Low-risk Privacy-preserving Electric Vehicle Charging with Payments

Andreas Unterweger, Fabian Knirsch, Clemens Brunner and, Dominik Engel
Center for Secure Energy Informatics, *Salzburg University of Applied Sciences*, Puch bei Hallein, Austria

***Abstract*—The increasing amount of electric vehicles and a growing electric vehicle ecosystem is becoming a highly heterogeneous environment with a large number of participants that interact and communicate. Finding a charging station, performing vehicle-to-vehicle charging or processing payments poses privacy threats to customers as their location and habits can be traced. In this paper, we present a privacy-preserving solution for grid-to-vehicle charging, vehicle-to-grid charging and vehicle-to-vehicle charging, that allows for finding the right charging option in a competitive market environment and that allows for built-in payments with adjustable and limited risk for both, producers and consumers of electricity. The proposed approach builds on blockchain technology and extends a state-of-the-art protocol with payments, while still preserving the privacy of the users. The protocol is evaluated with respect to privacy, risk and scalability. It is shown that pseudonymity and location privacy (against third parties) is guaranteed throughout the protocol, even beyond a single protocol session. In addition, both, risk and scalability can be adjusted based on the used blockchain.**

I. Introduction

Electric vehicles (EVs) are gaining widespread attention in both, academia and real-world implementation, see e.g., [7], [13], [14]. In order to meet the increasing demand, the widespread roll out of EVs also requires to establish a massive charging infrastructure, which also impacts the electricity grid in terms of demand and supply. In the context of heterogeneous market participants in *smart grids* and *local energy communities*, the finding of suitable charging stations and the payment processes are of particular importance. These processes are executed in an environment that is shaped by a large number of players and participants that do not necessarily trust each other to full extent and where the privacy of customers is crucial. Customer privacy can be impacted severely by allowing charging stations or other EVs to track the customer, to establish movement profiles and to learn customer habits [12].

EVs can either use the (public) electricity grid for charging and approach one of the charging stations available or EVs use another EV to charge. This leads to a dynamic and competitive market situation with volatile demand and supply. In order to simplify and optimize the process of finding a charging station, a number of protocols have been proposed [2], [11], [24]. These protocols often build on blockchain technology in order to have a public and immutable record for managing and ordering requests and offers. Furthermore, some protocols propose blockchain technology for handling the payment.

However, the proposed protocols often (i) do not cover customer privacy to a full extent; (ii) do not allow for combined bidding and payment transfer with limited risk for both, the EV and the charging station; and (iii) do not cover both, grid-to-vehicle and vehicle-to-vehicle charging.

Due to limited trust and anonymity in privacy-preserving systems, there is also a substantial financial risk for both, the EV (or the consumer in general) and the charging station (or the producer in general). While the EV runs the risk of paying without receiving a sufficient amount of energy (or any energy at all), the charging station runs the risk of providing energy and not receiving sufficient compensation. This is largely unaddressed in prior work.

Following a privacy-preserving protocol for grid-to-vehicle charging presented in [11], in this paper, we present a comprehensive protocol for EV charging with payments. The protocol preserves the privacy of all participants and the location privacy of the EVs during the exploration and bidding phase. Furthermore, pseudonymity is preserved during the charging phase and the payment phase, and a parameter is proposed which allows for controlling risk. Two different implementations for transferring installments in exchange for energy are described and evaluated. These implementations are compared in terms of risk, scalability, performance and privacy.

The rest of this paper is structured as follows: Section II describes EV charging, blockchain technology, hash time-locked contracts and state channels. Section III describes the proposed privacy-preserving protocol. Section IV evaluates the protocol with respect to risk, privacy and scalability. Section V provides an overview of related work. Section VI summarizes this paper.

II. Background

This section summarizes the relevant background for EV charging and blockchain technology.

A. Electric Vehicle Charging

One of the most common types of EVs relies on batteries which need to be recharged from an electric power source [15]. Depending on their capacity and usage, these batteries may retain significant portions of their initial charge over longer periods of time. Three different types of charging can be distinguished [15], [20]: (i) *G2V (Grid-to-Vehicle) Charging*: The EV is charged by the power grid. This is the most common case and is usually done via a charging station, see e.g., [15]

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021
21 February 2021
ISBN 1-891562-68-1
https://dx.doi.org/10.14722/autosec.2021.23001
www.ndss-symposium.org

(ii) *V2V (Vehicle-to-Vehicle) Charging*: As described in [20], EVs may also rely on other EV's batteries instead of charging stations to recharge; and (iii) *V2G (Vehicle-to-Grid) Charging*: Reversing the G2V process, the EV may also provide power to the power grid during peak hours [15]. Due to its properties, the EV can act as both, a consumer (G2V, V2V) and a producer (V2V, V2G). In this paper, all three types of charging are supported, despite existing standards, e.g., ISO 15118 [9] and OCPP [17], focusing on the V2G case. To the best of our knowledge, at the time of writing, no finalized standards for V2G and V2V exist.

B. Blockchain

A blockchain is a decentralized append-only database, initially presented by Bitcoin [16], to enable a chronologically ordered and practically tamper-proof log of financial transactions.

To interact with the decentralized database, signed transactions are used as write requests. *Blockchain nodes*, which are responsible to find a consensus [1] for the global state, group multiple transactions together and create a new block, which is cryptographically linked to the previous block. The index of the block is denoted as block height. Users in a blockchain are represented by public-private key pairs. The ID of a user is the public key or the hash of the public key and it is possible to use a new ID for each transaction. Blockchains are often used as a decentralized programmable service. Additionally, blockchains enable programmable and conditional payments, which require that predefined constrains are met before the payment is considered valid. Conditional payments in Bitcoin are enabled by a scripting language [1] with limited functionality. In contrast to Ethereum, [22], where a Turing complete language, e.g., Solidity, [2] allows for the creation of smart contracts where any condition for payments can be implemented.

1) HTLCs: Hash Time Locked Contracts (HTLCs) are conditional payments, supported by both, the Bitcoin scripting language and by smart contracts. They consist of a hash and a time lock and are mostly used to allow for off-chain payments over multiple untrusted hops [8], [18] as well as other applications [6]. A transaction that transfers x coins from A to B, secured with a HTLC can be represented by the function $HTLC(A, B, x, y, t)$ [5]. To create this HTLC, A needs to create a random number r with $y = H(r)$ and specify t, which is the time (maximum block number) where the transaction can be spent by B. To unlock the $HTLC$, B need to publicly disclose (cryptographically proof) the knowledge of r via a blockchain transaction within the period defined in t. If B does not provide the necessary information to unlock the transaction, A gets back the control over x coins and can spend them again. $HTLC$ can also be time-bounded commitment schemes with additional payment functionalities. The random value r used to open the hash lock can be replaced by a commitment value of A.

2) State-Channels: An alternative to HTLCs is the use of state channels. They can be implemented in blockchains with support for Turing complete smart contracts, such as Ethereum [22]. The purpose of a state-channels is to reduce the number of on-chain transactions by enabling an off-chain negotiation of a locked portion of a global blockchain state. For this, a state-channel uses three steps: (i) opening; (ii) off-chain state modifications; and (iii) closing. In the opening step, a predefined set of participants p lock a collateral by sending a single on-chain transaction to a previously deployed smart contract. Once all participants locked a state, the off-chain state modification starts. In this step, all participants need to exchange signed off-chain messages, in which the new distribution of the locked state is defined. The new off-chain state is considered valid if signatures of all participants have been collected. The negotiation can be repeated as often as needed. In the last step, the state channel will be closed by using an signed off-chain state and the new distribution of the locked collateral will be send back to the participants. A detailed description of state-channels and off-chain solutions can be found in [8] and a comparison of use cases for state-channels in the energy domain is summarized in [4].

In order to create and use a state-channel with n participants, n on-chain transactions are needed to lock the collateral for all participants. In addition, for deploying the smart contract and for closing the state channel two additional transactions are required.

For the protocol proposed in this paper, we use the blockchain to publicly store and timestamp small amounts of data and to enable conditional payments for the consumed electricity.

III. Electric Vehicle Charging with Payments

This section describes the proposed EV charging protocol and its separate phases. The protocol builds upon [11], but includes a built-in payment phase. Furthermore, it generalizes the role of the EV as it can act as both, a producer and a consumer, as described in Section II-A. Thus, as opposed to [11], where the EV is always assumed to be a consumer, the proposed protocol uses the notion of *producers* for entities who offer electrical power and *consumers* for entities who require it. The EV may be either or both, at the same time, depending on the use case.

For the description of the phases of the protocol the structure and notation of [11] are retained. Figure 1 provides an overview of the phases in the protocol and shows the operations by the actors and the exchanged messages.

ζ denotes the unique ID of a consumer looking to acquire (charge) an energy amount $e \in \mathbb{Q}^+ \backslash \{0\}$, e.g., 20 kWh, within a specified time interval $T \in \mathcal{P}(\mathbb{T})$, e.g., between 12 p.m. and 2 p.m., within a certain geographical (world) region $R \in \mathcal{P}(\mathbb{W})$, e.g., the city of Salzburg, Austria. Similarly, i denotes the unique ID of a producer at a location $w_i \in \mathbb{W}$. Both, the unique ID of a consumer and a producer are represented by blockchain ID. While the protocol is expressed from the point of view of one consumer ζ, there can be arbitrarily many producers, each denoted with an index i equal to its ID.

A. Exploration

In order to find producers who can offer the required energy amount e within the time interval T in the region

[1] https://en.bitcoin.it/wiki/Script [Last access: April, 2020]

[2] https://solidity.readthedocs.io/en/latest/ [Last access: April,2020]

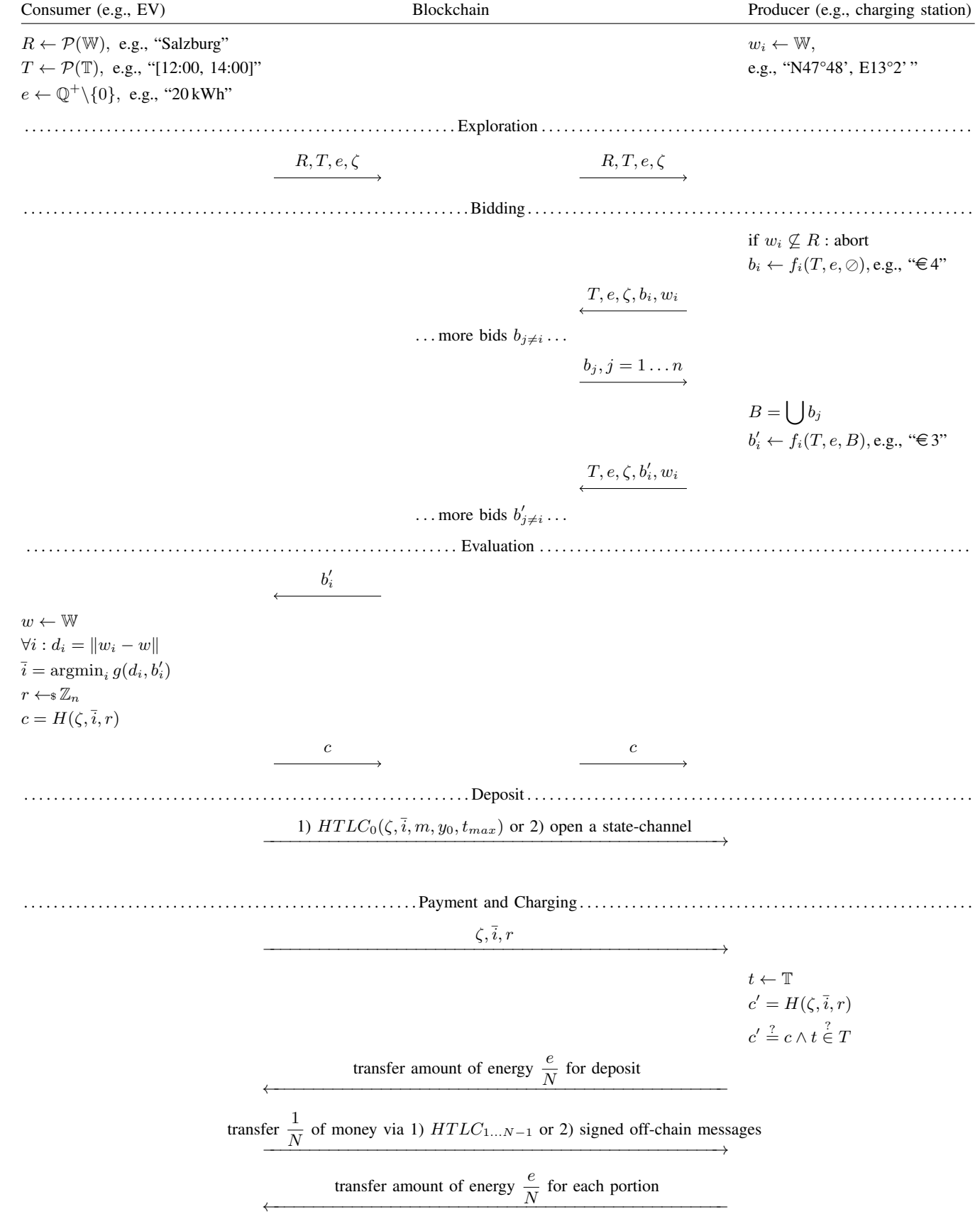

Fig. 1. This diagram shows the phases of our proposed protocol and the protocol presented in [11]. In the deposit phase either 1) HTLCs or 2 state channels can be used. Messages are exchanged between a consumer, a blockchain and a producer.

R, a consumer posts its ID ζ, together with the aforementioned required parameters on the blockchain. The request (R, T, e, ζ) is visible to all actors in the network and allows all producers to subsequently prepare bids.

B. Bidding

After a request has been placed, all actors who can provide energy within the specified region R (producers) can post prices for the desired time interval T and energy amount e on the blockchain, considering an actor-specific price-computing function $f_i(T, e, \oslash)$. The bid $b_i = f_i(T, e, \oslash)$ is the initial offer of producer i, which may also be an EV. Producers may act upon observing other actors' bids b_j and, in turn, update their own bid, b_i to b_i'. To do so, they consider the other bids in their actor-specific price-computing function f_i so that the new bid $b_i' = f_i(T, e, \cup_j b_j)$ considers the existing parameters as well as the other actors' bids b_j.

C. Evaluation

After either a certain number of bids has been observed or a time limit has passed, the consumer collects all bids and computes the best one using its decision function $g(d, b)$ that is based on the distance d to each producer and the bidding price b that this producer offers, i.e., the consumer chooses the desired producer $\bar{i} = \text{argmin}_i\, g(d_i, b_i')$, where $d_i := ||w_i - w||$ is the geographical distance between the consumer and the producer i and b_i' is the most recent bid of producer i. Once the consumer has decided to use the producer $\bar{i}$, it commits to this producer, its bid $b_{\bar{i}}'$ and the time interval.

D. Deposit

In order to communicate the decision for producer i and time interval T, the consumer creates a commitment for a payment in N installments in order to reduce the risk on both sides. In order to implement the installments on a blockchain, the payment can either be split up into a total of N HTLCs or alternatively a state channel is created. Instead of submitting the full payment of $b_{\bar{i}}'$ at once, one N-th is used as a deposit in both cases.

1) HTLCs: For HTLCS, initially, an $HTLC_0(\zeta, \bar{i}, m, y_0, t_{max})$ is created, where the sender is ζ, the receiver is $\bar{i}$, m is the amount of money to be locked and $y_0 = H(r_0)$ is created with a fresh random number r_0. t_{max} is chosen by the consumer with respect to the charging time interval so that this value lies before the beginning of the charging period, i.e., $t_{max} < \min(T)$. The monetary amount $m := \frac{b_{\bar{i}}'}{N}$ is one N-th of the agreed-upon price. The HTLC guarantees that only the consumer ζ (who knows r_0) can reveal itself and the payment, at the producer. To activate the initial payment and to unlock the deposit from $HTLC_0$, the producer needs to know r_0, the pre-image of y_0, which is communicated from the consumer to the producer before the charging process can start. If r_0 is not revealed or if it is revealed too late, the charging process cannot begin.

2) State Channel: Alternatively, for state channels, the total amount $\bar{i}$ is locked as collateral by the consumer. The initial state of the channel is defined, so that one N-th of the amount belongs to the producer and the remaining amount is used for off-chain transfers during the payment and charging phase.

E. Payment and Charging

During payment and charging the risk for both, consumer and producer is minimized by continuously transferring fractions of the payment for exchange of energy. More precisely, after each transfer one N-th of the total energy e, one N-th of the payment is released. If either the consumer or the producer violate the protocol, e.g., by not confirming the charge and withholding the next installment, the charging process can be aborted with a maximum remaining loss of $\frac{e}{N}$ in energy and m in funds.

1) HTLCs: When using HTLCs, once the producer has received r_0 and thus the deposit, the charging process can start. After having received $\frac{e}{N}$, i.e., one N-th of the agreed-upon charge, the consumer confirms the receipt and reveals r_1 to unlock the next fraction of the payment through $HTLC_1$. This process continues for every fraction of energy $\frac{e}{N}$ received until charging is completed, i.e., the N-th HTLC, $HTLC_{N-1}$, is opened and the full amount e has been charged.

2) State Channel: When using state channels, all intermediate states are handled off-chain. After having received $\frac{e}{N}$, i.e., one N-th of the agreed-upon charge, the state is updated, so that another N-th of the collateral is assigned to the producer. Both, the producer and the consumer need to sign this state change off-chain. After exchanging the last N-th of energy, one final on-chain transaction is required to lock the last agreed-upon state on the blockchain.

IV. Evaluation

In this section, we evaluate our proposed protocol with respect to risk, scalability, performance and privacy.

A. Risk

Since this protocol is about a financial transaction in exchange for a good, i.e., electricity, there is a risk of not receiving either the good or the money. In different phases of the protocol the risk is with different entities.

If the full amount of money is paid upon reserving a charging slot at the producer, the risk of not receiving energy is with the consumer. Conversely, if the payment happens after receiving the energy, the risk of not receiving any money for the provided energy is with the producer. In order to minimize the risk for both, the producer and the consumer, the payment is split into a total of N fragments. A fraction of $\frac{1}{N}$ of the total amount $b_{\bar{i}}'$ is reserved as a deposit upon reservation via either an HTLC or a state channel. If the producer ceases communication fraudulently, the loss is limited to $\frac{1}{N}$ on the consumer side. While the producer suffers no damage, a scoring system can be used to mark the producer as non-trustworthy for future consumers [2]. If, on the other hand, the consumer does not show up for charging, the lost time of the producer is compensated by the deposit of $\frac{1}{N}$.

After the charging process is started successfully and a fraction of $\frac{1}{N}$ of the total amount to be charged e has been transferred from the producer to the consumer, the risk on both sides is zero. The consumer has received what he paid for and the producer has provided not more than he has been paid. For the next fraction $\frac{1}{N}$ of the payment and energy, the same risk distribution applies: While there is a maximum risk of $\frac{1}{N}$ of

the total amount with the consumer directly after payment, the risk goes to zero for the producer and the consumer after the corresponding fraction of energy has been transferred. This repeats for the remaining fractions, but limits the risk with $\frac{1}{N}$ at any time. For small values of N, the risk is relatively large, while higher values of N reduce and limit the risk. However, in case of HTLCs, a larger number of N requires more HTLCs and therefore more transactions, which impact scalability.

B. Scalability

In case of HTLCs, the number of blockchain transactions is proportional to N, and the charging process is limited by the reserved time interval T. Thus, the number of transactions per second is proportional to $\frac{N}{||T||}$ (where $||T||$ denotes the length of the time interval). For example, a charging time of 10 minutes in two installments requires less than one transaction per minute. Conversely, a charging time of one hour in 100 installments, more than 3 transactions per second are required. The number of transactions per second is limited by the blockchain design and varies greatly [1]. It is thus crucial to select a blockchain with sufficient throughput, especially considering that multiple charging sessions may be ongoing at the same time. Any practical implementation of the protocol must therefore find reasonable bounds for (i) the number of installments N; (ii) the length of charging intervals T; and (iii) the number of concurrent charging sessions in a given blockchain.

However, when using state channels instead of HTLCs, only four on-chain transactions are required, one for deploying, two for opening the state channel and one for closing it. Since all other transactions are performed off-chain, the number of transaction on-chain are independent of the number of installments N.

C. Performance

From a producer and consumer perspective, the guarantees and results of both, HTLCs and state channels, are the same. However, in terms of performance, the two implementations vary significantly.

Table I summarizes the key performance metrics of the proposed protocol as described in the sections above. First, the risk for producer and consumer is the same for both, HTLCs and state channels (see Section IV-A). Second, the required number of on-chain transactions is dependent on N for HTLCs and limited to four for state channels (see IV-B). Conversely, HTLCs do not require off-chain transactions, whereas a state channel requires $N-1$ updates off-chain until the full deposit belongs to the producer. Third, the scalability of the blockchain in terms of transactions per second, is proportional to the number of on-chain transactions. Note that the costs for on-chain transactions are proportional to the number and speed in which they need to be processes. Thus, for high values of N and the corresponding low risk, HTLC transactions are expected to be impracticably expensive (e.g., splitting a ten Dollar payment into $N = 10$ installments with transaction costs of one Dollar each, would incur transaction costs as high as the energy costs [21]). In contrast, state channels avoid this issue and require a constant amount and therefore constant costs.

TABLE I. PERFORMANCE COMPARISON OF HTLCS AND STATE CHANNELS.

	HTLC	**State Channel**
Number of on-chain transactions	N	4
Number of off-chain transactions	0	$N-1$
Required blockchain scalability	$\frac{N}{\|\|T\|\|}$	$\frac{4}{\|\|T\|\|}$
Maximum consumer risk	$\frac{b^I_i}{N}$	$\frac{b^I_i}{N}$
Maximum producer risk	0	0

D. Privacy

The proposed protocol is designed to preserve the privacy of both, the consumer and the producer. The location privacy of the consumer and producer is preserved during the bidding phase and pseudonymity is preserved during the charging phase and the payment phase. While, for the charging process itself, the consumer has to approach a producer, the location of either participant is neither revealed to each other nor to third parties before the charging process and as long as no contract is established. Within the blockchain, each participant is identified with a unique ID. This ID can be changed after each protocol run to preserve privacy. Each new ID is a pseudonym of the participant. Thus, pseudonymity is preserved [19].

V. RELATED WORK

Related work in the area of e-mobility is roughly clustered in the following areas: (i) blockchain-based approaches, having the focus on a decentralized approach for finding charging stations or for handling payments; (ii) approaches that primarily focus on privacy-preservation; and (iii) protocols that discuss similar use cases, such as ride sharing, but attempt to provide comparable guarantees for privacy.

In [2], a privacy-preserving ride sharing protocol based on a blockchain is presented. The proposed protocol uses zero knowledge proofs and is evaluated in an Ethereum test net. This protocol provides similar privacy guarantees with respect to location privacy and the protocol implements a pay-as-you-go service where the driver proofs the elapsed distance in order to get paid. In contrast, our approach uses HTLCs in order to spread payments over a longer period of time and we propose a risk-limiting variable for balancing risk and costs. This allows for high flexibility in various practical settings and is widely blockchain independent.

While our proposed protocol allows individual consumers, e.g., EVs, to find a producer, e.g., a charging station, individually, approaches exist in literature which aim at optimizing more globally given multiple charging requests [3], [23]. However, these protocols do not allow for individual decisions and introduce a waiting time until the optimized solution is computed. [23] supports V2V charging with these limitations via a distributed optimization process. [3] uses such a process – on the basis of a blockchain – not for EV charging, but for the use case of privacy-preserving energy storage unit charging.

In [10], an approach similar to ours is proposed, but privacy aspects are not considered as they remain future work. In contrast, the protocol in our paper is designed with strong

guarantees for location privacy and identity. Furthermore, the risk for the producer and the consumer is fixed in [10], i.e., it cannot be changed. In contrast, our proposed approach allows for flexible distribution of risk with a risk parameter.

In [24], privacy additions to ISO 15118 and other common standards for EV charging are analyzed and it is found that this is not possible in a fully privacy-preserving way. The authors propose their own protocol to mitigate this, but they require pre-installed trusted platform modules (TPMs) in the EVs, which puts the required trust to the entities manufacturing these TPMs. In contrast, our approach is blockchain based, which means that the trust is distributed among all actors, minimizing single points of failure in a security sense.

VI. Conclusion

In this paper we present a protocol for privacy-preserving charging of EVs with payments, supporting vehicle-to-grid, grid-to-vehicle and vehicle-to-vehicle configurations. It has been demonstrated that the proposed protocol preserves pseudonymity and location privacy. Furthermore, the scalability and risk of both, the producer and the consumer, have been evaluated. A novel risk parameter has been shown to allow for adjusting the trade-off between risk and scalability. The performance has been evaluated for two implementation variations, HTLCs and state channels. It is found that state channels are better-suited to implement risk-minimized charging due to its lower number of on-chain transactions and thus practical costs.

VII. Acknowledgment

The financial support by the Federal State of Salzburg is gratefully acknowledged.

References

[1] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Consensus in the Age of Blockchains," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. New York, NY, USA: ACM, 2019, pp. 183–198. [Online]. Available: http://arxiv.org/abs/1711.03936

[2] M. Baza, N. Lasla, M. M. Mahmoud, G. Srivastava, and M. Abdallah, "B-Ride: Ride Sharing with Privacy-preservation, Trust and Fair Payment atop Public Blockchain," *IEEE Transactions on Network Science and Engineering*, pp. 1–16, 2019.

[3] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. Ashiqur Rahman, "Blockchain-based charging coordination mechanism for smart grid energy storage units," in *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*. Atlanta, USA: IEEE, 2019, pp. 504–509.

[4] C. Brunner, A. Madhusudan, D. Engel, and B. Preneel, "Off-chain state channels in the energy domain," in *Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. Washington, DC, USA: IEEE, 2021.

[5] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," in *Symposium on Stabilization, Safety, and Security of Distributed Systems*, vol. 9212. Edmonton, AB, Canada: Springer, Cham, 2015, pp. 3–18.

[6] A. Deshpande and M. Herlihy, "Privacy-Preserving Cross-Chain Atomic Swaps," in *4th Workshop on Trusted Smart Contracts (WTSC'20) in Association with Financial Cryptography 20 (FC 2020)*, C. Springer, Ed., Kota Kinabalu, Sabah, Malaysia, 2020.

[7] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks," *IEEE Network*, vol. 32, no. 6, pp. 184–192, nov 2018.

[8] L. Gudgeon, P. Moreno-sanchez, S. Roos, P. Mccorry, and A. Gervais, "SoK: Layer-Two Blockchain Protocols," in *Financial Cryptography and Data Security*. Kota Kinabalu, Sabah, Malaysia: Springer, 2020.

[9] International Standardization Organization, "Road vehicles — Vehicle to grid communication interface (ISO 15118)," 2019.

[10] B. Kirpes and C. Becker, "Processing electric vehicle charging transactions in a blockchain-based information system," in *Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018*, 2018, pp. 1–5.

[11] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving Blockchain-based Electric Vehicle Charging with Dynamic Tariff Decisions," *Journal on Computer Science - Research and Development (CSRD)*, vol. 33, no. 1, pp. 71–79, 2018.

[12] L. Langer, F. Skopik, G. Kienesberger, and Q. Li, "Privacy Issues of Smart E-Mobility," in *39th Annual Conference of the IEEE Industrial Electronics Society, IECON 2013*. Vienna, Austria: IEEE, 2013, pp. 6682–6687.

[13] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive Blockchain-Based Electric Vehicle Participation Scheme in Smart Grid Platform," *IEEE Access*, vol. 6, pp. 25 657–25 665, 2018.

[14] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "Roaming electric vehicle charging and billing: An anonymous multi-user protocol," in *2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014*. Venice, Italy: Institute of Electrical and Electronics Engineers Inc., jan 2015, pp. 939–945.

[15] F. Mwasilu, J. J. Justo, E. K. Kim, T. D. Do, and J. W. Jung, "Electric vehicles and smart grid interaction: A review on vehicle to grid and renewable energy sources integration," *Renewable and Sustainable Energy Reviews*, vol. 34, pp. 501–516, 2014.

[16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Tech. Rep., 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[17] Open Charge Alliance, "Open Charge Point Protocol (OCPP) 2.0.1," 2020.

[18] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," Tech. Rep. 0, 2016. [Online]. Available: https://lightning.network/lightning-network-paper.pdf

[19] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," in *Security and Privacy in Social Networks*, Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, and A. Pentland, Eds. New York: Springer New York, 2013, pp. 197–223.

[20] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. C. Tian, and N. Zhang, "A Secure Charging Scheme for Electric Vehicles with Smart Communities in Energy Blockchain," *IEEE Internet of Things Journal*, 2018.

[21] A. Unterweger, F. Knirsch, C. Leixnering, and D. Engel, "Lessons Learned from Implementing a Privacy-Preserving Smart Contract in Ethereum," in *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. Paris, France: IEEE, 2018, pp. 1–5.

[22] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum, Tech. Rep., 2017. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[23] F. Yucel, K. Akkaya, and E. Bulut, "Efficient and privacy preserving supplier matching for electric vehicle charging," *Ad Hoc Networks*, vol. 90, p. 101730, 2019. [Online]. Available: https://doi.org/10.1016/j.adhoc.2018.07.029

[24] D. Zelle, M. Springer, M. Zhdanova, and C. Krauß, "Anonymous charging and billing of electric vehicles," *ARES 2018*, 2018.