Blockchains, the web and standardization: the big opportunity

Keynote

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
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

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

Do this on the blockchain.

Done. Here’s the proof.

Untrusted server

Standardization targets

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
What is @<user>’s public key?

Here’s the answer.

You can verify it yourself.

Standards as a way to avoid human-crypto interaction.
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 …
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
Blockchain as stone soup

Kathleen Breitman @R3CEV: "Blockchain is a stone soup for capital markets technologies"
mitbitconexpo
Which blockchain? It matters.

Do this on the blockchain.

Done. Here’s the proof.

 Depends on the blockchain.

Untrusted server
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