HBA CONSULTING AG

Bitcoin und Blockchain – bestehen Auswirkungen auf Aktuare?

qx-Club am 31. Mai 2017 in Zürich

Mathias Ott, HBA-Consulting AG

HBA-Consulting AG

HBA Consulting AG

- Gründung 2004 als aktuarielles Beratungshaus
- Neutraler und unabhängiger Berater in privater Hand (Management)
- ca. 50 hochqualifizierte Spezialisten
- namhafte Kunden und Referenzen

Kernkompetenzen

- Strategieevaluierung
- Prozess- und Organisationsberatung
- Produkte und aktuarielle Beratung
- IT-Beratung und Umsetzung
- hochspezialisierte Lösungen

Marktfokus

- Versicherungen und Altersvorsorgeeinrichtungen
- Banken, Bausparkassen und Spezialkreditinstitute

Ziele / Vision

- Führendes unabhängiges Beratungs-haus und verlässlicher Partner
- Zusatznutzen beim Kunden durch ausgeprägte Fachkenntnis sowie eigene Lösungen / Assets
- Herausragender Arbeitgeber mit kreativen, ergebnisorientierten und eigenverantwortlichen Mitarbeitern
- **Projekte zum Erfolg bringen**

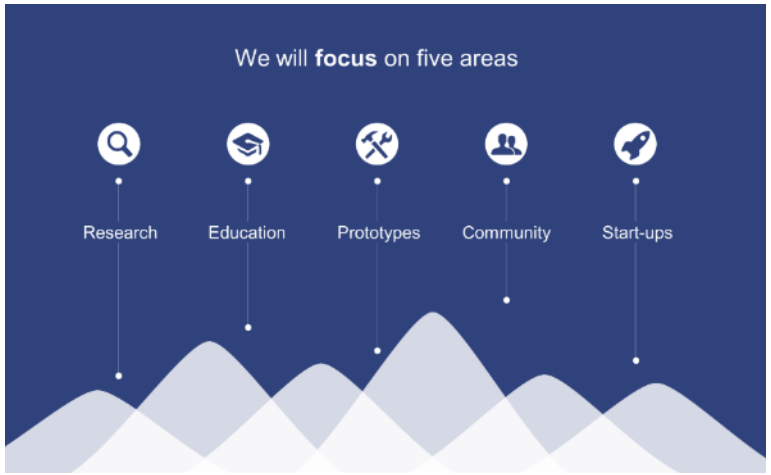
Partnerschaften und Zusammenarbeit

DAV
DEUTSCHE AKTUARVEREINIGUNG e.V.

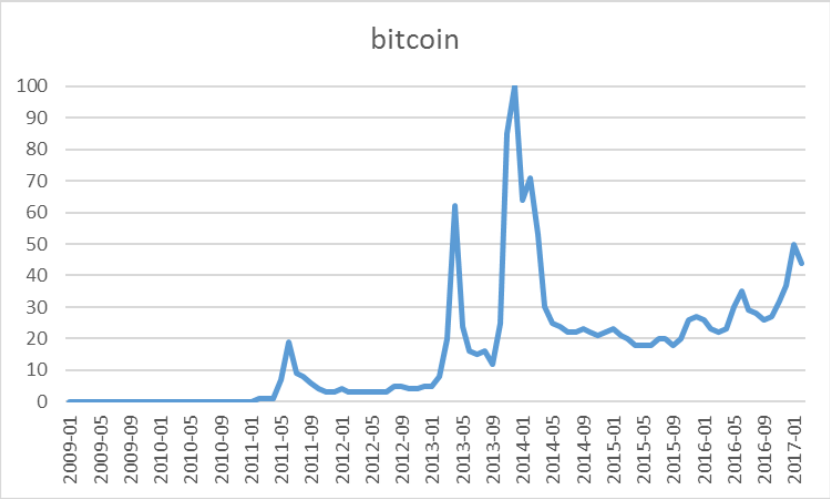
DGVFM
DEUTSCHE GESELLSCHAFT FÜR VERSICHERUNGS- UND FINANZMATHEMATIK e.V.

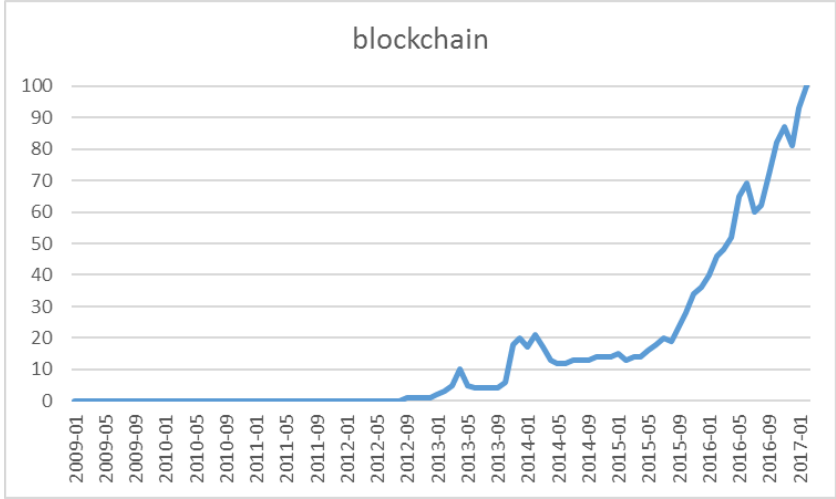
qx - Club

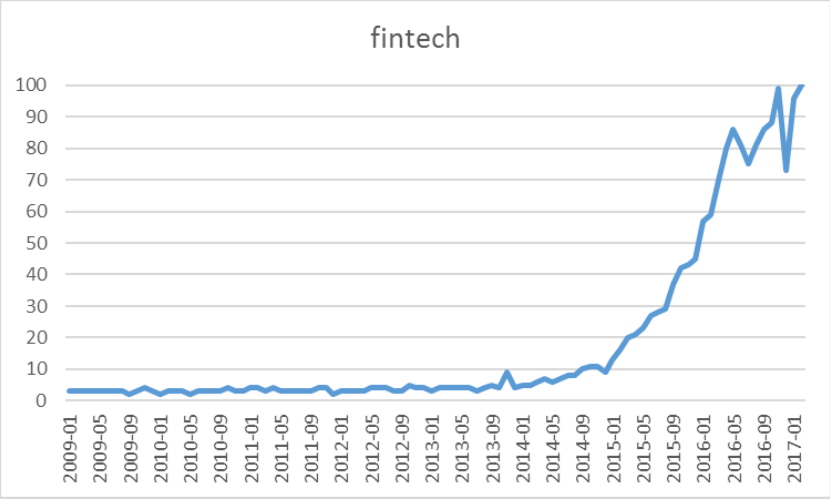
ICA CIA
BERLIN 2018

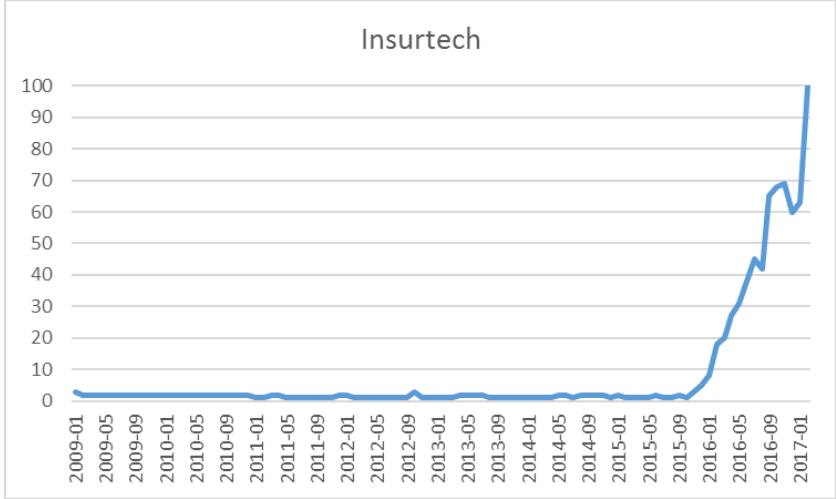


Interesse an den Begriffen …

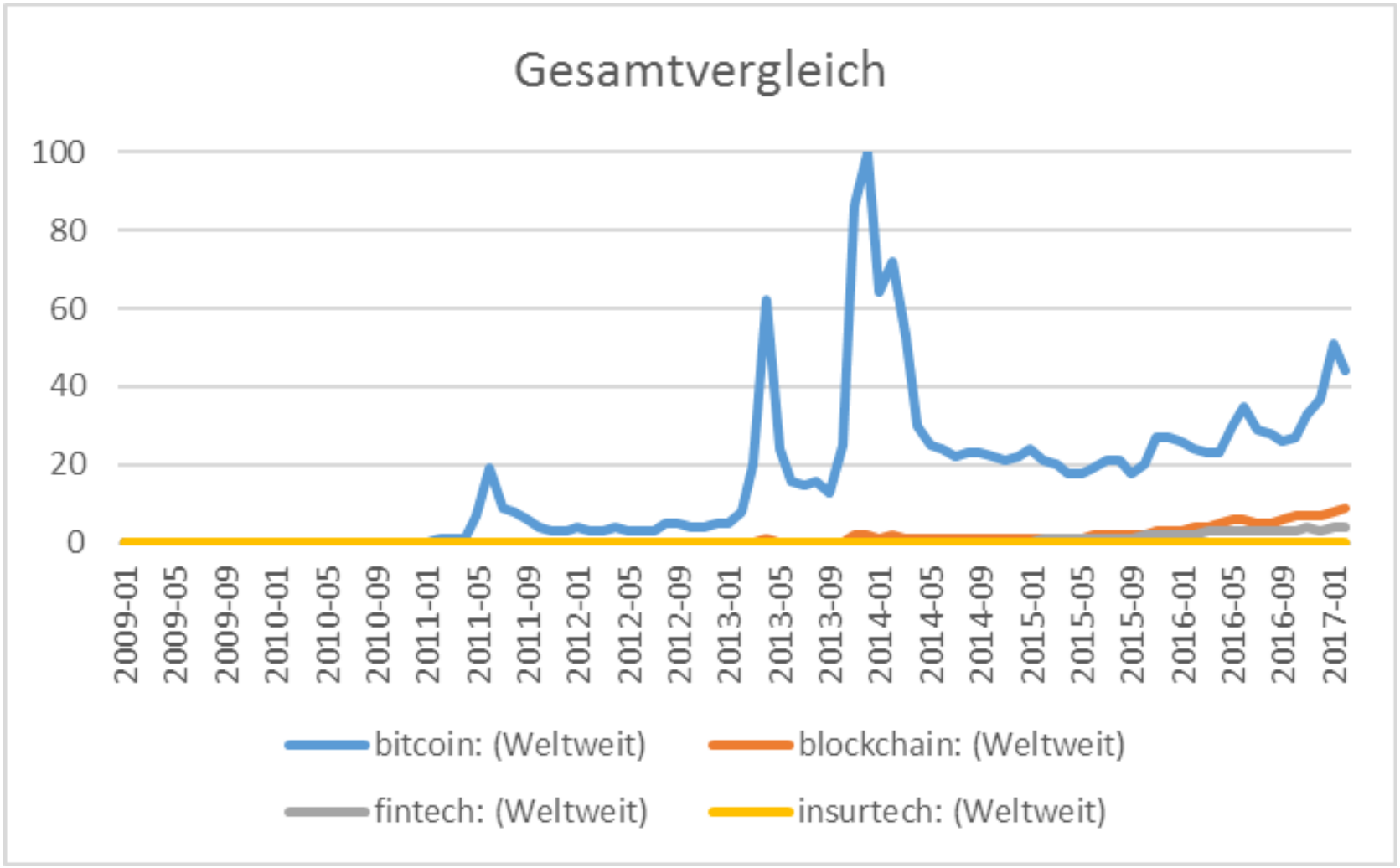








Interesse an den Begriffen …



Agenda

1 **Bitcoin – eine digitale Revolution**

Wie elektronische Währungen unsere Welt verändern können.

2 **Blockchain – die technologische Basis**

Welche Technologie im Maschinenraum von Bitcoin arbeitet.

3 **Blockchain – Beispiele für die digitale Revolution**

Wie künftige Versicherungsmodelle aussehen könnten.

Was ist eigentlich Geld?

Geldfunktion (Quelle: https://de.wikipedia.org/wiki/Geld)

In der Volkswirtschaftslehre wird Geld funktional definiert

- Geld hat **Zahlungsmittelfunktion**. Unter einem Tausch- oder Zahlungsmittel versteht man ein Objekt oder auch ein erwerbbares Recht, das ein Käufer einem Verkäufer übergibt, um Waren oder Dienstleistungen zu erwerben. Geld vereinfacht den Tausch von Gütern und die Aufnahme und Tilgung von Schulden.
- Geld ist ein **Wertbewahrungsmittel**.
- Geld ist ein **Wertmaßstab** und eine **Recheneinheit**. Der Wert einer Geldeinheit wird als Kaufkraft bezeichnet.

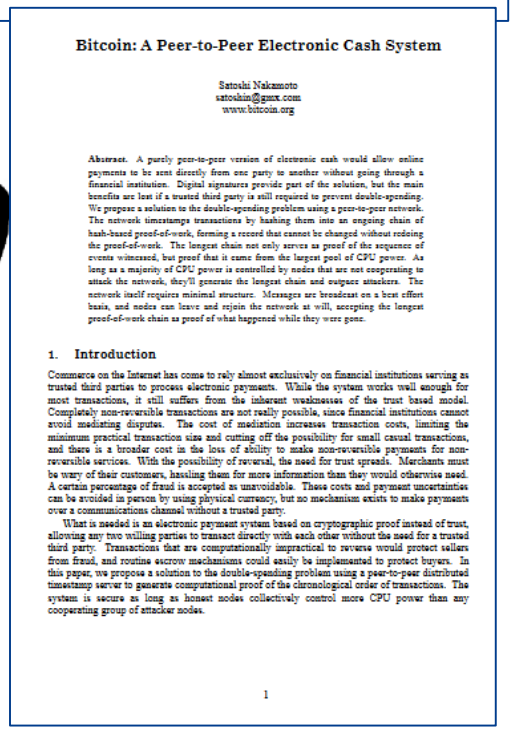
Je besser ein Gut die Geldfunktionen erfüllt, umso eher wird es als Geld angesehen.

Bitcoin – eine digitale Revolution (www.bitcoin.org)

Veröffentlichung
31. Oktober 2008,
9 Seiten

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

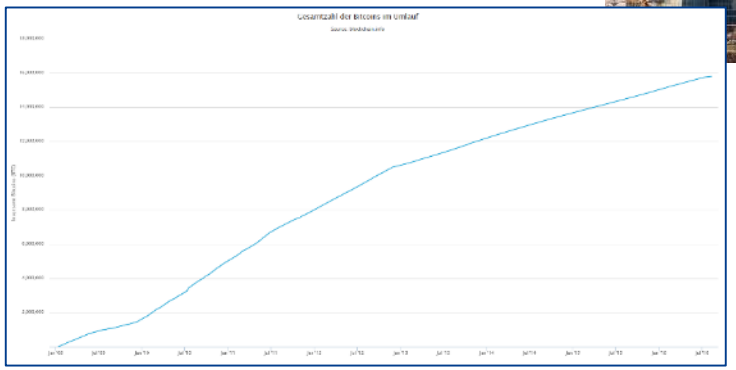
What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

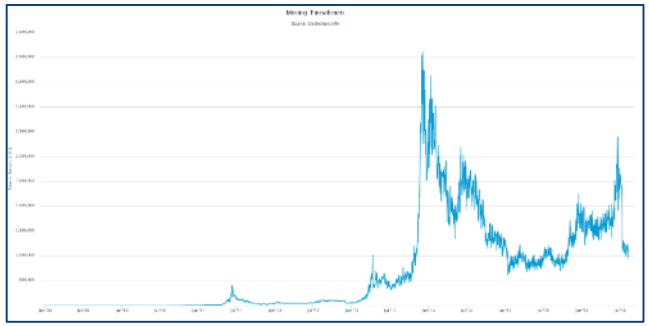
- Satoshi Nakamoto
- Kritik am aktuellen elektronischen Bezahlsystem
- Vorstellung eines elektronischen Zahlsystems basierend auf
  - Kryptografie
  - unumkehrbare Transaktionen
  - kein zentraler Verwalter – peer-to-peer system
- **„We define an electronic coin as a chain of digital signatures.“**

Bitcoin – Eigenschaften (ausgewählt)

- Philosophie
  - Garantien ohne Garantiegeber (Legitimation des Geldes)
    „Es ist vollständig dezentralisiert, ohne Server oder zentrale Autorität“
  - öffentlicher, aber anonymer/pseudonymer Zahlungsverkehr
    (Bitcoin-Adressen statt Konten)
- Geldmenge
  - maximal 21 Millionen Einheiten
  - festgelegt durch das Netzwerkprotokoll

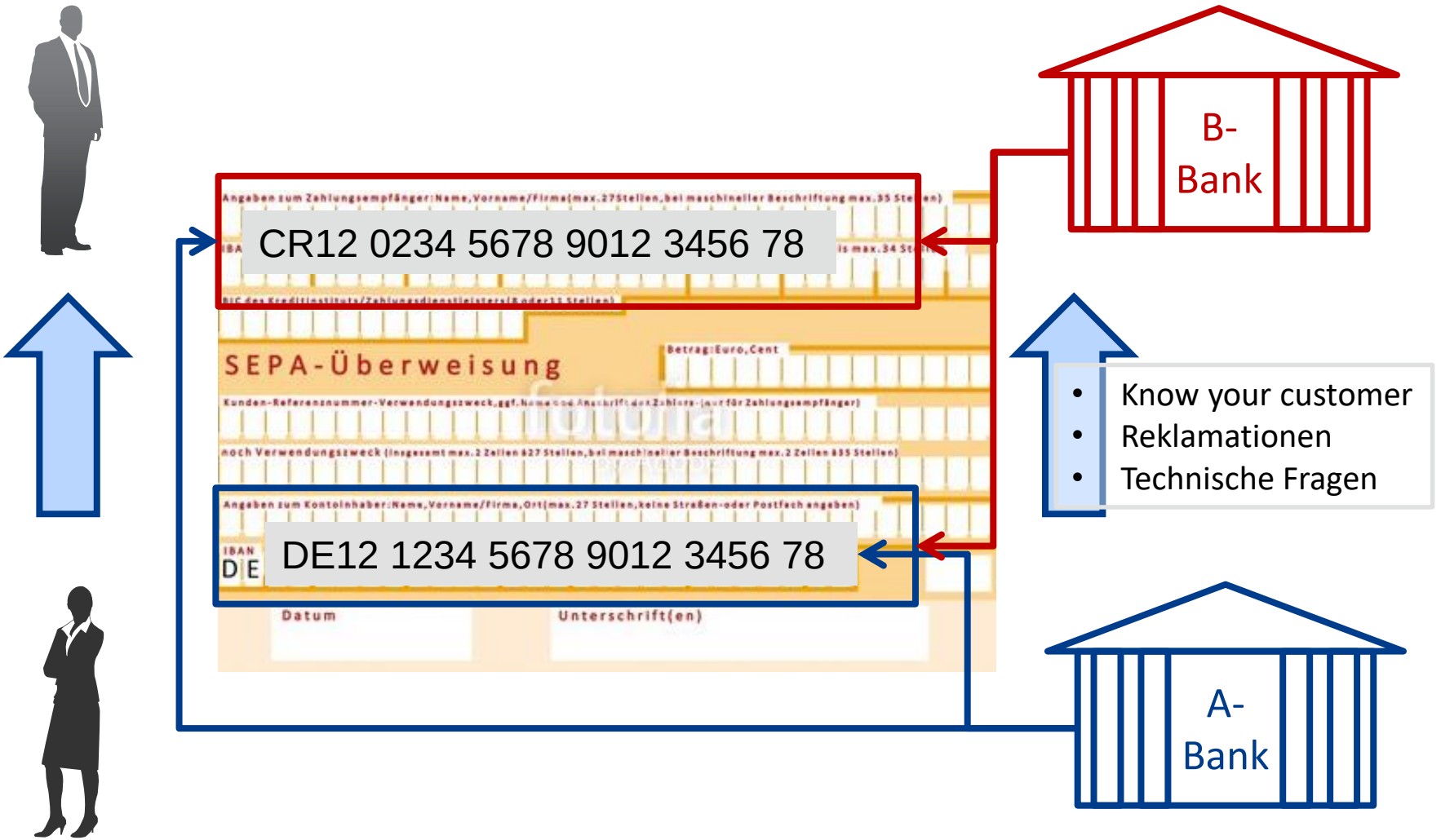


- Geldschöpfung und Seignorage
  - Mining
  - Seignorage alle 10 Minuten (angfänglich 50 Bitcoin, inzwischen 12,5 Bitcoin)
  - Halbierung der Seignorage alle 210.000 Blöcke



Quelle: blockchain.info/de/charts/

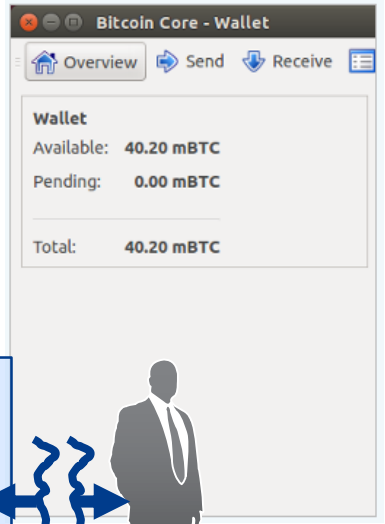
Überweisung heute – ein Vergleich

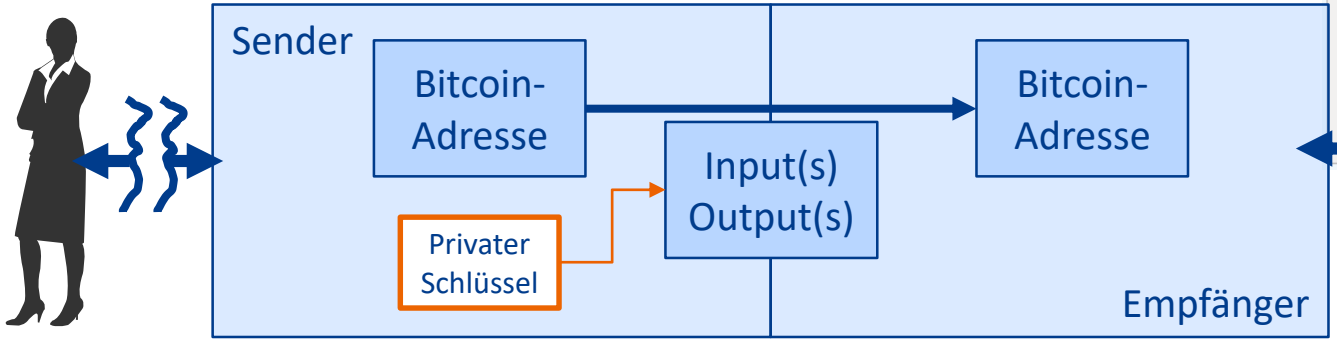


- Know your customer
- Reklamationen
- Technische Fragen

Bitcoin – Nutzung im täglichen Leben

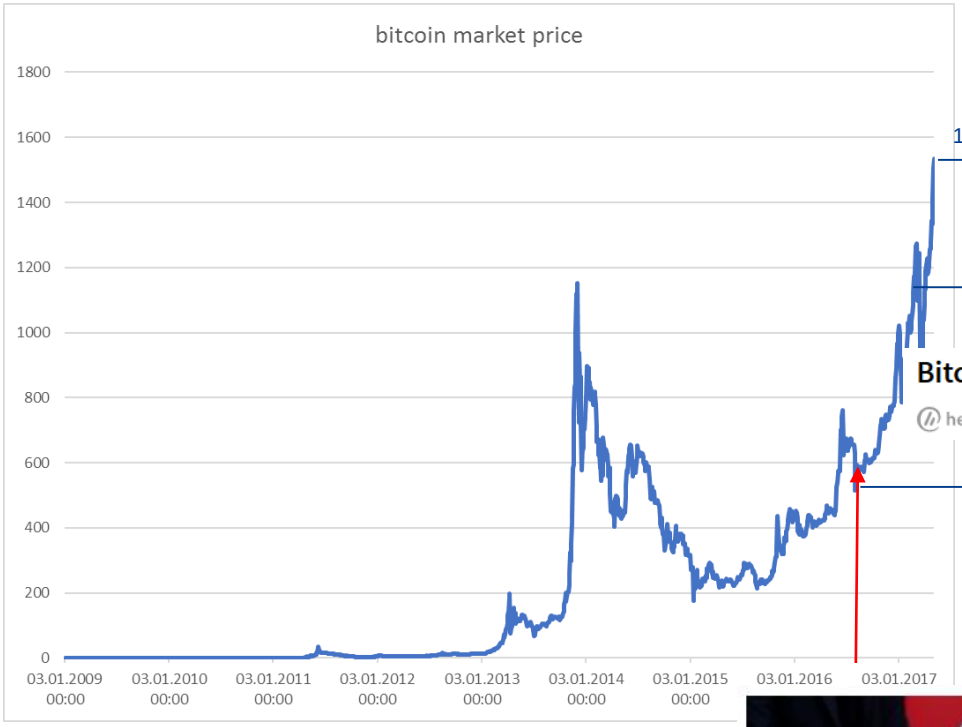
- Nutzung
  - Bitcoin-Clients für jede Plattform – mobile phone, Windows, Mac, …, Online-Wallets (Hot Storage)
  - Spezialität: Papier-Wallets (Cold Storage)
  - Transaktion aus Nutzersicht





- Kursschwankungen, Probleme, Integration in die old economy
  - Mt. Gox (2014: 650.000 Bitcoin ≈ knapp ½ Mrd. US$)
  - Bitfinex (2016: 120.000 Bitcoin ≈ ca. 58 Mio. €)
  - Ponzi-Schema

Ist Bitcoin nun Geld?



Quelle: blockchain.info/de/charts

10.05.2017

~ 1.500 $

~ 1.100 $

Bitcoin erreicht zeitweise neues Rekordhoch über 1200 US-Dollar

heise online 24.02.2017 15:04 Uhr vorlesen

~ 600 $

Millionendiebstahl bei Tauschbörse

Bitcoin-Anleger verlieren ein Drittel ihrer Einlagen

Bitcoin im Wert von rund 58 Millionen Euro sind Nutzern der Digital-Börse Bitfinex gestohlen worden. Der Verlust soll nun auf alle Kunden umgelegt werden. mehr...

Quelle Spiegel Online (08.08.2016 – 12:31 Uhr):
http://www.spiegel.de/netzwelt/web/bitcoin-boerse-bitfinex-kunden-verlieren-36-prozent-ihrer-einlagen-a-1106583.html

Ist Bitcoin nun Geld?

Maßnahme vom 27. April 2017
Thema > Unerlaubte Geschäfte

Onecoin Ltd (Dubai), OneLife Network Ltd (Belize) und One Network Services Ltd (Sofia/Bulgarien): Untersagung von Geschäften mit „OneCoins“ in Deutschland

...Die BaFin hat der *Onecoin* Ltd (Dubai) und der OneLife Network Ltd (Belize) heute untersagt, im Internet ein öffentlich zugängliches System anzubieten, um darüber Geschäfte mit „*OneCoins*“ durchzuführen. Darüber hinaus hat sie die Unternehmen angewiesen, jegliche Werbung für den Vertrieb und Verkauf...

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Verbrauchermitteilung/unerlaubte/2017/vm_170427_Onecoin_Ltd.html

Agenda

1 **Bitcoin – eine digitale Revolution**

Wie elektronische Währungen unsere Welt verändern können.

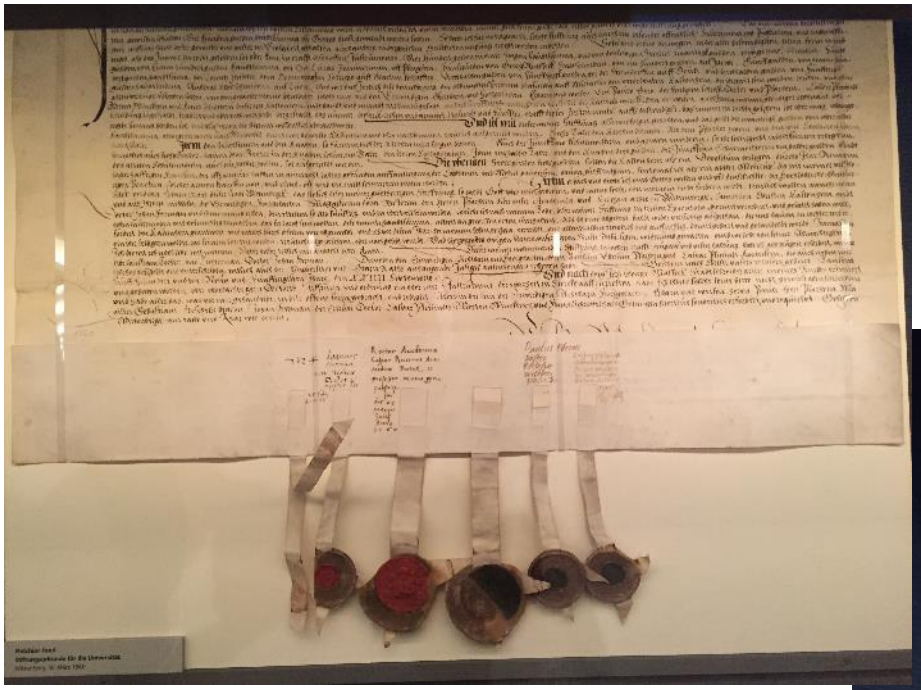
2 **Blockchain – die technologische Basis**

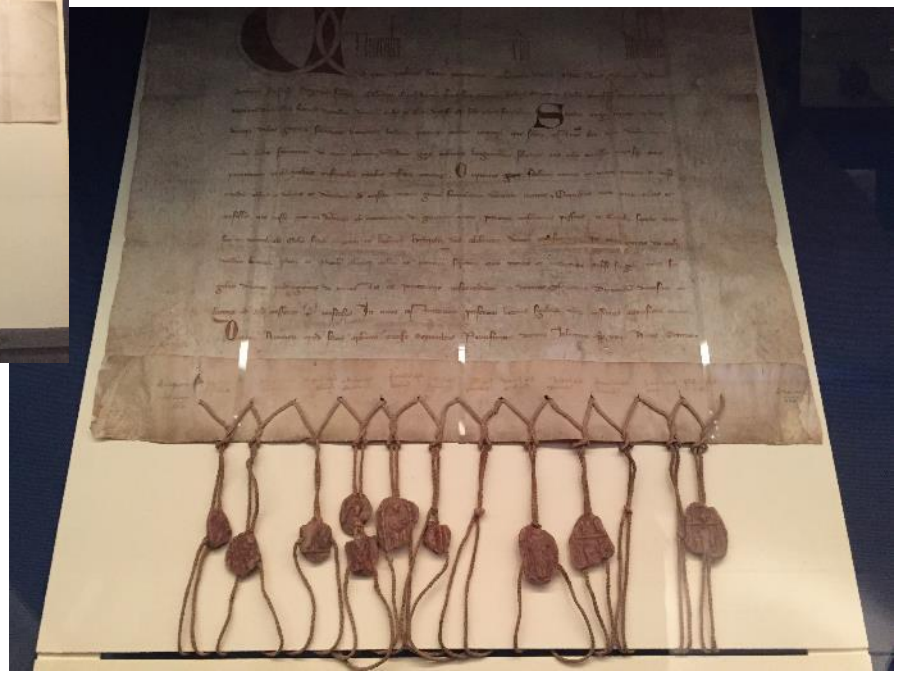
Welche Technologie im Maschinenraum von Bitcoin arbeitet.

3 **Blockchain – Beispiele für die digitale Revolution**

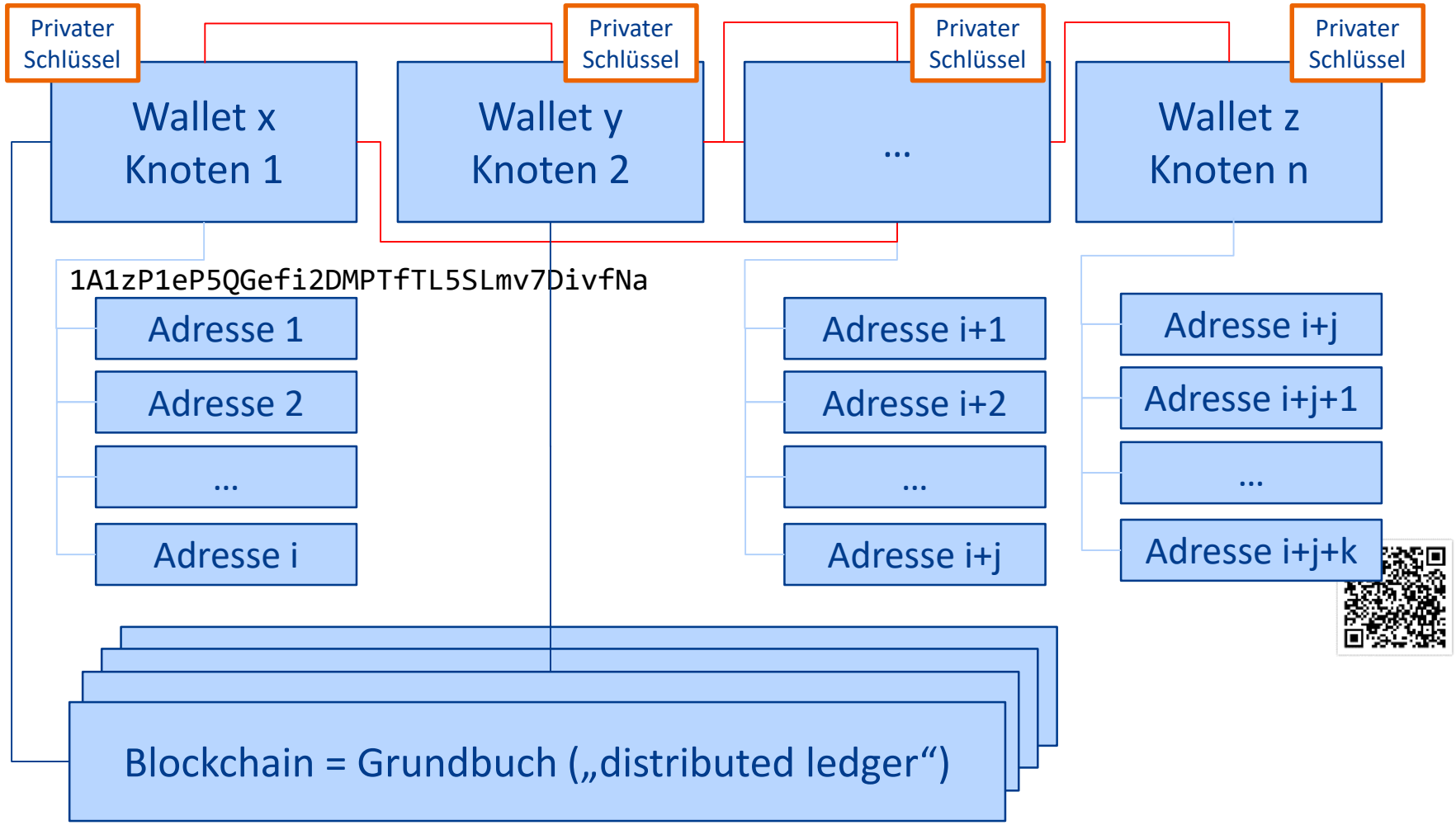
Wie künftige Versicherungsmodelle aussehen könnten.

Frühe Formen der Blockchain

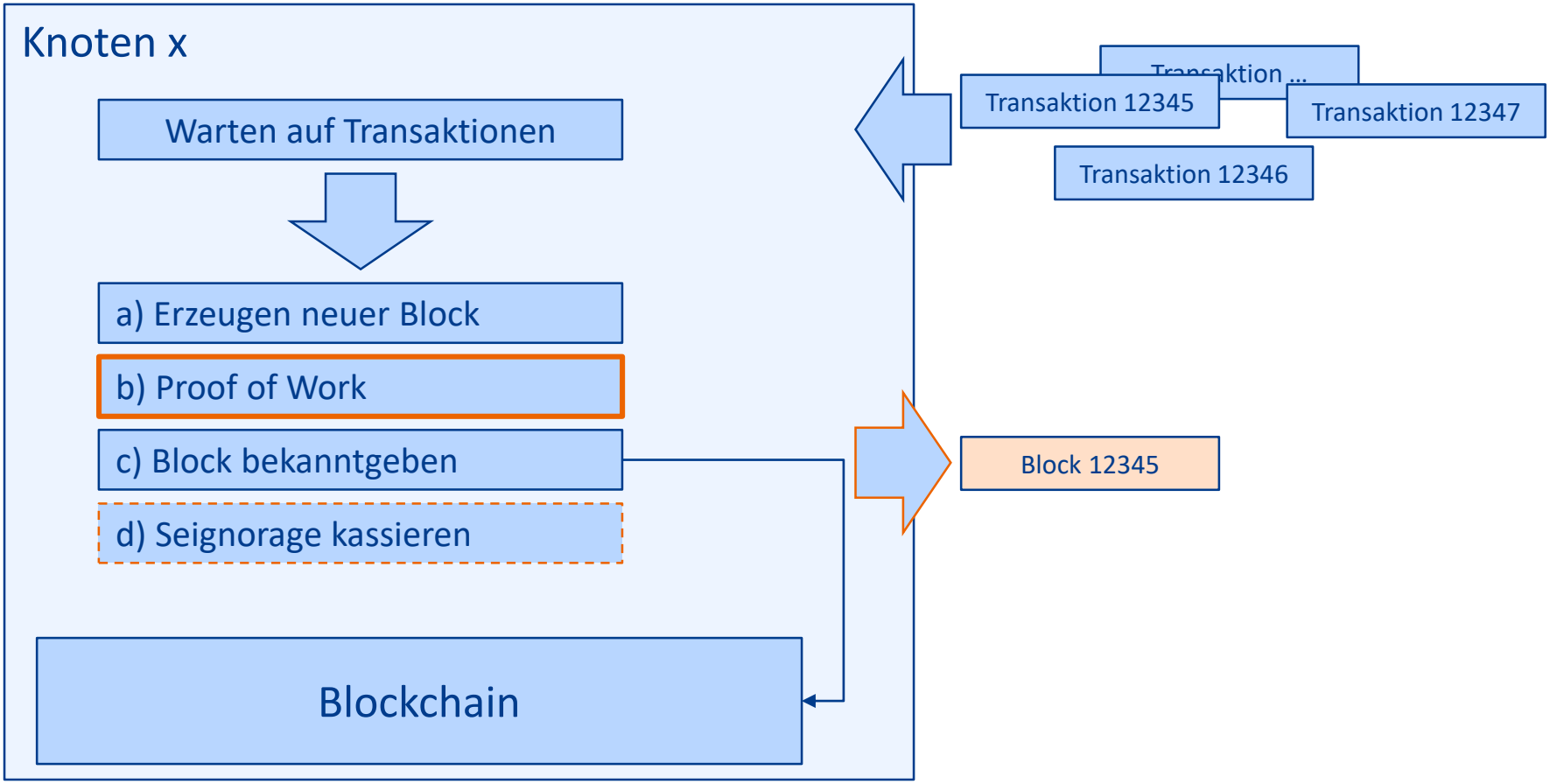




Blockchain – die technologische Basis

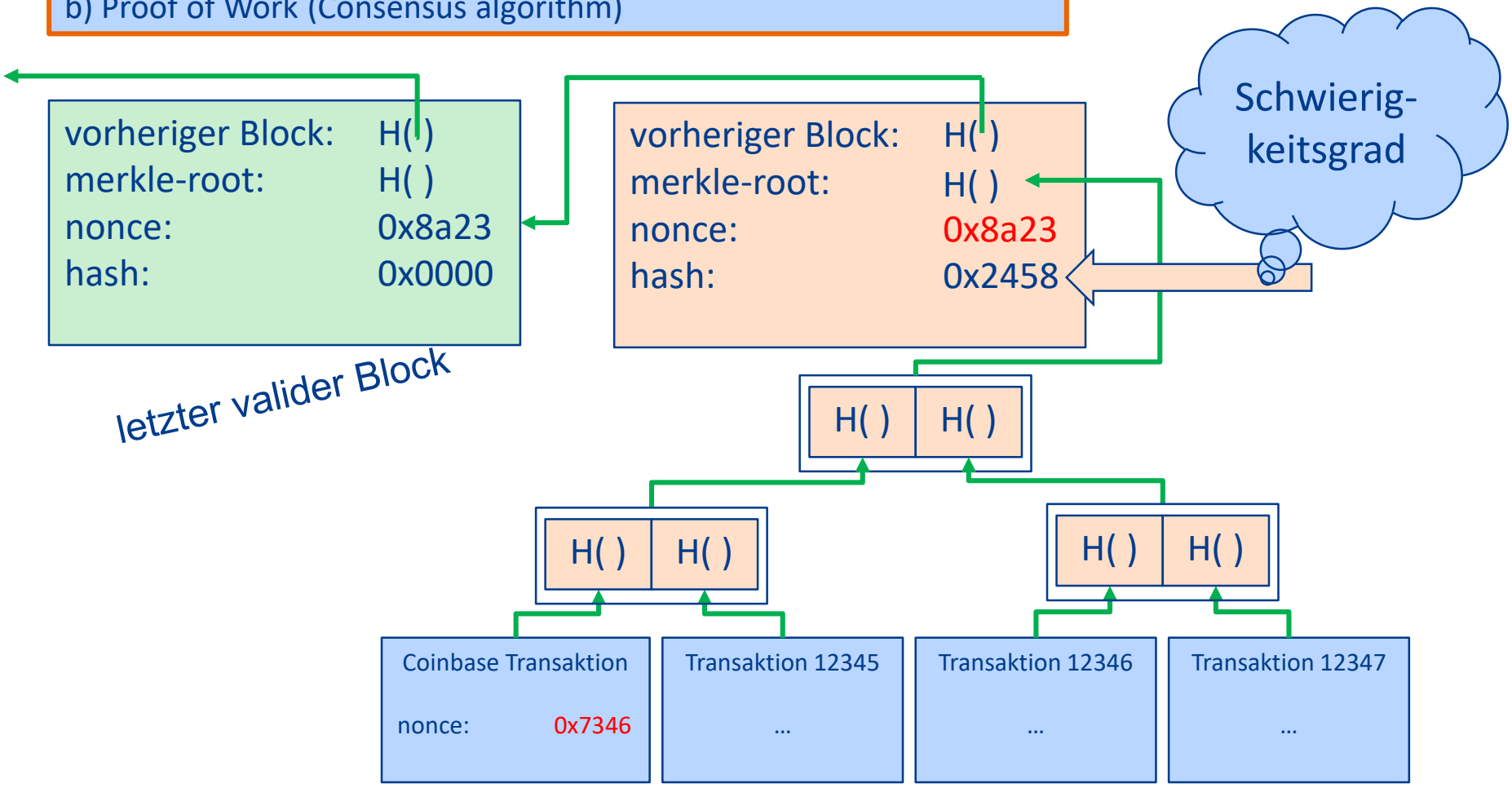


Blockchain – die tägliche Arbeit (Mining)



Blockchain – proof of work (find a valid Block)

b) Proof of Work (Consensus algorithm)



Blockchain – proof of work (find a valid Block)

Ein Block ist genau dann valide, wenn der Hash-Wert kleiner als

0000000000000000172EC0000000000000000000000000000000000000000000

(hexadezimale Darstellung, Stand März 2015) ist. Der Schwierigkeitsgrad ändert sich alle zwei Wochen.

Veränderbar sind die „nonces“

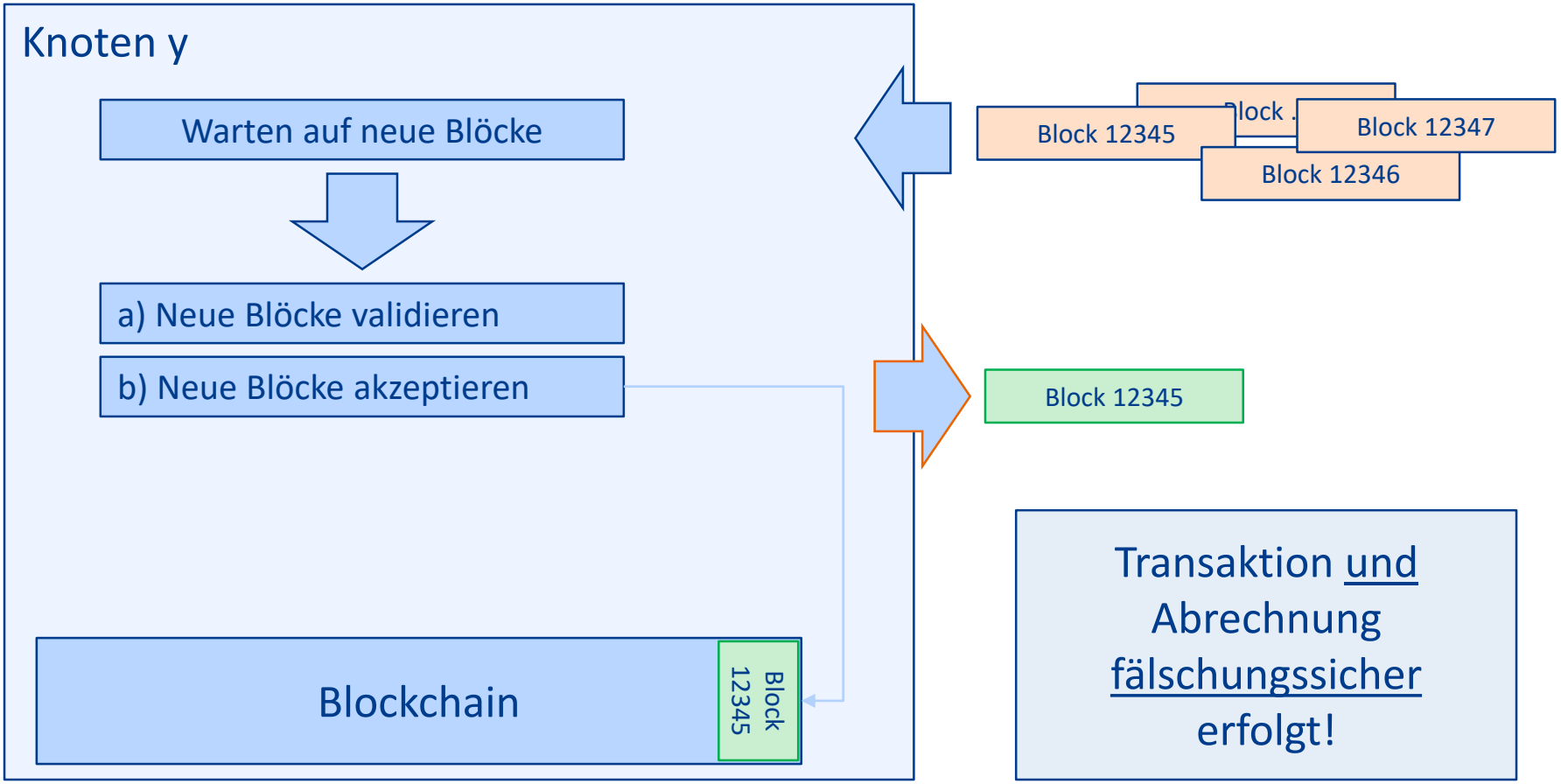
- zwei 32 Bit Zahlen
- Neuberechnung der Hashes H(…) und Prüfung, ob der Hash-Wert kleiner als der Schwierigkeitsgrad ist.
- H(…) = SHA256(…)

Sehr anspruchsvolle „**Suche**“

- spezielle Hardware (Ganzzahl-Operationen!)
- sehr hoher Energieverbrauch
  (Schätzungen 2011 – zwischen 24 und 200 Megawattstunden)

Einfache (umgekehrte) **Validierung** H(…)

Blockchain – die tägliche Arbeit (Validation)



Smart Contracts – in aller Kürze

Der Begriff „Smart Contract“ wurde etwa 1993 durch den Computer-wissenschaftler Nick Szabo geprägt.

Smart Contracts sind Computerprotokolle, die

- Verträge abbilden oder
- überprüfen oder die
- Verhandlung oder Abwicklung eines Vertrags technisch abbilden (bzw. unterstützen).

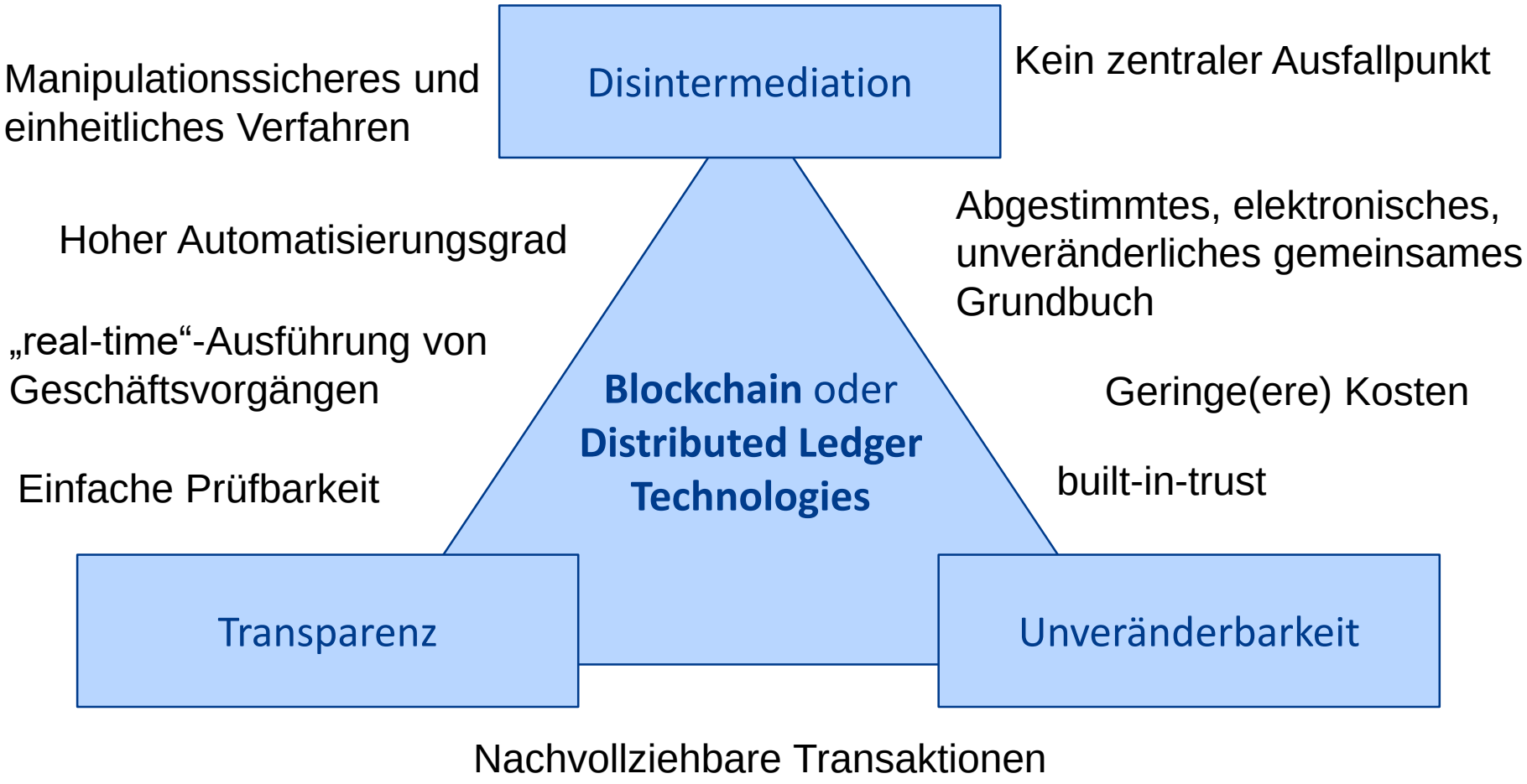
Eine Infrastruktur für Smart Contracts kann durch ein

- repliziertes Asset-Register und
- Vertragsausführung über kryptographische Hash-Ketten und
- fehlertolerante Replikation

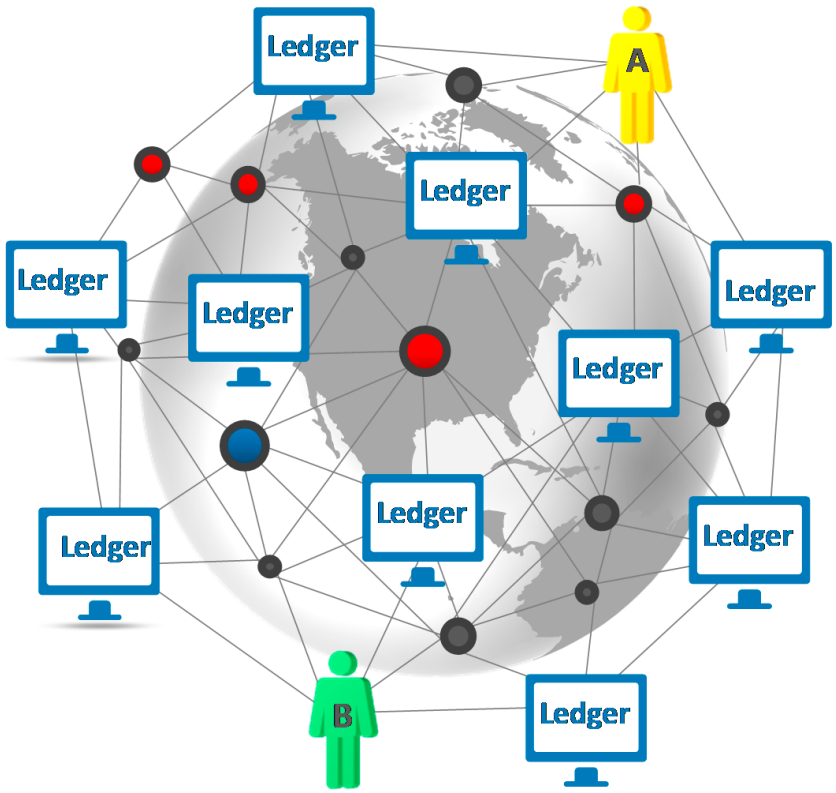
implementiert werden.

https://de.wikipedia.org/wiki/Smart_Contract

Blockchain / DLT – zentrale Eigenschaften



Blockchain – viele weitere „Geheimnisse“



Quelle: IWF, January 2016 SDN/16/03

Weitere Aspekte

- gemeinsame Entscheidungen
- Umgang mit Fehlern
- Umgang mit „bösartigen“ Knoten
- Konsistenz der Daten
- ….

Buchempfehlung zu den Grundlagen

Roger Wattenhöfer, The Science of the Blockchain

Agenda

1 **Bitcoin – eine digitale Revolution**

Wie elektronische Währungen unsere Welt verändern können.

2 **Blockchain – die technologische Basis**

Welche Technologie im Maschinenraum von Bitcoin arbeitet.

3 **Blockchain – Beispiele für die digitale Revolution**

Wie künftige Versicherungsmodelle aussehen könnten.

Parametric Insurance – eine kurze Definition

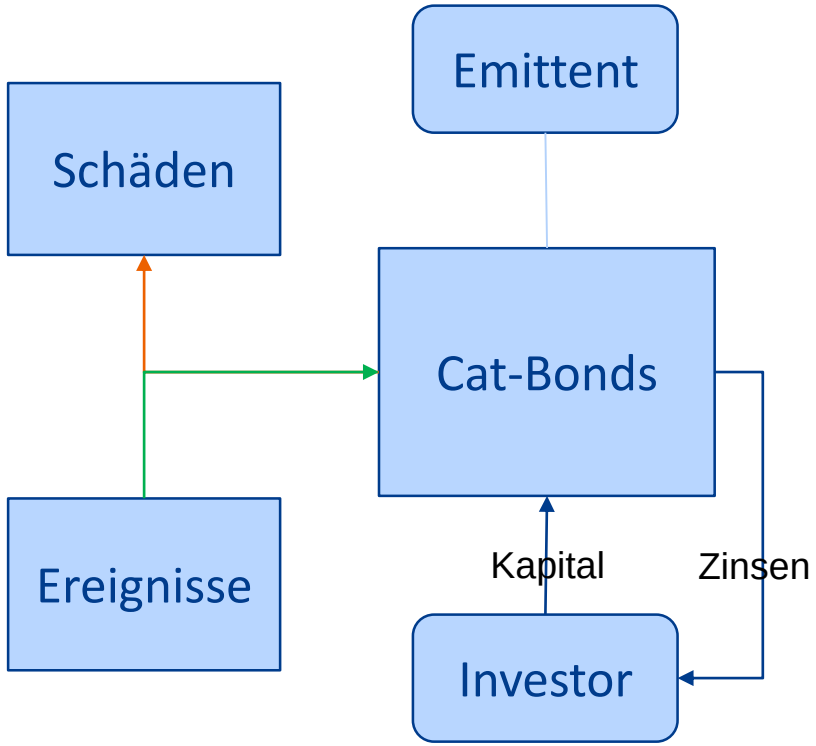
Die **parametrische (Wetter)-Versicherung** ist ein Absicherungsinstrument von (Wetter)-Risiken. Im Gegensatz zu klassischen Schadenversicherungen versichert die parametrische (Wetter)-Versicherung den Versicherungsnehmer gegen das Eintreten alltäglicher Wetterereignisse. So wird beispielsweise die Über- oder Unterschreitung bestimmter Niederschlagsmengen, Sonnenstunden oder auch Temperaturhöhen in einem vereinbarten Zeitraum versichert. Die Versicherungsleistung basiert auf den **Messwerten** der jeweiligen Messstation und nicht auf **konkreten Schäden**, die dem Versicherungsnehmer entstehen.

Frei nach https://de.wikipedia.org/wiki/Parametrische_Wetterversicherung

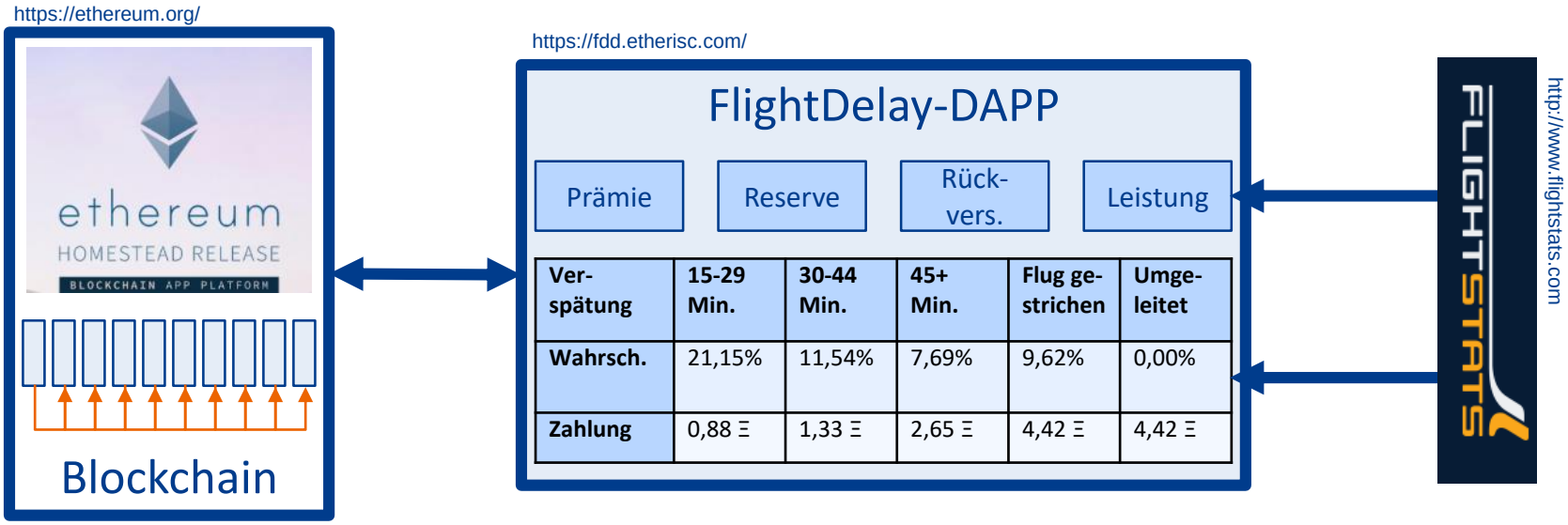
Parametric Insurance – Cat-Bonds

- Allianz Katastrophen-Anleihen (Pressemitteilung vom 15.06.2016)
- Die „Smart Contract“-Technologie erleichtert und beschleunigt den Auslösemechanismus von Naturkatastrophen-Swaps und -Anleihen
- Das Pilotprojekt von Allianz Risk Transfer (ART) ist eines von mehreren Testfeldern: Allianz Team „Disruptive Technlogies“ untersucht künftige Einsatzmöglichkeiten von Blockchain
- Denkbar ist der Einsatz der Blockchain-Technologie auch in anderen Versicherungs-transaktionen.

Erfolgreiches Pilotprojekt: Allianz Risk Transfer und Nephila realisieren Katastrophen-Swap mit Blockchain-Technologie



DApp FlightDelay - Flugverspätungsversicherung



Zahlungsverkehr, Datenhaltung und Durchführung

SmartContract Leistungsversprechen und -erfüllung

Statistische Daten und Sensoren / Auslöser

Bitsurance und Blocksurance – Definitionen

BITSURANCE

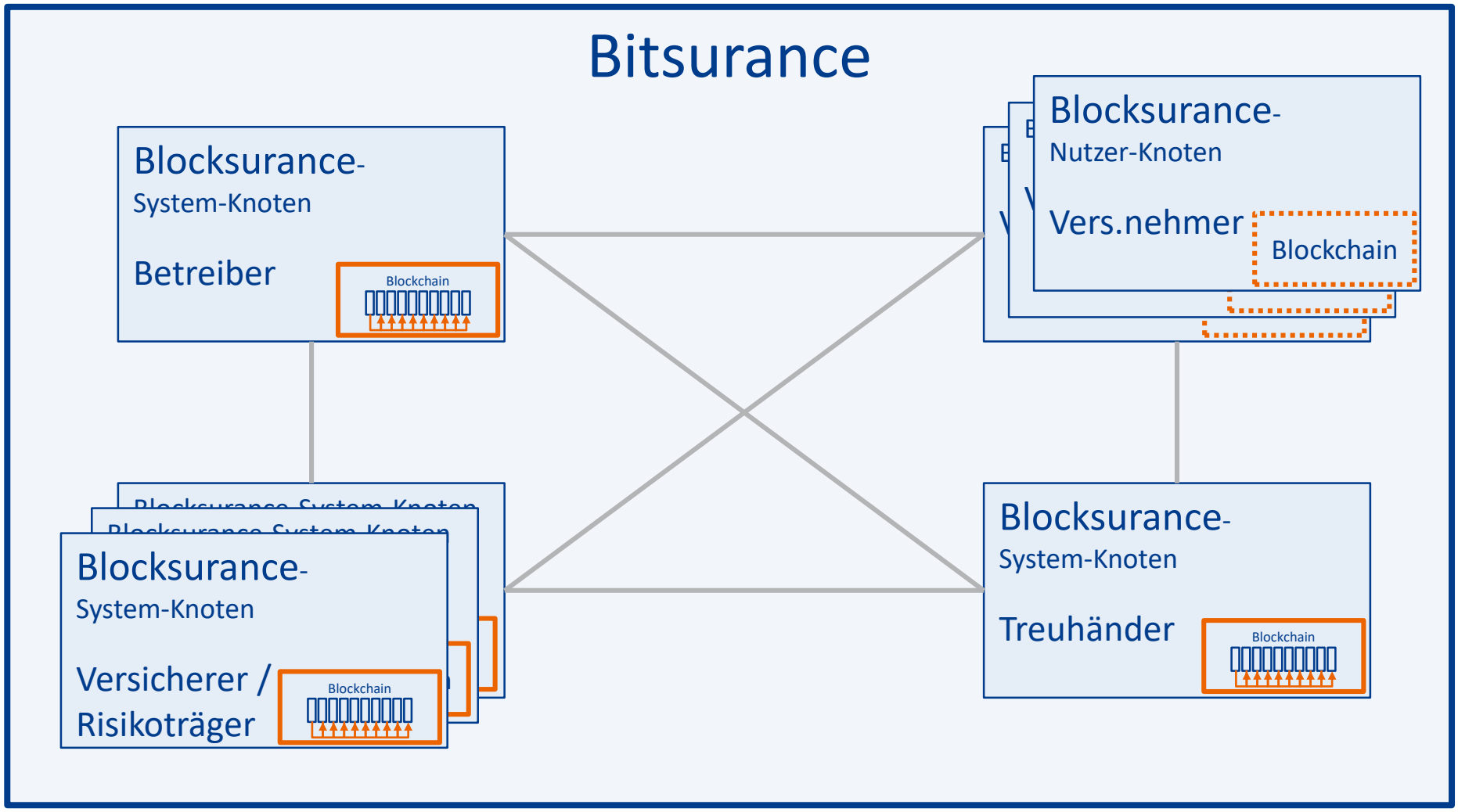
Als Bitsurance (Vertrag) bezeichnen wir einen Versicherungsvertrag, der vollständig automatisiert, digital und transparent geschlossen und administriert wird.

BLOCKSURANCE

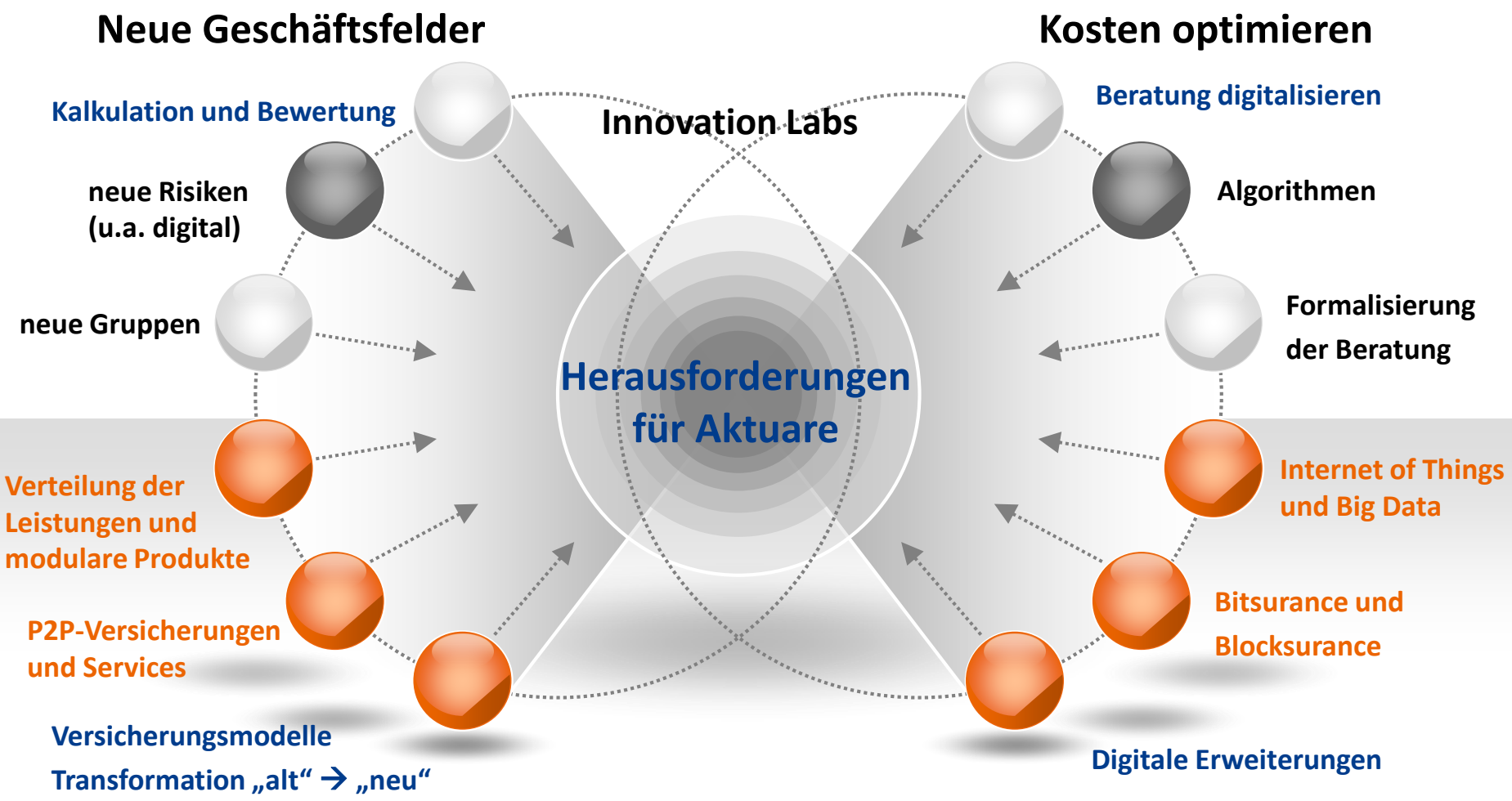
Als Blocksurance (System) bezeichnen wir eine dezentrale, fachliche und technische Systemkomponente, die Versicherungsverträge mit Hilfe der Blockchaintechnologie verwaltet.

Zentral ist dabei die Verwendung der Blockchaintechnologie als verteiltes, fehlertolerantes, nicht änderbares (= manipulationssicheres), digital und öffentlich geführtes Buchhaltungsjournal unter Nutzung von Smart Contracts.

Bitsurance und Blocksurance – könnte es so funktionieren?



InsureTech's und aktuarielle Herausforderungen



Links (eine ganz kleine Auswahl!)

Basics

- de.wikipedia.org/wiki/SHA-2

BitCoin

- www.bitcoin.org
- https://de.bitcoin.it/wiki/Hauptseite

Ethereum / Smart Contracts

- www.ethereum.org
- www.etherbasics.de
- de.wikipedia.org/wiki/Ethereum
- de.wikipedia.org/wiki/Smart_Contract

Links (eine ganz kleine Auswahl!)

FinTech – allgemeine Informationen

- www.fintechforum.de
- www.bundesfinanzministerium.de/Web/DE/Themen/Schlaglichter/FinTech-Deutschland/fintech-deutschland.html
- www.bafin.de/DE/Aufsicht/FinTech/fintech_node.html

InsurTech‘s

- www.knip.de
- www.massup.de
- www.friendsurance.de
- www.heyguevara.com
- www.versicherix.ch
- www.hioscar.com

Kontakt

Mathias Ott
m.ott@hba-consulting.de
+49 (241) 400 50 39 - 1

Wiesbadener Str. 73

65510 Idstein

www.hba-consulting.de