Krypto-Währungen und Blockchains

Münchner Finance Forum

18. September 2018

13:40 – 14:15

Excellence in Management Education

Professor Dr. Markus Rudolf
Allianz Endowed Chair of Finance
WHU – Otto Beisheim School of Management
Campus Vallendar: Burgplatz 2, 56179 Vallendar, Germany
Campus Düsseldorf: Erkrather Str. 224 a, 40233 Düsseldorf, Germany
www.whu.edu

References

Bitcoin Blocks:	https://blockchain.info
Ether Blocks:	https://etherscan.io
Hashing:	http://www.blockchain-basics.com/HashPuzzle.html
Geldautomaten:	https://coinatmradar.com/countries
Annahmestellen von Bitcoins:	http://coinmap.org/#/map/48.13534183/11.58298016/16

Blcokchain video on the WHU youtube channel: https://www.youtube.com/watch?v=UiviQx9h-w0

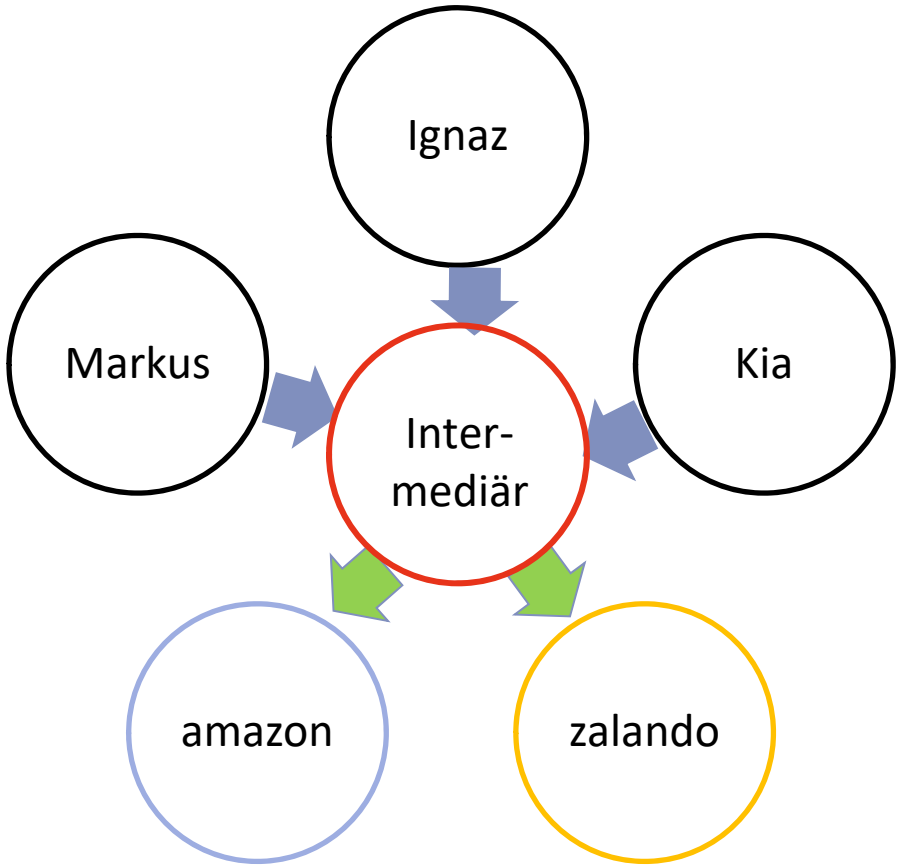
Kryptowährungen und Blockchains
Agenda

1) Zahlungssysteme
2) Blocks und Transaktionen
3) Proof-of-Work
4) Ether
5) Schlussbetrachtung

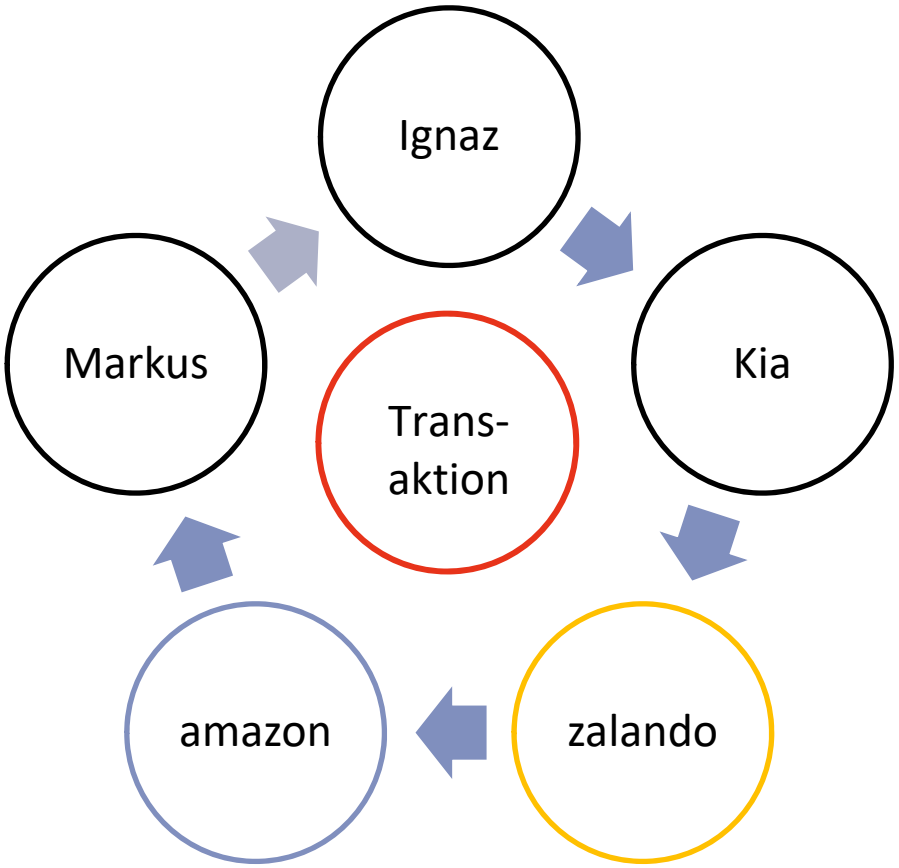
Hier werden die Grundlagen von digitalem Geld und der zugrunde liegenden Kryptografie aufgearbeitet. Wichtige Algorithmen und Konzepte erklären Verschlüsselungen mit Hash Keys und dem SHA-256 Standard, die die Basis für die Blockchain sind. Diese Konzepte werden für die Kryptowährungen Bitcoin und Ether dargestellt. Das Ziel dieses Moduls ist es Verständnis dafür zu erarbeiten, wie Krypto-Geld sichere und anonyme digitale Bargeld-Transaktionen ermöglicht. Es geht hier weniger um Anlageeigenschaften oder die Preisentwicklung auf den Kapitalmärkten von Kryptowährungen.

Zahlungssysteme

FIAT Geld basierend auf Intermediären



- Bei einer klassischen Zahlungstransaktion mit „Fiat“ Geld bezahlt Ignaz sein Guthaben an den Intermediär, der es dann an zalando weitergibt
- Intermediär: Kreditkartenfirma, Bank, PayPal, etc.
- Der Intermediär führt ein Handelsbuch in dem steht, welche Konten belastet bzw. erkannt werden müssen
- Bei einer Fiat Transaktion braucht man also 3 Parteien
- Bitcoins: Ein neuer peer-to-peer Ansatz ohne Intermediäre, Zahlungen zu organisieren



Satoshi Nakamoto (2008) – der Erfinder von Bitcoins als digitalem Zahlungsmittel:

- Problem bei peer-to-peer Netzwerken: Eine digitale Münze kann mehrmals ausgegeben werden (double spending problem)
- Lösung: Es gibt zwar keinen Intermediär, der die Gültigkeit der Transaktion bestätigt, sondern es gibt totale Transparenz, so dass jeder im Netzwerk sich davon überzeugen kann, dass die elektronische Münze bisher nicht ausgegeben wurde.

Zahlungssysteme

Die wichtigsten Kryptowährungen

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)
1	Bitcoin	$112.217.397.849	$6.499,38	$4.241.496.637	17.265.850 BTC	3,02%
2	Ethereum	$20.873.463.316	$204,77	$2.146.144.154	101.935.143 ETH	18,60%
3	XRP	$11.204.504.500	$0,282138	$317.183.899	39.712.852.387 XRP *	6,57%
4	Bitcoin Cash	$7.921.448.354	$456,67	$361.909.836	17.346.288 BCH	8,00%
5	EOS	$4.941.766.791	$5,45	$697.348.630	906.245.118 EOS *	12,55%
6	Stellar	$3.905.691.388	$0,207929	$73.868.442	18.783.812.627 XLM *	4,05%
7	Litecoin	$3.187.095.114	$54,69	$309.089.710	58.274.831 LTC	10,77%
8	Tether	$2.749.777.408	$0,997590	$2.881.070.811	2.756.421.736 USDT *	-0,43%
9	Monero	$1.864.931.161	$113,69	$44.890.661	16.403.140 XMR	12,30%
10	Cardano	$1.809.797.182	$0,069803	$88.282.670	25.927.070.538 ADA *	9,93%
11	Dash	$1.650.182.224	$198,38	$221.349.984	8.318.257 DASH	14,10%
12	IOTA	$1.629.071.692	$0,586096	$33.354.481	2.779.530.283 MIOTA *	10,47%
13	TRON	$1.321.802.733	$0,020104	$125.420.744	65.748.111.645 TRX *	14,32%
14	NEO	$1.189.491.406	$18,30	$61.870.605	65.000.000 NEO *	7,99%

Die Netzwerk-Zeitstempelung der Transaktionen erfolgt durch Hashing in eine fortlaufende Kette von Hash-basiertem Proof-of-Work (PoW) und bildet einen Eintrag, der nicht geändert werden kann, ohne den PoW zu wiederholen.

Quelle: https://coinmarketcap.com/, Daten vom 16. September 2018

Zahlungssysteme
Ethereum versus Bitcoin

- Ethereum basiert auf der Blockchain Technologie, ähnlich der zu Bitcoin
- Zentrales Element für beide ist der Proof of Work (PoW) Algorithmus
- Beide PoW Algorithmen basieren auf dem secure hash algorithm (SHA), der auf Guido Bertoni, Joan Daemen, Michaël Peeters und Gilles Van Assche (2013) unter dem Namen Keccak zurückgeht. Ihre Konzepte präsentierten sie auf der „Annual International Conference on the Theory and Applications of Cryptographic Techniques“
- https://github.com/ethereum/wiki/wiki/Ethash: Während Bitcoin SHA1 verwendet, nutzt Ether das Ethash Mining Verfahren. Ethash verwendet den Keccak hash, der zu einem SHA3 Standard entwickelt wird. SHA3 basiert auf einem 1 GB großen Datenset. Hierbei werden Daten von beliebiger Länge in einen Datensatz von fester Länge umgewandelt. Dieser Datensatz wird alle 30.000 Blocks regeneriert. Folglich muss nicht jeder Block neu berechnet werden. Es ist eher so, dass Miner den bereits erzeugten Datensatz betrachten. Sie suchen Nonces, die helfen können das Hash-Puzzle zu lösen.
- Folge: Ether Mining ist schneller und verbraucht weniger Energie als Bitcoins

Blocks und Transaktionen
Bitcoin Blocks

- https://www.blockchain.com/de/explorer
- Ein Bitcoin Konto kann als ein Zustandsübergangssystem betrachtet werden, wo es einen "Zustand" gibt, der aus dem Besitzstatus aller existierenden Bitcoins und einer "Zustandsübergangsfunktion" besteht, die einen Zustand und eine Transaktion annimmt und einen neuen Zustand ausgibt.
- Bestandteile einer Bitcoin Transaktion
  - Bezug zu einem UTXO (nicht ausgegebene Bitcoin)
  - Unterschrift des Eigentümers
  - Neue UTXO's
- Bestandteile eines Bitcoin Blocks
  - Zeitstempel (timestamp)
  - Nonce
  - Hash des vorangehenden Blocks
  - Übersicht aller Transaktionen seit des letzten Blocks

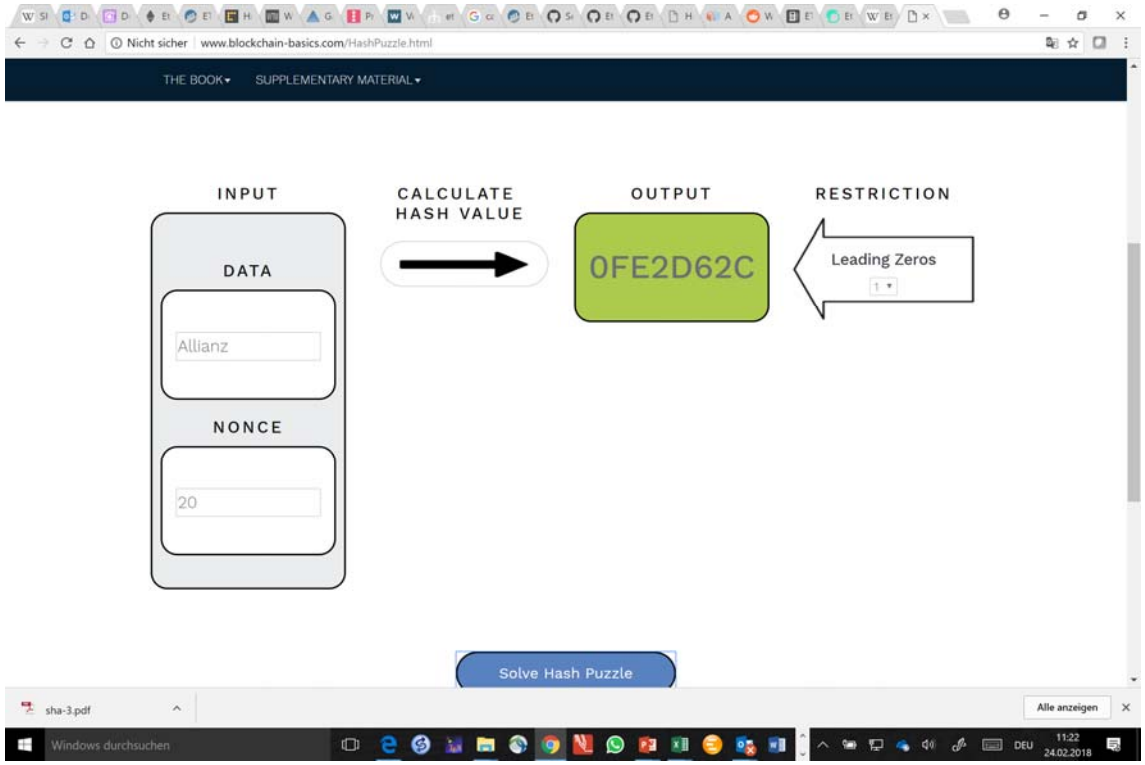
Quelle: Buterin (2013)

Blocks und Transaktionen
Ether Blocks

- https://etherscan.io
- Bestandteil eines Ether Kontos
  - Nonce
  - Balance des Ether Kontos
  - Programmierungscode des Kontos und falls vorhanden: externes Eigentum oder Vertragskonten
  - Archivierung des Kontos
- Bestandteil einer Ether Transaktion
  - Empfänger
  - Unterschrift
  - Menge des zu sendendem Ether
  - Zu sendende Daten
  - STARTGAS
  - GASPRICE

Quelle: Buterin (2013)

Proof-of-Work
(Cryptologische) Hash Funktion



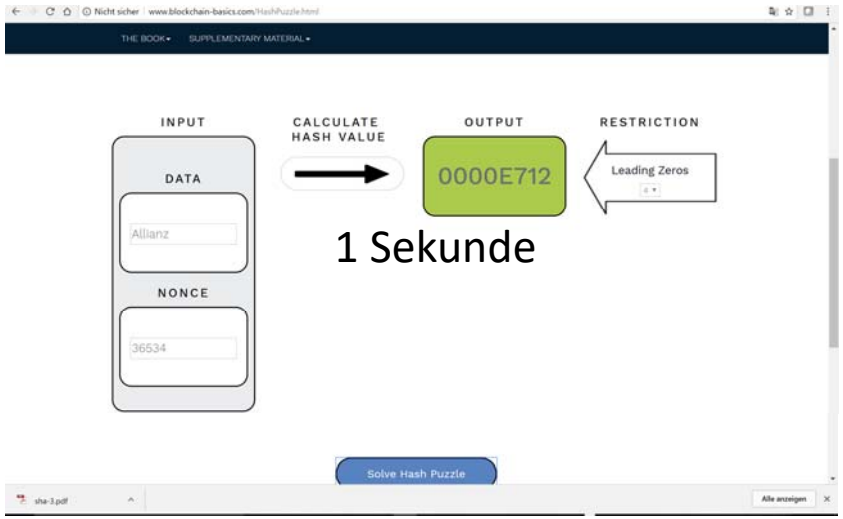
- Die Eingabe "Allianz" wird in eine 8-stellige Hexadezimalzahl umgewandelt
- Unter SHA-256 hat die Ausgabezeichenfolge 64 Hexadezimalziffern, d. H. 256 Binärziffern
- Bei keiner führenden Nullstelle beträgt die Rechenzeit zur Identifizierung der Nonce << 1 Sekunde

- Ein Pseudocode zum Erzeugen eines SHA1-256 Hashwertes kann unter https://de.wikipedia.org/wiki/Secure_Hash_Algorithm gefunden werden

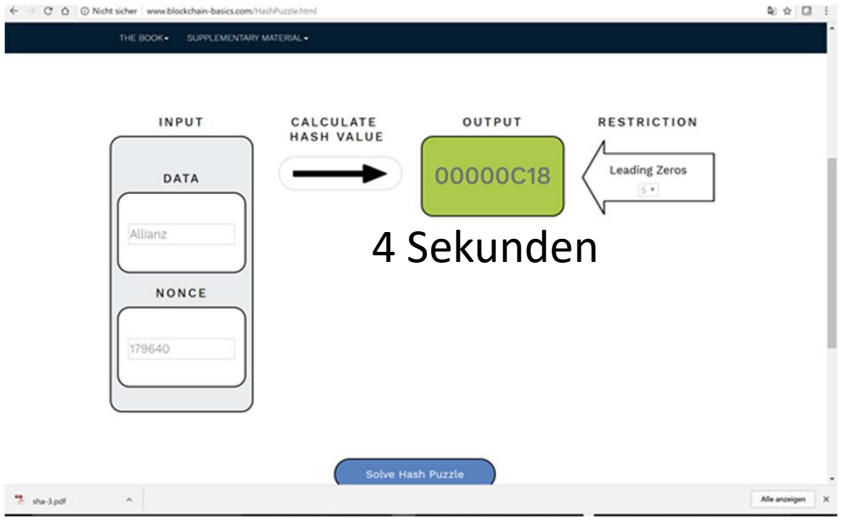
Quelle: http://www.blockchain-basics.com/HashPuzzle.html

Proof-of-Work

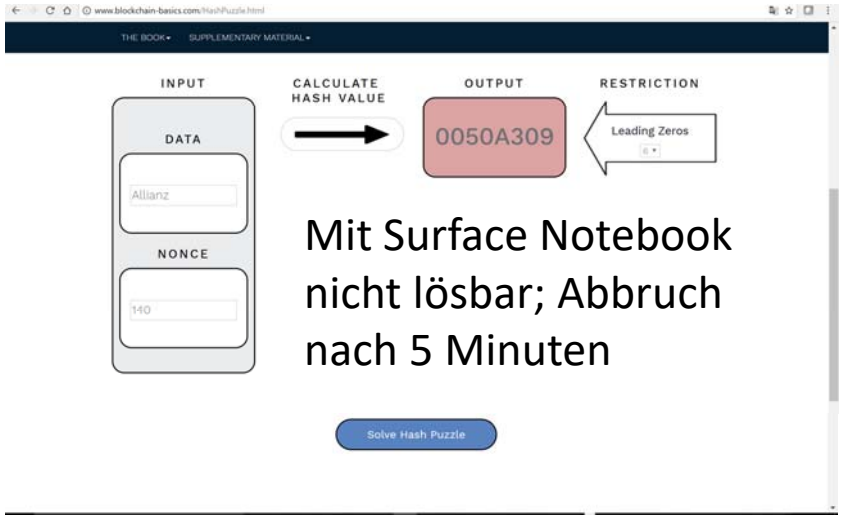
SHA 32 – Beispiele



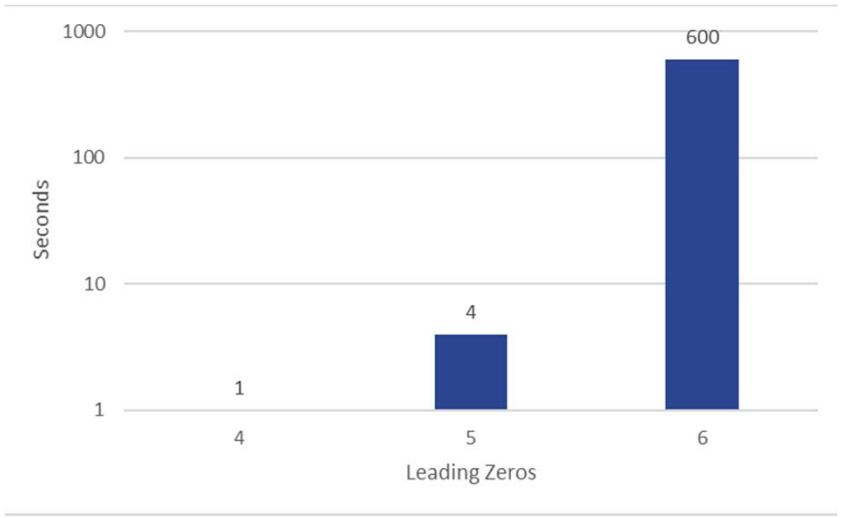
1 Sekunde



4 Sekunden

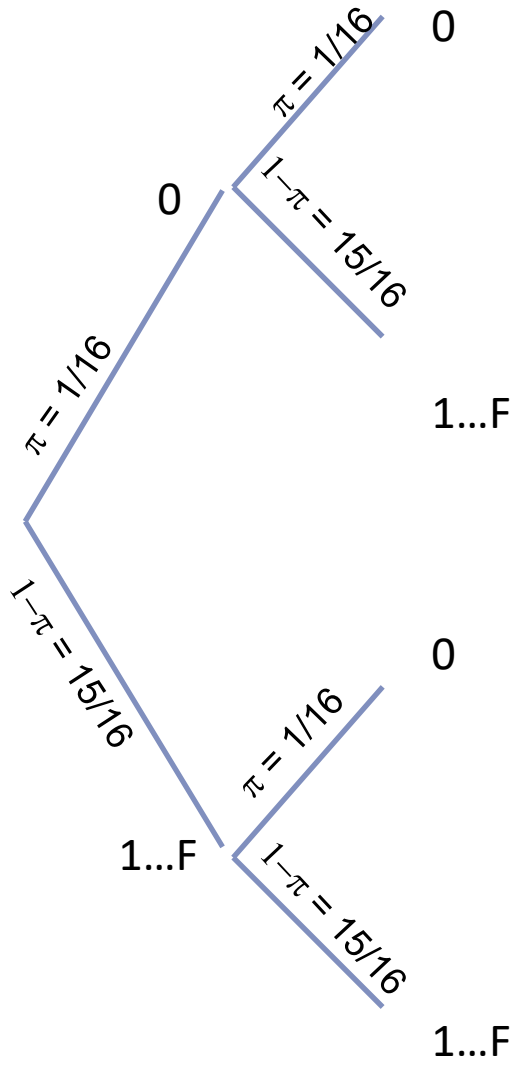


Mit Surface Notebook nicht lösbar; Abbruch nach 5 Minuten



Proof-of-Work

Bitcoin: Schwierigkeit bei 18 führenden Nullwerten in SHA1-256



Puzzle: Berechne die Zeit, um den Hash mit 18 führenden Nullen zu finden

- Baumdiagramm repräsentiert die ersten 2 von 64 Schritten, um den Hash Key des Blocks zu bestimmen
- Die Wahrscheinlichkeit 18 führende Nullstellen zu finden beträgt $1/16^{18} = 2{,}1 \cdot 10^{-22}$
- Ein Computernetzwerk kann $6{,}5 \cdot 10^{18}$ Hashes pro Sekunde rechnen (siehe https://blockchain.info)
- Die Rechenzeit, um einen Hash mit 18 führenden Nullstellen zu finden, beträgt:

  $2{,}1 \cdot 10^{-22} * 6{,}5 * 10^{18} = 0{,}825$

  = 734 Sekunden = 12,2 Minuten
- Wenn CPUs sich weiterentwickeln und schneller werden, könnten 19 führende Nullstellen für den Hash benötigt werden

Proof-of-Work

Ethash: Ether Dauer bis das SHA3-256 Puzzle gelöst ist

- Das Ethash Mining Verfahren basiert auf einem 1 GB Datensatz
- Der Datensatz wird alle 30.000 Blocks aktualisiert
- Daher muss nicht für jeden Block alles neu berechnet werden. Vielmehr müssen Miner durch den bereits generierten Datensatz gehen. Sie versuchen Nonces zu finden, die das Hash-Puzzle lösen

GB	MB	KB	Byte	Bit
1	1.000	1.000.000	1.000.000.000	8.000.000.000

Anmerkung:
in Dezimalpräfix

- Jeder Hash umfasst 256 bit = 32 byte

Hashes under SHA 256	3.906.250.000
Access time to hard disk in seconds: 10 milli seconds per hash	39.062.500
Access time to RAM in seconds: 60 nano seconds per hash	234,4
Access time to CPU Cache in seconds: 3 nano seconds per hash	11,7

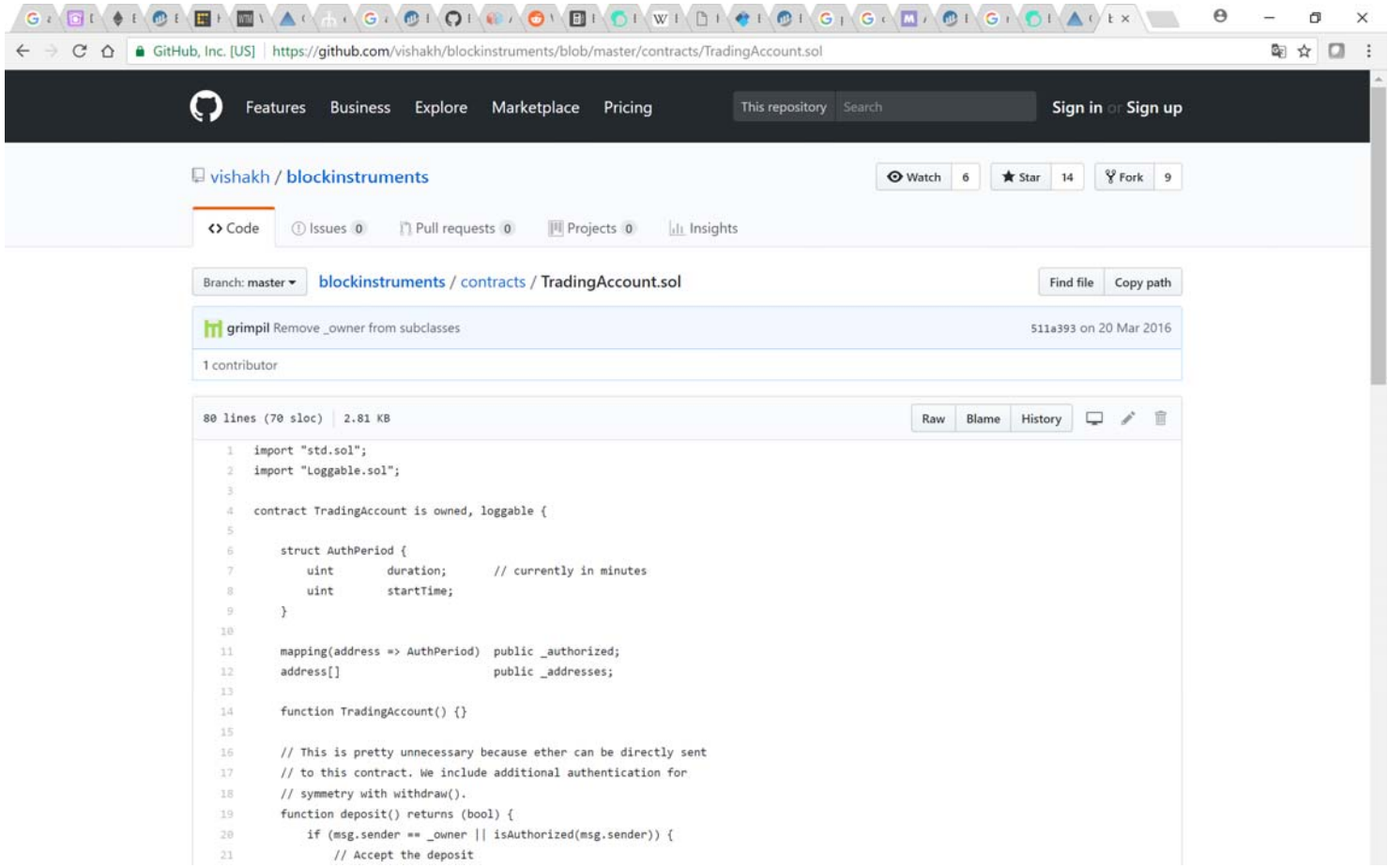
- Beweis: Im Gegensatz zum PoW, bei dem es teuer ist den nächsten Block zu erstellen, „bestraft“ der PoS Miner, die den falschen Block unterstützen, indem sie eine Einlage von ihrem Konto abziehen

Ether
Smart Contracts

- Ether ist eine Blockchain mit einer eingebauten Programmiersprache - Bitcoin basiert "nur" auf einem Skriptsystem
- Aber Ether kann auch für ICOs verwendet werden
- Programmiersprachen können Solidity, Serpent, Go, C ++, Python, Java, Javascript, Ruby usw. sein. Sie sind "Turing-complete", d.h. sie ermöglichen Schleifen
- Jeder kann eine intelligente Anwendung schreiben
- Da der Code (Computer-)Raum und (Computer-)Zeit benötigt, muss die Verwendung von Daten in GAS bezahlt werden
- GAS-Preise können von Transaktionsgesellschaften als marktorientierten Anreiz für die Bestätigung von Transaktionen durch Miner festgelegt werden
- Das verwendete GAS hängt von der CPU-Nutzung des Smart-Vertrags ab
- Ether ist eine Plattform, die nicht zu Zahlungszwecken dient. Das am häufigsten verwendete Token auf der Ether-Plattform heißt Ether
- Ether als Konzept für: Escrow-Dienste, P2P-Marktplätze, soziale Netzwerke, Börsen für Derivate, Währungen oder Aktien, Ether Wallets, Notar-Dienstleistungen, etc.

Ether

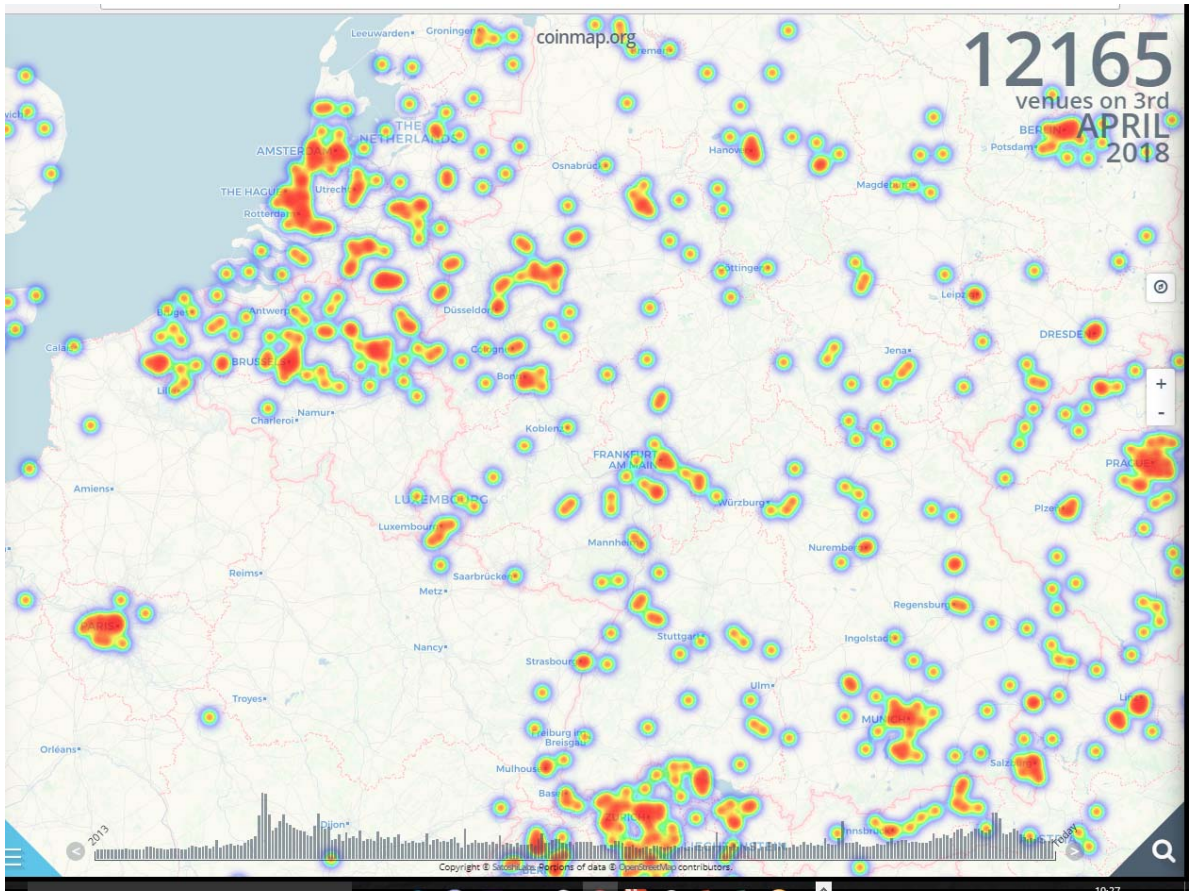
Smart Contracts – Programmierungs-Code für Trading Konto



C++ code

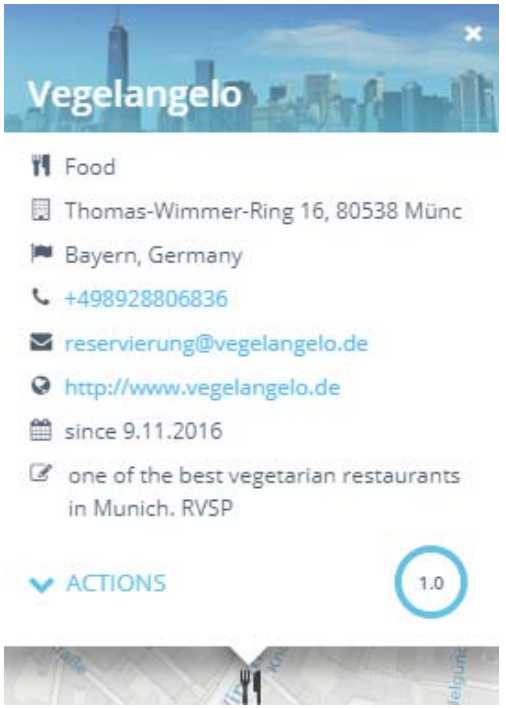
Quelle: https://github.com/vishakh/blockinstruments/blob/master/contracts/TradingAccount.sol

Schlussbetrachtungen
Bitcoin Ausgaben



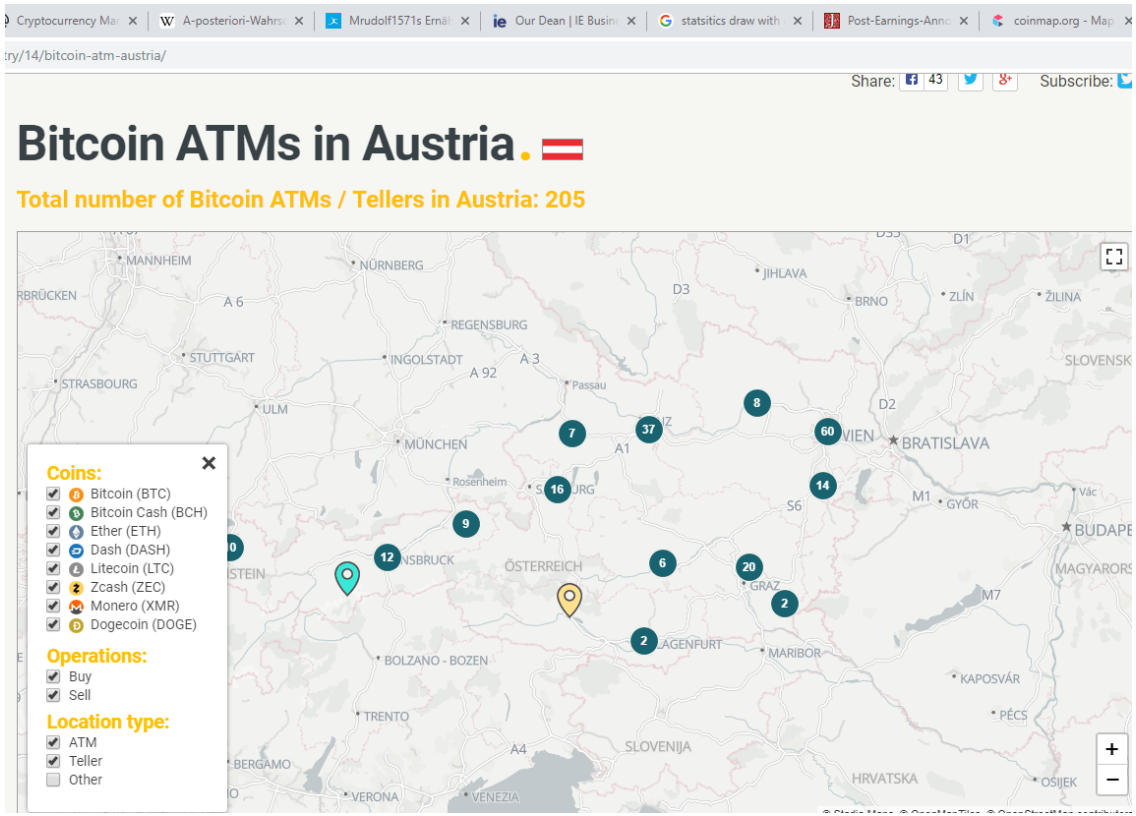
München:
13 Einzelhändler, die Bitcoins akzeptieren

Beispiel:



Quelle: coinmap.org

Schlussbetrachtungen
Crypto Geldautomaten



- Es gibt keine Crypto Coin ATMs in Deutschland
- Aber es gibt 205 in Österreich

Quelle: https://coinatmradar.com/countries/

Schlussbetrachtungen

- Bitcoins: 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.
- Das Angebot an Bitcoin Münzen ist auf 21.000.000 begrenzt, weil pro geschürftem Block degressiv viele Bitcoins ausgezahlt werden
- “Blockchain technology" typically refers to the transparent, trustless, publicly accessible ledger that allows us to securely transfer the ownership of units of value using public key encryption and proof-of-work methods
- Electricity consumption of Bitcoins is huge
- Ether allows for smart contracts and is therefore much more flexible than Bitcoins
- Das Angebot an Ether Münzen wächst linear mit 3 Ether pro Block
- Ethereum is a blockchain app platform on www.ethereum.org on which you can built unstoppable applications
- Ether nodes: https://www.ethernodes.org/network/1 and bitcoin nodes: https://bitnodes.21.co/