Chain & Context

Chain Prism

디지털자산 거래 실질 통합 분석 프레임워크

ON/OFF-CHAIN PRISM · OCP v1.0

기술적 권한이 곧 권리나
통제를 뜻하지는 않는다

수록 USDC 공개보고서의 범위 한정 검토, DEMO-USD에서 판단이 수정되는 과정, 국내 발행통제 가상 사례, 그리고 작성 양식·검증 패턴·기능 카드를 담은 실무 도구집



사례 보완판
2026년 11월

Vanzi

발행 정보와 이용 범위

제목	Chain Prism: 디지털자산 거래 실질 통합 분석 프레임워크
방법론	On/Off-Chain Prism(OCP) v1.0
판	사례 보완판 · 2026-11-18 (최초 작성 2026-11-14) · 2026년 11월 편집 개정
저자	Vanzi
발행	Chain & Context
자료 확인일	본문과 각주에 개별 표기
구성	제1편 연구 보고서 · 제2편 실무 도구집 합본

이 보고서가 다루는 범위

이 보고서는 디지털자산 거래의 코드·거래·계약·원장을 연결해 질문을 정하고, 근거와 판단을 기록하는 분석 방법론을 제시한다. 회계·준법·AML·IT감사 실무자의 학습과 적용을 위해 작성되었다.

수록 사례는 성격이 서로 다르다. USDC 사례는 고정 블록의 단일 공개 RPC 응답과 공식 참고 자료, 그리고 2026년 9월 공개 준비자산 보고서의 수치 재계산에 기초한 실제 공개자료 사례다. 배포 소스 대응, 내부 운영, 준비자산의 원장 대사는 남은 과제로 표시했다. 건물 RWA, DEMO-USD, 회계 시범 사례, 국내 발행통제 사례는 분석 순서를 보여주기 위해 만든 교육용 가상 사례이며, 가상 자료 안의 관찰·추론과 실제 사실을 구분해 서술한다.

이용상 유의사항

이 프레임워크를 사용한다는 사실 자체가 공식 의견, 보증, 보안감사의 결론을 뜻하지 않는다. 이 보고서의 내용은 실제 보증업무·법률 의견·회계감사 결과로 사용할 수 없으며, 특정 상품의 가격이나 권리에 대한 의견도 아니다. 관할·회계기준·정책·기준일이 필요한 전문 판단은 그 조건을 지정해 별도로 수행해야 한다. 고객 업무에 적용할 때에는 목적·기준·권한·모집단·검토 책임을 별도로 확정해야 한다.

공개자료 수집·재조회 스크립트는 USDC 착수팩으로 제공된다. 자동 귀속, 회계 판단, 계정 매핑, 자동 전기 엔진은 구현되지 않았다. 이번 사례 보완은 OCP v1.0의 등록 판본이나 등록 범위가 이 내용까지 갱신되었다고 주장하지 않는다.

함께 제공되는 자료

작성 양식(F-01~F-06), 증거 연결표, 검증 패턴(RF), 기능 카드(FC)는 제2편 『실무 도구집』에 수록한다. 본문에서는 해당 도구를 이름과 번호로 참조한다.

Preface

머리말

디지털자산 거래를 이해하려면 서로 다른 언어로 쓰인 기록을 함께 읽어야 합니다. 코드는 실행 조건을, 블록체인은 거래와 상태의 변화를, 계약은 당사자의 권리와 의무를, 장부는 경제적 사건을 기록합니다. 각 기록은 중요한 사실을 담고 있지만, 어느 하나만으로 거래 전체를 설명하기는 어렵습니다.

관리자 권한을 가진 주소를 찾았다고 해서 그 권한을 실제로 행사하는 주체까지 확인한 것은 아닙니다. 토큰이 이전되었다고 해서 자산이 매각된 것은 아니며, 준비자산의 총액이 유통량을 웃돈다고 해서 보유자의 상환권과 지급 가능성까지 확인되는 것도 아닙니다. 판단에 필요한 연결은 기록과 기록 사이에 남아 있습니다.

Chain Prism은 '그 연결을 어떻게 확인하고 기록할 것인가'라는 질문에서 출발했습니다. 온체인에서 관찰한 사실을 계약과 원장에 대조하고, 기술적 권한을 권리·통제·경제적 귀속과 구분하며, 확보한 근거가 어느 범위의 판단을 뒷받침하는지 설명하는 작업 체계를 만들고자 했습니다. 회계와 감사의 시각에서 디지털자산 거래를 읽으며 생긴 질문들이 이 작업의 출발점이 되었습니다.

이 책에서 중요하게 다루는 것은 결론에 도달하는 과정입니다. 처음에는 타당해 보였던 해석도 추가 자료에 따라 달라질 수 있습니다. 서로 맞는 숫자가 서로 다른 대상을 가리킬 수도 있고, 설명되지 않는 차이가 질문을 다시 정하게 만들 수도 있습니다. 그러므로 무엇을 확인했는지와 함께 무엇이 남아 있는지, 어떤 자료가 들어오면 판단을 바꿔야 하는지도 기록해야 합니다.

제1편 연구 보고서에는 이러한 관점을 적용하는 절차와 사례를 담았고, 제2편 실무 도구집에는 질문과 근거를 정리할 양식, 검증 패턴, 기능 카드를 모았습니다. 실제 공개자료를 검토한 사례와 교육용 가상 사례는 구분했습니다. 독자는 자신의 목적에 맞는 질문에서 시작해 필요한 도구를 선택하고, 자료가 허용하는 범위까지 분석을 이어갈 수 있습니다.

Chain Prism 역시 적용과 검토를 통해 다듬어져야 합니다. 새로운 거래구조, 코드의 변경, 반례와 재현 결과는 이 책의 질문과 절차를 수정하는 근거가 될 것입니다. 이 책이 디지털자산을 검토하는 실무자와 학습자에게, 서로 다른 기록을 연결하고 그 판단을 다른 사람에게 설명할 수 있는 출발점이 되기를 바랍니다.

2026년 11월

Vanzi

Chain & Context

Contents

목차

머리말 · Executive Summary

이 보고서를 읽는 법

제1부 분석 방법론

1.1 하나의 거래 질문에서 출발하는 분석 체계
1.2 실행 절차: 판단이 막힌 곳에서 되돌아간다
1.3 1단계 · 질문: 분석은 코드가 아니라 질문에서 시작한다
1.4 2단계 · 증거: 자료의 양보다 질문과의 적합성
1.5 온·오프체인 증거의 연결
1.6 3단계 · 구조와 귀속: 권한, 권리, 통제, 귀속은 서로 다른 주장이다
1.7 4단계 · 전문 판단: 과세와 과세정보 보고를 나누어 묻는다
1.8 5단계 · 정합성: 대사는 숫자의 일치에서 끝나지 않는다
1.9 6단계 · 결론: 근거와 다음 행동이 분명한 결론

제2부 도구 통합과 증거 처리

2.1 OCP는 도구의 결과를 증거로 바꾸는 계층이다
2.2 도구는 확인할 질문에서 고른다
2.3 공통 입력 양식
2.4 “표시되었다”와 “실제로 그렇다”의 구분
2.5 수용 전 확인과 도구 간 충돌
2.6 실행과 재현의 기록

제3부 실증 사례

3.1 USDC: 실제 공개자료에 대한 부분 적용 실제
3.2 건물 RWA: 자산 가치와 권리 가치 가상 25~28쪽
3.3 DEMO-USD: 106%에서 100%로, 판단이 수정되는 과정 가상 29~34쪽
3.4 국내 발행통제: 승인·원장·공급량의 차이 가상 84~87쪽

제4부 거래 실질에서 회계까지

4.1 동작에서 회계까지: transfer 기록만으로는 사건을 알 수 없다
4.2 거래는 이름이 아니라 변화로 분류한다
4.3 권리·의무 구조의 비교
4.4 생애주기: 상태 전환과 회계 사건의 분리
4.5 통제 테스트: 존재·설계·운영 효과성
4.6 회계 판단에서 계정 매핑까지
4.7~4.9 시범: 자기 지갑 이전 · 발행·상환 · RWA 채권 가상

제5부 적용 범위, 한계와 후속 과제

5.1 현재 상태: 명세가 자세하다고 엔진이 실행된 것은 아니다
5.2 ‘완료’는 어디까지 말할 수 있는가
5.3 후속 과제: 발전은 분량이 아니라 적용 결과로 결정한다

부록 명세와 출처

A 회계 규칙·계정 명세 · B RWA 가치평가 연결표 · C 주장별 증거 판정 · D 출처·재현·개정 기록

제2편 실무 도구집 T1 작성 양식 · T2 작성 예시 · T3 검증 패턴 · T4 기능 카드

Executive Summary

기술적 권한이 곧 권리나 통제를 뜻하지는 않는다. 둘을 잇는 증거는 따로 확인해야 한다

디지털자산 거래를 분석할 때 코드와 거래 기록, 계약, 원장은 서로 다른 곳에 흩어져 있다. Chain Prism은 이 자료들을 하나의 질문 아래 연결하고, 확인된 사실과 추론과 가정을 끝까지 구분해 기록하는 분석 체계다.

문제의식

스마트컨트랙트에 기록된 관리자 주소는 특정 기능을 실행할 수 있다는 사실을 보여준다. 그러나 그 주소를 누가 실제로 운영하는지, 그 권한 행사가 누구의 의사결정이며 경제적 책임이 누구에게 귀속되는지는 코드만으로 알 수 없다. 키 보유나 기술적 권한을 소유권, 회계상 통제, 조세상 귀속으로 자동 전환하는 순간 분석은 사실이 아니라 추정 위에 서게 된다. 마찬가지로 문서에 상환권이 적혀 있다는 사실과 실제로 상환이 이행되었다는 사실, 소스코드를 확인했다는 사실과 그 코드가 안전하다는 사실은 서로 다른 주장이다.

Chain Prism의 접근

분석은 기술 용어가 아니라 하나의 거래 질문에서 출발한다. '이 토큰의 보유자는 누구에게 무엇을 청구할 수 있는가'와 같은 질문을 먼저 고정한 뒤, 범위 설정부터 종합 판단까지 여섯 단계를 거친다. 검토 관점은 규제·AML, 회계·감사·보증, 조세·과세정보 보고, 거래구조화·가치평가, IT감사·기술 리스크의 다섯 모듈 가운데 질문에 필요한 것만 고른다.

이 과정에는 세 가지 규칙이 고정되어 있다. 첫째, 관찰 사실(F), 추론(I), 가정(H)을 나누고 해석과 결론은 별도로 쓴다. 둘째, 권한과 권리를 나눈다. 셋째, 질문 → 사실 → 기준 → 판단 → 한계 → 다음 조치의 순서로 결론과 근거를 연결한다. 핵심 사실이 없으면 결론을 강행하지 않고 자료 보완, 조건부 분석, 결론 유보 가운데 하나를 택한다.

사례가 보여주는 것

1 USDC: 확인한 범위와 확인하지 않은 범위를 함께 고정했다 실제 사례

첫 실제 적용은 모든 기능을 완결하기보다 어디까지 확인했는지를 고정하는 데 초점을 두었다. Ethereum 메인넷의 native USDC를 기준 블록 26,407,530(2026-11-13 17:26:47 UTC)에서 단일 공개 RPC로 조회했고, 이후 2026년 9월 공개 준비자산 보고서의 유통량과 준비자산을 재계산했다. 보고서 내부의 유통량, 두 소계, 총계에는 재계산 차이가 없었으며, 보고서 수치 기준 비율은 100.1053%다. 이 비율이 무엇을 뜻하는지는 정확히 읽어야 한다. 100.1053%는 보고서가 스스로 제시한 준비자산을 같은 보고서의 유통량으로 나눈 값으로, 보고서 안의 정의와 수치가 서로 맞는다는 것을 보여줄 뿐이다. 11월에 조회한 Ethereum 공급량으로 9월의 전체 준비자산을 나눈 비율이 아니며, 준비자산 전체의 대사나 독립적인 보증이 완료되었다는 뜻도 아니다. 독립적인 체인 집계, 은행·수탁 원장 대사, 배포 소스와 바이트코드의 대응, 키 운영 확인은 여전히 남은 과제다.

2 DEMO-USD: 비율보다 분자와 분모의 범위가 판단을 바꾼다 가상

최초 보고서는 은행잔액 1,230만 달러와 상환의무 1,160만 달러로 약 106%를 제시했다. 추가 자료에서 은행잔액 가운데 30만 달러가 회사 운영계좌였고, 상환 신청 40만은 지급 전 대기 상태로 청구권이 존속한다는 사실이 드러났다. 범위를 바로잡으면 준비자산과 상환의무는 모두 1,200만 달러로 100%가

된다. 이 사례가 보여주는 것은 숫자의 크기가 아니라 조정 이유를 설명할 수 있는지이며, 통제 효과성은 추가 자료 이후에도 유보했다.

3 국내 발행통제: 같은 차이도 원인을 나누면 조치가 달라진다 가상

가상 기관의 승인 기록, 권리 원장, 토큰 공급량 사이의 100,000 차이를 원장 미반영 50,000과 승인에 대응하지 않는 발행 50,000으로 분해했다. 가상 정책과 단독 실행 경로 사이의 통제 설계 공백도 식별했다. 그러나 실제 위법성, 자산 손실, 회계 오류 금액, 통제 운영 효과성은 이 자료로 확정할 수 없다. 금융위원회가 안내한 토큰증권 제도화 법률의 시행일(2027-02-04)을 앞둔 통제 설계 연습으로 읽어야 한다.

4 건물 RWA: 자산의 가치와 토큰이 담은 권리의 가치는 다르다 가상

가치 100억 원의 건물에 차입금 40억 원이 있고 60만 개의 토큰이 잔여가치에 비례해 참여한다고 가정하면 단위당 기준값은 1만 원이다. 건물 가치가 80억 원이 되면 약 6,667원으로 떨어지고, 권리 구조를 담보부 채권형으로 바꾸면 같은 계산식을 더 이상 쓸 수 없다. 단위당 값은 가정하의 단순 계산이며 실제 발행가격이나 공정가치와 같다고 볼 수 없다.

한계와 활용

이 보고서의 결론은 명시한 입력과 범위 안에서만 성립한다. 독립 검토자의 재현은 수행되지 않았고, 가상 사례는 실제 기관의 거래나 시스템을 검사한 결과가 아니다. 실무자는 제1부의 절차와 제2편 실무 도구집의 양식을 이용해 자신의 사례에서 질문, 증거, 판단, 한계를 같은 형식으로 남길 수 있다. 후속 과제와 미검증 영역은 제5부에 정리했다.

이 보고서를 읽는 법

모든 결론에는 자료의 성격과 판단의 상태가 함께 붙는다

이 보고서는 처음부터 모든 전문 판단을 수행하도록 요구하지 않는다. 분석할 거래와 질문을 고르고, 확보한 자료가 무엇을 보여주는지 정리한 뒤, 필요한 검토 관점만 선택하면 된다.

독자가 가장 먼저 확인해야 할 것은 지금 읽는 내용이 어떤 자료에 근거하고, 무엇을 실제로 수행했는지다. 이 보고서는 이를 세 개의 축으로 나누어 각 사례와 카드의 첫머리에 표시했다(도표 0-1). 자료 성격은 실제 공개자료, 교육 목적의 가상 자료, 참고 코드와 표준을 구분한다. 카드 상태는 질문 도구가 얼마나 다듬어졌는지를, 수행 범위는 공개 RPC 읽기인지 서술과 계산인지 질문 명세에 그쳤는지를 나타낸다. 세 축은 서로 독립적이므로 '미검증'이라는 하나의 상태로 합치지 않는다.

도표 0-1 자료와 수행을 표시하는 세 개의 축

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

자료: Chain Prism 사례 보완판(2026-11-18) 세 축 배지 안내. 원본의 '합성' 표기는 이 판에서 '가상'으로 바꾸었다.

두 번째로 확인할 것은 판단의 상태다. 같은 '결론'이라도 성립하는 조건이 다르기 때문이다(도표 0-2). 판단 상태는 자료 성격과 다른 질문에 답한다. 가상 자료 안에서도 계산은 '확정·범위 한정'일 수 있지만, 그 확정은 가상 입력의 범위를 넘지 않는다. 이와 함께 본문에서는 개별 주장마다 관찰 사실(F), 추론(I), 가정(H)을 구분한다. 예컨대 가상 자료에 어떤 수량이 기재되어 있다는 진술은 그 자료 안의 관찰일 뿐, 그 수량이 실제 체인에서 확인되었다는 뜻이 아니다. 실제 공개 사례에서도 도구가 표시한 라벨(F)과 실제 주체에 대한 귀속(I)은 나누어 적는다.

도표 0-2 판단 상태의 세 가지 표시

표시	의미
확정 · 범위 한정	명시한 입력과 범위 안에서 근거와 계산이 맞는다.
조건부	가정이 유지되거나 추가 조건이 충족될 때만 성립한다.
유보	필요한 증거가 없어 결론에 도달하지 않았다.

자료: Chain Prism 사례 보완판(2026-11-18).

본문에는 여러 식별자가 등장한다. 전문 검토 관점(M1~M5), 작성 양식(F-01~F-06), 기능 카드(FC), 검증 패턴(RF), 사례(R-USDC는 실제 공개 사례, V는 가상 사례군), 자료와 판단 기록(D, I, H), 출처(S) 등이다. 이 식별자는 새로운 개념이 아니라 결론에서 원자료와 판단 기록으로 되돌아가기 위한 주소다. 본문은 이름으로 읽으면 되며, 식별자는 각주와 도표 출처에 두었다. 전체 식별자 체계는 부록 D의 도표 D-1에 정리했다.

읽는 순서는 독자의 목적에 따라 달라진다. 방법론의 전체 흐름이 궁금하다면 제1부부터, 실제 적용 결과가 궁금하다면 제3부의 USDC 사례부터 읽어도 된다. 직접 분석을 수행하려는 실무자는 제1부와 제2편 실무 도구집을 함께 보고, 구현을 준비하는 독자는 부록의 개발·운영 명세를 추가로 참고하면 된다.

제1부 · 01 분석 체계

분석은 하나의 거래 질문에서 출발하고, 필요한 관점만 골라 쓴다

Chain Prism은 여러 도구와 자료의 결과를 증거로 정리해 전문 판단을 지원하는 작업 체계다. 방법론, 작업 순서, 전문 모듈, 기록 양식은 같은 분석을 서로 다른 각도에서 정리한 것이다.

OCP의 출발점은 복잡한 기술 용어가 아니라 하나의 거래 질문이다. 예를 들어 '토큰을 보유하면 누구에게 무엇을 청구할 수 있는가'를 정한 뒤, 코드·거래·계약에서 그 답의 근거를 찾는다. 분석에 들어가는 것은 판단할 질문과 대상 거래·상품·사업이고, 처리 과정은 증거 확보, 구조 복원, 전문 분야별 판단, 대조로 이어지며, 결과물은 결론과 그 조건·한계·추가 조치, 그리고 다른 사람이 다시 확인할 수 있는 재현 자료다. 앞의 Executive Summary에서 설명한 세 가지 규칙은 이 질문이 분석 과정에서 다른 주장으로 바뀌지 않도록 붙잡아 두는 장치다.

이 체계를 이루는 요소의 역할은 서로 다르다. OCP는 온·오프체인 증거를 전문 판단으로 연결하는 전체 방법론이고, 여섯 단계(범위 → 증거 → 구조 → 판단 → 정합성 → 결론)는 지금 무엇을 해야 하는지 알려주는 작업 순서다. 전문 모듈 M1~M5는 어떤 기준으로 볼지를 정하고(도표 1-1), 작성 양식 F-01~F-06은 각 단계에서 무엇을 남길지를 정한다. 기능 카드(FC)는 동작별 질문을, 검증 패턴(RF)은 징후별 검증 방법을 이 흐름에 공급한다. 따라서 모든 도구를 한꺼번에 적용할 필요는 없다. 도구가 내놓은 결과는 입력 명세로 받아 이 작업 순서와 모듈에 연결하며, 거래·권리·상태·통제·회계를 잇는 내용은 제4부에서, 구현 상세는 부록에서 다룬다.

도표 1-1 다섯 개의 전문 검토 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

자료: Chain Prism OCP v1.0.

보고서의 도식도 같은 원칙을 따른다. 적합한 증거로 뒷받침된 관계는 실선과 증거 식별자로, 추론했거나 확인하지 못한 관계는 점선과 I 표시로, 가정·스트레스·대안으로 바꾼 관계는 별도 색상과 H 표시로 그린다. 화살표에는 자금 이동, 권리 이전, 권한 행사, 분석 순서 가운데 무엇을 뜻하는지 이름을 붙인다. 색상만으로 의미를 구분하지 않으며, 절차도의 화살표는 작업 순서를 뜻한다.

제1부 · 02 실행 절차

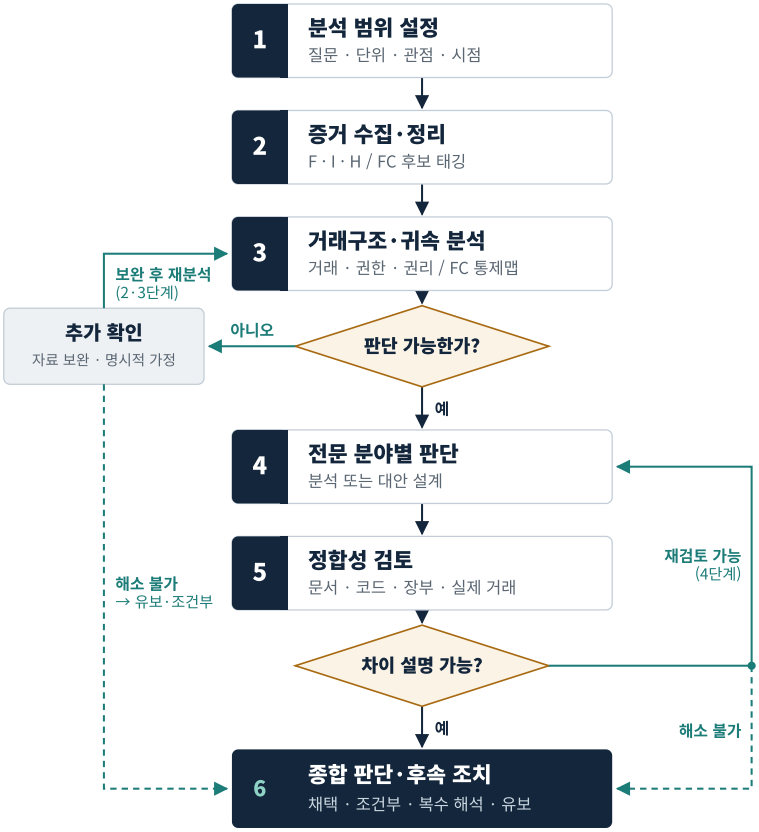
분석은 직선이 아니라, 판단이 막힌 곳에서 되돌아가는 절차다

Chain Prism은 여섯 단계로 진행되지만, 각 단계는 한 번 통과하면 끝나는 관문이 아니다. 두 개의 판단 지점에서 분석은 앞 단계로 돌아가거나, 명시적 가정 아래 조건부로 나아가거나, 유보로 종료된다.

분석은 범위를 정하는 데서 시작한다. 질문과 분석 단위, 관점, 기준시점을 정한 뒤(1단계) 증거를 모아 정리하고(2단계), 그 증거로 거래구조와 귀속 관계를 복원한다(3단계). 이후 전문 분야별로 판단하고(4단계), 그 판단을 문서·코드·장부·실제 거래와 대조해 정합성을 검토한 다음(5단계), 종합 판단과 후속 조치로 마무리한다(6단계).

그러나 앞 단계의 결론은 뒤 단계에서 흔들릴 수 있다. 거래구조를 복원하는 도중 당사자를 확인하지 못하는 일도 있고, 정합성 검토에서 앞선 판단과 어긋나는 차이가 드러나는 일도 있다. 그래서 이 절차에는 분석이 되돌아갈 수 있는 두 개의 판단 지점을 두었다.

도표 1-2 Chain Prism 실행 절차와 재검토 경로



실선은 기본 경로, 청록 실선은 되돌아가는 경로, 점선은 해소되지 않은 쟁점을 안고 종합 판단으로 넘어가는 경로다. 자료: Chain Prism OCP v1.0.

첫 번째 판단 지점은 거래구조와 귀속을 분석한 직후다. 이 단계에서 판단이 가능하지 않다면 분석은 전문 판단으로 넘어가지 않고 추가 확인으로 향한다. 자료를 보완할 수 있으면 증거 수집과 구조 분석(2~3단계)을

다시 수행하고, 보완이 어렵다면 명시적 가정을 세워 그 가정 아래에서 분석 가능한 부분만 조건부로 진행한다. 추가 확인으로도 해결할 수 없는 쟁점은 유보한다.

두 번째 판단 지점은 정합성 검토 직후다. 발견된 차이가 해석의 문제라면 전문 분야별 판단(4단계)으로 돌아가 다시 검토한다. 해석을 고쳐도 해소되지 않는 차이는 덮지 않고 종합 판단으로 가져가, 채택·조건부·복수 해석·유보 가운데 하나로 결론을 정리한다. 이렇게 되돌아간 이유와 보완한 자료를 함께 기록하면, 최종 결론뿐 아니라 판단이 달라진 과정까지 설명할 수 있다.

제1부 · 1단계 질문

분석은 코드가 아니라 질문에서 시작한다

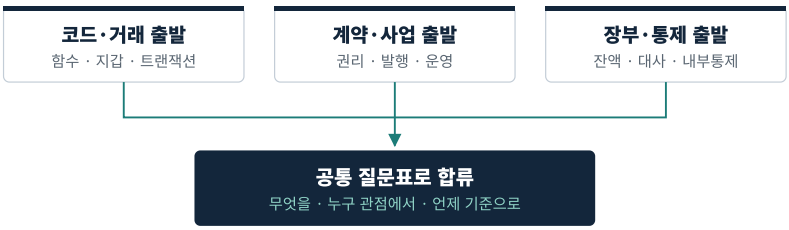
같은 스마트컨트랙트라도 무엇을 묻느냐에 따라 필요한 자료가 달라진다. Chain Prism은 코드를 읽기 전에 질문, 관점, 기준시점부터 고정한다.

모든 사례가 코드에서 시작할 필요는 없다. 투자자의 권리를 설명하려는 분석과 운영자의 권한을 점검하려는 분석은 같은 컨트랙트를 대상으로 하더라도 서로 다른 자료를 요구한다. 그래서 Chain Prism은 코드부터 읽기보다, 무엇을 누구의 관점에서 어느 시점을 기준으로 판단할지를 먼저 정한다.

질문이 범위를 결정하는 방식은 상환 가능성 분석에서 잘 드러난다. 상환 함수가 존재한다는 사실만으로는 보유자가 실제로 상환받을 수 있는지 답할 수 없다. 누가 청구할 수 있는지, 어떤 자산으로 언제 지급되는지, 청구권을 제한하는 조건이 무엇인지까지 범위에 넣어야 비로소 질문에 답할 수 있다. 반대로 단순한 수량 대사가 목적이라면 이 모든 전문 판단을 한 번에 끝내려 할 필요는 없다.

분석의 출발점은 사례마다 다르다. 함수·지갑·트랜잭션 같은 코드와 거래 기록에서 시작하는 분석이 있고, 권리·발행·운영을 정한 계약과 사업 구조에서 시작하는 분석이 있으며, 잔액·대사·내부통제 같은 장부와 통제 자료에서 시작하는 분석도 있다. 출발점이 어디든 표준·사례·전문 기준은 하나의 공통 질문표로 모인다(도표 1-3).

도표 1-3 세 가지 출발점과 공통 질문표



표준·사례·전문 기준을 질문으로 모으는 순서. 자료: Chain Prism OCP v1.0.

이 질문표가 1단계의 산출물인 분석 범위·질문표(F-01)다.[1] F-01은 다섯 가지를 고정한다. 첫째는 판단할 질문으로, 예컨대 '이 토큰의 보유자는 누구에게 무엇을 청구할 수 있는가'와 같은 형태다. 둘째는 분석 단위와 관점이다. 거래 1건, 상품 1개, 사업자 전체 가운데 무엇을 대상으로 삼고, 투자자·발행자·수탁자 가운데 누구의 입장에서 볼지를 정한다. 셋째는 관할권, 대상기간, 기준일, 기준 블록이다. 넷째는 적용할 전문 모듈로, 규제·AML, 회계·감사·보증, 조세·과세정보 보고, 거래구조화·가치평가, IT 감사 가운데에서 고른다. 다섯째는 종료

기준이다. 중요 질문에 어디까지, 언제까지 답할지를 정해 두고, 끝내 해결되지 않는 질문은 조건부 판단·복수 해석·유보로 종료할 수 있게 한다.

범위를 좁히는 일은 분석을 가능하게 하지만, 동시에 범위 밖으로 밀려난 자료를 보이지 않게 만들 위험도 있다. 범위를 좁히는 일이 자료 누락을 숨기는 일이 되지 않도록, F-01에는 포함한 항목뿐 아니라 제외한 항목도 기록한다. 기준 사례와 변경할 가정 역시 이 단계에서 구분해 둔다.

1 작성 양식 F-01(분석 범위·질문표). 고정 항목은 판단 질문, 대상·관점, 범위·시점, 모듈 선택, 종료 기준의 다섯 가지다.

제1부 · 2단계 증거

증거는 양이 아니라 질문과의 적합성으로 평가한다

자료를 모으는 단계의 핵심은 관찰한 내용과 그 의미에 대한 설명을 나누는 것이다. 어떤 자료가 무엇을 직접 보여주고, 어디서부터 추론이나 가정이 시작되는지를 처음부터 표시한다.

증거는 두 영역에서 나온다. 온체인 증거는 코드, 상태, 이벤트, 실행 추적, 권한, 거래이고, 오프체인 증거는 계약, 공시, 원장, 은행·수탁 자료, 운영 기록이다. 어느 쪽이든 자료의 양보다 판단 질문을 뒷받침하는 적합성이 중요하다. 도구가 특정 주소에 라벨을 표시했다는 기록은 남길 수 있지만, 그 주소의 실제 통제자가 누구인지는 별도의 근거가 필요하다.

그래서 Chain Prism은 모든 주장에 성격을 표시한다(도표 1-5). 이 분류는 자료를 버리기 위한 등급표가 아니라, 후속 확인이 필요한 연결을 드러내는 방식이다. 공개되지 않은 내부 원장을 학습용 숫자로 보완했다면 그 숫자는 가정(H)으로 남는다. 나중에 공식 자료를 받아 같은 값이 확인되더라도 가정을 사실로 소급해 바꾸지 않고, 새 자료와 확인 과정을 추가로 기록한다. 그래야 분석 당시 무엇을 알고 있었고 무엇을 예상했는지 구분할 수 있다.

가상의 예로 설명하면 이렇다. 분석 시점에 내부 원장을 받지 못해 어떤 계좌의 잔액을 학습용 숫자로 가정하고 판단을 진행했다고 하자. 몇 주 뒤 공식 원장을 받아 보니 같은 숫자가 확인되었다. 이때 처음의 기록을 '사실(F)'로 고쳐 쓰면, 분석 당시에는 그 값을 확인하지 못한 채 판단했다는 사실이 기록에서 사라진다. 그러면 나중에 검토하는 사람은 당시의 판단이 확인된 근거 위에서 내려진 것으로 오해하게 된다. 그래서 원래의 가정(H) 기록은 그대로 두고, 공식 원장을 새 증거로 추가해 두 기록을 연결한다.

도표 1-5 주장의 세 가지 성격

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

자료: Chain Prism OCP v1.0.

자료가 부족할 때의 선택지도 미리 정해 둔다. 자료를 추가로 확보할 수 있다면 요청하거나 다시 수집한다. 확보는 어렵지만 가정을 세워 분석할 수 있다면 그 가정을 명시하고 민감도를 함께 보인다. 핵심 판단 자체가

불가능하다면 결론을 유보하고 한계를 보고한다. 이 단계에서 특히 구분해야 할 것은 문서에 상환권이 적혀 있다는 사실과 실제로 상환이 이행되었다는 사실, 그리고 소스코드를 검증했다는 사실과 코드의 안전성을 검증했다는 사실이다.

2단계의 산출물은 증거·가정 목록과 공통 입력 명세(F-02)다.[1] 여기에는 원본, 출처, 시점, 변환 이력, F/I/H 구분, 수용 상태를 남기고, 기능 카드 후보를 태깅해 주장·범위·확인 상태를 함께 기록한다.

1 작성 양식 F-02(증거·가정 목록). 제2편 실무 도구집 T1.2 수록.

제1부 · 증거 연결

두 영역에 자료가 있다는 것과, 두 자료가 같은 거래를 가리킨다는 것은 다르다

온체인 기록과 계약이 각각 존재해도, 둘이 같은 거래를 가리킨다는 연결은 따로 확인해야 한다. 온·오프체인 증거 연결표는 핵심 질문에서 출발해 두 영역의 확인 사항을 대사하고, 발견과 조치로 이어지는 도구다.

금액이 비슷하다는 이유만으로 온체인 기록과 오프체인 자료를 대응시켜서는 안 된다. 대상, 시점, 당사자, 단위를 먼저 맞춰야 한다. 대사에서 차이가 나면 먼저 단위, 기준시간, 포함 범위를 확인한다. 발행량은 토큰 수량인데 입금액에는 수수료가 포함되어 있을 수 있고, 한쪽은 요청 시점이고 다른 쪽은 지급 시점일 수 있다. 차이를 설명하는 조정 항목이 확인되면 원래 수치와 조정 후 수치를 모두 남겨 계산의 경로를 보여준다.

도표 1-6 판단 요소별 온·오프체인 확인과 연결 방법

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-승인자를 연결하고 실제 실행과 승인 기록을 대사
상환 처리와 의무	잠금, 이전, 소각, 총공급량	청구권, 요청 상태, 지급완료, 원장	요청 ID별로 지급·소각·의무 잔액을 시점 대사
준비자산과 부채 범위	공급량, 관련 지갑, 기준 블록	은행·수탁, 명의, 담보, 제약, 보고 범위	분자와 분모의 주체·대상·시점을 맞춰 계산
RWA의 권리 연결	보유, 이전, 자격, 분배 로직	기초자산, 계약, 신탁, 명부, 집행 조건	토큰 단위와 청구권을 연결하고 이전 요건을 비교

자료: Chain Prism OCP v1.0.

연결의 상태는 결론과 별도로 기록한다. 어떤 주장에 맞는 증거로 각 영역의 항목을 확인했다면 '온체인 확인' 또는 '오프체인 확인'으로, 두 영역에서 확인한 대상이 같은 주체·권리·거래·시점임을 뒷받침했다면 '연결 확인'으로 표시한다. 남은 연결은 추론이나 가정으로 표시하거나 '연결 미확인', '비적용'으로 그 사유를 남긴다. 이렇게 하면 증거가 있는 부분과 해석에 의존하는 부분이 연결표 위에서 드러난다.

이 가운데 가장 혼동하기 쉬운 것이 '확인'과 '연결 확인'의 차이다. '온체인 확인'과 '오프체인 확인'은 각 영역 안에서 해당 항목이 확인되었다는 뜻일 뿐이다. 예를 들어 온체인에서 발행 권한을 가진 주소를 확인하고, 오프체인에서 서명자 명부를 확인했다고 하자. 두 항목은 각각 확인되었지만, 그 명부에 적힌 서명자가 바로 그

주소의 키를 실제로 운영한다는 사실은 아직 확인되지 않았다. 주소와 키와 승인자를 잇는 이 마지막 연결이 증거로 뒷받침될 때 비로소 '연결 확인'이 된다. 그 전까지 두 자료를 이어 붙인 결론은 추론(I)으로 남는다.

모든 질문에 온체인 증거가 필요한 것은 아니다. 질문에 온체인 증거가 필요하지 않다면 오프체인 증거만으로 평가하고 비적용 이유를 남긴다. 다만 양쪽 자료가 모두 존재한다는 것과 두 자료가 서로 연결된다는 것은 별개의 사실이라는 점을 끝까지 유지해야 한다.

제1부 · 3단계 구조와 귀속

기술적 권한, 법적 권리, 회계상 통제, 경제적 귀속은 서로 다른 주장이다

3단계에서는 거래구조를 복원하고 그 구조 안의 당사자에게 무엇이 귀속되는지를 판단한다. 이 단계에서 가장 흔한 오류는 한 종류의 증거로 다른 종류의 주장을 확정하는 것이다.

어떤 주소가 토큰을 발행할 수 있다는 사실은 기술적 권한에 관한 주장이다. 그 주소를 운영하는 회사가 토큰 보유자에게 상환의무를 진다는 것은 법적 권리에 관한 주장이고, 그 회사가 관련 자산을 재무제표에 인식해야 한다는 것은 회계상 통제에 관한 주장이며, 그 거래에서 생긴 이익이 누구에게 과세되는지는 경제적·조세적 귀속에 관한 주장이다. 이 네 가지는 같은 거래를 가리키더라도 서로 다른 증거를 요구한다. 따라서 Chain Prism은 먼저 거래구조를 네 요소로 나누어 그린다(도표 1-7).

도표 1-7 거래구조를 이루는 네 요소와 각 요소가 답하는 질문



네 요소를 분리해 그린 뒤, 요소 사이의 관계를 귀속 질문별로 따로 검증한다. 자료: Chain Prism OCP v1.0.

구조를 나눈 다음에는 실제 주체가 누구인지를 확인한다. 이 작업은 다섯 단계로 진행된다(도표 1-8). 먼저 무엇을 판단하려는지 고정한다. 키 운영자인지, 의사결정자인지, 법적 권리자인지, 회계상 통제자인지, 조세 귀속자인지에 따라 필요한 증거가 다르기 때문이다. 그다음 공식 주소 공시, 법인 공시, 프로젝트 문서, OSINT 같은 공개자료로 후보 주체를 찾는다. 이때 분석 도구의 라벨이나 주소 클러스터는 후보를 찾는 단서일 뿐 결론이 아니다.

세 번째 단계는 문서상 권한의 확인이다. 이사회 의사록, 법적 위임장, 키 관리 정책, 서명자 명부를 확보했다면 누가 작성했는지, 진본인지, 언제까지 효력이 있는지, 위임 범위가 어디까지인지 확인하고 사본, 누락, 변경 이력을 표시한다. 그러나 문서가 있다는 것만으로는 충분하지 않다. 네 번째 단계에서 온체인의 역할·관리자·서명 주소, 문서상의 담당자, 실제 승인·키 변경·실행 기록을 같은 거래와 같은 기간 위에서 연결해야 한다. 이

과정에서 위탁 운영, 공동 권한, 회수되지 않은 권한처럼 문서와 실제가 어긋날 수 있는 경우와 반대 증거를 함께 검토한다.

도표 1-8 주체 귀속의 증거 확보·교차검증 절차

단계	확인·대사와 기록
1 질문 고정	키 운영자 / 의사결정자 / 법적 권리자 / 회계상 통제자 / 조세 귀속자 중 무엇을 판단하는가. 자산·거래·관할·기준기간을 지정한다.
2 공개 식별	공식 주소 공시·법인 공시·프로젝트 문서와 OSINT의 URL·판본·확인일·원출처를 보존한다. 라벨·클러스터는 후보 주체를 찾는 단서로 사용한다.
3 문서상 권한	이사회 의사록·법적 위임장·키 관리 정책·서명자 명부의 작성 주체·진정성·효력 기간·위임 범위를 확인하고 사본·누락·변경 이력을 표시한다.
4 실제 운영 대조	역할·관리자·서명 주소, 문서상 담당자, 승인·키 변경·실행 기록을 같은 거래·기간으로 연결한다. 위탁·공동 권한·미회수 권한과 반증을 검토한다.
5 기준별 평가	관계별로 확인 / 추론 / 미확인과 한계를 남기고 분야별 기준으로 판단한다. 충돌이나 핵심 공백이 남으면 보완 요청·조건부 판단·유보 중에서 선택한다.

자료: Chain Prism OCP v1.0. 주장별 필수 기록과 FC-C02 실무 체크리스트는 제2편 실무 도구집 T4.4에 수록.

마지막으로 관계마다 확인된 것, 추론한 것, 확인하지 못한 것을 나누어 남기고 각 분야의 기준으로 판단한다. 여기서 강조할 점은 문서의 개수나 도구의 점수가 주체를 확정하는 공통 문턱이 되지 않는다는 것이다. 서명자 명부는 실소유자 명부가 아니며, 서명할 수 있다는 사실이 곧 법적 권리나 경제적 통제를 뜻하지도 않는다. 충돌하는 증거나 핵심 공백이 남는다면, 그 상태를 숨기고 결론을 내리기보다 보완을 요청하거나 조건부로 판단하거나 유보하는 편이 정확하다.

이 단계의 기록은 세 양식에 나뉜다. 당사자 사이의 관계는 거래구조표(F-03)에, 그 관계를 뒷받침하는 근거는 증거 목록(F-02)에, 문서와 실제 사이의 차이는 불일치·추가 확인표(F-05)에 남긴다. 기초자산, 청구권, 토큰 가격 역시 서로 다른 대상이므로 구분해 기록한다.[2]

2 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 판단을 대신하는 체크리스트가 아니다.

제1부 · 4단계 전문 판단

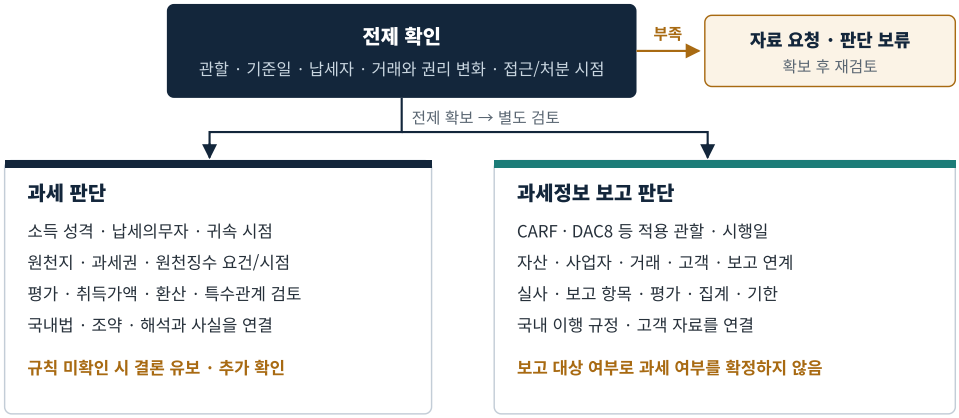
조세 판단은 '과세되는가'와 '보고해야 하는가'를 나누어 묻는다

4단계에서는 같은 사실을 다섯 개의 전문 모듈 가운데 필요한 기준으로 읽는다. 이 절은 판단 흐름이 가장 복잡한 조세 모듈(M3)을 예로 든다. 아래의 흐름은 국가별 세율이나 과세 시점을 정하는 규칙이 아니라, 사실과 적용 법규를 확인하고 쟁점을 기록하는 절차다.

모듈은 같은 사실을 서로 다른 질문으로 읽는다. 규제·AML 모듈(M1)은 사업자와 행위를 분류하고 그에 따른 의무와 위험을 묻는다. 회계·감사·보증 모듈(M2)은 인식, 측정, 검증, 계정 매핑을, 거래구조화·가치평가 모듈(M4)은 권리, 현금흐름, 발행조건, 가치를, IT감사·기술 리스크 모듈(M5)은 권한, 데이터, 시스템, 통제를 다룬다. 분석자는 1단계에서 정한 질문에 필요한 모듈만 선택한다.

조세 모듈은 판단의 순서가 특히 중요하다. 어떤 판단이든 먼저 관할, 기준일, 납세자, 그리고 거래로 인해 어떤 권리가 어떻게 바뀌었는지를 확인해야 한다. 거주지, 거래 상대방, 대가, 자산에 접근하거나 처분할 수 있게 된 시점과 그 증거도 이 단계에서 확보한다. 이 전제가 부족하다면 판단을 보류하고 자료를 요청한 뒤, 자료가 확보되면 다시 검토한다.

도표 1-9 M3 거래별 조세 쟁점 판단 흐름



자료: Chain Prism OCP v1.0. 공식 참고: OECD CARF·CRS 2023(M3-S1), OECD 이전가격 지침 2022(M3-S2). 참고 범위 확인 2026-11-14.

전제가 확보되면 판단은 두 갈래로 나뉜다. 하나는 과세 판단이다. 소득의 성격과 납세의무자, 귀속 시점을 정하고, 원천지와 과세권, 원천징수의 요건과 시점을 검토하며, 평가와 취득가액, 환산, 특수관계 여부를 따진 뒤, 국내법·조약·해석을 확인된 사실과 연결한다. 다른 하나는 과세정보 보고 판단이다. CARF나 DAC8 같은 보고 체계가 어느 관할에서 언제부터 적용되는지, 어떤 자산·사업자·거래·고객이 보고와 연계되는지, 실사·보고 항목·평가·집계·기한은 무엇인지를 확인하고 국내 이행 규정과 고객 자료를 연결한다.

두 갈래를 나누는 이유는 둘이 서로를 대신하지 않기 때문이다. 어떤 거래가 과세정보 보고 대상이라는 사실이 그 거래가 과세된다는 결론을 뜻하지 않으며, 그 반대도 마찬가지다. 또한 과세 판단에서 적용할 규칙을 확인하지 못했다면, 유사한 규칙을 끌어다 결론을 내리기보다 결론을 유보하고 추가 확인 대상으로 남기는 것이 이 절차의 원칙이다.

사례에 따라서는 추가로 물어야 할 질문이 생긴다. 특수관계 거래가 있다면 해당 관할에서 특수관계의 정의와 적용 범위를 먼저 확인한 뒤 기능·자산·위험·계약·가격 산정과 이전가격 자료를 검토한다. 포크, 에어드랍, 리베이스가 있다면 권리가 언제 발생했는지, 접근하거나 처분할 수 있게 된 것은 언제인지, 수량과 지분은 어떻게 변했는지, 가치와 조건은 무엇인지를 구분한 뒤 현지 기준에 따라 소득과 귀속 시점을 검토한다. 국제적 연결이 있는 경우에도 체인 간 이동을 곧바로 국경 간 거래로 분류해서는 안 된다. 납세자, 상대방, 거주지, 서비스, 원천지에 관한 사실부터 확인해야 한다.

4단계의 결과는 질문 → 사실·증거 → 적용 법규와 그 판본·기준일 → 판단과 대안 → 누락과 후속 조치의 순서로 판단 기록(F-04)에 남긴다. 실제 구조를 복원하는 '분석'과 목표·제약 아래 구조를 고르는 '설계'는 구분한다. 설계안은 비용, 세후 결과, 복잡성을 비교한 뒤 3~5단계로 다시 검토한다. 국가별 적용 법규, 조약, 해석의 최신 상태는 각 사례에서 별도로 확인해야 한다.

제1부 · 5단계 정합성

대사는 숫자가 같은지 확인하는 데서 끝나지 않는다

5단계에서는 문서·권리, 코드·권한, 장부·원장, 실제 거래·자산이라는 네 자료군을 같은 대상과 같은 기준시점에 놓고 비교한다. 목표는 차이를 없애는 것이 아니라, 차이의 이유와 그 차이를 보완하는 장치가 설명되는지 확인하는 것이다.

정합성 검토는 숫자의 일치 여부보다 넓다. 코드상의 상태가 계약에서 약속한 권리와 연결되는지, 장부가 실제 지급이나 이전과 같은 시점을 사용했는지도 함께 확인한다. 계약·약관·공시, 실행 규칙과 관리자, 자산·부채·고객 기록, 온체인·은행·수탁의 실제 거래와 자산을 같은 기준 위에 올려 두면, 단순한 계산 오류와 범위나 정의의 차이를 구분하기 쉬워진다.

코드와 약관이 다르다는 사실을 발견하더라도 곧바로 오류라고 부르지 않는다. 일부 처리가 처음부터 오프체인에서 이뤄지도록 설계되었을 수 있고, 약관의 판본이나 구현 버전이 서로 다를 수도 있기 때문이다. 설명할 수 있는 차이는 그 근거를 남기고, 설명되지 않는 차이는 그것이 권리·금액·통제에 미치는 영향과 함께 후속 확인 대상으로 삼는다. 발견된 차이의 유형에 따라 다음 행동은 달라진다(도표 1-10).

도표 1-10 차이의 유형과 다음 행동

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.

자료: Chain Prism OCP v1.0.

기능 카드의 연결 검증 항목은 그대로 대사 항목으로 쓸 수 있다. 이 단계의 산출물은 불일치·추가 확인표(F-05)다. 사실의 문제로 드러난 차이는 2~3단계로, 해석의 문제로 드러난 차이는 4단계로 돌아가 다시 검토하며, 끝내 해소되지 않는 차이는 그 조건과 한계를 밝힌 채 종합 판단으로 넘긴다.

제1부 · 6단계 결론

좋은 결론은 단정의 강도가 아니라, 근거와 다음 행동이 분명한 결론이다

6단계에서는 결론을 확정하고 다음 행동을 정한다. 각 결론에는 위험, 해석의 명확성, 증거의 충분성을 따로 표시하고, 그 결론이 성립하는 조건을 함께 남긴다.

결론을 정리할 때는 확인한 사실, 그 사실이 지지하는 판단, 아직 남은 조건을 구분한다. 이 구분이 있어야 추가 자료가 들어왔을 때 무엇을 다시 검토해야 하는지 알 수 있다. Chain Prism은 결론을 네 가지로 분류한다. 중요한 전제가 확인되고 판단 근거가 충분하면 '채택', 가정이나 조건이 충족되는 범위에서만 판단할 수 있으면 '조건부 채택', 합리적인 대안 해석이 함께 성립하면 그 해석과 결과의 차이를 나란히 적는 '복수 해석', 사실·기준·검토 범위가 부족하면 그 부족을 명시한 '결론 유보'다.

결론마다 붙이는 평가는 세 개의 축으로 나뉜다(도표 1-11). 이 세 축은 서로 다른 것을 측정하므로 합산해 하나의 신뢰도 점수로 만들지 않는다. 위험이 크다는 사실과 증거가 부족하다는 사실은 서로 다른 정보이며, 하나의 숫자로 합치는 순간 어느 쪽 때문에 결론이 약한지 알 수 없게 된다. 같은 이유로 가정은 증거가 아니므로 H로 따로 관리하고, 증거는 출처, 직접성, 완전성, 시점에 비추어 평가한다. 특히 운영 효과성에 관한 증거 없이 통제 위험을 낮다고 확정해서는 안 된다. 통제가 설계되어 있다는 사실과 그 통제가 실제로 작동한다는 사실은 다른 주장이기 때문이다.

도표 1-11 결론에 붙이는 세 가지 평가 축

평가 축	기록 방식
위험	유형 + 영향도 + 발생가능성. 이미 발생한 오류·사고는 별도로 기록한다.
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 축은 합산하지 않는다. 자료: Chain Prism OCP v1.0.

분석을 마치기 전에는 네 가지를 스스로 묻는다. 무엇을 어떤 범위에서 결론 내렸는가. 그 결론은 어떤 사실, 기준, 가정에 의존하는가. 무엇이 아직 확인되지 않았고, 누구에게 확인해야 하는가. 그리고 무엇이 바뀌면 다시 분석해야 하는가. 이 질문에 대한 답은 결론 요약서(F-06)에 남기며, 추가 자료와 조치 담당, 재검토 조건까지 함께 적는다.

제2부 · 01 판단 지원 계층

OCP는 분석 도구를 대체하지 않는다. 도구의 결과를 증거로 바꾸는 계층이다

거래 추적, SQL 집계, 정적 분석, 원장 처리처럼 각 도구는 서로 다른 일을 잘한다. OCP는 그 결과를 하나의 증거 구조로 연결하고, 각 결과를 어떤 주장에 사용할 수 있는지 검토한다.

이 구조에서 도구의 출력은 판단의 입력이다. 도구가 제시한 점수나 라벨이 그 자체로 전문가의 결론이 되지는 않는다. OCP는 도구 결과와 업무자료를 받아 어댑터, 정규화, F/I/H 구분, 연결·대사를 거쳐 전문 모듈로 넘기고, 그 과정에서 원본, 출처, 버전, 변환 이력, 판단 식별자를 추적한다. 최종적인 발견, 영향, 대안, 조치와 그에 대한 승인과 책임은 사람의 판단과 검토에 남는다(도표 2-1).

도표 2-1 분석 도구, OCP, 사람의 판단의 세 계층



자료: Chain Prism OCP v1.0.

세 계층의 경계는 분명하다. 분석 도구는 조회, 탐지, 귀속, 시각화, 대사 같은 결과와 그 한계를 그대로 보존한다. OCP는 입력의 범위와 성격을 검토하고 질문, 증거, 전문 판단, 발견을 연결해 기록한다. 기준의 선택, 대안 해석, 중요성 판단, 최종 결론과 업무상 사용은 분석자와 검토자가 결정한다.

이렇게 계층을 나누면 도구가 바뀌어도 질문과 근거의 연결은 유지된다. 같은 집계를 다른 플랫폼에서 재현하거나 새로운 귀속 자료를 받으면 관련된 주장과 입력만 갱신하면 된다. 다만 두 도구의 결과가 비슷하다고 해서 입력 범위까지 같다고 보아서는 안 되며, 조회 조건과 원본의 계보를 먼저 비교해야 한다. 이 확장은 기존의 6단계를 바꾸지 않는다. 주로 2단계의 입력 검토, 3단계의 연결 분석, 4~6단계의 판단과 보고를 지원하며, 특정 도구의 기능을 대체하거나 어떤 기능이 없다고 전제하지 않는다.

제2부 · 02 도구 선택

도구는 제품 이름이 아니라 확인할 질문에서 고른다

거래 수량을 복원하려면 조회·집계 자료가, 실제 당사자를 연결하려면 주소 정보와 오프체인 자료가 함께 필요하다. 특정 제품을 보유했다는 사실이 분석의 충분성이나 정확성을 보장하지 않는다.

도표 2-2는 질문별로 가능한 도구와 자료의 조합을 예시한 것이다. 여기에 등장하는 제품명은 예시일 뿐이며, 실제로 사용할 때에는 계정, 계약, 권한, 지원 범위를 확인한 뒤 가능한 형식으로 자료를 받는다. 도구 사용권이나 유료 API 접근을 새로 가정하지 않으며, 내보내기·저장·재배포가 허용되는지와 실제로 제공되는 필드를 확인한다. 도구의 버전이나 내부 근거가 제공되지 않으면 '미제공'으로 기록하고, 모든 결과에 같은 신뢰도 수치나 증거 등급을 억지로 부여하지 않는다.[3]

도표 2-2 확인할 질문별 도구·자료와 OCP에 받을 내용

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 분석 오탐, 실행 맥락
기록과 실제 자금은 맞는가?	원장·은행·수탁 / Excel·Python	원본 행·계정·거래 ID·대사식·예외	모집단, 마감시점, 취소, 미결, 단위
실제로 어떤 권리인가?	계약·공시·명부 / 문서 추출	원문·조항·버전·추출 위치·요약	최신성, 원문 일치, 당사자, 조건·요건

제품명은 예시다. 자료: Chain Prism OCP v1.0. 출처 S1~S4.

자료에 접근할 수 없는 문제는 도구를 추가한다고 해결되지 않는다. 비공개 계약이나 고객 원장이 필요한 질문은 공개 체인을 아무리 반복해서 조회해도 답이 남는다. 그런 경우에는 분석 범위를 줄이고, 공개자료로 확인한 결과와 추가 자료 없이는 답할 수 없는 부분을 나누어 보고하는 편이 더 정확하다.

도구를 도입하는 순서도 단계적이다. 처음에는 PDF, CSV, JSON, 화면 결과를 원본과 함께 수동으로 등록한다. 같은 형식의 자료가 반복되면 매핑과 검증 스크립트로 작업을 정형화하고, 필요한 경우에만 승인된 API나 내부 시스템과 연계한다. 공개 포트폴리오에는 공개 가능한 범위만 싣는다.

3 S1 Chainalysis, S2 TRM, S3 Dune, S4 Slither의 공식 자료로 기능 설명을 확인했다(확인일 2026-11-14). 제품별 버전·요금·내보내기·API·라이선스는 적용 시 확인한다. 전체 URL은 부록 출처 목록에 수록.

제2부 · 03 공통 입력 양식

서로 다른 도구의 결과는 원래 맥락을 잃지 않는 공통 기록으로 옮긴다

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

여러 도구의 결과를 연결하려면 공통의 기록 항목이 필요하다. 원본의 위치, 조회 시점, 대상, 변환 이력을 남겨 두면 같은 숫자가 어디에서 만들어졌고 어떤 조건에서 달라지는지 추적할 수 있다. 이 입력 명세의 목적은 자료를 획일화하는 것이 아니라, 원래의 맥락을 잃지 않은 채 비교할 수 있게 하는 최소한의 연결 구조를 만드는 것이다(도표 2-3).

특히 상위 입력 식별자(parent_input_id)와 변환 이력은 같은 원문을 여러 번 독립 근거로 세는 일을 막는다. 원문을 CSV로 옮기고 SQL로 합계를 냈다면 파일은 세 개가 생기지만, 경제적 사실의 원천이 세 개가 되는 것은 아니다. 원본, 변환, 집계, 판단을 구분해 두면 오류가 어느 단계에서 생겼는지도 찾아가기 쉽다.

도표 2-3 공통 입력 양식의 필드 그룹

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

증거·가정 목록(F-02)의 입력 명세로 사용한다. 자료: Chain Prism OCP v1.0.

입력의 최소 단위는 파일이 아니라 주장이다. 한 파일을 하나의 결론으로 취급하지 않고, 같은 원본에서 나온 내용이라도 주장별로 나누어 기록한다. 예를 들어 어떤 주소에 라벨이 표시되었다는 사실과 그 주소의 실제 통제 주체에 관한 주장은 서로 다른 주장 식별자(assertion_id)를 갖는다. 이와 함께 '미제공', '미확인', '비적용'을 구분하고 정규화하기 전의 원본을 보존한다. 해시는 원본이 이후에 바뀌었는지 점검하는 수단일 뿐, 내용이 진실하다는 것을 증명하지는 않는다.

제2부 · 04 주장의 분류

“도구가 이렇게 표시했다”와 “실제로 그렇다”는 서로 다른 주장이다

하나의 출력 안에도 관찰과 추론이 섞여 있다. Chain Prism은 도구 전체를 믿거나 불신하는 대신, 개별 주장마다 필요한 근거와 남은 확인 절차를 정한다.

어떤 분석 도구가 한 주소에 ‘거래소 X’라는 라벨을 붙였다고 하자. 여기에는 두 개의 주장이 겹쳐 있다. 하나는 ‘그 도구의 화면에 X라는 라벨이 표시되었다’는 주장이고, 다른 하나는 ‘그 주소의 실제 통제자는 X다’라는 주장이다. 첫 번째 주장은 화면이나 출력으로 직접 확인할 수 있는 관찰 사실(F)이다. 두 번째 주장은 그 라벨이 어떤 근거로 붙었는지, 그 근거가 얼마나 직접적인지를 따져야 하는 추론(I)이며, 경우에 따라 별도의 보완 자료가 필요하다.

이 구분은 라벨에만 적용되지 않는다(도표 2-4). 특정 블록에서 totalSupply 함수가 어떤 값을 반환했다는 것은 관찰이지만, 그 값이 경제적 의미의 전체 공급량이나 고객의 청구권, 발행자의 상환의무와 같은지는 별도의 분석이 필요하다. 정적 분석기가 경고를 냈다는 사실과 실제로 취약점이 있고 악용될 수 있다는 판단 사이에도 코드와 실행 맥락에 대한 검토가 놓인다. 내부 원장에 고객의 수량이 기록되어 있다는 사실 역시 그 기록의 완전성, 고객의 권리, 실소유 여부, 외부 잔액과의 일치를 보장하지 않는다.

도표 2-4 입력별로 직접 확인할 범위와 추가로 연결해야 할 주장

입력	F: 직접 확인할 범위	I·전문 판단: 추가 연결
주소에 거래소 X 라벨	제공자 화면·출력에 그 라벨이 표시되었다.	실제 통제자가 X라는 귀속은 근거를 검토하고, 제공 근거의 직접성에 따라 보완한다.
기준 블록의 totalSupply 응답	지정 네트워크·구현체·블록에서 특정 값이 반환되었다.	그 값이 전체 경제적 공급·고객 청구권·상환의무인지 별도로 분석한다.
Dune 쿼리 집계	해당 실행·SQL·필터에서 집계값이 산출되었다.	데이터 포괄성·누락·집계 정의가 거래 실질에 맞는지 검증한다.
정적 분석기 경고	특정 코드·규칙·설정에서 경고가 출력되었다.	실제 취약성·악용 가능성·통제 영향은 코드·실행 맥락으로 검토한다.
내부원장 고객 귀속	원장에 해당 고객·수량·거래가 기록되었다.	완전성·권리·실소유·외부 잔액과의 일치 여부를 검토한다.

자료: Chain Prism OCP v1.0.

주장별로 질문을 나누는 이유는 도구의 품질과, 특정 결론을 지지하는 증거의 충분성을 구별하기 위해서다. 주소 라벨의 확신도가 높더라도 법적 당사자나 실소유자가 확정되는 것은 아니다. 같은 이유로 도구가 제공하는 신뢰도(confidence)와 OCP의 증거 충분성은 같은 값이 아니며, 둘 사이에 임의로 점수를 변환하지 않는다. 원장 기록과 온체인 수량을 연결할 때에도 각 기록의 신뢰성뿐 아니라 두 기록이 같은 사건을 가리키는지를 검토해야 한다.

F라고 표시했다고 해서 모든 실제 사실이 확정되는 것도 아니다. F 옆에는 무엇을 관찰한 것인지 그 범위를 적고, 실체에 관한 주장에는 별도의 근거와 검토 상태를 붙인다. 이렇게 하면 원본 입력에서 원본 위치, 정규화·변환, 주장, 증거 연결표, 판단, 발견, 조치에 이르는 연결을 끝까지 따라갈 수 있다. 보완·스트레스·설계·실험을 위한 가정은 H로 별도 표시한다.

제2부 · 05 수용 전 확인

여러 도구가 같은 답을 냈다고 해서 증거가 여러 개인 것은 아니다

도구 결과를 증거로 받아들이기 전에는 범위를 확인하고 원본과 대사한 뒤 수용 상태를 정한다. 결과의 다수결보다 근거의 독립성과 비교 조건을 먼저 본다.

여러 도구가 같은 결과를 냈더라도 같은 원천 자료를 다시 사용했을 수 있다. 반대로 결과가 다르다면 어느 한쪽이 틀렸다고 단정하기 전에 시점, 단위, 범위, 주소 묶음의 정의가 달랐을 가능성부터 살핀다. 예컨대 한 도구는 주소별 잔액을, 다른 도구는 특정 집계 범위를 보여준다면 두 숫자가 달라도 곧바로 오류라고 할 수 없다. 정의를 맞춘 뒤에도 남는 차이만이 실제 검증 대상이다. 충돌을 기록할 때에는 비교 전의 수치를 지우지 않고 각 결과의 조회 조건과 사용 목적을 함께 남긴다.

도표 2-5 수용 전 확인 지점과 문제 발견 시의 처리

확인 지점	실행할 점검	문제 발견 시
대상·시점	체인 ID·주소·자산·블록·시간대·데이터 기준일 일치	잘못된 대상·시점이면 재수집한다. 단순히 최신 결과로 교체하지 않는다.
완전성	행 수·기간·필터·페이지·실패·누락·업데이트 상태	부분 결과로 제한하거나 모집단을 보완한다.
변환 정확성	단위·decimals·환율·부호·취소·중복·조인 검산	원본을 유지하고 변환 단계를 수정해 버전을 기록한다.
근거 독립성	여러 도구가 같은 라벨·원장을 재사용하는지 확인	두 도구의 일치를 독립 증거 두 개로 계산하지 않는다.
검토 상태	수용 / 조건부 수용 / 재확인·보류	핵심 공백은 결론과 다음 자료 요청에 연결한다.

자료: Chain Prism OCP v1.0.

라벨, 수량, 경고가 도구마다 다를 때에는 네 단계로 처리한다. 먼저 어떤 주장이 충돌하는지 분리하고, 각 결과의 대상·범위·시점·원본·데이터 계보를 비교한다. 이어서 서로 다른 기준이나 클러스터 범위를 쓴 것인지 검토하고, 해결한 차이와 남은 차이를 불일치·추가 확인표(F-05)에 기록한다. 이 과정에서 다수결, 브랜드 순위, 도구 점수의 평균으로 결론을 정하지 않는다. 자동화는 수집, 정규화, 대사, 예외 표시를 도울 수 있지만, 무엇을 증거로 받아들이고 누구에게 귀속시키며 어떻게 판단할지에 대한 책임은 분석자와 검토자에게 있다.

제2부 · 06 실행과 재현

도구를 실행한 기록과 그 결과를 판단에 쓴 기록은 둘 다 남아야 한다

입력을 받아들인 이유, 확인한 한계, 후속 검토 대상이 남아 있어야 다른 사람이 같은 과정을 따라갈 수 있다. 도표 2-6은 이 기록의 순서와 위치를 정리한 것이다.

도표 2-6 도구 사용 실행표

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

자료: Chain Prism OCP v1.0.

마지막 단계인 재수행은 같은 원본, SQL, 설정, 코드 버전으로 결과를 다시 만들어 보는 것이다. 이때 재현한 결과와 새로 조회한 최신 결과는 구분해야 한다. 최신 결과가 다르다는 것은 데이터가 바뀌었다는 뜻일 수 있고, 재현 결과가 다르다는 것은 처음의 분석 과정에 문제가 있었다는 뜻일 수 있기 때문이다. 원본 접근이 제한되어 있다면 재현이 가능한 범위도 함께 기록한다.

이 장에서 소개한 도구의 기능 설명은 각 제품의 공식 자료를 참고했으며, 공통 입력, F/I/H, 검토 절차는 Chain Prism의 설계다.[4] 제품별 버전, 요금, 내보내기, API, 라이선스는 실제로 적용할 때 확인해야 한다.

4 S1 Chainalysis(조사·추적 도구), S2 TRM(Forensics·귀속 정보), S3 Dune(실행별 결과 조회·메타데이터), S4 Slither(Solidity/Vyper 정적 분석). 공식 자료 확인일 2026-11-14. URL은 부록 출처 목록에 수록.

제3부 · 3.1 USDC · 실제 사례

USDC: 확인한 범위만큼만 결론을 내린다

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

USDC는 Chain Prism을 실제 공개자료에 처음 적용한 사례다. 이 사례의 성과는 모든 기능을 검증한 데 있지 않다. 어디까지 확인했는지를 고정하고, 확인한 것과 확인하지 않은 것을 끝까지 나누어 기록한 데 있다.

이 절은 두 개의 기준점을 다룬다. 첫째는 2026년 11월 13일 Ethereum 메인넷의 특정 블록에서 USDC 컨트랙트를 조회한 온체인 관찰이고, 둘째는 2026년 9월 30일 기준 USDC 공개보고서의 수치를 다시 계산한 검토다. 두 기준점은 날짜도, 대상 범위도 다르다. 그래서 이 절은 둘을 하나의 숫자로 합치지 않고, 각각에서 무엇을 말할 수 있는지를 따로 정리한다. 결론을 먼저 말하면, 보고서 내부의 산술 정합성은 '확정(범위 한정)'이고, 나머지 질문은 모두 '유보'다.

분석 범위를 먼저 고정했다

첫 실제 적용에서 가장 먼저 한 일은 분석의 범위를 고정하는 것이었다. 대상은 Ethereum 메인넷(chain ID 1)의 native USDC이고, 기준 블록은 26,407,530(UTC 2026-11-13 17:26:47, 한국시간 2026-11-14 02:26:47)이다. 조회한 것은 이 블록에서의 블록 정보, 저장 슬롯, 역할, 공급량, 배포 바이트코드이며, 모두 PublicNode라는 단일 공개 RPC의 읽기 응답이다. 코드의 기능을 해석하기 위한 참고 자료로는 Circle의 stablecoin-evm 저장소의 특정 커밋을 고정했다(도표 3-1).

이 범위 설정에는 의도적인 한계가 있다. 이 사례는 외부 공개자료 분석이며, Circle의 내부 운영이나 준비자산 자료까지 확보한 것으로 범위를 넓히지 않는다. 검토 관점은 IT감사·기술 리스크(M5)를 중심으로 하고 규제·AML(M1)과 회계·감사·보증(M2)의 증거 질문을 연결했으며, 조세(M3)와 구조화·평가(M4)는 필요한 쟁점만 기록했다. 또한 확정 블록이라는 표시는 RPC 제공자의 응답을 그대로 기록한 것이며, 독립된 노드로 교차 검증하지는 않았다.

도표 3-1 USDC 첫 적용의 고정 범위

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

자료 성격: 실제 공개 / 수행 범위: 단일 RPC 읽기·참고 소스. 사례 ID R-USDC-01.

범위를 고정한 뒤에는 네 개의 질문을 세웠다. 누가 발행자(minter)와 발행 한도를 설정하며 실제 발행 경로는 무엇인가(발행, FC-A01). owner, masterMinter, pauser, blacklister와 프록시 관리자는 서로 어떤 관계인가(역할, FC-C02). 표준 슬롯 밖의 구현·관리 경로와 배포 소스는 어떻게 연결되는가(변경, FC-E01). 그리고 어떤 호출 경로와 대상, 예외에 거래 제한이 적용되는가(동결, FC-D02).

슬롯은 비어 있는데, 구현 코드는 존재했다

조회 결과 중 가장 해석에 주의가 필요한 것은 프록시 관련 저장 슬롯이었다. 업그레이드가 가능한 컨트랙트는 보통 사용자가 호출하는 '프록시'와 실제 로직을 담은 '구현 컨트랙트'로 나뉘고, 프록시는 어떤 구현을 쓰는지와 누가 관리하는지를 정해진 저장 위치(슬롯)에 기록한다. 오늘날 널리 쓰이는 표준인 ERC-1967은 이 위치를 정해 두고 있다. 그런데 기준 블록에서 USDC의 ERC-1967 구현 슬롯과 관리자 슬롯은 둘 다 0이었다. 반면 그보다 앞선 방식인 ZeppelinOS 계열의 구현 슬롯과 관리자 슬롯에는 각각 주소가 기록되어 있었고, 그 구현 주소에서는 실제로 코드가 반환되었다(도표 3-2).

여기서 말할 수 있는 것은 제한적이다. ERC-1967 슬롯이 비어 있다는 관찰만으로 구현이 없다거나 업그레이드가 불가능하다고 결론 내릴 수 없다. 다른 계열의 슬롯에는 구현 주소가 있고 코드도 조회되었기 때문이다. 이 관찰이 주는 교훈은 프록시를 분석할 때 표준의 이름이 아니라 실제 저장과 실행의 경로를 따라가야 한다는 것이다. 다만 코드가 존재한다는 사실과 그 코드를 바꿀 수 있는 권한이 적절하게 관리되는지는 별개의 질문이다.

도표 3-2 기준 블록에서 관찰한 슬롯과 역할의 반환값

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
admin() · implementation()	이번 요청 조건에서 execution reverted
owner()	`0xfcb19e6a322b27c06842a71e8c725399f049ae3a`
masterMinter()	`0xe982615d461dd5cd06575bbea87624fda4e3de17`
pauser()	`0x4914f61d25e5c567143774b76edbf4d5109a8566`
blacklister()	`0x0a06be16275b95a7d2567fbdae118b36c7da78f9`

기준 블록 26,407,530, PublicNode 단일 공개 RPC 응답. 역할 주소의 차이는 승인 독립성의 증명이 아니다.

또 하나 설명이 필요한 관찰은 프록시의 admin()과 implementation() 함수를 일반적으로 호출했을 때 실행이 되돌려졌다(reverted)는 점이다. 보존한 공식 소스의 주석에는 2020년 5월 13일에 이 두 함수에서 관리자만 호출할 수 있게 하는 제한(ifAdmin)을 제거했다는 기록이 있다. 이를 근거로 하나의 가설을 세울 수 있다. 실제로 배포된 프록시가 이 수정 이전의 관리자 제한형이어서, 관리자가 아닌 주소의 호출이 구현 컨트랙트로 넘어가 되돌려졌을 수 있다는 것이다. 그러나 이는 검증 전의 추론(I)이다. 배포된 코드가 이 소스와 같은지 확인하지 않았으므로, 수정 이전 버전을 쓰고 있다고 확정하지 않는다.

이 가설을 확인하는 다음 단계도 정해 두었지만 아직 수행하지 않았다. 같은 블록, 같은 프록시, 같은 함수와 호출 데이터에서 호출자(from)만 관찰된 관리자 주소로 지정한 읽기 시뮬레이션을 일반 호출과 비교하고, 반환값을 슬롯과 대조하며, 실제 배포된 프록시 코드의 분기와 소스 이력을 확인하는 것이다. 이때 주의할 점이 있다. 호출자를 지정하는 것은 읽기 시뮬레이션의 조건일 뿐, 그 주소의 키를 보유하고 있다거나 실제로 서명할 권한이 있다는 것을 증명하지 않는다. 시뮬레이션이 성공하더라도 구체적인 소스 버전과 되돌림의 원인을 확정하려면 코드 대응이 필요하고, 실패한다면 다른 원인을 조사해야 한다. 재조회를 하면 그 요청과 응답, 기준 블록을 새로운 관찰 사실(F)로 기록하고, 위 가설이 지지되는지 기각되는지와 남은 한계를 갱신한다.

확인한 신호는 결론이 아니라 다음 질문이 된다

관찰한 주소와 참고 코드의 기능은 기능 카드별 질문을 구체화하는 재료다. 그러나 역할 주소를 읽었다는 사실만으로 모든 실행 경로를 검토한 것은 아니며, 참고 저장소에 있는 기능을 현재 배포된 컨트랙트의 동작으로 자동 전환하지도 않는다. 도표 3-3은 현재 확보한 근거가 어느 카드로 연결되고 다음에 무엇을 확인해야 하는지를 보여준다.

도표 3-3 기능 카드별 확보한 근거와 다음 확인

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

자료: R-USDC-01, 단일 RPC 읽기·참고 소스.

규제·AML 관점의 동결 질문은 특히 ‘blacklister가 누구인가’에서 끝나지 않는다. 거래 제한이라는 행위는 세 부분으로 나누어 확인해야 한다. 먼저 제한을 결정한 주체, 대상, 사유, 시점과 그 근거가 된 정책·승인·문서다. 다음은 기술적 차단의 실제 범위, 즉 코드와 상태와 실행 경로가 어떤 고객·주소·수탁 관계에 영향을 미치는지다. 마지막은 해제 기준과 승인, 로그, 고객 통지와 이의 처리 기록이다. 그리고 각 부분의 판단에 앞서 관할과 사업자 지위, 적용 요건을 별도로 특정해야 한다. 이번 사례에서는 이 오프체인 자료를 확보하지 못했으므로 요청 항목으로 남겼으며, 기술적 차단 기능이 있다는 것을 확인한 사실을 규제상 의무를 이행했다는 확인으로 표현하지 않는다.

조세 관점은 아직 자료 요청 단계다. 거래 유형, 고객, 거주지, 서비스 제공자, 보고 범위에 관한 자료가 필요하며, 한국·미국·EU의 구체적인 적용 결론은 작성하지 않았다. 이 단계까지의 성과는 실제 적용의 범위와 추가 질문을 좁힌 것이다. 기술적 역할 주소를 규제상 책임자나 고객의 실소유자로 곧바로 귀속시키지 않는다.

11월의 온체인 관찰과 9월의 보고서는 섞지 않는다

이후 사례 보완에서 2026년 9월 USDC 공개보고서를 검토 대상으로 추가했다. 이때 가장 경계한 것은 서로 다른 두 기준점을 하나로 합치는 일이다. 11월 관찰에서 기준 블록의 totalSupply는 44,630,813,371.668586 USDC(decimals 6)였다. 이 값은 11월 13일 시점, Ethereum 한 체인의 공급량이다. 반면 9월 보고서의 유통량은 9월 30일 시점, 보고서가 정의한 모든 승인 체인을 합친 값이다. 날짜도 모집단도 다르므로, 11월의 Ethereum 공급량으로 9월의 전체 준비자산을 나눈 비율은 제시하지 않는다. 기존의 11월 관찰은 착수 당시의 응답을 인용해 보존했으며, 이번 개정에서 RPC를 다시 조회하지 않았다. 과거 20,000,000번 블록에 대한 상태 접근 실패와 Etherscan 직접 대조 미완료 역시 기존 기록대로 남겨 두었다.

보고서 검토의 범위도 먼저 고정했다. 원문은 Circle 투명성 페이지에 연결된 공식 PDF(S1, 6쪽)이며, 보고서 일자는 2026년 10월 26일, 검토 기준시점은 2026년 9월 30일 23시 59분(UTC)이다. 이 보고서는 Circle Internet Group, Inc. 경영진의 주장에 대해 Deloitte & Touche LLP가 수행한 examination이다. 즉 특정 시점의 경영진 주장에 대한 제3자의 검토이며, 이 보고서의 작성자가 독립적으로 감사를 수행한 것으로 바꾸어 표현해서는 안 된다. 공식 PDF 원문은 웹 문서 열람으로 확인했고, 로컬 원본 파일의 보관과 해시는 확보하지 못했다. 정리는 Vanzi가 2026년 11월 18일에 했으며 독립 검토는 수행되지 않았다.

보고서 내부의 수치는 서로 맞는다

재계산은 보고서에 표시된 정수를 그대로 옮겨 적은 뒤 수행했다. 승인된 체인의 총공급량 75,866,964,179 USDC에서 발행이 허용되었으나 아직 발행되지 않은 토큰(Tokens Allowed But Not Issued) 1,856,810,081, 접근이 제한된 토큰(Access Denied Tokens) 131,245,845, Circle Gateway의 소각 대기분(pending burns) 46,939를 차감하면 73,878,861,314 USDC가 되며, 이 값은 보고서의 유통량과 일치한다. 준비자산은 펀드 부문(국채 25,361,578,416달러, 환매조건부 거래 36,654,000,000달러, 현금 1,003,847,741달러, 시차·결제 차이 순액 −552,000,382달러)이 62,467,425,775달러, 기타 부문(국채 1,757,678,272달러, 금융기관 현금 9,502,194,346달러, 시차·결제 순액 229,389,308달러)이 11,489,261,926달러로, 합계 73,956,687,701달러가 보고서 총계와 같다(도표 3-4).

도표 3-4 유통량 조정과 준비자산 재집계 (2026-09-30 23:59 UTC, 보고서 표시 정수 기준)

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

차액 = 준비자산 − (유통량 × USD 1). 비율 = 준비자산 ÷ (유통량 × USD 1) × 100. 반올림은 최종 비율 표시에만 적용. 자료: S1 PDF 1~2·4~6쪽(E-R01~E-R03), 계산 C-R01.

따라서 유통량, 두 소계, 총계 어디에서도 재계산 차이는 없었다. 보고서 수치를 따르면 준비자산은 유통량을 1 USDC당 1달러로 환산한 금액보다 77,826,387달러 많으며, 비율로는 100.1053%다. 계산에서 두 가지는 의도적으로 하지 않았다. 폐기된 FLOW 체인의 동결분 993,225 USDC는 보고서 주석에서 이미 유통량 제외 항목으로 다루고 있으므로 총공급량에서 다시 차감하지 않았다. 또 접근이 제한된 토큰을 유통량에서 제외했다고 해서 그 토큰에 대한 법적 상환의무가 소멸했다고 해석하지 않았다.

같은 문서 안의 일치는 독립된 교차 검증이 아니다

이 재계산이 보여주는 것은 정확히 어디까지일까. 이 질문에 답하기 위해 검토의 주장을 다섯 개로 나누고, 각 주장마다 근거와 연결 상태를 따로 판단했다(도표 3-5). 핵심은 '같은 문서 안에서 숫자가 서로 맞는다'는 것과 '서로 다른 자료가 같은 실체를 가리킨다'는 것을 구분하는 데 있다. 재계산에 쓴 세 개의 증거(E-R01~E-R03)는 서로 독립된 세 출처가 아니라 같은 보고서의 세 부분이다. 따라서 이들 사이의 일치를 독립적인 교차 검증으로 표시하지 않는다.

도표 3-5 주장별 증거 연결과 판단 상태

주장	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.** 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: case_id=R-USDC-01-R / source=S1 / report_date=2026-09-30T23:59Z / currency=USD / unit=USDC. 숫자는 S1에서 전사한 표시값이다.

유보된 네 주장은 각각 구체적인 차이로 이어진다. 첫째는 시점과 모집단의 차이다. 11월의 Ethereum 관찰과 9월의 전체 승인 체인을 대사하려면 체인과 계약의 목록, 기준시각에 해당하는 블록, 노드 응답과 집계가 필요하다. 둘째는 유통량 정의의 차이다. 미발행, 접근 제한, 소각 대기, 폐기 체인이라는 조정 항목이 중복 차감되거나, 기술적 상태와 법적 권리가 혼동될 위험이 있으므로 조정별 주소·상태·약관·권리 근거가 필요하다. 셋째는 준비자산의 기초자료다. 공시된 명세를 은행·수탁 기록이나 내부 원장과 대조하지 않았으므로 실재성, 권리, 부담을 직접 확인하지 못했다. 넷째는 결제시차 순액이다. 펀드 부문의 −552,000,382달러와 기타 부문의 +229,389,308달러는 합산 자체는 맞지만, 개별 조정 항목이 실재하는지와 어느 기간에 귀속되는지는 검증하지 않았다. 다섯째는 보고일 이후의 사건과 실행 경로다. 후속 흐름, 배포 코드 대응, 권한 운영에 관한 자료 없이는 현재의 지급능력이나 통제 효과성으로 결론을 넓힐 수 없다.

이 차이들은 모두 미해결이거나 외부 자료를 확보하지 못한 상태다. 각 차이에는 필요한 자료와 담당 역할, 재검토 조건을 연결해 두었다. 여기서 담당은 실제로 배정된 사람이 아니라 필요한 역할을 뜻하며, 자료 요청·수령·완료일은 접근 권한과 업무 범위를 합의한 뒤에 정한다. 그리고 관찰된 차이를 곧바로 오류나 부정, 준비자산 부족으로 판단하지 않는다. 그것이 정당한 기준의 차이인지, 자료의 부족인지, 처리의 오류인지를 먼저 구분한 뒤 결론을 갱신한다.[5]

결론: 공개보고서의 내부 산술은 확정, 나머지는 유보

이 사례의 결론은 범위별로 나뉜다. 보고서에서 옮겨 적은 표시값을 기준으로 유통량 조정, 준비자산의 소계와 총계, 차액과 비율을 산술적으로 재현했다는 것은 '확정'이다. 단, 보고서 기초자료의 진실성은 자체적으로 확인하지 않았다. 보고서 기준시각의 전체 체인과 조정 모집단을 독립적으로 재구성하지 않았으므로, 기존 11월 Ethereum 관찰과의 실질적인 대사는 '유보'다. 준비자산의 실재·권리·부담, 특정 보유자의 상환권, 이후의 지급능력과 통제 효과성에 대해서도 독립적인 결론을 내리지 않고 '유보'한다.

수행한 일과 수행하지 않은 일도 분명히 해 둔다. 공식 공개 문서를 열람하고, 숫자를 옮겨 적고, 산식을 실행해 차이 0과 준비자산 초과액을 확인했으며, 증거 연결표와 불일치·추가 확인표, 결론 요약서를 작성했다. 독립 RPC 교차 조회, 은행·수탁 확인, 내부 원장 대사, 소스와 바이트코드의 대응, 법적 권리에 관한 의견, 독립 검토자의 재현은 수행하지 않았다. 같은 결과를 재현하려면 동일한 입력과 부호, 수식을 적용하면 되며, 새로운 월의 보고서 숫자를 섞어 바꾸지 말고 별도 판본으로 실행해야 한다.

그러므로 이 사례의 '완료'는 공개보고서 내부 산술 검토와 증거 공백의 정리에 한정된다. 이를 R-USDC-01 전체의 엔드투엔드 검증이나 독립 보증, 또는 현재 준비율의 확인으로 표현해서는 안 된다.

5 차이 항목 D-R01(시점·모집단), D-R02(유통 정의), D-R03(준비자산 기초자료), D-R04(결제시차 순액), D-R05(후속 사건·실행 경로)는 각각 판단 J-R02~J-R05의 재검토 조건에 연결된다. 상세 표는 제2편 실무 도구집 T2.1의 F-05 작성 예시로 수록.

제3부 · 3.2 건물 RWA · 가상 사례

같은 건물이라도, 자산의 가치와 토큰이 담은 권리의 가치는 다르다

자료 · 가상 카드 · 비적용 범위 · 서술·계산

이 교육 사례는 부동산 수익참여형 토큰 하나를 가정해, 자산 전체의 가치와 투자자가 보유한 권리의 가치가 어떻게 달라지는지, 그리고 가치 계산과 권한의 적정성 판단을 왜 분리해야 하는지를 보여준다. 모든 수치는 절차를 설명하기 위한 가정이며 실제 상품, 가격, 법률 의견이 아니다.

가치 100억 원의 건물이 있고, 이 건물을 담보로 40억 원을 차입했다고 하자. 투자자의 토큰은 부채를 갚고 남는 잔여가치에 비례해 참여하는 권리라고 가정하고, 발행 수량은 60만 개로 둔다. 설명을 단순하게 하기 위해 비용과 세금은 생략한다. 이 가정에서 토큰 1단위의 기준값은 (100억 − 40억) ÷ 60만 = 1만 원이다.

이 1만 원이라는 숫자가 무엇을 뜻하는지가 이 사례의 핵심이다. 토큰 보유자가 받는 것은 건물 가치 100억 원이 아니라, 차입금과 비용·배분 조건을 거친 뒤에 남는 현금흐름에 대한 권리다. 그래서 자산 가치의 변화는 토큰 가치에 더 크게 전달된다. 건물 가치가 80억 원으로 20% 떨어지면 잔여가치는 40억 원으로 줄고, 단위당 기준값은 약 6,667원으로 3분의 1가량 낮아진다. 권리의 구조가 바뀌면 계산식 자체가 달라진다. 토큰을 잔여가치 참여형이 아니라 담보부 채권형으로 설계했다면 이 계산을 그대로 쓸 수 없고, 원리금·만기·담보·회수구조를 다시 모형화해야 한다. 토큰 이전에 제한을 추가하는 경우에도 그것이 가치에 미치는 영향은 투자자 자격, 유동성, 이전 로직을 따로 분석해야 한다(도표 3-6).

도표 3-6 가정과 변경 가정에 따른 단위당 기준값

가정	계산 결과	추가 확인
기준(H-01)	(100억 − 40억) ÷ 60만 = 1만 원	조건부 계산. 시장가격·공정가치 결론 아님
건물 가치 80억(H-02)	(80억 − 40억) ÷ 60만 ≈ 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

자료 성격: 가상 / 수행 범위: 서술·계산. 비용·세금·배분순위는 생략했다.

이 단위당 값은 가정 아래의 단순 계산이다. 실제 발행가격, 시장가격, 공정가치와 같다고 단정하지 않는다. 실제 사례에서는 실제 공개자료로 기준 분석을 먼저 만든 뒤 가정(H)을 추가하고, 기준과의 차이를 설명하는 방식으로 진행한다.

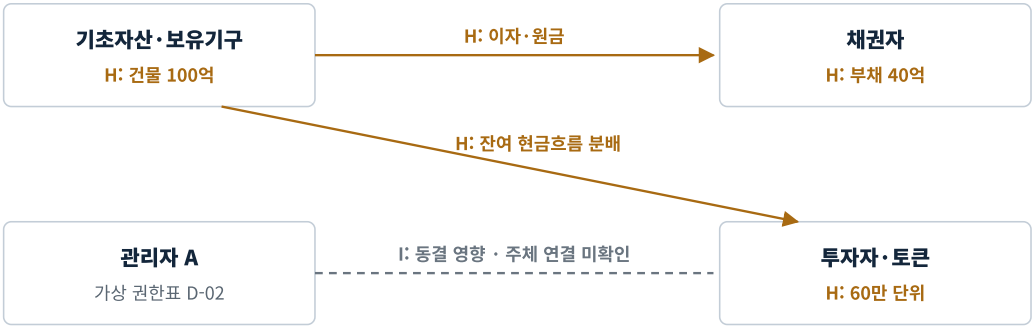
가치 계산과 권한 판단은 따로 기록한다

이 사례는 작성 양식을 실제로 채워 보는 연습이기도 하다. 분석 단위는 부동산 수익참여형 토큰 상품 하나이고, 질문은 '투자자 관점에서 관리자의 권한과 이전 제한이 설명 문서와 일치하는가'다. 기준 시점은

학습용 시점 T0로 두고 특정 법역에서의 법적 유효성 판단은 제외했으며, 거래구조화·가치평가(M4)와 IT감사·기술 리스크(M5)를 선택하고 권리관계는 공통 전제로 검토했다.

증거 목록에는 두 개의 가상 자료가 있다. 하나는 '적격 투자자 사이에서만 이전할 수 있고, 운영사가 단독으로 동결할 수 없다'고 적은 설명문(D-01)이고, 다른 하나는 '관리자 A가 동결과 해제를 할 수 있다'고 설정한 권한표(D-02)다. 둘 다 실제 계약이나 배포 코드가 아니다. 여기서 관찰할 수 있는 사실(F)은 두 자료에 서로 다른 조건이 적혀 있다는 것뿐이다. 설명과 권한 설정 사이에 정합성 문제가 있을 수 있다는 것은 추론(I)이며, 실제 권리나 운영에 미치는 영향에 대한 결론은 유보한다.

도표 3-7 건물 토큰의 거래구조·귀속 분석도



그림은 모두 가상 자료와 가정에 기반한다. 가정 관계는 H, 확인되지 않은 관계는 점선과 I로 표시했다. D-02는 실제 주체의 신원을 증명하지 않으며, 표시된 권한은 법적 정당성·회계상 통제와 별도로 판단한다.

거래구조도는 토큰의 이동을 그리는 데서 한 단계 더 나아간다. 자산 보유자, 채권자, 투자자 사이의 계약 관계와 현금 이동을 함께 표시해야 기술적 기록이 어떤 경제적 권리와 연결되는지 볼 수 있다(도표 3-7). 이를 바탕으로 판단표에서는 수치 계산과 권리 해석을 분리해 기록한다. 단위당 기준값 1만 원과 약 6,667원은 각각 가정 H-01과 H-02에 따른 조건부 계산이다. 권한 설명의 불일치는 예시 자료 사이의 불일치일 뿐 실제 코드나 실행으로 검증한 것이 아니다. 통제 개선안으로는 운영사의 단독 승인을 다중 승인과 기록 절차로 바꾸는 설계(H-03)를 제시했지만, 그 효과는 키와 서명자, 우회 경로, 실제 운영 테스트로 별도 검증해야 한다.

검토 중 발견한 차이가 모두 같은 종류의 문제는 아니다. 설명과 권한이 다르다는 차이에는 배포·구현 코드와 실제 권한·키 관리 자료를 요청하고, 관리자 A의 실제 통제자가 확인되지 않았다는 공백에는 서명·승인·운영 근거를 확보하되 주소 라벨만으로 주체를 확정하지 않는다. 설계 대안은 우회 권한, 가용성, 비용, 실행 지연을 비교하고, 실제 데이터와 테스트가 수행되지 않았으므로 미승인 이전·동결·권한 교체의 예상 결과와 실제 결과를 기록하는 검증 계획을 남긴다.

종합 결론은 다음과 같다. 학습용 자료의 권한 설명은 서로 불일치하지만, 실제 상품의 법적·운영상 결론은 유보한다. 위험은 기술·운영 위험으로, 조건에 따라 영향이 중대할 수 있으나 실제 증거가 부족해 발생가능성은 평가를 유보했다. 예시 문구의 비교는 해석 명확성이 높지만 실제 권리·규제 효과는 판단을 유보했으며, 실제 주체·운영·권리에 관한 핵심 증거는 확보되지 않았다(E4). 추가 자료를 확보하기 전까지 결론은 유보하고, 자료가 확보되면 2~5단계를 다시 수행한다. 재검토 조건은 구현체·권한·약관의 변경, 주체를 확인할 수 있는 자료, 또는 실제 테스트 결과의 확보다.

제3부 · 3.3 DEMO-USD · 가상 사례

106%가 100%로 바뀐 이유는 숫자가 아니라 범위에 있다

자료 · 가상 카드 · 시드 범위 · 서술·계산

DEMO-USD는 처음 제시된 준비율이 왜 그럴듯해 보이는지에서 출발해, 추가 자료가 들어오면서 판단이 어떻게 수정되는지를 순서대로 보여주는 가상 사례다. 핵심은 최종 비율이 아니라, 분자와 분모에 무엇을 넣었는지를 설명할 수 있느냐다.

가상의 스테이블코인 DEMO-USD의 약관은 적격 보유자가 1단위당 1달러를 상환받을 수 있고, 상환을 요청하면 지급 절차가 시작되며, 지급이 완료되기 전까지는 청구권이 존속한다고 정한다. 분석 기준은 시점 T0에서 자료들이 서로 정합한지다. 처음 받은 자료는 다섯 가지다(도표 3-8). 발행사의 보고서는 은행잔액 1,230만 달러와 상환의무 1,160만 달러를 근거로 약 106%의 준비율을 제시했다.

도표 3-8 최초 자료

자료 ID	내용
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.

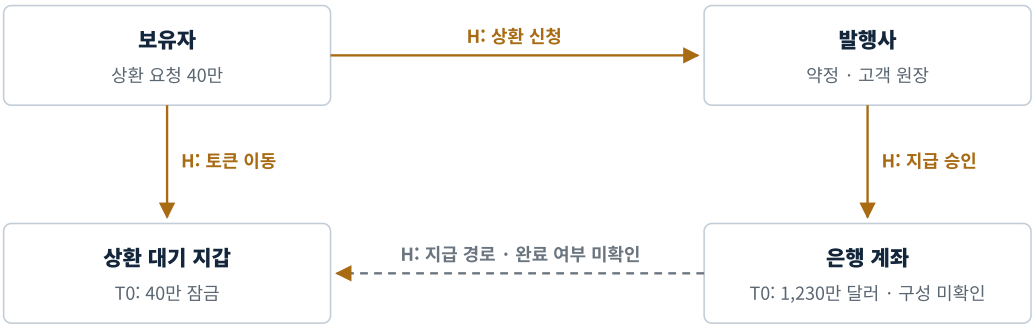
자료 성격: 가상 / 수행 범위: 서술·계산.

이 자료만 보아도 네 개의 질문이 생긴다. 공급량과 상환 대기분, 보고된 의무의 잔액은 서로 연결되는가. 은행잔액 전체가 이 상품의 준비자산인가. 상환의 신청, 잠금, 소각, 지급을 구분했는가. 그리고 '발행은 다중 승인'이라는 설명이 업그레이드와 별도로 존재하는 발행 권한에도 적용되는가. 이 사례를 연습할 때는 뒤의 추가 자료를 먼저 읽지 말고, 최초 자료만으로 필요한 확인 질문을 써 보는 편이 좋다. 106%라는 결과를 다시 계산하는 일과, 그 비율에 쓰인 자산과 의무가 같은 상품의 범위인지 묻는 일은 다른 작업이다.

잠금은 소각이 아니고, 요청은 지급이 아니다

총공급량과 상환의무를 비교하려면 토큰이 어디에 있는지만이 아니라 그 상태가 어떤 권리를 뜻하는지를 봐야 한다. 체인 스냅샷에서 총공급량 1,200만은 일반 보유 지갑의 1,160만과 상환 대기 지갑의 40만으로 이루어져 있다. 그런데 운영 설명에 따르면 발행사는 상환 신청 40만을 이미 보고 의무에서 차감했다. 이 차감이 옳은지는 그 40만이 지금 어떤 상태인지에 달려 있다. 상환 대기 지갑에 잠겨 있다는 것은 지급이 완료되었다는 것과 같지 않고, 토큰이 소각되었다는 것과도 같지 않다. 가상의 약관은 지급이 완료되기 전까지 청구권이 존속한다고 정하고 있으므로, 요청만으로 관련 의무가 사라지는지는 검토가 필요하다(도표 3-9).

도표 3-9 DEMO-USD의 거래·권한·의무 구조



지급 경로는 가정(H)이다. 다음 확인 대상은 T0 시점의 지급 완료 여부와 은행 계좌의 구성이다.

다른 영역에도 열린 질문이 남는다. 은행잔액 1,230만 달러가 어떤 계좌로 구성되어 있고 명의와 제약이 무엇인지는 확인되지 않았다. 권한 면에서는 업그레이드의 다중 승인과 별도로 존재하는 발행 권한을 구분해야 하며, 키와 승인자, 실제 운용은 확인되지 않았다. 귀속 면에서는 가상의 발행사를 계약상 의무자로 전제하되, 관리자 주소의 실제 키 통제는 별도의 증거가 필요하다. 이 단계에서 세울 수 있는 초기 추론은 세 가지였다. 의무 40만이 너무 일찍 차감되었을 가능성, 은행자금에 상품과 무관한 자금이 섞였을 가능성, 그리고 발행 승인의 범위에 공백이 있을 가능성이다.

추가 자료는 분자와 분모의 범위를 다시 정했다

이후 가상의 추가 자료 세 건이 들어왔다. 추가 자료는 최초 자료와 별도의 버전으로 기록하며, 최초 결론을 방어하기보다 어떤 전제가 달라졌는지를 남긴다. 첫째 자료(V-D06)는 상환 요청 40만이 아직 요청·잠금 단계이며, 현금 지급은 T0 이후 예정이고 소각도 실행되지 않았다는 것이었다. 따라서 T0 시점에 그 40만에 대한 청구권은 존속하며, 보고 의무에서 차감한 처리는 다시 검토해야 한다. 둘째 자료(V-D07)는 은행잔액 1,230만이 상품 계좌 1,200만과 별도의 회사 운영계좌 30만으로 이루어져 있다는 것이었다. 운영계좌 30만은 이 시나리오에서 상품의 준비자산에서 제외한다. 셋째 자료(V-D08)는 분석 기간의 발행 승인 기록 한 건뿐이었고, 전체 모집단이나 키의 독립성에 관한 자료는 없었다. 일부 승인 기록이 있다는 사실과 통제 전체의 효과성은 구분해야 한다.

도표 3-10 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 목적의 의무다. 정식 회계 분류와 분개는 별도 질문으로 남긴다.

범위를 바로잡은 결과 준비자산과 보고 목적의 상환의무는 모두 1,200만 달러가 되고, 비율은 106.03%에서 100%로 바뀌었다(도표 3-10). 여기서 주의해야 할 것은 이 숫자가 무엇을 증명하지 않는가이다. 106%에서 100%로의 변화는 분자와 분모의 범위를 같은 상품, 같은 시점, 같은 의무에 맞춘 계산의 결과일 뿐이다. 비율이 맞아졌다는 사실을 자산의 안전성, 유동성, 무담보성, 상환능력을 입증한 결과로 확대해서는 안 된다. 또한 같은 조정이 다른 구조의 상품에도 필요한지는 별도로 검토해야 하므로, 이 계산을 스테이블코인 일반의 비율 산식으로 옮겨 쓰지 않는다. 기록상의 변화도 남겨 두었다. 처음에는 '40만 차이의 원인 미확인'이었던 판단이 추가 자료 이후 '지급 전 대기분의 차감'으로 구체화되었고, 통제 효과성은 추가 자료 이후에도 유보되었다.

세 가지 발견과 그 범위

이 사례에서 얻은 발견은 세 가지다. 첫째, 지급 전의 대기 청구권 40만 달러가 보고 목적의 의무에서 미리 차감되었다(V-F01). 가정한 약정 아래에서 의무는 40만 늘어나며, 상환 상태별 대사와 처리 규칙을 정비해야 한다. 둘째, 은행 총액에 운영계좌 30만 달러가 섞여 있었다(V-F02). 이 사례의 상품 준비자산에서 30만을 제외하고, 계좌와 보고 범위를 연결해야 한다. 셋째, 업그레이드의 다중서명과 별도의 발행 권한은 구분되는데 승인 기록은 한 건만 확보되었다(V-F03). 설명만으로는 발행 통제 전체의 설계와 운영 효과를 결론 낼 수 없으므로 키, 모집단, 승인 테스트 자료를 요청한다.

각 발견은 다른 사례에서 다시 쓸 수 있는 검증 패턴으로 연결된다. 조기 차감은 잠금과 소각의 구분(RF-01)으로, 범위 혼입은 비율의 범위(RF-03)로, 승인 통제의 공백은 권한과 통제(RF-02)로 이어진다. 다만 패턴 식별자는 이 사례에서 얻은 질문을 재사용하기 위한 연결일 뿐, 같은 문제가 반복되었다는 판정은 아니다. 발견 옆에 근거와 패턴, 영향받는 모듈을 함께 적어 두면, 보고서를 읽는 사람이 세부 자료를 모두 읽지 않아도 검토 경로를 따라갈 수 있다.

종합 판단: 정합성은 조건부 채택, 나머지는 별도 증거가 필요하다

종합 판단은 계산 결과와 전문 판단의 범위를 구분해 정리했다. 대사 결론으로는 준비자산과 보고 목적의 상환의무를 각각 1,200만으로 조정해 100%를 얻었다. 발행 통제에 대해서는 업그레이드 승인과 별도 발행자를 구분했으며, 승인 한 건만으로 기간 전체의 운영 효과성이나 키의 독립성을 확정할 수 없다고 판단했다. 모듈별로는 회계(M2)가 범위와 상태의 대사를, IT감사(M5)가 권한과 승인을 맡고, 규제(M1)와 조세(M3)는 관할·고객·거래 자료를 요청하며, 구조화(M4)는 지급·소각·실패 절차를 설계한다. 결론의 범위를 정리하면 자료 사이의 정합성은 '조건부 채택'이고, 자산의 존재·무담보성·권리 집행·상환능력은 별도의 증거가 필요하다.

후속 조치에는 '추가 확인 필요'라고만 적지 않고, 무엇을 받으면 어떤 판단을 다시 할 수 있는지를 쓴다. 예컨대 승인 기록의 모집단이 확보되면 건별 대사의 범위를 정할 수 있지만, 서명자의 독립성을 설명하려면 별도의 운영 자료가 필요할 수 있다. 이 사례의 개선·검증 계획은 재무 담당이 T0+2영업일 안에 대기 의무와 계좌 범위를 반영해 보고를 수정하고 원장을 대사하며, 운영 담당이 다음 상환 배치에서 요청·지급·소각·실패 상태를 고객 청구권과 연결하고, 기술·리스크 담당이 T0+5영업일 안에 발행·변경 모집단과 키·승인·우회·한도를 검토하며, 전문 담당이 외부에 활용하기 전 관할과 기준별 권리·회계·조세 판단을 별도로 작성하는 것으로 정했다(담당과 기한은 예시). 약관·구현·권한의 변경, 지급·소각의 실패, 계좌 범위나 제약의 변경, 새로운 관할이나 거래 유형이 생기면 다시 검토한다.

형식이 다른 출력을 늘려도 증거는 늘지 않는다

마지막으로 이 사례는 도구 입력의 계보가 왜 중요한지를 보여준다. 같은 원문을 도구별 형식으로 바꾸어 받아도 독립된 증거가 새로 생기는 것은 아니다. 예를 들어 노드 형식의 공급량 1,200만(V-T01)과 SQL 형식의 대기 주소 40만(V-T02)은 모두 체인 스냅샷(V-D03)을 다시 표현한 것이고, 원장·계좌 CSV의 1,160만과 1,230만(V-T05)은 보고서(V-D02)를 다시 표현한 것이다. 귀속 라벨 '발행사 A 관련'(V-T03)은 라벨 표시와 실제 통제의 추론을 분리해야 하고, 정적 분석 형식의 '별도 minter'(V-T04)는 탐지 결과와 실제 영향을 구분해 권한·실행·승인 자료와 연결해야 한다.

이벤트 집계와 원장의 재표현이 같은 자료에서 나왔다면 둘을 교차 확인한 것처럼 세지 않는다. 변환 과정에서 원문에 없던 정보가 가정으로 추가되었다면 그 위치를 표시한다. 이렇게 입력의 계보를 유지하면 형식이 다양한 출력 때문에 증거가 풍부해 보이는 착시를 줄일 수 있다. 이 사례에서 판단을 바꾼 것은 도구의 개수가 아니라, 추가 자료 V-D06·V-D07과 권한의 연결이었다. 여기에 등장하는 도구 입력은 모두 가상 자료를 재표현한 예시이며, 특정 제품을 실제로 실행한 출력이 아니다.

제3부 · 3.4 국내 발행통제 · 가상 사례

같은 100,000의 차이도, 원인을 나누면 조치가 달라진다

자료 · 가상 범위 · 서술·계산

가상 기관의 토큰화 증권에서 발행 승인, 권리 원장, 토큰 공급량 사이에 차이가 생겼다. 이 사례는 그 차이가 어디서 발생했고 어떤 결론까지 가능한지를 묻는다. 모든 기관명, 거래, 승인, 원장, 수량, 권한 기록은 교육용 가상 입력이며, 실제 금융회사나 계좌관리기관의 시스템을 점검한 사례가 아니다.

이 사례를 읽기 전에 제도적 맥락을 먼저 짚어 둔다. 금융위원회는 토큰증권 제도화를 위한 개정 법률의 시행일을 2027년 2월 4일로 안내하고 있다(부록 D 사례 출처 S2). 따라서 이 사례는 시행을 준비하는 단계에서의 통제 설계 연습이다. 현행 의무를 위반했는지, 혹은 아직 확정되지 않은 하위 규정을 준수하는지를 판정한 사례로 사용해서는 안 된다. 실제로 적용할 때에는 적용 법률과 시행일, 최종 하위 규정, 증권의 종류, 계좌관리 방식과 기관의 역할을 먼저 확정해야 하며, 체인 위의 공급량과 법적 발행잔액을 같은 개념으로 전제해서도 안 된다.

분석의 전제는 다음과 같이 고정했다. 대상은 가상 기관 A의 단일 토큰화 증권 클래스이고, 작성과 검토는 Vanzi가 했으며 독립 검토는 수행하지 않았다. 가상의 기준시각은 2026년 11월 18일 0시(UTC)이며 모든 입력이 같은 시각을 기준으로 한다고 가정했다. 가상 계약에서는 토큰 1개가 승인된 권리 1단위에 해당한다고 가정했지만, 이것은 법적 효력에 관한 실제 판단이 아니다. 대상 범위는 생산망의 단일 클래스·단일 계약이며 브리지, 래핑, 테스트망, 부분권리, 분할·통합은 없는 것으로 가정했다. 검토 관점은 통제·시스템(M5)과 규제 질문(M1)이고, 기능 카드는 발행(FC-A01), 역할(FC-C02), 변경(FC-E01)을 사용했다. 검토할 주장은 수량 대사, 승인과 실행의 일치, 권한 통제, 법적 권리, 회계 영향의 다섯 가지다.

세 잔액은 모두 다르다

기초 시점에는 권리 원장과 토큰 공급량이 모두 1,000,000으로 일치했다. 이후 네 건의 사건이 있었다. 승인 A에 따라 150,000이 원장에 반영되고 토큰도 발행되었다. 승인 B에 따라 50,000이 발행되었지만 원장에는 반영되지 않았다. 권한 주소가 대응하는 승인이나 원장 기록 없이 50,000을 추가로 발행했다(X). 그리고 적법한 소각과 권리 감소를 가정한 50,000이 승인·원장·토큰에서 모두 일치하게 처리되었다. 이 결과 승인을 기준으로 기대되는 권리잔액, 실제 권리 원장, 토큰 공급량이 모두 달라졌다(도표 3-11).

도표 3-11 세 잔액의 대사

잔액	산식	결과
승인 기준 기대 권리잔액	1,000,000 + 200,000 − 50,000	1,150,000
실제 권리 원장	1,000,000 + 150,000 − 50,000	1,100,000
토큰 공급량	1,000,000 + 250,000 − 50,000	1,200,000
토큰 − 원장	**원장 미반영 50,000 + 승인 미대응 50,000**	**100,000**

가상 입력 H-K01~H-K04. 수량·거래 ID·기준시각·클래스가 일치한다는 전제 아래의 계산이다. H-K01~H-K07은 이 교육 사례에 부여한 입력·가정 식별자로, 실제 관찰 사실(F)이나 증거로 재표기하지 않는다.

토큰 공급량과 권리 원장의 차이 100,000은 성격이 다른 두 부분으로 나뉜다. 50,000은 승인과 발행은 있었지만 원장에 반영되지 않은 차이(B)이고, 나머지 50,000은 승인도 원장 기록도 없는 발행(X)이다. 고정된 입력 안에서 이 산술 분해는 확정이다. 그러나 여기에는 중요한 단서가 붙는다. 일반적으로 '승인서가 없다'는

관찰과 '실제로 승인이 없었다'는 사실은 다르다. 승인서가 다른 곳에 보관되어 있거나 긴급 절차로 처리되었을 수도 있기 때문이다. 이 사례에서는 제공된 승인 모집단이 완전하고 X에 대한 승인이 없다고 명시적으로 가정했기 때문에 X를 승인 미대응 발행으로 분류할 수 있었다. 실제 사례라면 체인 이벤트의 완전성, 실패·재조직·재발행, 원장의 컷오프, 취소·소각의 효력부터 검증해야 하며, 현재의 차이를 곧바로 법적 의미의 초과발행으로 단정해서는 안 된다.

기술적 한도 안이라도 승인 통제를 벗어날 수 있다

차이의 원인을 이해하려면 권한의 경로를 봐야 한다. 가상의 정책은 모든 발행을 내부 승인자 두 명의 승인 뒤에 실행하도록 정했고, 정상 경로는 승인자 → 실행자 → minter 주소 → mint 호출 → 토큰 잔액으로 이어진다. 권리 원장은 이와 별도의 반영 절차를 거친다. 그런데 가상 입력에서는 minter 주소가 단독으로 mint를 호출할 수 있고 가상의 한도는 300,000이라고 가정했다. X의 발행량 50,000은 이 기술적 한도 안에 있었다. 이 사례가 보여주는 것은, 온체인 한도를 넘지 않았다는 사실이 내부 승인과의 일치를 보장하지 않는다는 점이다. 정책과 실제 실행 경로 사이에 통제 설계상의 공백이 있는 것이다. 다만 키의 소유자, 위임, 업그레이드 경로에 관한 실제 자료가 없으므로 이 공백을 특정인의 법적 책임으로 귀속시키지 않는다.

이 공백을 검증하려면 몇 가지 통제 질문에 답해야 한다. 승인 식별자가 실행 요청과 원장 기록에 똑같이 남는가. 중복과 재시도가 차단되는가. 한도와 권한을 바꿀 때에도 승인이 필요한가. 우회 경로, 긴급 권한, 업그레이드가 통제를 무력화하지 않는가. 나머지 두 주장은 판단을 유보했다. 법적 권리에 관해서는 '토큰 1개 = 권리 1단위'라는 가정 외에 실제 법률 자료가 없으므로 실제 초과발행 여부, 투자자의 권리, 대항력은 판단하지 않았다. 회계 영향에 관해서도 실제 계약, 발행대금, 상환, 총계정원장이 없으므로 분개, 손익, 부채 금액을 확정하지 않았고, 수량 차이를 손실액으로 바꾸어 읽지 않았다.

발견에서 조치까지

네 개의 발견에는 각각 다른 조치가 따른다. 원장 미반영 50,000(D-K01)은 원장과 고객 권리잔액을 왜곡할 수 있으므로, 원장 운영 담당이 승인 B의 결제·배분·컷오프를 확인한 뒤 정정 여부를 결정한다. 이때 B가 중복되거나 취소된 것은 아닌지, 권리가 유효한지를 확인하고 정정 이력과 정정 전후의 대사 차이를 보존한다. 승인 미대응 50,000(D-K02)은 발행 통제가 우회될 수 있다는 뜻이므로, 발행 통제·기술·법무 담당이 사건을 보존하고 권한, 키, 대체 승인을 조사한 뒤 필요한 조치를 검토한다. 종결하려면 승인 모집단, 위임, 긴급 절차, 테스트 여부를 검증하고 적법한 시정 조치와 재대사를 거쳐야 한다.

minter가 한도 안에서 단독 실행할 수 있다는 점(D-K03)은 수량 한도와 승인 통제가 어긋나 있다는 발견이다. 통제 설계자가 승인과 실행의 연계, 역할 분리, 독립 대사, 예외 경보를 검토하고, 정상·미승인·중복·우회·권한변경 시나리오를 테스트한 뒤 독립 검토를 받는다. 권리와 회계 영향이 확정되지 않았다는 점(D-K04)에 대해서는 법무·회계 담당이 계약, 등록, 대금, 고객 원장, 총계정원장을 확보하고, 권리자·의무·금액·시점·적용 기준을 확정한 뒤 법률과 회계의 결론을 별도로 작성한다.

범위별 결론은 다음과 같다. 가상 자료 기준의 계산에서 100,000의 차이는 원장 반영 누락과 승인 미대응 발행으로 분해된다. 통제 설계 면에서는 가상 정책과 단독 실행 경로 사이에 공백이 있다. 그러나 실제 위법성, 자산 손실, 회계 오류 금액, 통제의 운영 효과성은 이 자료로 확정할 수 없다.

시정 이후의 기대치도 실행 결과가 아니라 조건부 기대치로만 제시한다. 유효한 B의 50,000을 원장에 반영하고 X의 50,000을 적법하게 해소한다는 조건이라면 기대 권리, 원장, 공급량은 각각 1,150,000이 된다. X의 해소는 임의 소각 지시가 아니며, 권리·계약·적법 절차를 확인한 뒤 결정한다. 이 사례에서 수행한 것은 가상 입력의 계산과 표 작성뿐이며, 시스템 변경, 권한 회수, 소각, 원장 수정, 고객 통지, 통제 테스트는 실제로 수행하지 않았다.

제4부 · 4.1 동작에서 회계까지

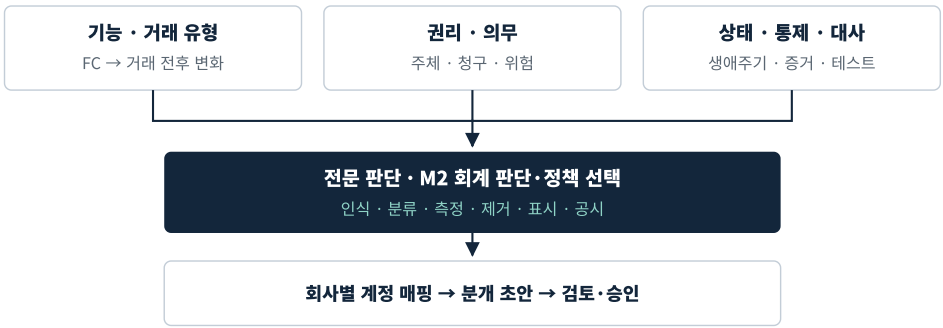
transfer 기록 하나만으로는 매각과 자기 지갑 이동을 구별할 수 없다

기술적 동작이 곧바로 회계 계정으로 이어지지는 않는다. 제4부는 체인 위의 동작을 거래, 권리, 상태로 해석한 뒤에야 회계 정책과 계정 매핑을 검토하도록 연결하는 방법을 다룬다. 이 과정에는 동작의 이름만 보고 분개를 고르는 지름길이 없다.

같은 토큰 이전(transfer)도 경제적으로는 전혀 다른 사건일 수 있다. 자기 지갑 사이의 이동일 수도, 다른 자산을 받고 내준 매각일 수도, 투자나 담보 제공일 수도 있다. 체인 기록은 토큰이 한 주소에서 다른 주소로 옮겨졌다는 사실을 보여줄 뿐, 그 대가로 무엇을 받았는지, 상대방이 누구인지, 통제와 권리가 어떻게 바뀌었는지는 알려주지 않는다. 따라서 이 세 가지를 확인해 경제적 사건을 먼저 정한 다음에야 회계 판단을 시작할 수 있다.

이 연결은 세 갈래의 분석이 하나의 전문 판단으로 모이는 구조다(도표 4-1). 기능 카드로 파악한 동작과 거래 전후의 변화, 권리·의무의 주체와 청구 내용과 위험, 그리고 상태의 생애주기와 통제, 증거, 테스트가 회계·감사·보증 모듈(M2)의 판단으로 모인다. M2는 인식, 분류, 측정, 제거, 표시, 공시를 판단하고, 그 결과가 회사별 계정 매핑과 분개 초안, 검토와 승인으로 이어진다.

도표 4-1 동작에서 회계 기록까지의 연결



자료: Chain Prism OCP v1.0. 규칙·계정 필드와 구현 상태는 부록 A·B.

이 장은 새로운 단계나 모듈을 추가하지 않는다. 6단계와 M1~M5는 그대로 유지하고, 기존 양식에 붙는 첨부 도구로 연결한다. 거래 유형과 권리 구조는 3단계에서 동작을 경제적 거래와 권리·의무로 연결하는 거래구조표(F-03)의 첨부다. 생애주기와 통제 테스트는 2~5단계에서 상태, 시점, 예외, 설계, 운영을 검토하는 불일치·추가 확인표(F-05)의 첨부다. 회계 규칙, 계정, 분개는 M2 판단 뒤에 계정 매핑과 분개 초안, 보고 근거를 연결하는 판단 기록(F-04)과 결론 요약서(F-06)의 첨부다. 기록은 기존의 사례·판단·증거 식별자를 그대로 재사용한다.

이 단계들은 자동화의 입력 조건을 만드는 과정이기도 하다. 그래서 원칙 하나를 분명히 둔다. 사실이 부족하면 회계 계정이 아니라 보완 질문이 출력되어야 한다.

제4부 · 4.2 거래 유형

거래는 이벤트의 이름이 아니라, 무엇이 변했는지로 분류한다

거래 분류는 이벤트 이름보다 어떤 자산·권리·의무가 변했는지에서 시작한다. 여러 트랜잭션이 하나의 거래를 이룰 수도 있고, 하나의 실행 안에 여러 경제적 사건이 들어 있을 수도 있다.

도표 4-2의 유형표는 거래의 후보를 좁히기 위한 도구다. 분류는 각 거래의 계약, 대가, 통제 조건을 확인한 뒤에 확정한다. 예를 들어 토큰을 어떤 프로토콜에 맡긴 거래는 보관일 수도, 투자일 수도, 대여일 수도 있으며, 받은 토큰에 어떤 권리와 회수 조건과 위험이 붙어 있는지를 확인해야 셋 가운데 무엇인지 알 수 있다. 담보를 설정한 거래라면 어떤 권리를 유지하고 제한하고 이전했는지를 따져야 하며, 자산을 장부에서 제거할지는 별도로 판단해야 할 수 있다.

도표 4-2 후보 거래 유형과 구분할 변화

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?

거래구조표(F-03) 첨부. 자료: Chain Prism OCP v1.0.

거래 한 건을 기록할 때에는 다섯 묶음의 정보를 고정한다. 관점과 식별(사례·경제적 사건 식별자, 보고기업, 거래 당사자, 연결된 기능 카드와 검증 패턴, 기준일), 거래 전후의 변화(보유 자산·청구권·의무·통제·위험과 수량·금액·단위), 구조와 대가(주고받은 자산, 계약상 대가, 현금흐름, 다른 거래와의 조건부 연결), 근거와 대안(주장 식별자, F/I/H, 증거, 가능한 다른 해석과 그것을 구분하는 증거), 그리고 결과와 상태(선택한 유형 또는 미분류·추가 확인, 판단 식별자, 관점, 한계, 검토자)다.

여기서 경제적 사건 식별자(economic_event_id)는 원본 트랜잭션을 대체하지 않는다. 체인, 거래 해시, 로그 인덱스, 내부 원장의 행을 다대다로 연결하고, 무엇을 묶고 무엇을 나누었는지 그 이유를 남긴다. 이 원칙이 중요한 이유는 중복 인식을 막기 위해서다. 토큰의 이동, 발행(mint), 소각(burn)이 기록에 따로 나타난다고 해서 각각을 독립된 회계 사건으로 자동 계산해서는 안 된다. 그것들이 하나의 경제적 사건을 구성하는 기술적 단계인지를 먼저 검토하지 않으면, 같은 거래를 두 번 인식하고 두 번 분개하는 오류가 생긴다.

제4부 · 4.3 권리·의무 구조

기초자산이 같아도, 투자자가 가진 권리가 다르면 다른 상품이다

토큰 잔액, 기초자산, 투자자의 청구권, 시장가격은 서로 다른 대상이다. 권리·의무 구조를 같은 항목으로 비교하면 토큰의 표시와 실제 권리 구조 사이의 차이가 드러난다.

같은 건물을 기초로 한 토큰이라도 투자자가 건물 자체의 지분을 가진 것인지, 건물을 보유한 특수목적기구(SPV)의 지분을 가진 것인지, 그 기구에 대한 채권을 가진 것인지에 따라 현금흐름도, 위험도, 회계 검토의 전제도 달라진다. 이 때문에 Chain Prism은 자산 자체, 발행기구의 지분, 채무 청구권을 같은 것으로 취급하지 않는다. 토큰 수량이나 기초자산의 명칭을 같게 맞추는 것만으로는 비교가 되지 않는다. 투자자가 받는 현금흐름, 우선순위, 환매·상환 조건, 남는 위험이 다르면, 같은 자산을 바탕으로 하더라도 서로 다른 청구권이다.

그래서 권리 구조는 언제나 같은 순서의 항목으로 비교한다(도표 4-3). 누가 누구에게 청구하고 지급하는지, 권리의 대상이 무엇인지, 수익과 상환은 어떤 산식과 조건을 따르는지, 담보와 우선순위는 어떻게 되는지, 토큰 이전 외에 권리가 성립하기 위한 다른 요건이 있는지, 누가 통제하고 위험을 부담하는지, 종료나 부실 시에는 어떻게 처리되는지를 차례로 묻고, 마지막으로 계약 조항과 코드 로직과 실제 지급 기록 사이의 연결을 확인한다.

도표 4-3 권리·의무 구조의 비교 항목

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.

거래구조표(F-03) 첨부. 자료: Chain Prism OCP v1.0.

같은 자산을 놓고 구조화 대안을 비교할 때에는 무엇을 고정하고 무엇을 바꾸었는지를 먼저 밝힌다. SPV 지분, 신탁수익권, 채권을 비교한다면 기초자산과 경제적 가정은 가능한 한 고정하고, 투자자의 권리, 비용, 차입, 우선순위, 회수 절차의 차이를 명시한다. 가치평가와 연결할 때에는 어느 주체의 어떤 현금흐름을 평가하는지를 먼저 정한 뒤, 현금흐름할인(DCF), 순자산가치(NAV), 분배 순서(워터폴)의 가정을 권리 구조와 연결한다. 학습용으로 설계한 대안은 실제로 법적으로 성립하는지, 실현 가능한지와 구분해 기록한다.

제4부 · 4.4 생애주기

“상태가 바뀌었으니 분개한다”는 규칙은 쓰지 않는다

거래의 기술적 상태가 바뀌는 순간과 장부에 반영할 사건이 생기는 순간은 같지 않을 수 있다. 요청, 잠금, 승인, 지급, 소각을 구분해야 어느 시점에 어떤 권리와 의무가 남아 있는지를 물을 수 있다.

상환을 예로 들어 보자. 보유자가 상환을 요청하고 토큰이 잠기는 것, 발행사가 현금을 지급하는 것, 토큰이 소각되는 것은 각각 다른 시점에 일어날 수 있다. 그리고 이 가운데 어느 사건이 의무를 소멸시키는지는 기술이 아니라 계약과 회계 기준과 회사의 정책이 정한다. 만약 지급이 먼저 완료되고 소각이 나중에 이루어진다면, 그 사이에는 토큰 공급량과 회계상 의무가 잠시 다를 수 있다. 이 차이는 시점의 차이일 수 있으므로 곧바로 오류로 보거나 새 분개로 처리하지 않고, 왜 다른지를 대사로 설명한다.

그래서 이 프레임워크는 상태의 전환 자체를 분개의 근거로 삼지 않는다. 승인된 회계정책에 비추어 그 상태가 인식, 제거, 재분류 가운데 어느 사건에 해당하는지를 먼저 판단한다. 도표 4-4는 실제 상품의 순서를 복원할 때 확인할 상태의 후보이며, 모든 상품에 강제되는 공통 순서가 아니다.

도표 4-4 상태·사건의 후보와 확인할 내용

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

불일치·추가 확인표(F-05) 첨부. 자료: Chain Prism OCP v1.0.

상태 전환 한 건을 기록할 때에는 식별과 관계(경제적 사건과 요청 식별자, 이전·다음 상태, 연결된 거래·로그·원장 행), 전환 조건(누가 어떤 시간·가격·승인·외부 지급·예외 조건으로 변경하는지), 시점과 증거(요청·실행·정산·회계 효력의 시점, 시간대와 블록, 증거와 F/I/H), 수량과 금액(토큰 수량·현금·청구권·의무 잔액과 단위, 미결·중복·취소 조정), 책임과 결과(담당, 통제, 미확인 사항, 후속 조치, 판단 식별자와 분개 초안 식별자, 인식 근거)를 남긴다. 이 생애주기 기록이 미완료, 실패, 재시도, 그리고 결산일의 차이를 설명하는 연결 고리가 된다.

제4부 · 4.5 통제 테스트

통제는 존재, 설계의 적절성, 기간 중 운영 효과성을 나누어 판단한다

기능이 설계되어 있다는 것과 실제 기간 동안 작동했다는 것은 다르다. 테스트 환경에서 한도가 작동했다는 결과는 운영 기간의 승인 기록이 완전하다는 증거를 대신하지 못한다.

통제 검토는 기능 카드에 통제 테스트를 붙이는 방식으로 진행한다. 각 테스트에는 그 통제가 막거나 탐지하려는 오류, 무단 행위, 누락, 중복, 변경을 먼저 적고, 정상적인 승인·실행 순서와 함께 예외, 대체 권한, 모듈, 외부 호출, 긴급 경로 같은 우회 경로를 기록한다. 실행 범위(대상 코드·블록·기간, 설계 검토·테스트·운영 검토 가운데 무엇인지, 모집단·표본·선정 근거), 기대 결과와 실제 결과, 테스트 환경과 재현 방법, 그리고 설계와 운영 각각의 결론과 보완 조치를 남긴다.

테스트 결과에는 사용한 코드, 환경, 입력과 기대 결과를 함께 남겨야 한다. 권한 없는 호출이 거절된 사례와 권한 변경 후 허용된 사례를 나란히 비교하면 통제가 어느 경로에 적용되는지 설명하기 쉽다. 그러나 실제 운영 이력이 필요한 질문은 이런 실험 결과와 분리해 추가 자료로 확인해야 한다. 도표 4-5는 발행 한도(FC-A01)를 예로 세 관점의 점검을 보여준다.

도표 4-5 예시: 발행 한도(FC-A01)의 세 관점 점검

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 비교한다. 예상과 실제 결과를 기록한다.
운영 검토	분석 기간의 가용 발행·변경 모집단과 승인 기록을 연결한다. 표본·누락·실제 키 운영의 한계를 명시한다.

불일치·추가 확인표(F-05) 첨부. 자료: Chain Prism OCP v1.0.

세 관점의 결과는 반드시 따로 기록한다. 설계가 적절하다는 결론, 테스트 환경에서 의도대로 작동했다는 결론, 분석 기간 동안 실제로 운영되었다는 결론은 서로 다른 증거를 요구하기 때문이다. 표본, 누락, 예외와 함께, 그 결과를 실제 운영으로 어디까지 확대해 말할 수 있는지도 남긴다.

제4부 · 4.6 회계 판단과 계정 매핑

회계 알고리즘은 토큰 이름을 계정코드로 바꾸는 사전이 아니다

회계 처리는 조건을 하나씩 확인하는 의사결정 절차에 가깝다. 거래의 실질과 적용 기준·정책이 정해져야 인식, 측정, 제거와 계정 매핑을 검토할 수 있다. 필수 사실이나 승인된 규칙이 없으면 분개 초안이 아니라 보완 질문을 먼저 만든다.

판단은 일곱 단계를 거친다(도표 4-6). 먼저 보고기업, 별도·연결의 관점, 회계기준, 기준일, 정책의 버전을 고정하고, 거래 유형·권리·의무·생애주기와 증거의 연결을 확인한다. 그 위에서 인식, 분류, 측정, 제거·재분류, 표시·공시의 순서로 회계 판단을 내리고, 적용 조건·제외 조건·유효기간·근거·승인 상태를 비교해 적합한 규칙을 고른다. 이어 공통 회계 개념을 회사의 계정코드와 보조계정, 차원에 연결하고, 금액·시점·환율·수수료·단위·차대 균형·중복·원장 대사를 확인해 분개 초안을 만든 뒤, 초안의 승인과 전기 가능 여부, 남은 공시·결산 과제를 기록한다.

도표 4-6 회계 판단에서 분개 초안까지의 일곱 단계

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

판단 기록(F-04) 첨부. 자료: Chain Prism OCP v1.0.

이 절차를 거친 거래는 세 가지 상태 가운데 하나가 된다. 핵심 사실, 승인된 정책, 활성 규칙과 매핑, 검산이 모두 갖춰진 반복 거래는 '자동 처리 가능'으로 분류되며, 실제 처리는 조직의 별도 권한 설정을 따른다. 규칙이 서로 충돌하거나, 새로운 거래이거나, 대안 해석이나 예외나 정책 변경이 있는 경우는 '검토 필요'로 분류해 근거와 후보를 제시하고 전문가가 검토한다. 주체, 권리, 금액, 적용 기준 같은 핵심 자료가 부족한 경우는 '판단 보류'로 두고, 계정을 억지로 고르지 않은 채 추가 자료를 요청한다.

여기서도 두 가지 판단을 나눈다. 핵심 사실이 얼마나 충실하게 확보되었는지와, 그 사실에 대한 해석이 얼마나 명확한지다. 사실은 충분해도 해석이 갈릴 수 있고, 해석은 명확해도 사실이 부족할 수 있다. 그리고 인식이나 분류가 확정되지 않았다면 계정과 분개도 확정하지 않는다.

제4부 · 4.7 시범 ① · 가상

자기 지갑 사이의 이동은 총계정 분개 없이 위치만 바뀔 수 있다

자료 · 가상 카드 · 관련 카드 시드 범위 · 계산·분개 초안

이 시범은 같은 주체가 통제하는 두 지갑 사이의 이동을 가정한다. 체인 위에서 이전이 일어나도 새로운 상대방과의 거래가 없다면, 기존 장부금액의 위치만 보조원장에서 바뀔 수 있다. 기업 A의 관점에서, 권리와 통제가 그대로이고 수수료가 0인 상황을 가정한다.

기업 A가 통제하는 지갑 W1에서 W2로 10단위가 이동했다. 제3자 수탁이나 담보, 교환이 아니며 실질적인 권리나 위험의 변화가 없다고 설정한다. 완료된 거래, 원장의 행, 키 운영 자료가 모두 같은 이전을 가리킨다고 가정했으며, 이전 기능 카드(FC-B01)의 상세 검토나 실행 검증은 수행하지 않았다. 가상의 정책(P-A01)은 기존 자산의 분류와 장부금액을 유지하고 위치만 바꾸며, 같은 총계정 아래 지갑별 보조원장을 쓰도록 정한다.

기초에 W1은 20단위(장부금액 1,000), W2는 0단위였고, 이전하는 10단위의 장부금액은 500으로 설정했다. 처리 결과 W1은 10단위와 500이 줄고 W2는 10단위와 500이 늘어나, 전체로는 20단위와 1,000이 그대로 유지된다. 총계정에는 새로운 분개가 없고 보조원장의 이동만 기록된다. 처리의 추적은 경제적 사건(V-A01-E1) → 가상 정책(P-A01) → 규칙(V-A01-R1·v0.1) → 매핑(V-A01-M1) → 기록(V-A01-J1, 총계정 분개 없음)으로 이어진다. 가상 자료의 가정과 그 안의 계산 결과를 실제로 확인된 사실로 바꾸어 표시하지 않는다.

이 결론은 전제가 하나라도 바뀌면 그대로 이어지지 않는다. W2가 외부 수탁 주소나 담보 주소라면 권리, 통제, 의무를 다시 검토하고 거래 유형과 정책을 새로 선택해야 한다. 가스나 수수료가 발생했다면 그것은 별도의 경제적 사건이므로 측정과 계정 처리를 따로 검토한다(이 예시에는 포함하지 않았다). 그리고 두 주소가 같은 주체에 귀속된다는 자료가 없다면, 동일 주체라는 전제 자체가 확인되지 않은 것이므로 판단을 보류하고 자료를 요청한다.

제4부 · 4.8 시범 ② · 가상

상환 요청과 지급에서 부채를 두 번 줄이면, 같은 의무를 두 번 제거하게 된다

자료 · 가상 카드 · 관련 카드 시드 범위 · 계산·분개 초안

이 시범은 상환의 요청·잠금, 현금 지급, 소각을 별도의 사건으로 나눈다. 의무가 언제 줄어드는지를 정책으로 먼저 정해 두었기 때문에, 공급량과 장부상 부채가 잠시 다른 상태도 설명할 수 있다. 앞의 DEMO-USD와는 별도의 소규모 예시이며, 금액 단위는 가상의 기능통화다.

이 시범이 겨냥하는 오류는 두 가지다. 하나는 상환 요청 때 부채를 줄이고 지급 때 다시 줄이는 것이다. 그러면 같은 의무를 두 번 제거하게 된다. 다른 하나는 지급은 끝났지만 아직 소각되지 않은 상태를 단순한 공급량 비교만으로 보는 것이다. 그러면 시점의 차이를 오류로 잘못 해석하게 된다. 이 예시는 같은 권리의 생애주기와 장부상의 사건을 연결해 시점 차이와 오류를 구별하는 연습이다.

전제는 다음과 같다. 발행사 B가 수령한 자금을 통제하고, 보유자에게 액면의 현금 상환의무를 진다. 가상의 승인 정책(P-A02)은 입금과 의무 성립 시점에 은행예금과 상환의무를 인식하고, 현금을 지급하면 해당 의무가 소멸한다고 정한다. 이 분류와 제거의 결론은 실제 상품에 대한 판단이 아니며, 수수료·환율·이자·손상·세금은 없는 것으로 둔다.

도표 4-7 발행·상환의 상태와 가상 정책에 따른 분개 초안

상태·경제적 사건	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 않는다.
T1 상환 요청·잠금 100	신규 분개 없음	현금 미지급, 의무 1,000 유지. 잠금은 소각·채무 소멸과 다르다.
T2 현금 지급 100·의무 소멸	차) 상환의무 100 대) 은행예금 100	현금·의무 900. 소각 전 공급 1,000과의 차이 100은 지급·소각 시차로 대사한다.
T3 기술적 소각 100	추가 총계정 분개 없음	공급 900·의무 900. 지급과 소각을 별도의 상환으로 중복 인식하지 않는다.

자료 성격: 가상 / 범위: 계산·분개 초안. 연결: FC-A01·A02·F03, RF-01·RF-03, 규칙 V-A02-R1·R2, 정책 P-A02, 매핑 M-A02, 초안 V-A02-J1·J2.

T1에서 분개가 없는 이유는 이 가정에서 요청과 잠금이 의무를 소멸시키지 않기 때문이다. T2의 지급이 의무를 소멸시키고, T3의 소각은 이미 소멸한 의무의 기술적 마무리이므로 다시 분개하지 않는다. T2와 T3 사이에 공급량(1,000)과 장부상 의무(900)가 100만큼 다른 것은 오류가 아니라 지급과 소각의 시차이며, 대사로 설명된다. 만약 지급 완료와 청구권 소멸에 대한 근거가 없다면 T2의 분개 초안은 보류한다. 발행과 상환의 회계상 인식·제거 시점은 실제로는 계약, 기준, 정책에 따라 별도로 검토해야 하며, 이 시범의 가정은 앞의 DEMO-USD 사례에서 내린 1,200만 대사나 회계 결론을 바꾸지 않는다.

제4부 · 4.9 시범 ③ · 가상

같은 '분배'라도 이자인지 원금인지에 따라 처리가 달라진다

자료 · 가상 카드 · 관련 카드 시드 범위 · 계산·분개 초안

토큰화된 채권의 회계처리를 연습할 때에도 먼저 어떤 계약상 청구권을 보유하는지 확인해야 한다. 이 시범은 투자자 C의 관점에서, 만기 1년의 토큰화 채권을 단순화한 모델로 취득, 이자, 상환을 따라간다.

이 금융자산은 계약상 원리금에 대한 청구권이며, 상각후원가로 측정할 조건을 충족한다는 별도의 판단이 승인되었다고 가정한다. 액면과 취득가는 1,000, 연 이자율은 5%이고, 수수료·할인·할증·환율 변화와 손실충당금은 모두 0으로 둔다. 실제 상품이라면 사업모형, 현금흐름의 특성, 신용손실, 인식 시점 등을 따로 검토해야 한다. 이 시범은 계산 구조를 드러내기 위해 그 변수를 단순화했다.

도표 4-8 취득·이자·상환의 분개 초안 (가상 정책 P-A03)

거래·권리·상태	분개 초안	연결 검증
취득 조건 충족·대금 지급 1,000	차) 투자 금융자산 1,000 대) 은행예금 1,000	계약·거래일 정책·명의·토큰·지급이 같은 권리로 연결되는지 확인한다.
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 대사한다. 장부금액 0.

자료 성격: 가상. 규칙 V-A03-R1~R3·v0.1 / 매핑 M-A03(DEMO-1501·1101·4101) / 초안 V-A03-J1~J3. 공식 참고: 회계-S3.

이 시범에서 가장 중요한 점은 이벤트의 이름이다. 체인 위에서는 이자의 지급과 원금의 상환이 모두 '분배(distribution)'라는 같은 이벤트로 나타날 수 있다. 그러나 회계상으로는 이자, 배당, 원금 반환, 자본 회수가 서로 다르게 처리되며, 그 구분은 권리, 원천, 지급 조건, 적용 기준으로 해야 한다. distribution이라는 이벤트 이름만 보고 수익 계정을 고르지 않는다. 권리와 분배의 명세가 확인되지 않았다면 분배의 성격과 계정 선택을 보류하고, 계약, 산식, 명세, 발행자의 기록을 요청한다.

가정을 바꿀 때에는 금액만 고치지 말고 적용 규칙, 계정 매핑, 대사 항목까지 함께 달라지는지 확인해야 한다. 실제 사례로 확장하면 취득가격, 수수료, 신용손실, 환율, 결산 시점의 차이가 추가로 검토 대상이 될 수 있다. 그리고 상각후원가를 모든 RWA 채권의 기본값으로 사용하지 않는다. 분류, 측정, 분배의 성격이 바뀌면 규칙과 초안을 다시 선택한다.

제5부 · 5.1 현재 상태

명세가 자세하다고 엔진이 실행된 것은 아니다

제5부는 이 보고서가 실제로 무엇을 했고 무엇을 하지 않았는지, 분석이 '완료되었다'고 말할 수 있는 기준은 무엇인지, 그리고 앞으로 무엇을 검증할 것인지를 정리한다. 이 구분은 보고서의 결론만큼 중요하다.

이 보고서에는 성격이 다른 세 가지가 함께 들어 있다. 방법론을 설명한 문서, 실제로 자료를 수집한 스크립트, 그리고 앞으로 구현할 판단 지원 기능의 명세다. 이 셋은 완성의 정도가 서로 다르다. 코드가 일부 존재한다고 해서 전체 분석이 자동화된 것은 아니며, 명세가 자세하다고 해서 그 엔진이 실행된 것도 아니다. 따라서 이후의 구현과 시험 결과는 실제로 수행 범위가 늘어난 만큼만 상태에 반영한다.

도표 5-1 문서·수집 도구·자동화의 현재 상태

구분	현재 상태
분석 명세·사례	6단계, 양식, 시드 FC/RF, 거래·권리·상태·회계 명세, 가상 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 자동으로 확정하지 않는다. 실제 거래 전송, 계정 접근, 운영 시스템 전기는 수행하지 않았다.

자료: Chain Prism OCP v1.0 부록 B. 일반 실무 독자는 본문으로, 구현 담당자는 부록 A와 함께 범위를 확인한다.

사례 보완판(2026-11-18) 시점의 수행 상태도 같은 원칙으로 정리했다. 기존 부록은 가치평가 방법표와 증거 판정 절차를 제안한 것이었고, 이번 보완에서는 USDC 공개보고서를 선정해 보고서 내부의 산술을 재현하고 증거 연결표, 불일치·추가 확인표, 결론 요약서를 작성했다. 추가 RPC 조회, 은행·수탁·내부 원장의 확보, 배포 소스 대응, 독립 검토자의 재현은 수행하지 않았다. 실제 공개자료 사례(R-USDC-01)와 국내 가상 교육 사례(S-KR-ISS-01)는 섞지 않으며, 가상 자료에서 계산이 맞았다는 것이 실제 발행통제의 효과성을 입증하지는 않는다.

5.2 '완료'는 어디까지 말할 수 있는가

분석이 완료되었다는 말은 자료의 종류에 따라 다른 의미를 갖는다. 공개자료 사례에서는 공개된 범위 안에서 답할 수 있는 질문을 고정하고, 출처·판본·조회 조건·원본과 판단의 연결을 남기며, 확보할 수 없는 내부 자료는 요청 목록과 그것이 결론에 미치는 영향으로 기록한다. 공개 근거로 답할 수 있는 결론, 조건, 유보를 확정했다면 그 범위의 분석은 완료할 수 있다.

고객자료 사례의 완료에는 더 많은 조건이 붙는다. 계약된 업무 범위, 자료 제공 권한, 대상 시스템·계좌·기간, 모집단의 완전성, 내부 승인·수탁·은행 자료의 연결을 추가로 확인해야 하고, 중대한 예외와 받지 못한 자료의 영향을 평가해 검토 기록을 남겨야 한다. 여기서도 자료를 확보했다는 사실 자체가 증거의 충분성을 확정하지는 않는다.

어떤 사례든 공통으로 지켜야 할 인수 기준이 있다. 분석 범위·질문표(F-01)의 질문과 제외 범위가 결론 요약서(F-06)의 결론과 대응해야 한다. 중대한 결론에는 근거, 기준, 가정, 한계가 있어야 한다. 미해결 항목마다 영향, 담당 역할, 후속 조치, 재검토 조건을 적어야 한다. 그리고 완료와 유보는 함께 존재할 수 있다. 어떤 질문은 완료되고 어떤 질문은 유보된 상태로 분석이 끝날 수 있다는 뜻이다.

USDC 사례에 이 기준을 적용하면 다음과 같다. 준비자산 보고서의 판본·시점·정의 확인, 문서 내부 계산, 주장별 증거 연결과 결론 범위 기록은 완료했다. 동일 시점의 전체 체인 재조회, 배포 코드와 권한 운영의 대조, 내부 준비자산 원장과 은행 확인, 독립 재현은 수행하지 않았다. 따라서 R-USDC-01 전체를 검증 완료로 표시하지 않는다.

독립 재현은 완료의 마지막 단계다. 다른 검토자가 같은 입력, 버전, 실행 지침으로 같은 관찰값과 계산을 재현하고, 판단에 대해서는 근거가 타당한지를 검토한다. 이때 관찰값이 일치하는 것과 전문 판단이 일치하는 것은 따로 기록한다. 실제 완료일, 결과, 차이, 수정 이력도 남긴다. 이번 보완에는 독립 검토자의 서명이 없다.

5.3 후속 과제: 발전은 분량이 아니라 적용 결과로 결정한다

OCP v1.0은 현재의 분석 절차와 공개자료 적용 범위를 묶은 기준판이다. 회계·준법·AML·IT감사 실무자를 위한 학습·적용 매뉴얼로서 본편과 개발·운영 부록으로 구성되었고, 자료 성격·카드 상태·수행 범위의 세 축으로 범위를 표시하며, 각 결론에 구체적인 증거의 한계를 기록했다. 실제 사례로는 USDC의 분석 범위와 고정 블록 관찰을 진행본으로 통합했고, 교육 사례로는 DEMO-USD를 통해 최초 자료에서 추가 자료를 거쳐 판단이 수정되는 과정을 제시했다. 기능 카드는 네 개의 시드 카드와 귀속 체크리스트, 복합 Web3 확장 계획으로 구성되어 있다.

이후의 발전은 분량이나 카드의 수가 아니라 실제 사례에서 확인한 누락, 반례, 재현성 문제를 근거로 결정한다(도표 5-2). USDC 실증은 배포 소스 대응, 통제맵, 샘플 거래, 준비자산 보고 범위를 확인해 실제로 확보한 범위만 반영한다. 규제(M1)와 조세(M3)는 공통 흐름과 과세·보고의 분리, 조건부 분기를 1.7절에 수록했으며, 관할별 규정·사실·증거의 적용과 국내 규제·조세 부록은 후속 과제로 남는다. 양식과 카드는 1.6절의 주체 귀속 절차를 사례에 적용해 개선하고, 관련 기본 기능을 보강한 뒤 확장 카드를 단계적으로 검토한다. 출처, 기준일, 버전, 가정, 원본을 보존하고, 추가 자료나 코드 변경으로 바뀐 판단은 이력으로 추적한다.

도표 5-2 다음 시범 구현과 검증 계획

범위	계획·완료 조건
입력·처리	JSON·CSV 가상 데이터 → 필수·참조 검증 → 사전 규칙 → 계정 매핑·분개 초안 또는 무분개·보류.
세 사례	자기 지갑 이전, 발행/상환, RWA 채권 취득/분배를 사용한다. 정상 조건과 누락·규칙 충돌·중복·기간 차이를 비교한다.
재현·책임	차대·수량·기초/기말·원본 연결을 검산한다. 정책·규칙·매핑·코드·데이터 버전과 검토·승인·전기 상태를 분리한다.
공통 기록	사건·주장·증거·권리·상태·판단·규칙·매핑·초안을 ID로 연결한다. 누락·미확인·비적용을 구분한다.
검증·변경	조건 충족·반례·결측·규칙 충돌·중복·시점·역분개를 시험한다. 과거 버전과 변경 영향을 기록한다.
승인·권한	규칙 설계·정책 승인·초안 검토·실제 전기의 책임을 구분한다. 활성화·변경·수동 수정 이력을 보관한다.
다음 사례	세 시범 사례를 실제 공개 자료로 확장한다. 외부 자료가 부족하면 가정을 유지하고 실제 검증 범위를 과장하지 않는다.
저장소·문서	코드·입력·검증 기록·실행 방법은 저장소에, 문서에는 범위·결과·한계·버전 연결을 둔다. 실제 공개 전에는 URL을 만들지 않는다.

자료: Chain Prism OCP v1.0 부록 B·C, v1.0 발전 계획.

구현이 완료되면 실제로 구현하고 검증한 기능만 릴리스, 커밋, 검증 기록과 함께 표시한다. 특히 '가상 데이터 기반의 계정 매핑·분개 초안 시범 구현'과 '실제 회계 판단·운영 연동·자동 전기의 완료'는 전혀 다른 수준의 주장이므로 반드시 구분한다. 현재 업무 자동화는 구현되지 않았으며, 공개자료 수집의 실제 수행 기록과 회계 시범 엔진의 향후 계획을 섞지 않는다. 자료의 충분성, 해석의 명확성, 남은 위험은 각각 따로 판단한다.

부록 A · 회계 규칙과 계정 명세

회계 규칙은 결론만이 아니라 적용 조건과 멈춤 조건까지 저장한다

이 부록은 4.6절의 회계 판단을 재사용 가능한 규칙과 계정 매핑으로 표현하기 위한 명세다. 사람이 검토한 판단을 조건, 분기, 출력, 시험 사례로 옮기는 양식이며, 구현이 완료되었다는 뜻이 아니다.

규칙을 재사용하려면 결론만 저장해서는 안 된다. 필수 증거가 없거나 정책·기준의 버전이 달라졌을 때 같은 초안을 내보내지 않도록, 적용 조건과 멈춤 조건을 함께 저장해야 한다. 조건은 분석자가 읽을 수 있는 문장과 기계가 확인할 수 있는 필드로 함께 표현하는 편이 좋다. 다만 숫자 필드가 채워졌다고 판단의 전제가 충족되는 것은 아니므로, 승인된 정책과 증거의 상태도 연결한다. 규칙 시험에는 정상 입력뿐 아니라 누락, 충돌, 경계값, 중복 사건이 어떻게 처리되는지도 포함한다.

도표 A-1 회계 규칙 1건의 고정 양식

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

판단 기록(F-04) 첨부. 공식 기준 참고: 회계정책 선택·판단은 회계-S2, 금융상품 인식·분류·측정의 개요는 회계-S3.

규칙을 활성화하기 전에는 조건을 충족하는 예시와 충족하지 않는 반례를 함께 검토하고, 회사 정책과 규칙의 승인·버전을 고정한다. 자산·부채 분류, 측정 기준, 계정 매핑은 각각 검토하며, 변경되면 영향을 받는 사례와 초안을 추적한다. 사례별 판단과 규칙의 승인 상태도 분리한다. 표준의 요약 페이지를 확인했다는 사실이 개별 거래의 회계정책 검토와 승인을 대신하지는 않는다.

공통 회계 개념과 회사 계정코드는 다른 층위다

같은 회계 개념도 회사의 계정체계, 보조원장, 거래 차원에 따라 다른 코드로 연결될 수 있다. 그래서 매핑과 분개 초안의 기록은 어느 정책·규칙·자료를 사용했는지를 추적하고, 승인 전의 초안과 실제 장부 반영을 구분하는 데 목적이 있다. 초안에는 금액과 차변·대변 외에 해당 사건과 규칙·매핑의 버전을 연결한다. 나중에 정책이 바뀌거나 거래가 취소되었을 때 어떤 초안을 다시 검토해야 하는지 찾기 위해서다. 실제 장부의 전기 여부와 수동 수정 이력은 초안 생성과 별도의 단계로 관리한다.

도표 A-2 가상 공통 개념과 가상 회사 계정코드

가상 공통 개념	가상 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

설명용 코드다. IFRS·K-IFRS가 지정한 공통 계정번호가 아니며 실제 회사에 그대로 적용하지 않는다. 지갑 주소·토큰명과 계정코드도 일대일로 고정하지 않는다.

분개 초안 한 건에는 다섯 묶음의 정보를 남긴다. 추적(분개 초안·경제적 사건·사례 식별자, 원본 거래·로그·원장 행, 중복 방지 키), 판단과 버전(판단·규칙·정책·매핑의 식별자와 버전, 증거·FC·RF 식별자), 차대와 측정(차변·대변·보조계정·기능통화 금액, 원자산·수량, 가격·환율·시점·출처), 검산과 예외(차대 균형·잔액·수량·기간·누락·중복, 수수료·평가·분배·역분개 연결), 상태와 책임(제안·검토·승인·전기 상태, 담당·검토자, 미확인·보류 사유, 재검토 조건)이다. 같은 자산을 어떤 지갑에서 보유하는지는 보조원장의 차원일 수 있으므로, 내부 위치가 바뀔 때마다 손익·취득·처분 분개를 만들지 않는다. 주소의 귀속, 권리의 변화, 회사의 계정정책을 먼저 확인한다.

부록 B · RWA 가치평가 연결표

토큰의 가치는 기초자산이 아니라 그 토큰이 나타내는 권리에서 출발한다

이 부록은 거래구조화·가치평가 모듈(M4)의 첨부로, RWA 토큰을 평가할 때 기초자산에서 토큰 단위까지 가치를 연결하는 다섯 단계와 계산 검산, 결론을 멈추는 조건을 정리한다. 분석 범위·질문표(F-01), 거래구조표(F-03), 판단 기록(F-04), 불일치표(F-05)와 연결된다.

첫 단계는 평가 대상을 고정하는 것이다. 기초자산 자체, SPV 지분, 신탁수익권, 채권, 토큰이 나타내는 개별 권리 가운데 무엇을 평가하는지 특정하고, 평가 목적, 기준일, 통화, 가치 기준, 평가 단위, 관점을 기록하며, 토큰 수량과 법적 권리 단위를 연결한다. 둘째 단계는 기초자산에서 투자자에게 귀속되는 현금흐름을 도출하는 것이다. 기초자산의 수입, 공실, 운영비, 자본적 지출, 세금, 처분대금과 그 근거를 기록하고, 차입 원리금, 수수료, 유보금, 우선권을 반영해 해당 투자자에게 귀속되는 현금흐름을 산정한다. 이때 자산 가치가 이미 차입 효과를 포함하고 있는지 확인해 부채를 두 번 차감하지 않도록 한다.

셋째 단계는 권리별 배분과 평가다. 배분순위, 손실 부담, 만기, 상환·청산 조건, 의결권, 이전 제한을 계약 조항과 코드 경로에 연결한다. 지분이라면 지분 현금흐름과 그에 대응하는 할인율을, 채권이라면 약정 지급과 신용·회수 위험을 검토한다. 기초자산의 순자산가치를 모든 토큰의 가치로 일괄 사용하지 않는다. 넷째 단계에서 토큰 단위로 연결한다. 동질·동순위 권리라면 배분 대상 권리가치를 그 권리를 나타내는 유효 단위 수로 나누어 기준값을 구한다. 미발행·금고 보유·소각·희석·다중 클래스는 계약상 권리와 분모 포함 여부를 확인해야 하며, 공급량만으로 분모를 확정하지 않는다. 다섯째 단계는 가격, 위험, 민감도의 대조다. 거래가격의 시점·시장·거래량·당사자·출처를 기록하고, 권리 가치와 가격의 차이를 제한·유동성·비용·정보·통제

위험으로 설명하되, 같은 위험을 조정과 할인율에 이중으로 반영하지 않는다. 공실, 금리, 채무불이행, 환매 중단에 대한 민감도도 제시한다.

간단한 가상 예시로 계산 구조를 확인해 보자. 건물의 자산가치가 100, 차입금의 공정가치가 40, 별도로 확정된 지급의무가 2, 현금이 0이라고 가정하고, 모든 토큰이 동일한 잔여 지분권이며 유효 권리 단위가 58,000개라고 하자. 추가 클래스, 우선권, 세금, 거래비용 조정은 없다. 이때 잔여 지분의 기준값은 100 − 40 − 2 = 58이고, 토큰 단위 기준값은 58 ÷ 58,000 = 0.001이다. 장부금액과 공정가치의 차이, SPV의 다른 자산·부채, 계약상 분배 제한이 있다면 다시 산정해야 한다.

도표 B-1 잔여 지분권 토큰의 단위 기준값 검산 가상

항목	값	비고
건물 자산가치	100	가정
차입금 공정가치	(40)	자산가치에 차입 효과가 이미 반영되지 않았는지 확인
별도 확정 지급의무	(2)	현금 0, 추가 클래스·우선권 없음
잔여 지분 기준값	**58**	100 − 40 − 2
유효 권리 단위	58,000	공급량이 아니라 권리 단위로 확정
토큰 단위 기준값	**0.001**	58 ÷ 58,000

설명용 가상 수치. 실제 가치 결론이 아니다.

계산 뒤에는 세 가지를 대사한다. 계약상 총 권리와 유효 토큰 단위, 모델의 총 배분액과 클래스별 합계, 기초·기말 공급량과 발행·소각·권리 변동이다. 각 차이의 원인과 계산 영향은 불일치표(F-05)에 연결한다. 평가 대상 권리, 우선순위, 기초자산의 범위, 중대한 부채 또는 유효 권리 단위를 특정하지 못하면 확정적인 단위가치 산정을 유보한다. 가정을 명시한 조건부 계산은 가능하지만 실제 가치 결론과는 구분한다. 결과로는 선택한 방법, 대안, 산식, 입력 근거, 민감도, 검산, 미확인 사항, 검토자를 남기며, 전문 평가기준의 구체적 적용과 감정·법률·세무 등의 추가 검토 필요성은 사례별로 정한다.

부록 C · 주장별 증거 판정

증거 등급은 문서의 수나 자동 합산 점수로 정하지 않는다

이 부록은 증거 목록(F-02), 판단 기록(F-04), 결론 요약서(F-06)의 첨부로, 자주 등장하는 세 가지 주장에 필요한 증거와 증거 충분성(E1~E4)의 적용 방법을 정리한다.

첫째, 어떤 주소의 실제 운영 주체에 관한 주장이다. 필수적으로 확인할 것은 대상 주소, 권한, 기준기간과 법인 또는 담당자의 연결이며, 공식 주소 공시, 위임·서명자 자료, 승인·실행 이력을 교차 검토한다. 공개자료 분석에서는 공식 공시를 근거로 범위를 제한할 수 있다. 서명에 성공했다는 사실은 키에 접근할 수 있음을 뒷받침하지만, 법적 권리나 실소유자를 단독으로 입증하지 않는다.

둘째, 상환 청구권과 의무에 관한 주장이다. 적용되는 약관의 판본, 청구할 수 있는 사람, 의무자, 지급 조건과 제한을 확인한다. 실제로 이행되었다는 주장에는 요청·지급·소각·원장의 연결이 추가로 필요하다. 소각 기록이나 과거 상환 사례만으로 모든 보유자의 권리를 확정하지 않으며, 약관과 실행이 충돌한다면 별도의 쟁점으로 기록한다. 셋째, 통제의 운영 효과성에 관한 주장이다. 설계의 확인과 실제 운영을 분리하고, 대상

기간의 모집단과 그 완전성, 승인·실행·권한 변경 기록, 표본 선정 근거와 예외 처리를 확보해야 한다. 재수행, 관찰, 독립 확인은 해당 주장에 적합할 때 서로를 대체하거나 보완한다. 핵심 기간이나 모집단이 확인되지 않았다면 운영 효과성에 관한 결론은 유보한다.

증거 충분성 등급은 다음과 같이 적용한다. E1은 범위 안의 핵심 주장에 적합한 근거와 연결이 충분하고 중대한 미해결 충돌이 없는 상태다. E2는 제한이 있지만 그 제한을 특정할 수 있어 결론의 범위를 좁혀 말할 수 있는 상태다. E3는 간접 근거나 미해결 충돌 때문에 핵심 추론이 남아 있는 상태이고, E4는 핵심 근거가 없어 판단이 어려운 상태다. 등급은 문서의 수나 자동 합산 점수로 정하지 않는다.

도표 C-1 증거 충분성 등급과 결론의 표현

등급	상태	결론의 표현
E1	범위 내 핵심 주장에 적합한 근거·연결이 충분하고 중대한 미해결 충돌이 없음	범위를 밝혀 확정
E2	제한이 있으나 그 제한을 특정할 수 있음	범위를 좁혀 확정 또는 조건부
E3	간접 근거나 미해결 충돌로 핵심 추론이 남음	조건부 또는 유보
E4	핵심 근거가 없어 판단이 어려움	유보, 추가 자료 요청

자료: Chain Prism 보완 부록(주장별 증거 판정). 결론 표현 열은 '이 보고서를 읽는 법' 도표 0-2의 판단 상태(확정·범위 한정 / 조건부 / 유보)에 대응시킨 편집상 정리다.

각 주장에는 반증과 검토의 기록도 붙인다. 반대 설명, 누락된 경로, 위임·복구·우회 권한, 상반되는 자료를 적고, 작성자와 검토자가 각각 등급과 이유를 기록한다. 두 사람의 판단이 다르면 기준, 추가 증거, 최종 승인 사유로 해소하며, 끝내 합의되지 않으면 복수 해석이나 유보로 남긴다. 이 기록에는 사례 식별자, 작성자·검토자, 기준일·블록, 출처·판본, 적용 기준, 가정, 미확인 사항을 함께 적고, 빈칸은 미확인·비적용·추가 요청 가운데 하나로 설명한다.

부록 D · 출처, 재현 지침, 개정 기록

출처와 재현 지침

이 보고서가 참조한 공식 자료와 그 자료가 실제로 뒷받침하는 범위, 계산을 다시 수행하는 방법, 판본의 개정 이력을 정리한다. 공식 자료는 판단의 근거를 찾는 출발점이며 개별 상품에 대한 자동 답안이 아니다.

출처는 최신성만큼 적용 범위도 중요하다. 특정 위원회의 논의가 모든 디지털자산의 분류를 결정하지 않으며, 금융상품 기준의 검토도 해당 권리와 거래의 사실에서 출발한다. 그래서 분석 메모에는 참고 문서와 그 판본, 그리고 그 문서가 실제로 뒷받침하는 판단의 범위를 함께 적는다.

식별자 체계

도표 D-1 본문과 도구집에 쓰인 식별자

식별자	뜻과 쓰이는 곳
M1~M5	전문 검토 관점. 규제·AML, 회계·감사·보증, 조세·과세정보 보고, 거래구조화·가치평가, IT감사·기술 리스크(1.1절)
F-01~F-06	작성 양식. 분석 범위·질문표부터 결론 요약서까지(제2편 T1)
FC-A01 등	기능 카드. 영문자는 A 공급~H 조합의 영역, 숫자는 영역 안 순번. FC-X01은 미분류 절차(제2편 T4)
RF-01~08	검증 패턴. 징후에서 출발하는 확인 질문(제2편 T3)
F · I · H	주장의 성격 표시. 관찰 사실, 추론, 가정
E1~E4	증거 충분성 등급(부록 C)
R-USDC-01, R-USDC-01-R	실제 공개자료 사례. 고정 블록 관찰과 공개 준비자산 보고서 검토(3.1절)
V-D · V-F · V-FC	DEMO-USD 가상 사례의 자료, 발견, 카드 적용 기록(3.3절, 제2편 T4.9)
S-KR-ISS-01, H-K	국내 발행통제 가상 사례와 그 입력·가정(3.4절, 제2편 T2.2)
E- · C- · J- · D-	사례 안의 증거, 계산, 판단, 차이·발견 기록. 뒤의 R·K는 USDC·국내 사례를 뜻한다
S · 회계-S · FC-S · M3-S	출처. 사례 출처, 회계 참고, 기능 카드 참고, 조세 참고(이 부록)

사례 출처

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. 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 조문과 최종 하위규정의 준수 여부는 판정하지 않았다.

도구 출처 (확인일 2026-11-14)

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

사례 출처 S1·S2와 도구 출처 S1~S4는 원본의 표기를 따른 별개의 번호 체계다.

회계 참고 (확인일 2026-11-14)

회계-S1 · 2019 가상통화 보유 의제결정. https://www.ifrs.org/content/dam/ifrs/supporting-implementation/agenda-decisions/2019/holdings-of-cryptocurrencies-june-2019.pdf — 계약을 발생시키지 않는 등 한정된 가상통화의 보유를 다룬다. 모든 스테이블코인·RWA에 일괄 적용하지 않는다.

회계-S2 · IAS 8 공식 개요. https://www.ifrs.org/issued-standards/list-of-standards/ias-8-basis-of-preparation-of-financial-statements/ — 회계정책 선택·판단.

회계-S3 · IFRS 9 공식 개요. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-9-financial-instruments/ — 금융상품.

회계-S4 · IFRS 13 공식 개요. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-13-fair-value-measurement/ — 다른 기준이 요구·허용하는 공정가치 측정.

적용 판본, 시행일, 조기 적용, 국내 채택 차이는 개별 분석에서 확인한다. 조세 참고 M3-S1(OECD CARF·CRS 2023), M3-S2(OECD 이전가격 지침 2022)는 1.7절 참조.

재현 지침

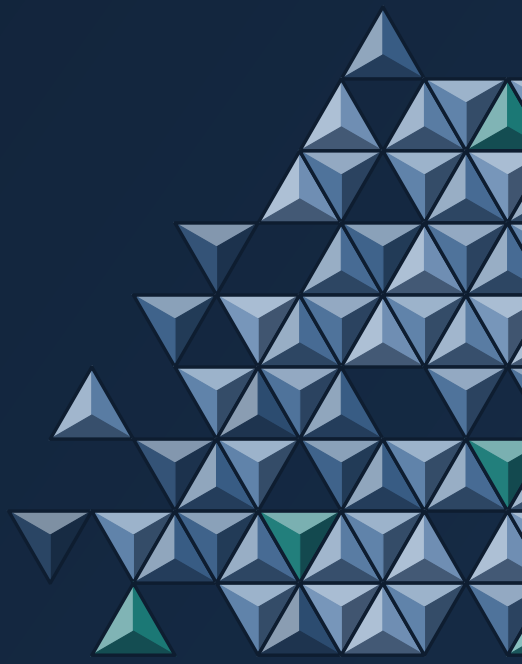
USDC 계산을 재현하려면 동일한 S1 판본의 9월 말 열만 전사하고, 괄호는 음수로 처리한다. 유통량 네 항목, 준비자산의 두 소계와 총계, 차액과 비율을 3.1절의 도표 3-4와 비교한다. 국내 가상 사례는 3.4절의 사건 A·B·X·C와 기초잔액으로 승인·원장·공급의 세 잔액을 각각 산출하며, 산술의 일치와 가정의 타당성을 분리해 검토한다. 계산은 문서를 작성하는 동안 실행해 확인했으나, 제3자의 독립 재현과 검토는 수행하지 않았고 검토자의 서명은 없다.

개정 기록

기준본은 Chain_Prism_Enhanced.pdf(77쪽, Vanzi 표기, 기존 가치평가 부록 포함)다. 사례 보완판(2026-11-18)에서는 USDC 사례의 상태와 수행 상태를 갱신하고, USDC 공개보고서 검토와 국내 발행통제 가상 사례, 출처·개정 기록을 추가했으며, 목차·북마크·쪽번호와 양식 참조를 연결했다. 그 밖의 본문, 기능 카드, 기존 사례, 부록 내용은 유지했다. 이 판은 OCP v1.0 본문을 바탕으로 한 사례 보완판이며, 별도의 저작권 변경등록이나 공개 홈페이지 반영은 수행하지 않았다.

이번 리뉴얼 편집본은 위 사례 보완판의 내용을 보존하면서 문체, 정보 구조, 도식, 조판을 개정한 것이다. 작성 양식, 검증 패턴, 기능 카드는 이 책의 제2편 『실무 도구집』으로 분리했다.

Chain Prism · OCP v1.0



제 2 편

실무 도구집

작성 양식 · 작성 예시 · 검증 패턴 · 기능 카드

이 도구집의 사용법

도구는 질문을 정형화할 뿐, 결론을 대신하지 않는다

이 편은 본 보고서의 분석 절차를 실제 업무에 적용할 때 쓰는 세 가지 도구를 모았다. 작성 양식은 분석 기록을 남기는 틀이고, 검증 패턴과 기능 카드는 무엇을 확인해야 하는지를 정리한 질문 모음이다.

세 도구는 출발점이 다르다. 기능 카드(FC)는 발견한 동작에서 출발해 “무엇을 확인할까”를 묻고, 검증 패턴(RF)은 의심스러운 징후에서 출발해 “무엇을 검증할까”를 묻는다. 두 도구가 만든 질문은 같은 증거 구조, 곧 증거 연결표와 통제맵, 전문 판단으로 들어가며, 그 결과는 작성 양식 F-01~F-06에 기록된다(도표 T0-1). 새 작업 단계를 하나 더 만드는 것이 아니라, 기존 여섯 단계의 기록을 채우는 질문을 구체화하는 것이 목적이다.

도표 T0-1 기능 카드와 검증 패턴이 증거 구조로 들어가는 경로



자료: Chain Prism OCP v1.0 기능 카드 개요. 카드나 패턴을 적용했다는 사실 자체를 결론으로 취급하지 않는다.

도표 T0-2 분석 단계별로 도구를 쓰는 위치

분석 단계	사용하는 도구와 기록
1단계 · 질문	F-01 분석 범위·질문표로 질문·관점·기준시점·모듈을 고정한다.
2단계 · 수집	F-02 증거·가정 목록. 기능 후보를 FC ID로 태깅하고, 함수·이벤트·역할·슬롯의 관찰 주장을 assertion_id에 기록한다.
3단계 · 구조	F-03 거래구조·귀속 분석도. 배포 코드·상태·경로로 동작과 범위를 확인하고 카드별 통제맵·실제 주체 연결을 작성한다.
4단계 · 판단	F-04 전문 분야별 판단표. M1~M5 중 필요한 질문만 적용하고, 기능 존재·실제 권리·통제 효과성의 결론을 분리한다.
5~6단계 · 대사·보고	카드의 연결 검증을 증거 연결표와 F-05에 반영하고, FC·RF·판단·발견 ID를 F-06에 남긴다. RF는 단계에 제한하지 않고 징후가 나타난 시점에 사용한다.

자료: Chain Prism OCP v1.0 기능 카드 적용·운영 기준.

도표 T0-3 상황별 찾아보기

이런 상황이라면	먼저 펼칠 도구
분석을 시작하며 질문과 범위를 정할 때	F-01 분석 범위·질문표(T1.1)
자료를 모으고 사실·추론·가정을 나눌 때	F-02 증거·가정 목록(T1.2), 증거 연결표(T1.3)
누가 실행하고 누가 바꿀 수 있는지 그릴 때	F-03 거래구조·귀속 분석도(T1.4), FC-C02 역할 기반 접근(T4.4)
공급량이 늘어난 경로를 확인할 때	FC-A01 발행(T4.3), RF-02·RF-03(T3.1)
코드가 바뀌었거나 프록시가 의심될 때	FC-E01 프록시 업그레이드(T4.5), 전체 영향 점검(T4.8)
거래가 막히거나 주소가 제한될 때	FC-D02 동결·블랙리스트(T4.6), RF-04·RF-05
잠금·이전·이벤트가 실제 결과와 달라 보일 때	RF-01·RF-06·RF-07(T3.1)
숫자가 맞지 않거나 비율의 범위가 의심될 때	F-05 불일치·추가 확인표(T1.6), RF-03, 작성 예시(T2.1·T2.2)
어느 카드에도 맞지 않는 동작을 만났을 때	FC-X01 미분류 동작(T4.7)
판단을 정리하고 보고할 때	F-04 전문 분야별 판단표(T1.5), F-06 결론 요약서(T1.7)

괄호 안은 이 도구집의 절 번호다.

도구를 쓸 때 지켜야 할 경계가 하나 있다. 카드의 점검 질문을 모두 확인했다고 해서 적법성, 회계 결론, 보안성, 통제 효과성이 인증되는 것은 아니다. 예를 들어 “mint 함수가 있는가?”보다 “어떤 경로가 공급량을 늘리며, 누가 그 경로를 실행·변경할 수 있는가?”를 물어야 하고, 이벤트 하나만으로 발행이나 권리의 성립을 확정하지 않는다. 함수명, 이벤트, 표준 표기는 후보 신호일 뿐이며, 동작과 적용 범위는 배포 코드, 상태 변화, 실행 경로로 확인한다. 또한 가상 사례(DEMO-USD, S-KR-ISS-01)에서 나온 예시와 패턴은 그렇게 표시했으며, 시드 단계의 패턴과 카드는 검증된 발견이나 업계 통계가 아니라 초기 검토 질문이다.

Contents

목차

이 도구집의 사용법

T1 작성 양식

T1.1 F-01 분석 범위·질문표
T1.2 F-02 증거·가정 목록
T1.3 F-02 첨부 · 증거 연결표
T1.4 F-03 거래구조·귀속 분석도
T1.5 F-04 전문 분야별 판단표
T1.6 F-05 불일치·추가 확인표
T1.7 F-06 결론 요약서

T2 작성 예시

T2.1 USDC 공개보고서: 증거 연결, 남은 차이, 범위별 결론 실제
T2.2 국내 발행통제: 증거와 권한의 연결, 발견에서 조치까지 가상

T3 검증 패턴

T3.1 징후는 오류 판정이 아니라 확인할 질문이다 (RF-01~08)
T3.2 패턴을 재사용 가능한 판단으로 축적한다

T4 기능 카드

T4.1 지금 사용할 카드와 다음 확장
T4.2 카드 한 장의 고정 양식
T4.3 FC-A01 발행
T4.4 FC-C02 역할 기반 접근
T4.5 FC-E01 프록시 업그레이드
T4.6 FC-D02 동결·블랙리스트
T4.7 FC-X01 미분류 동작
T4.8 카드를 확장하고 재검토하는 기준
T4.9 가상 사례와 자동화에 연결하기
T4.10 공식 근거와 복합 구조의 확장 순서

이 편은 Chain Prism 사례 보완판(2026-11-18)의 작성 양식·검증 패턴·기능 카드와 사례 기입 예시를 재구성했다. 본 보고서의 절 번호는 “본 보고서 1.6절”처럼, 이 편의 절 번호는 “T4.4”처럼 표기한다.

T1 작성 양식 · T1.1 F-01

분석 범위·질문표

작성 목적. 분석 범위를 좁히고, 필요한 모듈과 자료를 정한다.

이 양식은 분석을 시작하기 전에 질문, 관점, 기준시점, 자료 범위를 정하는 데 쓴다. 넓은 분야명 대신 "누가 어떤 의무를 부담하는가"처럼 답할 수 있는 질문으로 적는다. 진행 중에 범위가 바뀌면 최초 범위를 덮어쓰지 말고 변경 이유와 영향을 함께 남긴다.

사례 ID	제목	기준일·블록	작성·검토

분석 단위·관점 보고기업·고객·발행자 등 누구의 관점인가	대상·관할·기준일·블록 체인·컨트랙트·계좌, 관할, 기준시점

이번에 답할 핵심 질문
답할 수 있는 형태의 질문 1~3개

모듈 선택

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 다루지 않는 질문·자산·기간	종료 기준·미해결 시 처리 어떤 상태가 되면 종료하는가, 유보 시 처리

필요 자료	접근 제한	담당·기한

본 보고서 1.3절 참조. 고정 항목은 판단 질문, 대상·관점, 범위·시점, 모듈 선택, 종료 기준의 다섯 가지다.

T1 작성 양식 · T1.2 F-02

증거·가정 목록

작성 목적. 관찰 사실(F), 추론(I), 가정(H)을 분리한다.

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

사례 ID	기준일	작성자	입력 명세 ID	FC ID

A. 증거 목록

ID	출처·주소·버전·원본 ID	확인 사실 (F)	한계·관련 질문

B. 가정 목록

H-ID	종류·내용	근거·목적	영향받는 판단

추가 확보할 자료	결론 유보에 미치는 영향

가정의 종류 사실 보완 / 스트레스 / 대안 구조 / 기술 실험. 미확인 사항을 관찰 사실로 표시하지 않는다. 작성 예시는 T2.1(USDC)과 T2.2(국내 가상 사례).

T1 작성 양식 · T1.3 F-02 첨부

증거 연결표

작성 목적. 같은 거래를 설명하는 온체인·오프체인 자료를 짝지어 확인한다.

기본 양식 여섯 종은 그대로 두고, 이 표는 F-02의 선택 첨부로 쓴다. 두 자료를 확보했다는 표시에 그치지 말고 대상, 금액, 시점, 주체가 실제로 맞는지 적는다. 연결을 확인하지 못했다면 부족한 자료와 그것이 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 각각의 증거 충분성을 평가한다. 실제 사례, 가상 자료, 가상 실험은 서로 다른 근거로 표시한다. 작성 예시: T2.1 도표 T2-1(USDC), T2.2 도표 T2-4(국내 가상 사례).

T1 작성 양식 · T1.4 F-03

거래구조·귀속 분석도

작성 목적. 거래, 권한, 주체, 현금흐름을 한 화면에 연결한다.

그림에는 주소, 법인, 고객처럼 서로 다른 단위가 섞이기 쉬우므로 노드가 무엇을 뜻하는지부터 정한다. 자산·현금·권리·권한의 화살표를 구분하고, 중요한 연결에는 증거 ID를 붙인다. 빈 연결이나 미확인 주체도 그대로 표시해 두면 후속 자료를 어디에 요청해야 하는지 드러난다.

사례 ID	FC ID	기준 블록·문서 버전

거래·자산 이동 주소·컨트랙트 간 이동	권한·승인·변경 실행·관리·변경 권한의 경로
실제 주체·권리·의무 법인·고객·수탁·발행자	현금흐름·부채·배분 은행·수탁 자금과 배분 순위

핵심 연결 검토 · 거래·권리 첨부 참조

연결 관계	근거 ID	추론·가정	미확인 사항

가치 구분 기초자산 / 투자자 청구권 / 토큰 시장가격을 같은 화살표로 그리지 않는다. 본 보고서 1.6절(귀속 절차)과 이 도구집 T4.4(FC-C02 귀속 체크리스트) 참조.

T1 작성 양식 · T1.5 F-04

전문 분야별 판단표

작성 목적. 사실과 적용 기준에서 결론까지 추적한다. 판단 한 건에 한 장을 쓴다.

각 전문 판단은 질문, 적용 기준, 근거, 결론, 한계를 한 줄로 추적할 수 있게 적는다. 모듈마다 다른 정의나 시점을 적용했다면 그 이유를 남겨 정당한 기준 차이와 사실의 모순을 구분한다. 적용하지 않는 항목은 공란으로 두지 말고 비적용의 근거를 적는다.

판단 ID	FC·RF ID	선택 모듈	관점·관할·시점
판단 질문		M2: 규칙·정책·매핑 ID	
확인 사실·귀속 추론 F와 I를 구분		증거 ID	
적용 기준·출처 기준의 문단·판본·효력		권리관계 전제	
판단·논거		대안 해석	
사용 가정	한계	추가 조치	
위험 유형·영향·가능성	해석 명확성	증거 등급 E1~E4	

증거 등급 E1~E4의 정의는 본 보고서 부록 C. 회계 판단은 부록 A의 규칙 양식과 연결한다.

T1 작성 양식 · T1.6 F-05

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 부족인지, 처리 오류인지, 범위 차이인지에 따라 담당자와 다음 행동이 달라진다. 조치를 마친 뒤에는 새 근거와 판단 변경 여부를 남겨 차이의 발견과 해소 과정을 이어 둔다.

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 1~6단계 중 어디로	**재검토 결과**

남은 차이 / 최종 결론에 미치는 영향

작성 예시: T2.1 도표 T2-2(USDC D-R01~05), T2.2 도표 T2-5(국내 가상 사례 D-K01~04).

T1 작성 양식 · T1.7 F-06

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 그 등급을 부여한 이유도 짧게 남긴다.

사례 ID	제목	기준일·블록	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

결론 예시: T2.1 도표 T2-3(USDC), T2.2 도표 T2-5 이하(국내 가상 사례).

T2 작성 예시 · T2.1 USDC 실제

같은 문서 안의 일치는 독립 교차 검증이 아니다

본 보고서 3.1절의 USDC 공개보고서 검토(R-USDC-01-R)를 증거 연결표, F-05, F-06에 실제로 기입한 예시다. 문서의 내부 일관성을 확인한 것과 서로 다른 자료가 실질적으로 연결된 것을 구분하는 방법을 보여 준다.

이 예시에서 가장 먼저 눈여겨볼 점은 증거의 독립성이다. E-R01~03은 서로 독립된 세 출처가 아니라 같은 S1 보고서의 세 부분이다. 따라서 그 안의 항목이 서로 일치한다는 사실을 독립 교차 검증으로 표시하지 않는다. 숫자는 S1에서 전사한 표시값이며, 기존의 블록 관찰은 E-R04로만 연결하고 같은 시점의 증거로 치환하지 않는다. 공통 식별자는 case_id=R-USDC-01-R, source=S1, report_date=2026-09-30T23:59Z, currency=USD, unit=USDC다.

도표 T2-1 주장별 증거 연결표 (F-02 첨부)

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 계산	**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	**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

자료: Chain Prism 사례 보완판(2026-11-18) USDC 증거 연결표. J-R02~05는 도표 T2-2의 D-R01~05로 이어진다.

남은 차이는 모두 조치로 연결한다(도표 T2-2). 다섯 항목 모두 미해결이거나 외부 자료를 확보하지 못한 상태이며, 담당 열은 실제로 배정된 인물이 아니라 필요한 역할을 나타낸다. 자료 요청·수령·완료일은 접근권한과 업무 범위를 합의한 뒤에 정하므로 지금은 비워 두었다. 원자료를 받으면 같은 기준시각·모집단·정의로 다시 계산하고, 이전 판단과 변경 사유를 함께 남긴다.

도표 T2-2 남은 차이를 조치로 연결한 F-05

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: 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 모집단과 제외 사유 확인 시 J-R02·04 재검토
D-R03 · 준비자산 기초자료 공시 명세 ↔ 은행·수탁·내부 원장	실재성·권리·부담을 직접 확인하지 못함	재무·수탁: 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: 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

자료: Chain Prism 사례 보완판(2026-11-18) USDC 불일치·추가 확인표. 관찰된 차이를 곧바로 오류·부정·준비자산 부족으로 판단하지 않는다. 정당한 기준 차이인지, 자료 부족인지, 처리 오류인지 구분한 뒤 결론을 갱신한다.

결론은 범위별로 종결한다(도표 T2-3). 판단의 흐름을 한 줄로 쓰면 다음과 같다. J-R01은 E-R01·02의 수치에서 출발해 S1의 정의와 표시단위를 기준으로 C-R01 계산이 일치함을 확인했고, 그 한계는 전사값과 문서 내부에 한정되며, 후속 조치는 독립 재현 요청이다. J-R02~05는 현재 자료의 공백 때문에 같은 시점·주체·범위라는 원칙을 충족하지 못해 유보했고, D-R01~05에 따라 증거를 확보한 뒤 재검토한다.

도표 T2-3 범위별로 종결한 결론 (F-04 / F-06)

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-05의 후속 증거가 필요하다.

자료: Chain Prism 사례 보완판(2026-11-18) USDC 결론 정리.

수행 기록도 결론과 같은 무게로 남긴다. 수행한 것은 공식 공개 문서 열람, 숫자 전사, 산식 실행, 차이 0과 준비자산 초과액 확인, F-02·F-05·F-06 작성이다. 수행하지 않은 것은 독립 RPC 교차조회, 은행·수탁 확인, 내부 원장 대사, 소스-바이트코드 대응, 법적 권리 의견, 독립 검토자의 재현이다. 재현할 때는 본 보고서 3.1절의 입력·부호·수식을 그대로 적용하고, 새로운 월 보고서의 숫자를 섞지 말고 별도 판본으로 실행한다.

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

T2 작성 예시 · T2.2 국내 발행통제 가상

수량이 맞지 않는 이유를 승인·원장·권한으로 나누어 기록한다

본 보고서 3.4절의 교육용 가상 사례(S-KR-ISS-01)를 증거 연결표, F-04, F-05, F-06에 기입한 예시다. H-K01~07은 자료를 확보했다는 표시가 아니라 이 교육 사례에 부여한 입력·가정 ID이며, 실제 관찰 사실(F)이나 고객자료 증거 ID로 재표기하지 않는다.

이 사례의 주장은 다섯 개로 나뉜다. 수량, 승인과 실행의 대응, 권한 통제, 법적 권리, 회계 영향이다. 앞의 두 주장은 가상 입력 안에서 확정할 수 있지만, 뒤의 두 주장은 실제 계약·법률·원장 자료가 없으므로 유보한다. 같은 표 안에서도 주장마다 결론의 강도가 다르다는 점이 이 예시의 핵심이다.

도표 T2-4 주장별 증거 연결표 (F-02 / F-04)

주장	온체인 측 가상 입력	오프체인 측 가상 입력	판단 / 상태
J-K01 수량	H-K04: 기초·발행 250,000·소각 50,000·기말	H-K01 원장 / H-K02 승인 목록	**가상 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 한도를 넘지 않아도 내부 승인과의 일치는 보장되지 않음. 통제 설계상 공백
J-K04 법적 권리	토큰 수량과 관리자 주소	H-K07: 1토큰=1권리 가정 외 실제 법률 자료 없음	**유보.** 초과발행·투자자 권리·대항력 판단
J-K05 회계 영향	발행·소각 수량	실제 계약·발행대금·상환·총계정원장 없음	**유보.** 분개·손익·부채 금액 확정. 수량 차이를 손실액으로 치환하지 않음

자료: Chain Prism 사례 보완판(2026-11-18) 국내 발행통제 증거 연결표.

도표 T2-5a 가상 권한 경로 (F-03)



가상 정책은 이중 승인을 요구하지만, H-K05에서는 minter가 단독 호출할 수 있다고 가정했다. 권리 원장은 별도의 반영 절차다. 키 소유자·위임·업그레이드 경로는 실제 자료가 없으므로 법적 책임자로 귀속시키지 않는다.

이 경로를 놓고 확인할 통제 질문은 네 가지다. 승인 ID가 실행 요청과 원장 기록에 똑같이 남는가, 중복과 재시도가 차단되는가, 한도와 권한을 변경할 때도 승인이 필요한가, 우회 경로·긴급 권한·업그레이드가 통제를 무력화하지 않는가. 이 질문에 대한 답이 발견별 조치로 이어진다(도표 T2-5).

도표 T2-5 발견에서 조치까지 (F-05)

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 여부와 권리 유효성 확인. 정정 이력과 전후 대사 차이 보존
D-K02 승인 미대응 발행 50,000 발행 통제 우회 가능	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

자료: Chain Prism 사례 보완판(2026-11-18) 국내 발행통제 불일치·추가 확인표. 담당·기한은 실제 업무 수임 시 배정한다.

F-06에는 결론을 범위별로 적는다. 가상 산술에서는 100,000의 차이가 원장 반영 누락과 승인 미대응 발행으로 분해된다. 통제 설계에서는 가상 정책과 단독 실행 경로 사이에 공백이 있다. 반면 실제 위법성, 자산 손실, 회계 오류 금액, 통제 운영 효과성은 이 자료로 확정할 수 없다.

시정 후의 기대치도 실행 결과와 구분해 적는다. 유효한 B 50,000을 원장에 반영하고 X 50,000을 적법하게 해소한다는 조건에서, 기대 권리·원장·공급은 각각 1,150,000이 된다. 여기서 X의 해소는 임의 소각 지시가 아니며, 권리·계약·적법 절차를 확인한 뒤 결정해야 한다.

> **수행 범위.** 이번 수행은 가상 입력의 계산과 표 작성이다. 시스템 변경, 권한 회수, 소각, 원장 수정, 고객 통지, 통제 테스트는 실제로 수행하지 않았다.

T3 검증 패턴 · T3.1

징후는 오류 판정이 아니라 확인할 질문이다

검증 패턴(RF)은 특정 결과를 미리 결론 내리는 규칙이 아니라, 혼동하기 쉬운 연결을 반복해서 확인하기 위한 질문의 묶음이다. 모든 패턴에는 정상 설명과 반증 조건을 함께 기록한다.

"잠금은 소각인가"처럼 혼동하기 쉬운 연결을 기억해 두면 다른 거래에서도 검토 지점을 빠르게 찾을 수 있다. 다만 패턴을 적용할 때는 사례의 계약, 코드, 상태가 패턴이 전제한 조건과 같은지 다시 확인해야 한다. 그래서 패턴에는 반례를 함께 둔다. 특정 잠금 상태에서 의무가 남는지는 계약과 실제 처리에 따라 달라지므로, "잠금이면 항상 같은 결론"이라는 규칙으로 만들지 않는다. 검증 질문을 적용한 뒤 조건이 맞지 않으면 비적용 이유를 남기고, 새로운 조건은 별도 사례로 축적한다.

도표 T3-1 패턴을 적용하는 순서

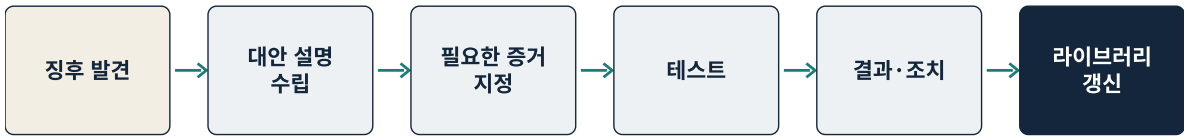


도표 T3-2 시드 검증 패턴 RF-01~08

ID · 징후	가능한 원인 · 정상 설명	확인할 증거 · 테스트	결과 · 조치
RF-01 · V-F01 잠금 ≠ 소각	예치·상환 대기·보호예수일 수 있음. 공급과 의무가 정상적으로 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	보유·통제·권리·유동성 결론을 분리
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

RF-01~03은 DEMO-USD 가상 사례(본 보고서 3.3절)와 연결된다. 나머지 항목도 초기 검토 질문이며, 실제 사례에서 검증된 독자적 발견이나 업계 빈도 통계로 제시하지 않는다.

T3 검증 패턴 · T3.2

결과만 저장한 패턴은 다른 구조에서 오판을 부른다

사례에서 발견한 문제를 재사용하려면 발생 조건과 적용 한계를 함께 남겨야 한다. 이 절은 징후, 확인 절차, 필요 증거, 반례를 함께 축적하는 기록 틀을 제시한다.

좋은 패턴 기록은 다른 분석자가 무엇을 다시 확인해야 하는지 알 수 있게 해 준다. 필요한 자료가 비공개여서 확인하지 못했는지, 실제 반례를 발견했는지, 아니면 질문 자체를 바꿔야 하는지를 나누어 적는다. 사례가 늘어날수록 패턴은 단순한 경고 목록이 아니라 조건과 검증 경로가 풍부해지는 방향으로 관리한다. 현재 목록은 시드 라이브러리이므로, 반복 적용으로 확인된 패턴과 아직 검증하지 않은 후보를 구분해 쌓아 간다.

도표 T3-3 패턴 한 건의 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 여부가 아니라 실제 적용 근거·반례·재현성으로 쌓인다.

도표 T3-4 검증 패턴과 기능 카드의 연결

검증 패턴	연결되는 기능 카드
RF-02	FC-A01 발행 · FC-C02 역할 기반 접근 · FC-E01 프록시 업그레이드
RF-03	FC-A01 발행
RF-04 · RF-05	FC-D02 동결·블랙리스트
RF-06	FC-C02 역할 기반 접근 · FC-D02 동결·블랙리스트 · FC-E01 프록시 업그레이드

자료: Chain Prism 사례 보완판(2026-11-18) 검증 패턴의 FC 연결.

T4 기능 카드 · T4.1

지금 사용할 카드와 다음 확장

이 판에는 네 개의 기능 카드와 미분류 절차 FC-X01의 시드 본문이 들어 있다. 분류표가 넓다고 해서 모든 기능을 분석할 준비가 끝났다는 뜻은 아니며, 확장 목록은 적용 사례에 맞춰 채운다.

카드는 두 층으로 구성된다. A~G는 기본 기능의 관점이고, H는 여러 기본 기능이 결합된 조합 메커니즘이다. 기본 카드라도 교차 컨트랙트나 외부 의존이 있으면 하위 카드로 분해한다. 순서는 분명하다. 먼저 네 개 카드와 미분류 절차를 실제 사례에 적용하고, 거기서 반복되는 질문·누락·반례를 근거로 다음 카드를 작성한다.

도표 T4-1 현재 본문에 수록한 시드 카드

카드	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

도표 T4-2 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 경로를 보강한 뒤 복합 적용의 우선순위는 H02 대출·청산 → H01 AMM·유동성 → G02 브리지다(T4.10). F03·F01·B03·F04는 RWA·스테이블코인 사례에 맞춰 병행한다. H 카드는 관련 기본 카드와 프로토콜별 순서·실패 조건을 묶는다.

T4 기능 카드 · T4.2

카드 한 장의 고정 양식

고정 양식은 기능 이름을 수집하는 대신 동작, 권한, 증거, 연결 검증을 같은 순서로 보게 만든다. 카드의 정적 정의와 사례별 적용 기록을 분리하며, 카드 자체를 사실이나 결론으로 취급하지 않는다.

같은 기능이라도 배포 버전이나 외부 모듈에 따라 경로가 달라질 수 있다. 그래서 카드의 탐지 상태와 성숙도, 사례의 수행 범위를 따로 기록한다. 이 구분이 있어야 “발견했다”와 “검증했다”의 차이가 유지된다. 이 장의 카드마다 붙은 세 개의 상태 표시(자료 성격, 카드 상태, 수행 범위)도 같은 원칙에서 나왔다.

도표 T4-3 카드의 고정 필드

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

도표 T4-4 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.

카드 적용 기록 한 줄 application_id / card_version / case_id / 체인·주소·블록 / 주장·증거 ID / F·I·H / 후보·동작 확인·미확인·비적용 / 차이·한계·검토자. T4.3~T4.6의 모든 카드에 공통으로 적용한다.

T4 기능 카드 · T4.3

FC-A01 · 발행

FC-A01 | 자료 성격 · 참고 코드·표준 | 카드 상태 · 시드 | 수행 범위 · 질문 명세

총공급량을 늘리는 경로는 무엇이며, 누가 그 경로를 실행하고 변경할 수 있는가?

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

도표 T4-3-1 FC-A01 확인 항목

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 후보다. 로그 기록(F)과 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 확인한다. 건별 대사와 공급량의 기간 대사를 병행한다.
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 고정한다.
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 조정한다.

도표 T4-3-2 전문 판단에 연결할 질문

모듈	질문
M2 · M4	토큰 발행이 어떤 의무·투자자 권리를 발생시키는가? 인식·평가의 기준 사건은 무엇인가?
M1 · M5	실제 운영 주체와 행위는 무엇인가? 발행 승인 우회·단일 키·상한 변경 경로가 있는가?
M3	유상 교환·무상 배정·보상 등 거래 조건은 무엇이며, 누구의 어떤 경제적 이익인가? 이름만으로 소득 성격을 정하지 않는다.

연결 · RF-02·RF-03·RF-07 / FC-C02·FC-E01·FC-A02·FC-A03
공식 참고 · FC-S1·FC-S2(T4.10). 적용 버전·구현은 사례별로 재확인한다.

FC-A01 · 현장 노트

발행은 건별로, 그리고 기간 합계로 확인한다

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.

일반적인 ERC-20 발행은 대상 토큰에서 다른 보유자의 잔액을 차감하지 않고 수령자의 잔액과 공급을 늘리는 경로다. 그렇다고 원자산 입금이나 다른 체인의 잠금이 없다는 뜻은 아니다. 리베이스, 래핑, 브리지는 해당 카드와 함께 분석한다. 발행에 관한 주장은 세 층위로 나누어 기록한다(도표 T4-3-3).

도표 T4-3-3 발행에 관한 주장의 세 층위

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.

대사도 두 수준에서 수행한다(도표 T4-3-4). 건별 대사는 개별 발행이 주문·승인·입금·고객 원장과 이어지는지를, 기간 대사는 전체 공급 변동이 발행과 소각의 합으로 설명되는지를 확인한다. 둘 사이에 차이가 나면 범위와 처리 시점부터 확인한다.

도표 T4-3-4 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 경로에서는 질문을 더한다. issue, deposit, bridgeIn 같은 다른 이름, 생성자·내부 호출·발행 관리자·업그레이드로 추가된 경로를 확인한다. 발행자별 한도가 있다면 그 상위 한도를 바꾸는 권한도 추적하고, 발행을 실행한 주소가 실제로 승인된 키·서명자와 연결되는지 확인한다.

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

T4 기능 카드 · T4.4

FC-C02 · 역할 기반 접근

FC-C02 | 자료 성격 · 참고 코드·표준 | 카드 상태 · 시드 | 수행 범위 · 질문 명세

누가 행위를 실행하고, 누가 그 사람의 권한을 바꿀 수 있는가?

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

도표 T4-4-1 FC-C02 확인 항목

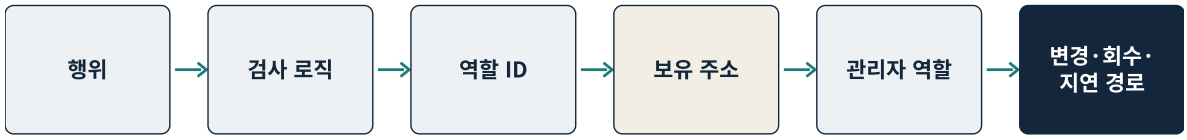
고정 항목	확인할 내용
동작 정의	역할에 따라 실행을 허용·차단하고 역할 보유자·관리자를 변경하는 경로. 행위 권한과 역할 관리 권한을 분리한다.
식별 신호	hasRole·getRoleAdmin·grantRole·revokeRole, RoleGranted·RoleRevoked 등은 구현에 따른 후보 신호다.
변형·우회	외부 권한 관리자, owner 경로, 사용자 정의 modifier, 업그레이드·모듈 호출. 역할 이름이 같아도 권한은 다를 수 있다.
통제맵	행위 → 검사 로직 → 역할 ID → 보유 주소 → 관리자 역할 → 변경·회수·지연 경로를 그린다. 순환·자기관리도 기록한다.
온체인 증거	기준 블록의 권한 상태와 전체 가용 변경 이력, 구현 코드. 보유자 열거가 불가능하면 로그 범위와 복원 한계를 명시한다.
오프체인 증거	이사회 의사록·위임장·키 관리 정책·멀티시그 서명자 명부·인사·승인·회수 기록. 진정성·효력 기간과 실제 운영을 대조한다(본 보고서 1.6절, 이 장 현장 노트).
연결 검증	역할 주소 ↔ 문서상 담당자 ↔ 실제 운영·승인·실행 기록. 명부와 실소유자, 서명과 경제적 통제를 분리한다. 부여·회수 시점과 잔존 권한을 대사한다.

도표 T4-4-2 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 지위나 회계상 지배로 단정하지 않았는가?

연결 · RF-02·RF-06 / FC-A01·FC-C01·FC-C03·FC-E01
공식 참고 · FC-S3(T4.10). 적용 버전·구현은 사례별로 재확인한다.

도표 T4-4-3 FC-C02 통제맵의 기본 경로



FC-C02 · 현장 노트

기술 권한에서 실제 주체로 연결한다

역할 보유자 목록을 실제 주체의 입증 자료로 쓰려면 권한의 관리 경로와 운영 기록을 연결해야 한다. 이 노트는 본 보고서 1.6절의 공통 귀속 절차를 체크리스트로 구체화한다.

이 부분은 판단이 가장 쉽게 미끄러지는 곳이므로 조금 더 자세히 쓴다. 확보한 문서가 많더라도 그 문서가 판단하려는 관계를 뒷받침하지 못한다면 추가 자료가 필요하다. 예를 들어 멀티시그 서명자 명부를 확보했다고 해서 그 명부가 실소유자 명부가 되는 것은 아니다. 서명할 수 있다는 사실은 키에 접근할 수 있음을 보여 줄 뿐, 법적 권리나 경제적 통제의 충분조건이 아니다. 그래서 먼저 기술 권한의 경로를 복원하고(도표 T4-4-4), 그 다음 관계별로 주체 귀속 증거를 확인한다(도표 T4-4-5).

도표 T4-4-4 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 추적한다.
부여·회수·이양	요청·승인·시행 시점 ↔ 체인 변경 ↔ 실행 거래를 연결한다. 퇴직자·구 키·다른 관리자 역할·업그레이드 권한이 남는지 확인한다.

도표 T4-4-5 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 구분한다.
☐ **문서상 권한**	이사회 의사록·위임장의 승인 주체·위임 범위·유효기간·재위임·철회 기록. 문서 진정성 확인 범위와 사본·누락을 표시한다.
☐ **키·서명 운영**	키 관리 정책·멀티시그 서명자 명부·변경 이력 ↔ 역할·관리자 주소·임계값·복구/모듈 경로. 실명·직책·외주·수탁·공동 권한을 연결한다.
☐ **실제 행사**	승인 기록·서명/키 운영 로그·역할 변경·실행 거래를 같은 사건·기간으로 대조한다. 명부·정책과 다른 운영, 미회수·긴급 권한을 확인한다.
☐ **반증·판단**	다른 설명·상충 자료·부족 범위를 기록한다. 기술 실행·법적 위임·의사결정·회계상 통제·세무 귀속을 각 기준으로 별도 평가한다.

공식 참고: FC-S3(기술 역할). 위 문서 체크리스트는 OCP의 분석 설계다. 카드 상태는 시드이며, 내부 문서를 실제로 확보했다는 뜻이 아니다.

목록의 완전성과 결론의 범위는 따로 기록한다. 열거 기능이 없으면 가용 로그에서 후보를 복원하고 기준 블록의 상태와 대조하되, 초기 설정·시작 블록·누락·자체 변경 경로를 확인하지 못했다면 전체 보유자 목록이라고 단정하지 않는다. 역할 주소와 정책상 직책을 일대일로 가정하지 말고 위임·외주·수탁 관계를 복원한다. 여러 주소와 여러 서명자가 서로 독립적인지도 실제 주체와 운영 자료로 확인한다. 기록할 항목은 주장과 대상 관계, 증거 ID·출처·판본·기간·진정성, 문서↔주소↔실행의 연결, 충돌·반증·누락, F·I·H, 적용 기준과 검토자이며, 자료 공백은 F-05에 요청과 재검토 조건으로 남긴다.

T4 기능 카드 · T4.5

FC-E01 · 프록시 업그레이드

FC-E01 자료 성격 · 참고 코드·표준 카드 상태 · 시드 수행 범위 · 질문 명세

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 제한 자체를 바꿀 수 있는지 살펴야 한다. 이 카드는 코드 변경과 일상 운영을 서로 다른 통제 평면으로 보면서, 두 경로가 만나는 지점도 확인한다.

도표 T4-5-1 FC-E01 확인 항목

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 확인한다. 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 기록한다.
오프체인 증거	변경 요청·검토·테스트·배포 승인·키 운영·사용자 고지·계약상 변경 근거. 코드 변경과 약정 변경을 구분한다.
연결 검증	승인 버전 ↔ 배포 코드 해시 ↔ 변경 거래·시점 ↔ 원장·사용자 영향. 전체 카드의 영향 여부를 점검하고 영향받는 판단을 재수행한다.

도표 T4-5-2 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?

연결 · RF-02·RF-06 / FC-C02·FC-C03·FC-C04·FC-E03
공식 참고 · FC-S4·FC-S5(T4.10). 적용 버전·구현은 사례별로 재확인한다.

적용 이력 · R-USDC-01 이 사례에서 질문을 보완했다. ERC-1967 밖의 슬롯과 조회 함수의 호출자 조건을 추가했다. 카드 상태는 시드로 유지하며, 되돌림 원인과 배포 버전은 아직 검증 전이다(본 보고서 3.1절).

FC-E01 · 현장 노트

레거시 슬롯과 호출자 조건까지 추적한다

슬롯과 조회 함수는 프록시를 탐색하는 단서이며, 배포 구조에 따라 다를 수 있다. 이 노트는 ERC-1967과 공식 참고 코드의 ZeppelinOS 레거시 슬롯을 나란히 비교한다. 확인일은 2026년 11월 14일이다.

두 계열은 슬롯을 만드는 방식부터 다르다. ERC-1967은 해시에서 1을 뺀 값을 슬롯으로 쓰고, ZeppelinOS 레거시는 문자열 해시 자체를 슬롯으로 쓴다. 따라서 표준 슬롯이 0이라고 해서 프록시가 아니라고 판단하지 말고 다른 계열을 확인한다. 일반 조회가 되돌려지면 호출자 조건을 검토하되, 그것을 USDC의 수정 전 버전 가설이 확인되었다는 뜻으로 읽지 않는다.

도표 T4-5-3 저장 슬롯과 참고 이벤트

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")`

근거: FC-S5 ERC-1967 / Circle 고정 커밋의 UpgradeabilityProxy·AdminUpgradeabilityProxy. 참고 코드와 실제 배포의 동일성은 별도로 검증한다. 슬롯·이벤트만으로 유형·변경 권한·이력의 완전성을 확정하지 않으며, ERC-1967의 이벤트 권고와 실제 구현도 구분한다.

도표 T4-5-4 구조에 따라 추가로 추적할 경로

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 구분한다.

업그레이드를 확인했다면 마지막으로 승인·공지·코드의 세 연결을 대조한다. 승인된 코드와 버전, 배포·변경 거래, 공지와 약정이 서로 맞는지 보고, 초기화·저장 구조·권한·경제 조건의 차이와 전체 카드에 미치는 영향을 확인한다. 영향받는 카드와 전문 판단은 재수행하고, 영향이 없다는 판단에도 근거를 남긴다. 과거 분석은 보존하고 현재의 적용 가능성은 별도로 검토한다. R-USDC-01의 조회 가설과 확인 계획은 본 보고서 3.1절에 있다.

T4 기능 카드 · T4.6

FC-D02 · 동결·블랙리스트

FC-D02 | 자료 성격 · 참고 코드·표준 | 카드 상태 · 시드 | 수행 범위 · 질문 명세

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 어떻게 연결되는지도 확인한다. 이 카드는 기능이 존재한다는 사실을 규제상 적정성이나 보유자 권리의 소멸로 자동 해석하지 않도록 구성했다.

도표 T4-6-1 FC-D02 확인 항목

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 범위를 비교한다.
통제맵	설정·해제자·관리자·대상·기간·사유·조건·우회 권한. 외부 모듈 교체가 제한 효과를 바꾸는지 확인한다.
온체인 증거	대상 상태·검사 경로·권한·변경 이력. 각 거래 경로의 실제 실행·실패를 분리한다. 테스트 결과는 테스트 환경으로 한정한다.
오프체인 증거	제한 사유·승인·고지·이의 절차·고객 상태·상환 약정. 특정 제재·규제 요건 충족은 별도 기준으로 검토한다.
연결 검증	제한된 주소 ↔ 고객·적격성 기록 ↔ 제한 결정 ↔ 차단 범위·해제·상환 처리. 옴니버스 지갑의 영향도 구분한다.

도표 T4-6-2 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?
M3	제한 중에도 보상·분배가 발생하는가? 권리 발생·청구·수령 시점이 어떻게 달라지는지 확인한 뒤 적용 기준을 검토한다.

연결 · RF-04·RF-05·RF-06 / FC-B03·FC-D01·FC-D03·FC-C02
공식 참고 · FC-S6(T4.10). ERC-3643은 한 구현 범위의 참고이며 보편 동작의 근거가 아니다. 적용 버전·구현은 사례별로 재확인한다.

FC-D02 · 현장 노트

동결의 근거와 효과를 연결한다

한 주소의 동결이 고객 한 명의 거래만 제한한다고 단정할 수는 없다. 이 노트는 기술적 차단, 승인 근거, 고객 대응을 나누고, 동결 뒤에도 남는 권리·의무의 검토로 이어 간다.

수탁이나 옴니버스 구조에서는 주소와 고객 원장의 연결을 복원해야 동결의 영향을 파악할 수 있다. 그래서 먼저 기술적인 제한 범위를 나누고(도표 T4-6-3), 그 다음 근거·승인·고객·상태를 오프체인 기록과 연결한다(도표 T4-6-4).

도표 T4-6-3 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?

도표 T4-6-4 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.

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

전문 판단의 경계도 분명히 해 둔다. M1은 해당 관할의 근거와 사업자 의무를 별도로 검토하고, M2와 M4는 발행자 의무의 지속, 보유자의 처분 가능성, 평가에 미치는 영향을 묻는다.

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

T4 기능 카드 · T4.7

FC-X01 · 미분류 동작

어떤 카드에도 맞지 않는 동작을 만나면 익숙한 이름에 끼워 맞추지 않고 상태 변화에서 다시 시작한다. 미분류 상태를 남기는 것은 실패가 아니라 범위를 정직하게 표시하는 방식이다.

FC-X01 자료 성격 · 참고 코드·표준 카드 상태 · 시드 수행 범위 · 질문 명세

무엇이 바뀌었고, 누가 바꿀 수 있으며, 어떤 기록과 연결해야 하는가?

분류표에 없는 동작을 만났을 때 가장 가까운 카드의 확인 항목은 참고하되 그 결론을 그대로 가져오지 않는다. 기존 카드와 닮은 점과 다른 점을 기록해 두면, 이후 사례에서 새 카드가 필요한지 판단하는 근거가 된다. 비슷한 동작이 반복되면 공통 조건과 예외를 정리해 새 카드 초안의 근거로 쓴다.

도표 T4-7-1 미분류 동작의 일곱 단계

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 쓰고 반례·경계·기존 카드 중복·검토 이력을 첨부한다.

새 카드로 승격할 때는 명칭보다 반복되는 상태 변화와 통제·검증 질문을 정의한다. 임시 후보 ID를 쓰고 검토 후 고정 ID를 부여하며, 기존 ID를 다른 기능에 재사용하지 않는다. 사례 한 건의 특수 조건을 보편 규칙으로 확대하지 않는다.

> **주의.** 소스나 실행 추적이 부족하면 “동작 미확인”으로 남긴다. 미분류는 오류나 취약성이라는 뜻이 아니며, 자동 탐지가 실패했다는 사실만으로 기능이 없다고 결론 내리지 않는다.

T4 기능 카드 · T4.8

카드를 확장하고 재검토하는 기준

카드는 작성한 뒤 고정하는 문서가 아니라 적용 결과로 다듬는 질문 도구다. 이 절의 기준은 카드의 질문 개선, 탐지 결과의 확인, 전문 판단의 책임을 서로 구분하면서 축적하기 위한 것이다.

사례에서 유용했던 항목뿐 아니라 작동하지 않은 신호와 반례도 기록한다. 특히 코드가 바뀌었을 때는 바뀐 기능 하나만 다시 보지 않고 전체 카드에 대한 영향을 점검한다. 본 보고서가 강조한 "어제의 분석이 오늘은 틀릴 수 있다"는 상황이 바로 이 지점에서 생기며, FC-E01의 영향 점검과 연결된다.

도표 T4-8-1 카드 보완의 원칙

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 2~3·5단계를 중심으로 4단계 판단과 6단계 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.

도표 T4-8-2 변경 후 전체 영향 점검과 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.

같은 동작이 두 사례 이상에서 반복되면 새 카드 초안의 작성을 검토할 수 있다. 다만 이것은 자동 승격 조건이 아니라 후보 신호다. 기존 카드의 변형이나 조합인지, 별도 카드가 필요한지 검토하고, 동작 경계·출처·반례·테스트·검토 이력을 갖춘 뒤에 고정 ID를 부여한다. 미분류 기록에는 FC-X01을 쓰고 기존 ID를 재사용하지 않는다.

T4 기능 카드 · T4.9

가상 사례와 자동화에 연결하기

기능 카드의 역할은 별도 보고서를 하나 더 만드는 것이 아니라 기존 분석 절차의 질문을 구체화하는 데 있다. 이 절의 사례 연결은 가상 자료의 적용 예시이며, 실제 자동 탐지나 회계 엔진의 수행 결과와 구분한다.

단계별로 카드를 쓰는 위치는 이 도구집 앞머리의 도표 T0-2에 정리했다. 여기서는 시드 카드를 본 보고서 3.3절의 DEMO-USD 가상 사례에 실제로 붙여 본 기록을 보여 준다(도표 T4-9-1). 네 카드 가운데 어느 것도 "확인 완료"에 이르지 않았다는 점, 그리고 FC-D02는 근거가 없어서 사례에 동결 기능이 있다고 새로 가정하지 않았다는 점이 중요하다.

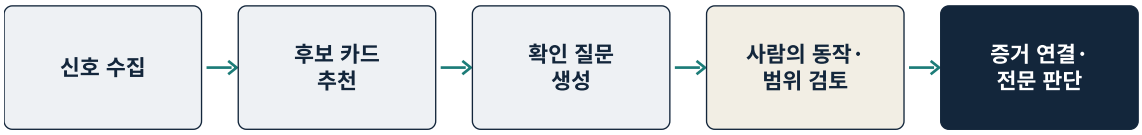
도표 T4-9-1 DEMO-USD에 붙인 시드 적용 기록

카드	기존 가상 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.

자료: Chain Prism 사례 보완판(2026-11-18) 기능 카드 적용 기록. 사례 상태 가상

자동화를 구현할 때도 같은 경계를 지킨다(도표 T4-9-2). 자동 탐지는 후보와 질문을 제시하고, 동작·범위·증거 연결은 검토자가 확인한다. 규칙마다 rule_id, 버전, 조건, 지원 범위, 오탐, 누락, 테스트를 별도로 기록한다. 역할 해시와 슬롯은 구현에 의존하고 과거 상태의 조회도 제한될 수 있으므로, 탐지되지 않았다는 사실이 부재의 증거가 되지는 않는다. 구현 현황과 계획은 본 보고서 5.1절과 5.3절에 있다.

도표 T4-9-2 자동화 구현의 경계



앞의 세 단계는 자동화 대상이고, 네 번째 단계부터는 검토자의 판단이다.

T4 기능 카드 · T4.10

공식 근거와 복합 구조의 확장 순서

공식 표준은 탐색의 출발점이며 실제 배포의 증거를 대신하지 않는다. 이 절은 기술 참고 자료와 OCP의 질문·판단 설계를 구분하고, 관련 기본 기능을 확인한 뒤 복합 사례를 하나씩 완주하는 순서를 제시한다.

H01·H02·G02는 확장 계획이며, 이 판에서 새 카드나 실제 분석이 완료된 것은 아니다. 아래 출처의 확인일은 2026년 11월 14일이며, OpenZeppelin 5.x 문서와 특정 배포의 동일성은 별도로 검증한다.

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

도표 T4-10-1 복합 Web3 구조의 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 조건: 실제 사례·기준일·코드 고정 → 관련 기본 카드·프로토콜별 질문 → 온·오프체인 근거 → 상태·현금흐름 대사 → 반례·실패 시나리오 → 판단·한계·재현 기록.

> 스마트컨트랙트는 누가 무엇을 실행할 수 있는지 보여준다. 그 실행이 누구의 권리와 의무를 만들고 장부와 계약에 어떻게 반영되는지는, 코드 밖의 자료까지 함께 읽어야 알 수 있다.

토큰을 발행할 수 있는 주소가 곧 발행의 경제적 책임을 지는 주체일까? 지갑에 토큰이 있다는 사실만으로 기초자산에 대한 권리까지 확인할 수 있을까? **Chain Prism · On/Off-Chain Prism(OCP)**은 코드·트랜잭션·계약·원장을 공통의 사실 기반으로 묶고, 규제·AML, 회계·감사, 조세·정보보고, 거래구조·가치평가, IT통제의 다섯 관점으로 거래의 실질을 검토하는 분석 프레임워크다.

세 가지 원칙

- **권한·권리·통제·귀속을 구분한다.** 키 보유자, 법적 권리자, 실제 의사결정자, 회계·조세상 귀속 주체를 자동으로 같게 보지 않는다.
- **온·오프체인 증거를 연결한다.** 코드와 거래기록으로 확인할 수 있는 것과 계약·원장·운영 자료가 필요한 것을 나누어 검토한다.
- **판단의 근거와 변화를 기록한다.** 사실·추론·가정과 출처·기준시점·한계를 남기고, 추가 자료로 달라진 판단을 추적한다.

이 책에 담긴 것

제1편	연구 보고서 — 분석 방법론, 도구 통합과 증거 처리, USDC 공개보고서 검토와 가상 사례, 거래 실질에서 회계까지, 적용 범위와 한계, 부록 A~D
제2편	실무 도구집 — 작성 양식 F-01~F-06, 작성 예시, 검증 패턴 RF-01~08, 기능 카드 FC

회계·준법·AML·IT감사 실무자와 디지털자산 거래구조를 공부하는 독자를 위해 썼다.

Vanzi
Chain & Context · chainandcontext.xyz

공개자료 검토와 교육용 가상 사례를 담았으며,
독립 보증·법률 의견·회계감사 결과가 아니다.