Blockchain

Bitcoin, Altcoin, Ethereum, ZCash

Juli 2017

Inhalt

- Bitcoin
  - Transaktionen
  - Blockchain
- Altcoins
- Ethereum
  - Turingvollständige Transaktionen
  - DAOs
  - Proof of Stake
- ZCash

Bitcoin

- Online-Bezahlsystem ohne zentrale Autorität
- Kontonummern sind Public Keys
- Transaktionen sind signierte Nachrichten

- Die Anzahl der Bitcoins ist auf ca. 21 Millionen beschränkt

- Problem:
  - Double Spending
- Lösung:
  - Blockchain

Transaktionen

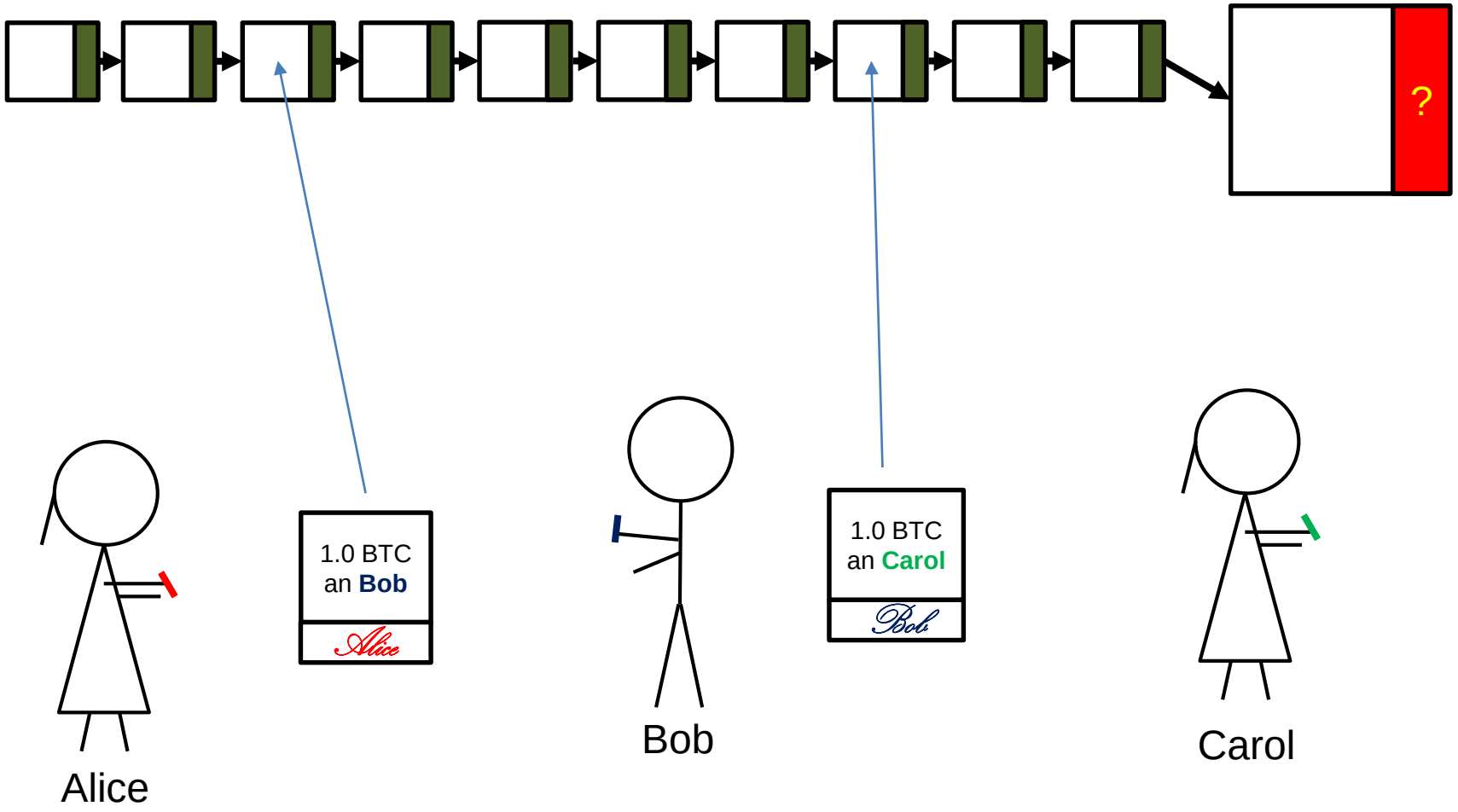
- Gültige Transaktionen in einem gemeinsamen Archiv sammeln

- Eine gewöhnliche Transaktion ist gültig, wenn:
  - Der Absender die nötigen Bitcoins hat
  - Der Absender eine gültige Signatur erzeugt hat

- Sobald der Empfang eines Bitcoins bestätigt ist, kann dieser wieder ausgegeben werden.

- Spezielle Transaktionen:
  - Treuhänder
  - Mehrfachsignaturen (frei definierbare Bedingungen)

Bitcoin – Transaktionen

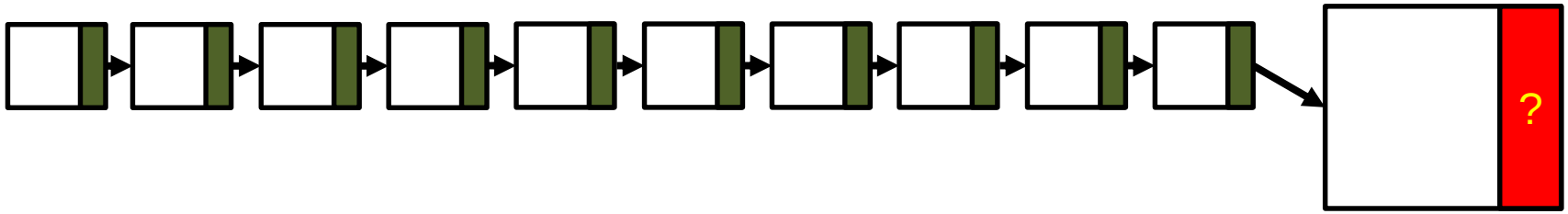


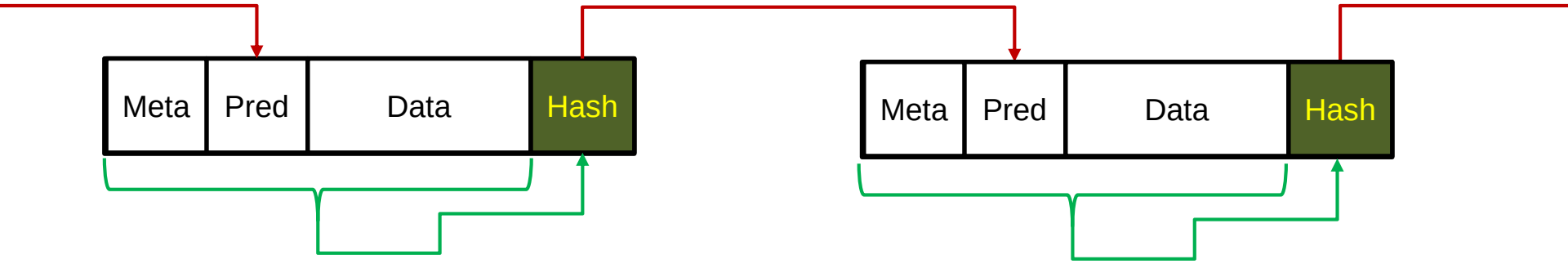
Bitcoin – Blockchain

- Archiv aller gültigen Bitcoin-Transaktionen

- Transaktionen werden zu Blöcken zusammengefasst
- Die Blöcke werden verkettet zur Blockchain

Bitcoin – Blockchain





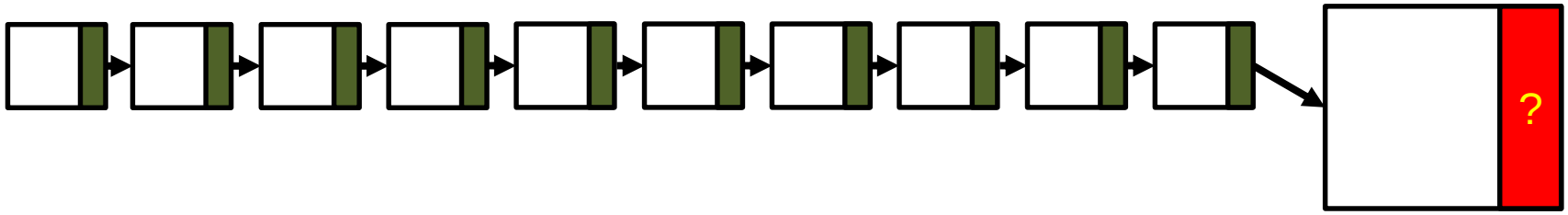
Bitcoin – Blockchain

- Archiv aller Bitcoin-Transaktionen

- Frage:
  - Wer kontrolliert das Archiv?

- Antwort:
  - Es wird kollektiv generiert
  - Daten können angehängt werden
  - Daten können nicht verändert oder gelöscht werden

Bitcoin – Blockchain



- Miner sammeln alle Transaktionen aus dem Netz und versuchen im Wettbewerb, den nächsten Block zu erzeugen

  1. Der Block muss den Regeln entsprechen.
  2. Alle Transaktionen im Block müssen gültig (Signatur) und gedeckt sein.
  3. Hashwert muss eine bestimmte Form treffen, z.B.:

     0x00000003ffffff…fff (d.h. 30 führende Nullen)

- Wer zuerst einen solchen Block findet, wird mit Bitcoins belohnt.

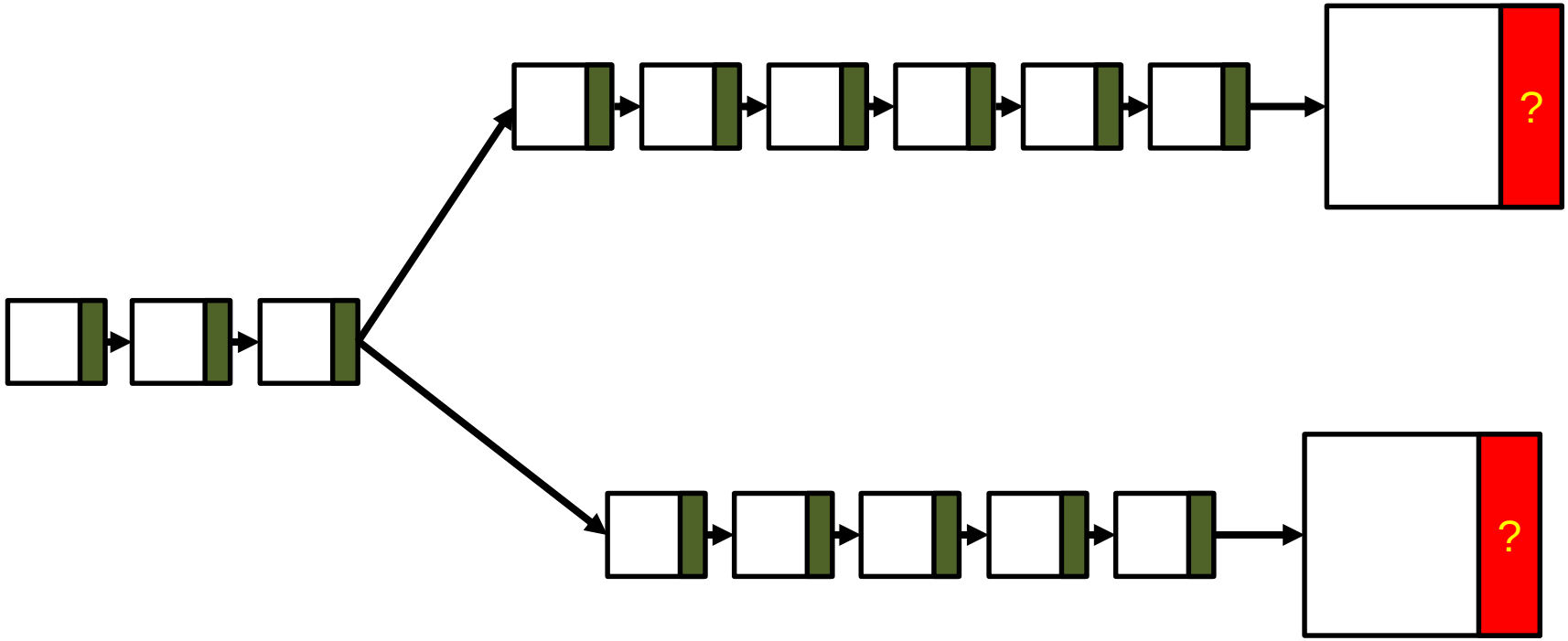
Bitcoin – Blockchain

- Die «Difficulty» zur Erzeugung eines neuen Blockes wird periodisch (ca. alle 14 Tage) angepasst.
- Die «Difficulty» gibt vor, welche Form der Blockhash erfüllen muss (Anzahl der führenden Nullen).
- Dadurch wird das Finden des Blocks leichter oder schwieriger.
- Die Vorgaben werden kollektiv so gewählt, dass statistisch unter allen Teilnehmern alle 10 Minuten ein neuer Block gefunden wird.

Bitcoin – Longest Chain Rule

- Was passiert, wenn zwei Miner je einen gültigen Block finden, bevor sie den Block des anderen sehen?
- Es entsteht ein Fork.
- Miner haben ein Interesse daran, an dem Blockchain-Zweig zu arbeiten, der sich später durchsetzt.
- Eine Belohnung im falschen Zweig wäre wertlos.
- Bei zwei konkurrierenden Zweigen wird immer die längere Kette als gültig betrachtet.
- Dabei ist nicht die Anzahl der Blöcke ausschlaggebend, sondern der darin enthaltene Arbeitsaufwand.
- D.h. eine kürzere Kette kann sich durchsetzen, falls ihre «Difficulty» hoch genug ist.

Bitcoin – Longest-Chain Rule



Altcoins – Alternative Coins

- Meistens Trittbrettfahrer, die Geld verdienen wollen

- In der Regel kaum Innovation:
  - Andere Grösse der erzeugen Geldmenge
  - Andere eingesetzte Algorithmen (Hash, Signatur)

- Altcoins mit bedeutenden Unterschieden zu Bitcoin:
  - Ethereum
  - ZCash

Ethereum

- Bitcoin-Transaktionen sind keine statischen Datenstrukturen, sondern ausführbare Skripte.
- Die Skriptsprache ist limitiert und enthält keine bedingten Sprünge.
- Ethereum-Transaktionen können beliebige Programme sein

- Problem:
  - Wie stellt man sicher, dass diese Transaktionsprogramme in akzeptabler Zeit ablaufen.

- Lösung:
  - Erzeuger bezahlt für die Ausführungszeit

Ethereum – DAOs

- Ethereum-Transaktionen erlauben die Implementierung komplexer Verträge

- Verträge können z.B. Institutionen implementieren:
  - Decentral Autonomous Organization (DAO)
  - Nutzer können Geld an eine DAO senden und Anteile kaufen
  - Die DAO kann gemäss ihrer programmierten Regeln Dividenden auszahlen

- Dabei ist Vorsicht geboten, Programmierfehler sind nicht auszuschliessen, siehe DAO-Fork von 2016

Ethereum – Proof of Stake

- Mining (Proof of Work):
  - Miner bestätigen neue Blöcke, indem sie Hashwerte berechnen (siehe Bitcoin)

- Proof of Stake:
  - Miner bestätigen neue Blöcke, indem sie diese mit ihren alten Schlüsseln signieren

ZCash

- Bitcoin-Adressen sind Pseudonyme
- Bitcoin-Transaktionen sind signiert mit ECDSA

- ZCash (früher auch Zerocoin, dann Zerocash) führt anonyme Transaktionen ein
- Es ist allgemein nachvollziehbar, welche Transaktionen gültig sind.
- Es ist jedoch nicht sichtbar, von welchem Schlüssel zu welchem anderen Schlüssel eine Zahlung erfolgt.
- Dies wird mit sogenannten Zero-Knowledge-Beweisen erreicht (daher der Name).

ZCash – Anonyme Transaktionen

- Transaktion bei Bitcoin:
  - Alice sendet Bob Geld, indem sie eine Transaktion mit dem Schlüssel ihres Kontos signiert

- Transaktion bei ZCash:
  - Alice sendet Bob Geld, indem sie eine Transaktion mit einem Beweis signiert, dass sie die Münze besitzt und noch nicht ausgegeben hat, ohne das Konto mit dieser Münze zu nennen

Danke

Stephan Verbücheln
stephan.verbuecheln@cnlab.ch
+41 55 214 33 36

Martina Minges
martina.minges@cnlab.ch
+41 55 214 33 42