Future Generation Computer Systems 124 (2021) 91–118

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Achieving cybersecurity in blockchain-based systems: A survey

Mar Gimenez-Aguilar [a,*], Jose Maria de Fuentes [a], Lorena Gonzalez-Manzano [a], David Arroyo [b]

[a] Computer Security Lab (COSEC), Universidad Carlos III de Madrid, Spain
[b] Institute for Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC), Spain

ARTICLE INFO

Article history:
Received 17 December 2020
Received in revised form 21 April 2021
Accepted 6 May 2021
Available online 27 May 2021

Keywords:
Blockchain
Cybersecurity

ABSTRACT

With the increase in connectivity, the popularization of cloud services, and the rise of the Internet of Things (IoT), decentralized approaches for trust management are gaining momentum. Since blockchain technologies provide a distributed ledger, they are receiving massive attention from the research community in different application fields. However, this technology does not provide with cybersecurity by itself. Thus, this survey aims to provide with a comprehensive review of techniques and elements that have been proposed to achieve cybersecurity in blockchain-based systems. The analysis is intended to target area researchers, cybersecurity specialists and blockchain developers. For this purpose, we analyze 272 papers from 2013 to 2020 and 128 industrial applications. We summarize the lessons learned and identify several matters to foster further research in this area.

© 2021 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

Nowadays, Internet connectivity is being offered in an increasing amount of places. The widespread use of cloud technologies and connected devices has enabled new forms of data and computation outsourcing, along with the irruption of the so called Internet of Things (IoT). Besides the explosion of IoT devices, network technologies are also evolving very fast. Speed and reliability of networks are continuously improving, thus enabling a permanent connectivity of devices as it happens with the recently developed 5G technology [1].

Both the increase of devices and the improvement of technologies have motivated the raise of decentralization approaches for many scenarios. Thus, instead of relying on a single device or entity, it is common to provide services and resources as a result of the collaboration among multiple communication nodes.

In what comes to cybersecurity of computer systems, one of the main concerns is where to put the trust. If a given application needs to manage sensitive information, it is usually solved by protecting a given node or device. Although this solution is cost-effective (only one resource needs to be protected), it also involves the single point of failure risk [2]. Thus, if the node is compromised, the whole cybersecurity is threatened. Thanks to decentralization, the likelihood of success of a cyber-attack can be reduced. In this vein, blockchain technologies offer a decentralized storage in which data can be securely stored without the need of any single trusted party [3]. Information is managed through a distributed ledger in which data is consecutively appended to existing records. Remarkably, nodes maintaining the ledger do not need to be mutually trusted, which promotes its application in trustless scenarios [4].

Blockchain technologies have already been applied in many different scenarios. For example, Bitcoin and many other cryptocurrencies leverage blockchains, in such a way that any economic transaction is appended as a new record. Every node connected to the network is able to verify that a given amount of funds have been transferred, thus preventing the overspending problem (i.e., that the payer uses the same coin in two or more payments) [5]. Thus, blockchains open up a vast array of novel applications and production models (e.g., social manufacturing [6]).

The increasing protagonism of blockchain technologies is attracting attention from both industry and academia. However, the frenetic pace of evolution can make this technology seem the Swiss knife for every new approach, thus leading to improper uses. Moreover, many related efforts can be carried out in parallel, resulting in overlapping approaches. Both issues can threat the widespread adoption of this technology.

Despite these concerns, in the last years we have witnessed a myriad of contributions focused on achieving cybersecurity when blockchain technologies are at stake. This trend calls for a systematic review of approaches to set the boundaries on suitable uses, current state of the art and open research and development areas. Cryptographic experts such as Bruce Schneier have already identified an unjustified hype surrounding this technology, by pointing out its limitations — *"A blockchain probably does not solve the security problems you think it solves. The security problems it*

* Corresponding author.
E-mail address: mgimenez@inf.uc3m.es (M. Gimenez-Aguilar).

https://doi.org/10.1016/j.future.2021.05.007
0167-739X/© 2021 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

solves are probably not the ones you have." [7]. Therefore, although blockchains provide with *some* cybersecurity guarantees, they cannot be regarded as a holistic solution.

To clarify how cybersecurity are achieved when blockchains come into play, in this paper we aim to analyze the proposed approaches in this regard. Note that we are not interested in the internal cybersecurity problems of blockchain technologies, which have already been explored [8]. Other surveys have already performed systematic literature reviews on blockchain-based applications, but without focusing on its use to provide cybersecurity [9]. Thus, the contributions of this paper are the following ones:

- A systematic review of 272 papers (between 2013 and 2020) and 128 business initiatives to analyze how cybersecurity are achieved when blockchain is at stake.
- A taxonomy of elements involved in the proposed analysis, namely cybersecurity properties, techniques per property, areas, technologies and the justified use of blockchains.
- Identification of lessons learned to point out relevant research issues to foster further works in this direction.

Paper organization. Due to its broad scope, this paper is addressed to a wide audience. Fig. 1 shows the different sections and points out those addressed to a particular profile. In particular, Section 2 introduces the background of blockchain technologies and cybersecurity. Section 3 describes the applied research methodology. As introduced therein, there are five research questions at stake. Concretely, Section 4 addresses academic approaches and tackles four research questions, three of them relevant for specific reader profiles. On the other hand, Section 5 focuses on a research question related to industrial approaches. Once the core of the analysis has been shown, Section 6 summarizes the lessons learned and points out future research issues. Afterwards, related works are compared in Sections 7 and 8 concludes the paper.

2. Background

In this Section, the main concepts of cybersecurity and blockchains are introduced. In particular, the foundations of blockchain technologies are presented in Section 2.1. Afterwards, in order to simplify the presentation of concepts in the analysis of the literature, a unified model of blockchain technologies is presented in Section 2.2. Last but not least, the main goals of cybersecurity are described in Section 2.3.

2.1. Blockchain overview

Blockchain technologies enable having a distributed ledger in which data is appended [10]. One important matter is that there is no need for a single, centralized trusted party — trust is distributed among all nodes. Therefore, in order to add data to the ledger, a consensus is usually needed to be reached among all (or a qualified portion of) involved nodes [11].

In order to provide with a general overview, blockchains can be classified depending on their nature and their underlying technology. Each of these issues is introduced below.

Nature

There are two factors that determine the nature of a blockchain, namely their access control and their data validation policy. Concerning access control, they can either be public, where everyone can join freely, or private, where only selected members can take part. With respect to the validation policy, it is related to the way in which the nodes allowed to update the ledger (called *miners* in the case of proof-of-work based blockchains, and validators from a general point of view) are chosen. Thus, blockchains in which any node can be a validator are called "permissionless", whereas those where only a specified set of users can take this role, are referred to as "permissioned".

Technologies

There are three blockchain technologies that are widely used. Bitcoin was the first cryptocurrency and also the first technology to build a blockchain. Proposed by Satoshi Nakamoto in 2008, it allows two parties to send transactions between each other without the involvement of a third one. It has a non-Turing-complete scripting language which supports different advanced features, such as the use of timelocks to prevent the execution of a given action before a deadline. Considering previous classification parameters, Bitcoin is a public permissionless technology.

On the other hand, Ethereum was released in 2015 and allows the execution of smart contracts. These are software artifacts that are executed by Ethereum nodes through its Ethereum virtual machine. They are written in specific languages such as Solidity or Serpent and then compiled into bytecode. Ethereum's main network is public [12,13].

Finally, the Hyperledger Project consists of a community of software developers building blockchain frameworks and platforms. It was announced at the end of 2015 by the Linux Foundation. There are different blockchain technologies included in this project, like Hyperledger Fabric or Hyperledger Iroha [14]. Among them, probably the most used is Hyperledger Fabric [15], which is a blockchain framework intended as a foundation for developing applications or solutions with a modular architecture. In this case, it is typically oriented towards private permissioned networks and it allows different consensus algorithms. Smart contracts written in Go, node.js or Java, can be executed and are called chaincodes [16].

2.2. Blockchain model

There are several entities or elements at stake when it comes to maintaining and using a blockchain (Fig. 2). On the one hand, there are a set of nodes (referred to as Blockchain Nodes, BCN) that are in charge of keeping the blockchain information itself, which could be either in clear or encrypted. Then, they cooperate to update blockchain data based on a consensus algorithm. Consensus is typically reached among a subset of BCNs. Indeed, data to be included in the blockchain is proposed by one of the BCNs. Such node is either chosen in a deterministic way or randomly validated based on some established mechanism. Therefore, the so called miners (which are not present in all types of blockchains), are a subset of BCNs.

Apart from BCNs, there is always another entity that comes into play — Blockchain Users (BCUs). BCUs are willing to insert information into the blockchain. Let us consider a hospital that manages clinical reports through a blockchain. Whereas BCNs will be nodes from the hospital taking care of the data, BCUs can be tablet devices held by doctors which send updated health results to be stored in the blockchain. In another setting, two BCUs that are cooperating may want to record the status of their transactions. For example, BCU_1 offers a service and BCU_2 wants to pay for it. Both of them will use the blockchain to store offers and payments, respectively.

Blockchain Observers (BCOs), on the other hand, are those users of the blockchain that gain something, by only retrieving the data present in the blockchain or by observing it. They do not contribute to the blockchain by adding data themselves. However, their retrieval might be recorded in the blockchain by means of a transaction or a interaction with a smart contract. For example,

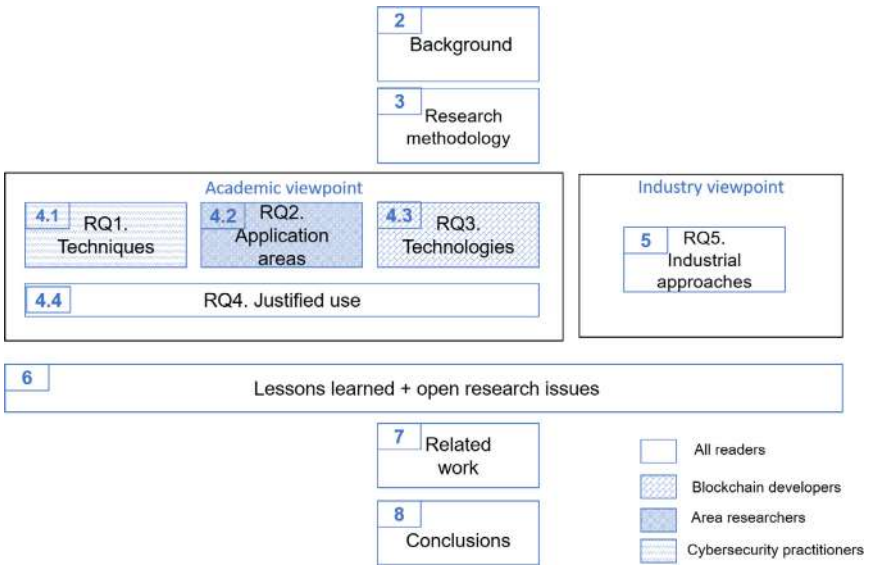

Fig. 1. Paper organization and intended audiences.

in [17] a transaction must be sent to the blockchain for data retrieval in order to check permissions and deliver information accordingly. Following the hospital case, patients (or insurance companies) are BCOs as long as they only want to see health information. This can be also the case of auditors of different systems, third companies buying or analyzing data, users retrieving their own data by using the blockchain as storage when IoTs are involved, etc.

Given that BCNs are, *de facto*, the only nodes having direct access to the blockchain, both BCUs and BCOs should trust them in that the information purportedly stored in or retrieved from the blockchain is the one that is being exchanged. However, no BCN is assumed to be trusted — any attempt to alter blockchain information will be mitigated by the underlying consensus protocol or access control/permission mechanisms in force. To further prevent mistrust, BCNs count on incentives such as rewards per successful transaction inserted in the ledger.

Moreover, as storing information in the blockchain is usually expensive and conveys scalability concerns [18] some additional storage (AS) in the form of cloud storage or Distributed Hash Tables (DHT), for example, could be used for this purpose [19]. In this case, blockchain vouches for data integrity and auditability by performing data anchoring, i.e., by storing in the ledger pointers to the data and the corresponding time stamping [20].

In addition, in some blockchain systems there are other software and hardware elements to provide all required capabilities. This is the case of extra hardware or off-chain software components. These elements are called Additional Infrastructure (AI).

2.3. Cybersecurity goals

According to the US National Institute of Standards and Technology (NIST), cybersecurity is defined as the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation" [21]. Therefore, cybersecurity is indeed a generic name that refers to the aforementioned five security dimensions, that will be defined in the following.

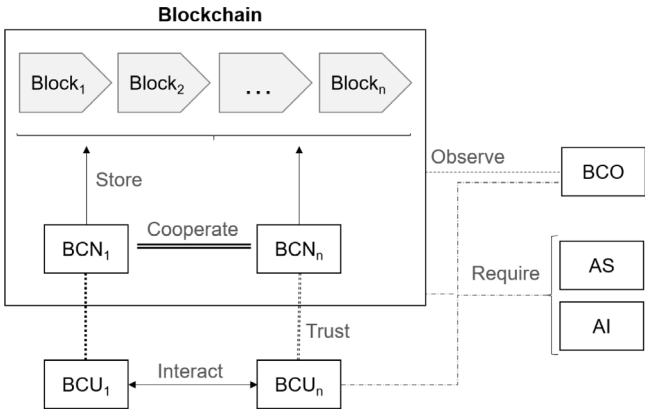

Fig. 2. Blockchain entities model.

Authentication refers to "the process of establishing confidence in the identity of users or information systems" [22]. As opposed to integrity, confidentiality and non-repudiation, this feature is related to system stakeholders and not to the data at stake.

With respect to confidentiality, it refers to the fact that "sensitive information is not disclosed to unauthorized entities" [22]. This matter is not provided by blockchain technologies by design, as soon as they have been designed to provide auditability, that is, enabling any party to verify the data contained therein.

Concerning non-repudiation, it corresponds to the "protection against an individual falsely denying having performed a particular action" [22]. Due to the large amount of potential actions that can be devised into an IT system, variants of this feature have appeared such as sender or receiver non-repudiation. In particular, sender non-repudiation is also essential in some blockchain use cases such as cryptocurrencies to avoid the double-spending problem [5]. Indeed, blockchains already provide with sender non-repudiation mechanisms via digital signatures.

A special situation happens with the remaining pair of cybersecurity features. On the one hand, availability is defined as "ensuring timely and reliable access to and use of information" [21]. Regarding availability, it is necessary to recall Brewer's CAP theorem — it is very complex to achieve consistency, availability and partitioning as a whole. Thus, for the sake of simplicity

we assume that availability is provided to some extent when blockchains come into play. On the other hand, integrity is "a property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored" [23]. In this survey, each cybersecurity property will be addressed separately, since each blockchain-based proposal may provide some of them. However, in the case of integrity, it is an intrinsic property of the blockchain technology itself. Therefore, the mere use of this technology provides integrity.

2.4. Actual need for blockchains

Blockchain is an emerging technology and its use has been steadily increasing over the years. However, sometimes its use can be unjustified. According to Greenspan [24], there are eight criteria that must be met in order to ensure that blockchains are suitable for a given use case:

- Need for a shared database, including a set of transactions forming a ledger.
- Existence of multiple writers willing to insert data to the said database.
- Inter-writer mistrust, so each writer is not willing to allow any peer to edit its entries.
- Disintermediation, so writers are not willing to give a third party full control over the database.
- Transaction interaction, so there is a certain undeniable link between transactions.
- Transaction verifiability, so each transaction can be accepted under a set of (automatically verifiable) requirements.
- Existence of validators, that is, nodes that verify transactions.
- Storing value, so each entry represents something that has real-world value.

3. Research methodology

In order to ensure the validity of our survey and its repeatability, the Typical Systematic Review Stages proposed in [25] have been followed. For the sake of clarity related phases have been grouped together, resulting in the following set of steps:

1. Identify and define the question this survey intends to address.
2. Determine and search the relevant studies regarding the previous question.
3. Identify those studies that meet the criteria.
4. Extract and synthetize the findings from the studies.
5. Write a report and consider potential effects.

Each of these steps are introduced below, with the exception of the latter which is indeed materialized in this manuscript.

3.1. Identify and define the question

The purpose of this paper is to analyze how cybersecurity has been tackled when blockchain technologies are at stake. So, the main question is: *Which mechanisms or techniques have been proposed to achieve cybersecurity in blockchain-based systems?* In order to answer this general question, a set of more concrete matters are identified:

1. RQ1. Which techniques have been adopted to achieve cybersecurity?
2. RQ2. In which application areas have cybersecurity been achieved assisted by blockchains?
3. RQ3. Which are the blockchain technologies that have been more/less combined with cybersecurity?
4. RQ4. Is there any evidence of unjustified use of this technology for cybersecurity in academic papers?
5. RQ5. How is the industry approaching the application of blockchains for cybersecurity?

Each of the aforementioned questions is targeted to a different audience profile (recall Fig. 1). In particular, RQ1 is relevant for cybersecurity practitioners, whose interest lies on the concrete details of the techniques that turn a blockchain-based system into a cybersecurity solution. On the other hand, RQ2 is interesting for researchers working on the provision of advanced services in a given topic area (e.g., IoT). In this case, they are not willing to know the internal, low-level description of the mechanisms but, the set of provided cybersecurity that if often guaranteed/provided for each one. RQ3 is interesting for blockchain developers as they want to spot which design decisions have received more attention and which ones are subject to further research. Last but not least, RQ4 and RQ5 are interesting for a general audience in order to know the real advancement from both academic and industrial perspectives. In order to provide with a more complete understanding of the matter, the evolution of each of these issues over time is considered as well. The only exception lies in industrial applications since it is not always possible to set their creation date.

3.2. Determine and search the relevant studies regarding the previous questions

The set of papers at stake is formed by both journal and conference/workshop papers. Due to the huge amount of publications in the last couple of years (2019 and 2020), the methodology for selecting academic papers published in these years is slightly different from the previous ones.

DBLP database [26] is considered to retrieve all manuscripts. Only contributions published in top venues are taken into consideration. Thus, only papers published in the first quartile of Computer Science in the Journal Citation Reports ranking [27] are at stake. Concerning conferences, those ranked in class A of the GII-GRIN-SCIE ranking [28] are selected. On the other hand, Google Scholar has been considered to filter out those papers with 100 citations or more. This promotes that papers that have not been published in the said venues, but are relevant for the research community, become part of the sample. However, this issue is not considered in 2019 and 2020 because of the little time for them to achieve a high number of citations.

The following query has been developed to filter out relevant contributions based on their title:

(Blockchain OR Bitcoin OR Hyperledger OR Ethereum OR Solidity) AND (contract OR secur OR priva* OR accountab* OR anonym* OR authentic* OR confident* OR identity OR access* OR trust* OR distributed OR encrypt* OR hash OR cryp* OR DDoS OR malware OR anomal* OR avail*) AND NOT (survey OR (literature AND review))*

The query above ensures that the main cybersecurity terms are considered, even in different forms. After this step, a total of 506 journal and conference papers were retrieved. Note that not all the used databases allow such a query. In such cases, it has been transformed into an equivalent set of queries using the allowed operators.

3.3. Identify those studies that meet the criteria

Once the initial amount of proposals is automatically retrieved, a manual review is carried out. This ensures that those papers that are not relevant for the sample (e.g., other literature surveys) or that do not contain any particular application for cybersecurity (e.g., smart contracts design related papers) are filtered out. After this analysis, the sample is definitely formed by 272 articles — 166 journal papers and 106 conference/workshop papers.

3.4. Extract and synthesize the findings from the studies

The chosen proposals are studied in detail, classifying them according to different features. In the case that a certain proposal fits into more than one category per feature, (e.g., belonging to IoT and Health areas), it is counted in each of them. Four aspects have been analyzed in each proposal, namely the offered cybersecurity properties and techniques, the application area, the underlying blockchain technology and the justification of using a blockchain. This classification, depicted in Fig. 3, will be used as the basis for the following analysis.

4. Academic approaches

In this section, all papers are analyzed to answer the proposed research questions related to academic approaches — RQ1 to RQ4 (recall Section 3.1). In particular, Section 4.1 answers RQ1 by explaining how cybersecurity properties are fulfilled and which techniques provide them. Afterwards, Section 4.2 answers RQ2 describing the areas in which blockchain-based systems have been applied to achieve cybersecurity. Section 4.3 analyzes the use of blockchain technologies and implemented cybersecurity properties to answer RQ3. Finally, Section 4.4 answers RQ4 by studying whether the use of blockchain technologies is justified in each proposal. For the sake of clarity, a table supporting this study is included in Appendix.

4.1. Cybersecurity properties and related techniques

Cybersecurity properties defined in Section 2.3 are individually analyzed. Three categories are considered for each property — whether it is fully, partially or not provided. Fig. 4 summarizes the provision of each property over time. The different techniques applied to provide them are also introduced.

Authentication

Authentication is studied considering all blockchain entities (recall Section 2.2).

- Complete authentication: All entities are always authenticated. To do so, a Certification Authority (CA) can be used [29,30]; the user can be registered or included in a private network (in which at least the administrator of the network knows his/her identity) [31,32]; roles can be assigned accordingly [33,34]; some off-chain communication or registration system can be applied [35]; or a unique public identifier can be used for authentication purposes [36].
- Partial authentication. Not all entities are authenticated. This occurs in [37], where vendors and system operators are publicly known but the system user is not. Other example is [38] where nodes within the same group know the identity of each other, but they do not know the nodes outside the group.
- No authentication. Authentication is not provided in any way or it is not mentioned, such as in [39,40].

On the other hand, the following techniques are commonly applied for authentication purposes:

- CA/Authority. Some proposals provide authentication by means of a CA or other similar entity (e.g. governments, Key Generation Centers, Attribute Grant Unit, etc.). These authorities usually grant the requester an identifying item (e.g., certificates, keys, roles/attributes). Proposals like [41–43] are included in this category.
- Registration/Pre-enrollment. Some works need participants to be registered in the system beforehand. This is the case of proposals using a private blockchain, in which only specific entities are able to join and have to be known or approved beforehand, by, for example, the blockchain administrator [44,45]. On the other hand, some works based on pre-existing public blockchain networks (e.g. Ethereum main network) need BCUs, BCOs and/or BCNs to register in the system before using it [46,47].
- Off-chain. Authentication is carried out outside of the blockchain. For example, in [48] the user needs to know the service identity to generate the compound identity. This identity is shared among two or more parties, where at least one becomes owner and the rest have restricted access (become guests) [48].
- Blockchain transaction/Smart contract. A transaction in the blockchain or the smart contract (or equivalent) is used to authenticate the different entities, e.g. [32,49].
- Public identifier. A unique public attribute is used. This is the case of [50] in which the DNS name is used, or [51] where the artist profile is linked to an Ethereum address [51].
- Other. Another method is used for authentication purposes. For instance, [52] uses biometric data to provide authentication and a token is applied in [53].

The use and need of authentication in blockchains has increased since 2014 (recall Fig. 4), when this feature was initially offered. In the following years, this number has increased and complete authentication is provided in around 67% of proposals in the last three years. Thus, the ratio has remained quite constant in the last years and it could be related to the appearance and raise of private and permissioned networks, versus the initial public permissionless ones (e.g., Bitcoin).

In terms of techniques (Table 1), in 2014 and 2015 authentication was provided off-chain. In the following years, the preferred method is registration/pre-enrollment. This technique could have a lot to do with the increase of private networks. Moreover, it is a significantly easy way to manage access control, as it has been used for many years now. Similarly, the use of an authority or trusted third party is also a common easy way to provide authentication even outside of blockchain systems. Indeed, the use of trusted third parties is a widespread solution to solve security issues, although these entities become a single point of failure. However, the use of these trusted entities has significantly decreased in 2020, trying to look for completely decentralized approaches.

Non-repudiation

Non-repudiation is studied considering all blockchain entities in the system, analyzing how it is provided.

- Complete non-repudiation: Actions of all entities are recorded in the blockchain, e.g. [54,55]. Blockchain technologies already provide some kind of non-repudiation by means of digital signatures.
- Partial non-repudiation. A low number of actions of some entities, e.g. BCOs, are not logged in the system. This occurs in [56,57] where the audit process is not recorded in the system. This could lead to entities denying having performed an action (e.g. the audit process).

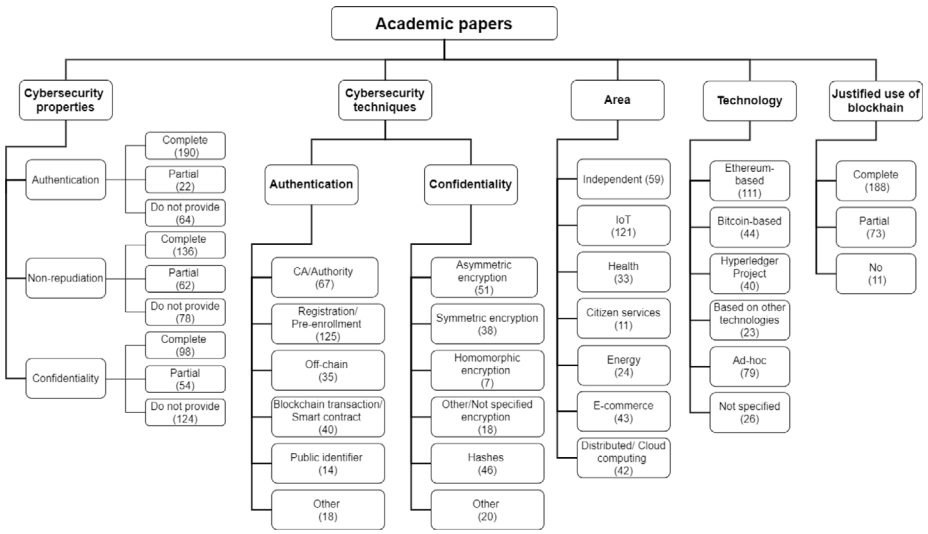

Fig. 3. Taxonomy of elements involved in the analysis. Numbers in brackets correspond to the amount of proposals that fit in each category.

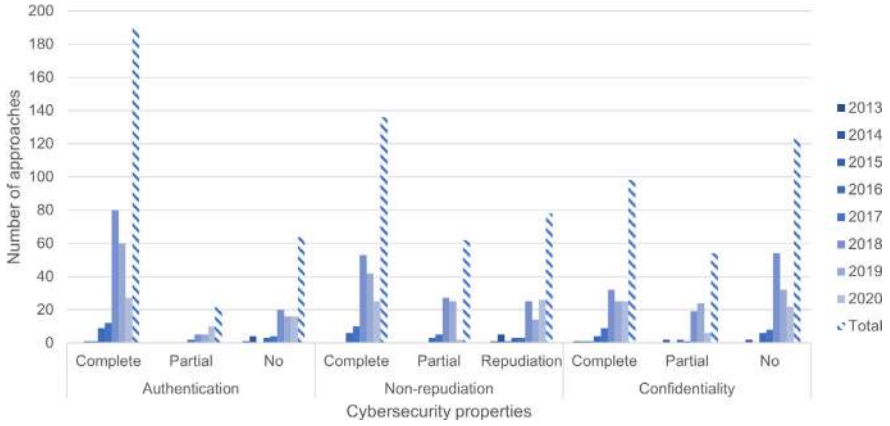

Fig. 4. Number of approaches regarding cybersecurity properties per year.

Table 1
Number of approaches regarding cybersecurity techniques per year.

	2013	2014	2015	2016	2017	2018	2019	2020	Total
Authentication									
CA/Authority	0	0	0	2	6	31	25	3	67
Registration/Pre-enrollment	0	0	0	5	9	51	47	13	125
Off-chain	0	1	1	3	3	10	5	12	35
Blockchain transaction/smartcontract	0	0	0	1	4	20	10	5	40
Public id.	0	0	0	2	4	0	7	1	14
Other	0	0	0	1	0	9	6	2	18
Confidentiality									
Asymmetric encryption	0	0	0	2	5	13	18	13	51
Symmetric encryption	0	0	1	2	0	8	12	15	38
Homomorphic encryption	0	0	0	0	1	1	5	0	7
Other/Not specified encryption	0	1	0	0	1	10	3	3	18
Hashes	0	0	1	1	1	17	15	11	46
Other	1	1	0	1	2	5	6	4	20

- Repudiation. Entities can deny having done actions or there is not much information to infer this issue, e.g. [58,59].

All proposals between 2013 and 2015 do not provide non-repudiation, see Fig. 4. From 2016 onwards, proposals provide complete non-repudiation in 50% of the cases or more and partial in around 25%. Despite the growth in the amount of papers, the ratio remains almost constant, except for 2020 in which it has decreased. The provision of some kind of non-repudiation is specially appropriate to look for better traceability and auditing processes.

Concerning applied techniques, non-repudiation is achieved in a simple way. Either all actions of the different elements in the

system are recorded in the blockchain or not. Logging is the only identified technique to achieve this cybersecurity property.

Confidentiality

Confidentiality is analyzed within the blockchain network, thus assessing whether the content of a message within the network is only accessible to authorized entities.

- Complete confidentiality. Only selected entities are able to know information from other entities, though there are elements inherent to the blockchain operation that are public and cannot be hidden, such as block headers [60]. This property is offered, for instance, in [61,62], where the block content is encrypted; or in [63,64], where hashes are the only interchanged data.
- Partial confidentiality. Some information is accessible to a particular set of entities while other data is public or can be used to infer additional information. For instance, in [65], which proposes a voting system using blockchain, votes are encrypted but the registration content is not. [66] proposes a similar approach, in which users' data is encrypted, but cloud service providers, token and resource addresses are not.
- No confidentiality. The content is public to all entities that interact with the blockchain, such as [41,67].

Confidentiality is achieved by encrypting transactions' content mainly, sharing only hashes of information and some other special cases. As different types of cryptographic algorithms are applied, different techniques are distinguished.

- Asymmetric encryption. It is also referred as public-key cryptography. It uses a pair of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner [68]. Different approaches use this kind of encryption. [69,70] use asymmetric encryption to encrypt the blockchain content.
- Symmetric encryption. In this case, the same key is used for encryption and decryption purposes. This key, also called secret key, is usually shared beforehand. It is also possible to derive the secret key based on assorted parameters. [44,47] use symmetric key algorithms to encrypt exchanged data.
- Homomorphic encryption. It is a special kind of encryption that allows performing calculations over encrypted data. It is adopted in some cases as a means to protect privacy and, implicitly, confidentiality. Proposals like [71,72] use this type of encryption.
- Other/Not specified encryption. Proposals that use other encryption types and those works in which the type is unknown are included in this category. For example, [73] uses secure certificateless multireceiver encryption which allows the sender to generate the same ciphertext for a chosen group of receivers solving the certificate management problem, while in [74] the type of encryption is not specified.
- Hashes. A hash is the result of applying a cryptographic non-reversible function, called hash function. They are usually used as indexes or as proofs of integrity because hash values are identical when applied over the same data. Hashes can be identified as pseudorandom numbers or strings with no meaning and they do not provide information by themselves. For example, in [64] and [75] document hashes are stored in the blockchain.
- Other. Any other technique is used to provide confidentiality. For example, [76] leverages additive secret sharing. Thus, the Key Distribution Center distributes n shares, derived from the requester secret key, to each user. Then, each user adds a share to contribute on blinding a given piece of data. All subsequent operations are performed on blind data. Finally, the impact of the share on the aggregated result can be eliminated by recovering the requester secret key.

Analyzing the trend over the years (recall Fig. 4), confidentiality is specially considered since 2017. However, less than half of the proposals provide it completely and a big fraction do not care about confidentiality. This may be reasonable as the need for this property may depend on the type of data at stake, e.g. health data should be considered confidential. By contrast, if some authentication and non-repudiation techniques are in place and a private network is applied, some level of confidentiality protection is achieved, despite not using encryption.

Considering the different techniques (Table 1), in 2013, the only work that falls into the 'other' category uses a mixing service and a coin distribution service to change the transmitted amount of money. In 2014, hashes, encryption and 'other' techniques are equally applied. In 2015, symmetric encryption was used, but from that year onwards, authors prefer the asymmetric one in most cases, following by only sharing hashes. The use of encryption is the most common way to provide confidentiality, regardless of the use of blockchains. Moreover, asymmetric encryption seems to be more appropriate in a distributed environment as there is no need to share decryption keys privately. Thus, in the last three years, in which confidentiality techniques have been specially applied, asymmetric, symmetric encryption and hashes are the most common alternatives.

4.2. Application areas and cybersecurity purposes

In this work seven areas are distinguished based on the content and goals of studied proposals:

- IoT: Internet of Things (IoT) is defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) devices based on interoperable information and communication technologies [77]. All proposals that suggest the use of blockchain in relation to IoT are included in this area. Devices/elements could be smartphones [78,79]; smart homes or related equipments [44,80]; sensors [32,81]: vehicles [30,41,82] or some other resource-constrained and potentially portable devices.
- Distributed/Cloud computing: Distributed computing is a system whose components are located on different networked computers, which communicate and coordinate their actions by passing messages to one another [83]. Cloud computing refers to the on-demand delivery of computer power, database storage, applications and other IT resources [84]. This could be used to increase the storage or computing power of a given system or application. In this category all kind of parallel, distributed and cloud computing systems are included. A special case of cloud computing is secure multiparty computation, which is used to increase data security by computing cryptographic operations, while keeping some data private [40,40,85].
- E-commerce: It focuses on the trade of goods via online services or over the Internet. Some common cases in this area are fair trade or fair lottery [40,86]; as well as the relevance of user security when buying or trading online [35,71,87,88]. Moreover, within this category we also consider e-business use cases, that is applications that affect economy in some way, but that are linked to business, such as the use of blockchain for doing supply chain inventory [89], or carrying out human resources' records management [90].

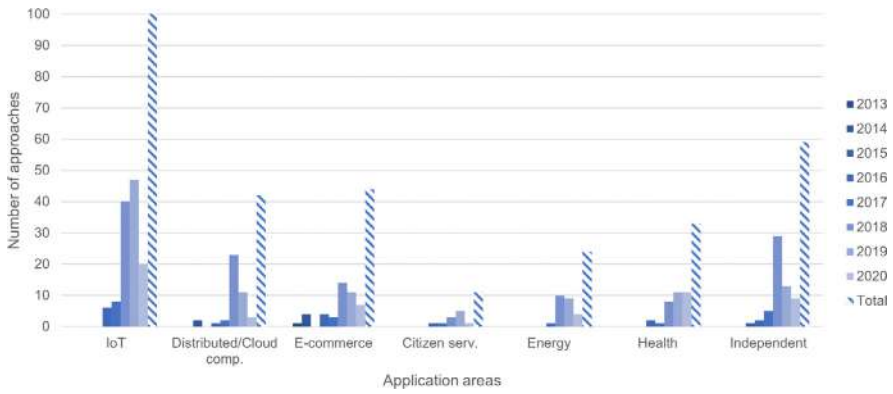

Fig. 5. Number of approaches per application area and year.

Table 2
Number of approaches regarding cybersecurity properties per application area.

		IoT	Distributed/cloud computing	E-commerce	Citizen services	Energy	Health	Independent
Authentication	Complete	88	27	22	9	18	28	41
	Partial	8	3	3	1	2	3	6
	Not provided	25	12	19	1	4	2	16
Non-repudiation	Complete	68	16	19	6	8	18	32
	Partial	26	14	11	3	8	5	12
	Not provided	27	12	14	2	8	9	18
Confidentiality	Complete	41	16	16	4	6	17	21
	Partial	26	13	10	2	2	7	7
	Not provided	54	13	15	5	16	9	34

- Citizen services: It involves proposals typically related to smart cities, where part of the government and citizenship duties, as well as institutional relationships between them are automated or centralized. In this way, electronic government (e-government) [91,92]; centralized student records [93]; or electronic voting (e-voting) [65] are included in this area.
- Energy: Smart grids and power distribution supply proposals using blockchains fall in this area. Their goal is the improvement of energy distribution [57,61,74,94].
- Health: Patient data or any kind of healthcare-related data could be managed through a blockchain. It can be applied, e.g., for improving patients access and control of their data [31,95] or for sharing data between health professionals or institutions [96,97].
- Independent: These proposals can be regarded as "area-independent" uses of blockchains. Some of them are indeed unrelated to any particular scenario, while other proposals focus on specific ones (e.g. software factories) but they could be easily adopted in other settings as well. Some examples include general access management mechanisms [73,98]; data provenance [99]; or information sharing applications [62,100]; as well as malware analysis or other cybersecurity-centered proposals like DDoS prevention [101].

In spite of the previous classification, some proposals fall in several areas. For example, [40] is related to IoT and distributed/cloud computing; and [29,102] can be involved in IoT, health and distributed/cloud computing proposals.

An analysis over time is depicted in Fig. 5. In the early years, most works were focused on e-commerce but this trend has changed. Although this area is still present in the following years, its percentage has decreased. Distributed/cloud computing related works seemed to be popular in 2014 and 2018 (40% and 21.9% of proposals respectively), but its popularity has also decreased over the years. IoT is the most popular area from 2016 to 2020, with more than 45.7% of the works. The second most popular one is area-independent, in an attempt to achieve generic solutions. 2017 and 2018 are specially remarkable because 27.8% and 27.6% of approaches fall in this category respectively.

4.2.1. Cybersecurity properties vs. areas

Cybersecurity properties and areas are simultaneously studied herein (Table 2) to identify if there are properties specially related to particular areas. The fulfillment of each of these cybersecurity characteristics will be achieved on the same bases as in — complete, partial or not provided.

Authentication

Almost all studies in citizen services (9 works), energy (18) and health (28) provide complete authentication and something similar happens in the IoT field (88). By contrast, e-commerce is the field in which this matter is less prevalent, just 22 proposals provide it completely and 3 partially. These results are probably related to the kind of provided service because, for instance, health and citizen services related proposals usually need to identify and authenticate users in the system before providing the service. Likewise, energy related works also need to authenticate entities as well as some other information (e.g. location). On the contrary, the use of blockchain in e-commerce was born to change the need of authentication, thus the lack of this property in these proposals is not surprising.

Non-repudiation

Most approaches in the health (23 works), citizen services (9) and IoT fields (94) provide complete and partial non-repudiation. Area-independent proposals also provide complete and partial non-repudiation in a large number of them, that is in 32 and 12 respectively. The remaining areas (cloud computing, e-commerce and energy) also present high provision of this property, 68.7% on average, but little lower that in other areas. Non-repudiation is usually a very important feature for the health and citizen services area, as personal information is commonly at stake. Being

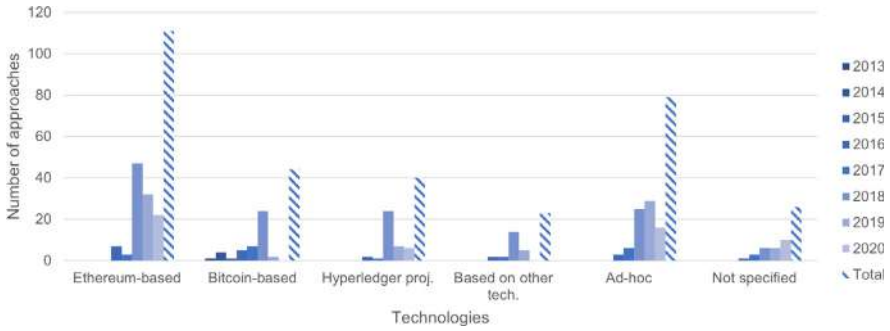

Fig. 6. Number of approaches regarding blockchain technology implementation per year.

Table 3
Number of approaches regarding cybersecurity properties per technology.

		Ethereum-based	Bitcoin-based	Hyperledger project	Based on other technologies	Ad-hoc	Not specified
Authentication	Complete	78	28	31	27	53	21
	Partial	9	2	3	5	7	2
	Not provided	24	17	6	13	20	3
Non-repudiation	Complete	56	16	26	20	43	13
	Partial	28	8	7	9	14	5
	Not provided	27	23	7	4	23	7
Confidentiality	Complete	28	19	12	19	20	12
	Partial	14	5	4	7	4	3
	Not provided	35	18	15	13	25	5

able to trace who accesses to which data and how it is carried out is very useful for accountability purposes. IoT devices sometimes also have access to private information related to people homes and lives, so the same reasoning applies. 68% of distributed/cloud Computing and energy proposals also provide this property. In these fields logging operations are not regarded as critical as the operations themselves.

Confidentiality

E-commerce is the field in which the biggest percentage of works offer complete confidentiality, 16 completely and 10 partially. Given that blockchain technologies where initially used for cryptocurrencies, where confidentiality could also be desirable to hide transactions' content, specially in permissioned networks. Health-related works usually count on high levels of authentication, strict access control policies and use private networks. However, probably because of the management of sensible data in health systems, this is the second area which provides confidentiality the most, 17 proposals completely and 7 partially. By contrast, energy works do not really care about this property, just 6 provide confidentiality completely and 2 partially. It is presumably due to the use of authentication techniques and the use of the blockchains to store power consumption data which is not considered sensible by itself.

4.3. Blockchain technologies and cybersecurity properties

Different technologies can be used when blockchains are involved. Bitcoin, Ethereum and the Hyperledger Project are three representative alternatives (recall Section 2.1). However, since there are different variants, several categories are identified. On the one hand, some authors rely upon a technology derived from Bitcoin or Ethereum, referred to as Bitcoin-based and Ethereum-based. Other authors propose an ad-hoc technology, for example by proposing new block or transaction formats that suit their needs. Another subset of proposals are based on different alternatives (classified as 'other'), that is, existing technologies different from the main ones. For example, [103] uses Monero, whereas [99] opts for Scrybe. Additionally, some proposals are technology-independent or can work with multiple ones and thus they will be included in each of the previous categories. For instance, [104] and [105] combine a public ledger with a private one. Last but not least, technology is not always specified — authors may not explicitly mention this issue or the proposal is so general that can be implemented using several technologies but without giving details in this regard, e.g. [69]. In these cases, proposals are classified as 'not specified'.

Fig. 6 shows the amount of proposals per technology and year. The most common technology is Ethereum-based, possibly due to its flexibility and the use of smart contracts [106–108]. The second largest group is ad-hoc technologies [74,95,109]. The third most popular technology is Bitcoin-based [35,43,110]. Hyperledger Project is in fourth place, being Fabric chosen in most cases [31,79,85]. One exception is [79] which uses Iroha. The fourth largest group correspond to proposals based on other technologies, for example LSB [69], BigchainDB [110], Zerocoin [111], Multichain [112], Scrybe [99] or Monero [103].

As the blockchain concept has gained popularity, new technologies have been developed. As seen in Fig. 6, Bitcoin (2013–2015) was the most well-known technology at the very beginning and received attention in 2017, but no proposal is identified in 2020. Nonetheless, after Ethereum emergence (2016-onwards), this technology gained ground, being the main one used in the whole period except for 2017. In 2016, ad-hoc technologies appeared for the first time, and have been gaining momentum over the years, being the second most popular choice since 2018. The great used of Ethereum can be linked to the fact that it allows the development of Turing-complete smart contracts and it can be used as a public network or as a private one.

Cybersecurity properties and the different technologies are simultaneously studied herein to identify if there is some link between them (Table 3). Note that proposals in which properties are not managed, because they are not explicitly pointed out or they cannot be inferred, are classified as "Not specified".

Authentication

The great majority of papers based on Hyperledger project (31 works), not specified (21) and Ethereum-based (78) categories

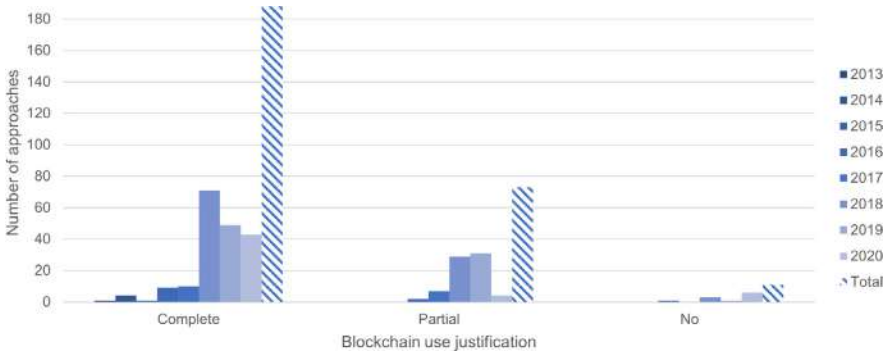

Fig. 7. Number of approaches regarding blockchain use justification per year.

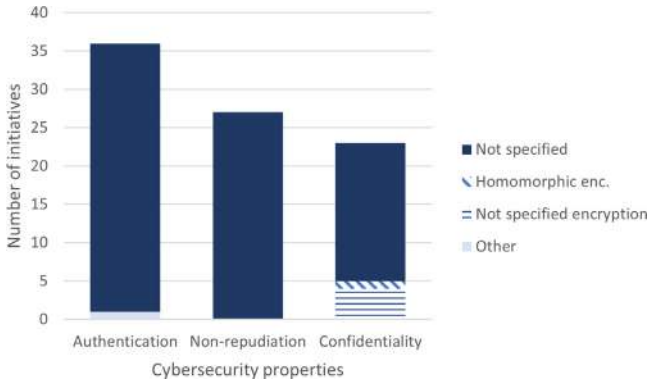

Fig. 8. Number of industrial initiatives that address cybersecurity properties and techniques applied.

provide complete authentication. Those based on other technologies also provide authentication in most of them (27 completely and 5 partially). On the other hand, a smaller set of works use Bitcoin-based technology (28 completely and 2 partially). These results are probably due to the fact that Hyperledger Project technologies are often private, so they need some kind of user authentication. Ethereum allows the use of private networks too, which could be the reason of providing authentication in most cases. However, regardless of the technology this cybersecurity property is provided quite often.

Non-repudiation

This property is considered in all technologies to some extent. Hyperledger project is present in the highest amount of proposals (26 completely and 7 partially) whereas Bitcoin-based is in the lowest one (16 completely and 8 partially). Thus, non-repudiation is most provided in technologies that allow private and/or permissioned networks (Hyperledger Project, Ethereum and ad-hoc) and less in public/permissionless ones (Bitcoin). However, in all cases complete non-repudiation is is preferred — in some cases it doubles the amount of proposals in contrast to partial non-repudiation.

Confidentiality

Confidentiality provision does not seem to be linked to particular technologies in any way. Proposals based on Ethereum-based and ad-hoc technologies are those in which it is less considered, 42 (18.9%) and 24 (15%) proposals respectively. By contrast, those Bitcoin-based or based on other technologies apply complete confidentiality more frequently, 26 (42.2%) and 24 (40.4%) proposals respectively. It may be due to being public networks in most cases.

4.4. Use of blockchain. Justification

The actual need for blockchain is studied in all proposals, considering the principles stated by Greenspan (recall Section 2.4). Based on the fulfillment of these principles, three different categories have been considered:

- Complete justification. All criteria are met. This includes proposals like [106,113]. At first glance, it may seem that private and permissioned networks do not achieve *Inter-writer mistrust* and/or *Disintermediation* because some level of trust is required between the peers– they often need to trust the organization(s) controlling the network. However, according to [24], users cannot trust each other even between the same organization. As a special note, those systems that only share hashes in the blockchain will be included in this category, as long as they fulfill all the remaining conditions and assuming that, though they do not *represent something that has real-world value* per se, they do serve as a pointer or proof to something that does (e.g. [114,115]).
- Partial justification. Systems in which a trusted third party or authority knows the nodes writing into the blockchain fall into this category. In this case, the *disintermediation* and even the *inter-writer mistrust* principles are not fully met. Thus, proposals are included in this category as long as the remaining principles are met. For example [41,116].
- No justification. The criteria are not fulfilled (except for those exceptions mentioned above). This happens, for example in [117] where, even though there are multiple users in the system, only OriginStamp submits transactions to the blockchain. Another example is [118], where an entity may be able to modify data stored in the blockchain.

Most proposals provide a complete justification (188), though this number has significantly increased in 2018 (71), see Fig. 7. A smaller amount of them integrate the blockchain in their systems with partial justification, being 2018 and 2019 years that stand out from the rest (29 and 31 proposals respectively). The high number of proposals with partial justification could be due to the need to trust an entity and the raise of technologies that allow private and permissioned networks in contrast to the initial preference for public ones (e.g. Bitcoin). On the other hand, the use of blockchain is not justified in 11 proposals. Though this is not a high number, it shows that some research results are using blockchains in an improper manner.

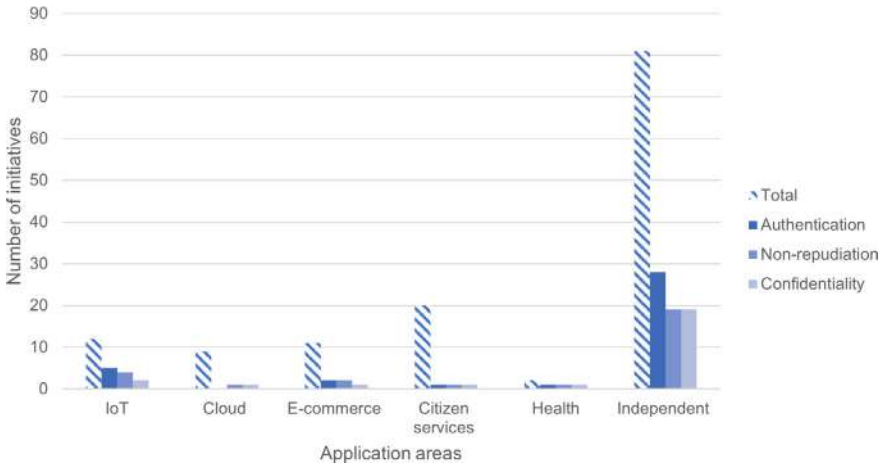

Fig. 9. Number of industrial initiatives per application area that address cybersecurity properties.

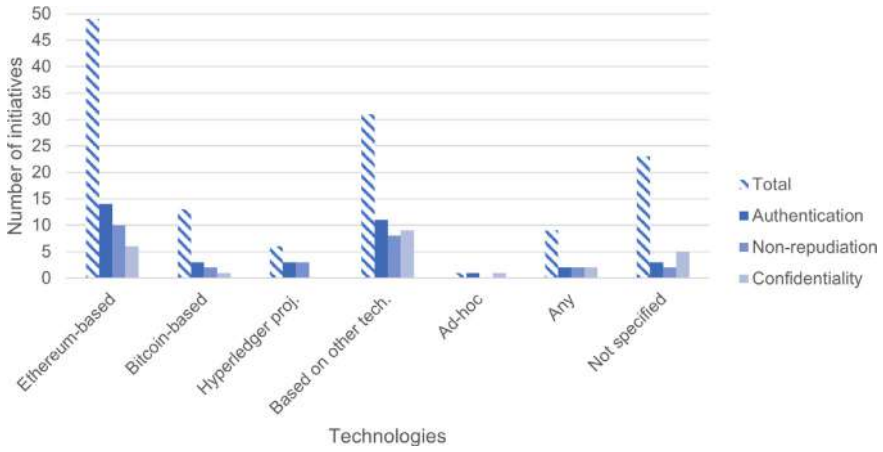

Fig. 10. Number of industrial initiatives per technology that address cybersecurity properties.

Whether the use of blockchain is justified or not has changed over the years, but maintained high percentages of complete justification (more than 60%). Most unjustified proposals are relatively novel as they belong to 2018 (4), 2019 (1) and 2020 (6). One potential reason is that blockchains were initially developed as an e-commerce technology. From then on, they have been used for many other activities and maybe some of them do not need all features they offer.

5. Industrial approaches

This Section discusses the status of the industry with respect to achieving cybersecurity by means of blockchain-based systems. Thus, after extensive search a total of 128 industrial applications have been studied following the same structure as academic papers (recall Fig. 3). Section 5.1 focuses on the techniques applied to meet cybersecurity properties, whereas Sections 5.2 and 5.3 analyzes this matter from the applications and technologies perspectives.

Note that a timeline cannot be established because there is not a clear way to specify the timing of industrial applications emergence. Similarly, industry provides less detailed descriptions and thus, opposite to academic approaches, the study cannot be performed with the same level of detail, e.g., analyzing the different degrees of confidentiality or techniques used to achieve cybersecurity properties. On the contrary, in line with academic approaches, all the industrial applications adhere to the principles of the integrity control of data at rest. The complete analysis of industrial applications is depicted in Appendix.

5.1. Cybersecurity properties and techniques

The seminal idea behind the first use of blockchain, Bitcoin, was conceived with cybersecurity goals in mind. Certainly, pseudonyms in Bitcoin are associated to public keys and financial transactions are validated on the grounds of challenge–response protocols. These procedures are not but integrity verification mechanisms, and availability and resilience are attained by the way those verification procedures are deployed in Bitcoin through a peer-to-peer network and an adequate rewarding scheme [119]. Consequently, in most industrial applications there exist underlying cybersecurity goals although they are not displayed as cybersecurity applications.

As depicted in Fig. 8, though studied industrial applications are focused on cybersecurity, most of the properties are not even mentioned and just a small set of them briefly describe how they are offered. For instance, authentication is provided by 36 proposals but only one of them can be classified into one of the previously defined categories for techniques. Similarly, in what comes to confidentiality only few of them provide enough

Table 4
Related works comparison concerning proposed research questions.

	RQ1	RQ2	RQ3	RQ4	RQ5
[122]	x	x	x	x	x
[123]	x	x	x	x	x
[124]	x	√	x	x	x
[9]	x	√	x	x	x
[8]	x	x	x	x	x
[125]	√[a]	√[a]	x	x	x
[126]	x	√	x	x	x
[127]	x	√[b]	x	x	x
[128]	√	√	x	x	x
[129]	√[c]	√[c]	x	x	x
OURS	√	√	√	√	√

[a]In fog — IoT.
[b]Industry — IoT.
[c]In healthcare.

information. As an example, homomorphic encryption is adopted in Consensus. This may be the result of several factors, such as the lack of expertise in the design and implementation of blockchain protocols [120] and the shortage of certification and auditing methodologies for the blockchain technology [121].

5.2. Application areas and cybersecurity properties

As part of Bitcoin, blockchain was used to guarantee the integrity and consistency of financial transactions. Additional application areas were incorporated as the blockchain ecosystem evolved, see Fig. 9, first by leveraging the OP_RETURN and optional fields of Bitcoin's data model [130], and subsequently by the incorporation of more complex logic through smart contracts and advanced access and authorization control models. In regard to cybersecurity goals, there are plenty of examples where the tamper-resistant characteristics of blockchain is exploited to scaffold event recording and assets traceability.

As it is underlined in [120], blockchain is mainly conceived as a means to harden the data life-cycle, which encompasses data validation/access and sharing, but also identity management [131]. This is coherent with the main conclusions of the application contexts derived from our analysis. Certainly, we have identified two preferential domains: citizen services (20 initiatives) and IoT (12 proposals), followed closely by e-commerce (11 cases). In both, citizen services and IoT scenarios, data traceability and the deployment of accountability solutions are core elements. As transparency and on-chain algorithmic governance are presented as defining features of blockchain, the vast majority of approaches (up to 81) are area-independent, thus offering these features as main advantages of blockchains over other IT services.

Fig. 9 also allows combining application areas and cybersecurity properties. The lack of information prevents from reaching meaningful conclusions. Indeed, it shows that in most areas, such as citizen services or area-independent approaches, a substantial amount of initiatives cannot be related to any particular cybersecurity property. On the contrary, other cases become clear. For example, Factom, Miirror and Atonomi provide authentication and non-repudiation. Also including Health, Prism manages all cybersecurity properties in IoT. In e-commerce Zorrosign provides authentication and non-repudiation and, by contrast, all cybersecurity properties are reached in DigiByte. In the cloud computing area, just DxChainGlobal provides confidentiality and non-repudiation. Similarly, in citizen services Metacert deals with authentication and non-repudiation and Blockarmour with confidentiality. As a result, just few initiatives provide all cybersecurity properties, as in the case of Prism for managing sensible data such as patient-related information.

5.3. Blockchain technology and cybersecurity properties

Though Bitcoin was the main initial technology, depicted in Fig. 10, industrial applications highlight the use of Ethereum-based technologies (49), mainly as a result of including advanced functionality for smart contracts. This fact is confirmed by analyzing the capitalization market in the blockchain ecosystem, though just 13 initiatives apply Bitcoin according to this study. Certainly, according to the information in CoinMarketCap,[1] Bitcoin and Ethereum are the platformas attracting more capital, which can interpreted as result of the technology adoption. Other important points are that both platforms have a more solid reference forum for programmers (as bitcoin.stackexchange [132] or ethereum.stackexchange [133]) and the list of tutorial and books to diving into the technology are much larger.

Besides the preponderance of Bitcoin and Ethereum in permissionless blockchains, in private permissioned blockchains Hyperledger Fabric is the most accepted solution, used in 6 industrial applications in this study. As it occurs with Bitcoin and Ethereum, it is not difficult to find documents and support information to develop blockchain protocols using Hyperledger Fabric.

There are many applications, 31 in particular, which do not use any of the most remarkable technologies. This may make more difficult to find software architectures and developers to be integrated as part of a continuous integration software development project. Furthermore, we have identified 62 projects without open source repositories, which can further hinder the supposed commitment with transparency of blockchain projects.

Similar to cybersecurity areas, there is no clear relationship between cybersecurity properties and blockchain technologies, as Fig. 10 depicts. Indeed, it shows that a fraction of initiatives per technology cannot be related to any cybersecurity property. These properties are considered in few Ethereum-based initiatives, e.g. Nodalblock provides confidentiality, authentication and non-repudiation. Something similar happens in Bitcoin-based approaches and, for instance, authentication and non-repudiation is achieved in Sovrin. By contrast, all Hyperledger project initiatives provide some cybersecurity property, e.g., authentication and non-repudiation is reached in Miirror and VON. Finally, it is noteworthy that initiatives applying more than one technology (Provable, Chainalysis, Ciphertrace, Blockcipher, OriginalMy) do not manage any cybersecurity property. It could be linked to the fact that their goal is providing services without a technology-oriented focus disregarding other issues.

6. Lessons learned and open research issues

Once the considered sample of academic papers and industrial approaches has been analyzed, it is possible to identify a set of lessons learned to summarize the main findings of the study. Some of them also serve to point out future research directions that can inspire forthcoming works.

6.1. Lessons learned

Lesson 1. Recent and growing interest. The academic interest of blockchain when cybersecurity is at stake has rocketed since 2016. Although our survey covers since 2013, it is in 2016 when a dramatic increase on the amount of papers is perceived.

Lesson 2. Preferred cybersecurity properties. Authors usually tend to implement some cybersecurity properties over others. Authentication and non-repudiation mechanisms are often provided, and though their joint application provides some kind of secrecy, if such countermeasures are bypassed, confidentiality

[1] https://coinmarketcap.com/.

Table 5
Analysis of academic papers (I), where – means not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network		Justification
		Conf.	Authen.	Non-repudiation		Nature	Permissions	
[39]	Independent	Complete	–	–	Bitcoin-based	Public	Permissionless	Complete
[78]	IoT	–	–	–	Bitcoin-based	Public	Permissionless	Complete
[134]	Independent	–	–	–	Ad-hoc	Public	Permissionless	Complete
[135]	Independent	–	Complete	Complete	Ethereum-based	Private	Permissionless	Complete
[41]	IoT	–	Complete	Complete	Ad-hoc	Private	Permissionless	Partial
[82]	IoT	–	Complete	Complete	Ad-hoc	Private	Permissionless	Partial
[114]	Distributed/Cloud computing	Partial	–	–	Bitcoin-based	Public	Permissionless	Complete
[106]	IoT	–	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[136]	IoT, Distributed/Cloud computing	–	Complete	Complete	Ad-hoc	Private	Permissionless	Complete
[44]	IoT	Complete	Complete	Complete	Ad-hoc	Private	Permissioned	Complete
[73]	Independent	Complete	Complete	Complete	Bitcoin-based	Private	Permissioned	Complete
[137]	IoT	–	Complete	–	Ad-hoc	Private, Public	Permissioned, Permissionless	Complete
[94]	Energy	–	Complete	–	Bitcoin-based	Private	Permissionless	Complete
[69]	IoT	Complete	Partial	Partial	Based on other technologies	Public	Permissioned	Complete
[118]	Independent	–	–	–	Ad-hoc	Any	Any	No
[138]	Independent	Complete	–	Complete	Hyperledger project	–	Permissioned	Complete
[61]	Energy	Complete	Complete	Complete	Ad-hoc	Private	–	Complete
[105]	Independent	–	Complete	Partial	Any	Private, Public	Permissioned, Permissionless	Complete
[95]	Health	Complete	Complete	Complete	Ad-hoc	Private	Permissioned	Partial
[87]	E-commerce	Partial	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[115]	Independent	Complete	–	–	Bitcoin-based	Public	Permissionless	Complete
[139]	Energy, IoT	–	Complete	Complete	Bitcoin-based	Private	Permissionless	Complete
[67]	IoT	–	Complete	Complete	–	–	–	Complete
[102]	Health, IoT, Distributed/Cloud computing	Complete	Complete	Complete	Ethereum-based, Hyperledger project	Private	Permissioned	Complete
[29]	Health, IoT, Distributed/Cloud computing	–	Complete	Partial	Ethereum-based, Hyperledger project	Private	Permissioned	Partial
[140]	IoT, Distributed/Cloud computing	–	–	–	Ad-hoc	Public	Permissionless	Complete
[98]	Independent	Complete	Complete	Partial	Bitcoin-based	Private	Permissionless	Complete
[38]	IoT, E-commerce, Distributed /cloud computing	Complete	Partial	Partial	Bitcoin-based	–	Permissionless	Partial
[62]	Independent	Complete	Complete	Complete	Ethereum-based	Private	Permissionless	Complete
[141]	Independent	–	Complete	Complete	Bitcoin-based	Private	Permissionless	Complete
[35]	E-commerce	–	Complete	Complete	Bitcoin-based	Public	Permissionless	Complete
[104]	Independent	Complete	–	–	Any	Public, Private	Permissionless, -	Complete
[30]	IoT	Complete	Complete	Complete	Ethereum-based	Private	Permissioned	Partial
[63]	Independent	Complete	Complete	Complete	Bitcoin-based	Private	Permissionless	Partial
[56]	IoT	Complete	Complete	Partial	–	Private	–	Partial
[142]	Independent	–	–	–	Ad-hoc	Public	Permissionless	Complete
[143]	E-commerce	Complete	–	–	Bitcoin-based	Public	Permissionless	Complete
[79]	IoT	Complete	Complete	Complete	Hyperledger project	–	Permissioned	Partial
[70]	E-commerce, IoT	Complete	–	–	Any	–	Permissioned	Partial
[144]	IoT	Complete	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[145]	Independent	Complete	Complete	Complete	–	Private	–	Complete
[146]	Independent	Complete	Complete	Complete	–	–	Permissioned	Complete
[147]	IoT	–	Complete	Complete	Any	Private	Permissioned	Complete
[57]	Energy	–	Complete	Partial	Ethereum-based	Public	Permissionless	Complete
[148]	IoT	Partial	Complete	Partial	Ad-hoc	Private	Permissionless	Partial
[100]	Independent	–	Complete	Complete	Ethereum-based	Public	Permissionless	Complete

would not be achieved. Indeed, confidentiality is applied to a lesser extent.

Lesson 3. Simpler and most well-known techniques to provide cybersecurity is often used. Authors seem to prefer the easiest, most well-known cybersecurity techniques when applied. For example, Registration/Pre-enrollment or simply using a CA/Authority in order to provide authentication, or asymmetric encryption and sharing hashes for confidentiality. There is a lack of approaches relying upon novel lightweight or non-conventional cryptographic techniques.

Lesson 4. Topic alignment, under-represented areas. Academic and industrial approaches are similar in their choice of focus — IoT and area-independent proposals are very prominent in both of them. While area-independent approaches can be perfectly valid, there is an underlying threat of forgetting specific requirements (e.g., tailored trust assumptions) that might render a particular use case unsuitable for blockchains. On the other hand, energy applications are not developed in industrial initiatives and just a small set in academia, considering only approaches in which cybersecurity is addressed using blockchain and not the general use of blockchain for energy provision. Something similar happens in academia concerning cybersecurity in citizen applications, as this area has received little attention.

Lesson 5. Preferred cybersecurity properties are strongly related to the area of the proposal. Depending on the area of the proposed system, some cybersecurity properties are preferred over others. For example, authentication and non-repudiation are often implemented in areas like health and citizen services, while not so much in e-commerce.

Table 6
Analysis of academic papers (II), where – means not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network		Justification
		Conf.	Authen.	Non-repudiation		Nature	Permissions	
[71]	E-commerce	Complete	–	–	Bitcoin-based	Public	Permissionless	Complete
[113]	Independent	–	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[149]	Independent	–	Partial	Complete	Any	–	–	Complete
[150]	Independent	–	Complete	Partial	–	–	–	Partial
[110]	IoT	Complete	–	–	Bitcoin-based	Public	Permissionless	No
[48]	Independent	Complete	Complete	–	Bitcoin-based	Public	Permissionless	Complete
[151]	E-commerce	Complete	–	–	Bitcoin-based	Public	Permissionless	Complete
[40]	E-commerce, Distributed/Cloud computing	–	–	–	Bitcoin-based	Public	Permissionless	Complete
[152]	E-commerce	Partial, Complete	–	–	Bitcoin-based	Public	Permissionless	Complete
[153]	Independent	–	Complete	Complete	Bitcoin-based	Private	–	Partial
[154]	Independent	–	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[155]	Distributed/Cloud computing	Complete	Complete	–	Ethereum-based	Private	Permissionless	Complete
[156]	Independent	–	–	–	Ad-hoc	Public	Permissionless	Complete
[101]	Independent	–	–	–	Bitcoin-based	Public	Permissionless	Complete
[157]	IoT	–	Complete	Complete	Bitcoin-based	Public	Permissionless	Partial
[64]	Independent	Complete	Complete	Complete	Based on other technologies	Public	–	Complete
[158]	Distributed/Cloud computing	–	Complete	Partial	Ethereum-based	Public	Permissionless	Complete
[159]	Distributed/Cloud computing	–	–	Partial	Ethereum-based	Public	Permissionless	Complete
[160]	Health, IoT	–	Complete	Complete	Ethereum-based	Private	Permissioned	Complete
[161]	Energy	–	–	–	–	–	Permissionless	Complete
[43]	Independent	–	Complete	Complete	Bitcoin-based	Public	Permissionless	Partial
[111]	Independent	Complete	Complete	–	Based on other technologies	Public	Permissionless	Complete
[66]	Distributed/Cloud computing	Partial	Complete	Complete	Ad-hoc	Private	Permissionless	Complete
[162]	Energy, E-commerce	Complete	Complete	Complete	Ad-hoc	Private	Permissionless	Partial
[31]	Health	–	Complete	Complete	Hyperledger project	Private	Permissioned	No
[163]	Health, IoT	–	Complete	–	Hyperledger project	Private	Permissioned	Complete
[164]	IoT	–	Complete	Complete	Any	Public	Any	Complete
[17]	Health, IoT	Partial	Complete	Complete	Ethereum-based	Private	–	Complete
[165]	IoT	Partial	Complete	Partial	Ethereum-based	Private	Permissioned	Complete
[166]	E-commerce	Partial	–	–	Ethereum-based	Public	Permissionless	Complete
[167]	Energy, E-commerce	–	Complete	Partial	Ethereum-based	Private	–	Complete
[85]	Distributed/Cloud computing	Partial	Complete	Complete	Hyperledger project	Private	Permissioned	Complete
[168]	Distributed/Cloud computing	–	Partial	–	Ethereum-based	Public	Permissionless	Complete
[169]	Distributed/Cloud computing	–	Partial	–	Ethereum-based	Public	Permissionless	Complete
[170]	Distributed/Cloud computing	Partial	Complete	Complete	–	Public	–	Complete
[171]	Distributed/Cloud computing	Partial	–	Complete	Ethereum-based	Public	Permissionless	Complete
[172]	Distributed/Cloud computing	Partial	Complete	Partial	Ethereum-based	Private	Permissionless	Complete
[32]	IoT	Partial	Complete	Complete	Hyperledger project	Private	Permissioned	Complete
[173]	IoT, Distributed/Cloud computing	–	–	–	Ad-hoc	Public	Permissionless	Complete
[86]	E-commerce, Distributed/Cloud computing	Complete	Complete	Complete	Ethereum-based	Public	Permissionless	Partial
[112]	Independent	–	Complete	Partial	Based on other technologies	Private	Permissioned	Partial
[174]	IoT	Partial	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[65]	Citizen services	Partial	Complete	Partial	Ethereum-based	Private	Permissionless	Partial
[175]	Independent	–	Complete	Complete	Any	Private	Permissioned	Complete
[176]	Independent	–	Complete	Complete	Hyperledger project	Private	Permissioned	Partial
[177]	Independent	–	Partial	Complete	Ethereum-based	Public	Permissionless	Complete
[178]	IoT	–	Complete	Complete	Ethereum-based	Private	–	Complete

Lesson 6. Ethereum prevalence. Both academia and industry are firmly choosing Ethereum-based technologies. One reason is the use of smart contracts, which are at stake in the majority of academic papers and in almost half of the industrial approaches. Another factor could be that most of the technical books, references and sources of information about blockchain are centered in Ethereum and Bitcoin. However, ad-hoc technologies have gained momentum over the years so this trend may change and it is considered the second preferred alternative, followed, by far, by Bitcoin-based and Hyperledger project technologies.

Lesson 7. The use of blockchain is mostly justified in academic approaches. Most academic proposals use blockchain technologies in a justified manner, though around 26% in a partial way.

Lesson 8. Undefined issues in industry. There is a worrisome lack of specification in a significant portion of industrial proposals. This lack of clarity enables questioning if the use of blockchains is justified at the light of Greenspan's principles. For instance, most initiatives do not provide information about the existence of some type of validator to verify transactions and if they pointed it out (e.g. ProtocolLabs or Ren), they do not provide an explanation. Similarly, industrial approaches provide minimal information about cybersecurity properties, which prevent us from selecting an initiative which, for instance, keeps the confidentiality of the data at stake. This issue highlights the need of giving more information about the insights of industrial developments, which does not mean to release industrial secrets, but to inform about how users' data is managed and thus, protected.

6.2. Open issues

Open issue 1. Development of a taxonomy to choose the right type of blockchain per area. For instance, a public blockchain can be specially useful in e-commerce, while a private one could be more appropriate in health applications. Combining this matter with cybersecurity technologies, a semaphore-like scheme could be created to easily represent the actual guarantees

Table 7
Analysis of academic papers (III), where – means not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network		Justification
		Conf.	Authen.	Non-repudiation		Nature	Permissions	
[33]	Energy	–	Complete	Partial	Ethereum-based	–	Permissioned	Complete
[179]	IoT	–	Complete	Complete	Hyperledger project	Private	Permissioned	Complete
[91]	Citizen services, IoT	Complete	Complete	Complete	Any	Public	–	Complete
[180]	Distributed/Cloud computing	Complete	–	–	–	–	–	Complete
[181]	IoT	Complete	Complete	Partial	Ethereum-based	Private	Permissioned	Partial
[96]	Health	Complete	Complete	Complete	Any	Private	Any	Complete
[182]	IoT	Partial	Complete	Partial	Ethereum-based	–	–	Partial
[183]	E-commerce	Complete	Complete	Partial	Ethereum-based	Any	Any	Partial
[116]	Independent	Complete	Complete	Complete	Hyperledger project	Private	Permissioned	Partial
[184]	Independent	–	Complete	Complete	Hyperledger project	Private	Permissioned	Partial
[99]	Independent	–	Complete	Partial	Based on other technologies	–	Permissioned	Partial
[107]	Distributed/Cloud computing, IoT, E-commerce	Partial	Complete	Partial	Ethereum-based	Public	Permissionless	Partial
[117]	E-commerce	Complete	Complete	Partial	Bitcoin-based	Public	Permissionless	No
[42]	Distributed/Cloud computing	Partial	Complete	Partial	Any	–	–	Partial
[185]	Independent	–	Complete	Partial	Ethereum-based	Public	Permissionless	Complete
[37]	Energy	–	Partial	Partial	Hyperledger project	Private	Permissioned	Complete
[103]	IoT	Complete	Complete	Complete	Based on other technologies	Public	Permissionless	Complete
[186]	Independent	–	Complete	Partial	Hyperledger project	Private	Permissioned	Complete
[187]	E-commerce	Complete	Complete	Partial	Ethereum-based	Public	Permissionless	Partial
[188]	Distributed/Cloud computing, E-commerce	Complete	Complete	Partial	Ethereum-based	Public	Permissioned	Partial
[34]	E-commerce	–	Complete	Partial	Bitcoin-based	Private	Any	Partial
[47]	IoT	Complete	Partial	Complete	Ethereum-based	Public	Permissionless	Complete
[50]	IoT, Distributed/Cloud computing	Partial	Complete	Complete	Hyperledger project	Private	Permissioned	Partial
[108]	Health	–	Complete	Complete	Ethereum-based	Private	Permissionless	Complete
[93]	Citizen services	–	Complete	Partial	Ethereum-based	Public	Permissionless	Partial
[92]	Citizen services	–	Complete	–	Any	Private	Permissioned	Complete
[189]	IoT	Complete	Complete	Complete	Any	–	–	Complete
[80]	IoT	–	Complete	Complete	Ad-hoc	Private	Permissioned	Complete
[46]	E-commerce	Partial	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[190]	Health, IoT, Distributed/Cloud computing	Partial	Complete	Partial	–	Private	–	Complete
[4]	E-commerce, IoT	–	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[191]	E-commerce, IoT	–	Complete	Complete	Ethereum-based	Private	–	Partial
[192]	Distributed/Cloud computing	Partial	Complete	–	Bitcoin-based	Public	Permissionless	Complete
[193]	Distributed/Cloud computing	–	Complete	Partial	Bitcoin-based	Public	Permissionless	Complete
[109]	Health, Distributed/Cloud computing	Complete	Complete	Complete	Ad-hoc	Private	Permissioned	Partial
[74]	Energy, IoT	Complete	Complete	Partial	Ad-hoc	Private	Permissioned	Partial
[58]	E-commerce	Partial	–	–	Bitcoin-based	Public	Permissionless	Complete
[81]	IoT	–	Complete	Complete	Ethereum-based	Private	Permissioned	Complete
[194]	IoT, Citizen services, E-commerce	Complete	Complete	Complete	–	Private	Permissioned	Partial
[195]	IoT	Complete	Complete	Complete	Ad-hoc	Private	Permissioned	Partial
[196]	IoT	Complete	Complete	Partial	Bitcoin-based	Public	Permissionless	Complete
[197]	IoT	–	Complete	Complete	Bitcoin-based	Public	Permissionless	Complete
[198]	IoT	–	–	Complete	Ad-hoc	Public	Permissionless	Complete
[199]	Energy, IoT, E-commerce	–	–	–	Ethereum-based	–	Permissionless	Complete
[36]	IoT	Partial	Complete	Complete	Ad-hoc	–	Permissionless	Complete
[200]	IoT	Partial	Complete	Complete	Ad-hoc	Private	Permissioned	Complete
[201]	IoT	–	Complete	Complete	–	Private	Permissioned	Complete
[202]	Energy	Complete	Complete	Complete	Hyperledger project	Private	Permissioned	Complete

provided by a proposal. This is in line with current practices, such as the privacy 'nutrition label' required by Apple to app developers [321]. This scheme might be developed leveraging current taxonomies on decentralized technologies, such as the one proposed by Samer Hasan et al. [322].

Open issue 2. Analysis of computationally efficient techniques to provide each cybersecurity property. For instance, techniques like homomorphic encryption algorithms to reach confidentiality could be a possibility, but this type of algorithms is computationally costly [323] and other alternative could be preferable.

Open issue 3. Analysis of the provision of cybersecurity properties concerning laws and regulations in different countries. As several traditional services, such as identity management or public notaries may leverage blockchains, achieving cybersecurity properties may not only be advisable but even forced by upcoming legislations.

Open issue 4. Development of a unified criteria to use blockchain technologies. There are different authors that analyze when a blockchain is necessary. In this paper Greenspan criteria are used for being well-known, but there are others like the framework in [324], the steps proposed in [325], or the set of questions created by Nitish Singh [326] that allow choosing the type of blockchain. Given the current widespread use of blockchain technology, the definition of common criteria about when and how to use this technology would help researchers and companies in the development of products and systems which really need a blockchain.

Table 8
Analysis of academic papers (IV), where – means not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network		Justification
		Conf.	Authen.	Non-repudiation		Nature	Permissions	
[203]	Independent	Partial	–	Complete	Bitcoin-based	Public	Permissionless	No
[204]	Independent	–	Complete	–	Ethereum-based	Public	Permissionless	Complete
[205]	Health	Partial	Complete	Partial	Ad-hoc	Private	Permissioned	Complete
[45]	IoT	Partial	Complete	Partial	Ad-hoc	Private	Permissioned	Complete
[206]	Independent	Partial	Complete	Complete	Ad-hoc	Private	Permissioned	Complete
[207]	IoT	–	Complete	Complete	Ad-hoc	Private	Permissioned	Complete
[208]	Health	Partial	Complete	Complete	Ethereum-based	Private	Permissioned	Complete
[209]	IoT	–	Complete	Partial	Hyperledger project	Public	Permissioned	Partial
[51]	Independent	–	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[210]	Citizen services	Partial	Complete	Complete	Ethereum-based	Private	Permissionless	Partial
[55]	IoT, Energy	–	Complete	Complete	Ethereum-based	Private	Permissioned	Complete
[211]	Energy	Partial	–	–	–	–	–	Complete
[212]	Health, IoT, Distributed/Cloud computing	–	Complete	Complete	Ethereum-based	Private	Permissionless	Complete
[213]	Health	Partial	Complete	Complete	Hyperledger project	Private	Permissioned	Complete
[52]	Citizen services	–	Complete	Complete	Ad-hoc	Public	Permissioned	Complete
[214]	IoT	Partial	Complete	Complete	Hyperledger project	Private	Permissioned	Pasrtial
[54]	IoT	–	Complete	Complete	Ethereum-based	Private	Permissioned	Partial
[215]	Independent	Complete	Partial	Complete	Ethereum-based	Private	–	Complete
[216]	E-commerce	Partial	Complete	Partial	Ad-hoc	Private	Permissioned	Complete
[217]	Health	–	Complete	Complete	Ad-hoc	Private	Permissioned	Partial
[218]	Independent	Complete	Complete	Complete	–	Private	Permissioned	Complete
[49]	Independent	Complete	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[219]	Distributed/Cloud computing	Complete	Complete	Partial	Ethereum-based	Public	Permissionless	Partial
[220]	E-commerce	–	Complete	Complete	Ethereum-based	Private	–	Partial
[221]	IoT, Distributed/Cloud computing	Partial	Complete	–	Ad-hoc	Private	Permissioned	Partial
[222]	IoT	–	Complete	Complete	Ad-hoc	Public	Permissioned	Partial
[223]	Distributed/Cloud computing, E-commerce	Complete	Complete	Complete	Ethereum-based	Public	Permissionless	Complete
[224]	Independent	Partial	Partial	Partial	Based on other technologies	Public	–	Complete
[225]	IoT	Complete	Complete	Partial	Ad-hoc	Private	Permissioned	Complete
[226]	E-commerce, Energy	Complete	Complete	Partial	Ad-hoc	Private	–	Partial
[76]	IoT, Distributed/Cloud computing	Complete	Complete	Partial	Hyperledger project	Private	–	Partial
[227]	Independent	–	Partial	Partial	Ad-hoc	Private	Permissioned	Complete
[228]	IoT	Partial	Complete	Partial	Ad-hoc	Private	Permissioned	Complete
[72]	IoT, Citizen services	Complete	–	–	Ad-hoc	–	–	Complete
[229]	IoT	–	Complete	Partial	Hyperledger project	Private	Permissioned	Partial
[230]	IoT	–	Complete	Partial	–	Public	Permissioned	Partial
[231]	Energy	–	Complete	Partial	Ethereum-based	Private	Permissioned	Complete
[232]	IoT	Partial	Complete	Complete	Ad-hoc	Public	Permissioned	Partial
[233]	IoT	Partial	Complete	Complete	Ad-hoc	Private	Permissioned	Partial
[234]	IoT	–	–	Partial	Ethereum-based	–	Permissionless	Complete
[235]	IoT	–	Complete	Partial	Ethereum-based	Private	Permissioned	Complete
[236]	IoT	Complete	Complete	–	Ad-hoc	Private	Permissioned	Partial
[237]	Energy, IoT	–	Complete	–	Based on other technologies	Public	Permissionless	Complete
[238]	Health, IoT	Complete	Partial	Partial	Ad-hoc	Public	Permissionless	Complete
[239]	IoT	–	Complete	Partial	Ad-hoc	Public	Permissionless	Complete
[240]	IoT	Complete	–	Complete	Ethereum-based	–	Permissionless	Complete
[241]	IoT	–	Complete	Complete	Ethereum-based	Public	Permissionless	Partial
[242]	IoT, Distributed/Cloud computing, E-commerce	Partial	–	–	Ad-hoc	–	–	Complete
[243]	Health	Partial	Complete	–	Ethereum-based	Public	Permissionless	Complete
[244]	Health	Complete	Complete	–	Ethereum-based	–	–	Complete

7. Related works

Blockchain is a trending topic nowadays and lots of surveys have been developed in this regard. Security has not been neglected either. For example, in [327] security issues of blockchain technologies are studied. [8] presents a deeper analysis, describing vulnerabilities and attacks of blockchain technologies. Also, [122] surveys security threats and real attacks against blockchain systems. Considering blockchain security but from a different perspective, [123] explores business, organizational and operational issues. In this vein, security issues at different levels, such as data, smart contracts or networking protocols are studied.

In terms of blockchain applications and cybersecurity, [124] points out blockchain advantages and classifies blockchain applications for cybersecurity. Similarly, [9] and [126] analyze blockchain-based applications, though the latter also points out blockchain security and privacy challenges. [125] surveys blockchain applications in the area of fog-enabled IoT. Given the relationship between blockchain and fog computing in IoT, it is studied the fulfillment of cybersecurity goals. In this same context, [328] analyzes the integration of blockchain, categorizing applications but without a clear focus on security, though highlighting its need and pointing it out as a challenge. Focusing on Industry 4.0, which can be considered within IoT solutions, [127] presents an extensive survey on how blockchain systems can overcome cybersecurity barriers. Some cybersecurity issues are analyzed, like failure of key nodes in centralized platforms, but this work does not directly analyze cybersecurity properties and techniques. To the best of the authors knowledge, only [128,129]

Table 9
Analysis of academic papers (V), where – means not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network		Justification
		Conf.	Authen.	Non-repudiation		Nature	Permissions	
[245]	IoT, Distributed/Cloud computing, E-commerce	–	Complete	Complete	–	Public, Private	–	Partial
[246]	Independent	Partial	Complete	Partial	Ethereum-based	Private	–	Partial
[247]	IoT	Partial	Complete	–	Bitcoin-based	Private	Permissionless	Partial
[53]	Energy	–	Complete	–	Hyperledger project	Private	–	Complete
[248]	IoT	Complete	Complete	Complete	Ethereum-based	Private	Permissioned	Partial
[249]	Citizen services, IoT	–	Partial	Partial	Ethereum-based	Private	Permissionless	Complete
[250]	Energy, IoT	Partial	Complete	Complete	Ad-hoc	Private	Permissioned	Partial
[251]	Distributed/Cloud computing, IoT, E-commerce	–	–	Complete	Based on other technologies	Any	Any	Complete
[252]	Energy, IoT	Complete	Complete	Partial	Ad-hoc	Private	Permissionless	Partial
[253]	Health, IoT	Partial	Complete	Complete	Ethereum-based	–	–	Partial
[254]	Independent	–	Complete	Complete	Based on other technologies	Private	Permissioned	Partial
[75]	IoT, Distributed/Cloud computing	Complete	Complete	Partial	Ethereum-based	Private	–	Complete
[255]	IoT	Complete	–	–	Ad-hoc	–	–	Complete
[59]	IoT	–	–	–	Ethereum-based	Public	Permissionless	Complete
[256]	Citizen services, IoT	Complete	Complete	Complete	Based on other technologies	Private	Permissioned	Partial
[257]	Health, IoT	–	–	Complete	Ethereum-based	Private	Permissioned	Complete
[258]	IoT	–	–	Complete	–	Private, Public	Permissioned	Partial
[259]	Independent	Partial	–	Complete	Ad-hoc	Public	Permissionless	Complete
[260]	Health	Complete	Complete	Partial	Ethereum-based	Public	Permissionless	Complete
[261]	IoT	Complete	Complete	Complete	Ad-hoc	Private	Permissioned	Partial
[262]	IoT	–	Complete	–	Ad-hoc	Public	Permissionless	Partial
[263]	IoT, Distributed/Cloud computing	Complete	–	Complete	Ethereum-based	Public	Permissionless	Complete
[264]	E-commerce	–	–	Complete	Ethereum-based	Public	Permissionless	Complete
[265]	IoT	Complete	Complete	Complete	Ad-hoc	Private	Permissionless	Complete
[266]	E-commerce	Complete	Complete	Complete	Ad-hoc	Private	Permissioned	Partial
[267]	Independent	Partial	Complete	Partial	Ethereum-based	Private	–	Partial
[268]	E-commerce	–	–	Complete	Ethereum-based	Public	Permissionless	Complete
[269]	Distributed/Cloud computing, IoT, E-commerce	Complete	–	Partial	Ethereum-based	Public	Permissionless	Complete
[270]	Health	Complete	Partial	–	Ad-hoc	Private	–	Complete
[271]	Independent	–	Partial	Partial	Ad-hoc	–	Permissioned	Complete
[272]	Independent	Complete	Complete	–	Ethereum-based	Public	Permissionless	No
[273]	Energy	–	Complete	–	Ethereum-based	–	Permissioned	Complete
[274]	Health	–	Partial	Partial	–	–	Permissioned	No
[90]	E-commerce	Partial	Complete	Complete	Ethereum-based	Public & Private	–	Complete
[275]	IoT	Complete	Complete	Complete	Ethereum-based	Public	Permissioned	Partial
[276]	IoT	Complete	Partial	Complete	Ad-hoc	Private	Permissioned	Complete
[277]	E-commerce	Complete	–	Complete	Ethereum-based	Public	–	Complete
[278]	Cloud computing	Complete	Complete	–	–	Public	–	Complete
[279]	Health	Complete	Complete	Complete	Ad-hoc	Private	Permissioned	Complete
[280]	Independent	Complete	Complete	–	Hyperledger project	Private	Permissioned	Partial
[281]	Health	Complete	Complete	–	Ethereum-based	Private	Permissionless	Complete
[282]	Health	Complete	Complete	–	Ad-hoc	Private	–	Complete
[283]	IoT	–	–	Complete	Ad-hoc	Private	Permissioned	Complete
[284]	E-commerce	–	–	Complete	Ethereum-based	Public	Permissionless	Complete
[285]	Independent	–	Complete	Complete	Hyperledger project	Private	Permissioned	Complete

focus on studying how cybersecurity is achieved when applying blockchains. In both cases the sample is substantially smaller, 30 and 33 papers in [128] and [129] respectively. Moreover, in [128] the analysis is quite limited, without providing a careful review of methods to provide cybersecurity. By contrast, [129] bases on electronic health record systems exclusively.

A summary of related works considering the proposed research questions is depicted in Table 4. Note that there are many other proposals focused on blockchain cybersecurity which look for analyzing attacks, threats and vulnerabilities, but only those that share the goal of this survey are considered herein. Indeed, this paper studies the relationship between cybersecurity objectives and blockchain capabilities, considering their application areas or technologies among other issues. Moreover, technologies at stake and the analysis on the justified use of blockchains (questions RQ3 and RQ4) have not been explored yet. Similarly, no other paper presents an extensive study joining academia and industry (question RQ5).

8. Conclusions

Blockchain-based approaches to provide with cybersecurity guarantees have rocketed in the last years. This is not only an academic trend — industrial approaches have also emerged firmly. Our review has addressed both academic manuscripts throughout 8 years as well as existing industrial approaches. It has been shown that blockchain is an enabling technology that is paving the way for smarter, enriched services. Our analysis shows that industry and academia have a remarkable similarity, that is the prevalence of Ethereum. As a result, some research venues that remain unexplored have been identified. Moreover, it has been shown that industrial proposals usually omit critical details in their approaches. Another worrisome fact is that there is a fraction of academic papers that are using blockchain disregarding (or at least not providing evidences of satisfaction of) all principles that justify its use. To foster further works in this direction, a set of open issues have been identified.

Table 10
Analysis of academic papers (VI), where – means not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network		Justification
		Conf.	Authen.	Non-repudiation		Nature	Permissions	
[286]	E-commerce	–	Partial	–	Ethereum-based	Public	Permissioned	Complete
[287]	Cloud computing	Complete	–	Complete	Ethereum-based		Permissioned	Complete
[288]	Energy, Citizen services	–	Complete	Complete	Ad-hoc	Private	Permissioned	Complete
[289]	Health	Complete	Complete	–	–	Private	Permissioned	Partial
[89]	E-commerce	–	–	Complete	Ethereum-based	–	–	Complete
[290]	IoT	Partial	Partial	Complete	Ad-hoc	–	–	Complete
[291]	E-commerce	–	Partial	–	Ethereum-based	–	–	Complete
[292]	Independent	Complete	–	–	Ethereum-based	Private	Permissioned	Partial
[293]	Health	Complete	Complete	–	Ethereum-based	Private	–	Complete
[294]	Cloud computing, IoT	Complete	Complete	Complete	–	–	–	Complete
[295]	IoT	–	–	–	Hyperledger project		Permissioned	Complete
[296]	Health	Complete	Complete	–	Ethereum-based, Hyperledger project	Private	–	Complete
[297]	IoT	–	Partial	–	–	Private	–	No
[298]	IoT	Complete	Complete	–	Ad-hoc	Private	Permissioned	Complete
[299]	Independent	Complete	Complete	Complete	–	–	–	No
[300]	IoT	Partial	–	–	Ethereum-based	Private	Permissioned	Complete
[301]	Energy	–	–	Complete	Ethereum-based	Public	Permissioned	Complete
[302]	Health	Complete	–	Complete	Hyperledger project	Private	Permissioned	Complete
[303]	IoT	Partial	–	–	Ethereum-based	–	–	Complete
[304]	IoT	Partial	Complete	Complete	Ethereum-based	Private	Permissioned	Complete
[305]	IoT	–	–	Complete	Ethereum-based	Public	Permissionless	Complete
[306]	Energy	–	Partial	–	Ad-hoc	–	–	Complete
[307]	IoT	–	Complete	Complete	–	Public and private	–	No
[308]	IoT	–	–	Complete	Ad-hoc	Private	Permissioned	Complete
[309]	IoT	Complete	Complete	–	Ethereum-based	Public	Permissioned	Complete
[310]	IoT	–	Complete	–	–	Private	–	No
[311]	IoT	Complete	–	Complete	Ethereum-based	Public	Permissionless	Complete
[312]	Health	Complete	Complete	Complete	–	Public	Permissioned	Complete
[313]	Independent	–	–	Complete	Ad-hoc	–	Permissioned	Complete
[314]	IoT	Complete	Complete	–	Ad-hoc	Private	Permissioned	Complete
[315]	Independent	–	Complete	Complete	Hyperledger project	Private	–	Complete
[316]	E-commerce	–	–	–	Ad-hoc	–	Permissioned	Complete
[317]	IoT	–	Partial	–	Ad-hoc	Public and private	–	Complete
[318]	Health	Complete	Complete	Complete	Ad-hoc	Private	Permissioned , Permissionless	Complete
[319]	Independent	Partial	Complete	–	Ethereum-based	Private	Permissioned	Complete
[320]	IoT	Complete	Complete	–	–	Public	Permissioned	Complete

As future work, the analysis on the risks posed by external technologies when interacting with the blockchain will be further explored. It must be noted that the direct or indirect interaction among technologies may be helpful to develop novel attacks. This may be extremely relevant in critical infrastructures such as industrial facilities.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors would like to thank the anonymous reviewers for their comments and suggestions, as well as Prof. Javier Lopez, Dr. David Galindo and Dr. David Nunez for their comments on the first stages of this paper.

This work has been partially funded by MINECO, Spain grants TIN2016-79095-C2-2-R (SMOG-DEV) and PID2019-111429RB-C21 (ODIO-COW); by CAM, Spain grants S2013/ICE-3095 (CIBERDINE), P2018/TCS-4566 (CYNAMON), co-funded by European Structural Funds (ESF and FEDER); by UC3M-CAM grant CAVTIONS-CM-UC3M; by the Excellence Program for University Researchers, Spain; and by Consejo Superior de Investigaciones Científicas (CSIC), Spain under the project LINKA20216 (“Advancing in cybersecurity technologies”, i-LINK+ program).

Appendix. Tables

The analysis of all the academic papers is depicted in Tables 5–10, whereas that of all industrial approaches is depicted in Tables 11–14.

Industrial approaches - Reference list

- UnboundTech, www.unboundtech.com/
- Dfinity, dfinity.org/
- Alastria, alastria.io/
- Nodalblock, www.nodalblock.com/es/
- Stampery, www.stampery.com/
- Sovrin, sovrin.org/
- Caterpillar, github.com/orlenyslp/Caterpillar
- ProtocolLabs, protocol.ai/
- Storj, storj.io/
- DxChainGlobal, www.dxchain.com/
- DigiByte, www.digibyte.co/
- Keychain, http://www.keychain.io
- Mythx, mythx.io/
- Interledger, interledger.org/
- Factom, www.factom.com/
- Web3labs, www.web3labs.com/
- Laava, www.laava.id/
- Nucypher, www.nucypher.com/
- IOHK, iohk.io/

Table 11
Analyses of industrial initiatives (I), where X means the property is considered and – not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network	
		Conf.	Authen.	Non-repudiation		Nature	Permissions
Unbound tech	Independent	–	–	–	–	–	–
Dfinity	Independent	–	X	X	Based on other technology	Public	Permissioned
Alastria	Independent	–	X	X	Ethereum-based	Public	Permissioned
Nodalblock	Independent	X	X	X	Ethereum-based	Any	–
Stampery	Independent	–	X	X	Bitcoin-based	Public	Permissionless
Sovrin	Independent	–	X	X	Hyperledger project	Public	Permissioned
Caterpillar	Independent	–	–	–	Ethereum-based	Public	Permissionless
Protocol labs	Independent	X	X	X	Based on other technology	Public	Permissionless
Storj	Independent	X	X	X	–	Public	Permissioned
DxChainGlobal (TrustLook)	Cloud computing	X	–	X	Based on other technology	–	Permissioned
DigiByte	E-commerce	X	X	X	Based on other technology	Public	Permissionless
Keychain	Independent	X	–	–	–	–	–
Mythx	Independent	–	–	–	Ethereum-based	–	–
Interledger	Independent	–	–	–	Based on other technology	Public	Permissioned
Factom	IoT	–	X	X	Bitcoin-based	Public	Permissioned
Web3 labs	Independent	–	–	–	Ethereum-based	–	–
Laava	IoT	–	–	–	Ethereum-based	Public	Permissionless
Nucypher	Independent	X	–	–	Based on other technology	Public	Permissionless
IOHK	–	–	–	–	Based on other technology	Public	Permissionless
Regis	Independent	–	–	–	Ethereum-based	Public	Permissionless
Komodo	E-commerce	–	–	–	Based on other technology	Public	Permissionless
a16zcrypto	–	–	–	–	–	–	–
Algorand	Independent	–	–	–	Based on other technology	Public	Permissionless
Qed-it	Independent	–	–	–	–	–	–
Aztec	Independent	–	–	–	Ethereum-based	–	–
Miirror	IoT	–	X	X	Hyperledger project	Private	Permissioned
Ligero	Independent	–	–	–	–	–	–
Calctopia	E-commerce	–	–	–	Ethereum-based	Public	Permissionless
DTR	Independent	–	–	–	Based on other technology	–	–
Prism	IoT, Health	X	X	X	Based on other technology	–	–
Nuls	Independent	X	–	–	Based on other technology	Public	Permissionless
Horizen	Independent	X	X	X	Based on other technology	Public	Permissionless
Blockarmour	IoT, Citizen services	X	–	–	–	Private	–
Civic	Independent	X	–	–	–	Public	–
Hacken	Independent	–	–	–	Ethereum-based	–	–
Ethereum name service	Independent	–	–	–	Ethereum-based	Public	Permissionless
Edge	Cloud computing	–	–	–	Ethereum-based	Public	Permissionless

- Regis, regis.nu/
- Komodo, komodoplatform.com/
- a16zcrypto, a16zcrypto.com/
- Algorand, www.algorand.com/
- Qed-it, qed-it.com/
- Aztec, www.aztecprotocol.com/
- Miirror, getmirror.io/
- Ligero, ligero-inc.com/
- Calctopia, www.calctopia.com/
- DTR, dtr.org/
- Prism, prismprotocol.com/
- Nuls, nuls.io/
- Horizen, www.horizen.global/
- Blockarmour, www.blockarmour.com/
- Civic, www.civic.com/
- Hacken, hacken.io/
- EthereumNameService, ens.domains/
- Edge, edge.app/
- Augur, www.augur.net/
- Provable, provable.xyz/
- Polkadot, polkadot.network/
- OpenZeppelin, openzeppelin.org/
- Chainlink, www.smartcontract.com/,
- Blockstream, blockstream.com/
- Iden30kims, http://www.iden3.io/, 0kims.org/
- Cosmos, cosmos.network/
- Enigma, enigma.co/
- Tezos, tezos.com/
- Aeternity, aeternity.com/
- Qtum, qtum.org/
- PrivacyBlockchain, www.privacyblockchain.io/
- Initc3, www.initc3.org/
- ClaimChain, claimchain.github.io/
- DEDIS, dedis.epfl.ch/
- VON, vonx.io/about/
- Kleros, kleros.io/
- InkProtocol, paywithink.com/
- Nemkrs, github.com/aenima86/NEMkrs
- Sentient, sentient.org/
- Consensus, consensus.ai/
- Safekee, http://www.safekee.io/
- Blockchainasfactchecker, www.blockchainasfactchecker.net/
- Bitpress, bitpress.news/
- Verifact, verifact.io/
- DNN, dnn.media/
- Zebi, www.zebi.io/
- Dmgblockchain:Blockseer, www.blockseer.com/
- Elliptic, www.elliptic.co/
- Chainalysis, www.chainalysis.com/
- Ciphertrace, ciphertrace.com/
- Blockcipher, www.blockcypher.com/case-studies.html
- Tcforensics, http://www.tcforensics.com/
- Zorrosign, www.zorrosign.com/
- Dascoin, dascoin.com/
- BlockchainintelligenceGroup, blockchaingroup.io/

Table 12
Analyses of industrial initiatives (II), where X means the property is considered and – not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network	
		Conf.	Authen.	Non-repudiation		Nature	Permissions
Augur	Independent	–	–	–	Ethereum-based	Public	Permissionless
Provable	Independent	–	–	–	Ethereum-based, Based on other technology, Hyperledger project	–	–
Polkadot	Independent	–	X	X	Ethereum-based	Public	Any
OpenZeppelin	Independent	–	–	–	Ethereum-based	–	–
Chainlink	Independent	–	–	–	Ethereum-based	–	–
Blockstream	Independent	X	–	–	Bitcoin-based	Public	Permissionless
Iden3 + 0kims	Independent	–	X	X	Ethereum-based	Public	Permissionless
Cosmos	Independent	–	–	–	Based on other technology	Public	Permissioned
Enigma	Independent	–			–	–	–
Tezos	Independent	–	–	–	Based on other technology	Public	Permissioned
Aeternity	Independent				–	Public	Permissionless
Qtum	Independent	–	–	–	Ethereum-based	Public	Permissionless
Privacy blockchain	Independent	–	–	–	Any	–	–
Initc3	Independent	X	X	X	Any	–	–
DEDIS	Independent	–	X	–	Based on other technology	Public	Permissionless
VON	Independent	–	X	X	Hyperledger project	Public	Permissioned
Kleros	Independent	–	–	–	Ethereum-based	Public	Permissionless
Ink protocol	Independent	–	–	–	Ethereum-based	Public	Permissionless
Nemkrs	Independent	–	–	–	Based on other technology	Any	Permissionless
Sentient	Independent	–	–	–	Based on other technology	Public	Permissioned
Consensus	Independent	X	X	–	Based on other technology	Public	Permissioned
Safekee	Independent	–	–	–	Based on other technology	–	–
Blockchainasfactchecker	Citizen services*	–	–	–	–	–	–
Bitpress	Citizen services*	–	–	–	Bitcoin-based	Public	Permissionless
Verifact	Citizen services*	–	–	–	Ethereum-based	Public	Permissionless
DNN	Citizen services*	–	–	–	Ethereum-based	–	–
Zebi	Independent	–	–	–	Ethereum-based	Private	Permissioned
Dmgblockchain: Blockseer	E-commerce	–	–	–	Ethereum-based, Bitcoin-based	–	–
Elliptic	E-commerce	–	–	–	Bitcoin-based	–	–
Chainalysis	E-commerce	–	–	–	Ethereum-based, Bitcoin-based	–	–
Ciphertrace	E-commerce	–	–	–	Ethereum-based, Bitcoin-based	–	–
Blockcipher	E-commerce	–	–	–	Ethereum-based, Bitcoin-based	–	–
Tcforensics	Citizen services	–	–	–	Bitcoin-based	–	–
Zorrosign	E-commerce	–	X	X	Based on other technology	Private	Permissioned

- Filament, filament.com/
- dsensor, http://www.dsensor.org/
- Provenance, www.provenance.org/
- Sentinel, sentinel.co/
- QuantNetwork, www.quant.network
- Zcash, z.cash/
- RenProject, renproject.io/
- Slock, slock.it/
- Guardtime, guardtime.com/
- Metacert, metacert.com/
- Atonomi, atonomi.io/
- Gitcoin, gitcoin.co/
- Aion, aion.network/
- Chainspace, chainspace.io/
- Kzen, www.kzencorp.com/
- Robonomics, robonomics.network/
- SKYFchain, www.skyfchain.io/
- Wibson, wibson.org/
- SingularityNET, singularitynet.io/
- TheOceanProtocol, oceanprotocol.com/
- Grex, grex.kryha.io/
- Golem, golem.network/
- Neuromation, www.neuromation.io/
- ATN, atn.io

- Matrix, www.matrix.io/
- Chronicled, www.chronicled.com/
- uPort, www.uport.me/
- Everest, everest.org/
- Sepior, sepior.com/
- YotiLedgerState, www.yoti.com/blog/yoti-and-ledgerstate-showcase-how-next-generation-blockchain-technology-can-transform-the-way-governments-handle-personal-and-data/
- Arbitrum, offchainlabs.com/
- DeepDefence, deepdefence.net/
- Extropy, http://extropy.io
- Quickblocks, quickblocks.io/
- Halborn, halborn.com/
- GroupIB, www.group-ib.com/
- Gochain, gochain.io/
- Bernstein, www.bernstein.io/
- OriginalMy, originalmy.com/
- RebelAI, www.rebelai.com/
- Wisekey, www.wisekey.com/
- Heroic, heroic.com/
- HashedHealth, hashedhealth.com/
- Hdac, www.hdactech.com/
- CryptoMove, www.cryptomove.com/
- OpenAVN, www.openavn.com/
- Cryptyk, www.cryptyk.com/
- Megahoot, www.megahoot.com/
- Anchain.ai, www.anchain.ai/
- Taekion, www.crunchbase.com/organization/taekion
- Haceram, hacera.com/
- Polyswarm, polyswarm.io/
- Trailofbits, www.trailofbits.com/
- ApolloCloud, www.promise.com/es/Products/Apollo/Apollo-Cloud-2-Duo

Table 13
Analyses of industrial initiatives (III), where X means the property is considered and – not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network	
		Conf.	Authen.	Non-repudiation		Nature	Permissions
Dascoin	Independent	–	X	X	Based on other technology	Public	Permissioned
Blockchain intelligence group	Citizen services	–	–	–	–	–	–
Filament	IoT	–	–	–	Any	–	–
Dsensor	IoT	–	X	–	Bitcoin-based	Public	Permissionless
Provenance	Independent	–	X	–	–	–	–
Sentinel	Independent	X	X	–	Ad-hoc/ Based on other technology	Public	–
Quant network	Independent	X	X	X	Any	Public	–
Zcash	Independent	–	–	–	Bitcoin-based	Public	Permissionless
Ren project	E-commerce	–	–	–	Ethereum-based	Public	Permissionless
Slock	IoT	–	–	–	Ethereum-based	Public	Permissionless
Guardtime	Independent	–	–	–	Based on other technology	Public	Permissioned
Metacert, MetacertProtocol	Citizen services*	–	X	X	Ethereum-based	Public	Permissioned
Atonomi	IoT	–	X	X	Ethereum-based	Public	Permissionless
Gitcoin	Independent				Ethereum-based	Public	Permissionless
Aion	Independent	–	–	–	Based on other technology	–	–
Chainspace	Independent	–	–	–	Based on other technology	–	–
Kzen (ZenGo)	Independent	–	–	–	Any	–	–
Robonomics	Independent	–	X	X	Ethereum-based	Public	Permissionless
SKYFchain	Independent	–	–	–	Ethereum-based	Any	Permissionless
Wibson	Independent	X	X	X	Ethereum-based	Public	Permissionless
SingularityNET	Independent	X	X	X	Ethereum-based	Public	Permissionless
The ocean protocol	Independent	X	X	X	Ethereum-based	Public	Permissioned
Grex	Independent	–	–	–	Any	–	–
Golem	Independent	X	–	–	Ethereum-based	Public	Permissionless
Neuromation	Independent	–	–	–	Ethereum-based	Public	Permissionless
ATN	Independent	–	X	–	Based on other technology	Public	Permissionless
Matrix	Independent	–	–	–	Based on other technology	Public	Permissioned
Chronicled	Independent	X	X	–	Ethereum-based	Public	Permissionless
uPort	Independent	–	X	–	Ethereum-based	Public	Permissionless
Everest	Independent	–	X	–	Ethereum-based	Public	Permissionless
Sepior	Independent	X	X	X	–	–	–
Yoti + LedgerState	Independent	–	X	–	Ethereum-based	Public	Permissionless
Arbitrum	Independent	–	–	–	Ad hoc	–	–
Deep defense	IoT	–	–	–	Ethereum-based	–	–
Clearmatics	E-commerce	–	–	–		Any	Permissionless
Extropy	Independent	–	–	–	Hyperledger project, Ethereum -based, Based on other technology	–	–
Quickblocks	Independent	–	–	–	Ethereum-based	–	–

Table 14
Analyses of industrial initiatives (IV), where X means the property is considered and – not specified.

Name	Area	Cybersecurity properties			Blockchain technology	Type of network	
		Conf.	Authen.	Non-repudiation		Nature	Permissions
Halborn	Independent	–	–	–	Any	–	–
GroupIB	Independent	–	–	–	Any	–	–
Gochain	Citizen services	–	–	–	Ethereum-based	Any	Any
Bernstein	Citizen services	–	–	–	Bitcoin	Public	Permissioned
OriginalMy	Citizen services	–	–	–	Bitcoin-based, Ethereum-based	Public	Permissioned
RebelAI	Citizen services	–	–	–	–	–	–
Wisekey	IoT, Citizen services	–	–	–	–	–	–
Heroic	Cloud computing, Citizen services	–	–	–	Ethereum	Public	Permissioned
HashedHealth	Health	–	–	–	–	–	–
Hdac	IoT	–	–	–	Based on other technology	–	–
CryptoMove	Cloud computing, Citizen services	–	–	–	–	–	–
OpenAVN	Cloud computing, Citizen services	–	–	–	–	–	–
Cryptyk	Cloud computing, Citizen services	–	–	–	Hyperledger project	Private	Permissioned
Megahoot	Citizen services	–	–	–	–	–	–
Anchain.ai	Independent	–	–	–	Any	–	
Taekion	Cloud computing, Citizen services	–	–	–	–	–	–
Hacera	Cloud computing, Citizen services	–	–	–	–	–	–
Polyswarm	Independent	–	–	–	Ethereum	Public	Permissionless
Trailofbits	Independent	–	–	–	Ethereum	Public	Permissionless
ApolloCloud	Cloud computing	–	–	–	–	–	–

References

[1] J.G. Andrews, S. Buzzi, W. Choi, S.V. Hanly, A. Lozano, A.C. Soong, J.C. Zhang, What will 5g be?, IEEE J. Sel. Areas Commun. 32 (6) (2014) 1065–1082.

[2] N. Kshetri, Can blockchain strengthen the internet of things?, IT Prof. 19 (4) (2017) 68–72.

[3] M. Swan, Blockchain: Blueprint for a New Economy, " O'Reilly Media, Inc.", 2015.

[4] R. Beck, J. Stenum Czepluch, N. Lollike, S. Malone, Blockchain–the gateway to trust-free cryptographic transactions, 2016.

[5] G.O. Karame, E. Androulaki, S. Capkun, Double-spending fast payments in bitcoin, in: Proc. 2012 ACM CCS, ACM, 2012, pp. 906–917.

[6] J. Leng, P. Jiang, K. Xu, Q. Liu, J.L. Zhao, Y. Bian, R. Shi, Makerchain: A blockchain with chemical signature for self-organizing process in social

manufacturing, J. Cleaner Prod. 234 (2019) 767–778.
[7] There's no good reason to trust blockchain technology, Wired (2019) URL https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/ (Last access Feb. 2021).
[8] H. Hasanova, U.-j. Baek, M.-g. Shin, K. Cho, M.-S. Kim, A survey on blockchain cybersecurity vulnerabilities and possible countermeasures, Int. J. Netw. Manag. 29 (2) (2019) 2060.
[9] F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telemat. Inform. 36 (2019) 55–81.
[10] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Working Paper, 2008.
[11] L. Axon, M. Goldsmith, Pb-pki: a privacy-aware blockchain-based pki, 2016.
[12] G. Wood, Ethereum yellow paper, 2019, URL https://ethereum.github.io/yellowpaper/paper.pdf.
[13] G. Wood, Poa private chains, 2015, URL https://github.com/ethereum/guide/blob/master/poa.md.
[14] Hyperledger, 2021, URL https://www.hyperledger.org/use (Last access Feb. 2021).
[15] Permissioned blockchain: 5 hyperledger projects in depth, 2018, URL https://4irelabs.com/5_hyperledger_projects_in_depth (Last access Feb. 2021).
[16] Hyperledger chaincode tutorials, 2021, URL https://hyperledger-fabric.readthedocs.io/en/release-1.3/chaincode.html (Last access Feb. 2021).
[17] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, M. Ylianttila, Secure and efficient data accessibility in blockchain based healthcare systems, in: 2018 IEEE Global Communications Conference (GLOBECOM), IEEE, 2018, pp. 206–212.
[18] Exploding costs of storing information on a blockchain, 2017, URL https://content-blockchain.org/newsarchive/2017/07/20/exploding-costs-of-storing-data-on-a-blockchain/ (Last access Feb. 2021).
[19] W. Galuba, S. Girdzijauskas, Distributed hash table, in: L. LIU, M.T. ÖZSU (Eds.), Encyclopedia of Database Systems, Springer US, Boston, MA, 2009, pp. 903–904.
[20] A. Stavrou, J. Voas, Verified time, Computer 50 (3) (2017) 78–82.
[21] C. Paulsen, C. Paulsen, P. Toth, Small Business Information Security: The Fundamentals, NIST, 2016.
[22] P.A. Grassi, M. Garcia, J. Fenton, DRAFT NIST Special publication 800-63-3 digital identity guidelines, NIST (2017).
[23] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid, Nist special publication 800-57, NIST Spec. Publ. 800 (57) (2007) 1–142.
[24] G. Greenspan, Avoiding the pointless blockchain project, 2015, URL https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/.
[25] R. Briner, D. Denyer, Systematic review and evidence synthesis as a practice and scholarship tool, 2012, pp. 112–129, http://dx.doi.org/10.1093/oxfordhb/9780199763986.013.0007.
[26] Dblp computer science bibliography, 2021, URL https://dblp.uni-trier.de/ (Last access Feb. 2021).
[27] Clarivate, J. Citation Rep. (2021).
[28] GII-GRIN-SCIE, The gii-grin-scie (ggs) conference rating, 2021.
[29] M.A. Rahman, E. Hassanain, M.M. Rashid, S.J. Barnes, M.S. Hossain, Spatial blockchain-based secure mass screening framework for children with dyslexia, IEEE Access 6 (2018) 61876–61885.
[30] N. Malik, P. Nanda, A. Arora, X. He, D. Puthal, Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks, in: IEEE Intl. Conf. on Trust, Security and Privacy in Computing and Communications, IEEE, 2018, pp. 674–679.
[31] T. Mikula, R.H. Jacobsen, Identity and access management with blockchain in electronic healthcare records, in: Proceedings - 21st Euromicro Conference on Digital System Design, DSD 2018, IEEE, 2018, pp. 699–706.
[32] D. Li, W. Peng, W. Deng, F. Gai, A blockchain-based authentication and security mechanism for IoT, in: Proceedings - International Conference on Computer Communications and Networks, ICCCN, Vol. 2018-July, IEEE, 2018, pp. 1–6.
[33] A.C. Tsolakis, I. Moschos, K. Votis, D. Ioannidis, T. Dimitrios, P. Pandey, S. Katsikas, E. Kotsakis, R. García-Castro, A secured and trusted demand response system based on blockchain technologies, in: 2018 Innovations in Intelligent Systems and Applications (INISTA), IEEE, 2018, pp. 1–6.
[34] P. Mell, Managed blockchain based cryptocurrencies with consensus enforced rules and transparency, in: IEEE Intl. Conf. on Trust, Security and Privacy in Computing and Communications, IEEE, 2018, pp. 1287–1296.
[35] E. Heilman, F. Baldimtsi, S. Goldberg, Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions, 2016, pp. 43–60.
[36] Z. Yang, K. Yang, L. Lei, K. Zheng, V.C. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet Things J. 6 (2) (2018) 1495–1505.
[37] X. Liang, S. Shetty, D. Tosh, Y. Ji, D. Li, Towards a reliable and accountable cyber supply chain in energy delivery system using blockchain, in: Intl. Conf. on Security and Privacy in Communication Systems, Springer, 2018, pp. 43–62.
[38] J. Wang, M. Li, Y. He, H. Li, K. Xiao, C. Wang, A blockchain based privacy-preserving incentive mechanism in crowdsensing applications, IEEE Access 6 (2018) 17545–17556.
[39] M.H. Ibrahim, Securecoin: A robust secure and efficient protocol for anonymous bitcoin ecosystem., IJ Netw. Secur. 19 (2) (2017) 295–312.
[40] M. Andrychowicz, S. Dziembowski, D. Malinowski, L. Mazurek, Secure multiparty computations on bitcoin, in: 2014 IEEE Symposium on Security and Privacy, IEEE, 2014, pp. 443–458.
[41] Z. Lu, W. Liu, Q. Wang, G. Qu, Z. Liu, A privacy-preserving trust model based on blockchain for VANETs, IEEE Access 6 (2018) 45655–45664, http://dx.doi.org/10.1109/ACCESS.2018.2864189.
[42] Y. Liu, J. Zhang, Q. Gao, A blockchain-based secure cloud files sharing scheme with fine-grained access control, in: 2018 International Conference on Networking and Network Applications (NaNA), IEEE, 2018, pp. 277–283.
[43] Y. Zhu, Y. Qin, G. Gan, Y. Shuai, W.C.-C. Chu, Tbac: transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization, in: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), 1, IEEE, 2018, pp. 535–544.
[44] J. Xue, C. Xu, Y. Zhang, Private blockchain-based secure access control for smart home systems, KSII Trans. Internet Inf. Syst. 12 (12) (2018) 6057–6078.
[45] L. Xie, Y. Ding, H. Yang, X. Wang, Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets, IEEE Access 7 (2019) 56656–56666, http://dx.doi.org/10.1109/ACCESS.2019.2913682.
[46] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, J. Mendling, Untrusted business process monitoring and execution using blockchain, in: Intl. Conf. on Business Process Management, Springer, 2016, pp. 329–347.
[47] E.F. Kfoury, D.J. Khoury, Secure end-to-end volte based on ethereum blockchain, in: 2018 41st International Conference on Telecommunications and Signal Processing (TSP), IEEE, 2018, pp. 1–5.
[48] G. Zyskind, O. Nathan, A.S. Pentland, Decentralizing privacy: Using blockchain to protect personal data, in: Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, 2015, pp. 180–184.
[49] S. Wang, R. Pei, Y. Zhang, Eidm: A ethereum-based cloud user identity management protocol, IEEE Access 7 (2019) 115281–115291, http://dx.doi.org/10.1109/ACCESS.2019.2933989.
[50] S. Ali, G. Wang, M.Z.A. Bhuiyan, H. Jiang, Secure data provenance in cloud-centric internet of things via blockchain smart contracts, in: IEEE SmartWorld, IEEE, 2018, pp. 991–998.
[51] H. Hasan, K. Salah, Combating deepfake videos using blockchain and smart contracts, IEEE Access 7 (2019) 41596–41606, http://dx.doi.org/10.1109/ACCESS.2019.2905689.
[52] B. Shahzad, J. Crowcroft, Trustworthy electronic voting using adjusted blockchain technology, IEEE Access 7 (2019) 24477–24488.
[53] K. Gai, Y. Wu, L. Zhu, M. Qiu, M. Shen, Privacy-preserving energy trading using consortium blockchain in smart grid, IEEE Trans. Ind. Inf. 15 (6) (2019) 3548–3558.
[54] W. She, Q. Liu, Z. Tian, J. Chen, B. Wang, W. Liu, Blockchain trust model for malicious node detection in wireless sensor networks, IEEE Access 7 (2019) 38947–38956, http://dx.doi.org/10.1109/ACCESS.2019.2902811.
[55] H. Liu, Y. Zhang, S. Zheng, Y. Li, Electric vehicle power trading mechanism based on blockchain and smart contract in V2g network, IEEE Access 7 (2019) 160546–160558, http://dx.doi.org/10.1109/ACCESS.2019.2951057.
[56] S. Li, M. Liu, S. Wei, A distributed authentication protocol using identity-based encryption and blockchain for LEO network, in: Intl. Conf. on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, 2017, pp. 446–460.
[57] C. Decusatis, K. Lotay, Secure, decentralized energy resource management using the ethereum blockchain, IEEE Intl. Conf on Trust, Security and Privacy in Computing and Communications (2018) 1907–1913.
[58] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, S. Goldberg, Tumblebit: An untrusted bitcoin-compatible anonymous payment hub, in: Network and Distributed System Security Symposium, 2017.
[59] K.R. Ozyilmaz, A. Yurdakul, Designing a blockchain-based IoT with ethereum, swarm, and lora: the software solution to create high availability with minimal security risks, IEEE Consum. Electron. Mag. 8 (2) (2019) 28–34.
[60] J. Frankenfield, Block header (cryptocurrency), 2019, URL https://www.investopedia.com/terms/b/block-header-cryptocurrency.asp (Last access Feb. 2021).
[61] J. Gao, K.O. Asamoah, E.B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang, G. Dong, Gridmonitoring: Secured sovereign blockchain based monitoring on smart grid, IEEE Access 6 (2018) 9917–9925.

[62] S. Wang, Y. Zhang, Y. Zhang, A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, IEEE Access 6 (2018) 38437–38450.
[63] D. Augot, H. Chabanne, O. Clémot, W. George, Transforming face-to-face identity proofing into anonymous digital identity using the bitcoin blockchain, in: 15th Annual Conf. on Privacy, Security and Trust (PST), IEEE, 2017.
[64] Z. Sui, S. Lai, C. Zuo, X. Yuan, J.K. Liu, H. Qian, An encrypted database with enforced access control and blockchain validation, in: International Conference on Information Security and Cryptology, Springer, 2018, pp. 260–273.
[65] G.G. Dagher, P.B. Marella, M. Milojkovic, J. Mohler, Broncovote: Secure voting system using ethereum's blockchain, 2018.
[66] K. Bendiab, N. Kolokotronis, S. Shiaeles, S. Boucherkha, Wip: A novel blockchain-based trust model for cloud identity management, in: Intl Conf on Dependable, Autonomic and Secure Computing, IEEE, 2018, pp. 724–729.
[67] D. Lin, Y. Tang, Blockchain consensus based user access strategies in D2d networks for data-intensive applications, IEEE Access 6 (2018) 72683–72690.
[68] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 1999.
[69] A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, Blockchain: A distributed solution to automotive security and privacy, IEEE Commun. Mag. 55 (12) (2017) 119–125, http://dx.doi.org/10.1109/MCOM.2017.1700879.
[70] Y. Kanza, E. Safra, Cryptotransport: blockchain-powered ride hailing while preserving privacy, pseudonymity and trust, in: Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, ACM, 2018, pp. 540–543.
[71] T. Ruffing, P. Moreno-Sanchez, Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin, in: International Conference on Financial Cryptography and Data Security, Springer, 2017, pp. 133–154.
[72] M. Shen, X. Tang, L. Zhu, X. Du, M. Guizani, Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities, IEEE Internet Things J. 6 (5) (2019) 7702–7712.
[73] C. Lin, D. He, X. Huang, K.-K.R. Choo, A.V. Vasilakos, Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, J. Netw. Comput. Appl. 116 (2018) 42–52.
[74] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium blockchain for secure energy trading in industrial internet of things, IEEE Trans. Ind. Inf. 14 (8) (2017) 3690–3700.
[75] S. Rathore, B.W. Kwon, J.H. Park, BlocksecIoTnet: Blockchain-based decentralized security architecture for IoT network, J. Netw. Comput. Appl. 143 (2019) 167–177.
[76] K. Zhao, S. Tang, B. Zhao, Y. Wu, Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing, IEEE Access 7 (2019) 74694–74710.
[77] Series Y: Global Information Infrastructure, internet Protocol Aspects And next-Generation Networks, Recommendation ITU-T Y.2060, 2012.
[78] W. Dai, J. Deng, Q. Wang, C. Cui, D. Zou, H. Jin, SBLWT: A secure blockchain lightweight wallet based on trustzone, IEEE Access 6 (2018) 40638–40648.
[79] M. Takemiya, B. Vanieiev, Sora identity: Secure, digital identity on the blockchain, Int. Comput. Softw. Appl. Conf. 2 (2018) 582–587.
[80] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: Intl. Conf. on Pervasive Computing and Communications Workshops, IEEE, 2017, pp. 618–623.
[81] O. Novo, Blockchain meets IoT: An architecture for scalable access management in IoT, IEEE Internet Things J. 5 (2) (2018) 1184–1195.
[82] C. Xu, H. Liu, P. Li, P. Wang, A remote attestation security model based on privacy-preserving blockchain for V2x, IEEE Access 6 (2018) 67809–67818.
[83] A.S. Tanenbaum, M.V. Steen, Distributed Systems: Principles and Paradigms, first ed., Prentice Hall PTR, USA, 2001.
[84] Amazon, What is cloud computing? - amazon web services, 2021, URL https://aws.amazon.com/what-is-cloud-computing/ (Last access Feb. 2021).
[85] F. Benhamouda, S. Halevi, T. Halevi, Supporting private data on hyperledger fabric with secure multiparty computation, in: Proc. IEEE Intl Conf. on Cloud Engineering, IEEE, 2018, pp. 357–363.
[86] Y. Lu, Q. Tang, G. Wang, Zebralancer: Private and anonymous crowdsourcing system atop open blockchain, Proc. - Int. Conf. Distrib. Comput. Syst. 2018-July (i) (2018) 853–865.
[87] H.R. Hasan, K. Salah, Proof of delivery of digital assets using blockchain and smart contracts, IEEE Access 6 (2018) 65439–65448.
[88] J. Diaz, S.G. Choi, D. Arroyo, A.D. Keromytis, F.B. Rodriguez, M. Yung, Privacy in e-shopping transactions: Exploring and addressing the trade-offs, in: International Symposium on Cyber Security Cryptography and Machine Learning, Springer, Cham, 2018, pp. 206–226.
[89] I.A. Omar, R. Jayaraman, K. Salah, M. Debe, M. Omar, Enhancing vendor managed inventory supply chain operations using blockchain smart contracts, IEEE Access 8 (2020) 182704–182719.
[90] T.-H. Kim, G. Kumar, R. Saha, M.K. Rai, W.J. Buchanan, R. Thomas, M. Alazab, A privacy preserving distributed ledger framework for global human resource record management: The blockchain aspect, IEEE Access 8 (2020) 96455–96467.
[91] O.B. Mora, R. Rivera, V.M. Larios, J.R. Beltrán-Ramírez, R. Maciel, A. Ochoa, A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures, in: 2018 IEEE International Smart Cities Conference (ISC2), IEEE, 2018, pp. 1–4.
[92] K. Biswas, V. Muthukkumarasamy, Securing smart cities using blockchain technology, in: IEEE Intl. Conf. on High Performance Computing and Communications, IEEE, 2016, pp. 1392–1393.
[93] M. Sharples, J. Domingue, The blockchain and kudos: A distributed system for educational record, reputation and reward, in: European Conference on Technology Enhanced Learning, Springer, 2016, pp. 490–496.
[94] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Dependable Secure Comput. 15 (5) (2018) 840–852.
[95] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, IEEE Access 6 (2018) 11676–11686.
[96] D. Hofman, C. Shannon, B. McManus, V. Lemieux, K. Lam, S. Assadian, R. Ng, Building trust & protecting privacy: Analyzing evidentiary quality in a blockchain proof-of-concept for health research data consent management, in: IEEE Intl. Conf. on Internet of Things, IEEE, 2018, pp. 1650–1656.
[97] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: 2016 2nd International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.
[98] Y. Wang, J. Gao, A regulation scheme based on the ciphertext-policy hierarchical attribute-based encryption in bitcoin system, IEEE Access 6 (2018) 16267–16278.
[99] S. Medury, A. Skjellum, R.R. Brooks, L. Yu, Scraaps: X. 509 certificate revocation using the blockchain-based scrybe secure provenance system, in: Intl. Conf. on Malicious and Unwanted Software, IEEE, 2018, pp. 145–152.
[100] Q. Xing, B. Wang, X. Wang, Poster: Bgpcoin: A trustworthy blockchain-based resource management solution for BGP security, in: ACM SIGSAC Conf. on Comp. and Comms. Security, ACM, 2017, pp. 2591–2593.
[101] M. Saad, M.T. Thai, A. Mohaisen, Poster: deterring ddos attacks on blockchain-based cryptocurrencies through mempool optimization, in: Asia Conference on Computer and Communications Security, ACM, 2018, pp. 809–811.
[102] M.A. Rahman, M.S. Hossain, G. Loukas, E. Hassanain, S.S. Rahman, M.F. Alhamid, M. Guizani, Blockchain-based mobile edge computing framework for secure therapy applications, IEEE Access 6 (2018) 72469–72478.
[103] T. Le, M.W. Mutka, Capchain: A privacy preserving access control framework based on blockchain for pervasive environments, in: Proceedings - 2018 IEEE International Conference on Smart Computing, SMARTCOMP 2018, IEEE, 2018, pp. 57–64, http://dx.doi.org/10.1109/SMARTCOMP.2018.00074, arXiv:1401.0532.
[104] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016, 2016, pp. 839–858, http://dx.doi.org/10.1109/SP.2016.55, arXiv:1608.00771.
[105] J. Gu, B. Sun, X. Du, S. Member, Consortium Blockchain-Based Malware Detection in Mobile Devices, Vol. 6, 2018.
[106] M.T. Hammi, B. Hammi, P. Bellot, A. Serhrouchni, Bubbles of trust: A decentralized blockchain-based authentication system for iot, Comput. Secur. 78 (2018) (2018) 126–142.
[107] D. Chatzopoulos, S. Gujar, B. Faltings, P. Hui, Privacy preserving and cost optimal mobile crowdsensing using smart contracts on blockchain, in: IEEE Intl. Conf. on Mobile Ad Hoc and Sensor Systems, 2018, pp. 442–450.
[108] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: Intl. Conf. on Open and Big Data, 2016, pp. 25–30, http://dx.doi.org/10.1109/OBD.2016.11.
[109] Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, Medshare: Trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.
[110] B. Gipp, J. Kosti, C. Breitinger, Securing video integrity using decentralized trusted timestamping on the bitcoin blockchain, in: Proc. of the 10th Mediterranean Conf. on Information Systems (MCIS), 2016, pp. 51.
[111] N.D. Sarier, Privacy preserving biometric identification on the bitcoin blockchain, in: A. Castiglione, F. Pop, M. Ficco, F. Palmieri (Eds.), Cyberspace Safety and Security, 2018, pp. 254–269.
[112] G. Bramm, M. Gall, J. Schütte, Bdabe-blockchain-based distributed attribute based encryption., in: ICETE (2), 2018, pp. 265–276.

[113] B. Leiding, A. Norta, Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance, in: Int. Conf. on Future Data and Security Engineering, Springer, 2017, pp. 181–196.
[114] Y. Zhang, R.H. Deng, J. Shu, K. Yang, D. Zheng, TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain, IEEE Access 6 (2018) 31077–31087.
[115] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, L. Sun, A blockchain based truthful incentive mechanism for distributed P2p applications, IEEE Access 6 (2018) 27324–27335.
[116] S. Tahir, M. Rajarajan, Privacy-preserving searchable encryption framework for permissioned blockchain networks, in: IEEE Intl. Conf. on Internet of Things, IEEE, 2018, pp. 1628–1633.
[117] T. Hepp, P. Wortner, A. Schönhals, B. Gipp, Securing physical assets on the blockchain: Linking a novel object identification concept with distributed ledgers, in: Proc. 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, in: CryBlock'18, ACM, 2018, pp. 60–65.
[118] M. Dai, S. Zhang, H. Wang, S. Jin, A low storage room requirement framework for distributed ledger in blockchain, IEEE Access 6 (2018) 22970–22975.
[119] A. Narayanan, J. Clark, Bitcoin's academic pedigree, Commun. ACM 60 (12) (2017) 36–45, http://dx.doi.org/10.1145/3132259.
[120] Deloitte, Blockchain survey 2019, Deloitte (2019) URL https://www2.deloitte.com/insights/us/en/topics/understanding-blockchain-potential/global-blockchain-survey.html?id=us:2em:3pa:emerging-technologies:eng:di:050619.
[121] N. Hewett, W. Lehmacher, Y. Wang, World Econ. Forum (March) (2019) 26.
[122] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. 107 (2020) 841–853.
[123] J. Leng, M. Zhou, L.J. Zhao, Y. Huang, Y. Bian, Blockchain security: A survey of techniques and research directions, IEEE Trans. Serv. Comput. (2020).
[124] F. Dai, Y. Shi, N. Meng, L. Wei, Z. Ye, From bitcoin to cybersecurity: A comparative study of blockchain application and security issues, in: 2017 4th International Conference on Systems and Informatics (ICSAI), IEEE, 2017, pp. 975–979.
[125] N. Tariq, M. Asim, F. Al-Obeidat, M. Zubair Farooqi, T. Baker, M. Hammoudeh, I. Ghafir, The security of big data in fog-enabled IoT applications including blockchain: A survey, Sensors 19 (8) (2019) 1788.
[126] B.K. Mohanta, D. Jena, S.S. Panda, S. Sobhanayak, Blockchain technology: A survey on applications and security privacy challenges, Internet Things 8 (2019) 100107.
[127] J. Leng, S. Ye, M. Zhou, J.L. Zhao, Q. Liu, W. Guo, W. Cao, L. Fu, Blockchain-secured smart manufacturing in industry 4.0: A survey, IEEE Trans. Syst. Man Cybern.: Syst. (2020).
[128] P.J. Taylor, T. Dargahi, A. Dehghantanha, R.M. Parizi, K.-K.R. Choo, A systematic literature review of blockchain cyber security, Digit. Commun. Netw. 6 (2) (2020) 147–156, http://dx.doi.org/10.1016/j.dcan.2019.01.005, URL http://www.sciencedirect.com/science/article/pii/S2352864818301536.
[129] S. Shi, D. He, L. Li, N. Kumar, M.K. Khan, K.-K.R. Choo, Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey, Comput. Secur. (2020) 101966.
[130] M. Bartoletti, B. Bellomy, L. Pompianu, A journey into bitcoin metadata, J. Grid Comput. 17 (1) (2019) 3–22.
[131] L. Lesavre, A taxonomic approach to understanding emerging blockchain identity management systems, 2019, arXiv Preprint arXiv:1908.00929.
[132] Bitcoin stack exchange, 2021, URL https://bitcoin.stackexchange.com/ (Last access Feb. 2021).
[133] Ethereum stack exchange, 2021, URL https://ethereum.stackexchange.com/ (Last access Feb. 2021).
[134] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, Y.-X. Yang, A secure cryptocurrency scheme based on post-quantum blockchain, IEEE Access 6 (2018) 27205–27213.
[135] C. Lin, D. He, X. Huang, M.K. Khan, K.-K.R. Choo, A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems, IEEE Access 6 (2018) 28203–28212.
[136] H.-W. Kim, Y.-S. Jeong, Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain, Hum.-Cent. Comput. Inf. Sci. 8 (1) (2018) 11.
[137] J. Chen, Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks, ACM SIGBED Rev. 15 (5) (2018) 22–28.
[138] X. Feng, J. Ma, T. Feng, Y. Miao, X. Liu, Consortium blockchain-based SIFT: Outsourcing encrypted feature extraction in the D2d network, IEEE Access 6 (2018) 52248–52260.
[139] X. Huang, C. Xu, P. Wang, H. Liu, Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem, IEEE Access 6 (2018) 13565–13574.
[140] P.K. Sharma, M.-Y. Chen, J.H. Park, A software defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access 6 (2017) 115–124.
[141] Y. Niu, L. Wei, C. Zhang, J. Liu, Y. Fang, An anonymous and accountable authentication scheme for wi-fi hotspot access with the bitcoin blockchain, in: IEEE/CIC Intl. Conf. on Communications in China, IEEE, 2017.
[142] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami, Blockchain contract: Securing a blockchain applied to smart contracts, in: 2016 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2016, pp. 467–468.
[143] I. Miers, C. Garman, M. Green, A.D. Rubin, Zerocoin: Anonymous distributed e-cash from bitcoin, in: 2013 IEEE Symposium on Security and Privacy, IEEE, 2013, pp. 397–411.
[144] E. Kfoury, D. Khoury, Securing natted IoT devices using ethereum blockchain and distributed TURN servers, in: 2018 10th International Conference on Advanced Infocomm Technology (ICAIT), IEEE, 2018, pp. 115–121.
[145] S. Wang, S. Zhu, Y. Zhang, Blockchain-based mutual authentication security protocol for distributed RFID systems, in: 2018 IEEE Symposium on Computers and Communications (ISCC), IEEE, 2018, pp. 00074–00077.
[146] B. Zhou, H. Li, L. Xu, An authentication scheme using identity-based encryption & blockchain, in: 2018 IEEE Symposium on Computers and Communications (ISCC), IEEE, 2018, pp. 00556–00561.
[147] M. Nuss, A. Puchta, M. Kunz, Towards blockchain-based identity and access management for internet of things in enterprises, in: International Conference on Trust and Privacy in Digital Business, Springer, 2018, pp. 167–181.
[148] Z. Lu, Q. Wang, G. Qu, Z. Liu, Bars: a blockchain-based anonymous reputation system for trust management in vanets, in: IEEE Intl. Conf. on Trust, Security and Privacy in Computing and Communications, IEEE, 2018, pp. 98–103.
[149] R. Neisse, G. Steri, I.N. Fovino, Blockchain-based identity management and data usage control, in: IFIP International Summer School on Privacy and Identity Management, Springer, 2017, pp. 237–239.
[150] N. Alexopoulos, J. Daubert, M. Muhlhauser, S.M. Habib, Beyond the hype: On using blockchains in trust management for authentication, in: Intl. Conf. on Trust, Security and Privacy in Computing and Communications, 2017, pp. 546–553, arXiv:1711.04591.
[151] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J.A. Kroll, E.W. Felten, Mixcoin: Anonymity for bitcoin with accountable mixes, in: Intl. Conf. on Financial Cryptography and Data Security, Springer, 2014, pp. 486–504.
[152] E.B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, Zerocash: Decentralized anonymous payments from bitcoin, in: IEEE Symp. on Security and Privacy, IEEE, 2014, pp. 459–474.
[153] Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu, W.C.-C. Chu, Digital asset management with distributed permission over blockchain and attribute-based access control, in: 2018 IEEE International Conference on Services Computing (SCC), IEEE, 2018, pp. 193–200.
[154] M. Almakhour, L. Sliman, A.E. Samhat, W. Gaaloul, Trustless blockchain-based access control in dynamic collaboration., in: BDCSIntell, 2018, pp. 27–33.
[155] X. Chen, J. Ji, C. Luo, W. Liao, P. Li, When machine learning meets blockchain: A decentralized, privacy-preserving and secure design, in: IEEE Intl. Conf. on Big Data, 2018, pp. 1178–1187.
[156] C. Badertscher, P. Gaži, A. Kiayias, A. Russell, V. Zikas, Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2018, pp. 913–930.
[157] P. Urien, Blockchain iot (biot): A new direction for solving internet of things security and trust issues, in: Cloudification of the Internet of Things, IEEE, 2018.
[158] R.B. Uriarte, R. De Nicola, K. Kritikos, Towards distributed sla management with smart contracts and blockchain, in: Intl. Conf. on Cloud Computing Technology and Science, IEEE, 2018, pp. 266–271.
[159] H. Zhou, C. de Laat, Z. Zhao, Trustworthy cloud service level agreement enforcement with blockchain based smart contract, in: Intl. Conf. on Cloud Computing Technology and Science, IEEE, 2018, pp. 255–260.
[160] K. Azbeg, O. Ouchetto, S.J. Andaloussi, L. Fetjah, A. Sekkaki, Blockchain and IoT for security and privacy: A platform for diabetes self-management, in: 4th Intl. Conf. on Cloud Computing Tech. and Apps, IEEE, 2018.
[161] K. Shuaib, J.A. Abdella, F. Sallabi, M. Abdel-Hafez, Using blockchains to secure distributed energy exchange, in: Intl. Conf on Control, Decision and Information Technologies, IEEE, 2018, pp. 622–627.
[162] Y. Wang, Z. Su, Q. Xu, N. Zhang, Contract based energy blockchain for secure electric vehicles charging in smart community, in: Intl Conf on Dependable, Autonomic and Secure Computing, IEEE, 2018, pp. 323–327.
[163] D. Mendes, I. Rodrigues, C. Fonseca, M. Lopes, J.M. García-Alonso, J. Berrocal, Anonymized distributed PHR using blockchain for openness and non-repudiation guarantee, in: International Conference on Theory and Practice of Digital Libraries, Springer, 2018, pp. 381–385.

[164] N. Zhang, J. Li, W. Lou, Y.T. Hou, Privacyguard: Enforcing private data usage with blockchain and attested execution, in: Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, 2018, pp. 345–353.

[165] R. Sharma, S. Chakraborty, Blockapp: Using blockchain for authentication and privacy preservation in iov, in: IEEE Globecom Workshops, IEEE, 2018, pp. 1–6.

[166] C. Li, B. Palanisamy, Decentralized privacy-preserving timed execution in blockchain-based smart contract platforms, in: 2018 IEEE 25th International Conference on High Performance Computing (HiPC), IEEE, 2018, pp. 265–274.

[167] Ö. Gürcan, M. Agenis-Nevers, Y.-M. Batany, M. Elmtiri, F. Le Fevre, S. Tucci-Piergiovanni, An industrial prototype of trusted energy performance contracts using blockchain technologies, in: IEEE Intl. Conf. on High Performance Computing and Communications, IEEE, 2018, pp. 1336–1343.

[168] S. Kirkman, A data movement policy framework for improving trust in the cloud using smart contracts and blockchains, in: 2018 IEEE International Conference on Cloud Engineering (IC2E), IEEE, 2018, pp. 270–273.

[169] S. Kirkman, R. Newman, A cloud data movement policy architecture based on smart contracts and the ethereum blockchain, in: 2018 IEEE International Conference on Cloud Engineering (IC2E), IEEE, 2018, pp. 371–377.

[170] J. Li, J. Wu, L. Chen, J. Li, Blockchain-based secure and reliable distributed deduplication scheme, in: International Conference on Algorithms and Architectures for Parallel Processing, Springer, 2018, pp. 393–405.

[171] J. Xue, C. Xu, Y. Zhang, L. Bai, Dstore: a distributed cloud storage system based on smart contracts and blockchain, in: Intl. Conf. on Algorithms and Architectures for Parallel Processing, Springer, 2018, pp. 385–401.

[172] P.J. Lu, L.-Y. Yeh, J.-L. Huang, An privacy-preserving cross-organizational authentication/authorization/accounting system using blockchain technology, in: IEEE Intl. Conf. on Communications, IEEE, 2018, pp. 1–6.

[173] D.B. Rawat, A. Alshaikhi, Leveraging distributed blockchain-based scheme for wireless network virtualization with security and qos constraints, in: Intl. Conf. on Computing, Networking and Communications, IEEE, 2018, pp. 332–336.

[174] A.Z. Ourad, B. Belgacem, K. Salah, Using blockchain for IOT access control and authentication management, in: International Conference on Internet of Things, Springer, 2018, pp. 150–164.

[175] K. Kim, Y. You, M. Park, K. Lee, Ddos mitigation: Decentralized CDN using private blockchain, in: 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), IEEE, 2018, pp. 693–696.

[176] W.-S. Park, D.-Y. Hwang, K.-H. Kim, A TOTP-based two factor authentication scheme for hyperledger fabric blockchain, in: Intl. Conf. on Ubiquitous and Future Networks, IEEE, 2018, pp. 817–819.

[177] A. Alnemari, S. Arodi, V.R. Sosa, S. Pandey, C. Romanowski, R. Raj, S. Mishra, Protecting infrastructure data via enhanced access control, blockchain and differential privacy, in: International Conference on Critical Infrastructure Protection, Springer, 2018, pp. 113–125.

[178] C.S. Kouzinopoulos, K.M. Giannoutakis, K. Votis, D. Tzovaras, A. Collen, S. Katsikas, Implementing a forms of consent smart contract on an IoT-based blockchain to promote user trust, in: 2018 Innovations in Intelligent Systems and Applications (INISTA), IEEE, 2018, pp. 1–6.

[179] L. Mendiboure, M.A. Chalouf, F. Krief, Towards a blockchain-based SD-iov for applications authentication and trust management, in: International Conference on Internet of Vehicles, Springer, 2018, pp. 265–277.

[180] Y. Zhu, X. Song, S. Yang, Y. Qin, Q. Zhou, Secure smart contract system built on SMPC over blockchain, in: Intl. Conf. on Internet of Things, IEEE, 2018, pp. 1539–1544.

[181] K.L. Brousmiche, A. Durand, T. Heno, C. Poulain, A. Dalmieres, E.B. Hamida, Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain, in: IEEE Intl. Conf. on Internet of Things, IEEE, 2018, pp. 1281–1286.

[182] A.S. Omar, O. Basir, Identity management in IoT networks using blockchain and smart contracts, in: IEEE Intl. Conf. on Internet of Things (IThings), IEEE, 2018, pp. 994–1000.

[183] K. Singh, N. Heulot, E.B. Hamida, Towards anonymous, unlinkable, and confidential transactions in blockchain, in: IEEE Intl. Conf. on Internet of Things, IEEE, 2018, pp. 1642–1649.

[184] U.U. Uchibeke, K.A. Schneider, S.H. Kassani, R. Deters, Blockchain access control ecosystem for big data security, in: IEEE Intl. Conf. on Internet of Things (iThings), IEEE, 2018, pp. 1373–1378.

[185] P. Holl, E. Scepankova, F. Matthes, Smart contract based api usage tracking on the ethereum blockchain, Softw. Eng. Softw. Manag. 2018 (2018).

[186] S. Ali, G. Wang, B. White, R.L. Cottrell, A blockchain-based decentralized data storage and access framework for pinger, in: Proc. 17th IEEE Intl. Conf. on Trust, Sec. and Priv. in Computing and Comms., IEEE, 2018, pp. 1303–1308.

[187] B. Li, Y. Wang, Rzkpb: a privacy-preserving blockchain-based fair transaction method for sharing economy, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1164–1169.

[188] B. Li, Y. Wang, P. Shi, H. Chen, L. Cheng, Fppb: a fast and privacy-preserving method based on the permissioned blockchain for fair transactions in sharing economy, in: 17th IEEE Intl. Conf. on Trust, Security and Privacy in Computing and Communications, IEEE, 2018, pp. 1368–1373.

[189] Y. Yuan, F.-Y. Wang, Towards blockchain-based intelligent transportation systems, in: Intl. Conf. on Intelligent Transportation Systems (ITSC), IEEE, 2016, pp. 2663–2668.

[190] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. 40 (10) (2016) 218.

[191] S.A. Abeyratne, R.P. Monfared, Blockchain ready manufacturing supply chain using distributed ledger, 2016.

[192] M. Andrychowicz, S. Dziembowski, D. Malinowski, Ł. Mazurek, Fair two-party computations via bitcoin deposits, in: International Conference on Financial Cryptography and Data Security, Springer, 2014, pp. 105–121.

[193] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: Proceedings - 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2017, 2017, pp. 468–477, http://dx.doi.org/10.1109/CCGRID.2017.8.

[194] P.K. Sharma, S.Y. Moon, J.H. Park, Block-VN: A distributed blockchain based vehicular network architecture in smart city., JIPS 13 (1) (2017) 184–195.

[195] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C.P. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Internet Things J. 4 (6) (2017) 1832–1843.

[196] A. Ouaddah, A. Abou Elkalam, A. Ait Ouahman, Fairaccess: a new blockchain-based access control framework for the internet of things, Secur. Commun. Netw. 9 (18) (2016) 5943–5964.

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

[198] B. Lee, J.H. Lee, Blockchain-based secure firmware update for embedded devices in an internet of things environment, J. Supercomput. 73 (3) (2017) 1152–1167.

[199] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, M. Bertoncini, Blockchain based decentralized management of demand response programs in smart energy grids, Sensors 18 (1) (2018) 162.

[200] M. Ma, G. Shi, F. Li, Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario, IEEE Access 7 (2019) 34045–34059.

[201] D. Zheng, C. Jing, R. Guo, S. Gao, L. Wang, A traceable blockchain-based access authentication system with privacy preservation in vanets, IEEE Access 7 (2019) 117716–117726.

[202] X. Chen, X. Zhang, Secure electricity trading and incentive contract model for electric vehicle based on energy blockchain, IEEE Access 7 (2019) 178763–178778.

[203] M.F. Hinarejos, J.-L. Ferrer-Gomila, L. Huguet-Rotger, A solution for secure certified electronic mail using blockchain as a secure message board, IEEE Access 7 (2019) 31330–31341.

[204] Z. Abou El Houda, A.S. Hafid, L. Khoukhi, Cochain-SC: An intra-and inter-domain ddos mitigation scheme based on blockchain using SDN and smart contract, IEEE Access 7 (2019) 98893–98907.

[205] Y. Wang, A. Zhang, P. Zhang, H. Wang, Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain, IEEE Access 7 (2019) 136704–136719.

[206] L. Xiong, F. Li, S. Zeng, T. Peng, Z. Liu, A blockchain-based privacy-awareness authentication scheme with efficient revocation for multi-server architectures, IEEE Access 7 (2019) 125840–125853.

[207] H. Chai, S. Leng, K. Zhang, S. Mao, Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles, IEEE Access 7 (2019) 175744–175757.

[208] E.-Y. Daraghmi, Y.-A. Daraghmi, S.-M. Yuan, Medchain: a design of blockchain-based system for medical records access and permissions management, IEEE Access 7 (2019) 164595–164613.

[209] S. Ding, J. Cao, C. Li, K. Fan, H. Li, A novel attribute-based access control scheme using blockchain for IoT, IEEE Access 7 (2019) 38431–38441.

[210] H. Li, D. Han, Edurss: A blockchain-based educational records secure storage and sharing scheme, IEEE Access 7 (2019) 179273–179289.

[211] X. Lu, L. Shi, Z. Chen, X. Fan, Z. Guan, X. Du, M. Guizani, Blockchain-based distributed energy trading in energy internet: An sdn approach, IEEE Access 7 (2019) 173817–173826.

[212] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Blockchain for secure ehrs sharing of mobile cloud based e-health systems, IEEE Access 7 (2019) 66792–66806.
[213] A.R. Rajput, Q. Li, M.T. Ahvanooey, I. Masood, EACMS: Emergency access control management system for personal health record based on blockchain, IEEE Access 7 (2019) 84304–84317.
[214] W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, W. Liu, Homomorphic consortium blockchain for smart home system sensitive data privacy preserving, IEEE Access 7 (2019) 62058–62070.
[215] L. Shi, Y. Li, T. Liu, J. Liu, B. Shan, H. Chen, Dynamic distributed honeypot based on blockchain, IEEE Access 7 (2019) 72234–72246.
[216] M. Sidorov, M.T. Ong, R.V. Sridharan, J. Nakamura, R. Ohmura, J.H. Khor, Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains, IEEE Access 7 (2019) 7273–7285.
[217] F. Tang, S. Ma, Y. Xiang, C. Lin, An efficient authentication scheme for blockchain-based electronic health records, IEEE Access 7 (2019) 41678–41689.
[218] S. Wang, C. Huang, J. Li, Y. Yuan, F.-Y. Wang, Decentralized construction of knowledge graphs for deep recommender systems based on blockchain-powered smart contracts, IEEE Access 7 (2019) 136951–136961.
[219] Y. Wu, S. Tang, B. Zhao, Z. Peng, BPTM: Blockchain-based privacy-preserving task matching in crowdsourcing, IEEE Access 7 (2019) 45605–45617.
[220] W. Xiong, L. Xiong, Smart contract based data trading mode using blockchain and machine learning, IEEE Access 7 (2019) 102331–102344.
[221] H. Yang, H. Cha, Y. Song, Secure identifier management based on blockchain technology in ndn environment, IEEE Access 7 (2019) 6262–6268, http://dx.doi.org/10.1109/ACCESS.2018.2885037.
[222] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, C.-C. Liu, Blockchain-based traffic event validation and trust verification for VANETs, IEEE Access 7 (2019) 30868–30877.
[223] Y. Yang, H. Lin, X. Liu, W. Guo, X. Zheng, Z. Liu, Blockchain-based verifiable multi-keyword ranked search on encrypted cloud with fair payment, IEEE Access 7 (2019) 140818–140832.
[224] S. Yao, J. Chen, K. He, R. Du, T. Zhu, X. Chen, Pbcert: Privacy-preserving blockchain-based certificate status validation toward mass storage management, IEEE Access 7 (2019) 6117–6128, http://dx.doi.org/10.1109/ACCESS.2018.2889898.
[225] X. Zhang, X. Chen, Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network, IEEE Access 7 (2019) 58241–58254.
[226] S. Zhang, M. Pu, B. Wang, B. Dong, A privacy protection scheme of microgrid direct electricity transaction based on consortium blockchain and continuous double auction, IEEE Access 7 (2019) 151746–151753.
[227] K. Hao, J. Xin, Z. Wang, K. Cao, G. Wang, Blockchain-based outsourced storage schema in untrusted environment, IEEE Access 7 (2019) 122707–122721.
[228] Y. Yao, X. Chang, J. Mišić, V.B. Mišić, L. Li, Bla: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services, IEEE Internet Things J. 6 (2) (2019) 3775–3784.
[229] S. Biswas, K. Sharif, F. Li, B. Nour, Y. Wang, A scalable blockchain framework for secure transactions in IoT, IEEE Internet Things J. 6 (3) (2019) 4650–4659, http://dx.doi.org/10.1109/JIOT.2018.2874095.
[230] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, Y. Yang, Blockchain-based secure time protection scheme in iot, IEEE Internet Things J. 6 (3) (2019) 4671–4679, http://dx.doi.org/10.1109/JIOT.2018.2874222.
[231] K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks, IEEE Internet Things J. 6 (5) (2019) 7992–8004.
[232] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, IEEE Internet Things J. 6 (3) (2019) 4660–4670, http://dx.doi.org/10.1109/JIOT.2018.2875542.
[233] M. Li, L. Zhu, X. Lin, Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing, IEEE Internet Things J. 6 (3) (2019) 4573–4584, http://dx.doi.org/10.1109/JIOT.2018.2868076.
[234] O. Novo, Scalable access management in IoT using blockchain: A performance evaluation, IEEE Internet Things J. 6 (3) (2019) 4694–4701, http://dx.doi.org/10.1109/JIOT.2018.2879679.
[235] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, Y. Zhao, Edgechain: An edge-IoT framework and prototype based on blockchain and smart contracts, IEEE Internet Things J. 6 (3) (2019) 4719–4732, http://dx.doi.org/10.1109/JIOT.2018.2878154.
[236] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, N. Zhang, A secure charging scheme for electric vehicles with smart communities in energy blockchain, IEEE Internet Things J. 6 (3) (2019) 4601–4613, http://dx.doi.org/10.1109/JIOT.2018.2869297.
[237] H. Wang, Q. Wang, D. He, Q. Li, Z. Liu, Bbars: Blockchain-based anonymous rewarding scheme for v2g networks, IEEE Internet Things J. 6 (2) (2019) 3676–3687.
[238] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet Things J. 6 (5) (2019) 8770–8781.
[239] Z. Yang, K. Yang, L. Lei, K. Zheng, V.C.M. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Internet Things J. 6 (2) (2019) 1495–1505, http://dx.doi.org/10.1109/JIOT.2018.2836144.
[240] K. Zhu, Z. Chen, W. Yan, L. Zhang, Security attacks in named data networking of things and a blockchain solution, IEEE Internet Things J. 6 (3) (2019) 4733–4741, http://dx.doi.org/10.1109/JIOT.2018.2877647.
[241] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, P.D. Drobintsev, Trust management in a blockchain based fog computing platform with trustless smart oracles, Future Gener. Comput. Syst. 101 (2019) 747–759.
[242] W. Feng, Z. Yan, Mcs-chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain, Future Gener. Comput. Syst. 95 (2019) 649–666.
[243] L. Chen, W.-K. Lee, C.-C. Chang, K.-K.R. Choo, N. Zhang, Blockchain based searchable encryption for electronic health record sharing, Future Gener. Comput. Syst. 95 (2019) 420–429, http://dx.doi.org/10.1016/j.future.2019.01.018, URL http://www.sciencedirect.com/science/article/pii/S0167739X18314134.
[244] A. Al Omar, M.Z.A. Bhuiyan, A. Basu, S. Kiyomoto, M.S. Rahman, Privacy-friendly platform for healthcare data in cloud based on blockchain environment, Future Gener. Comput. Syst. 95 (2019) 511–521.
[245] M. Yang, T. Zhu, K. Liang, W. Zhou, R.H. Deng, A blockchain-based location privacy-preserving crowdsensing system, Future Gener. Comput. Syst. 94 (2019) 408–418.
[246] L. Zhu, Y. Wu, K. Gai, K.-K.R. Choo, Controllable and trustworthy blockchain-based cloud data management, Future Gener. Comput. Syst. 91 (2019) 527–535.
[247] J. Wan, J. Li, M. Imran, D. Li, et al., A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Trans. Ind. Inf. 15 (6) (2019) 3652–3660.
[248] D. Liu, A. Alahmadi, J. Ni, X. Lin, X. Shen, Anonymous reputation system for iIoT-enabled retail marketing atop pos blockchain, IEEE Trans. Ind. Inf. 15 (6) (2019) 3527–3537.
[249] P.K. Sharma, N. Kumar, J.H. Park, Blockchain-based distributed framework for automotive industry in a smart city, IEEE Trans. Ind. Inf. 15 (7) (2019) 4197–4205, http://dx.doi.org/10.1109/TII.2018.2887101.
[250] Y. Wang, Z. Su, N. Zhang, Bsis: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network, IEEE Trans. Ind. Inf. 15 (6) (2019) 3620–3631.
[251] J. Xu, S. Wang, B.K. Bhargava, F. Yang, A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing, IEEE Trans. Ind. Inf. 15 (6) (2019) 3538–3547.
[252] L. Jiang, S. Xie, S. Maharjan, Y. Zhang, Blockchain empowered wireless power transfer for green and secure internet of things, IEEE Netw. 33 (6) (2019) 164–171.
[253] M. Shen, Y. Deng, L. Zhu, X. Du, N. Guizani, Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach, IEEE Netw. 33 (5) (2019) 27–33.
[254] G. Ali, N. Ahmad, Y. Cao, Q.E. Ali, F. Azim, H. Cruickshank, Bcon: Blockchain based access control across multiple conflict of interest domains, J. Netw. Comput. Appl. 147 (2019) 102440.
[255] D.G. Roy, P. Das, D. De, R. Buyya, Qos-aware secure transaction framework for internet of things using blockchain mechanism, J. Netw. Comput. Appl. 144 (2019) 59–78.
[256] J. Hu, D. He, Q. Zhao, K.-K.R. Choo, Parking management: A blockchain-based privacy-preserving system, IEEE Consum. Electron. Mag. 8 (4) (2019) 45–49.
[257] I. Paliokas, N. Tsoniotis, K. Votis, D. Tzovaras, A blockchain platform in connected medical-device environments: Trustworthy technology to guard against cyberthreats, IEEE Consum. Electron. Mag. 8 (4) (2019) 50–55.
[258] Q. Wang, R.Y.K. Lau, X. Mao, Blockchain-enabled smart contracts for enhancing distributor-to-consumer transactions, IEEE Consum. Electron. Mag. 8 (6) (2019) 22–28.
[259] Y. Chen, H. Xie, K. Lv, S. Wei, C. Hu, Deplest: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks, Inform. Sci. 501 (2019) 100–117.
[260] S. Cao, G. Zhang, P. Liu, X. Zhang, F. Neri, Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain, Inform. Sci. 485 (2019) 427–440.
[261] M. Conti, M. Hassan, C. Lal, Blockauth: Blockchain based distributed producer authentication in icn, Comput. Netw. 164 (2019) 106888.
[262] A. Jindal, G.S. Aujla, N. Kumar, Survivor: A blockchain based edge-as-a-service framework for secure energy trading in sdn-enabled vehicle-to-grid environment, Comput. Netw. 153 (2019) 36–48.
[263] J. An, H. Yang, X. Gui, W. Zhang, R. Gui, J. Kang, Tcns: node selection with privacy protection in crowdsensing based on twice consensuses of blockchain, IEEE Trans. Netw. Serv. Manag. 16 (3) (2019) 1255–1267.

[264] R. Zhu, C. Ding, Y. Huang, Efficient publicly verifiable 2pc over a blockchain with applications to financially-secure computations, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 633–650.

[265] A.S. Sani, D. Yuan, W. Bao, P.L. Yeoh, Z.Y. Dong, B. Vucetic, E. Bertino, Xyreum: A high-performance and scalable blockchain for iiot security and privacy, in: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2019, pp. 1920–1930.

[266] B. Faber, G.C. Michelet, N. Weidmann, R.R. Mukkamala, R. Vatrapu, Bpdims: A blockchain-based personal data and identity management system, in: Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019.

[267] C. Zhang, C. Xu, J. Xu, Y. Tang, B. Choi, Gemˆ 2-tree: A gas-efficient structure for authenticated range queries in blockchain, in: 2019 IEEE 35th International Conference on Data Engineering (ICDE), IEEE, 2019, pp. 842–853.

[268] H. Zhou, X. Ouyang, Z. Ren, J. Su, C. de Laat, Z. Zhao, A blockchain based witness model for trustworthy cloud service level agreement enforcement, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, IEEE, 2019, pp. 1567–1575.

[269] H. Duan, Y. Zheng, Y. Du, A. Zhou, C. Wang, M.H. Au, Aggregating crowd wisdom via blockchain: A private, correct, and robust realization, in: 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom, IEEE, 2019, pp. 1–10.

[270] C.-T. Li, D.-H. Shih, C.-C. Wang, C.-L. Chen, C.-C. Lee, A blockchain based data aggregation and group authentication scheme for electronic medical system, IEEE Access 8 (2020) 173904–173917.

[271] T. Cai, Z. Yang, W. Chen, Z. Zheng, Y. Yu, A blockchain-assisted trust access authentication system for solid, IEEE Access 8 (2020) 71605–71616.

[272] M. Hojjati, A. Shafieinejad, H. Yanikomeroglu, A blockchain-based authentication and key agreement (AKA) protocol for 5g networks, IEEE Access 8 (2020) 216461–216476.

[273] Z. Liu, D. Wang, J. Wang, X. Wang, H. Li, A blockchain-enabled secure power trading mechanism for smart grid employing wireless networks, IEEE Access 8 (2020) 177745–177756.

[274] X. Xiang, M. Wang, W. Fan, A permissioned blockchain-based identity management and user authentication scheme for E-health systems, IEEE Access 8 (2020) 171771–171783.

[275] P. Zeng, X. Wang, H. Li, F. Jiang, R. Doss, A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology, IEEE Access 8 (2020) 33644–33657.

[276] L. Xiao, D. Han, X. Meng, W. Liang, K.-C. Li, A secure framework for data sharing in private blockchain-based WBANs, IEEE Access 8 (2020) 153956–153968.

[277] M.F. Hinarejos, J.-L. Ferrer-Gomila, A solution for secure multi-party certified electronic mail using blockchain, IEEE Access 8 (2020) 102997–103006.

[278] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, K. Yu, Authprivacychain: A blockchain-based access control framework with privacy protection in cloud, IEEE Access 8 (2020) 70604–70615.

[279] N. Garg, M. Wazid, A.K. Das, D.P. Singh, J.J. Rodrigues, Y. Park, Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment, IEEE Access 8 (2020) 95956–95977.

[280] H. Xu, Q. He, X. Li, B. Jiang, K. Qin, Bdss-FA: A blockchain-based data security sharing platform with fine-grained access control, IEEE Access 8 (2020) 87552–87561.

[281] F. Zerka, V. Urovi, A. Vaidyanathan, S. Barakat, R.T. Leijenaar, S. Walsh, H. Gabrani-Juma, B. Miraglio, H.C. Woodruff, M. Dumontier, et al., Blockchain for privacy preserving and trustworthy distributed machine learning in multicentric medical imaging (c-distrim), IEEE Access 8 (2020) 183939–183951.

[282] J. Sun, X. Yao, S. Wang, Y. Wu, Blockchain-based secure storage and access scheme for electronic medical records in IPFS, IEEE Access 8 (2020) 59389–59401.

[283] A.S. Hosen, S. Singh, P.K. Sharma, U. Ghosh, J. Wang, I.-H. Ra, G.H. Cho, Blockchain-based transaction validation protocol for a secure distributed iot network, IEEE Access 8 (2020) 117266–117277.

[284] C.-H. Liao, H.-E. Lin, S.-M. Yuan, Blockchain-enabled integrated market platform for contract production, IEEE Access 8 (2020) 211007–211027.

[285] S. Kakei, Y. Shiraishi, M. Mohri, T. Nakamura, M. Hashimoto, S. Saito, Cross-certification towards distributed authentication infrastructure: A case of hyperledger fabric, IEEE Access 8 (2020) 135742–135757.

[286] Y. Chen, H. Yin, Y. Xiang, W. Ren, Y. Ren, N.N. Xiong, Cvt: A crowdsourcing video transcoding scheme based on blockchain smart contracts, IEEE Access 8 (2020) 220672–220681.

[287] Y. Miao, Q. Huang, M. Xiao, H. Li, Decentralized and privacy-preserving public auditing for cloud storage based on blockchain, IEEE Access 8 (2020) 139813–139826.

[288] Y. Long, Y. Chen, W. Ren, H. Dou, N.N. Xiong, Depet: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and K-anonymity, IEEE Access 8 (2020) 192587–192596.

[289] S. Son, J. Lee, M. Kim, S. Yu, A.K. Das, Y. Park, Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain, IEEE Access 8 (2020) 192177–192191.

[290] A. Gu, Z. Yin, C. Cui, Y. Li, Integrated functional safety and security diagnosis mechanism of cps based on blockchain, IEEE Access 8 (2020) 15241–15255.

[291] M. Debe, K. Salah, M.H.U. Rehman, D. Svetinovic, Monetization of services provided by public fog nodes using blockchain and smart contracts, IEEE Access 8 (2020) 20118–20128.

[292] A. Pinheiro, E.D. Canedo, R.T. De Sousa, R.D.O. Albuquerque, Monitoring file integrity using blockchain and smart contracts, IEEE Access 8 (2020) 198548–198579.

[293] A.E.B. Tomaz, J.C. Do Nascimento, A.S. Hafid, J.N. De Souza, Preserving privacy in mobile health systems using non-interactive zero-knowledge proof and blockchain, IEEE Access 8 (2020) 204441–204458.

[294] B. Ernest, J. Shiguang, Privacy enhancement scheme (PES) in a blockchain-edge computing environment, IEEE Access 8 (2020) 25863–25876.

[295] W. Li, H. Guo, M. Nejad, C.-C. Shen, Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach, IEEE Access 8 (2020) 181733–181743.

[296] M.A. Rahman, M.S. Hossain, M.S. Islam, N.A. Alrajeh, G. Muhammad, Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach, Ieee Access 8 (2020) 205071–205087.

[297] H. Tan, I. Chung, Secure authentication and key management with blockchain in vanets, IEEE Access 8 (2019) 2482–2498.

[298] D. Wang, X. Zhang, Secure data sharing and customized services for intelligent transportation based on a consortium blockchain, IEEE Access 8 (2020) 56045–56059.

[299] B. Liu, L. Xiao, J. Long, M. Tang, O. Hosam, Secure digital certificate-based data access control scheme in blockchain, IEEE Access 8 (2020) 91751–91760.

[300] T.A. Alghamdi, I. Ali, N. Javaid, M. Shafiq, Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain, IEEE Access 8 (2019) 1048–1061.

[301] A. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh, D. Patel, Secured energy trading using byzantine-based blockchain consensus, IEEE Access 8 (2019) 8554–8571.

[302] M. Zghaibeh, U. Farooq, N.U. Hasan, I. Baig, Shealth: A blockchain-based health system with smart contracts capabilities, IEEE Access 8 (2020) 70030–70043.

[303] T. Liu, J. Wu, L. Chen, Y. Wu, Y. Li, Smart contract-based long-term auction for mobile blockchain computation offloading, IEEE Access 8 (2020) 36029–36042.

[304] M.M. Badr, W. Al Amiri, M.M. Fouda, M.M. Mahmoud, A.J. Aljohani, W. Alasmary, Smart parking system with privacy preservation and reputation management using blockchain, IEEE Access 8 (2020) 150823–150843.

[305] Q. Wang, T. Ji, Y. Guo, L. Yu, X. Chen, P. Li, Trafficchain: A blockchain-based secure and privacy-preserving traffic map, IEEE Access 8 (2020) 60598–60612.

[306] S.-V. Oprea, A. Bâra, A.I. Andreescu, Two novel blockchain-based market settlement mechanisms embedded into smart contracts for securely trading renewable energy, IEEE Access 8 (2020) 212548–212556.

[307] A. Gauhar, N. Ahmad, Y. Cao, S. Khan, H. Cruickshank, E.A. Qazi, A. Ali, Xd-bauth: Blockchain based cross domain authentication and authorization framework for internet of things, IEEE Access 8 (2020) 58800–58816.

[308] X. Liu, H. Huang, F. Xiao, Z. Ma, A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets, IEEE Internet Things J. 7 (5) (2019) 4101–4112.

[309] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, Z. Weizhe, Blockchain-enabled decentralized trust management and secure usage control of IoT big data, IEEE Internet Things J. 7 (5) (2019) 4000–4015.

[310] D.V. Medhane, A.K. Sangaiah, M.S. Hossain, G. Muhammad, J. Wang, Blockchain-enabled distributed security framework for next-generation iot: An edge cloud and software-defined network-integrated approach, IEEE Internet Things J. 7 (7) (2020) 6143–6149.

[311] D. Liu, J. Ni, C. Huang, X. Lin, X.S. Shen, Secure and efficient distributed network provenance for iot: A blockchain-based approach, IEEE Internet Things J. 7 (8) (2020) 7564–7574.

[312] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, K.-K.R. Choo, M. Aledhari, Decentralized authentication of distributed patients in hospital networks using blockchain, IEEE J. Biomed. Health Inf. 24 (8) (2020) 2146–2156.
[313] S. Zhou, H. Huang, W. Chen, P. Zhou, Z. Zheng, S. Guo, Pirate: A blockchain-based secure framework of distributed machine learning in 5g networks, IEEE Netw. 34 (6) (2020) 84–91.
[314] Y. Tian, Z. Wang, J. Xiong, J. Ma, A blockchain-based secure key management scheme with trustworthiness in dwsns, IEEE Trans. Ind. Inf. 16 (9) (2020) 6193–6202.
[315] S. Guo, X. Hu, S. Guo, X. Qiu, F. Qi, Blockchain meets edge computing: A distributed and trusted authentication system, IEEE Trans. Ind. Inf. 16 (3) (2019) 1972–1983.
[316] H. Cui, Z. Wan, X. Wei, S. Nepal, X. Yi, Pay as you decrypt: Decryption outsourcing for functional encryption using blockchain, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3227–3238.
[317] Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, J. Chen, A hybrid blockchain-based identity authentication scheme for multi-wsn, IEEE Trans. Serv. Comput. 13 (2) (2020) 241–251.
[318] S.M. Pournaghi, M. Bayat, Y. Farjami, Medsba: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption, J. Ambient Intell. Humaniz. Comput. (2020) 1–29.
[319] Q. Lyu, Y. Qi, X. Zhang, H. Liu, Q. Wang, N. Zheng, Sbac: A secure blockchain-based access control framework for information-centric networking, J. Netw. Comput. Appl. 149 (2020) 102444.
[320] C. Stach, C. Gritti, D. Przytarski, B. Mitschang, Trustworthy, secure, and privacy-aware food monitoring enabled by blockchains and the IoT, in: 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, 2020, pp. 1–4.
[321] Apple rolls out privacy-focused 'nutrition labels' for apps, 2020, URL https://www.pcmag.com/news/apple-rolls-out-privacy-focused-nutrition-labels-for-apps (Last access Feb. 2021).
[322] S. Hassam, P. De Filippi, Decentralised autonomous organisation, 2021, URL https://policyreview.info/glossary (Last access Feb. 2021).
[323] D. Reis, J. Takeshita, T. Jung, M. Niemier, X.S. Hu, Computing-in-memory for performance and energy efficient homomorphic encryption, 2020, arxiv Preprint arxiv:2005.03002.
[324] B.A. Scriber, A framework for determining blockchain applicability, IEEE Softw. 35 (4) (2018) 70–77, http://dx.doi.org/10.1109/MS.2018.2801552.
[325] A. Pedersen, M. Risius, R. Beck, A ten-step decision path to determine when to use blockchain technologies, MIS Quart. Exec. 18 (2019) 99–115, http://dx.doi.org/10.17705/2msqe.00010.
[326] N. Singh, When to use blockchain technology?, 2020, URL https://101blockchains.com/when-to-use-blockchain/ (Last access Feb. 2021).
[327] I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges., IJ Netw. Secur. 19 (5) (2017) 653–659.
[328] H. Baniata, A. Kertesz, A survey on blockchain-fog integration approaches, IEEE Access 8 (2020) 102657–102668.

Mar Gimenez-Aguilar is Ph.D. student working in the Computer Security Lab at the University Carlos III of Madrid, Spain. She holds a M.Sc. in Cybersecurity, (Carlos III University of Madrid). Her research interests are cybersecurity, specially steganography and cryptography, and blockchain. At the moment, she is focused studying different aspects of cybersecurity in relation with blockchain technologies.

Jose Maria de Fuentes is Associate Professor in the Computer Science and Engineering Department at University Carlos III of Madrid, Spain. He is Computer Scientist Engineer and Ph.D. in Computer Science by the University Carlos III of Madrid. His main research interests are cybersecurity as well as security and privacy in the internet of things and ad-hoc networks. He has published several articles in international conferences and journals. He is participating in several national R+D projects.

Lorena Gonzalez-Manzano is Associate Professor working in the Computer Security Lab at the University Carlos III of Madrid, Spain. She is Computer Scientist Engineer and Ph.D. in Computer Science by the University Carlos III of Madrid. Her Ph.D. focuses on security and privacy in social networks. She is currently focused on Internet of Things and cloud computing security, as well as, on cybersecurity. Indeed, she has published several papers in national and international conferences and journals and she is also involved in national R+D projects.

David Arroyo is Tenured Scientist at the Institute of Physical and Information Technologies of the CSIC, Spain. He is higher Telecommunications Engineer from the University of Seville (2002) and Ph.D. from the Polytechnic University of Madrid (2009). His research activity is focused on the protection of information security and privacy. He is author in international journals and national and international conferences related to his field of expertise. He participates in the committees CTN 320 (Cybersecurity and Protection of Personal Data) and CTN 71/SC 307 (Blockchain and Distributed Registry Technologies) of UNE (Spanish Association for Standardization).