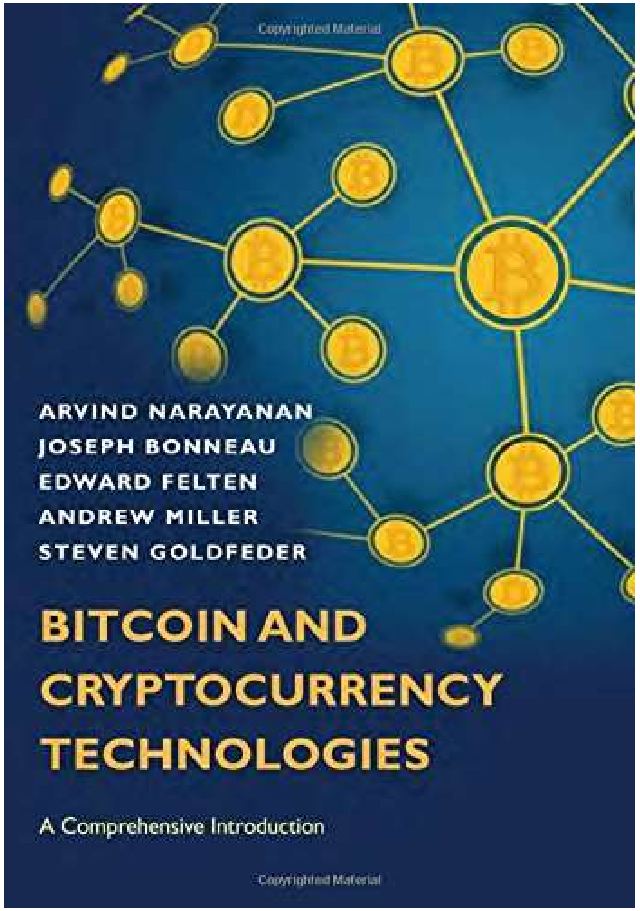
Blockchain
&
Business Application

Lecture:

Bitcoin as a Platform for
General Business Applications

Chapter 9
Bitcoin as a Platform



- So far, Bitcoin as a currency (CC)
- What other possible applications?

- Some already implementable
- Some needs modifications

- Consider Bitcoin as an ***Append-Only-Log***
- Once data written
  - Tamper-proof
  - Forever available
- Everything in order
  - Hash pointers,
  - Not timestamps
    - miners can lie about timestamps,
    - miners’ clocks may not be synchronized,
    - latency on the network.
  - If timestamp too weird (1 hour difference) rejected

- We want to be able to prove that:

  We know some value *x* @*T*.

- Might not want to *reveal* *x* @*T* .
- Instead, we only want to reveal *x* when we actually make the proof @T+t

- However, once proof is OK, we want the evidence to be permanent

Recall committing data

- Instead of publishing x, we can publish H(x)

- Later, no y such that x !=y but H(x) = H(y)

- H(x) reveals no info about x.

Applications of timestamping 1

- Suppose we wanted to prove that some invention we filed a patent on was actually in our heads much earlier

- Publish the hash of the design document

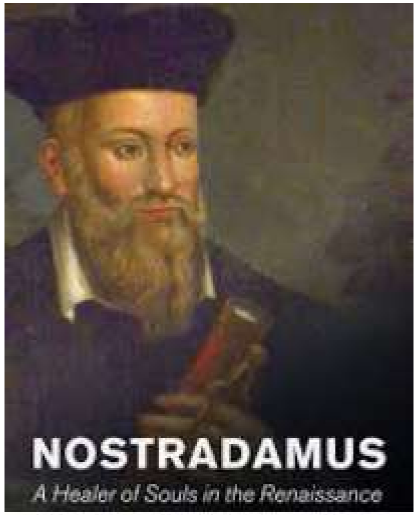
- Later anytime, publish the design document
- Anyone can compute H(d. doc) and compare

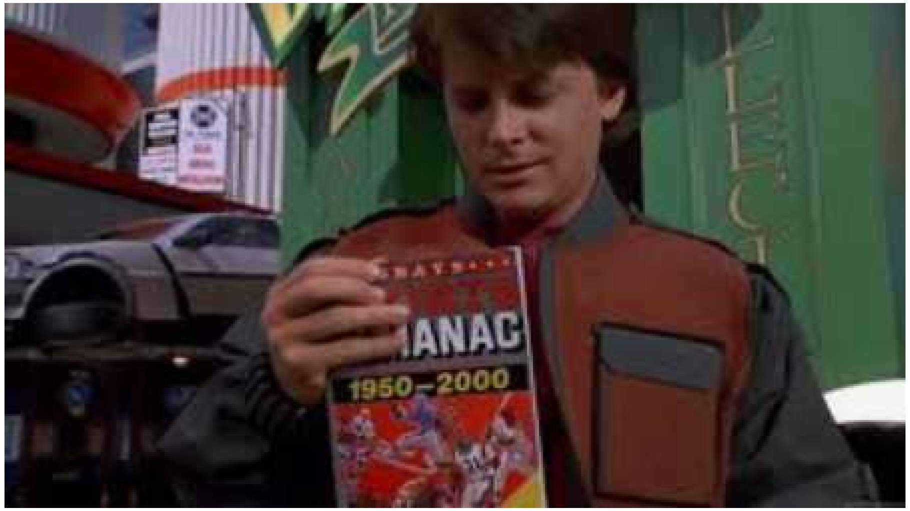
Applications of timestamping 2

- Suppose Alice hires Bob to perform a programming job;
- Their contract requires Bob to submit his work to Alice by a specific time.
- A&B published the hash of Bob’s submitted work signed by both
- If any dispute later, straightfw to check

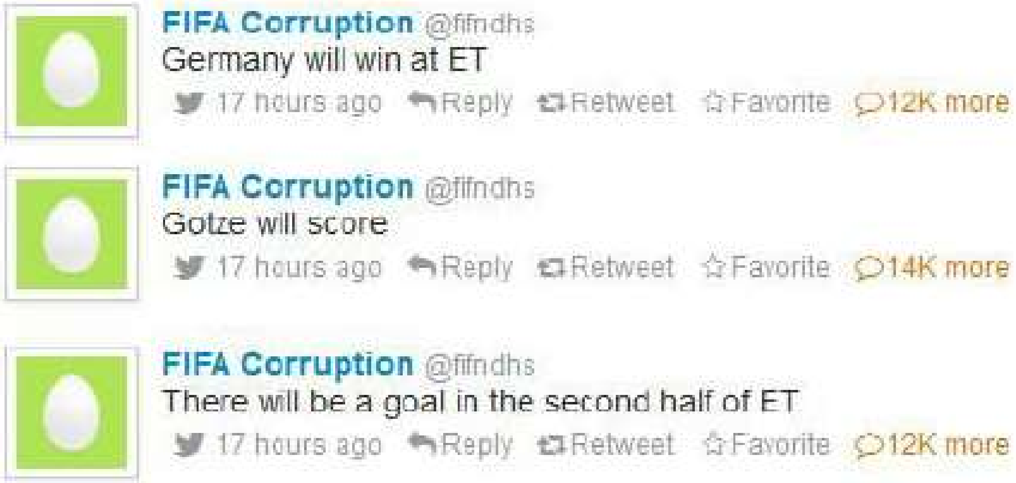
Attacks on Proof-of-Clairvoyance

- Clairvoyance: Ability of predicting the future!
- Publish a commitment about a future event
- After it occurred, publish your words





- A Twitter account attempted to “prove” 2014 FIFA Men’s World Cup Final was rigged by “predicting” the outcome of the match



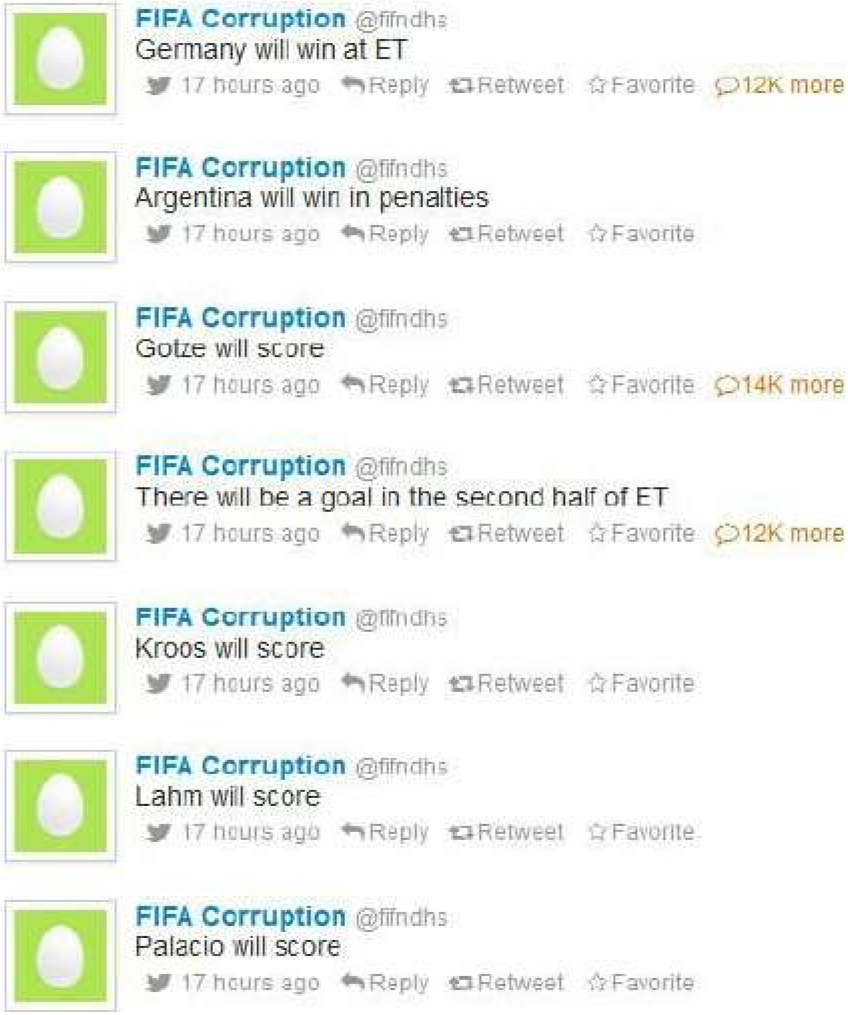
FIFA Corruption @fifndhs
Germany will win at ET

FIFA Corruption @fifndhs
Gotze will score

FIFA Corruption @fifndhs
There will be a goal in the second half of ET

- How come? Is it Possible?

- Tweeted all possibilities
- Kept ones ended true
- Deleted all others



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
Lahm will score
17 hours ago Reply Retweet Favorite

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

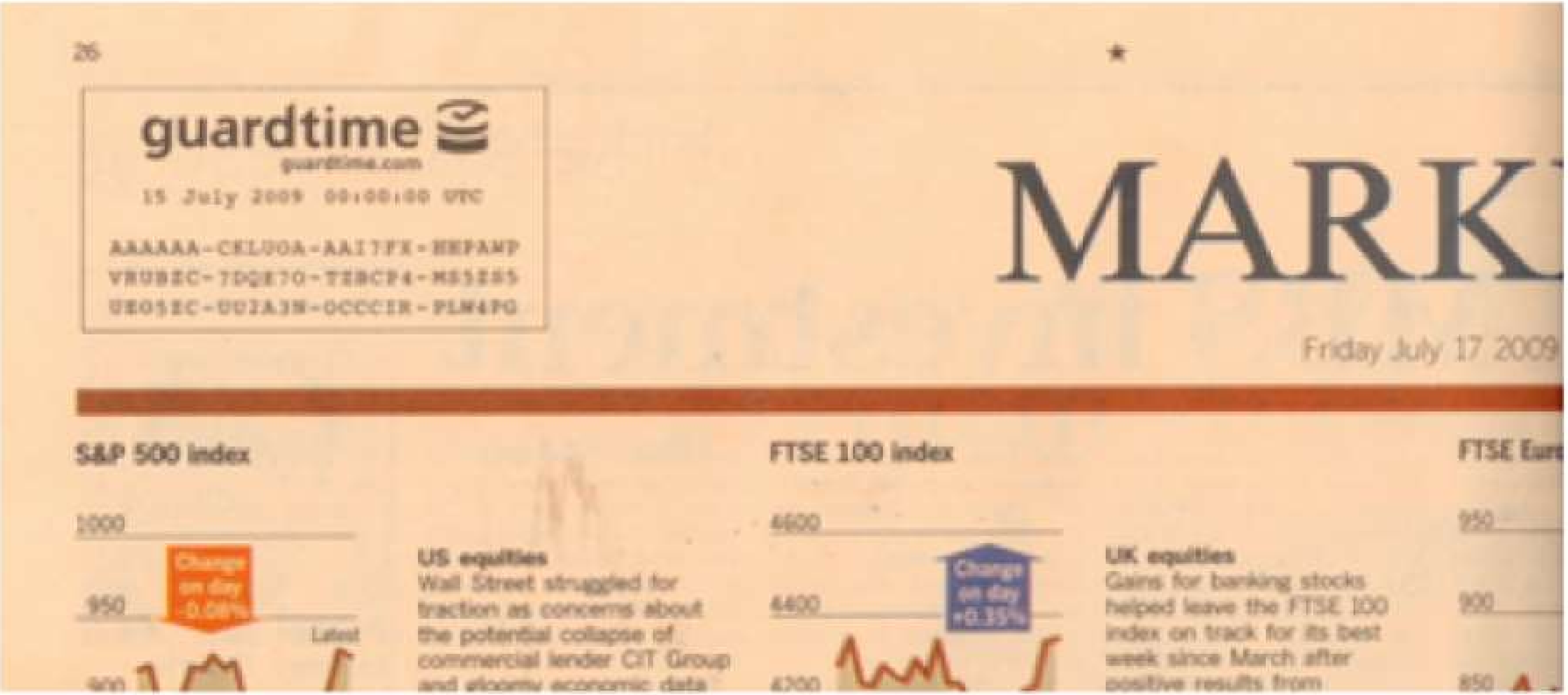
Bitcoin

- Secure timestamping system does not tie commitments to any individual’s public identity.
- If you don’t reveal them, it is easy to publish a large number of commitments
- The ones you never reveal cannot easily be traced back to you.

Anonymity vs. decentralization

How to achieve a secure timestamping in Bitcoin?

Secure timestamping the old-fashioned way



26

guardtime

guardtime.com

15 July 2009 00:00:00 UTC

AAAAAA-CKLUOA-AAI7FX-HHPAWP
VRUBZC-7DQE7O-TZBCP4-MS5ZS5
UZO5ZC-UUJA3N-OCCCIR-PLM4PG

MARK

Friday July 17 2009

S&P 500 index
1000
950
900
Change on day -0.08%
Latest
FTSE 100 index
4600
4400
4200
Change on day +0.35%
FTSE Eur
950
900
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

Figure 9.2: A timestamping service (GuardTime) that publishes hashes in a daily newspaper rather than the Bitcoin block chain.

Bitcoin: Unspendable outputs.

- *OP_RETURN* instruction → unspendable output
  - returns immediately with an error
  - so that this script can never be run successfully,
  - the data you include is ignored
- Cost: One transaction fee, 1 penny
- Drawback: Arbitrary data? Child pornography?
- Would you become a miner?
- U.S. Code 2252:
  - "*knowingly* possesses, or *knowingly* accesses with intent to view"

Overlay Currencies

- We *can* write any data we want into Bitcoin
- Use Bitcoin as an append-only-log
- Build a new CC *on top of Bitcoin*
- Without need to develop a consensus mech.

- Bitcoin Miners won't validate the data (ignore)
- Complicated logic required
- Double spend?

Counterparty

- All of its transactions written on Bitcoin
- In 2014, 1% of Bitcoin transactions carried it

- Counterparty's developers don't need to deal with consensus, etc. → Can develop sophisticated applications, smartcontracts, etc

- Ability to create a new CC without consensus mechanism and new miners? Looks good!
- Drawbacks?

Bitcoins as “Smart Property”

- Use bitcoins to represent sth other than a unit of currency in the Bitcoin system
- Following transaction graph, you can trace ownership of value in the Bitcoin system over time (bad for anonymity)
- No actual “coins” just unspent transactions

- Bitcoins are not fungible (not like gold)
- Histories are different; it “may” matter

Give a *meaning* to history of..

- Paper currency, first?
- Not jokes but some meaning
- Even a db to match s.n. → no need to stamp
- Inherit the anti-counterfeiting of paper money

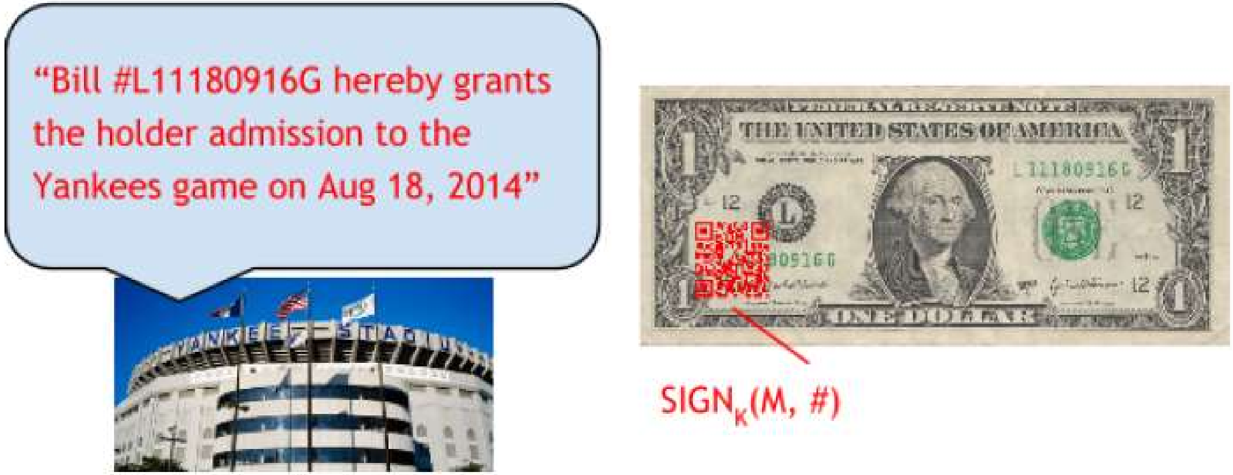

"Bill #L11180916G hereby grants the holder admission to the Yankees game on Aug 18, 2014"
SIGN$_K$(M, #)

Figure 9.4: An example of adding useful metadata to ordinary bank notes

Bitcoin

- Colored coins: Color as an extra metadata
- “issuing” transaction, we’ll insert some extra metadata

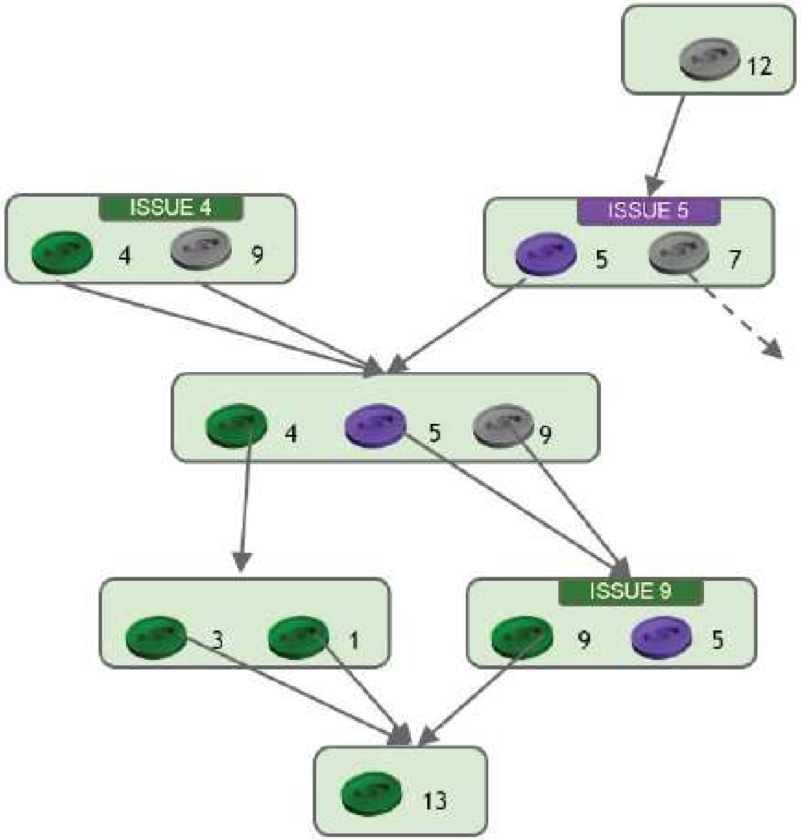


Figure 9.5: Colored coins. The transaction graph shown illustrates issuance and propagation of color

OppenAssets

- Most popular application using “colors”
- Assets issued using special Pay-to-Script-Hash (P2SH) address
- A transaction to that address adds color
- More than one “color” is OK
- Compatible with Bitcoin (only if color, extra value)
- When using “colored coin”, use a marker
  - To prevent double payment (e.g. ticket)
- Miners don’t check colors, trust a 3rd party

Secure Multi-Party Lotteries in Bitcoin

- Traditional betting
  - Alice and Bob want to bet five dollars.
  - They both agree to the bet in future, and the method
  - Bob will flip a coin in the air
  - while it’s rotating Alice calls out “Heads” or “Tails”.
  - When the coin lands,
  - both immediately see who won
  - Both know the outcome was random (no influence)
  - Both “trust” that looser is going to pay

Cryptographic coin flipping

- If designed, build various applications
- “Secure multiparty computation”
  - two or more mutually untrusting parties
  - each have some data
  - want to compute a result depends on all data
  - but without revealing the data to each other

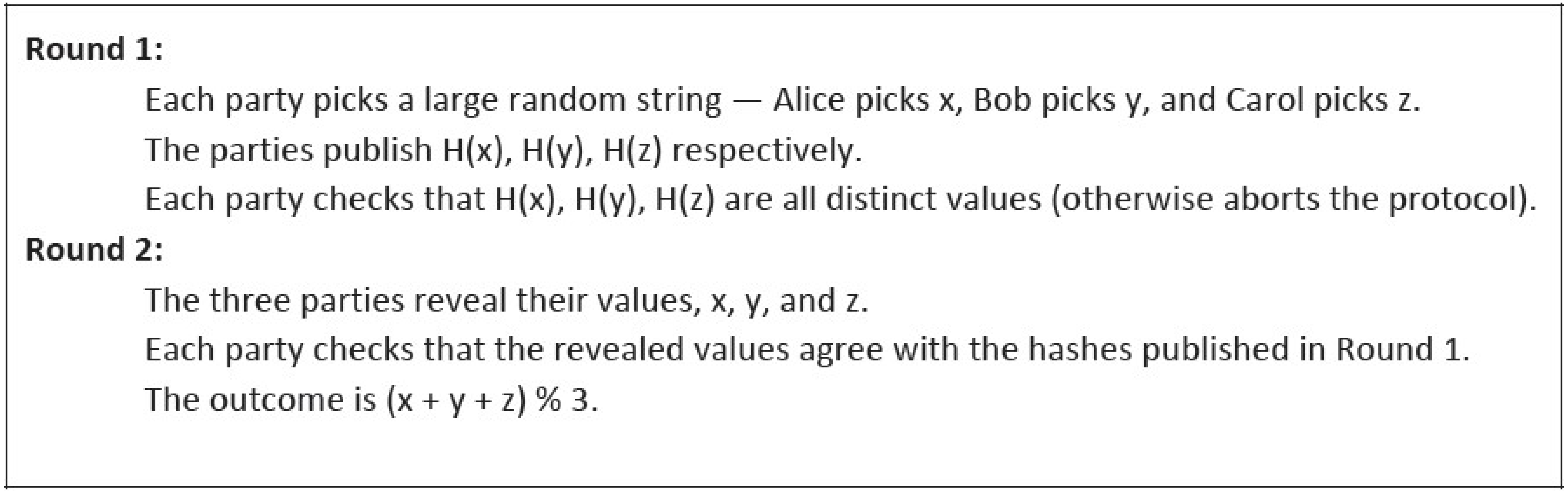
- Sealed-bid auction, without a trusted auctioneer

- We might want
  - the result of the *computation* to determine a *monetary* outcome in an irrevocable way.
  - to ensure that the winning bidder in the auction pays the seller;
  - we even want to ensure that the seller’s (smart) property being auctioned is automatically transferred to the winning bidder
  - to penalize parties if they deviate from the protocol.

Coin Flipping Online

- Online game
  - Alice, Bob, and Carol
  - All want to select 0,1 or 2 with equal probability
  - They can pick large random numbers x, y, z
  - Compute (x+y+z) % 3
- If each sends number simultaneously, OK.
- If not, problem!
- Solution?

- Commitment



Round 1:

Each party picks a large random string — Alice picks x, Bob picks y, and Carol picks z.

The parties publish H(x), H(y), H(z) respectively.

Each party checks that H(x), H(y), H(z) are all distinct values (otherwise aborts the protocol).

Round 2:

The three parties reveal their values, x, y, and z.

Each party checks that the revealed values agree with the hashes published in Round 1.

The outcome is (x + y + z) % 3.

Figure 9.6: Using hash commitments to implement a fair random number generator.
This protocol can be easily extended to support any number of parties.

- What if Carol gives up declaring z?
- How to force each to declare in a limited time
  - Called “fairness” in cryptography

- Bitcoin’s “timed commitment” great for this
  - Some technical details

Bitcoin as Public Randomness Source

History

- NBA Draft Lottery
  - 1985 in NY
  - NY Knicks won

Conspiracy theories

  - Envelope's corner bent
  - Envelope kept it freezer

- U.S. military draft lottery
  - 1969, which young men to join the Army
  - To make it “look fair”

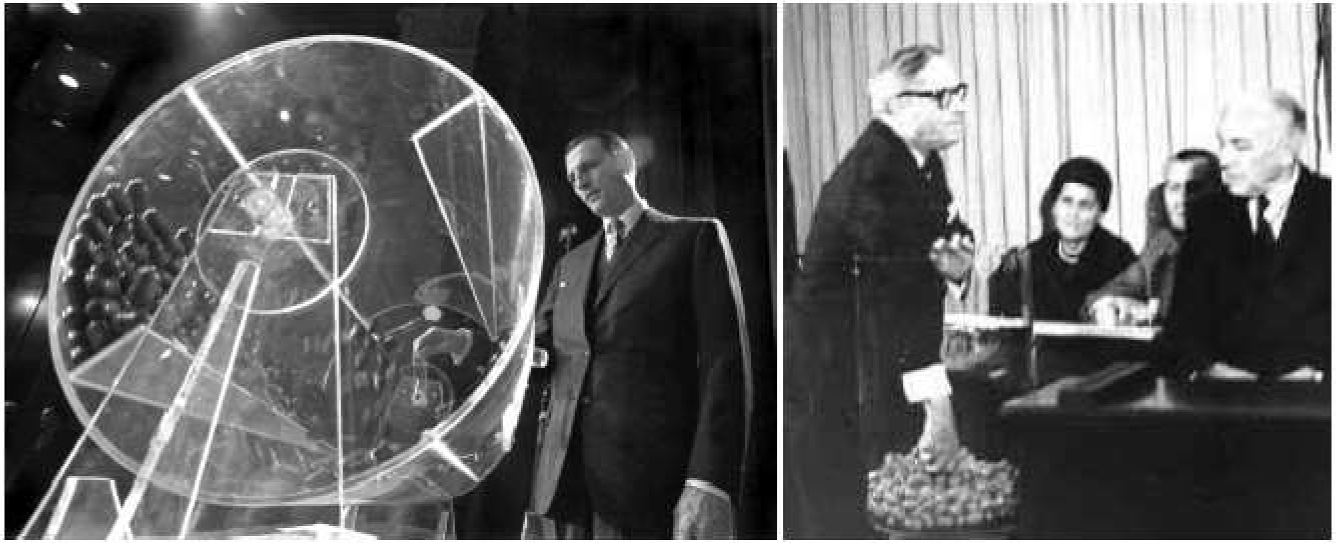


Figure 9.8: Images from the 1969 (Vietnam war) military draft lottery.

- In 1 week, statisticians observed a pattern
- Watched the tapes again and see:
  - – Drums rotated exactly even numbers!

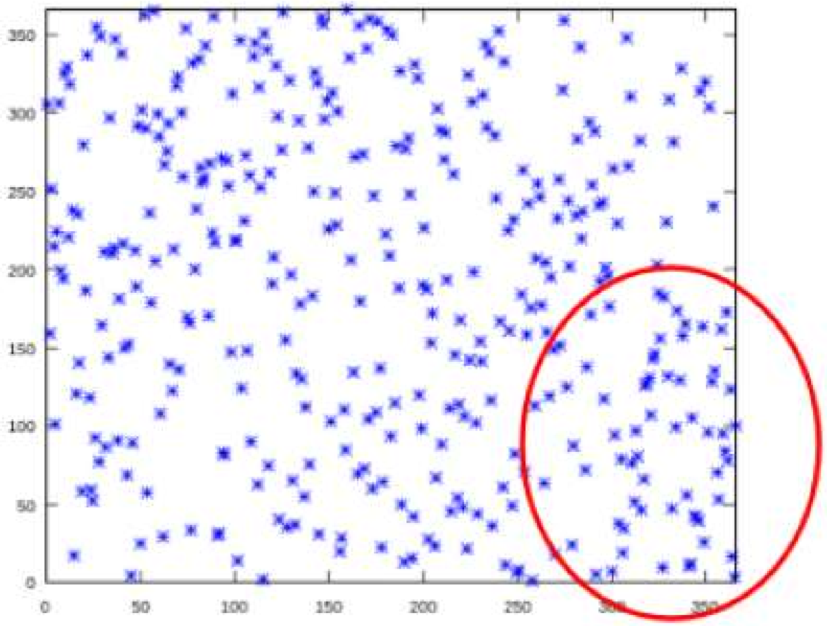


Figure 9.9: Statistical bias of the 1969 draft lottery. Day of the year (x-axis) versus lottery number (y-axis).

- Very difficult to prepare a “fair” setup
  - Actually, impossible with classical physics
  - *Determinism!*
  - Just ignore some parameters → pseudorandom
  - We need non-determinisim
  - A quantum bit provides perfect random bit!
- Even if “fair”, how to convince the public?

Cryptographic beacon

- If we have a perfect cryptographic beacon
  - Continuously publishing a random string
  - People could trust
  - No need to efforts drums, etc.
  - No need to cryptographic efforts
- We have no perfect *(classical)* beacon yet

NIST Quantum Beacon ‘2011

- Preparing two entangled photons,
- Measuring photons’ states
- Outcome is QM non-deterministic
- Do you trust QM
  - Uncertainty, superposision, entanglement?
- Do you trust that
  - Men in the lab actually doing it?
  - Not modifying the results after the measurement?

Other ways

- Criteria
  - public observability,
  - security against manipulation,
  - an acceptable level of unpredictability
- Possible methods
  - Tomorrow’s temperature?
  - Sunspots?
  - Cosmic background radiation?
  - *All actually based on QM?*

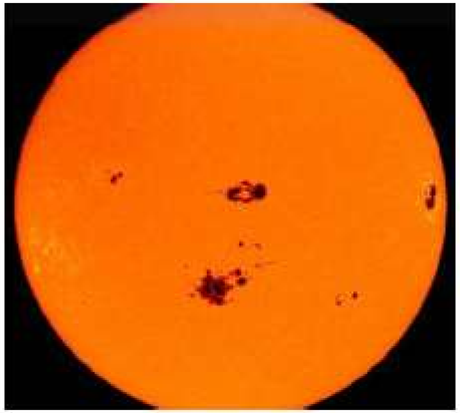


Figure 9.10: NASA image of sunspots.

Drawbacks of natural phenomena

- Slow
  - Temp once a day?
  - Sunspots change slow
- Expertise
  - Public visible but is it really DIY?
- Measurement imprecision
- Requires trust to experts

Financial Data

- Stock market prices
- Low-level fluctuations
  - A good level of randomness
  - Difficult to predict
- Drawbacks?

Financial Data

- Drawbacks of low-level fluctuations
  - If you can predict, why not make direct profit
  - You manipulate stock market, need lots of $ ☺
  - Need to trust the people in charge

- In summary, **trust** is needed!

Bitcoin as a Beacon?

- Miners compute lots of hash values
- No one “can” predict the hash of next block

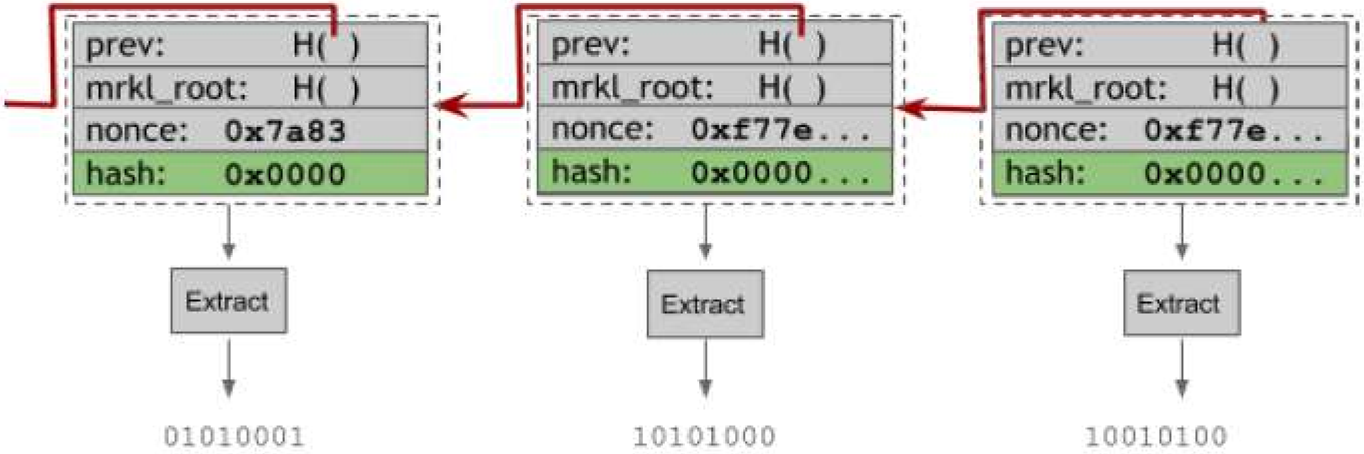


Figure 9.11: Extracting public randomness from the hashes of blocks in the block chain.

Bitcoin as a Beacon?

- Security?
  - You find a block, you know its hash
  - Publish it, or play lottery?
- Timing?
  - Next block, exactly when?
- Pool members discarding the blocks?

- Interesting but unproven way