Innovation im Facility Management

DHBW – Stuttgart
Willie Laszlo Laubenheimer

Einführung in Ethereum – Inhalt

- Geschichtlicher Hintergrund
  - Bitcoin
  - Ethereum
- Technische Beleuchtung
  - Infrastruktur
  - Blockchain
  - Konsensalgorithmen
  - Sicherheitsaspekte
  - Token Standards
- Ausblick
- Hands-On

Geschichtlicher Hintergrund - Bitcoin

- Börsencrash ab 2007 bis zum Höhepunkt 2008
- Bitcoin Whitepaper Veröffentlichung durch einen Pseudonym Satoshi Nakamoto im Jahre 2009
- Erste GitHub Veröffentlichung von Quellcode auch 2009
- Stetige Entwicklung ab 2011, vorher gibt es größere Lücken
- Nicht Turing-vollständig
- Pseudoanonym
- neue Form einer „Unternehmensstruktur“

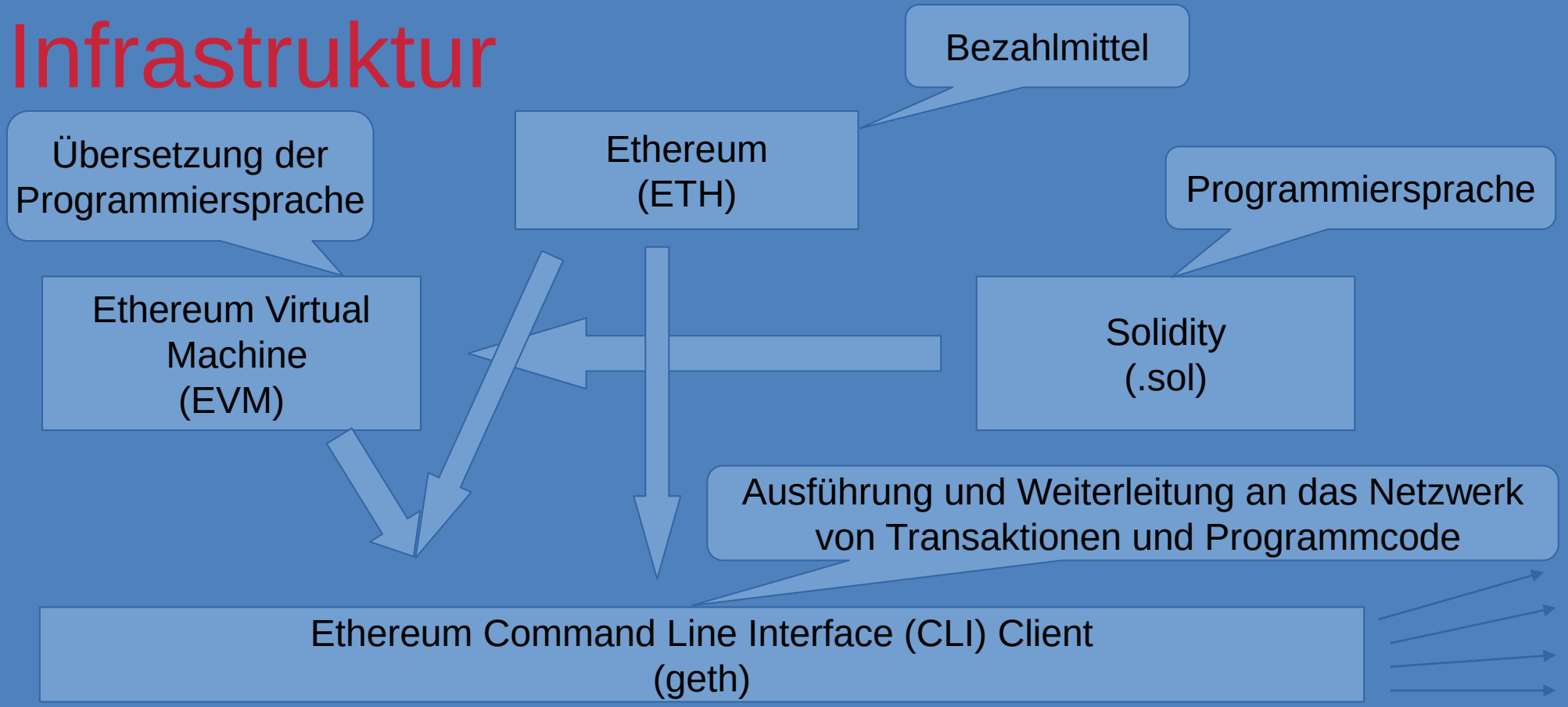
Geschichtlicher Hintergrund - Ethereum

- Erste Whitepaper Veröffentlichung von Vitalik Buterin Ende 2013/Anfang 2014, die Geburtsstunde von Ethereum
- Turing-vollständig, schleifen sind möglich (while, for, …)
- Unternehmensstruktur vorhanden
- Erste Finanzierung mithilfe von Bitcoins (ICO-Initial Coin Offering), um das vorgeschlagene Projekt zu entwickeln
- Großer Hack eines „smart contracts“ in 2016 (bekannt als „The DAO“)
- Aufteilung der Nutzer in Ethereum (ETH) und Ethereum Classic (ETC)

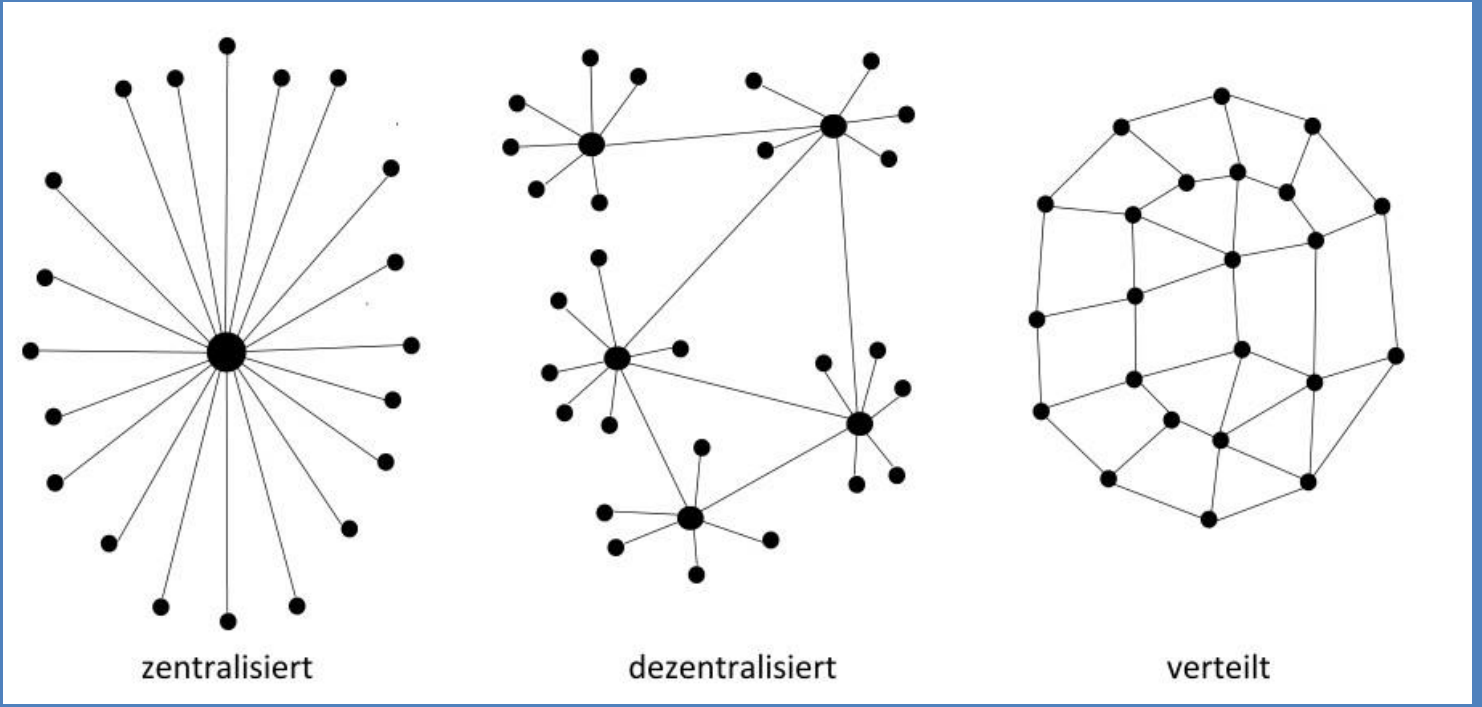
Technische Beleuchtung – Infrastruktur

- Offener Quellcode auf GitHub
- „Lizenzfrei“ weltweit nutzbar
- Entwicklung und „interne“ Kommunikation öffentlich einsehbar (EIP)
- Dezentrale/Verteilte „Rechenzentren“ (Mining, Ethhash z.B. ist eine Variante des SHA3 Algorithmus)
- Dezentrale/Verteilte Validierung (Nodes)

Technische Beleuchtung - Infrastruktur



Technische Beleuchtung – Infrastruktur



Quelle: https://www.dotnetpro.de/img/1/0/2/8/9/3/3/1_ce-de-dis_w915_h437.jpg

Technische Beleuchtung – Blockchain

- Methode zur Datenspeicherung
- Verkettung von Ereignissen, die in einem Block zusammengefasst und mit dem vorigen Block verknüpft werden
- Meist werden Hashes von Transaktionen als Merkle-Baum verknüpft und zuletzt wird durch ein Zeitstempel, sowie dem Hash des vorigen Blockes ein neuer Hash erstellt
- Somit entsteht eine zeitlich aufeinander folgende Kette (Reihe) von Datenblöcken, dessen Echtheit leicht zu überprüfen ist (Hashing mit den Inputs aus der Blockchain)

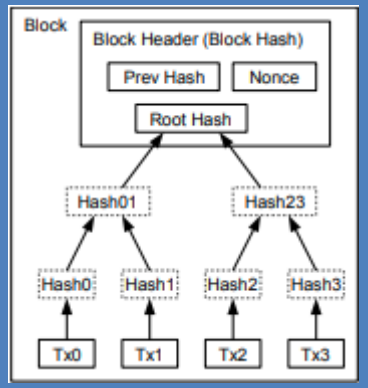
Technische Beleuchtung – Konsensalgorithmen

- Proof of Work – Rechenkapazität (Hashing mit Schwierigkeitsgrad)
  - Hoher Zeitaufwand
  - Hohe Rechenleistung
  - Hoher Energieverbrauch
  - Schwer korrumpierbar
- Proof of Stake – Anteilseigner ($€…)
  - Geringer Zeitaufwand
  - Zentralisierungsgefahr
  - Niedriger Energieverbrauch
  - Leichter korrumpierbar

Technische Beleuchtung - Konsensalgorithmen

- Grundprinzip: Einigung über Einhaltung der festgelegten Regeln (Konsens)
- Hauptproblem: Double-spending und Wahrung der Historie
- Weiteres Problem (der Blockchain): Größe der gespeicherten Datenmenge

Technische Beleuchtung – Konsensalgorithmen - PoW



- Erstellen eines Merkle-Baumes valider Transaktionen
- Hashing mit Zeitstempel
- Fordern einer gewissen Anzahl an 0-en zu beginn des Hashes durch hinzufügen einer sich verändernden Variable (Beispiel) (Mining, hoher Rechenaufwand)
- Validierung durch das Netzwerk, also jeden einzelnen Knoten (Node, niedriger Rechenaufwand)

Technische Beleuchtung – Konsensalgorithmen - PoS

- Analog zu PoW mit dem Unterschied, dass beim Hashing keine bestimmte Anzahl von 0-en gefordert wird
- Die Erstvalidierung darf nur von Knoten durchgeführt werden, die einen bestimmten Anteil an Token vorweisen können

Technische Beleuchtung – Zusammenfassung

- Einheiten einer Kryptowährung sind aus informatischer Sicht eine Verkettung von Zeichen (Token)
- „Kryptowährungen“ innerhalb von Ethereum sind Mappings(Zuordnungen) innerhalb eines Programmes in der Blockchain, Adresse a → hat b
- Miner erstellen aus validen Transaktionen einen Block und verknüpfen ihn mit dem vorherigen Block
- Nodes überprüfen den Inhalt der Blöcke auf Einhaltung aller Regeln

Technische Beleuchtung - Sicherheitsaspekte

- Turing vollständig (Schleifen wie for, while, ec. sind möglich)
- Hohe Updaterate der Programmiersprache solidity (i.d.R. monatlich)
- Teilweise Quellcodeanpassung der bereits veröffentlichten Programme („smart Contracts“) nötig
- Fehlerhaft programmierte Programme können zum Verlust von „Token“ und somit indirekt von konventionellem Geld führen (z.B. DAO-hack)
- Weitere Sicherheitslücken

Technische Beleuchtung - Token Standards

- ERC steht für Ethereum Request for Comment und die Nummer i.d.R. für die Issue-nummer
- ERC20 nicht unterscheidbare Token (Beispiel)
- ERC721 unterscheidbare Token (Beispiel)
- ERC777 Erweiterung und Optimierung des ERC20 Token Standards (Beispiel)
- ERC1155 Multitoken (Beispiel)

Hands On

- Metamask: https://metamask.io
- DHBW-Token
- DHBW-FM22-Token
- DHBW-Token empfangen und senden
- DHBW-FM22-Token generieren

bc1qzz8l5s9eskynpk6rjk93eneswaej0xwzpcvuz5 https://laubenheimer.eu 0xc3577e1BF219c041306dDa4689a1D1Fb531329A0

Danke für Ihre Aufmerksamkeit !

Innovate