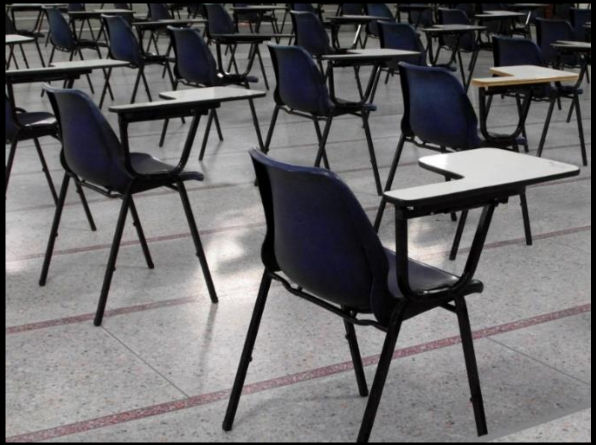
How Bitcoin works

Dr.-Ing. Markus A. Stulle, Munich | markus@stulle.ai // stulle.ai

What we are exploring together today

1. Past and present: History of money
2. Distributed systems – Can we do without a bank?
3. The Bitcoin blockchain
4. Asymmetrical cryptography
5. The Bitcoin payment system
6. Bitcoin in practice
7. Future



Source of the pictures in this lecture: [pixabay.com]
Public Domain according to: [Creative Commons CC0]
Source of screenshots: [Stulle]

Money in the past 125 years

- First publication of Dow Jones Index (May 26, 1896)
- German Inflation (1914 – November 1923)
- Black Thursday (October 24, 1929)
- Bretton Woods (1944 – 1973)
- European Monetary System, ECU (1979 – 1998)
- European Exchange Rate Mechanism, Euro (January 1, 1999)
- Bankruptcy Lehman Brothers (September 15, 2008)
- [Paper] „Bitcoin: A Peer-to-Peer Electronic Cash System" published by Satoshi Nakamoto (November 1, 2008)

A child of crisis!

German Notgeld (February 15, 1924)

Gold standard

- Mark, 1871 – 4. August 1914
- Pound Sterling, until September 19, 1931
- US-Dollar, until 1933

- No link between gold standard, stable prices and economic growth [Robert Whaples]

One Hundred Dollars Gold Certificate, Thomas Hart Benton (1922)

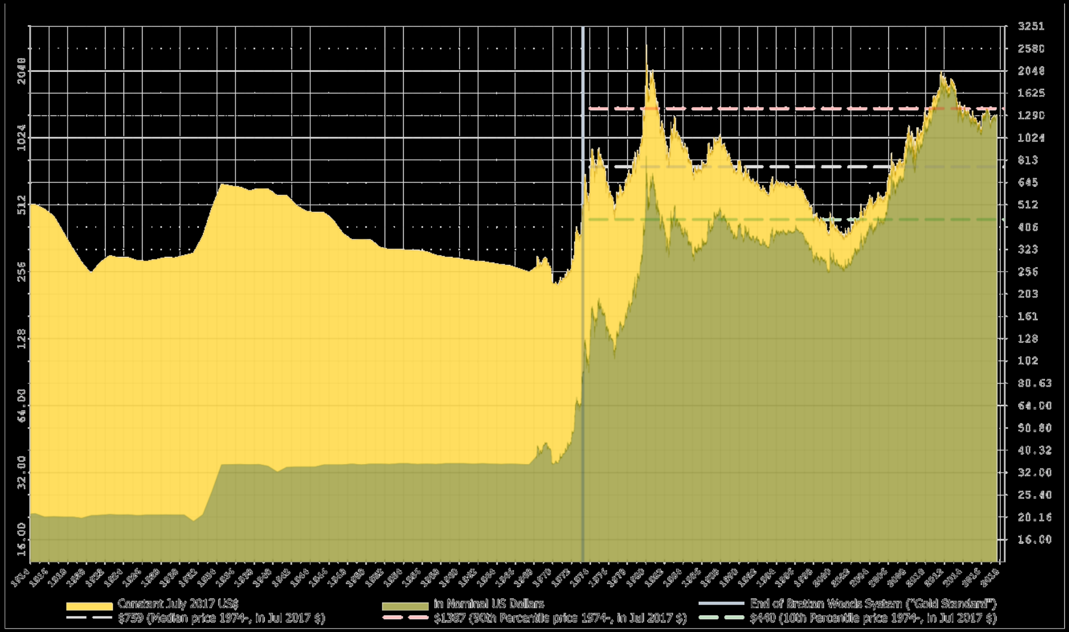
Five Dollars Federal Reserve Note, Abraham Lincoln (1928)

Fiat money

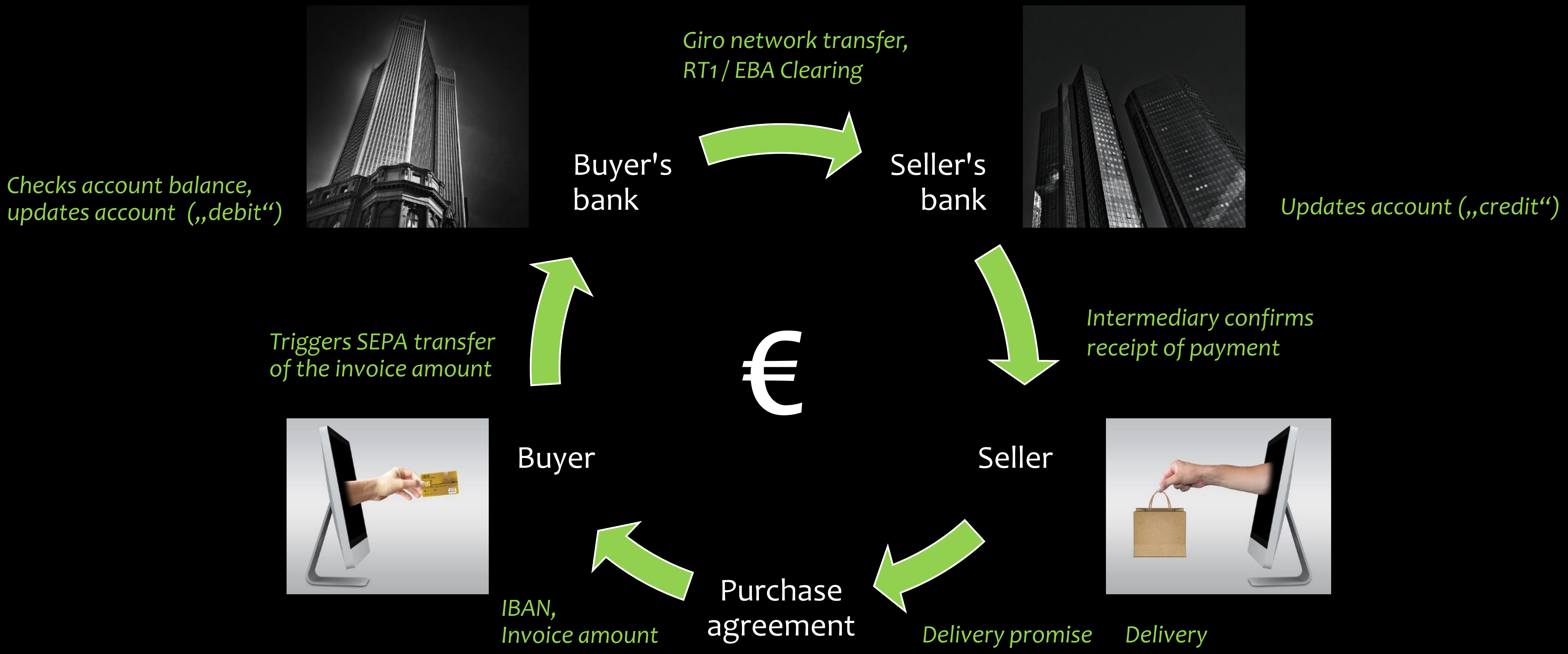
- „Fiat lux!“
- Object with *no intrinsic value*
- The *external value* is based on usefulness – as with crypto currencies
- Trust in central banks?
- Allows money creation in any amount, inflation!
- Nominal increase in gold price from 1974 to July 2017 from $ 440 to $ 1387

Intrinsic value = sourcing costs: 10.9 Cent

FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
E 34112707 E
WASHINGTON, D.C.
E
ONE
SERIES 2003
Treasurer of the United States.
Secretary of the Treasury.
WASHINGTON
ONE DOLLAR
1
5
C2
C77



Payment transaction with an intermediary



Buyer

IBAN,
Invoice amount

Purchase agreement

Triggers SEPA transfer of the invoice amount

Buyer's bank

Checks account balance, updates account („debit“)

Giro network transfer, RT1 / EBA Clearing

Seller's bank

Updates account („credit“)

Intermediary confirms receipt of payment

Seller

Delivery

Delivery promise

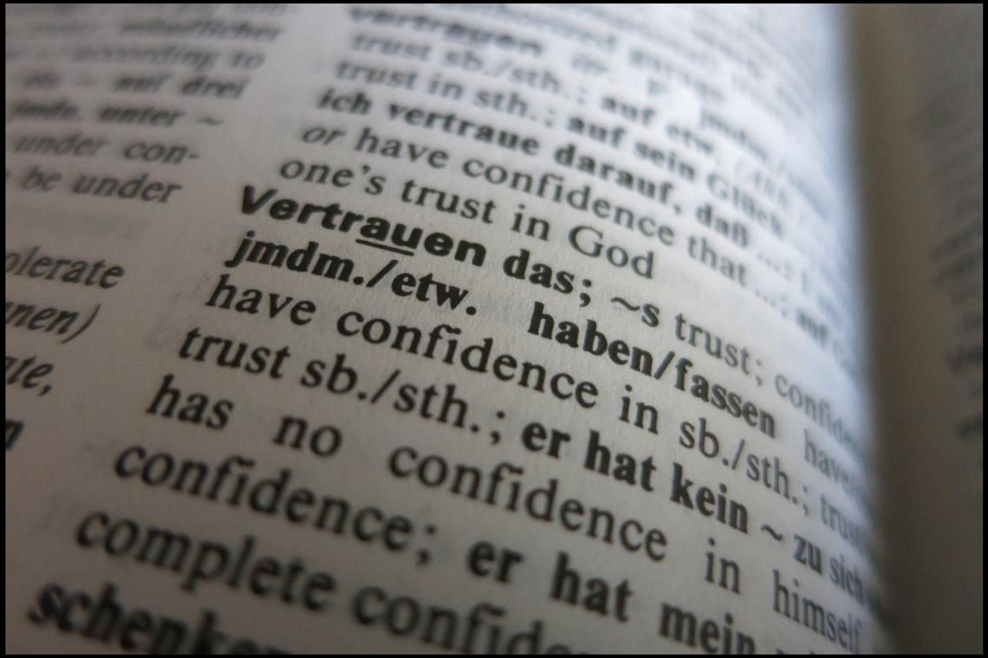
€

Who trusts whom?

- Prepayment – the buyer trusts the seller: *Does he keep his delivery promise?*
- Both parties trust their banks
- Banks among themselves!

Central ledger managed
by the buyer's bank
prevents Double-Spending

Buyer can only spend money once!



trust sb./sth.
trust in sth.; auf etw.
ich vertraue darauf, daß
or have confidence that
one's trust in God
Vertrauen das; ~s trust; confi-
jmdm./etw. haben/fassen
have confidence in sb./sth.;
trust sb./sth.; er hat kein ~ zu sich
has no confidence in himself
confidence; er hat mein
complete confid-

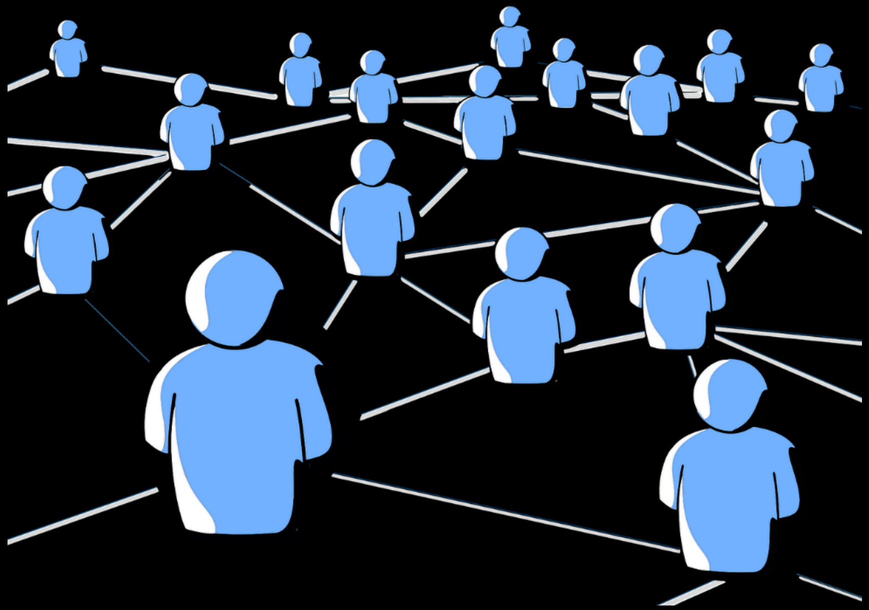
What we are exploring together today

1. Past and present: History of money
2. Distributed systems – Can we do without a bank?
3. The Bitcoin blockchain
4. Asymmetrical cryptography
5. The Bitcoin payment system
6. Bitcoin in practice
7. Future

Source of the pictures in this lecture: [pixabay.com]
Public Domain according to: [Creative Commons CC0]
Source of screenshots: [Stulle]

Peer-to-Peer Networking (P2P)

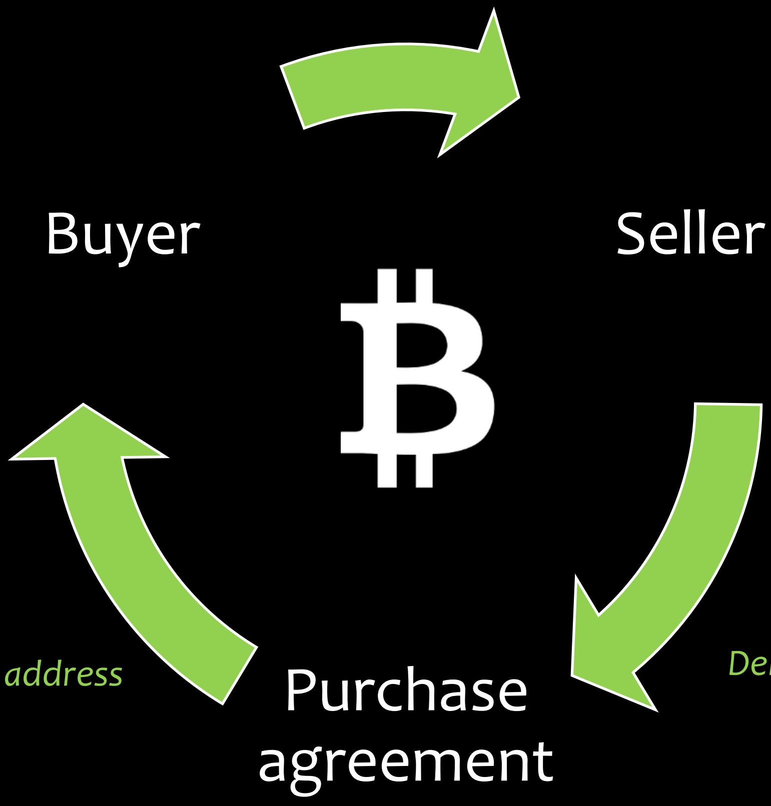
- Computers of unknown owners communicate via Internet protocols (TCP/IP)
- No controlling authority, no server
  – but that also means: No user service!
- Default setting: Suspicion
- Challenge: Identify evil intentions, find consensus
- Application file sharing:
  Napster (1999), Gnutella (2000), BitTorrent (2001)
- Application anonymization: Tor (2002)



Payment transaction w/o intermediary

Create Transaction
using the wallet

Processing of transaction
through P2P network



Seller finds transaction
in the blockchain

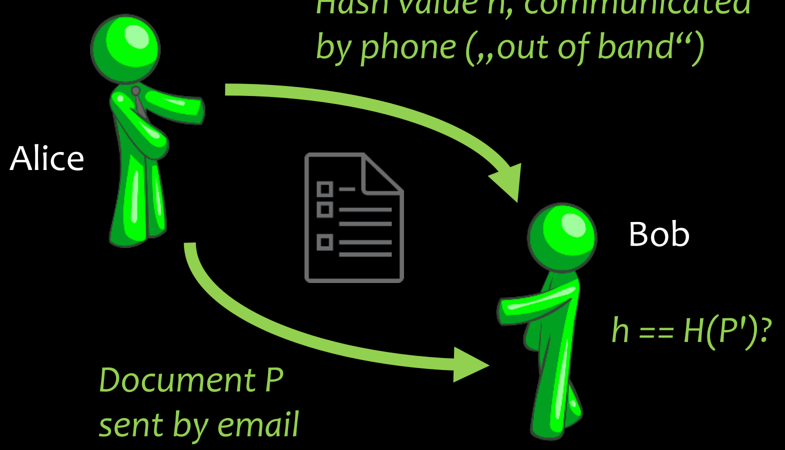
Delivery

Delivery promise

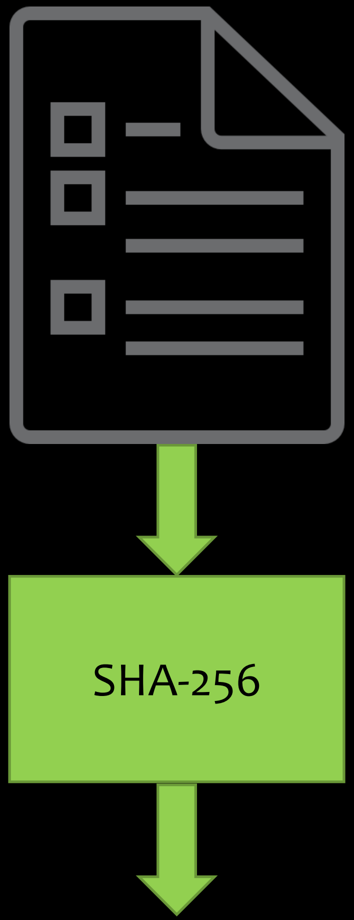
Instead of IBAN: Bitcoin address
Invoice amount

Basis: *Hash function*

- Function *h = H(P)* returns „fingerprint“ of Document *P*
- One-way function
- Characteristic: even small changes to *P* lead to major changes to *h* – high entropy, mathematical chaos



Document P, (almost) arbitrarily large

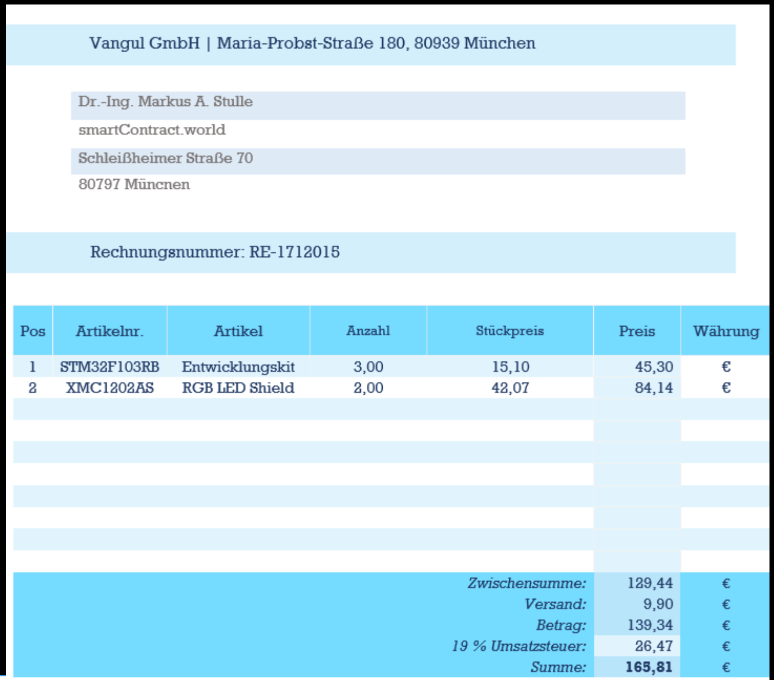


Hash value h, constant size of 32 bytes

```
e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24
27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55
```

VIVA Aspect *Integrity*

- VIVA Aspects of information security – Confidentiality, Integrity, Availability, Authenticity
- Definition of *Hash Puzzle* –
  Modify document *P* such that
  the value of the hash function *H(P)*
  fulfills a criterion, e.g. $h < h_c$



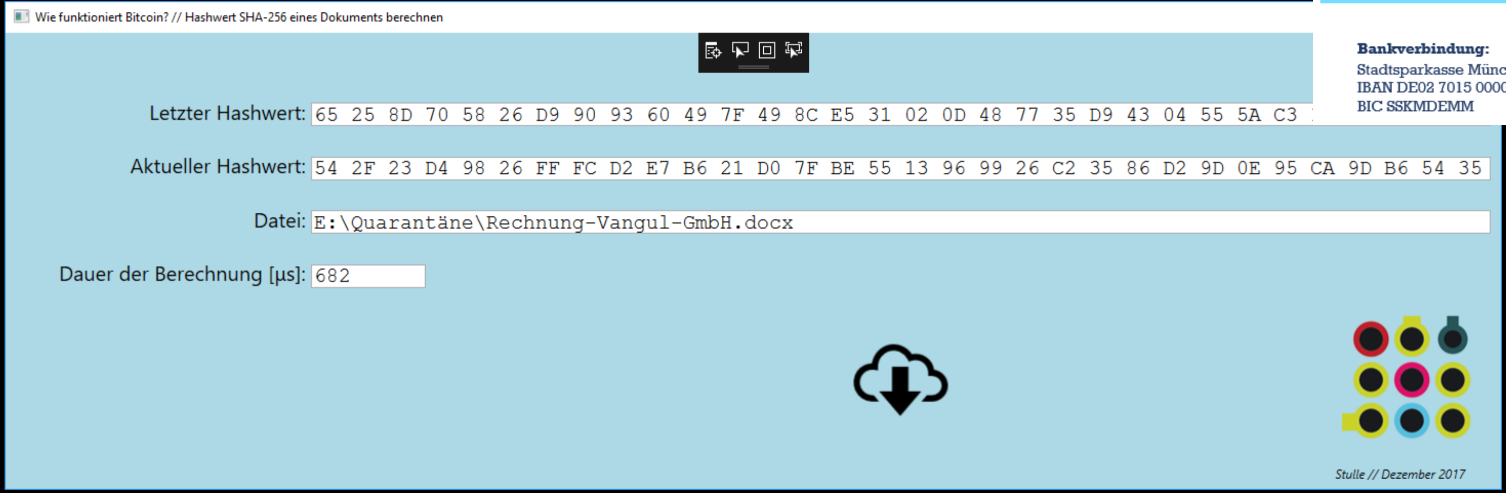
Vangul GmbH | Maria-Probst-Straße 180, 80939 München

Dr.-Ing. Markus A. Stulle
smartContract.world
Schleißheimer Straße 70
80797 Müncnen

Rechnungsnummer: RE-1712015

Pos	Artikelnr.	Artikel	Anzahl	Stückpreis	Preis	Währung
1	STM32F103RB	Entwicklungskit	3,00	15,10	45,30	€
2	XMC1202AS	RGB LED Shield	2,00	42,07	84,14	€
				Zwischensumme:	129,44	€
				Versand:	9,90	€
				Betrag:	139,34	€
				19 % Umsatzsteuer:	26,47	€
				Summe:	**165,81**	€

Bankverbindung:
Stadtsparkasse München
IBAN DE02 7015 0000 0000 5949 37
BIC SSKMDEMM



Wie funktioniert Bitcoin? // Hashwert SHA-256 eines Dokuments berechnen

Letzter Hashwert: 65 25 8D 70 58 26 D9 90 93 60 49 7F 49 8C E5 31 02 0D 48 77 35 D9 43 04 55 5A C3

Aktueller Hashwert: 54 2F 23 D4 98 26 FF FC D2 E7 B6 21 D0 7F BE 55 13 96 99 26 C2 35 86 D2 9D 0E 95 CA 9D B6 54 35

Datei: E:\Quarantäne\Rechnung-Vangul-GmbH.docx

Dauer der Berechnung [µs]: 682

Stulle // Dezember 2017

Document P has been transferred unchanged?

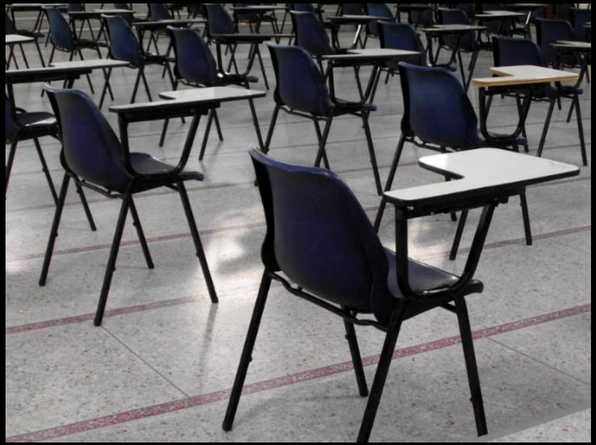
[github.com/relianz/HashGui]

Excursus: *Big natural numbers*

Power of 10	Examples
10^{12} *Trillion*	Germany's **national debt** amounts to € 2.1 trillion (2016) There are about 3 trillion **trees** on Earth **Proxima Centauri** is 39.7 trillion kilometres from Earth (4.24 ly)
10^{27} *Octillion*	A **human being** (= 70 kilograms of water) consists of 7 octillion atoms
10^{78} *Quinquavigintillion*	Number of **SHA-256** hash puzzle options Maximum number of private **bitcoin keys** The **universe** known to us contains 10^{79} = 10 quinquavigintillion of atoms
10^{231}	Modulus n = p·q of the public part of a 768 Bit **RSA key** 4194710539436274208221193987350677135843701756369167540803125688386 000805925985894892042570501977600226811988347329905923326168042471 468173843602232900103487295396441373050508162027365351286097330880 04576046110570456189513172669412

What we are exploring together today

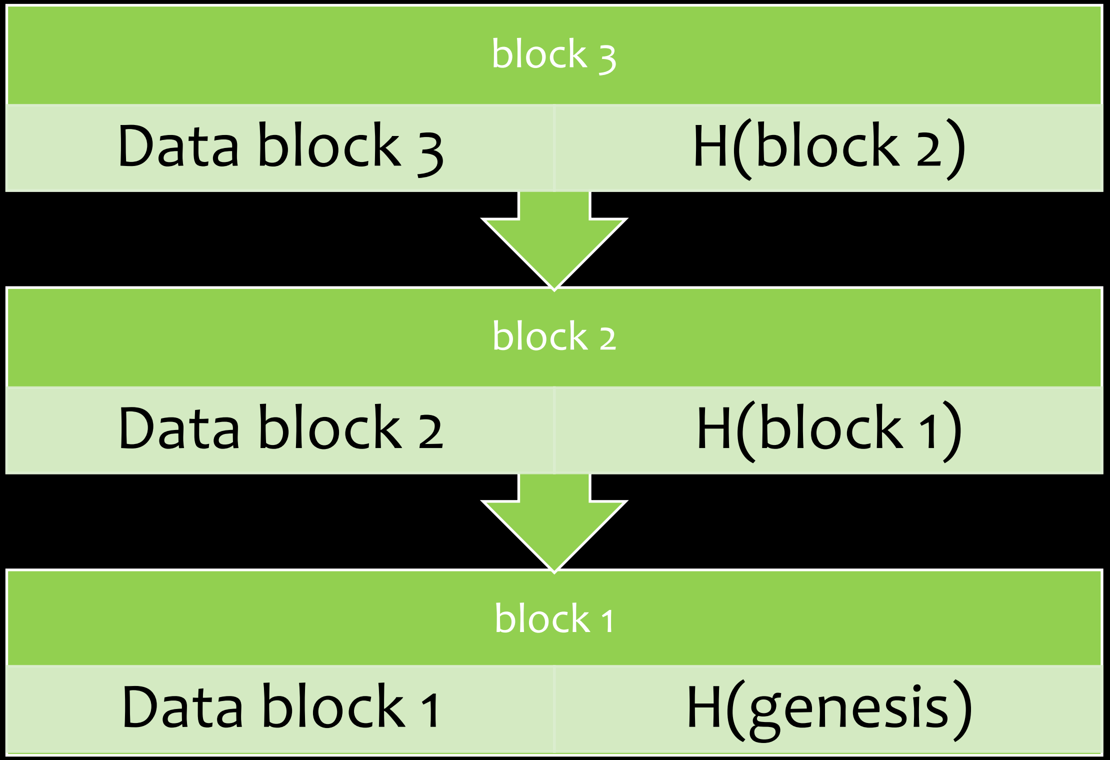
1. Past and present: History of money
2. Distributed systems – Can we do without a bank?
3. The Bitcoin blockchain
4. Asymmetrical cryptography
5. The Bitcoin payment system
6. Bitcoin in practice
7. Future



Source of the pictures in this lecture: [pixabay.com]
Public Domain according to: [Creative Commons CC0]
Source of screenshots: [Stulle]

Hash function app: *The Blockchain*

- *Well known:*
  Storing data in blocks
- *New (1991, Haber/Stornetta):*
  Each block contains the hash value of its predecessor!
- The smaller the block number, the more expensive manipulations
- Bitcoin blockchain
  Height > 512.000 blocks à 1 MB, about 2.000 transactions / block
- Blocks also contain Proof-of-Work = valuable result of hash puzzle



Live data: [blockchain.info]

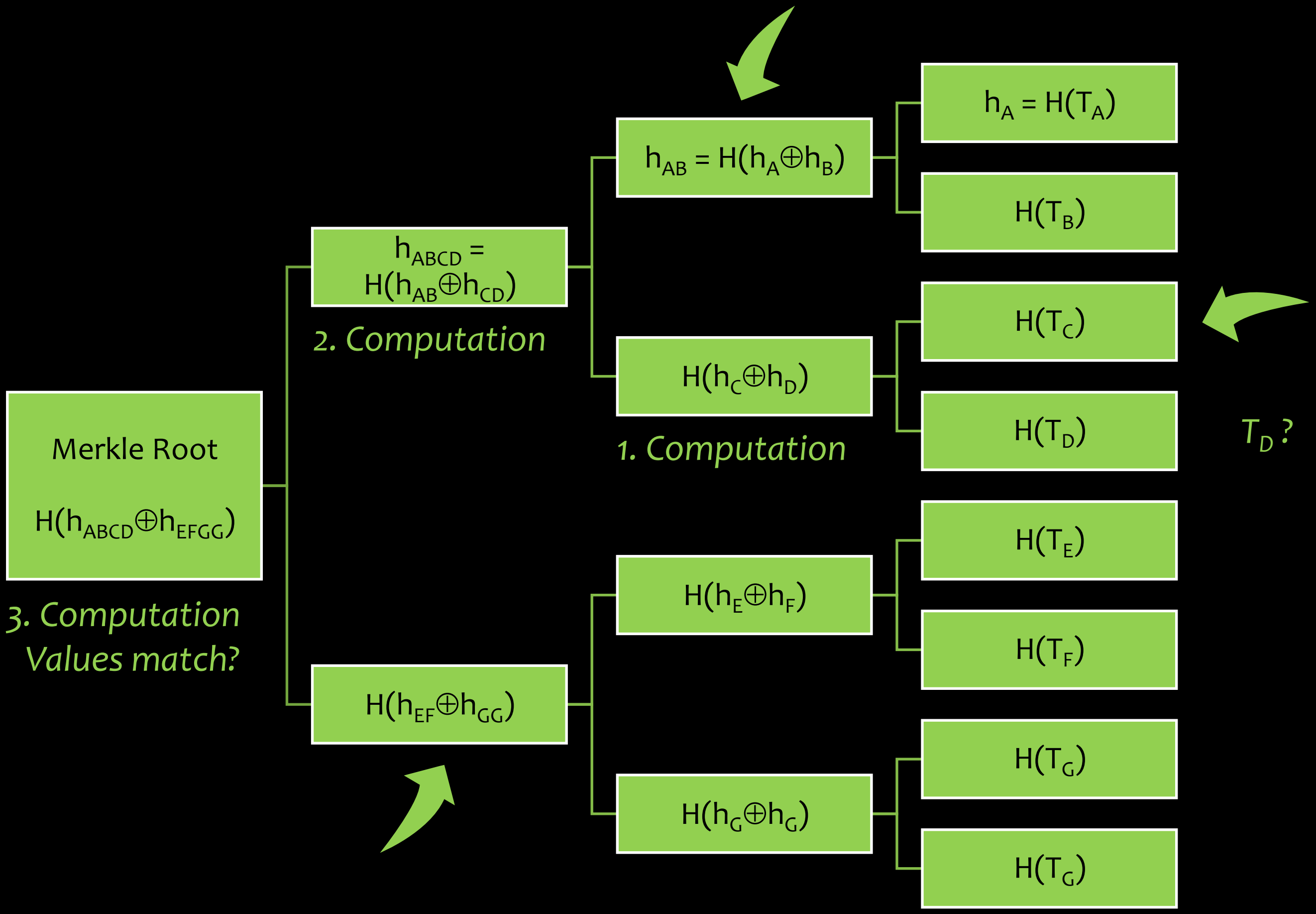
Checking integrity quickly: *Merkle Tree*

- *Objective:*
  Efficient verification of the Membership of a transaction T_x in a block („Audit Proof“)

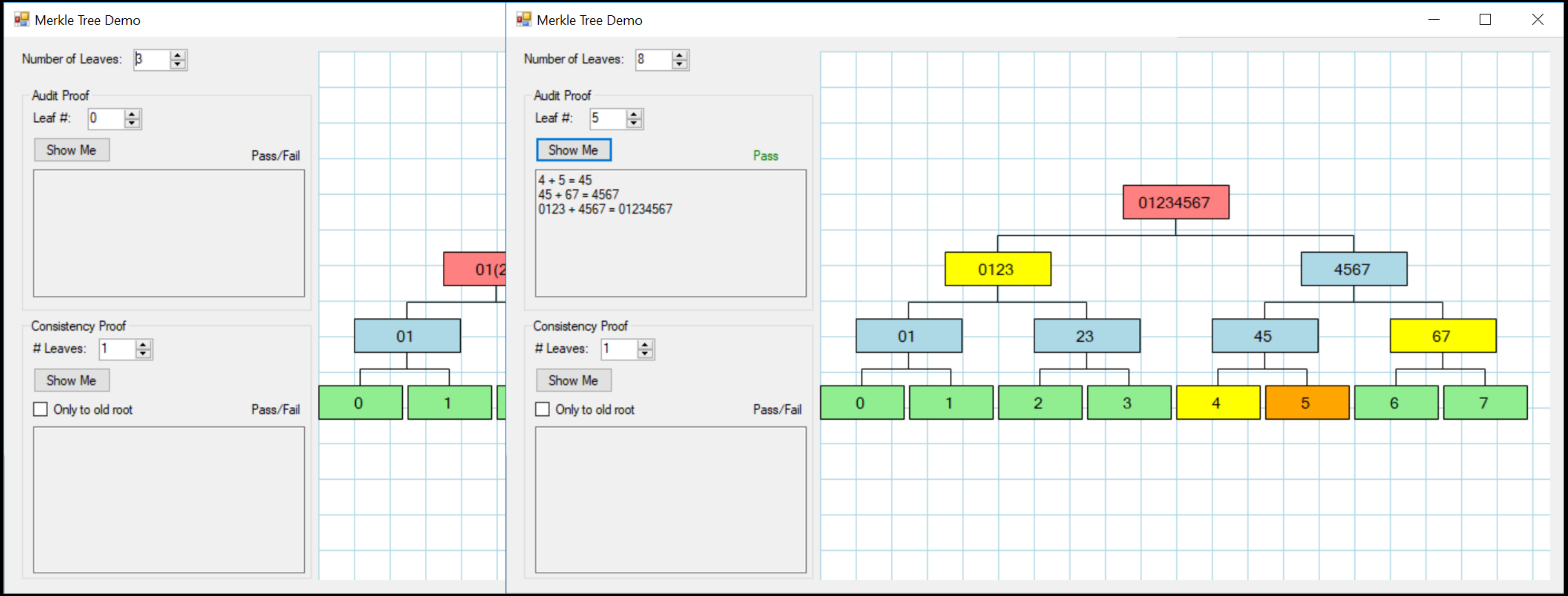
- *Idea:*
  Header of the block contains Binary hash tree

- *Feature:*
  Check for T_x with n transactions requires $\leq 2 \cdot \log_2(n)$ computations

- *Other applications:*
  Git, Oracle Btrfs, IPFS, ZFS



Merkle Tree: *Sample implementation* (C#)



Merkle Tree Demo

Number of Leaves: 3

Audit Proof

Leaf #: 0

Pass/Fail

Consistency Proof

Leaves: 1

□ Only to old root

Pass/Fail

Merkle Tree Demo

Number of Leaves: 8

Audit Proof

Leaf #: 5

Pass

```
4 + 5 = 45
45 + 67 = 4567
0123 + 4567 = 01234567
```

Consistency Proof

Leaves: 1

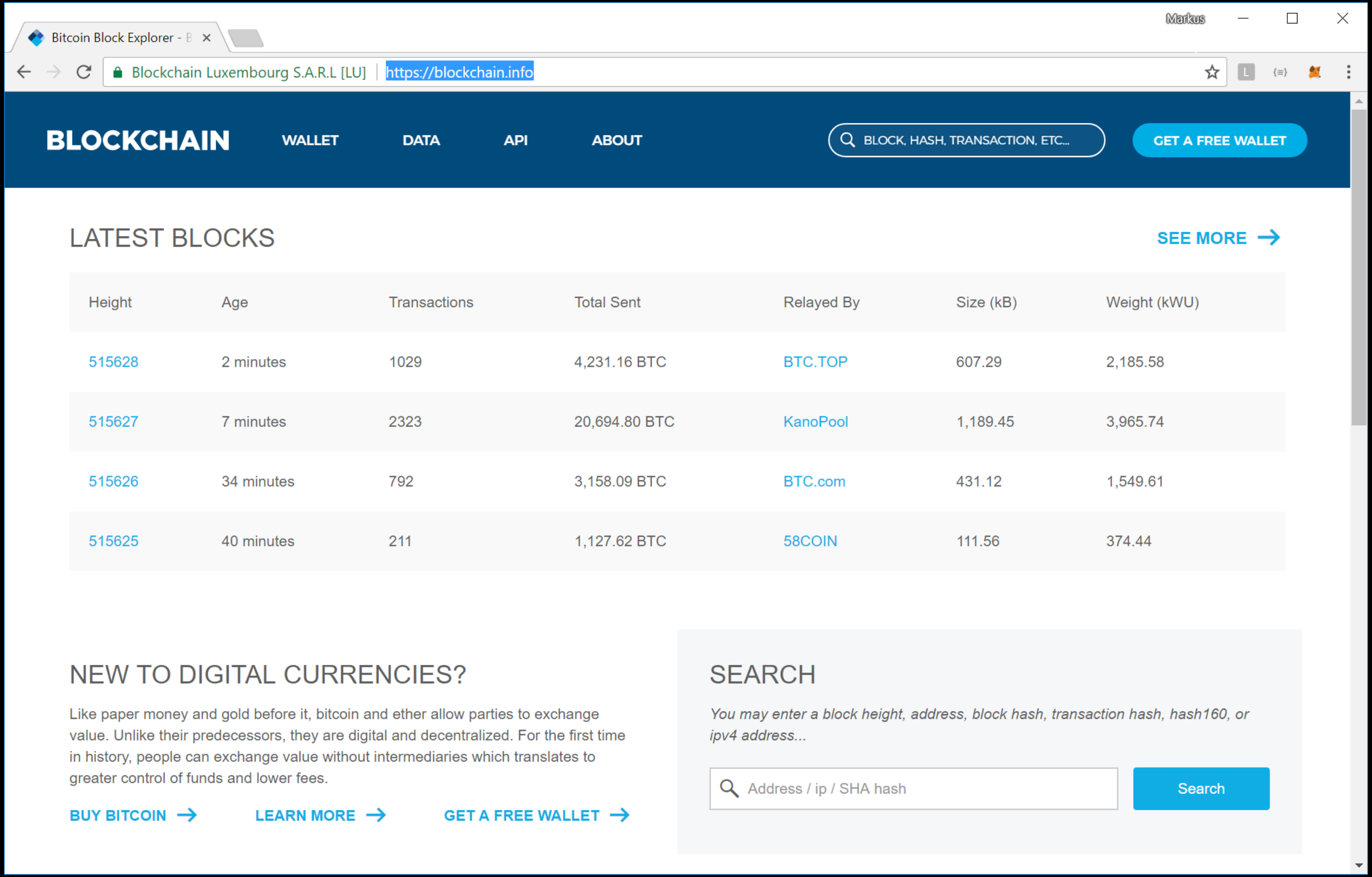
□ Only to old root

Pass/Fail

[github.com/cliftonm/MerkleTree]

Bitcoin blockchain: *Live data*

- Chain grows by 6 new blocks per hour
- approx. 3 transactions per second
- *Compare this to:* Mastercard > 2.500 tps!



Bitcoin Block Explorer - B
Markus
Blockchain Luxembourg S.A.R.L [LU]
https://blockchain.info
BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET

LATEST BLOCKS

SEE MORE →

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)	Weight (kWU)
515628	2 minutes	1029	4,231.16 BTC	BTC.TOP	607.29	2,185.58
515627	7 minutes	2323	20,694.80 BTC	KanoPool	1,189.45	3,965.74
515626	34 minutes	792	3,158.09 BTC	BTC.com	431.12	1,549.61
515625	40 minutes	211	1,127.62 BTC	58COIN	111.56	374.44

NEW TO DIGITAL CURRENCIES?

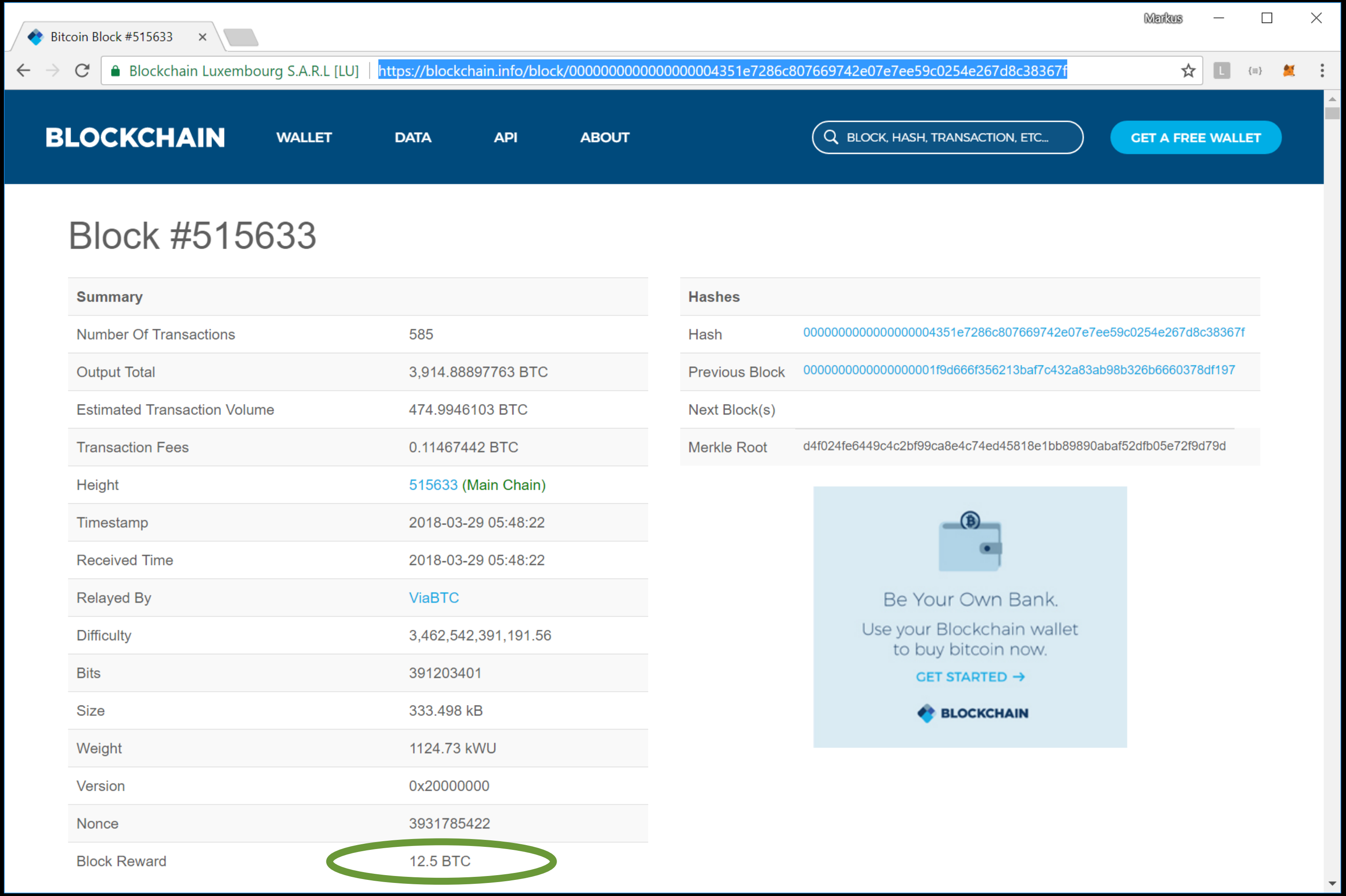
Like paper money and gold before it, bitcoin and ether allow parties to exchange value. Unlike their predecessors, they are digital and decentralized. For the first time in history, people can exchange value without intermediaries which translates to greater control of funds and lower fees.

SEARCH

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

Bitcoin block: *Live data*

- Block Reward:
  money creation
  12.5 BTC p.B.
  ≈ 100,000 €
- per month:
  4,500 blocks
  = 56,000 BTC
  ≈ 450 million €
- *for comparison:*
  EAPP of ECB
  ≈ 60 billion €
- [Cut in half] every
  210,000 blocks



Bitcoin Block #515633
Markus
Blockchain Luxembourg S.A.R.L [LU]
https://blockchain.info/block/00000000000000000004351e7286c807669742e07e7ee59c0254e267d8c38367f
BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET

Block #515633

Summary	
Number Of Transactions	585
Output Total	3,914.88897763 BTC
Estimated Transaction Volume	474.9946103 BTC
Transaction Fees	0.11467442 BTC
Height	515633 (Main Chain)
Timestamp	2018-03-29 05:48:22
Received Time	2018-03-29 05:48:22
Relayed By	ViaBTC
Difficulty	3,462,542,391,191.56
Bits	391203401
Size	333.498 kB
Weight	1124.73 kWU
Version	0x20000000
Nonce	3931785422
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000004351e7286c807669742e07e7ee59c0254e267d8c38367f
Previous Block	00000000000000000001f9d666f356213baf7c432a83ab98b326b6660378df197
Next Block(s)	
Merkle Root	d4f024fe6449c4c2bf99ca8e4c74ed45818e1bb89890abaf52dfb05e72f9d79d

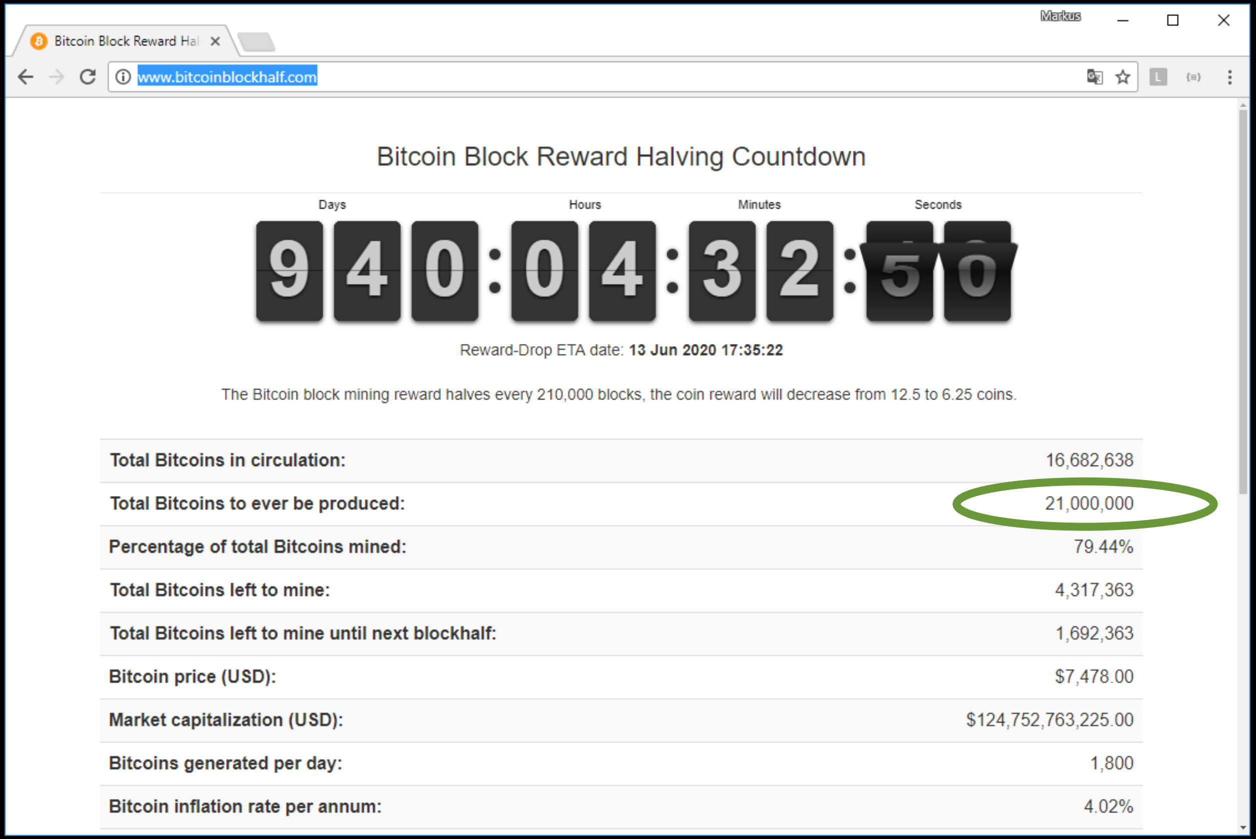
Decline of *Block Reward*

- Money creation will ebb away around 2040

Year	Reward [BTC]	Reward [€]
2016	12,5000	100.000,00
2020	6,2500	50.000,00
2024	3,1250	25.000,00
2028	1,5625	12.500,00
2032	0,7813	6.250,00
2036	0,3906	3.125,00
2040	**0,1953**	**1.562,50**
2044	0,0977	781,25

- 6 B/h · 24 h/d · 365 d/y · 4 y/p
= 210,240 Blocks/period
⇒ max. amount of money
= 210,240 · 100 · $\sum_{n=1}^{\infty} 2^{-n}$ BTC
= 21,024,000 BTC

- *what will happen next?*



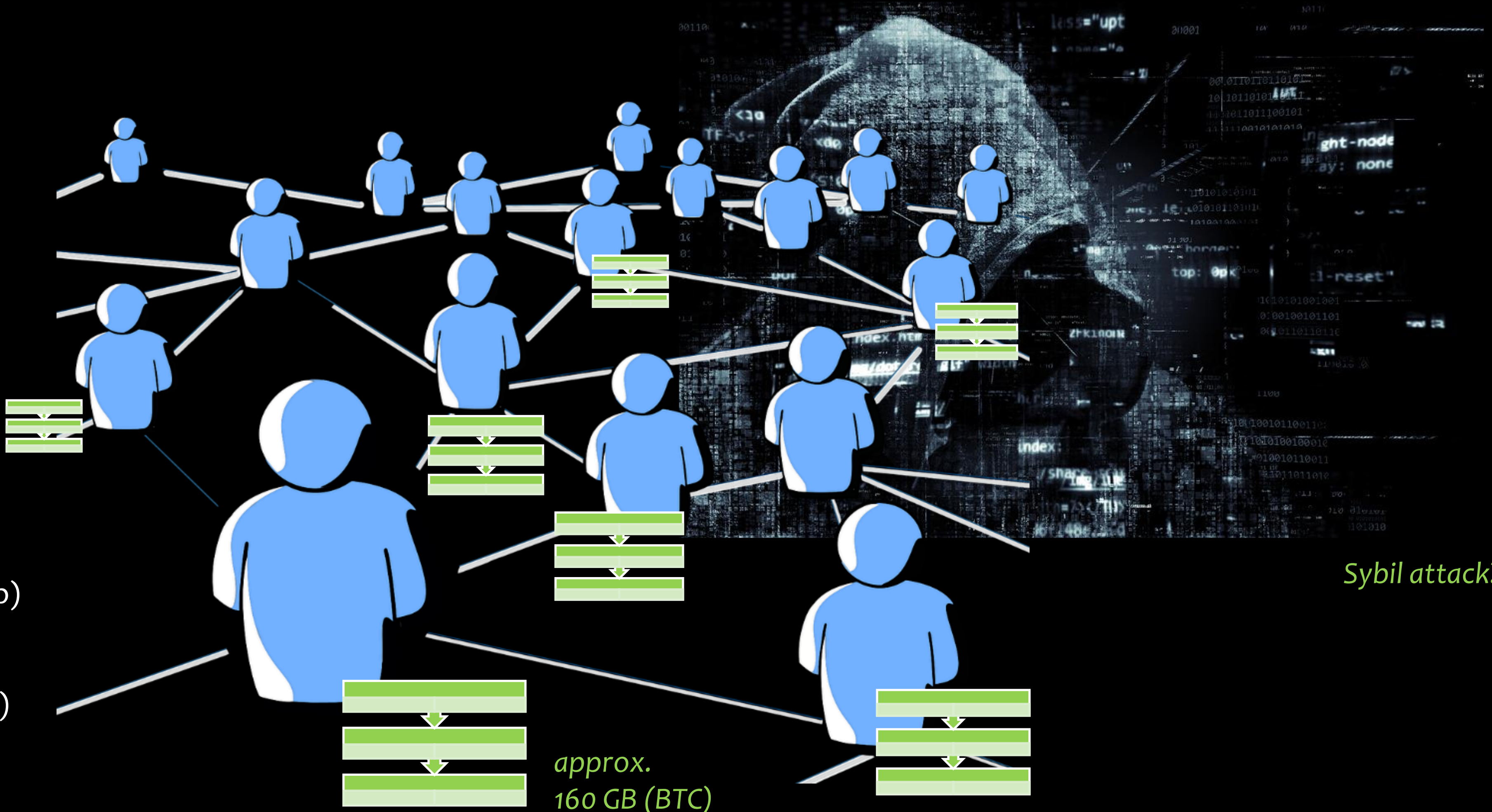
Bitcoin Block Reward Halving Countdown

Reward-Drop ETA date: **13 Jun 2020 17:35:22**

The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12.5 to 6.25 coins.

Total Bitcoins in circulation:	16,682,638
Total Bitcoins to ever be produced:	21,000,000
Percentage of total Bitcoins mined:	79.44%
Total Bitcoins left to mine:	4,317,363
Total Bitcoins left to mine until next blockhalf:	1,692,363
Bitcoin price (USD):	$7,478.00
Market capitalization (USD):	$124,752,763,225.00
Bitcoins generated per day:	1,800
Bitcoin inflation rate per annum:	4.02%

Decentralized storage of the blockchain



P2P network
of Bitcoin nodes (8333/tcp)

Bootstrap: find nodes
via irc.lfnet.org (6667/tcp)

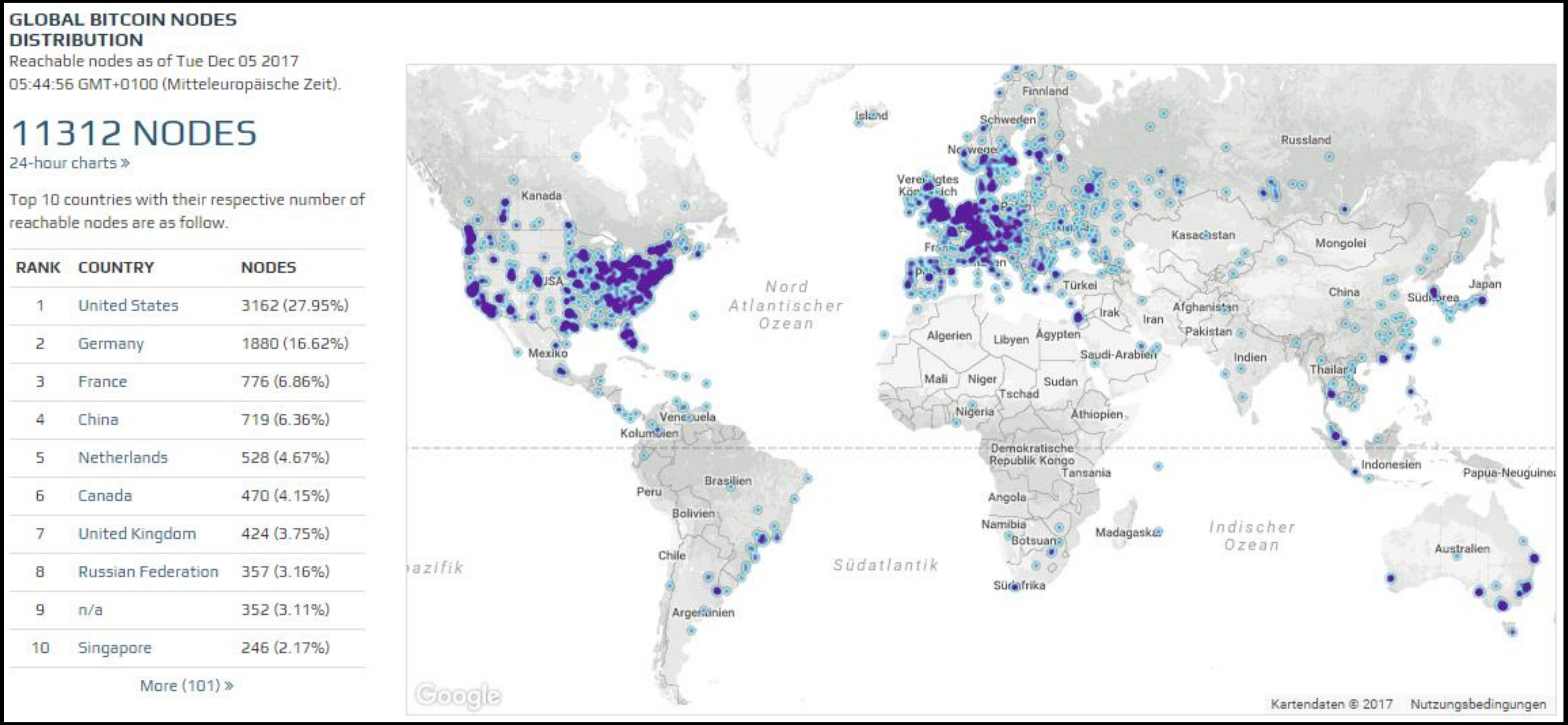
[bitnodes.earn.com]

*approx.
160 GB (BTC)*

Sybil attack?

Bitcoin nodes: *Distribution*

[bitnodes.earn.com]



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Tue Dec 05 2017 05:44:56 GMT+0100 (Mitteleuropäische Zeit).

11312 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

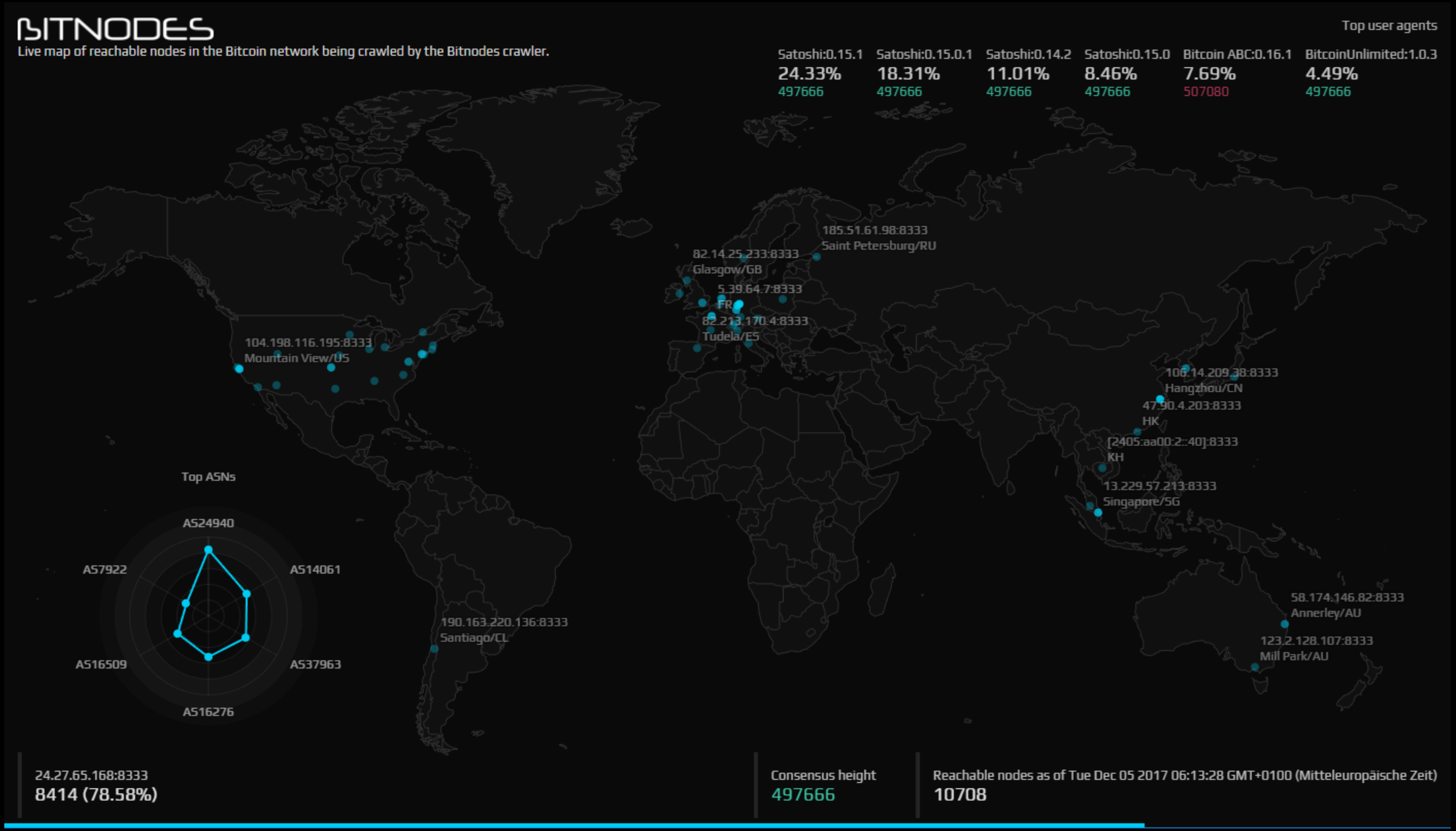
RANK	COUNTRY	NODES
1	United States	3162 (27.95%)
2	Germany	1880 (16.62%)
3	France	776 (6.86%)
4	China	719 (6.36%)
5	Netherlands	528 (4.67%)
6	Canada	470 (4.15%)
7	United Kingdom	424 (3.75%)
8	Russian Federation	357 (3.16%)
9	n/a	352 (3.11%)
10	Singapore	246 (2.17%)

More (101) »

Bitcoin nodes: *Live data*

[bitnodes.earn.com/nodes/live-map]

- Web crawler checks for port 8333/tcp
- ASN = *Autonomous System Number*



BITNODES

Live map of reachable nodes in the Bitcoin network being crawled by the Bitnodes crawler.

Top user agents

Satoshi:0.15.1	Satoshi:0.15.0.1	Satoshi:0.14.2	Satoshi:0.15.0	Bitcoin ABC:0.16.1	BitcoinUnlimited:1.0.3
24.33%	18.31%	11.01%	8.46%	7.69%	4.49%
497666	497666	497666	497666	507080	497666

24.27.65.168:8333
8414 (78.58%)

Consensus height
497666

Reachable nodes as of Tue Dec 05 2017 06:13:28 GMT+0100 (Mitteleuropäische Zeit)
10708

Excursus: *Randomness*

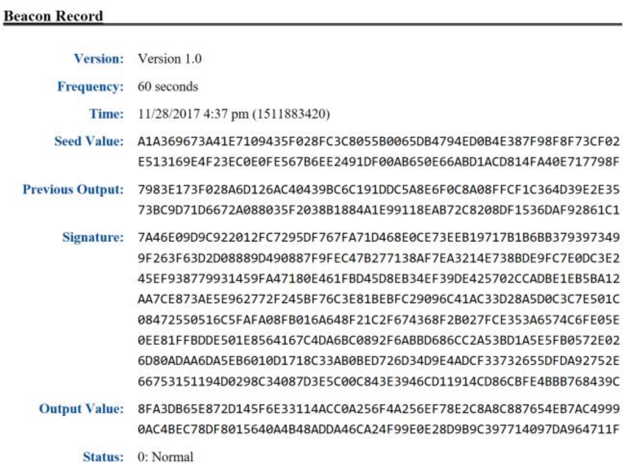
- Natural randomness,
  if for an event no causal explanation

- Synthetic randomness should provide equally distributed values:
  next value of a sequence unpredictable!

- Randomness is the basis for the generation of cryptographic secrets – good generators very valuable!

- Mallory tries to recognize patterns in sequences of public keys – defense: hash function, see Bitcoin address

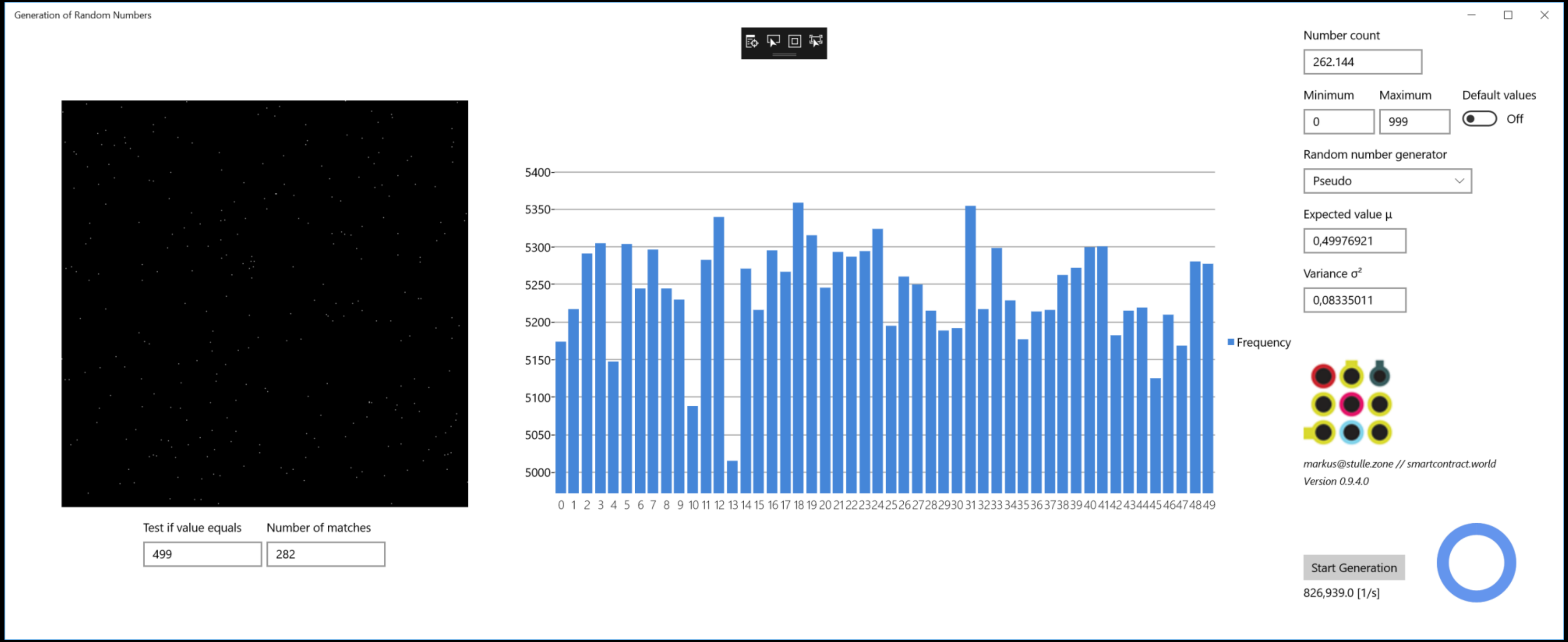
- Perfect: [NIST Randomness Beacon] *(Quantum physics)* delivers 512 bits of maximum entropy every 60 seconds



Beacon Record

Version:	Version 1.0
Frequency:	60 seconds
Time:	11/28/2017 4:37 pm (1511883420)
Seed Value:	A1A369673A41E7109435F028FC3C8055B0065DB4794ED0B4E387F98F8F73CF02 E513169E4F23EC0E0FE567B6EE2491DF00AB650E66ABD1ACD814FA40E717798F
Previous Output:	7983E173F028A6D126AC40439BC6C191DDC5A8E6F0C8A08FFCF1C364D39E2E35 73BC9D71D6672A088035F2038B1884A1E99118EAB72C8208DF1536DAF92861C1
Signature:	7A46E09D9C922012FC7295DF767FA71D468E0CE73EEB19717B1B6BB379397349 9F263F63D2D08889D490887F9FEC47B277138AF7EA3214E738BDE9FC7E0DC3E2 45EF938779931459FA47180E461FBD45D8EB34EF39DE425702CCADBE1EB5BA12 AA7CE873AE5E962772F245BF76C3E81BEBFC29096C41AC33D28A5D0C3C7E501C 08472550516C5FAFA08FB016A648F21C2F674368F2B027FCE353A6574C6FE05E 0EE81FFBDDE501E8564167C4DA6BC0892F6ABBD686CC2A53BD1A5E5FB0572E02 6D80ADAA6DA5EB6010D1718C33AB0BED726D34D9E4ADCF33732655DFDA92752E 66753151194D0298C34087D3E5C00C843E3946CD11914CD86CBFE4BBB768439C
Output Value:	8FA3DB65E872D145F6E33114ACC0A256F4A256EF78E2C8A8C887654EB7AC4999 0AC4BEC78DF8015640A4B48ADDA46CA24F99E0E28D9B9C397714097DA964711F
Status:	0: Normal

Randomness: *Sample implementation (C#)*



Generation of Random Numbers

Number count: 262.144

Minimum: 0

Maximum: 999

Default values: Off

Random number generator: Pseudo

Expected value μ: 0,49976921

Variance σ²: 0,08335011

Test if value equals: 499

Number of matches: 282

markus@stulle.zone // smartcontract.world

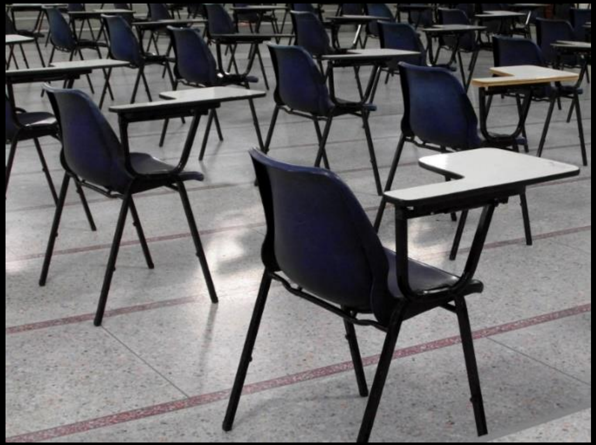
Version 0.9.4.0

826,939.0 [1/s]

[github.com/relianz/Random-Numbers]

What we are exploring together today

1. Past and present: History of money
2. Distributed systems – Can we do without a bank?
3. The Bitcoin blockchain
4. Asymmetrical cryptography
5. The Bitcoin payment system
6. Bitcoin in practice
7. Future



Source of the pictures in this lecture: [pixabay.com]
Public Domain according to: [Creative Commons CC0]
Source of screenshots: [Stulle]

Basis: *Asymmetric cryptosystem*

- Basis RSA – Ron Rivest, Ami Shamir und Ben Adleman (1978):
  Integer factorization $n = p \cdot q$ of big numbers cannot be carried out efficiently!
  Algorithm [Number Field Sieve] – though not exponential, but *superpolynomial*

  6.750.622.348.964.143.051.956.305.469.326.962.117.763.788.889.781.985.387 $\approx 10^{54}$
  = 7 · 97 · 997 · 9.973 · 99.991 · 999.983 · 9.999.991 · 99.999.989 · 999.999.937 · 9.999.999.967

  Naive Factorization takes ≤ 90 seconds on a i7-6700K!

- Basis DHM – Diffie-Hellman-Merkle (1976):
  Discrete logarithm $y = log_b x$ of big numbers cannot...

That's it!

- Keys in the asymmetric cryptosystem
  always consist of two parts :
  public key k_{pub} – private key k_{priv} (= *your secret!*)

RSA key generation

Challenging – you remember?

- Select randomly two big primes p and q, compute modulus $n := p \cdot q$
  Example: $n = 17 \cdot 23 = 391$ *(key length: 9 Bit, recommended:* $\geq$*2048 Bit)*

- Compute Euler's totient function – since factors are prime: $\varphi(n) = (p\text{-}1) \cdot (q\text{-}1)$
  Example: $\varphi(391) = 16 \cdot 22 = 352$, *there are 352 numbers that don't divide 391*

- Select natural number e, that has no common divisors with $\varphi(n)$.
  Favorable exponents have binary few ones: 3, 17, 257 or 65,537
  Example: $e = 257$

- Communicate the public key $k_{pub} = (n\,;\,e)$
  Example: $k_{pub} = (391\,;\,257)$

- Compute $d := e^{-1} \bmod \varphi(n) \Leftrightarrow$ find d $\therefore$ $d \cdot e = 1 \bmod \varphi$
  and store the private key $k_{priv} = (d\,)$ in a secure way!
  Example: $d \cdot 257 = 1 \bmod 352 \Rightarrow d = 641$, *Check:* $641 \cdot 257 = 468 \cdot 352 + 1$

RSA modular arithmetic

Encryption

- Alice wants to encrypt message P to Bob – Assumption: P is an integer
  Alice knows Bob's public key $k_{pub|Recipient} = (n ; e)$
  Example: $P = 42$, $k_{pub|Bob} = (391 ; 257)$
- Alice computes ciphertext $C := P^e \bmod n$ – *Modulo exponentiation*
  Example: $C = 42^{257} \bmod 391 = 365$

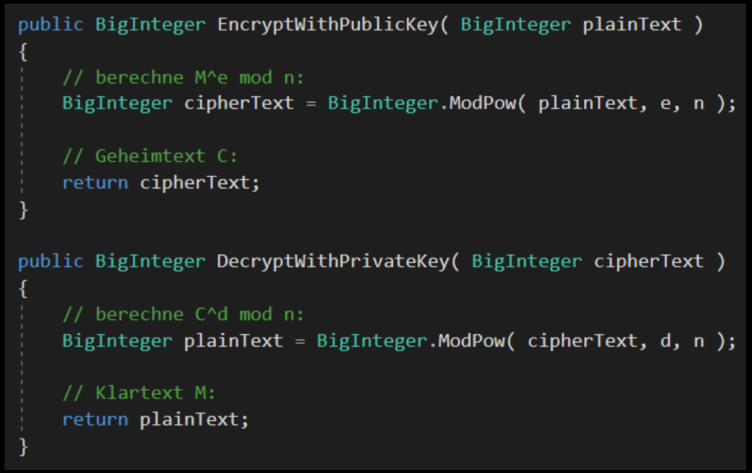
Decryption

- Bob receives C and computes using $k_{priv|Recipient} = (d)$
  the plaintext $M := C^d \bmod n$ – *Modulo root extraction*
  Example: $d = 641 \Rightarrow M = 365^{641} \bmod 391 = 42$

Security!

- Mallory must guess d, he does not know p und q!

[System.Numerics]



```
public BigInteger EncryptWithPublicKey( BigInteger plainText )
{
    // berechne M^e mod n:
    BigInteger cipherText = BigInteger.ModPow( plainText, e, n );

    // Geheimtext C:
    return cipherText;
}

public BigInteger DecryptWithPrivateKey( BigInteger cipherText )
{
    // berechne C^d mod n:
    BigInteger plainText = BigInteger.ModPow( cipherText, d, n );

    // Klartext M:
    return plainText;
}
```

VIVA aspect: *Confidentiality*

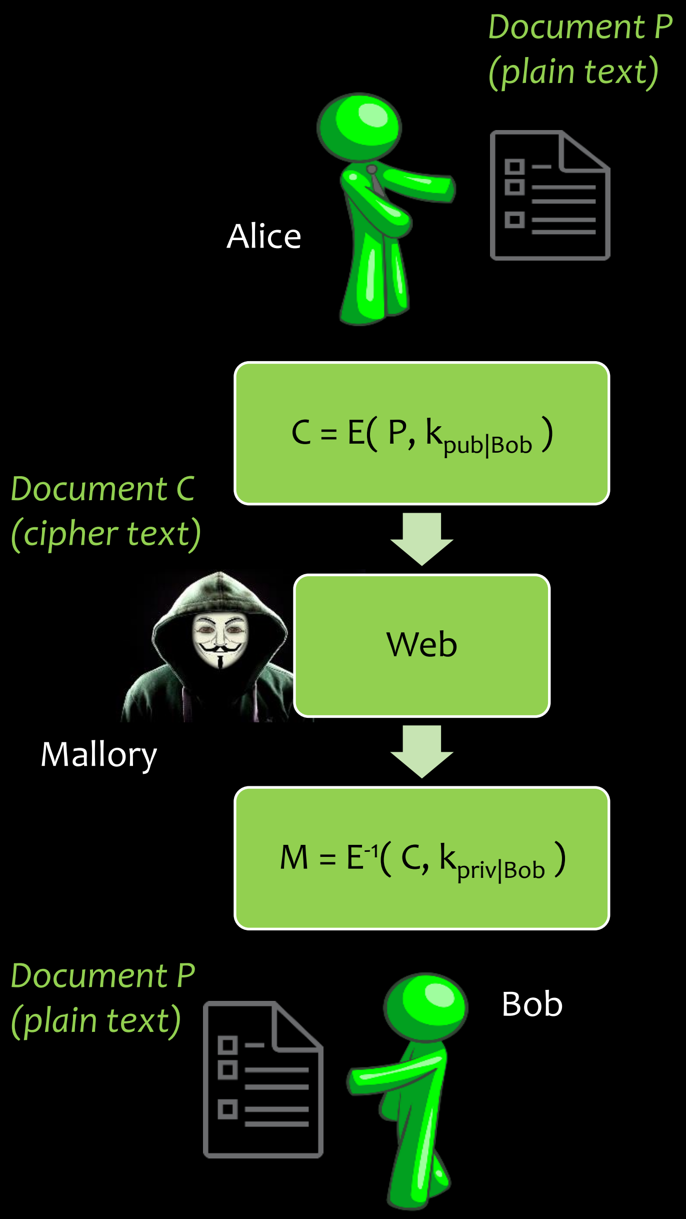
- Objective:
  Protection of confidential information
  in document *P* from unauthorized access

- Method:
  Encryption of *P* with k_{pub} of recipient –
  only Bob can decrypt *C* with his secret k_{priv}

- Precondition:
  Alice knows Bob's public key,
  securing integrity through transmisson by hash function

- Advantage over symmetrical algorithms:
  no shared secret between Alice and Bob et al.

- Confidentiality for the next N years (*quantum computing?*)



Document P
(plain text)

Alice

$C = E(P, k_{pub|Bob})$

Document C
(cipher text)

Web

Mallory

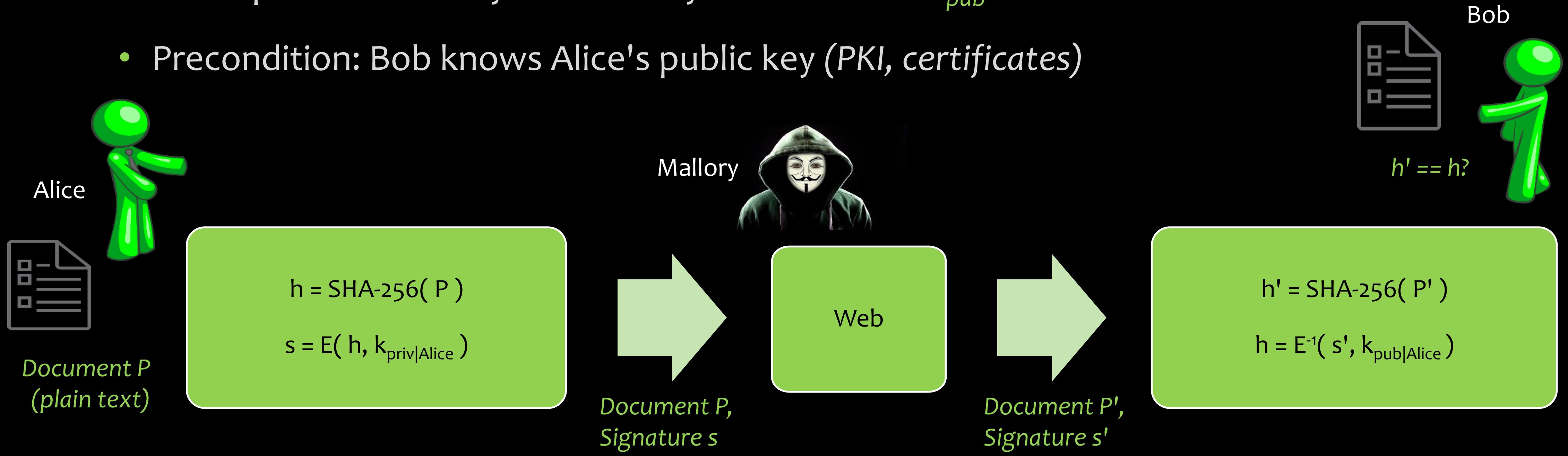
$M = E^{-1}(C, k_{priv|Bob})$

Document P
(plain text)

Bob

VIVA aspect: *Authenticity*

- Objective: Document *P* really comes from the sender of the message and is untampered
- Method:
  Digital signature of document with sender's k_{priv} –
  all recipients can verify authenticity with sender's k_{pub}
- Precondition: Bob knows Alice's public key *(PKI, certificates)*



Alice

Document P
(plain text)

h = SHA-256(P)

$s = E(h, k_{priv|Alice})$

Document P,
Signature s

Mallory

Web

Document P',
Signature s'

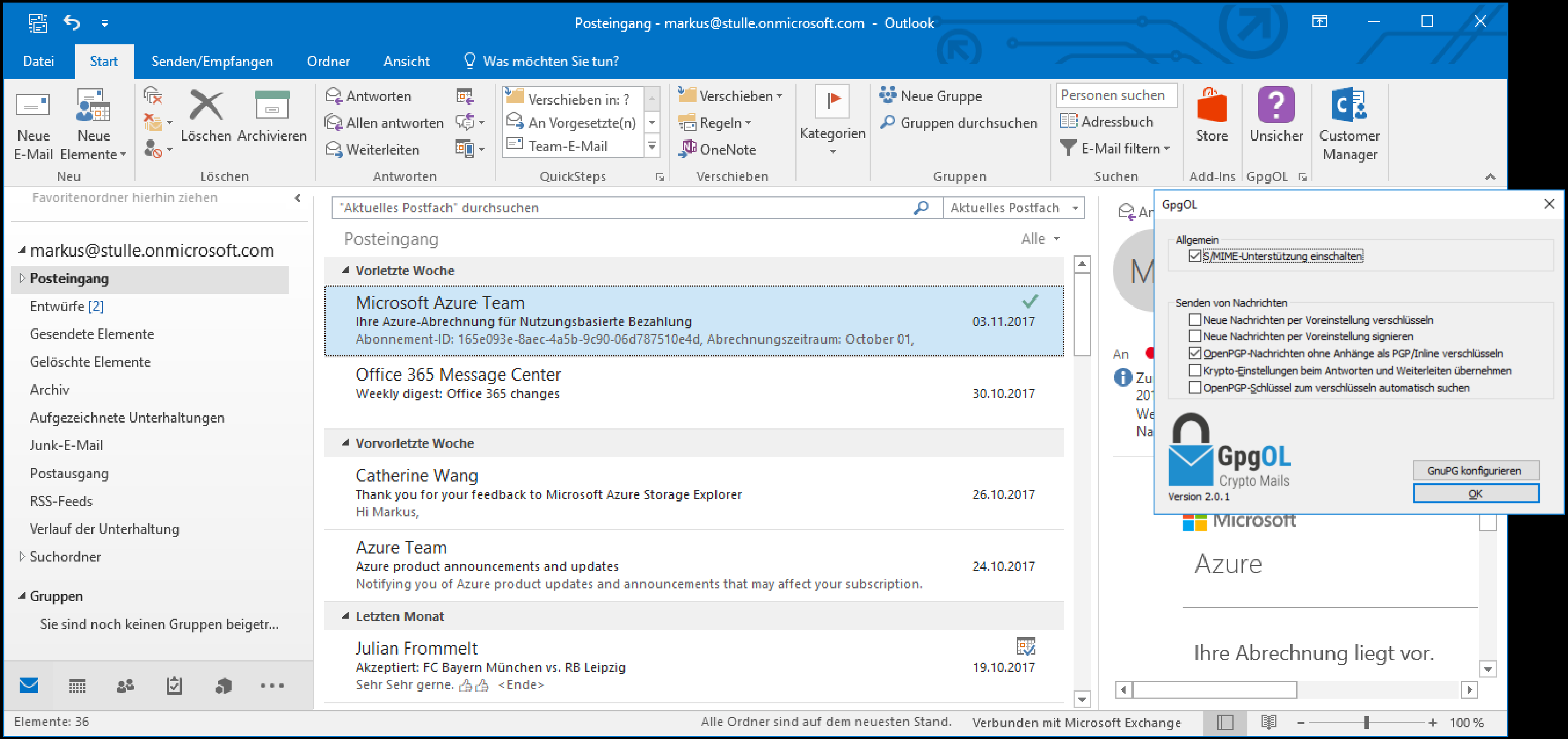
Bob

h' == h?

h' = SHA-256(P')

$h = E^{-1}(s', k_{pub|Alice})$

RSA in the office: *GnuPG for Outlook*



Vorletzte Woche

Microsoft Azure Team
Ihre Azure-Abrechnung für Nutzungsbasierte Bezahlung — 03.11.2017
Abonnement-ID: 165e093e-8aec-4a5b-9c90-06d787510e4d, Abrechnungszeitraum: October 01,

Office 365 Message Center
Weekly digest: Office 365 changes — 30.10.2017

Vorvorletzte Woche

Catherine Wang
Thank you for your feedback to Microsoft Azure Storage Explorer — 26.10.2017
Hi Markus,

Azure Team
Azure product announcements and updates — 24.10.2017
Notifying you of Azure product updates and announcements that may affect your subscription.

Letzten Monat

Julian Frommelt
Akzeptiert: FC Bayern München vs. RB Leipzig — 19.10.2017
Sehr Sehr gerne. <Ende>

GpgOL

Allgemein
☑ S/MIME-Unterstützung einschalten

Senden von Nachrichten
☐ Neue Nachrichten per Voreinstellung verschlüsseln
☐ Neue Nachrichten per Voreinstellung signieren
☑ OpenPGP-Nachrichten ohne Anhänge als PGP/Inline verschlüsseln
☐ Krypto-Einstellungen beim Antworten und Weiterleiten übernehmen
☐ OpenPGP-Schlüssel zum verschlüsseln automatisch suchen

GpgOL Crypto Mails
Version 2.0.1

GnuPG konfigurieren
OK
Microsoft
Azure
Ihre Abrechnung liegt vor.
Elemente: 36
Alle Ordner sind auf dem neuesten Stand.
Verbunden mit Microsoft Exchange
100 %

Elliptic Curve Cryptography (ECC)

Again: Challenge randomness!

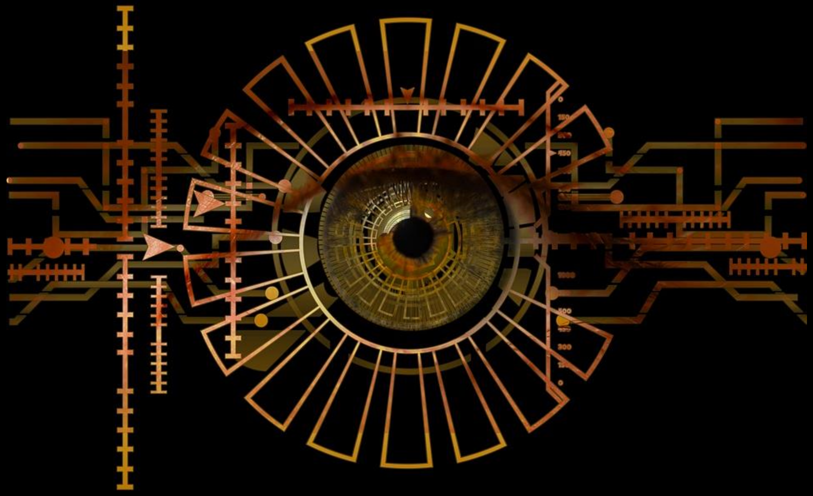
- NIST standard [secp256k1] („*Bitcoin curve*“) – elliptic curve $y^2 = x^3 + 7$ over finite field $\mathbf{F}_p$
  with prime $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \approx 10^{77}$

- Select k_{priv} as a random natural number $1 < k < n = 2^{256}$
  n = 115.792.089.237.316.195.423.570.985.008.687.907.852.837.564.279.074.904.382.605.163.141.518.161.494.336

- Compute $k_{pub} := k_{priv} \cdot G$
  with generator $G = (g_x\ g_y)$:
  g_x = 55.066.263.022.277.343.669.578.718.895.168.534.326.250.603.453.777.594.175.500.187.360.389.116.729.240
  g_y = 32.670.510.020.758.816.978.083.085.130.507.043.184.471.273.380.659.243.275.938.904.335.757.337.482.424

- Securtity comparable with RSA key length of 3.072 Bit
  Energy for Brute-force search: $1{,}9 \cdot 10^{26}$ \$ ($GNP_{world} = 7{,}9 \cdot 10^{13}$ \$, $T_{earth < 30\,°C} = 9 \cdot 10^8$ years)
  [Nemec et al.], [Weis & Forler 34C3]

Summary Cryptography



VIVA Aspects

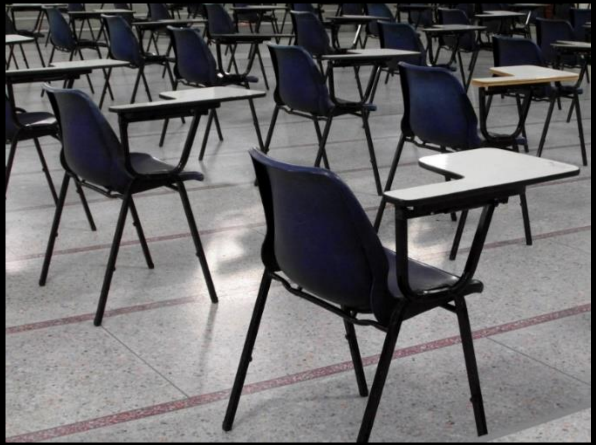
- Hash function ensures Integrity
- Encryption ensures Confidentiality
- Digital Signature ensures Authenticity
- *Availability comes from P2P Network!*

Special features Bitcoin

- ECDSA – Elliptic Curve Digital Signature Algorithm
  BSI Technical Guideline [TR-03111], Version 2.0
- Lining up hash functions [SHA-256] and [RIPEMD-160] for Bitcoin Address

What we are exploring together today

1. Past and present: History of money
2. Distributed systems – Can we do without a bank?
3. The Bitcoin blockchain
4. Asymmetrical cryptography
5. The Bitcoin payment system
6. Bitcoin in practice
7. Future

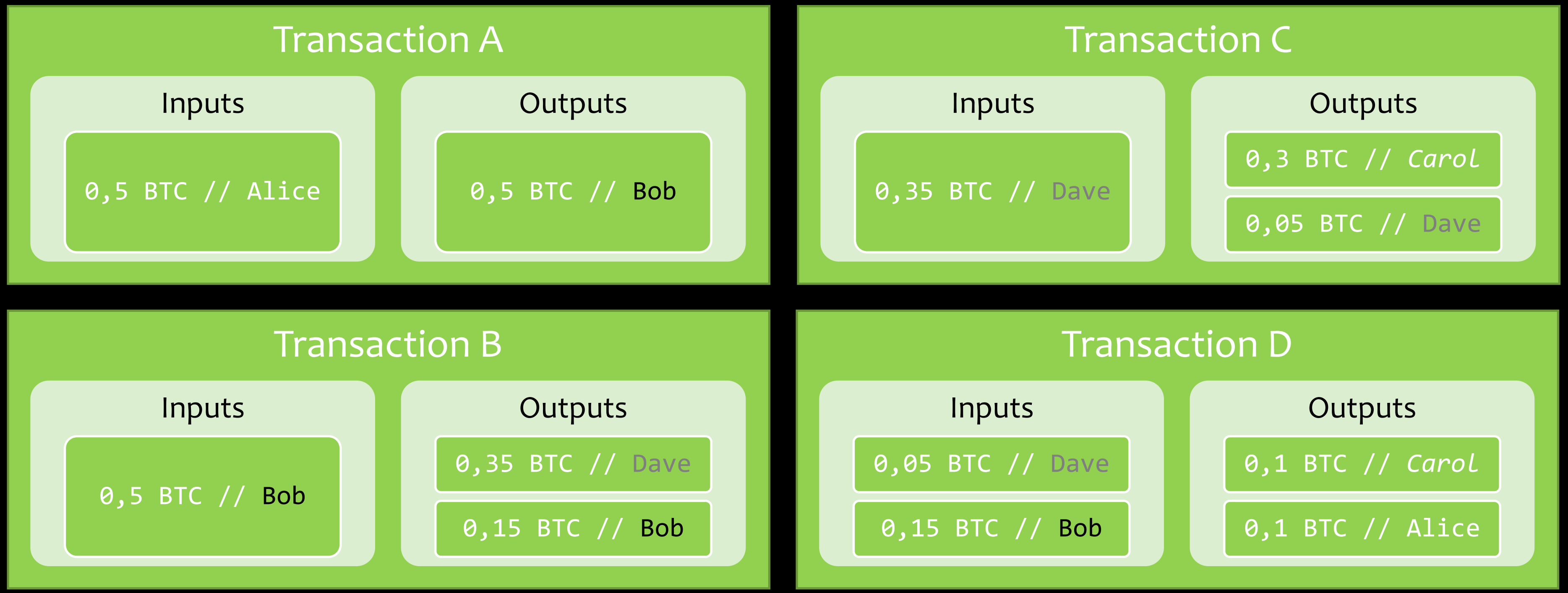


Source of the pictures in this lecture: [pixabay.com]
Public Domain according to: [Creative Commons CC0]
Source of screenshots: [Stulle]

Transfering crypto assets: *Transactions*

- UTXO – Unspent Transaction Output
  Balance := Sum of all UTXO (*requires reading the whole blockchain!*)

Can anyone really spend Bob's money?!



Transaction A

Inputs: 0,5 BTC // Alice

Outputs: 0,5 BTC // Bob

Transaction C

Inputs: 0,35 BTC // Dave

Outputs: 0,3 BTC // *Carol*; 0,05 BTC // Dave

Transaction B

Inputs: 0,5 BTC // Bob

Outputs: 0,35 BTC // Dave; 0,15 BTC // Bob

Transaction D

Inputs: 0,05 BTC // Dave; 0,15 BTC // Bob

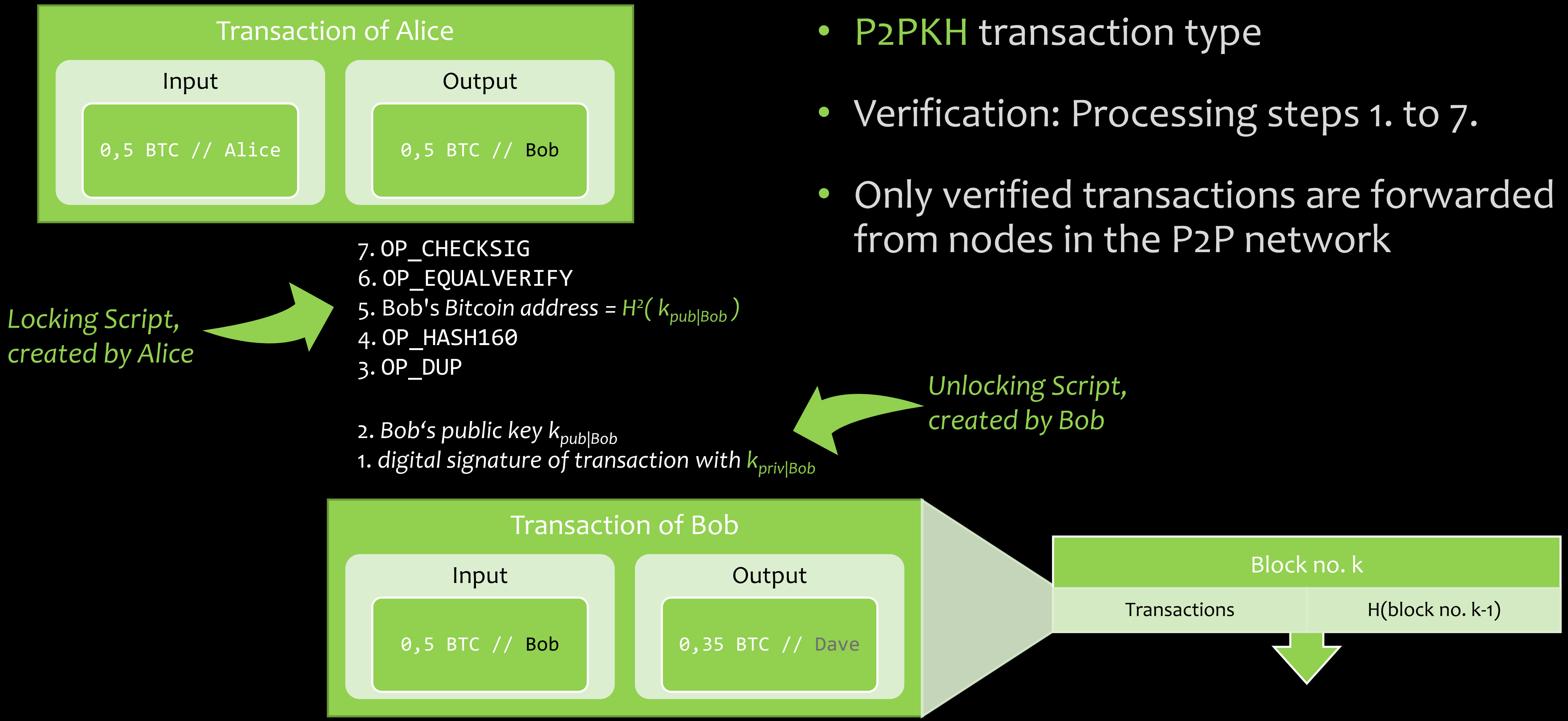
Outputs: 0,1 BTC // *Carol*; 0,1 BTC // Alice

Balance Carol?

CoinJoin

Securing a crypto asset transaction

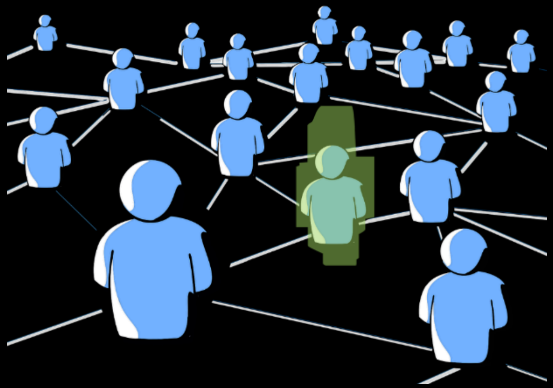
- P2PKH transaction type
- Verification: Processing steps 1. to 7.
- Only verified transactions are forwarded from nodes in the P2P network



7. OP_CHECKSIG
6. OP_EQUALVERIFY
5. Bob's *Bitcoin address* = $H^2(k_{pub|Bob})$
4. OP_HASH160
3. OP_DUP

2. *Bob‘s public key* $k_{pub|Bob}$
1. *digital signature of transaction with* $k_{priv|Bob}$

Bitcoin consensus algorithm



1. New transactions are distributed to all nodes

2. Each node participating in the mining process combines new transactions into a block

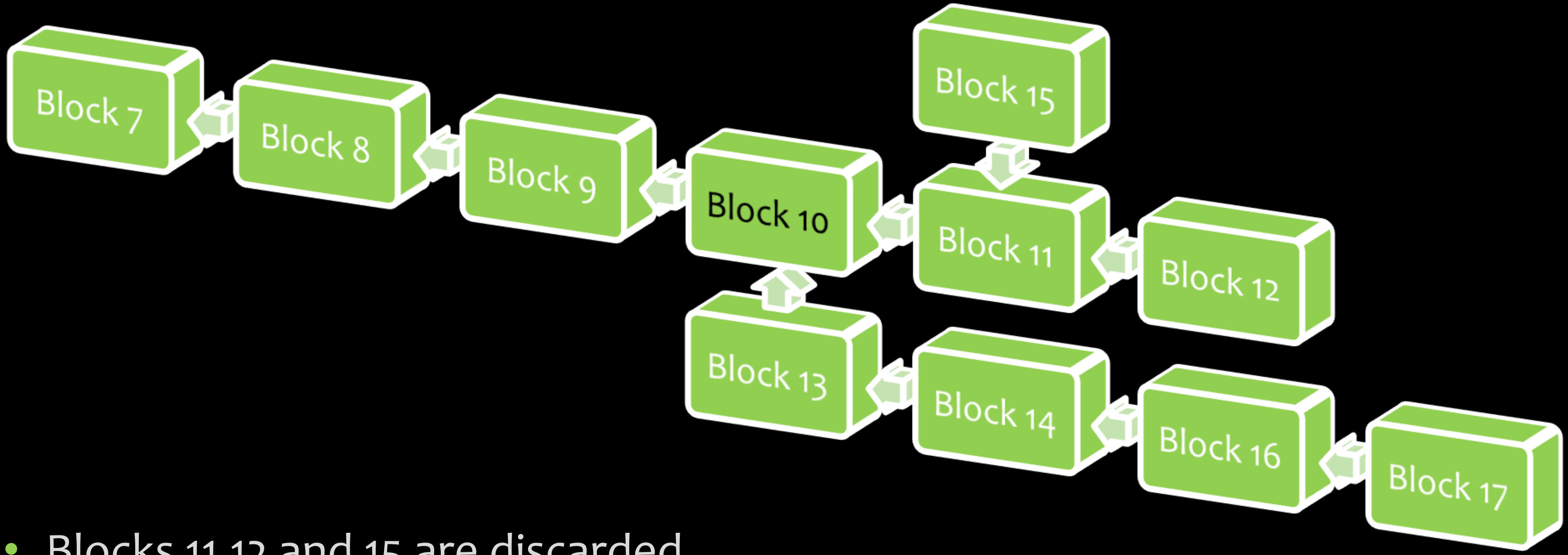
3. *In every round of consensus building:*
   a randomly selected node publishes its newly formed block in the net

4. The other nodes only accept the new block if all transactions contained in it are valid

5. Acceptance of the new block causes its hash value to be included in the next generated block, it is thus attached to the blockchain

6. The nodes always follow the longest path in the chain.

BTC nodes follow the longest path



- Blocks 11,12 and 15 are discarded
- 51% attack: Mallory would have to create more blocks than the rest of the net
- Recommended: qualifying period ≥ 6 blocks before delivery of „expensive“ goods!

Random selection of a P2P full node

Antminer S9

- Proof-of-Work – Miners must solve hash puzzle:
  Add numbers to block B
  such that hash value $H(B) < h_{target}$ [difficulty]

- Hash function is one-way:
  Solving the puzzle by trial and error!

- Competitive mining requires ASICs
  and a lot of electrical power :
  (½ · 12.5 BTC/B · 8,000 €/BTC · 6 B/h) / 0.05 €/kWh = 6,000 $\mathrm{MW_{el}}$

Central system?

- Nodes work together in pools [survey], share of China > 81%

- Alternatives: Solving meaningful tasks
  [Folding@home], [climateprediction.net] (BOINC)
  or implementing Proof-of-Stake

Proof-of-Useful-Work

1. Producibility
   Task easy to create and difficulty well controllable

2. Verifiability
   Result of work can be checked with little effort

3. Randomness
   all participants have identical chances to find the solution of the task in the next calculation step (→ [Bernoulli process])

4. Statelessness
   the race starts anew in each round of consensus finding

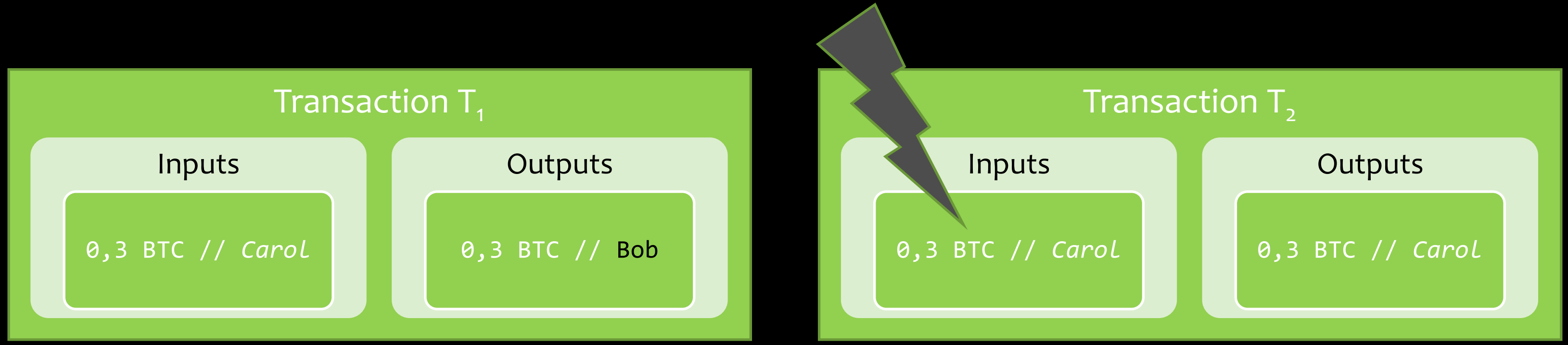
5. Usefulness
   The result of the work is not only a contribution to the hygiene of the blockchain but also an economic benefit or serves humanity.

1. – 4. perfectly fulfilled by hash puzzle SHA-256

ASIC resistant hashes: scrypt, Argon2, Catena

Double-spending?

- Carol transfers 0.3 BTC to Bob
- ...and the same UTXO to herself!
- Fully-fledged P2P neighbours („full nodes“) reject transaction T_2, because UTXO is already consumed by T_1 – functions in [Bitcoin Core]: *AcceptToMemoryPool*, *CheckTransaction* und *CheckInputs*
- Corollary: There must be more honest than dishonest knots (51% attack).



Transaction T_1

Inputs

0,3 BTC // Carol

Outputs

0,3 BTC // Bob

Transaction T_2

Inputs

0,3 BTC // Carol

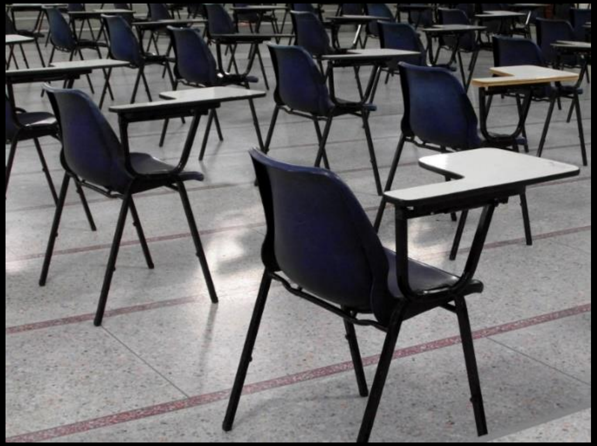
Outputs

0,3 BTC // Carol

[Statistics]

What we are exploring together today

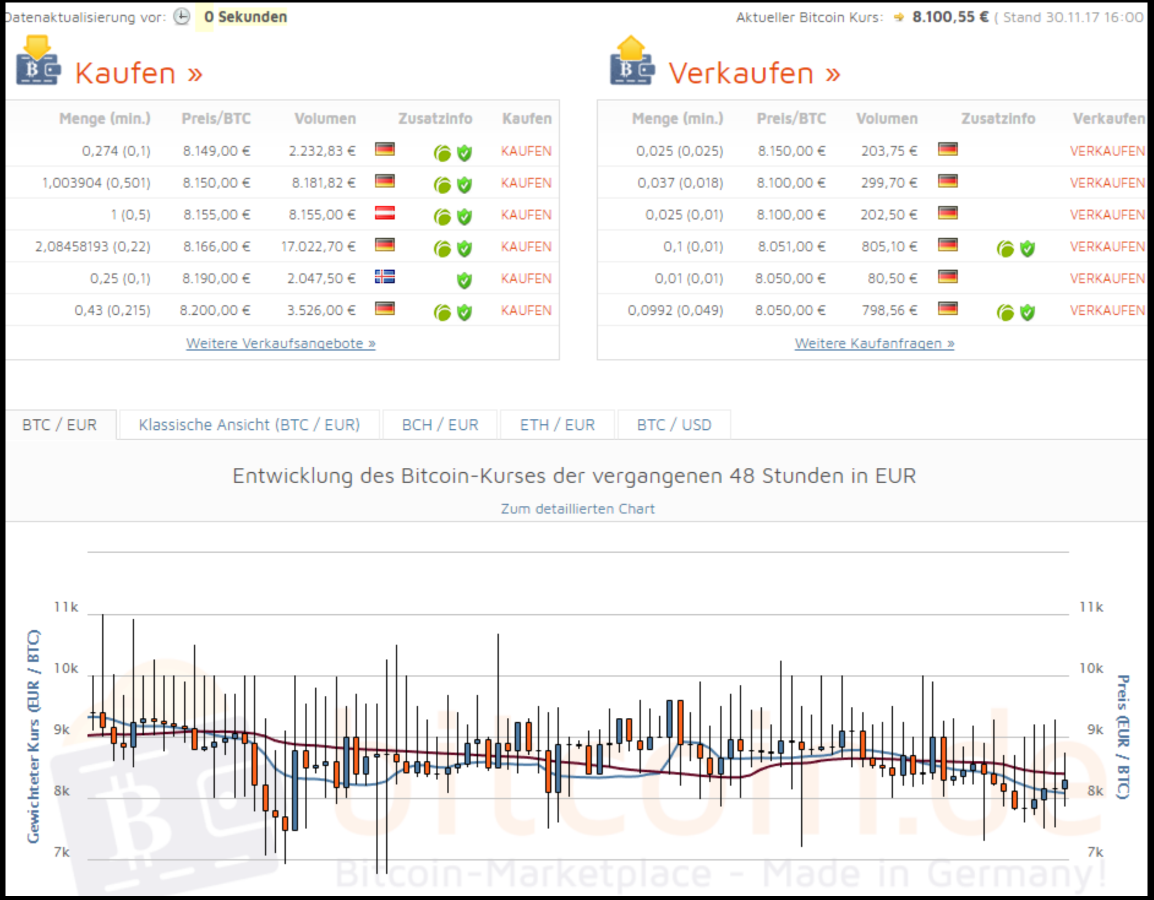
1. Past and present: History of money
2. Distributed systems – Can we do without a bank?
3. The Bitcoin blockchain
4. Asymmetrical cryptography
5. The Bitcoin payment system
6. Bitcoin in practice
7. Future



Source of the pictures in this lecture: [pixabay.com]
Public Domain according to: [Creative Commons CC0]
Source of screenshots: [Stulle]

Exchange Bitcoin for fiat money

- Market place [bitcoin.de]
  trading BTC, BCH and Ether
- Login with
  Multi-Factor Authentication:
  1. Username / password
  2. Captcha (image recognition)
  3. Time-based One-time Password,
     works best with smartphone app
- Prerequisite for trading:
  account with a direct bank [fidor.de]
- Bitcoin keys
  stored in Online-Wallet



Datenaktualisierung vor: 0 Sekunden

Aktueller Bitcoin Kurs: ➜ **8.100,55 €** (Stand 30.11.17 16:00

Kaufen »

Menge (min.)	Preis/BTC	Volumen		Zusatzinfo	Kaufen
0,274 (0,1)	8.149,00 €	2.232,83 €	🇩🇪	● ✓	KAUFEN
1,003904 (0,501)	8.150,00 €	8.181,82 €	🇩🇪	● ✓	KAUFEN
1 (0,5)	8.155,00 €	8.155,00 €	🇦🇹	● ✓	KAUFEN
2,08458193 (0,22)	8.166,00 €	17.022,70 €	🇩🇪	● ✓	KAUFEN
0,25 (0,1)	8.190,00 €	2.047,50 €	🇮🇸	✓	KAUFEN
0,43 (0,215)	8.200,00 €	3.526,00 €	🇩🇪	● ✓	KAUFEN

Weitere Verkaufsangebote »

Verkaufen »

Menge (min.)	Preis/BTC	Volumen		Zusatzinfo	Verkaufen
0,025 (0,025)	8.150,00 €	203,75 €	🇩🇪		VERKAUFEN
0,037 (0,018)	8.100,00 €	299,70 €	🇩🇪		VERKAUFEN
0,025 (0,01)	8.100,00 €	202,50 €	🇩🇪		VERKAUFEN
0,1 (0,01)	8.051,00 €	805,10 €	🇩🇪	● ✓	VERKAUFEN
0,01 (0,01)	8.050,00 €	80,50 €	🇩🇪		VERKAUFEN
0,0992 (0,049)	8.050,00 €	798,56 €	🇩🇪	● ✓	VERKAUFEN

Weitere Kaufanfragen »

Entwicklung des Bitcoin-Kurses der vergangenen 48 Stunden in EUR

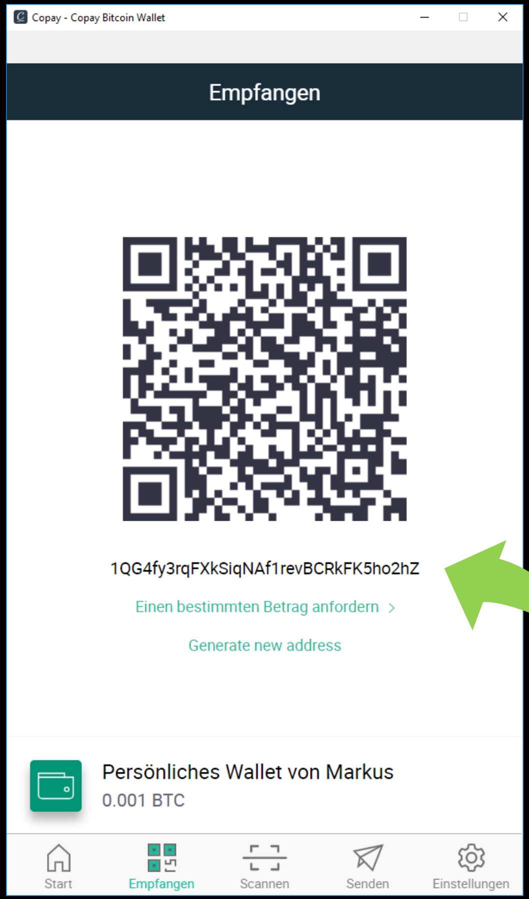
Zum detaillierten Chart

11k
10k
9k
8k
7k
Gewichteter Kurs (EUR / BTC)
Preis (EUR / BTC)
bitcoin.de
Bitcoin-Marketplace - Made in Germany!

Storing keys in local wallet

- Example: Open source product [Copay] available for numerous platforms
- Uses Bitcore Wallet Service by HTTP/REST
  ⇒ no access to local computer „from outside“
- Creates a new Bitcoin key pair (= address) after each receive
- Often: Bitcoin transfer
  from the market place to the local wallet
- Absolutely necessary: Regular data backups

Important! → No access to UTXO
if private keys are lost!


Copay - Copay Bitcoin Wallet

Empfangen

1QG4fy3rqFXkSiqNAf1revBCRkFK5ho2hZ

Einen bestimmten Betrag anfordern >

Generate new address

Persönliches Wallet von Markus
0.001 BTC

Bitcoin address
= $H^2(\,k_{pub}\,)$

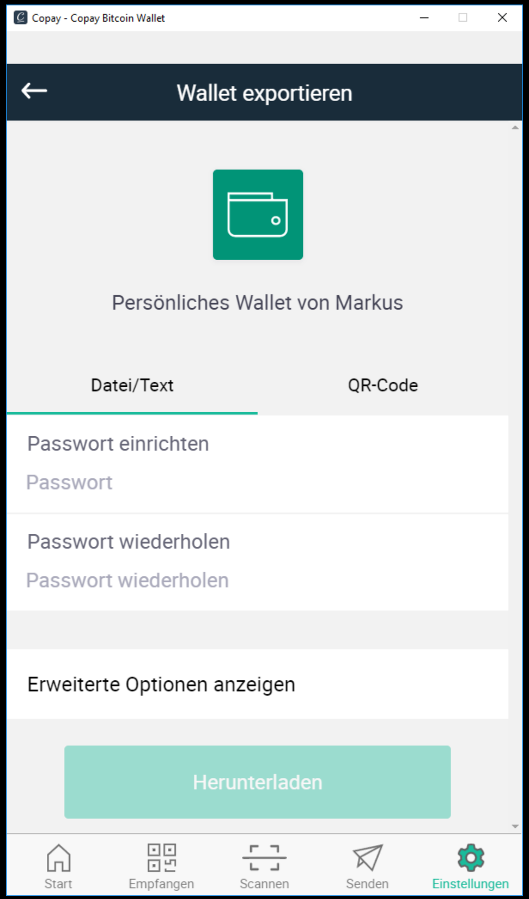
Saving your wallet data

- Export function in Copay accessible via *Settings / Wallet selection / More Options / Wallet export*
- Checking the JSON file of the export:

```
C:\> powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\> $json = ${E:\Betrieb\Datensicherung\BTC\Copay.aes.json}
PS C:\> $json | ConvertFrom-Json | ConvertTo-Json
{
    "iv":  "2/VI/5xEmd5fTdoUP+qs+g==",
    "v":  1,
    "iter":  10000,
    "ks":  128,
    "ts":  64,
    "mode":  "ccm",
    "adata":  "",
    "cipher":  "aes",
    "salt":  "PD1ArGGPJwA=",
    "ct":  "5Ct5eIvLUD0tsKhPKyWUiicDaC5/5/SKhJC5IxFotbDvuPu4rLu..."
}
```

Data encrypted using AES with key derived from password



Copay - Copay Bitcoin Wallet

Wallet exportieren

Persönliches Wallet von Markus

Datei/Text | QR-Code

Passwort einrichten

Passwort

Passwort wiederholen

Passwort wiederholen

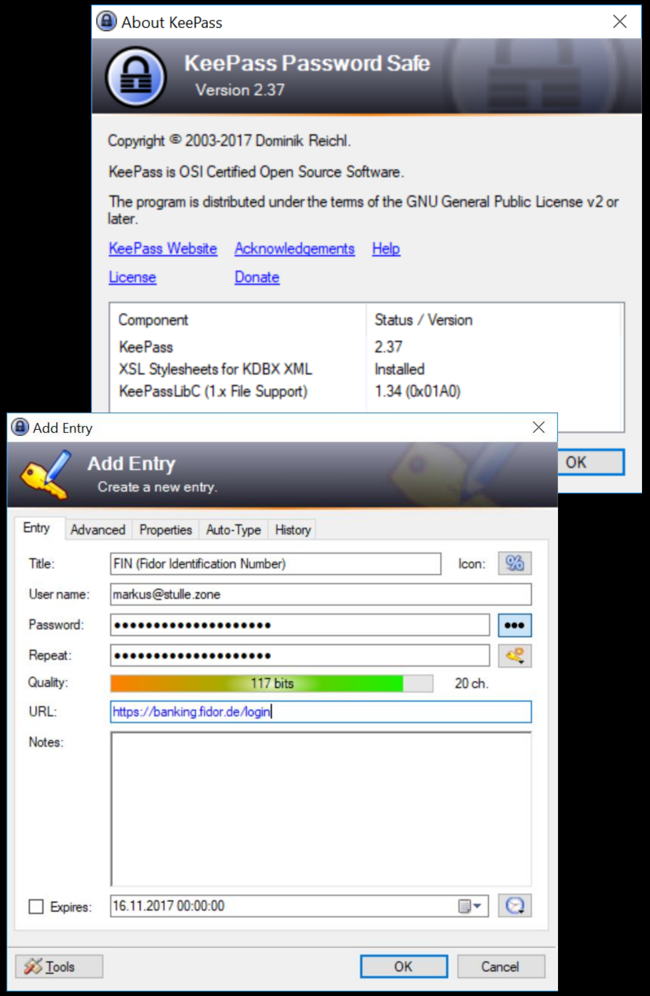
Erweiterte Optionen anzeigen

Herunterladen

Start | Empfangen | Scannen | Senden | Einstellungen

Exkurs: *For your security*

- Use tools like [KeePass]
  to generate and store really strong passwords!
- When applying cryptography –
  use open source products whenever possible
- Apply [Gpg4win], practice PKI process!
- Clarify your digital heritage! Storage media?
  Store wallets for large UTXO offline („cold storage“),
  also: print keys and put it in the safe deposit box
- Do not store unencrypted data in the Cloud –
  apply products like [Boxcryptor]



About KeePass

KeePass Password Safe
Version 2.37

Copyright © 2003-2017 Dominik Reichl.

KeePass is OSI Certified Open Source Software.

The program is distributed under the terms of the GNU General Public License v2 or later.

KeePass Website Acknowledgements Help
License Donate

Component	Status / Version
KeePass	2.37
XSL Stylesheets for KDBX XML	Installed
KeePassLibC (1.x File Support)	1.34 (0x01A0)

Add Entry

Add Entry
Create a new entry.

Entry | Advanced | Properties | Auto-Type | History

Title: FIN (Fidor Identification Number)
User name: markus@stulle.zone
Password: ••••••••••••••••••••
Repeat: ••••••••••••••••••••
Quality: 117 bits 20 ch.
URL: https://banking.fidor.de/login
Notes:
□ Expires: 16.11.2017 00:00:00

Bitcoin myths

- Transactions are anonymous
  No – Bitcoin only offers pseudonymity,
  De-Anonymization possible thru „Taint Analysis"

  „An Analysis of Anonymity in the Bitcoin System",
  F. Reid and M. Harrigan, Cornell U. – Mai 2012 [PDF]

- Bitcoin is suitable for money laundering
  No – Market places for exchange BTC / fiat money are subject to strict rules („KYC")

  „New York's BitLicense Proposal", [NYDFS] – Juni 2015 [PDF]

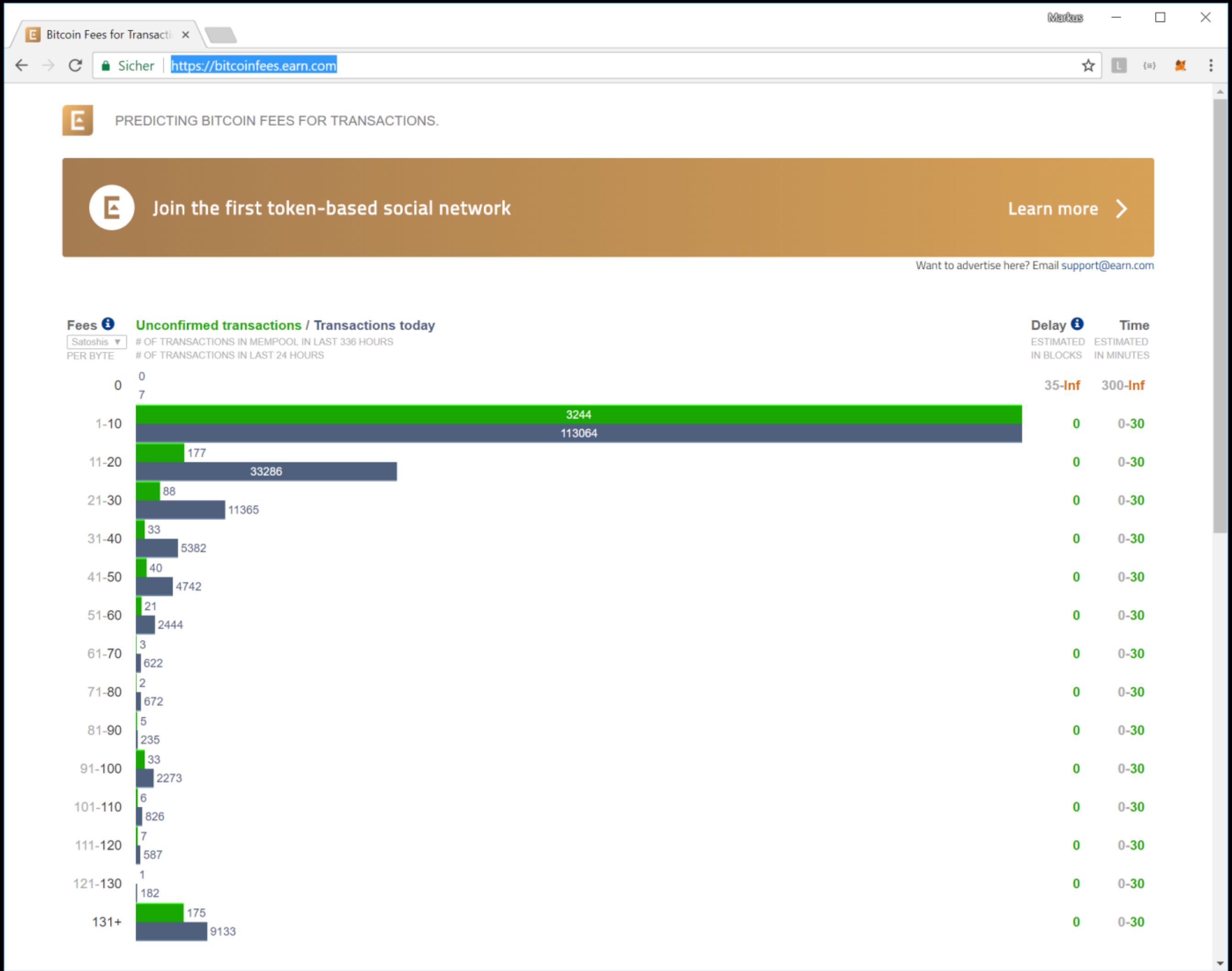
- Bitcoin transactions are cheap
  No – Transaction costs much higher than for credit card payments: [bitcoinfees.earn.com]
  Example: 150 Satoshi/Byte · 512 Byte/transaction = 76,800 Satoshi/T ≈ 6,2 €/T

Transaction costs: *Live data*

- Costs are determined by the originator of a transaction
- Stinginess is punished with delay

Only from 61 Satoshi p.B. secure chance of transaction in the next block

[Unconfirmed transactions]

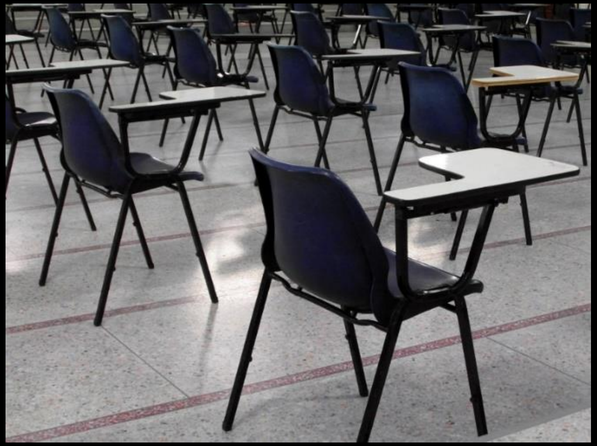


PREDICTING BITCOIN FEES FOR TRANSACTIONS.

Fees Satoshis ▼ PER BYTE	Unconfirmed transactions # OF TRANSACTIONS IN MEMPOOL IN LAST 336 HOURS	Transactions today # OF TRANSACTIONS IN LAST 24 HOURS	Delay ESTIMATED IN BLOCKS	Time ESTIMATED IN MINUTES
0	0	7	35-Inf	300-Inf
1-10	3244	113064	0	0-30
11-20	177	33286	0	0-30
21-30	88	11365	0	0-30
31-40	33	5382	0	0-30
41-50	40	4742	0	0-30
51-60	21	2444	0	0-30
61-70	3	622	0	0-30
71-80	2	672	0	0-30
81-90	5	235	0	0-30
91-100	33	2273	0	0-30
101-110	6	826	0	0-30
111-120	7	587	0	0-30
121-130	1	182	0	0-30
131+	175	9133	0	0-30

What we are exploring together today

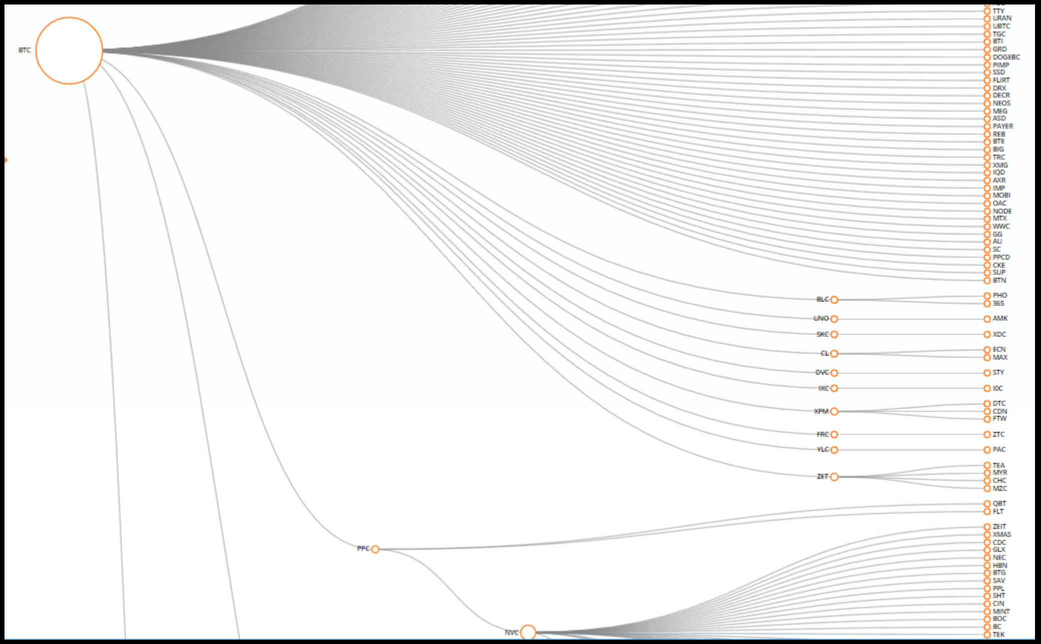
1. Past and present: History of money
2. Distributed systems – Can we do without a bank?
3. The Bitcoin blockchain
4. Asymmetrical cryptography
5. The Bitcoin payment system
6. Bitcoin in practice
7. Future

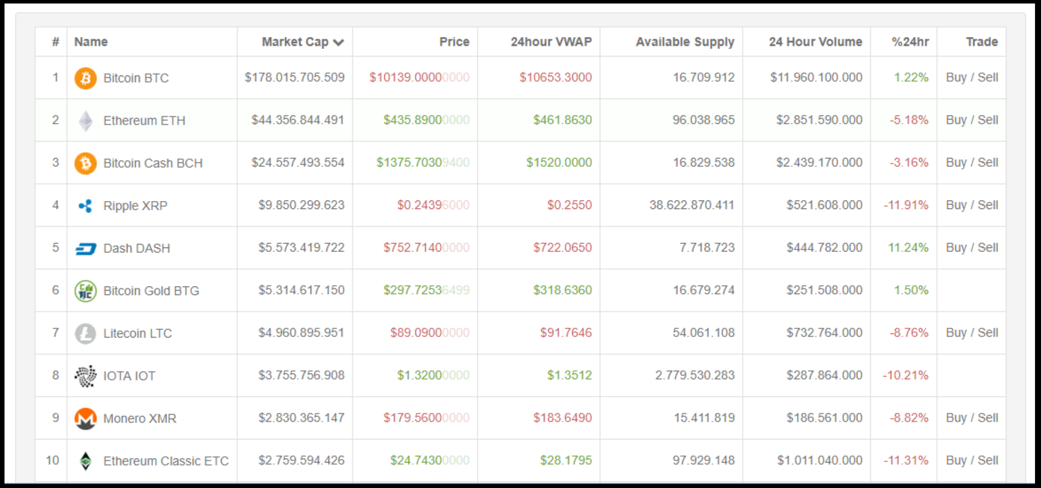


Source of the pictures in this lecture: [pixabay.com]
Public Domain according to: [Creative Commons CC0]
Source of screenshots: [Stulle]

Forks

- A “hard fork” leads to incompatible splits of the blockchain –
  UTXO are doubled!
- Bitcoin Cash *(BCH // August 1, 2017)*
  Block size of 8 MB to increase transaction performance
- Bitcoin Gold *(BTG // October 23, 2017)*
  Mining with Equihash algorithm to push back ASICs
- Overview of market capitalization at [coincap.io]





#	Name	Market Cap ⌄	Price	24hour VWAP	Available Supply	24 Hour Volume	%24hr	Trade
1	Bitcoin BTC	$178.015.705.509	$10139.00000000	$10653.3000	16.709.912	$11.960.100.000	1.22%	Buy / Sell
2	Ethereum ETH	$44.356.844.491	$435.89000000	$461.8630	96.038.965	$2.851.590.000	-5.18%	Buy / Sell
3	Bitcoin Cash BCH	$24.557.493.554	$1375.70309400	$1520.0000	16.829.538	$2.439.170.000	-3.16%	Buy / Sell
4	Ripple XRP	$9.850.299.623	$0.24396000	$0.2550	38.622.870.411	$521.608.000	-11.91%	Buy / Sell
5	Dash DASH	$5.573.419.722	$752.71400000	$722.0650	7.718.723	$444.782.000	11.24%	Buy / Sell
6	Bitcoin Gold BTG	$5.314.617.150	$297.72536499	$318.6360	16.679.274	$251.508.000	1.50%	
7	Litecoin LTC	$4.960.895.951	$89.09000000	$91.7646	54.061.108	$732.764.000	-8.76%	Buy / Sell
8	IOTA IOT	$3.755.756.908	$1.32000000	$1.3512	2.779.530.283	$287.864.000	-10.21%	
9	Monero XMR	$2.830.365.147	$179.56000000	$183.6490	15.411.819	$186.561.000	-8.82%	Buy / Sell
10	Ethereum Classic ETC	$2.759.594.426	$24.74300000	$28.1795	97.929.148	$1.011.040.000	-11.31%	Buy / Sell

Disruptive blockchain applications

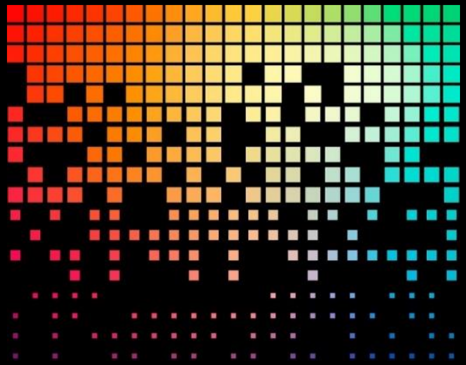
- Already available today
  - Digital Identity of citizens, e.g.: [City of Zug]
  - Prediction Markets, e.g.: [predictious.com]
  - Auctions, e.g.: [domraider.io]

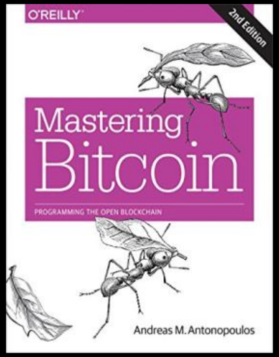
- Future applications
  - Rental of Smart Properties –
    Car or apartment door as Bitcoin node (SPV)
  - Saving the hash values of data of IoT-enabled devices,
    e.g.: Real driving emissions of vehicles
  - Hedging, also for private users –
    insuring short-term life risks, inexpensive derivatives and futures contracts for all!
- For more: [smartcontract.world/Blockchain.pdf]

Risks

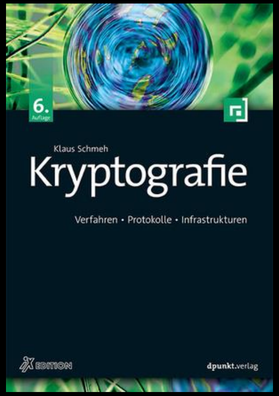
- Bugs in [Bitcoin Core] („Code is law!“)
- Pollution of the blockchain with data whose possession is punishable by law
  - [Paper] “A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin” by Roman Matzutt et al. // February 1, 2018
- Collapse of important exchanges, Bsp.: [Mt. Gox]
- P2P network imbalances, 51% attack
- Gossip & Politics
  - Prohibition of PoW mining due to high energy consumption
  - Ban on crypto currencies through lobbying by financial dinosaurs

Related Literature

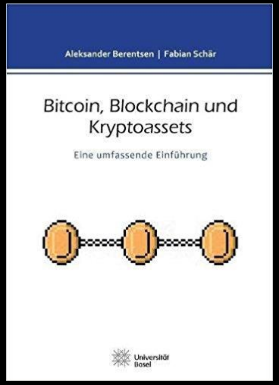




- Andreas M. Antonopoulos
  Mastering Bitcoin
  2nd Edition, O'Reilly 2017
  ISBN-13: 978-1491954386 – [bitcoinbook.info]



- Klaus Schmeh
  Kryptografie – Verfahren, Protokolle, Infrastrukturen
  6. Auflage, dpunkt.verlag 2016
  ISBN-13: 978-3864903564 – [dpunkt.de]


Aleksander Berentsen | Fabian Schär
Bitcoin, Blockchain und Kryptoassets
Eine umfassende Einführung
Universität Basel

- Aleksander Berentsen, Fabian Schär
  Bitcoin, Blockchain und Kryptoassets
  Universität Basel
  ISBN-13: 978-3738653922 – [blockchainbuch.de]

Thank you!

- Dr.-Ing. Markus A. Stulle
  Munich | Germany

- markus@stulle.ai
  stulle.ai

„The best way to predict the future is to invent it!“ – Alan Kay