Technisch (hoffentlich immer noch) korrekte aber stark vereinfachte

Erklärung des Lightning-Netzwerkes

*Weshalb es Bitcoin und andere Kryptowährungen für Konsument*innen und Unternehmen alltagstauglich macht.*

Rene Pickhardt (Data Science Consultant)

https://www.rene-pickhardt.de

Bitcoin Bootcamp - München 6.Juli 2018

Disclaimer und Motivation

Dieses Slidedeck soll die Kernidee des Lightning-Netzwerkes so vereinfacht wie möglich aber dennoch mit den technischen Grundbegriffen erläutern. Hierfür werden einige Grundbegriffe der Bitcoin-Technologie (zum Teil stark vereinfacht) wiederholt.
Dieses Slidedeck soll zum Verständnis und für einen technischen Einstieg beitragen. Im letzteren Falle wird dringend empfohlen, weitere Fachliteratur zu konsultieren, nachdem die Ideen durch das Slidedeck klar wurden.

Geld ohne Verzögerung einmal um die Welt schicken

Geld ohne Verzögerung einmal um die Welt schicken

- niedrige Gebühren
- Direkte Kontrolle
- Micropayments (und Milliardenbeträge) möglich
- Trustless (!)
- **Unrealistisch?**

Outline & Struktur

- Probleme mit Bitcoin
- Analogie Bitcoinwallet / Bankkonto
- Ablauf einer Bitcoin-Transaktion
- Kernidee: Der Payment-Kanal (& HTLC)
- Onion-Routing (Payment Channel Network)
- Status Quo und technische Herausforderungen
- Die Alltagstauglichkeit
- Geschäftsmodelle

Bitcoin kann maximal 1‘756‘080 Transaktionen pro Tag verarbeiten

- Jede Transaktion muss in einem Block gespeichert werden

- 1‘000‘000 Bytes pro Block für non witness data

- Transaktion braucht 82 Bytes non witness data

→ Maximal 12195 Transaktionen pro Block*

- 144 Blöcke pro Tag

→ maximal 1,7 Mio. Transaktionen

* Quelle: https://bitcoin.stackexchange.com/questions/59408/with-100-segwit-transactions-what-would-be-the-max-number-of-transaction-confi

In Stoßzeiten verarbeitet Visa ca. 47'000 Transaktionen pro Sekunde!*

- → ca. 4 Mrd. Transaktionen pro Tag
- ca. 2000 mal mehr als mit Bitcoin aktuell technisch möglich ist
- Zwei Lösungen:
  - a) Blockgröße anpassen
  - b) Sidechain- / Offchain-Transaktionen

* Quelle: http://lightning.network/lightning-network-paper.pdf

Vorschlag a) Blockgröße anpassen

- Visa verarbeitet ca. 2000 mal so viele Transaktionen wie Bitcoin

→ Blockgröße von 2 GB
  - 288 GB pro Tag
  - 105 TB pro Jahr
  - 160 GB Blockchain herunterladen und validieren dauert aktuell mehrere Stunden

- Validieren & speichern der Blockchain mit Notebook unmöglich
  → nicht dezentralisiert + weitere (!) Probleme

Vorschlag b) Lightning-Netzwerk

- Die meisten Transaktionen finden außerhalb der Blockchain statt
- keine Veränderung der Blockgröße nötig
- Trustless (!)
- Grundidee: Blockchain fungiert wie ein Gericht

Grundidee des Lightning Netzwerks

Im Geschäftsleben gilt:

- **Verträge** können bilateral ohne unsere **Gerichte** geschlossen werden. Meist ist es nicht nötig ein **Gericht** zu involvieren.

Analog im Bitcoin-/Lightning-Netzwerk:

- **Transaktionen** können bilateral ohne die **Blockchain** abgewickelt werden. Meist ist es nicht nötig diese der **Blockchain** mitzuteilen.

Bankkonto

- Bedarf Authentifizierung zur Eröffnung
- Bank kann Kunden ablehnen
- Bank kann Geldbeträge über der Einlagensicherung verlieren
- Man erhält nur eine Kontonummer
- Überweisungen von einem Konto zu einem anderen werden
  - online durch Passwort + TAN autorisiert
  - offline durch Unterschrift autorisiert

Bitcoinwallet

- Bedarf **keiner** Authentifizierung zur Eröffnung
- Kann jeder Mensch **ohne Erlaubnis** erstellen
- Geldbeträge sind durch **Kryptographie gesichert**
- Man erhält eine **Bitcoinadresse**
- Transaktionen von einer Adresse zu **mehreren anderen** werden durch die Signatur eines (oder mehreren) **privaten Schlüssel(s)** autorisiert

→ Wir müssen verstehen wie eine Bitcoin Transaktion abläuft.

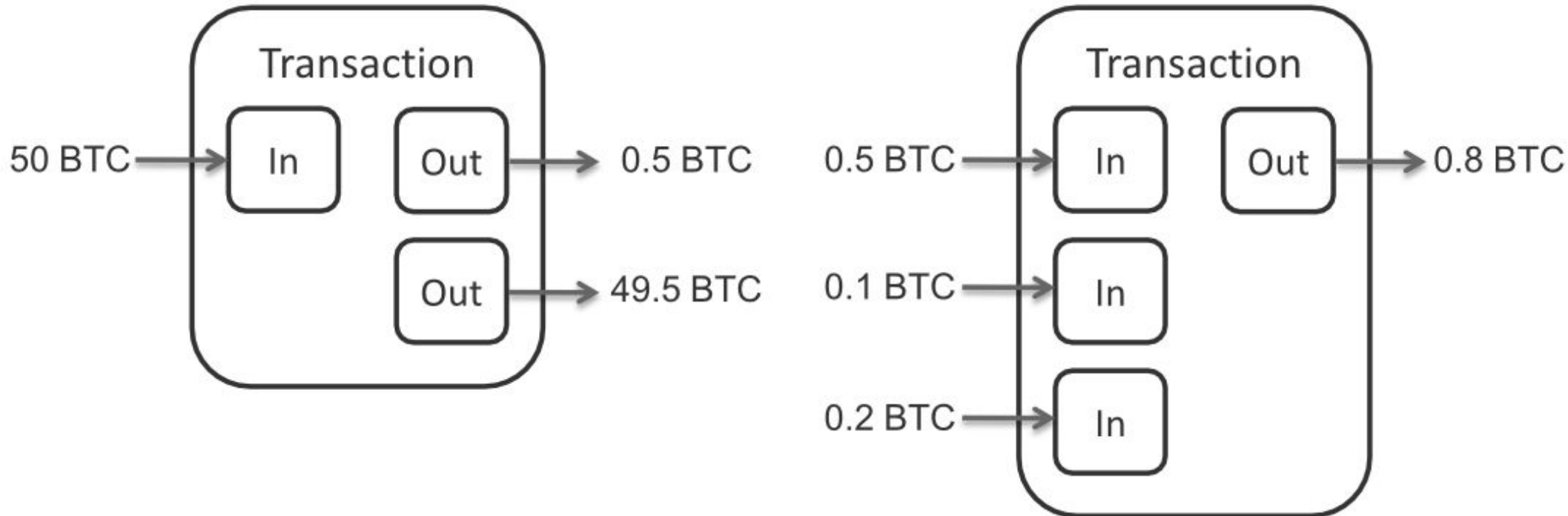
Was ist technisch betrachtet ein Bitcoin bzw. eine Bitcointransaktion?

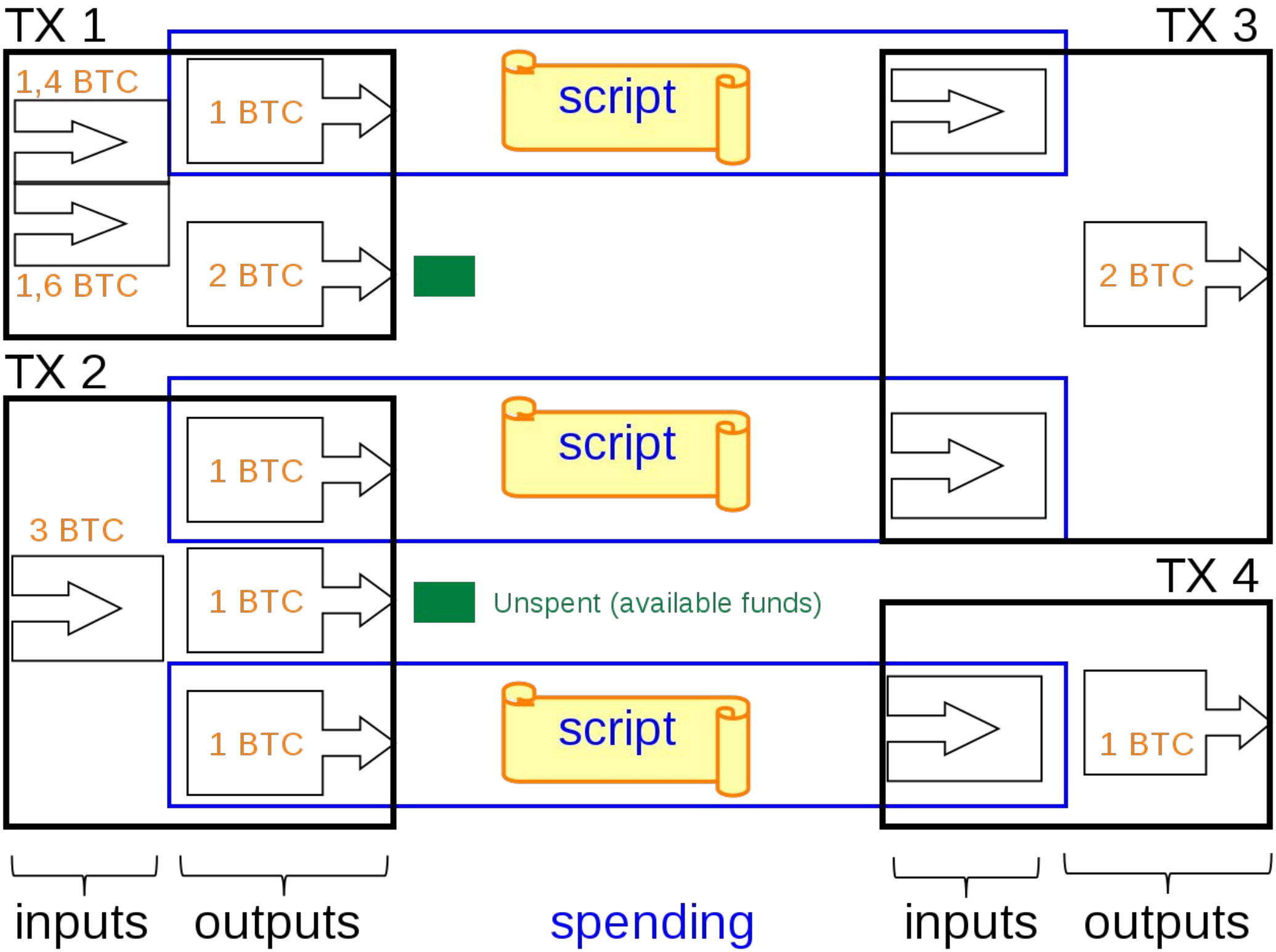
- Ein Bitcoin ist der Betrag eines nicht ausgegeben Transaktionsoutputs
  - engl. unspent transaction output (UTXO)

- Man bezahlt mit Bitcoin in dem man nicht ausgegebene Transaktionen ausgibt
  - Wie sehen solche Transaktionen aus?
  - Wo entstehen solche Transaktionen?
  - Wie gibt man sie aus?

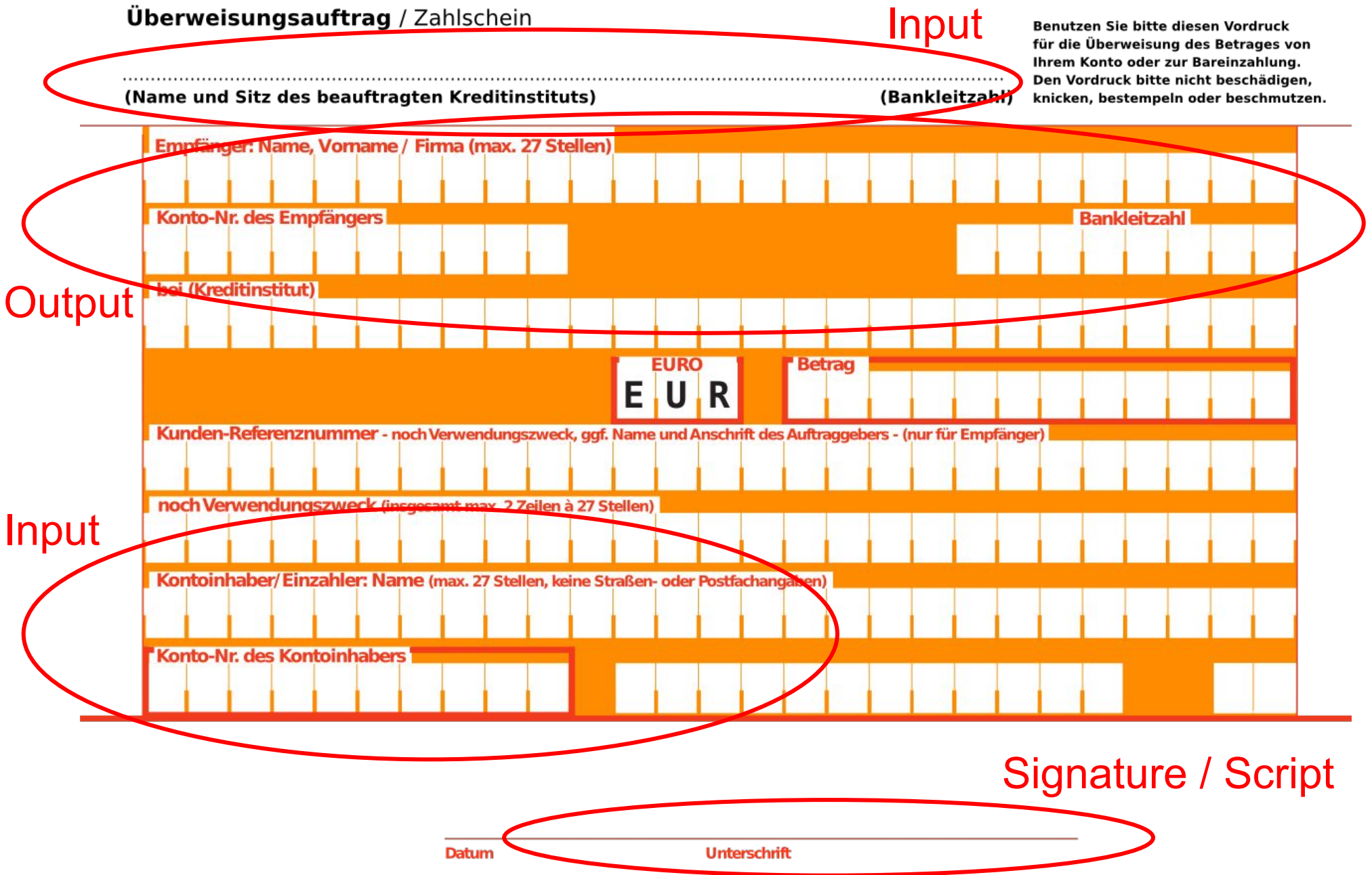
Wie sehen Bitcoin-Transaktionen aus? (vereinfacht)

- Eine Transaktion konsumiert einen oder mehrere Inputs
- Diese gehen an einen oder mehrere Outputs
  - Jeder Output beinhaltet für gewöhnlich eine Empfangsadresse



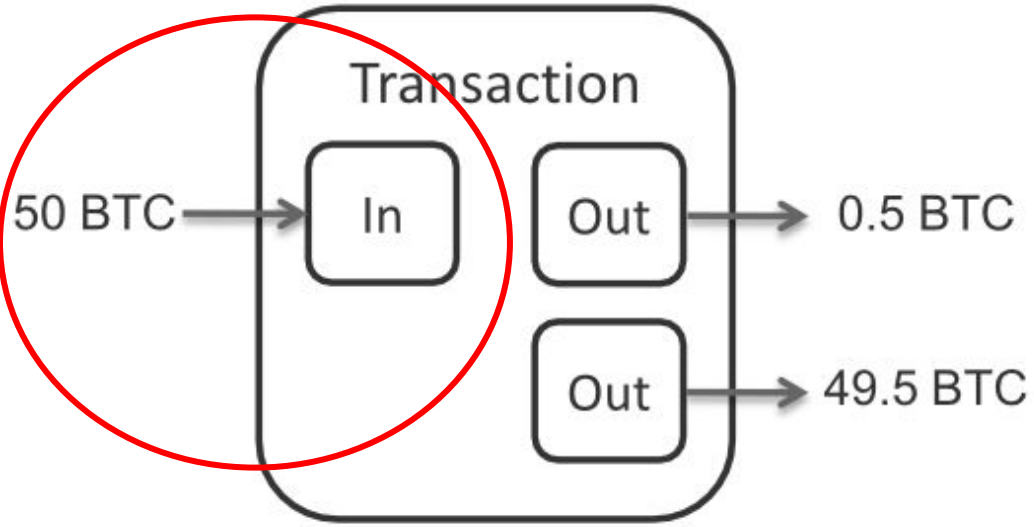

TX 1
1,4 BTC
1,6 BTC
1 BTC
2 BTC
script
TX 3
2 BTC
TX 2
3 BTC
1 BTC
1 BTC
1 BTC
script
script
Unspent (available funds)
TX 4
1 BTC
inputs
outputs
spending
inputs
outputs

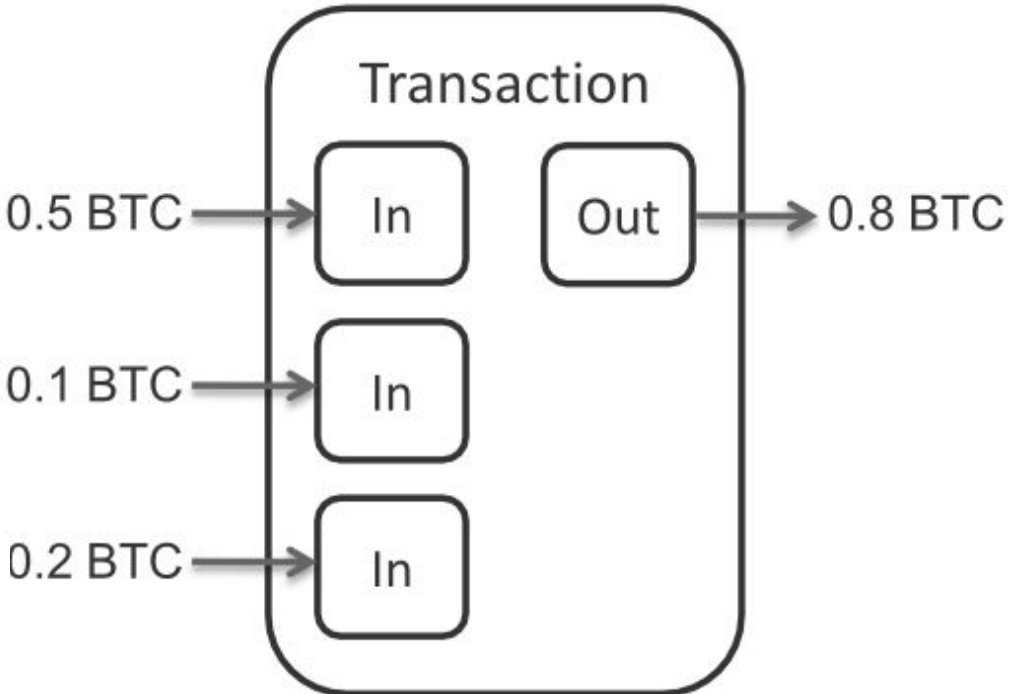
Analogie Banküberweisung



Wie entstehen solche Transaktionen? (vereinfacht)

- Indem man sie erstellt.
  - Genauer: Wie entsteht der erste Input?
- Als Teil des Protokolls ist es erlaubt, dass die erste Transaktion eines Blocks einen fiktiven Input mit einem zuvor definierten Wert ausgibt





Fiktiver Input darf beim Mining generiert werden (aktuell 12.5 BTC)

Wie gibt man die Transaktionen aus? (vereinfacht) Teil 1

- Eine Transaktion wird ausgegeben, indem man das Script einer Transaktion erfüllen kann
- Meist, indem man das Geheimnis zu einem Hash bereitstellen kann
- Zum Beispiel die Signatur der Transaktion mit dem privaten Schlüssel der Bitcoin-Adresse
- Die signierte Transaktion wird gebroadcastet

Wie gibt man die Transaktionen aus? (vereinfacht) Teil 2

- Bitcoin-Node (Miner) prüft die Gültigkeit der Transaktion
- Bei Gültigkeit wird sie via P2P mit anderen Nodes geteilt und im Mempool registriert
- Transaktionen des Mempools werden zum nächsten Block zusammengefasst und es wird nach einer Hash-Kollision gesucht.

Die fertige Transaktion wird gebroadcastet

- Bis die Transaktion publiziert und gemined ist kann der UTXO des Inputs anderweitig verbraucht werden.

- Doppeltes Bezahlen ist nicht möglich, da Transaktionen nur in einen Block aufgenommen werden, wenn der Input nicht verbraucht wurde.

- Möglichst zeitnah broadcasten, da sie sonst aus Sicht des Netzwerkes nicht stattgefunden hat

Payment-Channels durch Verheimlichung von signierten Transaktionen (!)

Wenn im Wald ein Baum umfällt und keiner da ist, um es zu sehen oder zu hören, ist der Baum dann tatsächlich umgefallen?*

* Zitat aus dem Lightning Network White Paper: http://lightning.network/lightning-network-paper.pdf

Alice & Bob erstellen ein 2-von-2-Multisignature-Wallet

- UTXO an die Adresse des Multisignature-Wallets können nur als Input dienen wenn
  - Alice die Transaktion signiert und
  - Bob die Transaktion signiert

- Alice und Bob senden zusammen insgesamt z.B. 0,5 BTC an das Multisignature-Wallet
  - Diese Transaktion wird **noch nicht** publiziert
  - Sie heißt **Funding-Transaktion**

Die Funding-Transaktion wird als Commitment-Transaktion ausgegeben

- 0,25 BTC gehen an Alice
- 0,25 BTC gehen an Bob

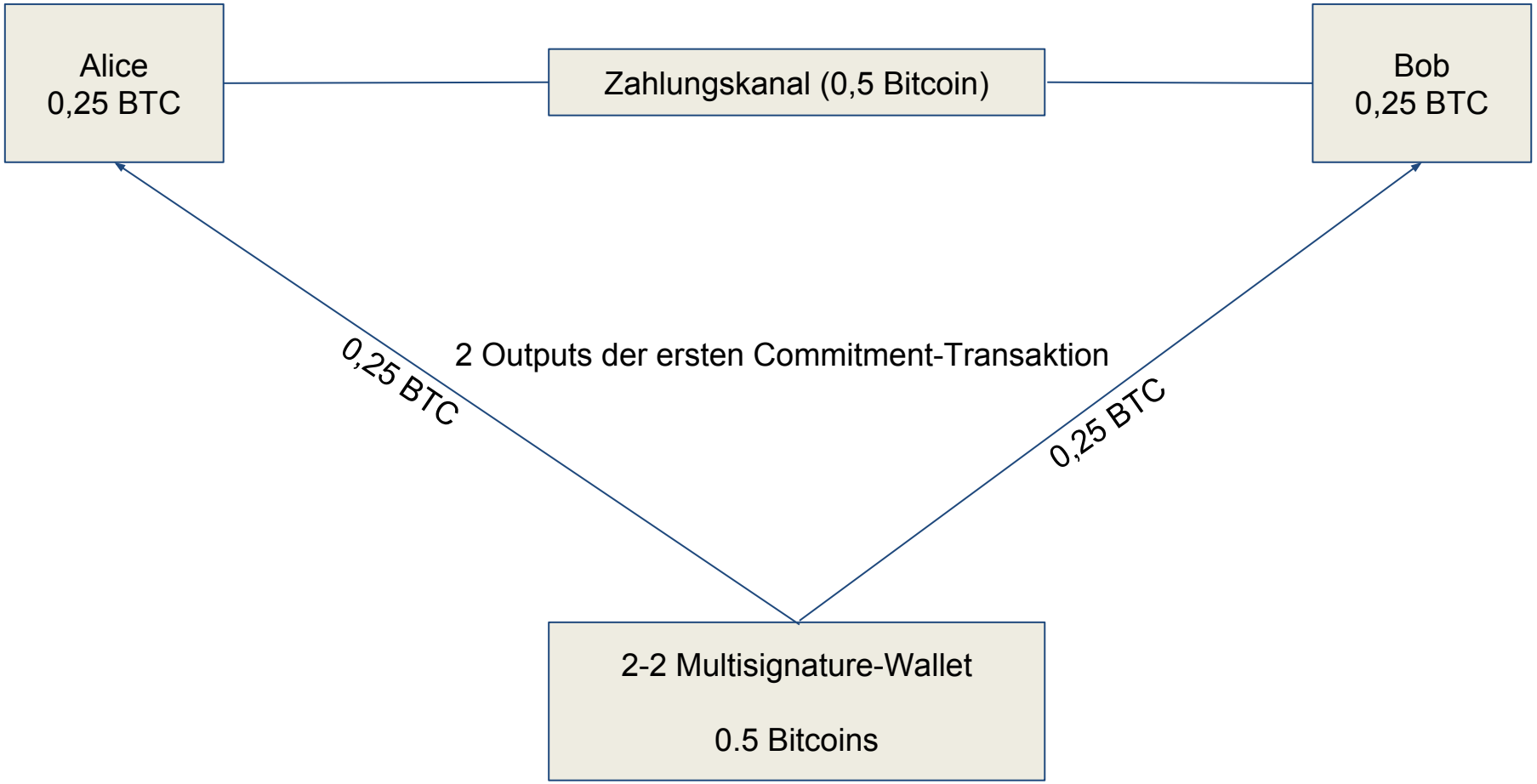
- Alice und Bob signieren die Commitment-Transaktion.*

- **Nun wird die Funding-Transaktion veröffentlicht**

- Jeder darf zu jedem Zeitpunkt die Commitment-Transaktion publizieren (Blockchain als Gericht)

* In Wirklichkeit werden 2 Commitment-Transaktionen mit dem gleichen Auszahlungen erstellt (zur Vereinfachung verzichten wir auf dieses Detail im Folgenden)

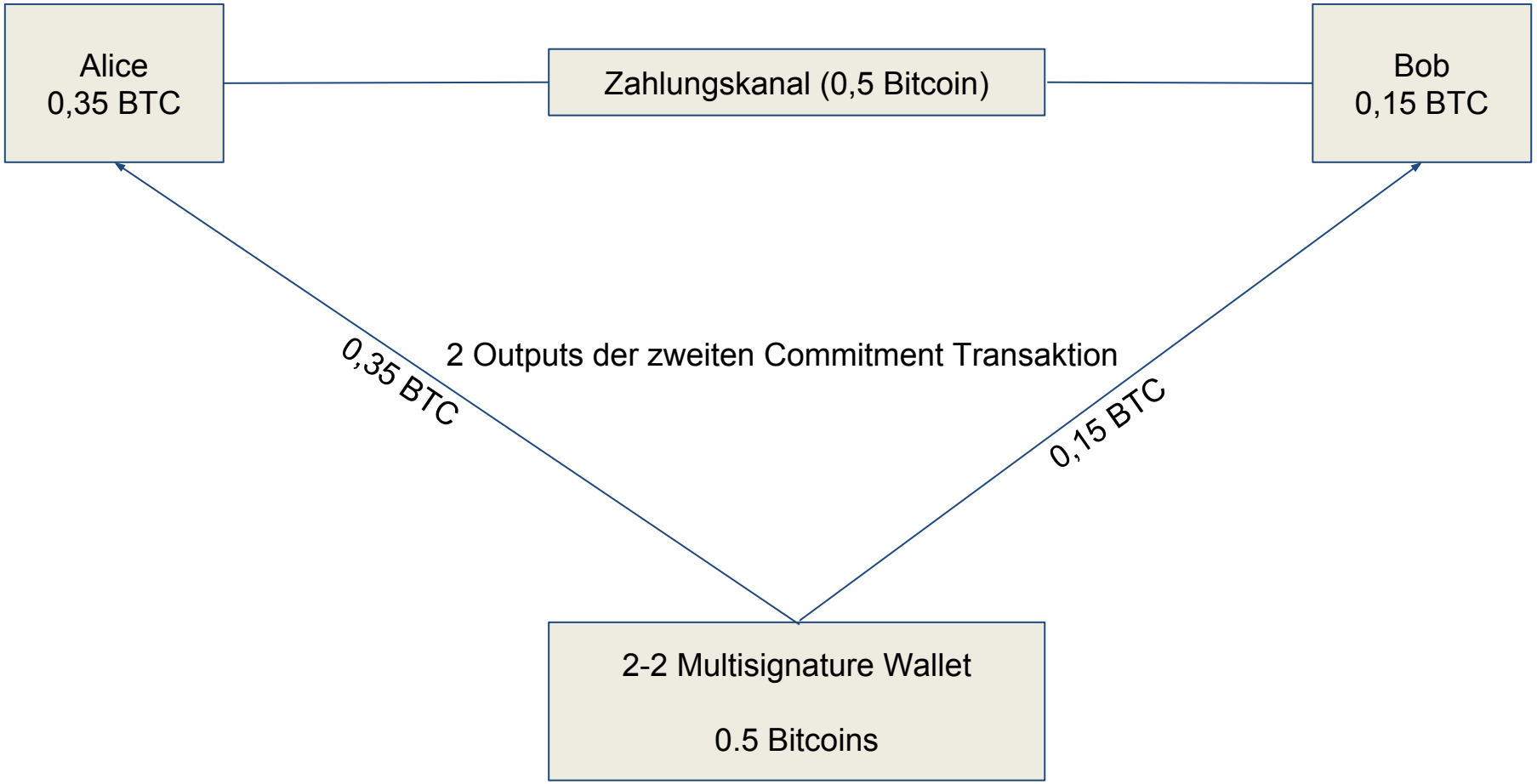
Schematische Darstellung des Zahlungskanals



Die Möglichkeiten einer nicht publizierten Commitment-Transaktion

- Bob möchte 0,1 Bitcoin an Alice senden
- Bob gibt die Funding-Transaktion wie folgt in einer zweiten Commitment-Transaktion aus
  - 0,35 Bitcoin an Alice
  - 0,15 Bitcoin an Bob
- Diese Transaktion wird von beiden signiert aber erneut nicht publiziert
- Die erste Commitment-Transaktion (0,25 Bitcoin an Bob und Alice) wird zerstört.

Schematische Darstellung des Zahlungskanals



Beobachtungen und Vorteile

- Bob und Alice konnten dieses Update durchführen ohne dass die Blockchain davon wusste
- Alice und Bob können jederzeit die Commitment Transaktion veröffentlichen
- Der Prozess lässt sich im Millisekundenbereich über das Internet ausführen (und wiederholen)
- Keine weiteren Transaktionsgebühren fällig

Wie lässt sich die erste Commitment-Transaktion zerstören?

- Bob & Alice haben eine Commitment Transaktion
- Jeder könnte beliebig viele weitere Kopien angefertigt haben
- Zerstören ist nötig, da Bob sonst, nachdem er die Dienstleistung erhalten hat, die erste Commitment-Transaktion veröffentlichen könnte
  - Er würde dann 0.25 Bitcoin erhalten
- Lösung: Revocation Keys und Hashed Timed

Die Commitment-Transaktion enthält in Wirklichkeit einen komplexen **Contract**

- Sie wird durch 2 Signaturen ausgegeben
  - Es gibt einen **Time Lock** von ca. 144 Blöcken
  - So lange kann der neue Output nicht ausgegeben werden
  - Aber sie kann anderweitig ausgegeben werden, wenn jemand das Geheimnis (Revocation Key) zu einem **Hash** in der Commitment-Transaktion bereit stellt.

- Der Revocation Key kann von Bob und Alice gemeinsam gefunden werden

Hashed Time Locked Contract (HTLC)

- Sie wird durch 2 Signaturen ausgegeben
  - Es gibt einen **Time Lock** von ca. 144 Blöcken
  - So lange kann der neue Output nicht ausgegeben werden.
  - Aber sie kann anderweitig ausgegeben werden, wenn jemand das Geheimnis (Revocation Key) zu einem **Hash** in der Commitment-Transaktion bereit stellt.

- Der Revocation Key kann von Bob und Alice gemeinsam gefunden werden

Streng genommen ist der HTLC nur beim Routing von Payments im Netzwerk nötig und hier darf nicht von HTLC gesprochen werden, sondern von Revocable Sequence Maturity Contracts (RSMC). Abstrakt sind die Konzepte hier jedoch hinreichend ähnlich, so dass wir den Begriff hier motiviert haben

Beeindruckende Mathematik hinter Revocation Keys (stark vereinfacht)

Es ist tatsächlich mit Hilfe von Kryptographie möglich, dass:

- Bob und Alice sich gemeinsam auf eine geheime Folge von Keys verständigen
- Beide den aktuellsten Key nicht kennen
- Der Hash des aktuellsten Keys bekannt ist
- Aus dem Key ablesbar ist, der wievielte Key der Folge es ist bzw.
- sich alle vorherigen Schlüssel aus einem Schlüssel der Folge errechnen lassen.
- Spätere Schlüssel können nur gemeinsam berechnet werden.

Zweck der Revocation Keys

- Alte Commitment-Transaktionen lassen sich als digitale Güter nicht zerstören.

- Ein betrügerisches Publizieren solcher ermöglicht der Gegenseite
  - den Revocation Key zu verwenden
  - die Bitcoins der Funding-Transaktion komplett selbst einzustreichen

- Bevor eine weitere Commitment-Transaktion signiert wird, muss der Revocation Key der aktuellen Commitment -Transaktion gemeinsam berechnet werden

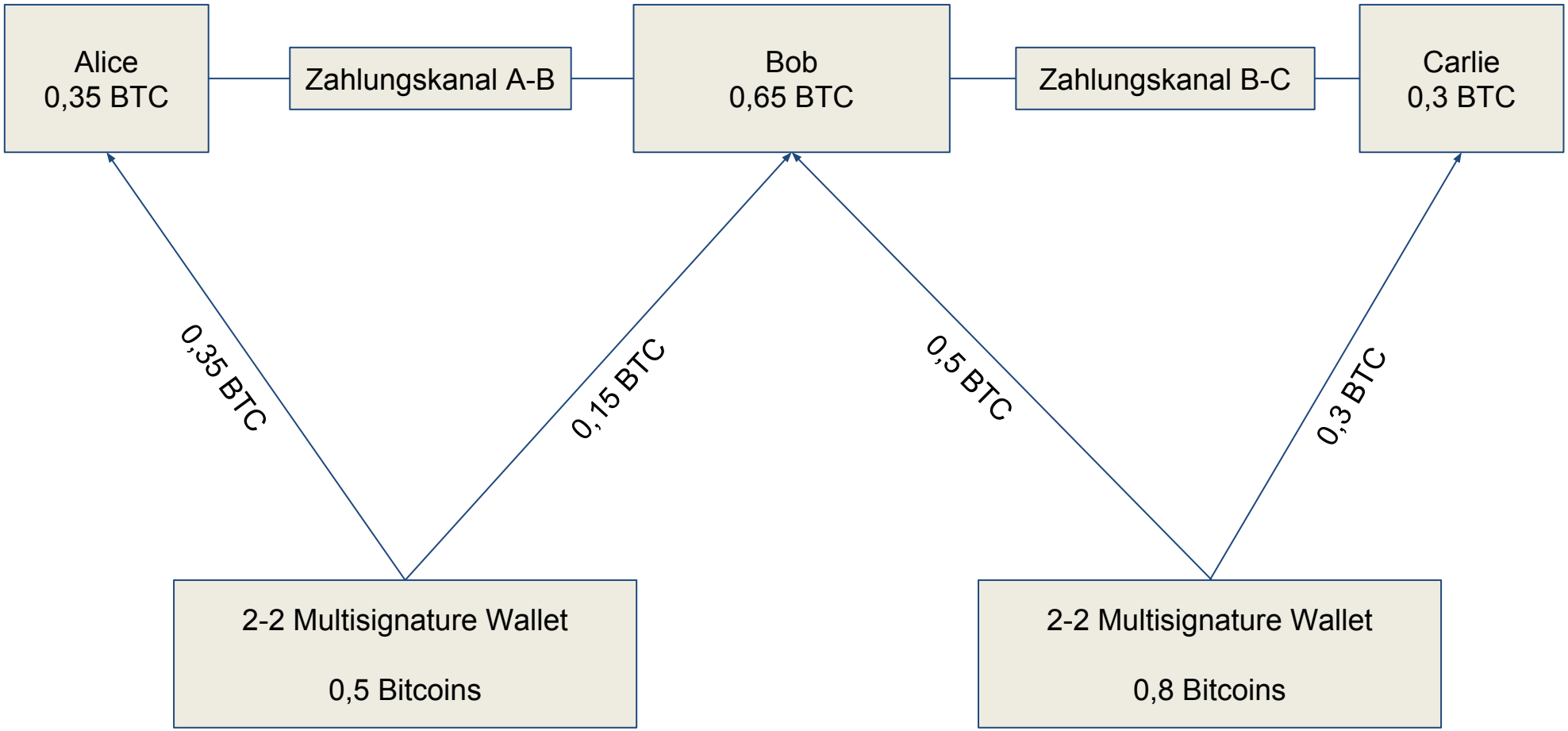
Zusammenfassung Zahlungskanal

- Alice und Bob können einander beliebig oft Bitcoins hin- und herschicken
- Die Blockchain und auch andere Menschen wissen davon nichts
- Der Kanal selbst ist trustless:
  - Alice kann Bob bestrafen, wenn er versucht zu betrügen (oder umgekehrt)
  - Der Kanal kann jederzeit durch veröffentlichen der Commitment-Transaktion einseitig geschlossen werden

Ein Netzwerk von Zahlungskanälen

- Alice und Bob haben einen Zahlungskanal
- Bob und Charlie haben einen Zahlungskanal
- Alice möchte Charlie Bitcoins schicken
- Sie schickt Bob die Bitcoins und er soll sie an Charlie weiterleiten
- Was, wenn Bob die Bitcoins nicht weiterleitet? Lässt sich das vermeiden?

Netzwerk von Zahlungskanälen



Frage: Wer kann wem in diesem Netzwerk wieviele BTC schicken?

HTLCs zum Routen von Zahlungen

- Auch hier lassen sich HTLCs einsetzen
- Transaktionen in einem Zahlungskanal können nur empfangen werden, wenn sie in einem anderen ausgegeben werden
- Alle Transaktionen können rückgängig gemacht werden, wenn ein Node auf dem Pfad sich nicht protokollkonform verhält
- Zahlungen zwischen Mitgliedern des Netzwerkes sekundenschnell möglich!

Entwicklung seit Januar 2018

- Alpha versionen der 3 Implementierungen (Eclair, c-lightning, lnd) im Januar 2018 online
- Erste Nodes im Lightning Network entstehen im Mainnet
- Blockstream stellt LApps vor
- Erste Phone Apps unterstützen das Lightning-Netzwerk
- Implementierungen erreichen Beta Status
- Satoshis Place als proof of Concept
- Juli 2018:
  - ca. 2600 Nodes
  - ca. 8500 Zahlungskanäle
  - ca. 32 Bitcoins sind im Lightning Netzwerk

Herausforderungen (inkl. Lösungen)

- Wie findet man einen Weg im Netzwerk von Alice zu Charlie?
  - Optimale Topologie des Netzwerks (inkl. Autopilot)
  - Atomic Multipath Payments
  - Liquidität bereitstellen
  - Splicing

- Was passiert wenn Bob offline ist während Alice probiert eine alte Commitment-Transaktion auszugeben?
  - Watchtower

Roadmap

- RFC 1.1 soll im Herbst gedraftet werden
- Software muss entsprechend erweitert werden
- Echte Adaption muss noch stattfinden
- Dezentrale Exchanges launchen ihren Service und bringen Liquidität in das Lightning-Netzwerk
- Atomic Swaps ermöglichen ein Overlay Bezahlnetzwerk über verschiedene Blockchains

Alltagstauglichkeit (mittel- bis langfristig)

- Bezahlen im Internet so einfach wie eine Banküberweisung
- Anwender*in braucht nicht zu wissen, dass diese Technologie verwendet wird
- Micropayments und milliardenschwere Transaktionen möglich
- Sekundenschnell
- BTC in direkter Kontrolle der Empfänger*innen

Alltagstauglichkeit für ander Kryptowährungen (vgl. Internet)

- Internet verbindet verschiedene Netzwerk Protokolle durch ein virtuelles Overlay Netzwerk
  - Ethernet
  - DSL
  - Wifi
  - ...
- Lightning Netzwerk verbindet durch Atomic Swaps verschiene Blockchain Protokolle
  - Bitcoin
  - Etherium
  - Litecoin
  - ....

Geschäftsmodelle mit dem Lightning Netzwerk

- Routing für Fees
  - Eher kein Geschäftsmodell
  - Nur für Player mit sehr hoher Liquidität

- Watchtower betreiben
  - Hängt davon ab, wie grundlegend Watchtower implementiert werden

- Dezentrale Exchange
  - Sowohl für Fiat als auch andere Kryptos durch Atomic Swaps

Möglichkeiten für Firmen

- Micropayments
  - z.B. für Webinhalte
  - Dienstleistungen
  - Informationen
- Disruptive Change für Finanzdienstleister
- Technologieprovider
- Beratung & Implementierung

Weitere Quellen

- Lightning Network Paper
- Bitcoin Whitepaper
- RFC (BOLT - Basics Of Lightning Technology)
- Wikipedia-Artikel (:
- Lightning Network Artikel im Bitcoin Wiki

- Wissenschaftliche Publikationen Keywords:
  - Payment Channel Networks (PCN)
  - Zahlungskanäle
  - Netzwerktheorie

Vielen Dank für Ihre Aufmerksamkeit

- Slides offen lizenziert verfügbar auf Wikimedia Commons

- Bei Fragen und Anmerkungen: https://www.rene-pickhardt.de

- Öffnen Sie einen Zahlungskanal mit meinem Lightning Network Node:

036f464b54416ea583dcfae3872d28516dbe85414ed838513b1c34fb3a4aee4e7a@144.76.235.20:9735

Bildnachweise:

- https://commons.wikimedia.org/wiki/File:Bitcoin_Transaction_Inputs_and_Outputs.png By Matthäus Wander CC BY-SA 3.0 from Wikimedia Commons
- https://www.pexels.com/photo/shallow-focus-photography-of-brown-globe-1169922/ by Ricky Gálvez CC-0 via Pexels
- https://commons.wikimedia.org/wiki/File:%C3%9Cberweisungstr%C3%A4ger-einzeln.png?uselang=de#filelinks von Erik Streb [GFDL (http://www.gnu.org/copyleft/fdl.html) oder CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons
- https://pixabay.com/en/innovation-business-information-561388/ by jarmoluk CC-0 via pixabay
- https://commons.wikimedia.org/wiki/File:Bitcoin_transaction_chain.svg By Wargo CC BY-SA 4.0, from Wikimedia Commons

Autorinnen und Autoren sowie Urheberrecht

Danksagung

Inhaltliche Anmerkungen und Rechtschreibkorrekturen von:

- Jeff Gallas (Fulmo Lightning - https://www.fulmo.org/)
- Jasper Raedsich (https://raedisch.net/)
- Stefan Richter (https://coinspondent.de/honigdachs-der-bitcoin-podcast-aus-leipzig/ oder https://bitcoinprivacy.net/)
- Alena Vranova (https://twitter.com/alenasatoshi)
- Christian (https://twitter.com/rootzoll)
- Wolfram T
- Ulf Heyden (http://www.heyden.net)