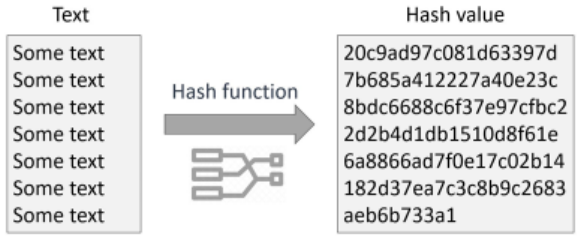
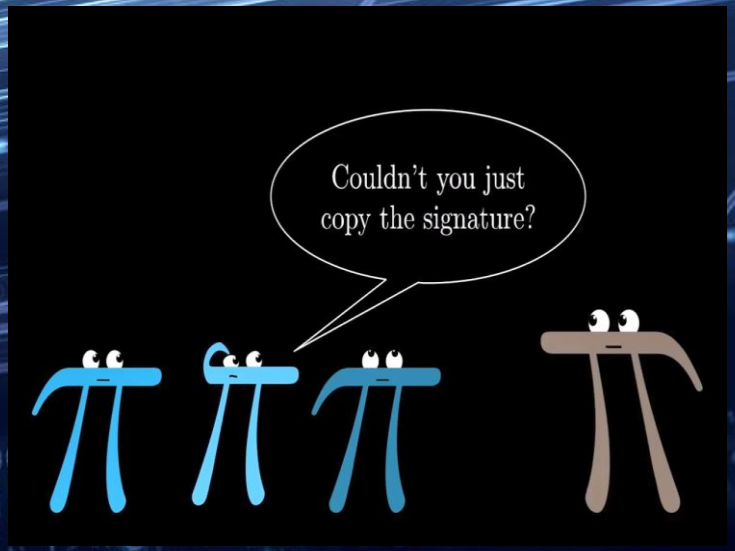
3 Protect Data
- Protecting the Security & Integrity of Data
(2) **Data Integrity with Encryption**

Eine **Hash-Funktion** erzeugt aus einem **beliebigen, langen Text** einen sog. **Hash-Wert fester Länge.**

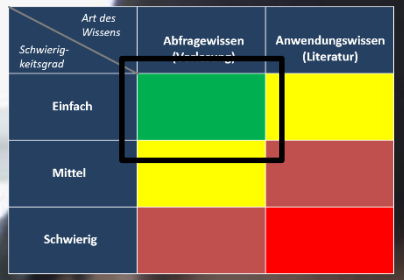


Kleinste **Änderungen** am **Text** führen zu deutlichen **Veränderungen** des **Hash-Wertes**.
Mit **Hash-Funktionen** kann man die **Integrität** von **Texten** prüfen.

19

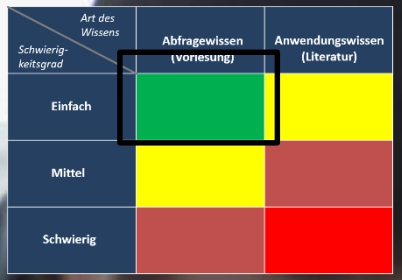


What is SHA-256?



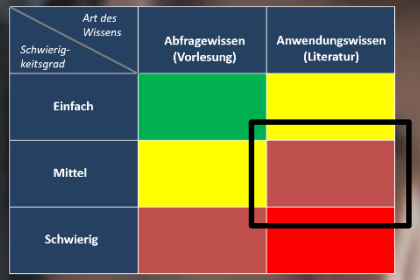
a) Hash value
b) Hash function
c) Hash database
d) Hash symbol
e) Hash text

Fill in the red box with the correct term.



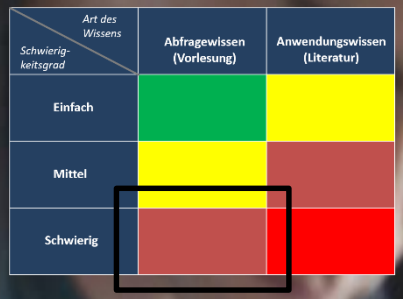
a) Hash Function
b) Hash Value
c) SHA-2
d) Hash Algorithm
e) Hash Application

If a previous digitally signed document is changed, ___ also changes.



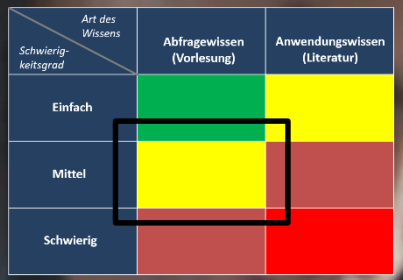
a) Public key
b) Hash value
c) Hash algorithm
d) Private key
e) All except hash algorithm

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



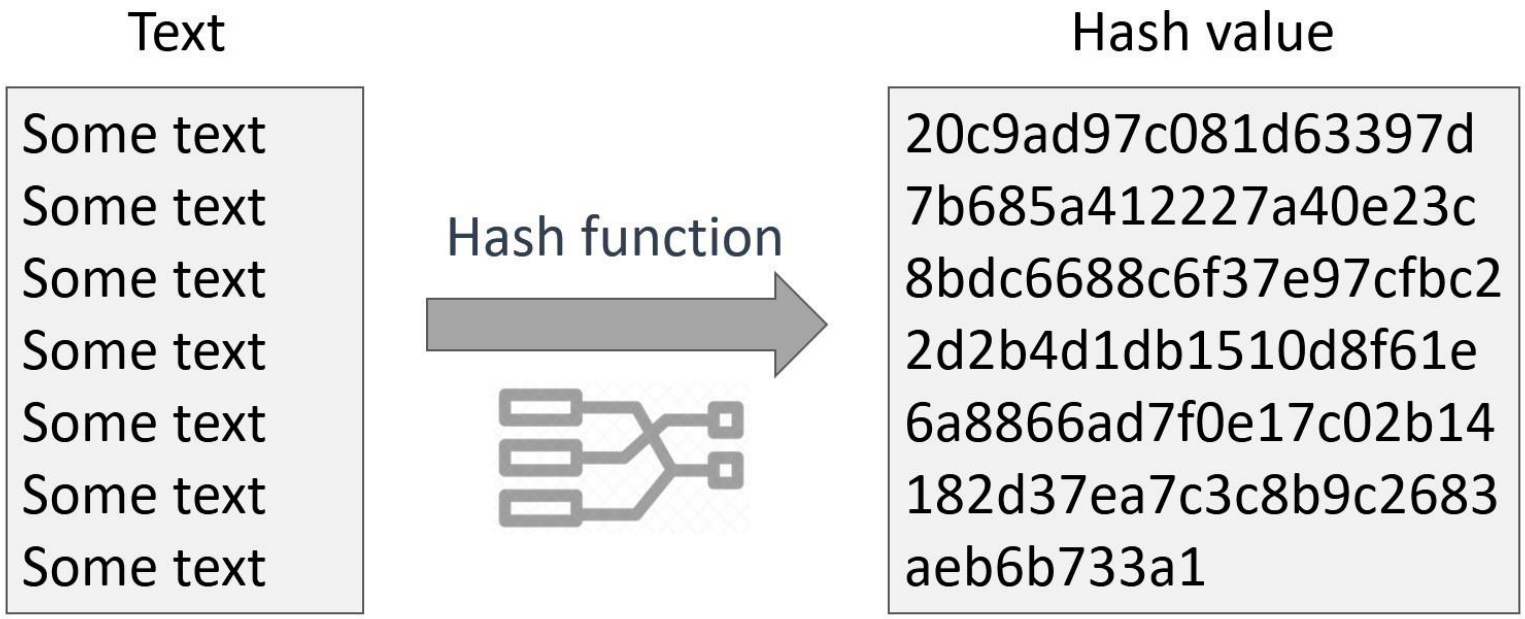
a) Hash function
b) Double-spending
c) Proof-of-work
d) CPU power
e) Bitcoin

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

Eine **Hash-Funktion** erzeugt aus einem **beliebigen, langen Text** einen sog. **Hash-Wert fester Länge.**



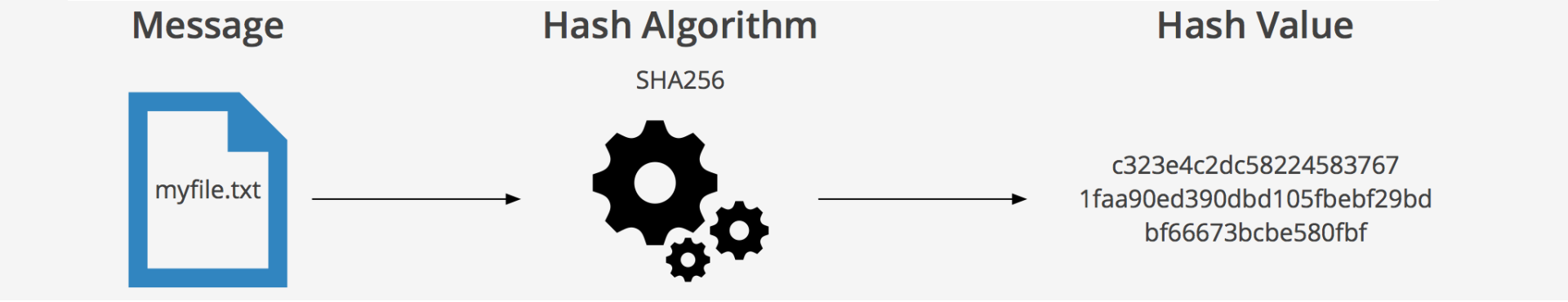
Kleinste **Änderungen** am **Text** führen zu deutlichen **Veränderungen** des **Hash-Wertes**.
Mit **Hash-Funktionen** kann man die **Integrität** von **Texten** prüfen.

Wikepedia zu SHA-256

SHA-2

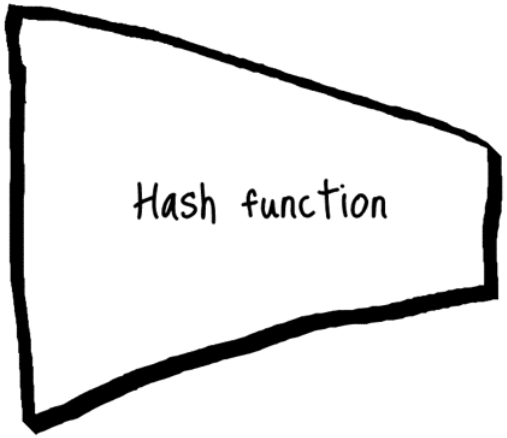
SHA-2 (von englisch *secure hash algorithm*, *sicherer Hash-Algorithmus*) ist der Oberbegriff für die kryptologischen Hashfunktionen **SHA-224**, **SHA-256**, **SHA-384**, **SHA-512**, **SHA-512/224** und **SHA-512/256**, die vom US-amerikanischen National Institute of Standards and Technology (NIST) als Nachfolger von SHA-1 standardisiert wurden.

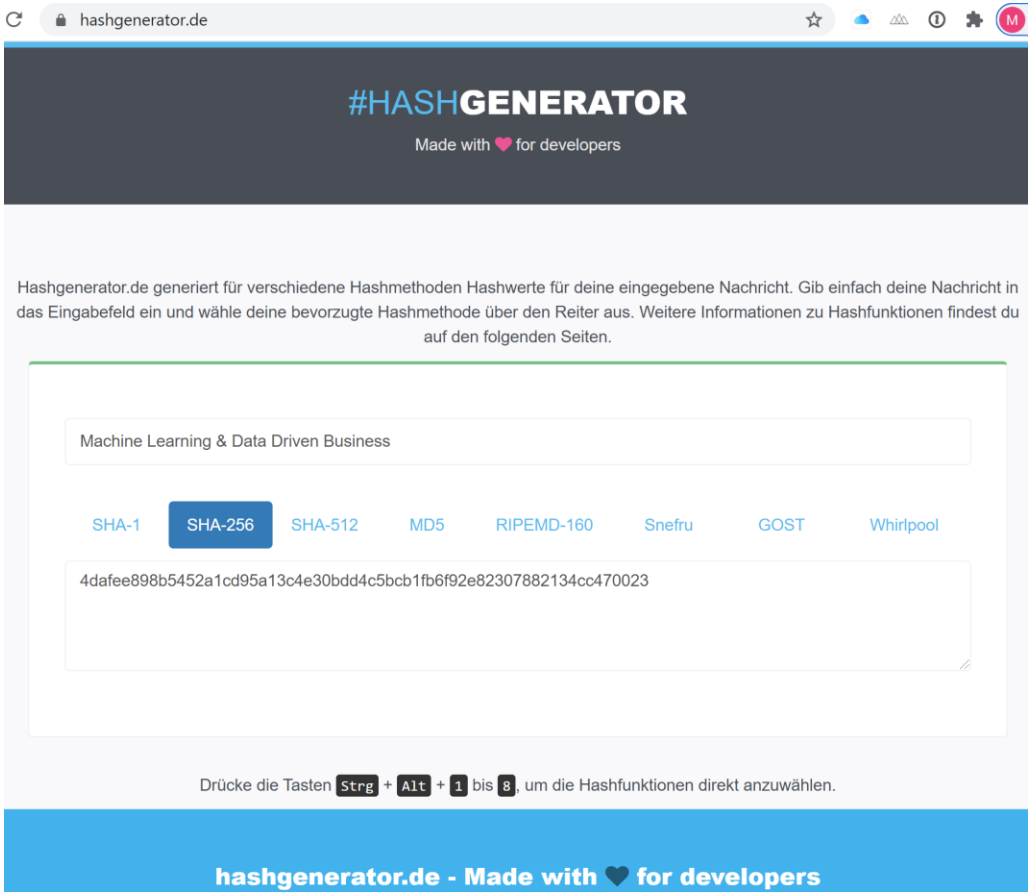
Inhaltsverzeichnis [Verbergen]



Die Hash-Funktion **SHA-256** (SHA: Secure Hash Algorithm) erzeugt **Hash-Werte** mit einer **Länge** von **256 Bit.**

SHA-256 Hash Generator



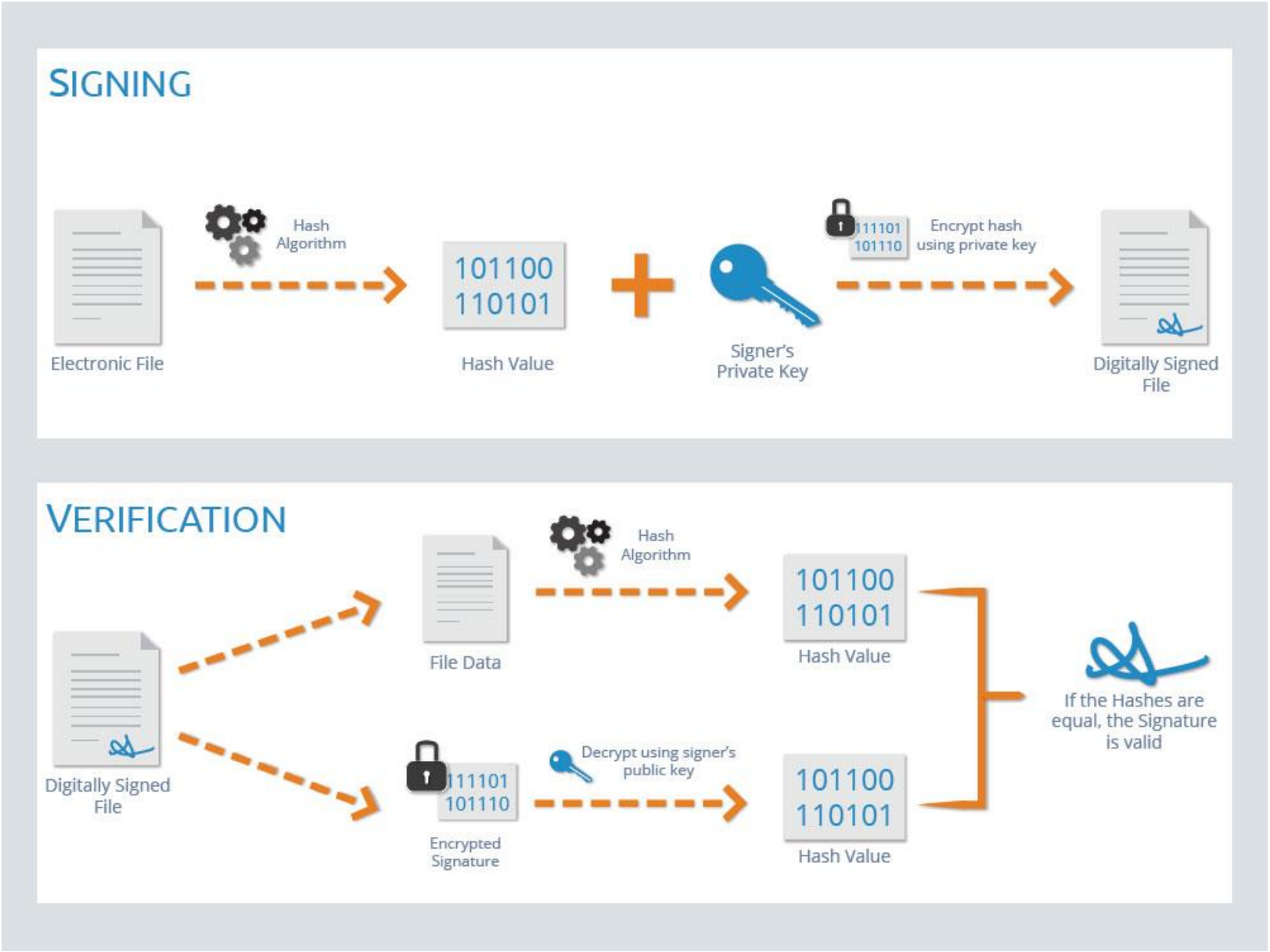


Hashgenerator.de

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)



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

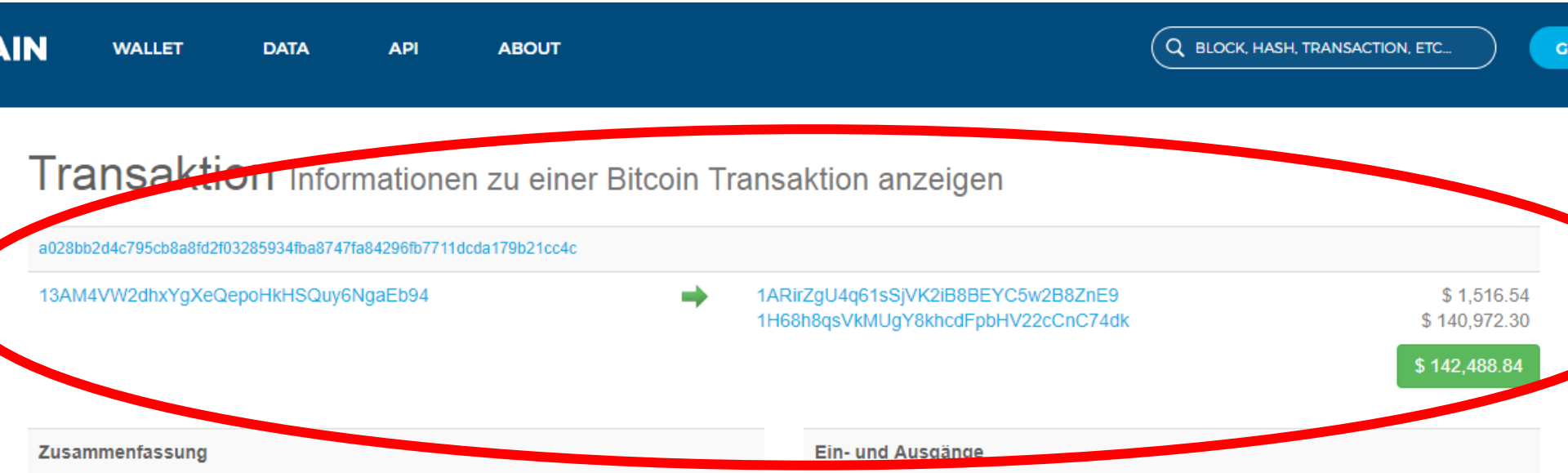
Zahlungsanfrage Spenden-Button

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**“)

Block #478789

Zusammenfassung	
Anzahl der Transaktionen	2359
Ausgang insgesamt	$ 1,206,937,377.37
Geschätztes Transaktionsvolumen	$ 102,176,632.18
Transaktions Gebühren	$ 31,717.68
Height	478789 (Hauptchain)
Zeitstempel	2017-08-03 03:39:15
Empfangene Zeit	2017-08-03 03:39:15
Weitergeleitet von	F2Pool
Schwierigkeit	860,221,984,436.22
Bits	402736949
Größe	1000.0 kB
Gewicht	3999.748 kWU
Version	0x20000012
Nonce	3623102768
Block Reward	$ 183,589.13

Hashes	
Hash	00000000000000000010b7b850ebea209fc1e693c113f4cf5e78456dd8842bb5a
Vorheriger Block	00000000000000000056b1869264b9825a767c6e139ddcefd4c888bef0eeabb5
Nächster Block	00000000000000000015430fd4a784b3e3cb541ff35fbf12271d7e2f8a81af6d
Merkle Root	04d88d28adcd88ee3b32be88899f315ab36a3c7db24dbf30e003955c2503e643

Transaktionen

842c80e199a9f9fb03fe0047f468d8f5802fc140d6b657d4428e16510df1736a 2017-08-03 03:39:15

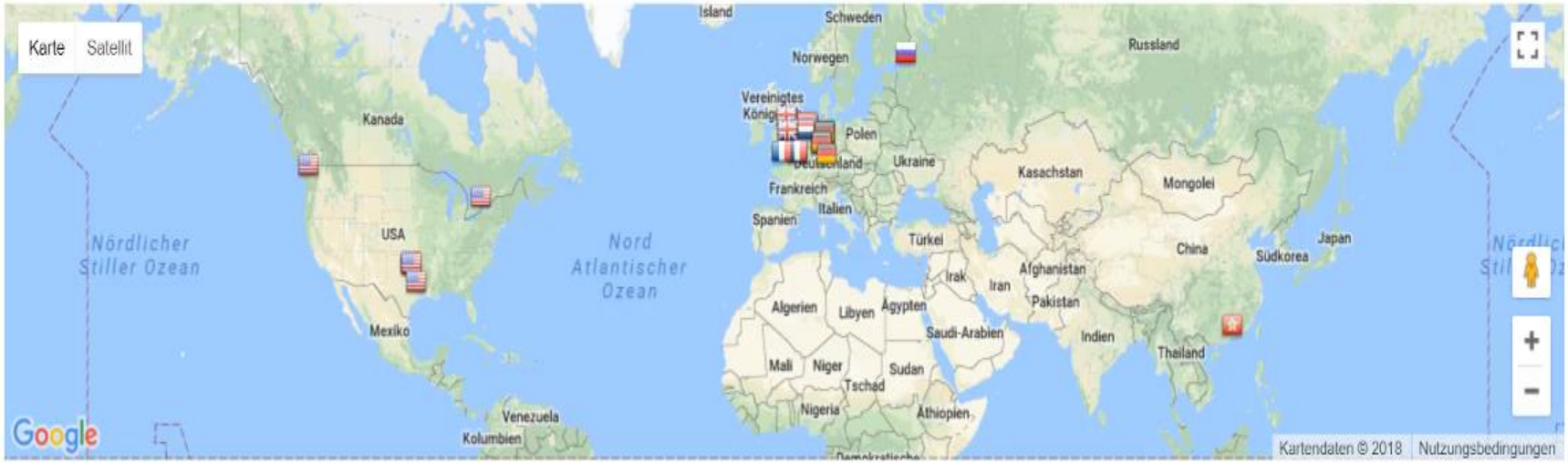
Wannacry, 12.5.2017 (Bitcoin-**Block** = ca. 2.500 **Transaktionen**)

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

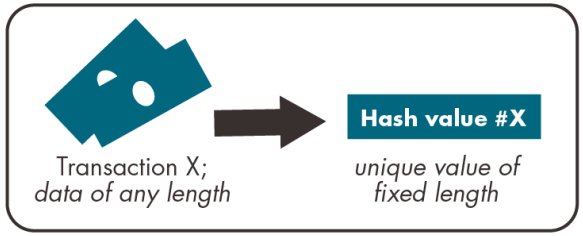
171056 unbestätigte Transaktionen Live aktualisierte Liste der aktuellen Bitcoin Transaktionen



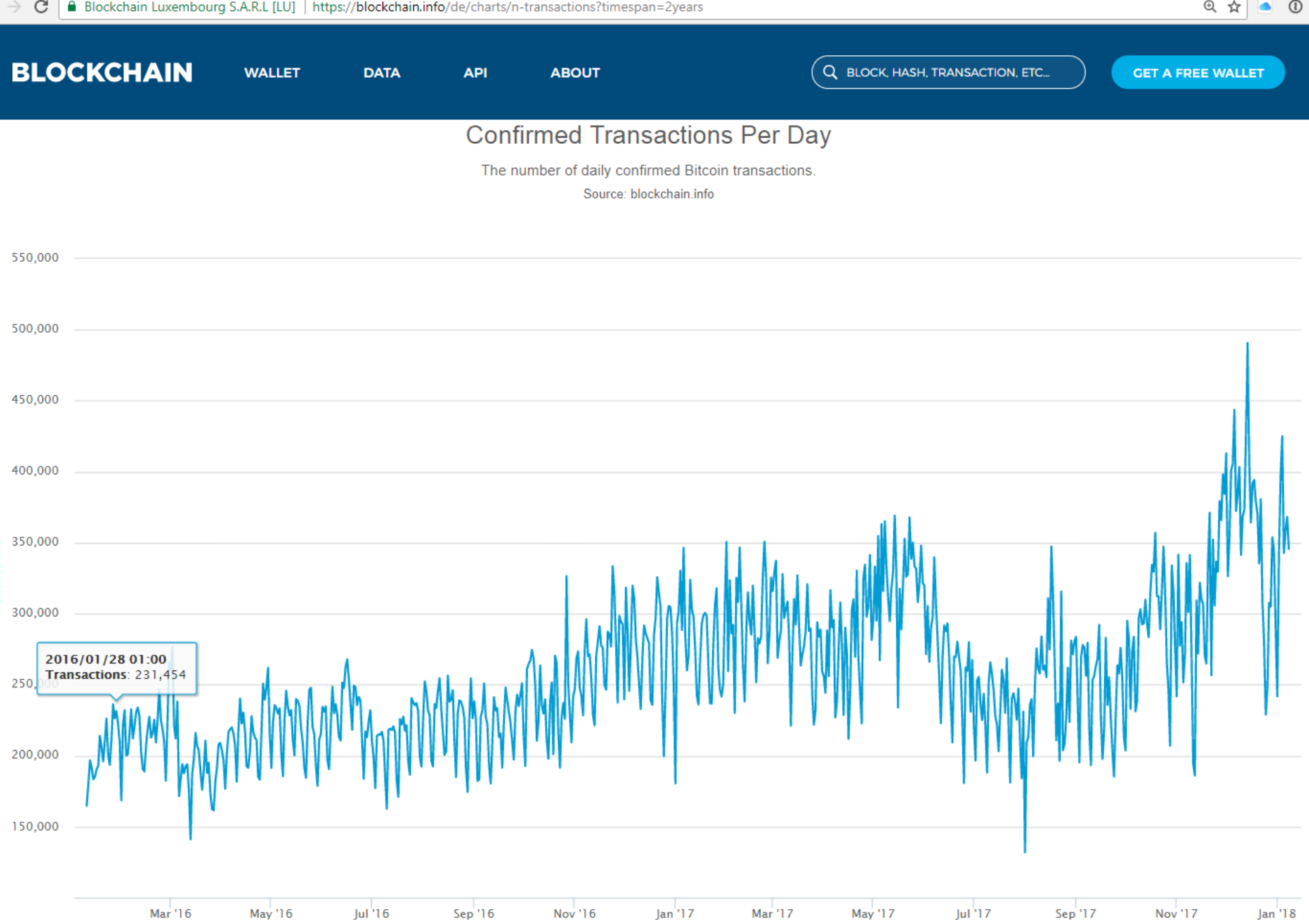
Zusammenfassung	Status: In Verbindung gebracht
Gebühren, gesamt	72.23228052 BTC

DEU 18:35
DE 08.01.2018

HOW THE BLOCKCHAIN WORKS



Reproduction of an original figure in "The Great Chain of Being Sure About Things" by the Economist



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.

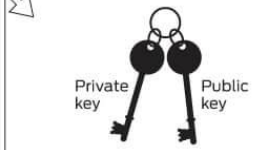
Wallets are files that provide access to multiple Bitcoin addresses.

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.

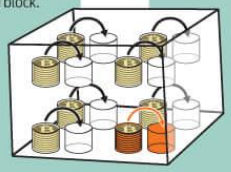
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

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

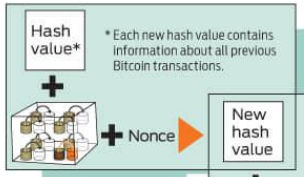
VERIFYING THE TRANSACTION

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.

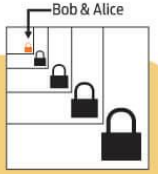
The root of all evil ???	0000 0000 0000 ...

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

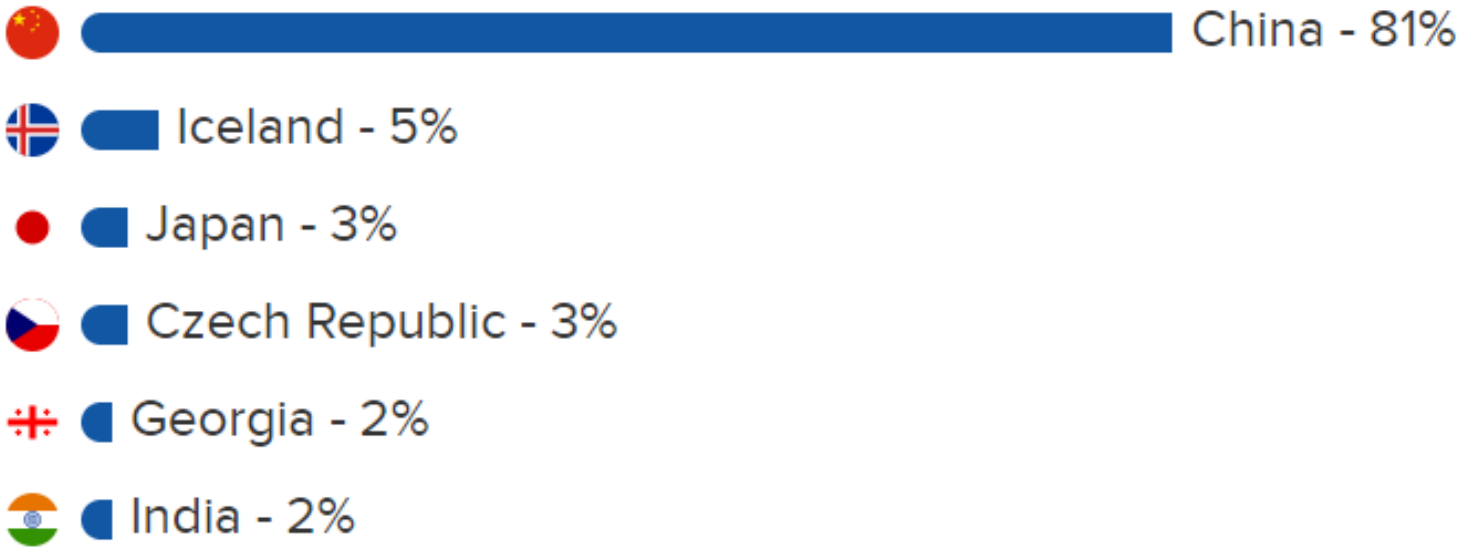


As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat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

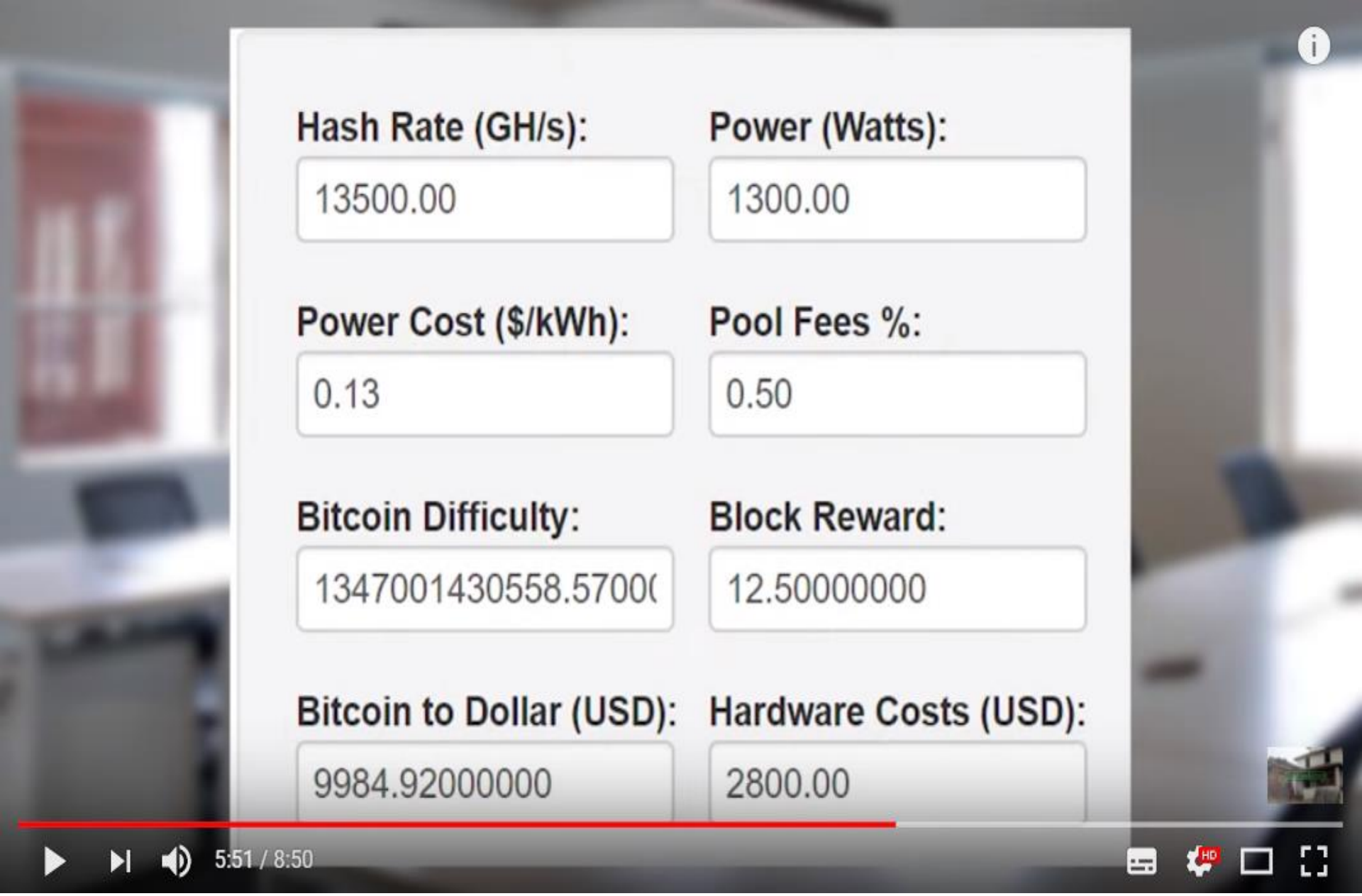
Pool Concentration in China

Before we get into the best mining pools to join, it's important to note that most mining pools are in China. Many only have Chinese websites and support. Mining centralization in China is one of Bitcoin's biggest issues at the moment.

There are about 20 major mining pools. Broken down by the percent of hash power controlled by a pool, and the location of that pool's company, we estimate that Chinese pools control ~81% of the network hash rate:



Statistiken von www.buybitcoinworldwide.com



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