mathematics

MDPI

Article

A Reliable and Privacy-Preserving Vehicular Energy Trading Scheme Using Decentralized Identifiers

Myeonghyun Kim [1], Kisung Park [2,*] and Youngho Park [1,*]

[1] School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, Republic of Korea; kimmyeong123@knu.ac.kr
[2] Department of Computer Engineering (Smart Security), Gachon University, Seongnam 13120, Republic of Korea
* Correspondence: kisung@gachon.ac.kr (K.P.); parkyh@knu.ac.kr (Y.P.)

Abstract: As the usage of electric vehicles (EVs) expands, various energy management technologies, including battery energy storage systems, are being developed to efficiently charge EVs using various energy sources. In recent years, many blockchain-based energy trading schemes have been proposed for secure energy trading. However, existing schemes cannot fully solve privacy issues and security problems during energy trading. In this paper, we propose a reliable and privacy-preserving vehicular energy trading scheme utilizing decentralized identifier technology. In the proposed scheme, identity information and trading result information are not revealed publicly; this is due to the use of decentralized identifiers and verifiable credential technologies. Additionally, only parties who have successfully conducted energy trading can manage complete transaction information. We also demonstrate our method's security and ensure privacy preservation by performing informal and formal security analyses. Furthermore, we analyze the performance and security features of the proposed scheme and related works and show that the proposed scheme has competitive performance.

Keywords: vehicular energy trading; decentralized identifier; blockchain; verifiable credential; authentication

MSC: 68M12

Citation: Kim, M.; Park, K.; Park, Y. A Reliable and Privacy-Preserving Vehicular Energy Trading Scheme Using Decentralized Identifiers. *Mathematics* **2024**, *12*, 1450. https://doi.org/10.3390/math12101450

Academic Editors: Cheng-Chi Lee and Dinh-Thuan Do

Received: 9 April 2024
Revised: 3 May 2024
Accepted: 6 May 2024
Published: 8 May 2024

1. Introduction

As the urgency to transition to eco-friendly transportation systems grows in the near future to significantly reduce fossil fuel consumption and CO_2 emissions, electric vehicles (EVs) have become critical as a primary mode of transportation by offering emission-free operation. However, the widespread distribution of EVs is creating problems for EV users, who are limited in time and space to charge their EVs. To address these issues and ensure smooth travel for EV users, it is necessary to expand the EV charging infrastructure, which may involve converting existing fossil fuel gas stations into electric-only charging stations and/or constructing new charging stations [1,2].

Specifically, the progress of smart grid (SG), energy management, and internet of vehicle (IoV) technologies enables EVs to charge everywhere from various energy resources, such as a grid stations, homes, and other vehicles [3–7]. However, despite the expansion of the EV market with the technologies mentioned above, the charging infrastructure remains at a preliminary stage in terms of commercialization. According to a report published by the (IEA) in 2020, the number of electric vehicles was estimated to reach 7.2 in 2019. In contrast, the number of charging stations was estimated to be approximately 0.8 million [8]. Furthermore, a market research report indicated that many countries face a shortage of charging stations compared to the growing demand for EVs [9]. Given that EVs are characterized by high mobility and unpredictability, energy demand can become concentrated based

on the time and location of operation. Integrating the energy flow for EVs into existing power grids can lead to issues like peak load increases, power loss, and voltage drops during charging and discharging processes. Consequently, high demand for EV charging, combined with inadequate infrastructure, can have severe negative impacts on existing smart grids [10,11]. Recently, to address these challenges, energy trading approaches that utilize smart grid technology such as battery energy storage systems have been researched in order to enable energy to be sourced from external sources rather than relying solely on existing power grids [12,13].

Several energy trading schemes for vehicular energy trading systems [14,15] have been proposed to provide reliable energy management. These schemes, on the one hand, offer an energy trading service based on a centralized infrastructure. However, because their scheme does not account for charging station overload, it is difficult to provide reliable service. Additionally, significant privacy concerns arise as the central authority node, which manages users' personal data and arranges energy transactions, is exposed to potential adversary attacks. In addition, communications regarding vehicular energy trading are performed on wireless channels, which can be exposed to various threats by attackers, such as impersonation attacks, replay attacks, and man-in-the-middle attacks. If the personal information is leaked to a malicious attacker, the attacker can conjecture the home, workplace, and hobbies of the driver [16–18]. Therefore, a secure authentication protocol is necessary.

Recently, research for decentralized energy trading systems [19–22] has been presented to resolve the security issues of a centralized system. A blockchain is regarded as a trusted distributed ledger that ensures data integrity and decentralization. In previous works, trading records were stored on the blockchain to ensure data privacy [23,24]. However, even if personal data are encrypted before being uploaded to the blockchain, security issues may arise later because the data recorded in the blockchain cannot be deleted or modified. Recently, due to privacy issues with blockchains, it is recommended not to store personal data on blockchains [25,26].

Decentralized identifiers (DIDs) are a new type of identifier that enable verifiable decentralized digital identities. DIDs provide a unique, decentralized way for entities to assert and control their identities without relying on centralized authorities. Each DID is generated by the entity it represents and is accompanied by a DID document containing cryptographic keys and verification methods. DIDs ensure interoperability across various decentralized systems and platforms while offering enhanced privacy and security. Users retain full control over their personal data, mitigating the risks associated with centralized identity management systems. In essence, DIDs empower individuals and organizations to manage their digital identities securely and autonomously in decentralized environments.

In this paper, we propose a reliable and privacy-preserving vehicular energy trading scheme using decentralized Identifiers to resolve the above-mentioned security challenges. In the proposed approach, the blockchain only records the information necessary for user verification, while personal information and transaction details are not stored. Moreover, completed transaction information is recorded using verifiable credentials, which can prove the validity of VCs later without any interaction using the blockchain.

This paper proposes a vehicular energy trading scheme using decentralized identifiers to address the security issues mentioned above while ensuring reliability and privacy protection. The proposed scheme does not store users' personal data and trading data on the blockchain; instead, the blockchain only operates to verify users' authenticity. Furthermore, digital signatures and verifiable credential technology are employed to ensure the reliability of transactions, and records of transaction outcomes are stored. Transaction participants can independently prove the validity of future verifiable credentials using the blockchain without the need for third-party assistance.

1.1. Motivation

The main motivation of this work is, first, to propose a solution that protects the privacy of energy traders. In existing decentralized energy trading schemes, most information, including transaction results, is recorded on the blockchain. However, while this method ensures data integrity and transparency, it also carries the risk of potential leakage to other participants. Additionally, storing a lot of data on a blockchain is costly and does not guarantee scalability.

Secondly, we aim to provide a reliable trading solution. Existing vehicle-to-vehicle energy trading methods require vehicles to arrive at the same time and place for energy trading. While advancements in battery energy storage systems (BESSs) have helped overcome the temporal constraints of vehicle-to-vehicle energy trading, the system's reliability could be compromised if malicious energy sellers pursue financial gain without delivering energy. Therefore, finding a solution that ensures the reliability of energy trading in such cases is essential. To address these issues, we are motivated to use a public blockchain, DID, VC, and commitment approaches to consider security, privacy, and reliability for the vehicular energy trading system.

1.2. Contributions

The main contributions of this paper are below.

- We propose a reliable and privacy-preserving vehicular energy trading scheme using decentralized identifiers (DIDs) and verifiable credential (VC) technologies. The energy purchaser's DID is not revealed during the authentication process at the reservation phase. Additionally, completed transaction information is not recorded in a public ledger but in VCs.
- In order to ensure reliability in energy trading, the initial VC shared during the reservation phase is incomplete. When the transaction parties successfully perform the energy trade, the signature of the CS is added to the VC, and it becomes valid.
- We analyze the proposed scheme using an ROR model and AVISPA simulation for demonstrating it resists malicious attacks and attains security features.
- We compare the performance and security features of the proposed scheme and related works to showcase the security and efficiency of our approach.

This paper is organized as follows. In Sections 2 and 3, we review the related works and relevant preliminaries, respectively. In Section 4, we propose a vehicular energy trading system model. Section 5 describes the details of the proposed energy trading scheme. In Section 6, we analyze the security of the proposed scheme. In Section 7, we analyze the performance of the proposed scheme compared to related schemes. Finally, we conclude this paper in Section 8.

2. Related Work

2.1. Decentralized Energy Trading System for Electric Vehicles

Energy trading systems for electric vehicles (EVs) have gained significant attention as a means to promote sustainable energy distribution. The traditional centralized approach to managing these energy transactions has security risks, such as single points of failure and data integrity issues. As a result, there is a growing interest in transitioning to a blockchain-based decentralized structure to enhance security [27–30]. The transition to a decentralized energy trading system using blockchain offers several security benefits:

- **Elimination of single points of failure**: In a centralized system, all information is processed through a central authority, creating a vulnerability. Blockchain decentralizes transaction processing, reducing the risk of system-wide failure due to a single compromised node.
- **Data integrity and immutability**: Blockchain records transactions in a manner that ensures data cannot be tampered with. This immutability is crucial for maintaining

accurate and trustworthy records in EV energy trading systems, which allows for robust auditing and accountability.

- **Enhanced security through decentralization**: By distributing transactions across a network of nodes, blockchain-based systems are inherently more secure against cyber-attacks. Encrypted data and consensus-based verification methods provide additional layers of protection.
- **Increased trust and transparency**: In a blockchain-based system, all participants can view the transaction history, which enhances transparency. This transparency builds trust among users, as they can independently verify the accuracy and legitimacy of transactions.

2.2. Privacy Protection and Reliability Research for Decentralized Energy Trading Systems

In recent years, research on vehicular energy trading schemes has been proposed to protect user privacy and ensure the reliability of transactions. Gai et al. [31] proposed a privacy-preserving approach for energy trading users in a blockchain-based energy trading system. They proposed a noise-based privacy protection scheme to resist linking attacks that violate energy purchasers' privacy by linking public information recorded in the blockchain with other datasets. However, their scheme does not consider privacy issues during data transmission and has the problem that energy traders rely on tokens issued by energy brokers to verify the legitimacy of the counterparties. Guan et al. [32] proposed privacy-preserving energy trading based on blockchain and attribute-based encryption (ABE). They focused on the problem of privacy leakage in blockchain-based energy trading systems, which exposes the raw information of users recorded in the blockchain. Their scheme proposed a ciphertext policy ABE-based access control method so that authorized users can access user information recorded in the blockchain. Xia et al. [33] proposed a V2V electricity trading scheme for the Internet of Vehicles by leveraging blockchain technology. Their scheme utilized a Bayesian game framework to model the strategic interactions among vehicles engaged in energy trading. By incorporating Bayesian inference techniques, vehicles can make informed decisions based on their private information and the observed behavior of other vehicles. The authors promote trust among participants by leveraging blockchain technology, which ensures transparency, security, and immutability of transactions, along with smart contracts, which are programmable codes that are reliable. Baza et al. [34] proposed blockchain-enabled secure energy trading schemes for both charging-stations-to-vehicle (CS2V) and vehicle-to-vehicle (V2V) scenarios. This scheme addresses privacy concerns by leveraging blockchain technology and smart contracts to facilitate transparent and tamper-proof transactions while ensuring fairness. The authors proposed a common prefix linkable anonymous authentication scheme to mitigate Sybil attacks and ensure system availability. Additionally, an anonymous and efficient blockchain-based payment system is proposed to prevent double-spending attacks. Li et al. [35] proposed a decentralized energy trading system named FeneChain that ensures privacy protection, verifiable fairness, and access control. They addressed security and privacy concerns in centralized energy trading systems and introduced mechanisms for anonymous authentication, timed commitments, and fine-grained access control. FeneChain addresses fairness issues in peer-to-peer (P2P) energy trading and aims to protect the rights of energy purchasers. Yahaya et al. [36] proposed a two-stage secure P2P energy trading model using a permissioned blockchain and cloud-based aggregator for secure and transparent P2P energy trading. Their scheme ensures mutual authentication, user privacy protection, and fair pricing and incentivizes energy contribution. A permissioned blockchain, off-chain authentication, and a reputation-based scoring system are employed to prevent impersonation and collusion. The model also features a privacy-preserving dynamic pricing mechanism based on the supply–demand ratio (SDR) and contract theory.

However, Baza et al. [34] use smart contracts to authenticate among EVs and take reservations for energy trading. To execute smart contract, EVs must produce transactions containing details regarding energy exchanges, revealing the identities of energy traders.

Despite attempts to obscure or encode the data, they remain permanently recorded in the blockchain as transaction. Additionally, the above-mentioned schemes [33–36] store information regarding energy trading and/or users in the blockchain, which does not solve the privacy issues. Certain blockchain nodes responsible for upkeep of the decentralized ledger possess the capability to decode these transactions. In our scheme, we utilize DIDs and VCs to provide confidentiality and to ensure privacy preservation by avoiding the recording of sensitive information in the blockchain for the vehicular energy trading system. Therefore, we propose a reliable and privacy-preserving vehicular energy trading scheme using decentralized identifiers to overcome the above-mentioned problems.

3. Preliminaries

The proposed scheme utilizes an elliptic curve cryptosystem (ECC), an elliptic curve Pedersen commitment, decentralized identifiers (DIDs), and verifiable credentials (VCs). The definitions and properties are introduced in this section.

3.1. Elliptic Curve Cryptosystem (ECC)

ECC is a public-key cryptosystem based on the mathematical principles of elliptic curves [37]. Let p be a large prime number and $E_p(a,b) : y^2 = x^3 + ax + b$ be an elliptic curve over a prime finite field $\mathbb{Z}_p$, where $(a,b) \in \mathbb{Z}_p$, $4a^3 + 27b^2 \neq 0 \pmod{p}$. G is a generator point on $E_p(a,b)$. The features of elliptic curve cryptosystems are defined as follows.

- Elliptic curve discrete logarithm problem (ECDLP): given a base point G and point $A = \alpha \cdot G$, it is difficult to find the $\alpha \in \mathbb{Z}_p$ in probability polynomial time.
- Elliptic curve decisional Diffie–Hellman problem (ECDDHP): given a base points G and two points $A = \alpha \cdot G$ and $B = \beta \cdot G$, it is difficult to compute $Q_1 = \alpha \cdot \beta \cdot G$ in probability polynomial time.

3.2. Elliptic Curve Pedersen Commitment

The elliptic curve Pedersen commitment is an efficient implementation of the Pedersen commitment scheme (PCS) [38,39] that uses the intractability of the ECDLP. In this scheme, a committer commits to secrets such that it is hard for a verifier to open the commitment. The description of the elliptic curve Pedersen commitment is presented in the following steps:

- Setup: Let G be a random generator point on $E_p(a,b)$ and $H = x_H \cdot G$ be a chosen generator point, where $x_H \in Z_p$. The trusted authority publishes $(p, E_p(a,b), G, H)$.
- Commit: The committer creates a commitment C; $x, r \in Z_p$ are random numbers, and $C(x,r) = x \cdot G + r \cdot H$, where $C(x,r)$ represents a dedicated value created by the committer.
- Open: To confirm the authenticity of C, the committer reveals x and r, and the verifier checks if $C = x \cdot G + r \cdot H$.

3.3. Decentralized Identifiers (DIDs)

Decentralized identifiers (DIDs) [40] are a new type of identifier that enables users to control their own identities and sovereignty without relying on trusted authorities. The DID ecosystem leverages blockchain technology for the storage of identities in a tamper-proof and interoperable way. A DID address consists of three fields. The first field, denoted as the DID scheme, is the URI schema of the identity. The second field, denoted as the DID method, defines how the DID scheme can be implemented on a particular distributed ledger. The last field, denoted as the DID method-specific identifier, is the unique identification string. DIDs are resolvable to DID documents, which contain public key parameters and additional information associated with a particular DID. The resolved DID document can be used for signature verification and authentication purposes for the DID subject. Figure 1 shows an example of a DID and Figure 2 shows an example of a DID document.

Figure 1. An example of a DID.

```
{
 "@context": [
  "https://www.w3.org/ns/did/v1",
  "https://w3id.org/security/suites/ed25519-2020/v1"
 ]
 "id": "did:example:123456789abcdefghi",
 "authentication": [{

  "id": "did:example:123456789abcdefghi#keys-1",
  "type": "Ed25519VerificationKey2020",
  "controller": "did:example:123456789abcdefghi",
  "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
 }]
}
```

Figure 2. An example of a DID document.

3.4. Verifiable Credentials (VCs)

A verifiable credential [41] is a tamper-resistant credential containing one or multiple statements about a specific identity. The primary qualification of the VC is to be programmable, privacy-preserving, and secure cryptographically. The issuer signs the VC by using its private key. The public key is stored in the public blockchain. The agent of the user's DID submits the VC, which includes the required official attestation statements from the issuer. Consequently, it is securely verified that the user can prove specific claims through the presentation of VCs with DID. Only users have the authority to manage and control their DIDs and VCs, and this is done while exposing as little of their claims and personal information as possible. VCs also provide consistent usability across different contexts.

In the W3C VC model [41], the subject should create a decentralized identifier through a verifiable data registry, which is a distributed ledger. The holder requests the issuer to generate a VC representing the specified properties of the identifier. Commonly, the holder is the subject of the VC he/she is maintaining (e.g., a parent maintains VCs for his/her child). The issuer confirms that the identifiers and the properties of the holder are valid, and it has authority to hold the subjects of VCs. Then, the issuer issues the VC. The holder can manage the VC after receiving it from the issuer. As a result, the holder creates a verifiable presentation based on VCs and presents it to the verifier. The identities of the verifiers are unknown to the issuers in this model. Figure 3 shows the workflow for W3C verifiable credentials.

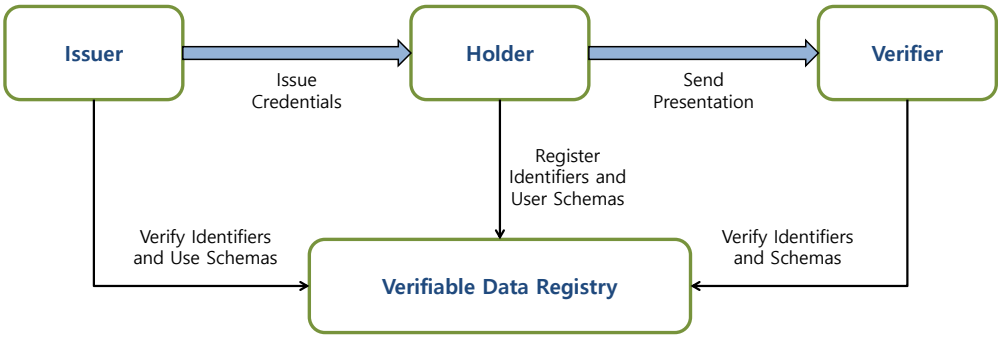

Figure 3. The workflow for W3C verifiable credentials.

4. Proposed Model

Our proposed blockchain-based V2V energy trading scheme is composed three entities: EVs, RSUs, and the blockchain. We describe each entity below. The proposed system model is also depicted in Figure 4.

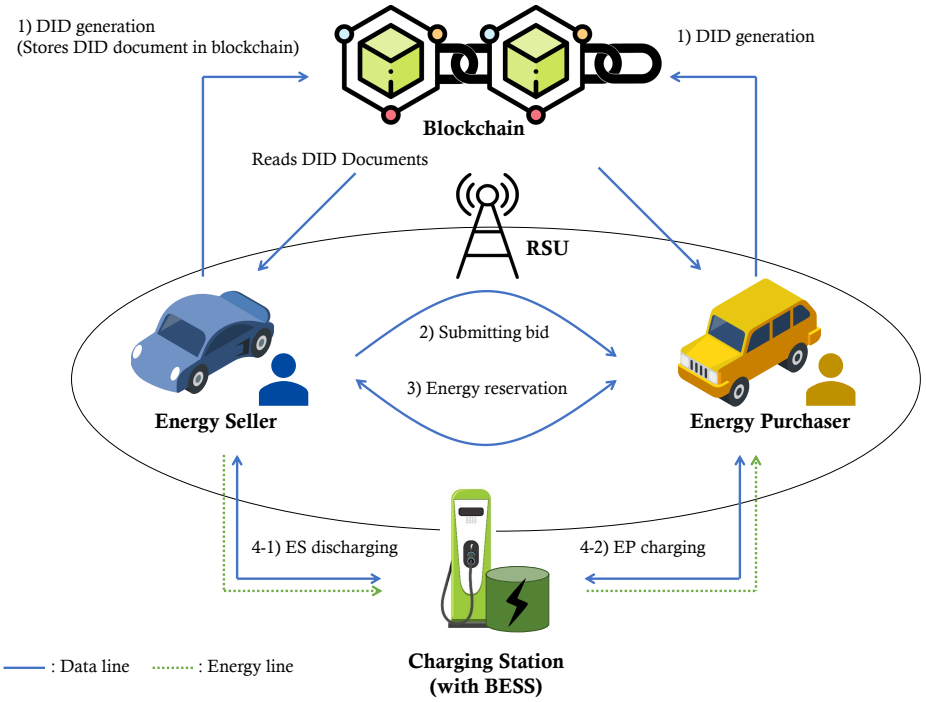

Figure 4. The proposed system model.

- **Electric vehicles (EVs)**: EVs embedded with OBU devices can communicate with external entities through dedicated short range communication (DSRC) or wireless access in vehicular environment (WAVE) and store data securely. Bidirectional EVs can purchase energy (charge) from electric vehicle supply equipment (EVSE) and sell energy to external loads (discharge). In this paper, we refer to the first vehicle as the energy purchaser and the second vehicle as the energy seller.
  Energy seller (ES): To sell surplus energy, the ES generates a bid containing the selling price, transaction time, energy volume, and other relevant information; then, it sends it to other EVs via the RSU. When the ES receives a message from an EP seeking to reserve an energy transaction, it verifies the message and shares the incomplete credentials and session key with the EP. Subsequently, the ES transfers energy and commitment to the promised CS according to the credential information and then completes the credentials by adding the signature received from the CS.
  Energy purchaser (EP): After selecting the optimal bid price, the EP sends a reservation message to the ES to plan energy trading. In the reservation phase, the EP shares incomplete credentials and a session key with the ES. When the EP arrives at the promised CS, the EP proves its commitment to the ES using the session key. If the proof is correct, the ES gets the energy stored in the CS.
  In this paper, RSU only provides a wide range of wireless communication services to EVs.

- **Smart charging stations (CSs)**: CSs are equipped with battery energy storage and a communication module for EV charging services. The CS receives the commitment and energy from the ES and stores it. The stored energy is passed on to the EP, who proves the same commitment. CSs are a type of semi-trusted authority. Even if the charging station is attacked by a malicious attacker, there is no advantage to the attacker because the charging station does not have specific information about the energy trading.
- **Blockchain**: The proposed energy trading system utilizes a public blockchain. Public blockchains are fully decentralized infrastructures, allowing all nodes on the network to easily participate without the intervention of a trusted authority and preventing single points of failure. To ensure that all participants in the system agree on a single source of truth, consensus algorithms are employed. In our system, this source comprises DID documents rather than energy trading information between EVs.

5. Proposed Scheme

We present the details of the proposed scheme in a vehicular energy trading environment. It is composed of five phases; initialization phase, DID generation phase, submitting bids phase, reservation phase, and charging phase.

5.1. Initialization Phase

Trusted authorities (TA)s first initiate the system's public parameters. The TA sets an elliptic curve $E(a,b) : y^2 = x^3 + ax + b$ over a prime finite field $\mathbb{Z}_p$, generators G and H, and a hash function $h(\cdot) : \{0,1\}^* \rightarrow Z_p$, where $a, b \in \mathbb{Z}_p, 4a^3 + 27b^2 \neq 0$. And the TA publishes system parameters $\{p, q, E(a,b), G, H, h(\cdot)\}$.

5.2. DID Generation Phase

In this phase, All system participant generate their own decentralized identifiers. Each EV selects aN identity ID_i, password PW_i, and random numbers $a_i, b_i \in Z_p$, where a_i is its private key SK_i. Then, the EV generates a public key $PK_i = SK_i \cdot G$ and stores the PK_i as a DID document on the blockchain. After the DID document is stored on the blockchain, the EV obtains the decentralized identifier DID_i corresponding to the DID document. After that, the EV calculates $HPW_i = h(b_i||PW_i)$, $A_i = b_i \oplus h(ID_i||PW_i)$, $B_i = h(ID_i||HPW_i||b_i)$ and stores $\{A_i, B_i\}$ securely in its storage. RSUs and CSs also create their own DIDs in a process similar to the DID generation steps of the EV.

5.3. Submitting Bids Phase

If the ES_i user wants to sell surplus energy, ES_i discloses the bids to potential buyers. EP_j, which endures a lack of energy, reviews bids and selects the best one. The detailed process of the submitting bids phase is as follows and is also shown in Figure 5.

- **Step 1:** ES_i user enters identity ID_i and password PW_i and computes $h(ID_i||PW_i)$, $b_i^* = A_i \oplus h(ID_i||PW_i)$, $HPW_i^* = h(PW_i||b_i^*)$, $B_i^* = h(ID_i||HPW_i^*||b_i^*)$. Then, ES_i verifies whether $B_i \stackrel{?}{=} B_i^*$. If it matches, ES_i generates a random number $x_i \in Z_p$ and a current timestamp T_i and computes $X_i = x_i \cdot G$, $HMS_1 = h(amount_i||price_i||DID_i||ext_i||T_i)$, signature $\delta_i = x_i + HMS_i \cdot SK_i$, and a bid $bid_i = \{amount_i, price_i, X_i, DID_i, ext_i\}$ to sell surplus energy, where $amount_i, price_i, ext_i$ denote an amount of energy to sell, a selling price, an expiration time for the transaction, respectively. ES_i propagates $\{bid_i, \delta_i, T_i\}$.
- **Step 2:** EP_j checks the freshness of timestamp $|T_2 - T_1| \leq \triangle T$ and uses DID_i to retrieve the corresponding DID document. Then, EP_j computes $HMS_1^* = h(amount_i||price_i||DID_i||ext_i||T_i)$ and checks whether $\delta_i \cdot G = X_i + HMS_1^* \cdot PK_i$. It is essential for EP_j to select the best bid and, at the same time, check the validity of the bid.

ES_i	EP_j
Inputs ID_i and PW_i	
Computes	
$b_i^* = A_i \oplus h(ID_i \| \| PW_i)$	
$HPW_i^* = h(PW_i \| \| b_i^*)$	
$B_i^* = h(ID_i \| \| HPW_i^* \| \| b_i^*)$	
Checks $B_i \stackrel{?}{=} B_i^*$	
Generates $x_i \in Z_p$ and T_1	
Computes	
$X_i = x_i \cdot G$	
$bid_i = \{amount_i, price_i, X_i, DID_i, ext_i\}$	
$HMS_1 = h(amout_i \| \| price_i \| \| DID_i \| \| X_i \| \| ext_i \| \| T_1)$	
$\delta_i = x_i + HMS_1 \cdot SK_i$	
$\xrightarrow{\{bid_i, \delta_i, T_1\}}$	
	Checks $\|T_2 - T_1\| \leq \triangle T$
	Retrieves DID document using DID_i
	Computes
	$HMS_1^* = h(amout_i \| \| price_i \| \| DID_i \| \| X_i \| \| ext_i \| \| T_1)$
	Checks
	$\delta_i \cdot G = X_i + HMS_1^* \cdot PK_i$

Figure 5. Submitting bids phase.

5.4. Reservation Phase

EP_j selects the ES_i that presented the optimal bid among multiple bids and sends a message to schedule an energy transaction with ES_i. When ES_i confirms the message and the transaction reservation between EP_j and ES_i is completed, EP_j and ES_i share a session key and incompletely verifiable credentials. The credentials contain information related to the energy transaction, including energy volume, price, and energy storage location. The detailed process is as follow and is also shown in Figure 6.

- **Step 1:** EP_j inputs ID_j and PW_j and then computes $h(ID_j||PW_j)$, $b_j^* = A_j \oplus h(ID_j||PW_j)$, $HPW_j^* = h(PW_j||b_j^*)$, $B_j^* = h(ID_j||HPW_j^*||b_j^*)$. ES_j checks $B_j \stackrel{?}{=} B_j^*$. If it is valid, EP_j generates a random number y_j and a timestamp T_3 and computes $Y_j = y_j \cdot G$, $EK_{ij} = h(y_j \cdot X_i)$, $EM_1 = EK_{ij} \oplus (bill_i, DID_j)$, $SymK_{ES_i-EP_j} = h(X_i \cdot sk_j||y_j \cdot PK_i)$, $HMP_1 = h(bill_i||T_3||Y_j||SymK_{ES_i-EP_j})$, $\delta_j = y_j + HMP_1 \cdot SK_j)$. Then, EP_j sends $\{EM_1, Y_j, \delta_j, T_3\}$ to ES_i.
- **Step 2:** ES_i checks the timestamp T_3 and computes $EK_{ij} = h(x_i \cdot Y_j)$, $(bill_i, DID_j) = EM_1 \oplus EK_{ij}$. Then, ES_i retrieves DID_j's document using DID_j to obtain PK_j and computes $SymK_{ES_i-EP_j} = h(x_i \cdot PK_j||Y_j \cdot SK_i)$, $HMP_1^* = h(bill_i||T_3||Y_j||SymK_{ES_i-EP_j})$. ES_i verifies the signature δ_j through $\delta_j \cdot G \stackrel{?}{=} Y_j + HMP_1^* \cdot PK_j$.
- **Step 3:** When ES_i and EP_j select the optimal charging station GS_z for energy trading, ES_i generates a temporary credential VCt_{rsv} recording a signature and information about the negotiated transaction and sends VCt_{rsv} encrypted with $SymK_{ES_i-EP_j}$ to EP_j.
- **Step 4:** EP_j decrypts the $Enc_{SymK}(VCt_{rsv})$ using $SymK_{ES_i-EP_j}$ and verifies the signature of ES_i recorded in VCt_{rsv}. After that, EP_j adds payment information and a signature to VCt_{rsv}. Then, EP_j sends VCt_{rsv}^* encrypted with $SymK_{ES_i-EP_j}$ to ES_i and stores VCt_{rsv}^*.
- **Step 5:** ES_i decrypts $Enc_{SymK}(VCt_{rsv}^*)$ using $SymK_{ES_i-EP_j}$ and verifies the signature of EP_j recorded in VCt_{rsv}^*. Then, ES_i stores VCt_{rsv}^*.

EP_j	ES_i
Inputs ID_j and PW_j	
Computes	
$b_j^* = A_j \oplus h(ID_j \| \| PW_j)$	
$HPW_j^* = h(PW_j \| \| b_j^*)$	
$B_j^* = h(ID_j \| \| HPW_j^* \| \| b_j^*)$	
Checks $B_j \stackrel{?}{=} B_j^*$	
Generates $y_j \in Z_p$ and T_3	
$Y_j = y_j \cdot G$	
$EK_{ij} = h(y_j \cdot X_i)$	
$EM_1 = EK_{ij} \oplus (bill_i, DID_j)$	
$SymK_{ES_i-EP_j} = h(X_i \cdot sk_j \| \| y_j \cdot PK_i)$	
$HMP_1 = h(bill_i \| \| T_3 \| \| Y_j \| \| SymK_{ES_i-EP_j})$	
$\delta_j = y_j + HMP_1 \cdot SK_j$	
	$\xrightarrow{\{EM_1, Y_j, \delta_j, T_3\}}$
	Check $\|T_4 - T_3\| \leq \triangle T$
	Computes
	$EK_{ij} = h(x_i \cdot Y_j)$
	$(bill_i, DID_j) = EM_1 \oplus EK_{ij}$
	Retrieves DID_j's document using DID_j
	$SymK_{ES_i-EP_j} = h(x_i \cdot PK_j \| \| Y_j \cdot SK_i)$
	$HMP_1^* = h(bill_i \| \| T_3 \| \| Y_j \| \| SymK_{ES_i-EP_j})$
	Verifies
	$\delta_j \cdot G = Y_j + HMP_1^* \cdot PK_j$
	Chooses CS_z
	Generates
	$VCt_{rsv} = \{Inf, ext_i, Sig_{SK_i}(Inf)\}$
	$,(Inf = \{amount_i, price_i, DID_i, DIDj, DID_z, ext_i\})$
	$\xleftarrow{\{Enc_{SymK}(VCt_{rsv})\}}$
Decrypts $Enc_{SymK}(VCt_{rsv})$ using $SymK_{ES_i-EP_j}$	
Verifies VCt_{rsv}'s $Sig_{SK_i}(Inf)$	
Computes	
$VCt_{rsv}^* = \{VCt_{rsv}, pay, Sig_{SK_j}(Inf, pay)\}$	
Stores VCt_{rsv}^*	
	$\xrightarrow{\{Enc_{SymK}(VCt_{rsv}^*)\}}$
	Decrypts $Enc_{SymK}(VCt_{rsv}^*)$ using $SymK_{ES_i-EP_j}$
	Verifies VCt_{rsv}^*'s $Sig_{SK_i}(Inf)$
	Stores VCt_{rsv}^*

Figure 6. Reservation phase.

5.5. Charging Phase

In this phase, EP_j and ES_i trade energy through the promised charging station equipped with BESS according to the initial credentials.

5.5.1. ES_i Discharging

According to the negotiation in VCt_{rsv}^*, ES_i stores the surplus energy in GS_z and then receives a signature from GS_z to make its VCt_{rsv}^* valid. GS_z receives a commitment and energy from ES_i and sends its signature to ES_i. A complete credential VCt_{rsv}^* proves that ES_i stored the energy in GS_z as negotiated. Figure 7 depicts the ES_i discharging phase.

ES_i	CS_z
Generates $n_i \in Z_p$ and T_5	
Computes	
$N_i = n_i \cdot G$	
$AK_{iz} = n_i \cdot PK_z$	
$HIF = h(inf\|\|pay)$	
$Com = SymK_{ES_i-EP_j} \cdot G + HIF \cdot H$	
$ESM_1 = AK_{iz} \oplus (HIF\|\|DID_i\|\|Com)$	
$\delta_{i2} = n_i + h(HIF\|\|Com\|\|N_i\|\|T_5) \cdot SK_i$	
$\xrightarrow{\{ESM_1, N_i, \delta_{i2}, T_5\}}$	
	Check $\|T_6 - T_5\| \leq \triangle T$
	Computes
	$AK_{iz} = N_i \cdot SK_z$
	$(HIF\|\|DID_i\|\|Com) = ESM_1 \oplus AK_{iz}$
	Verifies
	$\delta_{i2} \cdot G \stackrel{?}{=} N_i + h(HIF\|\|Com\|\|N_i\|\|T_5) \cdot PK_i$
	Generates $Sig_{sk_z}(HIF)$
	$ESM_2 = AK_{iz} \oplus Sig_{sk_z}(HIF)$
$\xleftarrow{\{ESM_2\}}$	
$Sig_{sk_z}(HIF) = ESM_2 \oplus AK_{iz}$	
Verifies $Sig_{sk_z}(HIF)$	
$VC^*_{rsv} = VC^*_{rsv} + Sig_{sk_z}(HIF)$	
$\xrightarrow{\{Energy, price\}}$	
	Stores $\{Com, price, Energy\}$

Figure 7. Charging phase—ES_i discharging.

- **Step 1:** ES_i generates an $n_i \in Z_p$ and a timestamp T_5. Next, ES_i computes $N_i = n_i \cdot G$, $AK_{iz} = n_i \cdot PK_z$, $HIF = h(inf||pay)$, $Com = SymK_{ES_i-EP_j} \cdot G + HIF \cdot H$, $ESM_1 = AK_{iz} \oplus (HIF||DID_i||Com)$, $\delta_{i2} = n_i + h(HIF||Com||N_i||T_5) \cdot SK_i$ and sends $\{ESM_1, N_i, \delta_{i2}, T_5\}$ to GS_z
- **Step 2:** GS_z checks the freshness of the T_5 and calculates $AK_{iz} = N_i \cdot SK_z$, $(HIF||DID_i||Com) = ESM_1 \oplus AK_{iz}$. If $\delta_{i2} \cdot G = N_i + h(HIF||Com||N_i||T_5) \cdot PK_i$ matches, GS_z generates $Sig_{sk_z}(HIF)$ and sends $ESM_2 = AK_{iz} \oplus Sig_{sk_z}(HIF)$ to ES_i.
- **Step 3:** ES_i calculates $Sig_{sk_z}(HIF) = ESM_2 \oplus AK_{iz}$ and verifies $Sig_{sk_z}(HIF)$ using GS_z's public key. If the signature is valid, ES_i records $Sig_{sk_z}(HIF)$ in VC^*_{rsv} and transmits vehicular energy and *price* to GS_z.
- **Step 4:** GS_z stores $\{Com, price\}$ in a database and energy in battery storage.

5.5.2. EP_j Charging

When EP_j arrives at the entrusted charging station CS_z, EP_j creates a commitment and submits it to CS_z. CS_z verifies the integrity of the message and validates the legitimacy of the commitment through a handshake with EP_j. If the commitment is valid, CS_z transfers the entrusted energy and signature to EP_j. EP_j adds the received signature to the VCt^*_{rsv} to complete it. Figure 8 depicts the EP_j charging phase.

EP_j	CS_z
Generates $m_j, l_j \in Z_p$ and T_7	
Computes	
$M_j = m_j \cdot G$	
$L_j = l_j \cdot H$	
$EPM_1 = M_j + L_j$	
$AK_{jz} = m_j \cdot PK_z$	
$HIF = h(Inf\|\|pay)$	
$Com^* = SymK_{ES_i-EP_j} \cdot G + HIF \cdot H$	
$EPM_2 = AK_{jz} \oplus (HIF\|\|Com^*\|\|EPM_1)$	
$EPM_3 = h(HIF\|\|Com\|\|EPM_1\|\|T_7\|\|M_j)$	
	$\{EPM_2, EPM_3, M_j, T_7\} \longrightarrow$
	Check $\|T_8 - T_7\| \leq \triangle T$
	Computes
	$AK_{jz} = M_j \cdot SK_z$
	$(HIF\|\|Com^*\|\|EPM_1) = EPM_2 \oplus AK_{iz}$
	$EPM_3^* = h(HIF\|\|Com\|\|EPM_1\|\|T_7\|\|M_j)$
	Verifies
	$EPM_3 \stackrel{?}{=} EPM_3^*$
	Retrieves Com from GS_z's database
	Generates $e_z \in Z_p$
	$\{e_z\} \longleftarrow$
Computes	
$\alpha = m_j + e \cdot SymK_{ES_i-EP_j}$	
$\beta = l_j + e \cdot HIF$	
	$\{\alpha, \beta\} \longrightarrow$
	Verifies
	$\alpha \cdot G + \beta \cdot H \stackrel{?}{=} EPM_1 + Com$
	Generates $Sig_{sk_z}(HIF)$
	$EPM_4 = AK_{jz} \oplus Sig_{sk_z}(HIF)$
	$\{EPM_4\}, Energy \longleftarrow$
Computes	
$Sig_{sk_z}(HIF) = EPM_4 \oplus AK_{jz}$	
Verifies $Sig_{sk_z}(HIF)$	
$VC_{rsv}^* = VC_{rsv}^* + Sig_{sk_z}(HIF)$	

Figure 8. Charging phase—EP_j charging.

- **Step 1:** EP_j generates random numbers $m_j, l_j \in Z_j$ and timestamps T_7 and computes $M_j = m_j \cdot G$, $L_j = l_j \cdot H$, $EPM_1 = M_j + L_j$, $AK_{jz} = m_j \cdot PK_z$, $HIF = h(Inf||pay)$, $Com^* = SymK_{ES_i-EP_j} \cdot G + HIF \cdot H$, $EPM_2 = AK_{jz} \oplus (HIF||Com^*||EPM_1)$, $EPM_3 = h(HIF||Com^*||EPM_1||T_7||M_j)$. Then, EP_j sends $\{EPM_2, EPM_3, M_j, T_7\}$ to CS_z.
- **Step 2:** After receiving the message from EP_j, CS_z verifies the freshness of the message. CS_z calculates $AK_{jz} = M_j \cdot SK_z$, $(HIF||Com^*||EPM_1) = EPM_2 \oplus AK_{iz}$, $EPM_3^* = h(HIF||Com||EPM_1||T_7||M_j)$ and checks whether $EPM_3 \stackrel{?}{=} EPM_3^*$ is correct. If it is correct, CS_z retrieves Com and sends a random number $e_z \in Z_p$ to EP_j.
- **Step 3:** EP_j computes $\alpha = m_j + e \cdot SymK_{ES_i-EP_j}$, $\beta = l_j + e \cdot HIF$ and submits $\{\alpha, \beta\}$ to CS_z
- **Step 4:** If $\alpha \cdot G + \beta \cdot H \stackrel{?}{=} EPM_1 + Com$ is correct, CS_z generates $Sig_{sk_z}(HIF)$, $EPM_4 = AK_{iz} \oplus Sig_{sk_z}(HIF)$ and transfers $\{EPM_4\}, Energy$ to EP_j.

- **Step 5:** EP_j calculates $Sig_{sk_z}(HIF) = EPM_4 \oplus AK_{jz}$ and verifies $Sig_{sk_z}(HIF)$ using GS_z's public key. If the signature is valid, EP_j records $Sig_{sk_z}(HIF)$ in VC^*_{rsv}.

6. Security Analysis

We carry out informal and formal analyses to verify the security of the proposed scheme. We utilize the real-or-random (ROR) oracle model to ensure the security of session keys and employ Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation [42] to assess resilience against several security attacks.

6.1. Informal Analysis

In this section, we carry out an informal analysis to verify that the proposed scheme resists various attacks and achieves security features such as confidentiality, reliability, and mutual authentication.

- Impersonation attack: Malicious attackers can attempt to impersonate a legitimate vehicle. However, as mentioned in Section 3.1, due to ECDLP and ECDDHP, attackers find it challenging to compute the vehicle's private key SK_x and session key $SymK_{ES_i-EP_j}$, making it difficult to impersonate a legitimate vehicle. Therefore, the proposed scheme is secure against an impersonation attack.
- Replay attack: Attackers can intercept messages transmitted over a public channel and resend or delay them to obtain sensitive information or to execute other security attacks. However, since messages transmitted over the public channel include timestamps and random numbers, recipients can verify the freshness of the message. Therefore, the proposed scheme is secure against replay attacks.
- Man-in-the-middle (MITM) attack: Attackers can participate in communication between two legitimate vehicles during the reservation phase to collect valuable information about the users and to later attempt to forge messages using this information. However, due to the use of one-way hash functions, random numbers, and timestamps, the integrity and freshness of the message is ensured. Additionally, since signatures δ_x are generated using private keys SK_x, attackers cannot create valid authentication messages. Therefore, the proposed scheme is secure against a man-in-the-middle attack.
- Confidentiality: In the proposed scheme, the DID of the energy purchaser is not exposed in order to conceal transactions between the energy seller and purchaser. However, the DID of the energy seller is exposed to publicly verify the legitimacy of the seller and invoices. Additionally, the charging station, which manages the energy received from the energy seller, provides energy only to vehicles that present the correct commitment Com, thus not requiring information about the energy purchaser. Moreover, only the parties involved in the energy transaction possess verifiable credentials to prove their participation.
- Reliability: To ensure the reliability of energy transactions between two vehicles in the proposed scheme, both vehicles share verifiable credentials during the reservation phase. These credentials are not valid until they obtain the signature from the charging station. As both vehicles successfully delegate and accept energy through the charging station, they can complete their credentials by obtaining the signature value from the charging station. Therefore, the proposed scheme provides reliability to energy traders so that they can proceed with the normal energy trading process.
- Mutual authentication: ES_i and EP_j authenticate each other. ES_i authenticates EP_j by checking whether $\delta_j \cdot G \stackrel{?}{=} Y_j + HMP^*_1 \cdot PK_j$ is correct during the reservation phase. EP_j authenticates ES_i by verifying whether $\delta_i \cdot G \stackrel{?}{=} X_i + HMS^*_1 \cdot PK_i$ is correct during the submitting bids phase. Therefore, the proposed scheme ensures mutual authentication.

6.2. Formal Analysis

We conduct a formal security proof by using the AVISPA simulation and the ROR oracle model.

6.2.1. ROR model

The ROR model, which is based on probabilistic game theory, is utilized for analyzing the semantic security of an authenticated key agreement. We utilize the ROR oracle model to evaluate the session key security for the proposed scheme. We briefly introduce the ROR oracle model.

In the ROR model, there are three parties: the energy seller $\mathcal{P}_{ES}^{t1}$ and the energy purchaser $\mathcal{P}_{EP}^{t2}$, where $\mathcal{P}_{ES}^{t1}$ and $\mathcal{P}_{EP}^{t2}$ are the instances of ES_i and EP_j. In Table 1, we define queries for the ROR oracle model, such as *Execute*, *Send*, *Reveal*, and *Test*. In addition, we use a collision-resistant one-way hash function *Hash* as a random oracle. We use Zipf's law to evaluate session key security.

Table 1. Various queries and descriptions.

Query	Description
$Execute(\mathcal{P}_{ES}^{t1}, \mathcal{P}_{EP}^{t2})$	Under this query, $\mathcal{A}$ performs an eavesdropping attack between $\mathcal{P}_{ES}^{t}$ and $\mathcal{P}_{EP}^{t}$ over a public channel.
$Send(\mathcal{P}^{t}, Msg)$	Under this query, $\mathcal{A}$ can send the messages Msg to the participant $\mathcal{P}^{t}$ and get the response message accordingly.
$Reveal(\mathcal{P}_{ES}^{t1}, \mathcal{P}_{EP}^{t2})$	Under this query, $\mathcal{A}$ compromises a current session key between $\mathcal{P}_{ES}^{t1}$ and $\mathcal{P}_{EP}^{t2}$.
$Test(\mathcal{P}^{t})$	An unbiased coin c is tossed prior to the start of the game, and the result is used to decide the output of the *Test* query. If $\mathcal{A}$ receives $C = 0$, the session key among $\mathcal{P}_{ES}^{t1}$ and $\mathcal{P}_{EP}^{t2}$ is fresh. If $\mathcal{A}$ receives $C \neq 0$, the session key is not fresh; otherwise, $\mathcal{A}$ obtains a null value ($\perp$).

Theorem 1. *$Adv_{\mathcal{A}}(t)$ is assumed that the advantage function of adversary $\mathcal{A}$ in order to break the session key security of the proposed scheme. Then, we derive the following:*

$$Adv_{\mathcal{A}}(t) \leq \frac{q_{hash}^2}{|Hash|} + 2\, Adv_{\mathcal{A}}^{ECDDHP}(t). \tag{1}$$

where q_{hash} is the number of Hash, $|Hash|$ is the range space of the hash function, and $Adv_{\mathcal{A}}^{ECDDHP}(t)$ is the $\mathcal{A}$'s advantage for breaching ECDDHP.

Proof. We indicate the four games with $G_i, i = [0, 3]$, and the probability of $\mathcal{A}$ for winning game G_i is denoted as $Pr[Succ_{G_i}]$.

- **Game 0:** G_0 is considered to be $\mathcal{A}$'s real attacks in our proposed scheme. $\mathcal{A}$ picks a random bit c at the beginning of G_0. Then, we obtain the following equation:

$$Adv_{\mathcal{A}}(t) = |2Pr[Succ_{G_0}] - 1|. \tag{2}$$

- **Game 1:** G_1 indicates that $\mathcal{A}$ executes an eavesdropping attack, in which the transmitted messages are intercepted between $\mathcal{P}_{ES}^{t1}$ and $\mathcal{P}_{EP}^{t2}$. For this game, $\mathcal{A}$ executes a $Execute(\mathcal{P}_{ES}^{t}, \mathcal{P}_{EP}^{t})$ query to obtain the communicated messages. After the end of this game, $\mathcal{A}$ carries out *Reveal*, and *Test* queries to compromise session key $SymK_{ES_i-EP_j}$. To derive $SymK_{ES_i-EP_j}$, $\mathcal{A}$ needs the short-term secret values x_i and y_j and private keys SK_i and SK_j. Hence, $\mathcal{A}$'s probability of winning G_1 by eavesdropping on the messages does not increase. Therefore, we obtain the result as follows:

$$Pr[Succ_{G_1}] = Pr[Succ_{G_0}]. \tag{3}$$

- **Game 2:** G_2 is considered to be active/passive attacks by executing *Send* and *Hash* queries to find hash collision. $\mathcal{A}$ can intercept the transmitted messages from the submitting bids phase to the reservation phase. The intercepted messages are safeguarded by the collision-resistant one-way hash function $h(\cdot)$. Furthermore, $\mathcal{A}$ tries to derive $SymK_{ES_i-EP_j} = h(x_i \cdot PK_j || Y_j \cdot SK_i) = h(X_i \cdot sk_j || y_j \cdot PK_i)$ by using intercepted messages. However, $\mathcal{A}$ needs to break the ECDDHP (defined in Section 3.1) in polynomial time t, which is a computationally infeasible problem for $\mathcal{A}$ to derive $SymK_{ES_i-EP_j}$. By applying the ECDDHP and the birthday paradox result, we obtain the inequality

$$|Pr[Succ_{G_1}] - Pr[Succ_{G_2}]| \leq \frac{q_{hash}^2}{2|Hash|} + Adv_{\mathcal{A}}^{ECDDHP}(t). \tag{4}$$

After executing all the games, $\mathcal{A}$ tries to guess the exact bit c to win the game using the *Test* query. Thus, we obtain the following:

$$Pr[Succ_{G_2}] = \frac{1}{2}. \tag{5}$$

Equations (2) and (3) help to derive

$$\begin{aligned} \frac{1}{2} Adv_{\mathcal{A}}(t) &= |Pr[Succ_{G_0}] - \frac{1}{2}| \\ &= |Pr[Succ_{G_1}] - \frac{1}{2}|. \end{aligned} \tag{6}$$

Furthermore, using Equations (4)–(6), we obtain the following inequality:

$$\begin{aligned} \frac{1}{2} Adv_{\mathcal{A}}(t) &= |Pr[Succ_{G_1}] - Pr[Succ_{G_2}]| \\ &\leq \frac{q_{hash}^2}{2|Hash|} + Adv_{\mathcal{A}}^{ECDDHP}(t). \end{aligned} \tag{7}$$

Finally, by multiplying both sides of Equation (7), we obtain the stipulated result $Adv_{\mathcal{A}}(t)$:

$$Adv_{\mathcal{A}}(t) \leq \frac{q_{hash}^2}{|Hash|} + 2\, Adv_{\mathcal{A}}^{ECDDHP}(t).$$

□

6.2.2. AVISPA Simulation

This simulation proves the formal security robustness of the cryptographic protocol against MITM and replay attacks. We implement the security simulation and demonstrate the security result. The AVISPA simulation tool is implemented using "High-Level Protocol Specification Language (HLPSL) to generate input format (IF)" and is linked to four backends, including the on-the-fly mode checker (OFMC), the Tree Automata based on Automatic Approximations for the Analysis of Security Protocols (TA4SP), the SAT-based model checker (SATMC), and the Constraint-Logic-based Attack Searcher (CL-AtSe). Only the CL-AtSe and OFMC provide the operation of bitwise exclusive-or (XOR) in these backends. AVISPA supports the DY model and can verify MITM and replay attacks.

The roles of the energy seller and energy purchaser nodes are described in Figures 9 and 10, respectively. The goals and the roles of the session and environment of the proposed scheme are indicated in Figure 11. The simulation results for the OFMC and CL-ATse backends are presented in Figure 12, which show that the proposed scheme is secure against MITM and replay attacks.

```
%%%%%%% Role Seller %%%%%
role seller(ES,EP : agent, H: hash_func, SND, RCV : channel(dy))
played_by ES
def=
local State: nat,
                MUL, ADD : hash_func,
                DIDi,PWi,G,PKi,SKi,HPWi,Ai,Aii,Bi,Xi,Ti,AMOUNTi,PRICEi,TIMEi,Xii,
HMS1,Sigmai,SHKesep:text,
                DIDj,PWj,PKj,SKj,HPWj,Aj,Ajj,Bj,Yj,Tj,Yjj,HMP1,Sigmaj,SHKepes:text

const sp1,sp2,es_ep_xi,ep_es_yi: protocol_id
init State:=0
transition
%%%%% Seller DID generation %%%%%%%
1. State=0 /\RCV(start)=|>
State':=1 /\Ai':=new()
                /\PKi':=MUL(SKi.G) /\HPWi':=H(PWi.Ai') /\Aii':=xor(H(DIDi.PWi),Ai')
/\Bi':=H(DIDi.HPWi'.Ai')
                /\SND({DIDi.PKi'})
                /\secret({SKi,Ai'},sp1,{ES})
%%%%% Submitting bids %%%%%
                /\Xi':=new() /\Ti':=new() /\AMOUNTi':=new() /\PRICEi':=new()
/\TIMEi':=new()
                /\Xii':=MUL(Xi'.G) /\HMS1':=H(AMOUNTi'.PRICEi'.DIDi.TIMEi'.Ti')
                /\Sigmai':=ADD(Xi'.MUL(HMS1'.SKi))
                /\SND(AMOUNTi'.PRICEi'.Xii'.DIDi.TIMEi'.Ti'.Sigmai')
                /\witness(ES,EP,es_ep_xi,Xi')
%%%%% Seller Energy reservation %%%%%
2. State=1
/\RCV({AMOUNTi'.PRICEi'.Xii'.DIDi.TIMEi'.DIDj.Yjj'}_SHKepes.MUL(Yj'.G).Tj'.AD
D(Yj'.MUL(H(AMOUNTi'.PRICEi'.Xii'.DIDi.TIMEi'.Tj'.MUL(Xi'.G).MUL(Yj'.G)).SKj)))=
|>
State':=2 /\SHKesep':=MUL(Xi.MUL(Yj'.G))
                /\request(EP,ES,ep_es_yi,Yj')
end role
```

Figure 9. Role of the energy seller

```
%%%%%%% Role purchaser %%%%%
role purchaser(ES,EP : agent, H: hash_func, SND, RCV : channel(dy))
played_by EP
def=
local State: nat,
                MUL, ADD : hash_func,
                DIDi,PWi,G,PKi,SKi,HPWi,Ai,Aii,Bi,Xi,Ti,AMOUNTi,PRICEi,TIMEi,Xii,
HMS1,Sigmai,SHKesep: text,
                DIDj,PWj,PKj,SKj,HPWj,Aj,Ajj,Bj,Yj,Tj,Yjj,HMP1,Sigmaj,SHKepes:
text

const sp1,sp2,es_ep_xi,ep_es_yi: protocol_id
init State:=0
transition

%%%%% Purchaser DID generation %%%%%%%
1. State=0 /\RCV(start)=|>
State':=1 /\Aj':=new()
                /\PKj':=MUL(SKj.G) /\HPWj':=H(PWj.Aj') /\Ajj':=xor(H(DIDj.PWj),Aj')
/\Bj':=H(DIDj.HPWj'.Aj')
                /\SND({DIDj.PKj'})
                /\secret({SKj,Aj'},sp2,{EP})
%%%%% Purchaser Energy reservation %%%%%
2. State=1
/\RCV(AMOUNTi'.PRICEi'.MUL(Xi'.G).DIDi.TIMEi'.Ti'.ADD(Xi'.MUL(HMS1'.SKi)))
=|>
State':=2 /\Yj':=new() /\Tj':=new()
                /\Yjj':=MUL(Yj'.G) /\SHKepes':=MUL(Yj.MUL(Xi'.G))
/\HMP1':=H(AMOUNTi'.PRICEi'.MUL(Xi'.G).DIDi.TIMEi'.Tj'.MUL(Xi'.G).MUL(Yj'.G))
                /\Sigmaj':=ADD(Yj'.MUL(HMP1'.SKj))
                /\SND({AMOUNTi'.PRICEi'.MUL(Xi'.G).DIDi.TIMEi'.DIDj.Yjj'}_SHKep
es.Yjj'.Tj'.Sigmaj')
                /\witness(EP,ES,ep_es_yi,Yj')
                /\request(ES,EP,es_ep_xi,Xi')

end role
```

Figure 10. Role of the energy purchaser.

```
%%%%%%%%%   session  %%%%%%
role session(ES,EP : agent, H: hash_func)

def=
local SN1, SN2, RV1, RV2 : channel(dy)
composition
seller(ES,EP,H,SN1,RV1)
/\purchaser(ES,EP,H,SN2,RV2)
end role

%%%%%  environments and goals  %%%%%%didi, didj, pki, pkj, yjj, xii : text,?
                /didi, pki, yjj, xii
role environment()

def=
const es,ep : agent,
h,mul,add: hash_func,
didi, didj, pki, pkj, yjj, xii : text,
es_ep_xi,ep_es_yi: protocol_id,
sp1,sp2: protocol_id

intruder_knowledge = {es,ep,didi, didj, pki, pkj, yjj, xii,h}
composition
session(es,ep,h)/\session(i,ep,h)/\session(es,i,h)
end role

goal
secrecy_of sp1, sp2
authentication_on es_ep_xi,ep_es_yi
end goal

environment()
```

Figure 11. Environment and goals.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/did1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.08s
  visitedNodes: 16 nodes
  depth: 4 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/did1.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 1 states
  Reachable  : 1 states
  Translation: 0.02 seconds
  Computation: 0.00 seconds
```

Figure 12. The result of AVISPA simulation via OFMC and CL-AtSe backends.

7. Performance Analysis

We compare the proposed scheme with related schemes suggested for vehicular energy trading environments. We show that the proposed scheme has comparable or better performances compared to the existing schemes in this section. We perform testbed experiments on cryptographic computation by leveraging MIRACL on PC. The detailed specifications of the PC are as follows: 8 GB memory, Intel Core i7-4790 at 3.60 GHz frequency, and Linux Ubuntu 18.04.4 LTS with 64 bits.

7.1. Security Features

We present the security properties of the proposed scheme and existing schemes [33–36]. As shown in Table 2, the related schemes [33–36] are subject to temporal constraints, as transactions can only occur at the same time. Furthermore, our scheme only utilizes the blockchain to retrieve information for authentication (except for the DID generation phase, which is recorded on the blockchain). However, other papers record transactions on the blockchain during the energy trading process, leading to increased costs over time. This can create scalability issues. Therefore, our scheme provides more security features compared to related schemes.

Table 2. Security and function properties comparison.

Security and Function Properties	Xia et al. [33]	Baza et al. [34]	Li et al. [35]	Yahaya et al. [36]	Proposed
SF_1	○	○	○	○	○
SF_2	○	○	○	○	○
SF_3	○	○	○	○	○
SF_4	○	×	×	○	○
SF_5	–	○	○	○	○
SF_6	○	○	○	○	○
SF_7	×	×	×	×	○
SF_8	–	×	×	–	○

○: provides security feature, ×: does not provide security feature, –: not considered, SF_1: impersonation attack, SF_2: replay attack, SF_3: MITM attack, SF_4: confidentiality, SF_5: reliability, SF_6: mutual authentication, SF_7: temporal constraint of trading, and SF_8: high scalability.

7.2. Computation Cost Analysis

We compare the computation costs of the energy trading process (from the authentication phase among EVs to the charging phase) between the proposed scheme and related works [33–36]. Table 3 shows the notation of each operation and the average cost calculated 100 times for each operator in the set environment.

Table 3. The notation of each operation and computation costs.

Notation	Depiction	Computation Cost
T_{hash}	one-way hash function	0.003 ms
T_{ecc}^{add}	point addition operation on elliptic curve	0.013 ms
T_{ecc}^{mul}	scalar point multiplication operation on elliptic curve	2.373 ms
T_{ecc}^{exp}	exponentiation operation on elliptic curve	0.819 ms
T_{pair}	bilinear pairing operation	6.575 ms
T_{sym}^{enc}	symmetric key encryption (e.g., AES-256)	0.001 ms
T_{sym}^{dec}	symmetric key decryption	0.001 ms
T_{asym}^{enc}	asymmetric key encryption (e.g., RSA)	0.304 ms
T_{asym}^{dec}	asymmetric key decryption	2.405 ms
T_{sig}^{gen}	signature generation	0.173 ms
T_{sig}^{ver}	signature verification	4.194 ms

Furthermore, the computation costs of "generating authentication proof" in [34] is similar to T_{sig}^{gen}. The computational costs comparison of the proposed scheme and the existing schemes are summarized in Table 4. The computational cost of our system is lower than that of [35] but higher than that of [33,34,36]. However, [33] has the drawback of relying on intermediaries to authenticate vehicles, and [34,36] incurs additional gas costs as it requires running Ethereum smart contracts. Therefore, our scheme is more efficient than other schemes in a decentralized energy trading system for vehicles.

Table 4. Computation costs comparison.

Schemes	EP_j	ES_i	RSU/Energy Broker	Total Costs
[33]	T_{asym}^{enc} $+T_{sig}^{gen}$ ≈ 0.477 ms	T_{asym}^{enc} $+T_{sig}^{gen}$ $+T_{sig}^{ver}$ ≈ 4.671 ms	$2T_{Dec-Asym}$ $+4T_{sig}^{ver}$ ≈ 21.586 ms	≈ 26.734 ms
[34]	$2T_{ecc}^{exp} + T_{sym}^{enc}$ $+T_{sym}^{dec}$ $+T_{sig}^{gen}$ ≈ 1.813 ms	$2T_{ecc}^{exp} + 2T_{sym}^{enc}$ $+T_{sig}^{gen}$ ≈ 1.813 ms	N/A	≈ 3.626 ms
[35]	$T_{hash} + T_{ecc}^{add}$ $+2T_{ecc}^{mul} + 4T_{ecc}^{exp}$ ≈ 8.038 ms	$2T_{hash} + 2T_{ecc}^{add}$ $+T_{ecc}^{mul} + 7T_{ecc}^{exp}$ $+4T_{sym}^{dec} + 7T_{pair}$ ≈ 54.167 ms	$2T_{hash} + T_{ecc}^{add}$ $+3T_{ecc}^{mul} + 16T_{ecc}^{exp}$ $+4T_{sym}^{enc}$ ≈ 20.246 ms	≈ 82.451 ms
[36]	$4T_{hash} + 3T_{ecc}^{mul}$ $+7T_{ecc}^{exp} + 2T_{pair}$ ≈ 26.014 ms	$4T_{hash} + 3T_{ecc}^{mul}$ $+7T_{ecc}^{exp} + 2T_{pair}$ ≈ 26.014 ms	N/A	≈ 52.028 ms
Proposed scheme	$9T_{hash} + 10T_{ecc}^{mul} + T_{ecc}^{add}$ $+T_{sym}^{enc} + T_{sym}^{dec}$ $+T_{sig}^{gen} + 2T_{sig}^{ver}$ ≈ 32.333 ms	$9T_{hash} + 11T_{ecc}^{mul} + 1T_{ecc}^{add}$ $+T_{sym}^{enc} + T_{sym}^{dec}$ $+T_{sig}^{gen} + 2T_{sig}^{ver}$ ≈ 34.706 ms	$2T_{hash} + 6T_{ecc}^{mul} + 3T_{ecc}^{add}$ $+2T_{sig}^{gen}$ ≈ 14.629 ms	≈ 81.668 ms

7.3. Communication Cost Analysis

We evaluate the communication costs of the proposed scheme compared to related schemes [33–36] during the authentication phase, during which the messages are exchanged by the registered vehicles. We first define that the bit lengths of the timestamp, random number, identity, hash output, symmetric encryption, elliptic curve point, and asymmetric encryption to be 32 bits, 160 bits, 160 bits, 160 bits, 256 bits, 320 bits, and 320 bits, respectively. Moreover, the bit length of request information is defined to be 160 bits. The bit length of authentication proof is defined to be 729 bytes [34]. Table 5 shows an analysis of the communication costs of the proposed scheme compared to related protocols. As a result of the comparison, our scheme has similar or slightly higher costs compared to others in terms of performance, but it can be suitable for achieving a reliable and privacy-preserving energy trading environment because it provides more security and functions.

Table 5. Communication costs comparison.

Scheme	Total Cost
Xia et al. [33]	2144 bits
Baza et al. [34]	12,560 bits
Li et al. [35]	3840 bits
Yahaya et al. [36]	2304 bits
Proposed scheme	5440 bits

8. Conclusions

Despite the rapid growth of the electric vehicle market, the problem of insufficient charging infrastructure persists. To address this issue, various technologies are being researched to enable EV charging from diverse energy sources, such as battery energy storage systems. However, vehicles in these systems are vulnerable to various security attacks because they exchange information over public channels. This paper proposes a vehicle energy trading mechanism that addresses the limitations of recent distributed energy trading schemes while ensuring reliability and privacy preservation. In the proposed scheme, only the authentication materials required for the energy transaction are stored in the blockchain, and the transaction results are recorded in verifiable credentials, thereby reducing the storage burden on the blockchain. User privacy is also protected by not storing users' personal data on the blockchain. We conducted an informal analysis and a formal analysis to include using the AVISPA and ROR oracle models to evaluate the security of the proposed method and ensure that it ensures confidentiality, reliability, and mutual authentication. Finally, we compared the performance and security features of the proposed scheme with related schemes to demonstrate that our proposed scheme provides more security functions without a loss of performance compared to related schemes in a vehicular energy trading environment.

Author Contributions: Conceptualization, M.K.; Methodology, Y.P.; Validation, K.P. and Y.P.; Formal analysis, M.K.; Writing—original draft, M.K.; Writing—review & editing, K.P. and Y.P.; Supervision, Y.P.; Funding acquisition, Y.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605.

Data Availability Statement: Data are contained within the article.

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

References

1. Global EV Outlook: Understanding the Electric Vehicle Landscapeto 2020. Available online: https://www.ourenergypolicy.org/wp-content/uploads/2013/09/GlobalEVOutlook_2013.pdf (accessed on 8 April 2024).
2. Electric Car Demand Growing, Global Market Hits 740,000 Units. Available online: https://cleantechnica.com/2015/03/28/ev-demand-growing-global-market-hits-740000-units/ (accessed on 8 April 2024).
3. Mouli, G.R.C.; Kefayati, M.; Baldick, R.; Bauer, P.; Integrated PV charging of EV fleet based on energy prices, V2G and offer of reserves. *IEEE Trans. Smart Grid* **2019**, *10*, 1313–1325. [CrossRef]
4. Zhong, W.; Xie, K.; Liu, Y.; Yang, C.; Xie, S. Topology-aware vehicle-to-grid energy trading for active distribution systems. *IEEE Trans. Smart Grid* **2019**, *10*, 2137–2147. [CrossRef]
5. Alvaro-Hermana, R.; Fraile-Ardanuy, J.; Zufiria, P.J.; Knapen, L.; Janssens, D. Peer to peer energy trading with electric vehicles. *IEEE Intell. Transp. Syst. Mag.* **2016**, *8*, 33–44. [CrossRef]
6. Shurrab, M.; Singh, S.; Otrok, H.; Mizouni, R.; Khadkikar, V.; Zeineldin, H. An efficient vehicle-to-vehicle (V2V) energy sharing framework. *IEEE Internet Things J.* **2021**, *9*, 5315–5328. [CrossRef]
7. Umesh, B.S.; Khadkikar, V.M.; Zeineldin, H.; Singh, S.; Otrok, H.; Mizouni, R. Direct electric vehicle to vehicle (V2V) power transfer using on-board drivetrain and motor windings. *IEEE Trans. Ind. Electron.* **2021**, *69*, 10765–10775.
8. Global EV Outlook 2020. Available online: https://www.iea.org/reports/global-ev-outlook-2020 (accessed on 8 April 2024).
9. Electric Vehicle Market by Component, Vehicle (Passenger Cars, CV), Propulsion (BEV, PHEV, FCEV), Vehicle Drive Type (FWD, RWD, AWD), Vehicle Top Speed (<125 mph, >125 mph), Charging Point, Vehicle Class, V2G, Region-Global Forecast 2030. Available online: https://www.marketsandmarkets.com/Market-Reports/electric-vehicle-market-209371461.html (accessed on 8 April 2024).
10. Chekired, D. A.; Khoukhi, L.; Mouftah, H. T. Fog-computing-based energy storage in smart grid: A cut-off priority queuing model for plug-in electrified vehicle charging. *IEEE Trans. Ind. Inform.* **2020**, *16*, 3470–3482. [CrossRef]
11. Zhang, P.; Qian, K.; Zhou, C.; Stewart, B. G.; Hepburn, D. M. A methodology for optimization of power systems demand due to electric vehicle charging load. *IEEE Trans. Power Syst.* **2012**, *27*, 1628–1636. [CrossRef]
12. Chen, J.; Zhang, Y.; Su, W. An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks. *China Commun.* **2015**, *12*, 9–19. [CrossRef]

13. Yan, Q.; Zhang, B.; Kezunovic, M. Optimized operational cost reduction for an EV charging station integrated with battery energy storage and PV generation. *IEEE Trans. Smart Grid* **2019**, *10*, 2096–2106. [CrossRef]
14. 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. Informat.* **2018**, *14*, 3690–3700. [CrossRef]
15. Aggarwal, S.; Kumar, N.; Gope, P. An efficient blockchain-based authentication scheme for energy-trading in V2G networks. *IEEE Trans. Ind. Informat.* **2020**, *17*, 6971–6980. [CrossRef]
16. 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]
17. Yucel, F.; Akkaya, K.; Bulut, E. Efficient and privacy preserving supplier matching for electric vehicle charging. *Ad Hoc Netw.* **2019**, *90*, 101730. [CrossRef]
18. Tandon, R.; Gupta, P.K. SV2VCS: A secure vehicle-to-vehicle communication scheme based on lightweight authentication and concurrent data collection trees. *J. Ambient Intell. Human. Comput.* **2021**, *12*, 9791–9807. [CrossRef]
19. He, Y.; Zhang, C.; Wu,B.; Geng, Z.; Xiao, K.; Li, H. A trusted architecture for EV shared charging based on blockchain technology. *High-Confid. Comput.* **2021**, *1*, 100001. [CrossRef]
20. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access* **2018**, *6*, 13565–13574. [CrossRef]
21. Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Trans. Ind. Informat.* **2017**, *13*, 3154–3164. [CrossRef]
22. Kim, M.; Lee, J.; Oh, J.; Park, K.; Park, Y.; Park, K. Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers. *Appl. Energy* **2022**, *322*, 119445. [CrossRef]
23. Sun, G.; Dai, M.; Zhang, F.; Yu, H.; Du, X.; Guizani, M. Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles. *IEEE Internet Things J.* **2020**, *7*, 7868–7882. [CrossRef]
24. Son, S.; Lee, J.; Kim, M.; Yu, S.; Das, A.K.; Park, Y. Design of blockchain-based lightweight V2I handover authentication protocol for VANET. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 1346–1358. [CrossRef]
25. Blockchain GDPR Privacy by Design. Available online: https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf (accessed on 8 April 2024).
26. Bernabe, J.B.; Canovas, J.L.; Hernandez-Ramos, J.L.; Moreno, R.T.; Skarmeta, A. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access* **2019**, *7*, 164908–164940. [CrossRef]
27. Zhang, H.; Wang, J.; Ding, Y. Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Eenrgy* **2019**, *180*, 955–967. [CrossRef]
28. 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]
29. 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]
30. Kumari, A.; Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. When blockchain meets smart grid: Secure energy trading in demand response management. *IEEE Netw.* **2020**, *34*, 299–305. [CrossRef]
31. 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]
32. Guan, Z.; Lu, X.; Yang, W.; Wu, L.; Wang, N.; Zhang, Z. Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid. *J. Parallel Distrib. Comput.* **2021**, *147*, 34–45. [CrossRef]
33. Xia, S.; Lin, F.; Chen, Z.; Tang, C.; Ma, Y.; Yu, X. A bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6856–6868. [CrossRef]
34. 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]
35. LI, M.; Hu, D.; Lal, C.; Conti, M.; Zhang, Z. Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things. *IEEE Trans. Ind. Informat.* **2020** *16*, 6564–6574. [CrossRef]
36. Yahaya, A.S.; Javaid, N.; Almogren, A.; Ahmed, A.; Gulfam, S.M.; Radwan, A. A two-stage privacy preservation and secure peer-to-peer energy trading model using blockchain and cloud-based aggregator. *IEEE Access* **2021**, *9*, 143121–143137. [CrossRef]
37. Cui, J.; Wu, D.; Zhang, J.; Xu, Y.; Zhong, H. An efficient authentication scheme based on semi-trusted authority in VANETs. *IEEE Trans. Veh. Technol.* **2019** *68*, 2972–2986. [CrossRef]
38. Chai, H.; Leng, S.; He, J.; Zhang, K.; Cheng, B. Cyberchain: Cybertwin empowered blockchain for lightweight and privacy-preserving authentication in internet of vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 4620–4631. [CrossRef]
39. Cani, A.S.; Bertino, E.; Yuan, D.; Meng, K.; Dong, Z.Y. SPrivAD: A secure and privacy-preserving mutually dependent authentication and data access scheme for smart communities. *Comput. Secur.* **2022**, *115*, 102610.
40. Decentralized Identifiers (DIDs) v1.0 Core Architecture, Data Model, and Representations. Available online: https://www.w3.org/TR/2021/PR-did-core-20210803/ (accessed on 8 April 2024).

41. Verifiable Credentials Data Model 1.0 Expressing Verifiable Information on the Web. Available online: https://www.w3.org/TR/2021/REC-vc-data-model-20211109/ (accessed on 8 April 2024).
42. Automated Validation of Internet Security Protocols and Applications. Available online: http://www.avispa-project.org/ (accessed on 8 April 2024).