IT-Tage 2017

11. – 14.12.2017
Frankfurt am Main

Dr. Jürgen Lampe

Blockchain-Essentials

#ittage

S&N INVENT

S&N Invent ist ein bundesweit aufgestelltes IT-Beratungs-Unternehmen mit der Dachgesellschaft S&N Group AG und den Tochtergesellschaften S&N Invent GmbH, ABISCON GmbH, ABISCON SAS GmbH und S&N CQM GmbH.

Branchenübergreifend bieten wir unseren Kunden ein ganzheitliches Leistungsspektrum für Ihren IT-Lifecycle mit einem soliden Fundament aus aktueller Architektur-, Technologie- und Methodenkompetenz.

Ergänzt wird dieses umfassende Leistungsportfolio um langjährige Projekterfahrung und ausgeprägte Branchen-expertise in der Finanz- und Versicherungswirtschaft und aktuelles SAP-Technologie-Know-how.

Neue Zürcher Zeitung

GASTKOMMENTAR

Blockchain – eine Technologie revolutioniert unser ganzes Denken

Milosz Matuschek
2.10.2017, 05:30 Uhr

Kein Vergleich zur Automobil-, Chemie- oder Bergbauindustrie alten Schlages oder der Gerontokratie der Aufsichtsräte. Die «New Kids on the Blockchain» profitieren derzeit auch davon, dass der Kern ihrer Technologie sich intuitiv nicht so leicht erschliesst und demnach fast als eine Art esoterisches Wissen im Kreise Eingeweihter zirkuliert. Erst wenn eine kritische Grösse erreicht ist, werden die Ausläufer dieser neuen Welt für jedermann sichtbar sein.

https://www.nzz.ch/meinung/kommentare/new-kids-on-the-blockchain-ld.1319020

Inhalt

- Blockchain
  - Begriff und Abgrenzung
- Technische Grundlagen
  - Kryptografische Hash-Funktionen
  - Merkle-Damgard-Transformation
  - Blockchain
- Dezentralisierte Buchführung
  - Idealisierte Version
  - Proof-of-Work-Version
- Grenzen und Probleme
- Fazit

Blockchain: Was ist das?

- Ein Hype

> *„Es tut mir leid für Sie, aber in zehn Jahren werden alle Ihre Banken nicht mehr existieren“, schleuderte in Davos ein Blockchain-Pionier der versammelten Hochfinanz entgegen. … Selbst Skeptiker wie Edward Budd von der Deutschen Bank in London räumen der Blockchain „gewaltiges Potential“ ein.*
>
> (FAZ, 16.03.2016, B. Weiguny: Bargeld, Banken und Betrüger)

- Eine Worthülse

> *Die ReiseBank und die kanadische ATB Financial haben erstmals eine transatlantische Zahlung mittels der Ripple-Blockchain-Technologie durchgeführt*
>
> (*ReiseBank AG, 19.07.2016:* http://www.presseportal.de/pm/116526/3382017)

> *Entwicklung bei Ripple: XRP->RCP->ILP (schon RCP war keine „Blockchain“ aus puristischer Sicht, da es einfach keine „Blöcke“ gab, sondern Einzeltransaktionen validiert wurden.*
>
> (*Dr. U. Milkau: Erste Erfahrungen mit der Blockchain in der Praxis, Frankfurt, 13. Sep. 2017*)

Abgrenzung

- Alle reden von *Blockchain* – meinen aber ganz unterschiedliche Dinge:
  - Spezielle Verkettung von Blöcken
  - Verfahren für ein verteiltes *Ledger of Transactions* (richtiger: verteiltes dezentrales Journal)
  - Die gesamte hinter Bitcoins u. Ä. stehende Technologie
  - *Smart Contracts*, Sofort-Überweisungen, …

- Fragen zu Authentifizierung, Identität, unverfälschter Übertragung usw. werden hier nicht betrachtet
  - Mit Public-Private-Key-Verschlüsselungsverfahren praktisch lösbar (s. Bitcoins)

Zielsetzung

- Zuverlässige *Geschäfte* (Transaktionen) in einem Netzwerk ermöglichen, unter folgenden Bedingungen:
  - Keine zentrale Teilnehmerverwaltung
  - Teilnahme/Nichtteilnahme jederzeit möglich
  - Keine zentrale Datenhaltung, aber gemeinsames Journal (Ledger)
  - Geringe Anforderungen an die Zuverlässigkeit der Teilnehmer („vertrauensloses“ Netzwerk)
  - Stabil gegen zeitweilige Verbindungsfehler

- Anmerkung: Nur wenn eine Anwendung diese Bedingungen tatsächlich einfordert, kann die Blockchain eine angemessene Lösung sein.

Technische Grundlagen: Kryptografische Hash-Funktionen

Hash-Funktion H(x)

Argument *x*: Zeichenkette fester Länge (z. B. 768 Bit), auf beliebige Länge erweiterbar

Ergebnis *y= H(x)* hat feste Länge (z. B. 256 Bit)

Funktion ist effizient berechenbar, d. h. für *n = length(x)* mit (Laufzeit-)Aufwand *O(n)* bestimmbar

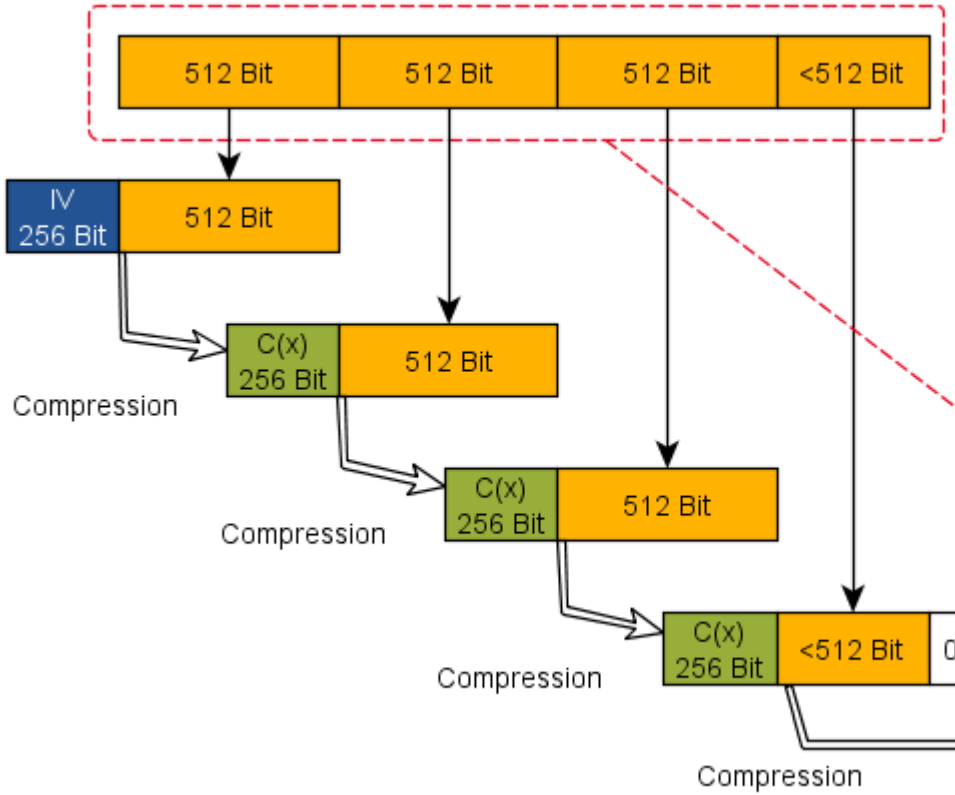
Kryptografische Hash-Funktionen müssen zusätzliche Bedingungen erfüllen:

- **Kollisionssicherheit:** *praktische* Unmöglichkeit, x und y so zu finden, dass zwar $x \neq y$, aber $H(x) = H(y)$ gilt
- **Verbergend:** für unbekanntes, zufälliges r, ist es praktisch unmöglich aus $y = H(r \| x)$ auf x zu schließen
- **Rätselfreundlich:** für jedes n-Bit *y* und ein zufällig gewähltes *k* ist es praktisch unmöglich mit einem zeitlichen Aufwand deutlich unter $O(2^n)$, ein *x* zu finden, sodass $y = H(k \| x)$

Häufig verwendet: **SHA-256** (***S**ecure **H**ash **A**lgorithm* mit Hash-Länge **256**)

Merkle-Damgard-Transformation

Hashberechnung einer beliebig langen Eingabekette



Anwendung einer Hash-Funktion, die für Eingaben fester Länge definiert ist (=***Compression***-Funktion) auf Eingaben beliebiger Länge

Kollisionssicherheit bleibt dabei (beweisbar!) erhalten

IV: Initialisierungsvektor (beliebig, aber fest)

Blockchain
(im eigentlichen/engen Sinn)

Ausgangspunkt: Daten als Schlüssel-Wert-Paare (Key-Value)

Hashpointer (Key)

Ein Schlüssel, der aus dem Hash-Wert der Daten bzw. des Datenblocks (Value) besteht.

Garantiert damit gleichzeitig die Integrität der Daten.

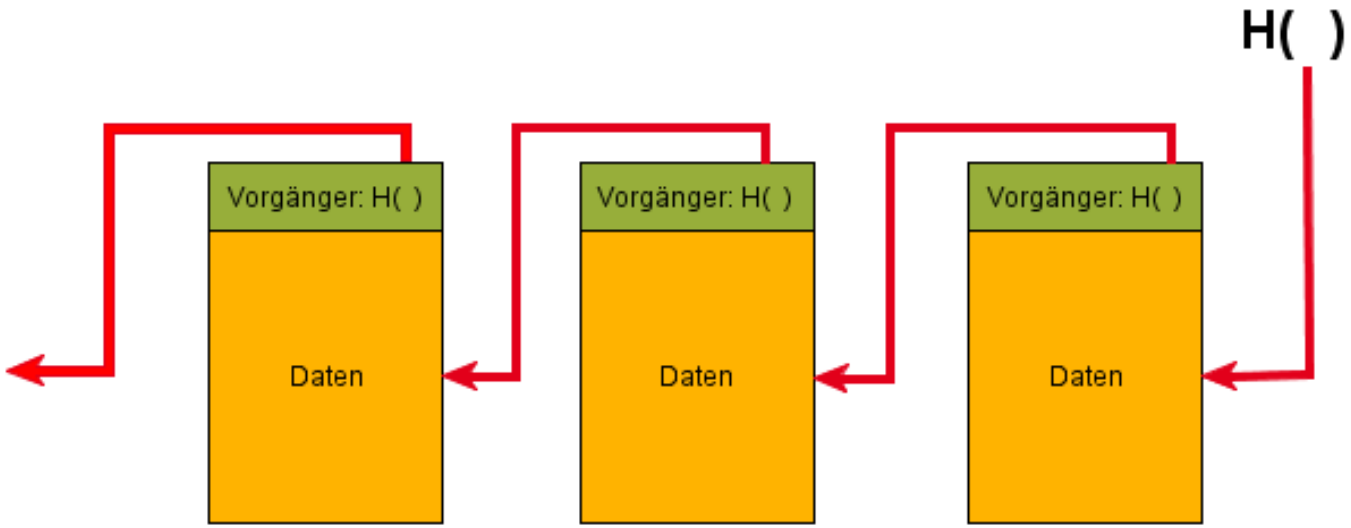
Blockchain

Eine Kette von über Hashpointer miteinander verknüpften Datenblöcken, wobei der Verweis (= Hashwert) auf den Vorgängerblock in die Berechnung des Hashwerts des aktuellen Blocks einbezogen wird.

$$H(Block_{aktuell}) = H(\boxed{H(Block_{voriger})} \,\|\, Daten_{aktuell})$$

Hashpointer des vorangehenden Blocks

Blockchain (Block-Kette)



- Verkettete Liste mit Hashpointern anstelle „normaler“ Verweise
- Beginnt mit einem speziellen Start-Block (*„genesis block“*)
- Kann nicht unbemerkt verändert werden (Inhalt u. Pointer), weil die Adresse (=Hashpointer) aus Inhalt und Verweis auf Vorgänger berechnet wird

Dezentralisierte Buchführung: Voraussetzungen

- *Peer-to-peer*-Verbindungsstruktur, Kommunikation: *Gossip-Protocol*
- Es gibt „Geschäftemacher“ und Buchführer (Teilnehmer-Rollen, nicht notwendig disjunkt)
- Teilnehmer können sich beliebig dazu- oder abschalten
- Jedes **Geschäft** wird an alle Teilnehmer publiziert
- Anzahl von Buchführern nicht beschränkt
- Alle Geschäfte werden in einem globalen Geschäftsbuch konsolidiert
- Jeder Teilnehmer hat eine Kopie des globalen Geschäftsbuchs (für Geschäftemacher optional)
- Jede neue **Seite des Geschäftsbuchs** wird an alle publiziert

➔**Probleme / Fragen:**

- Wer publiziert Geschäftsbuchseiten?
- Wie beugt man Manipulationen vor?

Kernproblem:
Verteilter Konsens (distributed consensus)

Verteiltes Konsensprotokoll

- Muss terminieren mit übereinstimmender Meinung aller *gutartigen* Knoten.
- Die akzeptierte Meinung muss von einem gutartigen Konten erzeugt worden sein.

Schwierig/unmöglich zu realisieren, deshalb pragmatisches (wahrscheinlichkeitsbasiertes) Vorgehen.

Impliziter Konsens

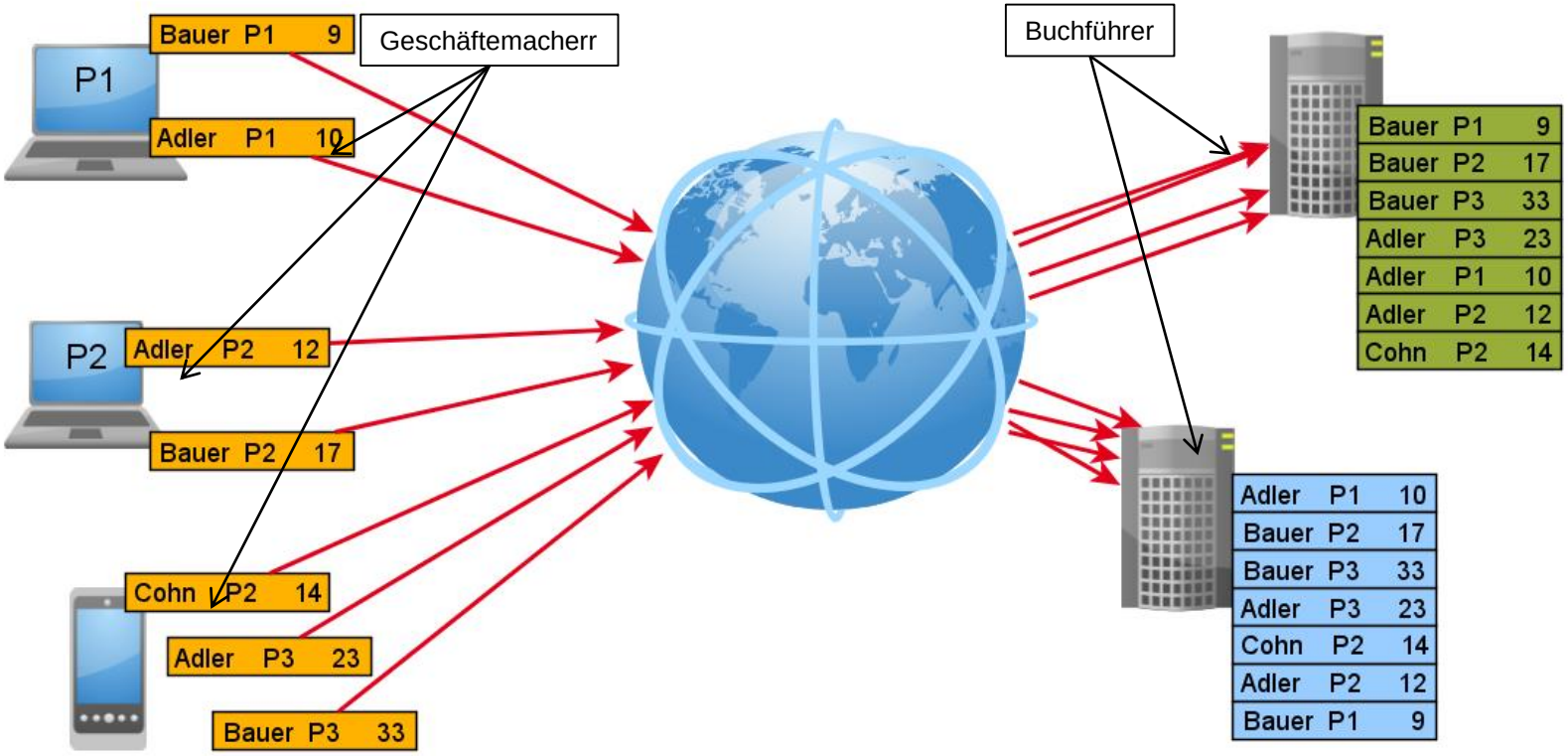
- Setzt voraus, dass die meisten Knoten konstruktiv (korrekt/gutartig) arbeiten
- Basiert wesentlich auf (echter) Zufälligkeit, keine Start- oder Endpunkte
- Konsens wird erst über mehrere Zyklen erreicht, ist aber nicht sicher, Unsicherheit vermindert sich exponentiell mit der Zeit
- Knoten akzeptieren eine Seite dadurch, dass sie die entsprechende Blockchain erweitern

Eine idealisierte Lösung

- Jeder Buchführer überprüft jede erhaltene Seite auf Korrektheit
  - Umfang und Möglichkeit abhängig von der konkreten Anwendung
- Nur als korrekt akzeptierte Seiten werden in die lokale Kette eingefügt
  - Korrumpierte Seiten werden ignoriert
- Ein Buchführer stellt neue Seite aus den empfangenen Geschäften zusammen mit Verweis auf die letzte Seite seiner lokalen Kette (= nächstes Glied) und sendet diese an alle Teilnehmer
- Idealisierung: Auswahl des *publizierenden* Buchführers erfolgt zufällig
  - Erschwert/verhindert Verfälschungen (solange Mehrheit korrekt arbeitet)
  - aber: Praktisch nicht realisierbar (ohne zentrale Steuerung und bei wechselnden Teilnehmern)
- Falls es bösartige Knoten geben kann, ist erst nach mehreren Schritten klar, welches „Ende“ die *Konsenskette* ist.

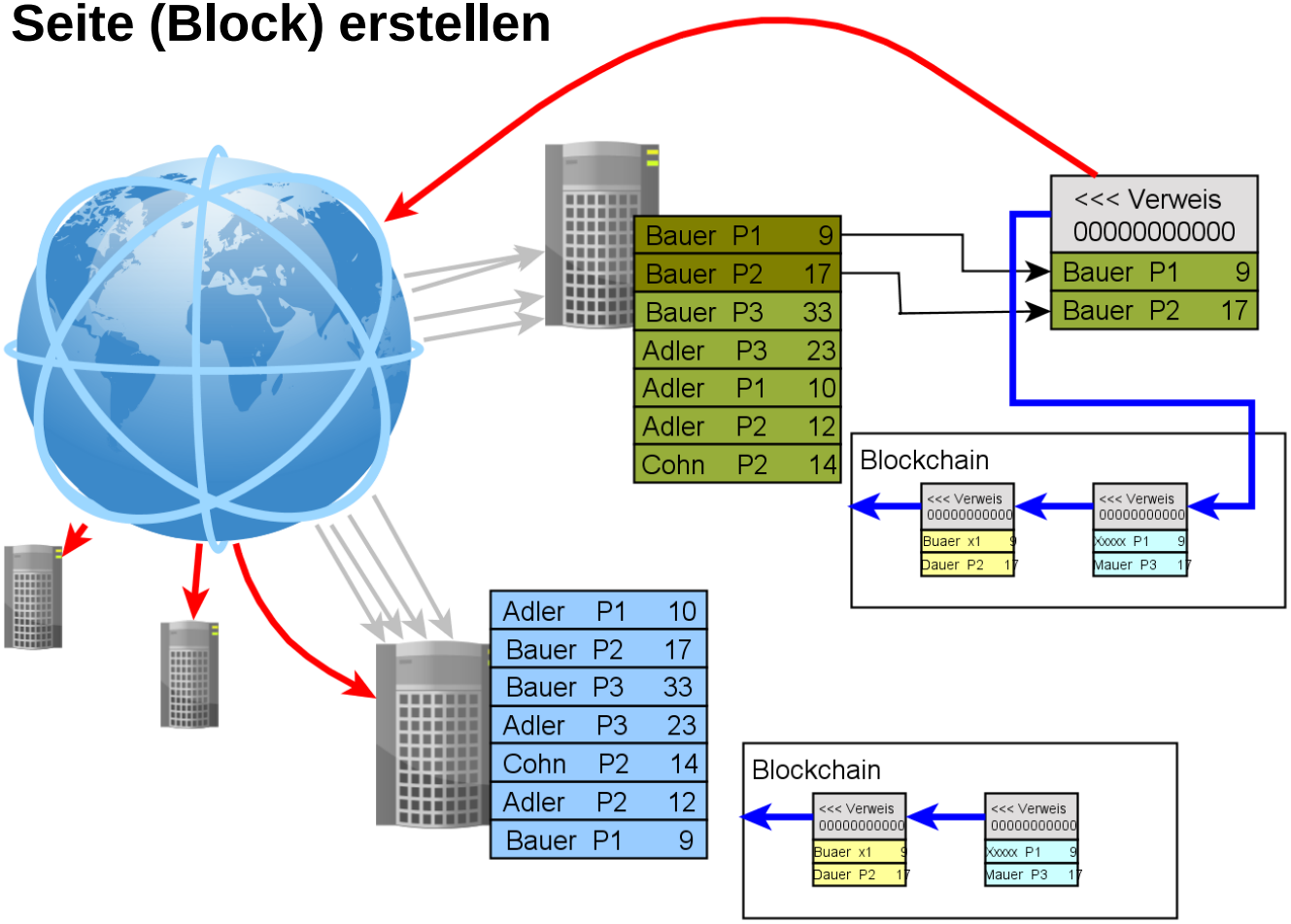
Beispiel – Schritt 1

Publikation der Geschäfte



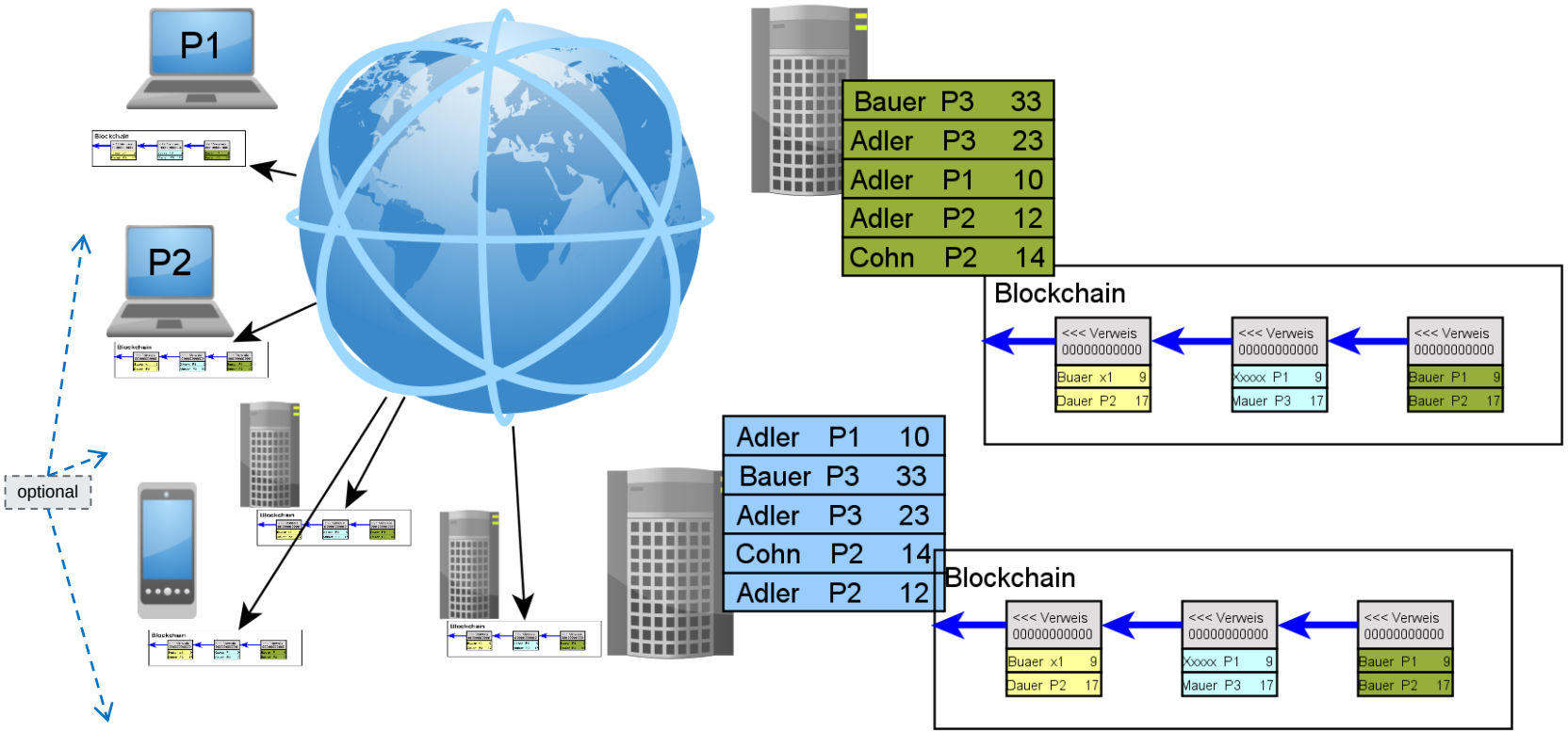
Beispiel – Schritt 2

Neue Seite (Block) erstellen



Beispiel – Schritt 3

Neue Seite in Kette (Blockchain) übernehmen



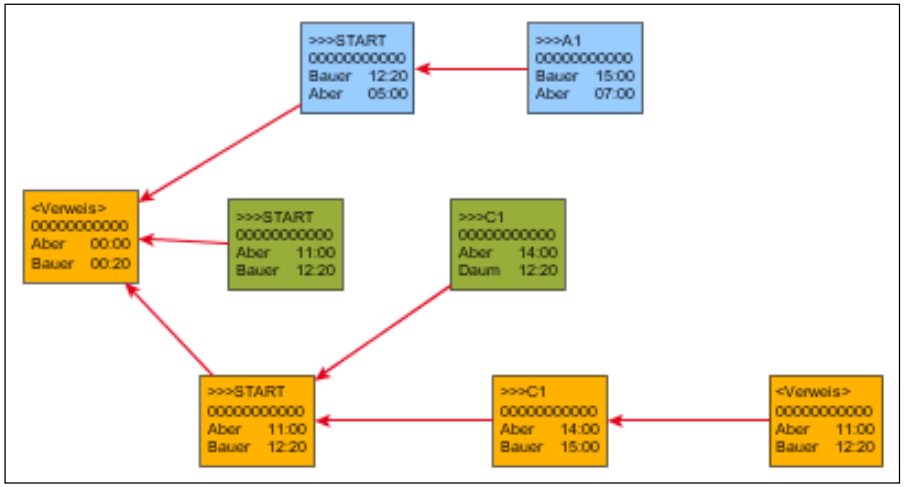
Grundlegende Eigenschaften

Idealisierte Lösung

- Buchführung (=Seitenerstellung) ist „getaktet“
  - Taktfrequenz und Seitengröße nicht unbeschränkt erhöhbar
- Mit Teilnehmerzahl wachsender Kommunikationsaufwand
  - Alle Geschäfte an alle Teilnehmer
  - Alle Seiten (Blöcke) an aller Buchhalter und (alle/viele) Geschäftemacher
  - Durch Peer-to-peer-Struktur redundante Lieferungen nicht vermeidbar
  - Jeder Teilnehmer benötigt mehrere Verbindungen zu anderen (möglichst zufällig ausgewählten) Teilnehmern, um Korrumpierung zu verhindern
- Mit der Zeit wachsende Größe der Blockchain
  - Blockchain kann nicht dezentral konsolidiert werden
  - Stetig wachsender Umfang (Verwaltung und Kommunikation)
- Überprüfbarkeit der Geschäfte abhängig vom Anwendungsfall
  - Bei Abhängigkeiten von „Altgeschäften“ (Normalfall?) wachsender Aufwand durch wachsende Blockchain

Pragmatische Lösung (Bitcoins-Verfahren)

- Mehrere (aber nicht alle), zufällig ausgewählte Buchführer publizieren ihre Seiten
  - Nicht nur einer, wie in der idealisierten Lösung → fehlertolerant, dezentralisierbar
  - Ergebnis: Kette mit Seitenketten



- Gutartige Knoten (Buchführer) hängen ihren Block immer an die längste Kette an
  - Es entstehen „verwaiste“ (orphan) Seitenketten
- Es gibt keine 100-prozentige Sicherheit, dass ein bestimmtes Geschäft in der Konsenskette endet
  - Wenn *k* Anzahl von Konsensrunden, dann steigt Zuverlässigkeit mit $O(e^k)$

Auswahlverfahren (d. h. Ersatz für Zufall)

Proof of Work

Hürde, bei der eine aufwendig zu lösende, aber leicht prüfbare Aufgabe als Zugangsberechtigung zu lösen ist (z. B. Primzahlzerlegung)

- Auswahl basiert auf einer nicht monopolisierbaren Ressource: Rechenleistung
  - Gelöst werden muss ein Hash-Puzzle:
    $$H(nonce \parallel block) < target$$
    wobei *nonce* ein zu findender (32-Bit-)Wert u. *target* eine vorgegebene Grenze sind (vgl. Rätselfreundlichkeit der Hashfunktion)
  - Kann nur durch Ausprobieren gelöst werden, daher ist die Wahrscheinlichkeit eine Lösung zu finden proportional zur eingesetzten Rechenleistung
  - Aufwand/Kosten durch *target* parametrisierbar
  - Leicht nachprüfbar
- Buchhalter bricht eigene Bemühungen ab, wenn er eine akzeptable (=korrekte) Seite empfangen hat

Proof of Work

Veranschaulichung (sehr stark vereinfacht)

```
private static String findNonce(String pointer, String block, int target) {
    long i= 100000000L;
    String s= "";
    int hc= 0;
    do {
        i++;
        s= pointer+i+block;
        hc= s.hashCode();
    } while (hc<0 || hc>target);
    return s;
}
```

Beispiel target= 1000, 100, 10

Hash	Block	Zeit
224	<<<Verweis,102582129,Bauer,P1,9;Bauer,p2,17	961 ms
41	<<<Verweis,156113257,Bauer,P1,9;Bauer,p2,17	22060 ms
5	<<<Verweis,577287498,Bauer,P1,9;Bauer,p2,17	192437 ms
57	<<<Verweis,103040429,Bauer,P1,9;Bauer,P2,17	1096 ms
57	<<<Verweis,103040429,Bauer,P1,9;Bauer,P2,17	1027 ms
5	<<<Verweis,277468715,Bauer,P1,9;Bauer,P2,17	68532 ms

Eigenschaften

- Simulation des Zufalls („Würfeln“) ist aufwendig (u. a. Energieverbrauch)
  - Aufwandsentschädigung für Buchführer erforderlich
    - Muss so gestaltet sein, dass echter Wettbewerb gefördert, aber Monopolbildung verhindert wird (Grundproblem der Wirtschaft)
    - Bitcoin: Jede angenommene Seite wird vergütet, daher: Mining
  - Evtl. der Punkt für den am ehesten eine alternative Lösung möglich erscheint (??)
- Mehrere Kandidaten für „nächste Seite“
  - Größerer Kommunikationsaufwand
  - Mehrere Versionen der Blockchain („Enden“) müssen parallel vorgehalten werden

Grenzen und Probleme

- Technische Begrenzungen
  - Skalierbarkeit begrenzt
    - *Bitcoin: Max. 7 Transaktionen/sec. (4000 T/block, 1 block/10 min) – inzwischen 3 T/s*
  - Keine unmittelbare Bestätigung
    - Akzeptanz erst nach mehreren „Takten“ ausreichend sicher
- Wirtschaftliche Faktoren
  - Hoher Energiebedarf beim Proof-of-Work
  - Stetig wachsende Blockchain
    - Wachsender Speicher- und Prüfaufwand
    - Aufwand für „Neueinsteiger“
- Weitere
  - Gefahr der Monopolisierung der Buchführung
  - Dezentrale Struktur und Vielzahl der Beteiligten erschweren Weiterentwicklung

Kapazitätsgrenze erreicht: Bitcoin-Transaktionen in der Warteschlange

Technology Review 15.03.2016 08:25 Uhr – Sascha Mattke

Bitcoin-Mining-Rack. (Bild: Marco Krohn / Wikipedia / cc-by-sa-4.0)

Das Digitalwährungssystem Bitcoin ist nicht für die riesigen Volumina ausgelegt, die es inzwischen erreicht. Jetzt zeigt sich dieses bislang theoretische Problem auch in der Praxis.

Technology Review
DAS MAGAZIN FÜR INNOVATION

KONGRESSE WETTBEWERBE FORUM AR(

ENERGIE INFOTECH LEBEN PRODU

Technology Review > Infotech > Bitcoin an der Grenze

Bitcoin an der Grenze

15.03.2016 – **Tom Simonite**

Am 3. März standen rund 30.000 Bitcoin-Transaktionen in der Warteschlange. Einige davon werden viel früher

Untersuchung des Bitcoin-Designs kommt zu dem Schluss, dass das System eine radikale Überarbeitung braucht. Denn bislang liege noch kein Vorschlag vor, der zuverlässig dafür sorgen würde, dass Bitcoin auch im sehr großen Maßstab funktioniert.

http://www.heise.de/newsticker/meldung/Kapazitaetsgrenze-erreicht-Bitcoin-Transaktionen-in-der-Warteschlange-3132893.html
https://www.heise.de/tr/artikel/Bitcoin-an-der-Grenze-3132891.html

„Blockchain's promise and peril"

(Bewertung durch Gartner)

Smarter With Gartner

The CIO's Guide to Blockchain

Blockchain is only the first step in a future of distributed ledger platforms that enable the programmable economy.

June 29, 2016
Contributor: Heather Pemberton Levy

Scalability: In the blockchain, the system requires significant computational power (hence, electricity) to verify and confirm each block of transactions. Due to the design of this process, a maximum of seven transactions per second can take place and each block of transactions requires a minimum delay of 10 minutes to confirm.

Lack of resistance to centralization: As the need for computational power to verify transactions has increased, proof-of-work activity has been mostly consolidated into four primary mining organizations, all based in China. This alters the conception of blockchain as a decentralized system.

Confidentiality/transparency: All transactions are public, which has its pros and cons in terms of access to transactional information but not necessarily identification of participants to the network.

Quelle: **http://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain**

Anwendungskriterien

- Unter den folgenden Voraussetzungen kann die Blockchain eine angemessenen Lösung sein:
  - Eine Menge von Datensätzen ist zu verwalten.
  - Es gibt mehrere/viele Produzenten solcher Datensätze.
  - Die Produzenten vertrauen sich gegenseitig nicht vollständig.
    - Es ist jedoch sicher, dass der größere Teil von ihnen vertrauenswürdig ist.
  - Es gibt keinen vertrauenswürdigen Dritten.
    - D. h. u. a. auch keine vertrauenswürdige zentrale Instanz.
  - Zwischen den Datensätzen bestehen Beziehungen
- Sobald eine dieser Vorbedingungen verletzt ist, existieren i. d. R. effizientere Verfahren.

Beurteilungskriterien

1. Handelt es sich überhaupt um eine Blockchain mit dezentraler Verwaltung?
2. Wie wird der verteilte Konsens erreicht und wie wird mit der dabei unvermeidlichen zeitlichen Verzögerung umgegangen?
3. Welche Auswirkungen hat die durch die Blockgröße beschränkte Skalierbarkeit?

Blockchain
Kurz zusammengefasst

- Völlig dezentrale Struktur
  - Keine zentrale Administration notwendig (und möglich)
  - Höherer Kommunikationsaufwand
  - Mindestteilnehmerzahl erforderlich
  - Schwierig zu verwalten (Updates usw.)
- Datenstruktur (fast) nicht korrumpierbar
- Durch Blockbildung getaktete Arbeitsweise
  - Beschränkt Kapazität/Skalierbarkeit
- Verzögerte Akzeptanz von Geschäften durch Aufnahme in Konsenskette
- Simulation der zufälligen Auswahl (Mining) kostspielig
- Start/Anfahren schwierig – Herunterfahren noch weitgehend unbeachtet

Fazit

Die Blockchain ist eine interessante Technologie, deren praktische Anwendbarkeit durch das Bitcoins-Projekt bewiesen ist.

Vor einer breiten Anwendung müssen jedoch noch entscheidende Probleme gelöst werden. Derzeit kann nicht gesagt werden, ob die gesuchten Lösungen überhaupt existieren, bzw. bis wann sie gefunden werden könnten.

Es wird sich zeigen, ob einzelne Features im Rahmen spezieller Aufgaben sinnvoll integriert werden können.

Die zeitliche Verzögerung und die begrenzte Kapazität sind die wesentlichen und gleichzeitig schwer überwindbaren Hürden, die der breiteren Anwendung im Wege stehen.

Vielen Dank.

Dr. Jürgen Lampe
S&N Invent GmbH
Frankfurter Str. 71-75
65760 Eschborn

Telefon: +49 (6196) 802690
E-Mail: juergen.lampe@sn-invent.de

Quellen: Bitcoins

- Bitcoin and Cryptocurrency Technologies
  - *Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder*
    - https://www.coursera.org/course/bitcointech/princeton-bitcoin_book.pdf
- The resolution of the Bitcoin experiment
  - Mike Hearn
    - https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.1122eoukj
- Weitere
  - Aktueller Blick auf das Bitcoins-Netzwerk (Kurse, Statistiken usw.)
    - https://blockchain.info/de/
  - Bitcoin Wiki
    - https://en.bitcoin.it/wiki/Main_Page
  - Technical Roadblock Might Shatter Bitcoin Dreams
    - https://www.technologyreview.com/s/600781/technical-roadblock-might-shatter-bitcoin-dreams/

Quellen: Blockchain

- http://www.blockchainstudies.org/
- http://btl.co/
- Http://www.gruenderszene.de/allgemein/blockchain-wie-geht-das
- http://www.blockchaintechnologies.com/blockchain-companies

- Hinter dem Blockchain-Hype
  - http://www.heise.de/tr/artikel/Hinter-dem-Blockchain-Hype-3086113.html

Frankfurter Allgemeine

Revolution der Finanzmärkte

Bundesbank und Börse erforschen neues Handelssystem

Gemeinsam haben sie ein Programm entwickelt, über das mit der Blockchain-Technologie gehandelt werden kann. Der Weg in die Praxis ist aber noch weit.

29.11.2016, von TIM KANNING

Es gibt jeweils eine Art Aufsichtsstelle, die die Ausgabe des Geldes und die Ausgabe der Anleihen überwachen und kontrollieren. Am Ende eines jeden Handelstages sammeln sie alles wieder ein und rechnen die Blockchain-Einheiten in echtes Geld um. Damit unterscheidet sich der Prototyp in entscheidendem Maße etwa von der Digitalwährung Bitcoin. Denn eine der

zu ersetzen. Vor allem dauerten die einzelnen Transaktionen noch viel zu lange im Vergleich zu den heutigen

Thiele und Kengeter. Er gehe davon aus, dass es noch Jahre dauere, bis die Blockchain in großem Umfang in der Praxis eingesetzt werden könne, sagte Kengeter. „Ob das eine ein- oder eine zweistellige Zahl von Jahren wird, muss sich noch zeigen." Sein Konzern erforsche derzeit an fünfzehn verschiedenen Stellen, wie die Blockchain verwendet werden könne.

http://www.faz.net/aktuell/finanzen/aktien/bundesbank-und-boerse-erforschen-neues-handelssystem-14549755.html