Received: 11 May 2020 | Revised: 19 July 2020 | Accepted: 9 August 2020 | Published on: 5 October 2020

DOI: 10.1002/spy2.131

SURVEY PAPER

WILEY

An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms

Mahdi Daghmehchi Firoozjaei | **Rongxing Lu** | **Ali A. Ghorbani**

Canadian Institute for Cybersecurity, University of New Brunswick, Fredericton, New Brunswick, Canada

Correspondence
Ali A. Ghorbani, Canadian Institute for Cybersecurity, University of New Brunswick, 46 Dineen Drive, Fredericton, NB, Canada, E3B 5A3.
Email: ghorbani@unb.ca

Abstract

Blockchain-based applications provide many promising opportunities to overcome the challenges associated with the Internet of Things (IoT) ecosystems (eg, centralized architecture, data integrity, and reliability). In particular, blockchain technology offers many desirable features for IoT infrastructures, such as decentralization, trustworthiness, trackability, and immutability. However, while logging all transactions in a distributed blockchain ledger provides transparency, it also makes it possible to compromise user's privacy, thus posing a grand challenge to IoT architects and implementers. Over the past years, a set of solutions have been proposed for various scenarios, to address these privacy issues. In this paper, we survey these solutions, classify, and analyze their advantages and disadvantages. We also introduce an evaluation framework to evaluate the quality of the privacy-preserving based on an adjustable weighting scheme. Finally, we rate the analyzed solutions based on their privacy ranks, and hope our evaluation can shed light on the future design of privacy-preserving solutions applicable for blockchain-based IoT platforms.

KEYWORDS

blockchain-based application, internet-of-things, privacy rank, privacy-preserving

1 | INTRODUCTION

Blockchain-based applications have been widely employed to address issues such as intensive centralizing, scalability, security, and reliability with Internet of Things (IoT) systems. IoT systems are characterized by multi-party ecosystems, with data exchange among different devices and parties.[1] The tamper-proof, immutability, and transparency features of blockchain make members able to trace all transactions (past and present), which provides a reliable way to identify data leakages or manipulation.[2-4] The integrity of huge amounts of IoT sensory data can be assured in a blockchain-based distributed cloud from sensor to service with no need to rely on trusted third parties.[5] Data provenance tracking can be provided by programmable smart contracts, which act as the policy evaluation entities and event loggers, and allows users to check all data transfers (eg, acquired automatically from IoT devices) and usage transactions providing assurance that only transactions conforming to the contract policies are authorized and registered in the blockchain.[6]

IoT system restrictions, namely resource-constrained devices, low computational power, and limited capacity and bandwidth limit blockchain-IoT applications. For this reason, different projects, such as Maru,* Riddle&Code,† IOTA,‡ and IBM's device democracy, aim to fit blockchain to IoT platforms, to achieve interoperability, trust machine-to-machine (M2M) interaction, data integrity, and device-based permission. Maru sensor platform, developed by chain of things

(CoT),§ is a hardware-as-a-service solution (HaaS) to address IoT's issues with identity, security, and interoperability in a multi-layer structure.[7] A cryptographic tagging solution for blockchain has been described by Riddle & Code in which IoT devices are given a trusted digital identity for trustful M2M interactions.[2] IBM describes a device democracy network[8] where each IoT device functions as a self-contained business, sharing capabilities and resources, such as compute cycles, bandwidth, and power, with other devices. IOTA is a blockless ledger providing fast transaction settlement and data integrity for the IoT industry based on the Tangle ledger. The Tangle is a directed acyclic graph (DAG) for storing transactions.[9] The transactions are the only data storage units in IOTA and are issued by nodes of the Tangle graph. To issue a transaction, users must contribute to the network's security and approve two other transactions.[9] Transactions are verified in parallel and accepted by Tangle almost instantly, which provides IOTA high transaction rate capacity.[5]

Despite the features and benefits of blockchain-IoT, the possibility of privacy disclosures in the blockchain is still a worrisome issue for IoT users. IoT networks are data-centric having a large number of devices generate and upload private data such as sensory, personal activities, and medical data.[5] Uploading such data to the blockchain with its distributed ledger directly opens the door to some or all of it being exposed via the linking attack[10,11] and traffic correlation.[12] The paparazzi-minded of the world might stage attacks on blockchain-IoT to automatically track patients and hospital's biomedical devices in a smart healthcare system,[13] monitor users' location and movement in IoT smart transportation systems,[14,15] and characterize users' power consumption in an IoT smart grid.[16,17] Much information can be gleaned from a single transaction. For instance, in a typical power transaction in an IoT network, a consumer needs to publish his/her own demand or supply to the blockchain. Thus, depending upon the conditions, the trading partners as well as all engaged devices are identified, authenticated, and connected through cloud servers.[18]

It has been shown that the basic privacy feature of blockchain, namely pseudonymous IDs, is insufficient to preserve privacy. Users are identifiable by mapping virtual identities in the transaction graph.[19,20] Linking digital assets and tracing transactions are possible by address mapping[21] and traffic correlation.[22,23] Several blockchain-based solutions have been introduced to address the privacy issues of blockchain-IoT systems. Generally, these solutions are based on peer-to-peer (P2P) transactions in the blockchain framework and can be classified into four classes, viz., obfuscating data or identity, trust grouping, secure data separation, and cryptographic methods. Different features are provided in each class depending on the targeted privacy issue, priority, and the techniques used.

In this paper, we review the privacy concerns of IoT users of blockchain-based applications. We classify the various solutions based on the aforementioned classes. Overall, our research is geared toward a design evaluation framework that facilitates quality evaluation of the privacy-preserving solutions. We define the evaluation criteria in two groups to indicate the advantages and disadvantages of a protection solution, namely privacy features and privacy risks. We introduce a weighting scheme to rank the individual criterion to indicate their influence on privacy protection. This weighting scheme can be adjusted based on privacy priority or evaluation purposes. This flexibility makes evaluators able to set the criterion based on their purposes. To represent the numeric value associated with each evaluated privacy-preserving solution, we introduce the privacy rank. The privacy rank of a privacy-preserving solution is the resultant of the provided privacy features and the created privacy risks.

The main contributions of this article are as follows:

- We classify the privacy-preserving solutions for blockchain-based IoT applications, and give a detailed analysis of the privacy protection offered by each solution. Our classification and analysis will be helpful for security engineers who want to preserve user's privacy in the blockchain-based IoT systems.
- We define an evaluation framework to calculate the quality of the protection provided by a privacy-preserving solution based on introduced privacy features and privacy risks. We introduce the privacy rank to show the overall quality of the privacy-preserving provided by a protection solution.

The rest of this article is organized as follows. In Section 2, we review blockchain-based IoT applications and explain the differences between blockchain-IoT implemented at the service layer and at the end-device level. Section 3 describes privacy concerns of IoT users in blockchain-based applications. In Section 4, we present our classification of the privacy-preserving solutions and review each one. Our proposed evaluation framework is introduced in Section 5 and the evaluation results and analysis are explained in Section 6. Finally, we conclude the paper in Section 7.

2 | BLOCKCHAIN-BASED IOT APPLICATIONS

Since IoT ecosystems are data-centric and consist of devices equipped with data-collecting sensors, most applications require special-purpose centers to store and analyze a hough amount of raw data. As shown in Figure 1, an IoT ecosystem

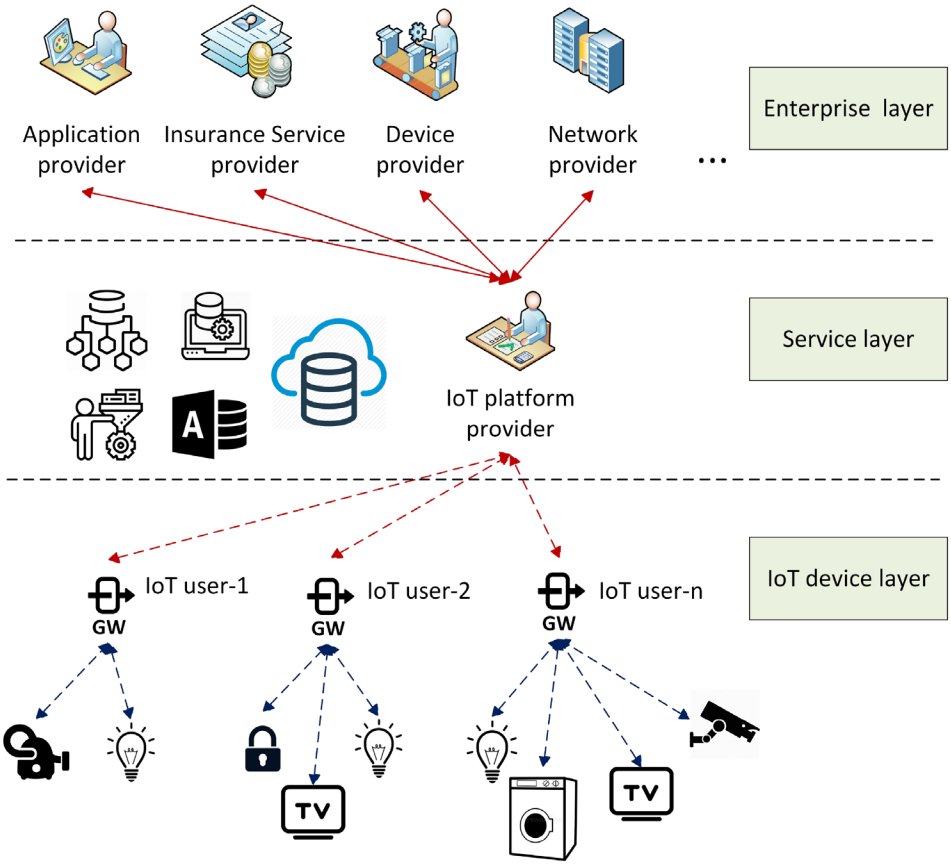

FIGURE 1 IoT ecosystem involves three layers of IoT device, service, and enterprise layers

can be divided into three layers, namely the IoT device layer, the service layer, and the enterprise layer. The device layer consists of physical components, such as IoT end-devices, gateways, and network connections. Normally, IoT devices are CPU, RAM/ROM, and/or I/O-constrained and have embedded low-power crypto-accelerators for security purposes.[24] The service layer has hardware and software for such things as data flow tools, stream processing, data storage, and external access. Access control and interconnections to other IoT platforms are done at the service layer. The enterprise layer is a collection of business applications and consists of service management technologies.

Blockchain technology can be employed at either the device level or at the service layer. Capabilities vary depending on where it is employed. Due to the computational and storage limitations of IoT devices, implementing blockchain at the service layer provides more flexiblity. Deploying at the service layer requires less modification to current platforms, like upgrading or reprogramming IoT devices. Furthermore, the sensory data gathered from IoT devices can be aggregated and analyzed by an agent, such as IoT gateway, to be packed into a blockchain.[5] Blockchain functions, that is, block generating and verifying, which are resource consuming, can be better performed on the service layer. In comparison to the simplicity of the blockchain-as-a-service (BaaS) model, employing blockchain on IoT end-devices is more complicated and distributing blockchain data on IoT devices is more vulnerable to distributed denial of service (DDoS) attacks.

On the other hand, deploying blockchain directly to IoT end-devices improves data integrity. Performing P2P identity authentication between IoT devices based on the distributed ledger improves the security of trust management for authentication.[25,26] In the BaaS model, the agent has a proxy role between IoT devices and the blockchain network. The trustworthiness and reliability of the agent are the worrisome issues. With this view, the single point of failure, man-in-the-middle (MitM) attack, tampering, and data injection are possible with an untrusted or compromised agent in the blockchain as a service deployment for IoT.[5]

2.1 | BaaS for IoT

In this implementation, the blockchain provides a service layer and IoT end-devices are not blockchain members. Normally, the IoT gateway is a member of the blockchain and collects the data from IoT end-devices to generate transactions.

In the smart home model introduced by Dorri et al,[27] a high resource device, known as the miner, controls all IoT devices. The miner centrally processes incoming and outgoing transactions to and from the smart home. IoT devices use the keys generated by the miner and all collected sensory data are managed by the miner in local storage. The miner implements the core function of blockchain, that is, authenticate, authorize, or audit transactions, and mining transactions into blocks.[5,27]

Ozyilmaz et al[28] proposed a blockchain-based P2P network of IoT gateways to store data and code fragments. In this network, the data is stored in a torrent-like distributed file system. IoT gateways operate as the blockchain nodes and also store and route data. IoT end-devices send their data to the gateway in an always-listening network based on LoRa¶ protocol. In the blockchain-based credit-sharing framework introduced by Firoozjaei et al[29] for electric vehicles (EVs), an EV joins the blockchain and plays a bridge role between other EVs and blockchain members. In the blockchain-based model introduced in Reference 30 the agents, running on IoT gateways, collaborate to detect DDoS attacks from IoT botnets. The IoT gateways, known as agents, employ a blockchain to securely reach a consensus about the information metrics that are locally calculated at the gateways of the system. The gateways' computational and storage capabilities are used to give more flexibility in software installation than IoT devices do.

Offloading the mining process is used by some solutions to circumvent resource limitations in networks with limited computational power, for example, IoT devices. Xiong et al[31] proposed supporting mobile blockchain applications where the mining process can be offloaded to a third party offering edge computing services. Exploiting cloud computing has been suggested to address storage limitations and mitigate latency issues with blockchain-IoT applications. To address storage issues, Sharma et al[32] proposed a blockchain-based distributed cloud architecture for IoT networks. The intermediate control nodes, enabled with a software-defined network (SDN), are located at the edge of the IoT network for computing purposes. The SDN technique can be used to move the computing resources to a fog layer at the edge of the IoT network to have a minimal end-to-end delay between IoT devices and computing resources. IoT data streams are gathered, classified, and analyzed at the edge of the network and the distributed cloud. In this model, IoT devices have no role in the blockchain and all blockchain functions are performed at the cloud layer with high storage capabilities.

2.2 | IoT-involved blockchain

Implementing a blockchain at the IoT device layer requires IoT devices to be able to provide blockchain functions, such as transaction generating, verifying, and even block mining. A blockchain vehicle ad-hoc network is an example of an IoT-involved blockchain. Leiding et al[33] introduced a blockchain-based vehicular ad-hoc network having a decentralized and self-managed VANET system. Due to the low computational power of most IoT systems, all blockchain functions cannot be done by the end-devices. Therefore, entities with different capabilities are needed to provide blockchain functions, that is, lightweight node, full node, and miner. In this case, miners mine transactions and pack them into blocks. The miners need to have enough computational power and capacity for storage and computation. The full nodes require massive storage to store all blockchain blocks and a modest amount of computation power. Full nodes do no mining processes. The IoT end-devices run as lightweight nodes generating transactions and storing block headers, but are not able to mine.[5]

The lightweight nodes require minimal storage capacity and computational power. In the blockchain-based IoT devices' firmware updating mechanism, suggested by Yohan et al,[34] a lightweight node does not participate in the mining process and only needs to synchronize data stored in the local ledger with that from the public ledger. The lightweight nodes (IoT devices) participate in access control management by generating private keys or registering with a certificate authority (CA).[5] The Hyperledger Fabric** introduces a blockchain with an execute-order-validate architecture in which each transaction needs only be executed by the subset of the peer nodes (eg, IoT devices) necessary to satisfy the transaction's endorsement policy. The enrolled nodes maintain their private keys for access control. In the Hyperledger Fabric-based blockchain proposed by Li et al[25] for IoT, two groups of nodes are introduced to manage the blockchain consensus, namely consensus nodes, and non-consensus nodes. The consensus nodes participate in the blockchain functions of block generating, verifying, and broadcasting, and the nonconsensus nodes are lightweight IoT devices. In this model, each node generates a key pair and needs to be enrolled with a CA in order for authentication.

The low storage capacity of lightweight IoT devices prevents them from storing all blockchains.[35] To address this limitation, Kim et al[36] proposed a storage compression consensus (SCC) algorithm, which compresses a blockchain on each device. The SCC improves existing voting-based consensus algorithms for private blockchain-based IoT networks.

With this algorithm, a node can reduce the size of the blockchain by hashing the previous block. The compressed block and the next block would be used for consensus.

3 | PRIVACY ISSUES

Due to the distributed nature of blockchain, the availability of transactional data in the shared ledger makes blockchain users susceptible to privacy attacks, such as linking attacks or malicious data mining. In a linking attack, an attacker tries to find some facts linked to a user's private data.[37,38] To characterize sensitive information, the attacker monitors users' transactions for a period of time. The malicious data miner is able to extract private information related to the users from the information available in the shared ledger. This information can be used for user profiling and behavior prediction. For instance, marketing firms could use behavior and appliance usage information for unwanted or malicious purposes, for example, directed advertisements.[39] To counter these attacks, several privacy approaches have been proposed to decouple users' pseudonymous identities from the specific transactions they make, thereby preventing attempts to link transacting parties based on data that appears in the blockchain.[23]

In this section, we introduce the possible privacy issues in blockchain-IoT applications. Basically, privacy challenges with users of blockchain-based IoT applications can be classified as either human-centric or device-centric. As shown in Figure 2, each class of these privacy challenges consists of different issues, which are explained as follows.

3.1 | Human-centric privacy issues

3.1.1 | User profiling

User profiling is a technique to characterize a user's behavior, for example, daily activities or interacting partners, and can be used to visualize user profiles, department profiles, organizational profiles, and multi-dimensional profiles.[40] In a smart grid, to match consumption on the power with available supply, the patterns of consumers' demands are extracted. Smart IoT devices, for example, smart meters, facilitate pattern extracting from power consumption. Blockchain-based applications for power systems make it easier to characterize consumers' power consumption which leads to user profiling. Albert et al[41] showed the possibility of consumer's thermal profiling based on temperature-dependent consumption such as air conditioning or heating. Power consumption related information available in the blockchain such as amount, manner, and time, can all lead to user profiling.

At the same time, predicting consumers' future usage is very useful and legitimate for demand management in a smart grid. Smart grid resource management, based on the current usage and the future demand, needs to monitor and predict consumers' future usage. In a blockchain-based IoT system, a consumer's future behavior can be predicted based on the information reported by the smart devices to the blockchain. For instance, a smart home may know the absence of the inhabitants, for example, based on their calendar, and it may trade energy future accordingly.[42] Publishing this information in the shared ledger makes it possible to infer an IoT users' future activities, for example, energy consumption or meeting a friend.

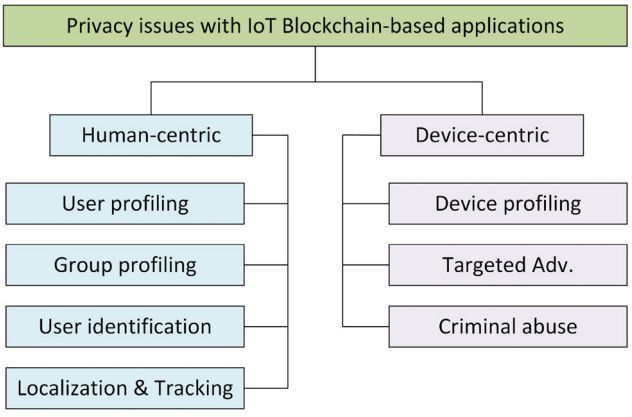

FIGURE 2 Privacy issues with the blockchain-based IoT applications

3.1.2 | Group profiling

In group profiling, an adversary uses IoT user profiles to model a group.[43] Group profiling is based on heterogeneous information associated with a group of IoT users who show similar interests, requirements, or similar behaviors/activities. The information available in the shared ledger is a good source of information which can be used directly or indirectly for profiling. The peer-to-peer (P2P) or device-to-device (D2D) transactions logged in blockchain ledger can be mined to extract the relationship and similarity factors for profiling a group of IoT users.

3.1.3 | User identification

Basically, the anonymity of users and transactions in the public permissionless blockchains (eg, Bitcoin) relies on pseudonyms.[44,45] Traffic analysis can easily identify a transaction's source and infer the trading rules of the pseudonyms by the transaction records in the ledger.[46,47] Based on this, an adversary is able to identify the user by monitoring and analyzing different transactions sent by or destined to the user. Meiklejohn et al[48] have shown that it is possible to identify Bitcoin users by clustering users' different addresses.

3.1.4 | Localization and tracking

The ability to determine and record an IoT user's location through time and space leads to localization and tracking threats. IoT technologies (eg, smart wearable devices) not only support the development of location-based services (LBSes) to improve their accuracy[49] but also expand those services to indoor environments for smart retail.[50] In blockchain location-based applications, such as EV charging and vehicle-to-vehicle payment (V2VP), the shared information of the interactions between smart things and the systems leave data trails which compromise a user's location privacy. In blockchain-based applications for electric vehicle charging (EVC) the location of the EVs and the charging station are used for finding charging stations and path routing. Detecting a user's position, tracking vehicles, and exposing a user's actual energy need are possible based on the information in the shared ledger.[51]

3.2 | Device-centric privacy issues

3.2.1 | IoT device profiling

As IoT devices become more connected, more private data will be shared to authorized and unauthorized entities.[52] Although the smart contracts in blockchain set the access rules, conditions, and time to restrict the control and access to the shared data,[53] there are enough data for device profiling. The information related to the ownership, identity, relationship attribute, capabilities, and features of IoT devices available in the blockchain, enable partners to identify and profile IoT devices related to a specific IoT user. For instance, in the blockchain-based authentication model introduced for IoT in Reference 25, the identity information of IoT devices needs to be registered in the blockchain every time a new device is added. In this model, each device's ID, public key, hash of critical data, and other information are stored in the shared ledger and all nodes need to be enrolled on the CA server. Relying on an intermediary center for authentication opens the possibility of device profiling.[35]

Non-intrusive load monitoring (NILM) systems collect power consumption data from smart devices (eg, advanced metering infrastructure [AMI]) and process to determine users' electrical load schedules. Typically, it is done by disaggregating the data stream available in the blockchain into individual load signatures and matching each signature with reference signatures stored in a database. NILM can be used to identify specific IoT device/appliance brands and might even identify malfunctioning appliances.[39]

3.2.2 | Targeted advertising

User's private data logged in the blockchain could be used by other members (eg, a service provider or a utility's partner) to send customers targeted advertisements. Targeted advertising based on user's in-home activities transgresses the current

norms of information flow and creates new privacy concerns. IoT user's transaction history available in the blockchain opens the door to target advertisements, such as device repairs or upgrades.[39] This information indicates IoT user's properties (eg, a particular IoT device), which can be used for advertising. Based on this, we classify it as a device-centric privacy issue, though the IoT user is targeted for advertising.

3.2.3 | Criminal abuse

Availability of device-related data (eg, power consumption data) from the blockchain makes criminals able to monitor and extract IoT devices' transactions and traffic. They could process data to compile lists of household IoT devices, which would lead to the proliferation of malware targeting IoT devices or some property crime.[39,54,55] The vulnerabilities of IoT devices can be used by IoT malwares to launch a wide range of distributed DDoS attacks.[55] The Mirai,[56] Bashlite,[57] Luabot,[58] and Hajime[59] are examples of botnet attacks launched exclusively by IoT devices, which have been compromised by IoT malwares.[54,60]

3.3 | Privacy issues with IoT blockchain implementation modes

The aforementioned privacy issues are potentially feasible in both modes of blockchain implementation in IoT systems, namely, BaaS and IoT-involved blockchain applications. In BaaS applications, the blockchain provides a service layer and its transactions are originated by or destined to IoT users. In these applications, human-centric privacy issues, for example, user profiling, are more challenging. Since IoT end-devices provide blockchain functions in the IoT-involved blockchain implementations, device-centric privacy issues are more challenging for IoT users. Transactions generated by IoT end-devices, logged in the blockchain, may reveal information related to the ownership, devices' types, identity, capabilities, and features.

4 | CLASSIFICATION OF PRIVACY-PRESERVING SOLUTIONS

Depending on the application and the importance of privacy, several solutions have been introduced to preserve IoT user's privacy in blockchain-based applications. Privacy-preserving solutions can be classified into four classes, namely obfuscation, cryptographic, trust group, and data isolation. Figure 3 shows the classification of the protection solutions. In the obfuscation class, which includes data hiding, rout hiding, and ephemeral pseudonyms solutions, the anonymity of user and transaction untraceability are the privacy goal. Data confidentiality, transaction unlinkability, and untraceability are the main privacy goals of the cryptographic class. The solutions of key management, zero-knowledge, ring signature, and multisignature are in this class. To share data in the trust group class, at first a trusted link must be created among

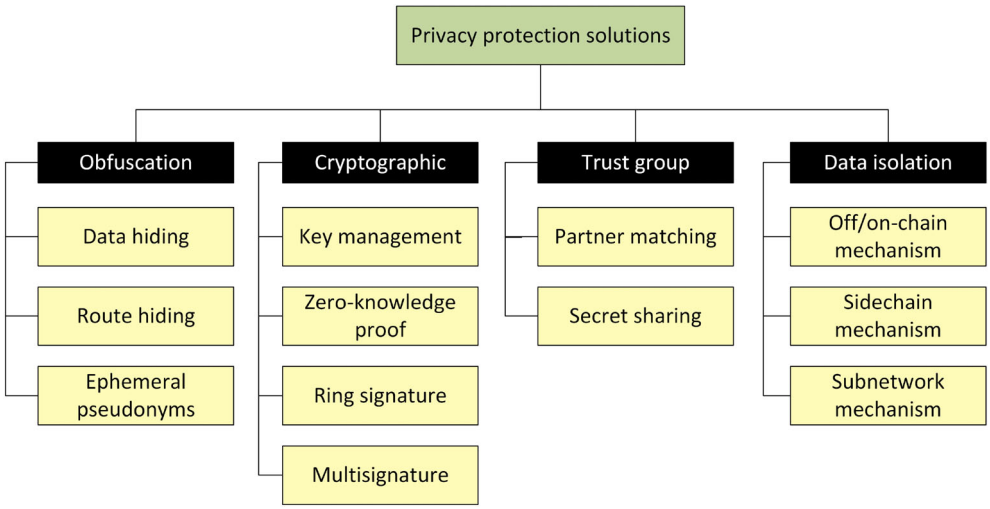

FIGURE 3 Classification of the privacy-preserving solutions for blockchain-based IoT applications

transaction parties. Transaction untraceability is the main privacy target in this class, which consists of partner matching and secret sharing solutions. In the data isolation class, private data is settled separately from the main blockchain ledger. Off/on-chain, sidechain, and subnetwork blockchain solutions are in this class, that has transaction anonymity as its primary privacy priority.

In this section, these solutions are described in more detail. We discuss the advantages and disadvantages of each solution and explain techniques that can attack them.

4.1 | Ephemeral pseudonyms

Ephemeral pseudonyms (eg, ephemeral wallets in Bitcoin[61]) are used to provide anonymous services in the blockchain. They make it difficult for a linking attacker to run the one-to-many mapping between a physical user and several virtual identities among the various transactions recorded in the shared ledger.[5,18,23] In such systems, users randomly generate new message addresses for each new transaction.[18,38,42,62] In the solution proposed by Dorri et al[38] a fresh ID (used as a key) is used for each transaction. To avoid connecting the pseudonym and a user by matching the energy consumption and the user's behaviors, in Guan et al[62] each user generates multiple pseudonyms and submits his power consumption data under different pseudonyms.

Despite these pseudonym solutions, heuristics analysis can identify users. Meiklejohn et al[48] identified the Bitcoin parties and the interactions between them using a clustering heuristic based on change addresses to cluster addresses belonging to the same user. Furthermore, the ephemeral pseudonym solutions are not practical for financial transactions, which need permanent or long-term IDs, and because of the heavy computational burden imposed on IoT devices.

4.2 | Data hiding or obfuscation

Obfuscating user's energy consumption data is used to protect user's privacy in References 63-65. The semantics of energy consumption can be used for IoT user profiling. Abidin et al[63] try to preserve consumer's privacy by hiding the details of their energy consumption. By aggregating the private data of the energy usage reported by the smart meters in Reference 63, the energy suppliers compute only the final monthly bill per customer, but not the individual metering data per time slot. Sun et al[64] hid household electricity load by using the thermal appliances and energy units. They propose an opportunistic use of household energy storage units like EVs and heating, ventilating, and air conditioning systems to reduce or eliminate the reliance on local rechargeable batteries for load hiding. Using an intermediate position between the service provider/aggregator and consumers is used to blur the energy consumption/generation data.

Azar et al[65] proposed a virtual power plant as an intermediator on behalf of a group of neighborhood prosumers to negotiate with the aggregator, where no private information of the prosumers is shared. Employing blockchain technology in the network of prosumers and the virtual plant addresses the possible trust issues. Laszka et al[42] introduced an intermediate mixing service, called privacy-preserving energy transactions (PETra) based on blockchain to anonymize all transactions. In this model, the ownership of the assets is obfuscated among a group of anonymous addresses. The mixing service prevents tracing assets back to their owners by mixing together multiple incoming and outgoing transfers. Although mixing the connections between the prosumers and the anonymous addresses helps to provide a transaction anonymity service, it cannot provide asset anonymity. Each anonymous address must be linked to a feeder to perform feeder safety checks in the blockchain-based smart contract.[66] Due to this linkage, the feeders' identities are not hidden and can be used by linking attacks to identify blockchain members.

4.3 | Route hiding

In a hidden route or anonymous connection, the communicating parties are able to exchange transactions without revealing identities. To make it difficult for observers to identify communicating parties from connection information, anonymous connection schemes, such as Onion routing[67] or Garlic routing,[68] encapsulate identifying information in multiple layers of encryption and pass it as data through the connection. In an Onion routing network (eg, Tor network), each Onion router can only identify the previous and next hop along a route. Data passed along an anonymous connection

appears differently at each onion router, so data cannot be tracked en route.[67] In Garlic routing, which is a version of Onion routing, several messages along with their delivery instructions are encapsulated into a single message.[68]

Route hiding solutions in blockchain are performed in the communication layer. Since the intermediate connection nodes know only the immediately preceding and following nodes, we achieve the anonymity of the original sender and the message.[18] Although anonymizing routing information hides connection routes, it is not sufficient for fully anonymous trading. Onion routing is vulnerable to traffic correlation attacks, where an adversary monitors a user's traffic as it enters and leaves the anonymity network to link the sender and receiver of the communication.[12] Biryukov et al[69] showed how using Bitcoin over Tor network exposes the user to MitM attacks in which an attacker controls which Bitcoin blocks and transactions the user is aware of. By setting an "address cookie" on user's machine, the attacker can correlate the same user across different sessions, even if he/she uses the Tor network. Furthermore, the MitM attacker exploits a Bitcoin built-in reputation based DoS protection to force specific Bitcoin peers to ban Tor Exit nodes of her choice. It leads to numerous attacks, such as the traffic correlation attack and correlating different Bitcoin addresses.

To achieve anonymous trading, Bergquist et al[70] exploited the features of Garlic routing and CryptoNote[71] ring signature. The provided anonymous connection prevents data identification and the ring signature helps to make the transactions untraceable. Despite anonymizing the transactions chain on the network communication and on the distributed ledger, it cannot provide a full anonymous trading. It can be proven that a bid or an ask has been responded to and that a transaction has taken place.[70] The routing scheme introduced in Reference 72 is a chessboard-clustering scheme for heterogeneous sensor networks. The routing consists of intra-cluster routing, between sensors and the cluster head, and inter-cluster routing, between cluster head sensors. This routing scheme was used by Du et al[73] for key management in his sensor network. In a garlic routing-based manner, keys are shared between the neighbor sensors that may communicate with each other. Therefore, each sensor can identify its communication neighbor (c-neighbor) as the next hop in the route. This prevents the attacker tracing the transactions based on the routing messages.

4.4 | Key management

To identify and authenticate the members participating in a blockchain, the public key infrastructure (PKI) is used[74] and members' IDs are used as their public keys. In the network of IoT devices with limited storage (eg, a sensor network), key distribution is an issue. Du et al[73] proposed a key management method for sensor networks, in which a sensor node does not need to share keys with all neighbors. Due to the small key size and low computational overhead of elliptic curve cryptography (ECC), this public-key cryptography was utilized in the sensor networks. Sharing keys with neighbor provides an ECC-based group signature in which a transaction's sender cannot be distinguished among other members of that group.[18] To preserve an IoT user's privacy in access control, Ouaddah et al[75] introduced FairAccess based on cryptocurrency blockchain mechanisms. A network of policy enforcement points (PEP) manages the protected resources. Blockchain is used to guarantee that policies are enforced by all interacting entities and detect any token reuse. To access a resource, an IoT device needs to obtain an access grant issued by the resource owner. Smart contracts are created for access control for each resource and requester pair.

Ma et al[76] introduced a blockchain-based key management scheme to preserve users' privacy in IoT systems that keep users' key information (eg, smart home). The key management operations of a hierarchical access control are stored in blockchains that act as public ledgers. In the presented IoT-involved blockchain, each blockchain is operated by a security access manager (SAM) in a fog layer as the full node. Each SAM is connected with several IoT devices and maintains the key information blockchain of its domain. The IoT devices act as lightweight nodes to process only self-correlative key information transactions. SAM acts as a CA to authorize access queries in a public and decentralized manner. In a cloud layer, SAMs are connected to each other to synchronize the public ledger. The multi-blockchains stored in the cloud support cross-domain interaction between side blockchains.

4.5 | Zero-knowledge proof

In the zero-knowledge proofs, a prover demonstrates possession of knowledge without revealing any computational information.[77,78] Based on zero-knowledge proofs, Hardjono et al[79] introduced ChainAnchor, to anonymously register IoT device commissioning and decommissioning data in the blockchain. This architecture uses the zero-knowledge proof protocol of enhanced privacy ID (EPID)[80] to allow a device to prove to a provenance verifier (and to the device owner) that

the device has the correct provenance and is coming from a given manufacturer. On the blockchain, the device is recognizable only through its transaction public key. To provide transactional privacy for a public blockchain, in which the entire sequence of actions taken in a smart contract are propagated and publicly recorded on the blockchain, Hawk[81] exploits zero-knowledge proofs. The transaction information in the blockchain is encrypted and based on the zero-knowledge proofs of the correctness of contract execution and money conservation are enforced. Hawk execution needs a manager, who can see the users' inputs. The manager computes the Hawk program, based on the transaction parties' data and currency, and constructs new private coins to be paid to each recipient. The new private coins and zero-knowledge proofs of their well-formedness are submitted to the blockchain by the manager. A compiler is used to compile the program using a cryptographic protocol between the blockchain and the users. Requiring a trusted manager to not disclose users' private data opens its own privacy issues.

To address the traceability issue with Bitcoin, Zerocoin[82] was introduced to break the link between individual Bitcoin transactions. To anonymously prove ownership, a non-interactive zero-knowledge signature is used instead of a public-key based signature. Coins are authenticated, by proving in zero-knowledge, that they belong to a public list of valid coins in the blockchain.[83] Despite transaction anonymity, the amount or other data about the transactions are not hidden in Zerocoin. To address those issues, Ben-Sasson et al[83] introduced Zerocash, a ledger-based currency constructed on decentralized anonymous payment schemes and leveraged zero-knowledge proofs. In addition to anonymous transactions, the transaction amounts and the values of coins held by users are hidden in Zerocash. A user can prove that she/he paid any taxes due on the transactions without revealing those transactions, their amounts, or even the amount of taxes paid. In Provisions,[84] the zero-knowledge proof is used to prove ownership and solvency in Bitcoin exchange. Using zero-knowledge proofs, an exchange proves that its total assets are equal to its liabilities without revealing which public keys it owns.

However, the computational and memory resources required for zero-knowledge proofs limits their applications, especially for IoT blockchains. For instance, redeeming Zerocoins requires double-discrete-logarithm proofs of knowledge and are longer than 45 kB and require 450 ms for verification.[83]

4.6 | Off/on-chain mechanism

In IoT ecosystems, M2M transactions between IoT devices or P2P connections between IoT users are the norm.[85] Registering all M2M micro-transactions in the blockchain not only compromises IoT user's privacy but also increases transaction fees. Off-chain interaction solutions are used to address the privacy issue with the blockchain by performing several P2P transactions between two parties without writing them into blockchain. To improve the speed of the transaction processing and save transaction fees, the off-chain mechanism enables deploying only the on-chain process onto the blockchain.[86] This conserves the resources of the blockchain and hides the sensitive information involved in the off-chain transactions from the public.[18,87] In the distributed electricity trading system introduced by Luo et al,[88] a multi-agent negotiation system runs between prosumers in the off-chain for contract negotiation. For each negotiated contract, a corresponding ledger entry is made to securely settle the contracts in the blockchain. The contract and ledger are stored separately. To detect any malicious manipulation, a verification mechanism is introduced to inspect any inconsistencies between the contract and ledger.

To preserve users' privacy, Zyskind et al[89] stored personal data in off-chain storage. Two types of transactions are proposed, namely, for access control and data storing/retrieving. The hash value of the data is retained in the blockchain to point to the data in the off-chain storage. To implement the off-chain key-value store, a distributed hashtable (DHT) is maintained by a network of nodes, separated from the blockchain network. To ensure availability, data are randomized and replicated across the nodes. The user can change the granted permissions at any time by issuing an access transaction with a new set of permissions. Erdin et al[90] proposed using an off-chain payment system for EV charging stations by building a payment network in parallel to the main ledger, with permission and signatures to minimize transaction fees and address the privacy exposure problem. Khalil et al[91] extend the payment channel to a set of users in a payment channel network. As payment networks, these subnetworks allow payments to be made between parties that are not simultaneously connected by a payment channel.

Although users in the off-chain system normally remain (pseudo) anonymous, it is possible to store service profiles on the blockchain and verify their identity.[89] Despite the benefits of the off-chain mechanism to preserve privacy and decrease transaction fees (eg, in Bitcoin), it has its limitations, namely limited channel capacity, data privacy in payment transaction routing, and the cost of opening and closing channels.[29,90]

4.7 | Sidechain mechanism

Sidechain mechanisms allow ledger assets (eg, Bitcoins) to be safely transferred from the main chain to other blockchains, and that can be securely transferred back.[92] Back et al[93] proposed pegged sidechains, with interoperable blockchains, to allow transferring ledger assets between multiple blockchains. To localize a disruption to a sidechain on which it occurs, sidechains should be independent, with users providing any necessary data from other chains. When moving assets from one blockchain to another, a transaction is created on the first blockchain locking the assets, then a transaction is created on the destination blockchain whose inputs contain a cryptographic proof that the lock was done correctly. In general, the main chain does not know the existence of the sidechain, but the sidechain must know the existence of the main chain.[92]

In a modular consortium IoT network, introduced by Ali et al,[94] IoT data privacy is preserved by grouping devices into sidechains, which are private blockchains. The sidechains are modularly connected to a decentralized P2P consortium network. Each sidechain includes a validator to manage its private blockchain. The consortium's validators run a blockchain to log any incoming access requests for user's IoT data and its access control. Although users' privacy is preserved by separating the logging responsibilities of the sidechains and those of the consortium blockchain, dependency on intermediate controllers opens other challenges (eg, single point of compromising). Cross-chain mechanisms used to trustfully transfer information between different blockchains mainly rely on techniques such as notary schemes, sidechains, hash-locking, and distributed private key control.[92] To have secure IoT data management, Jiang et al[95] proposed a cross-chain framework to connect blockchains. A consortium blockchain is used as a control station in an access model and connects with sidechains of IoT devices through the notaries. IOTA Tangle†† is used as the backbone of the interconnected IoT devices. IoT devices are connected to the consortium blockchain through notary nodes and IoT devices for a single-use case are grouped into sub-Tangles. Incoming access to any data is recording and access control mechanism is performed on these requests using the consortium blockchain. The notary network confirms each cross-chain transaction by the voting mechanism.

4.8 | Subnetwork blockchain

Based on the sidechain mechanism, in a subnetwork mechanism, a main blockchain has some subnetwork blockchains which are connected together by interconnection positions. The main idea of a subnetwork blockchain is to handle the P2P transactions of a group of IoT users in a subnetwork blockchain. The subnetwork blockchain is independent of the main blockchain and the interconnection node exchanges transactions between them. The interconnection node needs to simultaneously join both main and subnetwork blockchains. To preserve users' privacy, the interconnection node prevents any private information in the subnetwork leaking to the main blockchain. Based on the current events in the subnetwork blockchain, new transactions are created and appended to the main blockchain by the interconnection node. Since a subnetwork blockchain is a private blockchain, it is limited to its authorized members, which can store the private ledger.[96] A recovery mechanism is needed to prevent the interconnection node doing any fraud or data manipulation when it transfers data to the main blockchain.

Based on the subnetwork mechanism, Firoozjaei et al[97] introduced Hy-Bridge, a hybrid blockchain to handle P2P transactions of IoT users in subnet blockchains. Interconnection nodes, called bridges, connect the main blockchain and its subnetwork(s). To prevent IoT users' private data leaking to the main blockchain, bridges perform an anonymization protection based on k-anonymity. The concept of k-anonymity was proposed by Samarati and Sweeney in Reference 98. By generalizing and data suppressing, k-anonymity guarantees that in a set of k objects with a similarity, the target object is indistinguishable from the other $k-1$ objects.[99-101] All P2P transactions generated in subnetwork blockchains are forwarded to the main blockchain after anonymizing by the bridge(s). The bridges manage the transactions in two different blockchains to avoid user profiling and user identification. Based on Hy-Bridge, EVChain[29] was introduced to privately share charging credits in the EV charging market. EVChain is a hybrid blockchain framework consisting of a main blockchain for billing and payment and one or more subnetwork blockchains for credit-sharing. It allows credit-sharing within a group of EV owners and preserves an individual group member's privacy with k-anonymity protection. A local block with a credit header is used to handle user-to-user (U2U) transactions of the credit-sharing group. The parameters of the credit header enable the members of the credit-sharing group to share the charging credit and manage it separately in the subnetwork blockchain with negotiated policies. All transactions in the credit-sharing group are anonymized by the bridge and no private data is leaked to the main blockchain.

4.9 | Partner matching

The stable matching problem is to match individuals from different sides of a bipartite graph.[102] The matching model was introduced by Gale and Shapley.[103] An individual (eg, buyer) gives a list ordered by preference of all the individuals (eg, sellers), from other groups, it wants to match, to create a preferred list or ranked list. To achieve stable matches, a buyer proposes to match himself/herself to his/her preferred seller. A seller who receives multiple proposals chooses greedily his/her favorite buyer and rejects all others. The rejected buyers propose to their next choice in the next stages and again sellers choose their most preferred option.[104]

Private information is disclosed or shared when partners are matched. For instance, in the location privacy method introduced by Yucel et al,[102] the location information of an electric supplier, which is encrypted, will be disclosed to an EV owner if they match. It exploits the homomorphic operation based on Pascal Paillier cryptosystem[105] between EVs and suppliers. When suppliers receive a charging request with an encrypted location, sent from an EV, they perform the necessary homomorphic operations (using an EVs homomorphic public key and their location information) to calculate the encrypted distance. In response, the EV receives the encrypted distance information sent by the vicinity suppliers and decrypts them to obtain the actual distance and forms a preference list of suppliers in the ascending order of distance. Eventually, based on the preference lists the matching is achieved by the distributed stable matching. The EV offers to its first preference of supplier in the list and the supplier accepts it if it has that EV in its list. Nunna et al[106] used symmetrical assignment problem based on naive auction algorithm to match the buyers and sellers in the energy market. The naive auction algorithm runs in rounds and only one buyer bids on the desired object in each round. The objective of assignment problem is to find an assignment (a set of buyer-object pairs) that maximizes total benefit.

To provide privacy and security services for IoT-based transactive microgrids, Laszka et al[66] introduced an auction and matching mechanism in a distributed setting. Each prosumer generates an anonymous address and uses it when interacting with the blockchain (eg, posting offers). An energy asset is defined to show the permission to sell or buy a specific amount of energy in a specific set of time intervals. Each prosumer can ask the distribution system operator (DSO) to transfer assets to an anonymous address. By approving the permission (eg, safety check and linking between anonymous address and a correct feeder), this transfer is recorded on the blockchain by the DSO. When the participant posts an offer from the anonymous address, the smart contract can check whether the address has the assets required for the offer. Relying on the DSO, that can link anonymous address to the participant is the model's privacy Achilles' heel.

4.10 | Ring signature

Normally, in group signatures any member can anonymously sign a message on behalf of the group and only the group managers/issuers are able to add users and trace or revoke users.[107] The centralized nature of the group signature makes it useful for a cooperative network, in which the group manager is a trusted party. In the ring signature,[108] which is signer-ambiguous, there is no pre-arranged group of users and no way to distribute specialized keys. To produce a ring signature, the actual signer declares an arbitrary set of possible signers that includes himself, and computes the signature entirely by himself using only his secret key and the others' public keys. The produced signature can be publicly verified to be signed by one of the group members. The group formation and the signature generation are both spontaneous, meaning that no participation or even knowledge of the other $r-1$ members are needed.[109] In fact, the security property of a ring signature is that it should be computationally infeasible to determine which of the group members' keys was used to produce the signature. Exploiting the public key of a standard signature scheme (eg, RSA), the produced anonymity guarantees that in a set of signatures of r members the actual signer is not distinguishable from the other $r-1$ members. The larger the value of r is, the greater is the implied privacy, as the anonymous objects are identifiable with the probability greater than $1/r$.[97]

Manlina et al[107] proposed lightweight ring signatures to provide anonymous transactions in a constrained environment such as an IoT network. By shuffling the public keys in the ring set, the authors tried to remove any possibility of identifying the actual signer. For users' anonymity and authenticity in healthcare IoT networks, the lightweight ring signature is exploited in Reference 110 for a blockchain of healthcare data. Monero‡‡ digital currency uses a ring signature to obfuscate a transaction's origin. In Monero's ring signature, a user's account keys are used with a number of public keys (known as outputs) pulled from the blockchain using a triangular distribution method. To form possible signer participants, past outputs are used multiple times. Since all signers are equal, it is difficult for an attacker to detect individuals. To prevent transaction linkability, users are able to obscure transaction graph and include chaff coins, called "mixins",

with the actual coins they spend. Miller et al[111] identified weaknesses in Monero's mixin selection policy, and showed the risk of linkability. A significant fraction (62%) of Monero transactions with one or more mixins are deducible and therefore can be conclusively linked.[111]

Despite the anonymity protection for the signer, there is no guaranty for unlinkability of the signature and the receiver.[5] Liu et al[109] showed the linkability of the ring signature. Although the signer remains anonymous, two signatures signed by the same actual signer can be identified. They showed how two signatures with the same public key list are linked if they are generated using the same private key. Basically, the linkable ring signature[112-114] is used in unforceability required applications (eg, e-voting). In a linkable ring signature, each message is signed not only with respect to a list of ring members, but also with respect to an issue/tag. If a user signs the same message twice with respect to the same list of ring members and the same issue label, then the two signed messages can be determined to have come from the same signer.[115] Due to the linking property, the linking ring signature provides a restricted anonymity feature, which makes fully privacy-preserving impossible.[116] To prevent any insider attacks, Franklin et al[115] introduced unique ring signature, in which signers in a ring cannot produce signatures for any messages with more unique identifiers than the size of the ring.

4.11 | Multisignature

Unlike ring signatures, multi-signatures have a trusted third party who cooperates in signing to ensure transaction validity.[18] In multi-signature wallets introduced by Zhao et al,[86] an exchange, as a trusted third party, is authorized by the participants in distributed energy trading. A set number of tokens, signed by the buyer and the exchange, are transferred from the blockchain account to the multi-signature wallets. The order contracts which contain buyers' order information and sellers' information are sent to the exchange. According to the kind of order and delivery time, the exchange classifies the submitted orders. After the delivery period, the electric data will be transferred to the settlement contract. The contract is executed and the tokens will be transferred from the multi-signature wallet of the buyer to the multi-signature wallet of the seller and the exchange account.

In the distributed contracts, multiple independent parties are required to sign a transaction to protect against theft. In this multi-signature transaction, a minimum m of n keys must sign a transaction before tokens can be spend.[117] To preserve privacy and secure transactions without reliance on trusted third parties, Aitzhan et al[117] adapted a proof-of-concept for a decentralized energy trading system based on multi-signatures. All nodes collectively act as a replacement for a trusted party, and vote on the validity of transaction by traversing through the publicly available history of the distributed chain of transactions. For anonymous messaging, users are forced to generate new messaging addresses for each new trade negotiation.

4.12 | Secret sharing

Generating ephemeral keys based on secrets shared between the involved parties helps secure data access or exchange over a public network.[118] As a secure key exchange method, Diffie-Hellman (DH) key exchange is used to generate ephemeral cryptographic keys. For instance, DH key exchange is used in Reference 27 to share a key between the miner and a new IoT device to add the IoT device to the smart home. Guo et al[119] proposed an attribute-based signature scheme with multiple authorities, in which computational bilinear DH is used to share the secret pseudorandom function seeds among them. A patient endorses a message according to the attribute and no information is disclosed other than the evidence that he/she has attested. Employing computation bilinear DH provides prefect privacy as well as being unforgeable under a selective predict attack. In CryptoNote[71] blockchain, DH exchange is used to get a shared secret between sender and receiver to provide unconditional unlinkable payments. Each CryptoNote output's destination is a public key, derived from a recipient's address and a sender's random data. By DH exchange, the sender and receiver get the shared secret. A one-time destination key is computed based on the shared secret. Upon receiving a transaction, a user scans all output keys and checks if he can recover the corresponding secret key. He succeeds if and only if that particular output was sent to his address. Creating a large number of transactions on the blockchain is a disadvantage of this solution, which is a trade-off between privacy and capacity. Furthermore, since the CryptoNote coin's receiver needs to sweep all transactions when it wants to send it, an adversary can track which keys go together in some manner.[120]

In the blockchain-based access management introduced in Reference 121, an IoT user can delegate the access right of an IoT device to another user. The anonymous feature of blockchain is used to protect users' sensitive information at a public blockchain. Three types of public keys, namely, a user's primary key, a one-time sub address, and a domain address, are used to exchange anonymous transactions. Each IoT user chooses a secret, which is also shared with his/her IoT device. The hidden value and sensitive information are encrypted with the one-time secret shared with the receiver and attached to the transaction.

5 | EVALUATION FRAMEWORK

To evaluate the quality of the privacy provided by the reviewed solutions, we propose an evaluation framework. The framework needs a set of criteria that lends credibility to the results and simplifies the evaluation process.[122] We define evaluation criteria for two groups of privacy factors. The first group enhances the privacy of users and their data. The second group are risks or attack vectors to which the solution is vulnerable.

5.1 | Privacy features

Privacy features are factors which determine the degree of protection. Table 1 shows the privacy features introduced for our privacy ranking. They help conceal IoT user's private data, shared in the blockchain ledger, and prevent an adversary (insider or outsider) from access it. These features fall into three groups, namely, user anonymity, asset anonymity, and transaction privacy. There are 12 criteria for privacy features. Depending on the protection provided and effectiveness, we rank the individual criterion of the privacy features on a scale of one to three. A weight of one indicates that a criterion is useful but not very effective. The weights of two and three indicate the effectiveness of a criterion to preserve IoT user's privacy, respectively, in medium level and high level.

User anonymity can be accomplished by using ephemeral ID, pseudonymous ID, or hiding a user's ID in an anonymity group. The asset anonymity feature includes two criteria of device ID hiding and ownership hiding. It addresses the privacy issues of IoT device profiling, targeted advertisement, and criminal abuse, which are common IoT device-centric privacy issues. The transaction privacy feature includes the criteria of data confidentiality (eg, data encryption, data obfuscation, private data separation, and data suppression), transaction untraceability, transaction anonymity, and anonymous trading. These criteria are used to conceal an IoT user's private data or prevent attackers tracing the transactions. For instance, anonymous trading guarantees that the adversary cannot find information about a transaction's data (eg, money amount) or its receiver.

As shown in Table 1, we scale each individual criterion based on our weighting model. To evaluate the privacy-preserving capabilities, we consider all protection criteria provided by a protection solution. To this end, we

TABLE 1 Privacy features

Privacy feature	Criterion	Weight
User anonymity	Pseudonymous ID	2
	Ephemeral ID	3
	Anonymity group	3
Asset anonymity	Device un-identifying	3
	Ownership un-identifying	2
Transaction privacy	Confidentiality—data encryption	3
	Confidentiality—data obfuscation/generalization	2
	Confidentiality—private data separation	2
	Confidentiality—data suppression	2
	Transaction untraceability	3
	Transaction anonymity	2
	Anonymous trading	1

assume that the criteria of the privacy features are not mutually exclusive. Therefore, there is no limitation and a protection solution can provide all privacy features' criteria to preserve IoT user's privacy. The weighting vector $\vec{W}_f$ represents the weights of these 12 criteria of the privacy features, where:

$$\vec{W}_f = (w_1, w_2, \ldots, w_{12}) = (2,3,3,3,2,3,2,2,2,3,2,1), \tag{1}$$

where w_i represents the weight of the ith criterion of the privacy features. Maximum privacy is defined as the maximum protection, when a protection solution offers all privacy features and achieves the total scale of:

$$\text{Maximum privacy} = \sum_{i=1}^{12} w_i = 28 \tag{2}$$

In the maximum privacy protection, a protection solution provides a full privacy over all aspects of user-centric issues and device-centric privacy issues.

5.2 | Privacy risks

We classify the factors which can be used to compromise an IoT user's privacy (eg, user identifying or chain reaction[123]) as the privacy risks. They can be residential privacy threats, that could not be covered by a protection solution or the side effects of the privacy-preserving, which are provided unwillingly. For instance, the risk of third party dependency is a side effect of a solution which depends on a trusted third party (TTP) to privately handle transactions (eg, multi-signature solution). These factors can be exploited by an attacker to launch attacks like linking attacks or user profiling. As shown in Table 2, there are four groups of privacy risks, namely, linkability, third party dependency, insider adversary, and performance issues.

Linkability risk is the potential to correlate data from different sources (eg, transactions).[124] It includes traffic correlation, address/ID correlation, and IoT device linkability. If an attacker can monitor traffic, he/she can analyze anonymous paths (eg, Tor) and identify the parties to a communication.[12] In a device-to-identity linking attack, the information about IoT devices are exploited to infer links between devices and user's.[11] Dependency on a third party, such as a system operator, a trusted third party (TTP), and an intermediate controller, to preserve IoT users' privacy in the blockchain is a risk as they may not keep their fiducial responsibility. Private data leakage and misusing are possible by the adversarial insiders. Data leakage, signature/token reuse, and transaction misrouting are the criteria of the insider adversary risk. Utility and performance conditions are important to evaluate the solutions. Practically, higher privacy imposes heavy computation, execution delay, and resource consumption, which leads to lower utility. We consider the criteria of bandwidth

TABLE 2 Privacy risks

Privacy risk	Criterion	Weight
Linkability	Traffic correlation	1
	Address/ID correlation	1
	Device linkability	1
Third party dependency	System operator (distributor/manager)	1
	Trusted third party (TTP)	1
	Intermediate controller	1
Insider adversary	Data leakage	1
	Signature/token reuse	1
	Transaction misrouting	1
Performance	Capacity issue (bandwidth)	1
	Memory issue (large number of transactions)	1
	Computational burden	1

(eg, capacity issue), memory (eg, large number of transactions), and the computational requirement to evaluate the performance of the solutions.

As shown in Table 2, we consider 12 criteria for the privacy risks. We consider each criterion to be of equal effect and give a weight of one to all of them. The weighting vector $\vec{V}_r$ represents the weights of these criteria, where:

$$\vec{V}_r = (v_1, v_2, \ldots, v_{12}) = (1,1,1,1,1,1,1,1,1,1,1,1), \tag{3}$$

where v_i represents the weight of the ith criterion of the privacy risks. Maximum risk is defined as the maximum privacy risk, when a protection solution leaves all introduced privacy risks and has the total risk scale of:

$$\text{Maximum risk} = \sum_{i=1}^{12} v_i = 12 \tag{4}$$

Maximum risk happens when a protection solution provides all side effects that leads to the maximum risk of privacy violation.

5.3 | Privacy rank

To obtain objective results, we devise an evaluation scheme for ranking the privacy-preserving solutions. Based on the technique used, each solution offers privacy features and has some risks (residential threats or side effects). The privacy features of a solution is expressed as a privacy feature vector, $\vec{P}_f$, where:

$$\vec{P}_f = (f_1, f_2, \ldots, f_{12}), \tag{5}$$

where f_i is 1 or 0 and shows whether the protection solution satisfies the ith criterion of the privacy features ($f_i = 1$) or not ($f_i = 0$). Similarly, the privacy risks of a solution is expressed as a privacy risk vector, $\vec{P}_r$, where:

$$\vec{P}_r = (r_1, r_2, \ldots, r_{12}), \tag{6}$$

where r_i is 1 or 0 and shows whether the solution has the ith criterion of the privacy risks ($r_i = 1$) or not ($r_i = 0$). In practice, the privacy risks have different feasibilities based on the ease of exploiting or their abundances. In this framework, we consider all privacy risks' criteria equal and indicate their feasibilities in the binary variables (0 or 1).

The resultant of the provided privacy features and the remained privacy risks shows the overall privacy-preserving provided by a protection solution. We call it the privacy resultant, which is calculated as follows:

$$\text{Privacy resultant} = \vec{P}_f \cdot \vec{W}_f - \vec{P}_r.\vec{V}_r = \sum_{i=1}^{12} f_i \times w_i - \sum_{j=1}^{12} r_j \times v_j. \tag{7}$$

Practically a solution cannot provide all privacy features and the maximum privacy protection is not feasible. Similarly, the maximum risk cannot be assigned to a privacy-preserving solution. Based on the introduced indexes of maximum privacy and maximum risk in 5.1 and 5.2, the privacy resultant is a value between −12 and 28. We have the minimum privacy resultant (−12) when a solution leaves all privacy risks and has no privacy feature. In a similar fashion, the maximum privacy resultant (28) is achieved when a solution offers all privacy features with no privacy risk. It is worth to note that, these values are based on the criteria introduced in Tables 1 and 2 and will be changed if other criterion weighing scales are used.

We introduce the privacy rank, to represent the numeric value associated with each evaluated privacy-preserving solution. The privacy rank of a solution is the normalized value of its privacy resultant. To this end, we normalize the values of privacy resultant and transfer them into a decimal range between 0 and 1 by the min-max normalization. For a given set of values $\{v_k\}$, $k = 1, 2, \ldots, n$, the min-max normalized values $\{v'_k\}$ are given by[125]:

$$v'_k = \frac{v_k - \min}{\max - \min}, \tag{8}$$

TABLE 3 Rating model for privacy rank

Rating scale	Privacy rank (PR)
Poor	$0 \leq PR < 0.2$
Fair	$0.2 \leq PR < 0.4$
Good	$0.4 \leq PR < 0.6$
Very good	$0.6 \leq PR < 0.8$
Excellent	$0.8 \leq PR \leq 1$

where max and min are the maximum and minimum values from the given set of values $\{v_k\}$, respectively. In our evaluation model, the maximum and minimum values of the privacy resultant are −12 and 28, respectively. Therefore, the privacy rank is:

$$\text{Privacy rank} = \frac{(\text{Privacy resultant}) - (-12)}{28 - (-12)} = \frac{(\vec{P}_f.\vec{W}_f - \vec{P}_r.\vec{V}_r) + 12}{40} \tag{9}$$

The value of privacy rank shows the quality of the privacy-preserving provided by a solution. A larger privacy rank indicates better protection and small rank shows the lower quality of protection. Therefore, the privacy rank with the value of 0 represents no privacy and the privacy rank of the value of 1 indicates full privacy.

We define a model to rate the scales of the privacy rank. Table 3 shows our rating model in the range between 0 and 1. We define five rating scales, namely, poor, fair, good, very good, and excellent. A privacy rank smaller than 0.2 is rated as poor rank. Privacy ranks in the range of [0.2; 0.4), [0.4; 0.6), and [0.6; 0.8) are respectively rated fair, good, and very good. The excellent rate is assigned to a privacy rank between or equal to 0.8 and 1. The lowest privacy-preserving is offered by a poor solution, which is usually vulnerable against most privacy threats, such as linking attacks. Although the fair rated solutions provide the basic privacy protection, they suffer from privacy risks, which dispose the private information. A good solution offers most effective protection criteria (eg, untraceability). Our evaluation shows that a very good solution should provide anonymity and confidentiality privacy features (eg, data encryption and untraceability) and be resistant against privacy risks. An excellent privacy-preserving solution has no privacy risk and provides a full anonymous trading with all features of privacy.

6 | EVALUATION RESULTS

The evaluation results of the reviewed privacy-preserving solutions are shown in Tables 4 and 5. Table 4 shows the criteria of the privacy features, the weight of each item (extracted from the weighting vector of $\vec{W}_f$), and the possibility of being covered by the solutions. Similarly, Table 5 indicates the privacy risks and their criteria, the weight of each criterion (extracted from the weighting vector of $\vec{V}_r$), and the possibility for a solution being vulnerable with the risk criterion. In these tables, the checkmark in front of each criterion indicates that the corresponding privacy-preserving solution provides that criterion of privacy feature or is suffering from the indicated criterion of the privacy risk.

As shown in Table 4, user anonymity is the most supported privacy feature. The pseudonymous ID criterion, which is a basic blockchain feature, is offered by all reviewed solutions. In comparison, the ephemeral ID is only provided by ephemeral pseudonym, multi-signature, and secret sharing solutions to make IoT user anonymous. Device un-identifying is provided only by the zero-knowledge solution. In this regard, zero-knowledge provides the most privacy features and covers seven criteria, the most among all reviewed solutions. Data hiding and subnetwork solutions cover six criteria. In spite of providing different criteria, the solutions of off/on-chain, sidechain, partner matching, ring signature, and secret sharing support five criteria. While ephemeral pseudonym, route hiding, and multi-signature cover four criteria, key management has the lowest criterion coverage. Although the number of criterion covered by a preserving solution is important, the weight of the criterion, which indicates its effectiveness, is a critical factor to calculate the privacy rank of a solution. For instance, data encryption criterion, which is weighted with three, is more effective than anonymous trading criterion with weight of one, in privacy rank calculation.

TABLE 4 Privacy features and the evaluation results of the privacy-preserving solutions

Privacy feature	Criterion	Weighting Vector ($\vec{W}_f$)	Ephemeral pseudonym	Data Hiding	Route Hiding	Key management	Zero-knowledge	Off/on-chain	Sidechain	Subnetwork	Partner matching	Ring signature	Multisignature	Secret sharing
User anonymity	Pseudonymous ID	$w_1 = 2$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Ephemeral ID	$w_2 = 3$	✓										✓	✓
	Anonymity group	$w_3 = 3$				✓		✓	✓	✓		✓		
Asset anonymity	Device unidentifying	$w_4 = 3$					✓							
	Ownership unidentifying	$w_5 = 2$	✓	✓	✓						✓	✓		
Transaction privacy	Confi.- data encryption	$w_6 = 3$					✓				✓			✓
	Confi.- data obfuscation	$w_7 = 2$		✓			✓				✓			
	Confi.- data separation	$w_8 = 2$						✓	✓	✓				
	Confi.- data suppression	$w_9 = 2$		✓	✓		✓	✓	✓	✓	✓		✓	
	Transaction untraceability	$w_{10} = 3$		✓	✓		✓					✓		
	Transaction anonymity	$w_{11} = 3$		✓	✓		✓					✓		✓
	Anonymous trading	$w_{12} = 1$	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

TABLE 5 Privacy risks and the evaluation results of the reviewed privacy-preserving solutions

Privacy risk	Criterion	Weighting Vector ($\vec{V}_r$)	Ephemeral pseudonym	Data Hiding	Route Hiding	Key management	Zero-knowledge	Off/on-chain	Sidechain	Subnetwork	Partner matching	Ring signature	Multisignature	Secret sharing
Linkability	Traffic correlation	$v_1 = 1$	✓		✓			✓	✓	✓		✓		
	Address/ID correlation	$v_2 = 1$	✓	✓	✓						✓	✓	✓	
	Device linkability	$v_3 = 1$		✓										✓
Third party dependency	System operator	$v_4 = 1$									✓			
	Trusted third party (TTP)	$v_5 = 1$					✓			✓			✓	
	Intermediate controller	$v_6 = 1$		✓		✓			✓					
Insider adversary	Data leakage	$v_7 = 1$				✓			✓	✓				
	Signature/token reuse	$v_8 = 1$										✓	✓	
	Transaction misrouting	$v_9 = 1$					✓						✓	
Performance	Capacity issue	$v_{10} = 1$				✓	✓							
	Memory issue	$v_{11} = 1$								✓				✓
	Computational burden	$v_{12} = 1$	✓			✓								✓

TABLE 6 Privacy feature vector and privacy risk vector for each privacy-preserving solution

Privacy-preserving solution	Privacy feature vector ($\vec{P_f}$)	Privacy risk vector ($\vec{P_r}$)
Ephemeral pseudonym	(1,1,0,0,1,0,0,0,0,0,0,1)	(1,1,0,0,0,0,0,0,0,0,0,1)
Data hiding	(1,0,0,0,1,0,1,0,0,1,1,1)	(0,1,1,0,0,1,0,0,0,0,0,0)
Route hiding	(1,0,0,0,1,0,0,0,0,1,1,0)	(1,1,0,0,0,0,0,0,0,0,0,0)
Key management	(1,0,1,0,0,0,0,0,0,0,0,0)	(0,0,0,0,0,1,1,0,0,0,0,0)
Zero-knowledge	(1,0,0,1,0,1,1,0,0,1,1,1)	(0,0,0,0,1,0,0,0,0,1,0,1)
Off/on-chain	(1,0,1,0,0,0,0,1,1,0,0,1)	(1,0,0,0,0,0,0,0,1,1,0,0)
Sidechain	(1,0,1,0,0,0,0,1,1,0,0,1)	(1,0,0,0,0,1,1,0,0,0,0,0)
Subnetwork	(1,0,1,0,0,0,1,1,1,0,0,1)	(1,0,0,0,1,0,1,0,0,0,0,0)
Partner matching	(1,0,0,0,1,1,0,0,1,0,0,1)	(0,1,0,1,0,0,0,0,0,0,1,0)
Ring signature	(1,0,1,0,1,0,0,0,0,1,1,0)	(1,1,0,0,0,0,0,1,0,0,0,0)
Multisignature	(1,1,0,0,0,0,0,0,1,0,0,1)	(0,1,0,0,1,0,0,1,1,0,0,0)
Secret sharing	(1,1,0,0,0,1,0,0,0,0,1,1)	(0,0,1,0,0,0,0,0,0,0,1,1)

Table 5 shows that the linkability risk is the most common vulnerability for the reviewed solutions. Most of them are vulnerable to correlation attacks. Solutions that use encryption techniques or exchange a huge number of transactions (eg, zero-knowledge and secret sharing) suffer performance issues. Our evaluation shows that route hiding and key management have the lowest privacy risk and the multi-signature solution has the highest privacy risk.

As mentioned before, we assign a weight for each criterion of the privacy features and the privacy risks based on our weighting scheme. This weighting is expressed in two weight vectors of $\vec{W_f}$ and $\vec{V_r}$, which are represented by Equations (10) and (11).

$$\vec{W_f} = (2,3,3,3,2,3,2,2,2,3,2,1) \tag{10}$$

$$\vec{V_r} = (1,1,1,1,1,1,1,1,1,1,1,1) \tag{11}$$

The criteria of the privacy features are ranked on a weight scale of one to three. Low, medium, and high effective criteria of privacy features are respectively weighted one, two, and three. We consider a same weight scale for each individual criterion of privacy risks and each one is ranked the weight of one. It is worth noting that, the introduced weighing scales can be changed and rearranged for different evaluation purposes. The weight of individual criterion can be set based on its priority and effect on the related evaluation model.

Table 6 represents the privacy feature vector ($\vec{P_f}$) and the privacy risk vector ($\vec{P_r}$) for the reviewed privacy-preserving solutions. $\vec{P_f}$ vector is extracted from Table 4 and indicates the privacy features offered by a privacy-preserving solution. $\vec{P_r}$ shows the privacy risks that threaten a privacy-preserving solution and is extracted from Table 5.

6.1 | Privacy-preserving analysis

Different privacy features and risks are created in each class due to the privacy priority and the techniques used. Anonymity is the main priority of the solutions in the obfuscation class. In this class of protection, the pseudonymous and ephemeral IDs are the major techniques used to anonymize a user. Furthermore, transaction anonymity is achieved by obscuring the routing data. Therefore, obfuscation class solutions are not suitable to protect the user's data. Although both blockchain implementation models for IoT, namely, BaaS and IoT-involved blockchains, can benefit anonymity service provided by these solutions, device-centric privacy protection (eg, IoT device anonymity) is better provided for IoT-involved blockchain model. Linkability is the main vulnerability for these solutions and threatens their services. An attacker is able to uncover hidden information (eg, user identification) by correlation by prolong traffic monitoring. Fully anonymous trading is not achievable by solutions in the obfuscation class.

Data encryption and digital signatures are commonly used by the privacy-preserving solutions in the cryptographic class. Data confidentiality is provided by encrypting the transaction data. Zero-knowledge solutions provide transaction untraceability and data confidentiality in which no private data is revealed. Despite these features, zero-knowledge proof is not proper for user anonymity purposes. In some cases (eg, Hawk[81]), a trusted manager is needed for private transactions and blockchain updates. Extreme computation and high network use limit zero-knowledge solutions for BaaS applications. Key management solutions use key sharing policies to authenticate and identify IoT users. It is a good choice for IoT-involved blockchain applications due to its simplicity.

In the ring signature solutions, the user is anonymous because the transaction's origin is obscured. It is difficult to trace transactions originated from a group of homogeneous signers. The number of signing ring members and their relationship directly affect the protection efficiency. Depends on the blockchain implementation model, we have different privacy features achieved by these solutions. For instance, user anonymity is possible for BaaS applications and IoT devices are anonymous in IoT-involved blockchain applications. There is no confidentiality feature and signature linkability makes ring signature solutions vulnerable to linking attack and insider adversaries. Similarly, multi-signature's main feature is user anonymity and requires a TTP for anonymous trading. Data leakage and transaction misrouting are possible with a compromised third party. Lightweight implementation makes these solutions a suitable choice for user's anonymity applications.

Although encryption techniques are used in partner matching and secret sharing solutions, we put them in a separate class. In the trust group class, the transaction parties make a secure link to exchange data. Although data confidentiality and transaction anonymity are provided by these solutions, user anonymity is limited to the pseudonymous feature, which is attacked by address correlation. Having to exchange a huge number of transactions to match a partner and dependency on an operator limit the applicability of the partner matching solution. The computational power and memory requirements should be considered for preserving user's privacy by the secret sharing solution. These solutions are more practical for BaaS models due to their performance conditions.

In the data isolation class, a user's private data is isolated from the main ledger and is logged separately. This protection class is more effective for BaaS applications. The access management and data storage are managed by IoT users in which more protection can be performed. For instance, in the subnetwork solution, an anonymity protection is added to the isolated data in the private storage by the bridge node. Although the off/on-chain solution provides data suppression and separation, it allows transaction to be traced. Hence, it has a linkability risk. Traffic correlation on the on-chain network can trace private data in the off-chain network. Furthermore, insider attackers can compromise a user's privacy in the off-chain network. This issue exists for sidechain and subnetwork solutions. Both these solutions need an intermediate controller or TTP to connect to the main blockchain. As well, interconnections between side blockchains and the main blockchain leads to traffic correlation, data leakage, and transaction tracking.

6.2 | Privacy rank

To rate the evaluated solutions, we use the privacy rank introduced in Section 5. The privacy rank represents a numeric value between 0 and 1 to each privacy-preserving solution and is calculated as follows:

$$\text{Privacy rank} = \frac{(\vec{P}_f.\vec{W}_f - \vec{P}_r.\vec{V}_r) + 12}{40}. \tag{12}$$

The privacy rank of a privacy-preserving solution is based on the resultant of the provided privacy features and the created privacy risks. Therefore, a proper preserving solution not only should provide more effective privacy features but also needs to create less privacy risks. Based on this, the privacy rank makes a comprehensive scrutiny of the quality of the privacy-preserving. The protection solutions are rated based on their privacy ranks. Rating based on normalized values makes our evaluation scheme independent from the criterion weighing scales. This flexibility makes the security engineers able to exploit our evaluation model for different weighting schemes. Table 7 includes the privacy rank of each privacy-preserving solution. It shows that the key management solution has the smallest privacy rank and the zero-knowledge solution has the largest ranking.

Based on the rating model introduced in Section 5 (Table 3), we rate the privacy-preserving solutions. On the basis of this rating scale, we do not rate any evaluated protection solution as a poor protection solution. The key management solution, with a privacy rank of 0.375, is a fair solution. Despite being easily implemented, this solution is not

TABLE 7 Privacy ranks and the rates of the privacy-preserving solutions

Rating scale	Privacy-preserving solution	Privacy rank (PR)
Poor ($0 \leq PR < 0.2$)	—	—
Fair ($0.2 \leq PR < 0.4$)	Key management	0.375
Good ($0.4 \leq PR < 0.6$)	Multisignature	0.4
	Ephemeral pseudonym	0.425
	Route hiding	0.475
	Off/on-chain	0.475
	Sidechain	0.475
	Partner matching	0.475
	Secret sharing	0.5
	Data hiding	0.525
	Subnetwork	0.525
	Ring signature	0.525
Very good ($0.6 \leq PR < 0.8$)	Zero-knowledge	0.625
Excellent ($0.8 \leq PR \leq 1$)	—	—

recommended. Based on this rating model, the privacy rank of a good protection solution is bigger than 0.4 and smaller than 0.6. Therefore, the good-rated solutions include the majority of the protection solutions, namely, multi-signature, ephemeral pseudonym, off/on-chain, sidechain, partner matching, route hiding, secret sharing, data hiding, subnetwork, and ring signature. Of note, the privacy rank indicates the privacy-preserving quality. Based on this, although the subnetwork solution and multi-signature solution are rated as good solutions, the protection quality of a subnetwork solution with the privacy rank of 0.525 is considerably higher than that of a multisignature solution with a privacy rank of 0.4. Despite the imposed computational burden, the zero-knowledge based solution was the best. The privacy rank of the zero-knowledge solution is 0.625 and is a very good solution. Our evaluations show that there is no privacy-preserving solution with a privacy rank in the range of [0.8;1]. Therefore, we could not rate a solution with excellent scale.

Our evaluations show that the key management solution is not recommended for preserving an IoT user's privacy in the blockchain systems, due to its privacy features. Although good-rated solutions have privacy ranks at the range of [0.4;0.6), the privacy-preserving solutions that their privacy ranks are bigger than 0.5 (eg, ring signature solution) offer better privacy features. We recommend the zero-knowledge solution for preserving IoT users' privacy in the blockchain-based applications due to its privacy rank.

7 | CONCLUSIONS

In this article, we presented users' privacy issues in blockchain-based IoT applications and classified proposed privacy-preserving solutions. We reviewed and analyzed each class of with respect to the privacy they afford. We proposed an evaluation framework to calculate the quality of each. In this framework, an adjustable weighting scheme is defined to score the privacy features and risks provided by each solution. We introduced the privacy rank, to represent the numeric value associated with each evaluated solution. The value of the privacy rank is in a decimal range between 0 and 1 and shows the overall quality of the privacy-preserving provided by a protection solution. The privacy rank value 0 represents no privacy and a larger rank indicates better protection. The privacy rank value 1 represents full privacy.

We rated the privacy-preserving solutions based on their calculated privacy ranks. This rating is based on the normalized values of the privacy resultant. It makes our evaluation scheme independent from the criterion weighing scales. This flexibility allows security engineers to use this evaluation model with different weighting schemes. Selecting a protection solution depends on the application domain and the privacy goal. In general view, our evaluation shows that the key management solution is a fair solution and the zero-knowledge solution provides the best protection. The zero-knowledge protection solution is rated as a very good solution and is recommended to preserve IoT user's privacy in the blockchain-based applications.

ACKNOWLEDGMENTS

The authors generously acknowledge the funding from the National Science and Engineering Research Council of Canada (NSERC) through the discovery grant (RGPIN 227441) and Canada Research Chair (Grant number CRC 950-230984) to Dr. Ghorbani.We would like to express our sincere gratitude to Evan R. Kennedy (Database Administration Services (Unit), Service New Brunswick, Fredericton, New Brunswick, Canada) for his helpful suggestions.

CONFLICT OF INTEREST

The authors declare no potential conflict of interests.

ENDNOTES

*https://www.chainofthings.com/marudevices
†https://www.riddleandcode.com/
‡https://www.iota.org/
§https://www.chainofthings.com/
¶https://lora-alliance.org/about-lorawan
**https://github.com/hyperledger/fabric
††https://www.iota.org/research/meet-the-tangle
‡‡https://web.getmonero.org/

ORCID

Mahdi Daghmehchi Firoozjaei https://orcid.org/0000-0002-0468-2227

REFERENCES

1. Chanson M, Bogner A, Bilgeri D, Fleisch E, Wortmann F. Blockchain for the IoT: privacy-preserving protection of sensor data. *J Assoc Inform Syst*. 2019;20(9):1274-1309.
2. Baecker O, Jain S. Can blockchain accelerate Internet of Things (IoT) adoption?. https://www2.deloitte.com/ch/en/pages/innovation/articles/blockchain-accelerate-iot-adoption.html; 2017.
3. Maroufi M, Abdolee R, Tazekand B. On the convergence of blockchain and internet of things (iot) technologies. arXiv Preprint arXiv:1904.01936; 2019.
4. Wang G, Shi Z, Nixon M, Han S. Chainsplitter: towards Blockchain-based industrial IoT architecture for supporting hierarchical storage. Paper presented at: 2019 IEEE International Conference on Blockchain (Blockchain); 2019, pp. 166-175.
5. Wang X, Zha X, Ni W, et al. Survey on blockchain for Internet of Things. *Comput Commun*. 2019;136:10-29.
6. Neisse R, Steri G, Nai-Fovino I. A Blockchain-based approach for data accountability and provenance tracking. Paper presented at: ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and Security; 2017, pp. 1-10.
7. Chain of Things. Maru. https://www.chainofthings.com/marudevices.
8. Pureswaran V, Brody P. Device Democracy: Saving the Future of the Internet of Things. https://www.ibm.com/downloads/cas/Y5ONA8EV; 2015.
9. Popov S. The Tangle. 2016, p. 131.
10. Pashalidis A, Meyer B. Linking anonymous transactions: the consistent view attack. In: Danezis G, Golle P, eds. *Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science*. Vol 4258. Berlin, Heidelberg: Springer; 2006:384-392.
11. Matte C, Achara J, Cunche M. Device-to-identity linking attack using targeted Wi-fi Geolocation spoofing. Paper presented at: Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks; 2015, pp. 1-6.
12. Johnson A, Wacek C, Jansen R, Sherr M, Syverson P. Users get routed: traffic correlation on Tor by realistic adversaries. Paper presented at: CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security; 2013, pp. 337-348.
13. Catarinucci L, De Donno D, Mainetti L, et al. An IoT-aware architecture for smart healthcare systems. *IEEE Internet Things J*. 2015;2(6):515-526.
14. Saarika PS, Sandhya K, Sudha T. Smart transportation system using IoT. Paper presented at: 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon); 2017, pp. 1104-1107.
15. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart Cities. *IEEE Internet Things J*. 2014;1(1):22-32.
16. Li L, Ota K, Dong M. When weather matters: IoT-based electrical load forecasting for smart grid. *IEEE Commun Mag*. 2017;55(10):46-51.
17. Morello R, De Capua C, Fulco G, Mukhopadhyay S. A smart power meter to monitor energy flow in smart grids: the role of advanced sensing and IoT in the electric grid of the future. *IEEE Sensors J*. 2017;17(23):7828-7837.
18. Wang N, Zhou X, Lu X, et al. When energy trading meets blockchain in electrical power system: the state of the art. *Appl Sci*. 2019;9(8):1561.
19. Reid F, Harrigan M. An analysis of anonymity in the Bitcoin system. In: Altshuler Y, Elovici Y, Cremers A, Aharony N, Pentland A, eds. *Security and Privacy in Social Networks*. New York, NY: Springer; 2013:197-223.
20. Ron D, Shamir A. Quantitative analysis of the full Bitcoin transaction graph. In: Sadeghi AR, ed. *Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science*. Vol 7859. Berlin, Heidelberg: Springer; 2013:6-24.

21. Koshy P, Koshy D, McDaniel P. An analysis of anonymity in Bitcoin using P2P network traffic. In: Christin N, Safavi-Naini R, eds. *Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science*. Vol 8437. Berlin, Heidelberg: Springer; 2014:469-485.
22. Fraga-Lamas P, Fernández-Caramés TM. Leveraging distributed ledger technologies and blockchain to combat fake news. arXiv preprint arXiv:1904.05386; 2019.
23. Henry R, Herzberg A, Kate A. Blockchain access privacy: challenges and directions. *IEEE Security Privacy*. 2018;16(4):38-45.
24. Shafagh H, Burkhalter L, Hithnawi A, Duquennoy S. Towards Blockchain-based auditable storage and sharing of IoT data. Paper presented at: CCSW '17: Proceedings of the 2017 on Cloud Computing Security Workshop; 2017, pp. 45-50.
25. Li D, Peng W, Deng W, Gai F. A Blockchain-based authentication and security mechanism for IoT. Paper presented at: 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou; 2018, pp. 1-6.
26. Alexopoulos N, Daubert J, Mühlhäuser M, Habib S. Beyond the hype: on using Blockchains in Trust Management for Authentication. Paper presented at: 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW; 2017, pp. 546-553.
27. Dorri A, Kanhere S, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: the case study of a smart home. Paper presented at: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI; 2017, pp. 618-623.
28. Ozyilmaz K, Yurdakul A. Designing a Blockchain-based IoT with Ethereum, swarm, and LoRa: the software solution to create high availability with minimal security risks. *IEEE Consumer Electron Mag*. 2019;8(2):28-34.
29. Firoozjaei MD, Ghorbani A, Kim H, Song J. EVChain: A blockchain-based credit sharing in electric vehicles charging. Paper presented at: PST2019; 2019, pp. 247-251.
30. Spathoulas G, Giachoudis N, Damiris G, Theodoridis G. Collaborative Blockchain-based detection of distributed denial of service attacks based on internet of things botnets. *Future Internet*. 2019;11(11):226.
31. Xiong Z, Feng S, Niyato D, Wang P, Han Z. Optimal pricing-based edge computing resource Management in Mobile Blockchain. Paper presented at: *2018* IEEE International Conference on Communications (ICC), Kansas City, MO; 2018, pp. 1-6.
32. Sharma P, Chen M, Park J. A software defined fog node based distributed Blockchain cloud architecture for IoT. *IEEE Access*. 2017;6:115-124.
33. Leiding B, Memarmoshrefi P, Hogrefe D. Self-managed and Blockchain-based vehicular ad-hoc networks. Paper presneted at: UbiComp '16: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct; 2016, pp. 137–140.
34. Yohan A, Lo N. An over-the-Blockchain firmware update framework for IoT devices. Paper presented at: 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan; 2018, pp. 1-8.
35. Hui H, An X, Wang H, et al. Survey on Blockchain for internet of things. *J Internet Services Inf Secur*. 2019;9(2):1-30.
36. Kim T, Noh J, Cho S. SCC: storage compression consensus for Blockchain in lightweight IoT network. Paper presented at: 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV; 2019, pp. 1-4.
37. Matte C, Achara J, Cunche M. Short: device-to-identity linking attack using targeted Wi-fi Geolocation spoofing. Paper presented at: WiSec '15: Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Network, New York, NY; 2015.
38. Dorri A, Steger M, Kanhere SS, Jurdak R. BlockChain: a distributed solution to automotive security and privacy. *IEEE Commun Mag*. 2017;55(12):119-125.
39. Lisovich M, Mulligan D, Wicker S. Inferring personal information from demand-response systems. *IEEE Security Privacy*. 2010;8(1):11-20.
40. Raviv G. Methods for user profiling for detecting insider threats based on internet search patterns and forensics of search keywords. https://patentimages.storage.googleapis.com/27/d9/28/7595ba6ea5bc93/US8375452.pdf; 2013. US Patent 8375452.
41. Albert A, Rajagopal R. Thermal profiling of residential energy use. *IEEE Trans Power Syst*. 2014;30(2):602-611.
42. Laszka A, Dubey A, Walker M, Schmidt D. Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems using Distributed Ledgers. Paper presented at: IoT '17: Proceedings of the Seventh International Conference on the Internet of Things; 2017, p. 13.
43. Schiaffino S, Amandi A. Intelligent user profiling. In: Bramer M, ed. *Artificial Intelligence An International Perspective. Lecture Notes in Computer Science*. Vol 5640. Berlin, Heidelberg: Springer; 2009:193-216.
44. Lim S, Fotsing P, Almasri A, et al. Blockchain technology the identity management and authentication service disruptor: a survey. *Int J Adv Sci Eng Inform Technol*. 2018;8(4–2):1735-1745.
45. Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K. A Blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Netw*. 2018;32(6):184-192.
46. Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in Bitcoin P2P network. Paper presented at: CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security; 2014, pp. 15-29.
47. Monaco V. Identifying Bitcoin Users by Transaction Behavior. Paper presented at: Proceedings of the SPIE 9457, Biometric and Surveillance Technology for Human and Activity Identification XII, 945704. International Society for Optics and Photonics, Bellingham, WA; 2015.
48. Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of Bitcoins: characterizing payments among men with no names. Paper presented at: IMC '13: Proceedings of the 2013 Conference on Internet Measurement Conference; 2013, pp. 127-140.
49. Firoozjaei MD, Yu J, Kim H. Privacy preserving nearest neighbor search based on topologies in cellular networks. Paper presented at: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu; 2015, pp. 146-149.
50. Ziegeldorf J, Morchon O, Wehrle K. Privacy in the internet of things: threats and challenges. *Security Commun Netw*. 2014;7(12):2728-2742.

51. Knirsch F, Unterweger A, Engel D. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Comput Sci Res Dev*. 2018;33(1–2):71-79.
52. Jia B, Zhou T, Li W, Liu Z, Zhang J. A Blockchain-based location privacy protection incentive mechanism in crowd sensing networks. *Sensors*. 2018;18(11):3894.
53. Khan M, Salah K. IoT security: review, blockchain solutions, and open challenges. *Future Gener Comput Syst*. 2018;82:395-411.
54. Ceron J, Steding-Jessen K, Hoepers C, Granville L, Margi C. Improving IoT botnet investigation using an adaptive network layer. *Sensors*. 2019;19(3):727.
55. Angrishi K. Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets. arXiv preprint arXiv:1702.03681 2017.
56. Antonakakis M, April T, Bailey M, et al. Understanding the Mirai botnet. Paper presented at: Proceedings of the 26th USENIX Security Symposium; 2017, pp. 1093-1110.
57. Marzano A, Alexander D, Fonseca O, et al. The evolution of Bashlite and Mirai IoT botnets. Paper presented at: 2018 IEEE Symposium on Computers and Communications (ISCC); 2018, pp. 00813-00818.
58. Malware MustDie. MMD-0057-2016-Linux/LuaBot-IoT botnet as service. https://blog.malwaremustdie.org/2016/09/; 2016.
59. Edwards S, Profetis I. Hajime: analysis of a decentralized internet worm for IoT devices. *Rapidity Networks*. 2016;16:1-18.
60. De Donno M, Dragoni N, Giaretta A, Spognardi A. Analysis of DDoS-capable IoT malwares. paper presented at: 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague; 2017, pp. 807-816.
61. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf; 2008.
62. Guan Z, Si G, Zhang X, et al. Privacy-preserving and efficient aggregation based on Blockchain for power grid Communications in Smart Communities. *IEEE Commun Mag*. 2018;56(7):82-88.
63. Abidin A, Aly A, Cleemput S, Mustafa M. Secure and privacy-friendly local electricity trading and billing in smart grid. arXiv Preprint arXiv:1801.08354 2018.
64. Sun Y, Lampe L, Wong V. Smart meter privacy: exploiting the potential of household energy storage units. *IEEE Internet Things J*. 2017;5(1):69-78.
65. Azar A, Nazaripouya H, Khaki B, Chu C, Gadh R, Jacobsen R. A non-cooperative framework for coordinating a neighborhood of istributed Prosumers. *IEEE Trans Ind Inform*. 2019;15(5):2523-2534.
66. Laszka A, Dubey A, Eisele S, Walker M, Kvaternik K. Design and implementation of safe and private forward-trading platform for iot-based transactive microgrids. arXiv preprint arXiv:1709.09614; 2018.
67. Reed M, Syverson P, Goldschlag D. Anonymous connections and onion routing. *IEEE J Selected Areas Commun*. 1998;16(4):482-494.
68. Liu P, Wang L, Tan Q, Li Q, Wang X, Shi J. Empirical measurement and analysis of I2P routers. *J Networks*. 2014;9(9):2269.
69. Biryukov A, Pustogarov I. Bitcoin over Tor isn't a good idea. Paper presented at: SP'15: Proceedings of the 2015 IEEE Symposium on Security and Privacy; 2015, pp. 122-134.
70. Bergquist J, Laszka A, Sturm M, Dubey A. On the design of communication and transaction anonymity in blockchain-based transactive microgrids. Paper presented at: SERIAL'17: Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers; 2017, pp. 1-6.
71. Van Saberhagen N. CryptoNote v 2.0. https://cryptonote.org/whitepaper.pdf; 2013.
72. Du X, Xiao Y. Energy efficient chessboard clustering and routing in heterogeneous sensor networks. *IJWMC*. 2006;1(2):121-130.
73. Du X, Xiao Y, Ci S, Guizani M, Chen HH. A routing-driven key management scheme for heterogeneous sensor networks. Paper presented at: 2010 8th World Congress on Intelligent Control and Automation, Jinan; 2007, pp. 3407-3412.
74. Pal O, Alam B, Thakur V, Singh S. Key management for blockchain technology. ICT Express; 2019.
75. Ouaddah A, Elkalam A, Ouahman A. Towards a novel privacy-preserving access control model based on Blockchain technology in IoT. In: Rocha Á, Serrhini M, Felgueiras C, eds. *Europe and MENA cooperation advances in information and communication technologies. Advances in intelligent systems and computing*. Cham: Springer; 2017:520, 523-533.
76. Ma M, Shi G, Li F. Privacy-oriented Blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. *IEEE Access*. 2019;7:34045-34059.
77. Feige U, Fiat A, Shamir A. Zero-knowledge proofs of identity. *J Cryptol*. 1988;1(2):77-94.
78. Rackoff C, Simon D. Non-interactive zero-knowledge proof of knowledge and chosen Ciphertext attack. In: Feigenbaum J, ed. *Advances in Cryptology—CRYPTO'91. CRYPTO 1991. Lecture Notes in Computer Science*. Vol 576. Berlin, Heidelberg: Springer; 1991:433-444.
79. Hardjono T, Smith N. Cloud-based commissioning of constrained devices using permissioned Blockchains. Paper presented at: The 2nd ACM International Workshop; 2016, pp. 29-36.
80. Brickell E, Li J. Enhanced privacy ID: a direct anonymous attestation scheme with enhanced revocation capabilities. *IEEE Trans Depend Secure Comput*. 2011;9(3):345-360.
81. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: the Blockchain model of cryptography and privacy-preserving smart contracts. Paper presented at: 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA; 2016, pp. 839-858.
82. Miers I, Garman C, Green M, Rubin A. Zerocoin: anonymous distributed E-cash from Bitcoin. Paper presented at: 2013 IEEE Symposium on Security and Privacy, Berkeley, CA; 2013, pp. 397-411.
83. Ben-Sasson E, Chiesa A, Garman C, et al. Zerocash: decentralized anonymous payments from Bitcoin. Paper presented at: 2014 IEEE Symposium on Security and Privacy, San Jose, CA; 2014, pp. 459-474.
84. Dagher G, Bünz B, Bonneau J, Clark J, Boneh D. Provisions: privacy-preserving proofs of solvency for Bitcoin exchanges. Paper presented at: CCS'15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security; 2015, pp. 720-731.

85. El Ioini N, Pahl C. A review of distributed ledger technologies. In: Panetto H, Debruyne C, Proper H, Ardagna C, Roman D, Meersman R, eds. *On the move to meaningful internet systems. OTM 2018 Conferences. OTM 2018. Lecture Notes in Computer Science*. Vol 11230. Cham: Springer; 2018:277-288.
86. Zhao S, Wang B, Li Y, Li Y. Integrated energy transaction mechanisms based on Blockchain technology. *Energies*. 2018;11(9):2412.
87. Li C, Palanisamy B, Xu R. Scalable and Privacy-preserving Design of On/Off-chain Smart Contracts. arXiv preprint arXiv:1902.06359; 2019.
88. Luo F, Dong Z, Liang G, Murata J, Xu Z. A distributed electricity trading system in active distribution networks based on multi-agent coalition and Blockchain. *IEEE Trans Power Syst*. 2018;34(5):4097-4108.
89. Zyskind G, Nathan O, Pentland A. Decentralizing privacy: using Blockchain to protect personal data. Paper presented at: 2015 IEEE Security and Privacy Workshops, San Jose, CA; 2015, pp. 180-184.
90. Erdin E, Cebe M, Akkaya K, Solak S, Bulut E, Uluagac S. Building a private Bitcoin-based payment network among electric vehicles and charging stations. Paper presented at 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada; 2018, pp. 1609–1615.
91. Khalil R, Gervais A. Revive: rebalancing off-blockchain payment networks. Paper presented at: CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security; 2017, pp. 439-453.
92. Deng L, Chen H, Zeng J, Zhang L. Research on cross-chain technology based on Sidechain and hash-locking. In: Liu S, Tekinerdogan B, Aoyama M, Zhang LJ, eds. *Edge Computing—EDGE 2018. EDGE 2018. Lecture Notes in Computer Science*. Vol 10973. Cham: Springer; 2018:144-151.
93. Back A, Corallo M, Dashjr L, et al. Enabling Blockchain Innovations with Pegged Sidechains. http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains; 2014; 72.
94. Ali M, Dolui K, Antonelli F. IoT data privacy via Blockchains and IPFS. Paper presented at: ACM International Conference Proceeding Series; 2017, pp. 1-7.
95. Jiang Y, Wang C, Wang Y, Gao L. A cross-chain solution to integrating multiple Blockchains for IoT data management. *Sensors*. 2019;19(9):2042.
96. Johng H, Kim D, Hill T, Chung L. Using Blockchain to enhance the trustworthiness of business processes: a goal-oriented approach. 2018 IEEE International Conference on Services Computing (SCC), San Francisco, CA; 2018, pp. 249–252.
97. Firoozjaei MD, Ghorbani A, Kim H, Song J. Hy-bridge: a hybrid Blockchain for privacy-preserving and trustful energy transactions in internet-of-things platforms. *Sensors*. 2020;20(3):928.
98. Samarati P, Sweeney L. Generalizing Data to Provide Anonymity when Disclosing Information. Paper presented at: PODS '98: Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of Database Systems.; 1998, pp. 275487-275508.
99. Samarati P. Protecting respondents identities in microdata release. *IEEE Trans Knowl Data Eng*. 2001;13(6):1010-1027.
100. Firoozjaei MD, Yu J, Choi H, Kim H. Privacy-preserving nearest neighbor queries using geographical features of cellular networks. *Comput Commun*. 2017;98:11-19.
101. Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramaniam M. L-diversity: privacy beyond k-anonymity. *ACM Trans Knowl Discov Data (TKDD)*. 2007;1(1):3.
102. Yucel F, Bulut E, Akkaya K. Privacy preserving distributed stable matching of electric vehicles and charge suppliers. Paper presented at: 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL; 2018: 1-6.
103. Gale D, Shapley L. College admissions and stability of marriage. *Am Math Monthly*. 1962;69:9-15.
104. van IJzendoorn VB. The challenge of decentralized marketplaces. arXiv preprint arXiv:1703.05713; 2017.
105. Paillier P. Public-key cryptosystems based on composite degree Residuosity classes. In: Stern J, ed. *Advances in Cryptology—EUROCRYPT '99. EUROCRYPT 1999. Lecture Notes in Computer Science*. Vol 1592. Berlin, Heidelberg: Springer; 1999:223-238.
106. Nunna HK, Doolla S. Multiagent-based distributed-energy-resource Management for Intelligent Microgrids. *IEEE Trans Ind Electron*. 2012;60(4):1678-1687.
107. Malina L, Hajny J, Dzurenda P, Ricci S. Lightweight ring signatures for decentralized privacy-preserving transactions. Paper preseted at: Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018), Vol 2: SECRYPT; 2018, pp. 692-697.
108. Rivest R, Shamir A, Tauman Y. How to leak a secret. In: Boyd C, ed. *Advances in Cryptology—ASIACRYPT 2001. ASIACRYPT 2001. Lecture Notes in Computer Science*. Vol 2248. Berlin, Heidelberg: Springer; 2001:552-565.
109. Liu J, Wei V, Wong D. Linkable spontaneous anonymous group signature for AD hoc groups. In: Wang H, Pieprzyk J, Varadharajan V, eds. *Information Security and Privacy. ACISP 2004. Lecture Notes in Computer Science*. Vol 3108. Berlin, Heidelberg: Springer; 2004:325-335.
110. Dwivedi A, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare Blockchain for IoT. *Sensors*. 2019;19(2):326.
111. Miller A, Möser M, Lee K, Narayanan A. An empirical analysis of Linkability in the Monero Blockchain. arXiv preprint arXiv:1704.04299; 2017.
112. Au M, Chow S, Susilo W, Tsang P. Short linkable ring signatures revisited. In: Atzeni AS, Lioy A, eds. *Public Key Infrastructure. EuroPKI 2006. Lecture Notes in Computer Science*. Vol 4043. Berlin, Heidelberg: Springer; 2006:101-115.
113. Chow SS, Susilo W, Yuen T. Escrowed Linkability of ring signatures and its applications. In: Nguyen PQ, ed. *Progress in Cryptology—VIETCRYPT 2006. VIETCRYPT 2006. Lecture Notes in Computer Science*. Vol 4341. Berlin, Heidelberg: Springer; 2006:175-192.

114. Tsang P, Wei V. Short linkable ring signatures for E-voting. In: Deng RH, Bao F, Pang H, Zhou J, eds. *Information Security Practice and Experience. ISPEC 2005. Lecture Notes in Computer Science*. Vol 3439. Berlin, Heidelberg: Springer; 2005:48-60.
115. Franklin M, Zhang H. A framework for unique ring signatures. *IACR Cryptol ePrint Arch*. 2012;2012:577.
116. Mercer R. Privacy on the blockchain: unique ring signatures. arXiv preprint arXiv:1612.01188; 2016.
117. Aitzhan N, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, Blockchain and anonymous messaging streams. *IEEE Trans Depend Secure Comput*. 2016;15(5):840-852.
118. Firoozjaei MD, Kim M, Song J, Kim H. O2TR: Offline OTR Messaging system under network disruption. *Comput Secur*. 2019;82:227-240.
119. Guo R, Shi H, Zhao Q, Zheng D. Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems. *IEEE Access*. 2018;6:11676-11686.
120. Noether S, Mackenzie A, The Monero Research Lab. Ring confidential transactions. *Ledger*. 2016;1:1-18.
121. Le T, Mutka M. The Monero Research Lab CapChain: a privacy preserving access control framework based on Blockchain for pervasive environments. Paper presented at: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina; 2018, pp. 57-64.
122. Bitting E, Carter J, Ghorbani A. Multiagent system development kits: An evaluation. Paper presented at: Proceedings of the CNSR; 2003, pp. 80-92.
123. Sood A, Enbody R. Chain exploitation—social networks malware. *ISACA J*. 2011;1:31.
124. Schnoor H, Woizekowski O. Active linkability attacks. arXiv preprint arXiv:1311.7236; 2013.
125. Tulyakov S, Jaeger S, Govindaraju V, Doermann D. Review of classifier combination methods. In: Marinai S, Fujisawa H, eds. *Machine Learning in Document Analysis and Recognition. Studies in Computational Intelligence*. Vol 90. Berlin, Heidelberg: Springer; 2008:361-386.

AUTHOR BIOGRAPHIES

Mahdi Daghmehchi Firoozjaei is a Postdoctoral research fellow at the Canadian Institute for Cybersecurity, University of New Brunswick, Canada, since September 2018. He received a BSc. degree in Telecommunication Engineering from the Scientific-applied Faculty of Post and Telecommunication, an MSc. degree in Telecommunication-Cryptology from Imam Hossein Comprehensive University, Tehran, Iran, and his PhD. degree in Computer Engineering from the Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea in 2000, 2005, and 2018, respectively. He worked for the Telecommunication Company of Iran (TCI), Babol, Iran, as a senior engineer from 2006 to 2014. His research interest focuses on blockchain, digital forensics, network security, and privacy-preserving. He was awarded the "Best Paper Award" in IEEE AINA 2015 and was the winner of the "2nd Prize for the Superior Research Award" of Sungkyunkwan University in 2017.

Rongxing Lu is currently an associate professor at the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore from April 2013 to August 2016. Rongxing Lu worked as a Postdoctoral Fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal", when he received his PhD degree from the Department of Electrical & Computer Engineering, University of Waterloo, Canada, in 2012; and won the eighth IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. He is presently a senior member of IEEE Communications Society. His research interests include applied cryptography, privacy-enhancing technologies, and IoT-Big Data security and privacy. He has published extensively in his areas of expertise and was the recipient of nine best (student) paper awards from some reputable journals and conferences. Currently, Dr Lu serves as the Vice-Chair (Conferences) of IEEE ComSoc CIS-TC (Communications and Information Security Technical Committee). Dr Lu is the Winner of 2016-2017 Excellence in Teaching Award, FCS, UNB.

Ali A. Ghorbani has held a variety of positions in academia for the past 38 years and is currently a Professor of Computer Science, Tier 1 Canada Research Chair in Cybersecurity, the Director of the Canadian Institute for Cybersecurity, which he established in 2016, and an IBM Canada Faculty Fellow. He served as the Dean of the Faculty of Computer Science at the University of New Brunswick from 2008 to 2017. Dr Ghorbani is also the founding director of the laboratory for intelligence and adaptive systems research. He has spent over 28 years of his 38-year academic career carrying out both fundamental and applied research in the area of cybersecurity, machine learning, and web intelligence. His current research focus is cybersecurity, Web Intelligence, and Critical Infrastructure Protection. Dr Ghorbani is the co-inventor on three awarded patents in the area of Network Security and Web Intelligence and has published over 270 peer-reviewed articles during his career. He has supervised over 180 research

associates, postdoctoral fellows, graduate, and undergraduate students during his career. His book, Intrusion Detection and Prevention Systems: Concepts and Techniques, was published by Springer in October 2010. Dr Ghorbani is the co-founder of the Privacy, Security, Trust (PST) Network in Canada and its annual international conference. He has served as General Chair and Program Chair/Co-Chair for 16 International Conferences and Workshops and served as the co-Editor-In-Chief of Computational Intelligence: An International Journal from 2007 to 2017. Dr. Ghorbani developed a number of technologies that have been adopted by high-tech companies. He co-founded two startups, Sentrant Security and EyesOver Technologies in 2013 and 2015, respectively. He is the recipient of the 2017 Startup Canada Senior Entrepreneur Award.

How to cite this article: Firoozjaei MD, Lu R, Ghorbani AA. An evaluation framework for privacy-preserving solutions applicable for blockchain-based internet-of-things platforms. *Security and Privacy*. 2020;3:e131. https://doi.org/10.1002/spy2.131