Digitale Knappheit (double spending)

Wie verhindert Bitcoin Double-Spending?

1. **Blockchain & Konsensmechanismus**
   - Jede Bitcoin-Transaktion wird in der **Blockchain** gespeichert und kann nicht rückgängig gemacht werden.
   - Das Netzwerk überprüft ständig, ob Coins bereits ausgegeben wurden.
2. **Proof-of-Work (PoW) & Mining**
   - Miner validieren Transaktionen und fügen sie einem neuen Block hinzu.
   - Nur die längste gültige Blockchain wird akzeptiert – doppelte Transaktionen werden abgelehnt.
3. **Bestätigungen (Confirmations)**
   - Jede Transaktion benötigt **mehrere Blockbestätigungen**, bevor sie als sicher gilt.
   - Je mehr Bestätigungen, desto unwahrscheinlicher ist ein Double-Spend-Angriff.

Fazit:

Bitcoin löst das Double-Spending-Problem durch ein **dezentrales Netzwerk, Mining und die Blockchain**, sodass keine Transaktion doppelt ausgegeben werden kann.

Blockchain

Die **Bitcoin-Blockchain** ist ein **dezentrales, öffentliches Kassenbuch**, das alle Bitcoin-Transaktionen speichert.

Wie funktioniert sie?

1. **Blöcke**: Jede Transaktion wird in einem **Block** gespeichert.
2. **Mining & Verifizierung**: Miner validieren Blöcke durch das **Proof-of-Work**-Verfahren (SHA-256).
3. **Verkettung**: Jeder Block enthält den Hash des vorherigen Blocks → **unveränderliche Kette**.
4. **Dezentral**: Kopien der Blockchain werden auf Tausenden von **Nodes** gespeichert.
5. **Transparenz & Sicherheit**: Jeder kann sie einsehen, aber sie kann nicht manipuliert werden.

Die Blockchain macht Bitcoin **fälschungssicher, transparent und dezentralisiert**.

SHA 256

SHA-256 (Secure Hash Algorithm 256-bit) ist eine kryptografische Hash-Funktion, die in Bitcoin für die Sicherung und Validierung von Transaktionen sowie das Mining verwendet wird. Sie wandelt Eingabedaten in eine 256-Bit lange, eindeutige Zeichenkette um. Wichtige Eigenschaften:

1. **Einweg-Funktion**: Der Hash kann nicht zurückgerechnet werden.
2. **Deterministisch**: Gleiche Eingaben erzeugen immer denselben Hash.
3. **Kollisionsresistenz**: Es ist praktisch unmöglich, zwei unterschiedliche Eingaben mit demselben Hash zu finden.
4. **Mining**: SHA-256 wird im Proof-of-Work-Verfahren genutzt, um Blöcke zu validieren.

Transaktionen

Eine **Bitcoin-Transaktion** überträgt BTC von einer Adresse zu einer anderen.

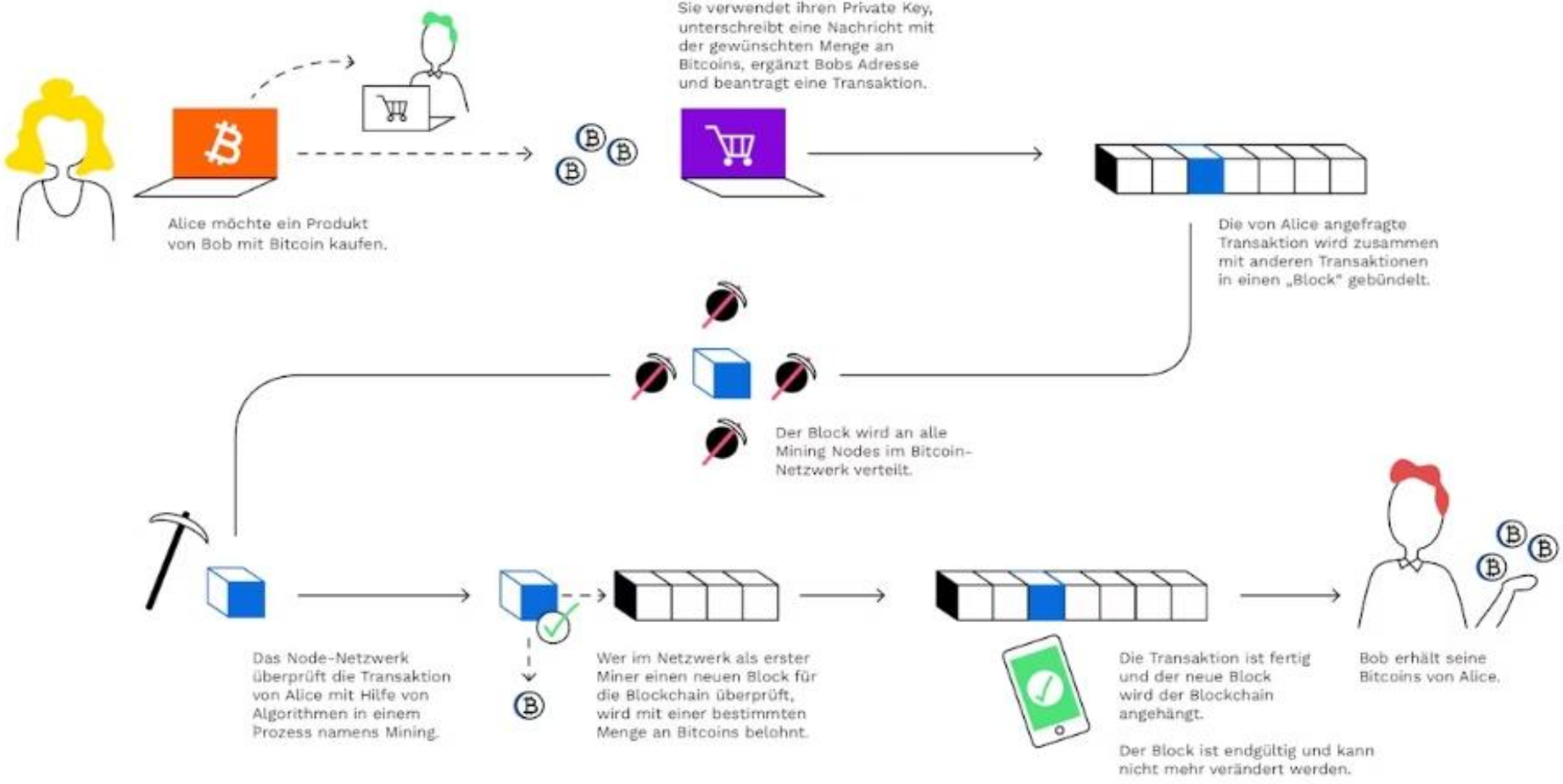
Wie funktioniert sie?

1. **Eingaben (Inputs)**: Verwendet vorher erhaltene BTC.
2. **Ausgaben (Outputs)**: Sendet BTC an eine neue Adresse.
3. **Signatur**: Der **Private Key** signiert die Transaktion zur Authentifizierung.
4. **Mempool**: Die Transaktion wartet auf Bestätigung durch Miner.
5. **Mining & Bestätigung**: Miner nehmen sie in einen Block auf.
6. **Blockchain**: Sobald sie in einem Block ist, gilt sie als bestätigt.

Je mehr **Bestätigungen**, desto sicherer ist die Transaktion!

Was ist Bitcoin Mining?

Der Ablauf einer Bitcoin-Transaktion



NODES

Bitcoin-Nodes sind Computer, die das Bitcoin-Netzwerk betreiben und absichern. Sie speichern die gesamte Blockchain, validieren Transaktionen und Blöcke und leiten diese an andere Nodes weiter. Es gibt verschiedene Arten von Nodes:

1. **Full Nodes**: Speichern die gesamte Blockchain und validieren alle Transaktionen selbstständig. Sie sind essenziell für die Sicherheit des Netzwerks.
2. **Light Nodes (SPV-Nodes)**: Laden nur relevante Block-Header und verlassen sich auf Full Nodes zur Verifizierung.
3. **Mining Nodes**: Sind mit Mining-Software verbunden und versuchen, neue Blöcke zu finden.
4. **Pruned Nodes**: Speichern nur einen Teil der Blockchain, um Speicherplatz zu sparen.

Full Nodes sind besonders wichtig, da sie das Bitcoin-Netzwerk dezentral und sicher halten.

Public Key & Private Key

Bitcoin nutzt ein **Public-Private-Key-Paar** für Sicherheit und Transaktionen:

- **Private Key**: Eine **geheime** Zahl, die den Besitz von Bitcoins sichert. Er wird zum **Signieren** von Transaktionen verwendet und darf **niemals** weitergegeben werden.
- **Public Key**: Wird aus dem Private Key abgeleitet und kann **öffentlich** sein. Er wird zur Erstellung von **Bitcoin-Adressen** genutzt und ermöglicht die **Verifizierung** von Transaktionen.

🔑 **Private Key** = Kontrolle über BTC (geheim)
🔓 **Public Key** = Empfang & Verifikation (öffentlich)

Transaktionen werden mit dem **Private Key** signiert, und das Netzwerk prüft sie mit dem **Public Key**.

Mining

Bitcoin-Mining ist der Prozess, bei dem neue Bitcoins erstellt und Transaktionen verifiziert werden. Es basiert auf dem **Proof-of-Work (PoW)**-Mechanismus und nutzt leistungsstarke Computer, um komplexe mathematische Rätsel (SHA-256-Hashing) zu lösen.

Wie funktioniert es?

1. **Transaktionsverarbeitung**: Miner bündeln Bitcoin-Transaktionen in einem neuen Block.
2. **Rätsel lösen**: Sie suchen eine **Nonce** (Zahl), die den Block-Hash unter eine bestimmte Schwelle bringt.
3. **Block hinzufügen**: Der erste Miner, der das Rätsel löst, sendet den Block ins Netzwerk.
4. **Belohnung erhalten**: Der erfolgreiche Miner erhält die **Block Reward** (neue Bitcoins + Transaktionsgebühren).

Warum ist Mining wichtig?

- **Sichert das Netzwerk** gegen Manipulation.
- **Validiert und speichert** Transaktionen in der Blockchain.
- **Schafft neue Bitcoins** (bis das Limit von 21 Mio. erreicht ist).

Mining

Wie geht es dann weiter?

1. **Einnahmen durch Transaktionsgebühren**
   - Miner verdienen nur noch an den **Fees**, die Nutzer für Transaktionen zahlen.
   - Falls die Nachfrage hoch bleibt, könnten diese Gebühren lukrativ genug sein.
2. **Netzwerksicherheit**
   - Solange genug Transaktionen stattfinden und Gebühren gezahlt werden, bleibt das Mining attraktiv.
   - Falls Gebühren zu niedrig sind, könnte die Mining-Leistung sinken, was das Netzwerk langsamer und potenziell unsicherer macht.
3. **Bitcoin als Wertaufbewahrung**
   - Da kein neues Angebot mehr dazukommt, könnte Bitcoin knapper und wertvoller werden.
   - Höherer Bitcoin-Wert könnte Miner auch mit geringeren Mengen an Gebühren belohnen.
4. **Alternative Lösungen?**
   - **Layer-2-Lösungen wie das Lightning-Netzwerk** könnten effizientere Zahlungen ermöglichen.
   -

21 Millionen

Warum genau 21 Millionen?

1. **Knappheit & Werterhalt**
   - Bitcoin soll digitales **Gold** sein, mit begrenztem Angebot.
   - Verhindert Inflation, wie sie bei Fiat-Währungen vorkommt.
2. **Mathematische Logik**
   - Die Belohnung für Miner **halbiert sich alle 210.000 Blöcke** (ca. alle 4 Jahre).
   - Start: **50 BTC pro Block**, dann 25, 12.5, 6.25 … bis fast 0 BTC bleibt.
   - Summe aller Belohnungen ergibt **max. 21 Mio. BTC**.
3. **Nachhaltigkeit & Sicherheit**
   - Sobald alle BTC gemined sind (ca. 2140), verdienen Miner durch **Transaktionsgebühren**.
   - Erhält langfristig das Netzwerk aufrecht.

Durch diese Begrenzung bleibt Bitcoin **wertvoll, deflationär und resistent gegen Manipulation**.

HALVING

Bitcoin Halving ist ein Ereignis, bei dem die **Block-Belohnung** für Miner halbiert wird. Es findet etwa alle **4 Jahre (alle 210.000 Blöcke)** statt und reduziert die Menge neuer Bitcoins, die ins Netzwerk kommen.

Warum passiert das?

- **Begrenztes Angebot**: Bitcoin hat ein Maximum von **21 Millionen Coins**.
- **Inflationsschutz**: Weniger neue Bitcoins bedeuten eine langsamere Angebotsausweitung.
- **Steigende Knappheit**: Geringeres Angebot kann langfristig den Preis beeinflussen.

Letzte Halvings:

1. **2012** → Belohnung von **50 BTC auf 25 BTC**
2. **2016** → **25 BTC auf 12,5 BTC**
3. **2020** → **12,5 BTC auf 6,25 BTC**
4. **2024** → **6,25 BTC auf 3,125 BTC**

Das Halving macht Bitcoin **seltener** und stärkt seine Rolle als digitales **Wertaufbewahrungsmittel**.

Ära	Bis Jahr (Schätzung!)	Subvention	Anzahl Blöcke pro Ära	Supply pro Ära	Supply Gesamt
1	2012	50	210000	10500000	10500000,00
2	2016	25	210000	5250000	15750000,00
3	2020	12,5	210000	2625000	18375000,00
4	2024	6,25	210000	1312500	19687500,00
5	2028	3,125	210000	656250	20343750,00
6	2032	1,5625	210000	328125	20671875,00
7	2036	0,78125	210000	164062,5	20835937,50
8	2040	0,390625	210000	82031,25	20917968,75
9	2044	0,1953125	210000	41015,625	20958984,38
10	2048	0,09765625	210000	20507,8125	20979492,19
11	2052	0,04882812	210000	10253,9052	20989746,09
12	2056	0,02441406	210000	5126,9526	20994873,05
13	2060	0,01220703	210000	2563,4763	20997436,52
14	2064	0,00610351	210000	1281,7371	20998718,26
15	2068	0,00305175	210000	640,8675	20999359,13
16	2072	0,00152587	210000	320,4327	20999679,56
17	2076	0,00076293	210000	160,2153	20999839,77
18	2080	0,00038146	210000	80,1066	20999919,88
19	2084	0,00019073	210000	40,0533	20999959,93
20	2088	0,00009536	210000	20,0256	20999979,96
21	2092	0,00004768	210000	10,0128	20999989,97
22	2096	0,00002384	210000	5,0064	20999994,98
23	2100	0,00001192	210000	2,5032	20999997,48
24	2104	0,00000596	210000	1,2516	20999998,73
25	2108	0,00000298	210000	0,6258	20999999,36
26	2112	0,00000149	210000	0,3129	20999999,67
27	2116	0,00000074	210000	0,1554	20999999,83
28	2120	0,00000037	210000	0,0777	20999999,91
29	2124	0,00000018	210000	0,0378	20999999,94
30	2128	0,00000009	210000	0,0189	20999999,96
31	2132	0,00000004	210000	0,0084	20999999,97
32	2136	0,00000002	210000	0,0042	20999999,97
33	2140	0,00000001	210000	0,0021	20999999,98
34	2144	0	210000	0	20999999,98
35	2148	0	210000	0	20999999,98

Mempool.space

Mempool.space ist ein **visuelles Block-Explorer-Tool**, das Echtzeit-Daten zur Bitcoin-Blockchain und zum **Mempool** anzeigt.

Hauptfunktionen:

- **Mempool-Überwachung**: Zeigt ausstehende Transaktionen vor der Bestätigung.
- **Fee-Analyse**: Empfiehlt optimale Transaktionsgebühren basierend auf Netzwerkauslastung.
- **Blockchain-Explorer**: Detaillierte Ansicht von Blöcken, Transaktionen und Adressen.
- **Lightning-Netzwerk**: Anzeige von Nodes und Kanälen im Bitcoin-Lightning-Netzwerk.

Es hilft Nutzern, die beste **Fee für schnelle Bestätigungen** zu wählen und gibt **transparente Einblicke** in das Bitcoin-Netzwerk.

mempool .space

Erkunde das ganze Bitcoin Ökosystem

~1 sat/vB	~1 sat/vB	~1 sat/vB	~2 sat/vB	~3 sat/vB	~6 sat/vB
1 - 1 sat/vB	1 - 1 sat/vB	1 - 1 sat/vB	1 - 3 sat/vB	2 - 4 sat/vB	4 - 402 sat/vB
0,01 BTC	**0,01 BTC**	**0,011 BTC**	**0,019 BTC**	**0,034 BTC**	**0,082 BTC**
42 Transaktionen	107 Transaktionen	1.355 Transaktionen	2.213 Transaktionen	2.987 Transaktionen	3.571 Transaktionen
In ~57 Minuten	In ~47 Minuten	In ~38 Minuten	In ~28 Minuten	In ~19 Minuten	In ~9 Minuten

882331	882330	882329	882328	882327	882326
~2 sat/vB	~3 sat/vB	~5 sat/vB	~2 sat/vB	~4 sat/vB	~5 sat/vB
2 - 23 sat/vB	3 - 79 sat/vB	3 - 453 sat/vB	2 - 57 sat/vB	3 - 178 sat/vB	4 - 276 sat/vB
0,025 BTC	**0,042 BTC**	**0,063 BTC**	**0,025 BTC**	**0,051 BTC**	**0,066 BTC**
1.544 Transaktionen	2.125 Transaktionen	3.228 Transaktionen	2.024 Transaktionen	3.262 Transaktionen	3.688 Transaktionen
Vor 46 Minuten	Vor 47 Minuten	Vor 54 Minuten	Vor 78 Minuten	Vor 79 Minuten	Vor 90 Minuten
Foundry USA	ViaBTC	SpiderPool	Foundry USA	F2Pool	Foundry USA

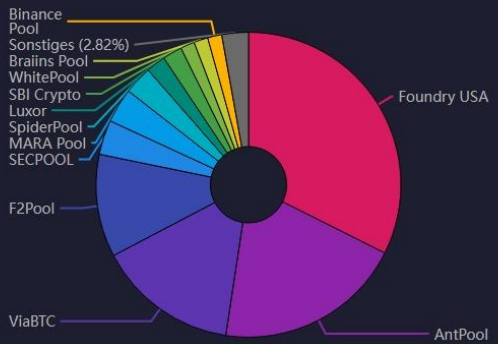
BELOHNUNGSSTATISTIKEN (144 BLÖCKE)

Miner-Belohnung	Durchschn. Blockg...	Durchschn. TX Ge...
455,75 BTC	0.0399 BTC/Block	1.65k sats/tx
44.558.020 $	3.906 $	1,62 $

SCHWIERIGKEITSANPASSUNG

Verbleibend	Schätzung	Nächste Halbieru...
677 Blöcke	▲ 5,15 %	14.04.2028
In ~4 Tage	Vorherige: ▼ 2,12 %	In ~3 Jahre, 69 Tage

Poolglück	Blöcke (1w)	Anzahl der Pools
105.56%	1064	22



Hashrate (1w)	Schwierigkeit
818.5 EH/s	108.11T

mempool .space

Erkunde das ganze Bitcoin Ökosystem

~1 sat/vB	~1 sat/vB	~2 sat/vB	~3 sat/vB	~4 sat/vB	~5 sat/vB
1 - 1 sat/vB	1 - 1 sat/vB	1 - 2 sat/vB	2 - 3 sat/vB	3 - 4 sat/vB	4 - 81 sat/vB
0,01 BTC	**0,011 BTC**	**0,018 BTC**	**0,029 BTC**	**0,039 BTC**	**0,061 BTC**
97 Transaktionen	1.286 Transaktionen	2.221 Transaktionen	1.888 Transaktionen	2.850 Transaktionen	3.919 Transaktionen
In ~57 Minuten	In ~47 Minuten	In ~38 Minuten	In ~28 Minuten	In ~19 Minuten	In ~9 Minuten

882333	882332	882331	882330	882329	882328
~7 sat/vB	~9 sat/vB	~2 sat/vB	~3 sat/vB	~5 sat/vB	~2 sat/vB
6 - 282 sat/vB	7 - 400 sat/vB	2 - 23 sat/vB	3 - 79 sat/vB	3 - 453 sat/vB	2 - 57 sat/vB
0,077 BTC	**0,126 BTC**	**0,025 BTC**	**0,042 BTC**	**0,063 BTC**	**0,025 BTC**
3.260 Transaktionen	3.081 Transaktionen	1.544 Transaktionen	2.125 Transaktionen	3.228 Transaktionen	2.024 Transaktionen
Vor 11 Minuten	Vor 24 Minuten	Vor 2 Stunden	Vor 2 Stunden	Vor 2 Stunden	Vor 2 Stunden
AntPool	Foundry USA	Foundry USA	ViaBTC	SpiderPool	Foundry USA

TRANSAKTIONSGEBÜHR

Keine Priorität	Niedrige Priorität	Mittlere Priorität	Hohe Priorität
2 sat/vB	5 sat/vB	6 sat/vB	6 sat/vB
0,28 $	0,69 $	0,83 $	0,83 $

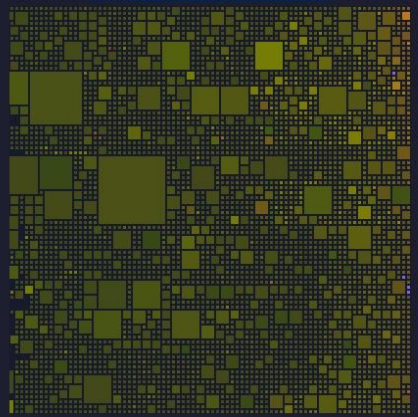
SCHWIERIGKEITSANPASSUNG

Schwierigkeit | Halving

~9.6 Minuten	▲ 4,76 %	In ~4 Tage
Durchschnittliche Blockzeit	Vorherige: ▼ 2,12 %	9. Februar um 13:21

Mempool Goggles™ : Alles

Alles | Konsolidierung | Coinjoin | Daten



Mindestgebühr	Speicherplatzverbrauch	Unbestätigt
1,00 sat/vB	40.1 MB / 300 MB	13.754 TX

Eingehende Transaktionen