Blockchain-based Trusty Buyer Coalition Scheme Using A Group Signature

Laor Boongasame[1], Supansa Chaising[2], and Punnarumol Temdee[3,*]

[1]*Department of Mathematics, Faculty of Science, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand*
[2]*Department of Information Technology, The International College, Payap University, Chiang Mai 50000, Thailand*
[3]*Computer and Communication Engineering for Capacity Building Research Center, School of Information Technology, Mae Fah Luang University, Chiang Rai 57100, Thailand*
E-mail: laor.bo@kmitl.ac.th; supansa_c@payap.ac.th; punnarumol@mfu.ac.th
[*]*Corresponding Author*

Received 15 February 2021; Accepted 02 August 2021;
Publication 30 September 2021

Abstract

Without trust, buyers may not join a coalition. Despite the tremendous need for trustworthy relationships in buyer coalitions, no current buyer coalition scheme explicitly tackles confidence issues with blockchain technology. This study proposes an algorithmic design, the blockchain-based trusty buyer coalition scheme, to satisfy the trust requirement among different actors while forming the coalition. All activities forming a coalition through a decentralized public ledger can be explicitly examined. Consequently, the proposed algorithm can ensure anonymity within a community, resulting in trusting relationships. Furthermore, the proposed algorithm can ensure correctness and accountability by recognizing misbehavior and enforcing alternative forms of punishment. Additionally, the discovered algorithm can be applied to mobile commerce applications.

Keywords: Digital signature, trusted third party, group buyer coalition, group signature, blockchain.

Journal of Mobile Multimedia, Vol. 18_2, 203–230.
doi: 10.13052/jmm1550-4646.1823
© 2021 River Publishers

1 Introduction

Recently, buyer coalitions are becoming increasingly significant, particularly in electronic commerce (e-commerce). The buyer coalitions provide benefits to both buyers and sellers. In general, a buyer coalition is a group of consumers who join together to bargain with sellers to purchase similar goods at a greater discount [1]. More importantly, consumers may increase their negotiating power and negotiate more favorably with the sellers at lower prices while buying items. Thus, a buyer coalition helps drive down the monetary value of participant contact. If the lot's price is less than the normal retail price, the buyers will profit from buying the goods in large bundles/lots by buyer coalitions. On the other hand, if the wholesale marketing expense (e.g., ads or bidding costs) is less than that of retail marketing, the sellers will benefit from selling the goods in larger packages by buyer coalitions. For real-life e-commerce, there is usually a third party, which is generally the website that facilitates the buying and selling process. Before the buyer coalition process, the buyers secretly provide the reservation price on the website and receive the coalition price in exchange. There is also a loosely established coalition for buying. Buyers only know if they can buy a product and how much they have to pay for it. Although the buyer coalition process takes place quickly through the third party, the facts and some important information, such as the exact numbers of the buyers formed and the proposed price of each buyer, are not disclosed. Consequently, particularly for the buyer coalition, there is a need to provide a testable third party.

There are already several buyer coalition systems. Many works do not explicitly address the relationship attributes—namely, the general and algorithmic aspects of buyer coalitions with bundles of items [2–5], multi-attribute coalitions [6–8], the strategy [9], the marketing/distribution approach [10], the knowledge management perspective [11], the mechanisms [4, 12–15], and having incomplete information [16, 17]. The second group of work explicitly addresses the relationship attributes, such as 'trust' and 'power' [18]. Trust is a measure of confidence in another party's integrity and justice, and it is vital for successful coalition formation. In the absence of trust, none of the participants will want to join the coalitions. Despite many existing buyer coalition schemes, no current scheme explicitly considers trust in a third party. Furthermore, despite extensive study on trusted third parties in other research fields, few studies prove the benefits of buyer coalitions formed as a result of trust, which is one of the reasons buyers may desire to build such coalitions.

A buyer coalition scheme is also commonly implemented with a trustable third party using a group signature, which is generally a digital signature that allows a member to anonymously sign a message on behalf of the group. As a result, executives and members alike are interested in this group signature scheme. A trustworthy group authority can manage each group as the members join and leave the group and can reidentify individual signatories in disputes. Moreover, different groups can choose to be governed by the same trusted group authority, or leadership over the group may be thoroughly distributed among its members. Similarly, the buyer coalition schemes using a group signature provide all buyers with the same information as the group information and guarantee anonymity, which ensures trust because a trusted group authority can confirm. However, it will be more trustworthy to have a transparent third party working on behalf of a group authority, as the primary purpose of this study.

Blockchain is a distributed ledger technology that enables data to be stored globally on thousands of peer-to-peer network servers while allowing everyone on the network to see the entries of anyone else in real-time [19]. The proof makes it difficult for one person to obtain control of the network. Furthermore, the blockchain is immune to changing its data because, without altering all subsequent blocks, the data cannot be altered once registered in any given block. This evidence helps the participants independently validate and inspect transactions. Satoshi Nakamoto effectively improved blockchain design by applying a mechanism to time stamp blocks without needing a trusted party to sign them [20]. Recently, the applications of blockchain can be found widely. For cryptocurrency [21], the blockchain's invention solves the double-spending problem without the need of a central server or a trusted authority for Bitcoin. For businesses [22], by offering the ability to build secure and real-time communication networks, blockchain maintains the promise of transactional transparency. For healthcare [23], blockchain promotes security by keeping an incorruptible, decentralized, and transparent log of all patient data. While blockchain is transparent, it can protect medical data's sensitivity by concealing any individual's identity with complex and secure codes. The technology's decentralized nature also allows patients, doctors, and healthcare providers to quickly and safely share the same information. Following the blockchain's principle, the blockchain-based trusty buyer coalition scheme using a group signature is proposed in this study to promote trust among the buyers while joining the coalition.

2 Literature Reviews

The literature reviews of this study include the buyer coalitions and blockchain-based applications, which are provided in Sections 2.1 and 2.2, respectively.

2.1 Buyer Coalitions

A buyer coalition is a group of buyers who negotiate with sellers at a higher discount to purchase similar goods. Buyer groups are becoming increasingly relevant. One explanation is that consumers will increase their bargaining power and negotiate more favorably with sellers to purchase products at lower prices [24]. Another reason is that a buyer coalition helps reduce the cost of communication between buyer and seller. If the lot price is less than the normal retail price, it is advantageous for the buyer group to purchase in bulk. On the other hand, sellers can profit from selling the items in larger bundles. Bargain hunters who are reluctant to pay full price for a selling item but are willing to wait a few days for a lower price to become available are motivated by group buying [25], which exists both in commerce and in-service industries—such as insurance—to pursue better deals for a group [9].

In general, all buyer alliance models have several stages [26]. First, the coalition leader, or a representative of the coalition, negotiates with the sellers to provide goods or services in a stage called negotiation. The next stage is the electing or voting stage, when the members nominate a coalition leader to oppose those offers. Not all coalition formation processes involve this stage. Next, in the coalition formation stage, the coalition leader invites new members to join his party. Then, during the payment collection stage, the coalition leader is in charge of collecting fees from coalition partners and ensuring that the entire sum is paid to the sellers. Once a contract is completed and the purchased goods arrive, they can deliver goods to coalition members in the execution/distribution stage.

For a buyer coalition, two main stages are involved: finding a coalition structure and splitting the surplus among the coalition buyers. Within the first structure, the buyer coalition research can be grouped into three categories: the buyer coalition with substitute items or a combination of items, the buyer coalition with either complete or incomplete information, and the buyer coalition with trusting relationships between agents or awareness level. The grouped buyer coalition research is shown in Table 1.

Table 1 The grouped buyer coalition research

Coalition Formation Research	
Items	Coalitions with substitute items [18]
	Coalitions with complementary items [17]
	Coalitions with bundles of items [5, 27]
Information	Coalitions with incomplete information [9,16]
	Coalitions with uncertain or heterogeneous information [6]
Trust	The trusting relationships between agents in a buyer coalition [18]
	Coalitions with various levels of awareness that buyers may have about other roles' actions/intentions [28]
	The trust is considered by investing 'centrality', 'closeness', and 'betweenness' attributes of the coalition leader [29]

It is unlikely that a buyer will join a group if they do not trust the other members' integrity. Many people express their faith in an unknown trustee by using the word "trust", which can be defined in a variety of ways [30]. However, direct confidence in a third party is not mentioned. In this analysis, the group signature was used and a buyer-partner system on the blockchain that is both reliable and secure is proposed. Ultimately, buyers who join a coalition should have a sense of trust in one another.

2.2 Blockchain-based Applications

Blockchain-based applications have attracted tremendous interest among many researchers for different purposes. For traceability purposes, blockchain technology was applied to design the software architecture community in a real-world project, called originChain, that was built for a case study of imported product traceability. The blockchain-based traceability system was constructed to restructure the current system by replacing the central database with blockchain [31]. It also introduced opportunities to apply blockchain to the agri-food industry [32], where blockchain technology can ensure food safety and integrity through a decentralized approach [33]. For the purpose of data storage, a blockchain-based decentralized storage scheme was proposed to enhance the full use of remaining personal disk space and solve the waste of resources [34]. Moreover, Kumar and Tripathi [35] proposed a blockchain-based framework for data storage that would share files by using content-addressable block storage in the peer-to-peer model.

For security purposes, Balaji et al. [36] proposed a secured and decentralized file transfer application based on a private blockchain network, which can be applied in small organizations. This application provided high-security file sharing by employing some algorithms from the cryptography aspect to safely encrypt the file. Patel [37] introduced a framework for secure and decentralized medical imaging data sharing through blockchain consensus. The proposed blockchain framework can enhance parties' consensus without relying on a central authority and eliminate third parties' access to protect personal health information. Recently, blockchain technology was applied in the food supply chain system to enhance information security, product quality, and safety management [38]. An application of blockchain technology can secure the data obtained from the financial transaction system, which can only be accessed by authorized clients using M2M authentication. Mainly, blockchain technology can protect the local system's data by using hashing [39]. Furthermore, a blockchain-based secure data sharing mechanism was proposed for distributed vehicular networks. This proposed mechanism can enhance security and privacy by incorporating the symmetric key cryptographic mechanism and providing a trust management mechanism to determine the authenticity of the nodes involved in the network [40]. In recent years, blockchain has been introduced widely for voting [41–43] and itself has introduced many business models in different applications, such as electrical trading [44–46], smart agriculture [47, 48], and healthcare services [49–51].

3 Theoretical Background

3.1 Auction

An auction is a process of purchasing and selling products or services by putting them up for sale, taking bids, and then selling or buying the item from the highest or lowest bidder [52]. There are four basic types of auctions that are commonly used and studied. First, in an ascending auction, the price is gradually increased until only one bidder remains, and that bidder wins the item at the final price. Conversely, in a descending auction, the auctioneer begins with a very high price and gradually lowers it until a bidder declares that she will accept the current offer. In a first-price seal-bid auction, each bidder submits a single bid without seeing the other bidders' offers, and the item is sold to the bidder with the highest bid; the winner pays the highest or "first" price bidder (i.e., the winner pays her bid). Finally, in a second-price

sealed-bid auction, each bidder submits a single bid without seeing other bids, and the item is sold to the bidder who makes the highest bid; the price she pays is the second-highest bidder's bid, or "second price".

3.2 Digital Signatures

A digital signature is a mathematical scheme for verifying the proper message transmission [53]. A private key and a public key are used for validation in the digital signature [54]. Typically, the recipient uses their public key to encrypt the data and their private key to decrypt it. More specifically, the private key is used to encrypt a smaller version of the digest message, while the public key is used at the receiver point to decrypt the digested message, with the receiver verifying receipt of the digested message. These two parallel processes occur at the same time. Furthermore, the original message is sent without encryption or decryption. Instead, the original message is sent to the recipient through the Message Digest algorithm and the result of these two processes is compared to the message received. The two parallel processes are shown in Figure 1. The development of the Message Digest sender and encryption algorithms is one of the processes. The other process indicates that the original message was sent without creating a Message Digest or encrypting/decrypting the sender/recipient point. Figure 1 also shows the receiver-side information on the two parallel processes above, where Message Digest is created and encrypted messages from the previous process are decrypted. If the results of the above two processes are the same, it will indicate that the message is authentic. Otherwise, the message received will be considered not authenticated, and then the signature would be validated.

3.3 Group Signature

A group signature scheme, one of the famous digital signature techniques, was introduced by Chaum and van Heyst [55] and allows each group member to anonymously produce signatures on behalf of the group. However, in a dispute, the identity of a signature's originator can be revealed by a designated entity, which is applied for such security applications as electronic auction and electronic voting. Unlike ordinary signature schemes, group signature schemes allow any member of a group of signatories to sign documents on behalf of the group. This study mainly focuses on the group signature scheme's properties in Table 2.

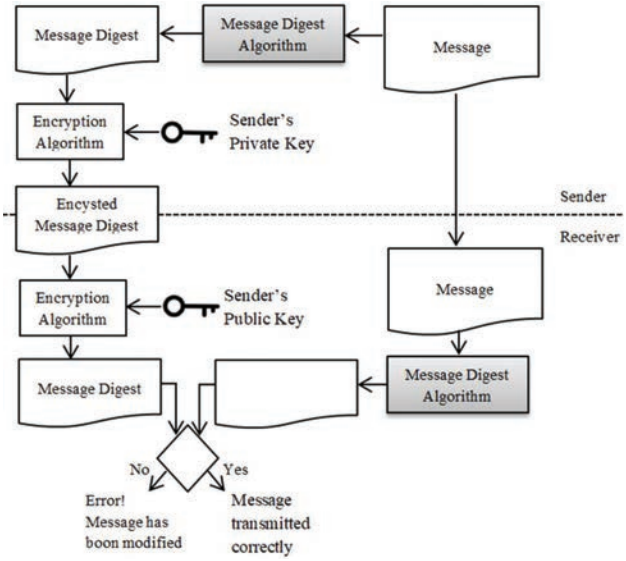

Figure 1 Digital signature [54].

Table 2 Group signature scheme's properties

CORRECTNESS	Signatures that are produced using the SIGN command by a group member must be accepted by VERIFY party.
UNFORGEABILITY	Only members of a group can sign messages on behalf of the group.
ANONYMITY	Identifying the actual signatory is unfeasible for everyone but the group manager after having the given valid signature of some messages.
UNLINKABILITY	It is unfeasible to determine if the same group member computed two different valid signatures.
EXCULPABILITY	No group member may produce signatures on behalf of other members, not even the group manager.
COALITION-RESISTANCE	No subset of group members should obtain and produce legitimate group signatures that are untraceable (perhaps including the group manager).

3.4 Smart Contract

Blockchain technology was introduced when Satoshi Nakamoto invented Bitcoin in 2008. It provided the software-based authentication, confirmation, recording, and integrity necessary for currency transfers. Furthermore, the

```
/* Joining network */
Join the network by connecting to known peers;
Start BlockGen();
 /* Main loop */
while running do
    if BlockGen() returns block then
      Write block into blockchain;
      Reset BlockGen() to the current blockchain;
      /* Gossiping rule */
      Broadcast block to peers;
  end
  /* Longest-chain/validation rule */
  if block received & is valid & extends the longest
  chain then
      Write block into blockchain;
      Reset BlockGen() to the current blockchain;
      Relay block to peers;
  end
end
/* PoW-based block generation */
Function BlockGen():
    Pack up transactions;
    Prepare a block header context C containing the
     transaction Merkle tree root, hash of the last block
     in the longest chain, timestamp, and other essential
     information reflecting blockchain status;
  return new block;
end
```

Figure 2 General procedure of Nakamoto consensus protocol (adopted from [56]).

blockchain structure is an append-only data structure, which ensures that new blocks of data can be added to it, but it cannot be modified or removed. In accordance with the stochastic consensus protocol based on Proof-of-Work (PoW), the blockchain method uses a decentralized public ledger to test how the blockchain achieves consensus. The abstract version of the Nakamoto consensus protocol is shown in Figure 2. Additionally, the blockchain can

form based on public or private modes. First, public blockchains give read access and the ability to transact to any user on that network. This type is often used for cryptocurrencies (e.g., Bitcoin and Ethereum). Alternatively, private blockchain not only limits both write access and read access to specific participants, who are able to verify their transaction internally.

For blockchain, smart contracts are lines of code that are stored and automatically executed on a blockchain when predetermined terms and conditions are met. Nobody may modify the code or alter its execution actions once the smart contract is deployed. Thus, smart execution of contracts guarantees, as written, binding parties to an agreement. This binding provides a powerful new form of trust that does not currently exist. The detailed features will be covered in Section 4.

4 Proposed Buyer Coalition Scheme

For this research, buyers and third parties (or authorities) can trust blockchain technology. First, the buyers and the third party will register on blockchain technology. Buyers then give a reservation price, which is the highest price that the buyer is still willing to pay for a single purchase from a seller on the blockchain. It is signed with a group signature scheme and written on the decentralized public ledger. When it is time to pay the coalition prices, the third party forms a coalition and publishes the hashed coalition prices of buyers in a coalition and the item's price schedule, which—in a homomorphic cryptosystem—is encrypted. The buyers define their coalition prices, and, in turn, the third party opens their payments. Moreover, if the total amount of buyer payments does not equal the sum of received coalition prices, third parties will ask the blockchain to find fraudulent buyers by sending the blockchain the obtained group signatures, corresponding buyer payments, and encrypted price schedule.

The price schedule and the reservation prices cannot be deduced through blockchain because they are written on a decentralized public ledger. The blockchain system will measure each buyer's actual coalition prices, thus identifying the misbehaving buyers, such as those who have committed the payments that differ from the actual coalition price. As buyers often pay their coalition price to the third party, the proposed scheme is right. The proposed framework would also increase the transparency that the originators of wrongdoing can still uncover, and an appropriate punishment mechanism can be applied to prevent repeated misconduct. Finally, the inability to link buyers and their coalition prices is imposed by the proposed framework.

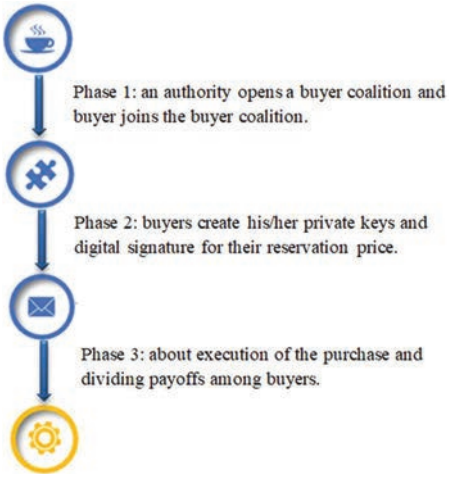

Figure 3 Three-phase proposed scheme.

In this section, an informal description of our buyer coalition process is described.

4.1 Proposed Mechanism Overview

The proposed scheme consists of two participants: the buyers and the third party. Initially, the third-party will form a coalition. Then, the buyers who want to join the coalition will place their reservation prices using the blockchain mechanism. In Figure 3, the proposed scheme is organized into three phases.

In the first phase, the third party opens a buyer coalition with a seller's price schedule. The seller's unit price of the item is represented in the following algorithms by a descending function P: a -> real number, where P(a) is a unit price that the seller would expect from selling a bundle of size 'a' of the item 't'.

The second phase is bidding. Buyers who want to join the buyer coalition will need registration to the blockchain system first. Then, buyers create his/her private keys and digital signature for their reservation price and broadcast or send them to other buyers in the coalition on the blockchain system.

Because of the buyers' discounted price, the third phase is conducting the purchase and dividing payoffs between buyers. This step calculates coalition prices through third party algorithms 1 and 2, which are comprehensively

summarized by Figures 9 and 10, respectively. The inputs to these algorithms are buyer reservation prices and the seller's actual price schedule. The third party cannot reduce the price schedule or modify any reservation prices because both price schedule and reservation price will be recorded in the blockchain.

After all, each buyer's coalition price is always lower than or equal to that buyer's reservation price. These returns result from the excess between the buyer's reserve price and the seller's price. Therefore, the coalition's price is the reservation price of the buyer minus any payout to the sellers.

4.2 Design Buyer Coalition Smart Contract in Blockchain

A use case diagram is a description of the dedication of a user of the software that shows the relationship of the user to the different use cases in which the user is engaged. The use case diagram of the buyer coalition smart contract is shown in Figure 4.

In Figure 4, the main actors are the third party, which can self-register and will form a buyer coalition, and the buyers, who can self-register, place a reservation price or bid, and get the coalition price. In addition, buyers in a buyer coalition forming process are registered first before the bidding time, and there are some conditions as follows:

(1) Registration must be completed before proposing.
(2) The functions cannot be called in any order.

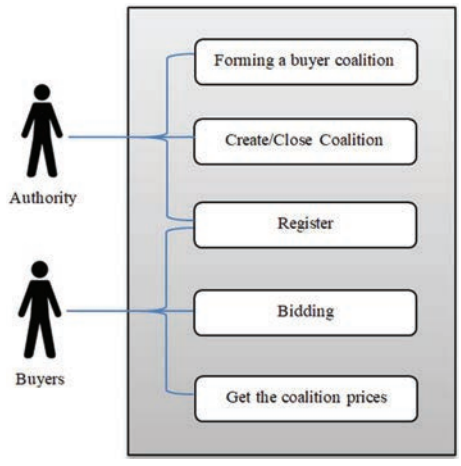

Figure 4 The use case diagram of the buyer coalition smart contract.

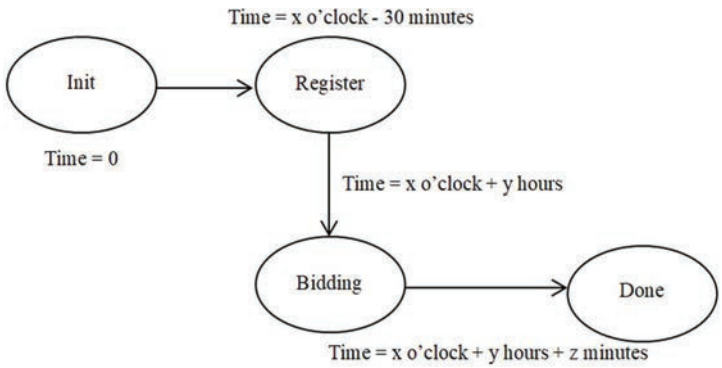

Figure 5 The finite state machine of the buyer coalition smart contract.

(3) Bidding is opened only for a specified period of time and specific item.
(4) The winner can only be determined after the forming buyer coalition is complete.

Note that the use case diagram provides only static details. Therefore, the design principle and the captured dynamics with a finite state machine diagram are applied, as shown in Figure 5.

A description of a Finite State Machine (FSM) is used to define the processes through which knowledge or tasks transfer from one state to another for action, under a set of rules [57].

This FSM is composed of:

(1) States, including a starting state and one or more ending states, indicated by double circles.
(2) Transitions that take one state to another.
(3) Inputs that bring out the transitions (such as T = 0, T + 10 days, and T + 11 days)
(4) Zero or more outputs during transitions that happen in the indicated states (e.g., registration (Regs), bidding (Bid), and get coalition price (Done))

From Figure 4, the system begins its operation after initialization in the Init state and then transitions into the Regs state, where registration can take place. Thirty minutes before the start bidding state, the system moves from the registration state into the bidding state. The bidding phase takes about y hours, after which the system enters the done state, at which point the coalition price can be requested. Transitions in this case are temporal, or time-driven, with Time = x o'clock = 30 minutes, Time = x o'clock + y

Table 3 Notations

$cost_b$	Payment of the committed coalition price to buyer b
sid	The coalition structure's selection session identifier
$Sig_X(m)$	The signature m was created by principal x
$Gs_b(m)$	Group signature of the m message generated by member of group b
gpk(G)	Public key for group G
pk(X)	Principal X's public key
sk(X)	Principal X's private key
h(m)	Message m's hash value
$Enc_{pk(X)}(m)$	The message m is encrypted with the X public key pk (X)
c_b	The buyer's coalition price
pay_b	The number of coalition prices that buyer b is currently paying to the third party
r_b	The reservation price for the buyer b

hours, and Time = x o'clock + y hours + z minutes limiting the duration of each phase. These dynamic rules for transitioning through the buyer coalition process must be captured in the smart contract to enable trust. Lastly, all protocols will be processed through digital signature and group signature.

4.3 Protocol Specifications

The four-part protocol is provided in this section. Such protocol sections include set-up, auction, establishment, and agreement of the buyer coalition, and they are discussed below. The notations used in this scheme are shown in Table 3.

4.3.1 Set-up

This step aims to establish a user ID or a PIN for the user. A third party who wants to create a buyer coalition will register, and the blockchain system will generate a PIN or user ID for the third party. Then, the third party creates the buyer coalition. Finally, buyers who want to join the coalition will register, and the blockchain system will generate a PIN or user ID for the buyer. The set-up protocol is shown in Figure 6.

4.3.2 Bidding

The process aims to show that buyers periodically submit reservation price signatures to the blockchain system and write the reservations to blockchain

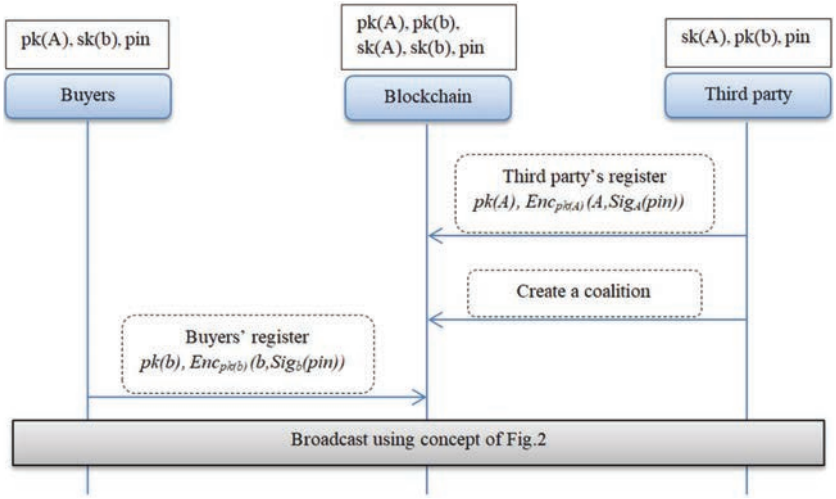

Figure 6 The set-up protocol.

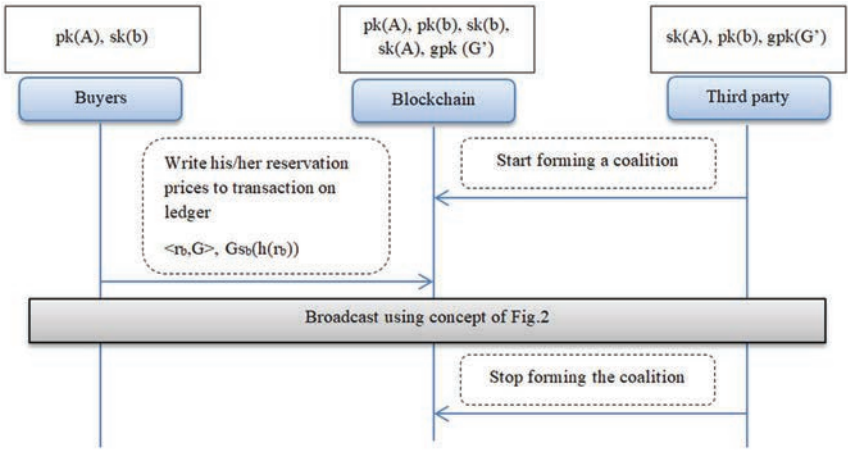

Figure 7 Protocol for coalition bidding.

transactions. A message from buyer b who is a member of group G is denoted by ($<r_b, G>$, $Gs_b(h(r_b))$, where (r_b, G) is the reserve price. If desired, the other buyers can verify $Gs_b(h(r_b))$ with the community public key gpk(G) after receiving this message. From Figure 7, the third party starts to form a coalition. Then, the buyers write their reservation price to a transaction on the blockchain system. Finally, the third party stops forming a coalition after all buyers position their reservation price or expire periodically.

4.3.3 Formation of a buyer coalition

A buyer coalition is created during this phase. Each of the elements in L' is the form ($h(c_b)$, where L' is the set of prices including the tuples of group G. Additionally, r_b denotes the reservation price of buyer b. The coalition composition protocol is shown in Figure 8.

From Figure 8, the third party forms a buyer coalition when the time is reached, and then divides the discounts and payoffs through Algorithms 1 and 2, respectively. Later, the third party appends the coalition price of all buyers to a transaction in the blockchain system. Then, the system broadcasts to all buyers, who will have to verify their validity after receiving the message. Then, the buyers will check whether their coalition prices are equal to or less than the buyers' reservation price so that they will return to the blockchain system. Afterwards, the coalition buyer is formed based on an existing study [58].

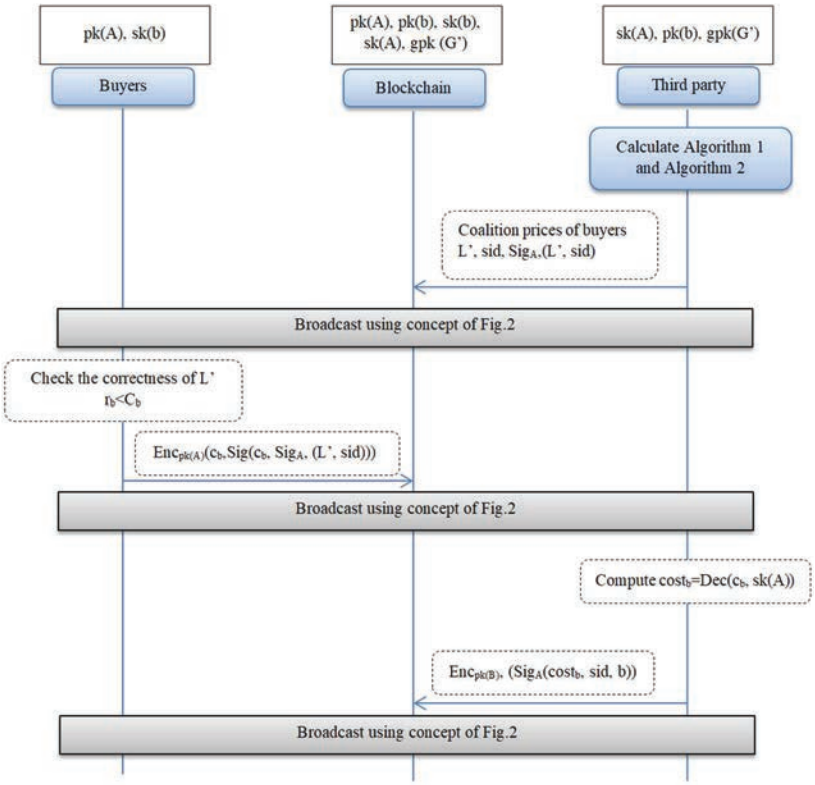

Figure 8 Protocol for the formation of a coalition.

4.4 Mechanism for Coalition Formation

As soon as all buyers are included in the coalition, the buyers with the lowest reservation prices will be removed one at a time until the coalition's utility value is greater than zero. A coalition structure G will be created in this study based on which has the highest number of buyers with non-negative utility or an empty coalition structure G*, and the algorithm will stop. Figure 9 shows the algorithm for creating and controlling coalitions.

There are two parts for next step. First, the actual rebates for all G^* coalition buyers are calculated using Algorithm 1. Then, the minimum discounts necessary and the actual discounts of all buyers are compared in the $G^* \backslash \overline{G}^*$. If the minimum discount required for any purchaser in $G^* \backslash \overline{G}^*$ is greater than or equal to the actual discounts of the purchaser, the purchaser will be added to G^*. Then, these two steps are repeated until no more $G^* \backslash \overline{G}^*$ buyers are added to G^*. Finally, there will be the calculation of the coalition price for each purchaser in coalition G. The algorithm for dividing the total discount of coalition G^* is shown in Figure 10.

Algorithm 1*: Coalition structure selection.*

Input: $G = \{b_1, b_2, \ldots, b_n\}$ is a set of buyers, R_b is the reservation price of buyer b_k in G, The unit price of the item can be represented by a descending function $P: a \rightarrow$ *real number* where $P(a)$ is a unit price that the seller would expect from selling a bundle of size *'a'* of the item t.

Output: G^* is a subset of buyers in G.

1. $G^* \leftarrow G$.

2. If $u(G^*) \geq 0$ then terminate with coalition structure G^* found when $u(G^*) = \sum_{b_k \in G^*} R_k - P(|G^*|) \times |G^*|$ and $P(|G^*|)$ is the coalition price of an item for the coalition G^*.

3. If $G^* \neq \emptyset$ then the buyer with the lowest reservation price in the coalition G^* is removed from G^*, and go to step 2; else terminate with no coalition structure found .

Figure 9 Algorithm 1: Structure selection of coalitions [59].

Algorithm 2: *Total discount division.*

Input: $G = \{b_1, b_2, \ldots, b_n\}$ is a set of buyers, G^* is the coalition found by using *Algorithm* 1, R_b is the reservation price of buyer b_k in the coalition G^*, $P(1)$ is the retail price of an item, $P(|G^*|)$ is the coalition price of an item for the coalition G^*.

Output: D_k is the actual discount of buyer b_k in coalition G^*, C_k is the coalition price of buyer b_k in coalition G^*.

1. $\bar{G}^* \leftarrow \emptyset, c_k = 0$ for $G - G^*$
2. $Flag \leftarrow True$.
3. $D_k \leftarrow \begin{cases} RD_k & (b_k \in \bar{G}^*) \\ \frac{(TD(G^*) - \sum_{b_k \in \bar{G}^*} RD_k) \times R_k}{\sum_{b_k \in G^* \setminus \bar{G}^*} R_k} & (b_k \in G^* \setminus \bar{G}^*) \end{cases}$

when the required minimum discount of buyer bk is defined as $RD_k = P(1) - R_k > 0$ and the total discount of coalition G is defined as $TD(G) = (P(1) - P(|C|)) \times |C|$.

4. Let $\Delta = \{b_k \in G^* \setminus \bar{G}^* : RD_k > D_k\}$.

   If $\Delta \neq \emptyset$ then $\bar{G}^* \leftarrow \bar{G}^* \cup \Delta$ and $Flag \leftarrow False$.

5. If $Flag = False$ then go to step 2.
6. $C_k \leftarrow P(1) - D_k$.

Figure 10 Algorithm 2: Division of the coalition's total discount [59].

5 Security Properties and Analysis

In this section, the correctness and the accountability properties are studied. The details are shown as follows.

5.1 Correctness

Buyers pay for their own coalition prices, and the ledger/blockchain collects the accurate amount of coalition prices. According to realistic coalition price

scenarios, there are two underlying assumptions. First, there is no intention for a buyer to pay more than his actual coalition prices. Second, others want no loss of buyers' coalition prices.

Let c_b be the actual amount of coalition prices to be charged by buyer b, and buyer b's actual payment for coalition prices is pay_b, which writes to a transaction after this scheme has been processed.

DEFINITION 1 (CORRECTNESS). *If the scheme needs no loss of coalition buyer prices and buyers have no intention of paying more than their coalition prices, then* $pay_b = c_b$.

Correctness of both the buyers and the ledger/blockchain are proven as follows.

1. By contradiction, this scheme forces each buyer to pay his real coalition price; that is, $pay_b = C_b$. Suppose that a buyer b has paid lower real coalition prices, or $pay_b < cost_b$.
2. The information of every step will be broadcasted. Therefore, it can detect such a situation and force the buyer to pay the rest.

THEOREM 1.1 The proposed coalition scheme guarantees accountability

In this scheme, a buyer cannot pay less because the consensus algorithm is processed in the consensus protocol.

5.2 Accountability

This property will detect malicious behavior. If a malicious action occurs, it can identify its originator.

DEFINITION 2 (ACCOUNTABILITY). *Let X'* $\subseteq$ X *be the attacks that currently occur in coalition price sessions during the implementation of this framework. For any* $\beta \in$ X', *our scheme is able to provide a set of evidence,* E' $\in$ P(E), *and there is a feature finding function:*

$$\text{P(E)} \times \text{X} \rightarrow \text{U} \textit{such that } \text{find } (\text{E}', \beta) = \text{attacker}(\beta).$$

The main theorem is used to show that the specified properties are met by our buyer coalition scheme.

THEOREM 2.1 The proposed coalition scheme guarantees correctness

THEOREM 2.2 The proposed coalition scheme guarantees accountability

Accountability. In this scheme, the set B is composed of the following misbehaviors:

- β_1: corrupt buyers write lower coalition price payment to transaction;
- β_2: malicious buyers deny paying coalition prices;
- β_3: the third party attaches wrong coalition prices to transaction;

The accountability is secured against the misbehaviors in B given the following conditions.

1. Assume $\alpha = (\beta_1, \text{b})$ happens (i.e., $pay_b < C_b$). For this case, b would be discovered by the Nakamoto consensus protocol.
2. Assume (β_2, b) happens. For this case, b would be discovered by the Nakamoto consensus protocol.

6 Discussion and Limitations

Blockchain and group signature alleviate the issue of buyer coalition's trust because the buyer coalition is formed through a decentralized public ledger. The current study's proposed algorithmic architecture protects customers' privacy within the alliance while ensuring that operations and organizations are both right and accountable. Furthermore, the proposed scheme allows the buyer to pay appropriately for the right coalition. In addition, the scheme is correct because the third party and blockchain collect an accurate sum of coalition rates from buyers and because it enforces transparency by being able to identify wrongdoers. Using an additional trusted blockchain function is observed in this theory. As a result, there is full trust in the blockchain network in the proposed scheme that the data obtained, such as reservation prices or coalition prices, are stored in all peer-to-peer nodes.

One significant drawback of the analysis is implementing a simplified case scenario to prevent unnecessary volume and presentation. Although this can be considered a limitation, this algorithm can accommodate more complex situations. Another limitation of this study was the absence of proof of concept, which can be demonstrated using a software simulation system. The current study does not provide any of these facilities, but focuses on the widespread logic and mechanism to establish trustful relationships. This evidence, however, sets out the future studies of the authors as discussed below.

7 Conclusion

This work suggested algorithmic architecture using blockchain technology for a novel buyer partnership scheme with trust. Neither of the proposed buyer coalition schemes discussed the trusting relationships in buyer coalitions, which is the significant gap in the current report's information because a lot of buyers might not be able to enter the coalitions without these trustful relationships. Therefore, a new trusting buyer coalition scheme using blockchain technology was proposed in this study. This suggested scheme used blockchain technology to create and maintain the trust mentioned above, and to achieve the trust objective. Mathematical notations include the suggested algorithmic architecture, which can then be translated into computerized implementation codes. Additionally, the discovered algorithm can be applied to mobile commerce applications. Future studies might focus on the production process and the review of criteria by the buyer coalition users.

Acknowledgment

The publication of this work was supported by Mae Fah Luang University.

References

[1] Blankenburg, B., R. K. Dash, S. D. Ramchurn, M. Klusch, and N. R. Jennings., 2005. Trusted Kernel-based Coalition Formation. In AAMAS '05 Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems, Utrecht, 989–996.

[2] Boongasame, L., Leung, H. F., Boonjing, V., & Chiu, D. K. (2009a, June). Forming buyer coalitions with bundles of items. In KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications (pp. 714–723). Springer, Berlin, Heidelberg.

[3] Boongasame, L., & Sukstrienwong, A. (2009b, September). Buyer coalitions with bundles of items by using genetic algorithm. In International Conference on Intelligent Computing (pp. 674–685). Springer, Berlin, Heidelberg.

[4] He, L., & Ioerger, T. R. (2004, July). Combining bundle search with buyer coalition formation in electronic markets: A distributed approach through negotiation. In AAMAS (Vol. 4).

[5] Li, C., Sycara, K., & Scheller-Wolf, A. (2010). Combinatorial coalition formation for multi-item group-buying with heterogeneous customers. Decision Support Systems, 49(1), 1–13.
[6] Indrawan, M., Kijthaweesinpoon, T., Srinivasan, B., & Sajeev, A. S. M. (2004, January). Coalition formation protocol for e-commerce. In International Conference on Intelligent Sensing and Information Processing, 2004. Proceedings of (pp. 403–408). IEEE.
[7] Hyodo, M., Matsuo, T., & Ito, T. (2003, June). An optimal coalition formation among buyer agents based on a genetic algorithm. In International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (pp. 759–767). Springer, Berlin, Heidelberg.
[8] Matsuo, T., Ito, T., & Shintani, T. (2004, July). A buyers integration support system in group buying. In Proceedings. IEEE International Conference on e-Commerce Technology, 2004. CEC 2004. (pp. 111–118). IEEE.
[9] Chen, J., Chen, X., & Song, X. (2002). Bidder's strategy under group-buying auction on the Internet. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 32(6), 680–690.
[10] Tsvetovat, M., Sycara, K., Chen, Y., & Ying, J. (2000, June). Customer coalitions in electronic markets. In International Workshop on Agent-Mediated Electronic Commerce (pp. 121–138). Springer, Berlin, Heidelberg.
[11] Anand, K. S., & Aron, R. (2003). Group buying on the web: A comparison of price-discovery mechanisms. Management Science, 49(11), 1546–1562.
[12] Chen, J., Chen, X., Kauffman, R. J., & Song, X. (2009). Should we collude? Analyzing the benefits of bidder cooperation in online group-buying auctions. Electronic Commerce Research and Applications, 8(4), 191–202.
[13] Li, C., & Sycara, K. (2002, July). Algorithm for combinatorial coalition formation and payoff division in an electronic marketplace. In Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1 (pp. 120–127).
[14] Li, C., Rajan, U., Chawla, S., & Sycara, K. (2003, September). Mechanisms for coalition formation and cost sharing in an electronic marketplace. In Proceedings of the 5th international conference on Electronic commerce (pp. 68–77).

[15] Matsuo, T., Ito, T., & Shintani, T. (2005, April). A volume discount-based allocation mechanism in group buying. In International Workshop on Data Engineering Issues in E-Commerce (pp. 59–67). IEEE.

[16] Kraus, S., Shehory, O., & Taase, G. (2003, July). Coalition formation with uncertain heterogeneous information. In Proceedings of the second international joint conference on Autonomous agents and multiagent systems (pp. 1–8).

[17] Kraus, S., Shehory, O., & Taase, G. (2004, July). The advantages of compromising in coalition formation with incomplete information. In Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems-Volume 2 (pp. 588–595).

[18] Breban, S., and J. Vassileva., 2002. A Coalition Formation Mechanism Based on Inter-agent Trust Relationships. In Proceedings of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1, New York: 306–307.

[19] Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications (pp. 1-307). Heidelberg: Springer.

[20] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

[21] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375.

[22] Dujak, D., & Sajter, D. (2019). Blockchain applications in supply chain. In SMART supply network (pp. 21–46). Springer, Cham.

[23] Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3.

[24] Chen, J., Chen, X., & Song, X. (2002). Bidder's strategy under group-buying auction on the Internet. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 32(6), 680–690.

[25] Chen, J., Kauffman, R. J., Liu, Y., & Song, X. (2010). Segmenting uncertain demand in group-buying auctions. Electronic Commerce Research and Applications, 9(2), 126–147.

[26] Tsvetovat, M., Sycara, K., Chen, Y., & Ying, J. (2000, June). Customer coalitions in electronic markets. In International Workshop on Agent-Mediated Electronic Commerce (pp. 121–138). Springer, Berlin, Heidelberg.

[27] He, L., and T. Ioerger., 2005. Combining Bundle Search with Buyer Coalition Formation in Electronic Markets: A Distributed Approach through Explicit Negotiation. Electronic Commerce Research and Applications 4(4): 329–344.

[28] Boongasame, L., F. Daneshgar., 2016. An awareness-based meta-mechanism for e-commerce buyer coalitions. Information Systems Frontiers 18 (3): 529–540.

[29] Boongasame, L., P. Temdee, and F. Daneshgar., 2012. Forming Buyer Coalition Scheme with Connection of a Coalition Leader. Journal of Theoretical and Applied Electronic Commerce Research 7: 17–18.

[30] McKnight, D. H., and N. L. Chervany., 2002a. What Trust Means in e-commerce Customer Relationships: An Interdisciplinary Conceptual Typology. International Journal of Electronic Commerce 6(2): 35–59.

[31] Xu, X., Lu, Q., Liu, Y., Zhu, L., Yao, H., & Vasilakos, A. V. (2019). Designing blockchain-based applications a case study for imported product traceability. Future Generation Computer Systems, 92, 399–406.

[32] Tripoli, M., & Schmidhuber, J. (2018). Emerging Opportunities for the Application of Blockchain in the Agri-food Industry. FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA, 3.

[33] Prashar, D., Jha, N., Jha, S., Lee, Y., & Joshi, G. P. (2020). Blockchain-Based Traceability and Visibility for Agricultural Products: A Decentralized Way of Ensuring Food Safety in India. Sustainability, 12(8), 3497.

[34] Zhu, Y., Lv, C., Zeng, Z., Wang, J., & Pei, B. (2019, June). Blockchain-based Decentralized Storage Scheme. In Journal of Physics: Conference Series, 1237(4), p. 042008. IOP Publishing.

[35] Kumar, R., & Tripathi, R. (2020). Blockchain-Based Framework for Data Storage in Peer-to-Peer Scheme Using Interplanetary File System. In Handbook of Research on Blockchain Technology, pp. 35–59. Academic Press.

[36] Balaji, S., Mohan, V., Soundarya. (2017). Secure and decentralized file transfer application using blockchain. International Journal of Current Engineering and Scientific Research (IJCESR), 4(4), pp. 169–175.

[37] Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health informatics journal, 25(4), 1398–1411.

[38] Dinesh Kumar K, Manoj Kumar D.S, Anandh R. (2020). Blockchain Technology In Food Supply Chain Security. International Journal of Scientific & Technology Research, 9(1), pp. 3446–3450.

[39] Kumari, S. & Farheen, S., (2020). Blockchain based Data Security for Financial Transaction System. 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp. 829–833, doi: 10.1109/ICICCS48265.2020.9121108.

[40] Javed, M. U., Rehman, M., Javaid, N., Aldegheishem, A., Alrajeh, N., & Tahir, M. (2020). Blockchain-Based Secure Data Storage for Distributed Vehicular Networks. Applied Sciences, 10(6), 2011.

[41] Benítez-Martínez, F. L., Hurtado-Torres, M. V., & Romero-Frías, E. (2021). A neural blockchain for a tokenizable e-Participation model. Neurocomputing, 423, 703–712.

[42] Khan, F. B. (2019). The game of votes: Visual media politics and elections in the digital era. SAGE Publishing India.

[43] Krishnan, S., Balas, V. E., Julie, E. G., Yesudhas, H. R., Balaji, S., & Kumar, R. (Eds.). (2020). Handbook of research on blockchain technology. Academic Press.

[44] Leelasantitham, A. (2020). A Business Model Guideline of Electricity Utility Systems Based on Blockchain Technology in Thailand: A Case Study of Consumers, Prosumers and SMEs. Wireless Personal Communications, 115(4), 3123–3136.

[45] Jamil, F., Iqbal, N., Ahmad, S., & Kim, D. (2021). Peer-to-Peer Energy Trading Mechanism based on Blockchain and Machine Learning for Sustainable Electrical Power Supply in Smart Grid. IEEE Access, 9, 39193–39217.

[46] Thukral, M. K. (2021). Emergence of blockchain-technology application in peer-to-peer electrical-energy trading: a review. Clean Energy, 5(1), 104–123.

[47] Jintapitak, M., Ansari, M. A., Kamyod, C., Singkhamfu, W., Kamthe, N. S., & Temdee, P. (2019, November). Blockchain Eco-System for Thai Insect Industry: A Smart Contract Conceptual Framework. In 2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC) (pp. 1–4). IEEE.

[48] Leduc, G., Kubler, S., & Georges, J. P. (2021). Innovative blockchain-based farming marketplace and smart contract performance evaluation. Journal of Cleaner Production, 306, 127055.

[49] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.
[50] De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., & Ueyama, J. (2020). A survey of blockchain-based strategies for healthcare. ACM Computing Surveys (CSUR), 53(2), 1–27.
[51] Marwan, M., Kartit, A., & Ouahmane, H. (2018). A cloud-based framework to secure medical image processing. Journal of Mobile Multimedia, 14(3), 319–344.
[52] Klemperer, P. (1999). Auction theory: A guide to the literature. Journal of economic surveys, 13(3), 227–286.
[53] McKnight, D. H., V. Choudhury, and C. Kacmar., 2002b. Developing and Validating Trust Measures for e-commerce: An Integrative Typology. Information Systems Research 13 (3): 334–359.
[54] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644–654.
[55] Chaum, D., and E. V. Heyst., 1992. Group Signatures, Vol. 547: 257–265. Berlin: Springer.
[56] Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. IEEE Communications Surveys & Tutorials, 22(2), 1432–1465.
[57] Ziogou C., D. Ipsakis, P. Seferlis, S. Bezergianni, S. Papadopoulou, S. Voutetakis S, 2013, Optimal production of renewable hydrogen based on an efficient energy management strategy, Energy, 55, 58–67.
[58] Chen, X., G. Lenzini, S. Mauw, and J. Pang., 2010. A Group Signature Based Electronic Toll Pricing System. In SAC'12, Riva del Garda, Italy.
[59] Boongasame, L., 2006. The Price Negotiation Scheme for Forming Community Buyer Coalitions. PhD dissertation, Department of Electrical and Computer Engineering, King Mongkut's University of Technology Thonburi.

Biographies

Laor Boongasame is a lecturer in the School of Science, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand. She obtained her Ph.D. in Computer Engineering from King Mongkut's University of Technology Thonburi, Thailand. Her research interests involve buyer coalitions, n-person game theory, and investment. She has published several research papers in internationally refereed journals and has presented several papers at several international conferences. She can be reached at laor.bo@kmitl.ac.th

Supansa Chaising received the bachelor's degree in accounting, the master's degree and the doctoral degree in computer engineering from Mae Fah Luang University, Thailand. She is currently an instructor in Department of Information Technology, The International College at Payap University, Thailand. Her research interests are artificial intelligence, machine learning, and business information systems.

Punnarumol Temdee received B. Eng. in Electronic and Telecommunication Engineering, M. Eng in Electrical Engineering, and Ph.D. in Electrical and Computer Engineering from King Mongkut's University of Technology Thonburi. She is currently a lecturer at School of Information Technology, Mae Fah Luang University, Thailand. Her research expertise is artificial intelligence-based application, context-aware computing, and pattern classification.