IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

Blockchain Based Electric Vehicle Energy Management

Babuvignesh. C[1], Kavya. S[2], Atul Choubey[3], Prasanth. B[4], Dr. Anitha Devi. N Ph.D[5]

B. Tech Scholar., CIT College, Coimbatore[1,2,3,4]

Assistant Professor, CIT College, Coimbatore[5]

Abstract: Smart charging allows a certain level of control over the charging process. It includes different pricing and technical charging options. The simplest form of incentive – time-of-use pricing encourages consumers to move their charging from peak to off-peak periods. Blockchains promise transparent, and secure systems that can enable novel business solutions, especially when combined with smart contracts. We propose a secure charging system for electric vehicles based on blockchain to resolve these security flaws. Our charging system ensures the security of key, secure mutual authentication, anonymity, and perfect forward secrecy, and also provides efficient charging.This paper has three main contributions: (i) a protocol is proposed that finds an optimum charging station, given public biddings as response to a query; (ii) at the same time the customer's geographic position is not revealed during protocol execution; and (iii) a blockchain is used as a decentralized and immutable storage for transparency and verifiability of these biddings. The protocol design keeps the communication overhead and the amount of data to be stored in the blockchain small, which allows to use existing blockchain technologies such as Bitcoin. The privacy of the protocol is evaluated in an honest-but-curious adversary model. This paper focuses on the privacy of the EV and assumes that charging stations and their bids are publicly known.

Keywords: Blockchains Security, Charging Station

I. INTRODUCTION

Energy systems are undergoing rapid changes to accommodate the increasing volumes of embedded renewable generation, such as wind and solar PV. Renewable Energy Sources (RES) have undergone massive development in recent years, enabled by privatisation, unbundling of the energy sector and boosted by financial incentives and energy policy initiatives. With widespread adoption of Electric Vehicles (EVs) and Internet-of-Things (IoT), smart grids with IoT have become promising solutions to control distributed energy and electricity generation. Internet-of-things is applicable to various forms for vehicular systems, such as vehicular ad hoc networks, Vehicle to Grid (V2G), Vehicle to Vehicle (V2V), and Internet of Vehicle (IoV). Vehicles generally have various communication and measuring sensors, including speed, position, Bluetooth, Wi-Fi and On-Board Units (OBU). The sensors in vehicle collect and share data such as speed, location, identity and movements. However, an adversary can intercept, modify and reuse the sensitive data of user, and then try to obtain user's sensitive data because it is transmitted via public network. Therefore, secure mutual authentication and key agreement must be guaranteed to provide secure communication and protect user's privacy. In the past decades, the numerous authentication and key agreement schemes for vehicular systems in IoT have been studied to achieve essential security requirements. Although these schemes try to ensure privacy and enhance efficiency, their scheme is vulnerable to various potential attacks such as distributed denial of service and privileged insider attacks because it is based on trusted third party to provide high security level. If the trusted third party is compromised, their schemes cannot provide services. For these reasons, authentication and key agreement schemes without a trusted third party must be proposed to achieve integrity, confidentiality, availability and reliability, considering resource-constrained devices. Several studies have proposed blockchain approaches to overcome these security weaknesses and enhance efficiency. Blockchain technology guarantees decentralization, verification, and integrity, and is applicable to various fields, including smart grids, healthcare, finance, markets, and voting. Generally, blockchains consists of data blocks, called transactions, where each transaction includes data regarding previous transactions using a hash algorithm. However, early blockchain studies focused on cryptocurrency, e.g., Bit coin and Ethereum, which have significant scalability problems. Hyper ledgers, which do not generate cryptocurrency, have been proposed to overcome these problems and solve scalability. Proposed blockchain based EV charging management security model using smart contracts and the lightning network.

II. LITERATURE REVIEW

This section provides the basic significance of workflow scheduling in cloud. It also provides thenumerous methodology. This development has resulted in huge usage of many applications. Zerocash: Decentralized Anonymous

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

Payments from Bitcoin - Bitcoin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bitcoin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Tackles some of these privacy issues by unlinking transactions from the payment's origin. Payments' destinations and amounts and is limited in functionality. Efficient, Verifiable, Secure, and Privacy-Friendly Computations for the Smart Grid - we present a privacy-preserving protocol between an energy provider and smart meters. Many details about the life of customers can be inferred from fine-grained information on their energy consumption. Different from other state-of-the-art protocols, the presented protocol addresses this issue as well as the integrity of electricity bills. Therefore, our protocol provides secure aggregation of measured consumption per round of measurement and verifiable billing after any period. Preventing Occupancy Detection from Smart Meters - Utilities are rapidly deploying smart meters that measure electricity usage in real-time. Unfortunately, smart meters indirectly leak sensitive information about a home's occupancy, which is easy to detect because it highly correlates with simple statistical metrics, such as power's mean, variance, and range. To prevent occupancy detection, we propose using the thermal energy storage of electric water heaters already present in many homes. You are where you've been: the privacy implications of location and tracking technologies - A decade ago, technologies that could provide information about the location of a motor vehicle, or a computer or a person, were in their infancy. A wide range of tools, processes and systems are now in use and in prospect, which threaten to strip away another layer of the limited protections that individuals enjoy. An understanding of the landscape of location and tracking technologies, and of the issues that they give rise to, depends on establishing a specialist language that enables meaningful and reasonably unambiguous discussion to take place.

III. PROPOSED METHOD

Blockchains promise transparent, and secure systems that can enable novel business solutions, especially when combined with smart contracts. We propose a secure charging system for electric vehicles based on blockchain to resolve these security flaws. Our charging system ensures the security of key, secure mutual authentication, anonymity, and perfect forward secrecy, and also provides efficient charging. This paper has three main contributions: (i) a protocol is proposed that finds an optimum charging station, given public biddings as response to a query; (ii) at the same time the customer's geographic position is not revealed during protocol execution; and (iii) a blockchain is used as a decentralized and immutable storage for transparency and verifiability of these biddings.
The protocol design keeps the communication overhead and the amount of data to be stored in the blockchain small, which allows to use existing blockchain technologies such as Bitcoin. The privacy of the protocol is evaluated in an honest-but-curious adversary model. This paper focuses on the privacy of the EV and assumes that charging stations and their bids are publicly known.

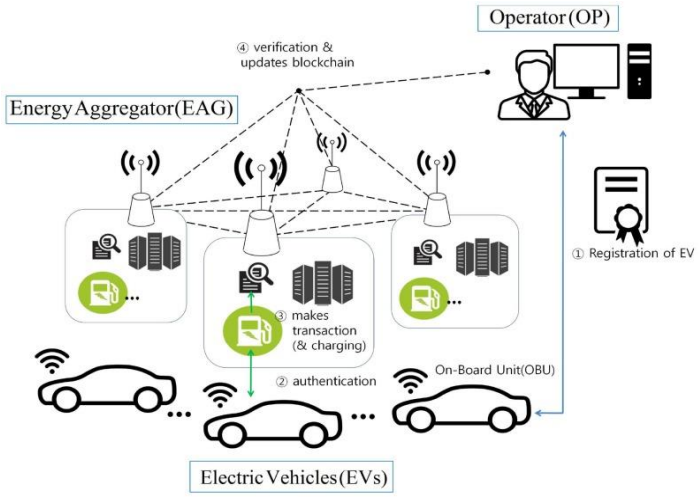

Fig 3.1 Proposed Block chain-based system model

3.1 System Model

Figure 3.1 presents the proposed charging system for EV based on blockchain and our charging system comprises three entities: operator, Charging station, and user/EV; & incorporates four phases: initialization, registration, authentication, and charging, as follows.

- Charging stationregisters their GPS Location &identity with the operator to access charging services.
- EV and charging stationauthenticate each other.
- Charging stationgenerates transactions.
- Charging stationverifies the transaction is valid and records transactions on blockchain networks.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

3.2 Tracking Drive Distances and Times

Our project is described at, and its high level vision is showed. This tracking application mainly stores time, GPS coordinates and user identification.

From the GPS coordinates it is easy to calculate travel distances. Using Google Maps we can represent the drive route and obtain the travel distance. From the travelled distance and EV efficiency we can estimate the remaining energy stored in the batteries of each EV (SOC – State of Charge level), as well as the community SOC level (sum of all individual community SOC levels).

After getting driver location information, the device operator will allocate and schedule the charging station for users based on users location and then also send price details for changing in vehicles from charging devices. User can view charging location and price details.

3.3 Charging phase

In the charging phase, the EV approaches the desired charging station i. This phase does not involve a blockchain, but is a transaction directly executed between the EV and a charging station. In order to verify that this charging station is the one actually chosen by the EV in the previous phase, the commitment is opened by sending, i and from the EV to the charging station. The charging station can then check the commitment by verifying that (ζi,r) =c and can further determine whether the current time matches the initially proposed timeframe of the EV. If both, the commitment and the time-frame, are valid, the amount of energies exchanged during the time interval T for the price b. Since this transaction is only executed between the EV and the chosen charging station, no information is released to the blockchain or any other third party. In particular, the actual position of the EV is only revealed to this single charging station. This is analyzed in more detail in the next section. While this phase could be handled in the blockchain as well, e.g., using some sort of cryptocurrency, the scope of this work is on finding the best tariff without limiting the protocol to a particular payment scheme. Currently, there are many different payment schemes for EV charging in the field, e.g., membership cards, credit cards or even cash could be used for anonymous payment. However, for other use cases, such as settlement and profiling, the actual amount of energy consumed by the EV can be written to the blockchain.

3.4 Storage through Blockchain

The blockchain is a digital ledger of past transactions. A transaction is an exchange of information between different entities that is broadcasted to the network. The transactions are stored in blocks in chronological order, and every block contains a hash of the previous block creating a chain of blocks. The first block in the chain, called genesis block, is the only block that does not contain the hash of the previous block. That block is almost always hardcoded into the software.

3.5 Privacy and security

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

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

3.6 Authentication Phase

When EVi wants to use the charging service, EVi and EAG must authenticate each other, and then generate a common session key. The authentication phase with detailed steps as follows

Step 1: EVi inputs identity IDi and password PWi; and calculates $a1=Di \oplus h(IDi||PWi)$, $rEV=h(a1||IDi||PWi) \oplus Ei$, $Ai=h(HIDi||ai)$, $kop=Bi \oplus Ai$, and $C*i=h(HIDi||a1||kop)$. Then, EVi checks whether $C*i=?Ci$. If valid, EVi computes $M1=\{rEV \cdot G,(a1||HIDi||Ti)+rEV \cdot PKEAG\}$, and $M2=h(a1||HIDi||T1)$; and sends {M1, M2, T1} to EAG.

Step 2: After receiving {M1, M2, T1} from EVi, EAG calculates $(a1||HIDi||T1)=(a1||HIDi||T1)+rEV \cdot PKEAG-rEAG \cdot (rEV \cdot G)$ using the private key rEAG. Then EAG computes $M*2=h(a1||HIDi||T1)$ and verifies $M*2=?M2$. If valid, EAG authenticates EVi and calculates $M3=b1 \oplus a1$, $M4=h(IDEAG||a1||b1||T2)$, and session key $SK=h(HIDi||IDEAG||a1||b1)$. Finally, EAG sends {M3, M4, T2} to EVi.

Step 3: When EVi receives {M3, M4, T2} from EAG, it computes $b1=M3 \oplus a1$ and $M*4=h(IEEAG||a1||b1||T2)$, and verifies $M*4=?M4$. If valid, mutual authentication between EVi and EAG has been accomplished. EVi calculates a shared session key, $SK=h(HIDi||IDEAG||a1||b1)$.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

IV. EXPERIMENTAL RESULTS

We shall explain the proposed results found in detail, and then summarize the relationship between these results and the synthetic distributions. We evaluate their performances based on three important criteria: Accuracy, Precision, and Recall.

Accuracy (%):

Table 4.1 Accuracy Results

Data	RSA	ECC	Block Chain
100	72.5	76.7	87.5
200	73.5	77.5	89.4
300	74.5	78.7	90.5
400	75.0	79.5	91.0

Precision (%):

Table 4.2 Precision Results

Data	RSA	ECC	Block Chain
100	72.5	76.7	87.5
200	73.5	77.5	89.4
300	74.5	78.7	90.5
400	75.0	79.5	91.0

Recall (%):

Table 4.3 Recall Results

Data	RSA	ECC	Block Chain
100	77.0	81.5	91.0
200	78.5	82.5	92.4
300	79.5	83.5	93.9
400	80.5	84.8	95.5

Security (%)

Table 4.4Security Results

Data	RSA	ECC	Block Chain
100	71.0	73.8	84.6
200	71.3	76.6	87.8
300	71.5	78.9	89.5
400	71.8	79.5	90.3

Graph Results

Accuracy

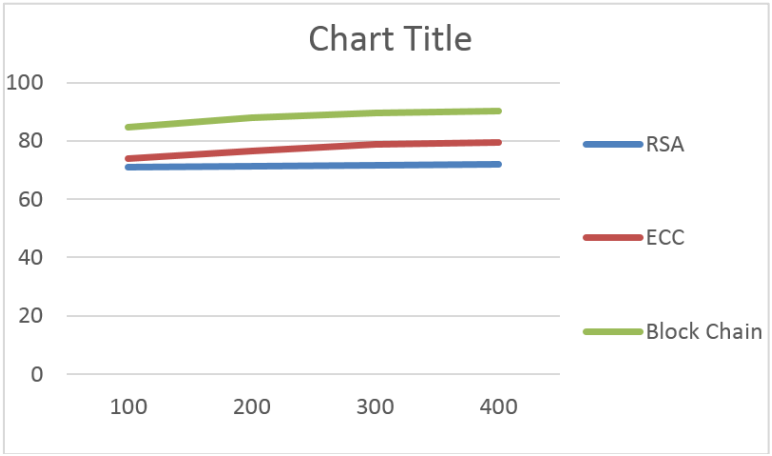

Fig 4.1 Accuracy Results

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 2, February 2020

Precision

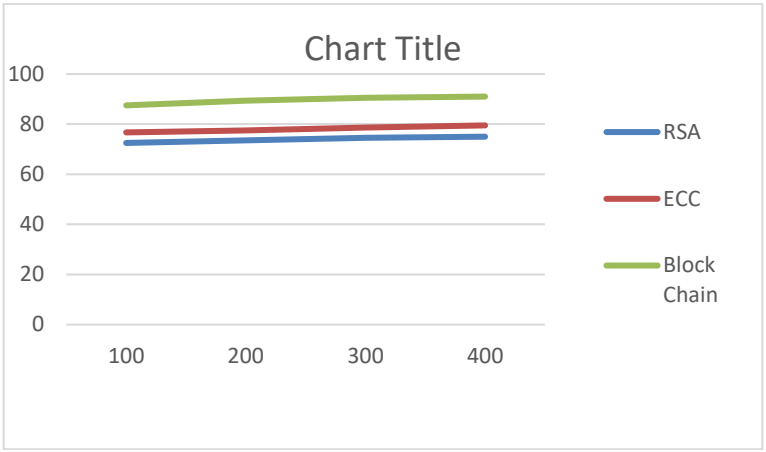

Fig 4.2 Precision Results

Recall

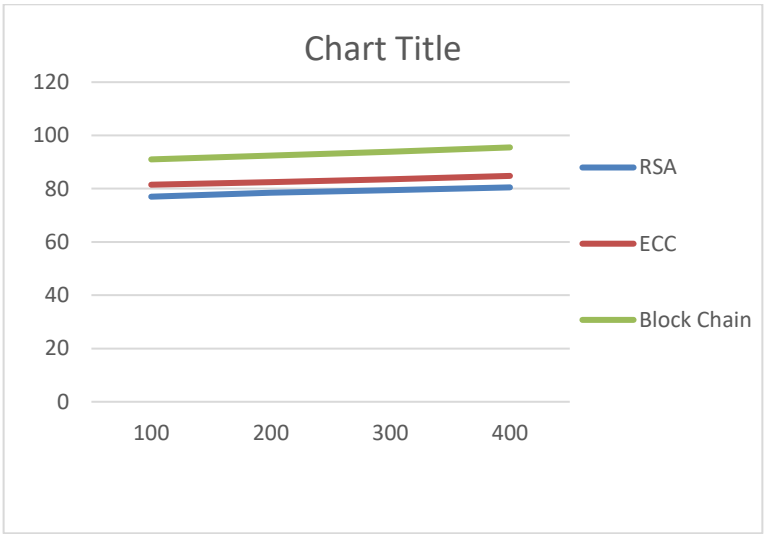

Fig 4.3 Recall Results

Security

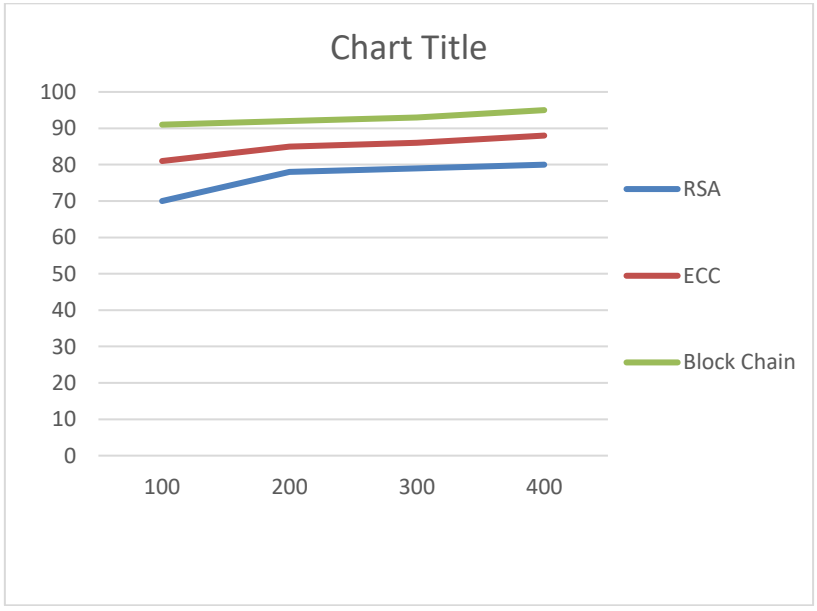

Fig 4.3 Security Results

V. CONCLUSION

We propose a secure charging system for electric vehicles based on blockchain to resolve these security flaws. Our charging system ensures the security of key, secure mutual authentication, anonymity, and perfect forward secrecy, and also provides efficient charging. The protocol design keeps the communication overhead and the amount of data to be stored in the blockchain small, which allows to use existing blockchain technologies such as Bitcoin. The privacy of the protocol is evaluated in an honest-but-curious adversary model. The protocol comes at little communication overhead (at most 38 bytes per block) and is therefore suitable to be used with existing blockchain technologies. Future work will focus on the scalability of the presented approach for a large number of electric vehicles with a high transaction volume and on handling the payment phase in the blockchain.

REFERENCES

[1]. Ben-Sasson E, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M (2014) Zerocash: decentralized anonymous payments from bitcoin. In: Proceedings—IEEE symposium on security and privacy. IEEE, pp 459–474. doi:10.1109/SP.2014.36
[2]. Borges F, Volk F, Mühlhäuser M (2015) Efficient, verifiable, secure, and privacy-friendly computations for the smart grid. In: PES conference on innovative smart grid technologies (ISGT). IEEE, Washington, DC
[3]. Chen D, Kalra S, Irwin D, Shenoy P, Albrecht J (2015) Preventing occupancy detection from smart meters. IEEE Trans Smart Grid 6(5):2426–2434. doi:10.1109/TSG.2015.2402224
[4]. Clarke R, Wigan M (2011) You are where you've been: the privacy implications of location and tracking technologies. J Locat Based Serv 5(3–4):138–155. doi:10.1080/17489725.2011.637969
[5]. Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, GünSirer E, Song D, Wattenhofer R (2016) On scaling decentralized blockchains. In: Clark J, Meiklejohn S, Ryan
[6]. PY, Wallach D, Brenner M, Rohloff K (eds) Financial cryptography and data security: FC 2016 international workshops, BITCOIN, 123 VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers. Springer, Berlin, pp 106–125. doi:10.1007/978-3-662-53357-4_8
[7]. Delmolino K, Arnett M, Kosba AE, Miller A, Shi E (2016) Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. In: Financial cryptography and data security. International Financial Cryptography Association, pp 79– 94
[8]. DESTATIS StatistischesBundesamt: Verwaltungsgliederung am 31.03.2017 (1. Quartal) (2017). https://www.destatis.de/DE/ZahlenFakten/LaenderRegionen/Regionales/Gemeindeverzeichnis/Administrativ/Archiv/Verwaltungsgliederung/Verwalt1QAktuell.html (Online). Accessed 21 April 2017
[9]. Dubois A, Wehenkel A, Fonteneau R, Olivier F, Ernst D (2017) An app-based algorithmic approach for harvesting local and renewable energy using electric vehicles. In: Proceedings of the 9th international conference on agents and artificial intelligence (ICAART 2017), Porto
[10]. Eibl G, Engel D (2015) Influence of data granularity on smart meter privacy. IEEE Trans Smart Grid 6(2):930–939. doi:10.1109/TSG.2014.2376613
[11]. Knirsch.F (2017) Privacy enhancing technologies in the smart grid user domain. IT InfTechnolThemat Iss: Recent Trend Energy Inform Res 1(59):13–22
[12]. Knirsch F, Unterweger A, Eibl G, Engel D (2017) Privacypreserving smart grid tariff decisions with blockchain-based smart contracts. In: Rivera W (ed) Sustainable cloud and energy services: principles and practices. Springer, Berlin
[13]. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C (2016) Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: 2016 IEEE symposium on security and privacy (SP). IEEE, pp 839–858
[14]. Langer L, Skopik F, Kienesberger G, Li Q (2013) Privacy issues of smart e-mobility. In: 39th annual conference of the ieee industrial electronics society, IECON 2013, pp 6682–6687. doi:10.1109/ IECON.2013.6700238
[15]. Lisovich M, Mulligan D, Wicker S (2010) Inferring personal information from demand-response systems. IEEE SecurPriv 8(1):11–20. doi:10.1109/MSP.2010.40
[16]. Lisovich MA, Wicker SB (2008) Privacy concerns in upcoming residential and commercial demand-response systems. In: Clemson power systems conference
[17]. McKenna E, Richardson I, Thomson M (2012) Smart meter data: balancing consumer privacy concerns with legitimate applications. Energy Policy 41:807–814. doi:10.1016/j.enpol.2011.11.049
[18]. Mwasilu F, Justo JJ, Kim EK, Do TD, Jung JW (2014) Electric vehicles and smart grid interaction: a review on vehicle to grid and renewable energy sources integration. Renew Sustain Energy Rev 34:501–516. doi:10.1016/j.rser.2014.03.031
[19]. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system, pp 1–9.https://bitcoin.org/bitcoin.pdf
[20]. Pedersen TP (1992) Non-interactive and information-theoretic secure verifiable secret sharing. In: Advances in Cryptology— Crypto'91, vol 91, pp 129–140. doi:10.1007/3-540-46766-1_9
[21]. Reid F, Harrigan M (2013) An analysis of anonymity in the bitcoin system. In: Altshuler Y, Elovici Y, Cremers AB, Aharony N, Pentland A (eds) Security and privacy in social networks. Springer, New York, pp 197–223. doi:10.1007/978-1-4614-4139-7_10
[22]. SchweizerischeEidgenossenschaft—BundesamtfürStatistik: Die 148 Bezirke der Schweiz am 1.1.2013 (2017).https://www.bfs.admin.ch/bfs/de/home/statistiken/querschnittsthemen/raeumliche-analysen/raeumliche-gliederungen.assetdetail. 466288.html(Online). Accessed 21 April 2017
[23]. Shokri R, Theodorakopoulos G, Le Boudec JY, Hubaux JP (2011) Quantifying location privacy. In: Proceedings—IEEE symposium on security and privacy, pp 247–262. doi:10.1109/SP.2011.18
[24]. Statistik Austria:PolitischeBezirke (2017). https://www.statistik.at/web_de/klassifikationen/regionale_gliederungen/politische_bezirke/index.html (Online). Accessed 21 April 2017
[25]. Unterweger A, Knirsch F, Eibl G, Engel D (2016) Privacypreserving load profile matching for tariff decisions in smart grids. EURASIP J InfSecur 2016(1):1–17. doi:10.1186/ s13635-016-0044-1
[26]. Wood G (2017) Ethereum: a secure decentralized generalised transaction ledger. Tech. rep., Ethereum. https://ethereum.github.io/yellowpaper/paper.pdf
[27]. Yilmaz M, Krein P (2013) Review of charging power levels and infrastructure for plug-in electric and hybrid vehicles and commentary on unidirectional charging. IEEE Trans Power Electron 28(5):2151–2169. doi:10.1109/IEVC.2012.6183208
[28]. Zyskind G, Nathan O, Pentland AS (2015) Decentralizing privacy: using blockchain to protect personal data. In: Proceedings—2015 IEEE security and privacy workshops, SPW 2015, pp 180–184. doi:10.1109/SPW.2015.27.