# HumanCoin

## Cryptocurrency via Proof of Human-work

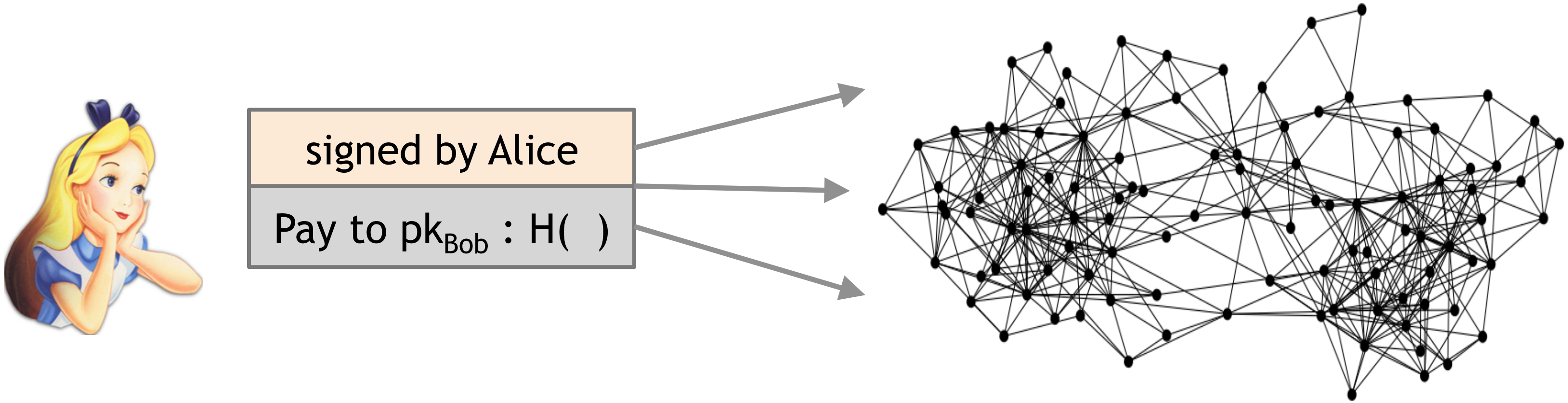
**Hong-Sheng Zhou**
Virginia Commonwealth University

joint with

**Jeremiah Blocki**
CMU/MSR

# Bitcoin is a peer-to-peer system

When Alice wants to pay Bob:
she broadcasts the transaction to all Bitcoin nodes



signed by Alice

Pay to $pk_{Bob}$ : H( )

slide credit: Andrew Miller

**new enabler for future finiancial trasactions and even more**

# Blockchain Technique

Consensus via …

proof of work puzzles (details later)

# Concerns

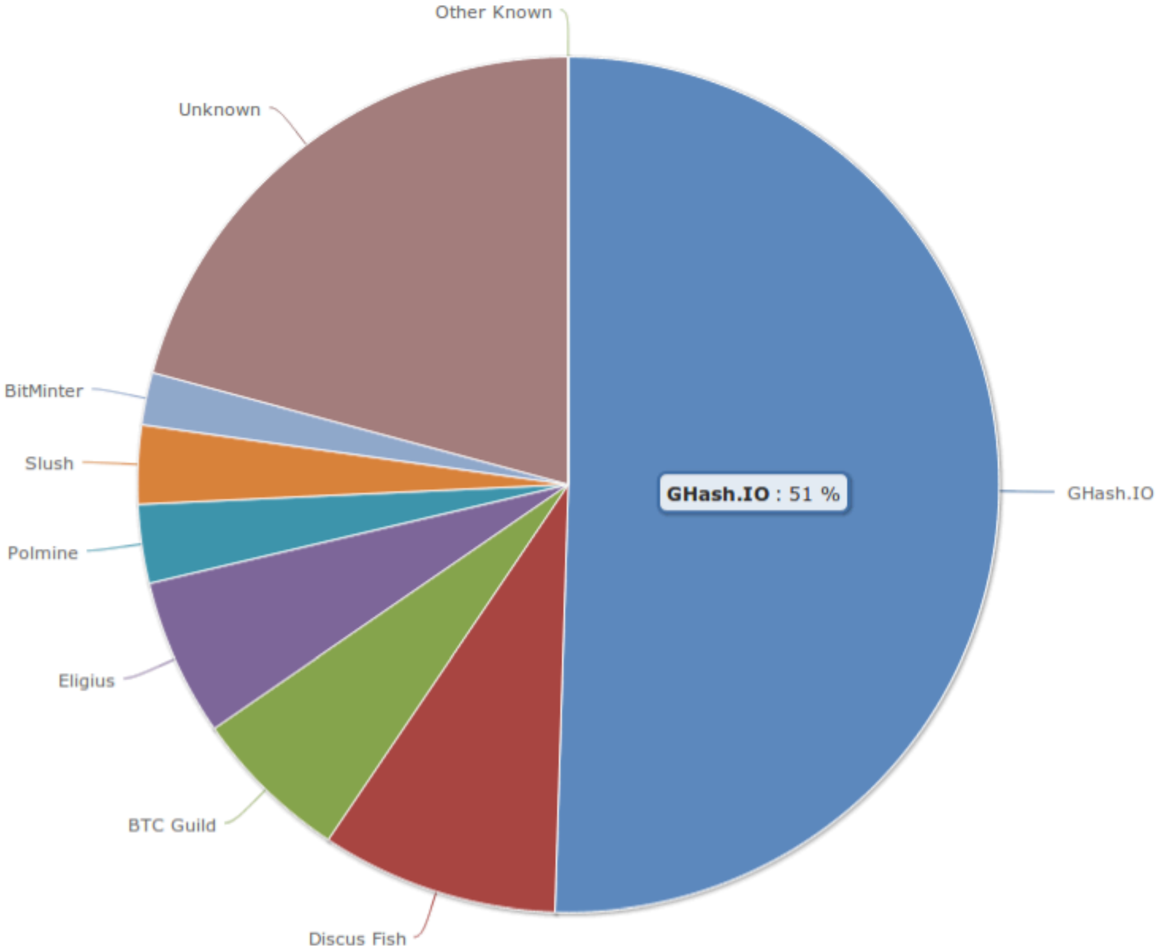
- Wasting computing resource/ electricity

- Main concern: stability

  see next slide

# June 12, 2014

## GHash.IO large mining pool crisis



slide credit: Andrew Miller

## …. invites new/alternative techniques

- proof of space
- proof of stake
- non-outsourcible proof of work
- ….

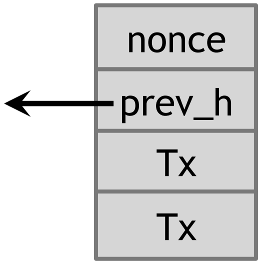
Here:

- proof of human-work

# HumanCoin via Proof of Human-work

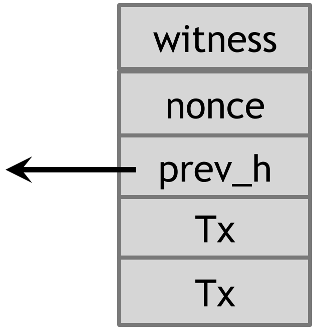
… at the moment you play Angry Birds, you actually contribute to securing a blockchain for cryptocurrency or for other applications….

# Proof of Work puzzles



To create block, find nonce s.t.
H(nonce || prev_hash || tx || … || tx) is very small

# Proof of Human-work puzzles


witness
nonce
prev_h
Tx
Tx

To create block, find nonce s.t.
H(witness||nonce||prev_hash||tx||…||tx) is small
where
puz=Sampler(nonce||prev_hash||tx||…||tx) and
witness is the solution to puzzle puz

AI assumption:
without human involved, the witness cannot be obtained

the first distributed consensus protocol from hard Artificial Intelligence problems.