EVChain: A Blockchain-based Credit Sharing in Electric Vehicles Charging

Mahdi Daghmehchi Firoozjaei, Ali Ghorbani
Canadian Institute for Cybersecurity
Faulty of Computer Science
University of New Brunswick
Fredericton, Canada
m.daghmechi@unb.ca, ghorbani@unb.ca

Hyoungshick Kim
Department of Computer Science and Engineering
Sungkyunkwan University
Suwon, South Korea
hyung@skku.edu

Jaeseung Song
Department of Computer and Information Security
Sejong University
Seoul, South Korea
jssong@sejong.ac.kr

***Abstract*—The Digital economy is based on confidence in its trustworthiness. Blockchain distributed consensus provides a reliable and trustful network for financial and non-financial transactions. Blockchain-based electric vehicles (EVs) charging applications benefit blockchain features to provide automated and verifiable services for EV charging market. Requirements for feasible charging operation and privacy concerns are challenging issues with blockchain-based EV charging approaches. To provide a feasible charging ability and preserve EV owner's privacy, we introduce EVChain. The EVChain is a trustful and decentralized platform based on blockchain technology to share charging credits in the EV charging market. To share credits, the main blockchain in EVChain is connected to one or more subnetwork blockchains. We introduce an interconnection position to preserve EV owners' privacy with *k*-anonymity protection. We simulate and evaluate the privacy protection it provides, based on an example EV charging scenario.**

***Index Terms*—Blockchain, Electric vehicles, Credit sharing, *k*-anonymity, Anonymization**

I. Introduction

Electric vehicles (EVs) are an important step toward green and smart cities. Their commercial success depends on the development of charging infrastructure that is accessible, inexpensive, and reliable. Distributed energy resources in the smart grid open new opportunities for EV charging platforms. Furthermore, blockchain technology provides new features for liberalizing EV charging markets in the smart grid. Cost negotiation, finding the cheapest charging station, and providing an automatic and reliable payment mechanism are feasible with blockchain-based technology. Independently, all nodes in a blockchain system hold their own copy of the blockchain ledger, and the current known state is calculated by processing each transaction as it appears [1]–[3]. Blockchain technology provides a verifiable and immutable data storage and contract initiation in a market where charging stations are owned by various operators [4].

Blockchain-based charging systems change the traditional energy market toward peer-to-peer (P2P) transactions by introducing new payment mechanisms. For instance, Blockcharge[1] is a prototype blockchain-based charging, authentication, and payment solution for the EV charging market. Fig. 1 depicts a typical blockchain-based EV charging system. Typically, in these solutions beside the blockchain an EV charging application is used to communicate with the interface. Due to the diversity of energy resources in the smart grid, an application provider can be a third party rather than the electric utility itself. Due to capacity limitation, the number of EV charging operations is much more compared to getting gas in a same distance. Therefore, charging ability is a critical requirement for EVs in the view of accessibility and credit.

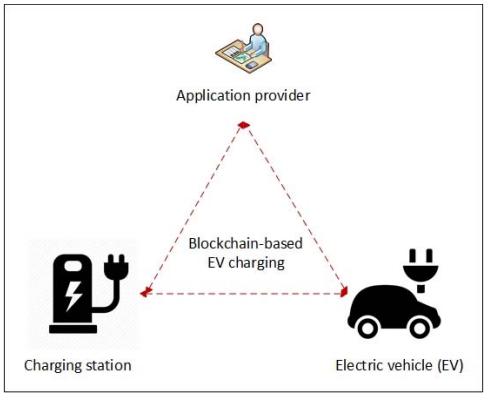

Fig. 1. A typical blockchain-based application for EV charging.

On the other hand, the intersection of blockchain and privacy is a concern for EV owners. Long-term analysis of EV charging information available in a blockchain could be used for user profiling. It may expose the user's driving patterns and whereabouts that could be used for criminal or financial purposes (e.g., sending appropriate ads) [5]. Some solutions use the off-chain mechanism to address these issues. The off-chain mechanism addresses the privacy issue by creating a bi- or unidirectional transaction channel between two parties in a blockchain. This mechanism helps cope with the scalability problem of blockchain. Despite the benefits of the off-chain mechanism to preserve privacy and decrease transaction fees (e.g., in Bitcoin), it has its limitations, namely limited channel capacity, data privacy in payment transaction routing, and the

[1]https://thefuturescentre.org/signals-of-change/16594/prototype-blockchain-electric-vehicle-charging-and-billing-system

978-1-7281-3265-5/19/$31.00 ©2019 IEEE

cost of opening and closing channels [5].

To provide a feasible charging ability, we propose EVChain for privately sharing charging credits between EV owners. It allows credit sharing within a group of owners and preserves an individual group member's privacy with *k*-anonymity protection. It exploits the decentralized nature of blockchain, in which the transactions are distributively logged and verifiable. Basically, EVChain is a hybrid blockchain framework consisting of a main blockchain for billing and payment and one or more subnetwork blockchains for credit sharing. We introduce an interconnection, called *bridge*, to interconnect the main blockchain and its subnetworks. The bridge separates transactions in the main blockchain from those in its subnetworks and provides anonymization.

The main contributions of this paper are as follows:

- We introduce EVChain, a trustful and decentralized blockchain-based EV charging platform to share charging credits. To handle credit sharing transactions in the subnetwork blockchain, we present a new block, called local block. It has an extra header to manage credit sharing activities.
- The interconnection role of the bridge is introduced to provide *k*-anonymity protection. A simulation of EVChain is done performed to analyze its performance and evaluate the privacy-preserving.

The rest of the paper is organized as follows. Section II describes preliminary concepts. Section III explains the architecture of EVChain as well as the bridge functions and the structure of local block. Implementation and transaction handling are discussed in Section IV. Privacy preserving attributes are evaluated in Section V. Finally, our conclusions and discussion of future work are found in Section VI.

II. Preliminary

A. Off-chain and hybrid blockchains

It has been shown that a blockchain cannot process more transactions than a single node can. Solutions that have been proffered to address the scalability limitation of blockchain are: increasing the size of block to handle more transactions (e.g., Bitcoin Cash), processing transactions off the blockchain (e.g., off-chaining process) and then writing them to the blockchain over intervals, and merging the mining power of several chains.

In off-chain processing, a.k.a. transaction channel, two parties perform several P2P payments without committing transactions to the Bitcoin shared ledger [5]. To this end, one party opens a payment channel by instantiating an escrow account with the receiver and deposits some Bitcoins by adding a transaction to the blockchain. With this payment channel, they perform several off-chain bi- or unidirectionally payments by locally agreeing on the new distribution of the deposit balance. Eventually, when the payment channel is closed, the payment parties perform another Bitcoin transaction to add the final balances to the blockchain [5], [6]. The on/off-chain mechanism enables deploying only the on-chain process onto the blockchain. This conserves the resources of the blockchain and hides the sensitive information involved in the off-chain transactions from the public [7].

To extend the P2P payment channel, local rebalances are used by the subnetworks within the blockchain network. As the payment networks, these subnetworks allow payments to be made between parties that are not at the same moment connected by a payment channel. These linked payments create a chain of payment channels as intermediate links between two parties that wish to transact with each other off-chain [8]. Although the payment networks address the inability of a payment channel to refund the balance without performing transactions on the blockchain with no need to open a new payment channel or conduct an on-chain transaction, the trustworthy issues are considerable with the payment network.

Blockchain systems are of two major types: public and private. In a public blockchain any node can join and leave the system, while in a private blockchain there is an access control mechanism to authenticate and authorize the nodes. Thus, the identity of each node in a private blockchain is known by the other nodes [9]. In other words, a node's activities in a private blockchain are only visible and limited to authenticated nodes. A hybrid blockchain is a combination of public and private blockchains and exhibits characteristics of both with the consensus process being controlled by known, privileged servers. Since the copies of the blockchain are only distributed among entitled participants, the hybrid blockchain is only partly decentralized [10].

B. K-anonymity

K-anonymity is a well-known and widespread privacy preserving method for achieving anonymity. It guarantes that in a set of *k* similar objects, the target object is not distinguishable from the other $k-1$ objects [11]–[13]. Thus, the probability to identify the target user is $1/k$ [14]. The degree of anonymity depends on the number of members in the anonymity group (*k*) and the adversary's knowledge. Practically, *k*-anonymity approaches require a trusted center to operate the privacy server. The privacy server acts as the anonymizer and modifies the initial data by applying the operations of data suppression or value generalization [14], [15].

To measure the anonymity level provided by the anonymity process, information entropy can be used for anonymity group. If we consider each individual in an anonymity model of X as an information point, $H(x)$ shows its entropy value. Suppose p_i is the probability of identifying the i^{th} individual in the anonymity set with k members; then:

$$H(x) = -\sum_{i=1}^{k} p_i log_2(p_i) \tag{1}$$

The maximum entropy, H_M, of a *k*-anonymity set is achieved when all k individuals have the same probability measure of $1/k$ to be identified. Therefore:

$$H_M = log_2(k) \tag{2}$$

The information that an adversary can achieve with an attack on this anonymity set can be expressed as:

$$\frac{H_M - H(x)}{H_M} \tag{3}$$

which is normalized by dividing by H_M [13]. Based on this, anonymity degree is defined by Diaz et al. [16] as:

$$d = 1 - \frac{H_M - H(x)}{H_M} = \frac{H(x)}{H_M} \tag{4}$$

An anonymity degree of d represents the anonymizing level of the anonymity model and is a value between 0 and 1, $(0 \leq d \leq 1)$. An anonymity model has a minimum value of the anonymity degree $(d = 0)$ if an individual in the anonymity set appears to be identified with the probability of $p = 1$, whereas if all individuals have the same probability of being identified $(p = 1/k)$, the model has the maximum value of anonymity degree $(d = 1)$ [13].

III. Model description

EVChain is a hybrid blockchain with a main blockchain (MaBC) used by an electric charging application and one or more subnetwork blockchains (SuBCs) for credit sharing group(s). Two types of transactions are defined in EVChain: user-to-server (U2S) transactions in MaBC and user-to-user (U2U) transactions between EVs in SuBC. By installing the charging application, the client joins the blockchain (MaBC) with charging stations and an application server. Each client is identified by a unique *client-id*, as its public key and necessarily has no relation to its real identity. A genesis transaction is created by the application server to start the MaBC blockchain. Any transactions related to the service, such as purchasing credits, spending credits, updating, and electric charging are packed in the block after being verified by a miner in the MaBC. To create a credit sharing group, a SuBC is established between the client who purchases the credit and some EVs. Basically, the SuBC is a subnetwork blockchain which shares ledger between the members of the credit-sharing group. We introduce an interconnection role called *bridge*, to connect the MaBC and its SuBCs.

A. Bridge

Fig. 2 depicts EVChain and bridge position connecting the MaBC and the SuBC. In EVChain, a client, who purchases the charging credit, is able to share it with other EVs in the credit-sharing group. This client plays an interface role in EVChain. Since this client simultaneously joins the MaBC and the SuBC(s), he is called the bridge. In fact, the bridge is the credit buyer in the MaBC and the credit coordinator in the SuBC(s). By separating the transactions in the subnetwork and the main blockchain, the bridge protects the privacy of the group members as an anonymizer. To this end, he performs the anonymization process of generalization by eliminating any identifying links to EV owners in the group. Due to data anonymization, U2S transactions do not show any private information about the user (i.e., EV owner's identity). In

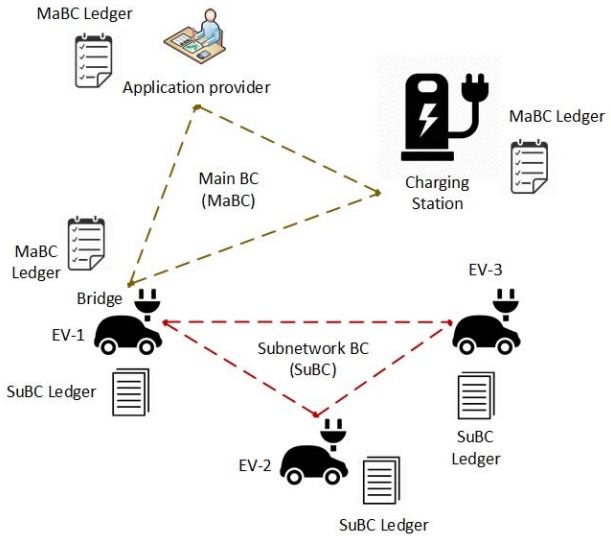

Fig. 2. EVChain model and the interconnection position of the bridge between MaBC and SuBC.

fact, the bridge is an interpreting position between the MaBC and the SuBC. To manage credit-sharing, the group members follow some policies or rules and monitor the credit state. The rules would depend upon agreements amongst the EV owners and the current status of those agreements. The credit is jointly shared between the members of the credit-sharing group. All access and use events are logged in the shared ledger in the SuBC with a U2U transaction. On other hand, a new block consisting of U2S transactions of electricity purchases is shared simultaneously with the bridge in MaBC.

B. Local block

Basically, in blockchain each block is composed of a header and a list of transactions. The header consists of the hash value of the previous block, timestamp, nonce, the hash value of all transactions in the block, and the hash of the state after processing the block. To detect any unauthorized data tampering, blockchain technology offers two levels of integrity protections. At the first level, the global states of the chain are protected by a hash (Merkle) tree root of all transactions in the block [9]. The block history is protected at the second level by chainlike linking to the previous blocks [9], [17].

To handle U2U transactions in the credit-sharing group we introduce a local block. Each local block has two headers, viz. a main header and a credit header. As shown in Fig. 3, the credit header has five parameters. The device management (DMG) parameter shows the EVs registered in the credit-sharing group and is used as *EV-id* to distinguish the group members. The security parameters required for credit access, such as identity management and access control, are in the security (SEC) parameter. The charge management field (CMF) parameter controls the negotiated policies required for charging management. EV owners use these policies to agree on conditions of credit use, such as access restriction, usage amount, and utilization priority. The total number of spent

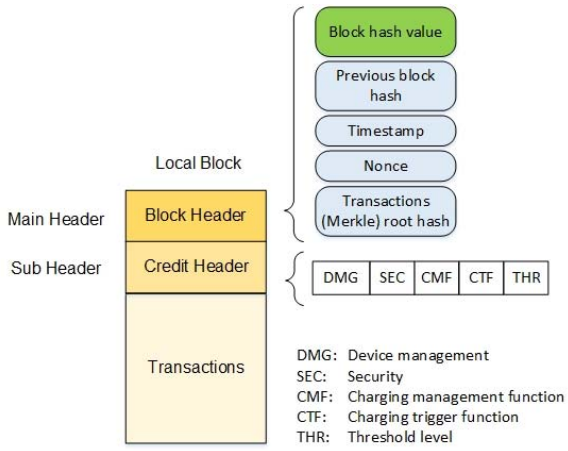

Fig. 3. Local block structure for U2U transaction.

credits is recorded by the charging trigger function (CTF) parameter. To manage credit use, we define a threshold at which point the access policy will be changed. The threshold (THR) parameter is self explanatory. When the threshold is reach, the charging service is available only for the predefined high priority EV.

IV. Implementation

To implement EVChain, we used and developed the Python blockchain package provided by E. Alcaide, available on GitHub[2]. In particular, we implemented the bridge node which interconnects the MaBC to the SuBC(s). Since the main focus of this implementation was to provide trustful transactions and a hashed ledger feature, the miner and mining process were not included. We implemented the bridge to connect and update both blockchains and evaluate the provided privacy preserving. The credit header in the local block needs to be initialized in order to initiate the credit sharing group. They are set as described in the preceding paragraph.

V. Privacy preserving

Credit use for the group is saved in a table and is available by U2U transactions in the SuBC. Table I shows an example of this where a credit of $1000KW$ is shared between four EVs. In this table, the information of EV's identity (*EV-id*), electricity usage in *KW* (*Usage*), the credit balance in *KW* (*Credit*) and the date and time of the charging event (*Date* and *Time*) are recorded for each charging event. To preserve the privacy, the bridge anonymizes the information of the credit-sharing group and generates a new table to be shared with the members in the MaBC. In fact, the data in the new table is a transformed version of the data of the credit-sharing group in the main table and is available through U2S transactions in the MaBC. Table II shows the credit usage information in the service group and is an anonymous view corresponding to Table I. Assuming that the number of EVs in the credit-sharing group is available to the service group members (in MaBC) by linking to external data (e.g., electric charging manner), Table II is a 4-anonymity view of Table I.

[2]https://github.com/EricAlcaide/pysimplechain

TABLE I
Credit utilization data in credit sharing group (SuBC)

Date	Time	EV-id	Usage (KW)	Credit (KW)
20190301	07:10	EV-2	30	970
20190301	10:26	EV-4	16.5	953.5
20190302	14:52	EV-1	42	911.5
20190302	18:00	EV-2	28.5	883
20190302	22:06	EV-4	16.5	866.5
20190303	09:44	EV-3	75	791.5
20190303	11:13	EV-2	30	761.5
20190303	19:30	EV-1	40	721.5
20190303	21:09	EV-4	15	706.5
20190304	17:11	EV-4	16.5	690

TABLE II
Credit utilization data in the application blockchain (MaBC)

Date	Time	Client-id	Usage (KW)	Credit (KW)
20190301	07:10	EVC-112	30	970
20190301	10:26	EVC-112	16.5	953.5
20190302	14:52	EVC-112	42	911.5
20190302	18:00	EVC-112	28.5	883
20190302	22:06	EVC-112	16.5	866.5
20190303	09:44	EVC-112	75	791.5
20190303	11:13	EVC-112	30	761.5
20190303	19:30	EVC-112	40	721.5
20190303	21:09	EVC-112	15	706.5
20190304	17:11	EVC-112	16.5	690

The data in Table II is anonymized by performing a generalization process on Table I. In this process, the attribute of EV's identity (*EV-id*) in Table I is generalized into client id (*Client-id*) in Table II. Other attributes are unchanged and Table II provides information about electric charging events related to registered client. Individually, there is no information about the EVs of the credit-sharing group and all electric charging data is related to the client id, which was registered at the time of service purchasing (*EVC-112* in this example). Therefore, the privacy of credit sharing members is kept by concealing their activities by the bridge in the transmitted information.

To measure the provided anonymity, we use the anonymity degree introduced in Section II. We assume that, based the side knowledge, the attacker knows the number of EVs in the credit-sharing group. This could be achieved by finding a link between a driver and his/her EV registered with another service and vehicle properties (e.g., battery capacity or charging speed). The identities of the credit-sharing group members are unknown to the attacker and there is no link between client id and EVs in the anonymity set. Based on the Table II, in the best anonymizing condition, in which the attacker is not able to distinguish EV drivers, the probability to identify an EV is $1/4$. In the created anonymity set, the anonymity degree equals to:

$$d = \frac{H(x)}{H_M} = \frac{-\sum_{i=1}^{4} p_i log_2 p_i}{log_2(4)} \tag{5}$$

In Table II, the maximum anonymity degree ($d = 1$) is

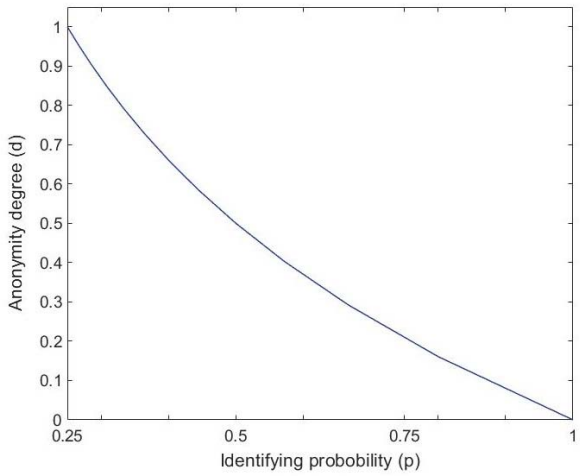

Fig. 4. Anonymity degree curve for anonymity set in Table II.

achieved by hiding EV identities. If the attacker finds an EV based on the sensitive attribute available in the table, the anonymity set is shrink to a 3-anonymity set and the attacker has the probability of $p = 1/3$ to identify other EVs. Fig. 4 depicts the curve of anonymity degree for the anonymity set in Table II. The anonymity set has the minimum anonymity degree ($d = 0$) if the attacker identifies EVs in a linking attack, based on side information from available attributes. For instance, by profiling the electric charging attribute or electrical properties of EV, the attacker has some clues to perform a linking attack.

VI. Conclusions

In this paper, we introduced EVChain, a credit sharing solution for EV charging systems based on blockchain. EVChain is a hybrid blockchain with subnetworks to establish credit sharing groups. The architecture described meets the basic requirements of providing an accountable and trustful environment for EV charging systems. Omitting the central authority makes a decentralized and global platform for EV charging networks with the data being handled at two levels of accessibility. Data related to the charging credit (e.g., credit update and utilization) is publicly accessible by the members of the MaBC while the private data of the credit-sharing group is privately available in the SuBC.

EVChain has a local block with a credit header to handle U2U transactions of the credit-sharing group in the SuBC. The parameters of the credit header enable the members of credit-sharing group to share the charging credit and manage it with negotiated policies. All credit access and use are logged and monitored in the distributed ledger. The bridge position separates U2U from U2S transactions and hides the activities of the credit-sharing group. To this end, the bridge provides anonymization protection based on *k*-anonymity. All U2U transactions in the credit sharing group are anonymized and no private data is leaked. By this protection, we are able to prevent the possibility of user profiling based on EV charging transactions in the blockchain. We showed that this anonymization model provides an acceptable degree of privacy protection. In the future, we will implement EVCharge and evaluate its performance.

Acknowledgment

The first two authors generously acknowledge the funding from the Atlantic Canada Opportunity Agency (ACOA) and the research grant from the National Science and Engineering Research Council of Canada (NSERC) to Dr. Ghorbani. The fourth author (Dr. Song) was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF-2017R1D1A1B03036285).

References

[1] D. Yaga, P. Mell, N. Robey, and K. Scarfone. Blockchain technology overview. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf, 2018.

[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564, June 2017.

[3] M. Crosby, N. Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman. BlockChain Technology. Technical report, Sutardja Center for Entrepreneurship & Technology, 2015.

[4] F. Knirsch, A. Unterweger, and D. Engel. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Computer Science - Research and Development*, 33(1):71–79, 2018.

[5] E. Erdin, M. Cebe, K. Akkaya, S. Solak, E. Bulut, and S. Uluagac. Building a Private Bitcoin-based Payment Network among Electric Vehicles and Charging Stations. In *2018 IEEE Confs on IoT*, pages 1609–1615, 2018.

[6] 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*, CCS '17, pages 455–471, 2017.

[7] C. Li, B. Palanisamy, and R. Xu. Scalable and Privacy-preserving Design of On/Off-chain Smart Contracts. *CoRR*, abs/1902.06359, 2019.

[8] R. Khalil and A. Gervais. Revive: Rebalancing Off-Blockchain Payment Networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 439–453, 2017.

[9] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, and J. Wang. Untangling Blockchain: A Data Processing View of Blockchain Systems. *Computing Research Repository (CoRR)*, abs/1708.05665, 2017.

[10] K. Sultan, O. Ruhi, and R. Lakhani. CONCEPTUALIZING BLOCKCHAINS: CHARACTERISTICS & APPLICATIONS . In *11th IADIS International Conference Information Systems*, 2018.

[11] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam. l-Diversity: Privacy Beyond k-Anonymity. In *22nd International Conference on Data Engineering*, ICDE'06, 2006.

[12] R. Xiangmin, Y. Jing, Z. Jianpei, and W. Kechao. An Improved RSLK-Anonymity Algorithm for Privacy Protection of Data Stream. *International Journal of Advancements in Computing Technology*, 4(9):218–225, 2012.

[13] M.D. Firoozjaei, J. Yu, H. Choi, and H. Kim. Privacy-preserving nearest neighbor queries using geographical features of cellular networks. *Computer Communications*, 98:11–19, 2017.

[14] P. Samarati and L. Sweeney. Generalizing Data to Provide Anonymity when Disclosing Information. In *Proceeding of the 17th ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, PODS '98, pages 188–, 1998.

[15] A. AboHossein, N.R. Darwish, and H.A. Hefny. Multiple-Published Tables Privacy-Preserving Data Mining: A Survey for Multiple-Published Tables Techniques. *International Journal of Advanced Computer Science and Applications*, 6(6):80–85, 2015.

[16] C. Diaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. In *the 2nd International Conference on Privacy Enhancing Technologies*, 2003.

[17] K. Christidis and M. Devetsikiotis. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4:2292–2303, 2016.