

블록체인 신뢰 프레임워크(K-BTF) 중장기계획 수립 연구

수행기관 : 블로코

2023. 12.

제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “블록체인 신뢰 프레임워크(K-BTF) 중장기계획 수립 연구”의 최종 연구개발 결과보고서로 제출합니다.

2023년 12월

수행 기관 : (주)블로코

연구책임자 : 대표이사 김 종 환

(블로코)

참여연구원 : 본 부 장 심 건 수

(블로코 사업본부)

연구소장 서 광 준

(블로코 EVM 연구소)

C T O 김 용 건

(블로코 리서치센터)

팀 장 박 상 길

(블로코 FE 챗터팀)

수 석 김 명 성

(블로코 FE 챗터팀)

본 부 장 강 연 주

(블로코 사업개발본부)

부 장 김 현 동

(블로코 세일즈팀)

팀 장 김 주 환

(블로코 프로젝트팀)

선 임 신 준 하

(블로코 프로젝트팀)

선 임 강 미 애

(블로코 제품기획팀)

요 약 문

1. 제목

블록체인 신뢰 프레임워크(K-BTF) 중장기계획 수립 연구

2. 서론

□ 본 연구를 통해서 블록체인 기반 공공서비스를 효율적으로 개발·운영하고, 쉽게 상호호환할 수 있는 블록체인 신뢰 프레임워크(K-Blockchain Trust Framework, 이하 K-BTF)의 종합적인 실행·추진 계획을 마련하고자 한다.

(1) 추진 배경

- 현재 공공분야에서 구축된 공공 블록체인 서비스들은 상호호환이 어려우며, 서비스 효율성 및 이용자 편의성이 저하하는 등의 한계점이 존재한다.
- 또한, 기존 공공 분야에서 블록체인 서비스 구축 시의 개발편의성 부재, 사용자 경험 부재, 현행 기술 수준에서 블록체인 서비스 발굴 및 활성화 체계 부재의 문제점을 개선하기 위해 K-BTF를 기획하게 되었다.
- K-BTF는 블록체인 서비스를 공공분야의 수요기관에게 간편하게 제공함으로써 신뢰성과 효율성, 확장성을 보장하고, 이를 통해서 블록체인 기반 대국민 공공서비스의 품질과 생산성 향상 확보를 목표로 한다.

(2) 연구 목적 및 범위

- (가) **(공동인프라 도출)** 주요국 국가 블록체인 플랫폼 및 국내 KISA 주관 블록체인 시범사업 과제를 분석하여 K-BTF 공동인프라를 도출하고, 사용자 시나리오를 발굴하여 필요성 및 타당성의 근거를 마련한다. 또한, K-BTF 공동인프라 정립 후 수요기관, 사용자, 블록체인 기업 등 참여자 관점에서 예상되는 정량적, 정성적 기대효과를 도출한다.
- (나) **(실행로드맵 수립)** K-BTF 서비스 생태계를 마련하기 위해 실현가능한 수준의 단계적 추진계획인 ‘K-BTF 실행로드맵’을 마련한다. K-BTF 실행로드맵에 따라 세부 추진방안 및 서비스별 제안요청서

내 요구사항을 도출한다.

- (다) (공통규격검증체계 마련) 중장기적으로 신뢰할 수 있는 K-BTF 서비스가 활용·확산될 수 있도록 K-BTF 공통요구사항과 시험검증 체계를 마련한다.
- (라) (거버넌스 체계 구축) K-BTF 정책수립, 블록체인 공통요구사항 등을 논의하기 위한 거버넌스 협의체를 구성하고 운영방안을 마련한다.

3. K-BTF 공동인프라 정립

(1) K-BTF 공동인프라 도출

- 해외 주요 국가의 블록체인 국가 플랫폼 현황 분석 및 국내 블록체인 시범사업 과제를 분석하여 분산신원(DID), 디지털인증서(NFT), 데이터 이력추적, 데이터 진본확인, 직접구축(Blockchain as a Service, 이하 BaaS), 디지털 지갑을 K-BTF 공동인프라로 도출하였다.

(가) 분산신원 공동인프라

- 분산신원으로 구현된 분산신원 서비스를 다수의 수요기관에서 다양한 서비스에서 제공하고 이용할 수 있는 공동인프라

(나) 디지털인증서 공동인프라

- 대체불가소유권을 가지는 NFT 기반의 디지털인증서를 바탕으로 신분 위조, 자격증명 등 각종 문서의 위변조 방지 및 소유권 증명, 멤버십 등 다양한 응용 서비스가 가능한 공동인프라

(다) 데이터 이력추적 공동인프라

- 데이터에 관한 모든 변동 사항을 타임스탬프 형식으로 기록하여 문제 발생 시 이에 대한 책임소재, 규제 이행 여부 등을 투명하게 공개하여 신뢰성 보장이 가능한 공동인프라

(라) 데이터 진본확인 공동인프라

- 다수의 노드가 참여하는 합의 알고리즘 기반으로 블록체인에 저장된 데이터의 위변조를 방지하고 진위여부를 확인할 수 있는 공동인프라

(마) 직접구축(BaaS)

- 블록체인 서비스 및 개발환경을 수요기관에 제공하여 원하는 블록체인 서비스를 빠르게 추진할 수 있으며 기존 블록체인 네트워크, 플랫폼들과의 연계 및 통합된 형태의 데이터 신뢰성과 블록체인 서비스 제공이 가능한 공동인프라

(바) 디지털 지갑 서비스

- 블록체인 내 지갑 기능을 손쉽게 사용할 수 있도록 비밀키를 안전하게 관리, 보관할 수 있으며, 이용자 계정과 연결되어 다양한 블록체인 서비스를 제공하는 디지털 지갑 서비스

(2) K-BTF 실행 로드맵

(가) 1단계 K-BTF : 시범 도입 단계

- 1단계는 K-BTF 생태계 마련을 위해 실현 가능한 수준의 K-BTF 공동인프라를 선별하여 시범사업을 통해 우선 적용한다.
- 1단계 시범사업은 구축사업과 시범운영 단계로 구분되며, 대상 공동인프라는 분산신원 공동인프라와 디지털인증서 공동인프라이다.
- 구축사업의 경우 분산신원 공동인프라와 디지털인증서 공동인프라를 보유한 공급기업을 대상으로 모집한다.
- 해당 서비스를 이용할 정부기관, 관련 부처 등이 수요기관 대상이다.

(나) 2단계 K-BTF : 도입확대 단계

- 2단계는 1단계를 통해 마련된 K-BTF 서비스 생태계를 기반으로 공공분야의 개방 확대를 목표로한다.
- 2단계 대상은 1단계 서비스인 분산신원 공동인프라와 디지털인증서 공동인프라를 확대 도입하고, 2단계에서 시작하는 데이터 이력추적 공동인프라, 데이터 진본확인 공동인프라, 직접구축(BaaS)을 시범사업으로 추진한다.
- 2단계의 데이터 이력추적 공동인프라와 데이터 진본확인 공동인프라, 직접구축(BaaS)을 보유한 공급기업을 대상으로 모집·선발한다.
- 해당 서비스를 이용할 정부기관, 관련 부처 등이 수요기관 대상이다.

(3) K-BTF 공통규격검증체계

(가) 공통요구사항 마련

- 공통요구사항은 블록체인 기술 및 플랫폼이 가지는 특성이 서로 다르더라도 K-BTF 공동인프라의 주요 기능을 공통으로 수행하기 위한 최소요구사항을 정의한다. 특정 플랫폼에 대한 의존성을 낮추고 상호호환을 통해 민간 블록체인 플랫폼의 공정한 경쟁환경을 마련과 공공 서비스 분야의 블록체인 활성화를 위해 공통요구사항을 마련하였다.
- 수요기관에서 블록체인 서비스를 도입하기 위해서는 기획, 개발, 운영 뿐만 아니라 민간 기업의 기술력 활용, 보안 및 인증 등 여러 요소를 고려해야 하는 부담감을 가진다. 이러한 어려움을 해소하고 공공분야에 블록체인 기업 진출 및 서비스 도입 유연성을 확보할 수 있다.
- 해외 블록체인 플랫폼인 유럽의 EBSI, 독일 GAIA-X, 중국 BSN, 싱가포르 OpenAttestation, 캐나다 OrgBook의 사례를 분석하여 공통요구사항을 도출하였다.

(나) 시험검증체계 마련

- 시험검증체계는 K-BTF의 최소한의 보안 수준을 마련하여 안전하고 신뢰할 수 있는 K-BTF 서비스 생태계를 마련하기 위한 목적을 가진다. 민간기업이 운영중인 블록체인 플랫폼은 시험검증체계를 거쳐 공동인프라로 선정된다. 선정된 공동인프라를 수요기관에 제공한다. 수요기관은 공동인프라에 대한 보안, 인증 고민 없이 블록체인 서비스를 기획·구축할 수 있으며, 국민은 해당 블록체인 서비스를 안심하고 이용할 수 있다.
- 시험검증체계는 ISMS-P 인증제도, 클라우드 보안인증제도(CSAP), 행안부 행정기관 및 공공기관 정보시스템 구축 운영 지침, 해외 시험검증체계 준용 사례를 중심으로 조사하였다. 이에 K-BTF 시험검증체계는 신규 인증제도를 마련하는 것이 아니라 현행 인증제도를 활용하여 블록체인 기업의 부담을 덜고자 하였다.

(4) 거버넌스 체계 수립

- 거버넌스는 K-BTF의 기술 및 관리·운영 등에 관련된 전반적인 영역에 대한 의사결정을 내리는 협의체이다. 거버넌스는 K-BTF의 기술 및 운영 측면에서의 윤리성 및 공공성을 확보하기 위한 의사결정 체계와 절차를 수립하여 이용자(국민), 공공기관(수요), 블록체인기업(공급)을 보호하기 위한 기구로서의 역할을 수행한다.
- 거버넌스 협의체의 역할은 정책수립, 공통요구사항, 추진체계마련, 역할 수립, 협의체 구성을 수행한다.

(가) 거버넌스 협의체 역할

- (정책수립) 거버넌스의 목표와 목표 달성을 위한 의사결정 구조, 권한과 책임의 배분, 의사소통 및 협력 방식을 규정하고 장기적인 지속 가능성을 확보하는 데 매우 중요한 역할을 한다.
- (공통요구사항) K-BTF 공동인프라와 관련된 공통요구사항을 관리한다.
- (추진체계마련) K-BTF의 4가지 역할과 절차에 따라 추진체계를 마련한다.
- (역할수립) 협의체를 구성하는 조직과 구성원들의 업무를 규정한다.
- (협의체 구성) K-BTF의 기술적, 관리적 측면에서의 심의, 검증, 개선 권고를 수행하고 의사결정을 내리는 기구이며 블록체인 관련 분야의 전문가들과 KISA 사무국의 정부분과(수요), 민간분과(기업), 전문가(학계, 정출연 등)으로 구성된다.

(나) 거버넌스 주요 역할 및 절차

- (신규 핵심서비스 및 공동인프라 선정 절차) 신규 공동인프라를 추가로 지정하여 운영할 수 있도록 논의하여 결정하는 절차이다.
- (신규 참여 사업자 선정 절차) K-BTF 참여를 원하는 사업자가 있을 경우, 자격을 갖추었는지 평가하고 이에 준하는 경우 K-BTF 지위를 인정해주는 절차이다.
- (서비스 사고 발생 사업자 퇴출 절차) K-BTF 서비스 중단, 개인정보 유출 등 사고 발생 시, 현장 점검 및 실사 등을 통해 현황을 파악하고 탈퇴, 책임부여, 복원/조치 이행 완료 여부 등을 진행하는 절차이다.

- (수요기관 의견수렴 절차) 공공기관(수요), 블록체인기업(공급)으로부터의 서비스 품질, 사업자 가격담합 등 K-BTF의 서비스 품질 향상을 위한 다양한 의견을 접수하고 심의하는 절차이다.

4. 결론

- 해외 국가별 블록체인 플랫폼과 국내 블록체인 관련 공공·민간사업의 시사점 분석을 통해 블록체인 네트워크 파편화, 미비한 상호호환성, 자원 비효율성 등의 문제점 파악으로 K-BTF의 필요성이 대두되었다.
- K-BTF는 블록체인의 상호호환성, 신뢰성, 효율성, 확장성, 보안성, 공공성을 보장하며 체계적인 운영 기반의 분산신원 공동인프라, 디지털인증서 공동인프라, 데이터위·변조 공동인프라, 데이터 이력추적 공동인프라, 직접구축(BaaS), 디지털 지갑 서비스를 개발, 운영할 수 있는 다양한 환경을 제공한다.
- 기존 대비 효율적인 구축·운영으로 인한 경제성과 다양한 블록체인 신규 서비스 및 확산이 가능하여, 국가적인 블록체인 기술 발전과 산업 육성 효과 및 다양한 경제 효과를 유발할 것으로 기대된다.
- K-BTF는 1단계 시범사업과 2단계 확산사업형태로 진행될 예정이며, 블록체인을 활용한 사회적 가치 창출의 목표를 가지는 다양한 사업 추진에 활용이 가능하다.
- 공공기관(수요)은 구축·운영과 관련한 경제적 효과 창출 및 상호호환성 확보를 토대로 다양한 블록체인 신규 서비스 및 확장 서비스 제공이 가능할 것으로 기대된다.
- 이용자(국민)는 일관된 형태의 공공 서비스를 이용할 수 있어 높은 서비스 편의성과 개별 구축된 서비스 비용 대비 저렴한 서비스 사용이 가능하다.
- 블록체인공급자(기업)은 자체 구축한 블록체인 또는 K-BTF 공동인프라를 상호호환하여 손쉽게 공공 서비스 진입이 가능하며 일관된 형태의 공공 서비스를 구축, 운영할 수 있어 낮은 비용, 높은 신뢰성 보장이 가능한 서비스 제공 및 운영이 가능하다.
- 국가적인 측면에서는 블록체인 기술 발전 경쟁에 선제적 대비 및 산업 성장 동력 확보를 바탕으로 대국민 블록체인 서비스 인식 신뢰도 개선 및 경제성에 기여할 것으로 기대된다.

목 차

제 1 장. 서론	1
제1절. 추진배경	1
1. K-BTF의 개요	1
2. K-BTF의 목표 및 특성	4
제2절. 연구 목적 및 범위	6
1. 연구 목적	6
2. 연구 범위	6
제 2 장. K-BTF 공동인프라 정립	8
제1절. K-BTF 공동인프라 도출	8
1. 실수요 중심의 K-BTF 공동인프라 수립	8
2. K-BTF 공동인프라 개요	9
3. K-BTF 공동인프라 기대효과	19
제2절. K-BTF 실행 로드맵	23
1. 중장기 K-BTF 실행로드맵 구축	23
2. 실행로드맵 세부 추진 방안	25
제3절. K-BTF 공통규격검증체계	30
1. K-BTF 공통규격검증체계 개요	30
2. K-BTF 공통요구사항의 목적 및 필요성	30
3. K-BTF 시험검증체계의 목적 및 필요성	31
제4절. 거버넌스 체계 수립	32
1. 거버넌스 협의체 구성 및 운영	32
2. 거버넌스 주요 역할 및 절차	34
제 3 장. 결론	39
부록 1. 해외 블록체인 국가 플랫폼 현황 분석	41
부록 2. 국내 블록체인 과제 현황 분석	50
부록 3. K-BTF 공동인프라 참여자별 시나리오	80
부록 4. K-BTF 공통요구사항 마련	109
부록 5. K-BTF 시험검증체계 마련	155
참고문헌	172

표 목차

표 1. K-BTF 참여자별 역할 정의	2
표 2. 신규 공동인프라 선정 절차	35
표 3. 신규 참여 사업자 선정 절차	36
표 4. 사업자 퇴출 세부 절차	37
표 5. 수요기관 의견수렴 절차	38
표 6. 해외 주요 국가의 블록체인 공동인프라 도출	48
표 7. 국내 블록체인 과제 현황 분석을 통한 K-BTF 공동인프라 도출	70
표 8. 유럽 EBSI 기능 및 API	105
표 9. 독일 GAIA-X 기능 및 API	108
표 10. 중국 BSN 기능 및 API	109
표 11. 싱가포르 OpenAttestation 기능 및 API	111
표 12. 캐나다 OrgBook 기능 및 API	112
표 13. 공개키 타입 분류	115
표 14. 디지털인증서 주요 기능	123
표 15. 데이터 이력추적 주요 기능	129
표 16. 데이터 진본확인 주요 기능	134
표 17. 디지털 지갑 주요 기능	145
표 18. ISMS-P 인증항목	152
표 19. 클라우드보안인증 심사 항목	156
표 20. 소프트웨어개발보안 진단 항목	161
표 21. 기술적용계획표 항목 기준	163

그림 목차

그림 1. K-BTF 개념도	1
그림 2. K-BTF 도입 필요성	3
그림 3. K-BTF 배경	3
그림 4. K-BTF 공동인프라 모델 개념도	10
그림 5. 해외(EBSI, BSN)와 국내 K-BTF 공동인프라 범위 비교	18
그림 6. 국민(이용자) 관점의 K-BTF 공동인프라 기대효과	19
그림 7. 공공기관(수요) 관점의 K-BTF 공동인프라 기대효과	20
그림 8. K-BTF 실행로드맵	23
그림 9. 1단계 K-BTF 시범사업 모델(1~3차년도)	25
그림 10. 2단계 K-BTF 공공확산사업 모델(4~6차년도)	28
그림 11. K-BTF 공통규격검증체계 개요	30
그림 12. K-BTF 거버넌스 체계 개념도	34
그림 13. 신규 공동인프라 선정 절차	35
그림 14. 신규 참여 사업자 선정 절차	36
그림 15. 서비스 사고 발생 사업자 퇴출 절차	37
그림 16. 수요기관 의견수렴 절차	38
그림 17. 분산신원(DID) 공동인프라 서비스 시나리오	77
그림 18. 분산신원(DID) 블록체인 환경 예시	78
그림 19. 분산신원(DID)를 이용한 신원확인 서비스 예시	79
그림 20. 분산신원(DID)를 활용한 공공 서비스 예시	80
그림 21. 디지털인증서(NFT) 공동인프라 서비스 시나리오	82
그림 22. 디지털인증서(NFT) 블록체인 환경 예시	83
그림 23. 디지털인증서(NFT)를 이용한 증명서 확인 서비스 예시	84
그림 24. 디지털인증서(NFT)를 활용한 공공 서비스 예시	85
그림 25. 데이터 이력추적 공동인프라 서비스 시나리오	87
그림 26. 데이터 이력추적 블록체인 환경 예시	88
그림 27. 데이터이력추적을 이용한 유통 이력 확인 서비스 예시	89
그림 28. 데이터이력추적을 활용한 공공 서비스 예시	90
그림 29. 데이터 진본확인 공동인프라 서비스 시나리오	91
그림 30. 데이터 진본확인 블록체인 환경 예시	92
그림 31. 데이터진본확인을 이용한 증명서 위변조 확인 서비스 예시	93
그림 32. 데이터진본확인을 활용한 공공 서비스 예시	94

그림 33. 직접구축(BaaS) 예시	96
그림 34. 디지털 지갑 서비스 시나리오	97
그림 35. 디지털 지갑 블록체인 환경 예시	98
그림 36. 디지털 지갑 서비스 예시	99
그림 37. 디지털 지갑을 이용한 간편로그인 서비스 예시	99
그림 38. 디지털 지갑을 이용한 자격증명 서비스 예시	100
그림 39. 디지털 지갑을 이용한 신분증명 서비스 예시	100
그림 40. 디지털 지갑을 이용한 전세계약/전입신고 서비스 예시	100
그림 41. 디지털 지갑을 이용한 민원서류증명/조회 서비스 예시	101
그림 42. 디지털 지갑을 이용한 스마트티켓 서비스 예시	101
그림 43. 디지털 지갑을 이용한 세금납부증빙/영수증발행 서비스 예시	101
그림 44. 디지털 지갑을 이용한 도서대출 서비스 예시	102
그림 45. 디지털 지갑을 이용한 농축산물유통이력조회 서비스 예시	102
그림 46. 디지털 지갑을 이용한 수출입통관이력 조회 서비스 예시	102
그림 47. 디지털 지갑을 활용한 공공 서비스 예시	104
그림 48. NIST U.S Cyber Trust Mark	166

제 1 장. 서론

제1절. 추진배경

본 절에서는 블록체인 신뢰 프레임워크(Korea-Blockchain Trust Framework, 이하 K-BTF)의 개요, 목표 및 특성에 대해 기술한다.

1. K-BTF의 개요

□ K-BTF의 정의

- K-BTF는 공공분야에서 블록체인 기반 공공 서비스를 효율적으로 개발·운영하고 쉽게 상호호환할 수 있도록 지원하는 이용체계이다.



그림 1. K-BTF 개념도

- K-BTF는 참여자, 핵심서비스모델, 공동인프라, 공동인프라를 위한 공통요구사항, 시험검증체계, 운영거버넌스 등으로 구성되어있다.
- (참여자) K-BTF의 참여자는 공공기관(수요), 공급기업(블록체인 기업), 국민(이용자)로 이루어지며, 각 역할은 다음과 같이 정의한다.

참여자	역할
공공기관(수요)	별도 블록체인 플랫폼 구축없이 K-BTF를 이용하여 공공신원인증, 공공증명서 발급 및 진본확인 등 블록체인 공공 서비스를 간편하게 기획, 운영, 관리하는 참여자
공급기업 (블록체인 기업)	K-BTF를 이용 또는 자체 구축한 블록체인 네트워크와 K-BTF를 상호 호환하여 블록체인 공공 서비스를 구축, 운영하여 비즈니스 모델 확보를 통한 경쟁력 확보가 가능한 참여자
국민(이용자)	공공기관(수요)를 통해 제공되는 블록체인 서비스를 이용하여 디지털 지갑, 증명서 발급, 인증, 공공기관 출입 등 서비스를 이용하는 참여자

표 2. K-BTF 참여자별 역할 정의

- (K-BTF 공동인프라) 공공분야에서 블록체인 기반 공공 서비스를 구축, 운영할 수 있는 서비스 모델이며 개발, 운영에 필요한 다양한 블록체인 기능 및 개발 환경이다.
- (공통요구사항) K-BTF 공동인프라가 갖추어야 할 기능 및 비기능 요구사항이다.
- (시험검증체계) K-BTF 공동인프라를 통해 공공기관이 블록체인 서비스를 제공하는데 요구되는 자격 여부를 제3기관을 통해 검증하는 체계이다.
- (운영거버넌스) K-BTF의 정책수립, 공통요구사항관리, 추진체계 마련, 역할 수립 및 협의체 운영을 통한 신뢰성있는 K-BTF 관리 체계이다.

□ K-BTF 도입 필요성

- K-BTF 현재 구축된 블록체인 공공서비스의 블록체인간 상호호환 불가, 서비스 효율성 저하, 중복투자우려의 한계를 극복하고 비용 절감, 개발편의성 증가, 사용자 경험 향상을 목적으로 한다.

블록체인 개별 구축의 한계를 극복하기 위한 혁신적 시도



그림 2. K-BTF 도입 필요성

- K-BTF는 현재 구축된 블록체인 공공서비스의 블록체인 간 상호 호환 불가, 서비스 효율성 저하, 중복투자분야의 한계를 극복하고 현행 제도, 현행 기술 수준에서 블록체인 서비스 발굴 및 활성화에 필요한 체계를 제공한다.

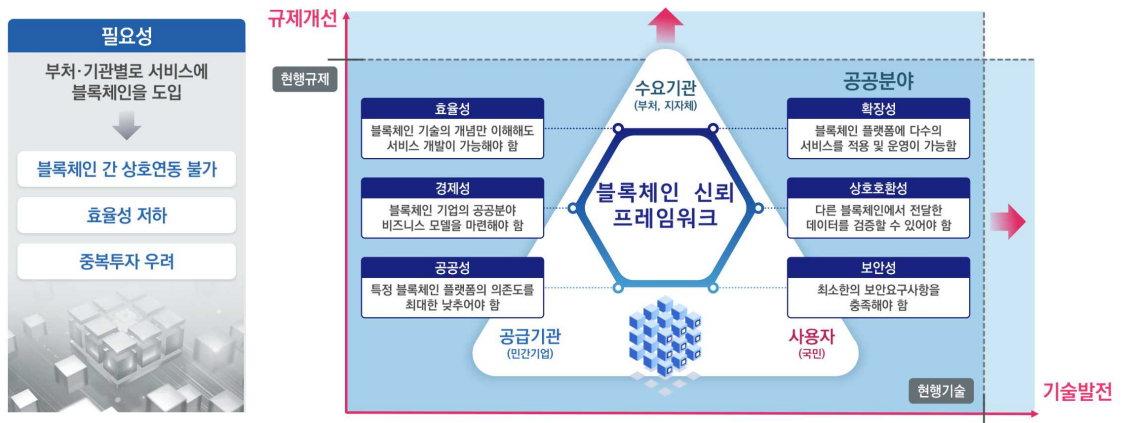


그림 3. K-BTF 배경

- K-BTF 공동인프라는 공공기관이 블록체인 플랫폼을 직접 구축하지 않고, K-BTF를 이용하여 간편하게 블록체인 서비스를 구축할 수 있도록 지원한다. 공공기관은 K-BTF 공동인프라 중 적합한 블록체인 플랫폼을 선택하여 활용할 수 있다.
- K-BTF는 분산신원(DID), 디지털인증서(NFT), 데이터 이력추적, 데이터 진본확인, 직접구축(BaaS), 디지털 지갑 서비스 등 6종의 공동

인프라를 제공한다. 공동인프라는 블록체인 기술과 산업 변화에 따라 추가되거나 변동될 수 있다.

- K-BTF의 공통요구사항, 시험검증체계, 거버넌스는 참여자들이 안전하고 신뢰성 있게 활용할 수 있도록 기준과 검증 그리고 이를 위한 거버넌스를 제공하여 공공 또는 민간 활용에 필요한 신뢰성 확보를 목적으로 한다.
- 블록체인 플랫폼에 관계없이 동일한 기능을 수행할 수 있도록 공통요구사항을 정의하여 민간기업의 블록체인 플랫폼의 기술 의존성을 낮춘다. 공통요구사항을 준수하는 블록체인 플랫폼은 상호호환을 지원한다.
- 시험검증체계는 안전하고 신뢰성 있는 K-BTF를 마련하기 위해 블록체인 플랫폼이 가지는 최소한의 보안 신뢰성을 확보한다.
- 거버넌스는 K-BTF 전반의 영역에 대한 의사결정 조직이다.

2. K-BTF의 목표 및 특성

□ K-BTF의 목표

- K-BTF는 블록체인 서비스를 공공기관 및 대국민에게 제공함으로써 신뢰성과 효율성 및 확장성을 보장하고, 이를 통한 블록체인 기반 대국민 공공서비스의 품질 및 생산성 향상 확보를 목표로 한다.
- 블록체인 기반 공공 서비스를 효율적으로 개발·운영하고, 쉽게 상호 호환할 수 있는 K-BTF의 종합적인 실행·추진 체계를 마련하고자 한다.

□ K-BTF의 특성

- K-BTF는 고유한 6가지의 특성을 가진다.
 - (1) (효율성) K-BTF는 수요기관이 블록체인 서비스 기획에 집중할 수 있는 개발·이용 환경을 제공한다. 이는 수요기관이 블록체인 서비스 개발을 위해 요구되는 높은 수준의 기술이해 없이도 간편한 기능만으로 손쉽게 블록체인 서비스를 효율적으로 기획·개발이 가능하다.
 - (2) (경제성) K-BTF를 이용하여 개발한 블록체인 서비스는 수요기관에서 제공하는 핵심서비스뿐만 아니라 지속 확장 가능한 구조를 갖는다.

수요기관이 다양한 블록체인 서비스의 도입 및 서비스 추가, 확장이 용이하도록 보장하고 민간기업은 공공서비스의 비즈니스 모델을 마련할 수 있다.

- (3) (상호호환성) K-BTF로 개발한 블록체인 서비스는 플랫폼에 관계없이 데이터를 발행하고, 조회하고, 검증하는 등 K-BTF 서비스 간 호환성을 제공한다.
- (4) (신뢰성) K-BTF는 공공기관의 데이터를 블록체인 메인넷에 저장하며, 데이터는 위조 또는 변조되지 않도록 무결성을 제공한다. 공동인프라에는 검증 목적의 공개 가능한 정보만을 저장하여 사용자 프라이버시를 보호하여 신뢰성을 제공한다.
- (5) (보안성) K-BTF에서 제공하는 블록체인 공동인프라는 공공분야를 위한 공통요구사항, 시험검증체계를 준수하는 플랫폼에 한하여 제공함으로써 수요기관이 서비스를 이용하는 과정에서 발생하는 정보에 대해 일정 수준 이상의 보안성을 보장한다.
- (6) (공공성) K-BTF는 민간의 블록체인 기술을 공익 목적으로 활용할 수 있도록 우수한 기술력을 지원한다. 또한, K-BTF는 민간기업의 블록체인 기술의 의존성을 낮추고 공정한 경쟁환경을 조성하여 수요기관에게 양질의 블록체인 서비스 이용환경을 제공한다.

제2절. 연구 목적 및 범위

1. 연구 목적

- 본 연구는 블록체인 기반 공공 서비스를 효율적으로 개발·운영하고, 쉽게 상호호환 할 수 있는 K-BTF를 마련하는데 목적이 있다.

2. 연구 범위

- 연구 범위는 첫째, K-BTF 공동인프라 정립, 둘째, 단계적 추진을 위한 실행 로드맵 수립, 셋째, 안전하고 신뢰할 수 있는 K-BTF 공동인프라 확보를 위한 시험검증체계 마련, 넷째, 체계적인 K-BTF 운영을 위한 협력체계 구축 순으로 진행한다.
- (1) **(공동인프라 모델)** 공공분야 수요기관의 수요가 높은 K-BTF 공동인프라 모델을 선정하고 이를 토대로 K-BTF 공동인프라를 정립한다.
 - 해외 주요국가의 블록체인 모델을 분석하여 주요 공동인프라를 도출한다.
 - 블록체인 기술이 다양해짐에 따라 KISA 주도로 진행된 블록체인 시범사업('21~'22년) 34개 과제를 분석하여 주요 공동인프라를 도출한다.
 - 그간 정부 블록체인 시범사업 서비스 분석과 수요기관·전문가 등의 의견수렴을 추진하여 실수요 중심의 K-BTF 공동인프라를 정립한다.
 - K-BTF 공동인프라별 사용자 시나리오를 발굴하고 각 서비스 모델 간 상호호환성, 활용성 등을 고려한 필요성 및 타당성 근거를 마련한다.
 - K-BTF 공동인프라 정립 후 수요기관, 사용자, 블록체인 기업 등 참여자 관점에서 예상되는 정량적, 정성적 기대효과를 도출한다.
- (2) **(실행로드맵 수립)** K-BTF 서비스 생태계를 마련하기 위해 실현가능한 수준의 단계적 추진계획인 'K-BTF 실행로드맵'을 마련한다.
 - 블록체인 시범사업에 K-BTF를 단계적으로 우선 적용하고, 이후 공공분야 전체로 K-BTF 개방·확대 추진하는 실행로드맵을 마련한다.
 - K-BTF 서비스를 마련하기 위한 중장기적 관점에서 실행로드맵 마일스톤에 따라 세부 추진방안을 도출한다.
 - K-BTF를 시범사업에 적용하기 위한 공동인프라 우선순위 및 단계적

확대방안을 마련한다.

- 수요기관이 K-BTF를 이용하는 경우 이용 프로세스와 각 프로세스별 주요사항을 도출한다.
- K-BTF 초기 시범운영을 위한 민간 플랫폼을 선정하기 위한 기능, 성능, 보안성 등 ‘K-BTF 공통요구사항’을 마련한다.
- K-BTF 공통요구사항은 네트워크 성능, 서비스별 기능 요건, 데이터, 보안 등을 제시한다.

(3) **(시험검증체계 마련)** 증장기적으로 신뢰할 수 있는 K-BTF 서비스의 활용·확산될 수 있도록 K-BTF 시험검증체계 거버넌스 방안을 마련한다.

- 민간 블록체인 서비스를 평가하고 K-BTF로 인증하기 위한 정책·인증심사기관 등의 K-BTF 시험검증체계 구축안을 마련한다.
- K-BTF 공동인프라 시범운영부터 인증기업 선정까지 각 단계별 추진 계획 및 시험검증체계 거버넌스 역할 등의 실행계획 마련한다.

(4) **(거버넌스 체계 구축)** K-BTF 정책수립, 공통요구사항 등을 논의하기 위한 거버넌스 협의체 구성 및 운영방안 마련한다.

- 거버넌스 분과(정부, 민간) 별 예상 참여주체 및 주요역할, 논의 안건 등 거버넌스 협의체 구성과 실제 운영에 대한 체계 설정한다.

제 2 장. K-BTF 공동인프라 정립

제1절. K-BTF 공동인프라 도출

본 절에서는 K-BTF가 제공하는 공동인프라에 대해 기술한다.

1. 실수요 중심의 K-BTF 공동인프라 수립

(1) 해외 주요국가의 블록체인 국가 플랫폼 현황 분석

- 유럽, 중국, 싱가포르 등 해외 주요 국가들은 국가 차원에서 블록체인 기술을 도입하여 대국민 서비스를 제공하고 있다.
- 해외 주요국가의 블록체인 플랫폼 현황을 분석하여 중요도가 높은 서비스를 중심으로 블록체인 국가 플랫폼의 구축현황, 목표, 주요 서비스 등을 중점으로 분석하고 중요도가 높은 서비스를 중심으로 K-BTF 공동인프라 후보 리스트를 도출하였다.
- 해외 주요국가의 블록체인 플랫폼 현황 분석 결과로 도출된 공동인프라는 분산신원 3건, 디지털인증서 3건, 데이터 이력추적 3건, 데이터 진본확인 4건, 디지털 지갑 1건, 직접구축(BaaS) 6건, 데이터 주권 1건, 전자영주권 1건, 전자선거 1건으로 집계되었다.
- 해외 주요국가의 블록체인 국가 플랫폼 현황 분석을 통해 도출된 공동인프라 도출 과정은 ‘부록 1. 해외 블록체인 국가 플랫폼 현황 분석’을 참고하기 바란다.

(2) 국내 블록체인 과제 현황 분석을 통한 공동인프라 도출

- 해외 주요국가의 블록체인 플랫폼 분석 과정에서 도출된 9개 공동인프라를 기준으로 국내 블록체인 사업을 분석하고 최종 K-BTF 공동인프라를 도출한다.
- 국내 블록체인 현황 분석 대상은 2021~2022년 진행된 KISA 34개 과제이며, 각 과제별 사업 목표, 사업 내용, 주요 성과 및 주요 서비스를 중심으로 분석을 진행하였다.

- 국내 블록체인 과제 현황 분석을 통해 도출된 공동인프라 분석 결과는 분산신원 19건, 디지털인증서 18건, 데이터 이력추적 17건, 데이터 진본확인 17건, 디지털 지갑 7건, 직접구축(BaaS) 4건, 전자선거 2건으로 집계되었다.
- 국내 블록체인 과제 현황 분석을 통한 공동인프라 도출 상세 내용은 ‘부록 2. 국내 블록체인 과제 현황 분석’을 참고하기 바란다.

(3) 최종 K-BTF 공동인프라 도출

- 해외 주요국가의 블록체인 플랫폼 후보 분석 결과 도출된 9개 공동인프라와 2021~2022년 국내 KISA에서 추진된 주요 블록체인 사업을 분석한 공동인프라 분석 결과를 종합하여 분산신원, 디지털인증서, 데이터 진본확인, 데이터 이력추적, 디지털 지갑, 직접구축(BaaS), 전자선거의 7개 공동인프라를 도출하였다.
- 도출된 7개 공동인프라 중 전자선거를 제외하고, 최종적으로 분산신원, 디지털인증서, 데이터 이력추적, 데이터 진본확인, 직접구축(BaaS), 디지털 지갑까지 총 6개를 K-BTF 공동인프라로 수립하였다.
- K-BTF 공동인프라 중 분산신원과 디지털인증서에 대한 용어의 명확한 구분을 위해 아래와 같이 정의한다.

구분	분산신원	디지털인증서
의미	Decentralized ID	Digital certificate
개요	<p>< Authentication ></p> <p>사용자의 신원을 증명하는 것 예) 로그인한 사용자는 인증된 사용자</p>	<p>< Certification ></p> <p>자격(자격증)을 증명한다는 의미임. 정해진 규격에 따라 검증, 평가 후 이에 부합하는 경우 인증(마크)이 부여하나 신원증명 의미는 아님</p>

- 본 보고서에서는 분산신원은 Authentication의 의미로, 디지털인증서는 Certification의 의미로 사용한다.

2. K-BTF 공동인프라 개요

- K-BTF 공동인프라란 블록체인을 구성하는 여러 가지 기술들과 K-BTF를 이용하여 공공기관이 대국민 블록체인 공공 서비스를 손쉽게

- 개발, 운영할 수 있는 기능을 제공하는 블록체인 서비스로 정의한다.
- K-BTF 공동인프라는 앞서 도출한 5개 공동인프라에 대해 참여자인 공공기관(수요), 공급기업(블록체인 기업), 국민(이용자)을 위한 블록체인 공동인프라(플랫폼)를 활용할 수 있도록 한다.
 - K-BTF 공동인프라의 참여자별 역할은 다음과 같이 정의할 수 있다.
 - 공공기관(수요)은 NFT 디지털배지, DID신분증명, 각종 증명서 및 데이터 이력관리 및 추적 등 공공 서비스 목적의 다양한 서비스를 기획하고 국민(이용자)에게 제공한다.
 - 공급기업(블록체인기업)은 각 사가 보유한 블록체인 네트워크와 K-BTF 공동인프라를 연계하여 합의알고리즘 상호호환 및 스마트계약 상호호환을 수행하여 공공 블록체인 서비스 모델 확보와 블록체인 공동인프라의 개발, 구축 및 운영을 담당한다.
 - 국민(이용자)은 상호호환이 가능한 디지털 지갑 서비스를 통해 DID, NFT를 소유하고, 공공 서비스를 이용한다.
 - K-BTF 공동인프라 개념도를 통해 공공기관(수요), 공급기업(블록체인기업), 국민(이용자) 간의 역할을 설명한다.



그림 4. K-BTF 공동인프라 모델 개념도

- 다음은 K-BTF 공동인프라 모델 수립 단계에서 도출된 6개의 K-BTF 공동인프라에 대한 이해를 위해 서비스 개요와 필요성을 중심으로 설명한다.

(1) 분산신원(Authentication) 공동인프라

(가) 서비스 개요

- 블록체인을 기반으로 온라인에서 신원 또는 자격증명 시 이용자가 증명 목적에 필요한 정보만을 선택하여 검증 기관에 제공함으로써 자기주권과 개인정보보호를 강화할 수 있는 디지털 신원확인 서비스를 의미한다.

(나) 필요성

- 분산신원 공동인프라는 개인의 신원 정보를 분산된 방식으로 관리하여 안전하고 투명하게 관리할 수 있으며, 다양한 상황에서의 신원증명 시 유용하게 활용할 수 있다.
 - (개인정보 보호 강화) 기존의 중앙집중식 신원증명은 신원정보를 중앙 기관에 집중적으로 보관함으로써 개인정보 유출의 위험이 높으나 분산신원은 개인이 자신의 신원 정보를 직접 관리함으로써 개인정보 유출을 예방할 수 있다.
 - (서비스 이용 편의성 향상) 기존의 중앙집중식 신원증명은 서비스마다 신원정보를 등록하고 인증해야 하는 번거로움이 있으나, 분산신원은 개인이 하나의 신원정보로 다양한 서비스를 이용할 수 있어 편리하다.
 - (신원정보 활용성 확대) 분산신원은 개인이 자신의 신원 정보를 직접 관리하기 때문에, 개인의 신원정보를 보다 폭넓게 활용할 수 있다.
 - (개방성 환경) 분산신원은 개방형 표준을 기반으로 구축가능하여 서비스와 플랫폼에서 통합적으로 사용할 수 있다.
- 분산신원(Authentication) 공동인프라는 다수의 지원 사업들을 통해 개별적으로 구축 운영되고 있으나, 각 공공기관(수요)별 DID를 사용하여 비용·기간, 운영관리의 비효율이 발생하고 이용자 입장에서 여러가지 DID 서비스에 가입해야하는 불편함이 존재한다.
- 신원증명을 활용한 신분증(조폐공사), 시민권(성남시) 등의 프로젝트가 추진되고 있으나, 공공서비스에서의 교육이력, 고용정보, 자격증명 등 공공 서비스 전반으로 사용 가능한 통합환경이 필요하다.

(2) 디지털인증서(Certification) 공동인프라

(가) 서비스 개요

- 대체불가토큰(NFT: Non-Fungible Token)을 가지는 디지털인증서를 바탕으로 신분 위조, 자격 증명 등 각종 문서의 위·변조 방지 및 다양한 응용(디지털 배지, 디지털 콘텐츠, 특허 등 지적재산권 거래 등)이 가능한 서비스이다.
- 신분 위조, 가짜 증명서 및 인증서 등 각종 문서의 위·변조가 불가능하고 누구나 출처, 발행, 소유자를 확인 가능한 대체불가토큰을 활용한 디지털인증서를 통해 투명성을 확보한다.

(나) 필요성

- 디지털인증서 공동인프라는 전자문서에 서명하거나, 온라인에서 본인(또는 본인 소유)임을 확인하는 목적으로 주로 활용 가능하다.
 - (데이터 무결성 보장) 디지털인증서는 문서나 데이터가 위조나 변조되지 않았음을 보장하고 신뢰성을 확보할 수 있다.
 - (소유권 보호) 디지털 자산은 복제나 위조가 쉬워 소유권을 보호하기 어려우나 디지털인증서를 이용하면 디지털 자산의 소유권을 기록하여 디지털 자산의 소유권을 보다 안전하게 보호할 수 있다.
 - (편리성) 디지털인증서를 사용하면, 전자문서에 서명하거나, 온라인에서 본인(또는 본인 소유)임을 확인하는 과정이 간편해진다.
 - (보안성) 디지털인증서는 강력한 암호화 기술을 사용하여 개인의 디지털 자산을 보호하고 이를 통해 개인의 정보를 안전하게 보호할 수 있다.
 - (효율성) 디지털인증서를 사용하면, 전자문서의 유효성 검증이나, 온라인에서의 확인 과정이 효율적으로 이루어져 업무 효율성이 높아진다.
- 디지털 시장 경제의 한 축으로 자리매김한 디지털인증서에 대한 수요가 증가되어 공공서비스 영역에서도 각 수요기관 별로 NFT를 활용한 다양한 서비스가 제공되고 있으나 데이터간의 상호호환성이 부족하여 통합된 기반환경 마련이 필요하다.

- 이러한 문제를 해결하기 위해서 디지털인증서 생성, 소유권 조회, 이력관리 및 폐기까지의 기능을 제공하여 기존과 대비한 운영 효율성 개선이 필요하다.
- 디지털인증서를 제공하는 기존의 블록체인 서비스는 지속적인 투자 및 운영 비용이 요구될 뿐 아니라 이에 대한 효용성 또한 떨어진다는 한계점이 존재한다.

(3) 데이터이력추적 공동인프라

(가) 서비스 개요

- 블록체인 내 저장된 데이터가 변경된 경우 원본 대조를 통한 변경 혹은 데이터 사용 이력 등을 제공하고 데이터의 유효성을 제공하는 서비스이다.
- 상호호환 가능한 블록체인 환경에서 각 공공기관별로 저장된 데이터의 모든 변동 사항을 타임스탬프 형식으로 기록하여 문제 발생 시 이에 대한 책임소재, 규제 이행 여부 등을 투명하게 공개하여 신뢰성 보장이 가능한 서비스이다.

(나) 필요성

- 데이터이력추적 공동인프라는 데이터가 생성, 수정, 삭제된 이력을 추적하고, 이를 통해 데이터 변경 내역 파악과 데이터 무결성 확인 용도로 주로 사용된다.
 - (데이터 무결성 확보) 데이터이력추적 서비스를 통해 데이터의 변경 내역을 파악하여 데이터의 무결성을 확보한다. 데이터가 무단으로 변경되거나 삭제되었다면, 데이터의 무결성이 훼손되었다고 판단한다.
 - (데이터 책임 소재 규명) 데이터 변경 내역을 파악하여 책임 소재를 규명할 수 있다.
 - (데이터 위변조 탐지) 데이터이력추적 서비스를 통해 데이터의 변경 내역을 파악하고 데이터 신뢰성 여부를 판단한다.
 - (데이터 감사) 데이터 변경 내역을 분석하여 데이터 사용 패턴이나 이상 징후를 파악, 이를 통해 데이터 분석 및 감사를 수행할 수 있다.

- 공공기관이 개별 블록체인을 활용하여 데이터이력추적을 제공하고 있으나, 상호호환성 부재로 인해 개별 블록체인 네트워크 내에서만 이력 추적이 가능하여 유관기관과의 데이터 접근성에 한계가 존재한다.
- 기존의 데이터이력추적의 한계를 극복하기 위해서는 블록체인 인프라 환경을 상호호환하여 공공 데이터 및 민간 서비스 영역까지의 데이터 이력추적이 필요하다.

(4) 데이터진본확인 공동인프라

(가) 서비스 개요

- K-BTF를 사용하는 공공기관에 저장된 데이터에 대한 위·변조 행위 방지하고 검증하는 서비스이다. 블록체인에 저장된 데이터를 위·변조 하기 위해서는 합의 알고리즘에 참여하는 다수 노드를 직접 공격해야만 하는데, K-BTF 데이터위·변조 공동인프라는 이러한 신뢰성이 보장 되는 노드에서 저장되는 데이터의 보안성과 신뢰성을 제공한다.

(나) 필요성

- 데이터진본확인 공동인프라는 데이터가 위조나 변조되지 않았음을 확인하는 용도로 주로 사용되며, 데이터 신뢰성 확보, 데이터 위/변조와 관련된 다양한 분야에 활용 가능하다.
 - (데이터 신뢰성 확보) 데이터의 위조나 변조 여부를 확인할 수 있으므로, 데이터의 신뢰성을 확보하여 데이터를 활용한 의사 결정이나 업무 수행을 보장한다.
 - (데이터 위/변조에 따른 피해 예방) 데이터의 위조나 변조 여부를 확인하여 공공증명서, 계약 체결, 공공서비스 이용 등 다양한 분야에서 피해 예방 가능하다.
 - (데이터 감사) 데이터 위변조 여부를 분석하여 진본 데이터와의 비교를 통한 감사 자료로 활용할 수 있다.
- 공공기관별 블록체인 환경에서 데이터 위·변조를 방지하기 위한 체계를 갖추고 있다. 하지만, 기관별 블록체인 서비스들은 각자 구축 및 운영 되어 있고, 상호호환성이 존재하지 않아 서비스 신뢰도 하락과 업무

비효율성이 발생한다.

- 공공기관별로 요구하는 데이터 구조가 상이하여 이로 인한 서비스 확장이 어려운 구조이며, 데이터 간의 상호호환성을 확보하여 서로 다른 블록체인 간의 데이터를 참조하여 위·변조 유무를 판별할 수 있도록 다양한 데이터 형식에 대응이 필요하다.

(5) 직접구축(BaaS)

(가) 서비스 개요

- 직접구축(BaaS)은 EBSI, BSN 등과 유사한 방식으로 클라우드 기반에서 개방형 블록체인을 구축하여 이더리움, 하이퍼레저 등 다양한 플랫폼의 메인넷 운영을 목적으로 하는 블록체인 플랫폼이다.
- 직접구축(BaaS)을 중심으로 블록체인 네트워크를 연계하고 통합된 서비스 환경을 제공한다. K-BTF 공동인프라와 개발 환경을 활용하여 공공기관이 원하는 서비스를 빠르게 추진할 수 있으며, 기존 블록체인 플랫폼 및 메인넷들과의 연계를 통해 공공 데이터 및 민간 서비스 영역까지의 통합된 형태의 데이터 신뢰성과 블록체인 서비스를 제공한다. 또한 직접구축(BaaS)은 K-BTF 공동인프라에서 제공하지 않는 서비스를 실험적으로 구축하기를 원하는 경우에도 사용이 가능하다.

(나) 필요성

- 직접구축(BaaS)은 공공기관이나 지자체 등이 블록체인 서비스를 구축, 운영할 수 있도록 지원하며 다음과 같은 목적으로 주로 활용된다.
 - (구축 비용 절감) 직접구축(BaaS)을 이용하여 블록체인 플랫폼을 직접 구축하고 관리할 필요가 없으며, 이에 대한 비용을 절감할 수 있다.
 - (시간 단축) 블록체인 기반 공공서비스를 보다 빠르게 출시하고 확장할 수 있고, 직접구축(BaaS)에서 제공하는 개발 도구와 블록체인 서비스를 활용하여 공공기관에 맞는 최적 서비스 제공이 가능하다.
 - (전문성 확보) 공공기관 담당자나 이용자는 블록체인 기술에 대한 전문성 없이도 블록체인 기반의 서비스를 구축, 운영, 활용할 수 있다. 직접구축(BaaS)은 블록체인 기술에 대한 전문성을 보유한 기업이 구축,

운영하므로, 서비스의 신뢰성을 확보할 수 있다.

- (확장성) 직접구축(BaaS)은 이용량 증가에 따라 블록체인 인프라를 쉽게 Scale-in/out 할 수 있다. 직접구축(BaaS)은 클라우드 기반의 블록체인 인프라를 제공하여, 트래픽 증가에 유연하게 대처 가능하다.
- (안정성) 블록체인 플랫폼의 안정성을 위해 다양한 보안 및 관리 기능을 제공하고, 안정적으로 운영할 수 있도록 환경을 제공한다.
- 공공기관에서 진행했던 대부분의 블록체인 관련 사업은 블록체인 기술을 이용하여 자체 시스템, 프라이빗 클라우드, 퍼블릭 클라우드 등 다양한 형태로 구축되어 관리 및 운영 상의 비효율성을 개선할 필요가 있다.
- 공공기관별 유사한 형태의 블록체인 서비스들 각자의 블록체인을 활용하여 구축하여 자체 신원증명, 데이터이력추적, 데이터진본 확인 등의 서비스를 제공하여 블록체인 간의 상호호환성이 존재하지 않아 타 기관의 데이터를 신뢰하기 어렵다.
- 이용자 입장에서 공공서비스별로 별도의 시스템에 접근하여 서비스를 이용해야 하는 불편함이 존재하여 개선이 필요하다.

(6) 디지털 지갑 서비스

(가) 서비스 정의

- 다수의 기관에서 블록체인을 활용하여 발행된 신분정보, 자격정보 등을 통합된 하나의 디지털 지갑으로 이용할 수 있는 서비스이다. 디지털 지갑의 주요한 기능(키 관리, 트랜잭션 전송 및 서명 등)을 하나의 디지털 지갑 앱을 통해 유용하게 사용할 수 있다.
- 디지털 지갑에서 블록체인 이용자 계정은 공개키와 비밀키로 분리하여 관리된다. 이중 비밀키는 블록체인에서 트랜잭션을 전송하기 위한 유일한 수단으로 블록체인 생태계에서 가장 핵심적인 요소이자 보안이 필수적인 요소이다. 비밀키를 분실할 경우 이용자는 계정에 접근할 수 없으며, 혹은 타인에게 노출될 경우 자신의 계정에 대한 소유권을 영구히 잃게 된다. 따라서 디지털 지갑의 핵심 기능은 이용자의 안전한

키 관리, 다양한 형태의 개인별 데이터 보관 및 관리, 그리고, 서비스 요청 및 검증에 관련된 트랜잭션을 수행할 수 있는 기능을 제공한다.

(나) 필요성

- 디지털 지갑 서비스는 개인키, DID, NFT, 디지털 콘텐츠를 보관하고 관리하는 서비스로 다음과 같은 목적으로 사용한다.
 - (편리성) 이용자는 하나의 디지털 지갑 앱을 통해 자신의 디지털 자산을 한 곳에서 관리할 수 있으며, 이는 편의성과 관리 효율성을 높인다.
 - (보안) 디지털 지갑 서비스는 보안 키, 인증 코드, 2단계 인증 등을 제공하여 무단 액세스로부터 보호할 수 있다.
 - (접근성) 단일 지갑앱 형태로 온라인 또는 모바일 기기를 통해 언제 어디서나 서비스를 사용할 수 있다.
 - (새로운 서비스 제공) 디지털 지갑은 새로운 블록체인 공공서비스에도 별도의 앱설치 없이도 이용 가능하다.
- 공공기관에서 발행하는 신분정보와 자격정보 등의 디지털인증서 서비스가 확산됨에 따라 민간분야의 디지털 지갑과 연계하여 사용자의 편의성을 증대할 필요성이 있다.
- 공공기관별 발행한 신분정보와 자격정보 등의 디지털인증서 서비스를 다수의 디지털 지갑에 발행, 보관, 관리하여 이용자 입장에서는 편의성 개선이 필요하다.

□ 해외(EBSI, BSN)와 국내 K-BTF 공동인프라 범위를 비교하면 다음과 같다.



그림 5. 해외(EBSI, BSN)와 국내 K-BTF 공동인프라 범위 비교

(1) 해외(EBSI, BSN)와 국내 K-BTF 공동인프라 범위 개요

- 해외(EBSI, BSN)의 관리영역은 블록체인 공급(기업)을 중심으로 블록체인 네트워크, 블록체인 코어, 블록체인 API/SDK/외부 인터페이스, 그리고 핵심서비스를 포함한다.
- 국내 K-BTF 공동인프라의 경우 관리영역은 블록체인 API/SDK/외부 인터페이스와 핵심서비스로, 민간영역은 블록체인 코어와 블록체인 네트워크로 구분한다.

(2) 국내 K-BTF에서 관리영역과 민간영역 범위를 구분하는 이유

- 해외(EBSI, BSN)의 관리영역은 블록체인 공급(기업)이 블록체인 네트워크부터 핵심서비스까지 모든 영역을 개발, 운영하는 반면, K-BTF는 핵심서비스와 블록체인 API/SDK/외부 인터페이스만을 관리영역에 두어 블록체인 코어 및 블록체인 네트워크는 민간영역으로 구분하고 있다.
- K-BTF 공동인프라에서 관리영역과 민간영역을 구분하는 이유는 다음과 같다.
- K-BTF 핵심서비스와 블록체인 API/SDK/외부 인터페이스를 제외한 블록체인 코어, 블록체인 네트워크는 다양한 블록체인 공급(기업)과 다양한 공공 서비스를 구축, 운영하고 있으며, 각 영역에서의

블록체인 서비스를 통해 블록체인 시장을 확대해 나가고 있다.

- 이에 K-BTF는 핵심서비스와 블록체인 API/SDK/외부 인터페이스만을 관리범위에 두어 신뢰성있는 K-BTF를 제공할 수 있도록 할 뿐만 아니라, 민간영역이 K-BTF를 활용 시 필요한 기술 및 서비스를 제공하여 레퍼런스 확보와 기술경쟁력 제고에 적극 활용할 수 있도록 환경을 마련하기 위함이 목적이다.

3. K-BTF 공동인프라 기대효과

(1) K-BTF 공동인프라 참여자별 기대효과

- K-BTF 공동인프라에 참여하는 참여자인 공공기관(수요), 공급기업(블록체인기업), 국민(이용자)별 기대효과는 다음과 같이 정리하였다.

(가) 국민(이용자)

- K-BTF와 호환되는 통합 디지털 지갑 앱을 통해 공공에서 발행하는 디지털신분증, 증명서 등을 발급받고 관리할 수 있다.
- 공공서비스 목적에 따라 민원, 관공서 출입, 각종 증명서 발급, 신분증, 공공안전 영역에서 다양한 공공서비스를 제공받을 수 있다.

! 국민은 K-BTF 호환 **디지털 지갑 하나**로 공공에서 발행하는 디지털 신분증, 증명서 등을 **발급받고 직접 관리 가능함**

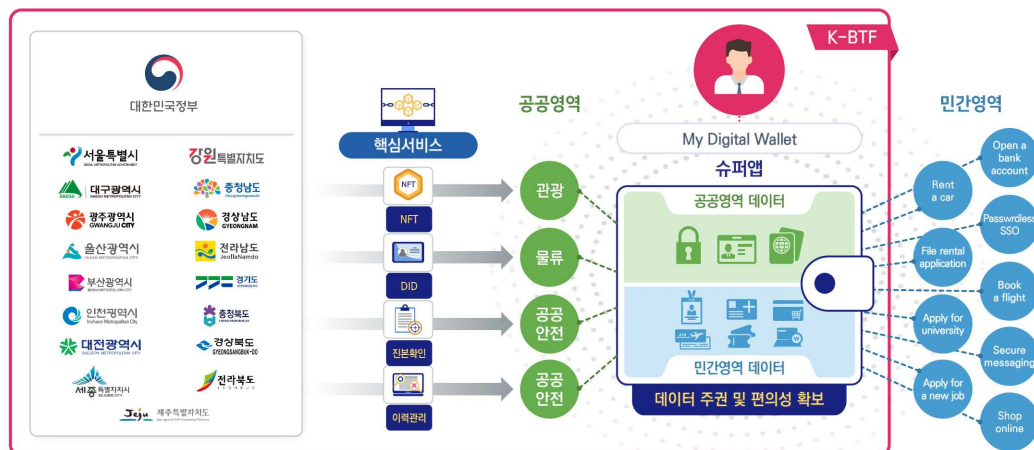


그림 6. 국민(이용자) 관점의 K-BTF 공동인프라 기대효과

(나) 공공기관(수요)

- 공공기관(수요)는 자체 블록체인 구축없이 DID, NFT 등 블록체인 서비스를 간편하게 기획, 운영, 관리할 수 있으며, 공공기관(수요)의

서비스를 빠르게 확대 적용할 수 있다.

- 공공기관(수요) 담당자는 낮은 블록체인 기술 이해도, 업무량, 사업 관리 등 다양한 업무 부담을 경감하고, 공공서비스의 기획, 경험, 비용, 실적관리에만 집중하여 대민 서비스를 제공할 수 있다.

! 수요기관은 블록체인 구축 없이 DID, NFT 등 블록체인 서비스를 간편하게 기획·운용·관리 가능함

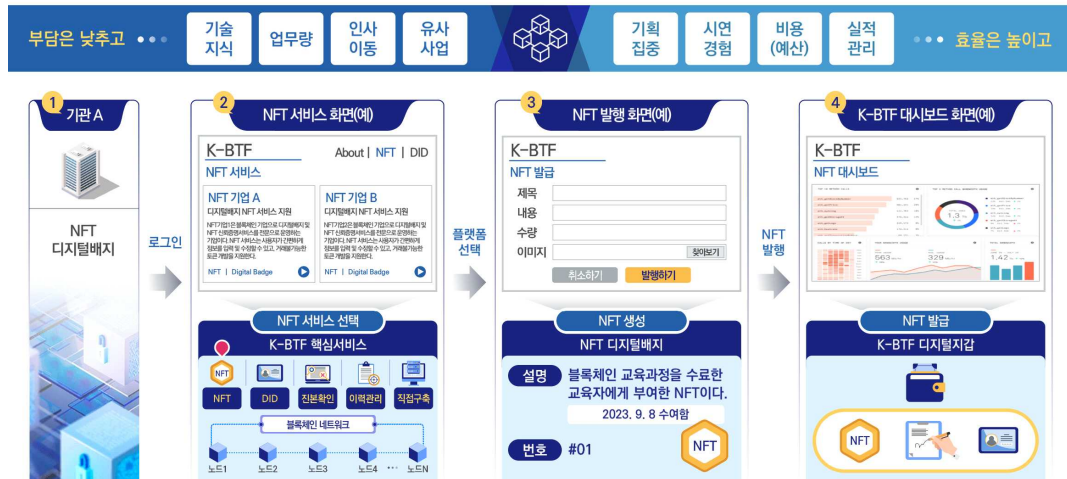


그림 7. 공공기관(수요) 관점의 K-BTF 공동인프라 기대효과

(다) 공급기업(블록체인기업)

- 자체 구축한 블록체인 네트워크와 K-BTF 공동인프라를 상호호환하여 블록체인 운영 경험을 향상하고, 공공 블록체인 비즈니스 모델 확보로 인한 새로운 시장 기반을 마련할 수 있다.
- 공급기업(블록체인기업)이 K-BTF 신규 참여 사업자로 선정되면 K-BTF 블록체인 전담기관임을 공증받으며, 기업이 제공하는 블록체인에 대해 K-BTF 서비스의 지위를 인정받게되어 경쟁력 확보가 가능하다.
- K-BTF 공동인프라 참여자인 이용자(국민), 공공기관(수요), 공급기업(블록체인 기업)별 시나리오는 ‘부록 3. K-BTF 공동인프라 참여자별 시나리오’를 참고하기 바란다.

(2) K-BTF 공동인프라별 기대효과

(가) 분산신원(Authentication) 공동인프라 기대효과

- 단일 DID로 다양한 분야에 이용이 가능하여 공공기관에서 기 구축한

블록체인 시스템과의 호환성을 가지며 관리 및 운영 효율성을 향상하고 이용자 입장에서 단일 또는 상호호환 가능한 DID 사용으로 편의성이 증대된다.

- 기존에 개별적으로 제공되었던 분산신원서비스에 비하여 K-BTF 공동인프라는 공동인프라 모델의 기준을 통하여 검증·도입되므로 신뢰성과 보안성이 증대되며 블록체인 네트워크 내 상호호환성을 확보함으로써 서로 다른 블록체인 네트워크의 DID 서비스를 통합적으로 이용·관리가 가능하므로 서비스 확장성에 유리하다.
- 또한 기존 민간에 의해 운영되는 분산신원 서비스를 K-BTF 분산신원 공동인프라의 블록체인 네트워크와 결합한다면 국가 기반의 통합 생태계를 구성할 수 있으므로 기존 이용자는 개별 서비스에 대한 별도의 신원 등록 절차 없이 서비스를 이용 가능하다는 이점을 갖는다.

(나) 디지털인증서(Certification) 공동인프라 기대효과

- 상호호환성을 바탕으로 서로 다른 블록체인 간 NFT 기반의 디지털 인증서 공동인프라 제공이 통합적으로 이루어지므로 공공기관들의 다양한 디지털인증서와 NFT를 일관성 있게 관리하고 구축 및 운영 효율성 향상이 증대된다.
- 또한 K-BTF 디지털인증서 공동인프라를 통해 블록체인 기반 디지털 인증서의 명확한 공통 기준을 활용한다면 기존 서비스에 비해 높은 신뢰성 및 투명성 확보가 가능하다.

(다) 데이터이력추적 공동인프라 기대효과

- 공공 분야에 데이터이력추적 공동인프라를 적용한다면, 공공 영역의 대표적인 서비스인 보건, 의료, 민원행정처리 및 민원서류발급, 취약 계층 관리 등 광범위한 데이터이력추적 서비스 제공이 가능하다.

(라) 데이터진본확인 공동인프라 기대효과

- 데이터 위·변조를 기반으로 한 데이터진본확인 서비스를 제공하고자 하는 공공기관의 경우 데이터진본확인 공동인프라의 도입을 통해 주민증, 민원서류, 자격증 등의 데이터 위·변조 방지와

관련된 공통 보안성 기준을 만족하게 되므로 보다 높은 보안성과 신뢰성이 보장되는 환경에서 서비스를 제공받는다.

(마) 직접구축(BaaS) 기대효과

- 기존 블록체인 시스템 또는 블록체인 네트워크들을 K-BTF와 통합 연계하여 국가 차원의 단일 공공 블록체인 플랫폼을 확보할 수 있다. 이는 각 수요기관의 관리 및 운영비용과 초기 투자비용을 절감하는 효과를 제공한다. 신규 블록체인 서비스에 K-BTF를 활용한다면 최소의 투자비용으로 원하는 서비스를 쉽게 구축할 수 있다.
- 또한 수요기관이 기존에 구축 및 운영하고 있는 분산신원인증, 디지털인증서, 데이터이력추적, 데이터진본확인, 디지털 지갑 등도 K-BTF 환경하에서 통합적으로 동작하게 되어 데이터 상호호환성 확보 및 보안에 대한 문제점을 해소할 수 있다.

(바) 디지털 지갑 서비스 기대효과

- 통합 디지털 지갑을 통해서 공공기관에서 발행한 디지털 증서와 민간에서 발행한 NFT를 통합 관리하여 대국민 편의성이 크게 증대되며 이와 연계된 다양한 신규서비스 제공받을 수 있다.
- 또한, 한 번 생성한 계정으로 타 서비스와의 호환성을 가지게 되어 K-BTF를 보다 편리하고 효율적으로 사용할 수 있게 된다.

제2절. K-BTF 실행 로드맵

본 절에서는 K-BTF 실행 로드맵에 대해 기술한다.

1. 중장기 K-BTF 실행 로드맵 구축

- 중장기 K-BTF 실행 로드맵은 1단계 K-BTF 시범사업 모델(1~3차년도)과 2단계 K-BTF 공공 확산사업 모델(4차~6차년도)로 단계적으로 진행한다.

		1단계 : K-BTF 시범사업 모델			2단계 : K-BTF 공공확산사업 모델		
구분		1차년도	2차년도	3차년도	4차년도	5차년도	6차년도
	디지털인증서(NFT)	핵심서비스 구축	핵심서비스 구축 시범운영		도입확대		
	분산신원증명(DID)	핵심서비스 구축	핵심서비스 구축 시범운영		도입확대		
	데이터진본확인		핵심서비스 구축	핵심서비스 구축 시범운영	도입확대		
	데이터이력추적		핵심서비스 구축	핵심서비스 구축 시범운영	도입확대		
	직접구축(BaaS)		핵심서비스 구축	핵심서비스 구축 시범운영	도입확대		
	디지털지갑	디지털 지갑 서비스 선정					

* 실행로드맵의 추진일정은 기술 및 정책 변화에 따라 달라질 수 있음

그림 8. K-BTF 실행로드맵

- 1단계 K-BTF 시범사업 모델(1~3차년도)에서는 K-BTF 서비스 생태계 마련을 위해 실현 가능한 수준의 K-BTF 공동인프라를 선별하여 시범사업을 통해 우선 적용한다.
- 1단계 K-BTF 시범사업 모델은 구축사업과 시범운영 단계로 다시 구분되며, 대상 공동인프라는 분산신원 공동인프라와 디지털인증서 공동인프라이다.
 - 1단계 중 구축사업은 분산신원 공동인프라와 디지털인증서 공동인프라를 보유한 공급기업을 대상으로 모집이 진행된다.
 - 1단계 K-BTF 시범사업 모델의 경우 해당 서비스를 이용할 정부기관, 관련 부처 등의 수요기관이 대상이다. 해당 서비스는 이미 국내 다수의 기관에서 시범사업으로 진행된 바 있으며 K-BTF 공동인프라를 쉽게 도입 적용할 수 있을 것으로 예상된다.
- 2단계 K-BTF 공공 확산사업 모델(4~6차년도)에서는 1단계 K-BTF 시범사업 모델(1~3차년도)을 통해 마련된 K-BTF 공동인프라 생태계를 기반으로 공공분야의 개방 확대를 목표로 진행한다. 2단계의 핵심 목표는

K-BTF 공동인프라의 공공 전 영역으로의 개방 및 확대를 위한 로드맵이다.

- 2단계 K-BTF 공공 확산사업 모델은 다시 1단계 결과물인 분산신원 공동인프라와 디지털인증서 공동인프라의 확산사업과 2단계에서 시작하는 데이터이력추적 공동인프라, 데이터진본확인 공동인프라, 직접구축(BaaS)의 구축사업 및 시범운영 사업으로 세분화하여 추진한다.
- 2단계 중 확산사업은 1단계 K-BTF 시범사업모델의 결과물인 분산신원 공동인프라, 디지털인증서 공동인프라는 확산사업을 진행한다.
- 2단계 중 구축사업과 시범운영 사업은 데이터이력추적, 데이터진본확인 및 직접구축(BaaS) 기술을 보유한 공급기업을 대상으로 구축사업을 모집, 선발하여 진행하며, 정부기관, 관련 부처 등의 수요기관이 시범 운영 사업을 진행한다. 2단계에서 추진하는 서비스 역시 국내 다수의 기관들을 통해 시범사업으로 진행되어 K-BTF 공동인프라로 쉽게 확산할 수 있을 것으로 예상된다.
- 이와 별개로 K-BTF 공동인프라 중 디지털 지갑 서비스는 차년도에 디지털 지갑 서비스 사업자 선정을 통해 별도 진행할 예정이며, 이는 K-BTF 공동인프라의 1, 2단계 추진을 위한 사용자인증 통합, 블록체인 네트워크 통합 등의 기반 마련을 목표로 추진될 예정이다.
- K-BTF 실행 로드맵 1단계와 2단계 사업의 검증을 위해 시험인증체계도 함께 병행한다. 1단계는 기능과 성능 중심의 시험인증체계, 2단계에서는 기능, 성능, 보안 중심의 통합시험인증체계를 통해 시범사업과 공공확산에 필요한 시험검증체계를 동시에 마련하고자 한다.
- 1단계 시험사업 단계의 기능시험은 K-BTF 공동인프라에서 요구하는 기능구현 및 기능 완성도를 중점적으로 평가한다. 성능시험은 K-BTF 공동인프라의 기능 완성도에 기반하여 해당 기능의 처리속도, 자원사용량, 데이터 기밀성 및 무결성, 안정성, 확장성 등의 주요 성능지표를 중심으로 평가한다.
- 2단계에서는 1단계 검증 지표인 기능, 성능에 보안 지표를 추가하여 기밀성, 무결성, 암호화 등 주요 보안 목표를 검증한다.

2. 실행로드맵 세부 추진 방안

(1) 실행로드맵 세부 추진 방안

(가) 1단계 시범사업 세부 추진 방안



그림 9. 1단계 K-BTF 시범사업 모델(1~3차년도)

1) 시범사업 대상 선정

- 1단계에서는 1차년도 ~ 2차년도 분산신원 공동인프라와 디지털인증서 공동인프라를 보유한 공급기업을 대상으로 축사업 진행 후 2차년도 정부기관 부처 등의 수요기관 중심의 시범사업을 진행한다. 분산신원 공동인프라와 디지털인증서 공동인프라의 경우 1차년도 구축사업 각 1건, 2차년도 구축사업 각 1건 및 시범운영 사업 각 1건을 목표로 하며, 데이터이력추적 공동인프라, 데이터진본확인 공동인프라, 직접 구축(BaaS)의 경우 2차년도 ~ 3차년도 구축사업 각 1건, 3차년도 구축사업 각 1건 및 시범운영 사업 각 1건을 목표로 진행한다.

- DID, NFT 등을 활용한 공공서비스는 이미 다수의 사례를 가지고 있으며, 유용성이 증명된 서비스를 중심으로 선정하였다.

2) 시범사업 추진 일정

- (구축사업) 분산신원 공동인프라와 디지털인증서 공동인프라의 경우 1차년도 구축사업 각 1건, 2차년도 구축사업 각 1건을 목표로 RFP를 공개하고, 사업 심사를 거쳐 구축 사업을 추진할 계획이다. 추진 일정은 1차년도 각 1건, 2차년도 각 1건을 목표로 한다. 1차년도에 진행하는 구축사업의 경우 K-BTF 공동인프라 구축을 목표로 진행하며, 2차년도에 진행하는 구축사업의 경우 시범사업과 병행진행하면서 수요기관의 서비스 개발, 운영을 지원한다. 또한, 2차년도 상반기 구축사업 개시를 목표로 데이터이력추적 공동인프라, 데이터진본확인 공동인프라, 직접구축(BaaS)에 대한 RFP를 1차년도 하반기에 공개하고, 1차년도 4/4분기에 심사를 거쳐 2차년도 1/4분기부터 구축 사업을 추진하며 2차년도 내 총 3건의 구축사업 완료를 목표로 한다.
- (시범운영) 2차년도 시범사업 개시를 목표로 분산신원 공동인프라와 디지털인증서 공동인프라를 이용할 정부기관, 부처 등으로부터 수요처를 모집 후 2차년도 1/4분기부터 시범운영 추진을 목표로 한다. 추진 일정은 2차년도 총 2건을 목표로 한다. 또한, 2차년도 구축사업이 완료된 데이터이력추적 공동인프라, 데이터진본확인 공동인프라, 직접구축(BaaS)도 마찬가지로 2차년도 1/4분기 시범운영 착수를 목표로 진행하며, 3차년도 총 3건을 목표로 한다.

3) 시범사업 검증

- 1단계 시범사업을 통해 진행된 분산신원 공동인프라와 디지털인증서 공동인프라의 검증을 위해 시험인증체계를 적용한다. 1단계에서는 기능검증과 성능검증을 위주로 진행한다. 1단계는 K-BTF 공동인프라의 가능성을 시범사업을 통해 확인하는 단계로 분산신원 공동인프라와 디지털인증서 공동인프라의 기능 중심으로 검증한다. RFP에 제시된

요구사항을 중심으로 기능별 정상 동작 여부와 이때 발생할 수 있는 주요 리스크를 점검한다. 또한, 1단계 완료 시점인 2차년도 하반기에는 성능 중심의 검증을 추가한다. 정상적으로 구현되고 동작하는 기능이 원하는 자원량, 처리속도, 확장여부 등 다양한 성능 지표를 기반으로 측정하고 검증한다.

4) 시범사업 기대효과

- 1단계 시범사업을 통해 분산신원 공동인프라와 디지털인증서 공동 인프라의 활용성 여부와 기능 및 성능을 검증할 수 있다. 성공적인 1단계 시범사업 추진을 통해 K-BTF 공동인프라의 공공확산을 위한 발판 마련, 기술 구현과 실용성 검증 그리고 기능과 성능 검증체계의 기반을 마련할 수 있다. 이를 통해 2단계 공공 확산사업 모델로의 개방 및 확산에 기여할 수 있을 것으로 판단한다.

(나) 2단계 공공확산사업 세부 추진 방안



그림 10. 2단계 K-BTF 공공확산사업 모델(4~6차년도)

1) 공공확산사업 대상 선정

- 2단계에서는 공공확산을 위한 단계로 K-BTF 공동인프라의 공공분야 개방 및 확산을 목표로 추진된다.
- 1단계 추진되었던 분산신원 공동인프라와 디지털인증서 공동인프라는 2단계 시작 시점인 1차년도부터 확산사업으로 추진되어 3차년도까지 매년 공동인프라별 1건씩의 확산사업 수행을 목표로 한다.
- 또한 데이터이력추적 공동인프라, 데이터진본확인 공동인프라, 직접구축(BaaS)는 2차년도부터 공공확산사업 형태로 진행하며 K-BTF 공동인프라별 각 1개씩의 사업을 매년 수행한다.
- 데이터이력추적 공동인프라, 데이터진본확인 공동인프라, 직접구축(BaaS)는 분산신원 공동인프라와 디지털인증서 공동인프라의 결과물을 연계하여 활용하는 사업형태로 추진될 것이며, 이미 다수의 공공기관을 통해 진행되어 많은 사례를 가지고 있어 K-BTF 공동인프라의 유용성 증명을 위해 최적의 서비스라고 판단한다.

2) 공공확산사업 추진 일정

- 1단계 시범사업을 통해 검증이 완료된 분산신원 공동인프라와 디지털인증서 공동인프라는 1차년도 상반기 사업 개시를 목표로 3차년도까지 3년 동안 공공확산사업을 추진한다. 사업자 공고를 통해 정부기관, 부처 등의 수요처를 대상으로 공공확산사업을 선발 후 서비스별 매년 각 1건씩 진행을 목표로 한다.
- 2차년도부터는 데이터이력추적 공동인프라, 데이터진본확인 공동인프라, 직접구축(BaaS)도 시범사업이 마무리되고 공공확산 사업을 전환하는 시점으로 5개 K-BTF 공동인프라에 대해 매년 각 1건을 목표로 공공확산사업을 추진한다.

3) 공공확산사업 검증

- 1차년도 공공확산사업 단계는 기능, 성능을 중심으로 K-BTF 공동인프라 5종에 대한 시험인증체계를 검증한다. K-BTF 공통요구사항과 RFP(제안요청서)에 제시된 기능별 정상 동작 여부와 이때 발생할 수 있는 주요 리스크를 점검하며 또한 자원량, 처리속도, 확장성

여부 등의 다양한 성능지표를 함께 검증한다. 2차년도 공공사업확산 단계에서는 보안 검증이 추가되어 암호화, 무결성, 기밀성, 가용성 관련 지표들을 추가하여 검증체계를 완성할 예정이다.

4) 공공확산사업 기대효과

- 2단계 공공확산사업을 통해 K-BTF 공동인프라의 활용성과 기능, 성능 및 보안에 대한 검증체계를 확보할 수 있다. 5개 K-BTF 공동인프라의 성공적인 사업 추진을 통해 공공확산을 위한 발판 마련, 기술 구현과 기능, 성능, 보안 검증체계를 마련할 수 있다. 이를 통해 모든 사업이 종료된 시점 이후부터는 다수의 공공사업에 즉시 활용 가능한 모델로서 기여할 수 있을 것으로 판단한다.

제3절. K-BTF 공통규격검증체계

본 절에서는 K-BTF 공통규격검증체계에 대해 기술한다.

1. K-BTF 공통규격검증체계 개요

- K-BTF 공통규격검증체계는 공통요구사항과 시험검증체계로 구성되어 있다. 공통규격검증체계는 블록체인 플랫폼에 관계없이 안전하고 상호 호환할 수 있는 서비스를 제공하기 위한 기술 요건을 제시하고 있으며, 시험검증체계를 통해 신뢰성 및 안전성을 확보하기 위함이다. 이를 위해 새로운 제도를 만드는 것이 아닌 최소한의 기능 점검 및 현행제도를 활용한 효율적인 검증체계를 목표로 한다.

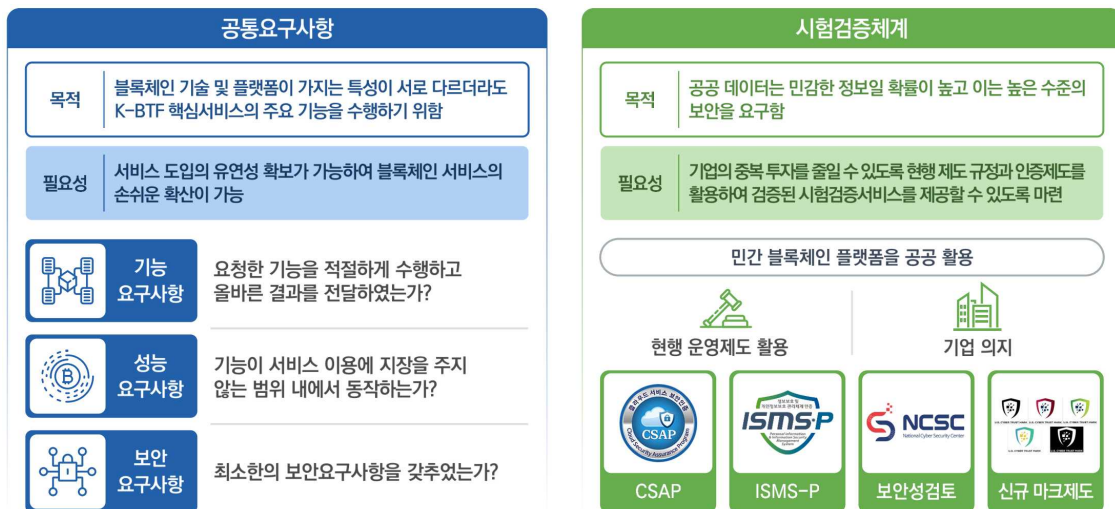


그림 11. K-BTF 공통규격검증체계 개요

2. K-BTF 공통요구사항의 목적 및 필요성

- (목적) K-BTF 공통요구사항의 목적은 블록체인 기술 및 플랫폼이 가지는 특성이 서로 다르더라도 K-BTF 공동인프라의 주요 기능을 수행하기 위함이다. 기존에 구축된 블록체인 플랫폼들은 상호호환되지 못하는 경우가 많고 특정 블록체인 플랫폼에 대한 의존성이 매우 높은 편이다. 이러한 특정 플랫폼에 대한 의존성을 낮추고 상호호환을 통해 민간 블록체인 플랫폼의 공정한 경쟁환경 마련과 공공서비스 분야의 블록체인 활성화를 위해 공통요구사항을 마련하였다.

- (필요성) 공공기관(수요)에서 블록체인 서비스를 도입하기 위해서는 기획, 개발, 운영 뿐만 아니라 민간기업의 기술력 활용, 보안 및 인증 등 여러 가지 요소를 고려해야 하는 부담이 있다. 이러한 제약 요소를 해소하기 위해 공통요구사항을 도출하여 적용한다면 공공분야에 블록체인 기업 진출 및 서비스 도입의 유연성 확보가 가능하여 블록체인 서비스의 손쉬운 확산이 가능하다. 공급기업(블록체인 기업) 입장에서는 각사가 보유한 블록체인 기술을 K-BTF 공동인프라와 연계하여, 블록체인 서비스 운영 경험과 공공서비스 분야의 새로운 비즈니스 모델 확보가 가능하다. 국민(이용자) 입장에서는 기존 공공기관별 블록체인 서비스를 상호호환이 가능한 통합 디지털 지갑으로 신원증명, 디지털인증, 모바일 신분증, 데이터이력추적, 데이터진본확인 등을 간편하게 사용할 수 있는 편의성 확보가 가능하다.
- 공통요구사항 도출에 필요한 과정은 ‘부록 4. K-BTF 공통요구사항 현황 분석’을 참고하기 바란다.

3. K-BTF 시험검증체계의 목적 및 필요성

- (목적) K-BTF 시험검증체계는 K-BTF 공동인프라를 활용하여 공공서비스가 제공되는 경우 공공서비스에 생성되고 유통되는 데이터는 국민(이용자) 및 공공기관(수요)의 민감한 정보일 확률이 높으며, 이는 높은 수준의 보안을 요구하게 된다. 이에 K-BTF 공동인프라의 시험검증체계과 최소한의 보안 수준을 마련하여 안전하고 신뢰성 있는 K-BTF를 마련하기 위한 목적이다.
- (필요성) K-BTF 시험검증체계는 국민(이용자)이 안심하고 서비스를 이용할 수 있으며, 공공기관(수요)이 보안, 인증에 대한 고민없이 블록체인 서비스를 제공하기 위해 필요하다. 또한 공급기관(블록체인 기업)이 K-BTF 공동인프라와 상호호환 시 보안 및 검증을 위한 준수 항목으로서 활용하기 위해서도 필요하다. 이때 공급기관(블록체인 기업)이 기존에 보유한 보안 인증 자격을 활용한다면 인증 및 검증에 소요되는 기업의 중복 투자를 줄일 수 있도록 현행 제도 규정과 인증제도를 활용하여 검증된 시험검증서비스를 제공할 수 있도록 마련되어야 한다.
- 시험검증체계 도출에 필요한 과정은 ‘부록 5. K-BTF 시험검증체계 현황 분석’을 참고하기 바란다.

제4절. 거버넌스 체계 수립

본 절에서는 거버넌스 체계 수립에 대해 기술한다.

1. 거버넌스 협의체 목적 및 역할

□ (목적) 거버넌스 협의체는 K-BTF의 기술 및 관리 등에 관련된 전반의 영역에 대한 의사결정을 내리는 조직이다. 거버넌스는 K-BTF 운영 과정에서 윤리성 및 공공성을 확보하고 기술 및 운영 측면에서의 불법행위 방지를 통해 이용자(국민), 공공기관(수요), 블록체인기업(공급)을 보호하기 위한 기구이다. K-BTF의 성공적인 운영과 사업 확산을 위해서는 투명하고 공정한 거버넌스가 필수적이며, 이를 위해 다양한 이해 관계자들이 참여하는 협의체의 수립이 매우 중요하다.

□ (역할) 거버넌스 협의체는 다음과 같이 구성하고 역할과 절차에 따라 정책 수립, 공통요구사항, 추진체계마련, 역할 수립, 협의체 구성의 역할을 수행한다. 다만, 거버넌스 협의체가 현재의 게임물등급관리 위원회나 방송 통신 위원회와 같이 근거법을 기반으로 하는 법적 구속력을 갖춘 조직을 기반으로 해야 하는지 아니면 일반적인 협회 수준이나 위원회나 형태 구성이어야 하는지에 대해서는 충분한 전문가들의 의견 수렴이 필요하다.

(1) 정책 수립

○ 거버넌스 협의체의 목표는 K-BTF의 성공적인 운영을 위한 투명하고 공정한 거버넌스를 구축하는 것이다. 정책 수립을 통해 거버넌스의 목표와 목표 달성을 위한 의사결정 구조, 권한과 책임의 배분, 의사소통 및 협력 방식을 규정한다. 거버넌스 정책을 통해 K-BTF의 효율성과 효과성을 높이고 이해 관계자와의 관계를 개선하여 장기적인 지속 가능성을 확보하기 위해 매우 중요한 역할을 한다.

(2) 공통요구사항

○ K-BTF 공동인프라와 관련된 공통요구사항을 관리한다.

(3) 추진체계마련

○ K-BTF의 4가지 역할과 절차에 따라 추진체계를 마련한다.

(4) 역할수립

- 협의체를 구성하는 조직과 조직 구성원들의 업무를 규정한다. 협의체의 주요 조직 및 구성원들은 K-BTF 거버넌스의 4가지 역할에 따라 각자의 고유 업무를 수행한다.

(5) 협의체 구성

- 협의체는 K-BTF 의 기술적, 관리적 측면에서의 심의, 검증, 개선 권고를 수행하고 의사결정을 내리는 기구이다. 협의체의 구성은 블록체인 관련 분야의 전문가들과 KISA사무국의 정부분과(수요), 민간분과(기업), 전문가(학계, 정출연 등)으로 구성된다. 상정된 안건에 대해 정기적, 비정기적으로 심의회를 진행하고 의사를 결정한다. 협의체 위원으로 참석하기 위해서는 임명 또는 참여, 추천과 같은 다양한 형태를 취할 수 있다. 다만 어느 경우에라도 정부분과(수요), 민간분과(기업), 전문가(학계,정출연 등)으로 구성된 전문가의 참여로 행정의 효율성 및 전문성을 제고할 수 있는 분권적·참여적 형태의 단독제 조직 구성 원칙을 유지하여야 한다.

□ (거버넌스 협의체 구성시 고려사항) 거버넌스 협의체 구성을 위해서는 다음과 같은 사항들을 고려해야 한다.

(1) 거버넌스 협의체의 구속력

- 거버넌스 협의체가 현재의 게임물등급관리 위원회나 방송 통신 위원회와 같이 근거법을 기반으로 하는 법적 구속력을 갖춘 조직을 기반으로 해야 하는지 아니면 일반적인 협회 수준이나 위원회나 형태 구성이어야 하는지에 대해서는 충분한 전문가들의 의견 수렴이 필요하다.
- 이를 위해 본 과업에서는 별도의 연구에 대해서는 진행하지 않는다.
- (거버넌스 협의체 사례) 캘리포니아 주지사 개빈 뉴섬(Gavin Newsom)은 2022년 5월, 웹3.0 생태계의 혁신 가속, 소비자 보호를 위한 블록체인 행정명령에 서명하였으며, 이를 통해 캘리포니아 주는 웹3.0 기술 발전을 위한 포괄적인 프레임워크를 만드는 미국의 첫 번째 주가 되었으며 해당 행정 명령에는 암호화폐의 기본적인 KYC/AML 지침 뿐만 아니라 정부 운영 기관 및 시장에서 신규 요구 사항 해결에 대해 블록체인 기술이 폭넓게 활용되는 경우 이를 검증 하기 위해 특정 목적에 맞는 블록체인 기술이 조달되었는지에 대한 적합성을 평가하고 캘리포니아 블록체인 워킹그룹이 식별한 적용에 대한 요소를 고려하기 위한 기초적인 법적 근거들이 담겨 있다.

(2) 의사결정 범위와 방법

- 거버넌스 협의회를 통해 논의되거나 결정되어야하는 사항들의 범위와 그 방법론에 대한 세밀한 검토가 필요하다.

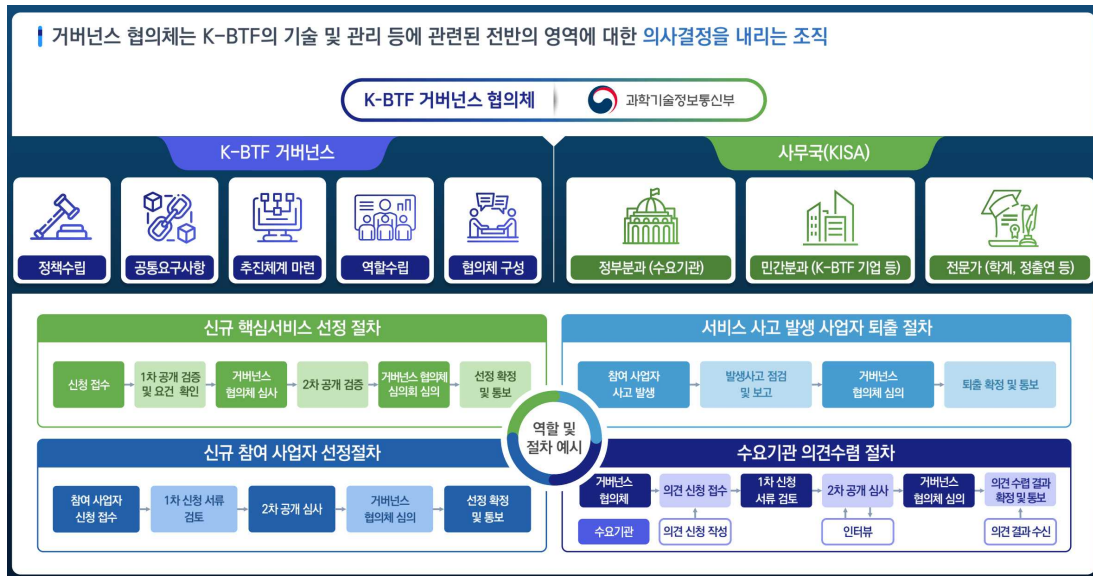


그림 12. K-BTF 거버넌스 체계 개념도

2. 거버넌스 주요 역할 및 절차

- K-BTF 거버넌스 체계의 역할은 신규 핵심서비스 및 공동인프라 선정, 신규 참여 사업자 선정, 서비스 사고 발생 사업자 퇴출, 수요기관 의견수렴의 4가지이며 이에 따른 절차를 준수해야 한다.

(1) 신규 공동인프라 선정 절차

- 블록체인 관련 규제가 점차 개선되고 기술이 발전과 시장 확산이 이루어지는 상황에서 K-BTF 현행규제, 현행기술 수준 내에서 활용 가능한 서비스 기술을 K-BTF 공동인프라로 추가 지정하여 운영할 수 있도록 논의하여 결정하는 절차이다.
- 공동인프라가 신규로 추가되는 경우라면, 이에 맞는 공통규격이 반영되어야 하며, 신규 공동인프라에 맞는 현행제도를 활용해야 한다.



그림 13. 신규 공동인프라 선정 절차

- 신규 공동인프라 선정은 신청접수 단계부터 선정 확정 및 통보까지 6단계를 거쳐 진행된다. 신규 공동인프라 선정을 위해서는 아래 절차를 따라 신규 공동인프라 선정이 마무리 된다.
- 신규 공동인프라 선정 세부 절차는 다음과 같다.

세부절차	세부절차 설명
1. 신청접수	<ul style="list-style-type: none"> K-BTF 신규 공동인프라 선정 희망 사업자
2. 1차 공개 검증 및 요건 확인	<ul style="list-style-type: none"> 신청 서류 검토 진행 신규 공동인프라 기술/사업 요건 검토 진행 현행규제, 현행기술 수준 검토
3. 거버넌스 협의체 심사	<ul style="list-style-type: none"> 거버넌스 협의체 내부 심사 진행 검증 결과 및 요건 확인 결과 심사 진행 서류 및 계획 내용 보완 요청 진행(필요시)
4. 2차 공개 검증	<ul style="list-style-type: none"> 거버넌스 협의체 심사 의견 검토 인터뷰 진행 요건확인 결과 및 검증 결과 종합 의견
5. 거버넌스 협의체 심의회 심의	<ul style="list-style-type: none"> 검증 결과 및 종합 의견 심의 심의 결과 확정(의사결정)
6. 선정 확정 및 통보	<ul style="list-style-type: none"> 결과 통보

표 3. 신규 공동인프라 선정 절차

(2) 신규 참여 사업자 선정 절차

- K-BTF 참여를 원하는 사업자가 있을 경우, 자격을 갖추었는지 평가하고 이에 준하는 경우 K-BTF 지위를 인정해주는 절차이다.
- K-BTF 사업자에 선정되면 우선 정부의 블록체인 전담기관 또는 부처 홈페이지 등에 K-BTF로 선정된 기업에 대한 내용을 표기하고, 이후 마크제가 만들어진 이후, 해당 기업에 K-BTF 마크를 부여할 예정이다.



그림 14. 신규 참여 사업자 선정 절차

- K-BTF에 참여를 원하는 사업자를 선정하는 절차는 참여 사업자 신청접수 단계부터 선정 확정 및 통보까지 5단계를 거쳐 진행된다.
- 신규 공동인프라 참여 사업자 선정 세부 절차는 다음과 같다.

세부절차	세부절차 설명
1. 참여 사업자 신청접수	<ul style="list-style-type: none"> K-BTF 참여를 원하는 사업자
2. 1차 신청 서류 검토	<ul style="list-style-type: none"> 신청 서류 검토 진행 K-BTF 기술 요건 검토 진행
3. 2차 공개 심사	<ul style="list-style-type: none"> 사업자 인터뷰 진행 신청 서류 검토 및 기술 요건 검토 진행 서류 및 계획 내용 보완 요청 진행(필요시)
4. 거버넌스 협의체 심의	<ul style="list-style-type: none"> 검증 결과 및 종합 의견 심의 심의 결과 확정(의사결정)
5. 선정 확정 및 통보	<ul style="list-style-type: none"> 사업자에게 결과 통보 K-BTF 선정기업 표기, K-BTF 마크부여(추후)

표 4. 신규 참여 사업자 선정 절차

(3) 서비스 사고 발생 사업자 퇴출 절차

- K-BTF 사업자의 서비스 중단, 개인정보 유출 등 사고 발생 시, 현장 점검 및 실사 등을 통해 현황을 파악하고 탈퇴, 책임부여, 복원/조치 이행 완료 여부 등을 진행하는 절차이다.
- 서비스 사고의 피해수준과 복구 가능성 등을 면밀하게 조사하여 원인을 분석하고, 경미한 경우 이에 대한 책임부여 및 조치 작업에 대한 절차를 진행한다.



그림 15. 서비스 사고 발생 사업자 퇴출 절차

- K-BTF 사업자의 철회를 위한 탈퇴절차는 참여 사업자 탈퇴 접수 단계부터 탈퇴 확정 및 통보까지 4단계를 거쳐 진행된다.
- 공급 기업의 부당행위나 불법행위가 적발되는 경우, 공동인프라 사업자의 탈퇴 접수 요청이 없었다고 할지라도 본 협의체에서는 이러한 원인을 근거로 해당 사업자의 탈퇴 절차를 진행할 수 있다.
- 공동인프라 사업자 퇴출 세부 절차는 다음과 같다.

세부절차	세부절차 설명
1. 참여 사업자 사고 접수	<ul style="list-style-type: none"> • 사고 접수
2. 발생사고 점검 및 보고	<ul style="list-style-type: none"> • 현장 조사 및 증적 확보 • 사고 경중, 복구가능성, 피해/심각도 판단 • 인터뷰 진행
3. 거버넌스 협의체 심의	<ul style="list-style-type: none"> • 조사 결과 및 종합 의견 심의 • 심의 결과 확정(의사결정)
4. 탈퇴 확정 및 통보	<ul style="list-style-type: none"> • 사업자에게 결과 통보 • 탈퇴/후속 작업 조치 안내
5. 후속 작업 조치 확인	<ul style="list-style-type: none"> • 탈퇴/후속 작업 조치 결과 확인

표 5. 사업자 퇴출 세부 절차

(4) 수요기관 의견 수렴 절차

- 공공기관(수요), 블록체인기업(공급)으로부터의 서비스 품질, 사업자 가격 담합 등 K-BTF의 서비스 품질 향상을 위한 다양한 의견을 접수하고 심의하는 절차이다.



그림 16. 수요기관 의견 수렴 절차

- K-BTF 수요기관이 K-BTF 서비스 품질 향상과 관련된 의견을 제시할 경우 의견 신청접수 단계부터 의견 수렴 결과 확정 및 통보까지 5단계를 거쳐 진행된다.
- 수요기관 의견 수렴 세부 절차는 다음과 같다.

세부절차	세부절차 설명
1. 의견 신청 접수	<ul style="list-style-type: none"> 수요기관 의견 수렴 서류 접수
2. 1차 신청 서류 검토	<ul style="list-style-type: none"> 신청 서류 검토 진행 기술 요건 검토 진행
3. 2차 공개 심사	<ul style="list-style-type: none"> 수요기관 인터뷰 진행 신청 서류 검토 및 기술 요건 검토 진행 서류 및 계획 내용 보완 요청 진행(필요시)
4. 거버넌스 협의체 심의	<ul style="list-style-type: none"> 검증 결과 및 종합 의견 심의 심의 결과 확정(의사결정)
5. 의견 수렴 결과 확정 및 통보	<ul style="list-style-type: none"> 수요기관에 결과 통보

표 6. 수요기관 의견 수렴 절차

제 3 장. 결론

K-BTF의 적용과 확산을 통한 기대효과는 다음과 같이 예상된다.

- 대부분의 공공서비스는 중앙 집중식 데이터 기반으로 구축 및 운영되어 확장성, 상호호환성, 효율성, 보안성, 공공성의 한계가 존재하여 이에 대한 해결책 마련이 대두되었다. 이에 대한 해결방안으로 데이터의 높은 신뢰성을 보장하는 블록체인 기술이 주목받아 다양한 공공서비스 분야에 도입되었다. 그러나, 해외 국가들의 블록체인 프로젝트와 국내 블록체인 관련 공공·민간사업을 분석한 결과 네트워크 파편화, 미비한 상호호환성, 자원 비효율성 등의 문제점이 발생하였다. 본 연구에서는 이를 해결하기 위한 실수요 중심의 K-BTF를 정립하고 K-BTF 공동인프라 모델 도출, K-BTF 실행 로드맵, K-BTF 시험검증체계 및 거버넌스 체계 수립에 대한 방안 및 전략을 제시하였다.
- K-BTF 공동인프라 모델은 블록체인을 도입하려는 공공기관이 별도의 블록체인 네트워크를 구축할 필요 없이 블록체인 기반 공공서비스를 제공할 수 있도록 6가지 공동인프라를 수립하였다. K-BTF 공동인프라는 상호호환성, 신뢰성, 효율성, 확장성, 보안성, 공공성을 준수하며 블록체인 네트워크, 공동인프라별 시나리오, 공통요구사항으로 구성된 체계적인 모델이다. K-BTF는 분산신원 공동인프라, 디지털인증서 공동인프라, 데이터 위·변조방지 공동인프라, 데이터이력추적 공동인프라, 디지털 지갑 서비스를 공공기관에게 제공하며 기관은 이를 활용하여 이용자(국민)를 대상으로 다양한 공공서비스를 효율적으로 구축 및 운영이 가능하다.
 - K-BTF 공동인프라 모델의 적용 및 확산은 다양한 측면에서 이점을 제공한다. K-BTF 공동인프라 모델에서 제공하는 분산신원 공동인프라, 디지털인증서 공동인프라, 데이터 위·변조 공동인프라 등을 포함한 여러 공동인프라를 통해 공공기관(수요)은 기존 대비 효율적인 구축·운영 경제성과 다양한 블록체인 신규서비스 및 확장 효과가 기대된다.
 - 이용자는 통합된 디지털 지갑의 사용으로 인해 높은 사용자 편의성과 저렴한 수수료를 바탕으로 다양한 산업의 대국민 참여 서비스가 기대된다. 위와 같은 이점을 바탕으로 국가적인 블록체인 기술 발전과

산업 육성 효과를 이끌어 낼 수 있으며, 나아가 경제 성장력의
동력원이 될 수 있다.

- 광범위한 블록체인 기술의 활용성과 다양한 미래 기술 개발 및 도입을
바탕으로 수많은 블록체인 플랫폼이 시장에 등장하였으나, 표준화된
규격이 존재하지 않고 서로 독립된 생태계를 구축하여 각 서비스가
고립된 환경을 구성하고 있는 것이 현실이다. 이를 K-BTF 공동인프라
모델을 통해 기존 파편화된 구조에서 탈피하여 효과적으로 통합된
블록체인 서비스 환경을 구성할 수 있다. K-BTF는 투명한 신뢰 사회
구축의 실현을 위한 블록체인 기반 공공서비스 모델의 일반화와 부수
적인 기술적·사회적·경제적 효과를 기대할 수 있다.

부록 1. 해외 블록체인 국가 플랫폼 현황 분석

1. 해외 주요 국가의 블록체인 국가 플랫폼 구축 현황 분석

(1) 유럽 EBSI






- (현황) 유럽 전역에 걸쳐 36개 노드를 구축 완료('21)를 하였으며 유럽 진행위원회의 유럽 블록체인 파트너십(European Blockchain Partnership, 이하 EBP)와 협력하여 시범운영 중이다. 2022년 5월 유럽연합 집행위원회(European Commission)는 EBSI에 연결하기 위해 소프트웨어에 대한 접근성을 공개하기로 공식 결정하였다.
- (목표) 유럽 전역에 분산된 블록체인 네트워크를 공공서비스 형태로 제공하며, EU 정책과 규제 준수는 물론 보안과 지속 가능한 블록체인 서비스 측면에서 유럽 시민과 기업들 간의 블록체인 기반의 협력을 증진시키고자 하는 것이 목표이다. 이를 통해 범유럽 블록체인 디지털 인프라 핵심 표준 확보 및 블록체인 기반 공공서비스 제공을 목표로 한다.
- (주체) EBP에서 추진하여 노르웨이, 리히텐슈타인 등 총 29개국이 참여했다. EBP 회원국을 중심으로 블록체인 인프라 구축과 4개 블록체인 공공 서비스(감사목적 문서 공증, 졸업증명서 인증, EU 자기주권 신원인증 프레임워크, 신뢰할 수 있는 데이터 공유)를 제공한다. EU 각 회원국이 국가 단위에서 자체적인 EBSI 노드를 운영하고, 노드가 분산원장 업데이트와 거래 생성 및 전송하는 기능을 수행하도록 구성되어 있다.
- (주요 서비스) 자기주권신원, 문서공증, 학위증명, 지적재산권 등의 서비스를 제공한다.
 - (가) 자기주권신원 : 중앙 기구에 의존하지 않고, 이용자들이 자신들의 디지털신원(식별, 인증 및 여러 유형의 ID 관련 정보 포함)을 생성, 제어 및 사용할 수 있도록 지원한다.
 - (나) 문서공증 : 문서의 진위여부 및 무결성을 보장하는 검증 기능 제공하여 데이터 또는 문서의 변화를 추적한다. 신뢰할 수 있는 디지털 감사 개체를 만들어 규정 준수확인(Compliance check)을 자동화하고 데이터

무결성을 보장하는 서비스이다.

(다) 학위증명 : 대학교 졸업증명서를 VC(Verifiable Credentials) 형태로 이
 용자에게 발행하고, 검증할 수 있는 기능을 지원한다. 블록체인의 자
 격증명을 게시하는 것과 같이 이용자들의 학위증명을 관리 시 디지털
 신원 인증 비용을 줄이고 신뢰성을 향상시키는 서비스를 제공한다.

(라) 지적 재산권(Intellectual Property) 관리 : 지적 재산의 관리 및 권리
 보유자를 확인하는 서비스이다.

○ (관련 공동인프라 키워드)

				
BaaS	분산신원	디지털인증서	데이터진본 확인	디지털 지갑

(2) 독일 GAIA-X

○ (현황) 2022년 4월에 GXFS(GAIA-X Federation Services)를 제공하고 있
 다. GXFS는 블록체인 인프라 생태계와 분산된 블록체인 데이터 생태계
 를 연결함으로써 이용자 인증, 정책, 데이터 교환 프로세스 등을 제공하
 는 서비스이다. 현재 오픈소스 기반으로 개발을 진행 중이다.

○ (목표) 유럽의 데이터 주권 확보와 미국-중국 주도의 데이터 플랫폼 기
 업에 대한 의존도 최소화를 목적으로 EU 전용 클라우드 구축과 혁신 데
 이터 생태계 인프라를 구성하는 것을 목표로 추진되고 있다.

○ (주체) 독일에서 2019년 10월 ‘GAIA-X 프로젝트’ 추진 계획을 발표하
 였고 독일 연방정부가 주도하는 범국가적인 사업이다.

○ (주요 서비스) ID 및 신뢰, 연합 카탈로그, 데이터주권, 규정준수 등의
 서비스를 제공한다.

(가) ID 및 신뢰 : 신뢰 격차 해소를 위해 GXFS를 사용하여 자격증명 유효
 성 검사를 통해 사용자를 인증하고 권한을 부여받는다.





(나) 연합 카탈로그(Federated Catalogue) : 하나의 연합 저장소에서 이용자

가 다른 이용자의 정보를 찾고 자기 주권 형태의 서비스를 제공할 수 있다. 하나의 연합 저장소를 위해 각 연방에 대한 기본 코드를 제공하여 연합 카탈로그를 구축한다.

(다) 데이터 주권 : 투명성이 보장되고 데이터 사용 제어를 가능하게 할 수 있는 서비스를 제공하여 연합의 이용자가 데이터에 대한 주권을 유지하도록 하는 서비스이다. 본 서비스에는 계약 협상을 용이하게 하고 연합 내에서 데이터 트랜잭션의 이력추적 서비스가 포함되어 있으며, 이를 활용하여 다양한 트랜잭션을 통해 데이터 사용량을 확인하고 추적가능하다.

(라) 규정 준수 : 이용자와 서비스가 GAIA-X 원칙을 준수하는지 평가할 수 있는 규정 준수 확인 서비스를 제공한다. 규정 준수 확인 서비스는 새로운 참가자를 온보딩 단계에서 확인할 수 있으며, 실행 중인 서비스를 지속적으로 모니터링 할 수 있다. 이용자 간의 신뢰할 수 있는 트랜잭션과 여러 자격증명 확인의 자동화를 지원하기 위해 공증 및 거버넌스를 제공하여 일련의 분산 서비스랑 상호 작용하도록 한다.

○ (관련 공동인프라 키워드)






					
BaaS	분산신원 증명	디지털 인증서	데이터 진본확인	데이터 이력추적	데이터 주권

(3) 에스토니아 전자정부

○ (현황) 2001년 개개인의 데이터베이스를 연결하는 엑스로드 프로젝트 진행 이후 20여년에 달하는 중장기 전략으로 중앙정부 주도형 전자정부 시스템을 구축하였다. 2007년 러시아로부터 대규모 사이버 공격을 받은 이후 블록체인 도입을 검토하였으며, 모든 정보를 블록체인에 올리는 대신 해시값만 올리는 방식으로 효율을 극대화하여 운영 중이다.

○ (목표) 지속 가능한 디지털 정부 서비스 구현을 목표로 중앙집권적인 데이터베이스가 아닌 블록체인을 활용을 추진하였다.

- (주체) 에스토니아 정부의 주도로 개발되고 있다.
- (주요 서비스) 납세 시스템, 보건 시스템, 선거 시스템 등 디지털 중앙 정부 서비스를 제공한다.
- (가) 납세(e-Tax) 시스템 : 납세자의 과세 및 환급을 지원하는 전자 납부 시스템으로, 모든 세금 신고 중 95%가 이 시스템을 이용하여 납부 중이다.
- (나) 보건(e-Health) 시스템 : 전자 건강기록(Electric Health Record) 데이터의 무결성을 보장하기 위해 블록체인을 도입하였다.
- (다) 선거(e-Voting) 시스템 : 물리적 위치와 디바이스에 무관하게 인터넷 연결만 되어있으면 간단하고 편리하게 투표할 수 있는 시스템으로 2005년 지방선거에 선거 시스템을 처음 사용하였다. 투표 이후 투표 마감까지 재투표가 가능한 것이 특징이다.
- (라) 전자 영주권(e-Residency) 시스템 : 온라인상에서 가상의 영주권을 발급받고 사이버 영토에서 바로 창업을 할 수 있게 해주는 서비스로 전 세계 누구든지 계좌개설부터 법인설립, 인터넷 뱅킹 등 각종 서비스를 이용할 수 있다.
- (관련 공동인프라 키워드)

				
전자영주권	전자선거	디지털 인증서	데이터 이력추적	데이터진본 확인

(4) 중국 BSN-Enterprise

- (현황) 현재 2022년 2월 기준으로 세계 114개 노드 확보('22.2) 후 40여 개의 공공서비스를 적용 중에 있다.
- (목표) 중국은 법적 제한에 따라 퍼블릭 블록체인 운영이 어렵고 기업용으로 부적합하다는 이유로 인해 허가형 블록체인을 선호해 왔으나 이의 육성과 개발을 위해서는 비용 부담, 상호호환성 미비, 배포 제한 등의

문제점이 존재하였다. 이를 극복하기 위하여 개발 비용 절감 및 편리성 증진, 상호호환성 확보를 통한 블록체인 기술의 개발과 보편적 적용 가속화를 목적으로 BSN(Blockchain Service Network)이 추진되었다.

○ (주체) 중국 국가발전개혁위원회(NDRC) 산하의 국가정보센터(国家信息中心, SIC)를 중심으로 여러 국영·민간 사업자로 구성되어 있다.

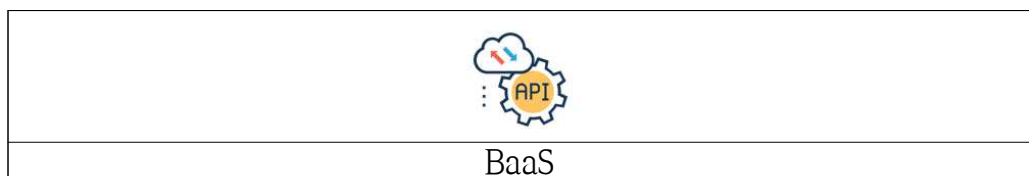
○ (주요 서비스) 블록체인 플랫폼, 블록체인 인프라·프레임워크, 디앱 개발환경 등의 서비스를 제공한다.

(가) 블록체인 플랫폼 : 주요 글로벌 블록체인 플랫폼인 이더리움(Ethereum), 테조스(Tezos), 폴카닷(Polkadot), 이오스(EOS), 클레이튼(Klaytn) 등과의 연동 기술을 지원한다.

(나) 블록체인 인프라·프레임워크 : 개발자가 모든 허가형 혹은 비허가형 블록체인 애플리케이션의 배포와 관리를 용이하도록 하는 기능을 제공한다. 개발자는 스마트 계약을 통해 업로드할 PCN을 선택하면 Fabric, FISCO BCOS 등을 포함한 허가형 블록체인과 퍼블릭 블록체인을 구축할 수 있다. 추가적으로, BSN에 배포된 모든 DApp은 사용 중인 프레임워크에 관계없이 BSN의 인터체인 통신 허브를 통해 상호 호출이 가능하다.

(다) 디앱 개발환경 : BSN을 활용하는 조직과 개인은 필요한 블록체인 서비스와 DApp을 빠르게 구축하고 운영할 수 있다. 자산 디지털화, 위조방지 추적성, 전자정부, 계약 서명, 의료 건강 등 다양한 분야에서 사용할 수 있다.

○ (관련 공동인프라 키워드)

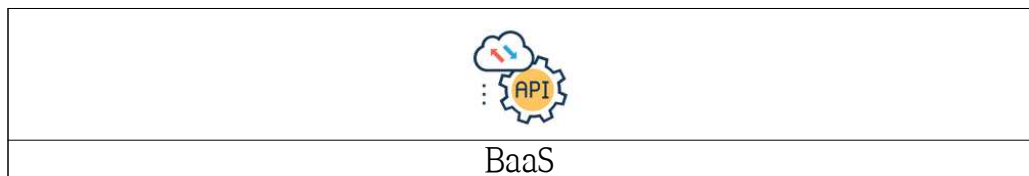


(5) 중국 BSN-Spartan

○ (현황) 비암호화폐 이더리움, 코스모스, 폴리곤 체인을 공개 체인으로 구

성하여 제공하며 개발용 SDK도 출시 예정이다. 체인 내 거래 수수료를 미국 달러(USD)로 결제하는 서비스를 제공하여 해외 확장을 추진하고 있다. 홍콩의 앰퍼러 그룹(Emperor Group), 프레네틱스(Prenetics), 란콰이푹 그룹(Lan Kwai Fong Group), 맥심스(Maxim's), HSBC 및 홍콩 후지필름 비즈니스 이노베이션(Fujifilm Business Innovation Hong Kong) 등이 참여하여 퍼블릭 체인을 통해 디지털 서비스 구축을 실험하는 중이다.

- (목표) 비암호화폐 기반 퍼블릭 블록체인 활용을 통한 BSN의 해외 진출을 목표로 한다.
- (주체) 중국 국가발전개혁위원회(NDRC) 산하의 국가정보센터(国家信息中心, SIC)와 여러 국영·민간 사업자가 주관하여 진행하고 있다.
- (주요 서비스)
 - (가) 퍼블릭 체인을 통해 디지털 서비스 구축을 실험하는 중이다.
- (관련 공동인프라 키워드)



(6) 싱가포르 GovTech의 블록체인 기반 OpenAttestation 프레임워크

- (현황) 2025년까지 세계최초의 스마트 국가 건설과 국제 경쟁력 선점 목표로 스마트네이션 이니셔티브를 본격적으로 추진하였다. 2017년 5월 스마트네이션 및 디지털정보국(SNDGG: Smart Nation and Digital Government Group) 설립 이후, 정부기술청(GovTech)이 총리실에 설치되어 안전한 디지털 서비스와 핵심 솔루션 플랫폼을 제공하고 있다. OpenAttestation은 싱가포르의 스마트네이션 이니셔티브의 일부로 블록체인을 사용하여 문서의 보증 및 검증을 단순화하는 오픈 소스 프레임워크로 개발되었다.
- (목표) OpenAttestation 오픈소스 프레임워크는 블록체인을 사용하여 문서의 무결성 보장, 문서 발급 상태 확인, 발급자 신원 확인을 위한 목적을 가지고 개발되었다.

○ (주체) 싱가포르 정보기술청(GovTech), 스마트네이션 이니셔티브
OpenAttestation

○ (주요 서비스)

(가) 블록체인 기반 문서 무결성 보장, 문서 발급 상태 확인, 분산 신원 증명
이 가능한 OpenAttestation 오픈소스 프레임워크를 개발하여 배포하
였다.

(나) 블록체인 기반인 OpenAttestation 오픈소스 프레임워크는 디지털헬스
여권 등 추가적인 서비스 개발에도 활용하고 있다.

○ (관련 공동인프라 키워드)

			
BaaS	분산신원	데이터이력추적	데이터진본확인

(7) 일본 디지털청의 디지털 사회 실행을 위한 정부 클라우드 및 솔루션 서
비스

○ (현황) 디지털 사회의 실행을 향해, 정부가 신속하고 중점적으로 실시해
야 할 시책을 명기하고, 디지털청을 비롯한 각부 부처가 구조 개혁이나
개별의 시책을 포함하고 있는 “디지털 사회의 실행을 향한 중점 계획”
이 2023년 6월 9일 결정되었다.

○ (목표) “디지털 사회의 실행을 향한 중점 계획”의 일환으로 정부 클라우
드 및 정부 솔루션 서비스(정부 네트워크 정비)의 공급을 목표로 한다.

○ (주체) 일본 디지털청 (Digital Agency)

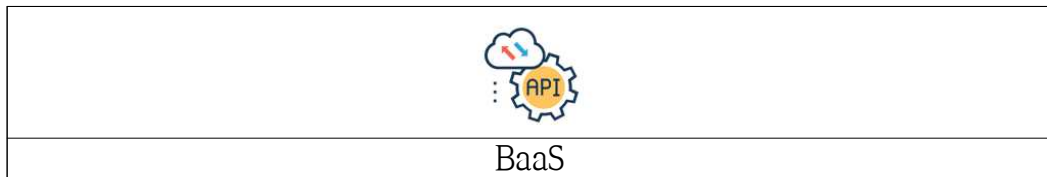
○ (주요 서비스)

(가) 정부 클라우드 서비스를 통해 디지털 사회의 “시스템 및 기술”에
관한 전략의 일환으로 2022년에는 지방자치단체가 주관하는 신규 사
업 및 디지털청의 웹사이트에 점진적으로 적용하는 방안을 시작하였
다. 이를 바탕으로 애플리케이션 개발자의 요구에 따라 자동으로 유연
하고 신속하게 인프라를 준비할 수 있는 환경을 클라우드 기술을 최

대한 활용하여 정부 주도로 공통 서비스를 제공한다. 최신 클라우드 기술을 활용할 수 있는 환경에 대한 템플릿을 사용하여 모범사례를 기본으로 하는 표준 환경을 제공하는 것으로, 정부나 지방 지자체의 애플리케이션 개발의 현대화를 수행한다.

- (나) 정보 솔루션 서비스를 구축하고 디지털청을 통해 정부에 공통적이고 표준화된 업무 수행 환경을 구축한다. 정부 공통의 표준 업무 실시 환경(퍼스널 컴퓨터나 네트워크 환경)의 제공한다. 최신기술을 채용하고, 각부 부처의 환경의 통합을 순차적으로 진행하는 것으로, 행정기관의 생산성이나 시큐리티의 향상을 도모한다.

○ (관련 공동인프라 키워드)



2. 해외 주요 국가의 블록체인 국가 플랫폼 구축 분석 결과 요약

- 유럽 EBSI, 독일 GAIA-X, 에스토니아 전자정부, 중국 BSN-Enterprise 및 BSN-Spartan, 싱가포르 OpenAttestation, 일본 디지털청의 사례를 분석하여 아래와 같이 공동인프라를 도출하였다.
- 해외 주요 국가의 블록체인 핵심서비스 모델 후보 리스트 도출 결과 요약은 다음과 같다.

사례		분산 신원	디지털인 증서	데이터이 력추적	데이터진 본확인	디지털 지갑	BaaS	데이터주 권	전자 영주권	전자 선거
유럽	EBSI	○	○		○	○	○			
독일	GAIA-X	○	○	○	○		○	○		
에스 토니아	전자정부		○	○	○				○	○
중국	BSN -Enterprise						○			
	BSN -Spartan						○			
싱가폴	OpenAttes tation	○		○	○		○			
일본	디지털청						○			
합계		3	3	3	4	1	6	1	1	1

표 7. 해외 주요 국가의 블록체인 공동인프라 도출

- 도출된 9개의 후보 공동인프라는 BaaS(블록체인플랫폼), 분산신원, 디지털인증서, 데이터이력추적, 데이터진본확인, 디지털 지갑, 데이터주권, 전자영주권, 전자선거이다.
- 이중 BaaS(블록체인플랫폼)은 에스토니아 전자정부를 제외한 분석 대상의 국가에 모두 적용된 서비스이며, 유럽 선진국을 중심으로 분산신원, 디지털인증서, 데이터이력추적, 데이터진본확인이 적용되었다.
- 디지털 지갑, 데이터주권, 전자영주권, 전자선거는 각 1개 국가에서 적용된 것으로 확인되었다.

부록 2. 국내 블록체인 과제 현황 분석

1. 국내 블록체인 과제 현황 분석



- (1) 자녀의 올바른 금융 활동을 도와주는 DID기반 부모인증 플랫폼 - (주)아이쿠카
- (목표) 은행 계좌 만들기에서 주식 계좌 만들기 등 시작은 했지만 생활 속 경제 교육의 어려움을 겪는 부모님들을 위해 자녀들은 생활 속에서 경제 원리와 습관을 익히고 부모들은 체계화된 용돈 관리와 경제교육 콘텐츠를 제공하기 목적으로 개발되었다.
 - (사업내용) 대법원 가족관계 증명을 위한 스크래핑 데이터를 토대로 블록체인 DID 증명서비스 개발을 진행하였다. 어린이 경제교육 챌린지 콘텐츠 개발하여, 부모님의 승인 프로세스를 통해 DID 가족관계 통합인증 결제 서비스로 구현하였다.
 - (주요성과) 어린이 경제교육 챌린지 콘텐츠(주제에 따라 챌린지, 온라인 영상 클래스 또는 줌 클래스, 준비물 연계 필요) 개발로 가정 및 학교에서 활용 가능하도록 하였다. 국내는 만 12세 이상부터 체크 카드를 사용할 수 있는 제도상의 문제를 피해 DID 가족관계 통합 인증 프로세스를 반영한 모바일 현장 결제가 가능한 서비스 개발하여 모바일 QR 또는 선불 카드를 통해 오프라인 현장 결제가 가능하고 이용 내역을 앱에서 확인가능하며, 어린이들도 현금을 사용하는 불편함을 선불카드 기능으로 해소하고 부모님이 자녀의 지출 내역 관리 할 수 있는 편리함 제공한다.
 - (주요 서비스) 자녀의 올바른 금융활동을 도와주는 DID기반 부모인증 플랫폼을 구축하여 부모님의 승인 프로세스를 통해 DID 가족관계 통합인증결제 서비스를 제공한다.
 - (공동인프라 키워드)



분산신원

(2) NFT를 포함한 디지털 자산 신뢰검증 서비스 - 한국조폐공사

- (목표) NFT 및 디지털자산 시장의 이해당사자 요구에 부응하여 안전한 생태계 구축이 가능한 신뢰기관의 검증서비스를 제공한다. NFT의 유통 신뢰성 확보를 위한 신뢰기관의 검증서비스를 제공하며 사용자는 신뢰할 수 있는 정보와 안전한 거래를, 제작사와 거래소는 저작물 위변조 및 저작권 검증이 가능한 서비스에 대한 수요가 증가하고 있는 추세이다.
- (사업내용) NFT의 진본성, 저작권 이슈 해소를 위한 혁신적인 블록체인 검증 서비스를 제공한다. 서비스의 검증 대상은 NFT 거래 사업자가 취급하는 NFT로 시범서비스를 시행(B2B모델)하고, 이후 축적된 노하우에 기반하여 자산종류 및 수요 범위를 확대해갈 예정이다. 보관 대상은 신뢰검증 서비스로 발행한 NFT의 원본이며, IPFS 등 외부 분산 저장소에 서의 유실, 훼손에 대비한 차별화 기능을 제공한다.
- (주요성과) NFT를 포함한 디지털자산 시장의 안전한 생태계 구축 기반을 마련하였다.
- (주요 서비스) NFT의 진본성, 저작권 이슈 해소를 위한 혁신적인 블록체인 검증 서비스를 제공하며, 검증 신청시 혹은 검증 완료 후 추가로 신청을 받아, NFT 원본 콘텐츠를 보관하고, NFT 발행 블록체인의 NFT 정보를 신뢰검증 서비스 블록체인에 기록, 검증 결과로서 검증서 조회를 위한 부가정보를 NFT 발행 블록체인에 기록한다.
- (공동인프라 키워드)

	
디지털인증서	데이터진본확인

(3) DID 기반 협업 인재 양성 플랫폼 - 매직에끌

- (목표) 블록체인 DID 기반으로 기업 내부와 외부에서 상호 검증할 수 있는 신뢰 기반 마련 플랫폼 개발을 목표로 하였다.
- (사업내용) 블록체인 DID를 기반으로 프로젝트 협업 이력 관리 주체가 개인을 중심으로 변화되었으며, 기업 내부와 외부에서 상호 검증할 수

있는 신뢰 기반 환경을 마련하였다.



- (주요성과) 매년 500개 기업 대상으로 10,000명을 대상으로 프로젝트 협업 교육을 진행하는 P컨설팅과 디지털 전환을 위한 IT 개발자 100만 명 양성으로 기업 수요 맞춤형 인재 양성을 주도하는 디지털 전환 시대 DID 기반 HR 프로젝트 협업 실증을 진행하였다.

- (주요 서비스) 프로젝트 협업 이력 조회, 서비스 제공자와 기업에 협업 플랫폼 제공을 제공한다.

(가) (프로젝트 협업 이력 조회) 참가자는 DID 앱을 통해 협업 데이터 내역을 블록체인을 통해 인증 및 관리하며, 서비스 제공자와 기업도 DID 앱을 통해 참가자의 활동 및 협업 이력을 조회해 DT 인재 발굴-육성-보상에 활용 가능하다.

(나) (서비스 제공자와 기업에 협업 플랫폼 제공) DID 기술이 접목된 PBT 협업 플랫폼을 클라우드 형태로 쉽게 사용할 수 있는 SaaS 형 API를 서비스로 제공한다.

- (공동인프라 키워드)

	
분산신원	직접구축(BaaS)

(4) NFT 졸업 전시회 서비스 - 블로코엑스와이지

- (목표) 블록체인과 NFT 기술을 이용하여 콘텐츠 소비자와 창작자를 직접 이어주고, 저작이나 소유권 강화를 뒷받침하는 서비스를 목표로 개발되었다.



- (사업내용) 온라인 졸업전시회 서비스를 구현하고, 예비창작자를 위한 콘텐츠, 이력 등재를 블록체인과 NFT를 이용하여 플랫폼 형태로 구현하였다.

- (주요성과) 블록체인과 NFT기술을 이용하여 무결성 및 신뢰성을 보장하는 Web 3.0 환경에서의 차세대 인증 모델을 구현하였다.

- (주요 서비스) 채용 서비스, NFT 기술 기반의 데이터베이스를 제공한다.



- (가) (채용 서비스) 졸업전시회 플랫폼을 통해 리크루팅 서비스를 제공한다.
- (나) (NFT 기술 기반의 데이터베이스) 창작자 프로필, 이력, 포트폴리오 데이터까지 일괄 제공하며 NFT 배지 기반 이력 인증을 통한 신뢰성 보장한다.

○ (공동인프라 키워드)

	
디지털인증서	데이터진본확인

(5) NFT 기반 게이미피케이션 학습 콘텐츠 유통 플랫폼 - 세종텔레콤(주)

- (목표) 게이미피케이션 교육 콘텐츠를 초, 중, 고교에 확산 지원하는 실증 사업을 진행하였다.
- (사업내용) NFT 기반 게이미피케이션 학습 콘텐츠 유통 플랫폼 구축을 진행하였다.
- (주요성과) 불법 복제 및 거래 등 저작권 보호가 가능한 플랫폼과 스마트 계약을 서비스 형태로 구현하였다.
- (주요 서비스) 블록체인 하이퍼레저 패브릭 시스템을 기반으로 학습 콘텐츠 등록 및 유통 서비스와 블록체인 NFT 발행 서비스를 제공한다.
- (공동인프라 키워드)

	
디지털인증서	데이터진본확인

(6) 기업간 신뢰 데이터 전송 및 이력 관리 서비스 - (주)시큐에버

- (목표) 회사/공공기관의 고객사 내부 정보자산(문서, 도면 등)을 블록체인 데이터로 변환한 후 공유 작업자에게 반출하여, 데이터 공유 경로, 상태, 사용 이력을 분산원장으로 관리함으로써 유통 이력에 대한 감사목적을 강화하고, 지속적이고 안전한 데이터 통제를 구현하는 비금융 분야 블록체인 서비스를 제공한다.

- (사업내용) 시큐버의 블록체인 특허 기술을 이용하여 “디지털 데이터 보안”을 적용한 안전한 데이터 공유 플랫폼을 구현하였다.
- (주요성과) 유일한 저작권 디지털 데이터 생성이 가능한 데이터 공유 플랫폼을 구현하고, 안전한 디지털 데이터 보관이 가능한 데이터 공유 플랫폼과 보증된 디지털 데이터 공유(배포, 추적, 삭제)가 가능한 데이터 공유 서비스를 제공한다.
- (주요 서비스) 블록 데이터 송수신 및 블록 정보검증, 분산원장에 의한 데이터 사용이력 보안 관리, 프린터 출력 차단/화면 워터마크 등 다양한 유출 차단 보안, 보안 드라이브 방식의 전자 지갑, 공유 파일의 삭제/회수 등의 서비스를 제공한다.
- (공동인프라 키워드)

		
분산신원	데이터이력추적	디지털 지갑

(7) 기부 펀드 연계 블록체인 플랫폼 - (주)아이티노매즈

- (목표) 한국 최초의 블록체인 기반의 투명성과 추적성을 적용한 기부자 다오(DAO) + 투자(펀드) + 기부 포털 플랫폼을 구축하였다.
- (사업내용) 자립 준비청년 지원을 위한 기부 펀드 연계 블록체인 플랫폼 구축 및 운영을 통해 기부 펀드 연계 블록체인 플랫폼 구축과 금융 영역 및 기부 영역에 대한 서비스를 제공한다.
- (주요성과) 국내 최초의 금융(펀드)와 기부 분야에 블록체인 기술을 적용한 플랫폼을 개발하여, 기부 펀드 운용 및 자립준비청년 지원 서비스를 제공한다.
- (주요 서비스) 기부 펀드 연계 블록체인 서비스를 제공하고, 기부 활성화를 위한 기부 기념 NFT배지 발행과 기부자 존중의 기부 의결권(DAO) 부여한다. 온라인과 오프라인을 통해 모집된 기부금의 펀드 운용 및 운용현황에 대한 블록체인 원장기록과 자립준비청년 지원활동 및 지원현황에 대한 원장기록을 통해 투명성을 보장한다.



○ (공동인프라 키워드)


디지털인증서

(8) NFT와 QR코드를 이용한 의류 정품인증 서비스 - 동대문패션타운관광특구협의회

- (목표) 원산지 위변조 방지, 패션 제조업 활성화, 국산 원자재 공급 촉진, 중소기업과의 상생협력을 목적으로 한 NFT와 QR코드를 이용한 의류 정품인증 서비스를 제공한다.
- (사업내용) 동대문에서 제조 및 상품화되는 의류의 정품인증 체계 적용하여 유통 및 소비자 보호 시스템 구축하고 NFT 기술 기반의 투명하고 신뢰성 있는 정보화 시스템 제공한다.
- (주요성과) 정품인증 시스템을 적용한 제조자의 생산 프로세스, NFT 기반의 유통 및 소비자 보호, NFT 기술 기반의 투명하고 신뢰성 있는 정보화 시스템을 제공한다.
- (주요 서비스) NFT와 QR코드 기반으로 정품인증 시스템을 적용하여 제조자의 생산 프로세스, 유통 및 소비자 정보시스템 구축하여 서비스를 제공한다.

○ (공동인프라 키워드)



	
데이터이력추적	데이터진본확인

(9) 웹 3.0 서비스 사용자를 위한 소셜인증 및 웹지갑 서비스 - (주)지란지교시큐리티

- (목표) 웹 2.0과의 호환성을 가진 웹 3.0기반의 통합인증 및 암호화폐 지갑 관리 서비스를 개발하여 토큰 배분과 고도의 인증/보안을 고려하지 않고도 쉽게 웹 3.0으로의 전환을 가능하게 해주는 웹 3.0 통합인증 API 및 암호화폐 지갑 관리 API 서비스를 개발하였다.
- (사업내용) 별도의 절차를 거치지 않고도 소셜 인증을 통해 쉽게 서비스에 가입하여 통합 웹 3.0 인증 서비스와 가상자산 지갑을 보유할 수 있

는 서비스를 제공한다. 자동으로 전자지갑을 생성하고 생성된 전자지갑의 키를 안전하게 클라우드 시스템에 분산 및 분리 보관하는 전자지갑 관리시스템을 통해 사용자가 자신의 지갑을 조회하고 필요에 따라 추가 삭제가 가능하고 다수의 지갑을 통합 관리할 수 있는 서비스를 GUI 형태로 제공한다.

- (주요성과) 개인의 가상자산을 안전하게 지켜내는 인증 및 자산통합관리 시스템의 구현과 웹 3.0 서비스 취약점 및 한계성 보완하였다.
- (주요 서비스) 통합인증 웹 3.0 포털과 전자지갑 관리시스템을 제공한다.
- (공동인프라 키워드)

	
디지털인증서	디지털 지갑

(10) 블록체인기반 '커리어뱅크' (공모전 수상 경력관리) 플랫폼 - 디엑스웍스 주식회사

- (목표) 공모전 수상자들이 손쉽게 본인의 이력을 공신력 있게 증명받고 진학. 취업. 창업 등에 활용함은 물론, 주최측에서도 자체적으로 관리시스템을 구축할 필요 없이 '블록체인 기반 공모전 수상/입상 경력관리 플랫폼'에서 관리될 수 있는 서비스를 제공한다.
- (사업내용) 블록체인 기반 공모전 경력관리 플랫폼을 구축하여 공모전 시작부터 마무리까지의 프로세스 주기 동안 생성되는 다양한 데이터를 블록체인 기술을 활용해 저장하고 활용한다. 개인정보 및 다수의 민감정보를 비식별화 및 암호화 기능을 통해 보호하며, 플랫폼 이해관계자의 역할에 맞는 공통 코드 관리, 회원 관리, 통계 관리, Open API 관리, 플랫폼 히스토리 관리 등 다양한 운영 기능을 구현하고 노드 및 블록체인 생성상태 모니터링 기능을 제공한다.
- (주요성과) 분산신원인증(DID) 기술을 활용하여 최소한의 개인정보만으로 신원을 인증하고, 블록체인상의 신원증명에 대한 주도권을 사용자가 가짐으로써 추후 발생할 수 있는 보안 문제를 해소하고, 플랫폼 전체를

자체 구축 클라우드에 적재함으로써 민간클라우드 서비스 운영에 유연함을 더하고 플랫폼 구축 및 운영에 발생하는 비용을 절감하는 효과가 있다.

- (주요 서비스) 공모전 관리 서비스, 포트폴리오 관리 서비스, 검증기능 서비스, 자체 오픈스택 클라우드 시스템 환경 구축 및 블록체인 플랫폼 제공한다.

- (공동인프라 키워드)

		
분산신원	데이터진본확인	직접구축(BaaS)

(11) 보육료 지원 사업 중복수급관리 - (주)리드포인트시스템



- (목표) '22년 블록체인 시범사업(복지급여 중복수급 관리)'의 플랫폼 확대 구축 및 보육료 지원사업 중복수급 관리에 필요한 효율적 업무처리 절차 제시로 국민 모두가 함께 잘사는 포용사회 비전 수립과 신뢰성의 제고를 목적으로 한다.

- (사업내용) 블록체인 확산 및 보육료 지원사업 중복수급 관리 구축을 통하여 국민 모두가 함께 잘사는 포용사회 수립에 효과적으로 대응할 수 있는 기반을 제공한다.



- (주요성과) 정부차원의 대국민 중복수급 공유 서비스, 특정산업/단체 차원의 공유 서비스를 제공하여 공유 서비스 외 타 업무에 활용이 가능하다.

- (주요 서비스) 보육료 지원사업 중복수급 관리 기능 제공, 통계 및 모니터링 보고서 서비스를 제공한다.

- (공동인프라 키워드)

	
디지털인증서	데이터이력추적

- (12) 블록체인 기반의 드론 자격·증명 서비스 체계 구축 - 마크애니 컨소시엄
- (목표) 조종자 확인, 기체 확인, 비행 승인 확인이 가능한 블록체인 기반의 드론 자격증명 서비스와 블록체인 신기술 적용 드론조종자 자격·기체신고, 증명 기술개발을 목적으로 진행되었다.
 - (사업내용) 드론조종자 자격·증명의 신뢰성, 투명성, 편의성을 제공하기 위한 블록체인 기반 드론 종합안전관리 플랫폼을 구축하였다.
 - (주요성과) 국민에게 신뢰받을 수 있는 DID 자격증명 체계 마련과 자격증명의 무결성 검증이 가능해 드론 자격증명 체계에 대한 신뢰성과 책임성 확보 토대 마련하였다. 세계 최초, 블록체인을 활용한 드론 자격증명 체계 실증 플랫폼 구축으로 디지털 자격증명 및 활용 사례를 남겼으며, 자격증명의 이력 및 내용 확인 서비스 등 향후 연계 및 확장 서비스가 가능하다.
 - (주요 서비스) 블록체인 기반 통합 회원관리 서비스, 블록체인 분산신원(DID) 기술을 이용한 모바일증명 서비스, 분산신원 검증 서비스를 제공한다.
 - (공동인프라 키워드)

	
분산신원	데이터진본확인

- (13) 블록체인 기반 바이오 원재료 이력관리 플랫폼 구축 - 블록오디세이
- (목표) 블록체인 기반의 바이오 원재료 이력관리 플랫폼 구축으로 충북 인삼 가공 제품 대상 실증기반 바이오 원재료 이력 관리 서비스를 제공한다.
 - (사업내용) 블록체인 기반 바이오 원재료 이력관리 플랫폼을 구현하고 플랫폼의 확산을 도모한다.
 - (주요성과) 블록체인 기반의 바이오 원재료 이력 관리를 통해 수요자의 만족도와 원재료 이력에 대한 신뢰성을 향상하였다.
 - (주요 서비스) 블록체인 기반 바이오 원재료 이력관리 플랫폼 구축과 서

비스를 제공한다.

- (공동인프라 키워드)





(14) 블록체인 기반 공공일자리 지원 사업 전자근로계약 및 이력관리 플랫폼 구축 - 비디젠 컨소시엄

- (목표) 블록체인 및 DID 기반 전자근로계약 서비스 구축을 통해 공공일자리 전자근로계약 도입 활성화와 일자리 지원사업 업무 효율 증대를 목표로 개발하였다.
- (사업내용) 서울시와 출자/출연기관이 수행하는 공공일자리 지원사업에 있어 전자근로계약 도입을 통해 근로자 편의성과 운영기관 업무 효율성을 제고하고 사용자 포탈 구축 및 서울지갑 앱 개선을 통한 전자근로계약 체결을 지원하여, 계약서 이력관리를 위한 블록체인 구축 및 TSA 원본 증명 연동과 공공일자리 근로계약에 대한 각종 증명서 발급 시 발생하는 근로자의 신청 절차의 번거로움과 이용기관의 과거 계약이력 확인을 위한 업무 부담을 경감시키는 서비스이다. 주요 서비스는 DID를 통한 계약증명, 재직증명, 경력증명 발급, 증명 데이터의 사용자 단말 저장을 통해 개인정보보호 및 근로자 자기주권 강화가 가능하다.
- (주요성과) 전자근로계약 도입 활성화를 통한 근로자 편의성 향상, 이용기관 업무 효율화 및 공공일자리 근로계약의 신뢰성 제고
- (주요 서비스) 블록체인 기반 공공일자리 지원 사업 전자근로계약 및 이력관리 플랫폼 서비스와 서울지갑 앱을 제공한다.
- (공동인프라 키워드)

				
분산신원	디지털인증 서	데이터이력 추적	데이터진본 확인	디지털 지갑

(15) 편리하고 투명한 아파트 관리 서비스 - 비케이위너(주)

- (목표) 공동주택 관리자들의 열악한 근무 조건 및 공동주택 관리사무소의 아날로그식 업무 환경을 개선하고 공동주택 관리사무소와 지자체 및 공공기관과의 연계 가능한 블록체인 기반의 서비스를 개발하였다.
- (사업내용) 전자 결재 규격화, 관리사무소 업무 환경 개선, 지자체 및 공공기관의 연계, 방문 차량 예약 시스템을 구축하였으며, 합의를 담당하는 Orderer 노드 추가, 주요 데이터의 변경 이력 추적 서비스, 블록 데이터 유효성 검증 서비스를 개선하였다.
- (주요성과) 공동주택 관리자들의 열악한 근무 조건 및 공동주택 관리사무소의 아날로그식 업무 환경을 개선하며, 보안성이 강화된 블록체인 기반의 아파트 관리 서비스를 구축하였다.
- (주요 서비스) 블록체인 기반의 표준화 전자 결재 서비스
- (공동인프라 키워드)

	
분산신원	데이터이력추적

(16) DID기반 신원인증 및 비대면 민원서비스 플랫폼 구축 - 에스지에이솔루션즈 컨소시엄

- (목표) DID 기반 공무원연금증을 통한 신원증명 서비스와 전자문서지갑을 활용한 비대면 민원서비스 개발로 공단의 비대면 서비스 확대 및 사용자 편의 향상 기여를 목적으로 진행하였다.
- (사업내용) DID 기반 온/오프라인 신원증명 서비스를 통해 연금수급자 모두 이용할 수 있는 신원인증 서비스 제공으로 신분증 관리 비용 절감, 사용자 편의성 및 개인정보보호 강화는 물론 전자문서지갑을 활용한 비

대면 민원서비스를 통해 민원서류의 비대면 발급/제출로 업무절차와 비용을 절감하고, 사용자 편의성 제고하였다.

- (주요성과) DID 및 블록체인 기술을 활용하여 비대면 서비스 확대 및 사용자 편의 증대와 비접촉 출입통제 시장 경쟁력 확보하였다.
- (주요 서비스) DID 블록체인 플랫폼, DID 기반 온/오프라인 신원인증 서비스, 전자문서지갑 기반 비대면 민원 처리 서비스를 제공한다.
- (공동인프라 키워드)

		
분산신원	데이터진본확인	디지털 지갑

(17) 모바일 선원자격증명 서비스 구축 - 오픈스엠 컨소시엄

- (목표) 블록체인 기반의 분산신원(DID)을 이용한 모바일 선원자격증명 서비스를 제공한다.
- (사업내용) 선원 민원 전산시스템의 디지털 전환과 선원 민원업무 보안 강화하였다.
- (주요성과) 선원 면허 증서 디지털 전산화 및 자격증명 서비스 고도화 향상을 통해 승하선 공인 업무 개선과 선원 자격증명서 등 글로벌 표준화 기반 마련하였다.
- (주요 서비스) 선원 자격증명 기반 통합 플랫폼을 구축하여 해양수산부 PORT-MIS 관리 연계, 선원 센터 직업 안정 시스템 연계, 선원 교육/시험 통합 시스템 연계 및 간편인증 서비스를 제공한다.
- (공동인프라 키워드)

		
분산신원	데이터이력추적	데이터진본확인

(18) 블록체인 기반 배움이력 통합관리 플랫폼 구축 - 이투스 컨소시엄

- (목표) 블록체인 기반 배움이력 통합 관리 플랫폼 구축을 통한 증빙서류

발급 제출 체계 개선. 증빙자료 진위 검증 업무의 전산화를 통한 업무 효율성 극대화를 목표로 진행하였다.

- (사업내용) 블록체인 기반 배움이력 통합 플랫폼 구축, 블록체인 기반 증빙자료 통합 저장 및 발급 플랫폼 구축, 블록체인 기반 참여 기관 연계 및 협업이 가능한 서비스 모델 개발, 데이터 저장, 기록, 발급을 위한 표준 데이터 구축, 학습이력 증빙서류 제출 및 자격요건 검증 시스템 구축, 자격증 신청 자격요건 검증에 필요한 업무 자동화 및 자격증 신청 자격요건에 대한 관리체계를 진행하였다.
- (주요성과) 업무시간 감소와 불필요한 종이 발급 비용 절감하고 안전성과 신뢰성 기반 블록체인 기술 적용한 이용자에 대한 편의성 및 간소화에 따른 삶의 질 향상과 자격증 취득 지원자(연간 9,700만명)등에 대한 수강이력 증빙자료 발급 간소화
- (주요 서비스) 배움이력통합관리전자지갑(App, 서비스명 변경 예정) 및 배움이력통합관리플랫폼(Web, 서비스명 변경 예정)을 제공한다.
- (공동인프라 키워드)

				
분산신원	디지털인증서	데이터이력추적	데이터진본확인	디지털지갑

(19) 블록체인 온라인투표시스템 기반 강화- (주)인재아이앤씨 컨소시엄

- (목표) 블록체인 기반 온라인투표시스템 개발을 통해 비밀투표 보장 및 익명성 검증성 강화를 통한 대국민 신뢰기반 조성하고, 주민투표의 온라인투표 실시 대비 서비스 구성 및 제공 기반 확보하여 다양한 선거수요 및 변화 대응을 통한 고객만족도 및 관리능력 향상을 목적으로 한다.
- (사업내용) 이해관계자 노드 정보 제공을 위해 최신 암호화 기술 적용 등 보안을 강화하고 HSM 및 영지식증명 도입, DID 및 동형암호화, 블록체인 시스템 성능 보장 및 인프라 확충, 블록체인 노드 성능 보장, 주민투표 대비 명부시스템 구축 및 투개표 플랫폼 신원확인체계 고도화, 블

록체인 온라인투표시스템 전용 선거인명부시스템 구축, 투표방식 및 본인인증 다양화 등을 추진하였다.

- (주요성과) 주민투표 시 개인정보 수집 최소화 및 온라인투표시스템 전용 선거인명부시스템 구축·운영을 통한 각종 선거 상황별 탄력적 대응 가능하며, 스마트폰 등 선거인 사용 단말기 종속성 탈피 및 다양한 선거 서비스 채널 제공 등 사용자 편의성이 향상되었다. 선거개설 및 명부 등록, 투표 및 개표 등 일련의 절차에 관련된 편리성 강화 및 보안 강화, 개인정보의 안전한 관리 및 선거인정보와 투표정보의 분리 등 비밀투표 기반 강화를 통한 정보관리의 신뢰성 및 안정성을 확보하였다.
- (주요 서비스) 블록체인 네트워크 구성, 키 관리 서비스, 블록체인 관리 서비스, OPEN-API 제공한다.
- (공동인프라 키워드)



					
분산신원	디지털인 증서	데이터이 력추적	데이터진 본확인	직접구축 (BaaS)	전자선거

(20) 블록체인기반 특허NFT 거래 플랫폼 구축 - (주)평가

- (목표) 지적 재산권의 발행, 거래 및 NFT 화할 수 있는 지적재산권 발행, 거래 플랫폼 구축을 진행하였다.
- (사업내용) 지적 재산권을 NFT화하여 디지털화하고 이 과정에서 발생할 수 있는 법적이슈와 권리 계약관계를 제도권 내에서 시스템화하고 소유권의 분할과 이전 및 거래가 가능한 플랫폼 구축을 진행하였다. 클라우드 기반 인프라 환경 구축, NFT 발행 플랫폼, 거래 플랫폼, 관리자 시스템으로 구성되며, 기타 규제 프레임워크와 경쟁력있는 상품 개발을 위한 방법 등이 적용되었다.
- (주요성과) 지적재산권 분할 판매 및 거래 시장 조성을 위한 지적재산권 거래 플랫폼을 통해 특허권 거래 시장을 창출하고 자체 알고리즘과 지적 재산권의 가치 평가를 쉽게 할수 있는 지표들을 제공하여 일반인들

에게 전달 가능하다. 특허권 변경 절차를 NFT를 통해 간소화할 수 있으며 블록체인을 통해 특허권 검증이 가능한 기능들을 제공한다.

- (주요 서비스) 클라우드 기반 인프라 환경에서 지적재산권 발행, 거래, 관리, 규제준수 프레임워크 제공 및 블록체인 기반 특허 NFT 거래 서비스를 제공한다.
- (공동인프라 키워드)

	
디지털인증서	데이터진본확인

(21) 블록체인 기반 한약 전주기 관리 플랫폼 구축 - 오픈스옴 컨소시엄

- (목표) 한약재 원료의 입고, 처방, 조제, 유통 과정별 생성 정보를 블록체인에 저장하여 일반 국민들의 복용 한약에 대한 불신감을 해소하고 원료 한약재의 수급 관리에 필요한 데이터 축적하기 위한 목적으로 진행되었다.
- (사업내용) 일반 국민들은 원료 한약재의 식용·약용 재료의 혼용, 불법 약재의 유통에 대한 우려로 한약 복용에 대해 불신을 갖고 있으며 이로 인한 한약 산업의 소비 위축과 개별 한방 기관 위주의 약재 처방과 조제, 유통 등으로 인해 원료 약재의 안정적인 수급 관리가 어려운 상황을 해결하기 위해, 위변조 방지를 위한 투명성 및 데이터 신뢰성이라는 블록체인의 기술적 장점을 활용하여 블록체인 기반의 관리 플랫폼을 구축하여 한약의 생산부터 복용까지의 전체 취급 업무의 투명성을 강화하고, 원료 약재의 수급 현황에 대한 데이터를 축적하여 수급 및 관리체계 효율화 방안 마련하였다.
- (주요성과) 분산 원장과 위변조 방지를 통한 한약 이력 데이터의 투명성 확보 및 데이터 신뢰성을 제공하는 블록체인의 기술적 장점을 활용하여 실제 일반 국민들이 체감할 수 있는 블록체인 활용성을 제시하였으며, 한약재 원료의 사용 현황 데이터의 축적 및 관리를 통한 안정적 한약 원료 수급 관리 체계 마련하고 안전한 한약재 유통에 대한 사회적 인식

의 확산과 대국민 신뢰도 제고하였다.

- (주요 서비스) 참여 기관별(hGMP, 표준조제시설, 한방병원, 한의학진흥원) 및 일반 국민 대상의 원료 한약재 분류 코드 및 관련 데이터를 활용한 사례검증 서비스를 제공한다.
- (공동인프라 키워드)

		
디지털인증서	데이터이력추적	데이터진본확인

(22) 건축, 공연예술 NFT제작 및 전시 플랫폼 구축 - (주)모핑아이

- (목표) 하이브리드 블록체인 기반의 공간예술 IP NFT제작과 스트리밍 플랫폼 구축으로 전 국민이 공간예술 IP를 검색, 나만의 공간 예술을 2차 창작/제작, 유통하여 현실과 메타버스에서 전시까지 할 수 있는 서비스를 구현하였다.
- (사업내용) 공간 예술영역 IP의 보호와 2차 창작활동 장려를 목표로 스마트 컨트랙트에 의한 적절한 보상 체계를 적용하기 위해 공간 예술과 관련된 IP들을 NFT 화하고 NFT 마켓플레이스에서 거래될 수 있는 다양한 서비스를 제공하였다.
- (주요성과) 그림과 음악에만 한정적으로 이용되고 있는 'NFT 산업군의 한계' 극복하여 수준 높은 수요처에 의해 예술가 아니면 작품을 선보이기 힘든 '수요처의 한계' 극복하고자 하였다.
- (주요 서비스) 공간 예술 IP NFT 제작하여 관리하는 NFT Bank 및 NFT Mall 구축하고 하이브리드 블록체인 기반 프로세스 관리 서비스 및 NFT 신뢰 검증 서비스를 제공한다.
- (공동인프라 키워드)

		
디지털인증서	데이터진본확인	직접구축(BaaS)

(23) 블록체인 적용 공공마이데이터 유통체계 신뢰기반 구축 - 솔리데오시스 템즈 컨소시엄

- (목표) 국민의 자기정보 통제권을 강화하는 공공 마이데이터 유통체계에 블록체인을 적용하여 정보주체가 제공한 데이터가 보유기관에서 전송되어 이용기관에서 활용되기까지 공공 마이데이터의 생애주기 관리를 통해 공공마이데이터 유통체계의 신뢰기반을 구축하기 위한 목적으로 진행되었다.
- (사업내용) 공공마이데이터 유통 체계 적용을 위한 블록체인 플랫폼 개발하고 블록체인을 활용한 진위확인 서비스와 시범서비스를 진행하였다.
- (주요성과) 블록체인 기반 신뢰 기반 확보를 통해 공공 마이데이터 활용성 극대화 및 신속하고 편리한 데이터 기반 행정 서비스 구현하였다.
- (주요 서비스) 블록체인 플랫폼 관리, 블록 관리 및 노드 구성, 접근통제 및 감사기록 관리 및 응용 시스템 연계 서비스 제공
- (공동인프라 키워드)





		
디지털인증서	데이터이력추적	데이터진본확인

(24) 블록체인 적용 공공 마이데이터 유통체계 신뢰기반 구축 - SK텔레콤 컨소시엄

- (목표) 백신접종증명 서비스 제공으로 DID 서비스 확산을 목표로 진행하였다.
- (사업내용) 코로나19 예방접종 정보를 발급하고 코로나19 예방접종 정보 발급/제출하는 앱 서비스를 개발한다. 이와 더불어 코로나19 예방접종 정보와 기존 증명 결합제출 기능을 개발하였다.
- (주요성과) 간편한 접종증명체계 확립하고 국민의 생활편익 증진에 기여하였으며 DID 서비스를 확산하였다.
- (주요 서비스) 질병관리청과 연동한 백신증명 발급 서비스 개발하였고, 통합 Verifier 서비스 구축 (별도 검증 앱 등으로 검증 시)하였다. 또한

서비스 연동 관련 기술 규격 및 개발 가이드 배포하였다. 이와 더불어 결합제출 QR 및 연동 규격, Holder App 연동 표준 규격을 제공하였다.

○ (공동인프라 키워드)



				
분산신원	디지털인증서	데이터이력추적	데이터진본확인	디지털지갑

(25) DID와 블록체인을 활용하여 개인의료정보 기반의 안심활동 정보 제공 - NDS컨소시엄

- (목표) 병원, 보건소, 검사기관 의료기관들이 개인의료정보를 안전하게 송수신하고, 이를 다시 정보 주체인 개인에게 전달하는 과정에서 DID와 블록체인을 활용하여 정보 전달 오류 및 위변조 방지 등 위험요소를 극복하여 안전한 전달할 수 있는 방법을 발굴하고, 코로나 19와 전염병 대응과 같이 빠르고 정확한 정보 전달 및 이력관리가 핵심인 사업에 적용하여 안심활동 정보 제공 등 효과적인 활용 방법을 발굴하였다.
- (사업내용) 개인의료정보를 익명으로 관리할 수 있도록 DID를 적용하여 기관과 개인간 안전한 데이터 연동 플랫폼 구축하였다. 검사 결과를 조회하기 위하여 병원, 보건소로부터 확보된 검사 데이터를 DID와 블록체인을 활용하여 안심패스 시스템으로 안전하게 전송 및 관리하며, 이를 활용하여 코로나19 안심 상태를 확인할 수 있는 코로나19 음성검사, 항체형성 검사 데이터를 통합 관리하고 백신예방접종 데이터를 추가하여 실시간으로 검증할 수 있는 모바일 앱 개발, 의료기관 간 데이터 연동을 검증할 DID, DID 상호인증 기능 검증 서비스 운영 시 발생하는 이슈와 대응 방안 검증을 통해 운영 기반 기술을 확보하였다.
- (주요성과) 개인의료정보가 포함된 데이터 연계를 DID와 블록체인 활용 연계기능 검증하고 안심패스 모바일 앱을 활용하여 팬데믹 속에서도 안심하고 일상생활을 할 수 있는 기반을 제공하였다. DID 기반으로 의료

데이터는 물론 금융 데이터에 대해서도 통합 가능성을 검증하여 MyData 사업 활성화 기반을 마련하였다.

- (주요 서비스) 수탁 검사기관 시스템 연계 및 안심 패스 플랫폼(DID, 블록체인)을 구현하고 연계 및 검증 시스템 간 유기적인 연동 체계를 구축하였다.
- (공동인프라 키워드)

	
분산신원	데이터이력추적

(26) 차세대 식당 국산김치 자율표시 시스템(K-Kimchi Labelling) 구축사업 - 퓨처센스 컨소시엄

- (목표) 차세대 식당 국산김치 자율표시 시스템(K-Kimchi Labelling) 구축사업은 대한민국김치산업이 외국산 김치의 위협 속에서 시장질서를 회복하고, 특히 식당을 중심으로 추진 중인 국산김치 자율표시의 성과를 내도록 지원하는데 그 목표를 두었다.
- (사업내용) 본 사업의 범위는 709,014개소의(2018년 기준, 2020 식품외식 통계) 식당과 국산김치 자율표시제도이며, 이를 위해 기존 운영 중인 식당 국산김치 자율표시 시스템을 통합하고, 차세대 식당 국산김치 자율표시 시스템(K-Kimchi Self Labelling) 구축하였다.
- (주요성과) 개인의료정보가 포함된 데이터 연계를 DID와 블록체인 활용 연계기능 검증하고 안심패스 모바일 앱을 활용하여 팬데믹 속에서도 안심하고 일상생활을 할 수 있는 기반을 마련하였다. 금융 데이터에 대해서도 통합 가능성을 검증하여 MyData 사업 활성화 기반을 마련한다.
- (주요 서비스) 차세대 식당 국산김치 자율표시 시스템(K-Kimchi Labelling)을 통해 국산김치 자율표시 서비스를 제공한다.
- (공동인프라 키워드)

		
분산신원	데이터이력추적	디지털 지갑

(27) DID 주주증명기반 비대면 전자주총 - 한국전자투표 컨소시엄

- (목표) DID를 활용한 주주증명을 통해 소외된 소액주주들의 주총 참여 및 의결권 행사를 강화하고 비대면 주주총회 확대를 통한 비용절감, 검증 등을 통한 투명성 확보 등을 목표로 한다.
- (사업내용) 기업소유의 주주명부 기반으로 주주증명서를 발급하고, 온라인 주주투표의 개설, 개시, 주주증명검증, 종료, 집계를 자동화한다. 또한 온라인 주주투표집계에 대해 블록체인기반의 검증기능을 제공한다.
- (주요성과) DID 주주증명기반 비대면 전자주총을 구축하여 개인정보 유출 방지, 해킹 위·변조 방지, 온라인투표 신뢰성 제고, 블록체인투표 표준 제시, 보안비용절감에 기여하였다.
- (주요 서비스) 전자 주주총회 시스템 및 관련 모바일 앱, Issuer 기능을 서비스 형태로 제공한다.
- (공동인프라 키워드)



			
분산신원	디지털인증서	데이터진본확 인	전자선거

(28) 바이오의약품 전용 스마트 콜드체인 플랫폼 구축 및 적용 사업 - 주식회사 한진 컨소시엄

- (목표) 바이오의약품 물류관제 플랫폼 및 전용 IoT장비 개발을 통한 생산에서 소비까지 전 과정의 콜드체인 물류체계 구축하고 블록체인 기술기반의 ‘미래형 블록체인 유통지원체계’를 실증하여 의약품 유통 품질 보증 및 국민보건 향상에 기여하기 위한 목적으로 진행되었다.
- (사업내용) 바이오의약품 물류관제서비스 플랫폼을 구축 및 운영하고 바이오의약품 품목 및 입출고 관리서비스 시스템 개발과 바이오의약품 배

송용기, 배송차량, 바이오의약품 물류 체계를 실증하였다.

- (주요성과) 의약품 유통 전 과정에서의 콜드체인 시스템 구축 및 적용을 통한 의약품 유통 품질 보증으로 국민보건 향상에 기여한다.
- (주요 서비스) 의약품 전용 온습도센서(용기 외부설치), 차량 및 냉장고용 IoT 온습도 센서, 게이트웨이, 항공물류 연계 물류관리 플랫폼 및 서비스 앱이다.
- (공동인프라 키워드)

	
디지털인증서	데이터이력추적

(29) 분산신원(DID) 기반 수요자 맞춤 모바일 교통카드 발급 및 무인 편의점 출입 서비스 - 코인플러그



- (목표) 분산신원 기반 수요자 맞춤 모바일 교통카드 발급 서비스 구축하고, DID 기반 수요자 맞춤 모바일 교통카드를 통한 복지 연계 서비스 기반을 마련하고, 분산신원 기반 신원확인을 통한 비대면 및 비접촉 무인 편의점 출입 서비스를 구축하였다.
- (사업내용) DID 기반 수요자 맞춤 모바일 교통카드 발급 서비스 구축하고, DID 기반 수요자 맞춤 모바일 교통카드를 통한 복지 연계 서비스를 제공한다. DID 기반 비대면 및 비접촉 무인 편의점 출입 서비스를 구축하였다.
- (주요성과) DID 기반 수요자 맞춤 모바일 교통카드 도입에 따른 비용을 절감하고, 대중교통 복지서비스 일원화에 따른 서비스 운영비용이 감소한다. DID 기반 신원인증을 통한 무인 편의점 출입으로 고정비용을 절감하였다.
- (주요 서비스) 분산신원(DID) 기반 수요자 맞춤 모바일 교통카드 발급 서비스와 DID 기반 수요자 맞춤 모바일 교통카드를 통한 복지 연계 서비스 그리고 분산신원(DID) 기반 신원확인을 통한 비대면 및 비접촉 무인 편의점 출입 서비스 및 B PASS 연계 서비스를 제공한다.

○ (공동인프라 키워드)


분산신원

(30) 블록체인 기반 차세대 미디어 콘텐츠 플랫폼 - 바른손 / 프렌즈게임즈

- (목표) P2P 스트리밍 서비스 이용자들의 참여정보에 블록체인을 적용하여 확장과 확산이 용이한 차세대 블록체인 기반 영화서비스 플랫폼을 제공한다.
- (사업내용) 실시간 딥러닝 업스케일링과 공간음향 및 극장 시뮬레이션 사운드, 실시간 번역 서비스 등의 기술을 통해서 타 스트리밍 플랫폼과 차별화하며 중소규모, 다양한 장르의 영화로 차별화된 콘텐츠를 지향하는 콘텐츠 플랫폼 구축하고 영화 인프라 및 행사들과 연계하여 영화 투자 환경 조성 및 온라인 영화제에 대한 새로운 접근을 시도한다.
- (주요성과) 유희 컴퓨팅 자원을 활용한 매쉬망 P2P 시스템과 딥러닝을 이용한 업스케일링과 TTS 기술을 통해 장비와 언어에 구애를 받지 않고 문화 향유의 장애물을 제거하였다.
- (주요 서비스) 블록체인 인증 서비스와 투자금 관리툴, 온라인 스트리밍 서비스를 제공한다.
- (공동인프라 키워드)



	
디지털인증서	데이터이력추적

(31) 블록체인 기반 의료용 마약류 관리 플랫폼 구축 - 오픈스옴 컨소시엄

- (목표) 병원 내 의료용 마약류 취급업무 정보를 스마트계약에 의해 블록체인에 저장하여 관리/감독자에게 블록체인 기반의 신뢰도 높은 통계 및 보고 자료를 제공하기 위한 목적으로 진행하였다.
- (사업내용) 병원 간 업무 체계 및 데이터의 비표준화로 인하여 의료용 마약에 대한 통계만 제공되고 있어 위·변조 방지를 통한 투명성 및 데

이터 신뢰성이라는 블록체인의 기술적 장점을 활용할 수 있는 블록체인 기반의 관리 플랫폼을 구축하여 의료용 마약류 취급업무의 투명성을 강화하고, 보고 및 관리체계 효율화 방안 마련하였다.

- (주요성과) 블록체인 기반의 의료용 마약류 취급 업무 관리를 통해 관리, 감독기관 보고 정보의 신뢰성을 강화하여 의료용 마약류 관리 감독 체계의 기반을 마련하였다.
- (주요 서비스) 블록체인 네트워크상에 플랫폼 서비스를 구축하고, 사용자 접근을 위한 애플리케이션 서비스와 외부 시스템 연동을 위한 시스템 서비스를 제공한다.
- (공동인프라 키워드)

	
디지털인증서	데이터이력추적

(32) 주문배송 O2O 생태계 전반 DID집중 구축 사업 - 코인플러그 컨소시엄

- (목표) 본 사업을 통해 구축되는 신규 마이키핀 기반 참여자 인증 시스템과 신규 주문/배달 중개 플랫폼을 구축하고 실증을 통해 얻은 데이터를 바탕으로 시스템 고도화하여 전국망으로 확대하고자 하였다.
- (사업내용) 소비자 주문앱 및 배달중개를 위한 소상공인 POS, 지급결제 및 정산시스템, 그리고 주문서버 및 배달중개 서버와 퍼블릭 블록체인 DID 인증시스템인 마이키핀 인증서버로 구성되며, 주문서버와 데이터센터 내 가상머신 서버로 API/SDK 구축을 진행하였다.
- (주요성과) 주문배송 분야에 있어서도 DID를 적용하여 배달 생태계 내의 사례를 확보하였다.
- (주요 서비스) 블록체인 DID 기반의 O2O 플랫폼을 통해 비대면 연령확인 인증서, 가맹점 POS 출금 권한 관리 서비스를 제공한다.
- (공동인프라 키워드)



분산신원

- (33) 블록체인 기반의 비대면 본인확인 및 결제 플랫폼 - 코인플러그 컨소시엄
- (목표) 블록체인 기반 DID인증과 생체인증(안면·음성)의 융합을 통해 인증의 신뢰성, 무결성을 동시에 확보하는 시스템을 구축하였다. 또한 비대면 환경에서 원격으로 사용자의 생존여부를 확인하여 국민연금의 부정수급을 방지하고 수급자를 대상으로 DID를 발급하여 수급자의 신원 증명이 가능하고 수급자가 제출하는 증빙서류에 대한 무결성 및 부인방지를 통한 정보 신뢰성을 확보하였다.
 - (사업내용) 블록체인 기반으로 국민연금 해외수급자를 대상으로 수급권 및 생존 확인 서비스를 제공한다.
 - (주요성과) 국민연금공단의 업무 효율성 및 투명성 확보하고 공단측 업무 비용 절감하였다.
 - (주요 서비스) 블록체인 기반 비대면 국민연금 수급권 확인 서비스를 제공한다.
 - (공동인프라 키워드)



분산신원

- (34) 블록체인 기반 위험 구조물 안전진단 플랫폼 - 시티랩스 컨소시엄
- (목표) 위험구조물 안전진단 기록을 블록체인 기반으로 관리하여 전국의 위험 건축물 약 2,738,500동 대상의 서비스를 제공하고 시민 생활 안전 확보 및 미래생활도시 구현을 목표로 한다.
 - (사업내용) 사물 DID가 부여된 IoT 센서를 통해 블록체인 기반 위험 구조물 안전진단 서비스 및 지역 사용자 모니터링 앱/웹을 개발하였다.
 - (주요성과) 안전 모니터링 진단 시스템을 통해 건설 산업 재해 발생을 실시간 모니터링으로 미연에 방지를 통한 재산, 인명, 건물 붕괴 및 사

고 점유율, 사고 발생 이후 사후 비용 감소를 유도한다. 또한 IoT 센서의 모니터링을 통해 위험 건축물들을 관리하여 재난 발생 전과 후, 중앙 관리시스템 및 로컬시스템의 실시간 모니터링 기능을 제공하였다.

○ (주요 서비스) 사물 DID가 부여된 IoT 센서 및 블록체인 기반 위험 구조물 안전진단 모니터링 시스템을 구축하였다.

○ (공동인프라 키워드)


분산신원

2. 국내 블록체인 과제 현황 분석을 통한 K-BTF 공동인프라 요약

구분	사례	분산 신원	디지털 인증서	데이터 이력추 적	데이터 진본확 인	디지털 지갑	BaaS	데이터 주권	전자 영주권	전자 선거
(주) 아이쿠카	자녀의 올바른 금융 활동을 도와주는 DID기반 부모 인증 플랫폼	○								
한국 조폐 공사	NFT를 포함한 디지털 자산 신뢰검증 서비스		○		○					
매직 에끌	DID 기반 협업 인재 양성 플랫폼	○					○			
블록코엑스 와이지	NFT 졸업 전시회 서비스		○		○					
세종 텔레콤(주)	NFT 기반 게이미피케이션 학습 콘텐츠 유통 플랫폼		○		○					

구분	사례	분산 신원	디지털 인증서	데이터 이력추 적	데이터 진본확 인	디지털 지갑	BaaS	데이터 주권	전자 영주권	전자 선거
(주) 시큐 에버	기업간 신뢰 데이터 전송 및 이력 관리 서비스	○		○		○				
(주)아 이티 노매 즈	기부 펀드 연 계 블록체인 플랫폼		○							
동대 문 패션 타운 관광 특구 협회	NFT와 QR코드를 이용한 의류 정품인증 서비스			○	○					
(주) 지란 지교 시큐 리티	웹3.0 서비스 사용자를 위 한 소셜인증 구현 및 웹지 갑 서비스		○			○				
디엑 스웁 스 주 식회 사	블록체인기반 '커리어뱅크' (공모전 수상 경력관리) 플 랫폼	○			○		○			
(주) 리드 포인 트 시스 템	보육료 지원 사업 중복수 급관리		○	○						

구분	사례	분산 신원	디지털 증서	데이터 이력추 적	데이터 진본확 인	디지털 지갑	BaaS	데이터 주권	전자 영주권	전자 선거
마크 애니 콘소 시업	블록체인 기반의 드론 자격·증명 서비스 체계 구축	○			○					
블록 오디 세이	블록체인 기 반 바이오 원 재료 이력관 리 플랫폼 구 축			○						
비디 젠 컨 소시 업	블록체인 기 반 공공일자 리 지원 사업 전자근로계약 및 이력관리 플랫폼 구축	○	○	○	○	○				
비케 이위 너(주)	편리하고 투 명한 아파트 관리 서비스	○		○						
에스 지에 이 솔루 션즈 콘소 시업	DID기반 신원인증 및 비대면 민원서비스 플랫폼 구축	○			○	○				
오피 스엠 콘소 시업	모바일 선원 자격증명 서 비스 구축	○		○	○					
이튜 콘소 시업	블록체인 기 반 배움이력 통합관리 플 랫폼 구축	○	○	○	○	○				

구분	사례	분산 신원	디지털 증서	데이터 추적	데이터 진본 확인	디지털 지갑	BaaS	데이터 주권	전자 영주권	전자 선거
(주)인 재아 이엔 씨 컨 소시 업	블록체인 온 라인투표시스 템 기반 강화	○	○	○	○		○			○
(주)평 커	블록체인기반 특허NFT 거 래 플랫폼 구 축		○		○					
오피 스엠 컨소 시업	블록체인 기 반 한약 전주 기 관리 플랫 폼 구축		○	○	○					
(주) 모평 아이	건축,공연예 술 NFT 제작 및 전시 플랫 폼 구축		○		○		○			
솔리 데오 시스 템즈 컨소 시업	블록체인 적 용 공공 마이 데이터 유통 체계 신뢰기 반 구축		○	○	○					
SK 텔레 콤 컨 소시 업	블록체인 적 용 공공 마이 데이터 유통 체계 신뢰기 반 구축	○	○	○	○	○				

구분	사례	분산 신원	디지 털인 증서	데이 터이 력추 적	데이 터진 본확 인	디지 털 지갑	BaaS	데이 터주 권	전자 영주 권	전자 선거
NDS 컨소 시업	DID와 블록체 인을 활용하 여 개인의료 정보 기반의 안심활동 정 보 제공	O		O						
퓨처 센스 컨소 시업	차세대 식당 국산김치 자 율표시 시스 템 구축 사업	O		O		O				
한국 전자 투표 컨소 시업	DID 주주증명 기반 비대면 전자주총	O	O		O					O
주식 회사 한진 컨소 시업	바이오의약품 전용 스마트 콜드체인 플 랫폼 구축 및 적용 사업		O	O						
코인 플러 그	분산신원 (DID) 기반 수요자 맞춤 모바일 교통 카드 발급 및 무인 편의점 출입 서비스	O								
바른 손 / 프렌 즈 게임 즈	블록체인 기 반 차세대 미 디어 콘텐츠 플랫폼		O	O						

구분	사례	분산 신원	디지털 증서	데이터 추적	데이터 진본 확인	디지털 지갑	BaaS	데이터 주권	전자 영주권	전자 선거
오픈 스텝 컨소 시움	블록체인 기 반 의료용 마 약류 관리 플 랫폼 구축		○	○						
코인 플러그 컨소시 엄	주문배송 O2O 생태계 전반 DID집중 구축 사업	○								
코인 플러그 컨소시 엄	블록체인 기 반의 비대면 본인확인 및 결제 플랫폼	○								
시 티 랩 스 컨 소 시 엄	블록체인 기 반 위험 구조 물 안전진단 플랫폼	○								
합계		19	18	17	17	7	4	0	0	2

표 8. 국내 블록체인 과제 현황 분석을 통한 K-BTF 공동인프라 도출

부록 3. K-BTF 공동인프라 참여자별 시나리오

1. K-BTF 공동인프라 참여자별 시나리오

(1) 분산신원을 이용한 참여자별 시나리오

(가) 참여자별 시나리오 개요

- 분산신원 공동인프라는 이용자가 신분증명발급기관에 본인확인(최초 1회)을 거쳐 모바일 신분증(증명서 형태)을 발급받으면, 이후 신분증명발급기관을 거치지 않고 신분증 사용 과정에서 필요한 '진위확인'을 할 수 있는 서비스를 제공한다.
- 신분증명발급기관은 신분증을 발급하면서 서명에 사용한 공개키를 '분산신원도큐먼트'에 담아 블록체인에 등록하기만 하면 역할은 끝난다. 이용자는 서비스업체에 신분증(발급기관 서명이 포함된 상태)을 제출할 때 자신의 서명을 담아 보내는데 이때도 역시 공개키가 포함된 분산신원 도큐먼트를 블록체인에 등록하게 된다. 결과적으로 서비스 업체는 발급기관 서명과 이용자 서명이 모두 들어간 신분증 정보를 받게 되고, 블록체인에 등록된 분산신원 도큐먼트를 통해 서명의 진위를 쉽게 확인할 수 있게 된다.

(나) 블록체인 기업(공급), 국민(이용자), 공공기관(수요) 관점의 분산신원(DID) 공동인프라 서비스 시나리오 구성

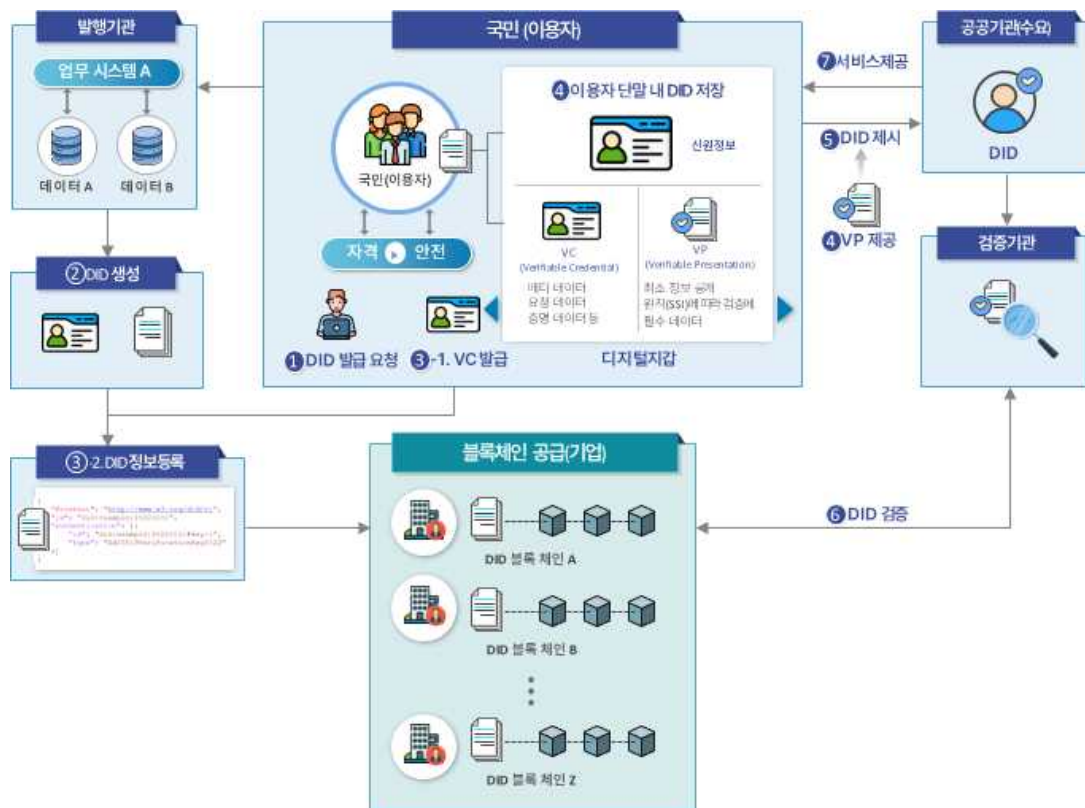


그림 17. 분산신원(DID) 공동인프라 서비스 시나리오

- 분산신원(DID)를 활용한 공공서비스 제공은 블록체인 공급기업, 서비스를 제공하는 공공기관, 그리고 모바일앱 기반의 이용자 환경에서 진행된다.
- (분산신원(DID) 발행 절차) 분산신원(DID) 발행 절차는 이용자(국민)의 DID 발행 요청에 따라 발행기관이 신원을 조회하고 DID를 생성하여 이용자(국민)의 디지털 지갑 모바일앱으로 VC를 발급하고 또한 블록체인 공급기업의 블록체인 네트워크에 DID 정보를 등록하는 과정을 거친다.
- (분산신원(DID) 요청 절차) 분산신원 요청 절차는 이용자(국민)의 디지털 지갑 모바일앱에서 DID를 제시하면 이와 관련된 VP가 제공되고, 이를 공공기관(수요)에 전달하면 검증기관의 DID 검증 확인에 따라 신원인증을 진행할 수 있다.
- 분산신원(DID)를 이용한 비대면 서비스는 개인 프라이버시를 보장받을 수 있는 개인정보보호의 장점뿐만 아니라, 기존의 번거로운 관리

절차나 수작업 대신 자동화된 서비스를 제공하여 관리 비용 절감과 공공 서비스 확산을 통한 경제 활성화가 가능할 것으로 예상된다.

- 분산신원(DID)는 향후 모바일 신분증, 모바일운전면허증, 시험검사, 채용, 증명서 등 투명성과 신뢰성이 필요한 공공서비스 분야에 적용하여 다양한 공공서비스 제공이 가능할 것으로 예상된다.

1) 블록체인 기업(공급)

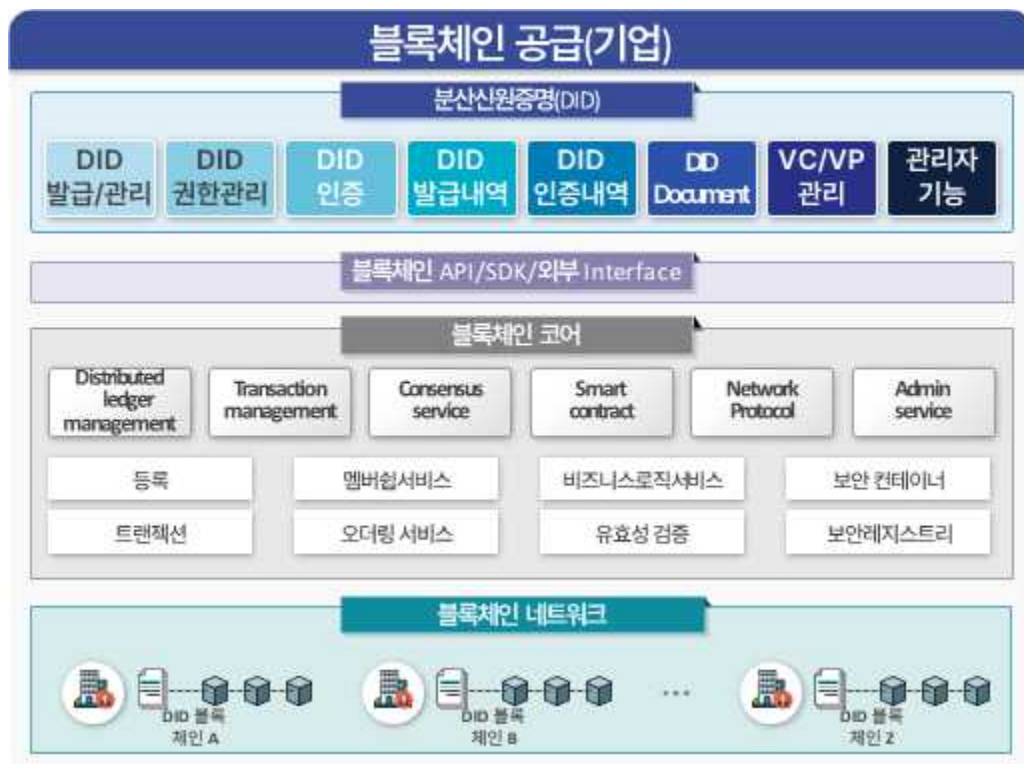


그림 18. 분산신원(DID) 블록체인 환경 예시

- 분산신원(DID)를 제공하는 블록체인 기업(공급)은 블록체인 네트워크를 구축하고 기존의 블록체인 네트워크와의 연계를 통해 플랫폼 구성이 가능하다. 블록체인 코어에서는 분산원장, 트랜잭션 관리, 합의 알고리즘, 스마트계약, 블록체인 네트워크를 구성하고 있으며, 블록체인 API, SDK, 외부 인터페이스를 제공하여 외부 연계 환경을 제공한다. 분산신원(DID)는 DID발급관리모듈, DID권한관리모듈, DID인증모듈, DID발급내역관리모듈, DID인증내역모듈, DIDdocument모듈, VC/VP관리모듈 그리고 관리자 기능 모듈로 구성되어 있다.

2) 국민(이용자)

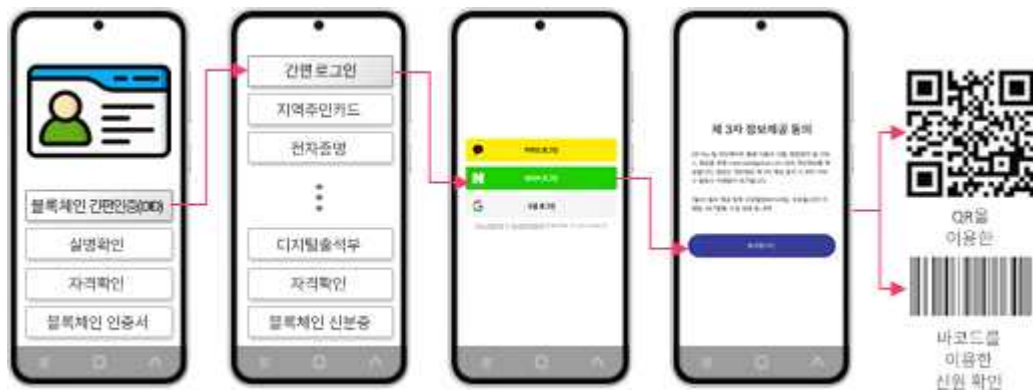


그림 19. 분산신원(DID)를 이용한 신원확인 서비스 예시

- 분산신원(DID) 공동인프라를 이용하고자 하는 국민(이용자)는 디지털 지갑을 설치하고 DID를 발급받는다. 발급된 DID는 디지털 지갑에 보관되며, 블록체인 서비스를 사용해야 할 경우 생체인증(지문, 안면 인식 등)을 활용하여 QR, 바코드, 전자신분증 등의 형태로 신원증명을 진행할 수 있다.
- 디지털 지갑은 스마트 주민증/학생증, QR코드, 바코드 등 서비스 형태에 따라 다양한 형식의 간편 인증을 진행할 수 있도록 기능을 지원한다.
- 예를 들어 모바일 주민카드를 발급받은 국민(이용자)들은 공공도서관 이용 시 비대면으로 간편하게 도서관 이용이 가능하다. 또한, 공공시설물 이용시 실물 신분증 없이 스마트주민증을 통해 신원확인 과 서비스를 편리하게 이용할 수 있다.

3) 공공기관(수요)



그림 20. 분산신원(DID)를 활용한 공공서비스 예시

- 분산신원(DID) 서비스를 제공하는 공공기관(수요)은 분산신원(DID)를 보유한 이용자(국민)를 대상으로 다양한 블록체인 공공 서비스를 제공할 수 있다.
- 공공기관의 홈페이지 로그인 시 DID 정보를 통해 발급된 QR코드를 활용하여 간편하게 로그인할 수 있는 서비스가 가능하다.
- 공공기관 출입시 분산신원(DID)를 통해 발급된 QR코드를 사용하여 신원확인 및 비대면 출입관리 서비스가 가능하다.
- 공공 도서 대여 서비스의 경우 분산신원(DID)를 통해 발급된 QR코드 또는 바코드를 활용하여 회원확인 및 도서 대여 기록을 관리할 수 있다.
- 온라인 민원 신청 서비스도 분산신원(DID)를 활용하여 가능하다. 홈페이지를 통해 온라인민원신청을 접수하면 행안부 전자증명발급시스템과 연계하여 각종 증명서 등 민원서류 발급 서비스를 이용할

수 있다.

- 분산신원(DID)으로 발급된 스마트 주민증/학생증을 보유한 국민(이용자)는 주민등록증, 운전면허증 등 실물 신분증 없이 영지식증명 기술로 개인 프라이버시를 보장받으며 자동화된 인증서비스를 이용할 수 있다.
- 공공 블록체인 서비스 연계를 통해 다양한 지역 공공시설 확인, 시험검사, 보조금 및 수당 지급, 공공기관 채용 등 다양한 형태의 비대면 온라인 원스톱 서비스 제공이 가능하다.

(다) 국내/외 유사 사례

- 한국, 2022, 모바일 운전면허증의 발급 및 운영
- 한국, 2021, 병무행정 서비스 (e-병무지갑)

(2) 디지털인증서를 이용한 참여자별 시나리오

(가) 참여자 시나리오 개요

- 디지털인증서 공동인프라는 NFT 기술을 기반으로 디지털인증서를 생성하고 활용할 수 있는 서비스들이 제공된다. 디지털인증서는 특정한 자산을 나타내는 블록체인에 저장된 데이터 단위로, 고유하면서 상호 교환할 수 없는 토큰 서비스이다.
- 디지털인증서를 이용한 참여자별 시나리오로는 온라인 교육 콘텐츠 플랫폼을 통하여 유통되는 과정에서 디지털 콘텐츠에 디지털인증서를 적용하여 온라인 상에서 해당 콘텐츠에 대한 원저작권, 콘텐츠 불법 복제 및 거래 차단 등의 서비스의 형태로 구현이 가능하다.

(나) 블록체인 기업(공급), 국민(이용자), 공공기관(수요) 관점의 디지털인증서(NFT) 공동인프라 서비스 시나리오 구성

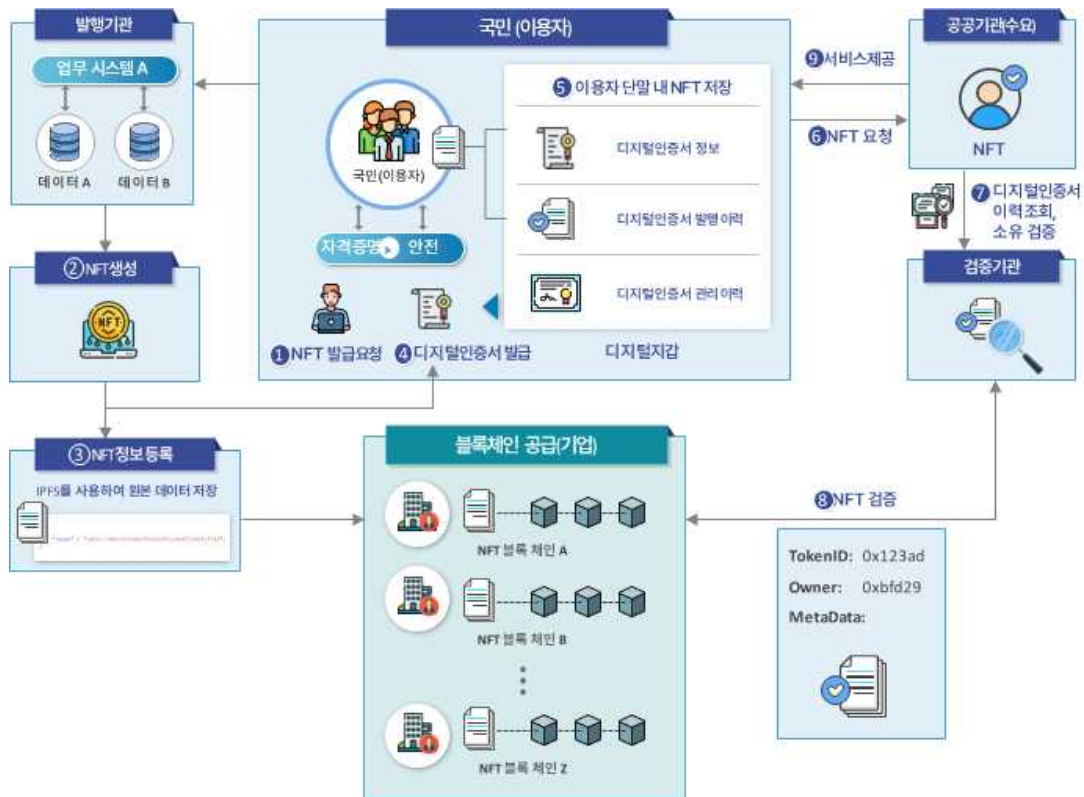


그림 21. 디지털인증서(NFT) 공동인프라 서비스 시나리오

- 디지털인증서(NFT)를 활용한 공공서비스 제공은 블록체인 공급기업, 서비스를 제공하는 공공기관, 그리고 모바일앱 기반의 이용자 환경에서 진행된다.
- (디지털인증서(NFT) 발행 절차) 디지털인증서(NFT) 발행은 이용자(국민)의 NFT 발행 요청에 따라 발행기관이 인증서 정보를 조회하고 NFT를 생성하여 이용자(국민)의 디지털 지갑으로 인증서를 전달하고 또한 블록체인 공급기업의 블록체인 네트워크에 NFT 정보를 등록하는 과정을 진행된다.
- (디지털인증서(NFT) 활용 절차) 디지털인증서(NFT) 확인 절차는 이용자(국민)의 디지털 지갑에서 제시된 NFT를 검증기관으로 디지털인증서 이력조회, 소유 검증이 요청되고, 그 결과를 공공기관(수요)에 전달하면 디지털인증서의 소유 여부를 확인할 수 있다.
- 디지털인증서(NFT)를 이용한 서비스는 기존의 증명서 관리 절차를 대신하여 비용 절감과 공공서비스 확산을 통한 대국민서비스 활성화가 가능할 것으로 예상된다.
- 디지털인증서(NFT)는 향후 투명성과 신뢰성이 필요한 공공서비스 분

야에 적용하여 다양한 디지털인증서에 적용 가능할 것으로 예상된다.

1) 블록체인 기업(공급)

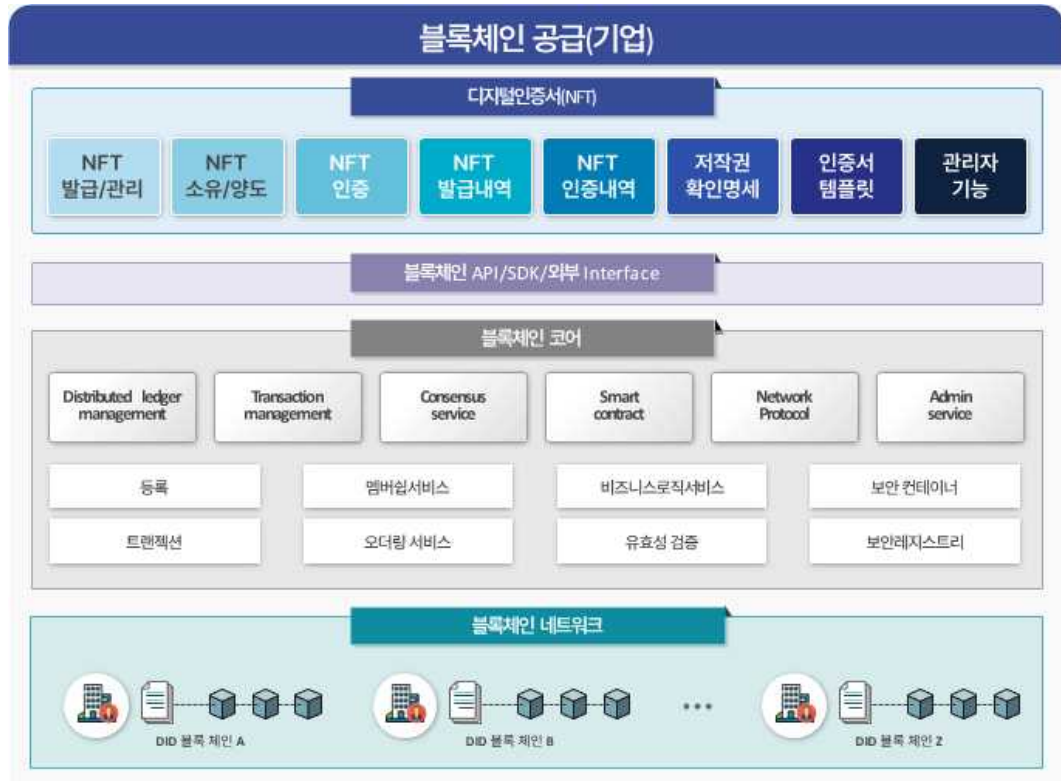


그림 22. 디지털인증서(NFT) 블록체인 환경 예시

- 디지털인증서(NFT)를 제공하는 블록체인 기업(공급)은 블록체인 네트워크를 구축하고 기존의 블록체인 네트워크와의 연계를 통해 플랫폼 구성이 가능하다. 블록체인 코어에서는 분산원장, 트랜잭션 관리, 합의알고리즘, 스마트계약, 블록체인 네트워크를 구성하고 있으며, 블록체인 API, SDK, 외부 인터페이스를 제공하여 외부 연계 환경을 제공한다. 디지털인증서(NFT)는 NFT발급관리모듈, NFT소유양도모듈, NFT인증모듈, NFT발급내역모듈, NFT인증모듈, 저작권확인모듈, 인증서템플릿모듈 그리고 관리자 기능 모듈로 구성되어 있다.

2) 국민(이용자)



그림 23. 디지털인증서(NFT)를 이용한 증명서 확인 서비스 예시

- 디지털인증서(NFT) 서비스를 이용하고자 하는 국민(이용자)는 디지털 지갑을 설치하고 개개인이 소유한 인증서를 신원인증을 통해 확인 후 디지털인증서(NFT)를 발급받는다. 발급된 NFT는 디지털 지갑에 보관되며, 디지털인증서 서비스에 사용해야 할 경우 생체인증(지문, 안면인식 등)으로 인증 후 QR, 바코드와 결합된 전자문서의 형태로 소유를 증명할 수 있다.
- 디지털 지갑은 졸업증명서, 위촉장, 디지털 신분증/학생증 등을 보관할 수 있으며, 서비스 형태에 따라 다양한 형식으로 디지털인증서를 제공할 수 있다.
- 예를 들어 운전면허자격증을 소유한 국민(이용자)들은 공공기관에서 원본없이 간편하게 신분증명 후 서비스 이용이 가능하다.

3) 공공기관(수요)



그림 24. 디지털인증서(NFT)를 활용한 공공서비스 예시

- 디지털인증서(NFT) 서비스를 제공하는 공공기관(수요)은 디지털인증서(NFT)를 보유한 이용자(국민)이 다양한 블록체인 공공서비스를 제공할 수 있도록 지원한다.
- 특정기관에서 요구하는 전자증명서를 NFT로 발급받아 디지털 지갑에 보관하며, 필요한 경우 이를 간편하게 증명할 수 있다.
- 국민(이용자) 개인이 취득한 자격증을 NFT로 발급받아 자격을 증명하거나, 실물 자격증을 대체하여 활용할 수 있다.
- 공공서비스를 통해 결제한 내역을 NFT형태의 전자영수증으로 발급받아 디지털 지갑에 보관할 수 있으며, 연말정산, 종합소득세 납부 등에 활용할 수 있다.
- 스마트 주민증/학생증을 디지털인증서(NFT)로 발급하여 전자신분증으로 활용할 수 있다. NFT로 발급된 스마트 주민증/학생증은 실물 신분증 없이 자동화된 신분확인이 가능하다.

(다) 국내/외 유사 사례

- 한국, 2022, NFT를 포함한 디지털 자산 신뢰검증 서비스
- 한국, 2022 NFT 졸업 전시회 서비스

- 한국, 2022 NFT 기반 게이미피케이션 학습 콘텐츠 유통 플랫폼
- (3) 데이터이력추적을 이용한 참여자별 시나리오

(가) 참여자별 시나리오 개요

- 데이터이력추적 공동인프라는 블록체인을 이용한 농식품 이력 관리 서비스는 신선 포장 농식품의 이력 데이터를 수집하고, 포장식품의 이력을 스마트폰을 이용하여 소비자 및 관리자가 실시간으로 현장에서 확인할 수 있는 블록체인 서비스이다.
 - 생산자는 스마트폰의 App으로 유통 중에 생성된 이력 정보를 수집한 후, 이력 정보의 암호화, 유효성 검증, 합의 등의 과정을 거쳐서 분산 원장(트랜잭션, 블록)을 생성하고 블록체인에 저장한다. 전국의 영농조합에 속한 농가는 딸기를 생육 단계별로 3가지 제품을 생산한다. 각 지역의 영농조합은 오픈 마켓(Open Market)에 판매가능 제품을 등록하고 고객은 오픈 마켓에서 제품을 선택하여 주문한다.
 - 오픈 마켓은 고객의 배송 주소를 확인하고 가장 가까운 영농조합에 주문을 알린다. 영농조합은 농가의 배송가능한 제품을 고객에게 배송한다. 오픈 마켓은 제품 생산정보 및 고객의 주문, 배송과정의 온도, 습도, GPS 정보를 블록체인에 저장한다. 고객은 제품을 받고 제품의 QR코드를 통해 제품의 이력정보를 조회할 수 있다.
- (나) 블록체인 기업(공급), 국민(이용자), 공공기관(수요) 관점의 디지털이력 추적 공동인프라 시나리오 구성

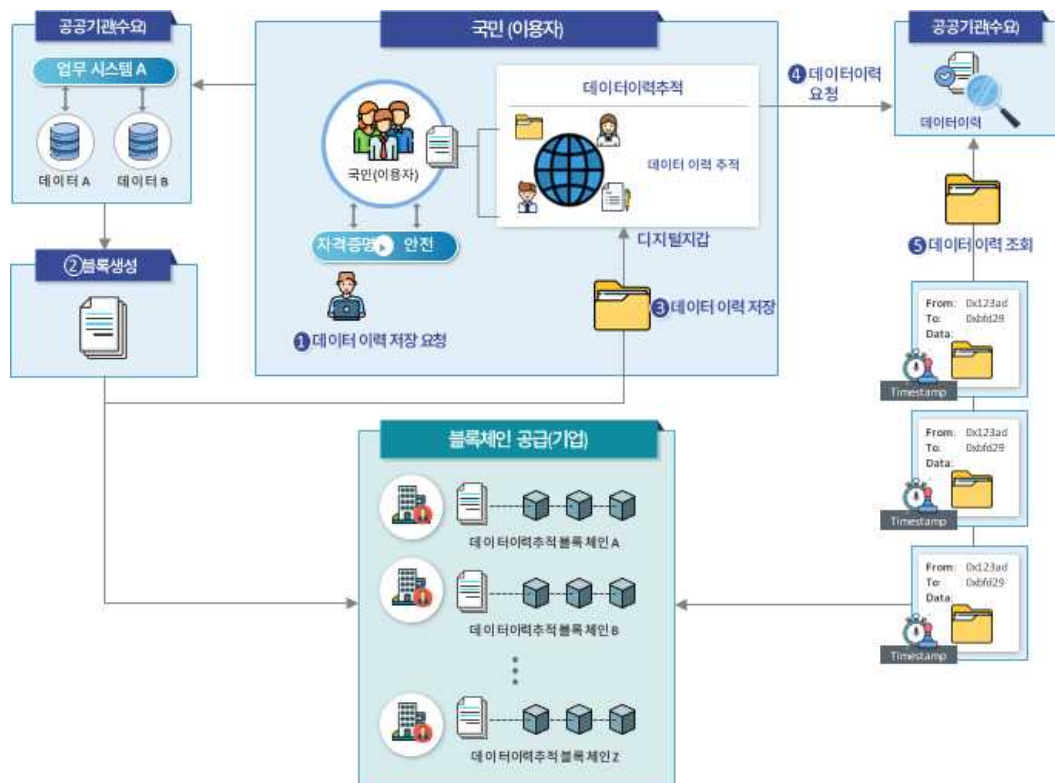


그림 25. 데이터이력추적 공동인프라 서비스 시나리오

- 디지털이력추적 공동인프라 기반의 공공서비스는 블록체인 공급기업, 서비스를 제공하는 공공기관, 그리고 모바일앱 기반의 이용자 환경에서 진행된다.
- (디지털이력추적 저장 절차) 디지털이력추적을 위한 데이터 저장은 이용자(국민)의 데이터 이력 저장 요청에 따라 공공기관(수요)이 저장할 데이터를 정제하여 블록체인 네트워크에 분산 저장한다.
- (디지털이력추적 조회 절차) 디지털이력추적 조회 절차는 이용자(국민)의 디지털 지갑에 표시된 데이터 저장 이력 정보를 공공기관(수요)으로 전달하면 이를 블록체인 네트워크에서 이력 조회를 통해 검증하고 데이터 이력을 조회할 수 있다.
- 디지털이력추적을 이용한 서비스는 앞서 설명한 농수산물 유통 이력 서비스가 대표적이며, 지속적 확산을 통한 대국민서비스 활성화가 가능할 것으로 예상된다.

1) 블록체인 기업(공급)

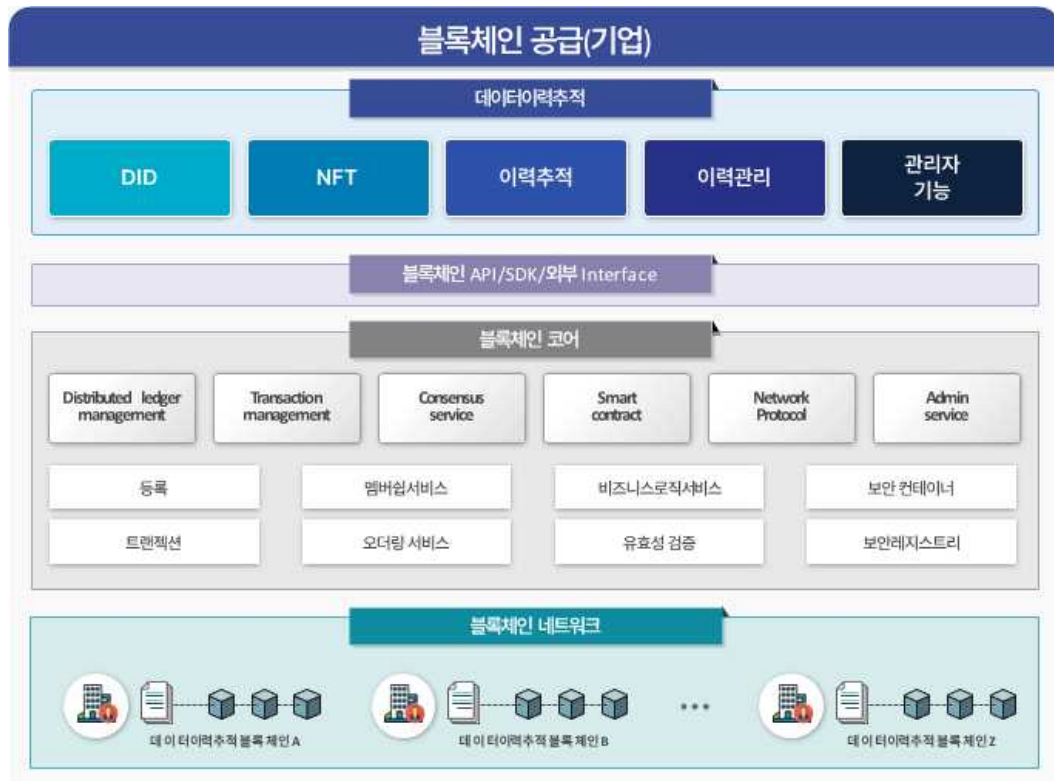


그림 26. 데이터이력추적 블록체인 환경 예시

- 데이터이력추적을 제공하는 블록체인 기업(공급)은 블록체인 네트워크를 구축하고 기존의 블록체인 네트워크와의 연계를 통해 플랫폼 구성이 가능하다. 블록체인 코어에서는 분산원장, 트랜잭션 관리, 합의알고리즘, 스마트계약, 블록체인 네트워크를 구성하고 있으며, 블록체인 API, SDK, 외부 인터페이스를 제공하여 외부 연계 환경을 제공한다. 데이터이력추적은 DID모듈, NFT모듈, 이력추적모듈, 이력관리모듈 그리고 관리자 기능모듈로 구성된다.

2) 국민(이용자)



그림 27. 데이터이력추적을 이용한 유통 이력 확인 서비스 예시

- 데이터이력추적 서비스를 이용하고자 하는 국민(이용자)는 두가지 형태로 이 서비스를 이용할 수 있다. 첫 번째는 데이터이력 정보의 등록 서비스이다. 디지털 지갑을 설치하고 데이터이력을 저장할 대상을 입력화면을 통해 진행하면 디지털 지갑의 인증서를 통해 신원 인증 후 해당 정보가 블록체인으로 저장되어 데이터이력을 기록한다. 두 번째는 저장된 데이터이력 정보의 조회 및 확인 서비스이다. 데이터이력을 관리하는 물품의 QR코드나 유통 관리번호(이력번호)를 디지털 지갑에 입력하면 해당 물품의 데이터이력정보를 조회할 수 있다.
- 데이터이력추적의 증빙은 변경 이력 내역 및 확인서 등으로 보관할 수 있다.

3) 공공기관(수요)



그림 28. 데이터이력추적을 활용한 공공서비스 예시

- 데이터이력추적 서비스를 제공하는 공공기관(수요)은 디지털 지갑을 설치하고 인증서를 보유한 이용자(국민)이 다양한 블록체인 공공서비스를 제공할 수 있도록 지원한다.
- 농수산물 유통 이력 등록, 농수산물 유통 이력조회, 수입물품 통관 이력, 우편물 배송 이력, 택배 배송 이력, 의약품 유통 이력 등의 등록과 조회가 가능하도록 공공기관에서 요구하는 유통 이력 등록 절차와 확인 절차를 QR코드 또는 이력번호를 사용하여 간편하게 처리할 수 있다.

(다) 국내/외 유사 사례

- 한국, 2022, 기업 간 신뢰 데이터 전송 및 이력 관리 서비스
- 한국, 2022, 보육료 지원 사업 중복수급관리

(4) 데이터진본확인을 이용한 참여자별 시나리오

(가) 참여자별 시나리오 개요

- 데이터진본확인 공동인프라를 기반으로 하는 데이터진본확인서비스는 이용자가 발행 기관으로부터 받은 데이터가 위·변조되지 않은 유효

한 데이터라는 사실을 서비스 제공자에게 입증하는 서비스이다.

- 데이터진본확인 공동인프라를 활용할 경우 공공기관(수요)가 전자문서를 생성하면서 해당 문서에 대한 고유 정보를 블록체인 서비스에 등록하고, 향후 이 문서의 진본 여부에 대한 검증을 확인할 수 있게 된다.

(나) 블록체인 기업(공급), 국민(이용자), 공공기관(수요) 관점의 데이터진본확인 서비스 구성

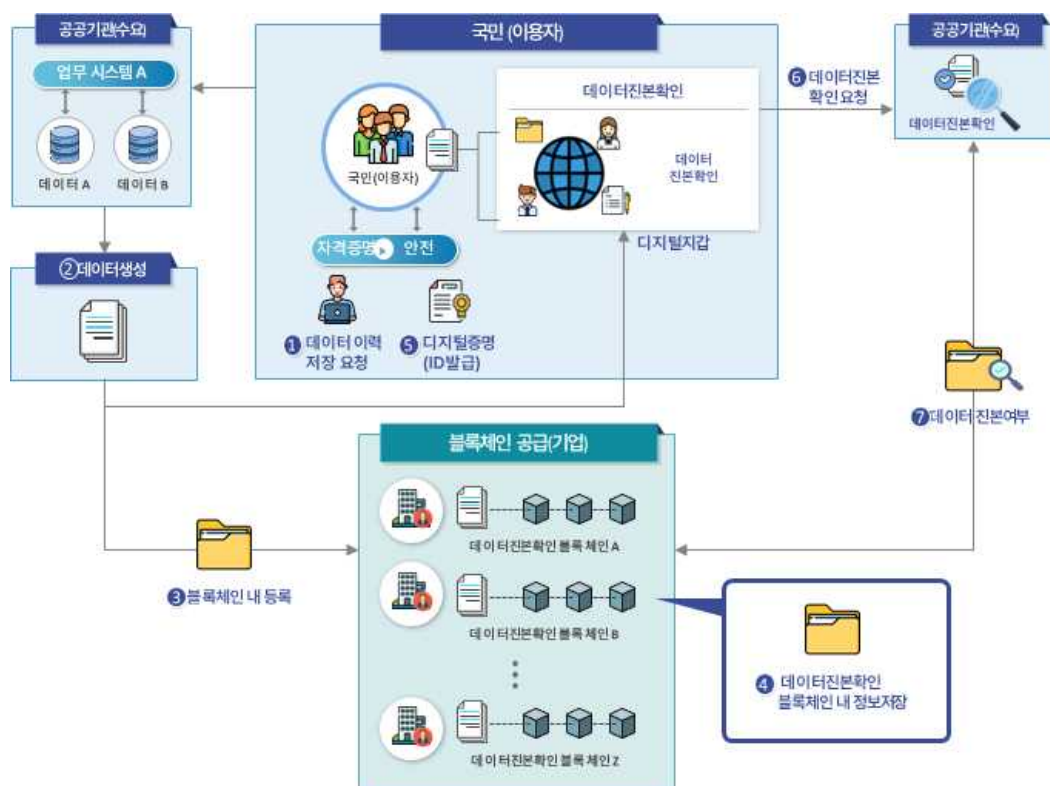


그림 29. 데이터진본확인 공동인프라 서비스 시나리오

- 데이터진본확인을 활용한 서비스는 블록체인 공급기업, 서비스를 제공하는 공공기관, 그리고 모바일앱 기반의 이용자 환경에서 진행된다.
- (데이터진본확인 등록 절차) 데이터진본확인 데이터 등록 절차는 이용자(국민)의 데이터 저장 요청에 따라 공공기관(수요)이 진본확인이 필요한 증명서를 조회하고 블록체인에 저장할 데이터를 추가하여 블록체인 네트워크로 저장하며, 디지털증명서를 발급하여 이용자(국민)의 디지털 지갑에 저장하는 과정을 진행된다.

- (데이터진본확인 조회 절차) 데이터진본확인 조회 절차는 이용자(국민)의 디지털 지갑에서 제시된 증명서를 공공기관(수요)으로 전달하여 증명서에 부가된 워터마크, 복사방지코드, 2D바코드 등의 정보가 변경되었는지를 확인하는 절차로 진행된다. 데이터진본확인에 필요한 복사방지코드, 2D바코드 정보가 조회되고, 그 결과를 공공기관(수요)에 전달하면 데이터진본확인의 위변조 여부를 확인할 수 있다.
- 데이터진본확인을 이용한 서비스는 기존의 증명서 관리 절차를 투명하고 신뢰성있게 적용할 수 있으며 다양한 공공서비스에 적용하여 활성화가 가능할 것으로 예상된다.

가) 블록체인 기업(공급)

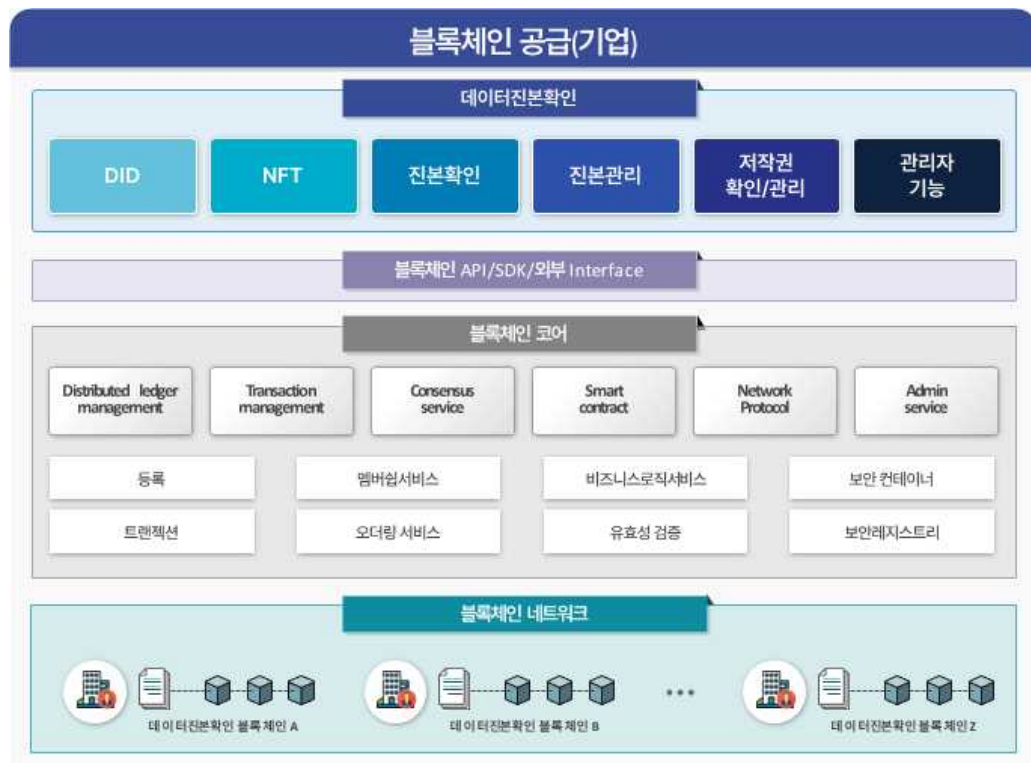


그림 30. 데이터진본확인 블록체인 환경 예시

- 데이터진본확인 블록체인 플랫폼을 제공하는 블록체인 기업(공급)은 블록체인 네트워크를 구축하고 기존의 블록체인 네트워크와의 연계를 통해 구성이 가능하다. 블록체인 코어에서는 분산원장, 트랜잭션 관리, 합의알고리즘, 스마트계약, 블록체인 네트워크 기능을 제공하고 있으며, 블록체인 API, SDK, 외부 인터페이스를 제공하여 외부

연계 환경을 제공한다. 데이터진본확인 핵심 모듈은 DID모듈, NFT 모듈, 진본확인모듈, 진본관리모듈, 저작권확인관리모듈 그리고 관리자 모듈을 제공한다.

나) 국민(이용자)

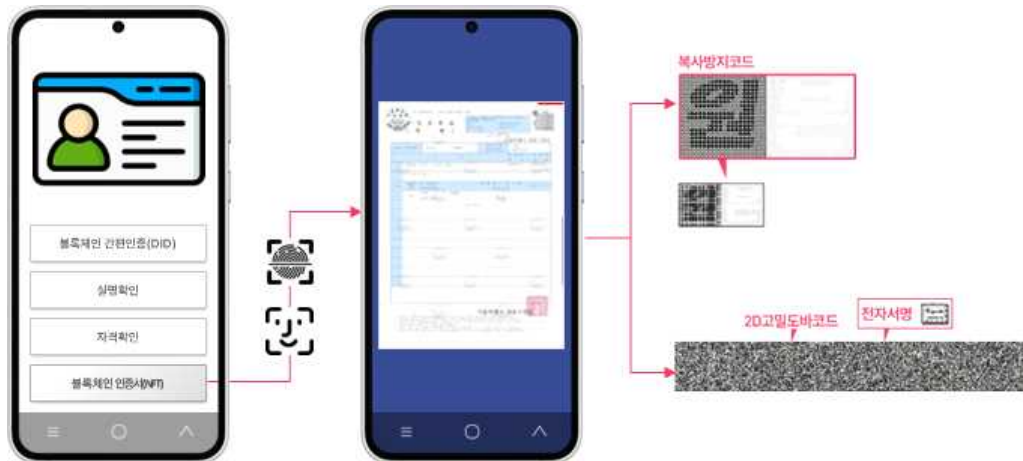


그림 31. 데이터진본확인을 이용한 증명서 위변조 확인 서비스 예시

- 데이터진본확인 서비스를 이용하고자 하는 국민(이용자)는 디지털 지갑을 설치하고 개개인이 소유한 인증서를 사용하여 신원인증하는 과정을 거친다. 국민(이용자)가 보유한 증명서, 자격증, 주민증 등을 데이터진본 관리를 위해 등록하며, 이때 이미지 데이터 외 복사방지 코드, 2D바코드 등이 함께 결합되어 블록체인 네트워크로 저장된다.
- 저장이 완료된 증명서, 자격증, 주민증 등은 디지털 지갑에 저장되며 필요한 경우 공공기관(수요)이 요구하는 데이터진본확인 서비스에 위변조 확인을 통해 사용 가능하다.
- 예를 들어 주민등록등본을 발급받은 경우 이를 디지털 지갑에 보관하고 있다가 온라인 상에서 민원서류 접수시 위변조 확인 과정을 거쳐 제출 후 추가적인 공공서비스 이용이 가능하다.

다) 공공기관(수요)



그림 32. 데이터진본확인을 활용한 공공서비스 예시

- 데이터진본확인 서비스를 제공하는 공공기관(수요)은 데이터진본확인을 통해 발급한 디지털증명서를 보유한 이용자(국민)가 비대면 환경에서 증명서를 온라인 상으로 확인할 수 있도록 지원한다.
- 공공기관(수요)에서 발행한 전자민원서류, 디지털자격증, 주민증/학생증 등을 데이터진본확인을 통해 위변조 여부 검증 단계를 거쳐 각종 민원 서비스에 제출서류 또는 증빙을 목적으로 활용할 수 있다.
- 공공 블록체인 서비스를 연계하여 공공기관(수요) 간의 증명서 등록, 확인 절차를 비대면 환경에서 진행하여 이용자(국민)이 편리하게 민원 업무를 수행할 수 있도록 활용 가능하다.

3) 국내/외 유사 사례

- 한국, 2021, 블록체인 기반 배움이력 통합관리 플랫폼 구축
- 한국, 2022, 블록체인기반 특허NFT 거래 플랫폼 구축
- 한국, 2022, 블록체인 기반 한약 전주기 관리 플랫폼 구축

(5) 직접구축(BaaS)를 이용한 참여자별 시나리오

(가) 참여자별 시나리오 개요

- 직접구축(BaaS)를 통해 공공기관이 블록체인 서비스를 개발할 경우 K-BTF의 모든 블록체인 메인넷, 블록체인 공동인프라, 블록체인 플랫폼을 사용하여 빠르고 편리하게 블록체인 서비스를 개발할 수 있는 환경을 제공한다. 공공기관이 원하는 대국민 서비스를 블록체인 기반에서 개발하고 서비스하여 블록체인에 대한 전문성 없이도 블록체인 인프라, 블록체인 코어 엔진, 블록체인 API 및 SDK를 활용하여 서비스를 개발할 수 있다.
- 직접구축(BaaS)의 형태는 중국 BSN-Enterprise, 싱가포르 OpenAttestation 프레임워크와 같이 공공의 주도로 만들어지는 블록체인 플랫폼을 활용하여 대국민 서비스를 블록체인 기반으로 구성할 수 있다.
- 또 다른 하나의 형태는 퍼블릭 클라우드 환경에서 블록체인 플랫폼 서비스를 구성하여 SaaS 형태의 블록체인 서비스와 대국민 공공 어플리케이션을 개발하도록 지원한다.

(나) 블록체인 기업(공급) 관점의 서비스 구성

- 직접구축(BaaS)를 활용한 공공서비스 제공은 블록체인 공급기업 기반의 환경에서 진행된다.

1) 블록체인 기업(공급)

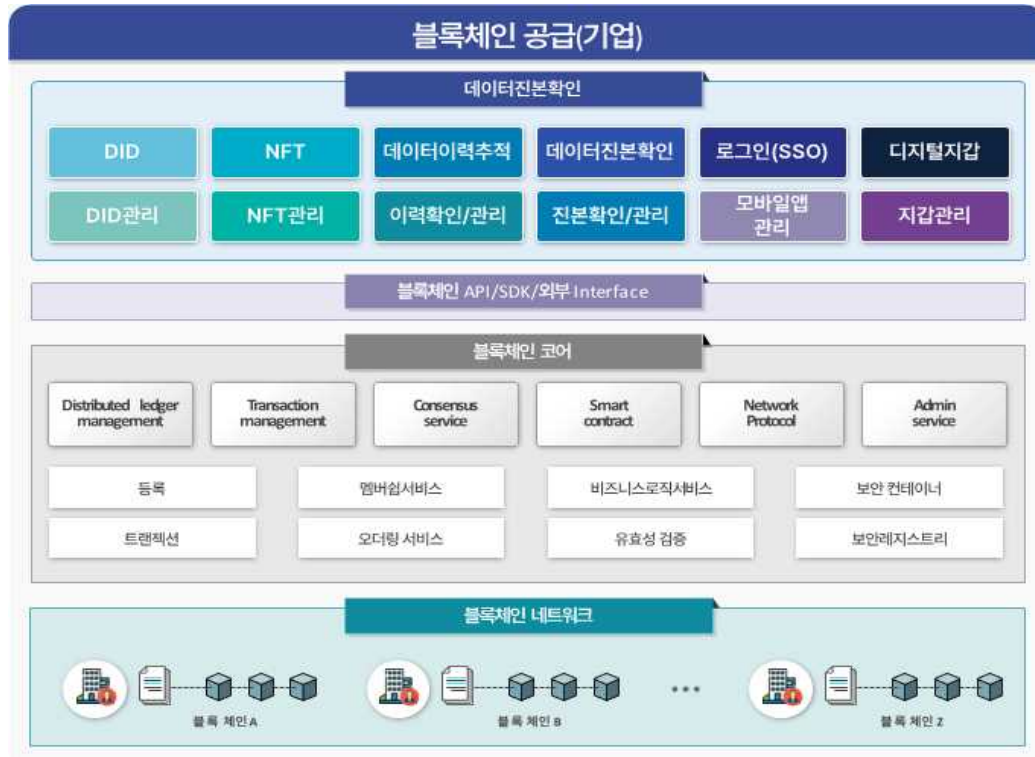


그림 33. 직접구축(BaaS) 예시

- 직접구축(BaaS)를 제공하는 블록체인 기업(공급)은 블록체인 네트워크를 구축하고 기존의 블록체인 네트워크와의 연계를 통해 플랫폼 구성이 가능하다. 블록체인 코어에서는 분산원장, 트랜잭션 관리, 합의알고리즘, 스마트계약, 블록체인 네트워크를 구성하고 있으며, 블록체인 API, SDK, 외부 인터페이스를 제공하여 외부 연계 환경을 제공한다. 블록체인 플랫폼은 DID모듈, DID관리모듈, NFT모듈, NFT 관리모듈, 데이터이력추적모듈, 데이터진본확인모듈, 데이터이력확인관리모듈, 데이터진본확인관리모듈, 로그인모듈, 모바일앱 관리 모듈, 관리자 모듈 그리고 디지털 지갑관리 모듈로 구성된다.

(나) 국내/외 유사 사례

- 중국, 2022, BSN-Enterprise
- 싱가포르, 2017, OpenAttestation 프레임워크
- 독일, 2022, GXFS(GAIA-X Federation Services)
- 유럽, 2021, EBSI

(6) 디지털 지갑 서비스를 이용한 참여자별 시나리오

(가) 참여자별 시나리오 개요

- 디지털 지갑 서비스는 분산된 지갑 기능(키 관리, 트랜잭션 전송 및 서명 등)을 암호화하여 보관하고 용이하게 사용할 수 있도록 하는 서비스이다.
- 디지털 지갑 서비스를 통해 무형의 가상자산을 보관하는 용도로 활용 가능하다. 비밀키와 가상자산을 보관하기 위해 자동으로 중앙지갑을 생성하고 생성된 중앙지갑의 키를 안전하게 클라우드 시스템에 분산 및 분리 보관하는 중앙전자지갑 관리서비스를 통해 사용자가 자신의 지갑을 조회하고 필요에 따라 추가 삭제가 가능하고 다수의 지갑을 통합 관리할 수 있는 서비스를 제공한다.

(나) 블록체인 기업(공급), 국민(이용자), 공공기관(수요) 관점의 디지털 지갑 서비스 구성



그림 34. 디지털 지갑 서비스 시나리오

- (디지털 지갑 발행 절차) 디지털 지갑 발행은 이용자(국민)의 디지털

지갑 발행 요청으로부터 발행기관의 이용자 신분 증명을 통해 인증서 정보를 조회하고 디지털 지갑을 생성한 후 이용자(국민)의 스마트폰으로 디지털 지갑 모바일앱을 설치할 수 있도록 안내한다. 또한 생성된 디지털 지갑 발급 정보는 블록체인 공급(기업)의 블록체인 네트워크에 분산 저장되어 관리된다.

- (디지털 지갑 활용 절차) 디지털 지갑 활용 시 이용자(국민)의 디지털 지갑 모바일앱에서 사용자 인증을 거쳐 지갑 내 DID, NFT, 데이터위변조, 데이터이력추적 등 다양한 블록체인 서비스를 이용할 수 있다.
- 디지털 지갑은 향후 편의성, 투명성, 신뢰성이 확대되어 다양한 공공서비스 분야에 적용될 것으로 예상된다.

1) 블록체인 기업(공급)

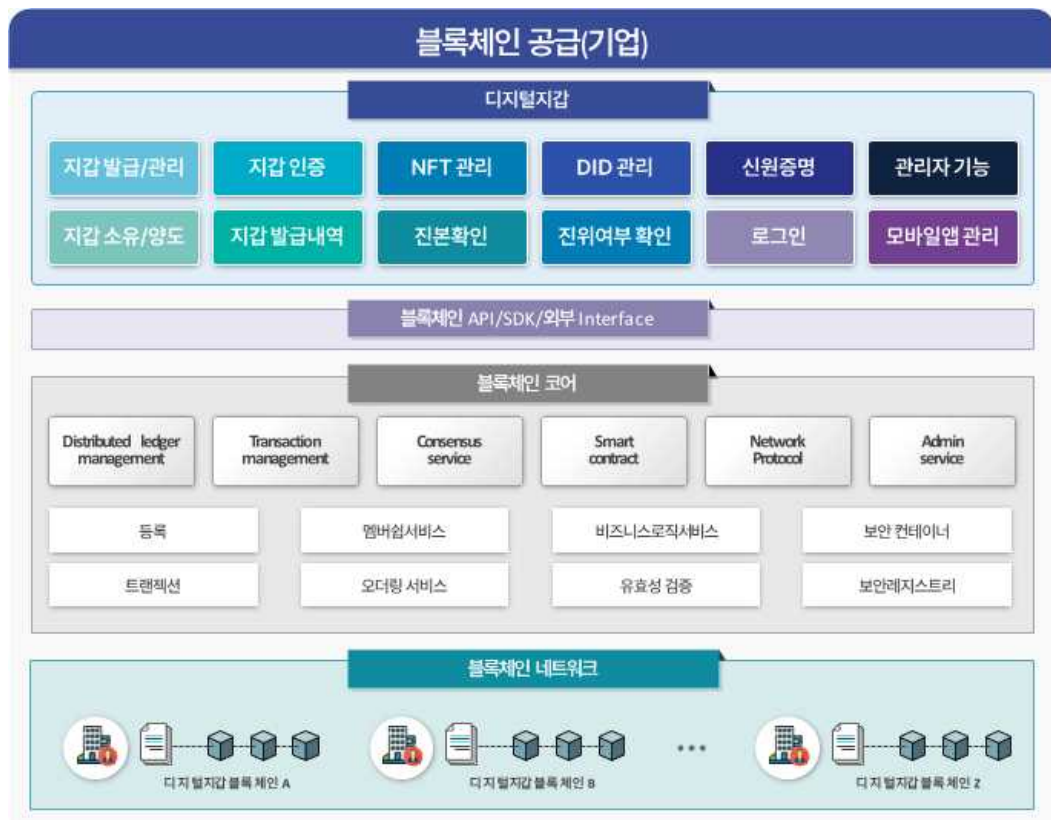


그림 35. 디지털 지갑 블록체인 환경 예시

- 디지털 지갑 블록체인 플랫폼을 제공하는 블록체인 기업(공급)은 블록체인 네트워크를 구축하고 기존의 블록체인 네트워크와의 연계를

통해 구성이 가능하다. 또한 블록체인 코어에서는 분산원장, 트랜잭션 관리, 합의알고리즘, 스마트계약, 블록체인 네트워크를 구성하고 있으며, API, SDK, 외부 인터페이스를 제공하여 외부 연계 환경을 제공한다. 디지털 지갑 블록체인 환경은 지갑 발급, 관리 및 인증 모듈, NFT 관리 모듈, DID 관리 모듈, 진본확인 모듈, 진위여부확인 모듈, 로그인 및 신원증명 모듈, 모바일앱 관리 모듈 그리고 관리자 기능을 제공한다.

2) 국민(이용자)



그림 36. 디지털 지갑 서비스 예시



그림 37. 디지털 지갑을 이용한 간편로그인 서비스 예시



그림 38. 디지털 지갑을 이용한 자격증명 서비스 예시



그림 39. 디지털 지갑을 이용한 신분증명 서비스 예시



그림 40. 디지털 지갑을 이용한 전세계약/전입신고 서비스 예시



그림 41. 디지털 지갑을 이용한 민원서류증명/조회 서비스 예시



그림 42. 디지털 지갑을 이용한 스마트티켓 서비스 예시



그림 43. 디지털 지갑을 이용한 세금납부증빙/영수증발행 서비스 예시



그림 44. 디지털 지갑을 이용한 도서대출 서비스 예시



그림 45. 디지털 지갑을 이용한 농축산물유통이력조회 서비스 예시



그림 46. 디지털 지갑을 이용한 수출입통관이력 조회 서비스 예시

- 디지털 지갑을 이용하고자 하는 국민(이용자)는 신청사이트에서 회원 가입 및 본인 인증 후 디지털 지갑을 설치하고 개개인이 소유한

인증서를 사용하여 디지털 지갑 모바일앱과 연동한다. 디지털 지갑에는 DID, NFT, 데이터이력추적, 데이터위변조 등 다양한 공공서비스의 주요 기능들이 메뉴별로 분류되어 구성되어 있다.

- 수십종의 전자증명서 보관, 서비스 자격여부, 비대면 온라인 인증, 모바일 신분증 등 다양한 공공서비스 기능을 한 곳에서 관리할 수 있다.
- 디지털 지갑내 저장된 분산신원(DID), 디지털인증서(NFT)를 활용하여 간편로그인 서비스, 자격증명 서비스, 신분증명 서비스 뿐만 아니라 전자전세계약 서비스, 민원서류 조회/증명 서비스, 스마트티켓 서비스, 세금납부내역 증빙/영수증 서비스, 도서대출 서비스, 농축산물유통이력조회 서비스, 수출입통관이력 조회 서비스 등 다양한 공공 서비스 분야에 활용할 수 있다.
- 디지털 지갑은 본인 인증 및 자격 증명 등 매우 중요한 개인 정보가 연동되어있어 개인정보 유출이 되지 않도록 유의해야 한다.
- 디지털 지갑은 블록체인 신뢰 프레임워크가 확산됨에 따라 다양한 공공서비스에 필요한 기능들이 계속 추가될 것이다.

3) 공공기관(수요)

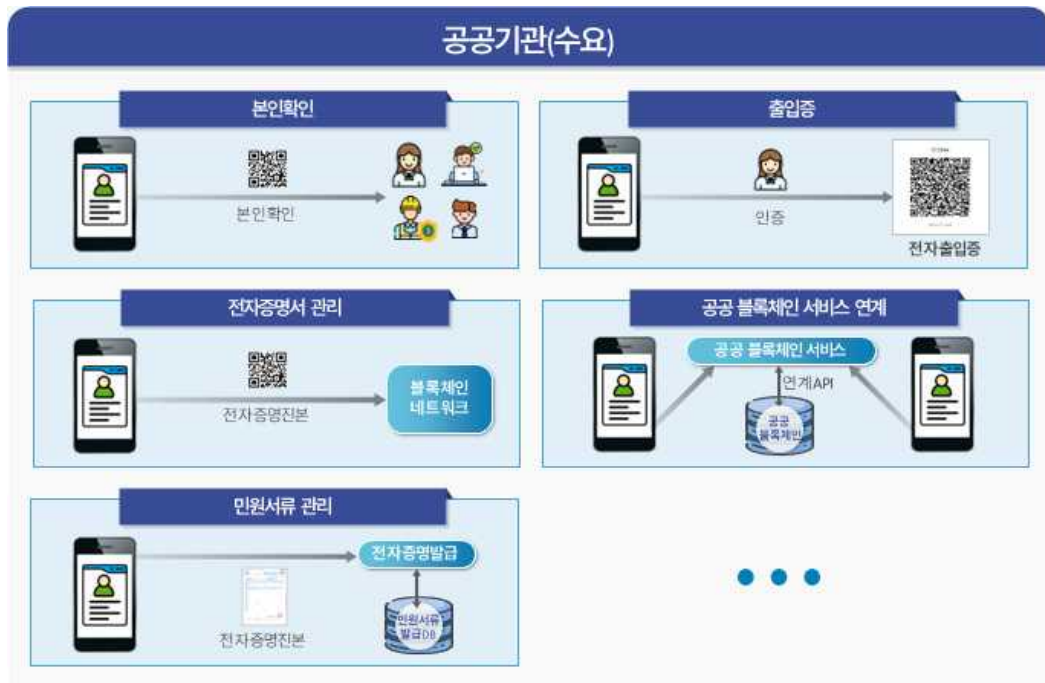


그림 47. 디지털 지갑을 활용한 공공서비스 예시

- 디지털 지갑 서비스를 제공하는 공공기관(수요)은 이용자(국민)가 비대면 환경에서 신원인증, 전자민원서류, 디지털자격증, 주민증/학생증, 진본증명 등을 보관하고 필요한 경우 바로 사용할 수 있는 서비스를 제공한다.
- 공공기관(수요)에서 발행한 인증, 전자민원서류, 디지털자격증, 주민증/학생증 등을 검증기관에 바로 제출 및 확인하여 검증을 통해 본인확인, 전자증명서, 민원서류, 출입 등 각종 민원 서비스에 활용할 수 있다.
- 디지털 지갑 호환성을 보장하여, 하나의 디지털 지갑으로 관리할 수 있어 편의성을 제공한다.

(다) 국내/외 유사 사례

- 한국, 2022, 기업간 신뢰 데이터 전송 및 이력 관리 서비스
- 한국, 2022, 웹 3.0 서비스 사용자를 위한 소셜인증 및 웹지갑 서비스

부록 4. K-BTF 공통요구사항 마련

1. 해외 주요 블록체인 모델의 공통요구사항 분석

(1) 해외 주요 국가의 블록체인 국가 플랫폼별 공통요구사항 분석

(가) 유럽 EBSI

- (개요) EBSI 포털¹⁾ 및 GitHub²⁾를 통해 개발문서 및 API를 제공하고 있다.
- (블록체인 네트워크 지원) EBSI 지원하는 퍼블릭 블록체인 네트워크는 dfuse-eos, EOS, ETH, Tezos, Findora, Near, Klaytn의 7종이다.
- (블록체인 프레임워크 지원) EBSI가 지원하는 블록체인 프레임워크는 Hyperledger Besu이다.
- (블록체인 프레임워크 기능)

1) 기능 목록 및 API

기능	API	기능설명
Authorisation API	Authorisation Service	OpenID 제공자 메타데이터
		OpenID 제공자 공개키
		프레젠테이션 정의 요구사항
		토큰 엔드포인트
Conformance	Auto Mock	Authorisation 서버 디스커버리 메타데이터
		Authorisation 서버의 JWKS 엔드포인트
		OIDC Authorisation 엔드포인트
		참조 요청
		직렬 포스트
		토큰 엔드포인트
	Issuer Mock	크리덴셜 발행자 디스커버리 메타데이터
		크리덴셜 엔드포인트

1) <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>

2) <https://github.com/protokol/ebs>

기능	API	기능설명
DID Registry	DID documents	연기된 크리덴셜 앤드포인트
		참조된 크리덴셜 오픈
		리스트 식별자
	JSON-RPC	DID 도큐먼트 획득 DID 수행 액션 JSON-RPC API
Ledger	Hyperledger Besu	Besu JSON-RPC API
Notification	Listnotification	Notification 목록
	Create a notification	Notification 생성
	Get a notification	Notification 획득
	Delete a notification	Notification 삭제
Proxy Data Hub	List Attributes	Attributes 목록
	Create an attribute	Attribute 생성
	Get an attribute	Attribute 획득
	Patch an attribute	Attribute 패치
	Delete and attribute	Attribute 삭제
Storage	Stores	저장소 목록
		저장소가 존재한다면 체크
	Proxy	Cassandra에 프록시 호출
	File Storage	Files 목록
		file 저장
		file 획득
		file의 메타데이터 패치
		file 삭제
		file의 메타데이터 획득
	Key-Value storage	Key-values 목록
		value 추가 또는 갱신
		value 획득
		key-value 삭제
Timestamp	Hash algorithms	hash algorithms 목록
		hash algorithms 획득
	Timestamps	timestamps 목록
		timestamp 획득
	Record	records 목록 record 획득

기능	API	기능설명
		record의 버전 목록
		version 획득
	JSON-RPC	JSON-RPC API
Trusted Apps Registry	Apps	apps 목록
		app 획득
		공개키 목록
		공개키 획득
		authorisations 목록
		authorisation 획득
	JSON-RPC	
Trusted Issuers Registry	Issuers	발행자 목록
		발행자 획득
		attributes 목록
		attribute 획득
		Revisions 목록
		proxies 목록
		proxy 획득
		StatusList2021Credential 획득
	JSON-RPC	
Trusted Policies Registry	Policies	policies 목록
		policy 획득
	User	users 목록
		user 획득
	JSON-RPC	JSON-RPC API
Trusted schemas Registry	Schemas	schemas 목록
		schema 획득
		schema 갱신 목록
		schema 갱신 획득
		메타데이터 갱신 목록
		metadata 획득
	JSON-RPC	JSON-RPC API
User Onboarding	Sessions	Sessions
	Authentication requests	Authentication 요청
	Authentication response	Authentication 응답

표 9. 유럽 EBSI 기능 및 API

2) 주요 기능별 공통 요구사항

- (Authorisation API) 디지털인증서를 위한 API로 인증(Authorisation) 서비스를 위한 OpenID, OpenID 메타정보, 공개키 제공 등의 기능을 제공한다.
- (DID Registry) 분산신원을 위한 API로 DID 도큐먼트에 대한 처리와 DID 실행에 필요한 기능을 제공한다.
- (Storage) 데이터를 저장할 저장소 및 데이터가 저장된 다양한 형식의 저장소로부터 파일을 불러와 CRUD하는 기능을 제공한다.
- (Trusted Apps/Issuers/Policies/schemas) 신뢰된 앱, 발행자, 정책, 스키마에 대한 리스트, 정보 조회 등을 위한 기능을 제공한다.

(나) 독일 GAIA-X

- (개요) GAIA-X 프레임워크 소개 형식으로
포털(<https://gaia-x.eu/gaia-x-framework/>) 및
GitLab(<https://gitlab.eclipse.org/eclipse/xfsc/>)을 통해 GAIA-X에 대한
주요 기능을 소개하고 있다.
- (블록체인 네트워크 지원) GAIA-X가 지원하는 퍼블릭 블록체인
네트워크는 공개되지 않았다.
- (블록체인 프레임워크 지원) GAIA-X가 지원하는 블록체인 프레임워크
는 공개되지 않았다.
- (블록체인 프레임워크 기능)

1) 기능 및 API

기능	API	세부 기능
Trust Services API	Policy evaluation	Policy 평가
	Policy management	Policy 관리
	Task controller	Task 컨트롤러
	Trust chain verification	신뢰 체인 확인
	JSON-LD signing and verifications	JSON-LD 사인 및 확인

기능	API	세부 기능
	eIDAS compliant signatures	eIDAS 준수 서명
	DID document resolving	DID 도큐먼트 해결
	Trusted caching	Trusted 캐시처리
	Trusted information exchange	Trusted 정보 교환
Notarization API	Internal Identity management	내부 Identity 관리
	Nortarization Request management	정규화 요청 관리
	Digital credential issuing	디지털 크리덴셜 발행
	eIDAS compliant signatures	eIDAS 준수 서명
	eIDAS compliant document verification	eIDAS 준수 도큐먼트 확인
	Electronic identification	전자 신분증

표 10. 독일 GAIA-X 기능 및 API

2) 주요 기능별 공통 요구사항

- (Trust services API) 신뢰기반 네트워크 체인을 위한 API로 DID, eIDAS, 신뢰기반 체인 검증 등의 기능을 제공한다.
- (Notarization API) eIDAS 에 대한 관리, 전자ID에 대한 공증에 필요한 기능을 제공한다.

(다) 중국 BSN

- (개요) BSN 개발자 포털³⁾ 및 GitHub⁴⁾를 통해 개발문서 및 API를 제공하고 있다.
- (블록체인 네트워크 지원) BSN 지원 퍼블릭 블록체인 네트워크는 dfuse-eos, EOS, ETH, Tezos, Findora, Near, Klaytn의 7종이다.
- (블록체인 프레임워크 지원) BSN이 지원하는 블록체인 프레임워크는 Hyperledger Fabric, FISCO BCOS, ConsenSys Quorum, Hyperledger Besu 4종이다.
- (블록체인 프레임워크 기능)

3) <https://bsnbase.io/g/main/documentation>

4) <https://github.com/BSNDA>

1) 기능 목록 및 API

기능	API 개수	기능 설명
PCN management	4	블록체인 PCN 정보, PCN의 리소스 가격 정보 등을 얻는 데 사용
Framework management	2	제휴 프레임워크의 판매 가능한 리소스 등 기본 프레임워크 정보를 얻는 데 사용
Dapp management	8	배포, 업그레이드, 시작 및 중지, 제거 및 리소스 구성 업그레이드와 같은 DApp 작업을 구현하는 데 사용
Dapp participation management	10	DApp 참여 관리, 사용자 권한 및 키 관리 구현에 사용
PCN information management	3	관련 DApp 및 블록체인 정보의 운영을 포함한 PCN 운영 상태 정보를 얻기 위해 사용
Data usage information	1	관련 DApp의 데이터 사용 정보를 얻기 위해 사용

표 11. 중국 BSN 기능 및 API

2) 주요 기능별 공통 요구사항

- (PCN management) 퍼블릭 블록체인 네트워크 관리를 위한 기능을 제공한다.
- (PCN information management) 퍼블릭 블록체인 네트워크 정보 관리를 위한 기능을 제공한다.
- (Framework management) BSN 프레임워크 관리를 위한 기능을 제공한다.
- (DApp management) DApp 관리를 위한 기능을 제공한다.
- (DApp participation management) DApp 참여자 관리를 위한 기능을 제공한다.
- (Data usage information) DApp과 관련된 정보 획득과 사용에 대한 기능을 제공한다.

(라) 싱가포르 OpenAttestation

○ (개요) OpenAttestation 개발자 포털⁵⁾ 및 GitHub⁶⁾를 통해 다양한

5)

기술문서와 데모용 소스코드를 제공하고 있다.

- (블록체인 네트워크 지원) OpenAttestation에서 지원하는 퍼블릭 블록체인 네트워크는 ETH이며 DID와 이더리움 스마트컨트랙트를 활용한다.
- (블록체인 프레임워크 지원) 자체 개발된 블록체인 프레임워크가 적용되었다.
- (블록체인 프레임워크 기능)
 - 1) 기능 목록 및 API

기능	API	기능 설명
Ethereum Smart Contracts	merkleRoot	머클루트
	Issuance	배급
	Revocation	폐지
	Issuance process and verification	배급 절차와 확인
DIDs	Issuance	배급
	Revocation	폐지
	Issuance process and verification	배급 절차와 확인

표 12. 싱가포르 OpenAttestation 기능 및 API

2) 주요 기능별 공통 요구사항

- (Ethereum Smart Contracts) 스마트계약 구현을 위한 머클루트, 발급, 해지와 관련된 기능을 제공한다.
- (DIDs) 분산신원 구현을 위한 발급, 해지, 발급 절차의 증빙을 위한 기능을 제공한다.

(마) 캐나다 OrgBook

- (개요) 캐나다 OrgBook은 개발자 사이트⁷⁾를 통해 기술 문서 및 기능별 API 가이드를 제공한다.
- (블록체인 네트워크 지원) 캐나다 OrgBook은 디지털 기록물의 공개

<https://www.openattestation.com/docs/developer-section/quickstart/create-verifiable-document-issuer>

6) <https://github.com/Open-Attestation/demo-verifiable-document-issuer>

7) <https://orgbook.gov.bc.ca/api/>

검색 가능한 디렉토리로 단순한 형태의 블록체인 네트워크를
지원한다.

○ (블록체인 프레임워크 지원) 블록체인 자격증명과 관련된 10개 기능
40종의 API를 제공한다.

○ (블록체인 프레임워크 기능)

1) 기능 목록 및 API

기능	API	기능 설명
credential	credential_list	크리덴셜 목록
	credential_read	크리덴셜 읽기
	credential_retrieve_formatted	크리덴셜 검색 포맷
	credential_get_latest	최근 크리덴셜 가져오기
	credential_verify	크리덴셜 확인
credentialtype	credentialtype_list	크리덴셜타입 목록
	credentialtype_read	크리덴셜타입 읽기
	credentialtype_fetch_language	크리덴셜타입 언어 패치
	credentialtype_fetch_logo	크리덴셜 로고 패치
feedback	feedback_create	피드백 생성
issuer	issuer_list	발행자 목록
	issuer_read	발행자 목록
	issuer_list_credential_types	크리덴셜 타입별 발행자 목록
	issuer_fetch_logo	발행자 로고 패치
quickload	api_v2_quickload	API v2 빠른 로드
schema	schema_list	스키마 목록
	schema_read	스키마 읽기
search	search_autocomplete_list	자동 완성 리스트 검색
	search_autocomplete_read	자동완성 읽기 검색
	search_credential_list	크리덴셜 목록 검색
	search_credential_facets	크리덴셜 facets 검색
	search_credential_topic_list	크리덴셜 토픽 목록 검색
	search_credential_topic_facets	크리덴셜 토픽 facets 검색
	search_credential_topic_read	크리덴셜 토픽 읽기 검색
	search_credential_read	크리덴셜 읽기 검색
status	api_v2_status	API v2 상태

기능	API	기능 설명
	api_v2_status_reset	API v2 상태 초기화
topic	topci_list	토픽 목록
	topic_retrieve_by_type	타입별 토픽 검색
	topic__ident_retrieve_by_type_for_matted	타입형태별 토픽 ID 검색
	topic_read	토픽 읽기
	topic_list_credentials	크리덴셜 토픽 목록
	topic_credential_list_active_credentials	활성화된 크리덴셜 토픽 목록
	topic_credential_list_historical_credentials	변경된 크리덴셜 토픽 목록
	topic_list_credential_sets	크리덴셜 셋 토픽 목록
	topic_retrieve_formatted	정형화된 토픽 검색
topic relationship	topic_relationship_list	토픽 관계 목록
	topic_relationship_read	토픽 관계 읽기
	topic_relationship_list_related_from_relations	상관관계별 토픽 관계 리스트
	topic_relationship_list_related_to_relations	상관관계간 토픽 관계 리스트

표 13. 캐나다 OrgBook 기능 및 API

2) 주요 기능별 공통 요구사항

- (Credential) 디지털자격증명을 위한 자격증명정보, 자격증명 확인, 자격증명 목록 확인 기능을 제공한다.
- (Credentialtype) 디지털자격증명 유형을 위한 자격증명유형정보 및 로그 등의 확인 기능을 제공한다.
- (issuer) 디지털자격증명 발행자에 대한 목록, 자격증명 유형 등을 위한 기능을 제공한다.

2. K-BTF 공통요구사항

(1) 분산신원 공동인프라의 공통요구사항

- (공통요구사항) 분산신원 공동인프라는 기존 구축된 민간사업자와의 상호호환성 확보가 필요하다. 민간의 적극적인 참여를 위해서는 블록체인

성능 요건과 블록체인 네트워크 간의 연계 요건에 대한 기준을 제시하는 방안을 고려해야 한다. 만약 K-BTF 자체적으로 또 다른 분산신원 서비스를 구축할 경우에 이에 해당하는 공통요구사항을 제시해야 한다.

- 분산신원 공동인프라는 크게 발급단계와 사용단계로 나눌 수 있다.
- (발급 단계) 이용자는 발행 기관에게 분산신원을 요청하여 신원 증명에 대한 정보를 발급받는다. 분산신원 발급 시 발행 기관은 분산신원 발행 정보를 K-BTF를 활용하여 저장 한다. 추후 발급받은 분산신원은 이용자 단말기 내 저장되며 이용자는 스스로 정보를 관리하고 필요한 경우 원하는 서비스를 이용한다.
- 블록체인 내에 저장된 정보는 분산신원 발급정보가 저장되기 때문에 민감한 개인정보가 아닌 공개 가능 정보이다. 즉, 민감한 정보인 발행 기관으로 받은 VC(Verifiable Credential)는 자신이 소유한 단말기에 저장한다. VC는 발급자 정보, 자격 정보, 발급자 서명 등을 포함한다. 블록체인에는 분산신원 발급정보의 경우 발급된 분산신원의 유효성 검증을 위한 정보들이 포함되어야 하기 때문에 다음과 같은 정보로 구성되며 이를 분산신원 문서(Documents)라고 한다.
- (@context) 본 속성은 데이터 교환이 필요한 경우 두 시스템 모두 이해 가능한 용어와 프로토콜을 명시한다. 속성 값은 반드시 하나 이상의 URIs이다.
- (ID) 분산신원은 반드시 하나의 유효한 값으로 표현되어야 한다. 하나의 주체를 유일한 식별자로 표시해야 분산신원으로 식별하고 분산신원 문서에 의해 항목들을 설명할 수 있다.
- (공개키(Public Key)) 서비스 지점간에 인증을 통해 안전한 통신 채널을 형성하는데 필요하다. 전자서명, 암호화 등 암호학적 도구를 사용하여 생성된다. 공개키 객체들의 배열로 구성하며 각 객체들은 타입, 컨트롤러 속성을 반드시 포함해야 한다.

공개키 타입	설명
RSA	RSA 공개키 값은 반드시 JWK(JSON Web Key) 혹은 PEM(Privacy Enhanced Mail) 포맷으로 인코딩한다.
ed25519	ed25519 공개키 값은 반드시 JWK 혹은 원시형태의 33바이트 공개키값을 Base58 비트코인 포맷으로 인코딩 한다.
secp256k1-koblitz	Secp256k1 Koblitz 공개키 값은 반드시 JWK 혹은 원시형태의 33바이트 공개키 값을 Base58 비트코인 포맷으로 인코딩한다.
secp256r1	secp256r1 공개키 값은 반드시 JWK 혹은 원시형태의 32바이트 공개키 값을 Base58 비트코인 포맷으로 인코딩한다.
Curve25519 (X25519)	Curve25519 공개키값은 반드시 JWK 혹은 원시형태의 32바이트 공개키 값을 Base58 비트코인 포맷으로 인코딩한다.

표 14. 공개키 타입 분류

- (인증(Authentication)) 분산신원 컨트롤러가 해당 분산신원과 연결되어 있다는 것을 암호화 방식으로 증명하는 것이며 타인이 자신의 분산신원 문서에 대한 제어 권한을 증명하지 않고도 업데이트하도록 인증과 권한 부여가 분리되어 있다. 인증 속성의 값은 검증 메소드의 배열이며 각 검증 방법에 대한 내용이 포함되거나 참조된다.
- (서비스 엔드포인트) 서비스 제공자를 지칭하며, 이를 분산신원 문서 내 저장하여 분산신원 주체가 공시한 모든 유형의 서비스를 검색할 수 있다.
- (이용 단계) 서비스를 제공하는 기관에게 올바르게 발급된 유효한 분산신원이 있다는 사실을 검증받는 과정이다. 즉, 이용자는 기관에게 서비스를 요청한 후 이용자 단말 내 저장되어있는 분산신원정보를 기관에게 제공한다. 기관은 K-BTF를 사용하여 분산신원정보 조회를 통해 유효성 검증을 진행한 후 이용자에게 서비스 제공 여부를 판단한다.
- 분산신원 사용 시 이용자는 분산신원 검증 데이터를 서비스를 제공하는 기관에게 전달해야한다. 이때, 이용자는 VC가 아닌 VP(Verifiable Presentation)의 형태로 제공해야 한다. VP는 자기 주권 신원(Self Sovereign Identity) 모델에서 최소 정보 공개 원칙에 따라 구성된 검증 데이터의 모음이다. 개인정보보호가 주 목적이기에 VC 내 포함된 개인 정보들을 모두 제공할 필요는 없다. 즉, 서비스를 제공받기 위해

최소한을 필요한 정보만 선택한 뒤 이용자의 개인키로 서명하여 기관에게 전달한다. 더불어 VP 내 정보 구성에 따라 이용자는 하나 또는 다수의 자격 증명까지 가능하다.

(가) 분산신원 공동인프라 공통요구사항 명세서

요구사항 정의	클라우드 기반 분산신원 공동인프라 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 및 컨테이너 기반 개발·검증환경 구축해야 함 <ul style="list-style-type: none"> - 개발 및 검증 환경 구축 일정 계획을 수립해야 함 - 소요자원(VM, vCPU, Memory, Network 등)을 검토해야 함 - 개발 및 검증 환경 구성 방안을 제시해야 함 - 효율적인 자원 운영 관리와 고가용성(HA) 확보 방안 제시해야 함 - 테스트를 위한 구성 변경 및 자원 할당 계획을 수립해야 함 ○ 시스템 아키텍처 설계와 구현 결과물의 정합성을 검증해야 함
요구사항 정의	분산신원 공동인프라 이용포털(대시보드) 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 회원 관리, 관리자 관리 등 서비스를 제공해야 함 ○ 관리자 관리 <ul style="list-style-type: none"> - 관리자(계정) 가입/승인/조회 및 상태 관리 - 관리자 계정 삭제 - 시스템 접근정보 이력관리 등 ○ 관리시스템 대시보드 <ul style="list-style-type: none"> - 관리시스템 메인 대시보드 - 이용자 관련 각종 현황 - 분산신원 관련 각종 현황 - 블록체인플랫폼 공동인프라 관련 각종 현황 - 디지털 지갑서비스 관련 각종 현황

요구사항 정의	분산신원 ID 생성·조회·변경·삭제·관리 모듈 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 분산신원 관리 모듈 ○ 분산신원 전주기 기능을 제공해야 함 <ul style="list-style-type: none"> - 분산신원발급, DID Document 및 개인키 생성/등록/조회/갱신/만료/폐기 기능을 제공해야 함 - 분산신원 Delegator, Registerer 및 Resolver 제공해야 함 - VC(Verifiable Credential)/VP(Verifiable Presentation) 관리기능을 제공(모바일기기내 안전한 저장 기능 제시)해야 함 - QR 기반의 인증 기능을 제공해야 함 - 외부 정보인터페이스(API, SDK 등)를 제공해야 함 ○ 외부 DID 연계 기능을 제공해야 함 ○ W3C 표준을 준수하여 관련 기능을 구현해야 함 ○ 분산신원 기능 연계를 위한 정규화된 API 및 문서를 제공해야 함 ○ 개인 신원정보(VC)를 모바일 기기에서 안전하게 관리할 수 있는 방안을 제안하여야 함 ○ 모바일 기기 제조사에서 안전한 저장소를 제공하는 경우 이를 사용하여야 함 ○ DID 관련 기술 표준을 준수해야 함 <ul style="list-style-type: none"> - W3C, Decentralized Identifiers(DIDs) v1.0 - W3C, Verifiable Credential Model v1.1
요구사항 정의	분산원장 규격
요구사항 상세설명	<ul style="list-style-type: none"> ○ 분산원장 무결성 확보해야 함 <ul style="list-style-type: none"> - 원장 무결성 확보 방안 및 각 노드의 데이터가 동등함을 보장할 수 있는 동기성 확보 방안을 제시해야 함 - 원장의 백업 및 복구 방안을 제시해야 함 ○ 스마트계약을 개발할 수 있는 환경(IDE)을 제공해야 함 <ul style="list-style-type: none"> - 스마트계약의 개발부터 배포까지의 형상관리 및 테스트 방안을 제시해야 함 - 스마트계약의 악성코드 검출 기능/도구를 제공해야 함 ○ 분산원장과의 인터페이스 및 dAPP개발을 위한 Node API 및 SDK를 제공해야 함 ○ 기타 서비스 운영에 필요한 기타 모듈을 제공해야 함

요구사항 정의	외부정보 인터페이스(시스템 연계)
요구사항 상세설명	<ul style="list-style-type: none"> ○ 외부정보 인터페이스(시스템 연계) 표준 수립 및 검증된 표준 인터페이스를 적용(정확성, 무결성, 정합성 검증 필요) ○ 연계 대상기관과의 인터페이스 정합성을 위한 기술을 지원해야 함 ○ 내부 연계, 외부 연계별로 관리 방안을 제시해야 함 ○ 송·수신 메시지에 대한 암호·복호화 방안을 제시해야 함 ○ 향후 연계기관 확대를 고려한 구축 방안을 마련해야 함 ※ 전달기관(KISA)와 사업자(제안사) 간 협의한 후 확정해야 함

(나) 분산신원 공동인프라 성능 요구사항 명세서

요구사항 정의	분산신원 공동인프라 성능 측정 및 목표 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 다수의 이용자가 안정적으로 분산신원 서비스를 이용할 수 있는 성능지표의 목표 수치를 제시해야 함 <ul style="list-style-type: none"> - 성능지표는 전 주기(DID 생성, 조회, 수정, 삭제, VC·VP 발행, 제출, 검증 등) 별 트랜잭션 처리속도(TPS), 평균 응답시간(Latency), 블록 확장 시간(Confirm Time), 데이터 정합성(Data Consistency) 임 ※ 성능지표는 추후 전달기관(KISA)과 협의에 따라 변경될 수 있음 ○ 사업 진행과정에서 제시한 목표 수치를 충족하지 못할 경우 개선 방안을 제시하고 목표치를 달성해야 함

(다) 분산신원 공동인프라 보안 요구사항 명세서

요구사항 정의	DB 및 오프체인 보안 요구사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구축, 정책설정, 권한설정 등 보안 준수사항을 고려하여 설계/지원해야 함 <ul style="list-style-type: none"> - 블록체인에 수록되는 개인정보, 민감정보 등에 대해 오프체인 기법을 통한 저장·관리해야 함 ○ 오프체인 성능검증 및 보완조치를 수행해야 함 ○ 암호복호화 정책, 비밀키 관리, 로그 관리, 운영관리 등 방안을 마련해야 함

요구사항 정의	개인정보 암호화 처리 방안 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 개인정보 암호화 방식은 API 방식으로 구현해야 함 ○ 암호화 대상은 고유식별정보(주민번호, 외국인번호, 여권번호 등, 이하 “주민번호”), 패스워드 등이며 향후 확장성을 고려하여 구축 <ul style="list-style-type: none"> ※ 암호화 알고리즘은 전담기관(KISA)과 사업 추진 시 협의 후 결정 ○ 외부 데이터 연계 시 암호화 처리 방안 제시해야 함

요구사항 정의	ISMS-P 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ ISMS-P를 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

요구사항 정의	클라우드 인증(CSAP) 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 인증을 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

(라) 분산신원 공동인프라 테스트 요구사항 명세서

요구사항 정의	분산신원 공동인프라 테스트 계획 수립에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트, 통합테스트, 성능테스트를 진행해야 함 ○ 테스트 사용자별 테스트 시나리오, 단계별 수행방법, 수행절차, 참여조직 및 역할, 점검사항, 테스트일정, 시험환경 및 평가 기준을 구체적으로 수립 및 제시해야 함 ○ 내·외부시스템 인터페이스 환경 및 데이터 연계 테스트는 테스트 데이터를 사용하여 진행해야 함

요구사항 정의	분산신원 공동인프라 단위테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트의 범위, 수행절차, 조직, 일정, 시험환경 및 평가기준을 구체적으로 수립해야 함 ○ 단위테스트 시나리오별, 처리 절차, 수행데이터, 예상결과 등을 사전에 정의해야 함 <ul style="list-style-type: none"> - 결함유형 분석(결함발생건수, 결함비율) - 결함발견 추세분석(테스트일시, 발견결함 수) - 테스트 커버리지

요구사항 정의	분산신원 공동인프라 통합테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 통합테스트 시나리오 별 단위테스트가 완료된 프로그램 대상으로 다음 사항을 검증해야 함 - 기능, 성능 등의 요구사항 및 설계사양 충족여부를 검증해야 함 - 기능의 정상적 수행여부를 검증해야 함 - 기능수행 후의 결과가 사전에 예측된 결과와 일치하는지를 검증해야 함 - 접근권한 및 업무 권한에 대한 적절성을 검증해야 함 - 연계 및 이를 포함하는 업무흐름을 검증해야 함 - 대외기관 연계 및 업무 흐름을 검증해야 함 - 결함 분석 및 원인 추적을 통해 결함을 제거해야 함

(마) 분산신원 공동인프라 품질 요구사항 명세서

요구사항 정의	분산신원 공동인프라 품질보증 일반사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 품질보증의 범위, 품질보증을 위한 조직, 절차, 점검방법 등을 제시하여야 함 - 품질관리를 위한 제반 절차 및 산출물을 사업수행계획서에 상세하게 기술해야 함 - 품질 또는 성능상의 문제 발생 시 성능 테스트 및 분석결과를 제시하고 개선해야 함 - 품질향상을 위한 전담기관(KISA)의 요구사항이 있을 경우 이를 검토하여 보완해야 함 - 품질관리 조직과 운영 절차를 구체적으로 제시하고 준수해야 함

요구사항 정의	분산신원 공동인프라 기능 구현 정확성
요구사항 상세설명	<ul style="list-style-type: none"> ○ 서비스에서 제공하기로 한 요구사항을 모두 제공해야 함 ○ 테스트를 통해 예상된 평가가 도출되었을 경우 기능 요구사항을 만족한 것으로 판단함

요구사항 정의	분산신원 공동인프라 결함의 발견과 발견된 결함의 조치
요구사항 상세설명	<ul style="list-style-type: none"> ○ 테스트 기간 동안 발견된 결함 수를 측정하며, 결함 발생률이 기대수준 이상이거나 중대 결함이 발생한 경우 서비스 오픈 시점을 연기하거나 보완 대책을 즉시 수립해야 함 ○ 테스트 기간 동안 발견된 결함은 100% 조치해야 함

요구사항 정의	분산신원 공동인프라 장애 발생에 따른 요구 및 신속한 복구 구현
요구사항 상세설명	<ul style="list-style-type: none"> ○ 사업자(제안사)는 장애발생 시 즉시 장애복구 조치에 임하여야 하며, 장애복구 조치로 해결이 불가능한 문제에 대해서는 4시간 이내 전문인력이 도착하여 정상복구를 위한 추가 조치를 수행해야 함 ○ 신속한 장애대응을 위하여 백업절차를 마련해야 함 ○ 장애 발생 처리 완료 후 장애 조치 보고서는 48시간 이내 제출해야 함

(바) 분산신원 공동인프라 데이터 요구사항 명세서

요구사항 정의	데이터베이스 설계 표준화 지침 준수
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구조 설계는 관련 서비스 처리 절차를 반영하여 표준화하고 향후 변동에 따른 확장성을 고려해야 함 <ul style="list-style-type: none"> - 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 DB 설계 ○ 향후 시스템 확장성 등을 고려하여 블록체인 데이터를 정의해야 함 <ul style="list-style-type: none"> - 블록체인 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 블록체인 데이터를 정의해야 함

(2) 디지털인증서 공동인프라의 공통요구사항

○ (공통요구사항) 디지털인증서 공동인프라를 효과적으로 구현하기 위해서 적절한 방안으로는 대체불가토큰(Non-Fungible Token, 이하 NFT)을 활용하는 것이다. 공공기관은 K-BTF의 디지털인증서 생성 기능을 활용하여 디지털인증서를 생성하고 이용자에게 발급한다. 이용자들은 발급받은 디지털인증서를 자신의 중앙지갑에 보유하고 다양한 기관에서 자격증명, 원본 유효성 검증 등에 대한 요청에 응대할 수 있다. 서비스를 제공하는 공공 기관 입장에서는 디지털인증서의 이력 조회와 소유자 검증을 바탕으로 서비스 제공 여부를 판단할 수 있다. 현재 NFT의 가장 보편적인 표준은 ERC721이며, 다음의 인터페이스를 표준으로 규정하였다.

- (balanceOf) 이용자가 가지고 있는 NFT 개수를 반환하는 기능
- (OwnerOf) 특정 NFT 아이디에 대한 소유주 주소를 반환하는 기능
- (approve) 특정 타인에게 자신이 소유한 특정 NFT 소유권을 허용하는 기능

- (transferFrom) NFT 소유권을 타인에게 전송하는 기능
- (safeTransferFrom) 타인이 NFT를 소유할 수 있는지 판단한 후 NFT 소유권을 전송하는 기능
- (getApproved) 특정 NFT가 타인에게 사용 승인되었는지 여부를 반환하는 기능
- (setApprovalForAll) 특정 타인에게 자신이 소유한 모든 NFT의 소유권을 허용하는 기능
- (isApprovedForAll) 이용자가 소유한 모든 NFT의 사용권을 특정 타인에게 허용했는지를 판단하는 기능
- NFT를 사용하여 디지털인증서 구현시 파일 저장에 대해 고려해야 한다. 블록체인 내 디지털인증서의 원본 파일을 함께 저장할 수 있으나 보안과 효율성을 위하여 분산형 P2P 파일 시스템인 IPFS(InterPlanetary File System) 사용이 권장된다. IPFS를 활용한 블록체인 데이터 저장 프로세스 구조의 핵심은 트랜잭션 내 원본 데이터의 저장이 아닌 IPFS 메타데이터를 저장하는 것이다. IPFS는 데이터가 작은 블록으로 쪼개져서 다수의 컴퓨터로 분산 저장되기 때문에 노드 간 신뢰와 단일 장애 지점(Single Point of Failure)이 없다. 이를 통해 음성, 영상과 같은 대용량 데이터에 대한 전송과 악의적인 해커나 서버로 인한 데이터의 변경, 삭제 문제에 대한 해결이 가능하다.
- (주요 기능) 디지털인증서 공동인프라에서는 NFT의 고유성을 바탕으로 인증서에 대한 자격증명, 원본 유효성 등의 기능을 구현하여 제공하는 것을 예상하며 다음과 같은 기능들이 필수적으로 요구된다.

기능	기능 설명
디지털인증서 스마트 계약 배포	수요 기관에서 사용하고자 하는 용도와 목적에 맞는 디지털 증서에 대한 스마트 계약을 배포하는 기능이다. 동일한 스마트 계약 코드로 배포될 수 있기 때문에 각 스마트 계약에 대한 식별자가 포함된다.
디지털인증서 생성	특정 디지털 증서를 생성하는 기능이다.
디지털인증서 소유권 확인	특정 디지털 증서에 대한 소유권을 확인하는 기능이다.
디지털인증서 소유권 이전	디지털 증서의 소유권을 특정 타인에게 이전하는 기능이다.
디지털인증서 소유권 이전 승인	디지털 증서의 소유권 이전을 제3자에게 위임하는 것으로 올바른 위임자만이 위임받은 디지털 증서의 소유권 이전을 진행할 수 있다.
디지털인증서 조회	디지털 증서의 정보를 조회하는 기능이다. 인자에 따라 하나의 디지털증서 정보, 다수의 디지털 증서 정보, 네트워크 내 모든 디지털 증서 정보 등을 선택 가능하다.
디지털인증서 소각	현재 보유하고 있는 디지털 증서를 소각하는 기능이다. 디지털 증서의 공급량을 조절할 수 있으며 무분별한 디지털 증서 생성을 방지할 수 있다.

표 15. 디지털인증서 주요 기능

(가) 디지털인증서 공동인프라 공통요구사항 명세서

요구사항 정의	클라우드 기반 디지털인증서 공동인프라 개발
요구사항 상세설명	<p>○ 클라우드 및 컨테이너 기반 개발·검증환경 구축해야 함</p> <ul style="list-style-type: none"> - 개발 및 검증 환경 구축 일정 계획을 수립해야 함 - 소요자원(VM, vCPU, Memory, Network 등)을 검토해야 함 - 개발 및 검증 환경 구성 방안을 제시해야 함 - 효율적인 자원 운영 관리와 고가용성(HA) 확보 방안 제시해야 함 - 테스트를 위한 구성 변경 및 자원 할당 계획을 수립해야 함 <p>○ 시스템 아키텍처 설계와 구현 결과물의 정합성을 검증해야 함</p>

요구사항 정의	디지털인증서 공동인프라 이용포털(대시보드) 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 회원 관리, 관리자 관리 등 서비스를 제공해야 함 ○ 관리자 관리 <ul style="list-style-type: none"> - 관리자(계정) 가입/승인/조회 및 상태 관리 - 관리자 계정 삭제 - 시스템 접근정보 이력관리 등 ○ 관리시스템 대시보드 <ul style="list-style-type: none"> - 관리시스템 메인 대시보드 - 이용자 관련 각종 현황 - NFT 관련 각종 현황 - 블록체인플랫폼 공동인프라 관련 각종 현황 - 디지털 지갑서비스 관련 각종 현황

요구사항 정의	디지털인증서 공동인프라 생성·조회·변경·삭제·관리·소각 모듈 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ NFT 생성·조회·변경·삭제·관리·소각 모듈을 개발하여 NFT 기능을 제공해야 함 <ul style="list-style-type: none"> - NFT생성·조회·변경·삭제·관리·소각 API를 지원해야 함 - 발행자/소유자 확인 기능을 제공해야 함 - 타 플랫폼으로의 NFT 전송 기능(public 오픈 마켓 포함)을 제공해야 함 - 스마트컨트랙트 제어 옵션을 제공해야 함 - 거래 가능 여부 제어 옵션을 제공해야 함 - 타인 NFT 조회/검증 사용자별 페이지 제공해야 함 ○ 디지털인증서 템플릿을 지원해야 함 <ul style="list-style-type: none"> - 템플릿 생성/조회/변경 관리 API 제공해야 함 - 복수기관이 사용 가능한 템플릿 관리자를 제공해야 함 ○ NFT 관련 표준을 준수해야 함 <ul style="list-style-type: none"> - TTA, 대체 불가능 토큰의 디지털 콘텐츠 저작권 정보 확인 명세 - 1EdTech, Open Badges Specification 3.0 Candidate Final Public - 1EdTech, Open Badges 3.0 Implementation Guide

요구사항 정의	분산원장 규격
요구사항 상세설명	<ul style="list-style-type: none"> ○ 분산원장 무결성 확보해야 함 <ul style="list-style-type: none"> - 원장 무결성 확보 방안 및 각 노드의 데이터가 동등함을 보장할 수 있는 동기성 확보 방안을 제시해야 함 - 원장의 백업 및 복구 방안을 제시해야 함 ○ 스마트계약을 개발할 수 있는 환경(IDE)을 제공해야 함 <ul style="list-style-type: none"> - 스마트계약의 개발부터 배포까지의 형상관리 및 테스트 방안을 제시해야 함 - 스마트계약의 악성코드 검출 기능/도구를 제공해야 함 ○ 분산원장과의 인터페이스 및 dAPP개발을 위한 Node API 및 SDK를 제공해야 함 ○ 기타 서비스 운영에 필요한 기타 모듈을 제공해야 함

요구사항 정의	외부정보 인터페이스(시스템 연계)
요구사항 상세설명	<ul style="list-style-type: none"> ○ 외부정보 인터페이스(시스템 연계) 표준 수립 및 검증된 표준 인터페이스를 적용(정확성, 무결성, 정합성 검증 필요) ○ 연계 대상기관과의 인터페이스 정합성을 위한 기술을 지원해야 함 ○ 내부 연계, 외부 연계별로 관리 방안을 제시해야 함 ○ 송·수신 메시지에 대한 암호·복호화 방안을 제시해야 함 ○ 향후 연계기관 확대를 고려한 구축 방안을 마련해야 함 ※ 전담기관(KISA)와 사업자(제안사) 간 협의한 후 확정해야 함

(나) 디지털인증서 공동인프라 성능 요구사항 명세서

요구사항 정의	디지털인증서 공동인프라 성능 측정 및 목표제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 다수의 이용자가 안정적으로 NFT 기능을 이용할 수 있는 성능지표의 목표 수치를 제시해야 함 <ul style="list-style-type: none"> - NFT의 성능지표는 전 주기(NFT 생성, 조회, 수정, 삭제, 발행, 제출, 검증 등) 별 트랜잭션 처리속도(TPS), 평균 응답시간(Latency), 블록 확장 시간(Confirm Time), 데이터 정합성(Data Consistency)임 ※ 성능지표는 추후 전담기관(KISA)과 협의에 따라 변경될 수 있음 ○ 사업 진행과정에서 제시한 목표 수치를 충족하지 못할 경우 개선 방안을 제시하고 목표치를 달성해야 함

(다) 디지털인증서 공동인프라 보안 요구사항 명세서

요구사항 정의	DB 및 오프체인 보안 요구사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구축, 정책설정, 권한설정 등 보안 준수사항을 고려하여 설계/지원해야 함 - 블록체인에 수록되는 개인정보, 민감정보 등에 대해 오프체인 기법을 통한 저장·관리해야 함 ○ 오프체인 성능검증 및 보완조치를 수행해야 함 ○ 암호화 정책, 비밀키 관리, 로그 관리, 운영관리 등 방안을 마련해야 함
요구사항 정의	개인정보 암호화 처리 방안 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 개인정보 암호화 방식은 API 방식으로 구현해야 함 ○ 암호화 대상은 고유식별정보(주민번호, 외국인번호, 여권번호 등, 이하 “주민번호”), 패스워드 등이며 향후 확장성을 고려하여 구축 ※ 암호화 알고리즘은 전담기관(KISA)과 사업 추진 시 협의 후 결정 ○ 외부 데이터 연계 시 암호화 처리 방안 제시해야 함
요구사항 정의	ISMS-P 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ ISMS-P를 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함
요구사항 정의	클라우드 인증(CSAP) 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 인증을 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

(라) 디지털인증서 공동인프라 테스트 요구사항 명세서

요구사항 정의	디지털인증서 공동인프라 테스트 계획 수립에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트, 통합테스트, 성능테스트를 진행해야 함 ○ 테스트 이용자별 테스트 시나리오, 단계별 수행방법, 수행절차, 참여조직 및 역할, 점검사항, 테스트일정, 시험환경 및 평가 기준을 구체적으로 수립 및 제시해야 함 ○ 내·외부시스템 인터페이스 환경 및 데이터 연계 테스트는 테스트 데이터를 사용하여 진행해야 함

요구사항 정의	디지털인증서 공동인프라 단위테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트의 범위, 수행절차, 조직, 일정, 시험환경 및 평가기준을 구체적으로 수립해야 함 ○ 단위테스트 시나리오별, 처리 절차, 수행데이터, 예상결과 등을 사전에 정의해야 함 <ul style="list-style-type: none"> - 결함유형 분석(결함발생건수, 결함비율) - 결함발견 추세분석(테스트일시, 발견결함 수) - 테스트 커버리지

요구사항 정의	디지털인증서 공동인프라 통합테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 통합테스트 시나리오 별 단위테스트가 완료된 프로그램 대상으로 다음 사항을 검증해야 함 <ul style="list-style-type: none"> - 기능, 성능 등의 요구사항 및 설계사항 충족여부를 검증해야 함 - 기능의 정상적 수행여부를 검증해야 함 - 기능수행 후의 결과가 사전에 예측된 결과와 일치하는지를 검증해야 함 - 접근권한 및 업무 권한에 대한 적절성을 검증해야 함 - 연계 및 이를 포함하는 업무흐름을 검증해야 함 - 대외기관 연계 및 업무 흐름을 검증해야 함 - 결함 분석 및 원인 추적을 통해 결함을 제거해야 함

(마) 디지털인증서 공동인프라 품질 요구사항 명세서

요구사항 정의	디지털인증서 공동인프라 품질보증 일반사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 품질보증의 범위, 품질보증을 위한 조직, 절차, 점검방법 등을 제시하여야 함 <ul style="list-style-type: none"> - 품질관리를 위한 제반 절차 및 산출물을 사업수행계획서에 상세하게 기술해야 함 - 품질 또는 성능상의 문제 발생 시 성능 테스트 및 분석결과를 제시하고 개선해야 함 - 품질향상을 위한 전담기관(KISA)의 요구사항이 있을 경우 이를 검토하여 보완해야 함 - 품질관리 조직과 운영 절차를 구체적으로 제시하고 준수해야 함

요구사항 정의	디지털인증서 공동인프라 기능 구현 정확성
요구사항 상세설명	<ul style="list-style-type: none"> ○ 서비스에서 제공하기로 한 요구사항을 모두 제공해야 함 ○ 테스트를 통해 예상된 평가가 도출되었을 경우 기능 요구사항을 만족한 것으로 판단함

요구사항 정의	디지털인증서 공동인프라 결함의 발견과 발견된 결함의 조치
요구사항 상세설명	<ul style="list-style-type: none"> ○ 테스트 기간 동안 발견된 결함 수를 측정하며, 결함 발생률이 기대수준 이상이거나 중대 결함이 발생한 경우 서비스 오픈 시점을 연기하거나 보완 대책을 즉시 수립해야 함 ○ 테스트 기간 동안 발견된 결함은 100% 조치해야 함

요구사항 정의	디지털인증서 공동인프라 장애 발생에 따른 요구 및 신속한 복구 구현
요구사항 상세설명	<ul style="list-style-type: none"> ○ 사업자(제안사)는 장애발생 시 즉시 장애복구 조치에 임하여야 하며, 장애복구 조치로 해결이 불가능한 문제에 대해서는 4시간 이내 전문인력이 도착하여 정상복구를 위한 추가 조치를 수행해야 함 ○ 신속한 장애대응을 위하여 백업절차를 마련해야 함 ○ 장애 발생 처리 완료 후 장애 조치 보고서는 48시간 이내 제출해야 함

(바) 디지털인증서 공동인프라 데이터 요구사항 명세서

요구사항 정의	데이터베이스 설계 표준화 지침 준수
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구조 설계는 관련 서비스 처리 절차를 반영하여 표준화하고 향후 변동에 따른 확장성을 고려해야 함 <ul style="list-style-type: none"> - 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 DB 설계 ○ 향후 시스템 확장성 등을 고려하여 블록체인 데이터를 정의해야 함 <ul style="list-style-type: none"> - 블록체인 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 블록체인 데이터를 정의해야 함

(3) 데이터이력추적 공동인프라의 공통요구사항

- (공통요구사항) 공공기관에서 보유한 정보를 블록체인 네트워크 내 저장
을 요청하면 데이터는 블록체인 내 트랜잭션의 형태로 저장된다. 트랜잭
션을 구성하는 데이터는 시간에 대한 이력 정보를 가진 타임스탬프를
포함하고 있다. 저장된 데이터는 여러 공공기관에서 데이터 이전, 검증
등의 다양한 서비스로 사용되며, 데이터이력추적 공동인프라에 사용될
때마다 타임스탬프가 포함된 트랜잭션이 발생되어 블록체인에 기록된다.
데이터이력추적 공동인프라를 통해 타 기관에서 특정 기간에 대한 데이
터 사용 이력 조회를 요청하면 기관은 블록체인 네트워크 내 저장된 데
이터의 사용 이력 정보를 반환받을 수 있다.

○ (주요 기능) 본 서비스를 구성하기 위해서는 필수적으로 아래와 같은 기능이 요구된다.

기능	기능 설명
정보 저장	네트워크 풀 내 정보를 저장 등록되는 정보는 기관에서 관리하는 이용자의 개인 정보를 노출시키지 않는다.
이력 조회	특정 데이터의 변경 이력을 타임스탬프와 결합된 형태로 반환한다.
이력 조회 내역	이력 추적을 요청한 개체, 횟수, 시간 등 특정 데이터에 대한 불특정 다수의 이력 조회 내역을 반환하는 기능이다.
이력 검증	제출된 데이터와 블록체인에 기록된 해당 데이터 이력을 비교하여 유효성을 검증하고 반환하는 기능이다.

표 16. 데이터이력추적 주요 기능

(가) 데이터이력추적 공동인프라 공통요구사항 명세서

요구사항 정의	클라우드 기반 데이터이력추적 공동인프라 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 및 컨테이너 기반 개발·검증환경 구축해야 함 <ul style="list-style-type: none"> - 개발 및 검증 환경 구축 일정 계획을 수립해야 함 - 소요자원(VM, vCPU, Memory, Network 등)을 검토해야 함 - 개발 및 검증 환경 구성 방안을 제시해야 함 - 효율적인 자원 운영 관리와 고가용성(HA) 확보 방안 제시해야 함 - 테스트를 위한 구성 변경 및 자원 할당 계획을 수립해야 함 ○ 시스템 아키텍처 설계와 구현 결과물의 정합성을 검증해야 함

요구사항 정의	데이터이력추적 이용포털(대시보드) 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 회원 관리, 관리자 관리 등 서비스를 제공해야 함 ○ 관리자 관리 <ul style="list-style-type: none"> - 관리자(계정) 가입/승인/조회 및 상태 관리 - 관리자 계정 삭제 - 시스템 접근정보 이력관리 등 ○ 관리시스템 대시보드 <ul style="list-style-type: none"> - 관리시스템 메인 대시보드 - 이용자 관련 각종 현황 - 분산신원 관련 각종 현황 - 블록체인플랫폼 공동인프라 관련 각종 현황 - 디지털 지갑서비스 관련 각종 현황

요구사항 정의	데이터이력추적 공동인프라 모듈 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 데이터이력추적 기능 <ul style="list-style-type: none"> - 정보 저장 - 정보 이력 조회 - 이력 조회 내역 - 이력 검증

요구사항 정의	분산원장 규격
요구사항 상세설명	<ul style="list-style-type: none"> ○ 분산원장 무결성 확보해야 함 <ul style="list-style-type: none"> - 원장 무결성 확보 방안 및 각 노드의 데이터가 동등함을 보장할 수 있는 동기성 확보 방안을 제시해야 함 - 원장의 백업 및 복구 방안을 제시해야 함 ○ 스마트계약을 개발할 수 있는 환경(IDE)을 제공해야 함 <ul style="list-style-type: none"> - 스마트계약의 개발부터 배포까지의 형상관리 및 테스트 방안을 제시해야 함 - 스마트계약의 악성코드 검출 기능/도구를 제공해야 함 ○ 분산원장과의 인터페이스 및 dAPP개발을 위한 Node API 및 SDK를 제공해야 함 ○ 기타 서비스 운영에 필요한 기타 모듈을 제공해야 함

요구사항 정의	외부정보 인터페이스(시스템 연계)
요구사항 상세설명	<ul style="list-style-type: none"> ○ 외부정보 인터페이스(시스템 연계) 표준 수립 및 검증된 표준 인터페이스를 적용(정확성, 무결성, 정합성 검증 필요) ○ 연계 대상기관과의 인터페이스 정합성을 위한 기술을 지원해야 함 ○ 내부 연계, 외부 연계별로 관리 방안을 제시해야 함 ○ 송·수신 메시지에 대한 암호·복호화 방안을 제시해야 함 ○ 향후 연계기관 확대를 고려한 구축 방안을 마련해야 함 ※ 전담기관(KISA)와 사업자(제안사) 간 협의한 후 확정해야 함

(나) 데이터이력추적 공동인프라 성능 요구사항 명세서

요구사항 정의	외부정보 인터페이스(시스템 연계)
요구사항 상세설명	<ul style="list-style-type: none"> ○ 외부정보 인터페이스(시스템 연계) 표준 수립 및 검증된 표준 인터페이스를 적용(정확성, 무결성, 정합성 검증 필요) ○ 연계 대상기관과의 인터페이스 정합성을 위한 기술을 지원해야 함 ○ 내부 연계, 외부 연계별로 관리 방안을 제시해야 함 ○ 송·수신 메시지에 대한 암호·복호화 방안을 제시해야 함 ○ 향후 연계기관 확대를 고려한 구축 방안을 마련해야 함 ※ 전담기관(KISA)와 사업자(제안사) 간 협의한 후 확정해야 함

(다) 데이터이력추적 공동인프라 보안 요구사항 명세서

요구사항 정의	DB 및 오프체인 보안 요구사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구축, 정책설정, 권한설정 등 보안 준수사항을 고려하여 설계/지원해야 함 - 블록체인에 수록되는 개인정보, 민감정보 등에 대해 오프체인 기법을 통한 저장·관리해야 함 ○ 오프체인 성능검증 및 보완조치를 수행해야 함 ○ 암호화 정책, 비밀키 관리, 로그 관리, 운영관리 등 방안을 마련해야 함
요구사항 정의	개인정보 암호화 처리 방안 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 개인정보 암호화 방식은 API 방식으로 구현해야 함 ○ 암호화 대상은 고유식별정보(주민번호, 외국인번호, 여권번호 등, 이하 “주민번호”), 패스워드 등이며 향후 확장성을 고려하여 구축 ※ 암호화 알고리즘은 전담기관(KISA)과 사업 추진 시 협의 후 결정 ○ 외부 데이터 연계 시 암호화 처리 방안 제시해야 함
요구사항 정의	ISMS-P 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ ISMS-P를 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함
요구사항 정의	클라우드 인증(CSAP) 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 인증을 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

(라) 데이터이력추적 공동인프라 테스트 요구사항 명세서

요구사항 정의	데이터이력추적 공동인프라 테스트 계획 수립에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트, 통합테스트, 성능테스트를 진행해야 함 ○ 테스트 이용자별 테스트 시나리오, 단계별 수행방법, 수행절차, 참여조직 및 역할, 점검사항, 테스트일정, 시험환경 및 평가 기준을 구체적으로 수립 및 제시해야 함 ○ 내·외부시스템 인터페이스 환경 및 데이터 연계 테스트는 테스트 데이터를 사용하여 진행해야 함

요구사항 정의	데이터이력추적 공동인프라 단위테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트의 범위, 수행절차, 조직, 일정, 시험환경 및 평가기준을 구체적으로 수립해야 함 ○ 단위테스트 시나리오별, 처리 절차, 수행데이터, 예상결과 등을 사전에 정의해야 함 <ul style="list-style-type: none"> - 결함유형 분석(결함발생건수, 결함비율) - 결함발견 추세분석(테스트일시, 발견결함 수) - 테스트 커버리지

요구사항 정의	데이터이력추적 공동인프라 통합테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 통합테스트 시나리오 별 단위테스트가 완료된 프로그램 대상으로 다음 사항을 검증해야 함 <ul style="list-style-type: none"> - 기능, 성능 등의 요구사항 및 설계사항 충족여부를 검증해야 함 - 기능의 정상적 수행여부를 검증해야 함 - 기능수행 후의 결과가 사전에 예측된 결과와 일치하는지를 검증해야 함 - 접근권한 및 업무 권한에 대한 적절성을 검증해야 함 - 연계 및 이를 포함하는 업무흐름을 검증해야 함 - 대외기관 연계 및 업무 흐름을 검증해야 함 - 결함 분석 및 원인 추적을 통해 결함을 제거해야 함

(마) 데이터이력추적 공동인프라 품질 요구사항 명세서

요구사항 정의	데이터이력추적 공동인프라 품질보증 일반사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 품질보증의 범위, 품질보증을 위한 조직, 절차, 점검방법 등을 제시하여야 함 <ul style="list-style-type: none"> - 품질관리를 위한 제반 절차 및 산출물을 사업수행계획서에 상세하게 기술해야 함 - 품질 또는 성능상의 문제 발생 시 성능 테스트 및 분석결과를 제시하고 개선해야 함 - 품질향상을 위한 전담기관(KISA)의 요구사항이 있을 경우 이를 검토하여 보완해야 함 - 품질관리 조직과 운영 절차를 구체적으로 제시하고 준수해야 함

요구사항 정의	데이터이력추적 공동인프라 기능 구현 정확성
요구사항 상세설명	<ul style="list-style-type: none"> ○ 서비스에서 제공하기로 한 요구사항을 모두 제공해야 함 ○ 테스트를 통해 예상된 평가가 도출되었을 경우 기능 요구사항을 만족한 것으로 판단함

요구사항 정의	데이터이력추적 공동인프라 결함의 발견과 발견된 결함의 조치
요구사항 상세설명	<ul style="list-style-type: none"> ○ 테스트 기간 동안 발견된 결함 수를 측정하며, 결함 발생률이 기대수준 이상이거나 중대 결함이 발생한 경우 서비스 오픈 시점을 연기하거나 보완 대책을 즉시 수립해야 함 ○ 테스트 기간 동안 발견된 결함은 100% 조치해야 함

요구사항 정의	데이터이력추적 공동인프라 장애 발생에 따른 요구 및 신속한 복구 구현
요구사항 상세설명	<ul style="list-style-type: none"> ○ 사업자(제안사)는 장애발생 시 즉시 장애복구 조치에 임하여야 하며, 장애복구 조치로 해결이 불가능한 문제에 대해서는 4시간 이내 전문인력이 도착하여 정상복구를 위한 추가 조치를 수행해야 함 ○ 신속한 장애대응을 위하여 백업절차를 마련해야 함 ○ 장애 발생 처리 완료 후 장애 조치 보고서는 48시간 이내 제출해야 함

(바) 데이터이력추적 공동인프라 데이터 요구사항 명세서

요구사항 정의	데이터베이스 설계 표준화 지침 준수
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구조 설계는 관련 서비스 처리 절차를 반영하여 표준화하고 향후 변동에 따른 확장성을 고려해야 함 <ul style="list-style-type: none"> - 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 DB 설계 ○ 향후 시스템 확장성 등을 고려하여 블록체인 데이터를 정의해야 함 <ul style="list-style-type: none"> - 블록체인 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 블록체인 데이터를 정의해야 함

(4) 데이터진본확인 공동인프라의 공통요구사항

- (공통요구사항) 블록체인 네트워크 내 저장되는 정보들은 공공기관에서 관리하는 개인의 비밀 정보가 아닌 공개 가능한 정보로 제한된다. 공개 가능한 정보들은 개인정보와의 연결성을 위하여 해시 함수, 암호화 등의 암호학적 도구를 사용하여야 한다. K-BTF 공동인프라를 활용하여 공개 가능한 정보를 블록체인에 등록하면 블록체인 내 트랜잭션 형태로 정보는 저장되며, 추후 타 기관에서 관련 정보에 대한 위·변조 유무를 파악하고자 하는 경우 블록체인에 저장된 정보를 가져온 후 검증 과정을 가진다.

- (주요 기능) 데이터진본확인 공동인프라를 구성하기 위해서는 아래와 같은 기능이 요구된다.

기능	기능 설명
공개 정보 등록	네트워크 풀 내 공개 정보를 등록하는 기능이다. 등록되는 정보는 기관에서 관리하는 이용자(국민)의 개인 정보를 노출시키지 않는다.
공개 정보 반환	네트워크 풀 내 저장된 특정 공개 정보를 반환받는 기능이다.
공개 정보 검증	K-BTF로부터 받은 공개 정보에 대한 유효성 검증을 수행하는 기능이다. 이용자(국민)으로부터 정보를 받아 유효성을 검증한다.

표 17. 데이터진본확인 주요 기능

(가) 데이터진본확인 공동인프라 공통 요구사항 명세서

요구사항 정의	클라우드 기반 분산신원 공동인프라 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 및 컨테이너 기반 개발·검증환경 구축해야 함 <ul style="list-style-type: none"> - 개발 및 검증 환경 구축 일정 계획을 수립해야 함 - 소요자원(VM, vCPU, Memory, Network 등)을 검토해야 함 - 개발 및 검증 환경 구성 방안을 제시해야 함 - 효율적인 자원 운영 관리와 고가용성(HA) 확보 방안 제시해야 함 - 테스트를 위한 구성 변경 및 자원 할당 계획을 수립해야 함 ○ 시스템 아키텍처 설계와 구현 결과물의 정합성을 검증해야 함
요구사항 정의	데이터진본확인 공동인프라 이용포털(대시보드) 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 회원 관리, 관리자 관리 등 서비스를 제공해야 함 ○ 관리자 관리 <ul style="list-style-type: none"> - 관리자(계정) 가입/승인/조회 및 상태 관리 - 관리자 계정 삭제 - 시스템 접근정보 이력관리 등 ○ 관리시스템 대시보드 <ul style="list-style-type: none"> - 관리시스템 메인 대시보드 - 이용자 관련 각종 현황 - 분산신원 관련 각종 현황 - 데이터진본확인 공동인프라 관련 각종 현황 - 디지털 지갑서비스 관련 각종 현황

요구사항 정의	데이터진본확인 공동인프라 모듈 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 데이터진본확인 기능 <ul style="list-style-type: none"> - 데이터진본 Asset 생성/민팅 - 데이터진본 Asset 정보 조회/업데이트 - 데이터진본 Ownership 이전/조회 - 데이터진본 전체 리스트 Batch 조회 ○ 데이터 유효성 기능 <ul style="list-style-type: none"> - 공개 정보 등록 - 공개 정보 반환 - 공개 정보 검증

요구사항 정의	분산원장 규격
요구사항 상세설명	<ul style="list-style-type: none"> ○ 분산원장 무결성 확보해야 함 <ul style="list-style-type: none"> - 원장 무결성 확보 방안 및 각 노드의 데이터가 동등함을 보장할 수 있는 동기성 확보 방안을 제시해야 함 - 원장의 백업 및 복구 방안을 제시해야 함 ○ 스마트계약을 개발할 수 있는 환경(IDE)을 제공해야 함 <ul style="list-style-type: none"> - 스마트계약의 개발부터 배포까지의 형상관리 및 테스트 방안을 제시해야 함 - 스마트계약의 악성코드 검출 기능/도구를 제공해야 함 ○ 분산원장과의 인터페이스 및 dAPP개발을 위한 Node API 및 SDK를 제공해야 함 ○ 기타 서비스 운영에 필요한 기타 모듈을 제공해야 함

요구사항 정의	외부정보 인터페이스(시스템 연계)
요구사항 상세설명	<ul style="list-style-type: none"> ○ 외부정보 인터페이스(시스템 연계) 표준 수립 및 검증된 표준 인터페이스를 적용(정확성, 무결성, 정합성 검증 필요) ○ 연계 대상기관과의 인터페이스 정합성을 위한 기술을 지원해야 함 ○ 내부 연계, 외부 연계별로 관리 방안을 제시해야 함 ○ 송·수신 메시지에 대한 암호·복호화 방안을 제시해야 함 ○ 향후 연계기관 확대를 고려한 구축 방안을 마련해야 함 ※ 전담기관(KISA)와 사업자(제안사) 간 협의한 후 확정해야 함

(나) 데이터진본확인 공동인프라 성능 요구사항 명세서

요구사항 정의	데이터진본확인 공동인프라 성능 측정 및 목표 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 다수의 이용자가 안정적으로 분산신원 공통서비스를 이용할 수 있는 성능지표의 목표 수치를 제시해야 함 <ul style="list-style-type: none"> - 성능지표는 전 주기(DID 생성, 조회, 수정, 삭제, VC·VP 발행, 제출, 검증 등) 별 트랜잭션 처리속도(TPS), 평균 응답시간(Latency), 블록 확장 시간(Confirm Time), 데이터 정합성(Data Consistency)임 ※ 성능지표는 추후 전담기관(KISA)과 협의에 따라 변경될 수 있음 ○ 사업 진행과정에서 제시한 목표 수치를 충족하지 못할 경우 개선 방안을 제시하고 목표치를 달성해야 함

(다) 데이터진본확인 공동인프라 보안 요구사항 명세서

요구사항 정의	DB 및 오프체인 보안 요구사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구축, 정책설정, 권한설정 등 보안 준수사항을 고려하여 설계/지원해야 함 <ul style="list-style-type: none"> - 블록체인에 수록되는 개인정보, 민감정보 등에 대해 오프체인 기법을 통한 저장·관리해야 함 ○ 오프체인 성능검증 및 보완조치를 수행해야 함 ○ 암호화 정책, 비밀키 관리, 로그 관리, 운영관리 등 방안을 마련해야 함

요구사항 정의	개인정보 암호화 처리 방안 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 개인정보 암호화 방식은 API 방식으로 구현해야 함 ○ 암호화 대상은 고유식별정보(주민번호, 외국인번호, 여권번호 등, 이하 “주민번호”),패스워드 등이며 향후 확장성을 고려하여 구축 ※ 암호화 알고리즘은 전담기관(KISA)과 사업 추진 시 협의 후 결정 ○ 외부 데이터 연계 시 암호화 처리 방안 제시해야 함

요구사항 정의	ISMS-P 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ ISMS-P를 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

요구사항 정의	클라우드 인증(CSAP) 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 인증을 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

(라) 데이터진본확인 공동인프라 테스트 요구사항 명세서

요구사항 정의	데이터진본확인 공동인프라 테스트 계획 수립에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트, 통합테스트, 성능테스트를 진행해야 함 ○ 테스트 사용자별 테스트 시나리오, 단계별 수행방법, 수행절차, 참여조직 및 역할, 점검사항, 테스트일정, 시험환경 및 평가 기준을 구체적으로 수립 및 제시해야 함 ○ 내·외부시스템 인터페이스 환경 및 데이터 연계 테스트는 테스트 데이터를 사용하여 진행해야 함
요구사항 정의	데이터진본확인 공동인프라 단위테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트의 범위, 수행절차, 조직, 일정, 시험환경 및 평가기준을 구체적으로 수립해야 함 ○ 단위테스트 시나리오별, 처리 절차, 수행데이터, 예상결과 등을 사전에 정의해야 함 <ul style="list-style-type: none"> - 결함유형 분석(결함발생건수, 결함비율) - 결함발견 추세분석(테스트일시, 발견결함 수) - 테스트 커버리지
요구사항 정의	데이터진본확인 공동인프라 통합테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 통합테스트 시나리오 별 단위테스트가 완료된 프로그램 대상으로 다음 사항을 검증해야 함 <ul style="list-style-type: none"> - 기능, 성능 등의 요구사항 및 설계사양 충족여부를 검증해야 함 - 기능의 정상적 수행여부를 검증해야 함 - 기능수행 후의 결과가 사전에 예측된 결과와 일치하는지를 검증해야 함 - 접근권한 및 업무 권한에 대한 적절성을 검증해야 함 - 연계 및 이를 포함하는 업무흐름을 검증해야 함 - 대외기관 연계 및 업무 흐름을 검증해야 함 - 결함 분석 및 원인 추적을 통해 결함을 제거해야 함

(마) 데이터진본확인 공동인프라 품질 요구사항 명세서

요구사항 정의	데이터진본확인 공동인프라 품질보증 일반사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 품질보증의 범위, 품질보증을 위한 조직, 절차, 점검방법 등을 제시하여야 함 - 품질관리를 위한 제반 절차 및 산출물을 사업수행계획서에 상세하게 기술해야 함 - 품질 또는 성능상의 문제 발생 시 성능 테스트 및 분석결과를 제시하고 개선해야 함 - 품질향상을 위한 전담기관(KISA)의 요구사항이 있을 경우 이를 검토하여 보완해야 함 - 품질관리 조직과 운영 절차를 구체적으로 제시하고 준수해야 함
요구사항 정의	데이터진본확인 공동인프라 기능 구현 정확성
요구사항 상세설명	<ul style="list-style-type: none"> ○ 서비스에서 제공하기로 한 요구사항을 모두 제공해야 함 ○ 테스트를 통해 예상된 평가가 도출되었을 경우 기능 요구사항을 만족한 것으로 판단함
요구사항 정의	데이터진본확인 공동인프라 결함의 발견과 발견된 결함의 조치
요구사항 상세설명	<ul style="list-style-type: none"> ○ 테스트 기간 동안 발견된 결함 수를 측정하며, 결함 발생률이 기대수준 이상이거나 중대 결함이 발생한 경우 서비스 오픈 시점을 연기하거나 보완 대책을 즉시 수립해야 함 ○ 테스트 기간 동안 발견된 결함은 100% 조치해야 함
요구사항 정의	데이터진본확인 공동인프라 장애 발생에 따른 요구 및 신속한 복구 구현
요구사항 상세설명	<ul style="list-style-type: none"> ○ 사업자(제안사)는 장애발생 시 즉시 장애복구 조치에 임하여야 하며, 장애복구 조치로 해결이 불가능한 문제에 대해서는 4시간 이내 전문인력이 도착하여 정상복구를 위한 추가 조치를 수행해야 함 ○ 신속한 장애대응을 위하여 백업절차를 마련해야 함 ○ 장애 발생 처리 완료 후 장애 조치 보고서는 48시간 이내 제출해야 함

(바) 데이터진본확인 공동인프라 데이터 요구사항 명세서

요구사항 정의	데이터베이스 설계 표준화 지침 준수
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구조 설계는 관련 서비스 처리 절차를 반영하여 표준화하고 향후 변동에 따른 확장성을 고려해야 함 <ul style="list-style-type: none"> - 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 DB 설계 ○ 향후 시스템 확장성 등을 고려하여 블록체인 데이터를 정의해야 함 <ul style="list-style-type: none"> - 블록체인 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 블록체인 데이터를 정의해야 함

(5) 직접구축(BaaS) 공통요구사항

- (공통요구사항) 직접구축(BaaS) 공통요구사항이란 블록체인 기술의 실행 및 기능 작동을 위한 구성요소의 집합과 이를 활용하고 개선하기 위한 솔루션 및 제반 환경 등으로 정의할 수 있다. 직접구축(BaaS)의 범위는 블록체인 네트워크를 구성하기 위한 노드 자원 뿐만 아니라, 분산 어플리케이션(DApp) 개발 도구, 보안, 모니터링 등 다양한 관련 기술의 지원 여부를 포함한다. 직접구축(BaaS)는 공공기관에게 클라우드 형태로 블록체인 서비스를 제공하여 별도 구축 과정 없이 쉽고 빠르게 서비스를 도입하고 운영할 수 있도록 한다.

(가) 직접구축(BaaS) 공통요구사항 명세서

요구사항 정의	직접구축(BaaS) 클라우드 기반 환경
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 및 컨테이너 기반 개발·검증환경 구축해야 함 <ul style="list-style-type: none"> - 개발 및 검증 환경 구축 일정 계획을 수립해야 함 - 소요자원(VM, vCPU, Memory, Network 등)을 검토해야 함 - 개발 및 검증 환경 구성 방안을 제시해야 함 - 효율적인 자원 운영 관리와 고가용성(HA) 확보 방안 제시해야 함 - 테스트를 위한 구성 변경 및 자원 할당 계획을 수립해야 함 ○ 시스템 아키텍처 설계와 구현 결과물의 정합성을 검증해야 함

요구사항 정의	직접구축(BaaS) 이용포털(대시보드) 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 회원 관리, 관리자 관리 등 서비스를 제공해야 함 ○ 관리자 관리 <ul style="list-style-type: none"> - 관리자(계정) 가입/승인/조회 및 상태 관리 - 관리자 계정 삭제 - 시스템 접근정보 이력관리 등 ○ 관리시스템 대시보드 <ul style="list-style-type: none"> - 관리시스템 메인 대시보드 - 이용자 관련 각종 현황 - 분산신원 관련 각종 현황 - 블록체인플랫폼 공통인프라 관련 각종 현황 - 디지털 지갑서비스 관련 각종 현황

요구사항 정의	직접구축(BaaS) 모듈 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 웹 UI/UX 기반의 유저 인터페이스를 제공해야 함. ○ 블록체인 코어 기능 모듈, 블록체인 서비스에 필요한 모듈을 제작하여 제공해야함 ○ 블록체인 연계 모듈 <ul style="list-style-type: none"> - 설정/구축/관리 기능 - 스마트컨트랙트 조회/배포/업그레이드 기능 - API Resolver를 통한 스마트 컨트랙트 연계 및 API Doc 제공 - 외부 IPFS(Amazon S3, Pinata, OpenSea 등) 연계 기능 ○ 블록체인 인프라 관리 모듈 <ul style="list-style-type: none"> - IaC 플랫폼 기반 리소스/자원 할당 - VLAN 기반 가상 네트워크 구성 ○ 분산신원 모듈 <ul style="list-style-type: none"> - 분산신원, VC, VP 발행/인증 모듈 - 분산신원 기능 연계를 위한 정규화된 API 및 Doc 제공 ○ 토큰 연계 모듈 <ul style="list-style-type: none"> - 다양한 인터페이스를 준수하는 토큰 및 스마트 컨트랙트 연계 - 일반적인 토큰에서부터, NFT/STO 등 다양한 인터페이스 맞춤형 API 제공 ○ 디지털인증서 모듈 <ul style="list-style-type: none"> - 스마트계약 배포 모듈 - 디지털인증서 생성/조회/변경/소각(폐기) 모듈 - 디지털인증서 공유 모듈 - 디지털인증서 소유권확인/소유권 이전 및 이전 승인 모듈 - 타인의 디지털인증서 조회/변경관리 모듈 ○ K-BTF 핵심서비스 운영에 필요한 기타 모듈 제공

요구사항 정의	분산원장 규격
요구사항 상세설명	<ul style="list-style-type: none"> ○ 분산원장 무결성 확보해야 함 <ul style="list-style-type: none"> - 원장 무결성 확보 방안 및 각 노드의 데이터가 동등함을 보장할 수 있는 동기성 확보 방안을 제시해야 함 - 원장의 백업 및 복구 방안을 제시해야 함 ○ 스마트 계약을 개발할 수 있는 환경(IDE)을 제공해야 함 <ul style="list-style-type: none"> - 스마트 계약의 개발부터 배포까지의 형상관리 및 테스트 방안을 제시해야 함 - 스마트 계약의 악성코드 검출 기능/도구를 제공해야 함 ○ 분산원장과의 인터페이스 및 dAPP개발을 위한 Node API 및 SDK를 제공해야 함 ○ 기타 서비스 운영에 필요한 기타 모듈을 제공해야 함

요구사항 정의	외부정보 인터페이스(시스템 연계)
요구사항 상세설명	<ul style="list-style-type: none"> ○ 외부정보 인터페이스(시스템 연계) 표준 수립 및 검증된 표준 인터페이스를 적용(정확성, 무결성, 정합성 검증 필요) ○ 연계 대상기관과의 인터페이스 정합성을 위한 기술을 지원해야 함 ○ 내부 연계, 외부 연계별로 관리 방안을 제시해야 함 ○ 송·수신 메시지에 대한 암호·복호화 방안을 제시해야 함 ○ 향후 연계기관 확대를 고려한 구축 방안을 마련해야 함 ※ 전담기관(KISA)와 사업자(제안사) 간 협의한 후 확정해야 함

(나) 직접구축(BaaS) 성능 요구사항 명세서

요구사항 정의	직접구축(BaaS) 성능 측정 및 목표 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 다수의 이용자가 안정적으로 분산신원 공통서비스를 이용할 수 있는 성능지표의 목표 수치를 제시해야 함 <ul style="list-style-type: none"> - 성능지표는 전 주기(DID 생성, 조회, 수정, 삭제, VC·VP 발행, 제출, 검증 등) 별 트랜잭션 처리속도(TPS), 평균 응답시간(Latency), 블록 확장 시간(Confirm Time), 데이터 정합성(Data Consistency)임 ※ 성능지표는 추후 전담기관(KISA)과 협의에 따라 변경될 수 있음 ○ 사업 진행과정에서 제시한 목표 수치를 충족하지 못할 경우 개선 방안을 제시하고 목표치를 달성해야 함

(다) 직접구축(BaaS) 보안 요구사항 명세서

요구사항 정의	DB 및 오프체인 보안 요구사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구축, 정책설정, 권한설정 등 보안 준수사항을 고려하여 설계/지원해야 함 - 블록체인에 수록되는 개인정보, 민감정보 등에 대해 오프체인 기법을 통한 저장·관리해야 함 ○ 오프체인 성능검증 및 보완조치를 수행해야 함 ○ 암호화 정책, 비밀키 관리, 로그 관리, 운영관리 등 방안을 마련해야 함

요구사항 정의	개인정보 암호화 처리 방안 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 개인정보 암호화 방식은 API 방식으로 구현해야 함 ○ 암호화 대상은 고유식별정보(주민번호, 외국인번호, 여권번호 등, 이하 “주민번호”), 패스워드 등이며 향후 확장성을 고려하여 구축 ※ 암호화 알고리즘은 전담기관(KISA)과 사업 추진 시 협의 후 결정 ○ 외부 데이터 연계 시 암호화 처리 방안 제시해야 함

요구사항 정의	ISMS-P 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ ISMS-P를 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

요구사항 정의	클라우드 인증(CSAP) 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 인증을 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

(라) 직접구축(BaaS) 테스트 요구사항 명세서

요구사항 정의	직접구축(BaaS) 테스트 계획 수립에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트, 통합테스트, 성능테스트를 진행해야 함 ○ 테스트 사용자별 테스트 시나리오, 단계별 수행방법, 수행절차, 참여조직 및 역할, 점검사항, 테스트일정, 시험환경 및 평가 기준을 구체적으로 수립 및 제시해야 함 ○ 내·외부시스템 인터페이스 환경 및 데이터 연계 테스트는 테스트 데이터를 사용하여 진행해야 함

요구사항 정의	직접구축(BaaS) 단위테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트의 범위, 수행절차, 조직, 일정, 시험환경 및 평가기준을 구체적으로 수립해야 함 ○ 단위테스트 시나리오별, 처리 절차, 수행데이터, 예상결과 등을 사전에 정의해야 함 <ul style="list-style-type: none"> - 결함유형 분석(결함발생건수, 결함비율) - 결함발견 추세분석(테스트일시, 발견결함 수) - 테스트 커버리지

요구사항 정의	직접구축(BaaS) 통합테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 통합테스트 시나리오 별 단위테스트가 완료된 프로그램 대상으로 다음 사항을 검증해야 함 <ul style="list-style-type: none"> - 기능, 성능 등의 요구사항 및 설계사양 충족여부를 검증해야 함 - 기능의 정상적 수행여부를 검증해야 함 - 기능수행 후의 결과가 사전에 예측된 결과와 일치하는지를 검증해야 함 - 접근권한 및 업무 권한에 대한 적절성을 검증해야 함 - 연계 및 이를 포함하는 업무흐름을 검증해야 함 - 대외기관 연계 및 업무 흐름을 검증해야 함 - 결함 분석 및 원인 추적을 통해 결함을 제거해야 함

(마) 직접구축(BaaS) 품질 요구사항 명세서

요구사항 정의	직접구축(BaaS) 품질보증 일반사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 품질보증의 범위, 품질보증을 위한 조직, 절차, 점검방법 등을 제시하여야 함 <ul style="list-style-type: none"> - 품질관리를 위한 제반 절차 및 산출물을 사업수행계획서에 상세하게 기술해야 함 - 품질 또는 성능상의 문제 발생 시 성능 테스트 및 분석결과를 제시하고 개선해야 함 - 품질향상을 위한 전담기관(KISA)의 요구사항이 있을 경우 이를 검토하여 보완해야 함 - 품질관리 조직과 운영 절차를 구체적으로 제시하고 준수해야 함

요구사항 정의	직접구축(BaaS) 기능 구현 정확성
요구사항 상세설명	<ul style="list-style-type: none"> ○ 서비스에서 제공하기로 한 요구사항을 모두 제공해야 함 ○ 테스트를 통해 예상된 평가가 도출되었을 경우 기능 요구사항을 만족한 것으로 판단함

요구사항 정의	직접구축(BaaS) 결함의 발견과 발견된 결함의 조치
요구사항 상세설명	<ul style="list-style-type: none"> ○ 테스트 기간 동안 발견된 결함 수를 측정하며, 결함 발생률이 기대수준 이상이거나 중대 결함이 발생한 경우 서비스 오픈 시점을 연기하거나 보완 대책을 즉시 수립해야 함 ○ 테스트 기간 동안 발견된 결함은 100% 조치해야 함

요구사항 정의	직접구축(BaaS) 장애 발생에 따른 요구 및 신속한 복구 구현
요구사항 상세설명	<ul style="list-style-type: none"> ○ 사업자(제안사)는 장애발생 시 즉시 장애복구 조치에 임하여야 하며, 장애복구 조치로 해결이 불가능한 문제에 대해서는 4시간 이내 전문인력이 도착하여 정상복구를 위한 추가 조치를 수행해야 함 ○ 신속한 장애대응을 위하여 백업절차를 마련해야 함 ○ 장애 발생 처리 완료 후 장애 조치 보고서는 48시간 이내 제출해야 함

(바) 직접구축(BaaS) 데이터 요구사항 명세서

요구사항 정의	데이터베이스 설계 표준화 지침 준수
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구조 설계는 관련 서비스 처리 절차를 반영하여 표준화하고 향후 변동에 따른 확장성을 고려해야 함 <ul style="list-style-type: none"> - 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 DB 설계 ○ 향후 시스템 확장성 등을 고려하여 블록체인 데이터를 정의해야 함 <ul style="list-style-type: none"> - 블록체인 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 블록체인 데이터를 정의해야 함

(6) 디지털 지갑 서비스의 공통요구사항

- (공통요구사항) K-BTF 공동인프라에서 디지털 지갑 서비스는 공공성을 위해서 이용자의 단말기에서 공개키, 비밀키, 분산신원 관련 정보, 디지털인증서 관련 정보 등의 안전한 저장 서비스를 제공한다. 이용자 비밀키는 블록체인 내 트랜잭션을 생성하기 위해서 필수적으로 보유하고 있어야 하기 때문에 비밀키의 분실은 블록체인 서비스 사용 불가의 문제로 이어진다. 개인의 비밀키 관리를 위해 디지털 지갑 서비스를 활용하여 비밀키의 관리를 투명하게 하고 암호학적 설계나 불법 사용에 대한 방지 대책도 필수적으로 포함해야 한다. 이용자는 비밀키를 분실하였을 때 디지털 지갑 서비스에서 제공하는 복구 기능으로 비밀키를 복구할 수 있어야 한다.
- (주요 기능) 위 내용을 종합하면 디지털 지갑 서비스는 다음과 같은 기능들이 필수적으로 요구되어야 한다.

기능	기능 설명
디지털 지갑 생성	새로운 지갑을 생성하는 기능으로 이는 내부적으로 공개키, 비밀키, 니모닉에 대한 생성을 의미한다. 다수의 지갑을 생성할 수 있도록 허용한다
디지털 지갑 복구	비밀키 혹은 니모닉을 통해 지갑을 복구하는 기능을 말한다.
비밀키 커스터디	지갑에 대한 암호키(비밀키, 니모닉) 관련 정보를 대신 보관해주는 기능이다.
디지털 지갑 활성화	사용하고자 하는 지갑을 활성화하여 블록체인에서 활성화한 지갑의 주소를 사용가능하도록 허용하는 기능이다.
디지털 지갑 비활성화	활성화된 지갑을 비활성화하여 네트워크 내 블록체인의 기능을 관련 지갑으로 사용하지 못하도록 하는 기능이다.
암호화	지갑과 관련한 해시 함수, 암호화, 서명 등의 암호학적 도구 기능을 제공한다.

표 18. 디지털 지갑 주요 기능

(가) 디지털 지갑 서비스 공통요구사항 명세서

요구사항 정의	디지털 지갑 모바일 앱(iOS, Android) 개발 및 배포
요구사항 상세설명	<ul style="list-style-type: none"> ○ 안드로이드용 앱 개발완료 후 구글 플레이 스토어에 정식 배포 ○ iOS(아이폰)용 앱 개발완료 후 애플 앱 스토어에 정식 배포 ○ Cross platform 앱 개발 <ul style="list-style-type: none"> - 앱은 API Gateway 인증 키를 앱 내에 보관하며, 이에 대한 각 스마트폰 OS가 제공하는 최신의 보안 기능 활용 및 최적화 필요 - 핀코드를 기본 제공하며, 핀코드 기반의 생체 인증 옵션으로 함께 제공 - 네이티브 앱 방식 또는 웹 앱 방식이 아닌 Cross platform 앱 방식으로 개발 ○ 모바일 앱 업데이트 배포 및 운영 관리 지원 <p>※ 앱 업데이트 배포 및 운영 관리 지원에 대한 세부 사항은 전담 기관(KISA)와 사전 협의</p>

요구사항 정의	디지털 지갑 생성·조회·변경·삭제·관리 모듈 개발
요구사항 상세설명	<ul style="list-style-type: none"> ○ 디지털 지갑은 생성·조회·변경·삭제(폐기)·복구·관리를 위한 기능을 제공해야 함 ○ 디지털 지갑 모바일 앱은 DID 공동플랫폼과 상호호환되어 신원 증명 기능을 제공해야 함 <ul style="list-style-type: none"> - 온라인·오프라인 환경에서 신원확인자가 사람인 경우 신분증의 진본성을 다양한 방법을 통해 증명해야 함 - VP 제출 시 선택적 제공(Selective disclosure) 기능을 제공해야 함 ○ 디지털 지갑 모바일 앱은 NFT 공동플랫폼과 상호호환되어 NFT 관련 기능을 제공해야 함 <ul style="list-style-type: none"> - NFT 발급신청, 진위확인 기능을 제공해야 함 - 계정주소를 이용하여 NFT 전송 및 트랜잭션 로그를 저장해야 함 ○ 디지털 지갑 모바일 앱은 필요에 따라 다양한 디바이스 인터페이스(NFC, Bluetooth, QR 등)를 활용한 VC/VP, NFT 정보제출 기능을 제공해야 함 <ul style="list-style-type: none"> - VC/VP 및 NFT 발급·제출·검증을 위한 기능을 제공해야 함 ○ 디지털 지갑 모바일 앱은 다양한 로그인 기능을 제공해야 함 <ul style="list-style-type: none"> - 소셜 로그인, 간편 로그인, 생체 인증 로그인 등 - 모바일에 생체인증 기능 없을 시, 초기 설정한 핀코드 사용 - 중요정보 제출·전송 시, 반드시 핀코드, 생체인증 등 이중 인증을 사용해야 함 ○ 디지털 지갑 모바일 앱은 일정시간 동안 사용자 액션이 없는 경우나 어플리케이션이 백그라운드로 내려가서 일정 시간이 경과하면 자동으로 잠겨야 함

요구사항 정의	디지털 지갑 모바일 앱 보안·관리·복구
요구사항 상세설명	<ul style="list-style-type: none"> ○ DID, NFT에 맞는 개인키 생성 지원과 보안 방안을 제공하여야함 ○ 개인키 복원 절차 수립하고 절차에 맞는 기능을 제공해야 함 ○ 디지털 지갑 외 다른 모바일 앱은 개인키 접근 불가 ○ 개인키 접근은 안전한 통신수단을 통해 전달/서명/검증하며 블록 체인 트랜잭션 서명과 함께 로그를 기록해야 함 <ul style="list-style-type: none"> - 휴대폰 도난/분실 시, 핀코드, 생체 인증을 통해 개인키 접근 불가하여야 함 ○ 모바일 앱 화면캡처방지 기능 <ul style="list-style-type: none"> - iOS, Android 화면 캡처 시 캡처 검출 메시지 표시 - 화면 캡처 시 중요정보는 노출되지 않도록 가려서 사진 저장

요구사항 정의	분산원장 규격
요구사항 상세설명	<ul style="list-style-type: none"> ○ 분산원장 무결성 확보해야 함 <ul style="list-style-type: none"> - 원장 무결성 확보 방안 및 각 노드의 데이터가 동등함을 보장할 수 있는 동기성 확보 방안을 제시해야 함 - 원장의 백업 및 복구 방안을 제시해야 함 ○ 스마트계약을 개발할 수 있는 환경(IDE)을 제공해야 함 <ul style="list-style-type: none"> - 스마트계약의 개발부터 배포까지의 형상관리 및 테스트 방안을 제시해야 함 - 스마트계약의 악성코드 검출 기능/도구를 제공해야 함 ○ 분산원장과의 인터페이스 및 dAPP개발을 위한 Node API 및 SDK를 제공해야 함 ○ 기타 서비스 운영에 필요한 기타 모듈을 제공해야 함

요구사항 정의	외부정보 인터페이스(시스템 연계)
요구사항 상세설명	<ul style="list-style-type: none"> ○ 외부정보 인터페이스(시스템 연계) 표준 수립 및 검증된 표준 인터페이스를 적용(정확성, 무결성, 정합성 검증 필요) ○ 연계 대상기관과의 인터페이스 정합성을 위한 기술을 지원해야 함 ○ 내부 연계, 외부 연계별로 관리 방안을 제시해야 함 ○ 송·수신 메시지에 대한 암호·복호화 방안을 제시해야 함 ○ 향후 연계기관 확대를 고려한 구축 방안을 마련해야 함 ※ 전달기관(KISA)와 사업자(제안사) 간 협의한 후 확정해야 함

(나) 디지털 지갑 서비스 성능 요구사항 명세서

요구사항 정의	디지털 지갑 성능 측정 및 목표제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 디지털 지갑은 이용자가 DID, NFT를 성능이 저하되지 않도록 이용할 수 있는 성능지표 수치를 제시해야 함 <ul style="list-style-type: none"> - 디지털 지갑 성능지표는 DID·NFT 공동플랫폼 및 서비스 사이의 트랜잭션 처리속도(TPS), 평균 응답시간(Latency), 블록 확장 시간(Confirm Time), 데이터 정합성(Data Consistency)임 ※ 성능지표는 추후 전달기관(KISA)과 협의에 따라 변경될 수 있음 ○ 사업자(제안사)는 사업 진행과정에서 제시한 목표 수치를 충족하지 못할 경우 개선 방안을 제시하고 목표치를 달성해야 함

(다) 디지털 지갑 서비스 보안 요구사항 명세서

요구사항 정의	DB 및 오프체인 보안 요구사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구축, 정책설정, 권한설정 등 보안 준수사항을 고려하여 설계/지원해야 함 - 블록체인에 수록되는 개인정보, 민감정보 등에 대해 오프체인 기법을 통한 저장·관리해야 함 ○ 오프체인 성능검증 및 보완조치를 수행해야 함 ○ 암호화 정책, 비밀키 관리, 로그 관리, 운영관리 등 방안을 마련해야 함
요구사항 정의	개인정보 암호화 처리 방안 제시
요구사항 상세설명	<ul style="list-style-type: none"> ○ 개인정보 암호화 방식은 API 방식으로 구현해야 함 ○ 암호화 대상은 고유식별정보(주민번호, 외국인번호, 여권번호 등, 이하 “주민번호”), 패스워드 등이며 향후 확장성을 고려하여 구축 ※ 암호화 알고리즘은 전담기관(KISA)과 사업 추진 시 협의 후 결정 ○ 외부 데이터 연계 시 암호화 처리 방안 제시해야 함
요구사항 정의	ISMS-P 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ ISMS-P를 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함
요구사항 정의	클라우드 인증(CSAP) 취득 계획 및 대응 방안
요구사항 상세설명	<ul style="list-style-type: none"> ○ 클라우드 인증을 취득하기 위한 구체적인 추진계획, 각 단계별 추진계획, 예상완료 시점 등을 제시해야 함 ○ 사업기간 내 미완수될 경우, 전담기관(KISA) 대응방안을 필수로 제시하고 계획에 따라 이행해야 함

(라) 디지털 지갑 서비스 테스트 요구사항 명세서

요구사항 정의	디지털 지갑 서비스 테스트 계획 수립에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트, 통합테스트, 성능테스트를 진행해야 함 ○ 테스트 이용자별 테스트 시나리오, 단계별 수행방법, 수행절차, 참여조직 및 역할, 점검사항, 테스트일정, 시험환경 및 평가 기준을 구체적으로 수립 및 제시해야 함 ○ 내·외부시스템 인터페이스 환경 및 데이터 연계 테스트는 테스트 데이터를 사용하여 진행해야 함

요구사항 정의	디지털 지갑 서비스 단위테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 단위테스트의 범위, 수행절차, 조직, 일정, 시험환경 및 평가기준을 구체적으로 수립해야 함 ○ 단위테스트 시나리오별, 처리 절차, 수행데이터, 예상결과 등을 사전에 정의해야 함 <ul style="list-style-type: none"> - 결함유형 분석(결함발생건수, 결함비율) - 결함발견 추세분석(테스트일시, 발견결함 수) - 테스트 커버리지

요구사항 정의	디지털 지갑 서비스 통합테스트에 관한 사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 통합테스트 시나리오 별 단위테스트가 완료된 프로그램 대상으로 다음 사항을 검증해야 함 <ul style="list-style-type: none"> - 기능, 성능 등의 요구사항 및 설계사항 충족여부를 검증해야 함 - 기능의 정상적 수행여부를 검증해야 함 - 기능수행 후의 결과가 사전에 예측된 결과와 일치하는지를 검증해야 함 - 접근권한 및 업무 권한에 대한 적절성을 검증해야 함 - 연계 및 이를 포함하는 업무흐름을 검증해야 함 - 대외기관 연계 및 업무 흐름을 검증해야 함 - 결함 분석 및 원인 추적을 통해 결함을 제거해야 함

(마) 디지털 지갑 서비스 품질 요구사항 명세서

요구사항 정의	디지털 지갑 서비스 품질보증 일반사항
요구사항 상세설명	<ul style="list-style-type: none"> ○ 품질보증의 범위, 품질보증을 위한 조직, 절차, 점검방법 등을 제시하여야 함 <ul style="list-style-type: none"> - 품질관리를 위한 제반 절차 및 산출물을 사업수행계획서에 상세하게 기술해야 함 - 품질 또는 성능상의 문제 발생 시 성능 테스트 및 분석결과를 제시하고 개선해야 함 - 품질향상을 위한 전담기관(KISA)의 요구사항이 있을 경우 이를 검토하여 보완해야 함 - 품질관리 조직과 운영 절차를 구체적으로 제시하고 준수해야 함

요구사항 정의	디지털 지갑 서비스 기능 구현 정확성
요구사항 상세설명	<ul style="list-style-type: none"> ○ 서비스에서 제공하기로 한 요구사항을 모두 제공해야 함 ○ 테스트를 통해 예상된 평가가 도출되었을 경우 기능 요구사항을 만족한 것으로 판단함

요구사항 정의	디지털 지갑 서비스 결함의 발견과 발견된 결함의 조치
요구사항 상세설명	<ul style="list-style-type: none"> ○ 테스트 기간 동안 발견된 결함 수를 측정하며, 결함 발생률이 기대수준 이상이거나 중대 결함이 발생한 경우 서비스 오픈 시점을 연기하거나 보완 대책을 즉시 수립해야 함 ○ 테스트 기간 동안 발견된 결함은 100% 조치해야 함

요구사항 정의	디지털 지갑 서비스 장애 발생에 따른 요구 및 신속한 복구 구현
요구사항 상세설명	<ul style="list-style-type: none"> ○ 사업자(제안사)는 장애발생 시 즉시 장애복구 조치에 임하여야 하며, 장애복구 조치로 해결이 불가능한 문제에 대해서는 4시간 이내 전문인력이 도착하여 정상복구를 위한 추가 조치를 수행해야 함 ○ 신속한 장애대응을 위하여 백업절차를 마련해야 함 ○ 장애 발생 처리 완료 후 장애 조치 보고서는 48시간 이내 제출해야 함

(바) 디지털 지갑 서비스 데이터 요구사항 명세서

요구사항 정의	데이터베이스 설계 표준화 지침 준수
요구사항 상세설명	<ul style="list-style-type: none"> ○ DB 구조 설계는 관련 서비스 처리 절차를 반영하여 표준화하고 향후 변동에 따른 확장성을 고려해야 함 <ul style="list-style-type: none"> - 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 DB 설계 ○ 향후 시스템 확장성 등을 고려하여 블록체인 데이터를 정의해야 함 <ul style="list-style-type: none"> - 블록체인 데이터 정합성을 유지하면서 성능을 저하시키지 않도록 블록체인 데이터를 정의해야 함

부록 5. K-BTF 시험검증체계 마련

1. K-BTF 시험검증체계 마련을 위한 현황 분석

(1) K-BTF 시험검증체계 마련을 위한 검토 대상 선정

- K-BTF 시험검증체계 마련을 위해 ① ISMS-P 인증제도 이용 방안, ② 클라우드보안인증제도(CSAP) 이용 방안, ③ 행안부 행정기관 및 공공기관 정보시스템 구축 운영 지침 이용 방안, ④ 해외 시험검증체계 준용 방안의 4가지 방안을 검토하였다.

(2) K-BTF 시험검증체계 마련을 위한 4가지 검증체계 분석

(가) ISMS-P 인증체계

- ISMS-P 인증체계는 국내 정보보안 및 개인정보보호 관련 인증체계로 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조 및 개인정보 보호법 제32조의2에 의거하고 있으며 정보보호 및 개인정보보호 관리체계 인증을 활용하여 K-BTF 시험검증체계의 1. 관리체계 수립 및 운영, 2. 보호대책 요구사항, 3. 개인정보처리 단계별 요구사항 항목별 시험인증체계를 구성할 수 있다.
- 1. 관리체계 수립 및 운영 인증항목은 관리체계 기반 마련, 위험관리, 관리체계 운영, 관리체계 점검 및 개선에 대한 16가지 분야로 구성되어 있다. K-BTF 인증 시 관리체계 수립 및 운영에 모두 적용 가능한 항목으로 구성된다.
- 2. 보호대책 요구사항 항목은 관리적, 물리적 기술적 보안과 관련된 정책,조직, 자산관리, 인적보안, 외부자 보안, 물리 보안, 인증 및 권한관리, 접근통제, 암호화 적용, 정보시스템 도입 및 개발 보안, 시스템 및 서비스 운영 관리, 시스템 및 서비스 보안 관리, 사고 예방 및 대응, 재해 복구를 포함하며 총 64개 분야로 구성된다. K-BTF 인증 시 적용 가능한 항목은 암호화 적용, 접근통제, 정보시스템 도입 및 개발 보안, 시스템 및 서비스 운영 관리, 시스템 및 서비스 보안 관리 등 소프트웨어, 인프라, 시스템, 네트워크와 관련된 기술 항목들의

활용이 가능하다.

- 3. 개인정보 처리단계별 요구사항 항목은 개인정보 수집시 보호조치, 개인정보 보유 및 이용시 보호조치, 개인정보 제공 시 보호조치, 개인정보 파기 시 보호조치, 정보주체권리 보호의 총 22개 분야로 구성된다. 개인정보보호 수집, 보유 및 이용시 및 제공 시의 점검분야를 활용하여 인증이 가능하다.

- ISMS-P 인증의 총 102개 인증항목을 기준을 만족하면 K-BTF 인증체계 확보가 가능하다.

영역	분야	항목
1. 관리체계 수립 및 운영	1.1 관리체계 기반 마련	1.1.1 경영진의 참여
		1.1.2 최고책임자의 지정
		1.1.3 조직 구성
		1.1.4 범위 설정
		1.1.5 정책 수립
		1.1.6 자원 할당
	1.2 위험 관리	1.2.1 정보자산 식별
		1.2.2 현황 및 흐름분석
		1.2.3 위험 평가
		1.2.4 보호대책 선정
	1.3 관리체계 운영	1.3.1 보호대책 구현
		1.3.2 보호대책 공유
		1.3.3 운영현황 관리
	1.4 관리체계 점검 및 개선	1.4.1 법적 요구사항 준수 검토
		1.4.2 관리체계 점검
		1.4.3 관리체계 개선
2. 보호대책 요구사항	2.1 정책, 조직, 자산 관리	2.1.1 정책의 유지관리
		2.1.2 조직의 유지관리
		2.1.3 정보자산 관리
	2.2 인적 보안	2.2.1 주요 직무자 지정 및 관리
		2.2.2 직무 분리
		2.2.3 보안 서약
		2.2.4 인식제고 및 교육훈련
		2.2.5 퇴직 및 직무변경 관리
		2.2.6 보안 위반 시 조치
	2.3 외부자 보안	2.3.1 외부자 현황 관리
		2.3.2 외부자 계약 시 보안
		2.3.3 외부자 보안 이행 관리
		2.3.4 외부자 계약 변경 및 만료 시 보안
	2.4 물리 보안	2.4.1 보호구역 지정
		2.4.2 출입통제

영역	분야	항목
		2.4.3 정보시스템 보호
		2.4.4 보호설비 운영
		2.4.5 보호구역 내 작업
		2.4.6 반출입 기기 통제
		2.4.7 업무환경 보안
	2.5 인증 및 권한관리	2.5.1 사용자 계정 관리
		2.5.2 사용자 식별
		2.5.3 사용자 인증
		2.5.4 비밀번호 관리
		2.5.5 특수 계정 및 권한관리
		2.5.6 접근권한 검토
	2.6 접근통제	2.6.1 네트워크 접근
		2.6.2 정보시스템 접근
		2.6.3 응용프로그램 접근
		2.6.4 데이터베이스 접근
		2.6.5 무선 네트워크 접근
		2.6.6 원격접근 통제
		2.6.7 인터넷 접속 통제
	2.7 암호화 적용	2.7.1 암호정책 적용
		2.7.2 암호키 관리
	2.8 정보시스템 도입 및 개발 보안	2.8.1 보안 요구사항 정의
		2.8.2 보안 요구사항 검토 및 시험
		2.8.3 시험과 운영 환경 분리
		2.8.4 시험 데이터 보안
		2.8.5 소스 프로그램 관리
		2.8.6 운영환경 이관
	2.9 시스템 및 서비스 운영관리	2.9.1 변경관리
		2.9.2 성능 및 장애관리
		2.9.3 백업 및 복구관리
		2.9.4 로그 및 접속기록 관리
		2.9.5 로그 및 접속기록 점검
		2.9.6 시간 동기화
		2.9.7 정보자산의 재사용 및 폐기
	2.10 시스템 및 서비스 보안관리	2.10.1 보안시스템 운영
		2.10.2 클라우드 보안
		2.10.3 공개서버 보안
		2.10.4 전자거래 및 핀테크 보안
		2.10.5 정보전송 보안
		2.10.6 업무용 단말기기 보안
		2.10.7 보조저장매체 관리
		2.10.8 패치관리
		2.10.9 악성코드 통제
	2.11 사고 예방 및 대응	2.11.1 사고 예방 및 대응체계 구축
		2.11.2 취약점 점검 및 조치
		2.11.3 이상행위 분석 및 모니터링

영역	분야	항목
	2.12 재해 복구	2.11.4 사고 대응 훈련 및 개선
		2.11.5 사고 대응 및 복구
		2.12.1 재해·재난 대비 안전조치
		2.12.2 재해 복구 시험 및 개선
3. 개인정보 처리 단계별 요구 사항	3.1 개인정보 수집 시 보호조치	3.1.1 개인정보 수집 제한
		3.1.2 개인정보의 수집 동의
		3.1.3 주민등록번호 처리 제한
		3.1.4 민감정보 및 고유식별정보의 처리 제한
		3.1.5 간접수집 보호조치
		3.1.6 영상정보처리기기 설치·운영
		3.1.7 홍보 및 마케팅 목적 활용 시 조치
	3.2 개인정보 보유 및 이용 시 보호조치	3.2.1 개인정보 현황관리
		3.2.2 개인정보 품질보장
		3.2.3 개인정보 표시제한 및 이용 시 보호 조치
		3.2.4 이용자 단말기 접근 보호
		3.2.5 개인정보 목적 외 이용 및 제공
	3.3 개인정보 제공 시 보호조치	3.3.1 개인정보 제3자 제공
		3.3.2 업무 위탁에 따른 정보주체 고지
		3.3.3 영업의 양수 등에 따른 개인정보의 이전
		3.3.4 개인정보의 국외 이전
	3.4 개인정보 파기 시 보호조치	3.4.1 개인정보의 파기
		3.4.2 처리목적 달성 후 보유 시 조치
		3.4.3 휴면 이용자 관리
	3.5 정보주체 권리보호	3.5.1 개인정보처리방침 공개
		3.5.2 정보주체 권리보장
		3.5.3 이용내역 통지

표 19. ISMS-P 인증항목

- K-BTF 공동인프라를 통해 공공서비스의 지속적인 확장이 이루어지고 일일평균 이용자수가 100만명 이상일 경우를 대비하여 초기 설계부터 ISMS-P 인증을 고려한 설계가 반영되어야 한다.
- K-BTF 공동인프라의 초기 확산을 위해 공공 블록체인 서비스가 운영 되는데 필요한 항목을 선택하여 인증 심사를 통해 인증을 획득할 수 있다.
- ISMS-P 인증심사를 진행하기 위해서는 사전 2개월동안 운영실적이 있어야 인증심사진행이 가능하며, ISMS-P 인증취득을 위해 요구되는 보안관리 체계 상의 심사항목을 적용해야 하는 등의 어려움이 존재할 수 있음.

- 클라우드보안인증은 인증획득 후 조달청의 디지털서비스 이용지원시스템 또는 디지털서비스몰에 입점하여 민간 기업의 서비스를 공공에서 손쉽게 제공할 수 있지만, ISMS-P는 인증 획득 후에도 공공영역에 서비스 제공을 하기에는 어려움을 있다.

(나) 클라우드 보안인증제도(CSAP: Cloud Security assurance program)

- K-BTF 공동인프라가 클라우드 환경에서 서비스를 제공할 경우라면 클라우드보안인증제도(CSAP)가 가장 대표적인 인증체계라고 할 수 있다. 클라우드 보안인증제도는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조의2에 따라 클라우드 서비스 제공자(Cloud Service Provider, 이하 CSP)가 제공하는 클라우드 컴퓨팅 서비스에 대해 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 보안인증을 수행하는 제도이다. 클라우드보안인증 유형은 인프라 영역인 IaaS, 서비스 영역인 SaaS 표준등급과 SaaS간편등급, 데스크탑 영역인 DaaS가 있으며 상·중·하등급·하등급SaaS 중 선택하여 인증 신청이 가능하다.
- 클라우드보안인증범위의 경우 IaaS 보안인증은 관리적·물리적·기술적 보호조치 및 공공기관용 추가 보호조치로 총 14개 분야 116개 통제항목으로, SaaS 표준등급 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 13개 분야 79개 통제항목으로, SaaS 간편등급 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 11개 분야 31개 통제항목으로, DaaS 인증은 관리적·물리적·기술적 및 공공기관용 추가 보호조치로 총 14개 분야 110개 통제항목으로 구성되어 있다. 또한 하등급 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 14개 분야 64개 통제항목으로, 하등급 SaaS 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 11개 분야 30개 통제항목으로 구성되어 있다.
- K-BTF 공동인프라를 퍼블릭/프라이빗 클라우드 환경에서 구축한 경우 IaaS 유형으로 인증을 진행하며, IaaS 인증을 이미 획득한 CSP의 클라

우드 환경에 구축할 경우에는 IaaS 인증은 취득하지 않아도 무방하다. K-BTF 공동인프라의 SaaS 인증을 취득할 경우 SaaS 표준과 SaaS 간편 중 선택하여 인증을 진행할 수 있다. DaaS 인증 유형의 경우 Desktop 가상화 환경에 대한 인증으로 K-BTF 공동인프라의 범위에 해당하지 않는 인증 유형이다.

- 클라우드보안인증의 범위 중 K-BTF 공동인프라 영역에 해당하는 인증기준을 아래 표에서와 같이 정리하였다.

(☐ : ISMS-P 인증 취득 시 심사 생략 가능 대상)

통제 분야	통제 항목	세부통제항목	IaaS	SaaS (표준)	SaaS (간편)	하등급 SaaS
1 정보보호 정책 및 조직	11 정보보호 정책	1.1.1 정보보호 정책 수립	○	○	○	
		1.1.2 정보보호 정책 검토 및 변경	○	○		
		1.1.3 정보보호 정책문서 관리	○	○		
	12 정보보호 조직	1.2.1 조직 구성	○	○		○
		1.2.2 역할 및 책임 부여	○	○	○	
2 인적보안	21 내부인력 보안	2.1.1 고용계약	○	○		
		2.1.2 주요 직무자 지정 및 감독	○	○	○	○
		2.1.3 직무 분리	○	○		
		2.1.4 비밀유지서약서	○	○		
		2.1.5 퇴직 및 직무변경	○			
	22 외부인력 보안	2.2.1 외부인력 계약	○			
		2.2.2 외부인력 보안 이행 관리	○			
		2.2.3 계약 만료 시 보안	○			
	23 정보보호 교육	2.3.1 교육 프로그램 수립	○			
		2.3.2 교육 시행	○	○	○	○
		2.3.3 평가 및 개선	○			
3 자산관리	31 자산 식별 및 분류	3.1.1 자산 식별	○	○		
		3.1.2 자산별 책임할당	○			
		3.1.3 보안등급 및 취급	○			
	32 자산 변경관리	3.2.1 변경관리	○	○		
		3.2.2 변경 탐지 및 모니터링	○			
		3.2.3 변경 후 작업검증	○			

통제 분야	통제 항목	세부통제항목	IaaS	SaaS (표준)	SaaS (간편)	하등급 SaaS
	3.3 위험관리	3.3.1 위험관리계획 수립	○			
		3.3.2 취약점 점검	○	○		
		3.3.3 위험분석 및 평가	○			
		3.3.4 위험처리	○			
4. 서비스 공급망 관리	4.1 공급망 관리정책	4.1.1 공급망 관리 정책 수립	○	○		
		4.1.2 공급망 계약	○	○		
	4.2 공급망 변경관리	4.2.1 공급망 변경 관리	○	○		
		4.2.2 공급망 모니터링 및 검토	○			
5. 침해 사고관리	5.1 침해사고 대응 절차 및 체계	5.1.1 침해사고 대응 절차 수립	○	○	○	○
		5.1.2 침해사고 대응 체계 구축	○	○		
		5.1.3 침해사고 대응 훈련 및 점검	○	○		
	5.2 침해사고 대응	5.2.1 침해사고 보고	○	○	○	○
		5.2.2 침해사고 처리 및 복구	○	○		
	5.3 사후관리	5.3.1 침해사고 분석 및 공유	○	○		
		5.3.2 재발방지	○	○		
6. 서비스 연속성 관리	6.1 장애대응	6.1.1 장애 대응절차 수립	○	○		
		6.1.2 장애 보고	○	○	○	○
		6.1.3 장애 처리 및 복구	○	○		
		6.1.4 재발방지	○	○		
	6.2 서비스 가용성	6.2.1 성능 및 용량 관리	○	○	○	○
		6.2.2 이중화 및 백업	○	○		
		6.2.3 서비스 연속성 점검	○			
7. 준거성	7.1 법 및 정책 준수	7.1.1 법적요구사항 준수	○	○	○	○
		7.1.2 정보보호 정책 준수	○			
	7.2 보안 감사	7.2.1 독립적 보안감사	○	○		
		7.2.2 감사기록 및 모니터링	○	○		
8. 물리적 보안	8.1 물리적 보호구역	8.1.1 물리적 보호구역 지정	○			
		8.1.2 물리적 출입통제	○			
		8.1.3 물리적 보호구역 내 작업	○			
		8.1.4 사무실 및 설비 공간 보호	○			
		8.1.5 모바일 기기 반출·입	○			

통제 분야	통제 항목	세부통제항목	IaaS	SaaS (표준)	SaaS (간편)	하등급 SaaS
	8.2 정보처리 시설 및 장비 보호	8.2.1 정보처리시설의 배치	○			
		8.2.2 보호설비	○			
		8.2.3 케이블 보호	○			
		8.2.4 시설 및 장비 유지보수	○			
		8.2.5 장비 반출·입	○			
		8.2.6 장비 폐기 및 재사용	○			
9. 가상화 보안	9.1 가상화 인프라	9.1.1 가상자원 관리	○	○		
		9.1.2 가상자원 회수	○			
		9.1.3 가상자원 모니터링	○			
		9.1.4 하이퍼바이저 보안	○			
		9.1.5 공개서버 보안	○	○	○	○
		9.1.6 상호 운용성 및 이식성	○			
	9.2 가상 환경	9.2.1 악성코드 통제	○	○		
		9.2.2 인터페이스 및 API 보안	○	○		
		9.2.3 데이터 이전	○	○		
		9.2.4 가상 소프트웨어 보안	○	○		
10. 접근통제	10.1 접근통제 정책	10.1.1 접근통제 정책 수립	○	○		
		10.1.2 접근기록 관리	○	○	○	○
	10.2 접근 권한 관리	10.2.1 사용자 등록 및 권한 부여	○	○		
		10.2.2 관리자 및 특수 권한 관리	○	○		
		10.2.3 접근권한 검토	○	○		
	10.3 사용자 식별 및 인증	10.3.1 사용자 식별	○	○		
		10.3.2 사용자 인증	○	○	○	○
		10.3.3 강화된 인증 수단 제공	○	○	○	○
		10.3.4 패스워드 관리	○	○	○	○
11. 네트워크 보안	11.1 네트워크 보안	11.1.1 네트워크 보안정책 수립	○	○		
		11.1.2 네트워크 모니터링 및 통제	○	○		
		11.1.3 네트워크 정보보호시스 템 운영	○	○		
		11.1.4 네트워크 암호화	○	○	○	○
		11.1.5 네트워크 분리	○	○	○	○
		11.1.6 무선 접근통제	○			

통제 분야	통제 항목	세부통제항목	IaaS	SaaS (표준)	SaaS (간편)	하등급 SaaS
12. 데이터 보호 및 암호화	121 데이터 보호	12.1.1 데이터 분류	○	○		
		12.1.2 데이터 소유권	○	○		
		12.1.3 데이터 무결성	○	○		
		12.1.4 데이터 보호	○	○	○	
		12.1.5 데이터 추적성	○	○		
		12.1.6 데이터 폐기	○	○	○	○
	122 매체 보안	12.2.1 저장매체 관리	○			
		12.2.2 이동매체 관리	○			
	123 암호화	12.3.1 암호 정책 수립	○	○	○	○
		12.3.2 암호키 관리	○	○	○	
13. 시스템 개발 및 도입 보안	131 시스템 분석 및 설계	13.1.1 보안요구사항 정의	○	○		
		13.1.2 인증 및 암호화 기능	○	○	○	○
		13.1.3 보안로그 기능	○	○		
		13.1.4 접근권한 기능	○	○		
		13.1.5 시각 동기화	○	○		
	132 구현 및 시험	13.2.1 구현 및 시험	○	○	○	○
		13.2.2 개발과 운영환경 분리	○	○		
		13.2.3 시험 데이터 보안	○	○		
		13.2.4 소스 프로그램 보안	○	○		
	133 외주 개발 보안	13.3.1 외주 개발 보안	○	○		
	134 시스템 도입 보안	13.4.1 시스템 도입 계획	○			
		13.4.2 시스템 인수	○			
14. 국가기관 등의 보안 요구사항	141 관리적 보호조치	14.1.1 보안서비스 수준 협약	○	○	○	○
		14.1.2 도입 전산장비 안전성	○	○	○	○
		14.1.3 보안관리 수준	○	○	○	○
		14.1.4 사고 및 장애 대응	○	○	○	○
	142 물리적 보호조치	14.2.1 물리적 위치 및 영역분리	○	○	○	○
		14.2.2 중요장비 이중화 및 백업체계 구축	○	○	○	○
	143 기술적 보호조치	14.3.1 검증필 암호화 기술 제공	○	○	○	○
		14.3.2 보안관제 제반환경 지원	○			○
		14.3.3 데이터 유출 방지				○

통제 분야	통제 항목	세부통제항목	IaaS	SaaS (표준)	SaaS (간편)	하등급 SaaS
		14.3.4 시스템 격리	○	○	○	○
		14.3.5 영역분리	○	○	○	○
총계			116	79	31	30

표 20. 클라우드보안인증 심사 항목

- 클라우드보안인증체계를 활용하여 K-BTF 시험검증체계를 빠르고 손쉽게 확보할 수 있다는 장점이 있다.
- ISMS-P 획득 후 클라우드보안인증을 받을 경우 인증심사에서 제외하는 항목이 있어서 빠르게 진행할 수 있다.
- 클라우드보안인증 SaaS 진행 시 클라우드보안인증 IaaS 인증을 보유한 국내 퍼블릭 클라우드 업체의 클라우드 환경을 기반으로 블록체인 서비스를 구축하고, SaaS(간편) 등급이나 하등급 SaaS으로 진행하다면 인증심사를 효율적으로 진행할 수 있을 것으로 판단한다.
- ISMS-P 인증 및 클라우드보안인증까지 인증을 획득하기까지 약 2년 이상의 대응기간이 소요된다.
- 클라우드보안인증 획득 후 조달청의 디지털서비스 이용지원시스템 또는 디지털서비스몰에 입점하여 민간 기업의 서비스를 공공에서 손쉽게 제공할 수 있다.

(다) 행안부 행정기관 및 공공기관 정보시스템 구축, 운영 지침

- 행안부 행정기관 및 공공기관 정보시스템 구축, 운영 지침은 전자정부법 제45조 제3항에 따라 행정기관 등의 장이 정보시스템을 구축·운영함에 있어서 준수해야 할 기준, 표준 및 절차와 법 따른 상호호환성 기술평가에 관한 사항을 제시하고 있다. 즉, 소프트웨어 나 보안 등 특정 분야의 인증체계가 아닌 정보시스템 구축·운영 중 준수해야 할 원칙, 절차, 항목 등을 제시하고 있다.
- 지침에는 소프트웨어보안 가이드에 소프트웨어 개발보안 대상 및 진단 기준을 제시하고 있으며 설계단계 보안 기준 총 20개 항목, 구현

단계 보안약점 제거 기준 총 49개 항목을 제시하고 있다.

- 또한 사업 수행사는 정보시스템 구축, 운영 기술 지침 기술적용계획표를 통해 플랫폼 및 기반구조 분야, 요소기술분야, 서비스 인터페이스 및 통합 분야, 서비스 접근 및 전달 분야로 구분하여 해당 기술의 적용 여부를 제시하고 감리 단계에서 감리 및 소프트웨어 개발 보안 진단을 통해 이상여부를 점검한다.
- 정보시스템 구축, 운영 기술 지침 내 소프트웨어개발 보안진단항목과 기술적용계획/결과표를 아래와 같이 정리하였다.

단계	보안약점구분	보안약점
설계단계	1. 입력데이터 검증 및 표현	1.1 DBMS 조회 및 결과 검증
		1.2 XML 조회 및 결과 검증
		1.3 디렉토리 서비스 조회 및 결과 검증
		1.4 시스템 자원 접근 및 명령어 수행 입력값 검증
		1.5 웹 서비스 요청 및 결과 검증
		1.6 웹 기반 중요기능 수행 요청 유효성 검증
		1.7 HTTP 프로토콜 유효성 검증
		1.8 허용된 범위내 메모리 접근
		1.9 보안기능 동작에 사용되는 입력값 검증
		1.10 업로드·다운로드 파일 검증
	2. 보안기능	2.1 인증 대상 및 방식
		2.2 인증 수행 제한
		2.3 비밀번호 관리
		2.4 중요자원 접근통제
		2.5 암호키 관리
		2.6 암호연산
		2.7 중요정보 저장
		2.8 중요정보 전송
	3. 예외처리	3.1 예외처리
	4. 세션통제	4.1 세션통제
구현단계	1. 입력데이터 검증 및 표현	1.1 SQL 삽입
		1.2 경로 조작 및 자원 삽입
		1.3 크로스사이트 스크립트
		1.4 운영체제 명령어 삽입

단계	보안약점구분	보안약점
		1.5 위험한 형식 파일 업로드
		1.6 신뢰되지 않는 URL 주소로 자동접속 연결
		1.7 XQuery 삽입
		1.8 XPath 삽입
		1.9 LDAP 삽입
		1.10 크로스사이트 요청 위조
		1.11 HTTP 응답분할
		1.12 정수형 오버플로우
		1.13 보안기능 결정에 사용되는 부적절한 입력값
		1.14 메모리 버퍼 오버플로우
		1.15 포맷 스트링 삽입
	2. 보안기능	2.1 적절한 인증 없는 중요 기능 허용
		2.2 부적절한 인가
		2.3 중요한 자원에 대한 잘못된 권한 설정
		2.4 취약한 암호화 알고리즘 사용
		2.5 중요정보 평문저장
		2.6 중요정보 평문전송
		2.7 하드코드된 비밀번호
		2.8 충분하지 않은 키 길이 사용
		2.9 적절하지 않은 난수값 사용
		2.10 하드코드된 암호화 키
		2.11 취약한 비밀번호 허용
		2.12 사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출
		2.13 주석문 안에 포함된 시스템 주요정보
		2.14 솔트 없이 일방향 해쉬 함수 사용
		2.15 무결성 검사 없는 코드 다운로드
		2.16 반복된 인증시도 제한 기능 부재
	3. 시간 및 상태	3.1 경쟁조건: 검사 시점과 사용 시점(TOCTOU)
		3.2 종료되지 않는 반복문 또는 재귀 함수
	4. 에러처리	4.1 오류 메시지를 통한 정보 노출
		4.2 오류 상황 대응 부재
		4.3 부적절한 예외 처리
	5. 코드오류	5.1 Null Pointer 역참조
		5.2 부적절한 자원 해제

단계	보안약점구분	보안약점
		5.3 해제된 자원 사용
		5.4 초기화되지 않은 변수 사용
	6. 캡슐화	6.1 잘못된 세션에 의한 데이터 정보 노출
		6.2 제거되지 않고 남은 디버그 코드
		6.3 시스템 데이터 정보노출
		6.4 Public 메소드부터 반환된 Private 배열
		6.5 Private 배열에 Public 데이터 할당
	7. API 오용	7.1 DNS lookup에 의존한 보안결정
		7.2 취약한 API 사용

표 21. 소프트웨어개발보안 진단 항목

분야	구분	항 목
플랫폼및기반 구조분야	데이터베이스	데이터베이스
	소프트웨어 공학	소프트웨어 품질 및 형상 관리
		시험관리
	데이터베이스	저장소
	서버	공통
		웹서버
		미디어서버
		응용서버
	소프트웨어 공학	통합개발환경
		방법론
		모델링
		시스템 관리
	네트워크	LAN
		가상멀티미디어회의
		무선 및 부가 통신
	하드웨어	서버 및 컴퓨터
		임베디드 장치
		주변 장치
	운영체제 및 기반환경	개방형 운영체제
		무선/이동용 운영체제
		오픈소스
요소기술 분야	데이터 표현	정적 표현
		동적 표현

분야	구분	항 목
		컨텐츠 저작
		무선/이동/음성표현
	사용자 인터페이스	이미지
		이미지맵
		공백
		스타일
		프레임
		스크린-사이즈
	프로그래밍	개방형 프로그래밍
	통합 패키지	포털
		그룹웨어
		BPM
		GIS
	데이터 교환	데이터 교환 프로토콜
		데이터 교환 형식
		데이터 압축
		국제화
	데이터 관리	데이터 표준화
		데이터베이스 접근
		데이터 처리
		데이터 검색
	보안	사용자 인증
		전자서명
		네트워크 보안
		데이터 보안
		시스템/응용 보안
		통합 보안
		침해사고 예방, 대응
		계정 및 비밀번호
		백업
		로그
		비상계획
		개인정보 보호
서비스 인터페이스 및	서비스 통합	웹서비스
		EAI

분야	구분	항 목
통합 분야	데이터 공유	데이터형식
		데이터 변환
		전자문서
	인터페이스	서비스 발견
		서비스 명세 및 인터페이스
서비스 접근 및 전달 분야	외부 접근장치	웹 브라우저
		시스템 대 시스템
	서비스 전달망	인트라넷(유/무선)
	서비스 요구사항	법률, 규정, 지침
	서비스 전송 프로토콜	응용 프로토콜
		전송 프로토콜

표 22. 기술적용계획표 항목 기준

- 정보시스템 구축, 운영 기술 지침은 구축, 운영 시스템 기준의 기술 적용 항목과 소프트웨어개발 보안 항목 통해 K-BTF의 적합성을 진단 받을 수 있다는 장점이 있지만 인증체계가 아닌 감리, 보안진단을 통한 시험검증체계에 가깝다. 또한 블록체인 만의 블록화, 암호화 등의 처리 시간, 처리량 등 성능지표는 인증을 받을 수 없다.

(라) 해외 시험검증체계

- (싱가폴 GovTech) GovTech를 적용한 싱가포르 정부의 모든 디지털 서비스에는 싱가포르 정부 온라인 로고가 포함된 공식적인 배너를 모든 페이지에 적용한다.
- (NIST U.S Cyber Trust Mark) 미국 NIST에서 제시한 사이버 보안 기준에 따라 IoT 장치 및 소프트웨어 개발 단계에서 해당 기준을 준수할 경우에 레이블을 부여하는 프로그램이다. 해당 프로그램은 두가지 영역으로 소비자 기준의 IoT 사이버 보안 라벨링 프로그램과 소비자 소프트웨어 기준의 보안 라벨링 프로그램이며 해당 기준 충족 시 사이버 보안 인증 및 라벨링 프로그램을 부여하는 인증체계이다. 해킹 등 사이버 공격에 덜 취약한 전자제품을 인증하여 소비자가 사이버 공격에서 더 안전한 스마트기기를 쉽게 고를 수 있도록 인증마크를

부착하는 제도이다. 하지만 23년 7월 계획이 발표되었고 요구사항이 확정되지 않은 상태이며, 강력한 기본 암호, 저장 및 전송된 정보에 대한 포괄적인 데이터 보호, 정기적인 보안 업데이트 및 사고 감지 기능 등이 포함될 것으로 예상된다.



그림 48. NIST U.S Cyber Trust Mark

출처: <https://www.fcc.gov/cybersecurity-certification-mark>

- 이와 유사한 국내 시험검증체계로는 전자정부표준프레임워크 호환성 인증이 있으며, 정부부처, 지자체, 공공기관 등 공공정보화 사업에서 전자정부 표준프레임워크와 상용 솔루션 간에 연동이 가능한지 확인하는 유료 서비스이다. 표준프레임워크 호환성 인증을 획득하면 표준프레임워크 포털에 등재되며 인증 마크를 부여한다.

2. K-BTF 시험검증체계 마련을 위한 시사점

- (단기적 측면) K-BTF의 조기 확산을 위해서는 기존 인증제도인 ISMS-P와 클라우드보안인증을 활용하는 것이 바람직하다.
 - 다만, 클라우드보안인증(SaaS)으로 인증을 받을 경우, 클라우드보안인증(IaaS)을 획득한 국내 민간 클라우드 사업자(CSP:Cloud Service Provider)의 클라우드 서비스를 이용해야 한다.
 - 국내 민간 클라우드 사업자의 경우 클라우드보안인증과 ISMS-P를 모두 획득한 사업자도 존재하며, ISMS-P 인증을 받은 서비스 위에 K-BTF 공동인프라를 구축할 경우 단기간에 안심할 수 있는 K-BTF 공동인프라 구성이 가능하다. K-BTF 공통요구사항을 준수하는

K-BTF 공동인프라를 SaaS 형태로 구성하고 클라우드보안인증(SaaS)로 진행할 경우 ISMS-P 인증과 클라우드보안인증(IaaS)를 동시에 획득한 민간 클라우드 서비스 환경에 구성하는 방안이 가장 적절하다.

□ (중장기적 측면) K-BTF 공동인프라를 위한 별도의 시험인증체계확립을 위해서는 근거 규정의 개선과 시험검증체계 개발을 위한 추가 프로젝트가 별도로 진행되어야 한다.

○ 새롭게 시험검증체계를 개발할 경우, 앞서 연구되었던 ISMS-P, 클라우드보안인증의 인증항목 위주로 구성하여 인증제도를 운영할 수 있다. 다만, 신규로 시험검증제도를 마련하는 경우 기업이 보유한 기존 인증에 중복하여 추가적인 부담을 줄 수 있다는 점과 신규 시험검증체계 개발을 위해 추가 프로젝트 진행에 대한 예산과 기간이 소요된다는 단점이 있다.

참고문헌

- [1] 국가정보원, 과학기술정보통신부, 국가보안기술연구소, 한국정보통신기술협회 (2020), 「국가·공공기관 도입을 위한 블록체인 암호기술 가이드라인」
- [2] 과학기술정보통신부 (2018), 「블록체인 기술 발전전략」
- [3] 과학기술정보통신부 (2020), 「블록체인산업실태조사」
- [4] 나재훈 (2021), 「ISO TC307 블록체인 정보보호 표준기술 동향」, 정보보호학회지
- [5] 라온시큐어, 「라온시큐어 공식 홈페이지」, www.raonsecure.com/ko/main
- [6] 메디블록, 「메디블록 공식 홈페이지」, <https://medibloc.co.kr/>
- [7] 모나체인, 「모나체인 공식 홈페이지」, <https://www.lgcns.com/business/web3/monachain/>
- [8] 박민정, 채상미, 이명준 (2018), 「개인정보보호법제 관점에서 본 블록체인의 법적 쟁점 GDPR 및 국내 개인정보보호법을 바탕으로」
- [9] 블록체인랩스, 「블록체인랩스 공식 홈페이지」, <https://bc-labs.net/ko/technology/>
- [10] 소프트웨어정책연구소 (2017), 「블록체인(Blockchain) 기술의 산업적·사회적 활용 전망 및 시사점」
- [11] 소프트웨어정책연구소 (2018), 「공공서비스 분야 블록체인 기술 활용 확산 방안」
- [12] 소프트웨어정책연구소 (2020), 「블록체인 서비스 적용을 위한 평가모델 연구」
- [13] 소프트웨어정책연구소 (2021), 「디지털 신뢰 감독의 필요성 (블록체인 기술 중심으로)」
- [14] 소프트웨어정책연구소 (2021), 「블록체인 개발, 적용을 위한 핵심 엔진으로서 BaaS에 대한 고찰」
- [15] 소프트웨어정책연구소 (2021), 「오픈소스 활성화를 위한 오픈소스 연구개발 생태계 연구」
- [16] 연구개발특구진흥재단 (2021), 「글로벌 시장동향보고서, 블록체인 시장」
- [17] 월드와이드웹 컨소시엄(W3C) (2022.07), 「Decentralized Identifiers (DIDs) v1.0」
- [18] 전자정부 표준프레임워크, 「표준프레임워크 개발환경가이드 4.0」, <https://www.egovframe.go.kr/wiki/doku.php?id=egovframework:dev4.0:dev4.0>
- [19] 전자정부 표준프레임워크, 「표준프레임워크 실행환경가이드 4.0」,

- <https://egovframe.go.kr/wiki/doku.php?id=egovframework:rte4.0>
- [20] 전자정부 표준프레임워크, 「표준프레임워크 운영환경가이드」,
<https://www.egovframe.go.kr/wiki/doku.php?id=egovframework:%EC%9A%B4%EC%98%81%ED%99%98%EA%B2%BD%EA%B0%80%EC%9D%B4%EB%93%9C>
- [21] 전자정부 표준프레임워크, 「표준프레임워크 공통컴포넌트가이드 4.0」,
<https://www.egovframe.go.kr/wiki/doku.php?id=egovframework:com:v4.0:init>
- [22] 정보통신산업진흥원 (2018), 「블록체인 관련 동향 및 시사점」
- [23] 정보통신산업진흥원 (2020), 『이슈리포트(2020-06호)』, 「블록체인 강국의 인프라 서비스형 블록체인(BaaS)」
- [24] (주)지크립토 (2022) 「블록체인 활용 · 확산을 위한 공통기반 연구 한국인터넷진흥원」
- [25] 질병관리청, 「COOV 소개」, <https://ncv.kdca.go.kr/menu.es?mid=a12502000000>
- [26] 한국블록체인협회 (2022. 05), 「「디지털자산」 동향 보고서」
- [27] 한국세계지역학회 (2018), 「블록체인 기술은 굿 거버넌스(Good Governance)를 만들 수 있는가?」
- [28] 한국인터넷진흥원 (2021), 「블록체인 산업의 경제적 파급효과 및 기여도 분석 연구」
- [29] 한국전자통신연구원 (2020), 「GAIA-X 분석 및 데이터 댐 발전 방향」
- [30] 한독경상학회 (2020), 「GAIA-X와 독일 정책플랫폼의 시사점」
- [31] 한성대학교 (2019), 「블록체인 기술을 활용한 공공가치 창출사례와 발전방향」
- [32] 행안부 행정기관 및 공공기관 정보시스템 구축 운영 지침,
https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBS_MSTR_000000000016&nttId=91659
- [33] 클라우드보안인증, 「클라우드보안인증 홈페이지」,
<https://isms.kisa.or.kr/main/csap/intro/index.jsp>
- [34] Blockchain-based Service Network, 「BSN 공식 홈페이지」,
bsnbase.io/g/main/documentation
- [35] Blockchain-based Service Network, 「BSN 공식 GitHub」,
<https://github.com/BSNDA>
- [36] Canada OrgBook, 「Canada 공식 홈페이지」, <https://orgbook.gov.bc.ca/api/>
- [37] ChainZ, 「ChainZ 공식 홈페이지」, <https://skdt.co.kr/chainz/>
- [38] EBSI, 「EBSI 공식 홈페이지」,
ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

- [39] EBSI, 「EBSI 공식 GitHub」, <https://github.com/protokol/ebs>
- [40] GAIA-X, 「GAIA-X 공식 홈페이지」, <https://gaia-x.eu/gaia-x-framework/>
- [41] GAIA-X, 「GAIA-X 공식 GitHub」, <https://gitlab.eclipse.org/eclipse/xfsc/>
- [42] IEEE Potentials (2022), 「Blockchain technology: An overview」
- [43] ISMS-P, 「ISMS-P 홈페이지」, <https://isms.kisa.or.kr/main/ispims/intro/>
- [44] Klaytn, 「클레이튼 공식 홈페이지」, [klaytn.foundation/
https://www.lgcns.com/business/blockchain/monachain/](https://www.lgcns.com/business/blockchain/monachain/)
- [45] Mohanty, Debasis & Anand, Divya & Aljahdali, Hani & Gracia Villar, Santos (2022), 『Sustainability』, 「Blockchain Interoperability: Towards a Sustainable Payment System」
- [46] M. Westerkamp and J. Eberhardt, IEEE European Symposium on Security and Privacy Workshops (2020), 「zkRelay: Facilitating Sidechains using zkSNARK-based Chain-Relays」
- [47] NIST U.S Cyber Trust Mark,
<https://www.fcc.gov/cybersecurity-certification-mark>
- [48] Singapore OpenAttestation, 「OpenAttestation 공식 홈페이지」, <https://www.openattestation.com/docs/developer-section/quickstart/create-verifiable-document-issuer>
- [49] Singapore OpenAttestation, 「OpenAttestation 공식 GitHub」, <https://github.com/Open-Attestation/demo-verifiable-document-issuer>

블록체인 신뢰 프레임워크(K-BTF) 중장기계획 수립 연구

인 쇄 : 2023 년 12 월

발 행 : 2023 년 12 월

발행인 : 이 원 태

발행처 : 한국인터넷진흥원(KISA, Korea Internet & Security Agency)

전라남도 나주시 진흥길 9

Tel: 1544-5118

인쇄처 : (주)블로코

<비매품>

1. 본 보고서는 과학기술정보통신부의 기금으로 수행한 사업의 결과입니다.
2. 본 보고서의 내용을 발표할 때에는 반드시 한국인터넷진흥원 사업의 결과임을 밝혀야 합니다.
3. 본 보고서의 판권은 한국인터넷진흥원이 소유하고 있으며, 당 진흥원의 허가 없이 무단 전재 및 복사를 금합니다.

※ 본 보고서의 내용은 한국인터넷진흥원의 공식 입장과는 무관합니다.