

## Class 7: The Blockchain

### Schedule

**Wednesday, September 23:** Checkup 2 (was originally scheduled for Monday, September 21)

**Readings** (should be completed by Monday, September 21 at the latest; covered by Checkup 2):

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. This is the original bitcoin paper, which is quite readable and historically interesting.
- *Chapter 6: The Bitcoin Network* and *Chapter 7: The Blockchain* from Andreas Antonopoulos' book.
- *Chapter 2: How Bitcoin Achieves Decentralization* and *Chapter 5: Bitcoin Mining* from Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*.

Note: ink markings may not appear in the embedded viewer. To see them, [download the slides](#).

### Blockchain in the News

*Blockchain initiative backed by 9 large investment banks*, Financial Times, 15 Sept 2015.

*Nine of the World's Biggest Banks Form Blockchain Partnership*, Re/Code, 15 Sept 2015.

*Bitcoin Is Only The Beginning For Blockchain Technology*, Forbes, 15 Sept 2015.

*Bitcoin's Shared Ledger Technology: Money's New Operating System*, Forbes, 9 Sept 2015.

### Trust

What are valid sources of *trust*?

What are potentially misleading sources of *trust*?

What mechanisms have humans evolved or constructed to enhance trust among strangers?

## Distributed Consensus

How well does the 2-out-of-3 network consensus public ledger protocol work?

## Proof-of-Work

Cynthia Dwork and Moni Naor. *Pricing via Processing or Combatting Junk Mail*, CRYPTO 1992.

**Pricing Function:** ( $f$ ) - moderately easy to compute - cannot be amortized - computing  $f(m_1), \dots, f(m_l)$  costs  $l$  times as much as computing  $f(mi)$ . - easily verified: given  $x$ ,  $y$  easy to check  $y = f(x)$ .

Adam Back. *Hash Cash Postage Implementation*

### Interactive Hashcash:

1. Sender to Receiver: Hello
2. Receiver to Sender:  $r$  (random nonce)
3. Sender to Receiver:  $x$ , Mail where  $x = f(r)$ .
4. Receiver verifies  $x = f(r)$ .

How well does this protocol work for sending mail?

How can we make this protocol non-interactive?

## Bitcoin Mining

Proof-of-work: Find an  $x$  such that:  $\text{SHA-256}(\text{SHA-256}(r + x)) < T/d$ .

$d$  is the “difficulty” (varies).

$T$  is a fixed target (256-bit number).

$r$  depends on hash of previous block, transactions, and other information.

What does it mean for the bitcoin difficulty to go down?