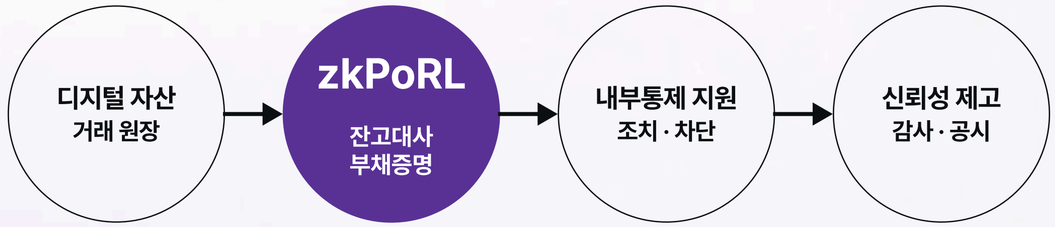
PRIVACY-PRESERVING VERIFICATION LAYER

zkPoRL

디지털자산 운영 신뢰를 위한 상시 잔고대사 · 증명 인프라

민감정보는 보호하고, **자산·부채 정합성은 공개 검증**합니다.



ZKRYPTO

WHO WE ARE

검증 가능한 신뢰를 만드는 ZKP* 딥테크

ZKRYPTO는 **민감할 수 있는 원장·잔고·거래 데이터를 대외적으로 공개하지 않고도,**
디지털자산 운영의 정합성을 검증할 수 있는 증명 인프라를 만듭니다.

영지식증명(ZKP,Zero-Knowledge Proof) : 비밀정보를 공개하지 않으면서도, 주장하는 내용이 맞다는 것을 검증 가능하게 하는 암호학적 기술

Privacy

민감정보를 외부에 직접
노출하지 않는 검증 구조

Verifiability

정의된 입력과 검증 명제의
수학적 정합성 확인

Operations

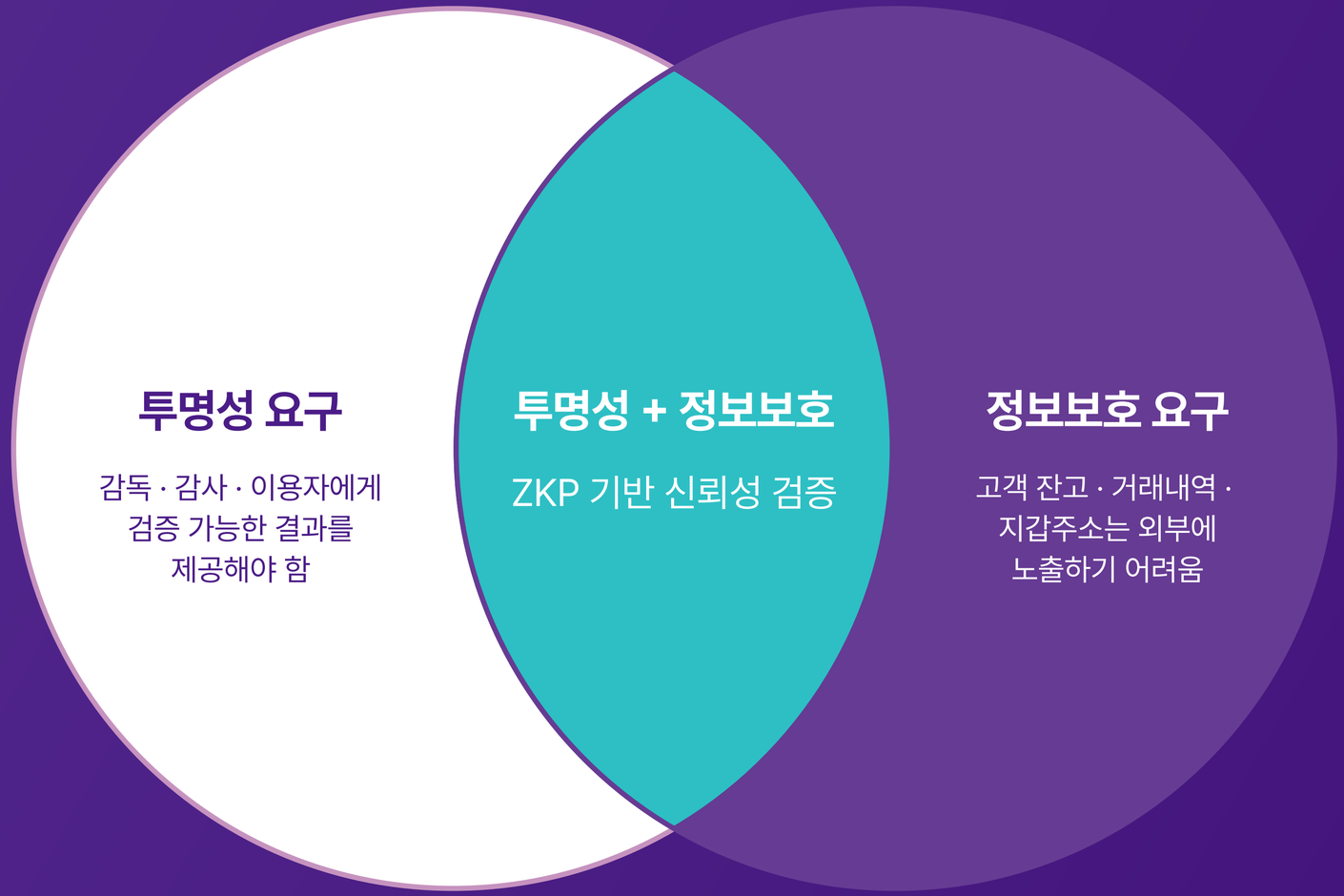
증명 결과를 **운영 대시보드,**
로그, 증적자료로 연결

기술의 목적은 **운영자가 믿고 확인할 수 있는 검증 흐름**을 모두가 볼 수 있게 공개하는 것입니다.

ZKP VALUE

왜 영지식증명(ZKP)인가

투명성과 정보보호의 딜레마를 동시에 해결합니다.



구분	일반 대사	zkPoRL
검증방식	원본 직접 대조	증명값 기반 검증
정보 노출	민감정보 노출 위험	민감정보 비공개
공시 신뢰	운영기관 발표 의존	수학적 검증 가능

PROBLEM

스냅샷과 후행점검만으로는 운영 중 리스크를 설명하기 어렵습니다

정기 감사와 특정 시점 리포트는 필요하지만, 점검 사이에 발생하는 장부 불일치,
기준시점 차이, 누락·중복 이벤트를 빠르게 포착하기 어렵습니다.

(기존 방식) 스냅샷 · 후행점검의 한계

점검 사이에 발생한 **장부 불일치**와 **이상징후**를 조기에 포착하기 어렵습니다.

대사 주기

일 · 월 · 분기 단위 확인

기준 시점

원장 · 지갑 · 온체인 대사 시점 불일치

민감정보

고객 잔고 · 거래내역 직접 공개 곤란

감사 대응

자료 분산 · 반복 취합 부담

💡 기업의 "**자산이 충분하다**"가 아니라, 고객의 자산을 반영한 "**지급의무**"를 보여줘야 합니다.

BUYING QUESTIONS

실제로 궁금해하는 질문

"왜 필요하고, 무엇이 달라지는가"

1

왜 필요한가?

장부와 실제 보유자산의 불일치를 더 짧은 주기로 확인하기 위해 필요합니다.

2

기존의 PoR과 무엇이 다른가?

특정 시점 리포트가 아니라 자산·부채·운영조치·감사증빙을 연결합니다.

3

무엇이 좋아지는가?

상시 대사, 이상징후 확인, 조치 이력, 감사자료 준비를 하나의 흐름으로 정리합니다.

4

시스템을 다 바꿔야 하나?

기존 거래엔진을 교체하지 않고, read-only 검증 레이어를 추가하는 방식입니다.

COMPARISON

zkPoRL은 기존 체계를 대체하지 않고 운영 검증 흐름을 보완합니다

내부 대사, PoR 리포트, 외부 실사, 자체 공시는 각각 필요합니다.
zkPoRL은 **원장·지갑·증명·조치·증빙**의 흐름을 연결합니다.

방식	장점	한계	zkPoRL 보완점
내부 수작업 대사	업무 방식에 맞춤	반복 업무 · 오류 가능성	장부 · 지갑 · 온체인 데이터 연결
기존 PoR(준비금증명) 리포트	대외 투명성 확보	특정 시점 중심	PoR/L과 운영통제 결합
외부 회계법인 실사	독립성 확보	실시간성 부족	실사 전 증빙자료 준비
자체 공시 시스템	고객 커뮤니케이션	감사증빙과 분리 가능	공시팩과 원천 증빙 정합성 강화

💡 **Snapshot 중심 → Continuous Control 중심**

SOLUTION FLOW

zkPoRL이 해결하는 문제

장부 · 지갑 · 온체인 · 감사증빙을 하나의 검증 흐름으로 연결합니다.

zkPoRL은 원천 데이터를 공개하지 않습니다. **정의된 데이터**와 **검증 명제**에 대한 **정합성을 확인**합니다.

HOW IT WORKS

데이터 수집부터 증빙 산출까지 하나의 검증 흐름으로 연결합니다

1 Read

전산원장 · 지갑 ·
온체인 데이터 읽기

2 Normalize

기준 시점과
자산 단위 정렬

3 Prove

PoR/L 관계와
변동 정합성 증명

4 Detect

variance, 누락,
중복 후보 확인

5 Package

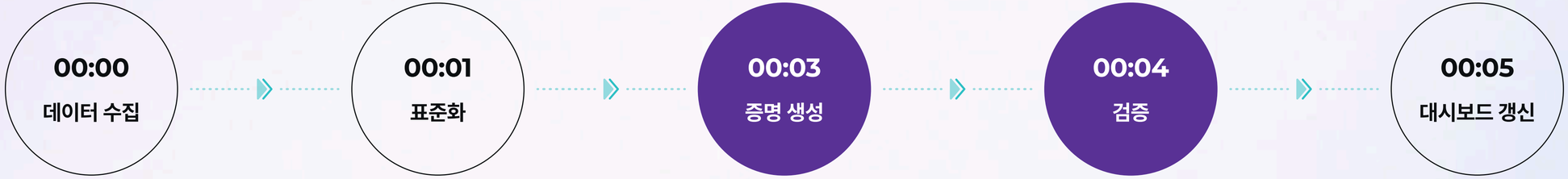
Case와 Evidence
Bundle로 정리

💡 고객은 **"증명값"**만 보는 것이 아니라, **"검증 결과"**도 같이 봅니다.

CORE FEATURE

핵심 기능 01. 5분 주기 상시 잔고대사

일 단위 확인에서 5분 주기 점검 체계로 전환합니다.



대사 주기

5분 이내

정책 기준에 맞춰 조정 가능

검증 대상

PoR/L

보유자산과 지급의무 관계 확인

이상 탐지

Variance

기준시점 · 누락 · 중복 후보 확인

💡 실제 운영 기준은 고객 시스템 구조, 자산 종류, 블록체인, 데이터 수집 정책 등에 따라 조정됩니다.

INCIDENT FLOW

핵심 기능 02. 이상징후 탐지와 조치 흐름

증명 실패를 운영자가 조치할 수 있는 Case로 전환합니다.

1

누락 · 중복 입력

원천 이벤트 불일치

Proof Blocked

expected ≠ actual

3

Case Open

원인 후보 확인

4

Sidecar Action

지급정지 · 차단 연계

5

Audit Trail

조치 이력 확인

💡 증명 실패는 "**ZK가 고장났다**"는 뜻이 아니라, 해당 기간의 잔고 변동을 설명하는 이벤트 집합이 닫히지 않았다는 운영 신호입니다.

EVIDENCE BUNDLE

핵심 기능 03. 감사·감독·공시 대응

반복적인 감사자료 취합을 증빙 패키지로 전환합니다.

산출물	활용 목적
Proof Run Summary	특정 기간 검증 결과 확인
Source Snapshot Hash	기준시점 데이터 무결성 확인
Incident Case	이상징후 · 조치 이력 확인
Exception Narrative	예외 발생 원인과 처리 설명
Disclosure Pack	이용자 · 외부 공시용 요약

* 증적자료 증빙 패키지는 감사 의견을 대신하지 않습니다. 감사인이 검토할 수 있는 증빙 흐름을 반복 생성하도록 지원합니다.

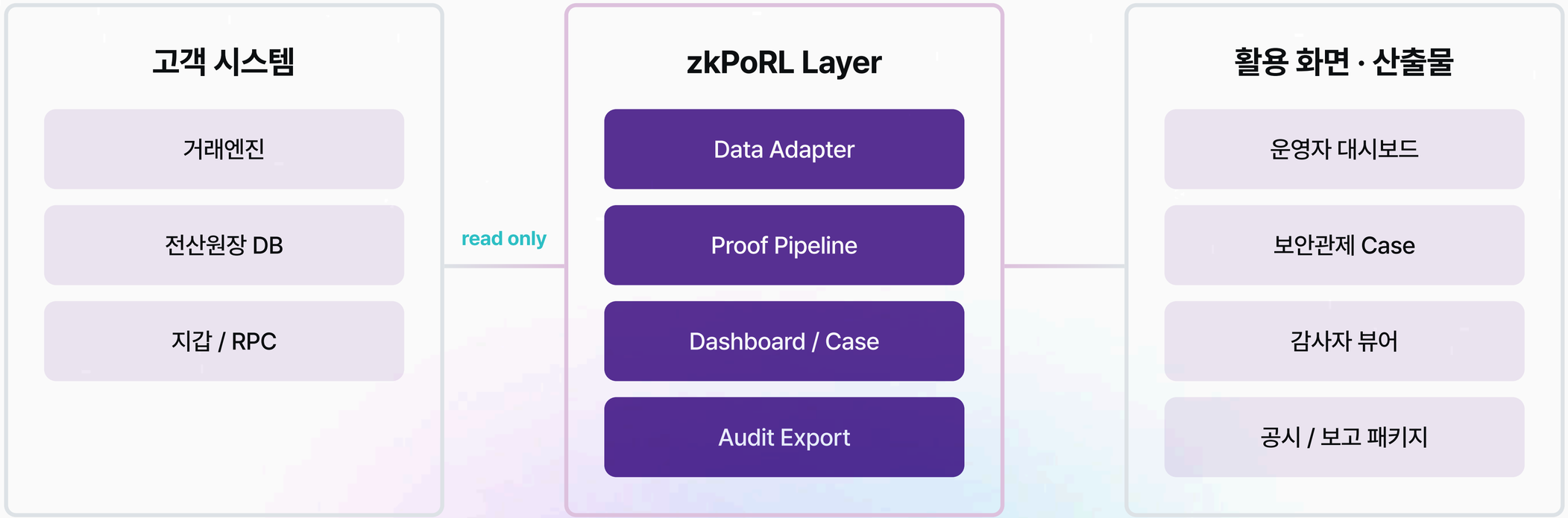
Audit Evidence Bundle.
(감사 증적자료 패키지)

- Proof Run 결과
- Source Snapshot Hash
- Alert / Incident Case
- Exception Narrative
- Disclosure Pack

DEPLOYMENT

도입 구조

기존 거래엔진을 바꾸지 않고 고객 내부망에 검증 레이어를 추가합니다.



💡 zkPoRL은 **차단의 근거를 제공**하고, 실제 지급정지·차단은 고객 정책 시스템이 수행합니다.

USE CASES

활용 시나리오 및 확장 계획

거래소에서 시작해 스테이블코인 · 수탁 · 지역화폐로 확장할 수 있습니다.

고객군	핵심문제	zkPoRL 메시지	우선 기능
원화마켓 거래소	규제 대응, 오지급, 감사자료 부담	5분 대사 + 이상 시 조치 + 월간 감사팩	상시 PoR/L, proof blocked, Case
지갑 · 수탁 사업자	지갑 소유권, 승인흐름, 보관증적	지갑 보유 · 승인 · 이동 증빙	지급의무 증명
스테이블코인 발행사	준비금, 발행량, 상환 정합성	준비금 검증 + 발행 · 상환 정합성	준비금 증명, 지급의무 증명
지역화폐 · 정책자금	정산 오류, 부정유통, 집행 정합성	유통량 · 정산 · 정책자금 증빙	유통량 증명

1 1차 거래소

2 2차 스테이블코인

3 3차 수탁 · 지역화폐

NEXT STEP

도입 효과 및 PoC 제안

zkPoRL은 규제 대응을 운영 시스템으로 전환합니다.

PoC 제안 범위

1. Mock Data 기반 5분 대사
2. proof blocked 시연
3. 운영자 Case 및 조치 이력
4. 감사자 Evidence Bundle
5. 고객사 연동 범위 정의

규제 대응

상시 잔고대사·외부감사·공시 확대 요구 대응

내부통제

이상징후 조기 탐지와 조치 흐름 확보

정보보호

고객 잔고·거래내역·지갑주소 비공개 검증

도입 유연성

기존 거래엔진 교체 없이 검증 레이어 추가

기술 설명 미팅 또는 데모 요청: contact@zkrypto.com

💡 감사 의견을 대신하지 않습니다. 감사와 감독이 요구하는 증빙을 반복 생산합니다.
상시 대사 · 이상징후 조치 · 감사 확인을 하나의 운영 흐름으로 연결

PoRL 용어 정리

사용자 잔액 (DB)

계좌 1	50
계좌 2	200
계좌 3	300
합계	550

거래소 보유 자산

온체인 토큰	600

금융기관 자산

현금	500
MMF	100
채권 등	50
합계	650

1 PoL : Proof of Liability

사용자 잔액 합계(지급의무) 증명

Cm1 + Cm2 + Cm3

(개별 잔액은 비공개)

= 550

2 거래소 PoRL(Proof of Reserve + PoL)

블록체인 상 보유 자산 ≥ 사용자 잔액 총합 대사

자산 (Blockchain)		부채 (사용자 잔액 총합)
600	≥	600

3 스테이블코인 PoRL

금융기관 현금성 준비금 ≥ 발행한 스테이블코인

자산 (현금성 준비금)		부채 (발행 스테이블코인)
650	≥	600