Privacy-Preserving Blockchain-Based Solutions in the Internet of Things

Nikolaos Zapoglou[1], Ioannis Patsakos[1], George Drosatos[2], and Konstantinos Rantos[1]

[1] Dept. of Computer Science, International Hellenic University, Kavala, Greece
{xizapog,iopatsa,krantos}@cs.ihu.gr
[2] Inst. for Language and Speech Processing, Athena Research Center, Xanthi, Greece
gdrosato@athenarc.gr

Abstract. Internet of Things (IoT) is a promising, relatively new technology that develops "smart" networks with a variety of uses and applications (e.g., smart cities, smart home and autonomous cars). The diversity of protocols, technologies and devices that IoT consists of, even though they add in value and utility, they create major privacy issues that can be exploited by malicious entities to benefit from or even violate privacy of IoT users. The special features of blockchain technology, such as immutability, transparency, accessibility, autonomy and decentralisation, has led the academics and the industry to search for further uses of it, besides financial applications (e.g., Bitcoin) that was initially applied. This paper is a survey on the existing literature regarding blockchain-based privacy-preserving solutions that have been proposed specifically for the IoT to address personal data protection and preserve user privacy.

Keywords: Internet of Things (IoT) · Blockchain Technology · Privacy-preserving solutions.

1 Introduction

In the past decade, a new technology named Internet of Things (IoT), has been introduced in most aspects of our modern life. Countless devices, such as meters, cameras and actuators, are connected to networks with the purpose to make our lives easier, our industry more efficient, our healthcare more patient-centric, our world "smarter" and much more [21]. Vast volumes of data, including personal ones, are being collected, generated, transferred and processed through IoT networks which mainly consist of devices with limited resources, where conventional security and privacy protection techniques do not work or are too expensive to adopt [38]. Given the sensitive nature of the data and the potentially harmful information that can be extracted from the IoT ecosystem, it soon became clear that effective and relatively easy ways to overcome these issues had to be invented.

Blockchain technology, a decentralised immutable public "database", can solve or address sufficiently some of the user privacy issues and personal data

ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2021
Published by Springer Nature 2021.
H. Santos et al. (Eds.): SmartCity 360 2020, LNICST, pp. 1–20, 2021.
https://doi.org/10.1007/978-3-030-xxxxx-x_x

protection in the IoT. It gained popularity due to the creation of the first digital cryptocurrency, Bitcoin [25]. There are a lot more applications than Bitcoin, where blockchain technology can be a pioneer and enhance existing technologies and their security and privacy properties.

The structure of a blockchain network, the use of advanced cryptographic mechanisms in a blockchain, and the use of smart contracts [5], are some of the key-factors that can contribute in upgrading/preserving privacy issues in various IoT networks. This paper provides a literature review of the various approaches and applications of blockchain technology to address privacy issues sourcing in the IoT ecosystem. The rest of this paper is organised as follows. Section 2 provides a brief background analysis on IoT and blockchain technologies. The methodology used in conducting this research is described in Section 3. Section 4 presents identified blockchain-based solutions that have been proposed for preserving users privacy in the IoT domain. Section 5 discusses the identified solutions and provides future research directions. Finally, Section 6 concludes the paper.

2 Background and Related Work

The IoT ecosystem comprises many applications and services that can be combined with other edge technologies, such as machine learning, big data and blockchain technology to provide the, so-called, smart environments with promising results. The amount of user-related personal data being generated, processed and transferred in the diversified IoT deployments (in terms of protocols, technologies, and devices), attract a lot of unwanted attention by threat agents who target, among others, users' personal data. Figure 1 depicts a typical example of a user IoT ecosystem with privacy challenges.

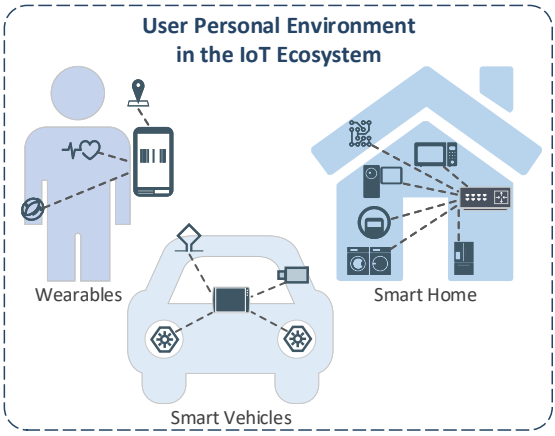

Fig. 1. Example of user personal environment in the IoT ecosystem.

Privacy is an ambiguous concept that cannot be clearly defined and can be affected by the individual's perception on the protection of its own personal environment. In compute science, it is recognised as data or information privacy, refers to the relationships between technology and the legal right to, or public expectation of, privacy in the collection and exchange of personal data [10]. Privacy restrictions typically stem from applicable legal frameworks. For example, in the European Union, the General Data Protection Regulation (GDPR) [12] has come into force to create an even higher level, than before, of privacy protection within the EU and gave citizens control over their personal data. Given the volume of the personal data being handled by IoT devices, it is easy to understand that the GDPR has many implications to many IoT domains.

Blockchain is an append-only decentralised digital public ledger based on cryptography. A record of all the transactions that take place inside the blockchain is being maintained in a chronological order (time-stamped) in a distributed database, in the form of blocks in a chain. All the participating nodes in this peer-to-peer network get a duplicated copy of the blockchain database.

When the participating nodes agree on the validity of a transaction and the requirements of the consensus algorithm have been satisfied, a time-stamped block is added to the blockchain. After a block becomes part of the blockchain it is nearly impossible to tamper with it [19]. Accordingly, the overall blockchain framework consists of three layers, as depicted in Figure 2: the application layer, the data layer and the network layer [17]. The application layer includes all the features, applications and uses of blockchain. The data layer is self-explanatory and the network layer handles all the connectivity matters of blockchain.

The applications of blockchain vary and include financial services, healthcare, rights management, IoT and security. The key features of blockchains, such as decentralisation, transparency, open source, accessibility, autonomy and immutability [19] make them very attractive to many environments, as they can successfully address significant security requirements. Still though, there are privacy challenges that need to be considered when applying blockchain technology [13].

Although blockchain technology has been extensively studied in the IoT [7, 31] and proposed to protect privacy for IoT devices [47], to the best of our knowledge, there has been only one similar work [43] reviewing blockchain-based methods that facilitate privacy preservation in IoT. However, Sharma et al. [43] in their work focus only on two issues, i.e. the device authentication and the decentralised identifiers. In this paper, we present a wider range of privacy preserving blockchain-based solutions in IoT and categorise them according to the topic in which they proposed a solution and the approach they used.

3 Research Methodology

The methodology that we followed consists of two main steps:

1. Extensive search in the research literature maintained in Scopus search engine (`www.scopus.com`), a certified academically approved tool. The goal

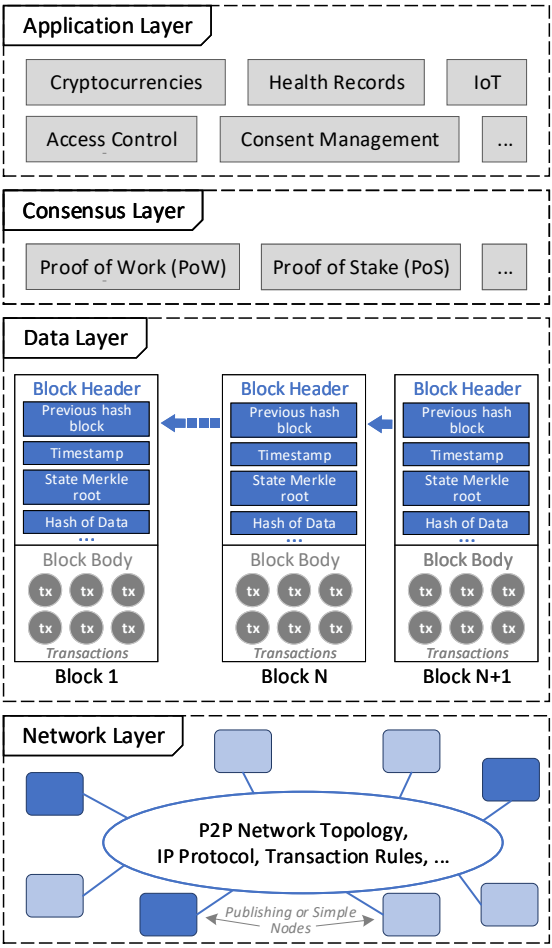

Fig. 2. Framework of blockchain technology.

of our search was to find explicitly the related keywords of "privacy" and "blockchain" in the title of the papers and the related keywords of "IoT" in the title, abstract and keywords. The exact query which was used in April 2020 and returned us 96 relevant papers, was the following:

```
TITLE((Privacy OR "Personal Data") AND (Blockchain OR "Distributed
    Ledger")) AND TITLE-ABS-KEY(IoT OR "Internet of Things" OR
    "Internet-of-Things")
```

2. By studying the Title – Abstract – Conclusion parts of each of the above papers we were able to narrow down even more the relevant, to our subject, papers. In this step we excluded papers that were addressing specific sectors of IoT networks (e.g., apply only in VANET, MIoT, UAV technology,

healthcare, etc.) and we focused on papers that had potential solutions in wider and more generalised application in IoT.

Figure 3 shows (i) the yearly distribution of publications that deal with privacy solutions in blockchain technology (i.e. the first part of our query in methodology), (ii) the number of publications per year that we focus on this paper based on the query of our methodology, and (iii) the percentage of (ii) in (i) for each year. This demonstrates the interest that the research community shows on the use of privacy-preserving blockchain solutions in the IoT ecosystem. Based on these statistical results we infer that the global interest in this kind of solutions is rising and gaining ground fast, with the amount of relevant to the matter papers almost doubling each year, since the publication of the first research paper in 2017.

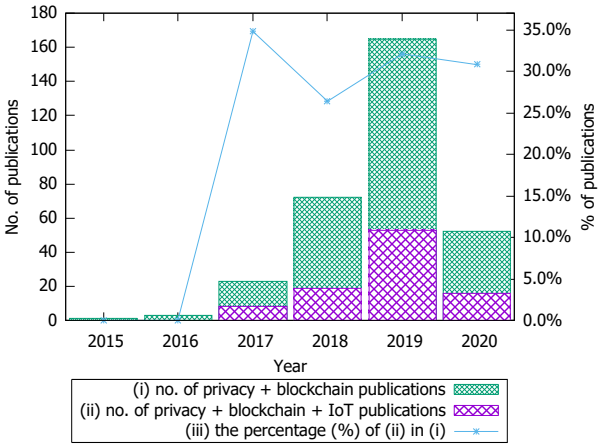

Fig. 3. Number and percentage of publications per year in Scopus.

4 Privacy Preserving Blockchain-based Solutions in IoT

This section presents, in a chronological order, the solutions that were identified in the literature by using the methodology described in Section 3. The subsections below provide a brief description about the functionality, usage, and the privacy preserving nature of each of the identified solutions. Table 1 summarizes some of their properties.

4.1 FairAccess

FairAccess is a privacy-preserving blockchain-based access control framework for IoT, introduced by Ouaddah et al. [28, 29], which combines access control

Table 1. Comparison of privacy preserving blockchain-based solutions in the IoT.

Proposed Solution	IoT Area	Blockchain Infrastructure	Privacy-Preserving Provided Service	Underlying Privacy Mechanism	Implementation
FairAccess [28]	IoT	Bitcoin	Access control	Encrypted authorization tokens with ECC	Proof of concept
BC Gateways [6]	IoT	Ethereum	Access control	Smart contracts & Preference policies	Proposal
PPB-ABE [34]	IoT	Public blockchain	Access control	Attribute-based encryption (ABE)	Numerical analysis
CapChain [20]	IoT	Monero	Access control	Capability obfuscation & Ring signature	Proof of concept
PPDAC [27]	IoT	Public blockchain	Access control	DMCP-ABE & zk-SNARKs	Proposal
ADVOCATE [37]	IoT	Public blockchain	Consent management	Data minimization & Hashing	Proof of concept
SecureSVM [44]	Smart City	–	Machine learning	Paillier homomorphic encryption	Experimental
TrustChain [18]	IoT	New permissioned blockchain	Distributed ledger	ZKP, Encryption & Anonymization	Proposal
PBEM-SGN [16]	Smart Grid	Permissioned blockchain	Energy transactions	Group signatures & Covert channel authorization	Experimental
PrivySharing [23]	Smart City	Hyperlegder Fabric	Access control & Data sharing	Smart contracts & Access control rules	Experimental
Xyreum [40]	IIoT	–	Multi-factor authentication & Key establishment	T-ZKPK & Authenticated encryption	Experimental
Hy-Bridge [15]	Smart Grid	Pysimplechain	Energy transactions	k-anonymity, Suppression & Data Generalization	Simulation
BFL-PPDS [22]	IIoT	Permissioned blockchain	Data sharing	Federated learning & Differential privacy	Experimental

and cryptocurrency mechanisms. Through the use of encrypted authentication tokens (data structures transferred from peer to peer via transactions) enforced by smart contracts [5], an IoT device owner can manage access rights and policies (get, revoke, update, etc.) in a flexible and easy to apply manner. The encryption of token is performed using the built-in elliptic-curve cryptosystem (ECC).

FairAccess addresses several IoT privacy and security requirements, such as decentralisation, lightweightness, identification (allowing thing-to-thing interactions), fine-grained and user-driven access control, transparency, unlikability and pseudonymity [27]. Although, some issues in IoT are successfully addressed thanks to FairAccess, some other critical issues emerged: (1) There is a discrepancy between the sensitive and private nature of access control policies and the transparent and public nature of blockchain technology. (2) Traceability, allowing third parties to detect thing-to-thing communication patterns and authorisation functionality patterns.

FairAccess is experimentally implemented with a Raspberry Pi 2 device and a local Bitcoin network (regression test mode) [28].

4.2 BC Gateways

Cha et al. [6] propose the usage of blockchain connected gateways (BC Gateways) to preserve users' privacy by providing access to the data of IoT devices according to a given preference policy. These gateways store user privacy preferences of IoT devices in a blockchain infrastructure. The blockchain gateways play the role of a mediator between users and IoT devices.

Users can acquire the information and privacy policies of an IoT device connected to a blockchain gateway and access the device via the blockchain gateway rather than accessing the device directly. Consequently, the blockchain gateway impede the device from obtaining personal data unless users accept the device's privacy policies. The data stored in a blockchain infrastructure is tamper-resistant, thus, user's preferences can be utilised to resolve disputes between users and IoT service providers. Finally, the above-mentioned system utilises Ethereum [5] to support its idea utilising smart contracts.

4.3 Privacy-Preserving Blockchain Based IoT Ecosystem using Attribute-Based Encryption (PPB-ABE)

Rahulamathavan et al. [34] proposed a solution that uses decentralised attribute-based encryption (ABE) to preserve confidentiality and privacy of transaction data in blockchain-based IoT applications. Their method, which is followed a similar approach with [9], utilises more powerful devices (e.g., smartphones and home routers) than IoT sensors as *cluster heads* to perform computationally expensive operations on behalf of IoT sensors. These operations are mainly data aggregation and encryption required in the generation of transaction data. The encryption of transaction data is performed by cluster heads and in such a way that can only be seen and verified by entities who have the *right attributes*.

Satisfying the requirements of ABE, the entities involved in the proposed scheme are (1) cluster heads, responsible of the aforementioned processing, (2) blockchain miners who verify transactions and contribute to the blockchain, (3) attribute authorities (AAs) and (4) the blockchain with blocks of transactions. The cluster head encrypts data wisely to target the particular miners with the right attributes. The blockchain miners verify the transacted data and the transaction itself. After that, they mine, add new blocks to the blockchain and get rewarded with tokens. The AAs have to verify and issue credentials for distinct users and miners according to their attributes. Finally, the authors provide a numerical analysis to estimate the added complexity of ABE in the blockchain.

4.4 CapChain

Le and Mutka proposed CapChain [20], a privacy preserving access control framework for pervasive environments that is based on blockchain technology. CapChain allows users to share access rights to devices they own by managing capabilities, i.e. tokens that represent access rights to IoT devices. Capabilities are generated and encrypted by the device's owner, and transferred by appropriate anonymous transactions that take place on a public blockchain. The latter serves as a public immutable ledger that records capabilities authorisations.

Device owners have full control over the delegations they provide as they can assign expiration dates on them, can track and revoke the whole chain of the delegations they provided, and control capabilities from multiple domains with the use of a single account. Participants identities and transaction details are protected. To ensure their privacy, CapChain adapts well-established techniques,

such as obfuscation to hide capability ID and ring signature to avoid unauthorised capability commitment. An overview of the access rights delegation process is shown in Figure 4.

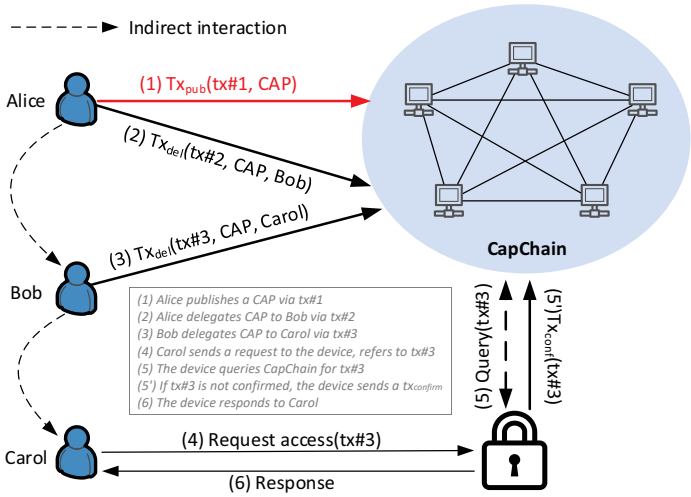

Fig. 4. CapChain overview [20].

CapChain employs a similar idea to transfer authorisation tokens through transactions such as FairAccess [28]. Simultaneously, it is affected by anonymous cryptocurrencies such as CryptoNote [39], Monero [26] and ZeroCash [41] since it proposes a token named CAP to get access in IoT device. In addition, the authors analyse their scheme as a case study under the consensus of an adapted proof-of-work (PoW) from Monero.

4.5 PPDAC

Ouaddah proposed a privacy-preserving distributed access control scheme that is called PPDAC [27]. PPDAC is a lightweight and privacy-preserving access control framework based on the rising blockchain technology, mainly the unlicensed and public type, to assure in-depth access control functions for IoT devices with strong anonymity guarantee for IoT end-users. The proposed scheme preserves the merits of blockchain to meet IoT security and privacy arising needs while overcoming the challenges in integrating blockchain to IoT. PPDAC is integrated over FairAccess [28] that successfully ensures IoTs security and privacy requirements. The reason why the author has developed PPDAC scheme was to strengthen users' anonymity and to maintain transparency features in FairAccess. More precisely, it is developed a policy-hiding access control scheme that protects both sensitive attributes and policies using a white box of distributed

multi-authority ciphertext policy attribute-based encryption (DMCP-ABE) [3]. Additionally, to enable untraceability of authorisation tokens, it is introduced a zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) protocol [4]. To sum up, the provided approach respects principles, such as security through transparency, user-driven policy, privacy by design and edge intelligence.

4.6 ADVOCATE

ADVOCATE is an innovative platform that addresses the problem that users are bound to face in the IoT ecosystem with managing their devices, and the personal data these devices manage [35,37]. The proposed solution tries to satisfy the GDPR [12] requirements about users being able to control their personal data and be informed and to consent to processing by third parties. It also helps third parties wishing to access such data to meet the requirements of the Regulation, such as informing users in a transparent and unambiguous manner about the data they manage, their purposes and the processing periods.

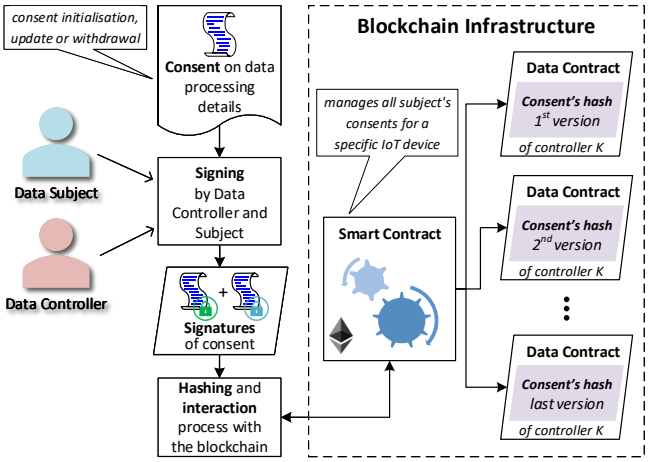

Fig. 5. The steps followed by the ADVOCATE to secure a consent [37].

ADVOCATE focuses on the management of devices that users own, and on allowing the latter to formulate and easily manage their personal data protection policy and consents. An Intelligent Policies Analysis Mechanism utilises intelligent adaptive technologies to identify contradictory or conflicting rules and policies related to the disposal of private information and ensure that these cannot be used for user profiling [8,36].

The consents management component responsible for providing integrity, versioning control, non-repudiation and validity of data subjects consents and data

controllers commitments is based on a blockchain. Signed consents to data controllers are added to the ledger without however, disclosing any details about the users' identities or the devices they handle (Figure 5).

The authors do not bind their architecture to a specific Blockchain solution. They rather focus on the consensus algorithm and they suggest the use of a Proof-of-Authority (PoA) one, which requires less messages exchanges and offers better performance.

4.7 SecureSVM

Shen et al. [44] proposed SecureSVM, a privacy-preserving Support Vector Machine (SVM) training scheme over blockchain-based encrypted IoT data. SecureSVM addresses the challenging task of incorporating blockchain into a machine learning training process. The first challenge was to design an appropriate training data format that could be easily accommodated by a blockchain solution while preserving the data privacy of each individual provider. The second challenge lied with the elaboration of a training algorithm that constructs accurate SVM classifiers using the data recorded on the blockchain without disclosing sensitive data.

The proposed supervised learning process consists of two phases, i.e. the training phase and the classification phase. In comparison to previous works, [46], [48] and [33], SecureSVM combines the Paillier cryptosystem [30] (an efficient additive homomorphic encryption system) with blockchain techniques to address the concerns about data privacy, integrity, and ownership, during training SVM classifiers with IoT data originating from different providers. Thus, the proposed privacy-preserving SVM training algorithm can be used without the need of a trusted third party and is able to train SVM classifiers without accuracy loss. The authors concluded that with the use of SecureSVM, each data provider is unable to acquire any knowledge regarding the data of other providers, while the data analysts model parameters are also kept hidden from data (data providers encrypt their data locally by using their own private keys).

The authors do not provide details about the types of blockchains that their proposed solution requires. Moreover, the experimental results they provide are about the performance of secureSVM in terms of accuracy and efficiency through experiments they conducted using real-world datasets, without however, experimenting on a specific blockchain solution.

4.8 TrustChain

A privacy-preserving permissioned blockchain, named TrustChain, is proposed by Jayasinghe et al. [18] to overcome issues related to energy consumption and delays found in traditional blockchain architectures. IoT devices do not have the enormous energy resources required to verify each block of data in the blockchain.

TrustChain does so by combining the power of blockchains with trust concepts. This research work studies how TrustChain can evolve in edge computing environments with dissimilar levels of enhancements to efface delays and privacy

concerns associated with centralised processing and to maintain resources in IoT ecosystem. TrustChain is designed to increase the privacy of its participants while improving the effectiveness of services. The main difference of TrustChain to other convectional blockchains is the application of computational trust on realising various functions inside the provided distributed ledger service. It develops a novel lightweight consensus management protocol by combining this trust with the Byzantine Fault Tolerance (BFT) protocol [45]. Indicatively, to evaluate the provided trust, it measures the reliability of participating parties before creating smart contracts and initiating interactions among them. Additionally, TrustChain delegates the edge computing architecture of IoT due to its durability with low storage and computing resources. Finally, TrustChain embeds unique techniques to improve privacy when dealing with sensitive personal data and complies with GDPR legislation [12] by applying techniques, such as zero knowledge proof (ZKP), encryption, and anonymization.

4.9 PBEM-SGN

Gai et al. [16], utilised a permissioned blockchain to address privacy protection and energy security in smart grids. The proposed system provides transparency and traceability on users' energy usage, without, however, revealing participating nodes identities. Users are identified in the blockchain by the use of pseudonyms.

Storing data on the permissioned blockchain facilitates data protection, while access authorisation is secured by the use of traditional access control methods, such as attribute-based authorisation, as well as Covert Channel Authorisation (CCA) techniques [42]. Edge node/user identities are registered with the use of a group signature algorithm and validated by a super node using CCA. The use of group signatures for edge nodes facilitates anonymity as nodes in the group do not know each other's identity but only the identity of the super node which is responsible for organising resource allocation. Figure 6 depicts the main activities that take place in the PBEM-SGN proposed blockchain.

The authors provided a practical proof of their proposed scheme on Ethereum, using the standalone client Geth and Ethereum Wallet.

4.10 PrivySharing

Makhdoom et al. [23], proposed a blockchain-based framework, called PrivySharing, that aims to facilitate data-sharing in smart cities while protecting users' privacy and providing data security. The authors utilise the channels mechanism of the Hyperledger Fabric platform [2] to control access to specific types of data, such as health and smart energy, by a group of authorised organisations. The adoption of multiple channels provides increased privacy of user data but also scalability to their proposed solution. Fine-grained access control to user data is further secured by the adoption of access control rules in the smart contracts, which allows data exposure to stakeholders, on the need-to-know basis.

Moreover, PrivySharing complies with some of the most significant data security and privacy requirements of the GDPR [12], such as the "right to forget".

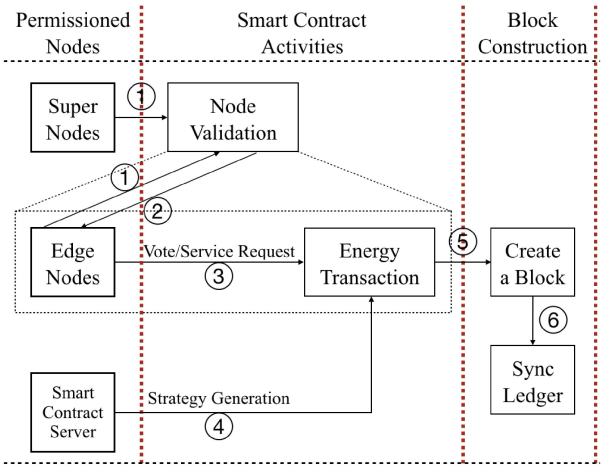

Fig. 6. Main activities in the PBEM-SGN blockchain system [16].

The methodology is based on agile blockchain application development guidelines [24], for reducing the transaction settlement time for real-time applications. Furthermore, the solution provides data integrity, tamper-resistance, and non-repudiation.

PrivySharing grants secure client access to the blockchain network through a REST API. It also defines a reward system for users sharing their data with stakeholders or third parties, with a local digital token named PrivyCoin. Finally, their experimental results verified that a multi-channel blockchain solution scales better than a single channel blockchain system.

4.11 Xyreum

Xyreum, proposed by Sani et al. [40], is a scalable high-performance blockchain scheme providing security and privacy for the Industrial Internet of Things (IIoT). The model aims to overcome problems in IIoT, such as high computational complexity and latency challenges, which are considered inappropriate for this environment. Their proposed Mutual Multi-factor Authentication and Key Establishment (MMFA-KE) protocol uses a Time-based Zero-Knowledge Proof of Knowledge (T-ZKPK) [14] scheme combined with authenticated encryption.

In the nodes registration phase, Xyreum relies on Pedersen commitments [32] (it supports homomorphic operations and can provide perfect hiding of real message with the same trapdoor) to assign them digital identities. Also, it authenticates nodes using T-ZKPK and derives shared secret session keys for securing transactions. The T-ZKPK usage mitigates eclipse attacks where proof of work (PoW) and proof of stake (PoS) are vulnerable.

A local blockchain, accessible by all nodes for verification purposes and managed by a master node, is used to record all transactions. Xyreum allows the

use of multiple such local blockchains in a distributed system, each with its own master node. Figure 7 depicts the block and transaction structures in a local blockchain.

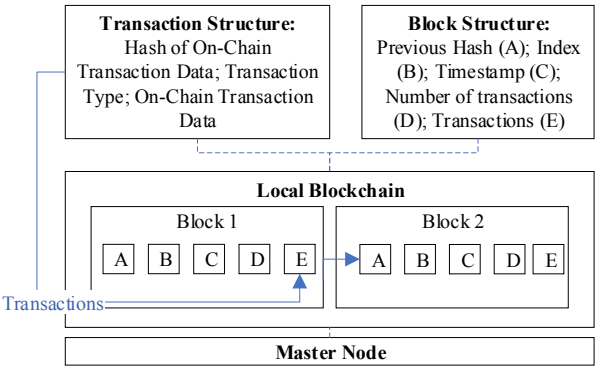

Fig. 7. Xyreum's local blockchain [40].

Furthermore, the authors explain how to use their scheme to strengthen security and privacy of the REMME protocol (`https://remme.io`), a blockchain-based security protocol, which they use as a case study. The experimental results reveal that Xyreum has low computational complexity compared to existing relevant schemes and, in terms of latency, it meets the required IIoT latency target.

4.12 Hy-Bridge

Firoozjaei et al. [15] propose a hybrid blockchain scheme for trustful billing and charging transactions in IoT energy and utility markets. The infrastructure consists of a main blockchain, which is used for billing and charging transactions, and subnetwork blockchains which are used for isolated Peer-to-Peer (P2P) energy transactions between neighbours in microgrids.

The introduced bridge, which links the main blockchain to its subnetworks, isolates users' P2P transactions and provides user anonymity. The bridge performs k-anonymity protection which allows IoT users access shared services anonymously in a credit-sharing group. As such, it helps avoid user profiling and identification by entities of the upper-layer of the smart-grid. An overview of the proposed scheme is depicted in Figure 8.

P2P transactions within credit-sharing groups in microgrids are handled by local blocks which accommodate an additional header, namely credit header, which is used for authorising IoT devices and enforcing the credit-sharing policy. The authors simulated a use case scenario of a smart building to evaluate the performance of their proposed solution. The blockchain used for this purpose is a Python blockchain package, available on GitHub [1].

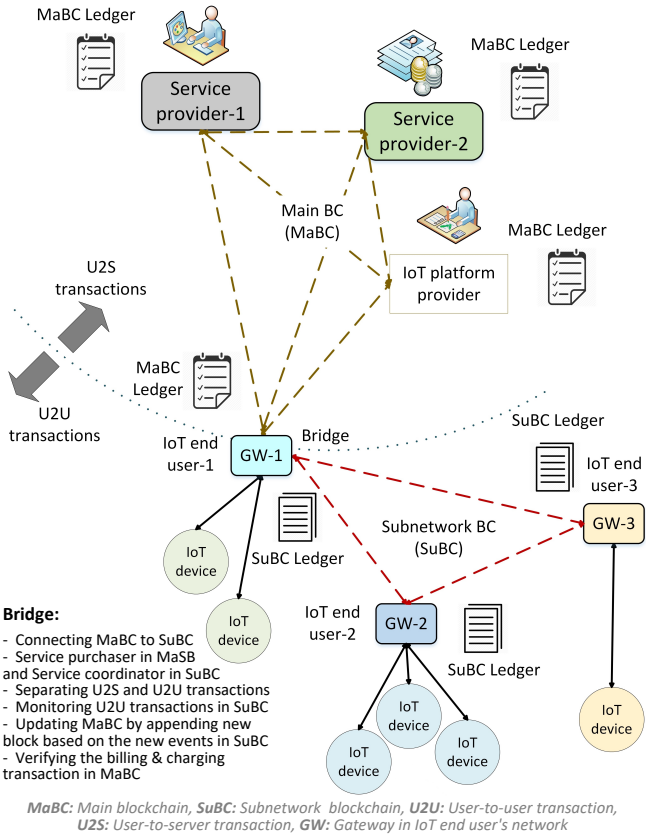

Fig. 8. Hy-Bridge Architecture [15].

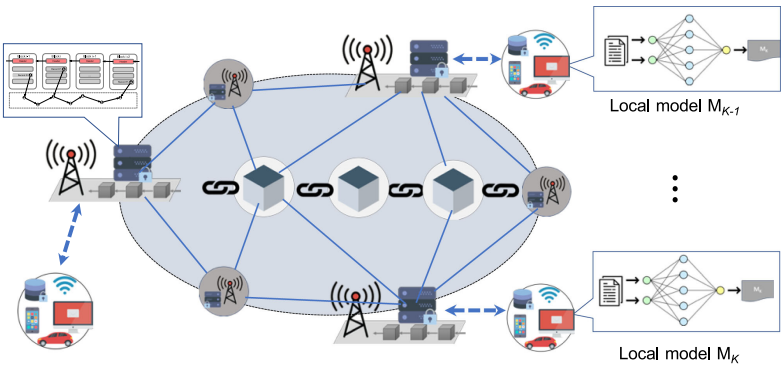

Fig. 9. Architecture of BFL-PPDS [22].

4.13 Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT (BFL-PPDS)

Lu et al. proposed a differentially private multiparty data sharing model for machine learning purposes in IIoT applications, that is based on permissioned blockchain [22]. In their approach, the actual raw data is not directly shared among the parties but used for building data models based on federated learning algorithms.

Additionally, the authors present a blockchain-based architecture that allows collaborative data sharing over the multiple parties located distributively in order to reduce data leakage risks. This decentralised architecture continues to support data owners to keep the control of their data and to provide selectively access to it. An overview of BFL-PPDS architecture is presented in Figure 9.

In order to enrich further the provided privacy, differential privacy methods [11] are integrated into federated learning by adding appropriate noise in the local raw data. Also, the proposed approach is evaluated for its effectiveness in two real-world datasets for data categorisation. The results show that the increase in data providers has little effect on the accuracy, while the running time is obviously increasing. Nevertheless, the authors do not provide experiments with any custom or real blockchain infrastructure.

5 Discussion

In this section, a short discussion is being conducted regarding the aforementioned privacy-preserving blockchain-based solutions in IoT based on their corresponding analysis. There are several issues emerging from our work that can be useful to future research.

As it is presented in Table 1, the majority of the proposed solutions focus on access control as a privacy-preserving provided service utilising public blockchain infrastructures. These solutions include FairAccess [28], BC Gateways [6], PPB-ABE [34], CapChain [20] and PPDAC [27]. PrivySharing [23], on the other hand, provides the same service, based on permissioned blockchain. All of these solutions lack evaluation with the exception of PrivySharing which provides both a security analysis and extended experimental results.

Another group of solutions, are more application oriented, and focus on privacy in energy transactions, like Hy-Bridge [15], which uses algorithmic techniques such us data suppression and generalisation, and PBEM-SGN [16] which uses group signatures. Both solutions provide sufficient experimental results, however, evaluation on a large scale would provide a better feasibility assessment.

Privacy-preserving solutions for machine learning in IoT data is proposed in SecureSVM [44] and BFL-PPDS [22]. SecureSVM [44], utilises homomorphic encryption to achieve user data privacy, a most frequently used method amongst the proposed methodologies. BFL-PPDS [22], introduces a new approach, which utilises federated learning and differential privacy. Both of the proposed services

provide only partial experimental results which need to be expanded to also cover blockchain technology aspects.

Finally, there are other proposed solutions in the literature, which look at the investigated topic, each of them, from a different point of view, such as ADVOCATE [37], which utilises blockchain technology to provide consent management of IoT data, Xyreum [40], which looks at distributed multi-factor authentication in IIoT, and TrustChain [18], which proposes a permissioned blockchain in IoT. Each of these topics needs to be further explored by the research community and requires extended evaluation.

6 Conclusions

In this survey paper, we presented privacy-preserving blockchain-based solutions in the IoT that address personal data protection and preservation of user privacy. In our analysis, we described the identified solutions and we compared them in regards to the focused IoT area, the applied blockchain infrastructure, the provided privacy-preserving service, the utilized underlying privacy mechanisms and the implementation level.

Blockchain technology, as revealed from the results of this paper, is recently adopted as a solution to cover various privacy issues related to the IoT, and so it is not odd that many of the proposed solutions are still in theoretical or early development/experimentation stage, with less than 50% providing implementation details. Thus, it is paramount that in order to provide viable solutions and attain a better grasp to the matter, further research and exploration has to be conducted from the research community.

Acknowledgement

This work was supported by the MPhil program "Advanced Technologies in Informatics and Computers", hosted by the Department of Computer Science, International Hellenic University, Kavala, Greece.

References

1. Alcaide, E.: Pysimplechain. `https://github.com/EricAlcaide/pysimplechain` (accessed on 5 June 2020) (2017)
2. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W., Yellick, J.: Hyperledger Fabric: A distributed operating system for permissioned blockchains. In: 13th European Conference on Computer Systems (EuroSys). ACM, New York, NY, USA (2018). https://doi.org/10.1145/3190508.3190538
3. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy (SP). pp. 321–334. IEEE (2007). https://doi.org/10.1109/SP.2007.11

4. Bitansky, N., Chiesa, A., Ishai, Y., Paneth, O., Ostrovsky, R.: Succinct non-interactive arguments via linear interactive proofs. In: Sahai, A. (ed.) Theory of Cryptography. pp. 315–333. Springer, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36594-2_18
5. Buterin, V.: A next-generation smart contract and decentralized application platform. `https://github.com/ethereum/wiki/wiki/White-Paper` (accessed on 5 June 2020) (2014)
6. Cha, S., Tsai, T., Peng, W., Huang, T., Hsu, T.: Privacy-aware and blockchain connected gateways for users to access legacy IoT devices. In: IEEE 6th Global Conference on Consumer Electronics (GCCE). pp. 1–3. IEEE (2017). https://doi.org/10.1109/GCCE.2017.8229327
7. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016). https://doi.org/10.1109/ACCESS.2016.2566339
8. Demertzis, K., Rantos, K., Drosatos, G.: A dynamic intelligent policies analysis mechanism for personal data processing in the IoT ecosystem. Big Data and Cognitive Computing **4**, 9 (2020). https://doi.org/10.3390/bdcc4020009
9. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized blockchain for IoT. In: IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). pp. 173–178. IEEE (2017)
10. Drosatos, G.: Utilization and protection of personal data in ubiquitous computing environments. Ph.D. thesis, Department of Electrical and Computer Engineering, Democritus University of Thrace, University Campus, Xanthi 67100, Greece (July 2013). https://doi.org/10.12681/eadd/30085
11. Dwork, C.: Differential privacy: A survey of results. In: Agrawal, M., Du, D., Duan, Z., Li, A. (eds.) Theory and Applications of Models of Computation. pp. 1–19. Springer, Berlin, Heidelberg (2008). https://doi.org/10.1007/978-3-540-79228-4_1
12. European Parliament and Council: Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union pp. 1–88 (2016)
13. Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N.: A survey on privacy protection in blockchain system. Journal of Network and Computer Applications **126**, 45 – 58 (2019). https://doi.org/10.1016/j.jnca.2018.10.020
14. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology – CRYPTO '86. pp. 186–194. Springer (1987). https://doi.org/10.1007/3-540-47721-7_12
15. Firoozjaei, M., Ghorbani, A., Kim, H., Song, J.: Hy-Bridge: A hybrid blockchain for privacy-preserving and trustful energy transactions in Internet-of-Things platforms. Sensors **20**(3), 928 (2020). https://doi.org/10.3390/s20030928
16. Gai, K., Wu, Y., Zhu, L., Xu, L., Zhang, Y.: Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet of Things Journal **6**(5), 7992–8004 (2019). https://doi.org/10.1109/JIOT.2019.2904303
17. Huynh, T.T., Nguyen, T.D., Tan, H.: A survey on security and privacy issues of blockchain technology. In: International Conference on System Science and Engineering (ICSSE). pp. 362–367. IEEE (2019). https://doi.org/10.1109/ICSSE.2019.8823094

18. Jayasinghe, U., Lee, G.M., MacDermott, Á., Rhee, W.S.: Trustchain: A privacy preserving blockchain with edge computing. Wireless Communications and Mobile Computing **2019** (2019). https://doi.org/10.1155/2019/2014697
19. Joshi, A.P., Han, M., Wang, Y.: A survey on security and privacy issues of blockchain technology. Mathematical Foundations of Computing **1**, 121–147 (2018). https://doi.org/10.3934/mfc.2018007
20. Le, T., Mutka, M.W.: CapChain: A privacy preserving access control framework based on blockchain for pervasive environments. In: IEEE International Conference on Smart Computing (SMARTCOMP). pp. 57–64 (2018). https://doi.org/10.1109/SMARTCOMP.2018.00074
21. Lee, M.J.W.: Guest editorial: Special section on learning through wearable technologies and the internet of things. IEEE Transactions on Learning Technologies **9**(4), 301–303 (2016). https://doi.org/10.1109/TLT.2016.2629379
22. Lu, Y., Huang, X., Dai, Y., Maharjan, S., Zhang, Y.: Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Transactions on Industrial Informatics **16**(6), 4177–4186 (2020). https://doi.org/10.1109/TII.2019.2942190
23. Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., Ni, W.: PrivyShare: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security **88**, 101653 (2020). https://doi.org/10.1016/j.cose.2019.101653
24. Marchesi, M., Marchesi, L., Tonelli, R.: An agile software engineering method to design blockchain applications. In: 14th Central and Eastern European Software Engineering Conference Russia (CEE-SECR). ACM, New York, NY, USA (2018). https://doi.org/10.1145/3290621.3290627
25. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf` (accessed on 5 June 2020) (2008)
26. Noether, S., Mackenzie, A., Monero Research Lab: Ring confidential transactions. Ledger **1**, 1–18 (2016). https://doi.org/10.5195/ledger.2016.34
27. Ouaddah, A.: A blockchain based access control framework for the security and privacy of IoT with strong anonymity unlinkability and intractability guarantees. In: Kim, S., Deka, G.C., Zhang, P. (eds.) Role of Blockchain Technology in IoT Applications, Advances in Computers, vol. 115, pp. 211 – 258. Elsevier (2019). https://doi.org/10.1016/bs.adcom.2018.11.001
28. Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A.: FairAcces: A new blockchain-based access control framework for the Internet of Things. Security and Communication Networks **9**(18), 5943–5964 (2016). https://doi.org/10.1002/sec.1748
29. Ouaddah, A., Elkalam, A.A., Ouahman, A.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. pp. 523–533. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-46568-5_53
30. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) Advances in Cryptology – EUROCRYPT '99. pp. 223–238. Springer, Berlin, Heidelberg (1999)
31. Panarello, A., Tapas, N., Merlino, G., Longo, F., Puliafito, A.: Blockchain and IoT integration: A systematic survey. Sensors **18**(8), 2575 (2018)
32. Pedersen, T.P.: Non-interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J. (ed.) Advances in Cryptology – CRYPTO '91. pp. 129–140. Springer, Berlin, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-1_9

33. Rahulamathavan, Y., Phan, R.C.., Veluru, S., Cumanan, K., Rajarajan, M.: Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud. IEEE Transactions on Dependable and Secure Computing **11**(5), 467–479 (2014). https://doi.org/10.1109/TDSC.2013.51
34. Rahulamathavan, Y., Phan, R.C., Rajarajan, M., Misra, S., Kondoz, A.: Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In: IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). pp. 1–6. IEEE (Dec 2017). https://doi.org/10.1109/ANTS.2017.8384164
35. Rantos, K., Drosatos, G., Demertzis, K., Ilioudis, C., Papanikolaou, A.: Blockchain-based consents management for personal data processing in the IoT ecosystem. In: 15th International Joint Conference on e-Business and Telecommunications (ICETE) - Volume 2: SECRYPT, pp. 572–577. SCITEPRESS (2018). https://doi.org/10.5220/0006911007380743
36. Rantos, K., Drosatos, G., Demertzis, K., Ilioudis, C., Papanikolaou, A., Kritsas, A.: ADvoCATE: A consent management platform for personal data processing in the iot using blockchain technology. In: Lanet, J.L., Toma, C. (eds.) Innovative Security Solutions for Information Technology and Communications. vol. 11359 LNCS, pp. 300–313. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12942-2_23
37. Rantos, K., Drosatos, G., Kritsas, A., Ilioudis, C., Papanikolaou, A., Filippidis, A.P.: A blockchain-based platform for consent management of personal data processing in the iot ecosystem. Security and Communication Networks **2019**, 1–15 (2019). https://doi.org/10.1155/2019/1431578
38. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks **57**(10), 2266 – 2279 (2013). https://doi.org/10.1016/j.comnet.2012.12.018
39. van Saberhagen, N.: CryptoNote v2.0. `https://cryptonote.org/whitepaper.pdf` (accessed on 5 June 2020) (2013)
40. Sani, A.S., Yuan, D., Bao, W., Yeoh, P.L., Dong, Z.Y., Vucetic, B., Bertino, E.: Xyreum: A high-performance and scalable blockchain for iiot security and privacy. In: IEEE 39th International Conference on Distributed Computing Systems (ICDCS). pp. 1920–1930 (2019). https://doi.org/10.1109/ICDCS.2019.00190
41. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from Bitcoin. In: IEEE Symposium on Security and Privacy. pp. 459–474. IEEE (2014). https://doi.org/10.1109/SP.2014.36
42. Shah, G., Molina, A., Blaze, M.: Keyboards and covert channels. In: 15th USENIX Security Symposium (USENIX-SS) – Volume 15. USENIX Association, USA (2006)
43. Sharma, M., Lim, J.: A survey of methods guaranteeing user privacy based on blockchain in Internet-of-Things. In: 2nd International Conference on Data Science and Information Technology (DSIT). p. 147153. ACM, New York, NY, USA (2019). https://doi.org/10.1145/3352411.3352435
44. Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M.: Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. IEEE Internet of Things Journal **6**(5), 7702–7712 (2019). https://doi.org/10.1109/JIOT.2019.2901840
45. Sousa, J., Bessani, A., Vukolic, M.: A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In: 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). pp. 51–58. IEEE (2018). https://doi.org/10.1109/DSN.2018.00018

46. Wang, W., Vong, C.M., Yang, Y., Wong, P.K.: Encrypted image classification based on multilayer extreme learning machine. Multidimensional Systems and Signal Processing **28**(3), 851–865 (2017). https://doi.org/10.1007/s11045-016-0408-1
47. Yu, Y., Li, Y., Tian, J., Liu, J.: Blockchain-based solutions to security and privacy issues in the Internet of Things. IEEE Wireless Communications **25**(6), 12–18 (2018). https://doi.org/10.1109/MWC.2017.1800116
48. Zhu, H., Liu, X., Lu, R., Li, H.: Efficient and privacy-preserving online medical prediagnosis framework using nonlinear SVM. IEEE Journal of Biomedical and Health Informatics **21**(3), 838–850 (2017). https://doi.org/10.1109/JBHI.2016.2548248