On/Off-Chain Prism · OCP

VERSION 1.0

Chain Prism

디지털자산 거래 실질 통합 분석 프레임워크

Substance over Code



사례 보완판 · 2026-11-18

USDC 공개보고서 검토 · 국내 발행통제 합성 사례 / 총 88쪽

Vanzi

최초 작성일 2026년 11월 14일 · OCP v1.0

코드·거래·권리·경제적 실질을 연결하는 분석 체계

6단계 · 5개 전문 모듈 · 증거 연결 · 기능 카드 · 검증 패턴

CONTENTS

목차

분석의 흐름을 읽고, 필요한 사례와 도구를 찾아 적용한다.
항목을 누르면 해당 본문으로 이동한다.

시작 **사용 안내 · 빠른 안내 · ID 지도** 3

01 **분석 방법론과 6단계** 6

02 **도구 통합과 증거 처리** 15

03 **실제 사례와 교육 사례** 21

- USDC · 최초 실제 부분 적용 21
- 건물 RWA · 권리와 가치 25
- DEMO-USD · 자료에서 판단 수정까지 29

04 **작성 양식 · 검증 패턴 · 기능 카드** 35

- 작성 양식 F-01~F-06 · 증거 연결표 35
- 검증 패턴 RF 42
- 기능 카드 FC 44

05 **거래 실질에서 회계까지** 59

부록 **규칙·계정 명세 · 구현·출처·발전 계획** 68

보완 부록 · 가치평가·증거 판정·완료 기준 73

사례 보완 · USDC 공개보고서 검토 78
국내 발행통제 합성 사례 84
출처·재현·개정 기록 88

기능 카드 바로 찾기
발행 47 · 역할 49 · 업그레이드 51 · 동결 53

START / READER & SCOPE

누가, 무엇을 위해 사용하는가

회계·준법·AML·IT감사 실무자를 위한 디지털자산 거래 분석 학습·적용 매뉴얼.

이 문서는 처음부터 모든 전문 판단을 수행하도록 요구하지 않는다. 먼저 분석할 거래와 질문을 고르고, 확보한 자료가 무엇을 보여주는지 정리한 뒤 필요한 검토 관점을 선택한다. 아래의 배지와 범위 안내는 각 페이지를 어디까지 읽고 활용할 수 있는지 알려주는 길잡이다.

코드·거래·계약·원장을 연결해 질문을 정하고 근거와 판단을 기록한다. 실무자는 방법론·사례·카드·양식을 먼저 읽는다. 구현을 준비하는 독자는 뒤의 개발·운영 부록을 추가로 참고한다.

세 축 배지를 읽는 법

축	표시 예	의미
자료 성격	실제 공개 / 합성 / 참고 코드·표준	실제 사례·가정·참고 자료를 구분한다. 실제 공개 자료도 신뢰성·범위를 검토한다.
카드 상태	시드 / 검토·개정 / 비적용	질문 도구의 성숙도다. 사례에서 기능이 확인됐는지와 별개다.
수행 범위	RPC 읽기 / 서술·계산 / 질문 명세	무엇을 수행했는지 표시한다. 코드 검토·실행·오프체인 연결은 서로 다른 범위다.

시드 카드의 상태는 해설 페이지에도 이어진다. 각 사례·카드의 시작에 배지를 표시하고, 수행 범위가 달라지는 곳에서 갱신한다. “미검증”이라는 하나의 상태로 세 축을 합치지 않는다.

공통 범위와 사용 안내

구분	이 문서의 범위
실제 사례	USDC는 고정 블록의 단일 공개 RPC 응답과 공식 참고 자료를 이용한 진행본이다. 배포 소스 대응·내부 운영·준비자산 대사는 남은 과제로 표시한다.
교육 사례	건물 예시·DEMO-USD·회계 시범 사례는 합성 조건으로 분석 순서를 보여준다. 합성 자료 안의 관찰·추론과 실제 사실을 구분한다.
전문 판단	관할·회계기준·정책·기준일을 지정해 별도로 판단한다. 프레임워크 사용 자체가 공식 의견·보증·보안감사 결론을 뜻하지 않는다.
소프트웨어	공개자료 수집·재조회 스크립트는 USDC 착수팩에 있다. 자동 귀속·회계 판단·계정 매핑·자동 전기 엔진은 미구현이다.

> 일반 안내는 이 페이지에 모았다. 개별 결론을 바꾸는 구체적 증거 한계—예: 키 운영 미확인, 계좌 범위 미확인, 규칙 전제 부족—는 해당 결론 옆에 유지한다.

→ 보완 부록 73~77쪽

01 / HOW TO USE

한 장으로 이해하는 Chain Prism

여러 도구와 자료의 결과를 증거로 정리하고, 전문 판단을 지원하는 작업 체계다.

OCP의 출발점은 복잡한 기술 용어가 아니라 하나의 거래 질문이다. 예를 들어 “토큰을 보유하면 누구에게 무엇을 청구할 수 있는가”를 정한 뒤 코드·거래·계약에서 답의 근거를 찾는다. 아래의 입력·처리·출력과 세 가지 규칙은 이 질문이 분석 과정에서 다른 주장으로 바뀌지 않도록 붙잡아 준다.

입력

판단할 질문과 대상 거래·상품·사업

처리

증거 확보 → 구조 복원 → 전문 분야별 판단 → 대조

출력

결론·조건·한계·추가 조치와 재현 자료

세 가지 고정 규칙

규칙	실행 방법
사실과 가정을 나눈다	F: 관찰 사실 / I: 추론 / H: 가정. 해석·결론은 별도 작성한다.
권한과 권리를 나눈다	키 보유·기술적 권한을 소유권·회계상 통제·조세 귀속으로 자동 전환하지 않는다.
결론과 근거를 연결한다	질문 → 사실 → 기준 → 판단 → 한계 → 다음 조치 순서로 기록한다.

필요한 모듈만 선택한다

규제·AML

사업자·행위·의무

회계·감사·보증

인식·측정·검증

조세·과세정보 보고

소득·귀속·보고

거래구조화·가치평가

권리·배분·가치

IT감사·기술 리스크

권한·시스템·통제

> 핵심 사실이 없으면 결론을 강행하지 않는다. 자료 보완, 조건부 분석, 결론 유보 중 하나를 선택한다.

읽는 순서 · 공통 안내·ID 3~5쪽 → 방법론·도구 6~20쪽 → 실제·교육 사례 21~34쪽 → 양식·RF · FC 35~58쪽 → 거래·회계 59~67쪽 → 개발·운영·출처 부록 68~72쪽 → 보완 부록 73~77쪽

START / RECORD MAP

이름으로 읽고, ID로 근거를 찾는다

ID는 추적용 주소다. 본문을 이해하기 위해 모든 접두사를 암기할 필요는 없다.

분석을 다시 확인하려면 결론뿐 아니라 그 결론이 나온 자료와 경로를 찾을 수 있어야 한다. ID는 이를 위한 연결 주소이며, 새로운 전문 개념을 뜻하지 않는다. 본문은 이름으로 읽고, 검산·재조회·변경 검토가 필요할 때 아래 지도를 이용해 원문과 판단 기록으로 돌아가면 된다.

표시·기록	독자가 읽을 이름	찾아갈 대상
M1~M5	전문 검토 관점	규제·AML / 회계·감사 / 조세·보고 / 구조화·평가 / IT감사
F-01~F-06	작성 양식	범위 → 증거 → 구조 → 판단 → 차이 → 종합 결론
FC-A01 등 / RF-01 등	기능 질문 / 검증 패턴	어떤 동작인가 / 어떤 징후를 검증할 것인가
R-USDC-01 / V-01·V-A01 등	사례	R-USDC는 실제 공개 사례. V는 이 문서의 합성 사례군
D-01·V-D01 / V-T01	자료 / 도구 형식 입력	원문·자료, 또는 기존 자료를 변환·재표현한 입력
I-01 / H-01 / V-F01	추론 / 가정 / 발견	사례 안의 판단 기록. V-F는 양식 F-01과 다름
S1 / FC-S1 / 회계-S1	출처	일반 도구 / 기능 카드 / 회계 참고의 출처. 섹션 범위를 함께 표기
case_id·assertion_id 등	데이터 필드	사례·개별 주장·원본·입력·변환·경제적 사건·적용 기록을 연결
rule_id·mapping_id·journal_draft_id	개발·회계 추적 필드	규칙 / 회사 계정 매핑 / 분개 초안. 상세 명세는 부록 A

F/I/H는 ID가 아니라 주장 성격이다

F 관찰 사실 · I 추론 · H 가정. 예를 들어 “V-D03에 수량이 기재됐다”는 합성 자료 내부의 관찰이다. 그 수량이 실제 체인에서 확인됐다는 뜻은 아니다. 실제 공개 사례에서도 라벨 표시 F와 실제 주체 귀속 I를 나눈다.

한 줄 추적 예

USDC 사례 → 슬롯 조회 원본 → 구현 주소 관찰 → 프록시 카드 → 연결 검토 → 결론·남은 질문

기존 ID는 자료 호환성을 위해 유지한다. 새 기록은 사례 ID를 상위 범위로 묶고, 화면에는 쉬운 이름을 우선 표시한다. 개발용 필드와 독자가 보는 설명을 분리한다.

PART 1 · 01A / ARCHITECTURE

방법론·절차·모듈·양식

작업은 6단계로 진행하고, 필요한 M1~M5만 선택해 기록한다.

방법론·작업 순서·전문 모듈·양식은 같은 분석을 서로 다른 각도에서 정리한다. 6단계는 지금 무엇을 할지, 모듈은 어떤 기준으로 볼지, 양식은 무엇을 남길지를 안내한다. 기능 카드와 검증 패턴은 이 흐름에 필요한 질문을 공급하므로 모든 도구를 한꺼번에 적용할 필요는 없다.

Chain Prism(OCP)은 전체 방법론, 6단계는 작업 순서, M1~M5는 검토 목적, F-01~F-06은 기록 양식이다. FC는 동작별 질문, RF는 징후별 검증 패턴이다. Part 5는 거래·권리·상태·통제·회계를 연결한다. 구현 상세는 부록에서 다룬다. 도구 결과는 입력 명세로 받아 이 작업 순서와 모듈에 연결한다.

방법론

OCP: 온·오프체인 증거를 전문 판단으로 연결

작업 순서

범위 → 증거 → 구조 → 판단 → 정합성 → 결론

기록

각 단계의 결과를 F-01~F-06에 남긴다.

사용자 화면의 전문 모듈

모듈	검토 목적	대표 결과물
M1 규제·AML	규제 적용과 사업자 의무·AML 위험	의무·위험 검토표
M2 회계·감사·보증	회계처리·재무보고·증거 검토	회계 메모·검증 절차
M3 조세·과세정보 보고	소득·귀속·시기·조세 실사·보고	세무·보고 쟁점표
M4 거래구조화·가치평가	권리·현금흐름·발행조건·가치	조건표·모델·구조도
M5 IT감사·기술 리스크	권한·시스템·데이터·통제	통제·테스트·예외표

도식의 공통 표기

표시	의미
실선 + 증거 ID	적합한 증거로 뒷받침된 관계
점선 + I 표시	추론하거나 확인하지 못한 관계
별도 색상 + H 표시	가정·스트레스·대안으로 변경한 관계
이름 붙인 화살표	자금 이동 / 권리 이전 / 권한 행사 / 분석 순서 구분

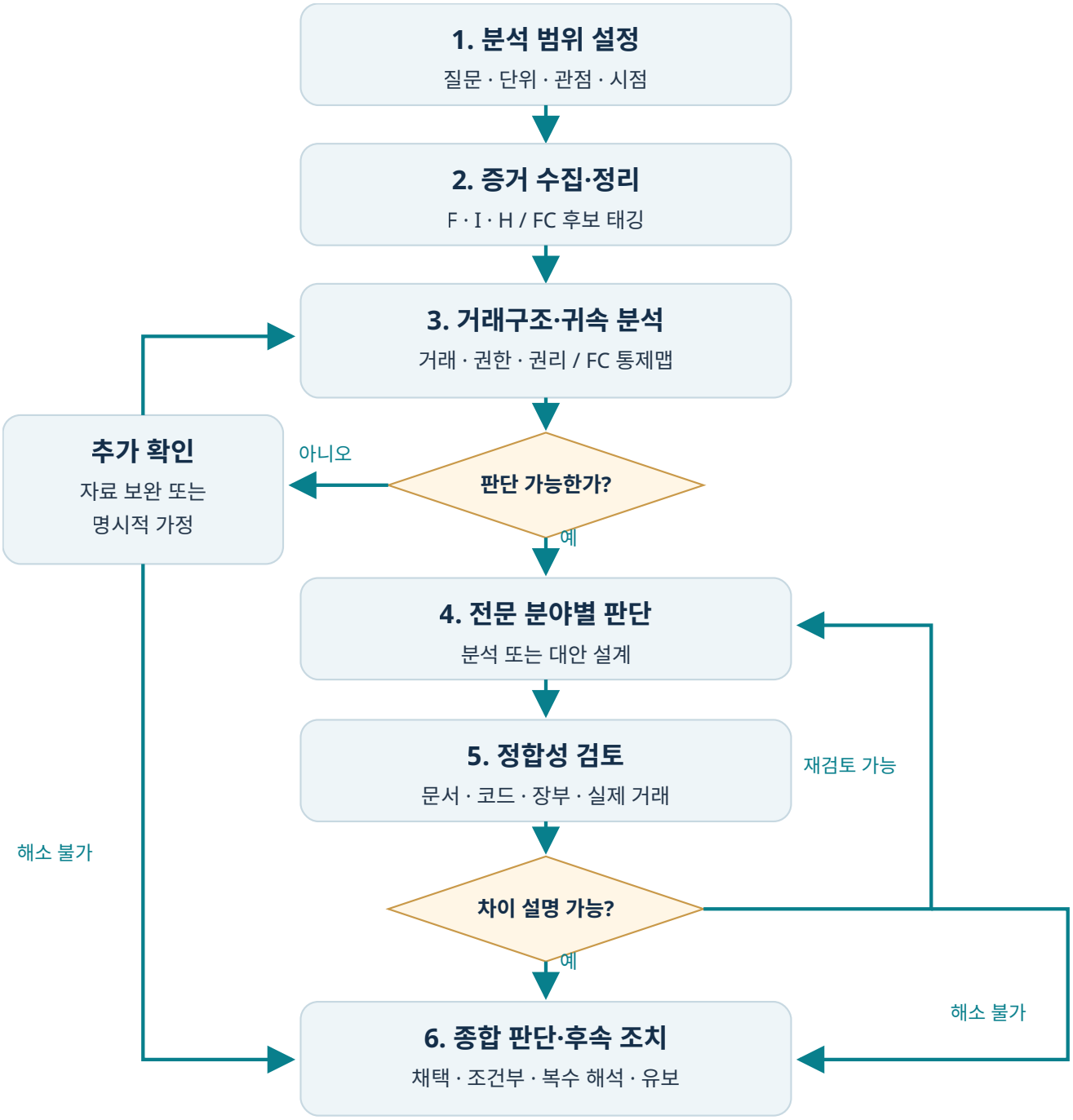
색상만으로 의미를 구분하지 않는다. 절차도의 화살표는 작업 순서를 뜻한다. 세부 기록의 위치는 앞의 ID 지도를 참고한다.

PART 1 · 02 / MASTER FLOW

Chain Prism 실행 절차도

반복 검토와 종료 조건을 함께 정한다.

아래 절차도는 한 번 통과하면 끝나는 직선 경로가 아니다. 구조를 복원하다 당사자를 확인하지 못하면 증거 수집으로 돌아가고, 정합성 검토에서 차이가 나오면 앞선 판단을 다시 살핀다. 되돌아간 이유와 보완 자료를 기록하면 최종 결론뿐 아니라 판단이 달라진 과정도 설명할 수 있다.



자료 보완이 가능한 경우 2~3단계, 해석 재검토는 4단계로 돌아간다. 추가 확인으로도 해결할 수 없으면 유보한다. 명시된 가정으로 분석 가능한 부분만 조건부로 진행한다.

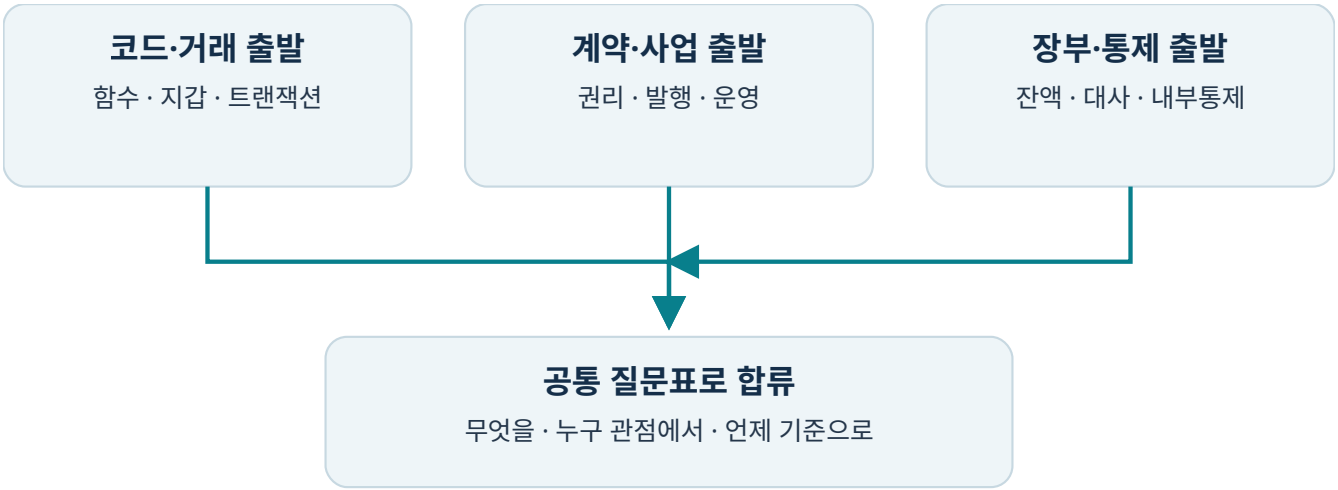
PART 1 · STEP 1 / QUESTION

먼저, 판단할 질문을 정한다

모든 사례가 코드에서 시작할 필요는 없다.

같은 컨트랙트라도 투자자의 권리를 설명할 때와 운영자의 권한을 점검할 때 필요한 자료는 다르다. 그래서 코드부터 읽기보다 질문·관점·기준시점을 먼저 정한다. 아래 그림은 표준·사례·전문 기준을 질문으로 모으는 순서이며, 범위를 좁히는 일이 자료 누락을 숨기는 일이 되지 않도록 제외 항목도 기록한다.

예를 들어 상환 가능성을 묻는 분석이라면 상환 함수의 존재만 확인해서는 질문에 답하기 어렵다. 누가 청구할 수 있는지, 어떤 자산으로 언제 지급하는지, 청구권을 제한하는 조건이 무엇인지까지 범위를 정해야 한다. 반대로 단순 수량 대사가 목적이라면 이 모든 전문 판단을 한 번에 끝내려 할 필요는 없다.



고정 항목	작성 질문
판단 질문	예: 이 토큰의 보유자는 누구에게 무엇을 청구할 수 있는가?
대상·관점	분석 단위: 거래 1건·상품 1개·사업자 전체 / 관점: 투자자·발행자·수탁자
범위·시점	관할권·대상기간·기준일·기준 블록은 무엇인가?
모듈 선택	규제·AML / 회계·감사·보증 / 조세·과세정보 보고 / 거래구조화·가치평가 / IT 감사
종료 기준	중요 질문의 답변 범위와 기한. 미해결 시 조건부 판단·복수 해석·유보로 종료 가능.

산출물 F-01: 분석 범위·질문표. 기준 사례와 변경할 가정을 이 단계에서 구분한다.

PART 1 · STEP 2 / EVIDENCE

자료를 확보하고 성격을 표시한다

자료의 양보다, 판단 질문을 뒷받침하는 적합성이 중요하다.

자료를 모으는 단계에서는 관찰한 내용과 그 의미에 대한 설명을 나눈다. 도구가 특정 라벨을 표시했다는 기록은 남길 수 있지만, 그 주소의 실제 통제자가 누구인지는 별도 근거가 필요하다. 아래 분류는 자료를 버리기 위한 등급표가 아니라 후속 확인이 필요한 연결을 표시하는 방식이다.

공개되지 않은 내부 원장을 학습용 숫자로 보완한다면 그 숫자는 H로 남는다. 이후 공식 자료를 받아 같은 값이 확인되더라도 가정을 사실로 소급해서 바꾸기보다 새 자료와 확인 과정을 추가한다. 이렇게 해야 분석 당시 무엇을 알고 있었고 무엇을 예상했는지 구분할 수 있다.

온체인 증거

코드 · 상태 · 이벤트 · 실행 추적 · 권한 · 거래

오프체인 증거

계약 · 공시 · 원장 · 은행·수탁 자료 · 운영 기록

표시	의미	기록 예시
F · 사실	자료에서 직접 확인	주소 A에 발행 권한이 설정돼 있다.
I · 추론	직접 관찰을 넘어선 연결·귀속 추론	주소 A가 운영사 B의 관리 주소일 가능성이 있다.
H · 가정	미확인 보완·스트레스·대안	공실률이 20%가 된다고 가정한다.

자료 부족 시 분기

추가 확보 가능
자료 요청 · 재수집

조건부 분석 가능
가정 명시 · 민감도

핵심 판단 불가능
결론 유보 · 한계 보고

문서에 상환권이 적혀 있다는 사실과 실제 상환이 이행됐다는 사실을 구분한다. 소스코드 검증과 코드의 안전성 검증도 구분한다.

> FC 후보를 태깅하고 주장·범위·확인 상태를 남긴다. 산출물 F-02: 증거·가정 목록과 공통 입력 명세. 원본·출처·시점·변환·F/I/H · 수용 상태를 남긴다.

PART 1 · SIGNATURE TOOL / EVIDENCE BRIDGE

온·오프체인 증거 연결표

핵심 질문 → 두 영역의 확인사항 → 연결·대사 → 발견과 조치

온체인 기록과 계약이 각각 존재해도 두 자료가 같은 거래를 가리킨다는 연결은 따로 확인해야 한다. 금액이 비슷하다는 이유만으로 대응시키지 말고 대상·시점·당사자·단위를 맞춘다. 아래 연결표에는 확인된 연결과 남은 질문을 함께 적어, 증거가 있는 부분과 해석에 의존하는 부분을 드러낸다.

대사에서 차이가 나면 먼저 단위·기준시간·포함 범위를 확인한다. 발행량은 토큰 수량인데 입금액에는 수수료가 포함되거나, 한쪽은 요청 시점이고 다른 쪽은 지급 시점일 수 있다. 차이를 설명하는 조정 항목이 확인되면 원래 수치와 조정 후 수치를 모두 남겨 계산의 경로를 보여준다.

온체인 확인

코드·권한·상태·실행 기록

연결 검증

주체·자산·거래 ID·기준시점 대사

오프체인 확인

계약·계좌·원장·운영·실제 자산

판단 요소	온체인에서 확인	오프체인에서 확인	연결·검증 방법
발행 권한과 실제 주체	권한 주소·역할·실행 이력	키·서명자·승인·위임·운영 기록	주소-키-승인자 연결. 실제 실행과 승인기록 대사
상환 처리와 의무	잠금·이전·소각·총공급량	청구권·요청 상태·지급완료·원장	요청 ID별 지급·소각·의무 잔액의 시점 대사
준비자산과 부채 범위	공급량·관련 지갑·기준 블록	은행·수탁·명의·담보·제약·보고 범위	분자·분모의 주체·대상·시점을 일치시켜 계산
RWA의 권리 연결	보유·이전·자격·분배 로직	기초자산·계약·신탁·명부·집행 조건	토큰 단위와 청구권을 연결하고 이전 요건 비교

구분 상태는 결론과 별도로 기록한다

상태	의미
온체인 확인 / 오프체인 확인	해당 주장에 맞는 증거로 그 영역의 항목을 확인
연결 확인	각 영역에서 확인한 대상이 같은 주체·권리·거래·시점임을 뒷받침
연결 미확인 / 가정 / 비적용	남은 연결을 추론·가정으로 표시하거나 비적용 사유 기록

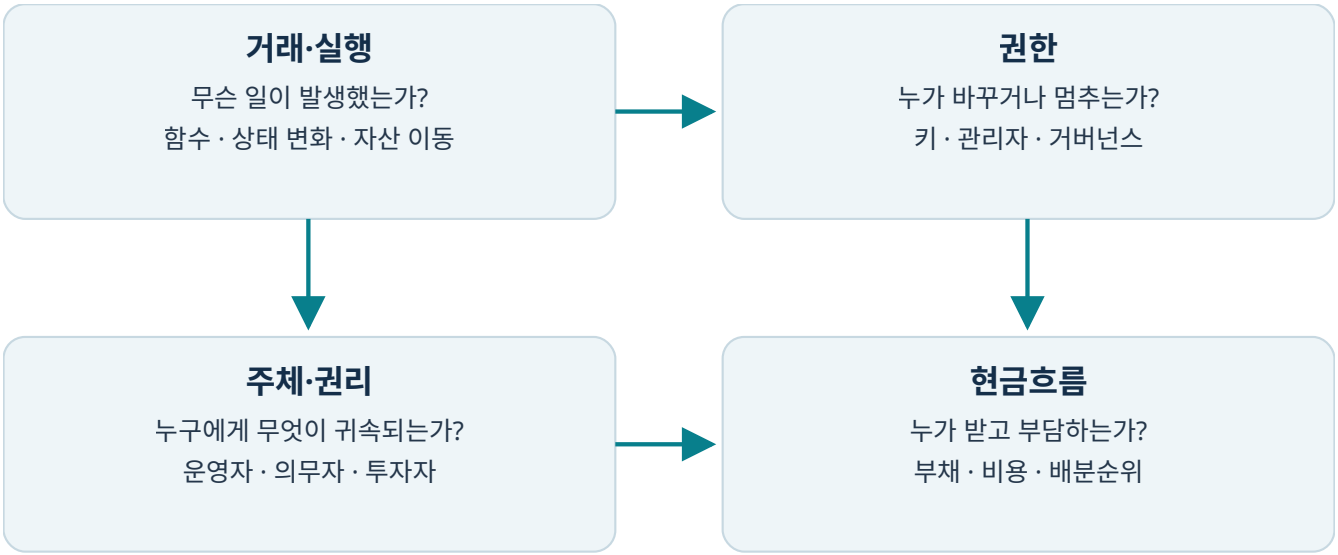
양쪽 자료가 존재하는 것과 서로 연결되는 것은 다르다. 질문에 온체인 증거가 필요 없는 경우 오프체인 증거만으로 평가하고 비적용 이유를 남긴다.

PART 1 · STEP 3 / STRUCTURE

구조 복원과 실제 주체의 귀속

네 요소를 분리하고, 공개 식별에서 실제 운영까지 연결한다.

기술적 권한·법적 권리·회계상 통제·경제적 귀속은 서로 다른 주장이다. 아래 구조도로 관계를 나눈 뒤, 귀속 질문별로 공개자료와 내부 문서, 실제 운영을 교차검증한다. 문서의 개수나 도구 점수가 주체 확정의 공통 문턱이 되지는 않는다.



주체 귀속 증거 확보·교차검증 절차

순서	확인·대사와 기록
1 · 질문 고정	키 운영자 / 의사결정자 / 법적 권리자 / 회계상 통제자 / 조세 귀속자 중 무엇을 판단하는가? 자산·거래·관할·기준기간을 지정.
2 · 공개 식별	공식 주소 공시·법인 공시·프로젝트 문서와 OSINT의 URL·판본·확인일·원출처를 보존. 라벨·클러스터는 후보 주체를 찾는 단서로 사용.
3 · 문서상 권한	이사회 의사록·법적 위임장·키 관리 정책·서명자 명부의 작성 주체·진정성·효력 기간·위임 범위 확인. 사본·누락·변경 이력 표시.
4 · 실제 운영 대조	역할·관리자·서명 주소 ↔ 문서상 담당자 ↔ 승인·키 변경·실행 기록을 같은 거래·기간으로 연결. 위탁·공동 권한·미회수 권한과 반증 검토.
5 · 기준별 평가	관계별 확인 / 추론 / 미확인과 한계를 남기고 분야별 기준으로 판단. 충돌·핵심 공백이 남으면 보완 요청·조건부 판단·유보 중 선택.

주장별 필수 기록 · 대상 주체·관계 / 근거 ID·출처·시점·진정성 확인 범위 / 실제 운영 연결 / 충돌·누락 / F·I·H / 판단 기준·검토자. 이는 기록의 최소 항목이며 충분한 입증을 보장하는 목록이 아니다.

> 서명자 명부 ≠ 실소유자 명부. 서명 가능성 ≠ 법적 권리·경제적 통제. F-03에 관계를, F-02에 근거를, F-05에 차이를 기록한다. FC-C02 실무 체크리스트는 50쪽. 기초자산·청구권·토큰 가격도 구분한다.

PART 1 · STEP 4 / MODULES

모듈 선택과 M3 조세 쟁점 판단

과세와 과세정보 보고를 분리하고, 사실·규칙이 부족하면 질문으로 돌아간다.

M1~M5는 같은 사실을 다른 기준으로 읽는다. 필요한 모듈을 고른 뒤 M3에서는 아래 공통 질문을 적용한다. 이 흐름은 국가별 세율·과세 시점을 정하는 규칙이 아니라, 사실과 적용 법규를 확인하고 쟁점을 기록하는 절차다.

모듈	질문·기록
M1 규제·AML	사업자·행위 분류, 의무·위험
M2 회계·감사·보증	인식·측정·검증·계정 매핑
M3 조세·과세정보 보고	아래 두 경로와 조건부 분기
M4 구조화·가치평가	권리·현금흐름·발행조건·가치
M5 IT감사·기술 리스크	권한·데이터·시스템·통제

M3 · 거래별 조세 쟁점 판단 흐름



조건부 분기	추가 질문
특수관계 거래가 있는가?	해당 관할의 특수관계·적용 범위 확인 후 기능·자산·위험·계약·가격 산정과 이전가격 자료 검토.
포크·에어드랍·리베이스가 있는가?	권리 발생·접근/처분 가능성·수량과 지분 변화·가치·조건을 구분. 현지 기준에 따라 소득·귀속 시점 검토.
국제적 연결이 있는가?	체인 간 이동을 국경 간 거래로 자동 분류하지 않음. 납세자·상대방·거주지·서비스·원천지 사실부터 확인.

출력: 질문 → 사실·증거 → 적용 법규/판본·기준일 → 판단·대안 → 누락·후속 조치(F-04). 분석은 실제 구조를 복원하고, 설계는 목표·제약 아래 비용·세후 현금흐름·권리·유동성·복잡성을 비교한 뒤 Step 3~5로 재검토한다.

공식 참고 · M3-S1 OECD CARF·CRS 2023 / M3-S2 OECD 이전가격 지침 2022. 참고 범위 확인: 2026-11-14. 국가별 적용 법규·조약·해석의 최신 확인은 각 사례에서 별도 수행.

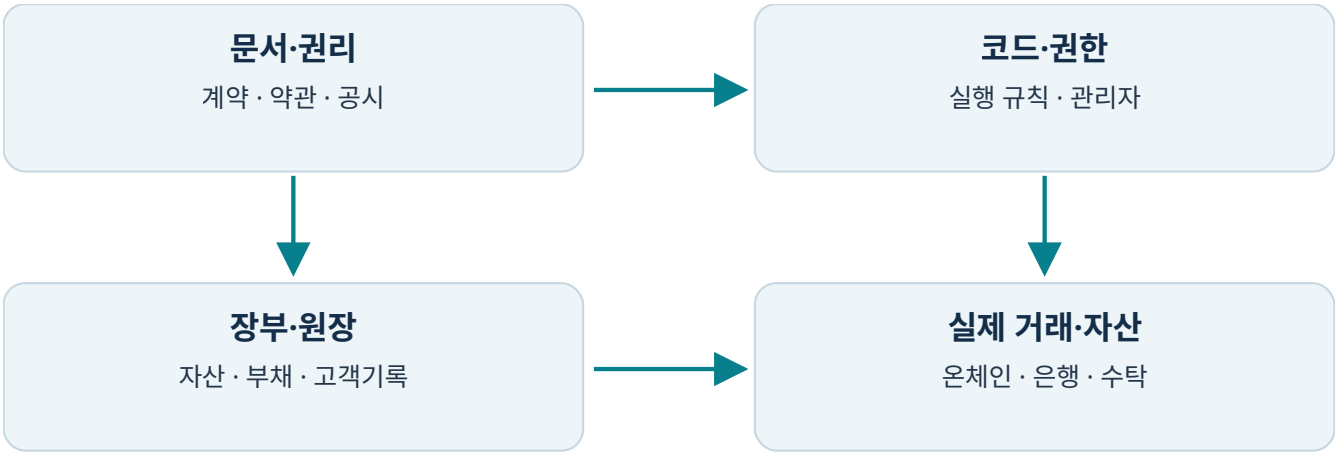
PART 1 · STEP 5 / RECONCILIATION

문서·코드·장부·거래를 대조한다

차이 자체보다 그 이유와 보완 장치가 설명되는지 확인한다.

대사는 숫자가 같은지 확인하는 데서 끝나지 않는다. 코드상 상태가 계약에서 약속한 권리와 연결되는지, 장부가 실제 지급·이전과 같은 시점을 사용했는지도 확인한다. 아래 네 자료군을 같은 대상과 기준시점에 놓고 비교하면 계산 오류와 범위·정의 차이를 구분하기 쉬워진다.

코드와 약관이 다르다는 사실을 발견해도 곧바로 오류라고 이름 붙이지 않는다. 일부 처리가 오프체인에서 이뤄지도록 설계됐는지, 약관의 판본이나 구현 버전이 다른지 먼저 확인한다. 설명 가능한 차이는 그 근거를 남기고, 설명되지 않는 차이는 권리·금액·통제에 미치는 영향과 함께 후속 확인 대상으로 삼는다.



차이 유형	다음 행동
사실·시점 불일치	출처·기준시점·범위를 재확인한다.
문서·구현 불일치	의도된 오프체인 처리인지 확인하고 권리·재무·통제 영향을 분석한다.
모듈별 전제 불일치	공통 사실·가정을 맞춘 후 재검토한다.
적용 기준에 따른 정당한 차이	차이의 이유를 설명하고 양쪽 결론을 보존한다.
미해결 차이	추가 자료·전문가 질문·유보 범위를 남긴다.

FC의 연결 검증을 대사 항목으로 사용한다. 산출물 F-05: 불일치·추가 확인표. 사실 문제는 2~3단계, 해석 문제는 4단계로 재검토한다. 해소 불가 시 조건·한계와 함께 종료한다.

PART 1 · STEP 6 / CONCLUSION

결론과 다음 행동을 확정한다

각 결론에 위험·해석·증거를 따로 표시하고 조건을 남긴다.

좋은 결론은 단정의 강도보다 근거와 다음 행동이 분명하다. 확인한 사실, 그 사실로 지지되는 판단, 아직 남은 조건을 구분하면 추가 자료가 들어왔을 때 무엇을 다시 검토할지도 알 수 있다. 아래 등급과 종료 기준은 분석을 멈출 지점과 다시 시작할 조건을 함께 정하기 위한 것이다.

채택

중요 전제가 확인되고 판단 근거가 충분하다.

조건부 채택

가정·조건이 충족되는 범위에서 판단한다.

복수 해석

대안 해석과 결과 차이를 병기한다.

결론 유보

사실·기준·검토 범위의 부족을 명시한다.

평가 축	기록 방식
위험	유형 + 영향도 + 발생가능성. 이미 발생한 오류·사고는 별도 기록.
해석 명확성	높음: 근거 명확 / 중간: 유추 필요 / 낮음: 합리적 해석 공존 / 유보 / 비적용
증거 충분성	E1: 핵심 근거 충분 / E2: 제한 존재 / E3: 간접·충돌 / E4: 핵심 미확보

세 축을 합산해 하나의 신뢰도 점수로 만들지 않는다. 가정은 증거가 아니므로 H로 별도 관리한다. 증거는 출처·직접성·완전성·시점에 맞춰 평가한다. 운영 효과성 증거 없이 통제 위험을 낮다고 확정하지 않는다.

마지막 네 질문

확인 항목	완료 전 질문
결론·범위	무엇을 어떤 범위에서 결론 내렸는가?
근거·가정	어떤 사실·기준·가정에 의존하는가?
미확인·조치	무엇이 미확인이고 누구에게 확인해야 하는가?
재검토	무엇이 바뀌면 다시 분석해야 하는가?

산출물 F-06: 결론 요약서. 추가 자료·조치 담당·재검토 조건까지 남긴다.

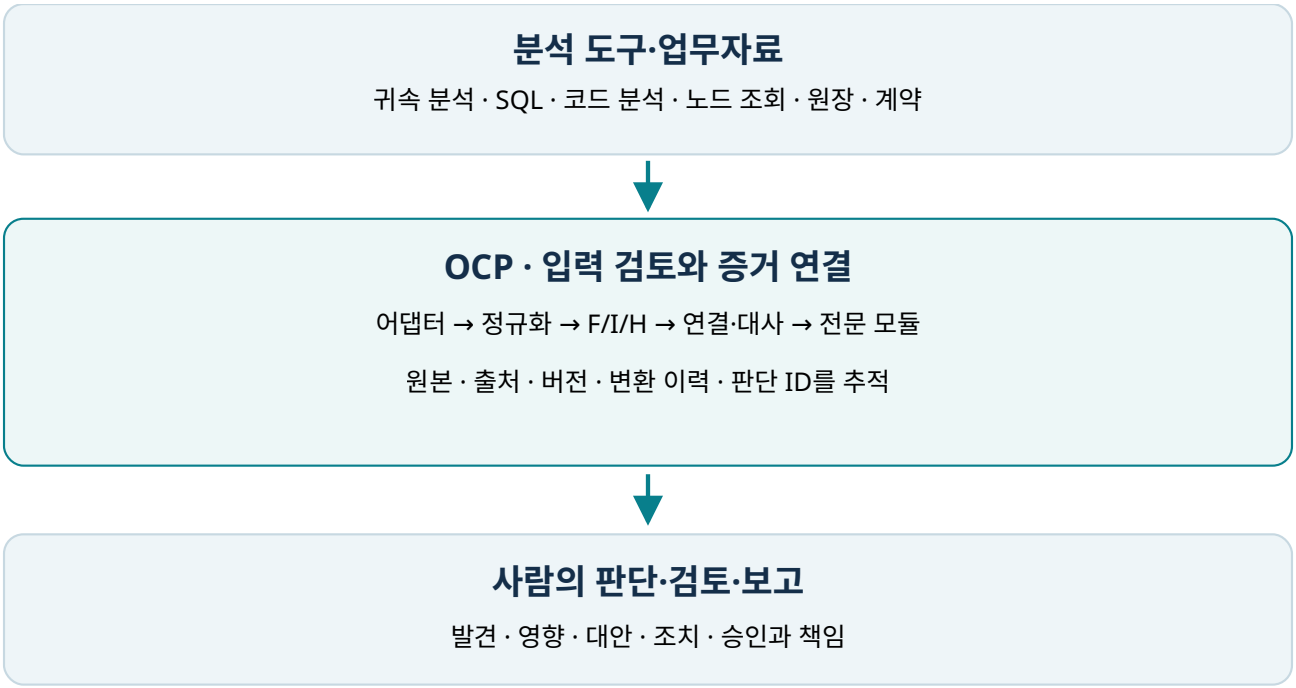
PART 2 · TOOL INTEGRATION / 1 OF 6

OCP는 판단 지원 계층이다

도구 결과와 업무자료를 받아 증거로 구조화하고, 전문가의 판단과 근거를 연결한다.

각 도구는 거래 추적·SQL 집계·정적 분석·원장 처리처럼 서로 다른 일을 잘한다. OCP는 이 결과를 하나의 증거 구조로 연결해 어떤 주장에 사용할 수 있는지 검토한다. 아래 구조에서 도구 출력은 판단의 입력이며, 도구가 제시한 점수나 라벨이 곧 전문 결론으로 바뀌지는 않는다.

이 구조에서는 도구가 바뀌어도 질문과 근거의 연결은 유지할 수 있다. 같은 집계를 다른 플랫폼에서 재현하거나 새로운 귀속 자료를 받으면 관련 주장과 입력만 갱신한다. 다만 결과가 비슷하다는 이유로 입력 범위까지 동일하다고 보지 말고 조회 조건과 원본의 계보를 먼저 비교한다.



역할	경계
분석 도구	조회·탐지·귀속·시각화·대사 등 도구가 제공하는 결과와 한계를 보존한다.
OCP	입력의 범위와 성격을 검토하고 질문·증거·전문 판단·발견을 연결·기록한다.
분석자·검토자	기준 선택·대안 해석·중요성·최종 결론과 업무 사용을 결정한다.

> 6단계는 그대로 유지한다. 이 확장은 주로 2단계 입력 검토, 3단계 연결 분석, 4~6단계 판단·보고를 지원한다. 특정 도구의 기능을 대체하거나 기능 부재를 전제하지 않는다.

PART 2 · TOOL INTEGRATION / 2 OF 6

질문에 맞춰 도구를 선택한다

제품명은 예시다. 계정·계약·권한·지원 범위를 확인한 뒤 가능한 형식으로 자료를 받는다.

도구 선택은 제품 이름보다 확인할 질문에서 시작한다. 거래 수량을 복원하려면 조회·집계 자료가 필요하고, 실제 당사자를 연결하려면 주소 정보와 오프체인 자료를 함께 봐야 한다. 아래 예시는 가능한 조합이며, 특정 제품을 보유했다는 사실을 분석의 충분성이나 정확성으로 평가하지 않는다.

자료에 접근할 수 없을 때도 도구를 추가하는 것만으로 문제가 해결되지는 않는다. 비공개 계약이나 고객 원장이 필요한 질문은 공개 체인 조회를 반복해도 남을 수 있다. 그 경우에는 가능한 분석 범위를 줄이고, 공개자료로 확인한 결과와 추가 자료 없이는 답할 수 없는 부분을 나누는 편이 더 정확하다.

확인할 질문	도구·자료 예시	OCP에 받을 내용	추가 확인
누구와 연결된 주소인가?	Chainalysis / TRM	주소·라벨·클러스터·출처·도구 신뢰도·시점	주체 귀속 근거·라벨 적용범위·동일 근거 중복 여부
어떤 거래가 얼마나 발생했나?	Dune / SQL / 노드·탐색기	쿼리·실행 ID·행·필터·블록 범위·조회 시각	결측·페이지네이션·중복·데이터 갱신·집계 정의
누가 코드를 바꾸거나 실행하나?	소스·노드 / Slither 등	코드·구현체·권한 상태·검사 규칙·탐지 결과	배포 코드 대응·프록시·정적 탐지의 오탐·실행 맥락
기록과 실제 자금은 맞는가?	원장·은행·수탁 / Excel · Python	원본 행·계정·거래 ID · 대사식·예외	모집단·마감시점·취소·미결·단위·절사
실제로 어떤 권리인가?	계약·공시·명부 / 문서 추출	원문·조항·버전·추출 위치·요약	최신성·원문 일치·당사자·조건·집행요건

도입 순서

1. 수동 입력

PDF · CSV · JSON · 화면 결과를 원본과 함께 등록

2. 반복 작업 정형화

동일 데이터 형식의 매핑·검증 스크립트 적용

3. 선택적 연결

필요한 경우 승인된 API · 내부 시스템 연계

도구 사용권이나 유료 API 접근을 새로 가정하지 않는다. 내보내기·저장·재배포 허용 여부와 실제 필드를 확인한다. 공개 포트폴리오에는 공개 가능한 범위만 사용한다.

> 도구 버전이나 내부 근거가 제공되지 않으면 “미제공”으로 기록한다. 모든 결과에 동일한 신뢰도 수치나 증거 등급을 강제로 부여하지 않는다. [S1~S4]

PART 2 · TOOL INTEGRATION / 3 OF 6

공통 입력 양식 · 어댑터 명세

어댑터는 서로 다른 출력 형식을 공통 기록으로 옮기는 매핑 규칙이다. 구현된 커넥터 목록이 아니다.

서로 다른 도구의 결과를 연결하려면 공통 기록 항목이 필요하다. 원본 위치·조회시점·대상·변환 이력을 남기면 같은 숫자가 어디에서 만들어졌고 어떤 조건에서 달라지는지 추적할 수 있다. 아래 입력 명세는 자료를 획일화하기보다 원래의 맥락을 잃지 않고 비교할 수 있게 하는 최소 연결 구조다.

특히 parent_input_id와 변환 이력은 같은 원문을 여러 번 독립 근거로 세는 일을 막는 데 도움이 된다. 원문을 CSV로 옮기고 SQL로 합계를 낸 경우 세 파일이 생겨도 경제적 사실의 원천이 세 개가 되는 것은 아니다. 원본·변환·집계·판단을 구분하면 오류가 생긴 단계도 찾아가기 쉬워진다.

필드 그룹	필수 기록
식별	input_id / case_id / question_id / source_id / parent_input_id
원본	원본 파일·위치 / 원본 행·페이지·JSON 경로 / 해시(확보 시) / 접근 권한
출처	제공자·제품·버전(가능 범위) / 결과 생성 시점 / 수집 시점 / 기준시점
분석 범위	체인·네트워크 / 주소·자산 / 블록번호·해시 / 거래기간 / 대상 주체
생성 조건	쿼리·실행 ID / SQL·매개변수 / 코드·컴파일·설정 / 필터·누락·페이지 범위
주장	assertion_id / 주장 내용 / 대상·관점 / F·I·H / 표시된 결과와 실체 주장 구분
변환	원시값 / 정규화값 / 단위·decimals·통화·시간대 / 변환식·스크립트 버전
근거·한계	근거 문서·도구 신뢰도 원문 / 독립성 / 제약·충돌·미확보 항목
검토·연결	수용·조건부·재확인 / 검토자·일자 / 증거 ID / 연결표·판단·발견·패턴 ID

입력의 최소 단위

한 파일을 한 결론으로 취급하지 않고, 같은 원본에서도 주장을 나눠 기록한다. 예를 들어 주소 라벨 표시 사실과 해당 주소의 실제 통제 주체에 대한 주장은 별도 assertion_id를 갖는다.

> 공통 양식은 F-02의 입력 명세로 사용한다. 미제공·미확인·비적용을 구분하고, 정규화 전 원본을 보존한다. 해시는 원본의 이후 변경 여부를 점검하는 수단이며 내용의 진실성을 증명하지 않는다.

PART 2 · TOOL INTEGRATION / 4 OF 6

도구가 아니라 주장을 분류한다

"도구가 이렇게 표시했다"와 "실제로 그렇다"는 서로 다른 주장이다.

하나의 출력 안에도 관찰과 추론이 섞여 있다. "도구가 X라는 라벨을 표시했다"와 "실제 통제자는 X다"는 서로 다른 주장이므로 나누어 기록한다. 아래 분류는 도구 전체를 믿거나 불신하는 방식 대신, 개별 주장에 필요한 근거와 남은 확인 절차를 정하도록 돕는다.

주소 라벨의 확신도가 높아도 법적 당사자나 실소유자가 확정되는 것은 아니다. 반대로 원장 기록과 온체인 수량을 연결할 때는 각각의 신뢰성뿐 아니라 두 기록이 같은 사건을 가리키는지도 검토한다. 주장별로 질문을 나누는 이유는 도구의 품질과 특정 결론을 지지하는 증거의 충분성을 구별하기 위해서다.

입력	F: 직접 확인할 범위	I·전문 판단: 추가 연결
주소에 거래소 X 라벨	제공자 화면·출력에 그 라벨이 표시됐다.	실제 통제자가 X라는 귀속은 근거를 검토한다. 제공 근거의 직접성에 따라 보완.
기준 블록의 totalSupply 응답	지정 네트워크·구현체·블록에서 특정 값이 반환됐다.	그 값이 전체 경제적 공급·고객 청구권·상환의무인지 별도 분석.
Dune 쿼리 집계	해당 실행·SQL·필터에서 집계값이 산출됐다.	데이터 포괄성·누락·집계 정의가 거래 실질에 맞는지 검증.
정적 분석기 경고	특정 코드·규칙·설정에서 경고가 출력됐다.	실제 취약성·악용 가능성·통제 영향은 코드·실행 맥락 검토.
내부원장 고객 귀속	원장에 해당 고객·수량·거래가 기록됐다.	완전성·권리·실소유·외부 잔액과의 일치 여부를 검토.

출처에서 결론까지 연결

원본 입력 ID → 원본 위치 → 정규화·변환 ID → 주장 ID → 증거 연결표 → 판단 ID → 발견 ID → 조치

H는 보완·스트레스·설계·실험 가정으로 별도 표시한다. 도구의 confidence와 OCP의 증거 충분성은 같은 값이 아니며 임의의 점수 변환을 하지 않는다.

> F라고 표시해도 모든 실제 사실이 확정되는 것은 아니다. 무엇을 관찰한 F인지 범위를 적고, 실체 주장에는 별도의 근거와 검토 상태를 붙인다.

PART 2 · TOOL INTEGRATION / 5 OF 6

수용 전 확인과 도구 간 충돌 처리

입력 → 범위 확인 → 원본 대사 → 수용 상태 → 증거 연결표

여러 도구가 같은 결과를 냈더라도 같은 원천 자료를 재사용했을 수 있다. 반대로 결과가 다르면 시점·단위·범위·주소 묶음의 정의가 달랐을 가능성부터 살핀다. 아래 절차는 결과의 다수결보다 근거의 독립성과 비교 조건을 먼저 확인하도록 설계되어 있다.

충돌 기록에는 비교 전 수치를 지우지 않고 각 결과의 조회 조건과 사용 목적을 남긴다. 예를 들어 한 도구가 주소별 잔액을, 다른 도구가 특정 집계 범위를 보여준다면 숫자가 달라도 바로 어느 쪽이 틀렸다고 할 수 없다. 정의를 맞춘 뒤에도 남는 차이를 실제 검증 대상으로 좁힌다.

확인 지점	실행할 점검	문제 발견 시
대상·시점	체인 ID·주소·자산·블록·시간대·데이터 기준일 일치	잘못된 대상·시점이면 재수집. 단순 최신 결과로 교체하지 않음.
완전성	행 수·기간·필터·페이지·실패·누락·업데이트 상태	부분 결과로 제한하거나 모집단 보완.
변환 정확성	단위·decimals·환율·부호·취소·중복·조인 검산	원본을 유지하고 변환 단계 수정·버전 기록.
근거 독립성	여러 도구가 같은 라벨·원장을 재사용하는지 확인	두 도구의 일치를 독립 증거 두 개로 계산하지 않음.
검토 상태	수용 / 조건부 수용 / 재확인·보류	핵심 공백은 결론과 다음 자료 요청에 연결.

라벨·수량·경고가 다를 때

순서	검토 작업
1 · 충돌 분리	어떤 주장이 충돌하는지 분리한다.
2 · 근거 비교	대상·범위·시점·원본·데이터 계보를 비교한다.
3 · 기준 확인	서로 다른 기준·클러스터 범위인지 검토한다.
4 · 차이 기록	해결한 차이와 남은 차이를 F-05에 기록한다.

다수결·브랜드 순위·도구 점수의 평균으로 결론을 정하지 않는다. 자동화는 수집·정규화·대사·예외 표시를 돕고, 수용·귀속·전문 판단의 책임은 분석자와 검토자가 맡는다.

PART 2 · TOOL INTEGRATION / 6 OF 6

도구 사용 실행표와 공식 참고

질문·조회·등록·검증·판단·재현의 순서와 기록 위치를 정한다.

실제 분석에서는 도구를 실행했다는 기록과 그 결과를 판단에 사용했다는 기록이 모두 필요하다. 입력을 수용한 이유, 확인한 한계, 후속 검토 대상을 남겨야 다른 사람이 같은 과정을 따라갈 수 있다. 아래 실행표는 이 기록의 순서를 정리하며, 공식 링크는 분석 시 적용 버전을 확인하는 출발점이다.

순서	작업	남길 기록
준비	질문·모듈·필요 데이터·사용권·원본 보관 범위 확정	F-01, 접근 범위·원본 위치
조회	주소·쿼리·블록·코드·원장 범위 고정 후 결과 확보	출력 원본·설정·실행 ID·생성 및 조회 시각
등록	공통 입력 양식에 매핑하고 단위·필터·F/I/H 검토	F-02 입력 명세·변환 로그
검증	범위·완전성·계보·충돌 검토, 증거 연결표 작성	F-02 첨부표·F-05
판단	M1~M5 검토 → 발견·영향·조치 → 책임자 검토	F-04·F-06·패턴 ID·한계
재수행	원본·SQL·설정·코드 버전으로 재현. 최신 결과와 구분	재현 결과·차이·변경 이력

제품 기능을 확인한 공식 자료

출처 ID	범위·링크
S1 Chainalysis	조사·추적 도구의 예시 https://www.chainalysis.com/solution/crypto-investigations/
S2 TRM	Forensics·귀속 정보의 예시 https://www.trmlabs.com/forensics
S3 Dune	실행별 결과 조회·메타데이터 https://docs.dune.com/api-reference/executions/endpoint/get-execution-result
S4 Slither	Solidity/Vyper 정적 분석·출력 사용 안내 https://github.com/crytic/slither

공식 자료 확인일: 2026-11-14. 아래 4개 URL을 직접 열어 공식 페이지의 접근 및 내용을 확인했다. 도구 기능 설명은 위 출처를 참고했고 공통 입력·F/I/H·검토 절차는 OCP의 설계다. 제품별 버전·요금·내보내기·API·라이선스는 적용 시 확인한다. 원본 접근이 제한되면 재현 가능 범위도 함께 기록한다.

PART 3 · REAL CASE / 1 OF 4

USDC: 실제 적용의 범위를 고정한다

R-USDC-01 · F-01 진행본. 현재 기준점을 보존한 뒤 4개 카드의 적용을 이어간다.

첫 실제 적용은 모든 기능을 완결하는 대신 어디까지 확인했는지를 고정하는 데 초점을 둔다. Ethereum USDC의 특정 블록 응답과 참고 소스를 묶되, 내부 운영과 준비자산 자료까지 확보한 것으로 넓히지 않는다. 아래 범위표를 기준으로 관찰·가설·추가 작업을 나누어 읽는다.

자료 · 실제 공개 | 카드 · 시드 | 범위 · 단일 RPC 읽기·참고 소스

범위 항목	고정한 내용
대상	Ethereum Mainnet native USDC / chain ID 1 0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48
기준 블록	26,407,530 / UTC 2026-11-13 17:26:47 한국시간 2026-11-14 02:26:47
블록 해시	0xd39bbb53541fa47b4bef7f741452eea5654d2fe2735db13cde083fe61cea8043
조회 범위	블록·저장 슬롯·역할·공급·배포 바이트코드. PublicNode 단일 공개 RPC의 읽기 응답
참고 소스	Circle stablecoin-evm 커밋 fc85788bc7c23cefe3df1a757133048bfddadeaa
분석 관점	외부 공개자료 분석. M5 중심으로 M1·M2의 증거 질문 연결. M3·M4는 필요한 쟁점만 기록

첫 적용의 네 질문

카드	질문
발행 FC-A01	누가 minter와 발행 한도를 설정하고 실제 발행 경로는 무엇인가?
역할 FC-C02	owner·masterMinter·pauser·blacklister와 proxy admin의 관계는?
변경 FC-E01	표준 슬롯 외의 구현·관리 경로와 배포 소스가 어떻게 연결되는가?
동결 FC-D02	어떤 호출 경로·대상·예외에 제한이 적용되는가?

확정 블록 표시는 제공자의 응답으로 기록했다. 독립 노드 교차 검증, 배포 소스-바이트코드 대응, 카드별 전체 경로 검토는 아직 완료되지 않았다.

PART 3 · REAL CASE / 2 OF 4

슬롯이 0인데, 구현은 존재한다

관찰 사실과 그 사실에서 가능한 해석을 분리한다.

조회 응답과 그 원인에 관한 설명을 구분해 읽는다.

자료 · 실제 공개 | 카드 · 시드 | 범위 · 단일 RPC 읽기·참고 소스

관찰 항목	지정 블록의 반환값
ZeppelinOS 구현 슬롯	0x43506849d7c04f9138d1a2050bbf3a0c054402dd
ZeppelinOS 관리자 슬롯	0x807a96288a1a408dbc13de2b1d087d10356395d2
ERC-1967 구현·관리자 슬롯	둘 다 0
코드 조회	위 구현 주소에서 코드 반환. 코드의 존재와 변경 권한의 적절성은 별도 질문
일반 함수 호출	admin()·implementation()은 이번 요청 조건에서 execution reverted

역할 상태의 스냅샷

조회	반환 주소
owner()	0xfcb19e6a322b27c06842a71e8c725399f049ae3a
masterMinter()	0xe982615d461dd5cd06575bbea87624fda4e3de17
pauser()	0x4914f61d25e5c567143774b76edbf4d5109a8566
blacklister()	0x0a06be16275b95a7d2567fbdae118b36c7da78f9

현재 말할 수 있는 것

ERC-1967 슬롯이 비었다는 관찰만으로 구현 부재·업그레이드 불가를 결론낼 수 없다. 다른 슬롯에는 구현 주소가 있고 코드도 조회됐다. 프록시 카드는 표준 명칭보다 실제 저장·실행 경로를 따라가야 한다.

I · 되돌림 원인에 관한 검증 전 가설

구분	기록
참고 소스의 기록	보존한 공식 소스 주석에는 2020-05-13에 admin()·implementation()의 ifAdmin을 제거했다고 적혀 있다. 배포 코드와의 동일성은 미확인.
I · 후보 해석	배포 프록시가 해당 수정 전의 관리자 제한형일 수 있다. 비관리자 호출이 구현체로 위임되어 되돌려졌을 가능성은 가설이며, 수정 전 버전 사용을 확정하지 않는다.
다음 확인 · 미수행	같은 블록·프록시·함수·calldata에서 from만 관찰된 관리자 주소로 지정한 eth_call을 일반 호출과 비교한다. 반환값과 슬롯을 대조하고 실제 배포 프록시 코드의 분기·소스 이력도 확인한다.

from 지정은 읽기 시뮬레이션의 호출자 조건일 뿐, 관리자 키 보유·실제 서명 권한을 증명하지 않는다. 성공해도 구체적 소스 버전·되돌림 원인의 확정에는 코드 대응 검토가 더 필요하다. 실패하면 대안 원인을 조사한다.

> R-USDC-01 → FC-E01(51~52쪽) 질문 보완. 재조회하면 요청·응답·기준 블록을 새 F로 기록하고, I의 지지·기각과 남은 한계를 갱신한다. 역할 주소의 차이는 승인 독립성의 증명이 아니다.

PART 3 · REAL CASE / 3 OF 4

확인한 신호를 카드의 질문으로 바꾼다

참고 저장소의 기능을 현재 배포 동작으로 자동 전환하지 않는다.

관찰된 주소와 참고 코드의 기능은 카드별 질문을 구체화하는 재료다. 그러나 역할 주소를 읽었다는 사실만으로 모든 실행 경로를 검토한 것은 아니다. 아래 표는 현재 확보한 단서가 어떤 카드에 연결되고, 다음 확인이 무엇인지 보여주며 규제·AML 판단에 필요한 오프체인 자료도 분리한다.

M1의 동결 질문은 “blacklister가 누구인가”에서 끝나지 않는다. 결정 주체·사유·대상·시점, 코드가 제한하는 범위, 해제와 고객 대응 기록을 각각 연결해야 한다. 현재 확보하지 못한 자료는 요청 항목으로 남기고, 기술적 차단 기능을 확인한 것을 규제상 의무 이행의 확인으로 표현하지 않는다.

자료 · 실제 공개 | 카드 · 시드 | 범위 · 단일 RPC 읽기·참고 소스

기능 카드	확보한 근거	다음 확인
발행 FC-A01	참고 코드의 minter별 한도 경로, masterMinter·공급 응답	배포 구현·외부 관리 계약·minter 모집단·실행 샘플 연결
역할 FC-C02	역할별 주소 응답, 자체 역할 구조의 참고 코드	검사·권한 변경·이양·우회와 실제 주체 연결
변경 FC-E01	슬롯 계열별 응답·구현 코드, 일반 조회 호출 되돌림	배포 프록시 접근 조건·구현 대응·업그레이드 이력
동결 FC-D02	blacklister 주소, 공식 Blacklistable 참고 코드	실제 구현의 이전·승인·발행·소각·서명 경로와 예외

M1: 동결을 서비스·행위와 연결

행위	확인할 사실·증거	판단 전제
제한 결정	결정 주체·대상·사유·시점 / 정책·승인·근거 문서	관할·사업자 지위·적용 요건을 별도로 특정
기술적 차단	코드·상태·실행 경로 / 고객·주소·수탁 관계	규범상 요구 범위와 기술적 효과를 구분
해제·고객 대응	해제 기준·승인·로그·통지·이의 처리 기록	제한·해제의 적정성과 실제 이행 근거 확인

M3는 거래유형·고객·거주지·서비스 제공자·보고 범위의 자료 요청 단계다. 한국·미국·EU의 구체적 적용 결론은 아직 작성하지 않았다.

> 현재 성과는 실제 적용 범위와 추가 질문을 좁힌 것이다. 기술 역할 주소를 규제상 책임자나 고객 실소유자로 곧바로 귀속시키지 않는다.

PART 3 · R-USDC-01 / PUBLIC-EVIDENCE UPDATE

공급과 준비자산, 두 기준점을 나눈다

11월 온체인 관찰은 보존하고, 9월 공개보고서의 수치 재계산을 별도 기준점으로 추가한다.

기존 Ethereum 조회는 단일 RPC 응답이다. 이번 보완은 공개 준비자산 보고서의 정의와 산술을 검토한 것이며, 같은 시점의 모든 체인 공급량이나 은행·수탁 원장을 직접 대사한 작업이 아니다.

기존 관찰 · 2026-11-13	보존한 결과
체인 / 대상	Ethereum Mainnet / native USDC · 프록시 주소는 21쪽 참조
기준 블록 / 시각	26,407,530 / 2026-11-13 17:26:47 UTC
totalSupply / decimals	44,630,813,371.668586 USDC / 6
증거 수준	기존 착수팩의 응답을 인용. 이번 개정에서 RPC를 재조회하지 않음

추가한 공개자료 검토 · 78~83쪽

완료한 범위	남은 범위
2026년 9월 보고서의 판본·기준시각·정의 고정	보고서 기준시각과 일치하는 전체 체인 공급의 독립 재구성
보고서 유통량 조정 및 준비자산 소계·총계 재계산	은행·수탁 확인, 내부 원장, 결제시차 개별 내역의 직접 대사
F-02 증거 연결, F-05 미해결, F-06 범위별 결론 작성	배포 코드 대응·키 운영·독립 검토자의 재현

기존 수집 제약의 상태

과거 20,000,000번 블록의 상태 접근 실패, Etherscan 직접 대조 미완료는 기존 기록대로 남긴다. 역할 주소만으로 실제 운영 주체·승인 독립성을 확정하지 않는다.

> 11월 Ethereum 공급으로 9월 전체 준비자산을 나눈 비율은 제시하지 않는다. 80쪽의 비율은 동일한 보고서 내부의 정의·수치에 한정한 산술 재현이다. 준비자산 전체 대사 또는 독립 보증의 완료를 뜻하지 않는다.

기존 출처: 공식 주소 / 고정 커밋 / 투명성 페이지 / 기존 USDC F-01 착수팩

PART 3 · 03 / WORKED EXAMPLE

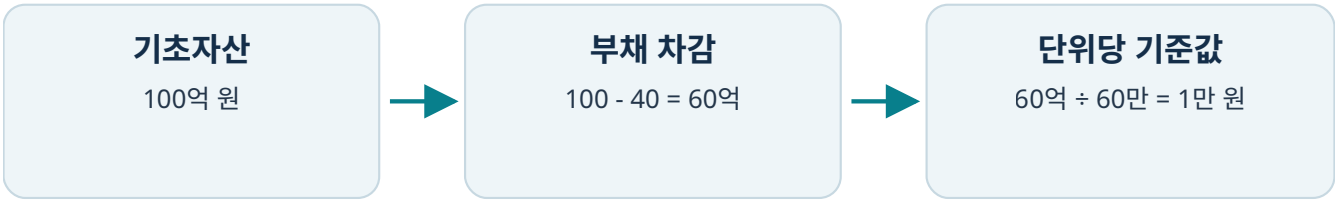
예시: 건물 토큰의 권리와 가치

전체 수치는 절차 설명을 위한 가정이다. 실제 상품·가격·법률의견이 아니다.

이 교육 사례는 같은 건물에서도 자산 전체의 가치와 투자자가 보유하는 권리의 가치가 달라질 수 있음을 보여준다. 차입금과 비용·배분 조건을 거치면 토큰 보유자에게 돌아가는 현금흐름의 범위가 달라진다. 아래 수치는 합성 조건이며 실제 상품의 권리나 가격을 설명하는 자료가 아니다.

자료 · 합성 | 카드 · 비적용 | 범위 · 서술·계산

가정	내용
기초자산 가치	100억 원
차입금	40억 원
비용·세금 등	설명 편의를 위해 생략
투자자 권리	잔여가치에 비례해 참여하는 권리로 가정
발행 수량	60만 개



위 단위당 값은 해당 가정하의 단순 계산값이다. 실제 발행가격·시장가격·공정가치와 같다고 단정하지 않는다.

변경 가정	계산 결과	추가 확인
건물 가치 80억 원	잔여 40억 → 단위당 약 6,667원	평가 근거·회수 비용·배분순위
담보부 채권형으로 변경	단순 잔여가치 배분식을 재사용할 수 없음	원리금·만기·담보·회수구조
토큰 이전 제한 추가	가치 영향은 별도 분석	투자자 자격·유동성·이전 로직

> 실제 케이스에서는 실제 공개자료로 기준 분석을 만든 뒤, H 가정을 추가하고 기준 대비 차이를 설명한다.

PART 3 · EXAMPLE / F-01 · F-02

작성 예시 1: 질문과 증거

교육용 합성 자료다. 특정 실제 상품이나 실제 컨트랙트 실행 결과가 아니다.

작성 예시는 처음부터 정답을 적는 방식보다 질문과 증거를 나누어 출발한다. 투자자 관점을 정한 뒤 어떤 문서가 권리를 설명하고 어떤 자료가 코드·수량을 보여주는지 구분한다. 아래 기록을 따라가며 확인 가능한 사실과 가정으로 보완한 부분을 같은 칸에 섞지 않는 연습을 한다.

자료 · 합성 | 카드 · 비적용 | 범위 · 서술·계산

F-01 분석 범위·질문표

항목	작성 내용
사례 ID · 분석 단위	EX-01 / 부동산 수익참여형 토큰 상품 1개
질문·관점	투자자 관점에서 관리자 권한과 이전 제한이 설명 문서와 일치하는가?
기준·관할	학습용 시점 T0. 특정 법역의 법적 유효성 판단은 제외.
선택 모듈	M4 거래구조화·가치평가, M5 IT감사·기술 리스크. 권리관계는 공통 전제로 검토.
종료 기준	권한·이전 제한 차이 식별, 단순 가치모델 검산, 후속 확인사항 제시.

F-02 증거·가정 목록

ID	예시 자료·가정	사용·한계
D-01	합성 설명문: 적격 투자자 간 이전, 운영사 단독 동결 불가	실제 계약 또는 공식 공시가 아님
D-02	합성 권한표: 관리자 A가 동결·해제 가능	배포 코드·실제 거래 검증 미수행
H-01	자산 100억, 부채 40억, 60만 단위 발행, 비용 생략	학습용 가치·현금흐름 가정
H-02	건물 가치가 80억으로 하락	기준 대비 스트레스 비교
H-03	운영사 단독 승인 → 다중 승인·기록 절차로 대체	통제 개선 설계. 효과는 별도 검증 필요

F: D-01과 D-02에 서로 다른 조건이 기재돼 있다. I: 설명·권한 설정의 정합성 문제가 있을 수 있다. 실제 권리·운영 효과에 대한 결론은 유보한다.

PART 3 · EXAMPLE / F-03 · F-04

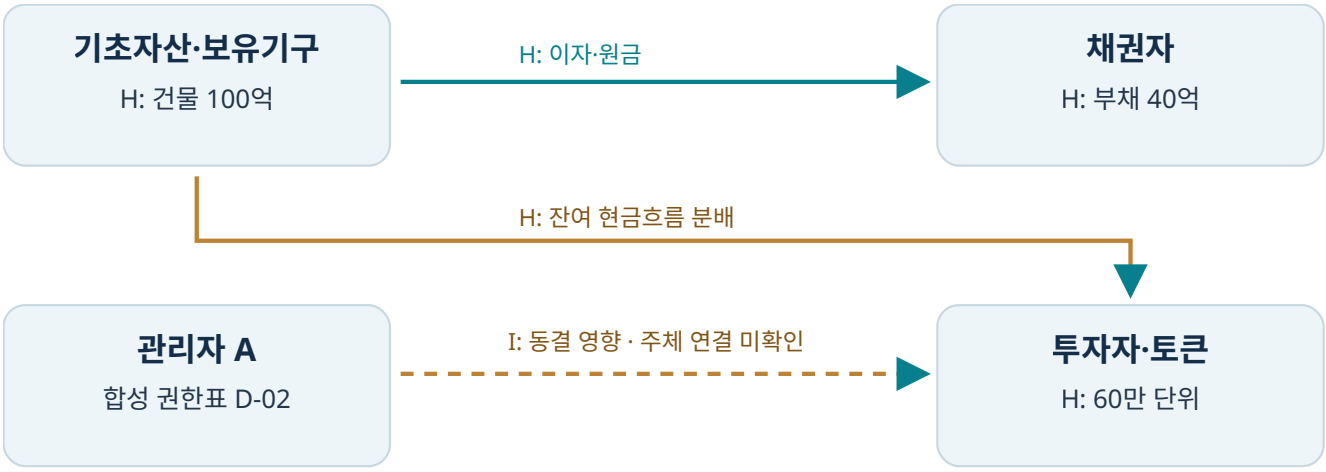
작성 예시 2: 구조와 판단

가정에 따른 경제적 계산과 권한의 적정성 판단을 분리한다.

거래구조도는 토큰 이동을 그리는 데서 한 단계 더 나아간다. 자산 보유자·발행자·투자자 사이의 계약 관계와 현금 이동을 함께 표시해야 기술 기록이 어떤 경제적 권리와 연결되는지 볼 수 있다. 아래 판단표는 이 연결을 바탕으로 수치 계산과 권리 해석의 전제를 분리해 기록한다.

자료 · 합성 | 카드 · 비적용 | 범위 · 서술·계산

F-03 거래구조·귀속 분석도



그림은 모두 합성·가정에 기반한다. D-02는 실제 주체의 신원을 증명하지 않는다. 표시된 권한은 법적 정당성·회계상 통제와 별도로 판단한다.

F-04 전문 분야별 판단표

질문	판단·근거	상태·한계
단위당 기준값은?	H-01: (100억 - 40억) ÷ 60만 = 1만 원	조건부 계산. 시장가격·공정가치 결론 아님
가치 하락 시?	H-02: (80억 - 40억) ÷ 60만 ≈ 6,667원	비용·세금·순위 생략. 추가 모형화 필요
권한 설명이 일치하는가?	D-01은 단독 동결 불가, D-02는 A의 동결 가능으로 설정	예시 자료의 불일치. 실제 코드·실행은 미검증
어떤 통제가 필요한가?	H-03: 승인 분리·권한변경 기록·사후 모니터링 대안	키·서명자·우회 경로·실제 운영 테스트 필요

설명 조건과 권한표를 대조하고, 정합성 차이가 권리·운영 판단에 주는 영향을 추가 확인한다.

PART 3 · EXAMPLE / F-05 · F-06

작성 예시 3: 차이와 후속 조치

재검토 후에도 해결되지 않는 질문은 명시적으로 남긴다.

검토 중 발견한 차이는 모두 같은 종류의 문제는 아니다. 자료가 부족한 경우, 코드와 문서가 다른 경우, 전문 기준의 정의가 다른 경우에는 후속 조치가 달라진다. 아래 예시는 차이를 발견한 뒤 자료 요청·판단 유보·재검토 조건으로 이어지는 기록 방식을 보여준다.

자료 · 합성 | 카드 · 비적용 | 범위 · 서술·계산

F-05 불일치·추가 확인표

항목	검토 내용	조치
설명 ↔ 권한	D-01과 D-02의 동결 조건이 다름	배포·구현 코드, 실제 권한·키 관리 자료 요청
권한 ↔ 주체	관리자 A의 실제 통제자 미확인	서명·승인·운영 근거 확보. 주소 라벨만으로 확정 금지
설계 대안	다중 승인으로 바꾸는 H-03	우회 권한·가용성·비용·실행 지연을 비교
검증 계획	실제 데이터·테스트 미수행	미승인 이전·동결·권한 교체의 예상/실제 결과 기록

F-06 종합 판단·후속 조치

항목	작성 내용
종합 결론	학습용 자료의 권한 설명은 불일치한다. 실제 상품의 법적·운영상 결론은 유보한다.
조건부 결과	단위당 1만 원 및 약 6,667원은 H-01/H-02의 계산 결과다.
위험	기술·운영. 영향: 조건부로 중대 가능. 발생가능성: 실제 증거 부족으로 평가 유보.
해석 명확성	예시 문구 비교: 높음. 실제 권리·규제 효과: 판단 유보.
증거 충분성	예시 자료 내 문구 확인과 실제 입증을 구분. 실제 주체·운영·권리의 핵심 증거는 E4.
조치·종료	추가 자료 확보 전 유보. 자료 확보 시 2~5단계 재수행.
재검토 조건	구현체·권한·약관 변경, 주체 확인 자료 또는 실제 테스트 결과 확보.

> 설계 대안의 예상 효과는 별도 테스트로 확인한다. 후속 자료와 실제 운영 결과를 연결한다.

PART 3 · DEMO-USD / 1 OF 6

의뢰와 최초 자료: 106%라는 설명

V-01 · 발행·상환·준비자산·권한의 정합성을 검토한다.

DEMO-USD는 처음 제시된 비율이 왜 그럴듯해 보이는지부터 출발하는 합성 사례다. 처음에는 은행잔액의 구성과 상환 대기의 처리 상태를 모두 알지 못한다. 아래 최초 자료만으로 질문을 만든 뒤, 뒤에서 추가 자료를 받아 판단이 어떻게 바뀌는지 순서대로 따라간다.

이 사례를 연습할 때는 추가 자료를 먼저 읽지 않고 최초 자료만으로 필요한 확인 질문을 써보는 편이 좋다. 106%라는 결과를 재계산하는 일과 그 비율에 사용된 자산·의무가 같은 상품 범위인지 묻는 일은 다르다. 정답 숫자를 맞추기보다 어떤 자료를 요청해야 판단이 달라지는지 찾아보는 것이 목적이다.

자료 · 합성 | 카드 · 시드 | 범위 · 서술·계산

가상 약관은 적격 보유자의 1단위당 1달러 상환청구권과 지급 전 권리 존속을 정한다. 분석 기준은 T0의 자료 간 정합성이다.

자료 ID	최초 자료
V-D01	약관: 1:1 상환, 요청 시 지급절차 개시. 지급 완료 전 청구권 존속.
V-D02	보고서: 은행잔액 1,230만 달러 / 상환의무 1,160만 달러 / 약 106%.
V-D03	체인 스냅샷: 총공급량 1,200만. 상환 대기 지갑 40만 포함.
V-D04	권한표: 업그레이드 2-of-3. 별도 발행자 mint 가능, 온체인 한도 없음.
V-D05	운영 설명: 발행은 다중 승인. 상환 신청 40만을 보고 의무에서 차감.

범위표의 네 질문

질문	확인할 연결
Q1	공급·상환 대기·보고 의무의 잔액이 연결되는가?
Q2	은행잔액 전체가 해당 상품의 준비자산인가?
Q3	신청·잠금·소각·지급을 구분했는가?
Q4	다중 승인 설명이 별도 발행 권한에도 적용되는가?

> 접수 → 구조 복원 → 초기 추론 → 추가 자료 → 판단 수정 → 발견·후속 조치. 자료 ID와 판단 이력을 연결하면서 새 증거가 결론을 어떻게 바꾸는지 따라간다.

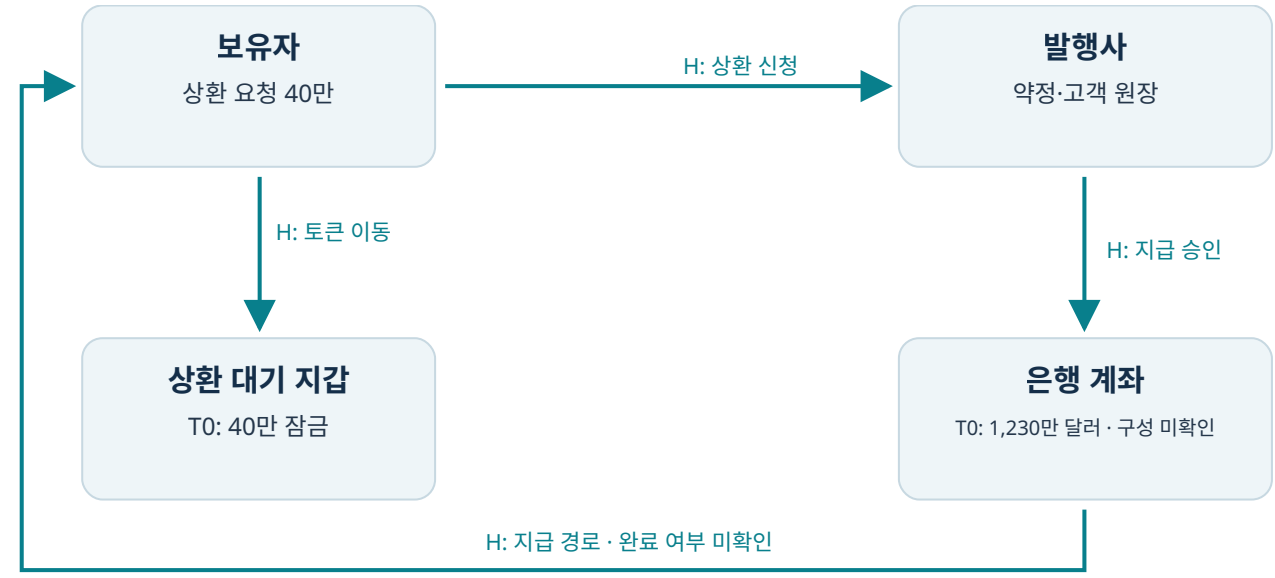
PART 3 · DEMO-USD / 2 OF 6

거래·권한·의무 구조 복원

Step 3 · 같은 토큰을 유통분과 상환 대기분에 중복 계산하지 않는다.

총공급량과 상환의무를 비교하려면 토큰이 어디에 있는지만이 아니라 그 상태가 어떤 권리를 뜻하는지 살펴야 한다. 상환 대기 지갑에 잠겨 있다는 사실은 지급 완료나 소각과 같지 않다. 아래 구조도는 보유자·발행자·계좌·대기 지갑을 연결하되 아직 확인하지 못한 계좌 구성은 열어 둔다.

자료 · 합성 | 카드 · 시드 | 범위 · 서술·계산



영역	복원한 구조·남은 질문
토큰	총공급량 1,200만 = 일반 보유 지갑 1,160만 + 상환 대기 40만. 잠금은 소각이 아님.
상환	가상 약관상 지급 전 청구권 존속. 요청만으로 관련 의무가 사라지는지 검토 필요.
자금	초기 은행잔액 1,230만의 계좌별 구성·명의·제약은 추가 확인 대상.
권한	업그레이드 다중 승인과 별도 발행 권한을 구분. 키·승인자·실제 운용은 미확인.
귀속	가상 발행사를 계약상 의무자로 전제하되, 관리자 주소의 실제 키 통제는 별도 증거 필요.

> 지급 경로는 H 가정이다. 다음 확인 대상은 T0 지급 완료 여부와 계좌 구성이다.

초기 추론 · 의무 40만 조기 차감 가능성, 은행자금 범위 혼입 가능성, 발행 승인 범위 공백을 추가 자료로 확인한다.

PART 3 · DEMO-USD / 3 OF 6

추가 자료를 받고 판단을 수정한다

Step 2~5 재수행 · 가상의 추가 자료는 최초 자료와 별도 버전으로 기록한다.

추가 자료가 들어오면 최초 결론을 방어하기보다 어떤 전제가 달라졌는지 기록한다. 이 사례에서는 지급 여부와 계좌 구성에 관한 자료가 분모·분자 범위를 다시 정하게 만든다. 아래 수정표와 계산은 그 연결을 보여주며 비율이 맞아졌다는 사실을 자산의 안전성 보증으로 확대하지 않는다.

여기서 중요한 것은 100%라는 최종 숫자보다 조정 이유를 설명할 수 있다는 점이다. 운영자금은 상품 준비자산과 구분하고, 미지급 상환 대기는 약정상 의무가 남는지 확인한다. 같은 수정이 다른 구조에서도 필요한지는 별도 검토해야 하므로 이 계산을 스테이블코인 일반의 비율 산식으로 옮기지 않는다.

자료 · 합성 | 카드 · 시드 | 범위 · 서술·계산

추가 자료 ID	새롭게 설정한 가상 내용	변경된 판단
V-D06	40만 상환은 요청·잠금 단계. 현금 지급은 T0 후 예정이며 소각도 미실행.	T0 청구권은 존속. 보고 의무 차감 재검토.
V-D07	은행 1,230만 = 상품 계좌 1,200만 + 별도 회사 운영계좌 30만.	운영계좌 30만은 본 시나리오의 상품 준비자산에서 제외.
V-D08	분석기간 발행 승인기록 1건만 제공. 전체 모집단·키 독립성 자료 없음.	일부 승인기록 존재와 전체 통제 효과성을 구분.

수정 대사 — 단위: 만 달러, 토큰은 만 단위

구분	초기 보고	조정	수정 기준
상품 준비자산	1,230	운영자금 -30	1,200
보고 목적의 총 상환의무	1,160	대기 청구권 +40	1,200
구성	일반 보유분 1,160	대기 청구권 40	합계 1,200
비율	1,230 ÷ 1,160 ≈ 106.03%	분자·분모 범위 조정	1,200 ÷ 1,200 = 100%

대사 기준은 V-D01의 약정과 보고 목적 의무다. 정식 회계 분류·분개는 별도 질문으로 남긴다.

> 변경 이력: 초기 “40만 차이 원인 미확인” → 추가 자료 후 “지급 전 대기분 차감”으로 구체화. 통제 효과성은 추가 자료 후에도 유보한다.

PART 3 · DEMO-USD / 4 OF 6

발견사항 요약: 무엇을 밝혔는가?

추가 자료로 해결한 차이와 아직 남은 질문을 함께 기록한다.

발견사항은 “차이가 있다”는 진술보다 원인·영향·근거를 함께 보여줄 때 유용하다. 아래 세 발견은 의무의 존속, 준비자산 범위, 기술 권한과 승인 기록의 연결을 각각 다룬다. RF 패턴 ID는 이 사례에서 얻은 질문을 다른 사례에 재사용하기 위한 연결이며 동일한 문제가 반복됐다는 판정은 아니다.

보고서를 읽는 사람은 각각의 발견이 어떤 자료에서 나왔고 무엇을 바꾸는지 빠르게 알 수 있어야 한다. 발견 ID 옆에 증거·패턴·영향받는 모듈을 연결하면 세부 자료를 모두 읽지 않아도 검토 경로를 따라갈 수 있다. 이를 통해 발견 요약은 긴 보고서의 결론을 되풀이하는 대신 근거로 들어가는 입구가 된다.

자료 · 합성 | 카드 · 시드 | 범위 · 서술·계산

발견 ID·핵심	근거와 영향	판단·조치
V-F01 · RF-01 상환 대기분 조기 차감	V-D01·03·06. 지급 전 대기 청구권 40만 달러가 보고 목적 의무에서 차감됨.	가정한 약정하에서 의무 +40만. 상환 상태별 대사·처리 규칙 정비.
V-F02 · RF-03 준비자산 범위 혼입	V-D02·07. 은행 총액에 운영계좌 30만 달러가 포함됨.	이 사례의 상품 준비자산에서 30만 제외. 계좌·보고 범위 연결.
V-F03 · RF-02 승인 통제의 확인 공백	V-D04·05·08. 업그레이드 다중서명과 별도 발행 권한은 구분됨. 승인 1건만 확보.	설명만으로 전체 발행 통제의 설계·운영 효과를 결론낼 수 없음. 키·모집단·승인 테스트 요청.

패턴 연결: V-F01 → RF-01 잠금·소각 / V-F02 → RF-03 비율의 범위 / V-F03 → RF-02 권한·통제.

증거 연결표 적용

주장	두 영역의 연결	해결·남은 질문
40만이 지급됐는가?	대기 지갑·소각 상태 ↔ 요청명세·지급기록	V-D06의 합성 자료로 T0 미지급 설정 확인. 의무 대사 수정.
1,230만이 전부 상품 자금인가?	공급·청구권 잔액 ↔ 계좌별 구성·보고 범위	V-D07로 상품 1,200만·운영 30만 구분. 실제 존재·제약은 별도.
발행 권한은 다중 승인되는가?	별도 minter ↔ 승인·키·운영 기록	일부 근거만 존재. 실제 운영 효과성은 남은 검토 과제.

> 비율 106.03% → 100%는 분자·분모 범위를 맞춘 계산 결과다. 자산의 안전성·유동성·무담보성·상환능력을 입증한 결과로 확대하지 않는다.

PART 3 · DEMO-USD / 5 OF 6

종합 판단과 후속 조치

발견 → 금액 영향 → 근거 → 담당·재검토 조건으로 인계한다.

종합 의견은 계산 결과와 전문 판단의 범위를 구분해 모은다. 일부 수치가 정리돼도 키 운영·승인 모집단·법적 권리의 자료가 부족하면 그 부분은 별도 과제로 남는다. 아래 표를 통해 확인된 조정, 아직 판단하지 못한 내용, 다음 자료 요청이 어떻게 하나의 보고서로 연결되는지 살펴본다.

후속 조치에는 단순히 “추가 확인 필요”라고 적기보다 무엇을 받으면 어떤 판단을 다시 할 수 있는지 쓴다. 예를 들어 승인 기록의 모집단이 확보되면 건별 대사의 범위를 정할 수 있지만, 서명자 독립성을 설명하려면 별도 운영 자료가 필요할 수 있다. 자료 요청과 판단의 연결이 분명할수록 다음 검토도 효율적이다.

자료 · 합성 | 카드 · 시드 | 범위 · 서술·계산

종합 항목	판단·남은 질문
대사 결론	V-D03·06·07에 따라 준비자산과 보고 목적 상환의무를 각각 1,200만으로 조정. 1,200 / 1,200 = 100%.
발행 통제	업그레이드 승인과 별도 minter를 구분. 승인 1건만으로 기간 전체 운영 효과성·키 독립성을 확정할 수 없음.
모듈 연결	M2는 범위·상태 대사, M5는 권한·승인. M1·M3는 관할·고객·거래 자료 요청, M4는 지급·소각·실패 절차 설계.
결론의 범위	자료 간 정합성은 조건부 채택. 자산 존재·무담보성·권리 집행·상환능력은 별도 증거 필요.

개선과 검증 계획

조치·담당 예	확인할 결과
재무 · T0+2영업일	대기 의무·계좌 범위 반영 보고 수정과 원장 대사
운영 · 다음 상환 배치	요청·지급·소각·실패 상태와 고객 청구권 연결
기술·리스크 · T0+5영업일	발행·변경 모집단, 키·승인·우회·한도 검토
전문 담당 · 외부 활용 전	관할·기준별 권리·회계·조세 판단을 별도 작성

재검토 조건: 약관·구현·권한 변경, 지급·소각 실패, 계좌 범위·제약 변경, 신규 관할·거래 유형. RF-01 잠금/소각, RF-02 권한/통제, RF-03 비율 범위와 연결한다.

PART 3 · DEMO-USD / 6 OF 6

도구 입력에서 기록·보고까지

동일 자료를 다른 형식으로 받은 경우, 독립 증거 수를 늘리지 않는다.

같은 원문을 도구별 형식으로 바꾸어도 독립 증거가 새로 생기는 것은 아니다. 이 페이지의 입력은 기존 합성 자료를 재표현한 예시이며 실제 제품을 실행한 결과가 아니다. 아래 흐름은 원문에서 입력·주장·검토·보고로 이어지는 연결을 설명하고 각 변환의 부모 자료를 유지하는 이유를 보여준다.

이벤트 집계와 원장 재표현이 같은 자료에서 나왔다면 둘을 교차 확인한 것처럼 세지 않는다. 원문에 없는 정보가 변환 과정에서 가정으로 추가됐다면 그 위치를 표시한다. 이렇게 입력의 계보를 유지하면 형식이 다른 출력 때문에 증거가 더 풍부해 보이는 착시를 줄일 수 있다.

자료 · 합성 | 카드 · 시드 | 범위 · 서술·계산

입력 ID	도구 형식·입력	연결·검토
V-T01	노드 형식: 공급 1,200만	V-D03 재표현. 코드·상태·기준 블록 연결.
V-T02	SQL 형식: 대기 주소 40만	V-D03 재표현. 주소-상환업무는 V-D05·06으로 연결.
V-T03	귀속 라벨: 발행사 A 관련	라벨 표시와 실제 통제 추론을 분리. 제공 근거·실제 키 운영 요청.
V-T04	정적 분석 형식: 별도 minter	탐지 결과와 실제 영향 구분. 권한·실행·승인 자료 연결.
V-T05	원장·계좌 CSV: 1,160 / 1,230만	V-D02 재표현. V-D06·07로 의무·계좌 범위 보완.

기록의 한 줄 연결

V-T02 → V-D03·05·06 → V-F01 → RF-01 → 상환 상태별 대사·처리 개선

양식	이 사례에서 남기는 기록
F-01~F-03	질문·관점·T0 / V-D01~08·출처·가정 / 거래·권한·의무·자금 구조
F-04~F-06	초기·수정 판단 / 차이·추가 요청 / 발견·영향·근거·후속 조치
FC 연결	FC-A01·C02·E01은 권한·발행 질문을 구성. FC-D02는 근거 부족으로 미확인.

> V-T01~05는 합성 자료의 재표현이다. 특정 제품을 실제 실행한 출력이 아니다. 판단을 바꾼 것은 도구 개수가 아니라 추가 자료 V-D06·07과 권한 검토의 연결이다.

PART 4 · F-01 / WORKSHEET

분석 범위·질문표

작성 목적: 분석 범위를 좁히고 필요한 모듈·자료를 정한다.

이 양식은 분석을 시작하기 전에 질문·관점·기준시점·자료 범위를 정하는 데 사용한다. 넓은 분야명을 쓰기보다 “누가 어떤 의무를 부담하는가”처럼 답할 수 있는 질문으로 적는다. 진행 중 범위를 바꾸면 최초 범위를 덮어쓰지 말고 변경 이유와 영향을 함께 남긴다.

사례 ID / 제목

분석 단위·관점 / 대상·관할·기준일·블록

이번에 답할 핵심 질문

모듈 선택	핵심 판단 질문
M1 규제·AML	
M2 회계·감사·보증	
M3 조세·과세정보 보고	
M4 거래구조화·가치평가	
M5 IT감사·기술 리스크	

범위 제외 / 종료 기준·미해결 시 처리

필요 자료 / 접근 제한 / 담당·기한

PART 4 · F-02 / WORKSHEET

증거·가정 목록

작성 목적: 관찰 사실 F, 추론 I, 가정 H를 분리한다.

확인한 자료와 분석을 위해 둔 가정을 나누어 적는다. 자료가 말하는 내용은 관찰로, 그 의미에 대한 설명은 추론으로 구분하고 출처·시점을 연결한다. 추가 자료로 가정이 확인되거나 기각되면 원래 기록을 보존하면서 상태와 후속 판단을 갱신한다.

사례 ID / 기준일 / 작성자 / 입력 명세 ID / FC ID

A. 증거 목록

ID	출처·주소·버전·원본 ID	확인 사실	한계·관련 질문

B. 가정 목록

H-ID	종류·내용	근거·목적	영향받는 판단

가정 종류: 사실 보완 / 스트레스 / 대안 구조 / 기술 실험. 미확인 사항을 관찰 사실로 표시하지 않는다.

추가 확보할 자료 / 결론 유보에 미치는 영향

PART 4 · F-02 / OPTIONAL ATTACHMENT

증거 연결표 · 작성 양식

기본 양식 6종은 유지한다. 이 표는 F-02의 선택 첨부표로 사용한다.

이 연결표는 같은 거래를 설명하는 온체인·오프체인 자료를 짝지어 확인하는 용도다. 단순히 두 자료를 확보했다는 표시보다 대상·금액·시점·주체가 맞는지 적는다. 연결을 확인하지 못했다면 부족한 자료와 결론에 미치는 영향을 함께 기록한다.

사례·판단 ID / FC·RF ID / 입력·변환 ID / 관점·기준일·블록

판단할 주장과 필요한 입증 요소

입증 요소	온체인 증거·ID	오프체인 증거·ID	연결·대사 / 상태

공통 식별자·주소·계정 / 기준시점·수량·금액 연결

발견한 차이 / 영향 / 관련 발견 ID

추론·가정 / 미확인 연결 / 필요한 추가 자료

다음 조치 / 담당 / 재검토 조건

온체인·오프체인·연결 상태를 구분하고, 각각 증거 충분성을 평가한다. 실제 사례·합성 자료·가상 실험을 서로 다른 근거로 표시한다.
사례 보완 · 기입 예시: USDC 81쪽 / 국내 합성 86쪽

PART 4 · F-03 / WORKSHEET

거래구조·귀속 분석도

작성 목적: 거래·권한·주체·현금흐름을 한 화면에 연결한다.

그림에는 주소·법인·고객 등 서로 다른 단위가 섞일 수 있으므로 노드의 의미를 먼저 정한다. 자산·현금·권리·권한의 화살표를 구분하고 중요한 연결에 증거 ID를 붙인다. 빈 연결이나 미확인 주체도 표시해 후속 자료 요청의 위치를 드러낸다.

사례 ID / FC ID / 기준 블록·문서 버전

거래·자산 이동	권한·승인·변경
실제 주체·권리·의무	현금흐름·부채·배분

핵심 연결 검토 · 거래·권리 첨부 참조

연결 관계	근거 ID	추론·가정	미확인 사항

가치 구분: 기초자산 / 투자자 청구권 / 토큰 시장가격

PART 4 · F-04 / WORKSHEET

전문 분야별 판단표

작성 목적: 사실과 적용 기준에서 결론까지 추적한다. 판단 1건당 1장을 사용한다.

각 전문 판단은 질문·적용 기준·근거·결론·한계를 한 줄로 추적할 수 있게 적는다. 모듈마다 다른 정의나 시점을 적용했다면 그 이유를 남겨 정당한 차이와 사실 모순을 구분한다. 비적용 항목에는 단순 공란 대신 비적용의 근거를 적는다.

판단 ID / FC·RF ID / 선택 모듈 / 관점·관할·시점

판단 질문 / M2: 규칙·정책·매핑 ID

확인 사실·귀속 추론 / 증거 ID

적용 기준·출처 / 권리관계 전제

판단·논거 / 대안 해석

사용 가정 / 한계 / 추가 조치

위험 유형·영향·가능성	해석 명확성	증거 등급

PART 4 · F-05 / WORKSHEET

불일치·추가 확인표

작성 목적: 오류와 정당한 기준 차이를 구분하고 재검토 경로를 정한다.

차이를 발견하면 먼저 무엇과 무엇이 다른지, 어떤 결론에 영향을 주는지 적는다. 자료 부족·처리 오류·범위 차이에 따라 담당자와 다음 행동을 달리 정한다. 조치를 완료한 뒤에는 새 근거와 판단 변경 여부를 남겨 차이의 발견과 해소 과정을 연결한다.

사례 ID / 관련 판단 ID / FC· RF ID / 상태·테스트 기록

대조 대상	확인 자료·버전	차이
문서 ↔ 코드		
장부 ↔ 온체인 거래		
온체인 ↔ 오프체인 자산		
분야별 전제·판단		

차이 유형 / 중요한 영향

사실·시점 / 구현 / 전제 / 정당한 기준 차이 / 미해결

추가 증거·추가 확인·재검토 / 담당·기한

되돌아갈 단계 / 재검토 결과

남은 차이 / 최종 결론에 미치는 영향

사례 보완 · 기입 예시: USDC 82쪽 / 국내 합성 87쪽

PART 4 · F-06 / WORKSHEET

결론 요약서

작성 목적: 발견 → 영향 → 판단 → 조치를 한 장으로 전달한다.

결론 요약서는 개별 발견을 의사결정자가 읽을 수 있는 형태로 모은다. 핵심 결과와 근거, 남은 조건, 추가 조치와 재검토 시점을 함께 제시한다. 등급은 설명을 대신하는 점수가 아니므로 중요한 판단에는 등급을 부여한 이유도 간단히 남긴다.

사례 ID / 제목 / 기준일 / 작성·검토

핵심 발견사항

발견 ID·내용	근거·영향	조치·담당

종합 판단 / 조건부·복수 해석·유보 대상

핵심 근거·기준 / 입력·변환·증거 ID / FC·RF ID / 사용 가정

위험 유형·영향·가능성	해석 명확성	증거 충분성

잔여 질문·필요 자료 / 다음 조치·담당·기한

재검토 조건 / 버전 이력 / 패턴·규칙·분개 초안 ID

사례 보완 · 결론 예시: USDC 83쪽 / 국내 합성 87쪽

PART 4 · PATTERN LIBRARY / 1 OF 2

레드플래그·검증 패턴

징후는 오류 판정이 아니라 확인할 질문이다. 정상 설명과 반증 조건을 함께 기록한다.

검증 패턴은 특정 결과를 미리 결론내리는 규칙이 아니라 반복해서 확인할 질문의 묶음이다. “잠금은 소각인가”처럼 혼동하기 쉬운 연결을 기억해 두면 다른 거래에서도 검토 지점을 빠르게 찾을 수 있다. 아래 패턴을 적용할 때는 사례의 계약·코드·상태가 같은 조건인지 다시 확인한다.

패턴에는 반례를 함께 두는 것이 중요하다. 예를 들어 특정 잠금 상태에서 의무가 남는지는 계약과 실제 처리에 따라 판단해야 하므로 “잠금이면 항상 같은 결론”이라는 규칙으로 만들지 않는다. 표의 검증 질문을 적용한 뒤 조건이 맞지 않으면 비적용 이유를 남기고, 새 조건은 별도 사례로 축적한다.

ID·징후	가능한 원인·정상 설명	확인할 증거·테스트	결과·조치
RF-01 · V-F01 잠금 ≠ 소각	예치·상환 대기·보호예수일 수 있음. 정상적으로 공급과 의무가 유지될 수 있음.	공급량·상태·이벤트 ↔ 요청·지급·권리 소멸 조건 대사.	상태 전이 확인. 조기 제거·중복 계상 여부 수정.
RF-02 · V-F03 업그레이드 ≠ 발행 통제	별도 minter 또는 정상적인 역할 분리. 오프체인 승인통제가 작동할 수도 있음.	권한 그래프·키·승인 모집단·실행 이력. 우회 경로 테스트.	권한별 통제와 실제 효과를 구분. 단일키·승인 공백 점검.
RF-03 · V-F02 비율의 범위 불일치	운영자금 혼입·대기 의무 제외·기준 시점 차이. 지표 정의 차이일 수도 있음.	분자·분모의 주체·자산·부채·단위·시점을 표로 고정.	정의 차이인지 오류인지 설명. 동일 범위 재계산.
RF-04 잔액 ≠ 권리·처분 가능성	수탁·담보·차입·공동관리 자산일 수 있음. 잔액은 맞아도 권리·제약이 다름.	지갑·은행·수탁 잔액 ↔ 명의·계약·담보·인출 제한 확인.	보유·통제·권리·유동성 결론을 분리.

패턴을 적용하는 순서

징후 발견 → 대안 설명 수립 → 필요한 증거 지정 → 테스트 → 결과·조치 → 라이브러리 갱신

RF-01~03은 DEMO-USD 가상 사례와 연결된다. 나머지 항목도 초기 검토 질문이며 실제 사례에서 검증된 독자적 발견이나 업계 빈도 통계로 제시하지 않는다.

> 현재 목록은 시드 라이브러리다. 반복 적용으로 확인된 패턴과 아직 검증하지 않은 후보를 구분해 축적한다.

PART 4 · PATTERN LIBRARY / 2 OF 2

패턴을 재사용 가능한 판단으로 축적

시드 항목의 정상 설명과 검증 절차를 보완하고 출처·사례 ID를 연결한다.

사례에서 발견한 문제를 재사용하려면 발생 조건과 적용 한계를 함께 남겨야 한다. 결과만 저장하면 다른 구조에 그대로 적용해 오판할 수 있다. 아래 기록 틀은 징후·확인 절차·필요 증거·반례를 함께 축적하여 패턴이 검토 경험에 따라 구체화되도록 한다.

좋은 패턴 기록은 다른 분석자가 무엇을 다시 확인해야 하는지 알 수 있게 한다. 필요한 자료가 비공개여서 확인하지 못했는지, 실제 반례를 발견했는지, 질문 자체를 바꿔야 하는지를 나누어 적는다. 사례 수가 늘어날수록 단순한 경고 목록보다 조건과 검증 경로가 풍부해지는 방향으로 관리한다.

ID·징후	가능한 원인·정상 설명	확인할 증거·테스트	결과·조치
RF-05 적격 주소 ≠ 최종 투자자	수탁·옴니버스 지갑 또는 자격 갱신 지연. 정상 수탁 구조일 수도 있음.	화이트리스트·이전기록 ↔ 고객·수익자 명부·자격 근거 대사.	주소와 사람을 자동 동일시하지 않고 역할별 귀속 기록.
RF-06 토큰 이전 ≠ 권리 이전	명부 갱신·승인·별도 절차를 요구하는 구조일 수 있음.	이전 로직·분배 ↔ 계약·명부·이전·집행 조건 검토.	이전 완료 조건과 오프체인 후속 절차를 설명.
RF-07 이벤트 ≠ 경제적 결과	수수료·래핑·내부 이전·실패 처리로 상태 변화와 다를 수 있음.	이벤트·실행 추적·잔액·순자산 변동 ↔ 원장·지급기록.	거래 실질·순액·중복·예외를 복원.
RF-08 NAV ≠ 시장가격 ≠ 환매금	평가주기·보수·스프레드·환매 시차·시장 수급의 정상 차이 가능.	평가기준·가격시각·수수료·유동성·환매조건 연결.	평가 대상·시점 구분. 괴리와 유동성 위험 설명.

패턴 1건의 고정 기록

항목	등록 내용
식별·상태	패턴 ID·관련 FC ID·명칭·사례 ID·관할·기준일 / 후보·가상 확인·실제 적용 확인·반례 확인
가설·검증	징후 / 오류 가능성 / 정상 설명 / 증거 / 테스트와 결과 / 적용 한계
축적·개선	영향·조치 / 반증 조건 / 재현 자료 / 검토자·버전 / 공개 범위

외부 공개 자료와 적법하게 확보한 비공개 자료를 구분한다. 신뢰성은 명칭이나 비공개 여부보다 실제 적용 근거·반례·재현성으로 축적한다.

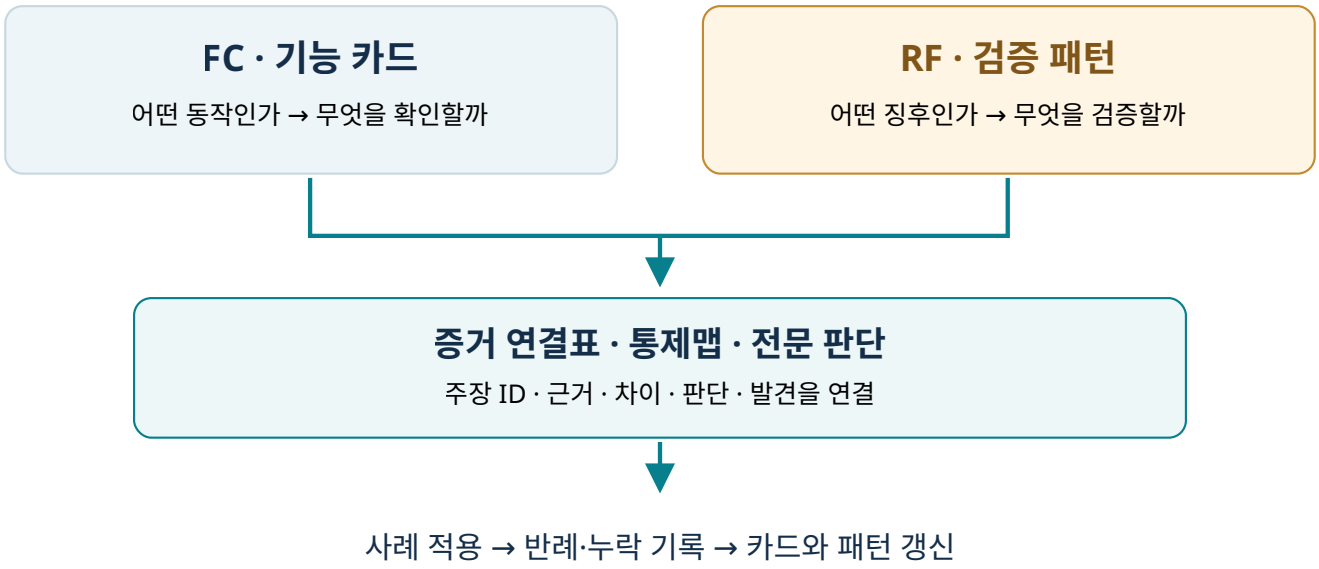
FC 연결 · RF-02 ↔ FC-A01·FC-C02·FC-E01 / RF-03 ↔ FC-A01 / RF-04·05 ↔ FC-D02 / RF-06 ↔ FC-C02·FC-D02·FC-E01.

PART 4 · FUNCTION CARDS / 01 / OVERVIEW

기능을 만나면, 확인할 질문을 꺼낸다

FC는 동작에서, RF는 문제 징후에서 출발한다. 둘 다 증거 연결표와 전문 판단으로 이어진다.

기능 카드와 검증 패턴은 서로 다른 출발점에서 같은 증거 구조로 들어온다. 기능 카드는 발견한 동작에서 확인 질문을 만들고, 패턴은 의심스러운 연결에서 검증 순서를 만든다. 아래 그림처럼 두 도구를 통제맵·증거 연결·전문 판단에 함께 사용하되 카드 적용 자체를 결론으로 취급하지 않는다.



구분	운영 방식
분류와 분량	현재 4개 기능 카드와 FC-X01의 시드 본문을 제공한다. 전체 32항목의 확장 범위는 다음 로드맵에 정리했다.
기본·조합	A~G는 기본 기능 관점, H는 조합 메커니즘이다. 기본 카드도 교차 컨트랙트·외부 의존이 있으면 하위 카드로 분해한다.
식별 원칙	함수명·이벤트·표준 표기는 후보 신호다. 배포 코드·상태 변화·실행 경로로 동작과 적용 범위를 확인한다.
목적과 한계	점검 질문을 정형화한다. 체크 완료가 적법성·회계 결론·보안성·통제 효과성의 인증은 아니다.

> 예: “mint 함수가 있는가?”보다 “어떤 경로가 공급량을 늘리며, 누가 그 경로를 실행·변경할 수 있는가?”를 묻는다. 이벤트 하나만으로 발행이나 권리 성립을 확정하지 않는다.

PART 4 · FUNCTION CARDS / ROADMAP

지금 사용할 카드와 다음 확장

본문에는 4개 기능 카드의 시드 본문과 FC-X01을 제공한다. 확장 목록은 적용 사례에 맞춰 채운다.

현재 사용할 수 있는 시드 카드와 앞으로 확장할 범위를 구분한다. 분류표가 넓다는 이유로 모든 기능을 분석할 준비가 끝났다는 뜻은 아니다. 먼저 네 개 카드와 미분류 절차를 실제 사례에 적용하고, 반복되는 질문·누락·반례를 근거로 다음 카드를 작성한다.

자료 · 참고 코드·표준 | 카드 · 시드 | 범위 · 질문 명세

현재 본문	확인 질문
FC-A01 · 발행	공급 증가 경로·한도·주체·대가를 연결
FC-C02 · 역할	행위 권한·역할 관리자·실제 주체를 연결
FC-E01 · 업그레이드	실행 구현·변경 권한·영향받는 판단 확인
FC-D02 · 동결	차단 범위·근거·예외·해제 연결
FC-X01 · 미분류	상태 변화에서 출발해 경로·통제·실질·반례 복원

확장 분류: 전체 32항목의 지도

영역·고정 ID	주요 확장 범위
A 공급 · A01~04	소각·공급 상한·리베이스
B 이전 · B01~05	이전·승인·permit · 적격성·수수료·락업
C 권한 · C01~06	소유자·멀티시그·타임락·거버넌스·이양
D 개입 · D01~04	중지·강제 이전·회수·긴급 출금
E 변경 · E01~03	파라미터·모듈·플러그인
F 가치·상환 · F01~04	볼트·래핑·상환 대기열·분배
G 외부 의존 · G01~03	오라클·브리지 메시지·외부 호출
H 조합 · H01~03	AMM · 담보 대출/청산·스테이킹/보상

기본 경로 보강 후 복합 적용 우선순위: H02 대출·청산 → H01 AMM · 유동성 → G02 브리지. 세부 전제·완료 조건은 58쪽. F03 · F01 · B03 · F04는 RWA · 스테이블코인 사례에 맞춰 병행. 기본 기능 A~G도 교차 컨트랙트이면 분해한다. H는 관련 기본 카드와 프로토콜별 순서·실패 조건을 묶는다.

PART 4 · FUNCTION CARDS / 04 / TEMPLATE

카드 한 장의 고정 양식

정적 정의와 사례별 적용 기록을 분리한다. 카드 자체를 사실 또는 결론으로 취급하지 않는다.

고정 양식은 기능 이름을 수집하기보다 동작·권한·증거·연결 검증을 같은 순서로 보게 만든다. 같은 기능도 배포 버전이나 외부 모듈에 따라 경로가 달라질 수 있다. 카드의 탐지 상태와 성숙도, 사례의 수행 범위를 따로 기록하면 “발견했다”와 “검증했다”의 차이를 유지할 수 있다.

자료 · 참고 코드·표준 | 카드 · 시드 | 범위 · 질문 명세

고정 필드	기록 내용
식별·범위	card_id · 명칭·분류·버전·작성자·근거 문서·지원 체인/표준·검토일
동작 정의	변경 전후의 상태·자산·권한. 총공급량·잔액·지분 등 무엇을 보는지 명시
식별 신호·변형	함수·이벤트·역할·슬롯 등 후보, 다른 이름·위임·우회·외부 호출 경로
통제맵	실행자·관리자·조건·한도·기간·변경권·실행 이력과 실제 주체 연결
증거 연결	온체인 증거 / 오프체인 증거 / 연결 키·시점·대사식 / 미확인 사항
판단·연결	관련 M1~M5 질문, RF ID · 관련 FC ID · 증거·판단·발견 ID
적용 인스턴스	application_id · case_id · card_version · 주소·블록·구현 버전 · assertion_id · 검토자
탐지·확인 상태	후보 / 동작 확인 / 미확인 / 비적용. 근거·한계와 상태 변경 이유
축적 이력	시드 → 검토·개정. 가상·테스트·실제 적용은 별도 이력과 사례 범위로 기록

상태는 세 가지를 분리한다

구분	예시
카드 성숙도	시드 / 검토·개정. 출처와 반례를 반영해 갱신한다.
적용 환경	가상 시연 / 테스트 실행 / 실제 사례 적용. 각 환경의 수행 여부를 기록한다.
사례별 결론	기능 확인 범위·근거 충분성·전문 판단을 각각 남긴다.

> 카드의 성숙도·적용 환경·사례별 결론을 각각 기록한다. 적용 사례와 반례를 모아 지원 범위를 개선한다.

PART 4 · FUNCTION CARDS / 05 / FC-A01

FC-A01 · 발행

질문: 총공급량을 늘리는 경로는 무엇이며 누가 실행·변경할 수 있는가?

발행을 확인할 때는 함수 이름보다 공급과 잔액이 늘어나는 경로를 찾는다. 발행량과 입금액이 같아도 같은 고객·시점·거래인지 따로 대사해야 한다. 아래 카드는 기술적 공급 변화에서 승인·대가·의무의 검토로 넘어갈 때 확인할 항목을 정리한다.

자료 · 참고 코드·표준 | 카드 · 시드 | 범위 · 질문 명세

고정 항목	확인할 내용
동작 정의	대상 토큰의 공급량 증가 경로. 리베이스·래핑·브리지·일시 발행을 구분하고 순증과 기간 중 총발행을 나눈다.
식별 신호	mint · _mint 호출, 발행형 Transfer(0 주소 발신), totalSupply 전후 차이는 후보. 로그 기록 F와 실제 발행 확인을 구분한다.
변형·우회	생성자 발행, 다른 함수의 내부 발행, 위임·외부 모듈·구현체 교체, 인덱스 조정. 한 블록 내 발행·소각 상계도 확인. 건별 대사와 공급량의 기간 대사를 병행.
통제맵	호출자·역할 관리자·상한·조건·수취인·변경권·이력. 역할명·해시를 정해진 상수로 가정하지 않는다.
온체인 증거	배포 코드·실행 경로·역할 상태·이벤트·공급 및 잔액 변동·트랜잭션 상태. 기준 블록과 구현 버전을 고정.
오프체인 증거	발행 승인·고객 주문·입금·키 관리·원장. 은행 입금과 발행이 항상 동시라는 전제를 두지 않는다.
연결 검증	발행량 ↔ 주문·입금·고객 원장. 거래 ID · 단위·기준시점을 맞추고 선·후입금, 수수료, 취소·미결을 조정.

전문 판단에 연결할 질문

모듈	질문
M2 · M4	토큰 발행이 어떤 의무·투자자 권리를 발생시키는가? 인식·평가의 기준 사건은 무엇인가?
M1 · M5	실제 운영 주체·행위는 무엇인가? 발행 승인 우회·단일 키·상한 변경 경로가 있는가?

연결 · RF-02 · RF-03 · RF-07 / FC-C02 · FC-E01 · FC-A02 · FC-A03
공식 참고 · FC-S1 · FC-S2. 적용 버전·구현은 사례별 재확인.

> 기록: application_id / card_version / case_id / 체인·주소·블록 / 주장·증거 ID / F · I · H / 후보·동작 확인·미확인·비적용 / 차이·한계·검토자

PART 4 · FUNCTION CARDS / FC-A01 / FIELD NOTES

발행을 건별·기간 합계로 확인한다

FC-A01 상세 · 이벤트 관찰, 실제 상태 변화, 경제적 판단을 분리한다.

이벤트 관찰, 실제 상태 변화 확인, 경제적 의미 판단은 서로 다른 작업이다. 로그만 집계하면 같은 사건을 중복 계산하거나 공급 변화의 다른 경로를 놓칠 수 있다. 아래 건별·기간별 대사를 함께 사용해 모집단과 기준시점을 맞추고, 차이가 나면 범위·처리 시점부터 확인한다.

동작 정의와 관찰의 범위

일반적인 ERC-20 발행은 대상 토큰에서 다른 보유자 잔액을 차감하지 않고 수령자 잔액과 공급을 늘리는 경로다. 원자산 입금·타 체인 잠금이 없다는 뜻은 아니다. 리베이스·래핑·브리지는 해당 카드와 함께 분석한다.

구분	기록할 주장
이벤트 관찰 F	해당 컨트랙트의 성공 거래에 0 주소 발신 Transfer 로그가 기록됐다. 체인·블록·거래·로그 위치·수량을 남긴다.
기술적 동작 확인	배포 코드·호출 경로와 공급·잔액 변화를 확인한다. 한 거래의 발행·소각 상계, 리베이스·외부 호출을 분리한다.
전문 판단	승인·대가·고객 원장·약정에 연결해 발행 주체, 권리·의무·귀속을 검토한다. 로그 자체에서 자동 도출하지 않는다.

두 수준의 대사

수준	실행할 검토
발행 건별	발행 ↔ 주문·승인 ↔ 입금 ↔ 고객 원장. 거래 ID·단위·금액·시점을 연결하고 선입금·후입금·수수료·취소·미결을 설명한다.
기간 전체	기말 공급량 − 기초 공급량 = 기간 발행량 − 기간 소각량 + 기타 공급 조정. 같은 단위·범위·기간으로 집계하고 조정의 중복 반영을 막는다.
조건부 단순식	기타 공급 조정이 없고 발행·소각 모집단이 완전한 범위에서만 “발행 − 소각 = 공급량 변동”을 적용한다.

변형·우회 경로에서 추가할 질문

issue·deposit·bridgeIn 같은 이름, 생성자·내부 호출·발행 관리자·업그레이드로 추가된 경로를 확인한다. 발행자별 한도가 있으면 상위 한도 변경 권한도 추적한다. 발행 실행 주소가 실제 승인된 키·서명자와 연결되는지 확인한다.

M3 추가 질문: 유상 교환·무상 배정·보상 등 거래 조건은 무엇이며, 누구의 어떤 경제적 이익인가? 이름만으로 소득 성격을 정하지 않는다. 공식 참고: FC-S1 · FC-S2.

> ERC-20의 발행형 이벤트는 탐색 단서다. 이벤트 기록의 사실과 실제 발행의 확인 범위를 별도로 남긴다. 기간 총발행량은 두 시점의 공급량 차이만으로 산출하지 않는다.

PART 4 · FUNCTION CARDS / 06 / FC-C02

FC-C02 · 역할 기반 접근

질문: 누가 행위를 실행하고, 누가 그 사람의 권한을 바꿀 수 있는가?

역할은 특정 동작을 실행할 수 있는 기술적 조건이다. 실제 권한 구조를 이해하려면 그 역할을 부여·회수할 수 있는 관리자와 상위 실행 경로도 따라가야 한다. 아래 카드는 표준 역할 이름이 없는 자체 구현까지 포함해 권한의 관리 구조와 실제 주체의 연결을 묻는다.

자료 · 참고 코드·표준 | 카드 · 시드 | 범위 · 질문 명세

고정 항목	확인할 내용
동작 정의	역할에 따라 실행을 허용·차단하고 역할 보유자·관리자를 변경하는 경로. 행위 권한과 역할 관리 권한을 분리한다.
식별 신호	hasRole · getRoleAdmin · grantRole · revokeRole, RoleGranted · RoleRevoked 등은 구현에 따른 후보 신호다.
변형·우회	외부 권한 관리자, owner 경로, 사용자 정의 modifier, 업그레이드·모듈 호출. 역할 이름이 같아도 권한은 다를 수 있다.
통제맵	행위 → 검사 로직 → 역할 ID → 보유 주소 → 관리자 역할 → 변경·회수·지연 경로를 그린다. 순환·자기관리도 기록.
온체인 증거	기준 블록의 권한 상태와 전체 가용 변경 이력, 구현 코드. 보유자 열거가 불가하면 로그 범위와 복원 한계를 명시.
오프체인 증거	이사회 의사록·위임장·키 관리 정책·멀티시그 서명자 명부·인사·승인·회수 기록. 진정성·효력 기간과 실제 운영 대조(11·50쪽).
연결 검증	역할 주소 ↔ 문서상 담당자 ↔ 실제 운영·승인·실행 기록. 명부와 실소유자, 서명과 경제적 통제를 분리. 부여·회수 시점과 잔존 권한 대사.

전문 판단에 연결할 질문

모듈	질문
M5	최소 권한·직무분리·변경관리·승인 독립성이 설계되고 실제로 작동하는가?
M1 · M2	운영 책임자·수탁 관계와 권한이 일치하는가? 기술 권한을 규제상 지위·회계상 지배로 단정하지 않았는가?

연결 · RF-02 · RF-06 / FC-A01 · FC-C01 · FC-C03 · FC-E01
공식 참고 · FC-S3. 적용 버전·구현은 사례별 재확인.

> 기록: application_id / card_version / case_id / 체인·주소·블록 / 주장·증거 ID / F · I · H / 후보·동작 확인·미확인·비적용 / 차이·한계·검토자

PART 4 · FUNCTION CARDS / FC-C02 / FIELD NOTES

기술 권한에서 실제 주체로 연결한다

FC-C02 상세 · 공개 식별 → 문서상 권한 → 실제 운영 → 기준별 판단.

역할 보유자 목록을 실제 주체의 입증 자료로 바꾸려면 권한의 관리 경로와 운영 기록을 연결해야 한다. 11쪽의 공통 귀속 절차를 아래 체크리스트로 구체화한다. 확보한 문서가 많아도 판단하려는 관계를 뒷받침하지 못하면 추가 자료가 필요하다.

먼저 기술 권한의 경로를 복원한다

추적 대상	질문
행위 → 역할 → 관리자	어떤 경로가 어떤 역할을 검사하는가? owner·자체 modifier·외부 관리자·멀티시그·타임락·모듈·업그레이드 우회와 자기관리·순환을 추적.
부여·회수·이양	요청·승인·시행 시점 ↔ 체인 변경 ↔ 실행 거래를 연결. 퇴직자·구 키·다른 관리자 역할·업그레이드 권한이 남는지 확인.

주체 귀속 증거 체크리스트 · 관계별로 반복

확인	기록·대사
☐ 공개 식별	공식 주소·법인 공시·문서 ↔ 대상 주소. 라벨·OSINT의 원출처·확인일·계보를 보존하고 후보와 확정을 구분.
☐ 문서상 권한	이사회 의사록·위임장의 승인 주체·위임 범위·유효기간·재위임·철회 기록. 문서 진정성 확인 범위와 사본·누락 표시.
☐ 키·서명 운영	키 관리 정책·멀티시그 서명자 명부·변경 이력 ↔ 역할·관리자 주소·임계값·복구/모듈 경로. 실명·직책·외주·수탁·공동 권한 연결.
☐ 실제 행사	승인 기록·서명/키 운영 로그·역할 변경·실행 거래를 같은 사건·기간으로 대조. 명부·정책과 다른 운영, 미회수·긴급 권한 확인.
☐ 반증·판단	다른 설명·상충 자료·부족 범위를 기록. 기술 실행·법적 위임·의사결정·회계상 통제·세무 귀속을 각 기준으로 별도 평가.

목록의 완전성과 결론의 범위를 따로 기록한다

열거 기능이 없으면 가용 로그에서 후보를 복원하고 기준 블록의 상태와 대조한다. 초기 설정·시작 블록·누락·자체 변경 경로를 확인하지 못하면 전체 보유자 목록으로 단정하지 않는다. 역할 주소와 정책상 직책을 일대일로 가정하지 않고 위임·외주·수탁 관계를 복원한다.

기록: 주장·대상 관계 / 증거 ID·출처·판본·기간·진정성 / 문서↔주소↔실행 연결 / 충돌·반증·누락 / F·I·H / 적용 기준·검토자. 자료 공백은 F-05에 요청과 재검토 조건으로 남긴다.
공식 참고: FC-S3(기술 역할); 위 문서 체크리스트는 OCP의 분석 설계다.

> 서명자 명부는 실소유자 명부가 아니다. 서명 가능성은 법적 권리·경제적 통제의 충분조건이 아니다. 여러 주소·여러 서명자의 독립성도 실제 주체·운영 자료로 확인한다. 카드 상태는 시드, 내부 문서의 실제 확보를 의미하지 않는다.

PART 4 · FUNCTION CARDS / 07 / FC-E01

FC-E01 · 프록시 업그레이드

질문: 어떤 코드로 실행되며, 누가 어떤 경로로 그 코드를 교체하는가?

업그레이드 검토는 구현 주소를 찾는 일과 그 주소를 바꾸는 권한을 확인하는 일을 함께 수행한다. 운영 역할이 분리되어 있어도 코드 교체가 그 제한을 바꿀 수 있는지 살펴야 한다. 아래 통제맵은 코드 변경과 일상 운영을 다른 평면으로 보면서 두 경로가 만나는 지점도 확인한다.

자료 · 참고 코드·표준 | 카드 · 시드 | 범위 · 질문 명세

고정 항목	확인할 내용
동작 정의	프록시 등의 실행 대상 구현체를 바꾸는 경로. 프록시 존재와 변경 가능성을 별도로 확인한다.
식별 신호	실제 위임 호출·구현 코드·변경 경로를 우선 추적한다. ERC-1967 및 ZeppelinOS 계열 레거시 슬롯, Upgraded 등 이벤트는 탐색 단서다. 표준 슬롯이 0이면 다른 슬롯 계열·비콘·자체 구조를 확인한다.
변형·우회	Transparent · UUPS · Beacon · ZeppelinOS 레거시·자체 구조. 관리자만 조회 함수를 쓸 수 있는 프록시는 일반 호출이 되돌려질 수 있다. 호출자 조건·위임 분기·별도 관리자·모듈을 추적한다.
통제맵	실제 교체 실행자·권한 검사·다중서명·지연·취소·초기화·다른 우회 경로. UUPS는 구현체의 승인 경로도 확인. 프록시 관리자(코드 교체)와 owner · 역할(운영 권한)은 서로 다른 통제 평면이다.
온체인 증거	기준 블록별 구현 주소·코드 해시·슬롯·변경 거래·호출 추적. 과거 상태 조회 불가와 이벤트 누락 범위를 기록.
오프체인 증거	변경 요청·검토·테스트·배포 승인·키 운영·사용자 고지·계약상 변경 근거. 코드 변경과 약정 변경을 구분.
연결 검증	승인 버전 ↔ 배포 코드 해시 ↔ 변경 거래·시점 ↔ 원장·사용자 영향. 전체 카드의 영향 여부를 점검하고 영향받는 판단을 재수행.

전문 판단에 연결할 질문

모듈	질문
M5	승인·테스트·지연·접근 통제가 실제 교체 경로 전체에 적용되는가?
M1 · M2 · M4	변경이 투자자 권리·현금흐름·회계 전제·서비스 의무에 영향을 주는가? 별도 문서 검토가 필요한가?

적용 이력 · R-USDC-01에서 질문 보완: ERC-1967 밖의 슬롯과 조회 함수의 호출자 조건을 추가. 카드 상태는 시드 유지. 되돌림 원인·배포 버전은 검증 전.
연결 · RF-02 · RF-06 / FC-C02 · FC-C03 · FC-C04 · FC-E03
공식 참고 · FC-S4 · FC-S5. 적용 버전·구현은 사례별 재확인.

> 기록: application_id / card_version / case_id / 체인·주소·블록 / 주장·증거 ID / F · I · H / 후보·동작 확인·미확인·비적용 / 차이·한계·검토자

PART 4 · FUNCTION CARDS / FC-E01 / FIELD NOTES

레거시 슬롯과 호출자 조건까지 추적한다

FC-E01 상세 · ERC-1967과 공식 참고 코드의 ZeppelinOS 슬롯. 확인일: 2026년 11월 14일.

슬롯과 조회 함수는 프록시를 탐색하는 단서이며 배포 구조에 따라 다를 수 있다. 아래에서는 ERC-1967과 ZeppelinOS 레거시를 나란히 비교한다. 일반 조회가 되돌려지면 호출자 조건을 검토하되, USDC의 수정 전 버전 가설이 확인됐다는 뜻으로 읽지 않는다.

슬롯 계열·대상	저장 슬롯 · 참고 이벤트
ERC-1967 구현 주소	`0x360894a13ba1a3210667c828492db98dca3e2076cc3735a920a3ca505d382bbc` Upgraded(address indexed implementation)
ERC-1967 관리자 주소	`0xb53127684a568b3173ae13b9f8a6016e243e63b6e8ee1178d6a717850b5d6103` AdminChanged(address previousAdmin, address newAdmin)
ERC-1967 비컨 주소	`0xa3f0ad74e5423aebfd80d3ef4346578335a9a72aeaee59ff6cb3582b35133d50` BeaconUpgraded(address indexed beacon)
ZeppelinOS 레거시 구현	`0x7050c9e0f4ca769c69bd3a8ef740bc37934f8e2c036e5a723fd8ee048ed3f8c3` `keccak256("org.zeppelinos.proxy.implementation")`
ZeppelinOS 레거시 관리자	`0x10d6a54a4754c8869d6886b5f5d7fbfa5b4522237ea5c60d11bc4e7a1ff9390b` `keccak256("org.zeppelinos.proxy.admin")`

ERC-1967은 해시에서 1을 뺀 슬롯, 위 ZeppelinOS 레거시는 문자열 해시 자체다. 표준 슬롯이 0이면 다른 계열을 확인한다. 슬롯·이벤트만으로 유형·변경 권한·이력의 완전성을 확정하지 않는다. ERC-1967의 이벤트 권고와 실제 구현도 구분한다.

구조에 따라 추가로 추적한다

구조	확인 경로
Transparent	관리자·관리 계약과 실제 승인 주체를 확인한다. 배포 버전에 따라 실제 권한 처리 방식과 저장 슬롯의 관계를 검토한다.
UUPS	구현체의 업그레이드 승인 로직·권한·실행 경로를 확인한다. 관리자 슬롯이 비었다고 변경 불가능으로 판정하지 않는다.
Beacon	비컨 주소 → implementation()의 대상 → 비컨 변경 권한을 추적한다. 영향받는 여러 프록시의 범위를 확인한다.
레거시·자체·모듈	다른 슬롯·위임·외부 모듈 교체를 확인한다. 관리자 제한 조회는 일반 호출과 관리자 from 읽기를 비교한다. 프록시 존재와 변경 가능성을 구분.

승인·공지·코드의 세 연결

승인 코드·버전 ↔ 배포·변경 거래 ↔ 공지·약정을 대조한다. 초기화·저장 구조·권한·경제 조건의 차이와 전체 카드의 영향을 확인한다.

> 영향받는 카드·전문 판단을 재수행하고 영향이 없다는 판단도 근거를 남긴다. 과거 분석은 보존하고 현재 적용성은 별도 검토한다. R-USDC-01의 조회 가설·확인 계획은 22쪽 참조.

근거 · FC-S5: ERC-1967 / Circle 고정 커밋의 UpgradeabilityProxy·AdminUpgradeabilityProxy. 참고 코드와 배포 동일성은 별도 검증.

PART 4 · FUNCTION CARDS / 08 / FC-D02

FC-D02 · 동결·블랙리스트

질문: 누구의 어떤 행위를 제한하며, 어떤 경로에는 제한이 적용되지 않는가?

동결은 사용을 제한하는 기술적 효과와 그 제한의 근거를 나누어 검토한다. 어떤 경로가 막히는지뿐 아니라 해제·예외·강제 이전과 연결되는지도 확인한다. 아래 카드는 기능의 존재를 규제상 적정성이나 보유자 권리의 소멸로 자동 해석하지 않도록 구성되어 있다.

자료 · 참고 코드·표준 | 카드 · 시드 | 범위 · 질문 명세

고정 항목	확인할 내용
동작 정의	주소·잔액·거래 경로에 제한을 설정·해제한다. 토큰 이동 제한과 법적 권리 박탈·소각을 구분한다.
식별 신호	동결 상태·제한 목록·사용자 정의 이벤트·이전 조건 검사. 모든 토큰에 공통인 함수·이벤트가 있다고 가정하지 않는다.
변형·우회	송신·수신·수량별 제한, transferFrom · 발행·소각·강제이전 예외, 외부 적격성 모듈. 중지 기능과도 범위 비교.
통제맵	설정·해제자·관리자·대상·기간·사유·조건·우회 권한. 외부 모듈 교체가 제한 효과를 바꾸는지 확인.
온체인 증거	대상 상태·검사 경로·권한·변경 이력. 각 거래 경로의 실제 실행·실패를 분리. 테스트 결과는 테스트 환경으로 한정.
오프체인 증거	제한 사유·승인·고지·이의 절차·고객 상태·상환 약정. 특정 제재·규제 요건 충족은 별도 기준으로 검토.
연결 검증	제한된 주소 ↔ 고객·적격성 기록 ↔ 제한 결정 ↔ 차단 범위·해제·상환 처리. 옴니버스 지갑의 영향도 구분.

전문 판단에 연결할 질문

모듈	질문
M1 · M5	고객·규제 요구와 차단 범위가 맞는가? 승인·해제·예외 관리가 작동하는가?
M2 · M4	제한이 처분 가능성·유동성·평가에 주는 영향은 무엇인가? 상환권·소유권 소멸로 확대 해석하지 않았는가?

연결 · RF-04 · RF-05 · RF-06 / FC-B03 · FC-D01 · FC-D03 · FC-C02
공식 참고 · FC-S6. ERC-3643은 한 구현 범위의 참고이며 보편 동작의 근거가 아니다. 적용 버전·구현은 사례별 재확인.

> 기록: application_id / card_version / case_id / 체인·주소·블록 / 주장·증거 ID / F · I · H / 후보·동작 확인·미확인·비적용 / 차이·한계·검토자

PART 4 · FUNCTION CARDS / FC-D02 / FIELD NOTES

동결의 근거와 효과를 연결한다

FC-D02 상세 · 동결은 기술 동작과 의사결정의 근거를 함께 검토한다.

한 주소의 동결이 고객 한 명의 거래만 제한한다고 단정할 수는 없다. 수탁·옴니버스 구조에서는 주소와 고객 원장의 연결을 복원해야 영향을 파악할 수 있다. 아래 기록은 기술적 차단, 승인 근거, 고객 대응을 나누고 동결 뒤에도 남는 권리·의무의 검토로 이어진다.

제한 범위를 먼저 나눈다

기술 범위	확인할 질문
대상·행위	송신·수신·일부 잔액·주소 전체 중 무엇을 막는가? transferFrom · 발행·소각·강제이전에도 적용되는가?
연결 기능	전체 중지·적격성 모듈·화이트리스트가 별도로 작동하는가? 동결 이후 회수·소각은 별도 권한·동작으로 분석했는가?
조회·모집단	동결 주소를 열거할 수 있는가? 이벤트로 복원했다면 기간·초기 설정·누락 범위와 기준 블록 상태를 대조했는가?

근거·승인·고객·상태의 연결

오프체인 기록	연결 검증
결정의 근거	약관·내부 정책·명령·요청 등 제시된 근거의 주체·대상·범위·시점을 확인한다. 요청이 존재한다는 사실과 적법성 판단은 구분한다.
승인·실행	승인자·키·동결 이벤트·대상 주소를 연결한다. 문서상 범위보다 넓거나 좁은 제한, 실행 지연을 확인한다.
고객·권리	주소와 고객 원장·수탁 관계를 연결한다. 옴니버스 지갑에서는 다른 고객에게 미친 영향도 구분한다.
통지·해제	고객 통지·이의 처리·해제 기준·승인·실제 해제 상태를 연결한다. 내부 정책이 있다는 것과 실제 이행을 구분한다.

전문 판단의 경계

M1은 해당 관할의 근거와 사업자 의무를 별도로 검토한다. M2 · M4는 발행자의 의무 지속, 보유자의 처분 가능성과 평가 영향을 질문한다. M3는 제한 중에도 보상·분배가 발생하는지, 권리 발생·청구·수령 시점이 어떻게 달라지는지 확인한 뒤 적용 기준을 검토한다.

공식 참고: FC-S6. ERC-3643의 동결·부분 동결·강제이전은 구분해서 확인한다. 일반 ERC-20 전체에 동일한 기능·이벤트·법적 효과가 있다고 가정하지 않는다.

> 동결 자체가 소각·채무 소멸·소유권 박탈·과세 시점 변경을 뜻하지 않는다. 온체인 제한 상태와 오프체인 권리·의무는 추가 증거로 연결한다.

PART 4 · FUNCTION CARDS / 09 / FC-X01

FC-X01 · 미분류 동작

어떤 카드에도 맞지 않으면, 익숙한 이름에 끼워 맞추지 않고 상태 변화에서 다시 시작한다.

분류표에 없는 동작을 만났을 때는 익숙한 카드에 억지로 맞추기보다 상태 변화에서 다시 출발한다. 무엇이 바뀌고 누가 바꿀 수 있으며 어떤 기록과 연결해야 하는지를 순서대로 묻는다. 기존 카드와 닮은 점과 다른 점을 남기면 이후 사례에서 새 카드가 필요한지 판단할 수 있다.

미분류 상태를 남기는 것은 실패가 아니라 범위를 정직하게 표시하는 방식이다. 카드와 다른 동작을 만났을 때 가장 가까운 카드의 확인 항목을 참고하되 결론을 그대로 가져오지 않는다. 비슷한 동작이 반복되면 공통 조건과 예외를 정리해 새 카드 초안의 근거로 사용한다.

자료 · 참고 코드·표준 | 카드 · 시드 | 범위 · 질문 명세

순서	확인 질문·남길 기록
1 · 변화 관찰	어떤 상태·잔액·공급·지분·권한·외부 자산이 언제 변했는가? 실패·되돌림·로그만 남은 것과 구분한다.
2 · 경로 복원	어떤 호출·내부 호출·위임·외부 의존이 변화를 만들었는가? 체인·블록·코드·입력·출력을 고정한다.
3 · 통제 연결	누가 시작·변경·중단·우회할 수 있는가? 주소의 실제 주체와 권한 근거는 어디까지 확인되는가?
4 · 실질 연결	계약·고객 원장·자금·권리·의무에서 무엇과 대사해야 하는가? 연결 키와 시점은 무엇인가?
5 · 대안·반례	같은 관찰을 설명하는 다른 원인은 무엇인가? 어떤 추가 증거가 현재 설명을 반증할 수 있는가?
6 · 임시 기록	application_id와 X01을 붙이고 사실·추론·가정, 미확인 사항, 추가 요청과 재검토 조건을 기록한다.
7 · 분류 결정	기존 카드 변형 / 여러 카드의 조합 / 새 카드 후보 중 하나로 정리한다. 반복은 후보 신호로 사용하고 반례·경계·기존 카드 중복·검토 이력을 첨부한다.

새 카드로 승격할 때

명칭보다 반복되는 상태 변화와 통제·검증 질문을 정의한다. 임시 후보 ID를 사용하고 검토 후 고정 ID를 부여한다. 기존 ID를 다른 기능에 재사용하지 않는다. 사례 한 건의 특수 조건을 보편 규칙으로 확대하지 않는다.

> 소스·실행 추적이 부족하면 “동작 미확인”으로 남긴다. 미분류는 오류·취약성이라는 뜻이 아니며, 자동 탐지가 실패했다는 사실만으로 기능이 없다고 결론 내리지 않는다.

PART 4 · FUNCTION CARDS / OPERATING RULES

카드를 확장하고 재검토하는 기준

FC-X01은 미분류 절차의 고정 ID다. 이름이 아니라 동작에서 출발한다.

카드는 작성한 뒤 고정하는 문서가 아니라 적용 결과로 다듬는 질문 도구다. 사례에서 유용했던 항목뿐 아니라 작동하지 않았던 신호와 반례도 기록한다. 아래 운영 기준은 카드의 질문 개선, 탐지 결과의 확인, 전문 판단의 책임을 서로 구분하면서 축적하기 위한 것이다.

보완 원칙	실행 방법
변형·우회 경로를 필수화	다른 이름·내부 호출·별도 권한·외부 모듈·예외·실패 경로를 확인한다. “없음”과 “미확인”을 구분하고 확인 범위를 남긴다.
RF·FC의 사용 단계	FC는 Step 2~3·5를 중심으로 Step 4 판단과 Step 6 보고까지 연결한다. RF도 특정 단계에 제한하지 않고 징후가 나타난 시점에 사용한다.
자동화 경계	식별 신호는 후보 탐지, 연결 검증은 대사 지원, 판단 질문은 검토 목록으로 구현한다. 동작·귀속·전문 결론을 자동 확정하지 않는다.
표준값·버전 관리	표준 출처·확인일과 적용 라이브러리 릴리스·코드 해시를 구분한다. 슬롯·역할·이벤트가 달라지는 변형을 규칙의 지원 범위에 반영한다.

변경 후 전체 영향 점검 → 필요한 재수행

순서	남길 기록
1 · 변경 포착	기준 블록·이전/이후 구현·코드 해시·변경 거래·승인·문서 차이.
2 · 전체 카드 영향 점검	기능·권한·외부 의존·파라미터·권리·현금흐름 전제에 변화가 있는지 확인. 적용 카드별 영향 / 무영향 / 미확인과 근거 기록.
3 · 재분석 범위 결정	영향받는 카드·RF·전문 판단을 재수행하고, 미확인 범위는 자료 요청·한계·유보로 처리.
4 · 과거·현재 구분	과거 결론을 덮어쓰지 않고 당시 기준일·버전과 함께 보존. 현재 결론과 차이·재검토 근거 연결.

두 사례 반복은 새 카드의 후보 신호다

같은 동작이 두 사례 이상에서 반복되면 초안 작성을 검토할 수 있다. 자동 승격 조건은 아니다. 기존 카드의 변형·조합인지, 별도 카드가 필요한지 검토하고 동작 경계·출처·반례·테스트·검토 이력을 갖춰 고정 ID를 부여한다.

> 장래 전자책의 “어제의 분석이 오늘은 틀릴 수 있다” 사례는 FC-E01의 영향 점검과 연결한다. 미분류 기록은 FC-X01을 사용하고 기존 ID를 재사용하지 않는다.

PART 4 · FUNCTION CARDS / 10 / APPLICATION

6단계·사례·자동화에 연결하기

새 작업 단계를 늘리지 않는다. 카드는 기존 증거·판단 기록을 채우는 질문 모음이다.

기능 카드의 역할은 별도 보고서를 하나 더 만드는 것이 아니라 기존 분석 절차의 질문을 구체화하는 데 있다. 발견한 기능은 증거 수집과 구조 복원에, 연결 검증은 정합성 검토에 사용한다. 아래 사례 연결은 합성 자료의 적용 예시이며 실제 자동 탐지나 회계 엔진의 수행 결과와 구분한다.

기존 단계	FC를 사용하는 위치
Step 2 · 수집	기능 후보를 FC ID로 태깅. 함수·이벤트·역할·슬롯의 관찰 주장을 assertion_id에 기록.
Step 3 · 구조	배포 코드·상태·경로로 동작과 범위 확인. 카드별 통제맵·실제 주체 연결 작성.
Step 4 · 판단	M1~M5 중 필요한 질문만 적용. 기능 존재·실제 권리·통제 효과성의 결론을 분리.
Step 5~6 · 대사·보고	카드의 연결 검증을 증거 연결표·F-05에 반영. FC·RF·판단·발견 ID를 F-06에 남김.

DEMO-USD에 붙이는 시드 적용 기록

카드	기존 합성 자료와의 연결	수행 범위·남은 질문
FC-A01 V-FC01	V-D03 공급 상태·V-D04 발행 권한 → RF-02·03	가상 자료 기반 질문 구성. 기간 전체 발행 경로·입금 대사는 미수행.
FC-C02 V-FC02	V-D04 권한표·V-D08 승인 1건 → V-F03 / RF-02	정확한 역할 ID·실제 키 주체·모집단 확인 안 됨. 설계·운영 효과성 유보.
FC-E01 V-FC03	V-D04·05 업그레이드 설명 → V-F03 / RF-02	구현 주소·슬롯·호출 검증 미수행. 다중서명 설명을 발행 통제로 확장하지 않음.
FC-D02 V-FC04	기존 자료에 동결 동작의 확인 근거 없음	미확인. 사례에 동결 기능이 있다고 새로 가정하지 않음. 코드·조건 추가 요청.

자동화 구현의 경계

신호 수집 → 후보 카드 추천 → 확인 질문 생성 → 사람의 동작·범위 검토 → 증거 연결·전문 판단

규칙에는 rule_id·버전·조건·지원 범위·오탐·누락·테스트를 별도로 기록한다. 역할 해시·슬롯은 구현 의존적이고 과거 상태 조회도 제한될 수 있다. 탐지되지 않음은 부재의 증거가 아니다.

> 자동 탐지는 후보·질문을 제시하고, 동작·범위·증거 연결은 검토자가 확인한다. 구현 현황과 계획은 부록 B를 참고한다.

PART 4 · FUNCTION CARDS / 11 / SOURCES & ROADMAP

기능 카드의 공식 근거와 확장 순서

확인일: 2026년 11월 14일. 기술 참고 자료와 OCP의 질문·판단 설계를 구분한다.

공식 표준은 탐색의 출발점이며 실제 배포의 증거를 대신하지 않는다. 관련 기본 기능을 확인한 뒤 아래 순서로 복합 사례를 하나씩 완주한다. H01·H02·G02는 확장 계획이며 이 판에서 새 카드나 실제 분석이 완료된 것은 아니다.

출처 ID·자료	범위·공식 링크
FC-S1 ERC-20	인터페이스·이벤트의 표준 범위 https://eips.ethereum.org/EIPS/eip-20
FC-S2 OpenZeppelin ERC20 API	공급·소각·상한 등 구현 예시 https://docs.openzeppelin.com/contracts/5.x/api/token/erc20
FC-S3 OpenZeppelin Access Control	소유·역할·관리 권한 https://docs.openzeppelin.com/contracts/5.x/access-control
FC-S4 OpenZeppelin Proxy API	Transparent·UUPS·Beacon 등 https://docs.openzeppelin.com/contracts/5.x/api/proxy
FC-S5 ERC-1967	프록시 정보 슬롯·이벤트 https://eips.ethereum.org/EIPS/eip-1967
FC-S6 ERC-3643	적격성·제한·동결 등 인터페이스 https://eips.ethereum.org/EIPS/eip-3643
FC-S7 ERC-4626	볼트·자산·지분의 표준 범위 https://eips.ethereum.org/EIPS/eip-4626

복합 Web3 구조 · 단계별 적용 우선순위

순서·전제	연구 질문·완료 조건
0 · 기본 경로 보강	현재 A01·C02·E01·D02·X01 시드 유지. F03·F01·B03·F04는 해당 사례와 병행. 오라클·외부 호출·파라미터·분배 경로를 필요한 범위에서 선행 복원.
1 · H02 대출·청산	담보 예치 → 차입 → 이자 → 청산 → 잔여 청구권. G01·E02·G03 등 관련 기능을 연결해 권리·오라클·실행자·손실 부담·회수 기록 비교.
2 · H01 AMM·유동성	예치 → LP 권리 → 수수료·손익 → 인출. 가격 경로·풀 상태·기준 대안·비용을 고정해 경제적 손익을 계산하고 회계 인식은 별도 기준으로 검토.
3 · G02 브리지	잠금/소각 → 메시지 검증 → 도착 체인 발행/해제 → 실패·복구. 양 체인의 코드·기록·주체와 계약을 연결. 기술 완료와 법적 권리 이전 시점을 분리.

각 복합 적용의 완료: 실제 사례·기준일·코드 고정 → 관련 기본 카드·프로토콜별 질문 → 온·오프체인 근거 → 상태·현금흐름 대사 → 반례·실패 시나리오 → 판단·한계·재현 기록. OpenZeppelin 5.x 문서와 특정 배포의 동일성은 별도 검증한다.

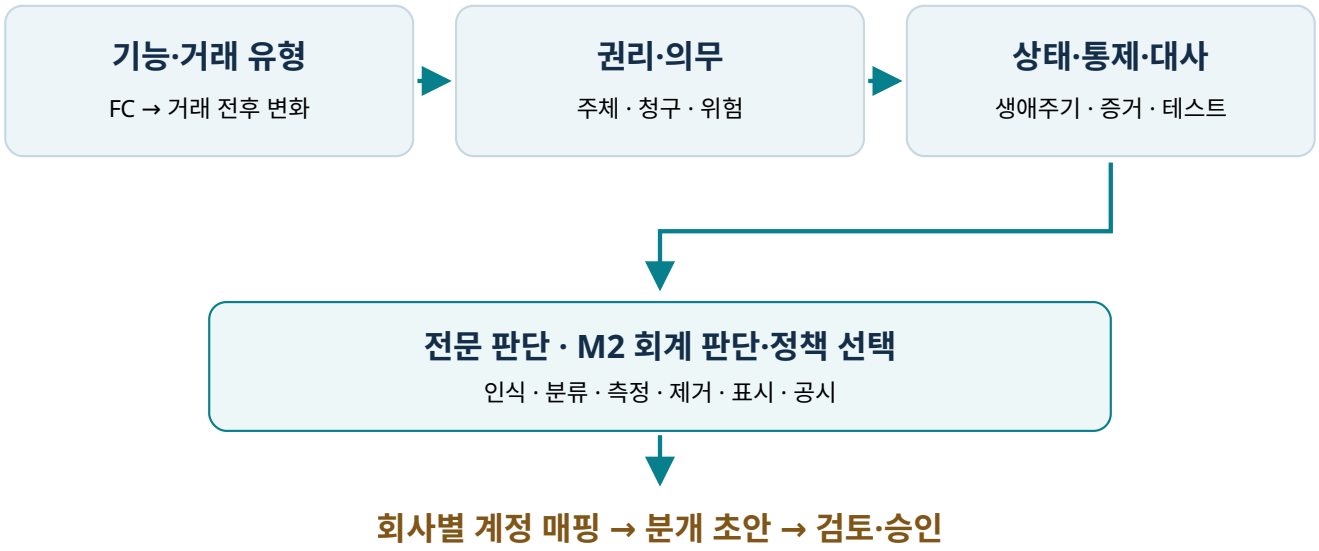
PART 5 · TRANSACTION TO ACCOUNTING / 01 / CONNECTION

동작에서 회계까지, 근거를 연결한다

6단계·M1~M5를 유지하고, 기존 양식의 첨부 도구로 연결한다.

기술적 동작이 곧 회계 계정으로 이어지지는 않는다. 같은 이전도 자기 지갑 이동·투자·담보 제공처럼 다른 경제적 사건일 수 있다. 아래 연결은 동작을 거래·권리·상태로 해석한 뒤 적용 정책과 계정 매핑을 검토하도록 하며, 이름만으로 분개를 선택하는 지름길을 두지 않는다.

예를 들어 transfer 기록 하나만으로 매각과 자기 지갑 이동을 구별할 수는 없다. 대가가 있었는지, 상대방이 누구인지, 통제와 권리가 어떻게 변했는지 확인한 뒤 경제적 사건을 정한다. 아래 단계들은 자동화의 입력 조건을 만드는 과정이기도 하며, 사실이 부족하면 회계 계정 대신 보완 질문이 출력되어야 한다.



첨부 도구	기존 양식·단계
거래 유형·권리 구조	F-03 첨부. Step 3에서 동작을 경제적 거래와 권리·의무로 연결.
생애주기·통제 테스트	F-05 첨부. Step 2~5에서 상태·시점·예외·설계·운영을 검토.
회계 규칙·계정·분개	F-04 · F-06 첨부. M2 판단 후 계정 매핑·분개 초안·보고 근거 연결.

새로운 약어·모듈을 외울 필요는 없다. 아래 기록은 기존 case_id · 판단·증거 ID를 재사용한다. FC는 동작을, 거래·권리 표는 실질을, 회계 규칙은 장부 반영 조건을 다룬다.

PART 5 · TRANSACTION TO ACCOUNTING / 02 / TRANSACTION

거래 유형을 이름보다 변화로 분류한다

F-03 첨부 · 하나의 거래는 여러 트랜잭션, 하나의 트랜잭션은 여러 경제적 사건을 포함할 수 있다.

거래 분류는 이벤트 이름보다 어떤 자산·권리·의무가 변했는지에서 시작한다. 여러 트랜잭션이 하나의 거래를 이루거나 하나의 실행 안에 여러 경제적 사건이 포함될 수도 있다. 아래 유형표는 후보를 좁히는 도구이며 각 거래의 계약·대가·통제 조건을 확인한 뒤 분류를 확정한다.

후보 유형	구분할 변화와 추가 질문
취득·매각·교환	무엇을 내주고 어떤 자산·권리를 받았는가? 거래상대방·가격·이행·수수료는?
예치·상환	보관·투자·대여 중 무엇인가? 받은 토큰의 권리·회수 조건과 위험은?
대여·차입·상환	누구에게 원리금을 청구하거나 지급하는가? 담보·기한·채무자는?
담보 설정·해제	어떤 권리를 유지·제한·이전했는가? 자산 제거와 별도 판단이 필요한가?
수탁·자기 지갑 이전	누구의 자산이며 실질 권리·위험·통제가 달라졌는가? 동일 주체를 확인했는가?
발행·소각·분배	공급 변화와 별개로 어떤 의무·대가·수익·자본 관계가 발생·소멸했는가?

거래 1건의 고정 기록

필드	기입할 내용
관점·식별	case_id / economic_event_id / 보고기업 / 거래 당사자 / 연결 FC·RF / 기준일
거래 전후	보유 자산·청구권·의무·통제·위험의 전후 변화와 수량·금액·단위
구조·대가	제공·수령 자산, 계약상 대가, 현금흐름, 다른 거래와의 조건부 연결
근거·대안	assertion_id · F/I/H · 증거 ID, 가능한 다른 거래 해석과 구분 증거
결과·상태	선택 유형 / 미분류·추가 확인 / 판단 ID · 관점·한계·검토자

economic_event_id는 원본 트랜잭션을 대체하지 않는다. 체인·거래 해시·로그 인덱스·내부 원장 행을 다대다로 연결하고, 묶거나 분리한 이유를 남긴다.

> 토큰 이동·mint · burn을 각각 독립된 회계 사건으로 자동 계산하지 않는다. 같은 경제적 사건의 기술 단계인지 먼저 검토해 중복 인식·중복 분개를 막는다.

PART 5 · TRANSACTION TO ACCOUNTING / 03 / RIGHTS

권리·의무 구조를 같은 항목으로 비교한다

F-03 첨부 · 토큰 잔액, 기초자산, 투자자 청구권과 시장가격의 범위를 구분한다.

기초자산이 같아도 투자자가 가진 권리가 다르면 현금흐름·위험·회계 검토의 전제가 달라진다. 자산 자체, 발행기구 지분, 채무 청구권을 같은 것으로 취급하지 않는 이유다. 아래 항목을 같은 순서로 비교하면 토큰의 표시와 실제 권리구조 사이의 차이를 드러낼 수 있다.

비교할 때는 토큰 수량이나 기초자산 명칭을 같게 두는 것만으로 충분하지 않다. 투자자가 받는 현금흐름, 우선순위, 환매·상환 조건, 잔여 위험이 달라지면 같은 자산을 바탕으로도 다른 청구권이 된다. 구조화 대안을 제시할 때는 무엇을 고정했고 무엇을 바꾸었는지 먼저 밝힌다.

고정 항목	질문·근거
권리자·의무자	누가 누구에게 청구·지급하는가? 주소·명의·수탁·실제 운영자의 관계는?
권리 대상	기초자산 자체 / SPV 지분 / 신탁수익권 / 채권 / 펀드 지분 / 상환청구권 중 무엇인가?
수익·상환	지급 산식·기한·조건·재량·공제 비용·미지급·취소·상환 거절 조건은?
담보·우선순위	담보 대상·설정·집행·순위·신용보강·손실 흡수 순서는?
이전·권리 성립	토큰 이전 외에 계약·명의·명부·승인·자격 등의 요건이 있는가?
통제·위험	누가 사용·변경·처분하고 어떤 이익·손실·제약을 부담하는가?
종료·부실	매각·만기·부도·청산·서비스 중단 시 권리가 어떻게 처리되는가?
증거 연결	계약 조항·버전 ↔ 보유·이전·상환 로직 ↔ 명부·원장·실제 지급. 연결 키·시점·공백 기록.

동일 자산의 구조 비교

대안	고정할 것 / 달리 볼 것
SPV 지분·신탁수익권·채권	기초자산·경제 가정은 가능한 한 고정하고 투자자 권리·비용·차입·우선순위·회수 절차의 차이를 명시.
가치평가 연결	어느 주체의 어떤 현금흐름을 평가하는지 먼저 정한다. DCF·NAV·워터폴의 가정과 권리 구조를 연결.

기록: economic_event_id / 권리 ID / 적용 관할·기준일 / 계약·FC·증거·판단 ID / F·I·H / 미확인·비적용 / 검토자. 학습용 대안 설계는 실제 법적 성립·실현 가능성과 구분한다.

PART 5 · TRANSACTION TO ACCOUNTING / 04 / LIFECYCLE

거래 상태와 회계 사건을 분리한다

F-05 첨부 · 실제 상품의 순서를 복원한다. 아래 상태 목록은 강제된 공통 순서가 아니다.

거래의 기술적 상태와 장부 반영 사건은 같은 순간에 생기지 않을 수 있다. 요청·잠금·승인·지급·소각을 구분하면 어느 시점에 어떤 권리와 의무가 남아 있는지 질문할 수 있다. 아래 생애주기 기록은 미완료·실패·재시도와 결산일 차이를 설명하는 연결 고리다.

상태·사건 후보	확인할 내용
요청·승인	요청 ID · 대상·권리 발생·승인 조건·거절·만료·취소
잠금·예치·발행	사용 제한·소유·통제·공급·대가 수령과 실제 법률 효과
실행·지급·정산	체인 실행과 은행 지급·대금 회수·원장 반영의 시점 차이
소각·해제·종료	기술 상태의 종료와 청구권·채무 소멸이 일치하는지
실패·되돌림·중단	실패 거래·재시도·중복·부분 정산·취소 후 잔여 권리

상태 전환 1건의 기록 양식

필드	기록 내용
식별·관계	economic_event_id / request_id / 이전·다음 상태 / 연결 거래·로그·원장 행
전환 조건	누가 어떤 조건으로 변경하는가? 시간·가격·승인·외부 지급·예외 조건
시점·증거	요청·실행·정산·회계 효력 시점 / 시간대·블록 / 증거 ID · F/I/H
수량·금액	토큰 수량·현금·청구권·의무 잔액과 단위. 미결·중복·취소 조정
책임·결과	담당·통제·미확인·후속 조치 / 판단 ID · 분개 초안 ID와인식 근거

상환 사례에서 생기는 질문

요청·잠금이 지급·소각·의무 소멸과 같은 사건인지 검토한다. 지급이 먼저 완료되고 소각이 늦어지면, 토큰 공급과 회계 의무가 잠시 다른 이유를 대사한다. 차이를 즉시 오류나 새 분개로 처리하지 않는다.

> “상태가 바뀌었다 → 분개한다”는 규칙을 쓰지 않는다. 승인된 회계정책에서 그 상태가 인식·제거·재분류 사건인지 먼저 판단한다.

PART 5 · TRANSACTION TO ACCOUNTING / 05 / CONTROL TEST

기능 카드에 통제 테스트를 붙인다

F-05 첨부 · 통제의 존재, 설계 적절성, 기간 중 운영 효과성을 나눠 기록한다.

통제 검토에서는 기능이 설계되어 있는지와 실제 기간 동안 작동했는지를 나눈다. 테스트 환경에서 한도가 작동한 결과는 운영 승인 기록의 완전성을 대신하지 않는다. 아래 표는 권한·한도·변경관리의 예상 동작을 테스트와 실제 이력에 각각 연결해 검토 범위를 분명히 한다.

테스트 결과에는 사용한 코드·환경·입력과 예상 결과를 함께 남긴다. 권한 없는 호출이 거절된 사례와 권한 변경 후 허용된 사례를 비교하면 통제가 어느 경로에 적용되는지 설명하기 쉽다. 실제 운영 이력이 필요한 질문은 이러한 실험 결과와 분리해 추가 자료로 확인한다.

고정 항목	기입 내용
목적·위험	어떤 오류·무단 행위·누락·중복·변경을 막거나 탐지하는가? 관련 FC·RF·판단
정상·우회 경로	정상 승인·실행 순서와 예외·대체 권한·모듈·외부 호출·긴급 경로
실행 범위	대상 코드·블록·기간 / 설계 검토·테스트·운영 검토 / 모집단·표본·선정 근거
기대·실제 결과	입력·사전조건·기대 상태·실제 상태·실패·되돌림·수량·시간·증거
환경·재현	테스트 환경·버전·코드·설정·실행 방법. 실제 운영과 차이·미수행 항목
결론·조치	예외·영향·대안 설명 / 설계·운영 각각 결론 / 보완·담당·기한·재검토

예: FC-A01 발행 한도

관점	점검 예시
설계 검토	한도가 있는가? 누가 바꾸는가? 다른 발행 경로·구현체 변경으로 우회할 수 있는가?
테스트 실행	허용량·경계값·초과량·권한 없는 호출·관리자 변경을 테스트 환경에서 비교. 예상과 실제 결과 기록.
운영 검토	분석 기간의 가용 발행·변경 모집단과 승인 기록을 연결. 표본·누락·실제 키 운영의 한계 명시.

> 설계 검토·테스트 환경·기간 중 운영 검토의 결과를 분리한다. 표본·누락·예외와 실제 운영으로 확대할 수 있는 범위를 남긴다.

PART 5 · TRANSACTION TO ACCOUNTING / 06 / ACCOUNTING FLOW

회계 판단에서 계정 매핑으로

M2 · F-04 첨부. 판단 → 계정 → 초안의 검토 흐름. 규칙·계정 필드와 구현 상태는 부록 A·B.

회계 알고리즘은 토큰 이름을 계정코드로 바꾸는 사전보다 조건을 확인하는 의사결정 절차에 가깝다. 거래 실질과 적용 기준·정책이 정해져야 인식·측정·제거와 계정 매핑을 검토할 수 있다. 아래 흐름에서 필수 사실이나 승인된 규칙이 없으면 초안 생성보다 보완 질문을 먼저 만든다.

순서	판단·처리	진행 조건
1 · 범위	보고기업·별도/연결 관점·회계기준·기준일·정책 버전 고정	관점·적용 범위 확인
2 · 사실	거래 유형·권리·의무·생애주기·증거 연결 확인	핵심 사실의 충실도 검토
3 · 회계 판단	인식 → 분류 → 측정 → 제거·재분류 → 표시·공시 검토	적용 기준·정책·결론 ID
4 · 규칙 선택	적용 조건·제외 조건·유효기간·근거·승인 상태 비교	적합 규칙 1개 또는 해결된 조합
5 · 계정 매핑	공통 회계 개념 → 회사 계정코드·보조계정·차원 연결	활성 매핑·승인 버전
6 · 분개 초안	금액·시점·환율·수수료·단위·차대 균형·중복·원장 대사	초안 생성과 검토 기록
7 · 승인·후속	초안 승인·전기 가능 여부·잔여 공시·결산 과제 기록	승인·전기·사후 대사를 구분

세 갈래의 처리 상태

상태	조건·행동
자동 처리 가능	핵심 사실·승인된 정책·활성 규칙·매핑·검산이 모두 충족된 반복 거래. 조직의 별도 권한 설정에 따라 처리.
검토 필요	복수 규칙 충돌·새로운 거래·대안 해석·예외·정책 변경 등. 근거와 후보를 제시하고 전문가 검토.
판단 보류	주체·권리·금액·적용 기준 등 핵심 자료 부족. 계정을 억지로 선택하지 않고 추가 자료 요청.

> 핵심 사실의 충실도와 해석의 명확성을 나눠 판단한다. 인식·분류 미확정이면 계정·분개를 확정하지 않는다.

PART 5 · TRANSACTION TO ACCOUNTING / 09 / V-A01

시범 ① 자기 지갑 간 이전

기업 A 관점. 동일 권리·통제 유지, 수수료 0인 상황을 가정한다.

이 시범은 같은 주체의 통제 아래 있는 두 지갑 사이의 이동을 가정한다. 체인상 이전이 발생해도 새로운 상대방과의 거래가 없으면 기존 장부금액의 위치만 보조원장에서 바뀔 수 있다. 아래 조건 중 통제·권리·수수료 가정이 달라지면 동일한 처리로 자동 이어가지 않고 거래 유형부터 다시 검토한다.

자료 · 합성 | 카드 · 관련 카드 시드 | 범위 · 계산·분개 초안

연결 단계	가상 입력·판단
거래·권리	A가 통제하는 W1 → W2로 10단위 이동. 제3자 수탁·담보·교환이 아니며 실질 권리·위험 변화가 없다고 설정.
기능·생애주기	FC-B01 이전. 완료 거래·원장 행·키 운영 자료가 같은 이전을 가리킨다고 가정. 실제 FC-B01 상세·실행 검증은 미수행.
회계 규칙	가상 정책 P-A01: 기존 자산 분류·장부금액을 유지하고 위치만 변경. 동일 총계정 아래 지갑 보조원장 사용.
기초 잔액	W1 20단위·장부금액 1,000 / W2 0. 이전하는 10단위의 장부금액은 500으로 설정.
처리 결과	W1 -10단위·-500 / W2 +10단위·+500. 총 20단위·1,000 유지. 총계정 신규 분개 없음·보조원장 이동만 기록.

처리 추적 예시

economic_event_id = V-A01-E1 → 가상 정책 P-A01 → 규칙 V-A01-R1 · v0.1 → 매핑 V-A01-M1 → 기록 V-A01-J1(총계정 분개 없음). 합성 자료의 가정 H와 그 안의 계산 결과를 실제 확인 F로 바꾸지 않는다.

예외를 추가하면	다음 행동
W2가 외부 수탁·담보 주소	권리·통제·의무를 재검토하고 유형·정책을 다시 선택.
가스·수수료 발생	별도 경제적 사건과 측정·계정 처리 검토. 본 예시에는 포함하지 않음.
주소 귀속 자료 없음	동일 주체 전제 미확인 → 판단 보류·자료 요청.

> 권리·통제·수수료 조건이 달라지면 거래 유형과 정책을 다시 검토한다. 동일 주체 전제가 미확인이면 자료 요청·보류로 전환한다.

PART 5 · TRANSACTION TO ACCOUNTING / 10 / V-A02

시범 ② 발행·상환의 상태와 분개

기존 DEMO-USD와 별도의 소규모 예시. 금액 단위: 가상 기능통화.

이 시범에서는 요청·잠금, 실제 지급, 소각을 별도 사건으로 나누어 본다. 가상 정책상 의무가 언제 줄어드는지를 먼저 정했기 때문에 공급량과 장부 부채가 일시적으로 다른 상태도 설명할 수 있다. 아래 분개는 이 합성 조건의 예시이며 스테이블코인 일반의 회계처리를 확정하는 규칙이 아니다.

상환 요청 때 부채를 줄이고 지급 때 다시 줄이면 같은 의무를 두 번 제거하는 오류가 생길 수 있다. 반대로 지급 후 소각 전의 상태를 단순 공급량 비교만으로 보면 차이를 잘못 해석할 수 있다. 이 예시는 같은 권리의 생애주기와 장부 사건을 연결해 시점 차이와 오류를 구별하는 연습이다.

자료 · 합성 | 카드 · 관련 카드 시드 | 범위 · 계산·분개 초안

발행사 B가 수령 자금을 통제하고, 보유자에게 액면 현금 상환의무를 부담한다고 설정한다. 가상 승인정책 P-A02는 입금·의무 성립 시 은행예금과 상환의무를 인식하고, 현금 지급으로 해당 의무가 소멸하는 조건을 둔다. 이 분류·제거 결론은 실제 상품에 대한 판단이 아니다. 수수료·환율·이자·손상·세금은 없는 것으로 설정한다.

상태·경제적 사건	가상 정책에 따른 분개 초안	대사
T0 입금·의무 성립 및 발행 1,000	차) 은행예금 1,000 대) 상환의무 1,000	계정 DEMO-1101 / 2201. 기술적 mint에 별도 중복 분개를 만들지 않음.
T1 상환 요청·잠금 100	이 가정에서는 신규 분개 없음	현금 미지급·의무 1,000 유지. 잠금은 소각·채무 소멸과 다름.
T2 현금 지급 100·의무 소멸	차) 상환의무 100 대) 은행예금 100	현금·의무 900. 소각 전 공급 1,000과 100 차이는 지급·소각 시차로 대사.
T3 기술적 소각 100	이 가정에서는 추가 총계정 분개 없음	공급 900·의무 900. 지급과 소각을 별도 상환으로 중복 인식하지 않음.

카드·규칙·검증 연결

FC-A01 · FC-A02 · FC-F03 / RF-01 · RF-03 → 요청 ID · 지급·소각·원장 연결 → 가상 규칙 V-A02-R1 · R2 / 정책 P-A02 / 매핑 M-A02 / 초안 V-A02-J1 · J2. 지급 완료와 청구권 소멸 근거가 없으면 T2 초안을 보류한다.

> 발행·상환의 회계 인식·제거 시점은 계약·기준·정책에 따라 별도 검토한다. 이 사례의 가정은 기존 DEMO-USD의 1,200만 대사나 회계 결론을 변경하지 않는다.

PART 5 · TRANSACTION TO ACCOUNTING / 11 / V-A03

시범 ③ RWA 투자 취득·분배

투자자 C 관점. 토큰화된 1년 만기 채권의 단순 모델.

토큰화된 채권의 회계처리를 연습하더라도 먼저 어떤 계약상 청구권을 보유하는지 확인해야 한다. 이 시범은 상각후원가 분류가 별도로 승인됐다는 가정에서 단순 현금흐름과 분개를 연결한다. 아래의 취득·이자·상환을 따라가며 같은 분배 이벤트도 이자·원금 등 성격에 따라 처리가 달라짐을 살펴본다.

실제 사례로 확장하면 취득가격·수수료·신용손실·환율·결산 시점의 차이가 추가 검토 대상이 될 수 있다. 여기서는 계산 구조를 드러내기 위해 그 변수를 단순화했다. 가정을 바꿀 때는 금액만 고치지 말고 적용 규칙과 계정 매핑, 대사 항목까지 함께 달라지는지 확인한다.

자료 · 합성 | 카드 · 관련 카드 시드 | 범위 · 계산·분개 초안

계약상 원리금 청구권을 보유하는 금융자산이며 상각후원가 측정 조건을 충족한다는 별도 판단이 승인됐다고 가정한다. 액면·취득가 1,000, 연 이자 5%, 수수료·할인·할증·환율 변화는 0, 손실충당금은 0으로 설정한다. 실제 상품에서는 사업모형·현금흐름 특성·신용손실·인식 시점 등을 따로 검토해야 한다.

거래·권리·상태	가상 정책 P-A03의 초안	연결 검증
취득 조건 충족·대금 지급 1,000	차) 투자 금융자산 1,000 대) 은행예금 1,000	계약·거래일 정책·명의·토큰·지급의 같은 권리 연결.
1년 이자 발생과 수령이 같은 시점 50	차) 은행예금 50 대) 이자수익 50	1,000 × 5% × 1년 = 50. 기간별 미수 인식·결산이 필요하면 별도 사건·분개.
원금 상환 1,000·권리 소멸	차) 은행예금 1,000 대) 투자 금융자산 1,000	상환·원장·명부·소각·잔여 청구권을 대사. 장부금액 0.

같은 “분배”라도 규칙은 달라질 수 있다

확인된 성격	검토 방향
이자·배당·원금 반환·자본 회수	권리·원천·지급 조건·적용 기준을 구분한다. distribution 이벤트 이름으로 수익 계정을 고르지 않는다.
권리·분배 명세 미확인	분배 성격·계정 선택 보류. 계약·산식·명세·발행자 기록 요청.

규칙 V-A03-R1~R3 · v0.1 / 매핑 M-A03(DEMO-1501 · 1101 · 4101) / 초안 V-A03-J1~J3. 공식 참고: 회계-S3. 상각후원가를 모든 RWA 채권의 기본값으로 사용하지 않는다.

> 분류·측정·분배 성격이 바뀌면 규칙과 초안을 다시 선택한다. 토큰명·distribution 이벤트만으로 수익을 결정하지 않는다.

APPENDIX A · RULE SPECIFICATION

회계 규칙 1건의 고정 양식

M2 · F-04 첨부. 회사별 계정코드에 앞서 공통 회계 판단과 정책을 정의한다.

규칙을 재사용하려면 결론만이 아니라 적용 조건과 멈춤 조건을 저장해야 한다. 필수 증거가 없거나 정책·기준 버전이 달라졌을 때 같은 초안을 내보내지 않도록 하는 장치다. 아래 양식은 사람이 검토한 판단을 조건·분기·출력·시험 사례로 표현하기 위한 명세이며 구현 완료를 뜻하지 않는다.

조건은 분석자가 읽을 수 있는 문장과 기계가 확인할 수 있는 필드로 함께 표현하는 편이 좋다. 다만 숫자 필드가 채워졌다고 판단 전제가 충족되는 것은 아니므로 승인 정책과 증거 상태도 연결한다. 규칙 시험에는 정상 입력뿐 아니라 누락·충돌·경계값·중복 사건이 어떻게 처리되는지도 포함한다.

필드	기록 내용
식별·효력	rule_id · 버전·보고기업·기준·관할·유효기간·승인자·승인일·시드/검토/활성/폐기
적용·제외 조건	자산·부채·권리·거래 유형·관점·사업모형·보유 목적·생애주기·예외 조건
필요 증거	계약·원장·지갑 귀속·가격·지급·통제 등 필요한 사실과 충실도·연결 상태
기준·정책 근거	적용 기준의 문단·판본·효력·회계정책·판단 ID. 규정·해석·회사 정책을 구분
분기·판단	조건 → 적용 처리 → 대안·미충족 시 검토/보류. 규칙 간 우선순위와 충돌 해결
회계 결과	인식 대상·시점·분류·측정·제거·재분류·표시·공시 및 후속 결산 과제
계정·분개 양식	공통 회계 개념·mapping_id · 차대 구조·금액 산식·환율·수수료·반올림·역분개 조건
통제·검증	중복 키·모집단·차대·가격·잔액 검산·테스트·검토 상태·재검토 트리거

규칙을 활성화하기 전

조건을 충족하는 예시와 충족하지 않는 반례를 함께 검토한다. 회사 정책과 규칙의 승인·버전을 고정한다. 자산·부채 분류, 측정 기준, 계정 매핑은 각각 검토하고 변경 시 영향받는 사례와 초안을 추적한다.

공식 기준 참고: 회계정책 선택·판단은 회계-S2, 금융상품 인식·분류·측정의 개요는 회계-S3. 표준 요약 페이지의 확인이 개별 거래의 회계정책 검토·승인을 대신하지 않는다.

> 규칙을 활성화하기 전 정책 승인·버전·조건·제외 조건·반례를 검토한다. 사례별 판단과 규칙의 승인 상태를 분리한다.

APPENDIX A · ACCOUNTS & JOURNAL

계정코드와 분개 초안을 추적한다

F-06 첨부 · 표준화된 회계 개념과 회사별 계정체계를 분리한다.

공통 회계 개념과 회사별 계정코드는 서로 다른 층위다. 같은 개념도 회사의 계정체계·보조원장·거래 차원에 따라 다른 코드로 연결될 수 있다. 아래 매핑과 분개 초안 기록은 어느 정책·규칙·자료를 사용했는지 추적하고 승인 전 초안과 실제 장부 반영을 구분하기 위한 것이다.

초안에는 금액과 차변·대변 외에 해당 사건과 규칙·매핑의 버전을 연결한다. 나중에 정책이 바뀌거나 거래가 취소되면 어떤 초안을 다시 검토해야 하는지 찾기 위해서다. 실제 장부 전기 여부와 수동 수정 이력은 초안 생성과 별도 단계로 관리한다.

가상 공통 개념	가상 회사 계정코드	연결 조건
은행예금	DEMO-1101	해당 회사가 통제하는 은행 자금으로 판단·승인된 경우
상환의무	DEMO-2201	사례별 권리·의무·인식 정책이 승인된 경우
투자 금융자산	DEMO-1501	금융자산의 구체적 분류·측정 결론을 따로 확정
이자수익	DEMO-4101	계약·기간·금액·인식 정책 확인 후 매핑

위 코드는 설명용이다. IFRS·K-IFRS가 지정한 공통 계정번호가 아니며 실제 회사에 그대로 적용하지 않는다. 지갑 주소·토큰명과 계정코드도 일대일 관계로 고정하지 않는다.

분개 초안 1건의 고정 기록

항목	내용
추적	journal_draft_id / economic_event_id / case_id / 원본 거래·로그·원장 행 / 중복 방지 키
판단·버전	judgment_id / rule_id·버전 / policy_version / mapping_id·버전 / 증거·FC·RF ID
차대·측정	차변·대변·보조계정·기능통화 금액 / 원자산·수량 / 가격·환율·시점·출처
검산·예외	차대 균형·잔액·수량·기간·누락·중복 / 수수료·평가·분배·역분개 연결
상태·책임	제안·검토·승인·전기 상태 / 담당·검토자 / 미확인·보류 사유·재검토 조건

> 같은 자산을 어떤 지갑에서 보유하는지는 보조원장 차원일 수 있다. 내부 위치 변경마다 손익·취득·처분 분개를 만들지 않는다. 주소 귀속·권리 변화와 회사 계정정책을 먼저 확인한다.

APPENDIX B · IMPLEMENTATION

문서·수집 도구·자동화의 현재 상태

일반 실무 독자는 본편으로, 구현 담당자는 이 부록과 부록 A로 범위를 확인한다.

방법론 문서, 실제 자료 수집 스크립트, 앞으로 구현할 판단 지원 기능의 상태를 구분한다. 코드가 일부 있다고 전체 분석이 자동화된 것은 아니며, 명세가 자세하다고 엔진이 실행된 것도 아니다. 아래 현황과 완료 조건을 기준으로 이후 구현·시험 결과를 기록하고 실제 수행 범위가 늘어난 만큼만 상태를 갱신한다.

구분	현재 상태
분석 명세·사례	6단계·양식·시드 FC/RF · 거래·권리·상태·회계 명세, 합성 사례와 USDC 진행본.
실제 수집 도구	USDC 착수팩의 공개 RPC 읽기·원본 보존·해시 계산·재조회 스크립트. 지정 블록 조회를 수행한 기록 포함.
업무 자동화 미구현	기능 자동 탐지·자동 귀속·회계 규칙 엔진·계정 매핑·분개 생성·ERP 자동 전기.
운영 경계	수집 코드는 전문 판단을 자동 확정하지 않는다. 실제 거래 전송·계정 접근·운영 시스템 전기는 수행하지 않음.

다음 시범 구현과 검증

범위	계획·완료 조건
입력·처리	JSON · CSV 합성 데이터 → 필수·참조 검증 → 사전 규칙 → 계정 매핑·분개 초안 또는 무분개·보류.
세 사례	자기 지갑 이전·발행/상환·RWA 채권 취득/분배를 사용. 정상 조건과 누락·규칙 충돌·중복·기간 차이 비교.
재현·책임	차대·수량·기초/기말·원본 연결 검산. 정책·규칙·매핑·코드·데이터 버전과 검토·승인·전기 상태 분리.
GitHub · 문서	코드·입력·검증 기록·실행 방법은 저장소, 문서는 범위·결과·한계·버전 연결. 실제 공개 전 URL을 만들지 않음.

완료 후 갱신할 상태

실제로 구현·검증한 기능만 릴리스·커밋·검증 기록과 함께 표시한다. “합성 데이터 기반 계정 매핑·분개 초안 시범 구현”과 실제 회계 판단·운영 연동·자동 전기의 완료를 구분한다.

> 현재 업무 자동화는 미구현이다. 공개자료 수집의 실제 수행 기록과 회계 시범 엔진의 향후 계획을 섞지 않는다.

APPENDIX C · ACCOUNTING SOURCES

공식 회계 참고와 적용 기록

공식 자료 확인일: 2026년 11월 14일. 표준 문서·회사 정책·알고리즘 규칙의 버전을 분리한다.

공식 회계 자료는 판단의 근거를 찾는 출발점이며 개별 상품에 대한 자동 답안이 아니다. 적용 기준과 회사 정책을 특정하고 거래의 사실관계를 연결해야 실제 판단을 설명할 수 있다. 아래 출처와 운영 과제는 규칙을 구현할 때도 기준·정책·버전·승인을 함께 관리해야 하는 이유를 정리한다.

출처의 최신성만큼 적용 범위도 중요하다. 특정 위원회 논의가 모든 디지털자산의 분류를 결정하지 않으며, 금융상품 기준의 검토도 해당 권리와 거래 사실에서 출발한다. 분석 메모에는 참고 문서·판본과 그 문서가 실제로 뒷받침하는 판단 범위를 함께 적는다.

공식 참고	확인 범위·링크
회계-S1 2019 가상통화 보유 의제결정	https://www.ifrs.org/content/dam/ifrs/supporting-implementation/agenda-decisions/2019/holdings-of-cryptocurrencies-june-2019.pdf
회계-S2 IAS 8 공식 개요·회계정책	https://www.ifrs.org/issued-standards/list-of-standards/ias-8-basis-of-preparation-of-financial-statements/
회계-S3 IFRS 9 공식 개요	https://www.ifrs.org/issued-standards/list-of-standards/ifrs-9-financial-instruments/
회계-S4 IFRS 13 공식 개요	https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/

회계-S1은 계약을 발생시키지 않는 등 한정된 가상통화의 보유를 다룬다. 이를 모든 스테이블코인·RWA에 일괄 적용하지 않는다. 회계-S2는 회계정책 선택·판단, S3은 금융상품, S4는 다른 기준이 요구·허용하는 공정가치 측정의 참고다. 적용 판본·시행일·조기 적용·국내 채택 차이는 개별 분석에서 확인한다.

규칙을 구현할 때의 우선 과제

과제	완료 조건
공통 기록	사건·주장·증거·권리·상태·판단·규칙·매핑·초안을 ID로 연결. 누락·미확인·비적용을 구분.
검증·변경	조건 충족·반례·결측·규칙 충돌·중복·시점·역분개를 시험. 과거 버전과 변경 영향을 기록.
승인·권한	규칙 설계·정책 승인·초안 검토·실제 전기의 책임을 구분. 활성화·변경·수동 수정 이력 보관.
다음 사례	세 시범 사례를 실제 공개 자료로 확장. 외부 자료가 부족하면 가정을 유지하고 실제 검증 범위를 과장하지 않음.

EDITION / v1.0

v1.0의 구성과 발전 계획

첫 공개를 위한 기준판. 방법론·사례·양식·기능 카드와 향후 검증 과제를 함께 담았다.

v1.0은 현재의 분석 절차와 공개자료 적용 범위를 묶은 기준판이다. 후속 발전은 분량이나 카드 수보다 실제 사례에서 확인한 누락·반례·재현성의 문제를 근거로 결정한다. 아래 계획은 이미 수행한 내용과 앞으로 검증할 내용을 구분하며 추가 자료로 판단이 달라진 이력을 축적하는 방향을 제시한다.

주요 구성	수록 내용
독자·구성	회계·준법·AML·IT감사 실무자를 위한 학습·적용 매뉴얼. 본편과 개발·운영 부록으로 구성.
범위·배지	공통 범위 안내와 자료 성격·카드 상태·수행 범위의 세 축 표시. 각 결론에 구체적 증거 한계를 기록.
실제 사례	USDC F-01과 고정 블록 읽기 관찰을 진행본으로 통합. 소스 대응·4개 카드 완결·준비자산 대사는 남은 과제.
카탈로그·ID	4개 시드 카드·귀속 체크리스트·복합 Web3 확장 계획. ID 지도와 쉬운 이름으로 사용 절차 안내.
교육 사례	DEMO-USD 교육 사례: 최초 자료 → 추가 자료 → 판단 수정의 과정을 수치·근거와 함께 제시.

후속 발전은 적용 결과로 결정한다

검토 과제	판단 기준
USDC 실증	배포 소스 대응·통제맵·샘플 거래와 준비자산 보고 범위 확인. 실제 확보 범위만 반영.
M1·M3 보강	M3 공통 흐름·과세/보고 분리·조건부 분기를 12쪽에 수록. 관할별 규정·사실·증거의 적용과 국내 규제·조세 부록은 후속 과제.
양식·카드 개선	11·50쪽 주체 귀속 절차를 사례에 적용. 관련 기본 기능 보강 후 H02 → H01 → G02를 단계적으로 검토(58쪽). 실행·반례·재현 이력으로 카드 개선.
공개·변경관리	출처·기준일·버전·가정·원본을 보존. 추가 자료나 코드 변경으로 바뀐 판단을 추적.

> 자료를 충분히 모았는지, 해석이 명확한지, 어떤 위험이 남는지는 각각 판단한다. 새로운 자료를 받으면 결론과 범위를 갱신하고 기존 판단을 이력으로 남긴다.

APPENDIX · EXISTING METHODS / UPDATED STATUS

보완 부록 / 적용 안내

기존 가치평가·증거 판정·완료 기준(73~77쪽)은 유지한다. 이번 사례 보완(78~88쪽)은 같은 F-01~F-06 양식의 적용 예시이며 새로운 전문 모듈을 추가하지 않는다.

기존 양식과 연결

가치평가 연결표는 F-01 / F-03 / F-04 / F-05, 증거 판정표는 F-02 / F-04 / F-06, 사례 완료표는 F-01 / F-06에 연결한다. 기존 case_id / assertion_id / evidence_id / judgment_id를 재사용한다.

완료 상태 · 2026-11-18

기존 부록은 방법표와 판정 절차를 제안한 것이다. 이번에는 USDC 공개보고서 선정·보고서 내부 산술 재현과 F-02 / F-05 / F-06 기입을 추가했다. 추가 RPC 조회, 은행·수탁·내부 원장 확보, 배포 소스 대응, 독립 검토자 재현은 수행하지 않았다.

필수 기록

각 표에 사례 ID, 작성자 / 검토자, 기준일 / 블록, 출처 / 판본, 적용 기준, 가정, 미확인 사항을 기록한다. 빈칸은 미확인 / 비적용 / 추가 요청 중 하나로 설명한다.

분석자 사용 순서

범위와 사례 유형 선택 → 주장별 증거 조건 설정 → 권리 / 현금흐름 복원 → 평가 / 전문 판단 → 대사 → 검토 / 종료. 새로운 자료가 들어오면 기존 판단을 보존하고 변경 사유를 기록한다.

> 실제 공개자료(R-USDC-01)와 국내 합성 교육 사례(S-KR-ISS-01)를 혼합하지 않는다. 합성 자료의 계산상 일치는 실제 발행통제의 효과성 입증이 아니다.

M4 첨부 / RWA 가치평가 연결표

1. 평가 대상을 고정한다

기초자산 자체, SPV 지분, 신탁수익권, 채권, 토큰이 나타내는 개별 권리 중 평가 대상을 특정한다. 평가 목적 / 기준일 / 통화 / 가치 기준 / 평가 단위 / 관점을 기록한다. 토큰 수량과 법적 권리 단위를 연결한다.

2. 기초자산에서 귀속 현금흐름으로

기초자산의 수입 / 공실 / 운영비 / 자본적 지출 / 세금 / 처분대금과 근거를 기록한다. 차입 원리금 / 수수료 / 유보금 / 우선권을 반영해 해당 투자자에게 귀속되는 현금흐름을 산정한다. 자산 가치가 이미 차입 효과를 포함하는지 확인해 부채를 중복 차감하지 않는다.

3. 권리별 배분과 평가

배분순위, 손실 부담, 만기, 상환 / 청산 조건, 의결권, 이전 제한을 계약 조항과 코드 경로에 연결한다. 지분은 지분 현금흐름과 대응 할인율, 채권은 약정 지급과 신용 / 회수 위험을 검토한다. 기초자산 순자산가치를 모든 토큰 가치로 일괄 사용하지 않는다.

4. 토큰 단위로 연결한다

동질 / 동순위 권리라면 배분 대상 권리가치 ÷ 해당 권리를 나타내는 유효 단위 수로 기준값을 구한다. 미발행 / 금고 보유 / 소각 / 희석 / 다중 클래스는 계약상 권리와 분모 포함 여부를 확인한다. 공급량만으로 분모를 확정하지 않는다.

5. 가격 / 위험 / 민감도를 대조한다

거래가격의 시점 / 시장 / 거래량 / 당사자 / 가격 출처를 기록한다. 권리 가치와 가격 차이를 제한 / 유동성 / 비용 / 정보 / 통제 위험으로 설명하되 조정과 할인율에 같은 위험을 중복 반영하지 않는다. 공실 / 금리 / 채무불이행 / 환매 중단의 민감도를 제시한다.

M4 첨부 / 계산 검산과 종료 기준

단순 합성 예시의 전제

건물 자산가치 100, 차입금 공정가치 40, 별도 확정 지급의무 2, 현금 0으로 가정한다. 모든 토큰은 동일한 잔여 지분권이며 유효 권리 단위는 58,000개다. 추가 클래스 / 우선권 / 세금 / 거래비용 조정은 없다고 가정한다.

예시 계산

잔여 지분 기준값 = 100 - 40 - 2 = 58. 토큰 단위 기준값 = 58 ÷ 58,000 = 0.001. 모든 수치는 합성 가정이다. 장부금액과 공정가치의 차이, SPV의 다른 자산 / 부채, 계약상 분배 제한이 있으면 다시 산정한다.

세 가지 대사

(1) 계약상 총 권리와 유효 토큰 단위의 대사 (2) 모델의 총 배분액과 클래스별 합계 대사 (3) 기초 / 기말 공급량과 발행 / 소각 / 권리 변동 대사. 각 차이의 원인과 계산 영향을 F-05에 연결한다.

결론을 멈추는 조건

평가 대상 권리, 우선순위, 기초자산 범위, 중대한 부채 또는 유효 권리 단위를 특정하지 못하면 확정 단위가치 산정을 유보한다. 가정을 명시한 조건부 계산은 가능하나 실제 가치 결론과 구분한다.

남길 결과

선택 방법 / 대안 / 산식 / 입력 근거 / 민감도 / 검산 / 미확인 사항 / 검토자를 기록한다. 전문 평가기준의 구체적 적용과 감정 / 법률 / 세무 등 추가 검토 필요성은 사례별로 정한다.

F-02 / F-04 첨부 / 주장별 증거 판정

주장 A / 주소의 실제 운영 주체

필수 확인은 대상 주소 / 권한 / 기준기간과 법인 또는 담당자의 연결이다. 공식 주소 공시, 위임 / 서명자 자료, 승인 / 실행 이력을 교차검토한다. 공개자료 분석에서는 공식 공시를 근거로 범위를 제한할 수 있다. 서명 성공은 키 접근을 뒷받침하지만 법적 권리나 실소유자를 단독 입증하지 않는다.

주장 B / 상환 청구권과 의무

적용 약관의 판본, 청구 가능자, 의무자, 지급 조건 / 제한을 확인한다. 실제 이행 주장은 요청 / 지급 / 소각 / 원장 연결이 추가로 필요하다. 소각 기록이나 과거 상환 사례만으로 모든 보유자의 권리를 확정하지 않는다. 약관과 실행의 충돌은 별도 쟁점으로 기록한다.

주장 C / 통제의 운영 효과성

설계 확인과 실제 운영을 분리한다. 대상 기간의 모집단 / 완전성, 승인 / 실행 / 권한 변경 기록, 표본 선정 근거와 예외 처리가 필요하다. 재수행 / 관찰 / 독립 확인은 해당 주장에 적합할 때 대체 / 보완한다. 핵심 기간 또는 모집단이 미확인되면 운영 효과성 결론을 유보한다.

E1~E4 적용

E1은 범위 내 핵심 주장에 적합한 근거와 연결이 충분하고 중대한 미해결 충돌이 없는 상태다. E2는 제한을 특정할 수 있어 결론 범위를 제한한다. E3는 간접 근거 / 미해결 충돌로 핵심 추론이 남는다. E4는 핵심 근거가 없어 판단이 어렵다. 등급은 문서 수나 자동 합산 점수로 정하지 않는다.

반증 / 검토 기록

주장마다 반대 설명, 누락된 경로, 위임 / 복구 / 우회 권한, 상반 자료를 기록한다. 작성자와 검토자가 각각 등급 / 이유를 적고, 불일치는 기준 / 추가 증거 / 최종 승인 사유로 해소한다. 합의되지 않으면 복수 해석 또는 유보로 남긴다.

APPENDIX · COMPLETION / UPDATED STATUS

F-01 / F-06 첨부 / 사례 완료 수준

공개자료 케이스의 완료

공개 범위 안의 질문을 고정하고 출처 / 판본 / 조회 조건 / 원본과 판단 연결을 남긴다. 확보할 수 없는 내부 자료는 요청 목록과 결론 영향을 기록한다. 공개 근거로 답할 수 있는 결론 / 조건 / 유보를 확정하면 해당 범위의 분석을 완료할 수 있다.

고객자료 케이스의 완료

계약된 업무범위, 자료 제공 권한, 대상 시스템 / 계좌 / 기간 / 모집단 완전성, 내부 승인 / 수탁 / 은행 자료의 연결을 추가한다. 중대한 예외와 미수령 자료의 영향을 평가하고 검토 기록을 남긴다. 자료 확보 자체로 증거 충분성을 확정하지 않는다.

공통 인수 기준

F-01의 질문 / 제외 범위와 F-06의 결론이 대응해야 한다. 중대한 결론에는 근거 / 기준 / 가정 / 한계가 있어야 한다. 미해결 항목마다 영향 / 담당 역할 / 후속 조치 / 재검토 조건을 적는다. 완료와 유보는 함께 존재할 수 있다.

USDC 수행 상태 · 78~83쪽 참조

완료: 준비자산 보고서 판본·시점·정의 확인, 문서 내부 계산, 주장별 증거 연결과 결론 범위 기록. 미수행: 동일 시점 전체 체인 재조회, 배포 코드·권한 운영 대조, 내부 준비자산 원장·은행 확인, 독립 재현. 따라서 전체 R-USDC-01의 검증 완료로 표시하지 않는다.

독립 재현과 개정

다른 검토자가 입력 / 버전 / 실행 지침으로 같은 관찰값과 계산을 재현하고, 판단은 근거의 타당성을 검토한다. 관찰값 일치와 전문 판단 일치를 따로 기록한다. 실제 완료일 / 결과 / 차이 / 수정 이력을 남긴다. 이번 보완에는 독립 검토자의 서명이 없다.

CASE SUPPLEMENT · 2026-11-18 / VANZI

사례 보완을 읽는 순서

공개자료에서 가능한 결론을 끝까지 연결하고, 불가능한 결론은 근거와 함께 멈춘다.

구분	범위	위치
R-USDC-01-R	실제 공개보고서 · 선정 / 내부 산술 / F-02 / F-05 / F-06	79~83
S-KR-ISS-01	국내 발행통제 · 전부 합성 자료 / 수량 대사 / 권한·권리 분리	84~87
출처·개정 기록	공식 출처 / 재현 지침 / 원문과의 연결	88

두 가지 완료를 구분한다

- USDC: 보고서에 기재된 수치와 정의를 확인하고 계산을 재현했다. 보고서의 기초자료를 독립 검증한 것은 아니다.
- 국내 사례: 고정한 합성 입력으로 차이를 식별하고 판단·조치까지 작성했다. 실제 기관의 거래나 시스템을 검사하지 않았다.

이번 개정이 바꾸지 않는 것

기존 6단계, 5개 전문 모듈, F-01~F-06과 FC 체계를 유지한다. 원문 21~23쪽의 RPC 관찰을 새 조회 결과로 대체하지 않으며, 원래 날짜·주소·제약을 보존한다. OCP v1.0의 등록 판본이나 등록 범위가 이번 내용까지 갱신되었다고 주장하지 않는다.

판단 상태

표시	의미
확정 · 범위 한정	명시한 입력·범위 안에서 근거와 계산이 맞음
조건부	가정이 유지되거나 추가 조건이 충족될 때만 성립
유보	필요 증거가 없어 결론에 도달하지 않음
합성	교육 목적의 가정 자료. 실제 관찰 사실 F와 구분

> 실제 보증업무·법률 의견·회계감사 결과로 사용하지 않는다. 고객 업무에서는 목적·기준·권한·모집단·검토 책임을 별도로 확정해야 한다.

R-USDC-01-R · F-01 / SCOPE

USDC / 보고서와 기준시점을 고정한다

질문: 공개보고서 내부의 준비자산·유통량 계산은 일관되는가? 기존 온체인 관찰과 무엇이 연결되지 않았는가?

항목	고정 값
작성 / 검토	Vanzi / 독립 검토 미수행 · 정리일 2026-11-18
원문 S1	2026 USDC Examination Report September 26 · 6쪽 / 공식 Circle 투명성 페이지 연결 PDF
발행·보고 시점	보고서 일자 2026-10-26 / 본 보완 기준 2026-09-30 23:59 UTC
보고 주체	Circle Internet Group, Inc. 경영진 주장 / Deloitte & Touche LLP의 examination
단위·범위	유통량 USDC / 준비자산 USD. 보고서 정의의 전체 승인 체인 및 자산 범위
분리한 기존 관찰	2026-11-13 Ethereum 블록 26,407,530. 다른 날짜·부분 체인 공급이므로 직접 분모로 사용하지 않음

증거 ID

ID	내용	이 문서의 상태
E-R01	S1 PDF 1~2쪽: 의견·경영진 주장·수량 정의	공개 문서 기재 확인
E-R02	S1 PDF 4~5쪽: 9월 말 준비자산 명세	공개 문서 기재 확인
E-R03	S1 PDF 6쪽: 제외 항목·시차 주석	공개 문서 기재 확인
E-R04	기존 원문 21~24쪽: 11월 RPC 관찰	기존 문서 인용 / 이번 재조회 없음
C-R01	80쪽 계산식	위 입력으로 산술 재계산

> S1은 특정 시점의 경영진 주장에 대한 제3자 examination이다. 이를 작성자의 독립 감사로 바꾸어 표현하지 않는다. 공식 PDF 원문은 웹 문서 열람으로 확인했으며 로컬 원본 파일 보관·해시는 확보하지 못했다. 상세 출처는 88쪽.

R-USDC-01-R · C-R01 / NUMERICAL REPERFORMANCE

USDC / 보고서 내부 수치를 재계산한다

기준: 2026-09-30 23:59 UTC · 보고서 표시 정수 기준. 독립 체인 집계나 원장 대사가 아니다.

유통량 조정 · E-R01	USDC
승인 체인 총공급량	75,866,964,179
차감: Tokens Allowed But Not Issued	(1,856,810,081)
차감: Access Denied Tokens	(131,245,845)
차감: Circle Gateway pending burns	(46,939)
재계산 유통량 = 보고서 유통량	73,878,861,314

준비자산 재집계 · E-R02	USD
펀드: 국채 + 환매조건부 거래 + 현금	25,361,578,416 + 36,654,000,000 + 1,003,847,741
펀드: 시차·결제 차이 순액	(552,000,382)
펀드 소계	62,467,425,775
기타: 국채 + 금융기관 현금 + 시차·결제 순액	1,757,678,272 + 9,502,194,346 + 229,389,308
기타 소계	11,489,261,926
재계산 준비자산 총계 = 보고서 총계	73,956,687,701

보고서상 차액 = USD 77,826,387
보고서 수치 기준 비율 = 100.1053%

차액 = 준비자산 - (유통량 × USD 1). 비율 = 준비자산 ÷ (유통량 × USD 1) × 100. 유통량·두 소계·총계의 재계산 차이는 모두 0이다. 반올림은 최종 비율 표시에서만 적용했다.

> FLOW의 폐기 체인 동결분 993,225 USDC는 주석상 유통량 제외 항목이다. 위 승인 체인 총공급량에서 다시 차감하지 않았다. 접근 제한분 제외를 법적 상환의무 소멸로 해석하지 않는다. [S1 PDF 2·6쪽]

R-USDC-01-R · F-02 / EVIDENCE LINKAGE

USDC / 주장별 증거 연결표

같은 문서의 일관성 확인과 서로 다른 자료의 실질적 연결을 구분한다.

주장 / 판단 ID	온체인 근거	오프체인·계산 근거	연결 상태와 결론
J-R01 공시 숫자의 산술 일관성	이번 전체 체인 조회 없음	E-R01·02 / C-R01	확정·문서 내부 한정. 유통량·준비자산 재계산 차이 0
J-R02 기준시각 공급·유통의 일치	E-R04는 11월 Ethereum 부분값	E-R01은 9월 전체 승인 체인 정의	유보. 시점·모집단 불일치. 동일 기준 체인별 재조회·조정 내역 필요
J-R03 준비자산 실재·권리·부담	체인 기록만으로 은행·펀드 권리 입증 불가	E-R02·03 및 E-R01의 제3자 의견	자체 독립 확인 유보. 은행·수탁 확인, 펀드 지분·권리 자료 필요
J-R04 총공급량 = 법적 상환의무	주소·잔액만으로 권리자 확정 불가	E-R01의 차감 정의	자동 등치 불가. 해당 관할·약관·권리자 유형·제한 효과 검토 필요
J-R05 보고일 이후 안정성·환금성	실시간 상태·흐름 미수집	과거 특정 시점 보고서	유보. 후속 잔액·상환 흐름·시장·신용·유동성 자료 필요

공통 식별자·변환

case_id=R-USDC-01-R / source=S1 / report_date=2026-09-30T23:59Z / currency=USD / unit=USDC. 숫자는 S1에서 전사한 표시값이다. 기존 블록 관찰은 E-R04로만 연결하며 같은 시점의 증거로 치환하지 않는다.

다음 조치

J-R02~05는 82쪽 F-05의 D-R01~05에 연결한다. 원자료를 받으면 같은 기준시각·모집단·정의로 다시 계산하고, 이전 판단과 변경 사유를 함께 남긴다.

> E-R01~03은 서로 독립된 세 출처가 아니라 같은 S1 보고서의 세 부분이다. 문서 내부 항목 간 일치를 독립 교차 검증으로 표시하지 않는다.

R-USDC-01-R · F-05 / EXCEPTIONS & FOLLOW-UP

USDC / 남은 차이를 조치로 연결한다

차이·질문	판단 영향	추가 자료 / 담당 역할 / 재검토 조건
D-R01 · 시점·모집단 11월 Ethereum ↔ 9월 승인 체인 전체	독립 준비율·유통량 대사 유보	체인 분석 담당: 체인·계약 목록, 기준시각 블록 매핑, 노드 응답·집계. 동일 시점 모집단 확보 시 J-R02 재검토
D-R02 · 유통 정의 미발행·접근 제한·소각 대기·폐기 체인	중복 차감·권리와 기술 상태 혼동 위험	발행 운영·법무: 조정별 주소·상태·약관·권리 근거. 조정 모집단 및 제외 사유 확인 시 J-R02·04 재검토
D-R03 · 준비자산 기초자료 공시 명세 ↔ 은행·수탁·내부 원장	실재성·권리·부담을 직접 확인 못함	재무·수탁 담당: 독립 확인, 계정 명세, 소유·보관·담보 문서. 적법한 접근권한과 기준일 일치 시 J-R03 재검토
D-R04 · 결제시차 순액 펀드 -552,000,382 / 기타 +229,389,308 USD	합산은 가능하나 개별 조정의 실재·기간귀속 미검증	재무·결제 담당: 건별 내역·원장·컷오프·후속 결제. 상계·중복·귀속 대조 후 J-R03 재검토
D-R05 · 후속 사건·실행 경로 보고일 이후 / 소스·키 운영	현재 지급능력·통제 효과성으로 확대 불가	리스크·기술·법무: 후속 흐름, 배포 대응, 권한 운영과 검토 기록. 자료와 평가 범위 확정 후 J-R05 재검토

상태·기한

모든 항목은 미해결 또는 외부자료 미확보 상태다. 담당은 실제 배정 인물이 아닌 필요한 역할을 나타낸다. 자료 요청·수령·완료일은 미정이며, 접근권한과 업무범위를 합의한 뒤 설정한다.

> 관찰된 차이를 곧바로 오류·부정·준비자산 부족으로 판단하지 않는다. 정당한 기준 차이인지, 자료 부족인지, 처리 오류인지 구분한 후 결론을 갱신한다.

R-USDC-01-R · F-04 / F-06 / CONCLUSION

USDC / 결론을 범위별로 종결한다

판단	결론 / 근거 / 한계
확정 · J-R01	전사한 S1 표시값을 기준으로 유통량 조정, 준비자산 소계·총계와 차액·비율을 산술 재현했다. 보고서 기초자료의 진실성은 자체 확인하지 않았다.
유보 · J-R02	보고서 기준시각의 전체 체인·조정 모집단을 독립 재구성하지 않았다. 기존 11월 Ethereum 관찰과의 실질적 대사 완료를 주장하지 않는다.
유보 · J-R03~05	준비자산 실재·권리·부담, 특정 보유자의 상환권, 후속 지급능력·통제 효과성에 대한 독립 결론을 내리지 않는다. F-05 후속 증거가 필요하다.

주장 → 사실 → 기준 → 판단 → 한계 → 조치

J-R01 → E-R01·02의 수치 → S1 정의와 표시단위 → C-R01 계산 일치 → 전사값·문서 내부 한정 → 독립 재현 요청. J-R02~05 → 현재 자료의 공백 → 같은 시점·주체·범위 원칙 → 유보 → D-R01~05에 따라 증거 확보 후 재검토.

수행 기록

- 수행: 공식 공개 문서 열람, 숫자 전사, 산식 실행, 차이 0 및 준비자산 초과액 확인, F-02·F-05·F-06 작성.
- 미수행: 독립 RPC 교차조회, 은행·수탁 확인, 내부 원장 대사, 소스-바이트코드 대응, 법적 권리 의견, 독립 검토자 재현.
- 재현 기준: 80쪽 입력·부호·수식을 동일하게 적용. 새로운 월 보고서로 숫자를 섞어 바꾸지 말고 별도 판본으로 실행.

> 완료 표시는 “공개보고서 내부 산술 검토 및 증거 공백 정리”에 한정한다. R-USDC-01 전체의 엔드투엔드 검증, 독립 보증 또는 현재 준비율 확인으로 표현하지 않는다.

S-KR-ISS-01 · F-01 / SYNTHETIC CASE

국내 발행통제 / 합성 사례의 범위

질문: 발행 승인·권리 원장·토큰 공급량의 차이는 어디서 발생했고, 어떤 결론까지 가능한가?

> 모든 기관명·거래·승인·원장·수량·권한 기록은 교육용 합성 입력 H다. 실제 금융회사나 계좌관리기관의 시스템·거래를 점검한 사례가 아니며, 실제 계약 배포·트랜잭션 실행·RPC 조회도 수행하지 않았다.

항목	고정한 가정
대상 / 작성·검토	가상 기관 A의 단일 토큰화 증권 클래스 / Vanzi / 독립 검토 미수행
가상 기준시각	2026-11-18 00:00 UTC. 모든 입력은 같은 시각 기준으로 가정
수량 단위	토큰 1개 = 승인된 권리 1단위라고 합성 계약에서 가정. 법적 효력에 관한 실제 판단 아님
대상 범위	생산망의 단일 클래스·단일 계약. 브리지·래핑·테스트망·부분권리·분할·통합은 없는 것으로 가정
전문 모듈 / FC	M5 통제·시스템 + M1 규제 질문 / FC-A01 발행·FC-C02 역할·FC-E01 변경
주요 주장	J-K01 수량 대사 / J-K02 승인과 실행 일치 / J-K03 권한통제 / J-K04 법적 권리 / J-K05 회계 영향

국내 제도와의 연결

금융위는 토큰증권 제도화 법률의 시행을 2027-02-04로 안내하고 있다(S2). 따라서 이 사례는 시행 준비를 위한 통제 설계 연습이다. 현행 의무 위반이나 미래 하위규정 준수를 판정한 사례로 사용하지 않는다.

실제 적용 시 적용 법률·시행일·최종 하위규정, 증권 종류, 계좌관리 방식과 기관 역할을 먼저 확정한다. 체인 공급량과 법적 발행잔액을 같은 개념으로 전제하지 않는다.

S-KR-ISS-01 · H-K01~04 / F-03 / CALCULATION

국내 발행통제 / 세 잔액을 대사한다

합성 입력 ID	사건 / 승인·원장·실행 연결	수량
H-K01	기초 권리 원장과 토큰 공급량 일치	1,000,000
H-K02-A / H-K04-A	승인 A / 원장 반영 / 토큰 발행. 같은 업무 ID로 대응	+150,000
H-K02-B / H-K04-B	승인 B / 원장 미반영 / 토큰 발행. 같은 업무 ID로 대응	+50,000
H-K04-X	권한 주소의 추가 발행 / 대응 승인·원장 없음	+50,000
H-K02-C / H-K04-C	적법한 소각·권리 감소를 가정 / 승인·원장·토큰 일치	-50,000

잔액	산식	결과
승인 기준 기대 권리잔액	1,000,000 + 200,000 - 50,000	1,150,000
실제 권리 원장 · 합성	1,000,000 + 150,000 - 50,000	1,100,000
토큰 공급량 · 합성	1,000,000 + 250,000 - 50,000	1,200,000

토큰 - 원장 = 100,000
= 원장 미반영 50,000 + 승인 미대응 50,000

J-K01: 위 고정 입력에서 차이의 산술 분해는 확정이다. 그러나 승인서가 없다는 관찰과 실제 승인 부재는 일반적으로 다르다. 이 사례에서는 제공된 승인 모집단이 완전하고 승인 X가 없다고 명시적으로 가정했다.

> 수량·거래 ID·기준시각·클래스가 일치한다는 전제하의 합성 계산이다. 실제 사례에서는 체인 이벤트 완전성, 실패·재조직·재발행, 원장 컷오프, 취소·소각 효력부터 검증해야 한다. 현재 차이를 즉시 법적 초과발행으로 단정하지 않는다.

S-KR-ISS-01 · F-02 / F-04 / SYNTHETIC INPUTS

국내 발행통제 / 증거와 권한을 연결한다

주장	온체인 측 합성 입력	오프체인 측 합성 입력	판단 / 상태
J-K01 수량	H-K04: 기초·발행 250,000·소각 50,000·기말	H-K01 원장 / H-K02 승인 목록	합성 입력 내 확정. 차이 100,000 = 50,000 + 50,000
J-K02 승인-실행	H-K04-A/B/C/X 거래 목록·업무 ID	H-K02-A/B/C 승인; X 없음	B는 원장 반영 누락, X는 승인 미대응 발행으로 분류. 모집단 완전성 가정 필요
J-K03 권한통제	H-K05: minter 단독 호출 가능, 가상 한도 300,000	H-K06: 모든 발행은 이중 승인 후 실행하도록 정한 가상 정책	기술 한도 미초과라도 내부 승인 일치가 보장되지는 않음. 통제 설계상 공백
J-K04 법적 권리	토큰 수량과 관리자 주소	H-K07: 1토큰=1권리 가정 외 실제 법률 자료 없음	실제 법적 초과발행·투자자 권리·대항력 판단 유보
J-K05 회계 영향	발행·소각 수량	실제 계약·발행대금·상환·총계정원장 없음	분개·손익·부채 금액 확정 유보. 수량 차이를 손실액으로 치환하지 않음

합성 권한 경로 / F-03

내부 승인자 2인 → 실행자 → minter 주소 → mint 호출 → 토큰 잔액. 권리 원장은 별도 반영 절차다. 가상 정책은 이중 승인을 요구하지만, H-K05에서는 minter가 단독 호출 가능하다고 가정했다. 키 소유자·위임·업그레이드 경로는 실제 자료가 없으므로 법적 책임자로 귀속시키지 않는다.

검증할 통제 질문

승인 ID가 실행 요청과 원장 기록에 동일하게 남는가? 중복·재시도가 차단되는가? 한도와 권한 변경에도 승인이 필요한가? 우회 경로·긴급 권한·업그레이드가 통제를 무력화하지 않는가?

> H-K01~07은 자료를 확보했다는 표시가 아니라 이 교육 사례에 부여한 입력·가정 ID다. 실제 관찰 사실 F나 고객자료 증거 ID로 재표기하지 않는다.

S-KR-ISS-01 · F-05 / F-06 / CLOSE-OUT

국내 발행통제 / 발견에서 조치까지

발견 / 영향	조치·담당 역할	재검토 / 종결 조건
D-K01 원장 미반영 50,000 원장·고객 권리잔액 왜곡 가능	원장 운영: 승인 B·결제·배분·컷오프 확인 후 정정 여부 결정	B의 중복·취소 여부 및 권리 유효성 확인. 정정 이력과 전후 대사 차이 보존
D-K02 승인 미대응 50,000 발행 통제 우회 가능	발행 통제·기술·법무: 사건 보존, 권한·키·대체 승인 조사, 필요 조치 검토	승인 모집단·위임·긴급 절차·테스트 여부 검증. 적법한 시정 조치·재대사
D-K03 minter 한도 내 단독 실행 수량 한도와 승인통제 불일치	통제 설계자: 승인-실행 연계·역할 분리·독립 대사·예외 경보 검토	정상·미승인·중복·우회·권한변경 시나리오 테스트와 독립 검토
D-K04 권리·회계 영향 미확정	법무·회계: 계약·등록·대금·고객원장·총계정원장 확보	권리자·의무·금액·시점·적용 기준 확정 후 법률·회계 결론 별도 작성

F-06 / 범위별 결론

합성 산술: 100,000 차이는 원장 반영 누락과 승인 미대응 발행으로 분해된다. 통제 설계: 합성 정책과 단독 실행 경로 사이에 공백이 있다. 실제 위법성·자산 손실·회계 오류 금액·통제 운영 효과성은 이 자료로 확정할 수 없다.

시정 후 기대치 · 실행 결과 아님

유효한 B 50,000을 원장에 반영하고 X 50,000을 적법하게 해소한다는 조건에서, 기대 권리·원장·공급은 각 1,150,000이 된다. X의 해소는 임의 소각 지시가 아니다. 권리·계약·적법 절차를 확인한 뒤 결정해야 한다.

> 이번 수행은 합성 입력의 계산·표 작성이다. 시스템 변경, 권한 회수, 소각, 원장 수정, 고객 통지 및 통제 테스트는 실제 수행하지 않았다. 담당·기한은 실제 업무 수임 시 배정한다.

CASE SUPPLEMENT · SOURCE REGISTER / 2026-11-18

출처·재현·개정 기록

S1 / USDC 공개 원문

Circle Transparency & Stability → 2026년 SEPT → USDC Examination Report, September 2026. 보고서 일자 2026-10-26 / 총 6쪽 / 열람 2026-11-18.

사용 위치: PDF 1쪽 제3자 의견, 2쪽 경영진 주장·유통량 정의, 4~5쪽 9월 말 준비자산, 6쪽 주석. 본 보완은 해당 공개 문서의 전사값을 사용했다. 로컬 다운로드는 접근 제한으로 완료하지 못했으므로 원본 바이트·해시·전자서명 검증 완료를 주장하지 않는다.

S2 / 국내 제도 배경

금융위원회, 민·관 합동 토큰증권 협의체 Kick-off 회의 개최, 2026-03-04. 토큰증권 제도화 법률 시행 예정일 2027-02-04와 분산원장을 이용한 계좌부 개념의 배경 자료. 열람 2026-11-18. 개별 조문·최종 하위규정의 준수 여부는 이 사례에서 판정하지 않았다.

재현 지침

- USDC: 동일 S1 판본의 9월 말 열만 전사한다. 괄호는 음수로 처리한다. 유통량 4항목, 준비자산 두 소계·총계, 차액·비율을 80쪽과 비교한다.
- 국내 합성: 85쪽 사건 A·B·X·C와 기초잔액으로 승인·원장·공급의 세 잔액을 별도 산출한다. 산술 일치와 가정의 타당성을 분리해 검토한다.
- 계산은 이번 문서 작성 중 실행해 확인했다. 제3자 독립 재현·검토는 미수행이며 검토자 서명은 없다.

개정 이력과 보존 범위

기준본: Chain_Prism_Enhanced.pdf, 77쪽 / Vanzi 표기 / 기존 가치평가 부록 포함. 24쪽 상태와 73·77쪽 수행 상태를 갱신하고, 78~88쪽을 추가했다. 목차·북마크·쪽번호와 양식 참조를 연결했다. 그 밖의 본문·FC·기존 사례·부록 내용은 유지했다.

> OCP v1.0 본문을 바탕으로 한 사례 보완판이다. 별도 저작권 변경등록이나 공개 홈페이지 반영은 수행하지 않았다.