mainproject 2018

mainproject 2018
Bitcoins & Blockchains – einige Erläuterungen und Einschätzungen

Industrie Center Obernburg, 16. Januar 2018

Prof. Dr. Georg Rainer Hofmann
Prof. Dr. Erich H. Ruppert

Version 16. Jan 2018 – 1

hochschule aschaffenburg
university of applied sciences

information management institut

Mainsite

SGM Educational Solutions

Fraunhofer FOKUS

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS

ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN

Projektpartner im ESF-Projekt mainproject 2018

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN

mainproject 2018

Information Management Institut (IMI)
an der Hochschule Aschaffenburg

- Zusammenarbeit mit der Wirtschaft und Praxis im Bereich Informationsmanagement und Wissensbewertung
- Akquisition und Durchführung von Drittmittelprojekten
- Unterstützung der akademischen Lehre und Forschung

Mainsite GmbH & Co. KG

- Betreibergesellschaft des Industrie Center Obernburg (ICO)
- Drittmittelgeber im Projekt mainproject 2018

SGM Solutions & Global Media GmbH

- Drittmittelgeber im Projekt mainproject 2018

Qualitätssicherung im Projekt mainproject 2018

- Regelmäßige Konsultationen
- überregionale Aspekte

ESF-Projekt KaRaBonita – April 2013 bis März 2015
(– „Kapital – Rating – Bonität“ –)
Wissenstransfer von Methoden zur Verbesserung der Kapitalausstattung von kleinen und mittelständischen Unternehmen der Region Bayerischer Untermain – KaRaBonita

ESF-Projekt *mainproject* – Oktober 2011 bis September 2014
Wissenstransfer von Methoden der Prozessoptimierung, Lean Management und des Dienstleistungsmanagements für Mitarbeiter regionaler Unternehmen, insbesondere im Industrie Center Obernburg (ICO) in Elsenfeld und Erlenbach am Main

ESF-Projekt *KontAkS* – Oktober 2009 bis September 2012
Wissenstransfer von Methoden nicht-technischer Innovationsforschung zur Ermittlung von **Kont**ext und **Ak**zeptanz von **S**ystemen

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN

mainproject 2018

ESF-Projekt mainproject 2018

Projektlaufzeit:
Mai 2015 bis April 2018
Erweiterung ab Mai 2017

Ziele:
Wissenstransfer, insbesondere im Kontext „Digitale Transformation“ zur Stärkung der Wettbewerbsfähigkeit von KMU in der Region Bayerischer Untermain

Herangehensweise:
- Bedarfe der Unternehmen erfassen
- Informationsdefizite und Einstiegshemmnisse abbauen
- Regionales Netzwerk für KMU aufbauen
- Hochschulseitig vorhandenes Wissen in die betriebswirtschaftliche Praxis umsetzen

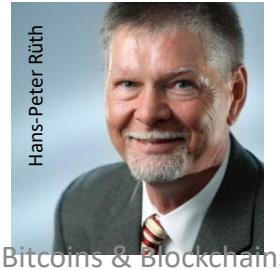
Informieren – Analysieren – Realisieren

mainproject 2018
Team

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN

mainproject 2018

mainproject 2018



Die Leitfragen der Maßnahme *mainproject 2018*

„Welche neuen Themen darf man als hiesiges Unternehmen nicht verpassen?“

„Wie kann man neue Themen im Unternehmen direkt und effektiv umsetzen?“

Netzwerk-veranstaltungen

Vortrag zu einem aktuellen Thema unternehmensübergreifend und vorwettbewerblich

Seminare

Vermittlung von Methoden, Schulung der Mitarbeiter, vorwettbewerblich

Digitaler Wissenstransfer

Seit Mai 2017

Digitale Aufbereitung von Wissens-transferinhalten aus Netzwerkver-anstaltungen und Seminaren in Form von Blended Learning

Workshops

Üben und Anwenden von Metho-den; wettbewerbsrelevant; auch Non-Disclosure und In-house;

Beratung

Auseinandersetzung mit konkretem Problem auf Seiten des Kunden, Non-Disclosure; Second-Opinions, Konzepte und Umsetzungshinweise

Beispiele:

- Netzwerkveranstaltung „Industrie 4.0 und IT-Sicherheit“
- Diverse KVP-Seminar
- Workshop Employer Branding
- Beratungsprojekte, z.B. Professional Service Firm
- Roadshow Social Virtual and Augmented Reality
- etc.

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN

Onlinekurse

- Elektronische Rechnungsstellung
- EU-Datenschutzgrundverordnung – in Vorbereitung
- Employer Branding – in Vorbereitung
- Industrie 4.0 – in Vorbereitung

Registrierung über unsere Webseite:
www.mainproject.eu/onlinekurse

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN

Q - LAB

Perfektes Arbeitsumfeld
für das Entwickeln von Ideen

Flipcharts,
Moderationswände
Beamer,
Lautsprecher
Flexible Tische
und Sitzmöbel
Umfangreiches Material
für Kreativprozesse

Video - LAB

Video und Audiotechnik für die
Digitalisierung von Lerninhalten

Green Screen Recording
für optimales Freistellen
Geschultes und erfahrenes
Redaktionsteam

an *mainproject 2018* teilhaben:

Immer up-to-date

Regelmäßige Veranstaltungshinweise und Themenvorstellungen über unseren **Newsletter** „mainproject 2018 informiert“
Registrierung über unsere Webseite www.mainproject.eu

Kooperationspartner werden

Für regionale KMU unentgeltlich!
Unterzeichnen der Absichtserklärung – Sprechen Sie uns an …
Erörterung bilateraler Interessen und Aufgaben
Definition der individuellen Vorgehensweise und Maßnahmen

mainproject 2018

Bitcoins & Blockchains

- einige Erläuterungen und Einschätzungen

Industrie Center Obernburg, 16. Januar 2018

Prof. Dr. Georg Rainer Hofmann
Prof. Dr. Erich H. Ruppert

hochschule aschaffenburg
university of applied sciences

information management institut

Mainsite

SGM Educational Solutions

Fraunhofer FOKUS

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS

ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN

Block

Blockchain

Geld – Geldfunktion

(elektronische) Zahlungsmittel

Bitcoin

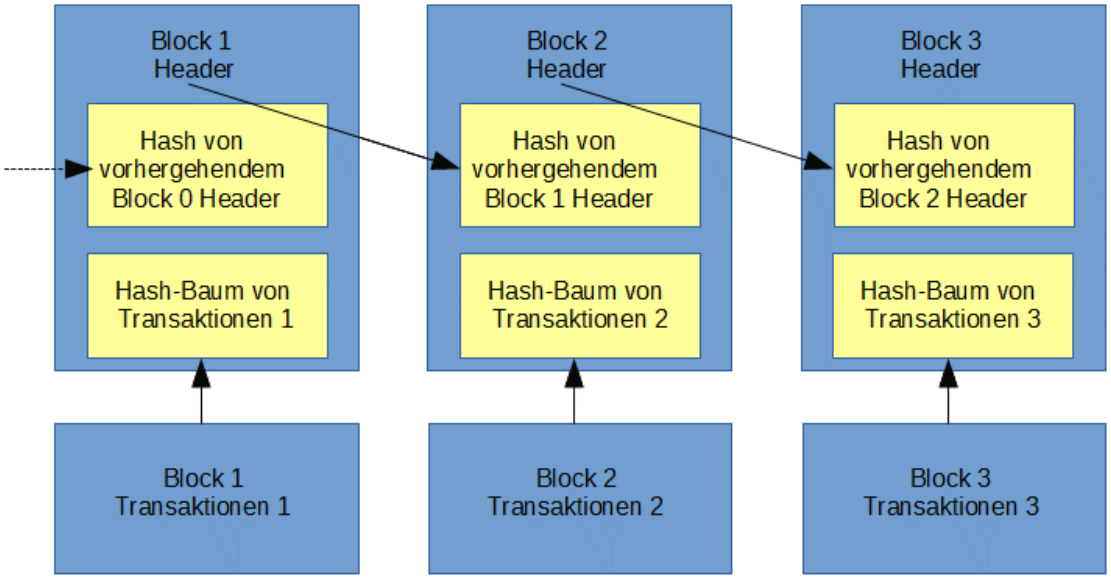
Währung

Offene verteilte Dokumente – distributed ledger technology

Spekulation – Hype

Block:
„Ausstattung“ eines Nutz-Datensatzes (Transaktionen) mit einem Merkmal („Hash“), das die Originalität des Datensatzes garantiert.

Blockchain:
Eine Kette – in jedem neu hinzugefügten Nutz-Datensatz (z.B. Transaktion) steckt das Merkmal („Hash“) des vorigen Datensatzes.



EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN
mainproject 2018

Ein einfaches Beispiel für ein Blockschema und eine Blockchain:

„E“	0	101161	64750	17	X
voriges Merkmal („H“)		Geb.-Datum	PLZ	„Zahl“	neues „H“

X = QS1 (QS * „Zahl“) = QS1 (40 * 17) = QS1(680) = 5

0 101161 64750 17 5

X = QS1 (64 * 36) = QS1(2304) = 9

5 090508 63739 36 9

usw.

One-Way Hash Function oder OWHF

Eine OWHF erfüllt die Bedingung der Einwegfunktion („Falltür“):
Es ist praktisch unmöglich, zu einem gegebenen Ausgabewert H einen Eingabewert E zu finden, den die Hashfunktion auf H abbildet (*preimage resistance*).

Eine OWHF erfüllt die Bedingung der schwachen Kollisionsresistenz:
Es ist praktisch unmöglich, für einen gegebenen Wert E1 einen davon verschiedenen E2 zu finden, der denselben Hashwert H ergibt.

Für Collision Resistant Hash Functions CRHF gilt die generelle Kollisionsresistenz:
es ist praktisch unmöglich, zwei verschiedene Eingabewerte E1 und E2 zu finden, die denselben Hashwert ergeben (*collision resistance*).

SHA – Secure Hash Algorithm:
Eine kleine Änderung der Nachricht E erzeugt einen ganz anderen Hash H
- diese Eigenschaft wird in der Kryptographie auch als Lawineneffekt bezeichnet.

SHA256("Franz jagt im komplett verwahrlosten Taxi quer durch Bayern")
= d32b568cd1b96d459e7291ebf4b25d007f275c9f13149beeb782fac0716613f8

SHA256("Frank jagt im komplett verwahrlosten Taxi quer durch Bayern")
= 78206a866dbb2bf017d8e34274aed01a8ce405b69d45db30bafa00f5eeed7d5e

Generierung und Mining *neuer Blocks*

Am einfachen Beispiel für ein Blockschema und eine Blockchain:

Proof-of-work
Alternativ (proof of stake)
als Validierungsmechanismus

Probieren !
In der Bitcoin-Blockchain braucht man dafür ca. 10 Min.

X = QS1 (QS * „Zahl“) = QS1 (40 * 17) = QS 680 = 5

0	101161	64750	17	5

X = QS1 (64 * 36) = QS 2304 = 9

5	090508	63739	36	9

9	080539	64711	YY	X

Ein neuer Satz Nutz-Daten.
Finde eine Zahl YY so, dass X einen ganz bestimmten Grenz-wert annimmt.

Distributed Ledger Technology (DLT)

→ Dezentral und Offen
- Jeder, der sich an die Regeln hält, hat Zugang

→ Diverse Protokolle, http, smtp, Post, etc.

→ Funktionen
- Lesen
- Schreiben
- Archivieren

→ Berechtigungen
- Im Konsens zu vergeben

→ Symmetrie
→ Proof-of-Work, etc.

→ Anwendungen
- Fälschungssichere Dokumente

→ Urkunden, Grundbücher
→ Ausweise
→ Zahlungsmittel, Wertpapiere

Verteilte Kontenbücher (DTL) - nicht nur Bitcoin

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN
mainproject 2018

- DLT-Teilnehmer haben gemeinsame Schreib-, Lese- und Speicherberechtigung
- traditionelle verteilte Datenbanken halten Daten auch im gesamten Netzwerk verteilt, eine Schreibberechtigung hat aber nur eine zentrale Instanz (mit Vertrauensstellung).
- Eine zentrale Datenbank mit einer Vertrauensstellung existiert für DLT nicht.

- Neue Informationen können von Teilnehmern bereitgestellt und über einen Validierungsprozess (Konsensmechanismen) in die Datenbank aufgenommen werden.
- Die neu erstellten Daten werden jeder Teilnehmerkopie des DL hinzugefügt, sodass alle Teilnehmer die jeweils aktuelle Version der gesamten Datenbank halten könnten (es in der Regel aber nicht tun werden).
- Um festzulegen, ob neue Daten der Datenbank hinzugefügt werden dürfen, existieren alternative Validierungsprozesse, auch Konsensmechanismen genannt (proof-of-work, proof-of-stake, Practical Byzantine Fault Tolerance (PBFT), ...)

Vgl. Deutsche Bundesbank Monatsbericht, September 2017, S. 36.

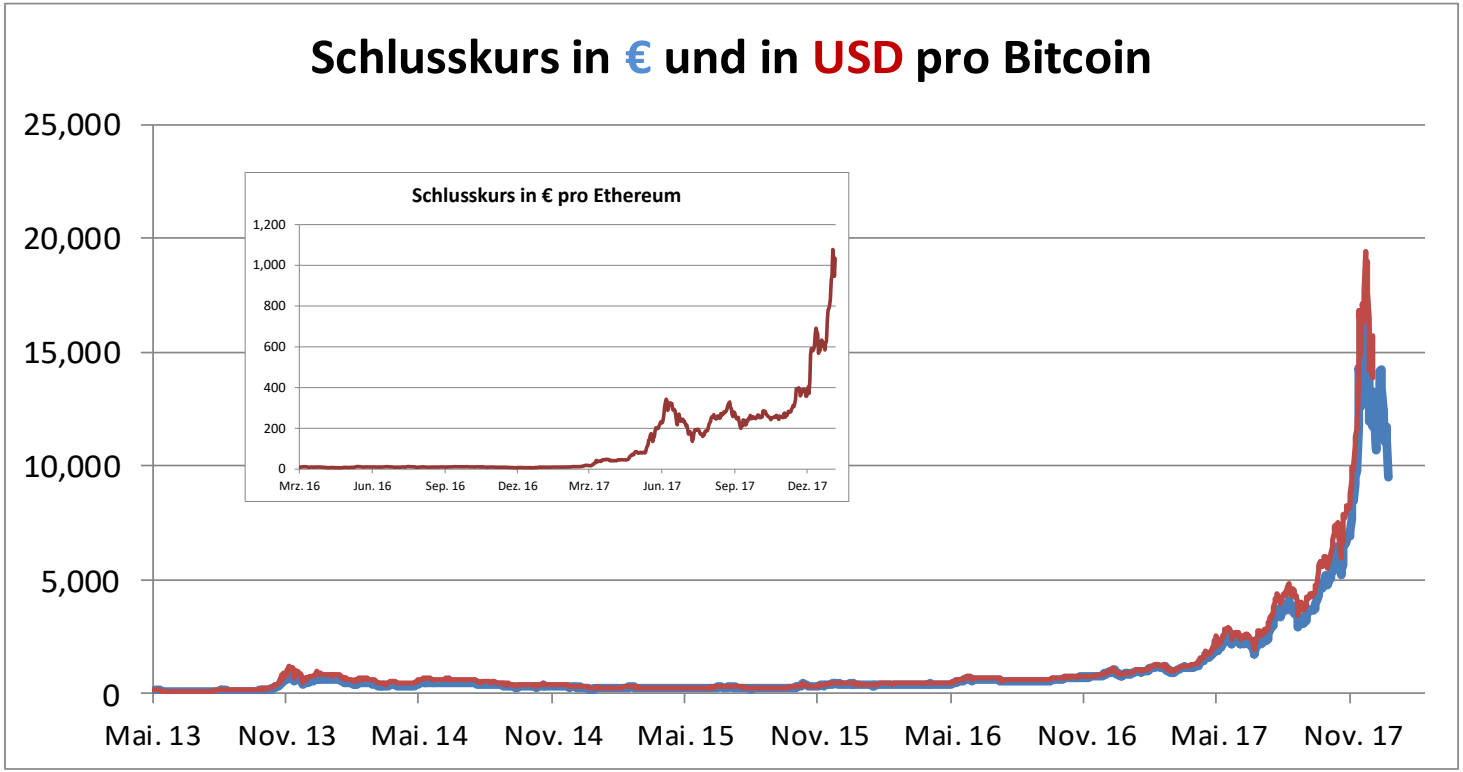
- Die Technologie der verteilten Kontenbücher (distributed ledger technology – DTL) wird von der Bundesbank als „*noch in einem frühen Stadium ihrer Entwicklungsreife*“ gesehen.

  (Deutsche Bundesbank Monatsbericht, September 2017, S. 36)

- Komplexere, an Bedingungen geknüpfte Vorgänge können abgebildet werden. Die automatische Prüfung solcher Bedingungen und die anschließende eigenständige Ausführung der Transfers durch einen Algorithmus werden häufig als Smart Contract bezeichnet.

- Bitcoin ist eine prominente Anwendung der Blockchain kombiniert mit der DTL-Technologie.
- In der Blockchain wird eine Transaktionshistorie mit Bitcoin abgelegt.
- Es entsteht eine „fälschungssichere“ Kette von chronologisch gereihten Blöcken, die im Nachhinein nicht veränderbar ist (auch keine Korrektur fehlerhafter Buchungen).
- Obwohl alle Transaktionen in Blöcken im verteilten Netzwerk von allen eingesehen werden können, sind die einzelnen Transaktionen dennoch anonym.
- Wurde eine Zahlung ausgeführt, sind Transaktionen also gültig und darf ein neuer Block mit mehreren Transaktionen der Kette hinzugefügt werden? Ein aufwändiger Validierungsprozesses (Abstimmungs-, Konsensmechanismus) erfolgt, um die Kette bei allen Teilnehmern um einen Block zu erweitern. Mining oder Schürfen.

Bitcoin Ist das relevant für uns?



EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN
mainproject 2018

Was ist Geld? – Money is what money does!

→ Geldfunktionen

- Tausch- und Zahlungsmittel
  (allgemein akzeptiert für den Kauf von Gütern und Diensten und zur Begleichung von Schulden)
- Recheneinheit
- Wertaufbewahrung (Depot)

→ „alles“ kann Geld sein !

→ Gesetzliche Zahlungsmittel:

→ man ist durch die Rechtsordnung verpflichtet, das Geld anzunehmen, wodurch eine Schuld mit rechtlicher Wirkung getilgt werden kann.

- „fälschungssichere“ Münzen und Noten
- Elektronisches Geld
- Buchgeld

→ anonym? universell?

→ Idealerweise billig herzustellen

Wofür ist das im Bezug auf Krypto„währungen“ wichtig?

- Akzeptanz
- einkommens- bzw. umsatzsteuerliche Konsequenzen

Bitcoin – *ist das Geld oder eine Währung?*

Antwort der Bundesregierung auf eine Anfrage des Bundestagsabgeordneten Frank Schäffler (FDP) vom 07.08.2013:
„Bitcoins“ sind weder E-Geld noch gesetzliches Zahlungsmittel und daher weder als Devisen noch als Sorten einzuordnen. Sie sind jedoch unter den Begriff der Rechnungseinheiten als Finanzinstrument nach §1 Absatz 11 Nummer 7 Kreditwesengesetz (KWG) zu subsumieren. Rechnungseinheiten sind Devisen vergleichbare Verrechnungseinheiten, die – anders als Devisen – nicht auf gesetzliche Zahlungsmittel lauten. Hierunter fallen Werteinheiten, die die Funktion von privaten Zahlungsmitteln bei Ringtauschgeschäften haben sowie jedes andere „private Geld“ oder sonstige Komplementärwährungen, die auf der Grundlage privatrechtlicher Vereinbarungen als Zahlungsmittel in multilateralen Verrechnungskreisen eingesetzt werden.

- keine allgemeine Akzeptanz (also kein *Geld*)
- man kann, aber man muss Bitcoin oder andere Krypto„währungen“ nicht akzeptieren
- einkommenssteuerlich wie Wertpapiergeschäfte
- keine pauschale Umsatzsteuerbefreiung (nach § 4 Nummer 8 Buchstabe b UStG), unterscheiden zwischen privaten Tauschgeschäften und gewerbsmäßigem Handel

Hype (Spekulationsblase, Preisblase)

→ Preisverlauf
- Massiv ansteigend, exponentiell
- „Zackeleien“ im Gipfel
- Reduktion auf „wahren Wert“
- Gipfel versus Basis: > 15 : 1

→ Beispiele
- Tulpenzwiebeln
- New Economy
- Asset-backed Securities
- etc.

→ Beteiligte
- Gegenseitige Spekulation
- Sachunkundige
- Hohe Popularität

→ Gegenstand
- Keinen adäquaten Nutzwert

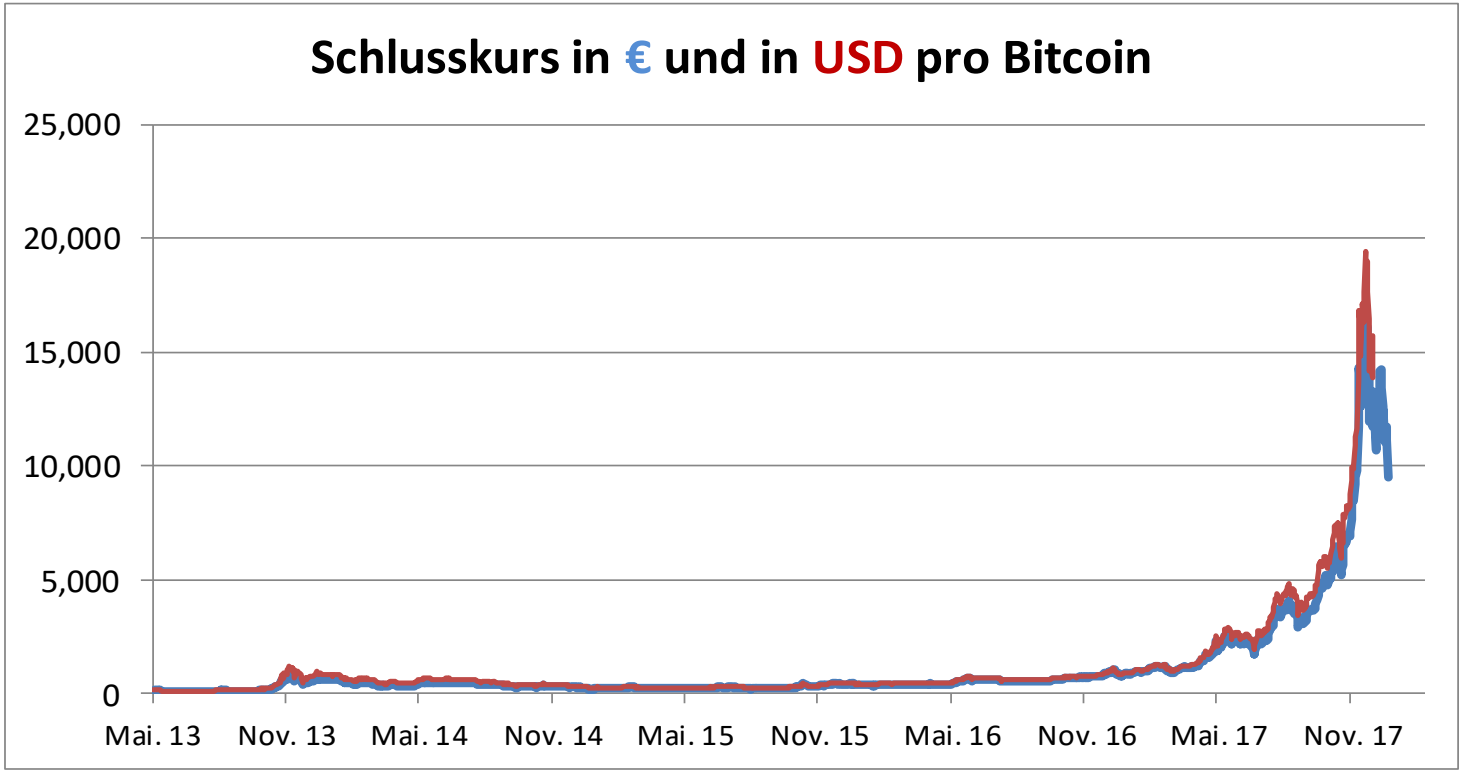
→ Trend
- Rational-ökonomische Basis
- Hypes als Begleiter von Trends

→ E-Commerce, E-Mail, etc.

Bitcoin – *das Ende der Inflation?*

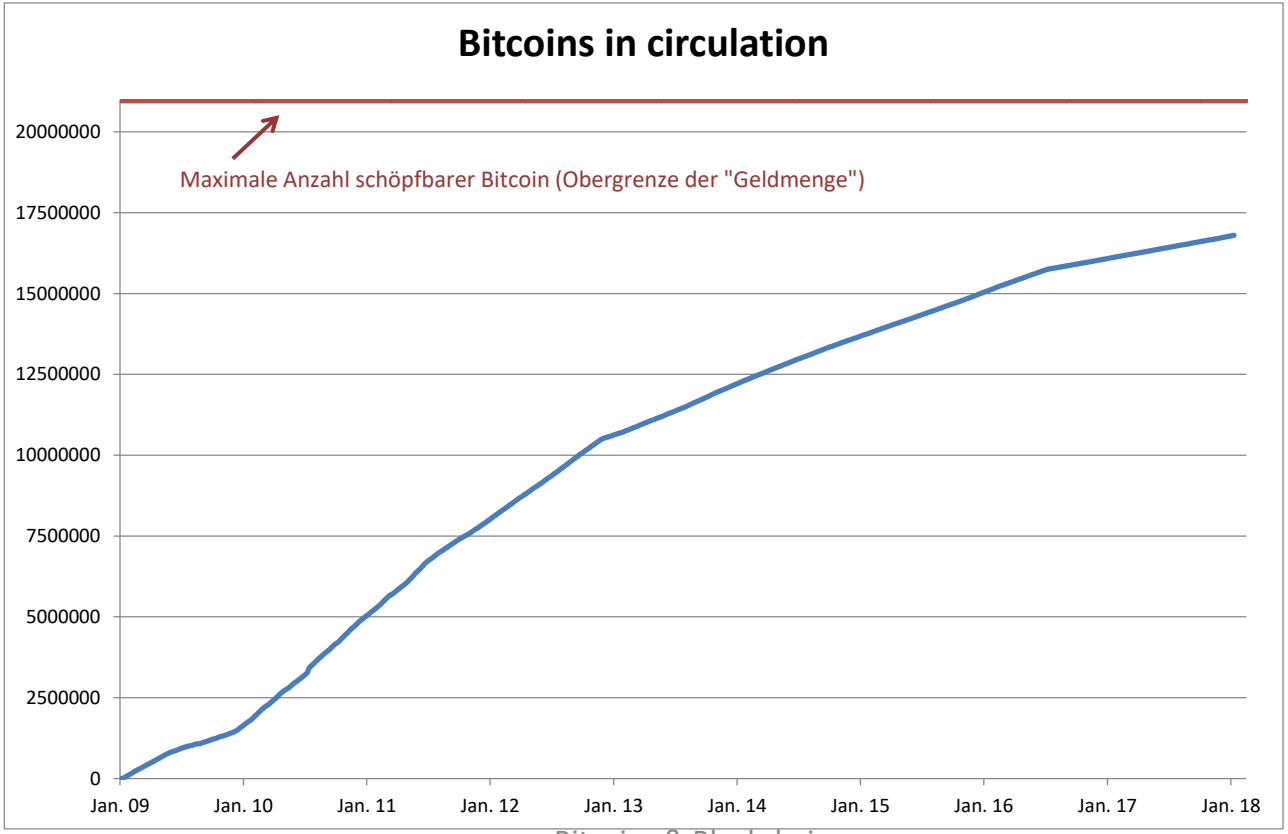
→ Bisher ja

- Für reale Gegenstände musste man in Bitcoin im Zeitablauf bisher immer weniger bezahlen.
- Wären Bitcoin Geld, wäre das eine massive Deflation.
- Wegen der hohen Volatilität des Kurses jedoch .
- Liegt fundamental an der Beschränkung der „Geldmenge“ auf 21 Millionen Bitcoin.
- Aber wer würde derzeit Bitcoin schon für Güterkäufe ausgeben (wenn man heute dafür einen Kleinwagen kaufen kann und in einem Jahr eine Yacht)?



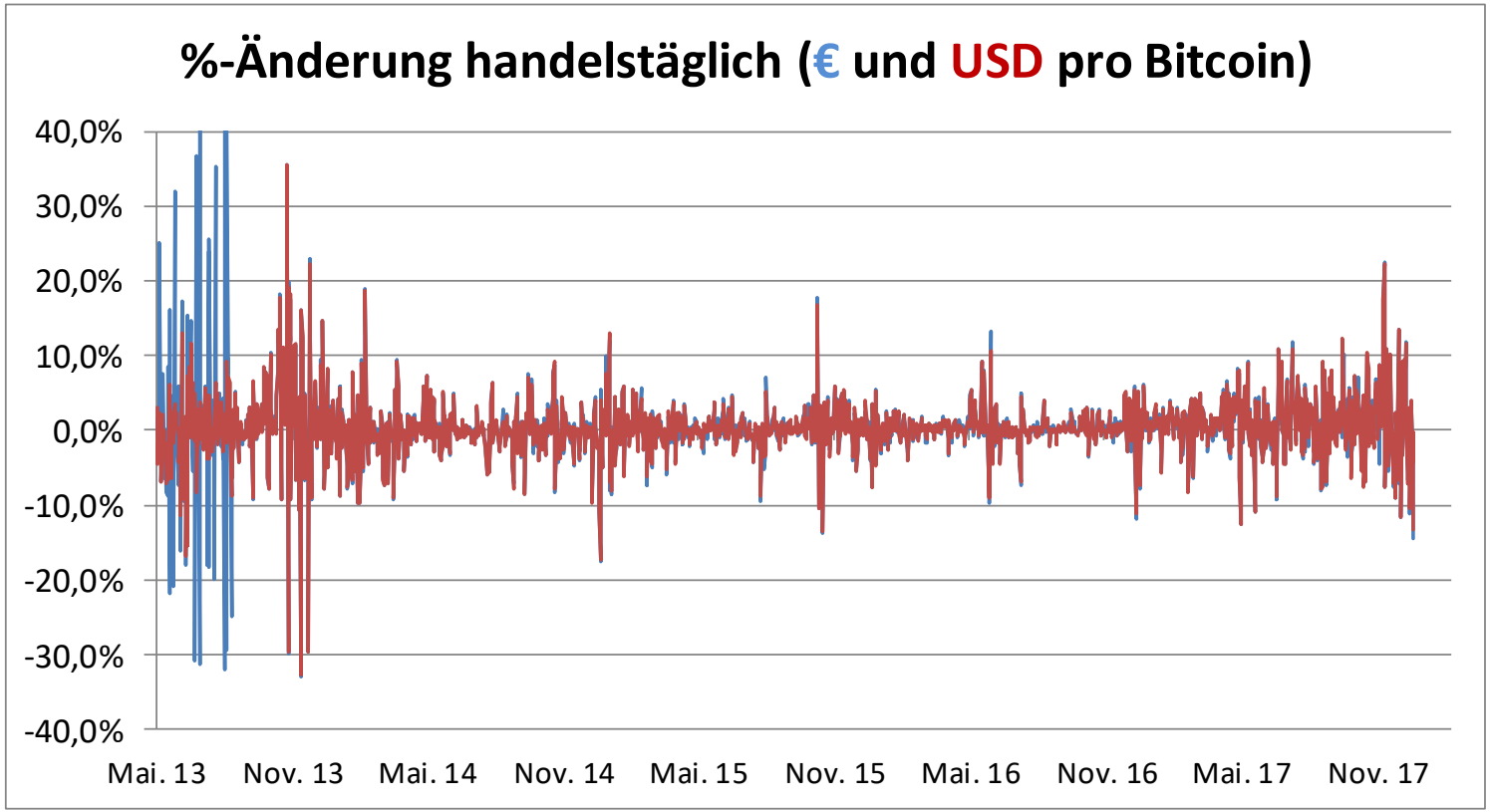
Haben wir das schon mal gesehen? Bsp. Telekomaktie

Bitcoin – Wie viele gibt es schon? (über 80%)



Das Mining neuer Blöcke wird von den Betreibern der Blockchain im Zeitablauf immer schwieriger gemacht, immer höhere Rechenleistungen und Energieverbräuche werden benötigt, um einen Block zu validieren.

Bitcoin – als Recheneinheit zu instabil



Bitcoin – *eine Spekulationsblase?*

- Spekulationsblasen liegen ökonomisch vor, wenn der Preis eines Vermögensgegenstandes für längere Zeit erheblich von einem fundamental gerechtfertigten Wert abweicht.
- Ein fundamentaler Wert ist für Bitcoin nicht erkennbar, noch nicht einmal historisch gibt es eine Beziehung zu realen Werten. Bitcoin „existieren“ nur in der Blockchain.
- Originär liegt der „Nutzwert“ der Bitcoin in ihrer Eignung für anonyme Transaktionen mit dem Charme der Anarchie (keine staatliche Regulierung)
- „Eine Blase zeigt sich erst, wenn sie platzt. Wir sehen eine rasante Wertentwicklung, die das Risiko rasanten Verlustes birgt.“ Aus einem Interview mit Carl-Ludwig Thiele, Mitglied des Vorstands der Deutschen Bundesbank, 23.12.2017

Beurteilung der Blockchain *bei Finanztransaktionen?*

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS
ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN
mainproject 2018

Datenschutz

- Identifizierbarkeit
- Vertraulichkeit
- Bezug zu realen Werten für virtuelle Blöcke, die außerhalb der Blockchain nicht existieren können

Volumen und Transaktions-geschwindigkeit

- Skalierbarkeit für hohe Transaktionsvolumina
- Konsensmechanismus
- Performanz und Speicher- und Rechenbedarf

Resilienz und Gültigkeit

- Differenzierte Lese-, Schreib- und Validierungsrechte
- Angriffsmöglichkeiten auf viele Knoten
- Finalität von Transaktionen nach Konsensmechanismus

Digitales „Geld“ *bisher ineffizient*

- *Existierende Krypto„währungen“ sind bisher weit weniger effizient als etablierte Zahlungssysteme. Die durchschnittlichen Kosten pro Transaktion mit Bitcoin werden in diesem Jahr bisher zwischen 100 und 135 USD ausgewiesen (das sind 1,05% bis 1,25% des Wertes der in einem Block zusammengefassten Transaktionen).*
- *Effizienzsteigerungen durch geänderte Konsensmechanismen sind möglich.*
- *Für alltägliche Zahlungen ist das System zu langsam. Bis zur Finalität durch Integration einer Zahlung (Transaktion) in die Blockchain vergingen im letzten Monat durchschnittlich 12 Minuten.*
- *Im Durchschnitt der bisherigen Handelstage dieses Jahres gab es 353000 Transaktionen in Bitcoin. (Visa Inc. etwa 445 Mio., Mastercard etwa 273 Mio., 75 Mio. im deutschen Zahlungsverkehr arbeitstäglich)*

Digitales „Geld“ *bisher ineffizient*

- *Die Kosten der Bitcoin Transaktionen bestehen aus der Vergütung der Miner, die neue Blöcke über den Konsensmechanismus mit einem proof-of-work validieren.*
- *Dieses Mining wird inzwischen mit optimierter Computer-Hardware kompetitiv betrieben, dennoch entstehen sehr hohe Kosten, überwiegend für die Hardwarekomponenten und den Energieeinsatz für Rechenleistung und Kühlung.*
- *Es gibt unterschiedliche Schätzungen für den Energiebedarf des Bitcoin-Netzwerks, die als Ausgangspunkt die Hash-Rate also die Anzahl der pro Sekunde erstellten Hashwertberechnungen haben. Aus der notwendigen Hashanzahl für die erstellten Blöcke und dem Energiebedarf der Maschinen pro Gigahash für Rechenleistung und Kühlung kann dann ein Jahresenergiebedarf derzeit zwischen 10 Terrawattstunden und 40 TWh ermittelt werden.*
- *Das wäre zwischen dem Energiebedarf von Uruguay und dem von Neuseeland, jedenfalls aber weniger als 0,7% des Jahresenergieverbrauchs der USA.*

Bitcoin - *Risiken*

- *Es gibt bereits mehr als 800 Krypto„währungs“-Systeme. Einige Gründungen erfolgen mit direkter Betrugsabsicht.*
- *Was passiert, wenn sich andere Währungen durchsetzen? Verliert die Bitcoin dramatisch an Wert relativ zum offiziellen Währungen.*
- *Risiko der Systemveränderung eine existierenden Blockchain (Bsp. Bitcoin Cash)*
- *Es bestehen Bedenken, dass über den anonymen peer-to-peer-Mechanismus einiger Krypto„währungs“ (Bitcoin) Steuerhinterziehung in größerem Umfang ermöglicht wird (Steueroasen).*

Blockchain und DTL – *das ist eine andere Sache*

- Generierung von privaten Zahlungsmitteln außerhalb von Zentralbanken (läuft massenhaft, 800 blochchain-basiert, andere ...).
- Schaffung von Blockchain-basiertem Zentralbankgeld
- Internationale Handelsfinanzierung bei nicht vertrauten Partnern
- Für Finanzmarkttransaktionen (Im Wertpapierhandel ein Experiment der Bundesbank mit der Deutsche Börse AG)
- Führung von Eigentümerverzeichnissen und Aufzeichnung von Transaktionen, wie z.B. Grundbücher und Immobilienkäufen. (Bsp. Honduras)
- …
- …

Vielen Dank
für Ihre Aufmerksamkeit

Fragen?

Kontakt

Prof. Dr. Georg Rainer Hofmann
06021-4206-700
georg-rainer.hofmann@h-ab.de

Dipl.-Bw. (FH) Meike Schumacher
06021-4206-746
meike.schumacher@h-ab.de

www.mainproject.eu
info@mainproject.eu