energies

MDPI

Article

Enhancing Trust in Transactive Energy with Individually Linkable Pseudonymous Trading Using Smart Contracts

Daniel Sousa-Dias [1], Daniel Amyot [1,*], Ashkan Rahimi-Kian [1,2] and John Mylopoulos [1]

[1] School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON K1N 6N5, Canada; dsous064@uottawa.ca (D.S.-D.); ashkan.kian@iemssolution.com (A.R.-K.); jm@cs.toronto.edu (J.M.)
[2] IEMS Solution Ltd., Communitech, Kitchener, ON N2G 1H6, Canada
* Correspondence: damyot@uottawa.ca; Tel.: +1-613-562-5800 (ext. 6947)

Abstract: The transactive energy market (TEM) is a recent development in energy management that enables prosumers to trade directly, promising many environmental and economic benefits. Prosumer trading necessitates sharing information to facilitate transactions. Additionally, many TEMs propose using blockchains to manage auctions and store transactions. These facts introduce privacy concerns: consumption data, trading history, and other identifying information pose risks to users if leaked. Anonymity by trading under a pseudonym is commonly presented as a solution; however, this creates risks for market participants: scammed users will not have recourse, and users with innocent malfunctions may be banned from trading. We propose the *Individually Linkable Pseudonymous Trading Scheme* (ILPTS), which enables users to trade under a pseudonym, protecting their identity, while a smart contract monitors reputations and can temporarily deanonymize a user, ensuring market integrity. ILPTS was developed in stages. Examination of existing TEM literature was performed to identify desirable features. Analysis of cryptography literature was performed to identify techniques that may confer certain features. It was found through formal analysis that ILPTS adheres to identified design goals, improves upon existing solutions, and resists common attacks against TEMs. Future work includes software simulation and on-device implementation to further verify security and feasibility.

Keywords: privacy; prosumer; smart contract; smart meter; transactive energy market; trust

check for updates

Citation: Sousa-Dias, D.; Amyot, D.; Rahimi-Kian, A.; Mylopoulos, J. Enhancing Trust in Transactive Energy with Individually Linkable Pseudonymous Trading Using Smart Contracts. *Energies* **2024**, *17*, 3568. https://doi.org/10.3390/en17143568

Academic Editor: José Matas

Received: 1 May 2024
Revised: 1 July 2024
Accepted: 16 July 2024
Published: 20 July 2024

Copyright: © 2024 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

Advanced metering infrastructure (AMI) has led to progress in functionality in the power delivery space [1]. Smart meters enable the collection of much more frequent and detailed data from virtual power plants (VPPs), smart homes/buildings, and smart grid facilities for improved power delivery services and better analytics for distribution system planning and optimal operations [2]. Developments like transactive energy (TE), improved demand response and power flow optimization, consumption prediction profiling, and machine learning-supported surge prediction are just a few examples of technological progress and innovations in power systems [3]. These innovations will enable greater economic efficiency through models like transactive energy, enabling high-frequency peer-to-peer energy trading. These models will also contribute to greater energy efficiency, due to improved generation and load balancing, intelligent demand response programs, and AI-assisted predictions [4].

Blockchain technology has emerged as a de facto foundation for transactive energy implementations due to its strong cryptographic security and resistance to false data injection [5–7]. However, publishing electricity transactions on a public ledger poses significant privacy risks to the energy prosumers, consumers, and distribution system operators (DSO) [8,9].

Current solutions make a tradeoff between privacy and regulation, either choosing to enforce greater privacy measures at the expense of being able to regulate market activity [10], or reducing prosumers' privacy to facilitate improved regulatory ability [11].

This paper contributes a new privacy scheme named *Individually Linkable Pseudonymous Trading Scheme* (ILPTS), which aims to alleviate the need for this tradeoff. In the proposed solution, prosumers are able to trade energy under totally anonymous pseudonyms, the true identities of whom are not known to any party including the DSO itself. Meanwhile, a recovery database is stored on a blockchain that enables reassociation of a user's true identity with their pseudonym if they consistently fail transactions. This process requires multiple parties to cooperate and can only be initiated by a self-governing smart contract; thus, no prosumer can be manually exposed.

The contributions of this paper are as follows:

- **New functionality**: previous systems had to decide between total anonymity and capacity to respond to errors. By enabling total but revocable privacy, ILPTS enables functionality not seen in other transactive energy market proposals. This would enable a DSO to be more responsive to network errors and to provide novel services such as in-home maintenance to users.
- **Enhanced privacy**: ILPTS would enhance the privacy of the basic blockchain-based TEM model by providing anonymity to energy clients. When implemented in a model that already provides this anonymity, ILPTS improves its functionality while retaining the existing anonymity. When implemented in a model with partial trust—i.e., anonymity in the public market but identities registered with the DSO—ILPTS improves privacy by hiding the user's identity more comprehensively, creating an effectively trustless system.
- **Equity**: ILPTS improves the fairness of TEM models by enabling repudiation and mediation, obviating the need for coarse punitive measures such as disconnecting power, and reducing false positives in fraud and malware detection.
- **Improved security**: while enabling the previously mentioned benefits, ILPTs's novel registration process is secure and fully distributed. Information is concealed and encrypted at every stage. In addition, the deanonymization process can only be initiated by the monitoring smart contract, greatly reducing the potential for abuse.

ILPTS will be useful to purveyors of smart grid technology as a proof-of-concept of the privacy and security stature of this new paradigm. It will also be useful to TEM designers to improve the equity, privacy, and legality of their distributed energy market systems. Finally, ILPTS provides a novel technique to achieve goals that are seemingly at odds in a secure, distributed, and validated manner, which will be of interest to researchers in the fields of TE, cryptography, and distributed computing.

The paper is structured as follows. Section 2 examines the state of privacy solutions in the field and works that motivated the development of this scheme. In Section 3, we describe the technologies involved, the architecture of TEMs, the fundamental problem we seek to address, and design requirements for a solution. Section 4 presents the research methodology used to design and evaluate our new solution. Section 5 introduces our ILPTS solution, providing both a high-level overview as well as a formal description. In Section 6, we evaluate the scheme's adherence to the design goals, as well as the security properties of the scheme and potential attacks that could be carried out. Section 7 concludes the study by evaluating the success of the scheme in achieving its design goals and discussing future research directions.

2. Related Work

Efforts to improve privacy in TEMs have focused on a few key areas, including privacy-preserving data aggregation, market privacy and anonymization, and privacy-preserving billing mechanisms. These advancements are critical for prosumers' safety and trust; the adoption of smart grids (SG) and TEM technology—which stand to present environmental and economic benefits—will be limited by prosumers' trust in their privacy

being maintained by such technology. A comparison of related schemes by relevant features can be found in Table 1.

Table 1. Comparison of related schemes. Type of study: (S)cheme, (P)latform/framework, or survey/systematic (R)eview. Other columns: (y)es, (n)o, or (-) unknown.

Approach	Type of Study	User Anonymity	Discusses Social Outcomes	Privacy-Preserving	Homomorphic Encryption	Modular	Fraud Detection	Auction Clearing Procedure	Decentralized	Employs a Cryptosystem	Blockchain	Smart Contracts	EV Focus	Extends Other Schemes	Registration Procedure	Facilitates P2P Trading
Sharma et al. [12]	P	y	n	y	n	n	n	n	y	y	y	y	y	n	y	n
Garg et al. [13]	S	y	n	n	n	y	n	n	n	y	y	n	y	n	y	y
Li et al. [14]	S	y	y	y	n	y	n	y	n	n	n	n	y	n	n	y
Li et al. [15]	S	y	n	y	y	y	n	y	n	y	n	n	y	n	n	n
Eisele et al. [10]	P	y	n	y	n	n	n	n	y	n	y	y	n	n	y	y
Baza et al. [16]	S	y	n	y	n	y	y	n	y	y	y	n	y	y	n	y
Baza et al. [17]	S	y	n	y	n	y	y	n	y	y	y	y	y	n	n	n
Bergquist et al. [18]	S	y	n	y	n	y	n	n	y	y	y	y	n	y	n	n
Laszka et al. [19]	S	y	n	y	n	y	n	n	y	n	y	n	n	y	n	y
Khorasany et al. [20]	P	y	n	y	n	y	y	n	y	y	y	y	n	n	n	y
Mollah et al. [21]	R	y	y	-	n	-	y	y	y	y	y	y	n	-	n	-
Ziu et al. [22]	P	n	y	n	n	n	n	y	y	n	y	y	n	n	n	y
Kang et al. [23]	P	n	n	n	n	n	n	n	y	n	y	y	n	n	n	y
Honari et al. [24]	R	n	y	-	n	-	y	y	n	n	y	y	y	-	y	-
ILPTS	S	y	y	y	y	y	y	n	y	y	y	y	n	y	y	n

The field of electric vehicle information security is particularly valuable for TE security research, and many of the studies mentioned here fall into that category. Much privacy research in the TE field has originated in research specific to electric vehicles (EVs) [12–17]. This is due to the unique position of EVs in transactive energy and smart grid architecture. Their ability to move freely and the identifying information they contain present novel challenges to TE and SG designers [13]. EVs can reveal different kinds of information to attackers compared to other advanced metering infrastructure (AMI), which can be more damaging in some cases, such as facilitating stalking [14].

As will be discussed in Section 4, a critical component of designing ILPTS was sourcing techniques from cryptography literature to imbue the scheme with certain properties. One such technique was homomorphic encryption, which is seen in other privacy-focused TEM literature, such as the privacy-preserving double auction scheme proposed by Li et al. [15]. In their scheme, homomorphic encryption is used to protect user information in the cloud when performing auction clearing operations. In ILPTS, homomorphic encryption supports the transparent yet private registration and validation of users during the onboarding process.

ILPTS is designed to build on top of existing TEM platforms and provide enhanced security for the underlying market. In the TRANSAX system [10], for example, users are anonymous within groups, which are used to ensure maintenance of safety restrictions with regards to energy transmission. Although TRANSAX provides the most anonymity among proposed TEM architectures (to the best of our knowledge), it suffers from the fact that the anonymity is irreversible. ILPTS could be used to improve TRANSAX's transparency and equity while retaining its grid safety offerings and other benefits. This sort of proposal is found in the literature; Baza et al. [16] introduce a privacy-preserving vehicle-to-vehicle trading scheme that extends their previous work, a privacy-preserving charging station-to-

vehicle trading scheme [17], and Bergquist et al. [18] propose a solution meant to extend the existing PETra protocol proposed by Laszka et al. [19] with additional communication security measures and transactional anonymity. Schemes may also work synergistically in a larger platform. For example, Khorasany et al. [20] propose *Anonymous Proof of Location* (A-PoL), a protocol that allows users to validate their location without sharing their identity. This is a good example of a scheme that could operate in concert with ILPTS, something we discuss in more detail in Section 6.3. It should be noted that ILPTS is not designed specifically for TRANSAX, but it serves as a compatible example.

As mentioned earlier, decentralized management of registration and user identity is rare in existing implementations [21]. However, many studies tacitly acknowledge the importance of decentralization by seeking to decentralize other components of their operation. Sharma et al. [12] acknowledge the importance of decentralization to avoid single point of failure and trust concerns, and propose a decentralized scheme to facilitate EV energy trading with minimal mediation. ILPTS seeks to improve the current state of affairs by bringing the benefits of decentralization to user identity management, registration, and anomaly detection.

While ILPTS has not yet been implemented in practice, other transactive energy platforms have been developed experimentally. Mollah et al. [21] explore nine practical distributed platforms for energy. While many offer some degree of trade obfuscation, none offer the full feature set of ILPTS; nor do they manage user identity in a distributed manner. Of course, these platforms have the advantage of having been implemented, making the comparison not totally fair. As such, creating an implementation of ILPTS to demonstrate its superiority is a high-priority future research item.

An important feature of ILPTS is its use of smart contracts to enable automated and immutable operations that cannot be manually interfered with. Other schemes make use of these properties of smart contracts, for example Ziu et al. [22] with their *iVPP P2P transactive energy framework*, a fully practical TEM model that was tested in a lab setting that also leverages the self-governing nature of smart contracts to ensure tamper resistance. Kang et al. [23] employ smart contracts to facilitate user registration; having evidence that this was achievable was central to the development of ILPTS. However, their solution does not take full advantage of the potential offered by such an implementation. In addition, Honari et al. [24] note that user registration via smart contract has not yet been thoroughly explored. ILPTS seeks to bring the benefits of smart contracts to registration as well with its novel onboarding process.

As will be discussed in Section 3, a critical motivating factor in the development of ILPTS was improving social outcomes. This concern is not always mentioned in the technical literature, but Li et al. [14] note that their locational-privacy-preserving double auction scheme achieves positive results with social welfare. ILPTS contributes another proposal with social good as a guiding principle, and hopefully a trend will emerge.

3. Background and Motivation

This section provides important background information that motivates the need for developing a new solution such as ILPTS.

3.1. Network Architecture

The network architecture is presumed to consist of:

- Distribution system operator (DSO): a centralized authority that authenticates users and manages the distribution (or retail) energy market.
- Smart meters: users connect to the grid and distributed market via smart meters.
- Fog nodes: auxiliary network computing nodes with elevated status and trust.
- Blockchain: a distributed ledger on which transactions and other information will be recorded.
- Smart contracts: scripts that execute on the blockchain and that may facilitate additional functionality or public information transfer.

3.2. Blockchain Markets

Blockchain, or distributed ledger technology, is a distributed database of transactions whose state is maintained by members of the *blockchain network*. Users on the network contribute computing resources to verify the state of the blockchain and facilitate transactions between members by way of *cryptocurrency*, the primary unit of value on the chain.

Blockchain technology offers several unique security benefits, including non-repudiation, an immutable record of transactions, and extreme cryptographic resistance against false data injection [25].

Modern implementations, such as Ethereum, have introduced the notion of scripting, employing the ledger as a state machine to facilitate distributed virtual computation [26]. The scripts that run on these blockchains are known as *smart contracts*.

Blockchain-based transactive energy markets are automated energy auctions where the market clearing functionality is handled by smart contracts, the blockchain ledger is used to maintain the record of energy exchange, and often an intermediary cryptocurrency token is used to manage energy transactions.

3.3. Reputation Mechanisms

An issue that arises with the use of highly anonymous distributed computing methods to facilitate real-world auctions is that of malicious users and associated cyberattacks or fraud.

In an earlier review [5], we discovered a common method for handling such concerns: reputation mechanisms. In some markets, users would be associated with a reputation value. An example of this mechanism, Q-Score, is introduced by Zaman and He [27]. This Q-Score reputation value would be penalized for participating in failed transactions. This provides a simple heuristic that identifies users who may be gaming the system in some way—for example, by forcing their meter to repeatedly claim that energy was not delivered, thus preventing an outbound transfer of funds.

Common methods of handling low-reputation users include access blocking [28] and separate trading pools [29]. The failed transaction metric illustrates the issue at hand regarding punishment, since users may also experience failed transactions due to hardware error, or other circumstances that are no fault of their own. Regardless of the reason, cutting off a user's access to energy is unethical due to the vitality of electricity in modern life [30].

3.4. Coin Mixing

Coin mixing is a protocol proposed by Ruffing et al. [31] intended to provide users on a blockchain a heightened level of anonymity. Blockchain technology is regarded as anonymous because a users' real identity (i.e., name, address, social security number, etc.) is not associated with their account, unlike with a credit card or bank account. However, because all transactions are public, if one's identity *is* ever connected to a particular account, their activity would be completely compromised.

A consideration for how to manage this might be to set up puppet accounts and trade using their funds. Again, though, the public nature of the blockchain makes this ineffective; it would be trivial to trace funds from the original, compromised account to its puppets.

Coin mixing aims to solve this problem by enabling a batch of users to untraceably send coins to a batch of proxy addresses.

3.5. Problem Statement

The technologies described all seek to solve problems that arise when designing systems to facilitate peer-to-peer energy trading, but their confluence creates novel problems that have not been encountered elsewhere. Blockchain technology enables the creation of truly distributed markets, but necessarily (by design) makes transaction information public. In an energy distribution setting, this can lead to dangerous attacks on user privacy.

Duguma et al. [11] highlight the exact predicament that ILPTS is designed to address, which they refer to as the transparency–privacy dilemma. A transparent system with high

traceability will be safer, more trusted, and more regulatable, but such a system necessarily sacrifices privacy, as greater privacy would harm transparency. Similarly, though, it is difficult to abide by regulations (including GDPR, as they note) and gain consumer trust without ensuring privacy. Indeed, this paradox was also discovered during our review [5], and served as the impetus for developing ILPTS.

One solution to the privacy problem is to disconnect users' real identities from their trading accounts, as is proposed by Eisele et al. [10] in their TRANSAX protocol. This has the benefit of foiling privacy attacks based on trading or energy usage patterns, but introduces safety, fraud, and repudiation concerns. As Zhang et al. [29] note, blockchain-based TEMs remain vulnerable to market participant attacks such as misreporting prices or refusing to confer payment or energy.

Reputation mechanisms such as those described in Section 3.3 constitute a blunt instrument that can be used to identify users who are repeatedly participating in failed transactions, as either buyer or seller of energy [27]. This can be the result of fraud but, notably, can also occur as a result of equipment malfunction or user error. Reputation mechanisms only detect misuse; they do not address it. Most proposed schemes employ these mechanisms by either disconnecting users whose reputation falls below a certain threshold, or placing such users in a lower priority auction pool [28,29]. These options are not acceptable for a vital utility such as electricity [30].

Our scheme seeks to address this weakness by providing the DSO with the capacity to handle faulty users—who are detected using reputation to track transaction failures—with discretion via temporary deanonymization. The system aims to provide security, reliability, and privacy through its decentralized design and distributed onboarding process (design goals are discussed in more detail in Section 3.6). While the primary aim of ILPTS is to provide market privacy in a governable manner, it is also a step towards further decentralization of grid operations—a widely understood need [12,22,32–34]—and thus a more robust grid.

3.6. Design Requirements

This section introduces important requirements that must be met by a privacy-preserving scheme for transactive energy markets. These requirements were generated by analyzing previous research [5]. In particular, the security properties associated with the different threats and solutions mentioned throughout the TEM literature were evaluated in order to identify the most important properties for the system to have. These then influenced the research and development phase, where these features guided decisions about information flow, storage, and the role of different parties. They also influenced research directions, since many properties were only possible to achieve (given domain restrictions) using techniques from adjacent fields like cryptography [35] and distributed ledger technology [31].

1. **Trustless**: The system architecture supporting the scheme shall not rely on any participant being 100% honest.
2. **Distributed**: The scheme shall rely on as few central authorities as possible in order to function.
3. **Individual Identification**: The scheme shall allow an *individual* to be identified from their pseudonym; not just a batch of users.
4. **Total Anonymity**: When trading, users shall be anonymous to all parties, including the DSO.
5. **Transparency**: The operations performed should be transparent to all users to promote trust in the system and fellow participants.
6. **Restorable Privacy**: After a user has been identified, they shall be able to resume trading under a new pseudonym with total anonymity.
7. **Automated**: The process of registering, validating, deanonymizing, and reanonymizing users shall be automated and require no manual intervention.

8. **Snoop-Resistant**: A curious party shall be prevented from revealing the true identity of a particular pseudonym, regardless of their level of privilege in the system. This shall be true at every stage of the process, including registration and deanonymization.

4. Methodology

The following research methodology was used in this paper.

Previous Research. Previous research [5] was used for the initial stages of the project. It was during this review that the transparency-privacy dilemma in relation to market privacy was identified as a high priority security topic.

This survey and other literature related to TEM security were then mined to evaluate related schemes both to provide a foundation and ensure that a proposed solution did not already exist.

In addition, the material was used to determine features that would be of high priority for the scheme to have. These features were discussed previously in Section 3.6.

Design. With general structure for the solution in mind, the design process moves forward by ironing out the details of each process involved with the scheme, including (but not limited to) registration, communication paths, the roles of each element in the network, and deanonymization.

As each of these processes were clarified, it was important to ensure that security properties were maintained at every stage. As well, the scheme evolved in order to better align with the design requirements that were determined earlier.

A notable part of this process was examining cryptography literature to find techniques that would enable the design to confer certain properties. These include:

- Homomorphic encryption [36,37], which supports transparent and anonymous multi-party validation on-chain.
- Cryptographic shuffling [38], which supports transparent and anonymous batch registration.
- Shamir's Secret Sharing Scheme [35], which enables distributed storage of recovery information.

Evaluation. The features specified in the design requirements are used to evaluate the success of the design process (more detail in Section 6.1). The design is also evaluated against various existing and theoretical attacks (more detail in Section 6.2).

Often, evaluation would lead to design adjustments, and sometimes even research, so the methodology execution is more iterative than expressed here, but it provides an accurate overview of the process.

5. ILPTS Scheme

The purpose of our ILPTS scheme is to enable users to maintain anonymity on the TEM blockchain from all parties (including the DSO and other users) while still being able to be identified in edge cases. Additionally, it is important that this anonymity can be restored after they have been identified so that they may resume trading safely and privately.

5.1. Overview

Transactive energy market applications run using smart contracts to enable functions like trading, automatic auctions, market clearing, and transaction verification, among others.

Total anonymity in this case refers to the market participant being anonymous from all parties, including trading partners, other market participants, and the market operator (or DSO). This distinction is important because it is trivial to make a user anonymous to market participants while being visible to the market operator, but this sacrifices privacy. Similarly, making a user anonymous to all parties is possible at the expense of governance. Our ILPTS scheme seeks to achieve both goals.

First, anonymity is achieved using an existing cryptographic protocol known as *coin mixing* [31]. This process enables a batch of users on a blockchain to transfer their funds into new accounts that are not associated in any way with their original accounts. The

process, which will be described in greater detail in the following sections, is impenetrable even to the batch of users involved in the mix. In the context of a TEM, batches of market participants associated with particular smart meters can transfer their funds (in whatever form they may appear) into anonymous accounts that can trade on the market with no association—digital or physical—to the original identity, account, or meter.

This creates a problem in situations where identification may be desirable. To amend this, a secondary blockchain (or separate storage on the main chain) is employed to store recovery information. Since information on the chain is public, it is mandatory that this recovery information be protected. Fog nodes are employed to encrypt and, when necessary, decrypt this recovery information. However, if the recovery information consisted of an encrypted ID and pseudonym pair, then an individual fog node would be able to deanonymize users. This reduces the privacy benefit that is being aimed to achieve.

To combat this, the real identity of the users is split using another existing protocol, *Shamir's secret sharing scheme* [35], which allows information to be split in a secure but recoverable way, where a threshold number of parts are required to reconstruct the original information.

The users' real identities are split into n parts, each of which are then encrypted—by the user—using a different fog node's public key for each part.

The user then sends a tuple containing each of these encrypted parts along with their pseudonym to the smart contract, which activates the pseudonym and stores the parts and pseudonym on the recovery blockchain. This way, no individual fog node can deanonymize the user. However, if deanonymization becomes necessary, the smart contract can make a request to the fog nodes to decrypt their parts and send them to the DSO. Fog nodes are semi-trusted, as in not trusted to not snoop, but trusted to cooperate (send the correct information) lest they lose their privileged status.

This description is somewhat simplified. In reality, a batch of users must send their ID parts and pseudonyms together; otherwise it is trivial to see who sent which pseudonym to be activated. To facilitate this, a batch of users creates their ID part, pseudonym tuples. They then shuffle these among themselves using *cryptographic shuffling* [38], which enables them to create a master list of tuples where ID parts are correctly associated with pseudonyms, but no member of the batch knows which other member of the batch corresponds to which pseudonym.

It is this master list that is sent to the smart contract, who then sends each tuple to the recovery blockchain. However, before doing so, it performs a validation step. This step is to check that the ID parts being sent are indeed correlated with the real IDs of the users in the batch. It does so by homomorphically adding the ID parts associated with each fog node, then requesting these sums be decrypted by the fog nodes. These sums of parts can then be used to reconstruct the purported sum of the IDs using Shamir's secret sharing scheme. If this reconstructed sum matches the sum of the IDs in the batch of users, then validation is considered successful. At this point, the smart contract will activate the pseudonyms of all members of the batch and transmit their recovery data to the recovery blockchain and the registration process is complete.

This is a full description of onboarding. All data transmission happens on-chain via smart contract to support transparency and verifiability.

The deanonymization process is demonstrated schematically in Figure 1 as well. Pseudonymous user reputations are maintained in the recovery blockchain by the market application. Reputations decrease if a prosumer is part of a failed transaction and increase when a transaction is successful, as described by Zaman and He [27]. A smart contract monitors the reputation of all market participants (who are all using pseudonyms). If the reputation of a pseudonymous market participant falls below a threshold, the contract locates the pseudonym ① and associated ID partitions in the recovery blockchain. It then sends a signal ② to each fog node containing the pseudonym. The fog node requests its ID partition ③, decrypts it and sends it to the DSO ④, which can then use the decrypted ID partitions to reconstruct the pseudonymous user's real identity. The DSO can then

cross-reference the user's ID with its own registry to retrieve their contact information. (Note: this does not have implications for the user's future ability to use the service, as they will be assigned a new pseudonymous ID after the matter is resolved).

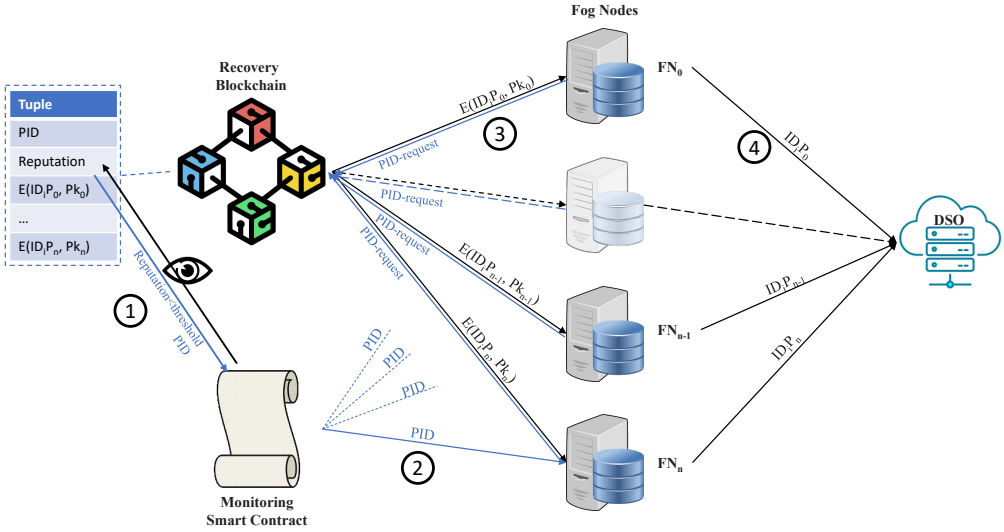


Figure 1. Deanonymization of a user under the ILPTS scheme.

From here, the DSO can investigate the cause of the user's reputation decline, which may be user error, hardware failure, or intentional hacking. It can then take appropriate actions. After a predetermined duration, the user can re-register on the market with a new pseudonym, recovering the ability to trade anonymously (until and unless their reputation declines again).

5.2. Formal Description

Here, we will describe the processes and algorithms in ILPTS formally for supporting implementations. The nomenclature used is defined in Table 2.

5.2.1. Onboarding

Initialization

The initialization process is as follows:

1. A batch of N_0 users with identifiers ID_0 through ID_N join.
2. A subset of n_0 fog nodes is requested, denoted FN_0 through FN_n.

Key Exchange

The key exchange process is as follows:

1. Fog nodes FN_0 through FN_n generate public keys Pk_0 through Pk_n respectively.
2. Each fog node FN_i sends its public key Pk_i to the smart contract SC.
3. The smart contract SC sends all n_0 public keys $Pk_0 - Pk_n$ to each of the users $ID_0 - ID_n$.

Registration

To begin the registration phase, users $ID_i \in B$ split their IDs and encrypt each part with a corresponding fog node's Pk. The user's pseudonym PID_i is appended to this list of encrypted parts. These tuples are then shuffled among the users so that no one user in the batch knows which ID parts are associated with which real ID (which would break security). The tuples are ultimately sent to the smart contract.

The registration process is detailed in Algorithm 1.

Table 2. Nomenclature.

ID_i	real ID of i^{th} user
ID_ip_j	part j of ID_i
FN_i	i^{th} fog node
Pk_i	Pk of fog node FN_i
Pk_i^u	Pk of i^{th} user ID_i
PK^B	list of Pks in batch B
PID_i	pseudonym of user ID_i
$\oplus$	homomorphic addition
SC	smart contract
$E(X, Pk)$	cyphertext of X encrypted using Pk
n_0	divisions of data
n	max FN ID when registering $(n_0 - 1)$
k_0	threshold to reconstruct data
k	max FN ID when deanonymizing $(k_0 - 1)$
B	batch of users registering
N_0	number of users in batch
N	max user ID when registering $(N_0 - 1)$
$X \rightarrow Y : W$	X sends W to Y
$X \leftarrow Y : Z$	X receives Z from Y
ω_i	registration data of i^{th} user
Ω	list containing registration data
Ω_i	state of list Ω at i^{th} user
$Shuffle(Y)$	randomize order of elements in list Y
$Partition(X)$	use [35] to generate $\gamma = [Xp_0, \ldots, Xp_n]$

Algorithm 1 Registration.

Input: n_0 ▷ number of FNs and ID parts
Input: $B = [ID_0 \ldots ID_N]$ ▷ batch of user IDs
Output: $\Omega = [\omega_0 \ldots \omega_N]$ ▷ list of recovery tuples
for each $ID_i \in B$ **do** ▷ IDs in batch
  $\omega_i := Partition(ID_i) = [ID_ip_0, \ldots, ID_ip_n]$ ▷ list of ID parts
  for each $ID_ip_j \in \omega_i$ **do** ▷ ID parts in list
    $\omega_i[ID_ip_j] = E(ID_ip_j, Pk_j)$
  end for ▷ replace ID parts with encrypted ID parts
  $\omega_i := append(\omega_i, PID_i)$ ▷ append pseudo ID
  ID_i: generate Pk_i^u, Vk_i^u ▷ user keys
  $ID_i \rightarrow B$: Pk_i^u ▷ broadcast Pk_i^u to batch B
  $ID_i \leftarrow B$: $PK^B \ni Pk_{i-1}^u, \ldots, Pk_{i-i}^u$ ▷ retrieve all previously generated Pk^u from batch B
  for each $Pk_j^u \in PK^B$ **do** ▷ Pks currently available in batch
    $\omega_i = E(\omega_i, Pk_j^u)$ ▷ sequentially encrypt ω_i with each $Pk^u \in PK^B$
  end for
  $ID_i \leftarrow B$: Ω_{i+1} ▷ ID_i will wait until ID_{i+1} makes this available
  for each $E(\omega_j, Pk_i^u) \in \Omega_{i+1}$ **do** ▷ encrypted lists in batch list
    decrypt$(E(\omega_j, Pk_i^u)) \rightarrow \omega_j$ using Vk_i^u
    $\Omega_{i+1}[E(\omega_j, Pk_i^u)] = \omega_j$ ▷ replace encrypted list with list
  end for
  $\Omega_i = \Omega_{i+1}$
  $\Omega_i.append(\omega_i)$ ▷ append current user tuple to batch list
  $Shuffle(\Omega_i)$
  $ID_i \rightarrow B$: Ω_i ▷ send updated batch list to batch
end for

Validation

The validation phase must ensure that the encrypted data being sent do indeed contain the real IDs of the users without revealing those data. To initiate this process, the contract homomorphically sums the parts of each tuple corresponding to each fog node and sends each of these sums to its respective fog node. Each fog node decrypts its sum and sends

this back to the smart contract. The smart contract then reverses the splitting process and reconstructs a number. This number is checked for equality against the sum of the real IDs of all of the users in the batch. If the equality check succeeds, the information is considered accurate and the pseudonyms can be activated.

The validation process is detailed in Algorithm 2.

Algorithm 2 Validation.

Input: n_0 ▷ number of FNs and ID parts
Input: Ω ▷ batch list of tuples
Output: Ω ▷ validated batch list of tuples
Initialize: $\Lambda = [\lambda_0 = E(0, Pk_0), \ldots, \lambda_n = E(0, Pk_n)]$ ▷ homomorphically encrypted 0s
for each $\lambda_j \in \Lambda$ **do** ▷ one for each FN
  for each $\omega_i \in \Omega$ **do** ▷ user tuples in batch list
    $\lambda_j = \oplus(\lambda_j, E(ID_i p_j, Pk_j))$ ▷ homomorphically sum ID parts encrypted by FN_j
  end for
  $\lambda_j = \sum_{i=0}^{n} E(ID_i p_j, Pk_j)$ ▷ sums of ID parts encrypted by each FN
  $SC \rightarrow FN_j$: λ_j ▷ send each FN their sum
  FN_j: decrypt$(\lambda_j) \rightarrow \sum_{i=0}^{n} ID_i p_j$
  $FN_j \rightarrow SC$: $\sum_{i=0}^{n} ID_i p_j$ ▷ send decrypted sum to SC
  $\Lambda[\lambda_j] = \sum_{i=0}^{n} ID_i p_j$ ▷ replace encrypted sums with sums
end for
$\phi \leftarrow Partition^{-1}(\Lambda)$ ▷ reconstruct sum of IDs by reversing secret scheme [35]
if $\phi = \sum_{i=0}^{n} ID_i$ **then** ▷ if reconstructed sum equals sum of known IDs
  Validation Successful
else
  Validation Failed
end if

Finalization

Once validation is successful, the identity recovery data will be sent onto the recovery blockchain for storage and retrieval. The pseudonyms of the users in the batch will be activated on the market blockchain.

Storage of recovery data: $SC \rightarrow BC : \Omega$

Activation of pseudonymous users: Activate$(PID_0, \ldots, PID_N)$

5.2.2. Deanonymization

Detection

Pseudonymous user PID_i's reputation score is updated after each transaction they participate in. This score is stored on the recovery blockchain along with their PID and recovery data (see Tuple in Figure 1). If PID_i is the seller and fails to provide energy, their score will decrease. If they are the buyer and fail to provide payment, their score will decrease. Otherwise, their score will increase. The exact algorithm used for this adjustment (such as Q-Score [27]) is not relevant to ILPTS; it suffices that the adjustment is performed.

The monitoring smart contract (Figure 1) tracks the reputation of each pseudonymous user as the auction is cleared at each iteration of the market (i.e., when transactions are executed). When the reputation is found to be below a particular threshold, the smart contract automatically initiates the deanonymization protocol.

Deanonymization

Deanonymization is performed as follows:

1. When the smart contract finds a reputation value below the threshold, it sends the PID of the offending pseudonymous user PID_i to all fog nodes.
2. Each fog node FN_j then retrieves the appropriate encrypted ID part $E(ID_i p_k, Pk_j)$ from the tuple containing PID_i on the recovery blockchain.

3. Each fog node FN_j uses its private key Vk_j to decrypt $E(ID_ip_k, Pk_j)$, producing ID_ip_k.
4. The fog nodes each send this plaintext to the DSO.
5. The DSO then performs $Partition^{-1}(ID_ip_0, \ldots, ID_ip_k0) = ID_i$.
6. The DSO can now use its customer database to retrieve ID_i's contact details and resolve the abnormality.

5.3. Full Sequence Diagrams

Figure 2 shows, using a sequence diagram, the process of deanonymizing a user when their reputation falls below the threshold. While Figure 1 illustrates the operation well conceptually, Figure 2 better visualizes the flow of information between participants. Figure 3 shows the secure registration process involving the users in the registration batch, the verifying fog nodes, and the smart contract coordinating the process. Included in this as well is the validation process that ensures users are submitting their real IDs for recovery in the future.

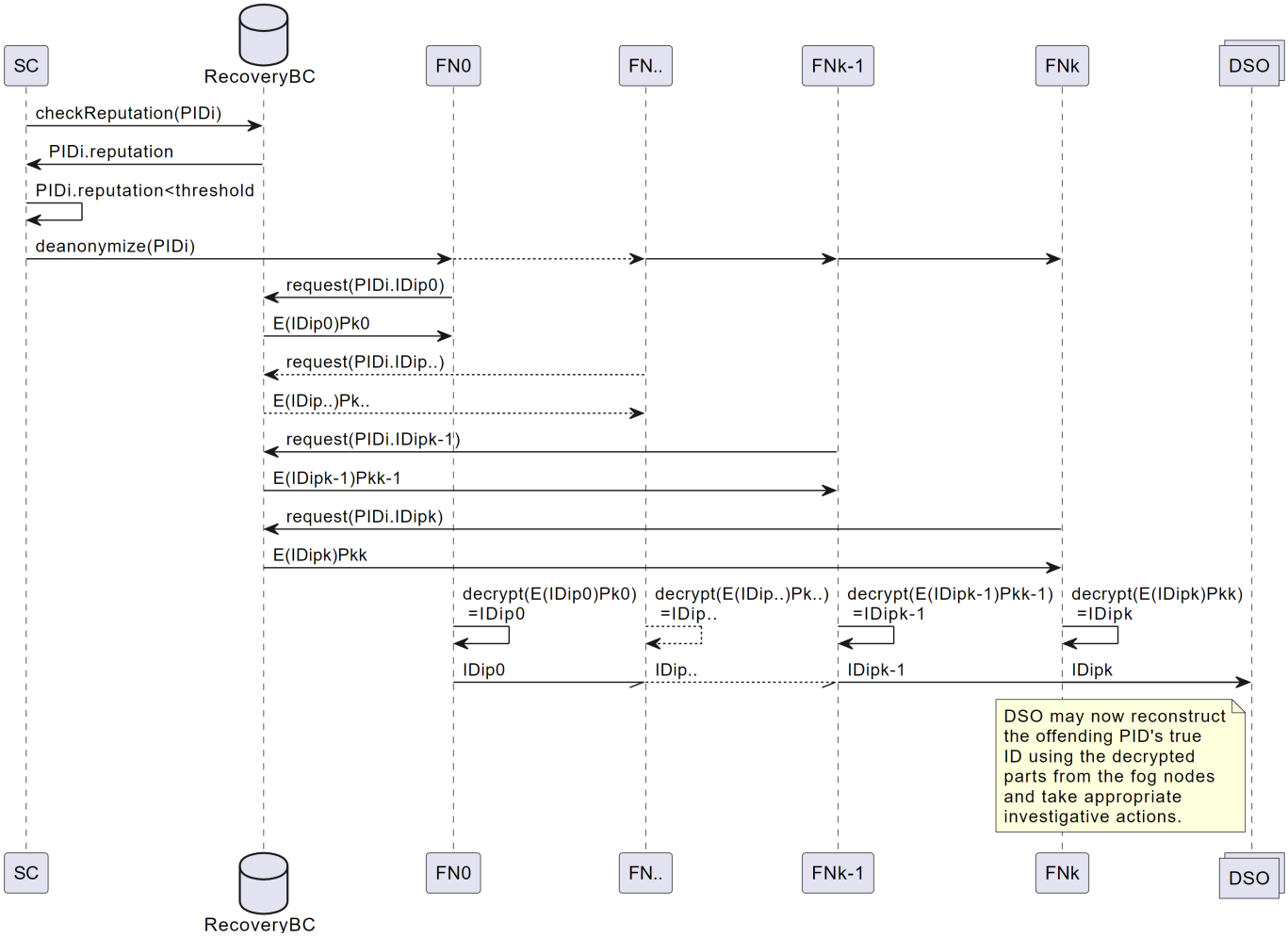


Figure 2. Sequence diagram of the deanonymization phase.



Figure 3. Sequence diagram of the registration phase, operating on a batch of 3 users and 3 fog nodes.

6. Discussion and Analysis

This section first assesses how well the requirements from Section 3.6 are met by ILTPS, and then reports on an informal security analysis of this proposed scheme.

6.1. Design Evaluation against Requirements

1. **Trustless**: The system successfully achieves a nearly trustless architecture. Registration and deanonymization are both automated and distributed, meaning no central authority or trusted third party is required. The only trust involved is that the fog nodes will correctly decrypt and forward the appropriate information to the DSO during deanonymization, but they are incentivized to do so, as we discuss in Section 6.2. Fog nodes could theoretically collude to deanonymize individual users, but due to the properties of the secret sharing scheme employed, such an attack would require k or more malicious nodes [35].

2. **Decentralized**: The registration process requires a blockchain, which is decentralized by nature, smart contracts, and fog nodes—no central authority. From this perspective, the scheme succeeds at this design goal. The fog nodes are semi-trusted; however, only a subset are required and they are interchangeable to a point. The monitoring and deanonymization processes are handled entirely by a smart contract and fog nodes. The information is of course transmitted to the DSO, but the process of deanonymizing the user for them is entirely automated and distributed. Moreover, the information sent to the DSO is not pre-reconstructed, making it less vulnerable to attacks (which we discuss in Section 6.2).
3. **Individual Identification**: ILTPS successfully allows users to sign up in batch, with validation that does not compromise the anonymity of their pseudonym, while still enabling individual identification when necessary.
4. **Total Anonymity**: Total anonymity is achieved since the true identities of the pseudonyms are split into many pieces which are each encrypted by different fog nodes. This property is important because previous schemes have had to decide between sacrificing a level of anonymity (by registering with the DSO) or traceability (having no mechanism to identify a pseudonym).
5. **Transparency**: The registration and validation process happen entirely on-chain and automatically, providing assurance to market participants that their peers have been honestly validated. In addition, the recovery blockchain is publicly visible and read-only, so manipulation is both improbable and detectable.
6. **Restorable Privacy**: A user can be reanonymized by simply undergoing the registration process again. If no new users are being added, a subset of existing users can be re-registered automatically to facilitate the batch registration process.
7. **Automated**: All information exchange and validation are handled automatically by an on-chain smart contract, fulfilling this design goal. Additionally, reputation monitoring and requests to fog nodes to deanonymize a target user are also handled automatically by a smart contract.
8. **Snoop-Resistant**: This design goal is achieved because the deanonymization process is initiated by the smart contract. The contract is written in such a way that manually initiating this process is not possible; it only occurs when a user's reputation is detected to have fallen below a certain threshold.

Overall, ILPTS achieves the primary objective of providing total anonymity while maintaining safety. The system successfully enables total anonymity while simultaneously retaining a link to the pseudonymous user's original identity. Users in markets employing this scheme will have their identities protected from all parties, including the DSO. The lack of centralized storage of links means that there is no single target for attackers, nor an internal leakage threat. Using a smart contract to monitor reputations and activate the deanonymization policy prevents the policy from creating a potential attack surface [22]; as long as the blockchain remains secure (a reasonable assumption), the policy will be protected.

6.2. Threat Analysis

This section evaluates how ILPTS handles certain attacks, highlights its security properties, and discusses attack methods that may be unique to the scheme.

6.2.1. Trust

It can be seen that our ILPTS scheme successfully pulls off private *and* regulatable market activities with validation, all without trusted parties.

Fog nodes are not trusted not to snoop (hence the splitting of IDs), but are trusted to send information when requested. While this is a form of trust, it is reasonable [39] given the following:

- Failure to oblige will cost their privileged status in the network, creating an implicit incentive to comply.

- Only k of n fog nodes need to comply (and not fault) in order for deanonymization to be successfully performed, meaning that some number of nodes could, in fact, maliciously not comply without affecting the integrity of the scheme. This ratio can be set arbitrarily by the DSO to their desired security level.

While fog nodes do have privileged status in the scheme, they do not need to be fully trusted nor do they all need to be trustworthy even simply with compliance. In addition, as stated, while there is no incentive for them not to snoop, doing so would not reveal any information.

6.2.2. Reputation Attack

In a reputation attack, a user could potentially configure their smart meter settings to ensure trading is carried out with a particular prosumer, and then cause those transactions to fail consistently leading to a decline in reputation for the victim. Luckily, in our system, the consequences of such an action are significantly reduced, since it would only cause an investigation rather than a wholesale ban from the market. As can be seen in Section 5, the anonymity of the user can easily be restored by re-registering with a new batch. Newly acquired anonymity is not damaged by past activation of the protocol; it is totally restored to its original state and even an individual at the DSO would not be able to trace a user between market identities.

6.2.3. Man-in-the-Middle Attack

There are several locations at which communication could be intercepted during each phase of the scheme. These include:

(A) $SM \rightarrow SC$ during registration
(B) $SC \rightarrow FN$ during registration
(C) $FN \rightarrow BC$ during registration
(D) $BC \rightarrow FN$ during deanonymization
(E) $FN \rightarrow DSO$ during deanonymization

Concerning locations A through D, there is little risk even if communication is intercepted. This is due to the fact that all information at these stages is both split and encrypted with multiple different keys, making the information inaccessible unless k fog nodes were to collude [35].

The greatest risk lies in location E; when the fog nodes send the ID parts to the DSO. This can be mitigated by encrypting the information with a public key from the DSO, but this is less secure than the multiple stages of encryption during the registration process. A positive confounding factor is that this does require multiple points of interception (specifically between k fog nodes and the DSO).

An *inside job* at the DSO is not a risk since the DSO cannot manually initiate the deanonymization protocol for an arbitrary user [22].

6.2.4. Robustness to Failure

SM Failure

Failure of a smart meter in the network would not impact ILPTS, because the protocol only relies on fog nodes (and the blockchain they support) to function. In fact, a failed smart meter should trigger the ILPTS protocol, leading the DSO to provide support in an automated and timely fashion.

Fog Node Failure

While the ID data associated with a particular PID are split into n parts, only k parts are required to recover it. This means that only k fog nodes need to be responsive at the time of deanonymization in order for the process to succeed.

These numbers can be tuned to suit the design requirements of the DSO and network infrastructure at a particular location to maximize reliability. For example, $n = 30, k = 10$ would mean that only $1/3$ of the fog nodes need to be responsive in order for ILPTS to

operate. Since the participation of a fog node demands few resources, it is feasible to include a high degree of redundancy.

Other Network Failures

Internet or total network outages would interrupt the functioning of ILPTS. However, in these situations, it would likely be the case that transactions would not be occurring either, removing the need for the system in the first place.

Because the state of the system is stored on-chain (state meaning reputations and PID–recovery data pairings), it will not be destroyed by a network outage. Rather, the system will resume operating as normal once the network issue is resolved.

Finally, since ILPTS operates in a distributed manner (including the system state, execution, and recovery data), localized network outages will not interrupt its operation—an important benefit of the system.

6.2.5. Collusion

A collusion attack is possible with the participation of at least k fog nodes as well as the DSO. Since the recovery blockchain is public, a subset k of the fog nodes could conspire to decrypt the ID parts of a particular PID and reconstruct their real ID. This alone does not provide much information, but the ID parts or real ID could be sent to the DSO, who could then recover the personal information of the affected pseudonymous user based on their ID.

This presents a tradeoff between reliability and security, where having a smaller number for k may provide greater reliability (by requiring fewer fog nodes to be online during execution) but simultaneously making a collusion attack easier. These factors would have to be considered given the specific network infrastructure at a particular TEM location.

Despite this, the collusion of a large number of fog nodes along with an insider at the DSO (something which would break most security implementations) is highly unlikely, especially considering that all parties have incentives to be honest (as discussed in Section 6.2.1).

6.3. Synergies

ILPTS can be used independently to provide anonymity on the transaction ledger in a safe, distributed, and ethical manner. However, it can also be used cohesively with other security solutions designed for transactive energy markets.

For example, TRANSAX [10], which we discussed earlier, would benefit directly from being used in conjunction with ILPTS. This combination would allow TRANSAX to continue offering its boundary safe anonymity, while mitigating the negative effects associated with group-level identification. Aside from platforms, ILPTS can work with other security-enhancing protocols, such as A-PoL [23], to further harden the security of a larger model.

Another example of this is a solution we previously developed called cyclic homomorphic encryption aggregation (CHEA) [40]. CHEA contributes to the security provided by ILPTS by protecting the dual of the information at risk on the transaction ledger: the energy consumption data produced and sent by the smart meters themselves. This information exfiltrated from either source can be cross referenced to identify a prosumer or used independently to invade their privacy. Thus, the combined effect of these schemes is to enhance this privacy from both directions.

Additionally, the unique properties of each scheme reinforce each other. For example, CHEA is an aggregation scheme that does not require fog nodes. Limiting the role of fog nodes in this way enhances overall security by reducing the trust requirements of each node; in particular, CHEA combined with ILPTS involves fog nodes *only* in the protection of identity recovery information. ILPTS used with traditional aggregation schemes would mean that fog nodes are involved in processing both channels of usage information, increasing the risk of collusion or malicious behaviour.

6.4. Improvements

ILPTS was initially designed with the intention of employing fog nodes to provide computational and storage resources while maintaining a distributed environment to reduce trust requirements and enhance reliability.

A goal throughout was to reduce the role of the fog nodes by structuring the scheme such that most if not all of the data could be kept on the blockchain. This was to decrease reliance on fog nodes, lower the chances of critical failure, and also to reduce the computational demands of the nodes. By the final stage of the ILPTS' development, the role of the fog nodes, from a processing and storage standpoint, had become limited enough that allowing the role to be handled by smart meters themselves became a consideration.

Replacing the fog nodes would require additional considerations beyond the scope of this work, but the basic idea would be to require each smart meter to generate a set of keys to be used when they are required to fulfill the *fog node* role in either of the policies. Registration and deanonymization would look largely similar, with a separate subset of smart meters replacing the fog nodes.

This concept confers benefits including increased reliability due to greater redundancy (as there are more smart meters to pull from than fog nodes), reduced collusion potential, and decreased infrastructural requirements. On the other hand, such a modification would need to take into account the reduced computational capacity of smart meters, mechanisms for ensuring a viable subset is available, fault tolerance, and the fact that smart meters often may be busy with other tasks.

7. Conclusions and Future Work

Our market privacy solution (ILPTS) aims to provide privacy, safety, and security to prosumers participating in a blockchain-based transactive energy market beyond that of existing solutions, in part by addressing the transparency–privacy dilemma. These goals have been achieved and ILPTS will serve to enhance prosumer safety, regulatory compliance, and market adoption of TE solutions.

A limitation of the work is that the scheme was not tested experimentally, either via implementation or software simulation, so security results are based solely on formal analysis. In particular, it was found by formal analysis that the ILPTS privacy solution successfully creates an environment where the design specifications are met, namely:

- Users are totally anonymous to all parties;
- This anonymity can be uncovered only by an autonomous system under specific circumstances;
- Anonymity can be restored when required;
- The solution does not contain centralized vulnerabilities.

This solution improves equity and ability to regulate in a TE environment, reducing the risk of fraud and the need for coarse punitive measures like priority pooling or disconnection.

Future work should include (ideally in situ) simulations of the solution and cyberattacks that may be performed, to further verify the robustness of the scheme proposed. This would necessitate creating a functional version of the scheme, with an appropriate blockchain environment, smart contract code, and client code, another future challenge. Finally, exploration of a further decentralized scheme, as discussed in Section 6.4, could prove an interesting research direction.

Author Contributions: Conceptualization, A.R.-K., D.A., D.S.-D. and J.M.; methodology, D.S.-D. and D.A.; formal analysis, D.S.-D.; investigation, D.S.-D.; data curation, D.S.-D.; writing—original draft preparation, D.S.-D. and D.A.; writing—review and editing, A.R.-K., J.M., D.S.-D. and D.A.; supervision, D.A., J.M. and A.R.-K.; project administration, D.A., J.M. and A.R.-K.; funding acquisition, D.A. and J.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the ORF-RE project "CyPreSS: Software Techniques for the Engineering of Cyber-Physical Systems", as well as by an NSERC Discovery Grant titled "Engineering Requirements for Socio-Technical Systems".

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

Acknowledgments: The authors thank Luigi Logrippo for feedback on this work and for providing pointers to useful references. We also thank Javad Fattahi for taking the time to examine this project and sharing his expertise with us.

Conflicts of Interest: Author Ashkan Rahimi-Kian was employed by the company IEMS Solution Ltd. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AMI	Advanced Metering Infrastructure
A-PoL	Anonymous Proof of Location
CHEA	Cyclic Homomorphic Encryption Aggregation
DSO	Distributed System Operator
EV	Electric Vehicle
FN	Fog Node
HE	Homomorphic Encryption
ID	Identifier
ILPTS	Individually Linkable Pseudonymous Trading Scheme
PID	Pseudonymous ID
SG	Smart Grid
SM	Smart Meter
TE	Transactive Energy
TEM	Transactive Energy Market
VPP	Virtual Power Plant

References

1. Lombardi, F.; Aniello, L.; De Angelis, S.; Margheri, A.; Sassone, V. A Blockchain-based Infrastructure for Reliable and Cost-effective IoT-aided Smart Grids. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018. [CrossRef]
2. Uribe-Pérez, N.; Hernández, L.; De la Vega, D.; Angulo, I. State of the Art and Trends Review of Smart Metering in Electricity Grids. *Appl. Sci.* **2016**, *6*, 68. [CrossRef]
3. Hassan, A.; Afrouzi, H.N.; Siang, C.H.; Ahmed, J.; Mehranzamir, K.; Wooi, C.L. A survey and bibliometric analysis of different communication technologies available for smart meters. *Clean. Eng. Technol.* **2022**, *7*, 100424. [CrossRef]
4. Chen, T.; Alsafasfeh, Q.; Pourbabak, H.; Su, W. The Next-Generation U.S. Retail Electricity Market with Customers and Prosumers–A Bibliographical Survey. *Energies* **2018**, *11*, 8. [CrossRef]
5. Sousa-Dias, D.; Amyot, D.; Rahimi-Kian, A.; Mylopoulos, J. A Review of Cybersecurity Concerns for Transactive Energy Markets. *Energies* **2023**, *16*, 4838. [CrossRef]
6. Kirli, D.; Couraud, B.; Robu, V.; Salgado-Bravo, M.; Norbu, S.; Andoni, M.; Antonopoulos, I.; Negrete-Pincetic, M.; Flynn, D.; Kiprakis, A. Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renew. Sustain. Energy Rev.* **2022**, *158*, 112013. [CrossRef]
7. Khan, H.; Masood, T. Impact of Blockchain Technology on Smart Grids. *Energies* **2022**, *15*, 7189. [CrossRef]
8. Asghar, M.R.; Dán, G.; Miorandi, D.; Chlamtac, I. Smart Meter Data Privacy: A Survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2820–2835. [CrossRef]
9. McDaniel, P.; McLaughlin, S. Security and Privacy Challenges in the Smart Grid. *IEEE Secur. Priv.* **2009**, *7*, 75–77. [CrossRef]
10. Eisele, S.; Eghtesad, T.; Campanelli, K.; Agrawal, P.; Laszka, A.; Dubey, A. Safe and Private Forward-Trading Platform for Transactive Microgrids. *ACM Trans. Cyber-Phys. Syst.* **2021**, *5*, 1–29. [CrossRef]
11. Duguma, D.G.; Zhang, J.; Aboutalebi, M.; Zhang, S.; Banet, C.; Bjørkli, C.; Baramashetru, C.; Eliassen, F.; Zhang, H.; Muringani, J.; et al. Privacy-preserving transactive energy systems: Key topics and open research challenges. *arXiv* **2023**, arXiv:2312.11564.
12. Sharma, G.; Joshi, A.M.; Mohanty, S.P. sTrade: Blockchain based secure energy trading using vehicle-to-grid mutual authentication in smart transportation. *Sustain. Energy Technol. Assess.* **2023**, *57*, 103296. [CrossRef]

13. Garg, S.; Kaur, K.; Kaddoum, G.; Gagnon, F.; Rodrigues, J.J.P.C. An Efficient Blockchain-Based Hierarchical Authentication Mechanism for Energy Trading in V2G Environment. In Proceedings of the 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]
14. Li, D.; Yang, Q.; An, D.; Yu, W.; Yang, X.; Fu, X. On Location Privacy-Preserving Online Double Auction for Electric Vehicles in Microgrids. *IEEE Internet Things J.* **2019**, *6*, 5902–5915. [CrossRef]
15. Li, D.; Yang, Q.; Yu, W.; An, D.; Yang, X.; Zhao, W. A strategy-proof privacy-preserving double auction mechanism for electrical vehicles demand response in microgrids. In Proceedings of the 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, USA, 10–12 December 2017; pp. 1–8. [CrossRef]
16. Baza, M.; Amer, R.; Rasheed, A.; Srivastava, G.; Mahmoud, M.; Alasmary, W. A Blockchain-Based Energy Trading Scheme for Electric Vehicles. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–7. [CrossRef]
17. Baza, M.; Sherif, A.; Mahmoud, M.M.E.A.; Bakiras, S.; Alasmary, W.; Abdallah, M.; Lin, X. Privacy-Preserving Blockchain-Based Energy Trading Schemes for Electric Vehicles. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9369–9384. [CrossRef]
18. Bergquist, J.; Laszka, A.; Sturm, M.; Dubey, A. On the Design of Communication and Transaction Anonymity in Blockchain-Based Transactive Microgrids. In Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers (SERIAL '17), New York, NY, USA, 11–15 December 2017. [CrossRef]
19. Laszka, A.; Dubey, A.; Walker, M.; Schmidt, D. Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers. In Proceedings of the Seventh International Conference on the Internet of Things, Linz, Austria, 22–25 October 2017. [CrossRef]
20. Khorasany, M.; Dorri, A.; Razzaghi, R.; Jurdak, R. Lightweight blockchain framework for location-aware peer-to-peer energy trading. *Int. J. Electr. Power Energy Syst.* **2021**, *127*, 106610. [CrossRef]
21. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2021**, *8*, 18–43. [CrossRef]
22. Ziu, D.; Verber, M.; Croce, V. iVPP P2P Transactive Energy Framework, 2022. EU Horizon 2020 Project IANOS, Deliverable D4.9. Available online: https://ianos.eu/wp-content/uploads/2022/09/IANOS_D4.9.pdf (accessed on 1 May 2024).
23. Kang, E.S.; Pee, S.J.; Song, J.G.; Jang, J.W. A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid. In Proceedings of the 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, Japan, 27–30 April 2018; pp. 472–476. [CrossRef]
24. Honari, K.; Rouhani, S.; Falak, N.E.; Liu, Y.; Li, Y.; Liang, H.; Dick, S.; Miller, J. Smart Contract Design in Distributed Energy Systems: A Systematic Review. *Energies* **2023**, *16*, 4797. [CrossRef]
25. Münsing, E.; Mather, J.; Moura, S. Blockchains for decentralized optimization of energy resources in microgrid networks. In Proceedings of the 2017 IEEE Conference on Control Technology and Applications (CCTA), Kohala Coast, HI, USA, 27–30 August 2017; pp. 2164–2171. [CrossRef]
26. Buterin, V. Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. 2013. Available online: https://ethereum.org/en/whitepaper/ (accessed on 1 May 2024).
27. Zaman, I.; He, M. A Multilayered Semi-Permissioned Blockchain Based Platform for Peer to Peer Energy Trading. In Proceedings of the 2021 IEEE Green Technologies Conference (GreenTech), Virtual, 7–9 April 2021; pp. 279–285. [CrossRef]
28. Nazari, M.; Khorsandi, S.; Babaki, J. Security and Privacy Smart Contract Architecture for Energy Trading based on Blockchains. In Proceedings of the 2021 29th Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, 18–20 May 2021; pp. 596–600. [CrossRef]
29. Zhang, P.; Wu, P.; Liu, Y.; Chen, Y.; Li, Y.; Yan, J.; Ghafouri, M. Toward a Blockchain-Based, Reputation-Aware Secure Transactive Energy Market. *Blockchains* **2024**, *2*, 61–78. [CrossRef]
30. Jayachandran, M.; Rao, K.P.; Gatla, R.K.; Kalaivani, C.; Kalaiarasy, C.; Logasabarirajan, C. Operational concerns and solutions in smart electricity distribution systems. *Util. Policy* **2022**, *74*, 101329. [CrossRef]
31. Ruffing, T.; Moreno-Sanchez, P.; Kate, A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In Proceedings of the Computer Security—ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, 7–11 September 2014; Kutyłowski, M., Vaidya, J., Eds.; Springer International Publishing: Cham, Switzerland, 2014; pp. 345–364.
32. Chen, G.; He, M.; Gao, J.; Liu, C.; Yin, Y.; Li, Q. Blockchain-Based Cyber Security and Advanced Distribution in Smart Grid. In Proceedings of the 2021 IEEE 4th International Conference on Electronics Technology (ICET), Chengdu, China, 7–10 May 2021; pp. 1077–1080. [CrossRef]
33. Afzal, M.; Li, J.; Amin, W.; Huang, Q.; Umer, K.; Ahmad, S.A.; Ahmad, F.; Raza, A. Role of blockchain technology in transactive energy market: A review. *Sustain. Energy Technol. Assess.* **2022**, *53*, 102646. [CrossRef]
34. Zhuang, P.; Zamir, T.; Liang, H. Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey. *IEEE Trans. Ind. Inform.* **2021**, *17*, 3–19. [CrossRef]
35. Shamir, A. How to Share a Secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
36. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In Proceedings of the Advances in Cryptology — EUROCRYPT '99: International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999; Stern, J., Ed.; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238.

37. Paillier, P.; Pointcheval, D. Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries. In Proceedings of the Advances in Cryptology—ASIACRYPT'99, Singapore, 14–18 November 1999; Lam, K.Y., Okamoto, E., Xing, C., Eds.; Springer: Berlin/Heidelberg, Germany, 1999; pp. 165–179.
38. Chaum, D.L. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Commun. ACM* **1981**, *24*, 84–90. [CrossRef]
39. Song, Z.; Zhong, W.; Zhou, T.; Chen, D.; Ding, Y.; Yang, X. SEMDA: Secure and Efficient Multidimensional Data Aggregation in Smart Grid without a Trusted Third Party. *Secur. Commun. Netw.* **2023**, *2023*, 6693296. [CrossRef]
40. Sousa-Dias, D.; Amyot, D.; Rahimi-Kian, A.; Bashari, M.; Mylopoulos, J. Cyclic Homomorphic Encryption Aggregation (CHEA)—A Novel Approach to Data Aggregation in the Smart Grid. *Energies* **2024**, *17*, 878. [CrossRef]

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.