Blockchains, the web and standardization: the big opportunity

~~Keynote~~ conversation starter

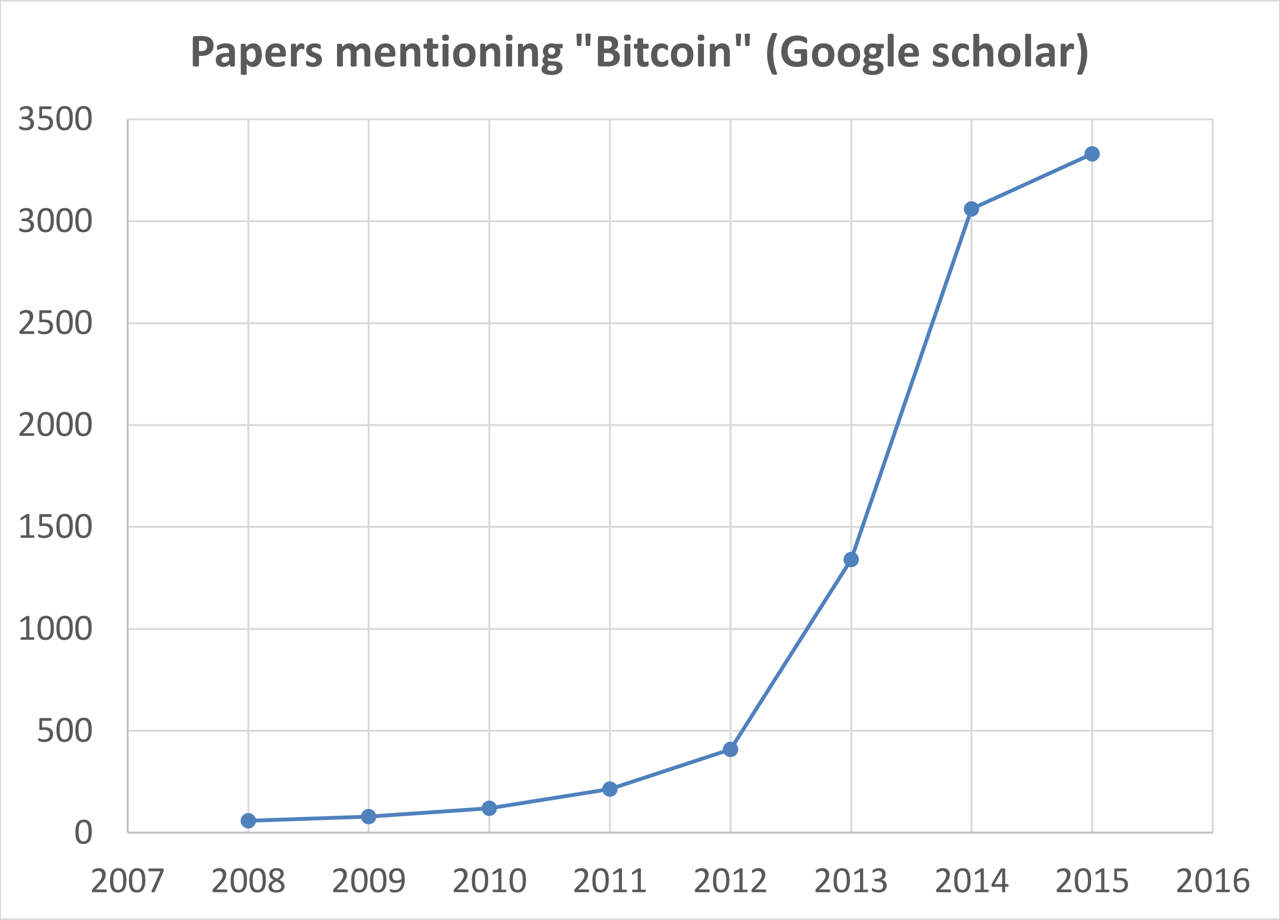
Arvind Narayanan
Princeton University

@random_walker

Standardization: is it too soon?

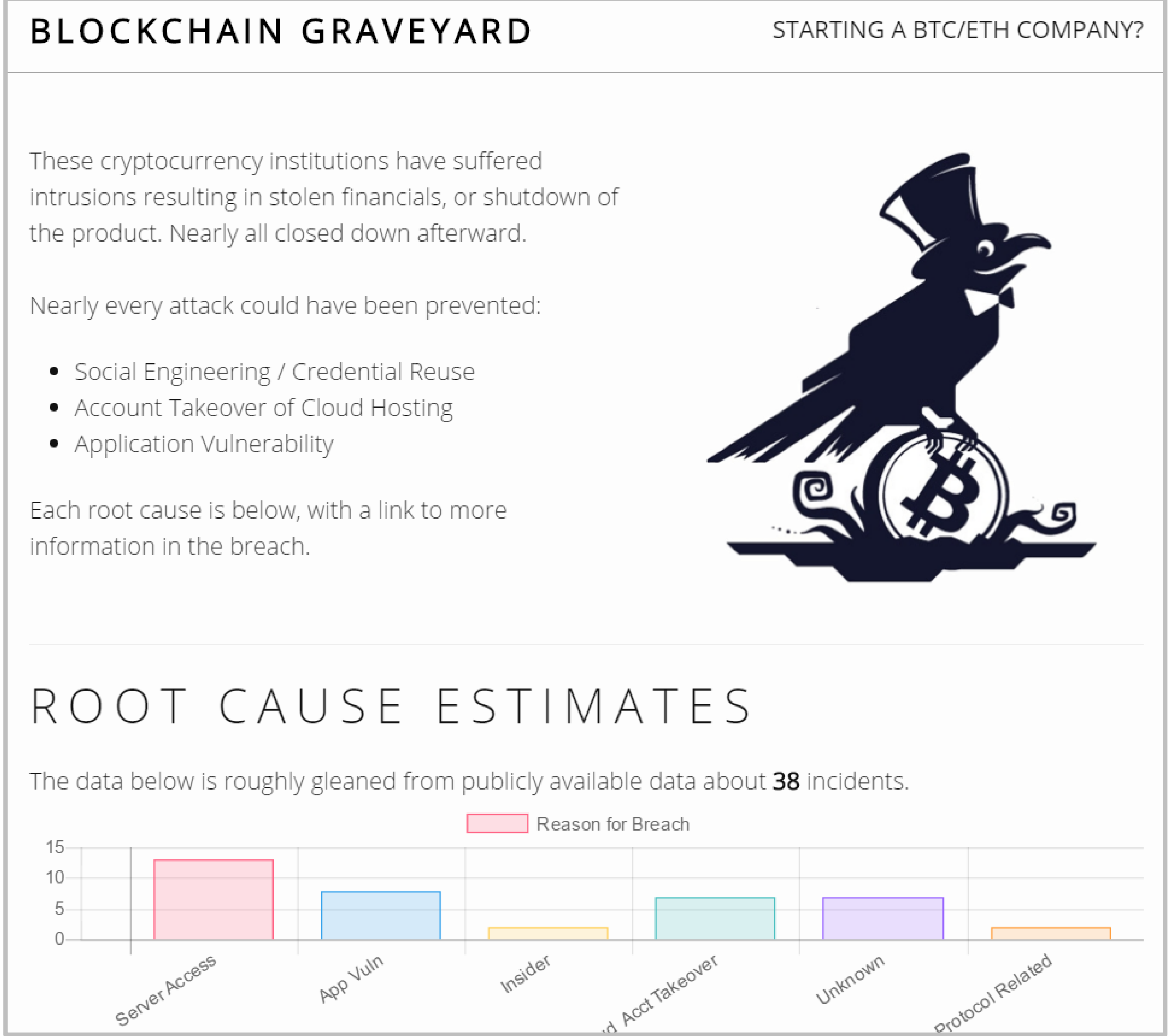
Are Bitcoin and other blockchains sound?

Academic research on Bitcoin



- No fundamental problems (so far)
- Various known concerns
  - e.g. selfish mining
- Works better in practice than in theory

Caveat: endpoint security



BLOCKCHAIN GRAVEYARD

STARTING A BTC/ETH COMPANY?

These cryptocurrency institutions have suffered intrusions resulting in stolen financials, or shutdown of the product. Nearly all closed down afterward.

Nearly every attack could have been prevented:

- Social Engineering / Credential Reuse
- Account Takeover of Cloud Hosting
- Application Vulnerability

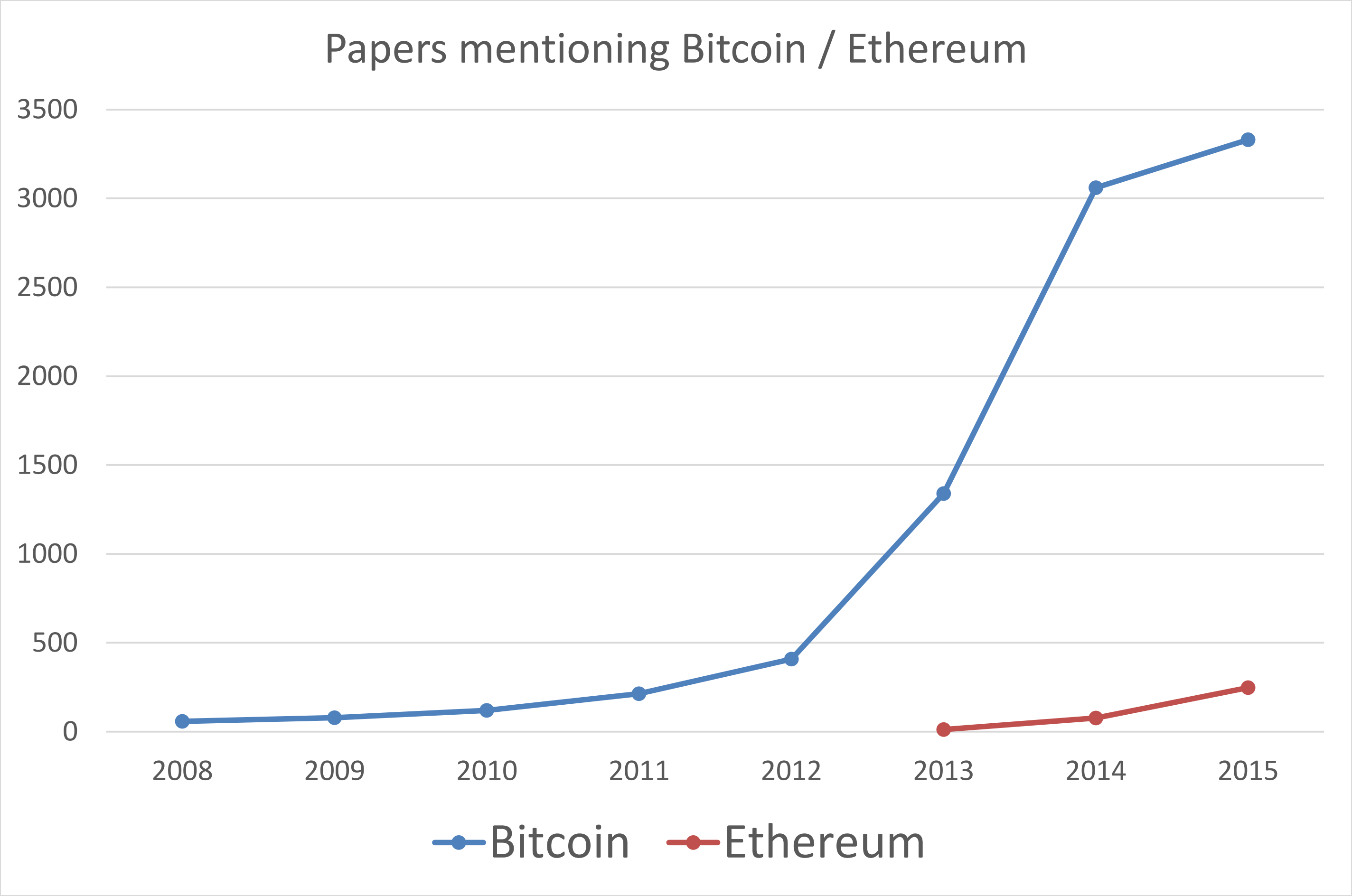
Each root cause is below, with a link to more information in the breach.

ROOT CAUSE ESTIMATES

The data below is roughly gleaned from publicly available data about **38** incidents.

Human-crypto interaction is an unsolved problem!

Bitcoin vs. Ethereum

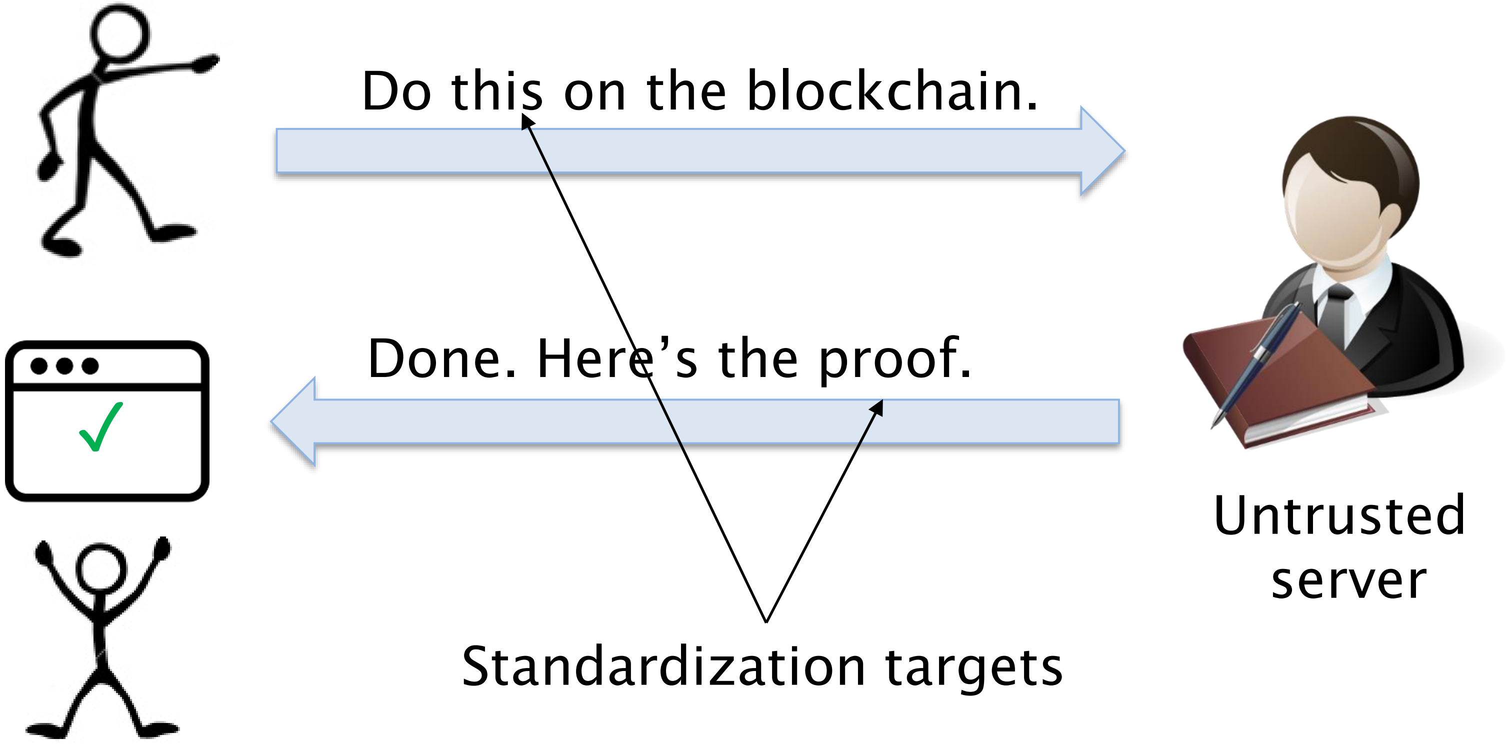


Fundamental concerns:

- Incentive misalignment
- Security of contracts

Can standardization enable new applications?

Standards enable new applications



Do this on the blockchain.

Done. Here’s the proof.

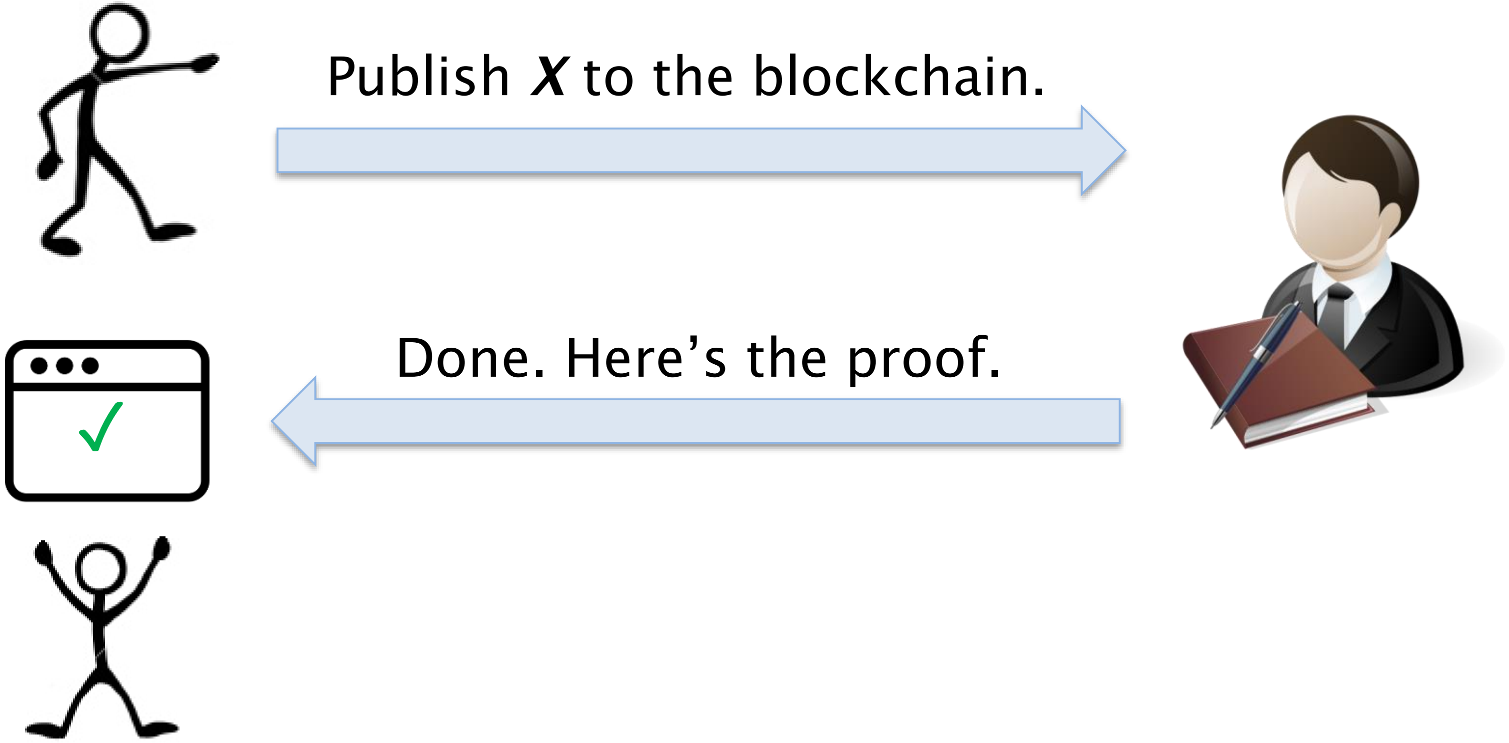
Standardization targets

Untrusted server

- Document timestamping
- Contracts
- Provenance
  - IP
  - Assets
- IoT
- Identity

The power of the blockchain + the reach of the web

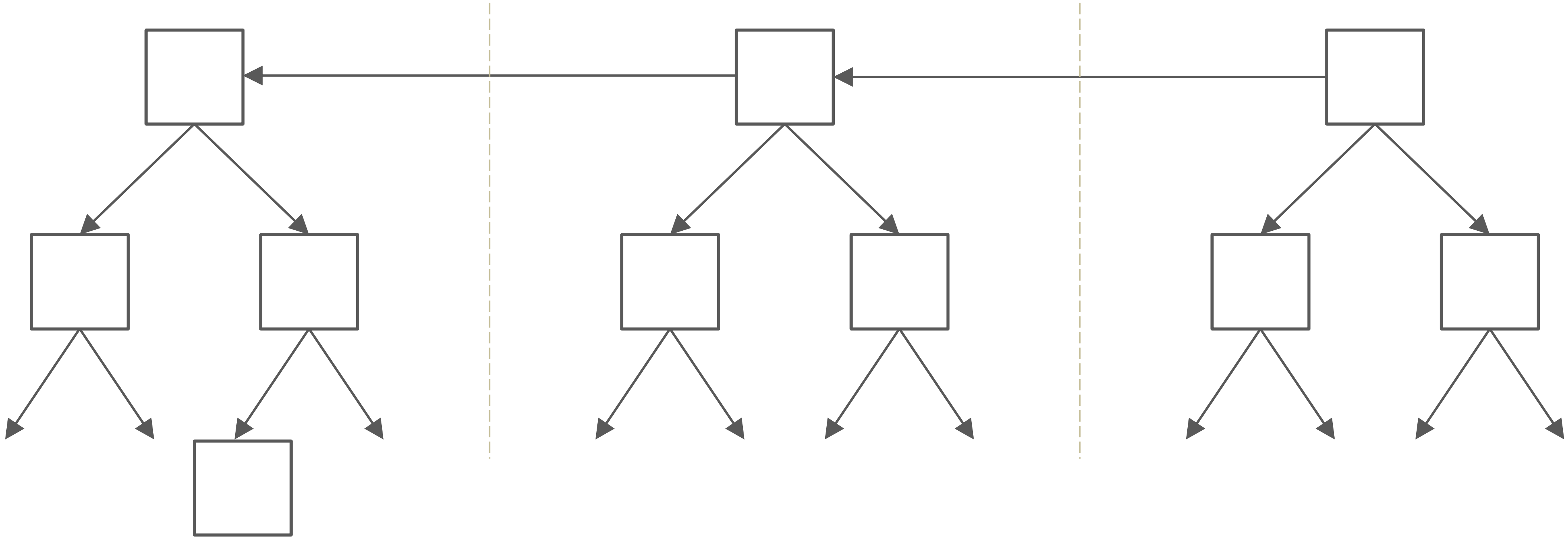
Aside: how efficient proofs work

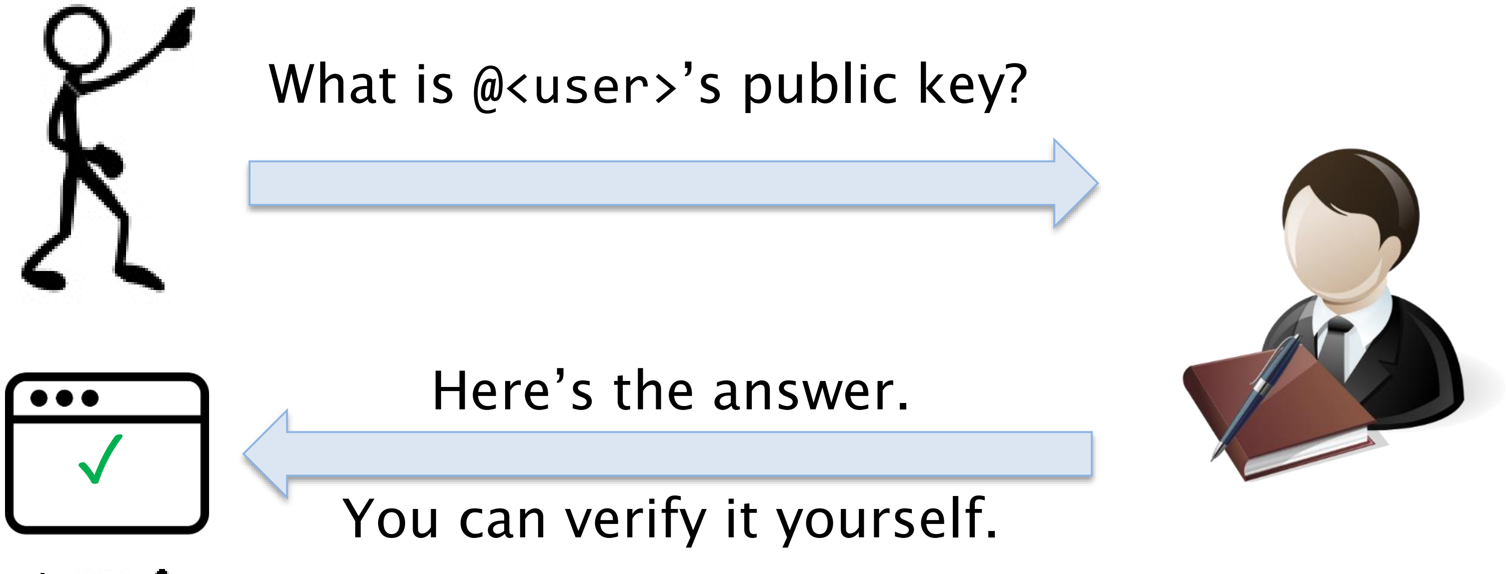


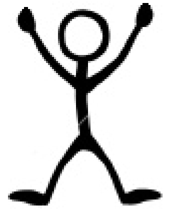
Publish ***X*** to the blockchain.

Done. Here’s the proof.

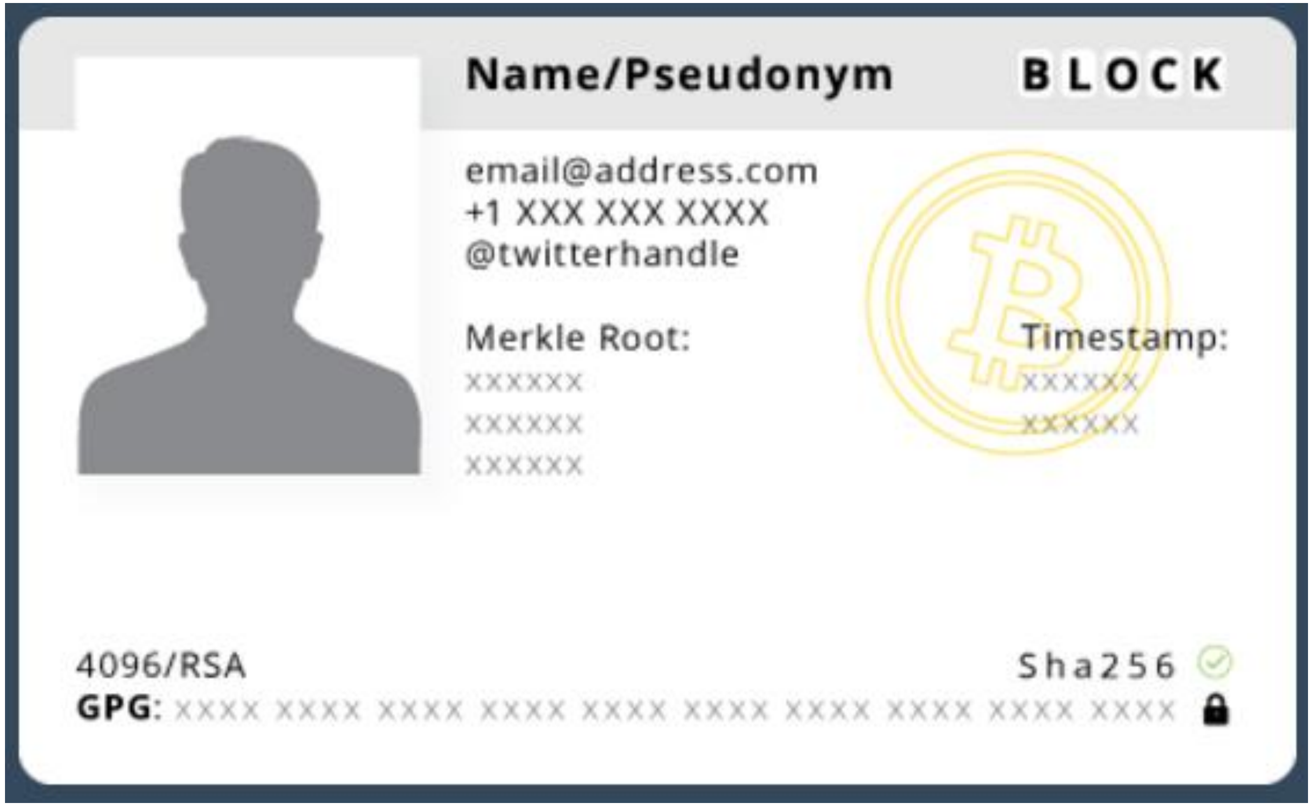
Aside: how efficient proofs work







Standards as a way to avoid human-crypto interaction.



Name/Pseudonym **BLOCK**

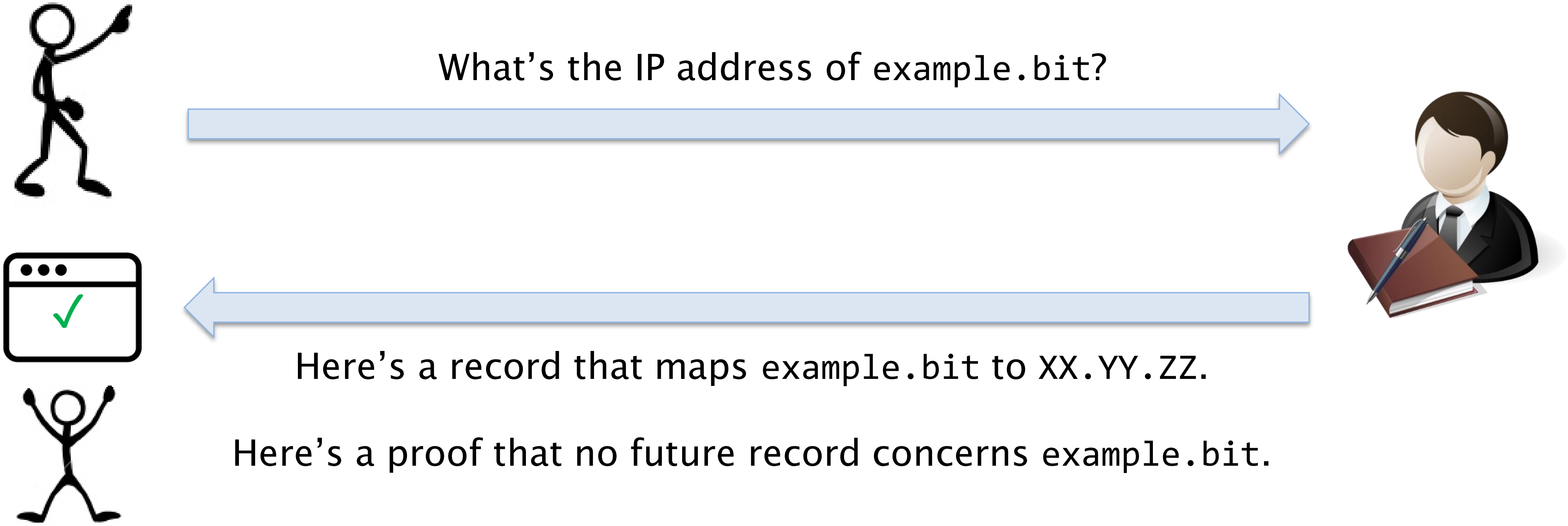
email@address.com
+1 XXX XXX XXXX
@twitterhandle

Merkle Root:
XXXXXX
XXXXXX
XXXXXX

Timestamp:
XXXXXX
XXXXXX

4096/RSA Sha256 ✓
GPG: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX 🔒

A more complicated proof: domain names



What’s the IP address of `example.bit`?

Here’s a record that maps `example.bit` to `XX.YY.ZZ`.

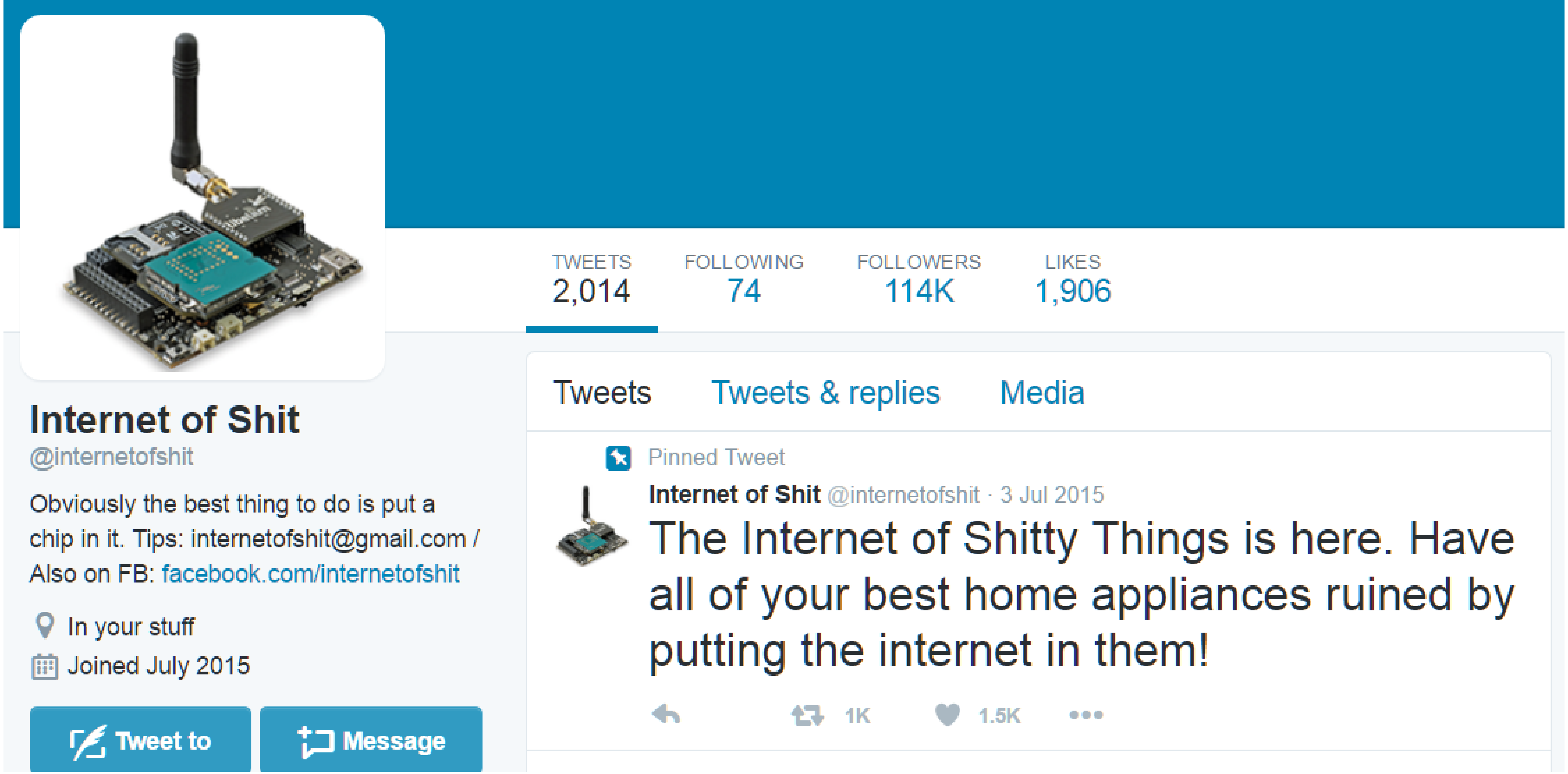
Here’s a proof that no future record concerns `example.bit`.

Standardize a small set of proofs? Standardize a language for proofs?

Verifiers could even be offline

Who are you?

Here’s a proof that I’m authorized
to drive you for 24 hours starting …



Internet of Shit
@internetofshit

Obviously the best thing to do is put a chip in it. Tips: internetofshit@gmail.com / Also on FB: facebook.com/internetofshit

In your stuff

Joined July 2015

TWEETS 2,014 FOLLOWING 74 FOLLOWERS 114K LIKES 1,906

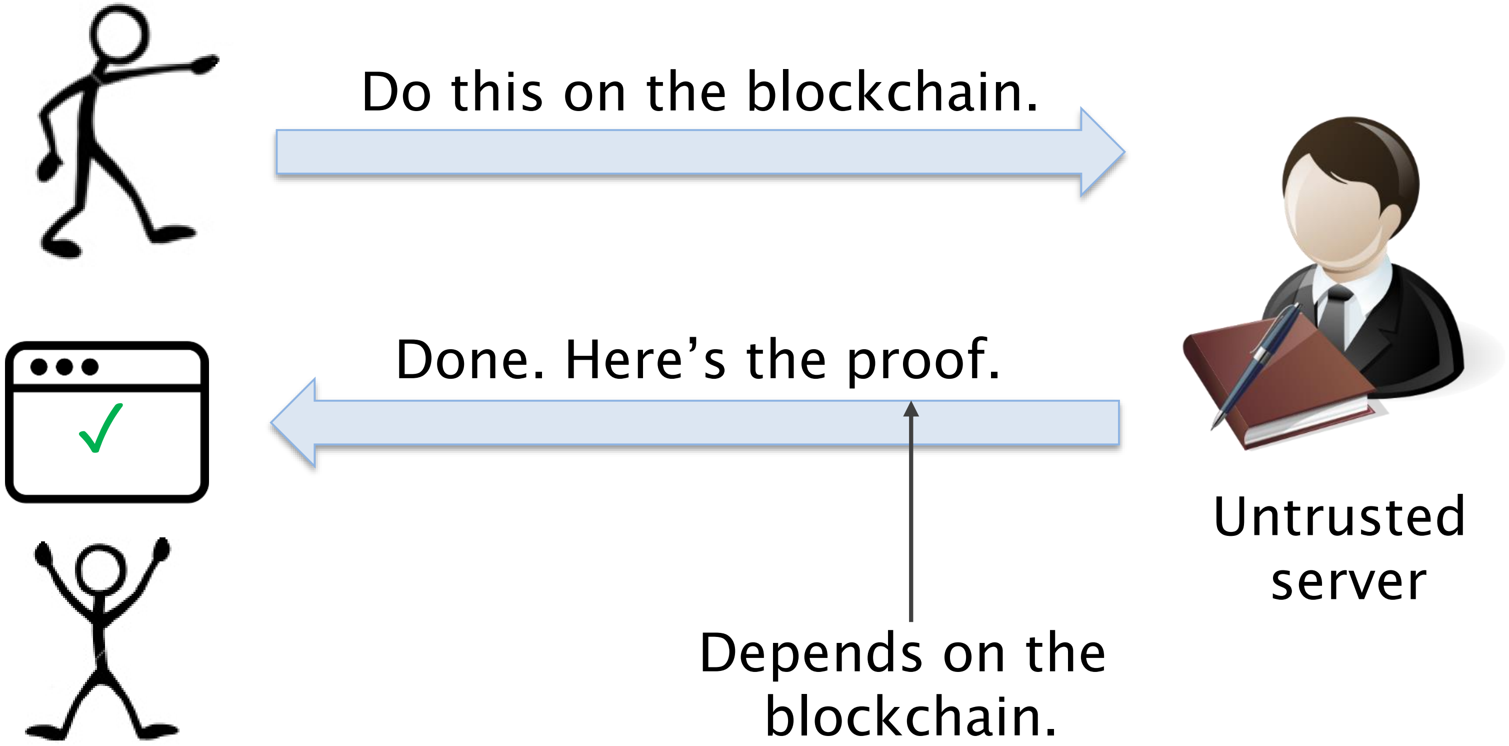
Pinned Tweet

Internet of Shit @internetofshit · 3 Jul 2015

The Internet of Shitty Things is here. Have all of your best home appliances ruined by putting the internet in them!

Standards as a means to keep clients thin and dumb.

Which blockchain? It matters.



Do this on the blockchain.

Done. Here’s the proof.

Untrusted server

Depends on the blockchain.

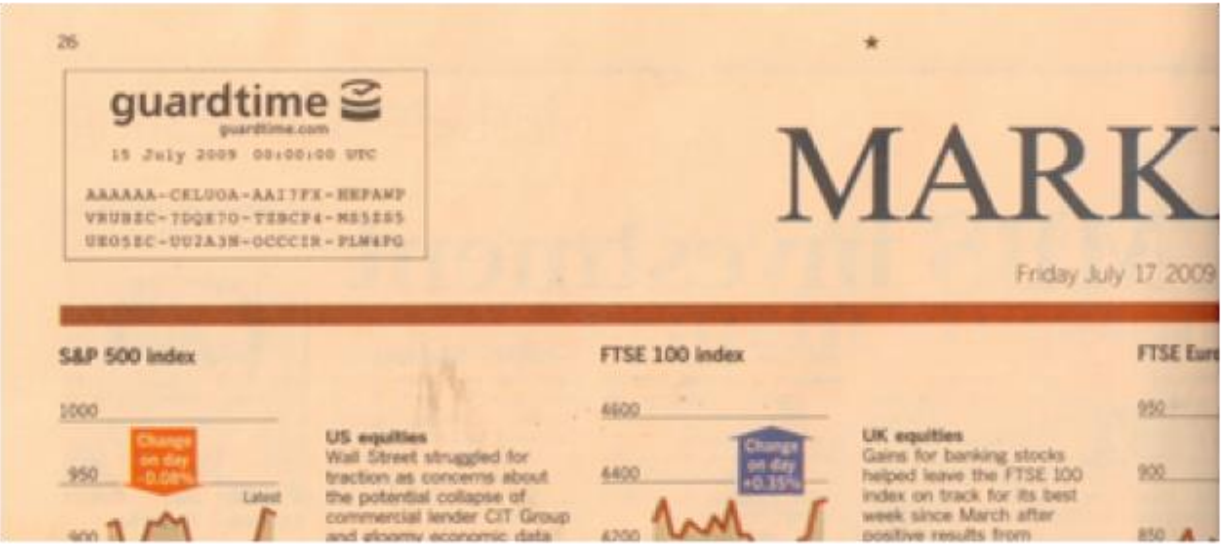
Example: public vs. private blockchains

Private blockchains (permissioned ledgers)

- Append-only log using hash pointers / Merkle trees
- Cryptographic identity

– Proof of work
– Nakamoto consensus
– Currency

+ Byzantine consensus



26 ★

guardtime
guardtime.com
15 July 2009 00:00:00 UTC

AAAAAA-CELUOA-AAI7FX-HEPAWP
VRUBZC-7DQE7O-TZBCP4-MS5ZS5
UEO5EC-UU2A3N-OCCCIR-PLM4PG

MARK

Friday July 17 2009

S&P 500 index

1000
950
900
Change on day -0.08%
Latest

US equities
Wall Street struggled for traction as concerns about the potential collapse of commercial lender CIT Group and gloomy economic data

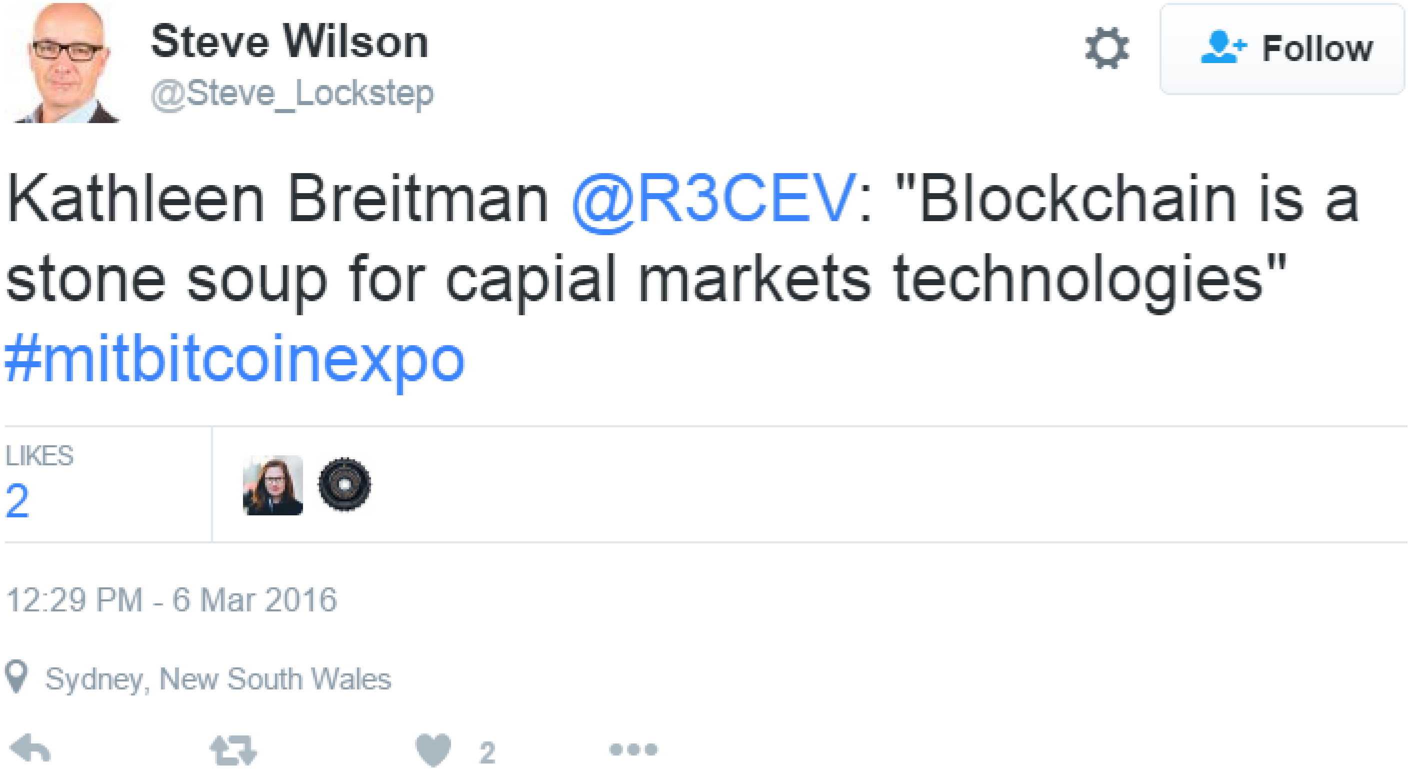
FTSE 100 index

4600
4400
4200
Change on day +0.35%

UK equities
Gains for banking stocks helped leave the FTSE 100 index on track for its best week since March after positive results from

FTSE Eur

Blockchain as stone soup



Steve Wilson
@Steve_Lockstep

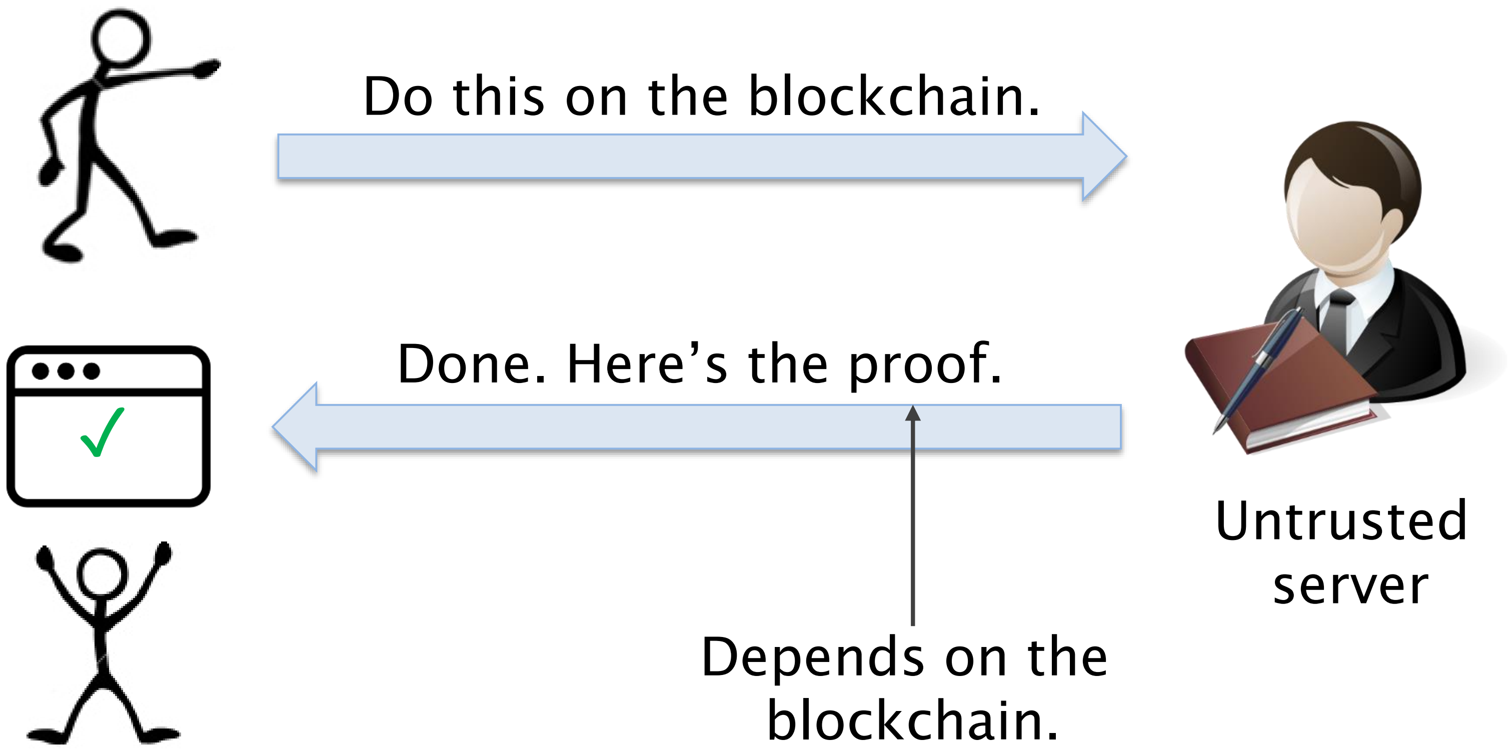
Kathleen Breitman @R3CEV: "Blockchain is a stone soup for capial markets technologies" #mitbitcoinexpo

LIKES
2

12:29 PM - 6 Mar 2016

Sydney, New South Wales

Which blockchain? It matters.



Do this on the blockchain.

Done. Here's the proof.

Untrusted server

Depends on the blockchain.

Different ledgers have vastly different security properties.

When you link / combine them, what happens to security?

A note of caution:
seeking tech solutions to social problems

Seeking tech solutions to social problems

Standardization processes can serve as a check!

- An opportunity for introspection
- A point of regulation
- Imparts legibility

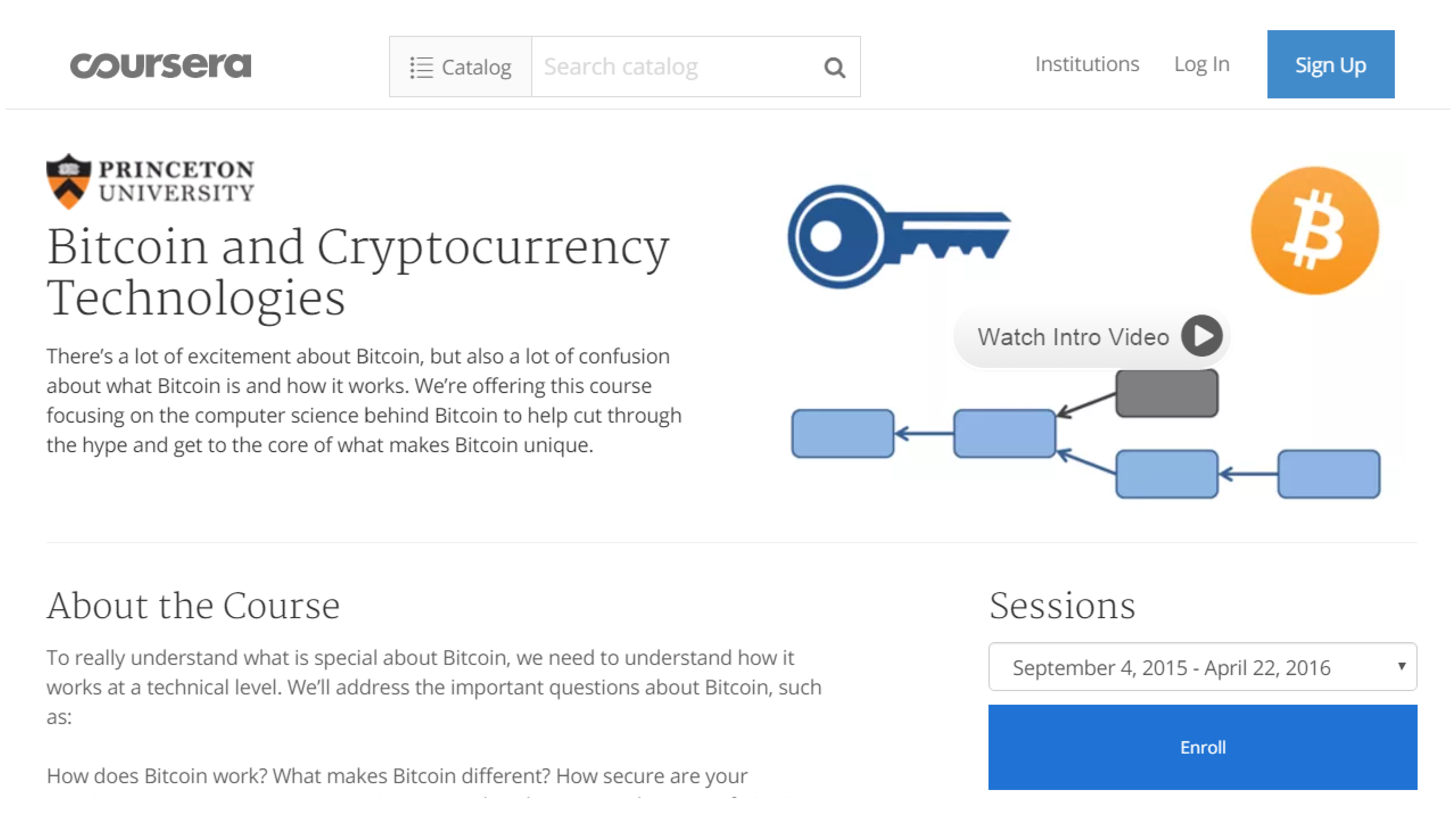
Takeaways / points for discussion

Standardization can enable new applications!

- Power of the blockchain + reach of the web.
- A way to avoid human-crypto interaction.
- A way to keep clients thin and dumb.

Which blockchain? It matters.

Standardization process is a chance to stop and think about social problems & tech.



Bitcoin and Cryptocurrency Technologies

There's a lot of excitement about Bitcoin, but also a lot of confusion about what Bitcoin is and how it works. We're offering this course focusing on the computer science behind Bitcoin to help cut through the hype and get to the core of what makes Bitcoin unique.

About the Course

To really understand what is special about Bitcoin, we need to understand how it works at a technical level. We'll address the important questions about Bitcoin, such as:

How does Bitcoin work? What makes Bitcoin different? How secure are your

Sessions

September 4, 2015 - April 22, 2016 ▾

Enroll

MultiChain

ethereum

ethereum