Zwischen Hype und Realität

–

Anwendung und Zukunft der Blockchain Technologie
ETOCS 2018

Benjamin Leiding

Georg-August-Universität Göttingen
Lehrstuhl für Telematik

benjamin.leiding@cs.uni-goettingen.de

31.05.2018

About Me

Akademische Laufbahn

- Gescheiterter "Banking and Finance" Student (Zürich)
- B.Sc. Informatik (Rostock, Dundee)
- M.Sc. Internet Technologies and Information Systems (Göttingen)
- Promotionsstudent (Göttingen)
- Forschungsgebiete:
  - (Self-Sovereign) identity systems und dezentrale Autorisierungsprotokolle $\rightarrow$ Authcoin.
  - Anwendungen auf Basis von Blockchains, z.Bsp., Akademisches Peer-Review, Machine-to-Machine Economy, Autonome Autos, usw.

About Me

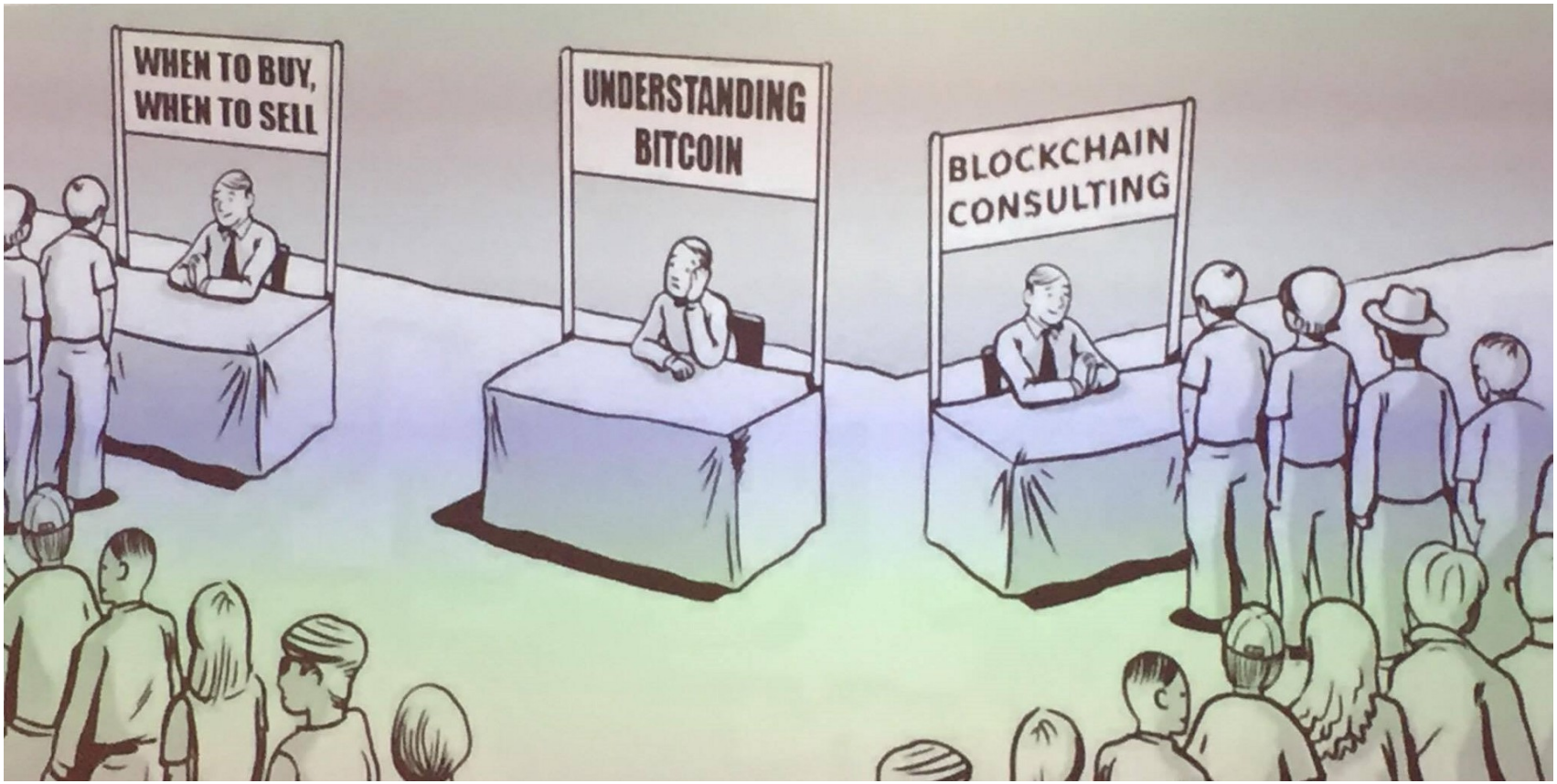
Entrepreneurship

- Gründer von Chaindrium
- Chief Scientist und Co-Founder in weiteren Start-Ups
- IT Consultant, (ICO) Advisor, etc.

Überblick

Einführung

Eine Mystische Welt



Quelle: `https://goo.gl/MYT7Uf`

Geschichte

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.

Figure: Das ursprüngliche Bitcoin Whitepaper (Quelle: [1])

Bitcoin Grundlagen

Bitcoin $\neq$ Blockchain

Was macht Bitcoin so besonders?

- Dezentrale, digitale Währung $\rightarrow$ Keine Zentralbank, keine Regierung
- Kein (vertrauenswürdiger) Dritter nötig, der Transaktionen validiert im Gegensatz zum Bankensystem, Papypal oder Western Union
- Bitcoins können transferiert aber nicht dupliziert werden
- Transparenz
- Pseudonym, aber nicht anonym!
- Deflationär (max. 21 Millionen Coins)

Blockchain Technologie

Überblick

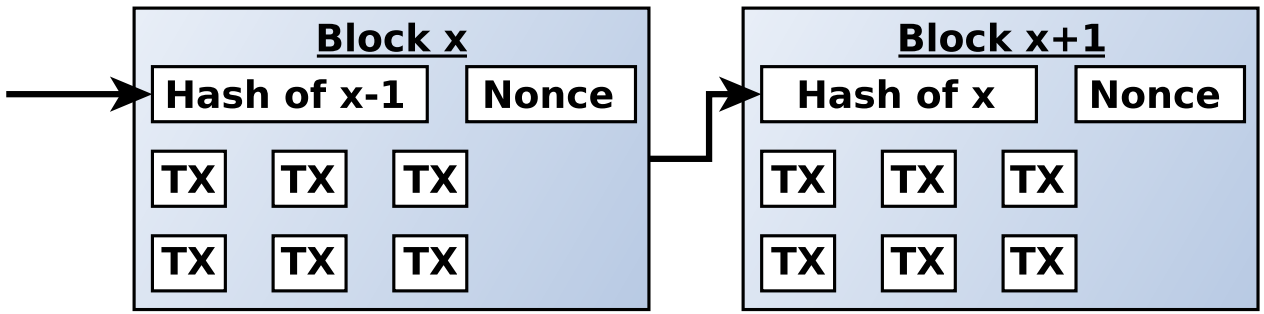
Die grundlegenden Konzepte sind nicht sonderlich revolutionär, alle waren seit Jahren bekannt. **ABER** die Kombination der einzelnen Teilkonzepte war ein revolutionäre Idee.

Im Grunde ist eine Blockchain ein:

- verteiltes,
- sicheres,
- Logfile.

Blockchain = Distributed Transaction Ledger (Hauptbuch)

- Eine sequentielle Append-only Datenstruktur (Liste)
- Neue Blöcke können nur am Ende der Liste (Kette) angehängt werden
- Blocks werden aneinander gekettet $\rightarrow$ Blockchain
- Manipulation eines Blocks erfordert die Neuberechnung aller nachfolgenden Blöcke
- Alle Informationen sind redundant verfügbar über ein P2P Netzwerk



$\Rightarrow$ Aber wie erreiche ich einen Konsens darüber, welche Daten (Transaktionen) im nächsten Block gespeichert werden?

Konsens in Netzwerken

- Einen globalen Konsens zwischen einer größeren Anzahl an Teilnehmern zu erreichen ist schwierig
- Noch schwieriger ist es, wenn einige der Teilnehmer sich nicht an die Regeln halten (Byzantine General Problem)
- Im Blockchain Umfeld haben sich verschiedene Konsens Algorithmen etabliert, z.Bsp.:
  - Proof-of-Work (Bitcoin und viele andere)
  - Proof-of-Stake/Luck/Activity/etc.
  - Algorand
  - IOTA's gerichteten azyklischer Graph (engl. diredirected acyclic graph - DAG), auch Tangle genannt

Dezentrale Anwendungen (DApps)

	Neblio	Nuls	Lamden	NEO	Waves	Lisk	EOS	QTUM	ICON
PROGRAMMING LANGUAGE (SUPPORT)	Python, JavaScript, Go, Ruby, Obj C, Java, C#, PHP	Java	Python	Python, Javascript, VB.NET, Java, C#, F#, Golang, Kotlin C++	Scala	JavaScript, TypeScript	C, C++, WebAssembly	Solidity	Python
PROTOCOL	PoS	PoC	DPoS + BFT	dBFT	LPoS	DPoS	DPoS	PoS	LFT
BLOCK TIME (SEC)	120	10	1	15-20	3	10	0.5	120	1
QUICK SYNC	✓	✗	CDNR *	✓	CDNR *	CDNR *	CDNR *	✗	✓
ATOMIC SWAPS	✓	✓	✓	✓	✓	✗	✗	✗	✓
TOKEN LAUNCH COST	10 NEBL	N/A	N/A	500 GAS	1 WAVES	Dynamic	N/A	N/A	N/A
MASTERNODES	✗	✓	✓	✗	✗	✗	✗	✗	✗
SIDECHAINS	✓	✓	✗	✓	✗	✓	✗	✓	✓
PRIVATE CHAINS	✓	✓	✓	✓	✓	✓	✗	✓	✓
MAINNET LAUNCH DATE	Jul 2017	May 2018	Q3 2018	Oct 2016	Jun 2016	Q2 2016	Jun 2018	Oct 2017	Jan 2018
DEC* TOKEN CREATION	✓	✓	✓	✗	✓	✓	✓	✓	N/A
TRANSACTION COST	0.0001 NEBL	0.01 NULS	Free	Free	0.001 WAVES	0.1 LSK	Free	0.004 QTUM	0.01 ICX
WALLETS	Desktop(Win, Mac, Linux), Android, Docker, Electrum, Pi, Orion Web	ERC20	ERC20	Windows, MacOS, Linux, Ledger	Windows, MacOS, Linux	Web, Windows, MacOS, Linux	ERC20	Web, Ledger Desktop(Win, Mac), Android/iOS,	Web

Quelle: `https://image-store.slidesharecdn.com/a02e16ef-100a-4d95-8488-38cb913d10a7-original.jpeg`

Smart Contracts

- Bitcoin hat eine sehr limitierte Script Sprache zum verarbeiten von Transaktionen → Smart Contracts können viel mehr
- Turing-vollständige Programmiersprachen (z.Bsp., Solidity)
- Smart Contract:
  - Contract code wird zu Bytecode für die Ethereum virtual machine (EVM) kompiliert
  - Ausführung des Codes benötigt eine Gebühr (tokens)
  - Autonome Ausführung des Codes
  - Jeder Node, führt jeden Contract aus (deterministisch)
  - Contracts können miteinander, oder sogar mit der äußeren Welt durch sogenannte "oracles" kommunizieren
- Smart Contract fähige Blockchains → Ethereum, Qtum, etc.
- Sind Smart Contracts die nächste Evolutionsstufe des Internets?

Dezentrale Anwendungen

Beispiele:

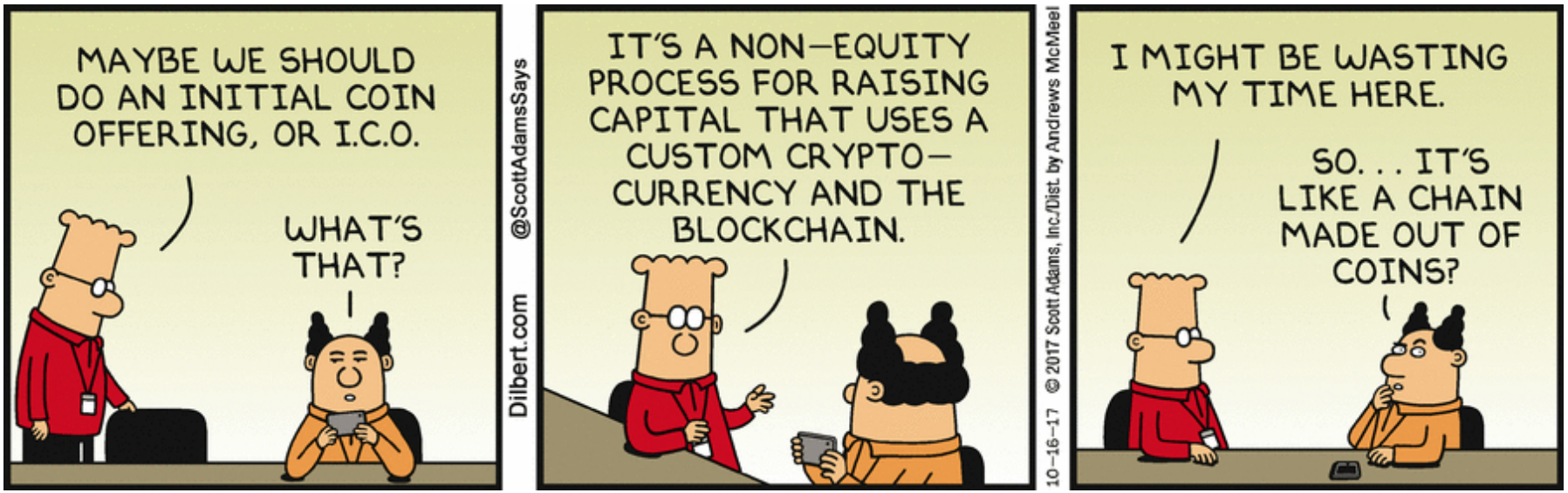
- Finanzdienstleistungen, e-Voting, etc.
- Verteilte PKIs
- Manipulationssichere Logfiles und Zeitstempel
- Zugangsberechtigungssystem
- Diffie-Hellman über die Blockchain
- Identitäts- und Autorisierungslösungen
- etc.

▸ Hier eine Auflistung von Ethereum-basierten DApps.

Initial Coin Offerings - ICOs

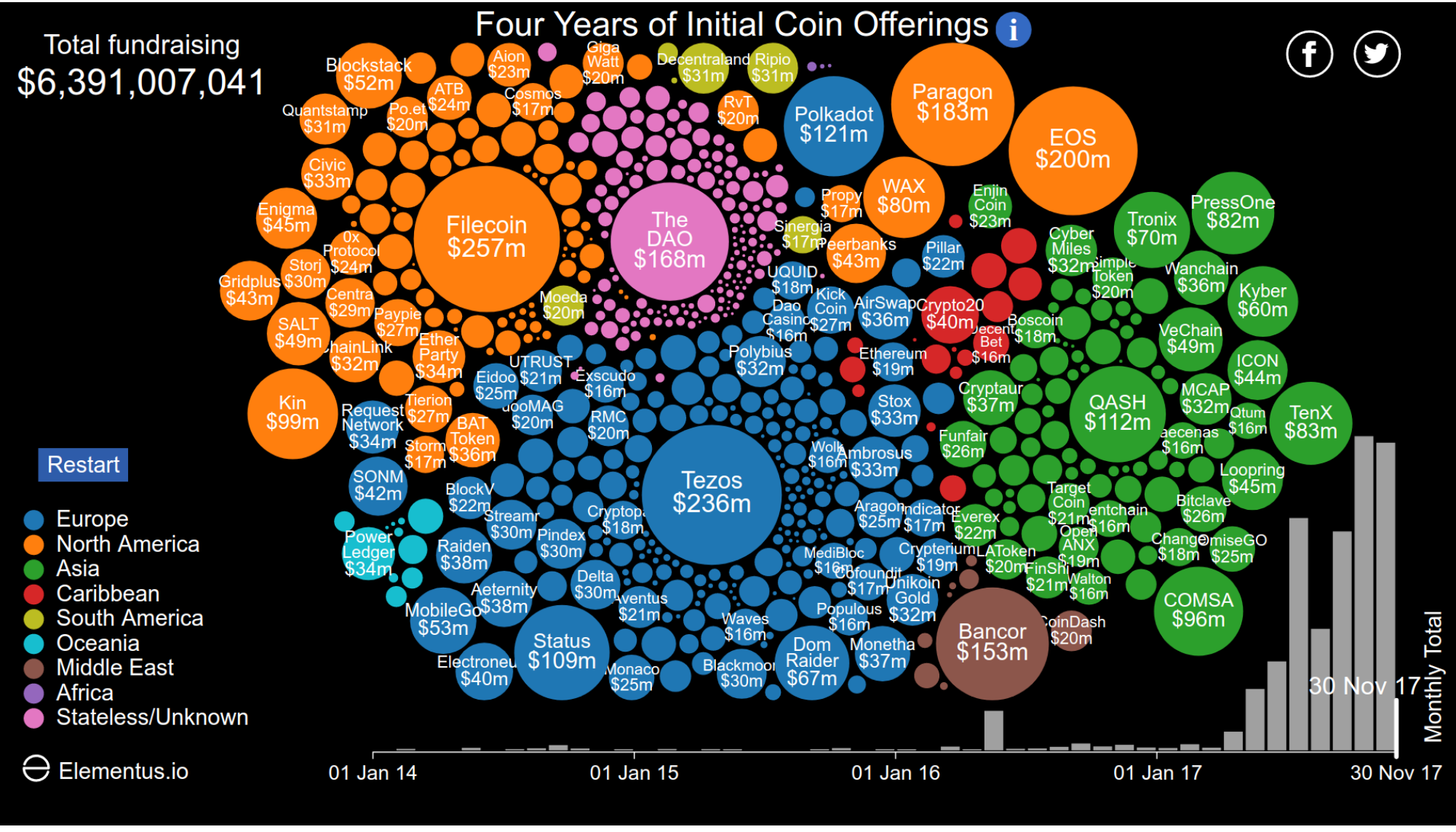
Initial Coin Offerings (ICOs)

- ICO = Börsengang auf Basis einer Blockchain.
- Finanzierung der Entwicklung einer Blockchain Idee → Finanzmittel im Austausch für Tokens.
- Produkt, Team, Marketing, Social Media, Whitepaper, Roadshows, Investoren, ...



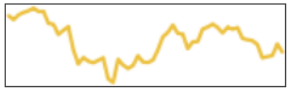
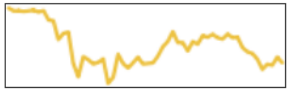
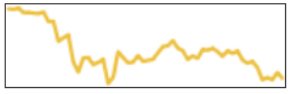
Quelle: `http://dilbert.com/strip/2017-10-16`

Initial Coin Offerings (ICOs)



Quelle: `https://elementus.io/token-sales-history`

Initial Coin Offerings (ICOs)

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$142,064,904,452	$8,338.58	$6,958,700,000	17,037,062 BTC	-2.94%	
2	Ethereum	$69,758,655,812	$701.28	$2,605,040,000	99,472,903 ETH	-2.88%	
3	Ripple	$27,142,697,673	$0.692593	$464,678,000	39,189,968,239 XRP *	-4.35%	
4	Bitcoin Cash	$22,029,625,524	$1,285.95	$1,034,780,000	17,131,013 BCH	-7.94%	
5	EOS	$10,678,247,769	$12.43	$1,816,310,000	858,973,870 EOS *	-8.98%	
6	Litecoin	$7,800,284,512	$137.92	$374,555,000	56,558,638 LTC	-2.56%	
7	Cardano	$6,459,522,208	$0.249142	$117,485,000	25,927,070,538 ADA *	-6.87%	
8	Stellar	$6,142,224,314	$0.330639	$46,665,000	18,576,829,453 XLM *	-8.30%	
9	IOTA	$5,177,986,964	$1.86	$88,264,700	2,779,530,283 MIOTA *	-6.20%	
10	TRON	$4,546,107,156	$0.069144	$429,154,000	65,748,111,645 TRX *	-1.51%	

Quelle: `https://coinmarketcap.com/` (16.05.2018)

Brauche ich überhaupt eine Blockchain?

Brauche ich eine Blockchain?

Burger King launches WhopperCoin crypto-cash in Russia

29 August 2017 Share

Customers will be able to claim coins as they scan receipts for meals at the fast-food chain

Quelle: `http://www.bbc.com/news/technology-41082388`

Brauche ich eine Blockchain?

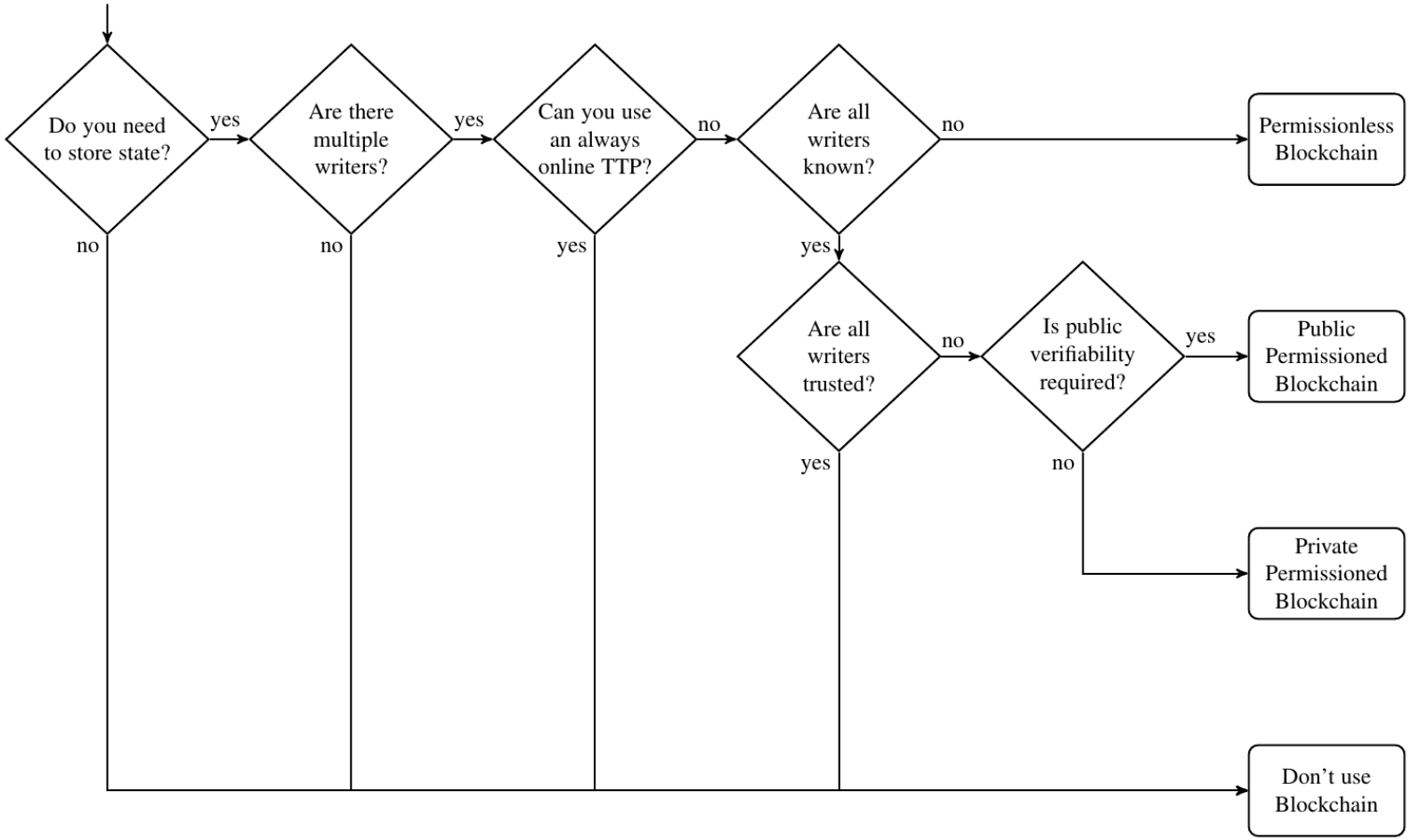


Figure: Brauche ich eine Blockchain? (Quelle: [2])

Die Zukunft von Blockchains

Zukunft

Beispiel Visionen

- Sharing Economy
- M2M Economy und das Internet der Dinge (IoT)
- Autonome, virtuelle Organisationen und Kollaborationen (Industrie 5.0?)
- Universelles Zahlungssystem
- Medizinische Daten (z.Bsp. Patientenakten, usw.)

"#InternetOfThings is when your toaster mines bitcoins to pay off its gambling debts to the fridge"
(Quelle: Das Internet)

Herausforderungen für die Zukunft

- Energiekonsum einiger Konsens-Algorithmen (Proof-of-Work)
- Fehlende Standardisierung der Plattformen
- Skalierbarkeit
- Regulierung
- Entwickler-Tools
- Entwickler
- Einfache Bedienbarkeit für den End-User
- Aufklärung und Bildungsarbeit

Fazit

Fazit

Take Home Message

- Bitcoin $\neq$ Blockchain
- Blockchains können diverse Probleme in dezentralen Systemen mit nicht-vertrauenswürdigen Dritten lösen
- Smart-Contracts als dezentrale Agenten und Anwendungen auf der Blockchain (Grundlage für Interaktionen und Transaktionen)
- **Aber:**
  - Blockchains sind kein Allheilmittel
  - Viele offene Fragen und ungelöste technische Probleme
  - Fehlende Standards und Regulierungen

Fragen?

Bibliography I


S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," URL: https://bitcoin.org/bitcoin.pdf, 2008, (Accessed December 20, 2017).


K. Wüst and A. Gervais, "Do you need a Blockchain?" IACR Cryptology ePrint Archive, vol. 2017, p. 375, 2017.