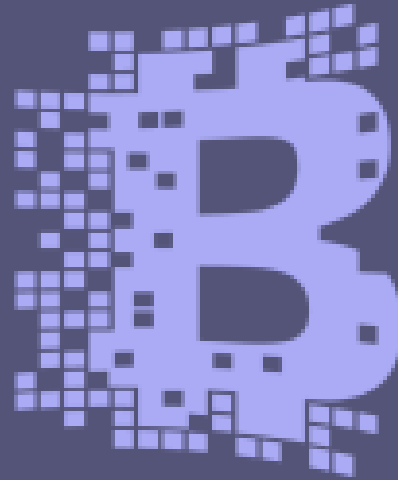




**BLOCKCHAIN**

# Blockchain: Der Wettlauf um die Technologie beginnt

**Startschuss** Blockchain könnte die Finanzwelt revolutionieren: Mit der Technologie sollen Geldströme sicher, schnell und günstig fließen. Die ganze Branche tüftelt an Blockchain - vorne dabei ist ein Zürcher.

[www.handelszeitung.ch/konjunktur/blockchain-der-wettlauf-um-die-technologie-beginnt-946047](http://www.handelszeitung.ch/konjunktur/blockchain-der-wettlauf-um-die-technologie-beginnt-946047)

If the Internet is the foundation for digital innovation of all kinds, blockchain technology is the underpinning of a radical rethinking of how we pay for things—as well as how we verify who owns what and who has the right to buy and sell it.

[www.pwc.com/us/en/financial-services/publications/viewpoints/assets/qa-what-is-blockchain.pdf](http://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/qa-what-is-blockchain.pdf)

# Revolutionäre Kette

Die Blockchain-Technologie wird die Finanzszene verändern. Wie genau, müssen die Schweizer Banken erst noch herausfinden. Viel Zeit bleibt ihnen dafür nicht.

[www.tagesanzeiger.ch/wirtschaft/geld/revolutionaere-kette/story/30544094](http://www.tagesanzeiger.ch/wirtschaft/geld/revolutionaere-kette/story/30544094)

## Digitale Goldgräber

Bitcoins genießen nicht den besten Ruf. Doch die Technologie dahinter könnte die Finanzbranche revolutionieren – und die Art, wie wir Verträge schließen und wie wir bezahlen.

[www.spiegel.de/spiegel/print/d-132909510.html](http://www.spiegel.de/spiegel/print/d-132909510.html)

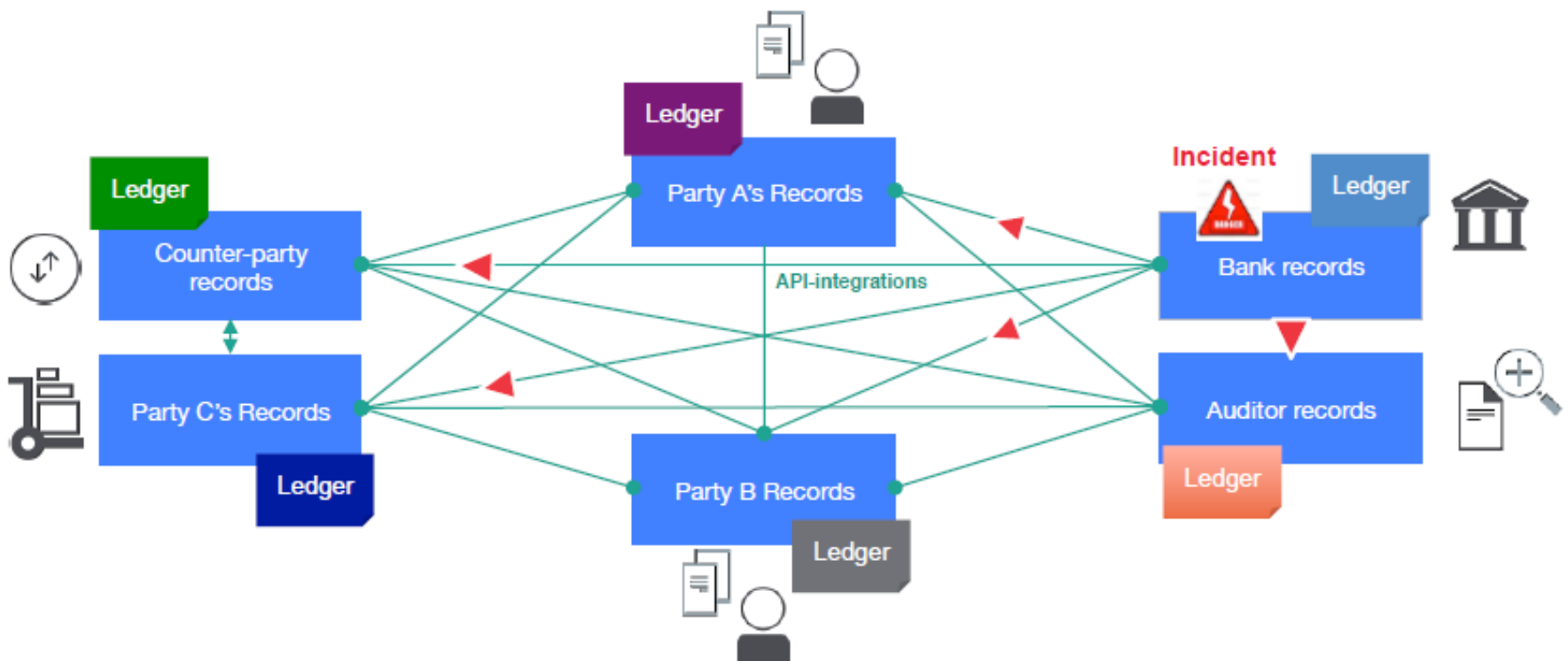
# Inhaltsverzeichnis

- Was ist Blockchain?
- Aufbau
- Was ist Bitcoin?
- Smart Contracts
- Einsatzgebiete

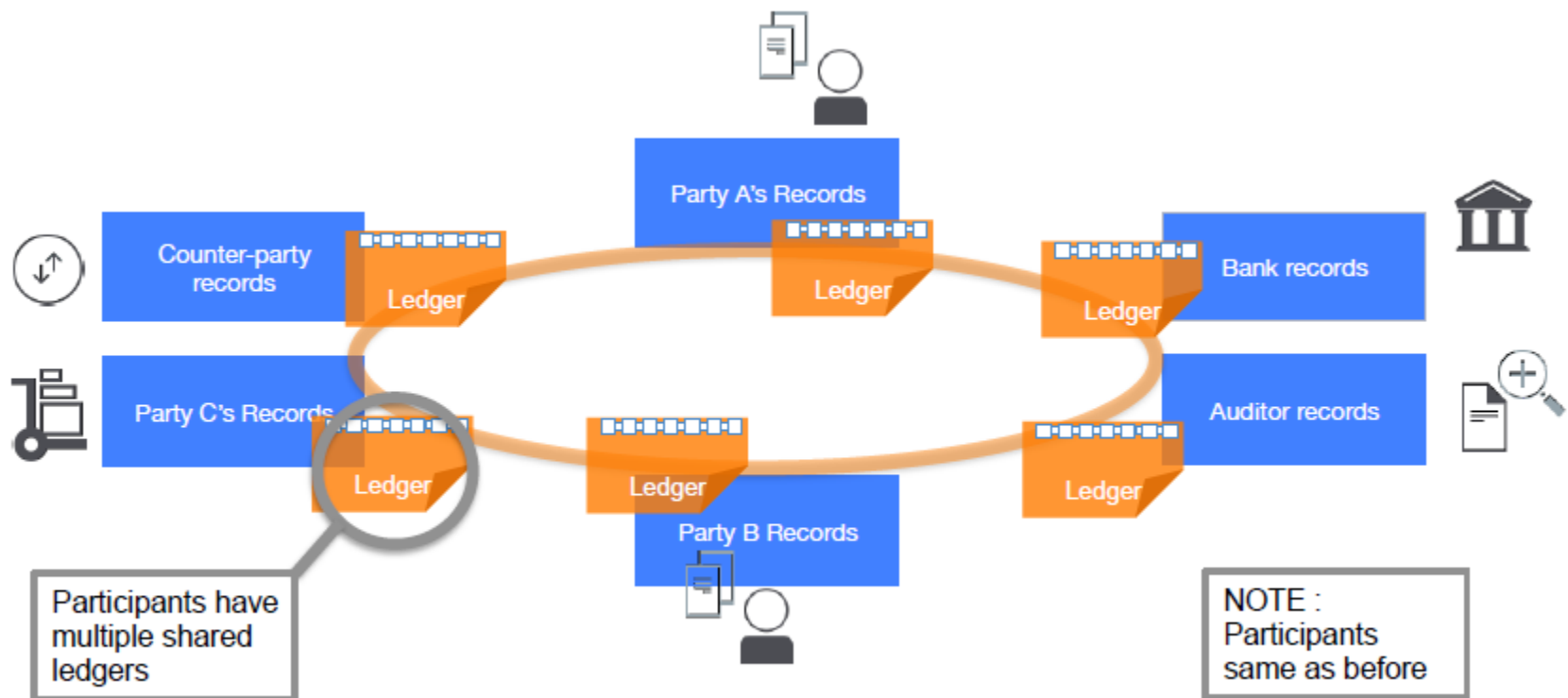
# Was ist Blockchain?

- Dezentralisiertes Register oder Liste aller Transaktionen in einem peer-to-peer Netzwerk.
- Transaktionen sind pseudoanonym
- Teilnehmer können beliebige Werte übers Internet transferieren (ohne zentrale Stelle)
- Ausführung von komplexen Operationen „Smart Contracts“

# Aufbau



# Aufbau



# Aufbau

- Transaktionen werden in einem sogenannten "Block" abgelegt.
- Ist ein Block voll wird ein neuer erzeugt und mit dem vorangehenden verlinkt
- Zur Sicherung gegen nachträgliche Manipulation wird eine Prüfsumme des vorangehenden Datensatzes hinzugefügt.
- Daten sind permanent und nicht änderbar und können durch jedermann verifiziert werden.

# Was ist Bitcoin?



Protocol für eine dezentrale, pseudo-anonyme, digitale, peer-to-peer Währung

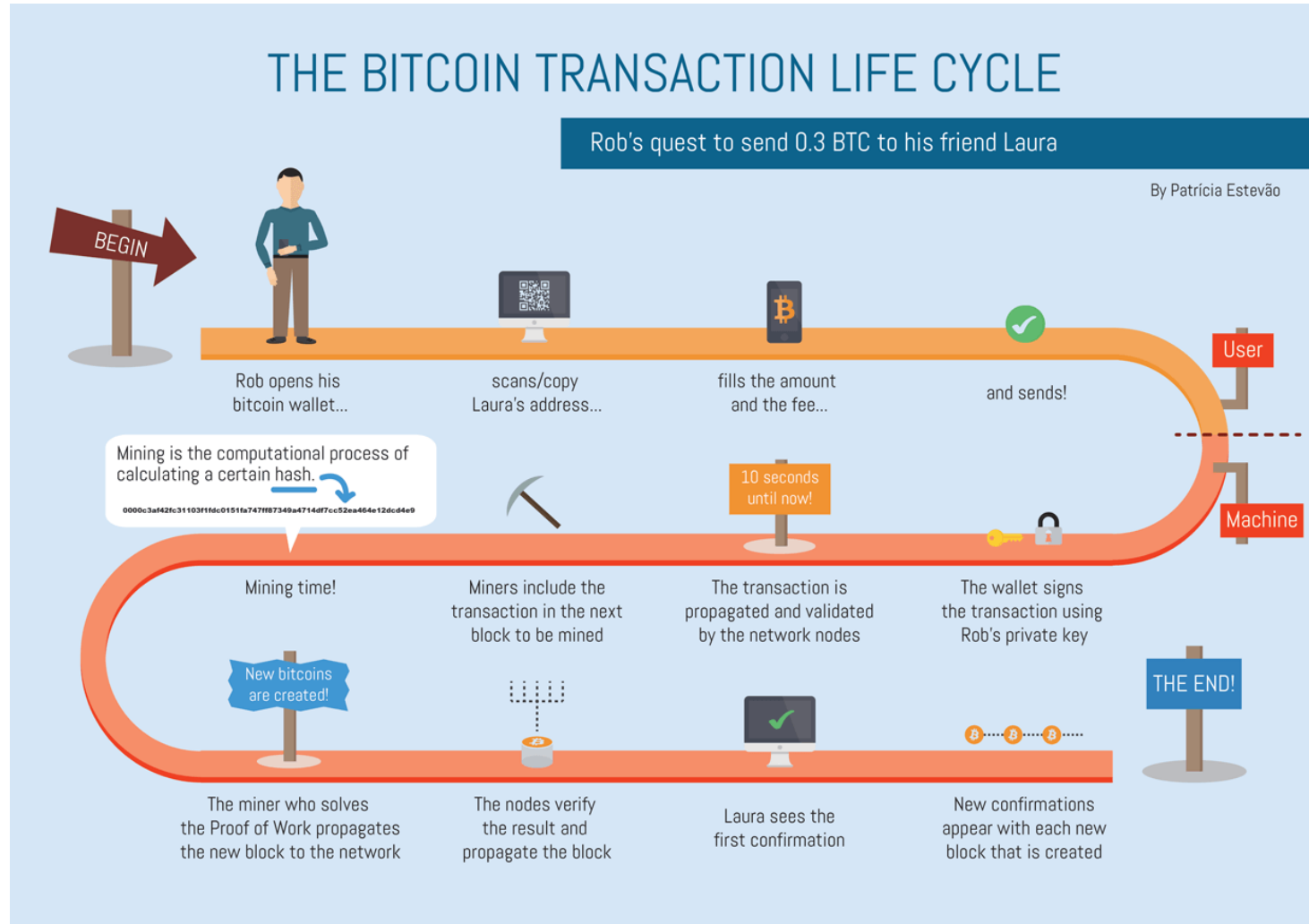
Öffentliches Register mit allen Transaktionen (Blockchain basierend)

Geringe Transaktionsgebühren

Deflationär d.h. der „Mining“ – Betrag wird alle 4 Jahre halbiert



# Überweisung von Bitcoins



# Proof of work

- „Proof of work“ stellt eine rechenintensive Aufgabe dar, welche sich jedoch leicht überprüfen lässt.
- Miners müssen einen Hash berechnen, bestehend aus allen Transaktionen, dem Hashwert des vorangehenden Blocks sowie einem sogenannten „Nonce“. (Bsp. 0000000000000000000000001b8ae144914353641d29f41793d73e7a16f8a53f879a31a)
- Bsp: Finde SHA-256 Hash mit „000“

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfd65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

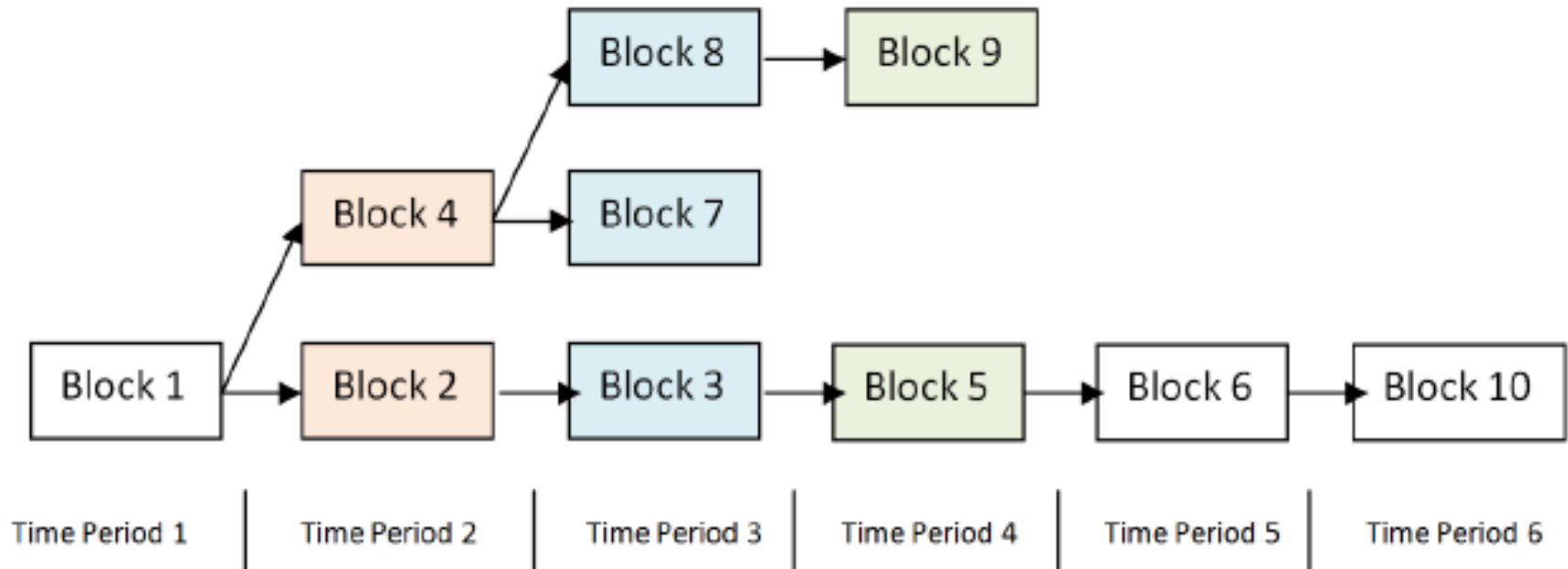
# Proof of work

- Der „Schwierigkeitsgrad“ einen Block zu finden wird regelmässig angepasst, abhängig von der verfügbaren Hash-Rechenpower
- Nur Hashwerte die kleiner als das aktuelle Target sind werden vom Netzwerk akzeptiert.
- Der erste Miner der den Hashwert berechnet gewinnt und die Aufgabe beginnt von neuem
- Für jede gelöste Aufgabe wird eine Belohnung bezahlt, zusätzlich können die einzelnen Transaktionen gebühren enthalten welche dem Aufgabenlöser gutgeschrieben werden.

# Reach a consensus

- Falls zwei Miner zur selben Zeit einen neuen Block hinzufügen kommt es zu einem Fork
- Der nächste Block entscheidet welcher Pfad gültig ist.
- Bitcoin Clients haben eine einfache Regel: "always trust the longest chain of blocks"
- Transaktionen von einem Blockchain Fork gehen in einen Cache mit unbestätigten Transaktionen
- Funktioniert solange ein Angreifer nicht mehr als 50% der Hash-Rechenpower kontrolliert

# Reach a consensus



# Reach a consensus

- Falls zwei Miner zur selben Zeit einen neuen Block hinzufügen kommt es zu einem Fork
- Der nächste Block entscheidet welcher Pfad gültig ist.
- Bitcoin Clients haben eine einfache Regel: "always trust the longest chain of blocks"
- Transaktionen von einem Blockchain Fork gehen in einen Cache mit unbestätigten Transaktionen
- Funktioniert solange ein Angreifer nicht mehr als 50% der Hash-Rechenpower kontrolliert

# Mining Hardware

- Anfangs wurden GPU's fürs Mining verwendet
- Heutzutage werden spezielle Hashing-Prozessoren sog. ASICs (Application-Specific Integrated Circuits) verwendet



14,000,000 Hashes/s

# Mining Hardware

## The Bitcoin network outperforms the top 500 supercomputers combined

By Grant Brunner on May 13, 2013 at 3:15 pm | [42 Comments](#)



For some, Bitcoin conjures ideas of a utopian decentralized currency, but many others these days think of it as a quick way to make a buck. Countless hordes of Bitcoin prospectors are now using their computers to “mine” for Bitcoins by solving for specific hashed values. Now, the processing power of these miners is being estimated to be six to

eight times greater than the top 500 supercomputers combined.

A Bitcoin-centric site called The Genesis Block recently broke down the data that shows just [how powerful the Bitcoin mining network actually is](#). The processing power estimates passed one exaflops ( $10^{18}$  floating-point operations per second) recently, and that is no small feat. [Sequoia](#), one of the world’s fastest supercomputers, is capable of 16.32 petaflops, but that’s only 1.6% of the estimated power of the Bitcoin mining network. As it turns out, the processing power of these computers dedicated to mining for Bitcoins is somewhere between six and eight times greater than all of the top 500 supercomputers combined.



# blockchain.info

 **BLOCKCHAIN**  
info

StartseiteChartsStatistikenMärkteAPIWallet

SucheDeutsch

## Startseite

Die aktuell gefundenen Blöcke in der Bitcoin Blockchain

Mehr ...

| Höhe   | Alter      | Transaktionen | Insgesamt gesendet | Weitergeleitet von        | Größe (kB) |
|--------|------------|---------------|--------------------|---------------------------|------------|
| 443261 | 15 minutes | 412           | 1,131.64 BTC       | <a href="#">HaoBTC</a>    | 998.09     |
| 443260 | 17 minutes | 345           | 1,326.50 BTC       | <a href="#">AntPool</a>   | 425.52     |
| 443259 | 18 minutes | 1204          | 6,431.77 BTC       | <a href="#">SlushPool</a> | 566.92     |
| 443258 | 25 minutes | 448           | 5,900.30 BTC       | <a href="#">BW.COM</a>    | 164.81     |
| 443257 | 27 minutes | 431           | 2,119.44 BTC       | <a href="#">SlushPool</a> | 172.44     |
| 443256 | 29 minutes | 1418          | 9,826.98 BTC       | <a href="#">BW.COM</a>    | 608.63     |

### Neueste Transaktionen

|                               |            |                |
|-------------------------------|------------|----------------|
| #526230b25e0284ac3c1ca85...   | < 1 minute | 1.22632957 BTC |
| e83481c8438f3791229f878bd...  | < 1 minute | 0.43268002 BTC |
| 31f2bab5ced68e724c727eca5...  | < 1 minute | 8.76325236 BTC |
| cfd1b11a10c13b5f9ae0b0c8a1... | < 1 minute | 1.39241097 BTC |
| 5ba8664a43c4b11754e3b8459...  | < 1 minute | 0.01208395 BTC |
| 9872be9e0ce78343098c77ce5...  | < 1 minute | 0.03233767 BTC |
| 9c17caeefc269ea4c321d29c4...  | < 1 minute | 1.01203441 BTC |
| fafdf2f6d328b313b2f763178...  | < 1 minute | 0.0392702 BTC  |
| 9c6eb83do8eed8b9d58e3d6d9...  | < 1 minute | 0.13159139 BTC |
| 88a496a032a14d88eee9207a7...  | < 1 minute | 0.01946057 BTC |

### Suchen

Hier können Sie nach Blockhöhe, Adresse, Blockhash, Transaktions-Hash, hash160 oder IPv4-Adresse suchen.

### NEWS

**Magnr - Bitcoin Trading Platform | Trade with Leverage**  
Magnr ← 1 minute vor  
Transactions right now 1.66 per second-----I can SPIT faster than that-----full blocks have to be banned to let bitcoin soar.  
/r/btc 8 minutes vor

**This Hedge Fund is Run by 7,500 Nameless, Blind Strangers**  
Bitcoinist 23 minutes vor  
Idea to add in "snapshot" state freeze blocks every 2 weeks.  
/r/bitcoin 51 minutes vor

**Blockchain "snapshots" to help with scaling**  
/r/btc 1 hour 8 minutes vor  
"Core discourages new (mining) competitors and directly contributes to the centralization of mining!" @John\_Blocke  
/r/btc 2 hours 8 minutes vor  
When you're thinking about all the stupid shit you bought at \$490...

17.12.2016

SGE

18

# blockchain.info

## Block #443262

### Zusammenfassung

|                                 |                           |
|---------------------------------|---------------------------|
| Anzahl der Transaktionen        | 438                       |
| Ausgang insgesamt               | 4,111.40595867 BTC        |
| Geschätztes Transaktionsvolumen | 427.0221545 BTC           |
| Transaktions Gebühren           | 0.20759702 BTC            |
| Height                          | 443262 (Hauptchain)       |
| Zeitstempel                     | 2016-12-13 08:00:19       |
| Empfangszeit                    | 2016-12-13 08:00:19       |
| Weitergeleitet von              | <a href="#">Telco 214</a> |
| Schwierigkeit                   | 288,765,766,820.55        |
| Bits                            | 402904457                 |
| Größe                           | 146.657 KB                |
| Version                         | 0x20000000                |
| Nonce                           | 3032497862                |
| Block Reward                    | 12.5 BTC                  |

### Hashes

|                  |                                                                  |
|------------------|------------------------------------------------------------------|
| Hash             | 000000000000000002e5025ea5e16c146c7f2bc298a588221686c1d572b086ce |
| Vorheriger Block | 0000000000000000036978f09921cc17c9737e46fd99d32fa2c7a9118b5c5329 |
| Nächster Block   |                                                                  |
| Merkle Root      | 57655dce0f50ff1e1290c18817f05e88a88bfb3d43175dd19c1349bf875a8a49 |

### Netzwerk Ausbreitung (Klicken um anzuzeigen)



## Transaktionen

[2f19c84a74aa43084e4f2057ed735e6a6b6b778b0f239a43bd88073d53753f29](#)

(Größe: 131 bytes) 2016-12-13 08:00:19

Keine Eingänge (neu erzeugter Münzen)



1DXRoTT87mCbhdHHL1i4J1xsSZHHnFxYR - (unverbraucht)

12.70759702 BTC

12.70759702 BTC

[e17e54ea2aa5720de112c6e5e2ea2a534bc8b2b8ba80cf2b0d0d71895151b3db](#)

(Gebühr: 0.01 BTC - Größe: 225 bytes) 2016-12-13 07:45:08



1JnLWfASkYbnyi3JmshVXUeZDHHWJrTILL - (unverbraucht)

0.01544516 BTC

# Vorteile

- Bitcoin-Netzwerk ist frei und unabhängig von Banken, Zahlungsdienstleistern oder staatlichen Regulierungsbehörden
- Bitcoin ist durch die automatische Überprüfung der Teilnehmer untereinander absolut fälschungssicher
- Bei Transaktionen mit Bitcoins fallen keine bzw. nur sehr niedrige Transaktionsgebühren an.
- Zwischen Bitcoinsender und Empfänger werden weder persönliche noch sensible Daten übertragen
- Keine Gefahr von Rückbelastungen

# Nachteile

- Eingebaute Deflation (begrenzt auf 21 Millionen)
- Geringe Akzeptanz in der Bevölkerung
- Wert schwankt stark, keine Wertgarantie
- Limitierte Blockgrösse (erlaubt derzeit nur 600000 Transaktionen/Tag)
- Hoher Energieverbrauch (900 Milliarden Berechnungen pro Aufgabe)
- Miner entscheiden über Aufnahme von Transaktionen in den Block (Verzögerung bestimmter Transaktionen)
- Mining-Pools erhöhen Gefahr das ein Miner 51% der Mining-Leistung besitzt

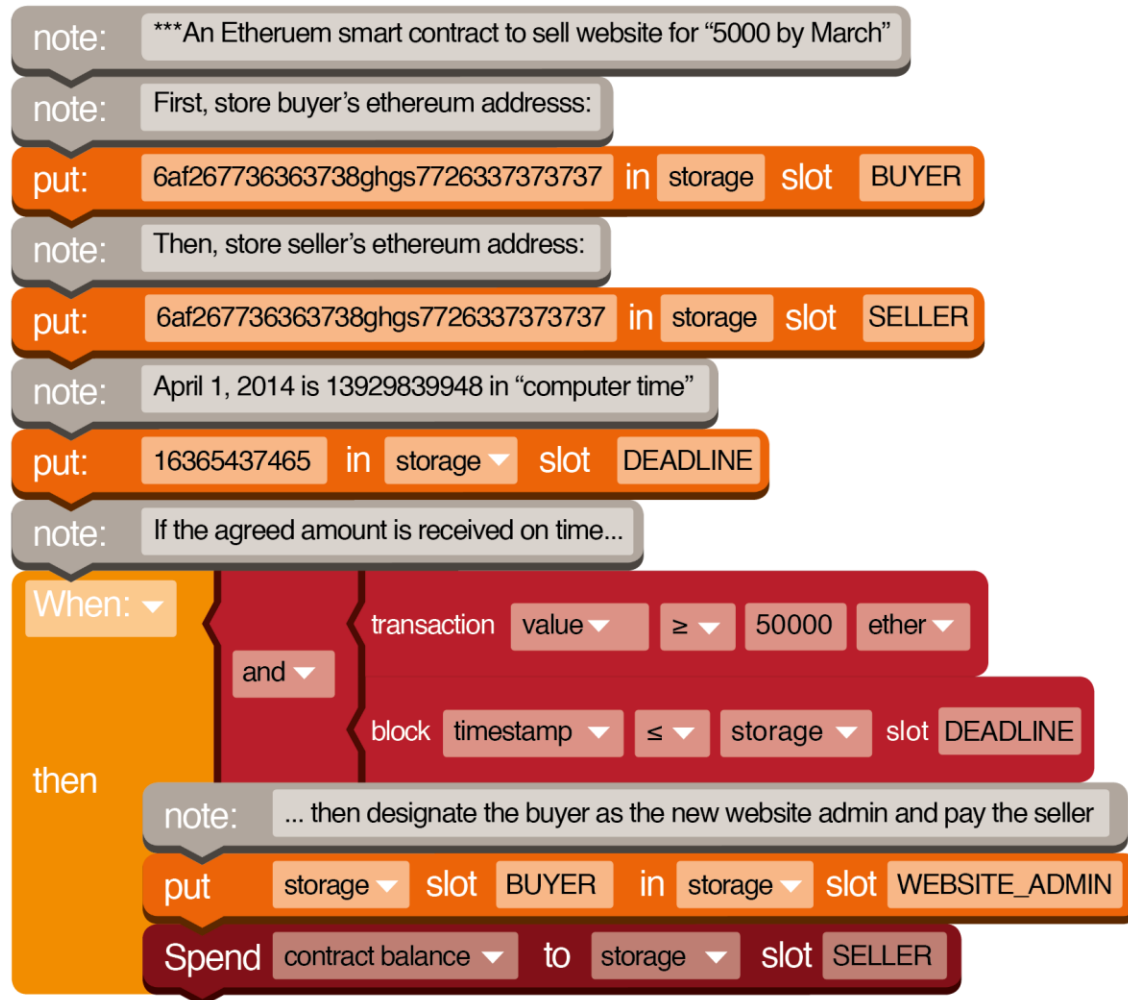
# Smart Contracts

- Die Grundprinzipien wurden bereits im Jahr 1994 vom Kryptologen Nick Szabo definiert
- Einsatzgebiete reichen von Abbildung, Überprüfung, Verhandlung und Abwicklung von Verträgen
- Die Verträge sind je nach Implementierung als Script oder als kompilierter Code auf der Blockchain abgespeichert

# Smart Contracts

- Erlaubt den automatischen Austausch von digital repräsentierter Gelder und andere Vermögenswerten.
- Nur wenn das Resultat bei allen Nodes identisch ist wird es in die Blockchain aufgenommen

# Smart Contracts (EtherScript)



# Herausforderungen

- Spezifikations- und Programmierfehler können schwere Folgen haben, da ein Smart Contract in der Blockchain persistent ist
- Fehler in der Implementierung können zu Vermögensverlusten führen
- Noch ist nicht klar, ob und inwieweit das bestehende Rechtssystem mit den Smart Contracts vereinbar ist.



# Einsatzgebiete Blockchain

- Dezentrale Stromgewinnung  
automatische Protokollierung wer wie viel Strom produziert hat.
- Aus Bankensicht sind die Marktsegmente Zahlungsverkehr und Kapitalmarkt von Interesse. Verwaltung und Abwicklung von Autofinanzierungen, Darlehens- und Hypothekenverträge über Smart Contracts.
- Blockchain Wedding  
Registrierung erfolgt in einem öffentlichen online Register

# Einsatzgebiete Blockchain

- Mobile Ladestation für E-Autos  
Steckdosenadapter mit dem an jeder normalen Steckdose das Auto aufgeladen werden kann. Kosten werden dem E-Auto-Besitzer verrechnet.
- Sichere Online-Wahlen «Followmyvote»  
Elektronischen Wahlen bergen ein Sicherheitsrisiko. Mit der Blockchain-Technologie liessen sich Wahlergebnisse nachverfolgen

# Literaturverzeichnis

- <https://en.bitcoin.it/wiki/Help:FAQ>
- <https://blockchain.info/>
- <https://www.ethereum.org/>
- <http://etherscripter.com/0-5-1/>