Privacy-Preserving Solutions for Blockchain: Review and Challenges

JORGE BERNAL BERNABE [1], **JOSE LUIS CANOVAS** [1], **JOSE L. HERNANDEZ-RAMOS** [2], **RAFAEL TORRES MORENO** [1], **AND ANTONIO SKARMETA** [1]

[1] Department of Information and Communication Engineering, University of Murcia, 30100 Murcia, Spain
[2] Joint Research Centre, European Commission, 21027 Ispra, Italy

Corresponding author: Jorge Bernal Bernabe (jorgebernal@um.es)

ABSTRACT Blockchains offer a decentralized, immutable and verifiable ledger that can record transactions of digital assets, provoking a radical change in several innovative scenarios, such as smart cities, eHealth or eGovernment. However, blockchains are subject to different scalability, security and potential privacy issues, such as transaction linkability, crypto-keys management (e.g. recovery), on-chain data privacy, or compliance with privacy regulations (e.g. GDPR). To deal with these challenges, novel privacy-preserving solutions for blockchain based on crypto-privacy techniques are emerging to empower users with mechanisms to become anonymous and take control of their personal data during their digital transactions of any kind in the ledger, following a Self-Sovereign Identity (SSI) model. In this sense, this paper performs a systematic review of the current state of the art on privacy-preserving research solutions and mechanisms in blockchain, as well as the main associated privacy challenges in this promising and disrupting technology. The survey covers privacy techniques in public and permissionless blockchains, e.g. Bitcoin and Ethereum, as well as privacy-preserving research proposals and solutions in permissioned and private blockchains. Diverse blockchain scenarios are analyzed, encompassing, eGovernment, eHealth, cryptocurrencies, Smart cities, and Cooperative ITS.

INDEX TERMS Blockchain, privacy, security, survey, bitcoin.

I. INTRODUCTION

The disintermediation provided by blockchain is changing the democratization, verifiability and universal access to tokenized digital assets of any kind, causing a revolution on diverse types of scenarios [1] beyond cryptocurrencies, such as healthcare [2], smart cities [3], decentralized Internet of Things (IoT) [4], intelligent transport systems [5] or e-Administration [6], to name a few. Blockchain allows transferring digital assets in a decentralized fashion using the *ledger*, without intermediary central third-parties, while enabling public verifiability as well as provenance of the digital transactions and data.

However, Blockchain solutions are subject to several different issues, such as compliance with legal regulations (e.g., the General Data Protection Regulation (GDPR) [7]), scalability and response times [8], security threats [9], or privacy

issues [10]–[12], which undermine user anonymity, confidentiality and privacy control in their transactions on the ledger.

These privacy issues rise concerns in citizens and companies that are still a bit wary to adopt blockchain in their processes and businesses, as it might imply sharing (even if encrypted and/or anonymized) in a public accessible database their data and transactions. Although the usage of pseudonyms avoids linking transactions to the real identity, users are not totally anonymous in their movements, since all usages behind these pseudonyms might be traceable and linkable, specially when handling multiple-entries transactions with several addresses from various accounts belonging to the same user [13].

In this context, emerging privacy-preserving proposals for blockchain [14], such as [15]–[19], and platforms, such as uPort [20] or Sovrin [21], propose enhanced decentralized ledgers that empower users with mechanisms to preserve their privacy in their digital transactions. The management

The associate editor coordinating the review of this manuscript and approving it for publication was Le Hoang Son.

of user's related information in permissioned Blockchains is being characterized by its privacy-preserving nature. With the rise of blockchain, Identity Management (IdM) systems are switching from traditional web-centric approach or identity federation approaches, towards the self-sovereign identity (SSI) paradigm [21]. Self-sovereign identities allow citizens to take control of their data in any-time in any online situation. Under this approach, user personal data is no longer kept in raw in third-parties services, neither in Service Providers or Identity Providers, and information regarding transactions and interactions of users in services can be anonymized. It avoids that third-parties can leak personal data, and, in the worst case, become a potential source of other, more important, risks, such as identity-related cyber-crimes (e.g. identity-theft). Nonetheless, despite the ideal features and benefits brought by SSI, as it has been analyzed in this paper, blockchain scenarios still need to face diverse privacy challenges, such as transaction linkability, blockchain P2P network privacy, private-keys management and recovery, cryptographic algorithms resistant to Quantum Computing, malicious Trusted Third Parties (TTP), malicious smart contracts, privacy-usability, non-erasable data in blockchain, compliance with privacy regulations, etc.

To cope with these challenges, some proposals for blockchain such as mixers services [22], [23] try to provide a third party in charge of concealing a transaction within a big amount of unrelated transactions. Thus, critical information such as the payer, payee, or payed amount [24] can be fully anonymized [25], although sometimes at expenses of transaction delays and more costs. Some other privacy-preserving crypto solutions are integrating SSI along with secure multi-party computation [26], or with Zero Knowledge Proofs (ZKPs), e.g. [16] and anonymous credential systems like [27] in the blockchain platform. Some other blockchain solutions use ring signatures [28] to conceal user's transactions.

This paper performs a systematic review of the blockchain privacy challenges as well as the privacy-preserving research proposals, techniques and solutions that are appearing to overcome the privacy issues in this promising technology. There already exist some other surveys about security in blockchain [9], but they are not directly focused on privacy. Besides, there are some other review papers on security and privacy in distributed ledgers such as [29], but they are mainly focused on bitcoin [30] or cryptocurrencies. There is another recent survey about privacy in blockchains [31], but, unlike this paper, they did not identify the privacy-related challenges, and the threats they cover are exclusively related to anonymity issues in transactions (which is just 1 of the 11 privacy-related challenges identified in this paper). In addition, they did not analyze the privacy solutions considering application scenarios neither the blockhain plafforms. Our survey paper targets a broader scope, including a review, not only about privacy-preserving crypto solutions in bitcoin, but also a review of privacy-preserving research proposals and platforms for diverse kinds of blockchain

scenarios, namely, eGovernment, eHealth, cryptocurrencies, Smart cities, and Cooperative ITS.

The contributions of this paper are manifold:

- First, this paper identifies and categorizes the main privacy challenges in blockchain.
- It performs a systematic review of the main privacy-preserving techniques and solutions for blockchain, including a taxonomy that categorizes the main techniques employed.
- In addition, the paper provides a survey of the privacy-preserving research proposals being adopted in main blockchain scenarios, comparing them and analyzing the current trends per scenario.
- Finally, we analyse the main privacy-preserving IdM systems and platforms in blockchain comparing their features.

The rest of the paper is organized as follows. Section II overviews main concepts about privacy and blockchain, and oversees the privacy-preserving IdM towards SSIs on blockchain. Section III reviews the main privacy challenges in blockchain. Section IV surveys the current state-of-the-art about main privacy approaches and techniques for both, permissioned and permissionless blockchains. Section V is devoted to the analysis and review of the main research papers and blockchain solutions/platforms for diverse kinds of blockchain-enabled scenarios.Then, Section VI describes several research directions derived from the previous analysis. Finally, the conclusions are drawn in Section VII.

II. BLOCKCHAIN AND THE PRIVACY-PRESERVING SELF-SOVEREIGN IDENTITY MODEL

The big data era is undermining the user's privacy in multiple digital scenarios. Large third-parties benefit from the management of their users data, by collecting, analyzing, correlating and controlling massive amounts of personal data. These organizations, and their services, are subject to security breaches and user data misuse, which might compromise users' privacy, even without user-awareness. Transactions in the blockchain are not immune to these privacy issues. Besides, individuals are given few options to control their personal data and their privacy during their online transactions, encompassing how, when, where, by whom, and which particular personal information is disclosed in each particular transaction. This problem is intensified in blockchain, as the private data included in the ledger is immutable and the user's rights to control and rectify personal information decrease. This situation is aggravated with the coming of IoT scenarios where billions of constrained smart objects, with scarce capabilities to enforce proper security mechanisms, strive to deal with cyber-attacks that might leak their handled data, and ultimately, sensitive and private information of their owners/users. Besides, in IoT, user privacy controls are difficult to apply, as the smart objects usually act on behalf of the user without user control and consent, undermining the adoption of the minimal personal disclosure principle.

In this context, the research community and stakeholders institutions are working to strengthen information privacy, which was highlighted by [32] as a key multilevel concept that has been studied by diverse disciplines. Diverse taxonomies of privacy have been defined in the literature [33], [34]. Furthermore, [35] provided an interdisciplinary review on information privacy, which can be defined as the ability to control information about oneself [36]. In this regard, as analyzed by [37], the notion of Privacy embraces two main areas, *Confidentiality* and *Control*.

On one hand, when it comes to *Confidentiality*, privacy is seen as the protection of personal data against unauthorized accesses, keeping personal data protected, anonymized and therefore private with regard to the general public. In this sense, many different mechanisms can be employed to anonymize the collected information, secure protected information, encrypt data, protect connectivity channels, etc., thereby ensuring integrity, anonymity, unlinkability, communication protection, undetectability and unobservability [38]. On the other hand, privacy refers also to the right given to citizens to *Control* and manage their personal data at any time, ensuring user self-determination, as defined in the European GDPR [7]. Privacy as Control can be implemented through Privacy Enhancing Technologies (PET), ensuring selective and minimal disclosure of credentials and personal attributes using, for instance, Anonymous Credential Systems [39] such as Idemix [27], which employs ZKPs to reveal the minimal amount of information to the verifier (usually a service provider), even without disclosing the attribute value itself.

Different surveys about privacy enhancing technologies have been provided (e.g., [40] or [41]), but they did not consider privacy-preserving mechanisms in blockchain. The following sections give an overview to blockchain and how it can be used along with PETs to increase user's privacy, considering the broad notion of privacy, i.e. as *Control* and as *Confidentiality*. Afterwards, this section will also introduce the privacy-preserving identity models that are being raised in blockchain to empower users with self-sovereignty, thereby giving them full control of their personal data and privacy configuration.

A. INTRODUCTION TO BLOCKCHAIN CONCEPTS

Blockchain shifts trust from a classical centralized approach to a fully decentralized network of nodes. It is based on a synchronized Distributed Ledger Technology (DLT), which acts as a decentralized database, keeping the information replicated and shared among multiples nodes spread in remote locations.

The concept of blockchain was first introduced by Satoshi Nakamoto in [30] as the technical foundations of a new peer-to-peer version of electronic cash. There are many blockchain definitions (e.g., [14] or [42]) that briefly defined the blockchain as *"a public ledger distributed over a network that records transactions (messages sent from one network node to another) executed among network participants.*

Each transaction is verified by network nodes according to a majority consensus mechanism before being added to the blockchain. Recorded information cannot be changed or erased and the history of each transaction can be re-created at any time."

Blockchain brings many advantages encompassing provenance, accountability, traceability and transparency of the transactions stored in the ledger. It provides a fully decentralized root of trust avoiding central authorities, thereby facilitating trust across initially non-trusted or unknown stakeholders and users. The decentralized nature makes highly difficult to alter transaction history. In addition, blockchain transactions are stored in a fully decentralized P2P network, which replicates data storage, thereby disabling potential data loss.

Figure 1 shows a high level representation of blockchain, including the main blockchain pillars and concepts, which are introduced below:

- *Transaction*: a single record in the ledger that can specify a piece of information or an operation over previous transactions, e.g. to send the funds from a previous transaction to another public address.
- *Block*: a group of transactions, establishing a chronological order between them. A block also includes a *Hash pointer* to the previous block of the blockchain.
- *Genesis block*: the first block in a blockchain, establishing a starting point for the linked list of hash pointers.
- *Chain*: the linked list of hash pointers from the genesis block to the last block. The chain determines the chronological order of all transactions, as well as the integrity of the entire blockchain. One can verify the integrity of the chain by computing the hashes from the genesis block to the last one; if any hash pointer to the previous block differs from the one computed, the chain has been altered.
- *Merkle Tree* [43]: a binary tree where the leaves are the hash pointers of the transactions in a block, and each parent node is the hash of the two children nodes. As can be seen in Figure 1, the root of the Merkle tree is a hash that gives integrity to all transactions in a block, including their order within it. The complete block's hash pointer is the hash of the Merkle tree root, with the hash pointer of the previous block and any consensus information that makes the node valid. When verifying integrity of the chain, the Merkle tree allows computing the valid hash of the block, without having the entire transaction information on the disk. Traditionally in Bitcoin, the Merkle tree is used to reclaim disk space from old spent transactions (which in theory are not used again), but the Merkle tree also allows to give proof of existence for a transaction in the blockchain without including in the proof the rest of transactions in the block.
- *Network*: referring to the *blockchain network*, it is the set of nodes that interact among them in a peer-to-peer (P2P) fashion, exchanging the blockchain data, adding
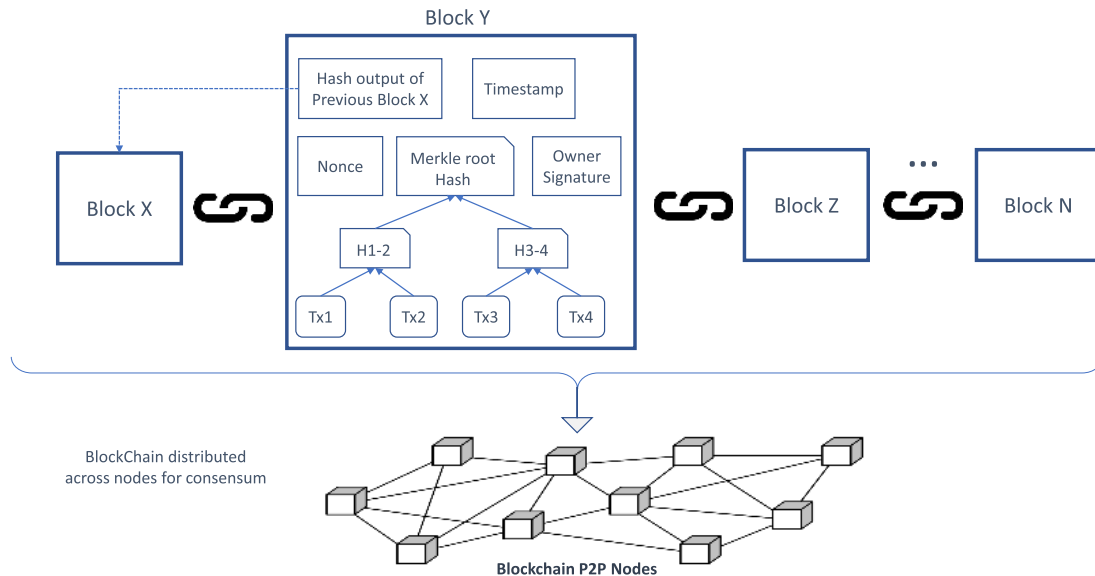
FIGURE 1. Blockchain overview.

transactions, validating them, and agreeing on what new blocks are added to the head of the chain.

- *Consensus*: the algorithm run by the nodes of the network to agree on the state of the blockchain. The set of all transactions, in turn, defines this state. When a new transaction is added, the state changes. Because of possible delays transmitting the new transaction to all nodes, the order in which transactions arrive at a node may differ with respect to other nodes. Since there is not a central authority node to decide which transaction arrived before, the consensus algorithm is run by the network and can be verified by any node, shifting the trust from a traditional central authority to a distributed verification through cryptographic methods.

- *Fork*: depending on the consensus algorithm, the network may accept two blocks at the same point of the chain. This creates a fork of the chain. Part of the network may continue to add blocks using one of the forks, while the other part uses the other fork. Because the hash pointers of each block will differ, the chains are incompatible, so that the network must agree on which fork to use. In Bitcoin, the longest fork is the valid one. This solves the problem of malicious nodes creating a fork before spending some funds to regain them. During the consensus algorithm, a new shorter fork is rejected.

- *Script*: piece of code embedded in a transaction, based on a limited programming language that establishes the conditions to validate a transaction. For example, in Bitcoin, the script allows differing a payment to a given date, or until more signatures from other nodes are present in the chain.

- *Smart Contract*: evolution of the script language, usually Turing complete, but deterministic, which allows shifting from a static transaction to execution of code. A transaction that is a result of executing a smart contract

can be verified by any other node by executing the same smart contract with the same inputs. For instance, the blockchain Ethereum defines the Solidity language, and the Ethereum Virtual Machine (EVM), where the compiled bytecode is executed [44].

Blockchain architectures depend on the rights given to the users to read/write on the ledger, that is, whether it offers public or private access for reading as well as whether it supports permissioned/permissionless access for writing and making consensus agreements. Three main different blockchain architectures can be identified:

- *Public Permissionless Blockchain*, where anyone can read, write and participate in consensus. The transactions are transparent but with participants using some anonymity or pseudo-anonymity. It is useful in cryptocurrencies, but it is, in general, subject to privacy issues, as will be described in Section V-E.

- *Private Permissioned Blockchain*, where the participating nodes must be granted access to the network, via an invitation or *permission*, in order to perform operations over the distributed ledger or participate in consensus. The access control mechanism could vary, and existing participants could decide future entrants; a regulatory authority could issue licenses for participation; or a consortium could make the decisions instead [45]. The consensus is carried out thanks to specific agreements among the participating stakeholders

- *Public Permissioned Blockchain*, a concept introduced by the Sovrin Foundation [21], identifies those blockchain instances that are open for all to use, that is, read or change the state of the ledger, but the network of nodes performing consensus is permissioned. This kind of blockchain also allows that only an elected group of participants could write in the ledger.
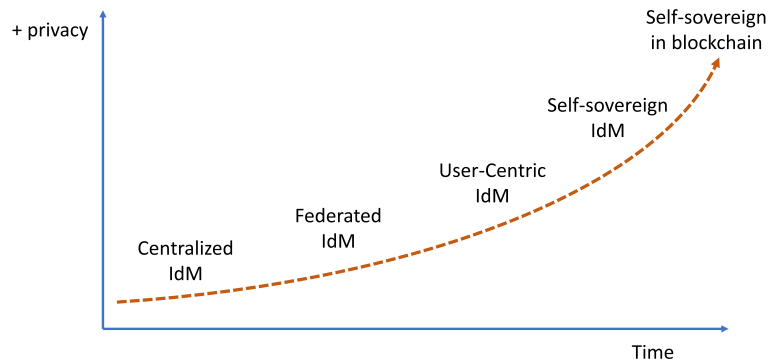
FIGURE 2. Identity management methods evolution over time, according to privacy preservation capabilities.

For further information about blockchain, the reader is referred to [46], which provides a comprehensive overview on blockchain technology, including consensus mechanisms, architectures.

B. SELF-SOVEREIGN AND PRIVACY-PRESERVING IDENTITY MODELS IN BLOCKCHAIN

This section introduces the privacy-preserving Identity Management (IdM) models that are being proposed to strengthen privacy in blockchain. To this aim, it describes the evolution of different IdM models over time, analysing their privacy-preservation features and implications.

In the past, traditional centralized IdM solutions, based on central authorities, set up silos of trust, meaning subjects cannot sign-on across different domains. This kind of IdM system is subject to different problems and threats such as data breaches, identity theft and privacy concerns. The rise of federated IdM models helped to mitigate partially those problems enabling Single Sign-on (SSO). This kind of server-centric systems enables users to adopt the same identity system across different domains. The user is redirected for authentication and user identity data retrieval to his home identity provider. Some federated IdM initiatives such as Stork [47], have gone a step forward implementing a cross-border and user-centric approach, since users are put in the middle to take control of their personal data. In this case, they are asked about their consent each time their data is released in the federation from its home identity provider (data controller) to the service provider (data processor).

Several technologies, such as OpenId [48], SAML [49] or Fido [50], can be used as a baseline for implementing this user-centric approach, empowering users to share its identity across different services. Nonetheless, user-centric identity federations are still subject to privacy issues, identity theft and data leakage, as user data related to his identity is still hold in the server side, and authentication is validated in the server (usually through a knowledge-base and some other weak authentication mechanisms, such as passwords).

Unlike those traditional approaches, IdM based on self-sovereign identities [21] (SSI) focuses on providing a privacy-respectful solution, enabling users with full control

and management of their personal identity data without needing a third-party centralized authority taking over the identity management operations. Thus, citizens are not anymore data subjects, instead, they become the data controller of their own identity. This is, they can determine the purposes, and ways in which personal data is processed, as they manage directly their personal data during their online transactions. Figure 2 shows a representation of the evolution of these IdM models as they have appeared over time, and its relationship with their privacy-preserving capabilities.

Chritofer Allen described in the detail this path [51] to SSI, and detailed the ten Principles of Self-Sovereign Identity: Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimalization, Protection. Diverse investigations in the scope of SSI have been conducted recently embracing a user-centric and privacy-preserving approach for mobiles using anonymous credential systems, verifiable attribute credentials and claims that use ZKPs, thereby giving full control to users to interact directly with the verifier. Examples of those research investigations can be found in the scope of Irma EU project [52], H2020 EU Aries project (see our recent works [53]), H2020 EU Olympus project [54] as well as for IoT scenarios, e.g. in our previous works [55], [56].

Unlike those proposals, nowadays, SSI has been brought forward, as it is being materialized through blockchain, which facilitates the governance of the SSI system, increasing the performance to Internet scale and enabling the accessibility of identities to everyone. Blockchain enables sovereignty as users can be endowed with means to transfer digital assets, including user decentralized identifiers (DID) [57], DID documents, identity attributes, verifiable claims and proofs of identity [58] (including ZKPs), to anyone privately, without rules in behind, which ultimately increases the global democracy in the world. In this sense, latest blockchain solutions [20], [21] make use of DLTs, along with user-centric and mobile-centric approaches, and therefore, empowering users to maintain securely protected (in their mobile wallet) the needed crypto-credentials. In this scenario, blockchain acts as distributed and reliable identity verifier, providing provenance and verifiability of identities. Thus, the ledger provides
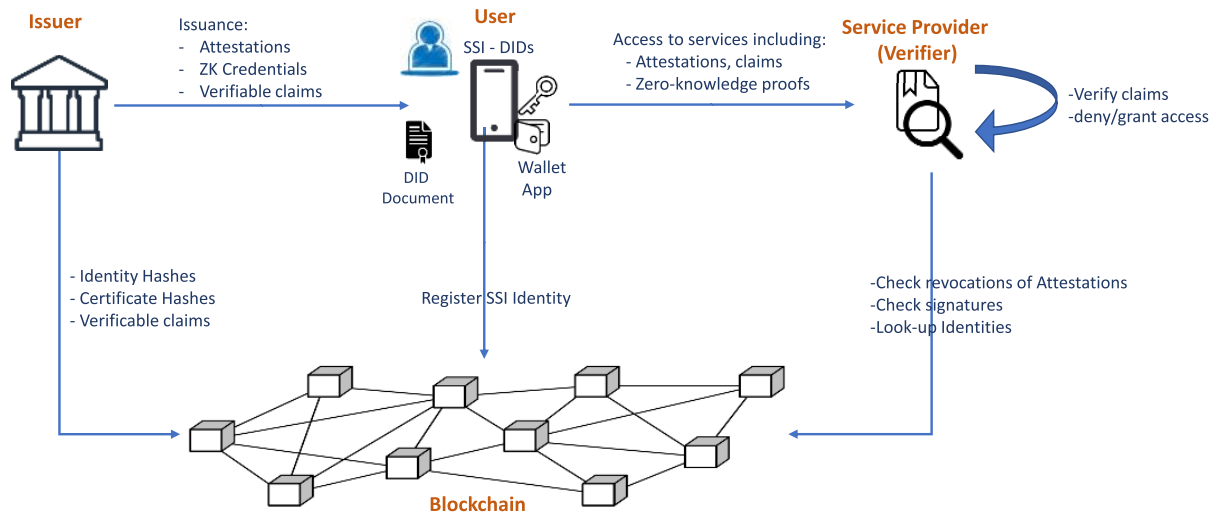
FIGURE 3. Self-Sovereign Identity Management Model in Blockchain.

a cryptographic root of trust, which facilitates identity management without external authorities. In this sense, [59] has recently described the main SSI concepts on blockchain and the road ahead.

These SSI concepts, their main processes and associated entities are depicted in Figure 3. As it can be seen, a User (holder) might have DIDs and obtain verifiable claims and credentials from the Issuer authority, in a user-centric way, using his smartphone whereby the private-keys are kept securely protected in the wallet. To increase the privacy-preserving capabilities in the SSI model, the user can be empowered with means to present Zero-Knowledge crypto proofs against a Service Provider acting as verifier that checks in the blockchain the attestations and signatures.

Despite the features and benefits brought by SSI and blockchain, they are subject to diverse privacy issues and challenges. The following section delves into the privacy challenges in blockchain.

III. PRIVACY CHALLENGES IN BLOCKCHAIN SCENARIOS

Since blockchain technology was created to support the Bitcoin cryptocurrency, the widest use of blockchain so far has been the creation of alternative cryptocurrencies. The blockchain solves the *double spending* problem. Without a central entity, a network of untrusted peers must agree on valid transactions (consensus), controlling that no malicious peers spend twice the same funds. Bitcoin solves it by making all transactions public on the ledger, so any node can keep track of the spent transactions. However, as it has been demonstrated in the literature, full anonymity is not ensured in bitcoin. In addition to cryptocurrencies, blockchain technology is revolutionizing also the way organizations manage their data and business/operational processes thanks to mechanisms that improve security and non-repudiation of operations. Along with these improvements, there are also a number of privacy challenges that appear in the application

of blockchain technology in different domains. These challenges are described in the following subsections.

A. TRANSACTION LINKABILITY

Although users of public blockchains can create new public addresses independently, the ledger keeps track of all their history in blockchain transactions graphs that link all independent public key addresses to the user [60]–[64]. In token based blockchains, multiple addresses of the same user could be correlated by:

- **Multi-entry transactions**: these kinds of transactions require having different addresses belonging to the same user, proving the knowledge of all private keys to spend them, making all input addresses linkable to the same user [10], [13], [15], [65]. In order to avoid this linkability problem, there should be different and one-time addresses for every transaction of digital assets, minimizing the number of input addresses in a transaction. A malicious user can relate transactions with wallets being able to discover balances, destinations or other sensitive information.

- **Transactions with change**: allows tracing the user when he is using the same public address to get some assets that have a change. To improve the privacy among these transactions, the user should create a new public address to receive the returns.

- **Curious/Malicious Mixing services**: outsourced and centralized Mixing services can be employed by users to improve their privacy by mixing transactions coming from different issuers. However, it can become a privacy issue as the service might know both input and output pairs; therefore, privacy relies on an honest intermediary [66]–[68].

- **Web payments**: the consumer identity may be linked to his real identity through browser cookies. When the user pays with a cryptocurrency, the service provider can link

the real identity to the token history in the blockchain, as shown in [69], which also states that the attack is resilient against mixing mechanisms like CoinJoin [70].

- **Blockchain P2P Network privacy**: the blockchain nodes communicate with each other in a P2P overlay network over the Internet, therefore, making the users traceable through the network [11] via their IP addresses when they submit new transactions. By observing the public addresses used in the blockchain, another blockchain network node could link the address with a wallet and real user, despite the supposed anonymity of new randomly generated addresses [71]. Privacy-focused blockchains, such as Monero [72], implement a privacy layer within their clients and the P2P blockchain network, by connecting first to another overlay network like TOR (onion routing) [73] or I2P (garlic routing) [74]. Nonetheless, [75] showed that using TOR as a network privacy layer to connect to the blockchain network opens a new set of vector attacks.

B. PRIVATE-KEYS MANAGEMENT AND RECOVERY

Private keys are used to sign each transaction in the blockchain; therefore, they are critical for the security and privacy of the user. In these cases, proper key management [76] systems needs to be enforced. If compromised, not only privacy leaks, but also identity theft may happen.

Blockchain wallets maintain, either on-line or (off-line) in user's devices, the blockchain keys. Unfortunately, wallets are subject to theft attacks [77], where the adversary might delete or stole user's private keys. This problem affects also to encrypted wallets, as diverse malware and trojans might crash a key recorder and access encryption keys.

The user may protect the keys kept within his own device (using wallet), or outsource the private keys management to a third party that acts on his behalf, as *cloud wallets*. This solution relies the security on a third party and trusts that it will not make a malicious use of the keys.

To prevent the loss of the private keys, traditional solutions can be applied, such as copy back-ups of the wallet file, as well as paper wallets with QR codes for the private and public keys, or password derived keys, where a master password and a pseudo-random number generator are used to derive the private keys [78].

When the user manages his own wallet, some solutions against malware attacks that may compromise his device consists on threshold cryptography [79], where the user partitions the private keys in shares stored in multiple locations, such that if one share is stolen or compromised, the keys are still secure and the user can recover them. Another proposal consists on super-wallets, where the user keeps the main wallet in a secure vault, and then sub-wallets with limited amounts are derived for the smart phone wallet for a daily use [80], minimizing lost or theft damage.

Hosting the private-keys in a third-party centralized service sparks additional risks, as these wallets are the entry point for billions of assets, which become a target for attackers.

To minimize the risk, the key management service can be decentralized, so that users can store their keys among different providers (proxies) that hold re-encryption keys versions of their master keys, as proposed by KMSChain[1] or NyCypher [81]. In these schemas, users perform client-side data-level encryption of the blockchain transaction data, using proxy re-encryption schemes, where proxies are semi-trusted entities that cannot be used to decrypt the data, avoiding centralized key management.

Losing the private keys blocks users to perform transactions with the assets associated with their private key. It might be a real problem not only to spend cryptocurrencies but also to impersonate users in blockchain services. Some blockchain solutions such as Uport [20] or Sovrin [82] deal with this issue by providing recovery and revocation mechanisms for the private keys. It is done by consensus mechanisms that recognize a user legitimacy with regard to the stolen/lost keys associated to his identity.

C. MALICIOUS SMART CONTRACTS

Smart contracts execution can raise vulnerabilities [83], such as, for instance, intellectual property theft. Smart contracts are executed by the validating nodes, and the ledger registers the code, input and outputs. A node could access the data being processed in the transaction compromising user's privacy. In addition, smart contracts are usually compiled to bytecode for the blockchain's virtual machine, e.g. the Ethereum Virtual Machine. Before executing a smart contract, the user should verify that the code of the smart contract actually compiles to the bytecode in the transaction. Smart contract analysis tools, such as Oyente open source tool, can help to perform vulnerability analysis of smart contracts as carried out in [84]. One example of privacy attack is the *odds and evens* betting game as a smart contract [85].

In addition, smart contracts can be run in trusted execution environment such as Intel SGX [86], however it is also subject to security issues [87]. Additional obfuscation methods for running the smart contracts, such as Security Multi-Party Computation (SPMC), are needed to ensure a privacy-preserving solution. In this sense, [88] follows an inter-disciplinary approach based on cryptography and formal verification using SMPC and proof-carrying code to enhance privacy in smart contracts.

D. NON ERASABLE DATA & ON-CHAIN DATA PRIVACY

As described in the previous section, a holistic vision of privacy involves privacy as *Confidentiality* and *Control*. To ensure confidentiality of data held in the blockchain, the data must be encrypted. Moreover, privacy as Control includes the right to erasure, however, the blockchain is immutable, which rises an important challenge. In this regard, hashed personal data provides pseudonymity but not anonymity. Similarly, encrypted personal data is considered

---

[1]KMSChain: Decentralized Key Management Service https://kmschain.com

pseudonymous (i.e. not anonymous). Furthermore, digital identifiers can be considered as personal data and should not be written into the ledger, or at least, there should be a different derived identifier for each interaction. However, nowadays blockchain solutions usually write DID's public keys on blockchain.

Therefore, personal data of any kind including hashes, encrypted personal data and DID should not be stored on-chain, ensuring the right of erasure in compliance with GDPR [7]. GDPR is not applicable to data that is fully anonymous, therefore, it is recommended to either, fully anonymize data or store personal data off-chain. It can be achieved, for instance, using InterPlanetary File System (IPFS) protocol, including on-chain only a link to the data along with a timestamp and a (preferably randomized) hash of the outsourced data for verification. It enables data removal and make the on-chain reference useless after deletion off-chain.

Nonetheless, some researches suggest mechanisms to enable erasure in blockchain, such as [89], which presents a block matrix data structure for integrity protection with erasure capability. It allows continuous addition of hash-linked records by enabling, at the same time, deletion of records. Likewise, in this regard, [90] presented Lition, a public blockchain that allows storage and deletion of private data. However, it requires setting trusted knowledge groups of nodes to manage the blockchain, that need to commit (e.g. through legal agreement) to not store real data hashes, and delete the data upon user request (without maintaining back-up copies).

E. POST-QUANTUM COMPUTING RESISTANCE

With the upcoming Quantum Computing, some proof-of-work algorithms and signatures are under risk [91]. Quantum algorithms like Shor's, could break in the future the log of elliptic curves public-key cryptography (ECDSA) or the large integer factorization problem (RSA) needed to generate a signature, which are the baseline of several crypto-protocols used in blockchains (e.g. in bitcoin). To mitigate this issue, hashes should not be stored on-chain without a previous randomization process. In addition, some blockchain research solutions [92], and platforms such as Tangle [93] or Wanchain [19] employ crypto-algorithms resistant to quantum computing.

F. CRYPTO-PRIVACY PERFORMANCE

Cryptographic mechanisms, such as ZKP [94] and ZK-SNARKS [95], are needed to ensure full anonymity in blockchain. However, most of ZKPs solutions are not efficient enough for large scale and responsive scenarios, as they require computational time to generate and validate proofs. Novel proposals based on Non-interactive zero-knowledge proofs of knowledge (NIZKPoKs) such as [96], which uses shorter proofs than traditional ZKP to enhance performance, or [97], which uses symmetric-key primitives, are employed to mitigate the computational problems raised with traditional ZKPs. In this sense, Section IV analyzes the main

advantages/disadvantages of main crypto-privacy techniques applicable to blockchain.

G. PRIVACY-USABILITY

The challenges associated to usability can be grouped according to two different aspects:

- *Privacy-aware development:* the development of smart contracts on blockchain should be agnostic to the underlying privacy-preserving mechanisms, otherwise, naive non-experienced developers would struggle to implement and enforce properly the privacy-preserving techniques in the decentralized environment. Therefore, an abstraction layer needs to be developed in blockchain architectures for the sake of developer-friendly smart contracts implementation, while reducing to the minimum latency introduced by such an privacy-preserving layer.
- *User-friendly Privacy management*: non-technical people will find difficulties to deal with the key management required in new SSI IdM systems in blockchains, specially during the key recovery process. In addition, configuring and selecting the personal attributes to be included in a claim - to meet the requirements imposed by the service provider (i.e. verifier) - might be also cumbersome and not privacy-friendly. Thus, protocols/specifications and their corresponding appealing front-end apps for blockchain are needed to automate the data release/consent/selection of blockchain verifiable claims [58] and management of DID Documents and data [57], and in general, to deal with end-user privacy management.

H. MALICIOUS-CURIOUS TTPS

In permissioned blockchains, the SSI IdM system deployed on the blockchain will be in charge of performing (or managing its outsourcing) the user ID proving (authentication and validation of the real user identity), and then, the issuance of DID Documents and attribute-based credentials to the users. In addition, the SSI IdM will be also in charge of validating the issued verifiable credentials and crypto-claims. This implies that the blockchain platform itself acting as issuer and verifier of credentials must be trusted and their code and procedures auditable and transparent. Otherwise, the blockchain platform might become a point of failure and compromise user's privacy. Indeed, the inspection capabilities envisaged in certain SSI IdMs that will allow de-anonymize and reveal the user real identity behind a pseudonym, in case of inspection grounds are met (e.g. as demanded by Law Enforcement Authorities in case of cyber-crime), might become a point of attacks and vulnerabilities.

I. PRIVACY ENFORCEMENT IN CONSTRAINED SYSTEMS

The Internet of Things (IoT) can benefit from blockchains deployments in many different ways, such as, for instance to achieve data provenance. In some IoT deployments, devices

will need to interact directly with the blockchain to carry out different kinds of transactions, e.g. to report certain sensed data or operations to achieve data provenance. However, due to their constrained capabilities in terms of hardware (memory, battery, processor), this kind of devices might have difficulties to accomplish certain blockchain-related operations. These operations encompass storing securely in the device the private crypto-keys associated to the IoT device, maintaining credentials and claims, holding and implementing the owner privacy policies and preferences, running key management protocols, and in general, performing operations to write and read in the blockchain in a privacy-preserving manner.

J. PRIVACY INTEROPERABILITY ACROSS DIFFERENT BLOCKCHAIN-ENABLED SCENARIOS

As it will be shown in Section V, blockchain is being applied in different kind of scenarios such as e-Admnistration [6] or Smart cities [3], which demand diverse privacy requirements. They can include full anonymity support (e.g. ZKPs), usage of Mixers, authentication and ID proofing support, mobile wallets, inspection and de-anonymization capabilities, smart contracts support, constrained environments requirements (e.g. IoT or Cyber-physical Systems (CPS)). This situation is leading to a fragmentation and diverse blockchain implementations that are not interoperable, and therefore, difficult to integrate between each other. In this regard, the W3C is standardizing some of the privacy-preserving building blocks, including privacy-related data models and techniques, such as Verifiable Claims [58] and Decentralized Identifiers (DID) [57]. Indeed, current blockchain implementations such as uPort [20] or Sovrin [82] are starting or planning to adopt these standards.

K. COMPLIANCE WITH PRIVACY AND DATA PROTECTION REGULATIONS

The existence of regulations, such as the General Data Protection Regulation (GDPR) [7], which empowers citizens with the rights to have their data rectified, erased or forgotten may come into conflict with Blockchain technology, since the chain should be immutable, persistent and unmodifiable. Blockchain solutions should comply with these regulations while giving guarantees to the user that his privacy is preserved.

GDPR [7] aims to avoid the collection (and processing) of personal data that is not reasonably essential to achieve the intended purpose, ensuring privacy-by-design and by-default. Different rights including, right to be informed, right to withdraw consent, direct access to data, correct-rectify data, forget, portable data, right to be informed on data breaches, need to be satisfied also in blockchain.

The GDPR's article 5 defines 6 clauses corresponding to 6 principles regarding processing personal data:

1) **Lawfulness, fairness and transparency:** processed lawfully, fairly and in a transparent manner in relation to the data subject. Transparency: informing the subject about the kind of data processing to be done.

Fair: the data processing must correspond to what has been described. Lawful: Processing must meet the tests described in GDPR.

2) **Purpose limitations**: personal data can only be obtained for "specified, explicit and legitimate purposes". Data cannot further processed in a manner that is incompatible with those purposes without further consent.

3) **Data minimisation**: data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

4) **Accuracy:** data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

5) **Storage limitations:** personal data is "kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed", that is, data no longer required should be removed. This clause is of paramount importance with regard to blockchain as highlighted in section 3.6 about "non erasable data".

6) **Integrity and confidentiality:** requires that data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

At the time of writing this paper, the European Union Blockchain Observatory has published a report about blockchain and the GDPR [98], where they identified and analyzed three main issues with regard to the Blockchain's compliance of GDPR. Firstly, there exist issues with the identification and obligations of data controllers (determines the purposes of personal data processing) and processors (deal with personal data on behalf of the controller), since when data subjects write directly data on blockchain, data controllers are difficult to identify. Secondly, there are issues with the anonymisation of personal data, since hashes of personal data and encrypted data used in common blockchains can not be considered anonymization (and therefore they falls into GDPR). Thirdly, there are difficulties in blockchain to exercise of some data subject rights, specially when it comes to the support given by blockchains to rectify or remove data, as we remarked previously.

Besides, public and permissionless blockchains entail significant GDPR compliance challenges than permissioned blockchains, because of its fully decentralized and openness conditions. Section V-F analyzes the most important blockchain platforms and how they address these GDPR principles.

In addition to privacy challenges, when it comes to security issues, vulnerabilities and attacks in cryptocurrencies, the reader is referred to the survey paper [29], where authors

TABLE 1. Main privacy cryptographic solutions for blockchain, and their main properties.

Cryptographic scheme	Blockchain application	Trusted Third Party	Succinct	Transparent	Zero-Knowledge	Transaction's privacy	Proof of execution	Maturity
Commitment Scheme [100]	[16], [17]	No	*	*	*	Yes*	No	High
SMPC [26]	[19]	No	*	*	*	Yes*	No	Medium
ZKP [101]	[16], [82]	No	*	*	Yes	Yes	Yes	High
Homomorphic Hiding [102]	[30]	No	*	*	*	No	No	High
zkSNARK [103], [104]	[25]	Setup Phase	Yes	No	Yes	Yes	Yes	High
STARK [105], [106]	[107]	No	Yes	Yes	Yes	Yes	Yes	Low
Group Signatures [108]		Group manager	*	*	*	No	No	High
Ring Signatures [109]	[28], [72], [110], [111]	No	*	*	*	Yes	No	High

summarize the major security attacks on bitcoin (e.g. Double spending, Finney attack, Brute force attack, Block discarding, 50% hash power,...) and the bitcoin network (e.g. bribery attacks, refund attacks, DDoS, Sybil, Tampering, Routing attacks,...), as well as their corresponding countermeasures.

IV. REVIEW OF PRIVACY-PRESERVING SOLUTIONS FOR BLOCKCHAIN

This section presents the main privacy-preserving techniques that can be applied in blockchain to deal with privacy for supporting transactions anonymity and privacy control (Section IV-A), enhancing data anonymization (Section IV-B), and support data confidentiality (Section IV-C).

A. MAIN PRIVACY-PRESERVING APPROACHES IN BLOCKCHAIN

This section introduces the main technologies and crypto-solutions that can be used as baseline to enable privacy preservation in blockchain, including Secure multi-party computation (SMPC), Zero-Knowledge Proofs (ZKP), Commitment schemes, zkSNARK, Ring Signatures and Homomorphic hiding. Table 1 summarizes the cryptographic privacy solutions that are explained in the following subsections.

1) SECURE MULTI-PARTY COMPUTATION (SMPC)

Secure multi-party computation (SMPC) [26] splits data or program states (e.g., states of blockchain's smart contract) between N parties using secret sharing. M parties of N are needed to cooperate and jointly perform distributed computation of a certain input, in order to generate the output and also to reveal data or program states. Each party only receives part of the input, and maintain a point on a different polynomial to identify a variable that sets up a part of the data.

This method requires the majority of participants to be honest. Besides, it is difficult for participants to demonstrate their work as part of the MPC, meaning that incentives to participants are difficult to manage. This makes MPC more suitable for permissioned/private blockchains. In addition, SMPC introduces network latency as nodes require exchanging data to compute the MPC. Actual SMPC approaches are

starting to be used in production along with Homomorphic Encryption (HE), Garbled circuit (GC), linear secret sharing (LSS) and oblivious RAM constructions [99].

In blockchain, SMPC can be used for splitting the smart-contract execution as well as account and key management without requiring any third-party participation, as proposed in [19], a ledger aimed to enable the exchange of digital assets among different blockchain networks. In this case, *storeman* nodes (groups of entities) keep part of the private keys of a source chain account, and manage a smart contract that locks the asset on the original chain, avoiding that a node can access to the full private key of such as original account.

2) ZERO-KNOWLEDGE PROOFS

A Zero-Knowledge Proof (ZKP) [101] is a cryptographic protocol that allows a party, the *prover*, to prove to another entity, the *verifier*, that a given statement is true, without revealing any information except that the proof itself is correct. For example, the statement of knowing a secret value is proved with a *Zero-Knowledge Proof of Knowledge*, where the secret value is kept private to the prover even after the ZKP is performed. For an in-depth understanding of the mathematical principles of ZKPs, we recommend reading [94].

The three requisites for a protocol to be a ZKP are:

- *Completeness*: If the statement to be proved is *true*, the prover can always carry out a successful proof.
- *Soundness*: If the statement to be proved is *false*, a cheating prover cannot convince the verifier that it is true, except for a small probability.
- *Zero-Knowledge*: There exists a polynomial-time bound algorithm that can generate on its own transcriptions of the protocol, that are indistinguishable from a successful proof between a prover and a verifier. This algorithm is called the *simulator*. It is Zero-Knowledge because if a third party (which does not know if the statement is true or false) can generate a valid transcript of the protocol, then neither the verifier nor an eavesdropper could obtain any extra information from a real transcript.

Because a ZKP is an interactive protocol, the applicability is limited to scenarios where a prover and verifier are synchronized. The Fiat-Shamir heuristic [112] solves

this problem using the random oracle model; in practice, the prover generates a proof replacing the verifier with a hash function.

Theoretically, the so-called *perfect* ZKPs assume that the prover is computationally unbounded, and the ensembles of the real transcriptions and the simulated transcriptions are identical. With less restrictive assumptions, there exist variations, such as *statistical* ZKPs or *computational* ZKPs, which relax the indistinguishability of ensembles, or *honest-verifier* ZKPs that apply restrictions over the verifier.

ZKPs are applied in different ways over the blockchain, either to validate transactions or to provide privacy to the data in the blockchain:

- ZKP based cryptocurrencies: Zerocoin
  Zerocoin [16] introduced *zero-knowledge proofs of set membership* as a privacy solution to Bitcoin's pseudonymity. They use ZKPs to solve the double spending problem without revealing the transaction associated to the funds. First, the prover, owner of the money, previously committed the funds with a secure digital commitment scheme. The funds correspond to a serial number S, and the commitment opens with a random r, both kept secret. When the prover wants to transfer the funds, it accumulates multiple commitments from the blockchain history, and proves that she knows the secret r such that one of the commitments opens to the value S. This proof doesn't reveal neither the secret r, nor which commitment of the chosen set was opened. This is called a *zero-knowledge proof of set membership*. In the transaction, the ZKP hides the origin of the funds, hindering linkability, and the revealed serial number S prevents the double spending, as every node keeps track of spent transactions as revealed serial numbers.

- ZKP based Anonymous Credential Systems on blockchain
  Another application of ZKP in the blockchain are the Anonymous Credential Systems (ACS) [39]. In this case, the blockchain acts as a decentralized PKI, where the credentials' public information is stored. These credentials allow off-ledger interactions between a prover and a verifier, such that the verifier can check on the ledger the validity of the *issuer*'s signature. Some ledgers such as Hyperledger Indy [2] has advanced privacy features including the use of decentralized identifiers (DIDs) [57], which represent globally unique and resolvable identifiers (via a ledger) that do not require any centralized resolution authority to enable the creation of secure 1:1 relationships between any two entities. DIDs make use of authentication encryption, ZKPs and a separation between credentials and proofs. ZKP over these credentials allow the prover the creation of unlinkable pseudonyms, a selective disclosure of attributes, or proving that a certain value meets

a specified range. The management of credentials is a key aspect in this type of ledgers; for this reason, the credentials are never stored on the blockchain to keep the prover's attributes secure. The issuer's public keys are stored on the ledger, so the credentials can be verified and trusted. Because in this type of blockchain the application of ZKP does not affect the validity of a transaction, the trust over an issuer depends on the reputation a verifier gives it. The reputation could be calculated with other data on the blockchain or with real world, off-chain information, in the same way a web browser trusts the CA certificates pre-installed within it.

A recent survey of non-interactive zero knowledge proof systems and their applications is presented in [113]. Since then, novel proposals [97] on Non-interactive Zero-Knowledge Proofs of Knowledge (NIZKPoKs) are appearing to mitigate computational inconveniences of ZKP. Furthermore, [114] is intended to target post-quantum era using efficient symmetric-key primitives and SMPC.

3) COMMITMENT SCHEMES

A commitment scheme [100] is a cryptographic tool for a party, *Alice*, to hide a secret value, but at the same time binding Alice to such value so when she shows the original value to *Bob*, he can verify if Alice is lying, therefore Alice commits to a secret value without unveiling it. In this direction, [115] showed that any ZKP can be constructed with commitment schemes. But they are used not only for ZKPs, but also in distributed computations as coin-flipping protocols, or in blockchains to hide a transaction's value, binding the owner to the real secret attributes, e.g. Zerocoin [16] or Zcash [17].

Furthermore, a commitment scheme can be based on, either unconditionally binding (Alice cannot open the commitment value to a different value than the original one) or unconditionally hiding (Bob cannot guess to what value Alice committed) [94]. A commitment scheme is therefore at most computationally hiding or binding, meaning that they are secure only to polynomial bounded machines. In blockchain this property is crucial, as the design must address whether to protect the private value stored in the immutable chain (unconditional hiding), or to protect the ledger from possible future attackers (unconditional binding).

4) zkSNARK

zkSNARK (*zero-knowledge Succinct Non-Interactive ARgument of Knowledge*) [95] is similar to ZKP, but their construction offers more possibilities that the blockchain technology [103], [104].

Like with ZKPs, there are a prover and a verifier, and the prover wants to convince the verifier about a statement, in this case, that she executed a given program. The verifier will trust that the prover executed it properly, without executing the code again to compare outputs. The acronym reveals the properties of a zkSNARK:

- They are *zero-knowledge*, meaning that the verifier learns nothing from the proof, except that it is valid.

---

[2]Hyperledger Indy: https://www.hyperledger.org/projects/hyperledger-indy

- They are *succinct*, in a way that the verification can be performed in a short lapse of time, and the proof can be stored in a relatively small number of bytes.
- They are *Non-Interactive*, so the prover and verifier do not need to communicate synchronously, it's only needed a message from the prover, the proof, which any verifier can validate off-line. This is also called the "public verifier" property, very useful in blockchain.
- They are *ARguments*, unlike the *proofs* from ZKPs. In a ZKP, a prover can be considered computationally unbounded. In an argument, the prover is limited in polynomial time. This means that an argument has only *computational soundness*, instead of *perfect soundness*. The *completeness* property is the same as in ZKP.
- They are *of Knowledge*, forcing the prover to know a *witness* or secret value in order to be able to construct the argument. This witness may be the same as in the NP class of problems, for example the prover knows the discrete logarithm to a public value and proofs that she knows said logarithm.

The importance of zkSNARKs is that they can be used to prove the correct computation of any function, in other words, there exists a zkSNARK that produces a valid proof of the function being properly executed. In blockchain, the node that wants to change the state of the ledger, that is, perform a transaction, can keep secret the function to run (Script or Smart Contract code) and the input parameters. Instead of unveiling those parameters, the node can upload a zkSNARK to proof that he performed the correct calculation, and the rest of the peers will trust him. The succinctness makes the proof suitable to be stored in a transaction, and the verification speed allows any other node to verify efficiently the proof.

zkSNARKs are applied in blockchain in Zerocash [25] and Zcash [17], blockchain-based token systems, also known as cryptocurrencies. The problem any cryptocurrency must address is the double spending of tokens. To achieve privacy-preservation and solve the double spending problem, the mentioned systems apply zkSNARKs to the creation of transactions. A user who transfers tokens from existing transactions to another user must create a proof that the transaction is valid. Instead of every validator node checking the transactions themselves like in Bitcoin, they verify an argument of the prover having checked the input and output amounts, and that the private keys correspond to the spending input transactions. Zcash also uses a commitment scheme based on hash commitments and nullifiers, together with ZKP, to track already spent transactions.

Nonetheless, zkSNARKs have two major disadvantages. The first one is the need of a trusted setup phase to generate a *common reference string* (CSR), public cryptographic values known by the verifiers and provers, but generated by the verifier from secret values which must be deleted. This means that during the setup phase a set of random values are chosen, hidden in a specific way, and then deleted by the verifier. In blockchain, is translated to a first secret trusted setup phase. At the beginning of the blockchain life, a trusted set of peers generate the CSR once, deleting the secret values, and then the rest of the blockchains lifetime works with the CSR only. It is important that this setup process is reliable in order to trust any proof based on the CSR.

The second disadvantage is the implementation efficiency of zkSNARKs regarding Smart Contracts. As stated in [116], an Ethereum Smart Contract implementation of arbitrary zkSNARKs would consume roughly all *gas* tokens in the chain, to pay the validator node that successfully runs the consensus protocol (mining).

Because of these two issues, the trusted setup one goes against the blockchain principle of not trusting any other nodes in the network. The research area around SNARKs aims to add the property of *transparency* to these succinct arguments. A protocol is transparent in case the setup and verifier queries are *public* random coins, that is, they don't depend on secret values that must be deleted for the security of the system [106], [117]. In this direction, [118] proposed a multi-party protocol for constructing the public parameters of the Pinocchio zk-SNARK [95], which is the baseline for Zcash [17].

Due to the popularity of SNARKs, the protocols with the transparency property are called STARKs, Succinct *Transparent* ARguments of Knowledge [105]. The origin of STARKs relates to the research of Scalable Computational Integrity and Privacy (SCIP) [119]. It is still a work in progress that promises post-quantum security, ZK, succinctness, scalability, etc. zk-STARKS are more scalable that zkSNARKS, faster proofs generation, and there is no need for trusted set up, as needed in zkSNARKS. zk-STARKS is being implemented in Asure scalable blockchain [107].

5) HOMOMORPHIC HIDING

Another method to share and perform operations over data without revealing private values is homomorphic encryption [102], originates from privacy homomorphism proposed by [120], where the encryption function has some properties that allow to operate over the ciphertext and obtain the same encrypted result, as if such operations had been performed over the cleartext, and then ciphered with the same encryption function.

One of the clearest examples of homomorphic hiding is the RSA encryption scheme. Given a public key (e, n) and private key (d), i.e. integers that check the equalities $n = p \cdot q$ with p and q prime and $d \cdot e \equiv 1 \mod \phi(n)$. The encryption of a message x is given by $E(x) \equiv x^e \mod n$. The group multiplication is then a homomorphic property of the RSA encryption: $E(x)E(y) = x^e y^e \equiv (xy)^e \mod n = E(xy)$.

Homomorphic hiding is one of the fundamental tools to create zkSNARKs, and private distributed computations in general, which is the scheme of prover-validator seen in blockchain.

Another direct use of homomorphic encryption in blockchain are Bitcoin ECDSA key pairs, which have additive and multiplicative homomorphic properties. A key pair

(a, A), respectively the private and public values, and another pair (b, B) can create a third valid Bitcoin address by adding the keys as $(a+b, A+B)$, giving grounds to *vanity* addresses, where Bob sells his address (b, B) to Alice by making public B, b and $A + B$, stating that only who knows the private key $a + b$ (only computable by Alice via a) can spend the coin. This way, Bob can sell its address to Alice, without having to protect any delivery of the private key b.

6) RING SIGNATURES

Given a group of members with private and public keys, ring signature [109] is a type of digital signature performed by one of the members of the group, but the signature itself does not reveal who signed it. The name comes from the shape representing the signature, not the algebraic structure. Preceding Ring Signatures, Group Signatures were introduced in 1991 [108]. Group Signatures specify a *Group manager* entity, which defines the set of users in a group and is capable of de-anonymizing any signature. Nonetheless, with a Ring Signature scheme, any user can create a custom set of users and sign a message without any other entity disclosing the real signer.

The mathematical idea behind the ring signature is that there exists a function that can be computed with only the public keys (verification), but knowing a private key allows to choose a value that makes the function output a desired specific value (signature). The signature process consists on a applying the function recursively to the previous calculated value plus a random seed, starting with a random *glue* value v; with the help of the private key, one of those random seeds is overwritten with a specific value, with the objective that the final computed value of the function is equal to v, closing the "ring".

Given the set of public and private key pairs of the members, $(P_1, S_1), \ldots, (P_n, S_n)$, one can compute the signature over the message m with only the input $(m, S_i, P_1, \ldots, P_n)$, where the only private key needed is one from any of the group. But to verify the signature it is only needed the public keys from all members.

Anyone can verify that a ring signature is valid given the public keys and seeds used in the computation, checking that the first value v equals the last computed value. But it is unfeasible to tell which "link" of the ring used the private key to choose its seed.

There exists an extension called *linkable ring signatures* [121], where given two signatures computed with the same private key, that fact can be detected, but not which key, there also exist other variations, like *threshold ring signatures* [122], where t out of n private keys are needed for a valid signature, etc.

In Blockchain ring signatures are applied to conceal the sender's identity, using several public keys at random from previous transactions in the chain, without the need of a special node that actively participates in the transaction to add privacy. Equivalent to the Zero-Knowledge statement of "I possess the private key of this public key", signing a transaction means "I possess at least one private key from this set of public keys". To protect the recipient node's identity, after each transaction a new public key is generated, and using a key-exchange algorithm like Diffie-Hellman's, the recipient is the only who can recover the private key. Thanks to the linkability property of some linkable ring signatures [123], the double spending can be detected, e.g. for detecting more than one vote in e-Voting, while still not revealing nothing about the signer (only that the signer is one of the users of the group). Example blockchain applications are CryptoNote [28] used in cryptocurrencies such as Bytecoin [3] or Monero [72]. Monero is based on CryptoNote and focuses on achieving strong privacy and anonymity by employing ring signatures for sender privacy, Ring Confidential Transactions [124] for amount obfuscation, and Stealth Addresses [125] for recipient privacy. Recently, Sun et al. propose RingCT [111], a linkable ring signature protocol for Monero cryptocurrency, that have the size of signature and transactions independent from the number of groups.

B. DATA ANONYMIZATION METHODS

1) MIXING

To anonymize email usage, [126] introduced the mixing methods in 1981. Since then, these techniques are used to anonymize different services with multiple users. The core procedure is to coordinate a sufficiently big set of users, which group together all their messages delaying them, and then resend them at the same time or in a randomized order. With the aggregation and delay of messages, there is no possible correlation between the user action of creating the message and the message traveling the network. This technique does not address any personally identifiable information (PII) that the message could have, only the timing correlation of the message in the network.

In blockchain, mixing techniques are used to conceal the history of a particular token. In Bitcoin, users can create one time accounts in the form of a public-key pair per transaction, instead of reusing previous ones, but the history of a transaction can link those previous addresses to the new ones, and when multiple input addresses are used, then all are correlated to be from the same owner. The use of a mixing technique un-correlates the addresses in the transaction's history.

Mixing services (e.g., [22] or [70]) are anonymous service providers that divide users' funds into smaller parts; then, these parts are randomly mixed to make users and transactions unlinkable. Users can mix their coins to generate one mixing transaction based on the users' addresses, in such a way that users are still able to verify that the correct amount of coins is sent to their output addresses.

Mixing protocols such as CoinJoin [70], Ring Signature blockchains like Monero [72] and Zero-Knowledge blockchains like Zerocoin [16], all hinder the token's history, making the owner's addresses uncorrelatable by hiding them in a set of possible owners. Mixing protocols depend on the

---

[3]Bytecoin https://bytecoin.org

coordination of the users, usually relying on a TTP server to perform the mixing. Meanwhile Zero-Knowledge and ring Signature blockchains can be applied by the user alone, without the need of other entities interacting. Nonetheless, the mixing protocols are applicable over existing blockchains like Bitcoin, while the cryptographic solutions require a new blockchain instantiation, with bigger transactions due to the size of the proofs or signatures.

2) DIFFERENTIAL PRIVACY

Differential privacy [127] deals with privacy-preservation by studying whether a data analysis methodology reveals or not information about an individual.

It consists on introducing a certain amount of random noise to data queries, in a way that any statistical analysis over the whole set is significantly close to the real results, but inference over any individual is infeasible.

In blockchain, Differential privacy is applicable for accessing private databases via queries that aggregate the data, and also to receive the individual data with statistical variations from the sources while reducing the PII collected from individuals. The first database scenario is applicable for private blockchains that allow third parties to use their anonymized data. The second case is applicable to log or sensor's data collecting blockchains, where the whole chain can be used for statistical analysis, but a single transaction has statistically shifted data.

Nonetheless, using differential privacy, data cannot be fully anonymized while being useful for analysis; it is a trade-off between utility and privacy. Certain differential privacy techniques achieve a certain degree of privacy, measured with the definition's constant ϵ, and the number of queries performed over time.

Differential privacy is being applied to blockchain to protect user's privacy in different scenarios. For instance, in [128] authors employ Differential privacy to avoid an adversary can infer sensitive personal information when performing federated learning, using the blockchain to record crowdsourcing activities.

C. DATA PROTECTION METHODS

Blockchain is immutable due to their linked list of hash pointers structure, where a deleted or modified transaction or block would change the block's hash pointer, invalidating all the following transactions integrity. This goes against privacy preserving principles and regulations like the GDPR.

The data running on the blockchain can be protected through different encryption methods, thereby achieving confidentiality and therefore, a holistic vision of privacy. It is especially relevant in scenarios such as eHealth were data are particularly sensitive.

Depending on the consumers of the encrypted data, different encryption and storage methods can be applied. With traditional symmetric or asymmetric encryption, the creator of the data would upload the encrypted transaction and then distribute the decryption key off-ledger, or using an instantiation

of a decentralized PKI over the blockchain like in Sovrin [82] to manage public keys.

Other approaches to sharing ciphered data between multiple peers in the chain are focused on allowing a set of nodes to be authorized to decrypt the data based on attributes. In this sense, Key-Policy Attribute-Based Encryption (KP-ABE) [129] or Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [130], which allows to define access control policies in the encryption itself, allows that only the users with the right attributes can decrypt the data. Therefore, a user could upload an attribute based encrypted document to the ledger, the nodes can check the encryption policy, and if they have the right attributes, they will be able to consume the transaction's data.

Another approach is called Secret Sharing, created independently by authors of [131] and [132]. It allows to split a document in N different pieces, give one share to N different nodes, and only if t out of those N nodes cooperate, or one node obtains t out of N shares of the pieced document, the original document can be reconstructed. This is also called a (t, N)-threshold scheme. One idea behind the ability to partition and reconstruct a document comes from the fact that two points define a unique line. Given the document, partition it as two points in the plane, create a line and give one random point of the line to each of the N nodes. Every pair of cooperating nodes can reconstruct the line and obtain the original document. This is a $(2, N)$-threshold scheme. To allow for a higher threshold, it suffices to use a polynomial instead of a line, with degree $t - 1$. With t different points, interpolation returns the original polynomial representing the shattered document. The case where $t = 1$ is equivalent to replicate the data across all N storing nodes.

Nonetheless, the size of ciphered data may make the blockchain instance to grow too much in size and the immutability of the chain may entail future privacy issues if the deciphering keys are stolen or broken. The alternative is to store large ciphered data in decentralized off-ledger databases, like IPFS [133], and include as a transaction the unique resource identifier and its hash to obtain integrity of the data and proof of existence. Incentivized decentralized storage [134]–[138] can be integrated with blockchain by paying blockchain tokens to the honest storage nodes, applying privacy measures to protect the data, and hashes in the transactions for integrity.

Depending on the blockchain's application, certain transactions might only serve to check the hash integrity of the chain, e.g. past transactions already spent, or may include private information that the user desires to delete from the chain. To address this problem, there are proposals to change the blockchain data structures to allow deletion of a transaction, without affecting the hash integrity validation of the chain [89], [139]. It changes the immutability property of a blockchain by the integrity, as the hash validation would still work, and the deletion of a transaction is accepted by the consensus rules of the network. Nevertheless, the privacy issue is not assured to be solved. The data is replicated in
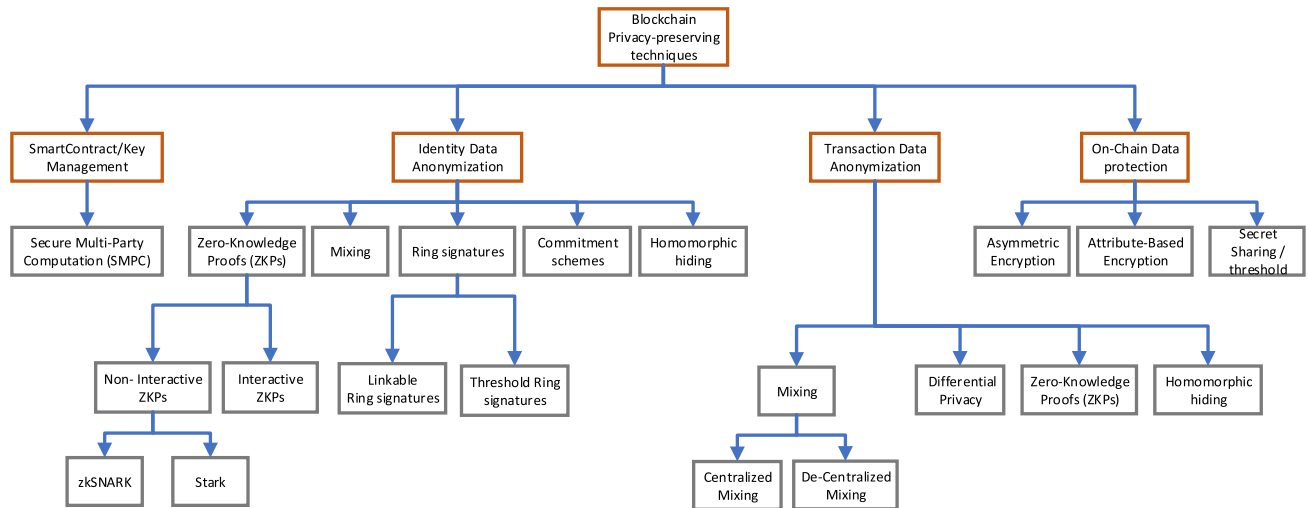
every blockchain node, and some nodes may still store it after a deletion in the chain.

D. PRIVACY-PRESERVING MECHANISMS ANALYSIS

The privacy-preserving techniques described previously can be categorized in 4 main areas according to their main privacy-preservation purpose. The resultant taxonomy of privacy-preserving techniques in blockchain is shown in figure 4. The four categories and the techniques can be summarized as follows: 1) Privacy-preservation of *Smart Contracts and Key Management* derivation, by using SMPC techniques. 2) *Identity Data Anonymization* category that groups the techniques employed to conceal the user identity in transactions, including ZKP, Mixing (to conceal the payee, payer), Ring Signatures (anonymize signer), Commitment Schemes and Homomorphic Hiding (e.g. for coins addresses exchange). 3) The *Transaction Data anonymization* embraces those privacy-preserving techniques intended to protect privacy of the contents of the blockchain transactions. It includes techniques such as Mixing (e.g. anonymizations of traded coins), Differential privacy, ZKPs, Homomorphic Hiding (transactions amount hiding). 4) *On-chain Data protection*, that groups those techniques aimed to protect the data on-blockchain through encryption mechanisms, including Asymmetric Encryption, Attribute-Based Encryption and Secret Sharing. It should be noted that some privacy-preserving techniques such as ZKPs and Homomorphic Hiding are being applied to achieve anonymization of both, identity data (e.g. payee, payer) and transaction data (e.g. traded coins).

Table 2 summarizes privacy techniques and cryptographic principles applied in blockchain, including their main advantages and disadvantages. Regarding the privacy challenges in blockchain listed in the previous section, these solutions focus mainly on the privacy of transactions correlation and mixing. Multi-entry transactions and transactions with

change that relate multiple addresses to the same user are hidden with the use of commitments and sets of possible owners, using either ZKP over accumulators, Ring Signatures or Mixing protocols. Another solution to this correlation is given by zkSNARKs, where the validator nodes trust in Zero-Knowledge that the transaction creator checked the validity of the transaction, hiding the transaction's information via commitments, but without grouping a set of possible owners.

Regarding the privacy for e-Administration, Anonymous Credential Systems based on ZKP showcase a privacy scenario with trust based on the public keys published in the blockchain.

Although blockchain is not suitable for large amounts of data, it provides integrity and proof of existence for other cloud storage services, centralized or distributed, e.g. IPFS. The use of secret sharing to split a document in multiple pieces, such that you need t out of n to reconstruct it provides privacy, for attacks of utmost $t-1$ colluders, and availability, for utmost $n-t$ unavailable nodes.

Solutions like differential privacy and erasure of transactions deal with the challenges of data protection laws, like GDPR, ensuring the citizen's rights of privacy. Differential privacy is also useful for IoT scenarios in Smart Cities, where the sensor's data can be gathered and statistically shifted without affecting the usefulness for the city. However, due to the distributed nature of blockchain, erasure of transactions is not guaranteed. Encryption enhances the privacy of non-deleted transactions, and Attribute-Based Encryption (ABE) systems allow key distribution based on policies over credentials. Nonetheless, if the blockchain does not allow transaction deletion or a node does not delete the transaction, any encrypted data is still susceptible of different attacks. A relevant aspect related to the inmutable nature of the blockchain is the well-known *garbage in, garbage out* (GIGO) principle, so that corrupted or incorrect data will

TABLE 2. Advantages-disadvantages of privacy mechanisms.

Privacy technique	Description	Advantages	Disadvantages
Commitment Scheme [100]	Hide a value while binding the user to it	Efficient Computational binding and hiding	Unconditional hiding or unconditional binding not both
ZKP [101]	Proof a statement without revealing any private information (zero-knowledge)	Proof any statement in zero-knowledge	Efficiency Size
Homomorphic Hiding	Arithmetic calculations in ciphertext translate to arithmetic in cleartext	Distributed computation with private values	Usually limited homomorphic operations
zkSNARK [103], [104]	Proof in zero-knowledge the correct computation of a given code	Succinct Zero-Knowledge	Trusted Setup Phase Inefficient Smart Contract implementation Attacks from computationally powerful provers poor computational efficiency of the prover
STARK [105], [106]	A zkSNARK without a trusted setup phase	Transparency: No trusted Setup Phase	Low maturity
Ring Signatures [109]	Sign a message with a private key and N public keys to conceal the real signer	Does not depend on trusty third party Variations like threshold signatures Users define custom sets autonomously	Difficult management and coordination of several signer entities.
Mixing [126]	Coordinate a set of users to perform operations while hiding the originator	Works over existing solutions Efficiency	Coordination of multiple users Use of mixing servers
Differential Privacy [127] [128]	Statistically shift data so the accumulated statistical studies are significant, while individual data is irrecoverable	Individual privacy of data Statistical usefulness	Now intrinsically applicable to blockchain
Attribute-Based Encryption [130]	Ciphered data can be deciphered if the user has valid attributes	Policies define authorized users	Credential system to issue attribute certificates
Secret Sharing [131], [132]	A document is partitioned and spread between N parties. Only if t-out-of-N cooperate, the document can be reconstructed	Not all nodes are necessary to recover the document	Collusion attacks
Transaction removal [89], [139]	A transaction is substituted in the chain such that the integrity calculation is valid	Right to delete private data	Deletion not guaranteed Deletion operation must be approved in consensus

also produce an incorrect output. Therefore, it is critical to ensure that the information sent to the blockchain has not been altered or modified, while considering privacy aspects in case of sensitive data. This aspect is particular relevant in the context of cyber-physical systems (CPS), which are usually deployed in uncontrolled environments prone to attacks and misuse. Indeed, with the trend of global connectivity, CPS could be remotely accessed and monitored without the explicit consent of their owner. Therefore, the GIGO principle sets out issues related to the correctness of the data itself, but also regarding the privacy issues that must be properly addressed in different scenarios, such as CPS.

V. PRIVACY-PRESERVING RESEARCH PROPOSALS FOR BLOCKCHAIN SCENARIOS

After describing the main privacy-preserving approaches that can be considered to mitigate privacy issues in blockchain, this section analyzes research proposals and blockchain platforms dealing with such issues in emerging scenarios. In particular, we study the privacy implications of the integration of blockchain into such use cases, and provide some insights derived from this analysis.

Table 3 summarizes the different research proposals according to a certain scenario. In addition to proposals

related to a specific scenario, it should be noted that we also consider *generic* approaches, which cope with privacy issues in blockchain and can be considered in different use cases. In this direction, the adoption of the SSI model through the use of blockchain-based approaches, and the associated privacy issues, have attracted a significant interest in recent years. Based on it, this section is intended to provide a description of recent research proposals addressing such aspects in different scenarios. In this direction, [140] analyzes the application of DLT technologies for identity management, in order to leverage their decentralized, tamper-resistant and inclusive nature. In particular, they analyze UPort [20], ShoCard [141] and Sovrin [82] as some of the main examples of DLT-based IdM approaches. From their analysis, usability and GDPR compliance are highlighted as two main issues to be overcome in the coming years. Privacy aspects of DLT approaches are considered by [142], which proposes a privacy-preserving architecture called ChainAnchor. The approach is based on an identity and privacy-preserving layer on top of the blockchain, so that anyone can read and verify transactions but only verified anonymous identities can have transactions processed. Towards this end, authors make use of ZKP mechanisms of the Enhanced Privacy ID scheme [143]. They call this scheme *semi-permissioned blockchains*.

TABLE 3. Blockchain research proposals addressing privacy aspects.

Research proposal	Year	Scenario	Anonymity	Pseudonymity	Cryptographic technique	Implemented/ Validated	Approach
Anonymous Identities for Permissioned Blockchains [142]	2016	Generic	Yes	Yes	ZKP based on the EPID scheme	No	Use of an RSA-based EPID scheme to build a semi-permissioned blockchain
Towards self-sovereign identity using blockchain technology [144]	2016	Generic	No	Yes	Attribute-based credentials, digital signatures	No	Use of tribute-based credentials in a blockchain-based scenario for a KYC use case
Decentralizing Privacy: Using Blockchain to Protect Personal Data [146]	2015	Generic	Yes	Yes	Secure Multi-party Computation (SMPC)	No	Combination of blockchain and off-blockchain storage to construct a personal data management platform in which the use of SMPC is considered
A Trustless Privacy-Preserving Reputation System [148]	2016	Generic	No	Yes	Blind signatures	No	Use of blind signatures to design a privacy-preserving blockchain-based reputation system
Hawk: The blockchain model of cryptography and privacy-preserving smart contracts [15]	2016	Generic	Yes	Yes	Based on Zerocash and zkSNARK	Yes	Generalization of Zerocash to ensure transactional privacy
ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability [149]	2017	Generic	No	Yes	Hashing functions	Yes	Application of hashing functions to users' identifiers to avoid correlation
Channels: Horizontal Scaling and Confidentiality on Permissioned Blockchains [150]	2018	Generic	No	Yes	ZKPs are considered and obfuscation through merkle trees	No	Extension of the *channel* concept from Hyperledger [228] for confidential transactions
Private Data System Enabling Self-Sovereign Storage Managed by Executable Choreographies [18]	2017	Generic	No	Yes	Public-key cryptography and division of private data into different pieces	No	Conceptual design of a SSI system focused on the enforcement of rules and regulations
Securing user identity and transactions symbiotically: IoT meets blockchain [166]	2017	Smart cities	No	Yes	Public-key cryptography	No	User of different types of certificates to enable selective information disclosure
Cloud-based commissioning of constrained devices using permissioned blockchains [167]	2016	Smart cities	Yes	Yes	ZKP based on the EPID scheme	No	A privacy-preserving EPID-based approach for the commissioning of IoT devices through blockchain
Privacy-preserving Blockchain-based IoT Ecosystem using Attribute-based Encryption [168]	2017	Smart cities	No	No	Attribute-based encryption	No	Use of ABE techniques to protect on-chain data
Providing Privacy, Safety, and Security in IoT-based Transactive Energy Systems Using Distributed Ledgers [172]	2017	Smart cities	No	Yes	Mixing services	No	Application of onion routing and mixing services to an energy trading scenario
Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams [174]	2016	Smart cities	No	Yes	Multi-signatures and encrypted data streams	Yes	A privay-enhancing energy trading systems based on multi-signatures
Blockchain for IoT security and privacy: The case study of a smart home [175]	2017	Smart cities	No	Yes	Public key cryptography	No	Lightweight blockchain-based framework for smart homes based on traditional cryptographic techniques
Fair and Transparent Blockchain-based Tendering Framework - A Step Towards Open Governance [196]	2018	eGovernment	No	Yes	Symmetric and public key cryptography	Yes, on Ethereum	Use of smart contracts to implement an open tendering scheme for eGovernment activities
An E-voting System based on Blockchain and Ring Signature [192]	2017	eGovernment	Yes	Yes	Ring signatures	Yes	Integration of blockchain and ring signatures to develop an e-voting prototype
A smart contract for boardroom voting with maximum voter privacy [195]	2017	eGovernment	Yes	Yes	ZKPs based on Schnorr proof and Fiat-Shamir heuristic	Yes, on Ethereum	Decentralized e-voting approach based on ZKPs
Blockchain Electronic Vote [193]	2015	eGovernment	No	Yes	Multi-signatures	No	A privacy-enhanced e-voting system based on 2-of-3 multisignature addresses.
An anonymous distributed electronic voting system using Zerocoin [194]	2016	eGovernment	Yes	Yes	ZKP based on zerocoin	No	Integration of Zerocoin for a privacy-preserving e-voting system
MediBchain: A blockchain-based Privacy Preserving Platform for Healthcare Data [229]	2017	eHealth	No	Yes	Public key cryptography	No	Use of ECC cryptography to encrypt eHealth data
Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control [208]	2016	eHealth	No	Yes	Secure Multi-Party Computation (SMPC)	No	User-centric architecture for eHealth in which the application of SMPC is considered
Towards Decentralized Accountability and Self-sovereignty in Healthcare Systems [209]	2017	eHealth	No	Yes	Anonymous credential systems (U-Prove)	No	Integration of Intel SGX and U-Prove system for a privacy-enhanced eHealth platform
Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology [211]	2018	eHealth	No	Yes	Homomorphic encryption	No	Use of smart contracts and proxy re-encryption to protect patients' data
BPDS: A blockchain-based Privacy-Preserving Data Sharing for Electronic Medical Records [213]	2018	eHealth	No	Yes	Attribute-Based Encryption (CP-ABE)	No	Off-chain storage of eHealth data that are CP-ABE encrypted
BlocHIE: a Blockchain-based platform for Healthcare Information Exchange [215]	2018	eHealth	No	Yes	Public key cryptography	No	Use of off-chain storage of eHealth data that are encrypted through public-key cryptography
FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data [216]	2018	eHealth	No	Yes	Public key cryptography	No	Use of blockchain cryptography to protect the access to eHealth data
A Decentralized Privacy-Preserving Healthcare Blockchain for IoT [214]	2019	eHealth	yes	yes	Ring signatures	yes	Uses lightweight Ring signatures appropriate for IoT devices to sign data anonymously.
A blockchain-based Liability Attribution Framework for Autonomous Vehicles [156]	2018	C-ITS	No	Yes	PKI and pseudonym certificates	No	A liability attribution model for autonomous vehicles based on PKI and pseudonyms
B-FICA: BlockChain based Framework for Auto-insurance Claim and Adjudication [218]	2018	C-ITS	No	Yes	PKI and pseudonym certificates	Yes	It is an extended version of [156] including evaluation results for a certain use case with automated vehicles
Block4Forensic: an Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles [219]	2018	C-ITS	No	Yes	PKI and pseudonym certificates	No	Use of PKI and pseudonyms in a blockchain-based forensics vehicular framework
Blockchain: a Distributed Solution to Automotive Security and Privacy [221]	2017	C-ITS	No	Yes	PKI, pseudonym certificates and multi-signatures	No	Straightforward application of blockchain to C-ITS through public key cryptography
Blackchain: Scalability for Resource-Constrained Accountable Vehicle-to-X Communications [222]	2017	C-ITS	No	Yes	PKI and pseudonym certificates	No	Use of blockchain for the revocation of misbehaving vehicles
Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains [223]	2017	C-ITS	No	Yes	Public key cryptography and pseudonyms	No	Application of traditional cryptography and different wallet addresses to improve privacy in energy trading for electric vehicles
Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions [224]	2018	C-ITS	No	Yes	Commitment schemes	No	Use of commitment schemes for privacy preservation in energy trading for electric vehicles
CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles [5]	2018	C-ITS	Yes	Yes	Threshold ring signatures and Combined Public Keys (CPK)	No	Integration of advanced cryptographic techniques for a blockchain-based incentive vehicular network
Zone Keys Trust Management in Vehicular Networks based on Blockchains [227]	2019	C-ITS	No	Yes	PKI and pseudonym certificates	No	Use of blockchain to store misbehavior information, in order to drive the generation of pseudonyms certificates valid for a certain zone of the road

Furthermore, [144] also explores the SSI model, through the case study of Know your Customer (KYC) regulation [145]. Based on this, authors design a conceptual architecture in which off-chain storage aspects are considered. A personal data management system is proposed by [146], in which privacy aspects are considered through a blockchain-based access control system with off-chain storage properties.

More focused on the application of smart contracts to deal with privacy aspects, [147] proposes a smart contract

management framework for aggregating on-line identity and reputation information to provide an approach for personal on-line behavioral ratings. Also related to reputation systems, [148] proposed a blockchain-based trustless reputation system, in order to provide raters' anonymity and unlinkability by using blind signatures and random address generation. Then, [15] proposed Hawk, a privacy-preserving decentralized smart contract system where the contractual parties interact with the blockchain using a generalization

of Zerocash [25], as ZKP mechanism. This approach do not store transactions data in clear to guarantee transactional privacy.

In addition to previous works, additional proposals have emerged to cope with privacy issues though the use of blockchain-based approaches. In this direction [149] introduces ProvChain, a blockchain-based data provenance architecture to provide assurance of data operations in a cloud storage application. The data provenance records are associated with hashed user's identifier for privacy preservation so that the blockchain cannot correlate data records associated with a specific user. Furthermore, [150] proposed the use of ZKPs and obfuscated merkle trees for permissioned blockchains, in order to provide transaction confidentiality among peers that belong to different blockchains that are linked to the same services. The SSI model for storage and sharing of private data is also analyzed by [18], which proposes an approach called Private Data System (PDS), so that users have the control over their private data. Furthermore, other proposals for storage services, such as Storj [137], Sia [138] or Filecoin [135] have been recently proposed.

Previous works address privacy considerations in generic blockchain-based scenarios. With the increasing interest of this technology, its application to specific use cases has attracted a significant attention. Below, we describe some of the main proposals associated to the following scenarios:

- **Smart cities**: current cities are being transformed into real smart cities through the integration of IoT technologies and platforms. To realize such vision, smart city services require trustworthy data from a huge number of heterogeneous sources. Consequently, the distributed nature of blockchain, and the guarantee of data immutability and verifiability could serve as a core component of more secure and trustworthy data-driven services, where privacy aspects need to be properly addressed [151], [152].

- **eGovernment**: the scenario of having citizens identities registered in the blockchain adds a new scope where the SSI model could be leveraged to cope with privacy aspects. Indeed, the integration of blockchain technologies into administration services has attracted the interest from governments of different countries, such as Switzerland (based on uPort [20]), Finland (for immigration services) or Estonia, which became the first country to dabble in using blockchain for healthcare on a national scale, and to allow people from anywhere to become a e-resident [153]. The digital identity issued by the Estonian administration enables commercial activities, as well as governmental activities. In this scenario, it is necessary to guarantee citizens' privacy through minimal disclosure approaches when accessing the corresponding services.

- **eHealth**: the application of blockchain technology is intended to be particularly valuable in the context of eHealth services. In particular, the management of personal health records could be significantly improved to provide a more effective and customized healthcare assistance. At the same time, eHealth data are especially sensitive, so they should be properly protected to avoid any potential privacy leakage. One of the main real blockchain-enabled eHealth systems is currently used by the Estonian Government to leverage the advantages of blockchain in terms of decentralization and data immutability [154].

- **C-ITS**: the evolution of current transportation methods into Cooperative Intelligent Transportation Systems (C-ITS) is being driven by the emergence of new wireless technologies. This trend will be strengthened in the coming years through the integration of artificial intelligence techniques to create fully *autonomous vehicles* [155]. To realize such approach, vehicle sensors are envisaged to collect significant data amount of personal information, which could represent a potential privacy threat. In this scenario, blockchain proposals are key to provide a decentralized infrastructure ledger to register the actions performed by such autonomous entities [156].

- **Cryptocurrencies**: through the last years, the most representative blockchain-based scenario is associated to the use of *cryptocurrencies*. With a market value of over \$600 billion,[4] cryptocurrencies represent the future of global payments and remittances, in which Bitcoin [30] accounts for 90% of the total market capitalization.[5] In these scenarios, it is essential to main the privacy of the entities involved in a transaction (i.e., *payer* and *payee*), as well as to hide the amount of coins to be transferred. In this direction, recent approaches such as ZeroCoin [16], CoinJoin [70], Zerocash [25] or Blindcoin [67], will be further discussed below.

In addition to these scenarios, it should be noted that other use cases have been also considered recently for the application of blockchain technology. Some of these proposals are leveraging the integration of blockchain with Artificial Intelligence (AI) techniques, as discussed in [157], which discusses potential scenarios, such as energy or smart agriculture. Also considering AI aspects, but with a different perspective, [158] proposes the use of Ethereum smart contracts to track the provenance of digital contents. In this case, AI techniques are considered as a potential driver for the proliferation of such fake content. Other relevant scenarios of the application of blockchain are represented by manufacturing/supply chain [159] and financial [160] sectors. For the sake of clarity, we focus our analysis on the scenarios of smart cities, eGovernment, eHealth, C-ITS and cryptocurrencies. The following subsections review the current state of the art on privacy-preserving solutions for blockchain according to these scenarios, which are summarized in Table 3.

---

[4]https://www.forbes.com/sites/forbestechcouncil/2018/03/20/cryptocurrencies-and-the-market/#7621d6f530f8

[5]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 52016SC0223&from=EN

In addition, subsection V-F analyses some of the main current privacy-preserving blockchain platforms.

A. SMART CITIES

As already mentioned, smart city scenarios represent an excellent ecosystem where blockchain approaches can be leveraged. However, while privacy aspects need to be addressed, they are usually ignored by recent proposals, as demonstrated by recent works regarding the integration of blockchain for smart cities [161], [162]. Indeed, the survey presented by [41] analyzed the existing privacy-enhancing technologies, and their potential application to smart cities. Based on it, only the work proposed by [146] was intended to deal with privacy aspects based on the use of blockchain. Consequently, this subsection aims to provide a description of recent works addressing privacy considerations in IoT-enabled smart cities where the use of blockchain is considered.

As a core aspect of smart cities, the integration of physical devices through the use of IoT technologies is key to enable the development of data-driven services. Indeed, [163] provides a comprehensive analysis of the potential applications of blockchain in IoT scenarios, as well as a review of potential challenges including privacy aspects. Another recent survey is proposed in [164], which highlights the need to address resource constraints, security/privacy concerns and scalability aspects to realize a blockchain-enabled IoT ecosystem. More focused on privacy issues, different proposals have emerged in recent years. In this direction, [165] designed an approach for the authentication of IoT devices based on the transactions recorded in a blockchain, as well as the privacy implications derived from it. Moreover, [166] proposes a scheme based on a permissioned blockchain to manage embedded systems. The approach is based on a distributed identity management scheme, which is designed on top of the use of different certificates. In particular, privacy is addressed through the use of transaction and enrollment certificates along with proofs of possession. This approach allows to hide information from unauthorized access, and enables a user or device to privately prove the possession of certain attributes in a selective way. Related to the previous approach, [167] describes the *ChainAnchor* architecture to enable a privacy-preserving commissioning of IoT devices, when they are deployed on a certain environment. The architecture makes use of the EPID scheme for ZKP. In the case of [168], authors proposed the integration of blockchain with attribute-based cryptography techniques, so that blockchain data are protected for privacy reasons.

Different use cases are derived from the realization of smart cities. One of the main examples is represented by *energy trading* approaches, which are proposed in the scope of smart energy systems [169]–[171]. In this direction, [172] presented a Privacy-preserving Energy Transactions system (PETra), which enables consumers to trade energy without sacrificing their privacy. To do this, they describe an architecture based on onion routing and mixing services to be implemented by a decentralized protocol, such as CoinShuffle [173]. Furthermore, [174] proposed an energy trading system (PriWatt) using blockchain, multi-signatures and encrypted message streams, enabling peers to anonymously negotiate and perform trading transactions. Authors also conducted a performance analysis of PriWatt, as well as a security analysis based on a set of security and privacy requirements. Moreover, [175] analysed the case study of a smart home, proposing a lightweight blockchain-based framework, in which the Proof of Work (POW) is removed. The approach is based on symmetric cryptography in which smart home devices are indirectly accessible, and managed by one miner that is responsible for handling the communication within and externally to each smart home.

One of the main challenges of the integration of blockchain in IoT-enabled smart cities is related to the adaptation of current blockchain implementations to be accommodated in scenarios with resource-constrained devices [4], [176]. Indeed, blockchain deployments require computationally expensive operations and a significant overhead, which hinder the adoption in the IoT paradigm. This issue has attracted a significant interest in recent years through the definition of more sophisticated blockchain-based architectures (e.g., [177] or [178]). As a blockchain alternative, the *tangle* [93] represents an emerging approach, which is the core concept of the IOTA cryptocurrency specifically designed for IoT [179]. Like in the case of blockchain, the tangle represents a set of transactions that are distributed and stored across a decentralized network of participants. However, the tangle is structured as a Directed Acyclic Graph (DAG) in which vertices represent transactions and edges the approvals. In order to make a transaction in the tangle, two previous transactions must be validated; then, the reward of this is, in turn, the validation of the new transaction, so that financial rewards are not required. At this point, the initial approaches for improving privacy in tangle transactions is the use of mixing techniques [180]. Tangle Mixing [181] is one of these proposals, which makes use of a NTRU public key cryptosystem [182] to anonymize the transactions. The user encrypts the data with the public NTRU key of the Tangle mixer service, and the service generates an encrypted response with the public NTRU key of the user containing the address to make the deposit, and then, the user can reach that address.

Summary and analysis of current trends While the use of blockchain is widely considered as a key enabler for the development of innovative IoT-enabled services [151], nowadays significant challenges hinder this integration. As already mentioned, one of these factors is the computationally expensive operations required by blockchain and the lack of scalability. This is exacerbated with the potentially huge number of IoT devices and components that could be part of a certain blockchain. In this direction, several works have been previously mentioned in which IoT devices are supposed to be part of the blockchain deployment. Another approach is proposed by [183], which describes a memory optimized and flexible blockchain (MOF-BC) in which users can use

multiple keys for different transactions to increase privacy. As already mentioned, the tangle approach is proposed as an alternative solution to blockchain for IoT scenarios. However, in spite of their advantages, the enforcement of privacy aspects in IoT devices could be still a difficult task, as discussed by [184]. While this is a very recent approach, it has already attracted a significant interest. Indeed, the ongoing EU project +CityxChange[6] is focused on smart city scenarios, in which the IOTA foundation aims to use such technology. Even if lightweight approaches can be designed, the integration with privacy-preserving mechanisms adds an additional challenge from the practical perspective. Indeed, the limitations associated to most of common IoT devices that are intended to act as *data sources* in many smart city use cases makes difficult to adopt privacy solutions. Consequently, there could be different scenarios in which a specific device is not able to manage blockchain-based operations. Beyond practical considerations, these devices will often operate on behalf of their owner; consequently, the application of empowerment techniques for end users is crucial to ensure privacy aspects are enforced in the next generation of IoT-enabled smart cities.

B. EGOVERNMENT

Blockchain can bring potential benefits to governments, such as data integrity, transparency, verifiability, decentralization, trust, and control. This can reduce disputes and intermediaries in transactions and lessen cybercrimes and corruption. The adoption of blockchain for eGovernment is discussed by [6], which provides a set of requirements based on technology, organization and environment categories. Furthermore, authors claim the need for the evaluation of blockchain technologies to evaluate their suitability in the public sector. Furthermore, [185] provides a critical perspective about the implications associated with the integration of blockchain into governmental services, as well as different research directions to address them.

From previous works, self-sovereign identities managed in the blockchain can be used as the baseline to foster the privacy-preserving deployment of those innovative e-government services, whereby citizens employ their virtual SSI identities to perform digital transactions of assets in a privacy-respectful way. In this direction, there exist different efforts performed by governments to consider blockchain in their services. For instance, the Public-Private Analytic Exchange Program in U.S. (AEP) analyzed the suitability of blockchain to government applications [186]. Their analysis reported a set of recommendations, and an overview of the current landscape of the use of blockchain around the world. Indeed, many governments are trying to accommodate blockchain technologies to their management processes [187]. In particular, [188] conducts a literature review to identity the major benefits and drawbacks of such integration. Authors describe several initiatives regarding the use of

blockchain for eID services (e.g., Switzerland), immigration services (Finland) or academic certificates (Malta). One of the most representative examples is Estonia,[7] whose initiative relies on a Keyless Signature Infrastructure (KSI) [189] to deliver countless number of e-services. KSI only uses a hash function for verification, by providing a scalable approach with negligible computational, storage and network overhead.[8] In addition, a more exhaustive survey of blockchain governmental initiatives is given by [190], where the author points out the need for privacy-preserving mechanisms, such as ZKP, multi-party computation or homomorphic encryption, in order to accommodate private data in the blockchain.

One of the most well-known eGovernment services that exploits blockchain features is *e-voting*, in which privacy restrictions need to be properly addressed. Indeed, [191] analyses the main shortcomings of blockchain-based e-voting systems including eligibility, consistency verification as well as performance and registration issues. This work reports that current e-voting proposals rise some scalability concerns regarding the number of voters. In this direction, [192] suggests the use of ring signatures and blockchain by developing a software called BlockVotes. Furthermore, [193] proposes multisignatures to deal with privacy aspects by considering a bitcoin infrastructure. Based on Zerocoin [16], [194] designs by analyzing the well-known properties of e-voting systems. A more comprehensive approach is proposed by [195] that implements a system on Ethereum in which each voter is in control of the privacy of their own vote, so that it can be only breached by a full collusion involving all other voters. Ethereum is also considered by [196] to build a verifiable government tendering scheme based on smart contracts and traditional cryptographic schemes.

Summary and analysis of current trends. eGovernment services represent one of the most attractive scenarios for blockchain to improve transparency, trust and efficiency of public administrations. Indeed, a recent European Commission (EC) report [197] analyzes the main benefits that blockchain could provide to eGovernment services, such as reduction of economic costs, time and complexity, as well as the increase of auditability and accountability of citizens' information. Furthermore, the report describes the main initiatives in the EU where the integration of blockchain in public services is addressed. Some of these examples include the use of the Blockcerts open standard [198], which is used by the government of Malta for the verification of academic credentials, or the pension administration system that is used in Netherlands based on different blockchain functionalities, such as distributed registration. These efforts demonstrate the interest in the use of blockchain to enhance eGovernment services, which already leverage this technology. Also in the scope of the EU, some research projects are currently analyzing the realization of eGovernment scenarios using blockchain. For instance, the EU H2020 project

---

[6]http://cityxchange.eu/

[7]https://e-estonia.com/
[8]https://guardtime.com/technology

DECODE (Decentralised Citizens Owned Data Ecosystem) [199] aims to increase trust between citizens, public institutions, and companies, which is essential for a stable, sustainable and collaborative economy. Towards this end, it is intended to provide tools that put individuals in control of their personal data private by using blockchain. Furthermore, the EU H2020 project PRIVILEDGE (Privacy-Enhancing Cryptography in Distributed Ledgers) [200] aims to develop cryptographic protocols enabling privacy, anonymity, for distributed ledgers, covering different aspects of e-government services, such as e-voting, diploma records and others. Other approaches are proposed by [201] and [202] in which blockchain is considered as a potential approach to foster the enforcement of local or EU regulations, such as the GDPR. These initiatives are leveraging the decentralization of blockchain, which is intended to cope with the traditional view of centralized government infrastructures. Nevertheless, privacy aspects need to be further considered to conciliate the requirements from citizens and public services. As already mentioned, a prominent example is represented by e-voting, which clearly requires a privacy-preserving approach for citizens. However, according to the analysis of [197], there is a lack of ongoing projects to cover e-voting and taxation services. This report points out the immaturity of large-scale blockchain deployments as a potential reason of this lack, which is specially relevant for the acceptance of blockchain-enabled eGovernment services.

C. EHEALTH

The application of blockchain foundations has attracted a significant interest in eHealth scenarios. Indeed, the eHealth ecosystem sets out unique privacy-related challenges due to the sensitivity of the data to be stored and shared with different stakeholders. Based on this, [203] provides a systematic review and analysis of current blockchain-based healthcare research works with the aim to come up with potential applications, and to highlight the associated challenges. Furthermore, [204] analyzes the application of blockchain in current healthcare systems, as well as the requirements and challenges to protect Electronic Health Records (EHR) (a.k.a., Electronic Medical Record (EMR)) that can be addressed through such integration. More focused on cloud-based eHealth scenarios, [205] describes the potential application of blockchain to cope with security and privacy aspects. In this case, authors highlight the need of off-chain storage mechanisms, so that medical data could be erased under certain circumstances in order to comply with privacy laws (e.g., the GDPR's Article 17 "Right to erasure ('right to be forgotten')". This aspect is also considered by [206] to remove fraudulent transactions in time by using a polynomial-based blockchain structure and a Lagrange interpolation method for efficiency reasons.

In particular, regarding the application of blockchain to address privacy aspects, [207] provides a blockchain-based approach to protect EHR in which patients' data are encrypted through ECC cryptographic primitives. Based on

more advance cryptographic mechanisms, [208] proposes a user-centric architecture called Healthcare Data Gateway (HDG) to enable patients to own, control and share their own health data. Furthermore, they point out SMPC as a promising approach for operating over health data, while privacy aspects can be preserved. Also, [209] analyzes the application of SSI to eHealth scenarios through the integration of Intel SGX [86] and blockchain to implement a patient-centric personal health data management system with accountability and decentralization. In addition, they design a token-based access control mechanism based on U-Prove [210] for the user registration process, which is required to collect health data. Moreover, [211] proposed a framework called Ancile, in order to preserve the privacy of medical data by taking into account security, interoperability, and efficiency aspects for the access of medical records. Ancile is based on the use smart contracts in an Ethereum-based blockchain in which hashes of the data references are stored. Furthermore, the proposed framework proposes the use of proxy re-encryption [212] to streamline the secure sharing of EHRs.

Also based on the notion of off-chain storage, [213] presents a system for privacy-preserving data sharing of EMRs, called BPDS. In this case, EMRs are stored in the cloud by using the CP-ABE scheme [130], while the indexes are stored in a consortium blockchain. In [214] authors propose a decentralized privacy-preserving healthcare blockchain for IoT, which provides full anonymity by relying on ring signatures. Moreover, BlocHIE [215] is a BLOCkchain-Based Platform for Healthcare Information Exchange that implements privacy and authenticability by combining off-chain storage and on-chain proof-of-existence of medical records, namely a hash containing the medical record plus signatures of patient and hospital. In addition, [216] describes the FHIRChain approach, which represents a blockchain-based architecture that is intended to meet the requirements from the Office of the National Coordinator for Health Information Technology (ONC) in USA regarding medical data sharing. Like in the previous work, FHIRChain employs traditional public key cryptography to encrypt meta-data instead of the data themselves. However, this approach provides a more interoperable solution through the use of the HL7 Fast Healthcare Interoperability Resources (FHIR) standard [217] for shared clinical data.

Summary and analysis of current trends. In addition to the set of previous research works, there are some examples about the application of blockchain to eHealth scenarios in Europe. Indeed, the EC points out about the needs and challenges related to the digital transformation of health and care, in which blockchain is referenced to play a key role for personalised healthcare services.[9] A prominent example of the realization of blockchain-based healthcare services is

---

[9]https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

represented by Estonia, which became one of the first countries in using blockchain in this context. Towards this end, the Estonian E-Health Foundation launched in 2016 a project to safeguard patient health records by using blockchain in archiving related activity logs.[10] Another ongoing initiative is represented by the H2020 EU project ''My Health - My Data (MHMD) [2], which is intended to define a privacy-by-design blockchain solution for healthcare. For this purpose, the approach is based on the definition of smart contracts that enforce dynamic consent mechanisms and peer-to-peer data transactions between public and private healthcare providers and patients. From the previous analysis, eHealth scenarios have particularly strong privacy restrictions that must be properly addressed from the technical and legal perspective. Indeed, recent European regulations or communications, such as the ''*Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*''[11] aim to provide guidelines about the needs and requirements of future eHealth services. In this sense, given the nature of healthcare data, the enforcement of GDPR and eHealth-specific regulations is a challenging aspect to be overcome in the coming year through the application of suitable PETs. Indeed, it should be noted that health data are considered as a special category of personal data by GDPR (Article 9), so that the processing is only authorized under certain circumstances. Another challenging aspect to be considered is the need for the participation of different eHealth stakeholders, including medical personnel for personalized healthcare services. Such aspect require the application of suitable privacy-preserving mechanism to be combined with cryptographic approaches to preserve citizens' privacy.

D. C-ITS

Most of the C-ITS research proposals for blockchain adopt temporal pseudonyms and certificates based on the use of a PKI to provide enhanced unlinkability. Indeed, the ''*European Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)*''[12] defines an architecture based on commonly changing pseudonym certificates and PKI to ensure authenticity and integrity with a minimum impact on privacy. Consequently, blockchain-based research proposals also consider the use of pseudonyms to address privacy aspects in C-ITS scenarios.

Based on it, [156] proposes a privacy-respectful liability model for blockchain that provides untampered evidences in autonomous vehicles scenarios for liability attribution and adjudication in an event of accident. It provides pseudonymity, through the usage of anonymous certificates

for an specific period of time. This work is extended by the same authors to provide evaluation results of a forensic system (B-FICA) [218] based on the approach proposed in the previous paper. Furthermore, Block4Forensic is proposed by [219] as a vehicular forensics system provides a decentralized blockchain-based approach to gather relevant information from different parties in case of an accident. In particular, the approach is based on the use of the IEEE 1609.2 standard [220] to manage the corresponding certificates and pseudonyms to enhance privacy. Furthermore, [221] proposed a blockchain-based architecture for C-ITS that minimizes blockchain linkability by using fresh keys for each of vehicle interaction. Each vehicle can consent the release of the information, and the on-chain transactions are encrypted. By using a similar approach, [222] proposes Blackchain, which is based on the use of blockchain for the revocation of misbehaving vehicles. This approach also employs temporal pseudonyms that can be revoked through consensus among a dynamic cluster of vehicles.

Focused on the use case of energy trading for electric vehicles, [223] proposes a blockchain-based mechanism by using random pseudonymous as public keys. Furthermore, it employs multiple wallet addresses to conceal the real address of the wallet, in order to preserve vehicles' privacy during trading. In addition, [224] presents a protocol for electric vehicle charging based on blockchain with privacy preservation for the car owners. None of the participants learns the position of the vehicle and only the vehicle and the selected station knows the transaction details. It addition, it uses commitment schemes for a vehicle to commit the decision for a particular charging station while avoiding disclosure of the chosen one. Other privacy solutions for C-ITS systems relies on more sophisticated privacy techniques. In this case, [5] defined and evaluated a privacy-preserving blockchain incentive vehicular network via an efficient anonymous announcement aggregation protocol, called CreditCoin. It allows that different users can send announcements and generate signatures in a potentially untrusted environment. CreditCoin achieves conditional privacy due to the ability of trace malicious users' identities in anonymous announcements with related transactions. Privacy is addressed using threshold ring signatures and Combined Public Keys (CPK) [225].

Summary and analysis of current trends. From the previous analysis, the use of sophisticated PETs is not widely considered in the scope of blockchain-based C-ITS proposals. Indeed, most of the works are based on well-known public key cryptographic mechanisms usually supported by a PKI. The main reason is that C-ITS services are mainly intended to improve roads' safety, so that privacy requirements could represent an obstacle in some cases. Furthermore, as already mentioned, current efforts towards a more interoperable consider these well-established approaches to provide authentication and integrity services. Indeed, the standard security approaches in C-ITS (e.g., based on ETSI [226]) are based on PKI for the management of enrolment and pseudonym certificates. However, taking into account the literature review,

---

[10]https://e-estonia.com/blockchain-healthcare-estonian-experience/

[11]https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering

[12]https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

TABLE 4. Comparison of privacy-preserving features on different research proposals in blockchain-based cryptocurrencies.

Research proposal	Year	Cryptographic technique	Implemented/Validated	Blockchain platform	Main approach
Mixcoin - Anonymity for Bitcoin with accountable mixes [22]	2013	Mixing	Yes[14]	Bitcoin	Accountable randomized mixing fees for bitcoin
Blindcoin: Blinded, Accountable Mixes for Bitcoin [67]	2015	Mixing	No	Bitcoin	Enhancement of the Mixcoin's privacy properties through blind signatures
CoinJoin: Bitcoin privacy for the real world [70]	2013	Mixing	Yes[15]	Bitcoin	Enhancement of the Mixcoin's privacy properties through blind signatures
TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub [23]	2017	Mixing	Yes[16]	Bitcoin	Use of an untrusted intermediary (i.e., the Tumbler) to enable anonymous off-chain payments
CoinParty: Secure Multi-Party Mixing of Bitcoins [234]	2015	Mixing	Yes[17]	Bitcoin	Decentralized mixing service based on a threshold variant of ECDSA
Sybil-Resistant Mixing for Bitcoin [235]	2014	Mixing	Yes	Bitcoin	Two-party mixing protocol to address specific sybil, Dos and timing attacks

most of these papers do not use standard ETSI components for the integration of blockchain techniques (even if PKI is considered). In spite of this, blockchain technologies could be significantly valuable for C-ITS scenarios, especially with the advent of autonomous transportation system. Indeed, blockchain's properties in terms of decentralization and data immutability could help to reflect the actions and events that are carried out in a road, to build a responsibility attribution framework [156]. Another recent approach [227] considers the integration of the existing standard PKI for C-ITS with a blockchain deployment, in which misbehavior information is shared in a large-scale deployment composed by different *jurisdictions*. In this case, pseudonyms are changed for privacy reasons according to the definition of different *zones* in the road. This approach highlights the need to consider standard deployments to foster the development of interoperable blockchain C-ITS services.

E. CRYPTOCURRENCIES SCENARIOS

As already mentioned, Bitcoin is the main example of blockchains-based cryptocurrencies; consequently, it is an attractive target for criminals. Indeed, several attacks have been already reported, for example the recent social engineering attack to the Slovenian-based bitcoin mining marketplace Nicehash,[17] in which nearly $64 million in bitcoin were stolen. Other security breaches have been described in research works, such as double spending (i.e., signing-over the same coin to two different users) [230], or transaction malleability [231], which makes reference to the fact that bitcoin signatures do not provide any guarantee of the signature's integrity itself. These aspects must be properly addressed, so that privacy of involved entities in cryptocurrencies transactions is not undermined.

In general, there are two main aspects in any blockchain-based cryptocurrency that could affect privacy. On the one hand, most of current cryptocurrencies are not able to provide anonymity properties in multi-input transactions, in which an entity must prove it is the owner of all the inputs. In this case, unlinkability cannot be provided because of the use of different input addresses from the same user. On the other hand, since the public chain reveals all the transaction data, the amount of coins in a transaction will be also visible for any participant. In the case of bitcoin, these aspects are highlighted by recent works, such as [29], which

---

[17]https://www.theguardian.com/technology/2017/dec/07/bitcoin-64m-cryptocurrency-stolen-hack-attack-marketplace-nicehash-passwords

suggests directions for future research towards provisioning stringent security and privacy techniques based on previous works [10], [12].

One of the main proposals for enabling privacy and improving anonymity in these scenarios is based on the use of mixing services (or tumblers) (as introduced in Section IV.B.1). Mixing services has been extensively used in the literature to create new cryptocurrencies with enhanced private properties. Below, some of these main proposals are discussed, and main solutions are recapped in Table 4. In this direction, [22] was one of the first mixing approaches, based on the use of randomized mixing fees and an accountability mechanism to expose theft. Furthermore, the approach provides an adaptation of mix networks to bitcoin for maintaining indistinguishability properties against active attackers. Furthermore, Blindcoin [67] extends the Mixcoin protocol to enhance privacy properties. In particular, authors propose the use of a blind signature scheme [232] to ensure the input/output address mapping for any user is kept hidden from the mixing server. Another mixing approach was proposed by [70], which describes CoinJoin. CoinJoin works as follows:

1) *N* users coordinate to create a joined transaction. It is assumed that they apply network anonymity methods like Tor or I2P. Each party indicates their desired destination address of the payment.
2) One of the users creates a transaction per destination address. All receive the same amount to hinder the correlation by different payment amounts.
3) Each party sends their due coins to the previous account that created the transaction to *N* destinations.
4) Only if the *N* users contribute with their payment, the transaction to *N* parties will take effect, otherwise, the funds are returned.

CoinJoin has been implemented on different bitcoin-based prototypes, such as DarkWallet [233], which is a bitcoin wallet that can be installed as a browser plugin. Moreover, Tumblebit [23] is a mixing service based on an untrusted intermediary called the Tumbler. TumbleBit replaces on-blockchain payments with off-blockchain puzzle solving, in which anonymity properties are also similar to blind signatures.

The use of Secure Multi-party Computation (SMPC) [26], introduced in section IV.A, is proposed by [234] to create a decentralized mixing service called CoinParty. Specifically, authors employ a threshold variant of the ECDSA algorithm

to create (in a distributed way) bitcoin addresses from which funds can only be redeemed in a threshold transaction, that is, only when a majority of the controlling peers agrees to do so. Another decentralized mixing service is presented in [235] that is named Xim. The approach describes a two-party bitcoin-compatible mixing protocol based on a previous exchange protocol [80], and focused on addressing sybil, Dos and timing attacks. Based on CoinJoin, CoinShuffle [66] is also a decentralized mixing protocol for bitcoin based on the anonymous group communication protocol Dissent [236] to ensure anonymity and robustness against DoS attacks. Then, an improved implementation of this approach is presented as Coinshuffle++ [173] that is based on a new P2P mixing protocol called DiceMix, which builds on the original DC-net protocol [237] to improve the performance of previous mixing protocols.

In addition to the use of mixing protocols, complementary approaches have been also considered to enhance privacy properties in blockchain-based cryptocurrencies. In this direction, Confidential Transactions (section IV.A.3) is an approach proposed by [238] based on homomorphic encryption following Pedersen commitments [239]. The main goal applied to is to make the amount of coins of a transaction only visible to the corresponding involved entities (i.e., payer and payee). Another approach is the use of Stealth Addresses [125] that is intended to protect payee's privacy. In this case, the main idea is inspired by the Elliptic Curve Diffie-Hellman (ECDH) algorithm, in such a way that the payer needs to create a one-time address for every transaction with a specific payee, in order to enhance unlinkability. Based on both approaches, [24] extends the mixing protocol CoinShuffle++, through the integration of Stealth Addresses and Confidential Transactions to provide a more comprehensive privacy-preserving approach. Moreover, a recent proposal called Möbius [240] describes an Ethereum-based mixing service that is built through smart contracts to enhance the protection against availability attacks.

Another privacy-preserving proposals for cryptocurrencies that relies on Confidential Transactions is Mimblewimble [241] which describes a blockchain with a totally different approach. The main differences with the usual blockchain is that Mimblewimble supports confidential transactions. Andrew Poelstra in a document with the same title [242] continues with the idea of Elvis Jedusor. To achieve these confidential transactions, all the values are homomorphically encrypted in a process called blinding factors. In this scheme the values or the destination of the transactions are unknown.

Regarding the applicability of ring signatures (section IV.A.6) in cryptocurrencies, CryptoNote [28] employs a custom one-time ring signature scheme. The destination of each CryptoNote output is a public key, derived from recipient's address and sender's random data. In cryptonote unlike Bitcoin each destination key is different. In CryptoNote, the sender performs a Diffie-Hellman in order to obtain a shared secret, that is derived from his data along with first part of the recipient's address. Afterwards,

a one-time destination key is computed, derived from such a shared secret the other part of the address. For these two esteps, it requires two EC-keys for the recipient, meaning that address in CryptoNote are larger than a Bitcoin wallet address. Similarly, receiver also carries out the Diffie-Hellman to get the secret key. CryptoNote might have concerns dealing with the ring signatures depending on the large of anonymity set *n*, as it requires that each transaction contains a ring signature of size $O(n)$. Besides, storing ring signatures in public blockchain might become a problem. Unlike CryptoNote, CoinJoin [70] or ValueShuffle [24] facilitate pruning, which is a drawback in Cryptonote, as rings signatures make the pruning difficult.

Regarding the usage of ZKP in cryptocurrencies, Zerocoin [16] is a cryptographic extension to Bitcoin that augments the protocol to allow fully anonymous currency transactions. It uses Zero-Knowledge Signature of Knowledge (ZKSoK) on message to sign the bitcoin transaction hash instead of using ECDSA. Zerocoin authenticates coins using ZKP to demonstrate that coins are in a public list of valid coins maintained on the blockchain. Similarly, Zerocash [25] is an decentralized anonymous payment scheme that provides a anonymity-by-design solution leveraging zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs). Zerocash outperforms Zerocoin, reducing size of transactions and verification time, hides transactions amounts and allows transactions of any kind.

Another ZKP-based approach is BulletProofs [96], that proposes a protocol based on non-interactive ZKP that employs short proofs and without the requirement of a trusted setup. It uses the Fiat-Shamir heuristic for making it non-interactive. This is built on different techniques based on the discrete logarithm assumption, and then the proofs are made. Multiple range proofs are aggregated in BulletProofs, e.g. for transactions with multiple outputs into a single short proof. It is used for CT in Bitcoin, as the transactions can have two or more outputs. It also allows to aggregate multiple range proofs from different users into one single aggregated range proof.

In [243] authors propose a privacy respecting approach for economy applications based in blockchain and zero-knowledge schemes. The participants use proxies for making the transactions instead of doing it directly and in the ledger, the only reference between the original identity and the proxy is a zk-SNARK proof which prevents privacy leaks.

Non-interactive zero-knowledge (NIZK) proofs have been proposed as a tool to enable complex privacy-preserving smart contracts. [244] have done an interesting analysis about the shortcomings in Zero Knowledge Contingent Payments (ZKCP) which are the ability of an attacker to learn partial information about the digital goods being sold and the problems of using ZKCP to provide services instead of goods. In order to solve these issues, they propose the use of Zero-Knowledge Contingent Service Payments (ZKCSP) which provides a proof-of-retrievability (PoR) and it is an evolution of the previous ZKCP.

TABLE 5. Privacy-preserving platforms in blockchain and their compliance with GDPR principles.

GDPR principles	Lawfulness, fairness and transparency	Purpose limitations	Data minimization	Accuracy	Storage limitations:	Integrity and confidentiality
uPort [20]	(-) usability privacy-implications are not totally shown to users.	(+)Prove ownership of uPortId and control of revealed attributes to whom	(+) unlinkability (uPortIDs) (+)verifiable claims, (+)Selective disclosure, (+) ID-KeysRecovery, (+) permits usage without IdProofing	(+) revocation of verifiable claims	(-) Even if encrypted, attributes stored in central registry could be analyzed, as they are public accessible	(+) attributes and attestations encrypted in FIPS repository (-) security in permissionless DLTs is more difficult to handle
Sovrin [21]	(+) Proof of Sharing Consent between DIDs, receipt without PPI (+) Consent for Proof Request (+) freedom to change Wallet providers and Agents (-) usability privacy-implications are not totally shown to users.	(+) Prove ownership of DID and control of revealed attributes to whom (+) Proof request state the purpose of data being requested	(+) unlinkability (+) verifiable claims (+) zero-knowledge proofs (+) ID recovery	(+) revocation is decentralized, asynchronous, and private, using cryptographic techniques (accumulators)	(+) Keeps private data, including hashes, off the Sovrin ledger.	(+) Permissioned DLT. stewards enforce security and run BFP consensus protocol (+) Confidential Agent-to-Agent communications off-ledger
ShoCard [141]	(+) User consent prior releasing	(+) permission-based user data release, (+) proof user consent	(+) user claims (-) unlikability against the Shocard server is not fully ensured	(+) user consent can be revoked	(+) blockchain certification records only maintain "signatures of hashes of data + code"	(-) Shocard server might store encrypted sensitive data (biometrics) (+) blockchain agnostic, sidechain speed up process
Civic [247]	(+) user consent using QR codes (-) private-solution. Lack of implementation and technical details of the system"	(+) multiple identity validation service providers (+) verification of submitted PII data	(+) attestations (+) release only necessary information to SP (-) unclear anonymity procedures (-) unclear ID-Keysrecovery"	(+) Identity data is revocable in blockchain by the authenticating authority.	(-) Civic SIP server can act as intermediary Authz Server between user and SP, which might trace user's.	(+) PII is maintained encrypted in the app, accessed with biometrics (+) multifactor authentication"

Summary and analysis of current trends

Despite their anonymity features, Zerocash and Zerocoin have the drawback that it is not possible to see the outputs that have been spent already, therefore, blockchain pruning is not possible. Zerocash uses zkSNARKS [116] meaning that a trusted setup must be ensured. Besides zkSNARKS might be subject to non-falsifiable cryptographic hardness assumptions [245]. One of the main issues of Zerocoin is performance, as it uses double-discrete-logarithm proofs of knowledge that takes around 450 ms to be verified (at the 128-bit security level). Besides, Zerocoin does not hide the amount of transactions, and it does not support payments of exact values.

Current research trend of privacy-preserving cryptocurrencies is to make computationally feasible the calculation of NIZK proofs when dealing with certain demanding scenarios, as actual solutions relying on zk-SNARKs such as Zerocash, incurs in high computational cost. This is important, for instance, when light Zcash clients need to be employed. Mimblewimble, based on Confidential Transactions, outperforms the computational cost of Zcash, so that some research works revolve around extending Mimblewimble with additional privacy features. Another current trend with cryptocurrencies is support multiples exchanges using NIZK when the asset has more than one owner, which imposes additional challenges. In this sense zk-SNARKS are being leveraged to support that [246] feature.

F. PRIVACY-PRESERVING IDENTITY MANAGEMENT SYSTEMS AND PLATFORMS IN BLOCKCHAIN

This section reviews the main permissioned blockchains platforms, analyzing their main features and privacy aspects. In addition, it compares those solutions considering their compliance with the GDPR principles enumerated in Section III-K, this comparison is shown in Table 5.

Uport [20] uses 20-byte hexadecimal identifier to represent the user's uPortID, with the address of a Proxy smart contract deployed in Ethreum. Such a contract introduces a layer of indirection between the user's private key - maintained on their mobile device - and the application smart contract being accessed by users. The user app contacts an instantiation of a Controller smart contract (which holds the main access control logic such as Authentication/authorization), which in turn, is the unique entity capable of interacting with the proxy. uPort support certain degree of unlikability, as user can create many unlinkable uPortIDs. Selective disclosure of attribute is allowed encrypting an attribute with a symmetric encryption key, which in turn, is individually encrypted with the public key of the identity allowed to read the attestation attribute. uPort also support identity recovery and rely on DID[18] standard and Verifiable Claims,[19] both being standardized by the W3C.

---

[18]https://w3c-ccg.github.io/did-spec
[19]https://www.w3.org/TR/verifiable-claims-data-model

Sovrin [21], is open-source decentralized identity network for permissioned blockchain. Sovrin is a utility identity deployed over Hyperledger-Indy[20] that implements Plenum [248] byzantine BPT consensus algorithm for consensus. The roadmap of Hyperledger Indy includes additional privacy-enhancing features such us mixing networks that are used to maintain pairwise pseudonymous connections between Decentralized Key Management System (DKMS) agents. Currently, Hyperledger Indy allows the building of interactions where the degree of disclosure is explicit and minimal. Sovrin supports DPKI (Decentralized Public Key Infrastructure), where every public key has its own public address in the ledger (DID, decentralized identifier) that enable universal verification of claims. Sovrin allows having different DID for every relationship the user has, with different keypairs, unlinkable each other. Like in uPort, Sovrin user generates crypto keypairs and maintain the private key in the user's mobile. It supports identity recovery and make use of software Agents that can act on behalf of the user to facilitate interactions with third party service provider agents. Unlike uPort, Sovrin supports, not only attestation and verifiable assertions, but also Anonymous credentials with ZKP to achieve fully unlinkability and comply with the minimal disclosure principle. Namely, in Hyperledger, anonymous credentials are based on Camenisch-Lysyanskaya's signature over Attribute-Based Credentials [27]. Sovrin allows demonstrate proofs offchain directly in a secure channel with the third party, without storing the attributes in the ledger. In this case, the blockchain is used to identify the trusted service endpoint to interact with. The web of trust supported by the sovrin trust anchors provides verifiability of the target party being interacted.

Shocard [141] uses the ledger as repository of certifications that maintains signatures-of-hashes-of each personal data along with with a code to avoid brute-force discovery. Shocard is blockchain agnostic and uses private parallel sidechains to speed up the transactions in the ledger. It supports that third party can verify and then certify an individual's identity and credentials. Shocard provides App that hold cryptokeys and entities can verify a user's claims of identity through certifications and signatures hold in the ledger. The ShoCardId can be boostrapped from trusted breeder document e.g. ePassport, through IDproofing stage to validate user's identity checking biometrics in the ePassport chip. However, the enrollment with biometrics requires storing encrypted sensitive data in the Shocard server. This server might trace interactions between Relying parties and ShoCardIDs.

Civic [247] is a decentralised trusted Identity application that provides identity proofing relying on existing eID documents like ePassports. The app stores private keys of user Civic ID used for record signed hashes of attestations in the blockchain. Support multiple-factor authentication, user-consent, and minimal disclosure. However, anonymity and

unlikability mechanisms are not seemed to be implemented in Civic yet. And the civic server can act as an intermediary Authz Server between user and SP, which raises privacy concerns.

Enigma [249], developed by MIT, allows secure data sharing, using multi-party computation (MPC) and homomorphic encryption. Enigma aims to allow developers to build *privacy by design* and decentralized applications, avoiding a trusted third party (TTP). Enigma cannot be defined as a cryptocurrency or a blockchain platform. Instead, Enigma connects to an existing blockchain, and performs computation offloading of the private and intensive computations on an off-chain network. Unlike in blockchain schemes, the incentives are based on fees instead of mining rewards, where nodes are compensated for providing computational resources. The nodes pay a security deposit, which deters malicious nodes. Enigma uses secure multi-party computation (sMPC) technology, in which data queries are distributively computed, and data is divided across different nodes each one computing certain functions in a distributed way without leaking information to the other.

Different solutions such as the Civic platform [247], are starting to apply the user-centric and decentralized blockchain approach to provide real-time authentication through biometrics, where identity data is encrypted in the mobile app. These solutions, uses Merkle tree randomized hashes using nonces signed by the validators entities, and supporting selective disclosure of the identity information (certain portions of the Merckle tree hashes are revealed) in the blockchain, after user consent, enabling user control privacy and enhancing security, since the attestations and proofs cannot be tampered in the blockchain.

VI. FUTURE RESEARCH DIRECTIONS

Based on the previous analysis, this section describes some of the main research directions on privacy aspects for blockchain:

- Existing and upcoming blockchain developments should be aligned with new regulatory frameworks. As described by the EU Blockchain Observatory and Forum report in 2018 [98], the inherent distributed nature of blockchain technologies sets out several obstacles to build compliant solutions with current data protection regulations, such as the GDPR. These concerns must be also considered in the scope of the "Proposal for a Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)",[21] which is intended to adapt the current ePrivacy Directive to the recent advances in ICT. In spite of the efforts to build more privacy-respectful solutions, there is still a need to ensure privacy properties as defined by such legal instruments.

---

[20]https://www.hyperledger.org/projects/hyperledger-indy

[21]https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

- From the previous analysis, one of the main issues is derived from the applicability of privacy-preserving techniques due to the cost of cryptographic operations. Indeed, the research community is working on novel crypto-privacy protocols to deal with the computational expensive operations required by emerging privacy techniques (e.g. ZK-SNARKS) for blockchain, which undermines the scalability and broad-adoption of blockchain in certain large-scale scenarios. These issues are exacerbated in scenarios in which devices or systems with resource constraints are widely considered, such as the IoT. Therefore, the development of new privacy-preserving approaches should cope with these issues, in order to foster the adoption of blockchain technologies

- Related to cryptographic aspects, another research direction is the definition of novel crypto-algorithms resistant to quantum computing, as traditional primitives based on large integer factorization problem, and log of elliptic curves public-key cryptography will be no longer strong enough. These aspects are highlighted by [250], which provides an initial set of recommendations for quantum-resistant algorithms. In addition, upcoming research works will have to evolve privacy-preserving solutions (e.g. SMPC) to protect privacy in the execution of smart-contracts while ensuring its formal verification. In this direction, recent works, such as [92], describe potential solutions to make current blockchain deployments resistant to quantum computing technologies.

- As already mentioned, usability aspects are crucial to ensure that end-users are able to manage their privacy in an effective way. Based on our analysis, we believe that there is a lack of comprehensive approaches for this purpose. This is specially relevant in scenarios such as eHealth, where sensitive data could be shared for personalized healthcare services. For that reason, several operations (e.g., key-recovery or selective disclosure) should be automated through the use of user-friendly tools.

- Another relevant aspect derived from our analysis is the existence of a huge amount of technologies and platforms intended to provide privacy aspects in blockchain systems. Therefore, ensuring the interoperability among such deployments is crucial to ensure large-scale blockchain scenarios. For that purpose, the use of interledger approaches [251] could help to mitigate potential interoperability concerns through a common platform, in which different blockchains could maintain their privacy preferences. In this direction, the use of interledger techniques (e.g., sidechains [252]) needs to be analyzed in the coming years as a tool to increase interoperability, as well as to reduce performance issues.

- In recent years, the integration of blockchain technologies has been strongly considered in many different everyday scenarios. From our analysis in Section V, most of these emerging proposals are not aligned with existing standards in such scenarios. One of the main

examples is represented by C-ITS, where there is a clear consensus between government institutions and industry to use PKI as the basis for providing security properties. However, most of recent research proposals consider blockchain as the only mechanism for that purpose. Therefore, the application of blockchain, and the inclusion of privacy-preserving techniques should be compliant (not only) with existing regulations, but with current standard in such scenarios, in order to ensure a broad-scale acceptance of new techniques.

VII. CONCLUSIONS

This paper surveyed the current state of the art on privacy-preserving technologies for blockchain. Several open research challenges and issues related to privacy-preservation on blockchain were identified, encompassing transaction linkability, crypto-keys management (e.g. recovery), issues with crypto-privacy resistance to quantum computing, on-chain data privacy, usability, interoperability, or compliance with privacy regulations, such as the GDPR. Based on this, we analyzed the current privacy-preserving mechanisms (e.g. SMPC, ZKPs, ring signatures, homomorphic hiding, Mixings), blockchain platforms and research proposals that are arising to deal with those issues. Furthermore, the review has covered the privacy-preserving mechanisms that are being applicable on the main scenarios that can benefit from blockchains deployments, including eGovernment, eHealth, cryptocurrencies, smart cities, and C-ITS.

Despite important analyzed efforts to devise and integrate novel crypto-privacy techniques, current blockchain solutions are still far to cope with those privacy challenges in an holistic way. This situation undermines user's rights, such as the right to become anonymous in certain situations, the right to erase data or withdraw consent, thereby lessening the realization of a truly privacy-preserving and Self-Sovereign Identity model on blockchain.

Efficient crypto-privacy algorithms are needed in order to evolve the performance of zero-knowledge techniques applicable on blockchains, as well as building quantum-resistant ledgers. These new proposals will allow to strengthen the privacy-preserving features for blockchain in challenging scenarios like IoT. Likewise, novel research initiatives are needed with the aim of improving privacy usability, and privacy control, thereby making blockchains deployments fully compliant with privacy regulations.

REFERENCES

[1] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] R. Panetta and L. Cristofaro, "A closer look at the eu-funded my health my data project," in *Proc. Digit. Health Legal*, Nov. 2017, pp. 10–11, doi: 10.5281/zenodo.1048999.

[3] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, 2017.

[4] M. Conoscenti, A. Vetrò, and J. C. D. Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2016, pp. 1–6.

[5] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "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.

[6] F. R. Batubara, J. Ubacht, and M. Janssen, "Challenges of blockchain technology adoption for e-government: A systematic literature review," in *Proc. 19th Annu. Int. Conf. Digit. Government Res., Governance Data Age*, New York, NY, USA, 2018, pp. 76:1–76:9.

[7] *Regulation (EU) 2016/679 of the European Parliament and of the Council 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)*, document 32016R0679, May 2016, vol. L119, pp. 1–88. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

[8] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Open Problems in Network Security*, J. Camenisch and D. Kesdoğan, Eds. Cham, Switzerland: Springer, 2016, pp. 112–125.

[9] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, to be published.

[10] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *Financial Cryptography Data Security*, A.-R. Sadeghi, Ed. Berlin, Germany: Springer, 2013, pp. 34–51.

[11] P. Koshy, D. Koshy, and P. McDaniel, "An analysis of anonymity in bitcoin using P2P network traffic," in *Financial Cryptography and Data Security*, N. Christin and R. Safavi-Naini, Eds. Berlin, Germany: Springer, 2014, pp. 469–485.

[12] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," in *Proc. IEEE 3rd Int. Conf. Social Comput. (SocialCom) Privacy, Secur., Risk Trust (PASSAT)*, Boston, MA, USA, Oct. 2011, pp. 1318–1326.

[13] J. Herrera-Joancomartí, "Research and challenges on bitcoin anonymity," in *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*, J. Garcia-Alfaro, J. Herrera-Joancomartí, E. Lupu, J. Posegga, A. Aldini, F. Martinelli, and N. Suri, Eds. Cham, Switzerland: Springer, 2015, pp. 3–16.

[14] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, pp. 6–10, Jun. 2016.

[15] 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 (SP)*, May 2016, pp. 839–858.

[16] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2013, pp. 397–411.

[17] Zcash. (2018). *Zcash—How ZK-Snarks Work in Zcash*. [Online]. Available: https://z.cash/technology/zksnarks.html

[18] S. Alboaie and D. Cosovan, "Private data system enabling self-sovereign storage managed by executable choreographies," in *Distributed Applications and Interoperable Systems*, L. Y. Chen and H. P. Reiser, Eds. Cham, Switzerland: Springer, 2017, pp. 83–98.

[19] Wanchain Foundation. (2018). *Building Super Financial Markets for the New Digital Economy*. [Online]. Available: https://www.wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf

[20] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. (2017). *Uport: A Platform for Self-Sovereign Identity*. [Online]. Available: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf

[21] A. Tobin and D. Reed. (2016). The Inevitable Rise of Self-Sovereign Identity. The Sovrin Foundation. [Online]. Available: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

[22] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2014, pp. 486–504.

[23] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: An untrusted bitcoin-compatible anonymous payment hub," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2017. [Online]. Available: https://open.bu.edu/handle/2144/29224

[24] T. Ruffing and P. Moreno-Sanchez, "ValueShuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin," in *Financial Cryptography and Data Security*. Cham, Switzerland: Springer, 2017, pp. 133–154.

[25] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2014, pp. 459–474.

[26] R. Cramer and I. B. Damgård, *Secure Multiparty Computation*. Cambridge, U.K.: Cambridge Univ. Press, 2015.

[27] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2002, pp. 21–30.

[28] N. Van Saberhagen. (2013). *Cryptonote v2.0*. [Online]. Available: https://cryptonote.org/whitepaper.pdf

[29] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.

[30] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[31] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, Jan. 2019.

[32] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quart.*, vol. 35, pp. 1017–1042, Dec. 2011. [Online]. Available: http://dl.acm.org/citation.cfm?id=2208940.2208951

[33] D. J. Solove, "A taxonomy of privacy," *Univ. Pennsylvania Law Rev.*, vol. 154, p. 477, Jan. 2006.

[34] R. L. Finn, D. Wright, and M. Friedewald, "Seven types of privacy," in *European Data Protection: Coming of Age*. Dordrecht, The Netherlands: Springer, 2013, pp. 3–32.

[35] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quart.*, vol. 35, no. 4, pp. 989–1016, Dec. 2011.

[36] E. F. Stone, H. G. Gueutal, D. G. Gardner, and S. McClure, "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations," *J. Appl. Psychol.*, vol. 68, no. 3, pp. 459–468, 1983.

[37] G. Danezis and S. Gürses, "A critical review of 10 years of privacy technology," in *Proc. Surveill. Cultures, Global Surveill. Soc.*, 2010, pp. 1–16.

[38] A. Pfitzmann and M. Hansen, *A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, vol. 68, no. 3, Washington, DC, USA: American Psychological Association, 2009, pp. 459–468. [Online]. Available: https://www.researchgate.net/publication/232567994_A_field_experiment_comparing_information-privacy_values_beliefs_and_attitudes_across_several_types_of_organizations

[39] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2001, pp. 93–118.

[40] Y. Shen and S. Pearson, "Privacy enhancing technologies: A review," *HP Lab.*, vol. 2739, pp. 1–30, Jun. 2011.

[41] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489–516, 1st Quart., 2018.

[42] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "To blockchain or not to blockchain: That is the question," *IT Prof.*, vol. 20, no. 2, pp. 62–74, Mar./Apr. 2018.

[43] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symp. Secur. Privacy*, Apr. 1980, p. 122.

[44] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: Platforms, applications, and design patterns," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Cham, Switzerland: Springer, 2017, pp. 494–509.

[45] P. Jayachandran. (2017). *The Difference Between Public and Private Blockchain—Blockchain Unleashed: IBM Blockchain Blog*. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

[46] Z. Zheng, S. Xie, H. Dai, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data, Big Data Congr.*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[47] C. Ribeiro, H. Leitold, S. Esposito, and D. Mitzam, "STORK: A real, heterogeneous, large-scale eID management system," *Int. J. Inf. Secur.*, vol. 17, no. 5, pp. 569–585, Oct. 2018.

[48] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in *Proc. 2nd ACM Workshop Digit. Identity Manage.*, 2006, pp. 11–16.

[49] J. Hughes and E. Maler, *Security Assertion Markup Language (SAML) V2. 0 Technical Overview*, document sstc-saml-tech-overview-2.0-draft-08, OASIS SSTC Work. Draft, 2005, pp. 29–38.

[50] A. Czeskis and J. Lang, *Fido NFC Protocol Specification V1.0*, FIDO Alliance Proposed Standard, Apr. 2017, pp. 1–5. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103642/01.01.01_60/tr_103642v010101p.pdf

[51] C. Allen, "The path to self-sovereign identity," Christopher Allen, Blog, Berkeley, CA, USA, Tech. Rep., 2017. [Online]. Available: https://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[52] F. van den Broek, B. Hampiholi, and B. Jacobs, "Securely derived identity credentials on smart phones via self-enrolment," in *Proc. Int. Workshop Secur. Trust Manage.* Cham, Switzerland: Springer, 2016, pp. 106–121.

[53] J. B. Bernabe, M. David, R. T. Moreno, J. P. Cordero, S. Bahloul, and A. Skarmeta, "Aries: Evaluation of a reliable and privacy-preserving European identity management framework," *Future Gener. Comput. Syst.*, to be published.

[54] R. T. Moreno, J. B. Bernabe, A. Skarmeta, M. Stausholm, T. K. Frederiksen, N. Martínez, N. Ponte, E. Sakkopoulos, and A. Lehmann, "OLYMPUS: Towards oblivious identity management for private and user-friendly services," in *Proc. Global IoT Summit (GIoTS)*, Jun. 2019, pp. 1–6.

[55] J. B. Bernabé, J. L. Hernandez-Ramos, and A. F. Gómez-Skarmeta, "Holistic privacy-preserving identity management system for the Internet of Things," *Mobile Inf. Syst.*, vol. 2017, pp. 6384186:1–6384186:20, Aug. 2017.

[56] J. L. C. Sanchez, J. B. Bernabe, and A. F. Skarmeta, "Integration of anonymous credential systems in IoT constrained environments," *IEEE Access*, vol. 6, pp. 4767–4778, 2018.

[57] D. Reed, M. Sprony, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized identifiers (DIDs) v0. 11 data model and syntaxes for decentralized identifiers (DIDs). W3C," W3C, Cambridge, MA, USA, Tech. Rep., 2018. [Online]. Available: https://w3c.github.io/did-core/

[58] M. Sporny and D. Longley, "Verifiable claims data model and representations," W3C, Cambridge, MA, USA, Tech. Rep., 2017. [Online]. Available: https://www.w3.org/TR/2017/WD-verifiable-claims-data-model-20170803/ and https://www.w3.org/TR/vc-data-model/

[59] K. Wagner, B. Némethi, E. Renieris, P. Lang, E. Brunet, and E. Holst, "Self-sovereign identity: A position paper on blockchain enabled identity and the road ahead," Blockchain Bundesverband, Berlin, Germany, Tech. Rep., 2018. [Online]. Available: https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018.pdf

[60] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed. Berlin, Germany: Springer, 2013, pp. 6–24.

[61] M. Ober, S. Katzenbeisser, and K. Hamacher, "Structure and anonymity of the bitcoin transaction graph," *Future Internet*, vol. 5, no. 2, pp. 237–250, 2013.

[62] M. Fleder, M. S. Kester, and S. Pillai, "Bitcoin transaction graph analysis," 2015, *arXiv:1502.01657*. [Online]. Available: https://arxiv.org/abs/1502.01657

[63] M. Spagnuolo, F. Maggi, and S. Zanero, "BitIodine: Extracting intelligence from the bitcoin network," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2014, pp. 457–468.

[64] S. Meiklejohn and C. Orlandi, "Privacy-enhancing overlays in bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2015, pp. 127–141.

[65] J. Herrera-Joancomartí and C. Pérez-Solà, "Privacy in bitcoin transactions: New challenges from blockchain scalability solutions," in *Modeling Decisions for Artificial Intelligence*. Cham, Switzerland: Springer, 2016, pp. 26–44.

[66] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical decentralized coin mixing for bitcoin," in *Computer Security—ESORICS*, M. Kutyłowski and J. Vaidya, Eds. Cham, Switzerland: Springer, 2014, pp. 345–364.

[67] L. Valenta and B. Rowan, "Blindcoin: Blinded, accountable mixes for bitcoin," in *Financial Cryptography and Data Security*, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds. Berlin, Germany: Springer, 2015, pp. 112–126.

[68] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2016, pp. 43–60.

[69] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of Web payments via cryptocurrencies," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 4, pp. 179–199, 2018.

[70] G. Maxwell, "CoinJoin: Bitcoin privacy for the real world," in *Proc. Post Bitcoin Forum*, 2013. [Online]. Available: https://bitcointalk.org/index.php?topic=279249.0

[71] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in bitcoin P2P network," in *Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 15–29.

[72] S. Noether, "Ring signature confidential transactions for monero," IACR Cryptol. ePrint Arch., Tech. Rep. 2015/1098, 2015.

[73] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proc. USENIX Secur.*, 2004, pp. 1–18.

[74] B. Zantout and R. Haraty, "I2P data communication system," in *Proc. ICN*, 2011, pp. 401–409.

[75] A. Biryukov and I. Pustogarov, "Bitcoin over Tor isn't a good idea," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2015, pp. 122–134.

[76] N. T. Courtois and R. Mercer, "Stealth address and key management techniques in blockchain systems," in *Proc. ICISSP*, 2017, pp. 559–566.

[77] L. Er-Rajy, A. El Kiram My, M. El Ghazouani, and O. Achbarou, "Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures," *J. Internet Banking Commerce*, vol. 22, no. 3, pp. 1–29, 2017.

[78] S. Eskandari, J. Clark, D. Barrera, and E. Stobert, "A first look at the usability of bitcoin key management," 2018, *arXiv:1802.04351*. [Online]. Available: https://arxiv.org/abs/1802.04351

[79] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," *J. Cryptol.*, vol. 20, no. 1, pp. 51–83, 2007.

[80] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better—How to make bitcoin a better currency," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2012, pp. 399–414.

[81] M. Egorov, M. Wilkison, and D. Nuñez, "NuCypher KMS: Decentralized key management system," 2017, *arXiv:1707.06140*. [Online]. Available: https://arxiv.org/abs/1707.06140

[82] S. Foundation, "Sovrin: A protocol and token for self-sovereign identity and decentralized trust," Sovrin Found., Northampton, MA, USA, Tech. Rep., 2018. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[83] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *Proc. 6th Int. Conf. Princ. Secur. Trust*, vol. 10204. New York, NY, USA: Springer-Verlag, 2017, pp. 164–186.

[84] H. Hasan and K. Salah, "Proof of delivery of digital assets using blockchain and smart contracts," *IEEE Access*, vol. 6, pp. 65439–65448, 2018.

[85] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *Principles of Security and Trust*, M. Maffei and M. Ryan, Eds. Berlin, Germany: Springer, 2017, pp. 164–186.

[86] V. Costan and S. Devadas, "Intel SGX explained," *IACR Cryptol. ePrint Arch.*, vol. 2016, no. 86, pp. 1–118, 2016.

[87] A. Moghimi, G. Irazoqui, and T. Eisenbarth, "CacheZoom: How SGX amplifies the power of cache attacks," in *Proc. Int. Conf. Cryptograph. Hardw. Embedded Syst.* Cham, Switzerland: Springer, 2017, pp. 69–90.

[88] D. C. Sánchez, "Raziel: Private and verifiable smart contracts on blockchains," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 878, Nov. 2017.

[89] D. R. Kuhn, "A data structure for integrity protection with erasure capability," NIST, Gaithersburg, MD, USA, Tech. Rep., May 2018. [Online]. Available: https://csrc.nist.gov/publications/detail/white-paper/2018/05/31/data-structure-for-integrity-protection-with-erasure-capability/draft

[90] B. Stein, K. Kuznecov, S. Lee, and J. Müller, "A public blockchain solution permitting secure storage and deletion of private data—Draft," Lition Foundation, Berlin, Germany, Tech. Rep., 2018. [Online]. Available: https://www.lition.io/docs/Lition_TechnicalWhitePaper_V0.7.1.pdf

[91] D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on bitcoin, and how to protect against them," 2017, *arXiv:1710.10377*. [Online]. Available: https://arxiv.org/abs/1710.10377

[92] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, and A. K. Fedorov, "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, 2018, Art. no. 035004.

[93] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin1, A. I. Lvovsky, and A. K. Fedorov, "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, 2018, Art. no. 035004, doi: 10.1088/2058-9565/aabc6b.

[94] J. Pieprzyk, T. Hardjono, and J. Seberry, *Computer Security Fundamentals*. Berlin, Germany: Springer, 2013.

[95] B. Parno, J. Howell, C. Gentry, and M. Raykova, "Pinocchio: Nearly practical verifiable computation," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2013, pp. 238–252.

[96] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Efficient range proofs for confidential transactions," Stanford Univ., Stanford, CA, USA, Tech. Rep. 2017/1066, 2017.

[97] S. Ames, C. Hazay, Y. Ishai, and M. Venkitasubramaniam, "Ligero: Lightweight sublinear arguments without a trusted setup," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2017, pp. 2087–2104.

[98] T. Lyons, L. Courcelas, and K. Timsit, "Blockchain and the GDPR," Tech. Rep., Oct. 2018.

[99] D. W. Archer, D. Bogdanov, B. Pinkas, and P. Pullonen, "Maturity and performance of programmable secure computation," *IEEE Security Privacy*, vol. 14, no. 5, pp. 48–56, Sep./Oct. 2016.

[100] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *J. Comput. Syst. Sci.*, vol. 37, no. 2, pp. 156–189, 1988.

[101] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, no. 1, pp. 186–208, Feb. 1989.

[102] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2009, pp. 169–178.

[103] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "Recursive composition and bootstrapping for SNARKS and proof-carrying data," in *Proc. 41th Annu. ACM Symp. Theory Comput.*, 2013, pp. 111–120.

[104] E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, and M. Virza, "SNARKs for C: Verifying program executions succinctly and in zero knowledge," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2013, pp. 90–108.

[105] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 46, Mar. 2018.

[106] R. S. Wahby, I. Tzialla, J. Thaler, and M. Walfish, "Doubly-efficient zkSNARKS without trusted setup," in *Proc. IEEE Symp. Secur. Privacy*, May 2018, pp. 926–943.

[107] P. Mizel, F. Raetz, and G. Schmuck, "Asure: First scalable blockchain network for decentralized social security systems," Asure Found., Zug, Switzerland, Tech. Rep., 2018. [Online]. Available: https://icosbull.com/whitepapers/10691/Asure_Network_whitepaper.pdf

[108] D. Chaum and E. van Heyst, "Group signatures," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Springer, 1991, pp. 257–265.

[109] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Springer, 2001, pp. 552–565.

[110] *Bytecoin*. Accessed: Nov. 11, 2019. [Online]. Available: https://bytecoin.org

[111] S.-F. Sun, M. H. Au, J. K. Liu, and T. H. Yuen, "RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero," in *Computer Security—ESORICS*, S. N. Foley, D. Gollmann, and E. Snekkenes, Eds. Cham, Switzerland: Springer, 2017, pp. 456–474.

[112] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Springer, 1986, pp. 186–194.

[113] H. Wu and F. Wang, "A survey of noninteractive zero knowledge proof system and its applications," *Sci. World J.*, vol. 2014, May 2014, Art. no. 560484.

[114] J. Katz, V. Kolesnikov, and X. Wang, "Improved non-interactive zero knowledge with applications to post-quantum signatures," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2018, pp. 525–537.

[115] M. Blum, "How to prove a theorem so no one else can claim it," in *Proc. Int. Congr. Mathematicians*, 1986, pp. 1444–1451.

[116] C. Reitwiessner, "zkSNARKs in a nutshell," *Ethereum Blog*, vol. 6, pp. 1–15, Dec. 2016.

[117] E. Ben-Sasson, "Towards transparent scalable computational integrity," Tech. Rep., 2017.

[118] S. Bowe, A. Gabizon, and M. D. Green, "A multi-party protocol for constructing the public parameters of the pinocchio zk-SNARK," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 602, Feb. 2018, doi: 10.1007/978-3-662-58820-8_5.

[119] E. Ben-Sasson, I. Bentov, A. Chiesa, A. Gabizon, D. Genkin, M. Hamilis, E. Pergament, M. Riabzev, M. Silberstein, E. Tromer, and M. Virza, "Computational integrity with a public random string from quasi-linear PCPs," in *Advances in Cryptology—EUROCRYPT*, J.-S. Coron and J. B. Nielsen, Eds. Cham, Switzerland: Springer, 2017, pp. 551–579.

[120] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, 1978.

[121] J. K. Liu and D. S. Wong, "Linkable ring signatures: Security models and new schemes," in *Proc. Int. Conf. Comput. Sci. Appl.* Berlin, Germany: Springer, 2005, pp. 614–623.

[122] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2002, pp. 465–480.

[123] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Information Security and Privacy*, H. Wang, J. Pieprzyk, and V. Varadharajan, Eds. Berlin, Germany: Springer, 2004, pp. 325–335.

[124] S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18, Dec. 2016.

[125] P. Todd. *Stealth Addresses, Post on Bitcoin Development Mailing List*. Accessed: Nov. 11, 2019. [Online]. Available: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html

[126] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[127] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.

[128] Y. Zhao, J. Zhao, L. Jiang, R. Tan, and D. Niyato, "Mobile edge computing, blockchain and reputation-based crowdsourcing IoT federated learning: A secure, decentralized and privacy-preserving system," 2019, *arXiv:1906.10893*. [Online]. Available: https://arxiv.org/abs/1906.10893

[129] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.

[130] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334.

[131] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[132] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS Conf.*, vol. 48, 1979, pp. 313–317.

[133] J. Benet, "IPFS—Content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*. [Online]. Available: https://arxiv.org/abs/1407.3561

[134] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing bitcoin work for data preservation," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2014, pp. 475–490.

[135] J. Benet and N. Greco, "Filecoin: A decentralized storage network," Protocol Labs, San Francisco, CA, USA, Tech. Rep., 2018. [Online]. Available: https://filecoin.io/filecoin.pdf

[136] D. Irvine, "Maidsafe.net," U.S. Patent Appl. 12/476,229, Mar. 11, 2010.

[137] S. Wilkinson, T. Boshevski, J. Brandoff, J. Prestwich, G. Hall, P. Gerbes, P. Hutchins, and C. Pollard. (2018). *STORJ: A Peer-to-Peer Cloud Storage Network*. [Online]. Available: https://storj.io/storj.pdf

[138] D. Vorick and L. Champine, "Sia: Simple decentralized storage," Nebulous, Boston, MA, USA, Tech. Rep., 2014, vol. 8, p. 2018. [Online]. Available: https://assets.coss.io/documents/white-papers/siacoin.pdf

[139] V. Demianets and A. Kanakakis, *Distributed Ledger With Secure Data Deletion—Revision 1.4*. Stockholm, Sweden, 2016.

[140] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.

[141] S. ShoCard. (2016). *Travel Identity of the Future*. [Online]. Available: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf

[142] T. Hardjono and N. P. Smith. (2016). *Anonymous Identities for Permissioned Blockchains*. [Online]. Available: https://www.semanticscholar.org/paper/Anonymous-Identities-for-Permissioned-Blockchains-(-Hardjono-Smith/427b43258710b39ec65fe0d95f684f273009280d and https://arxiv.org/abs/1903.04584v1

[143] E. Brickell and J. Li, "Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 3, pp. 345–360, May /Jun. 2012.

[144] D. S. Baars, "Towards self-sovereign identity using blockchain technology," M.S. thesis, Dept. Elect. Eng., Math. Comput. Sci., Univ. Twente, Enschede, The Netherlands, 2016.

[145] D. Mulligan, "Know your customer regulations and the international banking system: Towards a general self-regulatory regime," *Fordham Int. Law J.*, vol. 22, no. 5, p. 2324, 1998.

[146] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. Secur. Privacy Workshops (SPW)*, May 2015, pp. 180–184.

[147] A. Yasin and L. Liu, "An online identity and smart contract management system," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Jun. 2016, pp. 192–198.

[148] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *Proc. SEC*, 2016, pp. 398–411.

[149] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput.*, May 2017, pp. 468–477.

[150] E. Androulaki, C. Cachin, A. De Caro, and E. Kokoris-Kogias, "Channels: Horizontal scaling and confidentiality on permissioned blockchains," in *Computer Security*, J. Lopez, J. Zhou, and M. Soriano, Eds. Cham, Switzerland: Springer, 2018, pp. 111–131.

[151] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[152] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[153] T. Kotka, C. I. V. A. del Castillo, and K. Korjus, "Estonian e-residency: Redefining the nation-state in the digital era," Univ. Oxford, Oxford, U.K., Tech. Rep., 2015, vol. 3, pp. 1–16. [Online]. Available: https://www.politics.ox.ac.uk/materials/publications/14883/workingpaperno3kotkavargaskorjus.pdf

[154] T. Kalvet and A. Aaviksoo. (2008). *The Development of Eservices in an Enlarged eu: Egovernment and Ehealth in Estonia*. [Online]. Available: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/development-eservices-enlarged-eu-egovernment-and-ehealth-estonia

[155] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations," *Transp. Res. A, Policy Pract.*, vol. 77, pp. 167–181, Jul. 2015.

[156] C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain based liability attribution framework for autonomous vehicles," 2018, *arXiv:1802.05050*. [Online]. Available: https://arxiv.org/abs/1802.05050

[157] K. Salah, M. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127–10149, 2019.

[158] H. Hasan and K. Salah, "Combating deepfake videos using blockchain and smart contracts," *IEEE Access*, vol. 7, pp. 41596–41606, 2019.

[159] K. Toyod, P. T. Mathiopoulo, I. Sasase, and T. Ohtsuk, "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

[160] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the Internet of money," in *Banking Beyond Banks and Money*. Cham, Switzerland: Springer, 2016, pp. 239–278.

[161] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun., IEEE 14th Int. Conf. Smart City, IEEE 2nd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2016, pp. 1392–1393.

[162] J. Sun, J. Yan, and K. Z. K. Zhang, "Blockchain-based sharing services: What blockchain technology can contribute to smart cities," *Financial Innov.*, vol. 2, no. 1, p. 26, 2016.

[163] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[164] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[165] A. Dorri, C. Roulin, R. Jurdak, and S. Kanhere, "On the activity privacy of blockchain for IoT," 2018, *arXiv:1812.08970*. [Online]. Available: https://arxiv.org/abs/1812.08970

[166] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.

[167] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *Proc. 2nd ACM Int. Workshop IoT Privacy, Trust, Secur.*, Xi'an, China, 2016, pp. 29–36.

[168] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Bhubaneswar, India, Dec. 2017, pp. 1–6.

[169] H. Lund, P. A. Østergaard, D. Connolly, and B. V. Mathiesen, "Smart energy and smart energy systems," *Energy*, vol. 137, pp. 556–565, Oct. 2017.

[170] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[171] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, 2018.

[172] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers," in *Proc. 7th Int. Conf. Internet Things (IoT)*, Linz, Austria, 2017, pp. 13:1–13:8.

[173] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "P2P mixing and unlinkable bitcoin transactions," in *Proc. NDSS Symp.*, San Diego, CA, USA, 2017, pp. 1–15.

[174] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2016.

[175] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PerCom Workshops)*, Kona, HI, USA, Mar. 2017, pp. 618–623.

[176] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[177] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. 2nd Int. Conf. Internet-Things Design Implement.*, Pittsburgh, PA, USA, 2017, pp. 173–178.

[178] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[179] B. Shabandri and P. Maheshwari, "Enhancing IoT security and privacy using distributed ledgers with iota and the tangle," in *Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Noida, India, Mar. 2019, pp. 1069–1075.

[180] U. Sarfraz, M. Alam, S. Zeadally, and A. Khan, "Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions," *Comput. Netw.*, vol. 148, pp. 361–372, Jan. 2019.

[181] (2017). *IOTA Mixer V1*. [Online]. Available: https://medium.com/iota-ucl/iota-mixer-91f3d39735c1

[182] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*, J. P. Buhler, Ed. Berlin, Germany: Springer, 1998, pp. 267–288.

[183] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 357–373, Mar. 2019.

[184] L. Tennant. (2017). *Improving the Anonymity of the IOTA Cryptocurrency*. [Online]. Available: https://pdfs.semanticscholar.org/490d/38d18dea9a61570ce4bc4cb8b1a3a7d527f2.pdf

[185] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Government Inf. Quart.*, vol. 34, pp. 355–364, Sep. 2017.

[186] "Blockchain and its suitability for government applications," U.S. Government, Public-Private Analytic Exchange Program, Washington, DC, USA, Tech. Rep., 2018. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/2018_AEP_Blockchain_and_Suitability_for_Government_Applications.pdf

[187] M. Jun, "Blockchain government—A next form of infrastructure for the twenty-first century," *J. Open Innov., Technol., Market, Complex.*, vol. 4, no. 1, p. 7, 2018.

[188] C. Alexopoulos, A. Androutsopoulou, Z. Lachana, M. A. Loutsaris, and Y. Charalabidis, "Blockchain technologies in government 3.0: A review," in *Proc. EGOV-CeDEM-ePart*, 2018, p. 11.

[189] A. Buldas, A. Kroonmaa, and R. Laanoja, "Keyless signatures' infrastructure: How to build global distributed hash-trees," in *Proc. Nordic Conf. Secure IT Syst.* Ilulissat, Greenland: Springer, 2013, pp. 313–320.

[190] A. Ojo and S. Adebayo, "Blockchain as a next generation government information infrastructure: A review of initiatives in D5 countries," in *Government 3.0—Next Generation Government Technology Infrastructure and Services*. Cham, Switzerland: Springer, 2017, pp. 283–298.

[191] S. Heiberg, I. Kubjas, J. Siim, and J. Willemson, "On trade-offs of applying block chains for electronic voting bulletin boards," Cryptol. ePrint Arch., Tech. Rep. 2018/685, 2018. [Online]. Available: https://eprint.iacr.org/2018/685

[192] Y. Wu, "An E-voting system based on blockchain and ring signature," M.S. thesis, School Comput. Sci., Univ. Birmingham, Birmingham, U.K., 2017. [Online]. Available: https://www.dgalindo.es/mscprojects/yifan.pdf

[193] P. Noizat, "Blockchain electronic vote," in *Handbook of Digital Currency*. Amsterdam, The Netherlands: Elsevier, 2015, pp. 453–461.

[194] Y. Takabatake, D. Kotani, and Y. Okabe, "An anonymous distributed electronic voting system using zerocoin," in *Proc. IA-Workshop Internet Archit. Appl.* Taipei, Taiwan: IEICE, 2016, p. 131.

[195] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Springer, 2017, pp. 357–375.

[196] F. S. Hardwick, R. N. Akram, and K. Markantonakis, "Fair and transparent blockchain based tendering framework—A step towards open governance," 2018, *arXiv:1805.05844*. [Online]. Available: https://arxiv.org/abs/1805.05844

[197] D. Allessie, M. Sobolewski, and L. Vaccari, "Blockchain for digital government: An assessment of pioneering implementations in public services," Joint Res. Centre, Seville Site, Brussels, Belgium, Tech. Rep. JRC115049, 2019.

[198] P. Schmidt, "Blockcerts—An open infrastructure for academic credentials on the blockchain," *ML Learn.*, to be published.

[199] P. Meessen and A. Sonnino, "D3.4 initial decentralised models for data and identity management: Blockchain and ABC MVPs," Decode H2020, Decode consortium, DECODE Project, Tech. Rep. H2020-ICT-2016-1, 2017.

[200] *Privacy-Enhancing Cryptography in Distributed Ledgers (Priviledge)*. Accessed: Nov. 11, 2019. [Online]. Available: https://priviledge-project.eu

[201] R. Neisse, G. Steri, and I. Nai-Fovino, "A blockchain-based approach for data accountability and provenance tracking," in *Proc. 12th Int. Conf. Availability, Rel. Secur.*, Reggio Calabria, Italy, 2017, p. 14.

[202] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A blockchain-based solution," 2019, *arXiv:1904.03038*. [Online]. Available: https://arxiv.org/abs/1904.03038

[203] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.

[204] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key requirements and challenges," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Ostrava, Czech Republic, Sep. 2018, pp. 1–7.

[205] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan./Feb. 2018.

[206] L. Cheng, J. Liu, C. Su, K. Liang, G. Xu, and W. Wang, "Polynomial-based modifiable blockchain structure for removing fraud transactions," *Future Gener. Comput. Syst.*, vol. 99, pp. 154–163, 2019.

[207] 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 Comput., Commun. Storage*. Cham, Switzerland: Springer, 2017, pp. 534–543.

[208] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.

[209] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, "Towards decentralized accountability and self-sovereignty in healthcare systems," in *Proc. Int. Conf. Inf. Commun. Secur.* Cham, Switzerland: Springer, 2017, pp. 387–398.

[210] C. Paquin and G. Zaverucha, "U-prove cryptographic specification v1.1," Microsoft, Redmond, WA, USA, Tech. Rep., 2011. [Online]. Available: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/U-Prove20Cryptographic20Specification20V1.1.pdf

[211] 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, May 2018.

[212] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. Syst. Secur.*, vol. 9, no. 1, pp. 1–30, 2006.

[213] 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," 2018, *arXiv:1811.03223*. [Online]. Available: https://arxiv.org/abs/1811.03223

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

[215] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: A blockchain-based platform for healthcare information exchange," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Taormina, Italy, Jun. 2018, pp. 49–56.

[216] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, Jul. 2018.

[217] D. Bender and K. Sartipi, "HL7 FHIR: An Agile and RESTful approach to healthcare information exchange," in *Proc. 26th IEEE Int. Symp. Comput.-Based Med. Syst. (CBMS)*, Porto, Portugal, Jun. 2013, pp. 326–331.

[218] C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri, and S. Jha, "B-FICA: Blockchain based framework for auto-insurance claim and adjudication," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Computing Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul./Aug. 2018, pp. 1171–1180.

[219] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," 2018, *arXiv:1802.00561*. [Online]. Available: https://arxiv.org/abs/1802.00561

[220] *IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages*, IEEE Standard 1609.2-2016, Mar. 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7426684

[221] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

[222] R. W. van der Heijden, F. Engelmann, D. Mödinger, F. Schönig, and F. Kargl, "Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication," in *Proc. 1st Workshop Scalable Resilient Infrastruct. Distrib. Ledgers*, Las Vegas, NV, USA, 2017, p. 4.

[223] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[224] F. Knirsch, A. Unterweger, G. Eibl, and D. Engel, "Privacy-preserving smart grid tariff decisions with blockchain-based smart contracts," in *Sustainable Cloud and Energy Services*. Cham, Switzerland: Springer, 2018, pp. 85–116.

[225] M. I. G. Vasco, F. Hess, and R. Steinwandt, "Combined (identity-based) public key schemes," *IACR Cryptol. ePrint Arch.*, vol. 2008, p. 466, Jan. 2008.

[226] *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, document ETSI TS 102 941 V1.1.1, 2018.

[227] G. Baldini, J. L. Hernández-Ramos, G. Steri, and S. N. Matheu, "Zone keys trust management in vehicular networks based on blockchain," in *Proc. Global IoT Summit (GIoTS)*, Aarhus, Denmark, Jun. 2019, pp. 1–6.

[228] E. Androulaki *et al.*, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Porto, Portugal, 2018, p. 30.

[229] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A blockchain based privacy preserving platform for healthcare data," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, Eds. Cham, Switzerland: Springer, 2017, pp. 534–543.

[230] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proc. ACM Conf. Comput. Commun. Secur.*, Raleigh, NC, USA, 2012, pp. 906–917.

[231] C. Decker and R. Wattenhofer, "Bitcoin transaction malleability and MtGox," in *Proc. Eur. Symp. Res. Comput. Secur.* Springer, 2014, pp. 313–326.

[232] D. Chaum, "Blind signatures for untraceable payments," in *Proc. Adv. Cryptol.* Boston, MA, USA: Springer, 1983, pp. 199–203.

[233] A. Greenberg. (2014). *'Dark Wallet' is About to Make Bitcoin Money Laundering Easier Than Ever*. [Online]. Available: http://www.wired.com/2014/04/dark-wallet

[234] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "CoinParty: Secure multi-party mixing of bitcoins," in *Proc. 5th ACM Conf. Data Appl. Secur. Privacy*, San Antonio, TX, USA, 2015, pp. 75–86.

[235] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, "Sybil-resistant mixing for bitcoin," in *Proc. 13th Workshop Privacy Electron. Soc.*, Scottsdale, AZ, USA, 2014, pp. 149–158.

[236] H. Corrigan-Gibbs and B. Ford, "Dissent: Accountable anonymous group messaging," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, Chicago, IL, USA, 2010, pp. 340–350.

[237] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *J. Cryptol.*, vol. 1, no. 1, pp. 65–75, 1988.

[238] G. Maxwell. *Confidential Transactions*. [Online]. Available: https://people.xiph.org/%7Egreg/confidential_values.txt

[239] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1991, pp. 129–140.

[240] S. Meiklejohn and R. Mercer, "Möbius: Trustless tumbling for transaction privacy," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 2, pp. 105–121, 2018.

[241] T. E. Jedusor. (2016). *Mimblewimble*. [Online]. Available: https://scalingbitcoin.org/papers/mimblewimble.txt

[242] A. Poelstra. (2016). *Mimblewimble*. [Online]. Available: https://github.com/apoelstra/mimblewimble-paper

[243] L. Xu, N. Shah, L. Chen, N. Diallo, Z. Gao, Y. Lu, and W. Shi, "Enabling the sharing economy: Privacy respecting contract based on public blockchain," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts*, 2017, pp. 15–21.

[244] M. Campanelli, R. Gennaro, S. Goldfeder, and L. Nizzardo, "Zero-knowledge contingent payments revisited: Attacks and payments for services," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2017, pp. 229–243.

[245] C. Gentry and D. Wichs, "Separating succinct non-interactive arguments from all falsifiable assumptions," in *Proc. 43rd Annu. ACM Symp. Theory Comput.*, San Jose, CA, USA, 2011, pp. 99–108.

[246] H. Gunasinghe, A. Kundu, E. Bertino, H. Krawczyk, S. Chari, K. Singh, and D. Su, "PrivIdEx: Privacy preserving and secure exchange of digital identity assets," in *Proc. World Wide Web Conf. (WWW)*, New York, NY, USA, 2019, pp. 594–604.

[247] Civic Technologies. (2017). *Civic White Paper*. [Online]. Available: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf

[248] (2018). *Plenum: Byzantine Fault Tolerant Protocol*. [Online]. Available: https://github.com/hyperledger/indy-plenum/wiki

[249] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," 2015, *arXiv:1506.03471*. [Online]. Available: https://arxiv.org/abs/1506.03471

[250] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[251] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger approaches," *IEEE Access*, vol. 7, pp. 89948–89966, 2019.

[252] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. (2014). *Enabling Blockchain Innovations With Pegged Sidechains*. [Online]. Available: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains

JOSE LUIS CANOVAS received the B.S. and M.Sc. degrees in computer science and the B.S. degree in mathematics from the University of Murcia, in 2017. He is a Research Fellow with the Department of Information and Communications Engineering, University of Murcia. His research interests include security and privacy technologies for the Internet of Things.

JOSE L. HERNANDEZ-RAMOS received the Ph.D. degree in computer science from the University of Murcia. He is currently a Scientific Project Officer with the Joint Research Centre of the European Commission. His research interests include the application of security and privacy mechanisms in the Internet of Things and transport systems scenarios. He has coauthored over 40 research articles in international conferences and journals. He has participated in FP7 and Horizon 2020 European research projects, such as SocIoTal, SMARTIE, or SerIoT, and has served as a TPC and chair member for different international conferences.

RAFAEL TORRES MORENO received the B.S. and M.Sc. degrees in computer science from the University of Murcia, in 2017, where he is currently pursuing the Ph.D. degree. He is also a Research Fellow with the Department of Information and Communications Engineering, University of Murcia. He has been a Visiting Researcher with IBM, Zurich. He has participated in H2020 EU research projects, such as Olympus. His research interests include security and privacy-preserving technologies applicable in decentralized systems.

JORGE BERNAL BERNABE received the B.S., M.S., and Ph.D. degrees in computer science and the M.B.A. degree from the University of Murcia, Murcia, Spain. He is currently a Postdoctoral Researcher with the Department of Information and Communications Engineering, University of Murcia. He has been a Visiting Researcher with the Cloud and Security Lab, Hewlett-Packard Laboratories, Bristol, U.K. He has authored several book chapters and more than 40 articles in international top-level conferences and journals. He has been involved in the scientific committee of numerous conferences and served as a reviewer for multiple journals. During the last years, he has been working in several European research projects FP6, FP7, and H2020, such as DESEREC, Semiramis, Inter-Trust, SocIoTal, ARIES, OLYMPUS, and CyberSec4EU. His scientific activity is mainly devoted to the security, trust, and privacy management in distributed systems. He is also interested in security and privacy aspects of the Internet of Things. He received the Best Ph.D. Thesis Award from the School of Computer Science, University of Murcia.

ANTONIO SKARMETA received the B.S. degree (Hons.), the M.S. degree in computer science from the University of Granada, Granada, Spain, and the Ph.D. degree in computer science from the University of Murcia, Murcia, Spain. He has been the Head of the Research Group, ANTS, since its creation in 1995. Since 2009, he has been a Professor at the University of Murcia, Murcia. He is also an Advisor to the Vice Rector of Research with the University of Murcia, for international projects, and the Head of the International Research Project Office. Since 2014, he has been the Spanish National Representative for the MSCA within H2020. He has published over 200 international articles and has been a member of several program committees. His research interests include integration of security services, identity, the IoT, and smart cities. He has also participated in standardization for IETF, ISO, and ETSI. He has worked on different research projects in the national and international area in the networking, security, and the IoT area, like Euro6IX, ENABLE, DAIDALOS, SWIFT, SEMIRAMIS, SMARTIE, SOCIOTAL, and IoT6.

• • •