Ethereum

- Blockchains im Allgemeinen
- Ethereum als Blockchain
- Mining von Ethereum
- Smart Contracts

Blockchain

- verteilte Datenbank
- Integrität durch Hashing gesichert
- Append-only - **alle** Transaktionen können nachgespielt werden (Hello Kafka!)
- Nutzung als Kryptowährung oder Transaktionslog
- Bitcoin (Litecoin, Dogecoin), Ethereum u.a.

Ethereum

- Beginn 2013 durch Vitalik Buterin, Betrieb ab Juli 2015
- Nicht nur Kryptowährung, sondern Plattform für DApps (Distributed Apps)
- DAOs, nicht *Data Access Object* sondern *Decentralized Autonomous Organization*
- Fork von Ethereum am 17. Juni 2016; Diebstahl von € 65 Mio durch Bug im Smart Contract von *The DAO*
  - *Ethereum* (ETH): Diebstal wurde zurückgerollt
  - *Ethereum Classic* (ETC): Diebstahl ist weiterhin vorhanden

Fiatgeld, Kryptowährungen und deren Gegenwert

- Fiatgeld: Banknoten und Münzen
- Warengeld: Tauschmittel in Form von Waren (Wasser, Tabak, Gold...)
- Kryptowährung: Konten mit ... was eigentlich? (später)

Von Adressen und Überweisungen

- Kryptowährung (Coins, Ether) wird auf Adressen in der Blockchain eingezahlt bzw. abgehoben
- Adresse = Konto, z. B. 0x4c1856C9021DB812f0B73785081b245f622D58ec
- Adresse kann durch Marktplatz gemanagt werden oder dir gehören
- Nur Geld auf deinen eigenen Adressen ist sicher
- Adressen sind durch Public/Private-Key-Verfahren gesichert

Überweisungen

Mit Hilfe von *geth*

```
var from = eth.accounts[0];
var to = '0x4c1856C9021DB812f0B73785081b245f622D58ec';
var amount = web3.toWei(1, 'ether');
web3.personal.unlockAccount(from, 'PASSWORD');
eth.sendTransaction({from: from, to: to, value: amount});
web3.personal.lockAccount(from);
```

Handel

- Marktplätze wie kraken.com
  - Kauf von Kryptowährungen für Fiat
  - Verkauf von Kryptowährungen in Fiat
  - Tausch von Kryptowährungen
- Handel ist **sehr** volatil
- ICOs von neuen Unternehmen
- mindestens 1 Jahr halten, ansonsten fallen Steuern (25%) an

Mining von Ethereum

- Proof of Work: f_hash(meta + nonce) = x_target
  - f_hash = KECCAK-256; ähnelt SHA3,ist es aber nicht
  - x_target = Hash mit bestimmten Format, z. B. 4 darauf folgenden "ff"s
  - meta = Metadaten aus der Blockchain-Transaktion
  - nonce = das ist zu finden
- Ethereum wird auf der GPU geminet, ASICs existieren (noch) nicht
- Gegenwert von Ether ist Rechenpower bzw. Strom
- Mit Wechsel zu Proof of Stake funktioniert Mining nicht mehr
- Steuerliche Aspekte

Mining aus der Praxis, Grafikkarten

- O-Töne
  - "Na, ihr wollt minen, wa?" (Verkäufer)
  - "Ihr seid schuld daran, dass ich keine neue Grafikkarte bekomme!" (Kollege)
- GTX 1070 eignet sich gut
- Preise der Grafikkarten haben extrem angezogen

Mining aus der Praxis, Strom

- O-Töne
  - "Du wolltest doch schon immer eine Fußbodenheizung, oder?" (ich)
  - "WIE HOCH ist der Stromverbrauch? Du spinnst ja." (potenzieller Hoster)
  - "Im Winter brauchen wir nicht mehr zu heizen, wuhu!" (Ehefrau)
  - "Ihr Stromverbrauch ist sehr hoch, suchen Sie gewerbliche Angebote?" (Stromvergleichsportal)
- Stromverbrauch = Wärme. Es bleibt kuschelig.
- 1.8 kWh für 12 GPU Mining Rig; 12 Monate: > € 4000 Stromkosten

Mining aus der Praxis, Trivia

- Claymore DualMiner ist besser als ethminer
- Bandbreite für das Mining relativ gering (~ 50 kBit/s)
- PCI Express Multiplexer anstelle von Riser-Karten
- Hohe GPU-Last stört WLAN massiv. Klingt blöd, ist aber so. Mehr dazu unter https://www.schakko.de/2017/07/13/fixing-periodically-occurring-wifi-logs-when-running-claymore-ethereum-miner/

Smart Contracts

- Applikationen, die im Ethereum-Netzwerk laufen
  - Byte-Code, Ethereum Virtual Machine (EVM), deterministisch, keine Seiteneffekte
  - Läuft auf **allen** Peers
  - Besitzen Storage
- Zum Ausführen eines Smart-Contracts muss der Auslösende Gas bezahlen
- Diverse Programmiersprachen, die nach EVM kompilieren, u.a. Solidity (angelehnt an JavaScript)

Smart Contract Beispiel

```
contract OwnedContract {
    bytes32 public name = 'Owned Contract';
    address public owner;

    function OwnedContract() {
        owner = msg.sender;
    }

    modifier isOwner() {
        require(msg.sender == owner);
        _;
    }

    function OwnedFunction() isOwner {
    }
}
```

Von http://linuxforme.com/ethereum-smart-contracts-in-a-nutshell-for-hackers.html

Fragen?

- Entweder per Twitter an @schakko
- oder per E-Mail an christopher.klein@neos-it.de
- Website-Besuch-Befehl: https://www.schakko.de