Chapter 33
Blockchain for Security of Cloud-Based Online Auction

Yun Shu
Auckland University of Technology, New Zealand

Jian Yu
Auckland University of Technology, New Zealand

Wei Qi Yan
Auckland University of Technology, New Zealand

ABSTRACT

Online auction is one of the most successful internet business models. However, auction fraud has become the highest threat and hazard to the future of this business model. The blockchain provides a new perspective to resolve this problem. It can be used for current financial services, certificates, remittances, and online payments; meanwhile it also provides several crucial services such as smart contract, smart property, trust system, and security services. This chapter discusses how to apply blockchain to a cloud-based online auction and the principle of operation. The purpose is to fundamentally solve the problem of online fraud caused by information asymmetry of electronic transactions. To the best of the authors' knowledge, this is the first time that the blockchain has been applied to authentication of online auction. The preliminary contribution is for preventing auction fraud from the aspects of smart properties and smart contract.

INTRODUCTION

As one of the most significant electronic markets, online auction transfers the collectables business and e-commercial business to a global billion-dollar market (Grazioli and Jarvenpaa, 2000; Peters, et al., 2015; Corcoran, 1999). With the idea of frictionless economy, online auction is considered to be rapid and efficient platform to eliminate geographic boundaries and establish the accurate price based on supply and demand (Ba, et al., 2003). Alibaba, Amazon, and E-Bay are the exemplar cases in this area.

DOI: 10.4018/978-1-7998-5351-0.ch033

These platforms offer low cost, excellent technical support, and massive data analysis so that traditional sales begin to transition to e-business model increasingly. The usage of online auction sites ranges from individuals to firms; however, the market fraud is rising. According to the Internet fraud operated by the National Consumers Union, online auctions were still the primary source of Internet fraud (Alanezi, 2016).

For this reason, a growing number of institutions, such as Alibaba, Samsung, Louis Vuitton, Internet Fraud Watch (www.fraud.org) and the Internet Fraud Complaint Center (www.ifccfbi.gov), are jointly developing new mechanism to combat this challenge (Chua and Wareham, 2004). Simultaneously, Alibaba and a myriad of financial institutions to propose a new solution - giant distributed database "block chain." The blockchain is secured by Byzantine fault tolerance (BFT). This database is used to maintain a continuous growth of blocks. As shown in Figure 1, the design of blockchain is to prevent data modification. Once the data are recorded, it cannot be altered reversely anymore.

In blockchain, each block consists of block hash link, timestamp, and valuable data as shown in Figure 2 The blocks can be transferred from one blockchain to another. This technology has approved that it can eliminate the double-spending problem (Pilkington, 2015).

Thus, it can be utilised to various scenarios, such as financial services and medical record (Peters and Panayi, 2016). The blockchain might become the most critical online promising technology for Internet interaction (Zheng, 2016). This database is more magic than we expected. It could be the final solution to online auction fraud.

Based on the distributed blockchain technology, we create a broad range of distributed applications. The revolutionary methodology in this area is the Etherum platform, which includes a complete programmable framework (English, 2016). This framework is utilised to implement smart contract. Moreover, the blockchain infrastructure facilitates virtual currency, such as Bitcoin, trust and contract applications. The most significant feature is that the linked data are decentralised so that we do not need to be dependent on central server anymore.

In this chapter, we will discuss the methodology that can prevent online fraud actively. The implementation of a blockchain can secure the currency transition of online action. We utilise the mechanism of smart contract and link data which ensures the security of online payment from end to end. Moreover, final transactions are permanently recorded in the database so that we are able to provide permanent records for all clients (Black, 2013). Finally, the Elliptic Curve Digital Signature Algorithm (ECDSA) is implemented in blockchains for offering trusted handshakes between blocks (Johnson, 2001).

The remaining parts of this chapter are organised as follows. In Section II, we will present the related work while the methodology will be introduced in Section III, the results database will be described in Section IV. The analysis and comparisons will be detailed in Section V, conclusion of this chapter will be stated in Section VI.

RELATED WORK

Type of the Online Fraud

The seriousness of auction fraud is actually far beyond our imagination. Victims do not actually have to participate in the Internet auction, but will suffer the consequences of fraud. The triangulation is used to implement an offline fraud via a merchant sells the product from the online auction (Chua and Wareham, 2004). For example, when a thief uses stolen money to buy valuable products and put them