Operationelle Risiken in Blockchain Geschäftsmodellen

Oktober 2019

pwc

Agenda

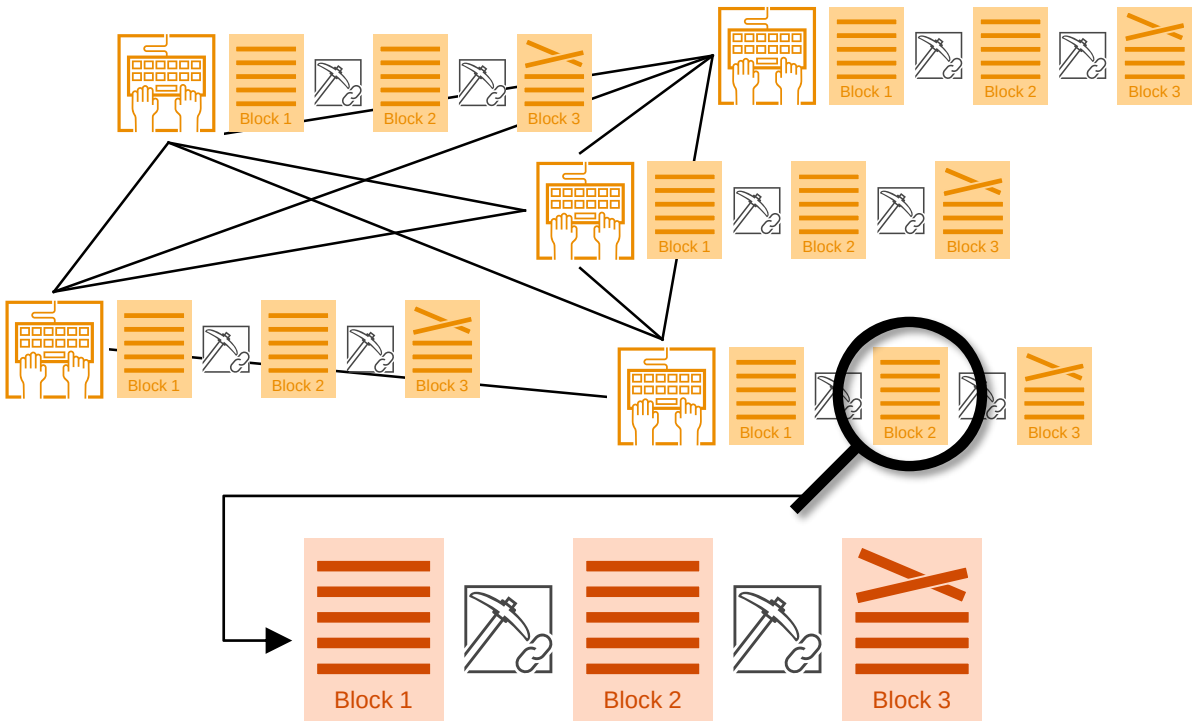
1. Einführung in Blockchain & Crypto Asset Geschäftsmodelle
2. Blockchain Technologie Risiken
3. Crypto Asset Risiken
4. Risiken und Compliance in Crypto Geschäftsmodellen
5. Zusammenfassung

1

Einführung Blockchain & Crypto Asset Geschäftsmodelle

Einführung in Blockchain

Verteiltes, dezentrales Hauptbuch an Transaktionen in Datenblöcken, die von den Benutzern gemeinsam genutzt und erstellt werden



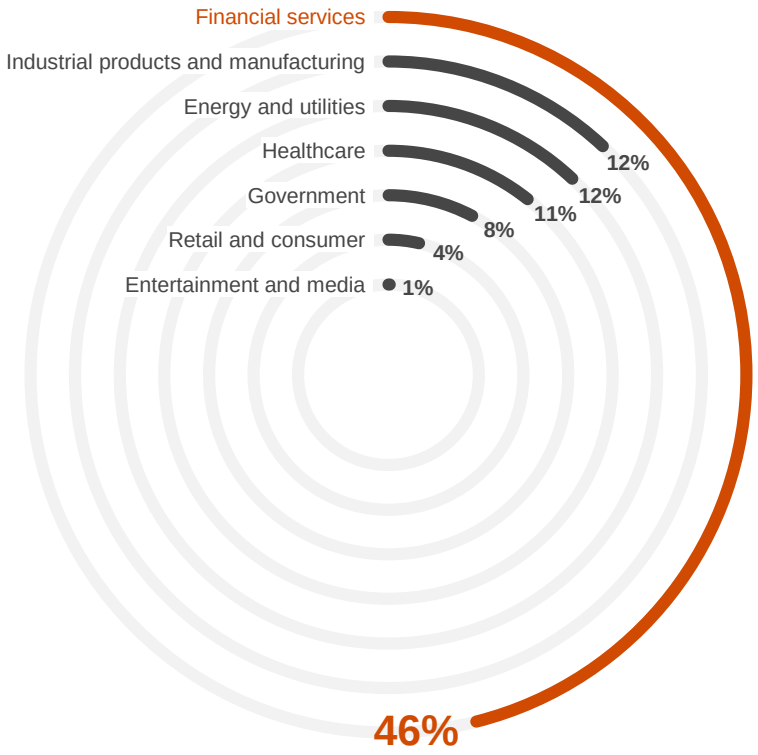
Hash verbindet einen Block mit dem vorherigen. Konsens-bildung wird gefördert durch Ausgabe von Block-Rewards im Rahmen von «Mining».

Verteiltes, dezentrales Hauptbuch (Ledger)

- Kontinuierlich wachsend
- Anreiz zur Bestätigung von Transaktionen durch Mining
- Liste der Transaktionen basierend auf Blöcken
- Jeder Block ist mit dem vorherigen durch einen Hash kryptographisch verknüpft.

Crypto Asset Produkte

Die Digitalisierung und Demokratisierung von Informationen führt zu neuen Anwendungen und Infrastrukturen, welche derzeit ein Ökosystem bilden



Note: Base: 600.
Q: Which of the following industries are the most advanced in developing blockchain today?
Source: PwC Global Blockchain survey, 2018

Digitalisierung & Demokratisierungstrend

- 24/7 Nutzbarkeit
- Transparenz
- Eigenständigkeit/Unabhängigkeit

Blockchain als Infrastruktur

- Beispiel: Tokenisierung von Assets
- CH Anbieter: Falcon Bank, Sygnum, SEBA etc.
- Status: Kauf, Verkauf und halten von Crypto Assets

Ökosystem

- Nutzung der Infrastruktur benutzerorientiert & als Digitalisierung im Backoffice
- Beispiel: we.trade; Ziel: Effizienzsteigerung durch verlässlichere und vereinfachte Dokumentennutzung

2

Blockchain Technologie Risiken

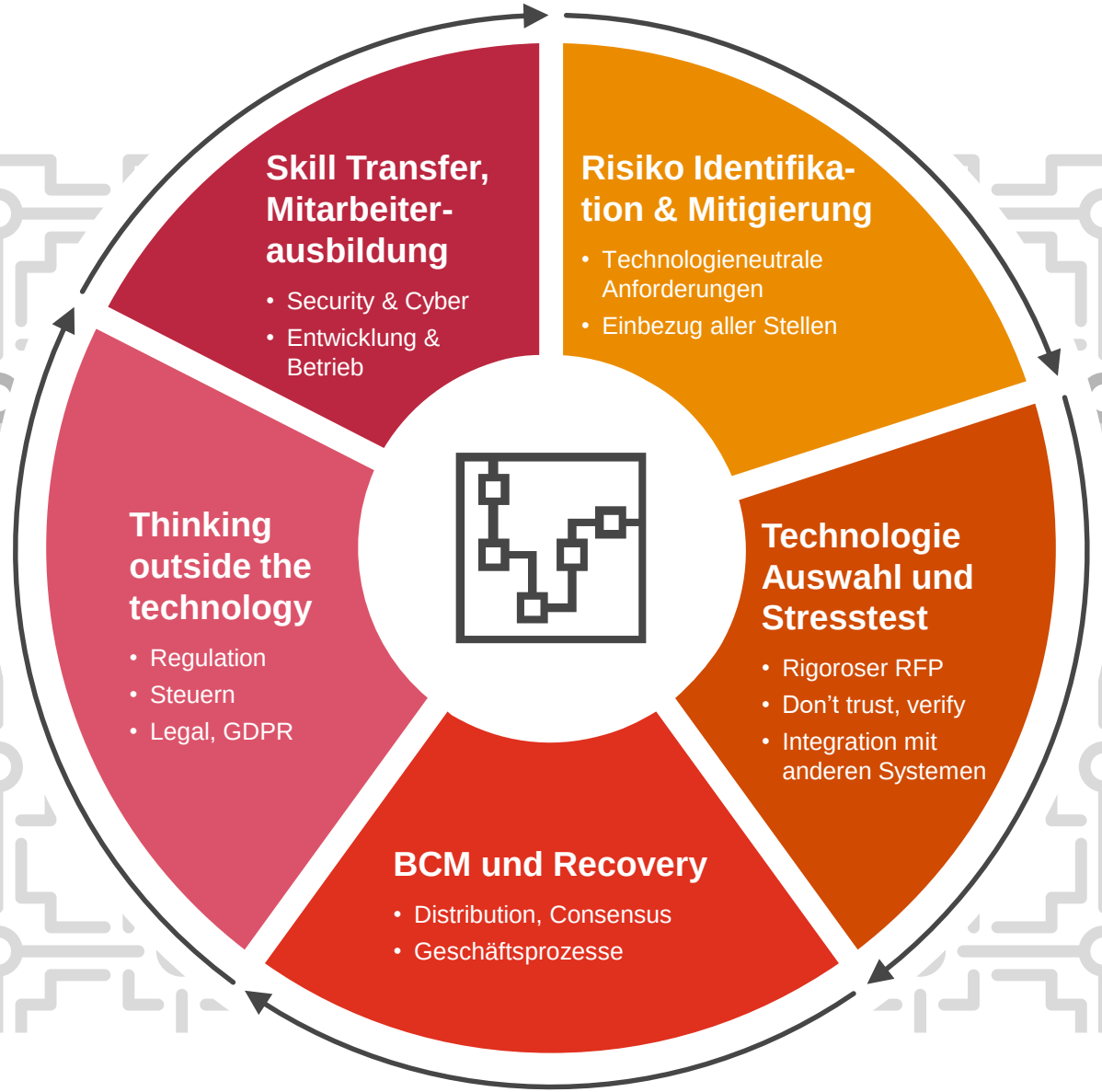
Blockchain als Technologie-Plattform

Aspekte für Due Diligence in der Technologie-Auswahl

- Robustheit und Art des Konsens Mechanismus (z.B. proof of work, proof of stake), Auswirkungen auf Master Data Management
- Robustheit der technischen Umsetzung der Blockchain
- Mitigierung von Cyber Risiken durch kryptographische Verschlüsselung, kontrollierte Benutzerberechtigungen
- Geschwindigkeit und Transaktionsdurchsatz
- Auditierbarkeit
- Erfahrung und Reputation der für das Projekt relevanten Führungspersonen (Business und Technologie) (ICO)
- Robustheit des beabsichtigten Business Plan (ICO)

Blockchain Go-Live Assurance

Risiko-Zyklus



3

Crypto Asset Risiken

“Weg ist weg

Sichere Aufbewahrung von Crypto Assets

Sicherheit der Privatschlüssel

- Sicherheit des Wallets zur Speicherung der Privatschlüssel
  - Hot Wallets wie z.B. Hardware Security Module (HSM)
  - Cold Wallets, z.B. «Paper» Wallet und andere offline Lösungen
- Sichere, zufällige Erstellung der Privatschlüssel
- Schutz der Privatschlüssel vor Verlust (BCM, Backup)
- Prozesse zum Schutz vor unautorisierten Transaktionen
- Konstante Überwachung der Transaktionen

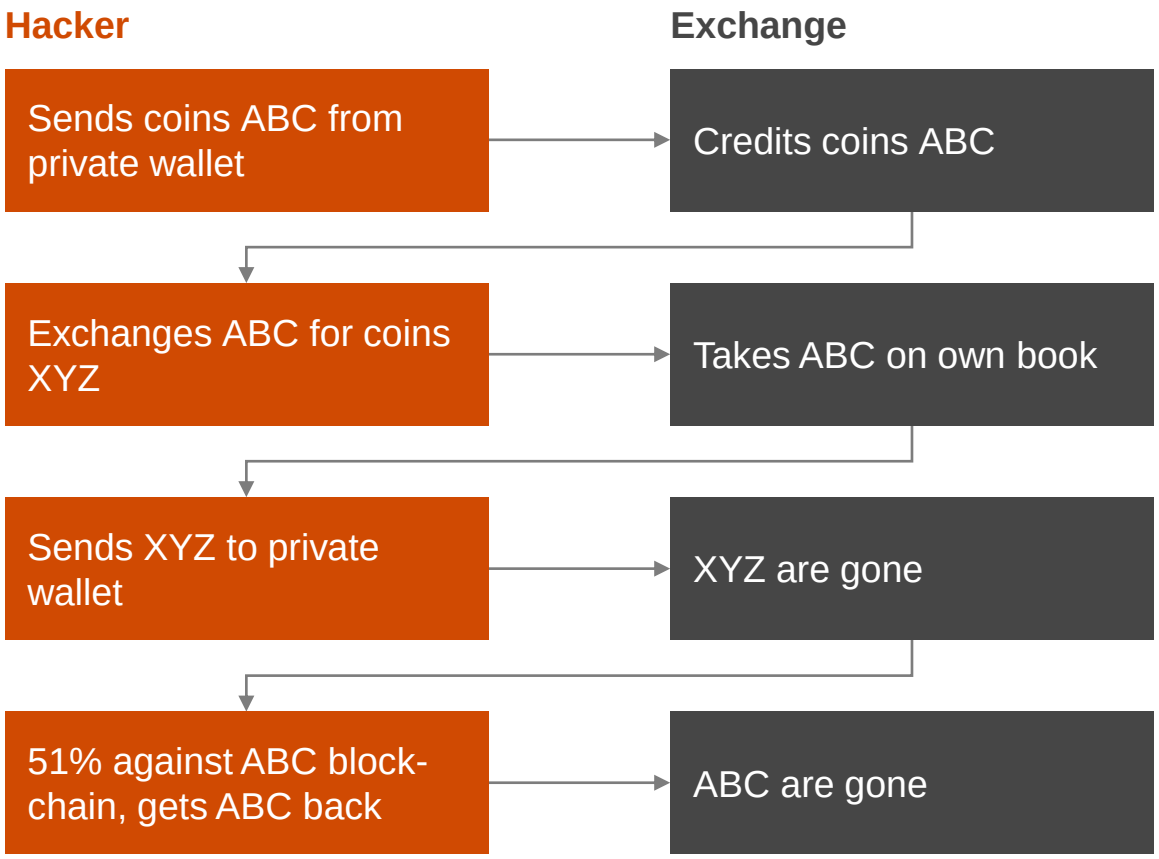
Aspekte zur Aufbewahrung

- Überwachung von allenfalls an Dritte ausgelagerte Aufbewahrung (Custodians, Exchanges) durch Audits oder Control Reports
- Multi-sig Unterzeichnungsberechtigungen zum Auslösen von Transaktionen als technische Implementation des Vier- oder Mehraugenprinzips
- Erhöhte Cyber-Risiken in den angeschlossenen Systemen

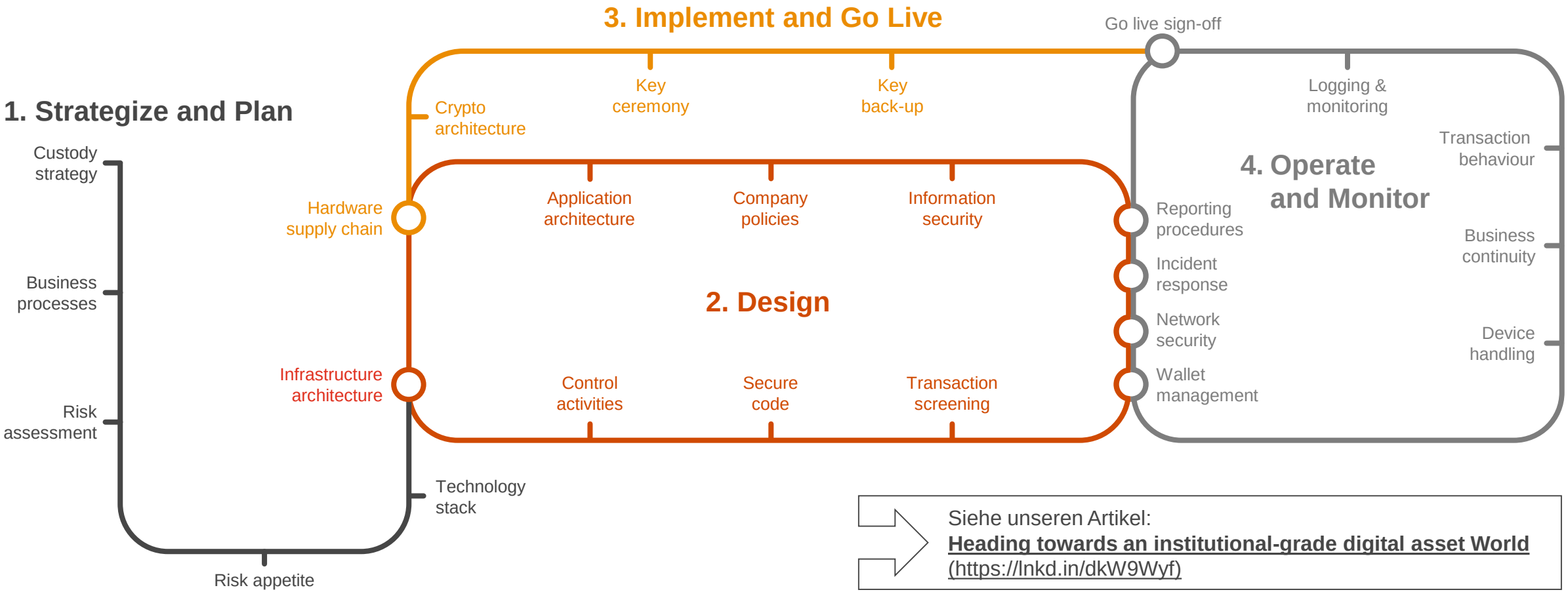
51% Attacke

Ablauf 51% Attacke auf Exchange

- Hacker sendet eigene ABC Coins von einem privaten, pseudonymen Wallet zum Exchange
- Tauscht ABC gegen andere Währung XYZ; damit wird Exchange (oder andere Exchange-Kunde) Eigentümer von ABC
- Hacker sendet XYZ weg vom Exchange auf ein privates, pseudonymes Wallet, somit hat Exchange keinen Zugriff mehr auf XYZ
- Hacker verwendet Mining Pool mit viel Rechenkraft zur 51% Attacke auf die ABC-Blockchain, schreibt die Blockchain um, so dass die initiale Transaktion rückgängig gemacht wird und der Hacker wieder im Besitz der ABC Coins ist. Es sieht aus, als hätten diese Coins nie das Wallet verlassen



Vier Schritte zur sicheren Crypto Custody Lösung



Siehe unseren Artikel:
Heading towards an institutional-grade digital asset World
(https://lnkd.in/dkW9Wyf)

4

Risiken und Compliance in Crypto Geschäftsmodellen

“

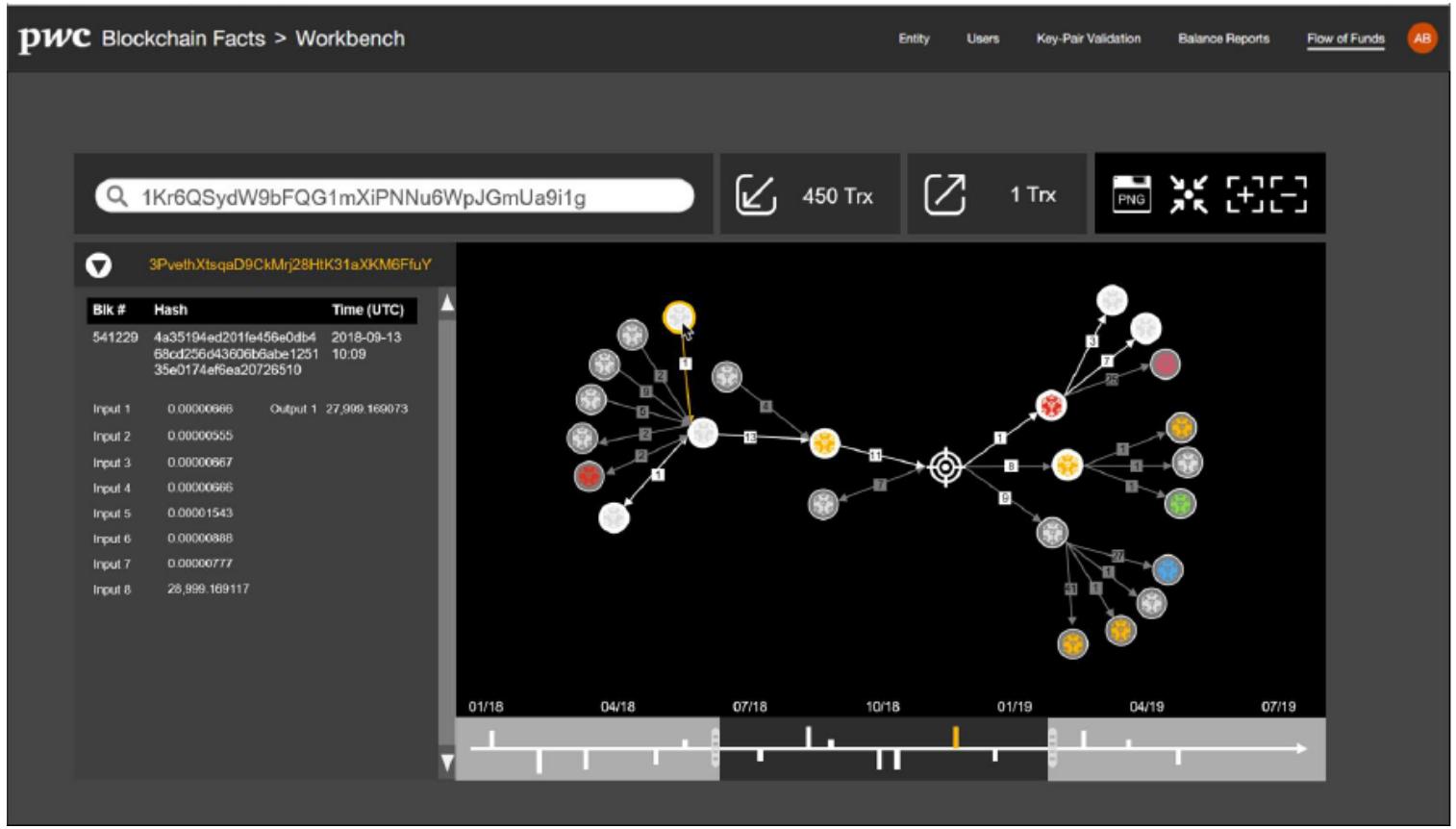
Von der FINMA beaufsichtigte Institute dürfen Kryptowährungen oder andere Token grundsätzlich nur an externe Wallets ihrer eigenen, bereits identifizierten Kunden schicken und auch nur von solchen Kryptowährungen oder Token entgegennehmen. FINMA-Beaufsichtigte dürfen keine Token von Kunden von anderen Instituten empfangen oder zu Kunden von anderen Instituten senden.

FINMA-Aufsichtsmitteilung: Konsequente Geldwäschereibekämpfung im Blockchain-Bereich, 26.8.2019

Analyse von Transaktionen am Beispiel Blockchain Facts

Analyse von Wallets und Transaktionen

- Herkunft von Crypto Assets
- Bestätigung des Eigentums
- Erkennbare illegale Aktivitäten
- Klassierung und Gruppierung von Adressen
- Monitoring der eigenen Adressen



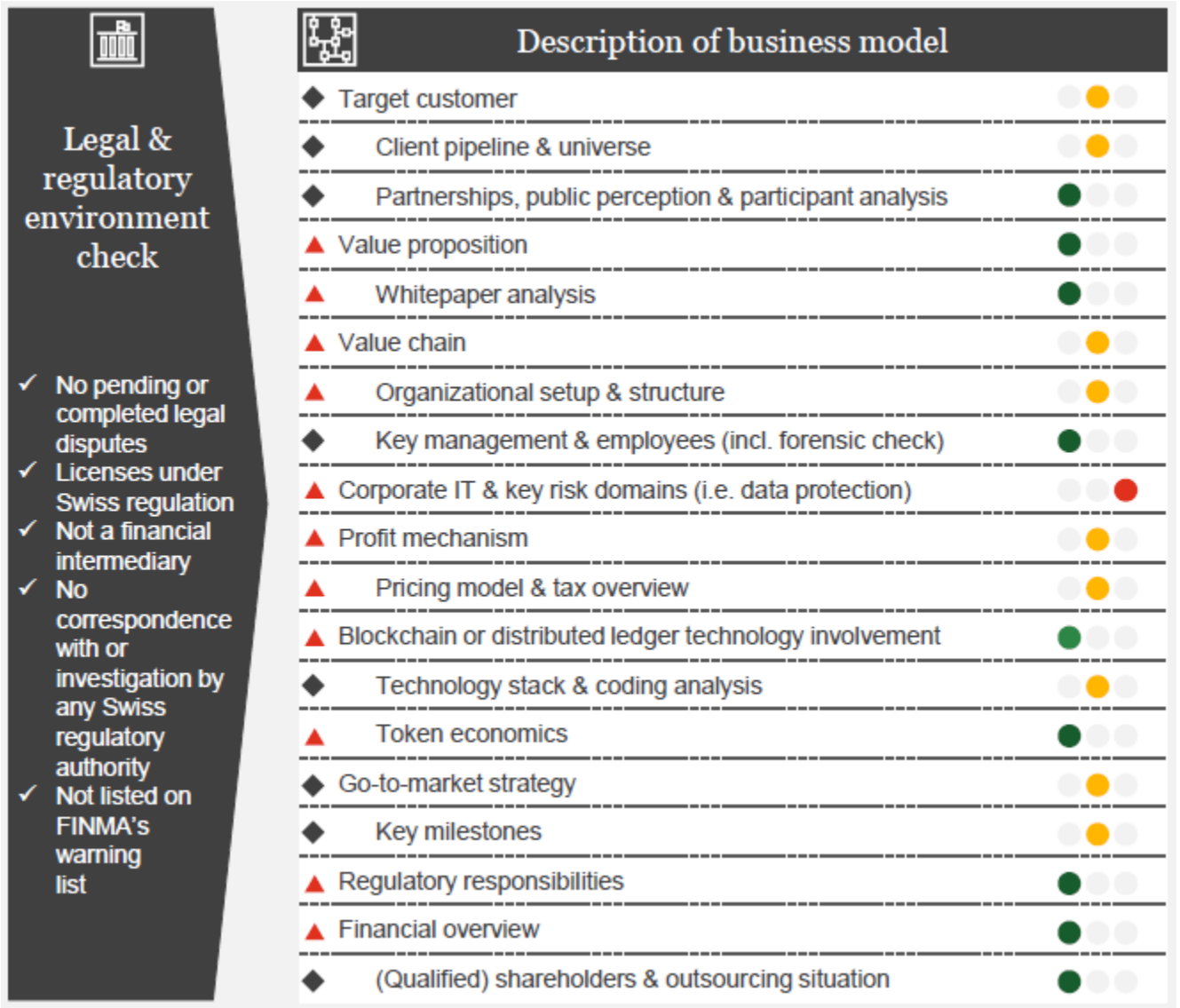
Geschäftsbeziehungen mit Crypto Unternehmungen

«Crypto Unternehmungen können kein Bankkonto eröffnen»

Schweizerische Bankiervereinigung (SBVg) veröffentlichte Leitfaden zur Eröffnung von Firmenkonti für Blockchain-Unternehmen.

- Good Governance
- Herausgabe von Tokens
- Finanzierung mit Crypto Assets (ICO/STO)
- Sorgfaltspflichten
- Geschäftsmodelle

Crypto Unternehmungen lassen DLT Transparency Report erstellen, welcher relevante Punkte bestätigt.



Grafik zeigt Auszug aus Beispiel-Transparency-Report ▶

5

Zusammenfassung

Thank you

Markus Perdrizat

Head of Blockchain Risk Assurance

markus.perdrizat@ch.pwc.com

Mobile: +41 79 345 4064

Jan Albers

Senior Consultant Risk Assurance

jan.albers@ch.pwc.com

Mobile: +41 79 431 3195

pwc.ch