A Smart Contract to Facilitate Goods Purchasing Based on Online Haggle

Hsing-Chung Chen[1,2,*], Bambang Irawan[1,4], Chieh-Yang Shih[1,*], Cahya Damarjati[1,5], Zon-Yin Shae[1,3,*], Fengming Chang[1,6]
[1] Department of Computer Science & Information Engineering, Asia University No.500, Liufeng Road, Wufeng District, Taichung City, Taiwan
[2] Dept. of Medical Research, China Medical University Hospital, China Medical University, Taiwan.
[3] Pervasive Artificial Intelligence Research (PAIR) Labs, Taiwan
[4] Department of Computer Science, Esa Unggul University, West Jakarta, Indonesia
[5] Dept. of information technology, Universitas Muhammadiyah Yogyakarta, Yogyakarta, Indonesia
[6] Dept. of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan, R.O.C.
* Corresponding e-mail addresses: shin8409@ms6.hinet.net, cdma2000@asia.edu.tw, zshae1@asia.edu.tw

Abstract. Blockchain technology is growing very rapidly, not only in the field of cryptocurrency transactions but also in other fields such as health, service companies, manufacturing. Smart contracts are a series of instruction codes, which automatically verify, execute, and tamper with. With the integration of blockchain technology, it can perform tasks in real time with a high level of security. In this study, we built a smart contract model based on online haggling in determining the purchase of a product. Buyers and sellers haggle with each other for the products they want via online the seller web app. Finally, we propose a smart contract design model using online haggling, which can help provide decision-making in determining the appropriate price from the seller and buyer agreement.

Keywords: Blockchain technology, cryptocurrency, smart contract, online haggle, purchases product

1. Introduction

Development in blockchain technology is increasingly rapid. This technology enables direct (peer-to-peer) transaction without the need to involve any trusted third parties. Although it was initially used in the financial sector, this technology brought great potential to be used in many fields. Traditional transactions involving third parties often require large costs and low levels of security. With blockchain technology, it is able to overcome this problem by allowing both parties to interact with each other directly, without having to provide a clear identity from the party who is transacting (anonymous). Online haggle is used to simulate the haggling process between the buyer and seller, the buyer will survey the goods to be purchased to get the right price. After getting an online shop that sells goods, the buyer will haggle with the seller until an agreement occurs in the seller web application. Smart contracts are used to execute

the agreement that occurs between the seller and the buyer. A smart contract is an executable code that runs on the blockchain to facilitate, implement, and enforce the terms of the agreement between parties that are not trusted. The agreed price will be kept in a Smart contract between the seller and the buyer. In making payment transactions, the seller and buyer must have an E-wallet as a means of sending coins (bitcoins, ether). The structure of this paper is as follows. Section 1 discusses background information about the research of this paper. Section 2 explains related works about blockchain technology, smart contract, E-wallet and online haggle adopted for our research. Section 3 discusses our scheme proposed model based on online haggling. Then, we present the discussion in Section 4. Finally, we draw our conclusions and examine future work in Section 5.

2. Related Works

In this section, we explain about blockchain technology and its related technology. Then we will explain our proposed scheme that can be implemented in the blockchain.

2.1 Blockchain technology

In this section, we describe the key concepts related to the blockchain. Blockchain technology was introduced by Satoshi Nakamoto[1]. Maher Alharby *et. al.*[2] states that blockchain is a distributed data structure that is used to maintain a continuous record list, called block. Every block contains a timestamp and a link to the previous block. In general, blockchain is managed by peer-to-peer networks that collectively follow certain protocols to validate a new block. The block forms a linear sequence where each block references the hash of the previous block. The blockchain is maintained by a network of nodes and every node executes and records the same transactions. The blockchain is a series of blocks. Each block contains data structures that are a collection of various types of transactions that will be embedded in a public distributed ledger. The blocks are made of headers, containing metadata, followed by a long list of transactions that make up most of their size. The block header is 80 bytes, while the average transaction is at least 400 bytes and the average block contains more than 1,900 transactions[3]. In a block, block transactions are 10,000 times larger than the block header. The block structure is described as shown in Table 1 and the transaction structure is illustrated as shown in Table 2. Each block within the blockchain is identified by a hash and is generated using the SHA256 cryptographic hash algorithm on the header of the block. Each block also references a previous block, known as the parent block, through the "previous block hash" field in the block header. In other words, each block contains the hash of its parent inside its own header. The sequence of hashes links each block to its parent creating a chain that goes back all the way to the first block ever created, known as the genesis block.

Table 1. Format of the block [3].

Size	Field	Description
4 bytes	Block Size	The size of the block
80 bytes	Block Header	The field from the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Table 2. Format of the transaction [4].

Transaction Header	
Hash	The transaction's hash value
Block number	Block containing the transaction
Order	The transaction's number in the block
Timestamp	Creation time of the transaction
Sender	Sender's ID
Receiver	Receiver's ID
Signature	Sig {the transaction's hash value}

Payload
$data_1$, $data_2$,..., *data*

2.2 Smart Contract

The smart contract concept was originated from Nick Szabo in 1994[5]. A smart contract[2][6], as shown in Fig. 1, is a piece of code that resides on a blockchain and is identified by a unique address. A smart contract includes a set of executable functions and state variables. The functions are executed when transactions are made to these functions. The transactions include input parameters that are required by the functions in the contract. Upon the execution of a function, the state variables in the contract change depending on the logic implemented in the function. Contracts can be written in various high-level languages (such as Solidity or Python). Language-specific compilers for smart contracts (such as Solidity or Serpent) are used to compile the contracts into bytecode. Once the compiled contracts are uploaded to the blockchain network, it will assign unique addresses to the contracts. Any user on the blockchain network can trigger the functions in the contract by sending transactions to the contract. The contract code is executed on each node in the network as part of the verification of new blocks. We build a smart contract for the case of offering goods between seller and buyer based on the online haggle. The smart contract will automatically make transactions in accordance with the agreement that has been written in the smart contract shown in Fig. 1.

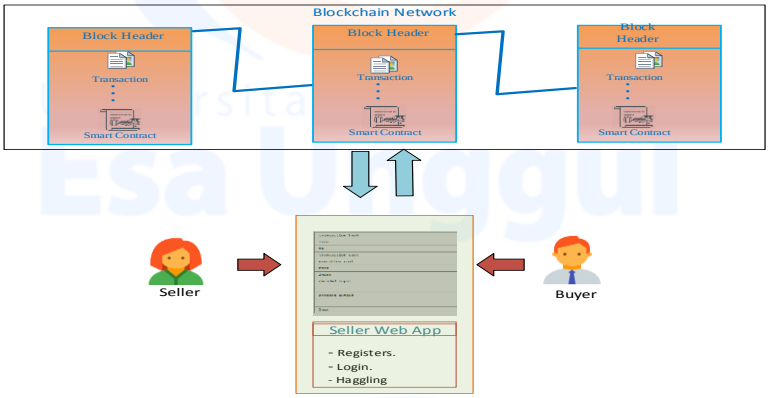

Fig. 1. The architecture of Seller Web App connected to the blockchain network.

2.3 E-wallet

Rajy Latifa *et. al.* [7] state that E-wallet is a receptacle for users to keep coins and make transactions. The address is public and is related to private key pairs and it is used for The history of the seller and buyer transaction is also stored in each wallet. As seen in Fig. 3, the wallet address of buyer-1 has 25-34 character identifiers consisting of numbers and small and large letters. The history of the seller and buyer transaction is also stored in each wallet. As seen in Fig. 2, the wallet address of buyer-1 has 25-34 character identifiers consisting of numbers and small and large letters. Most of the addresses used have 33 or 34 characters. The address usually starts with 1 and never contains the number 0 or uppercase "O", or lowercase "l" or "I" for better.

To receive a coin, the seller makes a wallet address derived from the parent address for each product as shown in Fig. 3. The Wallet-Product-A will receive coins sent by the buyer based on transaction agreed by both parties when buying product A. The product has the address of each wallet, which will receive coins based on the price of each product. More details can be seen in Fig. 4, The Wallet-Product-A with the address "1A7Gja85tvUF9CxoNQk5BM1qcVyuJkPj9b" get coins "0.0005" from the transaction to purchase product A.

Fig. 2. Wallet address for the buyer

Fig. 3. Product wallet address to receive coins.

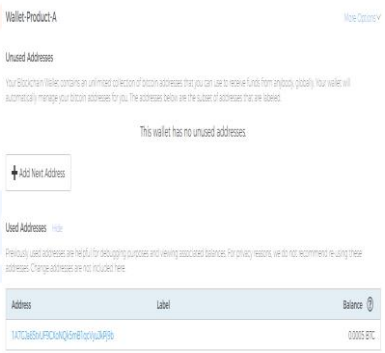

Fig. 4. Wallet-Product-A for the accept transaction.

2.4 Online Haggle

The haggle or bargain is when two parties, buyer and seller involved in a transaction such as the purchase of goods and services negotiate prices until both parties can mutually agree to a fair price. The haggling process involves two parties who make counter offers by raising or lowering price each other until the price is agreed. Individuals who try to buy goods and services try to pay as little as possible, while the seller's main goal is to maximize the selling price. Haggle is a recurring process in determining prices agreed upon by sellers and buyers. Uchendu in 1967 [9] said: "price for specific transactions, acceptable to both buyers and sellers, within the price range that prevails in the market." Online haggle[10][11] means that the haggling process carried out by using electronic devices between two parties through public channels until the agreement occurs for the price of a product or services.in developing online haggle systems, methods, and computer programs are needed to facilitate the process.

3. Our Scheme

In this paper, the proposed framework is based on the Ethereum smart contract platform on blockchain technology with haggling. The smart contract is used to execute agreements that have been agreed between the two parties, Smart contracts will execute automatically according to the agreement chosen. To make payments using cryptocurrency stored in the E-wallet that has a public key and private key, the two keys will be used between the seller and the buyer. Suppose there are two people (seller and buyer), where the seller offers goods consisting of 3 goods, goods A with price X, goods B with price Y, goods C with price Y and price of combination goods. As shown in Table 4.

Table 4. Goods & prices.

Goods	**A**	**B**	**C**	**A+B**	**A+C**	**B+C**	**A+B+C**
Price	*X*	*Y*	*Z*	*X+Y*	*X+Z*	*Y+Z*	*X+Y+Z*

a. Buyer

A person who buys goods chooses a product with a discount if he thinks that the price can be minimized and the goods function properly as needed. However, most buyers rarely consider aspects of quality and assurance in decision making. The buyer does not get enough information about "goods" so that the aspects into consideration factors are usually price, quality, etc. Most buyers have little interest in products without discounts.

b. Seller

The seller offers three types of goods at different prices, goods with discount prices and goods without discount prices. Where the cost of making these three types of goods is different. The seller provides a bid price for the buyer for the goods being sold. After the buyer knows the price of the goods he wants, the buyer offers a price via the seller web app. The seller can approve the buyer offer or appeal the buyer offer until a price agreement is reached between the two parties. In addition, the seller can provide a discount with a certain amount for the buyer with a certain amount of purchase terms. For example, if the buyer purchases above 5 goods, the buyer will get a 5% discount of the total price. The value of the discount amount can be given based on the haggling of the seller and buyer. The processes of the scheme we propose as shown in Fig. 5. First, the notations used in the scheme are listed in Table 5.

Table 5: The notations used in the proposed scheme.

Notation	meaning
K_p^s	E-wallet seller private key
$addr_{1..m}^s$	Address product seller or public address product from 1..m
$K_p^{B_i}$	E-wallet buyer private key
$addr_j^{B_i}$	E-wallet buyer address or public address
U_{bi}	The bi^{th} buyer
e_{bi}	The bi^{th} email buyer
PW_{bi}	The bi^{th} password default buyer
PW_{bibi}	The bi^{th} new password buyer
T_i and T_{tr}	The register timestamp and transaction timestamp
pro_{bi}	The purchased product
sum_{bi}	The sum of product purchased
prc_{bi}	The haggle prices from the buyer of the product
pro_s	The products offered by the seller
sum_s	The sum of seller product
prc_s	The haggle product prices from the seller
$Toprc^{B_i}$	The total price
X	The coin amount

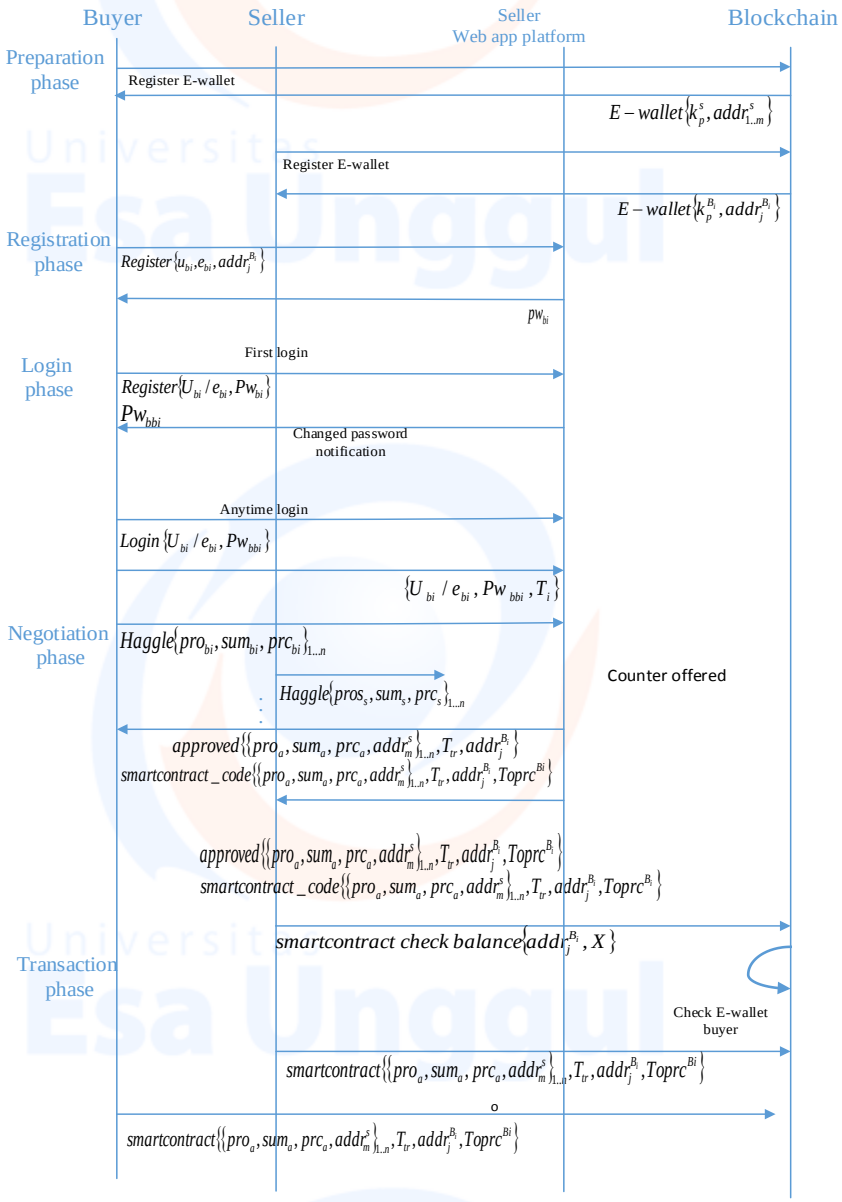

Fig. 5. Our scheme processes.

To allow for fair trading, the smart contract that contains the agreement between seller and buyer is created. We made 3 smart contract algorithms for our scheme in online haggling as follows:

1. Smart contract algorithm to check coins in the E-wallet buyer to ensure sufficient coins in product purchase transactions on the seller side in **Algorithm 1**.

Algorithm 1 Pseudo-Code of `checkCoin()`,
Which check coin in E-wallet buyer

1: **Input:**
`Public address buyer` i^{th}
`X Uint amounts of coin buyer`
$Toprc^{bi}$ `Total price for the transaction`

2: **If (**`Public address buyer,X) >=` $Toprc^{bi}$ **Then**
the transaction is continued to the `smart contract seller address`
Else
Log out or exit
End if

2. Smart contract algorithm for sending coin from E-wallet buyer to seller's wallet according to the product address purchased on the buyer side in **Algorithm 2**.

Algorithm 2 Pseudo-Code of `sendCoin()`,
Which sent coins from E-wallet buyer to E-wallet seller product according to the product purchased

1: **Input:**
{ pro_a `products purchased types`
Sum_a `product purchase amounts`
Prc_a `Product price`
$Address\ product_a$ `E-wallet product`
}
T_{tr} `Timestamp transaction`
`Public address buyer` i^{th}
$Toprc^{bi}$ `Total price for the transaction`

Output: subtract(`Public address buyer,X)`
2: $\{pro_a, Sum_a, Prc_a, Address\text{-}product_a\}_{1..n}$ ←transaction for product $a_{1..n}$
3: Balance(`Public address buyer,X)-` $Sum(Prc_{a1..n})$ `:=` $Toprc^{bi}$
Send balance $Toprc^{bi}$ `-` Prc_{a1} `:=` $(Address\text{-}product_{a1}, X)$ ←send coin
.
.
.
4: Send balance $Toprc^{bi}$ `-` Prc_{an} `:=` $(Address\text{-}product_{an}, X)$

3. The smart contract algorithm for receiving coins in the wallet seller according to the product address sent by the buyer through E-wallet buyer on the seller side in **Algorithm 3**.

Algorithm 3 Pseudo-Code of `ReceiveCoin()`,
Which receive coins from E-wallet buyer to E-wallet seller product according to the product purchased

1: **Input:**
`{` pro_a products purchased types
Sum_a product purchase amounts
Prc_a Product price
Address $product_a$ E-wallet product
`}`
T_{tr} Timestamp transaction
Public address buyer i^{th}
$Toprc^{bi}$ Total price for the transaction

Output: subtract(`Public address buyer,X)`
2: $\{pro_a, Sum_a, Prc_a, Address\text{-}product_a\}_{1\ldots n}$ ← transaction for product $a_{1\ldots n}$
3: Balance(`Public address seller,X)-` $Sum(Prc_{a1..n}) := Toprc^{bi}$
Receive balance $(Address\text{-}product_{a1}, X)$ ← receive coin
.
.
.
4: Receive balance $(Address\text{-}product_{an}, X)$

4. Discussion

In this section, online haggling has grown a lot starting from retail, where sellers can sell directly to the ultimate consumer. Terwiesch Christian *et. al.* [11] proposed the model where the retailer waits for potential buyers to submit offers for a given product and then chooses to either accept or reject them. Consumers whose offers have been rejected can invest in additional haggling effort and increment their offers. Muleshkov Angel S. and *et. al.* [12] develop a model for price haggling between a single buyer and a single seller. They are proposing a non-probabilistic haggling model which determines how a single buyer and a single seller determine the price of a good according to a predetermined rule. This model differs from other models for haggling and bargaining, as it does not make explicit use of probability or utility maximization for decision making. Blockchain technology can be combined with online haggling efficiently for product purchases in order to get a fair price between buyer and seller. By an embedded smart contract, it will be easier for both parties to transact according to the agreement contained in the smart contract. Smart contract will trigger a transaction when both parties have made an online offer and agree on the price for the offered product.

Conclusion

In this article, we have explained the principles of online haggling for some product transactions between sellers and buyers. The web app platform is used as a means of haggling between the two parties until an agreed price occurs. Transactions can be triggered automatically with the smart contract option embedded on the blockchain based on online haggling for product purchase decisions. With embedded smart contracts, the level of security will be higher, because it is resistant to interference, Non-repudiation, personal has no reputation, and cannot be changed because all transactions are recorded in the distributed ledger that is decentralized.

Acknowledgments. This study is supported by the Ministry of Science and Technology (MOST), Taiwan, Republic of China, under the grants of MOST 107-2221-E-468-015. This research is also partially supported by the MOST through Pervasive Artificial Intelligence Research (PAIR) Labs, Taiwan under the grants MOST 108-2634-F-468-001

References

1. Nakamoto, S.: Bitcoin : A Peer-to-Peer Electronic Cash System. (2008) 1-9
2. M. Alharby., A. van Moorsel. : Blockchain Based Smart Contracts : A Systematic Mapping Study. in *Computer Science & Information Technology*, (2017) 125–140
3. Andreas M. Antonopoulos.: Mastering Bitcoin. O'ReillyMedia, (2017) https://github.com/bitcoinbook/
4. L. Zhou, L. Wang, Y. Sun, and P. Lv.: BeeKeeper: A Blockchain-Based IoT System with Secure Storage and Homomorphic Computation. *IEEE Access*, vol. 6, (2018) 43472–43488
5. N. Szabo, Ed.: Formalizing and securing relationship on public networks. vol. 2, no. 9, (1997)
6. Mohanta B. K, Panda S. S., and Jena D.: An Overview of Smart Contract and Use Cases in Blockchain Technology. 9th Int. Conf. Comput. Commun. Netw. Technol. (2018)1–4
7. Latifa E.-R., My Ahemed E. K., Mohamed E. G., Omar A.: Blockchain: Bitcoin Wallet Cryptography Security. Challenges and Countermeasures, J. Internet Bank. Commer., vol. 22, no. 3, (2017) 1–29
8. Eskandari S.,. Barrera D, Stobert E., Clark J.: A First Look at the Usability of Bitcoin Key Management. *arXiv preprint arXiv:1802.04351*, (2018)
9. Uchendu, Victor C.: Some principles of haggling in peasant markets. Economic Development and Cultural Change 16.1 (1967) 37-50
10. Thirumalai S., Hill C.,. Joseph B. A, Green M. K., (54) {HAGGLING IN AN ELECTRONIC COMMERCE SYSTEM}, (2012) 19
11. Terwiesch C., Savin S., Hann I.-H.: Online Haggling at a Name-Your-Own-Price Retailer: Theory and Application. *Manage. Sci.*, vol. 51, no. 3, (2005)339–351
12. Muleshkov A.S. , Sweat K. R.: Price haggling between a single buyer and a single seller. 1-13