IEEE Open Journal of the Computer Society

Received 12 December 2020; accepted 11 January 2021. Date of publication 20 January 2021;
date of current version 12 February 2021. The review of this article was arranged by Associate Editor Peng Li.

Digital Object Identifier 10.1109/OJCS.2021.3053032

A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture

QUANG NHAT TRAN [1], BENJAMIN P. TURNBULL [1], HAO-TIAN WU [2], A. J. S. DE SILVA [3], KATERINA KORMUSHEVA [3], AND JIANKUN HU [1] (Senior Member, IEEE)

[1]UNSW Canberra, The University of New South Wales, Canberra, ACT 2600, Australia
[2]School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China
[3]Telsoft Limited, Canberra 2586, Australia

CORRESPONDING AUTHOR: JIANKUN HU (e-mail: j.hu@unsw.edu.au)

This work was supported by ARC funds under Grants DP190103660, DP200103207, and LP180100663.

ABSTRACT Blockchain and smart contracts have seen significant application over the last decade, revolutionising many industries, including cryptocurrency, finance and banking, and supply chain management. In many cases, however, the transparency provided potentially comes at the cost of privacy. Blockchain does have potential uses to increase privacy-preservation. This paper outlines the current state of privacy preservation utilising Blockchain and Smart Contracts, as applied to a number of fields and problem domains. It provides a background of blockchain, outlines the challenges in blockchain as they relate to privacy, and then classifies into areas in which this paradigm can be applied to increase or protect privacy. These areas are cryptocurrency, data management and storage, e-voting, the Internet of Things, and smart agriculture. This work then proposes PPSAF, a new privacy-preserving framework designed explicitly for the issues that are present in smart agriculture. Finally, this work outlines future directions of research in areas combining future technologies, privacy-preservation and blockchain.

INDEX TERMS Biometrics, blockchain, consensus protocol, internet of things, privacy, privacy-preservation, smart agriculture, smart energy.

I. INTRODUCTION

Far from its origins in cryptocurrency, blockchain has shown its applicability in various fields, including supply chain management [1]–[6], biomedical healthcare [7]–[10], cloud computing [11], [12], identity management [13], [14], marketing [15]–[17], and even tourism [18]. An interesting different field of application is in marketing, where the authors of [19], illustrate how blockchain technology can act to empower the consumer-centric paradigm. By fostering disintermediation, blockchain can act as the mechanism to create traceability and transparency. This also links to the latest evidence questioning the effectiveness of advertising, and in particular digital advertising [19], [20]. Repeated studies have shown TV ads [21] and search words digital advertising [20] to be not as effective as suggested by the advertisement empires that run them. The future of linking producers and consumers through a transformative new platform like blockchain, which enables enhanced information, and guarantees the quality of information, without the endogeneity effect of advertising, enables a very different role for marketing. However, the nature of blockchain does not immediately consider user or data privacy, and the paradigm structure poses a challenge for these. Sensitive information leakage may have significant impacts on the use-case of the system; this may include information leakage, data exposure or the exposure of party identities. For instance, a blockchain-enabled vehicle infrastructure platform would, by its very nature, expose locations, transactions and other Personally Identifiable Information (PII), for which there are potentially serious impacts. However, there has been research in the intersection of blockchain and multiple forms of privacy preservation; both general, and applied to specific areas. Hence, there is a necessity to collate, review and

categorize these published works on privacy preservation as applied to different Blockchain applications.

In this survey, we first outline the general structure of a Blockchain and some of its current privacy issues in Section II. Afterward, Section III of this work categorizes the studies that have been proposed in privacy-preserving blockchain, and reviews the key advances. Based on the outcomes, a categorization on the privacy preservation in Blockchain is established and summarized. Then, a novel PPBS-based framework is proposed for smart framing. Finally, Section VI provides a summary of predictions on the future trends of privacy preservation as applied to Blockchain technologies.

II. BLOCKCHAIN TECHNOLOGY

Blockchain was first proposed by Chaum [22] in 1979. In 1992, Bayer *et al.* [23] improved this concept by incorporating Merkle trees as part of the block design. The structure is an ever expanding list of blocks that are cryptographically connected: each block contains the previous block's cryptographic hash, a timestamp, and the main data, which is also referred to by transaction data. Owing to this design, blockchain is strongly resistant against data modification. Year of 2008 marked the day when blockchain commenced its technology widespreading by being conceptualized in Nakamoto's studies. In all of its applications, the purpose of blockchain is to deliver data to parties with integrity.

A. HOW BLOCKCHAIN WORKS

Blockchain is an immutable database in which only new records (or blocks) can be appended. A peer-to-peer network manages the communication for the chain of blocks, allowing applications to access the data contained in each block by broadcasting the whole structure to all the nodes based on a consensus algorithm. As such, a blockchain does not require a central server, making decentralization one of its advantages for deployment. In order to add a new block to the chain, a consensus algorithm is used such that all nodes in the network (for a public blockchain) or the managing entities (for a consortium/private blockchain) must validate the transactions before creating the block. This prevents the issue of double-spending, which is the risk that a unit of digital currency is spent twice due to digital information replication.

There are two most famous consensus algorithms used in blockchain: Proof of Work (PoW) and Proof of Stake (PoS). Conceptually, the miners compete against one another to look for the solution of a mathematically complicated problem. In PoW, the miners use their own computational power to calculate the hash value of the blockchain data and a variable data (called nonce in Bitcoin). This hash value must satisfy certain conditions given by the protocol. As a miner finds the valid hash, he/she gets rewarded with cryptocurrency for the computational power spent. Due to low efficiency of computational power, PoS was proposed. In PoS, there is no mining, thus, no miners. Users in the system are chosen based on some factors. One of these is called "stake," which is the predetermined amount of cryptocurrency to be locked up. When chosen, the user is required to propose a block, which is validated by the *validators*. If this block is valid, they receive a reward. If the user is found dishonest, the stake is taken. The system works as, given an input, any node in the network can verify the validity of the block to update the blockchain.

On the other hand, the ledger is used for the main purpose of blockchain: deliver data between parties. Each party's address is a unique pseudonym in the network, generated by the PKI, ensuring the identity of the involved parties. When a communication happens, a transaction is created to record the addresses, the signatures of the parties, and the data. A block is generated, carrying the hash value of the previous block and a timestamp, to store transaction data in a Merkle tree. Note that the first block in the chain does not have previous block. Due to this structure, blockchain data is robust against tampering attacks.

The term 'Smart contract' is a multi-definition term that is dependent on how it is used and implemented in each framework. Generally, a smart contract provides mechanisms for documenting and executing contracts without the need for a human trusted intermediary. There are several well-known smart contract platforms, including Ethereum, Hyperledger Fabric, Nem, and Stellar, all of which are based on, but extend, the Blockchain paradigm.

There are three distinct forms of blockchain, to account for different use-cases. These are:

- Public: A public blockchain grants access to all participants as they can read the data from it or even create a new transaction to attach to it. Hence, this type of blockchain is accessible even to an adversary. Public blockchains are the most common and include cryptocurrencies, particularly Bitcoin, Dogecoin as well as smart contract platforms such as Ethereum.
- Consortium: A consortium (or semi-private) blockchain grants a number of parties the right to confirm blocks. In a consortium blockchain, the consensus algorithm is operated by a number of nodes in the network. Participants may still read the data, but not the general public. Consortium blockchains are used for cases when there are several related, but not mutually trusted, entities that are working together or require data sharing.
- Private: A private blockchain retains the write privilege to an entity or organization while the read permission might be open to public or to certain parties. Private blockchains are often applied in government or banking disciplines where access control must be monitored, but where other data storage processes are less optimal.

Each of these forms of blockchain has its own advantages or disadvantages. While public blockchains are entirely decentralized, the information contained is exposed to adversaries. Consortium blockchains are effective when data sharing is needed. However, its security depends on the architecture and security techniques outside of the paradigm. Last but not least, private blockchains remove the decentralization characteristics. As a result, a casual centralized data storage and

TABLE 1. Privacy Categorization

	Biometric Privacy	Identity Privacy		Data Privacy
		Personal	Object	
Biometric Template Protection with Blockchain	[35], [37], [38]			[36], [37]
E-Voting	[88]–[92]	[88]–[93]		[88]–[94]
Health Records Management	[28], [29]	[24]–[34]	[30]	[24]–[33]
Smart Energy (IoT)		[56], [57], [59], [61], [62]	[57], [58], [60]–[63]	[56]–[63]
Smart Transportation		[68], [70], [73]–[76]	[64]–[67], [71], [72], [76]	[65], [66], [69]–[73], [75], [76]
Smart Agriculture			[4], [77]–[79]	[4], [77]–[79]
Others		[80], [83], [84], [87]	[83], [86]	[33], [80], [82]–[87]

processing systems tend to have more benefits over the use of a private blockchain. There are some advantages to private blockchain implementations; for example, private blockchains have the benefit of transaction transparency, for example, which can provide numerous benefits for specific use-cases.

B. CURRENT PRIVACY CHALLENGES IN CURRENT BLOCKCHAIN IMPLEMENTATIONS

One of the chief advantages of blockchain is its decentralized nature. However, the fully decentralized nature of blockchain means that all data is available to all nodes; on a public blockchain, this means its available to the public, and on a consortium blockchain, all participants. This has the potential to expose sensitive information of the parties involved, depending on the data within each block. Access control methods may be imposed to ensure that only authorized personnel have access to the data, but these methods usually require the storage of passwords or biometric template, or possession of token, which is contrary to the decentralized environment and making the traditional PKI unsuitable. If a user loses his/her private key, the privacy is exposed to dangerous threat. Such mechanisms are often outside the paradigm, and are therefore also less effective.

Blockchain is utilized differently based on the application. Moreover, the difference in the data used in each application differentiates the types of privacy. Hence, the privacy-preserving techniques are not the same across various applications. There are some generic concepts that are application-agnostic, but many advances are either specific to a field, or have not been considered for application in other problem domains. In this article, we will look at the privacy-preserving techniques that have been devised in each field that applies blockchain technology.

III. APPLICATIONS OF BLOCKCHAIN

This section reviews the blockchain's implementations towards different problem domains. In this survey, we categorize the applications into the following types of blockchain application area:

- Cryptocurrency
- Data Management and Storage
- E-voting
- IoT and Internet of Everything Ecosystems

The need for, and types of privacy, vary per application. Based on its nature, the privacy is classified into: Biometric Privacy, Identity Privacy (consisting of Personal and Object Privacy), and Data Privacy. The relation between the types of application and privacy is presented in Table 1.

A. CRYPTOCURRENCY

The famous cryptocurrency Bitcoin is one of the first implementations of blockchain technology. It was proposed by a pseudonymous person (or group of people) named Satoshi Nakamoto. Bitcoin uses a public blockchain,for which transactions are available to all the nodes in the peer-to-peer network. The transactions are created and written to a block. The new blocks are added to the blockchain based on the PoW consensus algorithm. Miners receive a portion of Bitcoin based on the amount of computation they spend to solve the hashing problem. Overall, the average time to create a new block is approximately 10 minutes. This amount of time makes the possibility of a Distributed Denial of Service (DDoS) attack almost infeasible.

As Bitcoin's blockchain is public, all information may be exposed to the adversaries. The security of Bitcoin depends on the public-private key pair. Each address in a transaction is associated with the public key. When a transaction is created, the private key is used to sign without being disclosed to the public. The corresponding public key that is used to verify the authority of this transaction. It is impossible to derive either the public key from the transaction's address or the private key from the public key. This is a privacy issue for Bitcoin as in theory, without the private key to sign, Bitcoin cannot be sent with any transaction. However, if a user loses his/her private key to an adversary, the privacy of the user cannot be maintained. Bitcoin is also exposed to the 51-percent attack in which the adversaries control a large amount of nodes in the network. As a result, they take full control of the mining, which prevents other users from mining properly. On the other hand, with less than 51 percent of the whole network's mining capacity, the successful probability is much lower.

B. DATA MANAGEMENT AND STORAGE

One of the key drivers for Blockchain has been as a data storage mechanism, allowing for platform-wide auditing and verification of data. This has several advantages: it provides

transparency for all participants; it makes data sharing more convenient whilst being simple to audit; it provides security defense techniques against the attack on centralized database. Thus, in this section, we look at how blockchain has been applied to Health Records Management and Biometric Template Protection.

1) HEALTH RECORDS MANAGEMENT

Electronic Health Records (EHR) storage is widely deployed in many countries to provide the convenient sharing of individuals medical history. There are several advantages to this; greater accountability, decreased administration burden, and increased care, especially in the event of an accident or emergency situation. Due to its nature, blockchain and smart contracts [24] have been leveraged to accomplish this task. However, it also raises the issues about the sensitive health information of a patient's being exposed to non-authorized personnel. This information could include (but is not limited to): medical history, treatments, location, and so on. Therefore, privacy-preserving techniques must be incorporated to protect the patient's data.

Omar *et al.* [25] proposed MediBchain, a blockchain-based electronic health record sharing framework in which the patient's health data is encrypted and stored in a blockchain. Sharing the data is dependent on the patient; only those who are authorized by the patients can receive and decrypt data. Dagher *et al.* [24] proposed Ancile, an Ethereum-based framework to control the access to electronic health records with cryptographic techniques for security using smart contracts. Liu *et al.* [26] proposed BPDS, a blockchain-based privacy-preserving data sharing in which the original electronic medical records are stored in the cloud while the indices are stored in a consortium blockchain, resulting in not only the mitigation of data leakage but also the prevention of arbitrary data modification. On the other hand, Xu *et al.* [27] devised Healthchain, a blockchain-based storage that is capable of preserving the privacy of users by allowing them to add or revoke authorized doctors. Mohsin *et al.* [28] devised a finger vein verification framework that incorporates blockchain, encryption, and steganography to protect a patient's medical information. This is unique in the sense that it integrates the use of steganography with other different security mechanisms in blockchain. Baqari and Barka [29] secured Electronic Health Records by incorporating biometric-based blockchain in which biometric is used to ensure not only the identity of a patient but also the recoverability of their access to the EHR system.

Similarly, Shen *et al.* [30] proposed a blockchain-based model to retrieve medical images while still preserving the privacy of the patients. This model extracts feature vectors from each medical images are extracted to enable the customization of the transaction design. Although this use-case is niche, it highlights the balance between privacy-preservation and utility in areas of e-health.

Ji *et al.* [31] sought to address the issue of location sharing in mobile medical services. They did so by proposing a blockchain-based multi-level privacy-preserving location sharing scheme. This scheme used Merkle trees with order-preservation to achieve this. Evaluation on the computation overhead of the scheme shows its feasibility, although it is yet to be implemented.

Claiming that privacy issues in remote patient monitoring might endanger a patient's life, Dwivedi *et al.* [32] proposed to protect the users' privacy in the blockchain network using a privacy-preserving ring signature scheme in addition to the double encryption of both data and the symmetric key. The authors also stressed that this scheme is more appropriate to wearable IoT devices as it does not require heavy computational capability.

Zhang and Lin [33] aimed to improve diagnosis in e-Health system by using two kinds of blockchain: A private blockchain to store the Personal Health Information (PHI) and a consortium blockchain to store PHI's indices. In this scheme, privacy-preservation is obtained by encrypting all the PHI data before storing in the private blockchain. Kuo and Machado proposed to solve the problem of privacy-preserving machine learning in healthcare with ModelChain, a framework that incorporates private Blockchain network which contributes model parameter data without revealing the patients' information [34].

2) BIOMETRIC TEMPLATE PROTECTION WITH BLOCKCHAIN TECHNOLOGY

A biometric template contains the biometric data recorded from the enrollment process. This type of data is used to be matched against newly retrieved biometric data to give a "match" or "non-match" decision. Biometric template protection was devised such that if a protected template is compromised, it can be revoked and a new template can be established. This means that the raw biometric data is safe. A noted current challenge in the biometric community is the security of biometric templates. Traditionally, biometric template data is stored in a centralized database. However, if the database is compromised, this template is lost to the hands of adversary, who can use it to cross-authenticate other applications that use the same biometric. More importantly, biometric data (especially physiological type) is very limited and not as revocable as a password would be. If a user loses his fingerprint to an attacker, he or she might never be able to use it in future applications. Hence, it is necessary to devise protection techniques for the biometric template. There have been various methods to achieve this goal. The most famous of these are cancelable templates and biometric cryptosystems. With its properties of cryptographic security, decentralized nature, and unalterable data transaction, blockchain has shown the potential to be the next biometric template protection method.

Goel *et al.* [35] presented a biometric recognition architecture that incorporated a private blockchain to extract

features. Matching is performed in a decentralized manner. The author showed that this architecture is able to reinforce the security of CNN-based model and biometric template by implementing with different biometrics. The authors proposed DeepRing [36] to protect CNN architecture from external adversaries using cryptography and blockchain technology. In addition, a tampering attack model is proposed to stress the role that blockchain technology can play in the world of machine learning. This work enables blockchain to protect CNN models, including those that are used for biometric authentication. Othman and Callahan [37] proposed Horcrux, a protocol that stores biometric credential in a decentralized manner via blockchain using decentralized identifiers and documents (DIDs) developed by W3C Verifiable Claims.

Recently, Accquah *et al.* [38] proposed a method that protects the fingerprint templates with blockchain technology in which fingerprint features are extracted, encrypted with AES, and finally uploaded to a symmetrically distributed storage system called InterPlanetary File System (IPFS) [39] after being split. The hash of the templates, separately to these, is stored on the Ethereum network. However, this work has three disadvantages that remain unaddressed; (1) biometrics are known for their uncertainty, which is why they are incompatible with conventional cryptography techniques. Despite this, the authors did not explain how they applied AES with fingerprints; (2) the process of matching has not been discussed; and (3) although the cost and efficiency of storage have been shown, the performance of the biometric authentication system has not been mentioned. This is an important characteristic of a biometric authentication system.

C. E-VOTING

Voting has played an important role in the development of civilization as it allows the people of a country or territory to choose their leaders. Voting is considered a cornerstone of democracy. There have been significant achievements on applying technology to voting, which if often referred to as Electronic voting or E-voting. There are numerous benefits to e-voting; including precision, speed in counting, and logistic considerations [40], [41]. E-voting even is even more promising when enabled by blockchain technology. The concept is simple: Each voter has a electronic currency wallet. When the voters vote for a candidate (or a number of candidates in some countries or regions), the electronic currency is transferred to the candidate(s)' wallet [42]. However, due to the privacy threats, e-voting has not been widely implemented. The potential disadvantages have been in the security of e-voting, and ensuring privacy. Hence, there exists urgent necessity to devise privacy-preserving e-voting systems to ensure the integrity of the voting process, whilst simultaneously ensuring voter privacy. In e-voting, privacy refers to the identity of the voters, the content of the vote, and their linkage, meaning that given a voter and a vote, one can not refer to one from another. In addition, the security of the vote must be ensured as its content cannot be tampered. The inherent privacy issues from blockchain hinder the public adoption of blockchain e-voting as public trust is necessary while in reality, this is rarely achievable. In addition, blockchain's complexity might also be an obstacle when implementing e-voting for a region with great population.

Ayed [43] introduced a secure blockchain-based e-voting system that achieves transparency by using open-source code. This system does not allow a registration process, which makes it dependent on a separate database. Liu *et al.* [41] proposed an e-voting protocol that integrates blockchain without a trusted third party. Using blind signature [44], the authors claimed that this protocol is transparent to public and importantly, maintains the anonymity of the voters as well as the privacy of the votes. Hjalmarsson *et al.* [45], in an on-going work, evaluated the use of blockhain as a service for an e-voting system. In details, the authors proposed a permissioned blockchain that utilizes smart contracts to ensure the privacy of the voters. However, the bridging problem has not been discussed in those works.

D. IOT AND INTERNET OF EVERYTHING ECOSYSTEMS

Internet of Things, commonly known as IoT, has attracted more and more interest in research due to its potentially wide range of applications, and the promises it makes in increasing flexibility, energy efficiency, and ease-of-use that such strong integration can provide *Things*. With the escalating development of blockchain technology, this future is closer than ever. However, given the need for cloud integration, data collection and remote analysis, the privacy of IoT users is potentially at stake. The definition of IoT has expanded over time, not only incorporating user and home devices, but industrial systems. This is often termed the Industrial Internet of Things (IIoT), or the Internet of Everything (IoE). This section is dedicated to review the efforts in research to protect users' privacy in the IoT, IIoT and IoE environments.

1) SECURITY ENHANCEMENT TECHNIQUES

The security of IoT has been a consideration since its inception. The combination of low-cost, low-powered systems, difficulties in upgrades and fixes, and wireless networking, has seen significant work outlining the potential security dangers of IoT. Blockchain has been utilized to construct cryptographic protocols or in order to enhance the security in IoT environments and ecosystems.

In 2016, Kosba *et al.* [46] introduced Hawk, an Application Programming Interface (API) to help programmers write privacy-preserving smart contracts code without the requiring them to implement their own cryptography, lowering the complexity of implementing such systems. In 2017, Ouaddah *et al.* [47] introduced a blockchain-based framework that is capable of integrating privacy preservation into authorization management of access control. This API and framework have enabled and expanded the use of blockchain to allow more applications to use blockchain technology without being concerned about privacy leakage. In the same year, Kaaniche and Laurent [48] presented a cryptographic technique using

blockchain technology to enable availability and accountability, whilst preserving privacy-preservation, in a a data usage auditing architecture. Recently, Shao *et al.* [49] achieved unlinkability and anonymity for transactions of a legitimate user in a blockchain whereas malicious users can be identified in a framework called AttriChain. Recently, Halpin introduced Nym credentials as a novel method to deploy anonymous authentication credentials to preserve user privacy in a blockchain environment [50].

Jiang *et al.* [51], [52] introduced Privacy-preserving Thin-client Authentication Scheme (PTAS) to improve the security for the users with limited storage IoT device by using Private Information Retrieval (PIR). In addition, thin-client data is protected against at most $(m-1)$ full node users' collusion with the $(m-1)$ private PTAS. Evaluation on the computational and communication overhead of these two methods are provided to show their potential. Recently, Patil *et al.* [53] proposed a blockchain-based protocol that utilizes the Physically Unclonable Function (PUF) model to achieve better authentication process whilst still preserving user privacy. In [54], Jones *et al.* compared the use of trusted third parties, cryptographic techniques, and blockchain smart contracts and concluded that each alone does not ensure privacy preservation. They implemented a hybrid approach combining the aforementioned techniques to share geolocation data securely in a trusted execution environment. With a similar aim of targeting the privacy when using location-based services, Qiu *et al.* [55] a location privacy preserving approach that leverages multiple private blockchains to protect the users' privacy without degrading the service's quality. This is still a proof-of-concept, but offers a unique service if expanded.

2) SMART ENERGY

Smart grids are an increasingly important form of Cyber-Physical System (CPS) infrastructure, providing power for future IoT environments. In a smart grid, a smart meter is installed at each household to collect consumption data. This data enables adaptive and efficient power generation and scheduling. Smart grids require the processing of smart meter data to operate effectively. As a result, this data had the potential to expose information that is potentially sensitive, including energy use patterns, and billing information. This has significant second-order effects, as this data can be used to infer movement patterns and other private information. Failure to protect smart grid data may lead to disastrous consequences in real life.

There is emerging research that has sought to develop processes in smart energy for privacy preservation. Guan *et al.* [56] presented a method to protect smart grid user data by separating the users into different groups, each of which with a private blockchain for data recording. The user data was held in a group protected from others in the same group through the creation and use of pseudonyms associating to each individual. Seeking to address the problem of uncoordinated charging of Energy Storage Units (ESUs), Baza *et al.* [57] constructed a decentralized charging coordination mechanism to which ESUs can perform anonymous authentication. In [58], Tan *et al.* addressed the problem of the privacy and security of the consumption and trading data using a blockchain-based energy scheduling model whose optimization is separated into trivial scheduling problems, which are then solved by consensus algorithm and smart contracts. Gai *et al.* [59] aimed to protect the privacy of the users in a smart grid by incorporating a permissioned blockchain with smart contracts and edge computing in which group signatures and covert channel authorization techniques are utilized. Keshk *et al.* [60] devised a framework to provide data privacy and security in smart power networks with two modules; The first being a two-level module that is dedicated to verify data integrity using proof of work blockchain along with applying a variational autoencoder to transform data, and the second being an anomaly detection module for training and validating the output of the first module. This second module uses deep learning techniques. Experiments show its competitiveness against state-of-the-art techniques in protecting data and identify anomalies. Recently, Hy-Bridge [61] has been proposed to not only help users secure their data against the service providers but also share credits with other users with the use of blockchain.

An electrical vehicle's information may also be linked to its owner, which reveals the privacy of an identity. Exposing this kind of information may lead to PII being leaked, including physical locations, times of movement, and information extrapolated from these. Aiming to protect users privacy whilst charging Electrical Vehicles (EV) in a Vehicle-to-grid (V2G) environment, Gao *et al.* [62] proposed a blockchain-based payment method that is capable of sharing users' data without revealing the privacy by enabling registration with digital signatures of a user and allowing auditing of payments by privileged users. On the other hand, Gabay *et al.* [63] introduced two approaches (token-based and Pederson Commitment Scheme-based) that incorporate zero knowledge proofs with blockchain and smart contracts to protect the privacy of the charging EV when authenticating for charging.

3) SMART TRANSPORTATION

Smart transportation is one of the key emerging use-cases for IoT systems and infrastructure. The rise of smart vehicles and vehicular networks can apply some of the promises of IoT; increased safety, improved communications to assist networks overall, and to provide timely updates to incidents such as accidents or road conditions. However, such data also creates potential privacy risks, as it includes vehicle identity information, residual locations, vehicle movements, and messages transmitted across networks. A number of studies have been dedicated to apply blockchain and privacy preservation in Vehicular Ad-hoc Networks (VANETs). Sharma and Chakraborty [64] devised BlockAPP as a method to authenticate vehicles with their privacy being preserved in the Internet of Vehicles (IoV). Lu *et al.* [65] proposed a

privacy-trust model for VANETs in which blockchain technology is employed to store the certificate and revocation transparency. In 2019, the authors proposed a privacy-preserving authentication scheme in an extended blockchain environment for VANETs [66]. Guehguih and Lu [67] proposed a dual blockchains as a solution for privacy-preserving authentication in VANETs in which the private blockchain is used for authentication while the public is utilized as event messages manager. Li *et al.* [68] solved the problem of carpooling users' information being disclosed in fog computing by incorporating blockchain-assisted vehicular fog computing that is capable of preserving the users' private information. Feng *et al.* [69] implemented a blockchain-assisted privacy-preserving authentication system (BPAS) in VANETs to verify the messages being transmitted in the network. Security analysis shows that this framework is able to achieve conditional privacy preservation.

To solve the problem of user anonymization and lack of motivation to forward announcements in Vehicular Social Networks (VSNs), Li *et al.* [70] proposed CreditCoin, a privacy-preserving blockchain-based announcement network with incentives, where announcements can be sent via an anonymous vehicular announcement aggregation protocol. Despite the anonymous nature, the identity of malicious users can be tracked with the system. Pu *et al.* proposed a privacy-preserving scheme that is capable of concealing a vehicle's identity in a VSN [71]. To prevent tampering, the data of the VSN is stored in a blockchain and Practical Byzantine Fault Tolerance (PBFT) is employed for the purpose of consensus. In [72], the authors proposed to combine a consortium blockchain with a privacy-preserving location-based service to address the issue of man-in-the-middle-attack and the requirement of certificate authority in communicating with limited-resources smart vehicles in a VSN. A lightweight certificate authority is devised in addition to the use of the privacy-preserving location-based service protocol, PPVC. The experimental evaluation and security analysis show the efficiency of this method in a VSN environment.

Smart transport has aspects far beyond the individual vehicle networks, and there are several other aspects of the field that have benefited from blockchain technology in a privacy-preserving manner to provide convenience and security.

Hu *et al.* [73] proposed a smart parking framework to protect the privacy of users. It did this with a blockchain to remove the need for a trusted third party. Similarly, Amiri *et al.* [74] applied a blockchain with PIR to construct a smart parking system that does not disclose drivers' sensitive information.

Interested in ridesharing, Baza *et al.* [75] claimed that a myriad of problems caused by the traditional central third-party ridesharing methods, including privacy concerns, could be resolved using their proposed public Blockchain in which drivers are allowed to offer ridesharing services without having to rely on a central provider. On the client's side, sensitive information such as locations, date, and time are preserved by sending cloaked requests, to which the drivers respond with encrypted offers. The smart contract platform Ethereum was used to implement this method, which showed feasibility in practice. Also working in privacy-enabled ridesharing, Li *et al.* [76] sought to address the problem of cross-organizational data sharing between ridesharing service providers. They did this by devising CoRide, a privacy-preserving hailing service using blockchain-assisted fog computing; a consortium blockchain to record the rides are constructed and smart contracts are utilized to pair riders with drivers. An Ethereum network was also used to implement this system. However, in this work, the assumption is that all users adopt the same data formats for matching and payment. This is rarely the practice in reality, as rideshare platforms have their own technology stacks and formats.

4) SMART AGRICULTURE

Agriculture has played a crucial role in the development of any civilization. With the development of new technologies, agriculture has promising ways to increase yields, quality and product shelf life. There are also changes in pressure from consumers, who increasingly want to know more about their food, including the origins of ingredients, details of the processes different foodstuffs have gone through over its development, and the chemicals and preservatives it has been exposed to. Smart Agriculture has been leveraged to achieve these goals as it integrates traditional agriculture with advanced technologies such as IoT. One of the recent trends for smart agriculture is the use of blockchain to ensure the transparency of food data. This needs to be balanced with the obvious commercial privacy requirements, as much of the information that can be collected with IoT devices is unique to each producer. Measurements such as soil moisture, temperatures and fertilisers used are commercially sensitive. Affording relevant information to consumers and buyers without leaking sensitive proprietary data is a unique challenge.

In 2018, Kim *et al.* [77] introduced Harvest Network, a farm-to-fork food traceability application that leverages smart contracts and GS1 message exchanging standards for IoT devices. However, this framework was only theoretical as there was no prototype to evaluate the effectiveness at the time. Caro *et al.* [4] devised AgriBlockIoT, a food traceability solution that is based on fully centralized blockchain. In details, the authors achieved traceability by deploying two blockchains on Ethereum and Hyperledger Sawtooth, respectively. Performance of the system on latency, CPU, network usage have been provided for a comparison of pros and cons. Lin *et al.* [78] devised a tamper-proof food traceability system based on blockchain to monitor the food's lifespan in smart agriculture. This system integrates trustworthy verification for blockchain and is able to work with low-power wide-area network (LPWAN) IoT system. However, no implementation and experiment results have been discussed. Salah *et al.* [79] proposed a smart contract-based approach to perform business transactions and traceability for soy bean in the agriculture supply chain. All transactions from every party involved in

the process are recorded in the blockchain with links to an IPFS [39].

E. OTHER FIELDS

The applicability of blockchain technology is still growing as it has been utilized in an increasing number of fields, including access control, cross-domain data sharing, and data integrity in IoT environments. Due to the huge amount of data to be used with blockchain, it is critical to use privacy-preserving aspects to ensure the security. Makhdoom *et al.* [80] proposed a method to share multiple types of data in a smart city environment based on blockchain technology using multichannel approach with the capability to protect users' privacy. Zhao *et al.* [81] presented a privacy-preserving software update protocol using blockchain technology with incentive. Zhao *et al.* [82] addressed the problem of remote data integrity checking for IoT Systems with a privacy-preserving blockchain scheme. Le and Mutka [83] introduced CapChain, a blockchain-based access control framework for users to share their access rights to IoT devices in public with privacy preservation. Lu *et al.* [84] applied blockchain to the problem of authentication in cross-organizational data sharing without the existence of a trusted third party. Targeting the users' privacy in recommendation systems, Casino and Patsakis [85] devised a Collaborative Filtering system based on blockchain to construct a decentralized architecture that is based on locality sensitive hashing classification.

In [86], the authors discussed three location-related vulnerabilities in the traditional crowdsensing system. They proposed a privacy-preserving crowdsensing system based on blockchain technology with incentive to address these issues as well as motivate the workers to complete the task. Chen *et al.* [87] described DEPLEST as a portable-device-compatible method to protect the social network users' privacy in which a modified blockchain model to secure their private information and passes non-private information for processing. In addition, a consensus protocol for blockchain ledger maintenance that is Byzantine-Fault Tolerant (BTF) is also proposed with experimental results to show its feasibility when compared with the PoW and PoS methods.

IV. PPSAF, A NOVEL FRAMEWORK FOR PRIVACY PRESERVATION IN SMART AGRICULTURE

Although there are many successful applications of PPBS (such as PPBS-based transportation systems and PPBS based e-health systems, for example), its application to smart farming is largely an unexplored territory. It is estimated that we need to produce 70% more food in 2025 than it did in 2006 in order to feed the growing population [95]. Therefore, smart farming has been heralded as the future of agriculture.

Data infrastructure is a foundational technology for smart farming and agriculture, whereby data is used to optimize farming efficiency and quality. Security and privacy issues can hinder its large-scale deployment. Recently, Huning *et al.* [96] have proposed a privacy-preserving mobile crowdsensing architecture for a smart framing application. In this architecture, a perturbation-based privacy mechanism is developed in conjunction with a trusted third party to ensure user privacy in the mobile crowdsensing environment. In general, no adequate and dedicated security/privacy data security infrastructure for smart farming. We observe that PPBS is an ideal security technology platform for smart farming as smart farming would need to securely store large amount of timestamped data which could be accessed by third parties. Also, the smart contract technology can help remove the cost of middleman in finding individual goods suppliers to collectively fulfil a big product order placed by a retailer. Therefore, we propose the Privacy Preserving Smart Agriculture Framework (PPSAF), a PPBS-based secure data framework for the smart farming. The proposed framework is shown in Fig. 1.

The PPSAF framework is comprised of the following components; field sensor networks, an aggregator, gateways, and a consortium blockchain. As outlined in Fig. 1, the system operates as follows: field sensor networks continuous collect data from crop fields, and the aggregator sends collected sensor network to the gateway of the farmer. The farmer stores the data to its own private ledger (private channel) in the cloud. This data may include crop information, site information, fertilizer distribution, soil readings, and other relevant information. Farmers, banks, logistics and retailer form a consortium blockchain built on a Hyperledger Fabric Platform. Data, including business transactions are encrypted, which can be accessed and verified among the consortium members, once authorized. Major players such as banks and retailers form the initial system and other potential participants must register first, subject to the approval from super nodes. The proposed framework provides two major applications for smart farming: (1) Secure Data Infrastructure for Data Storage and Access, and (2) Smart Contract for Business Bidding. Each of these is discussed separately.

A. SECURE DATA INFRASTRUCTURE FOR DATA STORAGE AND ACCESS

The power of smart farming lies in the smart use of data for accurate farming. However, data such as fertilizer density in the field, field temperate and moisture, are commercially sensitive data and therefore must be protected. The data could also be used by the trusted third party in providing big data analysis service. The PPSAF framework provides the following solution: In the local sensor network, field data (up to the aggregator) are encrypted with a lightweight cryptography mechanism. The data will then be forwarded to the farmer's gateway which is installed in the farm. Upon receiving the encrypted data forwarded by the aggregator, the gateway decrypts the data, compresses them into corresponding time-interval (e.g., hourly) blocks. The farmer encrypts this block of data with a stronger cryptographic scheme, signs the encrypted data block which will be placed in the farmer's private blockchain in the cloud. A signed transaction notice will be broadcast in the consortium blockchain. This transaction notice will contain

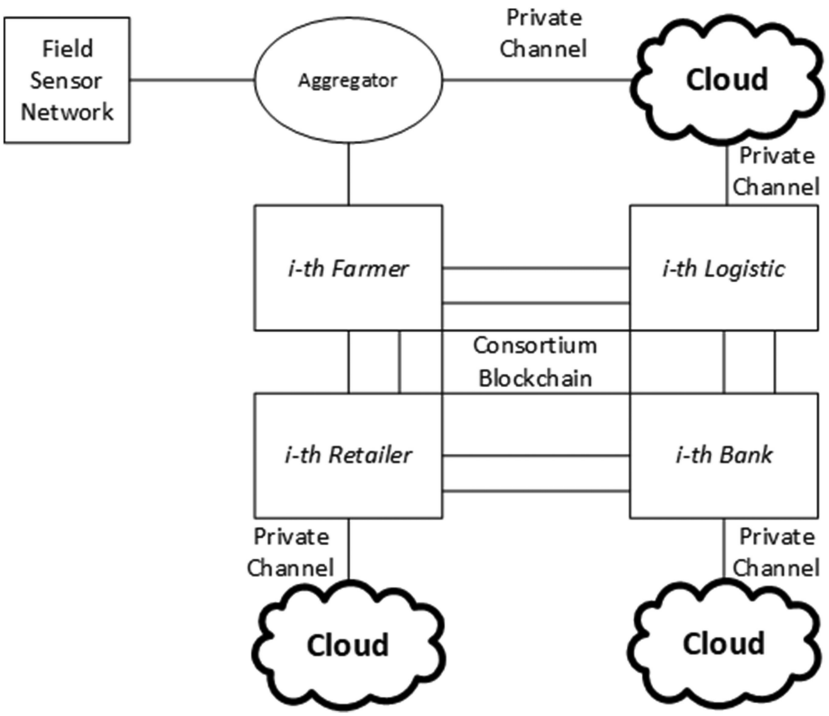

FIGURE 1. PPBS-based Framework For Smart agriculture.

the description of the data block including the pointer to data block stored in the farmer's private blockchain channel in the cloud. The consortium blockchain will store this transaction notice once the involved data block and transaction notice have been confirmed by the Consortium via majority voting. As the value of a data block is associated with the time, e.g., field temperature in the morning, and evening etc., each block should be encrypted with a different session key if symmetric encryption is used. Or different data block is equipped with a different access control policy so that access to the data is based on the block-level.

Data Access:

- Owner access: has full access
- Access from other consortium members: other members have access to the encrypted data block in the owner's private blockchain channel in the cloud for the verification purpose. Access to the content of a specific data block must get permission from the data owner. The negotiation of the permission including the decryption key distribution is conducted out of band.
- Third party access: No public access to the owner's private channel. Access to the data must be negotiated with the owner via out of band mechanisms.

B. SMART CONTRACT FOR BUSINESS BIDDING

Secure automated business biding and trading order processing are another major application of smart framing. There is no adequate and dedicated framework for this process. The PPSAF framework can also be applied to addressing issue. The proposed solution is illustrated as follows: Suppose a retailer agent RA would like to place an order for certain goods, e.g., grapes, from farmers. For convenience, we assume relevant transactions are broadcast over the Consortium Blockchain, signed and are validated by the Blockchain, unless specified otherwise. After the broadcast has occurred, the negotiation process is conducted out of band. Goods orders are as follows:

Step 1: RA fetches the membership ID list of the Consortium Blockchain and selects a group S that consists of targeted members, e.g., grape farmers.

Step 2: RA constructs an order for goods in a smart contract format specifying legal terms/conditions, parameters of goods such as quality, minimum individual supply quantity threshold, minimum and maximum total supply quantity, banking institutions, and date of delivery etc...

Step 3: RA broadcast the signed and encrypted smart contract to the group S via Identity-based broadcast encryption schemes.

Step 4: Farmers in the group S can decrypt the smart contract. Those who are interested in supplying the goods and are satisfied with the terms and conditions set in the smart contract will broadcast their signed agreements that are encrypted with RA's public key.

Step 5: RA's smart contract will periodically check transmitted agreements and the smart contract will be triggered once the condition, such as total supply volume threshold, is met.

Step 6: Similar to Step 3, the bank broadcast the payment transaction receipts for RA's payment/deposit to individual farmer/supplier F_i which are encrypted with the group (RA,

F_i). This ensures only the payment recipient F_i and the payer RA can decrypt the receipts. At this stage, we assign the bank to issuing payment transaction evidence only and do not include a smart contract triggering the bank's automated payment. This is because existing banking systems have either in-person security check for large sum payment or Internet banking, which offers more security control.

Step 7: Individual supplier F_i will arrange logistics for the goods delivery. Similar to the RA, logistics companies can also deploy smart contracts for the order to arrange delivery for a set of suppliers.

This protocol can be tailored to accommodate bidding process. For example, multiple logistics companies can place different orders, which can only be viewed by targeted suppliers. Farmers can choose their preferred contracts securely and independently.

V. FUTURE TRENDS FOR PRIVACY PRESERVATION WITH BLOCKCHAIN TECHNOLOGIES

As we can see, blockchain has already expanded its applicability to more and more areas. As a result, more fields should appear with privacy protection in the existing list of blockchain applications enabled. There are several domains in which there is both a need for transparency and tamper-proof. Let us take E-voting for example. E-voting requires all the processes to be transparent and accurate. However, the proposed E-voting schemes have not resolved the privacy requirements to ensure the anonymity of the voters and especially the bridging from voters to vote data. Therefore, E-voting is very likely to attract interest with the application of blockchain with privacy-preserving techniques. In addition, given that more applications have been smart-contracts-enabled, there is a potential for both blockchain and smart contracts to assist in this space.

There are several architectural areas of future work aspects that, once developed, will provide significant benefit. There is a need for a greater number of reference blockchain and smart contracts architectures for different purposes, preferably in a field-agnostic manner. This could provide templates and reference architectures that assist across many fields, allowing researchers and developers to implement best-of-breed adaptations with confidence that their implementation is fit for purpose. This would not work across all fields, as each implementation may require unique characteristics.

Given the continuing research and development in IoT, there is an increasing need for more work to integrate Blockchain and smart contract paradigms into these emerging ecosystems. Importantly, fuelled by success, the promises of IoT are closer than ever, with multiple paradigms that are able to communicate with one another, resulting in more consensus algorithms. This will lead to an increase in IoT ecosystems that actively use consensus algorithms and blockchain. Hence, there is a necessity to ensure the privacy of systems, devices, data and entities. Security techniques and protocols are also expected to bloom, providing more various ways to ensure the privacy. In addition, due to the fact that biometric authentication systems have provided a more convenient way to control the access in IoT, the protection of biometric templates in IoT environment is critical since unlike database where it is stored in a centralized manner, blockchain has decentralized the IoT environment. Therefore, decentralized biometric authentication systems with template protection mechanism should be the next interesting area to which researchers pay attention.

VI. CONCLUSION

As blockchain has found its way to be a useful tool in real life thanks to its decentralized manner and robustness against data manipulation, the privacy of the involved parties as well as data transparency is still an open question. In order to fully leverage the power of blockchain technology without compromising the security, techniques to ensure the privacy ought to be implemented.

In this survey, we have discussed the current challenges in privacy protection when applying Blockchain in different fields. Based on that, we have provided two layers of categorization for privacy-preserving blockchain applications by first reviewing some key advances in different blockchain's applicability areas, then categorized the types of privacy accordingly. Importantly, we proposed PPSAF, a novel Privacy-Preserving Smart Agriculture Framework based on blockchain to further explore this technology's potential in smart farming and smart agriculture. The future trends for privacy protection in blockchain have also been discussed, as we expect advances in the areas of blockchain and privacy-preservation to create new opportunities in e-voting, smart farming and agriculture, smart cities, and smart contract-enabled applications in the near future. As a result, the demand for a better security while maintaining the transparency and decentralization will only increase, and technologies such as blockchain will likely underpin these advances.

REFERENCES

[1] N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: Trick or treat?," in Proc. Digitalization Supply Chain Manage. Logistics: Smart Digit. Solutions Ind. 4.0 Environ. *Proc. Hamburg Int. Conf. Logistics*, vol. 23. Berlin: epubli GmbH, 2017, pp. 3–18.

[2] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, 2019.

[3] N. Kshetri, "1 blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manage.*, vol. 39, pp. 80–89, 2018.

[4] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," in *Proc. IoT Vertical Topical Summit Agriculture-Tuscany.*, 2018, pp. 1–4.

[5] R. Cole, M. Stevenson, and J. Aitken, "Blockchain technology: Implications for operations and supply chain management," *Supply Chain Manage. An Int. J.*, vol. 24, no. 4, pp. 469–483, 2019.

[6] D. Shakhbulatov, J. Medina, Z. Dong, and R. Rojas-Cessa, "How blockchain enhances supply chain management: A survey," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 230–249, 2020.

[7] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Informat. Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017.

[8] G. Drosatos and E. Kaldoudi, "Blockchain applications in the biomedical domain: A scoping review," *Comput. Struct. Biotechnol. J.*, vol. 17, pp. 229–240, 2019.

[9] M. Johnson, M. Jones, M. Shervey, J. T. Dudley, and N. Zimmerman, "Building a secure biomedical data sharing decentralized app (DAPP): Tutorial," *J. Med. Internet Res.*, vol. 21, no. 10, 2019, Art. no. e13601.

[10] A. F. Hussein, A. K. ALZubaidi, Q. A. Habash, and M. M. Jaber, "An adaptive biomedical data managing scheme based on the blockchain technique," *Appl. Sci.*, vol. 9, no. 12, 2019, Art. no. 2494.

[11] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *Symmetry*, vol. 9, no. 8, 2017, Art. no. 164.

[12] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Inf. Sci.*, vol. 462, pp. 262–277, 2018.

[13] O. Jacobovitz, "Blockchain for identity management," *The Lynne William Frankel Center Comput. Sci. Dept. Comput. Sci.* Beer Sheva: Ben-Gurion University, 2016.

[14] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020.

[15] A. V. Ertemel, "Implications of blockchain technology on marketing," *J. Int. Trade, Logistics Law*, vol. 4, no. 2, pp. 35–44, 2018.

[16] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous reputation system for iiot-enabled retail marketing atop pos blockchain," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3527–3537, Jun. 2019.

[17] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "How blockchain technology can benefit marketing: Six pending research areas," *Front. Blockchain*, vol. 3, pp. 1–12, 2020.

[18] I. Antoniadis, K. Spinthiropoulos, and S. Kontsas, "Blockchain applications in tourism and tourism marketing: A short review," in *Strategic Innovative Marketing and Tourism*. Berlin, Germany: Springer, 2020, pp. 375–384.

[19] T. Hwang, *Subprime Attention Crisis: Advertising and the Time Bomb At the Heart of the Internet*. New York, NY, USA: Farrar Straus Giroux, 2020.

[20] T. Blake, C. Nosko, and S. Tadelis, "Consumer heterogeneity and paid search effectiveness: A large-scale field experiment," *Econometrica*, vol. 83, no. 1, pp. 155–174, 2015.

[21] B. Shapiro, G. J. Hitsch, and A. Tuchman, "Generalizable and robust tv advertising effects," *NBER Working Paper*, 2020, Paper w27684.

[22] D. L. Chaum, *Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups*. Electronics Research Laboratory, Univ. California, California, USA, 1979.

[23] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," in *Sequences Ii*. Berlin, Germany: Springer, 1993, pp. 329–334.

[24] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, 2018.

[25] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *Proc. Int. Conf. Secur., Privacy Anonymity Computation, Commun. Storage*. Berlin, Germany: Springer, 2017, pp. 534–543.

[26] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "Bpds: A blockchain based privacy-preserving data sharing for electronic medical records," in *Proc. IEEE Global Commun. Conf.*, 2018, pp. 1–6.

[27] J. Xu *et al.*, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019.

[28] A. Mohsin *et al.*, "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication," *Comput. Standards Interfaces*, vol. 66, 2019, Art. no. 103343.

[29] M. A. Baqari and E. Barka, "Biometric-based blockchain ehr system (bbehr)," in *Proc. Int. Wireless Commun. Mobile Comput.*, 2020, pp. 2228–2234.

[30] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," *IEEE Netw.*, vol. 33, no. 5, pp. 27–33, Sep.–Oct. 2019.

[31] Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, "BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems," *J. Med. Syst.*, vol. 42, no. 8, 2018, Art. no. 147.

[32] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, 2019, Art. no. 326.

[33] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, 2018, Art. no. 140.

[34] T.-T. Kuo and L. Ohno-Machado, "Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," 2018, *arXiv:1802.01746*.

[35] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, "Securing cnn model and biometric template using blockchain," *IEEE Int. Conf. Biometrics Theory, Appl. Syst.*, 2019, pp. 1–6.

[36] A. Goel, A. Agarwal, M. Vatsa, R. Singh, and N. Ratha, " Deepring: Protecting deep neural network with blockchain," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops*, 2019, pp. 2821–2828.

[37] A. Othman and J. Callahan, "The horcrux protocol: A method for decentralized biometric-based self-sovereign identity," in *Proc. Int. Joint Conf. Neural Netw.*, 2018, pp. 1–7.

[38] M. A. Acquah, N. Chen, J.-S. Pan, H.-M. Yang, and B. Yan, "Securing fingerprint template using blockchain and distributed storage system," *Symmetry*, vol. 12, no. 6, 2020, Art. no. 195.

[39] "Interplanetary file system," Accessed: Dec. 1, 2020. [Online]. Available: https://ipfs.io/

[40] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," *Comput. Secur.*, vol. 21, no. 6, pp. 539–556, 2002.

[41] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain," *IACR Cryptol. Eprint Arch.*, vol. 2017, 2017, Art. no. 1043.

[42] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Softw.*, vol. 35, no. 4, pp. 95–99, Jul./Aug. 2018.

[43] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *Int. J. Netw. Secur. Its Appl.*, vol. 9, no. 3, pp. 1–9, 2017.

[44] D. Chaum, "Blind signature system," in *Advances in Cryptology*. Berlin, Germany: Springer, 1984, pp. 153–153.

[45] F. Hjalmarsson, G. K. Hreidharsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-based e-voting system," in *Proc. IEEE 11th Int. Conf. Cloud Comput.*, 2018, pp. 983–986.

[46] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy.*, 2016, pp. 839–858.

[47] A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," *in Europe and MENA Cooperation Advances in Information and Communication Technologies*. Berlin, Germany: Springer, 2017, pp. 523–533.

[48] N. Kaaniche and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl.*, 2017, pp. 1–5.

[49] W. Shao, C. Jia, Y. Xu, K. Qiu, Y. Gao, and Y. He, "Attrichain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain," *Comput. Secur.*, 2020, Art. no. 102069.

[50] H. Halpin, "Nym credentials: Privacy-preserving decentralized identity with blockchains," in *Proc. Crypto Valley Conf. Blockchain Technol.*, 2020, pp. 56–67.

[51] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "A privacy-preserving thin-client scheme in blockchain-based PKI," in *Proc. IEEE Glob. Commun. Conf.*, 2018, pp. 1–6.

[52] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI," *Future Gener. Comput. Syst.*, vol. 96, pp. 185–195, 2019.

[53] A. S. Patil, R. Hamza, A. Hassan, N. Jiang, H. Yan, and J. Li, "Efficient privacy-preserving authentication protocol using pufs with blockchain smart contracts," *Comput. Secur.*, vol. 97, 2020, Art. no. 101958.

[54] M. Jones, M. Johnson, M. Shervey, J. T. Dudley, and N. Zimmerman, "Privacy-preserving methods for feature engineering using blockchain: Review, evaluation, and proof of concept," *J. Med. Internet Res.*, vol. 21, no. 8, 2019, Art. no. e13600.

[55] Y. Qiu, Y. Liu, X. Li, and J. Chen, "A novel location privacy-preserving approach based on blockchain," *Sensors*, vol. 20, no. 12, 2020, Art. no. 3519.

[56] Z. Guan *et al.*, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[57] M. Baza, M. Nabil, M. Ismail, M. Mahmoud, E. Serpedin, and M. A. Rahman, "Blockchain-based charging coordination mechanism for smart grid energy storage units," in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 504–509.

[58] S. Tan, X. Wang, and C. Jiang, "Privacy-preserving energy scheduling for escos based on energy blockchain network," *Energies*, vol. 12, no. 8, 2019, Art. no. 1530.
[59] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.
[60] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K. R. Choo, "A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5110–5118, Aug. 2020.
[61] M. Daghmehchi Firoozjaei, A. Ghorbani, H. Kim, and J. Song, "Hybridge: A hybrid blockchain for privacy-preserving and trustful energy transactions in internet-of-things platforms," *Sensors*, vol. 20, no. 3, p. 928, 2020.
[62] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192, Nov./Dec. 2018.
[63] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-Preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5760–5772, Jun. 2020.
[64] R. Sharma and S. Chakraborty, "Blockapp: Using blockchain for authentication and privacy preservation in iov," in *Proc. IEEE Globecom Workshops*, 2018, pp. 1–6.
[65] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for vanets," *IEEE Access*, vol. 6, pp. 45 655–45 664, 2018.
[66] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for vanets," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Dec. 2019.
[67] B. Guehguih and H. Lu, "Blockchain-based privacy-preserving authentication and message dissemination scheme for vanet," in *Proc. 5th Int. Conf. Syst., Control Commun.*, 2019, pp. 16–21.
[68] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2019.
[69] Q. Feng, D. He, S. Zeadally, and K. Liang, "Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.
[70] L. Li *et al.*, "Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.
[71] Y. Pu, T. Xiang, C. Hu, A. Alrawais, and H. Yan, "An efficient blockchain-based privacy preserving scheme for vehicular social networks," *Inf. Sci.*, vol. 540, pp. 308–324, 2020.
[72] H. Shen, J. Zhou, Z. Cao, X. Dong, and K.-K. R. Choo, "Blockchain-based lightweight certificate authority for efficient privacy-preserving location-based service in vehicular social networks," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6610–6622, 2020.
[73] J. Hu, D. He, Q. Zhao, and K.-K. R. Choo, "Parking management: A blockchain-based privacy-preserving system," *IEEE Consum. Electron. Mag.*, vol. 8, no. 4, pp. 45–49, Jul. 2019.
[74] W. Al Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Privacy-preserving smart parking system using blockchain and private information retrieval," in *Proc. Int. Conf. Smart Appl., Commun. Netw. (SmartNets)*, 2019, pp. 1–6.
[75] M. Baza, M. Mahmoud, G. Srivastava, W. Alasmary, and M. Younis, "A light blockchain-powered privacy-preserving organization scheme for ride sharing services," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC2020-Spring)*, 2020, pp. 1–6.
[76] M. Li, L. Zhu, and X. Lin, "Coride: A privacy-preserving collaborative-ride hailing service using blockchain-assisted vehicular fog computing," in *Proc. Int. Conf. Secur. Privacy Commun. Syst*. Berlin, Germany: Springer, 2019, pp. 408–422.
[77] M. Kim, B. Hilton, Z. Burks, and J. Reyes, "Integrating blockchain, smart contract-tokens, and iot to design a food traceability solution," in *Proc. IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf.*, 2018, pp. 335–340.
[78] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and iot based food traceability for smart agriculture," in *Proc. 3rd Int. Conf. Crowd Sci. Eng.*, 2018, pp. 1–6.
[79] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019.
[80] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Comput. Secur.*, vol. 88, 2020, Art. no. 101653.
[81] Y. Zhao, Y. Liu, A. Tian, Y. Yu, and X. Du, "Blockchain based privacy-preserving software updates with proof-of-delivery for internet of things," *J. Parallel Distrib. Comput.*, vol. 132, pp. 141–149, 2019.
[82] Q. Zhao, S. Chen, Z. Liu, T. Baker, and Y. Zhang, "Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems," *Inf. Process. Manage.*, vol. 57, no. 6, 2020, Art. no. 102355.
[83] T. Le and M. W. Mutka, "Capchain: A privacy preserving access control framework based on blockchain for pervasive environments," in *Proc. IEEE Int. Conf. Smart Comput.*, 2018, pp. 57–64.
[84] P. J. Lu, L.-Y. Yeh, and J.-L. Huang, "An privacy-preserving cross-organizational authentication/authorization/accounting system using blockchain technology," in *Proc. IEEE Int. Conf. Commun.*, 2018, pp. 1–6.
[85] F. Casino and C. Patsakis, "An efficient blockchain-based privacy-preserving collaborative filtering architecture," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1501–1513, 2019.
[86] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, 2019.
[87] Y. Chen, H. Xie, K. Lv, S. Wei, and C. Hu, "Deplest: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks," *Inf. Sci.*, vol. 501, pp. 100–117, 2019.
[88] D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, "Secure online voting system using biometric and blockchain," in *Data Management Analytics and Innov.* Berlin, Germany: Springer, 2020, pp. 93–110.
[89] E. Akbari, Q. Wu, W. Zhao, H. R. Arabnia, and M. Q. Yang, "From blockchain to internet-based voting," in *Proc. Int. Conf. Comput. Sci. Comput. Intell.*, 2017, pp. 218–221.
[90] S. Panja and B. K. Roy, "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain," *IACR Cryptol. Eprint Arch.*, vol. 2018, 2018, Art. no. 466.
[91] R. Nimje and D. Bhalerao, "Blockchain based electronic voting system using biometric," in *Proc. Int. Conf. Sustain. Commun. Netw. Appl*. Berlin, Germany: Springer, 2019, pp. 746–754.
[92] T. Roopak and R. Sumathi, "Electronic voting based on virtual id of aadhar using blockchain technology," in *Proc. 2nd Int. Conf. Innov. Mechanisms Ind. Appl.*, 2020, pp. 71–75.
[93] R. Bosri, A. R. Uzzal, A. Al Omar, A. T. Hasan, and M. Z. A. Bhuiyan, "Towards a privacy-preserving voting system through blockchain technologies," in *Proc. IEEE Intl. Conf. Dependable, Autonomic Secure Comput., Intl. Conf. Pervasive Intell. Comput., Intl. Conf. Cloud Big Data Comput., Intl. Conf. Cyber Sci. Technol. Congr.*, 2019, pp. 602–608.
[94] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019.
[95] A. Meola, "Smart farming in 2020: How IoT sensors are creating a more efficient precision agriculture industry," *Bus. Insider*, 2020, Accessed: Dec. 4, 2020. [Online]. Available: https://www.businessinsider.com/smart-farming-iot-agriculture?r=AU&IR=T
[96] L. Huning, J. Bauer, and N. Aschenbruck, "A privacy preserving mobile crowdsensing architecture for a smart farming application," in *Proc. 1st ACM Workshop Mobile Crowdsensing Syst. Appl.*, 2017, pp. 62–67.

QUANG NHAT TRAN received the B.S. degree majoring in computer science from New Mexico Highlands University, Las Vegas, NM, USA, in 2012 and the master's degree in 2017 from the University of New South Wales, Sydney, NSW, Australia, where he is currently working toward the Ph.D. degree. In 2013, he was a Lecturer with the Department of Computer Science and Technology, Posts and Telecommunication Institute of Technology, Hanoi, Vietnam. His research interests include computer security, biometric template protection, biometric cryptography, and blockchain technology.

BENJAMIN P. TURNBULL is currently a Senior Lecturer with the Australian Centre for Cyber Security, University of New South Wales, Sydney, NSW, Australia. His research interests include cyber-resilience, cyber-kinetic impact analysis, and novel methods for network analysis. He was with the Australian Defence Force.

HAO-TIAN WU received the B.Eng. and M.Eng. degrees from the Harbin Institute of Technology, Harbin, China, in 2002 and 2004, respectively, and the Ph.D. degree in computer science from Hong Kong Baptist University, Hong Kong, in 2007. He is currently an Associate Professor with the School of Computer Science and Engineering, South China University of Technology, Guangzhou, China. His research interests include image enhancement, homomorphic encryption, privacy preservation, and reversible data hiding. He has published in top publications such as the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY and the IEEE SIGNAL PROCESSING LETTERS.

A. J. S. DE SILVA received the Ph.D. degree in computer science from the Australian Defence Force Academy (ADFA) and University of New South Wales. He is the Group Managing Director of TelSoft Pty Ltd., and has implemented Telecommunications projects in more than 40 counties. He is the Founding Director of Smartfarmnet Australia.

KATERINA KORMUSHEVA received the Ph.D. degree in marketing management from Australian National University, Canberra, ACT, Australia. She is a Certified Practicing Marketer by the Australian Institute of Marketing and a Professional Certified Marketer by the American Marketing Association. She has published in top service and marketing publications such as *The Journal of Services Marketing*.

JIANKUN HU (Senior Member, IEEE) received the B.E. degree from Hunan University, Changsha, China, in 1983, the Ph.D. degree in control engineering from the Harbin Institute of Technology, Harbin, China, in 1993 and the Masters by Research in computer science and software engineering from Monash University, Melbourne, VIC, Australia, in 2000. He is currently a Full Professor with the School of Engineering and Information Technology, University of New South Wales, Canberra, Australia. He was with Ruhr University, Bochum, Germany, on the prestigious German Alexander von Humboldt Fellowship 1995-1996 and from 1998 to 1999, a Research Fellow with Melbourne University, Melbourne, VIC, Australia. He has authored or coauthored many papers in his field of research in high quality conferences and journals including the IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, which include cyber security, including Image Processing, Forensics and machine learning. He was on the Editorial Board of seven international journals including the top publication IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and was the Security Symposium Chair of the IEEE flagship conferences of the IEEE ICC and the IEEE Globecom. He has obtained nine ARC (Australian Research Council) grants and has served at the prestigious Panel of Mathematics, Information and Computing Sciences (MIC), ARC ERA (The Excellence in Research for Australia) Evaluation Committee.