Blockchain

Potentiale der Nachhaltigkeit

Gliederung

- Marktformen
- Standards der Blockchain
- Funktionsweise
- Smart Contracts und Ethereum
- Ziele und Gefahren
- Anwendungen der Blockchain

Blockchain ist …

Centralized	Decentralized	Distributed
Zentrale Instanz, ausschließlich zur Datenbereitstellung Client-Server-Architektur	Mehrere Zentraleinheiten, die jeweils mit Clients verbunden sind Clients (Knoten) treffen jeweils eigene Entscheidungen Peer-to-Peer Master-Slave-Architektur	Zusammen unabhängiger Knoten, die sich als ein System präsentieren Peer-to-Peer Client-Server (Knoten als Serverrolle zur Koordination) n-Tier-Architektur Geringe Latenz

…in der Regel als verteiltes System aufgebaut, welches als dezentrales Ledger fungiert!

Quellen: www.geeksforgeeks.org; academy.binance.com

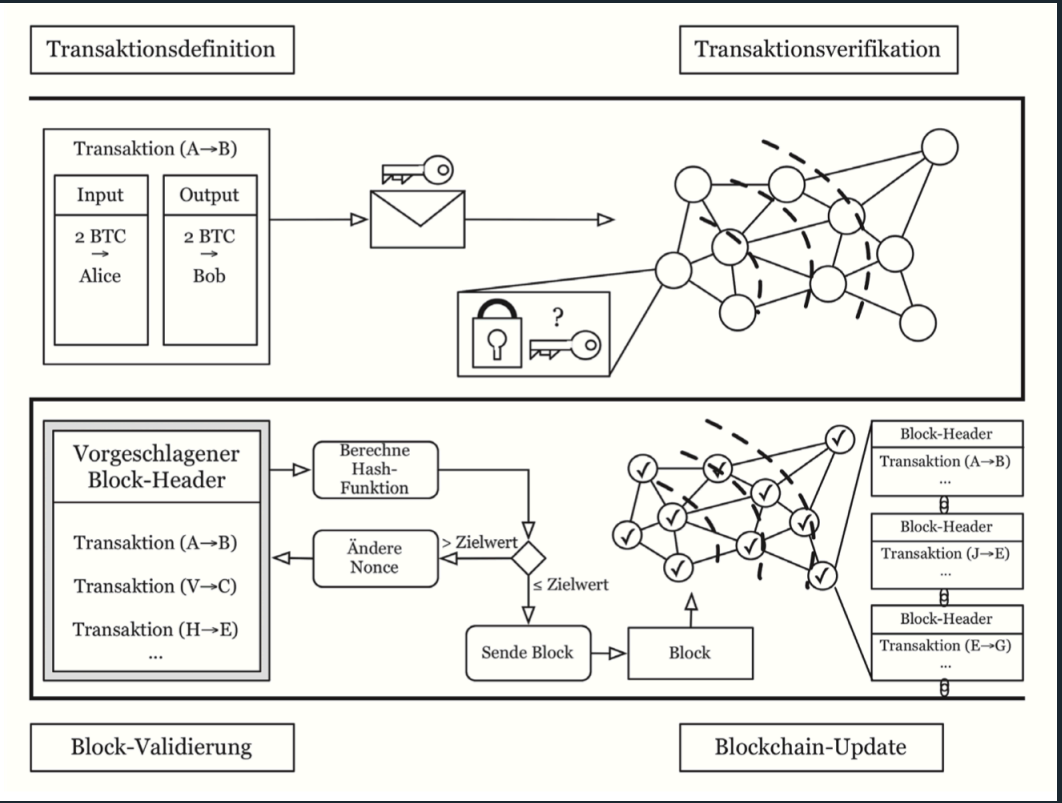
Blockchain ist …

Centralized	Decentralized	Distributed
	Blockchain 2.0 Integration von Smart Contracts, Entwicklung von neuen Applikationen (Ethereum)	
	Entwicklung →	
	Blockchain 1.0 einfache Strukturen, die die Transaktionen veränderungssicher aufnimmt (Bitcoin)	**DLT** Schnell agierende und hochskalierbare Struktur; Integrieren Blockchains verschiedener Protokolle (IOTA)

…in der Regel als verteiltes System aufgebaut, welches als dezentrales Ledger fungiert!

Quellen: „Global Blockchain Benchmarkin Study“, Hileman et. al. 2017

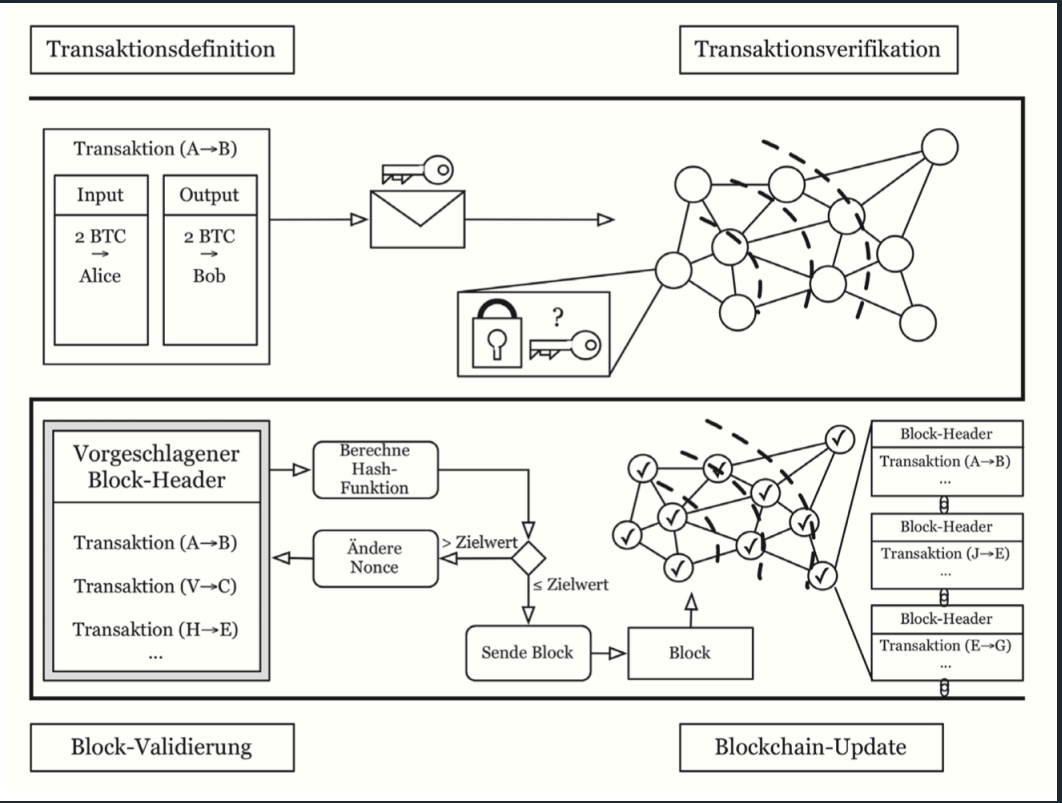
Funktionsweise BTC



1. A schickt Nachricht mit Transaktionsdetails (Betrag und Adresse von B + frühere Transaktions von A)
2. A muss alle Inputs mit den zugehörigen Schlüsseln digital signieren
3. Signierte Transaktion wird dann an das Netzwerk geschickt
4. Jeder Netzknoten erhält die unbestätigte Transaktion (noch nicht in der Blockchain)
5. Erster Netzknoten prüft, ob der beteiligte Input nicht schon anderweitig verschoben wurde + Vergleich von Input und Output + Gültigkeit der Signatur
6. Verteilung zur Prüfung an andere Knoten + Aufnahme DB für unbestätigte Transaktionen

Quelle: „Blockchain: Grundlagen, Anwendungen und Potentiale", Schlatt et. al., 2016

Funktionsweise BTC

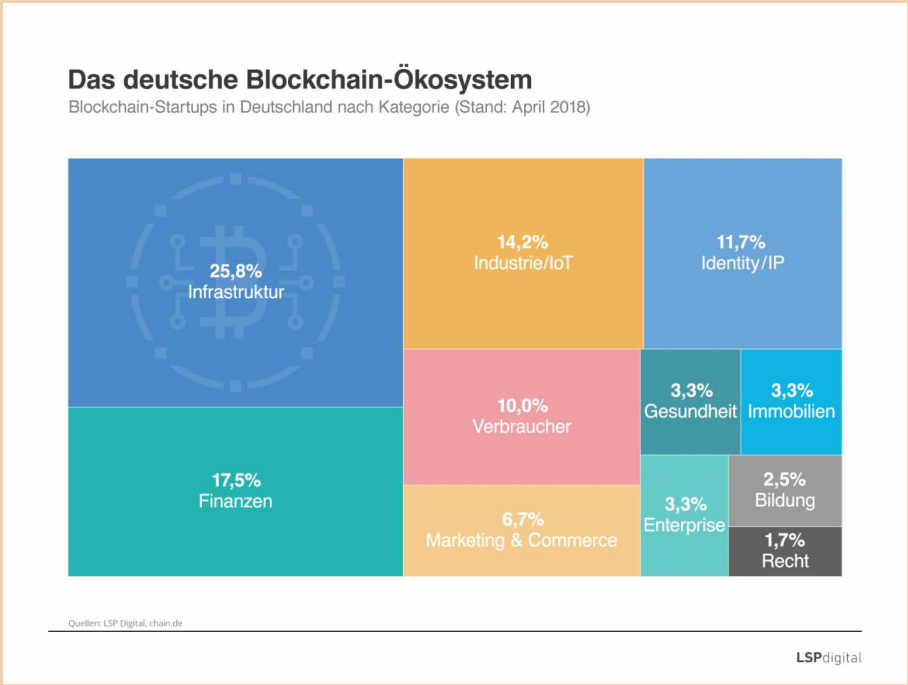


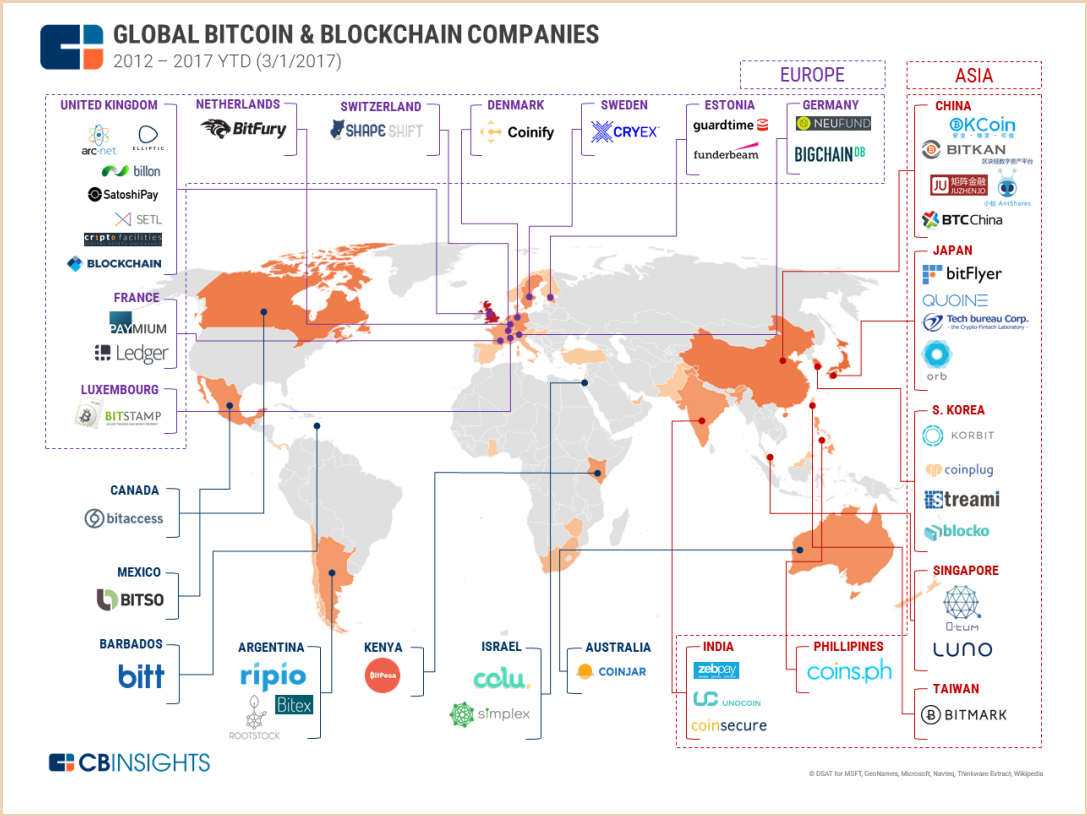
1. Typen: Mining-Netzknoten und passive Netzknoten
2. Transaktion: annehmen, prüfen, weiterleiten
   - über die Funktion SHA256 Hashfunktion generiert
   - diese ist durch die Miners zu finden
   - hohe Rechenleistung erforderlich
3. Zusammenfassung unbestätigter Transaktion + Bildung eines Blockheaders
4. Blockheader bekommt eine Referenz
5. Update der Blockchain aller 10 min
6. Als Anreiz bekommen Miners die Transaktionsgebühren (0,0001 BTC)

Quelle: „Blockchain: Grundlagen, Anwendungen und Potentiale“, Schlatt et. al., 2016

Video

Verteilung





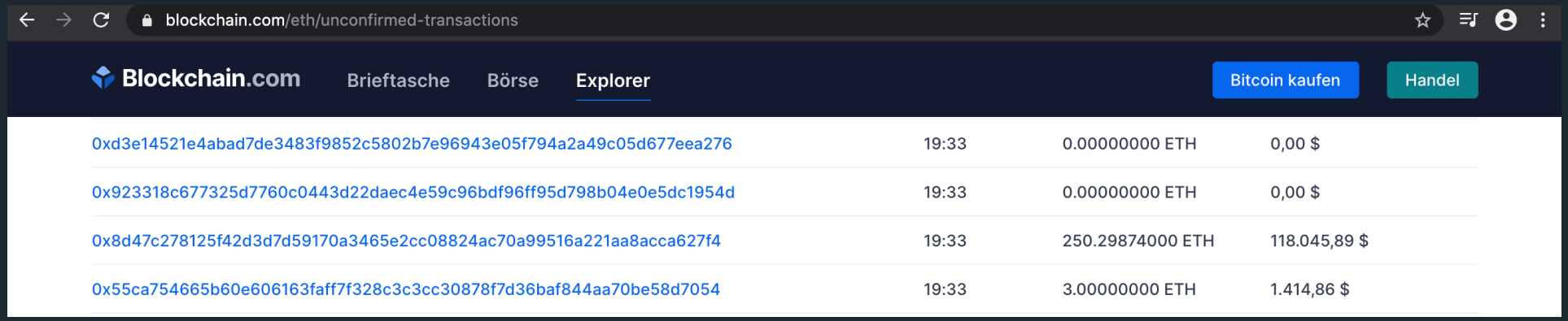
Quellen: https://cbi-blog.s3.amazonaws.com/blog/wp-content/uploads/2017/03/2017.02.22-Geographic-Heatmap-v2.8.png / https://www.lsp.de/sites/default/files/styles/default/public/media/article-insight/20180607_Blockchain_LSP.jpg?itok=rXujrMo9

Smart Contracts

- Eines der meistgenutzten Funktionen von Unternehmen in einer Blockchain
- Führt eine Funktion automatisch aus, wenn ein vordefiniertes Ereignis vorliegt
- Ausführung durch Systemregeln garantiert
- Ergebnis durch alle Netzwerkbeteiligten überprüfbar
- Keine Abhängigkeit durch Drittanbieter

Ethereum

- Open-Source-Plattform für dezentrale Anwendungen
- Herzstück der Architektur ist die Etherum-Virtual-Maschine
- Code wird direkt in der VM ausgeführt
- Eigene Kryptowährung Ether 1 ETH = 468 USD (Stand 16.11.2020)
- Block-Update ca. 15s
- Beliebtheit hoch, viele Aktivitäten auf GitHub
- Jede Transaktion und Service kostet Ether (1,461 ETH – Stand 16.11.2020)



Quelle: https://www.blockchain.com; bitinfocharts.com

Ziele und Gefahren von Blockchain

- Transparenz, Authentifizierung, Prüfung, Vertrauen
- schnell, kostengünstig, direkt

- Keine vollständige Anonymität beim Kauf von Kryptowährungen
- Kaum Rechtsgrundlagen und -sicherheit (z.B. Diebstahl)

Diebstahl - Ether

Datensicherheit und Datenschutz

- Problem: Blockchain – Möglichkeit zur vollständigen Transparenz
- Bekannt: Sender – Transaktionshöhe – Empfänger
- Unbekannt: Sender- und Empfängeradresse (Pseudonymität)
- Gefahr: Identitäten zuordnen kann = Transaktionsgraph (Aufdeckung der Privatsphäre)
- Schnelle Offenlegung der Adresse durch z.B. Kauf von Waren mit Kryptowährungen über Drittbeteiligte
- Sicherer Erwerb von Coins mit Einzahlung von Bargeld (LocalBitcoins)

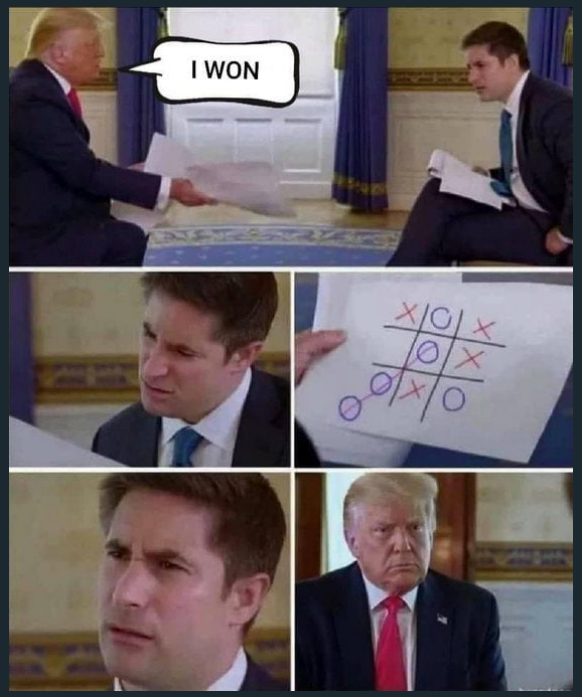
Welternährungsprogramm

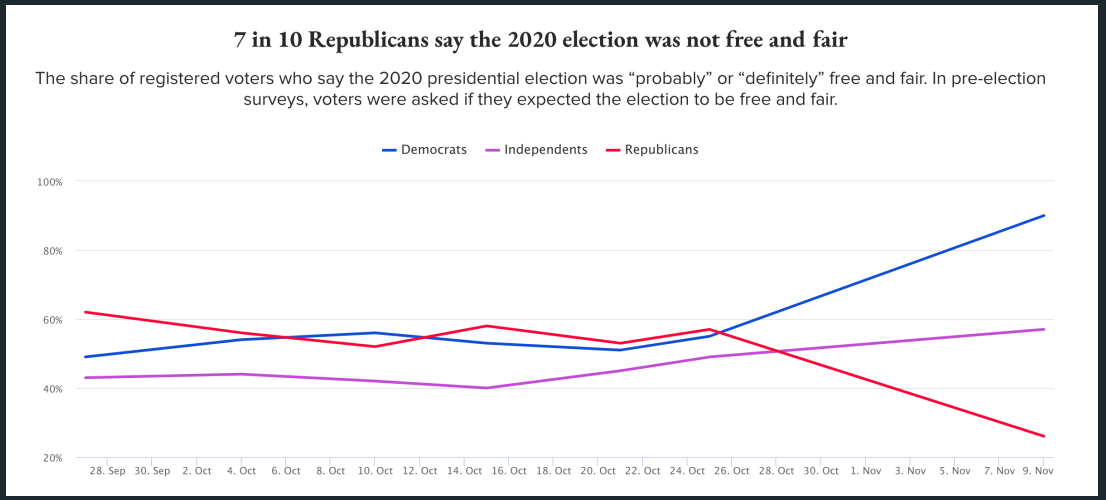
- Flüchtlingsunterkunft an der Grenze von Jordanien
- Zahlung in Shops und Lebensmittelmärkten
- Führung eines virtuellen Konto
- Vorteile: keine Bankgebühren (inkl. Bargeldverfügbarkeit)
- Framework: Hyperledger Fabric

Blutdiamanten

- Unterbindung der Finanzierung von gewalttätigen Konflikten
- Gesellschaftliches Interesse an einem sicheren Herkunftsnachweis
- Lösung: Zertifizierung und Listing von Diamanten
- Problem: Förderung in politisch instabilen Ländern
- Framework: EverLedger

US-Wahlen 2020





Quellen: https://morningconsult.com/form/tracking-voter-trust-in-elections/; https://9gag.com/gag/amvQgoX ; https://9gag.com/gag/aj94KqR
https://content.fortune.com/wp-content/uploads/2020/11/Screen-Shot-2020-11-04-at-7.00.13-AM.png

- *„Ein Wahlsystem kann die Sicherheit der Blockchain und der Post nutzen, um ein zuverlässiges Wahlsystem bereitzustellen. Ein registrierter Wähler erhält in der Post einen computerlesbaren Code und bestätigt bei der Wahl seine Identität. Zudem bestätigt der Wähler die Korrektheit der Wahlinformationen. Das System trennt Wähleridentifikation und Stimmabgabe, um die Anonymität der Wahl zu gewährleisten, und speichert die Stimmen auf verteilten Ledgern in einer Blockchain.“* – Patentanmeldung des USPS

Quelle: cvj.ch

»Die generelle gesamtglobale Antwort wäre, immer wenn ich mehrere Akteure habe, die sich nicht zwingendermaßen vertrauen, kann ich die Blockchain einsetzen.« (Quelle: bitcom.org)

Quellen

- https://academy.binance.com/de/articles/difference-between-blockchain-and-bitcoin (abgerufen am 14.11.2020)
- https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/ (abgerufen am 14.11.2020)
- „Gobal Blockchain Benchmarking Study", Hileman, Dr Garrik, Rauchs, Michel, 2017, Zugriff: https://j2-capital.com/wp-content/uploads/2017/11/GLOBAL-BLOCKCHAIN.pdf
- „Blockchain: Grundlagen, Anwendungen und Potentiale", Schlatter, V., Schweizer, A., Urbach, N., Fridgen, G., Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, 2016, Zugriff: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf
- https://www.bitkom.org/sites/default/files/2019-06/190613_bitkom_studie_blockchain_2019_0.pdf (abgerufen am 17.11.2020)
- https://bitinfocharts.com/de/comparison/ethereum-transactionfees.html
- https://cvj.ch/fokus/blockchain/us-postbehoerde-meldet-patent-fuer-blockchain-basiertes-wahlsystem-an/