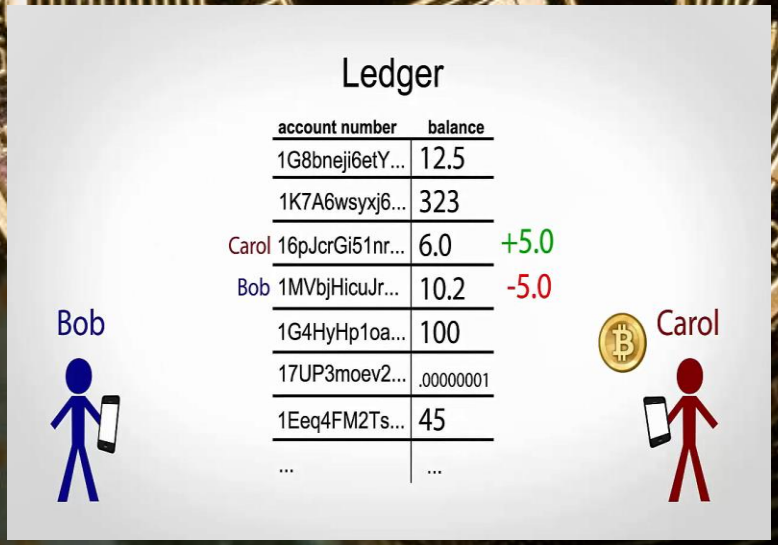
3 Protect Data

- Protecting the Security & Integrity of Data

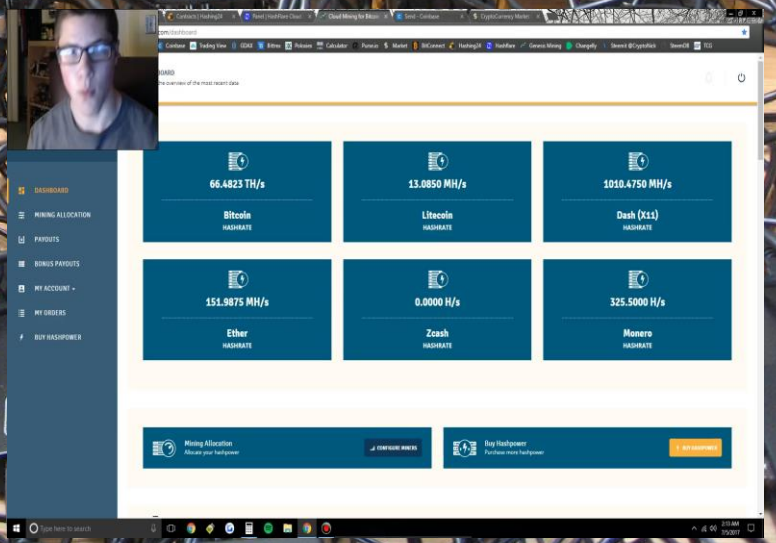
(3) **Bitcoin Crypto Currency**



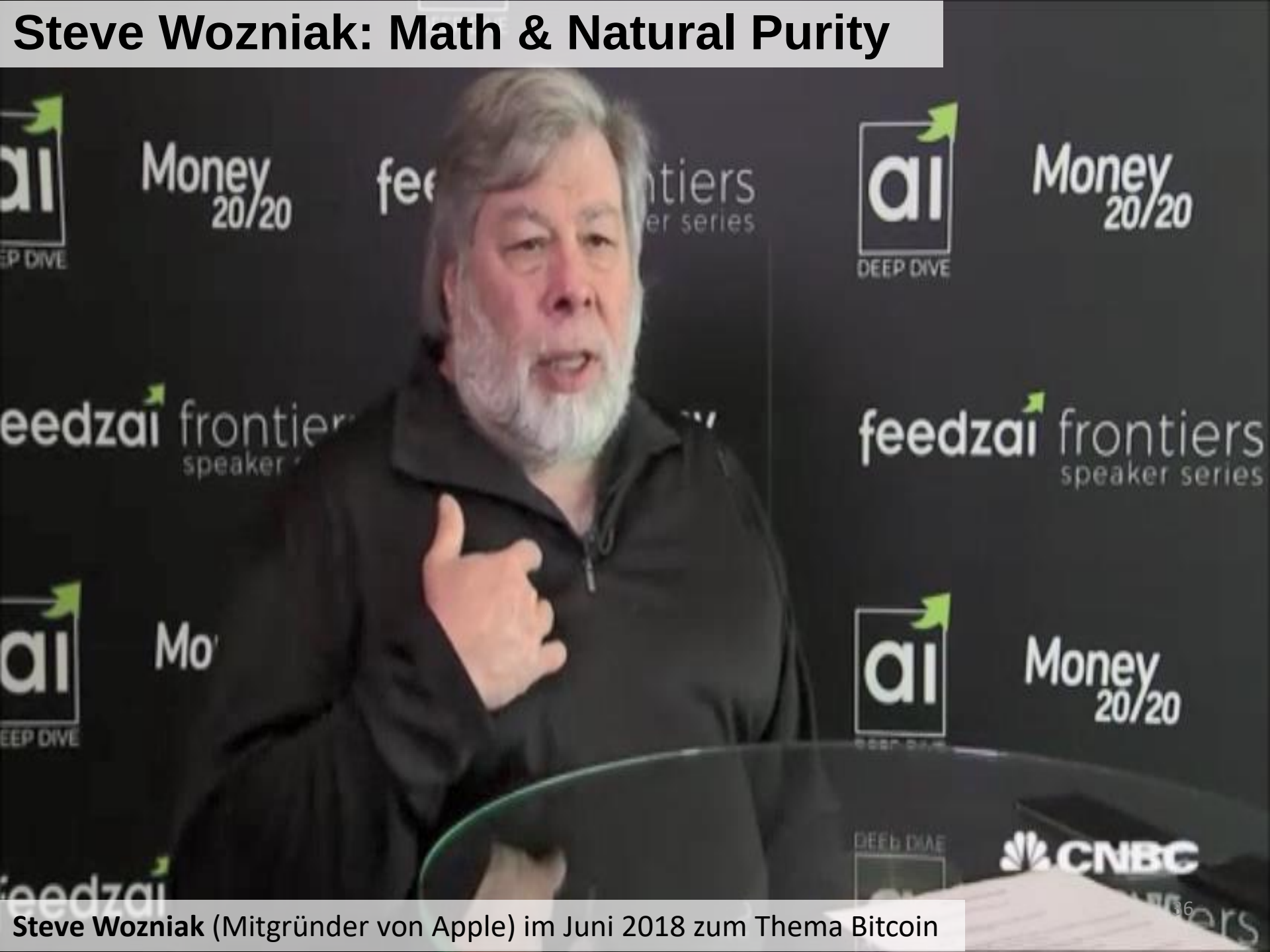
3 Protect Data

- Protecting the Security & Integrity of Data

(5) **Bitcoin Miner & Mining**



Steve Wozniak: Math & Natural Purity



Steve Wozniak (Mitgründer von Apple) im Juni 2018 zum Thema Bitcoin

Steve Wozniak: Math & Natural Purity?

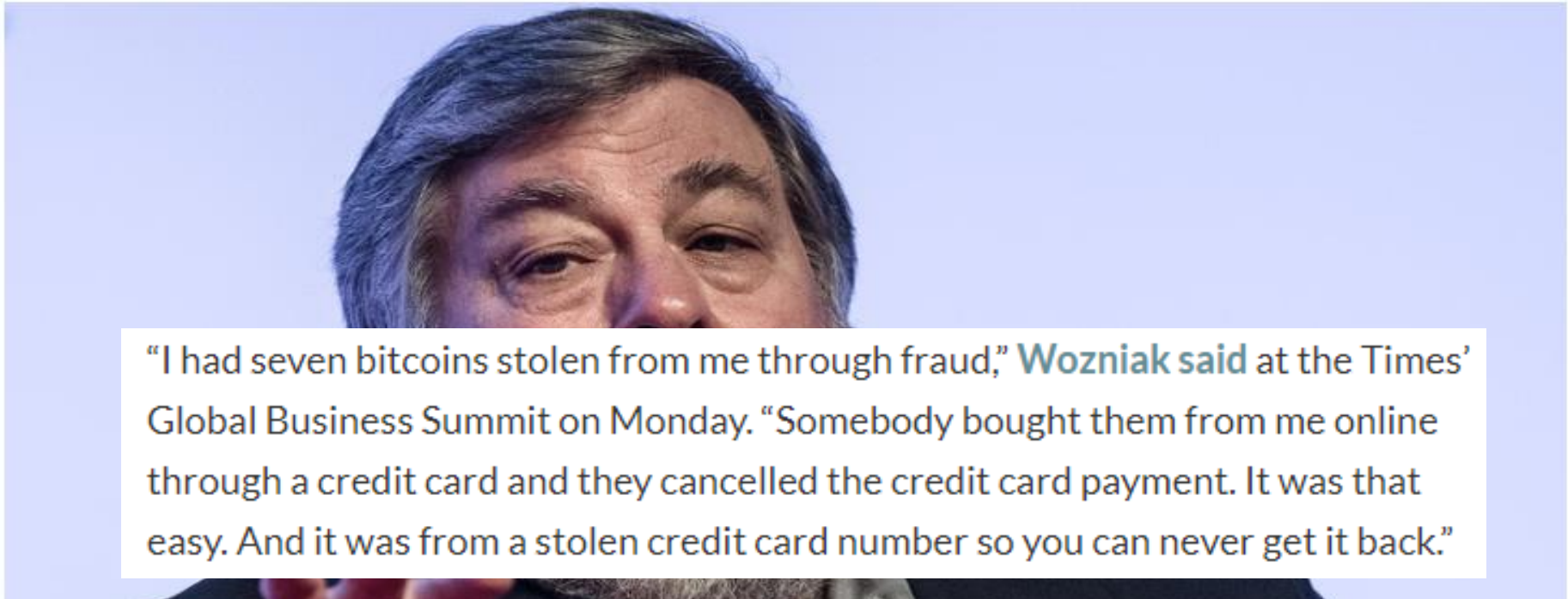
Steve Wozniak had $70,000 in bitcoin stolen after falling for a simple, yet perfect, scam

Published: Feb 28, 2018 11:53 a.m. ET

39

Aa

Will you be smarter than the Apple co-founder?



"I had seven bitcoins stolen from me through fraud," Wozniak said at the Times' Global Business Summit on Monday. "Somebody bought them from me online through a credit card and they cancelled the credit card payment. It was that easy. And it was from a stolen credit card number so you can never get it back."

Warren Buffet: Bitcoin is not a Currency

Warren Buffet im CNBC Interview zum Thema Bitcoin

Warren Buffet: Bitcoin is not a Currency?

Warren Buffet: Bitcoin is not a Currency?

Elon Musk: No Value except Illegal Transactions

Elon Musk (CEO von Tesla und Space X) im Dezember 2016 zum Thema Bitcoin

Elon Musk: No Value except Illegal Transactions?

IDEAS • BITCOIN

Why Bitcoin Matters for Freedom

By ALEX GLADSTEIN December 28, 2018

IDEAS

Gladstein is Chief Strategy Officer at the Human Rights Foundation and Guest Lecturer at Singularity University

But innovation happens at the edge. Today, Venezuelans are adopting and experimenting with Bitcoin to evade hyperinflation and strict financial controls. Speculation, fraud, and greed in the cryptocurrency and blockchain industry have overshadowed the real, liberating potential of Satoshi Nakamoto's invention. For people living under authoritarian governments, Bitcoin can be a valuable financial tool as a censorship-resistant medium of exchange.

Take, for example, remittances. After ravaging the domestic economy, the Venezuelan regime is now taking a cut of money coming in from abroad. New laws force Venezuelans to go through local banks for foreign transactions, and require banks to disclose information on how individuals get and use their money. According to Alejandro Machado, a cryptocurrency researcher at the Open Money Initiative, a wire transfer from the United States can now encounter a fee as high as 56% as it passes from dollars to bolivares in a process that can last several weeks. Most recently, Venezuelan banks have, under pressure from the government, even prevented clients using foreign IP addresses from accessing their online accounts.

Jack Ma: No Value to Society

Jack Ma (Gründer von Alibaba) im November 2017 zum Thema Bitcoin

3 Protect Data
- Protecting the Security & Integrity of Data

Content:

1. **Motivation**
2. **Data Integrity**
3. **Bitcoin** Crypto Currency
4. **Blockchain** Technology
5. Bitcoin **Miner**
6. **Smart Contracts**
7. **IOTA**
8. **Crypto Currency Opinions**
9. **Summary**

Cameron Winklevoss : Better than Gold

Winklevoss Brüder (Bitcoin-Investoren) im Dezember 2018 zum Thema Bitcoin

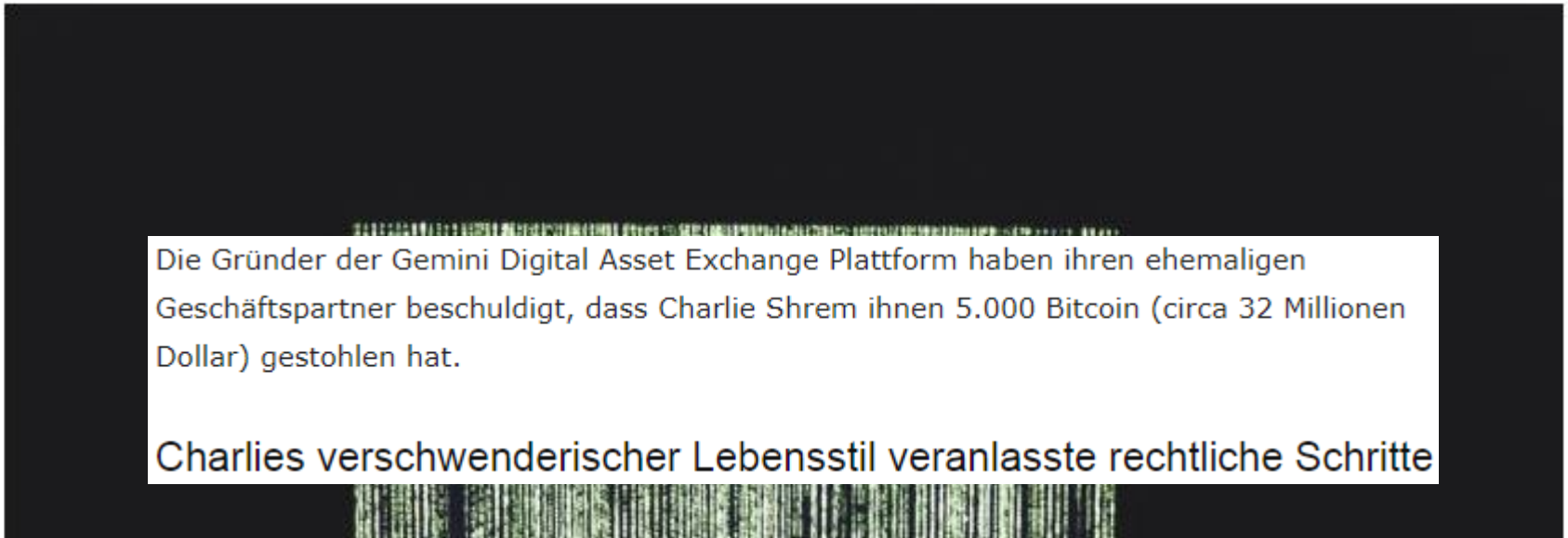
Cameron Winklevoss : Better than Gold?

Bitcoin News

Anklage: Winklevoss Zwillinge beschuldigen Shrem 5.000 Bitcoin gestohlen zu haben

Von **Patrik Eberle** - 3. November 2018 0

Twitter Facebook Linkedin Email Pinterest +



Die Gründer der Gemini Digital Asset Exchange Plattform haben ihren ehemaligen Geschäftspartner beschuldigt, dass Charlie Shrem ihnen 5.000 Bitcoin (circa 32 Millionen Dollar) gestohlen hat.

Charlies verschwenderischer Lebensstil veranlasste rechtliche Schritte

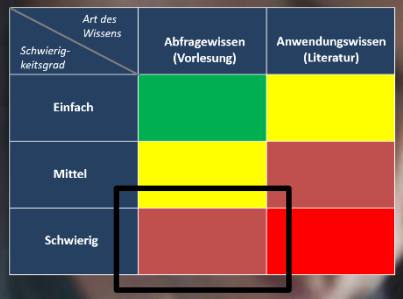
3 Protect Data
- Protecting the Security & Integrity of Data

Content:

1. **Motivation**
2. **Data Integrity**
3. **Bitcoin** Crypto Currency
4. **Blockchain** Technology
5. Bitcoin **Miner**
6. **Smart Contracts**
7. **IOTA**
8. **Crypto Currency Discussions**
9. **Summary**

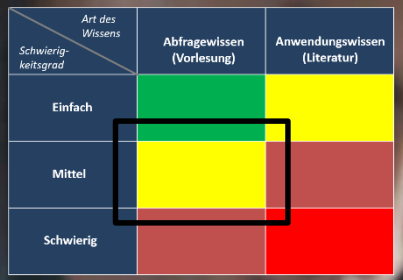
- **Data** is the new **Gold**.
- **Encryption** is **key** to **Data Integrity.**
- **Blockchain** helps in **applications** with **no trust** in **networks**.
- **Crypto Currencies** are on the rise.

Satoshi Nakamoto proposed a solution to the _____ problem using a peer-to-peer network.



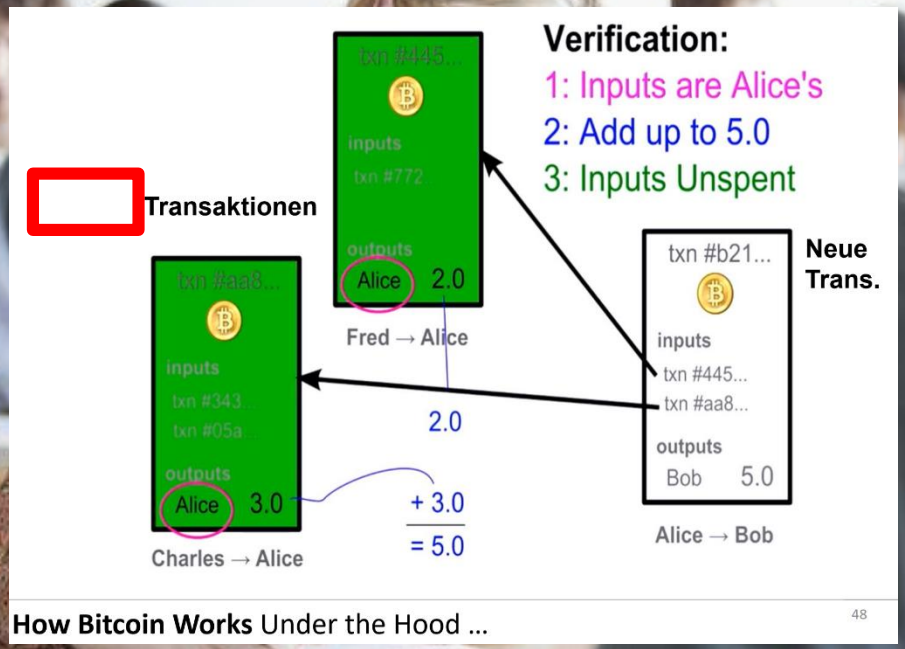
a) Hash function
b) Double-spending
c) Proof-of-work
d) CPU power
e) Bitcoin

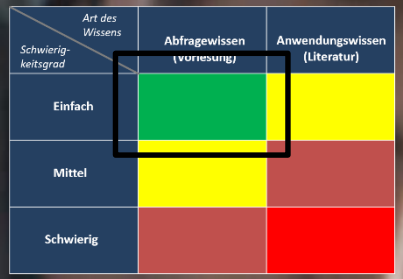
According to the "Bitcoin Whitepaper", what is not an element of the Bitcoin transaction system?



a) Digital signature
b) Timestamps
c) Hash function
d) Proof-of-Stake
e) Blockchain

Transaktionen basieren auf ____ Transaktionen.





a) ältere
b) neue
c) die ersten
d) noch nicht abgeschlossene
e) alle

Kryptowährungen und ihre **Kurse**

Kryptowährung kurse

Top Kryptowährungen Liste | Kryptowährung Liste 2019 | Neue kryptowährungen 2020

Preise an 29 börsen, 10986 handelspaare online

Share:

#	Kryptowährung	Kurs in USD	Kurs in BTC	Marktkap	Austauschvolumen 24std
1	BTC Bitcoin	$ 16,051.12 +0.98% ($155) in 12std +6.99% ($1,048) in 7t	1 BTC +0% in 12 std +0% in 7 tage	$ 297,646,336,609 18,543,651 BTC	352,416 BTC 352,415.67 BTC 5,656,665,656.77 USD
2	ETH Ethereum	$ 461.02 +0.21% ($0.96) in 12std +5.53% ($24.2) in 7t	0.029 BTC -0.76% in 12 std -1.36% in 7 tage	$ 52,295,526,274 113,433,268 ETH	5,178,798 ETH 148,746.84 BTC 2,387,553,152.92 USD
3	XRP XRP	$ 0.274 +2.61% in 12 std +9.28% in 7 tage	0.000017 BTC +1.62% in 12 std +2.15% in 7 tage	$ 12,092,981,469 44,112,853,111 XRP	1,290,603,795 XRP 22,042.25 BTC 353,802,728.19 USD
4	LTC Litecoin	$ 63.34 +0.63% ($0.40) in 12std +7.55% ($4.44) in 7t	0.0039 BTC -0.34% in 12 std +0.52% in 7 tage	$ 4,202,230,638 66,339,058 LTC	5,563,567 LTC 21,956.27 BTC 352,422,708.16 USD
5	BCH Bitcoin Cash	$ 253.37 -1.43% ($3.68) in 12std -0.62% ($1.57) in 7t	0.016 BTC -2.38% in 12 std -7.11% in 7 tage	$ 4,702,462,206 18,559,461 BCH	905,036 BCH 14,286.33 BTC 229,311,572.06 USD
6	LINK ChainLink	$ 12.58 +0.45% ($0.06) in 12std +5.82% ($0.69) in 7t	0.00078 BTC -0.52% in 12 std -1.09% in 7 tage	$ 4,401,908,219 350,000,000 LINK	15,436,513 LINK 12,095.31 BTC 194,143,176.81 USD
7	UNI Uniswap	$ 4.17 +8.7% ($0.33) in 12std +64.64% ($1.64) in 7t	0.00026 BTC +7.65% in 12 std +53.89% in 7 tage		43,161,772 UNI 11,212.31 BTC 179,970,186.3 USD
8	TRX TRON	$ 0.026 +2.29% in 12 std +2.75% in 7 tage	0.0000016 BTC +1.3% in 12 std -3.96% in 7 tage	$ 1,292,007 50,015,001 TRX	5,638,421,298 TRX 9,074.38 BTC 145,653,915.88 USD
9	EOS EOS	$ 2.54 +0.48% in 12 std +1.57% in 7 tage	0.00016 BTC -0.5% in 12 std -5.06% in 7 tage	$ 2,602,350,289 1,024,437,269 EOS	55,142,361 EOS 8,726.91 BTC 140,076,647.39 USD
10	BNB Binance Coin	$ 28.08 +1.01% ($0.28) in 12std +0.82% ($0.23) in 7t	0.0017 BTC +0.03% in 12 std -5.76% in 7 tage	$ 4,155,123,728 147,956,562 BNB	4,890,223 BNB 8,556.05 BTC 137,334,107.03 USD

bitinfocharts.com/de/markets/

Homework

1. How big is the **Bitcoin Blockchain?**

2. How many **Bitcoin Transactions** have there been?

Wie viele **Bitcoin** hast du? Unterwegs im Hamburger Nachtleben …

WEB \ TECH \ FACEBOOK

The Winklevoss twins are now Bitcoin billionaires

60

From an $11 million investment in 2013

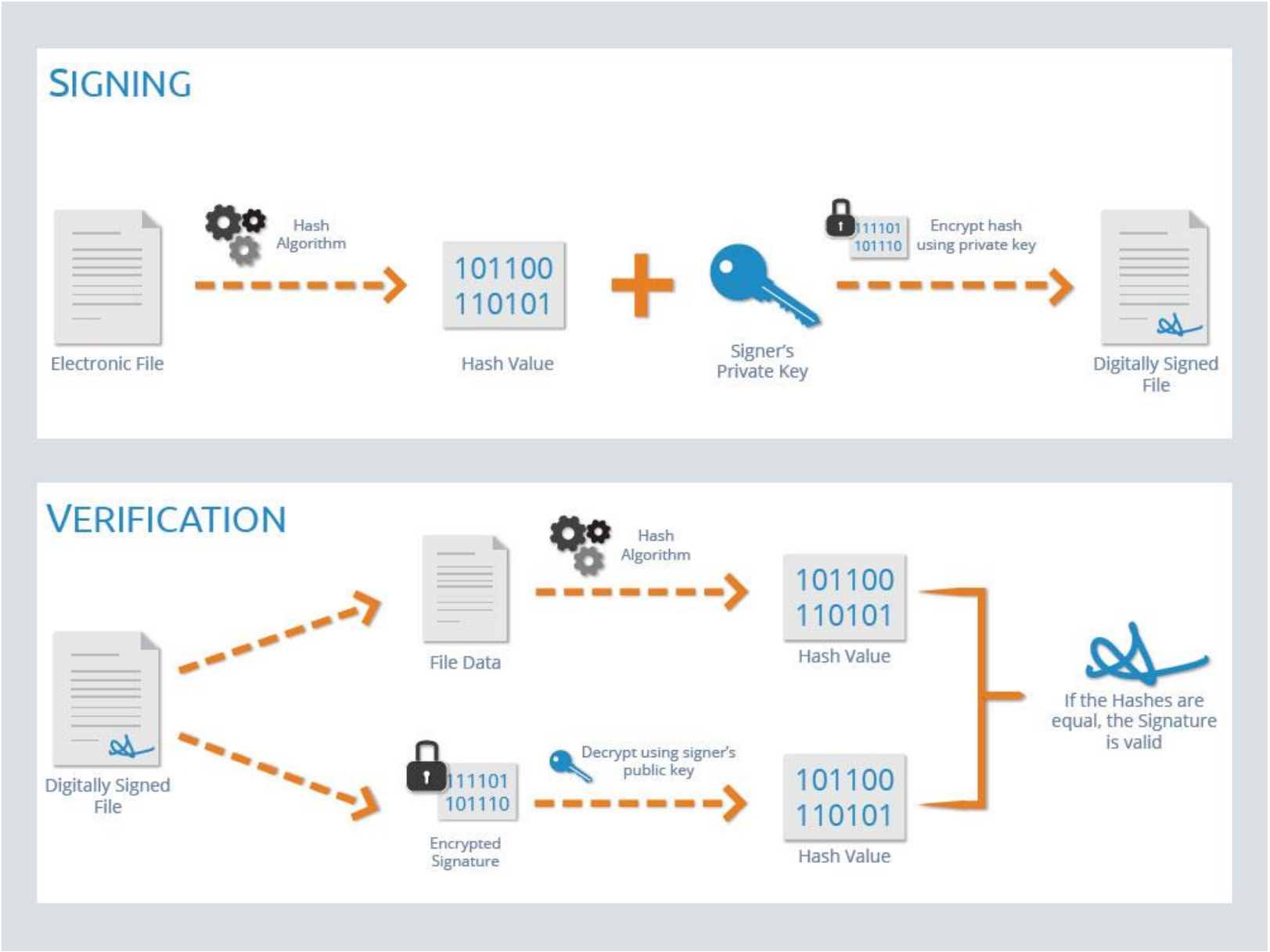
By Thuy Ong | @ThuyOng | Dec 4, 2017, 7:39am EST

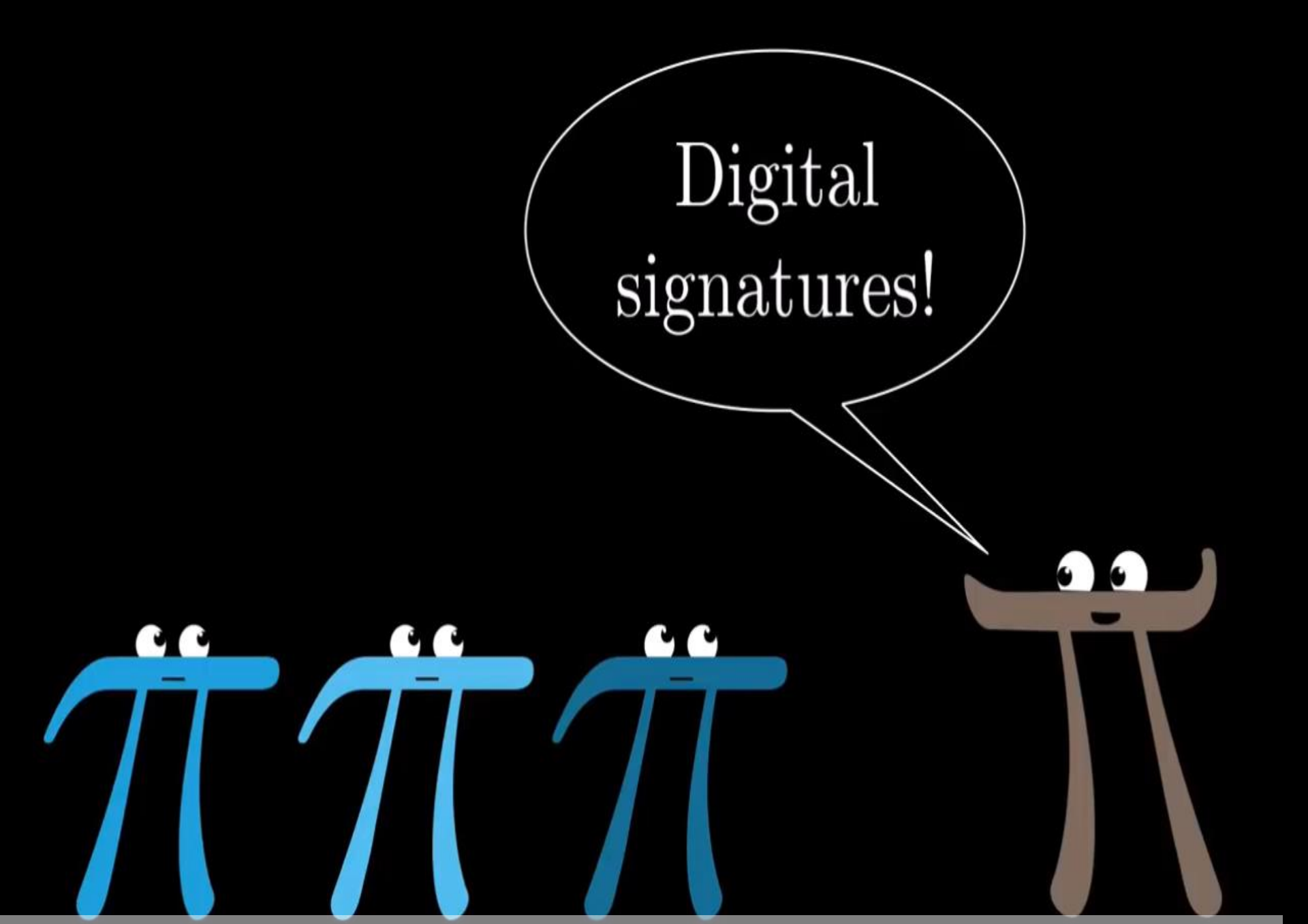
The Winklevoss twins, famously known for suing Mark Zuckerberg after claiming he stole their idea for Facebook, are now Bitcoin billionaires, according to a few reports. Cameron and Tyler Winklevoss won $65 million from the Facebook lawsuit, and invested $11 million of their payout into Bitcoin in 2013, amassing one of the largest portfolios of Bitcoin in the world — 1 percent of the entire currency's dollar value equivalent, said the twins at the time. Their slice of the Bitcoin pie is now worth over $1 billion after Bitcoin surged past $10,000 last week to now trade at $11,100, according to *CoinDesk*. The cryptocurrency has surged over 10,000 percent since the Winklevoss' investment, when one coin traded at around $120.

Math Puzzle: Eine rechenintensive Aufgabe mit Hash-Funktionen (für Bitcoin relevant)

Hash Puzzle: Ergänze Dein **Dokument** (Nachricht) mit einer **Zahl**, so dass der **Hash-Wert** kleiner ist als ein **Ziel-Hash-Wert** (z.B. beginne mit 30 Nullen) ist.
Kann man nur **ausprobieren** und ist daher sehr **rechenintensiv.**

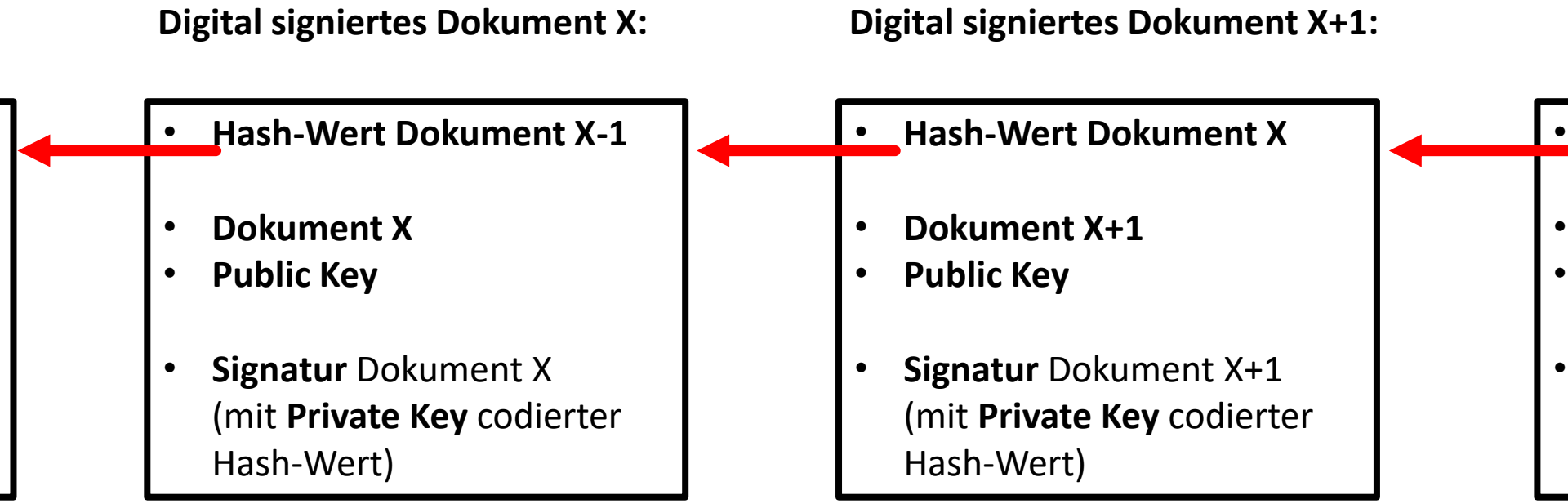
Digital signiertes Dokument (für Bitcoin relevant)





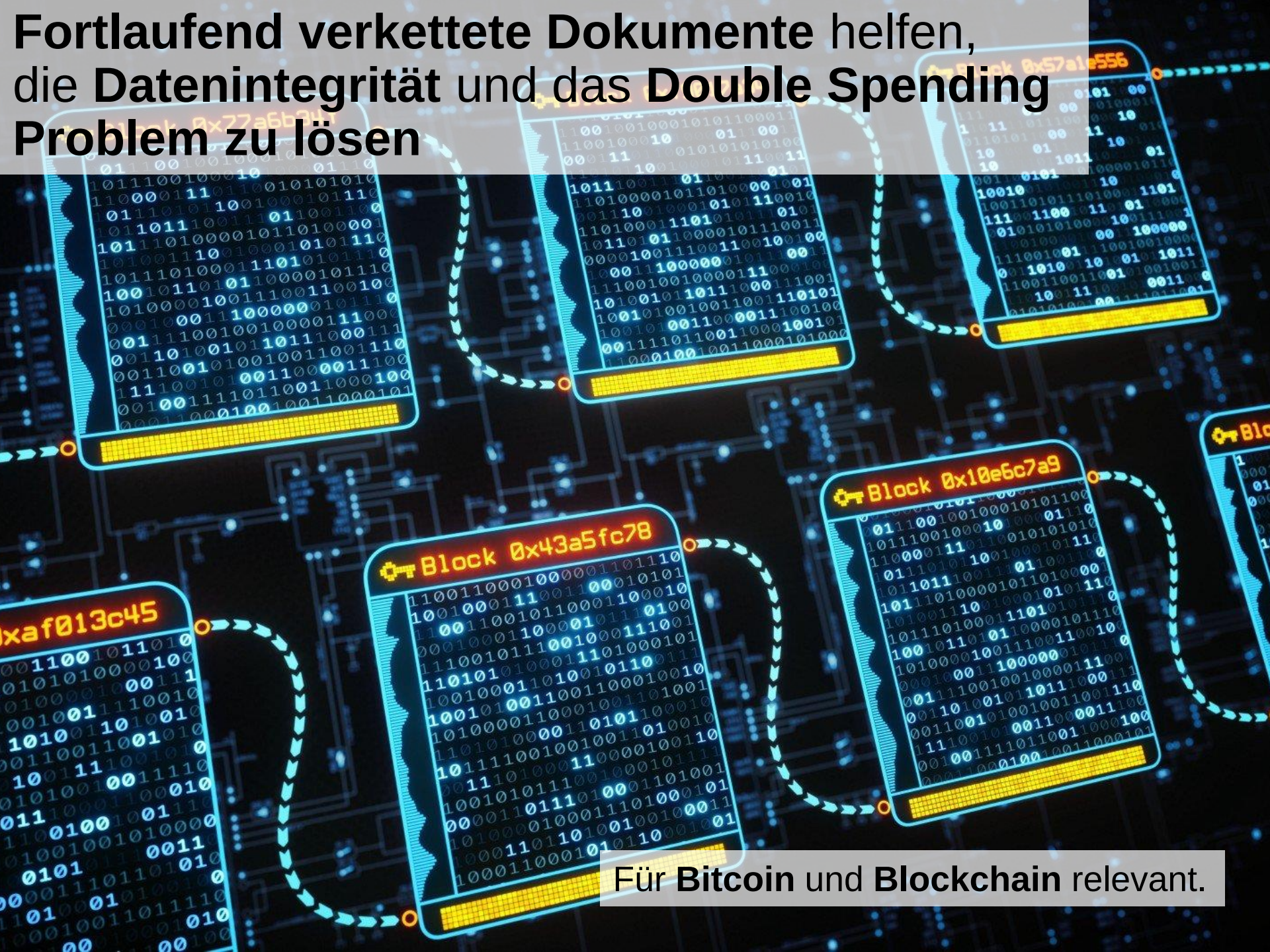
Ever wonder how **Bitcoin** (and other cryptocurrencies) **actually work?**

Kette von digital signierten Dokumenten
(für Bitcoin relevant)



Die **Signatur** bezieht sich auf das **Gesamtdokument** und umfasst den **Hash-Wert** vom **Vordokument** und den **Public Key**.

Bei **Änderung** eines **Vordokumentes** müssen alle **Folgedokumente** auch geändert werden (**Reihenfolge** der Dokumente ist festgelegt).


Fortlaufend verkettete Dokumente helfen, die Datenintegrität und das Double Spending Problem zu lösen
Block 0x43a5fc78
Block 0x10e6c7a9
Für Bitcoin und Blockchain relevant.

Michael Amberg

Todays Content:

1. **Motivation**
2. **Data Integrity**
3. **Bitcoin** Cryptocurrency
4. **Blockchain** Technology
5. Bitcoin **Miner**
6. **Smart Contracts**
7. **IOTA**
8. **Crypto Currency Discussions**
9. **Summary**

Ledger

	account number	balance	
	1G8bneji6etY...	12.5	
	1K7A6wsyxj6...	323	
Carol	16pJcrGi51nr...	6.0	+5.0
Bob	1MVbjHicuJr...	10.2	-5.0
	1G4HyHp1oa...	100	
	17UP3moev2...	.00000001	
	1Eeq4FM2Ts...	45	
	...	...	

Ledger ist hier vereinfacht dargestellt. Nicht **Kontostände**, sondern **Transaktionen** werden gespeichert.

Twitter, Inc. [US] | https://twitter.com/actual_ransom?lang=de

Startseite | Mitteilungen | Nachrichten | Twitter durchsuchen | Twittern

Tweets 432 | Follower 6.464 | Folgen

actual ransom
@actual_ransom

This bot is watching the bitcoin wallets tied to the #WannaCry ransomware attack. USD amounts as of time of tweet. By @collinskeith

inside a raspberry pi

Beigetreten Mai 2017

Tweet an actual ransom

Tweets | Tweets & Antworten

actual ransom @actual_ransom · 3. Jan.
Someone just paid 0.0001 BTC ($1.5 USD) to a bitcoin wallet tied to #WannaCry ransomware. blockchain.info/address/13AM4V...
Original (Englisch) übersetzen
3 | 6

actual ransom @actual_ransom · 3. Jan.
Someone just paid 0.0001 BTC ($1.52 USD) to a bitcoin wallet tied to #WannaCry ransomware. blockchain.info/address/13AM4V...
Original (Englisch) übersetzen
4 | 5

actual ransom @actual_ransom · 2. Jan.
Someone just paid 0.0201 BTC ($297.63 USD) to a bitcoin wallet tied to #WannaCry ransomware. blockchain.info/address/13AM4V...
Original (Englisch) übersetzen
20 | 26

Wem folgen? · Aktualisieren · Alle anzeigen

Deutsche Lichtmiete @Lic... Folgen Gesponsert

Martin Klarmann @Marti... Folgen

Gesponserter Tweet

Wannacry, 12.5.2017 (Bitcoin-**Adresse** = „Bitcoin-**Konto**“)

Blockchain Luxembourg S.A.R.L [LU] | https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

BLOCKCHAIN WALLET DATA API ABOUT BLOCK, HASH, TRANSACTION, ETC... GET A FREE WALLET

Bitcoin-Adresse Adressen sind Kennungen, die verwendet werden um Bitcoins an eine andere Person senden.

Zusammenfassung	
Adresse	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Hash 160	17b4bd9a139158614e8f54c6b800a1822609436a
Tools	Kennzeichnungen - Unausgeglichene Ausgänge

Transaktionen	
Anzahl der Transaktionen	136
Gesamtempfang	$ 318,065.22
Endgültige Balance	$ 2,842.16

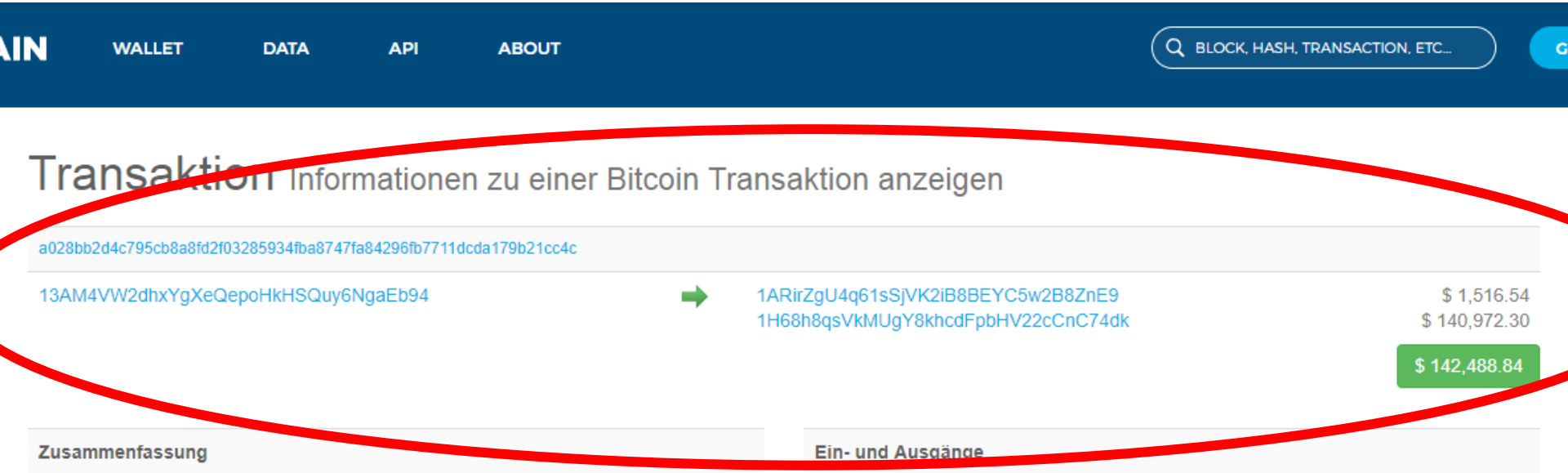
Zahlungsanfrage Spenden-Button

Transaktionen (Die ältesten zu erst) Filter

f02992bd48551f4d9ec2d2c4f6f82dab42b5a20f22593a5b2a656153162a9855			2018-01-03 22:31:06
1soKWfCPVrr2GAuN2v3SbXGjrYsCEs2TG	→	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	$ 1.60
			$ 1.60

103ec673850e844b10e38941953b44ee73a8b80e5bfee5eb56d3401428d73820			2018-01-03 03:23:16
11WoLbasoiauFbe2cVV5VuaJYkwSJn72z	→	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94	$ 1.60
			$ 1.60

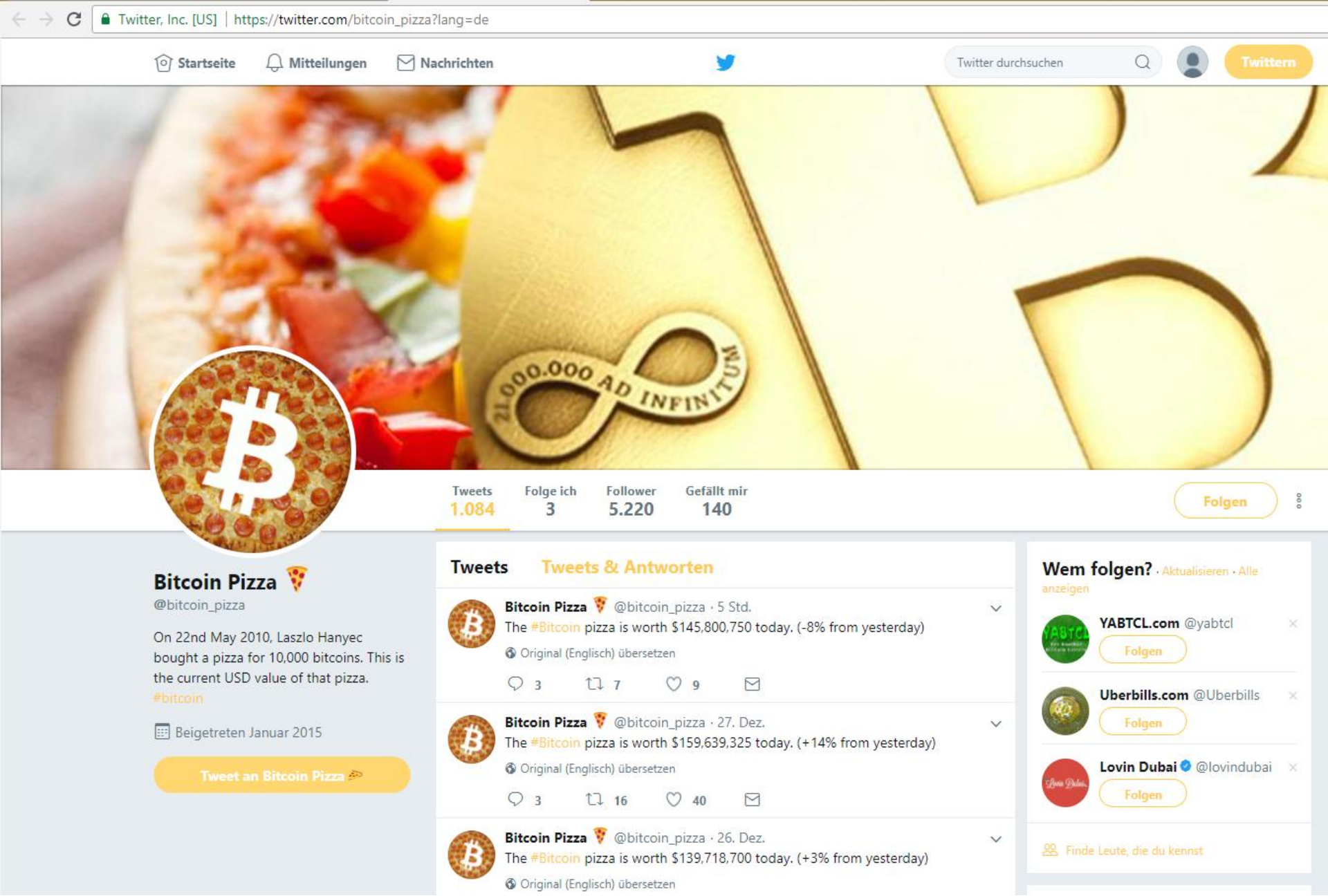
Wannacry, 12.5.2017 (Bitcoin-**Adresse** = „Bitcoin-**Konto**“)



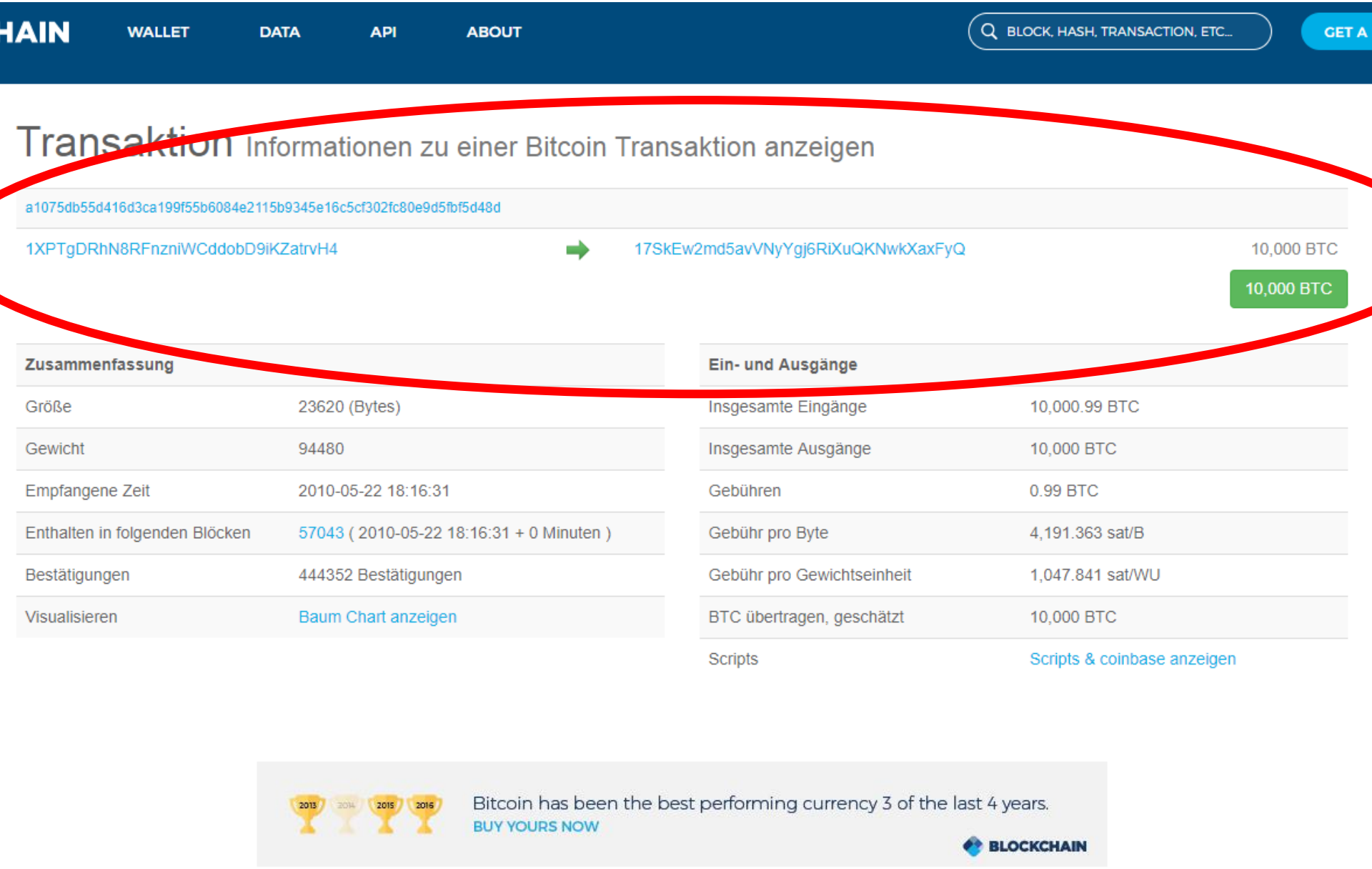
Zusammenfassung	
Größe	7600 (Bytes)
Gewicht	30400
Empfangene Zeit	2017-08-03 03:25:03
Enthalten in folgenden Blöcken	478789 (2017-08-03 03:39:15 + 14 Minuten)
Bestätigungen	24392 Bestätigungen
Visualisieren	Baum Chart anzeigen

Ein- und Ausgänge	
Insgesamte Eingänge	$ 142,646.40
Insgesamte Ausgänge	$ 142,488.84
Gebühren	$ 157.56
Gebühr pro Byte	140.633 sat/B
Gebühr pro Gewichtseinheit	35.158 sat/WU
BTC übertragen, geschätzt	$ 140,972.30
Scripts	Scripts & coinbase anzeigen

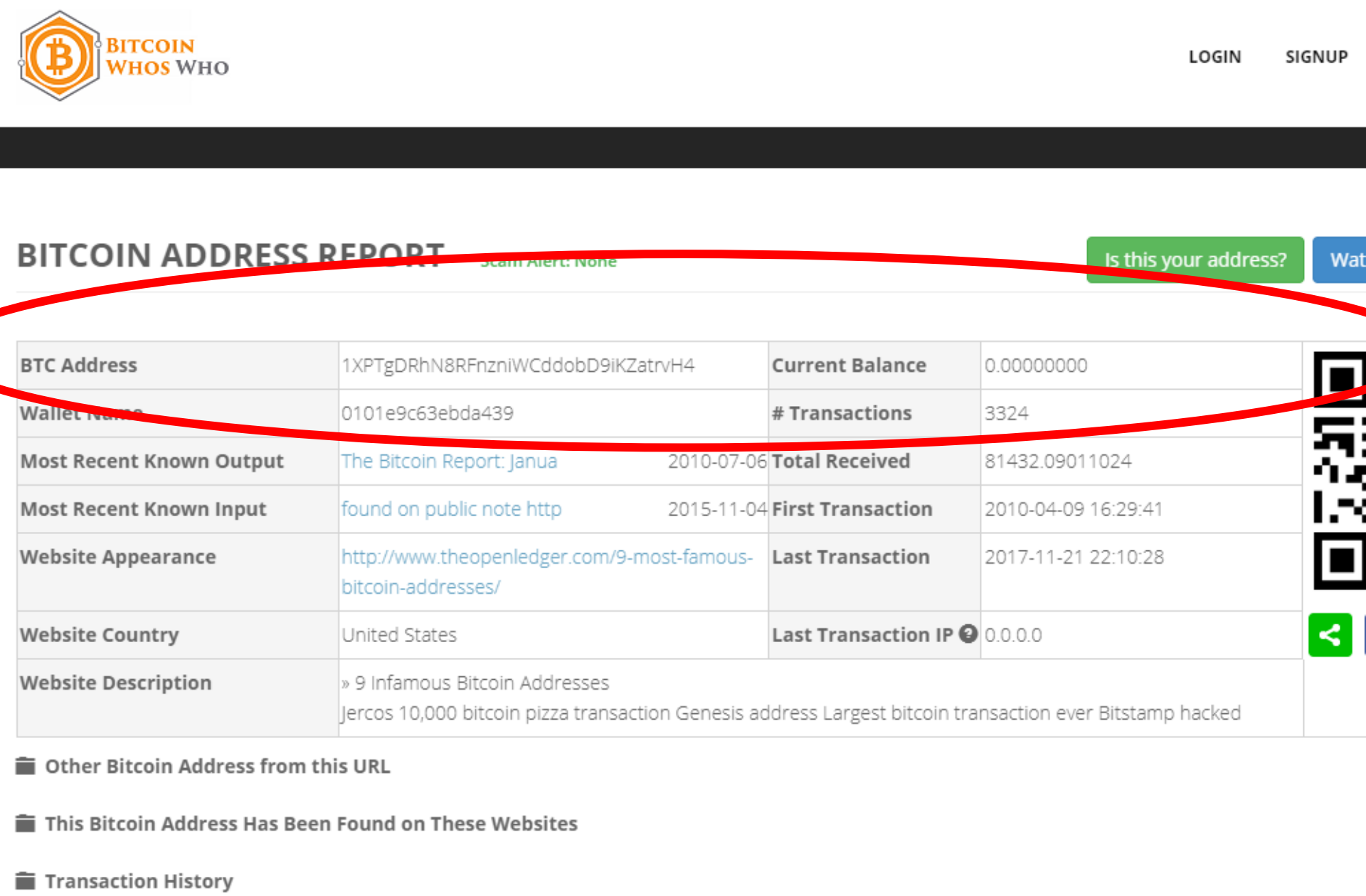
Wannacry, 12.5.2017 (Bitcoin-**Transaktion** = „Bitcoin-**Überweisung**“)



Die **teuerste Pizza der Welt …** (twitter.com/bitcoin_pizza)



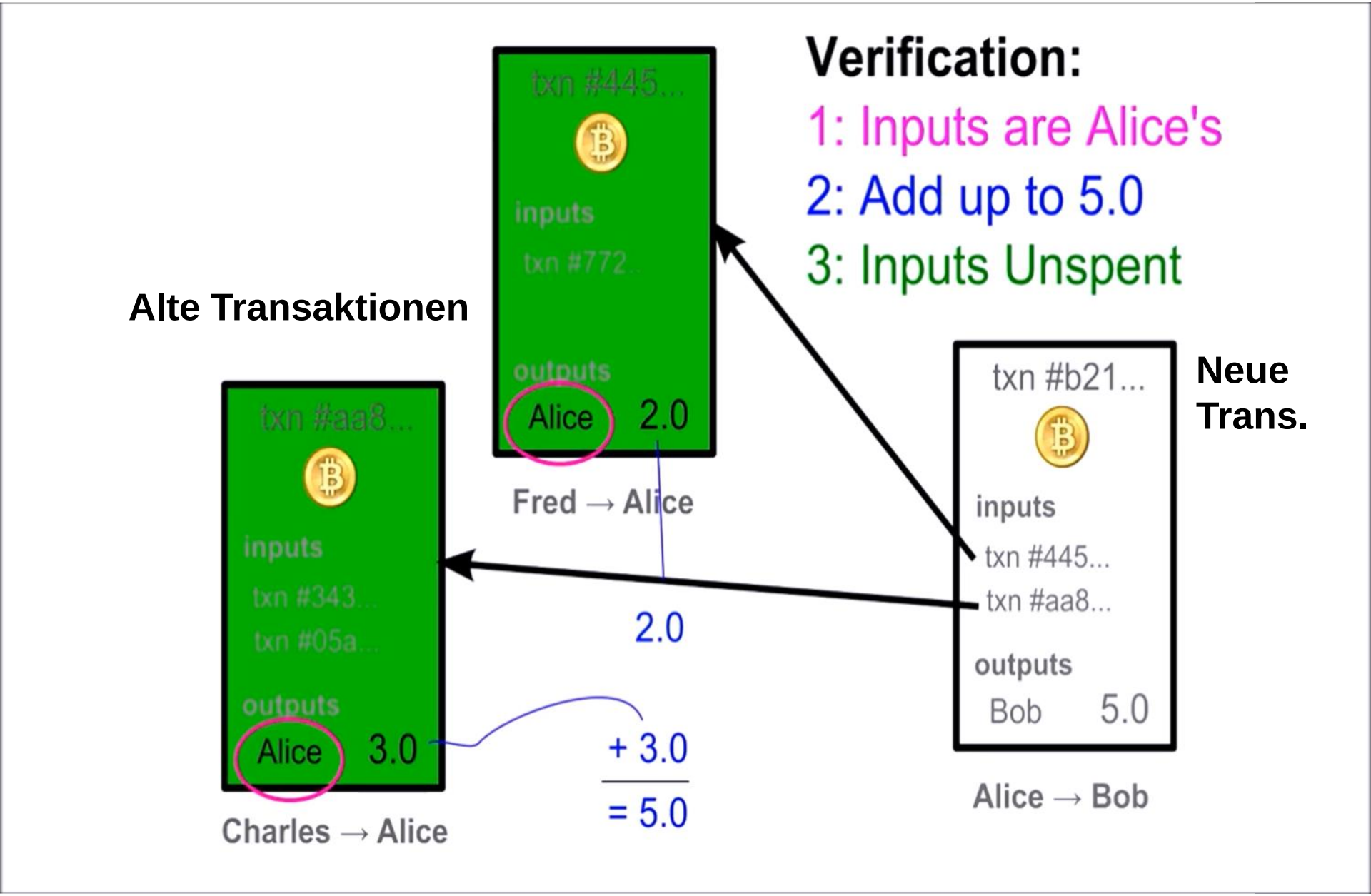
Eine **“berühmte” Bitcoin-Transaktion …** (blockchain.info)



Das **Konto** von **Laszlo Hanyecz**? (bitcoinwhoswho.com)

12/2017: James Howells hat **7.500 Bitcoins verloren** … (12/2017)

Transaktionen „verbrauchen“ ältere Transaktionen



Transaktionen „verbrauchen“ ältere Transaktionen

Inputs

Previous output (index)[2]	Amount[2]	From address[2]	Type[2]	ScriptSig[2]
eb38f77560ca...:1	8	1P9SgqzjFWgWVAuZBFwimNPV7LuuaJpgTj	Addres	30450220078df7c48ed152bd40eaee4a73afefc31 044760639da2c0d6158484e1a4dab332fefc4bb
b912994fca58...:1	0.03	18Mk65wV1E5kCVHFShvUTU6zt4yVFKM5Ft	Addres	304502204e877fc5ca3783e165052e64c4788dd 04769bbfc55cbd412784e024c8624f8c4f42d7cb
58379d94fe85...:15	1	1G4hfnM2ufAPEECdawg5gtvUTBB2PxvLr2	Addres	3044022075d23fd4a8004866777210f51f46c960 046dd45b37fe3ff33f1563458cfbdfb7f922d1b4a
fc9d1cd1c2ac...:1	130	1LpQVnJSMgqqibQBGZwbobdX2Ghn9YWyC7	Addres	3046022100a65a188b89a4e5ae2eaa5ba387503 04ba81a1a538c5ddf7e0c76884497ab522456b9
7b6f7d4a521c...:1	0.55357267	16Kb6XppHUbjgmYQDpRyxz9jNE9Az5Xvcb	Addres	3045022100eeb76e61abe62d38fd462eafd1d11f 04f4fa1d3e26f3e7058038871a31b8bf63fd127f6
544097a30e09...:0	0.03270607	1JnsDx1g6c757z8AnJUemj46YQgCTw54QN	Addres	3045022100859df2ced47493e86a849cce10615 04de257fe6490bd16188be6d06ca7b34816fa4b

+

139.6

Outputs

Outputs[2]

Index[2]	Redeemed at input[2]	Amount[2]	To address[2]	Type[2]	ScriptPubKey[2]
0	8baaca27d158...	0.01071174	1F7BgzQbyWTWzEMUKNzzLdjkbjaQT9K96m	Address	OP_DUP OP_HASH160 9abd2e0c0a63dea36b75c3128fe15d82f274e394 OP_EQUALVERIFY OP_CHECKSIG
1	1bb973b4ccc8...	139.605567	1NT2zFMa11NiCZydt4kqgXRZPf3iS6ZPGZ	Address	OP_DUP OP_HASH160 eb471d7a903e538cb94c1f2faf20eaadad8479af OP_EQUALVERIFY OP_CHECKSIG

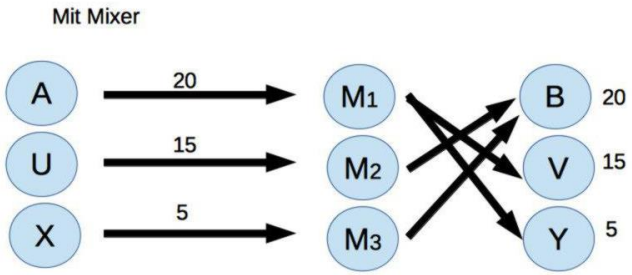
+

139.6

Bitcoin Mixer

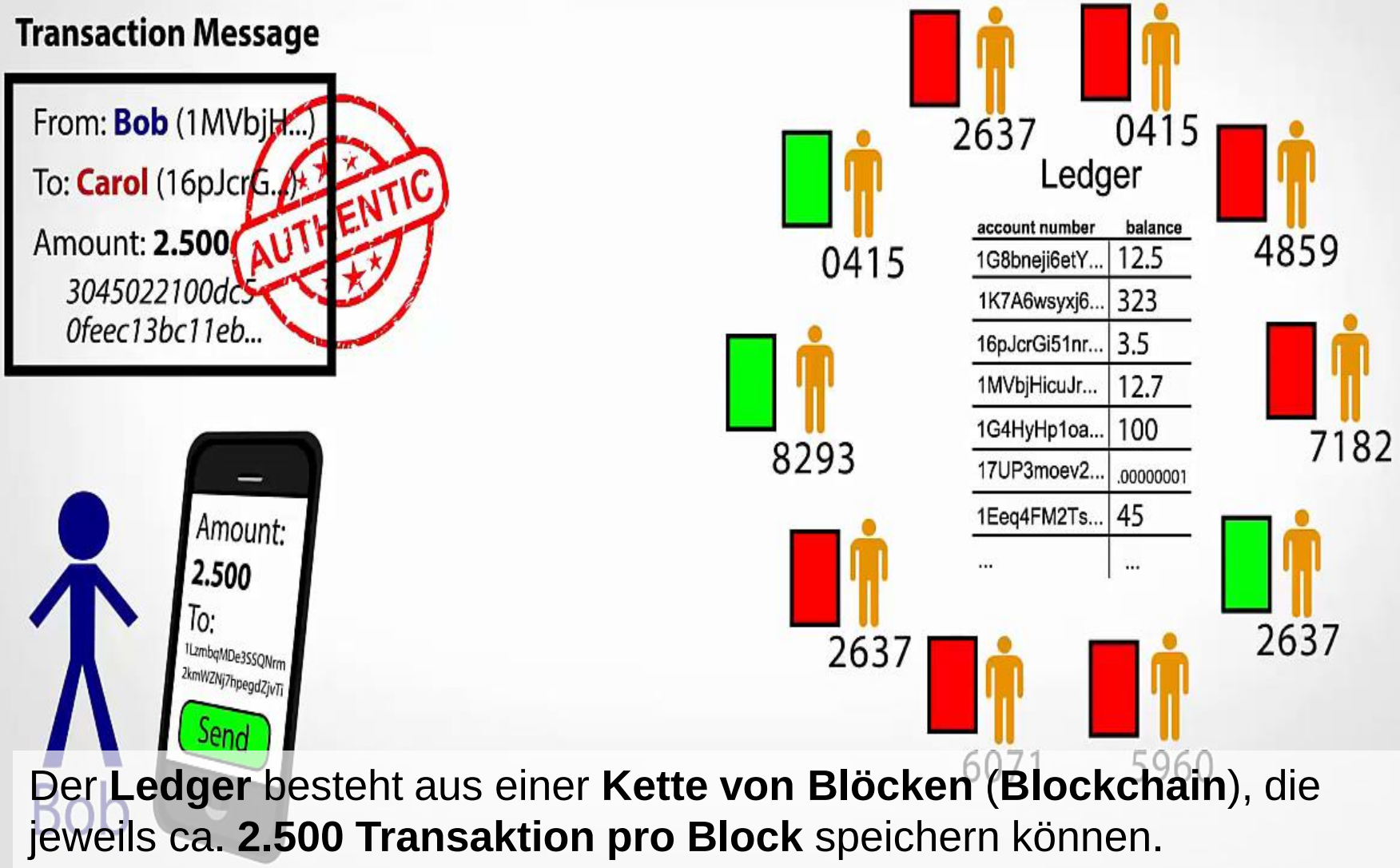
Bitcoin Mixer sind Angebote, die dazu dienen, die Geldflüsse Deiner Bitcoins (BTC) zu verschleiern. Damit helfen sie, die Privatsphäre Deines Vermögens zu schützen. Kritiker sehen Bitcoin Mixer als Werkzeuge, um kriminelle Aktivitäten der Beobachtung zu entziehen.

Bitcoin (BTC) als erste und führende Kryptowährung hat zwar in seinem Konzept prinzipiell Anonymität verankert. Doch in der Realität ist bei der üblichen Nutzung von BTC diese Anonymität nicht oder nur in geringem Ausmaß gewährleistet. Denn alle Transaktionen werden in der öffentlich einsehbaren Blockchain für immer dokumentiert. Sobald es jemandem gelingt, die Adresse einer Bitcoin Wallet einer konkreten Person oder Unternehmen zuzuordnen, lässt sich also nachvollziehen, von wo und wohin diese Wallet Transaktionen durchgeführt hat und um welche Beträge es dabei ging. Verglichen mit dem klassischen Bankkonto heißt das, jeder könnte herausfinden, von wem du wie viel Geld bekommst und wofür Du es wieder ausgibst. Um diese Schwachstelle im Konzept von BTC zu schließen, wurden Bitcoin Mixer erfunden.

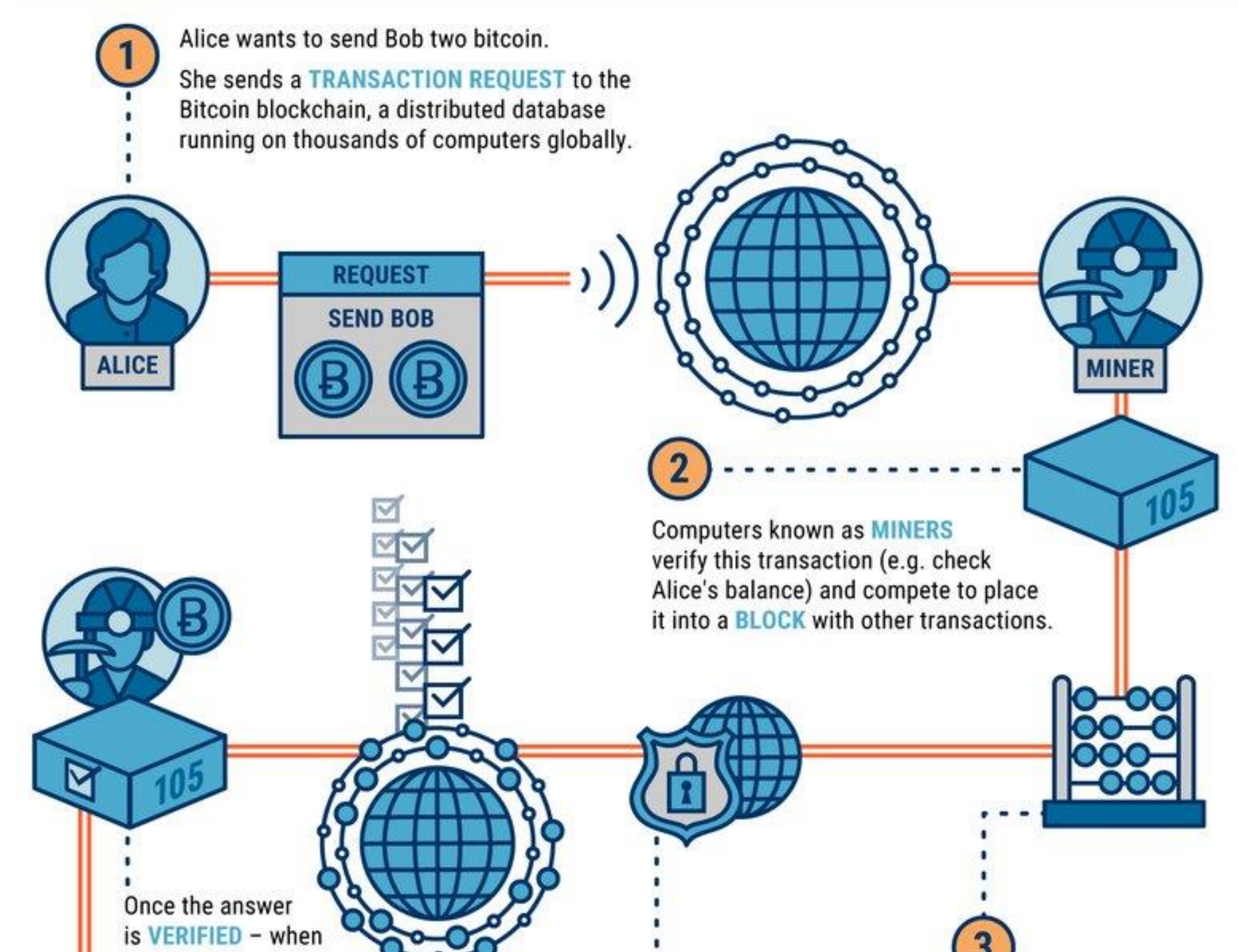


4. Blockchain
The Technology Behind Bitcoin

Summary



Der **Ledger** besteht aus einer **Kette von Blöcken** (**Blockchain**), die jeweils ca. **2.500 Transaktion pro Block** speichern können.

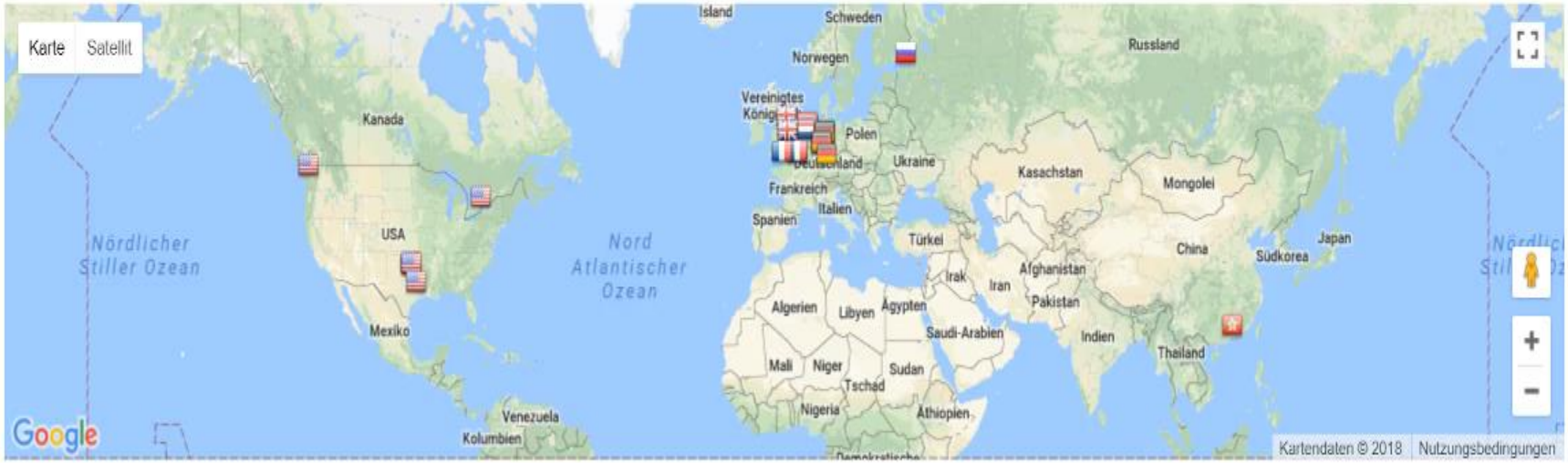

1
Alice wants to send Bob two bitcoin.
She sends a TRANSACTION REQUEST to the Bitcoin blockchain, a distributed database running on thousands of computers globally.
ALICE
REQUEST
SEND BOB
MINER
2
105
Computers known as MINERS verify this transaction (e.g. check Alice's balance) and compete to place it into a BLOCK with other transactions.
105
Once the answer is VERIFIED – when
3

171054 unbestätigte Tra

Blockchain Luxembourg S.A.R.L [LU] | https://blockchain.info/de/unconfirmed-transactions

BLOCKCHAIN WALLET DATA API ABOUT BLOCK, HASH, TRANSACTION, ETC... GET A FREE WALLET

171056 unbestätigte Transaktionen Live aktualisierte Liste der aktuellen Bitcoin Transaktionen



Zusammenfassung	Status: In Verbindung gebracht
Gebühren, gesamt	72.23228052 BTC

DEU 18:35
DE 08.01.2018

Proof of Work (Wikipedia)

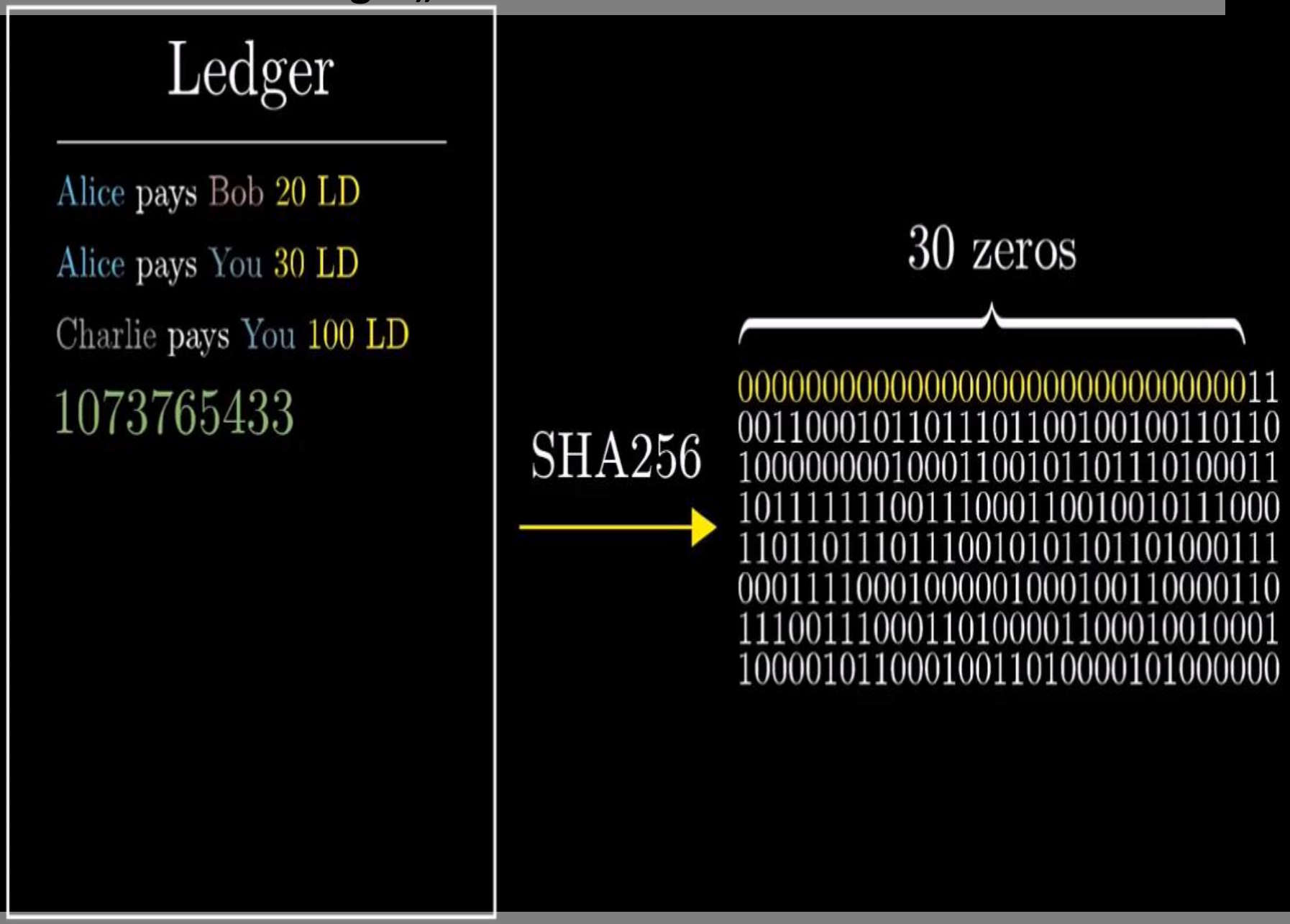
Proof of work

From Wikipedia, the free encyclopedia

This article may **require cleanup** to meet Wikipedia's quality standards. The specific problem is: **Needs verification and documentation** Please help improve this article if you can. *(May 2015) (Learn how and when to remove this template message)*

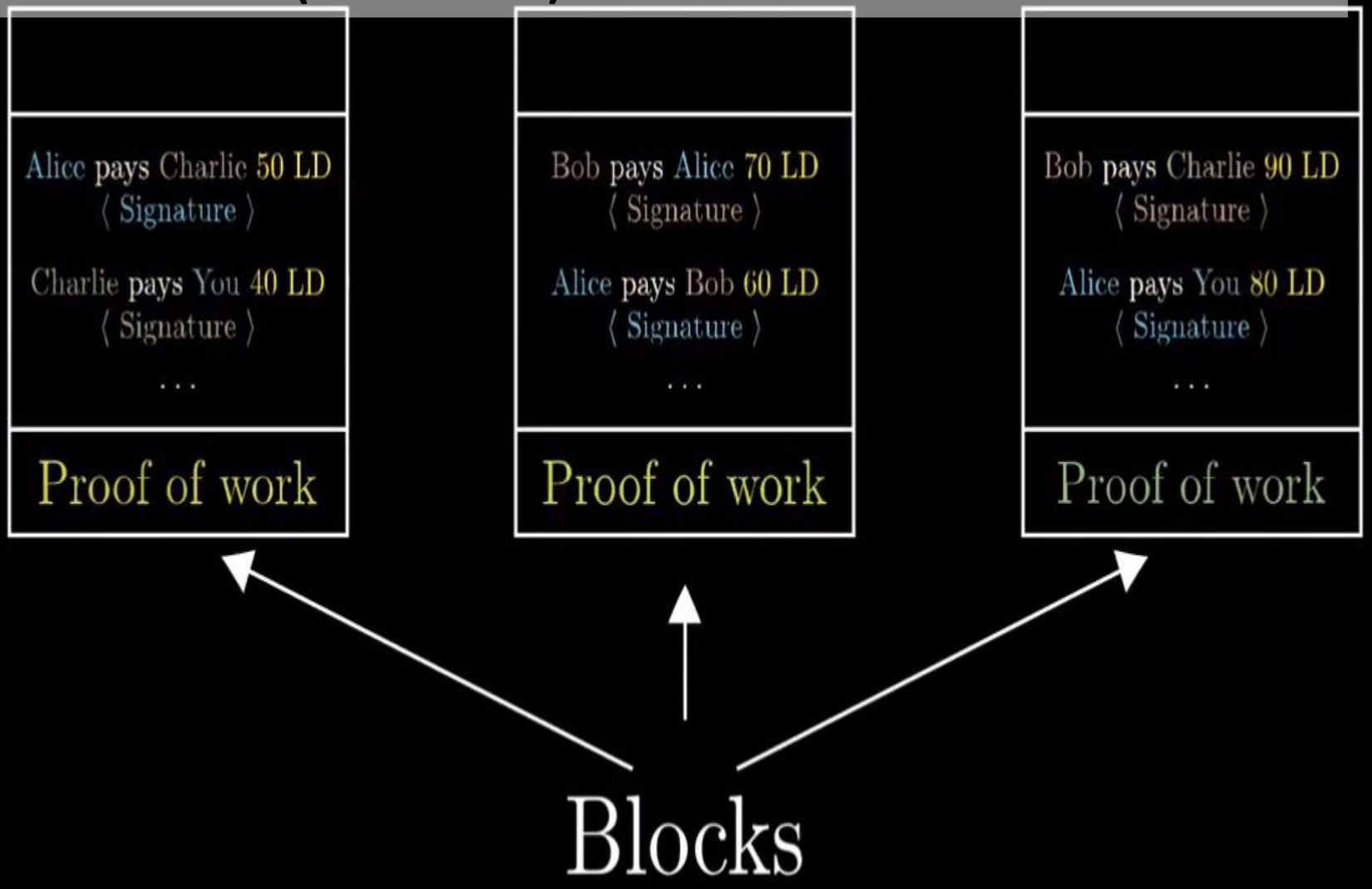
Proof of work (**PoW**) is a form of cryptographic zero-knowledge proof in which one party (the *prover*) proves to others (the *verifiers*) that a certain amount of computational effort has been expended for some purpose. Verifiers can subsequently confirm this expenditure with minimal effort on their part. The concept was invented by Cynthia Dwork and Moni Naor in 1993 as a way to deter denial-of-service attacks and other service abuses such as spam on a network by requiring some work from a service requester, usually meaning processing time by a computer. The term "proof of work" was first coined and formalized in a 1999 paper by Markus Jakobsson and Ari Juels.[1][2] Proof of work was later popularized by Bitcoin as a foundation for consensus in permissionless blockchains and cryptocurrencies, in which miners compete to append blocks and mint new currency, each miner experiencing a success probability proportional to the amount of computational effort they have provably expended. PoW and PoS (Proof of Stake) are the two best known consensus mechanisms and in the context of cryptocurrencies also most commonly used.[3]

Math Puzzle: Finding a „Nonce“

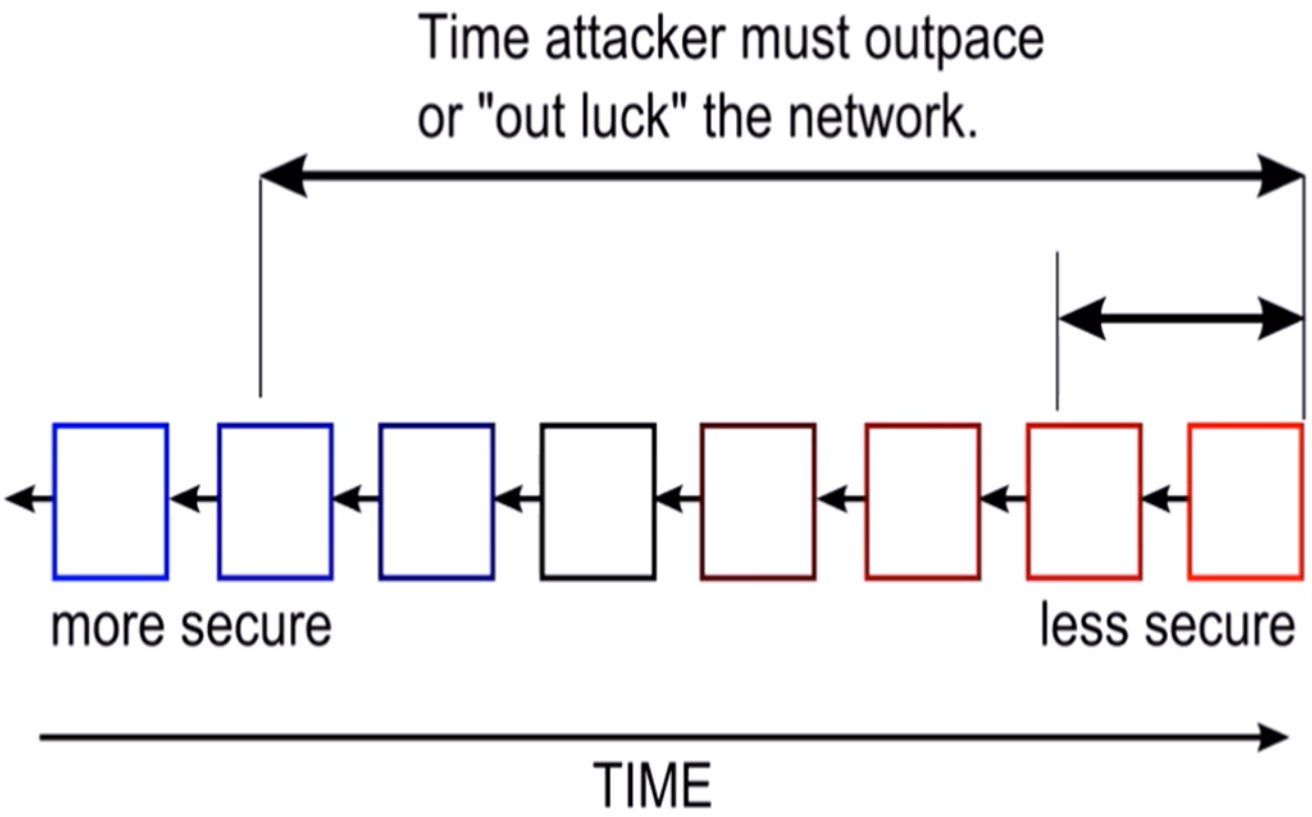


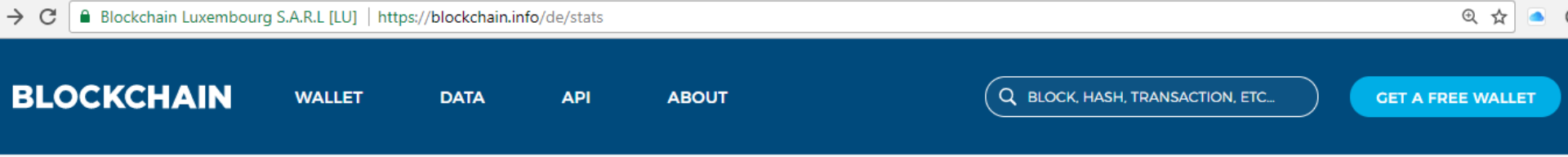
Ever wonder how **Bitcoin** (and other cryptocurrencies) **actually work?**

A Chain of Blocks (Blockchain) is harder to hack



Ever wonder how **Bitcoin** (and other cryptocurrencies) **actually work?**


Time attacker must outpace
or "out luck" the network.
more secure
less secure
TIME



Währungs Statistik

Summary of bitcoin statistics for the previous 24 hour period.

BLOCK SUMMARY

Blöcke gefunden	155
Zeit zwischen den Blöcken	8.69 Minuten
Bitcoins gefunden	1,937.50000000 BTC

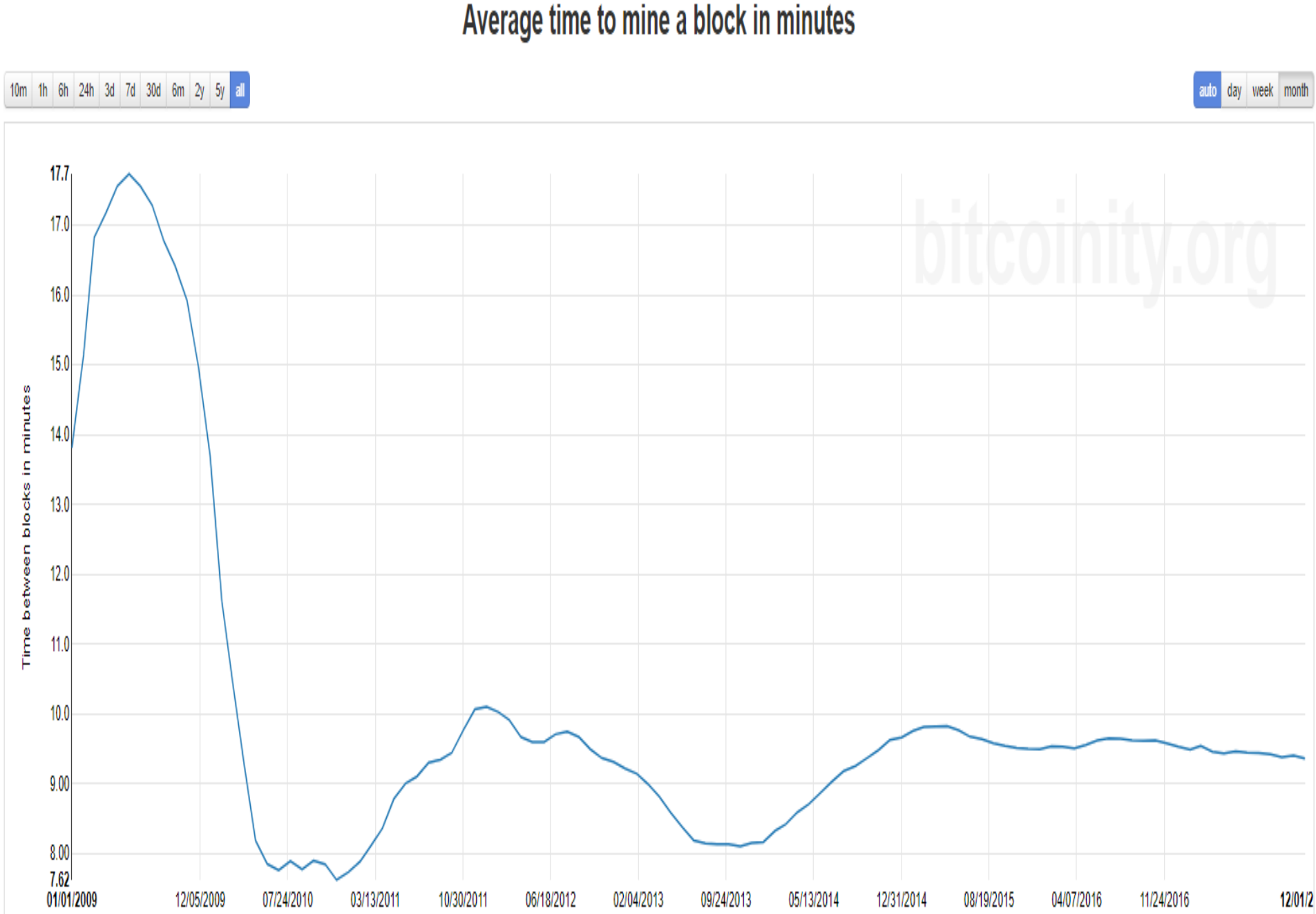
MARKTÜBERSICHT

Marktpreis	$14,841.45	Diagramm anzeigen
Handelsvolumen	$1,287,568,036.15	
Handelsvolumen	84,515.71000000 BTC	

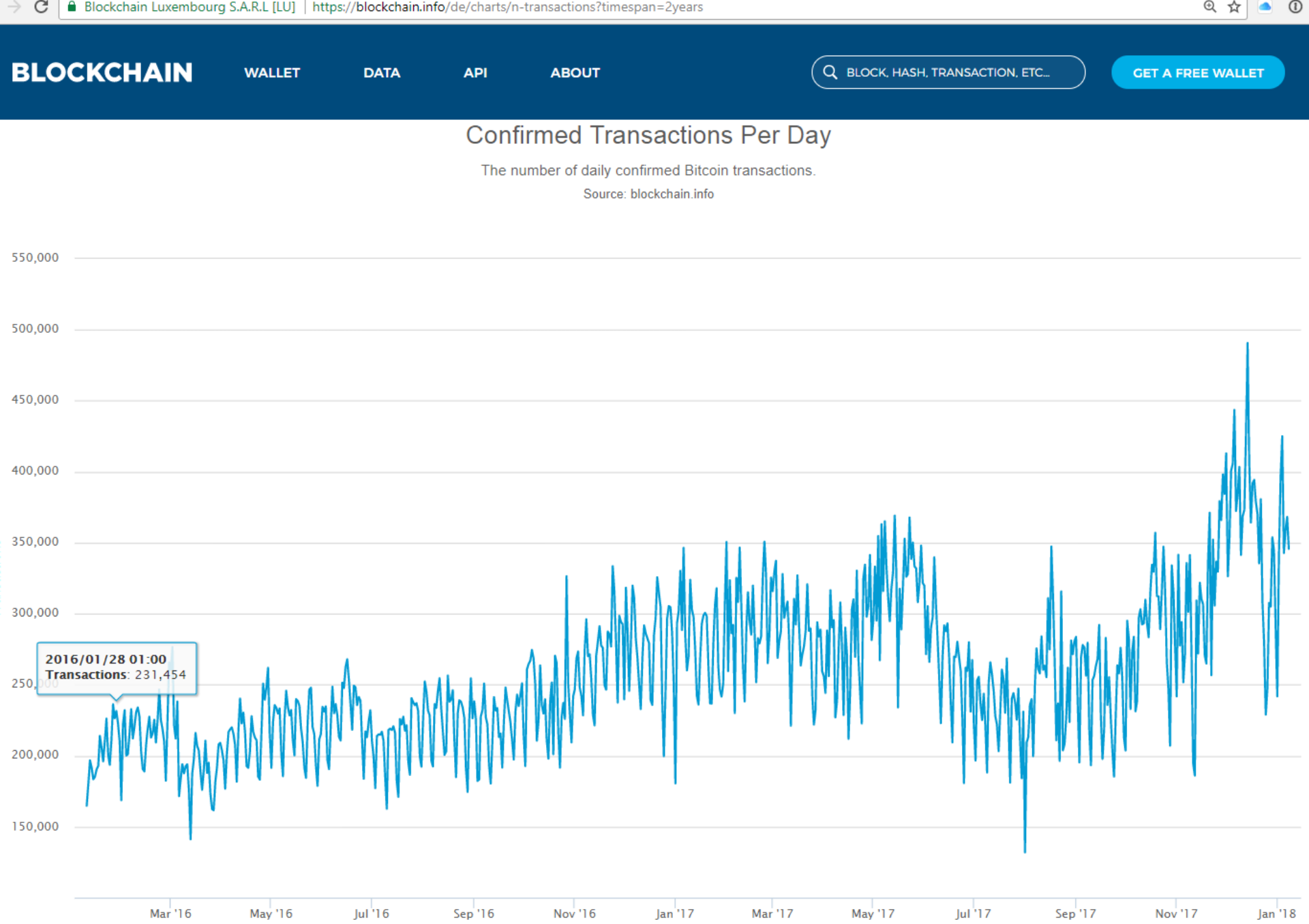
TRANSACTION SUMMARY

Gesamte Transaktions-Kosten (BTC)	709.38512803 BTC	Diagramm anzeigen
Anzahl der Transaktionen	337,427	Diagramm anzeigen
Total Output Volume (BTC)	2,070,244.34016876 BTC	Diagramm anzeigen
Geschätztes Transaktions Volumen (BTC)	244,720.83521011 BTC	Diagramm anzeigen
Geschätztes Transaktions Volumen (USD)	$3,728,238,311.47	Diagramm anzeigen

Statistiken zu Bitcoin (blockchain.info)



Statistiken zu Bitcoin (blockchain.info)



Anzahl erfolgreicher **Bitcoin-Transaktionen** pro Tag (blockchain.info)

How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

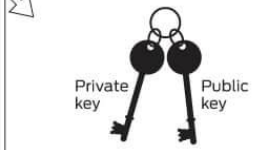
Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.



Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.

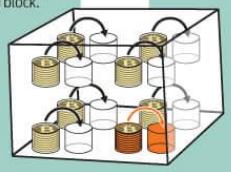
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

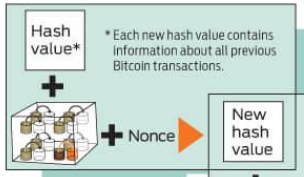
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.



The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

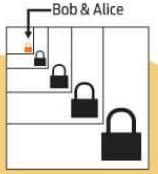
The root of all evil ???	0000 0000 0000 ...

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED

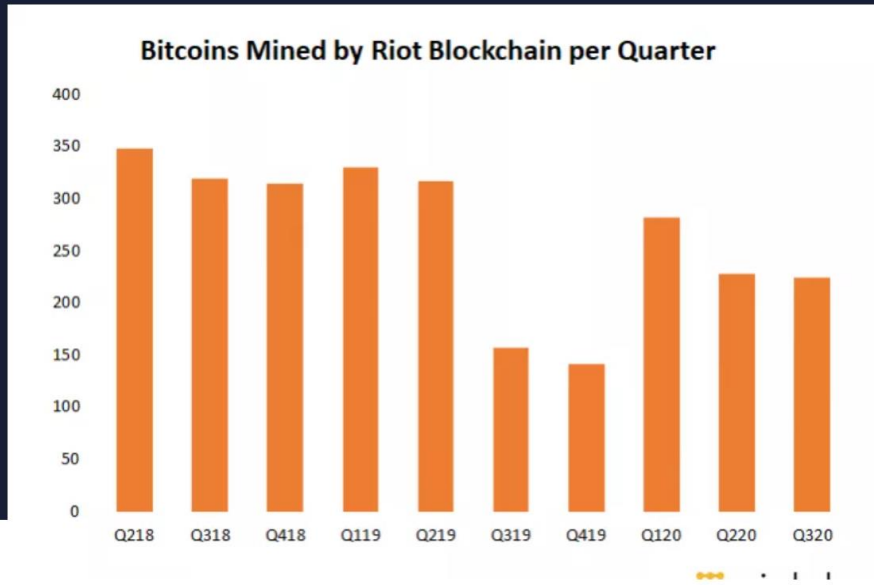


As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

5. Bitcoin **Miner**

Riot Blockchain Mined 222 Bitcoins in Q3

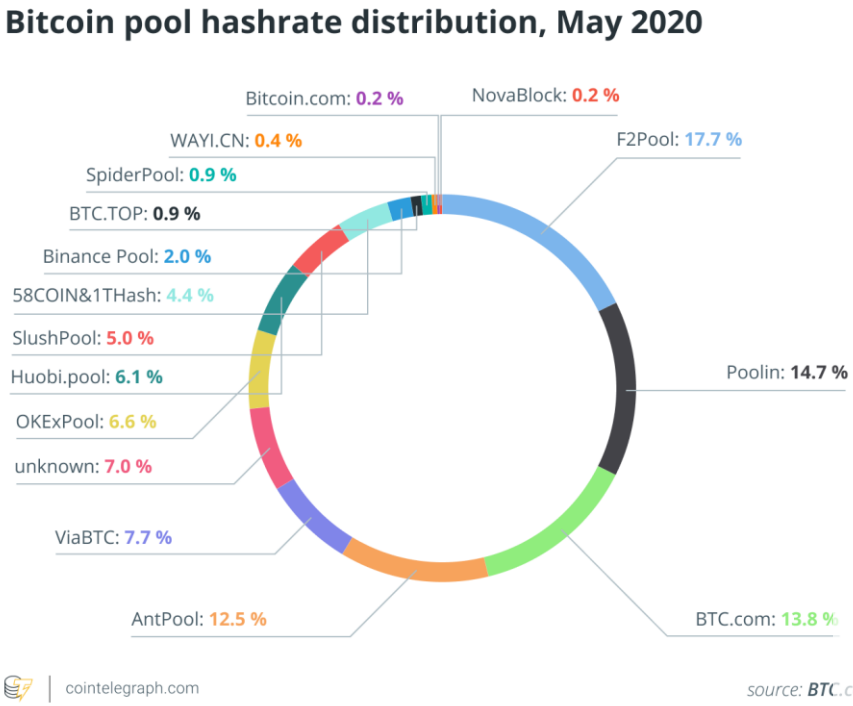
Nov 10, 2020 at 2:32 a.m. ▪ Updated Nov 10, 2020 at 2:41 p.m.

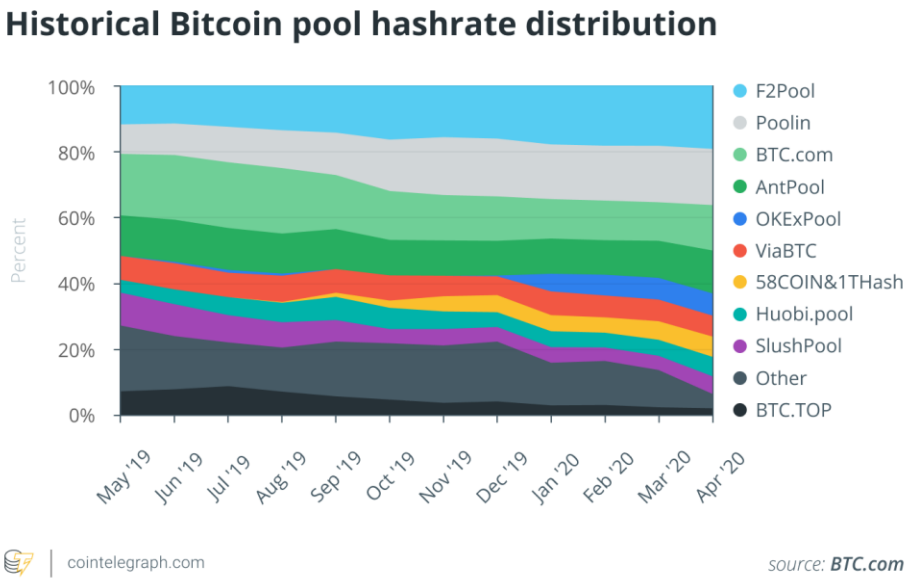


Bitcoins mined per quarter by Riot since Q2 2018

Publicly traded bitcoin mining company Riot Blockchain

Bitcoin Mining Pools





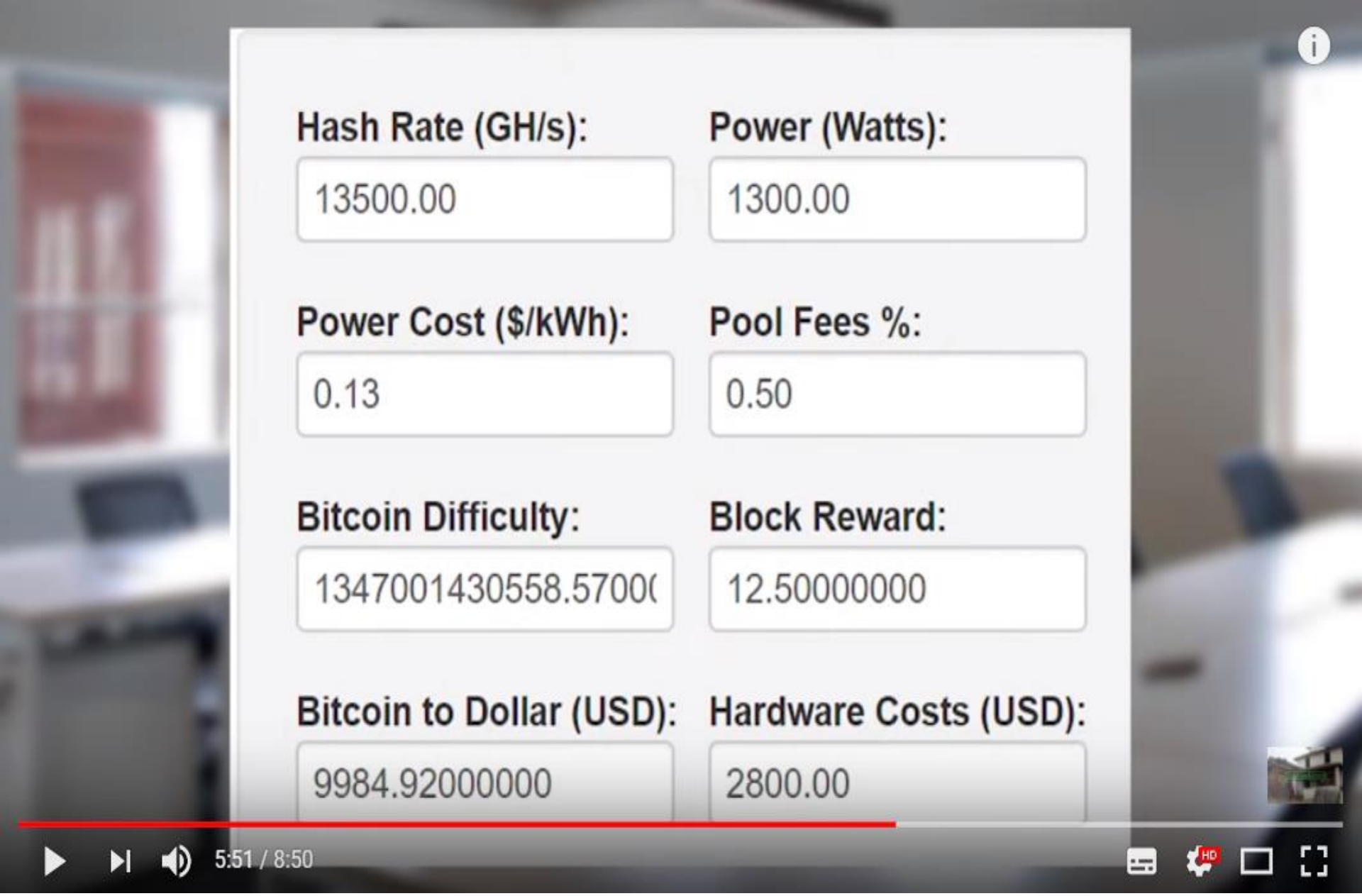
Grobe Kalkulation für **BTC.com**:

- ca. **2.000 BTC pro Tag** werden ausgezahlt
- Anteil BTC.com **13,8%** = **276 BTC pro Tag**
- = **8.280 BTC pro Monat** (bei 30 Tagen)
- = **132.48 Mio US Dollar pro Monat** (bei Kurs 16.000$)

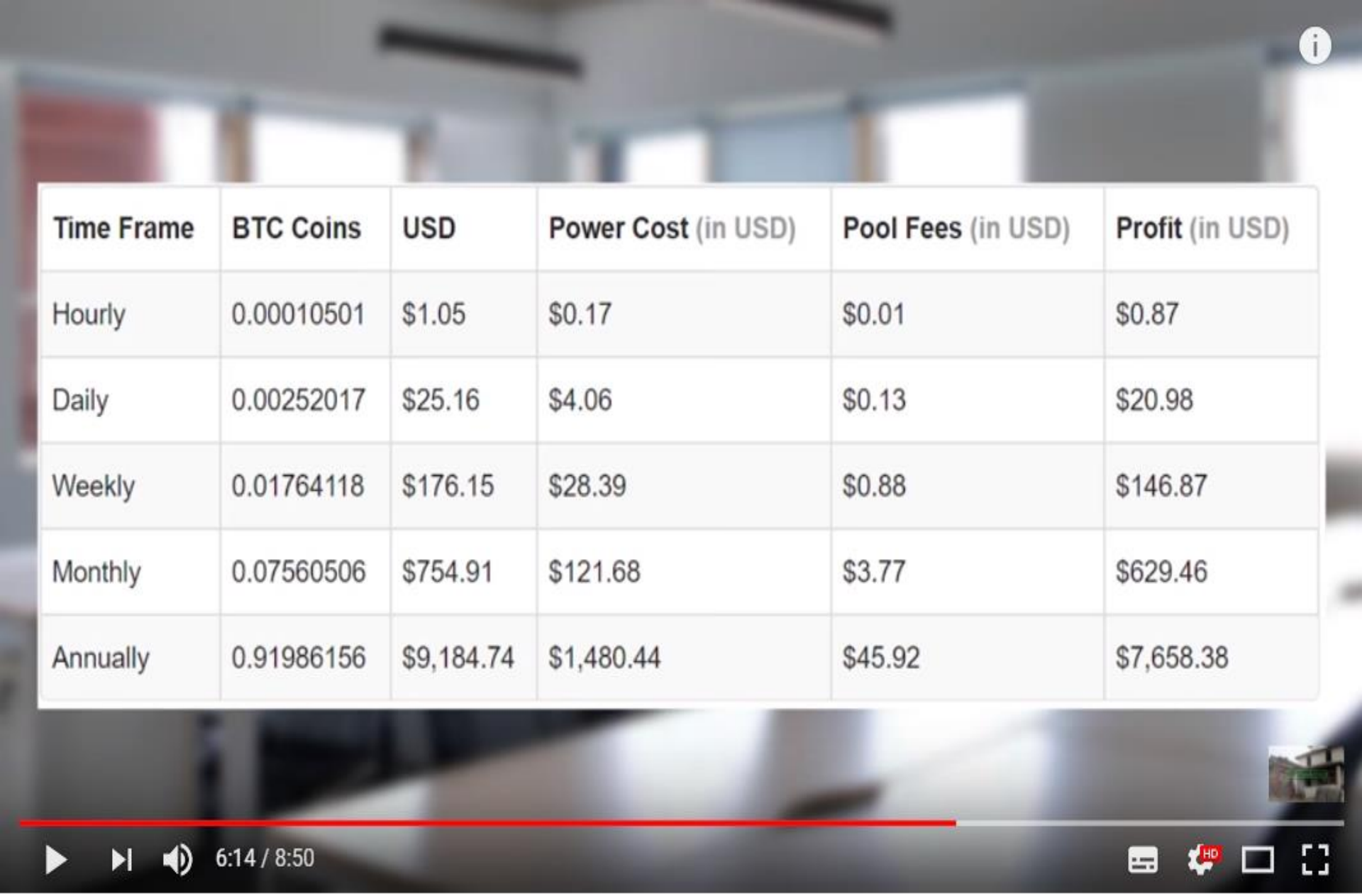
Statistiken von BTC.com

Life Inside a **Secret Chinese Bitcoin Mine**, 2015

Bitcoin Mining in December 2017 - Still **Profitable**?



Bitcoin Mining in December 2017 - Still **Profitable**?



Bitcoin Mining in December 2017 - Still **Profitable**?

Contracts | Hashing24 | Panel | HashFlare Cloud | Cloud Mining for Bitcoin | Send - Coinbase | CryptoCurrency Market

com/dashboard

Coinbase | Trading View | GDAX | Bittrex | Poloxiex | Calculator | Purse.io | Market | BitConnect | Hashing24 | Hashflare | Genesis Mining | Changelly | Steemit @CryptoNick | SteemDB | TCG

BOARD

he overview of the most recent data

DASHBOARD

MINING ALLOCATION

PAYOUTS

BONUS PAYOUTS

MY ACCOUNT

MY ORDERS

BUY HASHPOWER

66.4823 TH/s

Bitcoin

HASHRATE

13.0850 MH/s

Litecoin

HASHRATE

1010.4750 MH/s

Dash (X11)

HASHRATE

151.9875 MH/s

Ether

HASHRATE

0.0000 H/s

Zcash

HASHRATE

325.5000 H/s

Monero

HASHRATE

Mining Allocation

Allocate your hashpower

CONFIGURE MINERS

Buy Hashpower

Purchase more hashpower

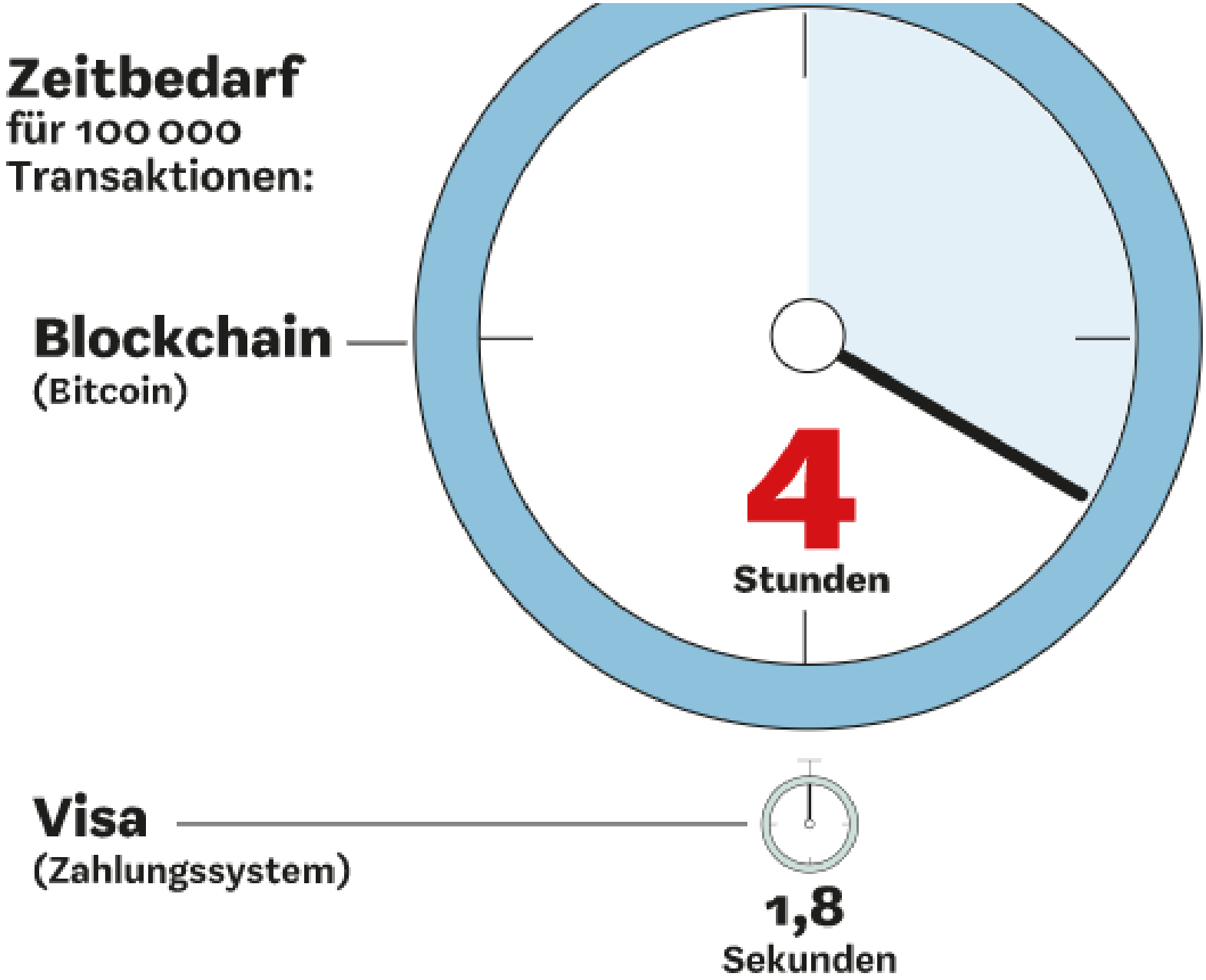
BUY HASHPOWER

Type here to search

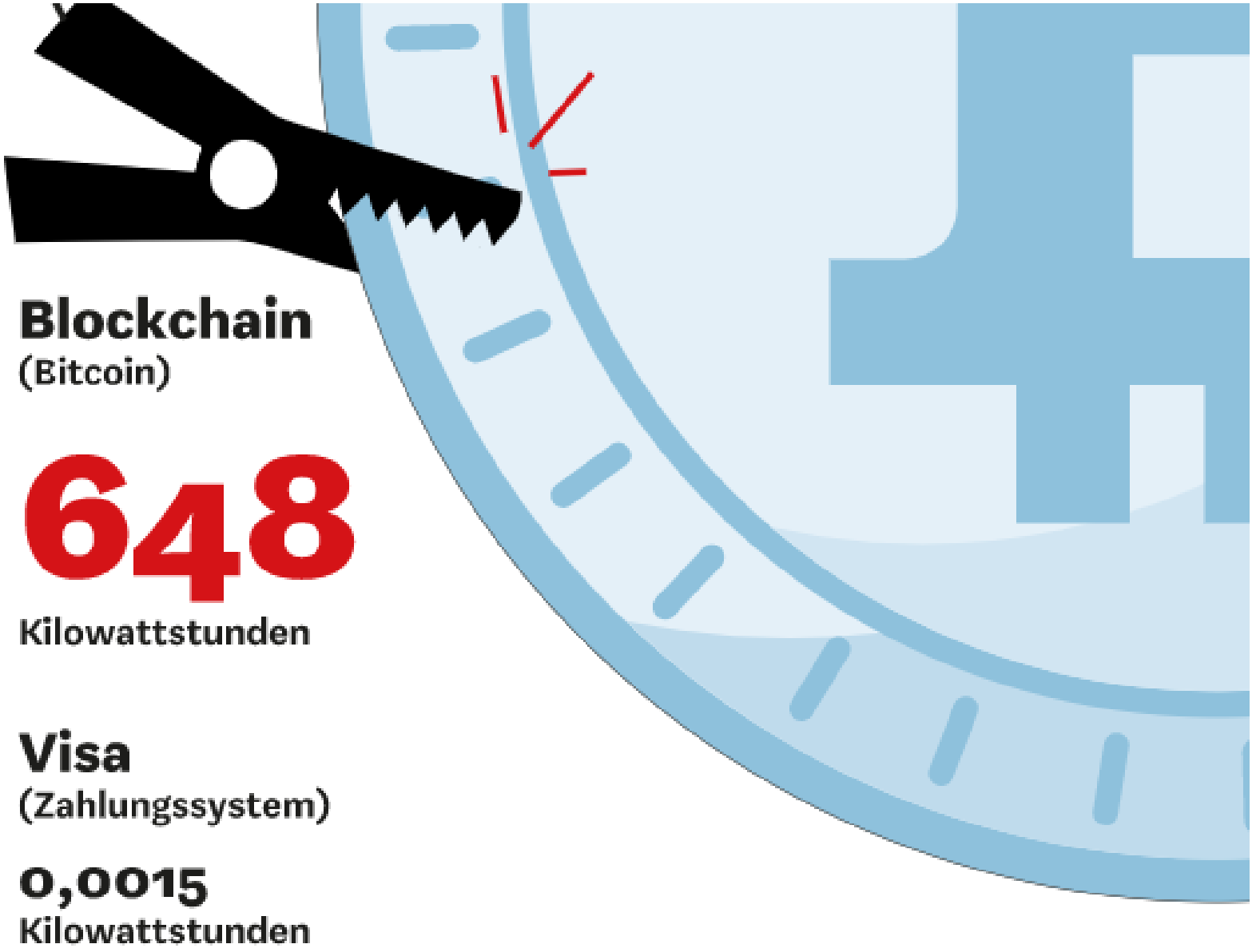
2:13 AM

7/5/2017

How I Earn $3500 Per Month Mining Cryptocurrency (7/2017)

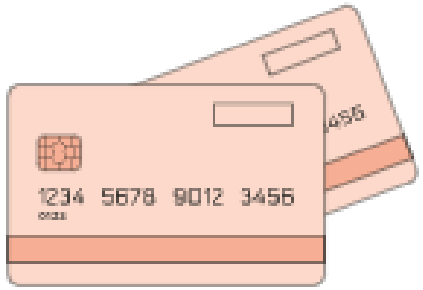


Laut WiWo 24.11.19: Wie viel Strom Bitcoin aktuell verbraucht



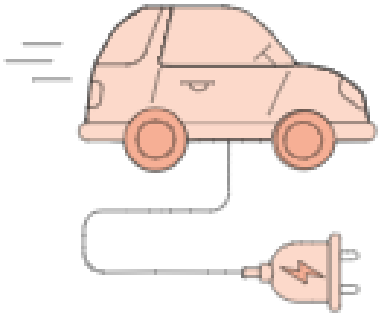
Laut WiWo 24.11.19: Wie viel Strom Bitcoin aktuell verbraucht

Was man mit 648 kWh Strom machen kann



429 000
Visa-Transaktionen

8,6 Jahre
einen Kühlschrank nutzen*



3240 km
mit einem E-Auto fahren**

Stand 13. November, Werte gerundet; * Gerät mit 290 Litern und 75 kWh Jahresverbrauch; ** bei einem Durchschnittsverbrauch von 20 kWh je 100 Kilometer
Grafik: Konstantin Megas; Multimedia-Umsetzung: Sebastian Feltgen
Quelle: Quellen: Bitcoin Energy Consumption Index, LSP Digital Research, Thomson Reuters, ADAC, Coindance, Defipulse, Bitcoinvisuals, Cambridge Center for Alternative Finance

Laut WiWo 24.11.19: Wie viel Strom Bitcoin aktuell verbraucht

Smart Contracts (Wikipedia)

Smart contract

From Wikipedia, the free encyclopedia

This article has multiple issues. Please help **improve it** or discuss these issues on the **talk page**. *(Learn how and when to remove these template messages)* [hide]

- This article **possibly contains original research**. *(December 2016)*
- This article's **factual accuracy is disputed**. *(August 2019)*

A **smart contract** is a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.[1][2][3][4] The objectives of smart contracts are the reduction of need in trusted intermediators, arbitrations and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions.[5][2]

Vending machines are mentioned as the oldest piece of technology equivalent to smart contract implementation.[3] 2014's white paper about the cryptocurrency Ethereum[6] describes the Bitcoin protocol as a weak version of the smart contract concept as defined by computer scientist, lawyer and cryptographer Nick Szabo. Since Ethereum, various cryptocurrencies support scripting languages which allow for more advanced smart contracts between untrusted parties.[7] Smart contracts should be distinguished from smart legal contracts. The latter refers to a traditional natural language legally-binding agreement which has certain terms expressed and implemented in machine-readable code.[8][9][10]