Blockchain Technologie

Margarethe Rosenova & Stefanie Steinberger

Paris Lodron Universität Salzburg

26. Januar 2018

Die Enstehung von Bitcoin

- 2008 wurde das Konzept von Bitcoin in einem White Paper von Satoshi Nakamoto vorgeschlagen.
- Die Idee einer kryptographischen Währung gab es schon seit 1998, die von Wei Dai als b-money und von Nick Szabo als bit gold bezeichnet wurde.
- Mit der Schöpfung der ersten 50 Bitcoins entstand am 3. Januar 2009 das Bitcoin Netzwerk.

Warum Kryptowährungen?

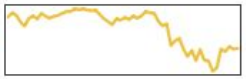
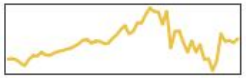
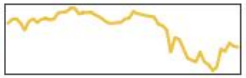
- Bisher bedarf es immer einer dritten Instanz/Partei, um elektronische Zahlungen abzuschließen.
- Zahlungen basieren auf einem Modell des Vertrauens und damit auch auf dessen Schwächen.
- Vertrauen in Banken, das Finanzsystem ect.

Kryptowährungen

Lösung:

- Transaktionen zweier Parteien untereinander ohne dritte Instanz ermöglichen
- Ein elektronisches Zahlungssystem basierend auf kryptographischem Nachweis(Proof of Work) anstatt auf Vertrauen.
- „With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.“
  - Satoshi Nakamoto

Kryptowährungen

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$193.612.433.911	$11.517,60	$18.703.000.000	16.810.137 BTC	11,51%	
2	Ethereum	$99.444.988.510	$1.024,62	$8.159.530.000	97.055.483 ETH	12,73%	
3	Ripple	$57.509.419.677	$1,48	$8.532.630.000	38.739.142.811 XRP *	39,64%	
4	Bitcoin Cash	$30.693.582.645	$1.814,26	$1.381.000.000	16.917.963 BCH	10,60%	
5	Cardano	$16.612.329.687	$0,640733	$1.587.590.000	25.927.070.538 ADA *	24,83%	
6	Litecoin	$10.522.504.173	$191,98	$1.346.680.000	54.810.133 LTC	14,37%	
7	NEO	$9.506.510.000	$146,25	$1.422.370.000	65.000.000 NEO *	29,61%	
8	NEM	$9.460.169.999	$1,05	$158.612.000	8.999.999.999 XEM *	28,36%	

Quelle: https://coinmarketcap.com

Blockchain Technologie

Blockchain:

Eine Kette von Blöcken, in welchen die Transaktionen gespeichert werden. Blöcke werden mithilfe einer Hashfunktion so miteinander verbunden, dass sie im Nachhinein nicht mehr verändert werden können. Die Blockchain ist wie ein riesiger öffentlicher Register (Ledger)

Transaktionen

- Jeder Nutzer im Bitcoin-Netzwerk besitzt eine Bitcoin-Wallet.
- Bitcoins sind keine physischen Objekte.
- Es gibt stattdessen nur Aufzeichnungen über Transaktionen zwischen verschiedenen Adressen und deren Guthaben.

Transaktionen

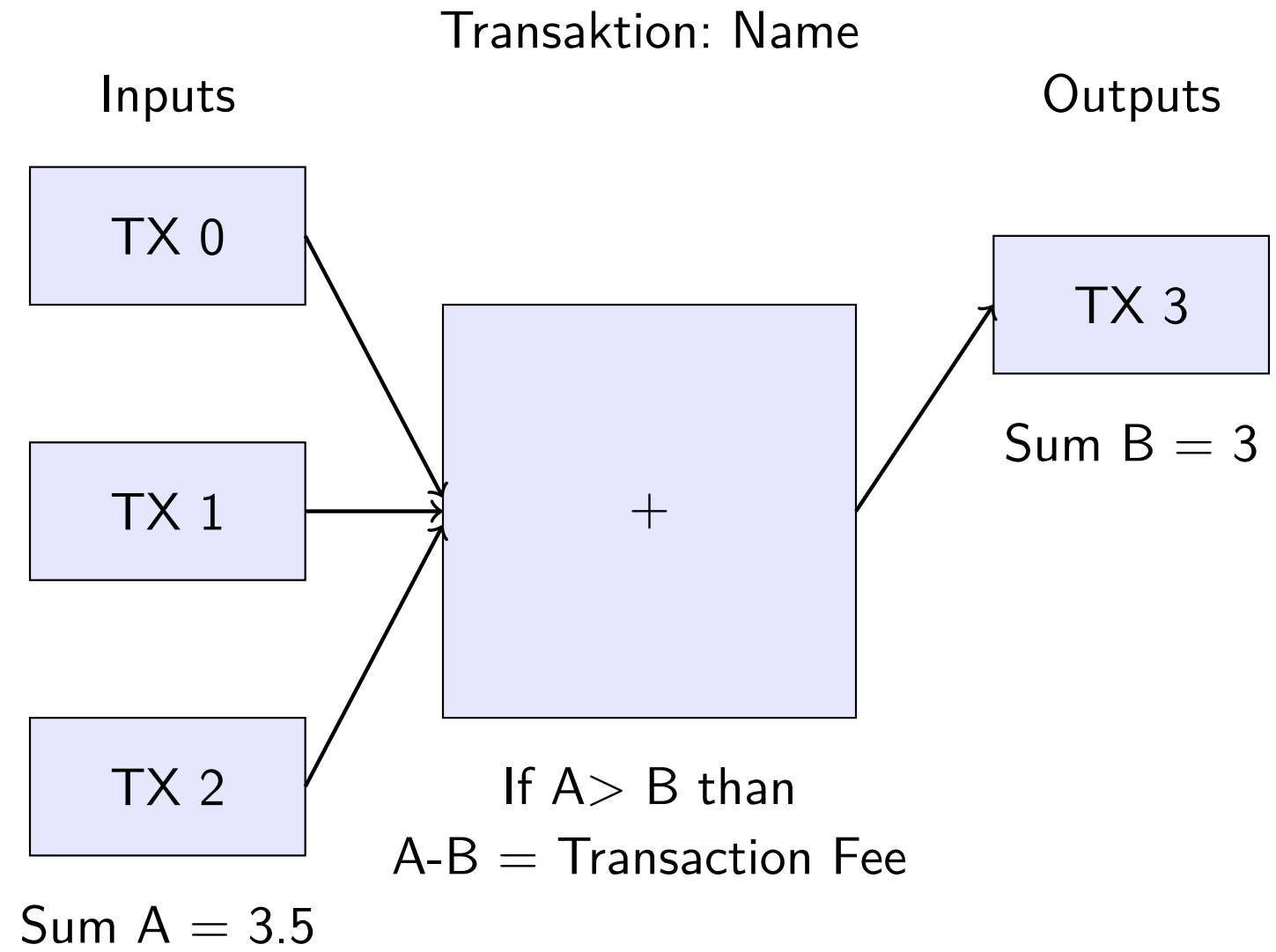
Eine Transaktion enthält immer drei Informationen:

- Input: Welche Sender-Adresse hat Alice zuvor die Bitcoins geschickt? (Es war Eva.)
- Menge: die Menge an Bitcoins, die Alice an Bob schickt
- Output: die Bitcoin-Adresse von Bob (Empfängeradresse)

Transaktionen

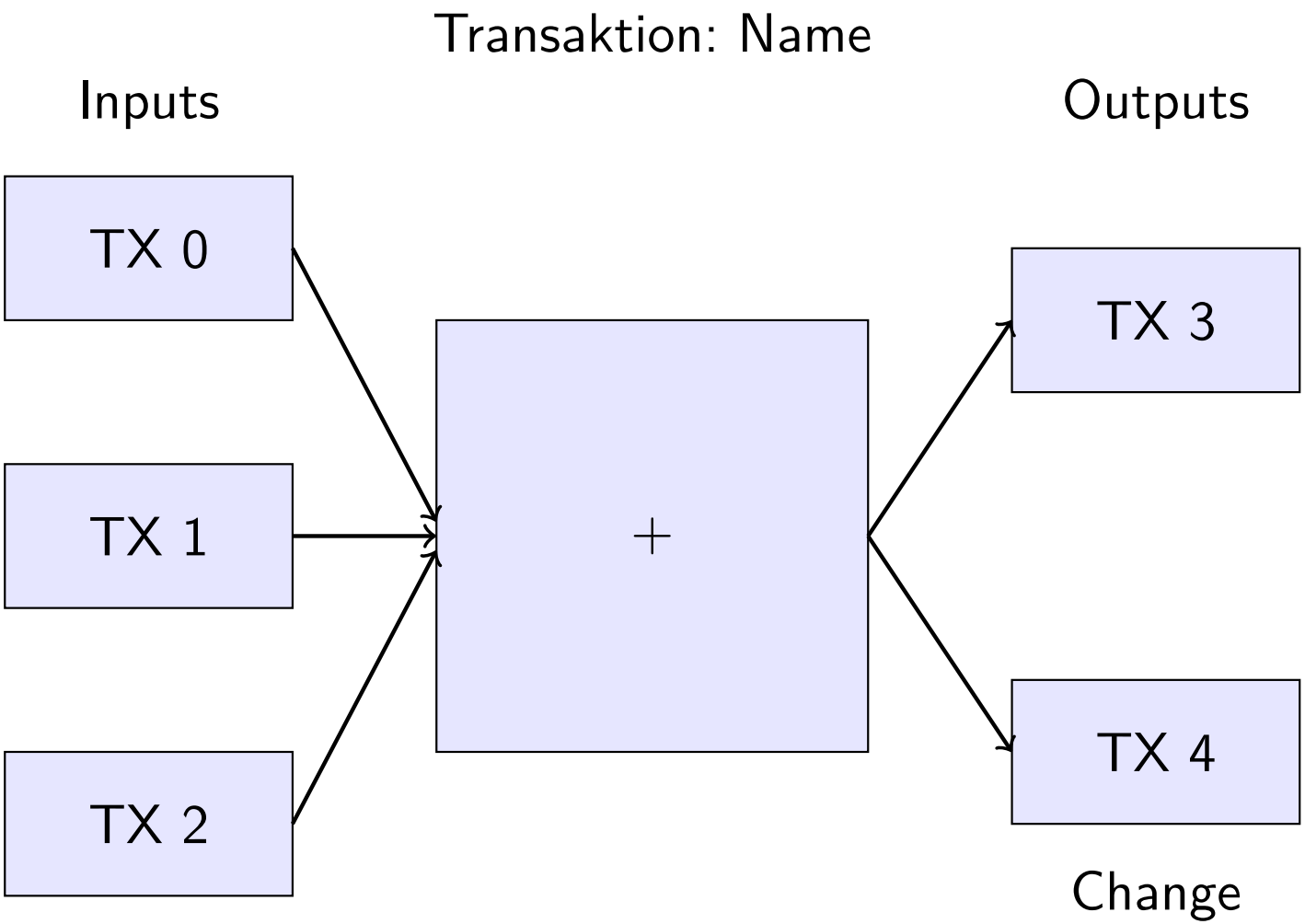
- Zudem benötigt man einen öffentlichen sowie privaten Schlüssel, der aus Zahlen und Buchstaben besteht.
- Dieser private Schlüssel wird dafür benutzt, die Nachricht/Transaktion zu signieren.
- Die Bitcoins werden an das Bitcoin Netzwerk gesendet. Dort müssen die Bitcoin-Miner die Transaktion verifizieren, damit sie anschließend in den Transaktionsblock gesetzt wird.

Transaktionen



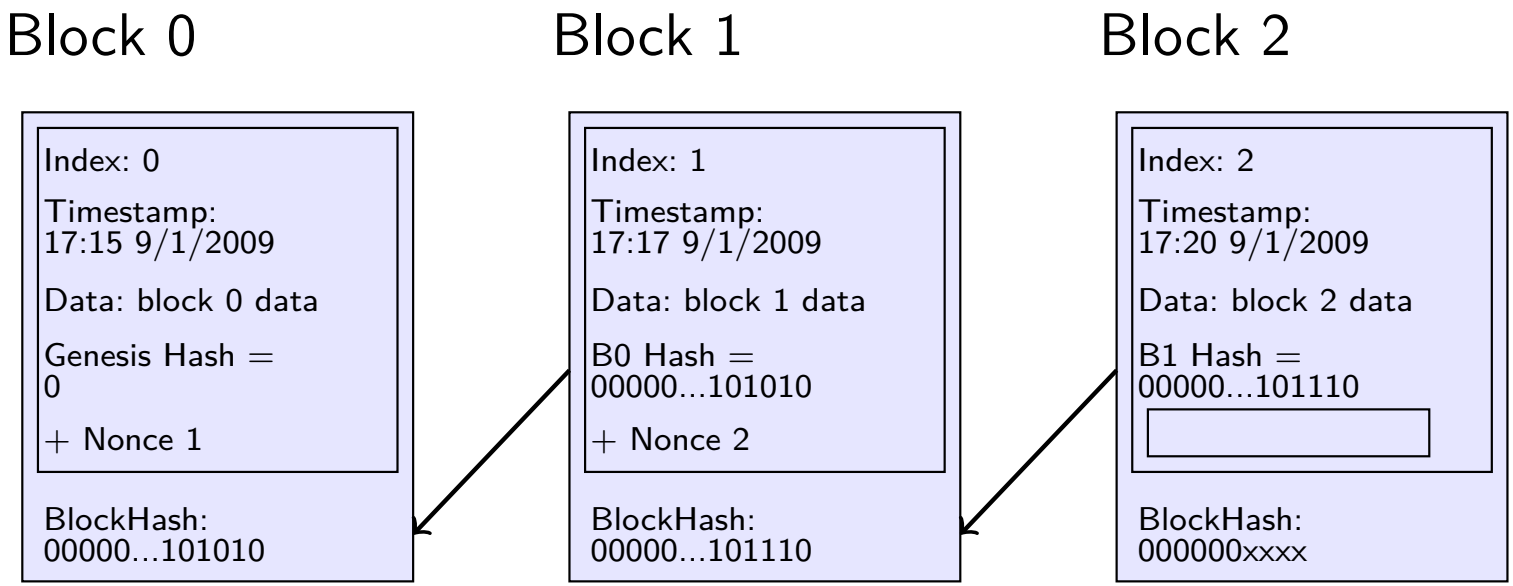
nach: https://www.youtube.com/watch?v=Em8nJN8IEes

Transaktionen



nach: https://www.youtube.com/watch?v=Em8nJN8IEes

Blockchain



nach: http://www.amarketplaceofideas.com/what-is-bitcoin-mining.htm

Verschlüsselung:

SHA256(“ “) =

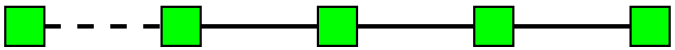
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Double-spending problem

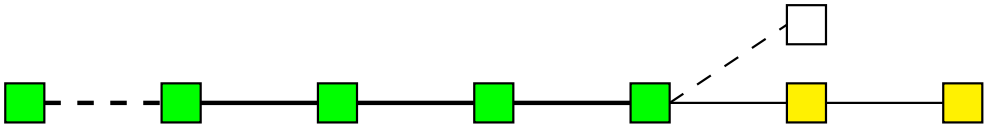
- Blockchain inklusive aller darin enthaltenen Transaktionen kann von jedem eingesehen werden.
- Transaktionen sind digitale Daten.
- Daten können prinzipiell von jedem kopiert werden.

Betrugsversuch: die selben Bitcoins mehrmals ausgeben

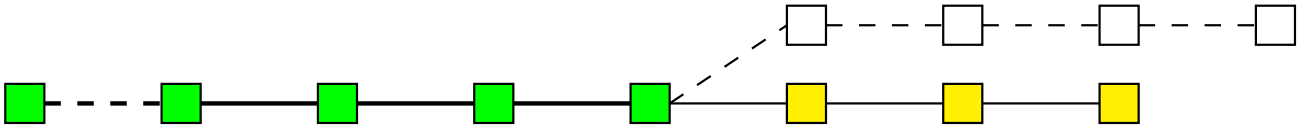
Double-spending problem



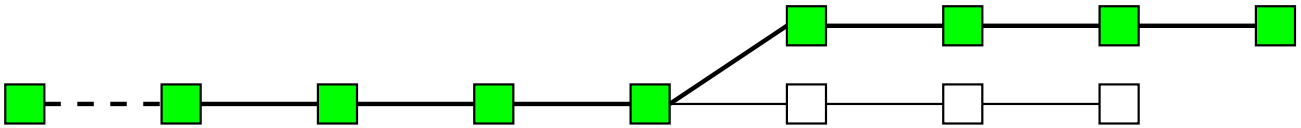
Initial state of the blockchain in which all transactions are considered as valid.



Honest nodes continue extending the chain by putting yellow blocks,
while the attacker secretly starts mining a fraudulent branch.



The attacker succeeds in making the fraudulent branch longer than the honest one.



The attacker's branch is published and is now considered the valid one.

nach https://www.deepdotweb.com/wp-content/uploads/2016/12/double-spend-png.png

Double-spending Problem

- Betrüger hofft darauf, dass Empfänger Gegenleistung erbringt, ohne auf Bestätigung der Transaktion zu warten
- Wie Betrug verhindern?
  - Vertrauen einer zentralen Autorität, die Transaktionen überwacht
  - Kryptographie: Erstellen von neuen Blocks erschweren
- Eine Lösung dafür: Beim Mining Proof-of-Work fordern

Mining

- Miner sammeln Bitcoin-Transaktionen und fügen von ihnen geminte Blöcke an die Blockchain an
- erhalten dafür Bitcoins

Ablauf:

- Daten sammeln: Transaktionen, die in den Block kommen sollen, Hash des Vorgänger-Blocks, Nonce aus verfügbaren Nonces wählen
- Diese Daten hashen: Hashwert muss kleiner sein als bestimmter vorgegebener Wert (abhängig von difficulty)
- Falls das zutrifft: Block kann an die Chain angefügt werden und der Proof-of-Work (Finden einer geeigneten Nonce) ist erbracht
- Falls Hashwert zu groß: Nonce ändern und weiter versuchen

Die Bitcoin-Blockchain aktuell

https://blockchain.info/

Double-spending problem

- Betrüger müsste also schneller minen können als das gesamte restliche Netzwerk zusammen
- Das ist aber sehr unwahrscheinlich, deshalb: Double-spending problem gelöst!

Danke für eure Aufmerksamkeit!

Quellen:

- Satoshi, Nakamoto: Bitcoin:A Peer-to-Peer Electronic Cash System, https://bitcoin.org.pdf
- https://www.bitcoin.de/de/bitcoin-whitepaper-deutsch-html
- https://www.btc-echo.de/tutorial/wie-funktioniert-eine-bitcoin-transaktion
- https://coinmarketcap.com/
- http://www.amarketplaceofideas.com/what-is-bitcoin-mining.htm
- https://www.deepdotweb.com/wp-content/uploads/2016/12/double-spend-png.png