Bitcoin

„Not your keys, not your bitcoin“

Kryptowährung

Kryptogeld

dezentral organisiertes Buchungssystem

Zahlungen werden kryptographisch legitimiert

Zahlungen werden über ein Netz gleichberechtigter Rechner (*peer-to-peer*) abgewickelt

beschrieben von *Satoshi Nakamoto* (Pseudonym)

Bitcoin-Einheiten werden durch die Lösung kryptographischer Aufgaben erzeugt (Mining)

฿

XBT

BTC

Satoshi — kleinste im aktuellen Protokoll darstellbare Unterteilung von 1/100.000.000

zur Durchführung einer Zahlung kann eine Gebühr abgeführt werden

kein zentrales Clearing der Geldbewegungen

Eigentumsnachweise an Bitcoin werden in persönlichen digitalen Brieftaschen gespeichert

Preisbildung auf dem freien Markt

2007 erfunden

2009 die erste Version der Referenzimplementierung
- **Bitcoin Core**
  - *bitcoin-qt* (mit Qt GUI)
  - *bitcoind* (Bitcoin Client ohne GUI)
- **Open Source**

die maximale Geldmenge ist durch das Netzwerkprotokoll auf knapp 21 Millionen (20.999.999,97690000) Einheiten festgelegt

dezentralen Datenbank mit allen Transaktionen- der Blockchain

Bitcoin-System hat keine geographischen Beschränkungen

Irreversibilität von Transaktionen — Bitcoin-Transaktion kann nicht widerrufen werden

Fälschungssicherheit

benötigt eine Internetverbindung

Transaktionskosten — mindestens 1.000 Satoshi (= 10 µBTC = 0,01 mBTC = 0,00001 BTC)

„vires in numeris“ — „Stärke in Zahlen“

Bitcoin-Wallets

geheime Phrase („Seed“)

über einen Algorithmus wird deterministisch eine beliebige Anzahl von privaten Schlüsseln herleiten

Identifizierung der Handelspartner ermöglicht Bitcoin nicht

eine vollständige Anonymität garantiert das System allerdings nicht

das Bitcoin-Netzwerk entstand am 3. Januar 2009 mit der Schöpfung der ersten 50 Bitcoin und dem „Block 0“

www.wenzlaff.de