applied sciences

MDPI

Article

Delegation-Based Personal Data Processing Request Notarization Framework for GDPR Based on Private Blockchain

Sung-Soo Jung [1], Sang-Joon Lee [2] and Ieck-Chae Euom [2,*]

[1] Research Center, DISEC, Daegu 41069, Korea; jssdisec@gmail.com
[2] System Security Research Center, Chonnam National University, Gwangju 61186, Korea; s-lee@jnu.ac.kr
* Correspondence: iceuom@jnu.ac.kr

Abstract: With the growing awareness regarding the importance of personal data protection, many countries have established laws and regulations to ensure data privacy and are supervising managements to comply with them. Although various studies have suggested compliance methods of the general data protection regulation (GDPR) for personal data, no method exists that can ensure the reliability and integrity of the personal data processing request records of a data subject to enable its utilization as a GDPR compliance audit proof for an auditor. In this paper, we propose a delegation-based personal data processing request notarization framework for GDPR using a private blockchain. The proposed notarization framework allows the data subject to delegate requests to process of personal data; the framework makes the requests to the data controller, which performs the processing. The generated data processing request and processing result data are stored in the blockchain ledger and notarized via a trusted institution of the blockchain network. The Hypderledger Fabric implementation of the framework demonstrates the fulfillment of system requirements and feasibility of implementing a GDPR compliance audit for the processing of personal data. The analysis results with comparisons among the related works indicate that the proposed framework provides better reliability and feasibility for the GDPR audit of personal data processing request than extant methods.

Keywords: GDPR; personal data; delegation; notarization; blockchain; non-repudiation

check for updates

Citation: Jung, S.-S.; Lee, S.-J.; Euom, I.-C. Delegation-Based Personal Data Processing Request Notarization Framework for GDPR Based on Private Blockchain. *Appl. Sci.* **2021**, *11*, 10574. https://doi.org/10.3390/app112210574

Academic Editors: Gianluca Lax and Antonia Russo

Received: 23 September 2021
Accepted: 8 November 2021
Published: 10 November 2021

1. Introduction

Information and communication technologies can potentially create high added value in various fields owing to the use of big data. In such applications of big data, various personal data are being collected, stored, analyzed, and utilized [1–5]. These collected personal data can be used for personalized marketing and consumption trend analysis and are recognized as a new type of highly valuable asset to service providers [6,7]. However, the importance of guaranteeing privacy and protecting collected personal data is being emphasized, as accidents involving the illegal collection, illegal distribution, and leakage of personal data by the service provider have become frequent, and related damage has increased [8].

In addition, owing to the development of the Internet and distributed storage technology, personal data that are not deleted over time have been identified as a new risk factor that can lead to serious invasion of privacy. Consequently, the importance of the right to request the processing of stored personal data of each data subject, such as the right to be forgotten, is also being focused upon [9]. Moreover, with the growing awareness of privacy, many countries are refining laws and regulations on personal data protection [10–13]. The general data protection regulation (GDPR), which came into effect in May 2018, focuses on strengthening the rights of data subjects and corporate accountability, and clarifying requirements for transfer of personal data outside the EU [8,14]. Under the implementation of the GDPR, other than member states of the EU, which are required to present implementations that meet the requirements of the GDPR, countries that desire to be incorporated into the EU and many other countries are amending or replacing existing laws to reflect certain aspects of the GDPR [8,14]. To protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, the GDPR sets out items on the protection and safe processing of collected data that controllers and processors must observe. In addition, it stipulates data processing policy according to the right to request processing of the private data of the data subject, and it ensures that member countries are obligated to manage and supervise compliance while stipulating that a strong administrative measure is imposed in case of violation [15,16].

However, since data subjects are guaranteed the right to request the processing of their personal data, which is stipulated in Articles 12 to 23 of Chapter 3, "Data Subjects' Rights," GDPR is a challenge. A personal data processing request is not an act entrusted to the service provider in the personal data processing consent that the data subject voluntarily proceeds before subscribing to the service to use the service provider's service. However, the records of requests such as the modification, deletion, and transfer of the data subject are managed by the service provider and used for GDPR compliance audits. Consequently, there is a risk of the service provider damaging, contaminating, or not creating the records for their own benefit. Therefore, the integrity and objective reliability of the data subject's request records managed by the service provider are not guaranteed. However, despite these problems, at present, the supervisory authority is obligated to rely on the evidence presented by the service provider for the GDPR compliance audit of service providers [17]. For example, if the data subject filed a legal lawsuit because the service provider did not faithfully comply with the regulations even though the data subject requested the service provider to delete its data under the right to be forgotten as stipulated in Article 17 of the GDPR, service providers may delete or corrupt the data subject's request record. A proposed countermeasure to this situation is a method wherein the data subject obtains a record of the requests for the processing of personal data and responses exchanged with the service provider from an external organization such as an email service provider, which are then notarized through a trusted notary organization. However, implementing this method is a challenge for any individual data subject owing to its complexity, cost, and cumbersome nature.

Thus far, several studies have researched systems and methods for safe and reliable GDPR management or audit. As analysis of that integrity and reliability of evidence data cannot be guaranteed through an existing centralized system method; certain studies focused on blockchain (BC) as a personal data storage, management, and GDPR [17–22]. However, to date, no realistic and reliable method to protect the data subject's right to request for the processing of personal data has been proposed [6,23,24]. Most of the previous systems and methods have proposed schemes to share personal data or to manage records of the processing of personal data from the perspective of service providers; this cannot guarantee the integrity and reliability of the data subject's request records necessary for the GDPR compliance audit. Data processing requests and their corresponding responses should exhibit an agreement between the data subject and service provider to ensure objectivity on credibility. The method that involves the management of data only from the perspective of the service provider cannot secure an objective view on credibility, while the method of storing all records of accessing or processing the data in a BC conflicts with GDPR regulations such as the right to be forgotten. Consequently, if further personal data are stored, the privacy problem associated with BC reproduces itself further [22–26].

This paper proposes a delegation-based personal data processing notarization framework for GDPR based on private BC technology. Figure 1 shows the conceptual configuration of the distributed storage and notarization of personal data processing request transactions using a BC-based notarization framework.

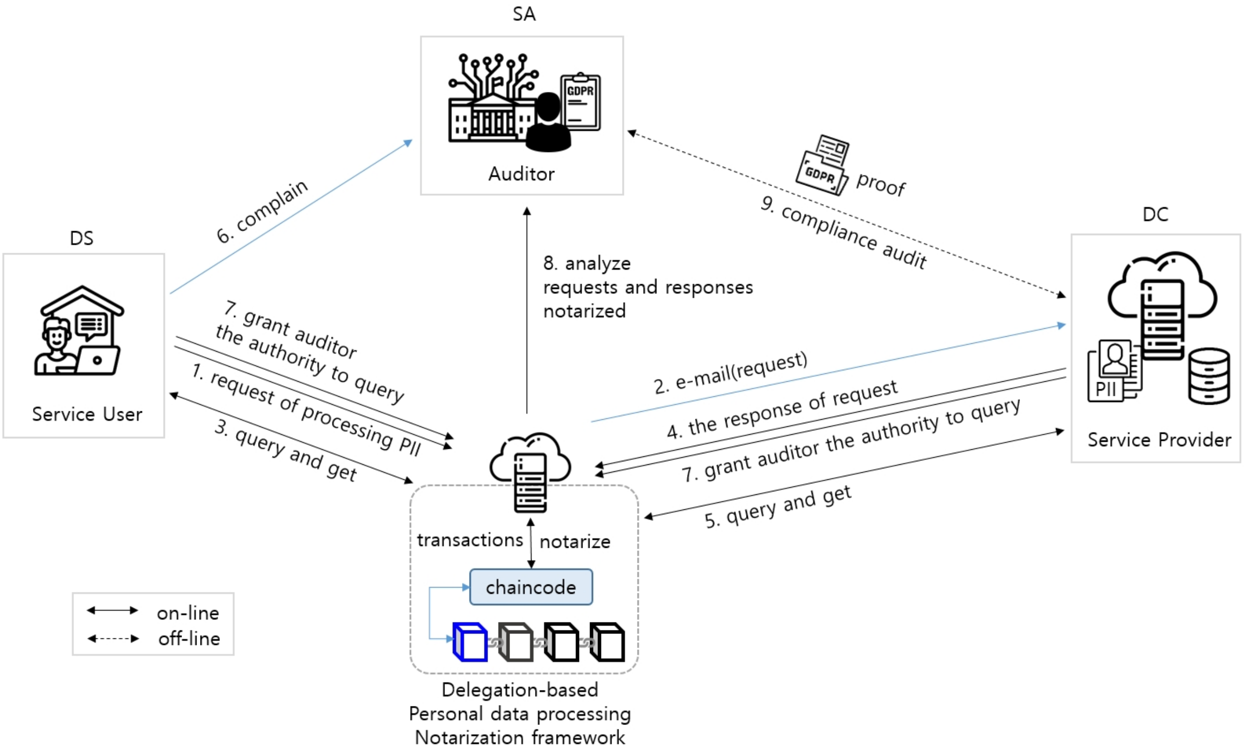

SA
Auditor
GDPR
DS
Service User
DC
Service Provider
PII
6. complain
8. analyze requests and responses notarized
GDPR
proof
9. compliance audit
7. grant auditor the authority to query
1. request of processing PII
3. query and get
2. e-mail(request)
4. the response of request
7. grant auditor the authority to query
5. query and get
transactions
notarize
chaincode
on-line
off-line
Delegation-based Personal data processing Notarization framework

Figure 1. A procedural overview of the personal data processing request notarization framework.

When the data subject requests the data controller to process personal data, the reliability and integrity of the requests and responses can be guaranteed by notarizing the request contents via the proposed notarization framework. Furthermore, transparency and security for data management is realized by distributing and storing the ledger wherein request transactions are recorded on the BC network and allowing only the auditor authorized by the transaction creator to access the stored transactions. Moreover, the proposed framework does not store personal data but only manages requests for the processing of personal data and response records that can perform GDPR compliance audits and secures the audit data without violating the GDPR. Furthermore, it can further strengthen and guarantee data subjects' rights to the processing of personal data.

The rest of this paper is organized as follows. Section 2 presents an overview of BC and GDPR and reviews the related works. Section 3 details the devised delegation-based personal data processing notarization framework, and Section 4 presents the implementation results of the proposed notarization framework by using Hyperledger Fabric (HLF). Furthermore, Section 5 presents the analyses of the functions and attributes of the proposed notarization framework, and the conclusions drawn from the study are presented in Section 6.

2. Background and Related Work

2.1. GDPR

GDPR, which came into force as of 25 May 2018, consists of 11 Chapters and 99 Articles, and it stipulates the rules related to the protection of natural persons related to the processing of personal data and the rules related to the free movement of personal data [15]. Among the role groups defined by the GDPR, the primary role groups for GDPR compliance are as follows:

- Data subject (DS): owner of the produced personal data who possesses the right to process his/her personal data; decides on the entrustment of the processing of own personal data to the service provider; requests to view, correct, delete, suspend processing,

or transmit personal data stored by the service provider and confirm the result; and can ask the supervisory authority to audit service providers for GDPR compliance.
- Service provider (SP): organization that provides various services by collecting and managing personal information; must comply with the GDPR regulations and prepare legal evidence for all actions involving collecting and managing personal data; and present the evidence upon request from DS and supervisory authorities.
- Data controller (DC): the person who is in charge of personal data management belonging to the SP; determines the purpose and method of the processing of personal data; and is responsible for managing and proving that the data for the DS is processed in a lawful, fair, and transparent manner.
- Supervisory authority (SA): the organization that conducts GDPR compliance audits; has the legal authority to regularly oversee and investigate the compliance of SPs with GDPR regulations; is an independent public authority responsible for monitoring the application of regulations to protect the basic rights and freedoms of natural persons regarding the processing of personal data and to promote the free flow of personal data within the Union.

One of the primary requirements when collecting and processing personal data in the GDPR is the technical implementation, which is required to guarantee the rights of the DS considering the concept of personal data protection. Violations can result in strong administrative penalties, such as fines, and they may be subject to laws and regulations even when conducting business in Europe [15]. On the basis of these requirements, a summary of the main Articles and Recitals particularly related to the processing of personal data is as follows:

- Articles 12–23: The DS may request a provision of information on personal data collected in relation to oneself, correction of inaccurate personal data about oneself without delay, deletion of personal data related to oneself without delay, and transmission of personal data provided by oneself to other DCs. Moreover, the DC shall not refuse to act in response to the DS's request for the exercise of these rights.
- Recital 59: Modalities should be provided for facilitating the exercise of DS's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. In addition, the DC should provide the means for requests to be made electronically, particularly where personal data are processed via electronic means.
- Recital 66: To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a manner that the DC who has made the personal data public must be obliged to inform the DCs that are processing such personal data to erase any links to, or copies, or replications of those personal data. Consequently, the DC must incorporate reasonable steps, considering the available technology and the means available to DC, including technical measures, to inform the DCs that are processing the personal data of the DS's request.

2.2. Blockchain

BC is a technology that distributes and verifies data within peer-to-peer network nodes in the form of blocks having a chain-type link. It is a data forgery prevention technique wherein several blocks are connected similar to a chain such that the hash of the current block becomes a component of the subsequent block using data encryption technology [27,28]. In the traditional transaction model, a central entity with authority functions as a gate and manages and guarantees the ledger data generated between nodes. In this centralized model, when a system with a central authority is incapacitated by internal or external intentional or unintentional attacks and failures, or when data are damaged or contaminated, the damage can spread throughout the entire network. In contrast, in the BC model, a copy of the ledger is distributed and stored to all nodes in the network, thereby reducing the risk and maintaining trust by removing the central authority. Owing to this structure, the BC has four key characteristics as follows [25]:

- Decentralization: BC network transactions can be performed between two peers (P2P) without authentication from a central authority.
- Persistence: As each transaction spreading through the network must be verified and recorded in blocks distributed throughout the network, tampering is almost impossible.
- Anonymity: Owing to the absence of a central system to store the personal data of the user, each user can communicate with the BC network using the created address, thus minimizing identity exposure.
- Auditability: In the BC, each transaction can repeatedly trace the previous transaction. This improves the traceability and transparency of the stored data.

Currently, the BC system can be divided into a public, private, and consortium BCs. Among these, private BC allows only authorized nodes to process consensus, can restrict read permission, and has high efficiency, so it is often used as a framework for corporate business processing [25].

2.3. Related Works of Blockchain-Based GDPR

Features of BC such as integrity, transparency, reliability, and traceability are effective when they are applied to tasks that require compliance management. To manage personal data or GDPR compliance, many researchers have performed research based on BC [8,15–25,28–42].

For related research analysis, by the SLR (Systematic Literature Review) approach, we selected research questions and derived key search terms such as ‘Personal Data’, ‘Blockchain’, ‘GDPR’, and ‘Notarization’ from the research questions, and we used them to search and collect papers. However, many of the extracted papers provide only preliminary methodological investigations. Through the primary analysis of the collected papers, we classified the papers with solution implementation plans or implementation examples and performed secondary intensive analysis. Table 1 shows related studies that suggest blockchain-based unique technologies in relation to GDPR compliance.

Table 1. Overview of related works based on BC.

No	Research Works	Proposed Technology
R01	Liang et al. in [29]	BC-based data provenance architecture in cloud environment with privacy
R02	Yan et al. in [30]	Protecting privacy and self-sovereignty through blockchains for OpenPDS
R03	Chowdhury et al. in [31]	BC as a notarization service for data sharing with personal data store
R04	Agarwal et al. in [32]	GDPR legislative compliance assessment
R05	Truong et al. in [33]	BC-based personal data management
R06	Truong et al. in [34]	GDPR-compliant personal data management
R07	Vargas in [35]	BC-based consent manager for GDPR compliance
R08	Kassem et al. in [36]	BC identity management system to secure personal data sharing in a network
R09	Rantos et al. in [37]	Consent management platform for personal data processing using BC
R10	Faber et al. in [38]	BC-based personal data and identity management system
R11	Piras in [39]	Privacy by design platform for GDPR compliance
R12	Mahindrakar and Joshi in [40]	Automating GDPR compliance using policy integrated BC
R13	Casaleiro in [41]	Protection and control of personal identifiable information
R14	Daudén-Esmel et al. in [42]	BC-based platform for GDPR-compliant personal data management

As a result of analyzing the related studies, the main research areas of the related studies are shown in Table 2.

Table 2. Related works by research field.

Major Research Field	Related Work's Number
Data provenance	R01
Access control	R05, R06
Notarization	R02, R03, R09
Identity management	R08, R10
Compliance assessment	R04, R12
Consent management	R07, R09, R14
GDPR compliance management	R06, R07, R11, R13

As a result of analyzing works related to BC-based personal data protection and GDPR compliance management, it can be seen that various methods and solutions are being studied for the expansion of GDPR compliance by using the characteristics of the BC such as integrity, confidentiality, transparency, and audit traceability. However, most of the works that tried to solve the privacy problem using BC do not consider GDPR, so it is difficult to apply it as a method to meet the requirements according to each regulation of GDPR. On the other hand, most of the works that suggested the application of BC to meet the requirements of the GDPR only present a conceptual design and did not present a practical implementation method of BC. Even works that presented practical implementation methods did not suggest a method to address the risk that BC-based systems may themselves violate GDPR principles because of their BC nature or how the records stored in BC could be utilized by an outer auditor for compliance audits. Most of the works designed the system structure under the premise that SP stores and manages personal data. So, the proposed architecture is designed so that users go through the system of SP to access BC. Nevertheless, the issue of the objective reliability of the data stored in BC was not taken into account. Most of the systems proposed by related works are designed to link the SP's system or storage with the blockchain through API. However, considering the actual situation, there may be a problem in GDPR application scalability due to difficulties in API development and the interworking module distribution in order to link the SP's legacy personal data management system with the BC-based proposed system. However, most studies do not take these issues into account. As shown in Figure 2, BC-based GDPR compliance solutions have been proposed in various areas; however, solutions for securing the reliability of personal data processing requests and response evidence are yet to be proposed [43].

Table 3 shows the limitations of previous related works for GDPR compliance audits so far.

Table 3. The limitations of related works for GDPR compliance audits.

Limitations	Related Work's Number
Lack of proposal of measures considering detailed regulations for GDPR compliance	R01, R02, R03, R05, R07, R08, R09, R10, R11
Lack of support for outer auditors	R05, R06, R08, R09, R10
Lack of consideration of scalability issues due to legacy system linkage	R01, R02, R03, R04, R05, R06, R09, R10, R12, R13, R14
Lack of consideration of personal data protection issues in BC (risk of privacy violations due to storage of personal data and all access records)	R01, R05, R06, R07, R13
Lack of presentation of a practical BC system implementation method	R02, R03, R07, R08, R10, R11, R12, R13, R14
Lack of research on GDPR compliance with personal data processing request	All except R06, R07, and R14

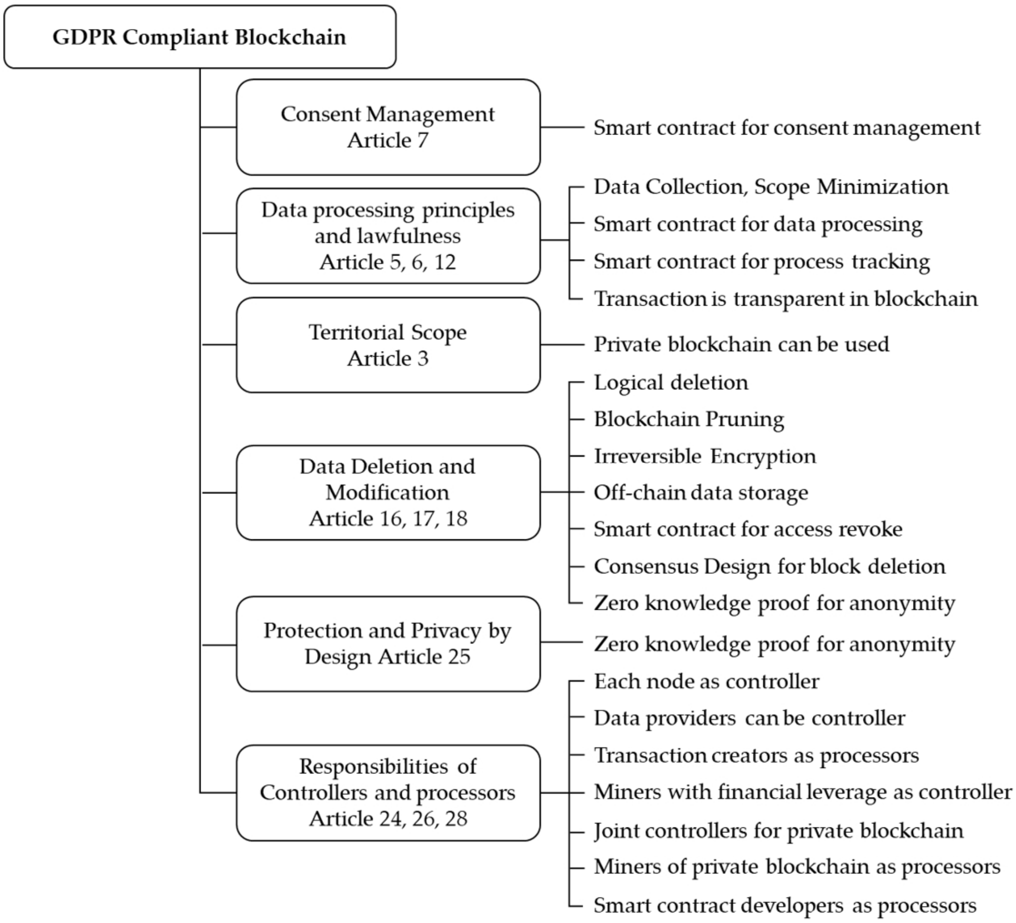

GDPR Compliant Blockchain
Consent Management Article 7
Smart contract for consent management
Data processing principles and lawfulness Article 5, 6, 12
Data Collection, Scope Minimization
Smart contract for data processing
Smart contract for process tracking
Transaction is transparent in blockchain
Territorial Scope Article 3
Private blockchain can be used
Data Deletion and Modification Article 16, 17, 18
Logical deletion
Blockchain Pruning
Irreversible Encryption
Off-chain data storage
Smart contract for access revoke
Consensus Design for block deletion
Zero knowledge proof for anonymity
Protection and Privacy by Design Article 25
Zero knowledge proof for anonymity
Responsibilities of Controllers and processors Article 24, 26, 28
Each node as controller
Data providers can be controller
Transaction creators as processors
Miners with financial leverage as controller
Joint controllers for private blockchain
Miners of private blockchain as processors
Smart contract developers as processors

Figure 2. Proposed solutions for GDPR compliance.

3. Delegation-Based Personal Data Processing Request Notarization Framework

This section proposes a delegation-based personal data processing request notarization framework that can notarize requests by the DS for the processing of personal data and its corresponding response. This was done to guarantee reliability and integrity for the GDPR audit. The DS delegates the request for the processing of personal data to the proposed framework, which forwards the request to the SP's DC by e-mail such that the DC responds to the request. For GDPR compliance, e-mail was used for a formal request proof of the processing of personal data from DS to SP. Herein, the request and response were recorded in the BC ledger. The ledger was notarized via nodes in the BC network. Consequently, the right of the DS to process personal data as stipulated by GDPR is guaranteed. Personal information may be included in the transaction sent by DS or DC to the proposed framework, so a method to protect personal data is required. The proposed framework protects personal data by using a session key-based encryption method. In order for the user to use the proposed framework, he/she must consent to the delegation of authority for personal data processing when he/she sign up for the service. This process is the same as general consent processing, so it is omitted from the proposed framework architecture.

To design a framework for GDPR compliance, we set the following design security. Based on the framework, the auditor can perform a GDPR compliance audit of security design goals to ensure reliability and credibility of data processing among network participants.

- Confidentiality: Network participants must be able to trust the transaction data that are evidence related to the processing of personal data.

- Integrity: It must be guaranteed that the created and managed transaction data are not illegally forged or altered.
- Non-repudiation: Denying related facts based on the subject of transaction data creation and management is not possible.

To design a new notarization framework, first, this section presents a derivation of the required features for GDPR compliance data processing, and thereafter, it proposes a private BC-based notarization framework that can satisfy the derived features.

3.1. GDPR Compliance Audit Scenario of Personal Data Processing Request

This section provides a service scenario based on a centralized system as shown in Figure 3 to withdraw certain required features to ensure GDPR compliance of the personal data processing request.

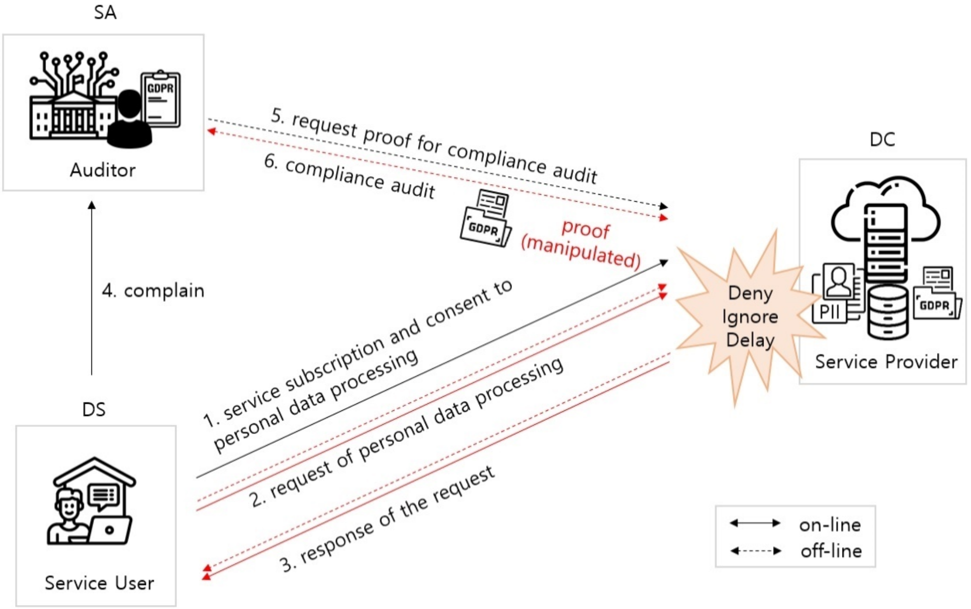

SA
GDPR
Auditor
5. request proof for compliance audit
6. compliance audit
GDPR
proof
(manipulated)
DC
Deny
Ignore
Delay
PII
GDPR
Service Provider
4. complain
1. service subscription and consent to personal data processing
2. request of personal data processing
3. response of the request
DS
Service User
on-line
off-line

Figure 3. GDPR compliance audit scheme in a conventional centralized environment.

Consider a system wherein each service provider stores various data in its own database, which is related to the personal data processing request trusted by the DS to provide various services. In this situation, GDPR SA conducts a GDPR compliance audit based on the evidence data submitted by the service providers. The scenario where network participants perform their own actions and the SA conducts a GDPR compliance audit related to the processing of SPs is as follows:

- The DS must consent to the processing of personal data to utilize the services of an SP and subscribe to services on the system. The SP is the DC of personal data.
- SPs collect and manage the personal data of DSs adhering to GDPR regulations.
- In accordance with GDPR regulations, the DS requests the SP to view, correct, delete, stop, and transmit his/her personal data at any time if needed.
- The SP accepts the request and performs all processes without any delay. After executing the process, the results of the processing are notified to the DS. Particularly, if the DS uses their request on an electronic method, it responds to the request through an electronic method. The SP must record the processing logs and establish legal evidence data to prove GDPR compliance.
- The SA manages SP to ensure compliance with GDPR regulations and performs a GDPR compliance audit by analyzing evidence data presented by the SP to certify them.
- DSs may request a GDPR compliance audit of the SP from the SA in the processing of their personal data based on a specific situation.

- SA investigates the operation status of SPs considering the requested GDPR compliance audit and takes appropriate measures based on results obtained from the investigation.

3.2. Challenges and Requirements of the GDPR Compliance Audit for Personal Data Processing Request

In this section, through scenario analysis, we discuss the challenges and solutions for securing the reliability of personal data processing, particularly requests and responses, in GDPR compliance audits. In the scenario, the SA receives all evidence data related to the GDPR compliance audit from the SP, which is the DC of personal data. GDPR compliance verification is performed through a record of delegation-based consensus between the DS and SP; that is, it is based on the consent given by the DS to the processing of personal data, the performance of the SP with GDPR compliance in managing the DS's personal data is verified. The request made by the DS for the processing of personal data is a right attributed to the DS stipulated in Chapter 12 of GDPR, and response to the request is a duty of the SP. However, as the record can be damaged and contaminated by the SP, its reliability cannot be assured as an objective view on credibility without any consent from the DS. This is because the request is not the processing of personal data entrusted by the DS to the SP in consent. Thus, for the DS to overcome this drawback without relying on evidence provided by the SP when it responds inappropriately to requests, external notarization is the approach used to secure the reliability of the request sent by the DS. However, notarizing the requests of DS is a challenge. First, maintaining records related to requests is difficult unless electronic methods such as e-mail are used. In addition, to notarize records such as e-mail, the data on those records must be requested from an e-mail SP, and thereafter, the data have to be notarized through an organization with legal authority. Consequently, the problem of securing an objective view of the credibility on records for requests and responses can be analyzed as "the need for reliable notarization for request for the processing of personal data that can be easily used without sharing personal data and is processed in real time." GDPR regulations regarding the requests of the DS that require external notarization are Article 12 and Articles 15–21. Further, for the regulations, the functions shown in Figure 4 are required to support GDPR compliance audits related to the personal data processing request.

Considering the environment in which many countries must comply with GDPR, it is necessary to establish a notarization system that supports a distributed environment for the notarization of personal data processing requests. The following functions are required to build a notary system in a distributed environment [44]:

- Sealing of data: The sealing of data ensures data integrity and not secrecy. It must produce the same value when the data are sealed and when they are verified. A third party cannot obtain the data, modify it, and produce a new value that is acceptable when the data and value are verified.
- Accessible to all: The notary must be accessible to all who desire to seal data.
- Trusted or certifiable: The notary must either be trusted or certifiable, as must its cryptographic keys.
- Highly trusted communications: If the notary exists in a different domain, then the communication between the notary and user must be highly secure. The client must possess the means of ensuring that the data he/she has notarized are the data that were requested to be notarized.
- Authentication: It is important that the user that starts a transaction is the only user to participate in that transaction or delegate work to other users. Consequently, the user that starts a transaction can be attributed with that transaction when it is committed.

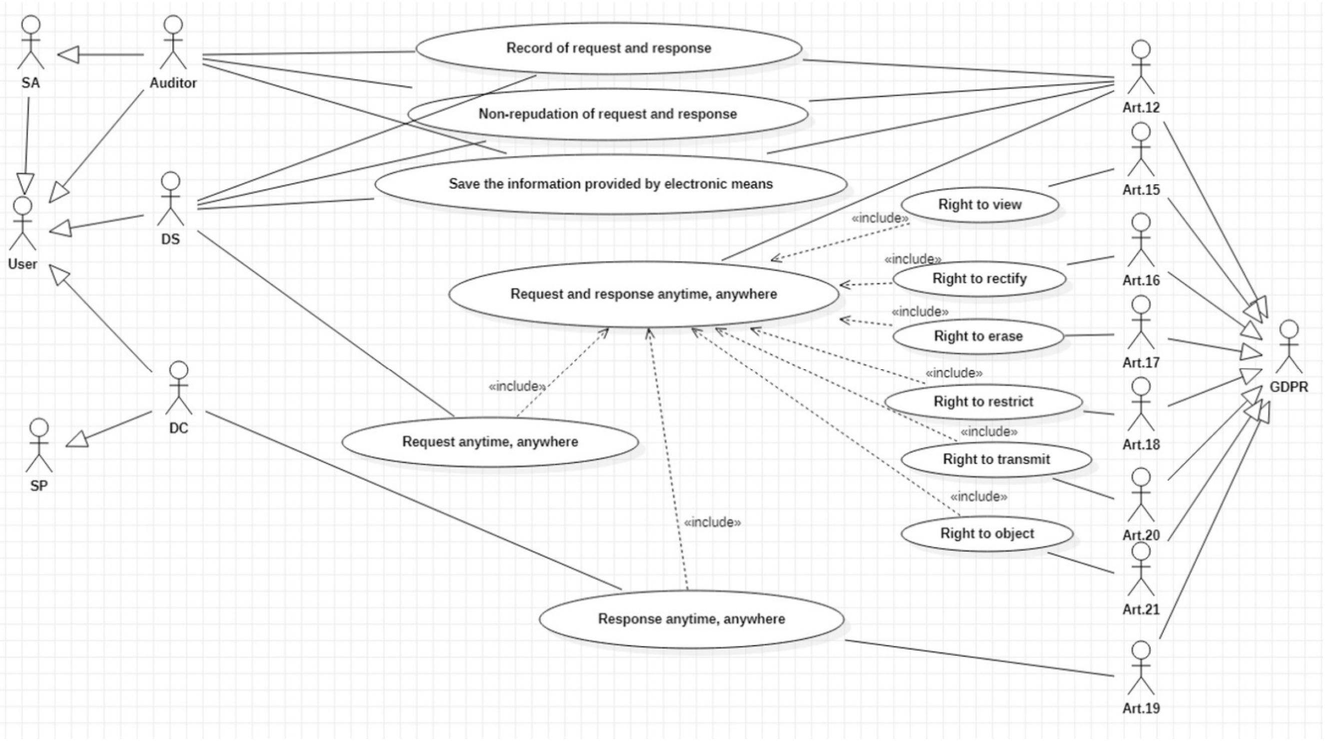

SA
Auditor
User
DS
DC
SP
Record of request and response
Non-repudation of request and response
Save the information provided by electronic means
Request and response anytime, anywhere
Request anytime, anywhere
Response anytime, anywhere
Right to view
Right to rectify
Right to erase
Right to restrict
Right to transmit
Right to object
«include»
Art.12
Art.15
Art.16
Art.17
Art.18
Art.20
Art.21
Art.19
GDPR

Figure 4. Requirements to support GDPR compliance audits regarding the DS's requests.

With respect to the processing of personal data, all DCs must comply with the GDPR principles relating to the processing of personal data as stipulated in Article 5 of the GDPR. This is also applicable for GDPR compliance audit management systems that deal with personal data. In particular, as deleting stored data is difficult, owing to the nature of the distributed environment in BC, the BC-based GDPR compliance audit management system is required to minimize personal data collection to not violate the GDPR principle by itself [36].

Finally, considering the reality that many SPs in various countries are operating personal data processing systems, the feasibility of minimizing modifications to the legacy system for linkage is required for the notarization framework to be applicable for GDPR compliance audit.

3.3. Design Goals

We analyzed the requirements for GDPR compliance audit management related to DS requests, requirements for a notarization system in a distributed environment, GDPR principles related to personal data processing, and the feasibility of applying to all SPs in a real environment. Based on the analysis, the design goals of the personal data processing notarization framework for GDPR compliance audit, a solution to the problem, were derived as shown in Figure 5.

The details of the functional design goals other than the security design goals mentioned previously in the derived design goals are as follows:

- Delegation for GDPR: DS must have the ability to delegate requests for the processing of personal data to the notarization system and deliver them to DC in an electronic manner. Data creators who want notarization should be easily accessible anytime, anywhere.
- Audit trail for GDPR: Requests and responses must be recorded in the form of 'who, when, to whom, and what' for GDPR compliance, and they must preserve integrity. Records must be stored in a manner such that they can be viewed by an auditor authorized by the DS and DC.

- Notarization of request for the processing of personal data: Verification of the personal data processing request and corresponding data through a number of trusted notaries should be enabled, and furthermore, the ability to notarize the integrity of the stored and retrieved data is important. The authenticity and key management of data creators and notaries should ensure that the reliability of the data cannot be denied.
- Managing permission for audit: Only the author or recipient of the data should have access to the relevant data. DSs and DCs must have the ability to authorize auditors to view data for GDPR compliance audits related to requests for the processing of personal data. However, searching for data other than the data of the approver that the auditor has authorized the inquiry authority to view should be disabled.
- Distribution of trust: The authentication of users using the notarization system and the authority that manages the ledger must be performed and mutually verified by certain trusted institutions across countries rather than one.
- Minimum collection: Personal data other than data related to requests and responses should not be collected, and GDPR compliance audits should be possible for requests from DSs without sharing them with DCs or not being provided them from DCs.

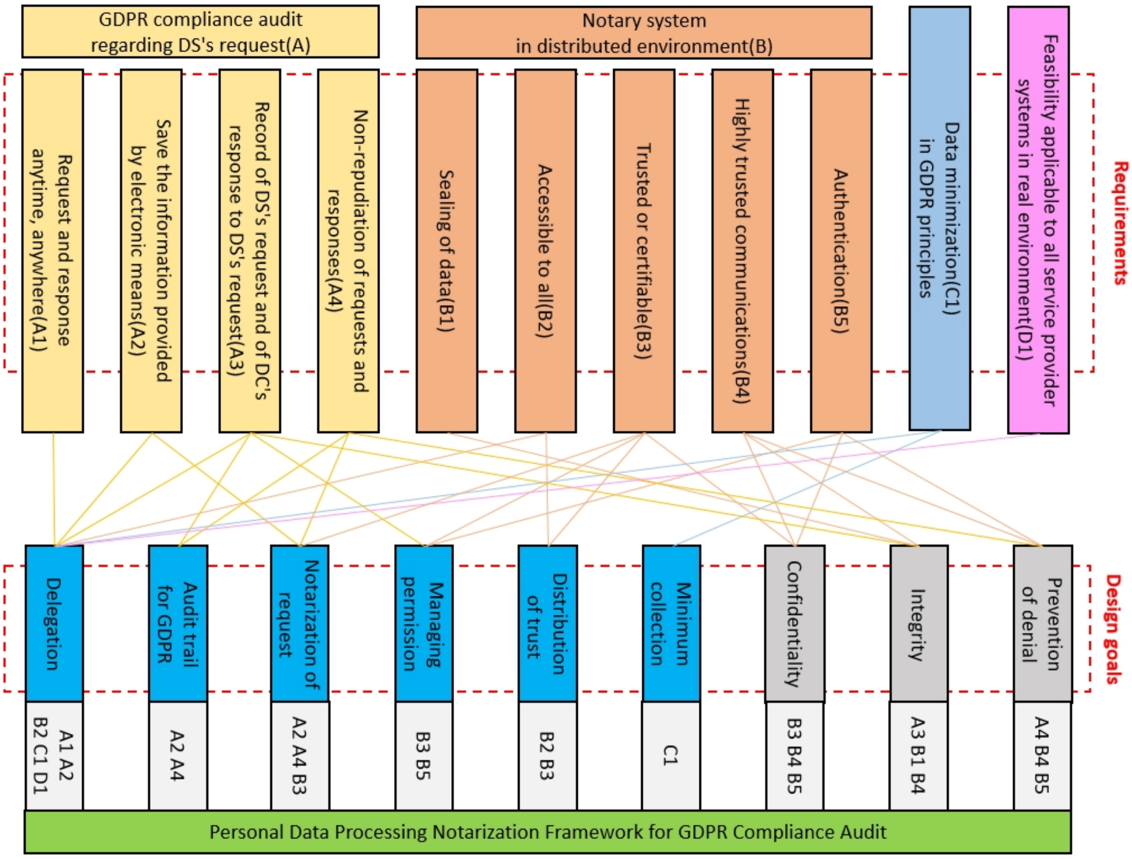

GDPR compliance audit regarding DS's request(A)
Notary system in distributed environment(B)
Request and response anytime, anywhere(A1)
Save the information provided by electronic means(A2)
Record of DS's request and of DC's response to DS's request(A3)
Non-repudiation of requests and responses(A4)
Sealing of data(B1)
Accessible to all(B2)
Trusted or certifiable(B3)
Highly trusted communications(B4)
Authentication(B5)
Data minimization(C1) in GDPR principles
Feasibility applicable to all service provider systems in real environment(D1)
Requirements
Delegation
Audit trail for GDPR
Notarization of request
Managing permission
Distribution of trust
Minimum collection
Confidentiality
Integrity
Prevention of denial
Design goals
A1 A2 B2 C1 D1
A2 A4
A2 A4 B3
B3 B5
B2 B3
C1
B3 B4 B5
A3 B1 B4
A4 B4 B5
Personal Data Processing Notarization Framework for GDPR Compliance Audit

Figure 5. Notarization framework design goals.

3.4. Notarization Framework

The proposed notarization framework aims to provide an objective view of credibility assurance for evidence data of processing requests and responses for GDPR audit on the processing of personal data. Figure 6 shows the conceptual network configuration of the proposed framework, consisting of DSs (service users), DCs (SPs), SAs (auditors), and notarization systems.

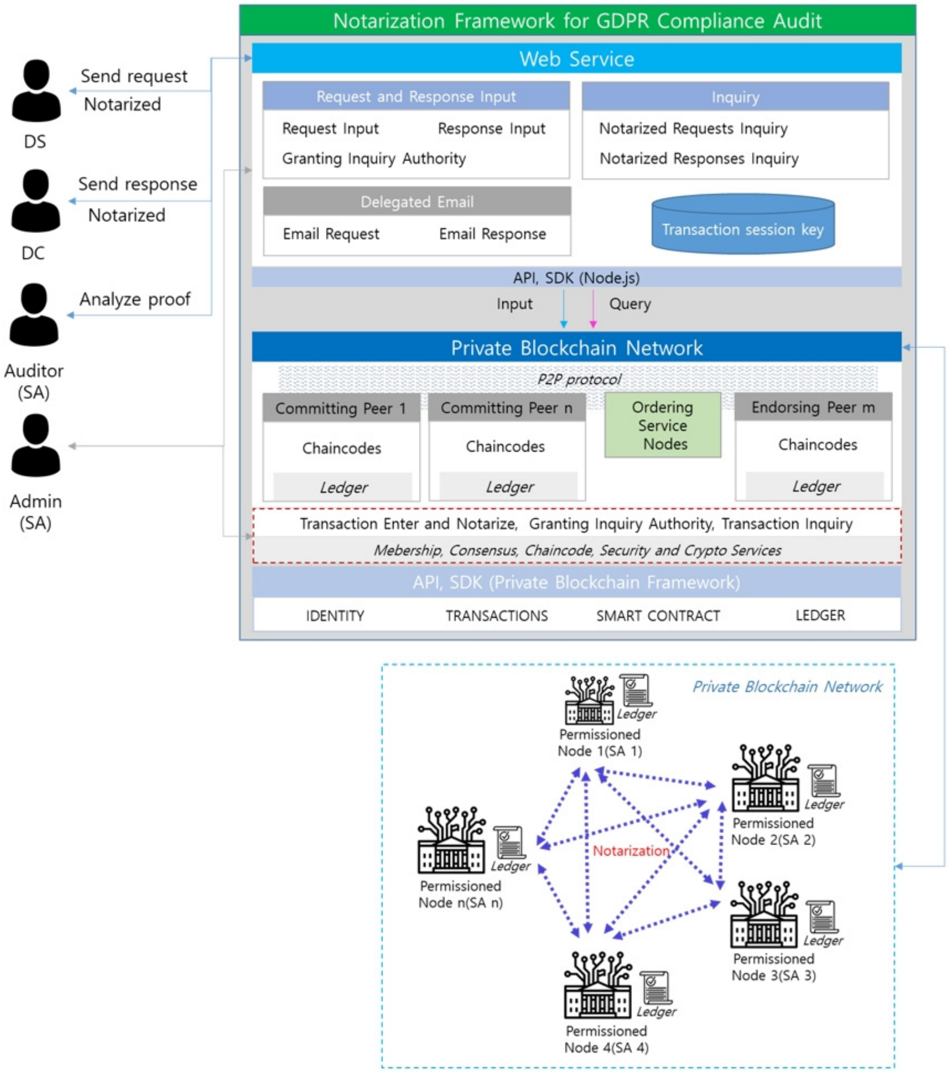

Notarization Framework for GDPR Compliance Audit
Web Service
Request and Response Input
Request Input
Response Input
Granting Inquiry Authority
Inquiry
Notarized Requests Inquiry
Notarized Responses Inquiry
Delegated Email
Email Request
Email Response
Transaction session key
API, SDK (Node.js)
Input
Query
Private Blockchain Network
P2P protocol
Committing Peer 1
Chaincodes
Ledger
Committing Peer n
Chaincodes
Ledger
Ordering Service Nodes
Endorsing Peer m
Chaincodes
Ledger
Transaction Enter and Notarize, Granting Inquiry Authority, Transaction Inquiry
Mebership, Consensus, Chaincode, Security and Crypto Services
API, SDK (Private Blockchain Framework)
IDENTITY
TRANSACTIONS
SMART CONTRACT
LEDGER
Send request
Notarized
DS
Send response
Notarized
DC
Analyze proof
Auditor (SA)
Admin (SA)
Private Blockchain Network
Ledger
Permissioned Node 1(SA 1)
Ledger
Permissioned Node 2(SA 2)
Ledger
Permissioned Node n(SA n)
Notarization
Ledger
Permissioned Node 3(SA 3)
Ledger
Permissioned Node 4(SA 4)

Figure 6. Notarization framework overview based on BC.

All data derived from the process of requesting and responding to the processing of personal data between the DS and DC are stored in the BC ledger through a notarization system. SAs can conduct transparent and reliable GDPR compliance audits based on the notarized ledger through the notarization system.

Moreover, for the reliability of notarization, only authoritative nodes should be allowed to participate in notarization. Therefore, the proposed notarization framework is based on a private BC framework wherein only authorized participants can participate in the BC network. The roles of the network participants are as follows:

- DS (Service user): To register request information for viewing, correction, deletion, suspension of processing, and transmission of personal information stored by SPs in the system. To query the request and the response records of the DC in the system. To complain to the SA if the DC fails to satisfactorily process the personal data of the DS against the interests and rights of the DS. To grant SAs the authority to query the records of requests for the processing of personal data through the system.
- DC (SP): To respond to requests by the DS for the processing of personal data and register responses in the system. To grant SAs the authority to query response records to requests for the processing of personal data through the system.
- Auditor (SA): With the authority authorized by the DS, to query the system regarding the records of the requests and response for the processing of personal data.

To conduct a GDPR compliance audit of the DC to determine compliance. To ensure that the DC adheres to the GDPR regulations and is authorized by the DC to inquire the data of the DC when performing an audit. To check the records of the response of the DC to the requests made by the DS stored in the system to determine the regulations are being adhered to.

- Notarization system: To provide services to the web through smart contracts, manage the BC ledger, and manage the authority of network participants. To store the data of the request in the BC when the DS registers a request for the processing of personal data in the system.

3.5. Notarized Data Structure

The main notarized data required for a GDPR compliance audit related to the processing of personal data comprises a request for data processing and a response to the request. The request, which is one of the primary data in the proposed framework, should have the request number, ID of the DS, URL of the SP, e-mail address of the SP, data processing type, and the information of the request. These are stored in blocks as a transaction and following the creation of a ledger block, the framework adds it to the BC to provide security and integrity. However, it is important to ensure controlled access and management of notarized data only by network entities who have the authority to access the framework. To realize this, a data structure should be defined for authorization control consisting of the authorization number, authorization type, authorization ID, SP URL, grantor's ID, and permitted authorization period. Details of the processing request, response on request, and authorization-related data structure for configuration of the BC ledger are as follows:

- Request: A structure requests for the processing of personal data sent by the DS to the DC.
- Response: A structure for a response to a request sent by the DC to the DS.
- Authorization: A structure of data access rights granted by the DS or DC.
- Parameters of data structures for transactions are as follows:
- Parameters of Request: The number of requests, DS's ID, SP's URL, SP e-mail, processing type, the content of the request and timestamp.
- Parameters of Response: The number of responses, the number of requests, DS's ID, data SP's URL, subject's e-mail, processing type, content of request, content of response, and timestamp.
- Parameters of Authorization: The number of grants, grantor type, auditor's ID, SP's URL, grantor's ID, and authority expiration date.

The value of the processing type, which is a parameter of the structure request and structure response, is pre-defined as reading, correction, deletion, processing suspension, and transmission, which are defined as the right of the DS to own data in the GDPR. The DS selects the type of processing, and thereafter, the request is delegated and notarized for the processing.

3.6. Identity Management

Considering that the proposed notarization framework is based on BC, a distributed environment, the entities must be uniquely identified. The proposed framework requires all entities to be authenticated via a Certificate Authority (CA) before using the proposed framework and to receive an asymmetric encryption key (public key, private key) and certificate. Furthermore, there is a need to define a unique concept of identity and the rules by which the identity is to be managed (identity verification) and authenticated (signature creation and verification) using a member service provider, which abstracts the user management functions provided by the private BC framework.

3.7. Personal Data Protection

Transactions registered with BC for notarization contain request and response contents that may contain sensitive personal data. Owing to the characteristics of the BC network, which copies and distributes the ledger, there is a risk of the sensitive personal data of transactions being exposed to unauthorized peers. Thus, to prevent this risk, the request and response contents should be encrypted and stored, and an encryption key that can decrypt data should be provided only to entities with the authority to inquire the data, such as the creator, receiver, and auditor. As shown in Figure 7, the proposed framework generates a session key for each transaction in the application before registering the request and response in BC. The transaction ID (trxId) key and {session key (sKey), DS's ID (dsId), SP's url (spUrl)} value pairs are saved to the application database. Subsequently, the request and response contents are encrypted using the session key and registered in the BC.

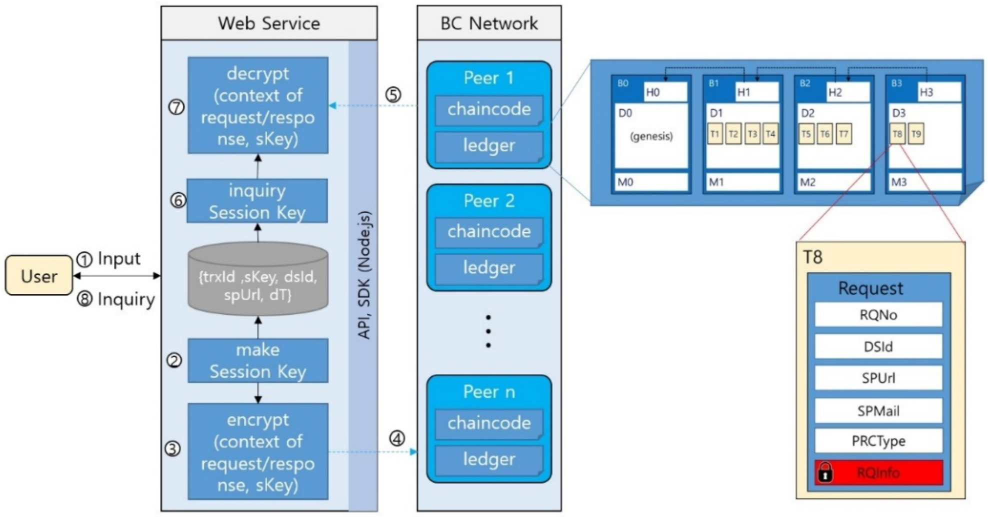


Figure 7. Personal data encryption process in transaction using session key.

The transaction ID generation algorithm is identical to the transaction key generation algorithm in the BC of the proposed framework. As in (1), the request combines {ID of DS, creation timestamp}, while the response combines {SP URL of DC, creation timestamp}. Algorithm 1 is an algorithm for generating a session key.

$$\begin{array}{c}\text{IF transaction type equal 'request' THEN}\\ \text{transaction ID} = \text{DS's ID} + \text{timestamp}\\ \text{IF transaction type equal 'response' THEN}\\ \text{transaction ID} = \text{SP's URL} + \text{timestamp}\end{array} \tag{1}$$

Algorithm 1. Make Session Key

```
INPUT: DS's ID, SP's URL, transaction ID, transaction type, private data, timestamp
OUTPUT: session key
IF transaction type equal 'request' THEN
    SET session key to result of
        SUM result of
            COMPUTE hash encode with transaction ID
                and result of
                COMPUTE hash encode with private data
    SET data array with transaction ID, session key, DS's ID, SP's URL, and timestamp
    ADD data array made key with transaction ID into application database
ENDIF
RETURN session key
```

To retrieve and decrypt a transaction that is encrypted using the generated session key, the transaction session key is required, but only the creator or receiver of the transaction can inquire. Algorithm 2 is an algorithm for querying the session key.

Algorithm 2. Inquiry Session Key

```
INPUT: user ID, transaction ID
OUTPUT: session key
SET user's type to the result of READ user type of user ID
IF user's type is equal to 'DS' THEN
    SET session key to the result of
        READ session key from application database
            where user ID equal DS's ID in DB
            and the transaction ID equals the transaction ID in DB
ENDIF
IF user's type equals 'DC' THEN
    SET SP's URL to the result of
        READ SP's URL from the user information in the DC's session
    SET session key to the result of
        READ session key from the application database
            where the SP's URL equals the SP's url in DB
            and the transaction ID equals the transaction ID in DB
ELSE
    SET session key to null
  ENDIF
RETURN session key
```

3.8. Notarization Process

DS transmits a request for processing personal data through the notarization system. The notarization system presents the notarization upon request and delivers it to the SP via e-mail. The SP, which is the DC, performs appropriate processing according to the request and thereafter submits the processing result to the notarization system. Consequently, the notarization system creates a block containing the processing request, processing result, and notarization content and then adds it to the ledger. Figure 8 shows the notarization process for the processing of personal data complying with the GDPR.

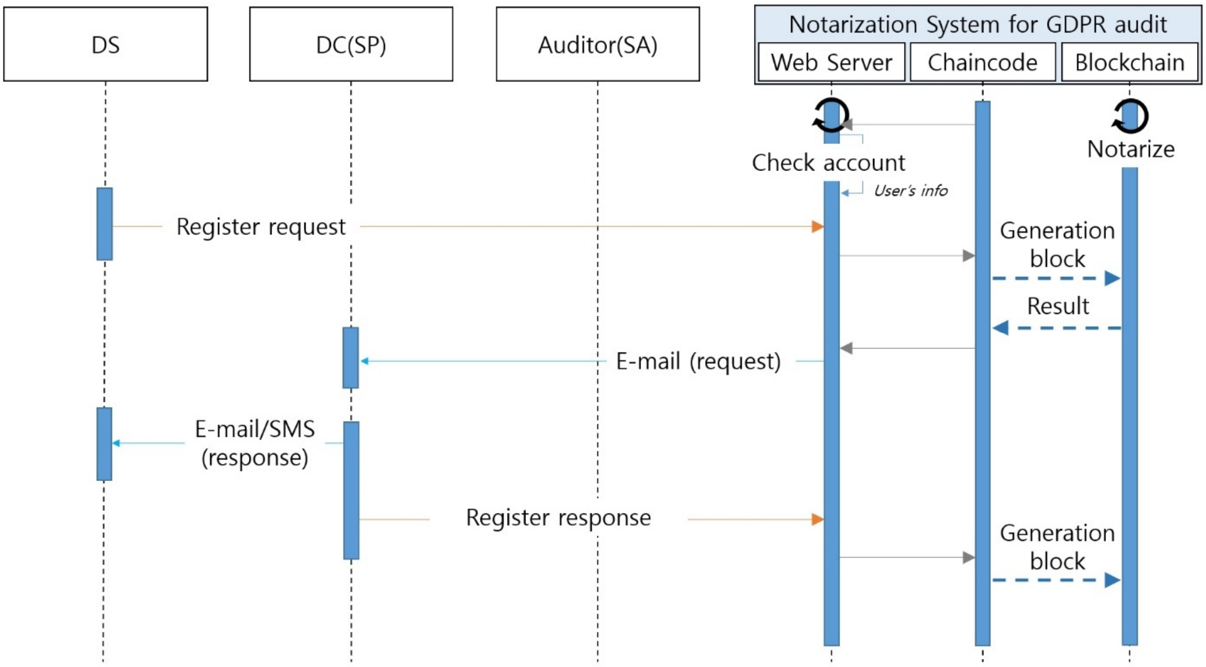


Figure 8. Notarization process of the request and response.

Algorithm 3 is the algorithm for smart contract implement of request registration in Figure 8.

Algorithm 3. Input Request

```
INPUT: DS's ID, SP's URL, SP's e-mail, process type, contents of request, timestamp
OUTPUT: transaction
  // make key
  SET transaction key to the result of
CALL make request number with the DS's ID and timestamp
            RETURNING request number
  SET request structure with the transaction key, DS's ID, SP's URL, SP's e-mail,
                            process type, contents of request, and timestamp
  SET JSON formed request to the result of
       CALL transform to JSON with request structure
             RETURNING JSON formed request
  RETURN the result of
     CALL make transaction with transaction key and JSON formed request
     RETURNING transaction
```

Algorithm 4 is the algorithm for the smart contract implement of response registration in Figure 8.

Algorithm 4. Input Response

```
INPUT: request transaction key, DS's ID, SP's URL, SP's e-mail, process type,
       contents of request, contents of response, timestamp
OUTPUT: transaction
  //check request being
     SET existing to the result of
       CALL checks whether it exists with request transaction key RETURNING existing
  IF existing is false THEN
     PRINT "the request does not exist"
     RETURN null
  ENDIF
  // make key
  SET transaction key to the result of
     CALL make response number with SP's URL and timestamp
          RETURNING response number
  SET response structure with transaction key, DS's ID, SP's URL, SP's e-mail,
       process type, contents of request, contents of response, timestamp
  SET JSON formed response to the result of
       CALL transform to JSON with response structure
            RETURNING JSON formed response
  RETURN the result of
     CALL make transaction with transaction key and JSON formed response
RETURNING transaction
```

Figure 9 shows the process of inquiring transactions stored in the notarization framework by an authorized participant.

3.9. GDPR Compliance Audit Process

The SA can perform a GDPR compliance audit on DC as needed. It may perform an audit by obtaining authority to inquire transactions related to the processing of personal data between DS and DC to validate the GDPR compliance of DC during the audit process. Figure 10 shows the audit procedure if the DS makes a request for a GDPR compliance audit to the SA on his/her personal data processing.

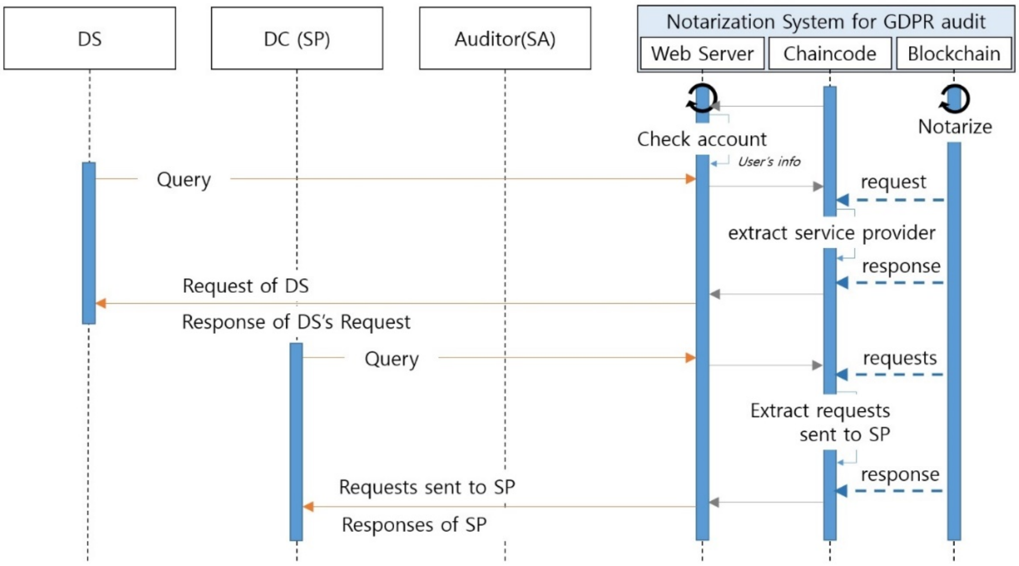


Figure 9. Transaction query process for the request and response for the processing of personal data.

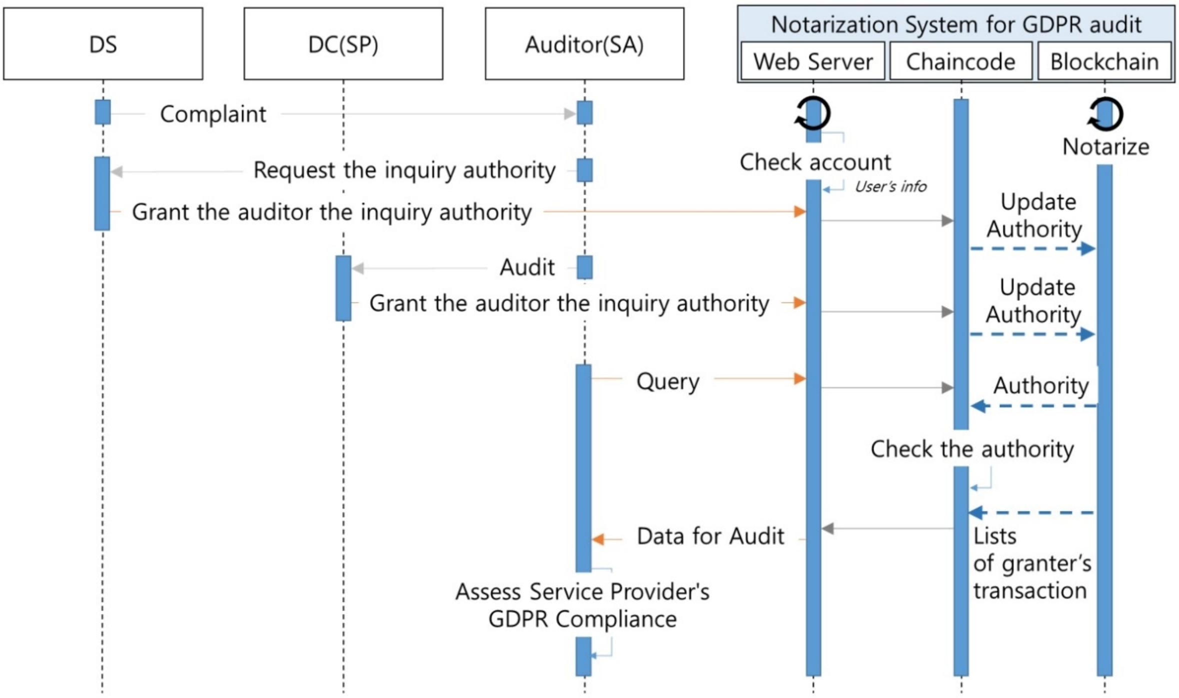

DS
DC(SP)
Auditor(SA)
Notarization System for GDPR audit
Web Server
Chaincode
Blockchain
Complaint
Request the inquiry authority
Grant the auditor the inquiry authority
Check account
User's info
Notarize
Update Authority
Audit
Grant the auditor the inquiry authority
Update Authority
Query
Authority
Check the authority
Data for Audit
Lists of granter's transaction
Assess Service Provider's GDPR Compliance

Figure 10. GDPR compliance audit process.

Algorithm 5 is an algorithm for the smart contract implement of granting inquiry authority in Figure 10.

Algorithm 5. Input Authority

```
INPUT: grant key, grant type, auditor's ID, SP's URL, grantor's ID, expiry date
OUTPUT: authority transaction
IF grant type equal "DS" THEN
    SET grant key to the result of JOIN auditor's ID and grantor's ID
ELSE
    SET grant key to the result of JOIN auditor's ID and SP's URL
ENDIF
  //check authority being
SET existing to the result of
     CALL checks whether it exists with grant key RETURNING existing
IF existing is true THEN
    SET authority transaction to the result of
        CALL update authority with grant key and expire date
             RETURNING authority transaction
ELSE
    SET authority structure with grant key, grant type, auditor's ID, SP's URL,
             grantor's ID, and expire date
    SET JSON formed response to the result of
        CALL transform to JSON with response structure
                 RETURNING JSON formed response
ENDIF
RETURN the result of
            CALL make transaction with transaction key and JSON formed response
RETURNING transaction
```

Algorithm 6 is the algorithm for the smart contract implementation of the query of notarized requests and responses in Figure 10.

Algorithm 6. Get Notarized Lists

```
INPUT: grant key, grant type, start date for query, end date for query
OUTPUT: request transaction list, response transaction list
  //check authority validation
SET validation of authority to the result of
     CALL authority validation with grant key RETURNING validation of authority
IF validation of authority is false THEN
     PRINT "The authority isn't valid"
RETURN null
ENDIF
  //separate and extract IDs
SET auditor's ID, DS's ID, SP's URL to the result of
     CALL extract IDs with grant key RETURNING auditor's ID, DS's ID, SP's URL
  // range query of DS's request
SET list of request to the result of
    CALL query by range with
         JOIN DS's ID and start date for query, JOIN DS's ID and end date for query
         RETURNING list of request
  // range query of SP's response
SET list of response to the result of
    CALL query by range with
         JOIN SP's URL and start date for query, JOIN SP's URL and end date for query
         RETURNING list of response
RETURN the result of
    CALL make transaction with list of request and list of response
RETURNING list of JSON formed request, list of JSON formed response
```

4. Implementation

The proposed framework was implemented using a private BC and HLF. In this section, the implementation results are presented in the order of development environment and notarization framework implementation.

4.1. Development Environment

BC was implemented using HLF 2.2, a private framework, Go chaincode, and node.js SDK for web services. Furthermore, raft was used for the BC consensus process. The raft ordering service is simpler and faster than other consensus algorithms, as it guarantees crash fault tolerance under the assumption that all nodes are honest. For transactions, the service server forms a consortium and runs channel settings and services through configtx.yaml. In addition, for a BC-based system simulation, the security and performance of the system must be considered by configuring an effective architecture of authority management and network according to the role of network participants. We constructed the proposed notarization framework network using Docker for simulation, as shown in Figure 11.

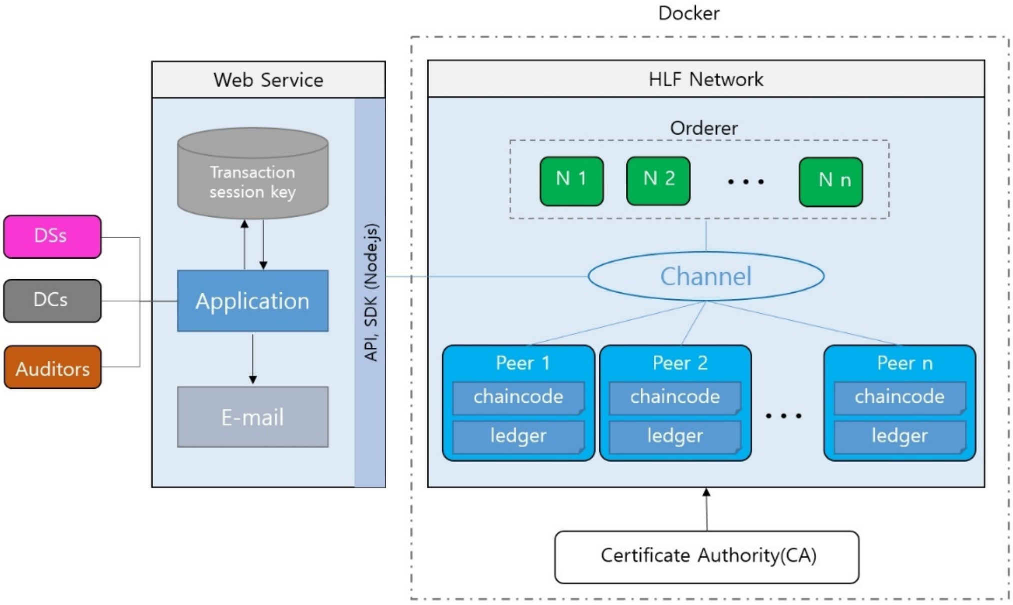


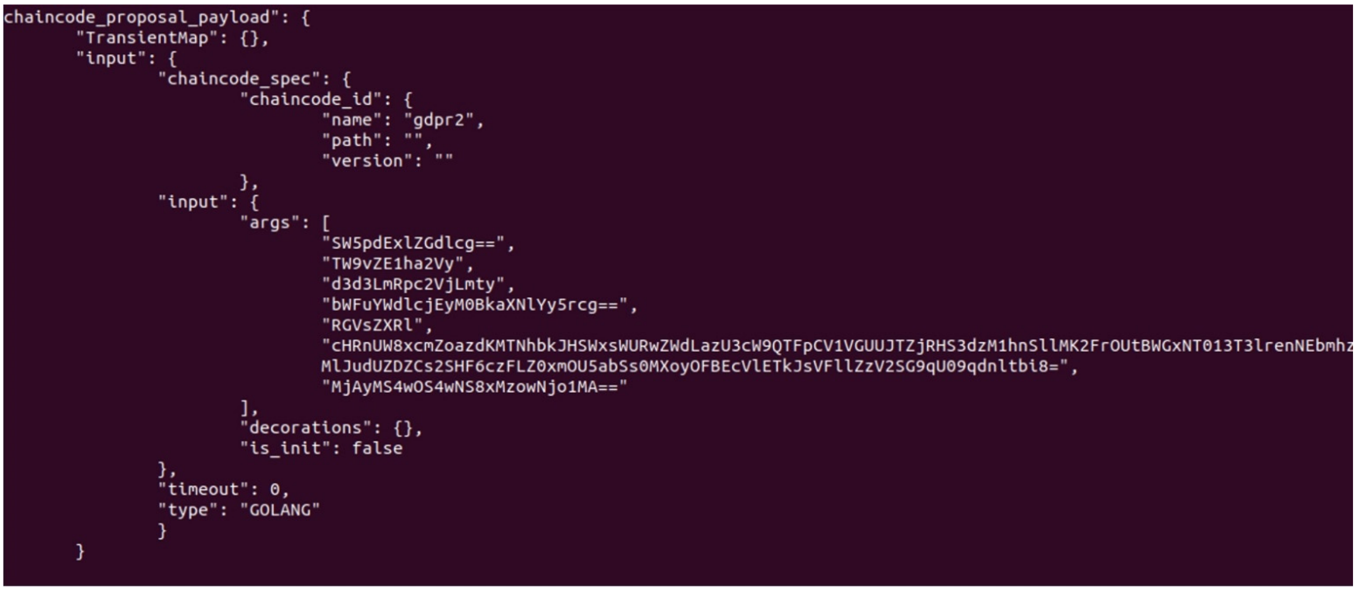
Figure 11. Simulation system architecture for the proposed framework using HLF.

4.2. Simulation

We considered the use case of conducting an audit with notarized data, using the framework proposed by the auditor of the SA when the DS requests the DC to process personal data but DC ignores the request without a good reason. Consequently, we developed and simulated a prototype of the framework.

DS, DC, and SA participated in the proposed framework for GDPR compliance audit. As shown in Figure 11, the DS and DC store the request and response transaction in the BC network through the proposed framework, and thereafter, the user DS, DC, and auditor retrieve the stored transaction through the proposed framework. Subsequently, the framework copies and forwards/verifies/distributes the transaction to each peer through the entity that ordered it. Herein, several selected peers perform the verification process and sign using their private key, which corresponds to the role of a notary public. Moreover, the peers are only operated by authorized SAs.

For authentication of all entities participating in the BC network, Fabric CA, a built-in CA provided by HLF by default was used. Fabric CA adopts a PKI hierarchical model and is used to generate X.509 digital certificates. A certificate contains an entity's key and related information. We set in docker-compose-ca.yaml, as shown in Figure 12, such that the CA service was run on port 7054 using Docker, and through this, all nodes and users were authenticated and authorized.



```
chaincode_proposal_payload": {
        "TransientMap": {},
        "input": {
                "chaincode_spec": {
                        "chaincode_id": {
                                "name": "gdpr2",
                                "path": "",
                                "version": ""
                        },
                "input": {
                        "args": [
                                "SW5pdExlZGdlcg==",
                                "TW9vZE1ha2Vy",
                                "d3d3LmRpc2VjLmty",
                                "bWFuYWdlcjEyM0BkaXNlYy5rcg==",
                                "RGVsZXRl",
                                "cHRnUW8xcmZoazdKMTNhbkJHSWxsWURwZWdLazU3cW9QTFpCV1VGUUJTZjRHS3dzM1hnSllMK2FrOUtBWGxNT013T3lrenNEbmhz
                                MlJudUZDZCs2SHF6czFLZ0xmOU5abSs0MXoyOFBEcVlETkJsVFllZzV2SG9qU09qdnltbi8=",
                                "MjAyMS4wOS4wNS8xMzowNjo1MA=="
                        ],
                        "decorations": {},
                        "is_init": false
                },
                "timeout": 0,
                "type": "GOLANG"
                }
        }
```

Figure 12. A transaction in a saved block viewed by peers.

The DS entered a personal data processing request including {SP's URL, DC's e-mail, processing type, content of request} through the web service of the proposed framework, and we delegated the delivery and notarization to the proposed framework. The transaction occurred in the block, as shown in Figure 12, when the json format data input by DS and delivered to the chaincode of the framework and the requested transaction are verified and agreed by the notary nodes; thereafter, the copied and stored block was inquired by the peer. Furthermore, as evident in Figure 12, the request content containing personal information is encrypted and cannot be verified by the peer.

Although the notarization framework sends the request made by the DS to the personal data manager email address entered by the DS, if there is no reasonable response from the SP, the DS requests the SA to audit the SP. Herein, the DS grants inquiry authority to the auditor such that his/her request transaction can be inquired. The auditor can perform GDPR compliance audits on SPs based on the querying request transactions.

5. Analysis and Evaluation

For the analysis of the proposed framework, the measurement of the degree of satisfaction of the requirements based on the requirements defined in Section 3 must be considered. This section details an analysis of the degree of satisfaction of the proposed framework and presents a comparison with related studies from the perspective of GDPR compliance audit.

5.1. Analysis of Meeting the Requirements of the Notarization Framework for GDPR Compliance Audits

The requirements proposed for analysis in Section 3.1 were considered as analysis elements of the system. The analysis was conducted to determine whether the functions and properties of the proposed notarization framework meet the following requirements.

5.1.1. Security Analysis

The proposed framework was designed as per the design goal of Figure 5, and all the security requirements of the notary framework for the GDPR compliance audit were achieved. Results of analysis of the satisfaction of the proposed framework with the security requirements are as follows:

- Data security: In the proposed framework, a transaction key was generated by automatically combining the DS's ID and timestamp in the chaincode when creating a request transaction, and the service provider URL of the DC and timestamp when creating a response transaction. The transaction was stored including the signature created by the private key of the creator. Furthermore, when searching for a stored transaction, the proposed framework compares the user's information (Uid, SPurl) with the stored transaction key in the chaincode. When the auditor desires to query the transaction of the DS and DC, the proposed framework checks whether the auditor has been granted the inquiry right by the DS and DC and that the authorization period is valid; then, the information (Uid, SPurl) of the approvers DS and DC is compared with the stored transaction key. The transactions are linked to each other using a hash algorithm in blocks, and their integrity is guaranteed due to it being copied and distributed to each peer in the BC network. The request and response contents that may contain sensitive personal data are encrypted and input by creating a symmetric key-type session key for each transaction in the application, and the session key is stored for each transaction in the application database. The creator, receiver, and auditor with inquiry authority can decrypt the data retrieved from the BC by inquiring the session key for each transaction. Thus, even if a transaction is exposed to an unauthorized peer in the BC network, the data cannot be decrypted unless the service is accessed through authentication in the proposed framework.
- Authentication and authorization: HLF provides Fabric CA as the default CA. Fabric CA is a public key infrastructure (PKI) based and used to generate X.509 digital certificates. All entities in the HLF must be identified by a digital ID before interacting with the BC network. An X.509 digital certificate contains key and related information of an entity and is either signed by the Fabric CA or self-signed. When implementing the proposed framework, we set the initialization value in the docker-compose-ca.yaml file and started Fabric CA using Docker. Furthermore, before interacting with the proposed framework, all entities were registered with the CA server using Fabric CA client or Fabric SDK and received the key and certificate. HLF provides an infrastructure management mechanism called "policy." Fabric policies represent the manner in which the members agree to accept or reject changes to a network, channel, or smart contract. We set policies in configtx.yaml to control all the actions each member desires to perform on the Fabric network. For example, although the DS and DC organizations allowed access to the transaction registration chaincode, the auditor group SA organization was allowed access only to the audit inquiry chaincode, while access to the notary group SA organization was not granted.
- Prevention of denial: In the proposed framework, transactions were created as blocks through the signature of the creator's private key, stored in the ledger, and shared in the BC network. In addition, by ensuring that the peers acting as the notary of the block are composed and operated only by SAs, the integrity and reliability of the stored data was increased to prevent the repudiation of notarized data.
- Accountability: In the proposed framework, request and response transactions were stored in the form of {who, when, who, what}. As the proposed framework inherits the integrity characteristics of BC, the data stored in the proposed framework can be used for GDPR compliance audits.

The proposed framework secures countermeasures against major cyberattack threats and major attack threats that may occur in BC-based systems, as shown in Table 4 by satisfying security and functional requirements.

Table 4. Countermeasure to the proposed framework for major cyberattacks on BC.

Attack	Description	Countermeasure
Race attack	Send two conflicting transactions in rapid succession.	Since it is different from cryptocurrency, multiple recipients who receive the same transaction will not be harmed if their own transaction is canceled.
Brute force attack	Attempt to decrypt any encrypted data.	Data are encrypted with an encryption algorithm recognized for stability that uses a key length of 256 bytes or more, such as AES-256. Brute force attacks on 256-byte keys are almost statistically impossible with current technology.
51% attack	After securing more than 50% of the hash computing power among all nodes, the transaction information is manipulated.	Authorizes only SAs as BC network nodes and controls malicious participants. It is possible that the proposed network is a private BC.
DoS (Denial-of-Service) attack	Sending massive amounts of traffic paralyzes BC networks and nodes.	Revokes access and authority of a party that mounts a DOS on the system since they are known identities rather than anonymous.
Unauthorized access attack	Access or modify a function or variable that should not be accessed.	Checks authentication and authority in web service and BC network. Respectively, manages authority for smart contract functions by the user group. Allows only own transaction to be accessed.
Replay attack	Copy a transaction that was added to the BC in the past and replay it in the network to distort its operation.	Users submitting a transaction with a transaction certificate should include in the transaction a random nonce, that would guarantee that two transactions do not result into the same hash.
Sniffing and capture attack	Monitoring and capturing all data packets passing through network.	TLS is used for all network sections. Encrypts the main data of the transaction based on the session key.

5.1.2. Function Analysis

The functions and properties of the proposed notarization framework were designed as per the design goal of Figure 5, and all the requirements of the notary framework for GDPR compliance audit were achieved. The proposed notarization framework receives a request for personal data processing from the DS, stores it in the ledger, notarizes it, and sends it to the DC by e-mail. In the event that the DC ignores, rejects, or delays the request without a good reason, it provides evidence to request legal sanctions, thereby guaranteeing the right of the DC to process their own data as defined in Chapters 12 to 21 of the GDPR. The proposed notarization framework assures an objective view on credibility by relaying and acting as a third party that notarizes requests and responses between the DS and DC and thus guarantees the reliability of records for GDPR compliance audits. In addition, the SPs need not modify the legacy personal data processing system or install a separate 3rd party module; thus, it is highly applicable to the actual environment. Table 5 shows the results of analysis of the satisfaction of the proposed framework with the requirements of Figure 5.

Table 5. Analysis result of meeting the requirements of the proposed framework.

A1	A2	A3	A4	B1	B2	B3	B4	B5	C1	D1
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Reasons for meeting each requirement of the proposed framework are as follows:

- Request and response anytime, anywhere (A1): The proposed framework was designed to delegate the DS's request and DC's response through the web service, notarize it in the BC network, and send it to the recipient through the e-mail service; thus, the DS and DC can make requests and responses anytime, anywhere. See Figure 6 in Section 3.4 and Figure 11 in Section 4.1.
- Save the information provided by electronic means (A2): The proposed framework stores all transactions related to personal data processing requests from DS and DC as electronic ledgers in BC. See Section 3.5 and Figure 11 in Section 4.1.
- Record of DS's request and of DC's response to DS's request (A3): The proposed framework stores all transactions related to personal data processing requests from DS and DC as electronic ledgers in BC. See Section 3.5 and Figure 11 in Section 4.1.
- Non-repudiation of requests and responses (A4): The DS and DC transmit the transaction together with the private key signature to the proposed framework, and the notary node of the proposed framework notarizes with the private key signature and stores it in BC, so the creator and notary cannot deny the stored data. See 'Prevention of denial' in Section 5.1.1.
- Sealing of data (B1): As the proposed framework is based on private BC, network participants can be managed. The proposed framework allows only the peers of the SA to participate in the network. Furthermore, the consensus procedure of HLF, which generates blocks after verification via multiple peers, has the function of notarization. Peers acting as notaries only include the signature generated by their private key in the transaction at the time of verification and do not cause any changes. Thus, the proposed framework using HLF's RAFT consensus algorithm meets the "sealing of data" requirement. See 'Data security' in Section 5.1.1.
- Accessible to all (B2): The proposed framework was designed to delegate the request of the DS and response of the DC through a web service and e-mail service. Both the DS and DC can access and use the framework after being authenticated and authorized by the CA. See Figure 11 in Section 4.1.
- Trusted or certifiable (B3): For the integrity and objective reliability of the ledger, the proposed framework restricts the nodes participating in notarization to authoritative organizations such as SAs. In the proposed framework, the algorithm that allows multiple notaries to participate and notarize inherits the RAFT algorithm of HLF, which has already been verified for stability.
- Highly trusted communications (B4): As the proposed framework uses HLF, a private BC framework, it inherits the integrity and confidentiality of the HLF's system, network, and data. HLF supports secure communication between nodes by using transport layer security (TLS) protocol, which is applied in the proposed framework.
- Authentication (B5): The proposed framework authenticates all entities using Fabric CA, which is a CA provided by HLF. See 'Authentication and Authorization' in Section 5.1.1.
- Data minimization (C1): The proposed framework only stores information for auditing the processing request transaction of the DS and DC's response to the request in the BC for the GDPR compliance audit, and it does not store any other personal data that the SPs have. See Section 3.5.
- Feasibility in real environment (D1): As the proposed framework was designed to delegate the DS's request and DC's response through a web service and an e-mail service, the SPs need not modify the legacy personal information processing system or install a separate third party module. Therefore, it can be applied as a GDPR compliance audit framework in a real environment.

5.2. Performance Evaluation

To evaluate the performance of the proposed framework, we installed Docker on Intel Core i5-8265U CPU @ 1.60 GHz, with 16 GB RAM specification system, and applied the two-peer three-order, and Raft consensus algorithm to configure and simulate the HLF network. In the performance evaluation of the proposed framework, the main issue area was found to be the BC area.

The performance of BC solutions is one of the characteristics that BC users are most concerned about. However, due to the diversity of consensus mechanisms and APIs, existing performance benchmarking frameworks cannot be directly applied to distributed ledger systems, making it very important to devise solutions to compare different platforms in a meaningful way. In order to perform and analyze the performance measurement in the BC area of the proposed framework on a consistent and systematic basis, this work used 'Hyperledger Caliper' (hereinafter referred to as 'Caliper'), which is a performance measurement framework optimized for the HLF BC environment. Caliper is a BC benchmark tool that allows users to measure the performance of a BC implementation with a predefined set of use cases. Caliper generates a report containing several performance indicators such as transaction per second (tps), transaction latency (latency), and resource utilization [45]. In this work, the performance of the proposed framework was measured by automatically generating loads by setting various use case sets of Caliper.

We increased the load from 50 to 300 tps by automatically creating a transaction and transferred it to the smart contract of the proposed framework. Furthermore, the processing result data of the proposed framework for the input data were measured, and the write and read throughput rates of the proposed framework in the BC area were analyzed. In addition, the proposed framework was designed on the basis of the assumption that SAs in various countries subject to GDPR configure peers and perform notarization; thus, performance analysis is required according to node expansion. We increased the number of peers from two to six and measured and analyzed the write and read throughput rates. This performance test was repeated five times in total, and the results were averaged. Figures 13 and 14 shows the results of analyzing the write and read throughput of the framework proposed in the BC area according to the change in the number of peers.

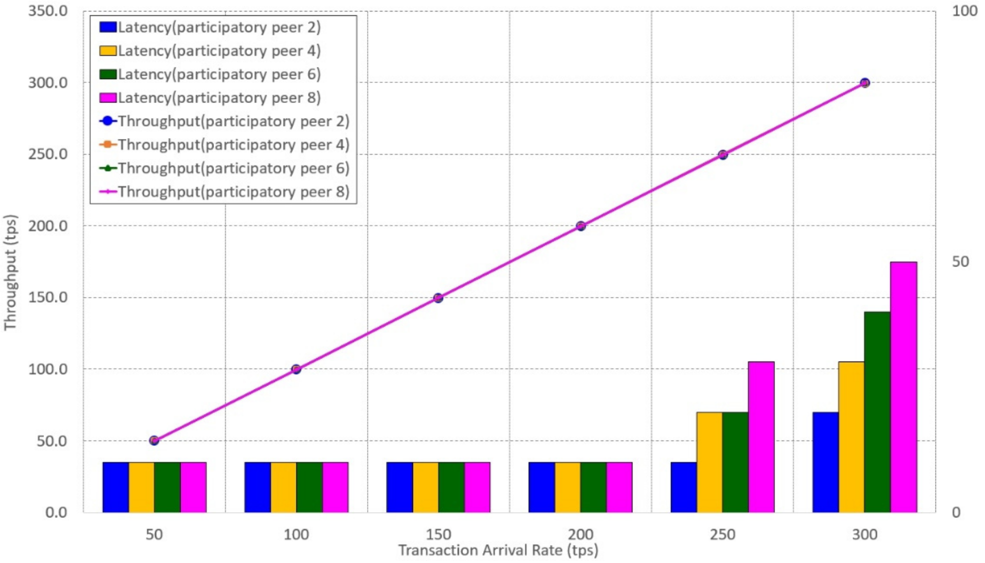


Figure 13. Performance of read in BC of proposed framework under different workloads and different number of peers.

It was confirmed that the read delay of the proposed framework increases from the peer over two peers, 250 tps area, and the write throughput is significantly reduced from the 200 tps area. Simultaneously, in the simulation, we set 50 users to continuously generate transactions. However, considering the service characteristics of the proposed framework, it is rare for users to continuously generate personal data processing requests. Moreover, considering that it is a simulation environment using Docker and there are limitations of computing resources such as CPU and memory, the performance is expected to be further improved in the actual implementation environment. In addition, considering the trade-off between security and performance according to scalability in a distributed environment, the performance decreases when nodes are increased, but security becomes stronger.

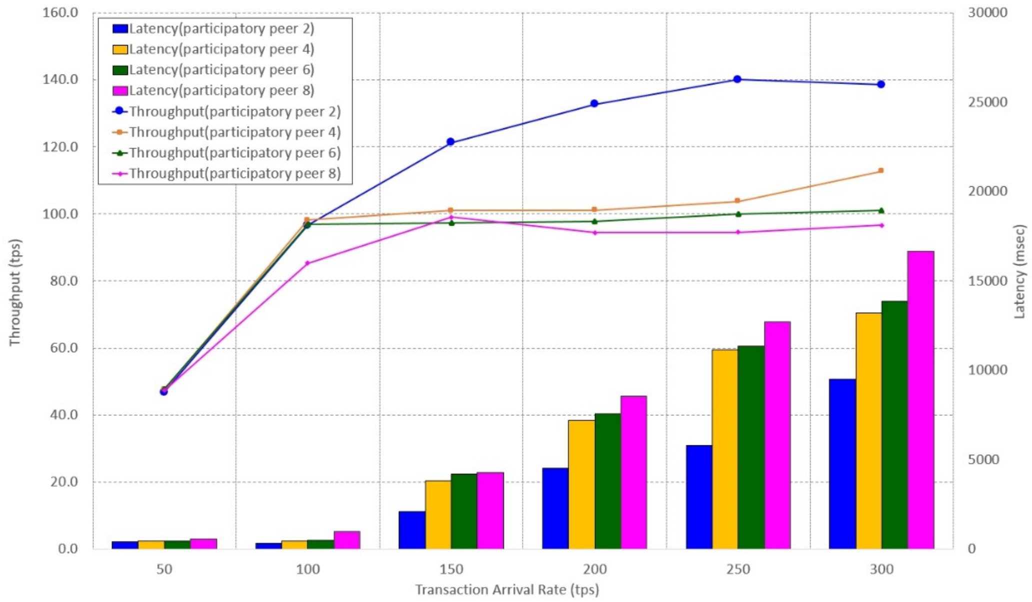


Figure 14. Performance of write in BC of proposed framework under different workloads and different number of peers.

5.3. Comparative Analysis of Related Works

The proposed delegation-based personal data processing notarization framework was designed to support the requirements of “reliable notarization of request for the processing of personal data that can be easily used without sharing personal data and processed in real time.” The framework was compared with the related works, which could confirm that the reliability and excellence of the framework are satisfied.

We compared and analyzed the superiority of the proposed framework, focusing on the work of Truong et al. that includes issues on data processing requests among works related to BC-based GDPR compliance. Table 6 presents the results of analyzing whether the functions and properties of the framework proposed by Truong et al. meet the requirements in Figure 5.

Table 6. Analysis result of meeting the requirements of the platform proposed by Truong et al.

A1	A2	A3	A4	B1	B2	B3	B4	B5	C1	D1
Y	Y	*N*	Y	*N*	Y	*N*	Y	Y	*N*	*N*

From the analysis results shown in Table 6, it is evident that the functions and properties of the framework proposed by Truong et al. did not meet requirements, which are as follows:

- Record of DS’s request and of DC’s response to DS’s request (A3): For an end user to request data processing to a resource server with personal data, the SP’s system is the only means to achieve it. However, this has the potential to allow the SP in the middle to ignore or manipulate the end user’s request. In addition, the proposed framework was designed around access control, such that although the access request for personal data processing is stored in the block chain before processing, the personal data processing is not stored until the resource server processes it. Furthermore, it is not designed to store the request contents of the DS because the scenario wherein the DS requests the SP to process it is not considered.

- Sealing of data (B1): It is possible for an end user to request data processing to a resource server with personal data only through the SP's system. However, this has the potential to allow the SP in the middle to manipulate the end user's request. Furthermore, as the proposed framework has been designed around access control, thus, the sealing and notarization process for end-user requests is not clearly presented.
- Trusted or certifiable (B3): It was assumed that a DS is "honest-but-curious", whereas SPs follow a malicious model. This indicates that the DS executes the required protocols, even though it might be curious about the results it receives after the operations. Most of the records of the processing of personal data are stored in the proposal framework by the resource server; however, if the resource server is not trusted, the data also cannot be trusted.
- Data minimization (C1): The proposed framework stores all personal data processing history of the SP. When the DS subscribes to the service of the SP, it delegates the processing of personal data to the SP. Therefore, owing to the excessive nature amount, all personal data processing of the SP delegated by DS for GDPR compliance audit and personal data related to personal data processing is also stored. Furthermore, considering the characteristics of the BC where data are replicated, distributed, and stored, and deletion is not easy, the more personal data are stored, the greater the risk of exposure and the greater the possibility of violating the principle of data minimization.
- Feasibility in real environment (D1): To apply the proposed framework, SPs must modify the legacy personal data processing system or install a separate third-party module. However, the application of the proposed framework to the real environment is difficult because enforcing it on all SPs in the real environment is a challenge.

The solution of Truong et al. is insufficient compared to the proposed framework when considering that there is no guarantee of an objective view on the credibility of the DS's request for the processing of personal data, it does not comply with the GDPR principle, and it could not directly apply to a real environment situation. The framework proposed by Truong et al. was not designed to store the personal data processing request of the DS without going through the SP. Moreover, if the SP does not add functions to the legacy personal data processing system to interface with the platform proposed by Truong et al., the problem for GDPR compliance audits remains unsolved. Thus, considering that in real situations, it is not possible to apply the platform proposed by Truong et al. to all SPs, it can be concluded that it is not an appropriate solution to the problem of GDPR compliance audit to ensure the right to request processing of personal data of DS.

Therefore, the proposed framework is superior in terms of the objective reliability of personal data processing requests, compliance with GDPR principles, and feasibility compared to solutions of previous works that allow the SP to manage the personal data processing request record of DS as in the work of Truong et al. Table 7 shows the comparative analysis results of the proposed framework and the platform proposed by Truong et al.

Table 7. Comparative analysis between this work and the work of Truong et al.

Work	A1	A2	A3	A4	B1	B2	B3	B4	B5	C1	D1
Proposed	Y	Y	**Y**	Y	**Y**	Y	*N*	Y	Y	**Y**	**Y**
Truong et al.	Y	Y	*N*	Y	*N*	Y	*N*	Y	Y	*N*	*N*

6. Conclusions

This study proposed a delegation-based personal data processing notarization framework based on a private BC to solve the problem of requiring an objective view on the credibility of records related to personal data processing requests. Furthermore, it could support the claim of the rights of DSs in a GDPR compliance audit. It can be easily used by users through the web, does not share personal data collected by DCs, adheres to the basic principles of GDPR, and is feasible. Furthermore, through the process of notarization, it is possible to secure the trust of all network participants with respect to records of the personal data processing request and response, and thus, it can be used for GDPR compliance audit. The management of the personal data processing requests in the proposed framework from the perspective of the DS and the objective view on credibility were guaranteed, thereby further strengthening the guarantee of rights of DS. Furthermore, the simulation results and subsequent analysis demonstrated that the proposed framework satisfied the functional and security requirements for a notarization system capable of GDPR compliance audit for personal data processing.

If an institution authorized by a government operates the notarization framework proposed in this paper, the reliability of the authentication and authorization of system users, including notaries, is increased, and thus, the reliability of notarization provided by the system is expected to be further increased. If the SA recommends that SPs who do not disclose the email address of the person in charge of personal data processing on the website, etc., sign up for a service using the proposed framework and disclose their email address, it is expected that the GDPR compliance for personal data processing requests will be spread just by registering as a member without forcing the SP to install an additional system. In addition, if an e-mail server of the proposed framework and the system linkage module of DC are developed and applied, DC can also delegate and notarize the notification sent to DS more easily.

For future research, studies need to be undertaken to guarantee the sovereignty of DS for personal data regarding GDPR compliance other than compliance with personal data processing, and research on notarization methods for a BC-based GDPR compliance audit is required to ensure that it does not violate GDPR regulations.

Author Contributions: Conceptualization, S.-S.J.; methodology, S.-S.J.; software, S.-S.J.; validation, S.-S.J., S.-J.L. and I.-C.E.; formal analysis, S.-S.J. and I.-C.E.; investigation, S.-S.J.; resources, S.-S.J.; data curation, S.-S.J.; writing—original draft preparation, S.-S.J.; writing—review and editing, S.-S.J., S.-J.L. and I.-C.E.; visualization, S.-S.J.; supervision, I.-C.E.; project administration, I.-C.E.; funding acquisition, I.-C.E. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by Institute for Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) under grant no. 2019-0-01343, regional strategic industry convergence security core talent training business.

Acknowledgments: The manuscript will be used as part of the author's doctoral dissertation.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Farahani, B.; Firouzi, F.; Luecking, M. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *J. Netw. Comput. Appl.* **2021**, *177*, 102936. [CrossRef]
2. Sellami, M.; Mezni, H.; Hacid, S. On the use of big data frameworks for big service composition. *J. Netw. Comput. Appl.* **2020**, *166*, 102732. [CrossRef]
3. Campanile, L.; Iacoco, M.; Marulli, F.; Mastroianni, M. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Inf. Process. Manag.* **2021**, *58*, 102511. [CrossRef]
4. Tamburri, D.A. Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. *Inf. Syst.* **2020**, *91*, 101469. [CrossRef]
5. Yang, X. Business big data analysis based on microprocessor system and mathematical modeling. *Microprocess. Microsyst.* **2021**, *82*, 103846. [CrossRef]
6. Bhattacharya, M.; Islam, R.; Abawajy, J. Evolutionary optimization: A big data perspective. *J. Netw. Comput. Appl.* **2016**, *59*, 416–426. [CrossRef]
7. Singh, A.; Click, K.; Parizi, R.M.; Zhang, Q.; Dehghantanha, A.; Choo, K.R. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *J. Netw. Comput. Appl.* **2020**, *149*, 102471. [CrossRef]
8. Parra Freund, G.; Fagundes, P.B.; Macedo, D.D.J. An analysis of blockchain and GDPR under the data lifecycle perspective. *Mob. Netw. Appl.* **2020**, *26*, 266–276. [CrossRef]

9. Eugenia, P.; Efthimios, A.; Constantinos, P. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *J. Cybersecur.* **2018**, *4*, 1–20.
10. Korea Legislation Research Institute. Personal Information Protection Act. Act No. 16930. 2020. Available online: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG (accessed on 29 May 2021).
11. European Union. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Available online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046 (accessed on 29 May 2021).
12. ICLG. USA: Data Protection Laws and Regulations. 2020. Available online: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (accessed on 29 May 2021).
13. Gobeo, A.; Fowler, C.; Buchanan, W.J. 4 Cyber Security and the GDPR. In *GDPR and Cyber Security for Business Information Systems*; River Publishers: Gistrup, Denmark, 2018; pp. 93–116.
14. Greenleaf, G. Global data privacy laws 2019: 132 national laws & many bills. *Priv. Laws Bus. Int. Rep.* **2019**, *157*, 14–18.
15. Team, I.P. *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*; IT Governance Ltd.: Ely, UK, 2017.
16. Cimina, V. The data protection concepts of 'controller', 'processor' and 'joint controllership' under Regulation (EU) 2018/1725. *ERA Forum* **2021**, *21*, 639–654. [CrossRef]
17. Wirth, C.; Kolain, M. Privacy by blockchain design: A blockchain enabled GDPR-compliant approach for handling personal data. In Proceedings of the 1st ERCIM Blockchain Workshop 2018, European Society for Socially Embedded Technologies (EUSSET), Amsterdam, The Netherlands, 8 May 2018.
18. Bernabe, J.B.; Canovas, J.L.; Hernandez-Ramos, J.L.; Moreno, R.T.; Skarmeta, A. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access* **2019**, *7*, 164922–164923. [CrossRef]
19. Sutton, A.; Samavi, R. Blockchain Enabled Privacy Audit Logs. In Proceedings of the International Semantic Web Conference, Vienna, Austria, 21–25 October 2017; pp. 645–660.
20. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
21. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 18–20 May 2015; pp. 180–184.
22. Hillmann, P.; Knupfer, M.; Heiland, E.; Karcher, A. Selective Deletion in a Blockchain. In Proceedings of the International Workshop on Blockchain and Mobile Applications (BlockApp 2020) during the International Conference on Distributed Computing Systems (ICDCS 2020), Singapore, 29 November–1 December 2020.
23. Tatar, U.; Gokce, Y.; Nussbaum, B. Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Comput. Law Secur. Rev.* **2020**, *38*, 105454. [CrossRef]
24. Carvalho, R.M.; Prete, C.D.; Martin, Y.S.; Rivero, R.M.A.; Onen, M.; Schiavo, F.P.; Rumin, A.C.; Mouratidis, H.; Yelmo, J.C.; Koukovini, M.N. Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects. *SN Comput. Sci.* **2020**, *1*, 217. [CrossRef]
25. Zheng, Z.; Xie, S.; Dai, H.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
26. Rieger, A.; Guggenmos, F.; Lockl, J.; Fridgen, G.; Urbach, N. Building a Blockchain Application that Complies with the EU General Data Protection Regulation. *MIS Q. Exec.* **2019**, *18*, 263–279. [CrossRef]
27. Hewa, T.; Ylianttila, M.; Liyangage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl.* **2021**, *177*, 102857. [CrossRef]
28. Asaf, K.; Rehman, R.A.; Kim, B.S. Blockchain technology in Named Data Networks: A detailed survey. *J. Netw. Comput. Appl.* **2020**, *171*, 102840. [CrossRef]
29. Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L. ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. In Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Madrid, Spain, 14–17 May 2017; pp. 468–477.
30. Yan, Z.; Gan, G.; Riad, K. BC-PDS: Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS. In Proceedings of the 2017 IEEE Symposium on Service-Oriented System Engineering, San Francisco, CA, USA, 6–9 April 2017; pp. 138–144.
31. Chowdhury, M.J.M.; Colman, A.; Kabir, M.A.; Han, J.; Sarda, P. Blockchain as a Notarization Service for Data Sharing with Personal Data Store. In Proceedings of the 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), New York, NY, USA, 1–3 August 2018; pp. 1330–1335.
32. Agarwal, S.; Steyskal, S.; Antunovic, F.; Kirrane, S. Legislative Compliance Assessment: Framework, Model and GDPR Instantiation. In *Annual Privacy Forum*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 131–149.
33. Truong, N.B.; Sun, K.; Guo, Y. Blockchain-Based Personal Data Management: From Fiction to Solution. In Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 26–28 September 2019; pp. 1–8.
34. Truong, N.B.; Lee, G.M.; Lee, G.M.; Guo, Y. GDPR-Compliant Personal Data Management: A Blockchain-based Solution. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1746–1761. [CrossRef]

35. Vargas, J.C. Blockchain-Based Consent Manager for GDPR Compliance. In *Open Identity Summit*; Gesellschaft für Informatik: Bonn, Germany, 2019; pp. 165–170.
36. Kassem, J.A.; Sayeed, S.; Marco-Gisbert, H.; Pervez, Z.; Dahal, K. DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. *Appl. Sci.* **2019**, *9*, 2953. [CrossRef]
37. Rantos, K.; Drosatos, G.; Demertzis, K.; Ilioudis, C.; Papanikolaou, A.; Kritsas, A. ADvoCATE: A consent management platform for personal data processing in the iot using blockchain technology. In Proceedings of the International Conference on Security for Information Technology and Communications (SecITC), Bucharest, Romania, 8–9 November 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 300–313.
38. Faber, B.; Michelet, G.; Weidmann, N.; Mukkamala, R.R.; Vatrapu, R. BPDIMS: A blockchain-based personal data and identity management system. *Int. Conf. Syst. Sci.* **2019**, *45*, 254–264.
39. Piras, L. DEFeND architecture: A Privacy by Design Platform for GDPR Compliance. In Proceedings of the 16th International Conference on Trust and Privacy in Digital Business (TrustBus), Linz, Austria, 26–29 August 2019; pp. 78–93.
40. Mahindrakar, A.; Joshi, K.P. Automating GDPR Compliance using Policy Integrated Blockchain. In Proceedings of the 2020 IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 25–27 May 2020; pp. 86–93.
41. Casaleiro, R. Protection and control of personal identifiable information: The PoSeID-on approach. *J. Data Prot. Priv.* **2020**, *3*, 199–228.
42. Daudén-Esmel, C.; Castellà-Roca, J.; Viejo, A.; Domingo-Ferrer, J. Lightweight Blockchain-based Platform for GDPR-Compliant Personal Data Management. In Proceedings of the 5th International Conference on Cryptography, Security and Privacy, Zhuhai, China, 4 May 2021; pp. 68–73.
43. Haque, A.B.; Islam, A.N.; Hyrynsalmi, S.; Naqvi, B.; Smolander, K. GDPR Compliant Blockchains—A Systematic Literature Review. *IEEE Access* **2021**, *9*, 50593–50606. [CrossRef]
44. Low, M.R. *The Notary, University of Hertfordshire Computer Science Technical Report*; University of Hertfordshire: Hertfordshire, UK, 1992; Volume 153, pp. 2–5.
45. Hyperledger Caliper Project. Hyperledger Caliper. Available online: https://www.hyperledger.org/projects/caliper (accessed on 30 October 2021).