Beyond Bitcoin - Blockchain Anwendungen in der Praxis

Dr. Uwe Ziegenhagen

24. August 2018

www.uweziegenhagen.de

Über mich

- Uwe Ziegenhagen aus Köln
- Studium von BWL & Statistik
- Arbeite in Credit & Treasury Operations
  für eine Düsseldorfer Bank
- LaTeX, Dingfabrik
- bin kein Blockchain-Experte, habe keine Cryptocoins

Motivation

Motivation

- „Bitcoin“ hier, „Blockchain“ dort, jede Woche neues ICO
- Bitcoin-Preise hoch volatil, Millionen gewonnen und wieder verloren
- „Long Island Iced Tea“ nennt sich „Long Blockchain“ $\Rightarrow$ 500% Kursanstieg, „Longfin“ Aktie steigt um 1300% nach Ankündigung, eine Cryptocoin-Firma kaufen zu wollen
- Sacha Lobo: „Bitcoin ist nur deshalb so viel wert, weil so viele Menschen daran glauben, dass Bitcoin so viel wert ist.“
- Erinnerungen an Tulpen-Manie im 17. Jahrhundert

Diese Präsentation

Ziel: Überblick zum Thema „Blockchain“

- Kurzer Abriss zur Geschichte
- Technologie anhand von Bitcoin erklären
- Vorstellung verschiedener Blockchain-Anwendungen

Historie I

- Geschichte von „Blockchain“ beginnt nicht mit Bitcoin
- Idee von dezentraler Währung reicht weit zurück
- Steinwährung auf dem Ulithi Atoll in Mikronesien, „Münzen“ bis 5 Tonnen Gewicht
- Wert wird bestimmt von der Mühe, Stein aus 400 Km über das Meer zu schaffen
- Physischer Transport unpraktikabel, stattdessen wird das Wissen verbreitet, wem welcher Stein gehört
- `https://de.wikipedia.org/wiki/Rai_(Währung)`

Historie II

- „Agoric Computing“ in den 1970ern/1980ern
- „Agora“: Zentraler Markt- und Versammlungsplatz in antiken griechischen Städten
- Idee: Auktionen und Ressourcen-Management in Software implementieren
- „Smart Contract“ Begriff geprägt von Nick Szabo 1994, Idee:

Bitcoin

- 2008: Globale Finanzkrise: Subprime
- Satoshi Nakamoto: „Bitcoin: A Peer to Peer Electronic Cash System“[1]
- Beschreibt ein Protokoll für eine dezentralisierte Währung, die in einem Netzwerk gehandelt wird, in dem sich die Teilnehmer nicht untereinander vertrauen
- Satoshi Nakamoto: Person? Gruppe?
- 2009: Bitcoin wird veröffentlicht, 12/2017: $\approx$ 18’000 USD, aktuell 6’500 USD

[1] `https://bitcoin.org/bitcoin.pdf`

Was ist die Blockchain

Zurück auf die Insel[2]

- Ausweitung des Handels auf der Insel
- Älteste können sich nicht alles merken
- Ein Buchhalter wird bestimmt, anfällig für Bestechung
- Ein Buchhalter pro Stamm, führt jeweils ein Buch über alle Transaktionen der Insel
- Neue Transaktionen werden auf dem Marktplatz ausgerufen
- Mehrheit entscheidet bei Unstimmigkeiten

[2] https://cryco.info/rai-mutter-der-blockchain/

Buchbeispiel 1

Abbildung 1: Quelle: Drescher (2017)

Buchbeispiel 2: Referenz auf vorherige Seite

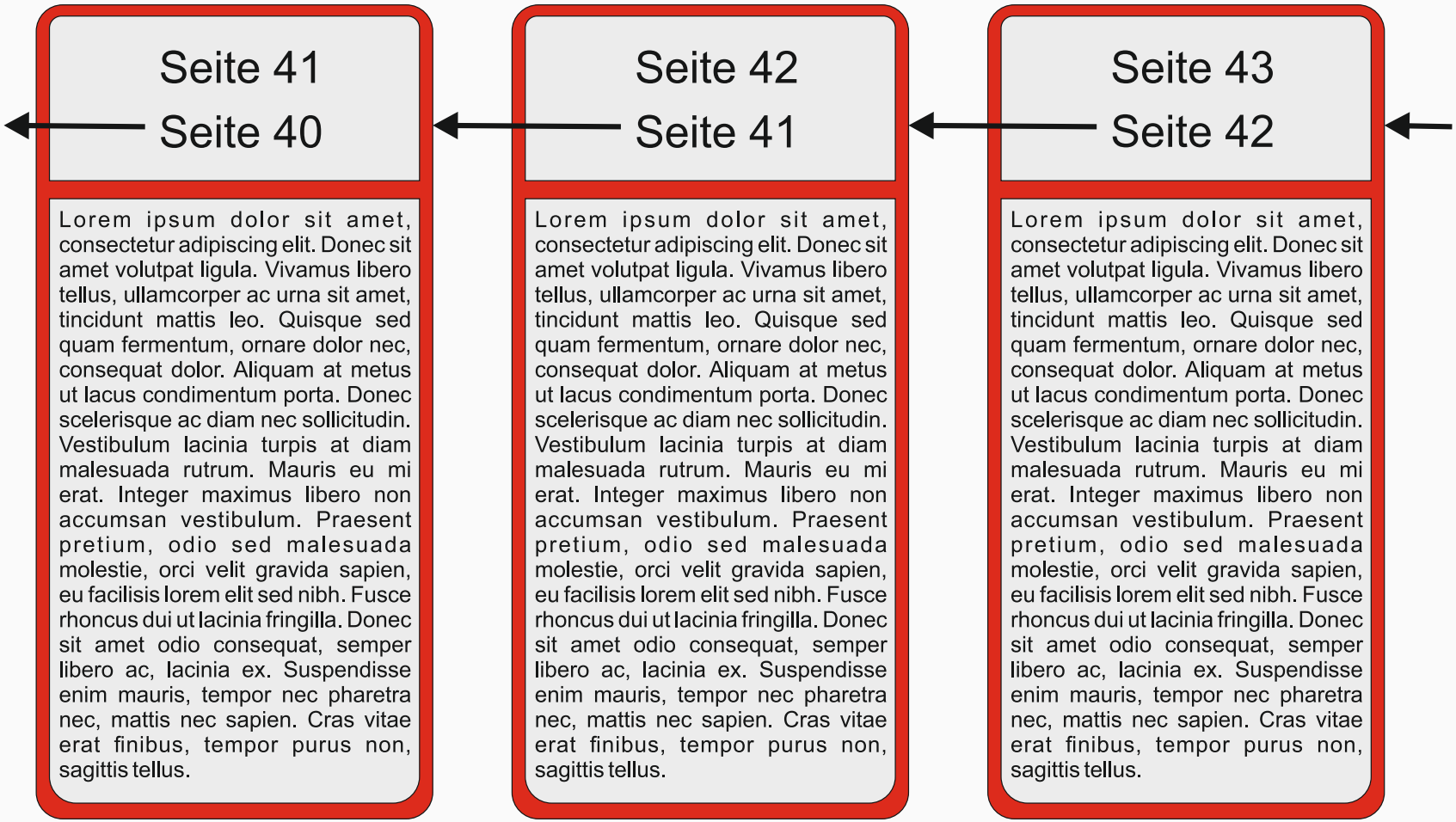

Abbildung 2: Quelle: Drescher (2017)

Buchbeispiel 3: Trennung Inhalt und Kopf

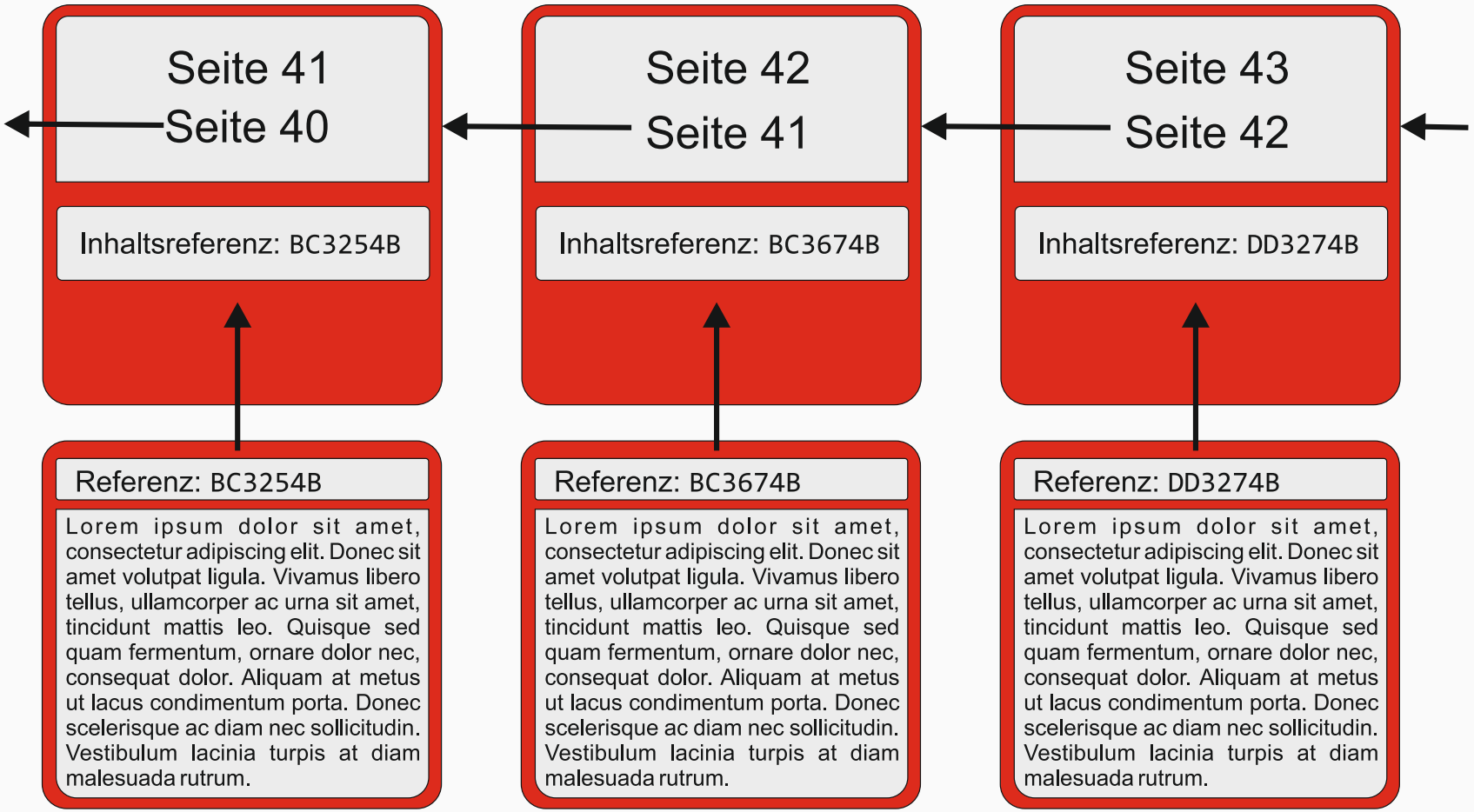

Abbildung 3: Quelle: Drescher (2017)

Buchbeispiel 4: Hashes

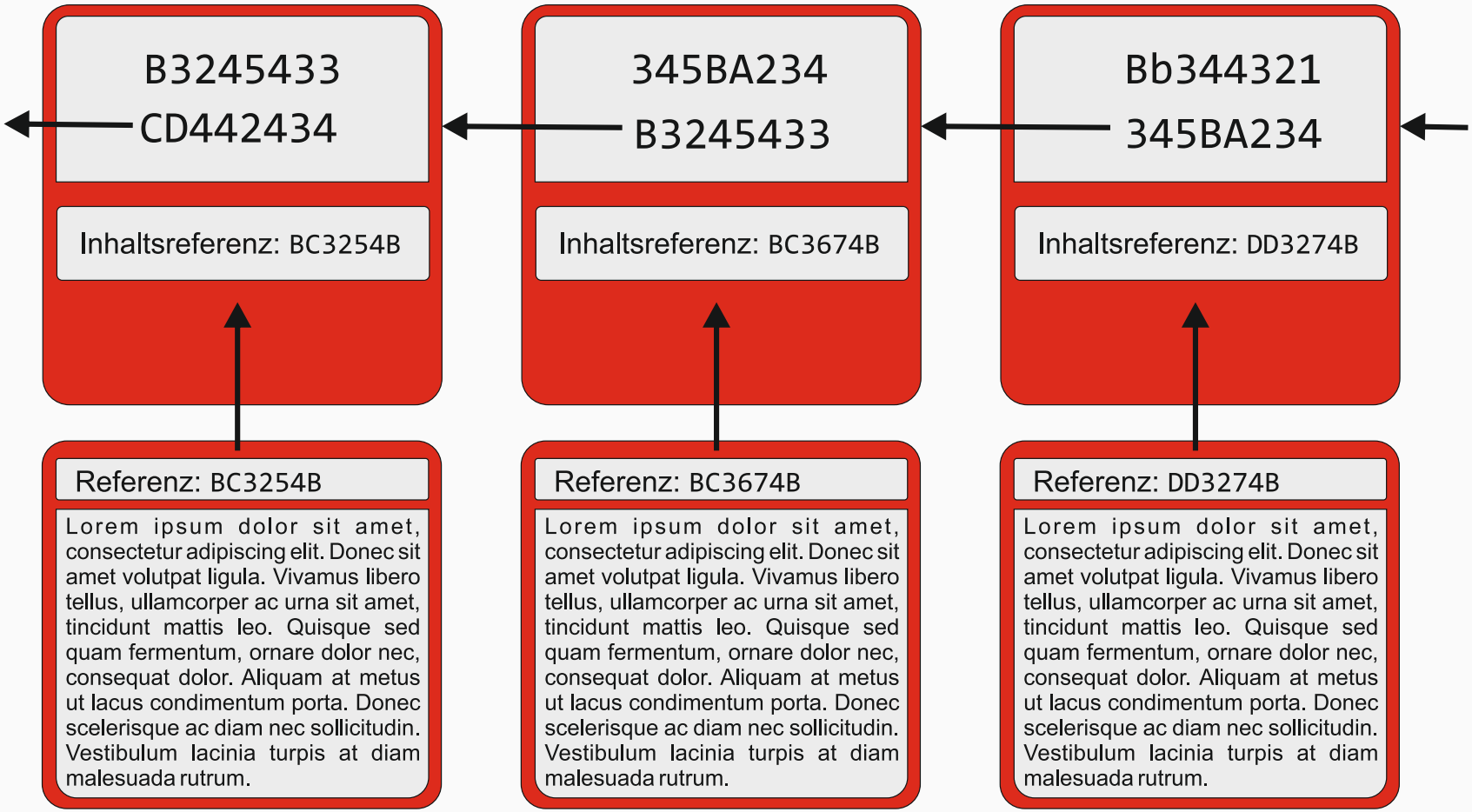

Abbildung 4: Quelle: Drescher (2017)

Buchbeispiel 5: Hashes

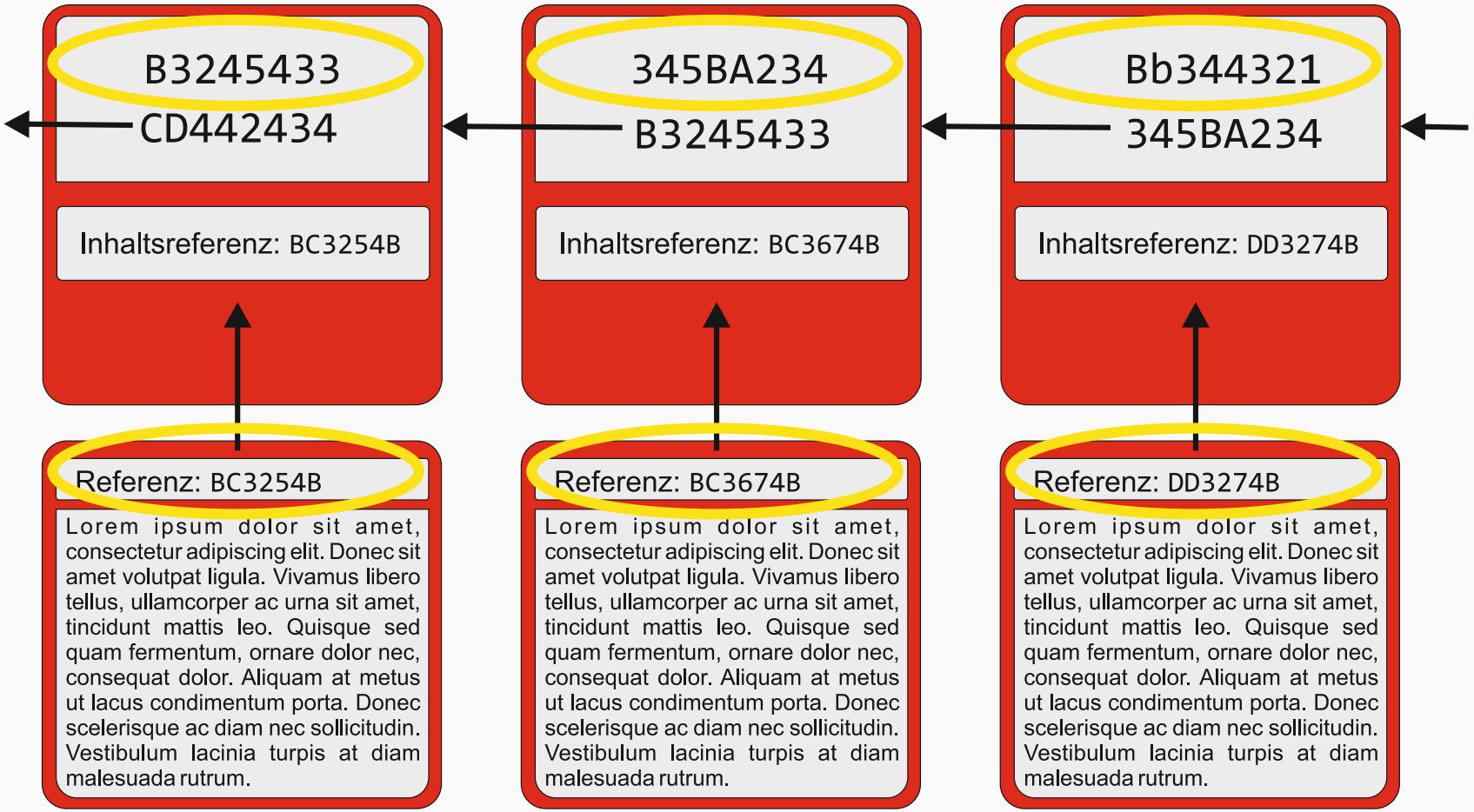

Abbildung 5: Quelle: Drescher (2017)

Buchbeispiel 6: Ergebnis

- Alle Seiten mit ihren Inhalten sind referenziert
- Blockchain als verteiltes elektronisches Buch
- Hash-Summen erlauben Check, ob Inhalt manipuliert wurde

Hash-Funktionen

- bilden Zeichenketten beliebiger Länge auf Zeichenfolgen fester Länge (dem „Hash“) ab
- Aus dem Hash kann man nicht auf die ursprüngliche Zeichenkette schließen
- Kollisionsresistenz: Es soll praktisch unmöglich sein, mehrere Zeichenketten mit identischem Hash zu finden
- Bekannte Algorithmen

  MD5 Häufig zu sehen, nicht zu empfehlen

  SHA-256 Wird von Bitcoin verwendet
- Siehe `https://hashgenerator.de`

Bitcoin: Blockchain

- Blockchain: Eine Kette von Datencontainern, Verbindung zum vorherigen Block immer vorhanden
- Container enthält Daten (bei Bitcoin: Transaktionen)
- Vergleichbar zu Transaktionsbuch in der Buchführung, verteilt auf tausende Computer („Distributed Ledger“)
- Jeder Block enthält Hashwert des vorigen Blocks
- Historie grundsätzlich gegen Manipulation geschützt

Blockchain Visualisierung

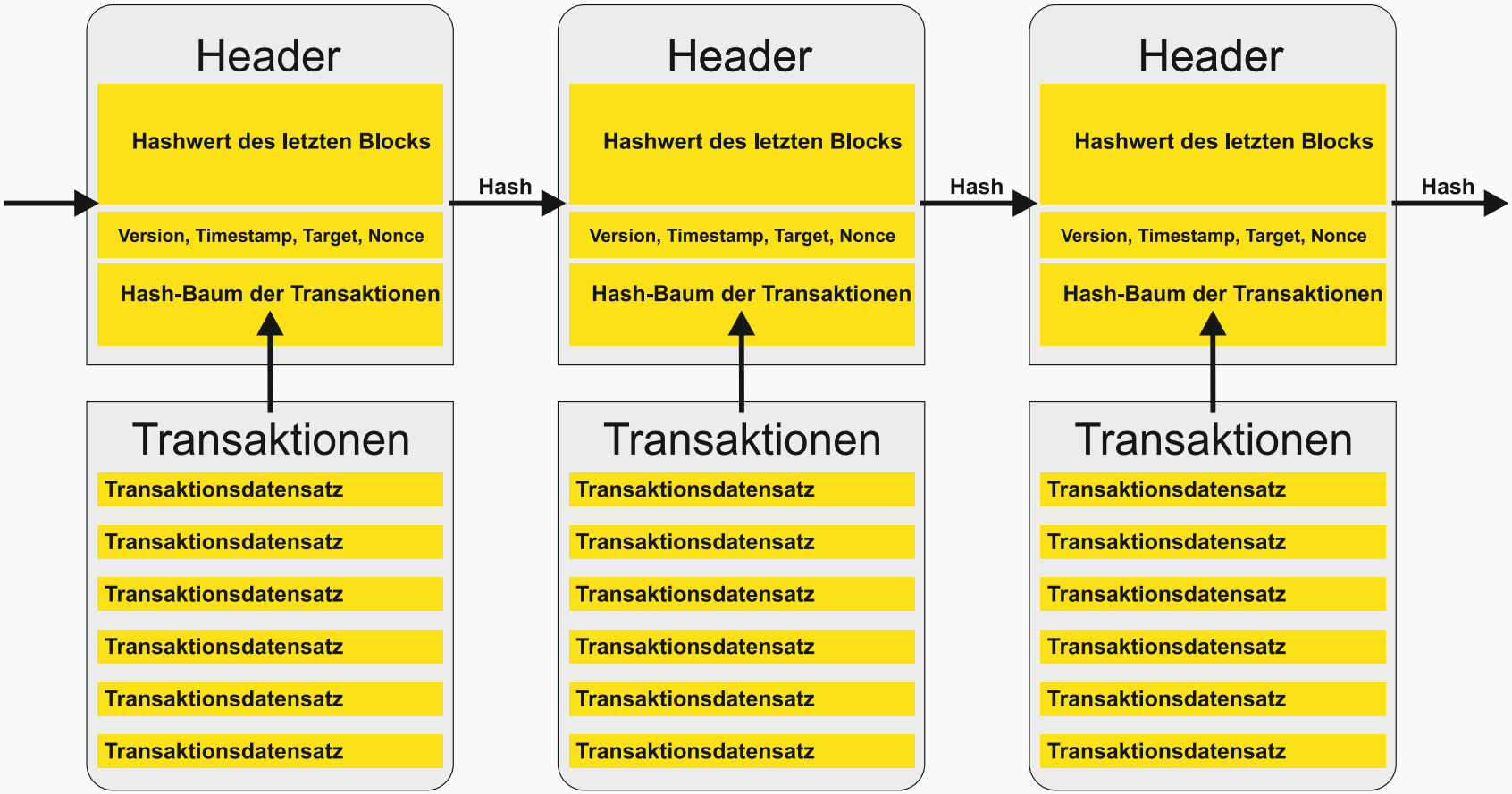

Abbildung 6: Quelle: Wikipedia,

`https://de.wikipedia.org/wiki/Blockchain`

Bitcoin: Funktionsweise[3]

Wie beginnt man mit Bitcoin?

- Erzeuge Schlüsselpaar aus public und private key
- Bitcoin-Adresse (das öffentliche Konto) wird gebildet aus Hash des public key
- Jeder weiß, wieviel auf dem Konto ist, aber nur der Besitzer des Private Key kommt ran
- Bitcoins besorgen: kaufen gegen echtes Geld oder selber „minen“

[3] https://www.heise.de/ct/artikel/So-funktioniert-die-Kryptowaehrung-Bitcoin-3742304.html

Bitcoins minen (Einfach erklärt)

- Gute Beschreibung unter `https://bitcoinblog.de/2015/08/05/bitcoin-ganz-einfach-wie-entstehen-neue-bitcoins/`
- Würfelspiel mit zwei Spielern, wer eine 6 würfelt, bekommt 50 Dicecoins gutgeschrieben
- Schwierigkeit wird so angepasst, dass im Mittel alle n Minuten neue Coins entstehen (z. B. zwei 6en erforderlich, zehn 6en, 1000 6en)

Bitcoins minen

- Installiere Bitcoin Software
- Hole Transaktionen aus Transaktionspool
- Datensatz („Candidate Node“) erzeugen aus:

Version Versionsnummer der Bitcoin Software
Previous block hash Referenz letzter Block
Merkle Root Struktur aller Transaktionen im Block
Timestamp Zeitstempel
Target 256-bit Zahl
Nonce Integer-Zahl

Target

- Target ist Bedingung, die es zu schlagen gilt
- So gewählt, dass im Mittel alle 10 Minuten ein neuer Block gefunden wird[4]
- neuer Hash größer als Target: Nonce erhöhen, nochmal rechnen
- Hash kleiner als Target: neuer Block entsteht, Miner erhält Belohnung in Form von Bitcoins
- Beispiel-Target: neuer Hash muss mit 25 Nullen beginnen

[4] Begrenzt auch die Anzahl der Transaktionen pro Minute

Transaktionen

- Transaktionen liegen im Memory Pool vor, der Sammlung unbestätigter Transaktionen
- Miner bekommt Transaktionsgebühr dafür, dass er eine Transaktion bestätigt
- Je höher diese Gebühr, desto eher wird die Transaktion berücksichtigt
- Gebühr wird in satoshis pro KB Transaktionsdaten gemessen (1 satoshi = 0.00000001 BTC)
- Bitcoin Miner nimmt *n* Transaktionen und baut sie in den neuen Block ein
- Andere nodes validieren neuen Block, fangen mit neuem Block an

Bitcoin Mining Pools

- Miner erhält zusätzlich zur Fee noch Bitcoins als Belohnung, aktuell 12.5 BTC/Block
- „Winner takes it all!“, alle anderen haben umsonst Energie „verbraten“
- Wahrscheinlichkeit, allein einen Block zu finden, ist sehr gering
- Mining Pools: tausende Miner schließen sich zusammen, Gewinn wird aufgeteilt
- Keine gesetzliche Regelung zur Gewinn-Teilung

Blockchain: Längste Kette

- Beispiel: Blockchain ist 20’000 Blöcke lang
- Zwei Miner A und B finden unabhängig voneinander nächsten Block, Block 20’001a bzw. Block 20’001b
- Senden ihre Blöcke an das Netz, weitere Nodes knüpfen an Block 20’001a oder Block 20’001b an
- Eine Kette setzt sich durch, Transaktionen der anderen gehen verloren
- Bis eine Transaktion wirklich validiert ist, braucht es mehrere Blöcke

Blockchain: Längste Kette

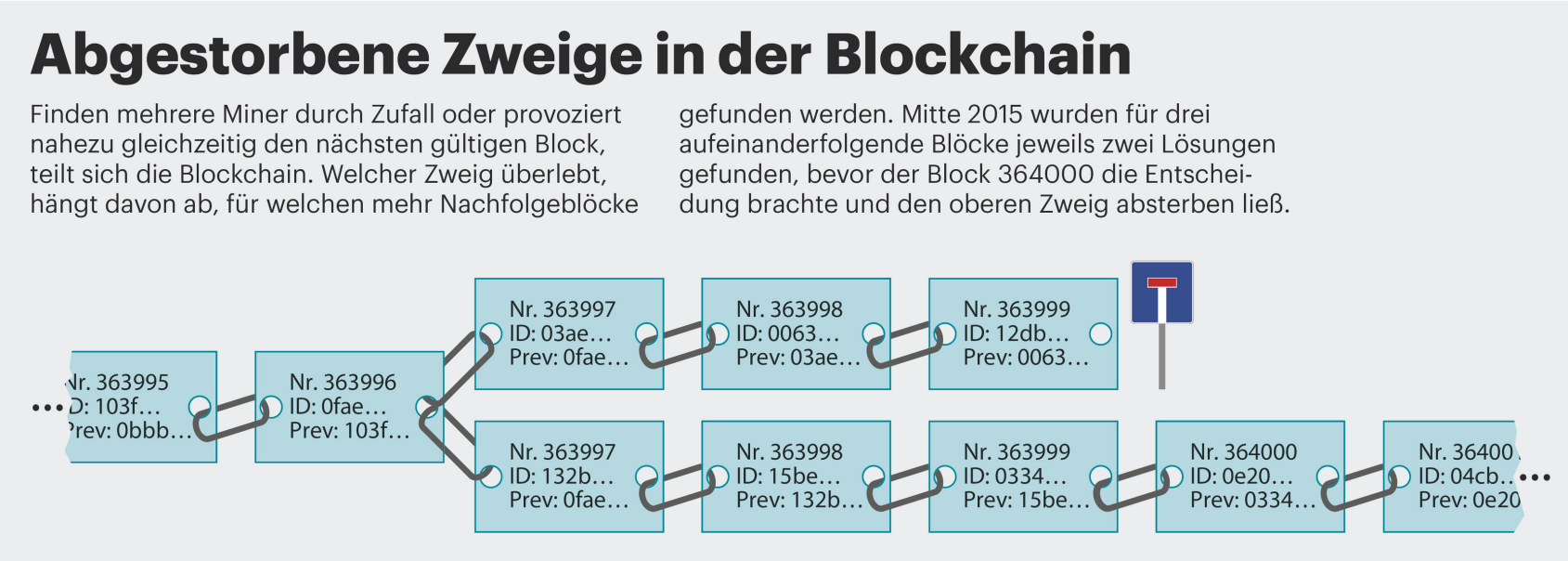

Abbildung 7: Quelle: „Wie abgeschlossene Transaktionen aus der Blockchain verschwinden“, c’t 8/2018

51% Problem

- Bitcoin Gold am 16.05.2018: 51% Attacke
- 170 MH/s-Mehrheit an Rechenleistung lässt Transaktionen sterben, Rest von 30 MH/s
- Schritt 1: Kriminelle haben neuen Block gefunden, aber nicht kommuniziert
- Auf Basis des neuen Blocks weitere Blöcke insgeheim geschürft, eigener Zweig
- Schritt 2: Verkauf von Bitcoin Gold an Händler, diese Transaktionen nur in offizieller Blockchain
- Schritt 3: Zweiter Verkauf der BCG an Händler, diese Transaktionen in eigenem Zweig
- Schritt 4: Veröffentlichung des eigenen Zweigs als offizielle Chain, erster Verkauf verschwindet damit.

51% Problem

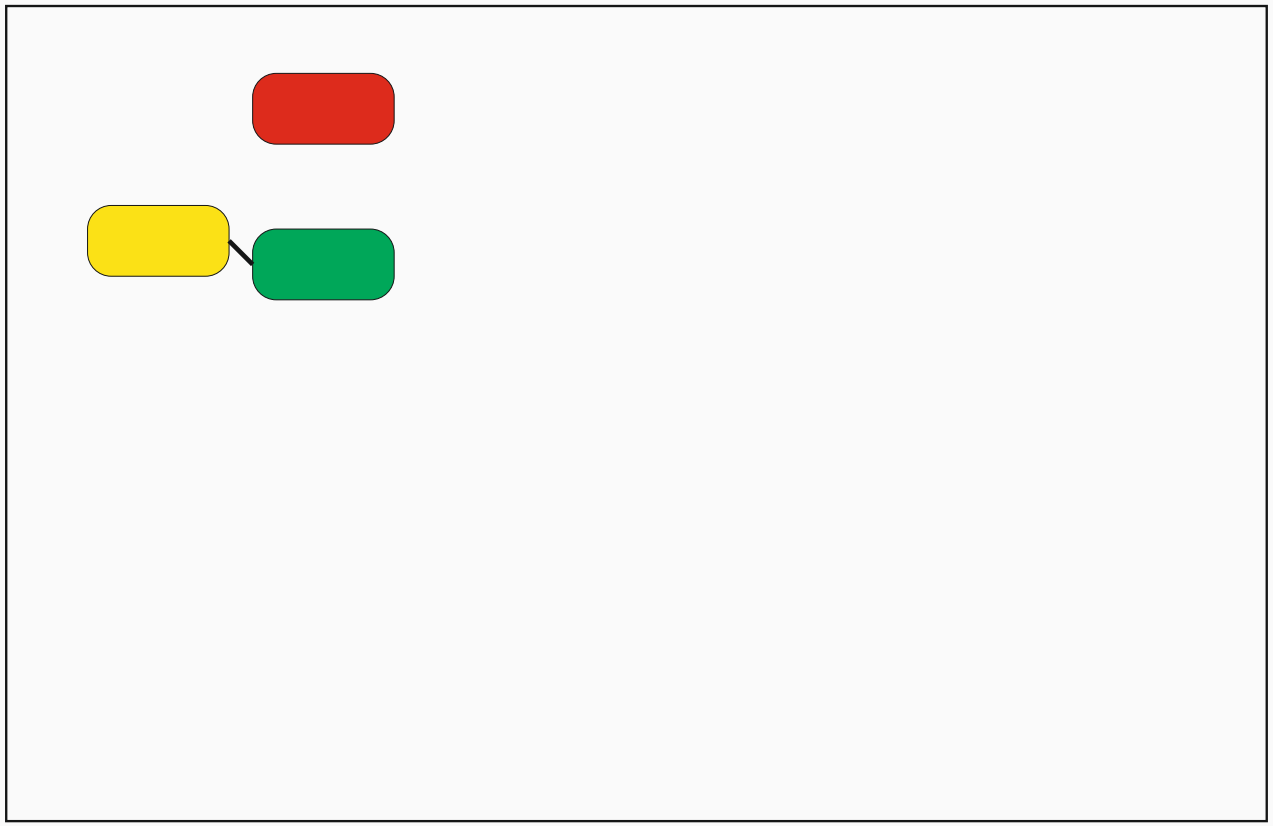

Abbildung 8: 51% Attacke: „Böse Buben“ finden auch Block

51% Problem

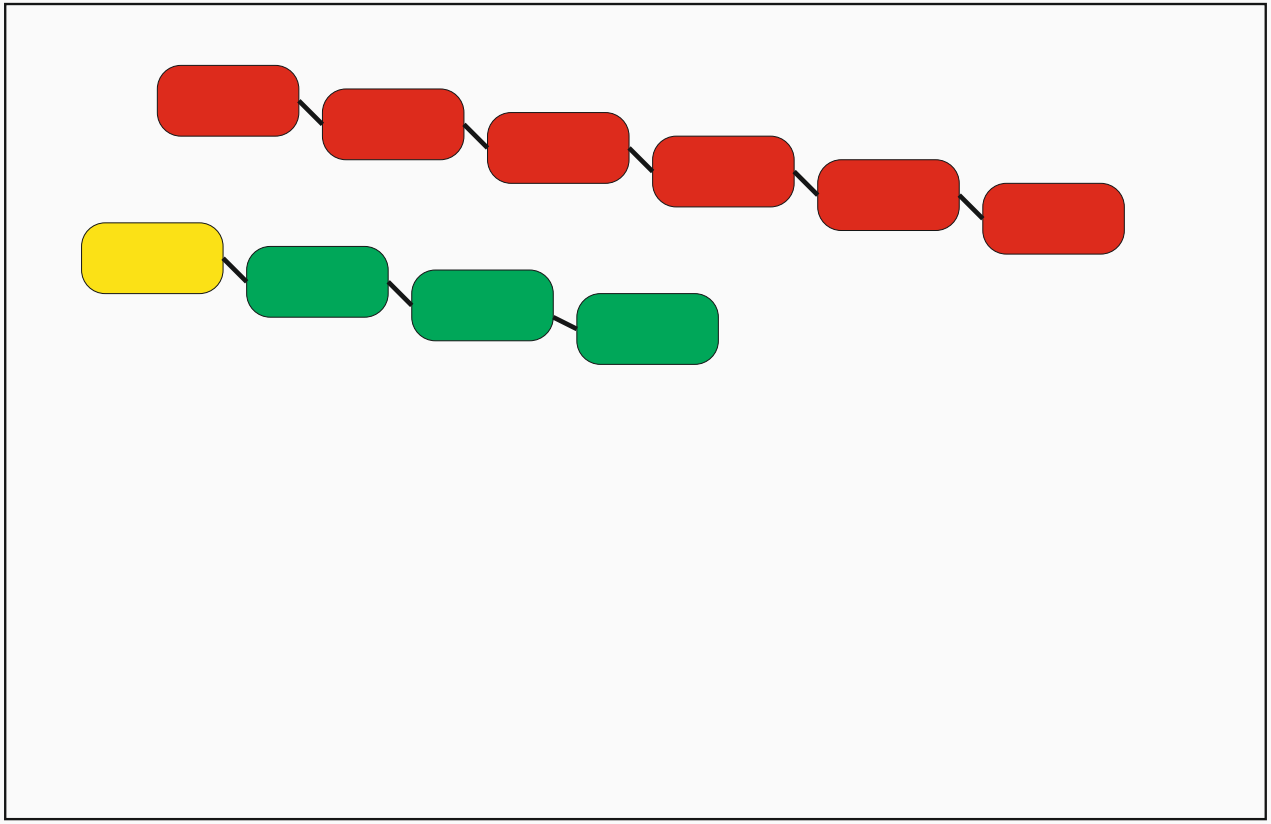

Abbildung 9: 51% Attacke: „böse Kette“ wächst länger

51% Problem

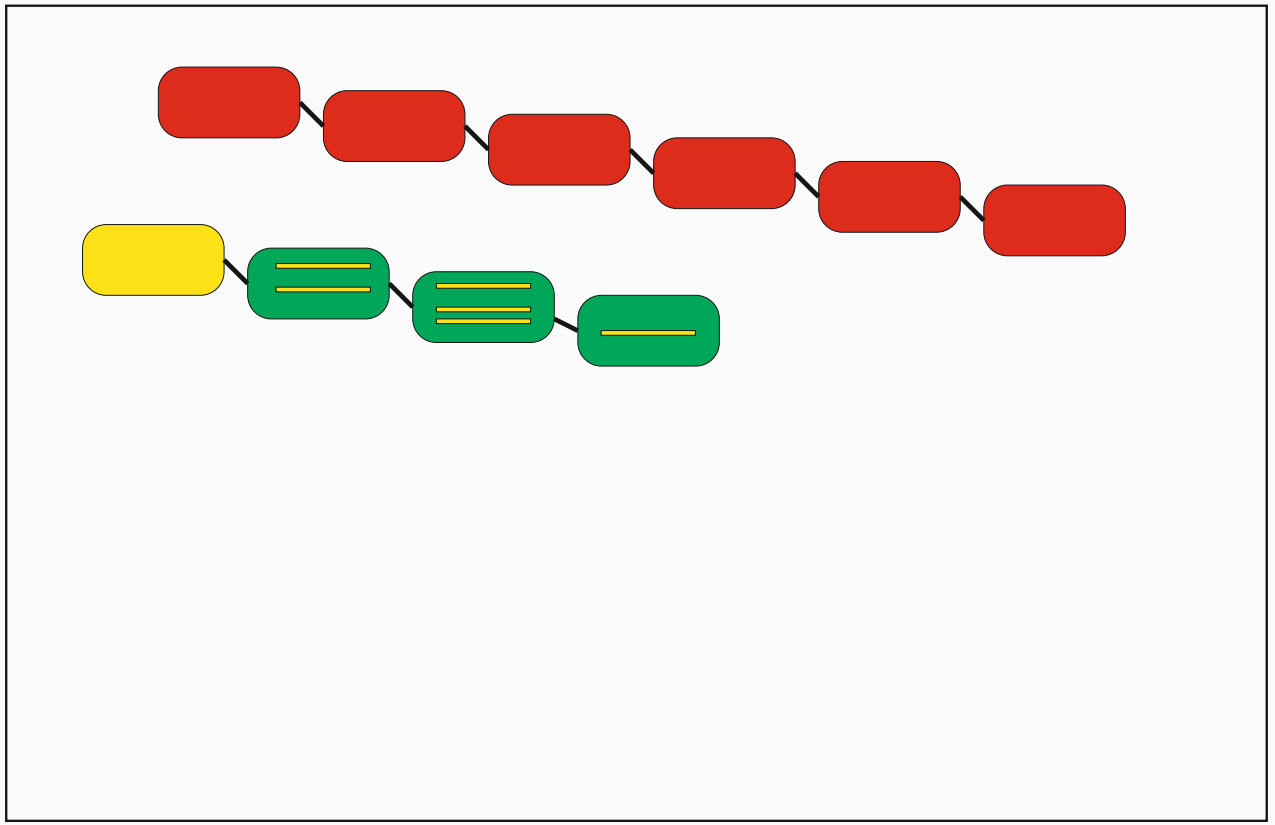

Abbildung 10: 51% Attacke: Legitime Transaktionen der „bösen Buben“

51% Problem

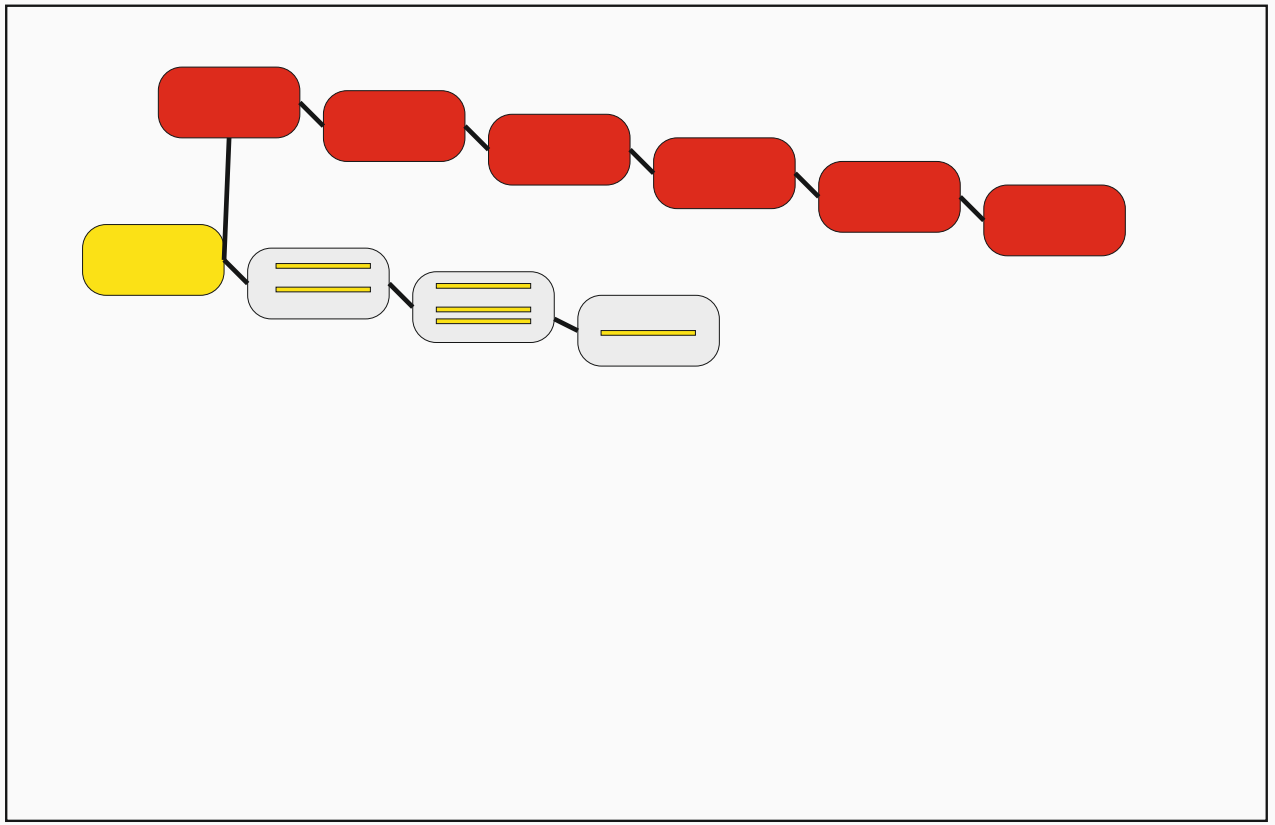

Abbildung 11: 51% Attacke: Publizierung der bösen Kette löscht gute Transaktionen

Zwischenfazit

- Kryptowährungen sind hoch spekulativ!
- Funktionieren nur, solange es Leute gibt, die einen Wert darin sehen
- Kosten Unmengen an Ressourcen!
- Sind nicht anonym!
- Werden mehr und mehr reguliert werden!

Gibt es sinnvolle Anwendungen der Technologie?

Blockchain

- Blockchain zweites Buzzword neben Bitcoin
- Google: „Ungefähr 140.000.000 Ergebnisse“
- „2016 Wall Street blockchain investment to top $1bn“
- hat Potential, „Disruptive Technologie“ zu sein
- Beispiele für Disruptive Technologien: Auto, Audio/Video Streaming

Blockchain Anwendungen

Herausforderungen in der Wirtschaft

- Wartezeiten bei Abwicklung von Transaktionen
- Unterschiedliche Informationsstände
- Inkompatible Systeme im Warenverkehr
- Gefahr von Betrug und Diebstahl durch Manipulation
- Mehrfache KYC-Prozesse
- Aufwändige Vertragserstellung (Konsortialkredite)
- Hohe Personalaufwände

IBM: Blockchains for Food Safety[5]

- Mehr Lebensmittelsicherheit durch Blockchain
- Fehlender Zugang zu Informationen, schlechte Rückverfolgbarkeit
- Ziel: Verunreinigte Produkte schnell identifizieren und zur Quelle zurückverfolgen
- IBM, Walmart, Dole und andere arbeiten zusammen
- Tracking von der Erzeugung bis zum Verkauf
- Barcodes auf einzelnen Bananen?

[5] `www-03.ibm.com/press/de/de/pressrelease/53029.wss`

Tru Budget - Entwicklungshilfe tracken[6]

- KfW = Kreditanstalt für Wiederaufbau
- Zahlt Entwicklungshilfe nach Afrika, viel versickert in dunklen Kanälen
- Blockchain: Mehr Transparenz, Transaktionen nicht mehr veränderbar
- Einsparung von Transaktionskosten
- Herausforderung: Schlechte Basis-Bedingungen, Infrastruktur

[6] https://www.devfinance.net/blockchain-track-public-spending-africa/

Beweisketten sichern mit Chronicled

- `chronicled.com/physical-chain-of-custody`
- Blockchain-basierte Beweiskette
- Sicherheits-Tags (NFC)
- Jede Interaktion mit Objekt wird in Blockchain vermerkt
- Soll Manipulation von Beweisen verhindern

KYC-Projekt von IBM & Crédit Mutuel Arkéa

- KYC = Know Your Customer, mit wem macht man Geschäfte?
- Verschiedene Geschäftszweige, kein einheitliches Stammdatenmanagement
- Einheitliche Stammdaten-Datenbasis über Blockchain
- einmal eingegebene Daten sind für alle (sofort) sichtbar

Schöner sterben mit Blockchain

- `blockchainapparatus.com/smart-contracts`
- Smart contract für die Zeit nach dem Leben
- Getriggered durch „Death Master File“
- Regelbasierte Verteilung der Assets

Literatur

Empfohlene Literatur

- Daniel Drescher (2017), *Blockchain Basics – A Non-Technical Introduction in 25 Steps*, ISBN 978-1-4842-2604-9
- `https://www.mckinsey.com/industries/financial-services/our-insights/the-promise-of-blockchain`
- Bettina Warburg, „How the blockchain will radically transform the economy“, `https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy`

That’s all, folks!

- Überblick zu Blockchain & Smart Contracts
- Thema wird „heiß“ bleiben, sinnvolle Anwendungen möglich
- Wird unser Leben beeinflussen
- Kommentare und Anmerkungen zum Vortrag sind willkommen
- Am Stand von Dante e. V. in der Mensa oder unter ziegenhagen@gmail.com