With or Without Blockchain? Towards a Decentralized, SSI-based eRoaming Architecture

Alexandra Hoess
SnT - Interdisciplinary Center for Security, Reliability and Trust
University of Luxembourg
alexandra.hoess@uni.lu

Tamara Roth
SnT - Interdisciplinary Center for Security, Reliability and Trust
University of Luxembourg
tamara.roth@uni.lu

Johannes Sedlmeir
Project Group Business & Information Systems Engineering
of the Fraunhofer FIT
Bayreuth, Germany
johannes.sedlmeir@fit.fraunhofer.de

Gilbert Fridgen
SnT - Interdisciplinary Center for Security, Reliability and Trust
University of Luxembourg
gilbert.fridgen@uni.lu

Alexander Rieger
SnT - Interdisciplinary Center for Security, Reliability and Trust
University of Luxembourg
alexander.rieger@uni.lu

Abstract

Fragmentation and limited accessibility of charging infrastructure impede the adoption of electric vehicles. To improve the availability of charging infrastructure independent of providers, eRoaming offers a promising solution. Yet, current eRoaming systems are typically centralized, which raises concerns of market power concentration. While the use of blockchain technology can obviate such concerns, it comes with significant privacy challenges. To address these challenges, we explore a combination of blockchain with self-sovereign identity. Specifically, we apply a design science research approach, which helps us to identify requirements, derive a conceptual architecture, and deduce design principles for decentralized eRoaming and beyond. We find that blockchain may best leverage its benefits when it takes a backseat as a public registry for legal entities. Moreover, we find that the use of self-sovereign identities could improve compliance with privacy regulations, but they should not be overused.

1. Introduction

Electric vehicles (EVs) are indispensable for more sustainable transportation [1]. Yet, the adoption of EVs still falls short of expectations [2]. One reason for this slow adoption is the limited availability and accessibility of charging points [3]. Unlike current fueling processes with regular petrol or diesel cars, EV users cannot simply plug and charge their vehicles at any charging point. Instead, charging points often require provider-specific contracts as well as provider-specific apps or RFID cards [4]. Consequently, EV users typically need to sign multiple contracts and use several apps or RFID cards to ensure access to a sufficient number of charging points. The resulting inconvenience may ultimately lead to a slower adoption of EVs [5, 6].

As a result, charging point providers have introduced the concept of eRoaming, which grants users access to charging points operated by various providers with a single contract [4, 7]. Yet, eRoaming requires technical interoperability, sophisticated identity management, and simple clearing processes between providers [4]. Current eRoaming systems typically address these requirements with centralized platform designs. That is, multiple providers connect to one platform to share their charging points [7–9]. Such eRoaming platforms are typically operated by an electric mobility clearing house (EMCH). However, centralized approaches are often ill-received, as they pose privacy risks due to centralized storage of data and might lead to concentration of market power in favor of EMCHs [7, 8].

Consequently, various concepts for decentralized eRoaming solutions have emerged [8, 10, 11]. These concepts typically propose to use blockchain for decentralized identity management [11, 12], and automated token-based clearing and settlement [8, 11, 13, 14]. Yet, the exchange of user data with blockchain often raises substantial privacy concerns [15, 16]. To mitigate privacy concerns of both centralized and blockchain-based eRoaming solutions, an identity management that stores personal information only with the identity subject – the user – is required [11]. In this context, the emerging construct of self-sovereign identity (SSI) receives increasing attention. SSI implementations often use blockchain as a decentralized public key infrastructure (PKI) [17], which may function as a foundation for identity management in blockchain-based eRoaming solutions [11]. However, when approaching blockchain-based SSI, a sensible use of blockchain is required to prevent privacy issues that result from storing identity information on-chain [16]. Hence, we ask:

RQ: *How can a decentralized eRoaming system be designed with blockchain and SSI?*

We explore this research question using a Design Science Research (DSR) approach [18]. The use of DSR helps us to identify requirements for decentralized eRoaming and to design a decentralized eRoaming system with blockchain and SSI. We started with a structured literature review (SLR) [19] to derive design objectives and requirements for decentralized eRoaming. Further investigation of current eRoaming systems helped us to develop a conceptual architecture for decentralized eRoaming. We qualitatively evaluated this architecture in 13 expert interviews [20]. Based on our emerging architecture, we deduced four generalizable design principles [21]. These design principles provide guidance for practitioners who implement decentralized eRoaming and may serve as a starting point for researchers to develop a design theory for eRoaming and similar service systems.

2. Theoretical Background

2.1. eRoaming

The current charging infrastructure for EVs is highly fragmented [7, 22]. Unlike the refueling at established gas stations, EV charging requires the interplay of two main actors: the charge point operator (CPO) and the electric mobility service provider (eMSP). While CPOs maintain the charging points and manage the charging process, eMSPs offer charging services to users [7, 23, 24]. By subscribing to an eMSP, users can access all charging points within an eMSP's network. At the same time, they cannot access charging points outside of the eMSP's network. Consequently, users often enter into multiple contracts with eMSPs to gain access to a sufficient number of charging points [22]. However, the need for multiple contracts creates barriers to EV charging and is considered cumbersome [5].

To reduce such barriers and increase network access for users, CPOs and eMSPs typically establish business-to-business (B2B) eRoaming agreements that allow for the provision of services on behalf of each other [22]. In general, eRoaming requires four main process steps: registration, authentication, charging, and clearing [24]. Prior to the charging process, users must conclude a contract with an eMSP. For *registration*, eMSPs typically assign each user a unique identifier – the electric mobility account identifier (EMAID) [24]. At the charging point, the user *authenticates* as a subscribed user by transmitting its EMAID to the CPO using an eMSP-specific RFID card or a mobile app. This initiates the actual *charging* process. After completion of the charging process, the charging point or the CPO's backend system creates a charge detail record (CDR) that serves as the basis for *clearing*. Specifically, the CDR includes a unique charging session identifier, the charged amount of energy, the EMAID, and the resulting payment [23–25]. The CPO forwards the CDR together with a B2B bill to the eMSP, who bills the user and pays the charged amount to the CPO.

The four process steps of eRoaming require a reliable exchange of contract information to enable seamless authentication and clearing between CPO and eMSP, and eMSP and user [4, 24]. Currently, multiple eRoaming systems and protocols exist with either a centralized or decentralized design. Centralized designs that connect multiple providers to one platform are the predominant design [7, 24, 26]. These platforms typically make use of proprietary protocols, such as OCHP, OICP, or eMIP to facilitate authentication and clearing [9]. However, centralization comes with significant security, privacy, and scalability challenges, and concerns regarding market monopolization [7–9].

In response to these challenges, decentralized approaches which store data decentrally and grant equal market access to all actors have gained traction [8, 9, 11]. For business-centric approaches, i.e. B2B information exchange, OCPI provides an emerging standardized messaging protocol for eRoaming [9]. More user-centric approaches try to map information exchange with blockchain technology to e.g., facilitate the clearing of charging events [8, 11, 14] or enable decentralized identity management [11, 12]. While blockchain-based approaches appear to be popular in literature, they come with significant privacy concerns [14]. First approaches also already exist that suggest the use of blockchain-based SSI for eRoaming [11]. Yet, proposed solutions anchor digital identities on-chain, which may again cause privacy-related issues and contradict data protection regulations such as the EU's General Data Protection Regulation (GDPR) [27]. Such solutions also introduce blockchain for clearing but fail to provide details on the execution of payments on-chain, the required type of blockchain, or the general acceptance of blockchain-based payments [11]. They also do not provide a rigorous analysis of general requirements and the role of blockchain for decentralized eRoaming. We, therefore, aim to provide a more rigorous analysis by conducting DSR with an architecture that combines blockchain and SSI for decentralized eRoaming.

2.2. Blockchain Technology

A blockchain is a distributed transactional database redundantly stored on the nodes of a peer-to-peer (P2P) network [28,29]. Transactions are aggregated into larger formations (blocks) and are chronologically linked via cryptographic hashes, forming a tamper-resistant chain of records [29]. The nodes reach agreement about the state of the blockchain by following a consensus protocol [29]. As each node stores a copy of the blockchain, blockchains enable a shared state of information without requiring a central authority [30]. Dependent on the type of blockchain, the rights of participants may differ [28]. While public blockchains enable every user to read and validate transactions, private blockchains restrict access to certain participants. Permissioned blockchains additionally restrict participation in the consensus process. To manage transactions and access rights, blockchains employ a decentralized PKI with asymmetric encryption and digital signatures [15].

This built-in PKI of blockchain has encouraged the development of decentralized certificate-based identity solutions [17, 31]. These solutions have their roots in identity management approaches that combine a PKI with digital certificates to enable secure digital authentication and proofs of permissions [32, 33]. Decentralized, certificate-based identity management has been used to authenticate servers way before the development of blockchain [33]. Yet, their lack of a sophisticated revocation mechanism prevented broad adoption on an end-user level [33,34]. Blockchain may, in this case, serve as a technical enabler of decentralized certificate-based identity solutions such as SSI [17,31].

2.3. Self-Sovereign Identity

SSI anticipates a digital identity management that is similar to physical identity management with plastic cards stored in a wallet [35]. To this end, SSI typically employs so-called verifiable credentials (VCs) that are digital certificates, equivalent to physical credentials, such as ID cards, stored in a user-specific digital wallet [27]. They are cryptographically signed and contain specific information (claims) about the identity of a subject [36]. To increase privacy, VCs are often combined with zero-knowledge proofs (ZKPs). These allow users to selectively disclose certain attributes of their digital identity on a case-by-case basis [36].

The use of such VCs involves three different roles: issuer, holder, and verifier. *Issuers* attest various claims about an identity, organize these as VCs, and transfer them to holders. *Holders* can then store VCs in a digital wallet, which gives them exclusive and full control of their VCs. A digital wallet is a software application (e.g., a mobile app) dedicated to managing VCs. The use of cryptographic keys ensures a level of security that is superior to physical wallets [35]. Holders can use their digital wallets and VCs to generate a verifiable presentation (VP) that proofs certain claims about their own identity to *verifiers* [31]. VPs can be derived from one or multiple VCs and provide a tamper-resistant presentation of identity attributes [36]. As VPs are cryptographically secured, verifiers can verify the integrity of the VP in solely bilateral interactions with the holder. The prerequisite is, however, that verifiers trust the issuer. To enhance trust, SSI is often complemented with governance frameworks to enable certification of issuers, ensure trustworthy processes, and provide industry-specific standards for VCs [35].

From a technical perspective, SSI implementations employ so-called decentralized identifiers (DIDs) to exchange VCs. The DIDs typically use verifiable data registries to store DIDs and refer to DID documents [35]. The DID documents commonly contain cryptographic information such as public keys and metadata. These can be used to prove control and establish secure communication channels with the DID controller [37]. As the use of a single DID for multiple connections may cause privacy risks, a set of pairwise-pseudonymous DIDs for each relationship can prevent such correlation [37]. These pairwise DIDs are often not stored in the registry [35]. While the general exchange of VCs does not require blockchain, it can be used as a verifiable registry to store information on accredited issuers or revocation of VCs [27,34].

3. Research Method

To explore the role of blockchain and SSI for decentralized eRoaming, we follow a DSR approach. DSR is a suitable method for the design and development of IT-based artifacts, such as constructs, models, or instantiations to extend organizational capabilities [21, 38]. Our artifact constitutes a conceptual architecture for decentralized eRoaming. Furthermore, we derive four design principles as the first steps towards a nascent design theory [21]. As successful DSR requires both rigor and relevance of research, we strictly followed the suggested process of Peffers et al. [18]. In doing so, we conducted a SLR [19] to ensure the rigor of our research, support our problem formulation, define the requirements and objectives of our solution, and inform the design of our artifact (process steps 1-3) [18,38]. We further presented and evaluated our conceptual architecture in 13 expert interviews (process steps 4+5) to ensure the relevance of our research [18, 38].

To provide a rigorous foundation, we grounded our work in literature by conducting a SLR [19]. For our SLR, we used the search string *electric vehicle* AND *charging* AND *roaming*, and analyzed the databases ACM Digital Library, AISEeL, IEEEXplore, ScienceDirect, Scopus, and Web of Science. Our search covered all full text and metadata analysis and resulted in a total of 357 articles (including 34 duplicates). We then conducted a three-stage screening process to remove all articles that did not focus on eRoaming or related sub-processes. After title (n-195), abstract (n-73), and full-text (n-48) screening, our analysis resulted in a subset of overall seven articles. A forward and backward search lead to one additional article. We also analyzed grey literature to incorporate practical expertise [38]. Using ResearchGate, the Google Search Engine, and reviewing websites of eRoaming initiatives, we identified 11 supplementary documents.

To evaluate our artifact and ensure the relevance of our research, we performed a qualitative evaluation [20]. As illustrated in Table 1, we conducted 13 interviews with experts from the energy sector who focus on eRoaming or decentralized energy systems. More specifically, we conducted interviews with technical as well as business-oriented experts from CPOs, eMSPs, eRoaming providers, consultancies, and research institutes to represent all relevant stakeholders. In these interviews, we first discussed the current status quo and challenges as well as requirements related to eRoaming. This enabled us to validate the identified design objectives and requirements. Thereafter, we presented and reviewed our emerging conceptual architecture for a decentralized eRoaming system and gathered feedback. With the help of this feedback, we continuously reviewed and refined our conceptual architecture in iterative build-and-evaluate loops [38]. We stopped scheduling new interviews once we reached theoretical saturation from the as yet limited practical experiences with SSI. All interviews were conducted in a semi-structured way to limit subjectivity and ensure flexibility as compared to predefined questions [39]. To analyze our data, we followed [40] and performed a two-stage process of inductive and deductive coding. First, two authors analyzed the data independently and assigned initial codes to identify challenges, requirements, and potential approaches to eRoaming. Thereafter, we assigned our initial codes to higher-level concepts that we identified in the literature (deductive coding) or emerged during our analysis (inductive coding). In total, we codified 543 statements organized in four first-order themes (i.e., *problem spaces, requirements, role of blockchain*, and *role of SSI*) and 17 second-order categories that match the core concept presented in the remainder of this work.

Table 1. Interview partners.

ID	Role (Organization)	Experience
1	IT-Developer (CPO & eMSP)	≥ 4 years
2	Business Developer (P2P Energy Trading)	≥ 3 years
3	Team Leader Mobility (Consultancy)	≥ 3 years
4	Researcher (Research Institute)	≥ 3 years
5	Director E-Mob (BLC & Energy Foundation)	≥ 2 years
6	Consultant (IT-Consultancy)	≥ 10 years
7	IT-Consultant (CPO & eMSP)	≥ 10 years
8	Project Manager Mobility (Consultancy)	≥ 1 years
9	Head of Venture Creation (Consultancy)	≥ 2 years
10	Product Manager (eMSP & CPO)	≥ 3 years
11	Researcher (Research Institute)	≥ 2 years
12	Product Manager (eRoaming Start-up)	≥ 4 years
13	CTO (eRoaming Start-up)	≥ 3 years

4. Towards Decentralized eRoaming

4.1. Design Objectives and Requirements

We derived six design objectives as well as 18 matching design requirements from our literature analysis, which were also confirmed by our experts in terms of our evaluation. These objectives and requirements provide the frame of our eRoaming architecture.

DO1 – Disintermediation: EMCHs typically rely on proprietary protocols. Due to network effects and high switching costs, EMCHs often have a monopolistic or oligopolistic position in the eRoaming market [7, 8, 26], which allows them to levy unduly high eRoaming fees. To mitigate this concern, researchers and practitioners recommend to *avoid concentration of market power* (R 1) by developing eRoaming systems that are independent of intermediaries (Experts 1, 5-7, 10-12).

DO2 – Accountability: To enable reliable eRoaming, CPOs and eMSPs must be able to avoid uncovered costs and potential fraud resulting from, for instance, charging with an invalid contract. Thus, every actor involved in a charging event must be *authenticated* (R 2) [23, 24, 41]. CPOs can therefore verify the validity of users' contracts to ensure that they are permitted to charge on behalf of their eMSP. In case of misuse, cancellation, or expiration, an eMSP can *revoke* the permission and respective contract (R 3) [11, 23, 24]. To protect both consumers and CPOs or eMSP, reliable eRoaming also has to ensure that charging events cannot be declared invalid retroactively. This makes *non-repudiation and data integrity* (R 4) an essential requirement [9, 24, 26, 41].

DO3 – Efficiency: For a reliable eRoaming process, seamless information exchange between involved entities is crucial. According to our experts, B2B billing and payment processes are not yet fully automated, which limits such a seamless exchange, and increases eRoaming fees. Thus, *end-to-end process automation* (R 5) is essential for seamless clearing and overall cost reduction [8, 25]. To this end, *a standardized, machine-readable information exchange* between CPOs and eMSPs is essential (R 6) [8, 9, 25]. Moreover, *a standardized ID schema* (R 7) may also simplify the verification of stakeholders [26]. A *public registry* (R 8) can additionally provide information on certified charging points, such as coordinates [22].

DO4 – Data Protection: As prior research illustrates, insufficient protection of personal information and the availability of geographic information, may enable the creation of charging or movement profiles [23, 24]. To prevent such privacy infringement, eRoaming solutions should comply with data protection regulations such as the GDPR or the CCPA. Moreover, *correlations of personally identifiable and charging-related information beyond information required for eRoaming should be avoided* (R 9) (Experts 1, 2, 4, 6 & 9). Specifically, information on a charging event should be accessible only to the user, and the corresponding eMSP for billing purposes [24, 41]. Apart from user data, eRoaming solutions should also protect sensitive business data of CPOs or eMSPs [22, 26] (Experts 5, 9 & 10). Thus, the *confidentiality of sensitive data should be ensured* (R 10) and only authorized entities should be able to access charging-related information. *Data minimization according to the need-to-know principle* (R 11) can, for instance, help CPOs and eMSPs to only receive information that is directly relevant to authentication and billing [23, 24, 41]. Moreover, eRoaming systems should *avoid centralized storage of data* (R 12) to prevent a single point of failure and reduce the risks of data breaches [11].

DO5 – Usability: To enhance EV adoption, eRoaming solutions should be *easy to use* and require at most as many user interactions as traditional charging systems (R 13). The interviewed experts particularly emphasized the principle of *one face to the customer* (R 14). That is, seamless eRoaming should be possible using a single contract, app, or RFID card. This also includes *non-discriminatory pricing and transparent communication of tariffs* (R 15) [9, 22]. Moreover, eRoaming systems should be easy to apply for CPOs and eMSPs and *require no more implementation effort* than current solutions (R 16) [9, 26]. A certain flexibility of eRoaming solutions to grant *business model independence* (R 17) may also help innovation and adoption of eRoaming [9, 26].

DO6 – Scalability: Our Experts 1, 4 & 7 expect an increase of EV adoption. Thus, eRoaming systems will have to cope with an increasing number of users and eRoaming activities. To meet the increasing demand, decentralized eRoaming systems should also consider their scalability to *handle at least as many transactions as centralized eRoaming systems* (R 18) without outages or long response times.

4.2. Conceptual Architecture

Building on the identified design objectives and requirements, we developed a conceptual architecture for decentralized eRoaming. As Figure 1 illustrates, our eRoaming architecture involves three entities: the CPO, the eMSP, and the user. The eRoaming system builds on a public blockchain and SSI for identity management, complemented by legacy systems and secure communication via REST-APIs and HTTPS (R 10). We employ HTTPS communication on a B2B level for clearing and payment, as HTTPS provides a well-established standard for server and client authentication (R 16). However, the X.509 certificates used in HTTPS do not support selective disclosure, and consequently, enable correlation of data [36]. To mitigate ensuing privacy concerns, our architecture employs SSI and VCs on a business-to-customer (B2C) level supported by ZKPs (R 9 - 11). To ensure the authenticity and enable verifiability of VCs, the public blockchain functions as a tamper-resistant verifiable data registry, such as currently provided by Hyperledger Aries and Indy. More specifically, Hyperledger Indy comprises a public permissioned blockchain framework mainly used for storing DIDs and corresponding DID documents, publishing VC schemata and definitions, and creating privacy-preserving revocation registries. Hyperledger Aries provides an interface layer and client-side tools for accessing data stored on the Indy blockchain as well as issuing, verifying, and storing VCs through an API.

For the use of SSI, users receive a digital wallet app installed on a smartphone to authenticate at charging points (R 13). During the installation process, the

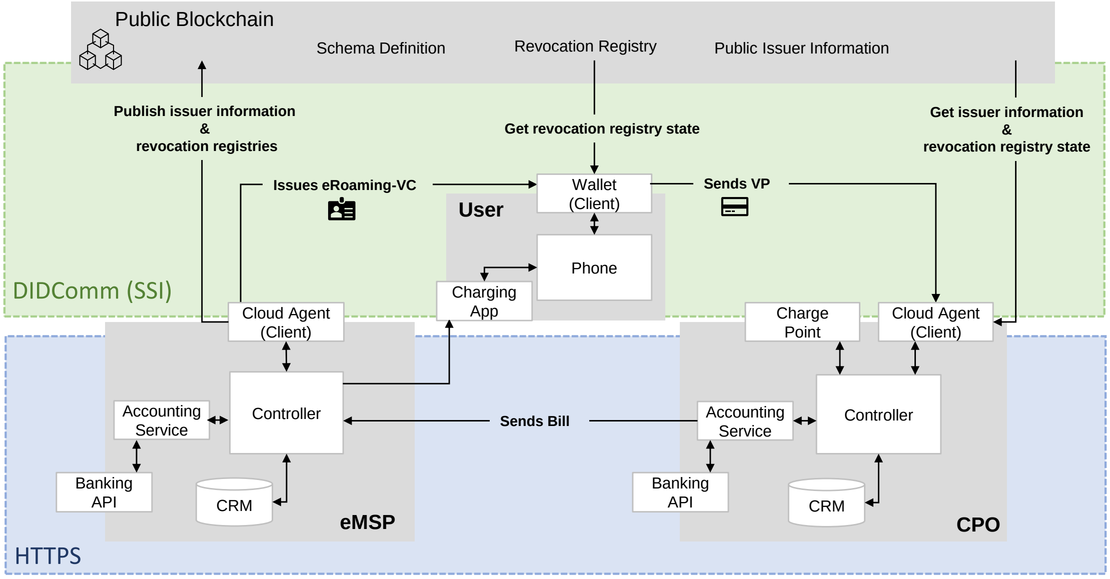

Figure 1. Conceptual architecture for decentralized eRoaming.

wallet generates a private holder binding (e.g., a cryptographic link secret) to limit opportunities for theft and intentional sharing of VCs. The wallet acts as a client that can connect to the blockchain to generate proofs of non-revocation or verify public issuer information (R 2). In addition, the user can install a mobile charging app that can be used for registration and additional services provided by the eMSP.

eMSPs issue VCs that certify the contractual relationship with users. For this purpose, eMSPs run a cloud agent that makes use of the tools provided by Hyperledger Aries. This cloud agent acts as a client that can connect to the blockchain, allowing eMSPs to publish issuer-related information such as DIDs and DID documents. Moreover, eMSPs can create an entry in the blockchain-based revocation registry to revoke previously issued VCs (R 3). The cloud agent also connects to a legacy system to handle the billing of charging events. The legacy system includes a customer relationship management (CRM) system, an accounting service, a banking API, and a controller.

CPOs act as verifiers by connecting their backend system with an Aries-based cloud agent to generate proof requests and validate VCs. The CPO's cloud agent acts as a client and reads the blockchain-based registry to verify the authenticity (signing key) and revocation state of the presented VC (R 2). On the side of CPOs, the legacy system includes a controller, a CRM system, and an accounting service that is connected to a banking API to check for the payment status of charging events. The controller serves as the core module for managing charging events and triggers all other components. In the following, we will outline the eRoaming process.

To enable eRoaming, users must conclude an eRoaming contract with an eMSP. Users can request such a contract, for instance, via a charging app provided by the eMSP. The eMSP's charging app forwards the contract request to the eMSP's controller and triggers a connection invitation. The controller sends the static connection invitation including the eMSP's public DID to the charging app. A deeplink within the connection invitation triggers the user's wallet. The wallet receives the invitation and resolves the DID and DID document via the blockchain to determine the service endpoint (cloud agent). The wallet transmits a newly generated pairwise DID to the eMSP's cloud agent and requests a secure connection. The cloud agent generates a new pairwise DID and establishes the connection (R 10). The eMSP sends the contract in printed form or via email and requests payment details from the user, who manually signs the contract and provides the requested information. To increase process automation, the registration could also employ VCs to authenticate users and transmit their payment detail (R 5).

Based on the provided information, the controller triggers the cloud agent to issue an eRoaming-VC. The cloud agent sends a VC offer to the user's wallet. The VC's attributes include at least the user's name, the EMAID, and the contract expiration date. Furthermore, the VC's metadata contains issuer information. The user verifies the offer and requests the VC. The wallet transmits a blinded link secret (i.e., hash of link secret including a random nonce) to the cloud agent to generate a private holder binding. Finally, the cloud agent issues the VC, which is stored in the user's wallet (R 12).

At the charging point, the user scans a static QR code that is attached to the charging point. The QR code includes a link containing the charging point's ID, initiating a proof request via the CPO's controller. As no secure connection between the user and CPO exists, the CPO's controller triggers the cloud agent to generate a so-called connectionless proof request. Thereby, additional steps such as the creation of pairwise DIDs and key pairs can be avoided. The CPO's cloud agent generates the proof request and directs it to the user's wallet via the controller. The proof request specifies that only credential definitions provided by a CPO's eRoaming partners are accepted (R 2). This ensures that the CPO is allowed to provide charging services on behalf of the eMSP. The wallet notifies the user about the proof request and suggests a VP. Based on the need-to-know principle, the required information may differ. In case of a flat rate contract, a ZKP that the customer has a non-revoked eRoaming-VC representing a contract with a reliable eMSP would suffice (R 11). To generate the ZKP, the wallet requests the revocation state from the blockchain. In case the user does not have a flat rate contract, the EMAID is additionally required for user accountability. As soon as the user confirms the VP, the wallet sends it together with a proof of non-revocation to the CPO's cloud agent. The CPO's cloud agent requests the revocation state from the blockchain to verify the proof and forwards the proof attributes to the controller, which stores the provided information. Upon receiving the information, the controller deletes the proof detail from the cloud agent to ensure steady performance and to avoid redundant storage of user data (R 12). The controller activates the charging point after successful user authentication.

Following a charging event, the charging point generates a CDR and sends it to the CPO's controller, which forwards it to the CPO's accounting service. The CPO's accounting service then receives and reads the CDR and requests the eMSP's billing information from the CPO's CRM system. The CPO's accounting service generates the B2B billing document and sends it to the eMSP's controller together with the corresponding CDR. This initiates the accounting process on the part of the eMSP. The eMSP's accounting service receives the CDR and billing document from the controller and verifies both. The accounting service then prompts a bank transfer to the CPO. In parallel, the eMSP's accounting service requests the user's payment detail from the eMSP's CRM system and generates the direct debit. The accounting service executes the bank transfer and commits the direct debit via the banking API.

5. Evaluation and Implications

We presented and evaluated our conceptual architecture in 13 expert interviews. The experts emphasized the user-friendliness of our framework, and confirmed its overall feasibility. Our conceptual architecture addresses many identified requirements for decentralized eRoaming but cannot ensure R 15 as the tariff-design may depend on the B2B eRoaming agreements. Scalability (R 18) cannot be assessed because we have not yet implemented our solution. The same applies to the correlation of data (R 9), which may not be entirely eliminated outside of a flat rate agreement. We thus advocate for an additional cryptographic mechanism (ZKPs) to enhance privacy.

In our interviews, we identified four generalizable design principles. These design principles help to determine the role of blockchain and guide practical implementations of SSI-based eRoaming and the presented architecture. Some design principles may also be abstractable to other use cases.

DP1 – Don't use blockchain for payment: Blockchain-based clearing would require the replacement of well-established accounting systems. For CPOs and eMSPs, this replacement entails substantial organizational overhead (R 16) and, according to our experts, could also raise legal concerns (Experts 1, 4, 5, 9 & 12). Expert 4 emphasized potential organizational constraints of blockchain-based payment – in particular for cases such as eRoaming where accounting is often conducted asynchronously on a monthly basis: *"There is no need for writing transactions retroactively on a blockchain. Instead, one could use traditional APIs"*. Legal concerns primarily result from the use of cryptographic tokens for accounting purposes. Expert 1, for instance, does not *"believe that blockchain will replace a traditional accounting system's functionality. On the contrary, such accounting systems are often legally required."* While the EU's Markets in Crypto Assets directive may reduce legal uncertainties regarding the use of tokens in the future, their use poses legal uncertainties today [42].

Moreover, CPOs and eMSPs often lack the technical capabilities for implementing blockchain-based payment systems (Experts 1 & 4). The know-how required to use blockchain, which according to our experts has not yet reached a level of maturity where it would be easy to understand and deploy, may overwhelm CPOs and eMSPs (R 16). The use of token-based payment is also ill-received from a usability perspective (Experts 5, 9 & 12). Users, in particular, but also legal entities such as CPOs or eMSPs often refuse to accept private tokens or public cryptocurrencies, not least as they require the cumbersome exchange of fiat currency into domain-specific tokens [10] (R 13). According to Expert 12, *"there are many projects that offer stable coins. However, they all just don't make sense as they require two or three additional steps, which reduces efficiency"*.

DP2 – Don't store sensitive data on-chain: Many decentralized eRoaming systems lack standardized PKIs for users [25]. According to Experts 5, 9 & 13, such PKIs could be achieved through the combination of VCs and blockchain technology. This would enable public auditability independent of certificate authorities [31]. While Expert 5 emphasizes the need for a blockchain *"as trust anchor [so that] certificates are unchangeable,"* others fear that the use of blockchain may jeopardize the competitiveness of CPOs and eMSPs. Storing too much charging-related information on-chain may make sensitive business data publicly available and present unwanted privacy challenges (Experts 5, 9 & 11) (R 10).

For users, privacy considerations are even more critical. Since VCs are predominantly used to identify natural persons, data privacy regulations, such as the GDPR, require that personal data can either be fully anonymized or even erased. However, *"this [erasure of personal data] is not possible with blockchain"* (Expert 13), which is why storing identifiable information of natural persons on-chain is difficult to reconcile with such regulation (Expert 2, 4, 9, 11 & 13). Moreover, tamper-resistant storage of VCs does not automatically guarantee their authenticity. Verifiers would have to validate the identity of a VC's issuer. To assess the integrity of such authorized issuers, it would be advisable to use a public blockchain as a verifiable registry for publishing essential and intently public information (Expert 5, 11 & 13) (R 2). The tamper-resistance of a blockchain thereby ensures the integrity of issuer information and prevents fraud. We considered this recommendation in our proposed architecture and only used the public blockchain for information on issuers and the revocation status of VCs. For personal information in the form of VCs and users' cryptographic keys, we used digital wallets to avoid conflicts with privacy expectations and regulation. This enables the required off-chain storage of personal information for SSI applications using blockchain [27].

DP3 – Don't overuse VCs: Our proposed architecture employs VCs for third-party verification of contract information to facilitate reliable user authentication. This entails VC-based information exchange between users and CPOs, and users and eMSPs. In addition, we also discussed the potentials of VCs as user receipts after charging or for direct communication between CPOs and eMSPs in our interviews. While some experts see benefits in these applications, opinions are divided. Experts 4, 5 & 9, for instance, deem VCs for both user receipts and the communication between CPOs and eMSPs redundant as involved parties communicate directly and no third-party verification is required: *"I don't see benefits [for using a VC for B2B data exchange], because it's just data that could also be transferred directly. The benefit of VCs is that they can be stored and repeatedly presented to a verifier"* (Expert 5). Other than being redundant, the use of VCs for user receipts may even be harmful to overall user-friendliness according to our interviewed experts. Receiving a VC after every transaction (e.g., charging event) would unnecessarily clutter the wallets of users without any added value. Instead, a consolidated monthly overview of charging sessions via email or the eMSP's charging app would suffice (Expert 4 & 6) (R 14). *"I think most end users, they're interested in the monthly statement at the end. And then you could list the individual charging processes in a PDF, if someone is interested"* (Expert 4).

That is, VCs should primarily be used for information that requires third-party verification and frequent presentation. In other cases, especially where direct communication between cooperating parties is involved, conventional channels are better suited for the transfer of information. Our experts would recommend a digital signature and the commonly used HTTPS (R 4) protocol for secure and tamper-resistant information exchange (Expert 1 & 11). HTTPS is also less complex than VCs (R 16) and users as well as eMSPs and CPOs can rely on a more mature technology.

DP4 – Don't exaggerate decentralization: In our architecture, SSI components run in the CPOs' backend and on mobile apps of users' mobile phones. We also discussed options for installing SSI components directly on hardware, for instance, EVs and charging points. Yet, charging points often have only limited computational functionalities, and CPOs typically connect their charging points to a backend system (controller). This enables the simultaneous operation of multiple charging points and considerably reduces complexity and costs. While blockchain and SSI are often associated with a maximum of decentralization, our experts would refrain from installing SSI components on each individual hardware separately, such as charging points (Experts 1, 4, 6 & 8-13). Instead, they argue for a level-headed approach that does not trade functionality and user-friendliness for maximal decentralization.

Many experts, however, believe that EV-based SSI may enhance functionality and user-friendliness although it would also lead to more decentralization. In this scenario, EVs, not users, would act as holders of VCs. A similar approach has already been suggested with the plug-and-charge ISO 15118 standard [23]. EVs would automatically present their VCs to the charging point to initiate charging-related transactions (Expert 2, 9, & 10). While such an approach may appeal to users, it would require substantial retrofitting of current EVs for car manufacturers to comply with technical requirements of SSI. To enable automatic charging, also charging points would have to be adapted for the direct reception and verification of VCs [25] (Expert 10 & 11).

To date, both car manufacturers and CPOs would resent major and often unnecessary adjustments of their hardware [34]. To retain the flexibility granted by decentralization albeit avoiding high retrofitting costs and potential fragmentation, Experts 3, 4, 6-8, 10 & 11 called for leveraging a single software-based SSI implementation compatible with CPOs' and eMSPs' legacy systems and independent of EVs. The cloud agent should accordingly be integrated into a CPO's backend system and user's digital wallet in the form of a mobile app, not to the charging point or EV itself. This would considerably reduce implementation and maintenance efforts and would benefit CPOs as it allows for the use of a single cloud agent for multiple charging points to further diminish fragmentation (R 16): *"I think it's easier to implement it in the backend, as otherwise, I would have to check the technical feasibility for each charging point"* (Expert 8).

6. Conclusion

eRoaming can improve access to charging infrastructure. Yet, current systems are predominately centralized and entail risks of market power concentration [7, 9]. While decentralized solutions with blockchain have been considered to mitigate such risks, they come with significant privacy concerns [8, 11]. We, therefore, aim to provide an alternative approach by investigating how a decentralized eRoaming systems can be designed with blockchain and SSI. Using DSR helped us to answer our research question by developing a conceptual architecture for decentralized eRoaming based on blockchain and SSI. In doing so, we derive four generalizable design principles as a theoretical contribution [21]. Our research provides a more nuanced understanding of the roles of blockchain and SSI for decentralized eRoaming and related service models. Specifically, we identified that SSI can address privacy-related problems of eRoaming. We also find that blockchain can function as a public registry, while it best leverages its benefits when it takes a backseat for other applications. Our findings provide practical guidance for roaming service architectures based on blockchain and SSI. However, this research is also subject to limitations. While the proposed architecture employs a blockchain as a public verifiable registry, traditional centralized databases might also serve this function. In this context, further research is necessary to assess the need and benefits of blockchain for SSI applications [43]. Moreover, as this work focuses on decentralized eRoaming, it provides limited generalizability. For future research, we aim to extend the scope of our analysis beyond eRoaming. In doing so, we aim to derive a more generalizable design theory for eRoaming and similar service models.

Acknowledgement

Supported by PayPal and the Luxembourg National Research Fund FNR, Luxembourg (P17/IS/13342933/PayPal-FNR/Chair in DFS/ Gilbert Fridgen) as well as by the Luxembourg National Research Fund (FNR) – FiReSpARX Project, ref. C20/IS/14783405/FiReSpARX/Fridgen.

References

[1] H. Lund and W. Kempton, "Integration of renewable energy into the transport and electricity sectors through V2G," *Energy Policy*, vol. 36, no. 9, 2008.

[2] P. K. Tarei, P. Chand, and H. Gupta, "Barriers to the adoption of electric vehicles: Evidence from India," *Journal of Cleaner Production*, vol. 291, 2021.

[3] R. R. Kumar and K. Alok, "Adoption of electric vehicle: A literature review and prospects for sustainability," *Journal of Cleaner Production*, vol. 253, 2020.

[4] J. Martínez-Lao, F. G. Montoya, M. G. Montoya, and F. Manzano-Agugliaro, "Electric vehicles in Spain: An overview of charging systems," *Renewable and Sustainable Energy Reviews*, vol. 77, no. 1, 2017.

[5] S. Hardman and G. Tal, "Understanding discontinuance among California's electric vehicle owners," *Nature Energy*, pp. 1–8, 2021.

[6] G. Harrison and C. Thiel, "An exploratory policy analysis of electric vehicle sales competition and sensitivity to infrastructure in Europe," *Technological Forecasting and Social Change*, vol. 114, pp. 165–178, 2017.

[7] R. Ferwerda, M. Bayings, M. van der Kam, and R. Bekkers, "Advancing e-roaming in Europe: Towards a single "language" for the European charging infrastructure," *World Electric Vehicle Journal*, vol. 9, no. 4, 2018.

[8] German Federal Ministry of Transport and Digital Infrastructure, "Opportunities and challenges of DLT (blockchain) in mobility and logistics."

[9] M. van der Kam and R. N. A. Bekkers, "Report D6.1-D6.3 for the EVRoaming4EU project," 2020.

[10] Bundesnetzagentur, "Die Blockchain-Technologie: Potentiale und Herausforderungen in den Netzsektoren Energie und Telekommunikation," 2019.

[11] J. C. Ferreira, C. Ferreira da Silva, and J. P. Martins, "Roaming service for electric vehicle charging using blockchain-based digital identity," *Energies*, vol. 14, no. 6, 2021.

[12] B. Kim, W. Shin, D.-Y. Hwang, and K.-H. Kim, "Attribute-based access control (ABAC) with decentralized identifier in the blockchain-based energy transaction platform," in *International Conference on Information Networking*, pp. 845–848, IEEE, 2021.

[13] S. Albrecht, S. Reichert, J. Schmid, J. Strüker, D. Neumann, and G. Fridgen, "Dynamics of blockchain implementation – A case study from the energy sector," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[14] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, vol. 100, pp. 143–174, 2019.

[15] N. Kannengießer, S. Lins, T. Dehling, and A. Sunyaev, "Trade-offs between distributed ledger technology characteristics," *ACM Computing Surveys*, vol. 53, no. 2, 2020.

[16] A. Rieger, F. Guggenmos, J. Lockl, G. Fridgen, and N. Urbach, "Building a blockchain application that complies with the EU General Data Protection Regulation," *MIS Quarterly Executive*, vol. 18, no. 4, pp. 263–279, 2019.

[17] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, 2019.

[18] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.

[19] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly*, vol. 26, no. 2, pp. 13–23, 2002.

[20] C. Sonnenberg and J. Vom Brocke, "Evaluation patterns for design science research artefacts," in *European Design Science Symposium*, pp. 71–83, Springer, 2011.

[21] S. Gregor and A. R. Hevner, "Positioning and presenting design science research for maximum impact," *MIS Quarterly*, vol. 37, no. 2, pp. 337–355, 2013.

[22] Renewable Energy Association, "The interoperability of public EV charging networks in the UK," 2019.

[23] C. Höfer, J. Petit, R. Schmidt, and F. Kargl, "POPCORN - Privacy-preserving charging for emobility," in *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles - CyCAR '13*, pp. 37–48, 2013.

[24] D. Zelle, M. Springer, M. Zhdanova, and C. Krauß, "Anonymous charging and billing of electric vehicles," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ACM, 2018.

[25] BDEW e. V., "Mindestanforderungen der Energiewirtschaft an Daten für zukunftssichere Ladeinfrastruktur 2020/21," 2020.

[26] K. Noyen, M. Baumann, and F. Michahelles, "Electric mobility roaming for extending range limitations," in *ICMB*, 2013.

[27] A. Rieger, T. Roth, J. Sedlmeir, and G. Fridgen, "The privacy challenge in the race for digital vaccination certificates," *Med*, vol. 2, 2021.

[28] M. Rossi, C. Mueller-Bloch, J. B. Thatcher, and R. Beck, "Blockchain research in information systems: Current trends and an inclusive future research agenda," *Journal of the Association for Information Systems*, vol. 20, no. 9, 2019.

[29] B.-J. Butijn, D. A. Tamburri, and W.-J. van den Heuvel, "Blockchains: A systematic multivocal literature review," *ACM Computing Surveys*, vol. 53, no. 3, 2020.

[30] G. Fridgen, S. Radszuwill, N. Urbach, and L. Utz, "Cross-organizational workflow management using blockchain technology-towards applicability, auditability, and automation," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[31] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, 2018.

[32] M. Backes, J. Camenisch, and D. Sommer, "Anonymous yet accountable access control," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp. 40–46, ACM, 2005.

[33] A. Lioy, M. Marian, N. Moltchanova, and M. Pala, "PKI past, present and future," *International Journal of Information Security*, vol. 5, no. 1, pp. 18–29, 2006.

[34] M. Kubach, C. H. Schunck, R. Sellung, and H. Roßnagel, "Self-sovereign and decentralized identity as the future of identity management?," *Open Identity Summit*, pp. 35–47, 2020.

[35] A. Preukschat and D. Reed, *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*. Manning Publications Co., 2021.

[36] M. Sporny, D. Longley, and D. Chadwick, "Verifiable credentials data model 1.0," 2019.

[37] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized identifiers (DIDs) v1.0," 2021.

[38] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[39] M. D. Myers and M. Newman, "The qualitative interview in is research: Examining the craft," *Information and Organization*, vol. 17, no. 1, pp. 2–26, 2007.

[40] M. B. Miles, A. M. Huberman, and J. Saldaña, *Qualitative data analysis: A methods sourcebook*. Sage Publications, 2018.

[41] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Roaming electric vehicle charging and billing: An anonymous multi-user protocol," in *International Conference on Smart Grid Communications*, pp. 939–945, IEEE, 2014.

[42] P. Sandner, "Crypto-europe: Comprehensive European regulation for crypto assets has been presented," 2020.

[43] S. Mahula, E. Tan, and J. Crompvoets, "With blockchain or not? opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the belgian case," in *DG. O2021: The 22nd Annual International Conference on Digital Government Research*, pp. 495–504, 2021.