A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review

SEJIN HAN AND SOOYONG PARK
Department of Computer Science and Engineering, Sogang University, Seoul 04107, South Korea
Corresponding author: Sooyong Park (sypark@sogang.ac.kr)

This work was supported in part by the Ministry of Science and, Information and Communication Technologies (MSIT), South Korea, through the Information Technology Research Center (ITRC) Support Program supervised by the Institute for Information & Communications Technology Planning & Evaluation (IITP) under Grant IITP-2022-2017-0-01628.

ABSTRACT As a service platform, blockchain has faced compliance issues since the General Data Protection Regulation (GDPR) came into effect in May 2018. Although many technical solutions have been proposed to solve the compatibility issues between blockchain and the GDPR, unresolved challenges remain. This study presents the gaps between the blockchain and the GDPR and explores solutions to bridge the gap. We review 91 previously published articles using a systematic literature review methodology. Then, we answer the following research questions: 1) Which solutions have been explored to allow the blockchain to comply with the GDPR? 2) What are the research gaps in the blockchain compliance field? Finally, we present five research gaps in this field: 1) development of a consent ontology model; 2) development of a methodology for monitoring fairness in the blockchain; 3) resolution of the contradiction between auditing and obfuscation; 4) development of a methodology for tracking controllers in the blockchain; and 5) integration of the different-purposed technical solutions without conflicts. Our research can raise the compatibility level of the blockchain and GDPR and guide the company adopting a blockchain to comply with the GDPR. Furthermore, it can advise the regulator to embrace new technologies into the GDPR while protecting a blockchain’s nature.

INDEX TERMS Access control, attribute-based encryption (ABE), blockchain, data subject, compliance, confidentiality, controller, general data protection regulation (GDPR), right to be forgotten, traceability.

I. INTRODUCTION
The blockchain was initially developed as a cryptocurrency technology. The growing popularity of cryptocurrencies has helped the technology gain public attention [1], [47], [67], [71], [73]. Ultimately, this has led to the evolution of the blockchain as a service platform. However, the use of the blockchain as a service platform has faced privacy issues. Privacy risks associated with the blockchain might be more serious than those of traditional information technology (IT) systems due to its immutable and decentralized nature [1], [47], [92], [93].

Meanwhile, the General Data Protection Regulation (GDPR) has been in force in the European Union (EU) since May 25, 2018. According to this regulation, the service provider (or controller) processing residents’ personal data in the EU must protect personal data [26], [29]; however, there are challenges to overcome for the blockchain to be compatible with the GDPR [9], [23], [26], [29], [98]. First, identifying the controller in the blockchain is difficult due to its decentralized nature. In a blockchain with no centralized entity, no one may be qualified or, sometimes, everyone is qualified as a controller; thus, the controller cannot be identified.

Second, a blockchain is an “append-only” database, so data cannot be deleted, even when the blockchain’s collection and retention periods expire. This contradicts the GDPR principle (art. 5(1)(b)–(e) GDPR).

Finally, technical references for bridging the gap between the blockchain and the GDPR are scarce. These references help understand regulations from a technician’s rather than a regulator’s point of view and could ultimately help bridge...
the gap. Many of the standardization organizations are releasing documents related to blockchain [2], [3], [94]; however, until now, there are few documents regarding legal and other compliance requirements of blockchain. ISO/TR23244:2020 addresses blockchain compliance. It provides guidelines for personal data protection applied to the blockchain, but it is just an overview [2], [3]. The ITU-T Focus Group on Application of Distributed Ledger Technology (DLT) released FG DLT D4.1, which provides the regulatory framework for DLT. It provides practical recommendations for users, regulators, and technologists to mitigate the risks of the legal concerns of blockchain [2], [3]. Germany has also published a local standard, DIN SPEC 4997. It discusses legal issues related to incorporating blockchains with the GDPR and provides technical guidelines for data protection. However, only outlines are described [2], [3]. In addition, European Union Agency for Network and Information Security (ENISA) and the Commission Nationale de l’Informatique et des Libertes (CNIL), although not standardization organizations, provide advice and best practices for blockchain use cases. ENISA analyzed the security vulnerability of the blockchain and recommended security countermeasures [4], but these only cover the financial sector. Meanwhile, the CNIL provides guidelines for privacy solutions [5], but such solutions are still insufficient to cover various blockchain use cases.

Furthermore, the compatibility of the blockchains and the GDPR is a less studied topic in the academic literature. Previous research proposed technical solutions to address some of the GDPR requirements, but only a few studies address the overall countermeasures to comply with the GDPR. [6] summarized the prior literature on compliance, but there were limits to offering comprehensive technical countermeasures to fill the gap between blockchain and GDPR. [7] identified blockchain as an emerging research front in healthcare by analyzing prior papers but did not address blockchain compliance issues as the main subject. [8] explored privacy-enhanced technology solutions concerning their use in the IoT; however, the focus is on privacy rather than GDPR.

This study presents gaps between the blockchain and the GDPR and explores solutions to bridge the gap. We systematically reviewed 91 relevant studies from major worldwide publisher databases and classified all literature from the perspective of GDPR principles. We presented current research progress, proposed solutions, and unresolved research gaps on blockchain and GDPR compatibility.

We have contributed to the literature by presenting the overall challenges, solutions, and research gap for integrating blockchain and the GDPR. Furthermore, our result can help resolve uncertainties in the EU’s GDPR-compliant blockchain policy and, consequently, can give considerable certainty to blockchain stakeholders.

The rest of the paper is structured as follows. Section II explains the basic concepts related to the blockchain, GDPR, and attribute-based encryption. Section III presents our methodology, Section IV summarizes the findings from the review, and Section V answers the research questions. Section VI discusses the findings and Section VII identifies contributions. Finally, Section VIII concludes the paper.

II. BACKGROUND

A. BLOCKCHAIN

The blockchain was first introduced in 2008 to implement the cryptocurrency bitcoin [10]. The blockchain is built on a peer-to-peer network with no central authority. Every node in the network maintains the same ledger copy, called the distributed ledger. The ledger consists of lists of blocks, which are sets of transactions collected for a certain period in chronological order. Each block is connected by referring to the previous block’s hash value. A new block is approved by a chosen node (called the miner) and appended to the current blockchain as a hash chain. This process is called consensus.

Consensus is a decision-making procedure in a distributed network without a central intermediary. All nodes in the blockchain can maintain the same ledger by consensus. Proof of Work (POW) was the first consensus algorithm adopted in bitcoin. According to the POW requirement, nodes compete with each other to find a number smaller than the difficulty target, and the first node(miner) to solve this problem creates a new block and receives an incentive (cryptocurrency) as a reward [11]. Blocks are generated approximately every 10 mins, however the block generation time is depends on the difficulty of the POW problem, and the difficulty is adjusted to the frequency of cryptocurrency issuance. Besides POW, several consensus algorithms exist, such as Proof Of Stake and Practical Byzantine Fault Tolerance. They are less computing-resource-consuming than POW.

Another key feature of blockchain is smart contracts. Smart contracts are self-executing codes that are automatically triggered if the conditions are met. The smart contracts were introduced with the launch of Ethereum in 2015, and are used by most blockchains, except for Bitcoin.

Meanwhile, blockchains can be divided into two types: permissionless blockchains with no restrictions on participation and permissioned blockchains with restrictions on participation. Although permissionless blockchains meet the initial design goal of the blockchain, that is, “fully decentralized,” it is vulnerable to privacy issues because the permissionless blockchain reveals all data to all participants on the network [51], [93], [100]. On the other hand, permissioned blockchains are more secure in terms of privacy because they can restrict participation and access to data [51], [93], [95], [100].

B. GDPR

The GDPR came into effect on May 25, 2018, to protect the personal data of EU residents. The GDPR replaced the Data Protection Directive 95/46/EC enacted in 1995 and is legally binding in all EU member states. The purpose of the GDPR is to protect the right to personal data protection for natural persons (art. 1(2) GDPR) and to ensure the free movement
of personal data within the EU (art. 1(3) GDPR). The GDPR regulates three entities: 1) the data subject is an individual or legal entity that owns the rights to their personal data; 2) the controller, natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of processing personal data (art. 4(7) GDPR); 3) the processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller (art. 4(8) GDPR). It does not directly hold personal data but processes personal data held by the controller through a contract with the controller. The GDPR specifies that the following rights of the data subject should be guaranteed: the right to be forgotten, the right of restriction to processing, the right to data portability, and the right to object. In addition, the controller’s obligations to protect the data subject’s personal data are as follows: recording of personal data processing activities, designation of a data protection officer (DPO), personal data risk-assessment, and data protection by design and by default. The controller or processor who processes personal data must comply with the seven principles of the GDPR (art. 5 GDPR) shown in Table 1.

### C. ATTRIBUTE-BASED ENCRYPTION

Attribute-based encryption (ABE) is a promising fine-grained access control scheme. It was first introduced in 2005 by Sahai and Waters [13]. ABE is an encryption scheme in which the ciphertext and the user’s secret key depend on attributes (e.g., position and affiliation). A user can decrypt ciphertext if the secret key matches the attribute policy (access structure), which is a predefined attribute set.

ABE is divided into two types: ciphertext policy-ABE (CP-ABE), which includes an access structure in the ciphertext, and key policy-ABE (KP-ABE), which includes an access structure in the user’s secret key [14], [15]. In general, CP-ABE is widely used in reality (this paper also uses CP-ABE). ABE is different from public key infrastructure in that it encrypts data using a public key reflecting user attributes instead of user identification. Thus, it allows a 1:N relationship between the encryptor and the decryptor. ABE is an effective way to restrict access to data in multiparty communication protocols involving the participation of an unspecified majority. However, many attributes or large-size messages will introduce an overhead. The overhead reduction is an important research topic [16], [17], [18]. In addition, revoking user attributes and updating the access structure of encrypted ciphertext are crucial research topics.

### III. METHOD

A systematic literature review (SLR) is a means of evaluating and interpreting all available research that is relevant to a particular research question [85]. We plan, conduct, and report the review of prior literature according to the principles of the SLR.

We select literature using keyword searching. The keywords used are “Blockchain” and “GDPR,” and the logical operator “AND” is used. We used the following procedure to choose the search keywords. We initially derived possible search keywords from the research topic, considering synonyms, abbreviations, and alternative terms for possible search keywords. The following terms were considered as initial keywords: “blockchain,” “Distributed Ledger Technology,” “DLT,” “General Data Protection Regulation,” “GDPR,” and “Privacy.” However, the terms “Distributed Ledger Technology” and “DLT” are excluded from the final search keywords because they are different from the blockchain in technical aspects even though they were derived from the same concepts [51], [95], [96]. In addition, the term “privacy” is excluded because the GDPR requirements are not considered in some papers that only consider “privacy.” Finally, the term “General Data Protection Regulation” is excluded according to the general rules regarding abbreviations/acronyms used in the academic paper. In the rules, all non-standard abbreviations should be written out...
in full at the first instance (in the abstract or introduction section) and followed by the abbreviated form in parenth-
theses, as in “General Data Protection Regulation (GDPR).”
Moreover, in most cases, the term “GDPR” is in the key-
words section. We ultimately included only “blockchain”
and “GDPR” as search keywords.

Then, we chose 32 major academic publisher databases
wherein the terms “blockchain” and “GDPR” were searched
in all articles’ titles, keywords, and abstracts. Instead of
choosing a particular database, such as WoS or Scopus,
we used major academic publisher databases worldwide,
as shown in TABLE 2, to broaden the search scope to include
technical, legal, and emerging blockchain specialized jour-
nals. Additionally, we use citation chaining to expand the
search scope. Citation chaining selects articles from the refer-
ces of searched articles that satisfy the exclusion and inclu-
sion criteria below; In this case, articles discussing privacy
requirements compatible with GDPR principles are accept-
able by inclusion criteria even though they do not address the
GDPR directly. Additionally, the Bitcoin white paper [10],
the official GDPR text [12], ABE research [13], [14], [15],
[16], [17], [18], and review methodology [85] were included
as basic materials for the review process although they do not
address the conflict issues on the GDPR and the blockchain.
The initial search results were extracted on December 27,
2021, and the number of articles was 201.

Then, we extract 91 final articles by applying the following
filtering rules:

**Exclusion criteria:**
- Duplicate articles;
- Articles that focused only on the blockchain or the
  GDPR in general.
- Articles that proposed no idea for blockchain compli-
  ance.

**Inclusion criteria:**
- Articles published in a journal and conference.
- Articles discussing at least one principle of the GDPR.

Fig. 1 describes the results of the search and selection
process, from the number of records identified in the search
to that of studies included in the review.

Table 2 represent initial articles and final articles catego-
rized into publishers. The final articles appear in the “Refer-
ence” section ([1]-[91]) of this paper.

To remove articles that meet the exclusion criteria, we reviewed the initial 201 titles, abstracts, and texts.
Moreover, duplicate articles and articles that only discuss
blockchain and GDPR, in general, are excluded. We also
excluded articles that discuss blockchain’s compliance with
GDPR but only raise issues and do not propose appropriate
solutions.

To include articles that meet the inclusion criteria, we set
the record type to journal and conference in the advanced
search system (https://library.sogang.ac.kr/eds/advanced).
Then, we filtered the articles to select papers that satisfy
the first inclusion criteria, that is, “Articles published in a
journal or conference.” To select papers that meet the second
inclusion criteria, that is, “Articles discussing at least one
principle of the GDPR,” we use GDPR ontology developed
for this review. Fig. 2 expresses GDPR and its related solution
as an ontology. We constructed it using the ontology tool,
“Protege.” The ontology is consists of three classes: articles
of the GDPR, principle of the GDPR, and the recommended
solutions constructed by referring to official references [2],
[4], [5]. The principles of the GDPR is a subclass of the arti-
cles of the GDPR, and parent of the recommended solutions
class. To determine whether the previous articles address
the principles of the GDPR, we searched the ontology using
SPARQL. The core sentence or words related to the GDPR
in the previous articles are used in the SPARQL search. If the
search result exists in the ontology, we determined it as an
article discussing the GDPR principle. Of course, we double-
checked the paper in more detail to ensure whether it contains
the principles of the GDPR.

Next, we defined the research questions that drive the
overall systematic review methodology. The research ques-
tion should be set such that it can solve the concerns
of blockchain stakeholders regarding the main topic of
our research [85]. The blockchain stakeholders and their
concerns are as follows [97]. 1) Blockchain users: The

### TABLE 2. Lists of articles.

| Publisher (Database) | Initial | Search/Citation chaining | Final | Search/Citation chaining |
|----------------------|---------|--------------------------|-------|--------------------------|
| ACM/ACM Digital Library | 16 | 14/2 | 3 | 1/2 |
| William S. Hein & Co., Inc. (HeinOnline) | 8 | 8/0 | 2 | 2/0 |
| MDPI | 13 | 12/1 | 6 | 5/1 |
| Emerald publishing | 4 | 4/0 | 2 | 2/0 |
| Springer-Verlag(SpringerLink) | 8 | 5/3 | 6 | 3/3 |
| Elsevier | 19 | 18/1 | 7 | 6/1 |
| IEEE(IEEE Xplore) | 86 | 72/14 | 34 | 20/14 |
| Taylor & Francis | 1 | 1/0 | 0 | 0/0 |
| Scholastica | 6 | 6/0 | 4 | 4/0 |
| JSTOR | 1 | 1/0 | 1 | 1/0 |
| Frontiers Media | 3 | 3/0 | 2 | 2/0 |
| ISTalks | 1 | 1/0 | 0 | 0/0 |
| HRČAK | 1 | 1/0 | 1 | 1/0 |
| De Gruyter | 3 | 3/0 | 1 | 1/0 |
| IOS press | 3 | 3/0 | 1 | 1/0 |
| Ingenta connect | 5 | 5/0 | 4 | 4/0 |
| NCBI(PubMed) | 2 | 1/1 | 2 | 1/1 |
| Prince of Songkla University | 1 | 1/0 | 0 | 0/0 |
| International Institute of Informatics and Systemics | 1 | 1/0 | 1 | 1/0 |
| Wiley Online Library | 1 | 1/0 | 0 | 0/0 |
| Hindawi | 1 | 1/0 | 1 | 1/0 |
| AIS | 1 | 1/0 | 0 | 0/0 |
| First Monday Editorial Group | 1 | 1/0 | 0 | 0/0 |
| Gesellschaft für Informatik | 1 | 1/0 | 1 | 1/0 |
| SciEpress | 2 | 2/0 | 2 | 2/0 |
| Edward Elgar Publishing(ElgarOnline) | 1 | 1/0 | 1 | 1/0 |
| Citeseer | 1 | 0/1 | 0 | 0/1 |
| The Publications Office of the EU | 1 | 0/1 | 0 | 0/1 |
| others* | 9 | 5/4 | 7 | 3/4 |
| Total | 201 | 173/28 | 91 | 63/28 |

* Cambridge University Press, The University of Petrozavodsk, The University of St Andrews Research, KoreaScience.
number of blockchain users has increased rapidly since 2011, and privacy concerns are growing fastly [97]. 2) Blockchain Developers: All blockchain developers should be aware of human rights, data protection, and privacy and consider how technology can protect individuals’ privacy without hindering technological advances [22]. They are concerned about the
FIGURE 2. A GDPR ontology model for blockchain compliance. This model represents GDPR ontology, including articles, principles, and the recommended solutions for the blockchain to allow compliance with the GDPR.

GDPR requirements and what solutions they can use while designing a blockchain. 3) Data Protection Officers: The data protection officers are responsible for monitoring compliance related to personal data protection, including assignment of responsibilities and related audits, providing advice on data protection impact assessment, and monitoring performance...
TABLE 3. Types of articles.

| Type          | Initial | Final |
|---------------|---------|-------|
| Conference    | 82      | 26    |
| Journal       | 116     | 62    |
| Technical reports | 3      | 3     |
| Total         | 201     | 91    |

TABLE 4. Article publishing years.

| Year | Initial | Final |
|------|---------|-------|
| 2005 | 1       | 1     |
| 2006 | 1       | 1     |
| 2007 | 2       | 2     |
| 2008 | 1       | 1     |
| 2009 | 1       | 1     |
| 2010 | 1       | 1     |
| 2015 | 1       | 1     |
| 2016 | 4       | 3     |
| 2017 | 9       | 7     |
| 2018 | 21      | 10    |
| 2019 | 45      | 18    |
| 2020 | 65      | 26    |
| 2021 | 49      | 19    |
| Total | 201 | 91 |

They are concerned about methods and tools to do these tasks in the blockchain service network. 4) Researchers: Many researchers who study the gap between the blockchain and GDPR have the same stance on establishing privacy-friendly blockchain design options [25] or principles [20], [21], [22], [49] to resolve the contradictions [19], [27], [30], [86] between them. 5) Regulators: Regulators are responsible for monitoring the application of the GDPR, handling complaints, conducting investigations into the application of the GDPR, and monitoring related developments (art. 57(1) GDPR). They have concerns regarding the methods and tools to execute these tasks in the blockchain service network [98].

Blockchain stakeholders have concerns regarding privacy issues and solutions in using, developing, auditing, monitoring, investigating, conducting research, and handling complaints, related with the GDPR compliance in blockchains. We defined the research questions that drive this study, which can best resolve the concerns of the blockchain stakeholders, as follows.

**RQ1. Which solutions have been explored to allow the blockchain to comply with GDPR?**

**RQ2. What are the research gaps in the blockchain compliance field?**

These research questions could address blockchain stakeholders’ concerns and provide directions for future research concerning challenges that have not yet been solved. To address RQ1, we explored the principles of the GDPR and related solutions from the prior literature, referring to Table 1 and Fig 2. The unsolved issues in the extant literature could be found by referring to the GDPR ontology model, shown in Fig 2, to address RQ2.

To present the final reporting, we first identify research trends in blockchain compliance. The published year and article type are identified, and Excel produces the statistics. Then, we categorize the solutions discussed in the article into types and present them in a table and pie chart with the corresponding GDPR principles. Finally, we identify unsolved issues in the previous articles by searching the GDPR ontology. The outcomes are compared with the GDPR ontology to assess reporting bias.

**IV. RESULTS**

**A. ANALYSIS OF THE TRENDS**

The final articles consisted of 62 journal articles, 26 conference articles, and 3 technical reports ([2], [4], [5]). Table 3 presents the article types. They began in 2005, but most papers have been published since 2017. The GDPR came into effect in 2018, and from that point on, blockchain compliance began to be discussed. Papers dealing with the GDPR compliance of blockchain have been steadily published every year since then. Table 4 shows the article publication years.

**B. ADDRESSING RQ1**

For the first research question in this study, we used SPARQL from the GDPR ontology to determine whether previous studies discuss GDPR clauses or principles, and their solutions. We summarize the findings into six groups of GDPR principles. The seven GDPR principles (Table 1) are recategorized into six because some principles have the same concept from the technical point of view.

1) **LAWFULNESS AND PURPOSE LIMITATION**

   **a: CHALLENGE**

   Personal data must be collected for specific, explicit, and legitimate purposes and processed lawfully. For processing to be lawful, personal data should be processed based on the data subject’s consent or some other legitimate basis (Recital 40 GDPR). “Consent” from the data subject means any freely given, specific, informed, and unambiguous indication of the data subject’s wishes by which he or she signifies agreement to the processing of personal data relating to him or her (art. 4(11) GDPR). A data subject could give and withdraw consent to process personal data at any time [2]. Every action of this nature should be written in a tamper-proof access log to prove when the data subjects have granted or revoked their consent to process their personal data [2]. However, implementing a blockchain system for managing such consent is extremely difficult. In particular, it is more challenging for permissionless blockchains with no intermediaries.

   Meanwhile, consent does not always guarantee lawfulness. Consent that is non-informed, implicit, not freely given, or bundled for several processing purposes, such as the current online service network consent culture, does not guarantee the lawfulness of personal data processing [78]. Lawfulness can be guaranteed by consent that satisfies the criteria under the GDPR. Thus, implementing a consent model that meets the GDPR’s valid consent requirements is a significant challenge for blockchain.
Another option for ensuring lawfulness is to process data on a legitimate basis, i.e., process personal data under contractually or legally permissible circumstances. For example, a courier is allowed to collect addresses and contact information to deliver a customer’s ordered goods. Firefighters can collect a person’s identity and location information in an urgent situation; however, measures are required to limit the personal data collected and used according to the controller’s affiliation and status. Such measures could represent significant challenges for permissionless blockchain.

b: SOLUTIONS

We explored the following three types of solution that support the lawfulness and purpose limitation principle in the blockchain.

A smart contract can be a useful tool for implementing consent in the blockchain. Many previous studies have proposed the use of a smart contract-based consent model [31], [33], [40], [43], [45], [46], [57], [60], [61], [63], [64], [66], [67], [74], [75], [79], [80], [81], [82], [83], [87], [88], [89], [90]. In such models, a data subject encodes an access policy or Terms of Service agreement using smart contract language (java, go) and shares it with controller. An access policy or Terms of Service agreement includes the identification of the controller allowed to access, the purpose of the individual activity, information about the collected and used personal data items or the type of personal data, and the consent flag of each above item [60]. A controller can process data only if the consent flag is set to True. Every action executed by the smart contract is recorded in an immutable blockchain to prove compliance. A data subject can inspect all activities.

However, the consent model using smart contracts have some problems. Smart contracts are programmed by humans; hence, they can sometimes be erroneous and cannot be encoded accurately and consistently. Many researchers have proposed a consent ontology model to solve this problem [31], [33], [61], [75], [80], [81], [82], [87]. Consent ontology systematically constructs knowledge expression for the various types of data, such as regulation, the privacy policy of service providers (controller), and consent or withdrawal of data subjects, and provides inference. By searching the consent ontology, we can determine whether the access request is lawful. Consent ontology can be easily encoded into a smart contract and used for automated policy-based access control on the blockchain. The consent ontology model can be created using a resource description framework (RDF) and policy modeling language (OWL, XMACML, and SecKit). Some studies have proposed the use of an intelligent service to detect conflicting rules or policies of ontology [61], [81], [87].

These consent models can also verify whether consent is legally valid based on the GDPR’s requirements. Therefore, non-informed consent, implicit consent, not freely given consent, consent bundled for several processing purposes, and consent for collecting more data than necessary cannot obtain the lawfulness of personal data processing and are rejected in the consent ontology model. In [75], the consent structure is formulated as an ontology using RDFa and stored in the blockchain. The data items users accessible, purpose of processing, retention period, and rights of the data subject, consent or revocation flags are modeled by the ontology. Data access requests are allowed or denied based on the consent structure. The consent ontology model formulated with a policy language (RDFa) is explicit, understandable, reusable, not modified without consent, and transparent. In another consent model, the text-type consent structure is parsed and then expressed as an ontology through a policy language (OWL). Ontology comprises the class of access control policy, the subclasses of collection, consent, external sharing, and access, and the association between the classes [80]. The consent class formulated with policy language provides clarity and consistency without ambiguity.

Consent is stored in the blockchain in the form of a key-value pair. The “key,” called the compound ID or complex ID (c-ID), is the set of public/private key pairs of data subject, controller, and processor. The “value” comprises an access policy (or Terms of Service) and consent flag [64], [74], [75]. A “value” is only allowed to the user with the c-ID.

Another option for lawfulness, data processing on a “legitimate basis,” should be controlled by applicable laws or individual contracts. Access to data shall be controlled according to the controller’s roles and responsibilities, guaranteed by law or assured by the contract between the data subject and the controller. This concept is technically identical to that of the access control mechanism, detailed in the Access Control part of Section IV-B5.

Table 5 and Fig. 3 summarize the solutions supporting the lawfulness and the purpose limitation principle.

2) FAIRNESS

The DIN SPEC 4997 mentions fairness, as follows:
In order for the processing of personal data to be fair, the expectations of the data subjects and the effects on privacy must be considered. This assessment of fairness is a legal one at its core and can only be carried out by a human being. Until now, there have been no technical means that allow a legal assessment of these complex questions [2].

Determining who will be in charge of assessing fairness or appointed as a DPO in the decentralized blockchain is challenging.

3) TRANSPARENCY
   a: CHALLENGE
   The controller must inform the data subject about collected data, users, purposes, periods, and rights transparently. A technical procedure for extracting the necessary information from the blockchain and providing it to the data subject in a timely and effective manner can be useful [2]. However, if the blockchain interoperates with external storage (cloud, IPFS), it may require an additional technical procedure.

   b: SOLUTIONS
   We found the following three types of solutions supporting the transparency principles.

   Several studies have proposed an architecture that ensures provenance tracking by a smart contract. In these architectures, all data activity is logged in the blockchain through a smart contract to ensure transparency [33], [42], [60], [67], [74], [75], [76], [89]. Using the smart contract log, the data subject can monitor who has processed the data, for what purposes, and when. Moreover, a data subject can check whether the activity complies with the GDPR. Log evidence can guarantee immutability, integrity, and nonrepudiation.

   In the environment where the blockchain interoperates with a cloud, a hooking method installed in the cloud collects all the action logs of the cloud. It generates provenance metadata from the logs and stores it in the blockchain in an encrypted form [44]. A data subject can monitor their compliance by accessing the provenance metadata. In another similar study [77], a monitoring agent in the cloud was used to collect provenance data. In this method, the agent extracts GDPR-related metrics from the provenance data and stores them in the blockchain. The monitoring agent is installed in a container; hence, it is compatible with any cloud platform.

   Table 6 and Fig. 4 summarize the solutions that support the transparency principle.

4) DATA MINIMIZATION, ACCURACY, AND STORAGE LIMITATION
   a: CHALLENGE
   A blockchain is incompatible with the data minimization, accuracy, and storage limitation principle due to its immutable nature. This is because these principles require the ability to delete data. However, incompatibility does not matter when immutability takes precedence over these principles (e.g., forensic) [25] because GDPR allows this situation by the exemption from deletion obligations (art. 17(3) GDPR); however, the exemption can only be applied in limited cases, for example, when blockchain is used for archiving for public interest. If not, blockchain can no longer be used for other purposes. Therefore, it should generally be able to provide data erasure capabilities.

   b: SOLUTIONS
   We found several articles addressing the mutability of the blockchain. We classified those articles into three types: bypassing immutability without modifying the design of the
blockchain, modifying the design of the blockchain, and amending the regulation.

One of the solutions that ensures the mutability of the blockchain is to store data as off-chain storage while storing only a hash value in the blockchain [5]. When the data stored in off-chain storage are deleted or modified, only the fact that a specific content version existed at a specific point in time is left in the blockchain. Many articles have adopted off-chain storage methods [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [60], [61], [62], [64], [71], [72], [73], [74], [75], [77], [80], [81], [82], [87], [88], [89]. However, the following are several serious problems associated with off-chain methods: 1) the goals of the blockchain may be ignored [27]; 2) complexity and additional delays in transferring on-chain data to off-chain storage may occur; 3) the security level of the blockchain reduces [47]; 4) this method makes the system inconsistent. Data synchronization is an ongoing process that synchronizes data between an off-chain layer and an on-chain layer and updates changes automatically to maintain consistency within the systems. The presence of program bugs in the synchronization process makes the system inconsistent [48]; and 5) As an off-chain database is combined with a blockchain system, the cost of the technology increases for the following reasons: First, the cost of deploying off-chain storage increased. Second, the complexity of the blockchain architecture could be increased as it combined with off-chain database, consequently it requires more cost of the technology to maintain it [54]. However, all solutions require compromises. Despite many challenges, off-chain could be an easy-to-build option until these hurdles are overcome or other technical alternatives become a viable option [54].

The other solution is irreversible encryption. In this method, stored data are encrypted in the blockchain, and the encryption key can be destroyed on user request [49] so that the data cannot be accessed anymore. However, it is uncertain that such a method will be compliant with the GDPR in the future [49]. Quantum computing could be a security risk that can compromise most cryptographic schemes in use today. DIN SPEC 4997 recommends the necessity of an “anonymity evaluation” when introducing cryptographic functions in the blockchain [2].

Another solution for mutability is blockchain pruning. In this method, old blocks are removed after a predefined period, and only the block header is kept in the blockchain [51]. Originally, pruning aimed to reduce the blockchain size, but consequently, it met the regulatory requirements of forgetting old transactions [51]. However, pruning may not comply with the GDPR because DIN SPEC 4997 recommends that data should be deleted upon the data subject’s request according to legal procedures.

We can delete data from the side-chain without changing the main chain [24]. A side-chain is a sub-chain connected to the main chain through a bridge. It is similar to an off-chain because it processes transactions delegated by the main chain. However, it is entirely different from an off-chain because it does not build a node for the side-chain itself and operates on the existing main chain.

A different way to delete blockchain data is to make the blockchain editable using a chameleon hash, a cryptographic hash function that includes a trapdoor. With knowledge of this trapdoor, we can efficiently create collisions. Knowing the key enables the deletion, modification, and insertion of blocks [51], [69]. However, if we abuse the chameleon hash, unauthorized changes to the blockchain may occur. Thus, strict change management procedures are necessary to prevent illegal modification, for example, allowing only a single trusted entity to delete data or applying a consensus mechanism to confirm the legitimacy of changes [25].

Another mutability method is the use of a truncated hash value to compute a block hash. Generally, we use a standard hash function, such as SHA-256, to create a block hash. We cannot modify or delete the transaction after the hash value has been created. To make the block mutable, we can create a block hash from the target value of the transaction, rather than from the transaction itself [52]. A target value can be created by truncating the appropriate number of leftmost bits of the hash value generated from a hash function with a larger message digest length. However, whether this technology is compliant with the GDPR remains unclear. Similar to a chameleon hash, malicious users or hackers could misuse it. Furthermore, no references recommend such a solution yet.

A consensus mechanism for the mutability of the blockchain has been studied. Generally, a consensus algorithm is used to decide in a distributed network without a central controller. Usually, it can verify a new block and add it to the current blockchain. Moreover, the consensus mechanism can be used for data deletion in the blockchain. We can also vote, and if the majority approves, then the data can be removed [53]. However, in this case, some problems may occur. Given that the old data in the blockchain are set into “blocks,” removing some would disrupt the block [53].

A different approach to mutability is to amend the GDPR to allow the following activities to operate as deletion methods [54]: 1) personal data are stored in the permissioned blockchain; 2) the data subject gives consent not to exercise their “right to be forgotten” and “right to data portability”; 3) moving to a new block; 4) a “fork” is created within the blockchain; 4) access rights are restricted so that only the data subject can access the data; and 5) personal data are hashed (i.e., hashed data are converted into anonymous data).

Table 7 and Fig. 5 summarize the solutions that support blockchain mutability.

5) CONFIDENTIALITY AND INTEGRITY

a: CHALLENGE

A controller must securely process personal data to guarantee confidentiality and integrity. They must know which data should not be disclosed to third parties and which appropriate technical measures are necessary. The requirements depend on the type of blockchain. Every user can access
TABLE 7. Solutions to the data minimization/Accuracy/Storage limitation principle.

| Article | Solution | Category |
|---------|----------|----------|
| [24], [31]–[47], [60]–[62], [64], [71]–[75], [77], [80]–[82], [87]–[89] | Sub-chain | Bypassing immutability |
| [45] | Off-chain | Irreversible encryption Pruning |
| [51] | Chameleon hash | Removing immutability |
| [52] | Truncated hash | Consensus |
| [53] | GDPR amendment | Regulation amendment |

b: SOLUTIONS

We discovered the following types of solutions for confidentiality and integrity.

Anonymization of data is a useful method to comply with the confidentiality and integrity principle. Data encryption is representative data anonymization skill. It encrypts transactions as an encryption algorithm to restrict unauthorized access [36], [57]. The DIN SPEC 4997 designated the encryption as a technical solution that complies with the GDPR [2]. Another way to encrypt data is the zero-knowledge proof (ZKP); thus, underlying data cannot be accessed, and only binary answers, such as true/false, are given [34]. However, the ZKP introduces an overhead, which could cause network latency. DIN SPEC 4997 recommends the ZKP as a technical solution that complies with the GDPR [2]. Meanwhile, local differential privacy anonymizes the data by adding some “noise” to the data. This allowed us to perform computations on anonymized data [56]. Moreover, the fully homomorphic encryption protocol allows mathematical operations to be performed on encrypted data [35], [58]. It is designated as a technical solution that complies with the GDPR by the DIN SPEC [2].

Another solution is access control mechanisms to restrict data access. Data access is regulated by a smart contract in which access policies are encoded. The access policy includes who can access data, when it can be accessed, and which data items can be accessed. Anyone who wants to access the data must invoke a smart contract. They can access the data if the access request satisfies the access policy; otherwise, the access will be rejected [32], [33], [42], [43], [45], [46], [60], [61], [62], [64], [67], [75], [79], [80], [81], [87], [90]. Access policies can be constructed in various ways. One way is attribute-based policy, which checks whether a user’s attribute satisfies the policy. One straightforward way is to compare the requested attribute to the stored attribute [68]. Meanwhile, another more complicated way is to allow only users with keys that satisfy the access policy to decrypt the ciphertext. In the former case, an immutable blockchain can be used as an attribute storage, and in the latter case, ABE is used, which is the method we focus on. In particular, CP-ABE has been studied for a long time as an access control method by many researchers [37], [38], [69], [70], [71], [72], [73]. However, the following are several shortages in the ABE scheme: computational overhead [16], [17], [18]; update issues on the access structure and attributes; and key escrow vulnerability. To overcome these shortcomings, prior studies have proposed improved ABE mechanisms. First, the decryption process can be distributed or outsourced to reduce the overhead [38], [73]. Second, update issues are solved by creating a new transaction that makes the World State Database up-to-date using the same blockchain address as used before [72]. Consequently, a user with an existing decryption key cannot decrypt data because of a mismatch with the new access structure. Similarly, user attributes can be revoked by updating the user attribute revocation list stored on the blockchain. Finally, the key generation center has a key escrow risk because it can generate the user’s secret key and decrypt ciphertext using its master key. The risk can be reduced by assigning the data subject node in the blockchain the role of key generation center (KGC) [37], [71].

In addition, various methodologies can be employed to comply with confidentiality and integrity. For instance, “Private data transaction” is a method where data are shared only with authorized peers in the hyperledger fabric [66]. In the scheme, the proposed transaction is transmitted only to a designated endorser and is propagated to the authorized peers through the gossip protocol. Other endorsers can only see the hash value of the data. Another approach to access control is to put a user request block on hold in the unprocessed request pool until the user’s key is verified. If the user’s key is confirmed to be valid, the block is approved through consensus [41].
Multichain is a blockchain model in which two types of blockchain are provided concurrently. It provides the advantages of permissionless and permissioned types. Permissionless blockchains, characterized by transparency, are used to store attributes, such as the hash value, encryption key, and log data. In contrast, permissioned blockchains, characterized by confidentiality, are used for storing data [69], [72]. Table 8 and Fig. 6 summarize solutions that support the confidentiality and integrity principle.

Table 8. Solutions to the confidentiality and integrity principle.

| Article | Solution | Category |
|---------|----------|----------|
| [34], [35], [55], [36], [57], [36], [58], [59] | ZKP Encryption Local differential privacy Homomorphic Encryption Quantum cryptography | Anonymization |
| [32], [33], [42], [43], [45], [46], [60]–[62], [64], [67], [73], [79]–[81], [87], [90], [37], [38], [69]–[73], [37], [38], [70]–[71], [73], [72], [68], [39] | Access control using smart contract Access control using ABE ABE with overhead reduction ABE embedded in consensus ABE with revocation/overhead reduction ABE with revocation Proof of attributes ACL | Access control |
| [41], [66], [69], [72] | Unprocessed request pool Private data transaction Multi-chain etc. |

FIGURE 6. Pie chart for the solutions to the confidentiality and integrity principle.

6) ACCOUNTABILITY

a: CHALLENGE

Identifying the controller in the blockchain is critical for demonstration of accountability. However, identifying the controller in a permissionless blockchain is challenging, as all nodes operate in a decentralized fashion [2], [25]. Thus, identifying a violation of the controller or demonstrating its compliance is difficult. If we cannot identify a controller, legal uncertainty and security risk increase. In contrast, we can easily identify a controller in a permissioned network because one can identify the entity that owns and makes decisions within the network [1]. Meanwhile, the actual owner of the controller must be traced, even if the controller is identified. However, blockchain addresses are pseudonymous, thus making tracking difficult. Therefore, a solution that tracks real data owners/users on the blockchain is needed.

b: SOLUTIONS

Table 9 summarizes the solutions that support the accountability principle.

Table 9. Solutions to the accountability principle.

| Article | Solution | Category |
|---------|----------|----------|
| [42], [74], [75], [67] | tracking controller by certificate tracking controller by IP address tracking controller by ID resolving | certificate IP ID |
| [89] | |

Table 10. Controllership in the blockchain.

| Article | Individual user | Miner | Data owner | Each node | Blockchain designer |
|---------|-----------------|-------|------------|-----------|---------------------|
| [1]     | o               | x     | o          | -         | -                   |
| [25]    |                 |       | -          | - o       | x                   |
| [24]    | o               | -     | o          | -         | -                   |

Table 10 shows the controller in the blockchain.

Controllers should be identified cautiously for the following reasons. Individual users, data owners, or each node are ordinary people in the real world. They cannot meet the obligations of a controller. Incorrectly assigning a controller may add risk when the data subjects’ personal data are misused [21].

V. ADDRESSING RQ2

In this section, we discuss the research gaps. The previous section presented solutions to resolve conflicts between the
TABLE 11. Research gaps in the prior literature.

| GDPR Principles                  | Topics of the prior literature                                                                 | Research gap                                                                 |
|----------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Lawfulness and Purpose limitation| consent management/consent ontology/access control/consent structure                          | consent ontology modeling                                                    |
| Fairness                         |                                                                                               | mechanism to monitor fairness                                               |
| Transparency                     | smart contract logging/server-side logging/client-side logging                                 | Resolving the contradiction between auditing and obfuscation                 |
| Data minimization/               | off-chain/ chameleon hash/truncated hash/pruning/ irreversible encryption/ side-chain/ consensus|                                                                               |
| Accuracy/                        |                                                                                               |                                                                               |
| Storage limitation               | access control/data anonymization                                                              |                                                                               |
| Confidentiality and              | who is the controller in the blockchain? / how can track controller identification?             | The controller tracking method                                               |
| Integrity                        |                                                                                               | Integration of the different-purposed technical solutions without conflicts   |
| Accountability                   |                                                                                               |                                                                               |
| All the principles               |                                                                                               |                                                                               |

GDPR and the blockchain. After carefully analyzing the articles considered for research and querying the GDPR ontology, we propose some research gaps that can be explored in the future.

First, we found 24 articles on the lawfulness and purpose limitation principles. They propose consent management and access control frameworks that comply with the GDPR principles. Eight articles proposed a consent ontology model briefly [31], [33], [61], [75], [80], [81], [82], [87]. The proposal aimed to support efficient decision-making on whether data processing behavior is lawful in a blockchain. Access to data may be permitted or denied, depending on the decision made by the ontology. However, their ontology model is not specific in how policy is configured, evaluated, and determined. Consent ontology modeling could be a good research direction in the future.

Second, we could not find any articles on fairness principles. So far, fairness has been the area that a person (or organization) can assess. However, fairness must be assessed using different methods in the blockchain. This is also a good research topic in the future.

Third, we found 11 articles on the transparency principle. The authors of these articles logged data access activities in the blockchain to allow provenance tracking and inspection. A smart contract in the blockchain recorded all data activity. Some articles have proposed that log data should be obfuscated so as not to reveal personal data. However, log data cannot be audited when they are obfuscated. We could not find any research articles on the paradox between obfuscation and audibility. Therefore, resolving this problem is a good research topic for the future.

Forth, we found eight articles relevant to the accountability principle. An individual user or a node qualifies as a controller and therefore is liable under the GDPR. However, nodes are distributed worldwide in the permissionless blockchain. As mentioned, finding the number, locations and identity of nodes is difficult. IP address, certificate, and application ID associated with blockchain address are not complete solutions to track identity. Hence, the blockchain controller tracking method is a useful research topic for the future.

Finally, in light of the requirements introduced by the GDPR, a significant concern is the interoperability of the different-purposed security mechanisms without conflicts. For example, the confidentiality achieved via encryption could conflict with the transparency principle mentioned above and with data minimization, accuracy, storage limitation principle, or unexpected principles. The most important work to be done in the future is to solve the interference that may arise from different-purposed solutions operating simultaneously in the framework for the GDPR compliance. The work should be performed at the beginning of blockchain design, following privacy-by-design principles (art.25 GDPR). That could be a useful research topic for the future.

Table 11 summarizes the research gaps identified concerning RQ2.

VI. DISCUSSION

We reviewed 91 previously published articles on blockchain compliance. A total of 36 articles discussed the confidentiality and integrity of blockchain, followed by data minimization/accuracy/storage limitation (42), lawfulness and purpose limitation (24), transparency (11), and accountability (8). Meanwhile, no articles have discussed fairness. Table 12 shows the GDPR principles and the number of corresponding articles.

However, the findings of the first research question, described in Section IV-B, have several issues. First, most of the studies focused on the principle of confidentiality and integrity and the principle of data minimization, accuracy, or storage limitation. Research articles on the principles of lawfulness, fairness, transparency, and accountability are scant. Therefore, the issues on the principles of lawfulness,
fairness, transparency, and accountability were not discussed sufficiently in this review.

Second, the proposed frameworks or solutions of those research satisfy most requirements to comply with the GDPR, except for some studies (the research gaps for some studies are discussed in the previous section). However, only a few articles proved the feasibility of the proposed solution or framework. Some of the papers proved the feasibility of the proposed system only theoretically. Moreover, the algorithm of the proposed system was not sufficiently investigated [32], [34], [35], [41], [55], [62], [63], [67], [68], [70], [71], and the performance was not analyzed through pilot construction [32], [35], [44], [55], [74], [75], [81], [87]. Therefore, we cannot be sure that their solution is feasible, except for some.

Third, when classifying previous articles according to blockchain type, we identified 25 articles and 20 cases on permissionless and permissioned blockchains, respectively. Table 13 shows the blockchain types discussed in the prior literature. We observed that permissionless blockchains, which are more vulnerable to privacy, have been studied more than permissioned blockchains. However, the advantages of decentralization decreased when building governance for privacy on a permissionless blockchain. The reason is as follows: The proposed technical measures or solutions could increase the blockchain’s centrality, and ironically, can threaten the security of the blockchain in the long run. For example, smart contract-based consent and off-chain solutions could increase the software centrality of the blockchain, consequently introducing bugs and contract code reuse issues [99]. Furthermore, the technical measures can sometimes increase the risk that the blockchain could be controlled by a small number of nodes. For example, for data confidentiality, the consensus mechanism proposed by [70] only allows nodes that meet the access policy as miners, and in [34], only a specific group of nodes called a block committee is allowed to approve new blocks. Here consensus work is delegated to a small number of nodes running self-developed software, which result in consensus centrality [99]. The consensus centrality consequently increases the authoritative centrality, which reduces the number of entities required to disrupt the system, and the blockchain’s security level [99]. However, the issues of the trade-off between decentralization and privacy were not discussed sufficiently in this review.

Finally, in this review, articles were identified through database searching, but the search strategy has some limitations. The keywords used were restricted to “blockchain” and “GDPR,” and only the title, abstract, and keywords were searched. Therefore, search strategy should be improved in further studies.

### VII. CONTRIBUTIONS

Through this SLR, we made theoretical contributions: First, we have contributed to the literature by presenting the overall challenges, solutions, and research gap for integrating blockchain and the GDPR. Our findings expand and advance the limits of the literature in the current situation wherein the literature review addressing the overall progress and technical measures for the compatibility of blockchain and GDPR is very scarce, and even related standardization is insufficient. We classified each solution proposed by 91 previous studies by 6 privacy principles and 15 application types, which helps manage solutions as principle groups and application types, and manage relationships among the groups. This helps identify the lack of solutions, assess the vulnerability of a specific type of application, minimize interference between collective solutions, and improve interoperability. This result is significant because it can help scholars study the compatibility between blockchain and the GDPR.

Second, this study contributed to suggesting a research direction for future study. The currently proposed solutions alone cannot achieve the goals of a particular group of principles. For example, the accountability principle group aims to link the pseudonymous world of blockchain with the real world of law through technical solutions; however, many barriers must be overcome, such as interoperability with real-world authentication, to interoperate the actual legal system through the proposed data logging and tracking solution. In addition, in the lawfulness and purpose limitation principles group, a consent ontology enables self-regulation of decentralized blockchain, but many challenges remain. Meanwhile, there is no solution in the fairness principles group to determine the fairness of blockchain data processing.

Another significant problem is that the goals and functions of one principle group might conflict with those of another group. For example, obfuscation of log data by the confidentiality principle may compromise readability and thus, conflict with the transparency principle. These challenges could broaden the scope of the blockchain compliance topic. Our SLR presents a meaningful, new research direction for integrating blockchain and the GDPR.
The practical implication of this study is as follows. Our result can help resolve uncertainties in the EU’s GDPR-compliant blockchain policy by grouping and interpreting the solutions from the perspective of the GDPR framework. According to the European Parliament Research Service, EU regulators have concerns about attempts to map the regulation to blockchain technologies because of uncertainty due to incompatibilities between blockchain and the GDPR. For example, it is unclear whether “erasure” in the common-sense understanding of the word is required or whether alternative technical approaches with a similar outcome may be sufficient [98]. However, the EU regulators promote blockchain policies to resolve the uncertainty caused by incompatibility, e.g., by providing specific guidance rather than the revision of the GDPR. From the GDPR principles perspective, we identified the gap between blockchain and the GDPR, presented the solutions that could fill the gap, and evaluated the solution’s potential risks. We raised the legal problems to the alternative solutions, such as “pruning” of the principle group of data minimization/accuracy/storage limits. We also raised administrative issues regarding the abuse of “chameleon hash” and “target value hash” and difficulties of law application related to controllership and ID tracking solutions of the accountability principle group. This result is significant as it can help the EU regulators understand the gap and the solutions from a legal perspective and clarify the legal requirements for specific concepts. Consequently, the resolution of uncertainty in blockchain policy can give considerable certainty to blockchain stakeholders who have struggled to design or monitoring a blockchain due to a lack of legal certainty.

VIII. CONCLUSION AND FUTURE WORK
Our research aimed to synthesize information from previously published literature on GDPR-compliant blockchains. We collected 91 articles from 32 major publishers and conducted a systematic review. We analyzed the current status, classified the challenges and solutions and found the following research gaps: 1) development of a consent ontology model; 2) development of a methodology for monitoring fairness in the blockchain; 3) resolution of the contradiction between auditing and obfuscation; 4) development of a methodology for tracking controllers in the blockchain; and 5) integration of the different-purposed technical solutions without conflicts.

However, our SLR has several technical limitations. Although we made an effort to remove bias, our search strategy has technical limitations and room for improvement. We use keywords derived from only “research topics,” searching only for titles, keywords, and abstracts, and we limited search databases to major publishers. Thus, it may result in missing crucial previous research or cause a slight bias in the results. Furthermore, the ability to assess the confidence of the evidence of outcome is technically limited. We verified the certainty of the following outcome through a self-developed GDPR ontology model: 1) whether the searched study meets the inclusion criteria; 2) the outcome for the second research question, i.e., the research gap; however, our GDPR ontology model has a limitation. Because it consists of GDPR legal terms, it may not be suitable for papers that do not use precise legal terms. Furthermore, solutions or technical measures mapped to GDPR principles in an ontology may be limited due to the limitations of the referenced materials. Thus, it may limit the quality of verification of the output.

We propose the following future study to overcome the technical limitations mentioned above. It is necessary to upgrade the process of data search, classification, and verification. Research relevant to the topic should be extracted and classified without bias and restrictions. Supervised machine learning is an advantageous technique for conducting these tasks; it can improve the outcome quality because it uses a word dictionary instead of search keywords and artificial neural network technology. Certainly, the accuracy of the machine learning algorithm must be guaranteed.

Meanwhile, it is necessary to research personal information protection laws other than the GDPR. This study examined the compatibility of the GDPR and blockchain. We selected the GDPR as the representative privacy law that affects the world; however, it is essential to study other personal information protection laws in the high-tech digital age, where cross-border transfers of personal data occur frequently. It would be a good research topic to study other personal information protection law and compare it with the GDPR in terms of compatibility with blockchain. We can gradually fill the gap between the blockchain and the regulations with such research.

REFERENCES
[1] M. Lucie and K. Ashley, “Blockchain and the general data protection regulation: Reconciling protection and innovation,” J. Securities Oper. Custody, vol. 11, no. 2, pp. 145–157, 2019.
[2] S. Schwalm. DIN SPEC 4997, Privacy by Blockchain Design: A Standardised Model for Processing Personal Data Using Blockchain Technology. Accessed: Jan. 1, 2022. [Online]. Available: https://www.researchgate.net/publication/340225011
[3] L. König, Y. Korobeinikova, S. Tjoa, and P. Kieseberg, “Comparing blockchain standards and recommendations,” Future Internet, vol. 12, no. 12, p. 222, Dec. 2020, doi: 10.3390/fi12120222.
[4] W. Hon, J. Palfreyman, and M. Tegart. Distributed Ledger Technology & Cybersecurity (Improving Information Security in the Financial Sector). Accessed: Jan. 1, 2022 [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security
[5] CNIL. Solutions for a Responsible Use of the Blockchain in the Context of Personal Data. Accessed: Jan. 1, 2022. [Online]. Available: https://www.cnil.fr/sites/default/files/atoms/files/solutionsBlockchain_en.pdf
[6] A. B. Haque, A. K. M. N. Islam, S. Hyrynsalmi, B. Naqvi, and K. Smolander, “GDPR compliant blockchains—A systematic literature review,” IEEE Access, vol. 9, pp. 50593–50606, 2021, doi: 10.1109/ACCESS.2021.3069877.
[7] F. Fatehi, F. Hassandoust, R. K. L. Ko, and S. Akhlaghpour, “General data protection regulation (GDPR) in healthcare: Hot topics and research fronts,” in Studies in Health Technology and Informatics, vol. 270. Amsterdam, The Netherlands: IOS Press, 2020, pp. 1118–1122.
[8] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, “Privacy enhancing technologies in the Internet of Things: Perspectives and challenges,” IEEE Internet Things J., vol. 6, no. 2, pp. 2159–2187, Apr. 2019, doi: 10.1109/JIOT.2018.2878658.
[9] J. B. Bernet, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, “Privacy-preserving solutions for blockchain: Review and challenges,” *IEEE Access*, vol. 7, pp. 164908–164940, 2019, doi: 10.1109/ACCESS.2019.2950872.

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

[11] V. Gramoli, “From blockchain consensus back to byzantine consensus,” *Future Gener. Comput. Syst.*, vol. 107, pp. 760–769, Jun. 2020, doi: 10.1016/j.future.2017.09.023.

[12] European parliament and of the council, “Regulation (EU) 2016/679 of the European parliament and of the council,” Off. J. Eur. Union, vol. 679, p. 2016, Apr. 2016.

[13] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Advances in Cryptology—EUROCRYPT 2005* (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed., Berlin, Germany: Springer, 2005, doi: 10.1007/11426399-27.

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

[15] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in *Proc. IEEE Symp. Secure Privacy (SP)*, Berkeley, CA, USA, May 2007, pp. 20–23.

[16] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A ciphertext-policy attribute-based encryption scheme with constant ciphertext length,” in *Proc. 5th Int. Conf. Inf. Secur. Pract. Prog.*, Xi’an, China, vol. 5451, Apr. 2009, pp. 13–23.

[17] J. Herranz, F. Laguillaumie, and C. Ràfols, “Constant size ciphertexts in threshold attribute-based encryption,” in *Public Key Cryptography—PKC 2010* (Lecture Notes in Computer Science), vol. 6056, P. Nguyen and D. Pointcheval, Eds., Berlin, Germany: Springer, 2010, doi: 10.1007/978-3-642-13013-7_2.

[18] L. Bisne and M. Parmar, “Composite secure MQTT for Internet of Things using ABE and dynamic S-box AES,” in *Proc. Innov. Power Adv. Comput. Technol. (i-PACT)*, Vellore, India, Apr. 2017, pp. 1–22.

[19] C. Millard, “Blockchain and law: Incompatible codes?” *Comput. Law Secur. Rev.*, vol. 34, no. 4, pp. 843–846, Aug. 2018, doi: 10.1016/j.clsr.2018.06.006.

[20] G. P. Freund, P. B. Fagundes, and D. D. J. De Macedo, “An analysis of blockchain and GDPR under the data lifecycle perspective,” *Mobile Netw. Appl.*, vol. 26, no. 1, pp. 206–216, Feb. 2021, doi: 10.1007/s11036-020-01646-9.

[21] R. Teperdjian, “The puzzle of squaring blockchain with the general data protection regulation,” in *Proc. 9th Int. Multi-Conference Complex., Informat. Cybern.*, Vellore, India, Apr. 2017, pp. 1–22.

[22] J. Investment Compliance, vol. 3, no. 3, pp. 310–322, 2020.

[23] D. E. Majdoubi, H. El Bakkali, and S. Sadki, “Towards smart blockchain-based system for privacy and security in a smart city environment,” in *Proc. 5th Int. Conf. Cloud Comput. Artif. Intell., Technol. Appl. (CloudTech)*, Marrakesh, Morocco, Nov. 2020, p. 44203, doi: 10.1109/CloudTech49835.2020.9365905.

[24] N. Al-Zaben, M. M. H. Onik, J. Yang, N. Lee, and C. Kim, “General data protection regulation complied blockchain architecture for personally identifiable information management,” in *Proc. Int. Conf. Comput., Electron. Commun. Eng. (iCCCEC)*, Southend, U.K., 2018, pp. 77–82, doi: 10.1109/iCCCEC.2018.8658586.

[25] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” *Information*, vol. 8, no. 2, p. 44, 2017, doi: 10.3923/info.200404.

[26] D. E. Majdoubi, H. El Bakkali, and S. Sadki, “Towards smart blockchain-based system for privacy and security in a smart city environment,” in *Proc. 5th Int. Conf. Cloud Comput. Artif. Intell., Technol. Appl. (CloudTech)*, Marrakesh, Morocco, Nov. 2020, p. 44203, doi: 10.1109/CloudTech49835.2020.9365905.

[27] N. Al-Zaben, M. M. H. Onik, J. Yang, N. Lee, and C. Kim, “General data protection regulation complied blockchain architecture for personally identifiable information management,” in *Proc. Int. Conf. Comput., Electron. Commun. Eng. (iCCCEC)*, Southend, U.K., 2018, pp. 77–82, doi: 10.1109/iCCCEC.2018.8658586.

[28] Q. Xia, E. B. Sifah, K. O. Assamoah, J. Gao, X. Du, and M. Guizani, “MedShare: Trust-less medical data sharing among cloud service providers via blockchain,” *IEEE Access*, vol. 5, pp. 14757–14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[29] I. Camilo, “Blockchain-based consent manager for GDPR compliance,” *Open Identity Summit*, vol. 2019, pp. 28–29, Mar. 2019.

[30] K. Miyachi and T. K. Mackey, “HOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design,” *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102535, doi: 10.1016/j.ipm.2021.102535.

[31] W. Zhang, L. Wei, S. Li, Y. Liu, and S.-C. Cheung, “DArcher: Detecting on-chain-off-chain synchronization bugs in decentralized applications, 2021, arXiv:2106.08440.
[49] D. Hofman, V. Louise Lemieux, A. Joo, and D. A. Batista, “The margin between the edge of the world and infinite possibility: Blockchain, GDPR and information governance,” Records Manage. J., vol. 29, no. 4, pp. 240–257, 2019, doi: 10.1108/RMJ-12-2018-0045.

[50] P. Hristova and W. Dimitrov, “The blockchain as a backbone of GDPR compliant frameworks,” in Proc. 8th Int. Multi-Disciplinary Symp. Challenges Opportunities Sustain. Develop. Through Quality Innov. Eng. Res. Manage. Petrosani, Romania: Univ. Petrosani, Oct. 2018, vol. 20, no. 1, pp. 305–310.

[51] E. Politou, F. Casino, E. Alepis, and C. Patsakis, “Blockchain mutability: Chal-lenges and proposed solutions,” IEEE Trans. Emerg. Topics Comput., vol. 9, no. 4, pp. 1972–1986, Oct. 2021, doi: 10.1109/TETC.2019.2949510.

[52] N.-Y. Lee, J. Yang, M. M. H. Onik, and C.-S. Kim, “Modifiable public blockchains using truncated hashing and sidechains,” IEEE Access, vol. 7, pp. 173571–173582, 2019, doi: 10.1109/ACCESS.2019.2956628.

[53] E. Kadena and P. Holica, “Security issues in the Blockchain(ed) world,” in Proc. IEEE 18th Int. Symp. Comput. Intell. Informat. (CINTI), Budapest, Hungary, Nov. 2018, pp. 211–215, doi: 10.1109/CINTI.2018.8928212.

[54] A. Mirchandani, “The GDPR-blockchain paradox: Exempting permissioned blockchains from the GDPR,” Fordham Intellectual Property, Media Education Law J., vol. 29, no. 4, pp. 1201–1242, 2019.

[55] I. Holzelzin, K. Bergstam, B. Cjea, and A. Veseih, “Electricity trading via blockchain in an energy community from a data protection point of view,” Energ. Energy Clim. J., vol. 10, pp. 31–41, Sep. 2020.

[56] N. Fotiou, I. Pittaras, V. A. Siris, G. C. Polyzos, and P. Anton, “A privacy-preserving statistics marketplace using local differential privacy and blockchain: An application to smart-grid measurements sharing,” Blockchain: Res. Appl., vol. 2, no. 1, Mar. 2021, Art. no. 100022, doi: 10.1016/j.hcrb.2021.100022.

[57] C. Rui, “Protection and control of personal identifiable information: The PoSeID-on approach,” J. Data Protection Privacy, vol. 3, no. 2, pp. 199–228, 2020.

[58] H. Karim and D. B. Rawat, “TollsOnly please—Homomorphic encryption access control scheme using blockchain for IoT,” J. Brit. Blockchain Assoc., vol. 9, no. 4, pp. 1972–1986, Oct. 2021, doi: 10.1109/JBB-3-2-(5)2020.

[59] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, “Secure service delivery,” in Proc. IEEE 18th Int. Symp. Comput. Intell. Informat. (CINTI), Budapest, Hungary, Nov. 2018, pp. 211–215, doi: 10.1109/CINTI.2018.8928212.

[60] K. Rantos, G. Drosatos, A. Kritsas, C. Ilioudis, A. Papanikolaou, and M. Abomohara, “GDPR compliant consent driven data protection in IoT ecosystems,” J. Brit. Blockchain Assoc., vol. 9, no. 4, pp. 1972–1986, Oct. 2021, doi: 10.1109/JBB-3-2-(5)2020.

[61] J. Ahmed, S. Yildirim, M. Nowostaki, R. Ramachandra, O. Elezaj, and M. Abomohara, “GDPR compliant consent driven data protection in online social networks: A blockchain-based approach,” in Proc. 3rd Int. Conf. Inf. Conf. Technol. (ICICT), San Jose, CA, USA, Mar. 2020, pp. 307–312, doi: 10.1109/ICICT50521.2020.00054.

[62] M. Barati, I. Petri, and O. F. Rana, “Developing GDPR compliant user data policies for Internet of Things,” in Proc. 12th IEEE Int. Conf. Utility Cloud Comput., Auckland, New Zealand, Dec. 2019, pp. 133–141, doi: 10.1109/UCC48827.

[63] A. Mahindrakar and K. P. Joshi, “Automating GDPR compliance using integrated blockchain,” in Proc. IEEE 6th Int Conf. Big Data Secur. (BigDataSec) Int Conf. High Perform. Smart Comput., (HPSC) IEEE Int Conf. Intell. Data Secur. (IDS), Baltimore, MD, USA, May 2020, pp. 86–93, doi: 10.1109/BigDataSec549724.2020.00026.

[64] K. Rantos, G. Drosatos, C. Ilioudis, and A. Papanikolaou, “Blockchain-based consents management for personal data processing in the IoT ecosystem,” in Proc. 15th Int. Joint Conf. e-Bus. Telecommun., Porto, Portugal, Jul. 2018, pp. 572–577.

[65] K. Demertzis, K. Rantos, and G. Drosatos, “A dynamic intelligent policy for personal data processing in the IoT ecosystem,” in Proc. IEEE 6th Int Conf. Big Data Secur. Cloud (BigDataSecurity) Int Conf. High Perform. Smart Comput., (HPSC) IEEE Int Conf. Intell. Data Secur. (IDS), Baltimore, MD, USA, May 2020, pp. 86–93, doi: 10.1109/BigDataSec549724.2020.00026.

[66] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, “A novel attribute-based access control scheme using blockchain for IoT,” IEEE Access, vol. 7, pp. 38431–38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[67] J. Lim, J. Chun, G. Noh, and J. Jeong, “GDPR compliant blockchain based access control (OCBAC),” J. Korea Inst. Inf. Secur. Cryptol., vol. 30, no. 6, pp. 981–997, 2020, doi: 10.3745/KIICS.2020.30.6.981.

[68] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, “Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption,” in Proc. IEEE Int. Conf. Adv. Netw. Telecom. Syst. (ANTS), Bhubaneswar, India, Dec. 2017, p. 44567, doi: 10.1109/ANTS.2017.8384164.

[69] S. Y. A. Zaidi, M. A. Shah, H. A. Khattak, C. Maple, H. T. Rauf, A. M. El-Sherbeny, and M. A. El-Melegy, “An attribute-based access control for IoT using blockchain and smart contracts,” Sustainabil., vol. 13, no. 19, pp. 10556, Sep. 2021, doi: 10.3390/su131910556.

[70] S. M. Pournaghi, M. Bayat, and Y. Farjami, “MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption,” J. Ambient Intell. Humanized Comput., vol. 11, pp. 4613–4641, Jan. 2020, doi: 10.1007/s12652-020-01710-9.

[71] K. Yu, L. Tan, M. Aloiqaily, H. Yang, and Y. Jararweh, “Blockchain-enhanced data sharing with traceable and direct revocation in IoT,” IEEE Trans. Ind. Informat., vol. 17, no. 11, pp. 7669–7678, Nov. 2021, doi: 10.1109/TII.2021.3010152.

[72] M. Barati, G. S. Aujla, J. T. Llanos, K. A. Duodo, O. F. Rana, M. Carr, and R. Ranjan, “Privacy-aware cloud auditing for GDPR compliance verification in online healthcare,” IEEE Trans. Ind. Informat., vol. 18, no. 7, pp. 4808–4819, Jul. 2021, doi: 10.1109/TII.2021.310152.

[73] M. Barati, I. Petri, and O. F. Rana, “GDPR compliant user data policies for Internet of Things,” in Proc. 12th IEEE Int. Conf. Utility Cloud Comput., Auckland, New Zealand, Dec. 2019, pp. 133–141.

[74] A. Mahindrakar and K. P. Joshi, “Automating GDPR compliance using policy integrated blockchain,” in Proc. IEEE 6th Int Conf. Big Data Secur. Cloud (BigDataSecurity) Int Conf. High Perform. Smart Comput., (HPSC) IEEE Int Conf. Intell. Data Secur. (IDS), Baltimore, MD, USA, May 2020, pp. 86–93, doi: 10.1109/BigDataSec549724.2020.00026.
K. Rantos, D. George, K. Demertzis, I. Christos, P. Alexandros, and A. Kritsas, “AdvoCATE: A Consent management platform for personal data processing in the IoT using blockchain technology,” in Proc. Int. Conf. Secur. Inf. Technol. Commun., Bucharest, Romania, Nov. 2018, pp. 300–313.

N. Kaaniche, M. Laurent, and C. Levallois-Barth, “ID-based user-centric data usage auditing scheme for distributed environments,” Frontiers Blockchain, vol. 3, p. 17, Apr. 2020, doi: 10.3389/fbloc.2020.00017.

A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” in Proc. 2nd Int. Conf. Open Big Data (OBD), Vienna, Austria, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

M. Barati and O. Rana, “Enhancing user privacy in IoT: Integration of GDPR and blockchain,” in Blockchain and Trustworthy Systems (Communications in Computer and Information Science), vol. 1156, Z. Zhong, H. N. Dai, M. Tang, and X. Chen, Eds. Singapore: Springer, 2019, doi: 10.1007/978-981-15-2777-7_26.

K. Awuson-Davidia, T. Al-Hadhramib, M. Alazabc, N. Shaha, and A. Shalaginov, “BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem,” Future Gener. Comput. Syst., vol. 122, p. 44574, Sep. 2021, doi: 10.1016/j.future.2021.03.001.

M. Conti, E. S. Kumar, C. Lal, and S. Rui, “A survey on security and privacy issues of bitcoin,” IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018, doi: 10.1109/COMST.2018.2842460.

N. Nawari and R. Shiraam, “Blockchain technology and BIM process: Review and potential applications,” J. Inf. Technol. Construct., vol. 24, pp. 209–238, May 2019.

A. Anjum, M. Sporny, and A. Sill, “Blockchain standards for compliance and trust,” IEEE Cloud Comput., vol. 4, no. 4, pp. 84–90, Jul./Aug. 2017, doi: 10.1109/MCC.2017.3791019.

H. D. Zabadi, Y.-W. Chong, K. Ko, S. M. Hanshi, and S. Karuppayah, “A review on the role of blockchain technology in the healthcare domain,” Electronics, vol. 8, no. 6, p. 679, Jun. 2019, doi: 10.3390/electronics8060679.

J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A survey of blockchain technology applied to smart cities: Research issues and challenges,” IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2899617.

S. Singh, A. S. M. S. Hosen, and B. Yoon, “Blockchain security attacks, challenges, and solutions for the future distributed IoT network,” IEEE Access, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

The European Parliament Research Service (EPRS). Blockchain and the General Data Protection Regulation—Can Distributed Ledgers be Squared With European Data Protection Law? Accessed: Apr. 30, 2022. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445(ANN1)_EN.pdf

SEJIN HAN received the B.S. and M.S. degrees in computer science and engineering from Sogang University, in 1998 and 2001, respectively, where she is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering. From 2001 to 2011, she worked as a Senior Network Security Engineer with Korea Telecom (KT). She has been working as a Fintech Supervisor with Financial Supervisory Service, South Korea, since 2011. She is also working as a Senior Manager with Financial Supervisory Service. Her research interests include Fintech, blockchain, and information security.

SOOYONG PARK received the B.S. degree in computer science and engineering from Sogang University, in 1986, the M.S. degree from Florida States University, and the Ph.D. degree in information technology from George Mason University. He is currently a Professor with the Department of Computer Science and Engineering, Sogang University. His research interests include blockchain, requirement engineering, and Fintech.