

Operationelle Risiken in Blockchain Geschäftsmodellen

Oktober 2019



Agenda

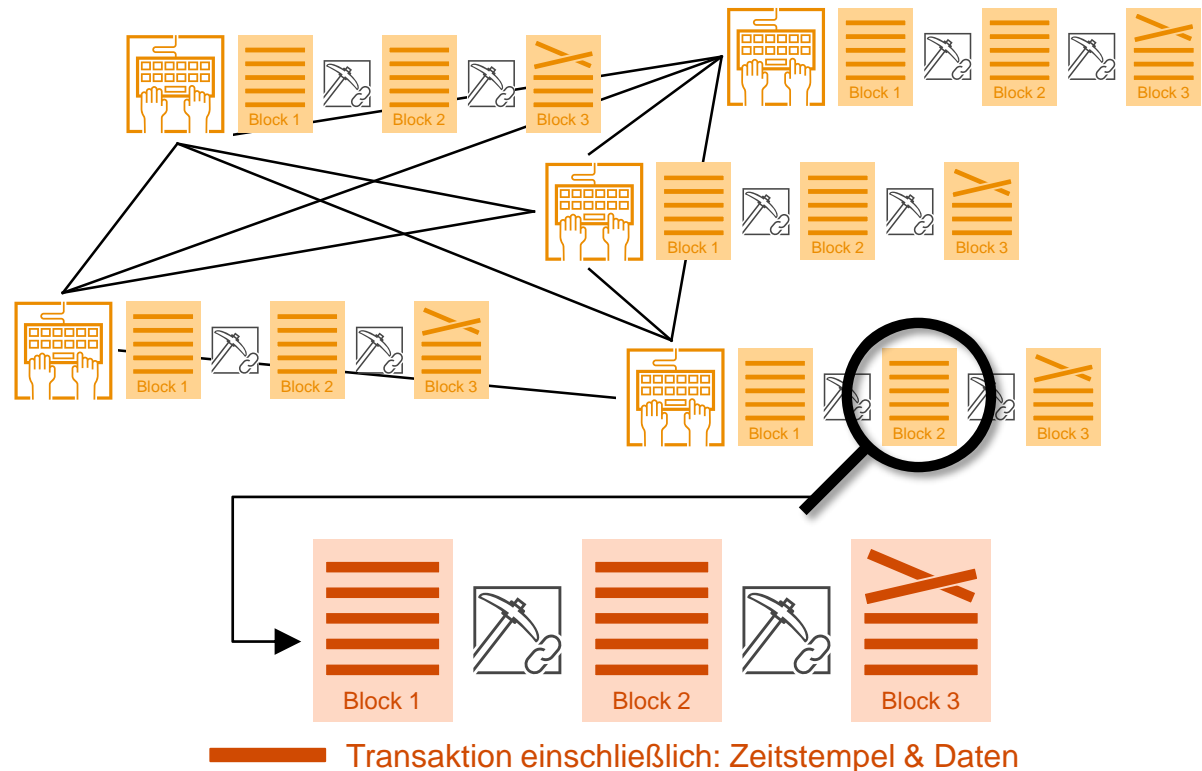
1. Einführung in Blockchain & Crypto Asset Geschäftsmodelle
2. Blockchain Technologie Risiken
3. Crypto Asset Risiken
4. Risiken und Compliance in Crypto Geschäftsmodellen
5. Zusammenfassung



Einführung
Blockchain &
Crypto Asset
Geschäftsmodelle

Einführung in Blockchain

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



Verteiltes, dezentrales Hauptbuch (Ledger)

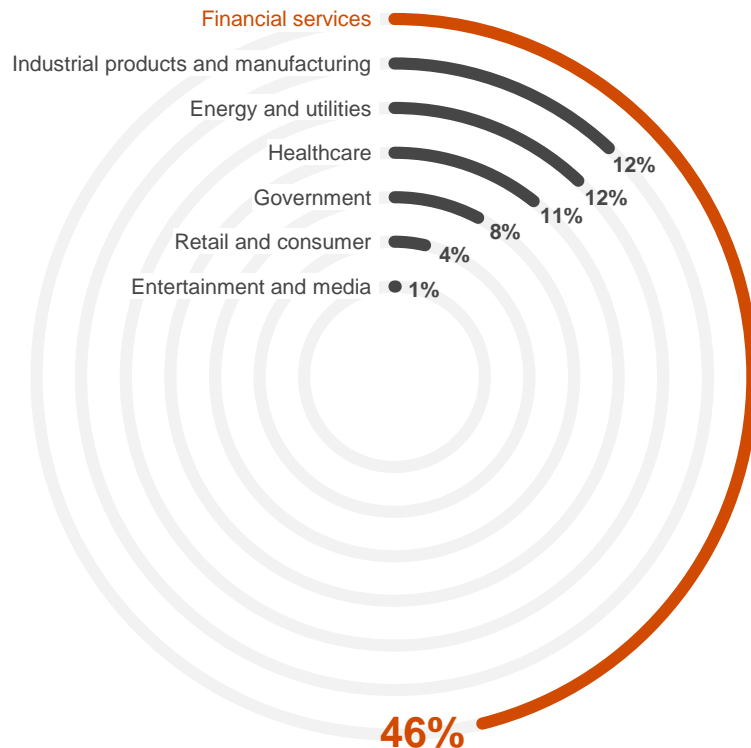
- Kontinuierlich wachsend
- Anreiz zur Bestätigung von Transaktionen durch Mining
- Liste der Transaktionen basierend auf Blöcken
- Jeder Block ist mit dem vorherigen durch einen Hash kryptographisch verknüpft.



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

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

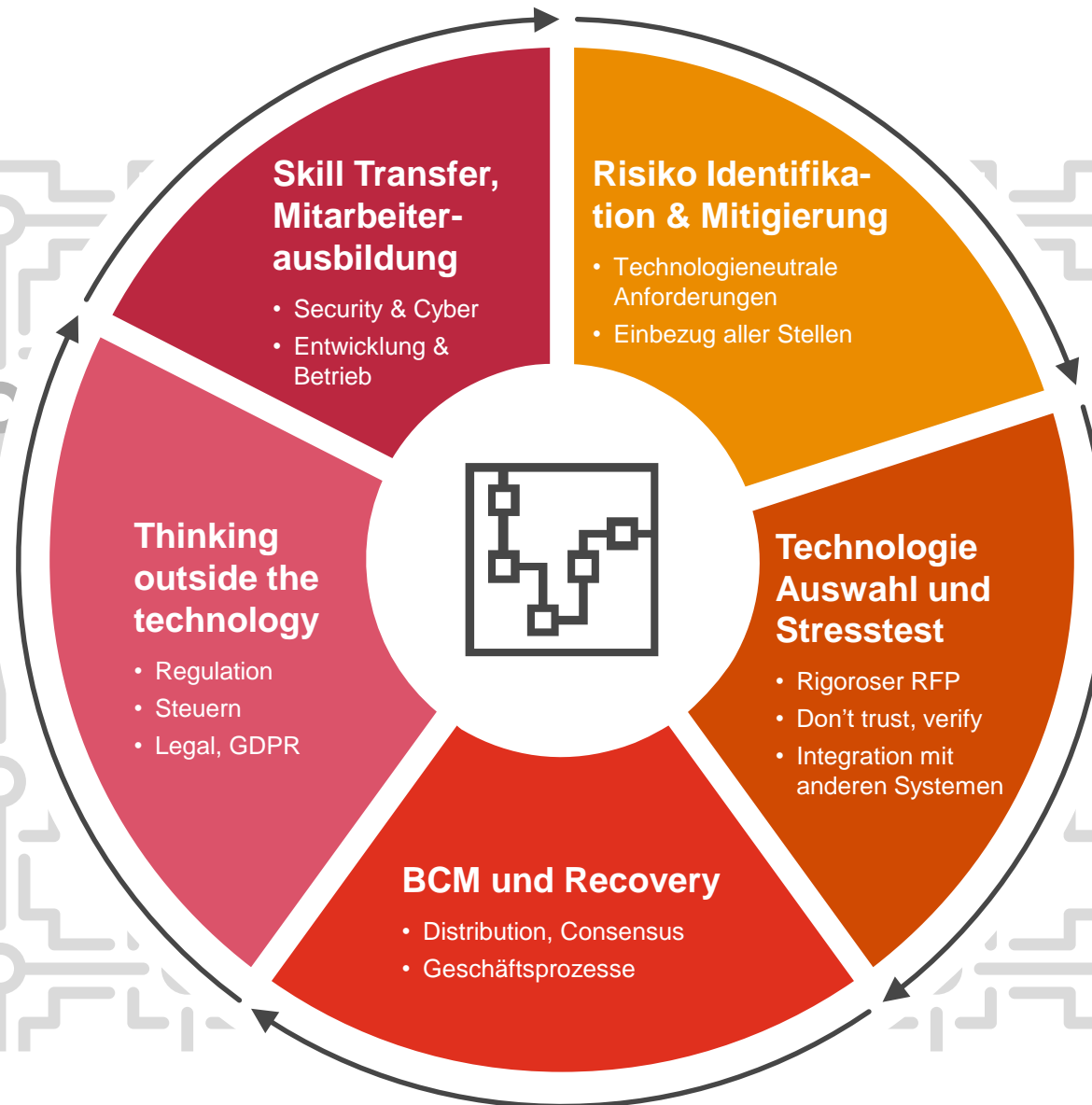


Aspekte für Due Diligence in der Technologie-Auswahl

- 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 Wahrung XYZ; damit wird Exchange (oder andere Exchange-Kunde) Eigentumer 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 ruckgangig gemacht wird und der Hacker wieder im Besitz der ABC Coins ist. Es sieht aus, als hatzen diese Coins nie das Wallet verlassen

Hacker

Sends coins ABC from private wallet

Exchanges ABC for coins XYZ

Sends XYZ to private wallet

51% against ABC blockchain, gets ABC back

Exchange

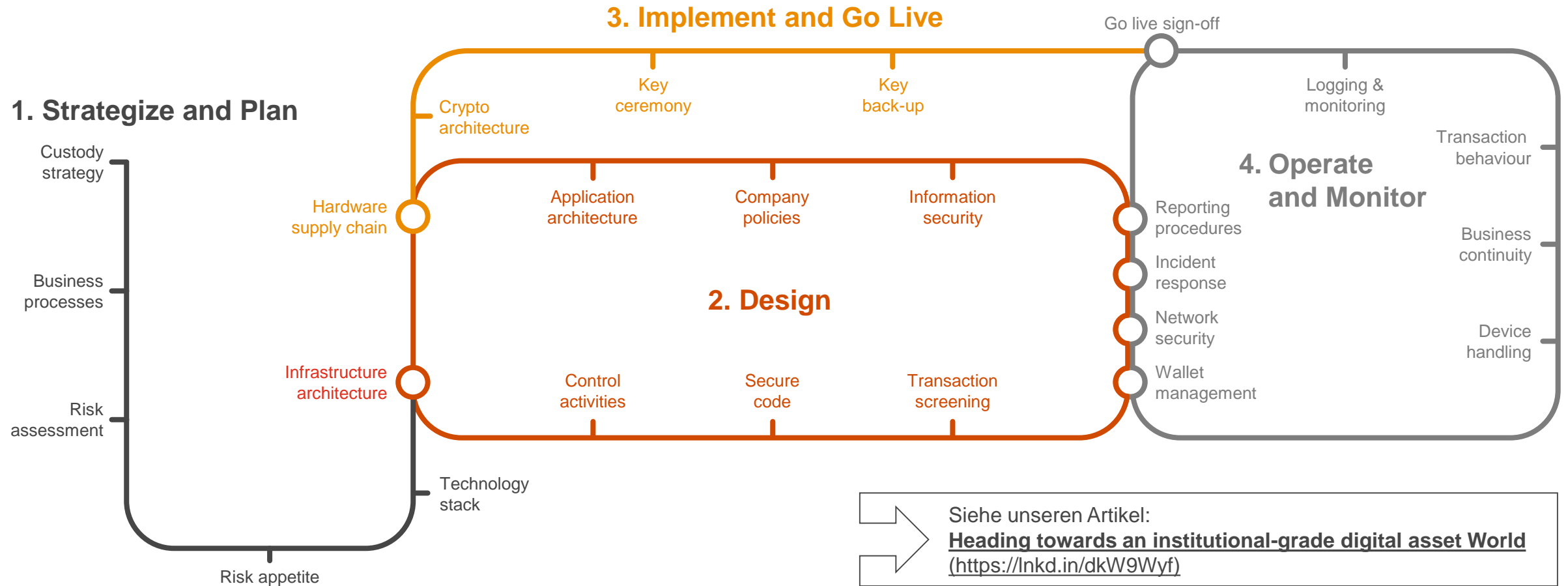
Credits coins ABC

Takes ABC on own book

XYZ are gone

ABC are gone

Vier Schritte zur sicheren Crypto Custody Lösung



Siehe unseren Artikel:
Heading towards an institutional-grade digital asset World
(<https://lnkd.in/dkW9WYyf>)

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.

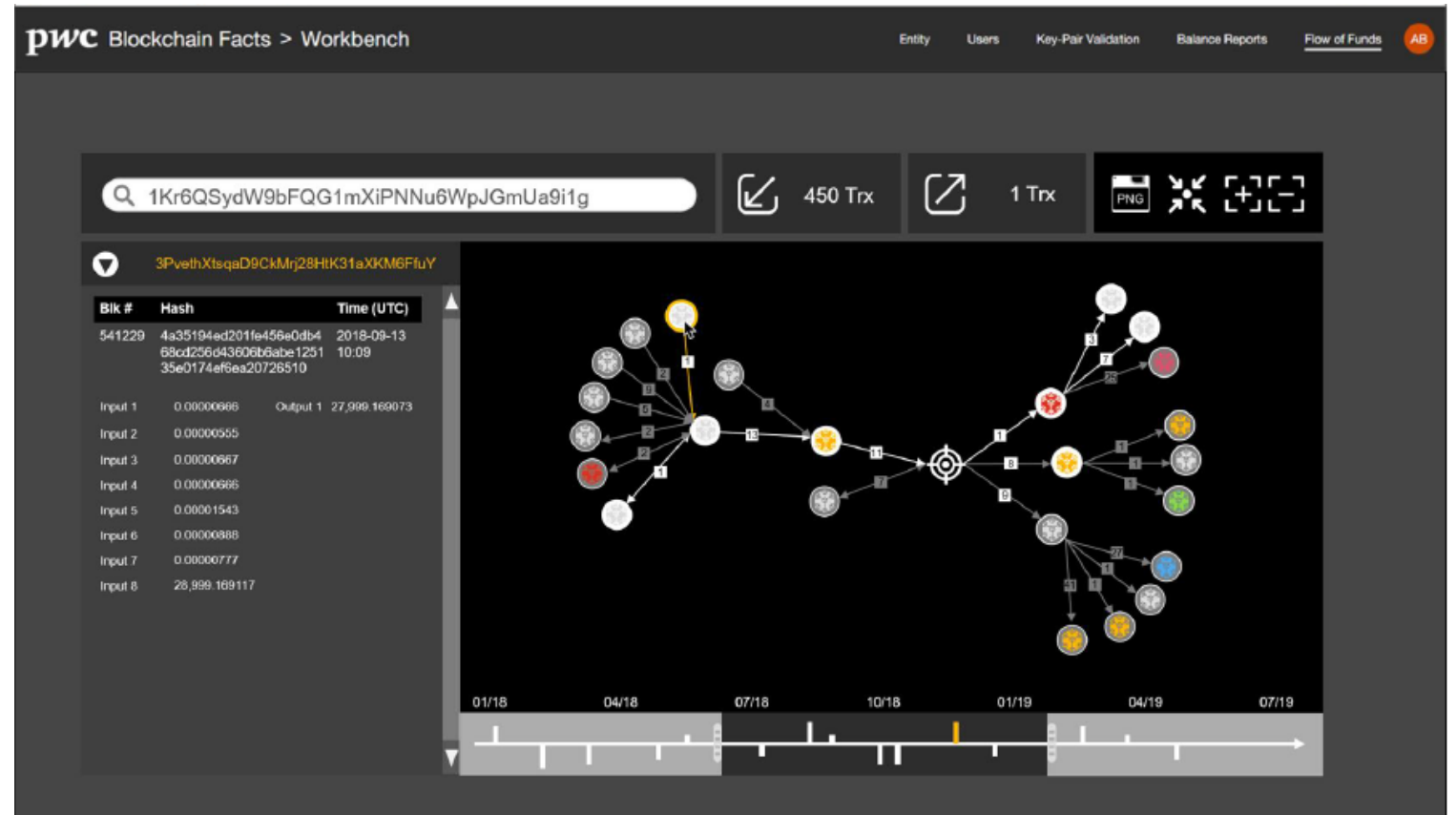
FINMA-Aufsichtsmitteilung: Konsequente Geldwäschereibekämpfung im Blockchain-Bereich, 26.8.2019

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 Unternehmen





«Crypto Unternehmen 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 Unternehmen lassen [DLT Transparency Report](#) erstellen, welcher relevante Punkte bestätigt.

 Legal & regulatory environment check	 Description of business model
<ul style="list-style-type: none"> ✓ No pending or completed legal disputes 	<ul style="list-style-type: none"> ◆ Target customer ● ● ●
<ul style="list-style-type: none"> ✓ Licenses under Swiss regulation 	<ul style="list-style-type: none"> ◆ Client pipeline & universe ● ● ●
<ul style="list-style-type: none"> ✓ Not a financial intermediary 	<ul style="list-style-type: none"> ◆ Partnerships, public perception & participant analysis ● ● ●
<ul style="list-style-type: none"> ✓ No correspondence with or investigation by any Swiss regulatory authority 	<ul style="list-style-type: none"> ▲ Value proposition ● ● ●
<ul style="list-style-type: none"> ✓ Not listed on FINMA's warning list 	<ul style="list-style-type: none"> ▲ Whitepaper analysis ● ● ●
	<ul style="list-style-type: none"> ▲ Value chain ● ● ●
	<ul style="list-style-type: none"> ▲ Organizational setup & structure ● ● ●
	<ul style="list-style-type: none"> ◆ Key management & employees (incl. forensic check) ● ● ●
	<ul style="list-style-type: none"> ▲ Corporate IT & key risk domains (i.e. data protection) ● ● ●
	<ul style="list-style-type: none"> ▲ Profit mechanism ● ● ●
	<ul style="list-style-type: none"> ▲ Pricing model & tax overview ● ● ●
	<ul style="list-style-type: none"> ▲ Blockchain or distributed ledger technology involvement ● ● ●
	<ul style="list-style-type: none"> ◆ Technology stack & coding analysis ● ● ●
	<ul style="list-style-type: none"> ▲ Token economics ● ● ●
	<ul style="list-style-type: none"> ◆ Go-to-market strategy ● ● ●
	<ul style="list-style-type: none"> ◆ Key milestones ● ● ●
	<ul style="list-style-type: none"> ▲ Regulatory responsibilities ● ● ●
	<ul style="list-style-type: none"> ▲ Financial overview ● ● ●
	<ul style="list-style-type: none"> ◆ (Qualified) shareholders & outsourcing situation ● ● ●

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

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers AG, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2019 PwC. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers AG which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.