Work) and the hash value of the previous block. The linked blocks form a chain. Each transaction is digitally signed and each user can verify its validity.

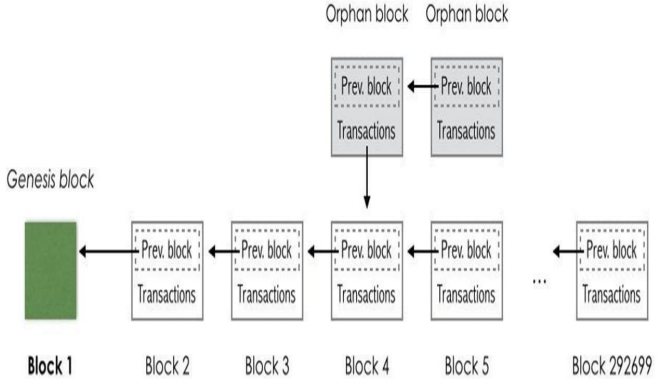

Figure 4.1: Example of Blockchain

To add a new block, the miner has to find a nonce such that:

$$H(nonce||H_{prevous}||trans_1||trans_2||trans_3||\ldots\ldots\ldots||trans_n) < target$$

where:

H= good and computationally hard hash function
Target = subset of the hash function output
$trans_i$= hashed value of the i-th transaction of the block

- The first who find the POW, can propose the block as the next block in the Blockchain and receive fees as incentive.
- The chain with the most cumulative Proof-Of-Work is always considered the valid chain by the network.

4.2 BLOCKCHAIN ADVANTAGES

The blockchain has some interesting advantages:

*Public every user can see the blocks and the transactions stored in them. This does not mean everyone can see the actual content of your transaction, indeed its content is protected by your private key.
*Decentralized there is no single authority that approves the transactions. This means that there's trust in BC, since all the participants in the network have to reach a consensus to accept transactions.

*Secure the existing database can only be extended and previous records cannot be changed (or rather, there's a very high cost if someone wants to tamper previous records).

4.3 BLOCKCHAIN IN IOT

Some features of Blockchain make it an attractive technology for addressing the security and privacy challenges in IoT:

- Decentralization the lack of central control ensures scalability and robustness by using resources of all participating nodes and eliminating many-to-one traffic flows. This also decreases delay and overcomes the problem of a single point of failure.
- Anonymity the inherent anonymity afforded is well-suited for most IoT use cases where the identity of the users must be kept private.
- Security Blockchain realizes a secure network over untrusted parties which is desirable in IoT with numerous and heterogeneous devices.

4.4 ETHEREUM

Proposed by Vatalik Buterin in 2013, Ethereum is a public blockchain-based distributed computing platform]. Unlike previous blockchain such as Bitcoin, it can work as a computer even though the performance will be slower than most of current PCs since it has a transaction time of around 12 seconds. But, because it has its own language such as Solidity or Serpent, it lets developers write and compile a program. Once compiled, it can run on Ethereum Virtual Machine. Just like any other computing environment, once it gets compiled, compiled code gets translated to opcode and then binary, which will be executed on Ethereum Virtual Machine environment. Thus Ethereum is unique in a sense that it combines computing system with blockchain. It is ground-breaking because it gives developers flexibility to write a code that can run on blockchain. Because it will be difficult
to maliciously manipulate or tamper the code, users who rely on the written code are almost guaranteed that it will behave as they expect it to.

The Ethereum Blockchain can be described as a transaction-based state machine. When it comes to computer science, a state machine is defined as something capable of reading a series of inputs and transitioning to a new state based on those inputs. When transactions are executed, the machine transitions into another state.

Every state of Ethereum consists of millions of transactions. Those transactions are grouped to form 'blocks,' with each and every block being chained together with its previous blocks. But before the transaction can be added to the ledger, it needs to be validated, that goes through mining.

4.4.1 SMART CONTRACT

Developers can write a program that can run on top of Ethereum called smart contract. A smart contract refers to the computer protocols or programs that allow a contract to be automatically executed/enforced taking into account a set of predefined conditions. Smart contracts define the application logic that will be executed whenever a transaction takes place. Ethereum is the largest decentralized platform that allows you to build unlimited Smart Contracts.

4.4.2 ADVANTAGES OF ETHEREUM PLATFORM

Ethereum platform benefits from all the properties of the Blockchain technology that it runs on. It is completely immune to any third party interventions, which means that all the decentralized apps and DAOs deployed within the network can't be controlled by anyone at all.

Any Blockchain network is formed around a principle of consensus, meaning that all the nodes within the system need to agree on every change made within it. This eliminates possibilities of fraud, corruption and makes the network tamper-proof. The whole platform is decentralized, which means there is no possible single point of failure. Hence, all the apps will always stay online and never switch off. Moreover, the decentralized nature and cryptographic security make the Ethereum network well protected against possible hacking attacks and fraudulent activities.

Ethereum also has its own added advantages. Since it has a transaction time of approximately 12 seconds, Ethereum is quicker. Ethereum platform allows to write complex programs, as the language used is Turing complete.

V. MANAGING IOT DEVICES USING ETHEREUM

5.1 SCENARIO

A few IoT devices are used instead of hundreds of devices in order to make a proof of concept. More specifically, a smart phone, and three Raspberry Pis are used. Each of the three Raspberry Pis is treated as a meter to keep track of electricity usage, an air conditioner, and a lightbulb since using actual device such as air conditioner would require too much overhead. Using a smart phone, user can set up the policy. For example, user can set devices to turn on energy saving mode when electricity usage hits 150 KW. When the user sets up the configuration via smartphone, the data is sent to the Ethereum network. In the meantime, devices such as lightbulb or air conditioner are retrieving values of policy periodically from Ethereum. Also meter keeps track of electricity usage and updates it on Ethereum. Thus three different processes are happening concurrently.

5.2 ETHEREUM MODEL

Unlike server-client model, Ethereum is a distributed computing platform, which means all of participating entities contain parts of Blockchain of Ethereum. Instead of sending to server, each device updating or making transactions contains Ethereum. Because blockchain is partially contained in contributing devices, transactions are executed and stored via consensus algorithm, which means attackers cannot forge or tamper data easily. Leveraging this characteristic lets us to build IoT system, which is strong enough to stand against many denial of service attacks and forgery attacks, if not all.

5.3 SMART CONTRACT

One of the most significant aspects of Ethereum lies in smart contract. The concept first introduced by Nick Szabo in 1994, smart contract brought innovation to blockchain. Ethereum uses smart contract on top of Blockchain so that developers can write a program on blockchain. In other words, using smart contract, Ethereum can be used as a computing platform. There are programming languages such as Solidity, Serpent, and LLL in Ethereum. At this point, solidity is the most widely used language and compiler. This high level
language once developed is compiled into byte codes. And those byte codes are deployed onto Ethereum. And since byte codes are simply a list of opcodes, Ethereum nodes follow those instructions in the code once the corresponding contract is executed from valid account. Three smart contracts are used here - one contract tracking the value of meter, one for saving policy values of each air conditioner and lightbulb. In order to authenticate valid account, signature and public key are added on both contracts. Thus, if malicious attackers try to manipulate the storage in smart contracts, computing systems in air conditioner or lightbulb can detect such attack and simply ignore them.

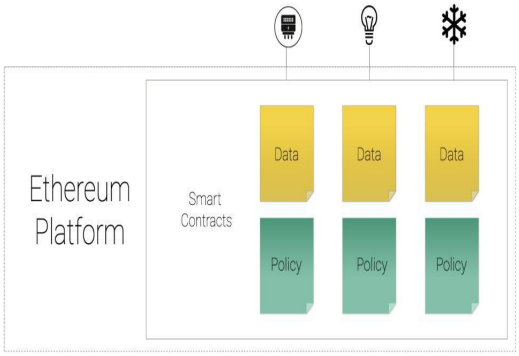

Fig 5.1: Managing IoT devices using Ethereum

Meter Contract: On a smart contract, meter periodically saves electricity use. Precisely, Raspberry Pi containing Ethereum account acts as an IoT device to monitor meter and sends the value to Ethereum. In order to show the identity of sender, sender needs to send its public key and signature along with electricity use. Meter device which contains Ethereum blockchain can simply sign and send input values of *value*, *publicKey*, and *signature*. Since each contract has its own unique address, the location to send data is known. In order to use *update* method, encode input values so it can run on Ethereum Virtual Machine.

Thus using meter contract, meter that is attached to Ethereum account can send values periodically to blockchain, which other entities such as air conditioner or lightbulb can retrieve.

Policy Contract: Along with meter, set up the policies. As mentioned in the scenario, set up policies for air conditioner and lightbulb. Given that if policy of air conditioner is set as 150KW, then once the meter reaches 150KW, air conditioner simply switches from normal mode to energy saving mode. The same scenario applies to lightbulb too. Similar to meter contract, policy needs to be registered. But instead of meter, smartphone is used to register. Smartphone that contains Ethereum account can send data to smart contract that manages policies. Once Ethereum account encodes policy with public key and signature, and sends them to Ethereum, those values are registered in contract.

Key Management: Given that all of those contracts are running on Ethereum, IoT devices such as air conditioner or light bulb need to retrieve values from both meter contract and policy contract. On values coming from meter contract, they check if inputs are valid using public key and signature. To be precisely, RSA algorithm is used, where smart phone and meter keep their secret keys. And on values from policy

contracts, they also check if inputs are valid using public key and signature. If the scenario where electricity use surpasses policy while periodically retrieving values, devices simply switch to energy saving mode.

CONCLUSION

A system with minimum number of devices was implemented to showcase the practical application of Ethereum platform to IoT. The proposed system make use of Ethereum, blockchain computing platform to manage IoT devices. As demonstrated, IoT devices can be managed and synchronized using the platform easily and effectively. Ethereum platform supports implementation of complex logic using its Turing complete language, which enables us to write our on application on top of the platform. The system forms a decentralized network offering advantages such as transparency and security. It also guarantees authentication, synchronization and data integrity through blockchain which is encrypted, distributed and consensus. Making use of blockchain, improvements on IoT occur where users of the technology do not need to worry about synchronization issues, denial of service attacks or data forgery challenges while serving them efficiently and fast.

REFERENCES

[1] Seyoung Huh, Sangrae Cho, Soohyung Kim, ”Managing IoT Devices using BlockchainPlatform”, 19th International Conference on Advanced Communication Technology (ICACT), pp 464-467, IEEE 2017

[2] Vignesh Govindraj, Mithileysh Sathiyanarayanan, Babangida Abubakar, “Customary homes to smart homes using Internet of Things (IoT) and mobile application”, International Conference On Smart Technologies For Smart Nation (SmartTechCon), pp 1059-1063, IEEE 2018

[3] Challenges in IoT security (https://developer.ibm.com/dwblog/2017/iot-security-challenges/)

[4] Introduction to Ethereum (http://ethdocs.org/en/latest/introduction/what-is-ethereum.html)