SOFTWARE ENTWICKLUNG AUF DER BLOCKCHAIN

Hannes Gransow, Dennis Fiehn, Nicolas Bergmann, Anna Mockenhaupt, Samira Rohde

INHALT

1. Was ist die Blockchain
2. Geschichte der Blockchain
3. Blockchain Heute & Beispiele für Applikationen
4. Pro und Contra
5. Live Coding TeamToast Coin
6. Beispiel Anwendungsentwicklung: Ethereum Smart Contracts oder dApps
7. Chancen und Herausforderungen
8. Fazit

Quellen

1.
WAS IST DIE BLOCKCHAIN?
Primär am Beispiel Bitcoin

Name	♥	Price	Mkt. Cap	24h Vol	24h	7d Price	30d
Bitcoin	♡	$ 3,593.96	$ 62.89 Bn	$ 5.27 Bn	-0.24%		-4.66% $ 3,769.68
XRP (Ripple)	♡	$ 0.3169	$ 13.01 Bn	$ 348.78 MM	-0.21%		-16.02% $ 0.3774
Ethereum	♡	$ 116.82	$ 12.21 Bn	$ 2.53 Bn	-1.21%		-8.13% $ 127.16
Bitcoin Cash	♡	$ 128.93	$ 2.27 Bn	$ 270.68 MM	-3.29%		-19.66% $ 160.48
EOS	♡	$ 2.43	$ 2.20 Bn	$ 655.91 MM	-0.49%		-3.84% $ 2.52
Tether	♡	$ 1.01	$ 2.04 Bn	$ 3.57 Bn	0.09%		-1.04% $ 1.02
Stellar	♡	$ 0.1019	$ 1.95 Bn	$ 103.10 MM	-1.69%		-14.49% $ 0.1191
Litecoin	♡	$ 32.32	$ 1.94 Bn	$ 583.88 MM	0.19%		5.73% $ 30.56
TRON	♡	$ 0.0269	$ 1.79 Bn	$ 209.09 MM	-0.15%		37.46% $ 0.0196
Bitcoin SV	♡	$ 74.48	$ 1.31 Bn	$ 51.86 MM	-1.98%		-19.30% $ 92.30
Cardano	♡	$ 0.0429	$ 1.11 Bn	$ 12.82 MM	-1.82%		5.89% $ 0.0405
Binance Coin	♡	$ 6.49	$ 838.52 MM	$ 32.33 MM	-0.87%		16.11% $ 5.59

Blockchain

> Die Blockchain ist eine dezentrale Datenbankstruktur bzw. ein digitales Register, das Transaktionen transparent verzeichnet. Sie dient als Grundlage vieler digitaler Währungen. Die besonderen Charakteristika der Blockchain-Technologie sind Dezentralität, Unveränderlichkeit und Transparenz. Häufig wird mit Blick auf die Dezentralität der Blockchain auch von Distributed Ledger Technology (Technologie verteilter Kassenbücher) gesprochen.

Blockchain

- Blockchain = Kette von Blöcken
- Ist Blockchain = Bitcoin?
  - **Nein**: Blockchain ist der theoretische und technische Unterbau von Bitcoin. Ähnlich wie www nicht das internet ist. Www ist eine konkrete Anwendung (vgl. Bitcoin) und das Internet die gesamte Plattform (vgl. Blockchain)
- Basis für zahlreiche weitere Blockchains, Technologien, Währungen, Datenbanken u.v.m.

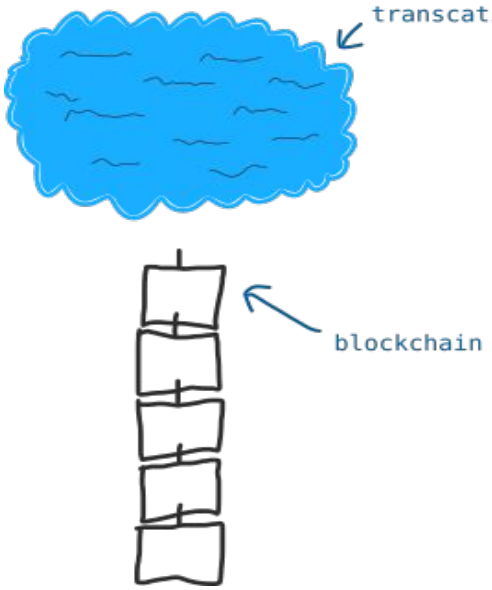
Blockchain (Bitcoin)

Block (~1MB):
- Kryptografisch gesicherter Hash des vorigen/nächsten Blocks
- Zeitstempel
- Transaktionsdaten (~500)
- Mining Difficulty

Chain/Kette bzw. Verbindung
- Kryptografischer Hash
- Hash ist einzigartig
- Zeigt auf den nächsten Block

Block 1  **Block 2**  **Block 3**

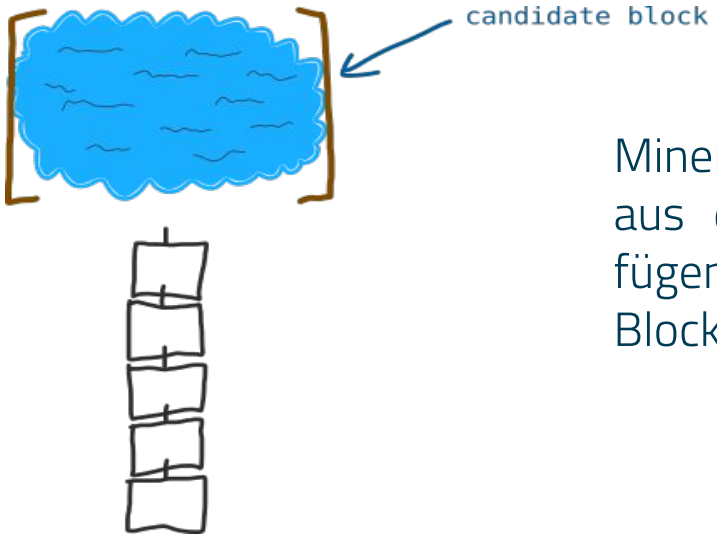
Mining



Getätigte Transaktionen werden nicht direkt an die Blockchain gehangen, sondern kommen in einen Transaction Pool. Hier warten sie Quasi darauf, an die Blockchain gehangen zu werden.

Quelle: http://learnmeabitcoin.com/guide/blocks

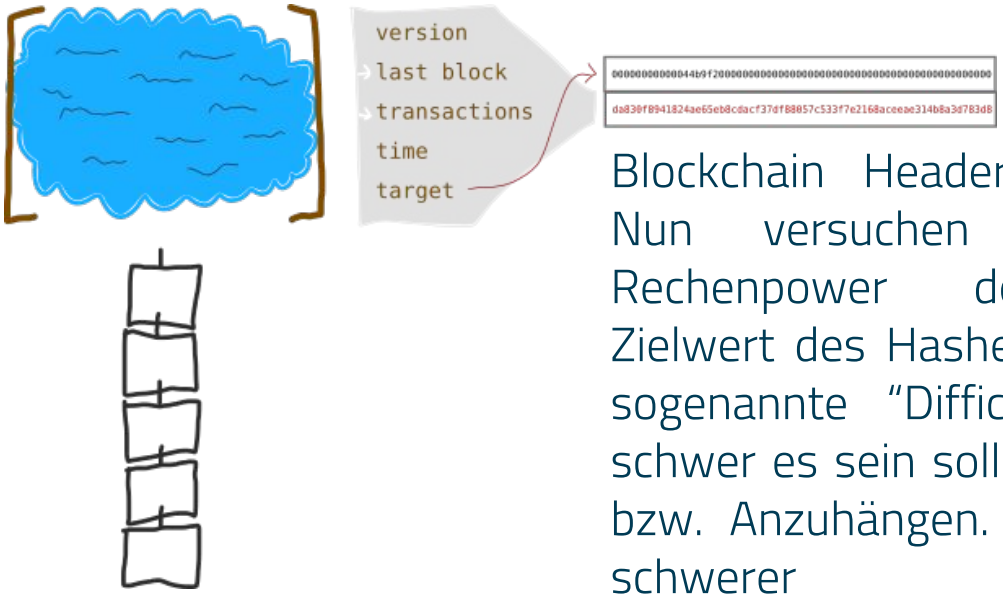
Mining



Miner sammeln Transaktionen aus dem Transaction Pool und fügen sie zu einem Candidate Block zusammen, bis er “voll” ist.

Quelle: http://learnmeabitcoin.com/guide/blocks

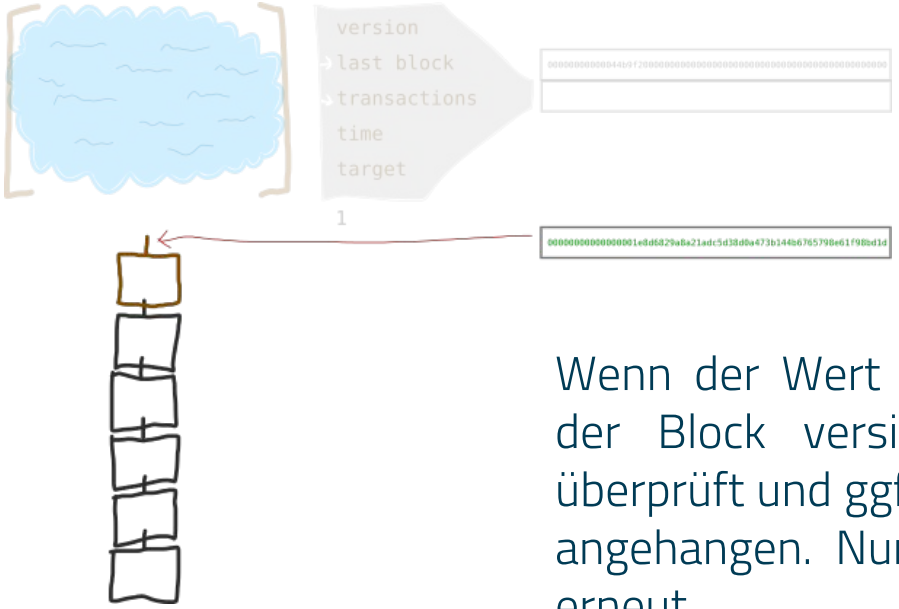
Mining



Blockchain Header wird hinzugefügt. Nun versuchen die Miner mit Rechenpower den vorgegebenen Zielwert des Hashes zu errechnen. Die sogenannte “Difficulty” gibt an, wie schwer es sein soll den Block zu Minen bzw. Anzuhängen. Mining wird immer schwerer

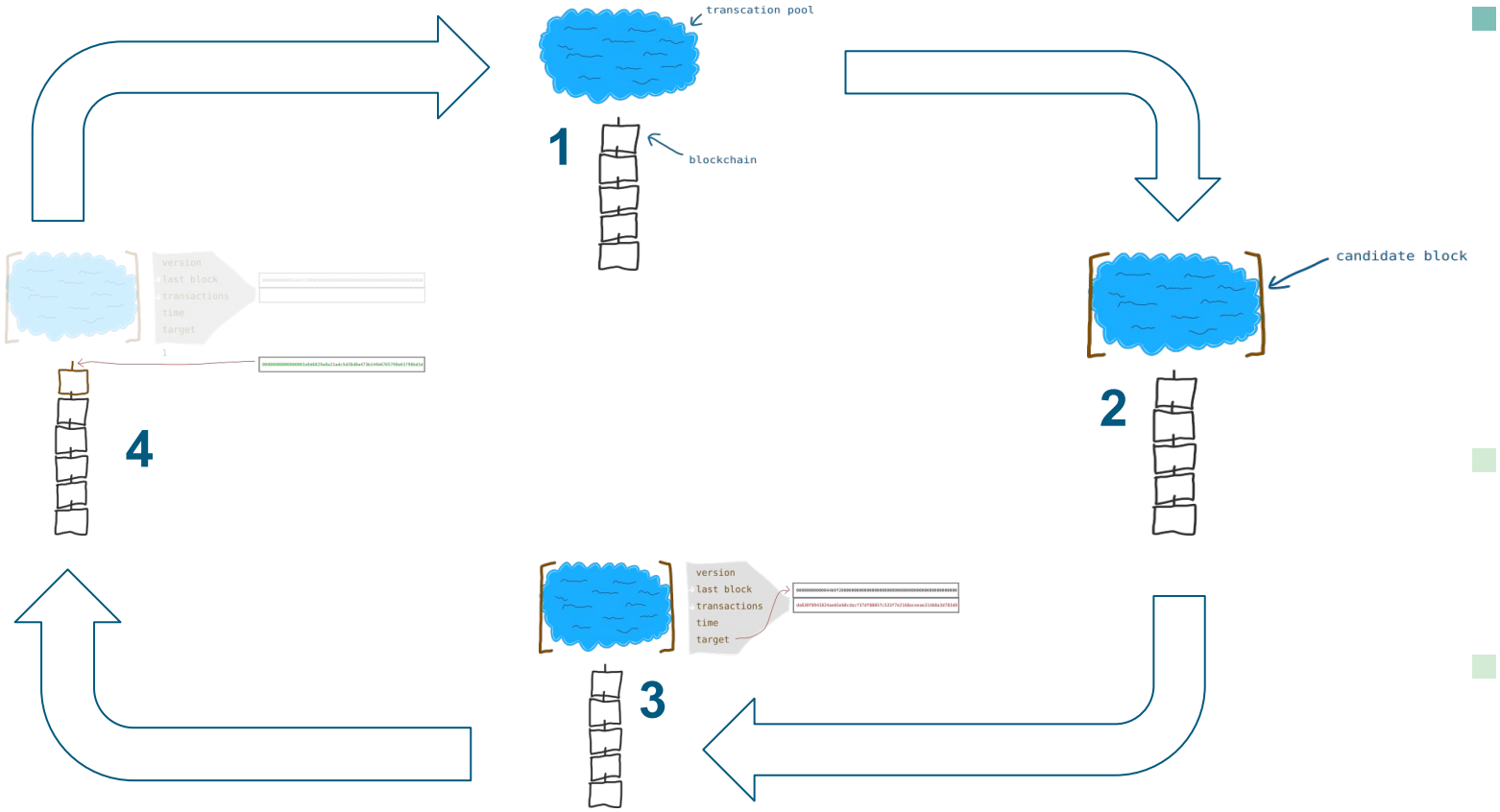
Quelle: http://learnmeabitcoin.com/guide/blocks

Mining



Wenn der Wert errechnet wurde, wird der Block versiegelt, vom Netzwerk überprüft und ggf. und an die Blockchain angehangen. Nun beginnt der Prozess erneut.

Quelle: http://learnmeabitcoin.com/guide/blocks



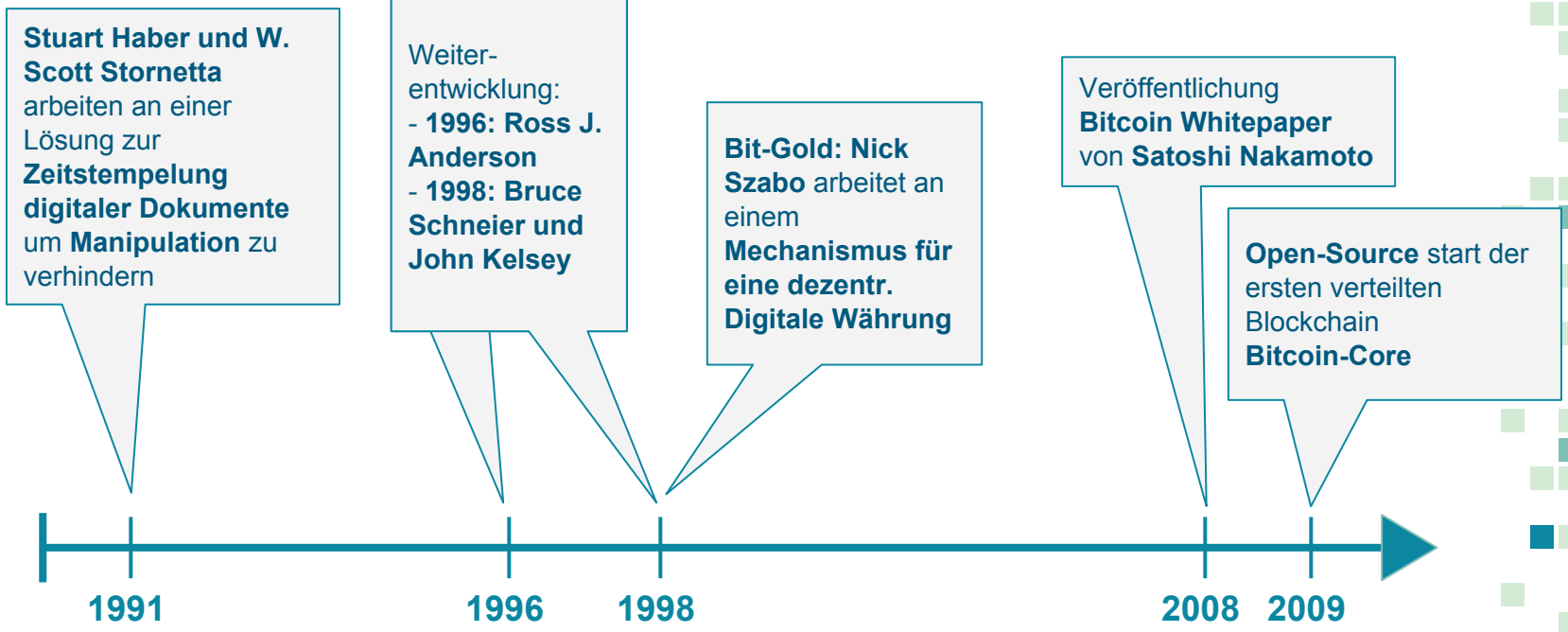
Quelle: http://learnmeabitcoin.com/guide/blocks

Mining

- Mining Netzwerk **bestätigt Transaktionen** und ist somit essentiell für das fortführen der Blockchain
- **Miner werden für ihre "Arbeit" belohnt** (z.B. mit Bitcoin). Transaktionen werden oft nach höhe der so genannten **"mining fee"** ausgewählt
- Mining ist unter anderem einer der **dezentralen Mechanismen**
- **Aufgabe ⇒ Hash Funktion:** Mathematisches Problem, welches **schwer zu lösen** ist, jedoch mit dem richtigen Ergebnis **einfach zu überprüfen** ist

2.
GESCHICHTE DER BLOCKCHAIN
Von 1991 bis 2019

GESCHICHTE DER BLOCKCHAIN



Satoshi Nakamoto

- **“Erfinder”** der Kryptowährung **Bitcoin**
- Veröffentlicht am **9. Januar 2009 die Bitcoin Software**
- **Bis 2010 aktiv an der Bitcoin-Core Entwicklung beteiligt**, danach übertrug Satoshi das Repository, die Bitcoin Domain und weiteres an Gavin Andresen
- Es ist **nicht bekannt**, welche Person oder Personengruppe hinter dem Pseudonym steckt
- **Viele Versuche** herauszubekommen wer Satoshi ist:
  - z.B.: Analyse seiner Texte um zwischen Britischem Englisch und Amerikanischem Englisch zu differenzieren, Aufstellen eines Diagramms anhand der Timestamps von Satoshis 500 Foren-Posts
- **Viele Vermutungen:** Nick Szabo, Dorian Nakamoto

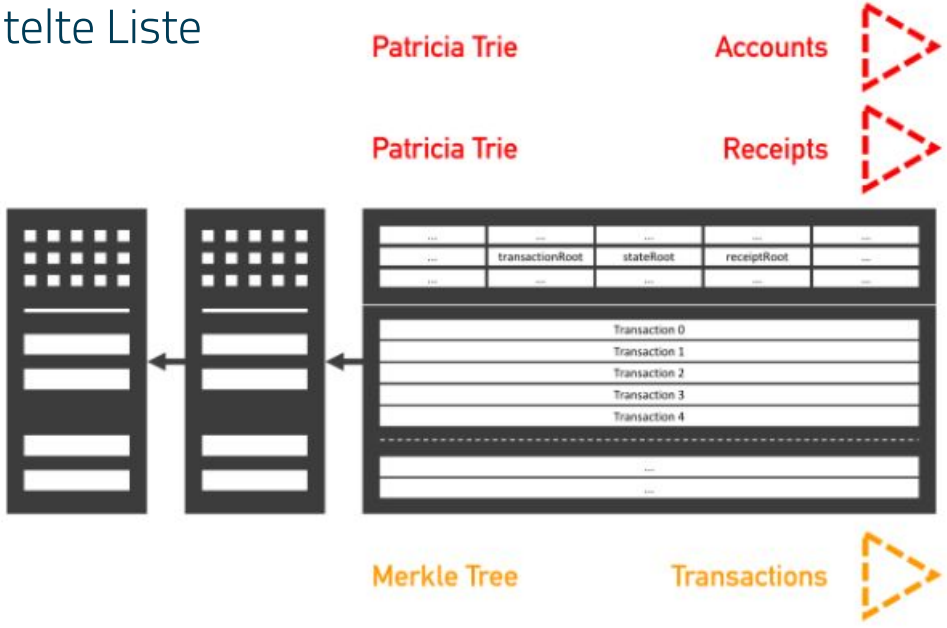
3.
BLOCKCHAIN HEUTE
Anhand verschiedener Technologien und Beispiele für deren Applikationen

Ethereum

- Ethers als Token (wie Bitcoins zu Bitcoin)
- Decentralized / Distributed / Permissionless / Tokenized
- Will Geschäftsmodelle mit Mittelsmännern ablösen
- Verträge in Form von SMART CONTRACTS
- 2 Account Arten
  - Normal Accounts
  - Contract Accounts
- 5 Blocks pro Minute!
- Entwickeln auf Morden (Testnet neben dem Mainnet)

Ethereum Blockchain

- Doppelt geschachtelte Liste



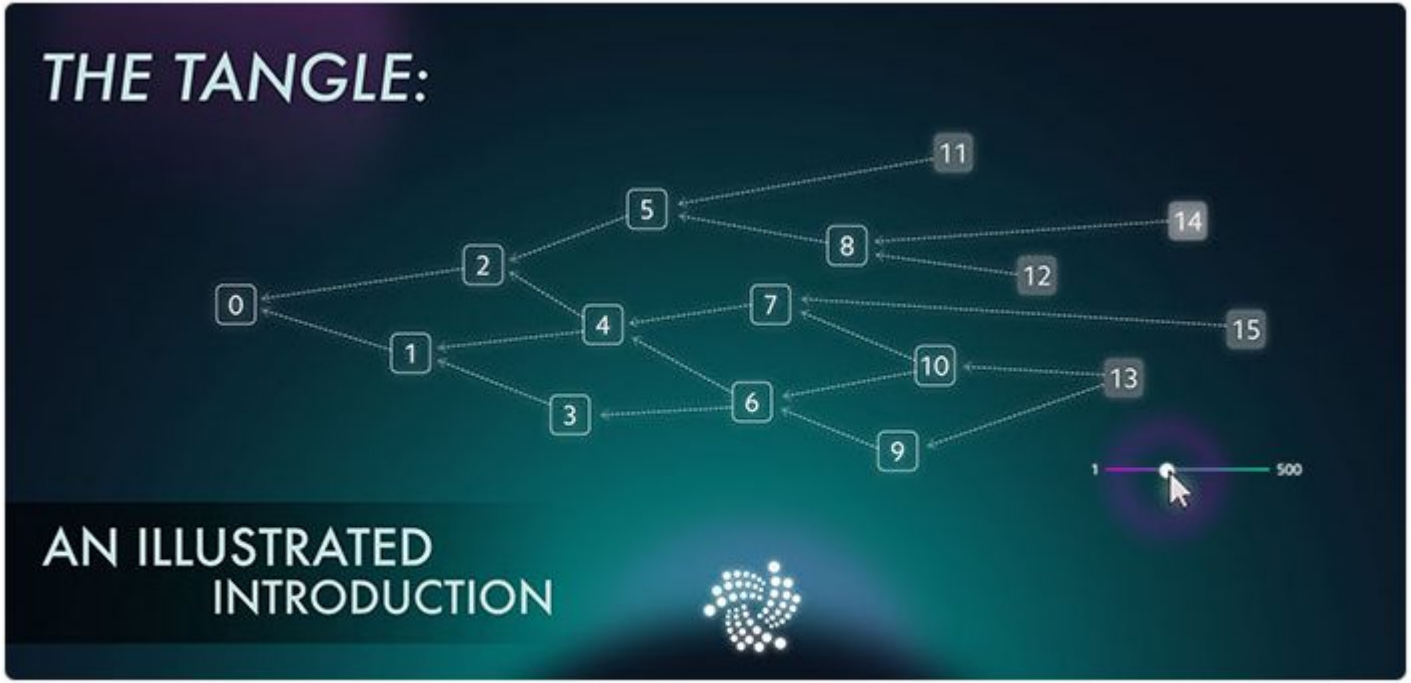
Ethereum Blockchain Application

- Investment Unternehmen DAO
  - Art Crowdfunding
  - Hinweise auf Sicherheitsrisiken
  - Hack über 50 Mio.
  - Hard Fork in Blockchain als Konsequenz

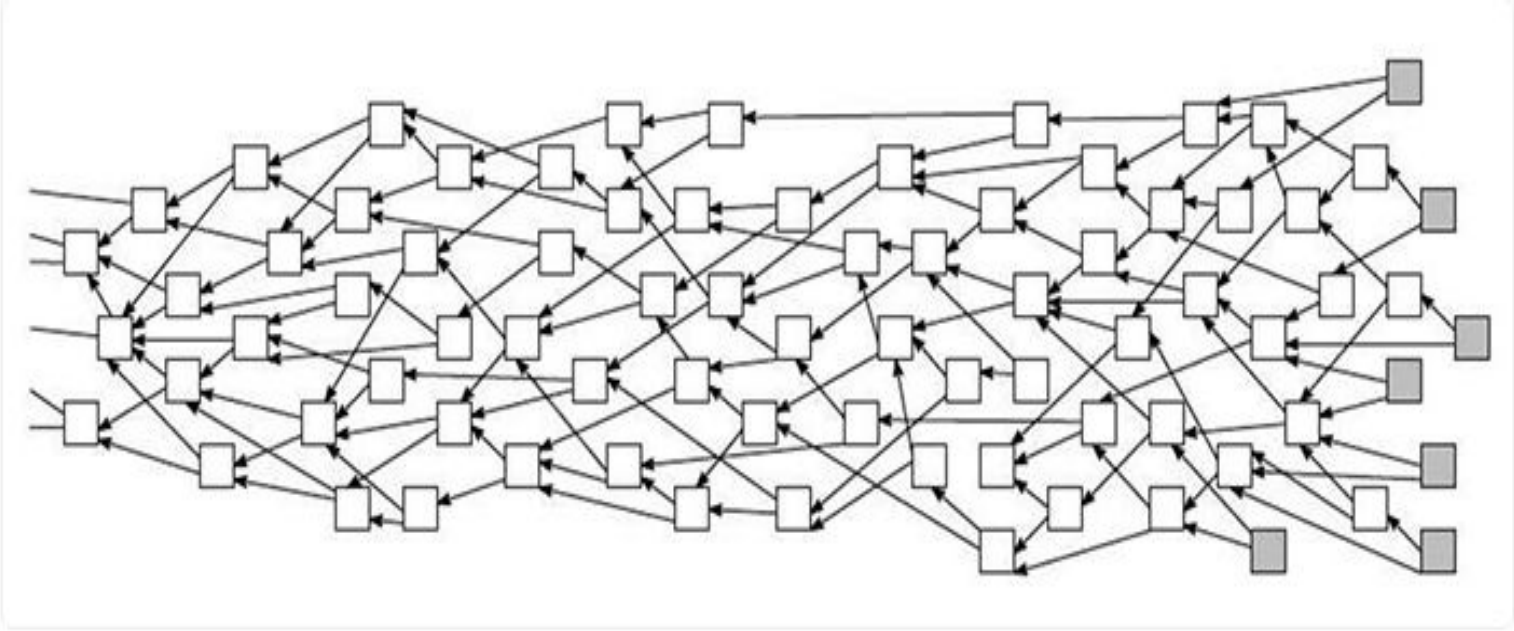
IOTA

- Für Internet of Things erdacht (IOT)
- Keine klassische Blockchain sondern Tangle
  - Gerichteter azyklischer Graph
  - Beliebig skalierbar
- Transaktionen als Knotenpunkte und zur Transaktionsbeglaubigung
- Beispiele für Applikationen:
  - Automobilindustrie
  - Smart Living

IOTA Tangle



Quelle: https://blog.iota.org/the-tangle-an-illustrated-introduction-c0a86f994445



Tangle Struktur / Quelle: IOTA Whitepaper

Monero

- Open Source
- Uneinsehbare Blockchain
  - Beliebte Zahlungsmethode Darknet
- Kompatibel für alle Systeme
- Hash-Algorithmus als Blockchain Grundlage
- Beispiel für Applikation:
  - Coin Hive

Dogecoin

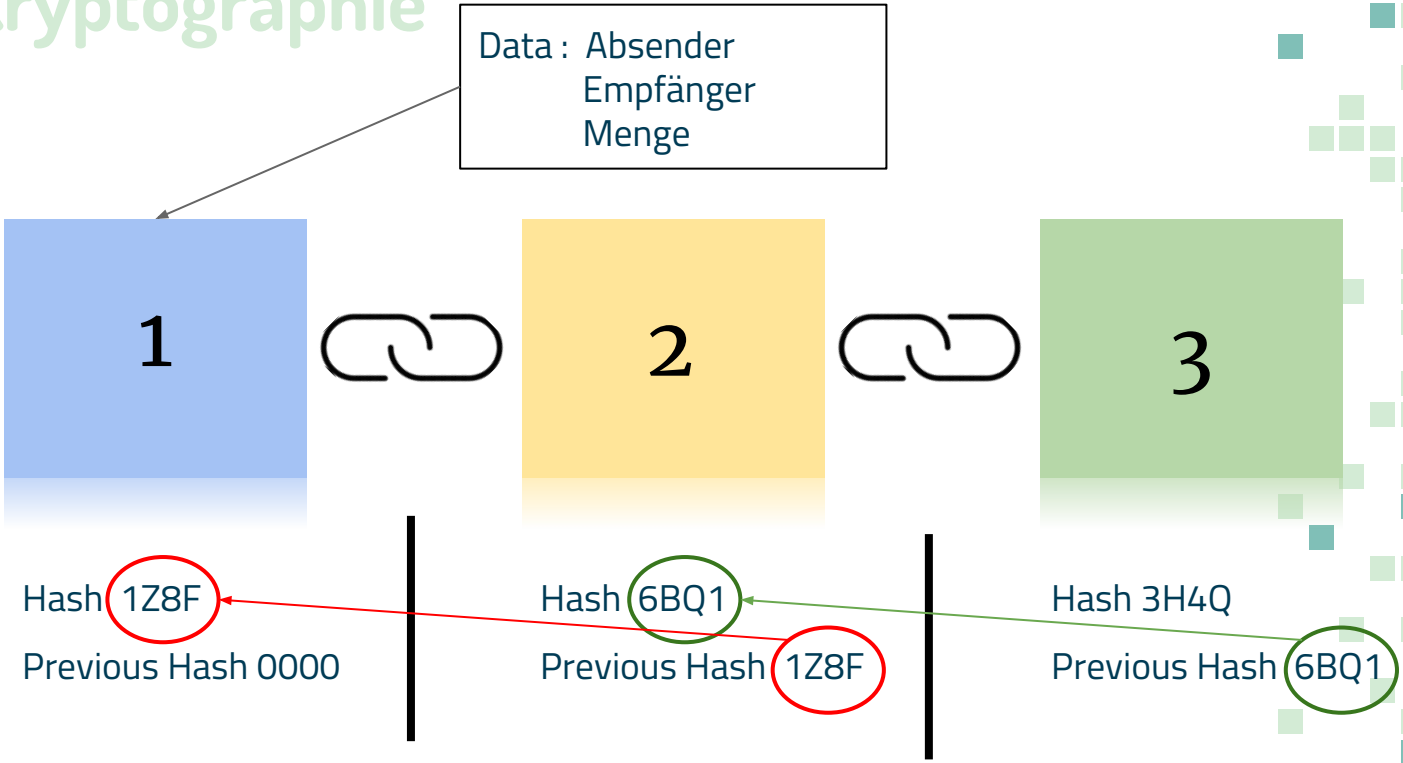
- Spaß Währung
- Peer-to-peer System
- Dezentrale Kryptowährung
- Beispiel für Verwendung:
  - Reddit oder Twitter

4.
PRO UND CONTRA

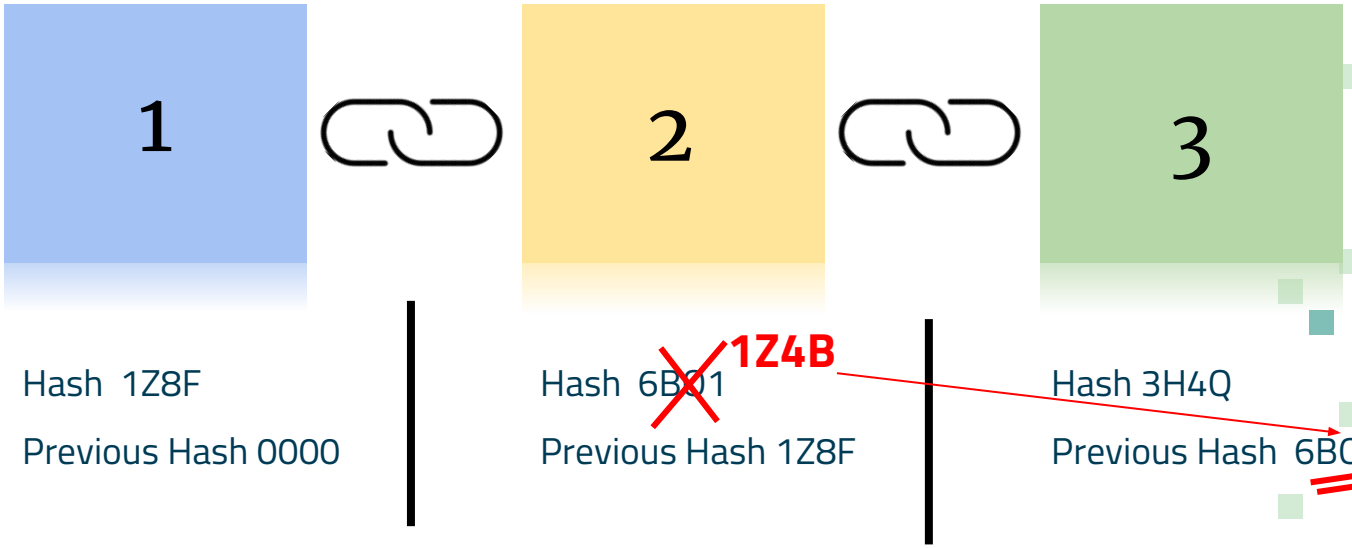
PRO

- Kryptographie
- Proof of Work
- Dezentralisierung

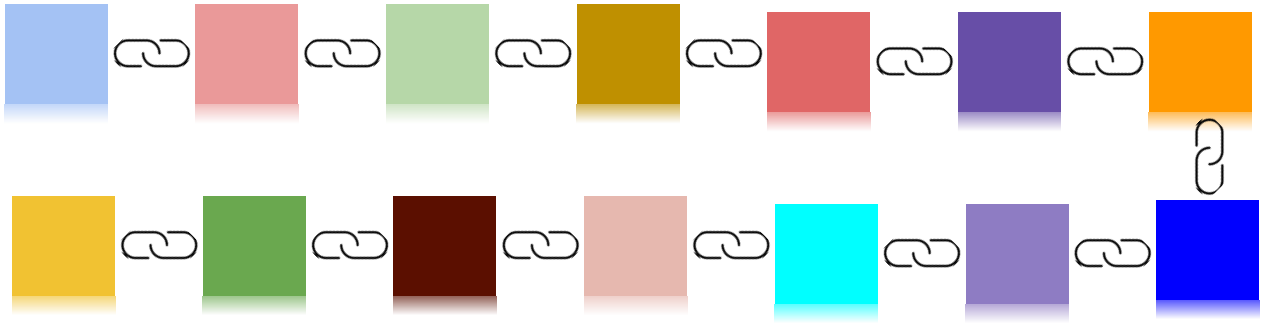
Kryptographie



Kryptographie



Proof of Work

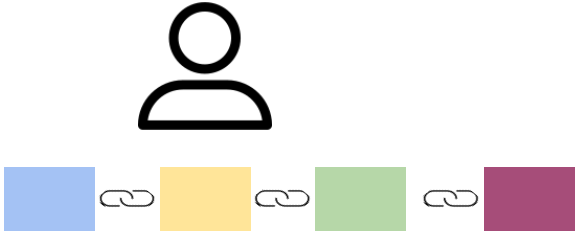


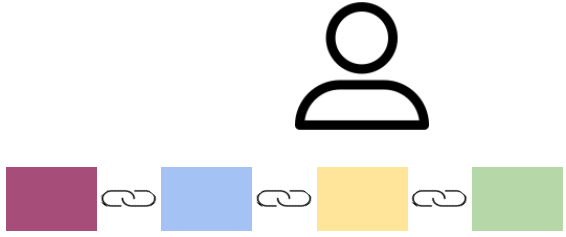
- Belohnung für das lösen einer Kryptografischen Aufgabe
- Difficulty Wert wird angepasst um Output konstant zu halten

Dezentralisierung

P2P-Network

new Block





CONTRA

- 51 % Attacke
- Datenschutz und Privatsphäre

51 % Attacke

- Angreifer tätigt Transaktion
- geheime alternative Fortsetzung der Blockchain erfolgt
- Coins werden an eine andere Adresse transferiert

Grund:

- überlegene Hashleistung
- mehr Blöcke können erzeugt werden
- längste Blockreihe wird bevorzugt
- Konkurrenz stirbt aus

Datenschutz und Privatsphäre

- Transaktionen weltweit einsehbar
- einfache Scripts lesen Transaktionen aus
- nicht Blockchain ist das Ziel, sondern Empfänger und Absender

Bitcoin Transaktionen

5.

LIVE CODING

Beispiel – TeamToast Coin

6.

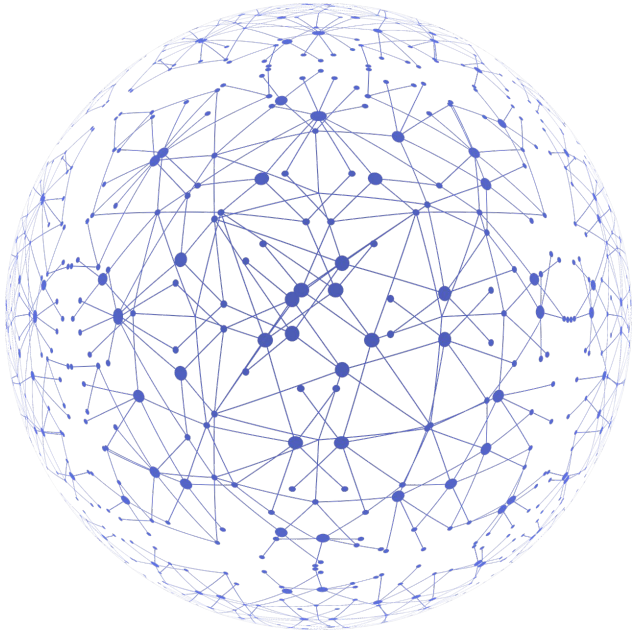
Anwendungsentwicklung

dApps & Smart Contracts

Decentralized Applications

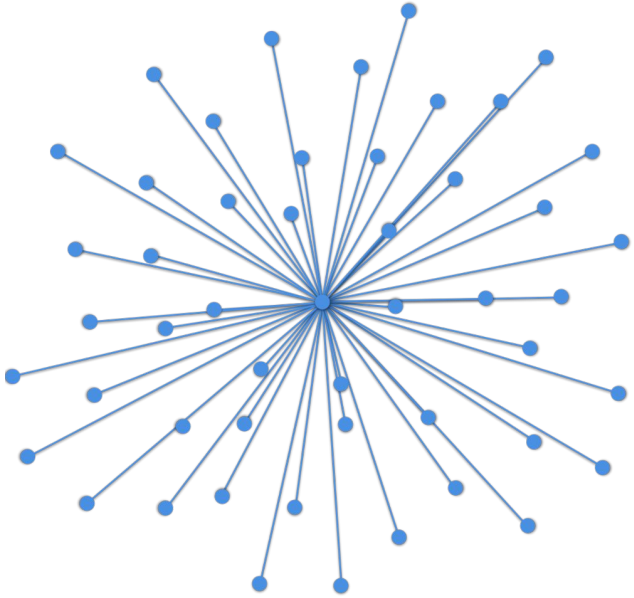
- Entwicklung von Software

  auf der Blockchain



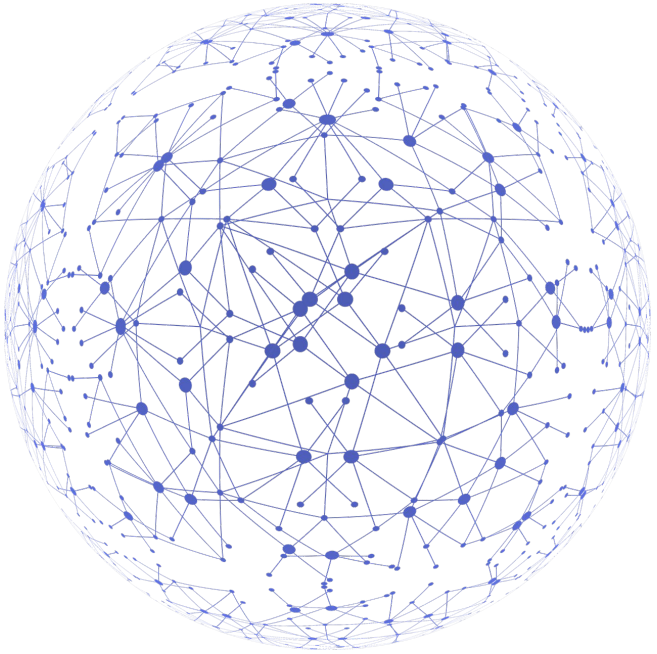
Centralized Applications

- Privatsphäre 👎
- Transparenz 👎
- Zensur 👎
- Community 👎
- Daten = 🤑

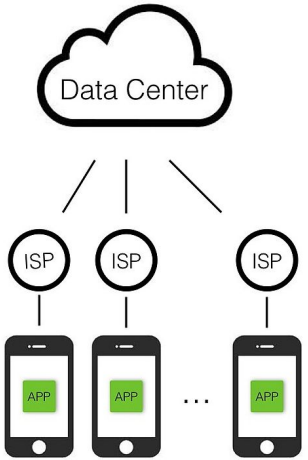


Dezentralisierung

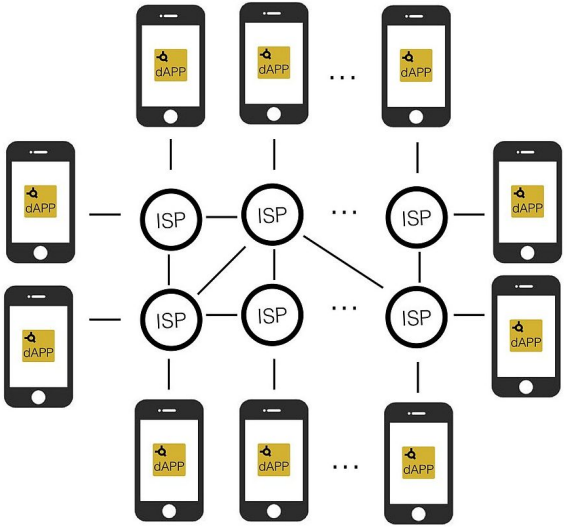
- Keine zentrale Autorität
- Keine Instanz hat Kontrolle über alle Daten und Prozesse



Apps


Data Center
ISP
ISP
ISP
APP
APP
APP

dApps


dAPP
dAPP
dAPP
dAPP
ISP
ISP
ISP
dAPP
dAPP
ISP
ISP
ISP
dAPP
dAPP
dAPP
dAPP

Decentralized Apps

- Open Source Entwicklung
- Blockchain-basiert
- Kryptographisch verschlüsselte Tokens

  -> Anreizmechanismus
- Ein Mechanismus der diese Tokens erzeugt

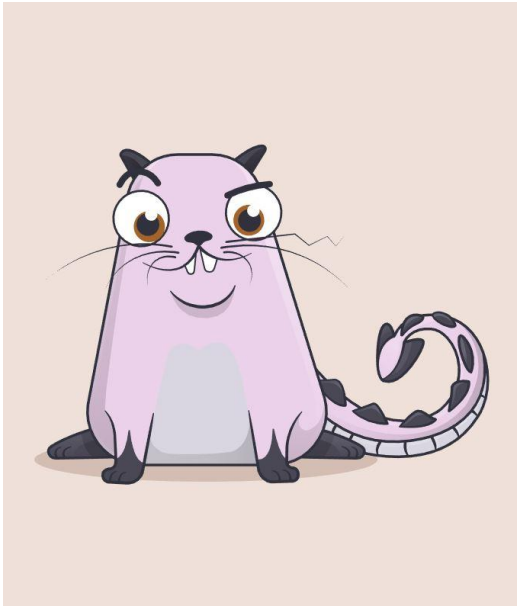
  -> Mining

Beispiele dApps -> Cryptokitties

- Onlinespiel auf der Blockchain
- Teuerste Katze:

  “Dragon”

  ~170.000 $



Beispiele dApps -> Decentraland

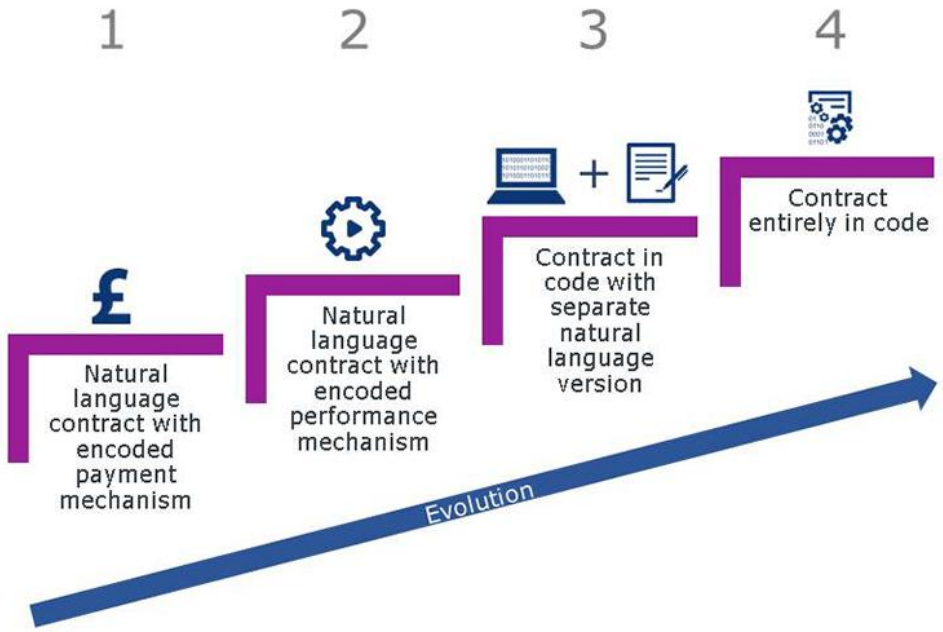
Smart Contracts

- Elektronische Verträge
- Automatisierte Aktivitäten
- Validierung durch Blockchain
- Prüfung der Konditionen Aller Vertragsteilnehmer

Smart Contracts -> Einsatzgebiete

- Smart Home
- Mieten
- Energiewirtschaft
- Banken
- Versicherungen
- Prozessoptimierungen

Smart Contracts -> Entwicklung

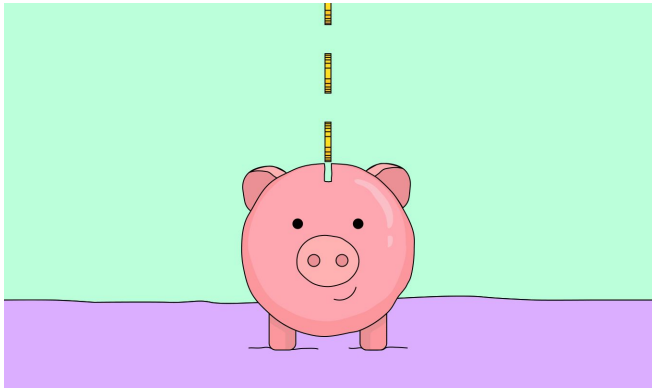


Smart Contracts -> Risiken

- Software ist nie fehlerfrei
- Veränderungen sind kompliziert
- Viel Verantwortung für Entwickler

Smart Contracts -> Chancen

- Papierkram sparen
- Prozesse optimieren
- Zeit sparen
- Geld sparen
- Ressourcen sparen
- Sicherheit optimieren



7.
CHANCEN UND HERAUSFORDERUNGEN
Anhand von Beispielen

CHANCEN **IN DER POLITIK**

- Authentifizierung der Identität der Wähler
- verlässliche Zahlen
- Blockchain-Tools als grundlegende Infrastruktur
- Erfassen von Stimmen durch Blockchain
    - überprüfbaren Prüfpfad
- “Follow my Vote”

followmyvote.com

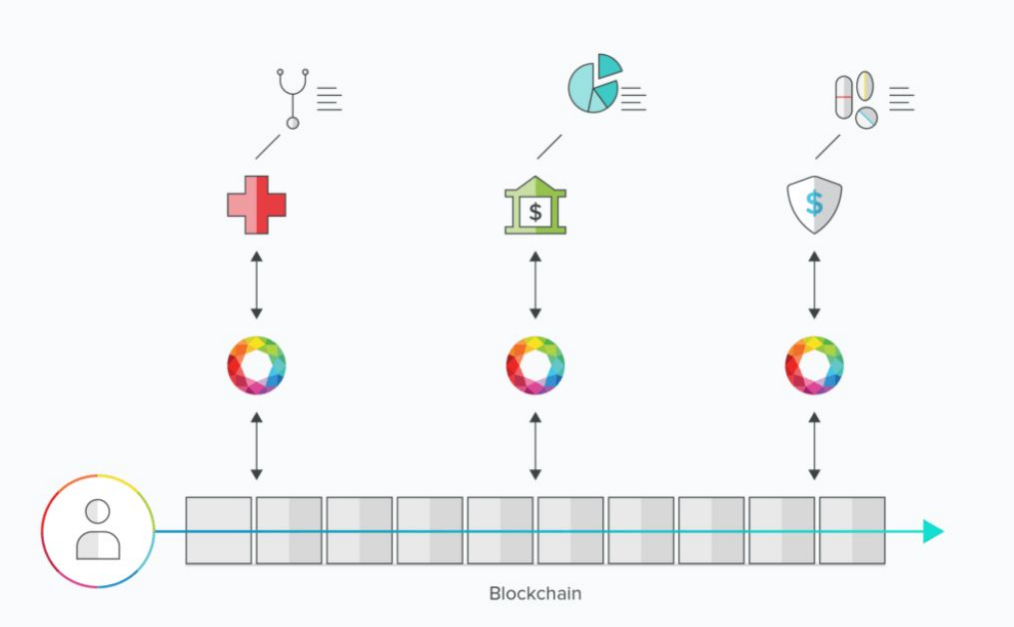
CHANCEN **IM GESUNDHEITSWESEN**

- Datenverlust
- Verbessertes Gesundheitswesen durch BCT
- Datentransparenz bietet höhere Wahrscheinlichkeit für genaue Diagnose
- “Gem”

GemOS

The blockchain operating system

- Alle Beteiligten (Kostenträger, Krankenhäuser etc) können Netzwerke gemeinsam nutzen



CHANCEN **IN DER WOHLTÄTIGKEIT**

- Genau Verfolgen an wen die Spende geht
- Rechenschaft und Transparenz
- Dauerhafte Dokumentation
- “GiveTrack”

CHANCEN **IN DER BILDUNG**

- Überprüfung der akademischen Nachweise weitgehend ein manueller Prozess
- Verifikationsverfahren
- “Sony Global Education”

CHANCEN **FÜR DIE UMWELT**

- Blockchain hilft dabei, die Ozeane aufzuräumen
- Token gegen Waren

plasticbank

HERAUSFORDERUNGEN

- Kriminalität (Darknet)
  - Online Drogen- oder Waffenhandel
  - Geldwäsche

  - Anonymität hat auch Nachteile

HERAUSFORDERUNGEN

- Das “Minen” von Blockchains (Proof-of-Work) ist sehr Rechenaufwendig
- 0,2% des weltweiten Energieverbrauchs
- Es ist prognostiziert, dass der Energiekonsum in den folgenden Jahren weiter zunehmen wird

FAZIT

- revolutioniert den Umgang mit sensiblen Informationen
- Viele attraktive Optionen in der Zukunft

- Bewusstes Auseinandersetzen mit der Technologie
- Trotz Hype einen kühlen Kopf bewahren und sich auch der Risiken bewusst sein

DANKE!

Fragen?

Quellen:

https://www.youtube.com/watch?v=SSo_EIwHSd4
https://www.datenschutzbeauftragter-info.de/bitcoin-technische-grundlagen-der-kryptowaehrung/
https://www.btc-echo.de/tutorial/was-ist-proof-of-work-wie-funktioniert-konsens-mechanismus/
https://blockchainwelt.de/bitcoin-difficulty-einfach-erklaert/
https://netzpolitik.org/2018/perspektiven-auf-die-blockchain-vom-demokratischen-ansatz-bei-bitcoin-ist-nicht-mehr-viel-uebrig/
https://www.blockchain.com/de/btc/unconfirmed-transactions
https://www.youtube.com/watch?v=zVqczFZr124&t=536s
https://www.youtube.com/watch?v=HneatE69814

Blockchain, Mining und Geschichte
http://learnmeabitcoin.com/guide/blocks
https://de.wikipedia.org/wiki/Blockchain
https://www.coindesk.com/information/what-is-blockchain-technology
https://en.wikipedia.org/wiki/History_of_bitcoin
https://www.binance.vision/de/blockchain/history-of-blockchain
https://www.bitcoinmining.com/
https://medium.com/swlh/how-does-bitcoin-blockchain-mining-work-36db1c5cb55d
https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo

Quellen:

dApp
https://www.coindesk.com/information/what-is-a-decentralized-application-dapp
https://github.com/ethereum/wiki/wiki/White-Paper#applications
https://hackernoon.com/what-are-decentralized-applications-dapps-explained-with-examples-7ff8f2c4a460
https://blockchainwelt.de/dapp-dezentralisierte-app-dapps/
https://towardsdatascience.com/what-is-a-dapp-a455ac5f7def
https://www.nasdaq.com/article/what-does-decentralization-actually-mean-cm860065

Centraland
https://decentraland.org/#why-decentraland
https://www.youtube.com/watch?v=-HmXrOTEmxg

Cryptokitties
https://kittysales.herokuapp.com/
https://www.cryptokitties.co/
Smart Contracts
https://wirtschaftslexikon.gabler.de/definition/smart-contract-54213
https://hackernoon.com/advantages-and-disadvantages-of-smart-contracts-in-financial-blockchain-systems-3a443145ae1c
https://www.pwc.de/de/newsletter/it-security-news/blockchain-und-smart-contracts.html

https://www.cbinsights.com/research/industries-disrupted-blockchain/
https://followmyvote.com/