Cryptocurrencies 101

TECHNIK, WIRTSCHAFT, GESELLSCHAFT

Definition

- Die Blockchain ist eine dezentrale Datenbank,
- die es dank eines (kryptographischen) Konsensalgorithmus schafft
- einen einheitlichen Zustand ohne zentrale Instanz herzustellen;
- Inhalte sind mitsamt ihrer ganzen Geschichte jederzeit einsehbar
- und können nur in bestimmten Zeitabständen (nicht in Echtzeit)
- nach einem vorab festgelegtem System eingespeichert werden.

Technik

KRYPTOGRAPHIE, BLOCKCHAINS, CONTRACTS

Wichtige Funktionsklassen

- Falltürfunktionen
  - Diskreter Logarithmus $b = g^a \mod p$
  - Primfaktorzerlegung $n = p \cdot q$
- Einwegfunktionen
- Hashfunktion
  - Näherung an Einwegfunktionen
  - Nicht bijektiv → Kollisionsangriff
  - Beispiele: MD5, SHA1, SHA512

Ausgangswert Funktionswert

Asymmetrische Kryptographie

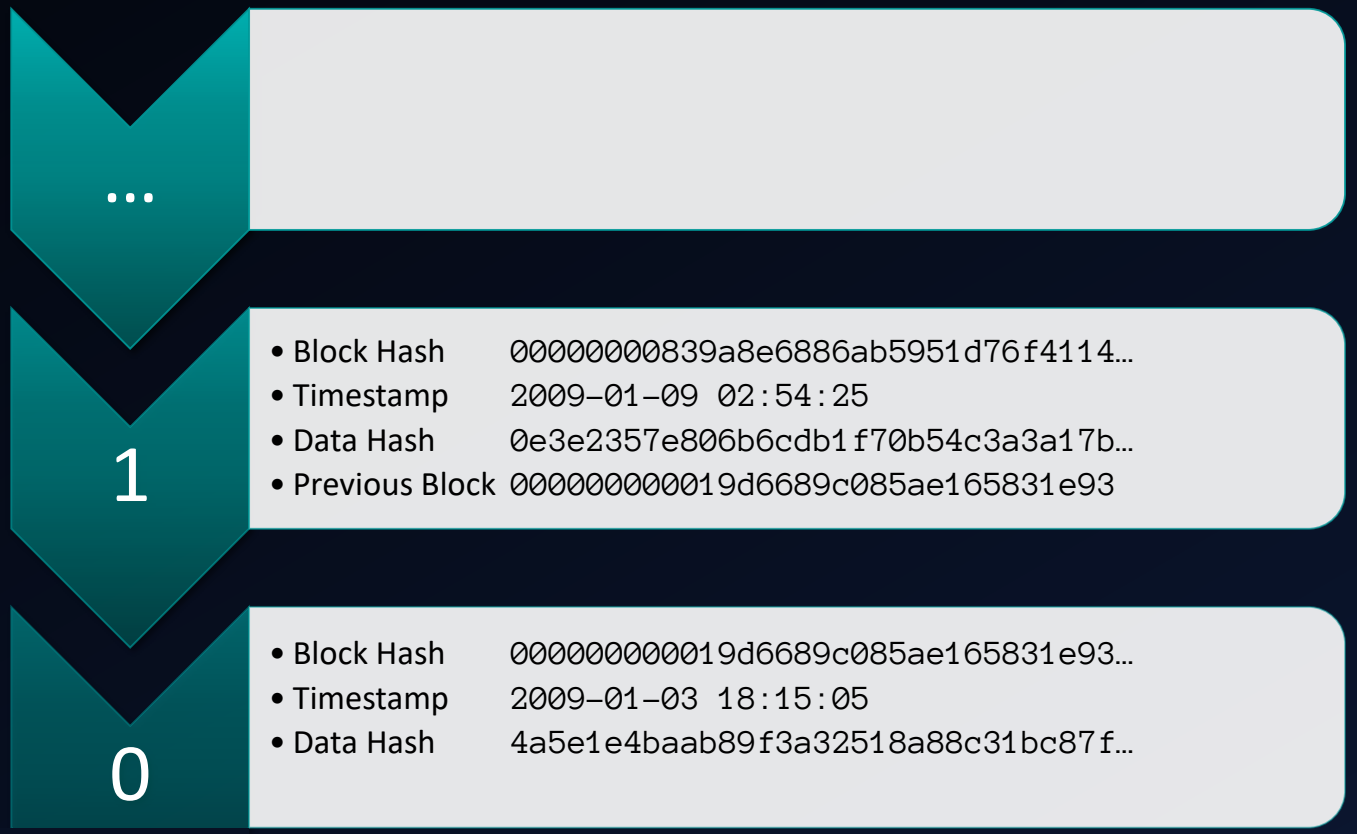
- Schlüsselpaar (a, g^a)
- Schlüsselaustausch
  - Erstellung eines gemeinsamen Geheimnis über einen öffentlichen Kanal
  - Diffie-Hellman Schlüsselaustausch
    - 1. Erstellung der Schlüsselpaare (a, g^a) (b, g^b)
    - 2. Austausch und gemeinsames Geheimnis g^{ba} g^{ab}
- Asymmetrische Verschlüsselung
  - Verschlüsselung mit asynchron erstellten gemeinsamen Geheimnis
  - Elgamal Verschlüsselung $g^a, b \Rightarrow c = m \cdot g^{ab} \Rightarrow g^b, c$

Digitale Signaturen

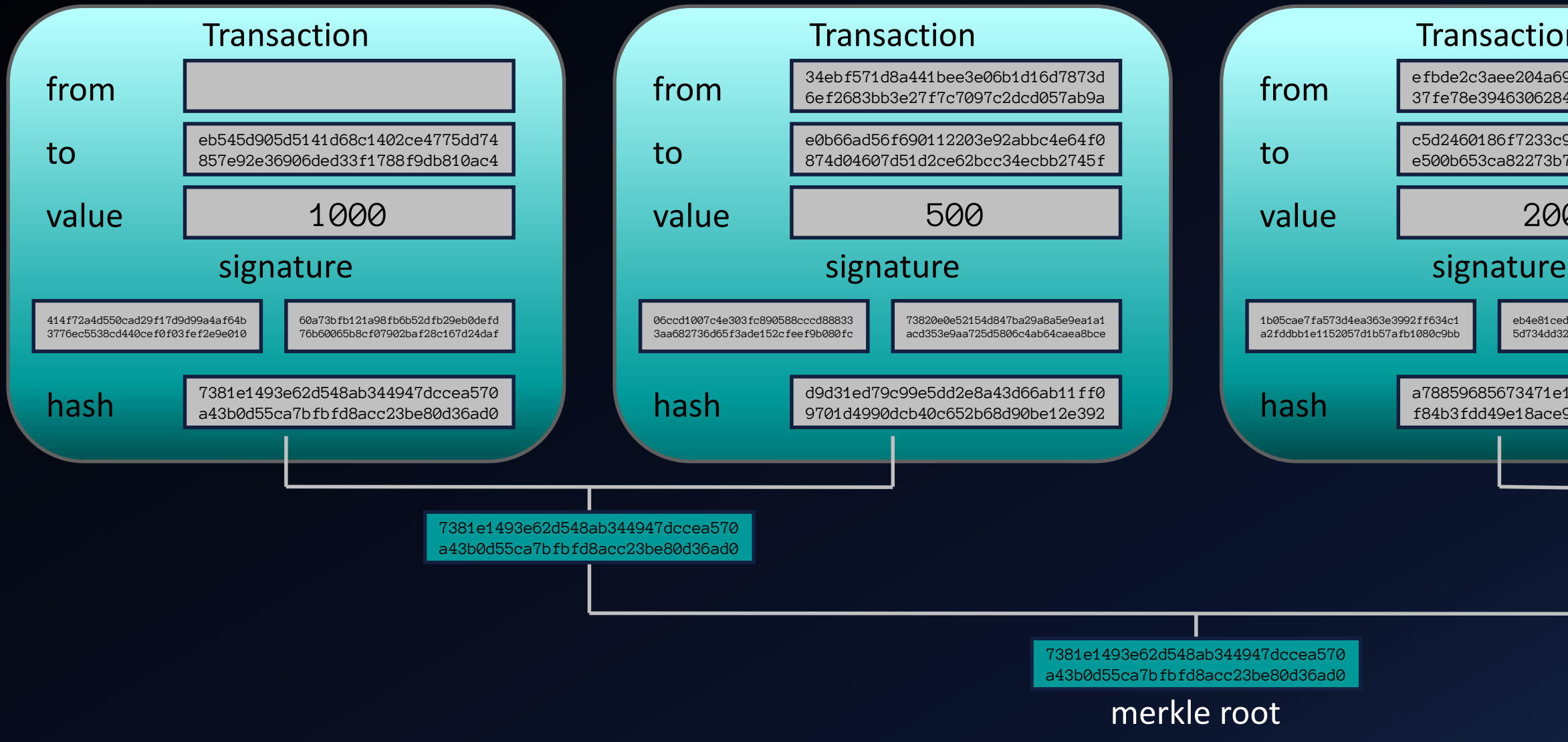
- Nur mit Geheimnis erstellbar, immer verifizierbar
- Elgamal Signatur (DSA)
  - 1. Gegebene Variablen (a, g^a) $h = hash(m)$
  - 2. Hilfsdaten erstellen (k, g^k) $s = (h - a \cdot g^k)k^{-1}$
  - 3. Veröffentlichung (m, g^k, s)
  - 4. Verifizierung $g^{a \cdot g^k} \cdot g^{k \cdot s} = g^{a \cdot g^k} \cdot g^{h - a \cdot g^k} = g^h$

Blockchain Datenstruktur

- Nutzer Account
  - $(sec_w, addr_w)$
  - $addr_w = hash(pub_w)$
- Inhalt
  - Header
  - Daten
- Forks
  - Zufälliges Auftreten
  - Geplant (Bitcoin, DAO)



Transaktionen



Cryptowährungen Beispiele

	Genesis	Blockdauer	Umsatz	Chaingröße	Preis
Bitcoin Core	09.01.2009	10 min	220.000T/h	181 GB	11.000$
Ethereum	30.07.2015	15 s	900.000T/h	338 GB	1.000$
ZCash	28.10.2016	2 min	350T/h	11 GB	500$

- Monero: CPU basiertes Mining
- ZCash: Zero Knowledge Transaktionsbeweise
- Bitcoin: Pionier und Lighning Network
- Ethereum: Smart Contracts

Angriffsszenarian

- Fremdes Geld ausgeben
  - Transaktionshash signieren
- Geld mehrfach ausgeben
  - Transaktionen und Blockchain validieren
- Geschichte verändern
  - Confirmation
  - Consensus
    - Längste Kette ist gültig, Überschreiben nur mit hohem Aufwand möglich
    - Verbreitester Ansatz (>90%): Proof of Work

Proof of Work

- Füge Zufallszahl (Nonce) in den Block hinzu
- Akzeptiere Block nur, falls hash < difficulty
  - Sha3(„Block 1“) `0501840df99e3a29d9c472b5804b1ecb…`
  - Sha3(„Block 20535“) `0000a500ede7c78376fca55242a1c139…`
- Stromverbrauch durch Mining

Bitcoin 2017:	27 TWh	Ξ	4 TWh
KKW Grafenrheinfeld 2014:	10 TWh	☀	0,04 TWh
Irland 2014:	26 TWH	CH	62 TWH

- Mining Angriffe: >50%, Selfish, Stubborn

Pool Mining

- Wahrscheinlichkeit für Blockerstellung sehr gering
  - 50MH/s: Blockerstellung ~8,4 Mio. Jahren (Fee: 3.5 + Reward 12.5 → 176.000$)
- Anschluss an Mining Pools
  - Gemeinsames Minen
  - Auszahlung durch Shares
- ASICs bedrohen Dezentralisierung
  - Bitcoin: 5 Pools liefern 78.8% (22.4 + 19.1 + 13.4 + 12.3 + 11.6, 6.7, 4.6)
  - Ethereum: 3 Pools liefern 59.6% (24.7 + 21.6 + 13.3, 8.6, 7.4, 5.8, 4.6)
  - Monero: 2 Pools liefern 24.4% (13.9 + 10.5, 9.1, 4.6)

Proof of Stake

- Nächster Ersteller wird zufällig, aber vermögensabhängig bestimmt
  - Idee: Besitz von 10% der Coins ermöglichen Validierung von 10% der Blöcke
  - „Nothing at stake“: Arbeiten an mehreren Chains sinnvoll
- Forging in NXT
  - Voraussetzung: 1 ausgehende Transaktion, Balance > 1000 (1440 Confirmation)
  - Erstellung: Hash(pubkey || prev block) < Base x Balance x Timediff
- Münzalter in Peercoin
  - Münzalter: Anzahl der Coins x Tage seit letzter Interaktion
  - Regelmäßige Checkpoints
- Varianten: Proof of Activity (PoS + PoW), Proof of Burn

Smart Contracts

- Programme auf der Blockchain
- Beschränkte Funktionalität
  - Daten aus der echten Welt
  - Automatischen Funktionsaufrufe
- Gas
  - Bezahleinheit für Berechnungen
  - Speichern besonders teuer
  - Muss mit Ether bezahlt werden
- Beispiel
  - Live-Demo: Gamble Contract
- DAO
  - Crowdfunding SC
  - Problem: Fallback function
  - DAO Hack: 50 Mio. $
  - Hardfork

Wirtschaft

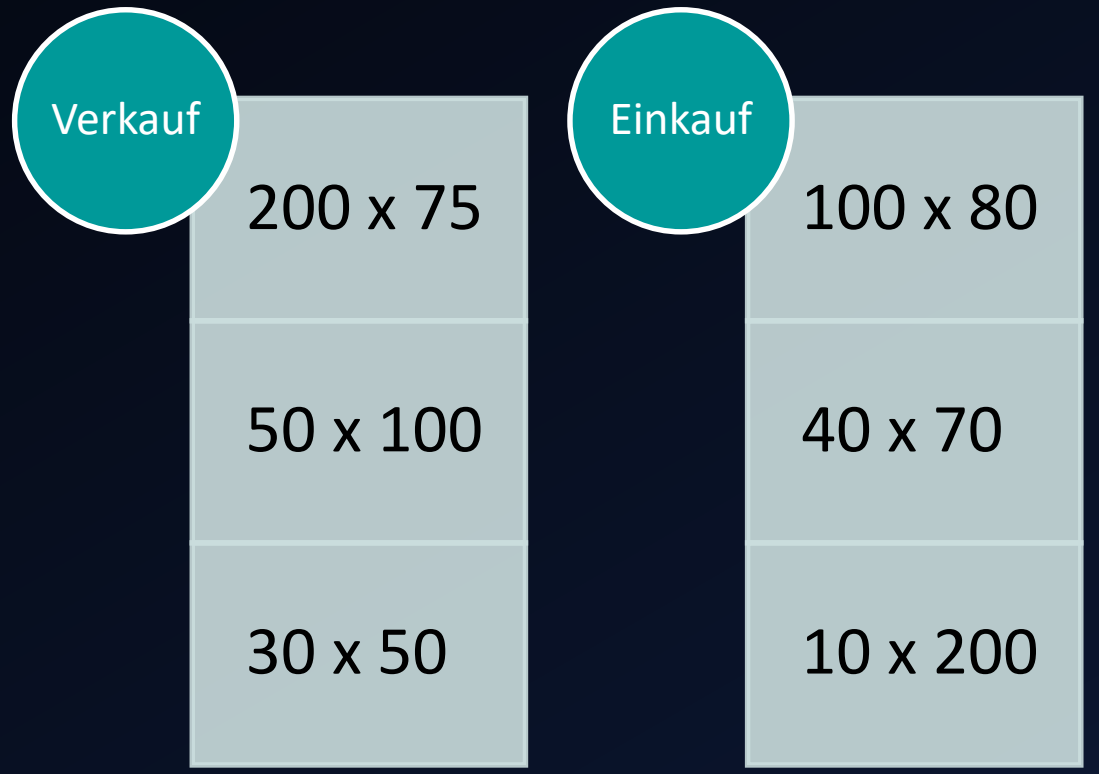
GRUNDLAGEN, ZOCKEN, GESCHÄFTSMODELLE

Gewinnmöglichkeiten mit Cryptocurrencies

- Mining
  - Stromkosten vs. Difficulty
- Schneeballsystem
  - ICO + Referral-System
  - PR / Memes
  - Fiat Geld
- Insidertrading
  - Ähnlich: High Frequency
- Zocken
  - „Wir als Informatiker sind schlauer als der durchschnittliche Anleger!“

Aktienhandel 101

- Grundprinzipien
  - Liquidität
  - Anzahl x Limit
- Beispiel
  - 100: VK 280 EK 10
  - 75: VK 230 EK 110
  - 50: VK 100 EK 150
- Üblich
  - Maximaler Stückumsatz + Einheitspreis
  - Kauf- und Verkaufspreis: 110 x 75 = 8250
- Egoistisch
  - Maximales Volumen + Staffelpreis + Eigengewinn
  - Kaufpreis: 10 x 200 + 100 x 80 + 40 x 70 = 13290
  - Verkaufspreis: 30 x 50 + 120 x 75 = 10500



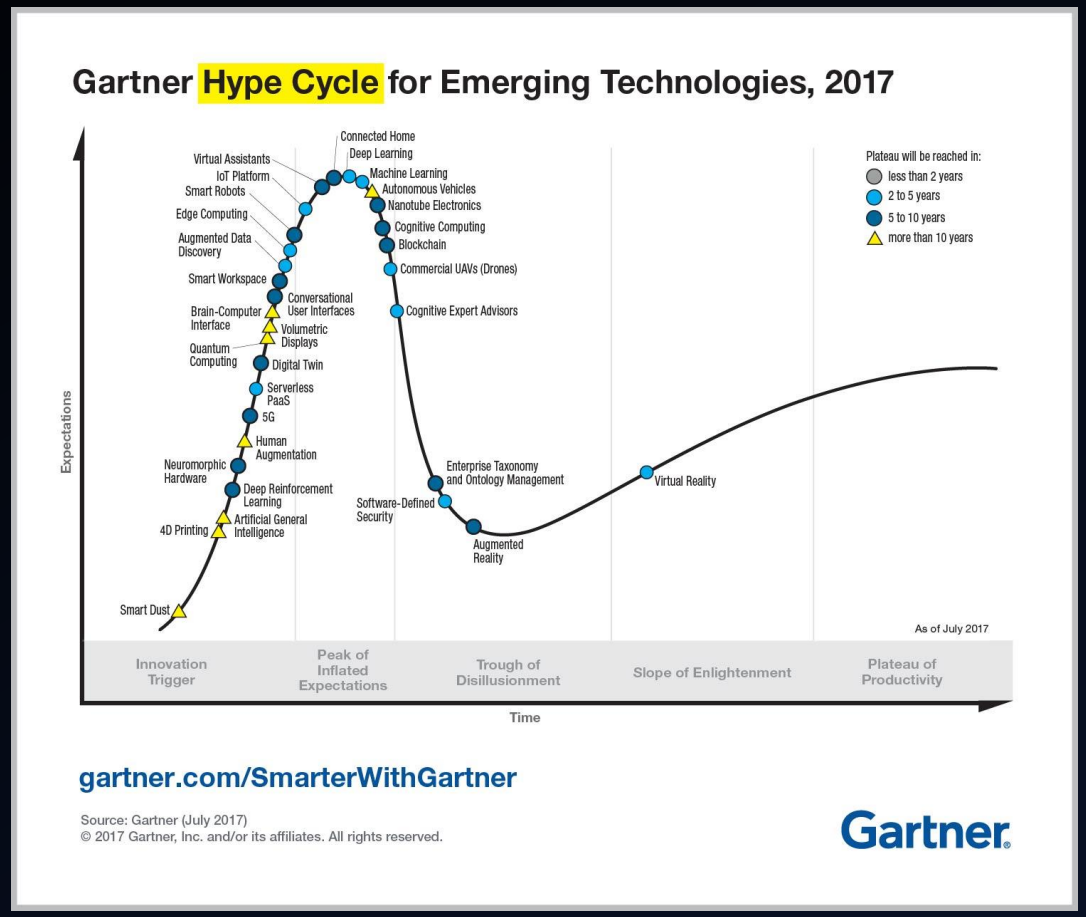
Börsenspekulation

- Option
  - Zocken auf Gewinne / Verluste
- Leerverkauf
  - Hintergrund: Bauern
  - VW 2008: Kurssteigerung von ~250€ auf >1000€
- Gesetzliche Lage
  - Deutschland: in Gewinnabsicht oder ungedeckt verboten (§26 BoersG / LeerverkaufsVO)
  - Amerika: Zwischen 1938 und 2007 verboten
- Kursschwankungen rentabler als stabile Steigung!

Soziale Entwicklung

UTOPIE, PROBLEME, EDUCATED GUESS

Technische Probleme für den Durchbruch



- Skalierung
  - Stromkosten
  - Durchsatz
- Ausfallssicherheit
  - Stromausfall
  - Internet abklemmen
- Systemintegrität
  - Gezielte Attacks auf Privatpersonen
  - Staatsangriffe (Stromproduktion!)

MBTI Persönlichkeitstest / Kersey Typen

Sensoric Judging

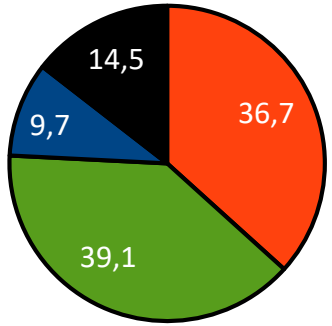
Ordnung
Verantwortung
Bewährtes

Introversion <-> Extraversion
Sensoric <-> Intuitive

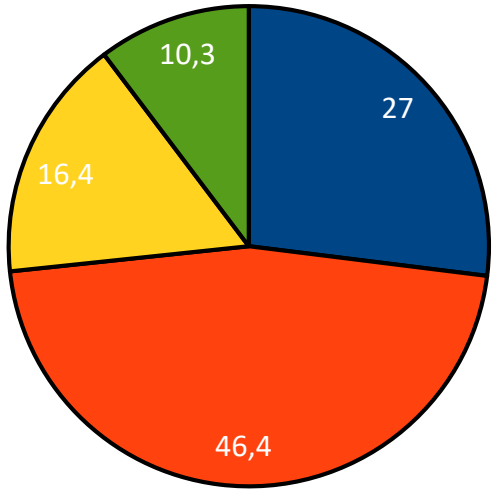
Unkonventionell
Hilfsbereit
Erfahrung

Sensoric Perceiving

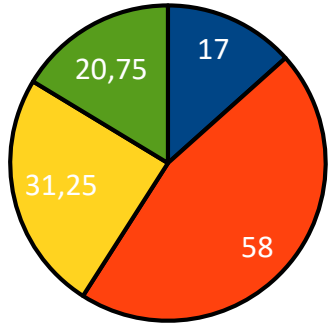
T Manager (Ashridge)



Bevölkerung



Lehrer (Florida)



Intuitiv Feeling

Gemeinschaft
Sinn
Kreativs

Thinking <-> Feeling
Judging -> Perceiving

Wahrheit
Herausforderung
Kompetenz

Intuitiv Thinking

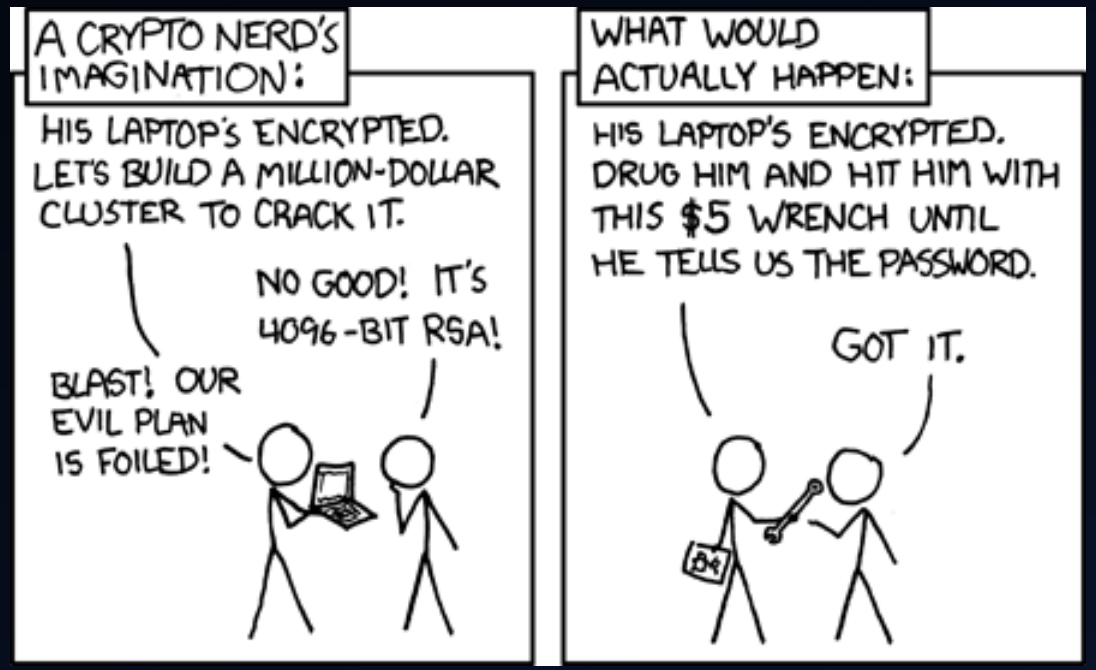
Gesellschaftliche Hindernisse

- System muss von jedem einsetzbar sein
  - Opa möchte Dauerauftrag einrichten lassen
  - Oma kann nicht mit Computern umgehen
- System muss alle Use Cases erfüllen
  - Passwort vergessen
  - Überweisung zurückholen
- Zuständigkeiten müssen geregelt werden
  - Social Engineering Angriffe auf Sekretärinnen
  - Programmierfehler in Smart Contracts

Szenarien

- Technische Utopie: Befreiung und Dezentralisierung von Macht
  - Unabhängigkeit der Finanzen von den Autoritäten / Banken
  - Technische Sicherheitsgarantien
  - Finanzierung der Internethelden durch Micropayments
  - Waschmaschine bestellt und bezahlt automatisch Waschmittel
- Soziale Dystopie: Technische Lösung für soziale Probleme
  - „Besuchen sie ihre Oma DLC“ im Altenheim
  - „Bezahlen Sie 0.2 BTC um Ihr Auto wieder benutzen zu können“
  - „Winken Sie für ihr Gehalt in die CCTV-Kamera auf der Staatsparade“

XKCD


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Diskussion

QUELLE: INTERNET