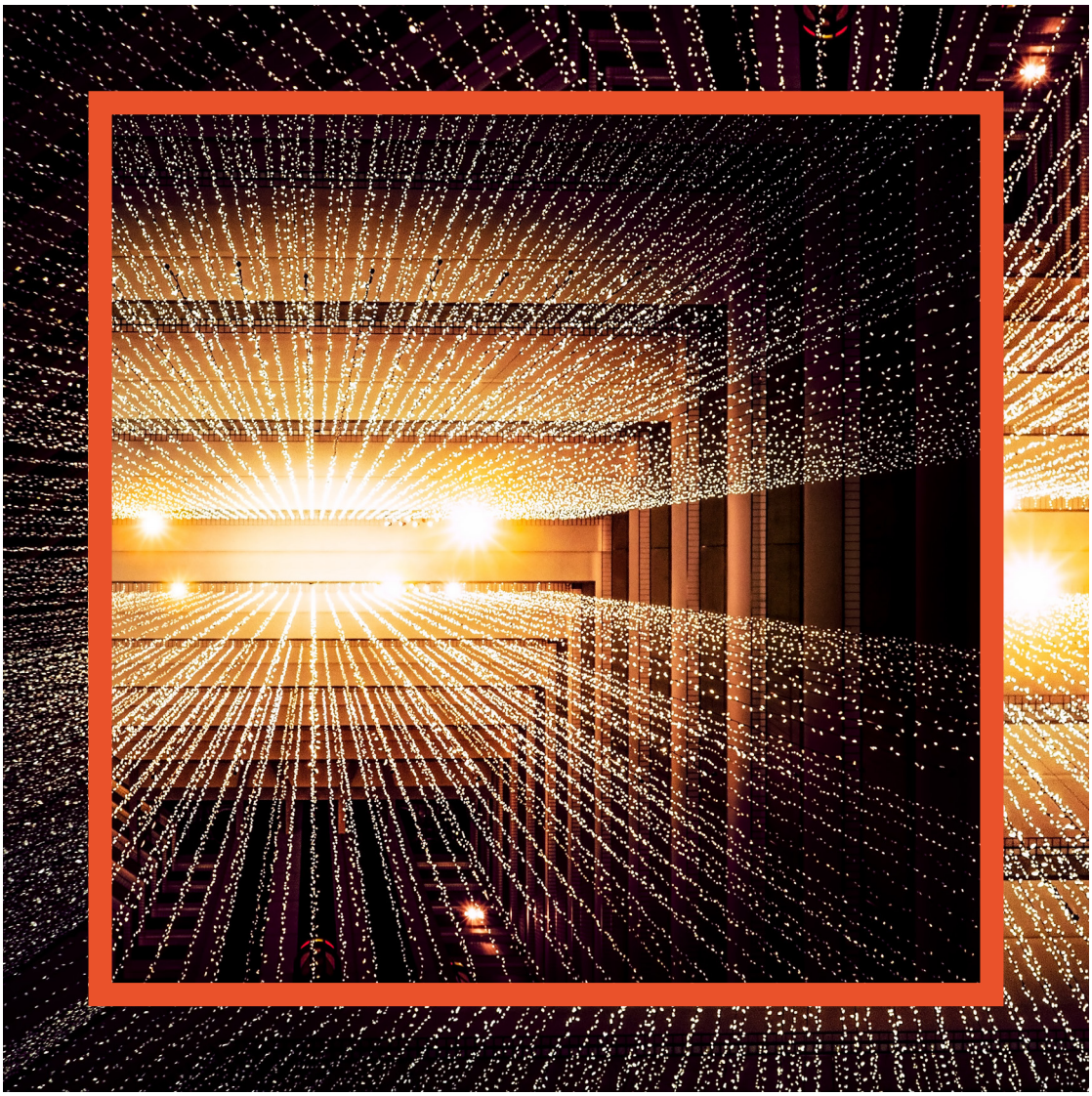
# KRYPTOWÄHRUNGEN:
von Bitcoin zu Ether



Swissquote

# Inhaltsverzeichnis

# BITCOIN (XBT)

## Die erste Kryptowährung

Bitcoin ist die allererste digitale Währung, die je geschaffen wurde. Sie wurde im Jahr 2009, einen Monat nach dem Zusammenbruch von Lehman Brothers, von dem japanischen Entwickler Satoshi Nakamoto entworfen. Bitcoin wird durch zwei Symbole dargestellt: XBT und BTC.

Das Ziel war in erster Linie, ein anonymes, transparentes, dezentralisiertes und leicht einzurichtendes elektronisches Zahlungssystem aufzubauen.

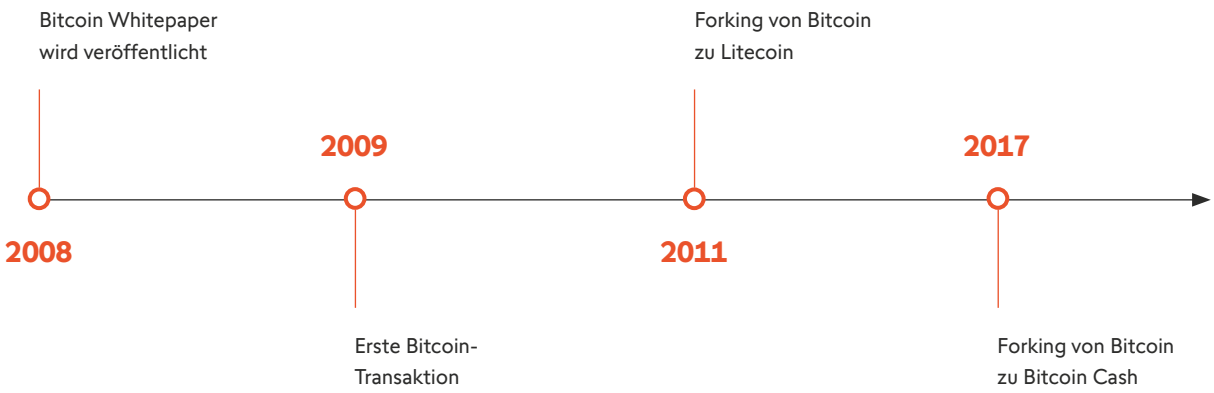
**KENNZAHLEN (STAND: 25. MÄRZ 2020)**

| Crypto | Ranking | Markt-kapitalisierung | Aktueller Kurs |
|---|---|---|---|
| XBT | #1 | EUR 113 Mrd. | EUR 6'148 |

## Kursdiagramm


**Quelle:** CoinMarketCap

# Allgemeine Aspekte




**KRYPTOWÄHRUNG:** Bitcoin ist ein nativer Coin, der sich auf eine digitale Abbildung eines Finanzwertes bezieht und übertragen werden kann. Er beruht auf einer leistungsfähigen Berechnung und mathematischen Verschlüsselung zur Absicherung von Informationen und Transaktionen.

**DEZENTRALISIERT:** Bitcoin ist dezentralisiert. Dies bedeutet, dass keine zentralen Administratoren und Mittelsmänner erforderlich sind. Bitcoin-Einheiten oder -Bruchteile können im Bitcoin-Blockchain-Netzwerk von einem Benutzer zum anderen gesendet werden.

**TECHNOLOGIE:** Die Blockchain ist eine Kette von Blöcken, die miteinander verknüpft und unter den Benutzern verteilt sind, um als unveränderliches Datenjournal zu fungieren.

**BEGRENZTES ANGEBOT:** Ähnlich wie viele Kryptowährungen zeichnet sich Bitcoin durch ein begrenztes Angebot aus. In der Praxis bedeutet dies, dass keine Bitcoins mehr generiert werden, sobald das maximale Angebot von 21 Millionen Einheiten erreicht ist.

**QUELLOFFEN:** Das Bitcoin-Protokoll ist quelloffen. Jedermann kann auf den Code zugreifen, Einblick in den Code nehmen und zur Entwicklung des Codes beitragen.

### Andere Blockchain-Anwendungsbereiche

**KARITATIVE TÄTIGKEITEN**
Optimierung der Transparenz bei der Verwendung empfangener Gelder.

**GESUNDHEITSWESEN**
Verbesserung der Sicherheit von digitalen Patientenakten und der Rückverfolgbarkeit der Arzneimittelversorgung.

# Die Blockchain

## Was ist die Blockchain?

Blockchain ist die Technologie, die Bitcoin und vielen anderen Kryptowährungen zugrunde liegt.

**Eine Blockchain ist eine Datenbank, die als dezentralisiertes digitales Journal (Ledger) fungiert. Die Datensätze werden zu Blöcken organisiert, die kryptografisch miteinander verbunden sind.**

Die wichtigsten Vorteile sind ihre permanente Verfügbarkeit, weil es keinen einzelnen Ausfallpunkt (Single Point of Failure) gibt, und ihre Stabilität, weil Daten nach der Registrierung in der Blockchain nicht verändert werden können. Durch die Blockchain-Technologie entfällt zudem die Abhängigkeit von Vermittlern und die Notwendigkeit, einer einzelnen Organisation zu vertrauen.

## Wodurch wird die Sicherheit der Blockchain gewährleistet?

Bei Bitcoin und vielen anderen virtuellen Währungen garantiert die Blockchain-Technologie, dass kein Bitcoin vernichtet oder dupliziert wird. Ermöglicht wird dies durch zwei wesentliche Blockchain-Eigenschaften:

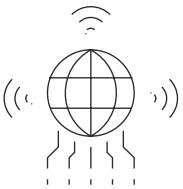
### Unveränderlichkeit

- Sobald eine Transaktion oder die Registrierung irgendeiner Art von Daten als gültig bestätigt ist, **ist keine Änderung mehr möglich und ihre Integrität ist garantiert.**

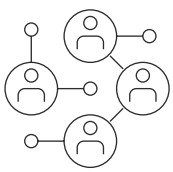
### Konsens

- **Fähigkeit, einen einzig wahren Status des Blockchain-Netzwerks u**nd dadurch die Gültigkeit jeder im Netzwerk erfassten Transaktion **zu gewährleisten.**

### Andere Blockchain-Anwendungsbereiche



**INTERNET OF THINGS**
Blockchain ermöglicht die Absicherung der Datenerfassungsmöglichkeiten, die das IoT bietet.



**LIEFERKETTE**
Verbesserung des Managements der Produktverteilung und Transparenz der Zahlungen.

## Wie funktioniert die Bitcoin-Blockchain?

Wie bereits erklärt, kann eine Bitcoin-Transaktion nach der Validierung nicht mehr geändert oder aus der Blockchain gelöscht werden. Tatsächlich werden Daten durch Blöcke hinzugefügt, die miteinander verkettet sind.

**Die Kette von Blöcken und Transaktionen ist nachprüfbar, da sie von jedermann gesehen werden können. Die Blockchain lässt sich als Verzeichnis beschreiben, in dem jede neue Eintragung mit der vorhergehenden verknüpft ist. Wenn wir uns z. B. den 452. Block ansehen, können wir überprüfen, dass er auf den 451. Block folgt. Selbst der bislang letzte Block wäre anders, wenn der allererste jemals geschaffene Block («Genesis-Block») auch anders wäre.**

## Wie sind Blockchain-Blöcke miteinander verknüpft?

Einfach ausgedrückt, ermöglicht die mathematische Verschlüsselung, die hinter der Bitcoin-Blockchain steckt, die Generierung eines eindeutigen Outputs durch jeden Block aus den in dem Block enthaltenen Daten. Dieser Output wird dann an den folgenden Block weitergegeben, sodass eine permanente Verknüpfung zwischen den beiden Blöcken entsteht. Auf diese Weise ist jeder Versuch einer nachträglichen Änderung von vorhergehenden Transaktionen von vornherein ausgeschlossen.

### WAS IST HASHING?

Als Hashing bezeichnet man den Vorgang, durch den verschiedene Inputs von unterschiedlicher Grösse verschiedene Outputs von konstanter Grösse generieren. Hashing-Algorithmen generieren ausserdem immer den gleichen Output aus dem gleichen Input.

**BLOCKCHAIN-ANALOGIE**

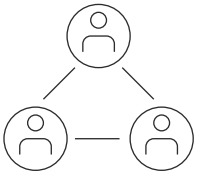
| Block-Rang | Block | Hash-Analogie |
|---|---|---|
| 1 | hsgAO → | EM |
| 2 | lzoEM → | OF |
| 3 | pmzOF → | LN |

## Wie werden Blockchain-Blöcke geschaffen?

Die Produktion neuer Blöcke ist das direkte Ergebnis eines Prozesses, den man als «Mining» bezeichnet. Wie schon gesagt, werden Blöcke mittels Kryptografie miteinander verknüpft. Die Produktion neuer Blöcke erfordert die Mitwirkung von Netzwerkteilnehmern, die durch den Einsatz ihrer Rechenleistung die mathematische Verschlüsselung von Transaktionsdaten ermöglichen.

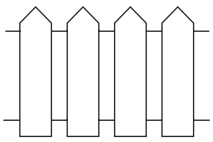
**Dadurch sind Miners für die Überprüfung aller Transaktionen verantwortlich. Ausserdem erhalten sie als Belohnung für ihre Mining-Tätigkeit neu geschaffene Bitcoins, die somit in das Netzwerk einfliessen.**

## Was bietet die Bitcoin-Blockchain?



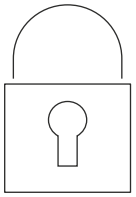
### MACHT GEGENPARTEIEN ÜBERFLÜSSIG

Alle Bitcoin-Zahlungen erfolgen, ohne dass eine Gegenpartei benötigt wird. Das ermöglicht niedrigere Transaktionsgebühren und eine Verringerung der Risiken, die üblicherweise mit der Einschaltung von Mittelsmännern verbunden sind.



### NIEDRIGE EINTRITTSBARRIEREN

Die Blockchain ist genehmigungsfrei. Das heisst, für die Teilnahme und Mitwirkung am Blockchain-Netzwerk ist keine Genehmigung erforderlich. Von daher braucht ein Benutzer lediglich eine Internetverbindung, damit er aktiv Bitcoin-Transaktionen tätigen kann.

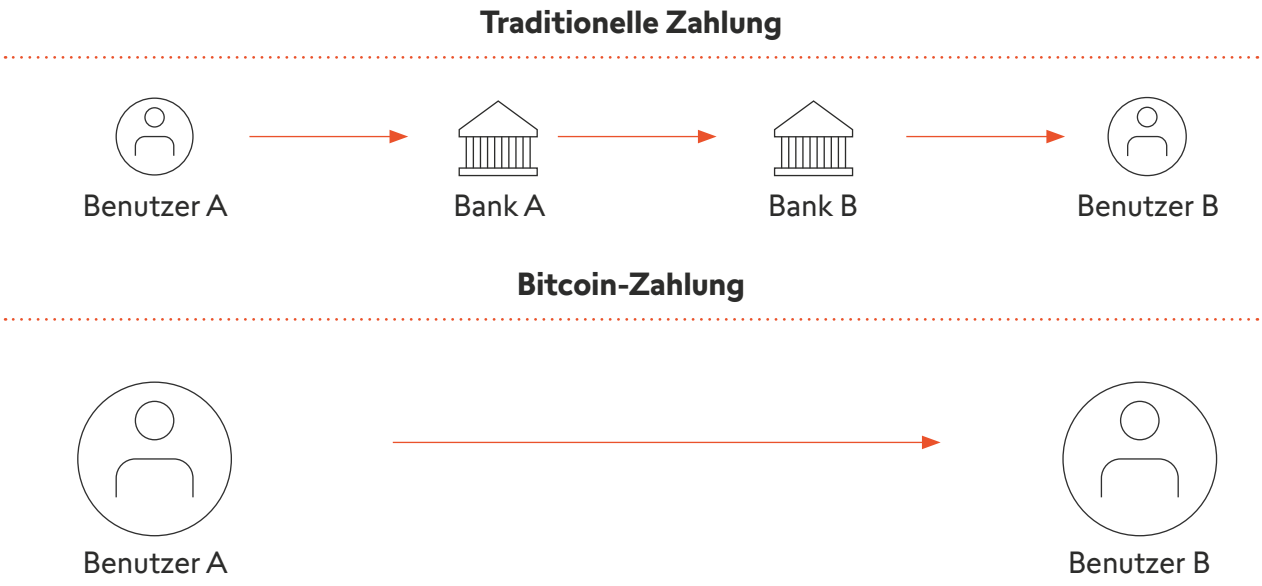


### VERBESSERTE SICHERHEIT

Aufgrund ihrer Dezentralisierung besteht in der Blockchain kein einzelner zentraler Server, der das Opfer böswilliger Handlungen werden könnte. Die Blockchain funktioniert durch ein Netzwerk verteilter Nodes. Ein Hacker müsste daher eine sehr grosse Zahl von Nodes auf einmal angreifen, um das Netzwerk zu gefährden.

# Bitcoin-Zahlungen

## Vergleich mit traditionellen Zahlungsmethoden




## Welche Non-Custodial-Speicheroptionen bestehen bei Bitcoin?

**Da es keinen Dritten gibt, entstehen häufig Fragen über die verschiedenen Möglichkeiten, die bei der Non-Custodial-Bitcoin-Speicherung zur Verfügung stehen. Hierbei gibt es zwei Hauptoptionen: Hot Wallets und Cold Wallets.**

Hot Wallets sind Online-Software, mit der Benutzer Bitcoins auf eine sehr einfache Weise speichern und senden bzw. empfangen können. Konten von Kryptowährungsbesitzern können als eine Art von Hot Wallet angesehen werden.

Demgegenüber werden Cold Wallets offline gespeichert – in der Regel auf einem physikalischen Medium – und bieten ein höheres Mass an Sicherheit. Ledger ist zweifellos der bekannteste Anbieter von Cold Wallets. Weitere Optionen sind u. a. Trezor, KeepKey und CoolWallet S.

# Bitcoin Nodes

## Was sind Bitcoin Nodes?

Bitcoin Nodes lassen sich als bestimmte Arten von Programmen definieren, die mit der Bitcoin-Blockchain in Interaktion treten. Da diese Nodes fortlaufend miteinander kommunizieren, kann Bitcoin als komplett dezentralisierte Kryptowährung fungieren, weil die Einhaltung aller definierten Regeln sichergestellt ist.

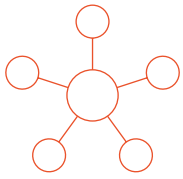
Full Nodes, Light Nodes und Mining Nodes sind die drei wichtigsten Arten von Nodes im Bitcoin-Netzwerk.

### FULL NODES

Diese Nodes stehen im Mittelpunkt der Bitcoin-Dezentralisierung. Von Full Nodes werden Transaktionen und deren Blöcke hochgeladen und überprüft.

### LIGHT NODES

Im Vergleich zu Full Nodes verfügen Light Nodes über eingeschränkte Möglichkeiten. Sie erfordern aber auch weniger Ressourcen. Mit ihrer Hilfe können Benutzer ihre Transaktion in einem bestimmten Block lokalisieren.



### MINING NODES

Mining Nodes lassen sich als Full Nodes beschreiben, die zusätzlich über die Mining-Fähigkeit und damit die Möglichkeit zur Block-Produktion verfügen. Diese Nodes validieren Transaktionen, bevor sie sie an andere Nodes weiterleiten.

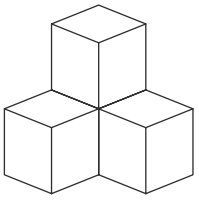
# Bitcoin-Halbierung

## Was bedeutet Bitcoin-Halbierung?

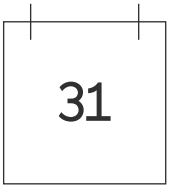
Bitcoin-Halbierung bedeutet, dass die übliche Belohnung, die Miners für die Überprüfung von Bitcoin-Transaktionen erhalten, durch zwei geteilt wird. Dies geschieht immer dann, wenn 210'000 Bitcoins geschaffen wurden. In der Regel passiert dies alle vier Jahre.

| | | **Block-Belohnung für Miners nach der Halbierung** |
|---|---|---|
| **Januar 2009** | Bitcoin-Auflegung | 50 BTC |
| **November 2012** | 1. Bitcoin-Halbierung | 25 BTC |
| **Juli 2016** | 2. Bitcoin-Halbierung | 12.5 BTC |
| **Mai 2020** | 3. Bitcoin-Halbierung | 6.25 BTC |
| **2024** | 4. Bitcoin-Halbierung | 3.125 BTC |
| **2028** | 5. Bitcoin-Halbierung | 1.5625 BTC |

**Erfolgt etwa alle 4 Jahre**



**Ein bedeutendes Ereignis zur Regulierung des Bitcoin-Angebots**




**Die nächste Halbierung erfolgt etwa am 18. Mai 2020**

## Warum kommt es zur Bitcoin-Halbierung?

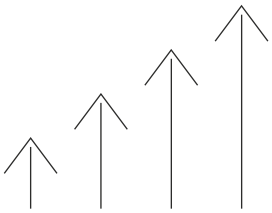
Die Bitcoin-Halbierung ist in der Blockchain-Software verankert und hat direkte Konsequenzen für Miners. Miners spielen eine wesentliche Rolle, denn ihre Tätigkeit ermöglicht die Überprüfung jeder Bitcoin-Transaktion.

**Transaktionen werden in Form von Blöcken überprüft. Sobald ein Block von Transaktionen überprüft wurde, erhält ein Miner eine Belohnung in Form einer Anzahl von neuen Bitcoins. Derzeit und bis zur nächsten Halbierung erhält ein Miner 12.5 BTC für jeden überprüften Block. Nach der nächsten Halbierung wird diese Belohnung halbiert.**

Bitcoin-Halbierungen erfolgen, bis das maximale Angebot von 21 Millionen Bitcoins erreicht ist. Voraussichtlich wird dies etwa im Jahr 2140 der Fall sein. Danach werden Miners immer noch Transaktionsgebühren erhalten, damit für sie weiterhin Anreize zur Überprüfung von Bitcoin-Transaktionen bestehen.

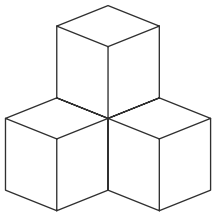
## Halbierungen und Bitcoin-Kursentwicklung

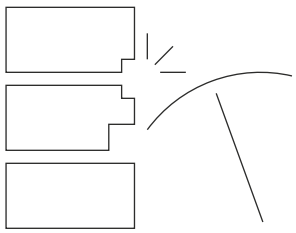
## Bitcoin-Halbierung



**SIn der Vergangenheit kam es einen Monat vor der Halbierung und in der Zeit nach der Halbierung zu einem deutlichen Anstieg der Bitcoin-Kurse.** Bisher sind die Bitcoin-Kurse noch nie unter den Wert gefallen, den sie vor der letzten Halbierung hatten. Dies lässt sich durch vielerlei Faktoren erklären, u. a. die erhöhte Aufmerksamkeit gegenüber Bitcoins und die automatische Verminderung des Angebots neuer Bitcoins.

**Die Halbierung ist eine unveränderliche, im Voraus festgelegte geplante Reduzierung der geschaffenen Bitcoins, die etwa alle 4 Jahre stattfindet, bis die maximale Anzahl an Bitcoin-Einheiten erzeugt wurde.** Auf diese Weise wird die Bitcoin-Inflation kontrolliert.





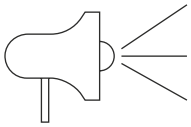
**Es lässt sich absehen, dass eine bestimmte Anzahl von Miners ihre Tätigkeit möglicherweise einstellt, weil sich die Block-Belohnung um 50% verringert und sie hierdurch ihre Rechen- und Energiekosten nicht abdecken können.** Dies dürfte jedoch keine Auswirkung auf die Geschwindigkeit haben, mit der Transaktionen überprüft werden, da die Schwierigkeit bei der Überprüfung von Transaktionen von der Software nahtlos angepasst wird.

# Bitcoin-Transaktionen

Wie funktioniert eine Bitcoin-Transaktion in der Praxis?

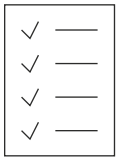
**Beispiel: Vanessa will 10 BTC an Chad senden**

1



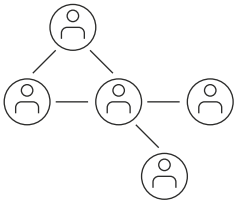
Vanessa informiert das Miners-Netzwerk, dass sie 10 BTC an Chad senden will. Sie liefert die Adresse von Chad, ihre persönliche Signatur und den öffentlichen Schlüssel, damit die Miners ihre Identität bestätigen können.

2



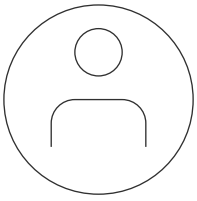
Die Miners vergewissern sich, dass sich die Überprüfung der Transaktion für sie lohnt. Dann stellen sie sicher, dass die 10 BTC Vanessa gehören und dass die Transaktion gültig ist – bevor sie diese in einen Block setzen.

3



Der Miner gibt die Informationen an das gesamte Miners-Netzwerk weiter, sodass die Miners ihre Gültigkeit überprüfen können, und alle fügen sie zu ihrer Kopie ihrer Blockchain hinzu.

4



Chad empfängt die 10 BTC, die ihm Vanessa gesendet hat.

**Automatisierte Identitätsprüfung**

**Keine Abhängigkeit von einer zentralen Gegenpartei**

**Verbesserte und permanente Rückverfolgbarkeit**

# Forks

## Was sind Bitcoin Forks?

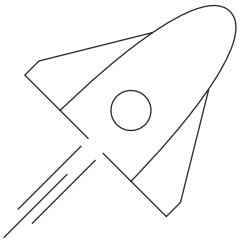
Forks sind für das Bitcoin-Protokoll das Gleiche wie Updates für die verschiedenen Computer-Software-Programme, die wir im täglichen Leben verwenden. In der Tat bieten Bitcoin-Forks die Möglichkeit, verschiedene Probleme des Protokolls zu beheben sowie dessen Möglichkeiten und Performance weiter zu verbessern.

**Das Bitcoin-Protokoll definiert die Regeln für das Funktionieren der Kryptowährung, die alle Nodes des Netzwerks befolgen müssen (z. B. die Grösse eines Blocks). Von daher kann jeder Fork erhebliche Konsequenzen auf die Art und Weise haben, wie Bitcoins funktionieren.**

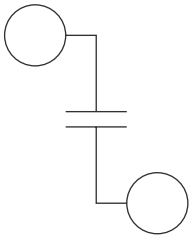
## Was ist ein Soft Fork?

Es gibt zwei Arten von Forks: Soft Forks und Hard Forks. Ein Soft Fork ist im Grunde eine Änderung des Bitcoin-Protokolls, wobei dieses mit seinen Vorgängerversionen kompatibel bleibt.

**In der Praxis bedeutet dies, dass ältere Nodes (also Nodes, die schon vor dem Fork existierten und nicht aktualisiert wurden) nach wie vor Transaktionen verarbeiten können, solange sie die neuen Regeln, die durch den Fork aufgestellt wurden, nicht verletzen. Nebenbei bemerkt, entscheiden sich ältere Nodes auch bei Soft Forks in der Regel zu Updates, da sie dann im Allgemeinen effizienter arbeiten können.**



**Für Benutzer bequemer, da keine Notwendigkeit zu einem Upgrade besteht**



**Geringere Wahrscheinlichkeit einer Aufspaltung der Kette**

## Was ist ein Hard Fork?

**Ein Hard Fork ist ebenfalls eine Änderung des Bitcoin-Protokolls, mit der Ausnahme, dass ältere Nodes, die kein Update auf die neueste Version des Protokolls durchführen, ihre Tätigkeit nicht weiter fortsetzen können.**

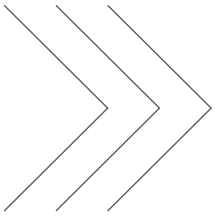
## Die beiden wichtigsten Arten von Hard Forks

### Geplante Hard Forks

Die überwiegende Mehrheit der Nodes nimmt freiwillig ein Update auf die neueste Version vor. Im Prinzip wird dadurch die ältere Version (also die alte Kette) aufgegeben. Hier verbleibt dann nur noch eine geringe Anzahl von Teilnehmern.

### Kontroverse Hard Forks

Üblicherweise geschieht dies, wenn in der Community Uneinigkeit über das Upgrade herrscht, und führt im Allgemeinen zur Bildung von zwei separaten Blockchains (also einer Spaltung der Kette) und damit zur Entstehung von zwei unabhängigen Kryptowährungen.



**Hard Forks ermöglichen deutlich grössere Spielräume, da keine Kompatibilität mit den Regeln der Vorgängerversionen gewährleistet werden muss**

### Der Bitcoin Hard Fork, aus dem Bitcoin Cash entstand

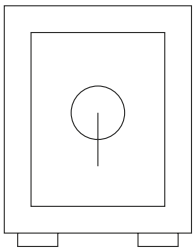
**Dieser Hard Fork ereignete sich im August 2017, da die Community geteilter Ansicht in der Frage war, wie Probleme im Zusammenhang mit der Bitcoin-Skalierbarkeit geregelt werden sollten. Da ein Fork immer auf der ursprünglichen Blockchain basiert, erhielten alle Bitcoin-Besitzer zum Zeitpunkt des Forks die gleiche Menge von Bitcoin Cash-Einheiten.**

# Proof-of-Work-Algorithmen

## Blockchain-Konsens

Wie bereits erwähnt, ist der Konsens eines der beiden Hauptmerkmale der Blockchain. Die Blockchain kann in der Regel Konsens durch 2 Arten von Algorithmen herbeiführen: Proof of Stake (PoS) und Proof of Work (PoW). Die Bitcoin-Blockchain nutzt PoW.

Das ursprüngliche Ziel von PoW-Algorithmen bestand darin, DoS-Attacken («Denial of Service») abwehren zu können. DoS-Attacken stören in der Regel den Zugang von Personen zu Netzwerken, indem sie die Netzwerke überlasten oder durch andere schädigende Transaktionen einen Netzwerkzusammenbruch herbeiführen.



**Durch die Nutzung von Proof-of-Work-Algorithmen würde eine erfolgreiche Attacke auf die Bitcoin-Blockchain enorme Rechenleistungen erfordern und wäre überaus zeitaufwendig. Ausserdem schrecken die hiermit verbundenen hohen Kosten von einem solchen Angriff ab.**

## Wie funktionieren Proof-of-Work-Algorithmen?

Damit ein Block zu der Bitcoin-Blockchain hinzugefügt werden kann, konkurrieren Miners über ihre Rechenleistung miteinander um die Lösung komplexer mathematischer Probleme (d. h. Erzeugung eines Hashs). Miners senden dann ihre Lösung an andere Nodes (Miners) im Netzwerk, damit diese prüfen, ob die Lösung richtig ist.

Jeder dieser Blöcke trägt einen Block-Hash, der im Prinzip die von den Minern geleistete Arbeit – also den Proof of Work – darstellt. Ein böswilliger externer Akteur, der die Bitcoin-Blockchain hacken will, müsste einen Ledger erzeugen, der länger als der vorhandene Ledger ist (mit allen Blöcken von Beginn an), was eine nahezu unerreichbare Rechenleistung erfordern würde.

# Zusammenfassung

## Die populärste Kryptowährung

Bitcoin ist 2009 entstanden und die bislang bekannteste Kryptowährung. Ziel war hierbei, ein elektronisches Peer-to-Peer-Bargeld für das Internet zu schaffen, das vollständig dezentralisiert ist und keine Zentralbank und keine vertrauenswürdigen Dritten für den Betrieb erfordert – so der Urton.

## Bitcoin wird durch Blockchain unterstützt

Die Kryptowährung wird durch Blockchain unterstützt, die ihr viele Funktionsmerkmale wie z. B. Unveränderlichkeit oder verbesserte Sicherheit und Rückverfolgbarkeit verleiht.

## Bitcoin wird ständig verbessert

Da das Bitcoin-Protokoll quelloffen ist, leistet eine grosse Community umfangreiche Beiträge zur Bitcoin-Entwicklung.

## Die Zukunft von Bitcoin

Aufgrund ihres begrenzten Angebots (21 Millionen Bitcoin-Einheiten) werden Bitcoins oft als das «digitale Gold» bezeichnet. Etwa 90% der Bitcoins wurden bisher geschaffen. Doch aufgrund der Bitcoin-Halbierungen dürften noch weitere 100 Jahre vergehen, bevor alle Bitcoins geschaffen sind. Aufgrund der Knappheit von Bitcoins und der Schwierigkeit, Bitcoins zu erzeugen, sowie der hohen Liquidität von Bitcoins sehen viele unabhängige Beobachter in der Kryptowährung einen sicheren Hafen und ein Instrument, dessen Wert im Laufe der Zeit steigen wird.

# ETHEREUM (ETH)

## Aktueller Handel

Ethereum ist im Jahr 2015 entstanden und wird oft als das «MS Windows» unter den Kryptowährungen bezeichnet. Ethereum wird zur Entwicklung von dezentralisierten Applikationen genutzt. Die zugehörige Kryptowährung – Ether – ist die zweitgrösste Kryptowährung am Markt.

Der Erfinder von Ethereum – Vitalik Buterin – hat das Konzept der «Smart Contracts» entwickelt. Das sind Programme, die in der Blockchain ausgeführt werden.

**KENNZAHLEN (STAND: 25. MÄRZ 2020)**

| Crypto | Ranking | Markt-kapitalisierung | Aktueller Kurs |
|---|---|---|---|
| ETH | Nr. 2 | EUR 14 Mrd. | EUR 123.16 |

### Kursdiagramm


**Quelle:** CoinMarketCap

# Allgemeine Aspekte

## Was ist Ethereum?

Ether und Bitcoin sind beides hinreichend bekannte Kryptowährungen. Der wesentliche Unterschied zwischen den beiden besteht darin, dass Ethereum **Smart Contracts** und die Entwicklung von **dezentralisierten Applikationen (dApps)** ermöglicht.

## Dezentralisierte Applikationen

Während es sich bei Bitcoins in der Hauptsache um ein System zur Überweisung von Geld handelt, dem eine Blockchain zugrunde liegt, verfolgt Ethereum ein anders Ziel, und zwar **Entwickler in die Lage zu versetzen, dezentralisierte Applikationen (sogenannte dApps) in seiner Blockchain zu erstellen und zu veröffentlichen.** Viele andere bei Swissquote verfügbare Kryptowährungen wie z. B. EOS, Chainlink oder Tezos bieten ebenfalls die Möglichkeit, dApps zu entwickeln und zu nutzen …

**Smart Contracts werden voraussichtlich ebenfalls mehrere Komplexitäten lösen, die sich Akteuren beim Wertpapierhandel, beim Clearing und bei der Abrechnung, bei der Abwicklung von Versicherungsansprüchen oder auch beim Management von Dokumenten in der Lieferkette stellen.**

## Ether – die Kryptowährung

Ethereum lässt sich als dezentralisierte Software-Plattform definieren und Ether als die hierzu gehörige Kryptowährung. **Von daher ist Ether nicht nur eine handelbare Kryptowährung, sondern wird auch von Entwicklern für die Bezahlung verschiedener Dienstleistungen verwendet, die im Ethereum-Netzwerk erbracht werden – beispielsweise der Betrieb oder die Monetisierung von Applikationen.**

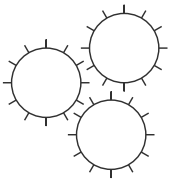
**Ether kann man sich sowohl durch den Handel an Börsen als auch durch Mining beschaffen.** Anders als bei Bitcoin erfordert das Mining von Ether keine industriellen Kapazitäten, da hierbei das dezentralisierte Mining durch Personen mit Proof-of-Work-Algorithmen gefördert wird (komplexe mathematische Probleme, die gelöst werden müssen, um die Bildung eines Blocks zu bestätigen).

# Smart Contracts

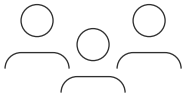
## Was ist ein Smart Contract?

Einfach ausgedrückt, lassen sich Smart Contracts als selbst ausführende digitale Verträge beschreiben. Genauer gesagt, handelt es sich um Computer-Code, der die Übertragung von Werten, Inhalten oder Eigentum erleichtern soll. **Das wesentliche Merkmal von Smart Contracts besteht darin, dass sie diese Eigentumsübertragung oder jede andere Transaktion ermöglichen, die sie nur dann unterstützen, wenn bestimmte im Voraus definierte Bedingungen erfüllt sind.** Dadurch können sichere Transaktionen zwischen unbekannten Dritten und mit einer beispiellosen Ausführungsgeschwindigkeit erfolgen.

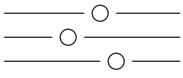
**Öffentlich im Ledger verfügbar**



**Automatische Ausführung von bestimmten Transaktionen und Transfers**



**Erfordert keine Einschaltung eines Mittelsmanns**



**Vollständig individuell anpassbar**

**VORTEILE**

- Sorgt für mehr Sicherheit bei traditionell durchgeführten Verträgen
- Reduziert die Transaktionskosten
- Gewährleistet komplette Sicherheit, selbst mit unbekannten Dritten

## Ethereum Virtual Machine (EVM)

**Die EVM wird oft als die zentrale Schlüsselinnovation von Ethereum bezeichnet. Es handelt sich hierbei um eine Software, die die Entwicklung und Ausführung von Blockchain-gestützten Applikationen auf möglichst effiziente Weise gestattet und diese gegen alle Interferenzen mit anderen Programmen in der Blockchain schützt.**

# LITECOIN (LTC)

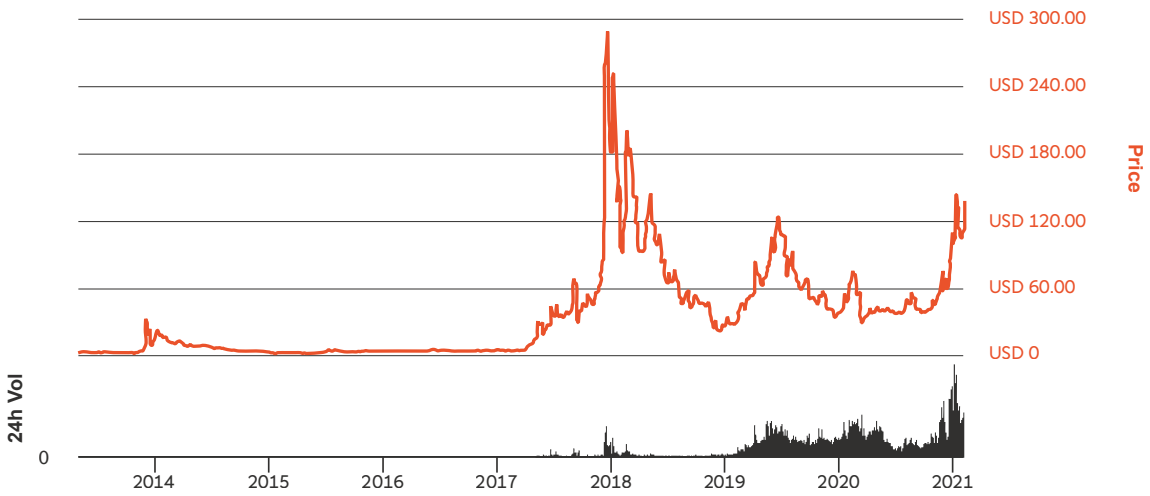
## Aktueller Handel

Litecoin wurde im Jahr 2011 durch Charlie Lee, einen ehemaligen Google-Ingenieur, entworfen und ist eine der ersten Kryptowährungen, die eingeführt wurden. Das Hauptziel lautete hierbei, eine digitale Währung zu schaffen, die für die alltägliche Verwendung besser geeignet ist als Bitcoin.
Litecoin beruht auf dem gleichen quelloffenen Code wie Bitcoin. Ihr wesentlicher Vorteil liegt darin, dass mit dem Litecoin-Code alle 2.5 Minuten ein Block generiert werden kann – statt 10 Minuten wie bei Bitcoin.

**KENNZAHLEN (STAND: 25. MÄRZ 2020)**

| Crypto | Ranking | Markt-kapitalisierung | Aktueller Kurs |
|---|---|---|---|
| LTC | Nr. 7 | EUR 2.3 Mrd. | EUR 35.78 |

### Kursdiagramm



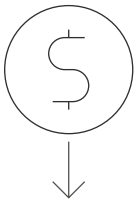

**Quelle:** CoinMarket Cap

# Allgemeine Aspekte

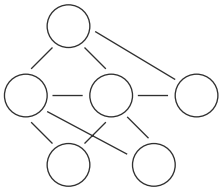
## Worin unterscheidet sich Litecoin von Bitcoin?

**Litecoin ist eine Kryptowährung, die aus einem Fork des Bitcoin Core Client resultierte. In der Praxis bedeutet dies, dass Litecoin auf der anfänglichen quelloffenen Code-Basis von Bitcoin beruht, zu der ihre Entwickler neue Funktionsmerkmale ergänzt haben. Von daher basiert Litecoin ebenfalls auf der Blockchain-Technologie und stützt sich auf ein vollständig dezentralisiertes System.** Allerdings wurden neue Funktionsmerkmale entwickelt, um die Zielsetzung von Litecoin zu erfüllen, nämlich Probleme zu lösen, für die Bitcoin nicht ausgelegt ist.

**4x schnellere Transaktionsgeschwindigkeit**



**Günstigere Transaktionen**



**Anderer Mining-Algorithmus**

## Schnelle und beinahe kostenlose Transaktionen

**Während Bitcoin ebenso wie Bitcoin Cash beide auf den Proof-of-Work-Algorithmus setzen, nutzt Litecoin Skrypt. Dieser Algorithmus scheint eine demokratischere Mining-Methode im Vergleich zum SHA-256-Algorithmus von Bitcoin zu sein.** Tatsächlich ist Skrypt weniger prozessorintensiv als SHA-256, weil der Algorithmus nicht zu einer höheren Mining-Schwierigkeit führt, die das Mining nur für Miners mit starker Rechenleistung zugänglich macht. **Der Skrypt-Algorithmus führt bei Litecoin zu einer drastischen Reduzierung der Transaktionskosten.**

## Ähnlichkeiten mit Bitcoin

Genau wie bei Bitcoin ist das Angebot von Litecoin beschränkt. Das schützt die Kryptowährung vor Inflation und hilft, ihren Wert zu erhalten. Litecoin-Transaktionen werden genau wie Bitcoin-Transaktionen überprüft – durch Miners, die für jeden bestätigten Transaktionsblock eine Belohnung erhalten. Und genau wie bei Bitcoin wird die Belohnung von Miners nach jeder Halbierung durch zwei geteilt (die nächste Halbierung erfolgt voraussichtlich im Jahr 2023).

# RIPPLE (XRP)

## Aktueller Handel

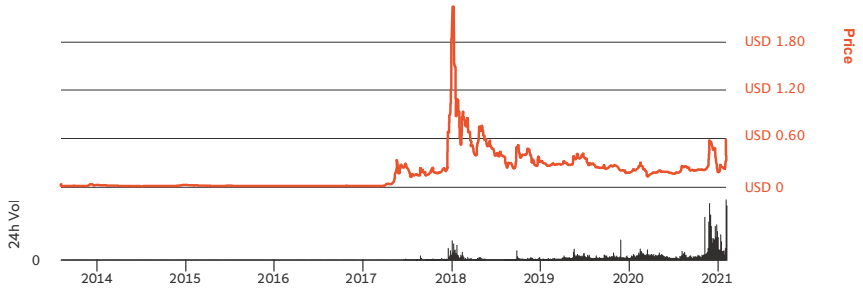
Ripple ermöglicht ultraschnelle Transaktionen (ca. 4 Sekunden) und bietet besonders niedrige Transaktionsgebühren in Verbindung mit einem skalierbaren Netzwerk. Das zentralisierte Echtzeitabrechnungssystem von Ripple kann rund 1'500 Transaktionen/Sekunde verarbeiten.

Das wesentliche Merkmal von XRP ist das Netzwerk, das XRP unterstützt und das als Börse angesehen werden kann, die Zahlungen zwischen Banken und anderen Finanzinstitutionen erleichtert.

**KENNZAHLEN (STAND: 25. MÄRZ 2020)**

| Crypto | Ranking | Markt-kapitalisierung | Aktueller Kurs |
|---|---|---|---|
| XRP | Nr. 3 | EUR 7.0 Mrd. | EUR 0.16 |

## Kursdiagramm




**Quelle:** CoinMarketCap

## Kurzer Rückblick

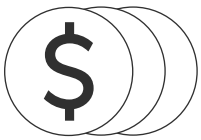
**2004** – Erster Ripple-Prototyp als dezentralisiertes digitales Zahlungssystem (RipplePay)

**2012** – Gründung von OpenCoin, ein Technologieunternehmen mit Schwerpunkt Zahlungslösungen für Finanzinstitutionen

**2015** – Offizielle Umfirmierung von Ripple Labs (ex-OpenCoin) in Ripple

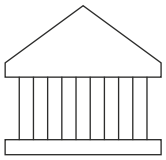
# Allgemeine Aspekte

## Hauptfunktionsmerkmale von Ripple



**Umtauschbar in alle Währungen**

**Transaktionen in weniger als 4 Sekunden abgewickelt**



**Entwickelt für Finanzinstitutionen**

## XRP Ledger

XRP Ledger (XRPL)

→ **Quelloffenes verteiltes System, das sofortige Finanztransaktionen,** die Speicherung von Abrechnungsdetails und Währungsumtauschdienste bietet.

→ **Konsens wird durch den proprietären Konsensalgorithmus von Ripple erreicht,** der durch ein Netzwerk von validierenden unabhängigen Nodes durchgesetzt wird.

→ **Ripple-Kunden haben Zugriff auf eine Liste vertrauenswürdiger Nodes (UNL), die sich allesamt auf den aktuellen Ledger-Status einigen müssen.** Deswegen beruht die Überprüfung von Ripple-Transaktionen nicht auf Mining.

## Kryptowährung für Finanzinstitutionen

Ripple ist die erste Kryptowährung, die sich gezielt an Banken und Finanzinstitutionen richtet. **Ziel von Ripple ist die Lösung von Problemen, die Banken und Finanzinstitutionen durch Liquiditätsbeschränkungen in Verbindung mit möglichen Wechselkursschwankungen haben, und eine hohe Abrechnungsgeschwindigkeit (4 Sekunden im Vergleich zu 2-3 Tagen bei traditionellen Zahlungssystemen). Gleichzeitig soll durch den Einsatz der Blockchain hohe Sicherheit geboten werden.**

# BITCOIN CASH (BCH)

## Aktueller Handel

Bitcoin Cash entstand durch den Bitcoin Fork im August 2017. Genau wie Bitcoin handelt es sich um ein elektronisches Peer-to-Peer-Bargeld für das Internet. Bitcoin Cash ist vollständig dezentralisiert ohne Zentralbank und erfordert keine vertrauenswürdigen Dritten für den Betrieb (Urton).

Hinter der Schaffung von Bitcoin Cash stand die Idee, schnelle, beinahe sofortige Transaktionen zu ermöglichen und die mit Bitcoin in Zusammenhang stehenden hohen Transaktionskosten zu senken. Infolgedessen kann Bitcoin Cash von Privatpersonen bei kleinen alltäglichen Transaktionen verwendet werden, was bei Bitcoin nicht der Fall ist.

**KENNZAHLEN (STAND: 25. MÄRZ 2020)**

| Crypto | Ranking | Markt-kapitalisierung | Aktueller Kurs |
|---|---|---|---|
| BCH | Nr. 5 | EUR 3.8 Mrd. | EUR 204.55 |

### Kursdiagramm


**Quelle:** CoinMarketCap

### Ursprünge von Bitcoin Cash

Bitcoin Cash ist im Jahr 2017 durch einen Hard Fork von Bitcoin entstanden. Die Blockchain von Bitcoin Cash wurde geändert, indem die Grösse eines Transaktionsblocks auf 8 bis 32 MB erhöht wurde – statt 1 MB wie bei Bitcoin.

# Allgemeine Aspekte

## Höhere Skalierbarkeit und niedrigere Gebühren

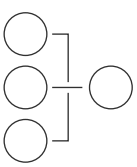
**Transaktionsverarbeitungskapazitäten**


Durch die wesentliche Vergrösserung der Blöcke verfolgt die neue Blockchain-Version von Bitcoin Cash das Ziel, Probleme im Zusammenhang mit den höheren Transaktionskosten zu lösen, mit denen einige Bitcoin-Nutzer konfrontiert waren.

**Die Blockchain von Bitcoin Cash verringert die Zeit, die Transaktionen für ihren Weg in einen Block benötigen, ohne dass Anreize für Miners in Form einer höheren Transaktionsgebühr notwendig sind. Deswegen scheint sich Bitcoin Cash besser für Mikrozahlungen zu eignen und ermöglicht dem Netzwerk, selbst in Zeiten hoher Aktivität eine Überlastung zu verhindern.**

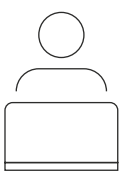
Dank seiner grösseren Blockgrösse kann Bitcoin Cash Minern ausserdem höhere Belohnungen für das Mining eines Blocks bieten, da der Block aus mehr Transaktionen besteht.

## Gemeinsamkeiten mit Bitcoin

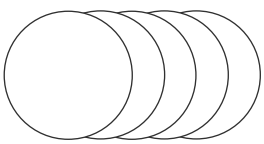


**Blockchain-basiert**

**Quelloffener Code**



**Proof-of-Work-Algorithmus**



**Begrenztes Angebot (21 Millionen Coins)**

# DIE NÄCHSTEN SCHRITTE – EINSTIEG IN DEN HANDEL MIT SWISSQUOTE

1

Gehen Sie zu **swissquote.com/trading**

2

Eröffnen Sie ein Demo-Konto.

3

Sie können das Trading mit
CHF 10'000 an virtuellem Geld üben.
Kein Risiko und keine Verpflichtung.

**Probieren Sie jetzt ein Demo-Konto aus!**

## Überzeugende Gründe für den Handel bei Swissquote?

- 20 Jahre Erfahrung im Online-Trading
- Zugang zu 3 Millionen Produkten an den wichtigsten internationalen Börsen
- Umfassendste Trading-Plattform auf dem Markt
- Mehrsprachiger Kunden-Support
- Training und Schulungen mit Online-Webinaren
- Leistungsstarke mobile Anwendungen
- Internationale Gruppe, kotiert an der SIX Swiss Exchange (SIX:SQN)

## Swissquote wird regelmässig von Finanzmedien in aller Welt zitiert und konsultiert.

Bloomberg

CNBC

FINANZ und WIRTSCHAFT

LE TEMPS

Investing.com

Neue Zürcher Zeitung

swissquote.com/crypto-assets/education