Journal of Cleaner Production 422 (2023) 138355

Contents lists available at ScienceDirect

Journal of Cleaner Production

journal homepage: www.elsevier.com/locate/jclepro

Leveraging self-sovereign identity & distributed ledger technology in renewable energy certificate ecosystems

Md Sadek Ferdous [a,b], Umit Cali [c,d], Ugur Halden [d,*], Wolfgang Prinz [e]

[a] *Department of Computer Science and Engineering, BRAC University, Science Complex, Dhaka, 1000, Bangladesh*
[b] *Imperial College Business School, Imperial College London, South Kensington Campus, Exhibition Rd, London, SW72AZ, United Kingdom*
[c] *University of York, School of Physics, Engineering and Technology, Heslington, York YO10 5DD, United Kingdom*
[d] *Department of Electric Energy, Norwegian University of Science and Technology, O. S. Bragstads Plass 2E, Trondheim, 7034, Trøndelag, Norway*
[e] *Fraunhofer Institute for Applied Information Technology, Schloss Birlinghoven, Konrad-Adenauer-Straße, Sankt Augustin, 53757, North Rhine-Westphalia, Germany*

ARTICLE INFO

Handling Editor: Giovanni Baiocchi

Keywords:
Self-sovereign identity
SSI
Renewable energy certificate
Blockchain technology
REC trading
Architecture

ABSTRACT

Renewable Energy Certificates (RECs) are tradable units that represent the commodity in the form of environmental attributes generated for each unit of electricity produced by a renewable energy source. Furthermore, the energy sector's digitalization ushers in new crucial enablers like Distributed Ledger Technology (DLT), which may be used for REC record tracking and trading. Unfortunately, there are a number of outstanding issues such as the lack of a common standard for the representation, communication, and verification of REC, reliance on centralized entities, and others. In order to harness the true potential of energy DLT and REC, it is imperative to address these issues. In this visionary article, we propose a holistic approach which leverages a novel decentralized identity mechanism called Self-sovereign Identity (SSI) and DLT. We present its architecture, based on a rigorous threat model and requirement analysis as well as detailed use-cases to illustrate how the architecture can be used in different REC use-cases.

1. Introduction

Renewable Energy Sources (RES) are replacing fossil fuels like coal and nuclear power in the production of electricity globally. This trend was initially sparked by climate change policies, but it has since been accelerated by rising economic competition and a growing desire among electricity consumers to buy clean energy (Pan and Dong, 2023). The Levelized Cost of Energy (LCOE) continues to decrease due to falling component prices as the manufacturing capacity of RES components like PV (Photovoltaic) modules, inverters, and other crucial components rise as a result of greater deployment and consumption, hence increasing the incentive for quick deployment (Zafoschnig et al., 2020). According to National Renewable Energy Laboratory (NREL) estimates, between 2010 and 2020, there were 64%, 69%, and 82% cost reductions between residential, commercial, and utility-scale solar PV installments (Feldman et al., 2021).

Additionally, as the energy industry became more democratic (Halden et al., 2021), consumers started to behave as producers as well, giving rise to the name "prosumers". During their Power Purchase Agreement (PPA), the end users can select a full renewable energy usage according to their personal preferences with their electricity suppliers. However, after being injected into the grid, it is impossible to discriminate between energy coming from traditional and renewable sources. Renewable Energy Certificates (RECs) were offered as a solution to this issue and to assure consumers that the energy they are paying for and using originates from RES (Bogensperger and Zeiselmair, 2020). Once the energy producer releases the generated energy to the grid, the RECs can be transferred to the open market by the issuer and then can be traded across the participating agents for various tasks such as ensuring the energy does indeed comes from renewable sources, or for offsetting emissions, acting as a carbon credit (Allayannis and Tenguria, 2011; Ashley and Johnson, 2018).

However, we have identified that the traditional REC mechanism has a number of issues: the lack of a common global standard for the representation, transfer and verification mechanism involving RECs, reliance on third parties, and a double counting issue when REC is retired. There is another important aspect in the existing setting is how users and different entities are identified and managed in a REC system. An Identity Management System (IMS) can be utilized to achieve this goal. There are a few IMSs: SAML (Security Assertion Markup Language)

* Corresponding author.
E-mail address: ugur.halden@ntnu.no (U. Halden).

https://doi.org/10.1016/j.jclepro.2023.138355
Received 30 May 2023; Received in revised form 27 July 2023; Accepted 5 August 2023
Available online 21 August 2023

(Hughes and Maler, 2005)), OpenID (Recordon and Reed, 2006) and OAuth (Open Authorization) (Hardt et al., 2012). Unfortunately, most of them are centralized in nature. In addition, they suffer from other issues as well: SAML is hard to manage whereas it is difficult to maintain trust with other (OpenID and OAuth) IMSs as they are based on the Open Trust paradigm (Ferdous, 2015). A novel decentralized identity construct called Self-sovereign Identity (SSI) (Ferdous et al., 2019) has been introduced to mitigate many of these issues. Unlike other systems, SSI transfers much of the control to the user, thus providing better privacy.

Since the introduction of Bitcoin, the concept of blockchain or Distributed Ledger Technology (DLT) has received much attention as it offers a unique combination of advantages such as distributed data sharing, data immutability, data availability, data provenance, accountability, and transparency (Bitcoin; Chowdhury et al., 2019). However, there has been a lot of unpredictability in the cryptocurrency field, and there have been a growing number of bad actors who have seized the opportunity to profit from the initial euphoria surrounding the said technology. Nevertheless, the underlying blockchain technology has grown independently, and a wide range of both hypothetical and actual use cases have surfaced such as the utilization of DLT within supply chains (T. H. foundation, 2019) and various energy-related applications such as the merge of Danish Energinet and the Concordium blockchain for energy provenance (C. news). Therefore, in recent years, the research area of DLT has seen major attention.

Together with the development of various DLT types such as Ethereum blockchain and Hyper Ledger Fabric (HLF) which supports autonomous code execution and code immutability (Ethereum), the outstanding and holistic issues within REC, such as how they are created, managed and traded can be solved. In this article, we present such a holistic vision leveraging SSI and Distributed Ledger Technology (DLT). Therefore, the major contributions of this article can be listed as:

- A novel decentralized SSI-based architecture for REC trading use-cases based on a rigorous threat model and requirement analysis.
- A detailed use-case to illustrate how the proposed architecture could be utilized in different aspects of REC trading.
- The demonstration of the potential benefits of using SSI for REC trading.
- A detailed analysis of the advantages and limitations of the proposed architecture.

Structure. In Section 2, we present a brief introductory discussion of Distributed Ledger Technology (DLT) and SSI. Then, in Section 3, we discuss the Energy DLT domain and highlight some of the issues in the current REC trading ecosystem. We present the proposed architecture in Section 4 with a discussion of the utilized threat model and requirement analysis. Section 5 provides detailed protocol flows in different REC use-cases utilizing the proposed architecture which showcases the applicability of our approach. We discuss different aspects of the proposed architecture in Section 6. We review the existing related research works and compare them with our proposal against a number of criteria in Section 7 and finally, we conclude in Section 8.

2. Background

In this section, we present a brief background on DLT (Section 2.1) and Self-sovereign Identity (Section 2.2).

2.1. Distributed ledger technology

Bitcoin is the first decentralized digital currency to be widely popular which can function even without relying on a central entity, such as a central bank (Nakamoto, 2019). Bitcoin is based on a novel underlying mechanism called *blockchain* which represents a technological breakthrough. A blockchain is an example of a distributed ledger-like data structure which is shared and maintained by a group of Peer-to-Peer (P2P) nodes (Chowdhury et al., 2019). That is why blockchain technology is often regarded as a Distributed Ledger Technology (DLT). A blockchain consists of chains of blocks which are grouped together by cryptographic mechanisms following rigorous sets of rules. Each of these blocks contains some transactions where each transaction facilitates either a financial transaction enabling a user to transact a certain amount of bitcoin to another user/users or a data transaction to transfer data between users and systems. Each block is structured in such a way that it refers to its previous block using a cryptographic hash, which refers to its previous block, thus forming the notion of chain of blocks or blockchain.

Strong research and development activities in the industry led to the evolution of next generation blockchain systems which can facilitate the deployment and autonomous execution of computer programs, known as *smart-contracts* (Ferdous et al., 2019). These smart-contracts are stored in the blockchain. The execution of these smart-contracts are carried by virtual machines whose states are stored and maintained on top of the respective blockchain. The utilization of blockchain in different aspects makes smart-contracts and their executions immutable and irreversible, a sought-after property in many application domains. Furthermore, such a smart-contract supporting blockchain system has some other advantages, namely, persistence and distributed control of data, accountability, transparency and data provenance.

A blockchain can have different types based on different properties. However, based on who can access a blockchain system, there are generally two types:

- **Public blockchain:** A public blockchain, also known as the *permissionless blockchain*, allows anyone to use the blockchain and to participate in the network for blockchain governance and transaction creation at any time. Examples of public blockchain systems are Bitcoin (Bitcoin), Ethereum (Ethereum), Litecoin (Litecoin) and Monero (Monero).
- **Private Blockchain:** On the other hand, a private blockchain system, also known as the *permissioned blockchain*, enforces rules which allow only authorized and trusted entities to participate in the system. Examples of private DLT systems are Hyperledger Platforms (Hyperledger), Quorum (Quorum Blockchain), and others.

2.2. Self-sovereign identity (SSI) & its ecosystem

Self-sovereign Identity (SSI, in short) is an emerging paradigm in the identity management domain. Its main motivation is to empower users with their identity data so that they can create and control their identities whenever they want without relying on any trusted parties (Allen, 2022; Ferdous et al., 2019, 2023), ultimately resolving some of the issues (e.g. the centralized nature of the existing IMSs and lack of user control over identity data) prevalent in the existing identity management systems and protocols.

Like other IMS, SSI also has a number of entities: Issuer, Holder, and Verifier, as illustrated in Fig. 1. An issuer (e.g. an academic institution) is responsible for issuing credentials (e.g. a degree) for a user when requested. A credential contains a number of digitally-signed claims regarding the user where a claim implies a statement about the user from the issuer (Ferdous et al., 2019). The user stores the credentials in a wallet and that is why a user is also known as a holder. In order to access a service (e.g. a job) a verifier (e.g. an employer) requests a presentation from the holder. A presentation is a subset of the previously released claims within a credential and is better suited for user privacy. Then, the holder releases the requested claims in the form of a presentation.

In order to facilitate the interactions of the SSI entities, the notion of Decentralized Identifiers (DIDs) (Decentralized Identifiers, 2022) and Verifiable Credentials (Verifiable Credentials Data Model 1, 2022) have been introduced. A decentralized identifier is an entity (e.g. machine and user) generated identifier which uniquely identifies the entity

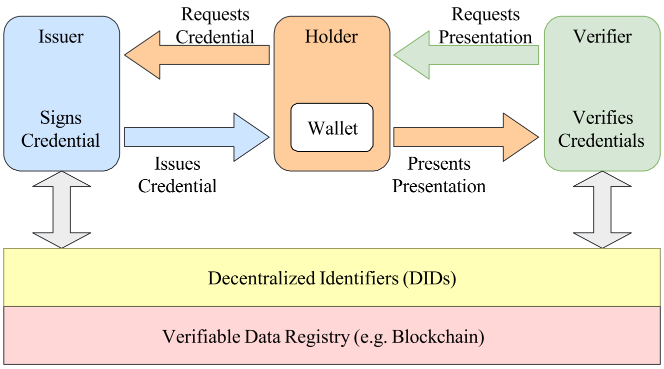

Fig. 1. SSI entities and their relations.

within an application domain. It is tied to a public key of the user and does not rely on any special organization. For example, an email is a centralized identifier as it can uniquely identify an entity within any application domain, however, is dependent on a centralized email provider. Since a DID is generated from a public key controlled by the user, there is no reliance on any other party. A DID Document (*DID Doc* in short) is a JSON object containing the DID of an SSI entity, its linked cryptographic public keys and further metadata.

Verifiable credentials (VCs) are collections of digitally-signed claims made by an issuer for a user (holder). A claim can express different attributes of the user, e.g. date of birth, degree entitlement and address as well as different relationships. When a user shares a VC in the form of a verifiable presentation (VP) to a verifier, the verifier can easily verify the claim by validating the digital signature. This will require the verifier to get hold of public keys of the issuer which can be retrieved using the corresponding DIDDoc of the issuer.

This verification mechanism can be backed with strong security guarantee only if the corresponding DIDDoC could be stored in an immutable and verifiable registry. A distributed ledger represents such an immutable, persistent and verifiable data registry and that is why it is widely used in the SSI ecosystem.

3. Energy DLT

Traditional centralized power grids experience a variety of changes as a result of the increasing usage of renewable energy sources (RES), including an increase in power system imbalances and a heightened vulnerability to cyberattacks. Various enabling technologies, such as Artificial Intelligence (AI), Machine Learning (ML), the Internet of Things (IoT), and Distributed Ledger Technology (DLT), can be used to mitigate such challenges.

DLT may be seen as one of the most disruptive enablers for the digitization of power systems and markets due to its potential to provide enhanced security, immutable audit trails, accountability and the removal of unnecessary third parties. DLT may be used in the energy industry for use-cases such as P2P energy trading, e-mobility, energy financing, and REC trading (Cali et al., 2022a).

3.1. Renewable energy certificate (REC) & its ecosystem

Distinguishing which electricity originates from RES and which comes from fossil fuels is impossible to achieve once the electricity is injected into the grid. As a response, a number of governmental organizations have introduced certificates that assist both users and producers of clean energy to enable the tracking of clean energy. Internationally, a wide range of certificates have been adopted, including British Renewable Energy Guarantees of Origin (REGO) (Renewable energy guarantees of origin, 2022), American RECs (Renewable energy certificates, 2022) and European Guarantees of Origin (GO). Since RECs are entirely digital assets, they have been referred to as “the money of renewable energy markets” because they are free from the physical and geographic limitations associated with energy exchange (Holt et al., 2011).

There are a number of entities within a REC ecosystem (Fig. 2). We discuss about these entities below:

- **Renewable Energy Sources (RES)** represents the renewable and clean energy producer,
- **REC Issuer:** is the governmental body with the ability to issue RECs,
- **REC Buyer/Seller** denotes the entities which aim to either buy or sell RECs,
- **REC Tracking System:** is the tracking system for REC and participating entities,
- **Broker/Aggregator:** is an agent with the executive right to perform buy and sell operations on behalf of a buyer and seller,
- **Auditor/Regulator:** is an entity which is responsible for enforcing regulatory frameworks and audits.

3.2. REC trading

The power flow from traditional generation methods like coal-based power plants or from renewable sources like PV or wind becomes indistinguishable as it enters the physical confines of the power grid. However, by using a REC, the energy source has the ability to be officially documented, giving end users the chance to confirm that the electrical energy they are using comes from renewable sources. This can in turn provide users a sense of support and increase incentives for rapid decarbonization (United States Environmental Protection Agency, 2021).

As a result, the REC trading framework provides a verifiable means for system participants to buy and sell renewable energy. The first stage is to assign a REC certificate to the energy produced, which can then be traded as shown in Fig. 2. In the meantime, factors such as certificate generation frequency (per kWh or per MWh), the system’s current energy supply and demand, etc., can be used to calculate the price of the certificate. In Fig. 2, the various interactions between the participating agents can be seen. The flowchart begins by the retrieval of RES generation data from the RES operator by the issuer. Later on, the appropriate amount of RECs are issued and sent back to RES operator, who then sells the RECs to a broker/aggregator. The REC buyers and sellers can then utilize the broker agent for buying and selling RECs or swapping the already bought RECs within themselves. Meanwhile, the REC tracking system keeps tracks of every interaction between various participating agents, while the auditor checks for any regulatory framework breaches.

DLT-based REC: Fig. 3 demonstrates the overview structure of a DLT-based REC Transaction and Trading System (RTTS) (Cali et al., 2022b). RTTS accommodates three main actors: 1) Renewable Energy Sources (RES), 2) REC Buyers and Sellers and 3) Auditor/Regulatory

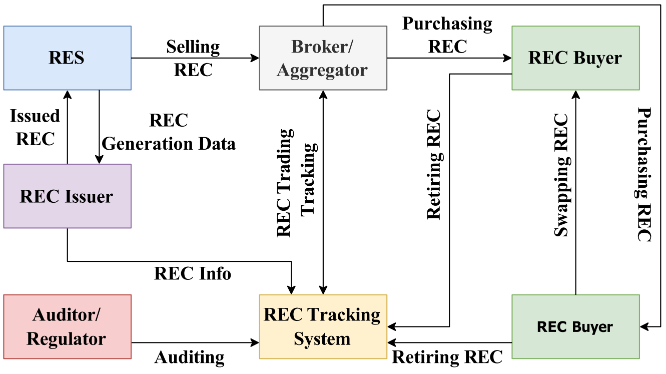

Fig. 2. Entities and their relations in traditional REC.

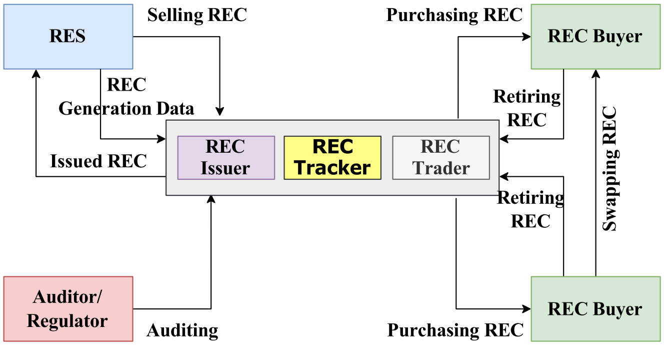

Fig. 3. Overview of DLT-based REC Transaction and Trading system.

Authority. The core part of the DLT-based RTTS ensures REC issuance, tracking and trading functionalities. Once the REC generation data are transmitted to the RTTS, the system issues a REC for this process and forwards the newly generated REC to the owner of the RES asset. The RES asset owner can sell the REC on the digital market, which is operated via RTTS's REC Trader Module. REC buyers can obtain RECs from the REC market. If they consume the REC, the status of the REC will be changed to "retired". The REC Buyers may prefer to swap or resell their RECs to another REC Buyer without using them. The REC Tracker module makes sure that the RECs and their status are track-recorded on-chain of the DLT network. The REC Tracker module has a special function of resolving the "double counting problem" as well. Depending on the market, the Auditor or Regulator can proceed with the track recording of the entire transaction flow to make sure that there is no violation of the rules.

Using this DLT-based approach has several advantages as discussed next. For an effective and stable electrical market (Zhang et al., 2020), grid operators should always be informed of the usage habits of their users. Thus, in decentralized marketplaces with several smaller participants, information security becomes even more crucial. Due to this alteration, it is necessary to determine who is in charge of the following aspects of the electricity market, including:

- Whom does the customer data belong,
- Regulations regarding the access and use of customer data,
- Data security and privacy of the customers.

Market participants can share information (such as energy production and consumption, current and voltage levels, power factor, etc.) with their utility provider by utilizing a smart meter. Blockchain technology combined with metering infrastructure may open the door for prosumers to receive automated energy service billing, which may result in lower administrative costs. Demand response and behavioral change can be encouraged by the traceability of energy generated and used, which can inform prosumers about the sources and cost of their power supply. Following data capture, a blockchain-based information management system can guarantee reliable state verification, data consistency, security from communication failures (Siano et al., 2019), and cyberattacks (Münsing et al., 2017).

3.3. Issues in a REC system and its potential solution

The processes involved in the current setting of the REC ecosystem have a number of issues as presented below:

- **I-1:** There is no commonly accepted and standardized global format for generating a new REC. There are regional REC issuers who are responsible for issuing RECs and they issue RECs in their own specified formats, which can create a major inter-operability issue.
- **I-2:** The verification process, and other associated security mechanisms, of a REC is not standardized. This means that different approaches might be deployed to verify RECs in different regions. A few examples of operations where security is of paramount importance are ensuring the provenance and integrity of REC data while they are being generated, ensuring the ownership of REC (particularly when they are sold) and facilitating the transparency of the REC ownership and the REC retiring process.
- **I-3:** The communication between different entities in the REC ecosystem is not standardized. Without a proper standardized communication mechanism, it is difficult to ensure security and inter-operability.
- **I-4:** Each of the entities within the ecosystem must be identified and authenticated to ensure that only correctly authenticated entities can participate in the ecosystem. Generally, an Identity Management System (IMS) is utilized to manage the identities of users or organizations and then identify when required using a standardized approach (Ferdous and Poet, 2012). There are many standardized approaches in the form of Identity protocols, however, most of them are privacy invasive, particularly for users and need to rely on a third party (Ferdous et al., 2019).
- **I-5:** The current REC system heavily depends on a third party called *brokers/aggregator* which might create a single point of failure when the respective entity is not functioning properly.
- **I-6:** The retired RECs' track record may not be inserted to the system properly or on time, introducing a double counting problem. For this reason, the retired RECs can still be counted as active RECs by the system.

Among these issues, the reliance on brokers (I-5) can be addressed by integrating DLT within the REC ecosystem. Towards this aim, there have been a number of proposals which can be found in (Lai et al., 2021; Spinnell and Zimberg, 2018; Wang et al., 2021; Cali et al., 2022b). Among these works, the work presented by Cali et al. (2022b) is simple and yet transformative and that is why we have based the current work on their work.

The scalability and energy consumption of the present consensus mechanisms are also two drawbacks of DLT-based REC transaction and trading systems. It should be emphasized, however, that the use of DLT as a facilitator for REC trading is an active research area, and to support this research area new consensus mechanisms are being developed, such as Proof of Generation (PoG) (Zhao et al., 2020).

Unfortunately, utilizing DLT alone cannot resolve other issues. IMS and their associated protocols such as Security Assertion Markup Languages (SAML, (Hughes and Maler, 2005)), OpenID (Recordon and Reed, 2006) and OAuth (Hardt et al., 2012) could be useful to mitigate some of the other issues as most identity protocols utilize standardized identification/authentication and communication methods. Therefore, they could be effectively leveraged to resolve the identified issues in the REC ecosystem. However, these protocols have their own issues. For example, SAML requires to build and maintain a trusted network which is difficult to scale (Alom et al., 2021). On the other hand, OpenID and OAuth are all based on open trust paradigms where there is no trusted entities. Moreover, all these protocol require to rely on centralized entities (an Identity Provider in the case of SAML and an OpenID provider for OpenID) to function which can create a single point of failure. Furthermore, these protocols are mostly organization centric and the problems a user faces to manage their organization-centric identities are often overlooked (Ferdous et al., 2019). Because of these reasons, these identity protocols are not ideal candidates for resolving the identified issues.

4. SSI-integrated REC

In this section, we present our proposed SSI-integrated REC system. Towards this aim, we present the threat model and requirement analysis

(Section 4.1) and then we present the architecture (Section 4.2).

4.1. Threat model & requirement analysis

Threat modeling is an integrated process of designing any secure system. Since a major aspect of the proposed SSI-integrated REC system would be to ensure its security in different scopes, it is imperative that a rigorous threat model is considered. A threat model identifies different security threats pertinent to (IT) assets in the respective domain, REC in the scope of this article. Then, in order to mitigate these threats, different security requirements need to be formulated (Myagmar et al., 2005). Towards this step, to model threats, we have chosen a well established threat model called STRIDE (Shostack, 2014). STRIDE is an abbreviation of six threats: **S**poofing Identity, **T**ampering with Data, **R**epudiation, **I**nformation Disclosure, **D**enial of Service (DoS) and **E**levation of Privilege. Next, we analyze how these threats are related to the proposed work.

T1. **Spoofing Identity:** This threat implies that an attacker can generate a VC-based REC by spoofing someone else's identity.
T2. **Tampering with Data:** This threat implies that an attacker can modify crucial information (e.g. claims in a VC or REC generation data) for malicious purposes.
T3. **Repudiation:** This threat implies that a corresponding entity can repudiate invalid and illegal operations (e.g. manipulating the REC retirement process and issuing fake RECs).
T4. **Information Disclosure:** This threat implies that sensitive data are revealed to an attacker unintentionally.
T5. **Denial of Service (DoS):** This threat implies that the whole REC ecosystem, particularly the Broker/Aggregator or the REC Tracking System is subject to a DoS attack.
T6. **Elevation of Privilege:** This threat implies that an attacker might use other attack vectors to elevate their access privilege within the online services.

In addition to these, we have considered an additional threat which is crucial for any secure system, however, not captured by the STRIDE model.

T7. **Replay:** This threat implies that an attacker might capture an old data packet (representing a request/response) and submit it afterwards, thus launching a replay attack.

Next, we present a set of functional and security requirements. The functional requirements capture the core functionalities of the proposed system while security requirements ensure that they mitigate the identified threats.

Functional Requirements (FR): The functional requirements are presented below.

F1. The system needs to be integrated with a smart-contract supporting blockchain platform so as to automate the majority of its functionalities by the smart-contract.
F2. The proposed system needs to support an SSI framework so that VC can be utilized in a seamless fashion.
F3. The roles of the REC ecosystem must be modified so that they can assume the roles of different SSI entities.
F4. The whole ecosystem needs to be redesigned in such a way that it can accommodate all the existing functionalities.

Security Requirements (SR): Next, we present a set of security requirements to address the identified security threats.

S1. The system must ensure that only authenticated and authorized entities can generate VC-based RECs. This will mitigate the *T1* threat.
S2. The system must guard against any unauthorized modification of REC data within a VC to mitigate the *T2* threat.
S3. The system must utilize digital signature in order to mitigate the *T3* threat.
S4. Any crucial data related to a VC or REC must be transmitted in encrypted format via networks so as to ensure the confidentiality of the data. This can mitigate the *T4* threat.
S5. The system should employ mechanisms which can mitigate or at least reduce the possibility of any DoS attack so as to mitigate the *T5* threat.
S6. The system should utilize an access control mechanism to ensure that an attacker cannot elevate their access privilege and thereby mitigating the *T6* threat.
S7. The system must take protective measures against any replay attack in order to mitigate the *T7* threat.

4.2. Architecture

In this section, we present the proposed architecture to integrate SSI functionalities within the REC ecosystem. The presented architecture will need to ensure that it satisfies all the (functional and security) requirements identified in Section 4.1.

Combined roles: Towards that aim, at first, we explore how the roles of SSI entities could be subsumed within different entities of the REC ecosystem. As discussed earlier, there are three roles within SSI: issuer, holder (user) and verifier. An issuer generates and releases a VC about a user which is stored within a wallet controlled by the holder and when required, the user releases that VC to the verifier for verification. The combined roles of SSI and REC entities are presented in Fig. 4 where the orange rectangle specifies the SSI role for each REC entity.

The SSI analogy could be extended for the REC ecosystem where the REC issuer will assume the role of a VC issuer (Fig. 4) by issuing a REC certificate in the form of a VC (denoted with VC_{REC} afterwards). This VC_{REC} is supplied to the RES which is stored in their wallet securely, hereby, the RES is acting as a Holder (Fig. 4). When the RES sells $VC - REC$ via the DLT-based transaction and trading system, a REC buyer buys $VC - REC$ after verifying it, thus the buyer takes the role of a verifier (Fig. 4). Once bought, $VC - REC$ is stored in their wallet and changes their role to be the holder. The auditor/regulator can verify each of this operation as they are carried out via the DLT-based transaction and trading system, hence, taking the role of a verifier (Fig. 4).

At the first instance, Fig. 4 might look like a repetition of Fig. 3. However, the first one (Fig. 4) is an extended version of the latter (Fig. 3). In Fig. 4, we have augmented the SSI entities with their corresponding SSI roles. In addition, different components in the DLT-based REC system (Fig. 4) has been subsumed within a single component called DLT-based Tracking & Trading System in Fig. 4.

Architecture: In Fig. 5, we present the high-level architecture of the proposed SSI-based REC system. There are a number of components

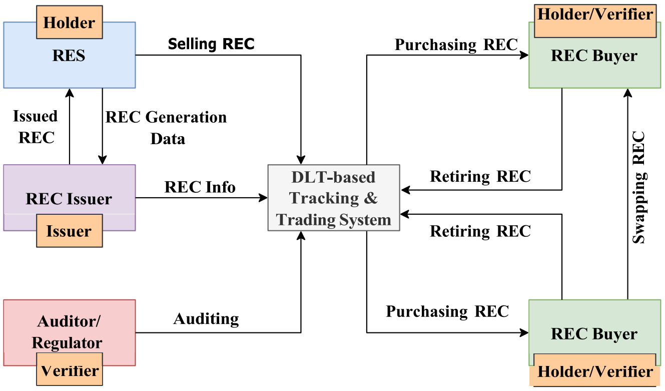

Fig. 4. Combined roles of SSI & REC entities.

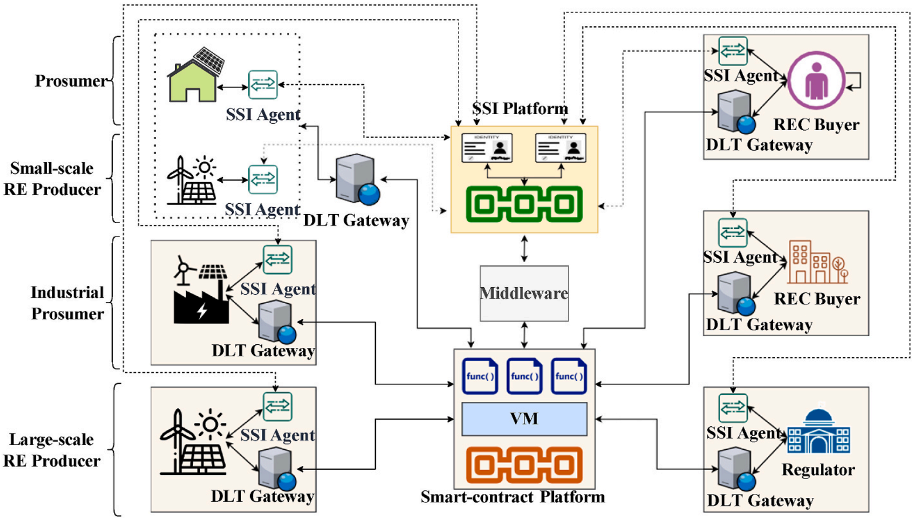

Fig. 5. High-level architecture.

within the system. We discuss each of the each components below.

- **Entities:** In the system, there are mainly three categories of entities (as in any REC system): RES, Regulators and REC Buyer. While the Regulator and the REC Buyers assume the roles discussed previously, we have differentiated between two types of RES: commercial RES and (general) RES. A commercial RES is a large scale power plant generating electricity from one or multiple green renewable energy sources. On the other hand, a (general) RES is an individual prosumer (producer and consumer) who has a small-scale renewable energy source (e.g. a solar panel) installed in their house and takes part in the REC ecosystem to generate or sell REC certificates. The motivation of this categorization is explained later.
- **Smart-contract Platform:** This platform is a smart-contract supporting DLT platform providing the functionalities of the DLT-based Transaction and Trading System as illustrated in Fig. 4. There will be a number of smart-contracts for the required functionalities. The smart-contract platform will be responsible for issuing RECs and recording the buying and selling of RECs over time.
- **DLT Gateway:** A DLT Gateway is a web server which serves two purposes: i) it exposes APIs for other web/mobile applications to interact with the DLT platform and ii) it utilizes respective libraries to establish communications with the DLT platform and invokes different smart-contracts. The core idea is that other web and mobile applications do not directly interact with the DLT platform, instead a DLT gateway is used for this purpose. Each respective entity must utilize a DLT gateway to interact with the DLT platform. This could be difficult for an individual RES as the DLT Gateway often needs to store the full blockchain to complete its functionalities and hence might require considerable storage and/or computation capabilities. To tackle this issue, we envision the utilization of a shared DLT Gateway which could be shared by many individual RES or REC Buyers. On the other hand, commercial RES and institutional REC buyers can afford to host their own DLT Gateways.
- **SSI Platform:** The SSI platform provides the SSI functionalities: VC-based REC generation, storage, release and the verification mechanism. Such SSI platforms usually rely on a specific DLT platform (e.g. Hyperledger Indy (Hyperledger Indy)). If such SSI functionalities could be facilitated by a general purpose smart-contract supporting DLT platform (e.g. Ethereum (Ethereum) or Hyperledger Fabric (Hyperledger Fabric)), we could essentially use a single DLT platform. However, for the time being, we would need to use a separate SSI platform to carry out the SSI functionalities.
- **Middleware:** A middleware is a web service which facilitates the communications between the SSI and the smart-contract platforms. If a smart-contract platform could provide SSI functionalities as we discussed and therefore, there is no need for a separate SSI platform and hence, this middleware could be completely excluded.
- **SSI Agent:** In order the interact with the SSI platform, each entity will need to utilize a software called the SSI Agent. An SSI agent is also the software which can be used for the storage and retrieval of any VC-generated REC. For individual users, such agents would presumably be mobile apps. However, for institutional entities, such agents could be web apps hosted within their premises.

5. Use-case

In this section, we present different use-cases within the REC ecosystem using the proposed architecture. At first, we introduce the mathematical notations that will be used in the use-case and then we present five different use-cases: Registration, VC-REC Issuance, VC-REC Buying/selling, VC-REC Swapping and VC-REC Retiring.

Mathematical notations: Before outlining the use-cases, we introduce the cryptographic notations to be used in the protocol flow for each use-case. The cryptographic notations are presented in Table 1. Next, using these cryptographic notations, we introduce a few other terminologies.

We use the notation *RES* to denote the combined set of RE (Renewable Energy) producers/consumers, such as individual prosumers, industrial prosumers, small-scale RE producers and large-scale RE producers. Thus, *RES* can defined in the following way (Equation (1)):

$$RES \triangleq \langle P \cup IP \cup SS \cup LS \rangle \tag{1}$$

Next, we use the notation E to denote the set of all principal stakeholders within the REC ecosystem. Hence, E is defined as per Equation (2):

$$E \triangleq \langle RES \cup REG \cup RB \rangle \tag{2}$$

Finally, we denote a VC with this notation $VC_{e_1}^{e_2}$ which signifies a VC produced by an entity e_1 for another entity e_2. Such a VC is defined as a collection of attribute name value pairs signed by e_1 and is defined as per Equation (3):

$$VC_{e_1}^{e_2} \triangleq \langle \{(a_1, av_1), (a_2, av_2), \ldots, (a_n, av_n)\}_{K_{e_1}^{-1|e_2}} \rangle \tag{3}$$

Table 1
Cryptographic notations.

Notations	Description
E	Set of all stakeholders
P	Set of Prosumers
IP	Set of Industrial Prosumers
SS	Set of Small-scale RE Producers
LS	Set of Large-scale RE Producers
RES	Set of RE producers and prosumers
RB	Set of REC buyers
REG	Regulator
SCP	Smart-contract Platform
$K_{e_1}^{e_2}$	SSI Public key of a e_1 to be used with e_2, here, e_1, $e_2 \in E$
$K_{e_1}^{-1\|e_2}$	SSI Private key of a e_1 to be used with e_2, here, e_1, $e_2 \in E$
K_e	General public key of a e, here, e $\in E$
K_e^{-1}	General private key of a e, here, e $\in E$
W_e	Wallet of entity e, here, $e \in E$
ID_e	General identifier of an entity e, here, $e \in E$
$DID_{e_1}^{e_2}$	DID of e_1 to be used with e_2, here, e_1, $e_2 \in E$
$DID_{e_2}^{e_1}$	DID of e_2 to be used with e_1, here, e_1, $e_2 \in E$
D_e	Data generated by an entity e, here, $e \in E$
$\mathscr{S}_e$	Digital signature by an entity e, here, $e \in E$
$VC - REC_{e_1}^{e_2}$	A VC-based verifiable credential issued by e_1 to e_2, here, e_1, $e_2 \in E$
$VC_{e_1}^{e_2}$	A verifiable credential issued by e_1 to e_2, here, e_1, $e_2 \in E$
$\{\}_K$	Encryption operation using a public key K
$\{\}_{K^{-1}}$	Signature using a private key K^{-1}
$H(M)$	SHA-512 hashing operation of message M
$[\ldots]_K$	Communication over an channel encrypted with key K
$[\ldots]$	Communication over an unencrypted channel

5.1. Registration

We start with the registration protocol. Every entity within the proposed VC-REC ecosystem needs be authenticated to participate in all other use-cases. The registration process completes the steps so that all entities can engage in other use-cases. The steps for the registration are illustrated in Fig. 6 and the protocol flows are presented in Table 2. We discuss the steps in the following:

M1: An entity (e, $e \in E$) interacts with their respective wallet (W_e) to generate the corresponding key pairs as presented in Table 2 (Step 1 in Fig. 6). The wallet W_e generates the key pair (K_e, K_e^{-1}) and an identifier (ID_e) for the entity (Step 2).
M2: The wallet returns the identifier and the public key to e (Step 3).
M3: The entity then interacts with the smart-contract platform (SCP) for the registration process by supplying the identifier, the corresponding public key and a digital signature over the respective data (Step 4). SCP creates another key pair for e $(K_{e'}, K_{e'}^{-1})$, to be used within the smart-contract platform. Then, the received public key, identifiers and the newly generated public key are stored in a registry in the blockchain (Step 5).
M4: SCP returns the new key pair with a registration successful message to e along with a digital signature of SCP covering the respective data (Step 6).

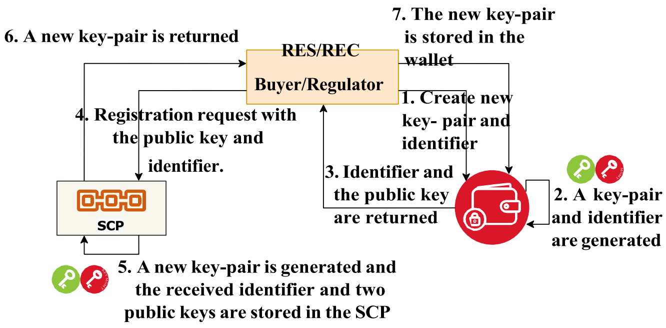
7. The new key-pair is stored in the wallet
6. A new key-pair is returned
RES/REC
Buyer/Regulator
1. Create new key- pair and identifier
4. Registration request with the public key and identifier.
3. Identifier and the public key are returned
2. A key-pair and identifier are generated
SCP
5. A new key-pair is generated and the received identifier and two public keys are stored in the SCP

Fig. 6. Registration of entities.

Table 2
Registration protocol.

$M1$	$e \rightarrow W_e$:	[Create New Key Pair and Identifier]
$M2$	$W_e \rightarrow e$:	$[ID_e, K_e]$
$M3$	$e \rightarrow SCP$:	$[\text{REG. REQ.}, ID_e, K_e, \mathscr{S}_e]_{HTTPS}$
$M4$	$SCP \rightarrow e$:	$[\text{REG. SUCCESS}, K_{e'}, K_{e'}^{-1}, \mathscr{S}_{SCP}]_{HTTPS}$
$M5$	$e \rightarrow W_e$:	$[K_{e'}, K_{e'}^{-1}]$

M5: e stores this new key pair in W_e (Step 7).

5.2. VC-REC issuance

In this use-case, we will elaborate how a VC-REC can be issued. The steps for this use-case are illustrated in Fig. 7 and the core protocol flows are presented in Table 3 where $res \in RES$ and SCP represents the smart-contract platform. At the first steps, both res and SCP interact with each other to establish an SSI connection (Steps 1a and 1b in Fig. 7). After establishing the SSI connection, the protocol flows for this use-case are discussed next.

M1: res generates electricity and D_{res} denotes the data representing the generated electricity. res transfers D_{res} via the established SSI connection (Steps 2 and 3 in Fig. 7) along with the corresponding digital signature. This is then transferred in a channel encrypted with the public key of SCP to be used with res.
M2: SCP creates a VC-REC ($VC - REC_{SCP}^{res}$) and its ownership record is recorded in the blockchain (Steps 4 and 5). Finally, $VC - REC_{SCP}^{res}$ returned back to the res in the previously established SSI connection, in a channel encrypted with the respective public key of res (Step 6).
M3: Upon receiving $VC - REC_{SCP}^{res}$, res stores it in the wallet (Step 7).

5.3. VC-REC buying/selling

Next, we explore the buying/selling use-case involving a VC-REC. In this use-case, the involved entities are one of the entities from the RES set, $res \in RES$ and one of the entities from the REC Buyer set (RB), $rb \in RB$. res would like to sell a VC-REC which can be represented with *REC1*. The steps for this use-case are illustrated in Fig. 8 and the core protocol flows are presented in Table 4.

As the first step, both res and rb interact with each other to establish an SSI connection (Step 1 in Fig. 8). Next, we discuss the other steps involved in this use-case.

M1: With the intention to sell *REC1*, res uploads the metadata of *REC1* to SCP along with a digital signature (Step 2 in Fig. 8).
M2: rb retrieves such metadata and decides to buy *REC1* (Step 3).
M3: *REC1* is transferred to rb via the established SSI channel, encrypted with the public key of rb to be used with res. This is represented as Step 4 in Fig. 8.
M4: rb verifies *REC1* and upon a successful verification, *REC1* is stored in the wallet of rb (Steps 5 and 6).
M5: res updates in the blockchain that *REC1* has been sold (Step 7). This is accompanied by the respective digital signature.
M6: rb updates in the blockchain that *REC1* has been bought (Step 8). This is accompanied by the respective digital signature.

5.4. VC-REC swapping

Next, the use-case where two entities (e.g. REC owners, denoted with $rb1$ and $rb2$ respectively) would like to swap their corresponding VC-RECs is explored. Here, $rb1$ owns a VC-REC, denoted with *REC1* and $rb2$ own another VC-REC denoted with *REC2*. Now, they would like to swap these VC-RECs. The steps involved in this use-case are illustrated in Fig. 9 and the core protocol flow are presented in Table 5. Like before, at first, $rb1$ and $rb2$ interact with each other to establish an SSI connection

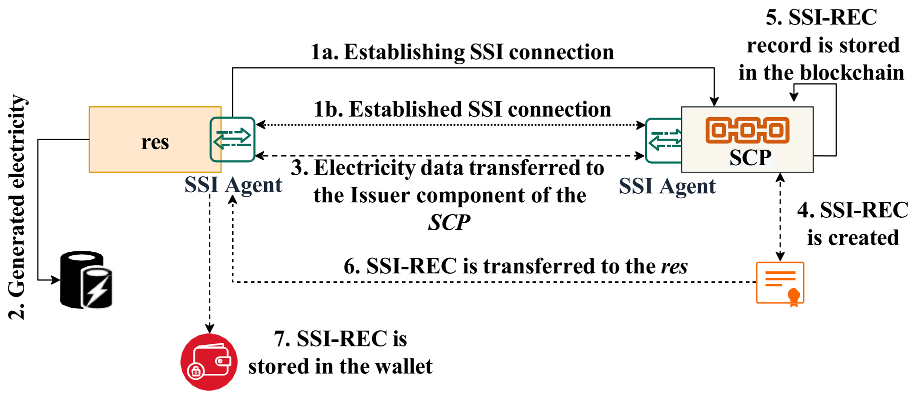
5. SSI-REC record is stored in the blockchain
1a. Establishing SSI connection
1b. Established SSI connection
2. Generated electricity
res
SSI Agent
3. Electricity data transferred to the Issuer component of the SCP
SCP
SSI Agent
4. SSI-REC is created
6. SSI-REC is transferred to the res
7. SSI-REC is stored in the wallet

Fig. 7. Issuance of VC-REC.

Table 3
VC-REC issuance protocol.

$M1$	$res \rightarrow SCP$:	$[D_{res}, \mathscr{S}_{res}]_{K^{res}_{SCP}}$
$M2$	$SCP \rightarrow res$:	$[VC - REC^{res}_{SCP}]_{K^{SCP}_{res}}$
$M3$	$res \rightarrow W_{res}$:	$[VC - REC^{res}_{SCP}]$

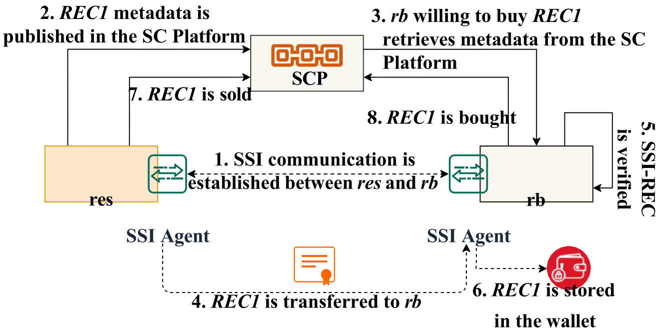
2. REC1 metadata is published in the SC Platform
3. rb willing to buy REC1 retrieves metadata from the SC Platform
SCP
7. REC1 is sold
8. REC1 is bought
5. SSI-REC is verified
1. SSI communication is established between res and rb
res
rb
SSI Agent
SSI Agent
4. REC1 is transferred to rb
6. REC1 is stored in the wallet

Fig. 8. Selling/buying of VC-REC.

Table 4
Buy/sell protocol.

$M1$	$res \rightarrow SCP$:	$[\text{Metadata of } REC1, \mathscr{S}_{res}]_{HTTPS}$
$M2$	$SCP \rightarrow rb$:	$[\text{Metadata of } REC1]_{HTTPS}$
$M3$	$RES \rightarrow rb$:	$[REC1]_{K^{res}_{rb}}$
$M4$	$rb \rightarrow W_{rb}$:	$[REC1]$
$M5$	$res \rightarrow SCP$:	$[REC1 \text{ is sold}, \mathscr{S}_{res}]_{HTTPS}$
$M6$	$rb \rightarrow SCP$:	$[REC1 \text{ is bought}, \mathscr{S}_{rb}]_{HTTPS}$

(Step 1 in Fig. 9). The subsequent steps in this use-case are presented next:

M1: *rb1* uploads the metadata of *REC1* to the *SCP* with the intention to swap (Step 2 in Fig. 9). This is accompanied with the respective digital signature.
M2: Similarly, *rb2* uploads the metadata of *REC2* to the *SCP* with the intention to swap (Step 3). This is also accompanied with the respective digital signature.
M3: *rb1* retrieves information regarding *REC2* from the *SCP* (Step 4).
M4: Similarly, *rb2* retrieves information regarding *REC1* from the *SCP* (Step 5).
M5: *REC1* is transferred to *rb2* via the established SSI channel, encrypted with the public key of *rb2* to be used with *rb1* (Step 6).
M6: *rb2* verifies *REC1* and upon a successful verification, *REC1* is stored in the wallet of *rb2* (Steps 7 and 8).
M7: *rb1* updates the ownership information of *REC1* in the *SCP* (Step 9). This step is accompanied by the respective digital signature.
M8: *REC2* is transferred to *rb1* via the established SSI channel, encrypted with the public key of *rb1* to be used with *rb2* (Step 10).
M9: *rb1* verifies *REC2* and upon a successful verification, *REC2* is stored in the wallet of *rb1* (Steps 11 and 12).
M10: *rb2* updates the ownership information of *REC2* in the *SCP* (Step 13). This step is also accompanied by the respective digital signature.

5.5. VC-REC retiring

In the final use-case we explore the steps involved for retiring a VC-REC (denoted with *REC*). This process is quite simple in comparison to the steps involved in other use-cases. The steps are illustrated in Fig. 10 and its protocol flow is presented in Table 6.

M1: The corresponding VC-REC (*REC*) is retrieved from the wallet of *rb* (Step 1 in Fig. 10).
M2: *REC* is consumed by *rb* and hence, *REC* is retired in the *SCP* by uploading the corresponding metadata which is accompanied with the respective digital signature (Steps 2 and 3).

6. Discussion

In this section we present a discussion of how the proposed architecture and the envisioned use-cases satisfy the formulated requirements (Section 6.1), the advantages of our proposal (Section 6.2) and the possible future work (Section 6.3).

6.1. Analyzing requirements

Functional Requirements: As evident from the architecture (Fig. 5), the proposed architecture utilizes a smart-contract supporting blockchain platform in order to issue VC-RECs as well as to maintain a register of identifiers and public keys of involved entities, thereby satisfying requirement *F1*. The architecture utilizes an SSI framework so that a REC is represented with a VC and hence, it satisfies requirement *F2*. In order to accommodate the SSI framework, the roles of the existing SSI ecosystem has been modified so that they can assume the responsibilities of different SSI entities. This satisfies requirement *F3*. Finally, as the use-case illustrates, the previous REC ecosystem has been redesigned in order to ensure that existing functionalities of REC can be realized within this envisioned setting, satisfying requirement *F4*.

Security Requirements: As per the proposed architecture, only registered entities can participate in the system. The proposed system needs to employ a mechanism which can determine which entity can generate VCs (VC-RECs) and other entities can verify if the entity is authorized to generate VC during the VC-REC verification process. In

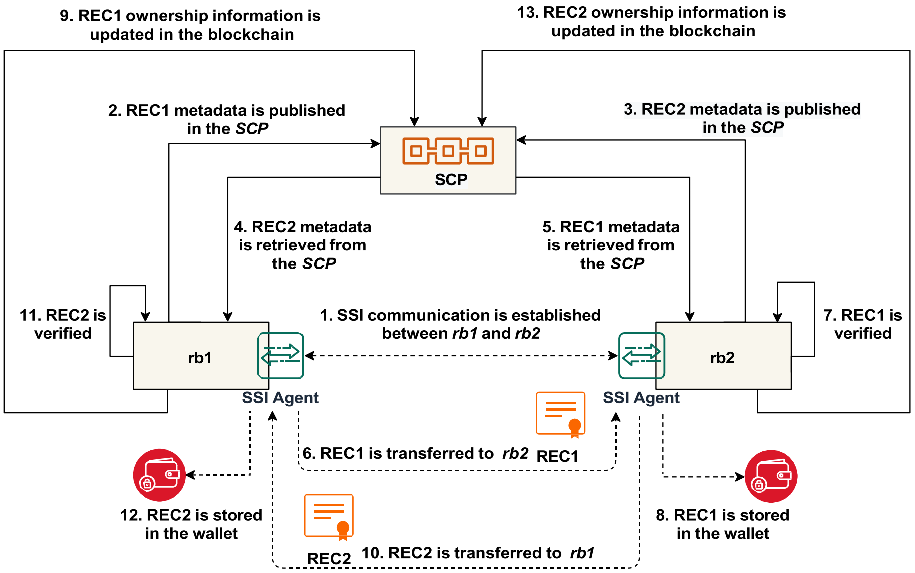
9. REC1 ownership information is updated in the blockchain
13. REC2 ownership information is updated in the blockchain
2. REC1 metadata is published in the SCP
3. REC2 metadata is published in the SCP
SCP
4. REC2 metadata is retrieved from the SCP
5. REC1 metadata is retrieved from the SCP
11. REC2 is verified
1. SSI communication is established between rb1 and rb2
7. REC1 is verified
rb1
rb2
SSI Agent
SSI Agent
6. REC1 is transferred to rb2
REC1
12. REC2 is stored in the wallet
8. REC1 is stored in the wallet
REC2
10. REC2 is transferred to rb1

Fig. 9. VC-REC swapping.

Table 5
VC-REC swapping protocol.

$M1$	$rb1 \rightarrow SCP$:	$[\text{Metadata of } REC1, \mathscr{S}_{rb1}]_{HTTPS}$
$M2$	$rb2 \rightarrow SCP$:	$[\text{Metadata of } REC2, \mathscr{S}_{rb2}]_{HTTPS}$
$M3$	$SCP \rightarrow rb1$:	$[\text{Metadata of } REC2]_{HTTPS}$
$M4$	$rb2 \rightarrow SCP$:	$[\text{Metadata of } REC1]_{HTTPS}$
$M5$	$rb1 \rightarrow rb2$:	$[REC1]_{K_{rb2}^{rb1}}$
$M6$	$rb2 \rightarrow W_{rb2}$:	$[REC1]$
$M7$	$rb1 \rightarrow SCP$:	$[\text{Updated ownership information of } REC1, \mathscr{S}_{rb1}]_{HTTPS}$
$M8$	$rb2 \rightarrow rb1$:	$[REC2]_{K_{rb1}^{rb2}}$
$M9$	$rb1 \rightarrow W_{rb1}$:	$[REC2]$
$M10$	$rb2 \rightarrow SCP$:	$[\text{Updated ownership information of } REC2, \mathscr{S}_{rb2}]_{HTTPS}$

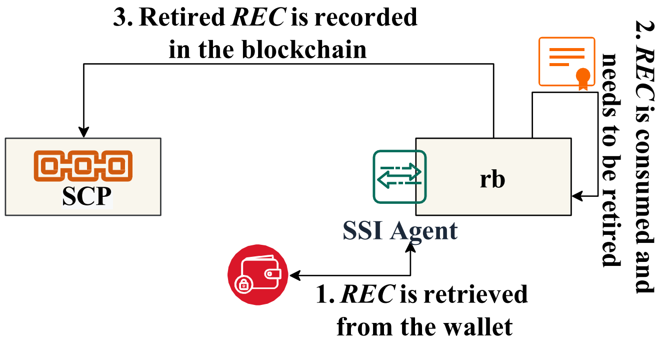
3. Retired REC is recorded in the blockchain
SCP
rb
SSI Agent
2. REC is consumed and needs to be retired
1. REC is retrieved from the wallet

Fig. 10. Retiring of VC-REC.

Table 6
Retiring protocol.

$M1$	$W_{rb} \rightarrow rb$:	$[REC]$
$M2$	$rb \rightarrow SCP$:	$[REC \text{ is consumed}, \mathscr{S}_{rb}]_{HTTPS}$

this way, the *S1* requirement can be satisfied. In order to combinedly satisfy *S2* and *S3* requirements, digital signatures have been extensively used in all required steps. The exception has been made in only those steps where VC-RECs have been transferred. Since a VC-REC is already digitally signed, no further digital signature has been used in the protocol. The protocol also ensures that either HTTPS or an encrypted SSI channel has been used in all steps of the protocol, thereby satisfying the *S4* requirement. Satisfying *S5* and *S6* requirements would require to employ appropriate measures during the implementation phase. Every step in the protocol flows for each use-case could utilize nonces to satisfy requirement *S7*.

6.2. Advantages

The proposed approach is the first to introduce this seminal idea of integrating the SSI framework within the REC ecosystem. The main motivation is to address the issues identified and presented in Section 3.1 and the architecture effectively addresses all these issues. For example, the VC format to represent a REC could be utilized to create a common standard for REC. However, all must agree to a common schema for the VC-REC in order to reduce the inter-operability issues.

The proposed approach presents a standardized way to verify an VC-REC. In addition, the proposed verification process does not rely on a trusted party, rather it utilizes the combination of a blockchain registry and SSI functionalities to achieve this goal. The communication between the involved entities are secure (the encrypted SSI channel) and based on standardized SSI protocols. Furthermore, the proposed architecture requires that every entity must be identified and authenticated in order to participate in different use-cases without relying on a provider-centric IMS, thus removing all the disadvantages on such IMS.

Finally, the reliance on the SCP for each use-case in the proposed approach implies that there is no entity assuming the role of a broker. Also, the status of each REC is immutably recorded in the SCP, thereby removing the possibility of any double counting issue within the REC ecosystem.

In short, we can state that the proposed approach addresses all the identified issues effectively and offers much more flexibility than the current state-of-the-art.

6.3. Future work

The major future work is to develop the proposed system. Once the system is fully developed, we would like to deploy it in real-life settings and evaluate its performance. The performance result would be an important indicator of the applicability of the system.

Also, once the system is fully deployed, we can envision many other interesting use-cases, e.g. autonomous execution of REC trading based on some pre-defined business logic set by the respective REC seller and integrating an AI/ML model to predict the price of a REC.

Since the proposed system introduces a novel way of interacting within the REC ecosystem, it would be crucial to test the usability of the system with all the stakeholders. It will help us to identify if there are any usability issues that might impact the adoption of the proposed system. Once the usability issues are identified, we can then take proper measures to reduce or eradicate any such usability issues.

7. Related work

In this section, in addition to the research work of Cali et al. (2022b) as presented in Section 3.2, we review a few additional related works. An SSI-based REC system as proposed in this article is a novel idea, as such there are no research works within the intersection of SSI, REC and DLT. Instead, we have reviewed a few existing research works which explored the utilization of DLT within the REC ecosystem.

The idea of utilizing a smart-contract supporting blockchain platform such as Ethereum for REC (denoted as *Renewable Energy Credit*) issuance and distribution was first presented by Leonhard et al. in (Leonhard, 2016). The authors proposed the idea of representing RECs as cryptocurrencies in Ethereum and explored different aspects of it. However, the proposal was presented just as an idea without much details.

Kim et al. presented a blockchain based REC trading system (Kim et al., 2020). In this work, the main motivation was to introduce a seal-bid auction mechanism which could be carried out via the blockchain system. As per their proposal, the RES would act as the seller (denoted as the *Auctioneer*) and they would sell RECs and there would be buyers who would be willing to buy those RECs. However, the buyers would participate in a seal-bid auction mechanism and would compete with other buyers to buy the corresponding REC. The bidding process and the respective result would be recorded in the blockchain.

In (Zuo, 2022), the idea of tokenizing RECs is presented. As per the proposal, each REC would be represented as a tokenized asset within a blockchain system. The REC trading would simply mean buy/selling of the respective token which can be easily carried out via the blockchain system. Since this trading would be implicitly recorded in the blockchain system, this mechanism would ensure the transparency and traceability of RECs. The proposal was simulated using a private blockchain platform (Multichain).

Gao et al. presented *HRECTS-CBC* which is a consortium blockchain based REC trading system (Gao et al., 2021). They envisioned that the blockchain network would be made of different entities from the REC ecosystem. Here, the buyer and the seller would participate in the Continuous Double Auction method in order to trade the RECs. The authors also included a REC price forecasting model in their system.

In (Wang et al., 2021), Wang et al. presented *HRECTS-PBC*, another consortium blockchain based REC trading system. Suripringly, both *HRECTS-PBC* and *HRECTS-CBC* (Gao et al., 2021) are quite similar in their functionalities as they both used a consortium blockchain platform and the continuous double auction method for trading RECs, even the architectures presented in these two works looked similar. However, *HRECTS-CBC* included a price forecasting model whereas *HRECTS-PBC* did not have any such model.

Spinnell et al. presented a theoretical analysis of blockchain based REC trading (Spinnell and Zimberg, 2018). They analysed different advantages this approach could bring with a focus on PJM environmental information services. However, they did not elaborate much on the technical details of their proposal.

In (Hsiao, 2018), a blockchain based REC verification mechanism was proposed with a specific focus to mitigating the fraudulent verification of RECs. The proposal lacked technical details of many aspects.

Lastly, Marques et al. (2023) proposed a model for REC trading using blockchain where a REC would be represented as a token. Their main focus was on the analysis of how such a tokenized REC could be used as an investment instrument and as such this work also lacked many technical details.

Comparative Analysis. A comparative analysis of the current work with the existing research works against a number of criteria is presented in Table 7 where the "●" symbol denotes if the respective work has satisfied a criterion and the "○" symbol denotes the specific criterion has not been satisfied. The selected criteria are SSI, VC, IMS (Identity Management System), Threat Model, Standardized REC, DLT & Smart-contract, Authenticated interaction, Encrypted communication and Broker reliance. These criteria represent the issues identified in Section 3.3.

We want all criteria to be fulfilled (i.e. having a "●" symbol) except the *Broker reliance* criterion for which it is desired that such a broker is not needed (i.e. having a "○" symbol). As evident from Table 7, the current work satisfies all the identified criteria without relying on a third party and hence, exceeds the current state-of-the-art.

8. Conclusion

The incorporation of SSI and DLT into the Renewable Energy Certificate (REC) ecosystem is a key step toward digital decarbonization. The capacity to sell the environmental features of renewable energy as REC units is essential to the digital revolution of the energy industry. However, obstacles such as a lack of shared standards and dependence on centralized institutions prevent DLT and REC from reaching their full potential.

In this article, we have proposed a holistic architecture which integrates SSI and DLT for the representation, trading and verification of REC in a decentralized way. This paves the way to create a common standard for the representation and verification of RECs using the notion of Verifiable Credentials (VCs). The proposed approach is fully decentralized in nature and offers better security and privacy in almost every aspect of REC trading. We strongly believe that this seminal approach will provide the required foundation to introduce a new wave of research within this domain.

Furthermore, the combined use of DLT and SSI for the REC Trading use-case has potential to make a significant impact towards the United Nations Sustainable Development Goals (UNSDGs). By creating a decentralized and privacy-friendly solution for the representation, trading, and verification of REC, the proposed architecture supports the transition towards a more sustainable energy future, contributing to UNSDG 7 (Affordable and Clean Energy) and UNSDG 13 (Climate Action). Moreover, the use of Verifiable Credentials (VCs) as a common standard for REC representation and verification enhances transparency and accountability in the energy sector, aligning with UNSDG 9 (Industry, Innovation, and Infrastructure) and UNSDG 16 (Peace, Justice and Strong Institutions).

CRediT authorship contribution statement

Md Sadek Ferdous: Conceptualization, original draft preparation, Writing – original draft, Methodology, Writing – review & editing. **Umit Cali:** Conceptualization, Methodology, Supervision, Writing – review & editing. **Ugur Halden:** Writing – review & editing, Validation. **Wolfgang Prinz:** Reviewing, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Table 7
Comparative analysis.

Criteria	RTTS (Cali et al., 2022b)	Kim et al. (Kim et al., 2020)	Zuo et al. (Zuo, 2022)	HRECTS-CBC (Gao et al., 2021)	HRECTS-PBC (Wang et al., 2021)	Spinnell et al. (Spinnell and Zimberg, 2018)	Hsiao et al. (Hsiao, 2018)	Marques et al., (Marques et al., 2023)	Current work
SSI	○	○	○	○	○	○	○	○	●
VC	○	○	○	○	○	○	○	○	●
IMS	○	○	Centralized	○	○	○	○	○	Decentralized
Threat Model	○	○	○	○	○	○	○	○	●
Standardized REC	○	○	○	○	○	○	○	○	●
DLT & Smart-contract	●	●	●	●	●	●	●	●	●
Authenticated interaction	○	○	●	○	○	○	○	○	●
Encrypted communication	○	○	○	○	○	○	○	○	●
Broker reliance	●	○	○	○	○	○	○	○	○

Appendix A. Nomenclature

Nomenclatures used in this article are presented in Table A.8.

Table A.8
Nomenclatures used in the manuscript

Nomenclature	Description
AI	Artificial Intelligence
DID	Decentralized Identifier
DIDDoc	DID Document
DLT	Distributed Ledger Technology
GO	Guarantees of Origin
IMS	Identity Management System
IoT	Internet of Things
JSON	JavaScript Object Notation
ML	Machine Learning
LCOE	Levelized Cost of Energy
OAuth	Open Authorization
P2P	Peer-to-Peer
REC	Renewable Energy Certificate
REGO	Renewable Energy Guarantees of Origin
RTTS	REC Transaction and Trading System
PV	Photovoltaic
SAML	Security Assertion Markup Language
SSI	Self-sovereign Identity
W3C	World Wide Web Consortium
VC	Verifiable Credential
VP	Verifiable Presentation

References

Allayannis, G.Y., Tenguria, S.K., 2011. Carbon Credit Markets.

Allen, C.. The path to self-sovereign identity - life with alacrity. URL. http://www.lifewithalacrity.com/previous/2016/04/the-path-to-self-sovereign-identity.html. (Accessed 27 April 2022).

Alom, I., Eshita, R.M., Harun, A.I., Ferdous, M.S., Shuhan, M.K.B., Chowdhury, M.J.M., Rahman, M.S., 2021. Dynamic management of identity federations using blockchain. In: 3rd IEEE International Conference on Blockchain and Cryptocurrency. ICBC).

Ashley, M.J., Johnson, M.S., 2018. Establishing a secure, transparent, and autonomous blockchain of custody for renewable energy credits and carbon credits. IEEE Eng. Manag. Rev. 46 (4), 100–102.

Bogensperger, A., Zeiselmair, A., 2020. Updating renewable energy certificate markets via integration of smart meter data, improved time resolution and spatial optimization. In: 2020 17th International Conference on the European Energy Market (EEM). IEEE, pp. 1–5.

C. news. The concordium blockchain contributes to Danish transmission energinet's new green energy certificate platform - concordium. https://news.cision.com/concordium/r/the-concordium-blockchain-contributes-to-danish-transmission-energinet-s-new-green-energy-certificat,c3715427. (Accessed 3 March 2023). February 2023.

Cali, U., Deveci, M., Saha, S.S., Halden, U., Smarandache, F., 2022a. Prioritizing energy blockchain use cases using type-2 neutrosophic number-based EDAS. IEEE Access 10, 34260–34276. https://doi.org/10.1109/access.2022.3162190.

Cali, U., Kuzlu, M., Sebastian-Cardenas, D.J., Elma, O., Pipattanasomporn, M., Reddi, R., 2022b. Cybersecure and scalable, token-based renewable energy certificate framework using blockchain-enabled trading platform. Electr. Eng. 1–12.

Chowdhury, M.J.M., Ferdous, M.S., Biswas, K., Chowdhury, N., Kayes, A., Alazab, M., Watters, P., 2019. A comparative analysis of distributed ledger technology platforms. IEEE Access 7 (1), 167930–167943.

Decentralized identifiers (DIDs) v1.0. URL. https://www.w3.org/TR/did-core/. (Accessed 27 April 2022).

Feldman, D., Ramasamy, V., Fu, R., Ramdas, A., Desai, J., Margolis, R., 2021. Us solar photovoltaic system and energy storage cost benchmark (Q1 2020). In: Tech. Rep. National Renewable Energy Lab.(NREL), Golden, CO (United States).

Ferdous, M.S., 2015. User-controlled Identity Management Systems Using Mobile Devices.

Ferdous, M.S., Poet, R., 2012. A comparative analysis of identity management systems. In: High Performance Computing and Simulation (HPCS), 2012 International Conference on. IEEE, pp. 454–461.

Ferdous, M.S., Chowdhury, F., Alassafi, M.O., 2019. In search of self-sovereign identity leveraging blockchain technology. IEEE Access 7, 103059–103079.

Ferdous, M.S., Ionita, A., Prinz, W., 2023. Ssi4web: a self-sovereign identity (ssi) framework for the web. In: Blockchain and Applications, 4th International Congress. Springer, pp. 366–379.

Gao, M., Yu, X., Ren, L., Cai, H., Wang, Z., Zhou, Y., 2021. A renewable energy certificate trading system based on blockchain. In: 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, pp. 1514–1518.

Halden, U., Cali, U., Dynge, M.F., Stekli, J., Bai, L., 2021. DLT-based equity crowdfunding on the techno-economic feasibility of solar energy investments. Sol. Energy 227 (August), 137–150. https://doi.org/10.1016/j.solener.2021.08.067.

Hardt, D., et al., 2012. The Oauth 2.0 Authorization Framework.

Holt, E., Sumner, J., Bird, L., 2011. Role of Renewable Energy Certificates in Developing New Renewable Energy Projects, vol. 6. https://doi.org/10.2172/1018490. URL. https://www.osti.gov/biblio/1018490.

Hsiao, J.I.-H., 2018. Blockchain for corporate renewable energy procurement-potential for verification of renewable energy certificates. US-China L. Rev. 15, 75.

Hughes, J., Maler, E., 2005. Security Assertion Markup Language (Saml) V2. 0 Technical Overview, OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08 13.

Kim, J., Park, H., Lee, G.H., Choi, J.K., Heo, Y., 2020. Seal-bid renewable energy certification trading in power system using blockchain technology. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, pp. 1752–1756.

Lai, C.S., Lai, L.L., Lai, Q.H., 2021. Blockchain applications in microgrid clusters. In: Smart Grids and Big Data Analytics for Smart Cities. Springer, pp. 265–305.

Leonhard, R., 2016. Developing Renewable Energy Credits as Cryptocurrency on Ethereum's Blockchain. Available at SSRN 2885335.

Marques, N.L., Gomes, L.L., Brandão, L.E., 2023. A blockchain-based model for token renewable energy certificate offers. Rev. Contab. Finanças 34.

Münsing, E., Mather, J., Moura, S., 2017. Blockchains for decentralized optimization of energy resources in microgrid networks. In: 2017 IEEE Conference on Control Technology and Applications (CCTA), pp. 2164–2171. https://doi.org/10.1109/CCTA.2017.8062773.

Myagmar, S., Lee, A.J., Yurcik, W., 2005. Threat modeling as a basis for security requirements. In: Symposium on Requirements Engineering for Information Security (SREIS), vol. 2005. Citeseer, pp. 1–8.

Nakamoto, S., 2019. Bitcoin: A Peer-To-Peer Electronic Cash System. Tech. rep., Manubot.

Pan, Y., Dong, F., 2023. Green finance policy coupling effect of fossil energy use rights trading and renewable energy certificates trading on low carbon economy: taking China as an example. Econ. Anal. Pol. 77, 658–679.

Recordon, D., Reed, D., 2006. Openid 2.0: a platform for user-centric identity management. In: Proceedings of the Second ACM Workshop on Digital Identity Management, pp. 11–16.

Renewable energy certificates (recs). URL. https://www.epa.gov/green-power-markets/renewable-energy-certificates-recs. (Accessed 27 June 2022).

Renewable energy guarantees of origin (rego). URL. https://www.ofgem.gov.uk/environmental-and-social-schemes/renewable-energy-guarantees-origin-rego. (Accessed 27 June 2022).

Shostack, A., 2014. Threat Modeling: Designing for Security. John Wiley & Sons.

Siano, P., De Marco, G., Rolan, A., Loia, V., 2019. A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. IEEE Syst. J. 13 (3), 3454–3466. https://doi.org/10.1109/JSYST.2019.2903172.

Spinnell, J.J., Zimberg, D.L., 2018. Renewable Energy Certificate Markets: Blockchain Applied. Energy System Engineering Institute, Lehigh University.

T. H. foundation. How wallmart brought unprecedented transparency to the food supply chain with hyperledger fabric. https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf. (Accessed 3 March 2023).

United States Environmental Protection Agency, 2021. Renewable energy certificate monetization. URL. https://www.epa.gov/repowertoolbox/renewable-energy-certificate-monetization.

Verifiable credentials data model 1.0. URL. https://www.w3.org/TR/vc-data-model/. (Accessed 27 April 2022).

Wang, D., Xuan, J., Chen, Z., Li, D., Shi, R., 2021. Renewable Energy Certificate Trading via Permissioned Blockchain, Security and Communication Networks 2021.

Zafoschnig, L.A., Nold, S., Goldschmidt, J.C., 2020. The race for lowest costs of electricity production: techno-economic analysis of silicon, perovskite and tandem solar cells. IEEE J. Photovoltaics 10 (6), 1632–1641.

Zhang, S., Rong, J., Wang, B., 2020. A privacy protection scheme of smart meter for decentralized smart home environment based on consortium blockchain. Int. J. Electr. Power Energy Syst. 121, 106140 https://doi.org/10.1016/j.ijepes.2020.106140.

Zhao, F., Guo, X., Chan, W.K.V., 2020. Individual green certificates on blockchain: a simulation approach. Sustainability 12 (9). https://doi.org/10.3390/su12093942. URL. https://www.mdpi.com/2071-1050/12/9/3942.

Zuo, Y., 2022. Tokenizing renewable energy certificates (recs)—a blockchain approach for rec issuance and trading. IEEE Access 10, 134477–134490.

"Bitcoin". URL. https://www.bitcoin.org/. (Accessed 10 July 2022).

"Ethereum". URL. https://www.ethereum.org/. (Accessed 10 July 2022).

"Hyperledger fabric". URL. https://www.hyperledger.org/use/fabric. (Accessed 30 April 2022).

"Hyperledger Indy". URL. https://www.hyperledger.org/use/hyperledger-indy. (Accessed 30 April 2022).

"Hyperledger". URL. https://www.hyperledger.org/. (Accessed 10 July 2022).

"Litecoin". URL. https://litecoin.org/. (Accessed 10 July 2022).

"Monero". URL. https://www.getmonero.org/. (Accessed 10 July 2022).

"Quorum blockchain". URL. https://www.goquorum.com/. (Accessed 10 July 2022).