A Secure Shopping Experience Based on Blockchain and Beacon Technology

Remo Manuel Frey
ETH Zurich
Weinbergstrasse 56/58
8092 Zurich
+41 44 632 48 18
rfrey@ethz.ch

Denis Vučkovac
ETH Zurich
Weinbergstrasse 56/58
8092 Zurich
+41 44 632 89 15
vdenis@ethz.ch

Alexander Ilic
University of St. Gallen
Dufourstrasse 40a
9000 St. Gallen
+41 71 224 73 00
alexander.ilic@unisg.ch

ABSTRACT

The present work proposes a novel approach for a future shopping system. Customers' personal data are protected by a blockchain-based storage network. Based on the bitcoin protocol, the system transacts encrypted data in a tamper-proof way and is able to run secure multiparty computations while no one but the data owner has access to the input data. Thus, a potential customer is able to allow a company to apply functions like a recommendation algorithm without revealing personal data. In combination with a low-energy transmitter (beacon), a completely new shopping experience arises. The beacon automatically triggers a recommendation process based on encrypted personal data. The resulting outcome is a recommendation system, a self-checkout system, and a payment system all in one, thereby full anonymity is guaranteed and the customer never lose control on her data.

CCS Concepts

- **Information systems→Recommender systems**
- **Security and privacy→Privacy-preserving protocols**
- **Information systems→Electronic commerce**
- **Human-centered computing→Mobile phones**

Keywords

Privacy; Blockchain; Beacon; Shopping; m-Commerce;
Recommender System; Self-Checkout;

INTRODUCTION

In an early stage of the Internet, the online and offline world were strictly separated. People either shopped in a physical store or they ordered a desired product online on their personal computer at home. Soon, a hybrid form of shopping behavior evolved [3]. People search online for product information and go afterwards to the store. Another mixed strategy is to search online, check it out in-store, and then buy it online. Due to the massive proliferation of smartphones in the last decade, several approaches try to fuse offline and online shopping. People are invited use their device in the stores to get an enriched shopping experience. A well-known application is self-checkout by customers' own mobile devices [1]. First, the customers pick products from the shelf, scan their barcodes to add them into a virtual basket, and may read additional product information on the screen. Then, they may activate online coupons and pays the products directly on their devices. No cashier is needed anymore in the store. In the present work, we propose a similar process which uses blockchain [6, 7] and beacon technology [4]. In contrast to the described application, the privacy of the customers is cryptographically guaranteed.

1. BEACON

Beacons enables a wide range of new application in retail sector. These are tiny, low-cost Bluetooth low energy devices whose single function is to broadcast a universal unique identifier. If a mobile application ('app') on a smartphone receives the signal, it displays a push notification on the screen to trigger user's attention. For instance, store owners can place one or more devices in front of the store. Potential customers who pass by are invited to enter the store and/or to check special offers or new products directly on their mobile device. In another scenario, a group of beacons can be used for indoor localization. Using triangulation, an app is able to guide customers to the shelf containing the searched products. Apple's iBeacon protocol [4] is de facto standard.

2. CONSUMER PROFILES

Several marketing studies proved that personalized offers are more successful than non-personal ones and the satisfaction of the customers increases [5]. Companies gather customer data and create individual profiles. They use it to predict consumer needs and future consumptions, and to optimize recommender systems for products and services. Sensors from the 'Internet of Things' additionally support the data collecting by observing people's daily life. Sharing such personal data with a company might be a benefit for companies and customers as well. Unfortunately, customers have often strong privacy concerns related to collecting, storing, and applying personal data, especially in the online context. Awad and Krishnan [2] provide a broad overview of corresponding research questions in recent privacy literature. Companies use several well-established countermeasures which primarily aim to reduce customers' risk perception. For example, they provide transparent information how they deal with user data or they enable customers to remove personal data themselves. Transparency and customer empowerment are two effective instruments among many others. But, a practicable mechanism to cryptographically guarantee the anonymity of a customer and the protection and controllability of personal data is still lacking.

3. SOLUTION

A fairly new approach, called 'Enigma', is described by Zyskind, Nathan, and Pentland [6, 7]. It contains a peer-to-peer network to jointly share data. A blockchain controls the network and manage the access control. The clue is that one can run computations within the network while keeping data completely private ('secure multiparty computation'). The authors provide detailed information about the technical realization and possibilities for innovative future applications. To overcome the mentioned deficiencies concerning personal data, we propose to use Enigma for a novel shopping system. In doing so, the customer invokes a contract with a company and gives access to a part of her personal

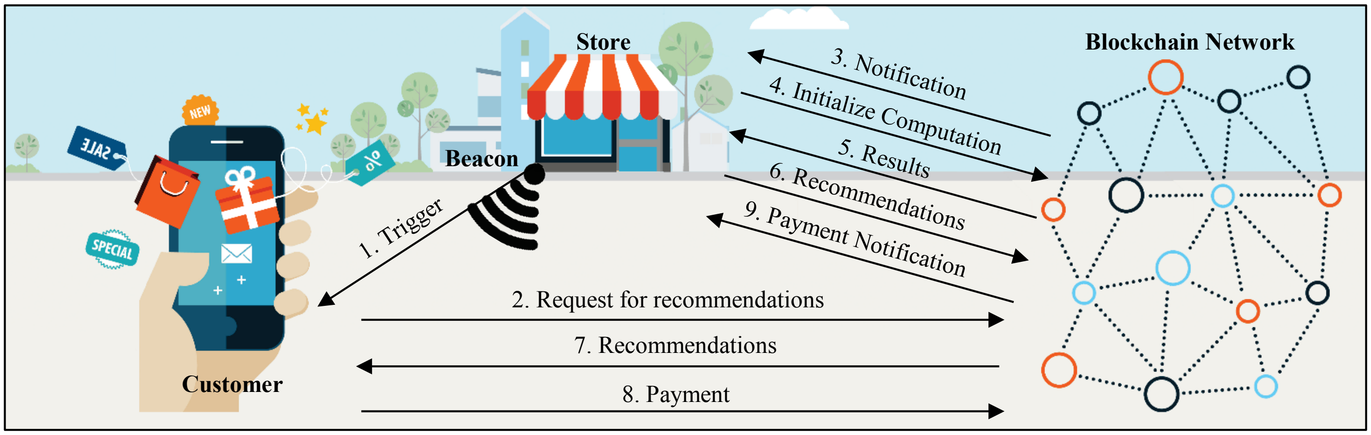

Figure 1: The interactions between customer, store, and blockchain network in the proposed shopping system.

data only for specific computation. The company has never access to customer's raw data directly. The computations a company is allowed to perform is regulated in a well-defined contract. For instance, an apparel company gets access for computing recommendations for clothes based on customer's body measurements. The company has never access to the measurements and the customer is even able to completely block other sensitive data like detailed textures resulted from a 3D body scan. All involved data are permanently encrypted. There is no need for a trusted-third party. In the next three subsections, we outline the process between a customer, a store, and a blockchain network like Enigma. An overview of the system is shown in Figure 1. In sum, it acts as a recommender, self-checkout and payment system.

3.1 Setup

First of all, the potential customer downloads and installs the company's app from a trusted app market platform like 'Google Play Store' or 'App Store'. On the app, she defines a contract about what kind of confidential data she is willing to share with the company and which kind of computations are allowed. It will be interesting to see how the companies align with the new situation in which they do not possess the user data anymore. Moreover, users could use of the data in, say, two shops to help make better recommendations in a third shop.

3.2 Recommender System

When she approaches the store, the Beacon sends a signal to her smartphone and triggers two actions (1). First, the app computes a new blockchain address for the upcoming transactions. Second, an encrypted message including the personal data and its permissions is automatically send into the blockchain network to company's address (2). The company gets a notification (3) and starts the recommendation algorithm (4). When the company receives the results (5), the recommendations are forwarded to user's address (6, 7). Finally, the app decrypts/visualize the recommendations.

3.3 Self-Checkout and Payment

The customer may decide to buy one of the recommended products. She selects the product on her smartphone and put it into a virtual shopping basket. Then she directly pays with a transaction into the blockchain network to the address of the company (8, 9). After completion, she may terminate all data access and computation permissions. During the whole process, the full anonymity for the customer is guaranteed and the company never received customer's personal data.

4. DISCUSSION AND FUTURE WORK

We outline an efficient and powerful solution in three core processes of current and future retail business: providing recommendations, self-checkout and mobile payment. Blockchain and beacon technology are merged together. The result is a smooth and secure shopping experience which fuses the advantages of online and offline worlds in retail. We plan to develop a prototype of the described solution with the aim to demonstrate the feasibility and reliability of the system. Analogue to Bitcoins, the technical feasibility is not sufficient to guarantee cryptographic secureness because an adequate number of users and network nodes are required as well. Therefore, user acceptance is crucial and we intend to evaluate consumer acceptance in terms of privacy concerns as a second step. We expect an increase of trust, better transparency, improved comfort, and support for the desire of controlling personal data. The system does not prevent companies to gather data without explicit user permission. But, we plan to extend our solution for a secure handover of such data to the customer. An additional payment option could then allow customers to sell their data and its usage.

5. REFERENCES

[1] Andriulo, S., Elia, V. and Gnoni, M.G. 2015. Mobile self-checkout systems in the FMCG retail sector: A comparison analysis. *International Journal of RF Technologies: Research and Applications*. 6, 4 (2015), 207–224.

[2] Awad, N.F. and Krishnan, M.S. 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*. 30, 1 (2006), 13–28.

[3] Farag, S., Schwanen, T., Dijst, M. and Faber, J. 2007. Shopping online and/or in-store? A structural equation model of the relationships between e-shopping and in-store shopping. *Transportation Research Part A: Policy and Practice*. 41, 2 (2007), 125–141.

[4] Newman, N. 2014. Apple iBeacon technology briefing. *Journal of Direct, Data and Digital Marketing Practice*. 15, 3 (2014), 222–225.

[5] Smutkupt, P., Krairit, D. and Esichaikul, V. 2010. Mobile Marketing : Implications for Marketing Strategies. *International Journal of Mobile Marketing*. 5, 2 (2010), 126–139.

[6] Zyskind, G., Nathan, O. and Pentland, A. 2015. Decentralizing privacy: Using blockchain to protect personal data. *Proceedings - 2015 IEEE Security and Privacy Workshops*. (2015), 180–184.

[7] Zyskind, G., Nathan, O. and Pentland, A. 2015. *Enigma: Decentralized Computation Platform with Guaranteed Privacy*. arXiv:1506.03471.