Cryptowährungen, digitale Währung

BitCoin  
Ethereum

Ziel ist eine verteilte, dezentrale und sichere digitale Währung.

# Prinzipien

1. verteilt: die Informationen wer wieviel Geld hat, bzw wieviel im Umlauf ist, sind verteilt auf viele Benutzer
2. dezentral: es steckt keine Bank, Zentralbank, Regierung, … dahinter, eine einzelne Institution kann die Produktion der Währungsmenge nicht beeinflussen
3. sicher: wird erreicht durch kryptografische Verfahren
4. digital: existiert nur als digitales Zahlungsmittel, es gibt keine Banknoten, Schecks,…
5. Informationen zum Geldfluss werden in einer eigenen Speicherform, der Blockchain gespeichert.
6. Es gibt fast 5000 digitale Währungen, die Marktkapitalisierung zB vom Bitcoin ist derzeit ca 150Mrd $
7. Die Blockchain kann aber auch zum Speichern anderer Informationen, als Geld, verwendet werden

# Blockchain bzw distributed ledger Technologien

Distributed ledger: verteiltes Kontobuch

Teilnehmer einigen sich auf ein Art der Verwaltung des Kontobuchs und tragen dort ihre Infos ein.  
Das Kontobuch ist für alle (viele) zugänglich, jeder hat eine Kopie des Buches. Einzutragende Infos können von der Gemeinsamkeit für gültig erklärt werden. Wenn sie für gültig erklärt wurden, bleiben sie permanent und nicht mehr änderbar im Kontobuch und alle Kontobuchbesitzer aktualisieren ihr Buch mit dem neuen Eintrag.  
Es muss bei den Einträgen nicht um Geld gehen, die Infos können auch Verträge, Zustände eines Systems, Infos von Personen, Trackingstationen eines Produkts usw. sein.

## Idee der Blockchain

Die chain besteht aus miteinander verbundenen Blöcken. Blöcke enthalten Transaktionen (oder allgemeine Infos). Es gibt mehrere Teilnehmer, die eine Kopie der chain besitzen. Die Teilnehmer sind mit einem peer to peer Netzwerk miteinander verbunden. Soll von einem Teilnehmer ein Block mit einer neuen Transaktion an die chain angehängt werden, werden alle anderen Teilnehmer darüber informiert. Diese können den neuen Block akzeptieren (über einen definierten Konsensalgorithmus), dann hängen sie ihn auch an ihre chain an. Die chain besteht also aus Blöcken, wobei jeder Block mit seinem Vorgänger und seinem Nachfolger (falls vorhanden) verknüpft ist. Der Urblock (also der erste Block) hat eine eigene Stellung im System

Jeder Block hat üblicherweise zumindest folgende Informationen

1. Blocknummer
2. Zeitstempel
3. Transaktionen (oder irgendwelche Informationen)
4. Hash des Vorgängerblocks
5. Hash der aktuellen Blocks (also der Infos 1 bis 4)

Da jeder Block den Hash des Vorgängerblocks enthält, und dieser wieder den seines Vorgängers usw, sind alle Blöcke miteinander verknüpft. Würde irgendein Block verändert, würde sich sein Hashwert ändern und somit auch der des Nachfolgers usw.. Um einen Block zu fälschen müsste man auch alle seine Nachfolger ändern. Nachdem aber viele Teilnehmer eine Kopie der chain haben würde das sofort auffallen.

## Gültigkeit eines Blocks bestätigen

**Proof of Work**

Beim Bitcoin durch mining und proof of work (Variieren einer nonce bis hashwert bestimmte Bedingung erfüllt), miner der die Rechenaufgabe schafft, bekommt eine Belohnung fürs Rechnen

Andere Konsensalgorithmen sind  
**Proof of Stake**: Durch ein Zufallsverfahren wird festgelegt, wer den Block bestätigen darf. Das Verfahren verwendet „Gewichte“ aus Teilnhmedauer und Vermögen

**Delegated proof of Stake**: es wird „gewählt“ wer den nächsten Block bestätigen darf

## Beispiel Bitcoins:

Es gibt fünf Möglichkeiten, Bitcoins zu bekommen:

1. Bitcoins über eine Börse kaufen.
2. Bitcoins als Bezahlung für Waren oder Dienstleistungen akzeptieren.
3. Bei Bitcoin-Händlern gegen Bargeld tauschen  
     
   oder Rechnen:
4. Selber einen neuen Block erzeugen (selber Rechnen, bringt derzeit 25 Bitcoins).
5. Sich an einem Mining-Pool beteiligen (also Rechenleistung zur Verfügung stellen).

### Erzeugung von Bitcoins:

Neue Bitcoins werden jedes Mal generiert, wenn ein Netzwerk-Knoten die Lösung zu einem bestimmten, schwer lösbaren mathematischen Problem findet (d.h. einen neuen Block erstellt), was einen sog. Proof-of-Work darstellt. Die Belohnung für die Lösung eines Blocks wird automatisch angepasst, so dass in den ersten vier Jahren des Bitcoin Netzwerkes 10.500.000 BTC geschaffen wurden. Der Betrag wird alle vier Jahre halbiert, so dass in den darauffolgenden vier Jahren 5.250.000 Bitcoins erstellt werden, danach 2.625.000 und so weiter. Auf diese Weise nähert sich die Gesamtzahl an Bitcoins über die Zeit etwa 21.000.000 an (wird ca im Jahr 2140 erreicht, die Blocknummer ist dann 6.929.999.

Es ist ein System in das Netzwerk integriert, das versucht im Durchschnitt alle 10 Minuten einen Block mit neuen Münzen irgendwo im Netzwerk zu vergeben. Mit der sich ändernden Zahl an Menschen, die versuchen Münzen zu generieren, ändert sich auch die Schwierigkeit, neue Münzen zu schaffen. Die Schwierigkeit wird vom gesamten Netzwerk vereinbart, und zwar basierend auf der Zeit, die für die Schaffung der letzten 2016 Blöcke benötigt wurde. Sie ist daher auf die durchschnittliche Rechenleistung bezogen, die über die Zeit eingesetzt wurde um diese letzten Blöcke herzustellen. Die Wahrscheinlichkeit, dass jemand einen dieser Blöcke "entdeckt" ist also abhängig von der Leistung des verwendeten Computers im Vergleich zur Leistung aller Computer im Netzwerk, die ebenfalls versuchen Blöcke zu generieren.

## Rechenaufgabe um Bitcoins zu berechnen:

Grundlage ist sha-256 (sha bedeutet secure hash algorithm)  
aus einem Datensatz wird ein Hashwert berechnet, aus dem hashwert kann man aber den Datensatz nicht herstellen. Kollisionsfreiheit heißt dabei , dass nicht zwei „sinnvolle“ Datensätze den gleichen Hashwert erzeugen können.  
Bei sha 256 (256 weil der hashwert 256 Bits hat) wird der originale Datensatz nacheinander in Blöcke zu je 512 Bits zerlegt und jeder Block wird iterativ mit Konstanten mathematisch verknüpft, wobei die Konstanten aus den Nachkommastellen der Wuzeln von Primzahlen berechnet werden.

Ca alle 10 Minuten wird ein neuer Block erzeugt. Ein Block besteht aus der Transaktionsliste (die ist am Anfang leer) und dem Blockheader, im Blockheader steht eine Zufallsszahl und die Referenz auf den vorhergehenden, zuletzt erzeugten Block.  
Beim Minen setzt der Miner in der Transaktionliste die eigene Adresse (seinen public key) ein und variiert die (64–stellige) Zufallszahl solange, bis der sha-256 Hashwert des gesamten Blocks ein bestimmtes Kriterium erfüllt. Das Kriterium besteht darin, dass eine bestimmte Anzahl an Nullen am Beginn des Hashwert stehen muss (eigentlich muss er kleiner sein als ein vorgegebener Wert, der selber immer kleiner wird, so dass es immer schwieriger wird durch Zufall einen noch kleineren Hashwert zu finden).  
Wenn man eine passende Zufallszahl gefunden hat, kann man den Block veröffentlichen, die Gemeinschaft prüft ob das mit dem Hashwert stimmt (das geht ja einfach), wenn ja gehört der Block dem der die passende Zufallszahl gefunden, er bekommt derzeit 12,5 Bitcoins gutgeschrieben.

Immer wenn 2016 Blöcke erzeugt wurden wird geprüft, wie lange das gedauert hat, wenn es zu schnell war, wird die Schwierigkeit (die Anzahl der geforderten 0en im Hashwert) erhöht oder erniedrigt, so dass im Durchschnitt wieder alle 10 Minuten ein Block erzeugt wird, egal wieviel Rechnepower weltweit ins Probieren gesteckt wird.

## Handeln mit Bitcoins

Der Erzeuger des Blocks ist am Anfang Besitzer der Bitcoins.  
Wenn Bitcoins den Besitzer wechseln wird dies in der Transaktionliste vermerkt. Vermerkt werden Verkäufer, Käufer und Menge, wobei die Transaktionsdaten mit dem private key des Verkäufers verschlüsselt werden. Dadurch kann mit dem public key des Verkäufers die Transaktionsgültigkeit geprüft werden.

Anschließend wird ein neuer Block erzeugt, der selber wieder einen Hashwert eingetragen hat, der aus dem Hashwert im letzten Block und dem public key des neuen Benutzer erzeugt wird. Dieser neue Block wird an den alten angehängt (Block-Chain) und wieder zum Eintragen einer passenden Zufallszahl an die miner weitergegeben, diesmal aber mit einem einfacher zu lösenden Hashaufgabe, die in ca 10 Minuten lösbar sein sollte. Wenn sie gelöst ist wird sie verifiziert und der Block mit der passenden Zufallszahl wird als verifiziert an die Blockchain angehängt.

Wenn man also schauen will wieviele Bitcoins, ein einzelner Besitzer hat, muss man die gesamte Blockchain durchsuchen, die ist mittlerweile schon recht groß und hat 120GB.

Nochmal zur Erklärung:

Der Einfachheit halber steht jedesmal der public key des neuen Besitzers (des Käufers) im Block. Wenn dieser eine Transaktion startet (und das kann ja nur er, weil der der Besitzer ist), trägt er den public key des Käufers ein und verschlüsselt die Transaktion mit seinem private key. Dadurch wird das Überprüfen der Richtigkeit von Blocks sehr erleichtert, weil man dann einen Block mit dem publick key des Vorgängerblocks entschlüsseln kann. Wenn das passt, ist bestätigt, dass tatsächlich der Besitzer des Vorgängerblocks die Transaktion gemacht hat. Der neue Besitzer wird nun bei der nächsten Weitergabe seinen private key verwenden, um eine Transaktion zu verschlüsseln und wiederum den publick key des Käufers eintragen usw.

## Wallets

Sind digitale Brieftaschen, oder noch einfacher ein Behälter für Informationen, die an eine Adresse (irgendein Name) gebunden sind, wobe zum Signieren bzw Identifizeiren ein private-publick key Schlüsselpaar verwendet wird.

## Ethereum

Ziel von Ethereum ist die Dezentralisierung persönlicher Daten, basierend auf der Blockchain-Technologie von Bitcoin, die alle Transaktionen dezentral speichert. Die Währung des Systems ist Ether. Doch im Unterschied zu Bitcoin umfassen Ethereum-Transaktionen nicht nur Beträge, sondern komplette Programme, die dezentral in der Etherum Virtual Machine ausgeführt werden.

Astrakt betrachtet ist die Blockchain ein Protokoll, um nicht duplizierbare Datenbankeinträge dezentral und irreversibel zu übertragen. Das ist gut für Bargeld, wäre aber auch praktisch für Aktien, Bodenrechte, Konzertkarten, Gutscheine und jede andere Art von “Asset” oder “Token.” Da die Bitcoin-Blockchain das nicht “nativ” unterstützt, wurde bei Ethereum eine andere Scriptsprache erstellt, die das kann und die BlockChain universell einsetzbar macht (so dass also nicht nur eine Geldbetrag drinnen steht, sondern beliebige Daten)

## Dezentralisierter Marketplace

Insgesamt ist die Idee also, dass man den Besitz von Dingen (nicht nur Geld) weitergeben kann, die Weitergabe wird in der Blockchain verwaltet und protokolliert. Es ist nicht eine zentrale Stelle dafür verantwortlich, sondern das peer to peer Netzwerk prüft und bestätigt die Transaktionen.

## Anwendungsgebiete der Blockchain

Fehlt noch – guter Artikel ist

https://morethandigital.info/blockchain-moeglichkeiten-und-anwendungen-der-technologie/