2019 the 4th IEEE International Conference on Big Data Analytics

A Reliable E-commerce Business Model Using Blockchain Based Product Grading System

Ching-Nung Yang
Dept. of Computer Science & Information Engineering
National Dong Hwa University
Hualien, Taiwan
e-mail: cnyang@gms.ndhu.edu.tw

Yi-Cheng Chen, Shih-Yu Chen, Song-Yu Wu
Dept. of Computer Science & Information Engineering
National Dong Hwa University
Hualien, Taiwan
e-mail: 610721225@gms.ndhu.edu.tw

Abstract—**The first step in online shopping is, apparently, to choose a reliable supplier. However, consumers and merchants may have different perceptions of product quality, and this may result in business disputes. The dispute about buying inferior goods may be caused from simple product photos or merchants make over the top claims about their products. This dispute problem cannot be resolved completely, even though customers choose reputable e-commerce companies, e.g., Amazon.com and Alibaba.com. In the final analysis, the cause is that e-commerce companies do not adopt quality rating to evaluate products. If there is an alliance, among e-commerce companies and trusted organizations, which establishes credible product grading system (PGS), online shoppers may buy genuine product at a fair price from this e-commerce alliance. In this paper, we propose blockchain based PGS (BPGS) to deal with big data for this business model. The blockchain is a decentralized technology, and thus we can speed up the verification of product grading. In addition, for the proposed BPGS, 51% of attacks cannot be completed unless 51% of merchants and e-commerce companies in this alliance are simultaneously compromised. Therefore, our e-commerce environment based on BPGS is not only reliable but also secure.**

Keywords- e-commerce; product grading system; blockchain; smart contract

I. INTRODUCTION

In 2017, an estimated 1.66 billion people worldwide purchase goods online, from online retailing corporations such as, Amazon.com, Alibaba.co, and JD.com. During the same year, global e-commerce sales amounted to 2.3 trillion U.S. dollars. Recently, more and more customers are fascinated with online shopping activities, e.g., the very famous "Double 11" shopping carnival. The Double 11 is originated from "Taobao Mall Promotion Day" held by the Chinese e-commerce company Alibaba on November 11, 2009, and it is a day when Chinese people go on massive Internet shopping carnival because many online stores offer huge discounts on this day. Now, Double 11 has evolved into an annual shopping spree, and affects the global retail industry.

The above implies that e-commerce is very important for our daily life. There are many online shoppers now shopping via their smartphone weekly, and this already becomes their main shopping way. Obviously, the first step in online shopping is to choose a reliable supplier, such that we can buy genuine products at a reasonable price. This is why many online shoppers get inspiration for purchasing from social networks. Via social circle, they try to insure the product quality and hope that the product is worth the price they paid. It seems that we are now entering the era of social shopping. However, there are many online shopping scams via social network, e.g., scammers pretend to be legitimate online sellers, either with a fake social account (Facebook, Line, or Wechat). Even though online shoppers choose reputable e-commerce companies, this dispute problem cannot be resolved completely. Because consumers and suppliers may have different perceptions of product quality.

To completely, solve this problem, in this paper, we form an alliance including e-commerce companies and trusted organizations to establish a credible product grading system (PGS). Based on the PGS, customers may buy products with high grades to insure product quality. To efficiently and securely to deal with such big data for product grading, we adopt a decentralized blockchain technology [1]. The structure of this paper is as follows. Section 2 discusses background information about blockchain and smart contract. Analysis of current situation and motivation are described in Section 3. Section 4 describes how Ethereum smart contracts were designed to implement the proposed BPGS, on which a more reliable and secure e-commerce business model is achieved. Conclusion is drawn in Section 5.

II. BACKGROUND

A. Blockchain Technology

The basic concept of blockchain was proposed by Nakamoto Satoshi [1]. Blockchain is a decentralized database using cryptographic technology to generate associated blocks, where each block records full transactions over a period of time. Each node contains a complete historical block, and even if one node is modified, it will not affect the verification of entire blockchain. The blockchain information is public, and anyone can search the chain for historical trading information. Blockchains require miners, when any node in blockchain generates a transaction, the transaction is broadcast to each miner, and all miners may verify the transaction through the proof of work mechanism [2]. Blockchain has the following main features: (i) the ability of anti-modification (ii) the ability of tolerance

978-1-7281-1282-4/19/$31.00 ©2019 IEEE

as some nodes are faulty (iii) the ability of reaching collaborative trust among nodes in this distributed peer-to-peer system without the third-party certification agency (iv) the ability of accessing information of blockchain at any node in this network.

A blockchain consists of continuous blocks, each block records and stores serial transections as a Merkle root by using Merkle tree algorithm in a period of time, and every block after the first block (called genesis block) has a cryptographic hash value of previous block (called parent block). All these hashed values are assembled into a chain, as shown in Fig. 1.

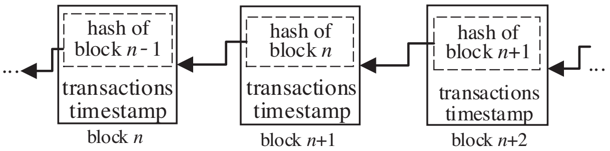


Figure 1. Construction of blockchain.

On the other hand, the private blockchain [3] has no mining mechanism and miner's role, because the private chain is usually used as a network within company, organization and members. For example, IBM blockchain platform provides a private chain for more than 400 cooperatives, Walmart offers solutions that provide traceability of food tracking through blockchains to make food supply chain safety, and Maersk builds a global platform to achieve efficient transportation. In fact, the blockchain is widely used in various intended applications, e.g., in Internet of Things [4-7], or use for small mobile payments [8], cloud computing [9], digital certificate [10, 11] and other application scenarios.

B. *Ethereum and Smart Contract*

The Ethereum virtual machine (EVM) is designed based on a peer-to-peer network protocol. Anyone can participate in the network and play the role of a verifier, i.e., a miner, which is a basic element in EVM. This virtual machine is an environment that runs smart contracts, which the term *smart contract* was first introduced by Szabo in 1994, where the smart contract is defined as "*a computerized transaction protocol that executes the terms of a contract*" [12]. Precisely, smart contracts are compiled as bytecodes and executed in EVM through the computer of miners, which is very similar to Java executed in Java Virtual Machine (JVM). When the smart contract operates, it must be packaged by the miner, and written into the blockchain. Each blockchain in Ethereum has various functions and purposes. We can develop intended applications in Ethereum by writing a smart contract [13-15].

Compared with traditional contract, a smart contract is an executable code stored and running in blockchain. The smart contract may execute independently and automatically without third parties, and these running results are irreversible on blockchain and are trackable by each participant. The main features of smart contract are given as follows [15]. The smart contract has stability that a smart contract has deterministic feature: the same input always produces the same output. Because smart contracts are executable codes stored in block chain, every network participant can inspect them. Meanwhile, all the interactions with a smart contract occur via signed messages on the blockchain (see Fig. 1), and thus every participant may verify and trace the contract's operations.

III. Situation Analysis and Motivation

A. *Analysis of Current Situation*

The online shopping has been on the rise. Because consumers and suppliers may have different perceptions of product quality, this may result in business disputes. Generally, the dispute about buying inferior goods is caused by the difficulty in distinguishing qualities of goods via simple product photos, advertisements that merchants make over the top claims about products, or online shopping scams via social media. Good consumption experiences may make customers buy more products, and it is a positive cycle in online shopping environment. This is a simplified and obvious observation, but how to easily buy genuine goods at a reasonable price from online shopping is a big challenge for both customer and e-commerce company. In this paper, we give it careful consideration.

B. *Motivation*

Some e-commerce companies already have the scheme to expand seller's business. For example, on Alibaba.com, seller may apply Gold Supplier (GS) membership in Alibaba.com. All suppliers who are interested in doing business with buyers worldwide, can apply GS membership. Through authentication and verification by Alibaba.com, sellers may gain more trust from buyers, and promote their products to maximize product exposure on Alibaba.com. Of course, GS must pass some checks by Alibaba.com to approve their membership, which should be updated every year.

The GS membership is only authenticated and verified for supplier. The proposed PGS is motivated from GS membership, but further apply authentication and verification on products rather than on sellers. In addition, GS is a paid membership only used in Alibaba.com. In the proposed PGS, we form an alliance including e-commerce companies and trusted organizations to finish product grading. After approval, suppliers are authorized to display the score of PGS (an icon to demonstrate their qualities of products). Because an alliance includes more than one e-commerce company, the PGS impacts widely in e-commerce environment than GS. Therefore, using PGS may create more awareness and give more exposure to the products. PGS is a better way to insure product quality (as we know, even famous sellers may have poor products), or rather PGS is a best way to resolve dispute problem in online shopping environment.

However, compared with the number of sellers, the number of products from all suppliers will be so huge. Therefore, in this paper, we adopt blockchain, a decentralized technology, to deal with such big data for product grading. In the proposed BPGS, 51% of attacks cannot be completed unless 51% of e-commerce companies and trusted organizations in this alliance are simultaneously compromised. Therefore, our business model based on BPGS is not only reliable but also secure.

IV. Design and Implementation of BPGS by Smart Contract

At the present, Ethereum is the most popular public blockchain platform for developing smart contracts, since it provides a built-in language called Solidity, which is a contract-oriented language that can be applied to deploy contracts to the EVM. In this section, we implement the proposed BPGS by using Remix to write Solidity smart contracts.

A. *Framework*

Fig. 2 illustrates the block diagram of the proposed BPGS in e-commerce business model. Suppliers provide products to the alliance, which includes e-commerce companies and trusted organizations (e.g., Consumers International, a non-profit organization), for product grading. After verification and product grading, the manager of alliance writes the data into a new block on the blockchain via operating smart contracts. Based on the proposed BPGS, customers may buy products with high grades to insure product quality. The information of the blockchain cannot be modified, and thus customers can trust the product grade. Meanwhile, the blockchain is a decentralized technology, and thus buyers can finish the verification of product grading via the BPGS efficiently and securely. Finally, customers may purchase goods in a reliable and secure online shopping environment.

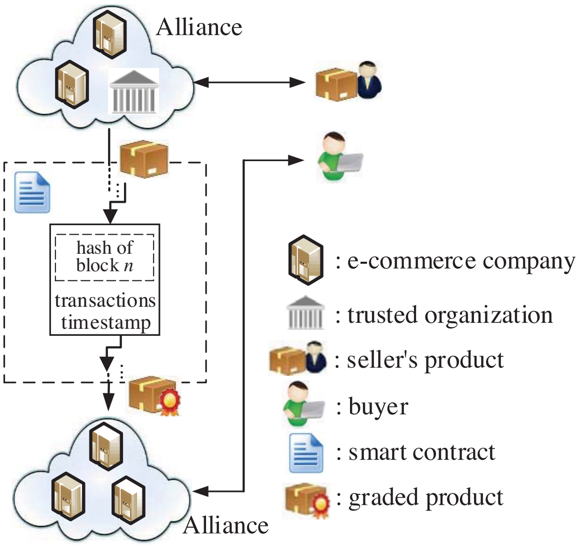
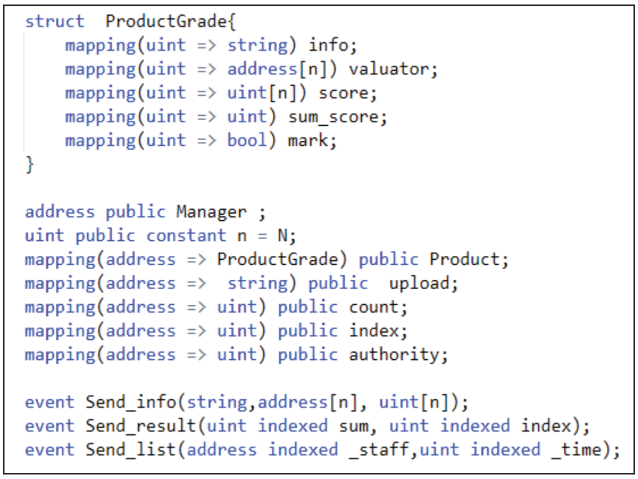


Figure 2. Block diagram of BPGS in e-commerce bussines model.

B. *Implementation Details*

We have implemented a prototype consisting of four different smart contracts in Figs. 3~6. As shown in Fig. 3, "**ProductGrade**" is used for storing product information, product grade, and the information of valuators. Note: *N* valuators are the members in this alliance (e-commerce company or trusted organization), and are assigned by the manager of this alliance. And, finally all information of product, valuators, and the score are recorded in the events: **Send_info**, **Send_result**, and **Send_list**. The code in Fig. 4 demonstrates that the constructor of smart contract is set as the manager of this alliance. When the manager and the valuator in this alliance want to carry out functions, e.g., the manage would like to assig some members as valuators, or the valuator wants to grade the product. They should be verified through **CheckManager()** and **CheckValuator()**.

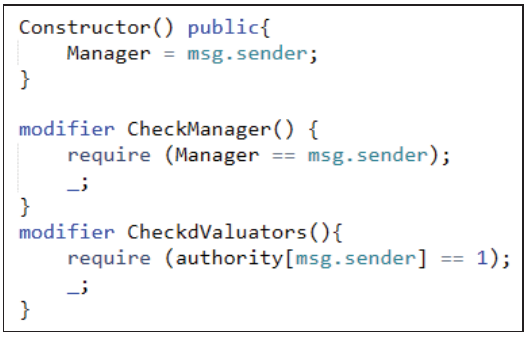


```
struct  ProductGrade{
    mapping(uint => string) info;
    mapping(uint => address[n]) valuator;
    mapping(uint => uint[n]) score;
    mapping(uint => uint) sum_score;
    mapping(uint => bool) mark;
}

address public Manager ;
uint public constant n = N;
mapping(address => ProductGrade) public Product;
mapping(address =>  string) public  upload;
mapping(address => uint) public count;
mapping(address => uint) public index;
mapping(address => uint) public authority;

event Send_info(string,address[n], uint[n]);
event Send_result(uint indexed sum, uint indexed index);
event Send_list(address indexed _staff,uint indexed _time);
```

Figure 3. Information of product, grade, and valuator in smart contract.

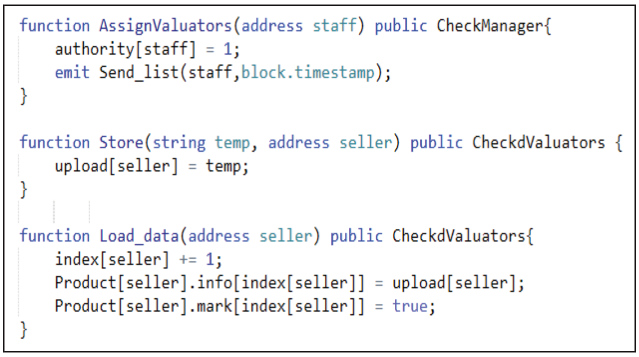


```
Constructor() public{
    Manager = msg.sender;
}

modifier CheckManager() {
    require (Manager == msg.sender);
    _;
}
modifier CheckdValuators(){
    require (authority[msg.sender] == 1);
    _;
}
```

Figure 4. Verfication of manager and valuator in smart contract.

The function **AssignVaulator()** in Fig. 5 is used for that the manage would like to assign some members as valuators. As show in Fig. 5, this function includes **CheckManager()**, such that only the manager can apply this function. Other two functions **Store()** and **LoadData()** in Fig. 5 store the information of product and supplier, on which valuators may grade thes products. To make sure that only valuators may apply the grading process, this function includes **CheckValuator()**.



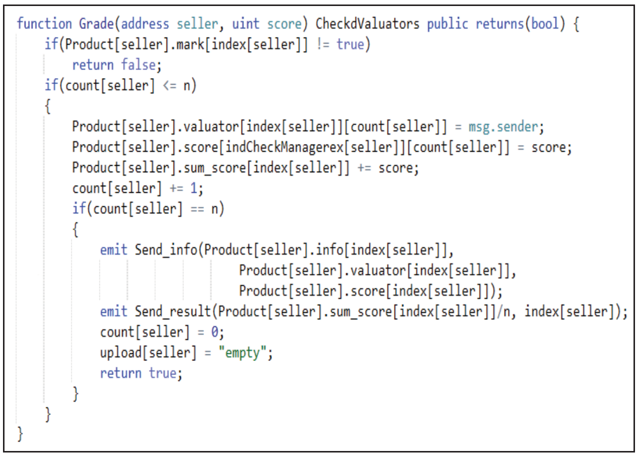
```
function AssignValuators(address staff) public CheckManager{
    authority[staff] = 1;
    emit Send_list(staff,block.timestamp);
}

function Store(string temp, address seller) public CheckdValuators {
    upload[seller] = temp;
}

function Load_data(address seller) public CheckdValuators{
    index[seller] += 1;
    Product[seller].info[index[seller]] = upload[seller];
    Product[seller].mark[index[seller]] = true;
}
```

Figure 5. Functions in smart contract.

Fig. 6 is the grading process "**Grade**" function. For grading products, all the scores of *N* valuators will be given and summarized by valuators, and then return the score to Send_result.



```
function Grade(address seller, uint score) CheckdValuators public returns(bool) {
    if(Product[seller].mark[index[seller]] != true)
        return false;
    if(count[seller] <= n)
    {
        Product[seller].valuator[index[seller]][count[seller]] = msg.sender;
        Product[seller].score[indCheckManagerex[seller]][count[seller]] = score;
        Product[seller].sum_score[index[seller]] += score;
        count[seller] += 1;
        if(count[seller] == n)
        {
            emit Send_info(Product[seller].info[index[seller]],
                                 Product[seller].valuator[index[seller]],
                                 Product[seller].score[index[seller]]);
            emit Send_result(Product[seller].sum_score[index[seller]]/n, index[seller]);
            count[seller] = 0;
            upload[seller] = "empty";
            return true;
        }
    }
}
```

Figure 6. Product grading in smart contract.

V. CONCLUSION

Motivated from the concept of Gold Supplier in Alibaba.com., we apply the grading system on products rather than on suppliers. Meanwhile, for dealing with huge verification and grading for products, we adopt blockchain, a decentralized technology, to deal with such big data for product grading. We design and implement the BPGS by smart contracts. Finally, our business model based on BPGS is reliable, efficient, and secure.

ACKNOWLEDGMENT

This work was partially supported by Ministry of Science and Technology, under Grant MOST 107-2221-E-259-007.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System,", 2008, available at https://bitcoin.org/bitcoin.pdf.

[2] C. Dwork and M. Naor, "Pricing via Processing or Combatting Junk Mail," Crypto'92, LNCS 740, pp. 139-147,1993.

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557-564, 2017.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things". IEEE Access, Vol.4, pp. 2292-2303, 2016.

[5] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," IT Professional, Vol. 19, pp. 68-72, 2017.

[6] D. Miller, "Blockchain and the Internet of Things in the Industrial Sector," IT Professional," Vol. 20, pp. 15-18, 2018.

[7] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for Large-Scale Internet of Things DataStorage and Protection," IEEE Transactions on Services Computing, doi: 10.1109/TSC.2018.2853167, 2018.

[8] A. Xu, M. Li, X. Huang, N. Xue, J. Zhang, and Q. Sheng, "A Blockchain Based Micro Payment System for Smart Devices," International Journal of Design, Analysis and Tools for Integrated Circuits and Systems (IJDATICS), 2016.

[9] Jin Ho Park, Jong Hyuk Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions", Symmetry, 9, 164; doi:10.3390/sym9080164, 2017.

[10] H. Orman, "Blockchain: the Emperors New PKI?," IEEE Internet Computing, Vol. 22, pp. 23-28, 2018.

[11] E. Karaarslan and E. Adiguzel, "Blockchain Based DNS and PKI Solutions," IEEE Communications Standards Magazine, Vol. 2, pp. 52-57, 2018.

[12] N. Szabo, "Smart Contracts," 1994, available at http://www. fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[13] D. Magazzeni and P. McBurney, "Validation and Verification of Smart Contracts: A Research Agenda," Computer, Vol. 50, pp. 50-57, 2017.

[14] V. Buterin, "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform," 2013, at http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[15] C. Braghin, S. Cimato, E. Damiani, and M. Baronchellli, "Designing smart-contract based auctions," The 2nd International Conference on Security with Intelligent Computing and Big-data Services (SICBS 2018), Guilin, China, Dec., 2018.