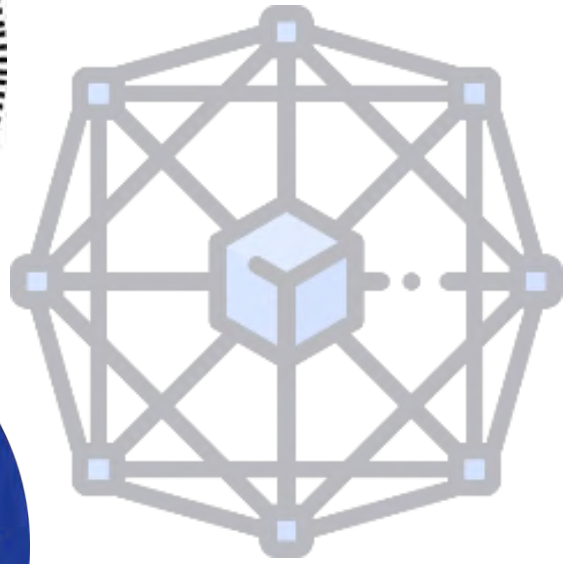
전남대학교
CHONNAM NATIONAL UNIVERSITY

폐쇄형 블록체인 기반 GDPR 개인정보처리 요청 공증 프레임워크

(Private Blockchain based
GDPR Personal Data Processing Request Notarization Framework)



정 성 수

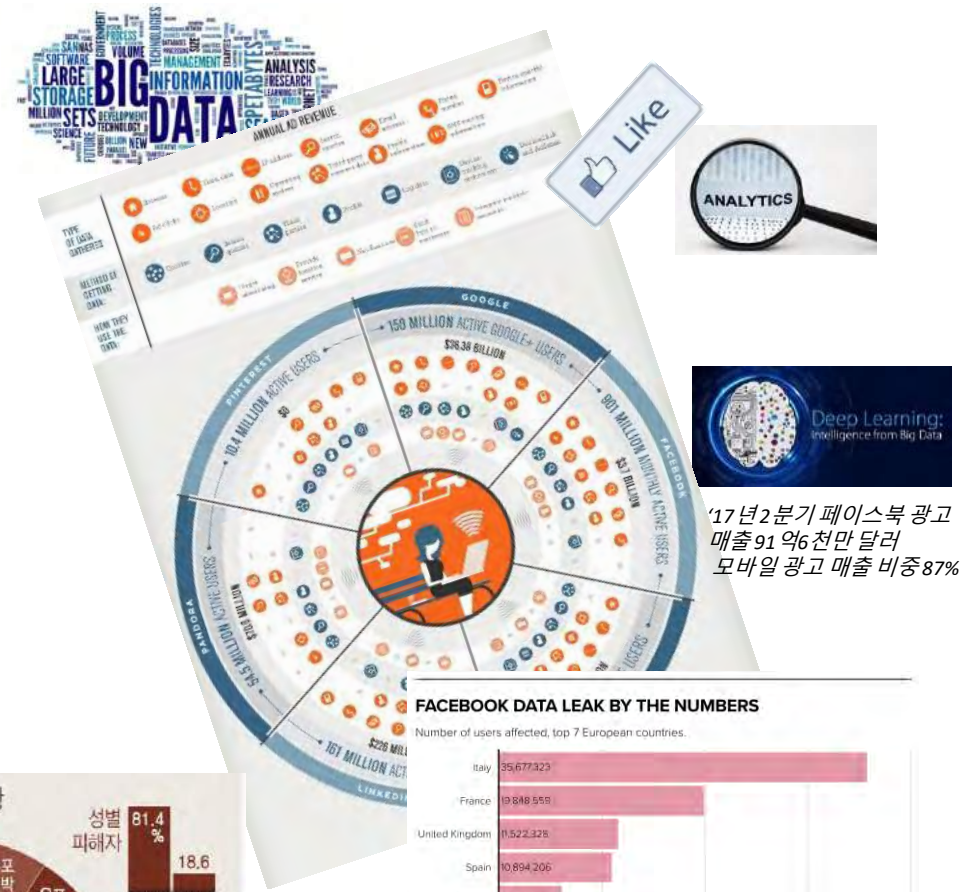
전남대학교 대학원
정보보안협동과정 박사과정

Outline

- 연구 배경
- 관련 연구 분석
- 연구 목표 및 주요 기여내용
- 개인정보처리 요청 공증 프레임워크 요구사항 분석
- 폐쇄형 블록체인 기반 GDPR 개인정보처리 요청 공증 프레임워크
- 구현 및 분석
- 결론 및 향후 일정
- 연구성과

개인정보보호

- '개인정보'란 식별되었거나 또는 식별 가능한 자연인(정보주체)과 관련된 모든 정보 (제4조 1항)
- 빅데이터, AI 기술 발전과 함께 기업의 새로운 자산으로 인식됨
- 개인정보 유출 등의 피해 우려 증가
- 삭제요청 같은 개인정보처리 요청에 대한 정보주체 권한 강화 필요



'17년2분기 페이스북 광고 매출91억6천만 달러
모바일 광고 매출 비중87%

(그림출처 : www.politico.eu/)

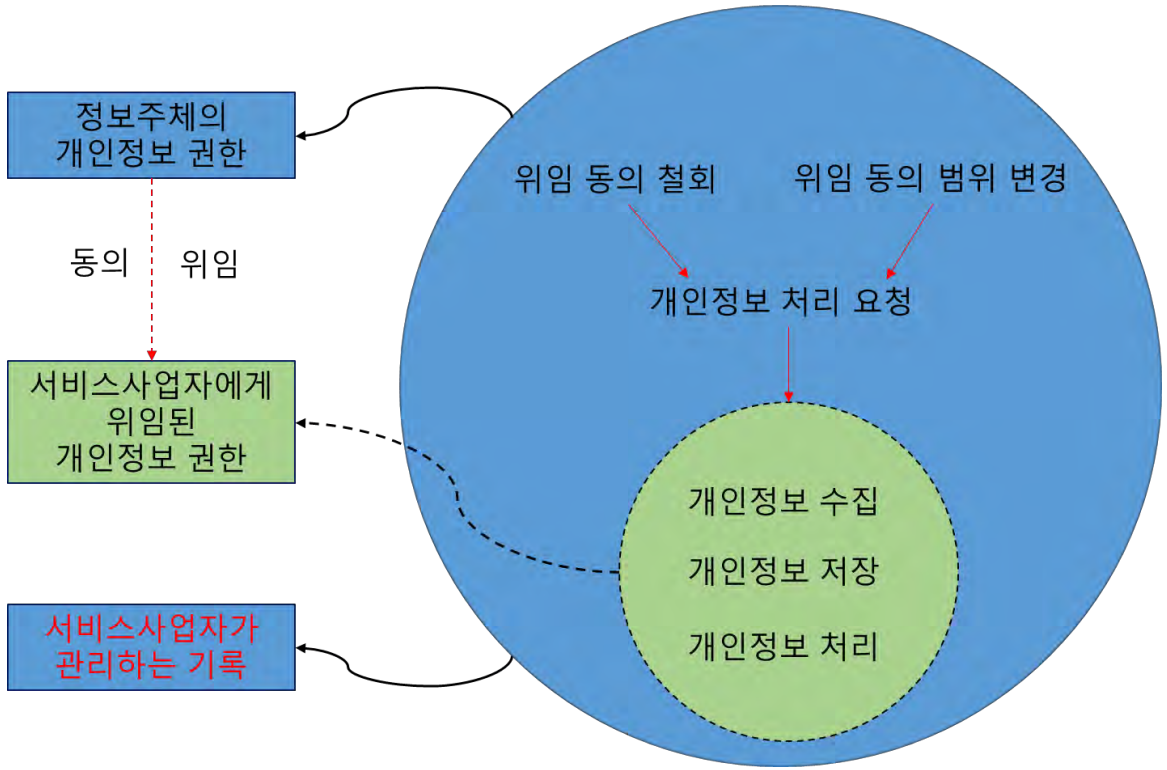
GDPR

- 대부분의 국가가 개인정보보호 관련 법규를 강화하고 있음
- 2018년 5월 시행 유럽연합의 일반 개인정보보호법(General Data Protection Regulation)
- 목적
  - 정보주체 권한 강화
  - 회사들의 책임강화
  - 개인정보 EU 역외 전송 요구사항 명확화
- 적용 범위
  - EU내 설립된 기관
  - EU 밖에서 EU내 정부주체에게 재화나 용역을 제공하는 경우
  - EU 내 정보주체가 수행하는 활동을 모니터링 하는 기관

(그림출처 : www.kisa.org/)

정보주체의 권리

- 자신의 개인정보에 대한 모든 권리
- 서비스 사업자에게 일부 권한 위임
- 서비스 사업자 GDPR 준법 증명 의무
- 위임 외 권한
  - 위임 동의 철회
  - 위임 동의 변경
  - 개인정보처리(조회/수정/처리중지/이동 /삭제-잊혀질 권리 등) 요청할 권리
  - 서비스 사업자 요청에 지체 없이 대응 의무



개인정보처리 요청 관련 GDPR 규정 및 GDPR 원칙

GRPR	핵심내용
제12조 개인정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식	◆ DC는 제15조부터 제22조까지에 따른 권리 행사를 위한 DS의 요청에 대한 조치를 거부해선 안 됨. ◆ DS가 전자적 수단으로 요청하는 경우, DS가 달리 요청하지 않는 한 가능한 한 전자적 수단으로 정보를 제공해야 함.
제15조 정보주체의 열람권	◆ DS는 DC로부터 자신에 관한 개인 데이터가 처리되고 있는지 여부와 그러한 경우 GDPR에 정의된 대로 개인 데이터 및 정보에 대한 액세스 권한을 얻을 권리가 있음. ◆ DC는 처리 중인 개인정보의 사본을 제공하여야 함.
제16조 정정권	◆ DS는 부당한 지체 없이 DC로부터 자신에 관한 부정확한 개인 정보의 수정을 받을 권리가 있음. ◆ DC는 잘못된 개인 데이터의 수정 요청에 대해 부당한 지체 없이 조치를 취해야 함.
제17조 삭제권('잊혀질 권리')	◆ DS는 과도한 지연 없이 DC로부터 자신에 대한 개인정보를 삭제할 권리가 있음. ◆ DC는 GDPR에 명시된 이유 중 하나라도 해당되는 경우 부당한 지연 없이 개인 데이터를 삭제할 의무가 있음.
제18조 처리에 대한 제한권	◆ DS는 GDPR에 명시된 이유 중 하나라도 적용되는 경우 DC로부터 처리 제한을 받을 권리가 있음. ◆ DC는 개인 데이터 처리 제한 요청에 대해 부당한 지체 없이 조치를 취해야 함.
제19조 개인정보의 정정이나 삭제 또는 처리의 제한에 관한 고지 의무	◆ DC는 16조, 17조 1항 및 18조에 따라 수행된 개인 데이터의 수정 또는 삭제 또는 처리 제한을 개인 데이터가 공개된 각 수신자에게 전달해야 함. ◆ DC는 DS가 요청하는 경우 해당 수신자에 대해 DS에 알려야 함.
제20조 개인정보 이전권	◆ DS는 개인 데이터가 제공된 DC의 방해 없이 해당 데이터를 다른 DC로 전송할 권리가 있음. ◆ DS는 기술적으로 가능한 경우 한 DC에서 다른 DC로 개인 데이터를 직접 전송할 권리가 있음. ◆ DC는 개인 데이터 전송 요청에 대해 부당한 지체 없이 조치를 취해야 함.
제21조 반대할 권리	◆ DS는 해당 조항을 기반으로 한 프로파일링을 포함하여 제6조(1)의 (e) 또는 (f)를 기반으로 한 개인 데이터 처리에 대해 언제든지 자신의 특정 상황과 관련된 이유로 이의를 제기할 권리가 있음. ◆ DC는 DC가 DS의 이익, 권리 및 자유를 무시하는 처리 또는 법적 청구의 설정, 행사 또는 방어를 위한 설득력 있는 정당한 근거를 입증하지 않는 한 더 이상 개인 데이터를 처리하지 않음.

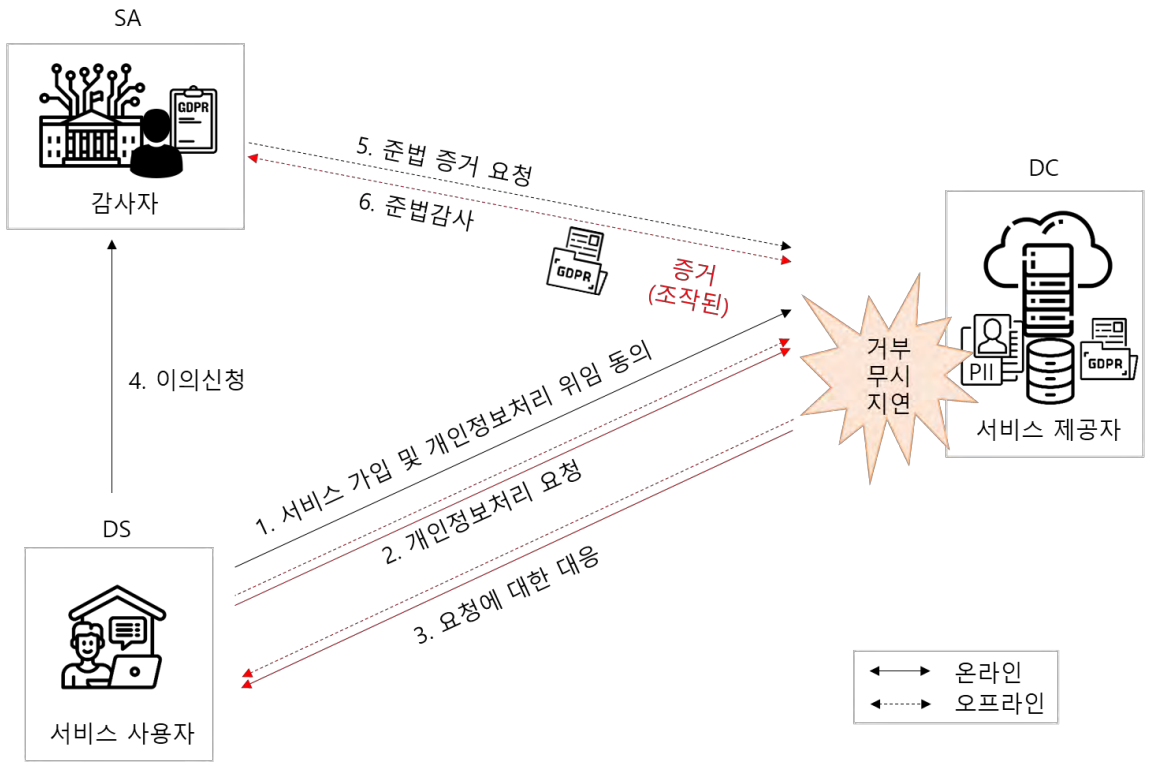
제 5조 개인정보처리 관련 GDPR 원칙
합법성
공정성
투명성
목적제한
데이터 최소화
정확성
저장 한정
무결성
기밀성
책임성

GDPR 준법 감사

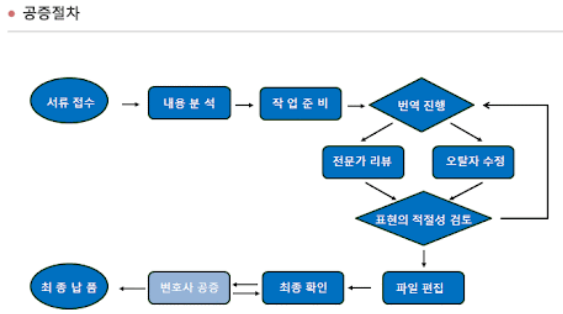
- 준법 감사를 위한 주요 역할
  - **정보 주체 (Data Subject, DS)** : 개인정보의 소유자 감독기관에 개인정보 처리에 관하여 모든 권리를 갖고 있음. 개인정보 관련하여 서비스 사업자에 대한 이의 신청을 하고 GDPR 준법 감사를 요청할 수 있음
  - **서비스 사업자(Service Provider, SP)** : 개인정보를 수집 관리하여 서비스를 제공하는 기관. GDPR 준법 기록을 관리하고 법적 증빙 자료를 마련하여야 함. 정보주체 및 감독 기관이 요청하면 제시하여야 함
  - **개인정보처리자 (Data Controller, DC)** : 서비스 사업자의 개인정보 관리자. 개인정보 처리의 목적 및 방법을 결정하며, 데이터 주체의 개인정보가 적법하고, 공정하며, 투명하게 처리되도록 관리 및 입증할 책임을 가짐
  - **감독기관 (Supervisory Authority, SA)** : GDPR 준법 감사를 실시하는 기관으로서 정기적으로 서비스 사업자의 GDPR 규정 준수 여부를 감독하는 법적 권한을 가진 독립적인 공공기관

GDPR 준법 감사 (문제점)

- 개인정보처리 요청의 기록을 서비스 사업자가 관리 -> 기록 훼손 가능, 신뢰성 상실
- 오프라인 공증 어렵고 시간 소요되며, 국가간 증빙 효력 인정 기준 다름
- 정보주체 개인정보처리 요청 권리 보장 안됨



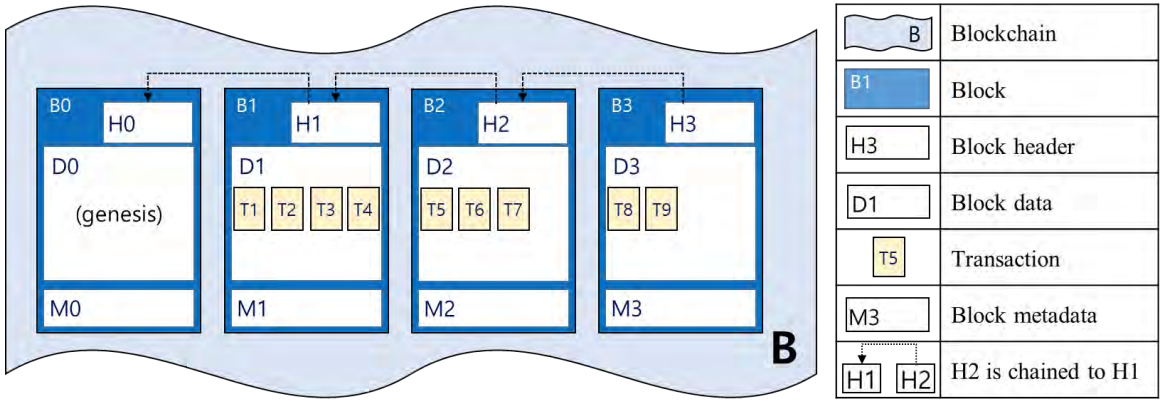
(그림출처 : www.joongang.co.kr)

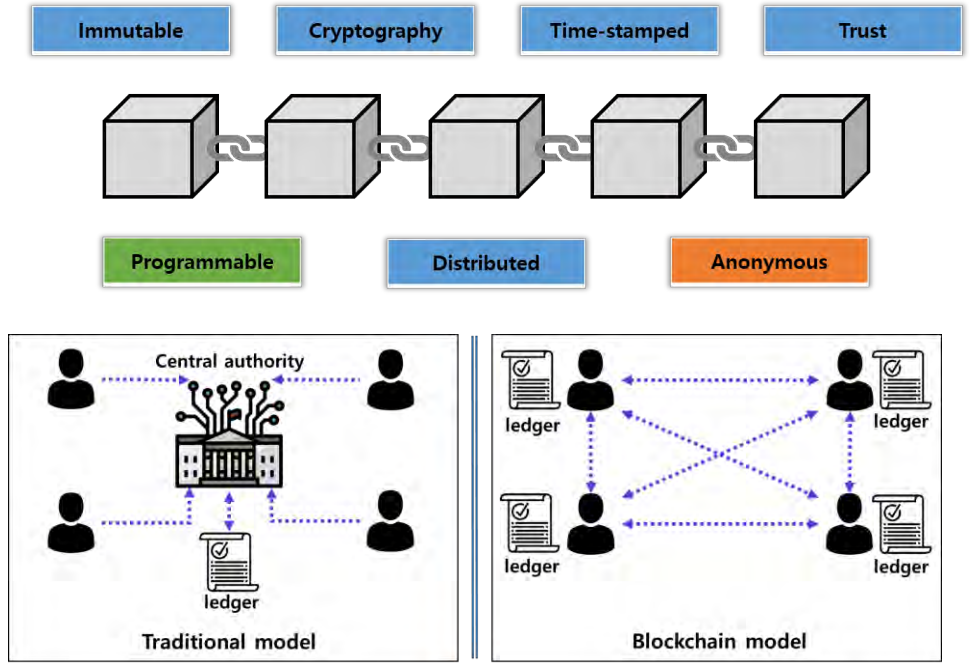


(그림출처 : totaltrans.kr/)

블록체인?

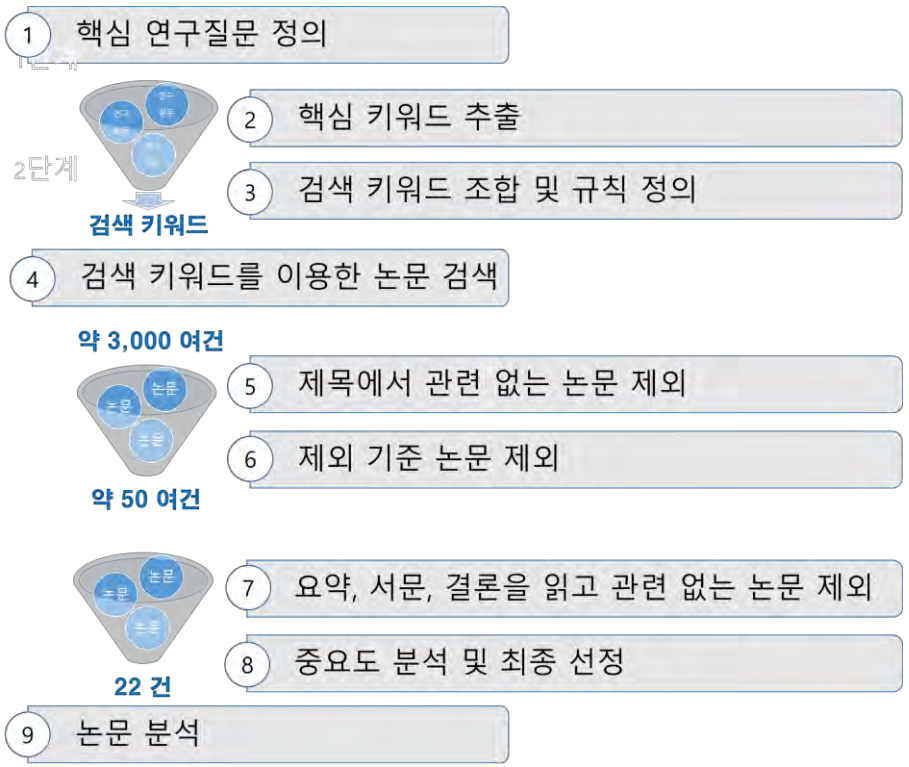
- 데이터를 체인 형태 연결고리를 가지는 블록 형태로 단대단(Peer to peer) 네트워크 노드들에 분산 저장, 검증하는 기술
- 분산성, 무결성, 익명성, 감사가능성 등으로 준법관리에 좋음
- 데이터 삭제, 수정 어려움 (GDPR 준법 위배)





관련 연구 선정 방법

- 체계적 문헌 검토(Systematic Literature Review, SLR) 접근 방법



번호	논문 제목	연도	출판유형
E01	Provchain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability [35]	2017	컨퍼런스
E02	BC-FDS: Protecting Privacy and Self-Sovereignty through BlockChains for OpenFDS [36]	2017	컨퍼런스
E03	Blockchain as a Notarization Service for Data Sharing with Personal Data Store [37]	2018	컨퍼런스
E04	Legislative Compliance Assessment: Framework, Model and GDPR Instantiation [38]	2018	저널
E05	Blockchain-based Personal Data Management: From Fiction to Solution [31]	2019	저널
E06	GDPR-Compliant Personal Data Management: A Blockchain-based Solution [39]	2019	저널
E07	Blockchain-based consent manager for GDPR compliance [40]	2019	컨퍼런스
E08	DLIS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network [41]	2019	저널
E09	ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology [42]	2019	저널
E10	BPDIMS: A blockchain-based personal data and identity management system [43]	2019	컨퍼런스
E11	DEFeIID Architecture: a Privacy by Design Platform for GDPR Compliance [44]	2019	컨퍼런스
E12	Automating GDPR Compliance using Policy Integrated Blockchain [45]	2020	컨퍼런스
E13	Protection and control of personal identifiable information: The PoSeID-on approach [46]	2020	저널
E14	Lightweight Blockchain-based Platform for GDPR-Compliant Personal Data Management [47]	2021	컨퍼런스

총 22개논문 :리뷰 4개, 해외 14, 국내 4개

연구 분야	관련 연구
연구 동향	R01, R02, R03, R04
데이터 출처	E01
접근 제어	E05, E06, K01, K02, K04
공증	E02, E03, E09
신원 관리	E08, E10
준법 평가	E04, E12
동의 관리	E07, E09, E14, K03
GDPR 준법관리	E06, E07, E11, E13, K01, K02

연구동향 1

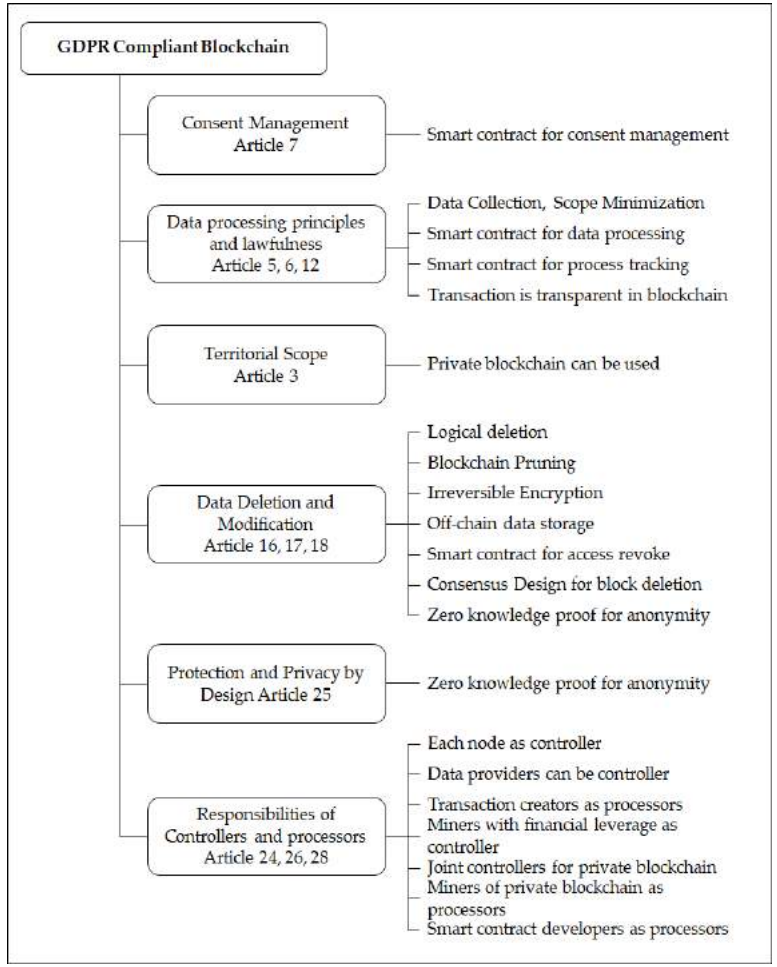
- 블록체인 기술 관련 암호화 기술과 자주적 신원관리 연구
  - GDPR 고려 부족
- GDPR 이행 촉진 위해 EU에서 GDPR 솔루션 프로젝트 지원
  - BPR4GDPR : GDPR 준수를 위한 비즈니스 프로세스 리엔지니어링 및 기능적 툴킷
  - DEFeND : GDPR 지원을 위한 데이터 거버넌스
  - SMOOTH : 소기업을 위한 GDPR 규정 준수 클라우드 플랫폼
  - PDP4E : 개인정보보호 및 데이터 보호 엔지니어링을 통한 GDPR 준수 방법 및 도구
  - PAPAYA : 보호된 개인정보를 위한 분석 플랫폼
  - PoSeID-on : 개인정보보호 강화 대시보드를 통한 안전한 정보 보호 및 제어
  - GDPR을 위한 다양한 도전과제를 다루지만 여전히 다루지 않는 영역 존재
  - 솔루션 자체 보안성 충족하는 기술적 측면의 설계 및 구현 제시 안됨

연구동향 2

- 블록체인 기반 동의 관리 연구
  - 아이디어 차원 연구, 실질적 구현 제시 부족
- GDPR 준법 블록체인
  - GDPR에 블록체인 적용하면 GDPR 원칙 위배 위험이 발생하는 역설을 해결하기 위한 연구
  - GDPR의 다양한 요구사항에 대한 충족 방안 연구
  - 하지만 여전히 다루지 않는 영역 존재
  - 실질적 구현 방안 제시 연구 부족
  - GDPR 준법 블록체인이 비교적 새로운 연구이며 미래에 탐구할 수 있는 몇 가지 주요 연구 격차 존재

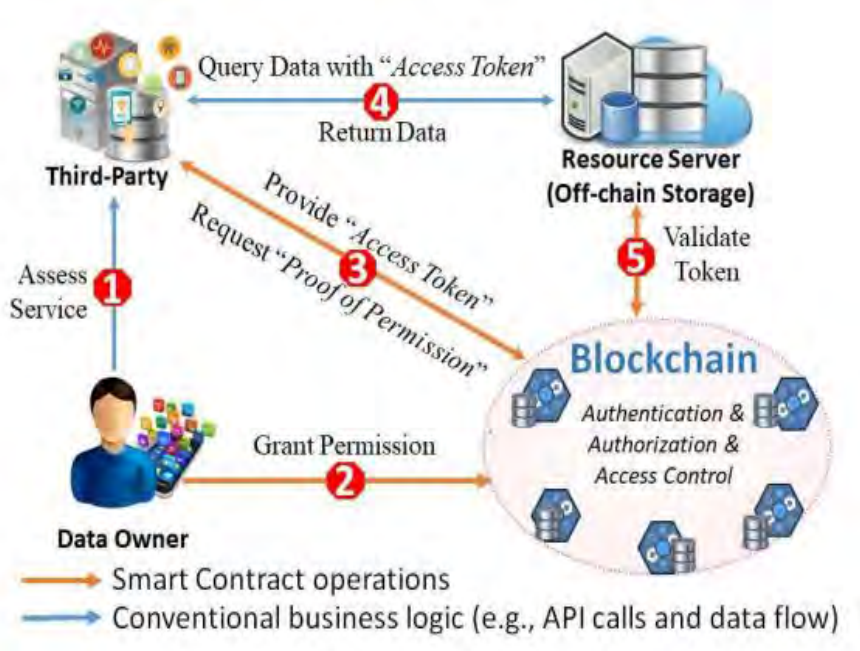
(예: 데이터 최소화, 폐쇄형 블록체인, 설계에 의한 개인정보보호 등)

GDPR 준법 영역별 제안된 솔루션

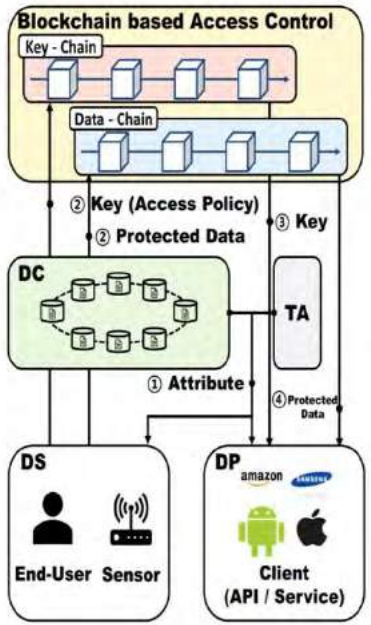


접근제어

- Truong 등
  - BC와 SC 기술 이용 "접근 토큰" 개념의 접근제어 시스템 제안
  - 데이터에 대한 모든 접근에 대한 허가의 개념
  - 사용자 및 시스템 과도한 부하

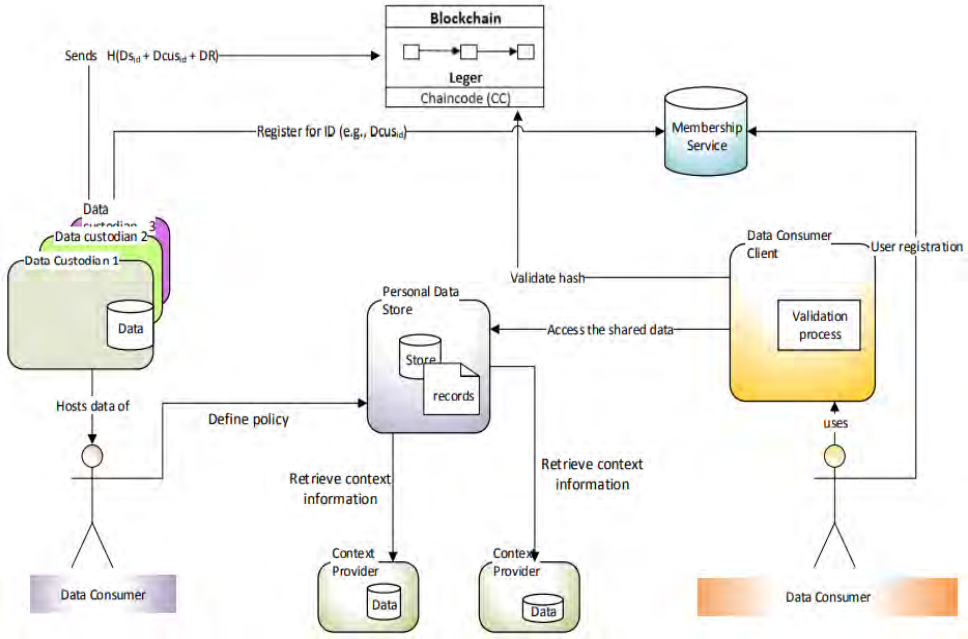


- 임준호 등
  - 다중 블록체인(multi-chain) 기반 접근제어 시스템을 제안
  - 블록체인에서 모든 접근 제어와 데이터 저장을 처리 시 처리 속도와 관련된 성능 문제 (합의 처리가 필요하여 일반 DB에 비해 성능 매우 떨어짐)

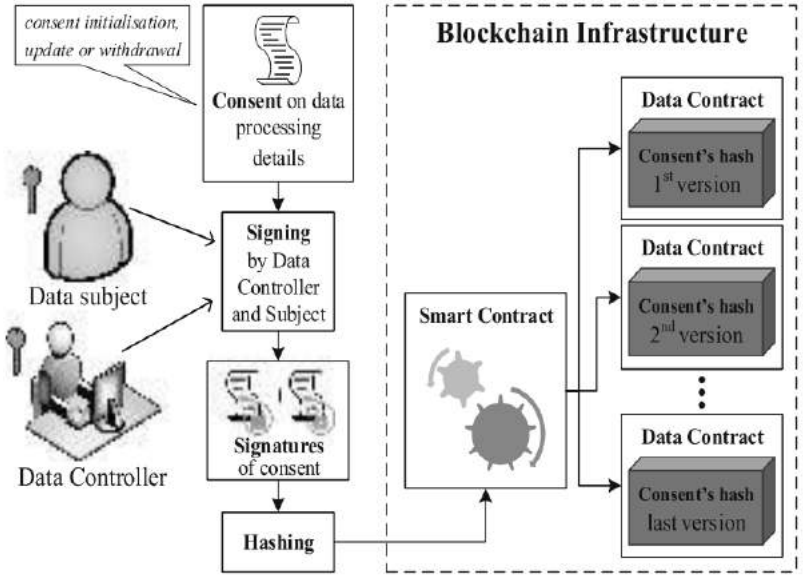


공증

- Chowdhury 등
  - 폐쇄형 블록체인을 이용하여 공증 서비스를 제공하는 시스템 제안
  - GDPR 준법을 위한 구체적인 규정 항목과 관련한 방안제시 미비

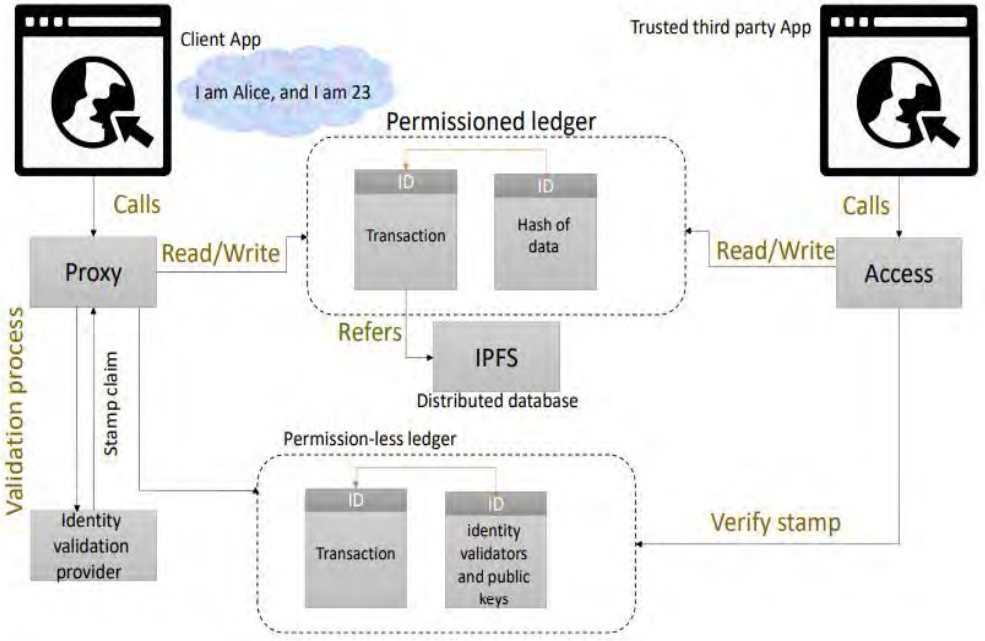


- Rantos 등
  - 사용자 중심 동의 관리 솔루션 및 동의의 무결성 보장을 위해 동의 공증 방안을 제안
  - 동의와 관련된 GDPR 준법을 위한 구체적인 규정 항목과 관련한 방안제시 미비

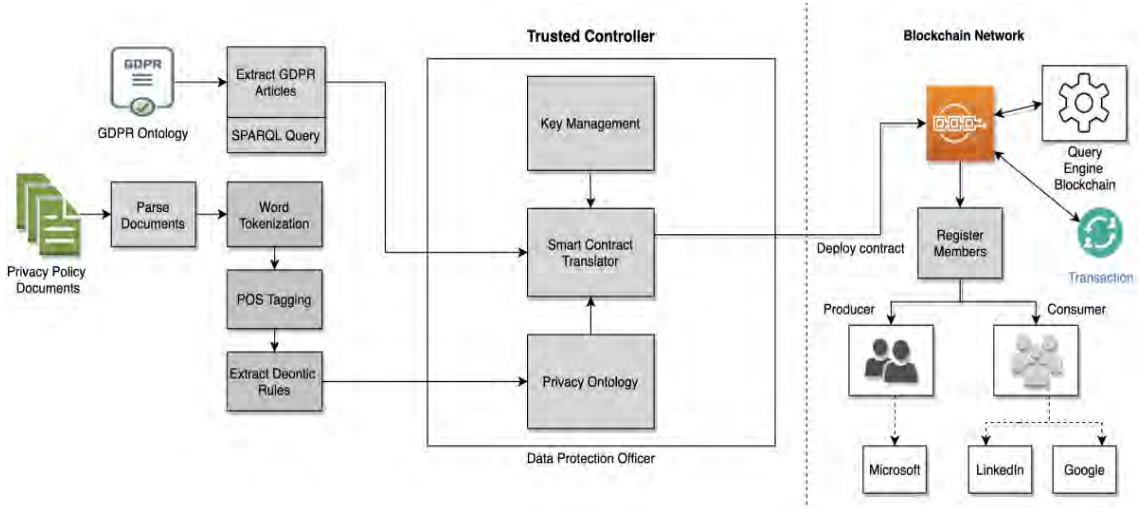


신원 관리, 준법평가

- Kassem 등
  - 사용자가 특정 속성과 관련된 ID를 유지하여 자주권 개념을 달성하는 스마트 계약 기반 ID 관리 시스템 제안
  - GDPR 준법을 위한 구체적인 규정 항목과 관련한 방안제시 미비

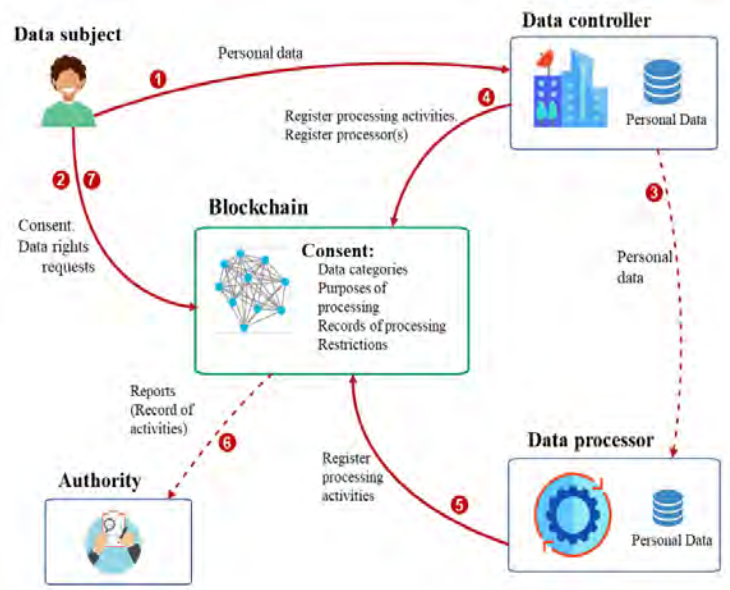


- Mahindrakar와 Josh
  - GDPR 온톨로지와 블록체인을 결합시켜 폐쇄형 블록체인 기반 자동 데이터 준법 시스템 제안
  - 온톨로지 기반 규정 관리 중심이어서 개인정보처리를 위한 GDPR 준법 관리를 위해선 타 시스템과의 연동이 필요

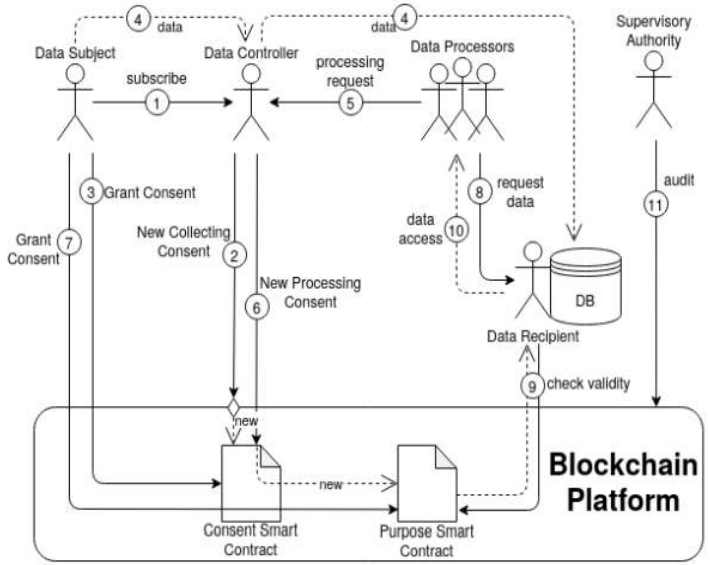


동의관리

- Vargas
  - 블록체인 기반 GDPR 준법관리를 위한 동의관리 솔루션의 개념 설계를 제시
  - GDPR 준법 감사를 위해 블록체인 기술 적용 가능성 및 적용 시 우수성을 제시
  - 구현방안 연구가 필요, 데이터 수집최소화 필요

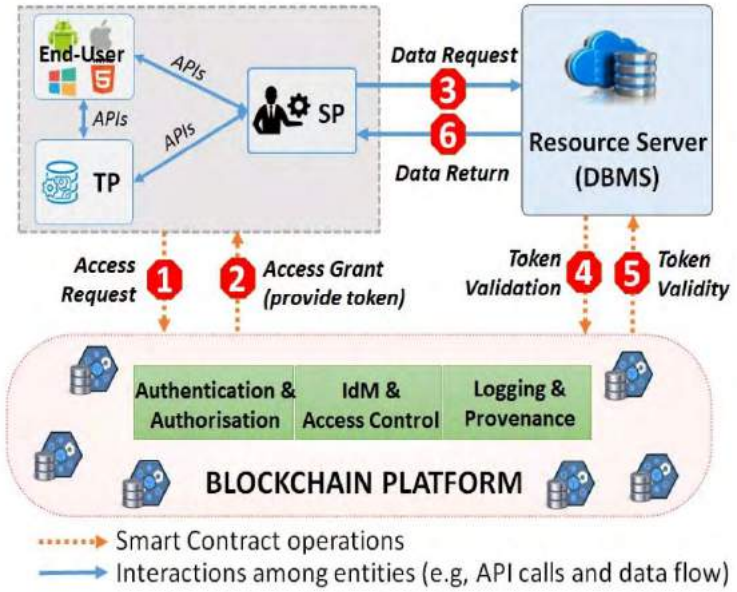


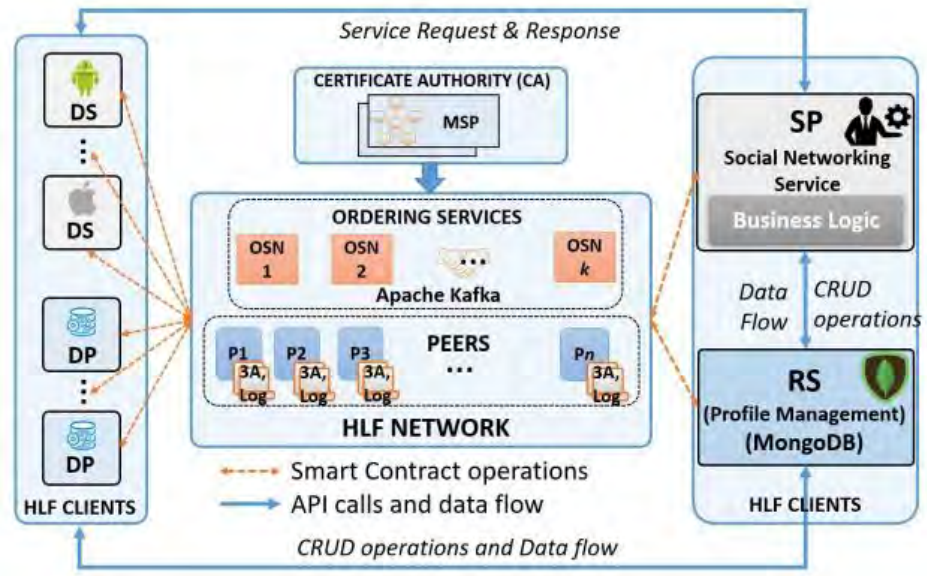
- Daudén-Esmel 등
  - 동의 및 개인정보처리와 관련된 GDPR 준법 관리를 할 수 있는 솔루션의 구축 방안을 제시
  - 기존 연구와는 다르게 GDPR 분석을 통한 시스템의 요구사항을 도출
  - 구현방안 없음. 설계오류(SC가 SC 생성)



GDPR 준법 관리

- Truong 등
  - 블록체인 기반의 GDPR 준수 개인정보 관리 플랫폼 제안
  - 블록체인 기반의 개인정보 관리 플랫폼 아키텍처, 데이터 모델, 알고리즘 등을 제시하고 하이퍼레저 패브릭 상의 구현을 제시
  - GDPR 준법 감사를 위한 감사자 고려 안 함, 현실에선 서비스 사업자 시스템과 API 연계 시 확산성 떨어짐, SP를 통한 블록체인 내 데이터 저장으로 데이터 공신력 부족





기존 연구의 한계점

- 개인정보 처리 요청 기록의 객관적 신뢰성 문제 및 정보주체 개인정보처리 요청 권리 확보 문제는 법적 영역에서만 연구, 기술적 영역에서는 아직 해결방안 연구되고 있지 않음

한계점	분석 대상 선택 관련 연구 번호
블록체인에서의 구체적 구현 방안 미비	E02, E03, E07, E08, E10, E11, E12, E13, E14, K01
GDPR 준법을 위한 구체적인 규정 항목과 관련한 방안제시 미비	E01, E02, E03, E05, E07, E08, E09, E10, E11, K01, K03, K04
개인정보 저장 및 모든 접속 기록에 의한 개인정보보호 위배 위험 문제 고려 미비	E01, E05, E06, E07, E13, K02, K04
제3의 감사자 지원 미비	E05, E06, E08, E09, E10, K01, K02, K03, K04
레거시 시스템과의 연계에 의한 확장성 문제 고려 미비	E01, E02, E03, E04, E05, E06, E09, E10, E12, E13, E14, K01, K02, K03, K04

연구 목표

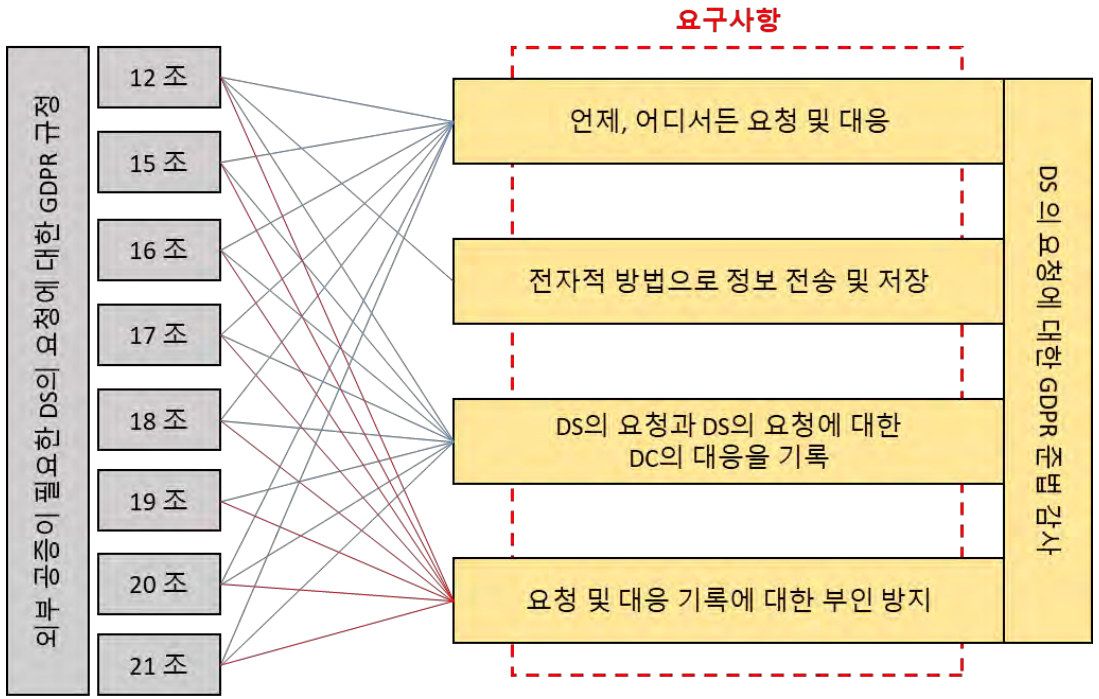
번호	연구 목표	구현 방법
RO1	GDPR 개인정보처리 요청 준법감사 지원	준법감사 요구사항 분석 및 감사 기능 설계
RO2	GDPR 개인정보처리 요청 솔루션 아키텍처 제시	온라인 GDPR 개인정보처리 요청 아키텍처
RO3	레거시 시스템과의 연계에 의한 확장성 문제 해결	이메일을 이용한 약한 연결구조의 위임 아키텍처
RO4	개인정보처리 요청 기록 객관적 신뢰성 확보	블록체인 합의 기반 트랜잭션 공증
RO5	개인정보처리 요청 기록의 무결성 확보	블록체인 내 저장 데이터 구조체 설계
RO6	BC에서의 개인정보 보호	개인정보저장 최소화 및 세션키를 이용한 암호화
RO7	실질적 BC 구현 방안 제시	핵심 스마트 컨트랙트 알고리즘 및 BC 네트워크 구성 & 시뮬레이션

주요 기여내용

- 정보주체 개인정보처리 요청권리 보호 방안 제시
- GDPR 개인정보처리 요청 준법감사 솔루션을 위한 요구사항 도출
- 여러 국가간 상호 신뢰할 수 있는 개인정보처리 요청관련 GDPR 준법 감사 솔루션 제시
- BC 기반 공증 아키텍처 제시
- BC 내 개인정보 암호화를 위한 가볍고 효율적인 세션키 생성 및 배포 방안 제시
- GDPR 원칙을 준수하는 BC 기반 솔루션 아키텍처 제시

개인정보처리 요청 공증 프레임워크 요구사항 분석(RO1) 1

- GDPR 준법 감사
  - 개인정보처리 요청과 관련된 GDPR 규정의 '외부 공증 가능한 개인정보처리 요청 준법감사 지원'을 위한 요구사항 분석



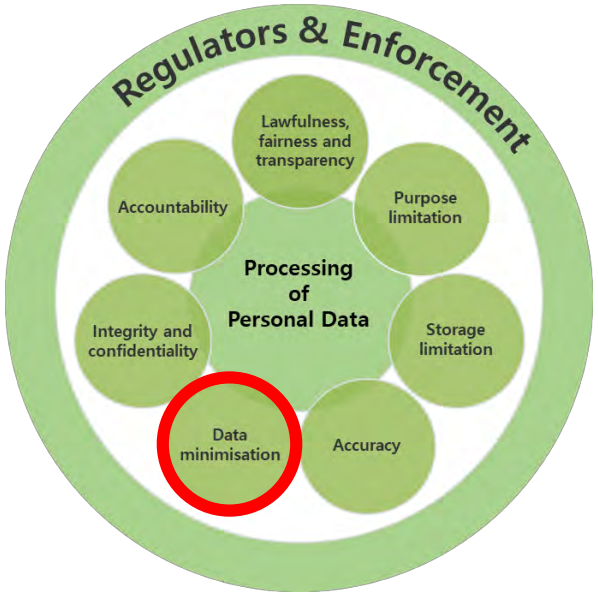
- 분산 환경에서의 실시간 공증
  - 다 국가 적용을 위한 온라인 환경기반 분산 환경에서의 공증 요구사항 (Low 연구 "The Notary" 기반)

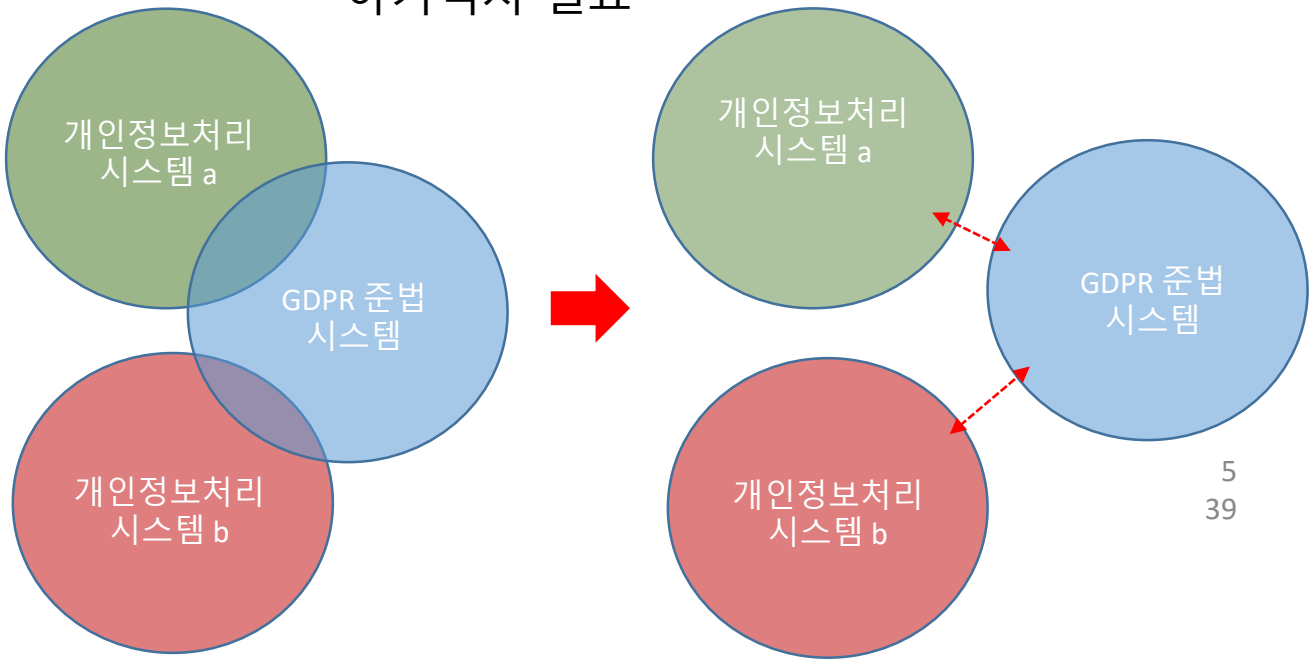
요구사항	충족사유
데이터 봉인	◆ 데이터는 봉인할 때와 검증할 때 동일한 값을 생성해야 함. ◆ 제3자는 데이터를 확보하여 데이터와 값을 검증할 때 교정한 새로운 값을 생성할 수 없어야 함
모두가 접근 가능	◆ 공증인은 데이터를 봉인하려는 모든 사람이 접근할 수 있어야 함
신뢰할 수 있거나 인증 가능	◆ 공증인은 암호 키와 마찬가지로 신뢰할 수 있거나 인증할 수 있어야 함
매우 신뢰할 수 있는 의사소통	◆ 공증인과 사용자 간에 매우 안전한 통신이 있어야 함 ◆ 자신이 공증한 데이터가 공증을 요청한 데이터인지 확인할 수단이 있어야 함
인증	◆ 트랜잭션을 시작하는 사용자는 해당 트랜잭션에 참여하거나 다른 사용자에게 작업을 위임할 수 있는 유일한 사용자여야 함

개인정보처리 요청 공증 프레임워크 요구사항 분석(RO1) 2

- GDPR 원칙 준수
  - 5조 개인정보처리와 관련된 GDPR 원칙 준수 요구사항
  - BC의 분산저장 특성에 따른 높은 위배가능성 감소를 위해 데이터수집 최소화 필요

- 실제 환경에서의 실현가능성
  - GDPR 준법 적용 확산을 위해 실현성 중요
  - 배포, 확산을 고려 필요
  - 기존 레거시 시스템의 수정 또는 3rd 파티 모듈 설치를 통한 결합을 최소화하는 유연한 약결합도 (Loosely coupling) 아키텍처 필요

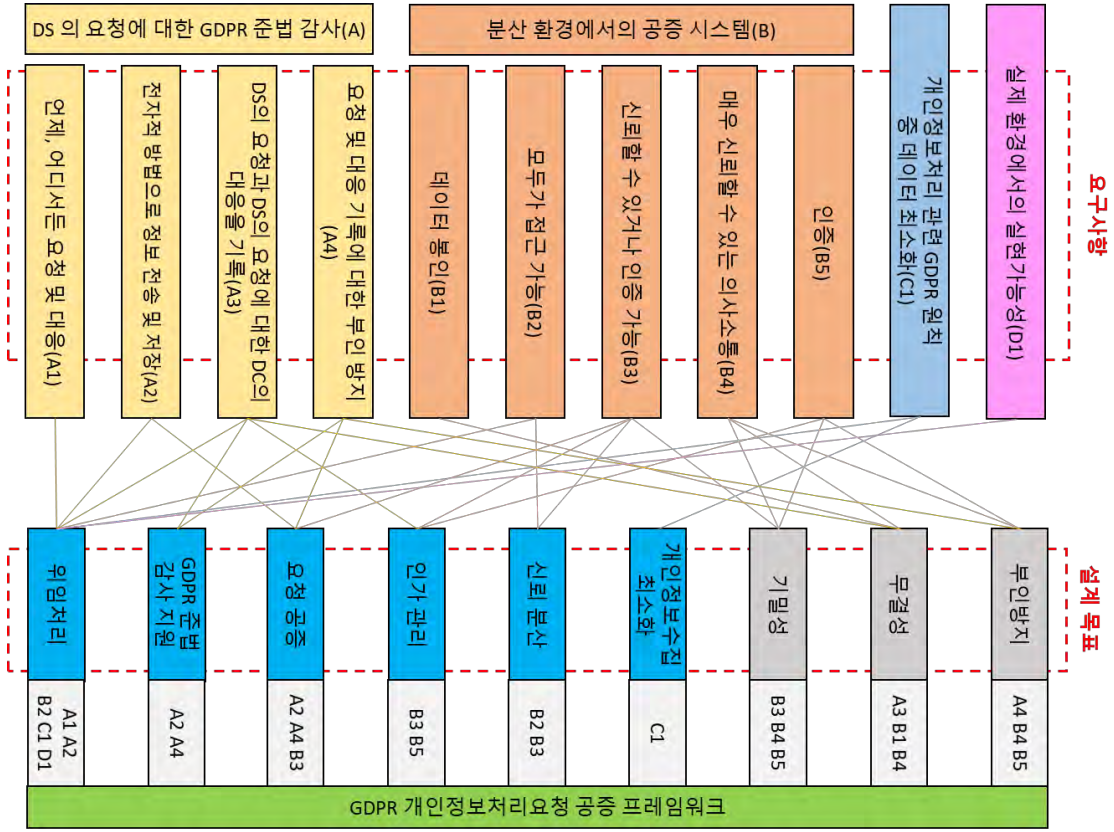




5
39

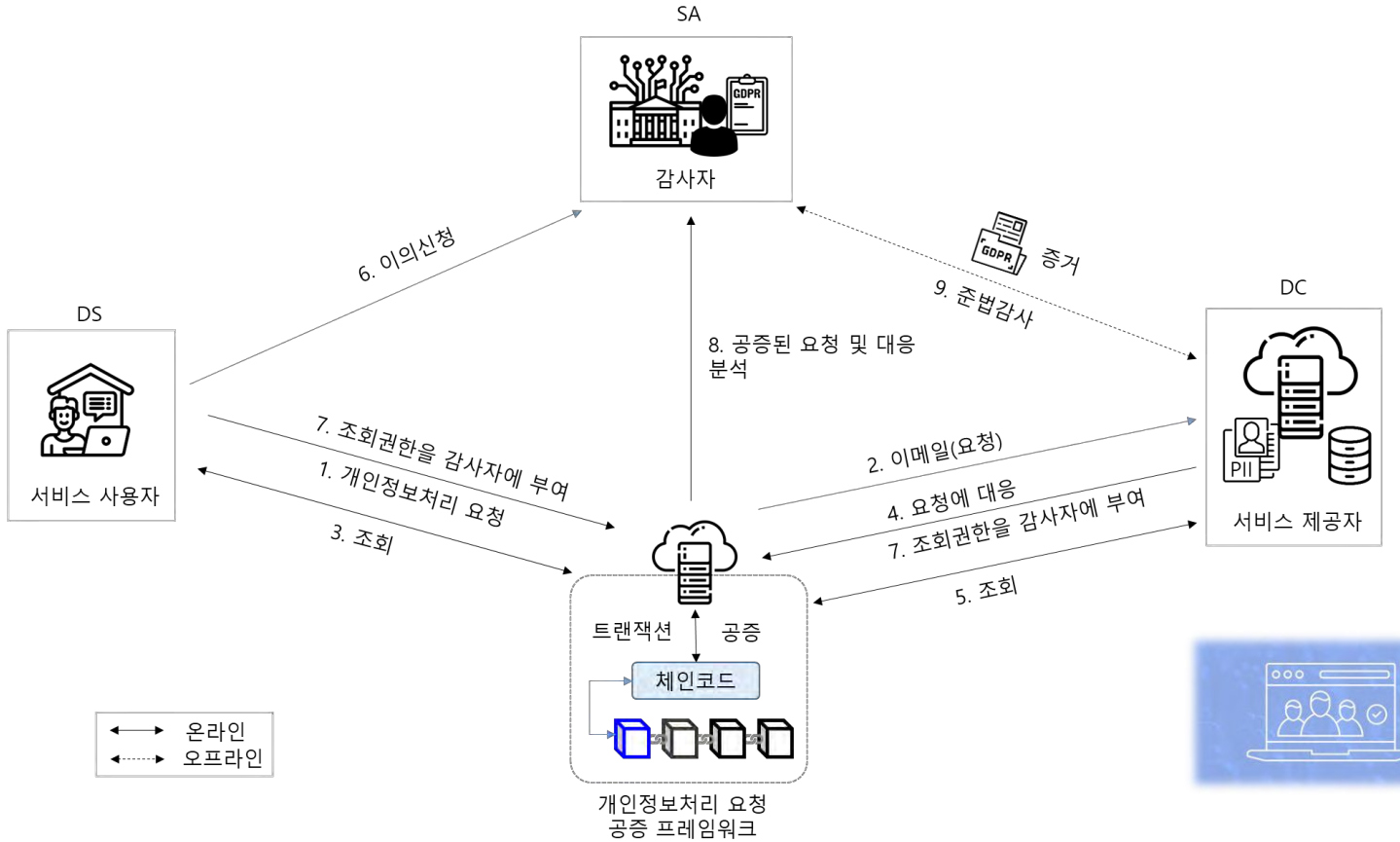
설계 목표(RO1)

- 도출된 요구사항을 바탕으로 요구사항을 충족할 수 있는 GDPR 개인정보처리 요청 공증 프레임워크의 기능, 보안 설계 목표 수립



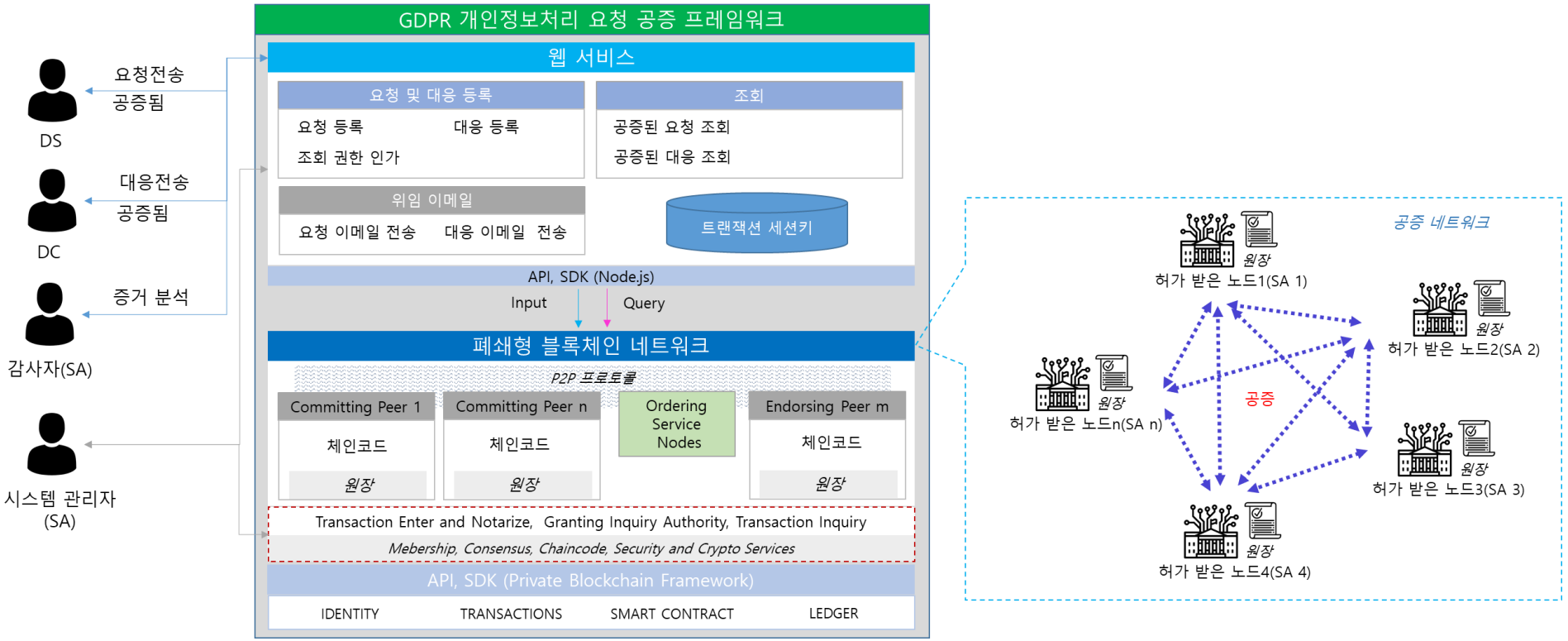
제안 프레임워크 감사 처리절차(RO2, RO3)

- "폐쇄형 블록체인 기반 GDPR 개인정보처리 요청 공증 프레임워크" 제안
- 제안 프레임워크를 이용하여 온라인 개인정보처리 요청 위임 및 공증, 공증된 기록으로 준법 감사



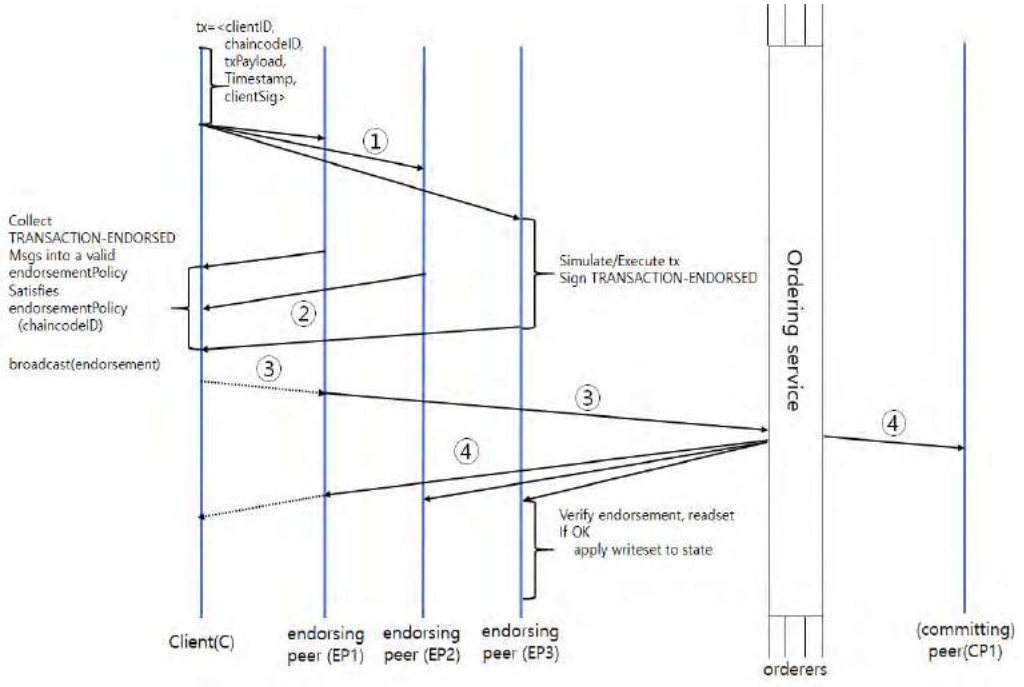
제안 프레임워크 아키텍처(RO2, RO3)

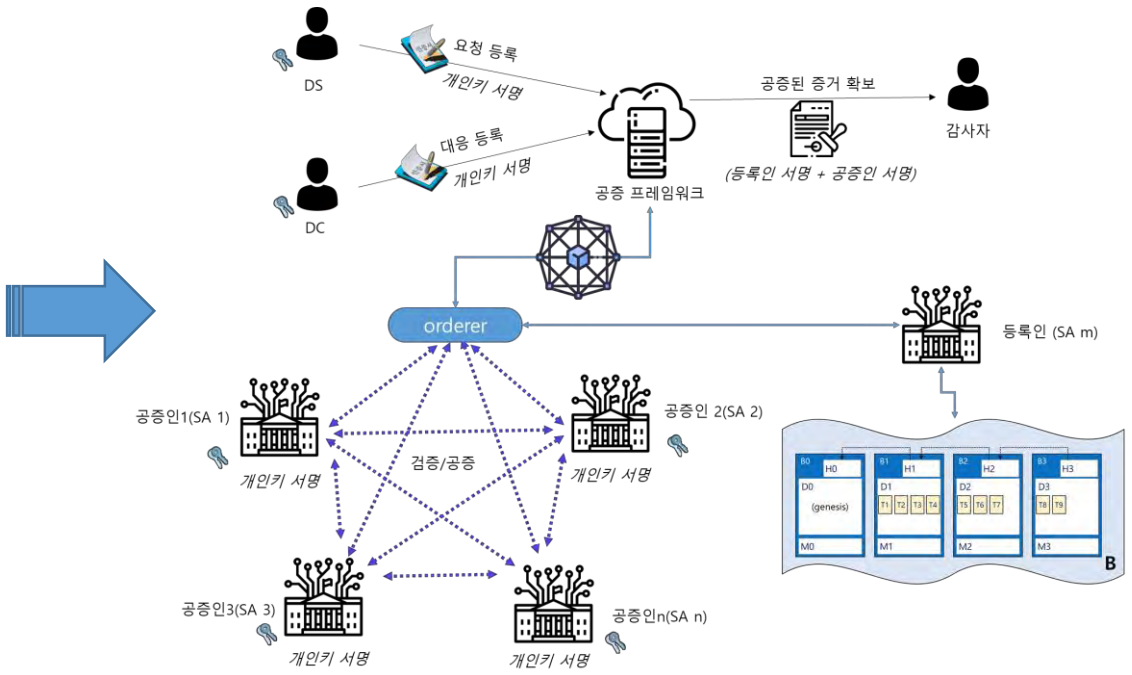
- 온체인(BC 기반), 오프체인(웹 서비스)으로 구성
- 온체인에서 공증 및 기록저장, 오프체인에서 요청전송 위임 및 세션키 생성/저장 등 처리



블록체인기반 공증처리 기법(RO4)

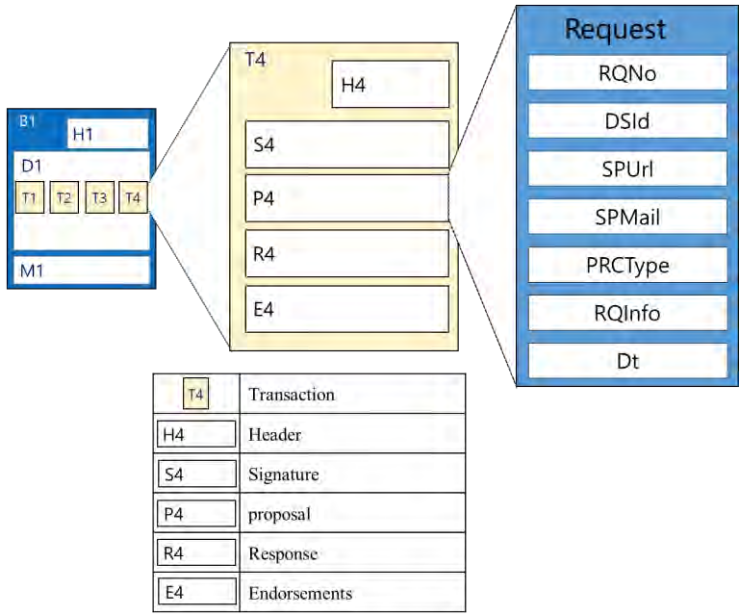
- 생성자와 공증인을 포함한 네트워크 참여자들의 PKI 기반 인증 및 개인키 서명기술을 이용하고 HLF의 합의 알고리즘을 활용 공증처리
- 공증인의 신뢰성 확보위해 폐쇄형 블록체인 특성인 권한관리를 적용하여 감독기관(SA)만 검증 피어로 참여하도록 설계





블록 및 트랜잭션 구조체 설계(RO5)

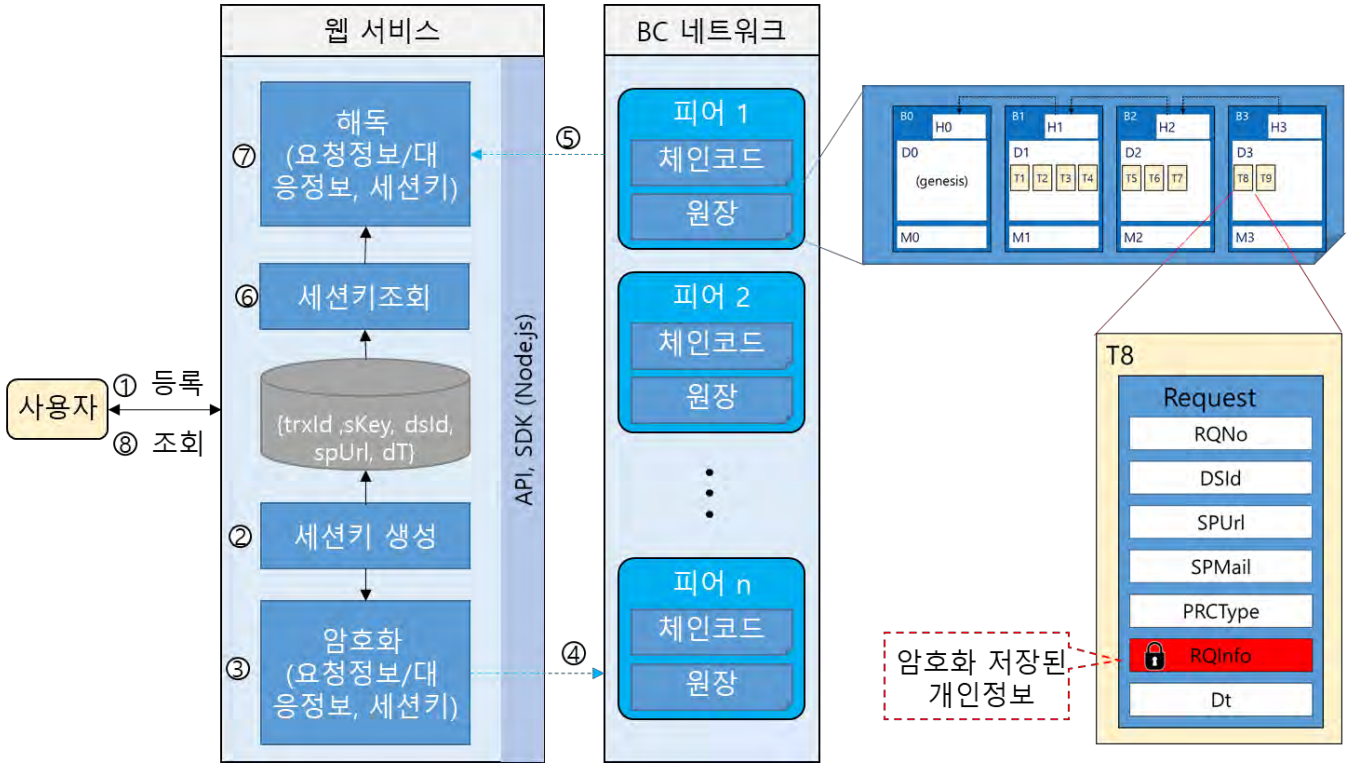
- S4 영역에 트랜잭션 생성자 시그니처 삽입 (부인방지)
- P4 영역에 체인코드에서 처리될 트랜잭션 구조체 삽입
- 감사를 고려한 요청, 대응, 감사권한 구조체 설계



이름	설명
Request	DS에서 DC로 보낸 개인 데이터 처리 요청 구조
	매개변수 : 요청 번호, DS의 ID, SP의 URL, SP 이메일, 처리 유형, 요청 내용, 타임스탬프
Response	DC가 DS로 보낸 요청에 대한 응답 구조
	매개변수 : 응답 번호, 요청 번호, DS의 ID, SP의 URL, DS의 이메일, 처리 유형, 요청 내용, 응답 내용, 타임스탬프
Authorization	DS 또는 DC에서 부여한 데이터 접근 권한의 구조
	매개변수 : 인가 번호, 인가자 유형, 감사인 ID, SP의 URL, 인가자 ID, 권한 만료일

세션키 이용 개인정보 암호화 절차(RO6)

- 피어 분산 원장 조회 시 중요개인정보 노출 우려 -> 암호화
- 트랜잭션별 키 생성 및 생성자 수신자만 키를 공유할 수 있는 가벼운 세션키 생성, 배포방안



세션키 알고리즘(RO6)

- 해쉬암호 기반 가벼운 키생성 알고리즘
- 인증된 사용자 정보와 애플리케이션 DB 기반 키배포 알고리즘
- 암호화 알고리즘은 기존 대칭키 알고리즘 사용
- DS의 ID, SP의 URL로 생성자/수신자만 공유

Algorithm 1: MakeSessionKey

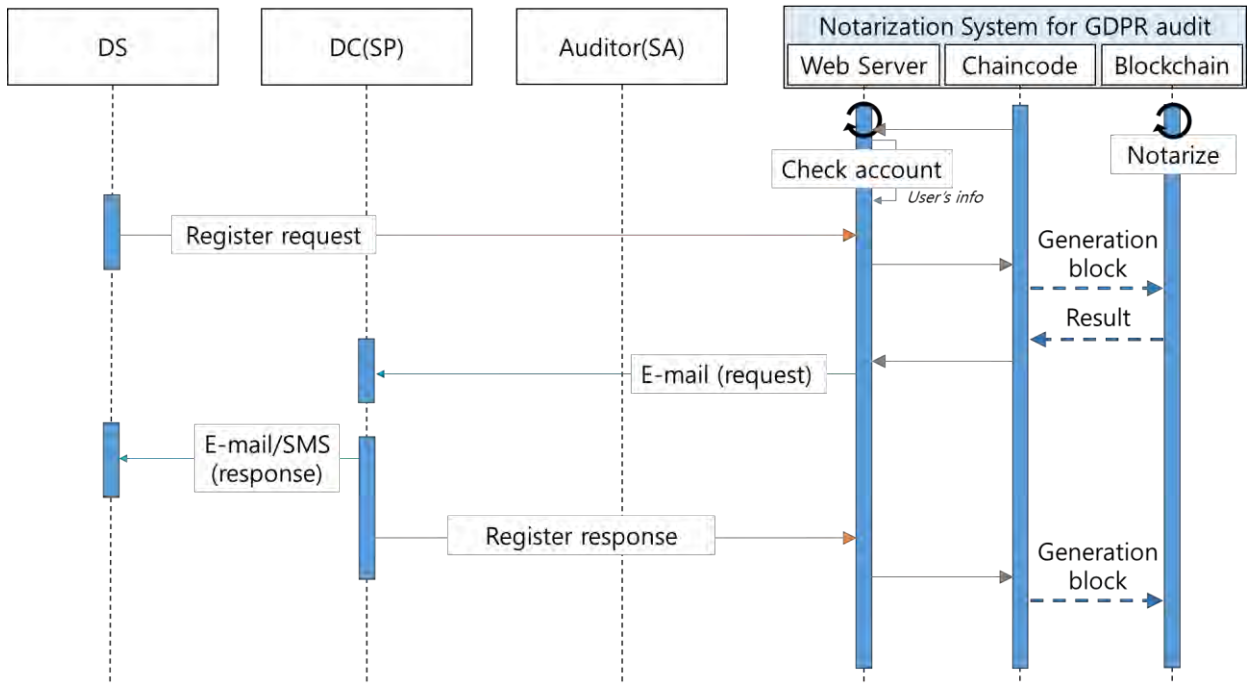
Input : DS's ID dsId, SP's url spUrl, transaction ID trxId, transaction type trxType, private data pData, timestamp dT
Output : Session Key sKey
1 **if** trxType equal request **then**
2 sKey ← Hash(Hash(trxId) + Hash(pData))
3 Add { trxId, sKey, dsId, spUrl)} in application database
4 **return** sKey

Algorithm 2: InquirySessionKey

Input : User ID uId, transaction ID trxId
Output : Session Key sKey
1 UserType uType ← Check User Type (uId)
2 **if** uType equal DS **then**
3 sKey ← Query sKey from application database
where uId equal dsId in DB
and trxId equal trxId in DB
4 **if** uType equal DC **then**
5 SP's url spUrl ← Get spUrl from user information in DC's session
6 sKey ← Query sKey from application database
where spUrl equal spUrl in DB
and trxId equal trxId in DB
7 **else**
8 sKey ← null
9 **return** sKey

개인정보처리 요청/대응 등록(RO7)

- 개인정보처리 요청/ 대응을 제안 프레임워크에 등록
- BC에 저장되고 공증된 요청/대응 메일 서버를 통해 전송



Algorithm 3: InputRequest

Input : DS's ID dSId, SP's url sPUrl, SP's e-mail sPMail, process type pRCType, contents of request rQInfo, timestamp dT

Output : Transaction trx

// make key

1 Transaction key rQNo, err ← MakeRQNo(dSId, dT)

2 **if** err != null **then**

3 **return** err

4 Request structure request ← Request{ rQNo, dSId, sPUrl, sPMail, pRCType, rQInfo, dT}

5 requestJSON, err ← Transform to JSON(request)

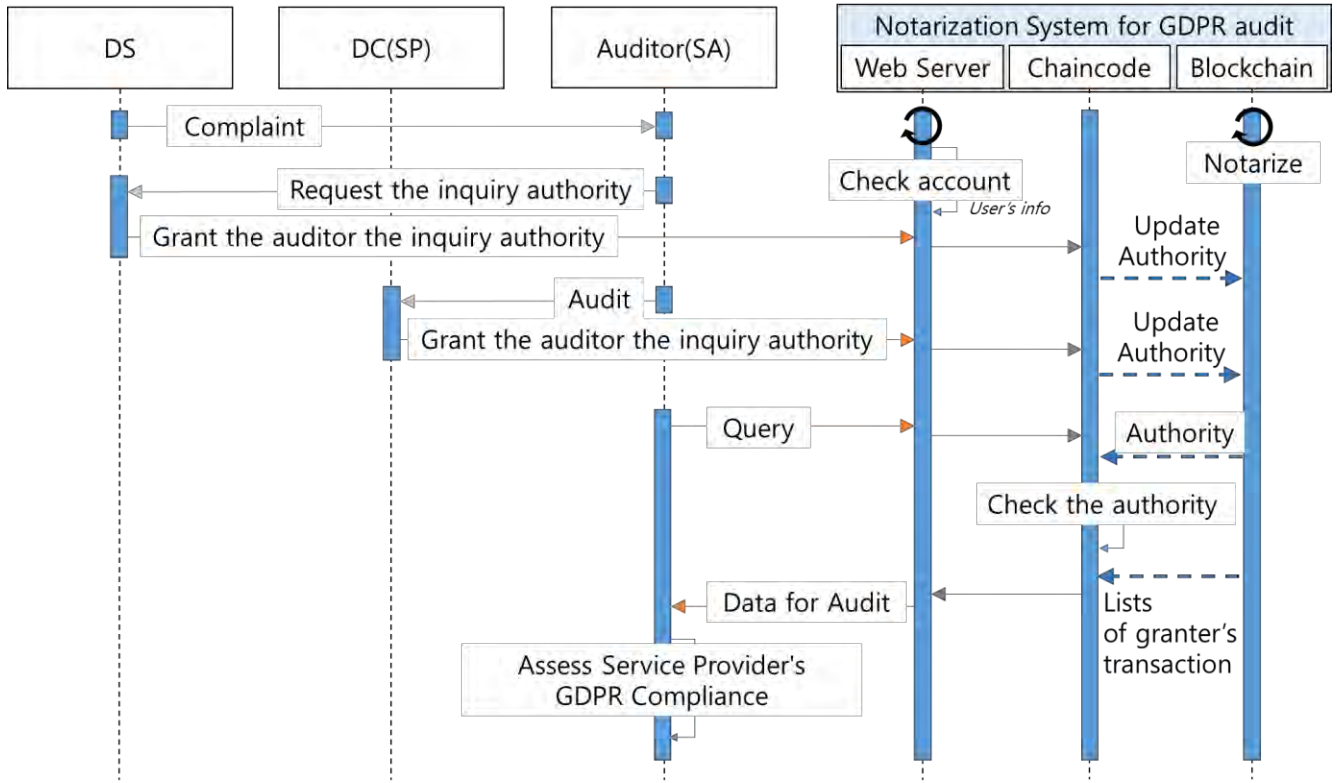
6 **if** err != null **then**

7 **return** err

8 **return** Make transaction(rQNo, requestJSON)

개인정보처리 감사권한부여/조회(RO7)

- 감사자에게 감사 요청 및 요청/대응 기록을 조회할 수 있는 권한 부여
- 권한 부여 받은 감사자가 제안 프레임워크 이용 기록 조회 후 준법감사 수행



스마트 컨트랙트 감사권한처리 알고리즘(RO7)

- 감사자에게 생성자가 자신의 트랜잭션을 한시적으로 조회할 수 있는 권한 부여
- 조회 권한을 받은 감사자가 요청/대응 이력 조회
- 조회 시 권한 체크

Algorithm 5: InputAuthority

Input : Grant key gTNo, grant type gTType, auditor's ID sAAId, SP's url sPUrl, Grantor's ID gTId, expire date expDate
Output : Transaction trx

```
    //check authority being
5 exists, err ← Check Authority Exists(gTNo)
6 if err != null then
7 return err
8 if exists then

9 trx ← Update Authority(ctx, gTNo, expDate)
```

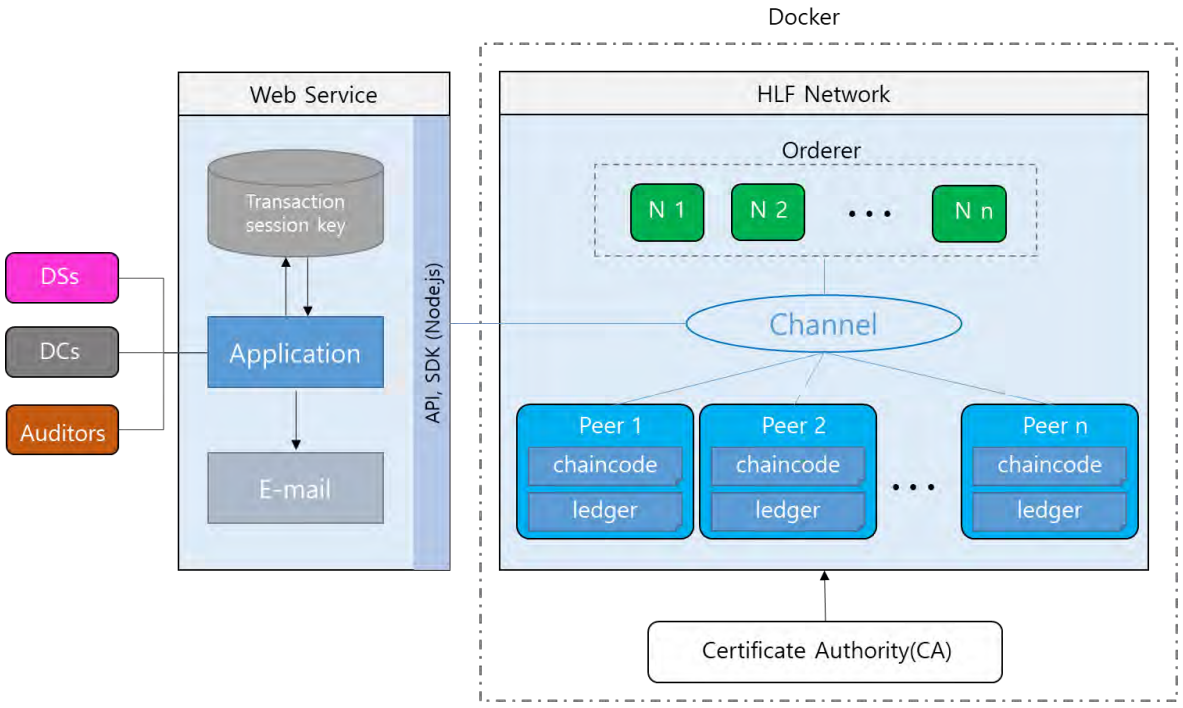
Algorithm 6: GetNotarizedLists

Input : Grant key gTNo, grant type gTType, start date for query fromDT, end date for query endDT
Output : Request Transaction list trxList1, Response Transaction list trxList2

```
    //check Authority validation
1 validation, err ← Authority Validation(gTNo)
2 if !validation then
3 return Print error("the authority %s doesn't valid", gTNo)
    //separate and extract IDs
4 Auditor's ID sAAId, DS's ID dSId, SP's url sPUrl, err
        ← Extract Ids(gTNo,)
    // range query of DS's request
5 requestIterator, err ← Query by range(dSId+fromDT, dSId+endDT)
```

구현 및 시뮬레이션(RO7)

- HLF2.2 와 Docker를 이용하여 BC 네트워크 구성 및 제안 프레임워크 파일럿 구현
- 체인코드는 Go, 웹 서비스는 node.js SDK, 합의 알고리즘은 Raft 적용하여 구현
- 개인정보처리 요청 관련 GDPR 준법 감사 시뮬레이션



< BC 네트워크 구성>

< 인증서버 구성>

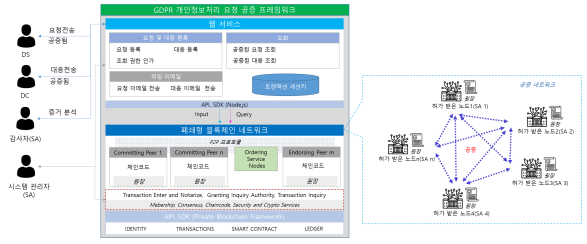
< 블록에 저장된 트랜잭션>

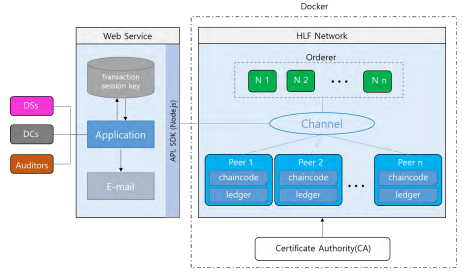
보안 분석

요구사항	충족사유
데이터 보안	◆ 체인코드에서 사용자의 정보(Uid, SPurl)를 저장된 트랜잭션 키와 비교하기 때문에 자신이 생성한 트랜잭션이 아니면 조회가 불가능. ◆ 오프체인에서 세션키를 이용하여 개인정보가 있는 요청내용 암호화, 온체인 피어에서 복사된 트랜잭션의 요청내용 복호화 불가능 ◆ BC 의 특성으로 무결성 보장
인증 및 인가	◆ HLF의 Fabric CA를 CA로 적용. Fabric CA는 PKI(공개 키 인프라)기반이며 X.509 디지털 인증서를 생성하는데 사용 ◆ HLF는 '정책'이라는 인프라 관리 메커니즘을 제공한다. Fabric 정책들은 구성원이 네트워크, 채널 또는 스마트 계약에 대한 변경 사항을 수락하거나 거부하는데 동의하는 방법을 나타냄 ◆ 본 연구는 configtx.yaml에서 정책을 설정하여 각 구성원들이 Fabric 네트워크에서 수행하려는 모든 작업을 제어함
부인 방지	◆ 생성자의 개인키 서명을 통해 블록으로 생성. ◆ 입력한 트랜잭션의 공증 및 이메일 등 위임기반 전송
감사 추적성	◆ 트랜잭션은 {누가, 언제, 누구에게, 무엇을} 형태로 저장 ◆ 폐쇄형 BC를 기반으로 하고 있어 BC의 무결성, 감사추적성 특성을 계승

기능 분석 1

요구사항	충족사유
DS 의 요청에 대한 GDPR 준법 감사(A)	
언제, 어디서든 요청 및 대응(A1)	◆ 제안프레임워크는 웹 서비스를 통해 DS의 요청과 DC의 응답을 위임하고 블록체인 네트워크에서 공증한 후 이메일 서비스를 통해 수신자에게 보내어 DS와 DC가 언제, 어디서나 요청하고 응답할 수 있도록 설계되었음. ◆ 4장 그림 4.8 '요청 및 응답의 공증 과정' 및 5장 그림 5.1 ' 제안된 프레임워크에 대한 HLF 시뮬레이션 시스템 아키텍처' 참조.
전자적 방법으로 정보 전송 및 저장(A2)	◆ 4장 표 4.1 '트랜잭션의 데이터 구조체' 및 5장 그림 5.1 ' 제안된 프레임워크에 대한 HLF 시뮬레이션 시스템 아키텍처' 참조
DS의 요청과 DS의 요청에 대한 DC의 대응을 기록(A3)	
요청 및 대응 기록에 대한 부인 방지(A4)	◆ 5.나.1).가) 보안분석 '부인방지' 참조





기능 분석 2

요구사항	충족사유
분산환경에서의 공증 시스템(B)	
데이터 봉인(B1)	◆ HLF의 합의 절차를 통해 공증을 하도록 설계. 공증인 역할을 하는 피어는 검증 시 자신의 개인 키로 생성된 서명만 트랜잭션에 포함하고 데이터를 변경하지 않음. 인증 및 인가를 통해 감독기관만 공증인으로 참여하도록 설계함. ◆ 5.나.1).가) 보안분석 '데이터 보안' 참조
모두가 접근 가능(B2)	◆ 제안프레임워크는 DS의 요청과 DC의 응답을 웹 서비스와 이메일 서비스를 통해 위임하도록 설계됨. ◆ DS 및 DC 누구나 CA의 인증 및 승인을 받은 후 프레임워크에 접근하고 사용할 수 있음. ◆ 5장 그림 5.1 ' 제안된 프레임워크에 대한 HLF 시뮬레이션 시스템 아키텍처' 참조
신뢰할 수 있거나 인증 가능(B3)	◆ 원장의 무결성과 객관적인 신뢰성을 위해 제안프레임워크는 공증에 참여하는 노드를 SA와 같은 권위 있는 기관으로 제한함. 제안프레임워크에서 여러 공증인이 참여하여 공증할 수 있는 알고리즘은 이미 안정성이 검증된 HLF의 RAFT 알고리즘을 상속함.
매우 신뢰할 수 있는 의사소통(B4)	◆ 제안프레임워크는 폐쇄형 블록체인 프레임워크인 HLF를 사용하기 때문에 HLF의 시스템, 네트워크, 데이터의 무결성과 기밀성을 계승함. HLF는 TLS를 사용하는 노드 간의 보안 통신을 지원함. 제안프레임워크는 HLF의 TLS를 적용하였음.
인증(B5)	◆ 5.나.1).가) 보안분석 '인증 및 권한 부여' 참조

기능 분석 3

요구사항	충족사유
개인정보처리 관련 GDPR 원칙(C)	
데이터 최소화(C1)	◆ 제안프레임워크는 개인정보처리 요청과 관련된 GDPR 준법 감사를 위해 DS의 요청 및 DC의 응답 처리 요청 트랜잭션 정보만 블록체인에 저장하고 SP가 가지고 있는 다른 개인 데이터는 저장하지 않음. ◆ 4장 표 4.1 '트랜잭션의 데이터 구조체' 참조
실제 환경에서의 실현가능성(D)	
실제 환경에서의 실현가능성(D1)	◆ 제안프레임워크는 웹 서비스와 이메일 서비스를 통해 DS의 요청과 DC의 응답을 위임하도록 설계되었으므로 SP는 요청을 수신할 책임자 메일만 공개하면 될 뿐 기존의 개인정보처리 시스템을 수정하거나 별도의 외부 모듈을 설치할 필요가 없음. ◆ 따라서 실제 환경에서 GDPR 준수 감사 프레임워크로 적용할 수 있음.

관련연구 비교 평가

- Truong 등이 제안한 프레임워크의 요구사항 충족 분석 결과 A3, B1, B3, C1, D1 요구사항을 충족하지 못하였음.

요구사항	미충족사유
DS의 요청과 DS의요청에 대한 DC의 대응을 기록(A3)	◆ 엔드유저가 개인정보가 있는 리소스서버에 데이터 처리를 요청하기 위해선 SP의 시스템를 통해서만 가능. 중간에 있는 SP가 엔드유저의 요청을 무시 또는 조작할 수 있음. ◆ DS의 요청 내용을 저장하도록 설계되어 있지 않음.
데이터 봉인 (B1)	◆ 요청 전달 중 SP가 엔드유저의 요청을 조작할 수 있음. ◆ 엔드유저의 요청에 대한 봉인과 공증 방안 제시되지 않음.
신뢰할 수 있거나 인증 가능(B3)	◆ 개인정보의 처리에 대한 기록을 대부분 리소스서버에서 제안 플랫폼에 저장을 하는데 리소스서버를 신뢰할 수 없다면, 데이터 또한 신뢰할 수 없음.
데이터 최소화(C1)	◆ 제안 플랫폼은 SP의 모든 개인정보처리 이력을 저장함. 하지만 DS가 SP의 서비스 가입 시 DS의 개인정보처리를 SP에게 위임함. 따라서 GDPR준법감사를 위해 DS가 위임한 SP의 모든 개인정보처리를 저장하는 것은 과도하며, 개인정보처리와 연관된 개인정보도 과도하게 저장하게 됨.
실제 환경에서의 실현가능성(D1)	◆ 제안프레임워크를 사용하기 위해선 SP들이 레거시 개인정보처리시스템을 수정하거나 별도의 외부모듈을 설치하여야 함. ◆ 현실 환경에서 준법감사를 위해 모든 SP에게 강제하기 어려움.

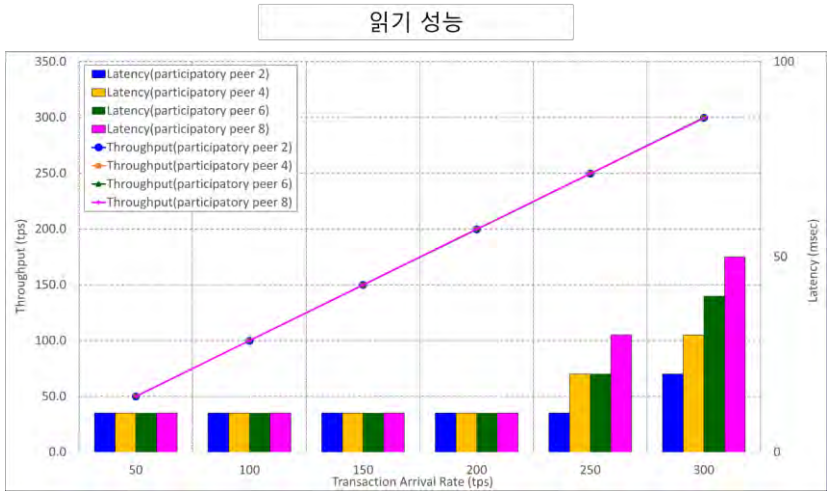
관련연구 비교 평가

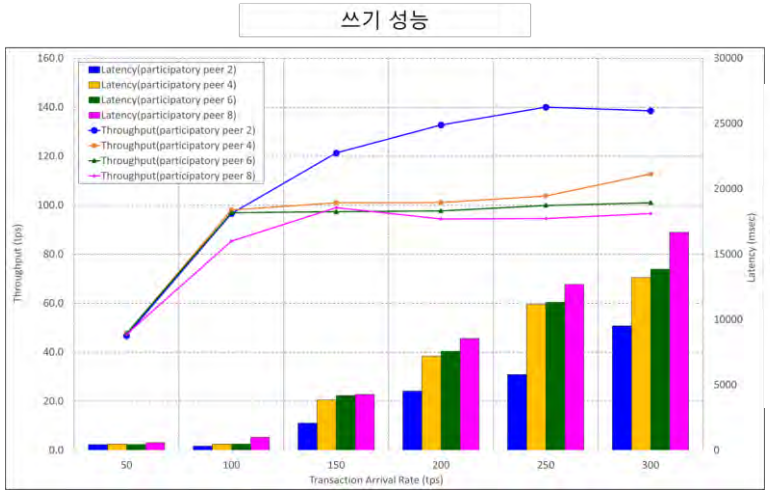
- BC 기반 GDPR 준법 연구 중 데이터 처리 요청에 대한 이슈를 포함하고 있고 구현을 통해 검증을 수행한 연구인 Truong 등의 연구 비교
- 제안 프레임워크가 Truong 등이 제안한 접근제어 방식 이전 연구의 솔루션에 비해 개인정보 처리 요청에 대한 객관적 신뢰성, GDPR 원칙 준수, 실현 가능성의 측면에서 더 우수함

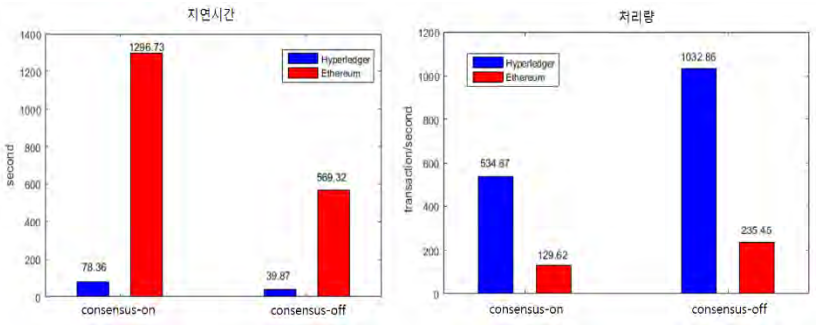
비교 연구	A1	A2	A3	A4	B1	B2	B3	B4	B5	C1	D1
Truong 등	**Y**	**Y**	*N*	**Y**	*N*	**Y**	*N*	**Y**	**Y**	*N*	*N*
본 연구	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**

성능평가

- Intel Core i5-8265U CPU @ 1.60GHz, with 16GB RAM 사양의 시스템에 도커를 설치하고 2피어 3오더러와 Raft 합의 알고리즘을 적용하여 HLF 네트워크를 구성하여 시뮬레이션
- 하이퍼레저 블록체인 환경에 최적화된 성능측정 프레임워크인 하이퍼레저 캘리퍼 사용
- 실제환경에서의 적용 가능성 검증
- 이전 연구들을 통해 HLF가 타 블록체인 프레임워크에 비해 성능 우수 검증됨







< HLF 이더리움 성능 분석 결과>

(지표 – Throupout : 처리된 트랜잭션 수, Transaction Arrival Rate : BC에 입력된 트랜잭션 수, Latency : 처리 지연시간, peer : 네트워크 참여 피어 수)

40

결 론 및 향후 일정

- 개인정보처리 요청과 관련된 기록의 신뢰성에 대한 객관적 관점 문제 해결을 위해 요구사항을 도출하고 폐쇄형 BC 기반의 개인정보처리 요청 공증 프레임워크를 설계하고 구축
- 폐쇄형 BC의 합의과정을 공증과정으로 맵핑하는 SC알고리즘, 가볍고 실용적인 세션키 생성 및 배포 알고리즘을 통해 개인정보를 암호화, 위임기반 약결합 아키텍처를 통한 배포 확산 방안 제시
- 시뮬레이션을 통해 보안 및 기능 요구사항을 충족하고 성능 테스트를 통해 현실환경에서의 적용 가능성 및 기존 연구의 솔루션보다 우수함 증명
- 현재 공증인은 법으로 규정 따라서 제안 방안의 법적 강제성 없음. 하지만 현재 국가간 법적 분쟁 시 객관적 자료 확보가 어렵기에, 제안 프레임워크의 기록이 참고 자료로 사용될 수 있으며, 향 후 GDPR 준법 감사를 위한 전자 공증 활용 법 개정 검토 시 본 연구의 제안 방안을 참고할 수 있음.
- 향 후 GDPR 준법 전반에 걸쳐 개인정보에 대한 DS의 주권을 보장해줄 수 있는 통합 GDPR 준법 감사를 위한 방안 연구 확대

연구성과

- “Delegation-based Personal Data Processing Request Notarization Framework for GDPR based on Private Blockchain”, Applied Sciences(SCIE 저널)에 21-09-23 투고, 현재 리뷰 중

- "Personal Data Processing Notarization Framework based on Private Blockchain for GDPR“, ICT-AES의 국제 컨퍼런스 “7th ICAEIC-2021”에 21-07-08 발표

- “블록체인 기반 경력 관리 시스템 - 전원주택 시공 경력 관리 사례”, 한국통신학회논문지(KCI 등재) 제46권 제3호에 21-03 출간

감사합니다!

Q & A