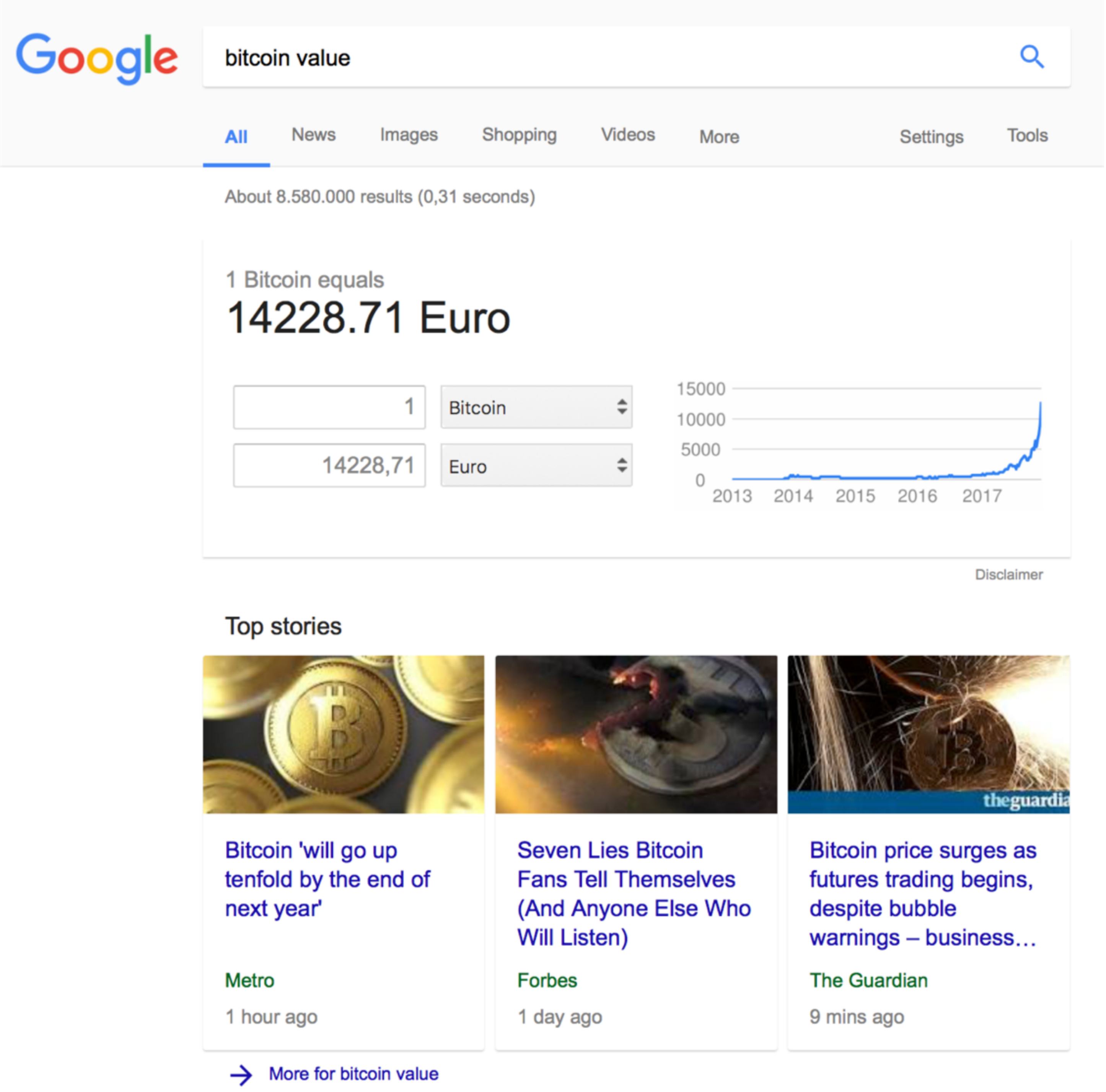
Blockchain for identity management, seriously?

Greg Alpar
January 30, 2018

Open Universiteit
www.ou.nl



About 8.580.000 results (0,31 seconds)

1 Bitcoin equals

14228.71 Euro

1	Bitcoin
14228,71	Euro

Top stories

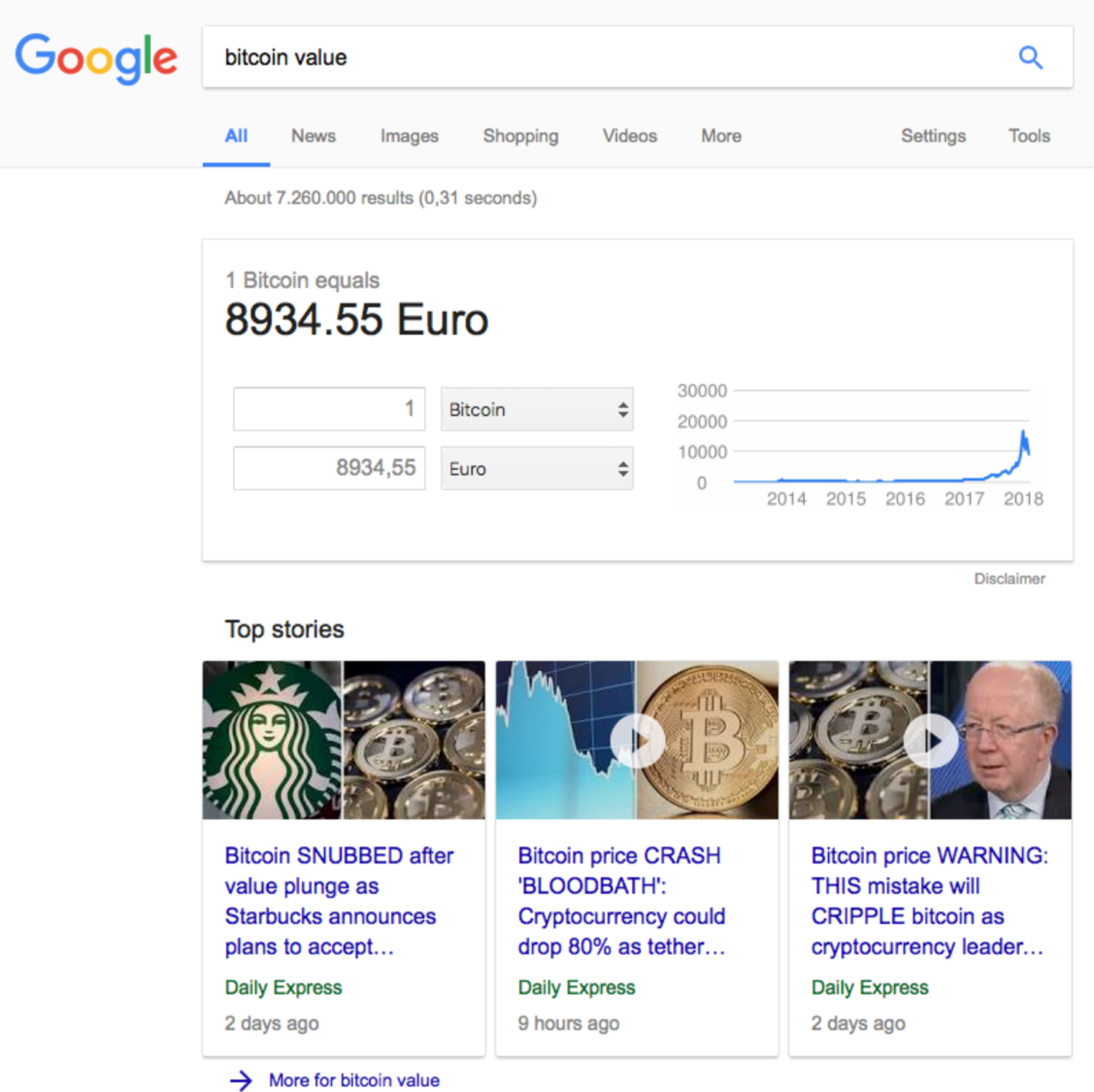
Bitcoin 'will go up tenfold by the end of next year'
Metro
1 hour ago

Seven Lies Bitcoin Fans Tell Themselves (And Anyone Else Who Will Listen)
Forbes
1 day ago

Bitcoin price surges as futures trading begins, despite bubble warnings – business…
The Guardian
9 mins ago

More for bitcoin value

201712111550



bitcoin value

About 7.260.000 results (0,31 seconds)

1 Bitcoin equals

8934.55 Euro

1	Bitcoin
8934,55	Euro

Top stories

Bitcoin SNUBBED after value plunge as Starbucks announces plans to accept…

Daily Express

2 days ago

Bitcoin price CRASH 'BLOODBATH': Cryptocurrency could drop 80% as tether…

Daily Express

9 hours ago

Bitcoin price WARNING: THIS mistake will CRIPPLE bitcoin as cryptocurrency leader…

Daily Express

2 days ago

More for bitcoin value

201801291642

Agenda

- Bitcoin
- Blockchain
- Identity management

Glossary

- Transaction (tx) – B, sender, receiver
- Block – a collection of transactions and *hash*
- Consensus – what tx?, how much money each user has
- Mining – to reach consensus solve a computational puzzle

```
0000000e7dd5f94780383e9dfa1f4def044319104ad16ab15e45eeb2a8dfc81b
db3bc996de44bcc8cfc4b9b2773a298356d1aac05b9a8ef90be67d64a737532c
```

- Incentive: 1. mining, 2. transaction fee
- Confirmation: last few blocks become permanent (6 blocks)

ANDERS' DEMO: BLOCKCHAIN

Benefits

- Distributed consensus
- Decentralised (?)
- Immutability (?)
- Redundancy

Challenges

- Volatility
- High transaction costs
- Scalability
- Power consumption
- **Privacy**

Agenda

- Bitcoin
- **Blockchain**
- Identity management

What’s the buzz?

- Secure hash (SHA-256)
  - Fixed-length output
  - Collision resistance
  - One-wayness
- Smart contracts
  - Ethereum
  - Running code (~tx) in each node (EVM)

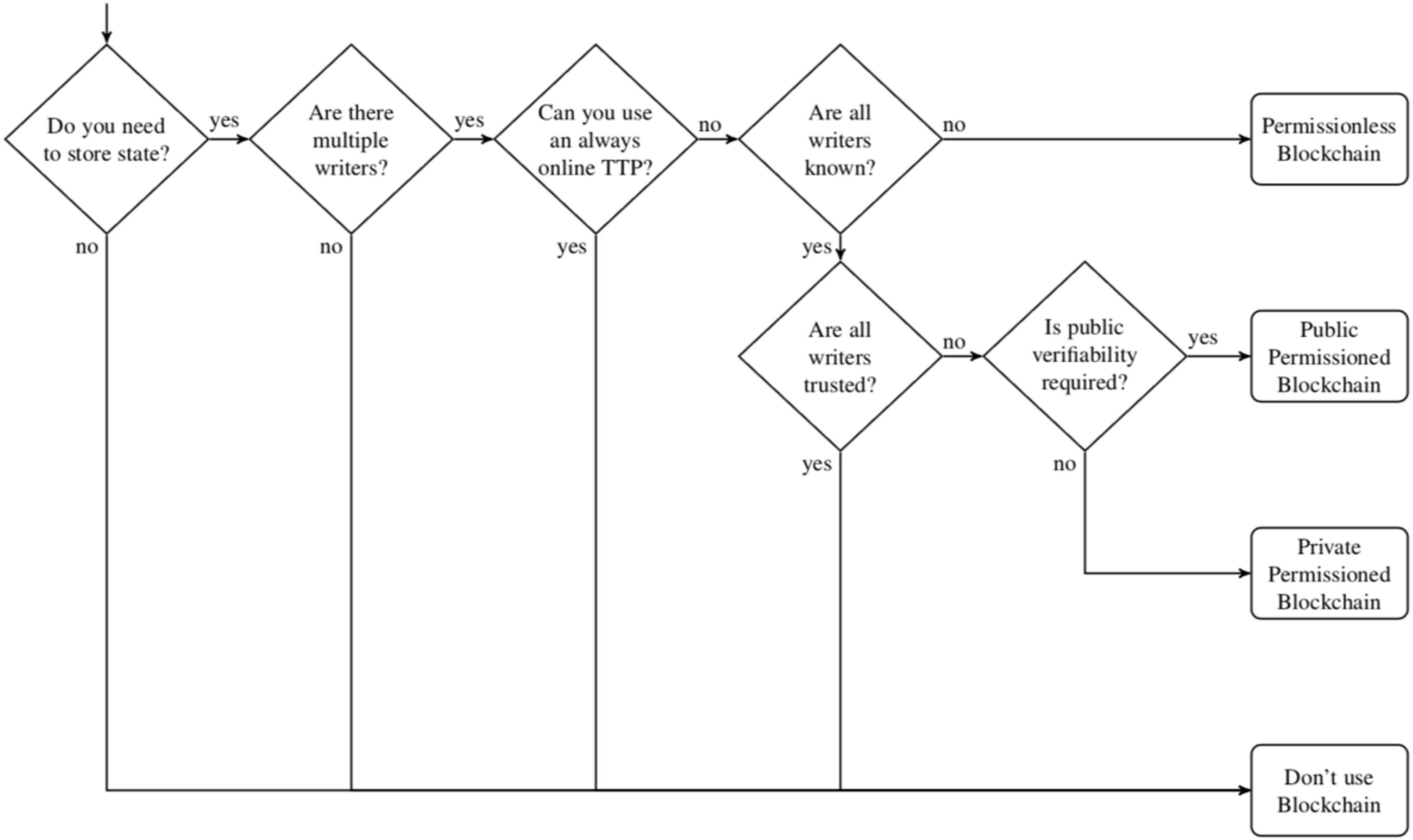
Kinds

- Writing (appending)
  - Permissioned
  - Permissionless
- Reading
  - Private
  - Public

Relation to other security mechanisms

- Ledger (append-only bulletin board)
- Signature
- Commitment
- Time stamp

Do you need a Blockchain?


Do you need to store state?
yes
no
Are there multiple writers?
yes
no
Can you use an always online TTP?
no
yes
Are all writers known?
no
yes
Permissionless Blockchain
Are all writers trusted?
no
yes
Is public verifiability required?
yes
no
Public Permissioned Blockchain
Private Permissioned Blockchain
Don't use Blockchain

Wüst, K.,&Gervais, A. (2017). Do you need a Blockchain?. *IACR Cryptology ePrint Archive*, *2017*, 375.

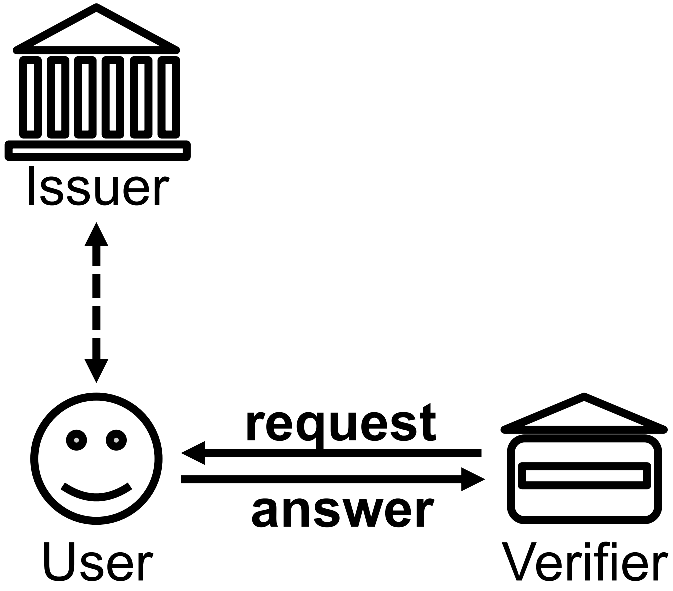
Agenda

- Bitcoin
- Blockchain
- **Identity management**

Open Universiteit
www.ou.nl

- Why?
  - Other IT tools
  - Other security tools
- Don’t
  - Not practical, efficient, etc.
  - Privacy invasive

Decentralised identity management



Issuer

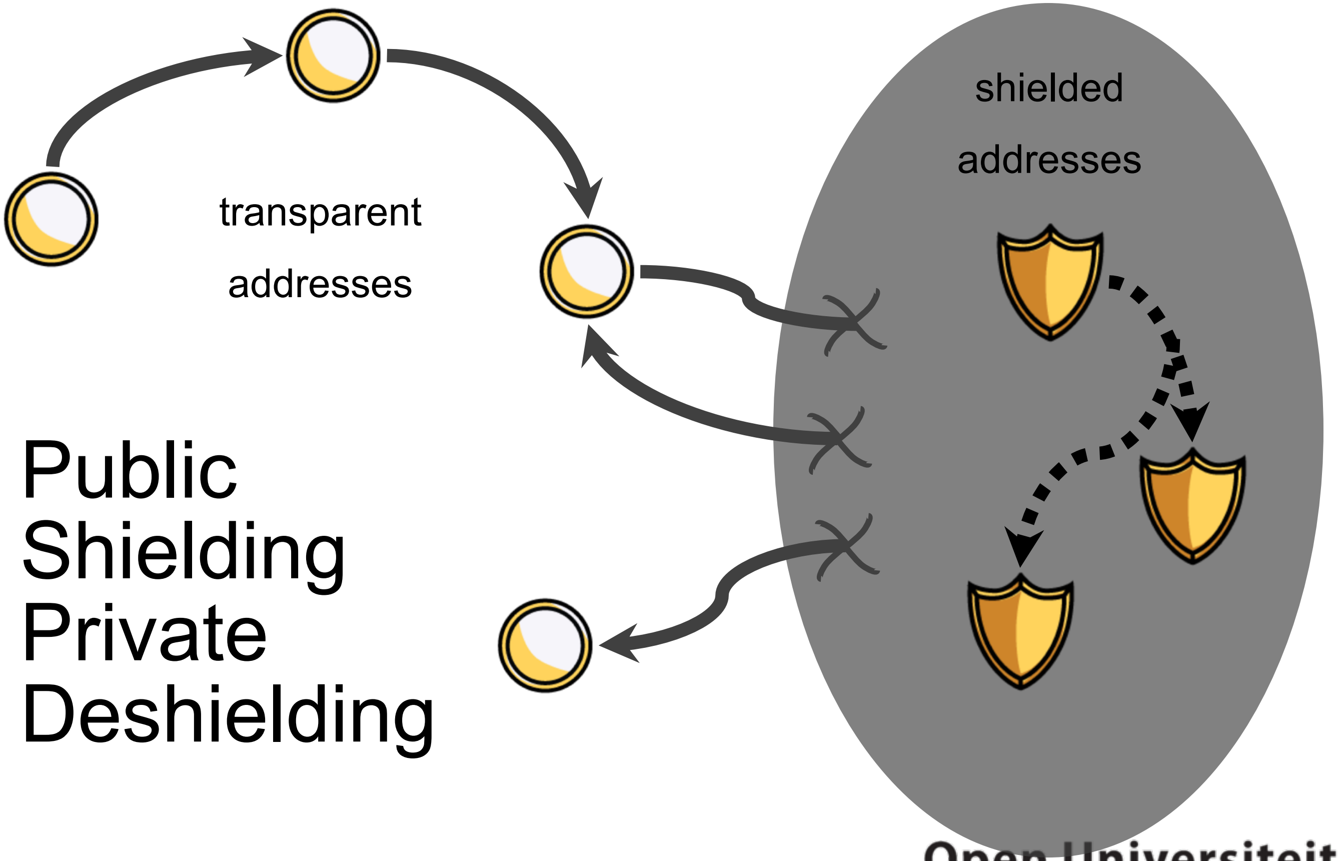
User

request

answer

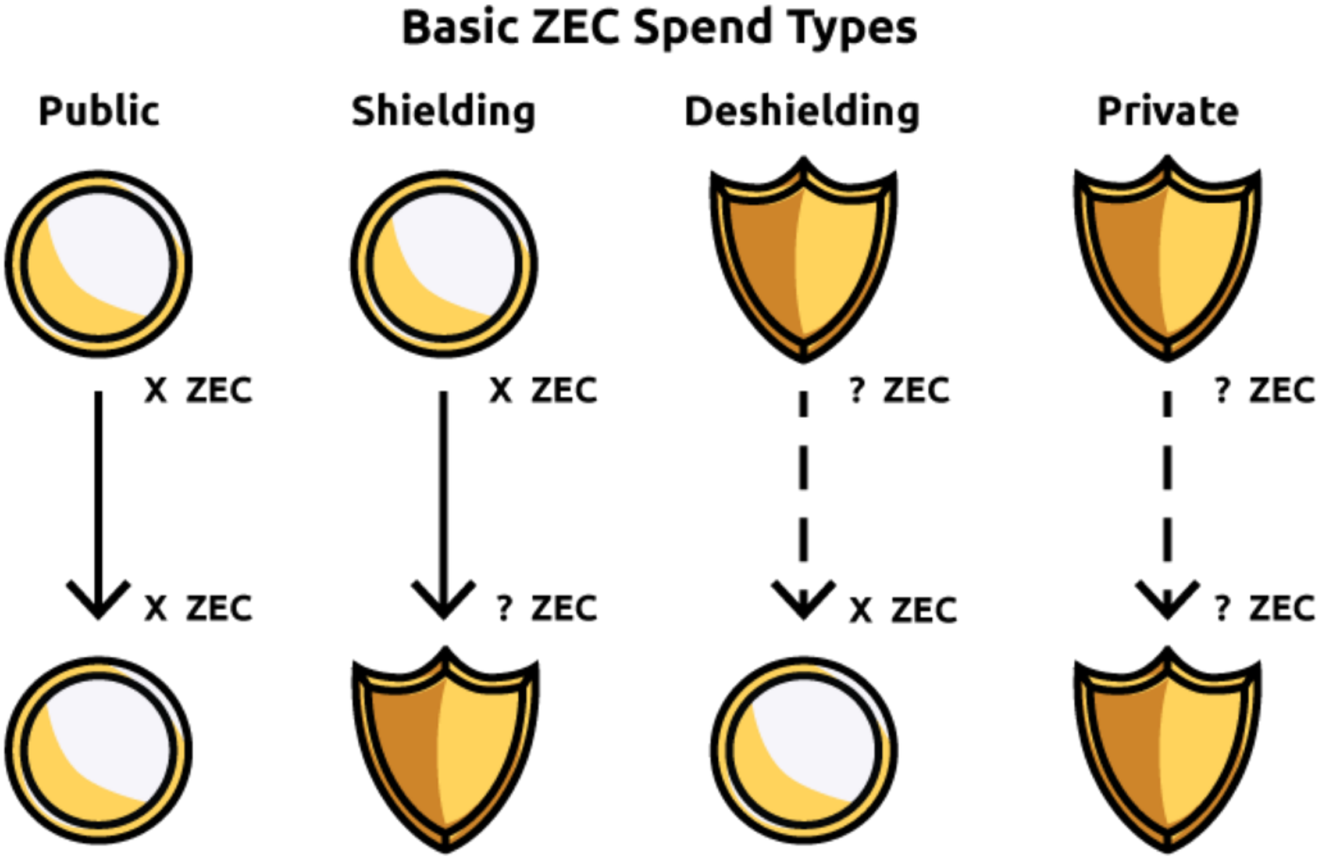
Verifier

Zerocoin (ZEC) transactions



Public
Shielding
Private
Deshielding

Zerocoin (ZEC) transactions



Open Universiteit
www.ou.nl

Promising: **Decentralised anonymous credentials**

- Credentials in the (Bitcoin) blockchain
- No need for credential signature (~CA’s signature in PKI)
  - Authenticity is by validation and consensus
- ZK proof that one of the credentials is yours
  - Not which
- ZK proof about the content
  - Selective disclosure

Open Universiteit
www.ou.nl

Garman, C., Green, M.,&Miers, I. (2014, February). Decentralized Anonymous Credentials. In *NDSS*.

Greg Alpar http://www.open.ou.nl/gaa/ Jan. 30, 2018

Blockchain for identity management, seriously?

THANK YOU!

Open Universiteit
www.ou.nl