



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

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

Quellen: [www.geeksforgeeks.org](http://www.geeksforgeeks.org); [academy.binance.com](http://academy.binance.com)

# Blockchain ist ...

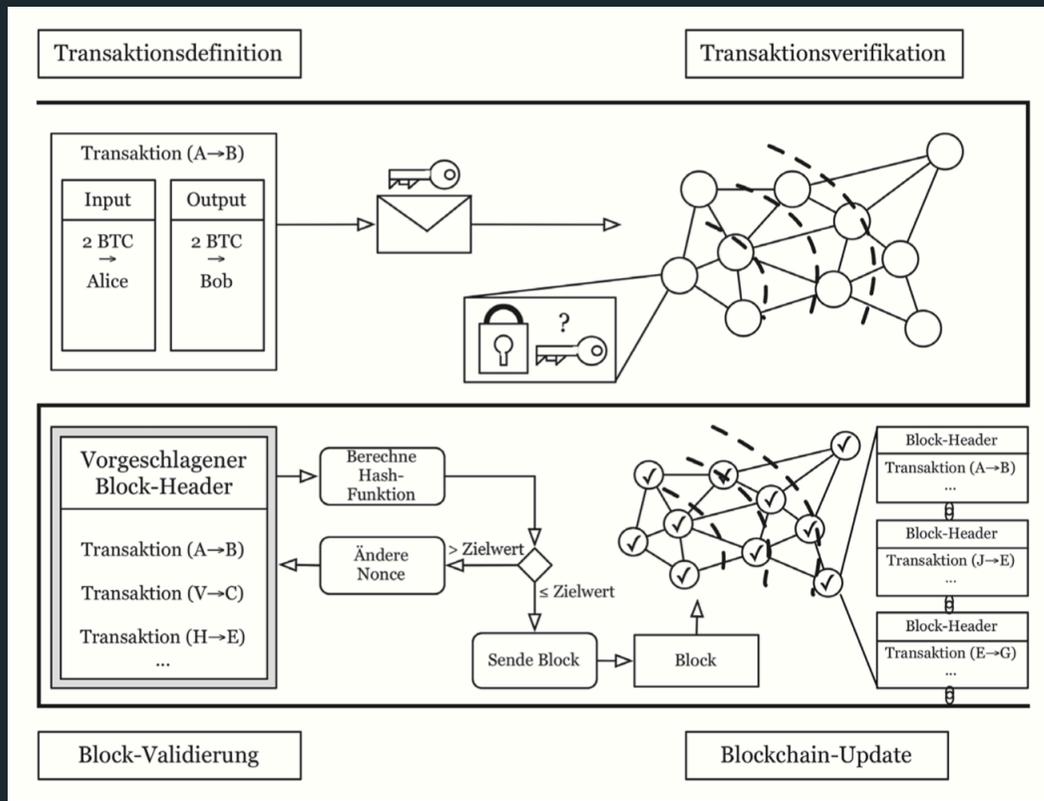
Centralized	Decentralized	Distributed
	<p><b>Blockchain 1.0</b> einfache Strukturen, die die Transaktionen veränderungssicher aufnimmt (Bitcoin)</p>	<p><b>DLT</b> Schnell agierende und hochskalierbare Struktur; Integrieren Blockchains verschiedener Protokolle (IOTA)</p>
	<p><b>Blockchain 2.0</b> Integration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

Entwicklung →

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

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

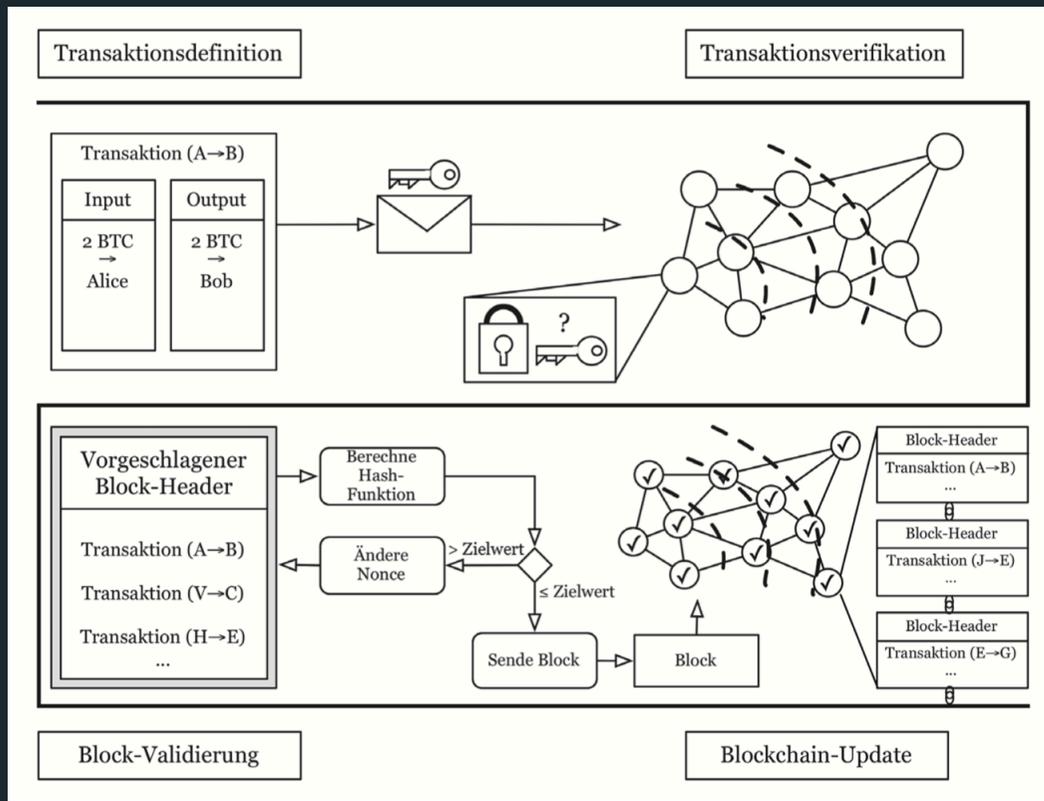
# Funktionsweise BTC



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

# Funktionsweise BTC

1. Typen: Mining-Netznoten und passive Netznoten
2. Transaktion: annehmen, prüfen, weiterleiten
  - über die Funktion SHA256 Hashfunktion generiert
  - diese ist durch die Miner 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 Miner die Transaktionsgebühren (0,0001 BTC)



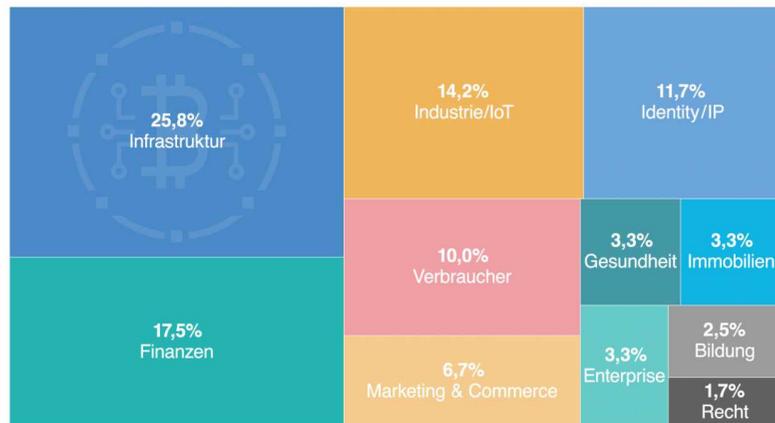
Quelle: „Blockchain: Grundlagen, Anwendungen und Potentiale“, Schlatt et. al., 2016

Video

# Verteilung

## Das deutsche Blockchain-Ökosystem

Blockchain-Startups in Deutschland nach Kategorie (Stand: April 2018)

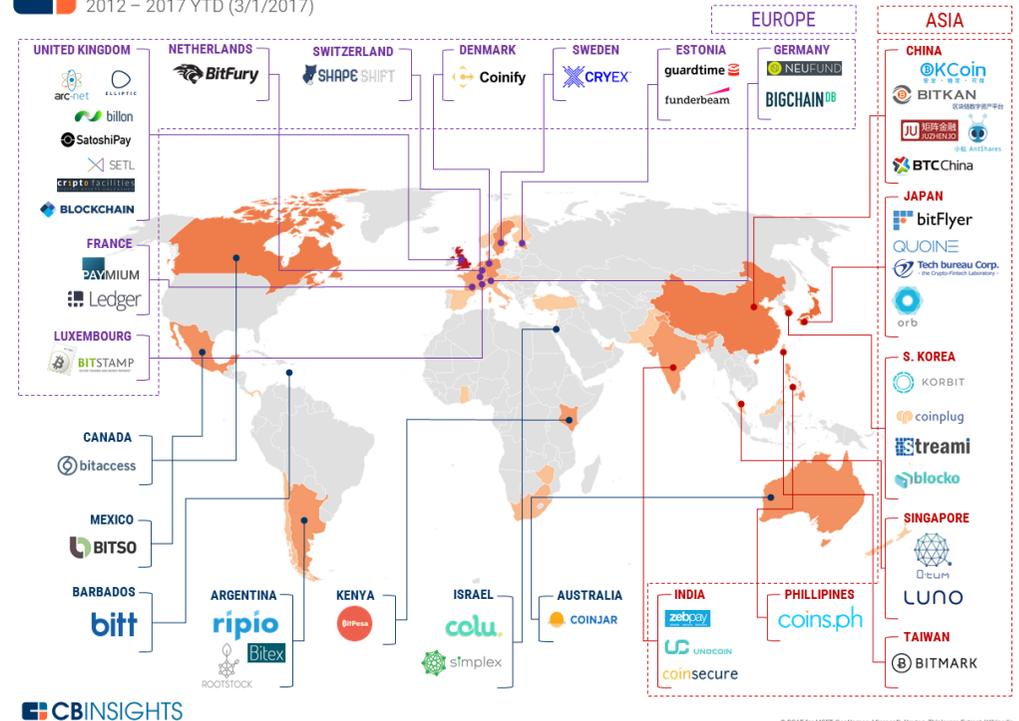


Quellen: LSP Digital, chain.de

LSPdigital

## GLOBAL BITCOIN & BLOCKCHAIN COMPANIES

2012 – 2017 YTD (3/1/2017)



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](https://www.lsp.de/sites/default/files/styles/default/public/media/article-insight/20180607_Blockchain_LSP.jpg?itok=rXuJrMo9)

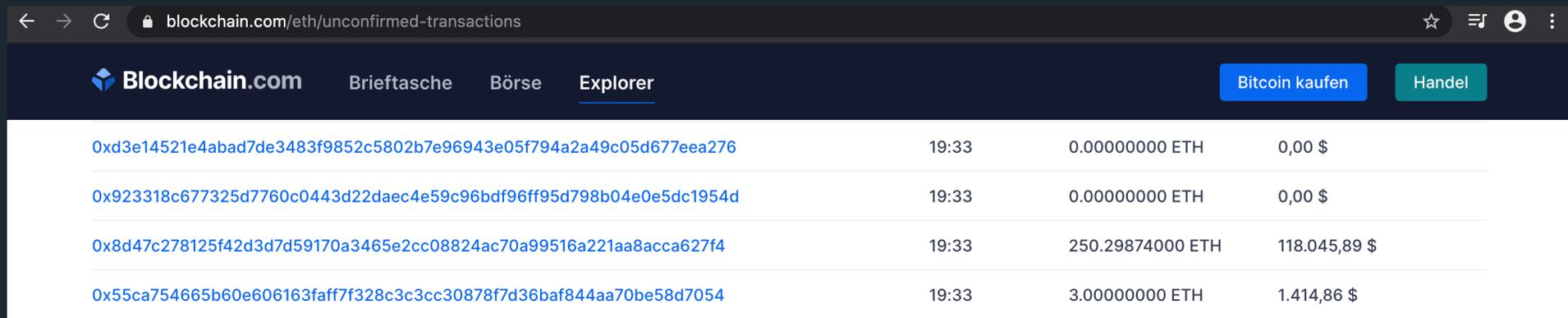
# Smart Contracts



- 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 Netzwerkteiligen überprüfbar
- Keine Abhängigkeit durch Drittanbieter

# Ethereum

- Open-Source-Plattform für dezentrale Anwendungen
- Herzstück der Architektur ist die Ethereum-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)



The screenshot shows the Blockchain.com Explorer interface. The browser address bar displays 'blockchain.com/eth/unconfirmed-transactions'. The navigation menu includes 'Blockchain.com', 'Brieftasche', 'Börse', and 'Explorer'. There are buttons for 'Bitcoin kaufen' and 'Handel'. The main content area displays a table of unconfirmed transactions with the following data:

Transaction Hash	Time	Amount (ETH)	Amount (\$)
<a href="#">0xd3e14521e4abad7de3483f9852c5802b7e96943e05f794a2a49c05d677eea276</a>	19:33	0.00000000 ETH	0,00 \$
<a href="#">0x923318c677325d7760c0443d22daec4e59c96bdf96ff95d798b04e0e5dc1954d</a>	19:33	0.00000000 ETH	0,00 \$
<a href="#">0x8d47c278125f42d3d7d59170a3465e2cc08824ac70a99516a221aa8acca627f4</a>	19:33	250.29874000 ETH	118.045,89 \$
<a href="#">0x55ca754665b60e606163faff7f328c3c3cc30878f7d36baf844aa70be58d7054</a>	19:33	3.00000000 ETH	1.414,86 \$

Quelle: <https://www.blockchain.com>; [bitinfocharts.com](https://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

www.cnn.com › 2017/07/20 › 32-million-worth-of-digit...

**\$32 million worth of digital currency ether stolen by hackers**

→ 2017 — More than 150000 ether tokens, a digital currency similar to bitcoin, were stolen by cybercriminals on Wednesday.

thenextweb.com › Hard Fork

**Hackers steal \$48.7M in Ethereum from South Korean ...**

27.11.2019 — South Korean cryptocurrency exchange Upbit has reported that hackers have ransacked its Ethereum \$ETHΔ3.37% "hot wallet," stealing ...

www.theguardian.com › nov › cry... ▾ Diese Seite übersetzen

**'\$300m in cryptocurrency' accidentally lost forever due to bug ...**

08.11.2017 — The lost money was in the form of Ether, the tradable currency that fuels the Ethereum distributed app platform, and was kept in digital ...

www.investopedia.com › news › c... ▾ Diese Seite übersetzen

**CoinDash: Ethereum Hacker Returned 20,000 Stolen Ether ...**

25.06.2019 — The hacker, whose identity is still unknown, hijacked the site and quickly stole 43,000 ether tokens, CoinDesk reported. The thief still has ...

# 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



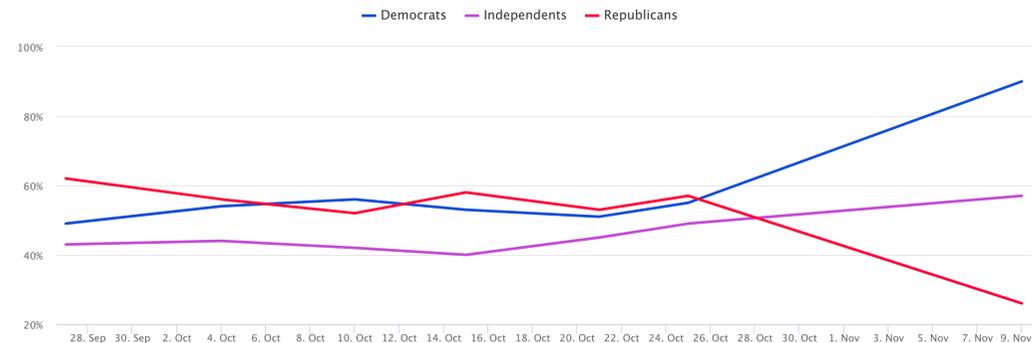
- Unterbindung der Finanzierung von gewalttätigen Konflikten
- Gesellschaftliches Interesse an einem sicheren Herkunftsnachweis
- Lösung: Zertifizierung und Listing von Diamanten
- Problem: Förderung in politisch instabilen Ländern
- Framework: EverLedger

# US-Wahlen 2020



## 7 in 10 Republicans say the 2020 election was not free and fair

The share of registered voters who say the 2020 presidential election was "probably" or "definitely" free and fair. In pre-election surveys, voters were asked if they expected the election to be free and fair.



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

»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.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](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/>