

Blockchain-Infrastruktur für das Bankwesen

Ihre Bank. Ihre Blockchain. Ihre Regeln.

Nutzen Sie diese Themen zur Strukturierung technischer Analysen und institutioneller Prüfungen. Schnittstellen, Verhalten und Zuständigkeiten werden für die konfigurierte Bereitstellung bestätigt.

Grundlagen von Netzwerk und Asset

Beginnen Sie mit Netzwerkidentität, Umgebungsgrenzen, Konsens und Validatorzuständigkeiten sowie dem Zweck des nativen Assets. Bestätigen Sie unveränderliche Kennungen und Genehmigungen vor der Erstellung.

Netzwerkarchitektur

Ermitteln Sie Komponenten, Grenzen, Abhängigkeiten, Rollen der Beteiligten und das vorgesehene Betriebsmodell. Halten Sie Annahmen für die technische Analyse fest.

Trennung der Umgebungen

Beschreiben Sie Produktions- und Nicht-Produktionsumgebungen, Zugriffswege, Datenverarbeitung und Zuständigkeiten für die Überführung von Änderungen.

Chain-ID und Netzwerkidentität

Prüfen Sie Chain-ID und weitere Netzwerkkennungen vor der Erstellung. Die Chain-ID ist danach unveränderlich.

Konsens- und Validatorzuständigkeiten

Dokumentieren Sie Konsenskonfiguration, Governance-Befugnisse und Validierungsplan. Weisen Sie Betrieb, Wartung, Zugriff, Überwachung und Störungsbehandlung der Validatoren institutionellen oder Service-Rollen zu.

Konfiguration des nativen Assets

Legen Sie Zweck, Benennung, administrative Kontrollen und Transaktionsrichtlinien fest. Die Asset-Konfiguration begründet keine Reserveunterlegung.

Eigentum und Trennung der Reserven

Die Institution besitzt und verwaltet ihre Reserven. Trennen Sie Reservevereinbarungen von Technologie- und Leistungsentgelten von FusionPointAI.

Kontrollen, Gebühren und Governance

Dokumentieren Sie Kontrollbefugnisse, Transaktionsrichtlinien, Gebührenfinanzierung und Governance als Entscheidungen der Institution. Testen Sie die konfigurierte Wirkung vor dem Produktivbetrieb.

Beschränkungen für Konten, Wallets und Vorgänge

Legen Sie Beschränkungsbedingungen für Konten, Wallets und Vorgangstypen fest. Dokumentieren Sie Entscheidungsbefugte, Nachweise, Prüfungs- und Aufhebungsverfahren sowie erwartete Ergebnisse zulässiger und abgelehnter Aktivitäten.

Teilweise und vollständige Beschränkungen

Beschreiben Sie die Wirkung teilweiser und vollständiger Beschränkungen, betroffene Vorgänge, Befugnisse, Dauer und Wiederherstellungsverfahren.

Administrative Governance

Konfigurieren Sie den Administrationsrat, die Mehrfachgenehmigungsschwelle, Vorschlagsbefugnisse, Ausführungsberechtigungen und geltende Verzögerungen. Änderungen bleiben nachvollziehbar.

Demokratische Governance

Konfigurieren Sie den Kreis der DAO-Stimmberechtigten, Stimmgewichte, Vorschlagsschwelle, Abstimmungszeitraum, Quorum und Ausführungsverfahren. Gleiches Stimmrecht wird nicht vorausgesetzt.

Hybride Governance

Legen Sie fest, wie administrative und demokratische Genehmigungen zusammenwirken, einschließlich einer Freigabe durch eine oder beide Seiten, sofern dies konfiguriert ist. Dokumentieren Sie Ausführung und Timelock-Zuständigkeiten.

Änderungen gesteuerter Parameter

Ordnen Sie gesteuerte Parameter nach Änderbarkeit, Genehmigungsanforderungen und Kompatibilitätsfragen und dokumentieren Sie abgestimmte Upgrade-Verfahren.

Transaktionsgebühren, Gas und Richtlinien für gesponserte Gebühren

Dokumentieren Sie Gebühren-Asset, Zahlungsverantwortung und Finanzierung getrennt von Leistungsgebühren und Reserven. Legen Sie zulässige Abwicklungs-Assets und Transaktionen, Budgets, Grenzen, Freigaben, Überwachung und Ausnahmeverfahren fest; die Zulässigkeit hängt von der Konfiguration ab.

Schnittstellen und institutionelle Integration

Behandeln Sie Schnittstellen und Integrationen als bereitstellungsspezifisch. Bestätigen Sie vor der Umsetzung Endpunktdetails, Authentifizierung, Support, Dateneigentum und Anbieterabhängigkeiten.

Schreibgeschützte JSON-RPC-Standardabfragen

Zu den schreibgeschützten Standardbeispielen gehören `eth_chainId`, `eth_blockNumber` und `eth_getTransactionReceipt`. Bestätigen Sie das tatsächliche Verhalten des Endpunkts für das bereitgestellte Netzwerk.

Transaktionslebenszyklus

Ordnen Sie Anfrage, Autorisierung, Übermittlung, Beobachtung der Bestätigung, Verarbeitung des Belegs, Wiederholungen und Abstimmungszuständigkeiten zu.

Explorer-Konfiguration

Legen Sie Zielgruppen, verfügbare Informationen, Markenanforderungen, Zugriffsgrenzen, Hosting, Aktualisierungen und Supportzuständigkeit fest.

Integration des Kernbankensystems

Prüfen Sie Systemschnittstellen, Datenzuordnung, Anbieterabhängigkeiten, Testzugriff, Sicherheitsprüfung und Umsetzungsverantwortung.

SSO- und IAM-Integration

Ordnen Sie Identitätsquellen, Authentifizierungsanforderungen, Rollen, Bereitstellung, Zugriffsprüfung und Entzug von Berechtigungen zu. Eine individuelle Prüfung ist erforderlich.

HSM und Schlüsselverwaltung

Dokumentieren Sie Schlüsselverwahrung, HSM-Anforderungen, Signaturgrenzen, Zugriff, Rotation, Wiederherstellung und technische Machbarkeit einer individuellen Integration.

Abhängigkeiten von SIEM, KYC und Compliance

Ermitteln Sie Ereignisquellen, Zugriffskontrollen, Aufbewahrung, Alarmzuständigkeiten und individuelle SIEM-Anforderungen. Beschreiben Sie institutionseigene KYC- oder Compliance-Abläufe und Datenabhängigkeiten; eine vorgefertigte Integration oder ein Compliance-Ergebnis wird nicht impliziert.

Sicherheit, Betrieb und kaufmännische Umsetzung

Schließen Sie die Analyse mit der Bestätigung von Bereitstellung, Sicherheit, Kontinuität, Servicezuständigkeiten und kaufmännischen Bedingungen ab. Zusagen gehören ausschließlich in genehmigte Vertragsunterlagen.

Zugriffsrollen und Genehmigungen

Legen Sie privilegierte Rollen, Funktionstrennung, Genehmigungswege, Zugriffsprüfungen, Notfallzugriff und Prüfungsnachweise fest.

Bereitstellungsgrenze

Vereinbaren Sie Hosting, Konnektivität, administrative Kontrolle, Standortanforderungen, Abhängigkeiten und Zuständigkeiten der Institution und des Dienstleisters.

Kapazitätsplanung

Planen Sie die Dimensionierung anhand der Arbeitslastanalyse und Architekturprüfung. Leiten Sie aus unverbindlichen Kapazitätsbeschreibungen keine Durchsatz- oder Servicegarantien ab.

Verfügbarkeits- und Ausfallsicherheitskonzept

Dokumentieren Sie Komponentenabhängigkeiten, Ausfallszenarien, Wiederherstellungsrollen und vereinbarte Ziele. Vertragliche Zusagen müssen ausdrücklich festgehalten werden.

Notfallwiederherstellung

Legen Sie Wiederherstellungsszenarien, Wiederherstellung von Daten und Konfiguration, Übungsumfang, Zuständigkeiten und von der Institution genehmigte Ziele fest.

Umfang der Sicherheitsbewertung

Vereinbaren Sie Bewertungsgrenzen, Nachweise, Ergebnisse und Zuständigkeiten. Eine Bewertung ist keine Zertifizierung und kein Prüfungsurteil.

Betriebssupport und Berichte

Legen Sie abgedeckte Komponenten, Supportkanäle, Eskalation, Berichtsquellen, Lieferformat und kaufmännische Bedingungen im Vertrag fest.

Migration und Änderungsmanagement

Prüfen Sie Ausgangszustand, Migrationsabhängigkeiten, Validierung, Umstellung, Rollback, Versionierung, Genehmigung und abgestimmte Upgrade-Verfahren.

Evaluierungsplan für das Pilotprojekt

Legen Sie Evaluierungsziele, Dauer, Testumfang, Datengrenzen, Zuständigkeiten, Ergebnisse und Abschlusskriterien fest. Ein Pilotprojekt ist kein Produktivbetrieb.

Preise, Angebot und Freigabe des Produktivbetriebs

Nutzen Sie aktuelle Datenbankpreise für unverbindliche Anzeigen. Der Produktivbetrieb erfordert ein verbindliches Angebot und einen unterzeichneten Vertrag; eine Pilotgutschrift unterliegt den genannten Voraussetzungen und Grenzen.

Preise

Umfang	Einrichtung	Monatlich	Erstes Jahr
Banking Blockchain Pilot	USD 15.000,00	USD 0,00	USD 15.000,00
Banking Core	USD 75.000,00	USD 15.000,00	USD 255.000,00
Banking Enterprise	USD 175.000,00	USD 30.000,00	USD 535.000,00
Banking Sovereign Ab	USD 350.000,00	USD 50.000,00	USD 950.000,00

Die Preisgestaltung richtet sich nach dem vereinbarten Umfang und den aktuellen Datenbankpreisen. Für den Produktivbetrieb sind ein verbindliches Angebot und ein unterzeichneter Vertrag erforderlich.

FusionPointAI | <https://fusionpointai.com/de/blockchain/banking>