Managing Smart Home Appliances with Proof of Authority and Blockchain

Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi and Sukumar Nandi

Department Computer Science and Engineering, IITG, CITK and NIT AP, India

Overview

- Introduction
- Problem Statement
- Motivation
- Related Work
- Proposed Mechanism
- Experimental Setup
- Results
- Conclusion

Smart Homes

- With advance in technology and growth in standard of living smart homes are becoming a reality.
- Consists of home appliances and IoT devices that communicate with each other to address residents need.
- Devices generate, share and consume large volume of data that are private and sometimes safety critical to the residents.

Source : https://www.helpnetsecurity.com/2015/10/23/smart-home-security-and-privacy-checklist/

Problem Statement

- Current state of the art cloud based smart home services have availability and privacy issues.
- Users have no control over how their data is being utilized by the service providers.
- Less transparency.

Source : https://www.helpnetsecurity.com/2015/10/23/smart-home-security-and-privacy-checklist/

Motivation

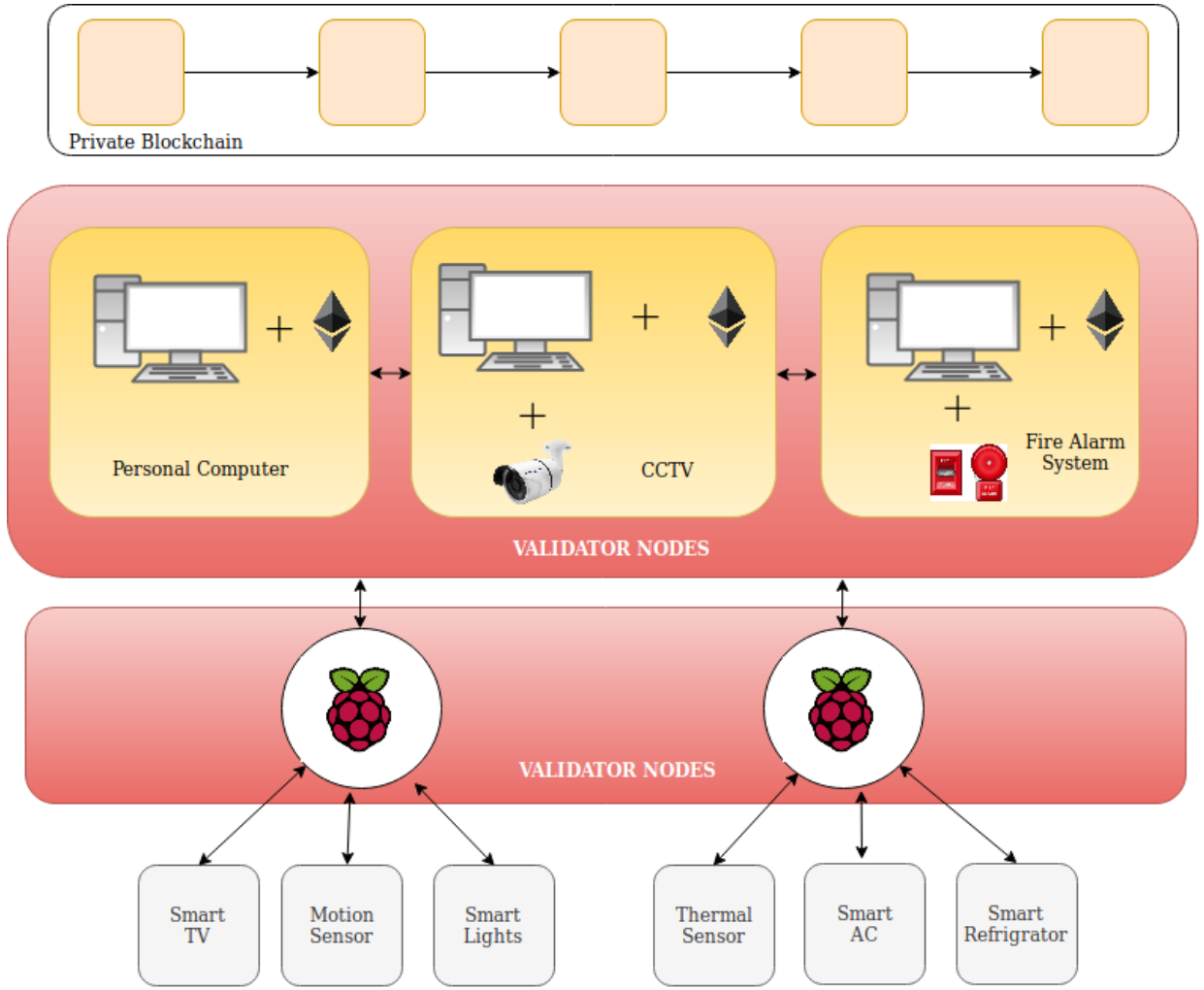
- Implement a smart home system to provide
  - High availability.
  - Efficient way of monitoring and auditing the in home happenings.
  - Preventing from non-repudiation of devices; identifying compromised and malfunctioned devices.
- Implementing low power consuming Proof of Authority(PoA) as the consensus mechanism for increased system performance .
- Removing the need of trust on untrusted cloud service providers.

Related Work

- In [10], the authors hacked into a variety of IoT enabled smart home devices
- In the past, numerous centralized solutions have been proposed
- Most of the solutions from industry deploy their proprietary solutions and serve as a centralized trusted third party.
- The major challenges with the centralized solutions are
  - Heavy communication and processing overheads on centralized server [3]
  - Transparency
  - Trust and privacy-related issues,
  - Access control and
  - Single point of failure.
- Various researchers [5,6,11,12,17] have turned-out the attention towards distributed framework and proposed popular blockchain based solutions

Proposed System Architecture

- **Home Owner :**
  - Configures home appliances,
  - Registers home residents to the system,
  - Deploys smart contract.
- **Validator Nodes:**
  - Devices having sufficient computing and storage capabilities.
  - Responsible for sealing of the blocks; and maintain the blockchain.
- **Smart Contract:**
  - Contains appropriate logic for interaction among the devices.
  - Specifies privileges of home residents.
- **Home Residents :**
  - Uses home appliances,
  - Make changes to the appliances; as per the privilege provided by the home owner.



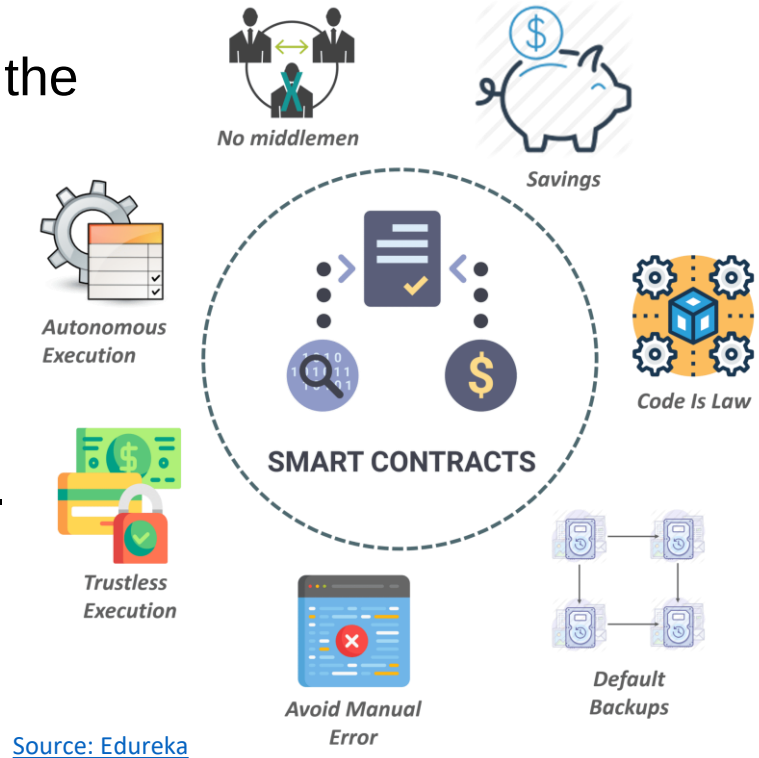
Blockchain Technologies Used

Ethereum:

- Public permissionless blockchain platform allows to setup a private and permissioned instance of the chain.
- Supports smart contracts (application specific code deployed on the blockchain).

Smart Contract:

- A bunch of self-executable code sitting on top of a blockchain.
- Consists of well-defined conditions and their corresponding actions.
- Triggered by the Transactions.

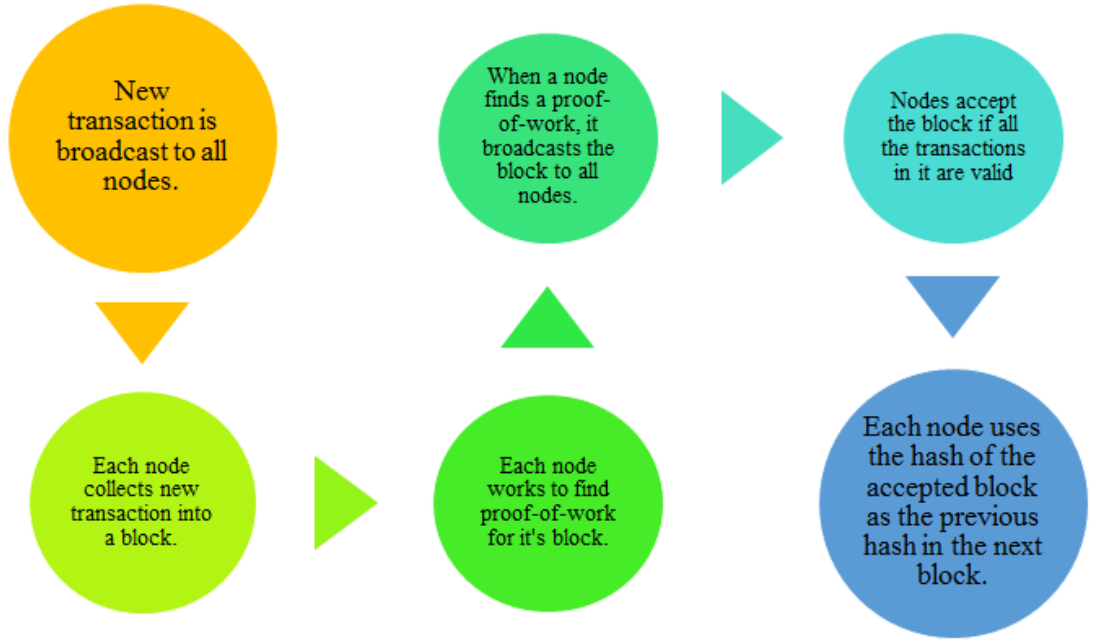


Source: Edureka

Consensus Mechanism

➢ Proof-of-Work (PoW):

- ❑ Have a variety of nodes such as full node, miner node, light node.
- ❑ In PoW mechanism, miners are responsible for maintaining the blockchain.
- ❑ Miners perform cryptographically hard and computationally resource intensive operations.



Source: EtherWorld.co

Consensus Mechanism Used

➢ Proof-of-Authority (PoA):

- ❑ A BFT consensus mechanism for private and permissioned blockchain.
- ❑ A set of validator maintains the blockchain,
- ❑ Run in rounds; A validator proposes a block in its respective round,
- ❑ Other validators verify the block and adds it onto the chain; reaching a consensus.

Source : https://cryptocurrencyhub.io/proof-of-authority-poa-b8faad1c768e?gi=cb0cc2a33d27

Experimental Setup

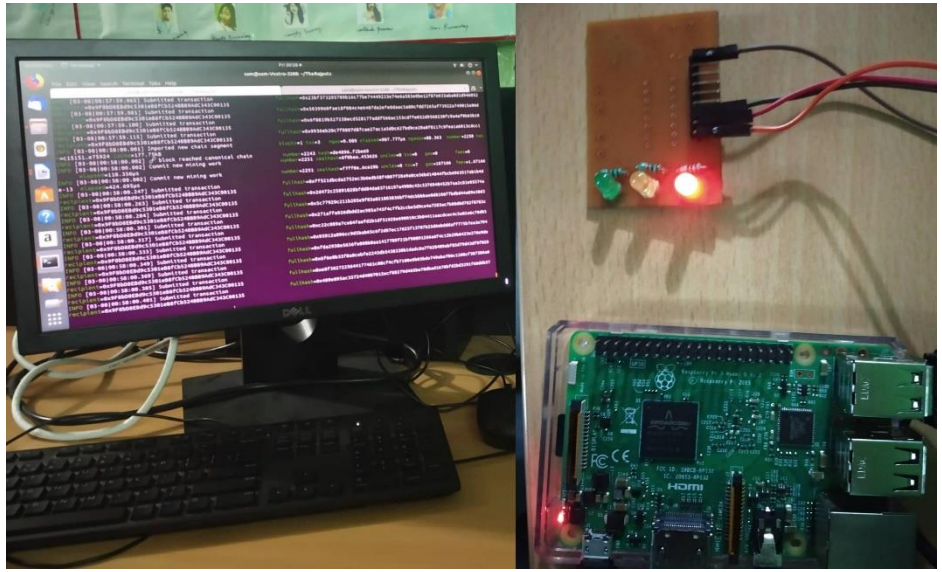


Fig. 1. Validator node & Processing Unit Setup

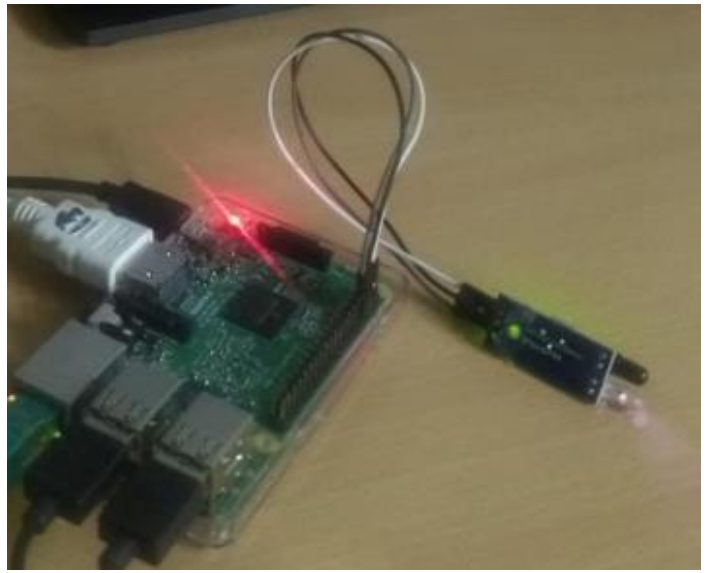


Fig. 2. IR sensor interfaced with Processing unit

Table 1. Devices and their role

Device name	No. of device	Geth version	Role
Dell-Vostro (8 GB RAM, i7-7700 CPU, 1 TB HDD)	1	v1.8.17-stable release	Validator
Raspberry Pi 3	1	geth 1.8.18 ARMv7	Validator (Processing Unit)
IR Sensor	1		Home IoT device
LED	2		Home appliance
nodeMCU	1		Home IoT device

System Characteristics

- Home resident can control the appliances via the smart contract.
- The activity is logged onto the blockchain.

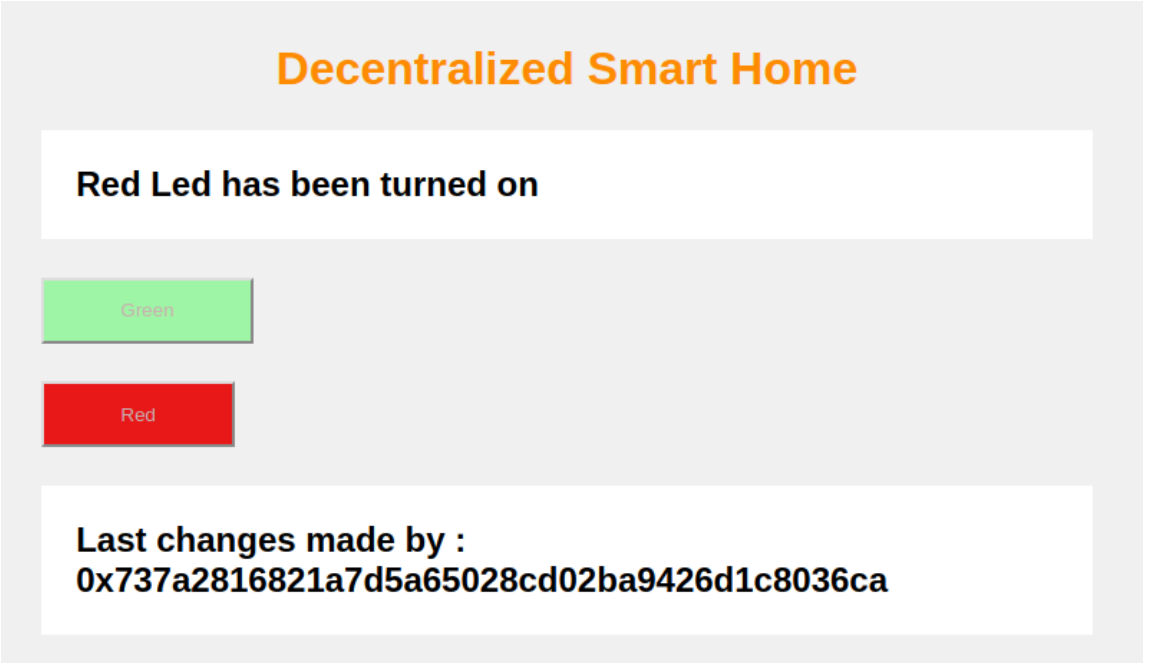


Fig. 3. User Interface

Results

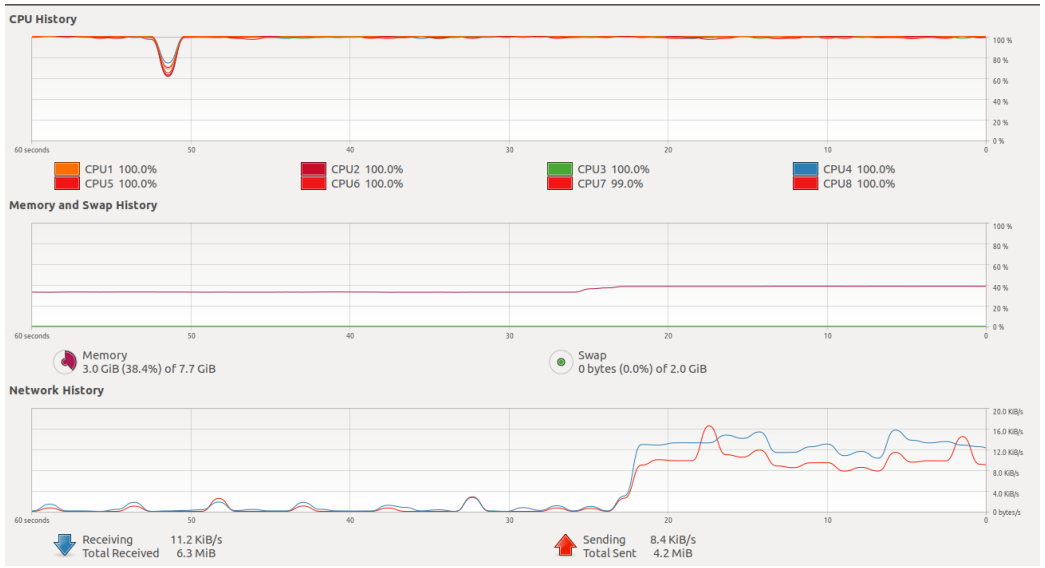


Fig. 4. Performance with PoW

Fig. 5. Performance with PoA

- We analyze the performance by evaluating the CPU utilization as the parameter
- Executed a set of 10,000 tx's for obtaining the plots.

Discussion

From the results, we can observe that

- The CPU utilization when using PoA as the consensus mechanism is far more lower in compare when the PoW mechanism is used.
- It shows that the PoA as a blockchain consensus mechanism can be one of the potential and lightweight solutions for IoT use cases such as smart homes.

Conclusion

- Our work presented a framework and a prototype implementation of a blockchain based approach for managing smart home appliances.
- Proposed system provides better, reliable and secure services to the residents.
- It also preserve the privacy of the user data, as it is not sent outside the home.
- The use of PoA over PoW not only increased the throughput but is also less expensive.
- The evaluation of the result demonstrates the feasibility of the system.

References

1. Connect All IP-Based Smart Objects (CALIPSO) FP7 EU Project. http://www.ictcalipso.eu/. Accessed 05 Mar 2019
2. Botta, A., De Donato, W., Persico, V., Pescap´e, A.: On the integration of cloud computing and internet of things. In: 2014 International Conference on Future Internet of Things and Cloud, pp. 23–30. IEEE (2014)
3. Cirani, S., Picone, M., Gonizzi, P., Veltri, L., Ferrari, G.: IoT-OAS: an Oauthbased authorization service architecture for secure services in IoT scenarios. IEEE Sens. J. **15**(2), 1224–1234 (2015)
4. De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V.: PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain (2018)
5. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized blockchain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 173–178. ACM (2017)
6. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerComWorkshops), pp. 618–623. IEEE (2017)
7. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
8. Mosenia, A., Jha, N.K.: A comprehensive study of security of internet-of-things. IEEE Trans. Emerg. Top. Comput. **5**(4), 586–602 (2017)
9. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
10. Notra, S., Siddiqi, M., Gharakheili, H.H., Sivaraman, V., Boreli, R.: An experimental study of security and privacy risks with emerging household appliances. In: 2014 IEEE Conference on Communications and Network Security, pp. 79–84. IEEE (2014)
11. Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A.: Fairaccess: a new blockchainbased access control framework for the internet of things. Secur. Commun. Netw.**9**(18), 5943–5964 (2016)
12. Pan, J., Wang, J., Hester, A., AlQerm, I., Liu, Y., Zhao, Y.: EdgeChain: an edge-IoT framework and prototype based on blockchain and smart contracts. IEEE Internet Things J. (2018)
13. Sivaraman, V., Chan, D., Earl, D., Boreli, R.: Smart-phones attacking smarthomes.In: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp. 195–200. ACM (2016)
14. Stojkoska, B.L.R., Trivodaliev, K.V.: A review of internet of things for smart home: challenges and solutions. J. Clean. Prod. **140**, 1454–1464 (2017)
15. Szabo, N.: Formalizing and securing relationships on public networks. First Monday **2**(9) (1997)
16. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. **151**, 1–32 (2014)
17. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., Wan, J.: Smart contract-based access control for the internet of things. IEEE Internet Things J. (2018)