

원화 스테이블코인 아키텍처 제안서 (요약본)

규제 원칙을 구현으로 연결하는 기술 및 운영 프레임워크

K-STAR

{ 카이아 DLT 재단 람다256(주) (주)안랩블록체인컴퍼니 (주)오픈에셋 }

2026년 3월

배경

이 문서는 “원화 가치에 연동되는 스테이블코인”을 단순한 토큰이 아니라, 실제 결제·정산 인프라처럼 안전하게 쓰기 위해 무엇이 필요하고(요구사항), 이를 기술과 운영 규정으로 어떻게 구현할 것인지(아키텍처/운영 정책)를 한데 모아 정리한 제안서다. 원화 스테이블코인은 ‘발행(mint)·소각(burn)’ 기능만 갖추면 끝나는 문제가 아니다. 법적 책임, 준비자산과 상환, 준법(AML/제재), 감사 가능성, 장애·사고 대응까지 포함해 처음부터 “운영 가능한 통합 시스템”으로 설계되어야 한다. 현재 제도와 규제 방향에 대한 논의는 진행되고 있지만, 이를 실제 시스템으로 구현하기 위한 기술·운영 설계는 상대적으로 구체화되지 않은 상황이다. 본 제안서는 원화 스테이블코인이 현실에서 적용되기 위해 필요한 기술적·운영적 요소를 중심으로 이를 정리하고자 한다. 체인과 스마트컨트랙트(권한·통제 기능), 지갑·커스터디·서명 구조, 발행·상환을 처리하는 백오피스 인프라, KYC/AML 및 모니터링, 노드/RPC·데이터·리포팅 같은 핵심 기술 요구사항을 먼저 정리한다. 그리고 이 기술 요소들이 서로 어떻게 맞물려 ‘운영과 통제’로 확장되는지—예컨대 권한 분리와 승인 흐름, 예외/보류 처리, 비상 모드 전환과 재개, 감사 가능한 로그와 보고 체계—까지 함께 구체화한다.

원화 스테이블코인 요구사항

이 문서가 말하는 “요구사항”은 단순 체크리스트처럼 기능을 나열하는 게 아니라, 원화 스테이블코인이 결제·정산 인프라로 쓰일 때 반드시 무너지지 않아야 하는 신뢰의 조건을, 기술과 운영이 함께 충족하도록 정리한 것이다. 흐름은 간단하다. 먼저 결제 인프라로서 최소한 갖춰야 할 안전장치(상환/준비자산/위기통제)를 세우고, 그 안전장치를 토큰(스마트컨트랙트) 레벨에서 어떻게 강제할지(권한·통제·복구·허가형 전송 규칙)를 정리한 뒤, 마지막으로 그 토큰을 실제 서비스로 굴리기 위해 필요한 백오피스/지갑/인프라/데이터/연동 요구를 “운영 가능한 통합 인프라” 관점에서 묶는다.

핵심은 이러한 요구 조건들이 시스템적으로 설계 되어야 한다는 것이다. 이를 아주 짧게 풀면 아래와 같다.

원화 스테이블코인 요구사항

- 책임 주체와 권한이 시스템에서 명확해야 한다.
 - 발행·상환·동결 등 핵심 기능은 임의의 주체가 수행할 수 없고, 법적 책임 주체(또는 그가 공식 위임한 역할)만 수행할 수 있도록 설계되어야 한다.
- 준비자산은 분리 보관이 기본이어야 한다.

- 토큰 발행량에 상응하는 원화(또는 안전자산)가 실제로 존재해야 하며, 준비자산은 발행사의 일반 자금과 분리되어 보관·관리되어야 한다.
- 상환은 표준화된 절차로 처리되어야 한다.
 - 사용자의 상환 요청은 임의 처리 방식이 아니라, 사전에 정의된 절차(요청→확인→지급→소각)에 따라 일관되게 처리되어야 한다.
- 준비자산과 토큰 수량은 지속적으로 대사 가능해야 한다.
 - 준비자산 잔고와 온체인 토큰 발행·유통량은 상시 비교·검증될 수 있어야 하며, 불일치 발생 시 정보 및 후속 조치가 연결되어야 한다.
- 발행·소각은 한도 통제와 기록이 수반되어야 한다.
 - 토큰 발행·소각 시 “누가, 얼마를, 어떤 근거로” 수행했는지가 기록되어야 하고, 역할별로 수행 가능한 한도도 정의되어야 한다.
- 권한은 기능별로 분리되어야 한다.
 - 발행, 동결, 정지, 규칙 변경 등 고위험 권한은 단일 주체에 집중되지 않도록 기능별로 분리·관리되어야 한다.
- 고위험 조치는 다중 승인 기반으로 수행되어야 한다.
 - 대규모 자산 이동 또는 강력한 통제 조치는 단독 집행이 불가하도록 다중 승인 체계를 전제로 하며, 승인·반려 이력 또한 기록되어야 한다.
- 사고 대응 기능과 정상화 절차가 내장되어야 한다.
 - 사고 발생 시 거래 제한(동결/차단) 또는 일시 정지 등 대응 수단이 준비되어야 하고, 정상화(재개) 조건과 절차도 사전에 정의되어야 한다.
- 전송 가능 범위는 정책적으로 조정 가능해야 한다.
 - 초기에는 참여자를 제한하는 방식(예: 승인된 지갑만 허용)으로 시작할 수 있어야 하며, 이후 확장 과정에서도 전송 규칙 변경은 절차와 기록에 따라 통제되어야 한다.
- 토큰 외부의 기반 인프라와 연동 체계가 함께 갖춰져야 한다.
 - 노드/RPC 등 필수 인프라의 안정성, 데이터·보고 체계, 외부 시스템 연동(브릿지/외부 결제·정산/교환 확장 등)에 대한 안전장치와 제한 규칙이 함께 마련되어야 한다.

기술 아키텍처(요구사항을 실제 시스템으로 구현하는 방식)

제안서의 3장은 2장에서 정리한 요구사항을 “운영자가 잘하면 된다”가 아니라, 시스템이 기본 동작으로 지키도록 만드는 기술 설계를 설명한다. 큰 방향은 다음과 같다. 스테이블코인 자체(체인 위 토큰)만 만들어서는 결제·정산에 쓰기 어렵고, 토큰을 둘러싼 지갑·서명·발행/상환 시스템·준법/보안·데이터/보고·필수 인프라가 함께 맞물려야 한다는 전제다. 그래서 문서는 전체를 여러 레이어(사용자 채널, 발행/관리 시스템, 블록체인/스마트컨트랙트, 인프라/데이터)로 나누고, 각 레이어가 같은 사건(발행/상환/통제 조치)을 같은 식별자(요청 ID)로 연결해 끝까지 추적 가능해야 한다고 정리한다.

가장 중심이 되는 것은 발행과 상환의 처리 흐름이다. 발행은 단순히 토큰을 찍는 행위가 아니라, (1) 발행 요청 접수, (2) 자격·한도·준법 기준 확인(신원 확인, 제재/이상거래 여부 등), (3) 준비자산 입금 확인(원화가 실제로 들어왔는지), (4) 필요한 승인 절차, (5) 온체인에서 mint 실행, (6) 내부 기록과 대사(준비자산과 토큰 수량이 맞는지 확인)까지 한 묶음으로 정의된다. 상환은 더 엄격하게 다룬다. 상환 요청이 들어오면, (1) 상환 대상 토큰을 확보(필요 시 동결/회수 포함), (2) 준법·보류 여부 확인, (3) 원화 지급 확정, (4) 온체인 burn, (5) 로그·증빙·대사까지 이어지는 구조로 설계한다. 핵심은 장애나 재처리 상황에서도 같은 상환이 두 번 처리되거나(이중 지급), 같은 발행이 중복 실행되는 일이 없도록 “중복 실행 방지”를 기술적으로 내장해야 한다는 점이다.

토큰(스마트컨트랙트) 자체도 “그냥 전송 토큰”을 넘어서 운영·통제 기능을 포함해야 한다는 입장이다. 문서는 USDT/USDC 같은 주요 사례에서 공통적으로 관찰되는 패턴을 근거로, 결제 인프라로 쓰이는 스테이블코인은 최소한 다음을 컨트랙트 수준에서 다룰 수 있어야 한다고 본다. 첫째, 발행·소각 권한이 역할로 분리되고, 역할별로 발행 가능한 한도(상한)가 관리되어야 한다. 둘째, 사고·법집행·제재 같은 상황에서 주소 단위 동결/제한, 필요 시 전체 일시정지 같은 통제 기능이 있어야 한다. 셋째, 업그레이드나 정책 파라미터 변경이 필요할 수 있으므로(취약점 대응, 정책 변경 반영 등), 이를 무작정 “바꿀 수 있음”이 아니라 정해진 절차와 기록을 동반하는 변경 체계로 설계해야 한다. 넷째, 예외 상황(오입금, 운영 오류 등)을 전제로 복구 기능 또는 복구 절차가 필요하되, 복구 권한이 남용되지 않도록 범위·승인·로그가 분리되어야 한다.

지갑·커스터디·서명 구조는 “사용 편의”만이 아니라 “책임과 통제”를 기술적으로 구현하는 수단으로 다뤄진다. 예를 들어 기관이 쓰는 지갑/서명 구조에서는 발행·상환·정책 통제 같은 민감 행위를 단일 키가 단독으로 수행할 수 없게 하고, 역할 분리와 다중 승인(여러 명이 함께 승인해야 실행) 흐름이 기본이 되도록 설계한다. 개인 사용자 구간에서도 완전 익명 모델을 전제로 하기보다, 신원 확인 상태와 거래 제한 상태가 운영 체계에서 관리될 수 있어야 하며(주소와 실사용자/기관의 연결), 분

쟁·오류·키 분실 같은 상황에서 보호·보류·복구 절차를 운영 정책과 함께 구현 가능한 형태로 갖추는 것을 강조한다.

또한 “토큰 바깥의 인프라”가 끊기면 결제·정산이 멈추기 때문에, 필수 인프라(노드/RPC/익스플로러), 데이터 수집·보관·리포팅, 외부 연동(오라클·브릿지·타 시스템 연결)에 대한 기술 요구도 함께 제시한다. 여기서 포인트는 단순히 “연동한다”가 아니라, 연동된 상태에서도 동일한 통제·기록 기준이 적용되게 만들고, 연동 리스크가 감지되면 제한/차단 같은 조치로 이어질 수 있어야 한다는 점이다. 더 나아가 온체인 교환/환전 같은 확장(오케스트레이션, 온체인 FX)을 다룰 때도, 실패 처리 규칙, 유동성 리스크 관리, 모니터링과 사고 대응까지 ‘결제 인프라 관점’에서 사전에 정의해야 한다고 정리한다.

운영 정책(기술이 실제 운영에서 흔들리지 않게 만드는 규정)

제안서의 4장은 3장의 기술 설계가 현실에서 일관되게 작동하도록, 책임·절차·기록·보고 체계를 운영 규정으로 고정한다. 문서가 반복해서 강조하는 운영 규정의 중심 원칙은 세 가지다. 권한이 한 곳에 몰리지 않게 할 것(권한 집중 방지), 실제로 집행 가능한 통제여야 할 것(문서 선언이 아니라 시스템/절차로 실행), 사후에 검증 가능한 기록이 남을 것(감사 가능한 증빙)이다. 즉, 어떤 조치를 “할 수 있다”가 아니라, 누가 어떤 근거로 어떤 승인 절차를 거쳐 언제 실행했고, 이후 어떻게 해제/정상화했는지가 남는 구조를 운영 규정으로 요구한다.

운영 정책의 출발점은 참여자와 책임 경계를 분명히 하는 것이다. 발행사(법적 책임 주체), 준비자산 보관/수탁 역할, 발행·상환 시스템 운영 역할, 준법/보안 운영, 유통 채널, 지갑/커스터디 제공자, 감사/검증 역할이 분리되는 구조를 전제로 두고, 각 주체가 무엇을 승인하고 무엇을 실행하며 무엇을 보고해야 하는지(역할과 책임 배분)를 명문화한다. 특히 발행·상환·동결·정지·정책 변경 같은 고위험 행위는 승인자와 실행자를 분리하고, 이해상충이 발생할 수 있는 경우에는 제척(해당 의사결정에서 배제) 원칙까지 포함해 권한 남용 가능성을 줄이는 방향으로 설계한다.

또 하나의 큰 축은 운영 모드(정상/제한/비상/중단)다. 사고를 “예외”가 아니라 “발생 가능”으로 전제하고, 어떤 경우에 제한 모드로 전환하는지, 비상 모드에서 무엇을 허용/금지하는지(예: 발행·상환·전송의 처리 방식 변화, 큐잉/보류 등), 전환은 누가 승인하는지, 전환 근거와 실행 시각, 재개 조건을 어떻게 기록하고 사후 보고하는지까지 표준 흐름으로 제시한다. 기자/일반인이 보기엔 “위기 때 멈출 수 있나” 정도로 보이지만, 문서의 핵심은 ‘멈춤’ 뿐 아니라 ‘부분 제한’, ‘질서 있는 재개’, ‘사후 검증 가능한 기록’을 한 세트로 묶는 데 있다.

리스크 관리는 “사고 나면 처리”가 아니라 “조기 신호와 기준으로 운영”하는 방식으로 정리한다. 문서는 리스크를 몇 가지 범주(준비자산/상환/준법/보안/인프라/연동 등)로 분류하고, 각 범주에 대해 핵심 리스크 지표(KRI: 위험을 조기에 감지하기 위한 지표), 임계치(트리거), 그리고 단계별 대응 플레이북을 연결한다. 예컨대 특정 지표가 임계치를 넘으면 경보가 발생하고, 관련 근거 데이터가 보관되며, 승인 절차를 거쳐 제한 모드 전환이나 특정 통제 조치로 이어지도록 운영 흐름을 표준화한다. 중요한 점은 이런 대응이 “사람이 기억해서 하는 것”이 아니라, 시스템과 규정이 함께 정해진 절차로 반복 가능해야 한다는 것이다.

상환과 준비자산에 대해서는 운영 규정이 특히 구체적이어야 한다는 관점을 유지한다. 상환은 보류/거절이 가능한 조건과 처리 기한, 고객 고지 기준, 승인 요건과 기록 항목이 정리되어야 하며, 위기 상황에서 상환을 어떤 원칙으로 처리할지(예: 우선순위, 제한 방식) 같은 부분도 운영 규정에 포함된다. 준비자산은 분리 보관의 형태, 잔고/구성 확인 방식, 정기 대사와 보고(공시/감독/감사 대응 산출물)의 범위·주기·책임이 정의되어야 하고, 정합성이 깨졌을 때 어떤 조치를 취하는지(예: 발행/상환 제한 신호)까지 운영 규정으로 연결한다.

마지막으로 변경관리와 보고 체계가 운영 정책의 중요한 축으로 제시된다. 규제/리스크 환경은 바뀔 수 있으므로, 정책 파라미터나 통제 규칙을 바꿀 필요가 생긴다. 이때 변경은 “누가 마음대로”가 아니라 정상 변경과 긴급 변경을 구분하고, 사유·영향·승인·공시·시행·사후 점검·롤백(원복) 기준까지 포함한 절차로 통제해야 한다고 정리한다. 동시에, 운영 전반에서 발생하는 주요 이벤트(발행/상환/통제 조치/모드 전환/정합성 점검 결과)가 로그와 리포트 형태로 남아 외부 이해관계자(감사, 감독, 파트너)에게 설명 가능한 상태가 되는 것을 운영 목표로 둔다.

적용(활용/적용방안) 요약

제안서의 6장은 “기술과 운영을 어떻게 쓰는가”를 사례로 보여주는 장이다. 여기서 문서는 3장과 4장에서 제시한 구조를 다시 증명하기보다, 스테이블코인 시스템의 성격상 현실에서 마주치는 전형적 채널(국내 지급결제, 플랫폼 채널, 해외 결제/송금/정산)에서 무엇이 같고 무엇이 달라지는지, 그리고 공통으로 지켜야 할 설계 포인트가 무엇인지에 초점을 둔다.

국내 지급결제 관점에서의 요지는 단순하다. 원화 스테이블코인이 “결제·정산에서 실제 돈처럼” 쓰이려면, 거래량이 늘수록 더 중요해지는 것은 속도나 편의 기능이 아니라, 상환과 준비자산 정합성, 사고 시 통제와 정상화가 시스템 절차로 작동하는지다. 그래서 운영 모드 전환(제한/비상/중단)과 상환 우선 처리 같은 원칙이, 기술(컨트랙트/시스템)과 운영 규정에 함께 박혀 있어야 한다는 방향으로 정리된다.

플랫폼 채널(예: 대형 앱/서비스)로 갈수록 “고객 접점이 넓고 다양해진다”는 점이 핵심 변수다. 문서는 이런 환경에서 유통 채널이 신원확인 및 고객지원의 1차 책임을 맡고, 고객별·채널별 한도와 거래 제한, 정책 고지 같은 통제가 일관되게 집행되어야 한다는 점을 전제로 한다. 즉, 어느 채널에서 들어온 요청이든 동일한 표준 워크플로우로 처리되고, 같은 기준으로 추적·증빙·보고가 되도록 “운영 가능한 통합 인프라”로 묶어야 한다는 결론으로 이어진다.

해외 결제/송금/정산의 경우에는 “여러 네트워크·참여자가 섞일수록 안전한 공통 레일이 필요해진다”는 메시지로 연결된다. 문서는 모드 전환을 대시보드 경고 또는 자동 규칙으로 수행하고, 위험 지표(KRI) 모니터링과 로그/정기 보고를 통해 다중 네트워크 환경에서도 신뢰성과 안전성을 유지해야 한다고 서술한다. 그리고 이런 구조가 원화 스테이블코인을 국내를 넘어 “공통 결제 레일”로 자리매김시키고, 아시아 디지털 경제를 연결하는 허브가 되는 기반이 될 수 있다는 방향으로 정리한다. 6장이 말하는 공통 설계 포인트를 요약하면, “채널이 달라도 코어는 하나”다. 모든 요청은 요청ID로 종단 간 추적 가능해야 하고, 표준 상태 전이 밖의 처리는 막아야 하며, 예외/보류/거절은 사유코드와 근거자료로 남아야 한다. 민감 권한은 역할 기반으로 분리되고 다자 승인으로 집행되며, 운영 모드는 트리거와 처리 원칙을 사전에 정의해 변경관리로 통제한다. 그리고 외부 시스템 연동은 인증/권한/오류코드/재시도 규칙까지 포함해 스펙화하고, 모든 호출/응답이 요청ID와 함께 로깅되어야 한다는 요구로 수렴한다.

마무리 제언(요약)

문서는 원화 스테이블코인 논의가 “무엇을 허용할 것인가”를 넘어 “무엇을 갖춰야 실제로 운영 가능한가”로 이동해야 한다고 제언한다. 특히 초기 실증(샌드박스·PoC) 단계에서 단순 데모 수준이 아니라, 실제 운영 환경에서 기술이 제대로 작동하는지와 동시에 책임·통제·보고 체계까지 함께 점검할 수 있도록 범위와 목표를 분명히 설정하는 것이 중요하다고 정리한다.

이를 위해 핵심은 구성요소를 각각 ‘완성’하는 것이 아니라, 발행·상환과 관리, 준법 연계, 기록·보고가 하나의 흐름으로 일관되게 작동하도록 처음부터 종단간으로 설계하는 것이다. 운영 측면에서도 권한·승인, 예외·고위험 상황 처리, 비상 전환·복구·재개 같은 기본 규칙을 사전에 정리해두면 참여자·채널이 늘어나는 과정에서 혼선과 시행착오를 줄일 수 있다고 본다. 특히 컨소시엄 방식이라면 책임 경계가 흐려지기 쉬우므로, 누가 무엇을 결정하고 집행하는지, 어떤 기준과 기록이 남아야 하는지를 가능한 한 초기부터 합의하는 것이 신뢰와 운영 품질에 직결된다고 강조한다.

구축 방식에 대해서는 모든 기능을 한 조직이 단독으로 만들기보다, 전문 파트너 협업을 전제로 역할과 연동 지점을 표준화하고 단계적으로 고도화하는 접근이 효과적이라고 제언한다. 정책·규제

논의 역시 원칙 선언을 넘어, 현장에서 일관되게 집행 가능한 형태의 규율(구현·운영 기준과 지침)을 함께 정교화해야 신뢰와 확장이 가능하다는 관점이다.

마지막으로 지금은 시장이 본격화되기 전 ‘초기 국면’이기 때문에, 한국이 제도 논의와 함께 실행 가능한 기준을 조기에 세팅하고 실증으로 고도화해 나가면 향후 표준과 인프라의 주도권을 확보할 수 있다고 정리한다. 준비가 늦어질수록 외부 표준을 사후 추종하는 구조가 굳어질 수 있다는 점을 리스크로 지적한다.