International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 21 (2015) pp 41757-41760

Situation-aware money for IoT payment using Bitcoin

Al shaima Mohammed, Taek Lee, Jonguk Jung, Hoh Peter In

Department of Computer Science Korea University, Seoul, Korea
alshaima@korea.ac.kr, comtaek@korea.ac.kr, sique@korea.ac.kr, hoh_in@korea.ac.kr

Abstract
IoT connect different types of electronic devices together for a great experience in the day-to day activities. Electronic devices are embedded with paid services and situation-aware system. Users need to pay products or services in the advent of IoT paid services. Bitcoin is a promising candidate for IoT payment. However Bitcoin cannot recognize changes in different situations. In this paper, we proposed a situation-aware money. Situation-aware functionalities were added to make the money smart enough to handle payment that change dynamically.

Keywords: IoT, situation awareness, Bitcoin, transaction

1. Introduction

IoT payment is presenting a new era of relation between suppliers and customers. Turning physical objects into smart objects by embedded payment on them and responding to consumers without user intervention and using card/cash, it will empower and enhance user experience in payment process. Users need money to use IoT services. Enormous amount of devices request transaction at scale is high. Micro transaction (small scale of transaction) will happen because fee is getting low. Therefore current payment methods cannot handle small transaction.

Bitcoin is a promising candidate to pay for IoT payed services. Bitcoin can handle micro transaction and several transaction in different places in same time. Massive number of transactions can happen smoothly without interrupt. Bitcoin uses P2P network which make Bitcoin safe and reliable. However Bitcoin is not enough to support situation-aware environment. The raw payment background of Bitcoin make it hard to predicate or adopt situations that change dynamically. As a result, there is a need for situation-aware money.

Situation-aware money is type of money that exist for transaction between objects or things. Moreover situation-aware money is smart enough to handle payment that change dynamically and can take actions according to those changes. Several functionalities of situation-awareness system had been added to the transaction to be aware of actions and respond. We estimate transactions will become complex and huge because number of devices and users keep increasing. Users will request many transactions in the same time from different devices, therefore users need reliable and fast payment technology. Situation-aware money will be aware of each transaction and each service will have different fee. Thus fee charge have to be flexible according to time, place and who is using it.

In this paper, our goal is situation-aware money which can handle different service situations. We adopt the Bitcoin technology as crypto currency and a situation-aware money model. We present a situation-aware description language to flexibly deal with the currency depending on different service situations (e.g., who, when, or where did users ask a service?)

2. Related Work

2.1 Payment in IoT

Few if not many of IoT payment exist. Payment-tracking system would tailor payments through a usage-based model [1]. For example, service providers such as gyms could charge fees based on how much a customer uses specific machine. Automate the process of in-store payments [1]. For instance, through chips embedded in wearables, stores could access certain shopper information upon a consumer's entrance into their shop. Those existing approaches have their flaws in some ways. They can collect information about consumer profiles and behavior. During payment process third party will be used such as credit card. Many research papers propose solutions models for authentication and security on IoT environment. [2] Presents a novel mutual identity authentication scheme which can be applied securely in Internet of Things. They propose an asymmetric mutual authentication scheme between the platform and the terminal node, which imposes light computation and communication cost.

2.2 Bitcoin

Bitcoin is peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution [3]. Bitcoin have many elements such as bitcoin address, bitcoin PKI and ledger. Bitcoin address is pair of keys public and private keys which verify the ownership of the address. Ledger is shared by all the users where transactions are recorded. Bitcoin PKI is a promising technology that we use to achieve our goal which is Authentication. For example Alice want to send Jack Bitcoin, Alice will take the previous transaction, and Jack public key, and sign those two together with her private key. Meanwhile in the Bitcoin network other users can verify that Alice send the coins and which public key has received the coins. [4] focused on security aspects, two-way Near Field Communication (NFC), and reducing the number of Bitcoin transaction by introducing a clearing center for fast and Reliable Mobile Bitcoin Payment System(MBPS)

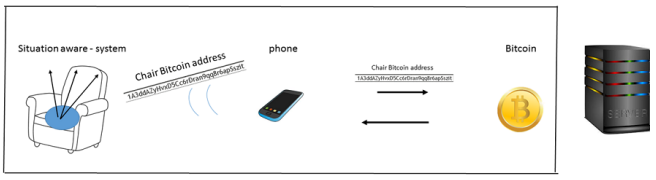

Figure 1. Payment system based on Bitcoin (an example of paid service of using a chair)

2.3 Situation- awareness

Situation-awareness means that different applications use different situation changes to trigger different application actions. "Situation is a set of past context attributes and/or action of individual devices which is relevant to determine future device actions" [5]. Situation- aware system adopts to its environment and react to evets which will result actions. It helps user to be aware of his current situation without need to interrupt. Many paper exist that focused on the architecture of situation-awareness. [6] Proposes a situation-awareness based self-adaptive system architecture (SASA) to support more efficient adaptation and, hence, achieve more accurate and successful missions, even in dynamic execution environments. They implemented a case study for air defense systems (ADS) using tests in a HLA/TRI-based real-time distributed simulation environment. In our paper, we adopted some of situation-awareness properties such as time awareness. Things or objects can measure time and react by issuing signals or actions. Another property is ability of sensing surrounding environment by connecting to user device or sensing user while using thing or object.

3. Our proposed situation-aware model and system

In this section, we explain our proposed payment system and situation-awareness model. We give overview picture of the proposed payment model and go in details to explain the model and system themselves.

3.1 Payment system design based on Bitcoin

As shown in (Figure 1), we designed a Bitcoin-based payment system for IoT environment (e.g., using a chair in charge). The system works with objects that provide paid services. The main purpose of this model is to ease transactions between objects and achieve secure and flexible payment in real time. The system includes things or objects, user devices, Bitcoin and a server. Things or objects provide paid services. User device (i.e., a phone in Figure 1) plays a role of a middleman between a thing and Bitcoin network. Crypto currency represented by Bitcoin works as end point payment. Server stores for example receipt information of transactions for future reference.

3.2 Situation-aware transaction model

(Figure 2) represents our proposed situation-aware transaction model. The model was designed to support a situation-aware transaction service over Bitcoin. We assumed that payment policies need to be changed depending on situation events: what service will be consumed by a user, when the user tries to use the service, where the user uses the service, who tries to use the service, and how the user used the service. Then, the payment system need to take an action on a certain condition of situation events. We call this is situation-aware rule and the rule is described with situation-aware modeling language that will be presented in Section 3.3. System actions include for example "charge fee", "block services", and "give warning". As a result, system actions generate output signals that are interpreted by the payment system and they trigger some necessary function. For example requesting a query for Bitcoin payment or issuing receipt information into a repository server (e.g., transaction success, fail, or shutdown).

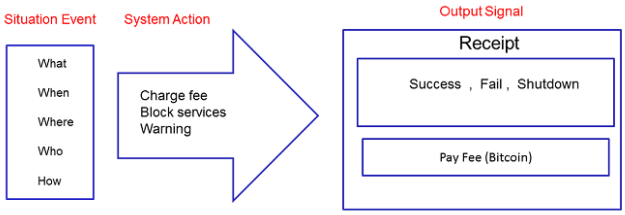

Figure 2. The concept of our proposed situation-awareness model

3.3 Situation-Awareness modeling language

In this section, we present a situation-awareness modeling language that is a tool being able to describe users' situation and their service usage scenarios supporting the model concept introduced in (Figure 2). The transaction model will take actions in respond to condition, system action and output signal. Set of conditions need to be satisfied starting with 5W1H situation events. The focus will be more on who and when using the system and according to that we charged for services. Moreover the system itself will have the ability to process actions in respond to users' actions such as warning or charge more. In (Figure 3), we specify how a thing or object should take action. We included set of conditions and when these conditions satisfy. As a result the system will take action and produce signal of success or fail.

TakeAction= (**Condition**, **SystemAction**, **OutputSignal**)
Condition = BooleanExpression
BooleanExpression= {x | □x is a combination using elements of **LogicalOperator**, **SituationEvent**, and **OutputSignal** □}
LogicalOperator= {AND, OR, NOT,→ }
SituationEvent= (Who, How, What, When, Where)
SystemAction= {Warning, Charge, ChargeMore, BlockService, Display}
OutputSignal={success, fail, shutdown, receipt}

Figure 3. The proposed situation-awareness modeling language

In (Figure 3), the command **TakeAction** has a tuple form consisting of three elements; when **Condition** was satisfied, the system takes an action depicted in **SystemAction**, and then it generates **OutputSignal**. With **SituationEvent**, we listed conditions that need to be met in processing payment.

The element **OutputSignal** will be responsible of announcing the success or fail of the transaction. **SystemAction** line will tell if transaction works right or something interrupt process.
For example in a classroom, suppose a scenario that a professor uses a chair equipped with our situation-aware money model. The professor uses it during office time and chair is located in a seminar room. Here is the scenario description with our situation-aware modeling language. First action will be:
TakeAction1 includes who is using chair and how long have been used and when exactly and where. After proccing these information, the compile fee will be charged and signal of success will be announced. Second action is a result of the first action. After **TakeAction2** generates signal of success, it will connect to server and display the result and issue a receipt.
Another example in a classroom, suppose a scenario that a student uses a chair more than the fixed time. Then our model will issue warning message and stop services. The following actions includes student and overtime and warning that been issue by our system which result in blocking services. After that a signal will be generate which include shutdown and block services actions. This signal is a warning message student get when uses overtime.

TakeAction1= ((professor, UseOnTime.1 hour, Chair, OfficeTime, SeminarRoom), Charge3$, □ Success □)

TakeAction2= (TakeAction1.OutputSignal→□ success □, Display, Receipt)

TakeAction3= ((Student, useovertime.over30mins, Chair, OfficeTime, seminar), block services □ shutdown □)

TakeAction4= (TakeAction11.OutputSignal→□ shutdown □, block services)

4. Case Study

To show validity of our study, we implemented and evaluated a prototype realizing an application scenario – users' payment on a charge of using a chair. We tested our situation-aware payment system and created a situation where payment transaction will happen between chair and user. This case study is one from many cases and it's applicable to other devices.

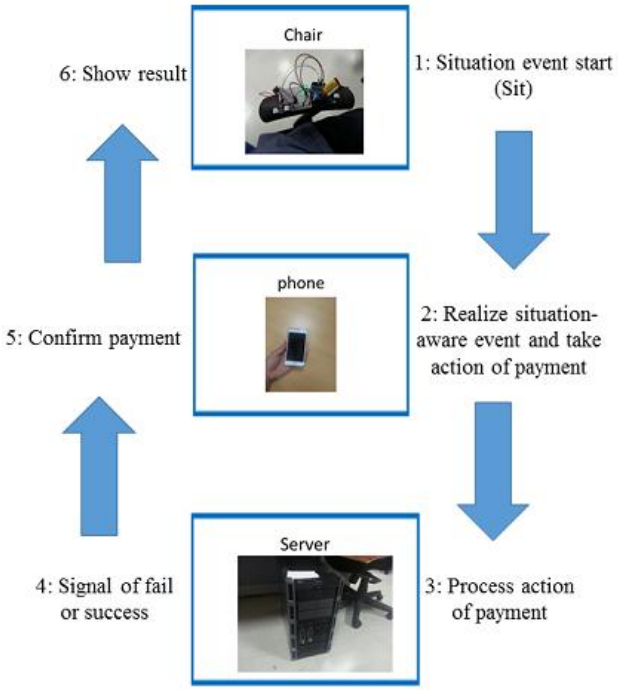

Figure 4. Flowchart describes our study case process

(Figure 4) Flowchart describes our study case process. Chair will be in red light mode and system not capable to identify any event or transaction. User will sit in chair while equipped with phone. As a result situation event will start. Phone will recognize situation-aware event and take action as request payment from server. Situation event decides amount of fee charged because it shows who and when using the system. Server will process action of payment send by phone. Server will issue signal such a fail, success and shutdown. Server sends payment result signal to phone. Phone will confirm payment and send confirmation to chair. Chair will show success or fail of payment by display green light. To implement our experiment, we used Arduino, Bluetooth module (or NFC module), distance sensor and Android.

5. Conclusion

In this paper, we presented a case study of a situation-aware money in IoT using Bitcoin. To implement the system, we proposed one enabling technology: situation-aware money. Situation-aware money is type of money that exist for transaction between objects or things. We present situation-aware model language for secure and flexible IoT payment services. Bitcoin will be used as crypto currency for payment. Our proposal is not limited to the chair-to-phone scenario (the case study in this paper) but applicable in many other IoT transaction scenarios. Our model is secure because it depends on Bitcoin PKI technology and also flexible depending on different payment situations.

Acknowledgment

This research was supported by the Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2012M3C4A7033345). This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2015-R0992-15-1011) supervised by the IITP(Institute for Information & communications Technology Promotion)." Email to Hoh P. In (hoh_in@korea.ac.kr), the corresponding author if there are any questions.

References

[1] Hailey Winston. http://www.yaleeconomicreview.org/archives/2204. 2014

[2] Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long, Ting Hu. "A Novel Mutual Authentication Scheme for Internet of Things." Proceedings of 2011 International Conference on Modelling, Identification and Control, Shanghai, China, June 26-29, 2011.

[3] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf

[4] Jeton Memeti. "Protocol Design and Implementation for a Fast and Reliable Mobile Bitcoin Payment System (MBPS) with two-way NFC". Thesis.University of Zurich. 2014

[5] Stephen S. Yau, Yu Wang, and Dazhi Huang, Hoh P. In. "Situation-Aware Contract Specification Language for Middleware for Ubiquitous Computing". Proceedings of the The Ninth IEEE Workshop on Future Trends of Distributed Computing Systems. May, 2003

[6] Sangsoo Kim, Jiyong Park, Hoh Peter In, Heeseo Chae. "Situation-Aware Based Self-adaptive Architecture for Mission Critical Systems". Proceedings of the 3rd international conference on Embedded Software and Systems. 2007