Bitcoin

Schnitzel

17. Mai 2013

Was ist Bitcoin

- Kryptowährung
- P2P - Keine zentralen Autoritäten
- Festgelegtes Maximum (21 Millionen Bitcoins)
- Transaktionen sind irreversibel
- Pseudonymes Zahlungsmittel
- Open Source

Das Netzwerk

- P2P-Netzwerk
- User
  - Nutzer eines Bitcoin-Clients
  - Hält Blockchain vor
  - Teilt Blockchain mit anderen Usern
  - Validiert Blöcke
- Miner
  - Erweitert Blockchain um Transaktionen

Die Blockchain

- Beginnt mit Genesis Block
- Verlauf aller Transaktionen
- Jeder Block enthält Hash des vorherigen

Doppeltes Ausgeben eines Coins wird erschwert.

Mining

- Bestätigung von Transaktionen in der Blockchain
- ist ein ressourcenhungriges Verfahren
- Miner werden für die verwendeten Ressourcen entlohnt

Transaktionen

1. Der Client erstellt die Transaktion
2. Der Client signiert die Transaktion
3. Das Netzwerk verifiziert die Transaktion
4. Die Transaktion wird in die Blockchain eingebaut

Probleme

Probleme im Netzwerk

- DoS-Angriffe
- Hijacking
- MITM bei IP-Transaktionen
- Übernahme des Bitcoin-Netzwerks

Probleme bei einzelnen Clients

- Skalierung der Blockchain
- Diebstahl der privaten Schlüssel

Altcoins

- Litecoin (scrypt)
- Namecoin (SHA256d)
- Novacoin (scrypt)
- ppCoin (SHA256)
- Terracoin (SHA256)
- Und viele mehr ...

Links

Informationen

- bitcoin.it - Bitcoin-Wiki mit zahlreichen Artikeln

Handel

- mtgox.com - Weltweit größte Bitcoin-Tauschplattform
- btc-e.com - Weitere große Handelsplattform

Community

- bitcointalk.org