applied sciences

MDPI

Article

A Privacy-Enabled, Blockchain-Based Smart Marketplace

Bello Musa Yakubu [1,*], Majid Iqbal Khan [2], Abid Khan [3], Adeel Anjum [4], Madiha Haider Syed [4] and Semeen Rehman [5,*]

[1] Department of Mathematics and Computer Science, Chulalongkorn University, Bangkok 10330, Thailand
[2] Department of Computer Science, COMSATS University Islamabad, Islamabad 45550, Pakistan
[3] School of Computing and Engineering, College of Science and Engineering, University of Derby, Derby DE22 1GB, UK
[4] Institute of Information Technology, Quaid i Azam University, Islamabad 15320, Pakistan
[5] Institute of Computer Technology, Technische Universitat Wien (TU Wien), 1040 Wien, Austria
* Correspondence: bellomyakubu.cui@gmail.com (B.M.Y.); semeen.rehman@tuwien.ac.at (S.R.)

Abstract: Advancements in sensor-enabled devices led to the emergence of resource trading models for smart communities, such as the smart marketplace (SMP). Most of the proposed SMP architectures are based on blockchain technology, which has a public ledger to achieve transparency. Consequently, safeguarding the participant's anonymity, untraceability, and transactional data privacy during trading becomes a challenging task. Most of the existing solutions to achieve anonymity are based on multiple account mapping, which is prone to identity-based attacks, and cryptographic techniques are used to achieve transactional data privacy, which often has a high computational overhead. In this work, we propose a lightweight privacy-enabled message exchange mechanism to accomplish our privacy goals in a blockchain-based SMP. Evaluation of the scheme was conducted to measure its resilience toward safeguarding participants' anonymity, untraceability, and transactional data privacy during trading cycles. Statistical game theory-based security analysis and simulation based performance analysis of the proposed scheme showed that it achieved the desired privacy goals with a low computational overhead compared with existing state-of-the-art schemes.

Keywords: anonymity; transactional data privacy; IoT; Ethereum; smart marketplace

check for updates

Citation: Yakubu, B.M.; Khan, M.I.; Khan, A.; Anjum, A.; Syed, M.H.; Rehman, S. A Privacy Enabled, Blockchain-Based Smart Marketplace. *Appl. Sci.* **2023**, *13*, 2914. https://doi.org/10.3390/app13052914

Academic Editor: Dimitris Mourtzis

Received: 26 January 2023
Revised: 16 February 2023
Accepted: 20 February 2023
Published: 24 February 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Increasing demand for resources in smart communities has prompted researchers to develop resource trading solutions in the form of the SMP [1,2]. The SMP is the result of advancements in network innovation, using sensor-enabled devices in smart homes to facilitate trade and the exchange of resources such as water, internet bandwidth and energy among the participants of a smart community. Most of the recently proposed SMP architectures are based on blockchain technology [3,4]. The blockchain is based on a public ledger and communication transparency between participants, which allow any participant to access information regarding transaction history, events and actions taking place in the SMP. Due to this very feature of the blockchain, ensuring privacy preservation of the participants becomes a challenging task, as participants may suffer from disclosure of confidential information, such as a participant's identity and details of the executed transactions [5].

Privacy parameters with respect to the participant are classified into two categories: (1) preservation of the participant's anonymity and untraceability, making the participant's identity unknown and untraceable, and (2) preservation of transactional data by hiding the transaction details of the participant [3–5]. Various techniques have been proposed to achieve these privacy parameters in an SMP that includes the use of multiple accounts and a Merkle tree [6,7] to achieve anonymity and untraceability for the participants. Cryptographic approaches such as the Elliptic Curve Digital Signatures Algorithm (ECDSA)

and elliptic curve cryptography (ECC) have been used to provide transactional data privacy [5,6,8]. The Bitmessage [9] method of decentralized peer-to-peer (P2P) message authentication and delivery based on the proof-of-work (PoW) consensus algorithm was adopted by many approaches, such as those in [6,10], to provide anonymity in a trustless network by broadcasting encrypted messages in messaging streams.

With respect to the use of the above approaches to accomplish the desired privacy parameters in a blockchain-based SMP, the following issues and limitations have been identified:

- The use of multiple accounts and Merkle trees, as in [6,7], is not very successful against blockchain analysis and other similar techniques [1,2,11]. Thus, they can be used to link multiple accounts of a participant to infer the participant's identity. On the other hand, the implementation of a Merkle tree in a blockchain-based network, such as the Ethereum network, may inevitably require a large-scale computing resource [12].
- Cryptographic approaches, such as the ECDSA and ECC [5,6,8], utilizes time-consuming procedures, such as bilinear pairings [13,14]. The process may lead to high computational and storage overheads, thus posing practical problems due to the resource constraint nature of the smart gateway in smart homes [15–17].
- Instead of using an encryption method that often makes the content of the encrypted blocks mutually dependent, Bitmessage encrypts each block individually. Through this, the adversary will be able to rearrange the message blocks in such a way that the recipient can interpret it as a legitimate message [18]. With this, the adversary can infer the transactional data stored in the blocks as well as identify the participants involved in the transactions.

The situation is further aggravated when one takes into account the type of trading mechanism used in the SMP. The trading approaches may allow a participant to have only a single (one-to-one) or multiple (one-to-many) simultaneous transactions. The objective of this work is to ensure the anonymity and untraceability of the participant and provide transactional data privacy under a one-to-many trading model. To achieve these goals, a novel lightweight scheme is presented that utilizes a pair of public/private IDs with anonymous messaging streams. Security analysis and experimental evaluation of the proposed solution is performed to evaluate and compare it against existing state-of-the-art schemes.

Contributions: The following are the contributions of this paper:

- A protocol is presented to ensure the participant's anonymity and untraceability during one-to-many trading in the SMP, using public/private pairs of communicating sessional IDs.
- A protocol is also presented to ensure privacy preservation of the transactional data of the participants during one-to-many trading in the SMP at a reduced computational overhead.
- Our results show that the proposed system is more resilient against identity-based attacks such as blockchain analysis attacks and achieves a lower probability of success of the adversary compared with that in [6,7] with a reduced computational overhead.

Organization of the Paper: The rest of this paper is organized as follows. Section 2 provides an overview of the related work. In Section 3, we present the system model. Section 4 describes the proposed security protocol. Section 5 discusses the security analysis. Section 6 explains the experimental analysis and results, and Section 7 presents the conclusions.

2. Related Work

Recently the use of the blockchain for the development of P2P resource trading models in SMPs has attracted huge attention [1]. Several approaches, such as those in [19–29], were proposed to realize participants' anonymity and transactional data privacy in SMPs. An account mapping technique was used in [21] to prevent attackers from directly accessing transactional data. In this method, the characteristics of both active and inactive users' accounts can be effectively obscured by creating multiple accounts. Similarly, in [22], it was

proposed to protect the privacy of participants by dividing them into various groups. Then, a miner is chosen among the group members to collect data from the group and add them into the community's private blockchain. This process protects the participant's data from leaking to other participants in the network. However, recent works [1,2,11] have shown that, using a detailed analysis process [11], multiple public addresses and accounts can be connected to infer and expose the identity of the participants in blockchain-based networks. One such method is known as blockchain analysis, where transactions, addresses and entity graphs are used to expose the true identites of blockchain users [1].

Some techniques [6,8,30] use elliptic curve-based security mechanisms, such as ECC and the ECDSA, to preserve the privacy of participants and enable them to anonymously trade with each other. These schemes protect participants against attacks such as address reuse, Sybil, inferential and collusive attacks. However, the techniques presented in [6,8] can be subjected to 51 percent attacks, high latency due to a long block generation time and other mining issues. In another approach [7], a participant, such as a resource buyer, uses digital currencies to generate multiple accounts and preserve the mapping information to avoid tracking. It also involves the use of a Merkle tree [12] to create a large pool of key pairs and achieve high anonymity. However, this approach may be prone to a blockchain analysis attack, and the implementation of Merkle trees in a blockchain-based network, such as the Ethereum network, can be computationally costly, which can slow down the execution of trading transactions. Therefore, there is a need to come up with a more scalable solution that will provide user anonymity, untraceability and transactional data privacy in the resource trading environment of SMPs. Table 1 summarizes some of the most recent and relevant research conducted in this domain.

Table 1. A Summary of the blockchain-based approaches.

Technique	Objectives	Attacks Model	Analysis
ECC, ECDSA and multi-address [6,8,30]	To protect identity and privacy of participants	Inferential attack, identity and data transaction disclosure	Provides participants anonymity and data privacy. Prone to Sybil attack, high computational overhead and blockchain analysis.
Merkle tree and multi-account [7]	To preserve participants' anonymity and untraceability	Inferential attack, identity and data transaction disclosure	Provides participants anonymity and untraceability. Prone to Sybil and blockchain analysis attacks, account or address reuse and high computational overhead.
Multi-account or address [19,20]	To achieve participants' anonymity and transaction privacy	Inferential attack, identity linking attacks and double spending	Provides trading transaction monitoring and participant privacy. Prone to blockchain analysis and Sybil attacks.
Multi-account mapping technique [21]	To achieve transactional data privacy	Inferential attack and identity and data transaction disclosure	Provides participants anonymity. Prone to account or address reuse and blockchain analysis.
Multi-account grouping [22]	To protect the privacy of participants	Identity linking attacks and address reuse	Provides participants privacy. Prone to Sybil and double spending attack and blockchain analysis.

3. System Model

This section discusses our system models, including the network model and trading model. Moreover, it presents the security requirements and the threat model.

3.1. Network Model

The SMP has a temper-proof smart gateway, referred to here as the Smart Market Gateway (SmGW), that is connected with several participating smart homes within the smart community through their respective temper-proof sensor-enabled smart gateways. Each smart home gateway in the SMP is presumed to be registered and authenticated as a trusted member via the SmGW. A smart home in the SMP can take part in resource trading

either as a resource provider (ProGW), resource requester (ReqGW) or both, as depicted in Figure 1. The system is based on private Ethereum blockchain technology accessible by the connected smart gateways, which are presumed to be computationally capable. Thus, it is assumed that all SMP participants have direct access to Ethereum smart contracts through the network, and each participant uses separate Ethereum accounts (EAs) to participate in the SMP. As a result, they can be identified by their Ethereum addresses (public keys) in the network. In addition, all participants have direct access to the public ledger of the blockchain, where all transactions are recorded and can be retrieved.

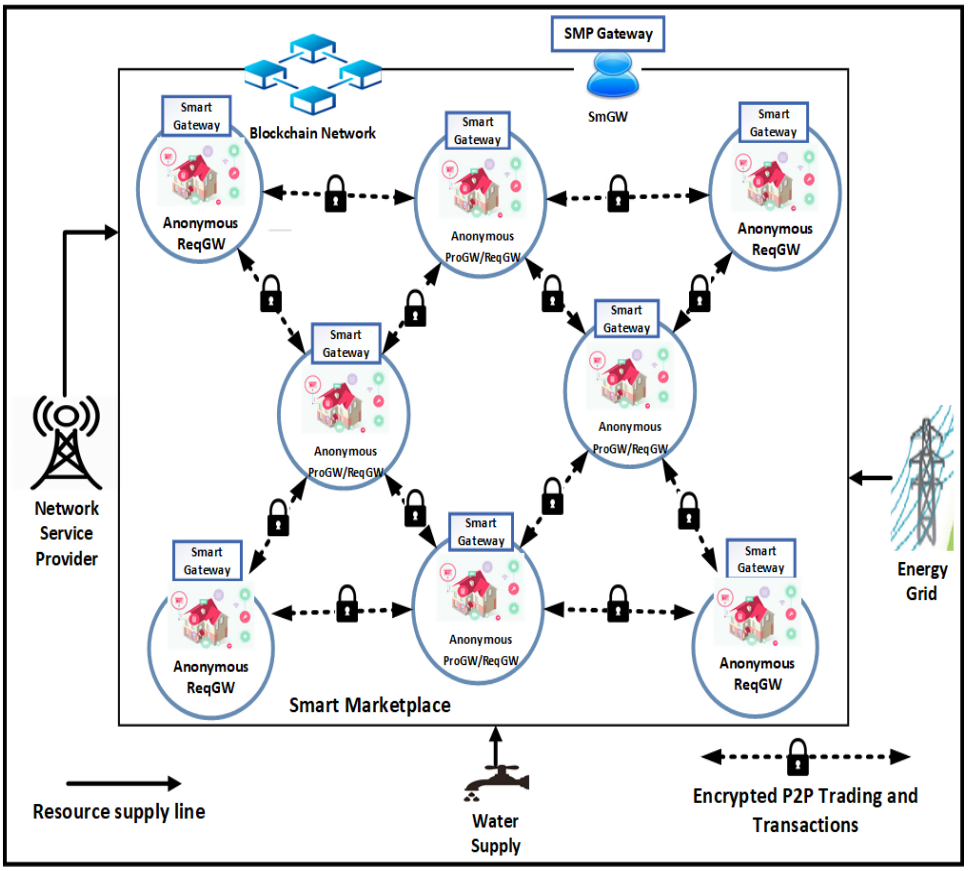


Figure 1. System model.

3.2. Trading Model

In Figure 1, three entities are involved in each transaction: the requester gateway (ReqGW), provider gateway (ProGW) and Smart Market Gateway (SmGW). $ProGW_j$, being the resource supplier (seller), first feeds the amount of the resource (e.g., energy) it is willing to sell out to the SMP resource chamber, such as the smart grid (energy grid), via a transmission channel. $ProGW_j$ then broadcasts the offerings anonymously to the blockchain auction board, also including the price, volume (amount), unit and type of the resource to be sold. $ReqGW_i$, being the potential resource requester (buyer), receives the copy of $ProGW_j$'s broadcasted message. If $ReqGW_i$ selects $ProGW_j$ as the potential supplier, then it sends a trading negotiation message to the respective $ProGW_j$ to initiate the trading negotiation process. After the successful negotiation, $ReqGW_i$ releases the agreed price, and the resource is released by $ProGW_j$, thereby completing the trading activity.

3.3. Privacy Requirements

In the context of the presented network and trading model, it is desired that the following two requirements regarding a participant's privacy should be accomplished:

- *Participant's anonymity and untraceability:* Protect the identities of participants and make them untraceable in the SMP. Their identities should be protected from identity-related attacks, such as address reuse, Sybil and blockchain analysis attacks during trading in the SMP.
- *Transactional data privacy:* Ensure protection against transactional data privacy attacks, such as inferential attacks and data leakage.

3.4. Threat Model

In this work, we consider the following features for the adversary $\mathcal{A}$:

- The adversary $\mathcal{A}$ has the ability to influence the means of communication of the SMP and to intercept all messages transmitted between the smart gateways.
- The adversary $\mathcal{A}$ has the ability to capture all of the session IDs in the SMP.
- $\mathcal{A}$ has the ability to launch identity-related attacks and transactional data privacy attacks.
- It was assumed that the smart gateways are temper-proof and therefore cannot be compromised.
- We assumed that the adversary cannot compromise the blockchain.

4. Anonymity, Untraceability and Transactional Data Privacy (AUT) Protocol

A secure protocol to achieve a participant's anonymity, untraceability and transactional data privacy in the SMP is presented in this section. Note that the anonymity, untraceability and transactional data privacy solutions in this work were provided during trading activities between participants. Thus, the protocol ensured the desired privacy parameters independent of the type of trading model (one-to-one or one-to-many) used in the SMP. In order to establish trusted message streams among the participants, a lightweight Bitmessage (L-Bitmessage) technique was adopted. This technique uses cryptographic proof-of-authority (PoA) and the sped up Rivest–Shamir–Adleman (RSA) cryptosystem along with a Chinese reminder theorem (CRT) for the encryption or decryption processes. The RSA cryptosystem is a commonly used public key cryptosystem for secure data transfers [31,32]. Additionally, it is one of the oldest. The proposed protocol is presented in Algorithm 1, and the workflow is depicted in Figure 2. Similarly, Table 2 provides a brief description of the important notations used in this work.

Table 2. Notations.

Symbols	Definitions
ACM_{track}	Actual ID correlation matrix
$\mathcal{A}$	Adversary or attacker
$\mathcal{A}^{\tau}$	Attacker who reacts to all game difficulties with statistical inferences
$\mathcal{C}$	A challenger who knows the correct assignment of addresses (public keys) to blockchain users
δ	An arbitrary bit chosen by $\mathcal{C}$
E_{track}	Consists of extra information which can be extracted from the SMP by $\mathcal{A}$
$Success_{\mathcal{A}}$	Extra success recorded by $\mathcal{A}$ against $\mathcal{A}^{\tau}$
$Failure_{\mathcal{A}}$	Extra failure recorded by $\mathcal{A}$ against $\mathcal{A}^{\tau}$
n_p	Number of participants in SMP
n_T	Number of transactions which occurred during time frame Δ,
$\mathcal{P}$	Participant in the SMP
Δ,	Period of time for SMP trading
e/d	Public or private IDs
$\{\alpha_0, \alpha_1, ...\alpha_n\}$	Set of IDs in the SMP
$Suc_{\mathcal{A}}$	Success of $\mathcal{A}$ in the game
ρ	The amount of running time of the attacker $\mathcal{A}$
γ	The fraction of IDs that cannot be correlated with other IDs
ω_i	The request message

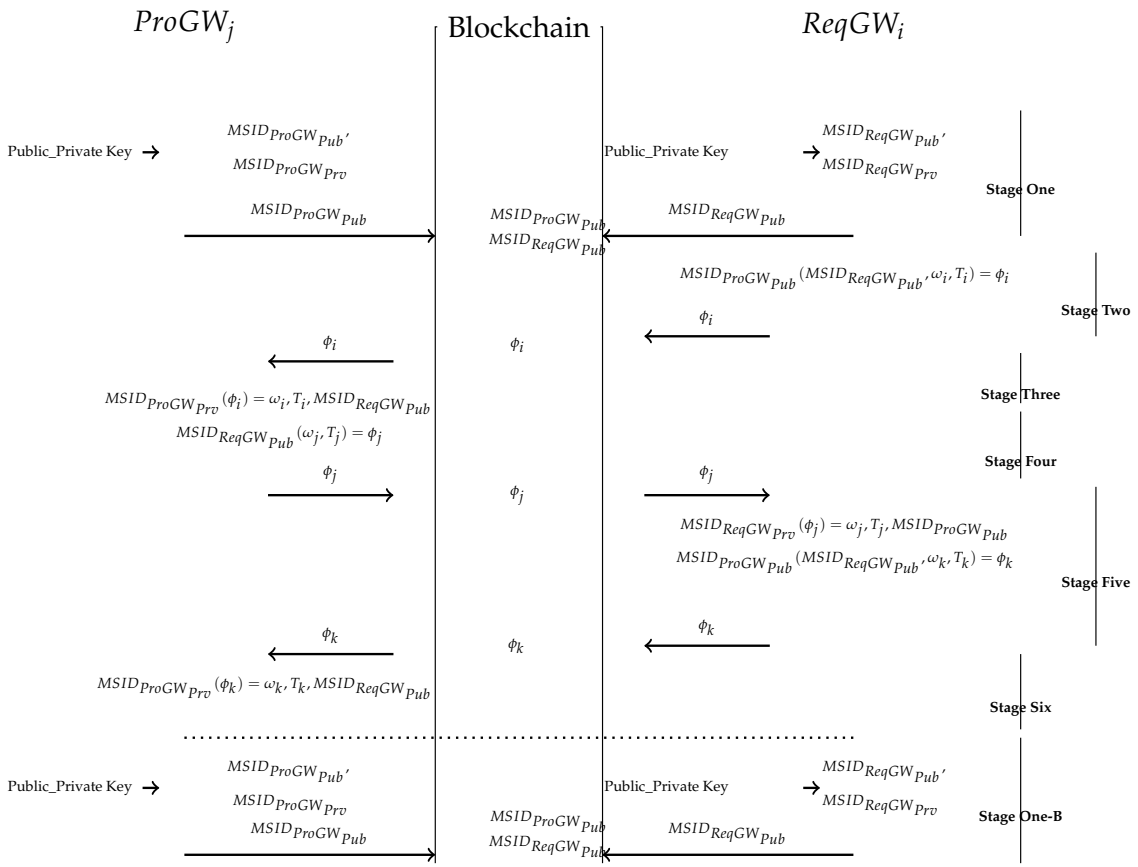


Figure 2. Proposed Anonymity and transactional data privacy protection protocol operation flow.

During the first stage in Figure 2, both $ProGW_j$ and $ReqGW_i$ create new pairs of session IDs $(MSID_{ProGW_{Pub}}, MSID_{ProGW_{Prv}})$ and $(MSID_{ReqGW_{Pub}}, MSID_{ReqGW_{Prv}})$, respectively, from their original pairs of public and private keys at the beginning of each trading activity in the system. The IDs are used to represent $ProGW_j$ and $ReqGW_i$ during trading activities. The IDs are sessional, and therefore, they are discarded after one complete trading transaction session. Both the *ProGW* and *ReqGW* public pair session IDs are generally chosen to be of relatively small prime values and of low hamming weights to ensure speeding up of the encryption process with a negligible computing overhead. Thus, $ProGW_j$ and $ReqGW_i$ remain anonymous under the pseudonyms of $MSID_{ProGw_{Pub}}$ and $MSID_{ReqGw_{Pub}}$, respectively, as well as untraceable without revealing their true identities (public keys). As depicted from line 1 to 13 of Algorithm 1, $ProGW_j$ sends a transaction ($T_{Broadcast}$) to broadcast its bids anonymously in the auction board as in Equation (1), which also includes $ProGW_j$'s public ID $(MSID_{ProGw_{Pub}})$, the block timestamp and the nonce:

$$T_{Broadcast} = MSID_{ProGw_{Pub}} \parallel Type \parallel Volume \parallel Price \parallel Timestamp \parallel Nonce \parallel Unit \quad (1)$$

In the second stage of Figure 2 and from line 14 to 18 in Algorithm 1, $ReqGW_i$ selects $ProGW_j$'s ID as the potential supplier and then encrypts a negotiation message using the chosen public ID of the potential $ProGW_j$ before broadcasting it anonymously in the blockchain network. This is achieved by encrypting the message with $ProGW_j$'s ID $(MSID_{ProGw_{Pub}})$ as follows:

$$MSID_{ProGW_{Pub}}(MSID_{ReqGW_{Pub}}, \omega_i, T_i) = \phi_i \quad (2)$$

where ω_i is the request message, T_i is the block timestamp and $MSID_{ReqGW_{Pub}}$ is $ReqGW_i$'s public ID. $ReqGW_i$'s identity remains anonymous behind a pseudonym $MSID_{ReqGW_{Pub}}$. However, its important to note that each time a message is broadcasted in the system, a validating authority (node) validates the message and adds it to the blockchain based on the proof-of-authority (PoA) consensus algorithm. With this, the encrypted message is published in the blockchain network, where all participant nodes will receive a copy of the package. In the third stage of Figure 2 and line 20 in Algorithm 1, only $ProGW_j$, which has the right private ID, will be able to decrypt the message:

$$MSID_{ProGw_{Prv}}(\phi_i) = \omega_i, T_i, MSID_{ReqGw_{Pub}} \tag{3}$$

Algorithm 1: Proposed anonymity and transactional data privacy protection protocol.

Input: Read the value:
$MSID_{pub_{ProGW_{Pub}}} \leftarrow hash(Public_Key_{ProGW})$
$MSID_{pub_{ProGW_{Prv}}} \leftarrow hash(Private_Key_{ProGW})$
$MSID_{pub_{ReqGW_{Pub}}} \leftarrow hash(Public_Key_{ReqGW})$
$MSID_{pub_{ReqGW_{Prv}}} \leftarrow hash(Private_Key_{ReqGW})$
Output: $Payment_{Broadcast}$, $Release_{Broadcast}$

1 **Function** $T_{Broadcast}(T(B))$**:**
2 $\mathcal{P} \leftarrow$ Participant
3 **if** $(\mathcal{P} = ProGW)$ **then**
4 $Type \leftarrow$ Type of *resource*;
5 $Volume \leftarrow$ Amount of *resource*;
6 $Price \leftarrow$ Price of *resource*;
7 $Unit \leftarrow$ Unit of *resource*;
8 Compute resource tender $T(R)$;
9 $T(R) \leftarrow (Type, Volume, Price, Unit)$;
10 $T_{Broadcast} \leftarrow \{MSID_{ProGW_{Pub}}, T(R), Timestamp\}$
11 **else**
12 $T_{Broadcast} \leftarrow MSID_{ReqGW_{Pub}}$
13 **end**
14 **Function** `Negotiation(`NG`)`**:**
15 Compute negotiation message ω_i;
16 $\phi_i \leftarrow$ Encrypt $\{MSID_{ReqGW_{Pub}}, \omega_i, T_i\}$;
17 $NG_{Broadcast} \leftarrow \phi_i$
18 **Function** `Acknowledgement(`ACK`)`**:**
19 Decrypt ϕ_i;
20 Compute acknowledgement message ω_j;
21 $\phi_j \leftarrow$ Encrypt $\{MSID_{ProGW_{Pub}}, \omega_j, T_j\}$;
22 $ACK_{Broadcast} \leftarrow \phi_j$
23 **Function** `Payment_Details(`PAY`)`**:**
24 Decrypt ϕ_j;
25 Compute Payment message ω_k;
26 $\phi_k \leftarrow$ Encrypt $\{MSID_{ReqGW_{Pub}}, \omega_k, T_k\}$;
27 $Payment_{Broadcast} \leftarrow \phi_k$
28 **Function** `Resource_Release(`RR`)`**:**
29 Decrypt ϕ_k;
30 Resource Released!
31 Compute Release message ω_z;
32 $\phi_z \leftarrow$ Encrypt $\{MSID_{ProGW_{Pub}}, \omega_z, T_z\}$;
33 $Release_{Broadcast} \leftarrow \phi_z$

In the fourth through sixth stage of Figure 2 and from line 21 to 37 of Algorithm 1, acknowledgement reply and payment messages are encrypted and decrypted accordingly to ensure speedy transmission of transactional messages in a secure and private manner at both sides of $ProGW_j$ and $ReqGW_i$ with a relatively low overhead until the trading activities are concluded. A new trading activity begins again with both $ProGW_j$ and $ReqGW_i$, creating new IDs from their public and private keys as depicted in stage one-B in Figure 2, which marks the beginning of the next trading session.

5. Security Analysis

Motivated by [32], blockchain-based game theory has been developed, comprising an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ in order to evaluate participant $\mathcal{P}$'s anonymity and untraceability. It is assumed that $\mathcal{C}$ knows the assigned addresses (public keys) of the blockchain users. The adversary $\mathcal{A}$ chooses an ID α_0 from the set of public pairs of the session IDs that were used in the SMP within a given time frame Δ, for which the adversary has no prior knowledge (conveyed in $\rho_{\mathcal{A}}$), and submits it to $\mathcal{C}$. Then, $\mathcal{C}$ chooses an arbitrary bit δ evenly. If $\delta = 1$, then $\mathcal{C}$ selects another ID α_1 arbitrarily from the SMP, where α_0 and α_1 belong to the same participant; otherwise, $\mathcal{C}$ arbitrarily chooses α_1 so that the two IDs belong to different participants. $\mathcal{C}$ directs $\{\alpha_0, \alpha_1\}$ to $\mathcal{A}$, which replies with his or her estimate $\delta^{'}$ for whether the two IDs are owned by the same participant. $\mathcal{A}$ wins the game if he or she responds appropriately (i.e., $\delta = \delta^{'}$).

5.1. Anonymity and Untraceability

Proposition 1. *The system achieves (preserves) $\mathcal{P}$'s anonymity and untraceability if for an adversary $\mathcal{A}$ and $\forall\{\alpha_0, \alpha_1\}$, in a probabilistic polynomial time, $\mathcal{A}$ has only at most an insignificant advantage over $\mathcal{A}^{\tau}$ to win; that is, this is true if*

$$\begin{aligned} Prob[\delta^{'} \leftarrow \mathcal{A}(SMP, \rho_{\mathcal{A}}, \alpha_0, \alpha_1) : \delta = \delta^{'}] - \\ Prob[\delta^{'} \leftarrow \mathcal{A}^{\tau}(\rho_{\mathcal{A}}, \alpha_0, \alpha_1) : \delta = \delta^{'}] \leq \varepsilon, \end{aligned} \tag{4}$$

where $\mathcal{A}^{\tau}$ is an adversary that reacts to all game difficulties with statistical inferences and ε is the difference in probabilities for the adversary $\mathcal{A}$, which is insignificant with respect to the security parameter ρ.

Proof. The proposed approach leverages the E-Bitmessage process during the course of communication in the SMP. Thus, the pair of session IDs is changed every time a session starts, therefore being used once and discarded. Hence, this makes it to almost impossible for $\mathcal{A}$ to reply with a correct estimate $\delta^{'}$. As a result, $\mathcal{A}$ has no or a less significant advantage over $\mathcal{A}^{\tau}$ to win the game. Thus, changing the session IDs for each connection improves the security in terms of perfect forward secrecy [10]. This implies that even if the private pair of the session IDs gets stolen by any means, such as correlation of the public pair of the session IDs in the SMP, not only are past communications still secure, but all following communications will also be secure. This feature strengthens and ensures transactional data privacy in the system.

All pairs of IDs only last for one trading session. However, encryption always needs the public key of the recipient, as well as decryption always needing the decryptor's private key. Unlike the public/private pairs of the session IDs, the original private/public key pairs are never dropped. Thus, even if the adversary is able to obtain one single ID out of the communication, it will neither be able to read messages from the past nor upcoming messages at a probabilistic polynomial time. □

Theorem 1. *If anonymity and untraceability are achieved (preserved) for a given participant $\mathcal{P}$, then it is presumed that the adversary $\mathcal{A}$ cannot be able to launch any identity-related attacks.*

Proof. (*By contradiction*) Assuming that $\mathcal{A}$ is able to launch any of the aforementioned attacks even when the participants are anonymous and untraceable, this implies that for all adversaries $\mathcal{A}$ and $\forall\{\alpha_0\}$, $\mathcal{A}$ has a significant advantage over $\mathcal{A}^\tau$ to win the game at a probabilistic polynomial time, even though the system has satisfied transactional data privacy, anonymity and untraceability for the participant $\mathcal{P}$. This statement contradicts Proposition 1. Hence, Theorem 1 holds. □

Theorem 2. *The participants' anonymity and untraceability offered by the proposed blockchain-based approach can be realized by measuring the degree to which the public pair of session IDs in the SMP can be linked to a particular address (public key) of a given participant.*

Proof. This can be achieved by computing the estimate of $\mathcal{A}$ using an $n_A X n_A$ matrix and E_{track}, where $E_{track}[i,j] = \{Prob_{i,j}\}, i,j \in [1, n_\mathcal{A}]$. Then, the attacker $\mathcal{A}$ calculates the probability $Prob_{i,j}$ for which, in every ID α_i, a given α_i belongs to the same participant as every α_i in the SMP. However, E_{track} also consists of extra information that can be extracted from the SMP by $\mathcal{A}$. This can be accomplished by means of statistical analysis or any other processes. Furthermore, the success of $\mathcal{A}$ in the game can be computed as follows.

Given the actual ID correlation matrix ACM_{track}, then $ACM_{track} = 1$ if α_i and α_j are of the same participant; otherwise, $ACM_{track} = 0$, $\forall i,j \in [1, n_\mathcal{A}]$. Moreover, for each α_i, the error in $\mathcal{A}$'s estimate can be calculated by taking the distance of $E_{track}[i,*]$ from the actual ID correlation of α_i with other IDs in the SMP:

$$\| E_{track}[i,*] - ACM_{track}[i,*] \|, \tag{5}$$

where $\| \, . \, \|$ implies the L1 rule of the corresponding row matrix.

Therefore, the success of $\mathcal{A}$ in the game $Suc_\mathcal{A}$ can be computed via $\mathcal{A}$'s maximum error:

$$max_{\forall \alpha_i \in \rho_\mathcal{A}}(\| E_{track}[i,*] - ACM_{track}[i,*] \|). \tag{6}$$

Equally, the estimate of $\mathcal{A}^\tau$ for all possible pairs of IDs can be represented in the game by the $n_\mathcal{A} X n_\mathcal{A}$ matrix E^τ_{track}, given as

$$E^\tau[i,j] = \vartheta_{i,j}. \tag{7}$$

If $\alpha_0, \alpha_1 \in \rho_\mathcal{A}$, then

$$E^\tau_{track}[i,j] = \gamma + (1-\gamma)1/2. \tag{8}$$

where $\vartheta_{i,j}$ denotes the probability that IDs α_0 and α_1 imply the same participant given $\rho_\mathcal{A}$, while γ denotes the fraction of IDs that cannot be correlated with other IDs. However, the probability of other IDs not included in $\rho_\mathcal{A}$ is given as $1/2(1+\gamma)$, which is the probability that one of the following occurs:

1. α_0 is the only ID of its owner;
2. $\mathcal{A}^\tau$ was not successful in guessing δ.

Thus, with this, the degree of achievement of $\mathcal{P}$'s anonymity and untraceability features can be measured by evaluating the extra success recorded by $\mathcal{A}$ in the SMP compared with that of $\mathcal{A}^\tau$. This success is computed as

$$Success_\mathcal{A} = (Suc_\mathcal{A} - Suc_{\mathcal{A}^\tau}/Suc_{\mathcal{A}^\tau}). \tag{9}$$

while failure is computed as

$$Failure_\mathcal{A} = 1 - (Suc_\mathcal{A} - Suc_{\mathcal{A}^\tau}/Suc_{\mathcal{A}^\tau}). \tag{10}$$

□

5.2. Transactional Data Privacy

To achieve faster encryption and decryption processes for transactional data privacy, RSA cryptosystem speedup techniques [33] were used. The decryption process is achieved using the Chinese remainder theorem (CRT), while the encryption process is achieved by choosing a very small value for the public ID. The objective is to provide a fast, secure and lighter cryptographic approach to the IoT-based resource-constraining devices for their transactional data privacy:

Proposition 2. *A secure encryption process can be accomplished with a relatively low prime value for a public ID e while at the same time achieving absolute speeding up of the entire process for data transactions.*

Remark 1. *The use of such public IDs, particularly those with a number of ones in binary representation (low hamming weight) such as* $e = 3$, $e = 17$ *and* $e = 2^{16} + 1$, *can result in a low number of exponentiation operations, thus speeding up the encryption process [33].*

Proof. For a given encryption or decryption process, the RSA bit length of the modulus n is given as $t + 1$ (i.e., $[\log_2 n] = t + 1$), where t is some integers. Therefore, the private ID d does not have its complete bit length of $t + 1$ yet, even with small value for e. As a result, the RSA cryptosystem is still secure with these short public keys, as described in Proposition 2. □

Proposition 3. *A secure decryption speeding up process with a factor of four can be achieved using the CRT technique.*

Remark 2. *In CRT exponentiation, all associated values (i.e.,* d_p, d_q, x_p *and* x_q*) are bounded by* p *and* q *and also have a bit length almost equal to* $t/2$ *bits, where* p *and* q *are prime figures,* x *is the base element and* d *is the decryption exponent. If the square-and-multiply method is used to compute two exponentiations, then each requires an average of* $1.5t/2$ *modular multiplications and squarings. In total, the number of modular multiplications and squarings is given as [33]*

$$SQ + MULT = 2 \times 1.5t/2 = 1.5t. \tag{11}$$

Proof. The CRT version of decryption requires both primes p and q as well as the decryption exponent d, so this may seem to be an extra source of insecurity. Nevertheless, factoring in the modulus n may be easy if the decryption exponent d is given, and therefore no security is lost while using this technique.

From Equation (11), we can observe that the computational complexity is the same with regular exponentiation without the CRT. Nevertheless, all the values associated with the process have $t/2$ bits, which contrasts with operation without the CRT, where t bit variables are computed for each multiplication. In a nutshell, it can be observed that the complexity of the multiplication increases quadratically with the increase in the bit length. As a result, each $t/2$ bit multiplication is four times faster than a t bit multiplication. □

6. Experimental Analysis and Results

In this section we have selected the benchmark models of Aitzhan et al. [6] and Dorri et al. [7] based on contextual resemblance and the state of the art, while the model from Folha et al. [30] was based on similitude and recency to our proposed model.

The efficiency of our proposed approach was compared with that of the benchmark models in terms of the success of $\mathcal{A}$ in discovering the participant's anonymity and untraceability in the SMP. All of these studies provided blockchain-based solutions in which interactions were based on transactions. These experiments were executed on the Ethereum blockchain, where all interactions are handled as transactions which can be quantified in terms of Ethereum gas per unit transaction.

Similarly, the efficacy of the chosen speeding up RSA cryptographic process at providing transactional data privacy was examined and compared to that of the standard RSA cryptographic process.

6.1. Experimental Set-Up

The experimental environment was built using the Solidity language. All the participants' smart gateways were defined during our implementation as mappings from the Ethereum addresses of the participating smart homes. In addition, the Ethereum address of the SmGW was also initialized. Twenty different authorized participants and their trading transactions were considered in the SMP to measure the success of $\mathcal{A}$ in the game against $\mathcal{A}^{\tau}$. Furthermore, we evaluated the success of $\mathcal{A}$ in recovering the public IDs of the participants in the proposed approach and the other base approaches in [6,7,30]. We also analyzed the trading transaction messages to investigate the effectiveness of the proposed approach at achieving transactional data privacy. The messages were encrypted and decrypted using both the traditional RSA and the sped up RSA, each of which was enabled in the approach for separate scenarios.

Across our tests, we replicated a simulation scenario to consider both the limited information and no information situations. In the limited information situation, we assumed that $\mathcal{A}$ was aware of the position or delivery of all SMP participants and, as such, could determine if a transaction was rendered in return for traded resources. In this scenario, we had both the IDs of the provider and requester in the prior knowledge of $\mathcal{A}$ while processing $Success_{\mathcal{A}}$. In the no information situation, we assumed a situation where $\mathcal{A}$ did not know the position or operation of all participants and, as such, did not have any previous information but believed that some trading transactions took place between some participants in the network.

6.2. Evaluating the Success of $\mathcal{A}$ at Discovering Participant's Anonymity and Untraceability in the SMP

We analyzed the metrics $Success_{\mathcal{A}}$ for the benchmark approaches [6,7,30] to check for the performance of $\mathcal{A}$ in exposing the participant's session ID with respect to our E-Bitmessage-based approach. The results in Figure 3 show that the probability of $\mathcal{A}$'s failure in our approach was more pronounced compared with that in [6,7,30]. This shows that the degree of achievement of $\mathcal{P}$'s anonymity and untraceability could be observed with high probability (0.848 on average) in our approach. Hence, the results confirm the claim made in Proposition 1 and Theorem 1.

Furthermore, it can be observed that there was no definite trend in Figure 3 with respect to the increasing number of participants. This was due to the fact that the system at a given time instance Δ was composed of multiple participants, each carrying a different number of trading transactions with a different number of parties (trading activities). Thus, the computational complexities applied to each participant during the trading activities depends on the number of activities carried out by that participant at the given time instance. For instance, participant 9, which had fewer trading activities (having two trading sessions) at given time instance Δ, would have a lower computational overhead as well as the lowest probability of $\mathcal{A}$'s success compared with participant 16 with the most trading activities (having eight trading sessions) at a given time instance Δ. In a nutshell, the findings show that the fewer trading activities a participant $\mathcal{P}$ has, the lower the computational complexity applied to it, and the lower the probability of $\mathcal{A}$'s success is with it.

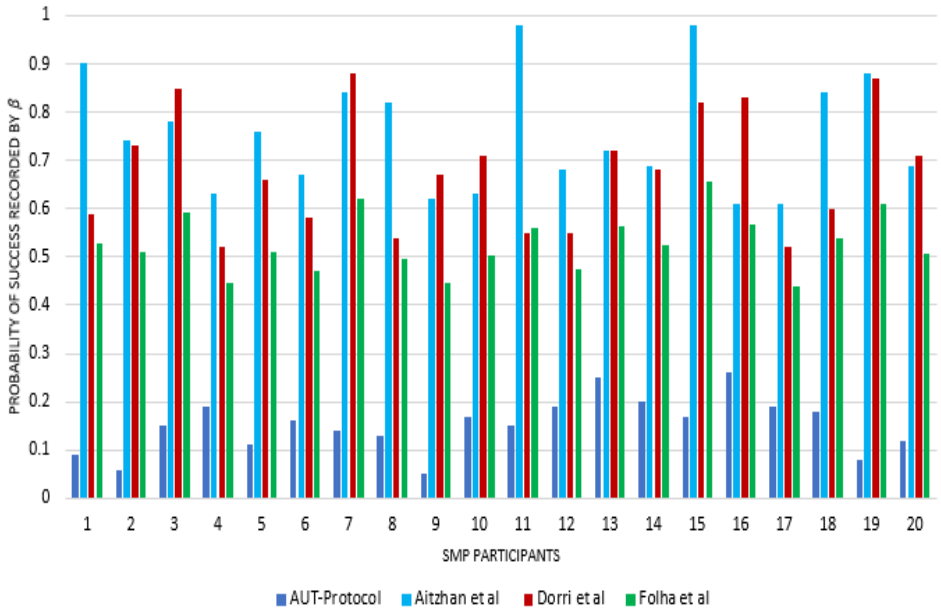


Figure 3. Probability of success recorded by $\mathcal{A}$ in the SMP.

To have a better understanding of the trend in the results, they are further summarized in Table 3, which is based on the sample of 20 participants categorized in an increasing order of five groups. The table shows that $\mathcal{A}$ had a negligible effect on the participants when using our approach, with an average efficiency of around 15% in terms of linking IDs to their correct owners. Similarly, it can be seen that the adversary exceeded $\mathcal{A}^{\tau}$ for the groups of Aitzhan et al. [6], Dorri et al. [7] and Folha et al. [30] by an average of about 75%, 68% and 53%, respectively, in the overall system. In addition, it can be realized that the success of $\mathcal{A}$ increased slightly as the fraction of the participants increased in our approach. The above disparities may result from the fact that Bitmessage users may add a little noise to the blockchain log during transactions. Similarly, it can be seen from Table 3 that the values in [6,7,30] were close to one. This implies that $\mathcal{A}$ performed much better than $\mathcal{A}^{\tau}$ and that the approximation selected by $\mathcal{A}$ was near a valid address linking to the appropriate participants. Thus, we infer that the anonymity of blockchain users can still be breached even though users manually generate new addresses to keep their addresses from being linked together.

Table 3. Results for $\mathcal{A}$'s success per group of participants in the system.

Groups of Participants	1–5	6–10	11–15	16–20
AUT-Protocol	0.12 ± 0.01	0.13 ± 0.01	0.19 ± 0.01	0.17 ± 0.02
Aitzhan et al. [6]	0.76 ± 0.01	0.72 ± 0.02	0.81 ± 0.01	0.73 ± 0.02
Dorri et al. [7]	0.67 ± 0.01	0.68 ± 0.02	0.66 ± 0.01	0.71 ± 0.02
Folha et al. [30]	0.52 ± 0.01	0.51 ± 0.02	0.56 ± 0.01	0.53 ± 0.02

In addition, our findings demonstrate that the benefit of $\mathcal{A}$ over $\mathcal{A}^{\tau}$ was not substantially influenced in the proposed approach by the number of SMP participants. This is because of the explanations given in Proposition 1 and Theorem 1. However, the findings demonstrate that the benefit of $\mathcal{A}$ in [6,7,30] increased equally as the number of participants rose. This is mostly attributed to the assumption that as the number of participants rises, the allocation of addresses to the appropriate participants becomes absolute due to a blockchain analysis attack. However, it is important to note that the system allows a participant $\mathcal{P}$ to execute O2M trading transactions at the same time. Therefore, it is probable for a participant to be present concurrently in two or more transactions.

6.3. Achieving Fast Encryption and Decryption for Transactional Data Privacy

Figures 4 and 5 provide the encryption and decryption times for a message observed for each participant in the SMP, respectively. The average encryption time for the proposed approach was 0.0095 s, while it was 0.1322, 0.1376 and 0.028 s for the approaches in [6,7,30], respectively. Similarly, the average decryption time of the proposed approach was 0.010 s, while for the approaches in [6,7,30], it was 0.029, 0.051 and 0.0176 s, respectively. This shows that the speedup factor of the proposed scheme was approximately 14 for encryption and 3.5 for decryption when compared with the results in [6,7,30].

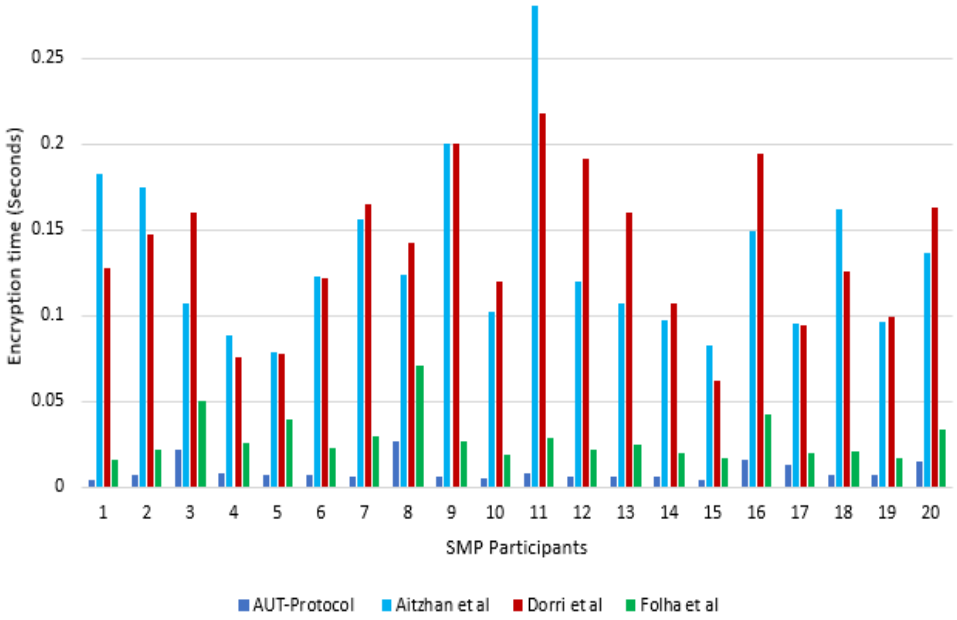


Figure 4. Comparison of the transactional message encryption times.

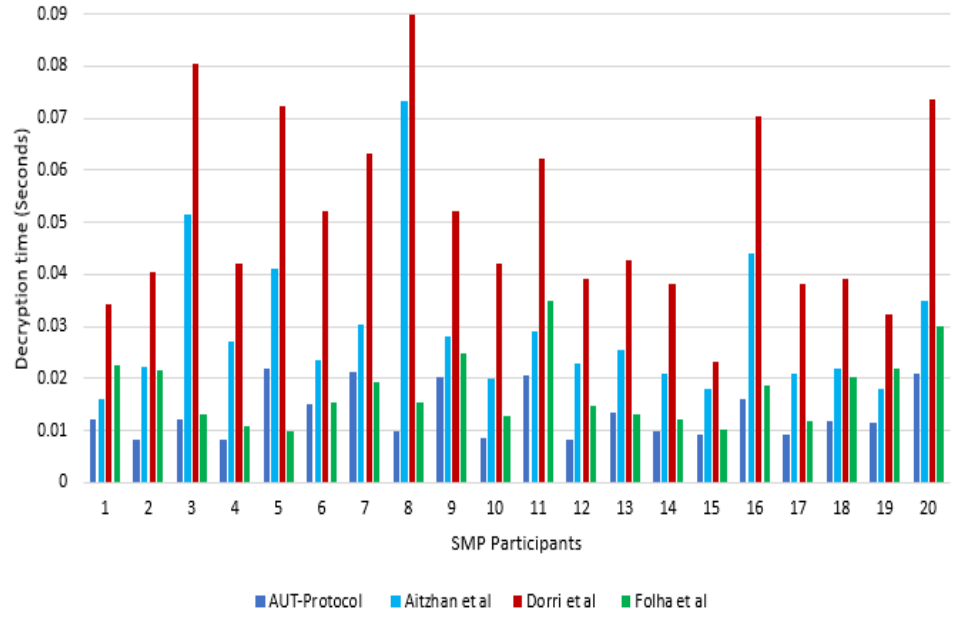


Figure 5. Comparison of the transactional message decryption times.

6.4. Security and Privacy Comparison

To summarize, Table 4 compares the proposed AUT protocol to two previously existing schemes from Aitzhan et al. [6], Dorri et al. [7] and Folha et al. [30]. We used the words "Yes" and "No" to indicate whether or not a scheme fulfilled the security and privacy

requirements that were evaluated. As can be seen in the Table, none of the schemes in [6,7] ensured the privacy of a participant's data throughout the data transfers.

Similarly, the table illustrates that the schemes in [6,7,30] failed to ensure the confidentiality of participant data in blockchain network applications. Finally, as shown before in this work, the schemes in [6,7,30] could not guarantee participant anonymity or untraceability. Additionally, recent studies have revealed flaws in the approaches used in these schemes [1]. Nonetheless, the proposed AUT protocol passed all of the considered security and privacy criteria in this work.

Table 4. Security and privacy comparison.

Security and Privacy Parameteres	Aitzhan et al. [6]	Dorri et al. [7]	Folha et al. [30]	AUT Protocol
Trasactional data privacy	No	No	Yes	Yes
Untreacibility	No	No	No	Yes
Intergrity	Yes	Yes	Yes	Yes
Anonymity	No	No	No	Yes
Non-repudiation	Yes	Yes	Yes	Yes
Confidentiality	No	No	No	Yes

6.5. Limitations of This Study

This study has two major limitations regarding its scalability. The first is that a smaller sample size was used to assess the proposed model. The second refers to the blockchain's architectural design. In the context of resource trade, malicious behavior is multifaceted and impacted by a number of circumstances. In the future, there will be a greater focus on participant behavior related to trust throughout the trading cycle in a blockchain network setting. Determining the characteristics that influence user behavior on blockchain-based trading platforms is another topic for future research that has been investigated. In addition, the influence of the proposed model on human behavior in a big trading environment can only be shown if the model's basic functions and components are technically possible. The major limitation of blockchain technology is its scalability. As generic solutions for improving the scalability of blockchain technology are established, it is fair to expect that these solutions can also be relevant to SMP-based trading environments. Therefore, future research should emphasize tackling the scalability issue.

7. Conclusions

Existing privacy-enabling schemes are not effective against identity-based attacks or ensuring transactional data privacy in blockchain-based network applications, such as resource trading in the SMP. In order to achieve a participant's anonymity, untraceability and transactional data privacy, we proposed a privacy-enabled message exchange mechanism among the participants of the SMP. Security analysis of the proposed scheme under different threat scenarios has shown that it is much more resilient to identity-based attacks compared with the benchmark protocols. Moreover, the simulation-based analysis showed that the proposed scheme not only minimizes the probability of success for the attacker but is also less computationally expensive.

Author Contributions: Conceptualization, B.M.Y. and M.I.K.; methodology, B.M.Y.; software, B.M.Y.; validation, B.M.Y., M.I.K., A.A. and A.K.; formal analysis, B.M.Y., M.H.S. and A.A.; investigation, B.M.Y., S.R. and A.K.; resources, A.K., M.H.S. and S.R.; data curation, A.A., M.H.S. and S.R.; writing—original draft preparation, B.M.Y. and M.I.K.; writing—review, editing and visualization, A.A., M.H.S. and S.R.; supervision, M.I.K.; project administration, B.M.Y. and M.I.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: https://github.com/sysbel07/AUT_model.git (accessed on 10 January 2023).

Acknowledgments: The authors acknowledge the supports and advice rendered by Pattarasinee Bhattarakosol of the Department of Mathematics and Computer Science at Chulalongkorn University, Bangkok, 10330, Thailand. The authors are thankful for the support and advice. The authors acknowledge TU Wien Bibliothek for financial support through its Open Access Funding Programme.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Conti, M.; Sandeep, K.E.; Lal, C.; Ruj, S. A survey on security and privacy issues of bitcoin. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3416–3452. [CrossRef]
2. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
3. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
4. Banerjee, M.; Lee, J.; Choo, K.K.R. A blockchain future for internet of things security: A position paper. *Digit. Commun. Netw.* **2018**, *4*, 149–160. [CrossRef]
5. Kumar, N.M.; Mallick, P.K. Blockchain technology for security issues and challenges in IoT. *Procedia Comput. Sci.* **2018**, *132*, 1815–1823. [CrossRef]
6. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852. [CrossRef]
7. Dorri, A.; Luo, F.; Kanhere, S.S.; Jurdak, R.; Dong, Z.Y. SPB: A secure private blockchain-based solution for distributed energy trading. *IEEE Commun. Mag.* **2019**, *57*, 120–126. [CrossRef]
8. Khan, S.; Khan, R.; Al-bayatti, A.H. Secure Communication Architecture for Dynamic Energy Management in Smart Grid. *IEEE Power Energy Technol. Syst. J.* **2019**, *6*, 47–58. [CrossRef]
9. Warren, J. Bitmessage: A Peer-to-Peer Message Authentication and Delivery System. White Pap. (27 November 2012). 2012; p. 5. Available online: https//bitmessage.org/bitmessage.pdf (accessed on 23 June 2021)
10. Shi, L.; Guo, Z.; Xu, M. Bitmessage Plus: A Blockchain-Based Communication Protocol With High Practicality. *IEEE Access* **2021**, *9*, 21618–21626. [CrossRef]
11. Wright, C.S. Bitcoin: A Peer-to-Peer Electronic Cash System. *SSRN Electron. J.* **2019**, *7859*, 6–24. [CrossRef]
12. Blockchain, C. Merkle Tree—Necessity or Atavism? Medium. Available online: https://medium.com/@credits/merkle-tree-necessity-or-atavism-d8ff3e263131 (accessed on 11 September 2020).
13. Odelu, V.; Das, A.K.; Wazid, M.; Conti, M. Provably Secure Authenticated Key Agreement Scheme for Smart Grid. *IEEE Trans. Smart Grid* **2018**, *9*, 1900–1910. [CrossRef]
14. Zhang, L.; Zhao, L.; Yin, S.; Chi, C.H.; Liu, R.; Zhang, Y. A lightweight authentication scheme with privacy protection for smart grid communications. *Futur. Gener. Comput. Syst.* **2019**, *100*, 770–778. [CrossRef]
15. Sousa, T.; Soares, T.; Pinson, P.; Moret, F.; Baroche, T.; Sorin, E. Peer-to-peer and community-based markets: A comprehensive review. *Renew. Sustain. Energy Rev.* **2019**, 367–378.. [CrossRef]
16. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *144*, 13–48. [CrossRef]
17. Košťál, K.; Helebrandt, P.; Belluš, M.; Ries, M.; Kotuliak, I. Management and Monitoring of IoT Devices Using Blockchain. Sensors 2019, 19, 856. [CrossRef]
18. Yakubu, B.M.; Khan, M.I.;Javaid, N.; Khan, A. Blockchain-based secure multi-resource trading model for smart marketplace. *Computing* **2021**, *103*, 379–400. [CrossRef]
19. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3690–3700. [CrossRef]
20. Li, Z.; Chen, S.; Zhou, B. Electric vehicle peer-to-peer energy trading model based on smes and blockchain. *IEEE Trans. Appl. Supercond.* **2012**, *31*, 5700804. [CrossRef]
21. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
22. Guan, Z.; Si, G.; Zhang, X.; Wu, L.; Guizani, N.; Du, X.; Ma, Y. Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities. *IEEE Commun. Mag.* **2018**, *56*, 82–88. [CrossRef]
23. Sober, M.; Scaffino, G.; Schulte, S.; Kanhere, S.S. A blockchain-based IoT data marketplace. *Cluster Comput.* **2022**. [CrossRef]
24. Yousafzai, A.; Khan, L.U.; Majeed, U.; Hakeem, O.; Hong, C.S. FedMarket: A Cryptocurrency Driven Marketplace for Mobile Federated Learning Services. *IEEE Access* **2022**, *10*, 87602–87616. [CrossRef]

25. Zhang, M.; Liu, J.; Feng, K.; Beltran, F.; Zhang, Z. SmartAuction: A blockchain-based secure implementation of private data queries. *Future Gener. Comput. Syst.* **2023**, *138*, 198–211; ISSN 0167-739X. [CrossRef]
26. Bracciale, L.; Raso, E.; Gallo, P.; Sanseverino, E.R.; Bianchi, G.; Loreti, P. Privacy in Blockchain-based Smart Grids. In Proceedings of the 2022 Workshop on Blockchain for Renewables Integration (BLORIN), Palermo, Italy, 2–3 September 2022; pp. 37–41. [CrossRef]
27. Diaconita, V.; Belciu, A.; Stoica, M.G. Trustful Blockchain-Based Framework for Privacy Enabling Voting in a University. *J. Theor. Appl. Electron. Commer. Res.* **2023**, *18*, 150–169. [CrossRef]
28. Mezquita, Y.; Gil-González, A.B.; Martín del Rey, A.; Prieto, J.; Corchado, J.M. Towards a Blockchain-Based Peer-to-Peer Energy Marketplace. *Energies* **2022**, *15*, 3046. [CrossRef]
29. Zhang, J.; Zhong, C. Differential Privacy-Based Double Auction for Data Market in Blockchain-Enhanced Internet of Things. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 8038846. [CrossRef]
30. Folha, R.; Times, V.; Carvalho, A.; Araújo, A.; Couto, H.; Viana, F. FoodChain: A Food Delivery Platform Based on Blockchain for Keeping Data Privacy. In *Database Systems for Advanced Applications*; DASFAA 2022. Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13247._43. [CrossRef]
31. Yakubu, B.M.; Chajera, P.; Garko, A.B. Advanced Secure Method for Data Transmission in Manet Using Rsa Advanced Secure Method for Data Transmission in Manet Using Rsa. *Int. J. Adv. Technol. Eng. Sci.* **2016**, *2015*, 176–185.
32. Iqbal, M.; Matulevičius, R. Exploring sybil and double-spending risks in blockchain systems. *IEEE Access* **2021**, *9*, 76153–76177. [CrossRef]
33. Paar, C.; Pelzl, J. *Understanding Cryptography: A Textbook for Students and Practitioners*; Springer Science & Business Media: Berlin, Germany, 2009.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.