Anonymous Crypto Currency

Stealth Address, Ring Signatures, Monero

Comparison to Zero.Cash

17 B$

60 M$

300 M$

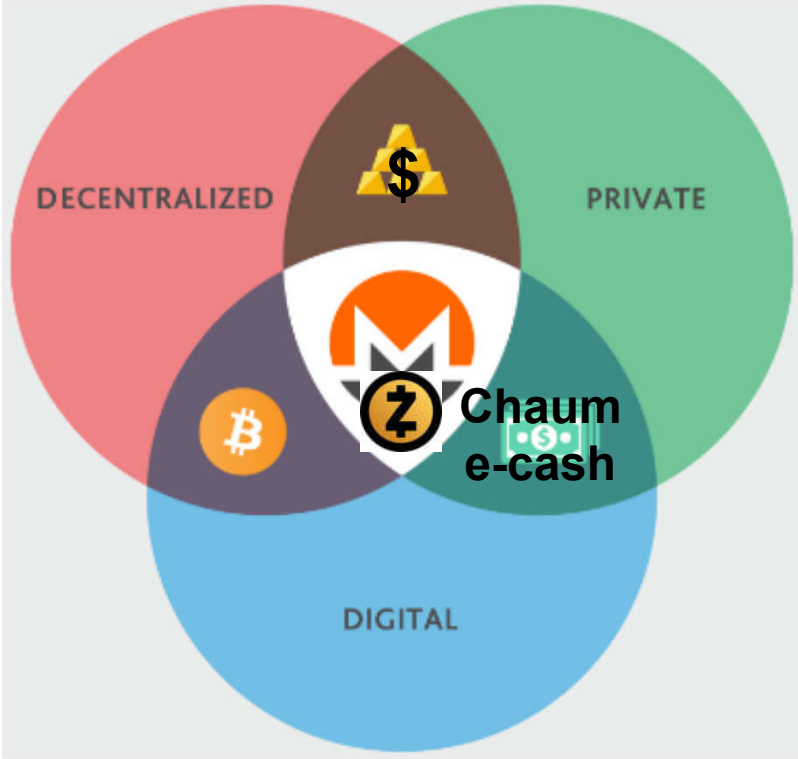
Nicolas T. Courtois

with help of Rebekah Mercer, Huanyu Ma, Mary Maller

- **U**niversity **C**ollege **L**ondon, UK

Topics

Bitcoin vs. Monero vs. ZCash



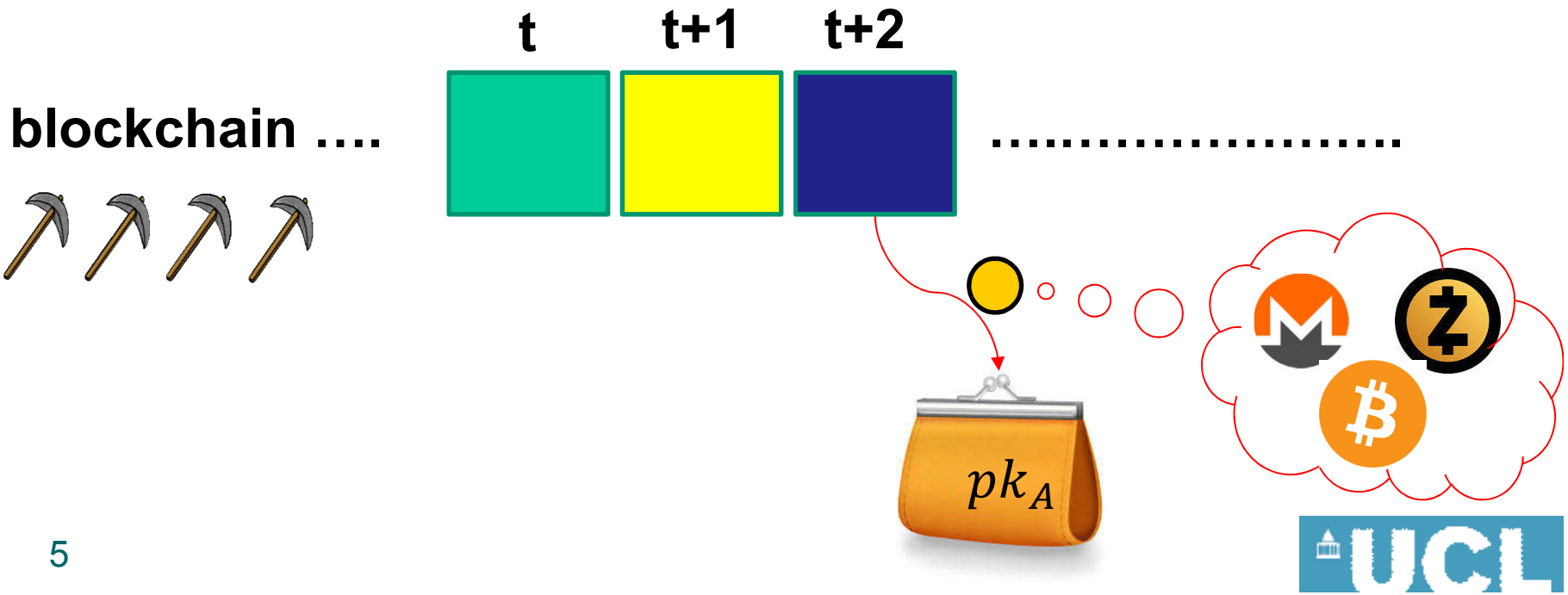
Privacy / anonymity:

- for senders [Ring Signatures,ZK proofs]
- for receivers [Stealth Address methods]
- for the transaction amount [CT] X

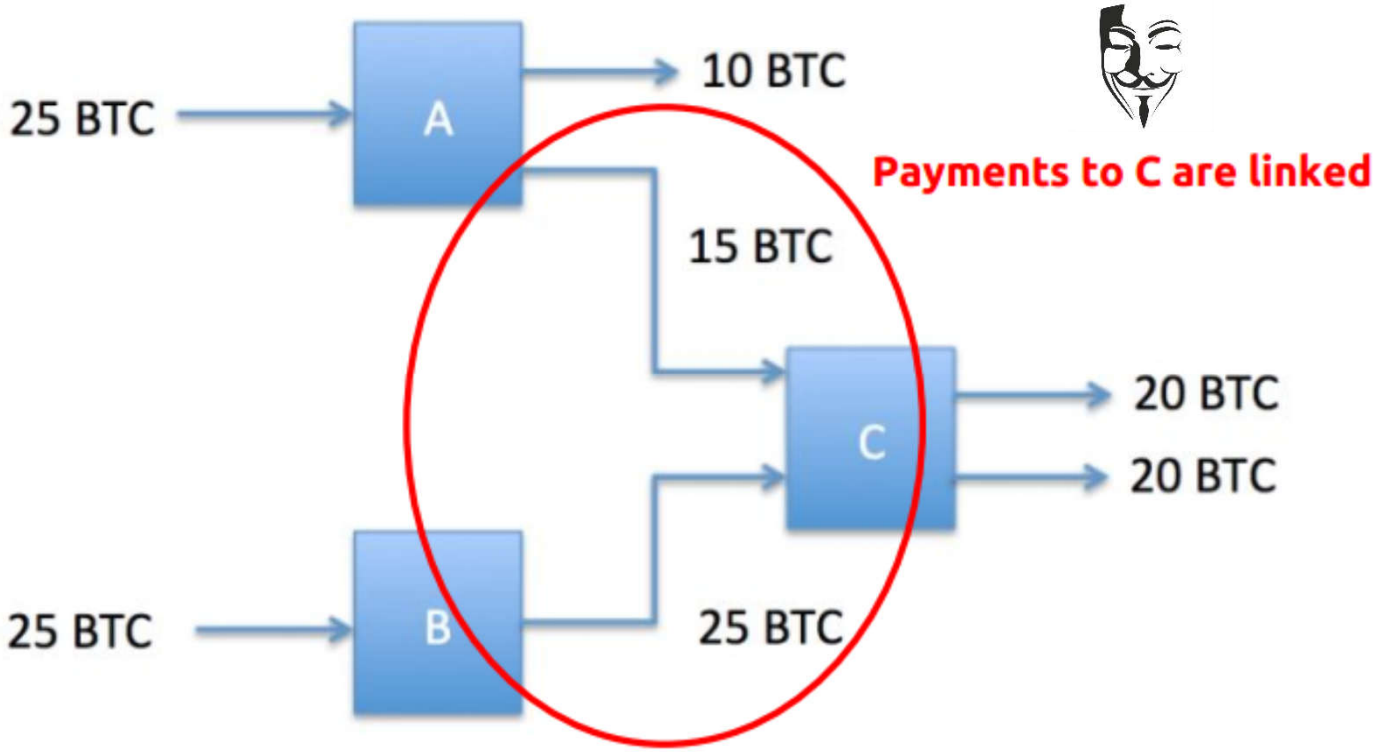
CT=Confidential Transactions, not studied here

PK-based currencies

blockchain says:
1 coin belongs to pk_A

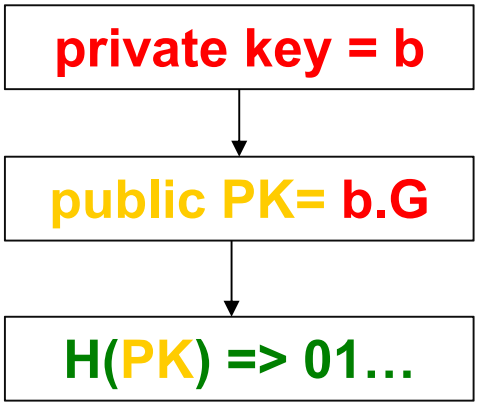


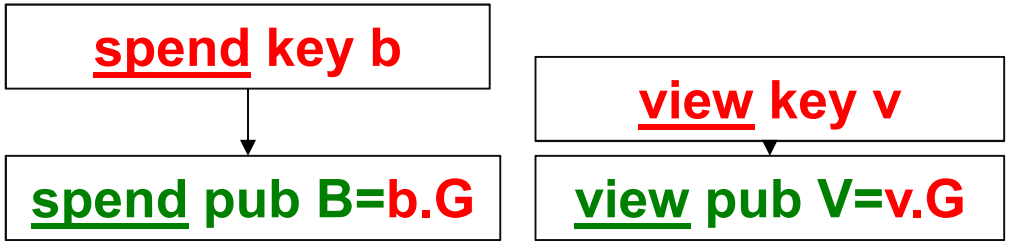
Pb In Bitcoin

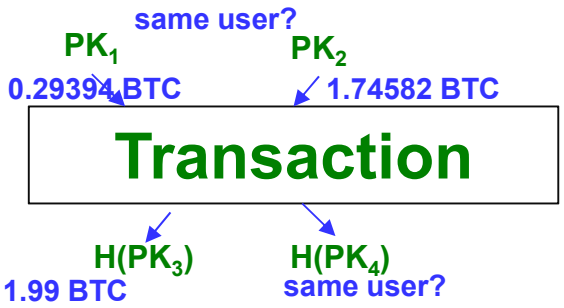


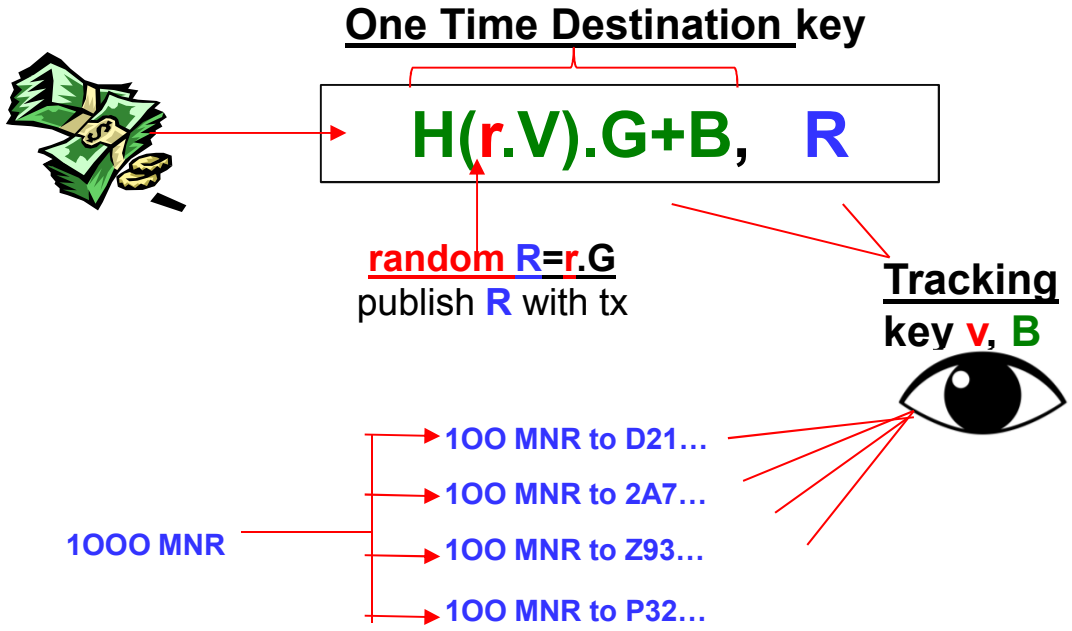
Q: Does Monero/ZCash remove this problem????

**Bitcoin vs. Monero



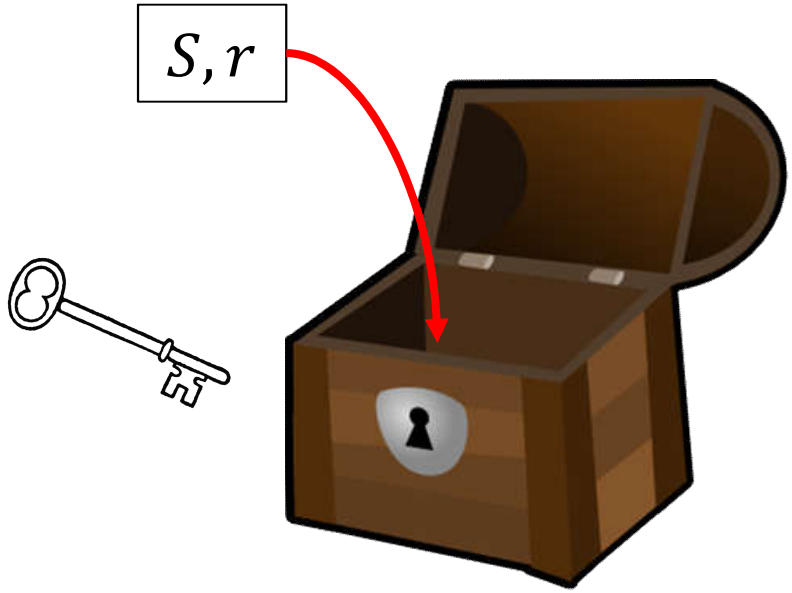




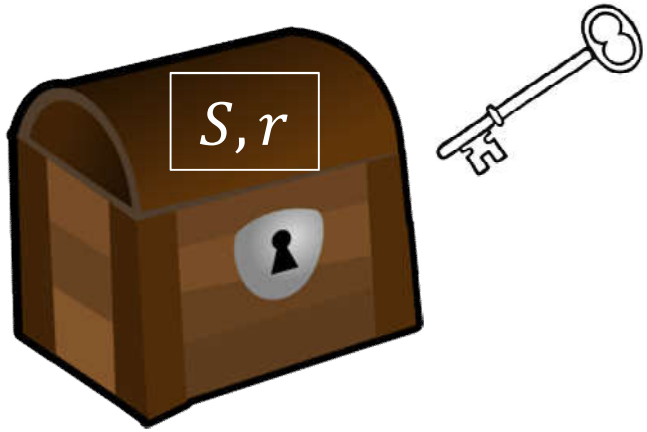


Advanced Crypto Magic

Commitments are used to Shield Coins:



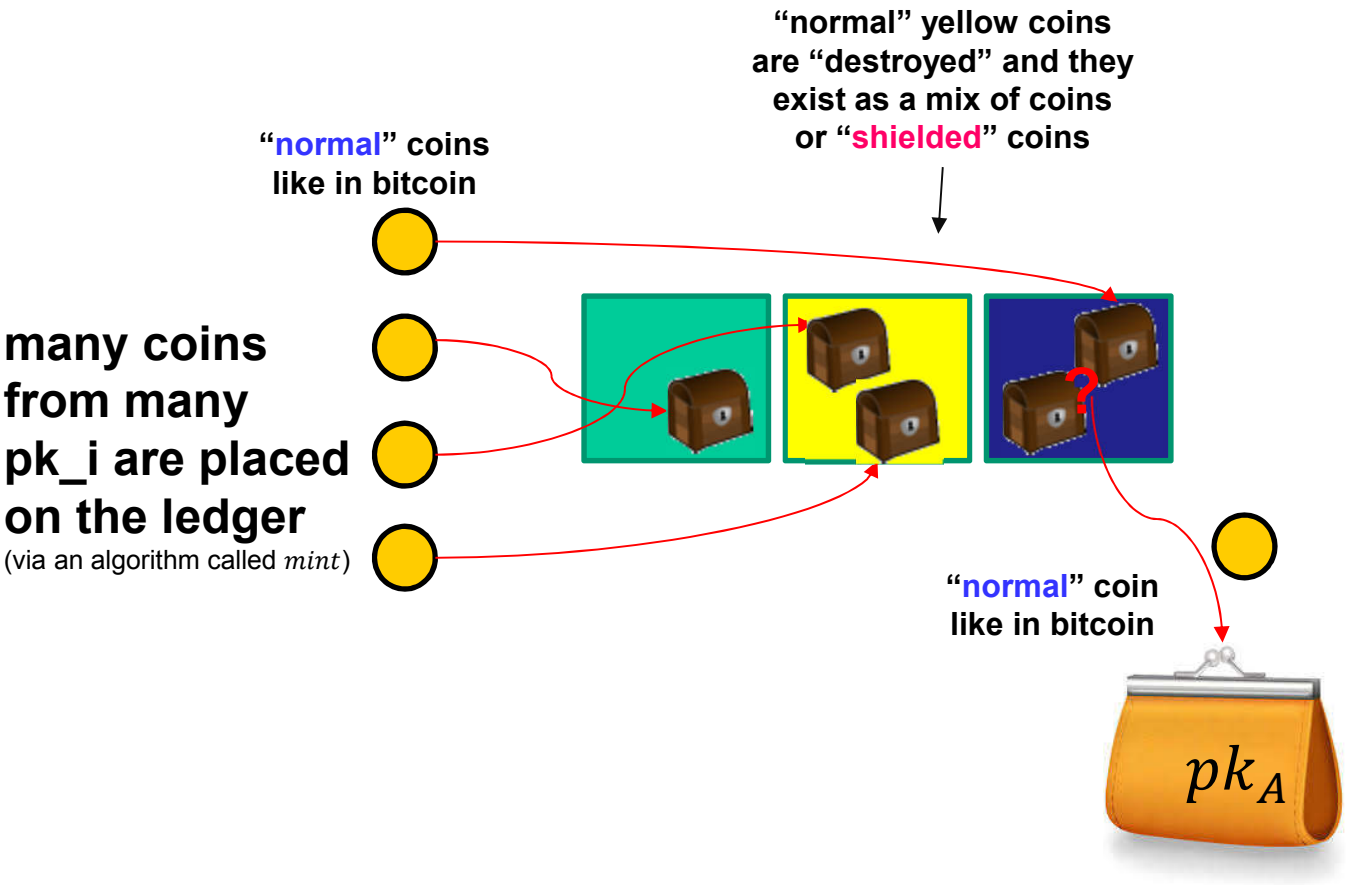
nobody can see what is inside.



only the owner can open

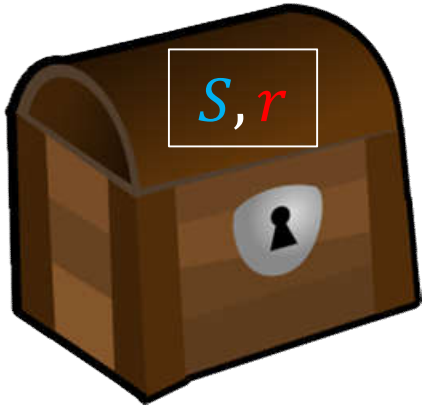
they NEVER actually get opened

ZCash = a Large Scale Mixer



one of the coins that is on the ledger is "re-born" and sent to pk_A, but it is impossible to tell which one?

Double Spending?

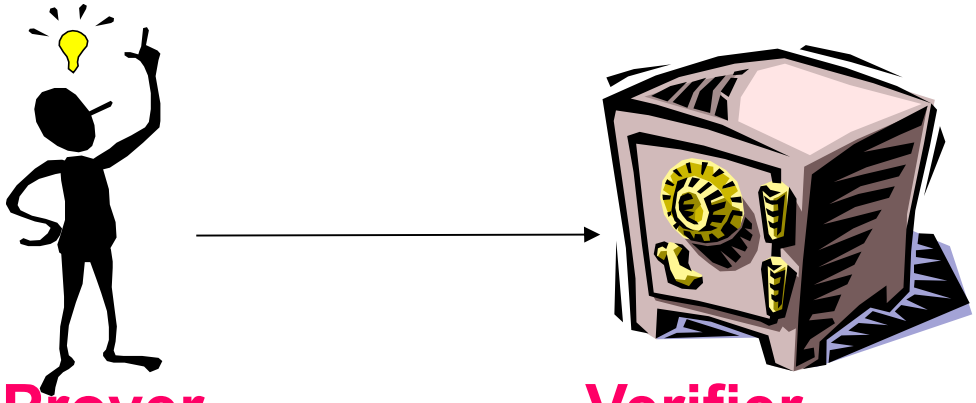


cannot be done twice!

S is revealed

r remains secret

Zero-Knowledge



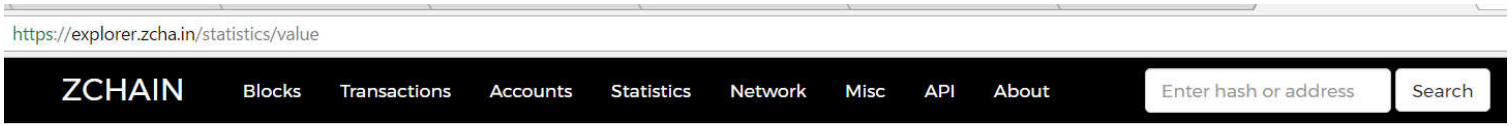
0. Completeness – honest signer always accepted

1. Soundness – dishonest signer always rejected

2. Zero-Knowledge – **the verifier does not learn ANYTHING**

the origin of money spent

Poor Adoption,
8GB of RAM etc…



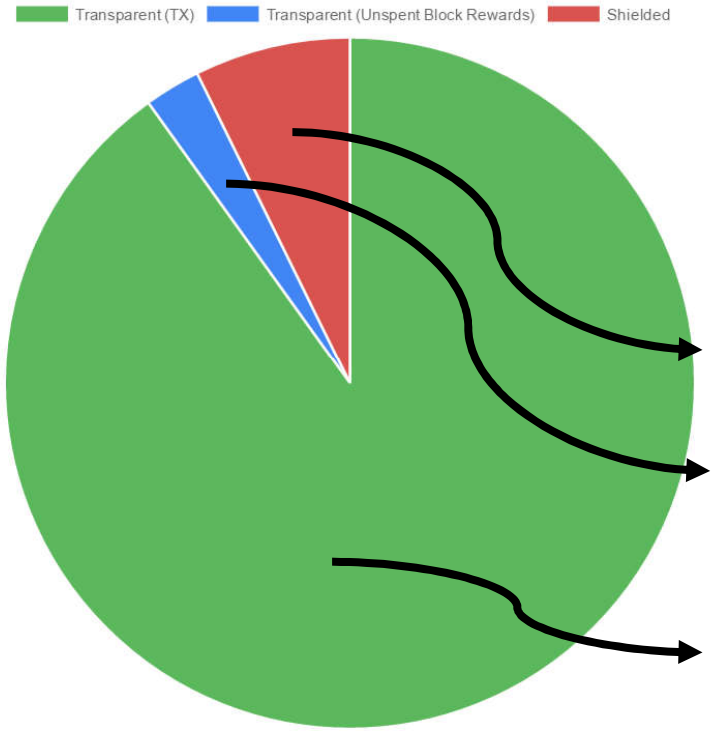
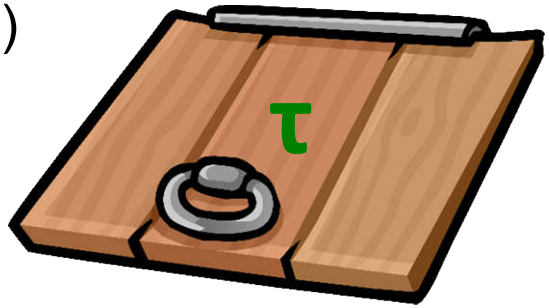


image accessed 14/03/17
explorer.zcha.in/statistics/value

- **shielded coins = 7.3%**
- **transparent unspent block rewards = 2.6%**
- **“normal” transparent coins = 90.1%**

Problems with Z.Cash

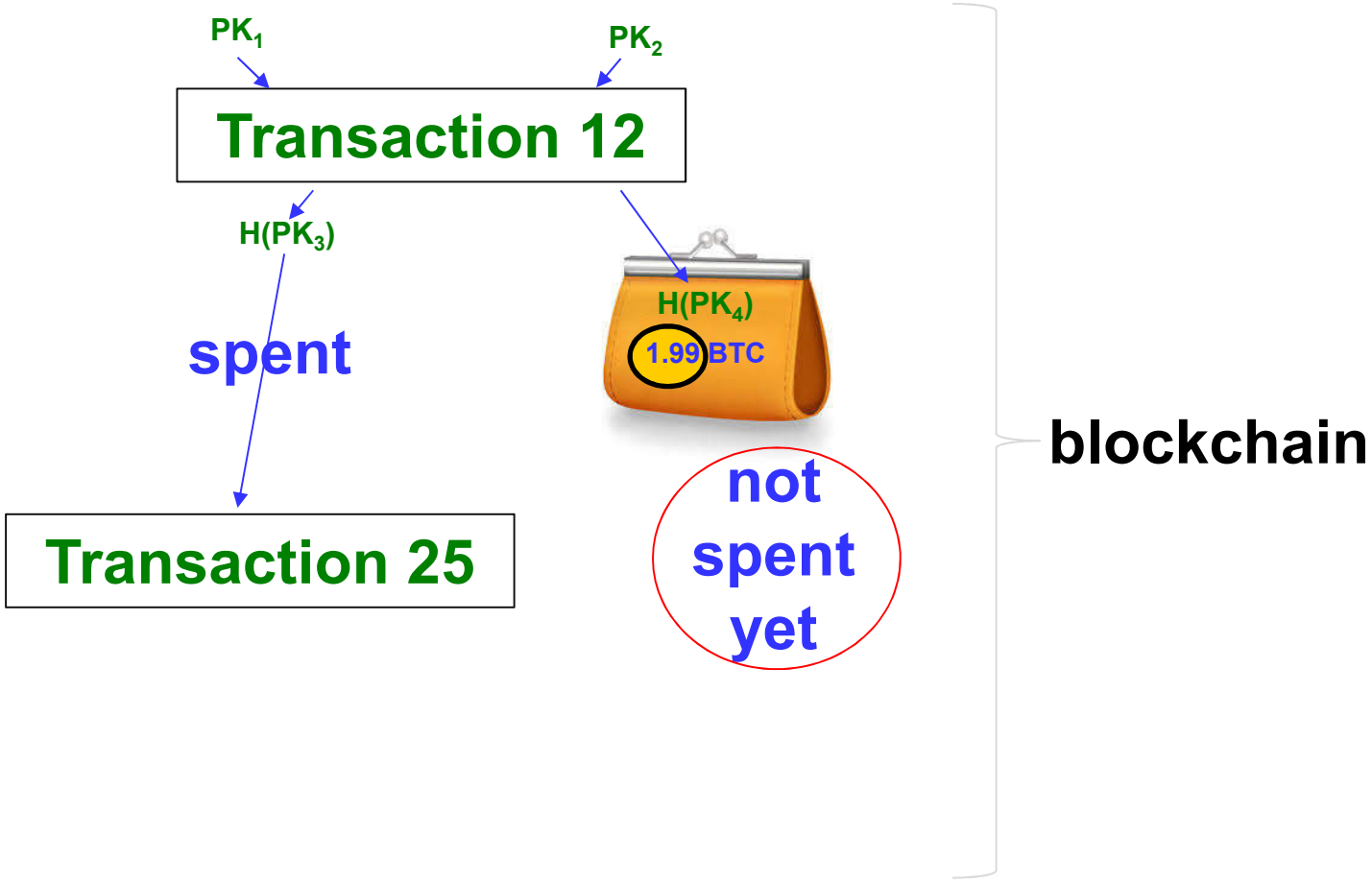
- Whoever sets-up the Z.Cash system (CRS-based) might keep hold of some trapdoor information.
  - This trapdoor τ is material and real: the only hope is that it was erased!



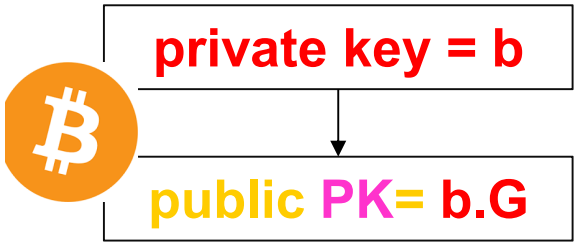
- τ does NOT allow to steal coins of other people
- τ is NOT quantum secure: $\mathbf{g^{\tau}\ mod\ p}$ is published.
- But trapdoor τ allows to create an UNLIMITED number of NEW coins!
  - current Z.Cash does not (yet) have an audit method…

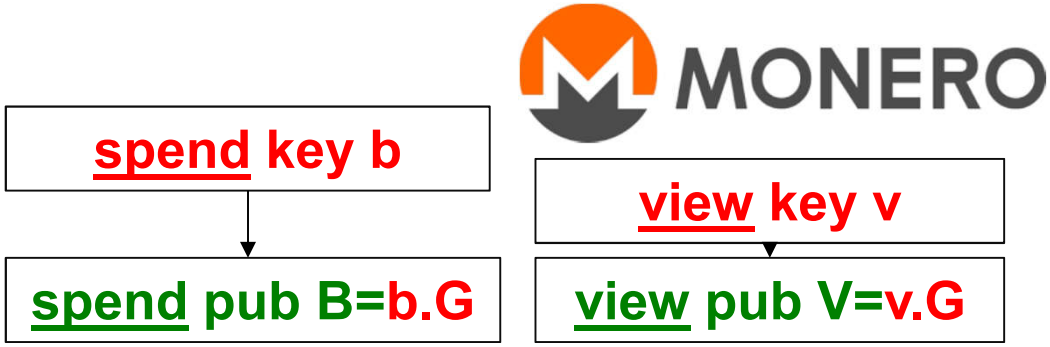
Monero Fundamentals

def: UTXO= Unspent Tx Output



Bitcoin and Monero





One Time Destination PK

PK=H(r.V).G+B, R

Same Principle:

1. **Money is attributed to PK,**
2. **You know the ECDL of this PK**

=>can spend the money!

In Monero the blockchain knows NOTHING except money is flowing between 'fresh' pseudonyms PK.

(also publishes R).

Monero - Covert Creation of Secrets

In Monero the blockchain knows NOTHING about the receiver identity=A,B, (the sender does use A,B).

The blockchain sees only PK

and the extra number **R** (helps to unlock what is inside).

One Time Destination PK

PK=H(r.V).G+B, R

Principle:

The receiver will have a “magical method” to

compute the private key for this one-time PK.

Based on DH + extra pieces.

Dark Wallet over Bitcoin

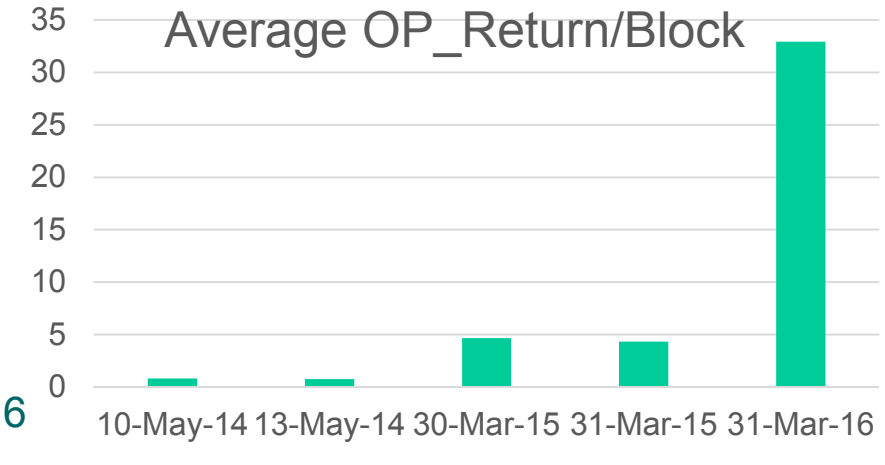
Censorship potential!

```
"script":"6a24aa21a9ed38538750abd25c3a84610d5b6e80c64672b01bcd3ea9d9c518f9de06288ff8d5"
```

Date	Avg/block
10/05/14	0.82353
13/05/14	0.75926
30/03/15	4.66667
31/03/15	4.30769
31/03/16	32.9804

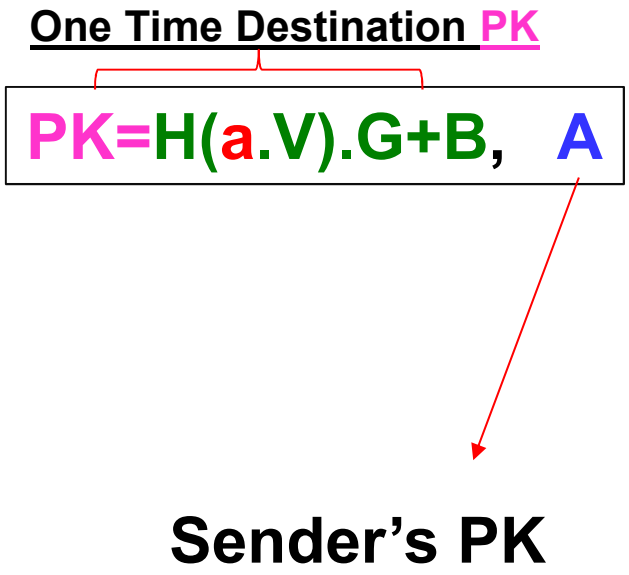
One Time Destination PK

PK=H(r.V).G+B, R



Super Dark Bitcoin

Fact:
there are methods to make these TOTALLY invisible in current bitcoin!

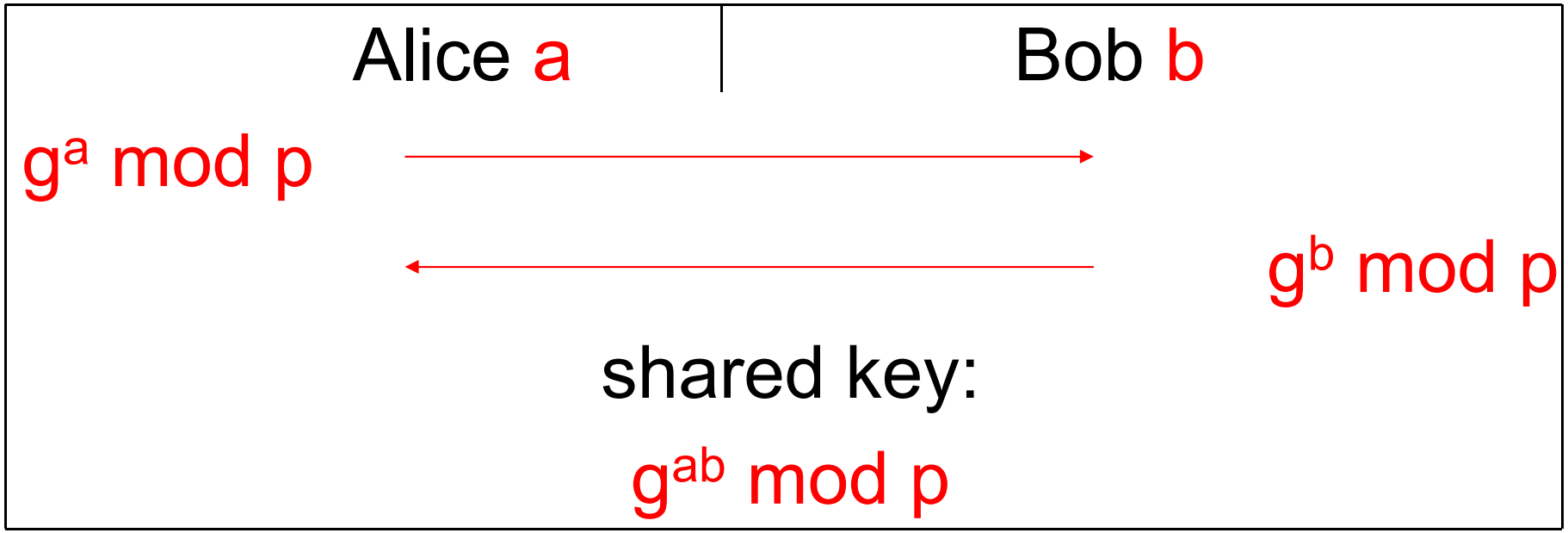


Stealth Address Method[s]

(several variants)

basic variant first

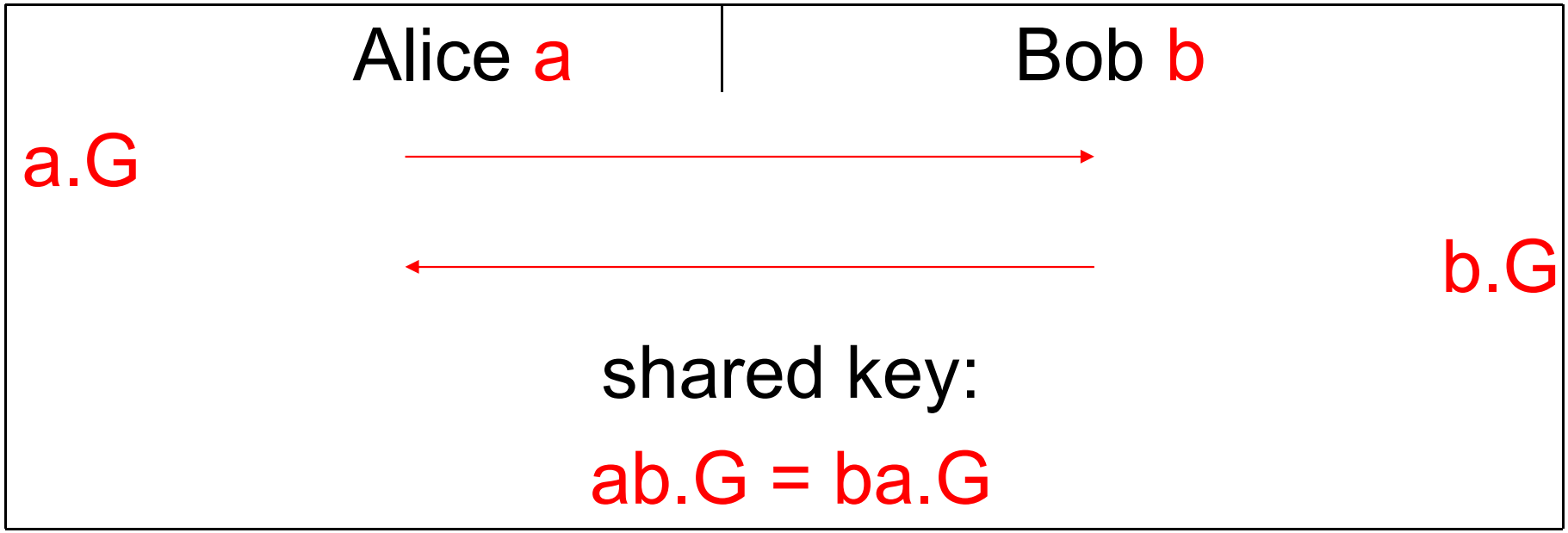
*Diffie-Hellman mod P



Alice computation: $(g^b)^a = g^{ab}$ mod p.

Bob's computation: $(g^a)^b$ mod p.

EC Diffie-Hellman



Alice computation: a.(b.G).

Bob's computation: b.(a.G).

**Most Basic Stealth Address – Short Summary

Payer/Sender a	Receiver b
a.G →	
	b.G →
shared key:	
S=a(b.G) = b(a.G)	

Sender: S=a.(b.G). Send bitcoins to E = H'(H(S).G).

Receiver: H(S)=H(b.(a.G)). Private key e=H(S)!!!

Stealth Address = "Invisible" Recipient

- Based on ideas by user=ByteCoin [Bitccoin forum

A Method to protect the recipient
[nobody knows I sent money to this recipient]

*Who is using Stealth Address?

- Dark Wallet, open source BTC wallet,
  - implements 102-chars long S.A. + coin mixing.

+"permission-less!"
-censorship pbs.


Cody Wilson


Amir Taaki

- Monero
  - Market cap $20M=>$320M recently

- SDC = Shadow cash,
  - Market cap $12M
- Vertcoin
  - Market Cap: $2M

SHADOW

ertcoir

Stealth Address = "Invisible" Recipient

- Using Diffie-Hellman. Sender=a Receiver=b private keys.
- Sender Sender/A knows the recipient's public key b.G mod P
  and Rec/B knows Send/A's public key a.G mod P.
- Sender/A computes S=ab.G.
- A computes H(S) and generates a deterministic new bitcoin private key **SK_transfer=**H(S). Transfer address E =H'(H(S).G).
- A sends bitcoins to this address (Send/A could take money back!)

Stealth Address = “Invisible” Recipient

- Using Diffie-Hellman. Sender=a Receiver=b private keys.
- Sender Sender/A knows the recipient’s public key b.G mod P
  and Rec/B knows Send/A’s public key a.G mod P.
- Sender/A computes S=ab.G.
- A computes H(S) and generates a deterministic new bitcoin private key **SK_transfer=**H(S). Transfer address E = H’(H(S).G).
- A sends bitcoins to this address (Send/A could take money back!)
- Due to DH magic, Rec/B also knows this private key H(b.(a.G)).
- B takes the money and transfers them to a new addresses,

Stealth Address = “Invisible” Recipient

- Using Diffie-Hellman. Sender=a Receiver=b private keys.
- Sender Sender/A knows the recipient’s public key b.G mod P
  and Rec/B knows Send/A’s public key a.G mod P.
- Sender/A computes S=ab.G.
- A computes H(S) and generates a deterministic new bitcoin private key **SK_transfer=**H(S). Transfer address E = H’(H(S).G).
- A sends bitcoins to this address (Send/A could take money back!)
- Due to DH magic, Rec/B also knows this private key H(b.(a.G)).
- B takes the money and transfers them to a new addresses, quickly!!!!

Security

- Risk:
  - The sender can spend! [Todd Jan 2014]
  - Both know private key **SK_transfer=**H(S).

  - Like 24h time to think about and change his mind.
  - The receiver MUST be active, ONLINE.

    ⇒move money ASAP to another account before Sender takes it back.

    ⇒active/real time=>easier to trace, poor anonymity,

      - good for catching criminals who ask for ransoms.

Security (contd)

- Increased disclosure:
  - Here Recipient/B knows public key b.G in advance (public directory? or e.g. disclosed to any user who visits a recipient web site).
  - In bitcoin it is not disclosed
    [NSA: pls crack ECDSA/ECDL in 1 second vs. 1 year].

- Nobody knows who is the recipient of a given transaction or we cannot relate it with Recipient/B public key b.G even though it is in a public directory. (must keep extra data not in the blockchain).

- Deterministic: same 2 principals A+B=>same Transfer address E.

- Recipient/B is anonymous only if he can hide his network presence (e.g. using TOR) when spending his attributions [issuing digital signatures].
  - He needs to be careful about how he is spending the money: next address not stealth, not protected!

Improved

Asymmetric

Stealth Address

Method

Improved Stealth Address = Stronger Spending Key

Sender/A and Recipient/B share this common secret:

A shared bitcoin private key for A/B

$$H(S) = H(ab.G)$$

One can derive a **stronger**/more interesting private key like:

$$e = H(S)+b$$ **One Time Spending key**

Asymmetry here: Recipient/B will be the ONLY person to know b.

Yet Sender/A CAN compute the corresponding public key [and he knows the recipient, other people don't].

$$E = H(S).G+b.G$$ **One Time Destination key**

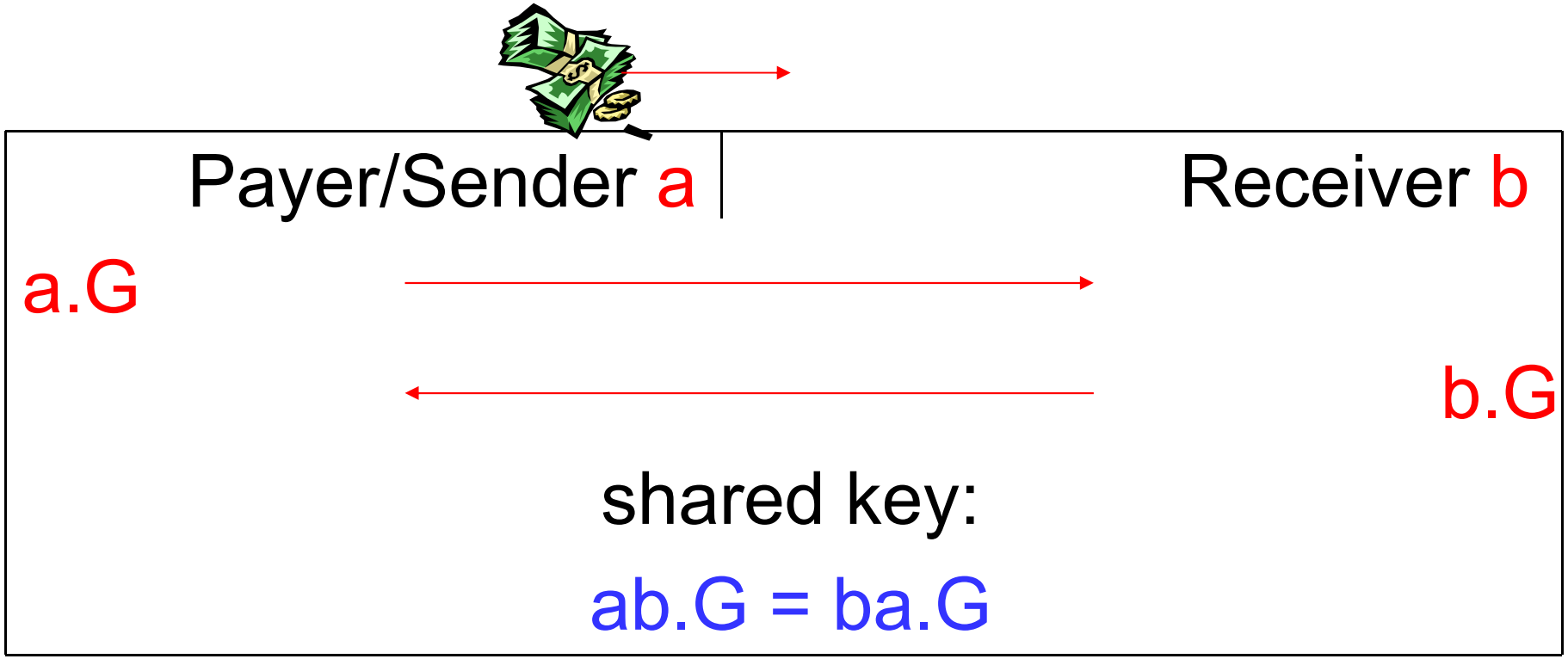
Later he just sends money to H'(E).

Sender cannot spend anymore!

*inevitably E will be revealed when this money is spent further.

***Only A and B can know if this E is valid [variant of DDH problem].

*Improved Stealth – DH View



Sender: S=a.(b.G). Send bitcoins to E=H(S).G+b.G.

Receiver: H(S)=H(b.(a.G)). Private key e=H(S)+b!!!

****variant with random nonce-keypair

Payer/Sender r | Receiver b

r.G →

← b.G

shared key:

rb.G = br.G

Sender: S=r.(b.G). Send bitcoins to E=H(S).G+b.G.

Receiver: H(S)=H(b.(r.G)). Private key e=H(S)+b!!!

Stealth Address - Drawbacks

- Must monitor ALL* transactions in blockchain!!!!
  Download last few months: 1 day on a PC.

***actually those with OP_RETURN ==6a…**

Yet Stronger:

2xKey
Stealth Address
Method

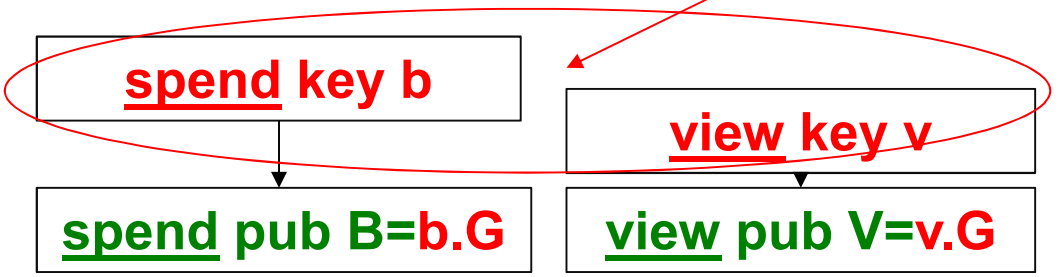
2-Key Stealth Address

* b,a in CryptoNote 2.0 paper by Nic van Sab.

- Current private key b
  will become 2 values:

user **Private User Key** = b,v

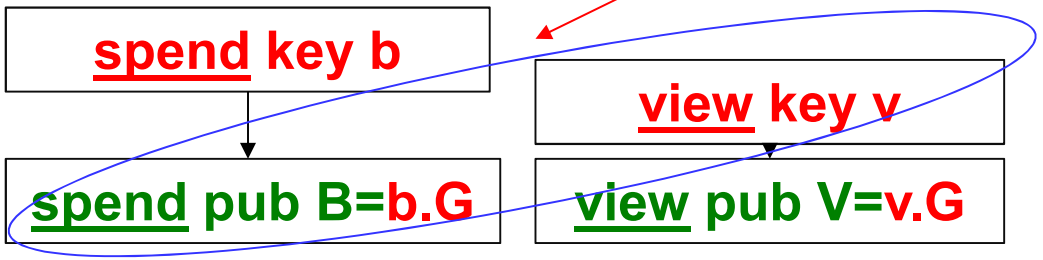
- 2 keys playing a different role,
  b is “more” secret.



2-Key Stealth Address

* b,a in CryptoNote 2.0 paper by Nic van Sab.

Private User Key = b,v



a.k.a. 'Scan pubkey'

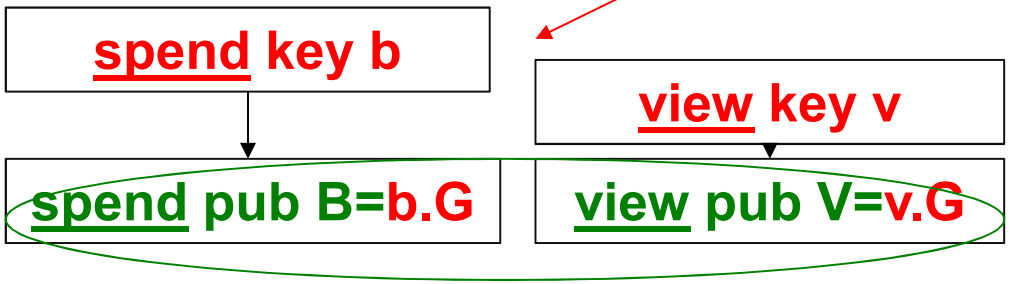
- One of them = v = View is given to a proxy entity to implement painful blockchain checks for us and notify us that payment has arrived.

  Tracking Key= v, b.G (removes anonymity).

2-Key Stealth Address

* b,a in CryptoNote 2.0 paper by Nic van Sab.

Private User Key = b,v



Tracking Key= v, b.G (removes anonymity).

- Receiver has **Public User key**= b.G, v.G.

Advertised/provided/listed by the receiver,
NOT visible in the blockchain transactions!

2-Key Stealth Address – Version A

- Recipient/B has **Private User Key** = b,v
- Proxy has **Tracking Key**= v, b.G (removes anonymity).
- Receiver **Public User key**= b.G, v.G.

- Let S=v.(a.G) = a.(v.G). Sender private a.
- Proxy and Receiver can compute v.(a.G) for every tx done by any A.
- Sender/A can do a.(v.G).
- A sends bitcoins to E=b.G+H(S).G.
- Proxy does not know e.
- Proxy can compute E and see transactions (**view key for this tx**).
- Only the recipient has b (**spend key for this tx**).
  - Private key e=b+H(S) allows to spend the bitcoins sent to E.

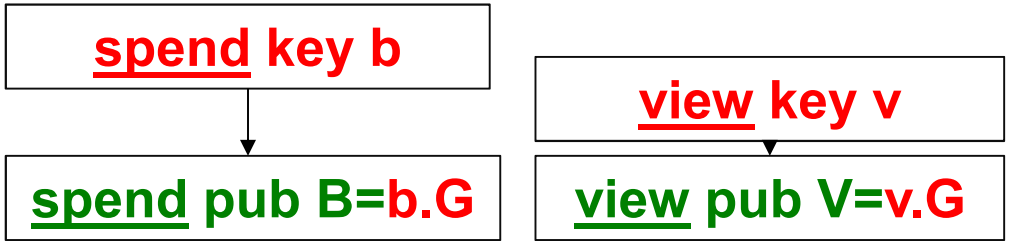
Better Stealth Address used in Monero

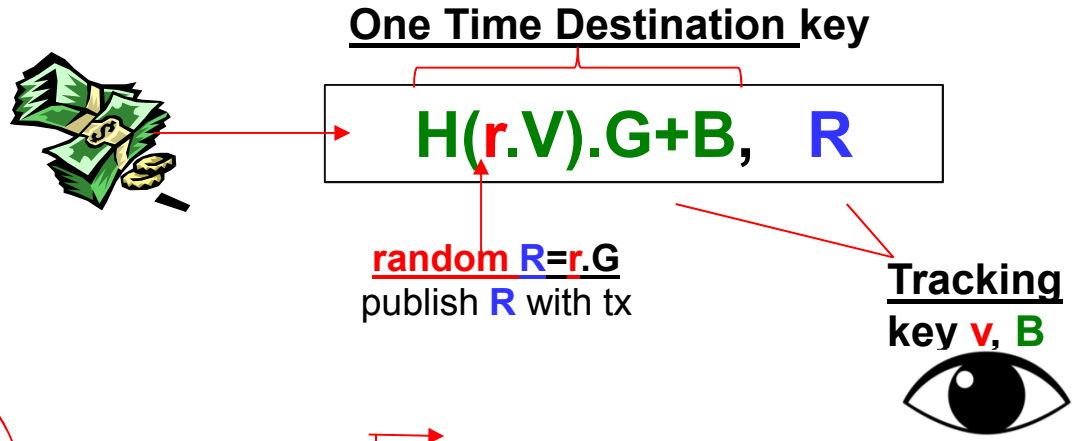
- Recipient/B has **Private User Key** = b,v
- Proxy has **Tracking Key**= v, b.G (removes anonymity).
- Receiver **Public User key**= b.G, v.G.

*fixed a was replaced by random r

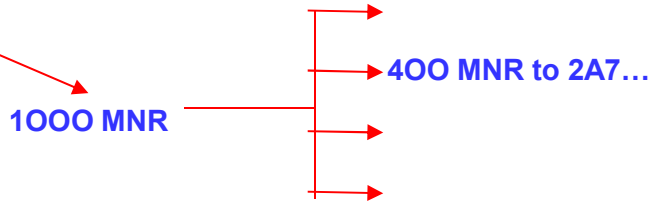
- Let S=v.(r.G) = r.(v.G). Sender random r, publishes R=r.G with this tx.
- Proxy and Receiver can compute v.(r.G) for every tx done by any A.
- Sender/A can do r.(v.G).
- A sends bitcoins to E=b.G+H(S).G.
- Proxy does not know e.
- Proxy can compute E and see transactions (**view key for this tx**).
- Only the recipient has b (**spend key for this tx**).
  - Private key e=b+H(S) allows to spend the bitcoins sent to E.

Sending Monero





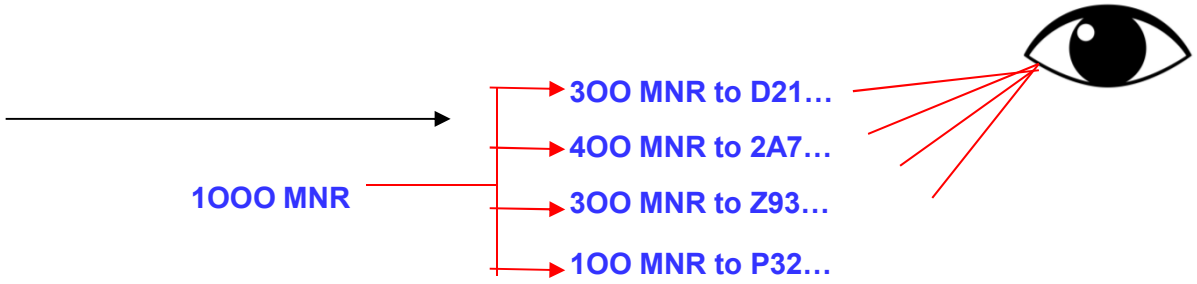
Money from several attributions to PKs: the sender must know the ECDL for ALL these inputs



MONERO

Privacy – Good?

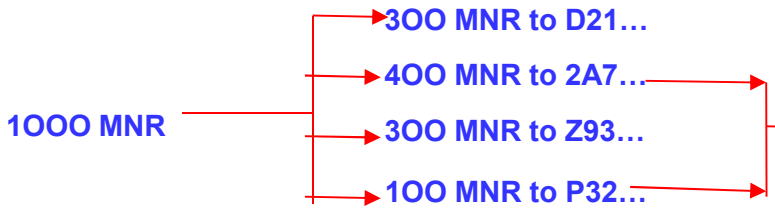
At this moment:
NO WAY to know which outputs are “change” and which are Recipient addresses



MONERO

Pb3.

Spending reveals information and compromises privacy



=>these 2 outputs ARE LINKED now!!

MONERO

Not Perfect

Paper by Monero labs:
Adam Mackenzie, Surae Noether and Monero Core Team:
“Improving Obfuscation in the CryptoNote Protocol”, Jan’15
https://lab.getmonero.org/pubs/MRL-0004.pdf

Citations:
“CryptoNote is very traceable”
[…]
“users **can receive** CryptoNote-based cryptocurrencies
with no concern for their privacy,
they **cannot necessarily spend** those currencies without
releasing some information about their past transactions”

Bitcoin and Z.Cash ALSO have this problem