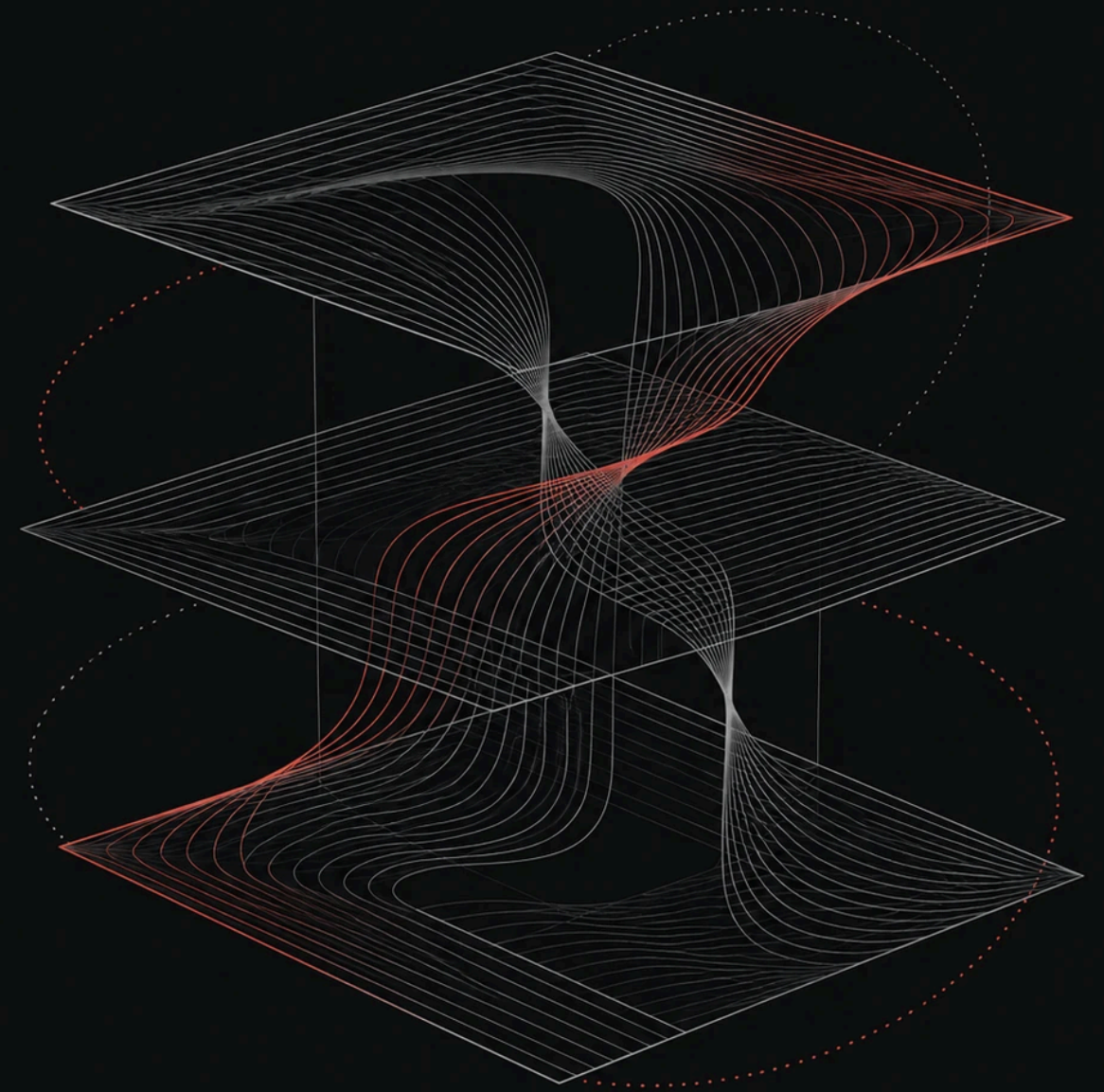


TECHNISCHER ANHANG / ARCHITEKTUR • KONTROLLEN • NACHWEISE

# Die Architektur hinter dem Kundenerlebnis.

Ein modulares Betriebsmodell für Banking-Arbeitsbereiche, freigegebene Dienste und nachvollziehbare Agenteninteraktionen.

Auf Hybrid-Technologie aufgebaut. Durch OVRYDE integriert.



## A01 / DER MODULARE AUFBAU

# Einheitliches Erlebnis. Klare Systemgrenzen.

Stellen Sie die Module rund um die maßgeblichen Daten Ihres Instituts und die ausgewählten Dienstleister zusammen.

**KUNDEN- UND MITARBEITEROBERFLÄCHEN**

E-Banking · Dashboard · assistierte Interaktion

**IDENTITÄT, GATEWAY & STEUERUNG**

Hybrid-ID · Berechtigungen · Richtlinien · Freigaben

**MASSGEBLICHES KERNSYSTEM & FINANZDIENSTE**

Bestehendes Kernsystem ODER Hybrid Core · ausgewählte Wallets / Anbieter

**GESCHÜTZTE DATEN & FREIGELEGEBENE NETZWERKE**

Prüfspur · begrenzter Agentenkontext · Nachweise · Federation / Schwester-Netzwerke

**Benutzeroberfläche**

E-Banking für Kunden, Arbeitsbereich für Mitarbeitende und assistierte Interaktionen.

**Steuerung**

Hybrid-ID, Gateway, Berechtigungen, Institutsrichtlinien und Prüfung.

**Finanzdienstleistungen**

Hybrid Core ODER bestehendes Kernbanksystem; gesondert abgenommene Wallets, Zahlungswege und Marktanbieter.

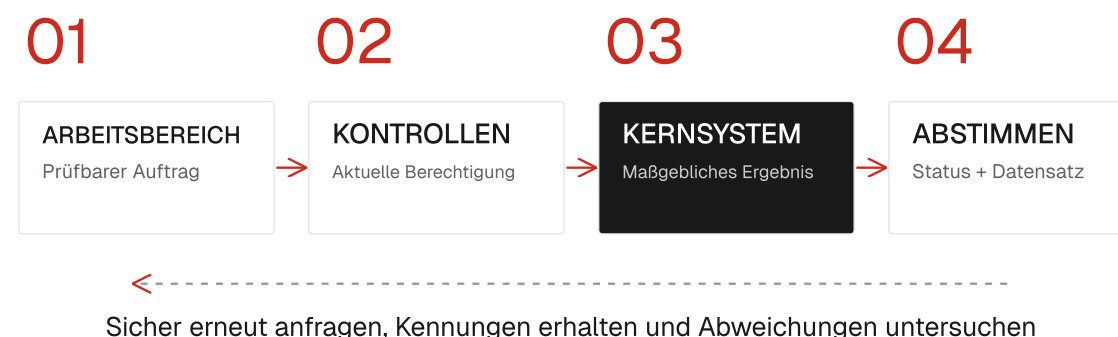
**Daten & Vernetzung**

Geschützte Unterlagen, zweckgebundener Agentenkontext, Nachweisdienste, Federation und freigegebene Schwester-Netzwerke.

A02 / DATEN, AUFTRÄGE & ABSTIMMUNG

# Ein maßgebliches Kernsystem. Eine synchronisierte Arbeitsansicht.

Bei einem bestehenden Kernbanksystem bereitet Hybrid Banking Aufträge vor und leitet sie weiter. Das Kernsystem bestätigt das tatsächliche Ergebnis.



## Lesen

Zulässige Kontextdaten mit Quellkennungen, Zeitstempeln und Status synchronisieren.

## Schreiben

Anfrage validieren, Berechtigung bestätigen und einen idempotenten Auftrag übermitteln.

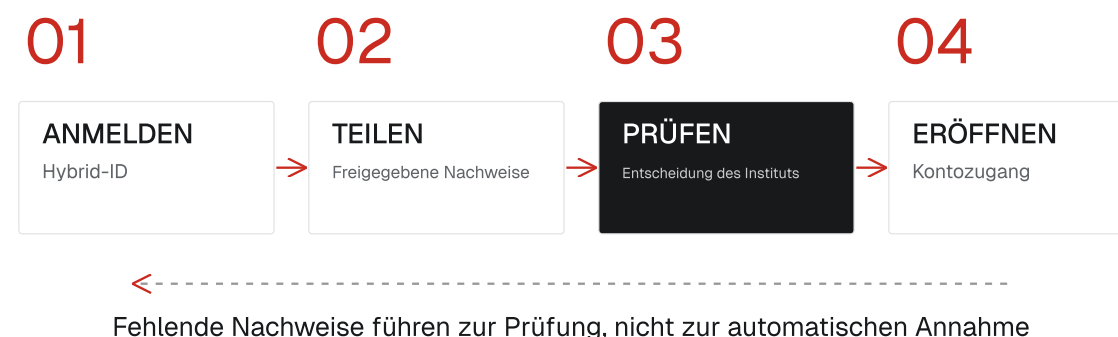
## Abstimmen

Das maßgebliche Ergebnis empfangen, sicher erneut anfragen und Abweichungen untersuchen.

A03 / IDENTITÄT & ONBOARDING

# Identität wiederverwenden. Zugangsvoraussetzungen prüfen.

Hybrid-ID-Anmeldung, freigegebene Verifizierungsnachweise und die Aufnahme als Bankkunde sind getrennte Entscheidungen.



## Kunde

Authentifizieren, gewünschte Datenfreigabe prüfen und Angaben zur Geschäftsbeziehung machen.

## Institut

Onboarding-Regeln anwenden, Nachweise prüfen und erforderliche Prüfungen abschließen.

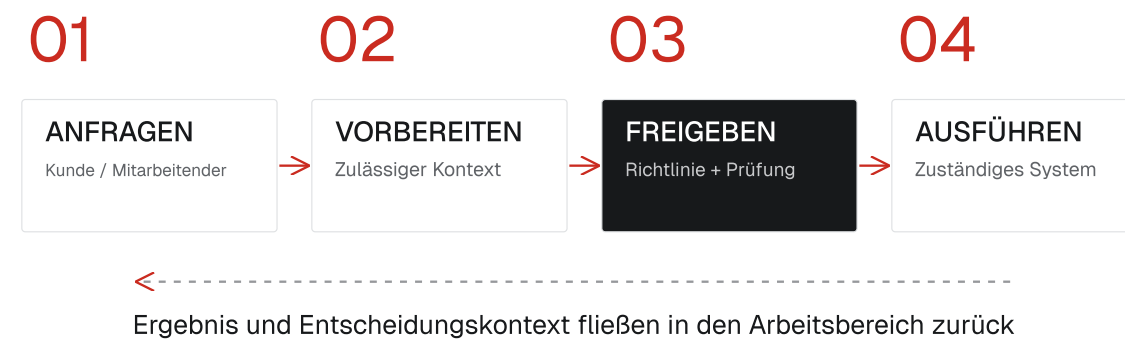
## Arbeitsbereich

Freigabe dokumentieren, den passenden Kontodatensatz anlegen und die Nachweiskette erhalten.

A04 / BERECHTIGUNGEN FÜR AGENTEN

# Ein Anliegen ist eine Eingabe. Die Befugnis wird geprüft.

Für Formulare und assistierte Schnittstellen gelten dieselben Berechtigungen und Richtlinien.



## Identität & Umfang

Den handelnden Akteur und die zulässige Operation an die Anfrage binden.

## Prüfung & Freigabe

Die geplante Aktion vorlegen, Kundenbestätigung einholen und gegebenenfalls unabhängig freigeben lassen.

## Ausführung & Dokumentation

An das zuständige System weiterleiten und Ergebnis, Freigabe sowie relevanten Kontext dokumentieren.

## A05 / ZAHLUNGEN &amp; EMPFÄNGER

# Das Ziel prüfen. Vor Freigabe erneut validieren.

Kontrollen greifen bei der Empfängeranlage sowie erneut bei der Autorisierung oder Verarbeitung einer Zahlung.

- |    |                                  |                                                                                                                                                                      |
|----|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 01 | <b>Empfängeranlage</b>           | Begünstigten und Zielkontext erfassen. Neue oder geänderte Empfänger den konfigurierten Kontrollen und Prüfungen zuführen.                                           |
| 02 | <b>Auftrag &amp; Freigabe</b>    | Betrag, Limits, aktuelle geografische Richtlinien und erforderliches Screening prüfen. Zweck, Akteur und notwendige unabhängige Freigabe sichern.                    |
| 03 | <b>Verarbeitung &amp; Status</b> | Nur über abgenommene Ausführungsanbindungen senden. Ausstehende, fehlgeschlagene und bestätigte Vorgänge unterscheiden und mit dem maßgeblichen Datensatz abstimmen. |

Termin- und Gehaltsprozesse bereiten Aufträge vor. Der Pilot impliziert keine externe ACH- oder Überweisungsabwicklung.

A06 / GEOGRAFISCHE RICHTLINIEN & SCREENING

# Länderregeln sind Richtlinien. Personentreffer sind Hinweise.

Geografische Beschränkungen sind von Anschrift und Staatsangehörigkeit gelisteter Personen zu unterscheiden.



Die Anschrift einer gelisteten Person begründet kein Länderembargo.

## Konservativer Ausgangspunkt

Im Pilot sind alle sechs unterstützten Sanktionslisten standardmäßig ausgewählt. Berechtigtes Compliance-Personal verwaltet die Konfiguration.

## Geografische Regeln anwenden

Beschränkungen an geprüfte länderbezogene Programmnachweise und Institutsrichtlinien binden. Geschützte Ausschlüsse sind nicht regulär übersteuerbar.

## Änderungen & Aktualität

Akteur, Begründung und Richtlinienversion erfassen. Fehlende Pflichtnachweise halten betroffene Aktionen an; neue Nachweise lösen eine Neubewertung aus.

## A07 / TRANSAKTIONSÜBERWACHUNG

# Aus einem Muster wird ein prüfbarer Fall.

Unterstützen Sie die Untersuchung veränderten Verhaltens, ohne eine Warnmeldung als Nachweis eines Fehlverhaltens darzustellen.

## Erkennen & erläutern

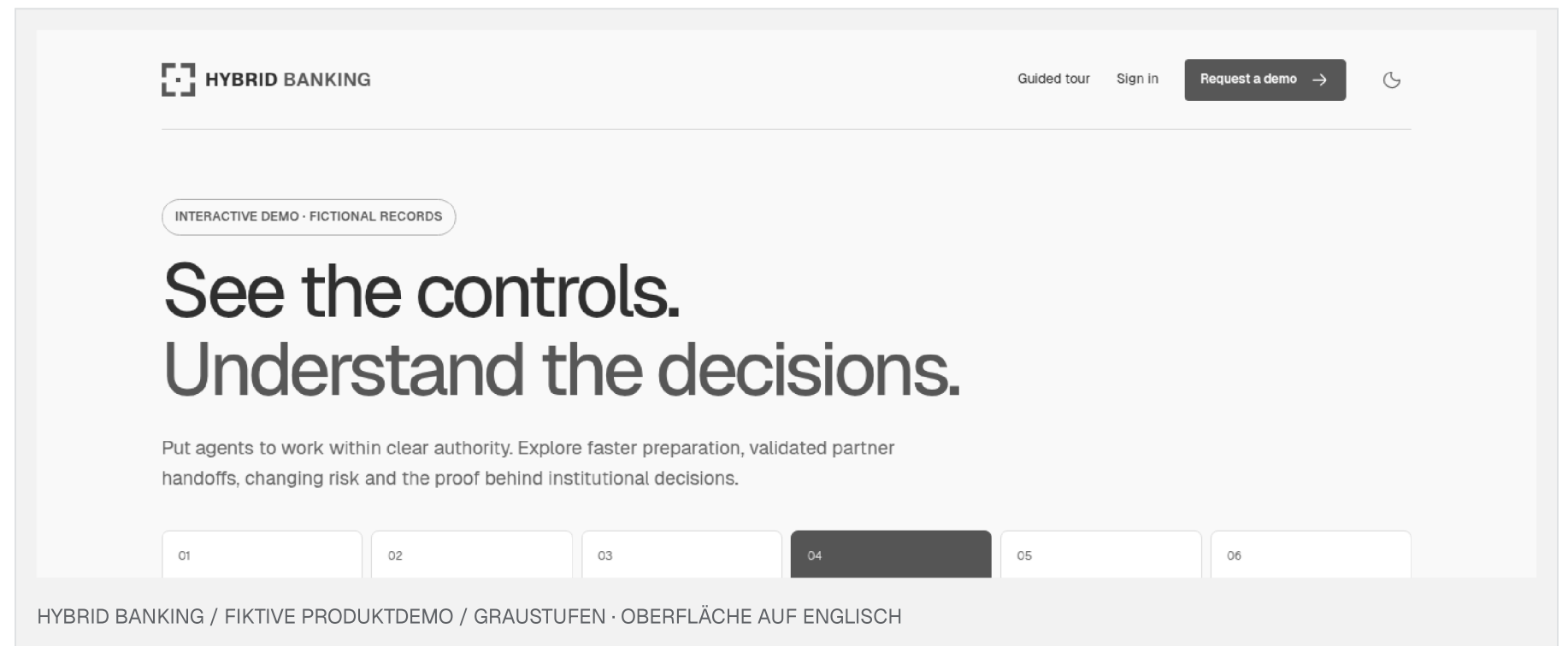
Konfigurierte Indikatoren wie wiederholte Kleinbeträge, Gesamtvolumen und rasche Geldbewegungen mit Regeln und zugrunde liegenden Ereignissen anzeigen.

## Untersuchen & entscheiden

Verantwortliche zuweisen, Risikofaktoren prüfen, Begründungen sichern und Fälle bei neuen Erkenntnissen wieder öffnen.

## Grenzen wahren

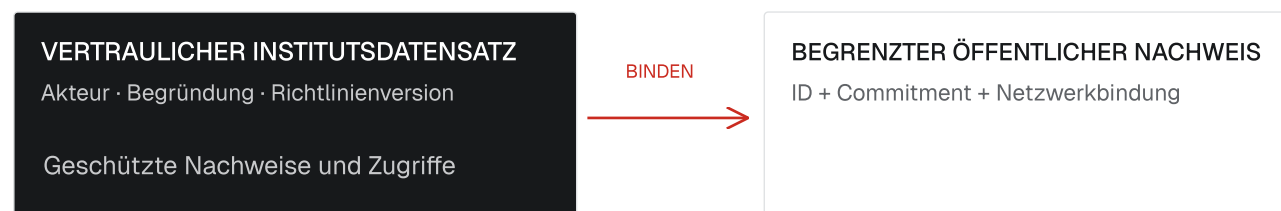
Begleitendes Monitoring unterstützt die Prüfung. Es ist weder automatische Sperre noch Beschuldigung oder Behördenmeldung.



A08 / VERTRAULICHE PRÜFSPUR & ÖFFENTLICHER NACHWEIS

# Daten vertraulich halten. Integrität prüfbar machen.

Ausgewählte Compliance-Richtlinien lassen sich über kryptografische Commitments prüfen, ohne Kunden- oder Richtliniendetails offenzulegen.



SCHWELLENWERT 3 / 4

Ein Betreiber · Testnet ohne Geldwert · verifizierte Inklusion

## Vertraulicher Datensatz

Akteur, Begründung, Richtlinienversion und Nachweise unterliegen geregelter Zugriff und Aufbewahrung.

## Veröffentlichung

Gebundene Veröffentlichungs-ID und Commitment werden an den Testnet-Nachweisdienst übermittelt. Der Eingang allein gilt als ausstehend.

## Verifikation

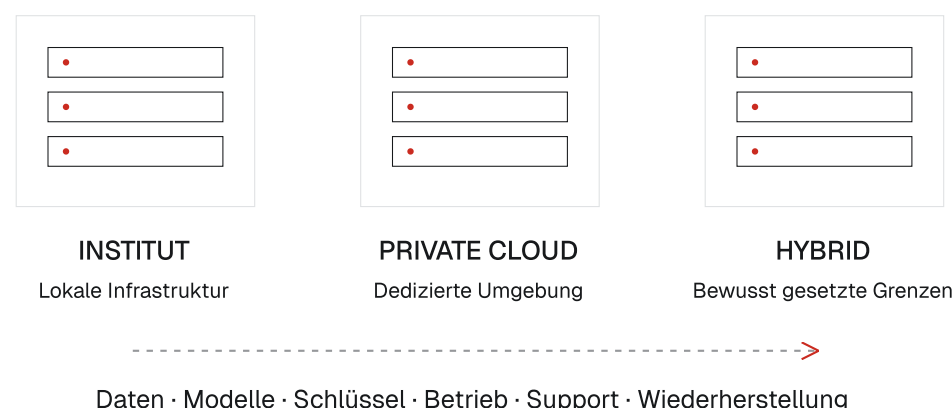
Netzwerk- und ID-Bindung, Signaturen, Quorum, Merkle-Inklusion und Kontinuität anhand eines vertrauenswürdigen Checkpoints prüfen.

3 von 4 Validator-Signaturen · ein Betreiber · Testnet ohne Geldwert

A09 / DATEN, KONTEXT & BETRIEB

# Kontext nutzbar machen. Freigaben bewusst steuern.

Legen Sie fest, wo Daten und Modelle betrieben werden, was Agenten abrufen dürfen und wie Zugriffe widerrufen werden.



## Institutsdaten

Datenstandort, Verschlüsselung, Aufbewahrung, Prüfzugriff, Wiederherstellung und Supportverantwortung definieren.

## Agentenkontext

Festlegen, welche Informationen gespeichert werden, wer sie abrufen darf und wofür. Identitätswiederverwendung gibt keine Bankdaten automatisch frei.

## Modellgrenzen

Lokale, Private-Cloud- oder hybride Inferenz anhand genehmigter Datenflüsse und Modell-Governance bewerten.

A10 / FEDERATION & PARTNERDIENSTE

# Unternehmen verbinden. Ihre Grenzen wahren.

Ein gemeinsames Teilnahme- und Berechtigungsmodell erleichtert die Suche und Integration freigegebener Dienste.

## Geschäftsbeziehung

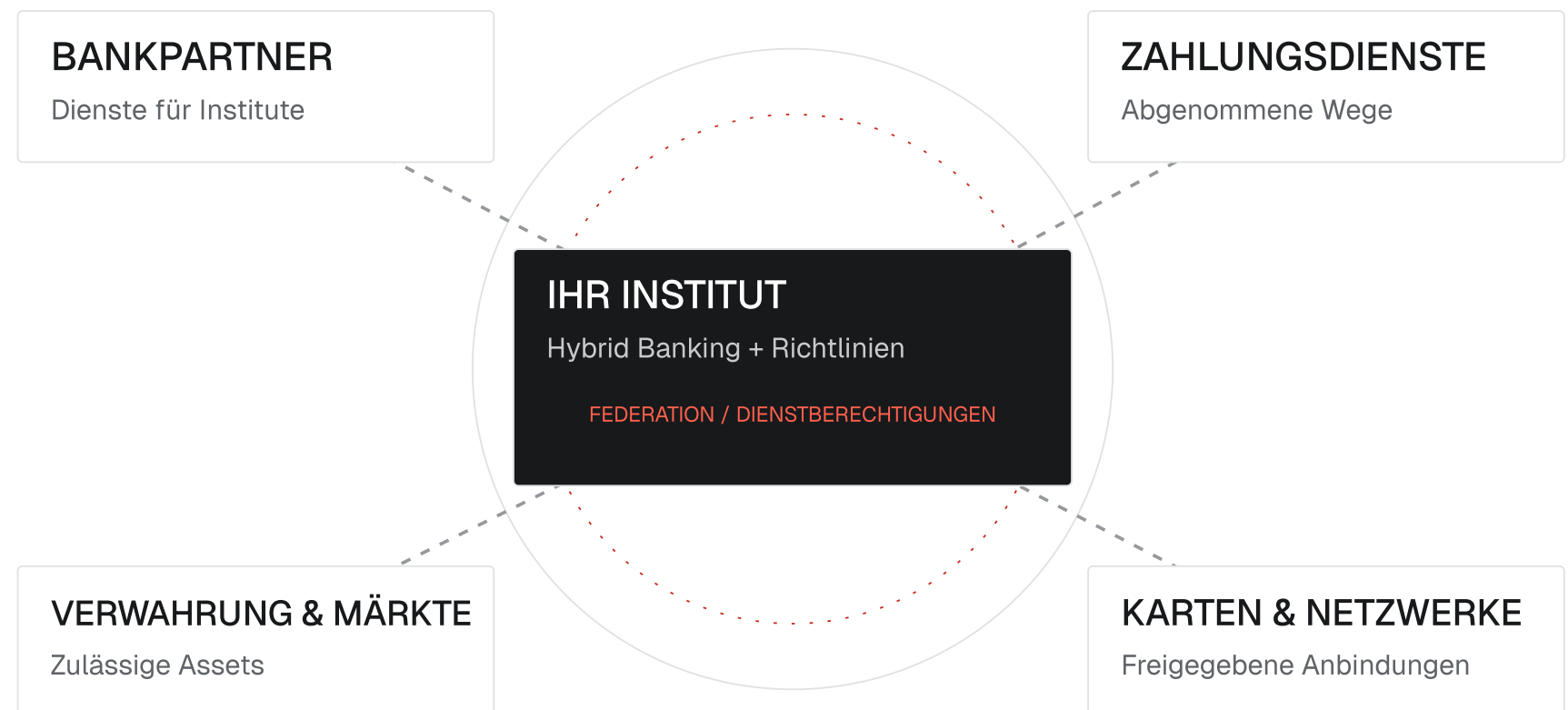
Rechtsträger, Rechtsordnung, Konditionen und verantwortliche Betriebspartei vereinbaren.

## Technische Beziehung

Authentifizierung, Operationen, zulässige Daten, Assets, Netzwerke und Fehlerbehandlung definieren.

## Abnahme

Gegenparteien, Abstimmung, Widerruf, Supporteskalation und Ausstieg vor Aktivierung der Verbindung testen.



# Den Prozess nachweisen. Dann gezielt erweitern.

Eine Freigabe stützt sich auf fachliche, kontrollbezogene und betriebliche Nachweise.

## Fachlicher Nachweis

Onboarding und Zahlungsauftrag vollständig durchlaufen, maßgebliche Daten abstimmen sowie abgelehnte, ausstehende und bestätigte Ergebnisse unterscheiden.

## Kontrollnachweis

Unberechtigte Akteure, veraltete Sanktionsdaten, gesperrte Ziele, doppelte Anfragen und ungültige Nachweisbelege testen.

## Betrieblicher Nachweis

Ausfallbehandlung, Wiederherstellung, Abstimmung, Schlüsselwechsel, Supportzuständigkeit und Datenexport beziehungsweise Ausstieg demonstrieren.

Ergebnis: vereinbartes Funktionsverzeichnis, Abnahmeprotokoll und klar begrenzter Aktivierungsbeschluss.