

Blockchains & Cryptocurrencies

Applications of Blockchains - I

Instructor: Abhishek Jain
Johns Hopkins University - Spring 2021

*Many slides based on NBFMG

What can we build on top of Bitcoin/Blockchains?

Why Applications from Bitcoin/Blockchains?

- Decentralization: Many applications easy to realize with a central trusted authority. Bitcoin/Blockchains can often help in removing central trust

Applications

- Timestamping
- Token tracking
- Public randomness
- Prediction markets
- Fair protocols: Multiparty lotteries, MPC
- One-time Programs
- Non-Interactive Zero Knowledge
- ...

Bitcoin as an append-only ledger

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 $H(key, x)$ is a commitment to x

- Can't find an $x' \neq x$ later s.t. $H(key, x') = H(key, x)$
- $H(key, x)$ does not reveal x in RO model

Can publish a commitment to x , reveal later

Secure timestamping applications

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

Non-application: proof of clairvoyance

Proof that FIFA
is corrupt??

TWEETS 5 FOLLOWERS 3,925 More ▾

Tweets Tweets and replies

FIFA Corruption @FifNdhs · 17h There will be a goal in the second half of ET
17K 3.3K ...

FIFA Corruption @FifNdhs · 17h Gotze will score
19K 3.8K ...

FIFA Corruption @FifNdhs · 17h Germany will win at ET
17K 3.4K ...

FIFA Corruption @FifNdhs · 17h Tomorrows scoreline will be Germany win 1-0

FIFA Corruption @fifndhs Germany will win at ET
17 hours ago Reply Retweet Favorite 12K more

FIFA Corruption @fifndhs Argentina will win in penalties
17 hours ago Reply Retweet Favorite

FIFA Corruption @fifndhs Gotze will score
17 hours ago Reply Retweet Favorite 14K more

FIFA Corruption @fifndhs There will be a goal in the second half of ET
17 hours ago Reply Retweet Favorite 12K more

FIFA Corruption @fifndhs Kroos will score
17 hours ago Reply Retweet Favorite

Proving clairvoyance requires proving you didn't timestamp multiple predictions

Offline solution: newspaper timestamp

26

guardtime guardtime.com
15 July 2009 09:00:00 UTC

AAAAAA-CELUOA-AAITFX-BEPAMP
VRUBBC-TDQE70-TBCTP4-M53E85
UE05EC-UU2A3N-0CCCIR-PLM4PG

MARK

Friday July 17 2009

S&P 500 index	FTSE 100 index	FTSE Euro
1000	4600	950
950	4400	900
900	4200	850

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

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

The image shows a newspaper clipping from July 17, 2009. In the top left corner, there is a timestamp from Guardtime: "guardtime guardtime.com 15 July 2009 09:00:00 UTC" followed by a string of random characters. To the right, the word "MARK" is printed in large letters. Below the date, there is a red horizontal bar with the text "Friday July 17 2009". The main content consists of three tables comparing S&P 500 index, FTSE 100 index, and FTSE Euro. Each table has three rows: the first row shows values 1000, 4600, and 950 respectively; the second row shows values 950, 4400, and 900; and the third row shows values 900, 4200, and 850. Each table includes a small chart showing a recent price movement. Below the first table, there is a section titled "US equities" with a brief news snippet. Below the second table, there is a section titled "UK equities" with another news snippet.

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

Provably unspendable commitments

```
OP_RETURN  
<arbitrary data>
```

Pros: cheap, no UTXO bloat

Cons: not a standard transaction

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?topic...



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

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



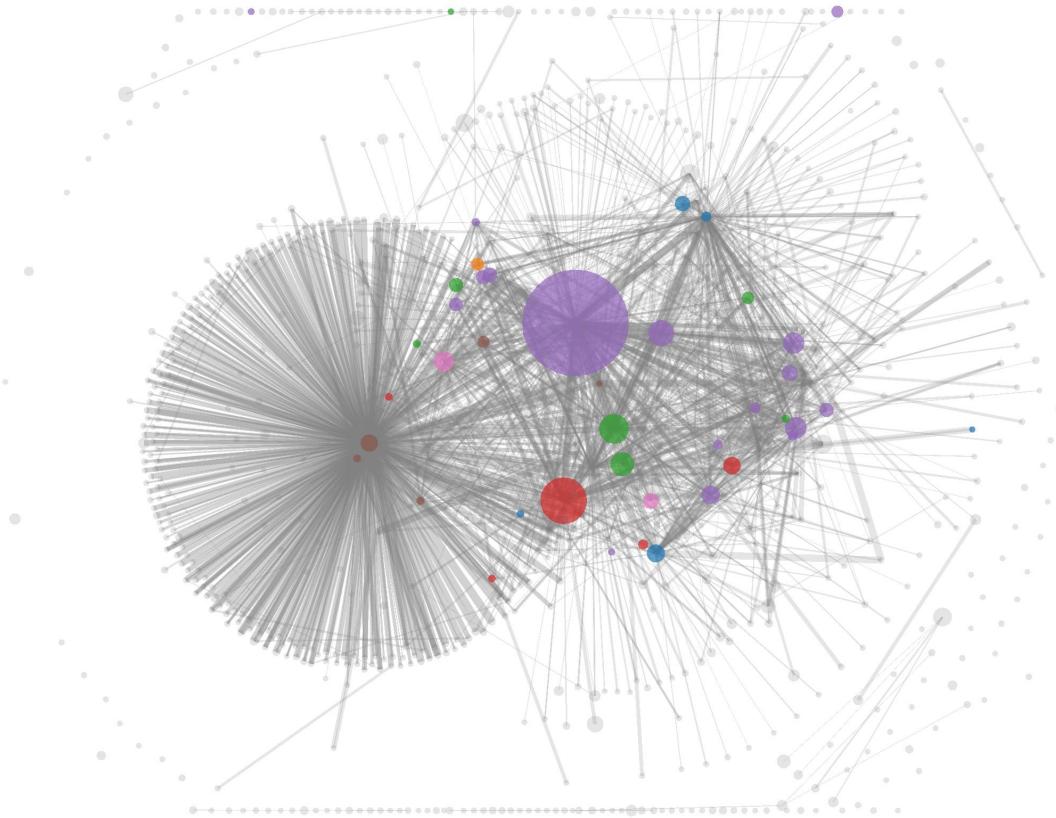
- **Goals:** overlay currency with richer transaction set
 - Smart property, smart contracts
 - User-defined currency

Pros: more features, faster development

Cons: reliant on Bitcoin, can be inefficient

Bitcoins as “smart property”

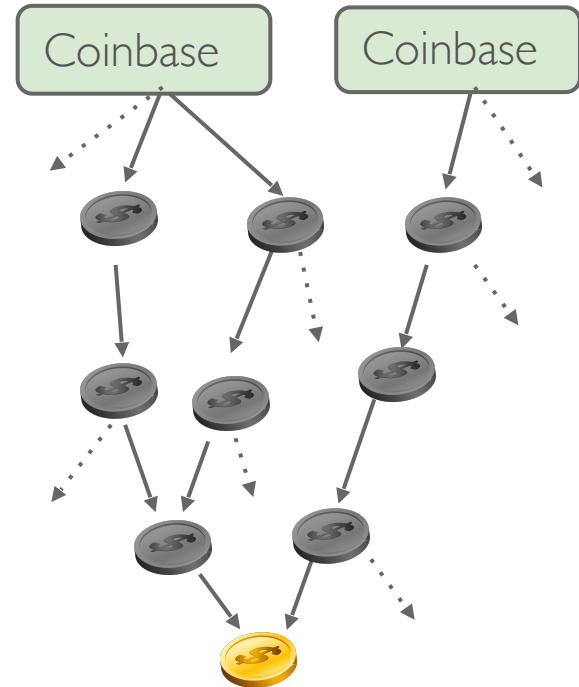
Recall: the transaction graph



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”



$\text{SIGN}_K(M, \#)$



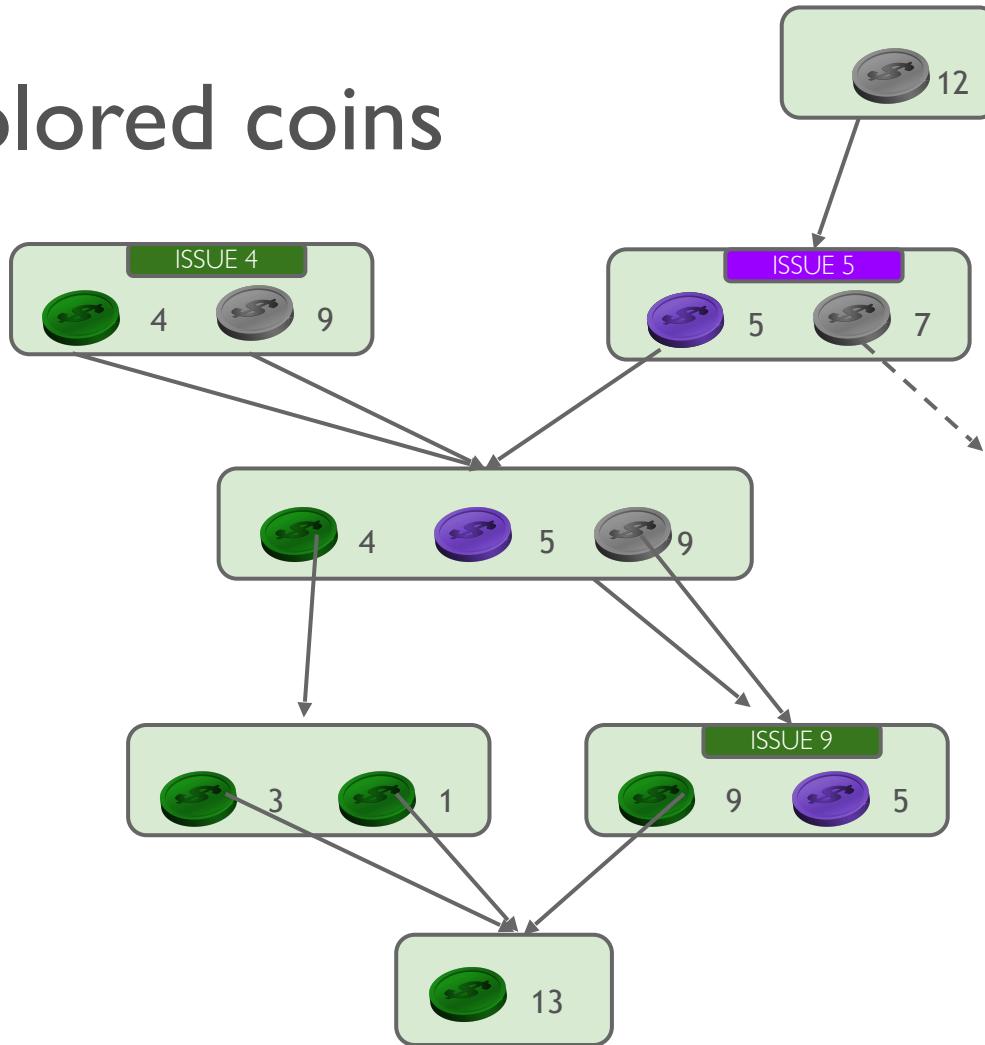
Stad
ium

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 transaction

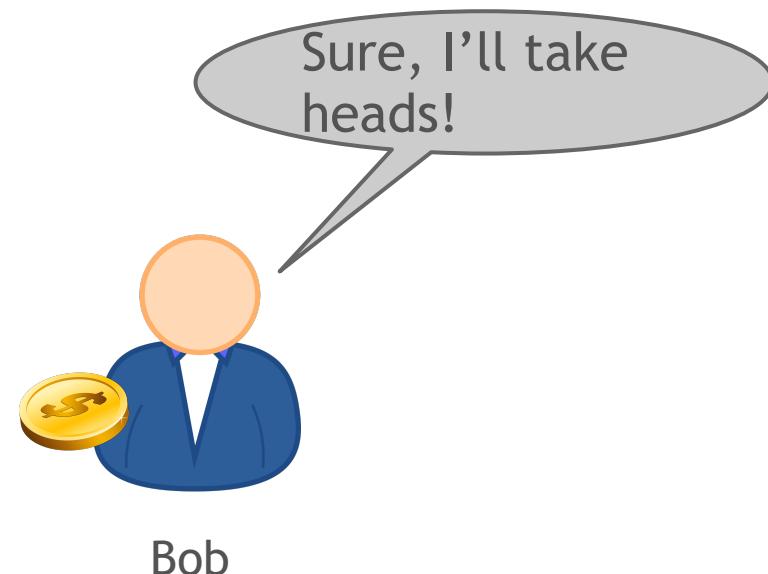
Applications

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

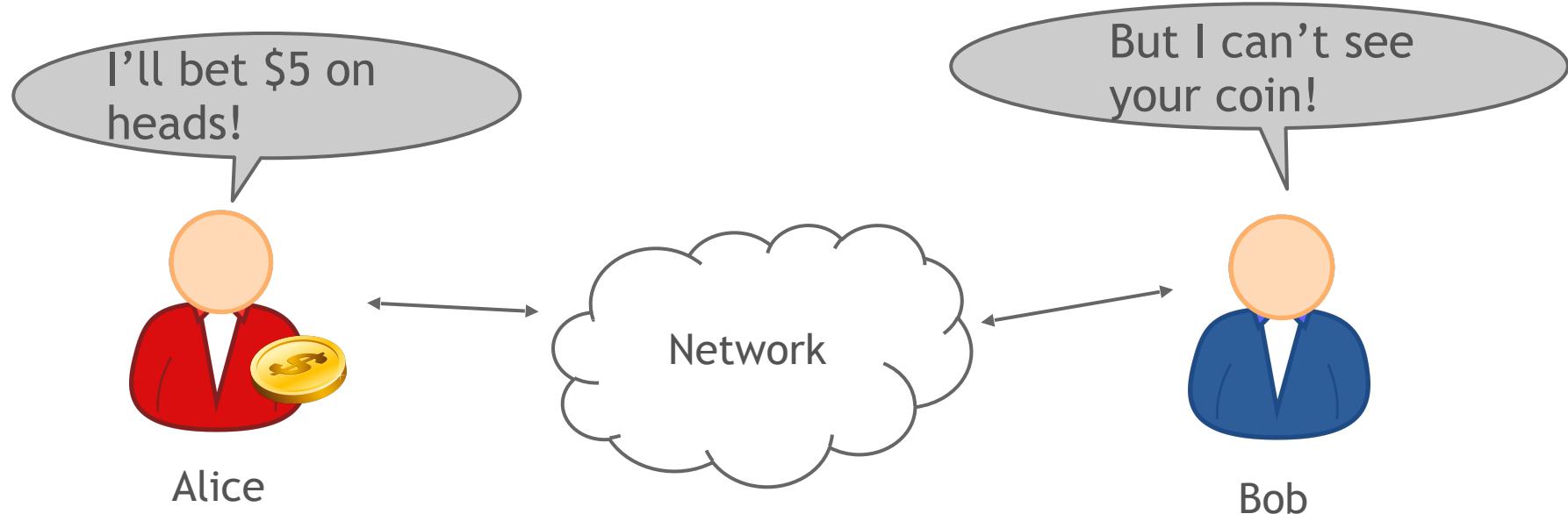
Secure multi-party lotteries in Bitcoin

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

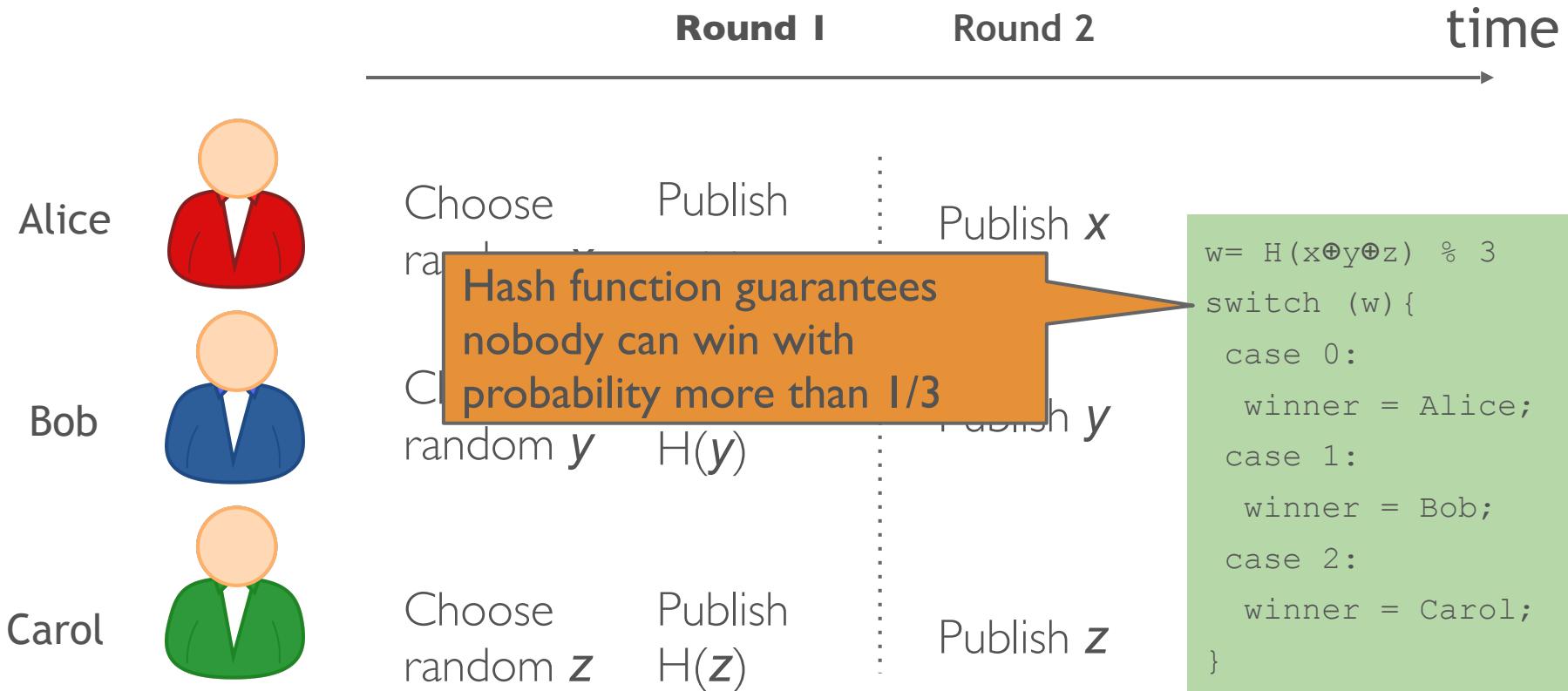
Hash commitments

Recall: Publishing $H(\text{key}, x)$ is a *commitment* to x

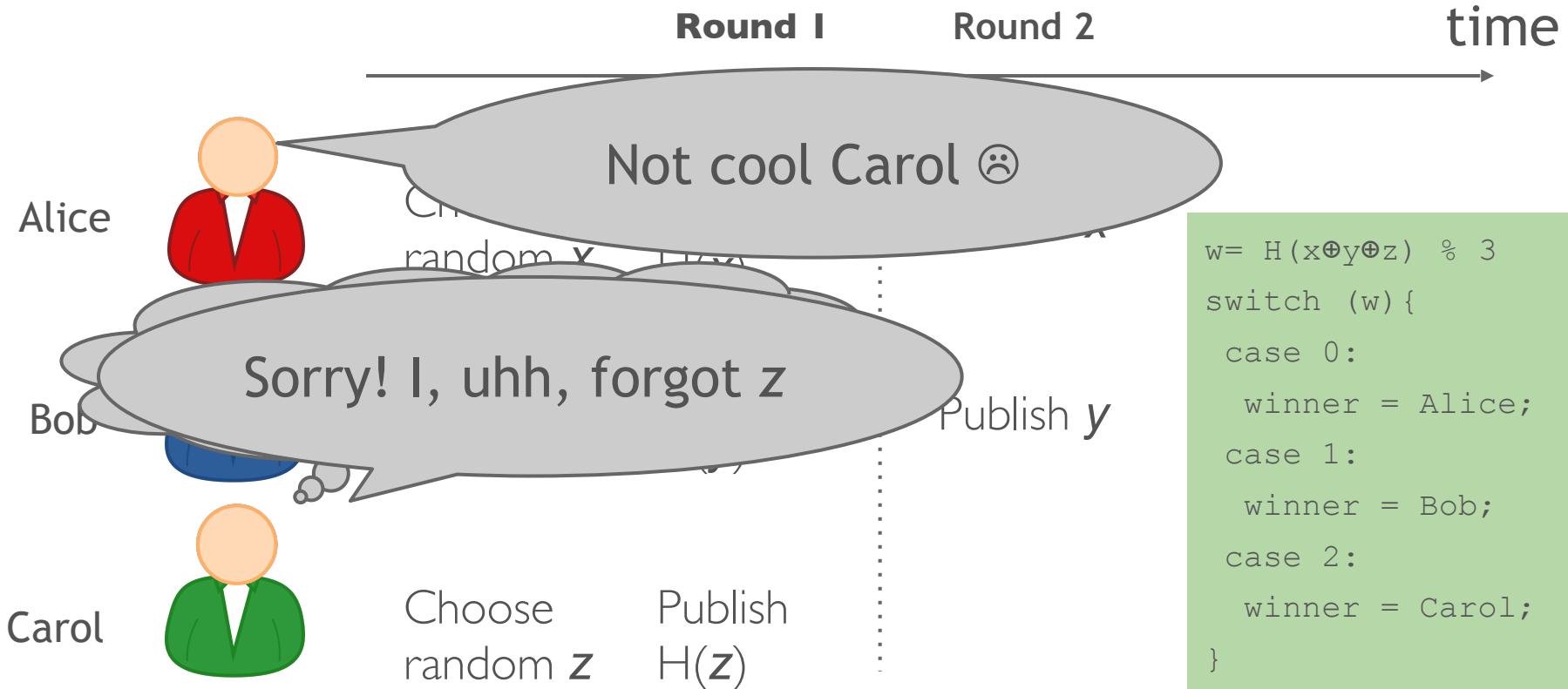
- Can't find an $x' \neq x$ later s.t. $H(\text{key}, x') = H(\text{key}, x)$
- $H(\text{key}, x)$ does not reveal x in RO model

Can publish a commitment to x , reveal later

A lottery with commitments

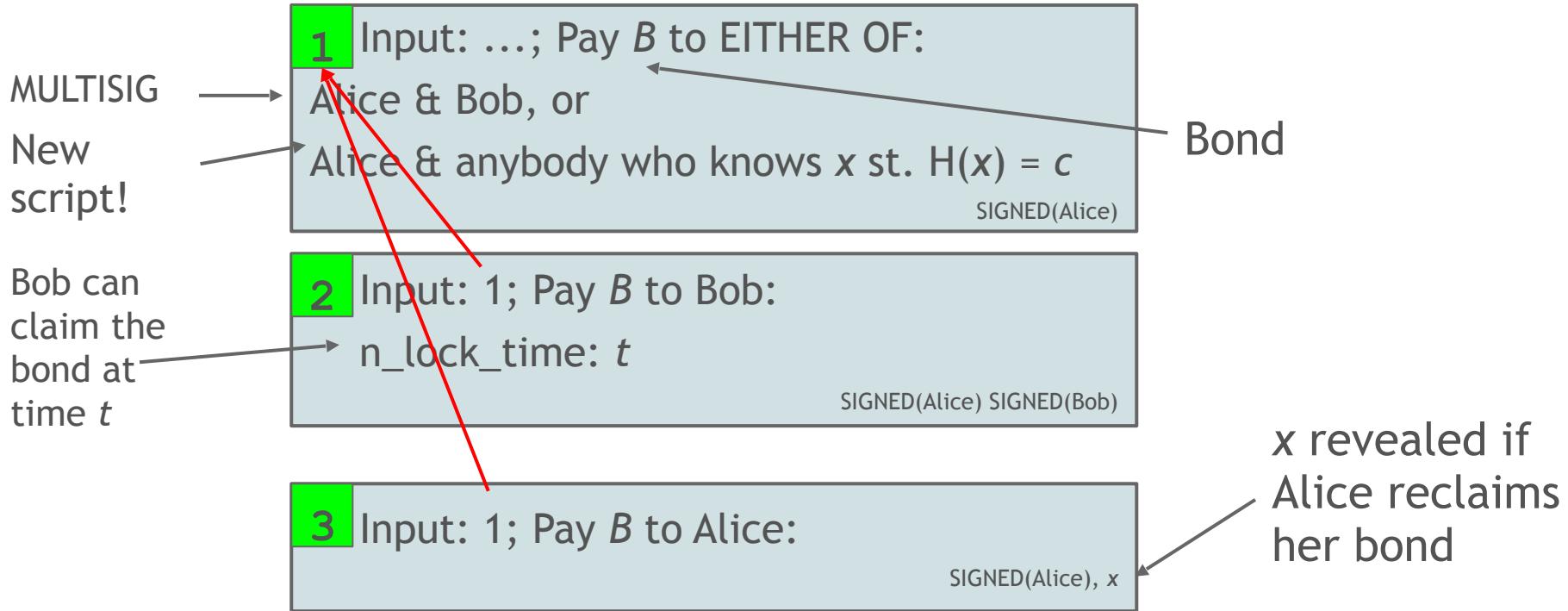


Failure to reveal commitment

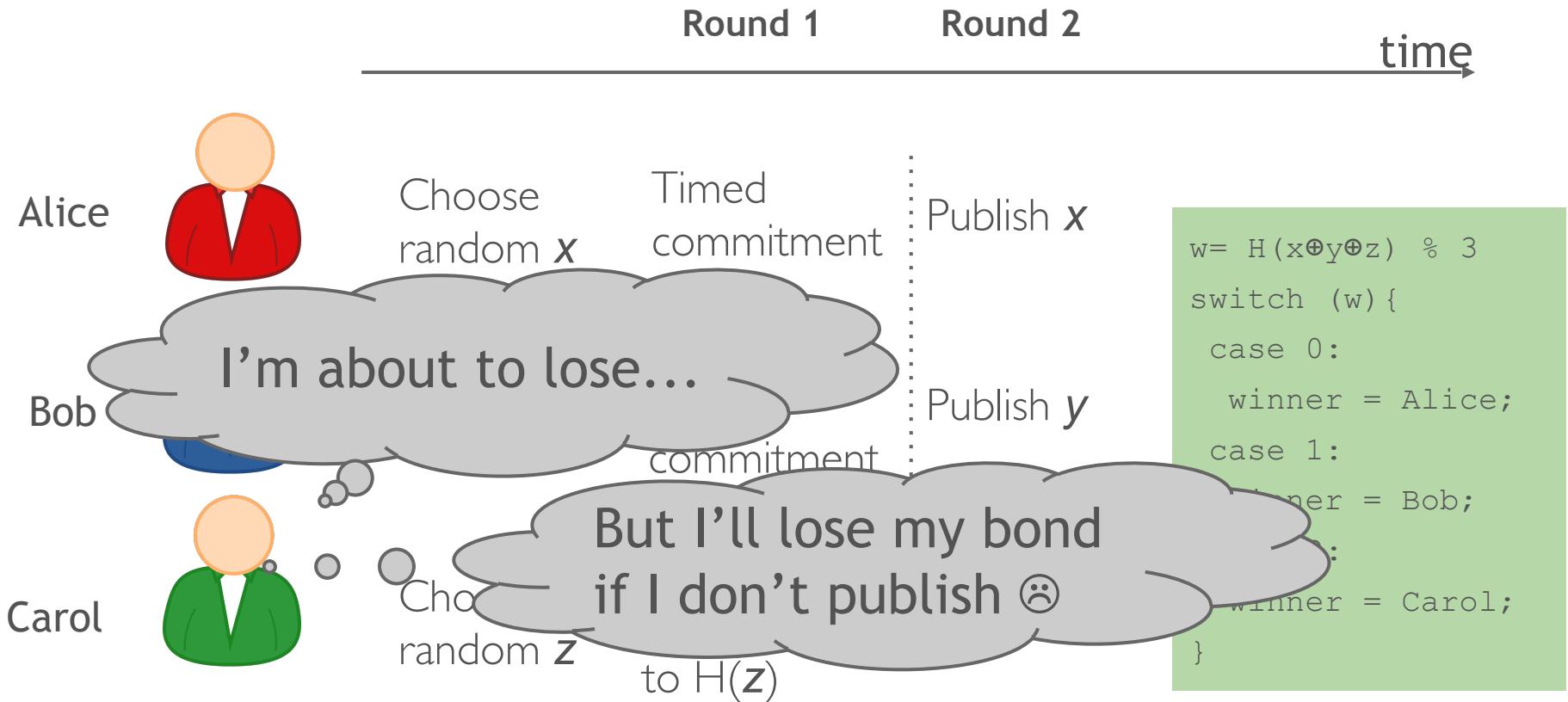


Timed hash commitments

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

Bitcoin as randomness source

Public randomness protocols

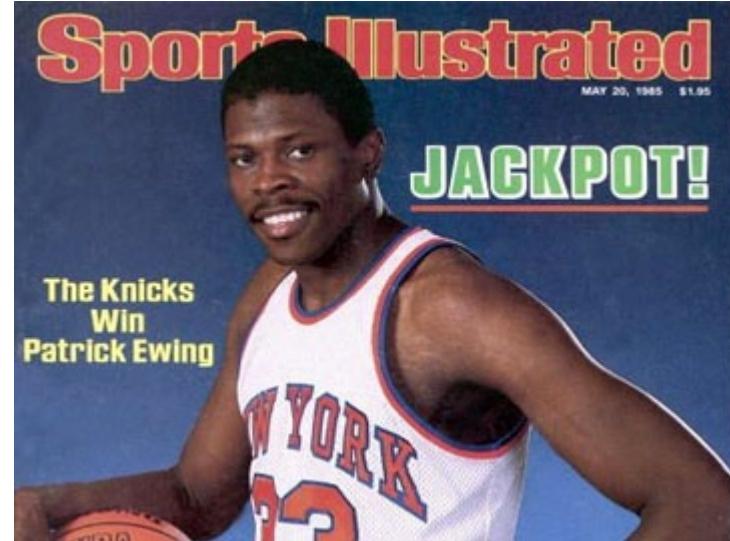
- Interactive coin-tossing protocols known in the literature
- “Non-interactive” source of convincing randomness?

NBA draft lottery



NBA Lottery 2014: Conspiracy Theories Plague Annual Event

By [Anthony Riccobono](#)  @tony_riccobono  a.riccobono@ibtimes.com
on May 20 2014 1:35 PM



1985: Knicks win rights to Patrick Ewing



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

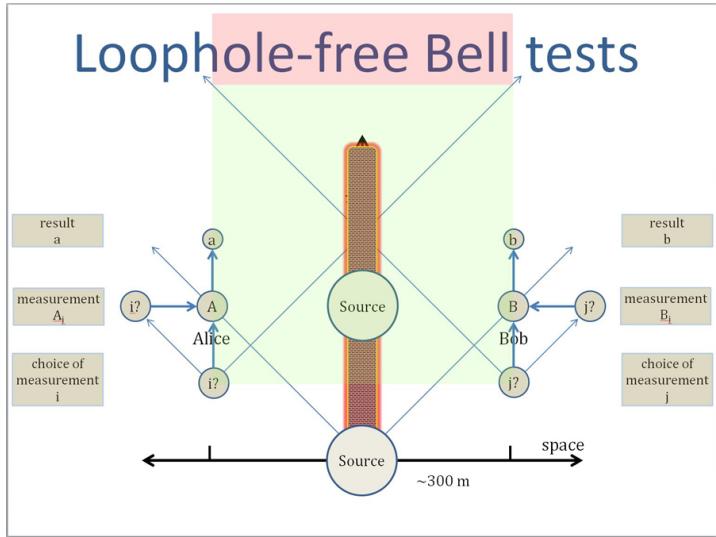


Pros: cheap, easy, simple to understand

Cons: must trust/audit operator

hard to trust remotely!

NIST beacon



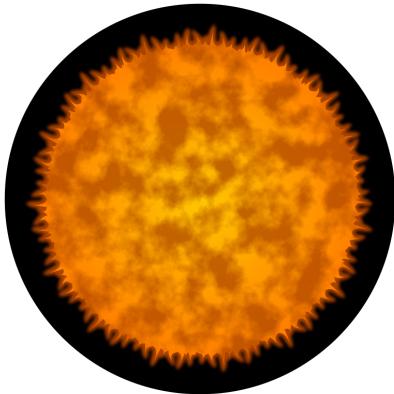
Beacon Record

Version:	Version 1.0
Frequency:	60 seconds
Time:	08/13/2014 12:36 pm (1407947760)
Seed Value:	27D7280A657B5E0A99721D47E21A2276C80B5CDFCA605E397D8BAA51C24A06 40C9C6E8B83BBB3D837011CA5B6CA08FADC78E2B8D36C75CC971757F82068A4
Previous Output:	2F2DE0662028D3C4D6F8DD7936262D9AFBDCFD0BD14BC733E257B14F48881A99 206BBC9429F09BFE719551EAB840CEE8157ACEABC80342CE4B66443C0859E216
Signature:	986C73CF88056635C5E0A018358D0D91CF10A2F2B16C8B8D91AA34B0A04D103B CFF347B714DAC343D5838E07FD0FC49BE6E398113500C0193D17CFE1BC4ED85B 7E3AC425EF7840E4E549D66D0F0FB383D09F290FDAEF2E520B8606A4F6C55FB 3B766CC9066494FAC1FE8983D58525224778F5AE3C3727FF0AC71DCE3B30E33B A6CFD767EE3D299A5324E371AFB49AEC46F88D60CAE6FCBF8B93D461B84C59CB 7577BE9A63FE0DB7C83944B545C501A4C787F87B15A0F8CFD8FB7FC191F677FB C4FB1C07E47C01B0D090BA5C564FEAFB0D0E24D90F01D2B2E66A31E7012CACD42 30EA94EF415C8F2B1751F09BD8255A2C142CE2C8C69587EE6CE788273E55AFAT
Output Value:	15E3B9DAA53DE7C20A60D3C2DECC2C6B2DB65FE07B1188D666A8A8476E4910F 592FB3F8049E4A01E5624FDF161A698EB0AA52515A79A46F3AFA1B8D7CEBB320
Status:	0: Normal

Pros: quantum-mechanical randomness

Cons: must trust NIST

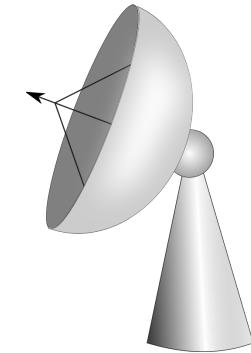
Natural phenomena



Sun spots



Weather

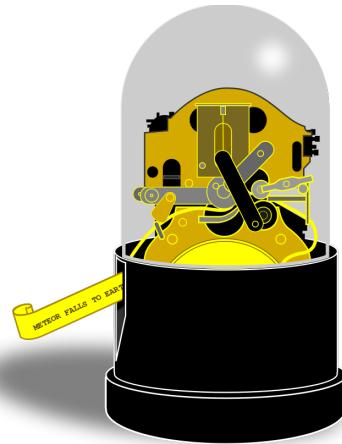


Cosmic background radiation

Pros: publicly observable, random

Cons: slow, need a trusted observer?

Stock-market beacon



61.230	0.472	-2.80%	N/A	0
61.8175	0.420	-1.53%	22.550	200
82.230	0.1325	-0.68%	30.400	200
16.370	1.250	-0.21%	N/A	0
39.500	0.340	-1.50%	N/A	0
62.748	0.340	-2.03%	16.310	600
1.570	0.412	-0.87%	38.900	3400
2.440	4.300	-0.65%	40.710	400
0.70	0.130	-0.96%	N/A	0
69	0.010	-0.80%	N/A	0
5	1.0331	-0.17%	6.080	12000
0.7825	0.7825	-1.55%	N/A	0
0.190	0.190	-2.15%	N/A	0
		-1.06%	12.200	17700
				80.3

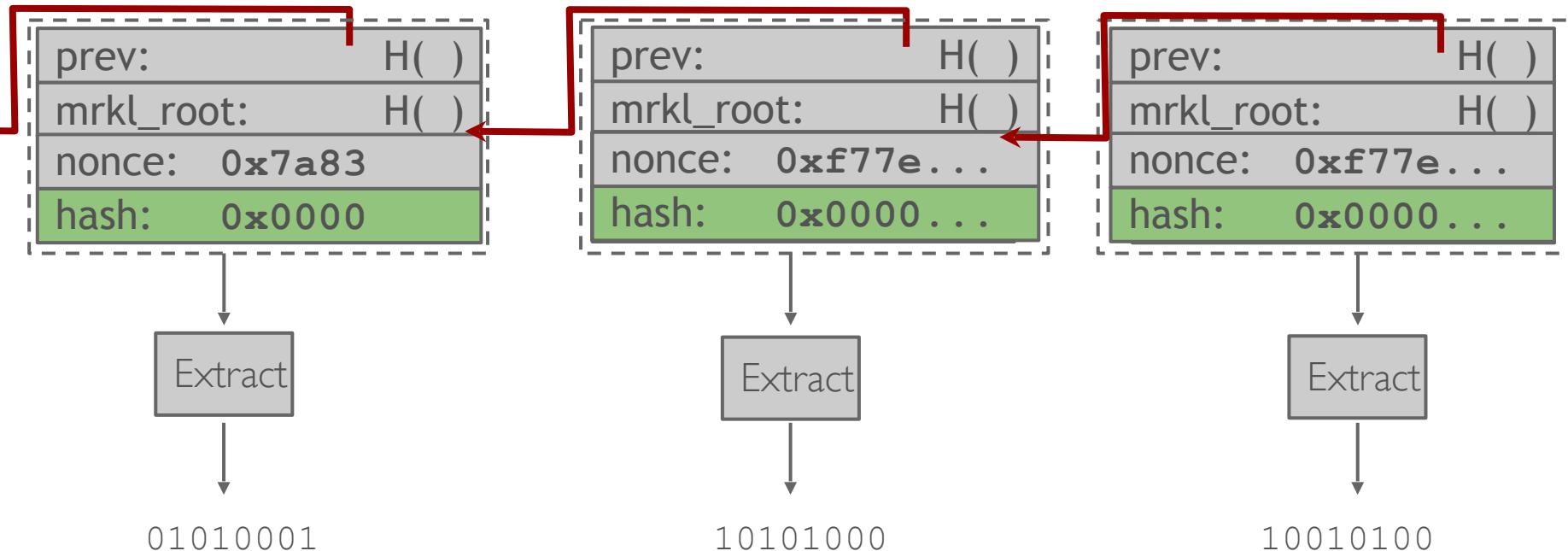
Pros: good randomness, costly to manipulate
Cons: slow, insider attacks?

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

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” 6.25 BTC

Cost of manipulation

Single coin flip: “secure” if wager is < 6.25 BTC

N -party lottery: “secure” if pool is < 6.25 $(n-1)$ BTC

Pros

- 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

