Bitcoin

Quelle: Bitcoin.org, Logo under CC0 1.0 License.

History

- 2009 Genesis Block
- 2010 15000 BTC Pizza, 1$ (Slashdot Welle 1)
- 2011 7$ (Slashdot Welle 2)
- 2012 30$
- 2013 260$ (DDOS MtGox), 1200$ (china)
- 2014 Gewinnmitnahmen, Abwertung auf 250$
- 2015 gewisse Stabilität

Mining

- CPU
- GPU
- FPGA
- ASIC

- Derzeit ca. 1000 mal mehr Power als die Supercomputer der Welt zusammen, würden sie hashen.. . (ca.400 Petahash/s (SHA256 2mal))

Wallets/Clients

- Bitcoin Core (volle lokale Blockchain)

Paperwallets (BitAddress.org, „Casacius“ Coins)

- Lightweight Wallets (bitcoin4android)
- Deterministische Wallets
- Brainwallets
- Hardware Wallets (trezor u.a.)
- Webwallets (blockchain.info)

Quelle: Trezor Image, © SatoshiLabs.com

Altcoins

- Basieren auf dem Bitcoin „Rezept“
- Über 750
- Andere Ansätze zu Proof of Work,Proof of Stake
- Anonymisierungsansätze (Darkcoin)
- Distributed DNS (Namecoin)

Quelle: litecoin.org, Logo under CC0 1.0 License

Praxis

- Micropayments (streamium)
- Gambling (z.B. Satoshidice)
- Remittance (aka Western Union)
- Dark Markets (Silk Road)
- OpenBazaar

BIP und weitere Ideen

- Bitcoin Improvement Proposal
- N aus M Multisignature Transaktionen
- Locktimeverify Transaktionen
- Time/Hashstamps
- Colored Coins
- Smart Contracts (Escrow, autonomes System, „Autoschlüssel“)

Exchanges

- MtGox no more
- Bitstamp.net
- Bitfinex.com
- Local Bitcoins
- P2P Transfer

Quelle: Screenshot from bitcoincharts.com

Anonymität

- Bitcoin ist nicht anonym, jede Transaktion ist nachverfolgbar
- Mehr Anonymität nur durch Aufmerksamkeit des Users möglich
- Waschmaschine/Bitcointumbler

KYC/AML/Gesetze

- Datenschutz quasi ein Feature von Bitcoin
- Man gibt nur preis, was man preisgeben will
- Einführung von strikten KYC/AML Gesetzen führt zur Abwanderung (siehe NYC License, Deutschland)
- BaFin hat restriktive Interpretation
- Steuerlich in Deutschland nicht ganz klar

Stuff/Aktuelles

- Preis nicht entscheidend
- Als Hauptanlage nicht empfehlenswert, da immer noch ein Experiment
- bitcoinobituaries.com
- Derzeitige Diskussion/Problem: Skalierung und die Vorgehensweise (Blockgröße/Overlaynetwork)
- „Stresstest“ von unbekannt