**Smart Parking**

By

H.A.C.D.Dayawansha- 218018282

Premtej Rajayya- 217346677

Gourav Sharma- 217486898

Supervisor : Mr. Arkady Zaslavsky

**Abstract**

The Internet of Things (IoT) refers to the interconnection of smart devices to collect data and make intelligent decisions. However, a lack of intrinsic security measures makes IoT vulnerable to privacy and security threats. With its “security by design,” Blockchain can help in addressing major security requirements in IoT (Giovanni, M.et al., 2018). Blockchain capabilities like transparency, immutability, data encryption , auditability and operational resilience can help solve most architectural shortcomings of IoT. This article proposes a smart car parking system with IOT, Coass and blockchain technology.

**Introduction**

Parking and traffic congestion are constant sources of frustration for drivers in most cities around the world, therefore, they are hungry for innovative solutions that will fix their day-to-day problems. Now smart parking seems to be a dream come true—with smart IoT devices, Coaas and blockchain technology, one can build a smart and connected parking system. Cruising for vacant and economical parking places causes time-consuming and frustrating driving experiences. Further it will causes the fuel waste and air pollution. Public parking places in crowded cities are scarce and expensive. On the contrary, private parking places usually have low utilization rates, and the place suppliers are willing to provide their extra parking resources due to a maintenance cost by charging parking fees. As this situation, it is more important to call for a smart parking system that collects and provides private parking to ease public parking concerns. However, when the drivers are searching for parking places, their privacy (e.g., location, identity) is inevitable to be disclosed and existing parking schemes cannot achieve anonymous authentication and anonymous payment simultaneously. All of this will be possible because of the Coaas and blockchain technology and today it is as a distributed ledger for crypto-currencies, most notably bitcoin. It can also be used to create a permanent, public, transparent ledger system for compiling data on sales, tracking digital use and payments.

**Key related work**

The blockchain is an undeniably ingenious invention. It originally was devised for digital currency such as Bitcoin, and now the tech community has found other potential uses for the technology. For example, some people have used it to create smart parking solutions, and the mobile app called Parksen and it is a well-known blockchain solution. According to the founder of Parksen, the platform will make money based on a kickback fee every time a parking session is started from the platform. It will be free-to-use for cities and commercial parking providers and this will help them save a lot of costs for development, hardware and maintenance costs. As a result, the solution is not just beneficial toward the drivers; it is good for public officials too.

**AIM OF THE PROJECT**

The aim of this report is to propose a pragmatic framework known as CoaaS(Context-as-a-service) on the Internet of Things ecosystem for smart car parking. The CoaaS is an innovative idea that can collect and query information about the individual and environment in real-time. This concept is known as Mobile Crowd Sensing(MCS) which helps to collect the data via the sensors connected to their devices. As the users start to get the real-time information of the available car parking spots then they will be willing to pay for parking by using their smart devices such as mobile phones, tablets and laptops. Security and privacy in the Internet of Things is the major challenge because of the IoT networks are distributed. In order to provide secure communication and transactions between the smart device, the blockchain technology provides a security framework. Blockchain provides decentralized security and privacy approach. So, this paper will present the Context-as-service for smart car park using IoT with blockchain based security.

**RESEARCH PROBLEMS AND QUESTIONARIES FOR IMPLEMENTING BLOCK CHAIN AND COOAS FOR IOT**

In The above mentioned Smart parking system, our Idea to betterment the system with the Blockchain Technology and CooaS to IoT has also concerns and unanswered question that we will witness alongside of the benefits, here are some of our issues that we have be considering

\* While using the IoT as a medium to provide interaction between the service provider and the service receiver, the issues such as scalability of the system. It will be beneficial if the system is small but as the network grows, the cost of managing the network along with the architecture and engineering will raise which will affect the security of the system

\* When considering security, it is believed that with the increase in usage of IoT devices that will provide enormous amount of data from Integrated devices, main frame system and other platforms, it is utmost importance that we maintain fair means of terms with the data providers to ensure that there is no data leakage and exposure of the data and at the same time it is expected that transmission and exchange of data should be delivered to the right person on time with no delays.

\* Also considering that the whole system is cloud based service, It is essential to be a step ahead to and analyse how big is the data and how are we going to store it and in what means it can further used to make it more meaningful and also how quick we scalable we are with the storage,

\* Also considering pro and cons about the CooaS technology, more research is needed as the technology is new and more information is required to implement this in our Smart Parking System.

\* What resources are provided by the services providers that we can quickly refine and use in the applications in short period of time?

\* Also talking about the time, to which extent can we produce this prototype application and workings would satisfy the needs with such short resources available in very short time.

These are some of the questions that we have come across the project but we believe that there are going to be more once we go in depth into its workings.

**THE RESEARCH METHODOLOGY**

The plethora of researches have been done on Context-awareness in the IoT. Using IoT, all the objects connected to the internet around the world can communicate with each other with minimum human involvement (Hauswirth, M. et al., 2009). Many applications are enabled by IoT in heaps of domains. These domains are categorized into three different types which are society, Industry and environment (Sundmaeker, H., Guillemin, P. & Friess, P., 2010). In addition to this, the large number of devices are connected to each other via the internet and they share vast amount of confidential data as well as privacy-sensitive information, so the chances are very high of getting the cyber-attacks. S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini,2015. In order to prevent from these cyber attacks, the blockchain is also involved and researched on.

**THE PROJECT TIMELINE WITH KEY MILESTONE DATES AND DELIVERABLES**

\* Project architecture design on 29/03/2019

\* Application overview and design on 05/04/2019

\* Sprint 1 implementation on 10/04/2019

\* Test Run on 10/04/2019

\* Sprint 2 and modification on 24/04/2019

\* Full operational test on 05/05/2019

\* Final output presentation on 10/05/2019

\* Releasing the application for Market 25/05/2019

**REFERENCES**

Hauswirth, M. et al., 2009, ‘Rapid Prototyping of Semantic Mash-Ups through Semantic Web Pipes’. Proceedings of the 18th International Conference on World Wide Web, Madrid, pp.581–590.

Sundmaeker, H., Guillemin, P. & Friess, P., 2010. ‘Vision and challenges for realising the Internet of Things’.

S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini, 2015."Security privacy and trust in internet of things: The road ahead", Computer Networks, vol. 76, pp. 146-164.

Giovanni, M. et al., 2018, ‘Blockchain and IoT Integration’.