UNIVERSITÄT
LEIPZIG

Wirtschaft im digitalen Wandel

Kryptowährungen, Hawala-System und alternativer Zahlungsverkehr

30.01.2019

Tom Dietze
Tino Barig

GLIEDERUNG

1. Kryptowährungen
   - Bitcoin
   - Blockchain
   - Möglickeiten und Kritik

2. Hawala-System

3. Alternativer Zahlungsverkehr

1 KRYPTOWÄHRUNGEN

Definition

*Kryptowährungen sind digitale **(Quasi-)Währungen** mit einem meist **dezentralen**, stets verteilten und **kryptografisch** abgesicherten Zahlungssystem.* (Bendler 2018)

1 KRYPTOWÄHRUNGEN

Top 3 Kryptowährungen 01/2019

Name	Symbol	Start	Marktanteil	Marktkapitalisierung
Bitcoin	BTC	2009	51,7 %	65,6 Mrd. $
Ripple	XRP	2012	11,4 %	14,5 Mrd. $
Ether	ETH	2015	11,1 %	11,1 Mrd. $

Stand 2018: ca. 4500 Kryptowährungen in Verwendung

1 KRYPTOWÄHRUNGEN

Merkmale :

- Bargeldloser Zahlungsverkehr ohne Abhängigkeit, Aufsicht, Mitwirkung von Banken oder Behörden

- Festlegung der Anzahl der Währungseinheiten **vor** der Erzeugung

  → Keine nachträgliche Vermehrung des Geldes (keine Inflation)

- **Blockchain** zum Erfassen und Beschreiben von Transaktionen auf mehreren Computern

  → Dezentrale Verwaltung

1.1 BITCOIN

Bildquelle: https://de.wikipedia.org/wiki/Bitcoin

- Grundidee ging aus der *Cypherpunkbewegung* der 90er Jahre hervor :
  → Schaffung einer virtuellen Währung ohne staatliche Aufsicht

- Erstes Konzept von „Satoshi Nakamoto“ innerhalb einer Mailingliste zum Thema Kryptographie

- Erste erfolgreich eingeführte Kryptowährung (2008)

1.1 BITCOIN

Bildquelle: https://de.wikipedia.org/wiki/Bitcoin

Motivation von Nakamoto:

- Konventionelle Währungen benötigen Vertrauen in die Zentralbanken, um zu funktionieren
- Bürger müssen Banken ihr Geld anvertrauen
- Banken vergeben ungedeckte Kredite, sammeln unkontrolliert und ohne Sicherheit personenbezogene Daten

→ Sowohl Geld, als auch Daten in Gefahr

→ Lösung: elektronische Währung mit starker Verschlüsselung ohne Mittelsmänner

1.1 BITCOIN

Bildquelle: https://de.wikipedia.org/wiki/Bitcoin

Verwendung

- jeder Nutzer besitzt **public Key** (Bitcoin-Adresse)
  - Referenz auf „Konto“ des Kunden
  - Benötigt zum Transfer Zum Nutzer
- jeder Nutzer besitzt **private Key**
  - Benötigt zum Transfer vom Nutzer zu einem anderen
  - **Wallet** zur Steuerung
- Speicherung aller Transaktionen in verteilter Datenbank → **Blockchain**

1.2 BLOCKCHAIN

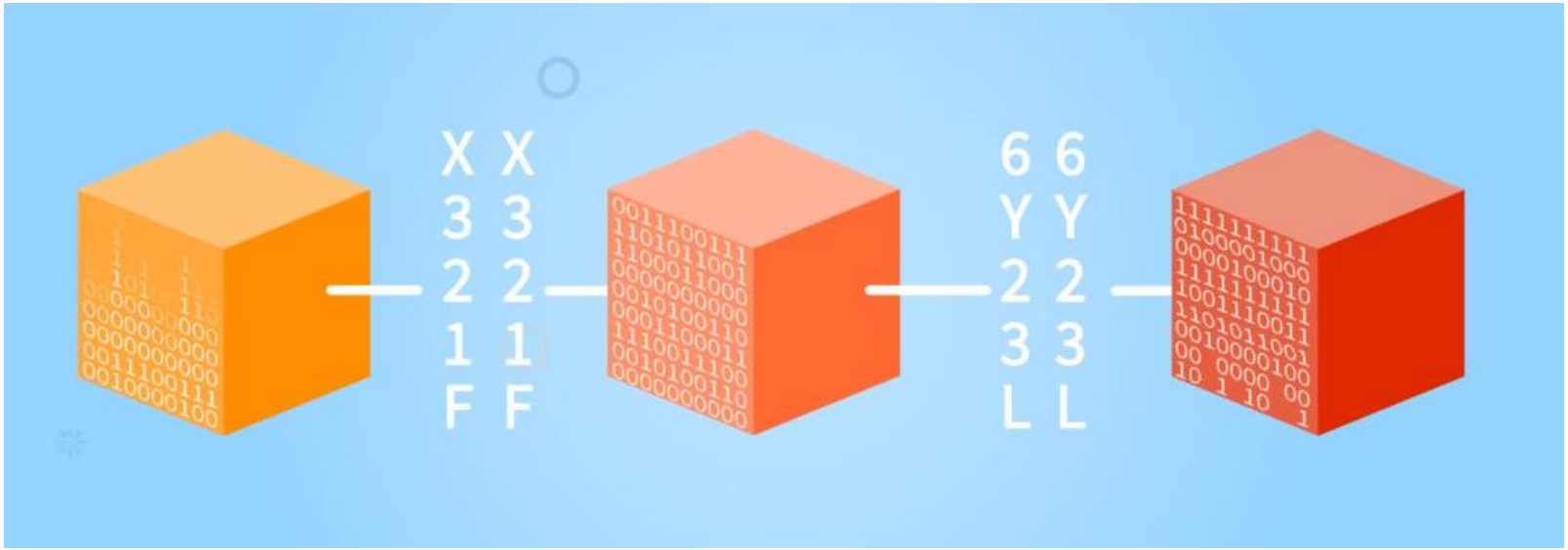
Definition

***Dezentrale**, chronologisch aktualisierte **Datenbank** mit einem aus dem Netzwerk hergestellten **Konsensmechanismus** zur dauerhaften digitalen Verbriefung von Eigentumsrechten.* (Mitschele 2019)

1.2 BLOCKCHAIN - MERKMALE

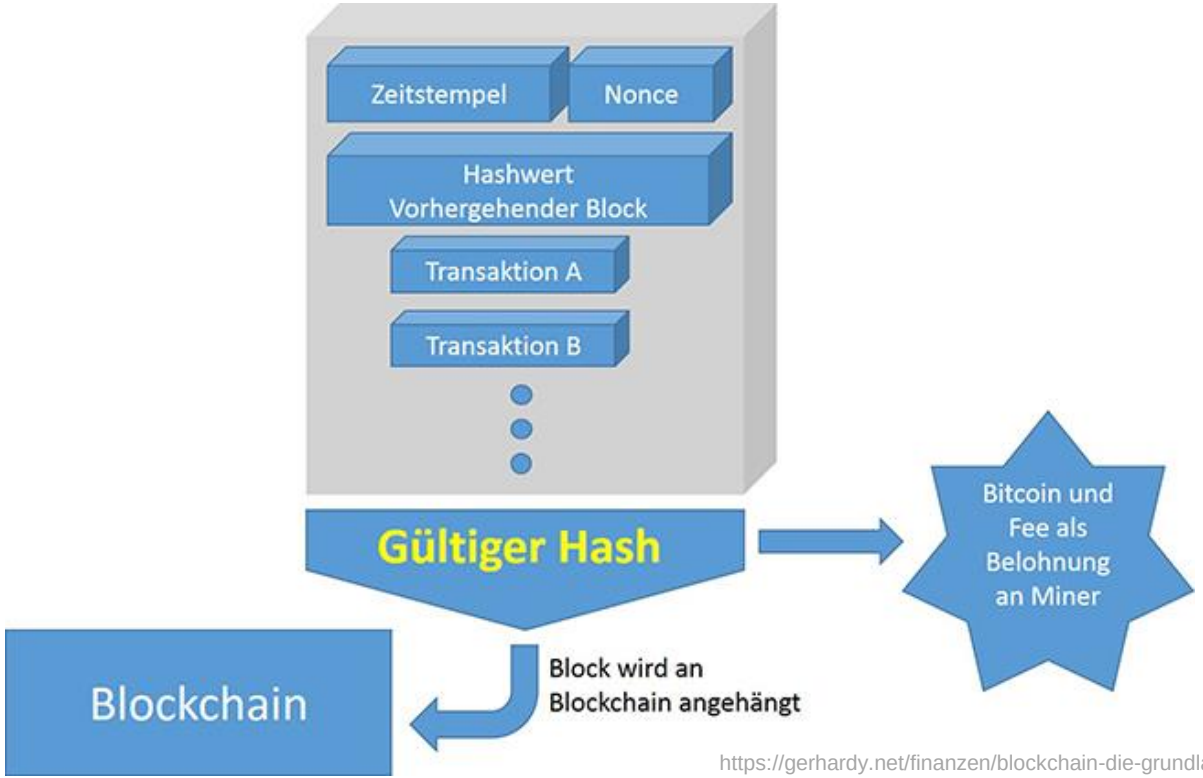
- **Verkettung**: feste Folge von Datenblöcken
- **Dezentrale Speicherung**: kein zentraler Server, alle Beteiligten führen Register
- **Konsensmechanismus**: Alle Teilnehmer stimmen algorithmisch über neue Blöcke ab.
- **Manipulationssicher**: kryptografische Sicherung der Blockchain
- **Transparenz**: Alle Daten von jedem einsehbar
- **Digitale Signatur**: alle Transaktionen eindeutig nachweisbar

1.2 BLOCKCHAIN - FUNKTIONSWEISE



Bildquelle: https://www.youtube.com/watch?v=4FU3tc-foaI

1.2 BLOCKCHAIN - FUNKTIONSWEISE

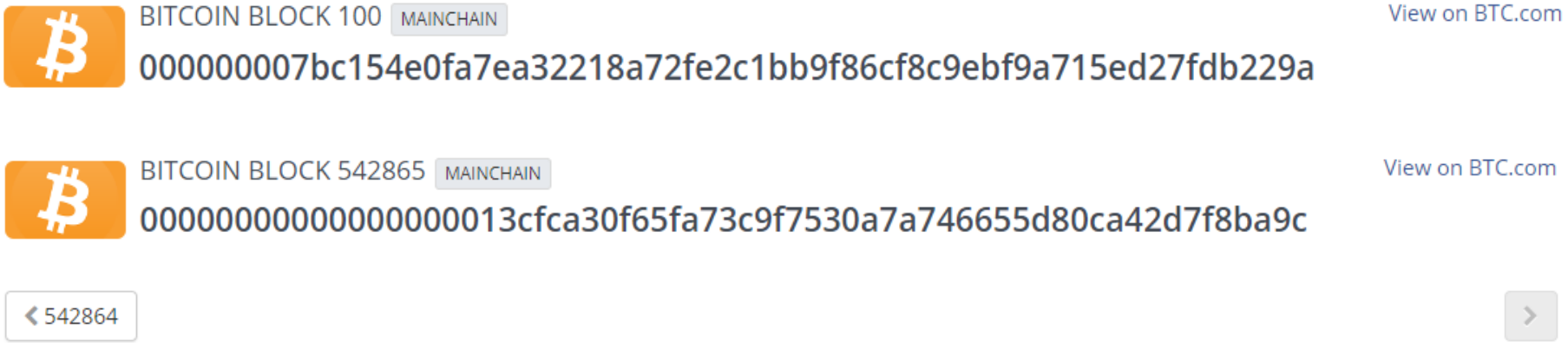


https://gerhardy.net/finanzen/blockchain-die-grundlage-der-bitcoins/

BLOCKCHAIN - FUNKTIONSWEISE

MINING DIFFICULTY

- Bsp Bitcoin



MINING

- Zu Beginn mit CPU’s
  - Später Umstieg auf GPU’s
    - Danach Umstieg auf *Field Programmable Gate Arrays* (FPGA)
      - Heute *Application Specific Integrated Circuits* (ASIC)

→ Maximierung der Rechenleistung bei minimalem Energieverbrauch

- Mining Pools vs eigenes Mining

KRYPTOWÄHRUNGEN - MÖGLICHKEITEN

- Bitcoin quasi virtuelles Bargeld

- Andere Anwendungsmöglichkeiten denkbar:
    - Tokens für Nutzungsrechte (social Media, Online Plattformen)
    - Tokens für Ressourcen (Wasser, Elektrizität)

BLOCKCHAIN - MÖGLICHKEITEN

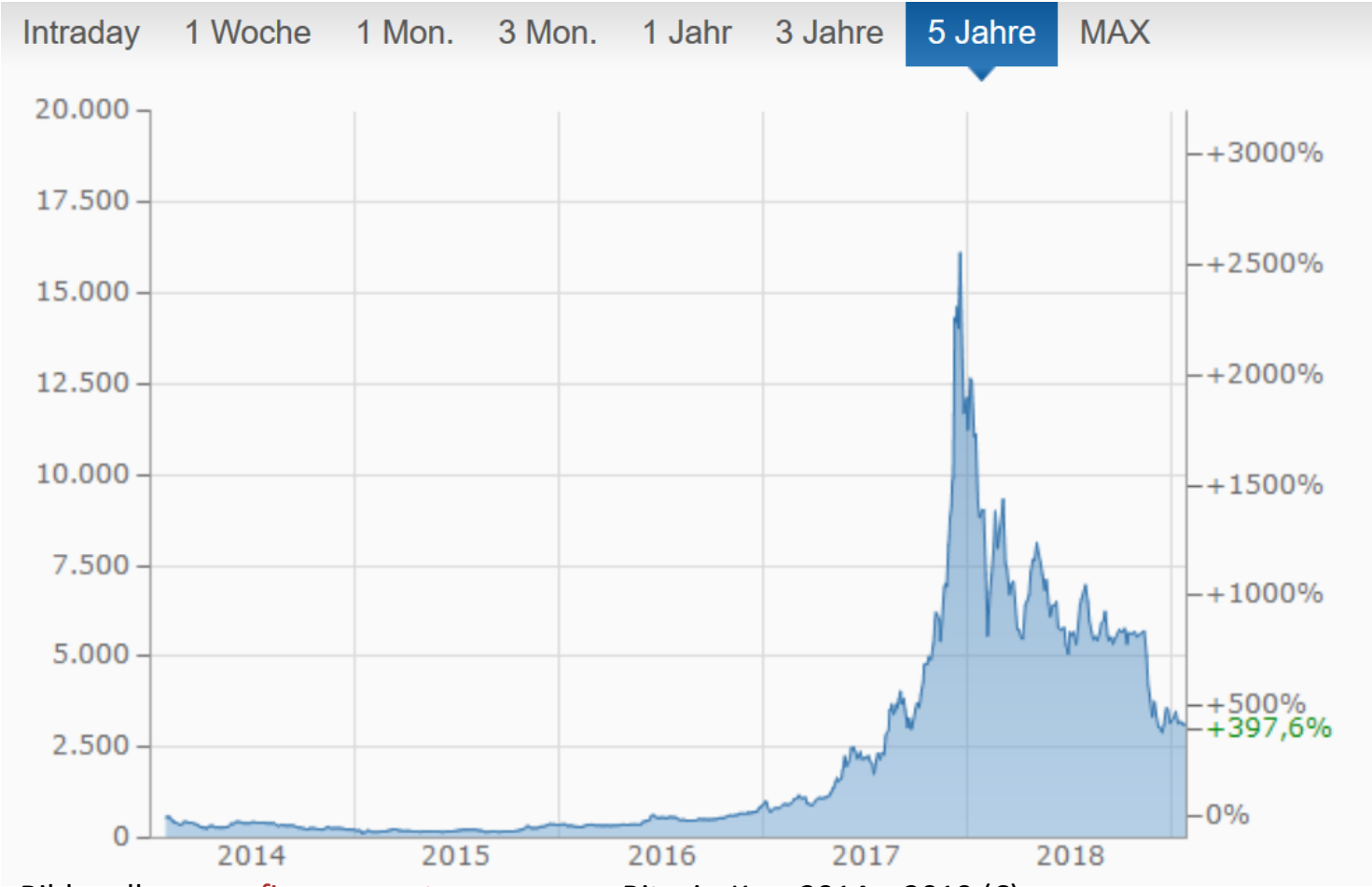
ZUKÜNFTIGER NUTZEN

- Banken (Transaktionen)
- Verhinderung Verkauf von Fälschungen (Kunst)
- Gegen Softwarepiraterie, Urheberrechtsverletzungen (Musik)
- Medizin (Patientendaten nur bei Bedarf an Arzt)
- Pharmazie (Supply-Chain), Verhinderung von Diebstählen

KRITIK

FINANZIELLE ASPEKTE

- Bitcoin ist keine Währung, sondern Handelsware
- Bei übermäßiger Last sind Transaktionen langsam → teuer
- Spekulation durch fehlende Kontrolle
- Hohe Kurse und Erwartungen vs geringe Nutzung im Kommerz
- Hyperinflation durch neue Währungen
- Informationsasymmetrie (leicht zu benutzen aber schwer zu verstehen)
- Schneeballsystem (Hype zieht Nutzer an, Nachzügler werden nur verlieren)



Bildquelle: www.finanzen.net

Bitcoin-Kurs 2014 – 2019 (€)

KRITIK

RECHTLICHE ASPEKTE

- Förderung von Kriminalität
    - Geldwäsche
    - Steuerhinterziehung
    - Drogen-/Waffenhandel

KRITIK

ÖKOLOGISCHE ASPEKTE

- Mining erfordert große Rechenanlagen
    - Enormer Stromverbrauch

- Mining-Farmen werden in Regionen mit günstigem Strom errichtet
    - Kohlestrom

- Jahresenergieverbrauch durch Mining übersteigt mittlerweile den Österreichs

KRITIK

TECHNISCHE ASPEKTE

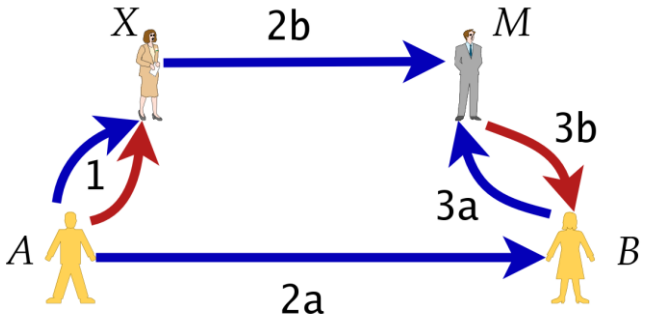
- Blockchain unanfällig für Angriffe
- Gefährdung des Systems nur durch 51% Angriff
- Nutzung der eigenen Bitcoins erfolgt durch Wallets und über Handelsplattformen
  - → Diese sind anfällig für Hackerangriffe
- Transaktionen lassen ohne zusätzliche Informationen nicht auf Personen schließen
  - → Anonymität trotzdem durch behördliche Nachforschungen gefährdet

HAWALA-SYSTEM

Das Hawala-System ist ein informelles Überweisungssystem das zum Großteil auf *Vertrauen* basiert.

Funktionsweise

- A gibt Geld und Code an X
- Code wird von X/A an M/B weitergeleitet
- B sagt M Code, und bestätigt damit Zahlungsverkehr



RECHTSGRUNDLAGE

- Überweisungen ohne Aufzeichnung
- In Deutschland verstoß gegen:
  - § 54 Kreditwesengesetz
  - Steuerhinterziehung
  - Embargo im Außenwirtschaftsgesetz
- gleiches System in
  - Ostasien (Viele Namen, meist „fliegendes Geld“ o.ä.)
  - Lateinamerika („Kolumbianisches System“)
  - Indien

NUTZUNG

- Überweisung von Migranten in ihr Heimatland
  - Heimatland meist kein funktionierendes Banksystem (mit Europa)
- Jährlich ca. 200 Mrd. Dollar transferiert
- Nach Schätzungen benutzt die Hälfte der indischen Wirtschaft das Hawala-System für Überweisungen
- Terrororganisationen wie ISIS werden mit diesem System durch Spendengelder finanziert

PAYPAL

- Betreiber eines Online-Bezahldienstes für Mittel- und Kleinbeträge vom Ein- und Verkauf
- Mehr als 192 Millionen Nutzer mit Möglichkeit Zahlungen von 100 versch. Währungen
- In mehr als 200 Märkten zur Verfügung
- Sitz in San José, Kalifornien
- Tochterunternehmen *Paypal Europe* in Luxemburg

FUNKTIONSWEISE

- Registrierung mit E-Mail Adresse -> Keine Kontonummer
- Sender:
  - Geld vom Bankkonto wird in „E-Geld“ umgewandelt und auf Paypal-Konto gespeichert
- Empfänger:
  - „E-Geld“ vom Paypal-Konto wird in Geld umgewandelt und auf Bankkonto transferiert

VORTEILE

- Sehr schnelles Bezahlen möglich
- Zuverlässiger Kundenservice
- Käuferschutz

NACHTEILE

- Kann „einfacher“ gehacked werden
- Durch Keylogger o.ä. unsicherer als Bankkonto

RECHTSGRUNDLAGEN / KRITIK

- Paypal sperrt Konten wenn sie illegale Aktivitäten ***vermuten***
- 2010 Konto zur Finanzierung von WikiLeaks gesperrt, da Paypal *keine illegalen Aktivitäten unterstützt*
- Paypal sperrt bei auffälligen Aktivitäten ebenfalls Konten verwandter Personen -> unzulässig nach deutschem Bankenrecht
  - Paypal betont hierbei, dass sie keine Bank sind, sondern ein Internet-Bezahldienst, für den andere Regelungen gelten
  - Sitz in Luxemburg -> andere Bedingungen
- Paypal speichert Fingerabdruck- und Standort-Daten
- Außerdem Angaben zu allen installierten Apps
  - Ziel ist es, Kontozugriffe zu erkennen, die nicht zum Standort passen und je nach Aufenthaltsort und zu Interessen passende Werbung einzuspielen.

BIOMETRISCHES BEZAHLEN

- Bezahlen m.H. biometrischer Daten, also
  - Fingerabdruck, Iris-Scan, Herzschlagrate,…
- Mit Einführung des Fingerabdrucksensors an Smartphones Grundstein gelegt
- 2016 Einführung „Apple Pay“ auf iPhones
- Mastercard erstes Unternehmen, dass Fingerprint und Gesichtserkennung getestet hat

BIOMETRISCHES BEZAHLEN - MEINUNGEN

- 1.877 Konsumenten wurden 2015 befragt, Befürworter:
  - Fingerabdrucksensor 75%
  - Iris-Scan 60%
  - Handlinien-Scans 50%
- Vorteile für Konsumenten:
  - Müssen sich keine Passwörter mehr merken (71% Zustimmung)
  - Denken, dass ihre Daten dadurch schwieriger zu stehlen sind (70% Zustimmung)

BIOMETRISCHES BEZAHLEN - SICHERHEIT

- Nutzer befürworten Sicherheit der Zahlungsmethode
- CCC hat bereits mehrfach Gegenteil bewiesen
- Bisher „sicherstes“ biometrisches Verfahren
  ist Venenerkennung
- Wurde 2015 aber ebenfalls umgangen vom CCC

Bildquelle: https://t3n.de/news/chaos-computer-club-fingerabdruck-586492/

SMART CONTRACTS

Definition

Smart Contracts sind Computerprotokolle, die Verträge abbilden oder überprüfen oder die Verhandlung oder Abwicklung eines Vertrags technisch unterstützen.

SMART CONTRACTS

- Basieren auf Blockchain-Technologien
- Ersetzen Mittelsmann -> schnellere Bearbeitung
  - zudem automatisiert
- Dezentrale „Verwahrung“ des Geldes, bis Vertrag (nicht) erfüllt wird

SMART CONTRACTS - SICHERHEIT

- Code sehr schwierig zu verstehen
- Code muss sehr viel abfangen, z.B. Tod einer Person
- Sicherheitslücken dadurch nicht leicht zu finden, aber sehr wahrscheinlich vorhanden
- Bsp.: DAO

QUELLEN

Bendler, Oliver (2018): Gabler Wirtschaftslexikon. Springer Gabler. https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160/version-277214 (27.01.2019)
Görgens, Egon (2007): Makroökonomik 10. Auflage. Lucius & Lucius: Stuttgart.
Mitschele, Andreas (2018): Gabler Wirtschaftslexikon. Springer Gabler.
https://wirtschaftslexikon.gabler.de/definition/blockchain-54161/version-277215
(27.01.2019)
https://coinmarketcap.com/ (27.01.2019)
https://kryptoszene.de/news/bitcoin-mining-verursacht-im-jahr-so-viel-co2-wie-1-million-transatlantik-fluege/ (27.01.2019)
https://www.btc-echo.de (27.01.2019)
Patrick M. Jost and Harjit Singh Sandhu, Interpol General Secretariat, Lyon, January 2000
http://documents.worldbank.org/curated/en/335241467990983523/The-money-exchange-dealers-of-Kabul-a-study-of-the-Hawala-system-in-Afghanistan (28.01.2019)
Werner Pluta: *US-Regierung setzt Paypal unter Druck*. In *golem.de*, 8. Dezember 2010
http://www.golem.de/1012/79994.html (28.01.2019)
Brauchen wir PayPal? Über Sinn und Unsinn des Online-Bezahlsystems.: In *it-recht-kanzlei.de*, 18. November 2010
http://www.it-recht-kanzlei.de/Brauchen_wir_PayPal.html (28.01.2019)
Bezahlen per Fingerabdruck statt mobile payment?
https://www.ifhkoeln.de/pressemitteilungen/details/bezahlen-per-fingerabdruck-statt-mobile-payment/ (28.01.2019)
Biometrische Authentifizierung: Chaos Computer Club hackt Fingerabdruck über Foto
https://t3n.de/news/chaos-computer-club-fingerabdruck-586492/ (28.01.2019)
https://de.wikipedia.org/wiki/Smart_Contract (28.01.2019)
https://www.kreditkarte.net/wissenswertes/smart-contracts/ (28.01.2019)
https://medium.com/coinmonks (27.01.2019)

UNIVERSITÄT
LEIPZIG

VIELEN DANK!

Tino Barig
Tom Dietze