Bitcoin, Ethereum & Co:
So funktionieren Kryptowährungen und Smart Contracts

Tobias Seyffarth
JCNetwork Alumniverein

Gemeinsame Vorstellung und Ihre Erwartungen an das Webinar.

- Wie heiße ich?
- Was studiere ich?
- In welchem Verein bin ich tätig?
- Was sind meine Erwartungen an den Workshop?
- …

Lernziele des Webinars.

- Sie kennen Funktionen und technische Realisierungen einer Blockchain.
- Sie verstehen die Funktionsweise einer Kryptowährung am Beispiel von Bitcoin.
- Sie verstehen die grundsätzliche Funktionsweise eines Smart Contracts am Beispiel von Ethereum.
- Sie können Anwendungsfälle für den Einsatz einer Blockchain erarbeiten und bewerten.

Inhalte des Webinars

1. Eine kleine Geschichte von Bitcoin & kryptografische Grundlagen
2. Gruppenarbeit 1: Wallets und Konsensalgorithmen
3. Blockchains der zweiten Generation und Smart Contracts
4. Gruppenarbeit 2: Anwendungsfälle für Blockchains
5. Weitere Themengebiete um Blockchain und Wrap-Up

Als Antwort auf die Finanzkrise wurde unter dem Pseudonym Nakamoto im Jahr 2008 die Kryptowährung Bitcoin vorgestellt.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

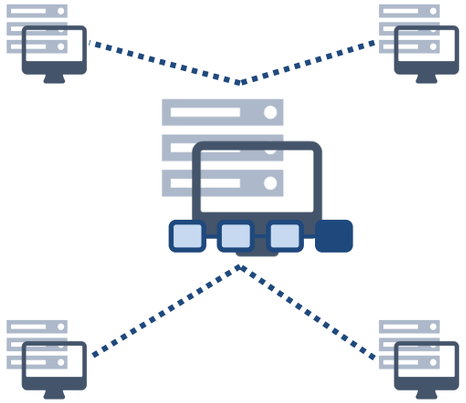
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions,

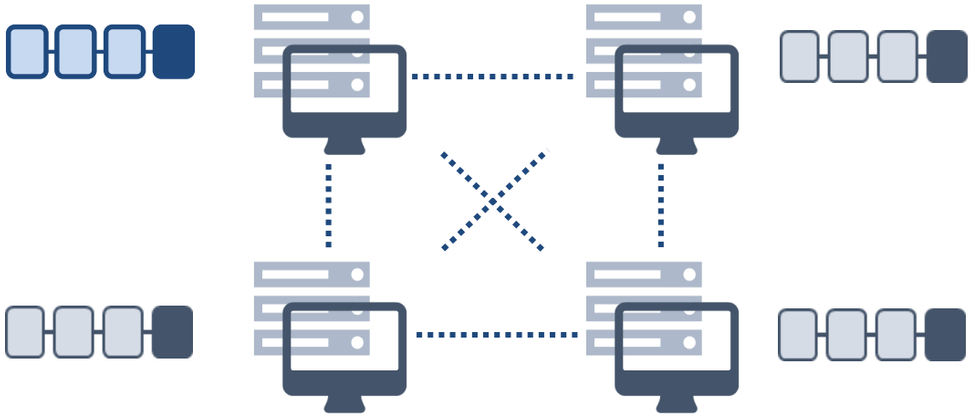
Nakamoto (2008)

Im Gegensatz zur klassischen Fiat-Währung wird eine Kryptowährung in einem dezentralen Netzwerk verwaltet.

Zentrale Verwaltung bei einer Fiat-Währung



Dezentrale Verwaltung bei einer Kryptowährung



Grundsätzlich basiert Bitcoin auf einem Distributed Ledger und einer verketten Transaktionsliste.

- Distributed Ledger
  - A *distributed ledger* is an append-only store of transactions which is distributed across many machines.
- Blockchain
  - A *blockchain* is a distributed ledger that is structured into a linked list of *blocks*. Each block contains an ordered set of transactions. Typical solutions use cryptographic hashes to secure the link from a block to its predecessor.

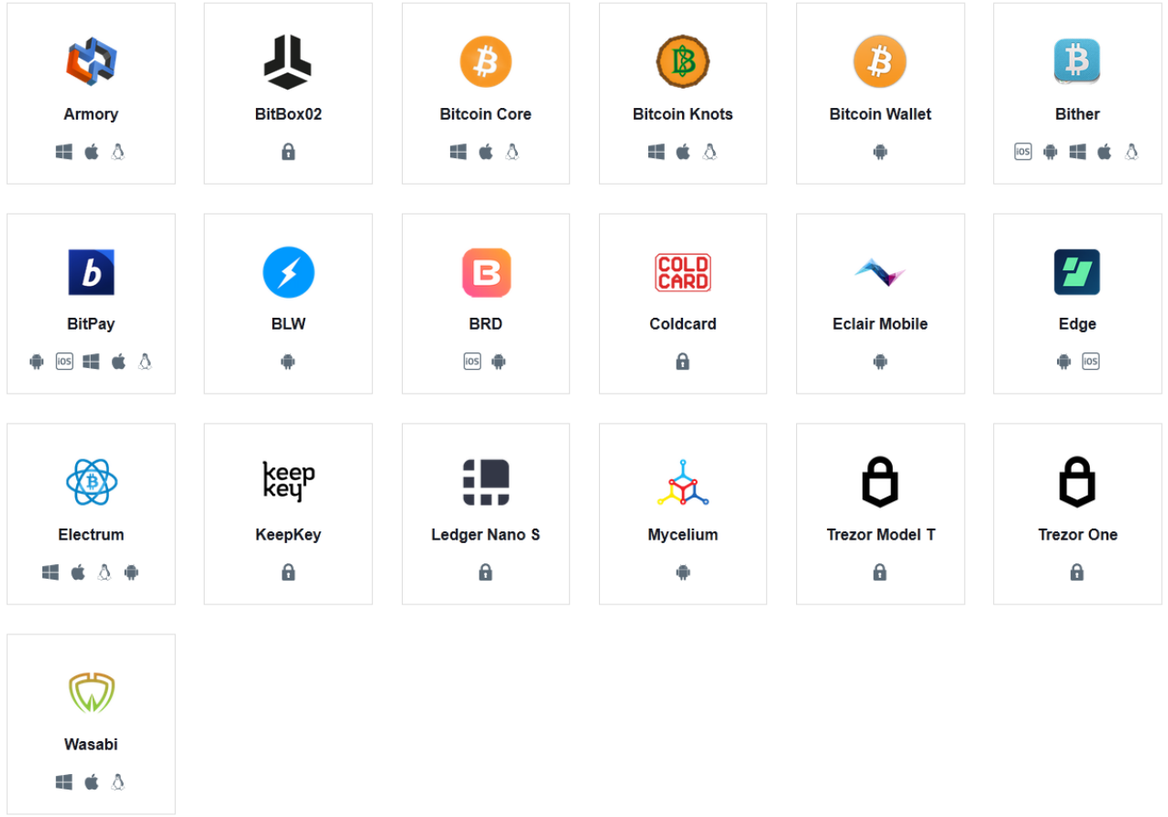
Neueste Blöcke Weitere Blöcke anzeigen

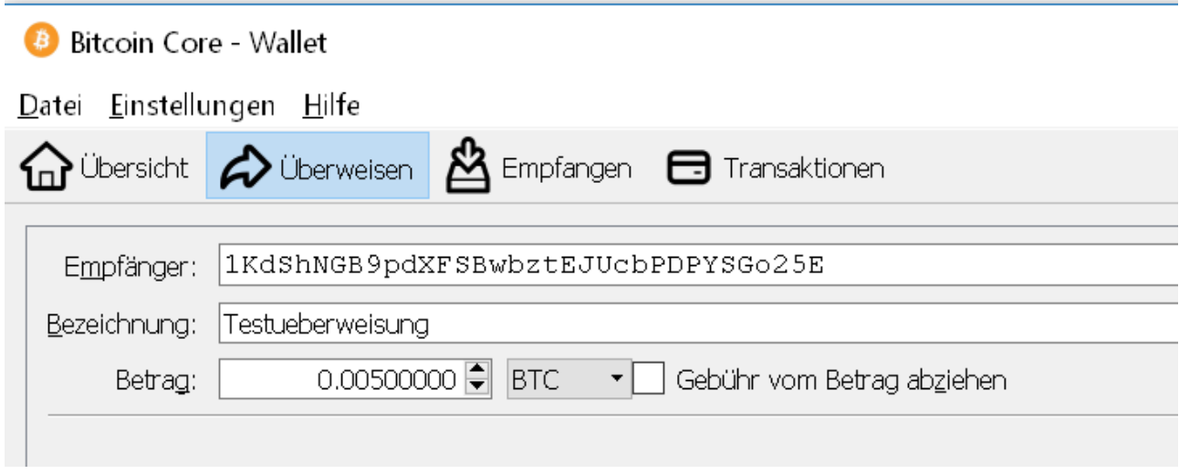
Nummer	Hash	Mined	Bergmann	Transaktionen	Größe
10200269	0x8cceac025b50dedb5430996de7ff…	19 seconds	0x4c549990a7ef3fea8784406c1eecc…	180	36,303 bytes
10200268	0xfa95c53db38e9e80c80f868bc810…	1 minute	0x829bd824b016326a401d083b33d…	169	39,081 bytes
10200267	0xc35c9b4d8b0af3c9932511cc137b…	1 minute	0x06b8c5883ec71bc3f4b332081519…	185	40,765 bytes
10200266	0xa5c5e97e288ae7caae65565a39c1…	1 minute	0x829bd824b016326a401d083b33d…	254	76,086 bytes
10200265	0x3b77f4c0f5ba3e0f7677f97fa3cb9…	1 minute	0x06b8c5883ec71bc3f4b332081519…	60	14,451 bytes
10200264	0x680df05a6e0bfc4072cc258692c6…	2 minutes	0x5a0b54d5dc17e0aadc383d2db43b…	106	23,393 bytes
10200263	0x748c872df01406054d15e5d05d8…	2 minutes	0xea674fdde714fd979de3edf0f56aa…	83	25,832 bytes
10200262	0x1106ad4b6851fa49d0a479154985…	2 minutes	0x829bd824b016326a401d083b33d…	120	25,205 bytes
10200261	0x15c353cb1574bd459e77a7a4ab07…	2 minutes	0x5a0b54d5dc17e0aadc383d2db43b…	97	35,270 bytes
10200260	0x9d825cadb52f9009f1b375a67897…	2 minutes	0xea674fdde714fd979de3edf0f56aa…	179	38,445 bytes
10200259	0xe7114d033246a890ff321d6d4cfc…	3 minutes	0x9d6d492bd500da5b33cf95a5d610…	125	24,867 bytes
10200258	0x7dd3d4d236c59e08af1833f646e3…	3 minutes	0xea674fdde714fd979de3edf0f56aa…	141	38,899 bytes

Xu et al. (2019), S. 5

https://www.blockchain.com/explorer?view=eth_blocks

Zur Ausführung von Transaktionen wird ein Wallet benötigt.





https://bitcoin.org/en/choose-your-wallet

Wöhner/Seyffarth (2017), S. 903.

Technisch gesehen ist Bitcoin nichts neues, alle Basistechnologien existierten bereits.

Verteilte Datenhaltung

- Speichern eines identischen Datenbestandes auf mehreren Maschinen.
- Sicherstellen der Verfügbarkeit.

Asymmetrische Kryptografie

- Verschlüsseln und Signieren von Informationen.
- Sicherstellen der Vertraulichkeit von Informationen.
- Sicherstellen der Authentizität von Teilnehmern.

Hash

- Abbilden einer Zeichenfolge beliebiger Länge in eine Zeichenfolge fester Länge.
- Sicherstellen der Integrität von Informationen.

Nakamoto (2008)

Ein Hash ist eine Einwegfunktion.

- Eine Hash-Funktion ist eine (fast) kollisionssichere Einwegfunktion, die schnell auszuführen ist.
- Es ist praktisch unmöglich zu einem gegeben Ausgabewert y den Eingabewert x zu finden: h(x) = y
- Es ist praktisch unmöglich zu einem gegebenen Wert x einen Wert x‘ zu finden, der den selben Hashwert ergibt: h(x) = h(x‘), x!=x‘

Willkommen auf dem JCNetwork Webinar Day.	5905d5aeba653f959aa3a6ee2193d160867aaf149faf1c9b64a61f71d141a979
Willkommen auf dem JCNetwork Webinar Day!	b9b218810547230c436f7c1bdd75c8506d833b786db21e8b3d64f5c7e84c58bf
Willkommen auf dem JCNetwork Webinar Day! Vielen dank für Eure Teilnahme.	11306133e18f48513a68b913b9a5981d60b0b23cba9f1cca1925e57877f94541

Schneier (2015)

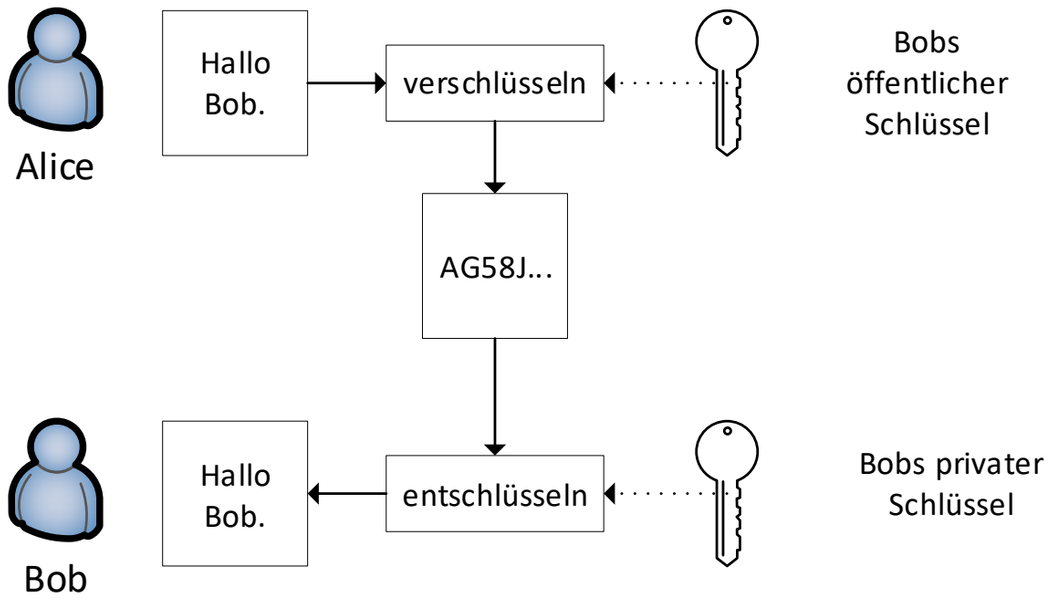
Bei der asymmetrischen Kryptografie gibt es einen öffentlichen und einen privaten Schlüssel.

- Das Schlüsselpaar (öffentlicher Schlüssel und privater Schlüssel) wird gemeinsam erzeugt.
- Der öffentliche Schlüssel kann an andere Teilnehmer verteilt werden.
- Der private Schlüssel verbleibt beim Ersteller des Schlüsselpaares.
- Einsatzzwecke sind das Verschlüsseln und Signieren von Informationen.

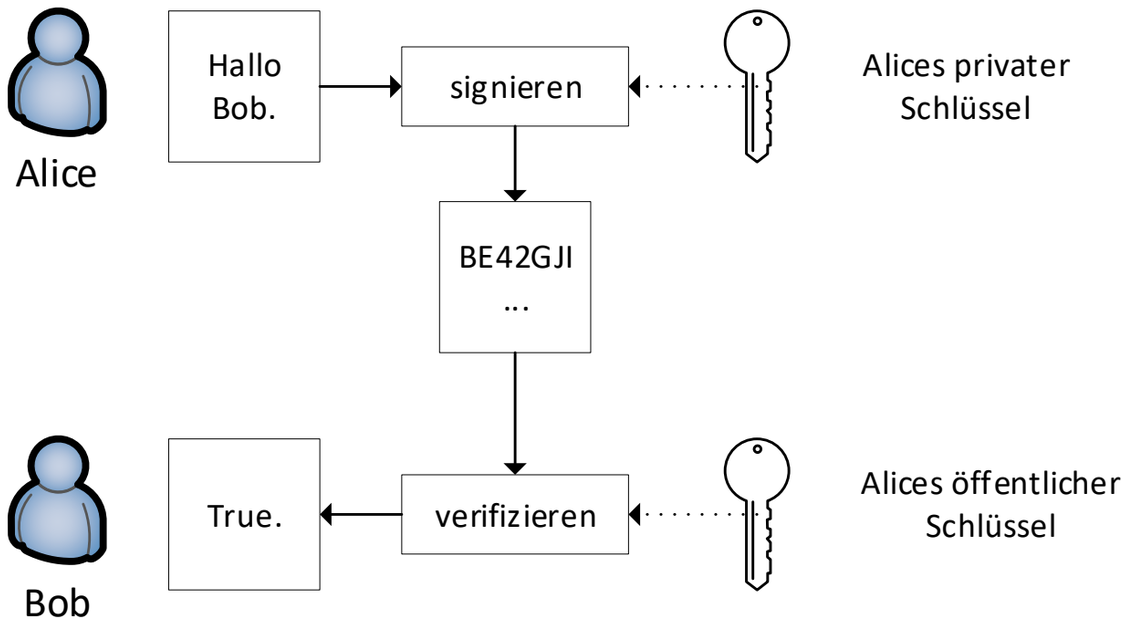
Schneier (2015)

Asymmetrischen Kryptografie kann zur Verschlüsselung und Signierung von Informationen verwendet werden.

Verschlüsseln von Nachrichten



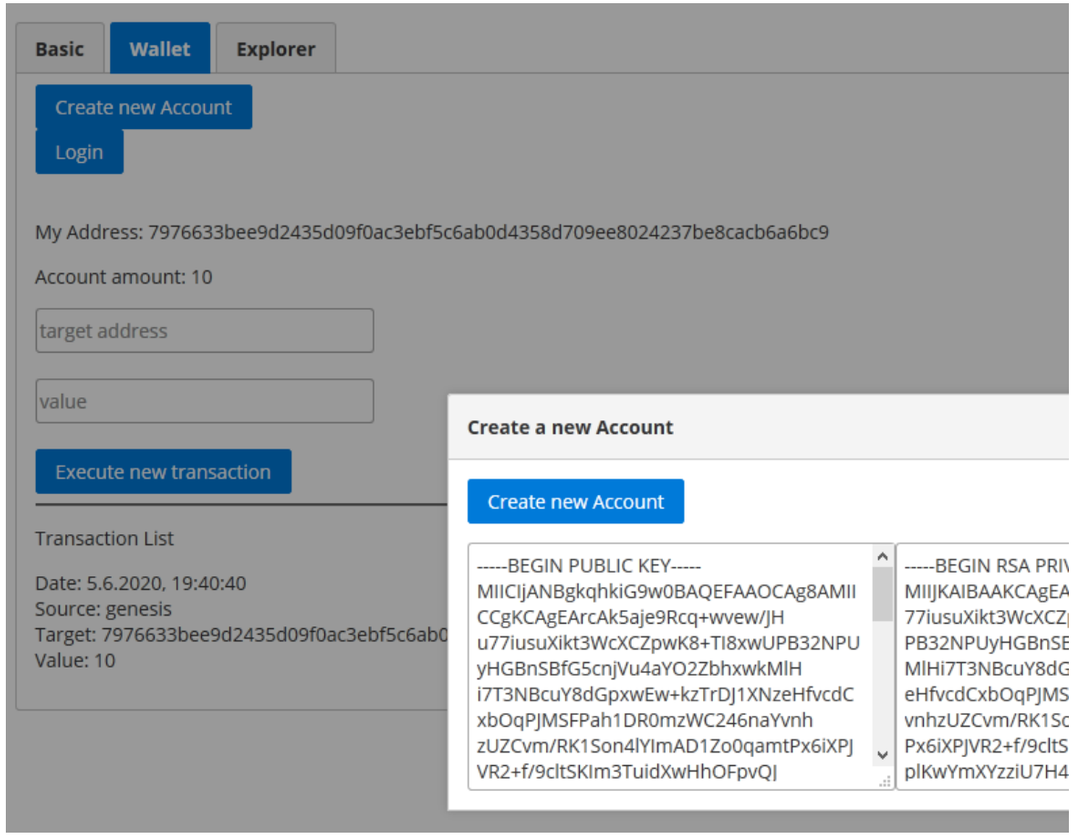
Signieren von Nachrichten



Schneier (2015)

Ein Blockchain-Demonstrator für die (kryptografischen) Grundlagen.

- Blockchain-Demonstrator verfügbar unter https://github.com/tobiasseyffarth/blockchain-demonstrator
- Basic Features
  - Hashen von Eingaben
  - Schlüsselgenerierung
  - Ver- und Entschlüsseln von Eingaben per RSA
- Demonstration
  - Erzeugen von Konten
  - Durchführen von Transaktionen zwischen Konten
  - Übersicht über alle Transaktionen in der Blockchain
  - Verifikation der Integrität der Blockchain



Die Konzepte der verteilter Datenhaltung, Hash und Kryptografie können auf Kryptowährungen übertragen werden.

Verteilte Datenhaltung

- Speichern eines identischen Datenbestandes auf mehreren Maschinen.
- Sicherstellen der Verfügbarkeit.

- → Speichern aller! Transaktionen auf jeder Maschine des Netzwerks.
- → Alle Transaktionen sind für jeden! einsehbar.

Hash

- Abbilden einer Zeichenfolge beliebiger Länge in eine Zeichenfolge fester Länge.
- Sicherstellen der Integrität von Informationen.

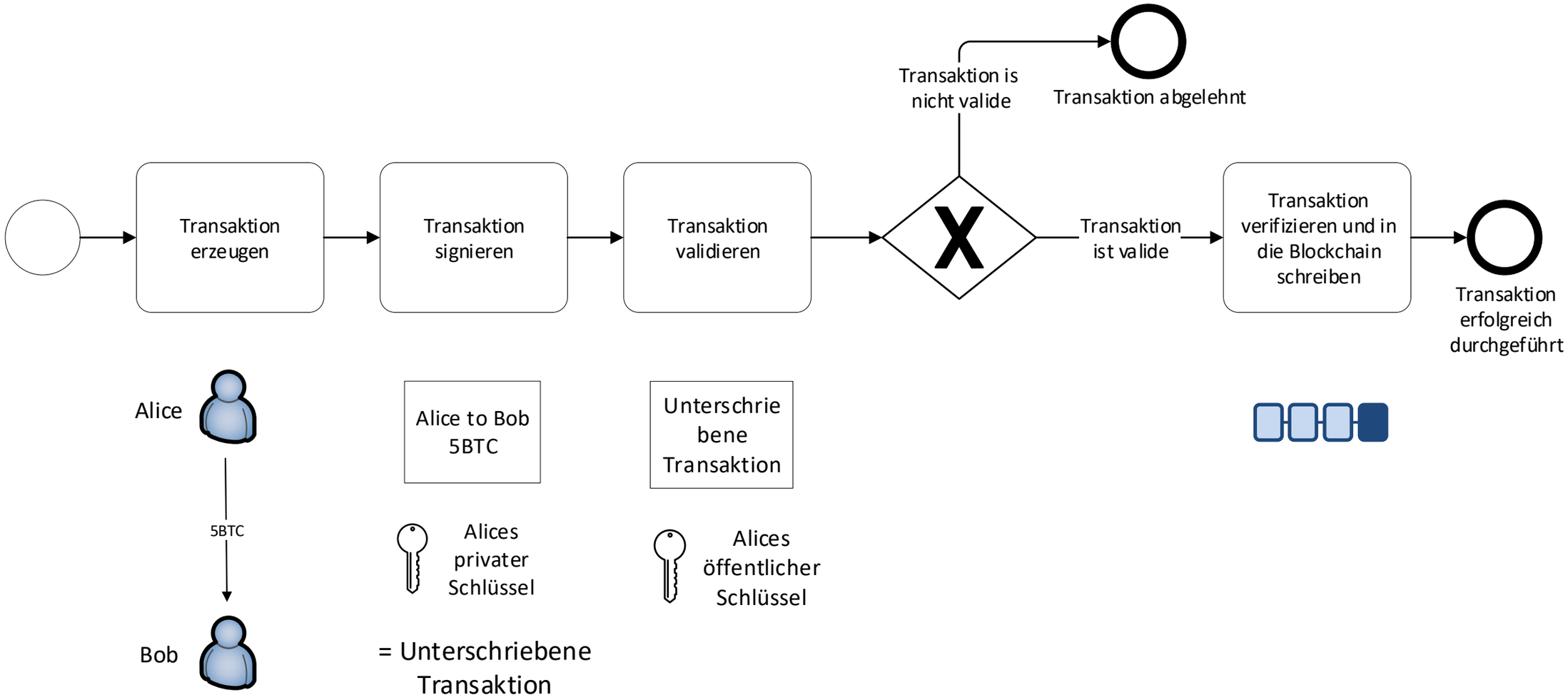
- → Adresse des Kontos: Hash des öffentlichen Schlüssels

Asymmetrische Kryptografie

- Verschlüsseln und Signieren von Informationen.
- Sicherstellen der Vertraulichkeit von Informationen.
- Sicherstellen der Authentizität von Teilnehmern.

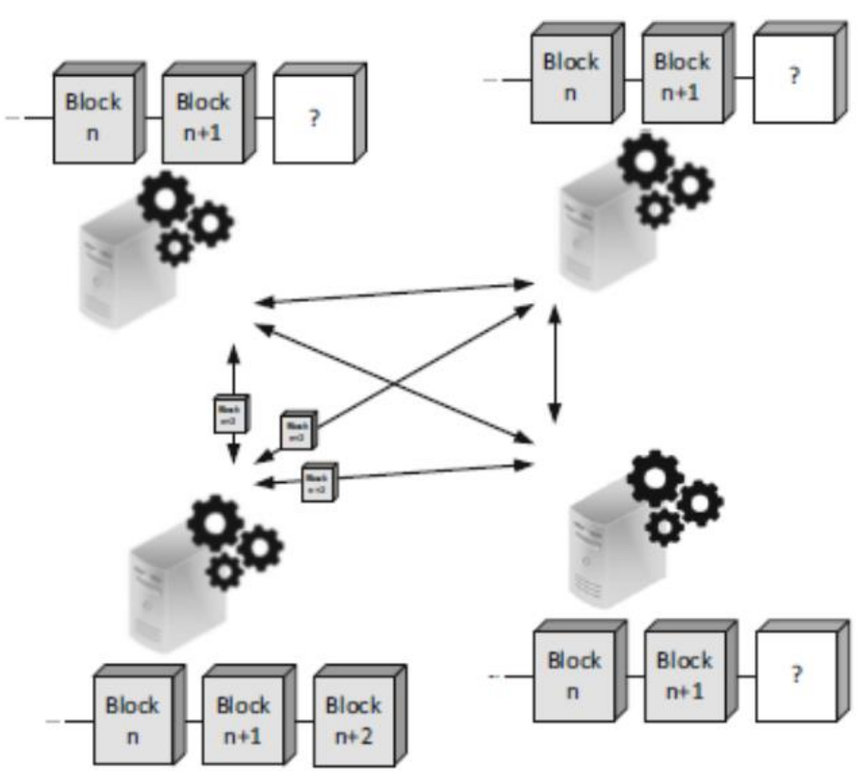
- → Privater Schlüssel: Nachweis über die Authentizität des Kontoinhabers

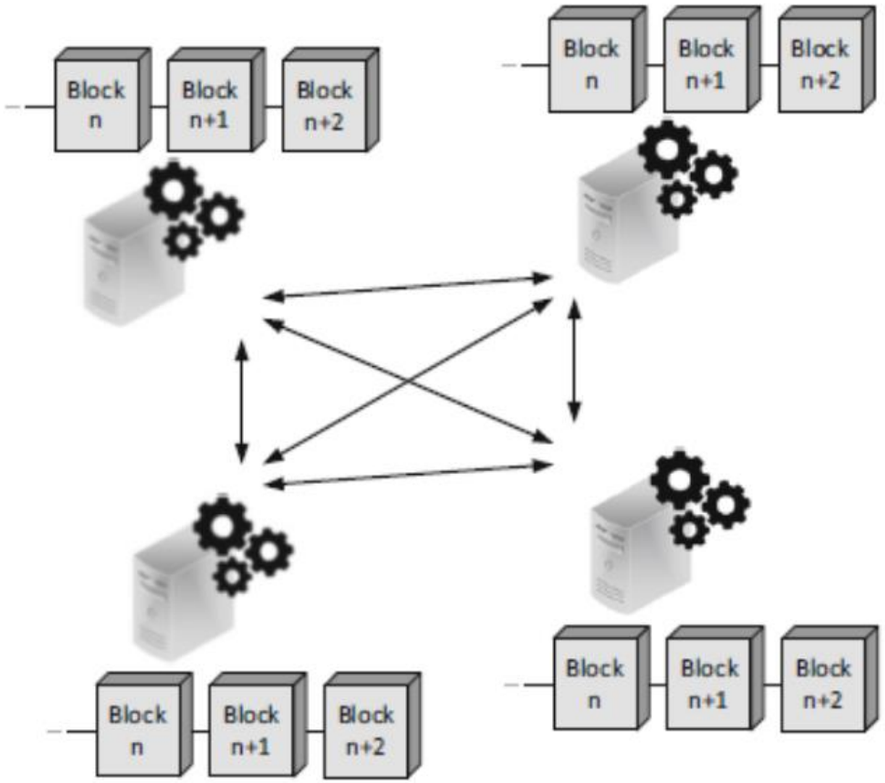
Ein einfacher Prozess zur Ausführung einer Transaktion.



Xu et al. (2019)

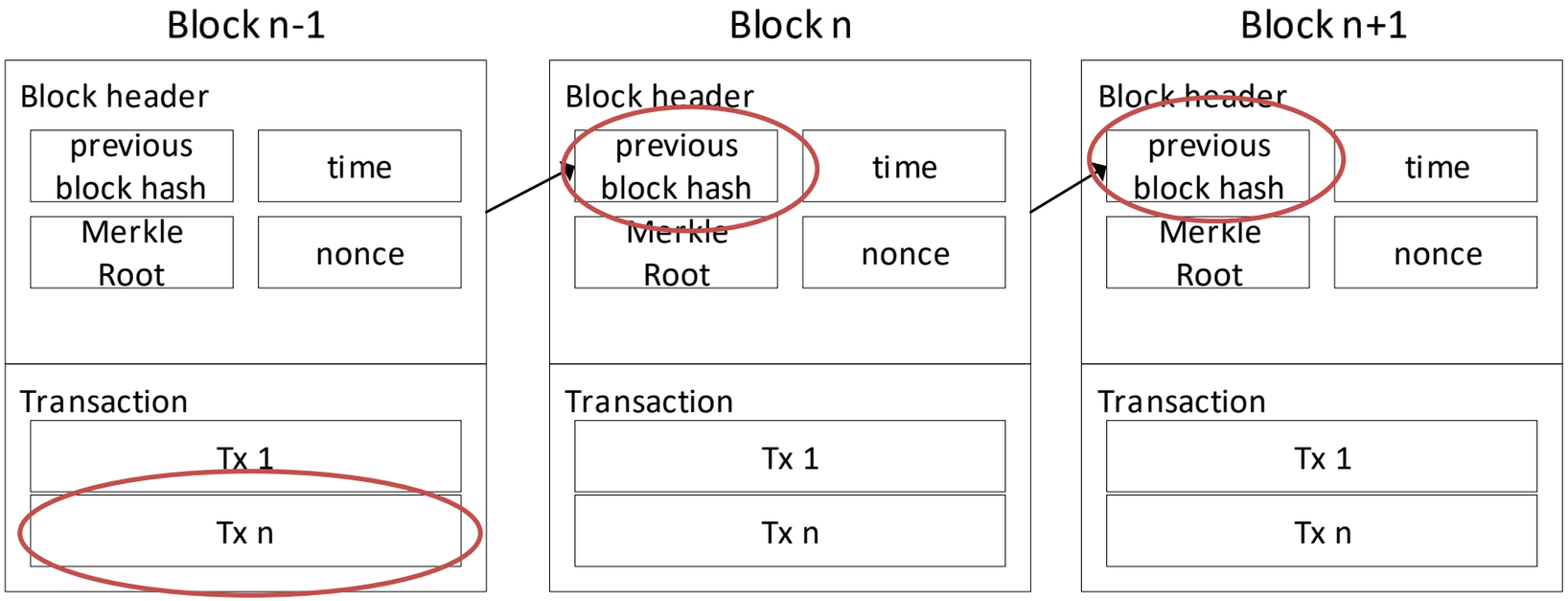
Miner schaffen durch bestimmte Algorithmen Konsens im Blockchain-Netzwerk.





Xu et al. (2019) S. 31 f.

Die Referenz auf den hash-Wert des Vorgängerblocks ermöglicht das „Verketten“ der Transaktionen.



5f86d081884c7d659a2feaa0c
55ad015a3bf4f1b2b0b822cd1
5d6c15b0f00a08

50303ae22b998861bce
3b28f33eec1be758a21
3c86c93c076dbe9f558c
11c752

5d61a03af4f77d870fc21e0
5e7e80678095c92d808cfb
3b5c279ee04c74aca13

a4e624d686e03ed2767
c0abd85c14426b0b115
7d2ce81d27bb4fe4f6f0
1d688a

a140c0c1eda2def2b83036
3ba362aa4d7d255c262960
544821f556e16661b6ff

Gruppenaufgabe 1: Wallets und Konsensmechanismen

Wallets
(Gruppe 1)

- Diskutieren Sie die Rolle des Wallets.
- Leitfragen:
  - Wozu werden Wallets benötigt?
  - Welche Arten von Wallets können unterschieden werden?
  - Wie können die Inhalte eines Wallets gesichert werden?
  - Welche Nachteile kann das Aufbewahren des Krypto-Guthabens in den Konten von Kryptobörsen haben?

Konsens-mechanismus Proof of Work
(Gruppe 2)

- Diskutieren Sie die Konsensmechanismen Proof of Work.
- Leitfragen:
  - Was ist die Basisidee des Konsensalgorithmus?
  - Wie erfolgt die Geldschöpfung?
  - Welche Rolle spielen die Transaktionsgebühren?
  - Was sind mögliche Vor- und Nachteile des Konsensalgorithmus?

25 min

Gruppenaufgabe 1: Wallets und Konsensmechanismen

Konsens-mechanismus Proof of Stake (Gruppe 3)

- Diskutieren Sie die Konsensmechanismen Proof of Stake
- Leitfragen:
  - Was ist die Basisidee des Konsensalgorithmus?
  - Wie erfolgt die Geldschöpfung?
  - Welche Rolle spielen die Transaktionsgebühren?
  - Was sind mögliche Vor- und Nachteile des Konsensalgorithmus?

25 min

Wallets – ein Lösungsvorschlag

Full Service Wallets

- a public key distribution program,
- a signing program,
- a networked program

Signing-Only Wallets

- Signatur-Wallet
- Networking Wallet

Offline Wallets

- Zwei Full Service Wallets
- Wallet 1 wird zur Erzeugung der Schlüssel verwendet
- Wallet 2 wird zur Publikation des Öffentlichen Schlüssels verwendet (manuell auf Wallet 1 importiert)

Konsensmechanismen – ein Lösungsvorschlag

PoW

- Finden einer Nonce, sodass Hash des Blocks ein ebstimmtes Aussehen aufweist
- Paralleles Suchen der Nonce durch Miner
- Höhe der Rechenleistung bestimmt die Wahrscheinlichkeit der erfolgreichen Blockerzeugung
- Transaktionsgebühren bestimmen die Wahrscheinlichkeit der Auswahl durch den Miner
- Dauer der Blockerzeugung ca. 10min
- Contra: langsam, hoher Energiebedarf

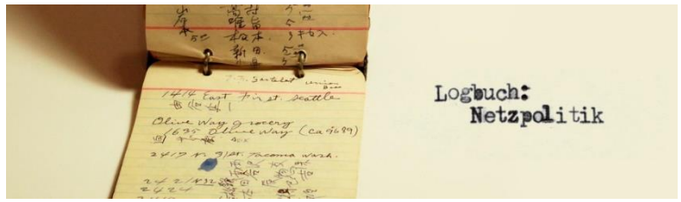
PoS

- Finden einer Nonce, sodass Hash des Blocks ein ebstimmtes Aussehen aufweist
- Miner, der den nächsten Block berechnen darf wird vorab bestimmt
- Mögliche Regeln: Menge der Token, Alter der Tokens
- Pro: schnell, geringerer Energiebedarf

Inhalte des Webinars

1. Eine kleine Geschichte von Bitcoin & kryptografische Grundlagen
2. Gruppenarbeit 1: Wallets und Konsensalgorithmen
3. Blockchains der zweiten Generation und Smart Contracts
4. Gruppenarbeit 2: Anwendungsfälle für Blockchains
5. Weitere Themengebiete um Blockchain und Wrap-Up

Break: Let‘s Talk about Podcast



Die Lage der Nation

https://www.kuechenstud.io/lagedernation/

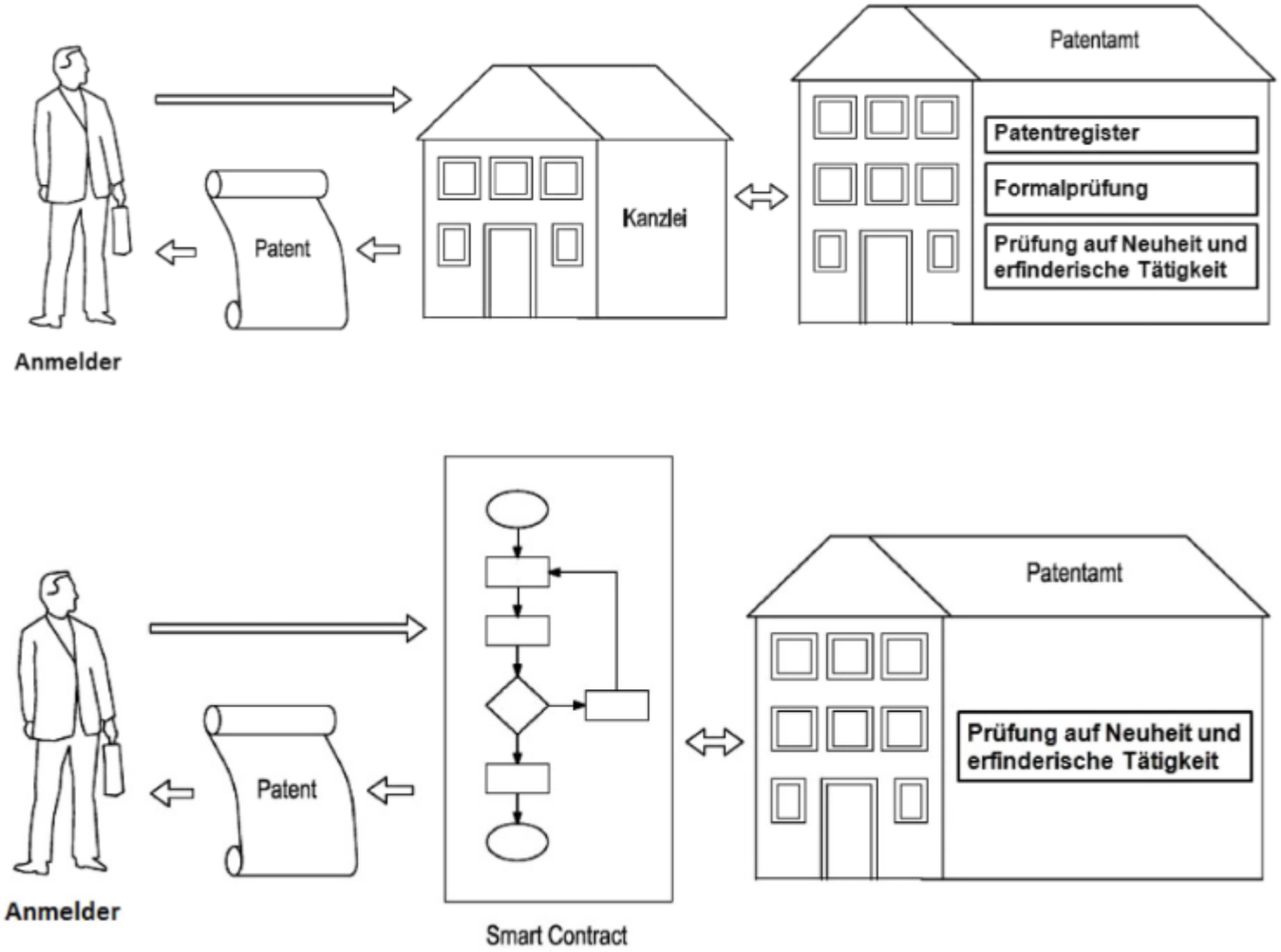
Logbuch Netzpolitik

https://logbuch-netzpolitik.de/

Forschergeist

https://forschergeist.de

Blockchains der zweiten Generation können Smart Contracts ausführen.



Meitinger (2017)

Smart Contract – (ausgewählte) Definitionen der Literatur.

- “Smart Contracts sind rechtliche Vereinbarungen, die sich IT-Technologien bedienen, um die eigene Durchsetzbarkeit sicherzustellen. Es werden durch Smart Contracts autonom Handlungen initiiert, die zuvor vertraglich vereinbart wurden.”

Meitinger (2017)

- “… is an instance of a computer program that runs on the blockchain, i.e., executed by all consensus nodes. A smart contract consists of program code, a storage file, and an account balance. Any user can create a contract by posting a transaction to the blockchain. The program code of a contract is fixed when the contract is created, and cannot be changed.”

Delmolino et al. (2016)

- “Smart contracts are scripts stored on the Blockchain. Since they reside on the chain, they have a unique address. We trigger a smart contract by addressing a transaction to it. It then executes independently and automatically in a prescribed manner on every node in the network, according to the data that was included in the triggering transaction.“

Christidis, Devetsikiotis (2016)

Aus den Definitionen können Eigenschaften von Smart Contracts abgeleitet werden.

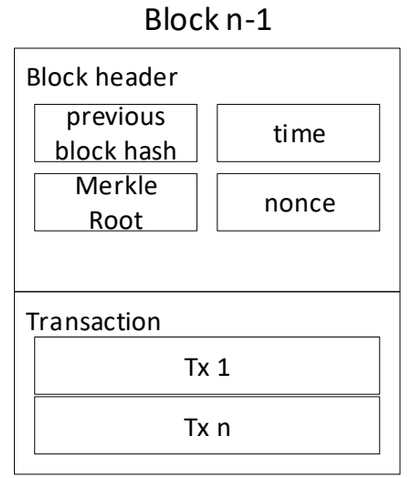
- Ein Smart Contract
  - … ist ein Computerprogramm, dass in der Blockchain ausgeführt wird.
  - … besteht aus einem unveränderbaren Programmcode, einem „Datenspeicher“ und einem Kontostand.
  - … kann von jedem Teilnehmer der Blockchain durch eine Transaktion erstellt werden.
  - … hat eine unique Adresse.
  - … kann durch eine Transaktion auf seine Adresse angesprochen werden.

```
pragma solidity >=0.4.0 <0.6.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```



https://solidity.readthedocs.io/en/v0.5.3/introduction-to-smart-contracts.html

Aus den technischen Grundlagen der Blockchain können ihre Eigenschaften abgeleitet werden.

Technical Underpinning	Main Features
Distributed Ledger	Transparency and Traceability
	Ensuring Availability of Transactions
	Decentral Management withtout a Third Party
Consensus Mechanism (Proof-of-Work)	Ensuring consistent Transaction
	Incentive
	Adjustment of Difficulty
Cryptographic Methods	Ensuring Authenticity of the Person Executing Transactions
	Ensuring Anonymity of the Person Executing and Receiving a Transaction
	Ensuring Integrity of Transactions
Public and Permissionless Shared Ledger	Non-discriminatory of Participants
	Universal Data Infrastructure
Smart Contracts	Automation
	Standardization
	Flexibility

Meironke et al. (2019)

Gruppenarbeit 2: Anwendungsfälle für Smart Contracts.

- Aufgabenstellung

  Erarbeiten Sie einen Anwendungsfall auf Basis einer Blockchain.

  Diskutieren Sie (1) die Problemstellung Ihres Anwendungsfalls, zeigen Sie (2) einen groben Vorschlag zur Problemlösung unter Berücksichtigung der Features von Blockchains und Smart Contracts.

- Annahmen
  - Netzwerk, in dem sich keiner vertraut
  - Referenzierte Features: Integrität, Verfügbarkeit, Authentizität, Transparenz

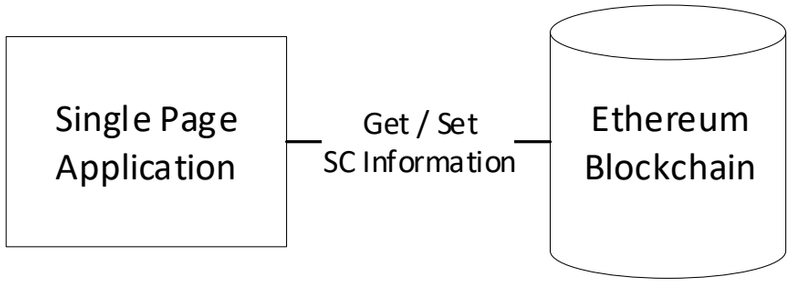
- Einige Anregungen für Gebiete möglicher Anwendungsfälle
  - Länderübergreifende Kooperationen
  - Pharmazie
  - Internet of Things
  - Digital Rights and IP Managment
  - Identitätsnachweis für staatliche Anwendungen
  - …

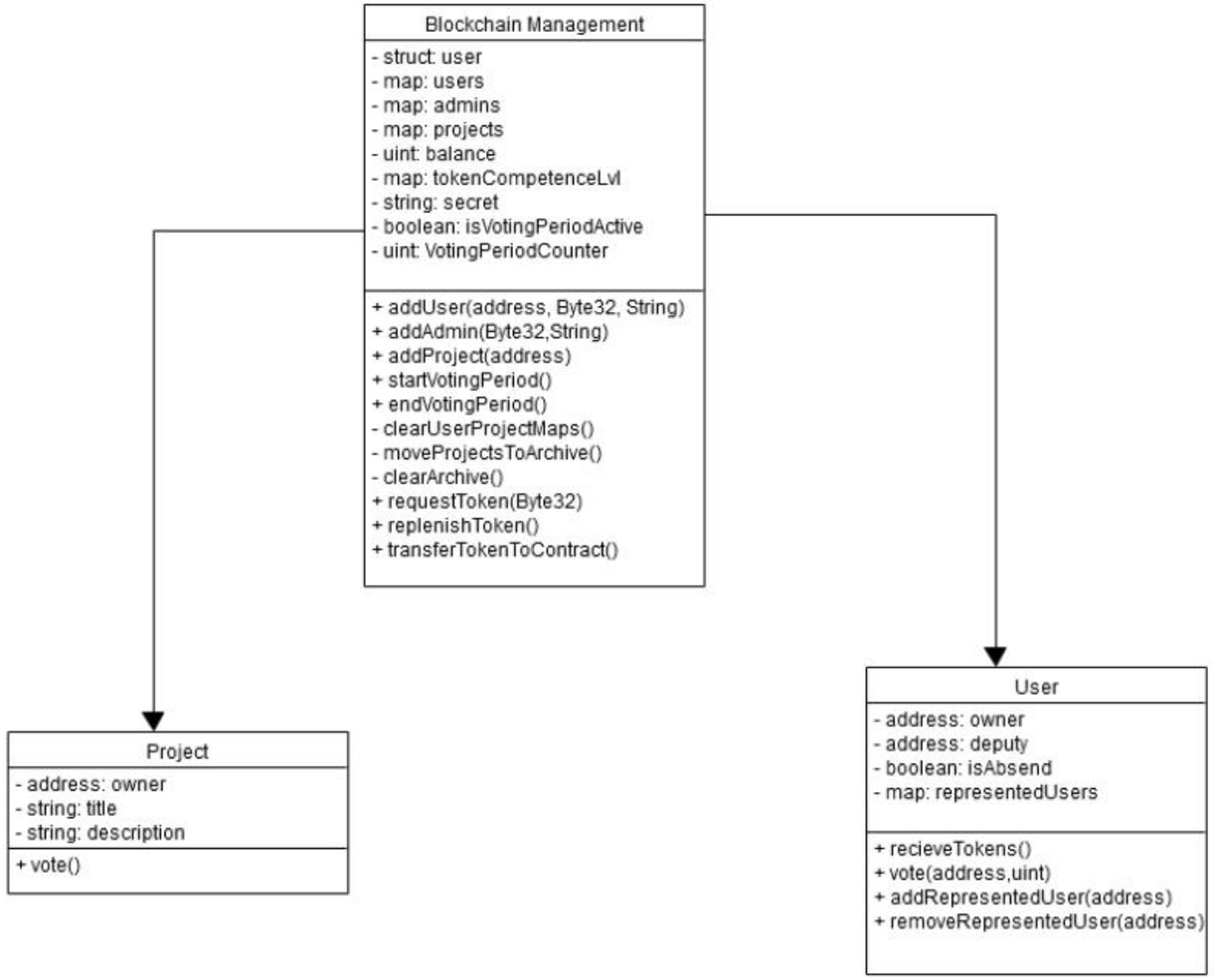
25 min

Ein beispielhfater Anwendungsfall: Elektronische Abstimmungen

- Ausgangslage:
  - Abstimmen über auszuführende Projekte in einem Unternehmen
  - Weitere Anforderungen: Vertretungsregelung, Stimmübertragung
  - Mitarbeiter:innen haben unterschiedliche Stimmengewichte

- Lösungsvorschlag

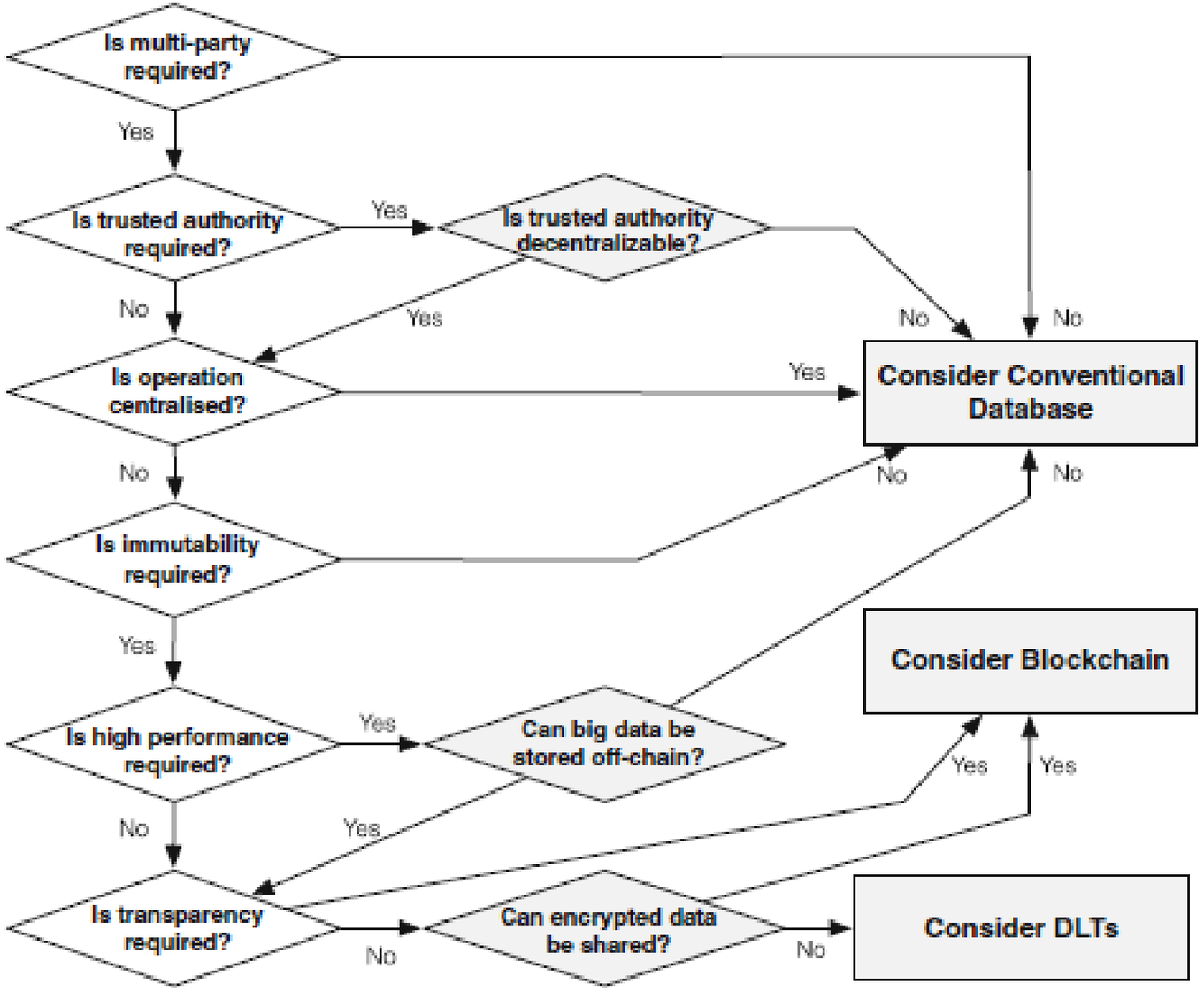




- Schwachstelle
  - Verteilung der initialen Schlüsselpaare

Ergebnisse eines studentischen Projektseminars

Ist die Blockchain überhaupt notwendig?



Lo et al. (2017)

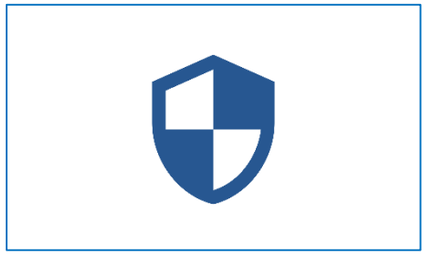
Inhalte des Webinars

1. Eine kleine Geschichte von Bitcoin & kryptografische Grundlagen
2. Gruppenarbeit 1: Wallets und Konsensalgorithmen
3. Blockchains der zweiten Generation und Smart Contracts
4. Gruppenarbeit 2: Anwendungsfälle für Blockchains
5. Weitere Themengebiete um Blockchain und Wrap-Up

Eine Auswahl weiterer relevanter Themengebiete rund um Blockchain.

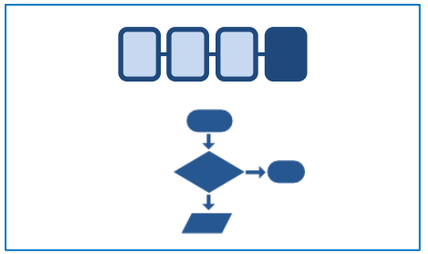
IT-Sicherheit

- 51% Angriff
- DDoS-Angriff
- …



Datenschutz

- Mögliche Grundlage: Artikel 17 DSGVO (Recht auf Löschung)
- Anonymisierte Speicherung von Daten
- Verschlüsselte Speicherung von Daten



Blockchain + X

- Anwenden der Blockchain-Technologie auf weitere Forschungsgebiete
- Geschäftsprozess-management
- Business Process Compliance

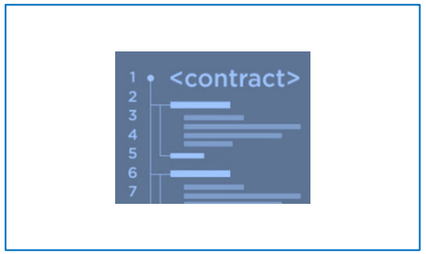
Wrap-Up des Webinars.

Kryptografie

- Kryptografische Hashfunktionen zur Verkettung von Blöcken
- Asymmetrische Verschlüsselungsverfahren zur Signierung der Transaktionen

Konsensalgorithmen

- Schaffen eines Konsens in einem dezentralen Netzwerk
- Proof of Work oder Proof of Stake als mögliche Verfahren/ Verfahrensklassen



Smart Contracts

- Computerprogramm, dass in der Blockchain ausgeführt wird
- Einsatz einer Blockchain nicht immer notwendig resp. sinnvoll?

Tobias Seyffarth

tobias@seyffarth.me

https://seyffarth.me

https://github.com/tobiasseyffarth

https://www.researchgate.net/profile/Tobias_Seyffarth

Literatur

- Christidis, K., Devetsikiotis, M., Blockchains and Smart Contracts for the Internet of Things, in: IEEE Access, 4. Jg. (2016), S. 2292–2303.
- Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E., Step by Step Towards Creating a Safe Smart Contract. Lessons and Insights from a Cryptocurrency Lab, in: J. Clark, S. Meiklejohn, P. Y.A. Ryan, D. Wallach, M. Brenner, K. Rohloff (Hrsg.), Financial Cryptography and Data Security, Berlin, Heidelberg 2016, S. 79–94.
- Lo SK, Xu X, Chiam YK, Lu Q (2017) Evaluating suitability of applying blockchain. In: The 22nd international conference on engineering of complex computer systems (ICECCS), Fukuoka
- Meironke, Anja; Seyffarth, Tobias; Damarowsky, Johannes (2019): Business Process Compliance and Blockchain. How Does the Ethereum Blockchain Address Challenges of Business Process Compliance? In: Wirtschaftsinformatik Proceedings 2019, S. 1894–1905.
- Meitinger, T. H., Smart Contracts, in: Informatik-Spektrum, 40. Jg. (2017), S. 371–375.
- Nakamoto, Satoshi (2008): Bitcoin. A Peer-to-Peer Electronic Cash System. Online verfügbar unter https://bitcoin.org/bitcoin.pdf, zuletzt geprüft am 05.06.2020.
- Schneier, Bruce (2015): Secrets and Lies: Digital Security in a Networked World.
- Wöhner, Thomas; Seyffarth, Tobias (2017): Kryptowährungen. In: WISU - Das Wirtschaftsstudium (8-9/2017), S. 903–906.
- Xu, Xiwei; Weber, Ingo; Staples, Mark (2019): Architecture for Blockchain Applications.