to appear in The International Conference on Blockchain (Blockchain-2018)

Building a Private Bitcoin-based Payment Network among Electric Vehicles and Charging Stations

Enes Erdin*, Mumin Cebe*, Kemal Akkaya*, Senay Solak†, Eyuphan Bulut‡ and Selcuk Uluagac*
*Florida International University, Miami, Florida
Email: {eerdi001, mcebe, kakkaya, suluagac}@fiu.edu
†University of Massachusetts Amherst, Amherst, Massachusetts
Email: solak@isenberg.umass.edu
‡Virginia Commonwealth University, Richmond, Virginia
Email: ebulut@vcu.edu

***Abstract*—Mass penetration and market dominance of Electric Vehicles (EVs) are expected in the upcoming years. Due to their frequent charging needs, not only public and private charging stations are being built, but also V2V charging options are considered. This forms a charging network with various suppliers and EV customers which can communicate to schedule charging operations. While an app can be designed to develop matching algorithms for charging schedules, the system also needs a convenient payment method that will enable privacy-preserving transactions among the suppliers and EVs. In this paper, we adopt a Bitcoin-based payment system for the EV charging network payments. However, Bitcoin has a transaction fee which would be comparable to the price of the charging service most of the time and thus may not be attractive to users. High transaction fees can be eliminated by building a payment network in parallel to main ledger, with permission and signatures. In this paper, we design and implement such a network among charging stations and mobile EVs with flow, connectivity and fairness constraints, and demonstrate results for the feasibility of the scheme under different circumstances. More specifically, we propose a payment network optimization model for determining payment channels among charging stations. We present numerical results on the characteristics of the network model by using realistic use cases.**

***Index Terms*—Vehicular Networks, Electric Vehicles, Charging, Vehicle-to-Grid Communication, Blockchain, Bitcoin, Payment Network**

I. Introduction

The popularity of electric vehicles (EVs) has been increasing since they can transform the modern transportation and energy systems with a reduced foreign-oil dependence and improved urban air quality. They can promote adoption of intermittent renewable energy sources by acting as energy storage systems [1] during the periods of strong wind or sun [2]. EVs can also help in realizing the foundation of smart cities of the future by injecting energy to the grid during periods of reduced production to balance demand. Due to such potential, many automotive companies have rolled out EVs as part of their product lines [3], [4].As a result, mass penetration and market dominance of EVs are expected in the upcoming years, particularly with reduced production costs.

One major issue with EVs is access to charging facilities. Currently, there are about 50,000 charging outlets (public and private) operating in the US [5]. Since a disruptive increase in number of EVs is imminent (15 million by 2030 [6]), there is an ongoing effort to expand the charging options for the users. For example, EV owners open their residential charging stations to other EV owners and share them through several charging network web sites such as PlugShare [7]. Similarly, Vehicle-to-Vehicle (V2V) charge sharing based solutions [8]–[10] are proposed recently to encourage EV owners with excessive charge share their charge with other EV owners in need. There are V2V charging products (e.g., Orca Inceptive [11] by Andromeda Power) in the market today and used by EV owners for charge sharing.

Another issue is the frequent charging needs, as opposed to fossil-fuel based vehicles, due to the short driving ranges of electric vehicles (e.g., 37 to 335 miles [12]). As charging takes much more time compared to getting gas, charging operations should be scheduled in advance by making appointments with charging stations. Considering the public and private charging stations as well as the EV owners which may act as V2V charging stations, this forms a large-scale charging network among EV users and charging stations that need to interact with each other.

However, frequent charging poses several privacy issues for the EV owners. The problem stems from the very nature of charging. It exposes the charging times and the amount of energy EV charges each time [13]. Long-term analysis of this charging information may expose user's driving patterns and whereabouts that can be used by marketers to send the driver appropriate ads. These privacy threats may hinder the successful large-scale penetration of EVs in the market as users see privacy as an important issue when using technology [14]. Thus, new EV charging approaches that should hide or limit the aforementioned location and charging information are needed to ensure that this new technology will not be misused to violate users' privacy.

While a number of approaches have been proposed recently to address privacy issues in EV charging [15]–[18], they lack the following aspects: 1) the approaches do not consider the payment problem as a privacy issue and thus, regardless of the efforts for charging privacy, the credit card like payments still leak location privacy to other parties; and 2) they are geared mostly for charging on the grid and within a single charging

provider without integrating recent solutions based on V2V [8]–[10], [19] or residential charging under a more comprehensive model which will raise additional privacy challenges due to increased exposure.

Considering the above privacy issues, we would like to build an independent payment system which will not be using credit cards or PayPal like systems. To this end, integration with one of the digital currencies would be the best option due to allowing anonymous peer-to-peer payments. Among many options, *Bitcoin* is the most mature and suitable one due to its widespread use as an alternative monetary system. For example, Expedia, Newegg and Overstock already use Bitcoin. However, Bitcoin suffers from slow confirmation and high transaction fees. The confirmation of a transaction can take hours, which may not be acceptable for EV owners or charging stations. Moreover, the transaction fee is too high for EV energy trade, because a typical charging cost may be between $3 and $12 [20] and paying considerable amount of transaction fee for such a cost will not be reasonable [21].

To overcome the challenges of high transaction fees and slow confirmation times, Bitcoin recently introduced a concept called *off-chain* payments [22], [23]. The idea behind *off-chain* is similar to creating an escrow account between two parties who can make multiple transactions without writing into Blockchain. As long as this off-chain channel is open, there will be no transaction fees charged. The only fees needed will be when opening and closing the off-chain channel. In addition, the transaction confirmation will be much faster.

This paper investigates incorporating the off-chain model into charging networks by building off-chain channels among charging providers. Our objective is to build an overlay distributed payment network where EV owners can make their payments through pre-established off-chain channels without any on-chain transaction cost and significant transaction confirmation times.

Nevertheless, there are several challenges in building such an overlay network. First of all, the topology of the resultant network is very crucial. The topology should not be like a hub-and-spoke model as in the current Internet backbone. This is not only detrimental to the privacy of the payments but can also create a monopoly where certain nodes may eventually would like to charge additional transfer fees. Similarly, hub or star like models as in the case of current credit card payment models are not desirable either for the same reasons. Instead, the topology should be purely peer-to-peer (P2P) and strive to distribute the off-chain channels to many pairs in order to reduce total transaction fees and increase the privacy of EV owners.

This paper aims to address the aforementioned issues by creating desirable topologies among charging stations. Specifically, we formulate this network design problem as a multi-commodity flow problem where establishment of payment channels between charging stations are optimized according to different cost-sharing scenarios among parties, while also ensuring the correct routing of the payments. The experimental results show that the proposed model can provide a cost-efficient decentralized payment network formation between parties.

The main contributions of this paper are:

- To the best of our knowledge, this is the first work to study the network design formulation of an overlay payment network. We present network optimization models that focus on the optimal assignment of payment channels among charging stations while taking into account accurate payment routing.
- We also study cost-sharing issues in a payment network and present formulas that tackle this issue to form a P2P payment network. This effort contributes to the realization of the decentralized payment channel networks.

The rest of the paper is organized as follows: Section II summarizes the related work. Section III provides the necessary background on Bitcoin, the off-chain mechanism, and defines the motivation of the problem through an attack model. Section IV is dedicated to the description of the proposed optimization model. We provide numerical results and discussion in Section V. Finally, in Section VI we conclude the paper by highlighting some future extensions.

II. Related Work

A number of approaches have been proposed recently to resolve these privacy issues during charging [15]–[18], [24], [25]. However, none of them addresses the privacy exposure during payment. Their focus is to hide user ID, location, schedule, etc. when this information is exchanged among EVs and charging stations. Our work in this paper is not in this category.

There are also several efforts in both industry and academic community to build payment channel network (PCN). These efforts can be classified in two categories. The first category relies on building PCN for intra-blockchain operations. One example study in this category is Lightning Network [22]. It allows transferring Bitcoin between parties over already existing off-chain link without any confirmation delay and transaction fee. The similar idea is followed by Raiden to build PCN for Ethereum [23]. The second category of works relies on building inter-blockchain operations to allow transfers between different cryptocurrencies without expensive on-chain confirmation. Examples include Inter-Ledger [26] and Atomic-CrossChain [27]. Existing PCNs are still in infant phase and therefore there are privacy challenges in routing of the payment. Blockchain community has started offer solutions to resolve privacy problem in PCN [28], [29]. However, all these studies design privacy-preserving routing solutions by assuming the availability of a perfect decentralized P2P PCN topology. None of these studies investigated the problem of network formation and its effects on privacy. In addition, the community of PCN assumes that there is already a trade between individual pairs and they allow other parties to use their channels via incentives such as *forwarding fees*. In our case, we investigate the problem of overlay network formation among these members so that they can share the channel

creation costs fairly and thus eventually there will be no forwarding fees needed.

III. Background and Preliminaries

A. Bitcoin and Off-Chain Mechanism

There are numerous cryptocurrencies on the market utilizing Blockchain technologies. Most of these digital currencies provide anonymity based on pseudonym addresses. Monero and Zcash, for instance, provide perfect anonymity by employing mixing and zero-knowledge proofs, respectively. However, they are not widely adopted. Currently, Bitcoin is the most widely used digital currency and its market cap is above 80% among all digital currencies. Thus, in this paper, we opt to choose Bitcoin to integrate to our payment service for EV charging as described in the paragraphs below.

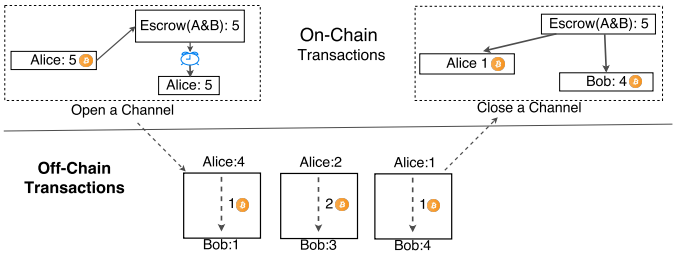

Fig. 1: Off-chain mechanism between two Blockchain nodes

Two important characteristics of Bitcoin are: 1) it is completely public and does not need a trusted authority during exchanges and; 2) it prevents double spending by keeping a public history of transactions. However, the confirmation of a transaction by a trader can take hours. Moreover, the transaction fee is too high, particularly for EV energy trade where payments will be much less.

To address these issues, Bitcoin introduced the *off-chain* mechanism [30], [31] that can significantly reduce transactions fees. The *off-chain* mechanism, which is also known as a transaction channel, allows to perform multiple direct P2P payments between two parties without committing every transaction to the Bitcoin shared ledger (i.e., on-chain) as shown in Fig. 1. An EV can create a unidirectional off-chain channel towards a charging supplier and can make payments until the capacity of this channel is reached without paying any Bitcoin transaction fee.

We explain the details of this scheme through the example scenario illustrated in Fig. 1. Alice opens a signed off-chain channel by instantiating an escrow account with Bob, and deposits 5 Bitcoins to the escrow account by performing an on-chain transaction. That determines the channel capacity as 5 Bitcoins. In the figure, we see 3 transactions in time, 1, 2, and 1 Bitcoins. Eventually, when the channel is closed, remaining 1 Bitcoin and transferred 4 Bitcoins are committed respectively to Alice and Bob, and written to Blockchain. Note that the payment channel provides guarantees to Alice and Bob to refund the balance in escrow account at any time or at a mutually agreed channel expiration time. These off-chain payments do not have any associated transaction fees. The only transaction fee charged for this operation will be while opening the channel and closing it. Although, the illustrated payment channel is unidirectional, it could be bi-directional.

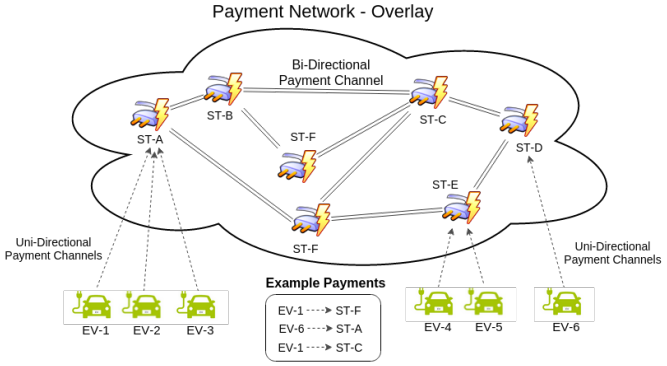

Fig. 2: An overview of the envisioned Payment Channel Network (PCN) for EV charging.

Note that secure protocol implementation for off-chain transactions is beyond the scope of this paper. We assume that an already established protocol is utilized in our study.

B. Problem Motivation and Definition

The main motivation of our problem is to minimize the transaction fees in Bitcoin payments, and eliminate the long waiting times for transaction verifications. We propose to utilize the off-chain idea to create payment channels among the suppliers assuming that every node in this network will create in-advance payment channels with some other nodes. Fig. 2 shows an overview of the proposed Payment Channel Network (PCN) with all components. If there exists a channel/link among every charging supplier, then a customer can utilize one or more of these links (i.e., multi-hop links) to reach another supplier for making a payment without paying any transaction fee while also maintaining its privacy. For instance, in Fig. 2, the EV-1 can be charged in ST-C but the payment can be made via ST-A, ST-B (e.g., EV-1, ST-A, ST-B, ST-C) in 3-hops using the payment channels already established.

The accomplishment of a payment between EV-1 and ST-C can be considered as Internet packet forwarding, and depends on the availability of a connecting path between pairs and sufficient capacity on each channel along the path. The intermediary nodes (e.g., ST-A and ST-B) work as a router and are not directly involved in the payment between the payer and the payee.

Based on these discussions, our problem can be formally defined as follows: "*Let us assume M charging suppliers some of which can be mobile, and N EV owners in a local region such as South Florida and a set of charging suppliers available to each EV. Let us also assume a PCN can be represented as a graph $G = (V, E)$, where V represents Bitcoin accounts and E represents payment channels. In our case, the set V of vertices represents the M charging stations and the set E represents the created payment channels among M charging stations and N EVs. Every edge between charging stations has a capacity u that denotes the amount of depositable Bitcoins.*

Every vertex $v \in V$ has an associated total-capacity C that denotes the upper bound of forwarded Bitcoins over it. Based on these inputs, how can we create a virtual topology PCN among the charging suppliers in such a way that 1) the average transaction fee for an EV will be minimized; 2) the total investment made by a station for creating channels with its neighbors (i.e., the cost related to the cration of capacity u) will be minimized; and 3) the privacy of EV owners will be preserved."

There are at least three challenges in designing such an overlay PCN. First, while the payments are enroute to the supplier, the source and destination address along with the payment amount will be in cleartext which may cause privacy leaks by analyzing network traffic. Second, if the capacity of a link is already utilized, a payment routed on that link needs to be aborted. This can lead to a starvation problem, and cause other payments to be aborted at previous links on the path as well. Finally, to minimize the costs of opening and closing channels, each supplier/EV owner needs to minimize the number of outgoing links from them. However, this will result in suppliers which will need to create very high capacity channels to accommodate transactions passing over them. Obviously, this is not desired since no supplier would like to make huge investments without charging additional forwarding fees.

C. Attack Model

In general, our primary attack model is limited to undermining the EV owner privacy. We consider a passive adversary who can 1) observe some fraction of payment traffic; 2) join the network as a charging station; and 3) compromise some fraction of nodes.

Replaying payments by introducing bogus payment transfers to fill the capacity is out of the scope of this paper, as they can be detected easily by traffic analysis and exclusion of malicious node. In general, we assume that the attacker is not able to compromise all selected set of nodes even if it knows the complete topology of the PCN.

IV. Proposed Optimization Model for PCN Creation

A. Overview

The proposed PCN in this paper will form a virtual topology on top of the on-chain operations, thus providing a valuable infrastructure which is able to guarantee P2P payment service without requiring any on-chain transactions. Before elaborating on the details of the proposed solution, we first emphasize some important points and summarize the overall approach.

The optimization of the placement of payment channels utilized by a PCN, as well as the fairness in the allocation of network design costs, are fundamental issues for the members who pay for the costs involved. While designing the network, the payment channels to a charging station should have enough capacity for both routing payments of others and for receiving the payments intended for that station. Moreover, the channel capacity between the stations should be organized in such a way that stations with similar intent and opportunity should contribute to the network in a similar way.

Our approach considers all these issues by proposing a mixed integer programming model inspired by multi-commodity network flow problems [32]. The model minimizes the PCN design cost according to different cost sharing scenarios. These costs are the network flow cost, link establishment cost and unfairness cost in capacity distribution among the stations.

B. Formulation of the Model

There are N users in the network with I defining the set of the EV users and $I = \{EV_1, EV_2, \ldots, EV_N\}$ and $N = |I|$. Similarly there are M stations (denoted as ST) in the payment system and P is the set of the stations and $P = \{ST_1, ST_2, \ldots, ST_M\}$ and $M = |P|$. From now on, the term "node" and "station" will be used interchangeably. Each EV owner will be registered to a station. Whenever a user receives charging service from a station, a payment will be initiated from the registered station to the payee station. Let the graph $G(V, E)$ be defined such that $V = I \cup P$ and $E = \{[(i, j) : i \in I, j \in P] \cup [(j, j') : j, j' \in P]\}$ Each EV owner, EV_i, is assumed to be making payments to a set of stations, J_i, during the payment period (these refer to the stations within the areas typically traveled by the EV). This period can be of any length, which impacts the size of J_i. Hence, $|J_i|$ is the expected total number of payments that will be made by EV_i. Let a_{ij} be the expected payment amount by EV owner $i \in I$ to charging station $j \in J_i$ during the planning period. Given these initially known values, we can define the total "supply" of an EV owner as:

$$s_i = \sum_{j \in J_i} a_{ij} \tag{1}$$

for all $i \in I$, and the total "demand" of a charging station as:

$$d_j = \sum_{i \in I} a_{ij} \tag{2}$$

for all $j \in P$.

Let decision variable $u_{jj'}$ denote the capacity of the payment channel on edge (j, j') to be established between $j, j' \in P$, where each unit of capacity incurs a variable cost of $c^v_{jj'}$ (i.e opportunity cost for keeping bitcoins in reserve). In our model, to represent a real-time scenario, we assume that setting up a payment channel will carry a fixed "channel establishment fee (i.e., Bitcoin transaction fee)". So, a fixed cost of $c^f_{jj'}$ is assumed if a payment channel is established between $j, j' \in P$.

Suppose that the optimization objective involves the minimization of a function of the total cost of establishing payment channels across the entire network (involving fixed and variable costs), while ensuring that all payments by EV owners will be processed following some path on the network where the termination node of the path corresponds to the recipient of a given payment.

To allow for a multi-commodity flow type integer programming formulation which is known to be NP-Complete [33],

we further define the following decision variables. We let x_{ij}^k define the payment flow on arc (i,j) for $i \in I, j \in P$ intended for station $k \in J_i$. Moreover, $y_{jj'}^{ik}$ refers to the flow on arc (j,j') for $j,j' \in P$ which has originated from EV owner $i \in I$ with destination $k \in J_i$. In order to indicate the channel 'opening' decision between any two charging stations, we define the binary variable $z_{jj'}$ such that $z_{jj'} = 1$, if there is positive flow on arc (j,j') for $j,j' \in P$, and $z_{jj'} = 0$, otherwise.

We then can formulate the optimization problem through equations (3)-(10) as follows:

$$\min \sum_{j\in P}\sum_{j'\in P} c_{jj'}^v u_{jj'} + c_{jj'}^f z_{jj'} \tag{3}$$

$$\text{s.t.} \sum_{j\in P} x_{ij}^k = a_{ij} \qquad \forall i \in I, k \in J_i \tag{4}$$

We need to have the node transaction conservation equations as:

$$\sum_{j'\in P} y_{j'j}^{ik} + x_{ij}^k - \sum_{j'\in P} y_{jj'}^{ik} = a_{ij} \qquad \forall j,i,k \in J_i \tag{5}$$

In addition, the capacity of the links should be large enough to accomodate the flows on the arcs and the fixed cost structure should be defined, while channel capacity from one node to the other should be symmetric:

$$\sum_{i\in I}\sum_{k\in J_i} y_{jj'}^{ik} \le u_{jj'} \qquad \forall j,j' \in P \tag{6}$$

$$\sum_{i\in I}\sum_{k\in J_i} y_{jj'}^{ik} \le C' z_{jj'} \qquad \forall j,j' \in P \tag{7}$$

$$u(j,j') = u(j',j) \qquad \forall j,j' \in P \tag{8}$$

$$x,y,u \in R^+, z \in \{0,1\} \tag{9}$$

where C' is some upper bound for the capacity on a given channel. That C' can also be chosen different for each possible arc.

Finally, in order to assign an EV user to a single predefined station, we include the following equation:

$$x_{ij}^k = a_{ik} \qquad \forall i \in I, k \in J_i \text{ and } j = ST_{ij}^k \tag{10}$$

For that equation to hold ST_{ij}^k is a station chosen randomly for delivering a payment from user i to station k starting at station j.

C. Fair Distribution of Network Design Costs Among Nodes

A member station of a PCN should open payment channels with other peers more than its own demand so that it can forward the payments of other charging stations. However, these payment channels have an associated cost due to keeping Bitcoin in escrow and related transaction fees. Therefore, the members of PCN strive to keep their investment costs at minimum while participating in the formation of a PCN.

Thus, in the optimization, a new cost, namely unfairness cost represented by Γ, is added in order to provide a mechanism for sharing network formation costs fairly. For that purpose, capacity difference between nodes with maximum and minimum outbound flows are multiplied by a parameter γ as follows:

$$totFlows_j = \sum_{i\in I}\sum_{k\in J_i}\sum_{j'\in P} y_{jj'}^{ik} \qquad \forall j \in P \tag{11}$$

$$maxFlow = max_j(totFlows_j) \tag{12}$$

$$minFlow = min_j(totFlows_j) \tag{13}$$

$$\Gamma = \gamma * (maxFlow - minFlow) \tag{14}$$

Note that $maxFlow$, $minFlow$, and $totFlows_j$ are non-negative decision variables in the appended formulation with fairness considerations.

D. Implications on Privacy

As we have focused on overall cost reduction as our key optimization objective along with multiple cost-sharing scenarios, our constructions and security definitions do not directly aim to ensure privacy.

However, the resultant PCN indirectly ensures privacy by forming a decentralized topology. This is particularly relevant since the existing studies that focus on routing privacy in PCN require PCN to be designed in a decentralized manner [28]. For instance, the study in [29] offers a source routing mechanism together with Tor-like onion payment forwarding. Their routing mechanism provides a strong user privacy by not letting intermediate nodes to find out source and destination of the payment. This will only be possible in a fully decentralized topology as provided by our optimization model.

V. Evaluation

A. Experimental Setup and Implementation

We make the following assumptions for the PCN elements: Current charging station facilities show differences in terms of available number of spots and charging speeds. For example, there are 2 stations at Miami Beach Municipal Parking lot and there are 6 Tesla super chargers on the 184th mile of Florida's Turnpike. In order to apply the model for larger facilities we assume there are 8 charging plugs in a facility. For the optimization implementation, the available number of stations are denoted as $number\_of\_stations$, so the number of customers, i.e. $number\_of\_EV$, will be 8 times the $number\_of\_stations$ in the model. For a typical network, the payment plan and the optimization can be done on a daily basis, however, for certain setups this can be done on a weekly or monthly basis. To this end, in our model we assume that a customer may make a payment to 6 different stations which is $payment\_per\_EV$ over the planning period. If we apply this assumption to the case of a Tesla owner, we can say that 6 full charges will let a Tesla travel more than 1000 miles, which can be roughly considered as one month's travel distance.

For the baseline optimization scenario, the unit flow cost between stations, $c_{jj'}^v$, is set to 1. The channel establishment fee cost multiplier is set to be equal for every link, i.e. $c_{jj'}^f = c^f$ and it varies from 50 to 650. γ varies from 20 to 80. For each EV user, the payee stations set is generated randomly. An EV user is registered to another random station,

which is different from the stations in the payee set. For ease of following the transactions and result comparisons, each transaction is selected to be 10 units, i.e., each EV user supplies 10 times $payment\_per\_EV$ to the network. Since stations are created randomly, the demand of a station may be different from another one. $number\_of\_stations$, $number\_of\_EV$ and $payment\_per\_EV$ are set to be 10, 80 and 6 respectively.

B. Metrics and Benchmarks

The solution to the optimization problem is evaluated based on the following metrics:

- **Betweenness centrality of a node:** Betweenness centrality of a node is a measure for the node which shows, in a network, how many times a node is visited while traveling between other nodes in the possible shortest distance routing.
- **Total Capacity of the Network:** This metric basically represents total required investment amount in the escrow accounts to form a PCN network among participants.
- **Number of Edges:** This metric shows the resulting number of payment channels created among the network.

We compared our approach against certain benchmarks. Specifically, we first consider benchmarks for creation of the network topology among charging stations as follows:

- **Random network topology** We assumed that the topology of the network is random. The edges are created by assuming that each station has more than 2 connections to other stations Our optimization model is applied on this randomly generated network.
- **Fixed Hub and Spoke topology:** 2 stations are assumed to be the most central stations and remaining stations are divided into 2 groups. Each of these groups are directly connected to those main stations. Again, optimization is carried out for that network.

C. Experiment Results and Discussion

1) Betweenness Centrality Comparison

Betweenness comparison of the networks is shown in Fig. 3. In the figure, note that, x-axis shows the node number renamed according to descending centrality score, y-axis is the centrality score. Hub-and-spoke network shows high betweenness for 2 nodes (center hubs) and the betweenness centrality value of the other stations is 0. Compared to hub and spoke network, there is a big change in betweenness centrality for random connected network. However, the optimized networks give better centrality results. Especially the network optimized with $c^f = 650$ and $\gamma = 20$ gives a flat betweenness centrality graph (0.083 centrality value), which yields a flat distribution of connections. As expected, optimized networks yield a more balanced network topology.

2) Total Capacity of the Networks

In this experiment, for our approach we fixed γ while varying c^f. Fig. 4 shows the resulting total capacity for different network topologies. As can be seen, our approach

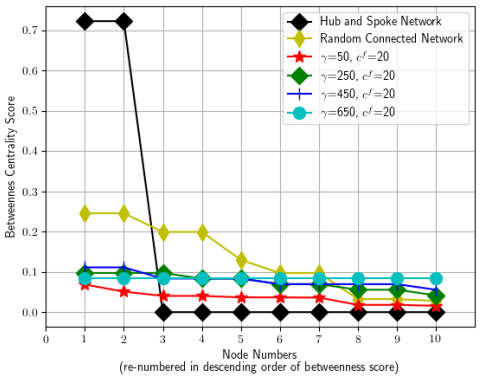

Fig. 3: Betweenness centrality comparison between the networks with respect to γ and c^f

helps the participants invest less money into the escrow accounts compared to hub-and-spoke and random connected topologies. When c^f decreases, our approach strives to reduce the total capacity as will be justified shortly. Note that in the experiments, total amount of money supplied by all EV owners is fixed which is 4800 units. From a business perspective, it can be argued that not so many people want to invest much more than the amount they will earn. Our approach ensures this. For instance, for our approach, the total capacity is always less than 7000 units while for hub-and-spoke the total capacity is over 10,000 units.

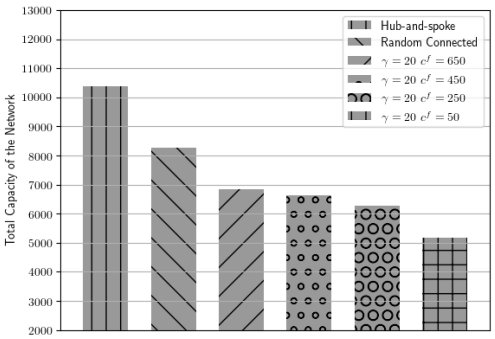

Fig. 4: Capacity of the networks

3) Total Edges in the Network

Fig. 5 depicts the number of edges established in resultant network topologies. Picked cost parameters plays an important role in the number of established edges. Decreasing c^f causes an increase in number of edges as connection fee cost starts to become less dominant in total cost calculation. Although fewer number of connection seems as a good choice, e.g., ring topology, relay stations for a particular transaction will have to invest more during the network establishment. Additionally, some of the stations might experience single point of failure problem in case of link terminations.

Overall, we can speculate that when there are fewer edges in the network, the transactions have less options to travel and thus they follow the available paths that are limited. In other words, there is not much liberty for a transaction. It has to follow longer routes in many cases. However, when there are

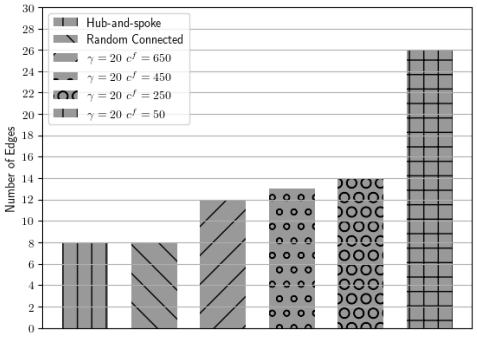

Fig. 5: Number of edges in networks

more edges in the topology (i.e., when $c^f = 50$ as shown in Fig. 5), this provides more options in terms of shortcuts for their travel paths. This means, instead of using multiple hops for a transaction, a single hop can be used which will reduce total capacity cost (see Fig. 4. As a result, when there is increased number of edges, our approach is able to reduce the total capacity of the network which is not the case in hub-and-spoke model.

VI. Conclusion and Future Work

In this paper, we designed a private payment network for Bitcoin transactions in a network of EVs and charging stations. The objectives were to eliminate the high transaction fees and verification times by using the off-chain concept of Bitcoin and establishing a privacy-aware payment network thanks to anonymous behavior of public blockchain based cryptocurrency. We formed an overlay payment network using an optimization model based on a multi-commodity flow problem structure. The resultant topology ensured that it minimizes the costs for establishing channels among stations. The topology also favors privacy since it prevents formation of hub nodes that can potentially monitor the source and destination of all payments. The results indicate that the topology can significantly save transaction fees for EVs.

For future work, we plan to investigate heuristics for large-scale formation of the payment network topology. Including EV registering process in the model is another study to be conducted.

References

[1] T. Markel, M. Kuss, and P. Denholm, "Communication and control of electric drive vehicles supporting renewables," in *Proc. of IEEE Vehicle Power and Propulsion Conference, VPPC'09*, pp. 27–34.

[2] N. DeForest, J. Funk, A. Lorimer, B. Ur, I. Sidhu, P. Kaminsky, and B. Tenderich, "Impact of widespread electric vehicle adoption on the electrical utility business–threats and opportunities," *Center for Entrepreneurship and Tech. (CET) Technical Brief*, no. 2009.5, 2009.

[3] Tesla Motors-High Performance Electric Vehicles, teslamotors.org.

[4] Nissan LEAF Electric Car, nissanusa.com/leaf-electric-car, 2017.

[5] "State of the charge report." [Online]. Available: evassociation.org/stateofthecharge

[6] E. W. Wood, C. L. Rames, M. Muratori, S. Srinivasa Raghavan, and M. W. Melaina, "National plug-in electric vehicle infrastructure analysis," National Renewable Energy Laboratory, Tech. Rep., 2017.

[7] PlugShare, https://www.plugshare.com/, 2017.

[8] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," *IEEE Intelligent Transportation Systems Magazine*, vol. 8, no. 3, pp. 33–44, 2016.

[9] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, 2017.

[10] E. Bulut and M. Kisacikoglu, "Mitigating range anxiety via vehicle-to-vehicle social charging system," in *Proceedings of Vehicular Technology Conference (VTC Spring), IEEE*, 2017.

[11] A. P. introduces portable DC fast charger, "Charles morris," 2013. [Online]. Available: https://chargedevs.com/newswire/andromeda-power-introduces-portable-dc-fast-charger/

[12] M. Yamauchi, "How far can you really drive in an electric vehicle? ev range comparison map," https://www.pluglesspower.com/learn/28-different-evs-can-cover-100-daily-driving-pure-electric-power, 2017.

[13] A. Cavoukian, J. Polonetsky, and C. Wolf, "Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation," *Identity in the Information Society*, vol. 3, no. 2, pp. 275–294, 2010.

[14] J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the privacy risk of location-based services." in *Financial Cryptography*, vol. 7035. Springer, 2011, pp. 31–46.

[15] Z. Yang, S. Yu, W. Lou, and C. Liu, "Privacy-preserving communication and precise reward architecture for v2g networks in smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 697–706, 2011.

[16] M. Stegelmann and D. Kesdogan, "Design and evaluation of a privacy-preserving architecture for vehicle-to-grid interaction," in *European Public Key Infrastructure Workshop*. Springer, 2011, pp. 75–90.

[17] Y. Cao, N. Wang, G. Kamel, and Y.-J. Kim, "An electric vehicle charging management scheme based on publish/subscribe communication framework," *IEEE Systems Journal*, 2015.

[18] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed protocol for electric vehicle charging," in *Communication, Control, and Computing (Allerton), 2014 52nd Annual Allerton Conference on*. IEEE, 2014, pp. 242–249.

[19] M. Wang, M. Ismail, R. Zhang, X. Shen, E. Serpedin, and K. Qaraqe, "Spatio-temporal coordinated v2v fast charging strategy for mobile gevs via price control," *IEEE Transactions on Smart Grid*, 2016.

[20] PlugAmerica, https://pluginamerica.org/how-much-does-it-cost-charge-electric-car/, 2017. [Online]. Available: https://pluginamerica.org/how-much-does-it-cost-charge-electric-car/

[21] "Bitcoin's high transaction fees show its limits," (Accessed on 14-Mar-2018). [Online]. Available: bloomberg.com/view/articles/2017-11-14/bitcoin-s-high-transaction-fees-show-its-limits

[22] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," *Technical Report (draft)*, 2015.

[23] "Fast, cheap, scalable token transfers for ethereum," (Accessed on 14-Mar-2018). [Online]. Available: raiden.network

[24] W. Han and Y. Xiao, "Privacy preservation for v2g networks in smart grid: A survey," *Computer Communications*, vol. 91, pp. 17–28, 2016.

[25] M. Stegelmann and D. Kesdogan, "Location privacy for vehicle-to-grid interaction through battery management," in *Information Technology: New Generations (ITNG), 2012 Ninth International Conference on*, pp. 373–378.

[26] S. Thomas and E. Schwartz, "A protocol for interledger payments," https://interledger. org/interledger. pdf, 2015.

[27] L. N. Team, "Atomic cross-chain trading." https://en. bitcoin.it/wiki/Atomic cross-chain trading. [Online]. Available: https://en. bitcoin.it/wiki/Atomic cross-chain trading

[28] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi, "Concurrency and privacy with payment-channel networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 455–471.

[29] P. Prihodko, S. Zhigulin, M. Sahno, A. Ostrovskiy, and O. Osuntokun, "Flare: An approach to routing in lightning network," 2016.

[30] R. Pass *et al.*, "Micropayments for decentralized currencies," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 207–218.

[31] B. Wiki, "Contracts: Example 7: Rapidly-adjusted (micro) payments to a pre-determined party."

[32] S. Even, A. Itai, and A. Shamir, "On the complexity of time table and multi-commodity flow problems," in *Foundations of Computer Science, 1975., 16th Annual Symposium on*. IEEE, 1975, pp. 184–193.

[33] C. H. Papadimitriou, "On the complexity of integer programming," *Journal of the ACM (JACM)*, vol. 28, no. 4, pp. 765–768, 1981.