Bitcoin as a Platform

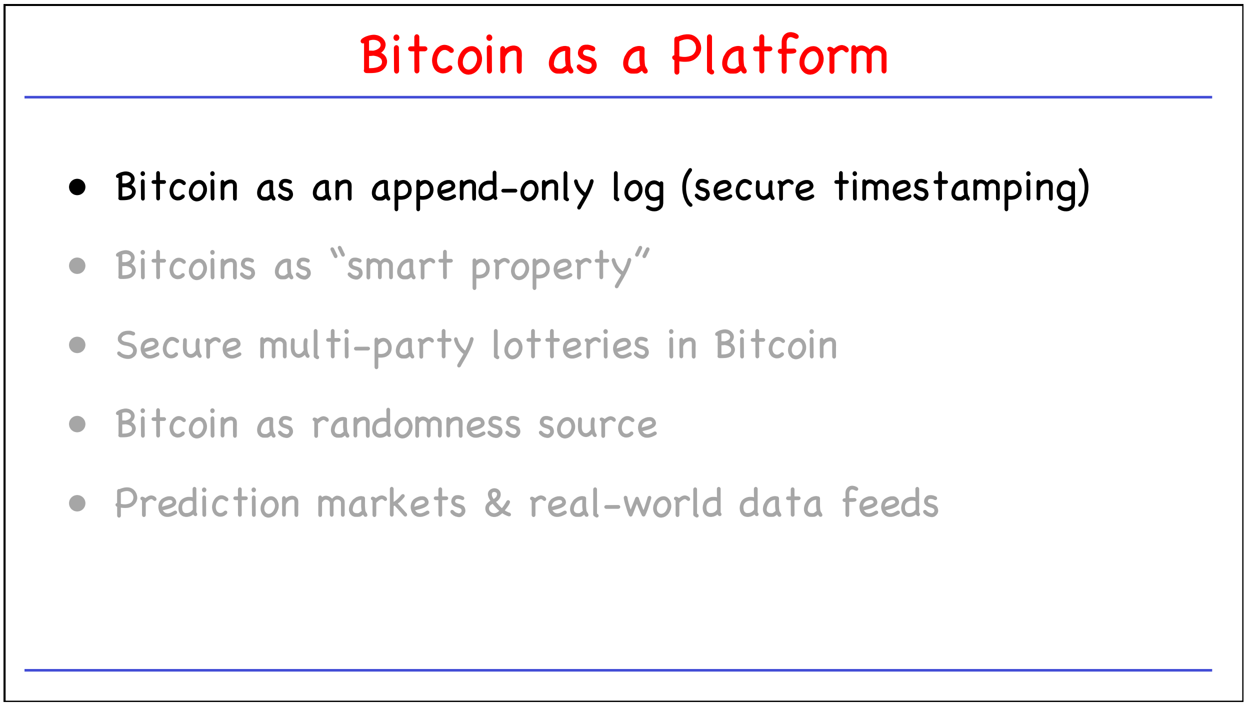
We have built Bitcoin. What can we build on top of it?

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

A fine stew o' ideas

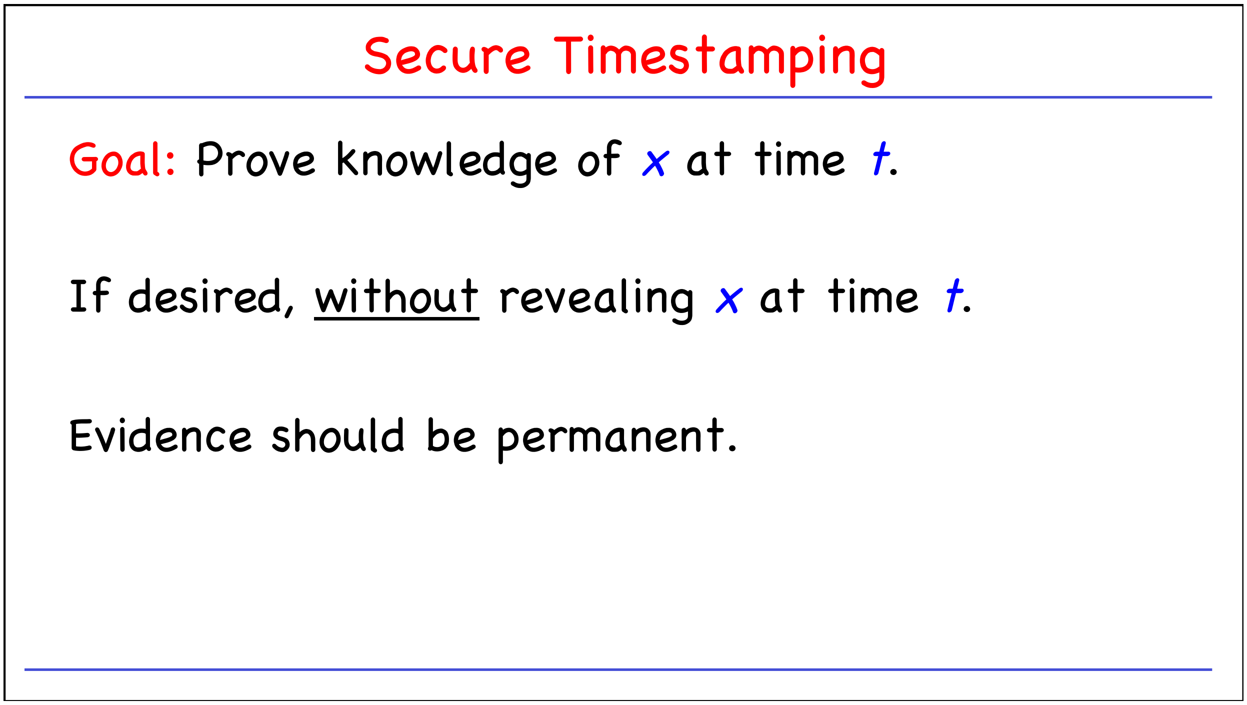
Bitcoin as a Platform

- Bitcoin as an append-only log (secure timestamping)
- Bitcoins as "smart property"
- Secure multi-party lotteries in Bitcoin
- Bitcoin as randomness source
- Prediction markets & real-world data feeds



Bitcoin as a Platform

- Bitcoin as an append-only log (secure timestamping)
- Bitcoins as "smart property"
- Secure multi-party lotteries in Bitcoin
- Bitcoin as randomness source
- Prediction markets & real-world data feeds



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.

We cannot find an x' != x later s.t. $H(x') = H(x)$

$H(x)$ reveal no information* about x

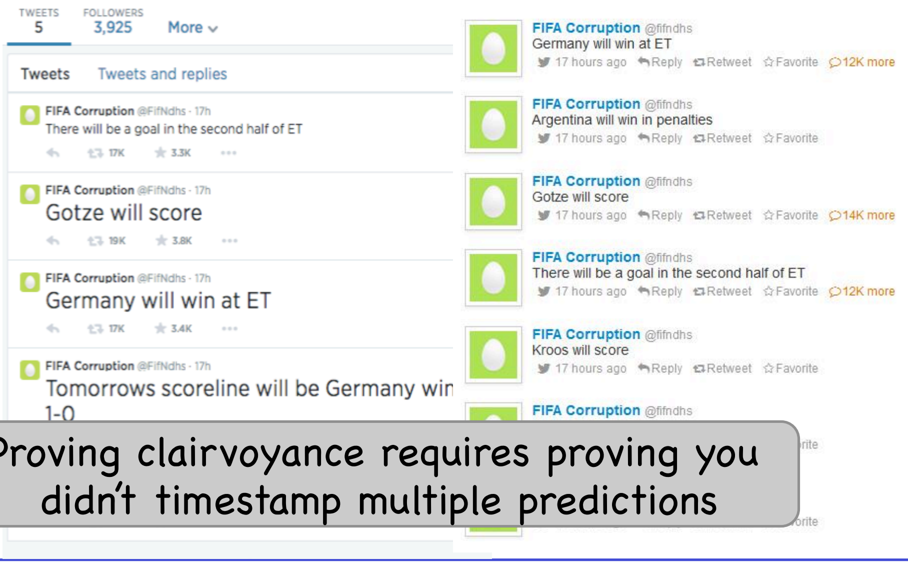
(*) assuming the space of possible x is big

Recall also: We can publish a commitment to x now and reveal x later.

Applications for Secure Timestamping

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

Non-Application: Proof of Clairvoyance



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

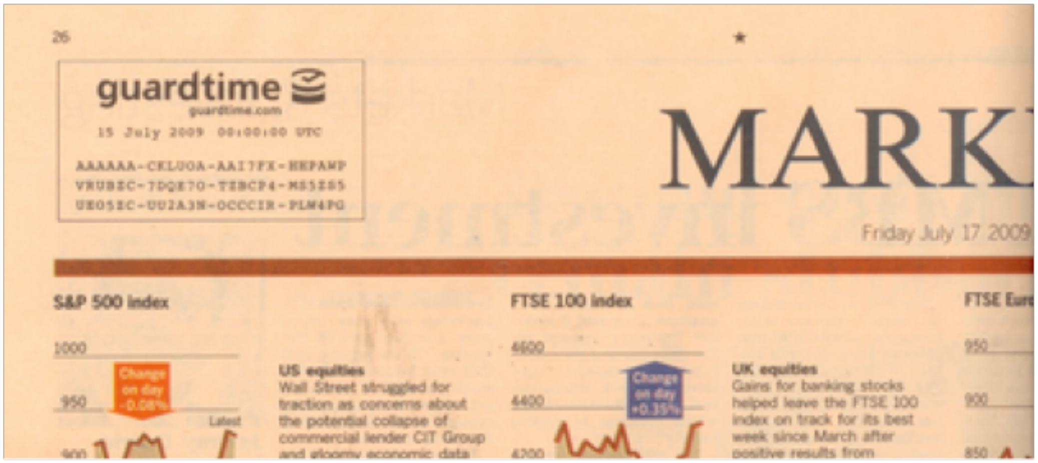
FIFA Corruption @fifndhs
Kroos will score
17 hours ago Reply Retweet Favorite

FIFA Corruption @fifndhs

Proof that FIFA is corrupt??

Proving clairvoyance requires proving you didn't timestamp multiple predictions

Offline Solution: Newspaper Timestamp



26

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

AAAAAA-CKLUOA-AAI7FX-HEPAWP
VRUBZC-7DQE7O-TEBCP4-MS5Z85
UE05ZC-UU2A3N-OCCCIR-PLM4PG

MARK

Friday July 17 2009

S&P 500 index

FTSE 100 index

FTSE Eur

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

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

Idea: Brute-force a public key & signature starting with the first n bits of your data hash.
[Cark, Essex 2012]

Pros: compatible, “invisible”, no UTXO bloat.

Cons: expensive, low data rate

Provably unspendable Commitments

```
OP_RETURN
<arbitrary data>
```

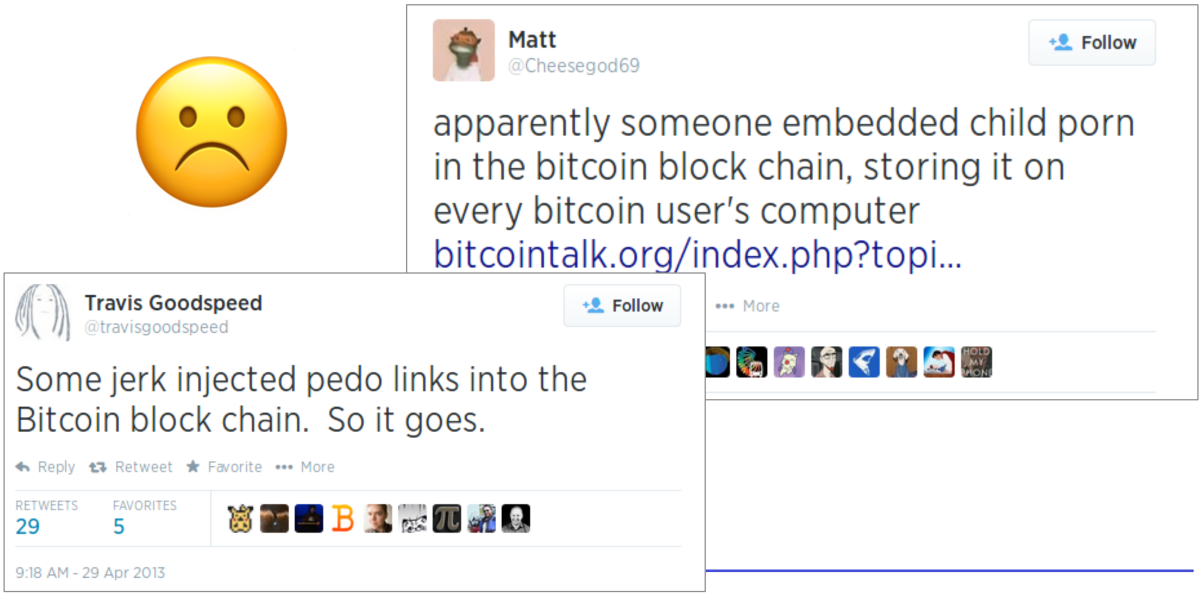
Pros: cheap, no UTXO bloat.

Cons: not a standard transaction

Data Rates

- 40-byte commitments for 1 TX fee
  - 0.00005 BTC (Spring 2017, US$0.05)
- Enough to commit to the hash of whatever you want!

Block Chain Poisoning



Matt
@Cheesegod69

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

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

RETWEETS	FAVORITES
29	5

9:18 AM - 29 Apr 2013

Puzzles (recap)

Incentive system steers participants

Basic features of Bitcoin's puzzle:

The puzzle is difficult to solve, so attacks are costly

… but not too hard, so honest miners are compensated

Q: What other features could a puzzle have?

Can we prevent Poisoning

- In general, no ☹️
- Pay-to-script-hash makes it a bit more expensive
- Food-for-thought: Can miners refuse to include "poison" transactions?

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

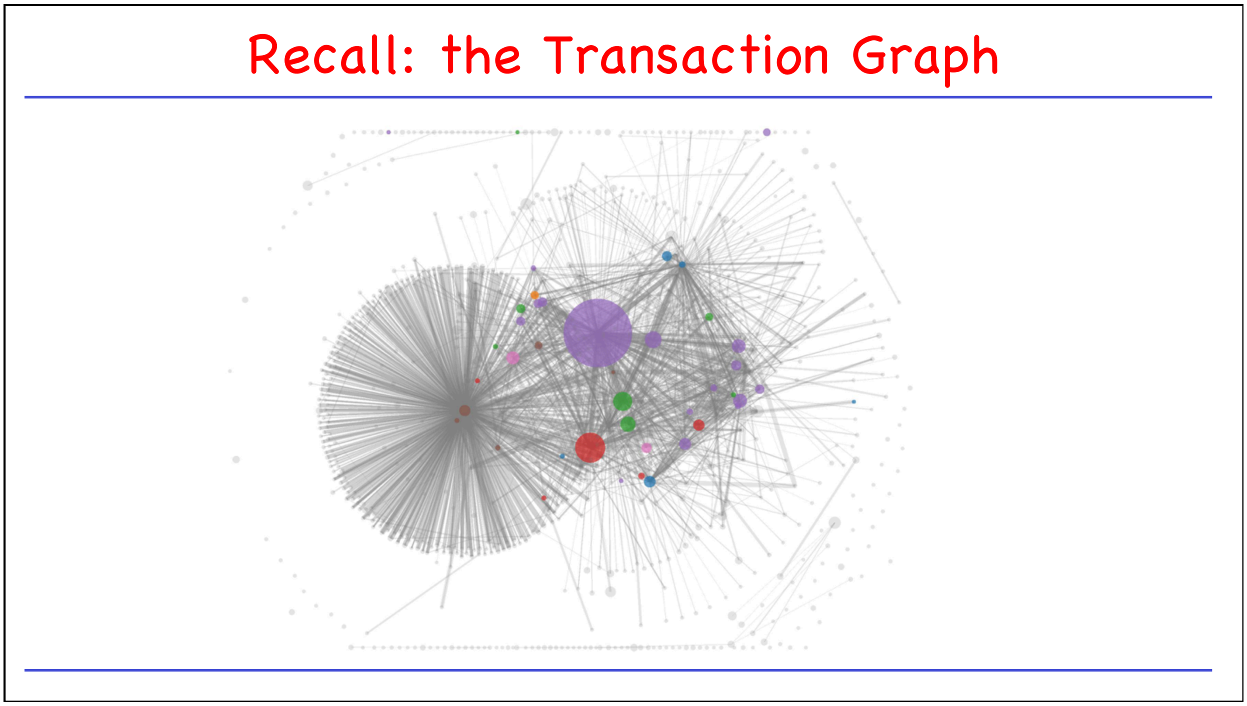
- Smart property, smart contracts
- User-defined currency

Pros: more features, faster development.

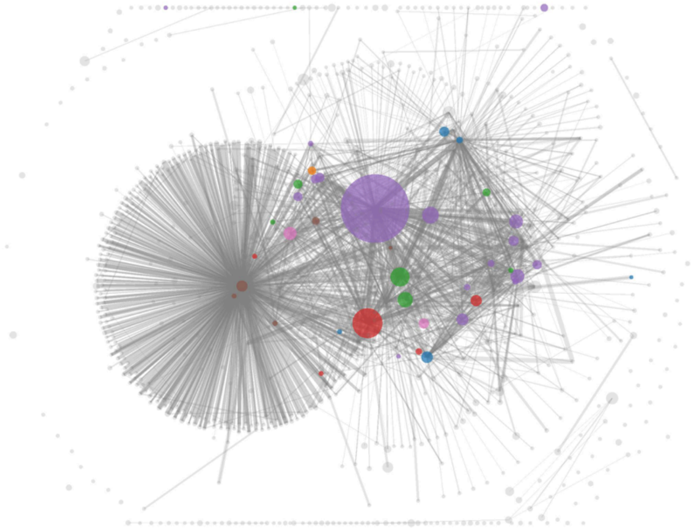
Cons: reliant on Bitcoin, can be inefficient.

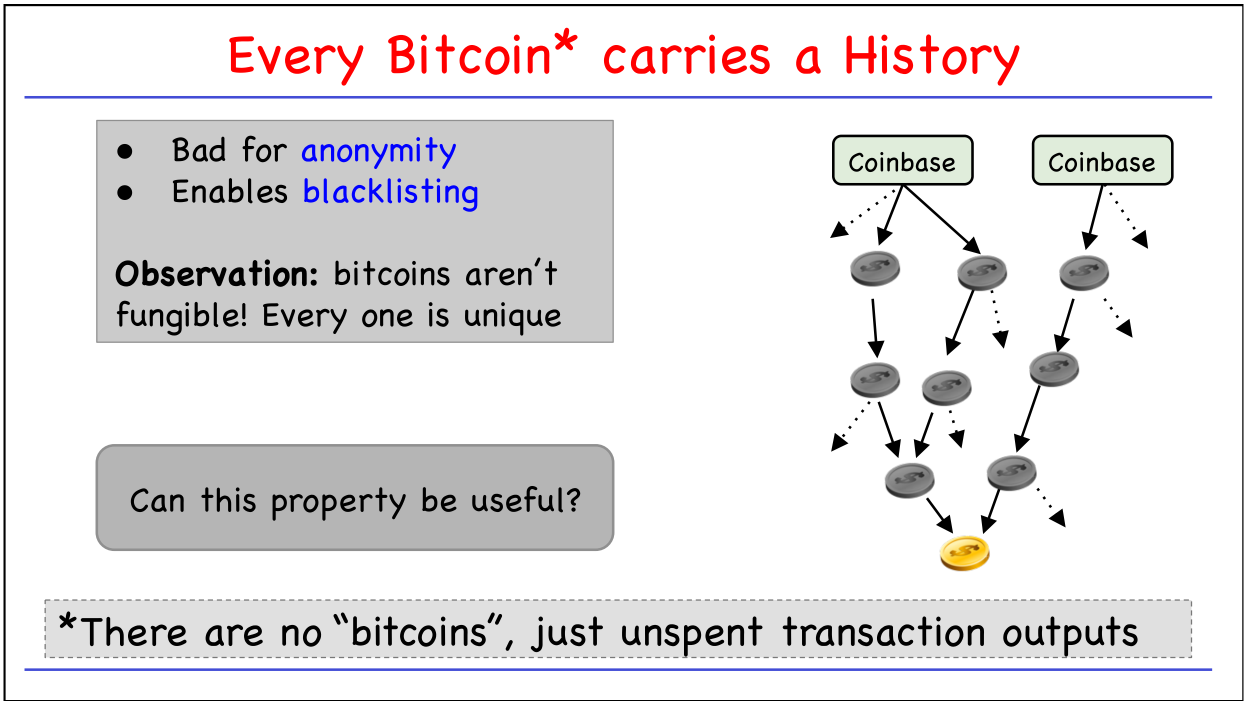
Bitcoin as a Platform

- Bitcoin as an append-only log (secure timestamping)
- Bitcoins as "smart property"
- Secure multi-party lotteries in Bitcoin
- Bitcoin as randomness source
- Prediction markets & real-world data feeds



Recall: the Transaction Graph



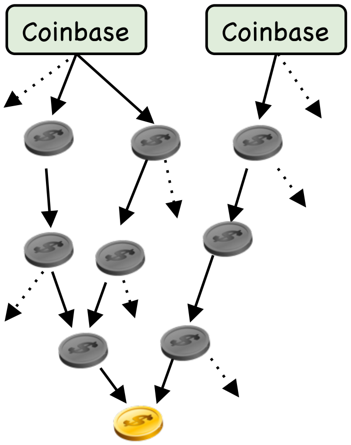


Every Bitcoin* carries a History

- 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 transaction outputs

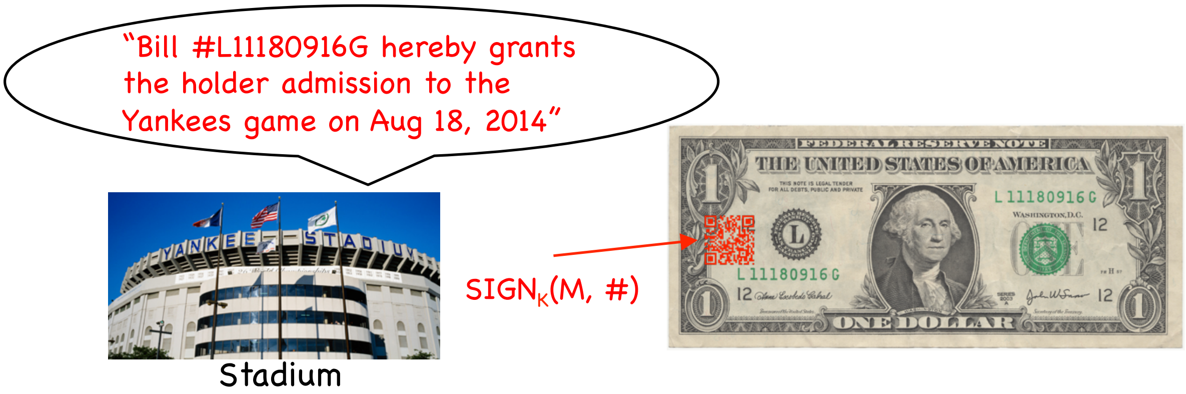
Adding Metadata to Currency

HAWAII
NOT TO BE USED FOR BRIBING POLITICIANS
THIS IS $1 MORE THAN BANK OF AMERICA PAID IN TAXES!!

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

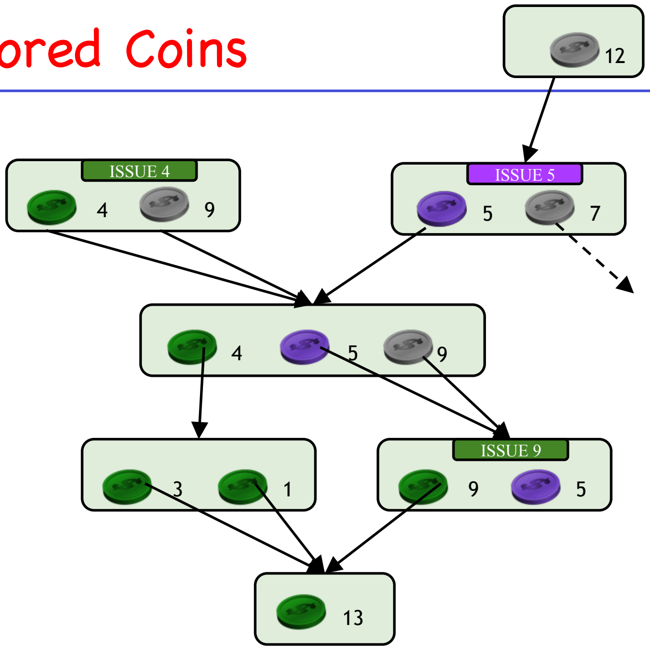
$\text{SIGN}_K(M, \#)$

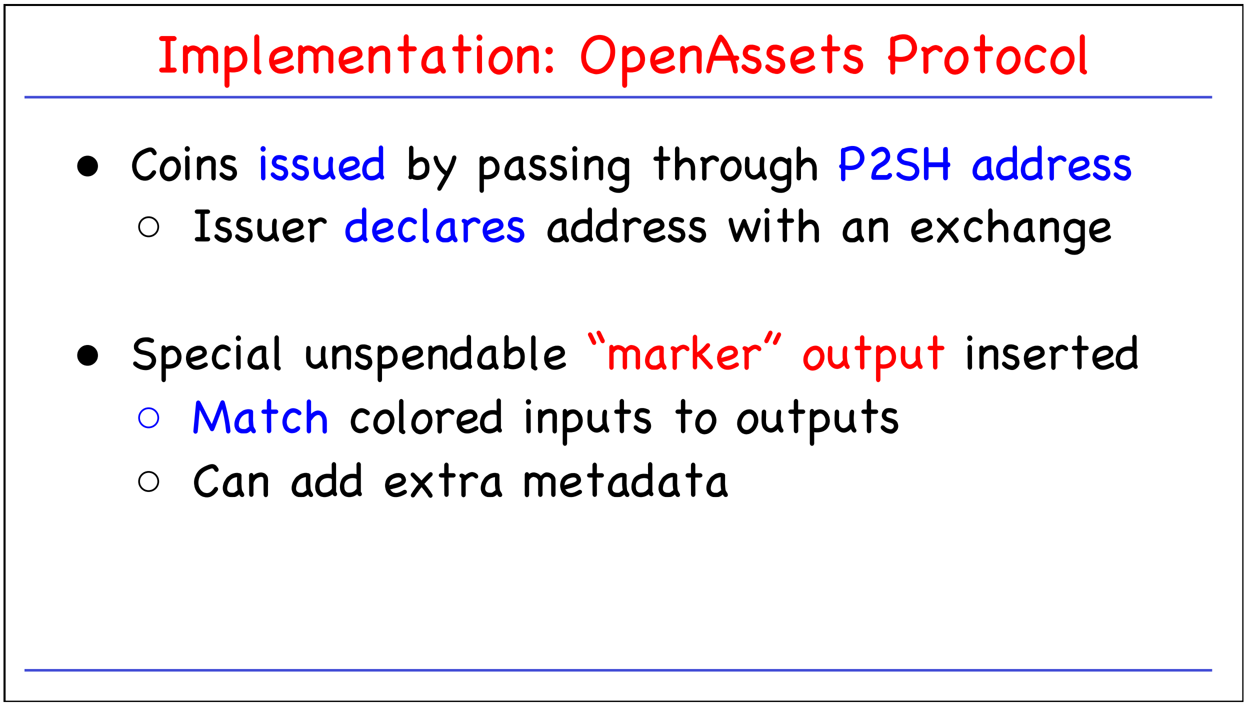
Authenticated Metadata for Currency

- 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?

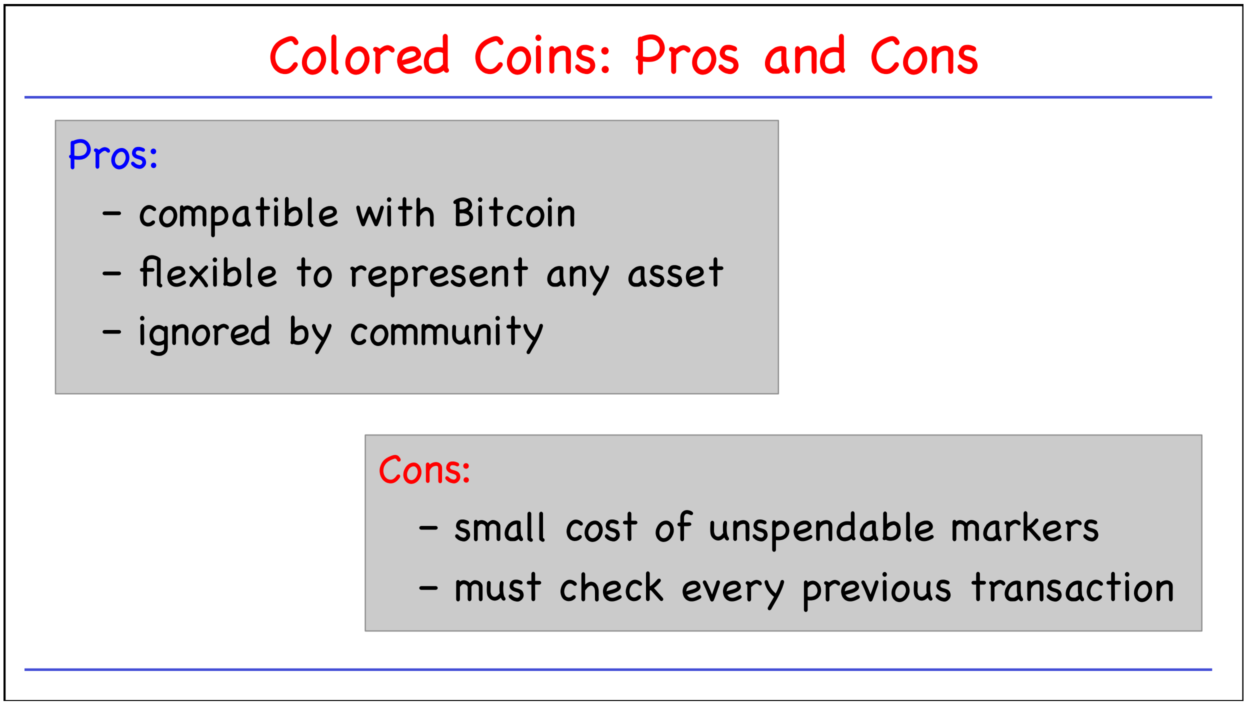
Colored Coins





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



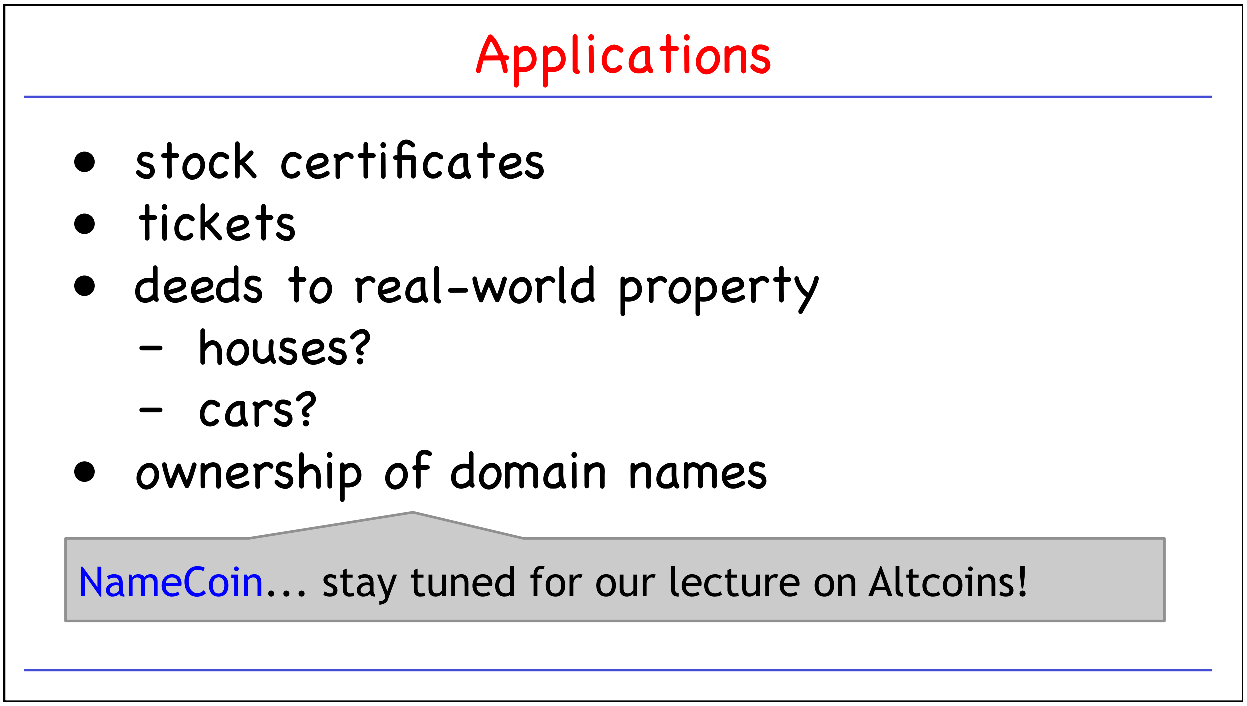
Colored Coins: Pros and Cons

Pros:

- compatible with Bitcoin
- flexible to represent any asset
- ignored by community

Cons:

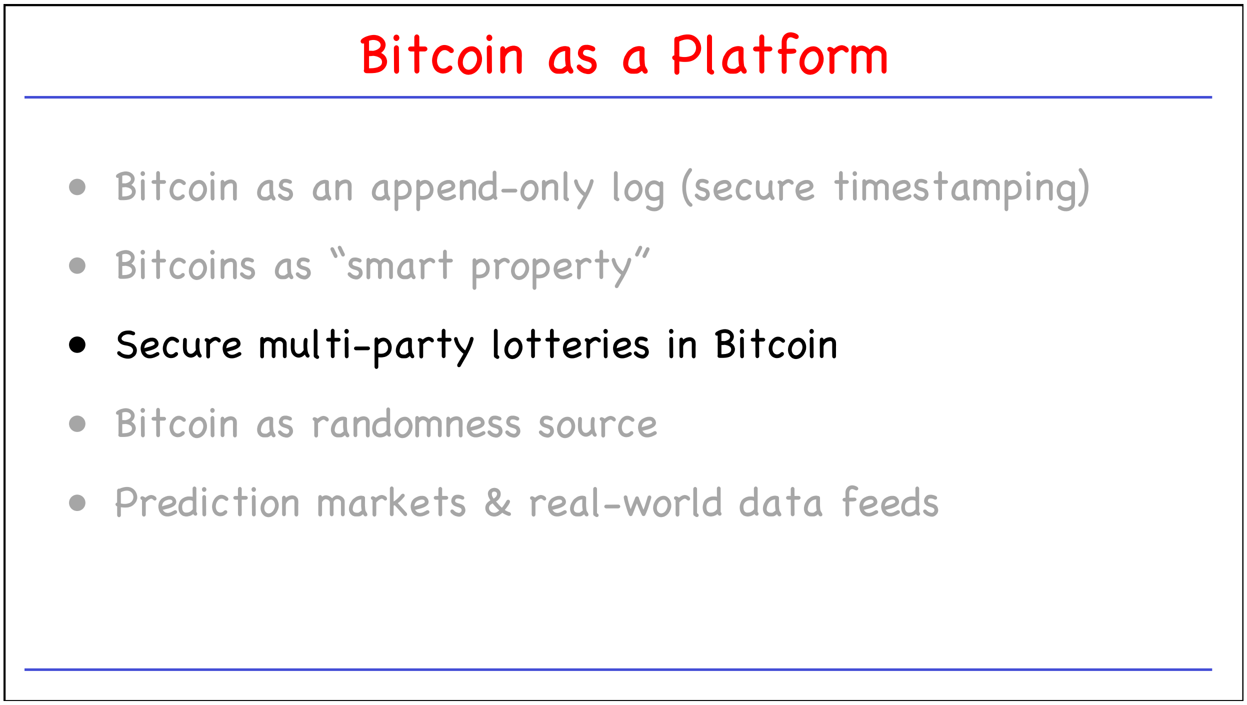
- small cost of unspendable markers
- must check every previous transaction



Applications

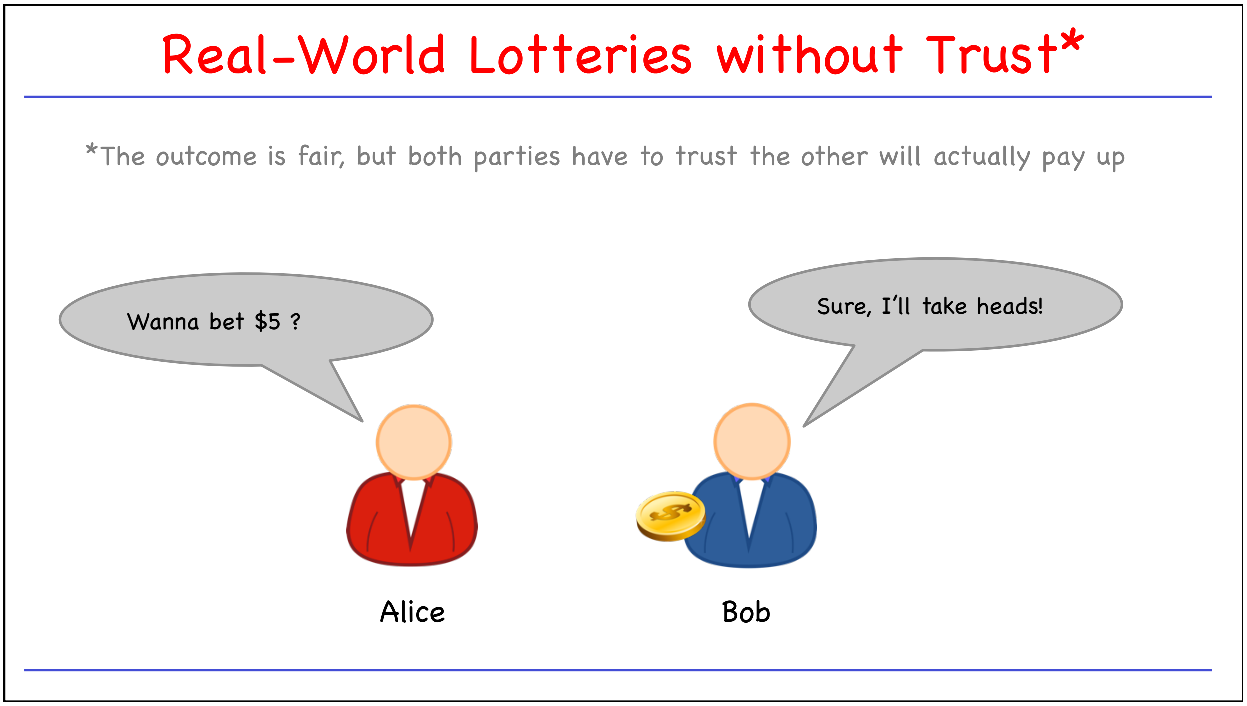
- stock certificates
- tickets
- deeds to real-world property
  - houses?
  - cars?
- ownership of domain names

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



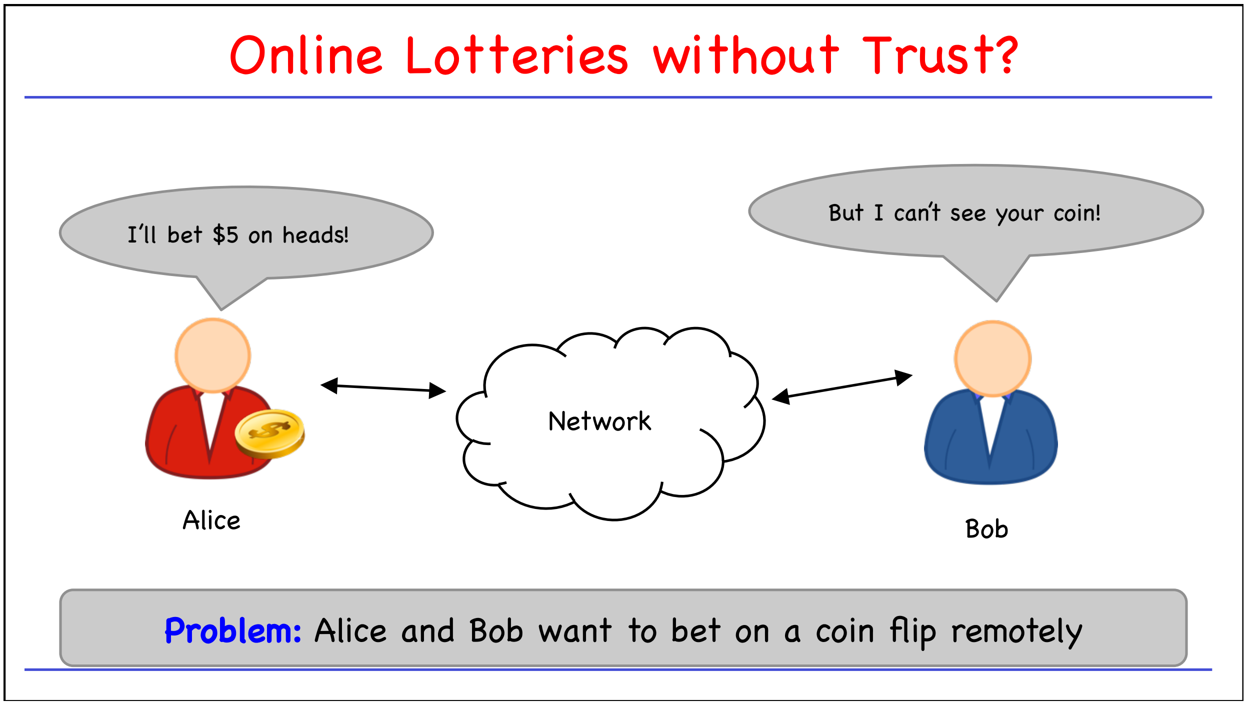
Bitcoin as a Platform

- Bitcoin as an append-only log (secure timestamping)
- Bitcoins as "smart property"
- Secure multi-party lotteries in Bitcoin
- Bitcoin as randomness source
- Prediction markets & real-world data feeds



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 (again)

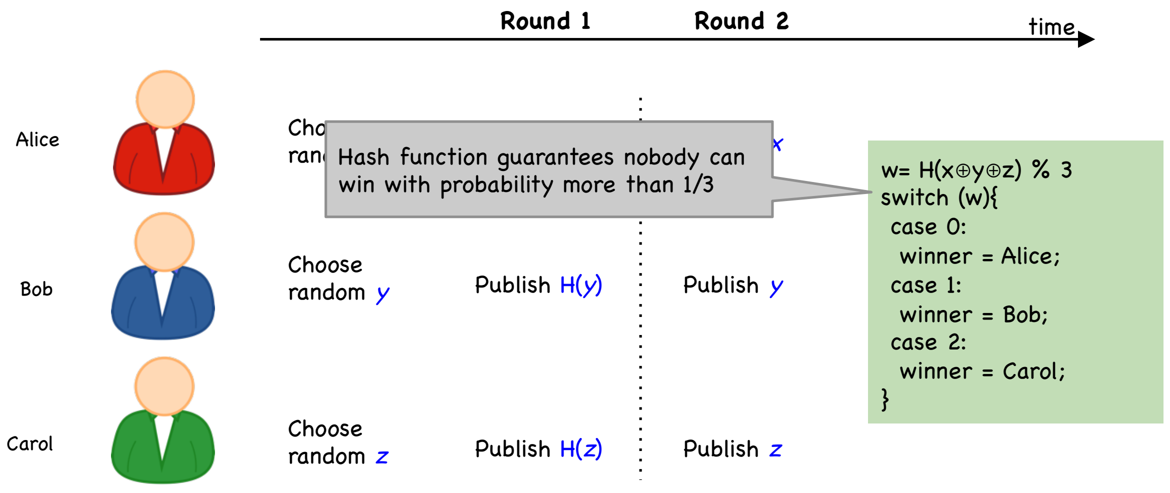
Recall: Publishing $H(x)$ is a commitment to x.

We cannot find an $x' \mathrel{!=} x$ later s.t. $H(x') = H(x)$

$H(x)$ reveal no information* about x

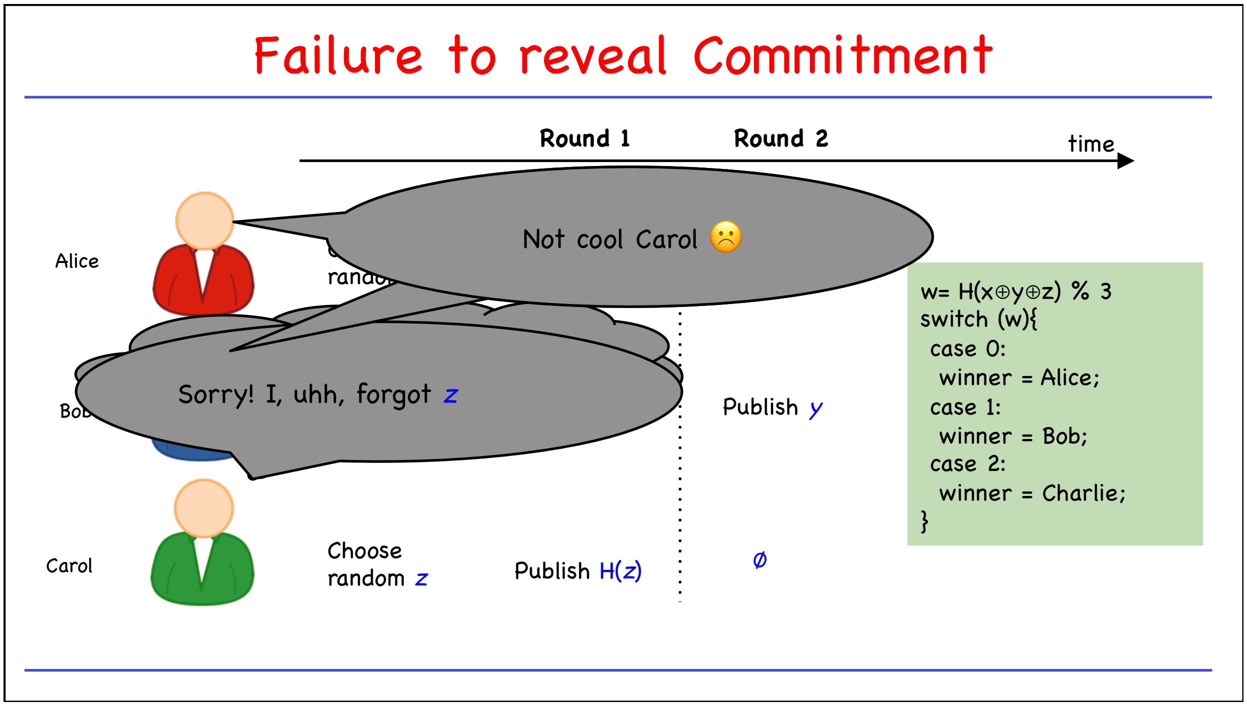
(*) assuming the space of possible x is big

A Lottery with Hash Commitments



Hash function guarantees nobody can win with probability more than 1/3

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



Failure to reveal Commitment

Round 1

Round 2

time

Alice

rando

Not cool Carol ☹

Bob

Sorry! I, uhh, forgot *z*

Publish *y*

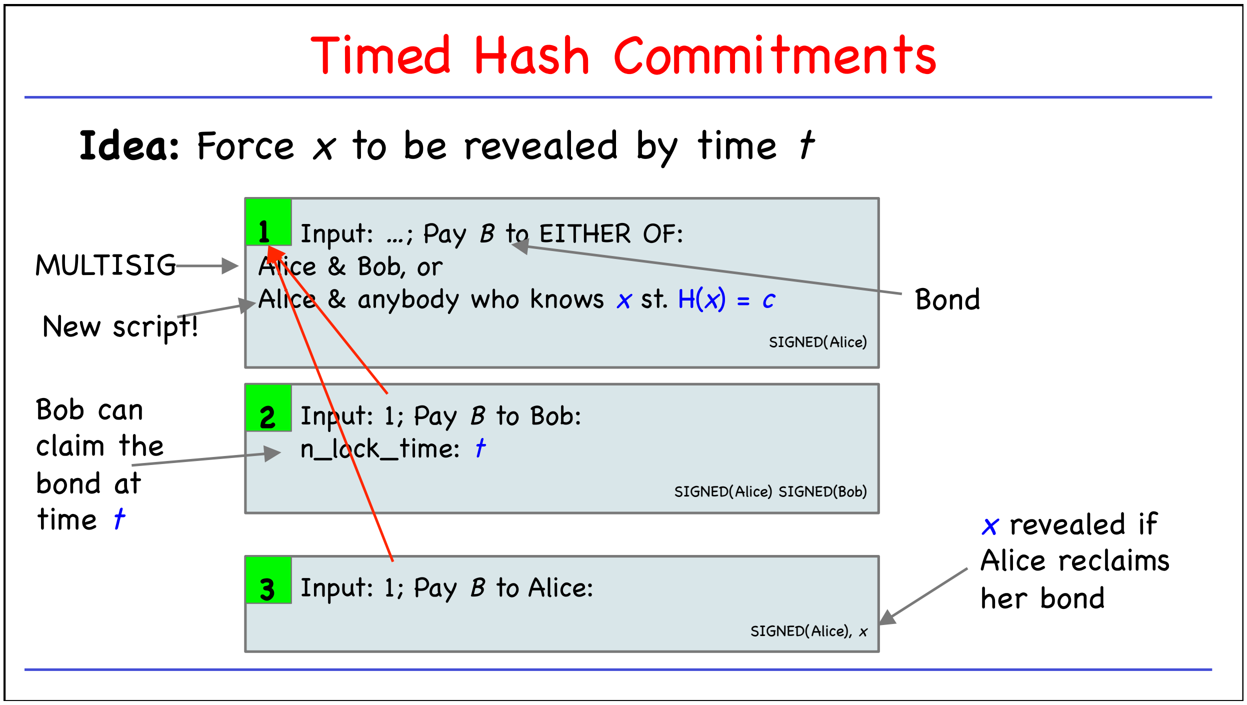
Carol

Choose random *z*

Publish H(*z*)

∅

```
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*

1 Input: …; Pay *B* to EITHER OF:
Alice & Bob, or
Alice & anybody who knows *x* st. H(*x*) = *c*
SIGNED(Alice)

2 Input: 1; Pay *B* to Bob:
n_lock_time: *t*
SIGNED(Alice) SIGNED(Bob)

3 Input: 1; Pay *B* to Alice:
SIGNED(Alice), *x*

MULTISIG

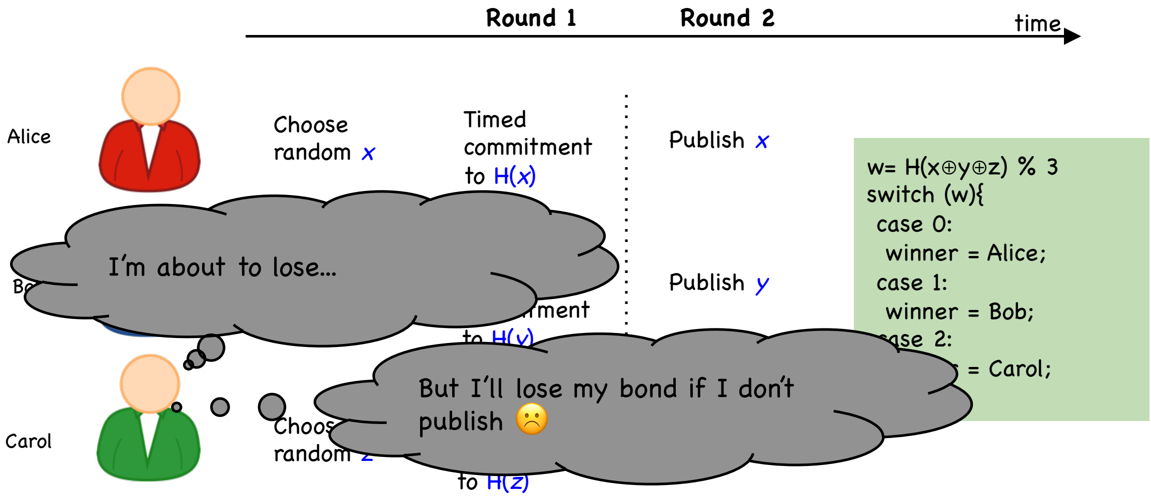
New script!

Bond

Bob can claim the bond at time *t*

x revealed if Alice reclaims her bond

Lottery with timed Commitments



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

Lottery with timed Commitments: Pros and Cons

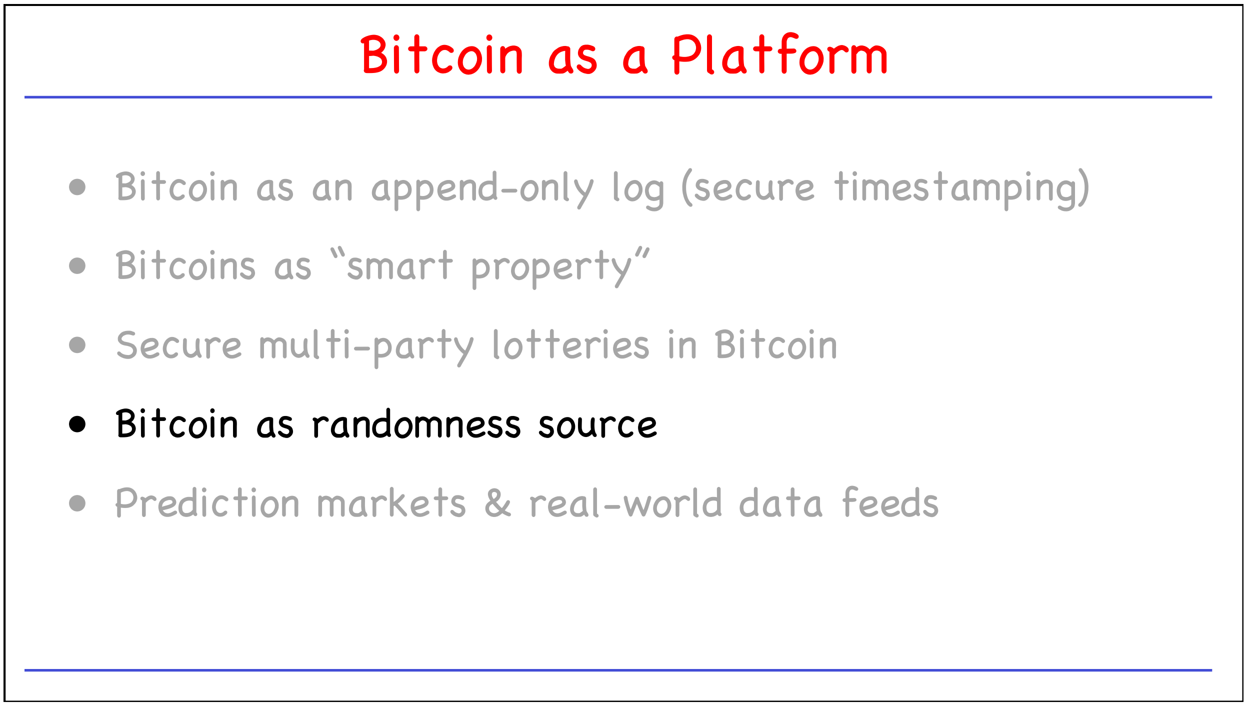
Pros:

- can be implemented on Bitcoin today

  (e.g. Andrychowicz, Dziembowski, Malinowski, Mazurek, 2014)

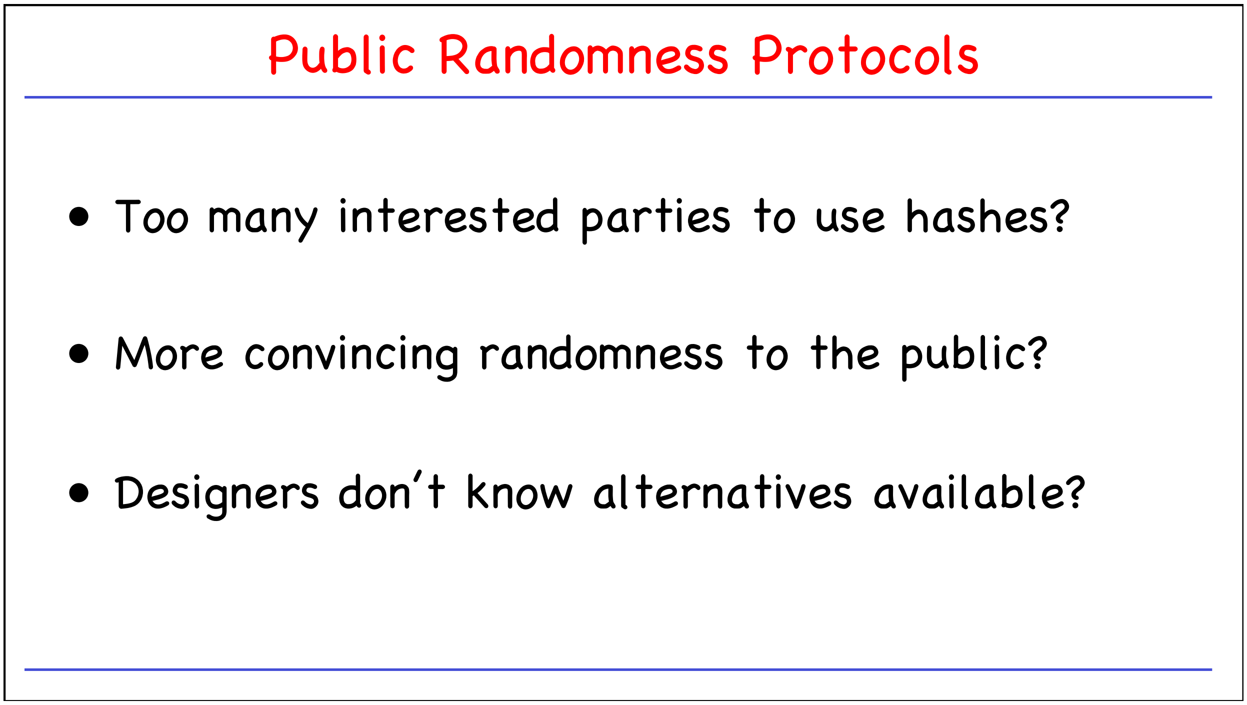
Cons:

- complexity is O(N2)
- bonds must be higher than amount bet
- griefers(*) still might shut down large pools



Bitcoin as a Platform

- Bitcoin as an append-only log (secure timestamping)
- Bitcoins as “smart property”
- Secure multi-party lotteries in Bitcoin
- Bitcoin as randomness source
- Prediction markets & real-world data feeds



Public Randomness Protocols

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

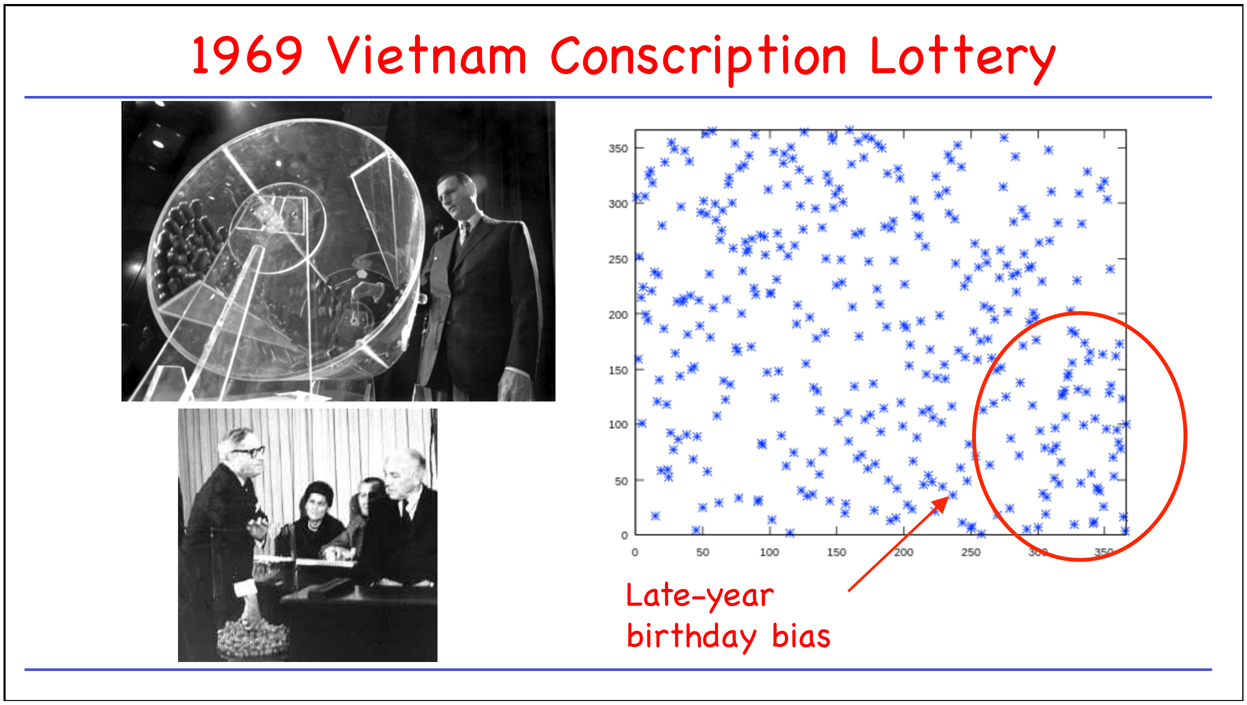
NBA Draft Lottery

INTERNATIONAL BUSINESS TIMES

NBA Lottery 2014: Conspiracy Theories Plague Annual Event

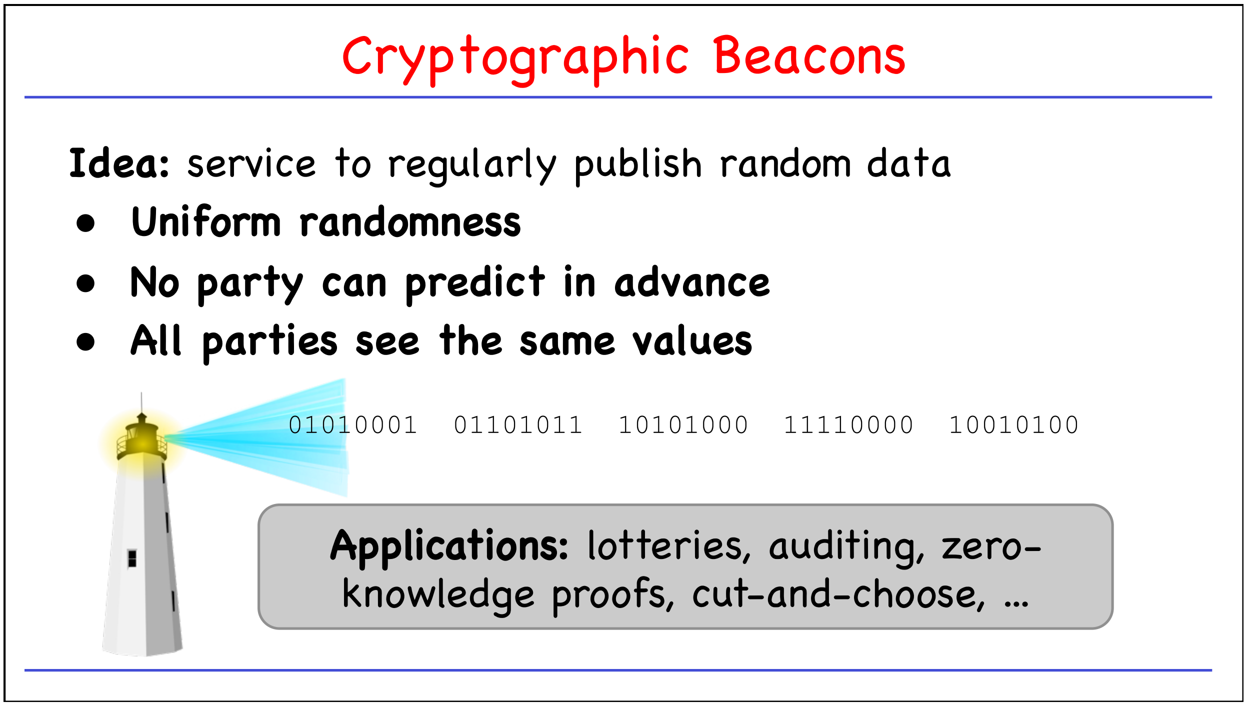
By Anthony Riccobono @tony_riccobono a.riccobono@ibtimes.com
on May 20 2014 1:35 PM

1985: Knicks win rights to Patrick Ewing



1969 Vietnam Conscription Lottery

Late-year birthday bias



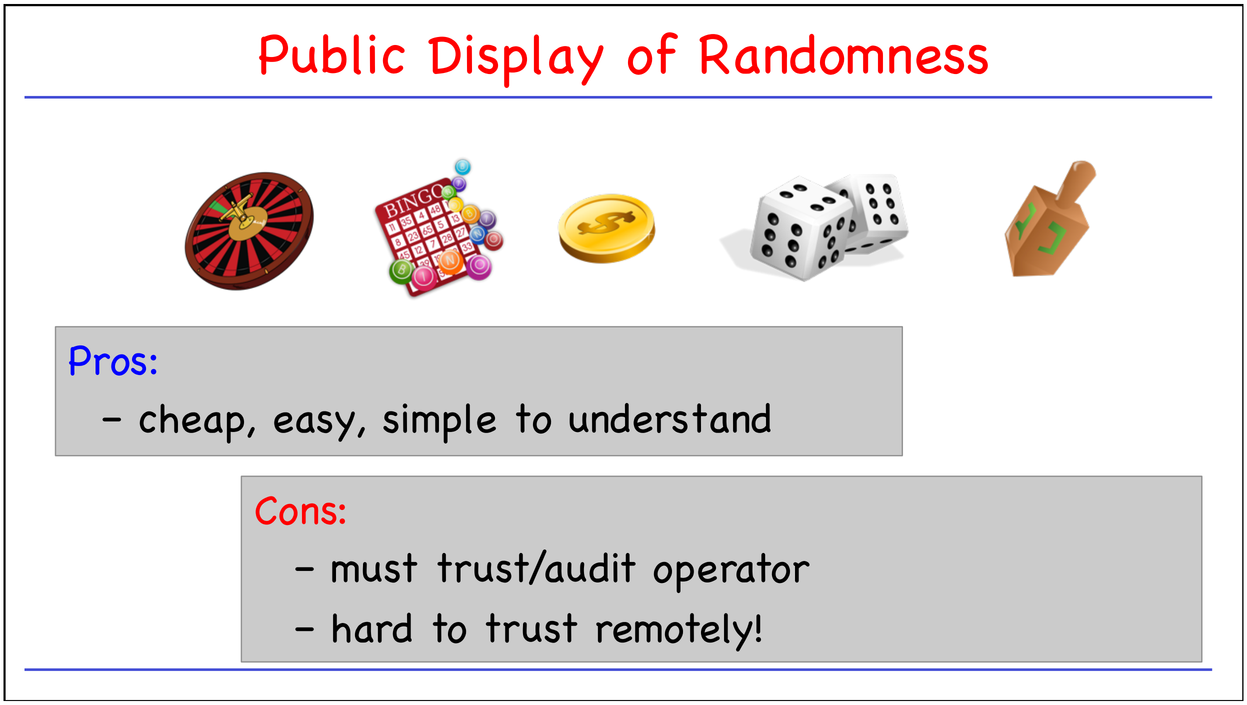
Cryptographic Beacons

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

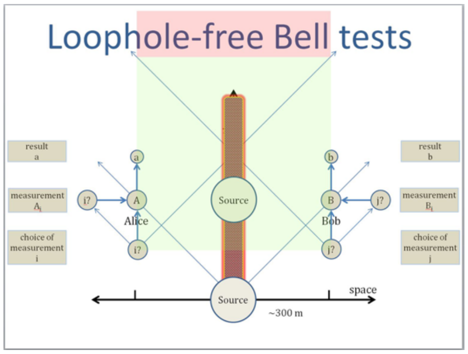
Pros:

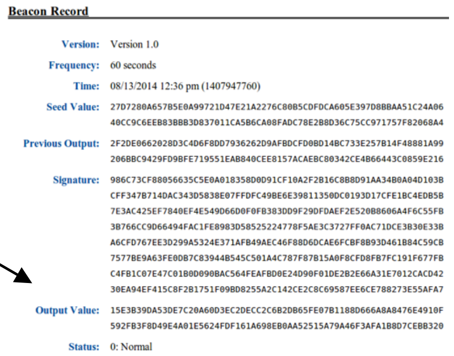
- cheap, easy, simple to understand

Cons:

- must trust/audit operator
- hard to trust remotely!

NIST Beacon





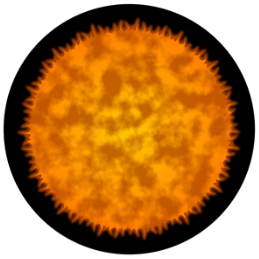
Beacon Record

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
3B766CC9D66494FAC1FE8983D5852522477 8F5AE3C3727FF0AC71DCE3B30E33B
A6CFD767EE3D299A5324E371AFB49AEC46F88D6DCAE6FCBF8B93D461B84C59CB
7577BE9A63FE0DB7C83944B545C501A4C787F87B15A0F8CFD8FB7FC191F677FB
C4FB1C07E47C01B0D090BAC564FEAFBD0E24D90F01DE2B2E66A31E7012CACD42
30EA94EF415C8F2B1751F09BD8255A2C142CE2C8C69587EE6CE788273E55AFA7
Output Value: 15E3B39DA53DE7C20A60D3EC2DECC2C6B2DB65FE07B1188D666A8A8476E4910F
592FB3F8D49E4A01E5624FDF161A698EB0AA52515A79A46F3AFA1B8D7CEBB320
Status: 0: Normal

Pros: quantum-mechanical randomness

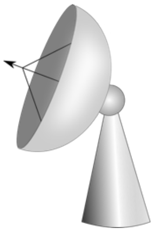
Cons: must trust NIST

Natural Phenomena



Sun spots

Weather

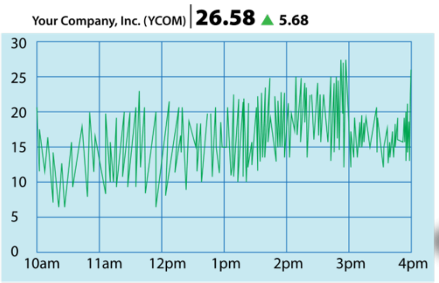


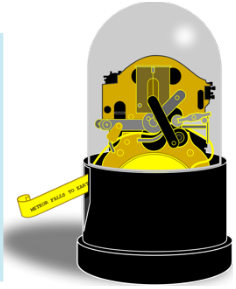
Cosmic background radiation

Pros: publicly observable, random

Cons: slow, need a trusted observer?

Stock-market Beacon





Pros: good randomness, costly to manipulate

Cons: slow, insider attacks?

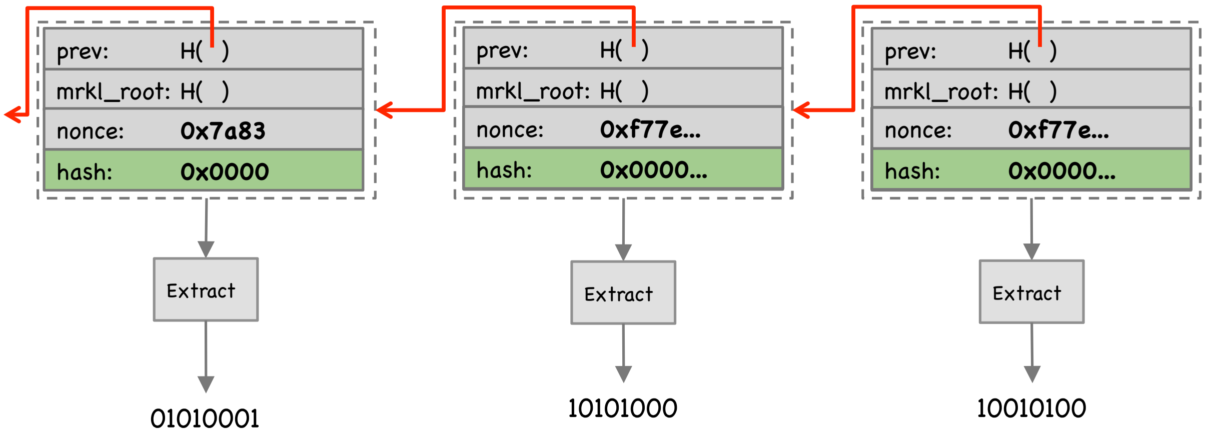
Why not use the Block Chain?

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



prev:	H( )
mrkl_root:	H( )
nonce:	0x7a83
hash:	0x0000

Extract

01010001

prev:	H( )
mrkl_root:	H( )
nonce:	0xf77e...
hash:	0x0000...

Extract

10101000

prev:	H( )
mrkl_root:	H( )
nonce:	0xf77e...
hash:	0x0000...

Extract

10010100

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" 12.5 BTC

Cost of Manipulation

Single coin flip: secure wager is < 12.5 BTC

N-party lottery: secure if pool is < 12.5 (n-1) BTC

Pros and Cons

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 (not synchronized with real time)
- Need to delay to insure against forks
- Manipulation may be too cheap for some applications.

Built-in Beacon Support in Scripts

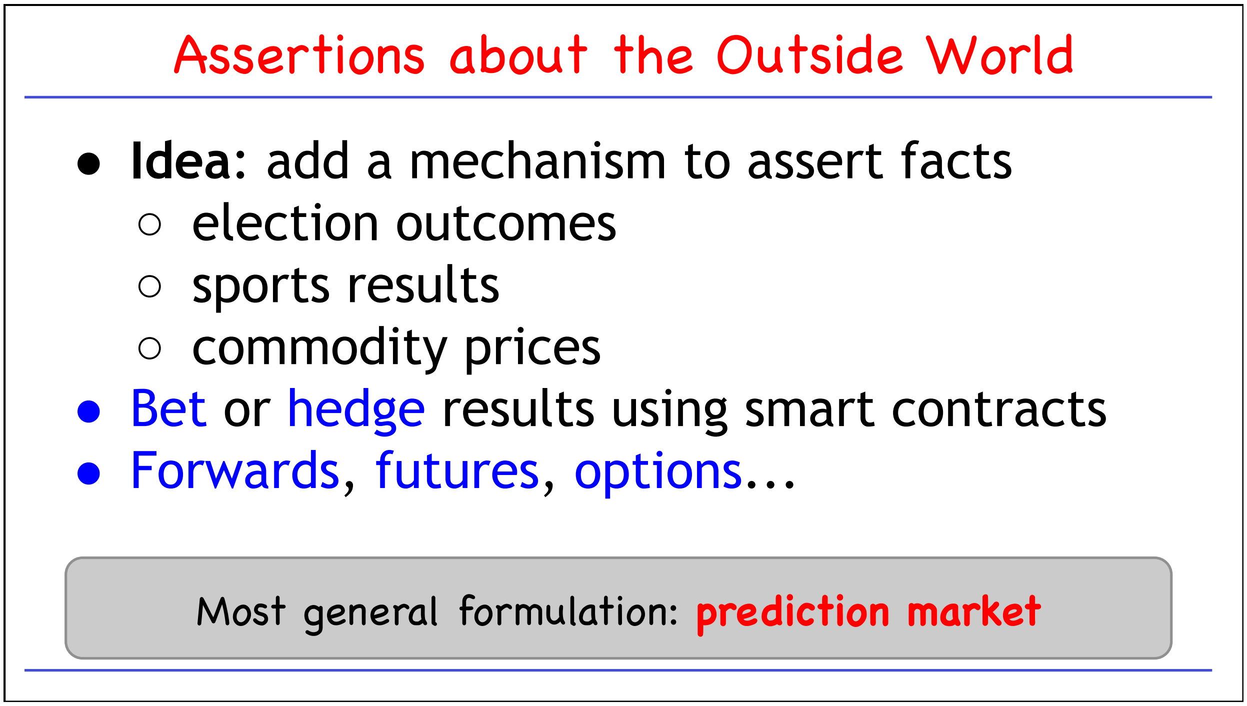
Idea: Add an opcode for a beacon call.

Can build multi-party lotteries

- ○ only one round
- ○ no bonds
- ○ no time delay for refunds

Bitcoin as a Platform

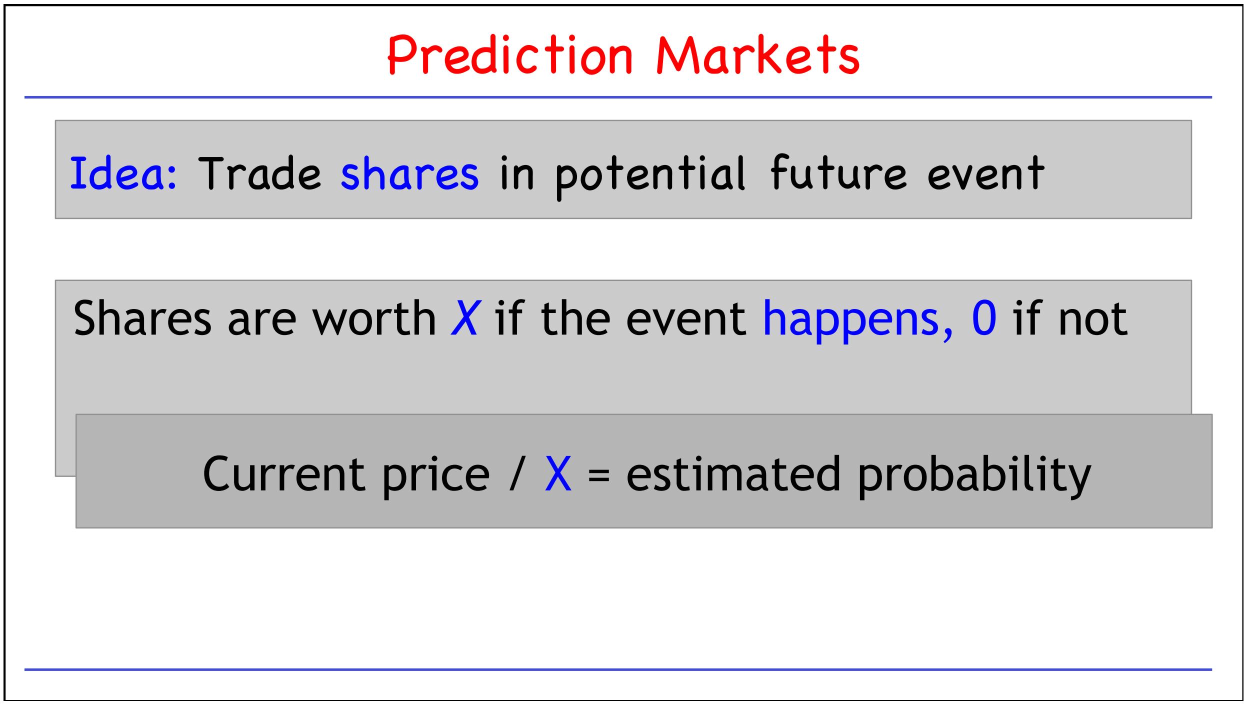
- Bitcoin as an append-only log (secure timestamping)
- Bitcoins as "smart property"
- Secure multi-party lotteries in Bitcoin
- Bitcoin as randomness source
- Prediction markets & real-world data feeds



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 potential future event

Shares are worth *X* if the event happens, 0 if not

Current price / X = estimated probability

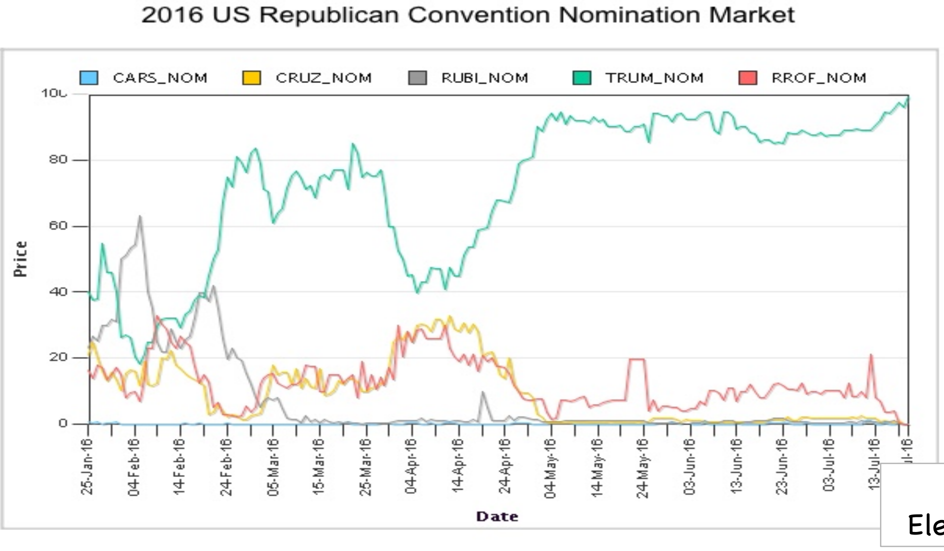
Example: World Cup 2014

	DEUTSCHER FUSSBALL-BUND	AFA	CBF	US	
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

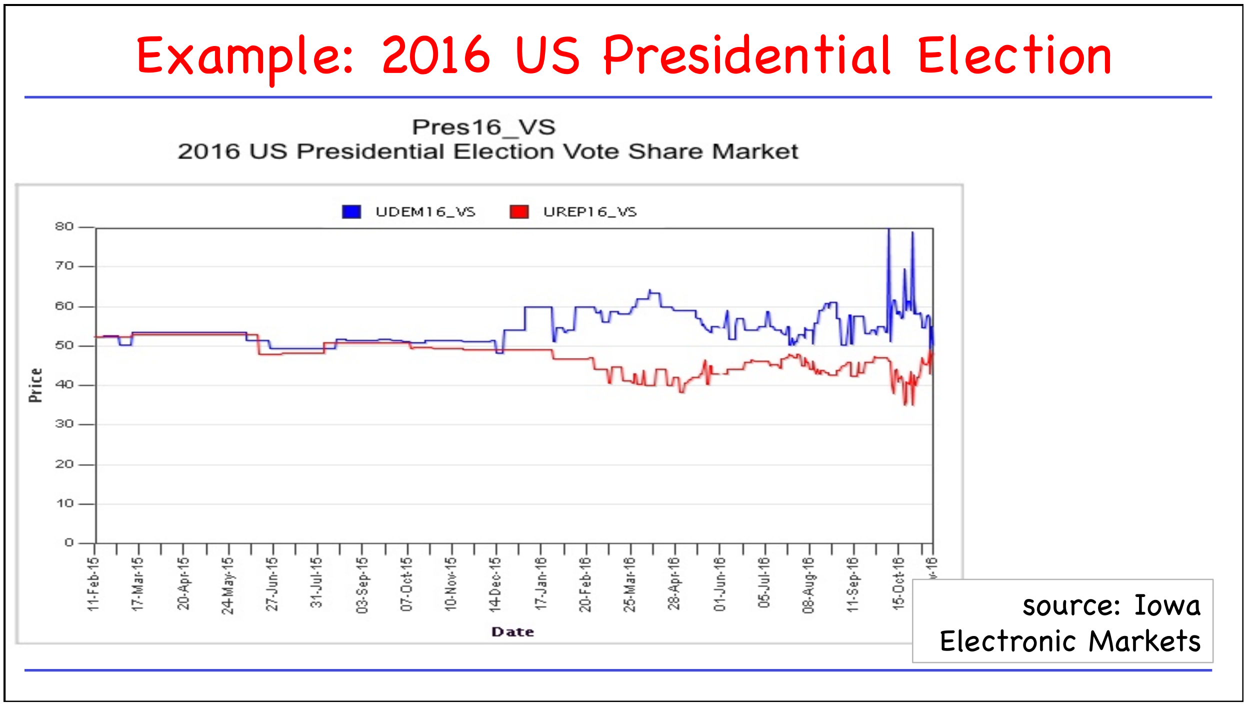
Can immediately profit!

Should have shorted

Example: 2016 Republican Primaries

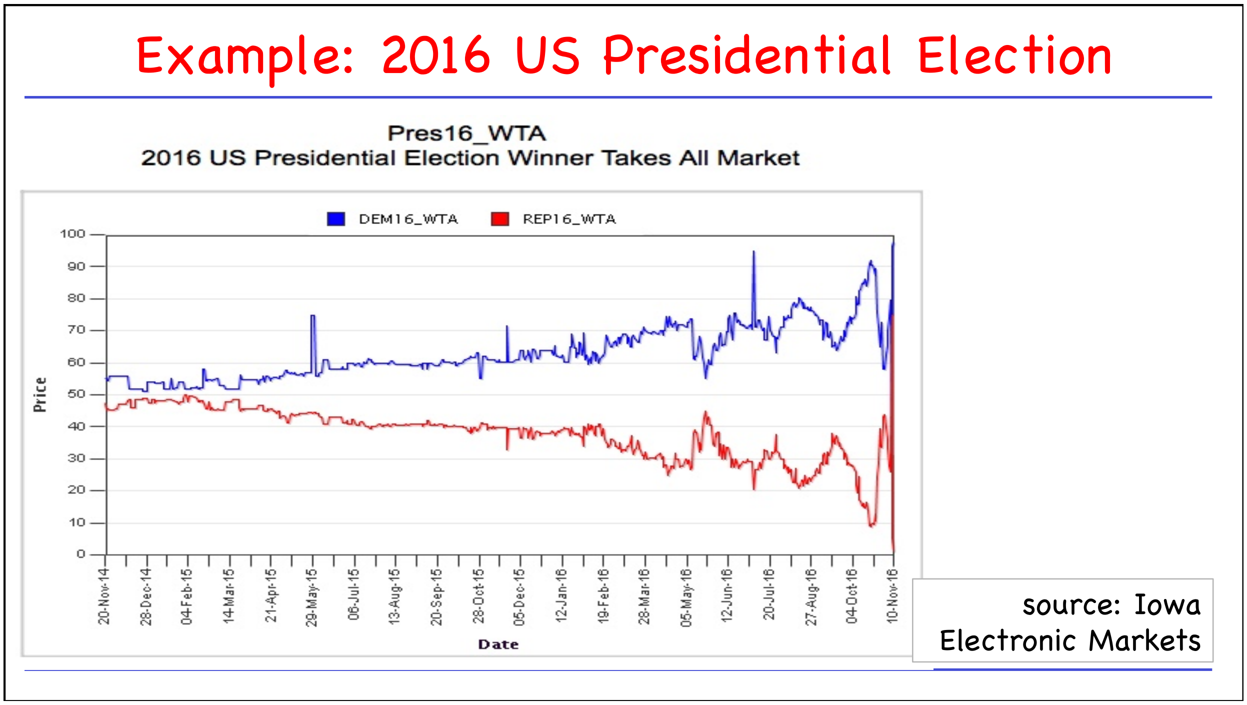


source: Iowa Electronic Markets



Example: 2016 US Presidential Election

source: Iowa Electronic Markets



Example: 2016 US Presidential Election

source: Iowa Electronic Markets

Prediction Markets

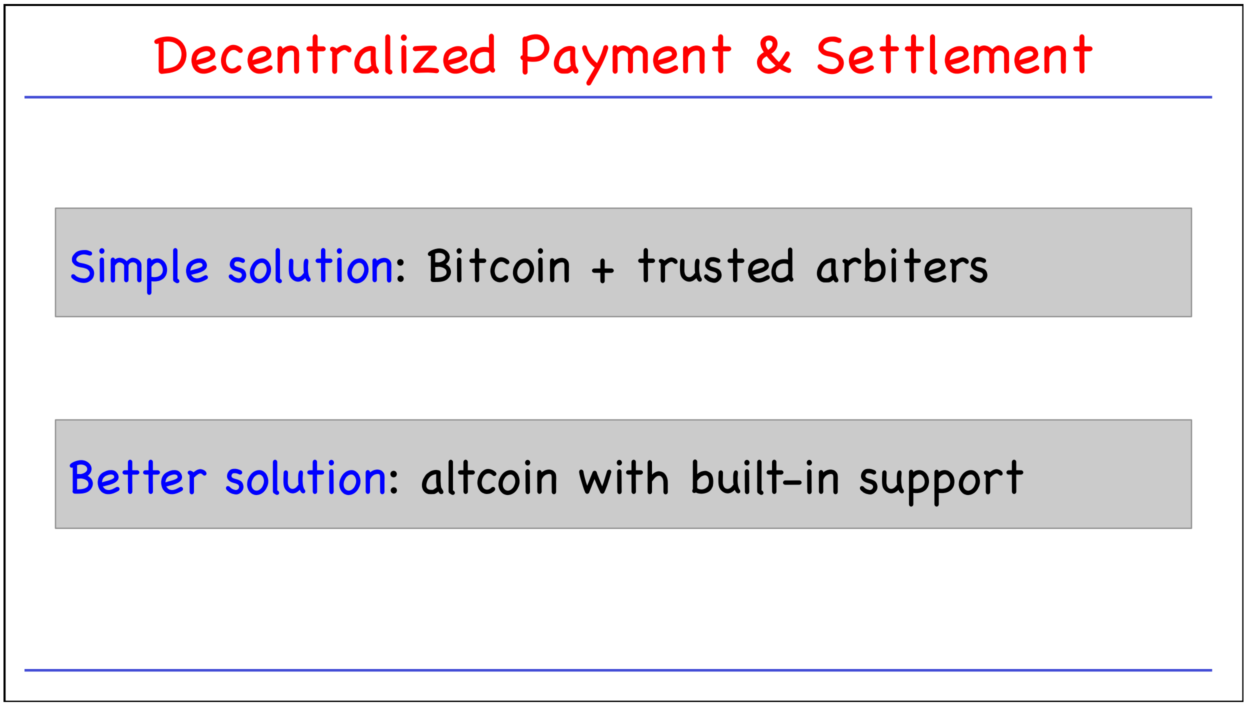
- Economists love them
  - reveal all knowledge about the future
    - (under a number of assumptions)
  - allows profit from accurate predictions
  - “a tax on BS”
- Often beat polls and expert opinions
- Significant regulatory hurdles
  - InTrade shut down in 2013

Decentralized Prediction Markets?

Decentralized payment & enforcement

Decentralized arbitration

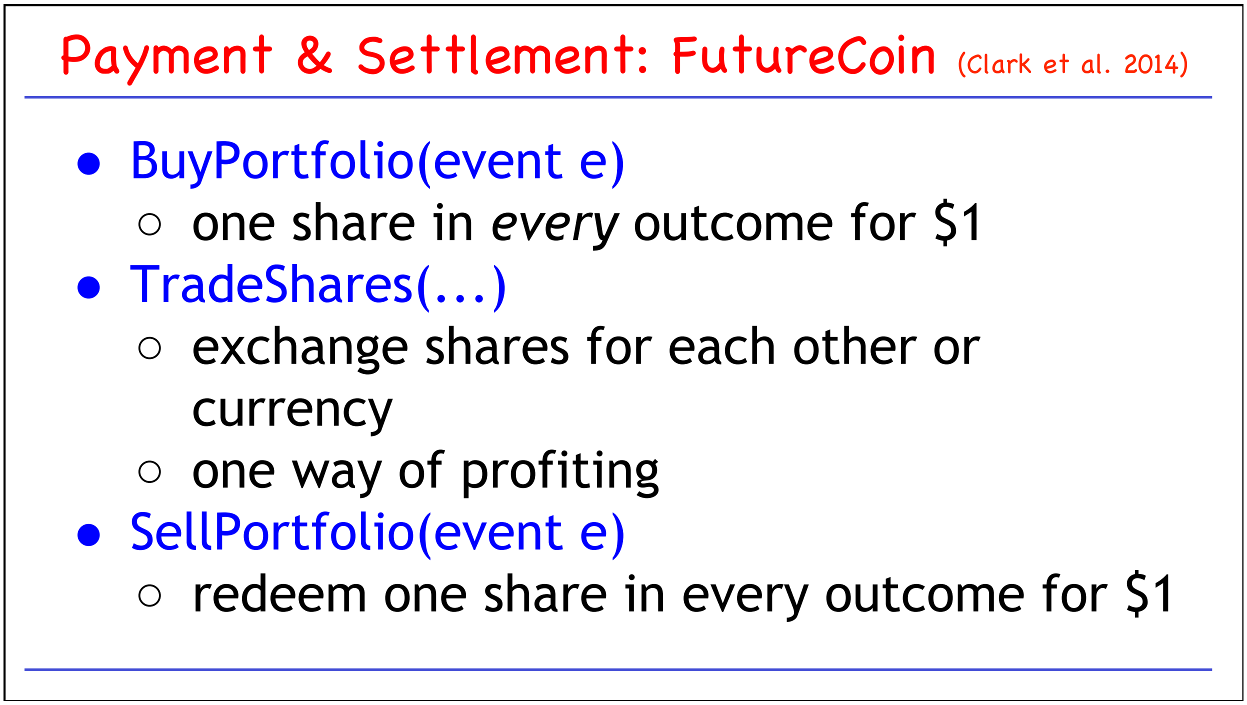
Decentralized order book



Decentralized Payment & Settlement

Simple solution: Bitcoin + trusted arbiters

Better solution: altcoin with built-in support



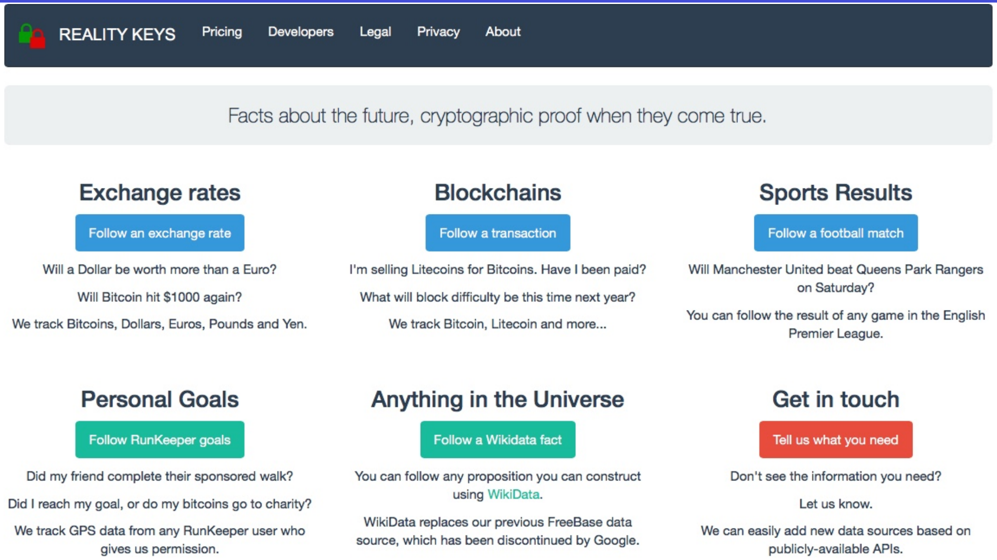
Payment & Settlement: FutureCoin (Clark et al. 2014)

- 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

Arbitration Model

- 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



Facts about the future, cryptographic proof when they come true.

Exchange rates

Will a Dollar be worth more than a Euro?

Will Bitcoin hit $1000 again?

We track Bitcoins, Dollars, Euros, Pounds and Yen.

Blockchains

I'm selling Litecoins for Bitcoins. Have I been paid?

What will block difficulty be this time next year?

We track Bitcoin, Litecoin and more...

Sports Results

Will Manchester United beat Queens Park Rangers on Saturday?

You can follow the result of any game in the English Premier League.

Personal Goals

Did my friend complete their sponsored walk?

Did I reach my goal, or do my bitcoins go to charity?

We track GPS data from any RunKeeper user who gives us permission.

Anything in the Universe

You can follow any proposition you can construct using WikiData.

WikiData replaces our previous FreeBase data source, which has been discontinued by Google.

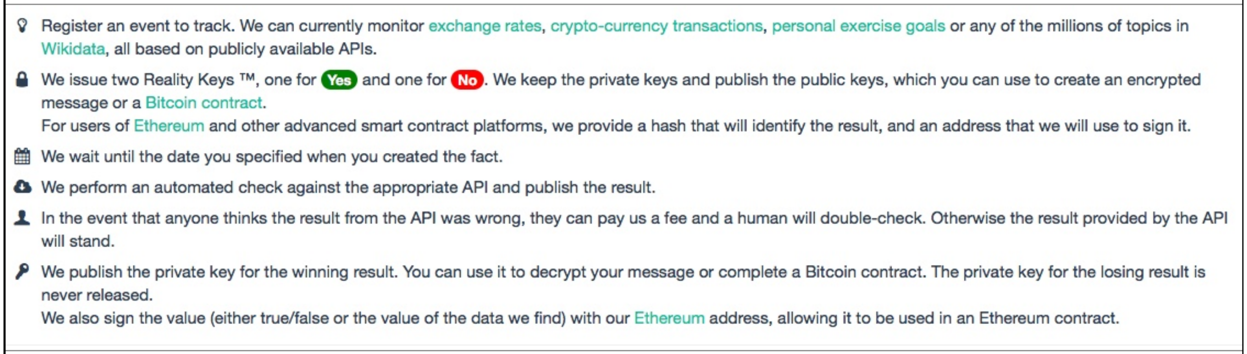
Get in touch

Don't see the information you need?

Let us know.

We can easily add new data sources based on publicly-available APIs.

RealityKeys (how it works)

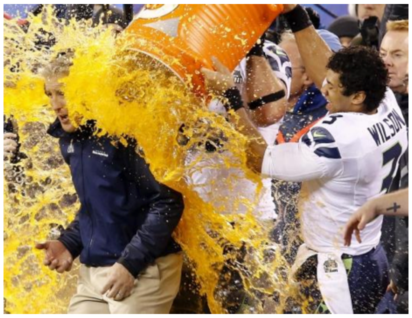


- Register an event to track. We can currently monitor exchange rates, crypto-currency transactions, personal exercise goals or any of the millions of topics in Wikidata, all based on publicly available APIs.
- We issue two Reality Keys ™, one for Yes and one for No. We keep the private keys and publish the public keys, which you can use to create an encrypted message or a Bitcoin contract.
  For users of Ethereum and other advanced smart contract platforms, we provide a hash that will identify the result, and an address that we will use to sign it.
- We wait until the date you specified when you created the fact.
- We perform an automated check against the appropriate API and publish the result.
- In the event that anyone thinks the result from the API was wrong, they can pay us a fee and a human will double-check. Otherwise the result provided by the API will stand.
- We publish the private key for the winning result. You can use it to decrypt your message or complete a Bitcoin contract. The private key for the losing result is never released.
  We also sign the value (either true/false or the value of the data we find) with our Ethereum address, allowing it to be used in an Ethereum contract.

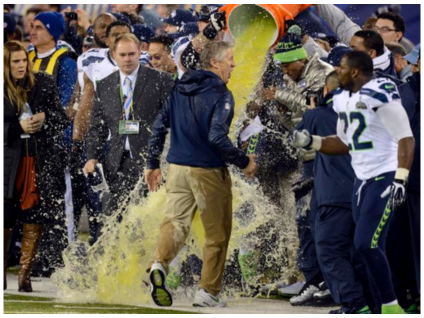
Reality can be complicated!

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
```

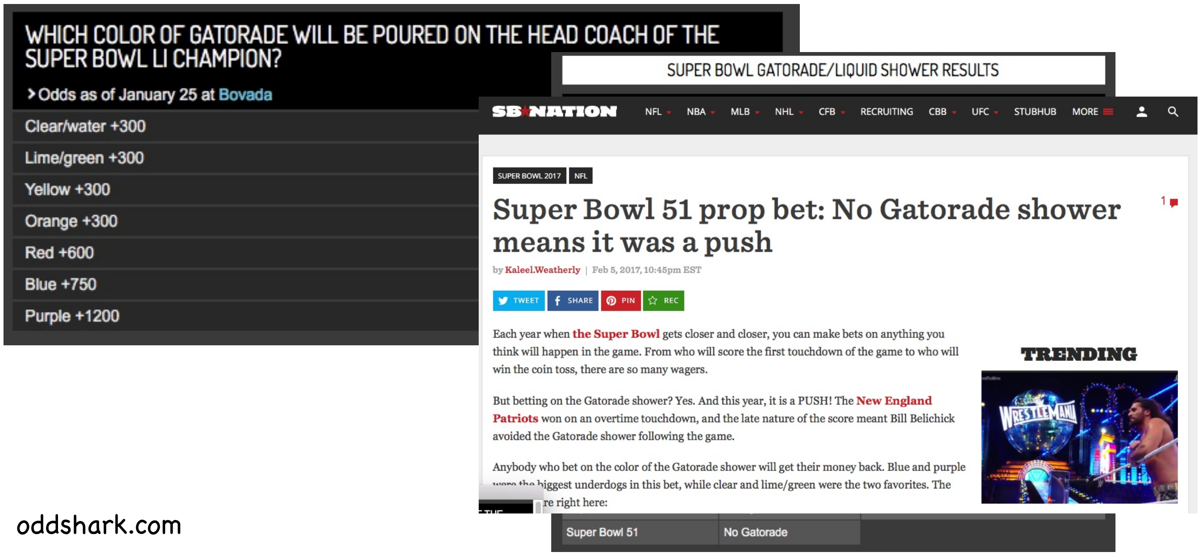


Orange?



Yellow?

Reality can be complicated! (II)



WHICH COLOR OF GATORADE WILL BE POURED ON THE HEAD COACH OF THE SUPER BOWL LI CHAMPION?

› Odds as of January 25 at Bovada

Clear/water +300
Lime/green +300
Yellow +300
Orange +300
Red +600
Blue +750
Purple +1200

SUPER BOWL GATORADE/LIQUID SHOWER RESULTS

SUPER BOWL 2017 NFL

Super Bowl 51 prop bet: No Gatorade shower means it was a push

by Kaleel.Weatherly | Feb 5, 2017, 10:45pm EST

Each year when the Super Bowl gets closer and closer, you can make bets on anything you think will happen in the game. From who will score the first touchdown of the game to who will win the coin toss, there are so many wagers.

But betting on the Gatorade shower? Yes. And this year, it is a PUSH! The New England Patriots won on an overtime touchdown, and the late nature of the score meant Bill Belichick avoided the Gatorade shower following the game.

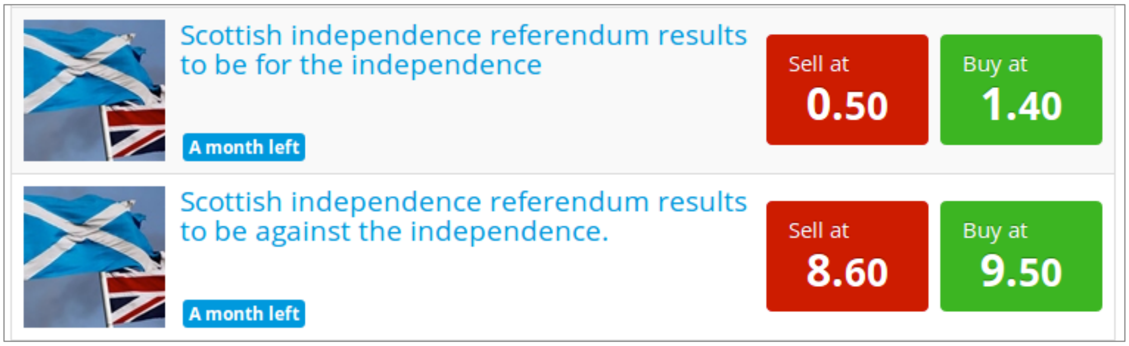
Anybody who bet on the color of the Gatorade shower will get their money back. Blue and purple were the biggest underdogs in this bet, while clear and lime/green were the two favorites. The re right here:

Super Bowl 51 | No Gatorade

oddshark.com

Order Books

Goal: match best bid and ask offers



Scottish independence referendum results to be for the independence

A month left

Sell at 0.50 | Buy at 1.40

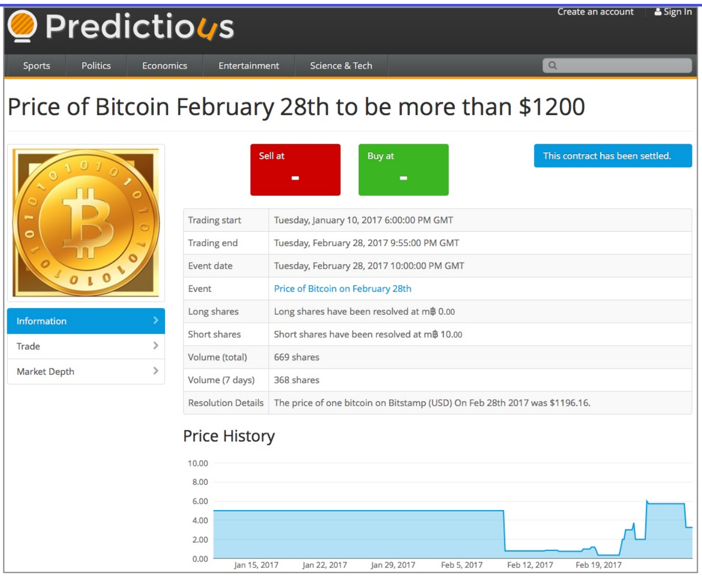
Scottish independence referendum results to be against the independence.

A month left

Sell at 8.60 | Buy at 9.50

Predictious.com

Order Books (cont)

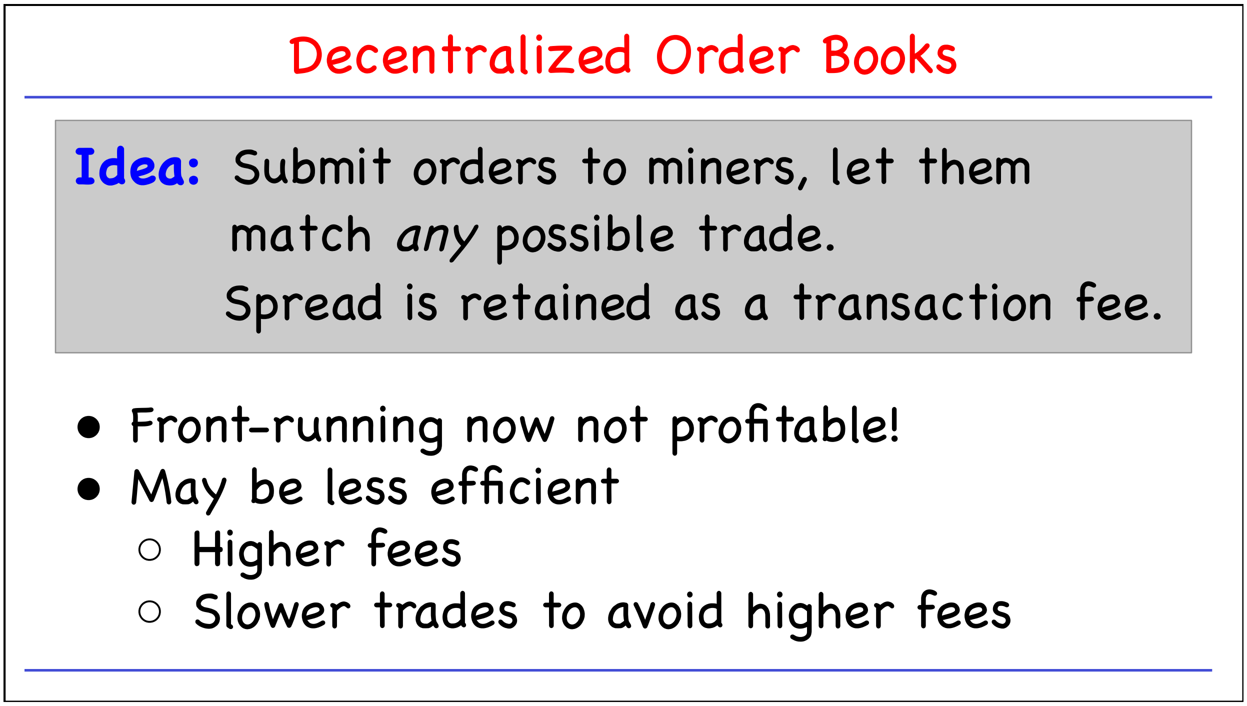


Price of Bitcoin February 28th to be more than $1200

Trading start	Tuesday, January 10, 2017 6:00:00 PM GMT
Trading end	Tuesday, February 28, 2017 9:55:00 PM GMT
Event date	Tuesday, February 28, 2017 10:00:00 PM GMT
Event	Price of Bitcoin on February 28th
Long shares	Long shares have been resolved at m฿ 0.00
Short shares	Short shares have been resolved at m฿ 10.00
Volume (total)	669 shares
Volume (7 days)	368 shares
Resolution Details	The price of one bitcoin on Bitstamp (USD) On Feb 28th 2017 was $1196.16.

Centralized Order Books

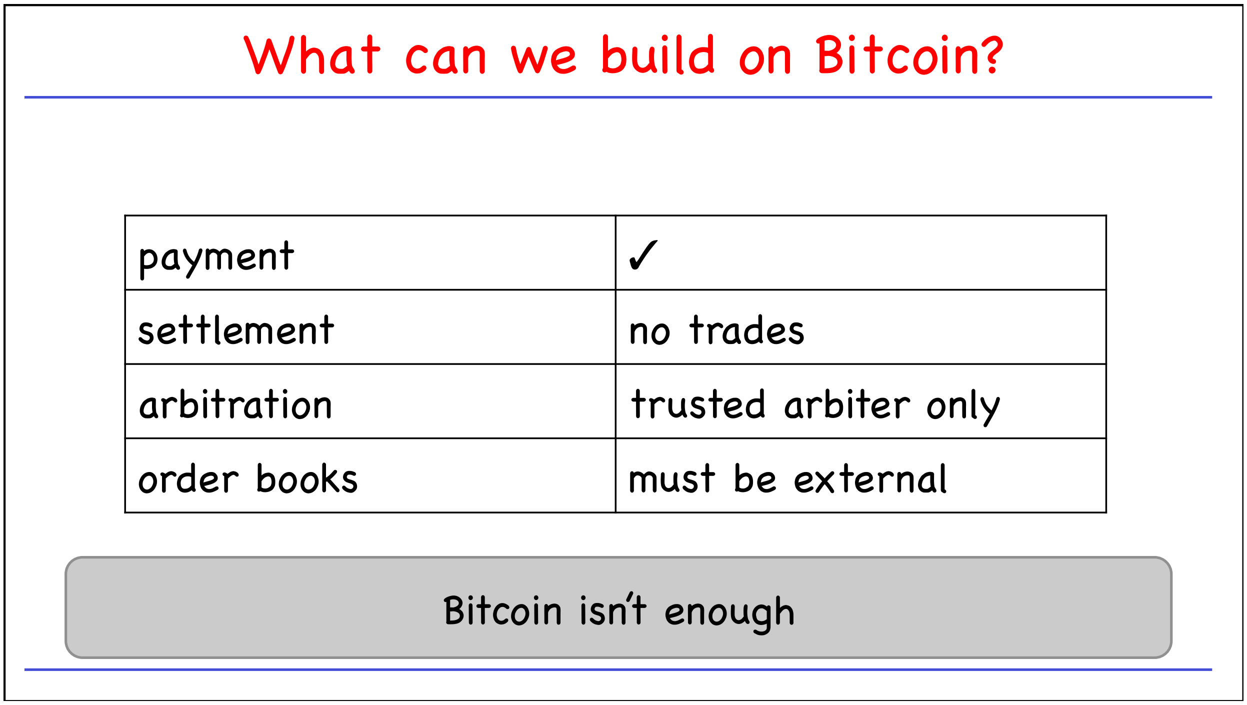
- Traditional model
- Promise to split surplus between buyer, seller
- Front-running is considered a serious crime!
  - require regulation, auditing, monitoring



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



What can we build on Bitcoin?

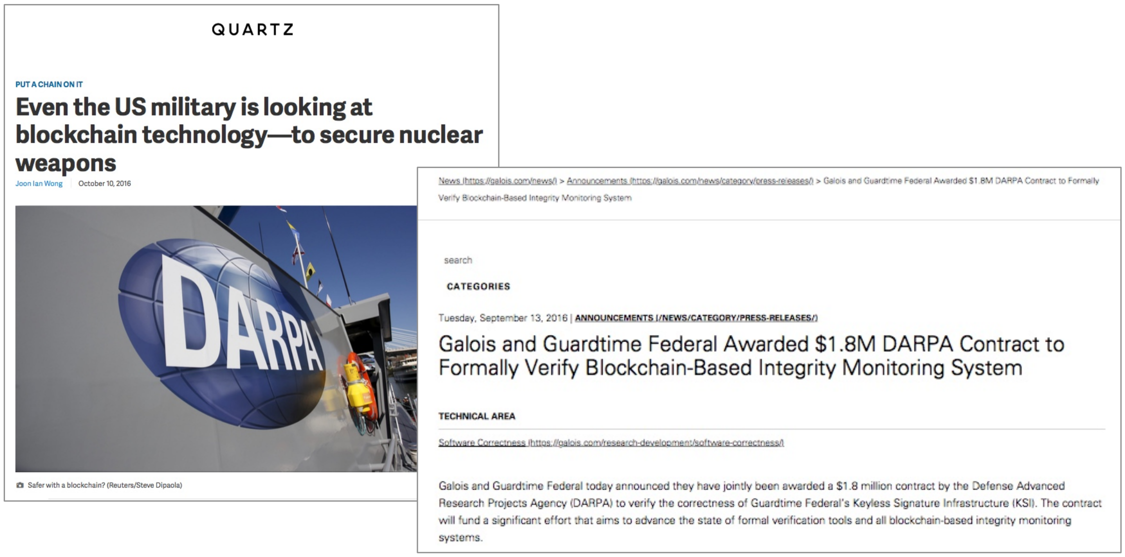
payment	✓
settlement	no trades
arbitration	trusted arbiter only
order books	must be external

Bitcoin isn't enough

Conclusion: Bitcoin can only take us so far

What if we could start again from scratch?

Block Chains: Other Applications



QUARTZ

PUT A CHAIN ON IT

Even the US military is looking at blockchain technology—to secure nuclear weapons

Joon Ian Wong | October 10, 2016

Safer with a blockchain? (Reuters/Steve Dipaola)

News (https://galois.com/news/) > Announcements (https://galois.com/news/category/press-releases/) > Galois and Guardtime Federal Awarded $1.8M DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System

search

CATEGORIES

Tuesday, September 13, 2016 | ANNOUNCEMENTS (/NEWS/CATEGORY/PRESS-RELEASES/)

Galois and Guardtime Federal Awarded $1.8M DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System

TECHNICAL AREA

Software Correctness (https://galois.com/research-development/software-correctness/)

Galois and Guardtime Federal today announced they have jointly been awarded a $1.8 million contract by the Defense Advanced Research Projects Agency (DARPA) to verify the correctness of Guardtime Federal's Keyless Signature Infrastructure (KSI). The contract will fund a significant effort that aims to advance the state of formal verification tools and all blockchain-based integrity monitoring systems.

Block Chains: General Impact

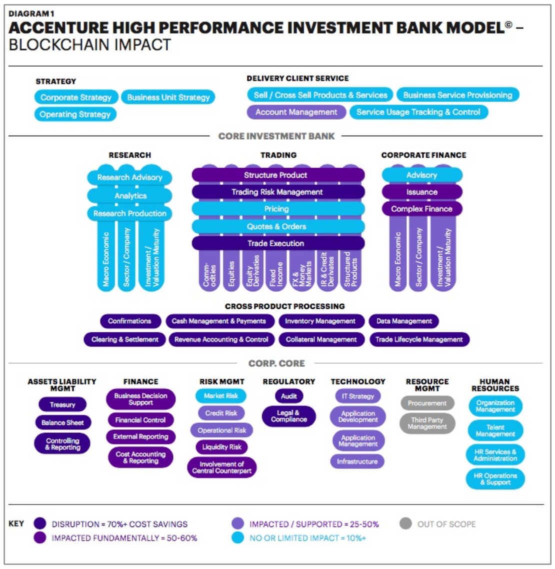


DIAGRAM 1

ACCENTURE HIGH PERFORMANCE INVESTMENT BANK MODEL© – BLOCKCHAIN IMPACT