BLOCKCHAIN FOR IMPROVED SAFETY OF SMART BUILDINGS

Salam Abdallah, Nishara Nizamuddin and Ashraf Khalil

*Abu Dhabi University
United Arab Emirates*

ABSTRACT

In this paper, we propose a blockchain powered automated self-incited fire detection sensors connected to smart buildings. This solution is based on utilizing Ethereum smart contracts to coordinate and monitor the interaction between the service providers, smart connected devices, and the end users. The smart contracts monitor the status of the fire detecting sensors; interact with a service provider according to pre-negotiated contract terms and conditions, and carries out the maintenance task in an automated fashion. When a failure occurs within the device, an internal sensor which indicates the failure generates a request for service on the blockchain. This transaction informs the service provider about the nature of the failure, identifying the specific device. The service provider can respond to the service request in a timely manner. Upon completion, the sensor reading indicates the completion of the maintenance/repair work carried out and can release payment to the service provider on the blockchain. Moreover, the proposed solution automates the payment process between the client and the service provider.

KEYWORDS

Smart Buildings, Fire Detecting Sensors, Blockchain, Ethereum, Smart Contracts

1. INTRODUCTION

The rapidly evolving internet technology and interrelated computing devices and the Internet of Things (IoT) have led to the integration of millions of sensors and smart devices that can interact with one another without any human guidance or intervention (Alaba et al, 2017) (Atzori, Iera, and Morabito, 2010). The need for a large scale deployment of IoT devices and sensors is ever growing and has gained wide acknowledgement and prevalence. The innovation in the IoT technology and cloud computing has paved a way to the perpetual global connection of devices, people, services and sensors. The term “things” in the IoT comprises of physical devices such as sensors that monitor and collect a huge amount of data about machines and day to day activities of human life (Yan et al, 2014). In the era of information technology, smart homes once a myth has now become a reality where any device in one’s home that uses electricity can be put on the home network and at the user’s command. Whether that command is given by voice, remote control, tablet or smartphone, the home reacts and responds (Aldrich, 2003). Most smart home applications relate to lighting, home security, home theatre and entertainment, and thermostat regulation (Aldrich, 2003) (Ding et al, 2011).

One of the most crucial and lifesaving sensors that are employed in modern day buildings are fire detection sensors. However, these sensors fitted in the smart homes come with a life time of 10-15 years, which doesn’t guarantee resistance to malfunction in due course of time (Home-security-systems, 2019). Many modern day smoke detectors will signal the “end-of-life” warning with a beep sound when their lifetime comes to an end. Despite the widespread use of fire detectors in both residential and industrial environments, the fire still claims many lives, causes grievous injuries and leads to huge financial loss. In the USA, over 362,000 residential fires were reported, leading to 2,500 deaths, 13,200 injuries and a loss valued at \$6.65 billion in the year 2010. As shown in Figure 1, in Europe, some 20,000-25,000 deaths occur due to fire each year (Bogue, 2013). Figure 1 shows the pictorial representation of the analysis of the death dataset taken from (U.S. Fire Administration, 2017). Some of the most common causes of fire detection system failures are identified as high ceilings, dirty smoke detectors, and wrong detection type. Poor maintenance, negligence or unidentified malfunction leads to fatal outcomes and claims human lives. Figure 2 shows the overall non-residential building fire, injuries, fatalities, and losses due to fire during the year 2006-2015 based on National Fire Protection Association, National Fire Incident Reporting System, and consumer price index in the US.

Figure 1. Fire deaths per million people

Year	Fires (in thousands)	Fire Deaths	Fire Injuries	Fire Dollar Loss Adjusted to 2015 Dollars (in \$ millions)
2006	98.9	75	1,350	\$2,756.6
2007	103.0	90	1,275	\$3,278.1
2008	97.1	100	1,250	\$3,800.4
2009	89.2	90	1,500	\$3,048.6
2010	84.9	80	1,375	\$2,609.5
2011	85.4	80	1,100	\$2,566.5
2012	92.8	65	1,450	\$2,550.9
2013	93.7	65	1,425	\$2,504.3
2014	99.5	60	1,200	\$2,579.1
2015	104.6	70	1,325	\$2,691.1

Figure 2. Non-residential building fire & losses
(U.S. Fire Administration, 2017)

1.1 Problem Statement

There is a considerable amount of time spent in identifying, reporting and maintaining faulty fire detection sensors. The conventional approach used is reliable but is tedious. Figure 3 shows the conventional approach of maintenance and repair of fire detection sensors in the smart buildings. The service provider sends its representative to address the reported issue by the sensors attached to the smart buildings.

Figure 3. Classical model for security maintenance of buildings

In large scale deployments of thousands of smart devices, maintenance and repair is still predominantly a manual process. Service requests from clients and payments are handled by administrators (from the service provider) who manage their maintenance, monitoring, and repair. The process is slow and time-consuming. Both the parties heavily rely upon the maintenance reports withheld by the respective parties. There arises a need for a robust solution that manages the maintenances and repairs of smart sensors in a much faster and dependable manner.

Since its initiation in 2008, blockchain continues to be one of the augmenting technological concepts following the success of Bitcoin, a cryptocurrency system based on decentralized infrastructure (Nakamoto, 2008). Blockchain implements a distributed ledger which is shared among all the authenticated participants in the network based on consensus property. The presence for a third party authenticator is phased out, making the system secure and decentralized. The transactions are digitally verified by all the miner nodes, validated and is finally logged in the blockchain. This growing list of records is linked using cryptography is completely decentralized, time-stamped and tamper proof ledgers (Nakamoto, 2008). Blockchain technology has gained importance and has been utilized in several industries such as healthcare, energy sector, and supply chain. Ethereum is a public, blockchain-based, open source, a platform featuring smart contract functionality. It uses

Ether as currency to carry out payments on Ethereum blockchain. Smart contracts are self-executing shared ledgers that use blockchain as the underlying technology to verify the prosecution of predefined terms. A smart contract not only defines the rules and penalties related to an agreement in the same way that a traditional contract does, but it can also automatically enforce those obligations. This is carried out by taking information as input, assigning values to that input through a set of rules in the smart contract and executes the actions. For example, determining whether an asset should go to one entity in the network or should be returned to other entity from which the asset originated (Christidis and Devetsikiotis, 2016) (Luu et al, 2016). Smart City initiatives by both government and private sector businesses to invest in information and communication technologies to find sustainable solutions to the growing issues has been an important factor in the effective management of smart cities. The Internet of Things (IoT) couldn't exist without smart sensors, and the growing use of smart technology is already transforming how manufacturers implement the IoT. Smart sensors are also bringing more connectivity and analytics to the development of smart cities and are the indispensable enablers of the IoT and the industrial IoT (Zanella et al, 2014). Smart sensors are particularly in residential apartments and warehouses because they can keep track of heat, temperature, and humidity, log data for historical records and quality management or be used as triggers for alarms or process management (Hancke et al, 2013) (Su et al, 2011). As the sensor networks have been playing a crucial role in setting up the smart cities, smart sensors compound to be crucial elements in the information technology world.

2. PROPOSED BLOCKCHAIN BASED SOLUTION

Motivated by the importance of having a practical and robust maintenance service of smart sensors and the implementation of blockchain in various fields, we propose a blockchain powered solution combined with sensing-as-a-service model in the safety of smart buildings maintenance and management. Figure 4 shows the proposed blockchain based solution for improving the safety of smart cities. There are 2 smart contracts namely- fire sensor smart contract and service provider smart contract. As shown in figure 4, in case of sensor failure, the smart contract dedicated to fire sensor is logged with a fire sensor failure transaction, which in turn raises a service request on the service provider smart contract. The service provider opens/raises a ticket for the issue. The service providers' representative is contacted who then repairs and fixes the issue raised. The fire sensor contract then propagates the message to complete the payment for the service provider following which the payment settlement is completed in an automated fashion. The union of smart sensors technology and blockchain can manage the log data effectively, improve the service provided with the help of a shared distributed database. Smart contracts can be utilized to automate the tasks that benefit the smart building maintenance in terms of safety. The automation afforded by the blockchain and smart contracts can regulate and automate the communication between multiple stakeholders, eliminate the need for a trusted third party (i.e. administrators from service provider's side) and prevent the occurrence of delay to service a malfunctioned/ defective fire detecting sensor in a building. Upon raising the service request, the smart contract executed will guarantee the enforcement of predefined rules such that all the authorized stakeholders can check the outcome of a transaction.

Blockchains are built for transaction consistency in a data store, allowing for auditability, atomicity, linearizability, durability, and data integrity (Nakamoto, 2008). They serve a similar purpose to distributed databases using data models and transaction mechanisms, where different replicas can be hosted by mutually cynical organizations. The models continually check each other's integrity and use a consensus protocol to agree on the transactions that should be executed. Blockchains use cryptographic auditing that relies on Merkle trees. Though blockchain has gained importance across many industries, there are several research issues still to be addressed before implementing a completely decentralized application such as Security flaws, Transaction costs, network speed, scalability, sustainability setting regulations and standards and a full swing adoption of this technology is still under research.

Figure 4. Blockchain-powered smart building security against fire sensor failures

3. FUTURE RESEARCH PLANNED

As a part of future research towards a blockchain-powered smart building security management, we are currently working on this project to contribute the following:

- To build the device self-service prototype using the Ethereum platform and smart contracts written in Solidity programming language on Remix IDE.
- To present a system that monitors safety by utilising the data and sensors' events in the smart buildings which help in detecting any sensor malfunction or repair and log events through smart contract.
- To offer a novel design that eliminates the need for a trusted third party (administrators in this case) between the service provider and the client.
- To carry out security vulnerability analysis of the smart contract code.

4. CONCLUSION

To date, the safety measures and maintenance of fire detecting sensors in smart buildings have been time consuming where the outcome of maintenance is manually administered or verified. In the near future, it is conceptualized that consumers and service providers will not settle for less than a tamper proof, secure and decentralized system especially when it comes to critical building services such as maintenance of fire detection sensors. Blockchain technology affirms and regulates safe and secure transactions. In this paper, we have proposed a model for improved safety of smart building maintenance by deploying smart contracts. Further, efforts and innovation are required by the research fraternity to design and build precise architecture, open source frameworks, and packages to execute critical sensor data-based services using blockchain platforms.

REFERENCES

- Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88, 10-28.
- Aldrich, F. K. (2003). Smart homes: past, present and future. In *Inside the smart home* (pp. 17-39). Springer, London.
- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.
- Bogue, R. (2013). Sensors for fire detection. *Sensor Review*, 33(2), 99-103.
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, 4, 2292-2303.
- Ding, D., Cooper, R. A., Pasquina, P. F., & Fici-Pasquina, L. (2011). Sensor technology for smart homes. *Maturitas*, 69(2), 131-136.
- Hancke, G., Silva, B., & Hancke Jr, G. (2013). The role of advanced sensing in smart cities. *Sensors*, 13(1), 393-425.
- Home-security-systems. Smoke Detector Problems and How to Solve Them. [Online] Available: <https://www.home-security-systems-answers.com/smoke-detector-problems.html>, Accessed 01 April 2019.
- Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 254-269). ACM.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Su, K., Li, J., & Fu, H. (2011, September). Smart city and the applications. In *2011 international conference on electronics, communications and control (ICECC)* (pp. 1028-1031). IEEE.
- U.S. Fire Administration. Available online: <https://www.usfa.fema.gov/data/statistics/>. Accessed on 01 April 2019.
- Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of network and computer applications*, 42, 120-134.
- Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1), 22-32.