Blockchain & Smart Contracts

Tobias Bitterli, Chief Product Officer

Windenergietage, 07. November 2019

Forum 16 - Aktuelle Themen

Ihr Referent: Tobias Bitterli

- Chief Product Officer & Mitgründer bei greenmatch AG
- Doktorand an der Universität Basel: Forschung im Bereich Blockchain, Distributed Ledger Technologies (DLT) & Kryptowährungen

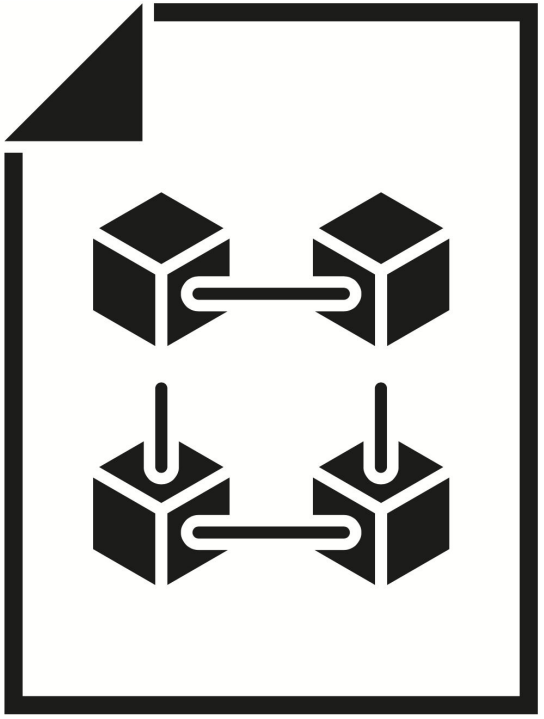
green[::]match | Finanzsoftware für erneuerbare Energien

Strukturieren, verwalten und vermarkten Sie Ihre Projekte in Windenergie, Photovoltaik, Wasserkraft und Biomasse zuverlässig und effizient. Die optimale Lösung für Projektentwickler, Investoren, Asset Manager, Banken und Berater.

1 Grundlagen

Eine Datenbank

Die Blockchain ist eine gemeinschaftlich geführte Datenbank



Datenbank

- Öffentliche Datenbank als Infrastruktur, die eine Vielzahl an Anwendungen ermöglicht

Charakteristika einer öffentlichen Blockchain

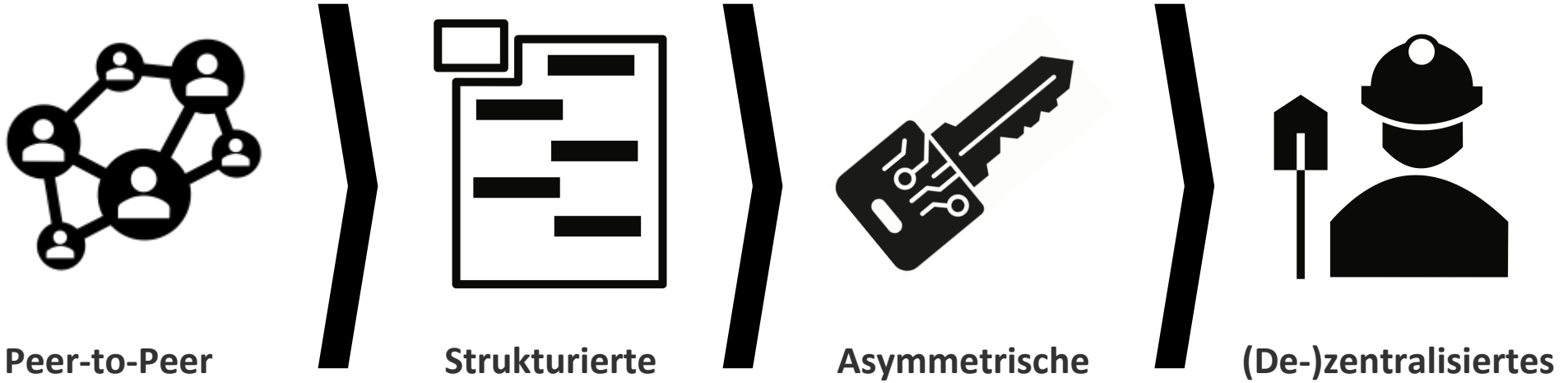
- Jeder kann eine Kopie der Blockchain halten
- Jeder kann alles eigenständig verifizieren
- Jeder kann die Blockchain erweitern

Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icon: istockphoto.com

Schlüsselkomponenten einer Blockchain

Kombination aus bestehenden Technologiekomponenten

→ Ziel: Eine dezentralisierte und nicht-manipulierbare Datenbank



Peer-to-Peer Netzwerk

Strukturierte Information

Asymmetrische Kryptografie

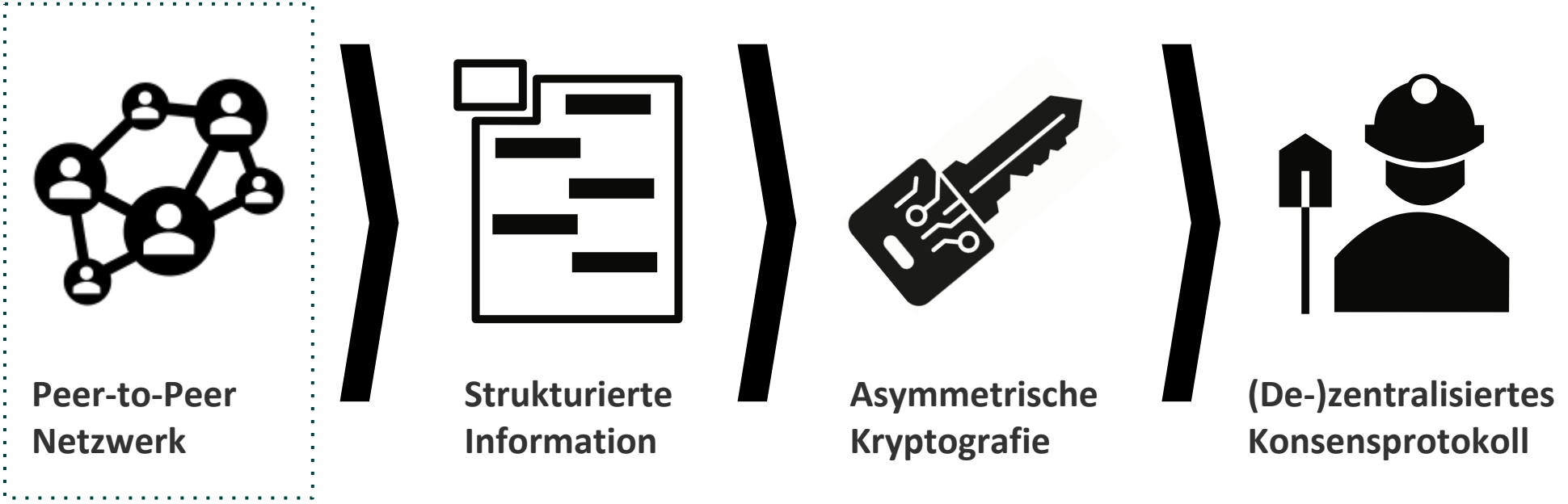
(De-)zentralisiertes Konsensprotokoll

Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Schlüsselkomponenten einer Blockchain

Kombination aus bestehenden Technologiekomponenten

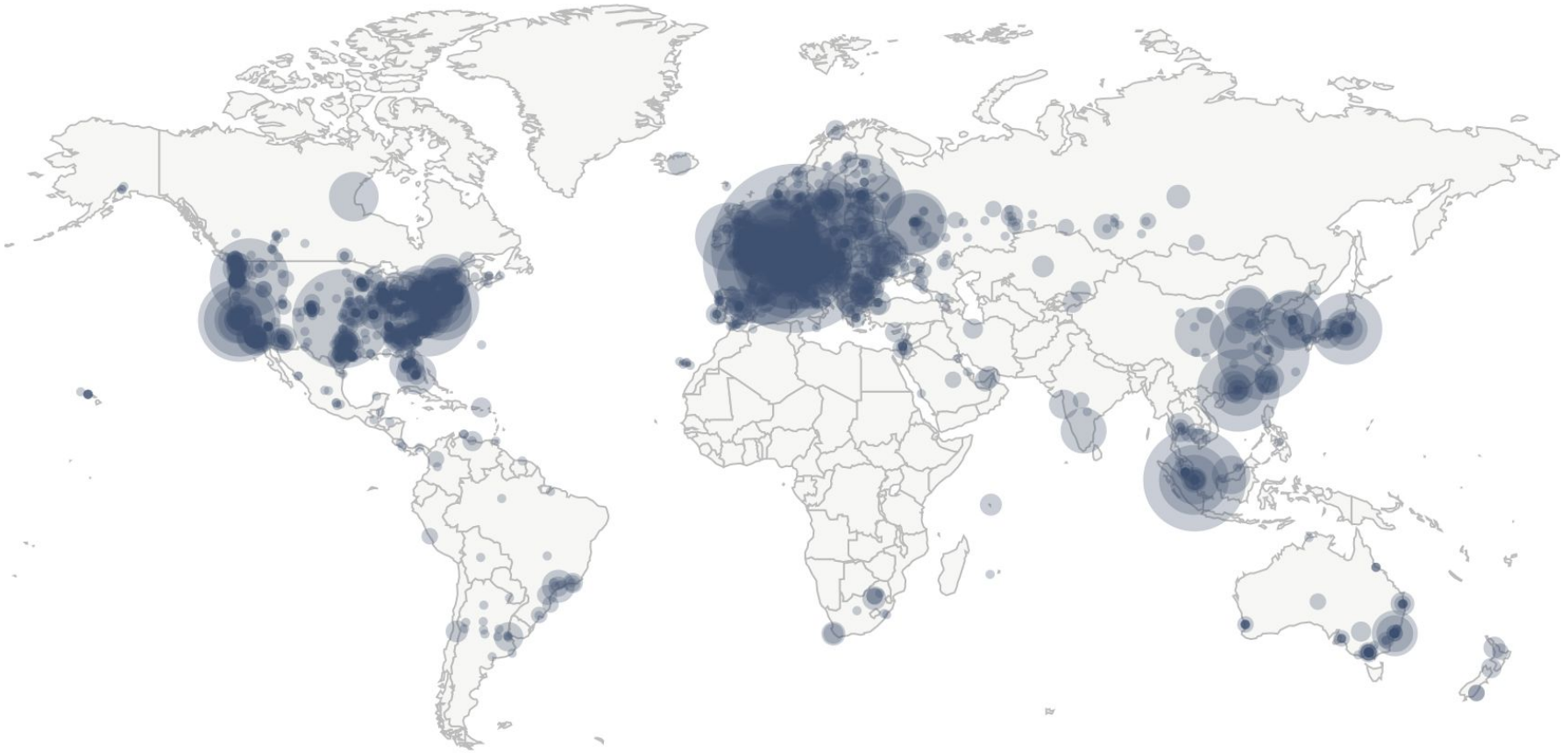
→ Ziel: Eine dezentralisierte und nicht-manipulierbare Datenbank



Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Aktive Nodes des Bitcoin-Netzwerkes (Schätzung)

9.435 Nodes (Stand 31.10.2019)

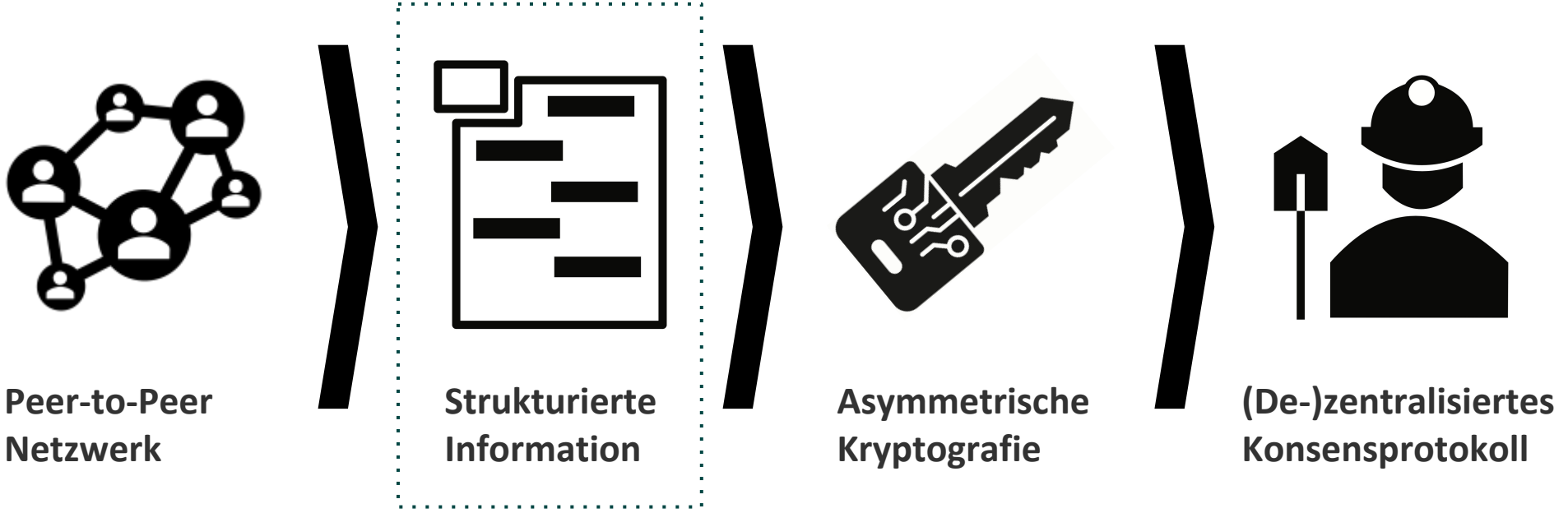


Quelle: https://bitnodes.earn.com/

Schlüsselkomponenten einer Blockchain

Kombination aus bestehenden Technologiekomponenten

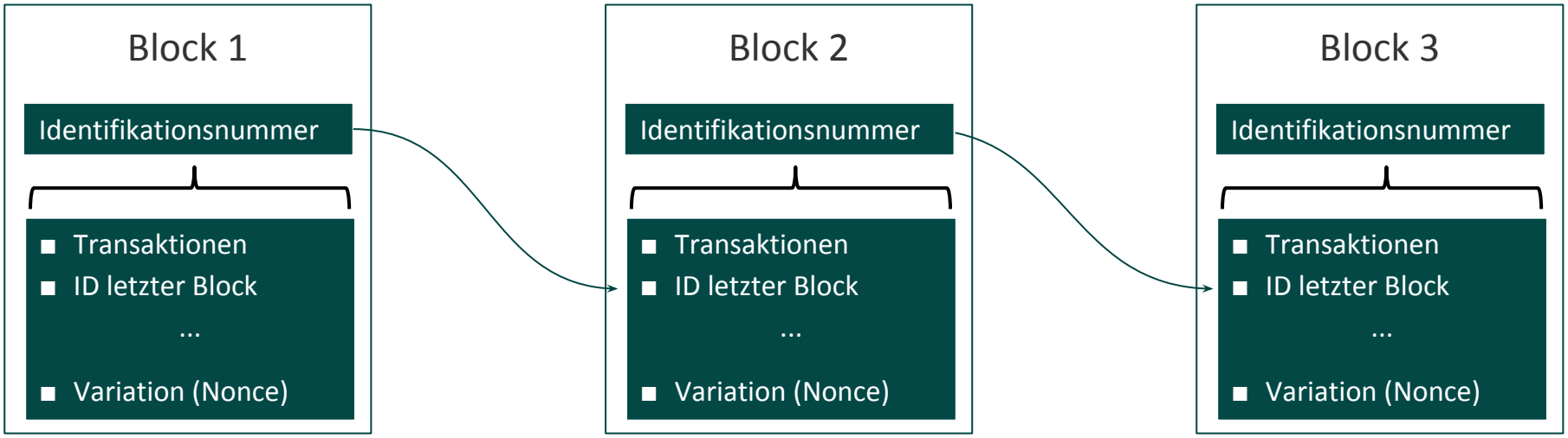
→ Ziel: Eine dezentralisierte und nicht-manipulierbare Datenbank



Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Beispiel einer Verkettung von Blocks

Vereinfachte Darstellung



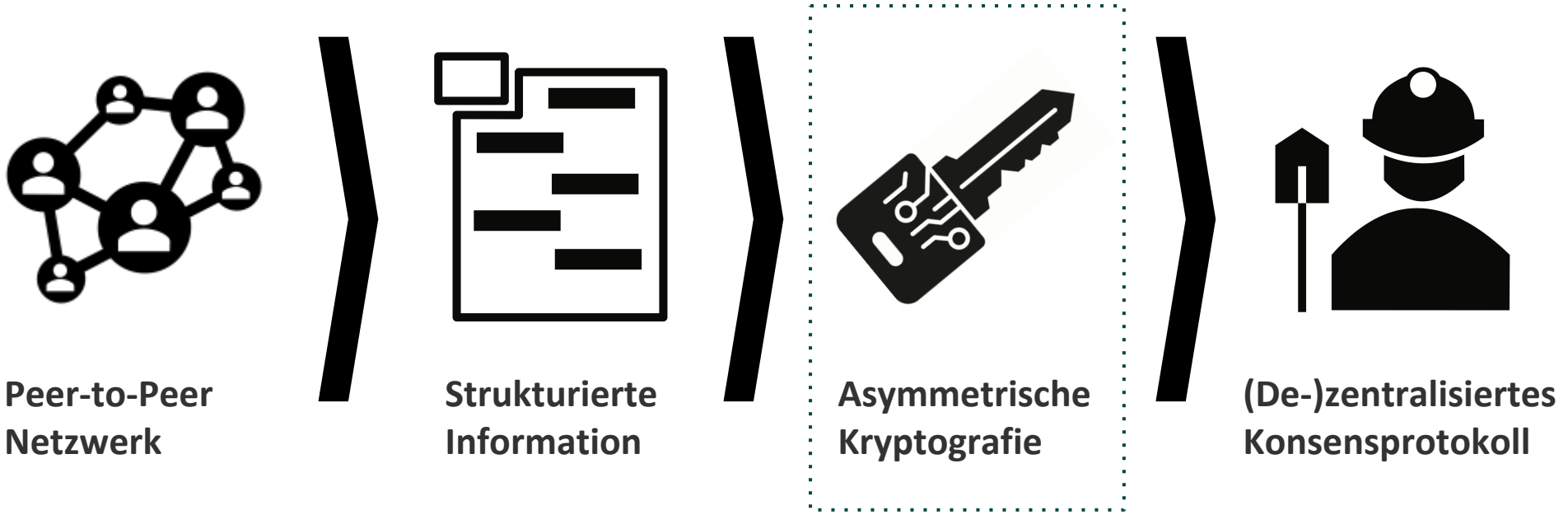
- Identifikationsnummer ist abhängig vom gesamten Inhalt des Blocks ⇒ Jede Änderung eines Blockbestandteils führt zu einer Änderung der Identifikationsnummer
- Wird der Inhalt eines vergangenen Blocks verändert, führt dies zu einer Inkonsistenz in der Kettenstruktur
- Konsensregel: Längste gültige Blockkette entspricht dem aktuellen Zustand

Quelle: Berentsen, Schär (2017): Bitcoin, Blockchain und Kryptoassets

Schlüsselkomponenten einer Blockchain

Kombination aus bestehenden Technologiekomponenten

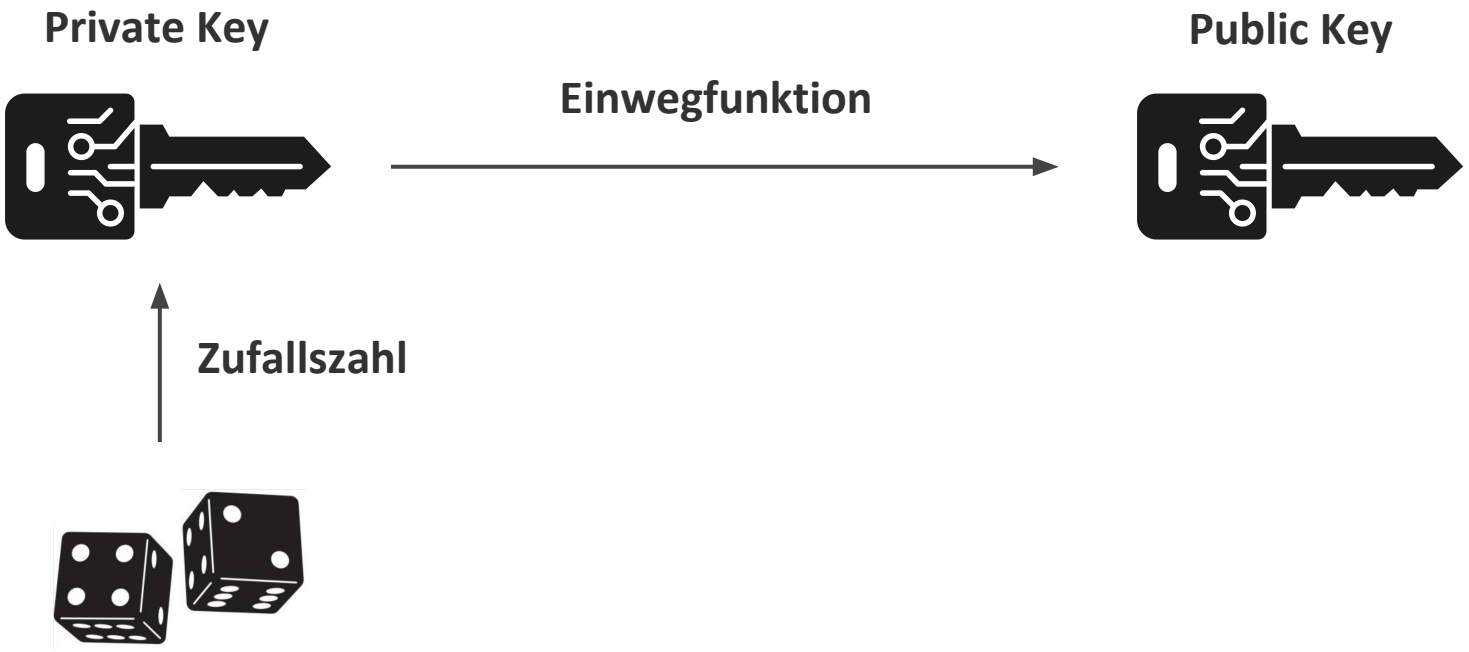
→ Ziel: Eine dezentralisierte und nicht-manipulierbare Datenbank



Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Asymmetrische Kryptografie

Ein Schlüsselpaar anstelle eines einzelnen Schlüssels



Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Die zwei Schlüssel-Prinzipien

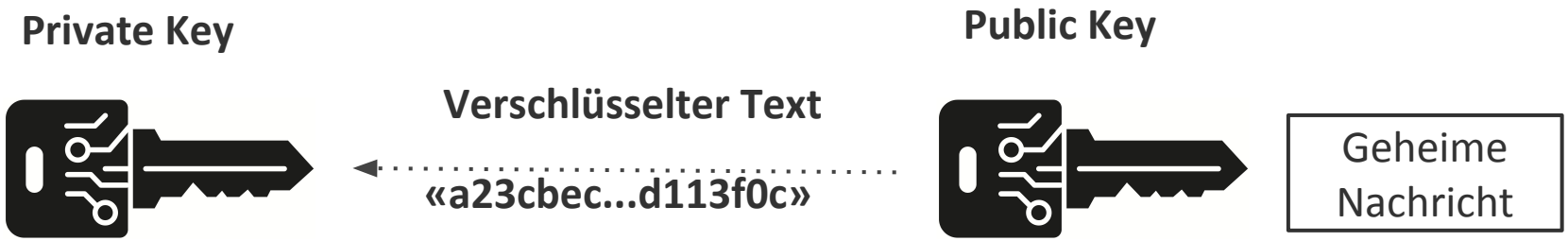
1. Der private Schlüssel muss zu jedem Zeitpunkt geheim gehalten werden.

2. Texte, die mit einem Schlüssel verschlüsselt werden, können ausschliesslich mit dem zugehörigen zweiten Schlüssel entschlüsselt werden.

Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icon: istockphoto.com

Anwendungsmöglichkeiten der asymmetrischen Kryptografie

Es gibt zwei Kategorien von Anwendungen
Geheimhaltung - Information verbergen:



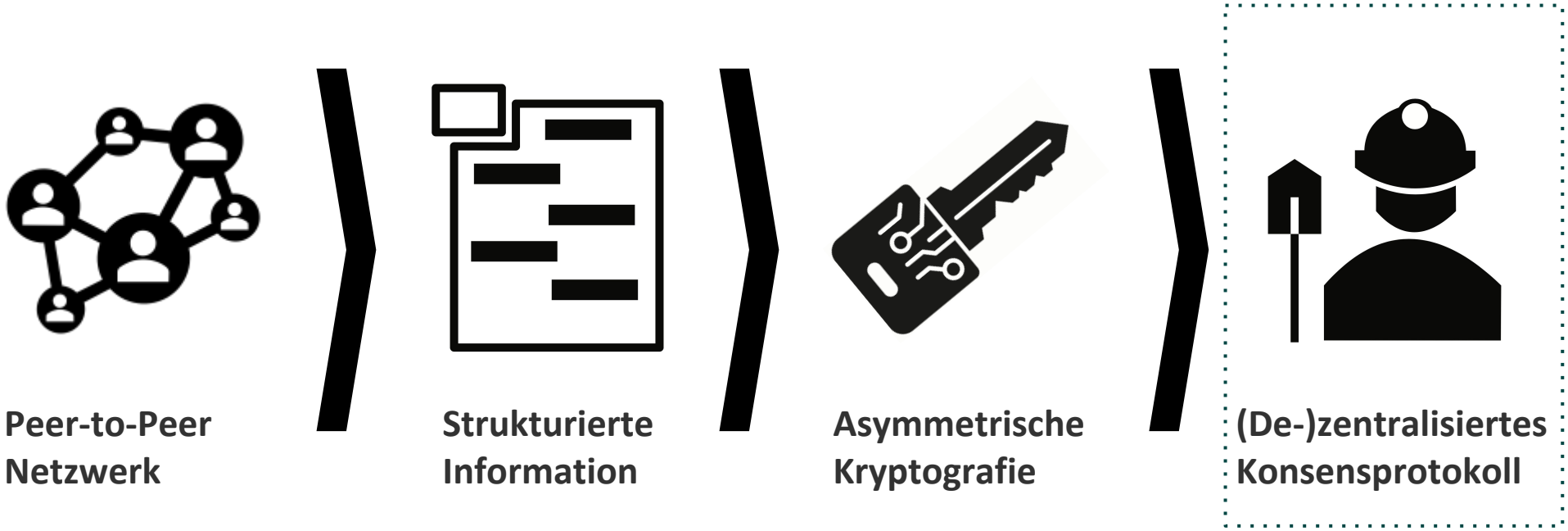
Authentizität und Integrität - Kryptografische Signaturen:

Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Schlüsselkomponenten einer Blockchain

Kombination aus bestehenden Technologiekomponenten

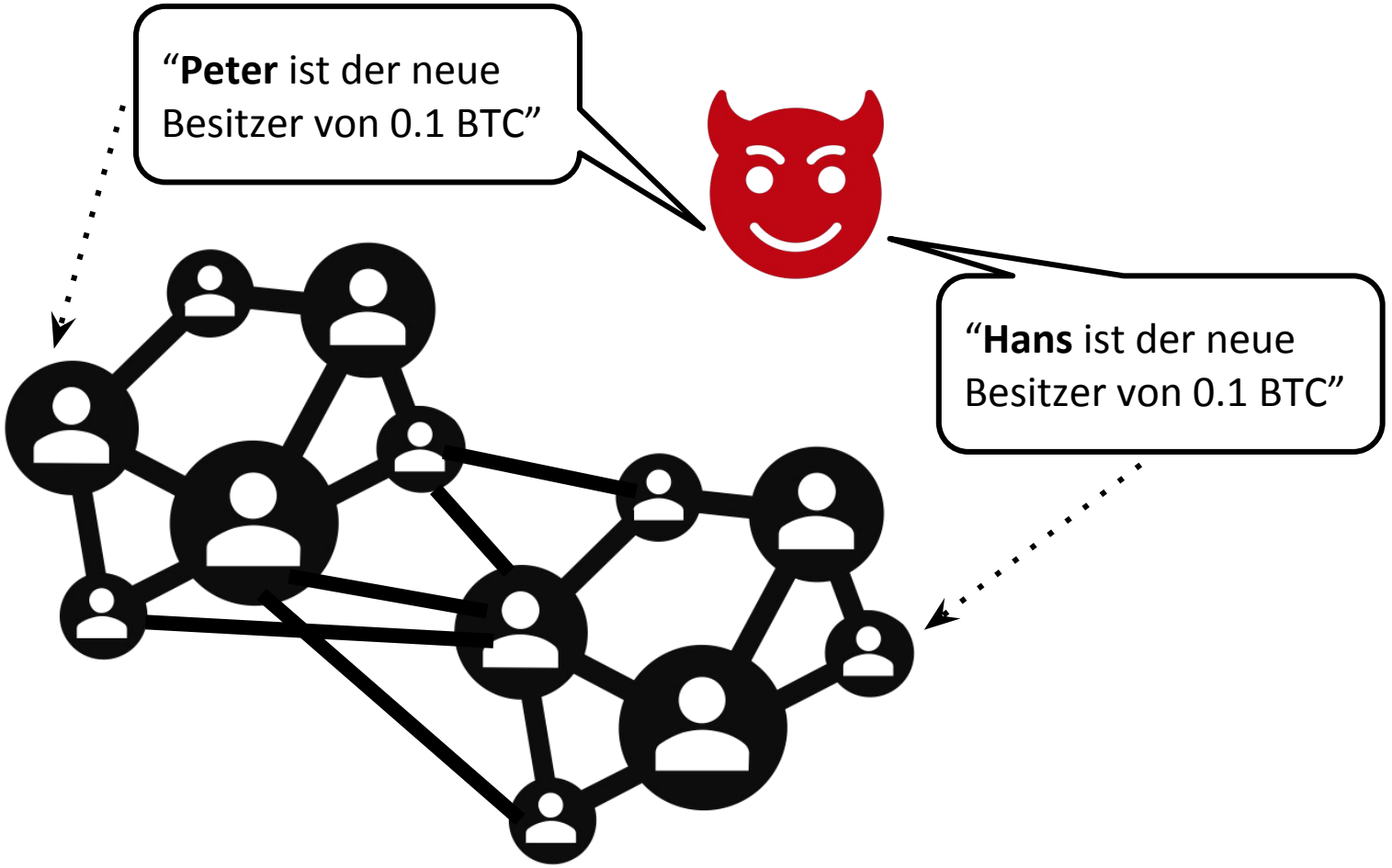
→ Ziel: Eine dezentralisierte und nicht-manipulierbare Datenbank



Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Schlüsselkomponenten einer Blockchain

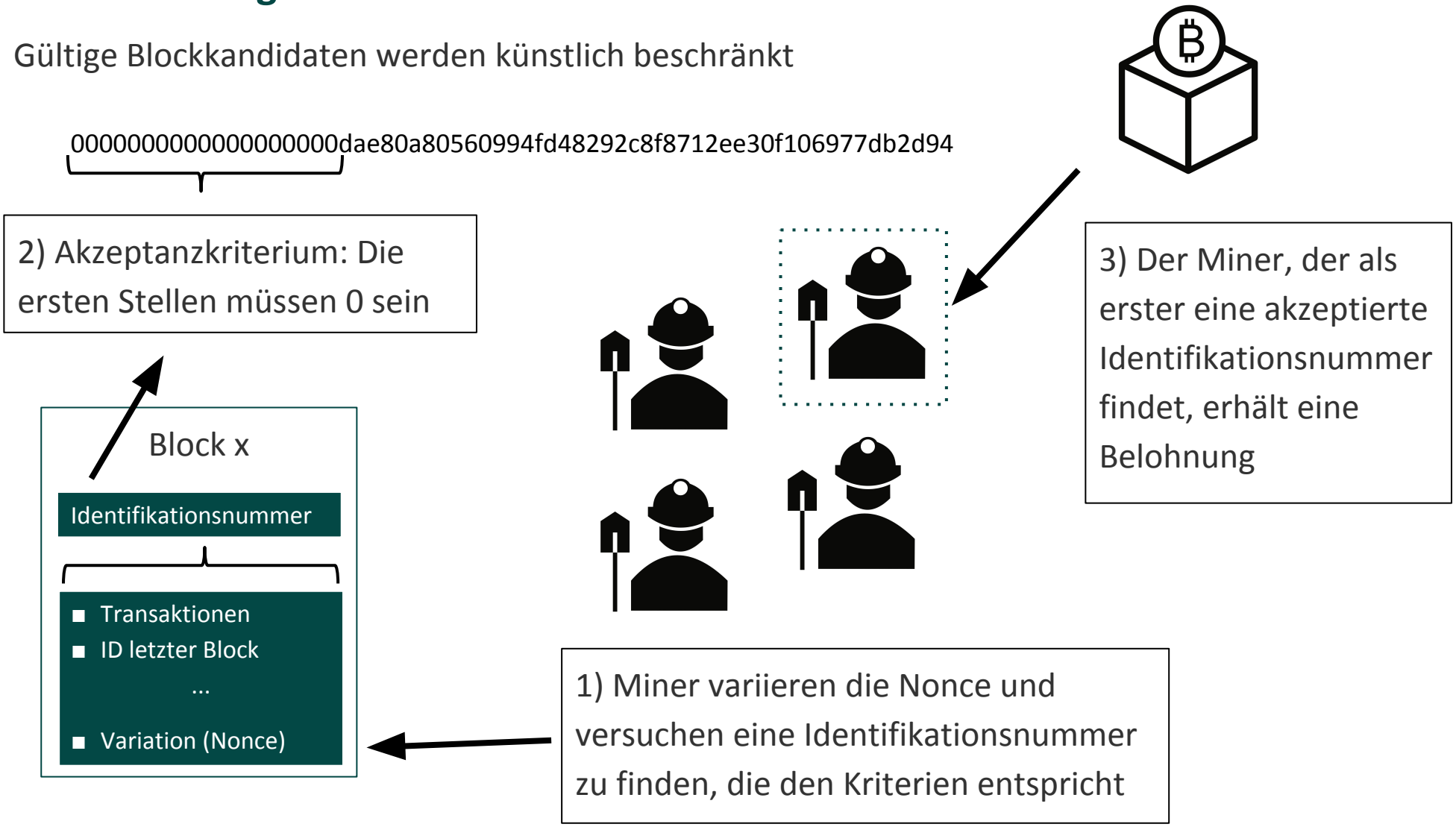
Ohne eine zentrale Instanz können Meinungsverschiedenheiten entstehen



Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Bitcoin Mining

Gültige Blockkandidaten werden künstlich beschränkt

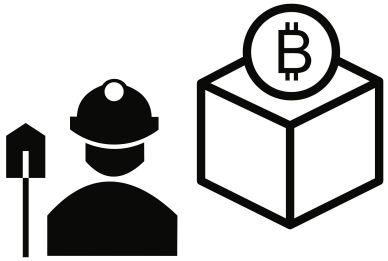


Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

Die verschiedenen Konsensprotokolle

Trade-Off zwischen Kosten

Dezentralisiert



Zentralisiert

Vertrauenskosten:

- Monopolrente
- Enteignung
- Single Point of Failure

Konsenskosten:

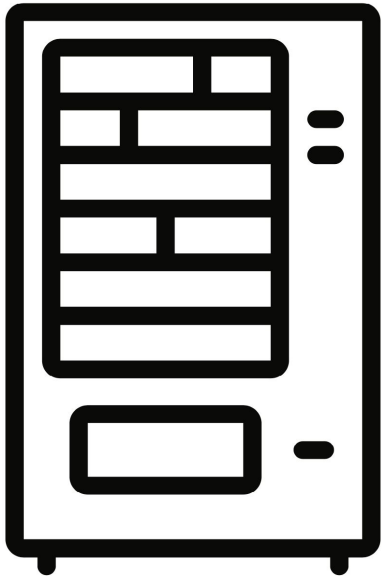
- Teures Konsensprotokoll
- Chaotische Governance

Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icons: istockphoto.com

2 Smart Contracts

Smart Contracts

Beispiel - Der Getränkeautomat



Simpler Getränkeautomat (Pseudo Code):

```
if(coin >= price) {
        dispenseBeverage();
        returnChange(coin - price);
}else{
        print("Guthaben zu klein");
}
```

⇒ Automatisierte Ausführung macht Vertragsbruch aufwändig.

Aber:

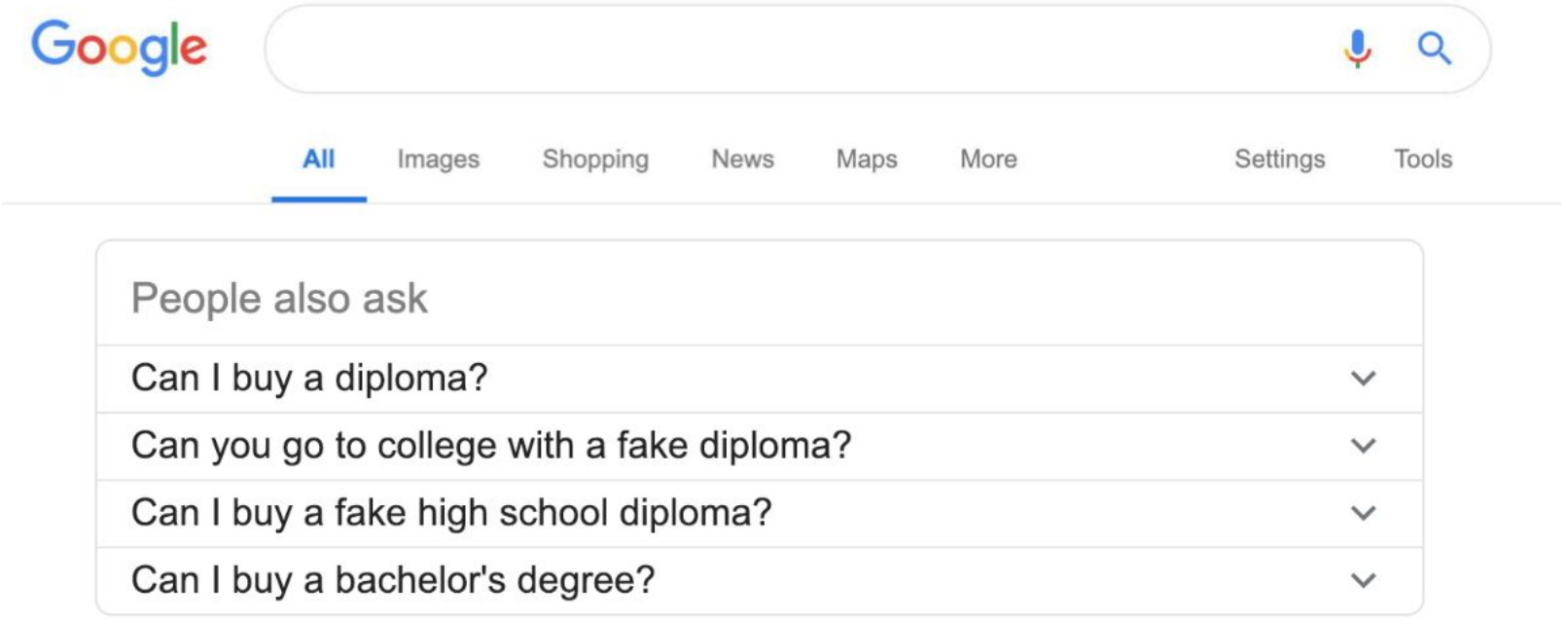
- Vertrauensbasiert, da closed source → Der Vertrag ist nicht beobachtbar
- Ausführungsumfeld: z.B. Hardware ist unter der Kontrolle des Verkäufers.

Quelle: Prof. Dr. Fabian Schär, Universität Basel; Icon: istockphoto.com

3 Anwendungsbeispiel

Gefälschte Diplome

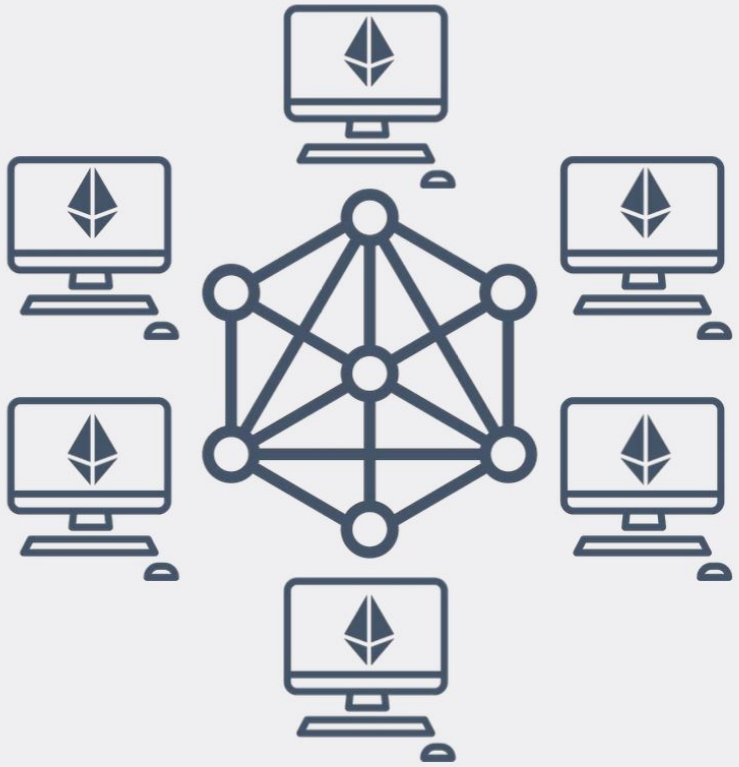
Ja das ist tatsächlich ein aktuelles Problem



Quelle: Prof. Dr. Fabian Schär, Universität Basel

Gefälschte Diplome

Öffentliche Blockchains können als Notarservice verwendet werden

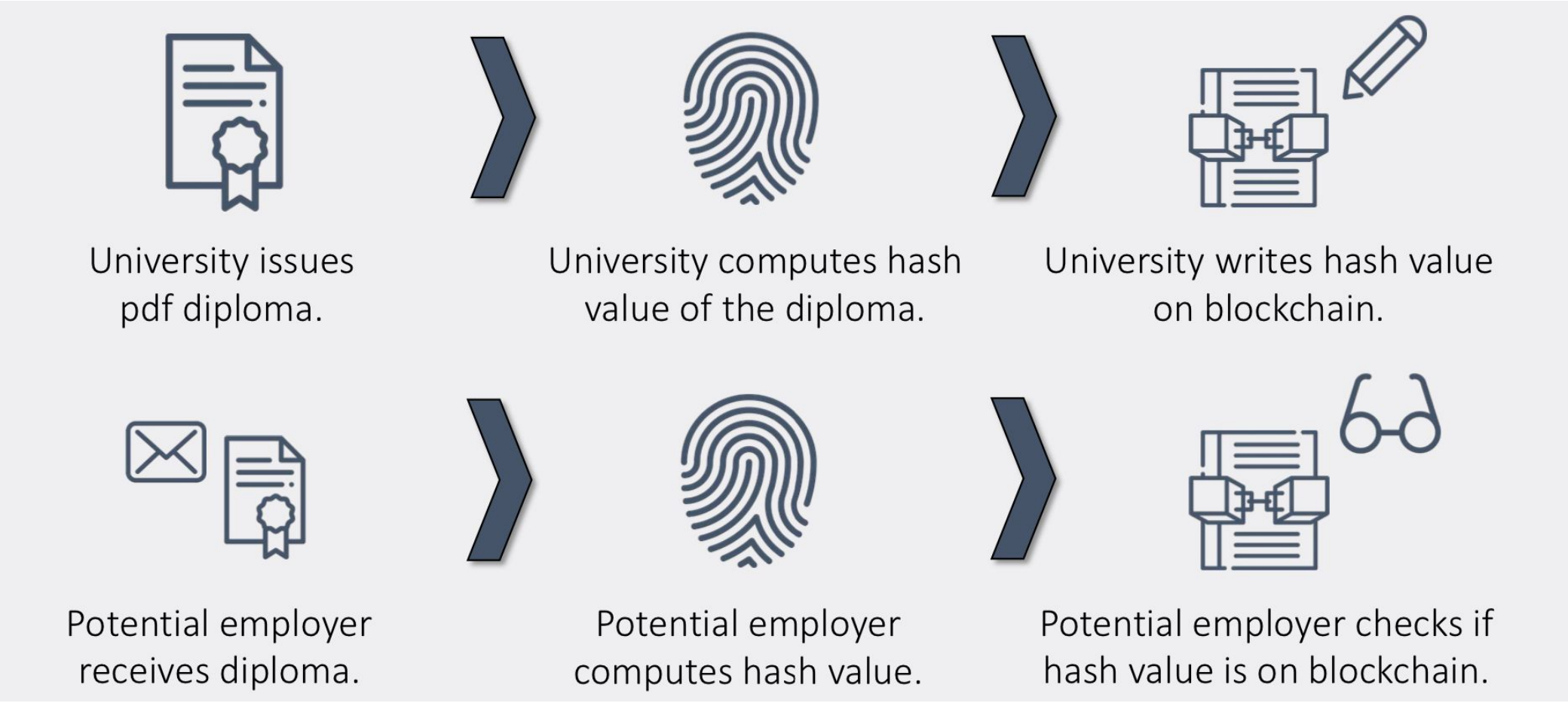


Information can be secured on a public Blockchain.

Quelle: Prof. Dr. Fabian Schär, Universität Basel

Gefälschte Diplome

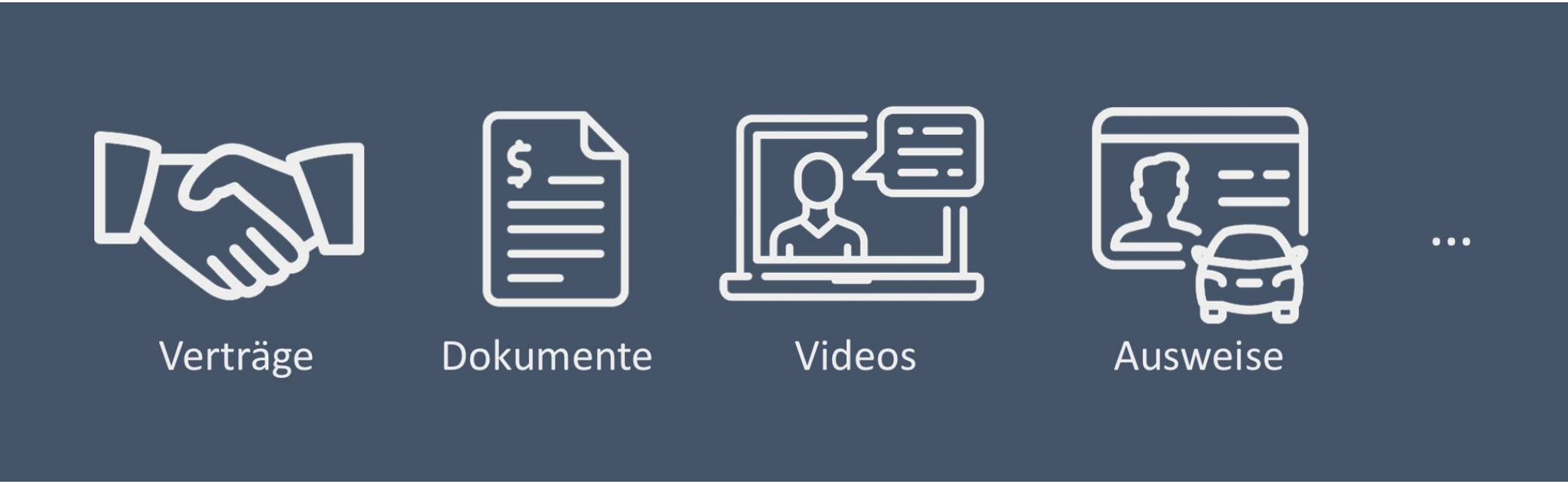
Prozess der Ausgabe und Überprüfung der Echtheit



Quelle: Prof. Dr. Fabian Schär, Universität Basel

Weitere Use Cases

Das gleiche Prinzip kann für jede Art von Dokument angewendet werden

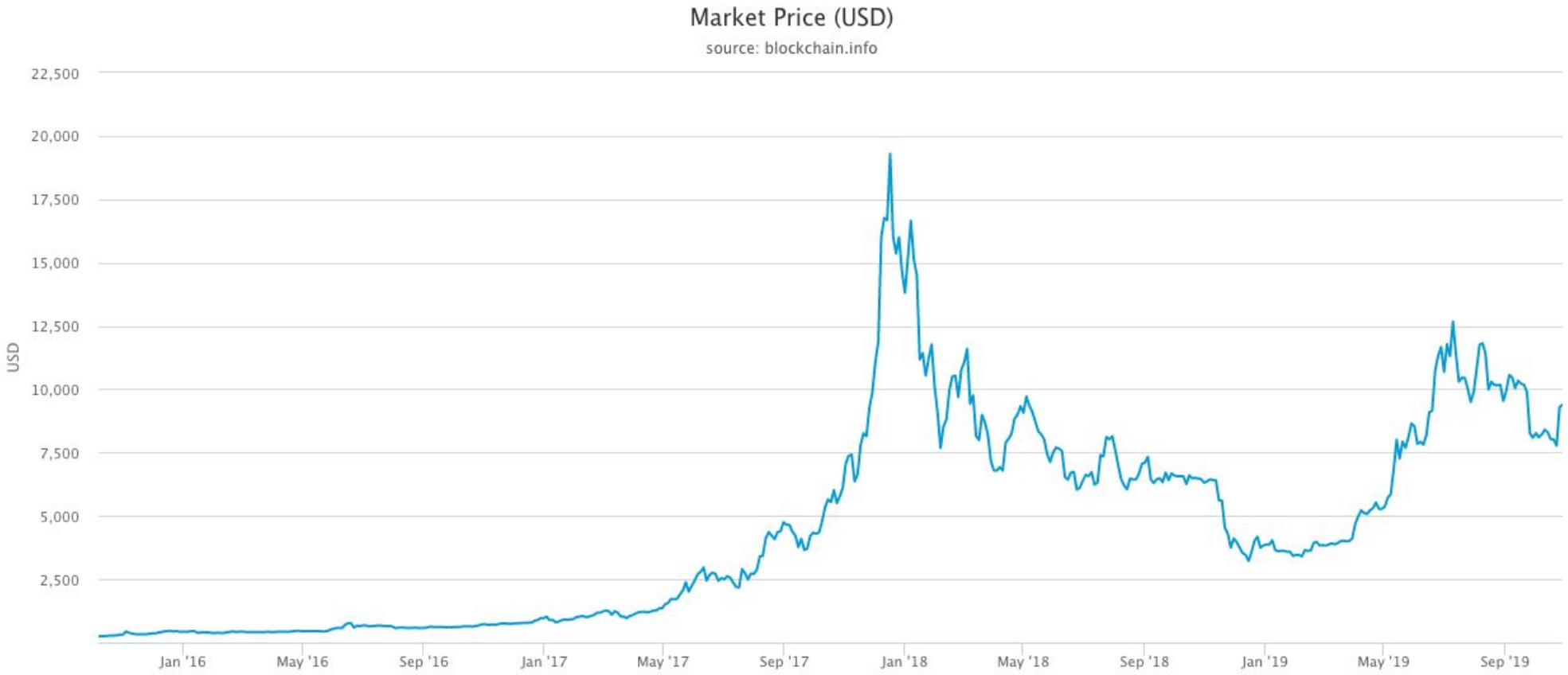


Quelle: Prof. Dr. Fabian Schär, Universität Basel

4

Aktuelle Zahlen

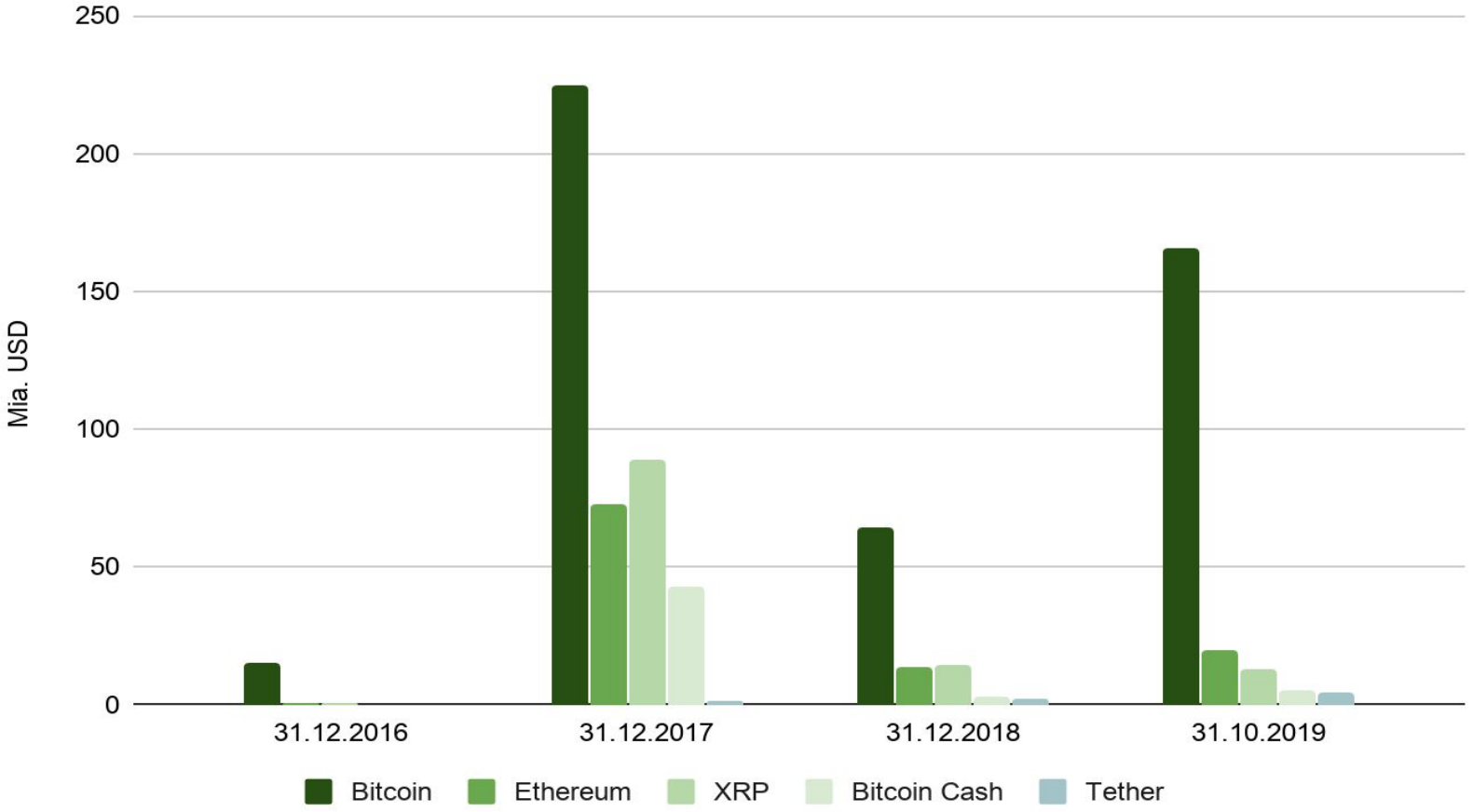
Bitcoin-Preis



Quelle: blockchain.info

Marktkapitalisierung der Top 5 Kryptowährungen

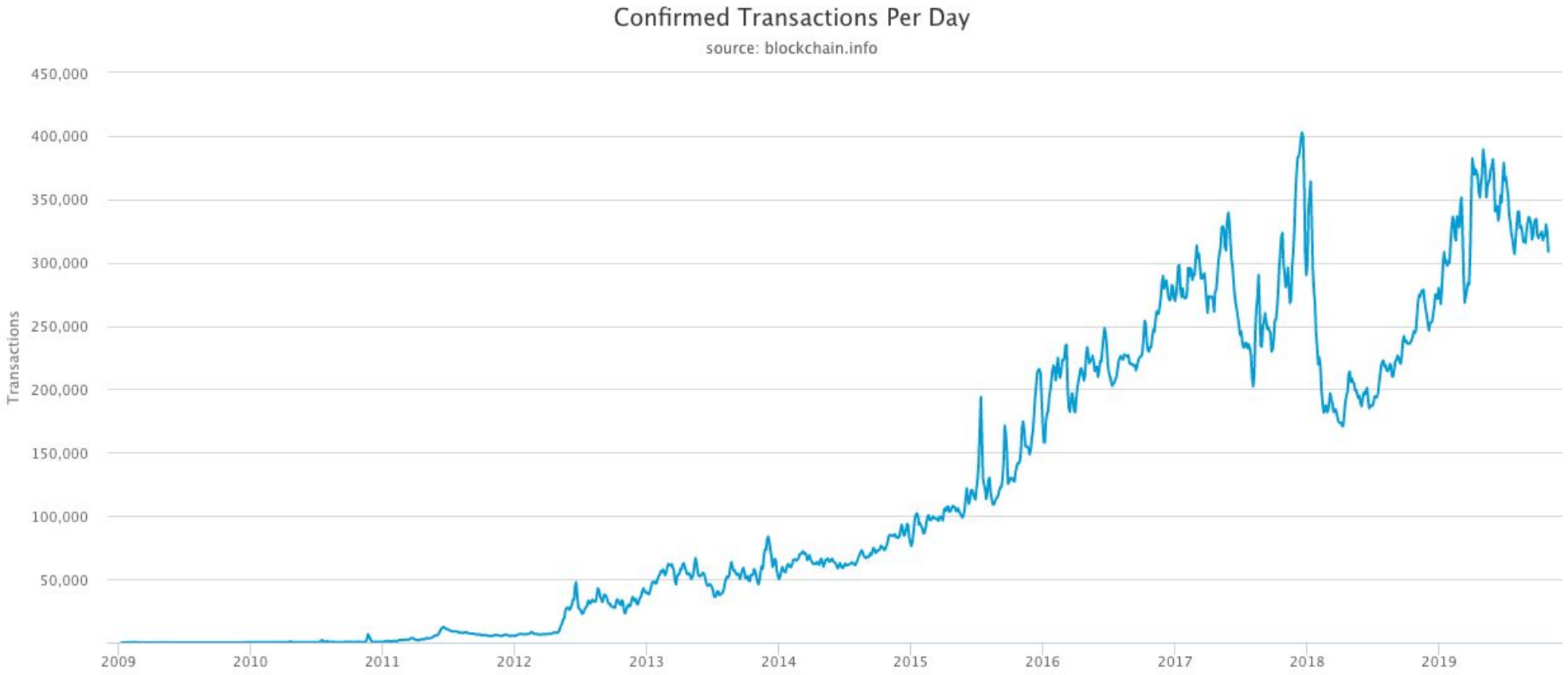
Bitcoin liegt weiterhin klar in Führung



Eigene Darstellung mit Daten von: https://coinlib.io/

Anzahl Bitcoin-Transaktionen

Transaktionen pro Tag



Quelle: blockchain.info

Die Blockchain ist eine öffentliche Datenbank, die eine Vielzahl an Anwendungen ermöglicht!

Besuchen Sie uns im Anschluss am Stand 55!

Tobias Bitterli
Chief Product Officer & Co-Founder

tobias.bitterli@greenmatch.ch
+41 (0) 61 301 50 00

green[::]match

@greenmatch
greenmatch-ag
www.greenmatch.ch