Lecture 9

Bitcoin as a platform

In this lecture

We've built Bitcoin. What can we build on top?

- Commitments
- Token tracking
- Multiparty lotteries
- Public randomness
- Prediction markets

A fine stew o' ideas

Lecture 9.1:

Bitcoin as an append-only log

Secure timestamping

Goal: Prove knowledge of *x* at time *t*

If desired, without revealing *x* at time *t*

Evidence should be permanent

Hash commitments

Recall: Publishing H(*x*) is a *commitment* to *x*

- Can't find an x'≠x later s.t. H(x') = H(x)
- H(*x*) reveal no information* about *x*
  *assuming the space of possible x is big

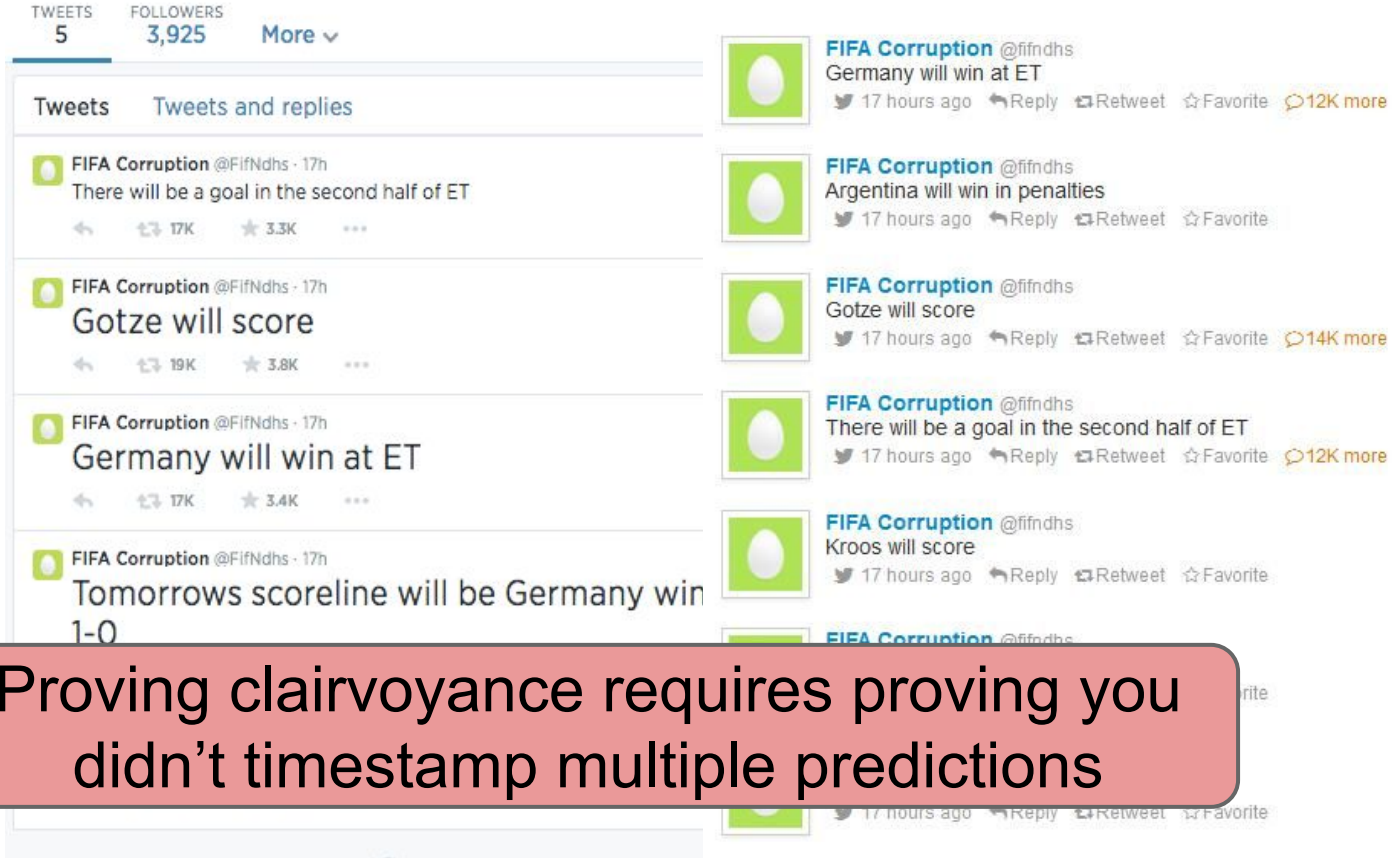
Can publish a commitment to x, reveal later

Secure timestamping applications

- Proof of knowledge
- Proof of receipt
- Hash-based signature schemes
- many, many more...

Non-application: proof of clairvoyance

Proof that FIFA is corrupt??



Proving clairvoyance requires proving you didn't timestamp multiple predictions

Offline solution: newspaper timestamp

Timestamping in Bitcoin

- **Idea**: Specify the hash of your data instead of a valid public key
- Send 1 satoshi to the address

Pros: compatible, easy
Cons: creates unspendable UTXO forever

Timestamping in Bitcoin: CommitCoin

- Clark, Essex 2012
- **Idea**: Brute-force a public key & signature starting with the first *n* bits of your data hash

Pros: compatible, “invisible”, no UTXO bloat
Cons: more expensive, low data rate

Provably unspendable commitments

```
OP_RETURN
<arbitrary data>
```

Pros: cheap, no UTXO bloat
Cons: not a standard transaction

Data rates

40-byte commitments for 1 TX fee

- 0.0001 BTC (currently ≈ US$0.05)

Enough to commit to the hash of whatever you want!

Block chain poisoning

☹

Matt
@Cheesegod69

Follow

apparently someone embedded child porn in the bitcoin block chain, storing it on every bitcoin user's computer bitcointalk.org/index.php?topi...

Travis Goodspeed
@travisgoodspeed

Follow

More

Some jerk injected pedo links into the Bitcoin block chain. So it goes.

Reply Retweet Favorite More

RETWEETS 29 FAVORITES 5

9:18 AM - 29 Apr 2013

Can we prevent poisoning?

- In general, no ☹
- Pay-to-script-hash makes it more expensive

Overlay currencies

- **Observation**: timestamping is all we need!

- Write all data to the Bitcoin block chain
  - No new mining/consensus required
- Invalid transactions may now be included
  - Need new rules-first valid tx wins

Mastercoin

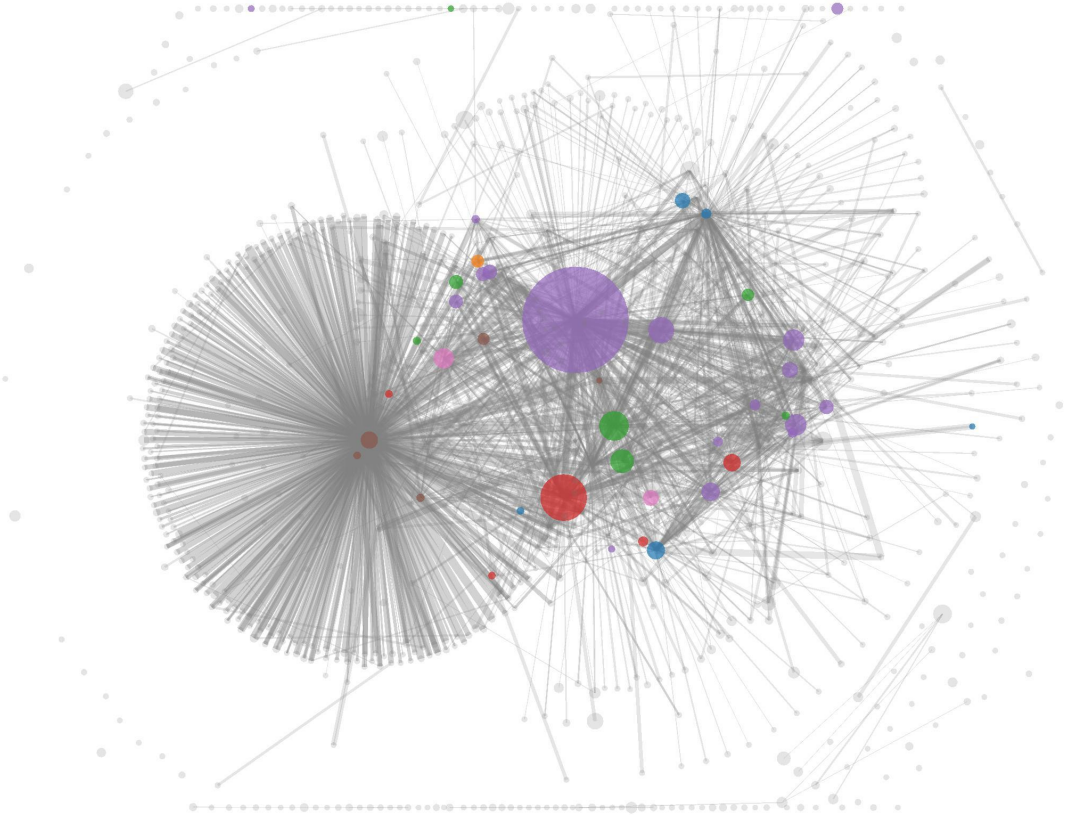
- **Goals**: overlay currency with richer transaction set
  - Smart property, smart contracts
  - User-defined currency

Pros: more features, faster development
Cons: reliant on Bitcoin, can be inefficient

Lecture 9.2:

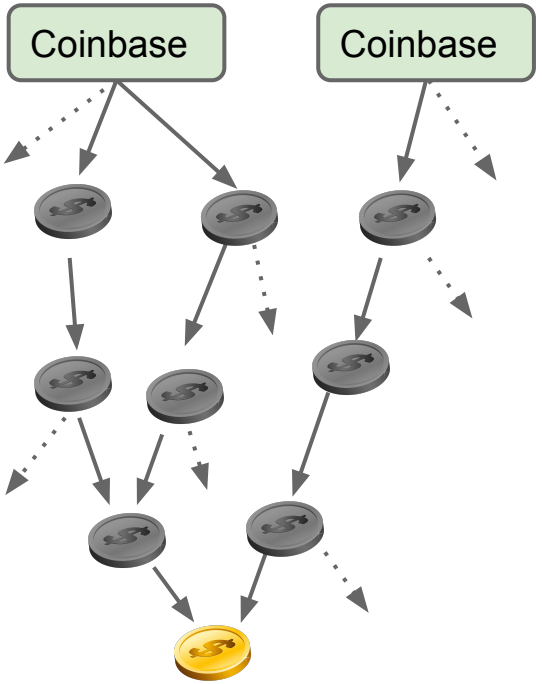
Bitcoins as “smart property”

Recall: the transaction graph



Every bitcoin* carries a history

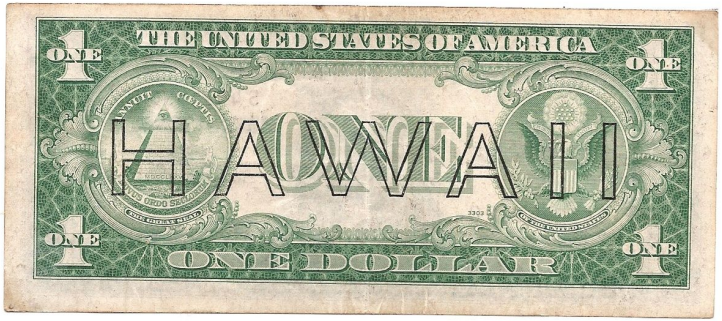
- Bad for anonymity
- Enables blacklisting
- **Observation:** bitcoins aren't fungible! Every one is unique



Can this property be useful?

*There are no "bitcoins", just unspent tx outputs

Adding metadata to currency



Without limitations on issuance, just a novelty

Authenticated metadata for currency

Idea: sign desired metadata + banknote serial #

"Bill #L11180916G hereby grants the holder admission to the Yankees game on Aug 18, 2014"

Stadium

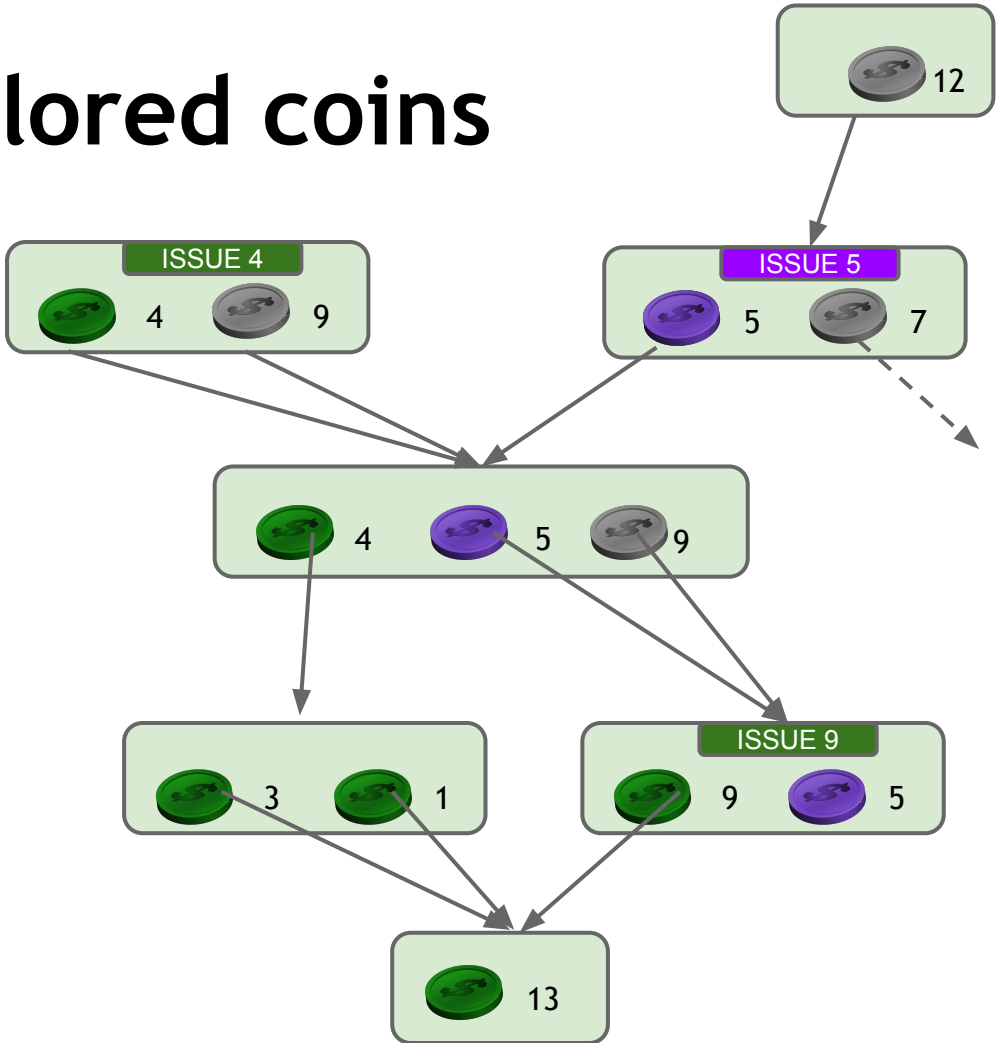
$SIGN_K(M, \#)$

Authenticated metadata for currency

- Currency can now represent anything!
- Anti-counterfeiting properties are inherited
- Underlying value also maintained!
- New meaning relies on trust in the issuer
- Some users may not understand new metadata

Can we build this on top of Bitcoin?

Colored coins



Implementation: OpenAssets protocol

- Coins issued by passing through P2SH address
  - Issuer declares address with an exchange
- Special unspendable “marker” output inserted
  - Match colored inputs to outputs
  - Can add extra metadata

Colored Coins

- Pros
  - compatible with Bitcoin
  - flexible to represent any asset
  - ignored by community
- Cons
  - small cost of unspendable markers
  - must check every previous tranasction

Applications

- stock certificates
- tickets
- deeds to real-world property
  - houses?
  - cars?
- ownership of domain names

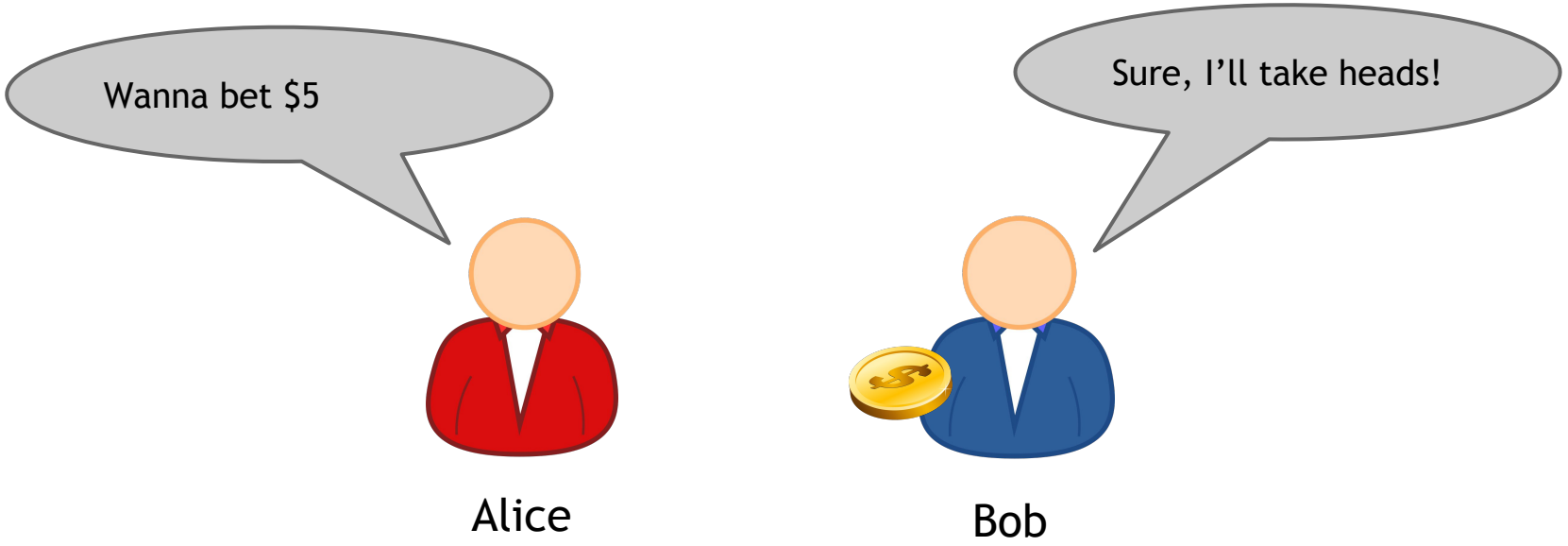
NameCoin... stay tuned for our lecture on Altcoins!

Lecture 9.3:

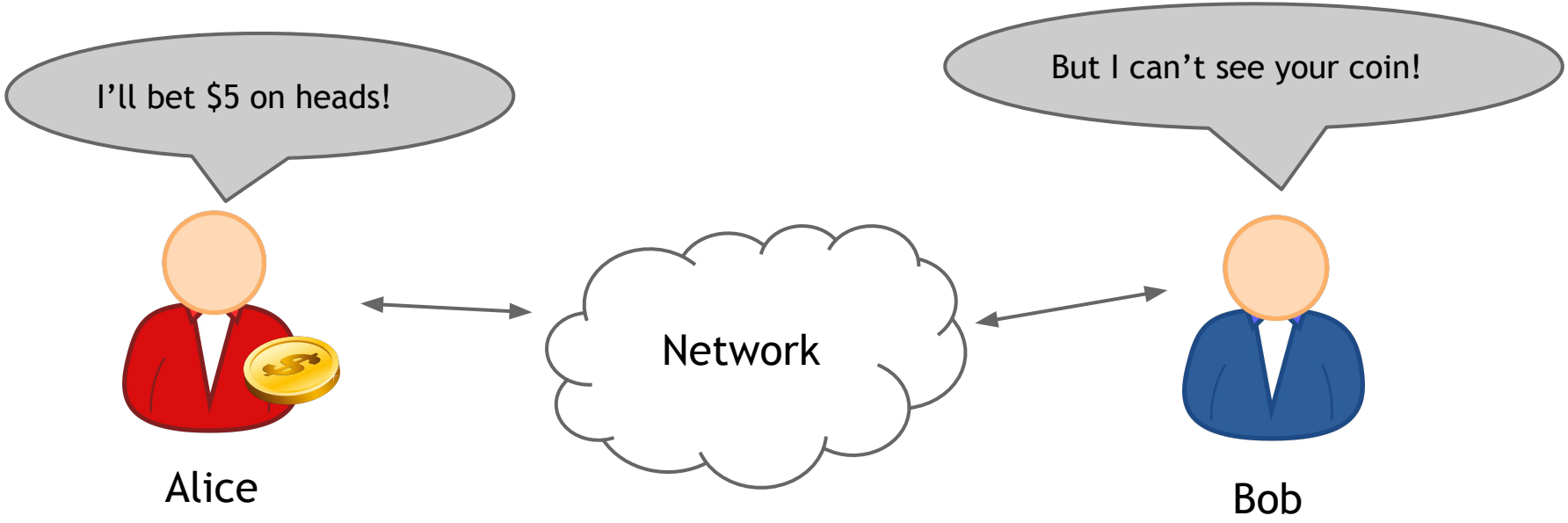
Secure multi-party lotteries in Bitcoin

Real-world lotteries without trust*

*The outcome is fair, but both parties have to trust the other will actually pay up



Online lotteries without trust?



Problem: Alice and Bob want to bet on a coin flip remotely

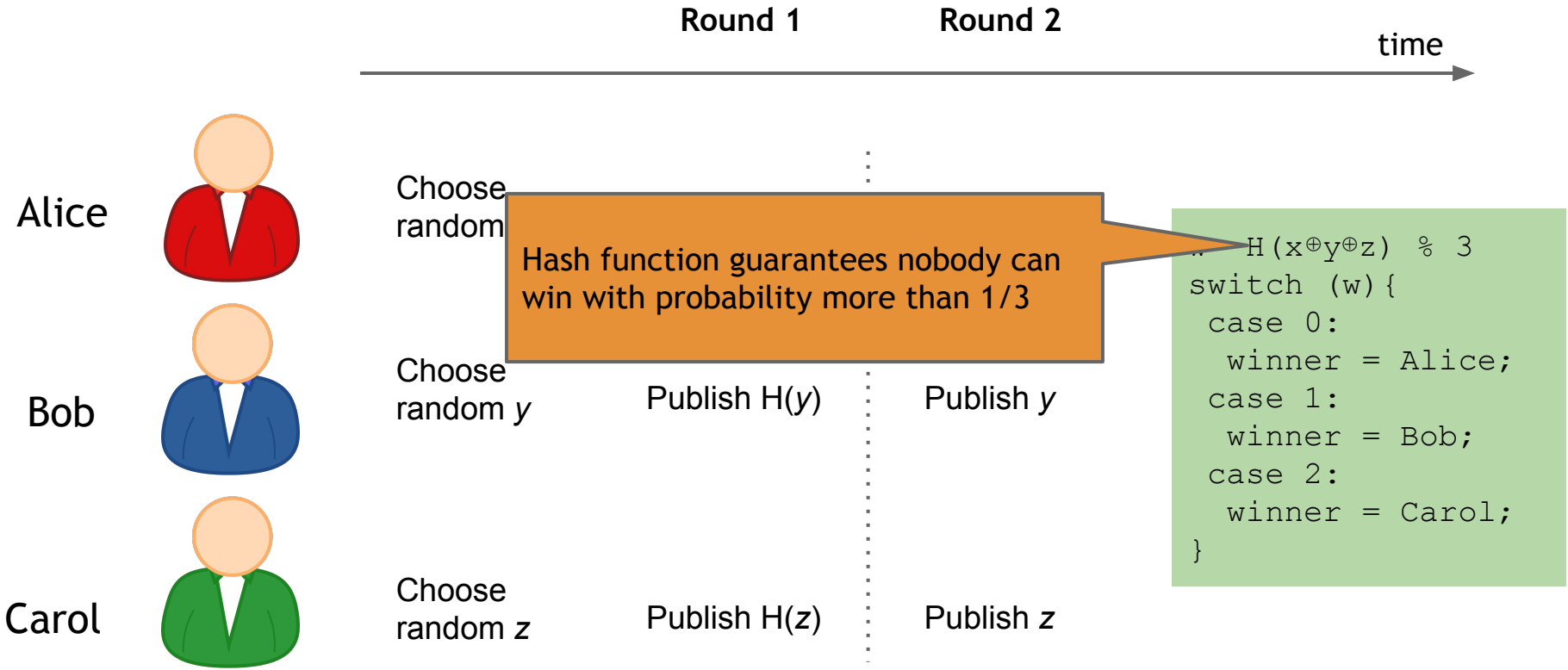
Hash commitments

Recall: Publishing H(*x*) is a *commitment* to *x*

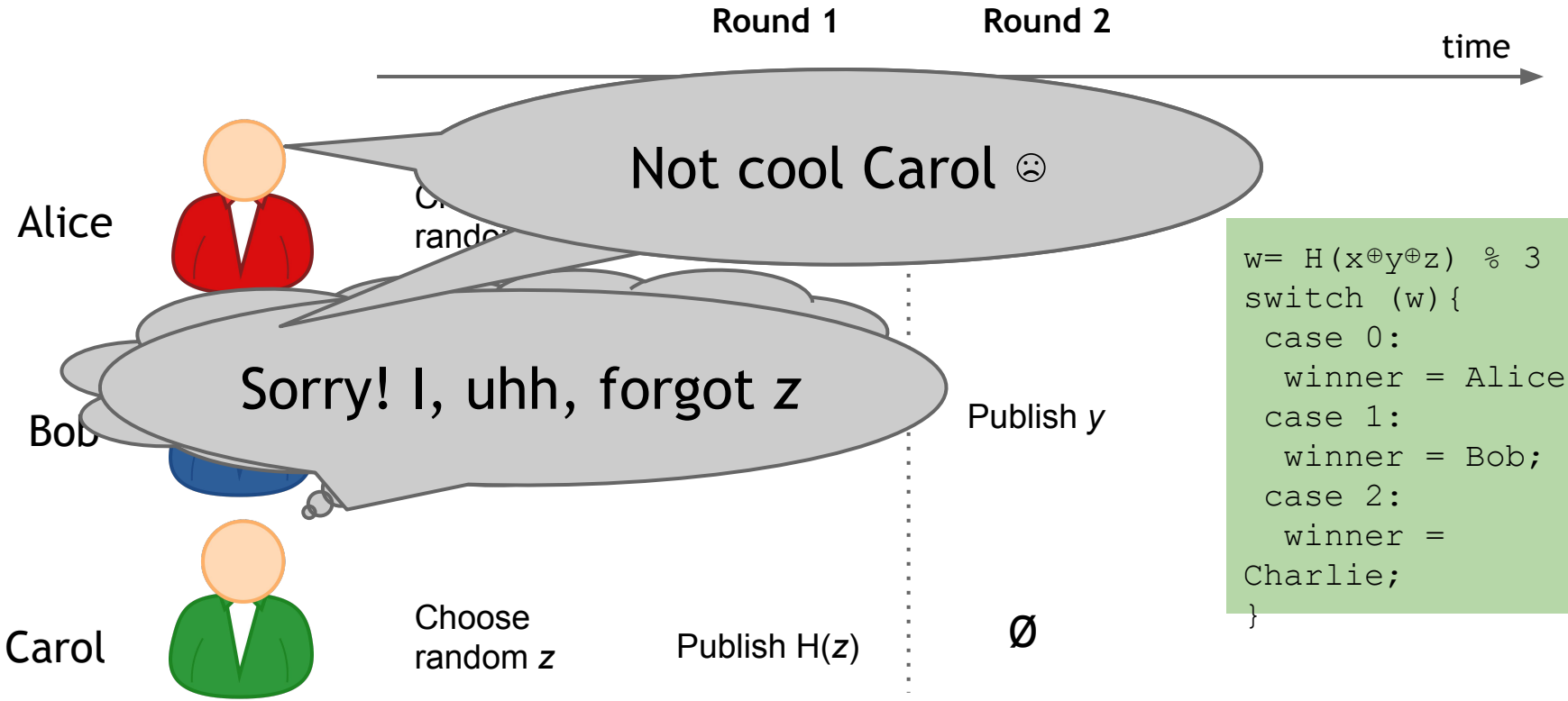
- Can't find an x'≠x later s.t. H(x') = H(x)
- H(*x*) reveal no information* about *x*

*assuming the space of possible x is big

A lottery with hash commitments



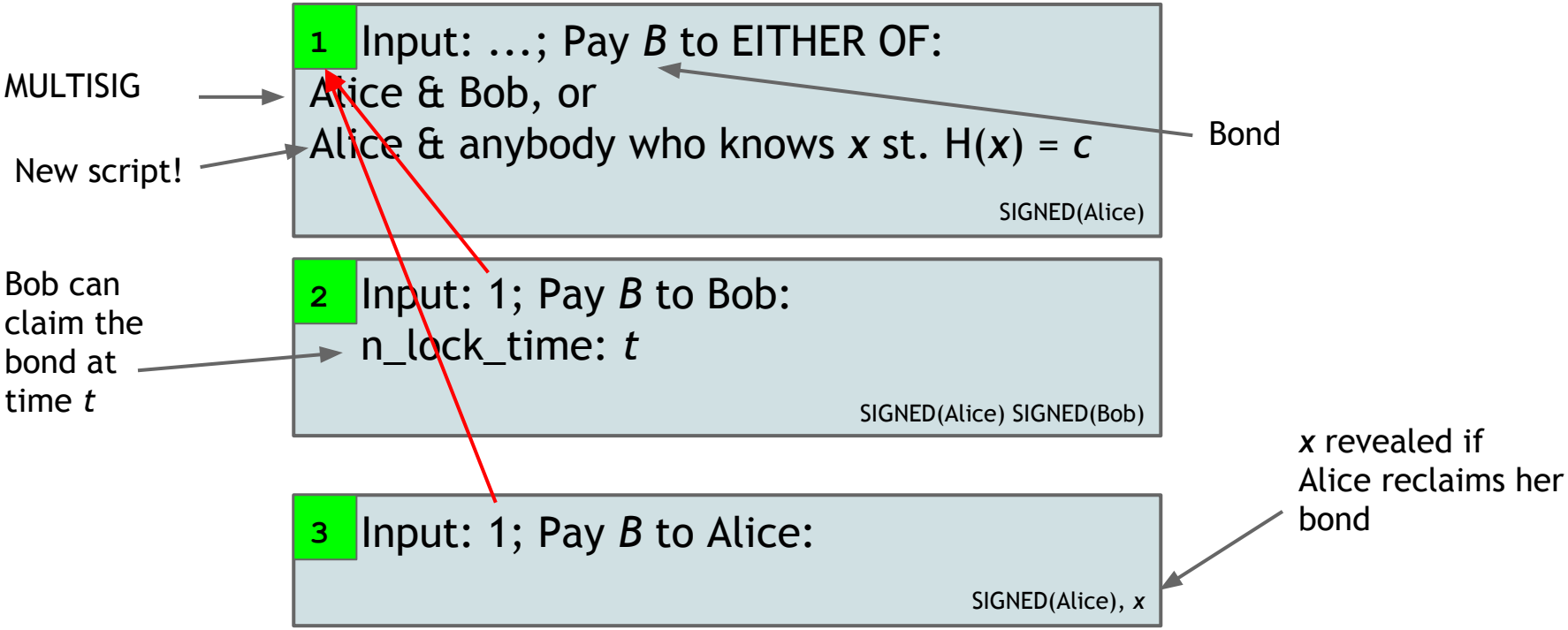
Failure to reveal commitment



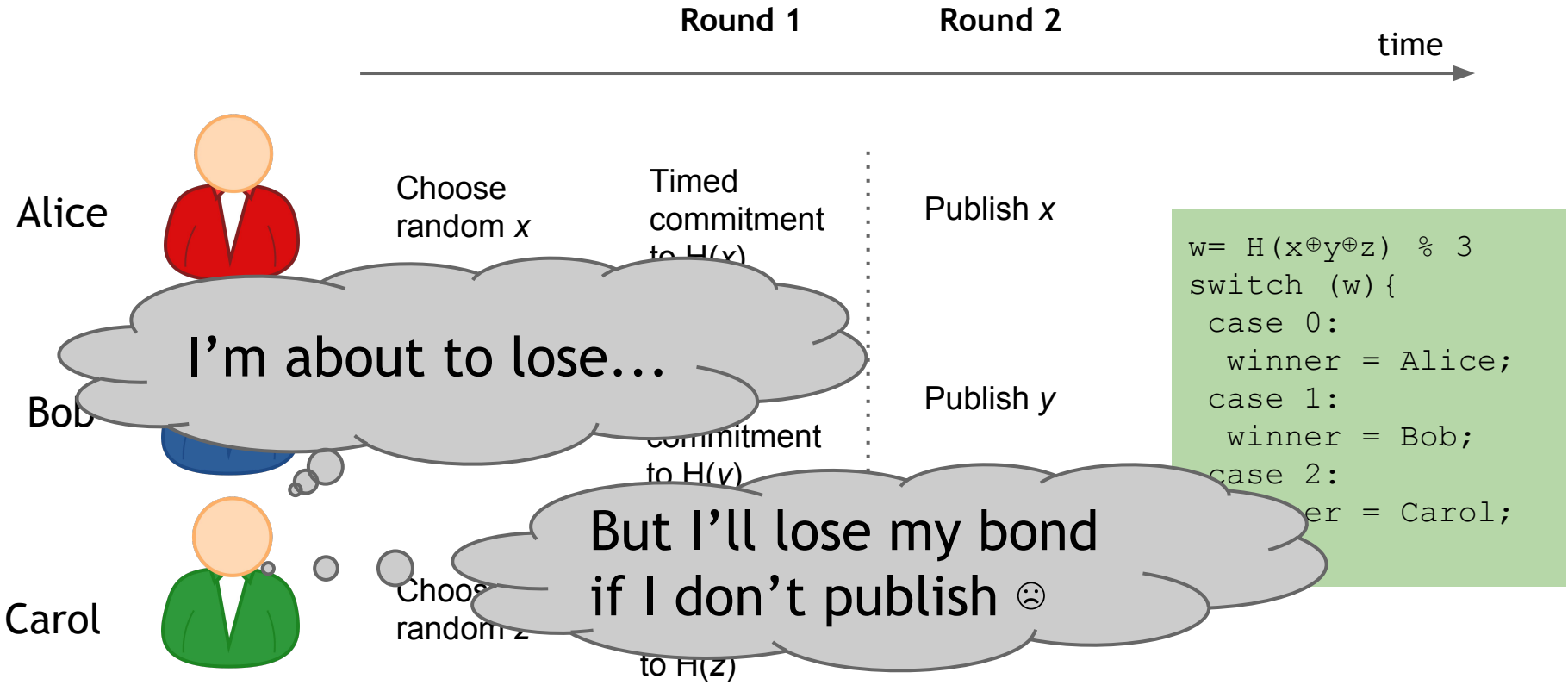

```
w= H(x⊕y⊕z) % 3
switch (w){
 case 0:
  winner = Alice;
 case 1:
  winner = Bob;
 case 2:
  winner =
Charlie;
}
```

Timed hash commitments

Idea: Force *x* to be revealed by time *t*



Lottery with timed commitments



Lottery with timed commitments

Pros:

- can be implemented on Bitcoin today
  - Andrychowicz, Dziembowski, Malinowski, Mazurek 2014

Cons:

- complexity is $O(N^2)$
- bonds must be higher than amount bet
  - griefers still might shut down large pools

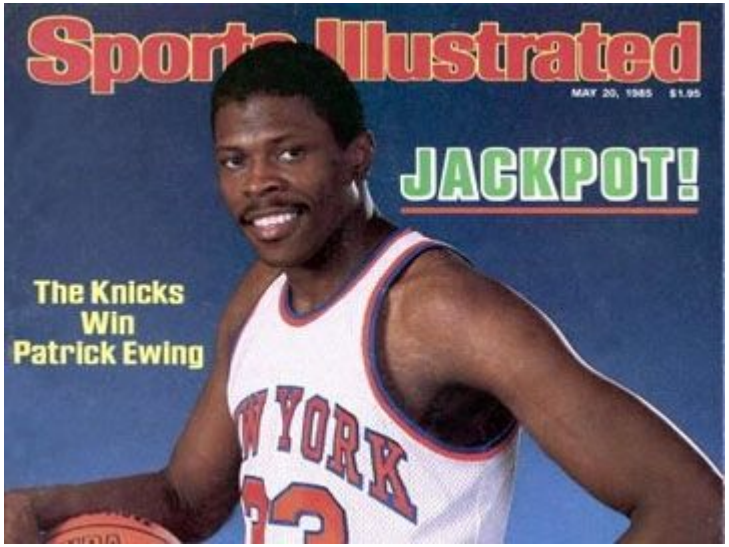
Lecture 9.4:

Bitcoin as randomness source

Public randomness protocols

- Too many interested parties to use hashes?
- More convincing randomness to the public?
- Designers don’t know alternatives available?

NBA draft lottery



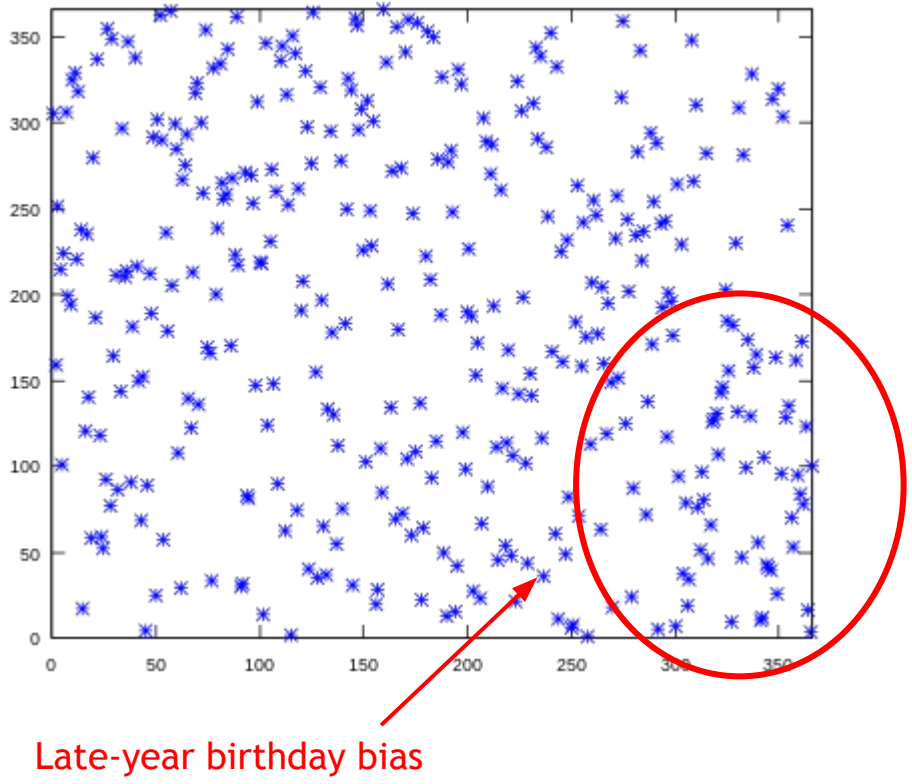
1985: Knicks win rights to Patrick Ewing

INTERNATIONAL BUSINESS TIMES

NBA Lottery 2014: Conspiracy Theories Plague Annual Event

By *Anthony Riccobono* @tony_riccobono a.riccobono@ibtimes.com
on May 20 2014 1:35 PM

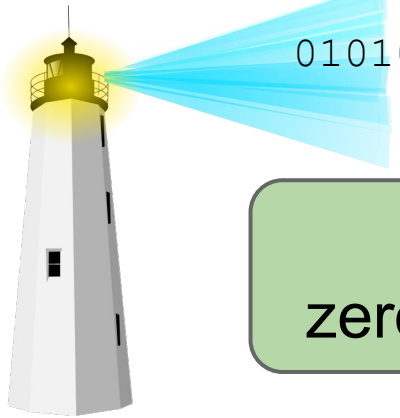
1969 Vietnam conscription lottery



Cryptographic beacons

Idea: service to regularly publish random data

- **Uniform randomness**
- **No party can predict in advance**
- **All parties see the same values**

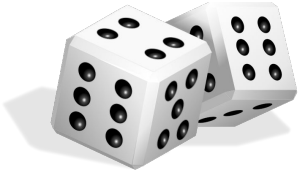


01010001 01101011 10101000 11110000 10010100

Applications: lotteries, auditing, zero-knowledge proofs, cut-and-choose, ...

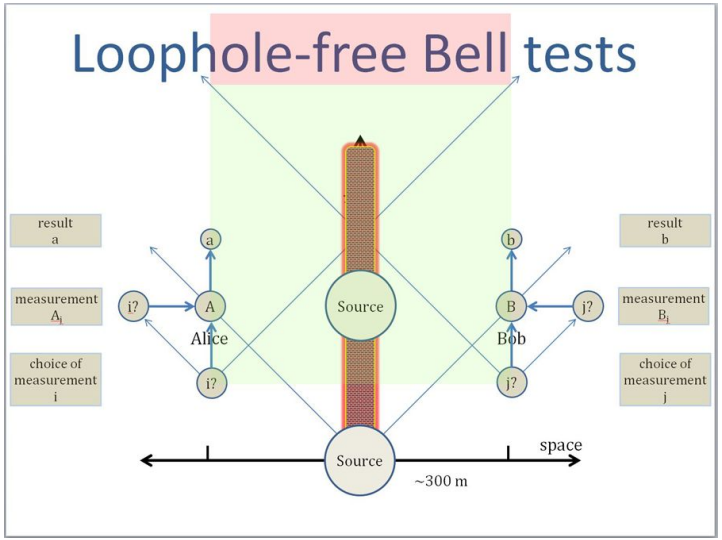
Public display of randomness






Pros: cheap, easy, simple to understand
Cons: must trust/audit operator
hard to trust remotely!

NIST beacon



Beacon Record

Version: Version 1.0

Frequency: 60 seconds

Time: 08/13/2014 12:36 pm (1407947760)

Seed Value:
27D7280A657B5E0A99721D47E21A2276C80B5CDFDCA605E397D8BBAA51C24A06
40CC9C6EEB83BBB3D837011CA5B6CA08FADC78E2B8D36C75CC971757F82068A4

Previous Output:
2F2DE0662028D3C4D6F8DD7936262D9AFBDCFD0BD14BC733E257B14F48881A99
206BBC9429FD9BFE719551EAB840CEE8157ACAEBC80342CE4B66443C0859E216

Signature:
986C73CF88056635C5E0A018358D0D91CF10A2F2B16C8B8D91AA34B0A04D103B
CFF347B714DAC343D5838E07FFDFC49BE6E39811350DC0193D17CFE1BC4EDB5B
7E3AC425EF7840EF4E549D66D0F0FB383DD9F29DFDAEF2E520B8606A4F6C55FB
3B766CC9D66494FAC1FE8983D58525224778F5AE3C3727FF0AC71DCE3B30E33B
A6CFD767EE3D299A5324E371AFB49AEC46F88D6DCAE6FCBF8B93D461B84C59CB
7577BE9A63FE0DB7C83944B545C501A4C787F87B15A0F8CFD8FB7FC191F677FB
C4FB1C07E47C01B0D090BAC564FEAFBD0E24D90F01DE2B2E66A31E7012CACD42
30EA94EF415C8F2B1751F09BD8255A2C142CE2C8C69587EE6CE788273E55AFA7

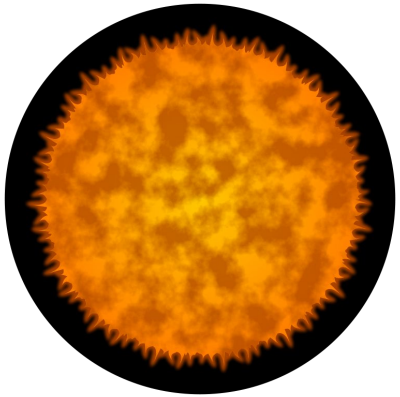
Output Value:
15E3B39DA53DE7C20A60D3EC2DECC2C6B2DB65FE07B1188D666A8A8476E4910F
592FB3F8D49E4A01E5624FDF161A698EB0AA52515A79A46F3AFA1B8D7CEBB320

Status: 0: Normal

Pros: quantum-mechanical randomness

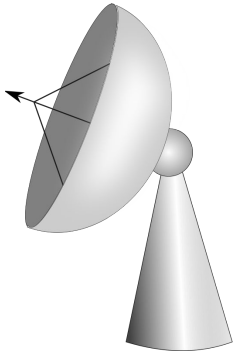
Cons: must trust NIST

Natural phenomena



Sun spots

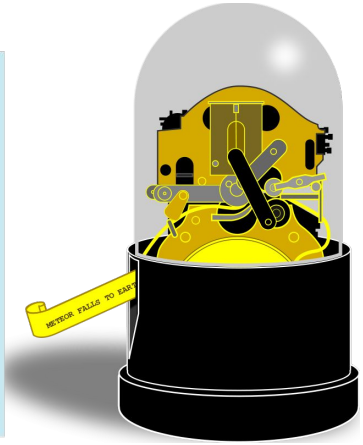
Weather



Cosmic background radiation

Pros: publicly observable, random
Cons: slow, need a trusted observer?

Stock-market beacon



Pros: good randomness, costly to manipulate
Cons: slow, insider attacks?

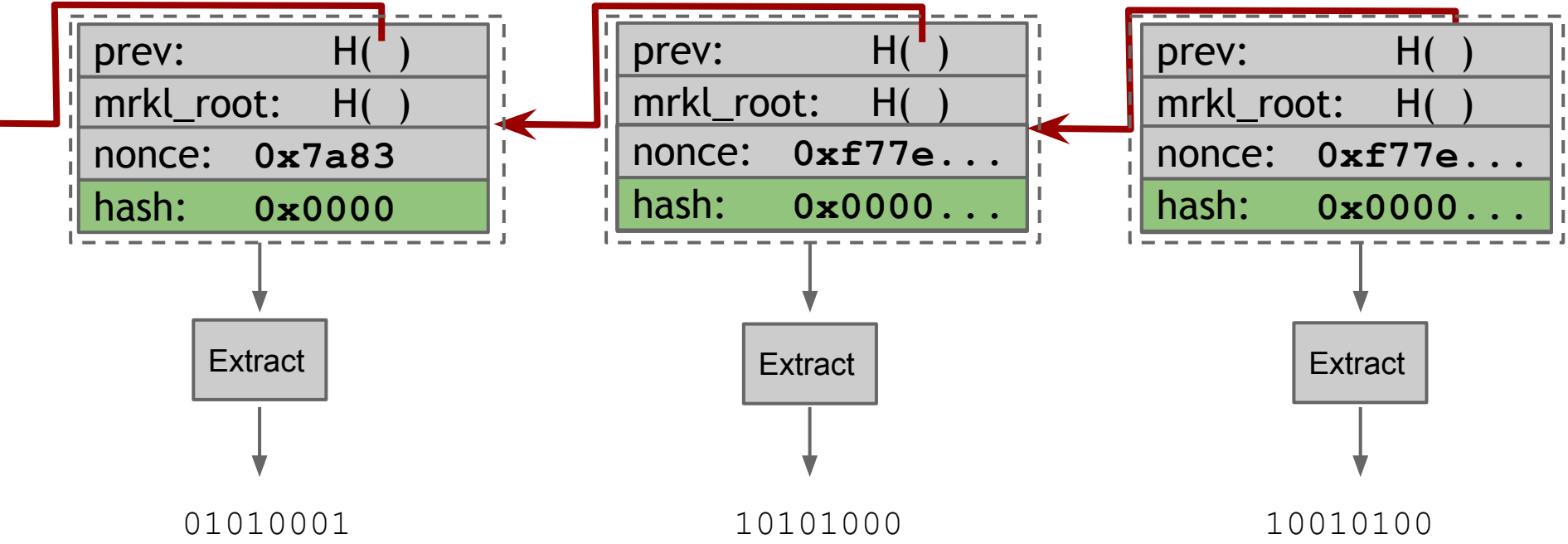
Why not use the block chain?

Recall: miners find random nonce for each block

If you could predict the next nonce with a greater than **1/d** probability, you'd have a mining shortcut

Currently, $d > 2^{66}$

Turning the block chain into a beacon



Cost of manipulation

Attacker might mine a block but discard it

- Or bribe other miners to do so

Bernoulli trials: forcing a beacon outcome with probability p requires discarding $1/p - 1$ blocks

Discarding a block “costs” 25 BTC

Cost of manipulation

Single coin flip: secure if wager is < 25 BTC

N-party lottery: secure if pool is < 25 (*n*-1) BTC

Pros

- First proposal for fully decentralized beacon
- Output every 10 minutes
- Can precisely analyze manipulation costs
- Can extend security with multiple blocks
  - Not very efficient

Cons

- Timing is imprecise
  - Block chain not synchronized w/ real time
- Need to delay to insure against forks
- Manipulation may be too cheap for some applications

Built-in beacon support in script

- **Idea**: add an opcode for a beacon call
- Can build multi-party lotteries
  - only one round
  - no bonds
  - no time delay for refunds

Lecture 9.5:

Prediction markets & real-world data feeds

Assertions about the outside world

- **Idea**: add a mechanism to assert facts
  - election outcomes
  - sports results
  - commodity prices
- Bet or hedge results using smart contracts
- Forwards, futures, options...

Most general formulation: **prediction market**

Prediction markets

- **Idea**: trade *shares* in a potential future event
- Shares worth X if the event happens, 0 if not
- Current price / x = estimated probability

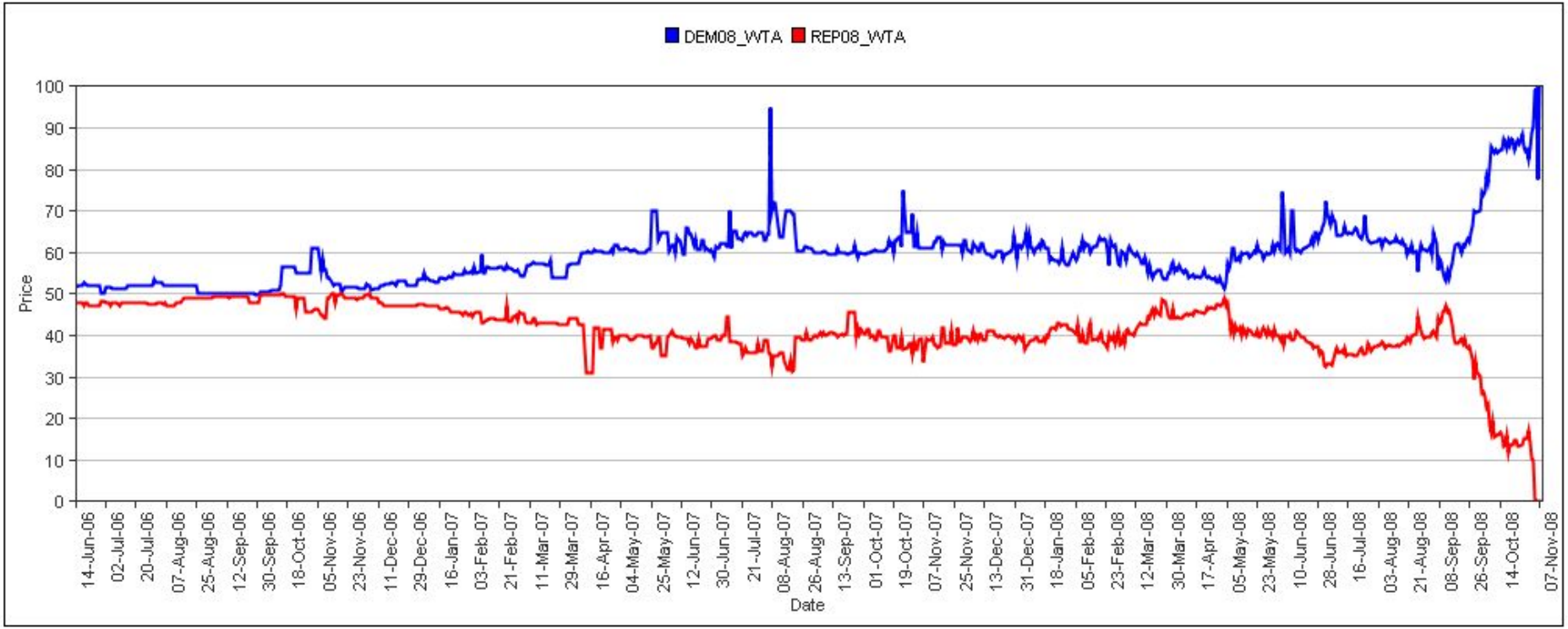
Example: World Cup 2014

					
pre-tournament	0.12	0.09	0.22	0.01	0.05
after group stage	0.18	0.15	0.31	0.06	0.00
before semis	0.26	0.21	0.45	0.00	0.00
before finals	0.64	0.36	0.00	0.00	0.00
final	1	0	0	0	0

Can immediately profit!

Should have shorted

Example: 2008 US Presidential election



source: Iowa Electronic Markets

Prediction markets

- Economists love them
  - reveal all knowledge about the future
    - (under a number of assumptions)
  - allows profit from accurate predictions
  - “a tax on BS”
- Often beat polls and expert opinions
- Significant regulatory hurdles
  - InTrade shut down in 2013

Decentralized prediction markets?

- Decentralized payment & enforcement
- Decentralized arbitration
- Decentralized order book

Decentralized payment & settlement

- Simple solution: Bitcoin + trusted arbiters
- Better solution: altcoin with built-in support

Payment & settlement - FutureCoin

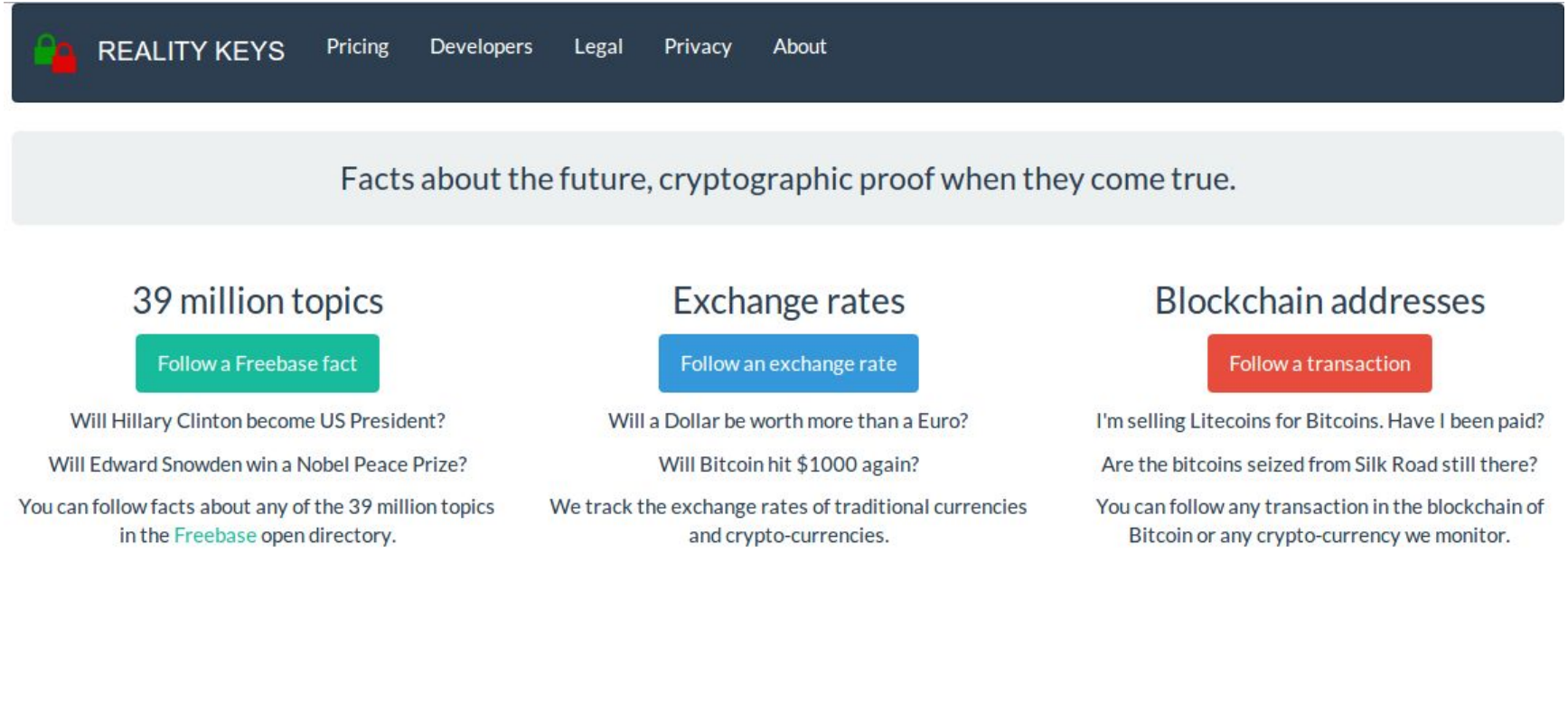
- BuyPortfolio(event e)
  - one share in *every* outcome for $1
- TradeShares(...)
  - exchange shares for each other or currency
  - one way of profiting
- SellPortfolio(event e)
  - redeem one share in every outcome for $1

Clark et al. 2014

Arbitration models

- Trusted arbiters
  - allow anybody to define & open a market
  - risk of incorrect arbitration, absconding
- Users vote
  - requires incentives, bonds, reputation
  - keynesian beauty contest?
- Miners vote
  - may be disinterested or not know

RealityKeys



Reality can be complicated!

Super Bowl XLVIII:
what color gatorade will be poured on the winning coach?

`Clear:0.31 Orange:0.22 Yellow:0.22 Blue:0.08 Red:0.08 Green:0.08`

Orange?

Yellow?

Order books

- Goal: match best bid and ask offers

Predictious.com

Centralized order books

- Traditional model
- Promise to split surplus between buyer, seller
- Front-running is considered a serious crime!
  - require regulation, auditing, monitoring

Decentralized order books

- **Idea:** Submit orders to miners, let them match *any* possible trade
- Spread is retained as a transaction fee
- Front-running now not profitable!
- May be less efficient
  - Higher fees
  - Slower trades to avoid higher fees

Decentralized order books

- **Idea:** Submit orders to miners, let them match *any* possible trade
- Spread is retained as a transaction fee
- Front-running now not profitable!
- May be less efficient
  - Higher fees
  - Slower trades to avoid higher fees

What can be built on Bitcoin?

payment	✓
settlement	no trades
arbitration	trusted arbiter only
order books	must be external

Bitcoin isn’t enough

In the next lecture

Bitcoin can only take us so far

What if we could start again from scratch?