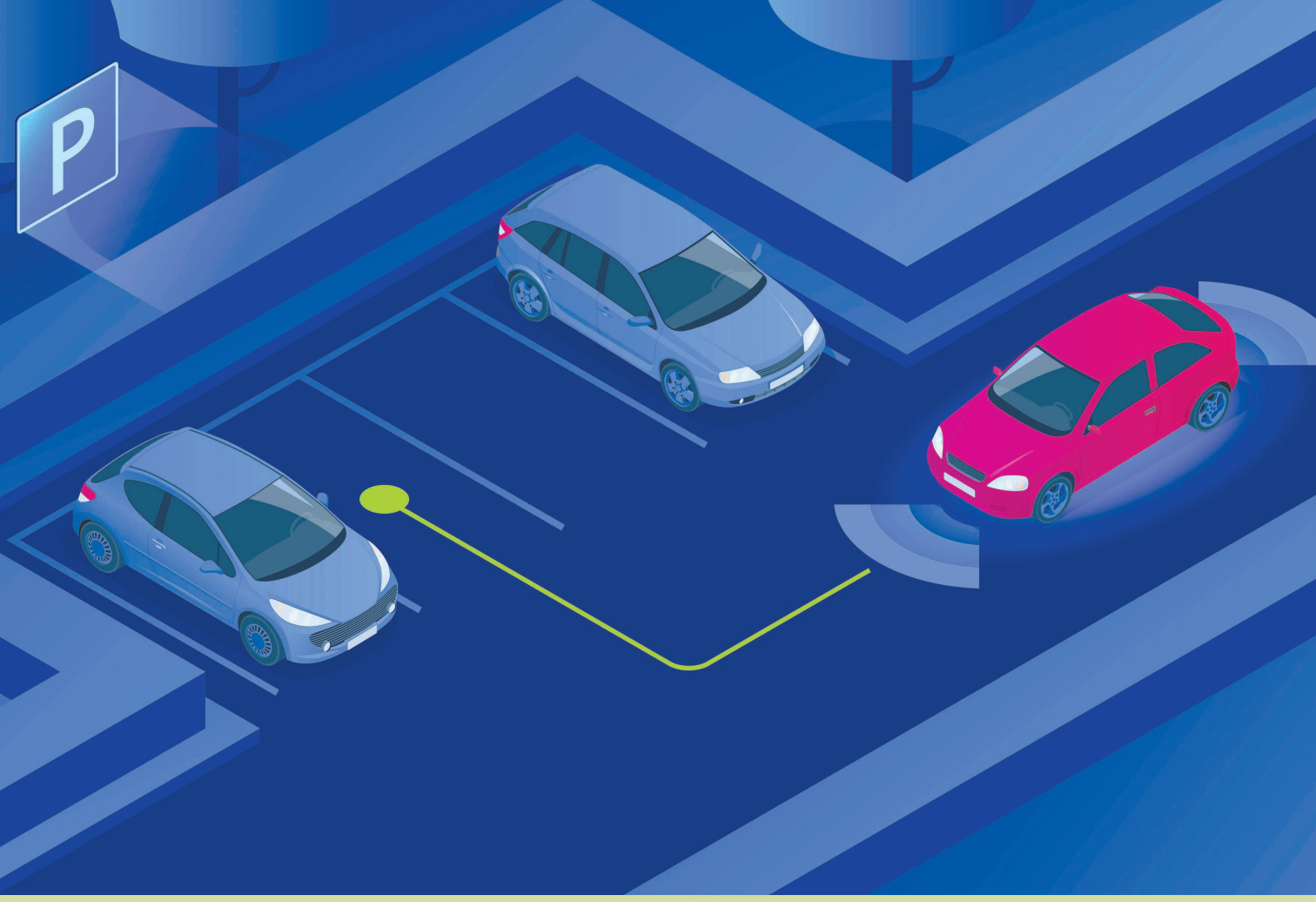

Parking Management

A blockchain-based privacy-preserving system.

In a smart city, smart parking systems generally strive to facilitate the renting of available private parking spaces to vehicle users (just like timesharing). Existing technologies can authenticate and manage parking spaces and vehicles, but they do not address the need to preserve users' privacy. This article presents the framework for a blockchain-based parking-management system designed to preserve the privacy of its users, without relying on a reliable third-party entity. The proposed system integrates BlockChainOpenSource (BCOS) and smart contract technology to share parking spaces.

AN IMPROVED PARKING SYSTEM

Parking is a constant challenge for residents and drivers in densely populated affluent urban areas. People who are driving around searching for available parking spaces are a key cause of traffic congestion, resulting in increasing petroleum consumption and greenhouse gas emissions [1]. In 2017, drivers searching for available parking spaces consumed an estimated 47,000 gal of gasoline and 95,000 h of driving [2]. These amounts highlight the need for an efficient parking system. Existing parking systems generally rely on a center to

By Jiaxi Hu, Debiao He, Qinglan Zhao, and Kim-Kwang Raymond Choo

Digital Object Identifier 10.1109/MCE.2019.2905490
Date of publication: 11 June 2019

Parking systems generally are not designed with security and privacy in mind; any compromise of the system can leak users' private information.

manage parking spaces, including private ones that offer reservation services. The owners of these parking spaces and vehicle users need to authenticate themselves with the parking system provider. Due to logistical challenges that come with managing parking spaces across different cities or regions, providers are usually local. Parking systems generally are not designed with security and privacy in mind; any compromise of the system can leak users' private information.

We introduce a blockchain-based parking system that securely stores user information and manages parking services. Our choice of a blockchain is mainly due to its inherent structure that constructs distributed systems without the need to involve a trusted third party. The success of BCOS, a consortium blockchain derived from Ethereum [3] technology, is noteworthy in that it also is a blockchain-based smart contract system that allows owners to set rules and control access.

The proposed system uses smart contracts to provide the supporting registration and transaction modules for both the parking space user (i.e., renter) and owner. The smart contract also allows the renter to search for a vacant parking space that meets his or her requirements. To preserve users' privacy, we chose a consortium blockchain to check the availability of user information. In this kind of blockchain, the transactions are controlled by privileged nodes, which makes information in the chain either open or visible only to members of the union. This system allows us to overcome geographical restrictions and enables users to make electronic transactions with each other. By omitting a centralized party to control the entire system, we will significantly reduce the costs of system maintenance and recovery. For a blockchain-based system running without an operator, the system data is maintained by all the blockchain nodes.

STATE OF THE ART

BLOCKCHAIN BASICS

Blockchain technology has gained prominence with the popularity of Bitcoin and other applications [4]. A blockchain is a type of distributed electronic ledger that is modeled as a linear sequence of blocks that can store information such as events and transactions. To join the chain, the majority of the network nodes must authenticate the block (with its information) by using consensus. All information is stored in the blocks and updated in chronological order. The blocks can form a data chain, with the head of every block containing its previous block's hash. When a block has been modified, all blocks subsequent to this particular one will also change. In other words, any unauthorized modifications can be trivially detected.

A blockchain generally can be categorized as public, consortium, or private. In a public chain, all peers in the network are equal, in the sense that they have the same access to data in the blockchain. This openness comes at the cost of user privacy. A private chain, on the other hand, is an entirely centralized blockchain in which only the creator can write information to it. This configuration has applications for deployment within an organization. While such a blockchain provides a higher level of privacy than public blockchain, it depends on a reliable center to authenticate the information. In a consortium chain, the effectiveness of blocks and transactions is determined by a group of super peers (i.e., union). If a user wishes to join the chain, most of the union members must approve it. The information in the chain can either be open (to the public) or visible only to members of the union. Thus, such a blockchain can provide privacy to an extent, while implementing partial decentralization.

BLOCKCHAIN APPLICATIONS

Like Bitcoin [4], Ethereum is a popular blockchain-based application. Ethereum has its own electronic currency. However, unlike Bitcoin, in Ethereum peers can create arbitrary decentralized applications by using smart contracts. In other words, Bitcoin locks a financial transaction, whereas smart contracts give system developers more room to explore other types of applications and maximize blockchain use. BCOS [5] is derived from Ethereum and, with it, developers can publish a smart contract to achieve a specific function. *Smart contracts* are broadly defined as a piece of code that can achieve arbitrary rules. Specifically, smart contracts are written in a binary format and stored in a blockchain, which can be executed by blockchain virtual machine [6]. Similarly, our proposed parking-management system requires the ability to write smart contracts for user certification and the sharing of parking spaces. So, we will use smart contracts to store relevant information (e.g., vehicle information), which will be used to administer the system. Blockchain technology is being explored for various Internet of Things applications [7], [8]. In [9], a privacy-preserving contract using a public blockchain and zero-knowledge technology is presented for the sharing economy. The chemical industry used a blockchain to create an electricity-sharing market based on Bitcoin [10], while a decentralized file-storage system using a blockchain and a linkable ring signature was used to implement privacy protection [11], [12].

THE PROPOSED BLOCKCHAIN-BASED SYSTEM

ENTITIES OF THE SYSTEM

Most of the existing smart parking platforms rely on a centralized party to manage the services, users, and data, and do not ensure security and privacy (Figure 1). We explore a blockchain's potential to facilitate the move away from a

centralized to a decentralized system, while offering security and privacy.

Users comprise vehicle drivers and the owners of parking spaces. Drivers can search for and rent vacant parking spaces that meet their requirements. The parking space's owner can publish and modify information that relates to their parking spaces, such as location, availability period (e.g., every Monday), price, and gate code. Both types of users can access the system and contribute data to it. Specifically, users need to provide basic information to the management layer to be authenticated. These types of private information and operations are stored on the blockchain.

The management layer contains trusted entities such as government departments and the certification authority. These entities are generally the issuers of the system and the authentication parties, and they are represented as privileged users of a consortium blockchain. The issuers own the smart contracts and are mainly responsible for designing, developing, initializing, and maintaining the system. Issuers can also publish relevant details and accept clients who request to join the network. The authentication party primarily manages authenticating users and ensuring users' privacy. The authentication party also acts as an arbitration institution in the event of a dispute between users.

In the storage layer, the consortium blockchain works as a distributed database. It continually grows as blocks are appended and linked to the previous one by using a hash. The user information and contract codes are stored on the chain and cannot be modified without detection. Transactions are used to access data from the blockchain repository for modification, analysis, or research, and all operations are traceable through the blockchain to ensure integrity.

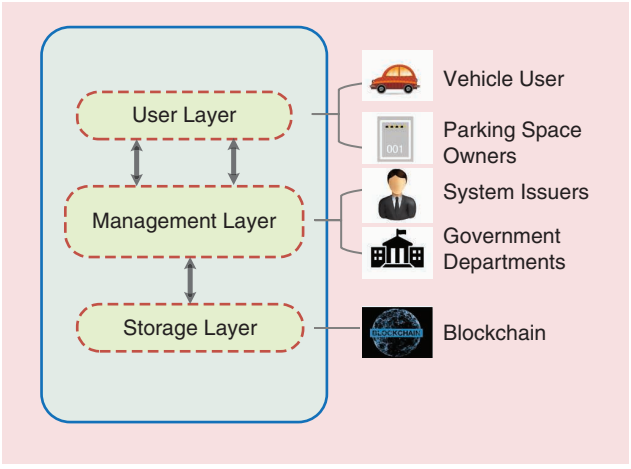

FIGURE 1. The parking-management system entities.

FUNCTION MODULES

The proposed system is deployed on the BCOS smart contracts framework (Figure 2) and its functional module has registration, search and rent, and payment modules.

REGISTRATION MODULE

A BCOS account represents each user, which is associated with a unique private key. In the registration phase, users submit their identities to the privilege nodes of the consortium blockchain

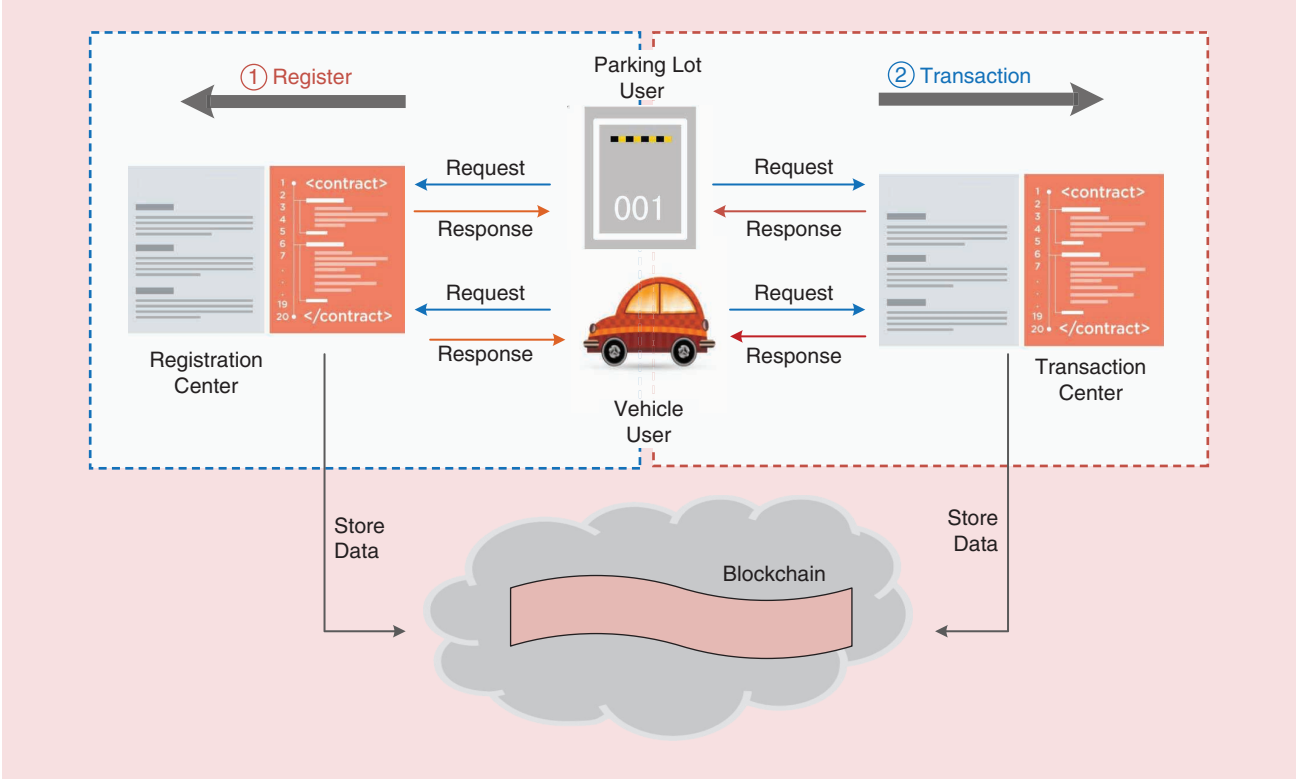

FIGURE 2. The overall system function module.

The proposed system is deployed on the BCOS smart contracts framework and its functional module has registration, search and rent, and payment modules.

and then each privilege node verifies the identities it received. The user can obtain a new address for each new transaction, so an adversary could not reveal the user's identity by tracking addresses. After users enter the network, they need to provide their basic information to the certification authority through the smart contract, which is stored on the blockchain.

The smart contract acts as the blockchain's interface to manage identities and attributes. For registration, it can record basic attributes of users and lock them on the blockchain. Vehicle users and parking space owners have different user type and input different information. The attributes of vehicle users include user identification (ID), car ID, and user address. For parking space owners, these attributes include parking ID, location, period of availability, price, and owner address. During registration, the owner needs to provide only his or her user ID and parking ID, and the other attributes are set to null.

The smart contract also provides interfaces that allow users to search, modify, or delete their information. After registering, the owners can publish and modify their information through the smart contract. For example, owners can update their availability period and price. The identity of each user is hidden behind a string of address characters, and only the privilege peers of the management layer are authorized to check this private information.

SEARCH AND RENT MODULE

This module allows vehicle users to search for available parking lots that satisfy their requirements by sending transactions that contain information, such as location and time, to the smart contract. If the administrator peers verify the sender of the transaction, the contract will then traverse the parking lot lists and return a list of suitable parking ID with their addresses. When the vehicle user wishes to rent an available parking space, he or she pays a deposit (e.g., BCOS cash, a currency used in BCOS) to the contract account. After the user completes the payment and leaves the parking space, the deposit will be returned to his or her account. Also, the status of the selected parking space will be updated to say locked or unavailable. This will avoid a double-booking situation, which is similar to double spending in Bitcoins.

BCOS has two kinds of accounts, external and contract. The former is similar to Bitcoin accounts, while the latter is used to hold smart contracts. While the contract account also has functions provided by the external account, the deposit is stored in the contract account, which can be accessed only by using the administrators' private key. BCOS also provides a one-time pad function implemented by a smart contract to help users reveal their identity. This function allows users to create a new address each time that they want to make a transaction with another contract or user.

PAYMENT MODULE

To invoke the money-transfer function, the payment will be processed. To transfer money, a vehicle user needs to construct a transaction with a set of inputs and a set of outputs. Each input consists of the sender's public key *pk_s* and secret key *sk_s*, the receiver's public key *pk_r*, and some BCOS cash. The *sk_s* is used to sign the transaction and the *pk_r* is used to encrypt the transaction. Thus, only the user with the right *sk_s* associated with *pk_r* can claim the payment.

As in Bitcoin, each input has a reference to a previous transaction output. There are three types of outputs: the recipient of the payment, change, and transaction fee. The transaction fee is given to the miner who publishes the transaction to the chain. The money-transfer function is used during both the rental and payment processes. During payment, after the vehicle user leaves the parking lot, he or she must transfer the correct amount of money to the owner's payment address through a BCOS money-transfer contract to have their deposit returned.

The three function modules are executed via sending transactions, which are signed using the user's private key. Thus, every operation will cost a small amount of BCOS cash, payable to the miner of the blockchain network. The operation will be stored on the blockchain to prevent tampering, falsification, or denial as every point in the chain network owns a copy of the full database.

SYSTEM IMPLEMENTATION

We construct a BCOS consortium blockchain, forming a chain and establishing a number of privilege peers (i.e., city administration and issuers). Solidity implements the smart contracts. We also use Truffle [13] to compile the smart contracts to binary codes and publish the contracts to the blockchain. To connect to a BCOS client's JSON-encoded remote procedure call protocol, we use JavaScript to develop a client that allows users to send and receive information in the BCOS. The client allows users to register and modify attributes from the blockchain, as well as to search or rent available parking spaces that satisfy the user's requirements. The client also provides an interface for users to pay money via BCOS cash. Before payment, vehicle users prepay some BCOS cash as the deposit, which is locked.

DISCUSSION

Our proposed system ensures the anonymity of both vehicle users and the parking space owners because only the amount of the transaction is open to the public, and the user's address is generated by his or her public key. A user can derive multiple addresses from the private key by using secure cryptographic algorithms. Thus, to conceal users' information (i.e., privacy), the BCOS platform provides a one-time pad mechanism and a group-signature mechanism [14]. A one-time pad means that users will receive a new address for each new transaction, so the adversary cannot reveal the user's identity by

tracking these addresses. A group signature mechanism reduces the connection between the identity of users and transactions, while the privilege node can track the user's identity. These mechanisms can prevent our system from undergoing statistical attacks. In other words, a passive attacker will not be able to analyze the behavior and track the users by monitoring and analyzing blockchain data.

Using a digital signature in the blockchain ensures data integrity, any modification will be detected. Specifically, data from the registration, search, rent, and payment processes are signed by the user's private key and recorded in the leaf nodes of the Merkle tree [6]. The latter is a hash tree in which every leaf node is labeled with a data block, and every nonleaf node is labeled with cryptographic hash of the labels of its child nodes. The hashes of two adjacent leaf nodes are recorded in the parent node. The block retains the process record of all the registration and transaction modules, which can provide the evidence required for subsequent tracking or auditing.

A centralized system allows the implementation of a paid parking schema between vehicles and parking space owners via existing mobile network technologies, which requires a central database to store user information and record user operations. However, such systems generally do not scale well, despite using cloud services. All user data stored in a central peer is a known weakness such as the single point of attack or failure. Therefore, in our proposed blockchain-based system, we retain the features of existing systems by using decentralized management and storage structure. As previously discussed, our system facilitates information sharing between different user nodes, in which each network node has a full copy of the block data and increments chronologically. The nodes can also update their data by accessing adjacent nodes directly, significantly improving the efficiency of information sharing between vehicle users and parking space owners. Due to the inherent nature of the consortium chain, our proposed framework can greatly protect the privacy of users. In addition, all data and business logic functionalities and access control are achieved using smart contracts, which reduce the cost of system development and maintenance.

CONCLUSION

We have discussed a blockchain-based parking system that facilitates the sharing of paid parking resources between the owners of parking lots and users. Unlike existing parking systems, we removed the need for a trusted third-party entity because the consortium chain ensures user privacy. This approach allows scaling up and down, without geographical restrictions. BCOS cash can be used for transactions with each other, every transaction can be traced, and other virtual payment can be used. Future research includes a full-fledged system and collaborating with a carpark operator, to implement and evaluate the system.

ACKNOWLEDGMENTS

This work was supported by the National Key Research and Development Program of China under grant 2017YFB0802504 and by the National Natural Science Foundation of China under grants 61572370 and 61572379.

ABOUT THE AUTHORS

Jiaxi Hu (whojx13@163.com) is pursuing her master's degree in the School of Cyber Science and Engineering, Wuhan University, China.

Debiao He (hedebiao@163.com) is a professor in the School of Cyber Science and Engineering, Wuhan University, China.

Qinglan Zhao (zhaoqinglan@foxmail.com) is an associate professor at Xi'an University of Post and Telecommunications, Xian Shaanxi, China.

Kim-Kwang Raymond Choo (Raymond.Choo@unisa.edu.au) holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio.

REFERENCES

[1] Y. Geng and C. G. Cassandras, "New 'smart parking' system based on resource allocation and reservations," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 3, pp. 1129–1139, 2013.

[2] Q. G. K. Safi, S. Luo, C. Wei, L. Pan, and Q. Chen, "PIaaS: Cloud-oriented secure and privacy-conscious parking information as a service using VANETs," *Comput. Netw.*, 2017.

[3] Ethereum Homestead, "Ethereum Homestead documentation." Accessed on: 2017. [Online]. Available: http://www.ethdocs.org/en/latest/

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Bitcoin, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[5] Blockchain Open Source Platform, "BCOS whitepaper." Accessed on: 2017. [Online]. Available: https://github.com/bcosorg/whitepaper

[6] A. Moinet, B. Darties, and J.-L. Baril, Blockchain based trust & authentication for decentralized sensor networks. 2017. [Online]. Available: https://arxiv.org/abs/1706.01730

[7] J.-H. Lee and M. Pilkington, "How the blockchain revolution will reshape the consumer electronics industry," *IEEE Consum. Electron. Mag.*, vol. 6, no. 3, pp. 19–23, 2017.

[8] S. Mayra and R. Deters, "Blockchain as a service for IoT," in *Proc. IEEE Int. Conf. Internet of Things, Proc. IEEE Green Computing and Communications, Proc. IEEE Cyber, Physical and Social Computing,* and *Proc. IEEE Smart Data*, 2016, pp. 433–436.

[9] X. Lei et al., "Enabling the sharing economy: Privacy respecting contract based on public blockchain," in *Proc. ACM Workshop on Blockchain, Cryptocurrencies and Contracts,* 2017, pp. 15–21.

[10] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Appl. Energy*, vol. 195, pp. 234–246, June 2017.

[11] H. Kopp, D. Mödinger, F. Hauck, F. Kargl, and C. Bösch, "Design of a privacy-preserving decentralized file storage with financial incentives," in *Proc. IEEE Eur. Symp. Security and Privacy Workshops,* 2017.

[12] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, 2018.

[13] Truffle, "Truffle framework." Accessed on: 2017. [Online]. Available: http://truffleframework.com/docs

[14] T.-H. Ho, L.-H. Yen, and C.-C. Tseng, "Simple-yet-efficient construction and revocation of group signatures," *Int. J. Found. Comput. Sci.*, vol. 26, no. 5, pp. 611–624, 2015.