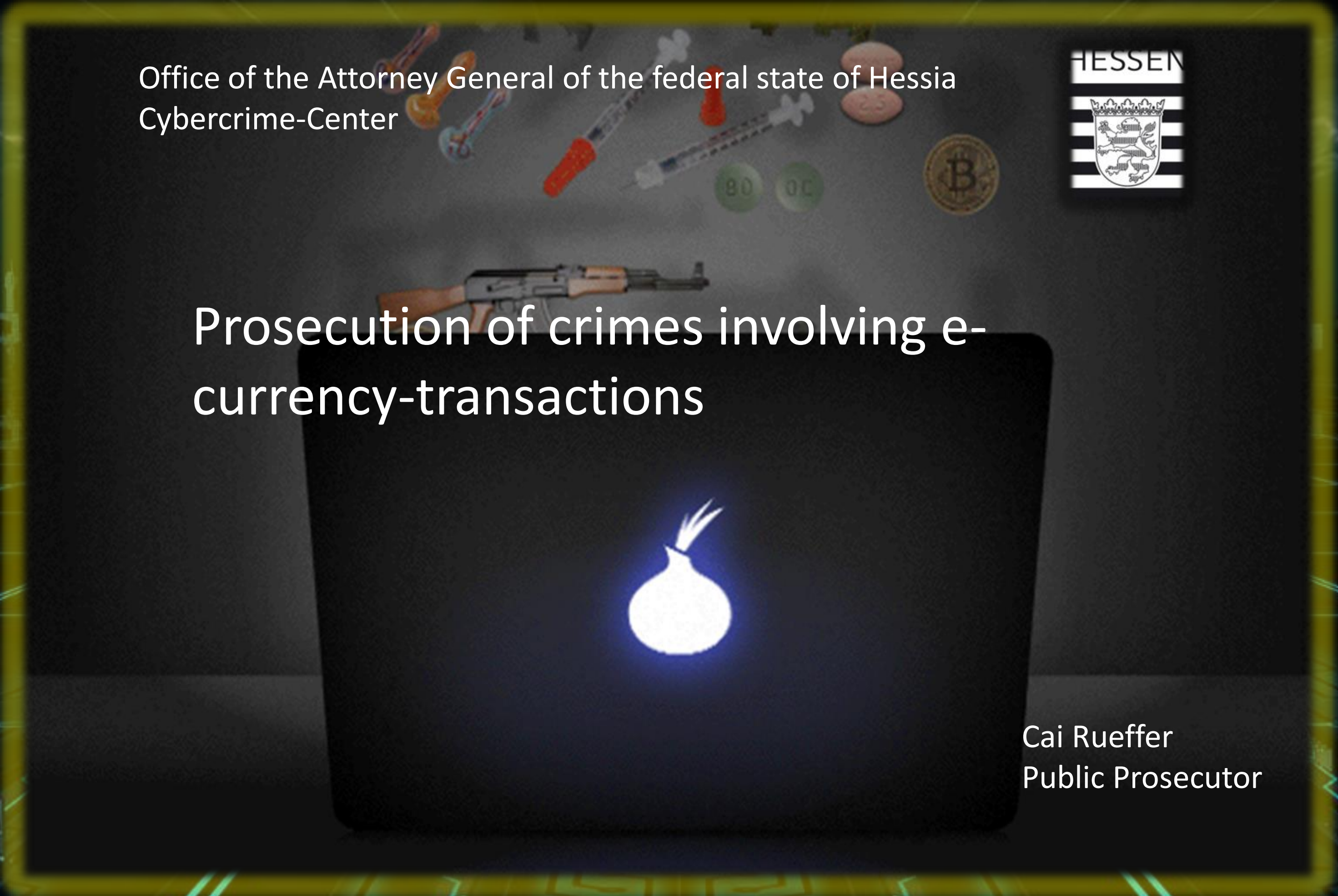
Office of the Attorney General of the federal state of Hessia
Cybercrime-Center

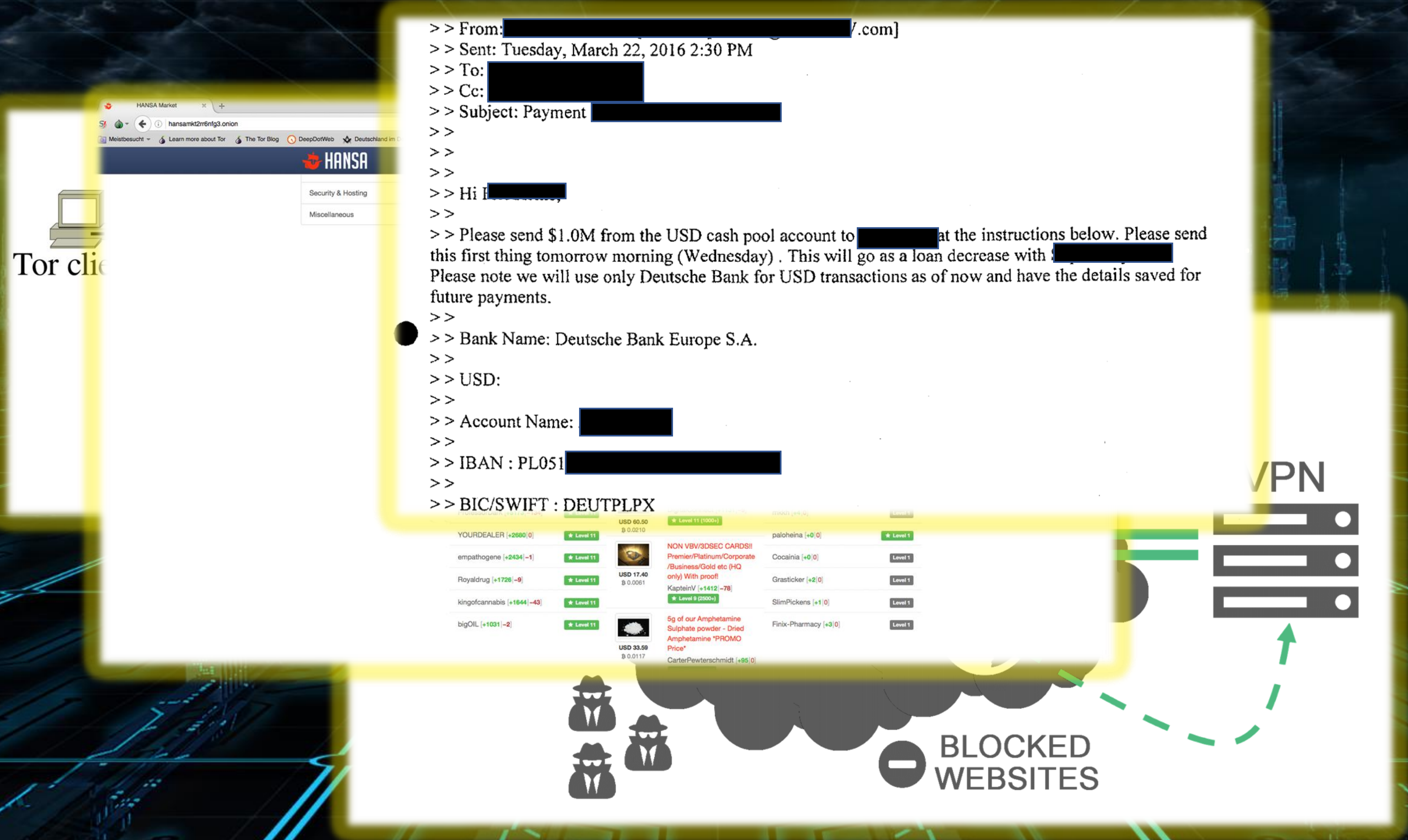
Prosecution of crimes involving e-currency-transactions



Cai Rueffer
Public Prosecutor

Agenda

1. General rule in prosecuting cybercrime: follow the way of the money
2. Crypto-currencies a new way of payment – what is this?
3. Crypto-currencies make investigations more difficult
4. Possible angles and solutions
5. Sequestration of crypto-currencies
6. Case study: OP Sushi



> > From: [redacted].com]
> > Sent: Tuesday, March 22, 2016 2:30 PM
> > To: [redacted]
> > Cc: [redacted]
> > Subject: Payment [redacted]
> >
> >
> >
> > Hi [redacted]
> >
> > Please send $1.0M from the USD cash pool account to [redacted] at the instructions below. Please send this first thing tomorrow morning (Wednesday) . This will go as a loan decrease with [redacted]
Please note we will use only Deutsche Bank for USD transactions as of now and have the details saved for future payments.
> >
> > Bank Name: Deutsche Bank Europe S.A.
> >
> > USD:
> >
> > Account Name: [redacted]
> >
> > IBAN : PL051 [redacted]
> >
> > BIC/SWIFT : DEUTPLPX

YOURDEALER [+2680|0] ★ Level 11
empathogene [+2434|−1] ★ Level 11
Royaldrug [+1726|−9] ★ Level 11
kingofcannabis [+1644|−43] ★ Level 11
bigOIL [+1031|−2] ★ Level 11

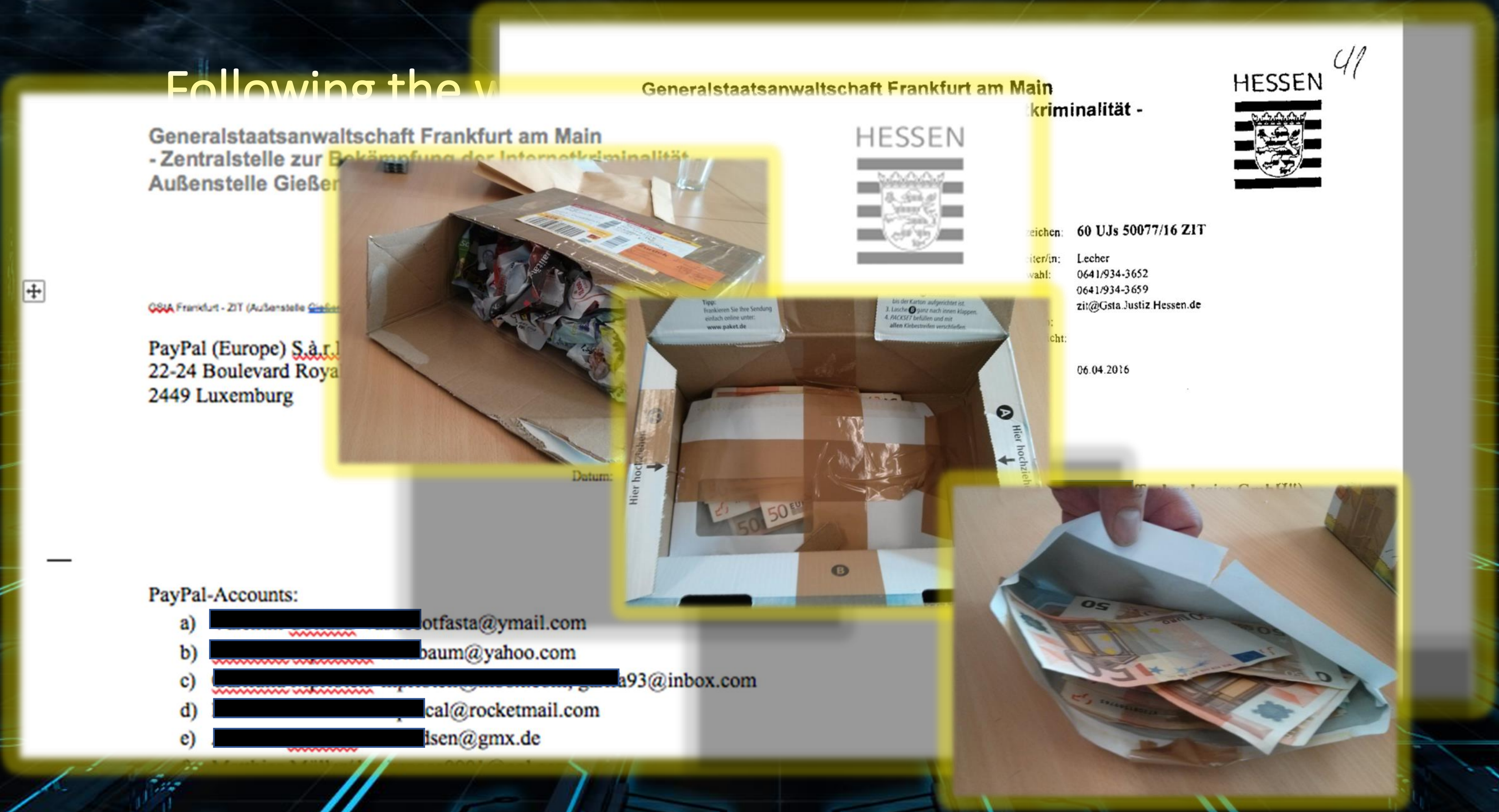
USD 60.50
฿ 0.0210
★ Level 11 (1000+)

NON VBV/3DSEC CARDS!! Premier/Platinum/Corporate /Business/Gold etc (HQ only) With proof!
USD 17.40
฿ 0.0061
KapteinV [+1412|−78]
★ Level 9 (2500+)

5g of our Amphetamine Sulphate powder - Dried Amphetamine *PROMO Price*
USD 33.59
฿ 0.0117
CarterPewterschmidt [+95|0]

paloheina [+0|0] ★ Level 1
Cocainia [+0|0] Level 1
Grasticker [+2|0] Level 1
SlimPickens [+1|0] Level 1
Finix-Pharmacy [+3|0] Level 1

Following the v



Generalstaatsanwaltschaft Frankfurt am Main
- Zentralstelle zur Bekämpfung der Internetkriminalität -
Außenstelle Gießen

HESSEN

GStA Frankfurt - ZIT (Außenstelle Gießen

PayPal (Europe) S.à.r.l.
22-24 Boulevard Roya
2449 Luxemburg

Datum:

PayPal-Accounts:

a) [redacted]otfasta@ymail.com
b) [redacted]baum@yahoo.com
c) ([redacted]a93@inbox.com
d) [redacted]cal@rocketmail.com
e) [redacted]dsen@gmx.de

Generalstaatsanwaltschaft Frankfurt am Main
kriminalität -

HESSEN

41

eichen: 60 UJs 50077/16 ZIT
iter/in: Lecher
wahl: 0641/934-3652
0641/934-3659
zit@Gsta.Justiz.Hessen.de

cht:

06.04.2016

Tipp:
Frankieren Sie Ihre Sendung
einfach online unter:
www.paket.de
bis der Karton aufgerichtet ist.
3. Lasche B ganz nach innen klappen.
4. PACKSET befüllen und mit
allen Klebestreifen verschließen.
A
Hier hochziehen
Hier hochziehen
B
50

Cryp

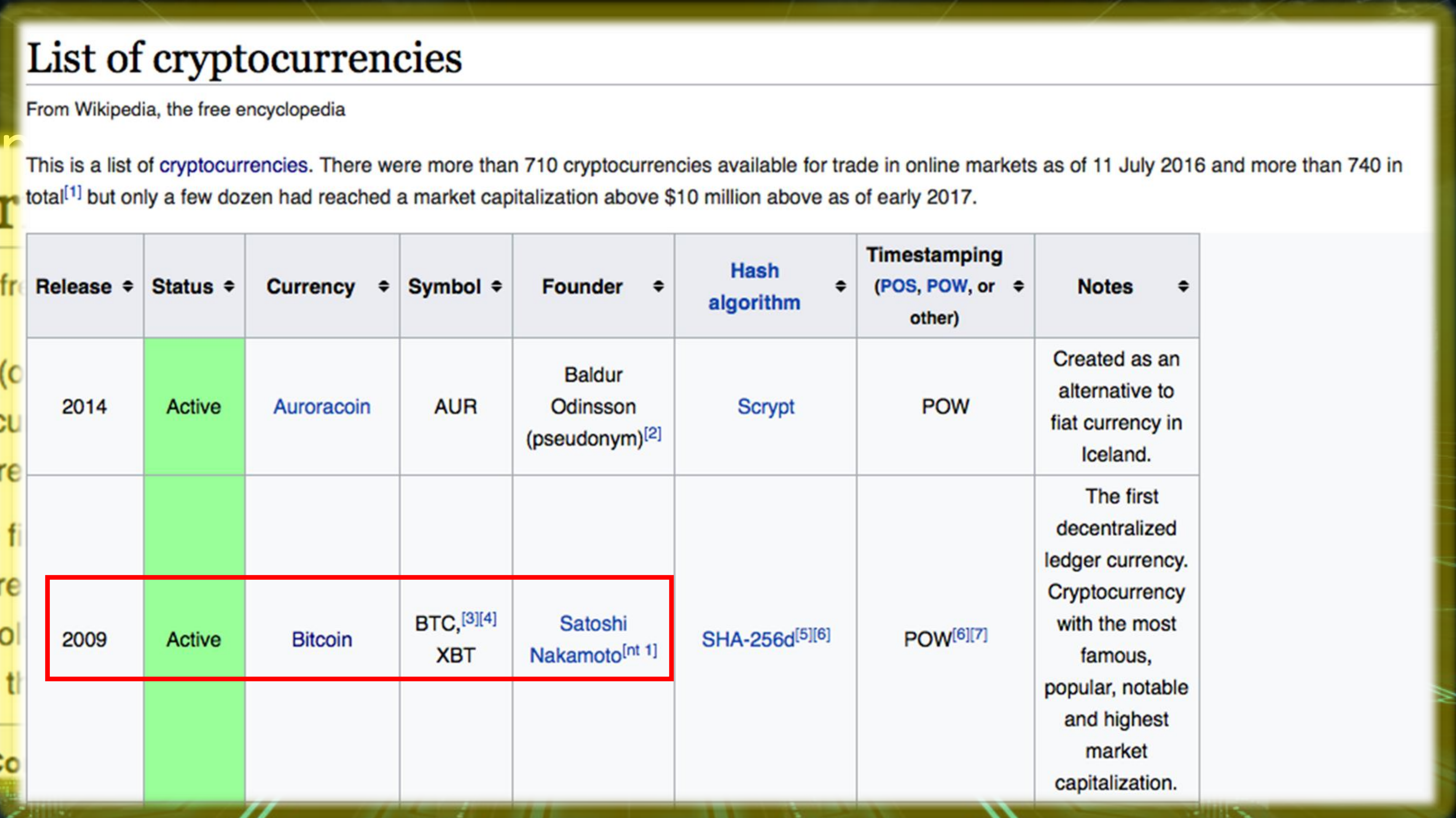
Cryptocur

From Wikipedia, the fr

A **cryptocurrency** (c
cryptography to secu
Cryptocurrencies are

Bitcoin became the fi
created.[3] These are
decentralized contro
control is related to th

Co



List of cryptocurrencies

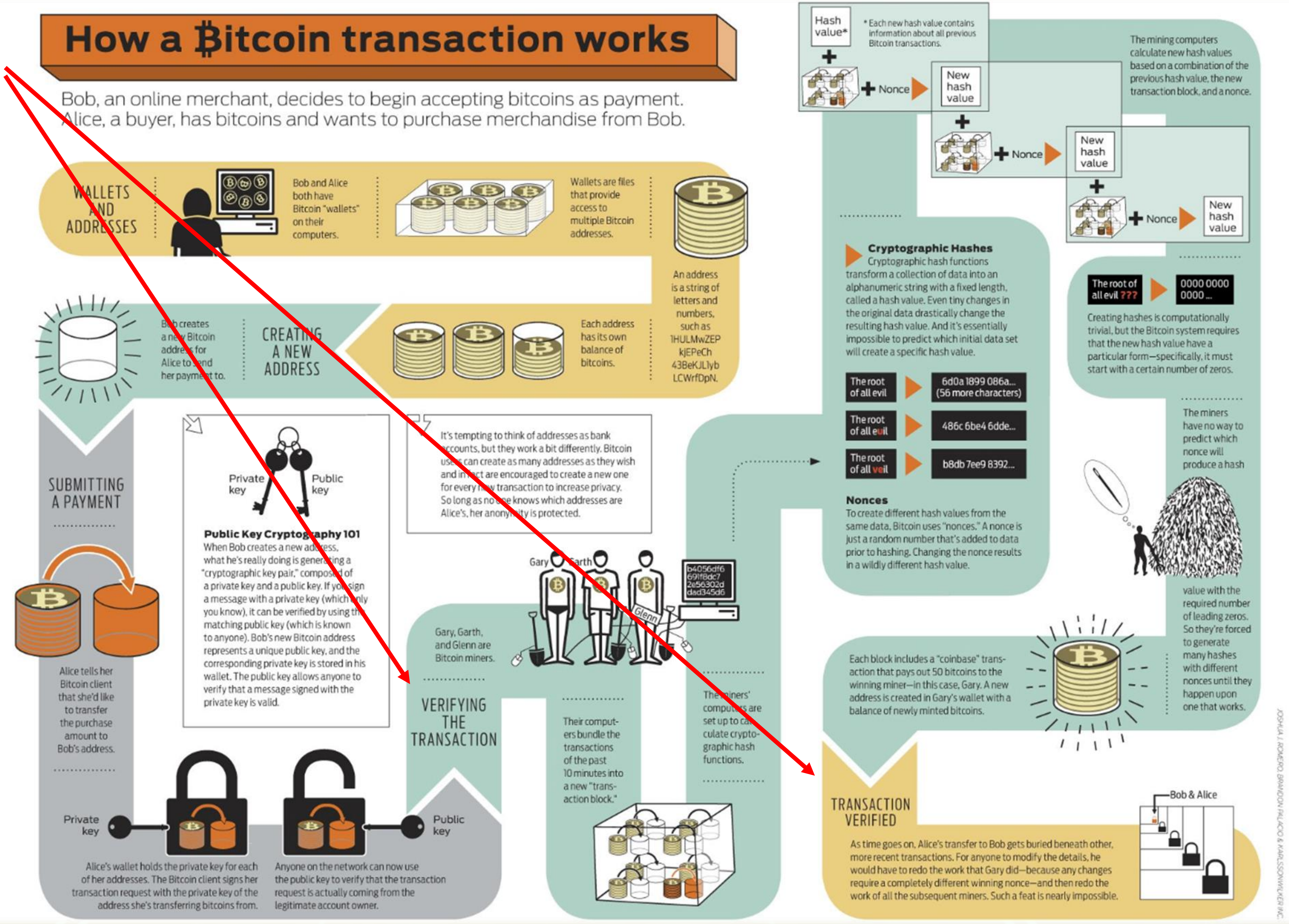
From Wikipedia, the free encyclopedia

This is a list of cryptocurrencies. There were more than 710 cryptocurrencies available for trade in online markets as of 11 July 2016 and more than 740 in total[1] but only a few dozen had reached a market capitalization above $10 million above as of early 2017.

Release ⬍	Status ⬍	Currency ⬍	Symbol ⬍	Founder ⬍	Hash algorithm ⬍	Timestamping (POS, POW, or other) ⬍	Notes ⬍
2014	Active	Auroracoin	AUR	Baldur Odinsson (pseudonym)[2]	Scrypt	POW	Created as an alternative to fiat currency in Iceland.
2009	Active	Bitcoin	BTC,[3][4] XBT	Satoshi Nakamoto[nt 1]	SHA-256d[5][6]	POW[6][7]	The first decentralized ledger currency. Cryptocurrency with the most famous, popular, notable and highest market capitalization.

How a Bitcoin 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 1HULMwZEPkjEPeCh43BeKJL1yb LCWrfDpN.

Each address has its own balance of bitcoins.

CREATING A NEW ADDRESS

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

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.

* Each new hash value contains information about all previous Bitcoin transactions.

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 euil	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.

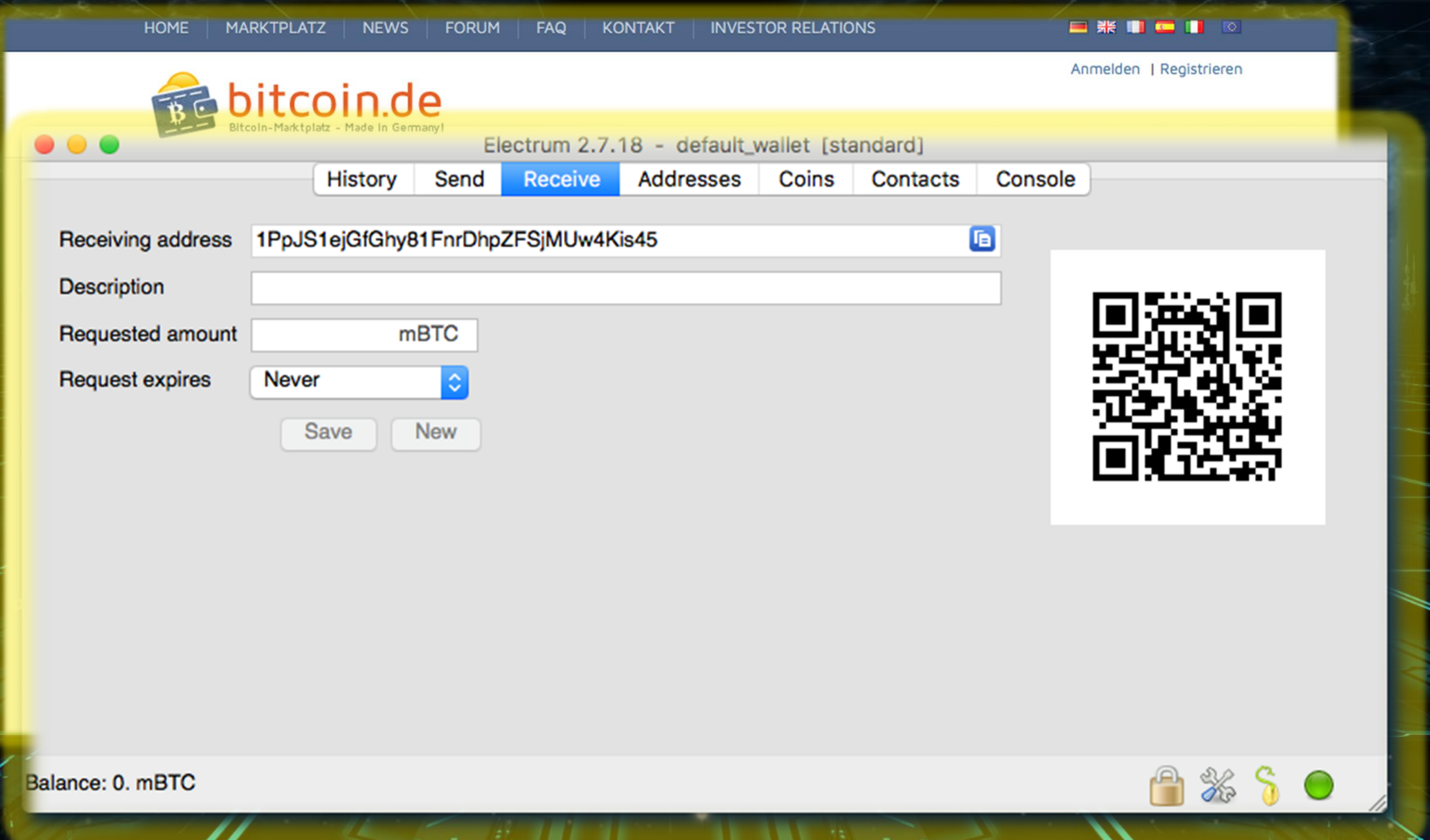
The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

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.

JOSHUA J. ROMERO; BRANDON PALACIO & KARLSSONWILKER INC.



Electrum 2.7.18 - default_wallet [standard]

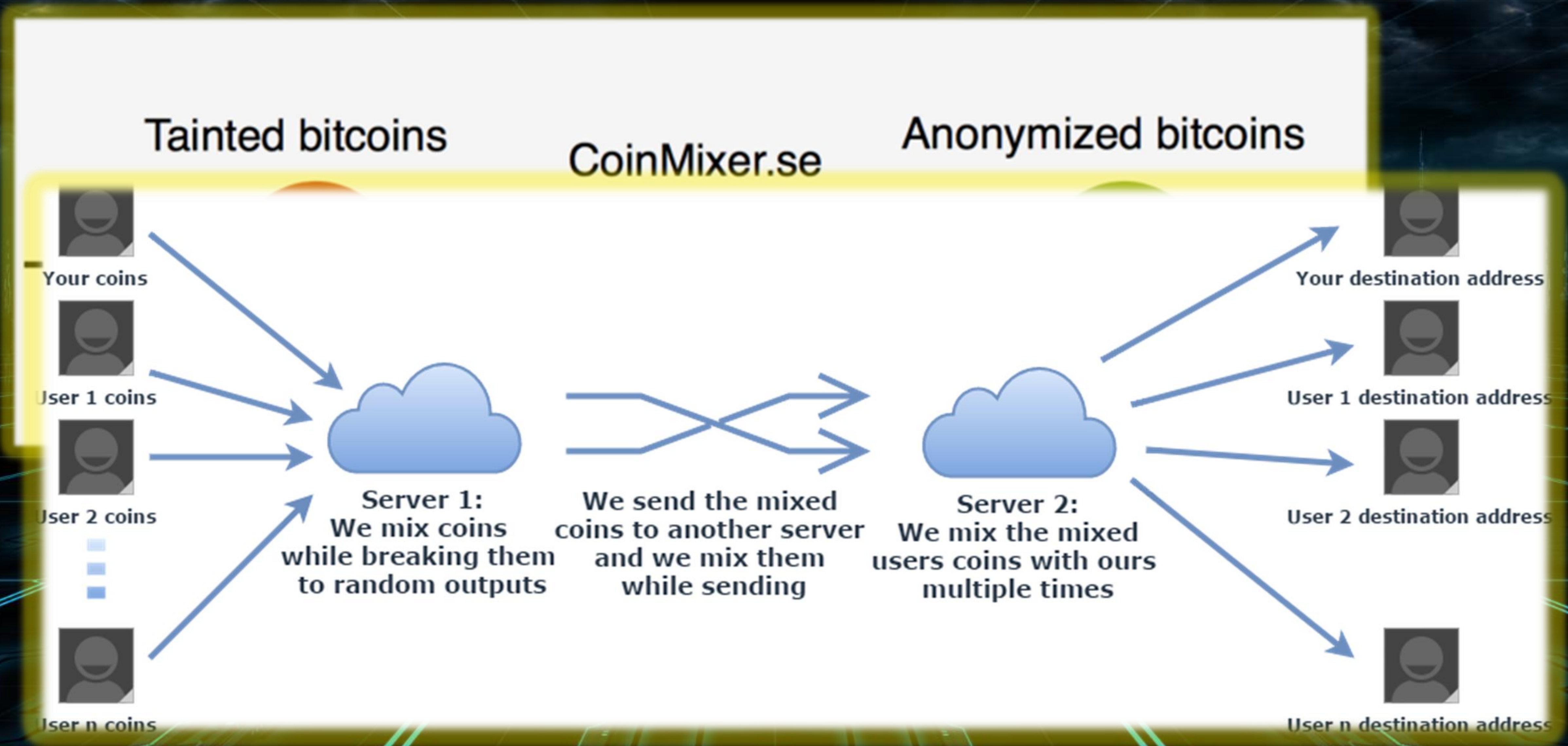
Receiving address: 1PpJS1ejGfGhy81FnrDhpZFSjMUw4Kis45

Description:

Requested amount: mBTC

Request expires: Never

Balance: 0. mBTC



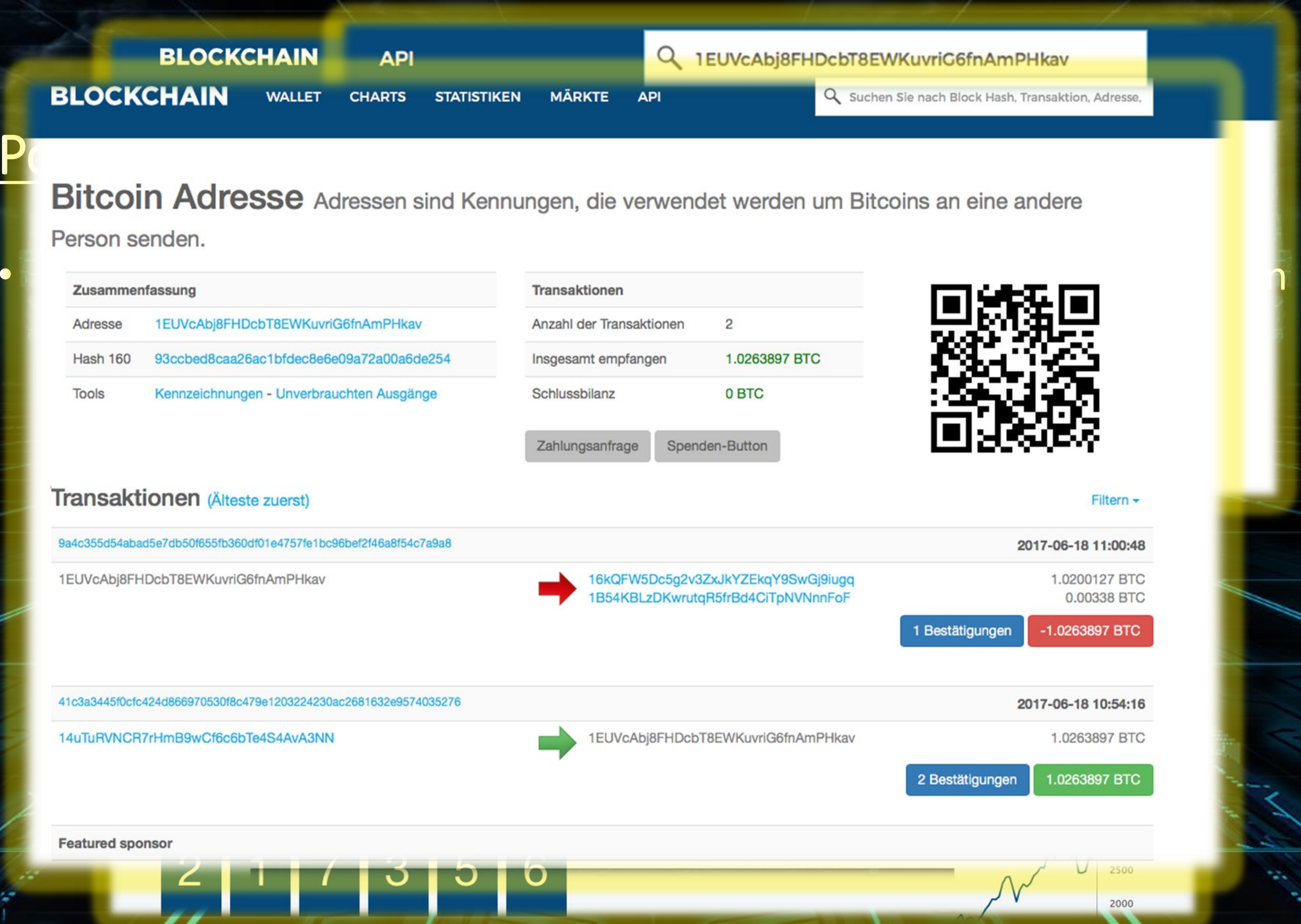
Server 1:
We mix coins
while breaking them
to random outputs

We send the mixed
coins to another server
and we mix them
while sending

Server 2:
We mix the mixed
users coins with ours
multiple times

Po

- n



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

Zusammenfassung	
Adresse	1EUVcAbj8FHDcbT8EWKuvriG6fnAmPHkav
Hash 160	93ccbed8caa26ac1bfdec8e6e09a72a00a6de254
Tools	Kennzeichnungen - Unverbrauchten Ausgänge

Transaktionen	
Anzahl der Transaktionen	2
Insgesamt empfangen	1.0263897 BTC
Schlussbilanz	0 BTC

Transaktionen (Älteste zuerst)

9a4c355d54abad5e7db50f655fb360df01e4757fe1bc96bef2f46a8f54c7a9a8 2017-06-18 11:00:48

1EUVcAbj8FHDcbT8EWKuvriG6fnAmPHkav → 16kQFW5Dc5g2v3ZxJkYZEkqY9SwGj9iugq 1.0200127 BTC
1B54KBLzDKwrutqR5frBd4CiTpNVNnnFoF 0.00338 BTC

1 Bestätigungen -1.0263897 BTC

41c3a3445f0cfc424d866970530f8c479e1203224230ac2681632e9574035276 2017-06-18 10:54:16

14uTuRVNCR7rHmB9wCf6c6bTe4S4AvA3NN → 1EUVcAbj8FHDcbT8EWKuvriG6fnAmPHkav 1.0263897 BTC

2 Bestätigungen 1.0263897 BTC

Featured sponsor

Datenaktualisierung vor: 5 Sekunden

Kaufen »

Menge (min.)	Preis/BTC	Volumen
1 (1)	2.310,00 €	2.310,00 €
0,2158 (0,2158)	2.314,99 €	499,57 €
0,44 (0,22)	2.319,71 €	1.020,67 €
0,5 (0,25)	2.320,00 €	1.160,00 €
1 (0,1)	2.320,00 €	2.320,00 €
0,33 (0,1)	2.322,99 €	766,59 €

Weitere Verkaufsangebote »

0.30519173 BTC

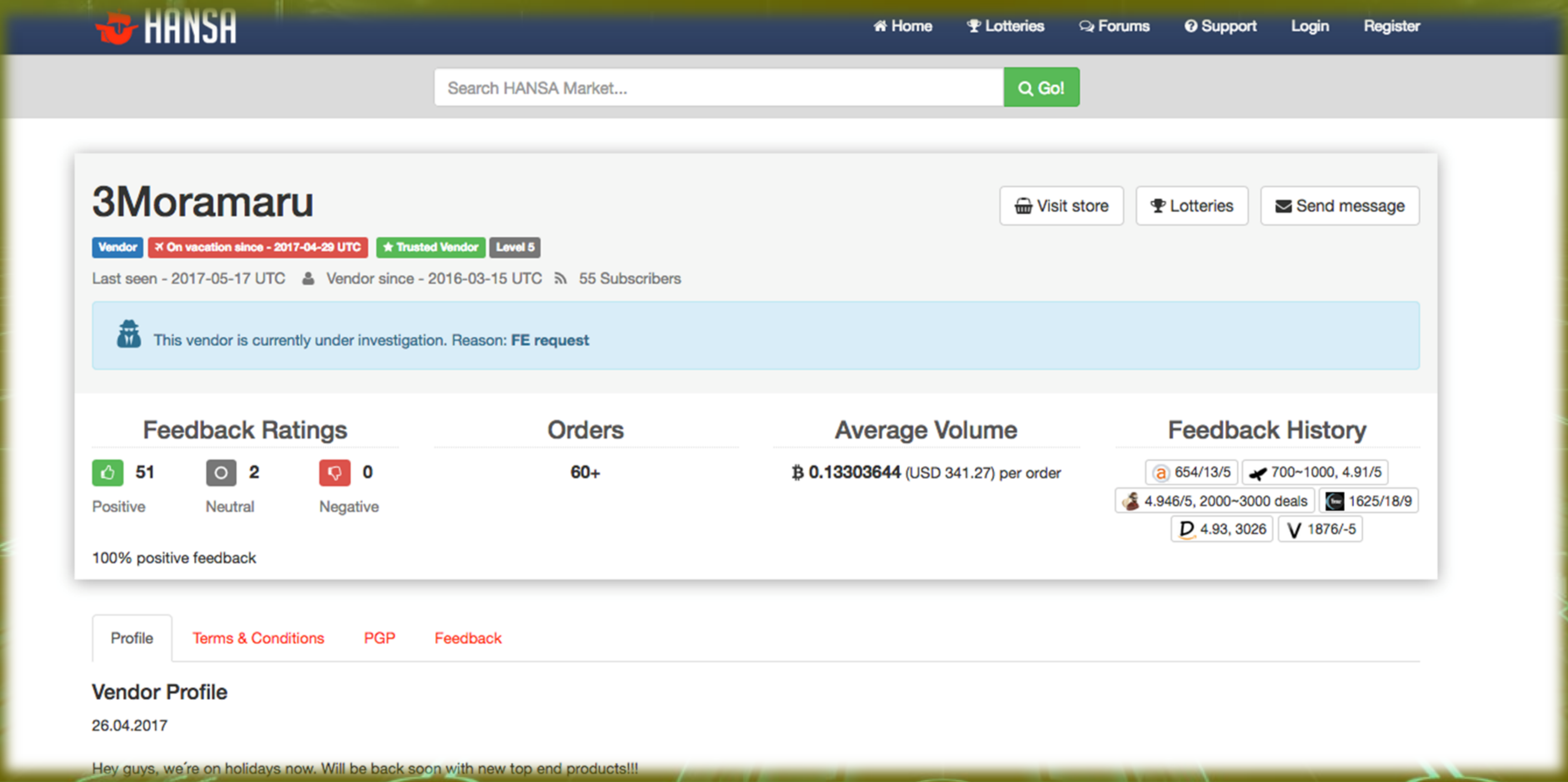
Total Transactions	4
Total Received	0.50519173 BTC
Total Sent	0.20 BTC
Final Balance	0.30519173 BTC

This Is Your Bitcoin Address

Sequestration of crypto-currencies

- In general no specific provisions on sequestration of crypto-currencies in domestic laws
- Thus, we apply the general rules for sequestration
- During house search we try to get access to the wallet…
- …and wire the coins to a police-wallet
- For this purpose we‘ve registered with commercial exangers
- Since the exchange-rates are generally extremely volatile, we apply same provisions as for perishable goods (e.g. fish etc.)
- Thus no court order is required to transfer crypto-money into fiat

Case study: Operation Sushi



3Moramaru

Vendor | On vacation since - 2017-04-29 UTC | ★ Trusted Vendor | Level 5

Last seen - 2017-05-17 UTC   Vendor since - 2016-03-15 UTC   55 Subscribers

This vendor is currently under investigation. Reason: **FE request**

Feedback Ratings	Orders	Average Volume	Feedback History
51 Positive 2 Neutral 0 Negative 100% positive feedback	60+	฿ **0.13303644** (USD 341.27) per order	654/13/5 700~1000, 4.91/5 4.946/5, 2000~3000 deals 1625/18/9 4.93, 3026 1876/-5

Profile | Terms & Conditions | PGP | Feedback

Vendor Profile

26.04.2017

Hey guys, we´re on holidays now. Will be back soon with new top end products!!!

Any questions?

Thanks for your attention!