글로벌 국가를 위한 주권 인프라

Sign Foundation

개정 2.2.0 (2025년 12월 4일)

목차

1 초록

블록체인 기술은 거버넌스 및 금융 시스템을 현대화할 막대한 변혁적 잠재력을 제공하지만, 규제 통제, 개인정보 보호, 운영 주권에 대한 우려로 인해 주권 국가의 채택은 여전히 제한적입니다. 전통적인 블록체인 구현은 종종 정부에게 투명성과 개인정보 보호, 혁신과 통제 사이에서 양자택일을 강요합니다. SIGN 프레임워크는 정부에 주권적 권한을 보존하면서 글로벌 디지털 경제에 참여할 수 있는 포괄적인 디지털 자산 인프라를 제공하여 이러한 근본적인 우려를 해결하고, 궁극적으로 국익과 국제 협력 모두에 기여하는 통일된 화폐 시스템을 지향합니다.

본 기술 백서는 블록체인 인프라, 자기주권 신원 원칙을 적용한 국가 디지털 신원, 디지털 자산 관리라는 세 가지 기본 축을 기반으로 구축된 주권 디지털 인프라를 위한 혁신적인 프레임워크를 제시합니다. 디지털 신원은 모든 하위 서비스를 가능하게 하는 전제 조건 인프라 역할을 합니다. 신뢰할 수 있는 신원 시스템 없이는 국가는 금융 포용, 디지털 서비스 제공 또는 대규모 경제 개발을 달성할 수 없습니다. 이 프레임워크는 듀얼 블록체인 아키텍처(퍼블릭 레이어 2 또는 레이어 1 스마트 계약, 그리고 프라이빗 Hyperledger Fabric X), 검증 가능한 자격증명을 통해 시민 데이터 주권을 가능하게 하는 포괄적인 국가 디지털 신원 및 증명 시스템, 프로그래밍 가능한 디지털 자산 분배를 통합합니다. 이 접근 방식은 정부가 인프라와 시민 신원 모두에 대한 완전한 운영 통제 및 규제 주권을 유지하면서 블록체인의 고유한 이점(투명성, 보안 및 효율성)을 활용할 수 있도록 지원합니다.

이 프레임워크는 디지털 거버넌스의 패러다임 전환을 나타내며, 정부에 차세대 공공 서비스를 개척하고 상호 연결된 글로벌 금융 생태계에 기여할 기회를 제공합니다. 우리는 분산 원장 기술이 주권 역량을 훼손하기보다는 강화하여 국가들이 통일된 디지털 화폐 세계를 구축하는 데 협력할 수 있는 길을 만드는 방법을 보여줍니다.

2 서론

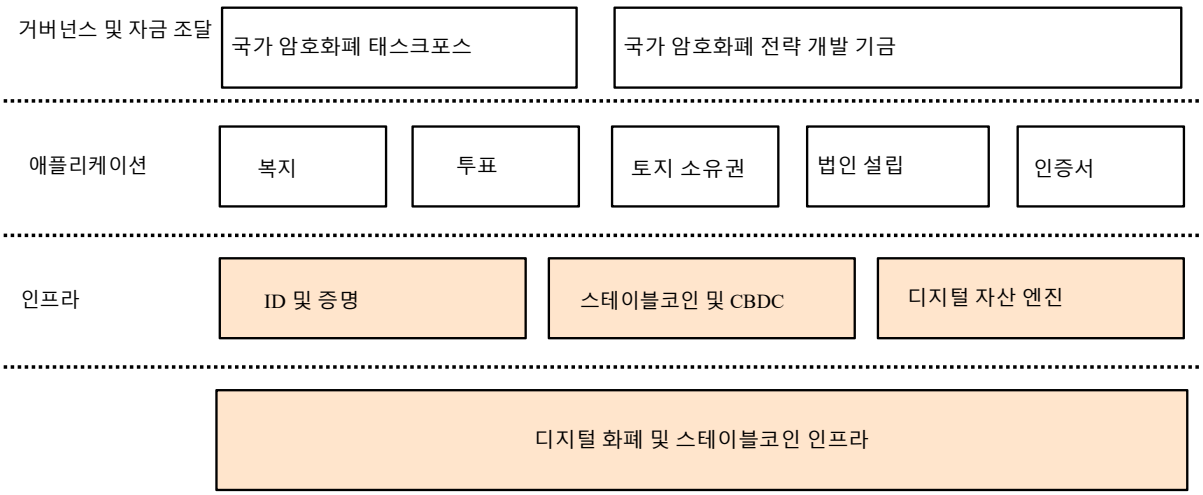
2.1 목표

디지털 거버넌스의 발전은 정부가 블록체인 기술을 통해 공공 서비스 제공을 개선할 수 있는 전례 없는 기회를 제공합니다. 전 세계 정부, 기관 및 기업들은 디지털 신원 발급, 디지털 화폐 출시, 필수 서비스 제공을 위해 온체인 시스템을 점점 더 많이 채택하고 있습니다. 기존 IT 시스템과 비교할 때 블록체인 인프라는 투명하고 실시간 감사를 가능하게 하면서 우수한 비용 효율성, 효율성 및 유지보수 용이성을 제공합니다.

이 프레임워크는 정부가 공공 행정에 필수적인 운영 통제 및 규제 권한을 유지하면서 블록체인의 고유한 이점인 투명성, 보안 및 효율성을 활용할 수 있도록 지원하는 주권적 접근 방식을 도입합니다.

- 국가 디지털 신원을 기반 인프라로 구축합니다. 신뢰할 수 있는 신원 시스템이 없으면 금융 디지털화와 디지털 서비스 제공은 달성할 수 없으며, 이는 시에라리온에서 농부의 60%가 신원 격차로 인해 디지털 농업 서비스를 받는 데 필요한 전화번호가 없는 사례에서 입증되었습니다.
- 블록체인의 보안 보장을 활용하면서 완전한 운영 권한을 유지합니다.

- 국가 규정에 부합하는 맞춤형 규정 준수 프레임워크를 구현합니다.
- 기존 정부 시스템과 원활한 통합 경로를 생성합니다.
- 공공 혜택 분배를 위한 고성능 프로그래밍 가능 시스템을 배포합니다.
- 시민 데이터 통제를 가능하게 하는 자기주권 신원 원칙을 통해 투명성 요구사항과 적절한 개인정보 보호의 균형을 맞춥니다.
- 지역 주권 자산을 표준화하고 글로벌 금융 시장에 노출시킵니다.
- 검증 가능한 자격증명을 사용하여 신원 기록(예: 국가 ID, 여권, 비자)을 표준화하여 데이터 개인정보 보호 및 소유권을 보존하면서 다른 국가와의 상호운용성을 높입니다.



이 혁신은 공공 부문 거버넌스 원칙과 최첨단 분산 원장 기술의 융합을 나타내며, 정부에 주권 역량을 훼손하기보다는 강화하는 디지털 전환을 위한 실용적인 경로를 제공합니다.

2.2 솔루션 개요

SIGN 스택은 블록체인이 기술적 기반을 제공하고, 신원 인프라가 시민의 접근과 참여를 가능하게 하며, 자산 분배가 정부 서비스를 제공하는 계층적 접근 방식을 사용합니다:

1. **디지털 화폐 및 스테이블코인 인프라**: (a) 투명한 운영을 위해 맞춤형 레이어 2 체인 또는 기존 퍼블릭 레이어 1 네트워크의 스마트 계약으로 유연하게 배포하고, (b) 개인정보를 보호하는 CBDC 운영을 위해 200,000+ TPS를 달성하는 Arma BFT 합의를 갖춘 Hyperledger Fabric X 기반 허가형 네트워크로 구성된 듀얼 경로 블록체인 아키텍처. 두 접근 방식 모두 정부가 각자의 보안 속성을 활용하면서 완전한 운영 통제를 유지할 수 있도록 합니다.
2. **디지털 신뢰 및 신원 인프라**: 국가 디지털 신원과 자기주권 신원 원칙을 통합하여 시민이 검증 가능한 자격증명을 통해 자신의 데이터를 제어할 수 있도록 하고, Sign Protocol의 온체인 증명 시스템과 결합한 포괄적인 프레임워크.

이것은 모든 디지털 서비스의 기본 전제 조건 역할을 하여 금융 포용, 정부 서비스 제공, 대규모 경제 참여를 가능하게 합니다. 신뢰할 수 있는 신원 인프라가 없으면 디지털 전환 노력은 성공할 수 없으며, 이는 시에라리온에서 기존 디지털 인프라에도 불구하고 신원 격차로 인해 시민의 3분의 2가 금융 서비스에 접근하지 못하는 사례에서 입증되었습니다.

3. **디지털 자산 엔진(TokenTable)**: 개인정보 보호 요구사항에 따라 스테이블코인 및 CBDC 인프라 모두에 걸친 분배를 지원하며, 혜택, 보조금 및 기타 정부 자산의 프로그래밍 가능한 지급을 위한 고처리량 시스템.

이 통합 접근 방식은 정부가 주권과 규제 준수를 유지하면서 블록체인 인프라에 공공 서비스를 배포할 수 있도록 합니다. 듀얼 블록체인 아키텍처는 특정 사용 사례 요구사항에 따라 투명한 공개 운영과 개인정보를 보호하는 금융 인프라 중에서 선택할 수 있는 유연성을 제공하며, 원활한 브리징 기능으로 두 시스템 간의 상호운용성을 가능하게 합니다.

3 디지털 화폐 및 스테이블코인 인프라

블록체인 인프라는 불변성, 투명성, 탈중앙성을 제공하며 디지털 정부 서비스의 기술적 기반을 제공합니다. 그러나 시에라리온과 같은 상황에서 입증되었듯이, 정교한 블록체인 인프라만으로는 접근을 가능하게 하는 신원 계층 없이는 시민에게 가치를 전달할 수 없습니다. 이 섹션에서는 디지털 신원 및 증명 시스템이 의존하는 블록체인 기반을 제시합니다. 블록체인이 기술적 기질 역할을 하지만, 그 위에 구축된 신원 인프라는 시민이 디지털 서비스에 참여하고 정부가 금융 포용과 대규모 서비스 제공을 달성하기 위한 전제 조건을 나타냅니다.

3.1 아키텍처 개요

정부는 분산 원장 기술의 이점을 제공하면서 주권을 보존하는 블록체인 인프라를 요구합니다. SIGN 스택은 특정 규제 요구사항 및 사용 사례에 맞게 각각 설계된 두 가지 보완적인 주권 블록체인 접근 방식을 제공합니다:

- **퍼블릭 블록체인 접근 방식**: 투명성, 글로벌 접근성, 공공 서비스 제공에 최적화된, 기존 퍼블릭 레이어 1 네트워크 위에 구축된 맞춤형 레이어 2 주권 체인.
- **프라이빗 블록체인 접근 방식**: 개인정보에 민감한 금융 운영 및 규제 준수에 최적화된 Hyperledger Fabric X 기반 CBDC 인프라.

두 접근 방식 모두 블록체인 기술의 보안, 효율성 및 투명성 이점을 활용하면서 완전한 정부 주권을 유지합니다. 정부는 어느 한 접근 방식을 독립적으로 배포하거나 두 가지를 조합하여 활용할 수 있으며, 원활한 브리징 인프라가 시스템 간의 상호운용성을 가능하게 합니다.

이 듀얼 경로 아키텍처는 현대 정부가 투명하고 전 세계적으로 접근 가능한 블록체인 서비스와 개인정보를 보호하는 금융 인프라를 모두 필요로 한다는 점을 인식합니다. 접근 방식 간의 선택 또는 두 가지 모두를 배포하기로 한 결정은 특정 규제 요구사항, 개인정보 보호 필요성 및 운영 목표에 따라 달라집니다.

3.2 퍼블릭 블록체인 접근 방식: 디지털 화폐 인프라

3.2.1 아키텍처 개요

주권 블록체인 인프라는 맞춤형 레이어 2 체인 또는 퍼블릭 레이어 1 네트워크의 스마트 계약으로 배포될 수 있습니다. 두 배포 접근 방식 모두 투명성, 글로벌 접근성, 정부 주권을 제공하면서 기존 블록체인 보안 및 네트워크 효과에 대한 접근을 제공합니다.

정부는 특정 요구사항에 따라 배포 접근 방식을 선택할 수 있습니다:

- **레이어 2 배포**: 합의 메커니즘, 블록 생성 및 체인 파라미터에 대한 완전한 통제권을 가진 독립적인 블록체인 인프라. 운영 독립성을 유지하면서 기본 레이어 보안을 상속합니다.
- **레이어 1 스마트 계약 배포**: 이더리움과 같은 기존 네트워크에서 업그레이드 가능한 스마트 계약을 통한 주권 통제. 기존 DeFi 생태계와의 직접적인 통합 및 네트워크 유동성에 대한 즉각적인 접근을 제공합니다.

두 접근 방식 모두 배포 선택과 관계없이 핵심적인 주권 역량을 제공합니다:

- 기존 네트워크의 보안 보장을 갖춘 운영 주권
- 맞춤형 접근 통제 및 규정 준수 메커니즘
- 프로토콜 업그레이드 및 파라미터 조정을 위한 유연한 거버넌스
- 국가 디지털 자산, 레지스트리 및 서비스의 기반
- 자산 브리지 또는 직접 통합을 통한 글로벌 유동성 접근 배포별 기술 고려사항은 부록 B에 제공됩니다.

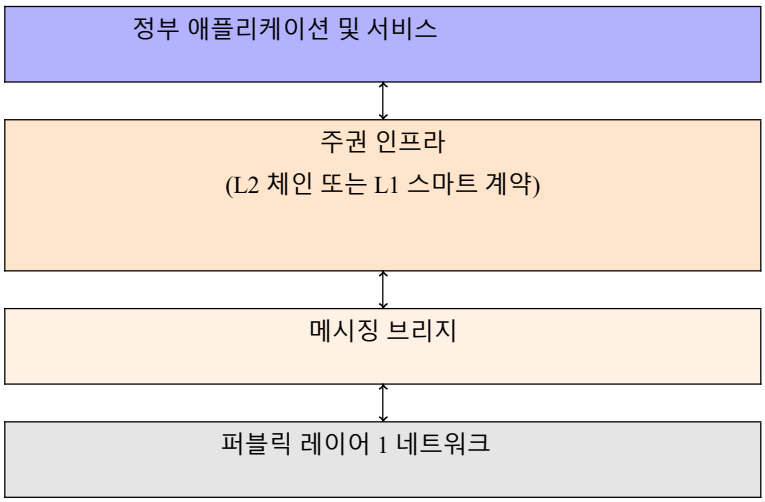


그림 1: 디지털 화폐 인프라 아키텍처

3.2.2 맞춤형 파라미터 및 거버넌스

주권 블록체인 인프라는 배포 방식과 관계없이 정부에 광범위한 맞춤화 옵션을 제공합니다:

- **접근 통제**: 규제 준수를 위한 주소 화이트리스팅 또는 블랙리스팅 구현 (L1의 경우 계약 수준, L2의 경우 체인 수준).
- **KYC 시행**: 스마트 계약 로직 또는 체인 파라미터를 통해 시행되는 신원 확인 요구사항.
- **거버넌스 구성**: 검증인 및 시퀀서(레이어 2) 또는 다중서명 권한 및 프록시 업그레이드 메커니즘(레이어 1 스마트 계약)에 대한 통제.
- **성능 최적화**: 맞춤형 블록 시간 및 처리량(레이어 2) 또는 가스 최적화 및 일괄 처리 전략(레이어 1 계약).

이러한 맞춤화 옵션을 통해 정부는 보안 이점을 유지하면서 특정 규제 프레임워크에 부합하는 블록체인 인프라를 구현할 수 있습니다. 각 배포 방식에 대한 자세한 기술 사양은 부록 B에 제공됩니다.

3.2.3 운영 통제

주권 블록체인 인프라는 정부에 인프라에 대한 포괄적인 운영 통제권을 제공합니다:

거래 수수료 정책 가장 중요한 사용성 개선 중 하나는 정부가 통제하는 거래 수수료(가스) 정책을 구현할 수 있는 능력입니다:

- **화이트리스트 기반 수수료 면제**: 정부는 특정 사용자나 서비스 제공업체를 거래 수수료에서 면제하기 위해 주소를 화이트리스트에 올릴 수 있습니다.
- **배포별 접근 방식**: 레이어 2 배포는 체인 전체의 가스 면제를 가능하게 하는 반면, 레이어 1 스마트 계약 배포는 계약 수준 로직 또는 메타 거래 패턴을 통해 수수료 후원을 구현합니다.

네트워크 통제 정부는 배포 방식과 관계없이 인프라 운영에 대한 통제권을 유지합니다:

- **레이어 2 검증인 통제**: 검증인 운영이 허용된 주체에 대한 기준을 정의하거나 화이트리스트를 작성합니다. 검증인 성능에 대한 모니터링 및 페널티를 구현합니다.
- **레이어 1 거버넌스 통제**: 프로토콜 변경을 승인하기 위해 승인된 정부 기관이 필요한 다중 서명 지갑 또는 DAO 기반 거버넌스.

프로토콜 거버넌스 주권 블록체인 인프라는 정부가 통제하는 메커니즘을 통해 운영 조정을 가능하게 합니다:

- **파라미터 조정**: 승인된 주체는 체인 거버넌스(L2) 또는 프록시 업그레이드(L1)를 통해 인프라 파라미터를 수정할 수 있습니다.
- **프로토콜 업그레이드**: 레이어 2 체인은 합의 기반 업그레이드를 지원하고, 레이어 1 계약은 원활한 업그레이드를 위해 프록시 패턴을 사용합니다.
- **비상 통제**: 필요한 경우 운영을 일시 중지하는 등 보안 사고에 대처하기 위한 메커니즘.

3.2.4 보안 모델

두 배포 방식 모두 기존 네트워크 보안을 활용하면서 운영 주권을 보존합니다:

레이어 2 배포 보안: 레이어 1에 대한 정기적인 상태 커밋은 더 넓은 네트워크에 의한 무결성 검증을 보장합니다. 사기 증명 메커니즘은 유효하지 않은 상태 전환의 감지 및 거부를 가능하게 합니다. 출구 메커니즘은 레이어 2에 문제가 발생할 경우 사용자에게 레이어 1 대체 옵션을 제공합니다.

레이어 1 스마트 계약 보안: 계약은 기본 네트워크의 검증인 집합 및 합의 메커니즘으로부터 보안 보장을 상속받습니다. 독립적인 합의 인프라가 필요하지 않습니다. 확립된 감사 관행과 실전 테스트를 거친 플랫폼은 배포 위험을 줄입니다.

두 접근 방식 모두 정부의 운영 통제를 유지하면서 기존 블록체인 네트워크의 입증된 보안 속성의 이점을 누립니다. 자세한 보안 고려사항은 부록 B에 제공됩니다.

3.2.5 글로벌 금융 접근성

국가적 프라이빗 블록체인을 만드는 것과 비교하여, 이 아키텍처는 주권 블록체인 인프라를 사용하여 표준화된 지역 금융 자산(예: ERC-20 스테이블코인 및 ERC-721 토큰화된 실물 자산)을 다른 글로벌 자산(예: BNB, ETH, WBTC, USDC, EURC 등)과 자유롭게 브리징하고 거래할 수 있게 합니다.

3.2.6 사용 사례

주권 블록체인 인프라는 여러 정부 애플리케이션의 기반 역할을 합니다:

- **국가 스테이블코인 및 CBDC**: 정부 지원 디지털 화폐의 발행 및 관리.
- **자산 토큰화**: 국가 자산, 토지 소유권 및 기타 정부 통제 자원의 표현.
- **결제 시스템**: 효율적이고 투명한 국가 주권 결제 인프라.
- **디지털 레지스트리**: 재산, 사업자 면허, 인증, 허가 등을 위한 안전하고 불변하는 레지스트리.

- **투표 시스템**: 투명하고, 비공개적이며, 검증 가능한 투표 메커니즘.

이러한 사용 사례는 배포 선택과 관계없이 달성할 수 있습니다. 배포 결정은 성능 요구사항, DeFi 통합 선호도 및 운영 독립성 필요성을 포함한 특정 정부 우선순위에 따라 달라집니다. 자세한 배포 결정 기준은 부록 B에 제공됩니다.

3.3 프라이빗 블록체인 접근 방식: Hyperledger Fabric X CBDC

3.3.1 허가형 네트워크 아키텍처

퍼블릭 블록체인 접근 방식은 투명성과 글로벌 접근성을 제공하지만, 중앙은행 디지털 화폐(CBDC)는 퍼블릭 EVM 블록체인에서는 충족시킬 수 없는 개인정보 보호 보장을 요구합니다. SIGN 스택의 프라이빗 블록체인 접근 방식은 Hyperledger Fabric X를 활용하여 개인정보에 민감한 금융 운영을 위해 특별히 설계된 주권적이고 허가된 인프라를 제공합니다. Fabric X는 모놀리식 피어를 독립적으로 확장 가능한 마이크로서비스로 분해하는 Hyperledger Fabric의 근본적인 재설계를 나타내며, 병렬 검증을 위한 거래 종속성 그래프와 Arma 샤딩 비잔틴 장애 허용 순서 지정 서비스를 포함한 혁신을 통해 초당 200,000건 이상의 거래 처리량을 달성합니다.

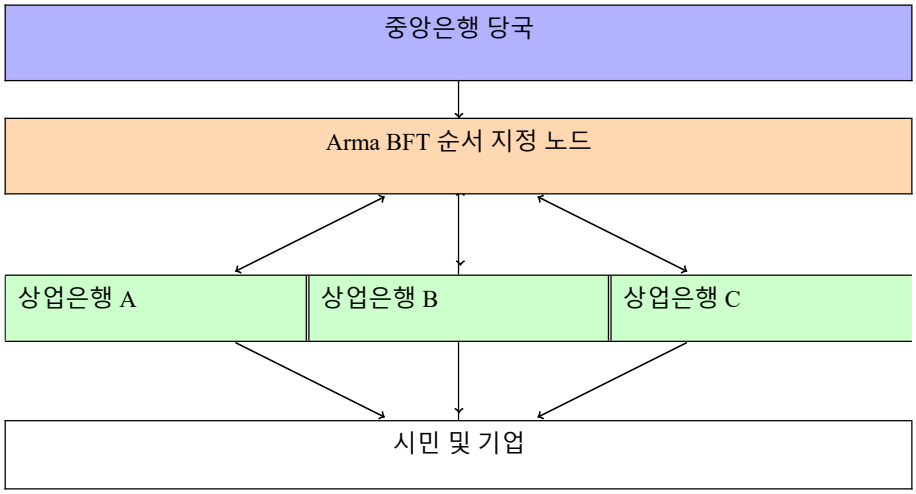


그림 2: Hyperledger Fabric X CBDC 네트워크 아키텍처

허가형 네트워크 아키텍처는 아키텍처 혁신을 통해 전례 없는 성능을 제공하면서 완전한 중앙은행 주권을 보장합니다:

- **중앙은행 당국**: 중앙은행은 Arma BFT 순서 지정 노드(라우터, 배치기, 합의 및 어셈블러 구성 요소)의 소유권을 통해 네트워크에 대한 완전한 통제권을 유지합니다.
- **마이크로서비스 아키텍처**: 피어는 코디네이터, 서명 검증기, 검증-커밋터를 포함한 독립적으로 확장 가능한 마이크로서비스로 분해되어 네트워크 대역폭, CPU 및 디스크 I/O 전반에 걸친 수평적 확장을 가능하게 합니다.
- **거래 종속성 그래프**: 여러 블록에 걸쳐 거래를 병렬로 검증하여 순차적 병목 현상을 제거하고 처리량을 극적으로 증가시킵니다.

- **샤딩된 분산 데이터베이스**: 백엔드 스토리지는 향상된 성능과 복원력을 위해 여러 데이터베이스 샤드에 분산됩니다.
- **상업은행 참여**: 중앙은행이 최종 권한을 보유하는 동안 상업은행은 거래를 검증하고 원장 사본을 유지하는 피어 노드를 운영합니다.
- **인증 기관 계층 구조**: X.509 인증서 기반 신원 관리는 승인된 주체만 네트워크에 참여할 수 있도록 보장합니다.

3.3.2 개인정보 보호 우선 설계

Hyperledger Fabric X CBDC 구현은 고급 암호화 메커니즘과 네임스페이스 격리를 통해 개인정보 보호를 우선시합니다:

네임스페이스 아키텍처 Fabric X는 네임스페이스 파티셔닝을 갖춘 단일 채널 아키텍처를 활용하여 성능을 유지하면서 다양한 CBDC 운영을 분리합니다:

- **거액 결제용 네임스페이스(wCBDC)**: 은행 간 결제 및 거액 이체를 위한 전용 네임스페이스로, 기존 RTGS 시스템과 유사한 투명성을 가집니다.
- **소액 결제용 네임스페이스(rCBDC)**: 송금인, 수취인, 규제 기관만 거래 세부 정보에 접근할 수 있는 강력한 개인정보 보호 요구사항을 갖춘 시민 및 기업 거래를 위한 별도의 네임스페이스.
- **규제용 네임스페이스**: 규정 준수 및 통화 정책 운영을 위한 적절한 접근 통제 기능을 갖춘 중앙은행 감독 네임스페이스.
- **고유한 승인 정책**: 각 네임스페이스는 자체 승인 정책에 의해 관리되어 세분화된 접근 통제 및 검증 요구사항을 가능하게 합니다.

Fabric Token SDK를 통한 영지식 증명 개인정보 보호 Fabric X는 UTXO(미사용 거래 출력값) 모델과 함께 Fabric Token SDK를 사용하여 암호화 기술을 통해 구성 가능한 개인정보 보호 수준을 제공합니다:

- **구성 가능한 개인정보 보호 수준**: 거래 개인정보 보호는 네임스페이스 및 사용 사례 요구사항에 따라 선택되는 영지식 증명을 사용하여 완전히 투명한 것부터 완전히 난독화된 것까지 다양합니다.
- **UTXO 거래 모델**: 토큰 이동은 거래가 미사용 출력을 소비하고 새로운 출력을 생성하는 방향성 비순환 그래프를 통해 추적되어 효율적인 개인정보 보호 운영을 가능하게 합니다.
- **소액 결제용 CBDC의 높은 개인정보 보호 수준**: rCBDC 거래는 고급 ZKP 기술을 활용하여 거래 세부 정보가 송금인, 수취인 및 지정된 규제 당국에만 표시되도록 보장하면서 암호화 무결성을 유지합니다.
- **거액 결제용 CBDC의 투명성**: wCBDC 거래는 은행 간 운영에 적합한 기존 실시간 총액 결제(RTGS) 시스템과 유사한 투명성 수준으로 운영됩니다.

- **선택적 공개**: 영지식 증명은 전체 거래 세부 정보를 공개하지 않고 특정 거래 속성(예: 이체 한도 준수)을 증명할 수 있게 합니다.
- **규제 기관 접근**: 지정된 규제 당국은 규정 준수, 감사 및 통화 정책 목적으로 거래 데이터에 대한 암호화된 접근 권한을 유지합니다.

3.3.3 듀얼 CBDC 모델

이 구현은 별개의 거액 결제용 및 소액 결제용 CBDC 모델을 지원합니다:

거액 결제용 CBDC (wCBDC)

- **네임스페이스 분리**: 고유한 승인 정책을 가진 전용 거액 결제용 네임스페이스 내에서 운영됩니다.
- **은행 간 결제**: 금융 기관 간의 거액 이체.
- **RTGS 수준의 투명성**: 중앙은행 감독 하의 은행 간 운영에 적합한 기존 실시간 총액 결제 시스템과 유사한 거래 투명성.
- **실시간 총액 결제**: 최종성을 가진 즉시 결제.
- **지급준비금 관리**: 기존 중앙은행 지급준비금 시스템과의 통합.

소액 결제용 CBDC (rCBDC)

- **네임스페이스 분리**: 고유한 승인 정책을 가진 전용 소액 결제용 네임스페이스 내에서 운영됩니다.
- **소비자 거래**: 시민과 기업을 위한 일상적인 결제.
- **강화된 개인정보 보호**: 영지식 증명을 활용하여 거래 세부 정보가 송금인, 수취인 및 지정된 규제 당국에만 보이도록 보장하여 시민의 금융 프라이버시를 보호합니다.
- **프로그래밍 가능한 화폐**: 시간 잠금 전송, 반복 결제, 규정 준수 자동화를 위한 토큰 기반 조건부 결제 기능.
- **오프라인 기능**: 연결성이 낮은 환경에서의 오프라인 거래 지원.
- **금융 포용**: 은행 서비스를 받지 못하는 인구를 위한 접근 가능한 디지털 결제.

3.3.4 기술적 구현

Arma BFT 합의 및 중앙은행 통제

- **샤딩된 비잔틴 장애 허용**: Arma는 최대 3분의 1의 비잔틴(악의적) 노드를 허용하는 BFT 합의를 통해 향상된 보안을 제공하며, 충돌 장애 허용 시스템보다 강력한 보증을 제공합니다.

- **4개 구성 요소 아키텍처**: Arma는 라우터 노드(거래 검증 및 라우팅), 배치기 노드(거래 그룹화), 합의 노드(배치 증명의 전체 순서 지정), 어셈블러 노드(최종 블록 구성)로 구성됩니다.
- **중앙은행 권한**: 중앙은행은 합의 노드를 운영하고 통제하며, 거래 순서 지정 및 네트워크 거버넌스에 대한 최종 권한을 유지합니다.
- **관심사 분리**: 거래 검증은 합의 순서 지정과 분리되며, 합의는 전체 거래 페이로드가 아닌 압축된 배치 증명에 대해서만 작동하여 처리량을 극적으로 증가시킵니다.
- **수평적 확장성**: 각 구성 요소 유형은 여러 시스템에 걸쳐 독립적으로 확장될 수 있어 계산 리소스의 선형적 확장을 가능하게 하고 초당 100,000건 이상의 거래 처리량을 달성합니다.
- **결정론적 순서 지정**: 감사 및 규정 준수를 위한 검열 저항 메커니즘을 갖춘 보장된 거래 순서 지정.
- **비상 통제**: 중앙은행은 보안 사고 발생 시 네트워크 운영을 일시 중지할 수 있습니다.

Fabric Token SDK를 통한 CBDC 토큰 운영

- **UTXO 기반 토큰 모델**: CBDC 토큰은 방향성 비순환 그래프가 토큰 이동을 추적하는 미사용 거래 출력 모델을 활용하며, 각 거래는 미사용 출력을 소비하고 새로운 출력을 생성합니다.
- **거래 협상 프로토콜**: 기존 체인코드를 Fabric-Smart-Client를 사용한 P2P 거래 협상으로 대체하여 더 효율적이고 개인정보를 보호하는 운영을 가능하게 합니다.
- **핵심 CBDC 운영**: 암호화 보증 및 감사 가능성을 갖춘 토큰 발행, 이전, 승인된 이전 및 상환.
- **자동화된 규정 준수**: 토큰 운영에 통합된 AML/CFT 확인, 이체 한도 시행 및 자동화된 규제 보고.
- **프로그래밍 가능한 결제**: 시간 잠금, 다중 서명 요구사항, 규정 준수 증명 및 기타 프로그래밍 가능한 조건에 기반한 조건부 토큰 이전.
- **지갑 관리**: 소유한 미사용 출력을 추적하고 투명 및 개인정보 보호 거래 모두를 위한 키를 관리하는 암호화 지갑 인프라.

ISO-20022를 통한 국제 금융 메시징 규정 준수

- **메시지 형식**: 국가 간 호환성을 위한 표준 메시지 구조.
- **결제 지시**: 표준화된 결제 개시 및 상태 메시징.
- **규제 보고**: 표준 형식의 규제 보고서 자동 생성.

- **국제 상호운용성**: 글로벌 금융 인프라와의 원활한 통합.

3.3.5 사용 사례

Hyperledger Fabric X CBDC 인프라는 포괄적인 주권 디지털 화폐 운영을 지원합니다:

- **주권 CBDC 발행**: 디지털 화폐 발행 및 분배에 대한 완전한 통제.
- **개인정보 보호 결제**: 엄격한 개인정보 보호 요구사항을 충족하는 기밀 거래.
- **국가 간 CBDC**: 다른 중앙은행과의 국제 CBDC 이체.
- **프로그래밍 가능한 금융 상품**: 조건부 이체 및 규정 준수 자동화를 포함한 복잡한 금융 상품을 위한 토큰 기반 프로그래밍 가능 운영.
- **실시간 결제**: 거액 및 소액 결제 거래 모두에 대한 즉시 결제.
- **금융 포용 프로그램**: 소외 계층을 위한 접근 가능한 디지털 화폐.

3.4 브리징 인프라

3.4.1 CBDC-스테이블코인 브리지 아키텍처

SIGN 스택은 개인정보 보호에 중점을 둔 Hyperledger Fabric X CBDC와 투명한 퍼블릭 블록체인 스테이블코인 시스템 간의 원활한 가치 이전을 가능하게 하는 정교한 브리징 인프라를 포함합니다.

3.4.2 브리지 운영

양방향 전환 브리지는 CBDC와 스테이블코인 간의 아토믹 스왑을 가능하게 합니다:

- **CBDC에서 스테이블코인으로**: 시민은 퍼블릭 블록체인 접근을 위해 개인 CBDC 보유액을 투명한 스테이블코인으로 전환할 수 있습니다.
- **스테이블코인에서 CBDC로**: 사용자는 개인정보에 민감한 거래를 위해 스테이블코인 보유액을 CBDC로 전환할 수 있습니다.
- **아토믹 운영**: 전환 작업은 아토믹(원자적)하여 이중 지불이나 자금 손실을 방지합니다.

중앙은행 통제 브리지 운영은 중앙은행의 주권을 유지합니다:

- **환율 관리**: 중앙은행이 CBDC-스테이블코인 환율을 통제합니다.
- **전환 한도**: 개인 및 총 전환에 대한 구성 가능한 한도.
- **규정 준수 통합**: 브리지 거래에 적용되는 AML/CFT 확인.
- **비상 중단**: 필요한 경우 중앙은행은 브리지 운영을 중단할 수 있습니다.

3.5 구현 전략

3.5.1 의사결정 프레임워크

정부는 특정 요구사항에 따라 블록체인 접근 방식을 선택해야 합니다:

사용 사례	권장 접근 방식	근거
공공 서비스	퍼블릭 블록체인 스테이블코인	투명성, 감사 가능성
금융 결제	둘 다	개인정보 보호 또는 투명성
국제 무역	둘 다	유연성, 호환성
사회적 혜택	퍼블릭 블록체인 스테이블코인	투명성, 효율성
은행 업무	Hyperledger Fabric X CBDC	개인정보 보호, 규제

표 1: 블록체인 접근 방식 결정 매트릭스

3.5.2 배포 패턴

병렬 배포 대부분의 정부는 두 가지 접근 방식을 모두 배포함으로써 이점을 얻을 수 있습니다:

- **보완적 시스템**: 각 시스템은 고유한 사용 사례를 최적으로 제공합니다.
- **사용자 선택**: 시민은 각 거래에 적합한 결제 방법을 선택할 수 있습니다.
- **위험 분산**: 다양한 인프라는 단일 실패 지점을 줄입니다.
- **미래 유연성**: 진화하는 규제 및 기술 요구사항에 대비합니다.

단계적 이전 정부는 단계적 접근 방식을 구현할 수 있습니다:

1. **퍼블릭 블록체인 스테이블코인**: 투명한 서비스를 위해 주권 블록체인 인프라(레이어 2 또는 레이어 1 스마트 계약)를 배포합니다.
2. **CBDC 파일럿**: 특정 금융 사용 사례를 위해 Hyperledger Fabric X CBDC를 구현합니다.
3. **브리지 통합**: 통제된 브리징 인프라로 두 시스템을 연결합니다.
4. **전면 운영**: 완전한 주권 디지털 화폐 생태계.

4 디지털 신뢰 및 신원 인프라

4.1 개요

이전 섹션에서 제시된 블록체인 기반 위에, 이 섹션에서는 시민과 기관이 디지털 서비스에 접근하고 상호 작용할 수 있게 하는 신원 인프라를 소개합니다. 디지털 신뢰 및 신원 인프라는 국가 디지털 신원과 자기주권 신원 원칙 및 블록체인 기반 증명 기능을 결합하여 모든 디지털 정부 서비스의 기본 전제 조건을 나타냅니다. 이 통합 프레임워크는 신뢰할 수 있는 신원 인프라 없이는 국가가 금융 포용, 디지털 서비스 제공 또는 대규모 경제 발전을 달성할 수 없음을 인식합니다. 시에라리온에서 입증되었듯이, 신원 격차는 연쇄적인 장벽을 만듭니다: 시민들이 금융 서비스에 접근하는 것을 막고, 농부들이 농업 보조금을 받는 것을 막으며, 기본 디지털 인프라가 존재함에도 불구하고 취약 계층이 사회 보호 프로그램에서 제외되게 합니다.

이 프레임워크는 두 가지 보완적인 구성 요소로 이루어져 있습니다: (1) 검증 가능한 자격증명을 통해 시민 데이터 주권을 가능하게 하는 자기주권 신원 원칙에 기반한 국가 디지털 신원 시스템, 그리고 (2) 블록체인 환경 전반에 걸친 암호화 검증을 위한 Sign Protocol의 온체인 증명 시스템. 이 두 구성 요소는 함께 다른 모든 디지털 서비스가 의존하는 기본 계층을 제공합니다.

4.2 국가 디지털 신원 및 자기주권 신원

4.2.1 기반 인프라로서의 신원

디지털 신원은 애플리케이션이 아닌 인프라로 기능합니다. 인터넷 연결 없이는 인터넷 서비스가 존재할 수 없듯이, 디지털 경제는 디지털 신원 없이는 기능할 수 없습니다. 국가적 구현 사례는 이러한 전제 조건을 보여줍니다. 예를 들어, 시에라리온에서는 시민의 73%가 신원 번호를 가지고 있지만 신분증을 소지한 사람은 5%에 불과하여 66%의 금융 소외, 60%의 농부가 디지털 농업 서비스를 받지 못하며, 기존 결제 인프라에도 불구하고 사회 보호 프로그램이 취약 계층에 도달하지 못하는 결과를 낳고 있습니다.

순차적 의존성은 명확합니다: 신뢰할 수 있는 신원은 금융 계좌 생성을 가능하게 하고, 이는 디지털 결제를 가능하게 하며, 이는 정부 서비스에 대한 접근을 가능하게 하고, 이는 경제 참여를 가능하게 합니다. 첫 번째 단계 없이는 기술적 정교함과 관계없이 후속 서비스는 접근할 수 없습니다. 이 프레임워크는 디지털 전환의 장애물을 제거하는 기본 인프라 계층으로서 신원을 다룹니다.

4.2.2 자기주권 신원 원칙

자기주권 신원(SSI)은 중앙 집중식 신원 관리에서 시민이 통제하는 디지털 신원으로의 패러다임 전환을 나타냅니다:

- **사용자 통제 및 동의**: 시민은 자신의 신원 데이터를 완전히 통제하며, 언제 누구와 자격증명을 공유할지 결정합니다. 중앙 기관은 시민의 개입 없이 일방적으로 신원 정보에 접근, 수정 또는 철회할 수 없습니다.
- **이동성 및 지속성**: 디지털 신원은 단일 조직이나 플랫폼과 독립적으로 지속됩니다. 시민은 신원 발급자의 허가 없이 여러 맥락(정부 서비스, 금융 기관, 민간 부문)에 걸쳐 자격증명을 제시할 수 있습니다.

- **설계 기반 개인정보 보호**: 신원 시스템은 선택적 공개를 통해 기술적인 개인정보 보호를 구현하여, 시민이 불필요한 개인 정보를 공개하지 않고 특정 속성(나이, 시민권, 자격)을 증명할 수 있게 합니다.
- **보안 및 암호화 검증**: 공개-개인 키 암호화는 수학적으로 검증 가능한 신원 주장을 가능하게 합니다. 검증자는 발급 기관에 연락하지 않고도 자격증명의 진위 여부를 암호학적으로 확인할 수 있어 오프라인 검증이 가능하고 시스템적 종속성을 줄입니다.
- **표준을 통한 상호운용성**: W3C 호환 분산 식별자(DID)와 검증 가능한 자격증명은 주권을 보존하면서 국경을 넘나드는 인식과 서로 다른 국가 시스템 간의 상호운용성을 가능하게 합니다.

4.2.3 검증 가능한 자격증명 프레임워크

이 프레임워크는 W3C 검증 가능한 자격증명 데이터 모델을 구현하여 디지털 자격증명 발급, 제시 및 검증에 대한 표준화된 접근 방식을 확립합니다:

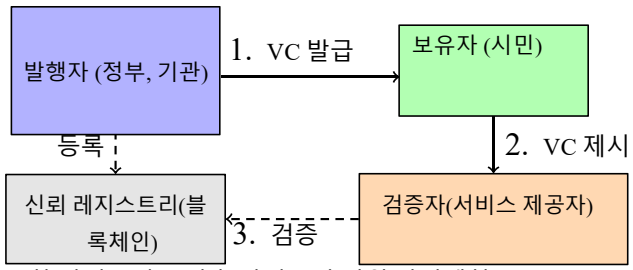


그림 3: 검증 가능한 자격증명을 갖춘 자기주권 신원 아키텍처

자격증명 수명 주기:

- **발급**: 정부 기관 또는 승인된 기관이 암호화 서명된 자격증명(교육 졸업장, 전문 면허, 신원 문서)을 생성하여 시민의 디지털 지갑으로 발급합니다. 자격증명에는 보유자에 대한 주장(이름, 생년월일, 자격)이 발급자의 개인 키로 서명되어 포함됩니다.
- **저장**: 시민은 자신의 기기에 있는 비수탁형 디지털 지갑에 자격증명을 저장하여 자격증명 접근에 대한 단독 통제권을 유지합니다. 지갑은 여러 발급자의 다양한 자격증명을 관리하기 위한 사용자 친화적인 인터페이스를 제공합니다.
- **제시**: 서비스에 접근할 때 시민은 관련 자격증명을 검증자에게 선택적으로 제시합니다. 선택적 공개는 예를 들어 정확한 생년월일을 공개하지 않고 연령 자격을 증명하는 등 필요한 속성만 공유할 수 있게 합니다.
- **검증**: 서비스 제공자는 블록체인 기반 신뢰 레지스트리에 등록된 발급자의 공개 키와 대조하여 디지털 서명을 확인하고, 자격증명이 변조되거나 폐지되지 않았음을 암호학적으로 검증합니다.

- **폐지**: 발급자는 필요한 경우(만료된 면허, 위조 문서) 블록체인에 기록된 폐지 레지스트리를 통해 자격증명을 폐지할 수 있으며, 검증자는 검증 과정에서 이를 확인합니다.

4.2.4 디지털 지갑 및 신뢰 레지스트리 비수탁형 디지

털 지갑:

디지털 지갑은 신원 인프라의 시민 대상 구성 요소 역할을 하며, 검증 가능한 자격증명의 안전한 저장 및 관리를 제공합니다:

- **기기 수준 보안**: 기기가 손상되더라도 무단 접근을 방지하기 위해 하드웨어 기반 암호화를 사용하여 기기 보안 영역(iOS Secure Enclave, Android Trusty)에 저장된 자격증명.
- **생체 인증**: 지갑 접근은 기기 PIN과 결합된 생체 인증(지문, 얼굴 인식)으로 보호되어 자격증명 소유자만 자격증명을 제시할 수 있도록 보장합니다.
- **자격증명 관리 인터페이스**: 사용자 친화적인 인터페이스를 통해 시민은 보유한 자격증명을 보고, 각 자격증명에 어떤 정보가 포함되어 있는지 이해하고, 공유 권한을 제어할 수 있습니다.
- **오프라인 기능**: 지갑은 QR 코드나 NFC를 사용하여 오프라인 자격증명 저장 및 제시를 지원하여 인터넷 연결 없이도 서비스 접근을 보장합니다. 이는 농촌 및 소외 인구에게 중요합니다.
- **크로스 플랫폼 지원**: 모바일 애플리케이션(iOS, Android)과 웹 기반 지갑은 다양한 기기와 기술 숙련도 수준에 걸쳐 접근성을 보장합니다.

블록체인 기반 신뢰 레지스트리:

신뢰 레지스트리는 자격증명 발급자의 정당성을 검증하기 위한 권위 있는 출처를 제공합니다:

- **발급자 등록**: 정부 기관 및 승인된 기관은 자신의 분산 식별자(DID)와 공개 키를 온체인에 등록하여 합법적인 자격증명 발급자로 확립합니다.
- **스키마 관리**: 표준화된 자격증명 스키마(신원 문서, 학력 자격증명, 전문 면허)를 온체인에 게시하여 일관성과 상호운용성을 보장합니다.
- **폐지 인프라**: 온체인에 유지되는 실시간 폐지 목록은 검증자가 발급 기관에 연락하지 않고도 자격증명의 유효성을 확인할 수 있게 하여, 폐지된 자격증명의 사용을 방지하면서 개인정보를 보호합니다.
- **거버넌스 프레임워크**: 발급자 인증, 자격증명 표준 및 분쟁 해결 절차를 정의하는 명확한 정책을 블록체인 기반 거버넌스 메커니즘을 통해 구현합니다.

4.2.5 참조 구현: 부탄 국가 디지털 신원

부탄은 2023년 10월 세계 최초로 SSI 기반 국가 신원 시스템을 출시하며 국가 규모의 자기주권 신원 구현 가능성을 입증했습니다:

구현 성과:

- **국가 규모 배포**: 75만 명 이상의 시민 등록(인구의 70% 이상 목표), SSI를 공식 국가 신원 인프라로 확립.
- **법적 기반**: 2023년 국가 디지털 신원법은 포괄적인 법적 프레임워크를 제공하며, 디지털 신원을 헌법에 명시된 기본권으로 인정합니다.
- **블록체인 진화**: Hyperledger Indy에서 Polygon(2024년)으로, 그리고 이더리움(2026년 1분기 목표)으로 이전하는 등 플랫폼 선택에 대한 실용적인 접근 방식을 통해 성능, 탈중앙화 및 보안 요구사항의 균형을 맞추는 유연성을 보여줍니다.
- **표준 준수**: W3C 검증 가능한 자격증명 및 DID를 구현하여 국제적 상호운용성을 보장하고 기술 발전에 대비합니다.
- **포괄적인 자격증명**: 기본 신원을 넘어, 시스템은 학력 자격증명(부탄 왕립 대학교), SIM 등록을 위한 휴대폰 번호 인증, 문서 인증을 위한 디지털 서명을 발급합니다.
- **개발자 생태계**: 국가 해커톤과 개발자 참여 프로그램이 혁신을 주도하며, 13개 이상의 팀이 정부 및 민간 부문 사용 사례 전반에 걸쳐 NDI 통합 애플리케이션을 구축하고 있습니다.

주요 성공 요인:

- **정부의 의지**: 전담 국가 법률을 통한 강력한 정치적 의지와 법적 지원.
- **개방형 표준**: W3C 표준 및 UN 디지털 공공재 연합이 보증하는 CREDEBL 플랫폼 채택으로 상호운용성 및 지속 가능성 보장.
- **단계적 접근**: 전국적 시행 전 초기 파일럿 프로그램을 통해 실제 피드백을 기반으로 반복적인 개선을 허용합니다.
- **시민 중심 설계**: 생체 인증, 기기 수준 암호화 및 직관적인 지갑 인터페이스는 사용자 경험과 보안을 우선시합니다.

4.2.6 표준 준수 및 상호운용성

이 프레임워크는 국가 주권을 보존하면서 글로벌 상호운용성을 보장하는 국제적으로 인정된 표준을 구현합니다:

표준 준수는 국경 간 자격증명 인식을 가능하게 합니다: 한 국가에서 발급된 전문 면허를 다른 국가에서 암호학적으로 검증할 수 있고, 학력 자격증명은 관할 구역을 넘어 원활하게 이전되며, 신원 확인은 각 국가가 자국의 신원 인프라에 대한 주권적 통제를 유지하면서 전 세계적으로 작동합니다.

표준	적용
W3C 검증 가능한 자격증명 2.0	모든 정부 발급 디지털 자격증명을 위한 핵심 자격증명 데이터 모델
W3C 분산 식별자 (DID)	시민과 기관을 위한 전 세계적으로 고유하고 암호학적으로 검증 가능한 식별자
W3C 비트스트링 상태 목록	개인정보 침해 없이 실시간 자격증명 폐지 확인
VC용 OpenID(OIDC4VCI/VP)	지갑 상호운용성을 가능하게 하는 자격증명 발급 및 제시 프로토콜
ISO/IEC 18013-5/7	모바일 운전면허증 및 정부 ID 호환성

표 2: 신원 스택 표준 준수

4.3 Sign Protocol: 증명 아키텍처

Sign Protocol은 다양한 형태의 암호화 증명을 생성, 검증 및 관리할 수 있는 포괄적인 온체인 증명 프레임워크를 제공합니다:

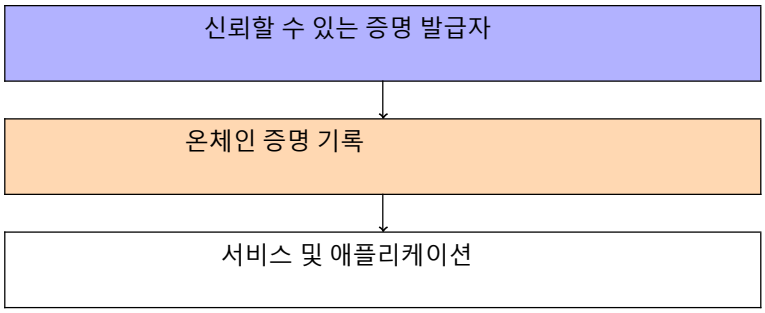


그림 4: Sign Protocol 증명 아키텍처

4.4 증명 프레임워크

Sign Protocol은 다음과 같은 기능을 갖춘 유연한 증명 프레임워크를 구축합니다:

- **증명 생성**: 승인된 주체는 다양한 주제에 관한 암호화 증명을 발급할 수 있습니다.
- **검증 메커니즘**: 증명의 진위 여부와 유효성을 검증하기 위한 여러 경로.
- **폐지 인프라**: 필요한 경우 증명을 폐지하기 위한 메커니즘.
- **만료 관리**: 자동 만료 기능이 있는 시간 제한적 증명 지원.
- **선택적 공개**: 증명 내용의 부분 공개를 허용하는 암호화 메커니즘.

이 프레임워크는 투명한 퍼블릭 블록체인 인프라와 개인정보를 보호하는 Hyperledger Fabric X CBDC 인프라 모두에서 사실, 자격증명 또는 주장에 대한 신뢰할 수 있는 검증을 요구하는 수많은 정부 애플리케이션의 기반을 제공합니다.

4.4.1 크로스체인 신원 통합

Sign Protocol 증명은 SIGN 스택 내의 두 블록체인 인프라에서 원활하게 작동합니다:

- **통합 신원 프레임워크**: 단일 디지털 신원 증명으로 CBDC(프라이빗) 및 스테이블코인(퍼블릭) 시스템 모두에 접근할 수 있습니다.
- **개인정보 보호 검증**: 영지식 증명을 통해 프라이빗 CBDC 인프라에 저장된 민감한 개인 데이터를 노출하지 않고 퍼블릭 체인에서 신원을 검증할 수 있습니다.
- **선택적 공개**: 시민은 특정 서비스를 위해 공개할 신원 속성을 선택할 수 있으며, 퍼블릭 블록체인과 프라이빗 블록체인 상호작용에 대해 서로 다른 개인정보 보호 수준을 사용할 수 있습니다.
- **규정 준수 브리징**: 신원 증명은 두 블록체인 환경 모두에서 일관된 AML/CFT 규정 준수를 보장합니다.

4.4.2 개인정보 보호

Sign Protocol은 검증 요구와 개인정보 보호의 균형을 맞추기 위해 영지식 증명(ZKP)을 지원합니다:

- **선택적 공개**: 사용자는 전체 데이터를 공개하지 않고 특정 속성(나이, 국적)을 증명할 수 있습니다.
- **비연결성**: 신원 사용에 대한 교차 컨텍스트 추적 방지.
- **최소 공개**: 데이터 최소화 원칙의 기술적 시행.

이러한 개인정보 보호 기능은 시스템이 필요한 검증 기능을 활성화하면서 데이터 보호 규정을 준수하도록 보장합니다.

4.5 사용 사례

Sign Protocol은 정부 운영에 필수적인 여러 증명 사용 사례를 지원합니다:

4.5.1 신원

Sign Protocol은 개인정보를 보호하고 시민이 정부 서비스와 상호 작용하는 방식을 혁신하는, 전 세계적으로 검증 가능한 디지털 신원 시스템을 가능하게 합니다. 거주자는 여권이나 주민등록증과 같은 기존 자격증명을 사용하여 등록하여 범용 디지털 신원 역할을 하는 온라인 신원 기록을 생성함으로써 실물 카드 없이도 사용할 수 있습니다. 이 시스템은 시민의 검증된 ID가 모든 디지털 서비스에 대한 인증된 계정이 되어 자산, 혜택 및 서비스 접근을 단일 온체인 신원에 연결하는 계정 연동 디지털 신원을 생성합니다.

이 접근 방식은 다음을 제공합니다:

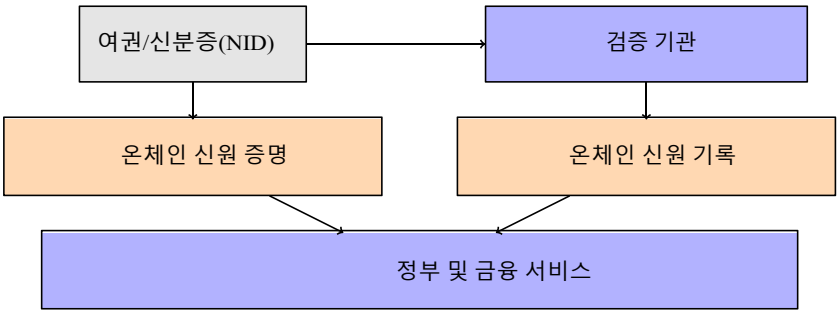


그림 5: Sign Protocol 신원 아키텍처

- **거주자 등록**: 거주자는 기존 정부 신분증(여권, 주민등록증 등)을 승인된 검증 기관에 제시하면, 기관은 신원 확인의 암호화 증명을 생성합니다.
- **범용 디지털 접근**: 검증된 신원 증명은 모든 정부 및 금융 서비스에서 범용 로그인 자격증명으로 사용됩니다.
- **글로벌 상호운용성**: 정부, 기관 또는 개인은 API나 특별한 허가 없이 온체인에서 직접 신원을 확인할 수 있습니다. 블록체인은 개방적이고 주권 중립적인 신원 레지스트리 역할을 합니다.
- **기존 시스템과의 통합**: ICAO 9303 호환 전자여권, NFC/칩 판독 및 생체 인식 시스템과 완벽하게 호환됩니다.
- **크로스체인 금융 통합**: 검증된 신원은 CBDC 계정(Hyperledger Fabric X)과 스테이블코인 계정(레이어 2) 모두에 연결될 수 있어, 개인정보를 보호하는 블록체인 인프라와 투명한 블록체인 인프라 모두에서 정부 서비스 및 금융 시스템에 원활하게 접근할 수 있습니다.

4.5.2 자격증명

Sign Protocol은 다음과 같은 자격 및 증명서 확인을 지원합니다:

- **학력 증명**: 학위, 졸업장 및 자격증 확인.
- **전문 면허**: 전문 자격 및 면허 증명.
- **교육 수료증**: 교육 프로그램 이수 확인.
- **공공 서비스 자격**: 특정 정부 직책에 대한 자격 증명.

4.5.3 재산권

Sign Protocol은 소유권 및 재산권 확인을 지원합니다:

- **토지 소유권**: 토지 등기 및 재산 경계 증명.
- **차량 등록**: 차량 소유권 및 등록 확인.
- **지적 재산권**: 특허, 상표 및 저작권 문서화.
- **디지털 자산 소유권**: 디지털 재산권 증명.

4.5.4 규제 기록

Sign Protocol은 간소화된 규제 준수를 가능하게 합니다:

- **사업자 등록**: 사업자 등록 및 정상 영업 상태 증명.
- **규제 승인**: 규제 요건 준수 확인.
- **감사 인증**: 완료된 감사 및 검사 증명.
- **수출입 허가**: 국제 무역 승인 문서화.

4.5.5 투표

Sign Protocol은 검증된 온체인 신원과 암호화된 투표용지 기록을 사용하여 안전한 디지털 투표를 가능하게 합니다. 영지식 증명은 유권자의 개인정보를 보호하면서 정확한 개표를 보장하고, 스마트 계약은 실시간으로 검증 가능한 결과를 제공합니다.

- **선거 보안**: 암호화된 검증은 사기를 방지하고 자격 있는 유권자만 참여하도록 보장합니다.
- **투명성**: 투표 비밀을 침해하지 않으면서 결과의 공개적 검증.
- **효율성**: 즉각적이고 수학적으로 검증된 결과를 통한 자동 개표.
- **접근성**: 해외 거주 시민 및 이동이 불편한 사람들을 위한 원격 투표.
- **비용 절감**: 실물 투표용지 인프라 및 수동 개표 과정 제거.

이 접근 방식은 강화된 보안과 개선된 접근성 및 투명성을 결합하여 민주적 절차를 강화합니다.

4.5.6 국경 통제

Sign Protocol은 정부가 국가 데이터 주권을 보존하면서 암호화된 블랙리스트 데이터베이스를 통해 세관 및 국경 보안을 협력적으로 관리할 수 있게 합니다. 개인 식별자는 암호화되어 온체인에 저장되므로, 국경 통제관은 여권을 스캔하여 국가 간 민감한 개인 데이터를 접근하거나 공유하지 않고도 보안 상태를 즉시 확인할 수 있습니다. 이 시스템은 여러 가지 이점을 제공합니다:

- **데이터 주권**: 국가의 민감한 데이터는 국내 통제 하에 유지되면서 국제 협력을 가능하게 합니다.
- **개인정보 보호**: 암호화 기술은 검증 과정에서 개인 정보가 노출되지 않도록 보장합니다.
- **강화된 보안**: 데이터 공유 없이 국제 보안 데이터베이스에 대한 실시간 검증.

- **운영 효율성**: 즉각적인 검증으로 처리 지연을 줄이고 국경 통과 경험을 개선합니다.
- **다자간 중립성**: 블록체인은 국제 안보 협력을 위한 중립적인 플랫폼을 제공합니다.

4.5.7 전자 비자 발급

Sign Protocol의 주권 블록체인 및 온체인 신원 시스템은 이민 서비스를 현대화하는 안전하고 효율적인 전자 비자 처리를 가능하게 합니다. 비자 신청자는 온라인으로 신청서를 제출하며, 신원 확인은 온체인에 저장된 영지식 여권 증명을 통해 이루어집니다. 스마트 계약은 처리 워크플로우를 자동화하여 투명성을 보장하고 사기나 부패의 기회를 최소화합니다. 주요 기능은 다음과 같습니다:

- **자동화된 처리**: 스마트 계약이 일상적인 처리 업무를 담당하여 관리 부담을 줄입니다.
- **신원 확인**: 기존 여권 인프라와 온체인 증명을 사용한 안전한 확인.
- **투명성**: 불변의 처리 기록은 책임성을 보장하고 처리 분쟁을 줄입니다.
- **비용 절감**: 기존의 종이 기반 시스템에 비해 관리 비용을 크게 절감합니다.
- **향상된 사용자 경험**: 신청자를 위한 실시간 상태 업데이트를 통한 빠른 비자 발급.
- **사기 방지**: 암호화된 검증으로 문서 위조 및 신원 사기를 방지합니다.

5 디지털 및 실물 자산 엔진

TokenTable은 전 세계 4,000만 명 이상의 사용자에게 서비스를 제공하는 검증된 디지털 자산 플랫폼으로, 정부의 자산 분배 및 실물 자산(RWA) 토큰화를 위한 포괄적인 인프라를 제공합니다. 이 플랫폼은 정부가 효율적으로 혜택 분배를 관리할 수 있게 하는 동시에, 부동산, 예술품, 수집품과 같은 실물 자산의 토큰화를 레지스트리 중심 프레임워크를 통해 지원합니다.

5.1 TokenTable: 플랫폼 아키텍처

TokenTable은 자산 발행 및 분배를 위한 고처리량 프로그래밍 가능 시스템을 제공합니다:

TokenTable은 정부 인프라 내에서 두 가지 주요 기능을 수행합니다: (1) 시민과 기업에 대한 혜택, 보조금 및 지급금의 효율적인 분배를 위한 **디지털 자산 분배**, 그리고 (2) 재산 등기부, 소유권 기록 및 자산 관리 시스템을 현대화하기 위한 **실물 자산 토큰화**. 이 이중 목적 아키텍처는 정부가 금융 분배와 실물 자산 디지털화 모두를 위해 통합된 플랫폼을 활용할 수 있게 합니다.

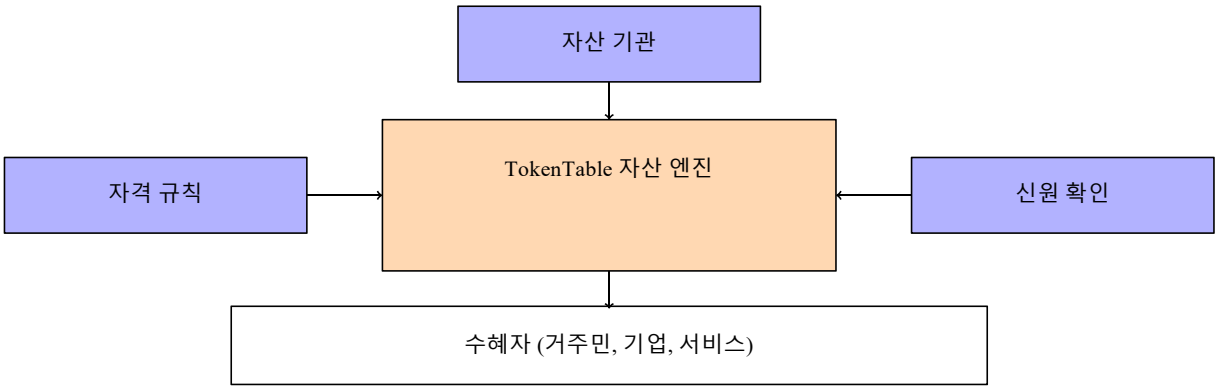


그림 6: TokenTable 아키텍처

5.2 디지털 자산 분배

다음 섹션에서는 정부 혜택, 지급금 및 보조금을 시민과 기업에 분배하는 TokenTable의 기능에 대해 설명합니다.

5.2.1 대규모 운영

TokenTable은 정부 혜택 및 지급금의 효율적인 발행 및 분배를 위해 설계되었습니다:

- **사용자 주도 일괄 처리**: 블록체인 혼잡을 최소화하면서 대규모 수혜자 그룹에 대한 대량 분배에 최적화되었습니다.
- **예약된 분배**: 연금 및 정기 보조금과 같은 반복적인 지급 지원.
- **다중 자산 지원**: 국가 디지털 통화 및 혜택 토큰을 포함한 모든 토큰화된 자산의 분배를 지원합니다.

5.2.2 신원 연계 타겟팅

TokenTable은 Sign Protocol과 통합하여 정밀한 분배 타겟팅을 가능하게 합니다:

- **검증된 수혜자**: 분배가 검증된 자격 있는 수혜자에게만 도달하도록 보장합니다.
- **속성 기반 타겟팅**: 특정 신원 속성(나이, 위치, 상태 등)에 기반한 분배.
- **중복 방지**: 중복 청구 및 지급의 기술적 방지.

이 통합은 검증된 디지털 신원이 정부 서비스와 금융 시스템 모두에 접근하는 기반이 되는 포괄적인 금융 포용 프레임워크를 만듭니다. 검증된 신원을 가진 시민은 개인정보를 보호하는 CBDC 계정(Hyperledger Fabric X)과 투명한 스테이블코인 계정(레이어 2) 모두에 원활하게 접근할 수 있어, 정부 대 시민 직접 지급을 가능하게 하고 이전에 은행 서비스를 받지 못했던 인구의 디지털 금융 서비스 접근을 확대합니다.

5.2.3 멀티체인 분배 기능

TokenTable은 SIGN 스택 내의 두 블록체인 인프라 모두에서의 분배를 지원합니다:

- **CBDC 분배**: 민감한 금융 지원 프로그램을 위한 Hyperledger Fabric X를 통한 개인정보 보호 분배.
- **스테이블코인 분배**: 투명성이 요구되는 공공 혜택 및 보조금을 위한 레이어 2를 통한 투명한 분배.
- **크로스체인 조정**: 프라이빗 및 퍼블릭 블록체인 시스템 모두에서 시민 혜택에 대한 통합된 보기.
- **지불 방법 선택**: 정부는 개인정보 보호 요구사항 및 정책 목표에 따라 분배 방법을 선택할 수 있습니다.

5.2.4 조건부 로직

TokenTable은 분배를 위한 정교한 조건부 로직을 지원합니다:

- **베스팅 일정**: 장기 혜택을 위한 시간 기반 자금 해제.
- **다단계 조건**: 여러 조건이 필요한 복잡한 자격 규칙.
- **사용 제한**: 분배된 자산의 활용 방법에 대한 제한.
- **지리적 제약**: 특정 지역이나 지방으로 사용 제한.

위의 모든 프로그래밍 기능은 정부가 분배 규칙의 기술적 시행을 통해 미묘한 정책 목표를 구현할 수 있게 합니다.

5.3 실물 자산 토큰화

정부 혜택 분배를 넘어, TokenTable은 실물 자산 토큰화를 위한 포괄적인 인프라를 제공하여 정부가 재산 등기부, 자산 소유권 추적 및 규제 준수 시스템을 현대화할 수 있도록 합니다. 이 레지스트리 중심 접근 방식은 블록체인 기술을 기존 정부 데이터베이스와 통합하여 자산 소유권 및 이전에 대한 투명하고 불변의 기록을 생성합니다.

5.3.1 레지스트리 통합

TokenTable은 기존 정부 인프라와 원활하게 연결됩니다:

- **토지 등기 시스템**: 재산 소유권 기록의 실시간 동기화를 위한 국가 토지 등기 데이터베이스와의 직접적인 통합.
- **재산 데이터베이스**: 지적 시스템, 세금 기록 및 시 재산 정보와의 연결성.
- **규제 프레임워크**: 현지 재산법, 이전 규정 및 과세 요구사항에 대한 내장된 준수.

- **레거시 시스템 브리징**: 기존 정부 데이터베이스를 블록체인 인프라와 연결하기 위한 API 및 어댑터.

이 통합 접근 방식은 정부가 기존 등기 시스템에 대한 운영 통제권을 유지하면서 블록체인의 이점을 활용할 수 있게 합니다.

5.3.2 자산 클래스

TokenTable은 여러 자산 범주에 걸친 토큰화를 지원합니다:

- **부동산**: 부분 소유 기능을 갖춘 주거, 상업 및 농업용 부동산 토큰화.
- **예술품 및 수집품**: 문화 자산, 박물관 소장품 및 귀중한 유물에 대한 디지털 출처 추적.
- **정부 자산**: 공공 인프라, 천연자원 및 국부 자산.
- **증권**: 국채, 재무 증권 및 규제된 금융 상품의 규정 준수 토큰화.

5.3.3 규정 준수 및 이전 통제

TokenTable은 자산 토큰화를 위한 정교한 규정 준수 메커니즘을 구현합니다:

- **이전 제한**: 냉각 기간, 투자자 인증 및 관할권 제한을 포함한 자산 이전에 대한 규제 요구사항을 시행하는 프로그래밍 가능한 규칙.
- **화이트리스팅**: 특정 자산 클래스를 검증된 자격 있는 당사자만 취득할 수 있도록 보장하는 신원 연계 이전 허가.
- **규제 보고**: 세무 당국, 토지 등기소 및 금융 규제 기관에 대한 자동화된 규정 준수 보고.
- **KYC/AML 통합**: 포괄적인 고객 확인 및 자금 세탁 방지 준수를 위해 Sign Protocol 신원 증명 활용.

5.3.4 출처 및 소유권

TokenTable은 자산 이력 및 소유권에 대한 불변의 기록을 생성합니다:

- **소유권 체인**: 모든 소유권 이전 및 거래에 대한 완전하고 검증 가능한 이력.
- **진위 확인**: 예술품, 수집품 및 귀중품에 대한 자산의 정당성 및 출처에 대한 암호화 증명.
- **분쟁 해결**: 법적 절차 및 소유권 분쟁을 지원하는 불변의 감사 추적.

- **국경 간 인식**: 양자 협정이나 복잡한 인증 절차 없이 자산 소유권의 국제적 확인.

레지스트리 통합, 규정 준수 통제 및 출처 추적의 조합은 정부가 규제 감독 및 법적 집행 가능성을 유지하면서 자산 관리 시스템을 현대화할 수 있게 합니다.

5.4 감사 가능성 및 투명성

TokenTable의 핵심 기능은 분배 및 토큰화 활동 전반에 걸친 포괄적인 감사 가능성입니다:

- **분배 원장**: 모든 혜택 및 지급 분배에 대한 불변의 기록.
- **자산 레지스트리**: 모든 토큰화된 실물 자산에 대한 완전한 소유권 이력 및 이전 기록.
- **실시간 모니터링**: 분배 진행 상황과 자산 토큰화 활동을 모두 모니터링하기 위한 대시보드.
- **조정 도구**: 분배를 위해 할당된 예산에 대한 자동 조정 및 자산 토큰화를 위한 외부 재산 등기부와의 동기화.
- **투명성 보고**: 총 분배 통계 및 토큰화된 자산 소유권 기록에 대한 공개적 가시성.

이러한 투명성 기능은 혜택을 분배하거나 토큰화된 자산 등기부를 관리하는 등 정부 운영의 책임성을 보장합니다.

5.5 사용 사례

TokenTable은 디지털 자산 분배와 실물 자산 토큰화 모두에서 다양한 정부 운영을 지원합니다.

5.5.1 분배 사용 사례

TokenTable은 정부 혜택 및 지급금의 효율적인 분배를 가능하게 합니다:

- **사회적 혜택**: 복지 수당, 실업 수당, 보편적 기본 소득 등의 분배.
- **연금 시스템**: 자격 있는 거주자에게 정기적인 연금 지급.
- **긴급 구호**: 위기 상황에서 긴급 자금의 신속한 분배.
- **농업 보조금**: 농부 및 농업 기업에 대한 표적 지원.
- **교육 장학금**: 교육 지원금 분배.
- **의료 혜택**: 의료 보조금 분배 관리.
- **개인정보 보호가 중요한 결제**: 익명성이 요구되는 기밀 지원 프로그램을 위한 CBDC 분배.

- **국경 간 지원**: ISO-20022 호환 CBDC 이체를 사용한 국제 원조 분배.
- **금융 포용 프로그램**: 이전에 은행 서비스를 받지 못했던 인구를 위한 CBDC 계좌 생성 및 자금 지원.

5.5.2 자산 토큰화 사용 사례

TokenTable은 자산 등기부 및 소유권 추적 현대화를 위한 인프라를 제공합니다:

- **부동산 토큰화**: 투명한 재산 소유권 추적, 부동산 부분 소유, 자동 세금 징수 및 규제 준수를 통한 간소화된 재산 이전을 가능하게 하는 디지털 토지 등기부.
- **예술 및 문화 유산**: 블록체인으로 검증된 출처를 가진 국립 박물관 소장품 및 문화 유물로, 진위 여부의 공개적 검증, 전시 이력 추적, 위조 및 불법 거래 방지를 가능하게 합니다.
- **국경 간 자산 검증**: 복잡한 양자 협정 없이 재산 소유권, 사업자 등록 및 자산 보유에 대한 국제적 인정을 통해 해외 투자, 국제 무역 및 글로벌 이동성을 위한 원활한 검증을 가능하게 합니다.

6 경제적 영향 및 가치 창출

6.1 비용 절감 및 효율성 증대

SIGN 스택은 여러 메커니즘을 통해 정부 운영에 측정 가능한 경제적 이점을 제공합니다:

- **행정 비용 절감**: 신원 확인, 혜택 분배, 규제 준수와 같은 일상적인 프로세스의 자동화는 수동 처리 비용을 크게 줄입니다.
- **사기 방지**: 암호화된 검증과 불변의 기록 보관은 혜택 프로그램, 비자 처리 및 신원 확인에서의 사기 기회를 최소화합니다.
- **실시간 감사**: 지속적인 투명성은 책임성을 향상시키면서 값비싼 정기 감사의 필요성을 제거합니다.
- **인프라 효율성**: 블록체인 인프라는 값비싼 중앙 집중식 데이터베이스 및 관련 유지보수 비용에 대한 의존도를 줄입니다.

6.2 금융 포용 및 경제 개발

이 프레임워크의 검증된 신원과 금융 서비스의 통합은 경제 참여 확대를 위한 기회를 창출합니다:

- **은행 접근성**: 검증된 온체인 신원을 가진 거주자는 이전에 KYC 장벽으로 인해 이용할 수 없었던 디지털 금융 서비스에 접근할 수 있습니다.

- **경제 통합**: 표준화된 디지털 신원은 국가 주권을 보존하면서 글로벌 금융 시스템과의 더 쉬운 통합을 가능하게 합니다.
- **투자 유치**: 간소화된 법인 설립 및 투명한 규제 절차는 국내외 투자를 유치합니다.
- **국경 간 효율성**: 표준화된 신원 및 자산 형식은 국제 무역 및 협력에서의 마찰을 줄입니다.

6.3 상호운용성

SIGN 프레임워크의 포괄적인 상호운용성 기능은 통합 비용 절감, 시장 접근 확대 및 운영 효율성 향상을 통해 상당한 경제적 가치를 창출합니다:

- **크로스체인 자산 관리**: 퍼블릭 네트워크와 프라이빗 네트워크 간의 네이티브 브리지 인프라는 비용이 많이 드는 수동 조정 프로세스를 제거하는 동시에 정부가 특정 사용 사례에 따라 투명성 및 개인정보 보호 요구사항을 최적화하여 운영 오버헤드를 줄일 수 있게 합니다.
- **국제 표준 준수**: ISO 20022 및 신흥 중앙은행 디지털 화폐 프로토콜의 구현은 글로벌 금융 네트워크와의 통합 비용을 절감하여 정부가 값비싼 맞춤형 통합 프로젝트 없이 국제 시장에 참여할 수 있게 합니다.
- **다국적 경제 조정**: 표준화된 국경 간 거래 기능은 효율적인 국제 무역 결제 및 송금을 촉진하여 기존 중개 은행 방식에 비해 거래 비용을 줄이고 결제 시간을 며칠에서 몇 분으로 단축합니다.
- **레거시 시스템 통합 가치**: 포괄적인 API 프레임워크 및 단계적 마이그레이션 도구는 디지털 전환 중 중단 비용을 최소화하여 정부가 서비스 중단 없이 인프라를 점진적으로 현대화하면서 기존 IT 투자를 보존할 수 있게 합니다.
- **민관 시장 확대**: 기존 금융 인프라와의 원활한 통합은 민간 부문 혁신 및 서비스에 대한 정부의 접근성을 확대하여 규제 감독 및 준수 요구사항을 유지하면서 민관 파트너십을 통해 새로운 수익 기회를 창출합니다.

7 시스템 통합

7.1 기존 정부 시스템과의 통합

이 프레임워크는 기존 정부 시스템과의 통합 기능을 포함합니다:

- **API 인터페이스**: 레거시 시스템과의 통합을 위한 표준 API.
- **데이터 마이그레이션 도구**: 기존 시스템에서 데이터를 마이그레이션하기 위한 유틸리티.
- **하이브리드 배포 모델**: 레거시 시스템에서 단계적으로 전환하는 것을 지원합니다.

7.2 기술 지원

상세한 문서 외에도 Sign Foundation은 소프트웨어 맞춤화 지점과 연중무휴 24시간 전담 기술 지원을 제공합니다.

8 보안 고려사항

8.1 시스템 보안

주권 인프라는 포괄적인 보안 조치를 구현합니다:

- **다층 보안**: 온체인 및 오프체인 모두에서 스택의 각 계층에 보안 통제.
- **정형 검증 및 감사**: 중요한 구성 요소는 정형 검증 및 엄격한 제3자 감사를 받습니다.
- **버그 바운티 프로그램**: 취약점의 책임 있는 공개에 대한 인센티브.

9 배포 방법론

9.1 단계적 구현

권장되는 단계적 구현 접근 방식:

1. **평가 및 계획**: 기존 시스템 및 배포 전략 평가.
2. **파일럿 배포**: 특정 사용 사례에 대한 제한된 배포.
3. **확장**: 추가 서비스 및 사용자 그룹으로 점진적 확장.
4. **완전 통합**: 정부 서비스 생태계와의 완전한 통합.

9.2 거버넌스 프레임워크

성공적인 배포에는 적절한 거버넌스 프레임워크가 필요합니다:

- **기술 거버넌스**: 기술적 변경 및 업그레이드를 관리하는 프로세스.
- **운영 거버넌스**: 일상적인 운영 감독.
- **정책 거버넌스**: 기술적 능력과 정책 목표의 일치.

10 결론

SIGN 스택은 정부에 운영 통제권과 주권을 유지하면서 블록체인 기술을 활용할 수 있는 포괄적인 솔루션을 제공합니다. 디지털 화폐 및 스테이블코인 인프라, Sign Protocol, TokenTable이라는 세 가지 통합 구성 요소를 통해 이 프레임워크는 블록체인 인프라에서 안전하고 효율적이며 투명한 공공 서비스 제공을 가능하게 합니다.

이전에 정부의 블록체인 기술 채택을 방해했던 주요 과제를 해결함으로써, 이 프레임워크는 공공 서비스의 디지털 전환을 위한 실용적인 길을 제공합니다. 구성 요소의 맞춤형 특성은 정부가 블록체인 기술의 고유한 이점을 누리면서 특정 규제 요구사항 및 정책 목표에 부합하는 솔루션을 구현할 수 있도록 보장합니다.

전 세계 정부가 서비스 제공을 현대화하고 투명성과 효율성을 향상시키고자 함에 따라, SIGN 스택은 혁신과 주권 및 규제 준수의 균형을 맞추는 기술적 기반을 제공합니다.

A 기술 사양

A.1 퍼블릭 블록체인 접근 방식: 디지털 화폐 인프라

A.1.1 배포 옵션

이 부록은 레이어 2 체인 배포와 레이어 1 스마트 계약 배포를 평가하는 정부를 위한 배포별 기술 세부 정보를 제공합니다.

레이어 2 체인 배포 레이어 2 배포는 정부에 최대의 운영 통제권을 제공하는 독립적인 블록체인 인프라를 제공합니다:

- **보안 상속**: 기본 레이어 1 네트워크에 대한 정기적인 상태 커밋은 무결성 검증을 보장합니다. 사기 증명 메커니즘은 유효하지 않은 상태 전환의 감지 및 거부를 가능하게 합니다.
- **시퀀서 아키텍처**: 정부는 정의된 기준, 화이트리스트 또는 허가된 검증인 요구사항을 통해 시퀀서 또는 검증인 집합에 대한 통제권을 유지합니다.
- **합의 맞춤화**: 권위 증명(PoA), 프랙티컬 비잔틴 장애 허용(PBFT) 변형 또는 맞춤형 알고리즘을 포함한 합의 메커니즘 선택에 대한 완전한 통제.
- **출구 메커니즘**: 레이어 2가 사용 불가능하거나 손상될 경우 사용자는 레이어 1으로 출금할 수 있어 자금에 계속 접근할 수 있도록 보장합니다.
- **독립 인프라**: 레이어 1 블록 공간이나 가스 가격에 의존하지 않고 블록 생성, 거래 검증 및 네트워크 파라미터에 대한 완전한 통제.

레이어 1 스마트 계약 배포 레이어 1 스마트 계약 배포는 기존 네트워크의 업그레이드 가능한 계약을 통해 정부에 주권적 통제권을 제공합니다:

- **업그레이드 가능한 프록시 패턴**: 사용자 계정을 방해하지 않고 프로토콜 업그레이드를 가능하게 하는 프록시 계약을 통해 구현된 정부 통제.
- **다중 서명 거버넌스**: 승인된 정부 기관이 변경 사항을 승인해야 하는 다중 서명 지갑을 통해 유지되는 주권적 권한.

- **접근 통제 구현**: 역할 기반 권한, 주소 화이트리스팅 및 KYC 통합을 포함한 계약 수준 메커니즘.
- **레이어 1 보안 모델**: 계약은 기본 네트워크의 검증인 집합의 보안 보장을 상속받습니다. 독립적인 합의 인프라가 필요하지 않습니다.
- **네트워크 효과**: 브리지 없이 기존 DeFi 프로토콜, 탈중앙화 거래소 및 유동성 풀과의 직접적인 통합.
- **가스 최적화**: 효율적인 계약 설계는 필요한 규정 준수 메커니즘을 구현하면서 거래 비용을 최소화합니다.
- **검증된 인프라**: 광범위한 감사와 성숙한 개발자 도구를 갖춘 실전 테스트를 거친 플랫폼을 활용합니다.

요소	레이어 2	레이어 1
운영 독립성	높음	중간
합의 통제	완전	L1 합의에 제한됨
블록 생성 통제	완전	해당 없음
DeFi와의 통합	브리지 필요	직접
거래 비용	최적화 가능	L1에 따라 다름
배포 복잡성	더 높음	더 낮음
보안 모델	L1 + L2	L1 전용
업그레이드 유연성	체인 거버넌스	프록시 패턴

표 3: 레이어 2 대 레이어 1 배포 비교

배포 결정 기준 두 배포 방식 모두 핵심적인 주권 역량을 제공합니다. 선택은 정부의 우선순위에 따라 달라집니다: 레이어 2는 맞춤형 합의를 통해 최대의 운영 독립성을 제공하는 반면, 레이어 1 스마트 계약은 더 간단한 배포로 즉각적인 DeFi 통합을 제공합니다.

메트릭	기능
런타임	EVM 기반
블록 시간	< 1초
초당 거래 수	최대 4000 (작성 시점 기준)
합의 알고리즘	PoA, PBFT 변형
완결성	1-5 블록 확인

표 4: 주권 레이어 2 체인 기술 사양(참조 구현)

기술 사양(레이어 2 참조 구현)

A.2 프라이빗 블록체인 접근 방식: Hyperledger Fabric X CBDC

메트릭	기능
합의 알고리즘	Arma BFT
처리량	100,000+ TPS
블록 완결성	블록 커밋 시 즉시
개인정보 보호 모델	네임스페이스 + 영지식 증명(구성 가능)
토큰 운영	UTXO 모델을 사용한 Fabric Token SDK
거래 모델	Fabric-Smart-Client를 통한 P2P 협상
신원 관리	MSP를 사용한 X.509 인증서
네트워크 거버넌스	중앙은행이 통제하는 합의 노드
표준 준수	ISO-20022 호환
네임스페이스 아키텍처	네임스페이스가 있는 단일 채널(wCBDC, rCBDC, 규제)
개인정보 보호 수준	wCBDC: RTGS 수준의 투명성; rCBDC: 높은 개인정보 보호(ZKP)

표 5: Hyperledger Fabric X CBDC 기술 사양

A.3 국가 디지털 신원 스택

구성 요소	사양
자격증명 데이터 모델	W3C 검증 가능한 자격증명 2.0
식별자 표준	W3C 분산 식별자 (DID)
자격증명 형식	VC-JWT, SD-JWT VC, BBS+를 사용한 JSON-LD
서명 알고리즘	ECDSA (secp256k1, P-256), EdDSA (Ed25519), RSA
영지식 증명 시스템	Groth16, Plonk, BBS+ (연결 불가능한 자격증명)
지갑 보안	기기 보안 영역, 생체 인증
키 관리	HSM 지원(FIPS 140-3 레벨 3), 소셜 복구
발급 프로토콜	검증 가능한 자격증명 발급용 OpenID(OIDC4VCI)
제시 프로토콜	검증 가능한 제시용 OpenID(OIDC4VP)
폐지 표준	W3C 비트스트링 상태 목록 v1.0
신뢰 레지스트리	블록체인 기반, OpenID Federation 1.0 호환
오프라인 지원	QR 코드 및 NFC 기반 자격증명 제시
mDL 호환성	ISO/IEC 18013-5/7

표 6: 국가 디지털 신원 기술 사양

A.4 Sign Protocol

메트릭	기능
서명 체계	ECDSA, EdDSA, RSA
영지식 증명	Groth16, Plonk, Honk, BBS+
전자여권 통합	ICAO 9303 호환

표 7: Sign Protocol 기술 사양

A.5 TokenTable

메트릭	기능
최대 분배 규모	무제한
처리량	최대 블록체인 TPS
분배 스케줄링	초 단위 및 달력 월 단위
감사 추적 저장	온체인

표 8: TokenTable 기술 사양