Comput Sci Res Dev (2018) 33:71–79
https://doi.org/10.1007/s00450-017-0348-5

energieinformatik2017
The Swiss-German-Austrian Research Summit on Energy Informatics

SPECIAL ISSUE PAPER

Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions

Fabian Knirsch[1] · **Andreas Unterweger**[1] · **Dominik Engel**[1]

Published online: 4 September 2017

Abstract Electric vehicles are gaining widespread adoption and are a key component in the establishment of the smart grid. Beside the increasing number of electric vehicles, a dense and widespread charging infrastructure will be required. This offers the opportunity for a broad range of different energy providers and charging station operators, both of which can offer energy at different prices depending on demand and supply. While customers benefit from a liberalized market and a wide selection of tariff options, such dynamic pricing use cases are subject to privacy issues and allow to detect the customer's position and to track vehicles for, e.g., targeted advertisements. In this paper we present a reliable, automated and privacy-preserving selection of charging stations based on pricing and the distance to the electric vehicle. The protocol builds on a blockchain where electric vehicles signal their demand and charging stations send bids similar to an auction. The electric vehicle owner then decides on a particular charging station based on the supply-side offers it receives. This paper shows that the use of blockchains increases the reliability and the transparency of this approach while preserving the privacy of the electric vehicle owners.

Keywords Blockchain · Privacy · Electric vehicles

✉ Fabian Knirsch
fabian.knirsch@fh-salzburg.ac.at

[1] Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control, Salzburg University of Applied Sciences, Urstein Süd 1, 5412 Puch b. Hallein, Austria

1 Introduction

Electric vehicles (EVs) are becoming more and more common and charging stations are a growing infrastructure, especially in urban areas. Furthermore, connecting EVs and blockchain technology is an upcoming issue [8]. EVs are also seen as a key component for a future intelligent energy grid [17]. This so-called *smart grid* does not only affect the way energy demand and production are handled and controlled, but also offers a whole new range of tariffs and dynamic pricing. In a liberalized market different charging stations from different operators or energy providers are competing entities. Each provider may also offer dynamic pricing depending on the energy needed and the time available for charging. Customers may, for instance, get cheaper tariffs if they are willing to charge over longer periods of time which allows the energy providers to better curtail load. If, however, a lot of energy is needed in a short period of time and during peak hours, this will increase the price. Charging stations can therefore optimize their utilization based on the current energy demand and supply.

It has been shown that such demand response and dynamic pricing use cases are subject to privacy issues, e.g., [3,14,15]. Furthermore, fine-grained position data allows, e.g., for position tracking, targeted advertisements and for identifying customer habits such as the workplace, regular working hours or other related properties [4,13]. Therefore, the collection and unauthorized processing of such data is a severe privacy issue. Hence, it is crucial to find an approach that allows customers to query charging stations for the lowest available price within a certain area, while at the same time preserving their privacy by not revealing their position and actual energy need to the public. In order to achieve this goal, instead of requiring some sort of trusted entity, this work uses a blockchain for verifiable and immutable data storage and

contract initiation. Blockchains are an upcoming technology originally introduced in 2008 by [18] as part of *Bitcoin*. Both, EVs and charging station operators do not need to trust a single entity, but trustful operation is achieved if at least half of the participants' computing power is spent honestly.

This paper has three main contributions: (i) a protocol is proposed that finds an optimum charging station, given public biddings as response to a query; (ii) at the same time the customers geographic position is not revealed during protocol execution; and (iii) a blockchain is used as a decentralized and immutable storage for transparency and verifiability of these biddings. The protocol design keeps the communication overhead and the amount of data to be stored in the blockchain small, which allows to use existing blockchain technologies such as Bitcoin. The privacy of the protocol is evaluated in an honest-but-curious adversary model. This paper focuses on the privacy of the EV and assumes that charging stations and their bids are publicly known.

The rest of this paper is structured as follows: Sect. 2 introduces preliminaries and related work in the field of privacy and security, electric vehicle charging and blockchains. Section 3 introduces the proposed protocol in detail, i.e., its four steps *exploration*, *bidding*, *evaluation* and *charging*. Section 4 evaluates the protocol with respect to privacy, security and communication overhead.

2 Preliminaries and related work

This section discusses the preliminaries and related work in the domain of privacy and security issues for EV charging and tariff-decisions, general issues of EV charging and the state-of-the-art in blockchains and smart contracts, as well as commitment schemes.

2.1 Privacy and security

General privacy issues in the smart grid are discussed in, e.g., [9,16]. Privacy issues specifically related to electric vehicles are investigated in [13]. The authors identify four cases of controlled (as in: controlled by the grid-operator) and uncontrolled charging in the customer premises and at foreign premises. In each case, privacy is affected differently. The authors find, e.g., that charging on foreign premises allows to learn about customers' social networks, employers and other habits, such as preferred routes.

The subject of location-privacy and the assessment of location-privacy protection mechanisms is discussed in [22]. The authors propose a framework that allows to evaluate the performance of protection mechanisms based on a generic attack model and statistical methods for evaluating these attacks. The advantage of the adversary is determined by the level of correctness when inferring the user's position. While the paper mainly addresses the privacy critical traces of mobile devices, e.g., from GPS sensors, this is also relevant for traces left by EVs when using public charging stations.

A protocol for privacy-preserving tariff-matching is proposed in [24]. This protocol allows customers to select an optimum tariff for their household from a set of tariffs offered by energy providers, given a load profile forecast and template load profiles. The approach uses embeddings in order to protect both, the customer's load forecast and the utilities' tariff options. While this approach still relies on a third party, in [11] the protocol is extended by a blockchain.

In this paper, the objective is to allow customers to publicly query a set of charging stations for an optimum tariff. This includes public charging stations and private charging stations that are vacant at the requested time interval. However, none of the involved parties should learn the customer's position and energy need during this phase.

Generally, privacy is preserved if participants do not learn anything beyond some particular function of someone's data [10]. In the proposed protocol privacy is preserved, if (i) none of the participants learns the exact position of the EV; (ii) no participant, except for the EV and the selected charging station, learn at which price energy is purchased; and (iii) EVs cannot be tracked over time. For this paper an honest-but-curious adversarial model is assumed, i.e., all participants follow the protocol but attempt to learn additional information.

2.2 Blockchains and smart contracts

Blockchains are a trustless and fully decentralized peer-to-peer data storage that is designed to hold immutable information once data is committed to the chain. Generally, a blockchain can therefore be described as a distributed, immutable database. After having originally been proposed in [18], blockchains are gaining an increased adaption in many fields, e.g., finance and stock markets, voting and smart contracts, as well as energy generation and distribution [12,27].

In the originally proposed Bitcoin protocol from [18] the blockchain is used to keep track of *coins*, i.e., a public list of financial transactions and how many coins are owned by each peer. Therefore, each transaction contains sender and receiver information, as well as the number of coins to be transferred. A number of such transactions—once confirmed by the peers—become a new block. Such a block also includes the hash of the previous block and is appended to the chain. The transactions are therefore permanently linked to the series of previous transactions.

This list of chained blocks is public and can be verified by all peers in the network by checking the integrity of the new block and the correct calculation of the hash. Peers in the network are identified by a private–public key pair, which

is often referred to as the *ID* or *address*. A blockchain does not require a single trusted party, but instead is trustless if at least half of the computing power used for creating and verifying blocks is spent by honest peers [18]. Furthermore, peers and transactions are anonymous in the sense that sender and receiver are only identified by their address and that a new pair of keys (and therefore a new address) can be created for every transaction.

In [1], the authors present an approach with stronger privacy guarantees where the contents of transactions are kept private by using zero-knowledge proofs. Further advances in blockchain technology are smart contracts, such as presented in [12,25]. While Bitcoin is only designed for financial transactions and has limited capabilities for storing additional data, smart contracts allow to perform turing-complete (e.g., Ethereum, Hawk) decentralized and verifiable calculations in the blockchain.

For the protocol proposed in this paper, there is no need to perform actual calculations in the blockchain, i.e., smart contracts such as in [12,25] are not required. Furthermore, only small amounts of data are stored in the blockchain, which does not require advanced transaction verification. This allows for the proposed protocol to be based on a lightweight blockchain or even Bitcoin, which is capable of embedding a limited amount (e.g., 80 bytes in OP_RETURN)[1] of additional data in transactions [18].

2.3 Commitment schemes

Commitment schemes have a binding and a hiding property. The schemes allow participants in a protocol to commit themselves to a value (binding property) and to keep this value secret (hiding property) until the commitment is opened. Common schemes for commitments include Pedersen commitments [2,19] and commitments based on cryptographic hash functions (e.g., SHA-2) [6].

As a practical example for the use of commitments consider an implementation of a rock-paper-scissors game as discussed in [6], where all players send their bets one after another. The bet should be hidden until all players have sent their respective value and, once sent, the bet should be locked so that the last player has no advantage over the others by knowing the previous bets. Given a cryptographic hash function $H(\cdot)$, players can hash their bet and a random number as a commitment by $H(\text{“bet”}|\text{“random number”})$. Once all bets are placed, i.e., all commitments have been sent, the players open their commitments by revealing “bet” and “random number”. All participants can verify each others’ commitment by recalculating H and comparing the hashes. If the hashes match, this ensures that no bet has been changed.

[1] https://en.bitcoin.it/wiki/OP_RETURN.

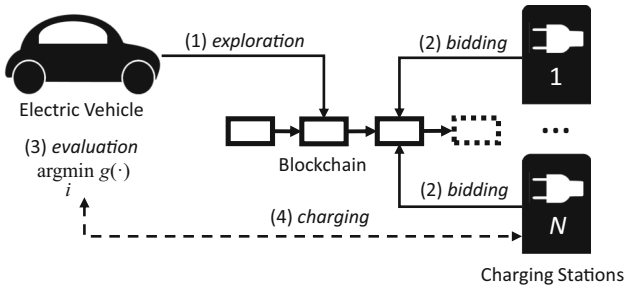

Fig. 1 Visual representation of the four steps of the proposed protocol: In step 1, *exploration*, the EV send a request to the blockchain. In step 2, *bidding*, the charging stations send bids for this request and one of them is chosen in step 3, *evaluation*, by the EV. Step 4, *charging*, is handled off the blockchain

In this paper such a commitment scheme is used by the EV to commit the decision for a particular charging station without immediately revealing the selection. The presented commitment scheme is very powerful in combination with a blockchain, where the hash function is responsible for the hiding property and the blockchain assures the binding property.

3 Protocol

In this section a protocol for privacy-preserving EV charging with a blockchain is presented. The protocol is executed between a single EV and one or more charging stations.

An EV is uniquely identified in the blockchain by an ID ζ (which is usually derived from the public key [18]). Each charging station is identified by a unique index i in a similar way. It is assumed that a list of charging stations, including their position, is available and publicly known.[2] To enhance privacy, ζ as the identity of the EV can be changed for every request.

For initialization, the EV chooses parameters R, T and e. R is a geographic region, e.g., the city of Salzburg and a radius of 10 km, which covers the inner city and some suburban areas. The values for e and T refer to the expected amount of energy that is needed and the desired time-frame for charging, respectively. For a *Tesla super charger*, for example, this could be $e = 90$ kWh and $T = [12{:}00, 13{:}15]$ (75 min).[3] More commonly, public charging stations serve for $e = 20$ kWh and $T = [12{:}00, 14{:}00]$ (120 min) [26].

The principal setup of the proposed protocol is shown in Fig. 1. In order to find an optimum charging station (i.e., one that minimizes costs or any other desired criterion), the EV and the charging stations run the four-stage protocol which

[2] E.g., as already available for most EU countries: https://e-tankstellen-finder.com/.

[3] https://www.tesla.com/supercharger.

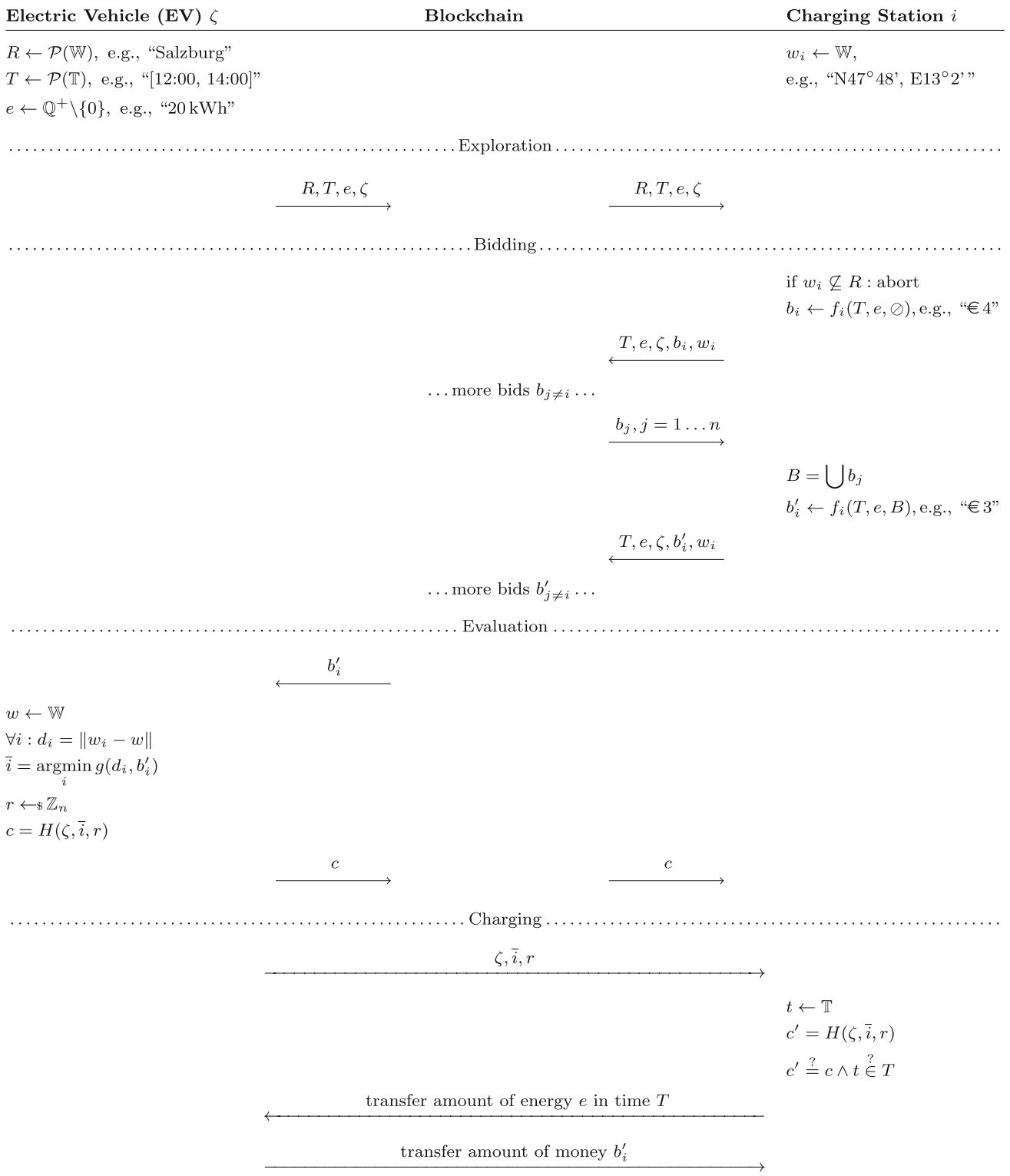

Fig. 2 This diagram shows the four stages of our proposed protocol between the EV, a blockchain and a particular charging station i. In the *exploration* phase the EV submits a region, a time frame and the desired amount of energy to the blockchain. In the *bidding* phase the nearby charging stations send one or more bids along with a commitment for the offered price to the blockchain. In the *evaluation* phase, the EV determines the optimum charging station in terms of price and distance and sends a commitment for this decision to the blockchain. The *charging* phase is handled off the blockchain and the EV communicates directly with the selected charging station. The EV opens its commitment and—if valid—the charging station begins the transaction at the previously agreed amount of energy for a given price over a given period of time

Table 1 Notation used in this paper

Symbol	Description
ζ	Unique identifier for electric vehicle
i	Unique index of charging station
$w \in \mathbb{W}$	World position, e.g., latitude and longitude
$R \subset \mathbb{W}$	Region (set of world positions)
$T \subset \mathbb{T}$	Time interval (set of timestamps)
$e \in \mathbb{Q}^+ \backslash \{0\}$	Energy needed by EV in kWh
b	Bid in monetary units
$f(\cdot)$	Heuristic to determine next bid
$r \leftarrow\$ \mathbb{Z}_n$	Sampling of a n bit random number
$H(\cdot)$	Cryptographic hash function, e.g., SHA-2
c	Commitment
d_i	Distance to charging station i
$g(\cdot)$	Heuristic deciding on charging station
$\bar{i}$	Selected charging station
$\oslash$	Empty set
$\mathcal{P}(\cdot)$	Power set

is described in detail in the following sections. The detailed sequence of exchanged messages is shown in Fig. 2. The notation used in this paper is listed in Table 1.

3.1 *Exploration* phase

In the *exploration* phase the EV places a request in the blockchain. This request is for an amount of energy $e \in \mathbb{Q}^+ \backslash \{0\}$ over a time interval $T \subset \mathcal{P}(\mathbb{T})$ within a geographic region $R \subset \mathcal{P}(\mathbb{W})$. The region is a set of world positions, each specified in latitude and longitude. Note that this request cannot be linked directly to a specific individual as only the ID ζ of the EV is revealed in the blockchain alongside the request and that this request does not contain the current position of the EV. Once a request is in the blockchain, it is visible to all charging stations (and naturally to all other participants, such as other EVs).

3.2 *Bidding* phase

In the *bidding* phase, only the charging stations act. They query the blockchain for new requests or some out-of-band signaling protocol can be used to notify charging stations of new requests. Those charging stations that are within the desired region R send bids for the lowest price. This auction is handled over the blockchain and is therefore fully decentralized and transparent. Given the request (R, T, e) from an EV, each charging station i first checks whether its own position is within the region R. In this case, it reads existing bids B from the blockchain (or $\oslash$ if no bids exist yet). The charging station then creates its own bid b_i based on some heuristic $b_i = f(T, e, B)$. Usually, this function will determine if the charging station i is willing to offer energy e in time T for price $b_i \leq b_j, j = 1, \ldots, N$. This bid is written to the blockchain and therefore public and immutable.

The public nature of the bids incentivizes other charging stations to offer a cheaper price. This is similar to traditional auction settings. The immutability of the bids further prevents the charging station from later denying that a certain bid has been made. While this makes the *bidding* phase more transparent and reliable, this information is only needed for a short period of time, but still takes up space in the blockchain. While this is an inherent feature of blockchains, i.e., even outdated information is still stored and available, the protocol is designed to be lightweight and with little communication overhead to minimize the amount of data to be stored in the blockchain.

The process of bidding is repeated until either the price converges, a certain amount of time has passed, or the EV stops the process. It is up to the EV to decide if (i) only the very first bid of each charging station is accepted; or if (ii) charging stations can send updated offers based on competitor bids. In the first case, this might motivate charging stations to already send their lowest offer first, whereas in the second case the price might slowly converge.

3.3 *Evaluation* phase

In the *evaluation* phase the EV gathers the bids from the blockchain that match the initial request. The EV then decides on a charging station based on some heuristic that finds an optimum tradeoff between price and distance to a charging station. For instance, the EV may not choose the lowest price in the region, but a charging station that offers a slightly higher price and is much closer to its current position. The decision may also be influenced by other parameters, such as nearby shops or activities to be done during the charging process. The decision is completely up to the EV and the customer, respectively, and computed privately off the blockchain.

Once a suitable charging station is found, the EV computes a hiding and computationally binding commitment $c = H(\zeta, \bar{i}, r)$ from the ID of the EV ζ, the index of the desired charging station $\bar{i}$ and a freshly drawn random number r. This commitment is written to the blockchain. Due to the one-way property of the hash, this does not reveal the decision to anyone until the commitment is opened. Therefore, even if this information is publicly available to anyone in the blockchain, it does not allow anyone to learn anything about the decision, apart from the fact that it has been made.

3.4 *Charging* phase

In the *charging* phase, the EV approaches the desired charging station $\bar{i}$. This phase does not involve a blockchain, but is a transaction directly executed between the EV and a charging station.

In order to verify that this charging station is the one actually chosen by the EV in the previous phase, the commitment is opened by sending $\zeta, \bar{i}$ and r from the EV to the charging station. The charging station can then check the commitment by verifying that $H(\zeta, \bar{i}, r) = c$ and can further determine whether the current time matches the initially proposed time-frame of the EV.

If both, the commitment and the time-frame, are valid, the amount of energy e is exchanged during the time interval T for the price b'_i. Since this transaction is only executed between the EV and the chosen charging station, no information is released to the blockchain or any other third party. In particular, the actual position of the EV is only revealed to this single charging station. This is analyzed in more detail in the next section.

While this phase could be handled in the blockchain as well, e.g., using some sort of cryptocurrency, the scope of this work is on finding the best tariff without limiting the protocol to a particular payment scheme. Currently, there are many different payment schemes for EV charging in the field, e.g., membership cards, credit cards or even cash could be used for anonymous payment. However, for other use cases, such as settlement and profiling, the actual amount of energy consumed by the EV can be written to the blockchain.

4 Evaluation

The proposed protocol is evaluated with respect to privacy and security, computational complexity and practicability. Furthermore, design considerations for a concrete blockchain technology are stated.

4.1 Privacy and security

The initially stated privacy requirements for this protocol are (i) none of the participants learns the exact position of the EV; (ii) no participant, except for the EV and the selected charging station learn at which price energy is purchased; and (iii) EVs cannot be tracked over time. For the privacy and security analysis all steps of the protocol are investigated in an honest-but-curious adversarial model.

First, and most importantly, all participants are anonymous, i.e., they are only identified by an ID in the blockchain. However, it has been shown that deanonymizing participants is possible by linking transactions and keys [20]. To mitigate this, for each request, the ID can be changed by generating a new key pair. Furthermore, the presented protocol for privacy-preserving dynamic tariff decisions adds an additional level of privacy, which is evaluated in this section.

In the *exploration* phase, the amount of energy, the period of time and a region are published by the EV. The region must be chosen broadly enough to preserve privacy, but sufficiently narrow to be within a feasible range for the EV. Within urban areas with a large number of charging stations, choosing a proper range should be relatively easy. For finding an optimum range, location-privacy assessment tools such as presented in, e.g., [22] can be employed. Neither the involved charging stations nor any other participants in the blockchain learn anything from that request beyond (R, T, e) and the unique ID ζ. As described above, ζ can be changed on every request, thus it does not allow to track an EV over multiple requests. Given only the values (R, T, e) and without a connection between different requests, none of the participants learns the exact position of the EV and EVs cannot be tracked over time.

In the *bidding* phase, the EV is not involved in the protocol, since only charging stations bid. Therefore, the privacy of the EV is not impacted in this phase. While the bids are publicly available in the blockchain, they are only linked to the parameters (R, T, e) and ζ. As discussed before, no connection between different requests is possible when ζ is changed on every request. Note that, at this stage of the protocol, the bids are only considered offers and that the EV has not established a contract with any of the charging stations. The blockchain assures the binding after publication in the blockchain, i.e., if the EV later decides on a particular charging station, the latter has to offer the energy at the previous bid's price.

In the *evaluation* phase, the EV privately decides on one of the bids off the blockchain. No information about this decision is leaked to the outside. Thus, no participant, except for the EV learns at which price energy is going to be purchased. However, a binding and hiding commitment is established by publishing the hash value to the blockchain. Given only the hash value it is infeasible to reconstruct the EV's decision, despite it being publicly available in the blockchain.

Note that this only holds if there is more than one bid for the request. For a single bid that is then chosen by the EV it is trivial to link the decision of the EV to this particular charging station.

In the *charging* phase, only the EV and the selected charging station are involved and communicate directly. Thus, no further data is published in the blockchain, assuring that only the EV and the selected charging station learn at which price energy is purchased. By opening the commitment, the EV reveals itself as the party with ID ζ. No other party can impersonate the latter with feasible effort due to the properties of the cryptographic hash function used for the binding commitment. This way, the charging station verifies that it is

communicating with the party that initiated the request for bids.

In summary, (i) none of the participants learns the exact position of the EV; (ii) no participant, except for the EV and the selected charging station, learn at which price energy is purchased (if there is more than one bid); and (iii) EVs cannot be tracked over time. Thus, in the proposed protocol, privacy is preserved for the EV.

4.2 Availability considerations

For the presented protocol, there are two possible behaviors for charging stations after the *bidding* phase. They can either (i) reserve the time slot exclusively for the requesting EV, regardless of whether or not the EV decides for this charging station; or (ii) send multiple bids for different requests for the same or for an overlapping time slot and accept the EV that arrives first.

In the first case, charging stations reserve the time slot exclusively and malicious participants could spam the protocol and the blockchain with requests and therefore effectively prevent an honest charging station from getting any customers. In order to prevent this kind of denial-of-service attack, a transaction fee can be charged for every request. Transaction fees or fees for the execution of smart contracts in the blockchain are applied by blockchain technologies for this purpose (e.g., *gas* in Ethereum [25]).

In the second case, where charging stations can bid multiple times for the same time slot, EVs are still guaranteed a certain price for a certain amount of energy in this timeframe at a particular charging station. However, the requested charging station might not be available. This is similarly reflected in the current situation where EVs approach any public charging station without prior knowledge of its availability.

In summary, while the proposed protocol protects the privacy of the customer, this comes at the cost of reduced utility. Either charging stations are not fully utilized or EVs are not guaranteed a time slot. However, providing any of these guarantees would limit the privacy of the EV.

4.3 Communication overhead

In this section we analyze the communication overhead of our proposed protocol. Due to the decentralized nature of the blockchain, the amount of data to be stored significantly impacts performance in practice [5]. Table 2 summarizes the amount of data that needs to be stored in the blockchain for each phase.

In the *exploration* phase (R, T, e) and ζ have to be stored in the blockchain. The unique ID ζ and the timestamp of the request are required to be stored by design as a feature of the blockchain (e.g., [1,25]), i.e., they are already included and therefore impose no overhead. The values T and e can be represented as two timestamps and an unsigned fixed-point integer, respectively. Due to the limited range of practically relevant values 2 bytes for each suffices. This allows for second-granularity for 3 weeks relative to the current point in time for the timestamps and approximately 650 kWh at a resolution of 10 Wh for the energy need.

Table 2 Summary of the communication overhead and data that needs to be stored in the blockchain per block in the proposed protocol

Phase	EV (bytes)	Charging station (bytes)
Exploration	8	–
Bidding	–	38
Evaluation	16	–
Charging	–	–

The specification of a region R is implementation-specific. For example, in the D–A–CH countries there are a total of 401 (Germany [7]), 117 (Austria [23]) and 148 (Switzerland [21]) districts ("Bezirke"). These districts can be numbered and represented by a 2 byte value. Using this example, in total, 8 bytes of data need to be stored in the blockchain in the *exploration* phase.

In the *bidding* phase, each bid consists of the values (T, e, ζ, b_i, w_i). As above, for T, e and w_i, 2 bytes each suffice. The bid b_i can be represented by 2 bytes, allowing for values up to approximately €650 at a resolution of €0.01. The ID ζ is a value of approximately 40 alpha-numeric characters[4] (which can be represented by 6 bits each, i.e., 30 bytes for the ID) and depending on the concrete blockchain technology (e.g., 20 bytes for Ethereum [25]). In total, one bid of a charging station imposes an overhead of 38 bytes. If N charging stations bid n times each, the total overhead is $38 \cdot N \cdot n$ bytes.

In the *evaluation* phase, a commitment is stored in the blockchain. Given SHA-256 as the cryptographic hash function, one hash, i.e., one commitment, requires 16 bytes to be stored. In the *charging* phase, no data is stored in the blockchain.

4.4 Blockchain design considerations

This section outlines the requirements for the blockchain infrastructure for the proposed protocol and discusses how these requirements are met by common blockchain technologies. For handling the protocol a blockchain with the following properties is required:

– *Data storage and transaction logic* The protocol neither requires to perform calculations in the blockchain

[4] https://github.com/bitcoin/bitcoin.

(such as smart contracts) nor to verify transactions itself. The blockchain only serves as a decentralized, immutable database that needs to store at most 38 bytes per transaction.
- *Transaction volume* For M EVs requesting an offer from N charging stations with n bids each, $2M + NMn$ transactions are sent.
- *Confirmation time* If a transaction requires c confirmations, the protocol must handle $\frac{(2M+NMn)c}{t}$ transactions per time slot t. The value of t depends on the period of time between requesting an offer and submitting the decision.
- *Transaction fees* In a public blockchain a small transaction fee can be charged to incentivize nodes to confirm transactions and to prevent the flooding of the network with invalid requests.

In the following, the requirements are discussed by example with the properties of well-established blockchains, such as Bitcoin [18], Ethereum [25] and Openchain.[5]

Bitcoin is a public blockchain which allows to store 80 bytes of additional data per transaction. In our proposed protocol, each transaction in each phase is strictly below this limit. For the Bitcoin protocol, a confirmation of one block takes 10 min on average [5]. The current recommendation is to wait for at least six blocks, i.e., 60 min.

Ethereum is a public blockchain that allows to perform Turing-complete calculations (smart contracts). While the proposed protocol could be realized as a smart contract, the ability to perform arbitrary calculations is not required. The Ethereum protocol has an average block time of 15 s and charges small transaction fees for the processing of smart contracts [25].

Both, Bitcoin and Ethereum have a proof-of-work based consensus algorithm. Openchain, by contrast, is a private blockchain that allows for almost instant transaction confirmations based on a proof-of-authority consensus algorithm. While the protocol can be realized with both, a public or private blockchain, for a private blockchain it is required that an authority manages participants and access permissions.

In summary, Bitcoin could be used, but the average block rate might be too low for our use case which needs to be analyzed in future work. Ethereum is more practical in this regard, but the overhead for smart contracts might be infeasible. Private blockchains, such as Openchain, pose little overhead and fast confirmations, but require a centralized authority.

All blockchain technologies meeting the above requirements can be used for the proposed protocol. In particular, Bitcoin and Ethereum seem a reasonable choice for a small number of EVs. Scaling this protocol to a larger number of EVs and investigating the confirmation time in detail remains future work.

[5] https://www.openchain.org/.

5 Conclusion

In this paper, a protocol for dynamic tariff decisions for electric vehicle charging has been presented. The protocol allows customers to find the cheapest charging station within a previous defined region and preserves the privacy of the electric vehicle. The customer's position is not revealed until the customer decides for a particular charging station and customers cannot be tracked over time. Different charging stations can send bids for tariffs based on the requested energy. A blockchain is used as a decentralized and immutable storage for transparency and verifiability of the bids. The protocol comes at little communication overhead (at most 38 bytes per block) and is therefore suitable to be used with existing blockchain technologies. Future work will focus on the scalability of the presented approach for a large number of electric vehicles with a high transaction volume and on handling the payment phase in the blockchain.

Acknowledgements Open access funding provided by FH Salzburg - University of Applied Sciences. The financial support by the Austrian Federal Ministry of Science, Research and Economy and the Austrian National Foundation for Research, Technology and Development is gratefully acknowledged. Funding by the Federal State of Salzburg is gratefully acknowledged.

References

1. Ben-Sasson E, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M (2014) Zerocash: decentralized anonymous payments from bitcoin. In: Proceedings—IEEE symposium on security and privacy. IEEE, pp 459–474. doi:10.1109/SP.2014.36
2. Borges F, Volk F, Mühlhäuser M (2015) Efficient, verifiable, secure, and privacy-friendly computations for the smart grid. In: PES conference on innovative smart grid technologies (ISGT). IEEE, Washington, DC
3. Chen D, Kalra S, Irwin D, Shenoy P, Albrecht J (2015) Preventing occupancy detection from smart meters. IEEE Trans Smart Grid 6(5):2426–2434. doi:10.1109/TSG.2015.2402224
4. Clarke R, Wigan M (2011) You are where you've been: the privacy implications of location and tracking technologies. J Locat Based Serv 5(3–4):138–155. doi:10.1080/17489725.2011.637969
5. Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Gün Sirer E, Song D, Wattenhofer R (2016) On scaling decentralized blockchains. In: Clark J, Meiklejohn S, Ryan PY, Wallach D, Brenner M, Rohloff K (eds) Financial cryptography and data security: FC 2016 international workshops, BITCOIN,

VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers. Springer, Berlin, pp 106–125. doi:10.1007/978-3-662-53357-4_8
6. Delmolino K, Arnett M, Kosba AE, Miller A, Shi E (2016) Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. In: Financial cryptography and data security. International Financial Cryptography Association, pp 79–94
7. DESTATIS Statistisches Bundesamt: Verwaltungsgliederung am 31.03.2017 (1. Quartal) (2017). https://www.destatis.de/DE/ZahlenFakten/LaenderRegionen/Regionales/Gemeindeverzeichnis/Administrativ/Archiv/Verwaltungsgliederung/Verwalt1QAktuell.html (Online). Accessed 21 April 2017
8. Dubois A, Wehenkel A, Fonteneau R, Olivier F, Ernst D (2017) An app-based algorithmic approach for harvesting local and renewable energy using electric vehicles. In: Proceedings of the 9th international conference on agents and artificial intelligence (ICAART 2017), Porto
9. Eibl G, Engel D (2015) Influence of data granularity on smart meter privacy. IEEE Trans Smart Grid 6(2):930–939. doi:10.1109/TSG.2014.2376613
10. Knirsch F (2017) Privacy enhancing technologies in the smart grid user domain. IT Inf Technol Themat Issue: Recent Trends Energy Inform Res 1(59):13–22
11. Knirsch F, Unterweger A, Eibl G, Engel D (2017) Privacy-preserving smart grid tariff decisions with blockchain-based smart contracts. In: Rivera W (ed) Sustainable cloud and energy services: principles and practices. Springer, Berlin
12. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C (2016) Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE symposium on security and privacy (SP). IEEE, pp 839–858
13. Langer L, Skopik F, Kienesberger G, Li Q (2013) Privacy issues of smart e-mobility. In: 39th annual conference of the ieee industrial electronics society, IECON 2013, pp 6682–6687. doi:10.1109/IECON.2013.6700238
14. Lisovich M, Mulligan D, Wicker S (2010) Inferring personal information from demand-response systems. IEEE Secur Priv 8(1):11–20. doi:10.1109/MSP.2010.40
15. Lisovich MA, Wicker SB (2008) Privacy concerns in upcoming residential and commercial demand-response systems. In: Clemson power systems conference
16. McKenna E, Richardson I, Thomson M (2012) Smart meter data: balancing consumer privacy concerns with legitimate applications. Energy Policy 41:807–814. doi:10.1016/j.enpol.2011.11.049
17. Mwasilu F, Justo JJ, Kim EK, Do TD, Jung JW (2014) Electric vehicles and smart grid interaction: a review on vehicle to grid and renewable energy sources integration. Renew Sustain Energy Rev 34:501–516. doi:10.1016/j.rser.2014.03.031
18. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system, pp 1–9. https://bitcoin.org/bitcoin.pdf
19. Pedersen TP (1992) Non-interactive and information-theoretic secure verifiable secret sharing. In: Advances in Cryptology—Crypto'91, vol 91, pp 129–140. doi:10.1007/3-540-46766-1_9
20. Reid F, Harrigan M (2013) An analysis of anonymity in the bitcoin system. In: Altshuler Y, Elovici Y, Cremers AB, Aharony N, Pentland A (eds) Security and privacy in social networks. Springer, New York, pp 197–223. doi:10.1007/978-1-4614-4139-7_10
21. Schweizerische Eidgenossenschaft—Bundesamt für Statistik: Die 148 Bezirke der Schweiz am 1.1.2013 (2017). https://www.bfs.admin.ch/bfs/de/home/statistiken/querschnittsthemen/raeumliche-analysen/raeumliche-gliederungen.assetdetail.466288.html (Online). Accessed 21 April 2017
22. Shokri R, Theodorakopoulos G, Le Boudec JY, Hubaux JP (2011) Quantifying location privacy. In: Proceedings—IEEE symposium on security and privacy, pp 247–262. doi:10.1109/SP.2011.18
23. Statistik Austria: Politische Bezirke (2017). https://www.statistik.at/web_de/klassifikationen/regionale_gliederungen/politische_bezirke/index.html (Online). Accessed 21 April 2017
24. Unterweger A, Knirsch F, Eibl G, Engel D (2016) Privacy-preserving load profile matching for tariff decisions in smart grids. EURASIP J Inf Secur 2016(1):1–17. doi:10.1186/s13635-016-0044-1
25. Wood G (2017) Ethereum: a secure decentralised generalised transaction ledger. Tech. rep., Ethereum. https://ethereum.github.io/yellowpaper/paper.pdf
26. Yilmaz M, Krein P (2013) Review of charging power levels and infrastructure for plug-in electric and hybrid vehicles and commentary on unidirectional charging. IEEE Trans Power Electron 28(5):2151–2169. doi:10.1109/IEVC.2012.6183208
27. Zyskind G, Nathan O, Pentland AS (2015) Decentralizing privacy: using blockchain to protect personal data. In: Proceedings—2015 IEEE security and privacy workshops, SPW 2015, pp 180–184. doi:10.1109/SPW.2015.27