블록체인 기술·정책·산업 동향 디지털기반본부 디지털신뢰단 블록체인정책팀

[글로벌]

블록체인 기반 데이터 스페이스 신뢰 기술

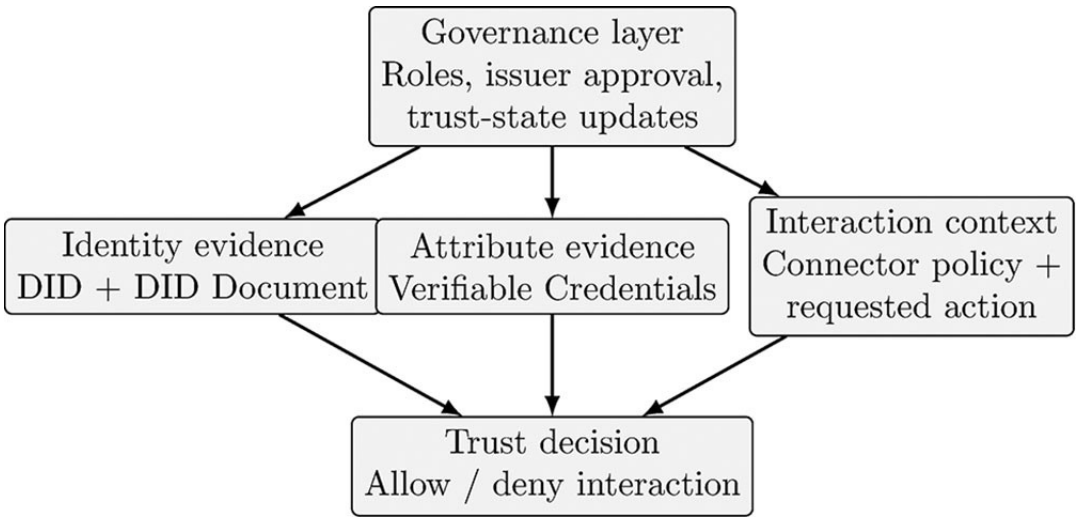
- 연합 데이터 스페이스 환경에서 블록체인과 자기주권신원(SSI) 기술을 결합하여 종합 아키텍처를 제시함
- EDC와의 기술적 상호운용성을 확보하고 커넥터 핵심 동작 전반에 신뢰 검증 절차를 성공적으로 통합함

IDBLOCK 시스템은 블록체인을 통한 검증된 신뢰 거버넌스 제공 및 자격 증명 기반의 접근 제어를 효과적으로 구현하여 데이터 스페이스 내 안전하고 투명한 상호작용을 확실하게 보장함

▶ 분산형 신뢰 아키텍처 도입의 필요성을 제시하고 기존 데이터 스페이스의 한계를 분석함

- 기존 페더레이션 데이터 스페이스는 중앙집중식 승인 주체나 연합 기관에 과도하게 의존하여 전체 참가자격을 심사하고 권한을 부여하는 대단히 제한적인 구조를 보유함
- 기존의 X.509 PKI 인증서 방식은 모든 신원 속성 검증을 발행자에게 전적으로 의존하므로 신규 정보 추가 시 인증서를 매번 번거롭게 재발급해야 하는 불편함이 있음
- OAuth2 및 OpenID Connect 기반 토큰 교환 방식은 사용자에게 상위 수준의 제어를 제공하지만 중앙 토큰 발급 주체에 구조적으로 의존하게 됨
- 자기주권신원(SSI) 기술 단독 적용 시 자격증명의 휴대성은 크게 향상되지만 유효한 발행자 등록, 역할 관리, 신뢰 상태 갱신 등의 투명한 공유 거버넌스가 근본적으로 결여되는 한계가 있음

[블록체인 거버넌스 기반 SSI 신뢰 모델의 개념 구조]



출처 : Open Research Europe, 'A blockchain-governed SSI trust architecture for EDC-based federated data spaces', 2026.07.22.

▶ 블록체인 연동 기반 자기주권신원(SSI) 기술 적용을 통하여 분산 신뢰 모델을 구조화함

- 탈중앙화 식별자(DID) 체계를 도입하여 개별 참가자를 독자적으로 식별하고 암호화 키 및 관련 서비스

엔드포인트 메타데이터를 DID Document에 정확하게 결합함

- W3C 글로벌 표준 데이터 모델인 Verifiable Credentials(VC) 형식을 적극 활용하여 참가자의 구체적인 역할, 조직 속성, 특정 전문 분야 소속 자격증 상태 등을 명확히 표현함

- 신뢰 권한이 사전 부여된 허가형 블록체인(Hyperledger Besu) 원장에 전체 역할 관리 및 DID 레지스트리 상태 변경 이력을 기록하여 집단적 거버넌스 체계를 구현함

- 신뢰 평가 실행 로직은 DID 유효성, 온체인 역할 상태, VC 보유 여부, 발급자의 정당성, 커넥터 정책 만족 여부 등을 종합적으로 검증하여 실시간 보안 판정을 내림

▶ 계층화된 거버넌스 역할을 체계화하고 데이터 보안을 위한 역할 분리 구조를 정립함

- 거버넌스 당국(Governance Authority)은 데이터 스페이스 내부 참여 규칙을 명확히 정의하고 신뢰에 매우 민감한 정체성 및 발행자 승인 업무를 전담함

- 네트워크 운영자(Network Operator)는 허가형 블록체인의 인프라 및 합의 과정을 안정적으로 유지하여 신뢰 기반의 높은 가용성을 완벽하게 보장함

- 신뢰된 발행자(Trusted Issuer)는 시스템 참여자 또는 커넥터에 대한 세부 속성 및 접근 권한을 담은 검증 가능한 자격증명을 무결하게 발급함

- 운영 참여자(Operational Participant)는 커넥터를 직접 운영하여 데이터 상호작용 발생 시 자신의 정체성 및 자격증명을 정식 제출하여 신뢰성을 증명함

- 민감한 개인 데이터 및 핵심 비즈니스 데이터는 온체인에 직접 저장하지 않고 외부 자격증명 형태로 보관하여 엄격한 GDPR 법적 요구사항을 준수함

▶ 공유 신뢰 도메인과 참가자 로컬 도메인 간의 계층적 아키텍처 설계를 체계화함

- 전체 시스템 구조는 네트워크 공유 신뢰 도메인(Shared Trust Domain)과 개별 참여자의 로컬 커넥터 도메인(Participant-Local Domain)으로 명확하게 격리 분리됨

- 네트워크 공유 신뢰 도메인은 허가형 블록체인 네트워크 원장, 거버넌스 스마트 계약 모듈, 그리고 자격증명 발급 서비스(Credential Issuer Service)로 통합 구성됨

- 개별 참가자의 로컬 도메인은 독립된 EDC 커넥터, 핵심 크리덴셜 저장소인 Identity Hub, 그리고 신뢰 중계 엔진인 Identity Proxy로 완전히 분리되어 개별 운영됨

- Hyperledger Besu 기반의 허가형 블록체인 환경을 구축하고 QBFT 합의 알고리즘을 통해 온체인 거버넌스 상태를 안전하게 저장함

- Identity Proxy는 커넥터와 블록체인 인프라 사이에서 신뢰를 중계하는 핵심 서비스로서 DID 해독 및 실시간 검증을 효율적으로 캡슐화하여 수행하며, Identity Hub는 로컬 자격증명 보관소 역할을 전담하여 커넥터 처리 로직과 민감한 자격증명 보관 업무를 분리함

▶ Eclipse Dataspace Components(EDC) 상호운용성을 확보하고 단계별 메커니즘의 세부 수행 흐름을 정립함

- 초기 온보딩 단계에서 신규 참여자는 거버넌스 레이어에 DID를 등록하고 역할을 부여받은 후 신뢰있는 발행자로부터 정식 참여 자격증명을 안전하게 발급받음

- 데이터 교환 시 데이터 소비자는 공급자의 DID를 먼저 확인하고 Identity Proxy를 통해 해석된 DSP 엔드포인트를 정밀하게 추출하여 커넥터 요청을 생성함

- EDC 제어 평면 내에서 카탈로그 조회 요청, 계약 협상, 데이터 전송 단계마다 프록시 및 정책 검증 레이어를 통해 식별자 및 VC 유효 상태를 실시간 재검증함

- 특정 분야 전용 자격증명(Sector-specific VC)을 기반으로 카탈로그 노출 범위를 정밀하게 필터링하여 오직 승인된 특정 전문 분야 참가자에게만 관련 데이터셋이 검색되도록 세부 접근을 제어함

▶ IDBLOCK 실증 실험을 통하여 종합적인 성능 평가를 수행하고 구체적인 측정 결과를 분석함

- 단일 노드 기반 Hyperledger Besu 인프라 환경에서 수행된 IDBLOCK 시스템 구현체 테스트 결과 신규 DID 등록 및 정보 업데이트 처리 동작에 약 2초의 블록 생성 대기 시간이 소요됨

- 시스템 프록시를 통과하는 Cold 경로 DID 해독 작업은 평균 2.59ms, VC 신규 발급은 0.94ms, VC 진위 검증 연산은 7.94ms 수준의 매우 신속하고 짧은 지연 시간을 기록함

- EDC 카탈로그 수신 요청의 평균 처리 지연 시간은 기본 기준 지표인 4.61ms에서 복합 신뢰 검증 레이어를 적용했을 때 134.65ms로 증가하여 전체 처리 과정 중 가장 큰 비중을 차지함

- 트랜잭션 계약 협상 단계(+12.54ms)와 실질적 데이터 전송 개시 단계(+16.57ms)에서 발생한 절대 오버헤드 지표는 20ms 미만의 지연 시간만을 지속적으로 유지하여 안정적인 제어면 통신 환경을 보장함

▶ 데이터 생태계의 보안성을 검증하고 탈중앙화 거버넌스 및 신뢰성을 정밀 분석함

- 시스템 내 TRUSTEE, STEWARD, ENDORSER 등 주요 제어 역할을 온체인 스마트 계약 로직으로 엄격히 강제함으로써 불투명한 오프체인 권한 남용 및 불법적 identity 등록 시도를 차단함

- 자격 증명 발급자의 정당한 권한이 박탈되거나 특정 참가자의 신뢰 인증 상태가 원위치로 변경되는 경우 온체인 트랜잭션을 실행하여 자격 취소 내역을 전체 데이터 생태계에 즉각 반영함

- 제반 권한 부여 기록과 DID 변경 이력 데이터 일체를 블록체인 네트워크에 영구적으로 기록 보관함으로써 향후 관련 규제 준수 검사 및 법적 분쟁 해결 과정을 지원하는 사후 감사 추적성을 선제 제공함

- 신뢰 검증자가 악의적 목적으로 작성된 자격 증명 오류를 철저히 가려내고 온체인 서명 검증 절차를 거침으로써 외부 프록시 데이터 침해나 DID 문서 위변조 공격 시도를 효과적으로 차단함

- 특정 중앙 기관에 의존하지 않고 데이터 주권과 보안 검증성을 완벽하게 확보함으로써, 향후 다양한 산업 분야의 연합 데이터 스페이스 구축을 위한 핵심 표준 프레임워크로 활용될 수 있음
- 카탈로그 수신 시 발생하는 처리 지연과 블록체인 인프라 운용 비용 부담 문제를 극복하기 위해, 실제 대규모 분산 노드 환경을 고려한 성능 최적화 및 고성능 분산 원장 연동 기술 개발이 필수적으로 요구됨

[출처]

- Open Research Europe, 'A blockchain-governed SSI trust architecture for EDC-based federated data spaces', 2026.07.22.