BLOCKCHAIN
Bayern e.V.

Wir bringen Blockchain in Bayern voran.

Einführung in die Blockchain

Maximilian Irlbeck

Prof. Dr. Florian Matthes

Blockchain Bayern e.V.

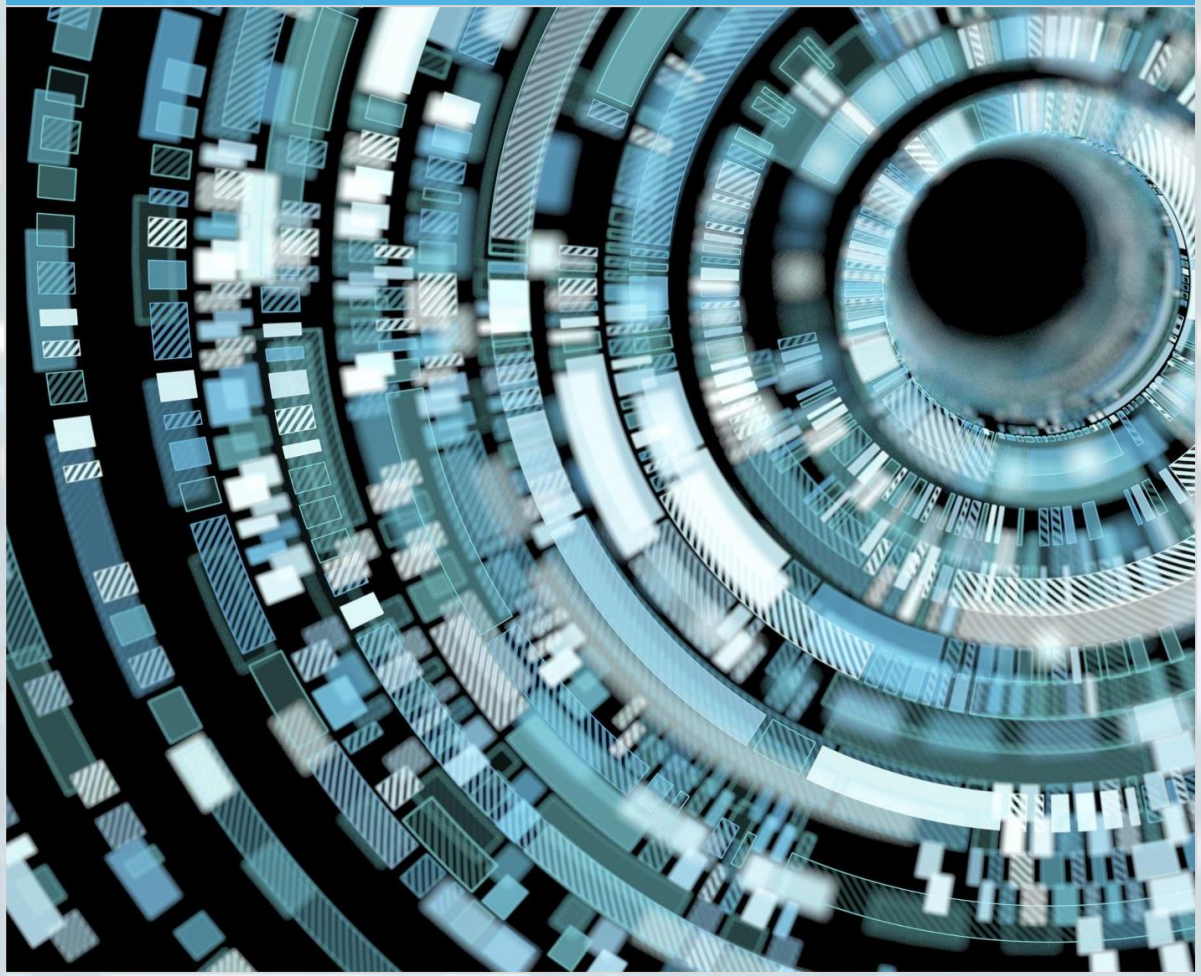
Blockchain für den Mittelstand, 04.05.2021

www.blockchain-bayern.de

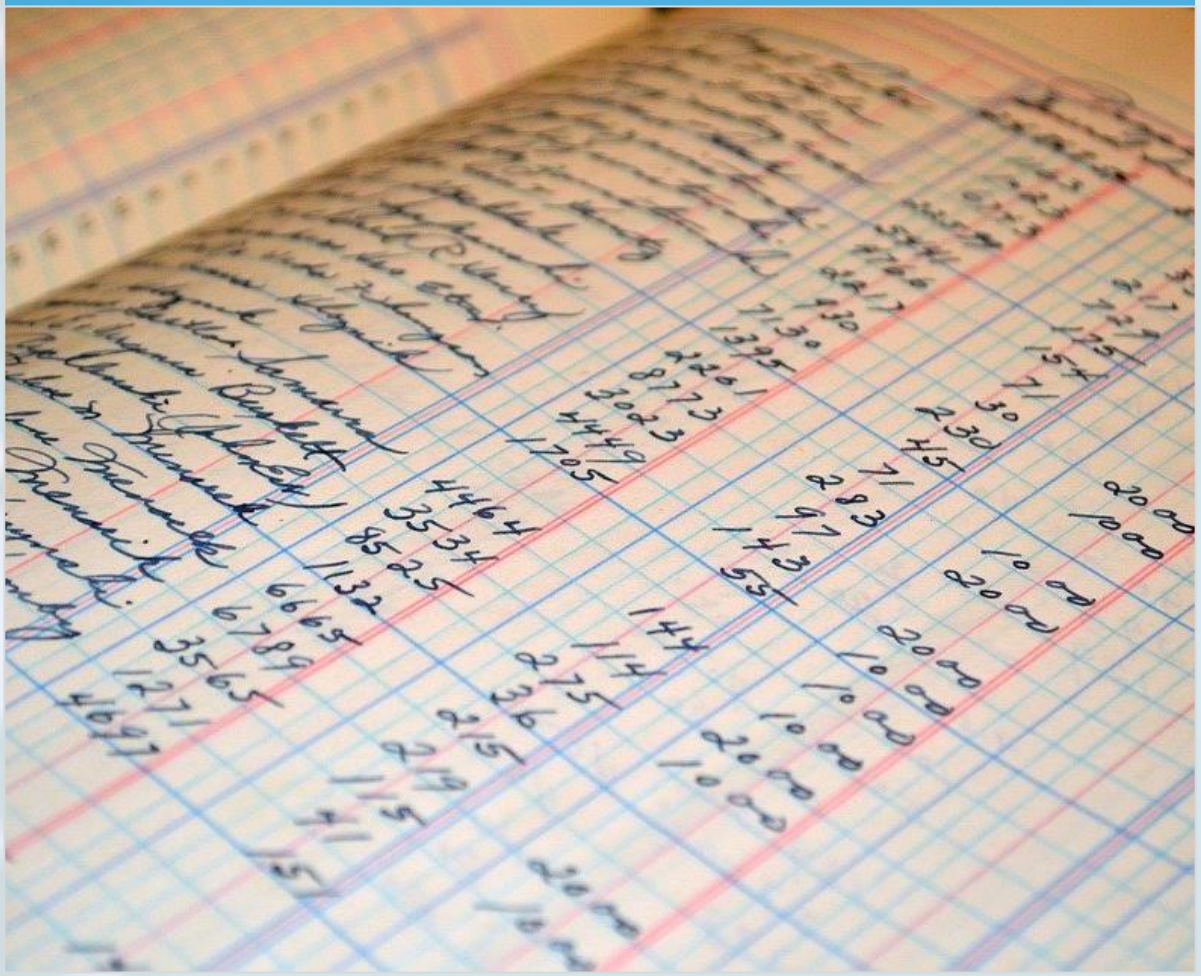
Was ist eine „Blockchain“?

BLOCKCHAIN Bayern e.V.

Eine dezentrale Datenbank



Ein dezentrales Register / Kassenbuch



Konzept eines zentralen Registers / Kassenbuchs

Transaktionen

Benutzer:in
(z.B. Bankkunde)

Register
(z.B. Bankkontenverwaltung)

Registerbetrieb
(z.B. Bank)

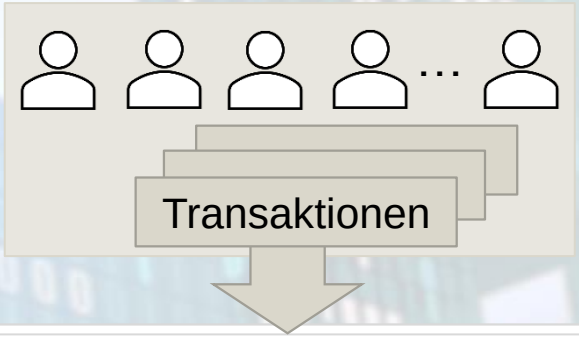
Synonyme:
- Intermediär
- Registerführende Stelle

Vertrauen
(z.B. durch Schufa, BaFin, Ausweis, etc.)

Währungseinheit
Euro

Beispiel für ein zentrales Register: Bank

Benutzer:innen (z.B. Bankkund:innen)



Register

Abheben | Einzahlen | … | Überweisung

- Prüfung des Kontostands
- Prüfung der Kontodaten
- Prüfung der Berechtigung

Datenbank mit Einzeleinträgen oder Sammeleinträgen

- Daten der Bankkunden
- Kontodaten
- Protokolldaten, …

Registerbetrieb

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Dauerhafte Speicherung
- Angemessene Ausführungszeit
- Register-Änderungen in Reihenfolge des Eingangs

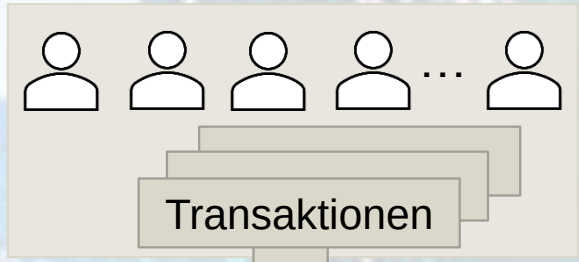
Vertrauen

Währungseinheit
Euro

Allgemeines Schema: Zentrales Register

BLOCKCHAIN Bayern e.V.

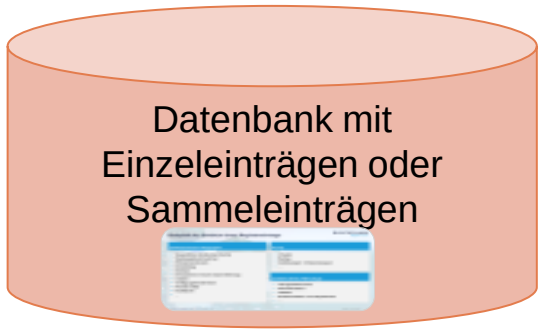
Benutzer:innen



Register

Operation 1 | Operation 2 | … | Operation X

- Prozesse und Programme zur Berechtigungsprüfung
- Durchsetzung der Registerregeln



- Daten der Nutzer
- Protokolldaten, …

Registerbetrieb

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Dauerhafte Speicherung
- Angemessene Ausführungszeit
- Register-Änderungen in Reihenfolge des Eingangs

Vertrauen

Währungseinheit
Euro

Beispiele für Struktur eines Registereintrags

BLOCKCHAIN Bayern e.V.

Elektronisches Wertpapier

- Wesentliche Inhalte des Rechts
- Wertpapierkennnummer
- Emissionsvolumen
- Nennbetrag
- Emittent
- Kennzeichen: Einzel-/Sammeleintrag
- Inhaber
- Verfügungshindernisse
- Rechte Dritter
- Kaufdatum
- …

Konto

- Inhaber
- Betrag
- Abhebungen / Überweisungen
- …

Zustand eines Fahrzeugs

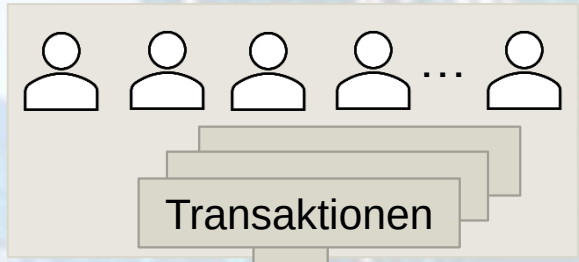
- Fahrgestellnummer
- Kilometerstand
- Inhaber
- Dokumentation von Reparaturen
- …

Allgemeines Schema: Zentrales Register

BLOCKCHAIN Bayern e.V.

Wie machen wir das Register dezentral?

Benutzer:innen



Register

Operation 1 | Operation 2 | … | Operation X

- Prozesse und Programme zur Berechtigungsprüfung
- Durchsetzung der Registerregeln

Datenbank mit Einzeleinträgen oder Sammeleinträgen

- Daten der Nutzer
- Protokolldaten, …

Registerbetrieb

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Dauerhafte Speicherung
- Angemessene Ausführungszeit
- Register-Änderungen in Reihenfolge des Eingangs

Vertrauen

Währungseinheit **Euro**

Wiederholung:
Konzept eines zentralen Registers / Kassenbuchs

BLOCKCHAIN Bayern e.V.

Transaktionen

Benutzer:in
(z.B. Bankkunde)

Register
(z.B. Bankkontenverwaltung)

Registerbetrieb
(z.B. Bank)

Vertrauen
(z.B. durch Schufa, BaFin, Ausweis, etc.)

Währungseinheit
Euro

Aufgabe:
Transformation in ein dezentrales
Blockchain Netzwerk

Rollen in Blockchain Netzwerken

Benutzer:in

Wallet Owner

- Hat Zugang für ein Blockchain Konto mit Geldbörse (**Wallet**)
- Zugriff auf zugeordnete Einheiten (**Tokens**)
- Tätigt **Transaktionen** mit Tokens

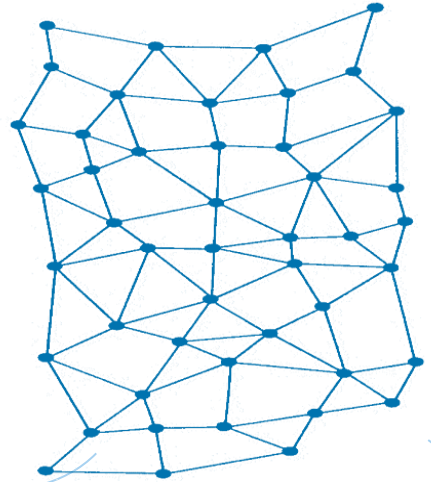
Währungseinheit

(Currency) Tokens

- z.B. Bitcoin, Ether
- Für Transaktionen

Transaktionen

Blockchain Netzwerk



- Full Nodes
- Miner

Register

Full Node

- **Verwaltet** und **speichert** die komplette Blockchain
- **Validiert** jede **Transaktion** und jeden Block
- Leitet alle neuen, validen **Transaktionen** an Miner weiter

Registerbetrieb

Miner

- Verhält sich wie Full Node
- **Erzeugt** aus mehreren Transaktionen einen **Block**
- Versucht, das **Mining-Puzzle** für Blöcke zu lösen
- Erhält **Belohnungen** (in **Tokens**) für neue **Blöcke** der Blockchain

Konzept einer Blockchain

BLOCKCHAIN Bayern e.V.

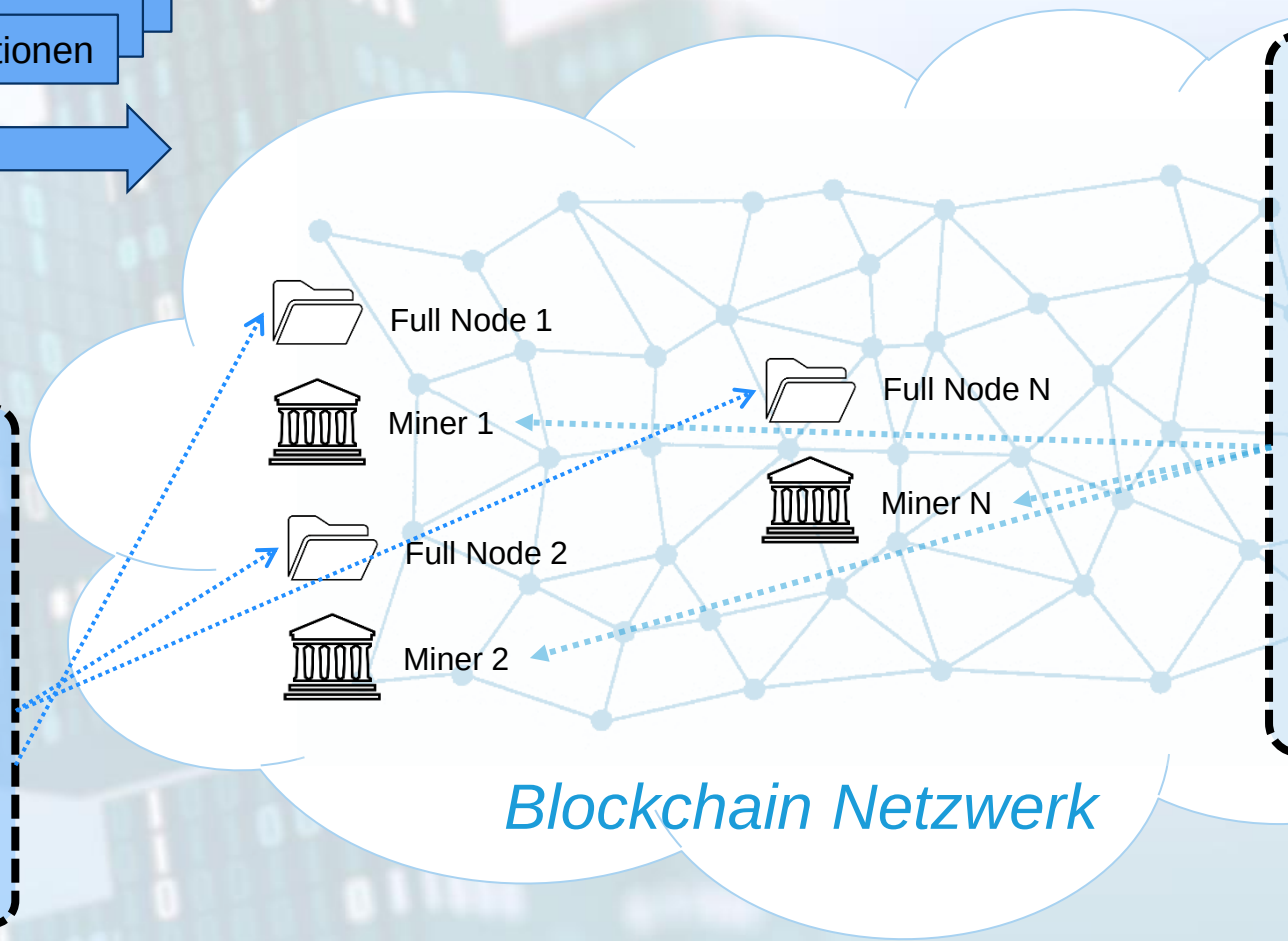
Vertrauen durch kryptographische Prüfung

Transaktionen

Wallet Owner

Full Nodes

- Dezentrales fälschungssicheres Aufzeichnungssystem
- Dezentrale Datenstruktur
- Vordefinierte Muster für Kontrollrechte



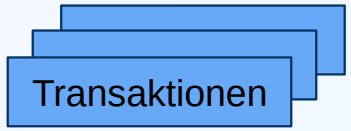
Miner

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Dauerhafte Speicherung
- Angemessene Ausführungszeit
- Register-Änderungen in Reihenfolge des Eingangs

Vertrauen durch kryptographische Prüfung

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.



Wallet Owner

- Hat Zugang für ein Blockchain Konto mit Geldbörse (**Wallet**)
- Besitzt die zugeordneten Einheiten (**Tokens**)
- Tätigt **Transaktionen** mit Tokens

Full Node

- **Verwaltet** und **speichert** die komplette Blockchain
- **Validiert** jede **Transaktion** und jeden Block
- Leitet alle neuen, validen **Transaktionen** an Miner weiter

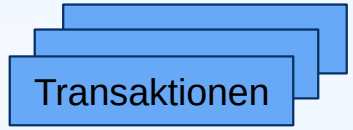
Miner

- Verhält sich wie Full Node
- **Erzeugt** aus mehreren Transaktionen einen **Block**
- Versucht, das **Mining-Puzzle** für Blöcke zu lösen
- Erhält **Belohnungen** (in **Tokens**) für neue **Blöcke** der Blockchain

Blockchain „eine Kette von Blöcken“

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.



Transaktion X
Kontonummer
Transaktionsdaten
Datum etc.
Signatur

senden

Blockchain „eine Kette von Blöcken“

Wie funktionieren Transaktionen bei einer Blockchain?

Transaktion X
Kontonummer ✓
Transaktionsdaten ✓
Datum etc. ✓
Signatur ✓

Überprüfen mit Blockchain

senden

Blockchain

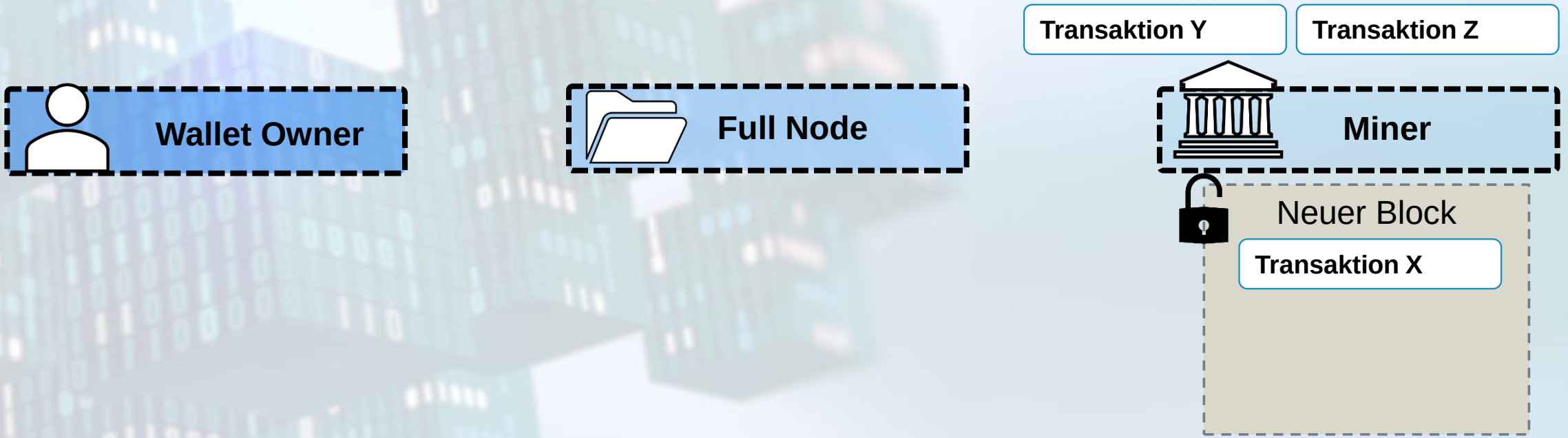
Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.

Transaktion X
Kontonummer ✓
Transaktionsdaten ✓
Datum etc. ✓
Signatur ✓

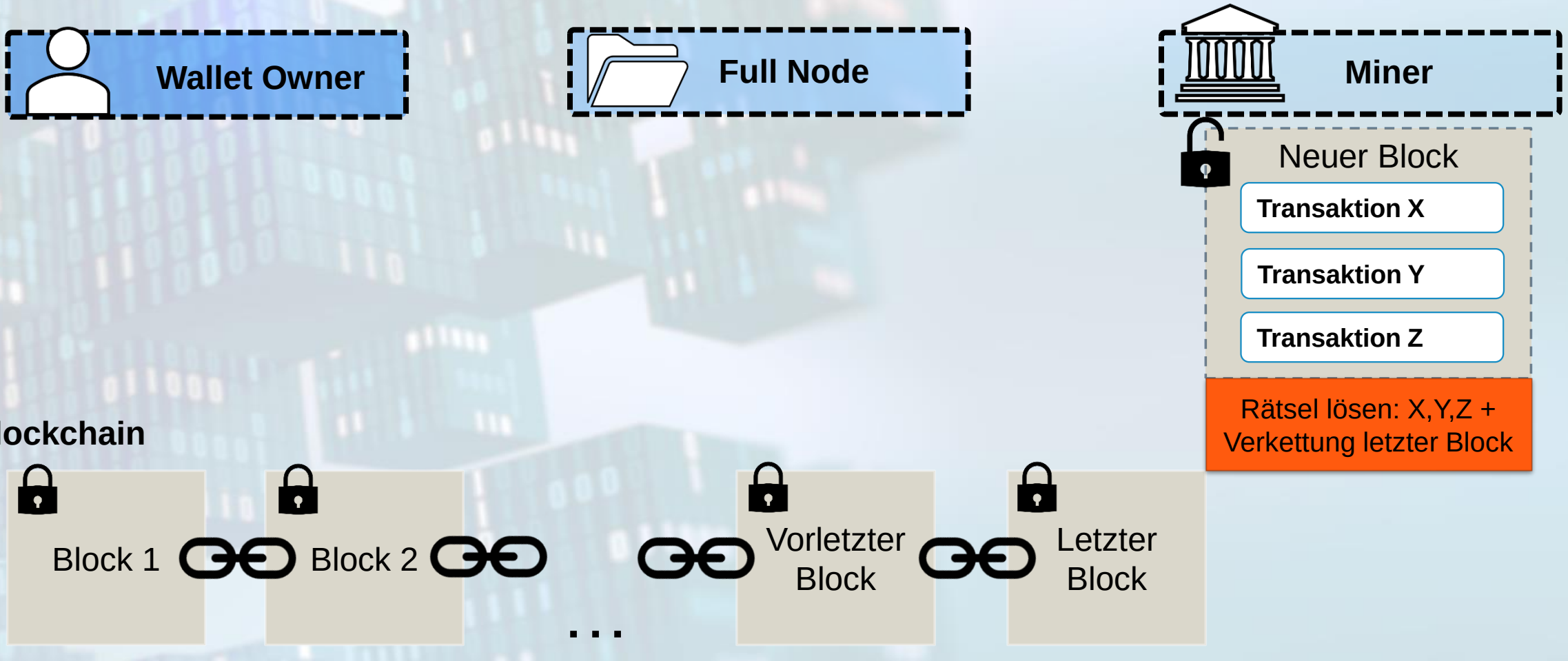
Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?

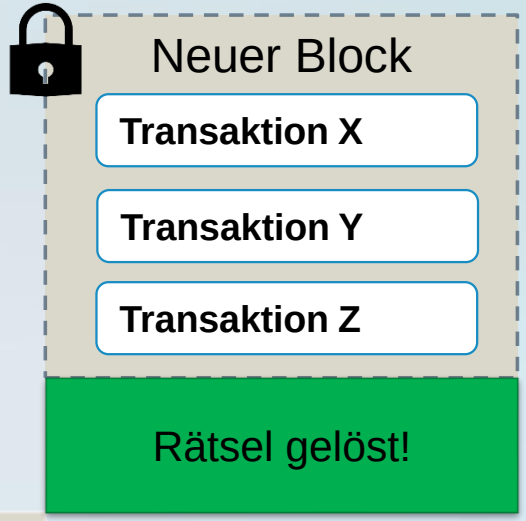


Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?



Wie funktionieren Transaktionen bei einer Blockchain?



Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.

Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.

Wallet Owner

Full Node

Miner

Überprüfen
des neuen Blocks
und Zusammenhang
aller Blöcke

Blockchain

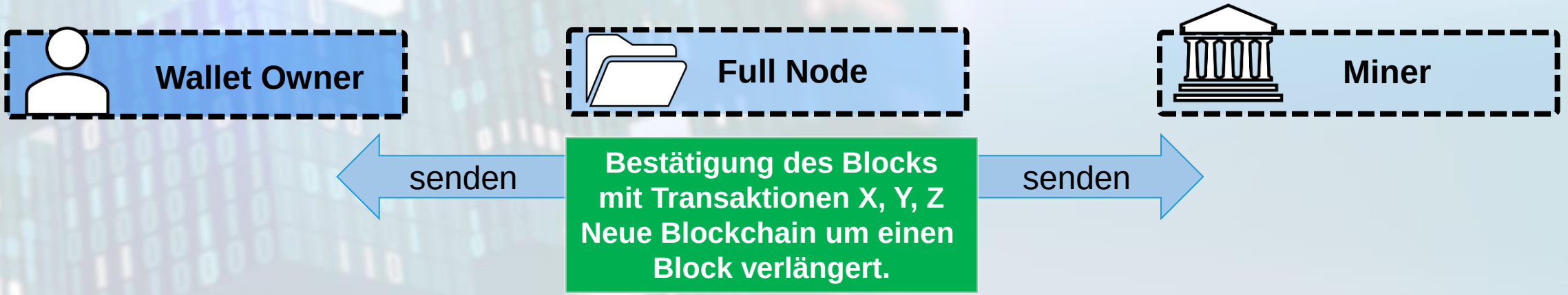
Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.

Bestätigung des Blocks mit Transaktionen X, Y, Z Neue Blockchain um einen Block verlängert.

Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?



Blockchain

Wie funktionieren Transaktionen bei einer Blockchain?

BLOCKCHAIN Bayern e.V.

Konsens!

Wallet Owner

Transaktion umgesetzt

Full Node

Neue Version der Blockchain mit einem Block mehr

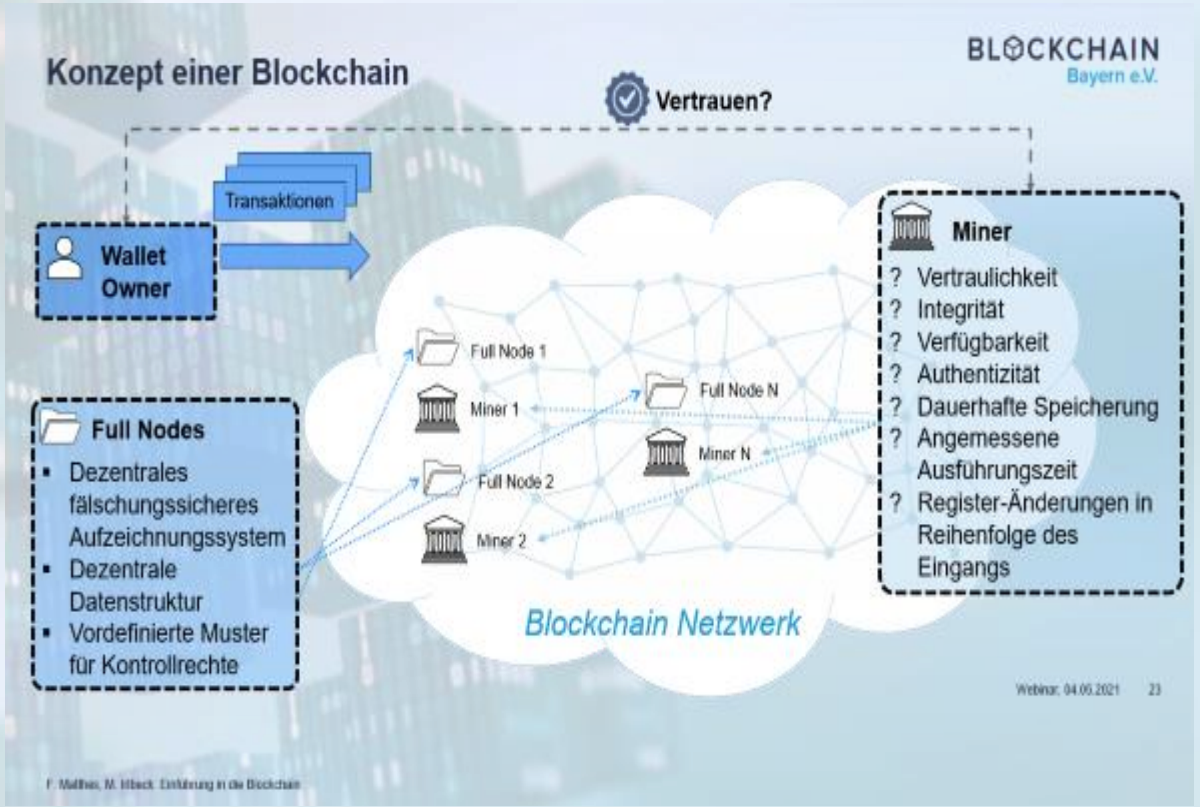
Miner

Erhält Belohnung auf sein Konto in Tokens

Blockchain

Tiefergehende Fragen – Mehr im nächsten Webinar

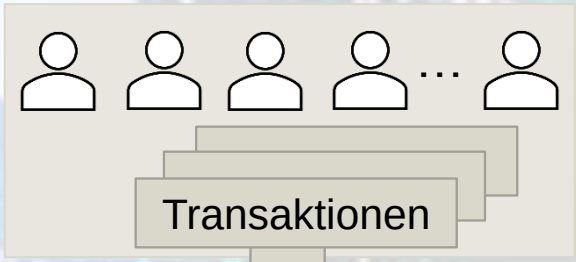
- Wie werden **Identitäten** festgestellt?
- Wie wird sichergestellt, dass die **Full Nodes** und **Miner** den **gleichen Datenstand** haben?
- Wie kann man **mehrfache Transaktionen** mit dem gleichen Geld im Netzwerk verhindern? (Double Spending Problem)
- Welche **kryptographischen Verfahren** werden eingesetzt?
- Was sind **Konsens Algorithmen**?



Smart Contracts: Programmierbare Blockchains

BLOCKCHAIN Bayern e.V.

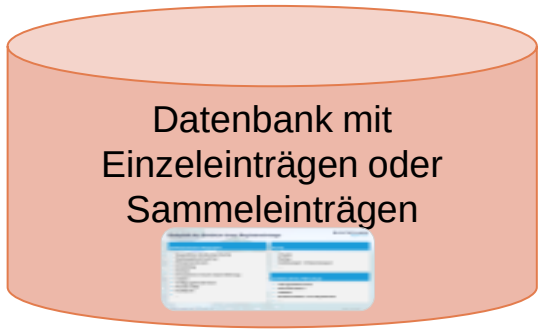
Wallet Owner



Blockchain

Operation 1 | Operation 2 | … | Operation X

- **Frei programmierbare** Operationen
- **Frei definierbare** Registerregeln



- Daten der Nutzer
- Protokolldaten
- **Code**
- **Frei programmierbare Datenstrukturen**
- …

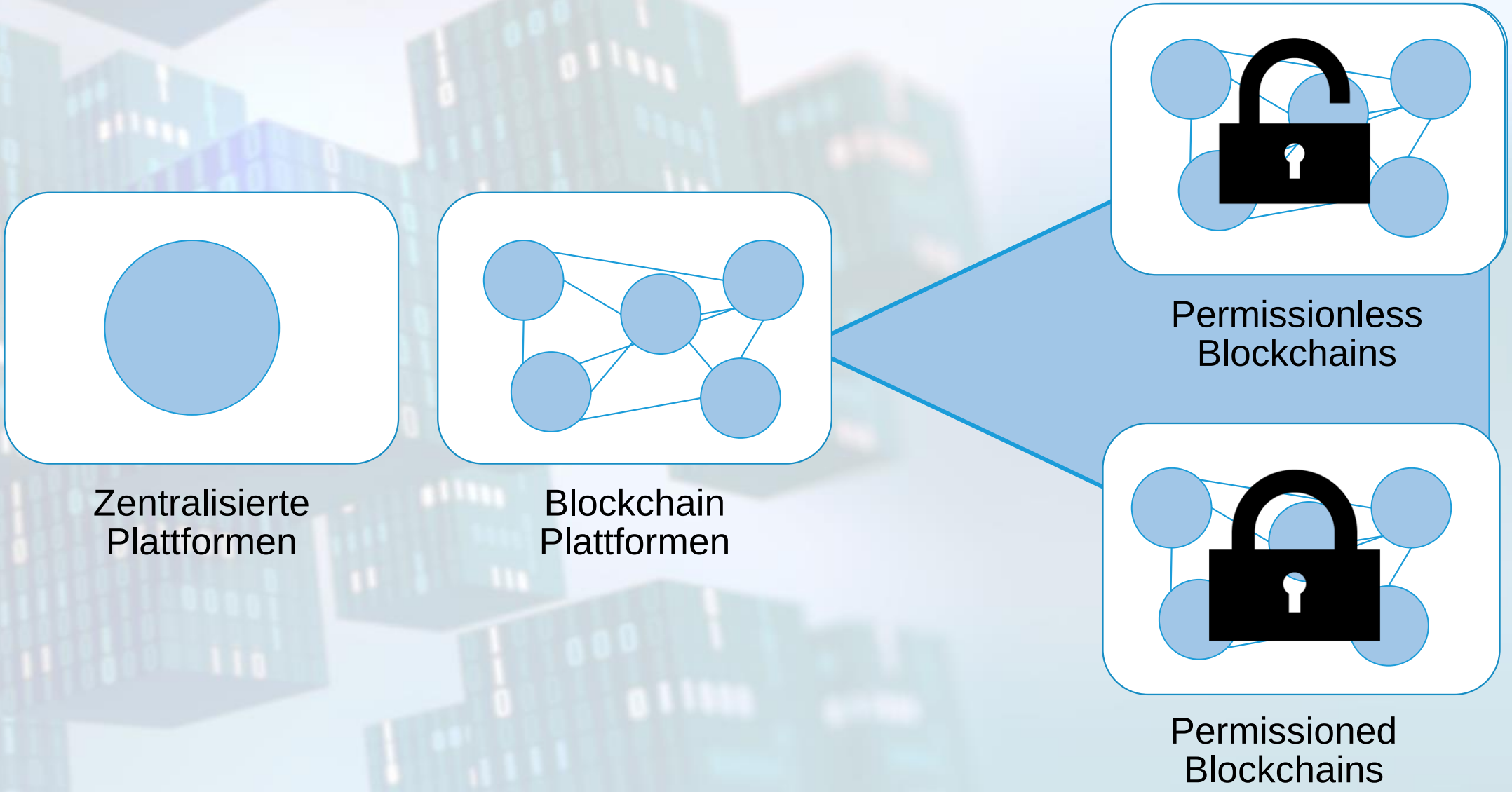
Miner

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Dauerhafte Speicherung
- Angemessene Ausführungszeit
- Register-Änderungen in Reihenfolge des Eingangs

Vertrauen

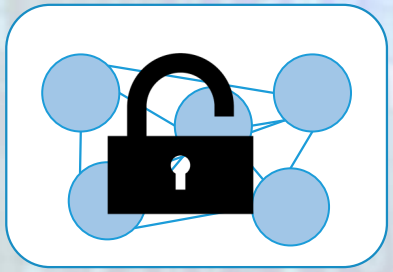
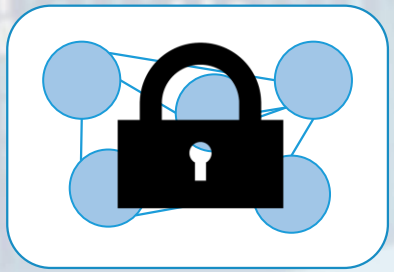
Währungseinheit
Token

Blockchain Plattformen: Zugangsarten



Wer darf welche Rollen einnehmen?

BLOCKCHAIN Bayern e.V.

	Wallet Owner	Node	Miner	Beispiele
 **Permissionless**	**Jeder** User und Konten sind pseudonymisiert	**Jeder** Alle Transaktionen sind öffentlich einsehbar	**Jeder** Mining ist öffentlich zugänglich	**Bitcoin** **Ethereum**
 **Permissioned**	**Kontrolliert** (z.B. durch Konsortium) User und Konten sind pseudonymisiert	**Kontrolliert** (z.B. durch Konsortium) Transaktionen sind meist nicht öffentlich einsehbar	**Kontrolliert** (als Teil des Konsortiums) Mining im Konsortium geregelt	**Corda** **Hyperledger**

BLOCKCHAIN
Bayern e.V.

Wir bringen Blockchain in Bayern voran.

Nutzung von Blockchains: Stärken, Schwächen, Anwendungsgebiete

Stärken der Blockchain-Technologie

Manipulations-sicherheit
Konsens
Kryptographische Verfahren

Zuverlässigkeit
Dezentrale Verfügbarkeit

Pseudonymität
Keine Klarnamen

Transparenz / Disintermediation
Kein Intermediär
Keine Datenkraken
Nutzung und Betrieb getrennt

Anpassbarkeit
Open Source Software

Offener Zugang
Daten und Trans-aktionen

Automatisierung von Transaktionen
Smart Contracts
Smart Oracles
(nächstes Webinar)

Schwächen der Blockchain-Technologie

Aktuelle und zukünftige Anwendungsgebiete (B2B & B2C)

BLOCKCHAIN Bayern e.V.

Branchen

Finanzindustrie	• Ersatz von Vermittlern bei Transaktionen • Kryptowährungen • Mikrokredite und Crowdfunding Peer-to-Peer • ICOs: Anschubfinanzierung
Automotive	• Lieferkettenverfolgung • Digitale Identität eines Autos • Digitale Mobilitätslösungen (z.B. Carsharing)
Pharma und Medizin	• Zugang zu dezentralen Patientenakten • Prävention von Verschreibungsmissbrauch • Prävention von gefälschten Arzneimitteln
Energie	• Kurzfristiger Stromlieferantenwechsel • Herkunftsnachweise • Peer2Peer Stromhandel

Branchenübergreifend, peer to peer

Dokumentation	• Eliminierung einiger Notardienste • Rückverfolgbare Lieferkette • Service- & Wartungsprotokolle • Digitale Ursprungszeugnisse
Digitale Identitäten	• Flüchtlinge zahlen per Retinascan • Direkte Vergütung der Lizenzinhaber • Ursprungszeugnisse des digitalen Zertifikats
Digitales Rechte-management	• Rechte an Patenten, Kunst oder Ideen auf der Blockchain (inkl. Zeitstempel) • Sichern von 3D-Druckermodellen • Direkte Vergütung der Lizenzinhaber
Sharing Economy	• Transaktionen ohne zentralen Plattformanbieter • Dezentrales dokumentiertes Tauschen • Nutzungspflichtversicherungen

Ist die Blockchain die Zukunft oder geht das alles wieder vorbei?

- Hohe **Entwicklungsgeschwindigkeit**
- **Großes finanzielles** Interesse
- **Großes Potential** bei Blockchain durch Automatisierung, Tokenisierung, digitale Assets und digitale Identitäten

- Blockchains sind nur für wenige Usecases das beste Mittel, es fehlt oft an **Know-How**
- Fehlende **Regulierungen**
- Unzureichende **Digitalisierung** in vielen Bereichen
- Komplexe **Governance**

- Klassische Geschäftsmodelle werden zunehmend unprofitabel
  - **Innovationsdruck steigt**

- Die **Interdisziplinarität** wird immer wichtiger, da Blockchain Branchen miteinander verbinden kann
- Blockchain ist ein **fester Bestandteil der digitalen Infrastruktur**
- Der Hype ist vorbei, Blockchain hat nun die Chance, das in ihr steckende Potential zu zeigen
- Blockchain ist weder Allheilmittel noch das größte Übel aller Zeiten

- **Die Zukunft kann man am besten voraussagen, wenn man sie selbst gestaltet.**
- **Nächstes Webinar (11.05.): Funktion der Blockchain**

Über Blockchain Bayern e.V.

BLOCKCHAIN Bayern e.V.

Wir bringen Blockchain in Bayern voran.

- **Gemeinnütziger Verein**, gegründet am 29. Mai 2019
- Vorstände: Prof. Dr. Florian Matthes, Maximilian Irlbeck, Christoph Möslein
- Schirmherrschaft: Judith Gerlach MdL, Bayerische Staatsministerin für Digitales
- Vereinsziel:
  - Blockchain in Bayern nachhaltig fördern und voranbringen.
  - Slogan: **Wir bringen Blockchain in Bayern voran.**
  - Sowohl für Blockchain Experten als auch Blockchain Anwender / Interessierte
- Unsere Ziele laut Satzung:
  - Förderung der **interdisziplinären Vernetzung**
  - **Forschung und Erfahrungsaustausch** zu Blockchain / Distributed Ledger
  - Erarbeitung und Verbreitung von **Informationsmaterialien**

- Mehr als **130 Mitglieder** aus ganz Bayern
  - aus Unternehmen, Wissenschaft und öffentlicher Verwaltung

- Persönliche und Firmenmitgliedschaften sind möglich

Mehr unter: www.blockchain-bayern.de

Gründungsfeier am 25.09.2019 in München mit mehr als 330 Teilnehmern

Das Gründerteam

BLOCKCHAIN
Bayern e.V.

Wir bringen Blockchain in Bayern voran.

Vielen Dank.

Ihre Fragen jetzt oder an:
kontakt@blockchain-bayern.de

www.blockchain-bayern.de