



AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Anwendungsfälle und Potenziale der Blockchain im Handel

Dr. Ross King

Senior Scientist

Thematic Coordinator Data Science

AIT Austrian Institute of Technology GmbH

ANERKENNUNG

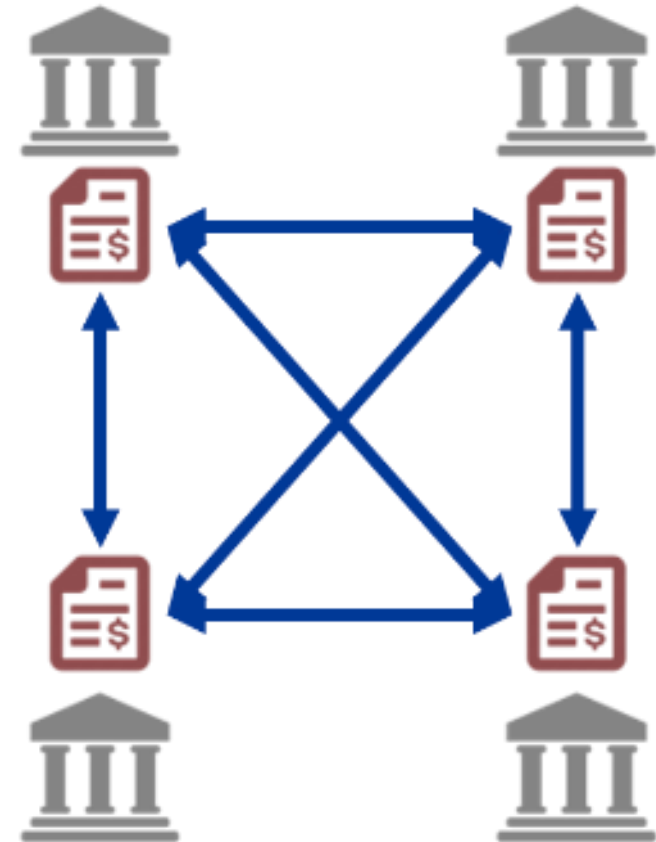
Diese Arbeit wurde durch die Austrian Development Agency, den Handelsverband, Import Austria und CRIF GmbH gefördert.

BLOCKCHAINS

Grundkonzepte

Was ist eine Blockchain?

- Eine Art *verteiltes Register* (*distributed ledger*).
- Eine Technologie, die es Personen, welche sich nicht kennen, erlaubt, einer gemeinsamen Aufzeichnung von Ereignissen zu vertrauen.
- Daten werden in sogenannten **Blöcken** gespeichert.
- Jeder Block enthält eine Referenz auf den vorhergehenden und den nächsten Block; dadurch entsteht eine Kette.



Underlying Technologies

Hashfunktionen

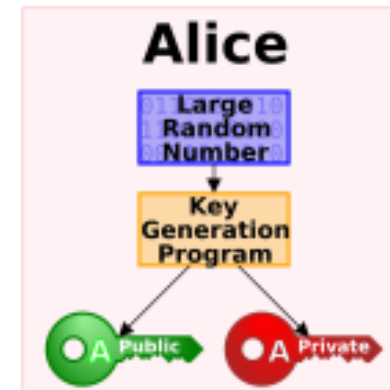
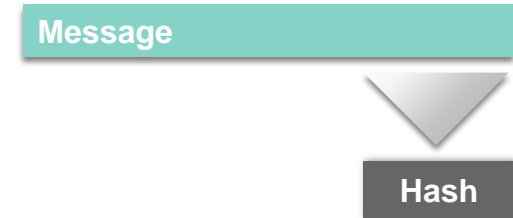
- Eindeutige Identifikation von Transaktionen
- Verhindert die Manipulation von Transaktionen

Asymmetrische Verschlüsselung

- Geheimhaltung
- Nichtabstreitbarkeit

Peer-to-Peer Netzwerke

- Dezentralisierung
- Fehlertoleranz



Blockchain Konsensus

Zwei Modelle des Konsensus-Mechanismus

- **Nakamoto Konsensus**

Zufällige, algorithmische Bestimmung eines Leiters ("Lotterie")

- Proof-of-Work (PoW) (*Bitcoin, Ethereum*)

→ geeignet für **offene** (öffentliche) Netzwerke



- **Byzantine Fault Tolerance (BFT)**

Abstimmung (auch mehrfach) unter den Mitgliedern, um einen Konsens zu erreichen

→ geeignet für **geschlossene** (private) Netzwerke

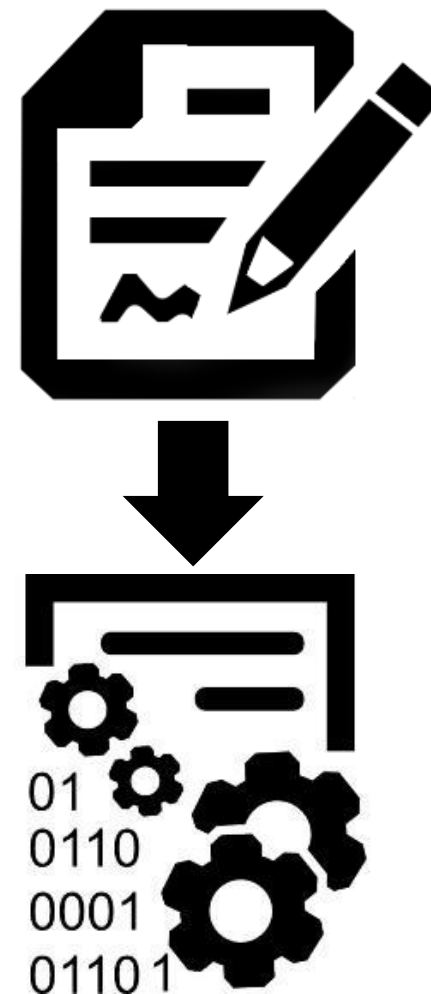
Smart Contracts

Smart Legal Contracts

- Rechtstexte, die so formuliert sind, dass sie in Smart Contract Code ausgedrückt und implementiert werden können, um diesem dadurch Legitimität zu verleihen.

Smart Contract Code

- Software, geschrieben in einer Programmiersprache und dazu gedacht, für die sie einsetzende Partei im Rahmen einer verteilten Buchführung automatisch bestimmte Verpflichtungen zu erfüllen, Rechte wahrzunehmen und gegebenenfalls Kontrolle über Kapital zu übernehmen.
- Daher übernimmt sie Aufgaben und Verantwortlichkeiten durch die Ausführung von Code, der die Vertragslogik der echten Welt modelliert oder nachbildet, obwohl die rechtliche Grundlage dafür möglicherweise unklar ist.



ANWENDUNGEN

Use Case: Einzelhändler und ihre Supply Chain

Beispiel: Bio-Shrimps

Motivation

- Biolebensmittel sind ein Wachstumsmarkt
- Entsprechende Zertifizierung erfordert umfangreiche Dokumentation
- biologischer Anbau führt zu mehr Nachhaltigkeit

Blockchain Lösung

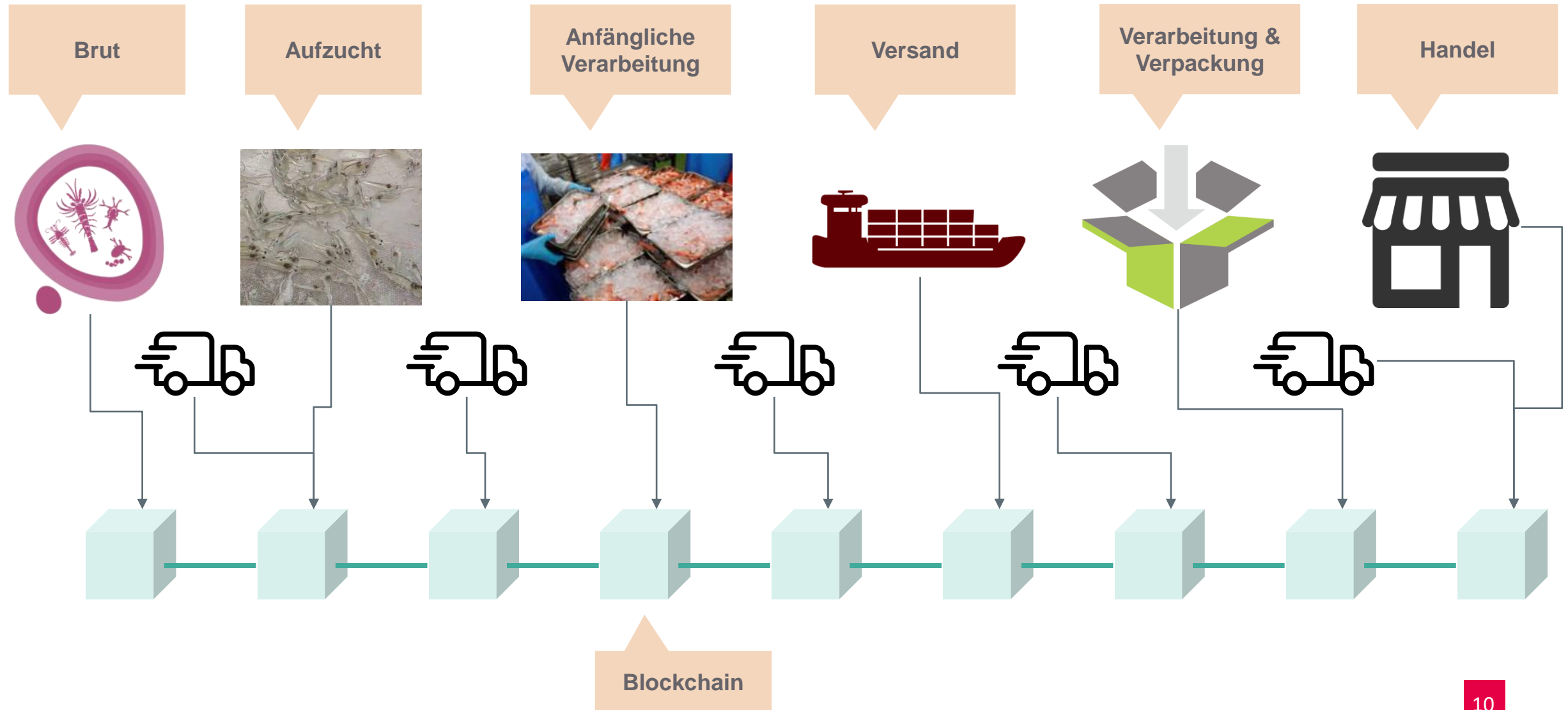
- Dokumentation sämtlicher Zwischenschritte und Transaktionen der Supply Chain in einer Blockchain

Nutzen

- Vertrauenswürdigere Zertifizierungen
- Einzelhändler erhalten Zugang zu lukrativen Märkten
- Landwirte können den Verkaufswert ihrer Produkte erhöhen



Use Case: Einzelhändler und ihre Supply Chain



Use Case: Rückverfolgung stärkt Exporteure

Beispiel: Kakaoproduktion

Motivation

- Produzenten sollen nicht nur angeben was sie anbieten, sondern auch zu welchen Bedingungen
 - Menge, Preis, **Qualität**

Blockchain Lösung

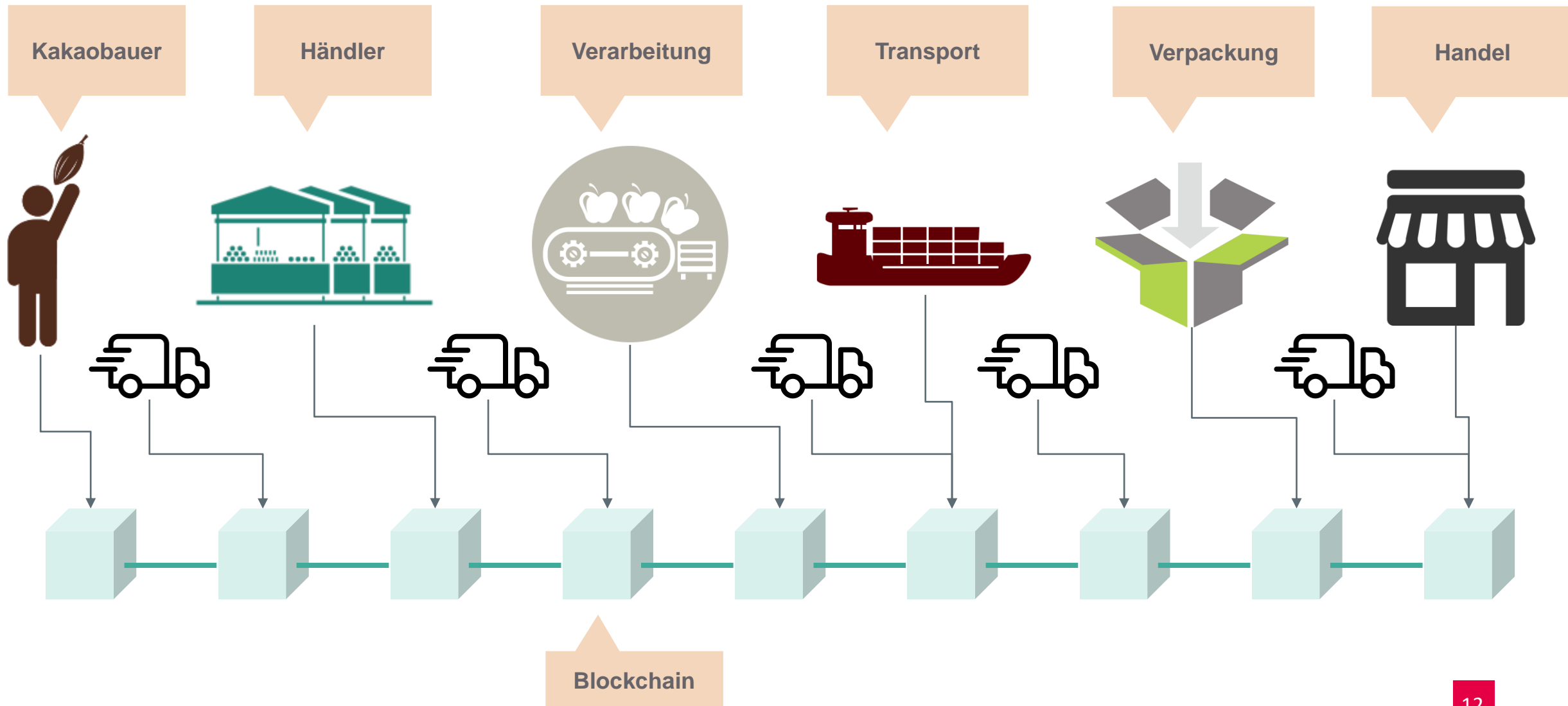
- Übertragung aller relevanten Informationen (Farm, Produktionsmethoden, Verarbeitung, etc.) in eine Blockchain

Nutzen

- Bauern bekommen Zugang zu:
 - neuen Absatzmärkten
 - besseren Versicherungen
 - besseren Krediten



Use Case: Rückverfolgung stärkt Exporteure



Auswertung Rückverfolgung

Stärken der Blockchain

- Robustes, offenes, dezentralisiertes Netzwerk
- Bereitstellung eines unveränderlichen Transaktionsdatensatzes

Schwächen der Blockchain

- Erfordert Infrastruktur, die in aufstrebenden Regionen möglicherweise nicht zuverlässig verfügbar ist
- Lösung erfordert Vertrauen außerhalb der Blockchain
- Prioritäten werden nicht behandelt (Produktivität)
- Bereits etablierte, zentralisierte Anwendungen sind auf dem Markt erfolgreich

Use Case: Verbesserung der Kreditwürdigkeit

Beispiel: Reputationssysteme

Motivation

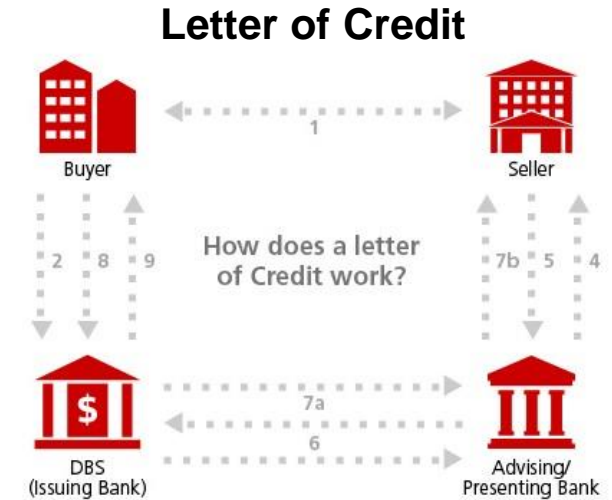
- Wie überzeugt man Importeure, das Risiko eines neuen Lieferanten einzugehen?

Blockchain Lösung

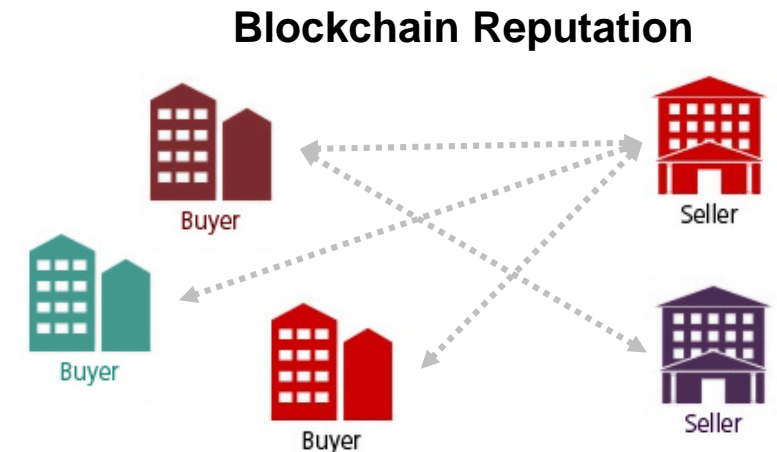
- Eine Peer-to-Peer Reputationsplattform
 - (Angelehnt an Letters of Credit)

Nutzen

- Exporteure erreichen neue Kunden
- Importeure finden neue Lieferanten



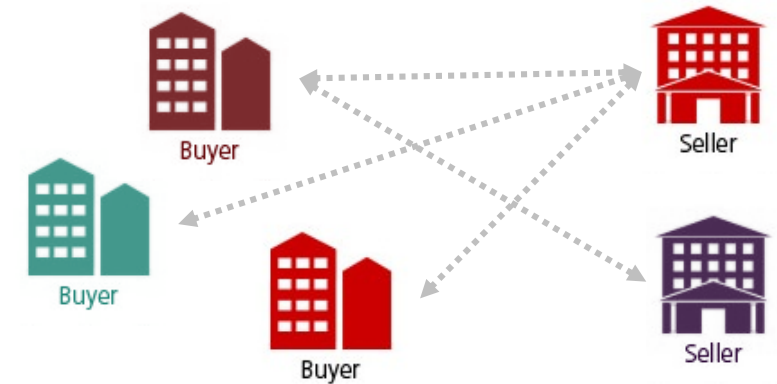
Quelle: <https://www.dbs.com.sg/sme/trade/import-services/letter-of-credit-issuance>



Verbesserung der Kreditwürdigkeit

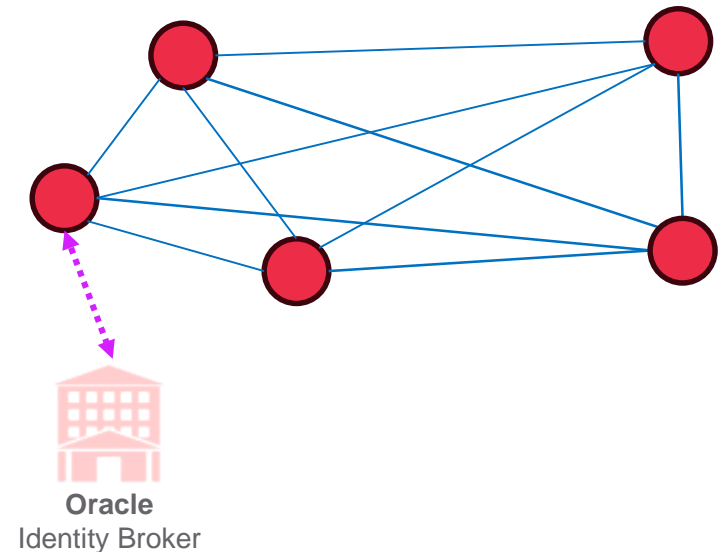
Stärken der Blockchain

- Positive Anreize für alle Teilnehmer
 - (externe Vertrauensprobleme wurden minimiert)
- Kein Mittelsmann erforderlich (im Unterschied zu Amazon, eBay) und dadurch effizienter



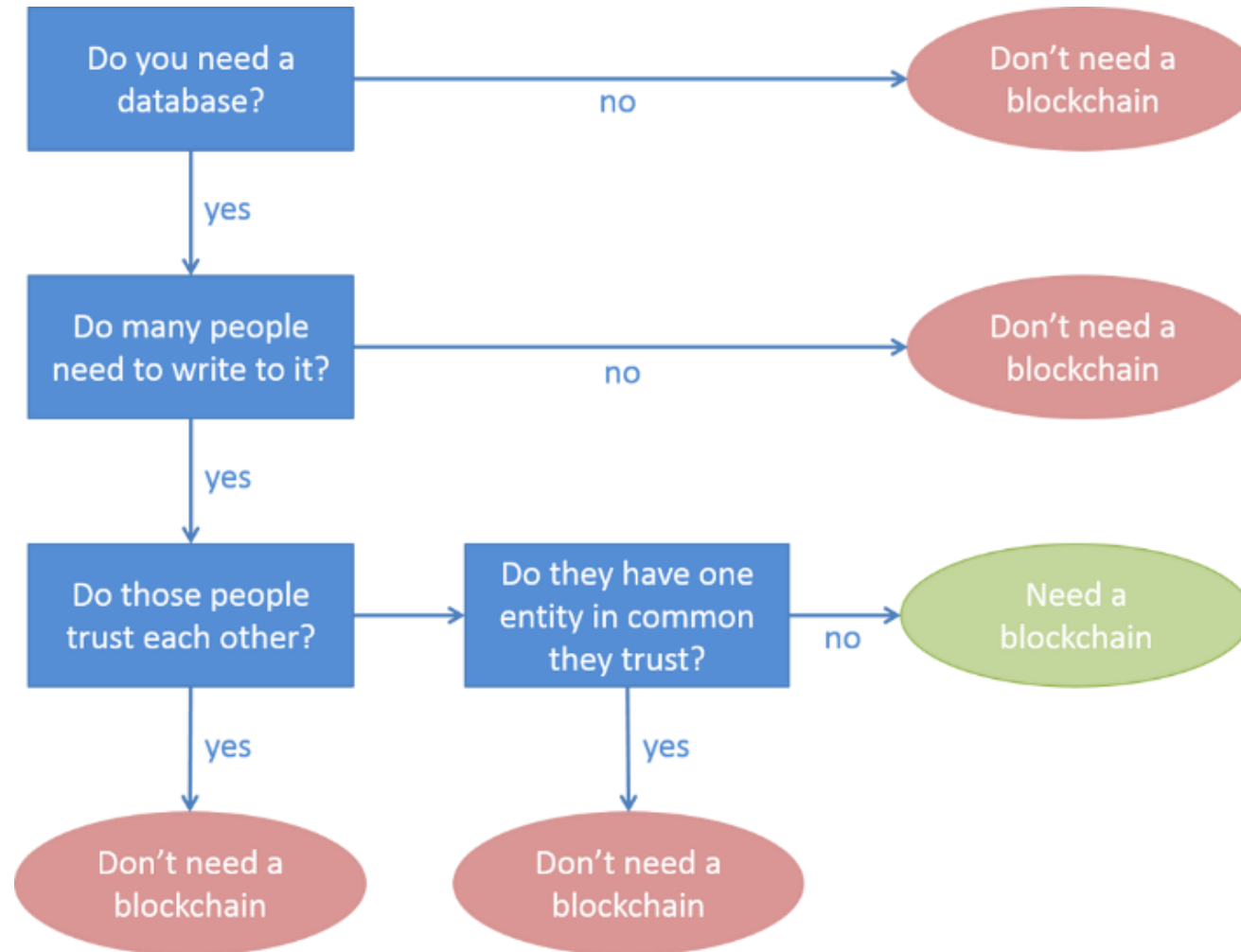
Schwächen der Blockchain

- Abhängigkeit von einem "Identity Broker Oracle"
 - Dies ist jedoch auch eine Stärke!
 - Bekannte Entitäten = Keine "Stroh Männer"
 - Geschäftsdaten außerhalb der Blockchain ermöglichen Einhaltung der GDPR



SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

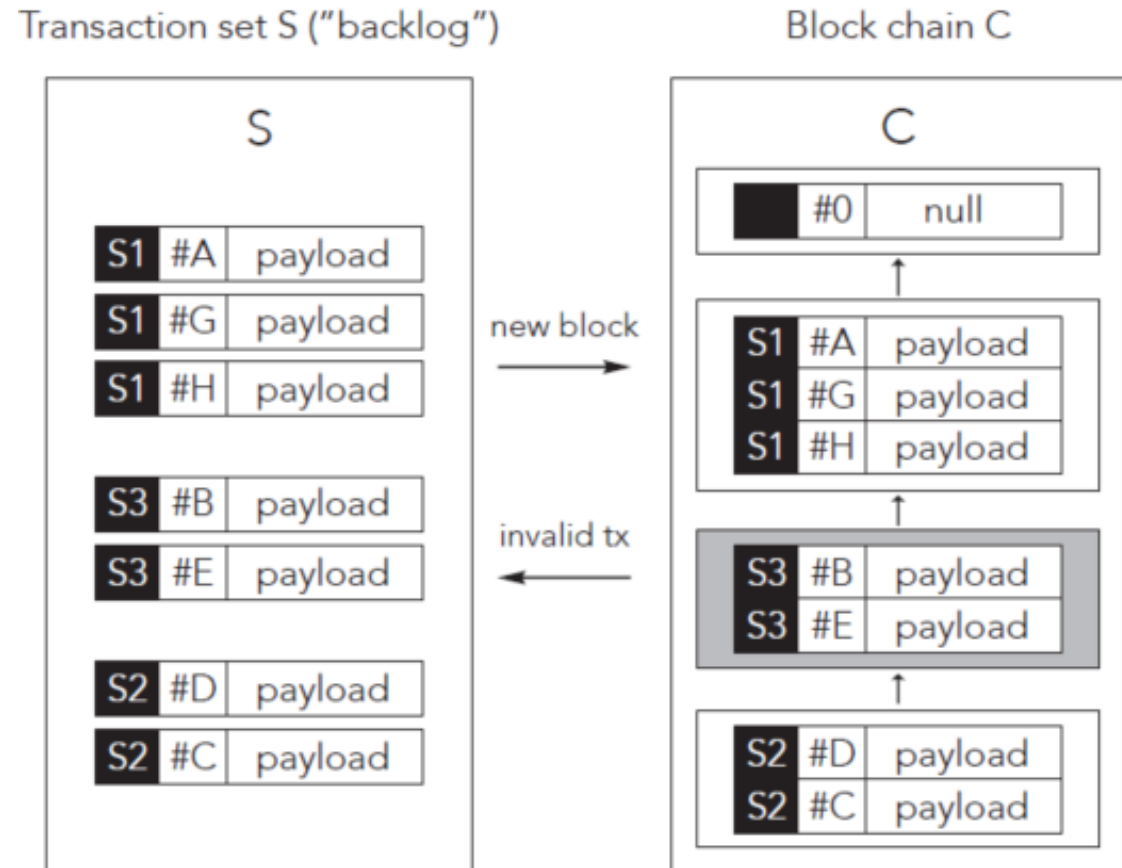
Wann brauche ich eine Blockchain?



Quelle: <http://blockchain.mazeus.eu/blog/when-to-use-a-blockchain>

Unveränderlichkeit innerhalb einer Blockchain?

- Unveränderlichkeit beruht auf Hashwerten und asymmetrischer Verschlüsselung.
- Diese Technologien können innerhalb von traditionellen relationalen Datenbanken eingesetzt werden.
- Sie können ebenfalls mit nicht-traditionellen, verteilten Datenbanken wie z.B. BigChainDB eingesetzt werden.



Trent McConaghy, Rodolphe Marques, Andreas Müller, Dimitri De Jonghe, T. Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto. Bigchaindb: A scalable blockchain database. Technical report, ascribe GmbH, 2016a.

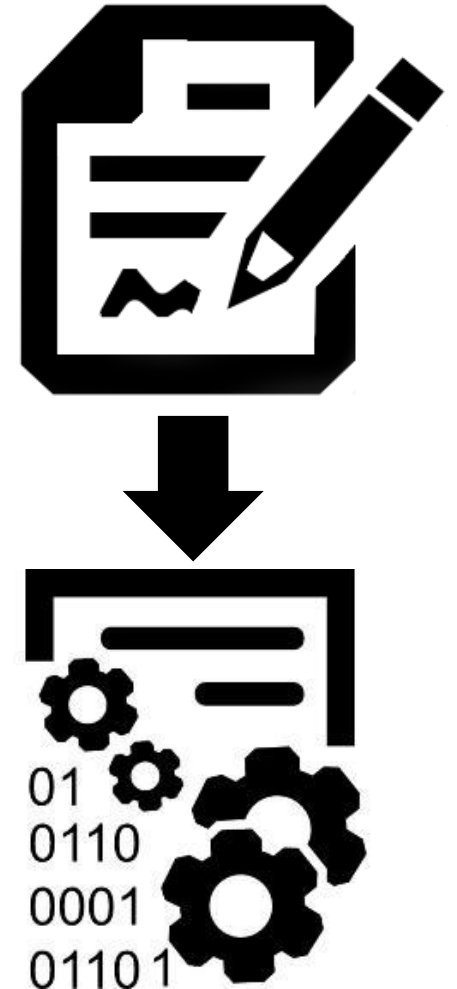
Smart Contracts – Vorsicht

Smart Legal Contracts

- Österreichisches E-Commerce-Gesetz (ECG)
- Bisherige Smart Contracts erfüllen die Anforderungen nicht
 - Der Nutzer muss u.a. über die folgenden Punkte verständlich und eindeutig informiert werden:
 - Die erforderlichen technischen Schritte, um den Vertrag abzuschließen und bekannt zu machen
 - Technische Mittel, um Fehler vor Abschluss des Vertrages zu Erkennen und zu beheben
- Rechtlicher Rahmen ohne Grundlage zur Durchsetzung

Smart Contract Code

- Herausforderungen
 - Bereitstellung von überprüfbarem Quellcode
 - Unveränderbarkeit des Codes



Schlussfolgerungen

Blockchains haben viele Vorteile für Supply Chains in Entwicklungsländern, unter anderem:

- Sichere und unveränderliche Transaktionshistorie
- Verteilte Architektur ohne Abhängigkeit von zentralen, vertrauenswürdigen Entitäten
- Widerstandsfähigkeit bei Hardwareversagen oder böswilligen Akteuren

Schlussfolgerungen

Wir haben **drei Anwendungen** im Zusammenhang mit Supply Chains in Entwicklungsländern untersucht:

- **Rückverfolgbarkeit in der Supply Chain**
 - Unterstützt Landwirte und Händler im lukrativen Biomarkt mit unveränderlichen Aufzeichnungen über Anbau und Transport, welche notwendig für entsprechende Zertifizierungen sind.
- **Rückverfolgbarkeit unterstützt Exporteure**
 - Blockchains erlauben es Bauern, Daten zu ihrer Farm, Produktionsmethoden, Verarbeitung, Ernte usw. zu kommunizieren und im Gegenzug Zugang zu neuen Märkten, besseren Versicherungen und besseren Kreditkonditionen zu bekommen.
- **Verbesserung von Kreditwürdigkeit**
 - Ein auf Blockchain basierendes Reputationssystem kann es Importeuren und Exporteuren ermöglichen, vertrauenswürdige Referenzen bereitzustellen und dadurch neue Kunden und Märkte zu finden.

Schlussfolgerungen

Wir haben verschiedene Herausforderungen in Bezug auf diese Use Cases identifiziert und festgestellt, dass Blockchains am effektivsten als **politische** oder **regulatorische** Lösungen sind, z.B. für

- Lebensmittelsicherheit
- Supply Chain Finanzierung

Der rechtliche Rahmen ist weiterhin unklar, allerdings werden offene Fragen in Bezug auf Rechtssicherheit und Steuern untersucht (z.B. Institut für Kryptoökonomie, WU Wien).

Blockchain Technologie entwickelt sich rasch weiter

- Neue Architekturen
- Neue Konsensprotokolle

Unsere Studie stellt ein Framework zur Verfügung, um zukünftige Technologien zu evaluieren.

DANKE FÜR IHRE AUFMERKSAMKEIT!

Dr. Ross King
AIT Austrian Institute of Technology GmbH
ross.king@ait.ac.at