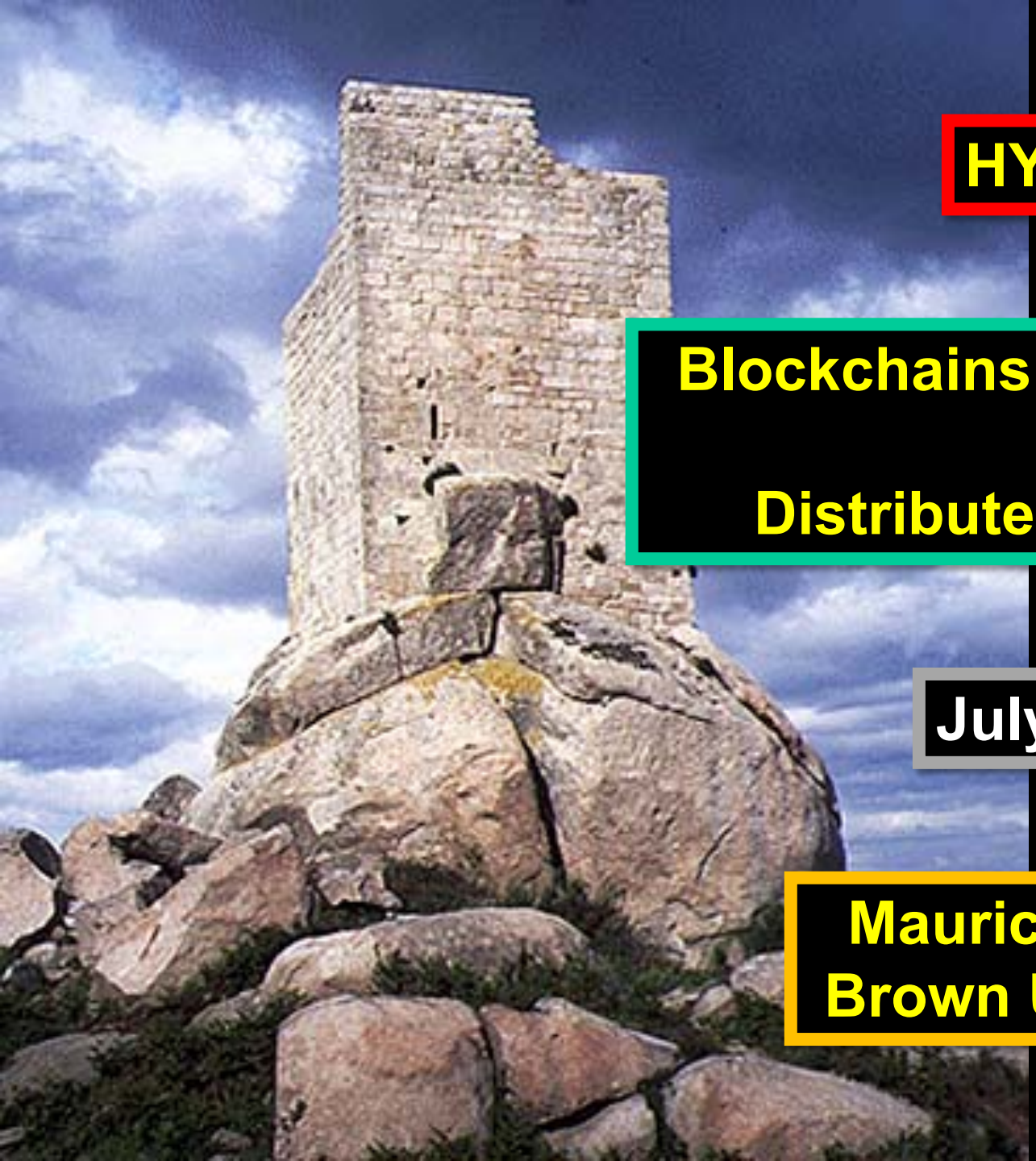


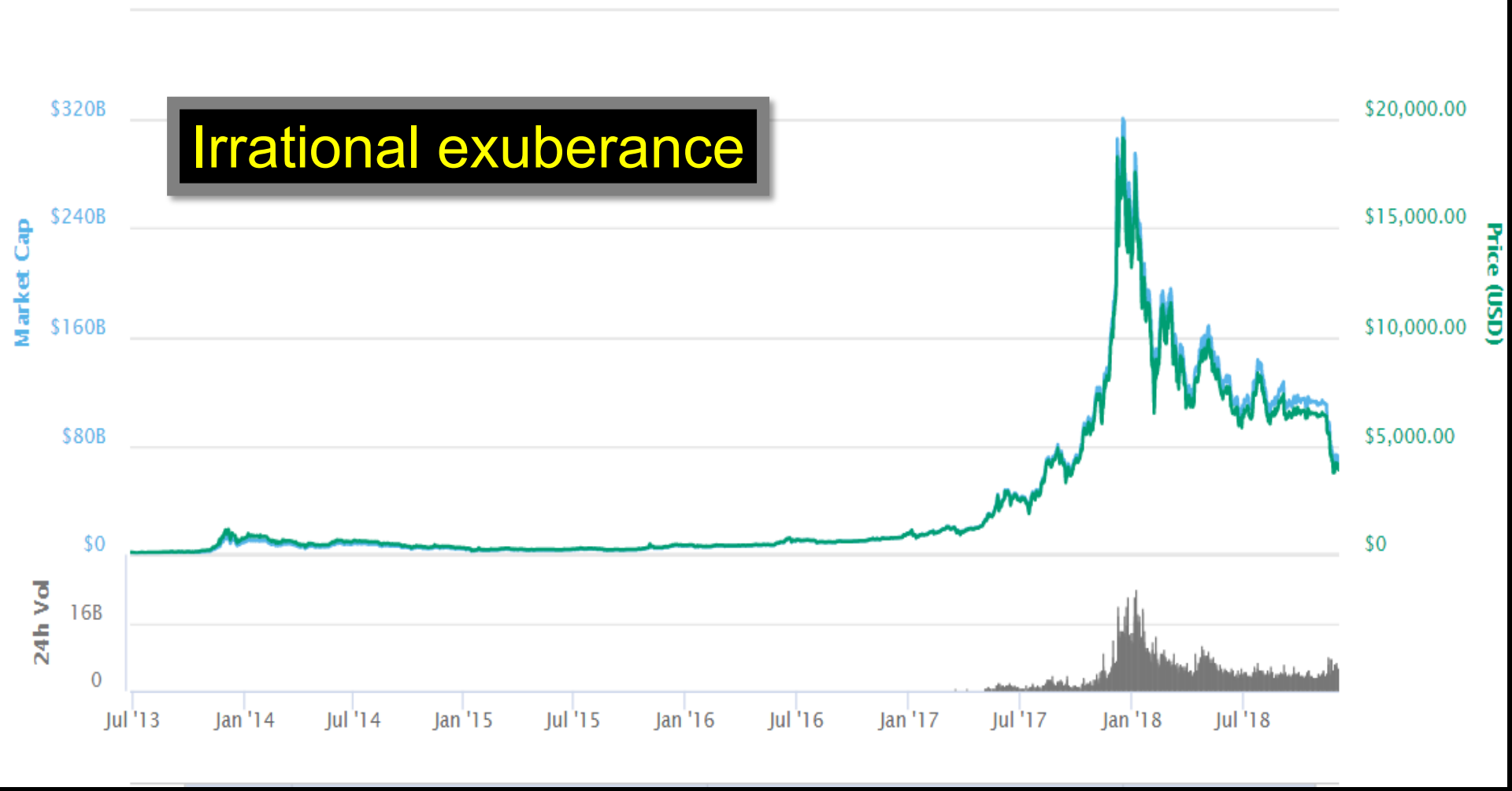
HYDRA

Blockchains and the Future of Distributed Computing

July 2019

Maurice Herlihy
Brown University


Bitcoin is in the news ….
and I, for one, just can’t look away …



"Buy a stock, if it goes up, sell it, if it goes down, don't buy it."

Yogi Berra


VISIBILITY
BTC at $20K
Peak of Inflated Expectations
Plateau of Productivity
BTC today?
Slope of Enlightenment
Trough of Disi
Our mission here
Technology Trigger
TIME


RED
The Untold Story of Silk Road, Part 1
THE
RISE
&
FALL
OF
SILK
ROAD
Part I
How a 29-year-old idealist built a global drug bazaar and became a murderous kingpin.
BY JOSHUAH BEARMAN
TOMER HANUKA
with additional reporting

true crime

DealBook
WITH FOUNDER
ANDREW ROSS SORKIN

Mt. Gox Creditors Seek Trillions Where The

By NATHANIEL POPPER MAY 25, 2016

vanishing millions

Who is Satoshi Nakamoto?

635 60

The Economist

World politics | Business & finance | Economics | Science & technology

Bitcoin's creator

Craig Steven Wright claims to be Satoshi Nakamoto. Is he?

All latest updates

Bitcoin's self-proclaimed founder says he lacks 'courage' to give more proof

Wright didn't explicitly withdraw his claim to
ete his blog posts. (Dominic Lipinski / Assoc

Craig Wright is not Satoshi Nakamoto

toshi Nakamoto before or after
Satoshi

Wright is not Satoshi Nakamoto.
suspected him to
himself to be on
about

mysterious identities

steemit trending new hot promoted search Sign up Login

6 Major Porn Sites Now Accept Bitcoin

PERSONAL FINANCE

7 months ago

PERSONAL FINANCE | RETIREMENT | CAREERS | SAVINGS | DEBT | TAX PLANNING | COLLEGE GAME

Bitcoin offers the cannabis industry an alternative

- An estimated 500 banks will wo
majority still won't.
- Experts say the
as a safer altern

Annie Nova
Published 10:00 AM ET Fri,

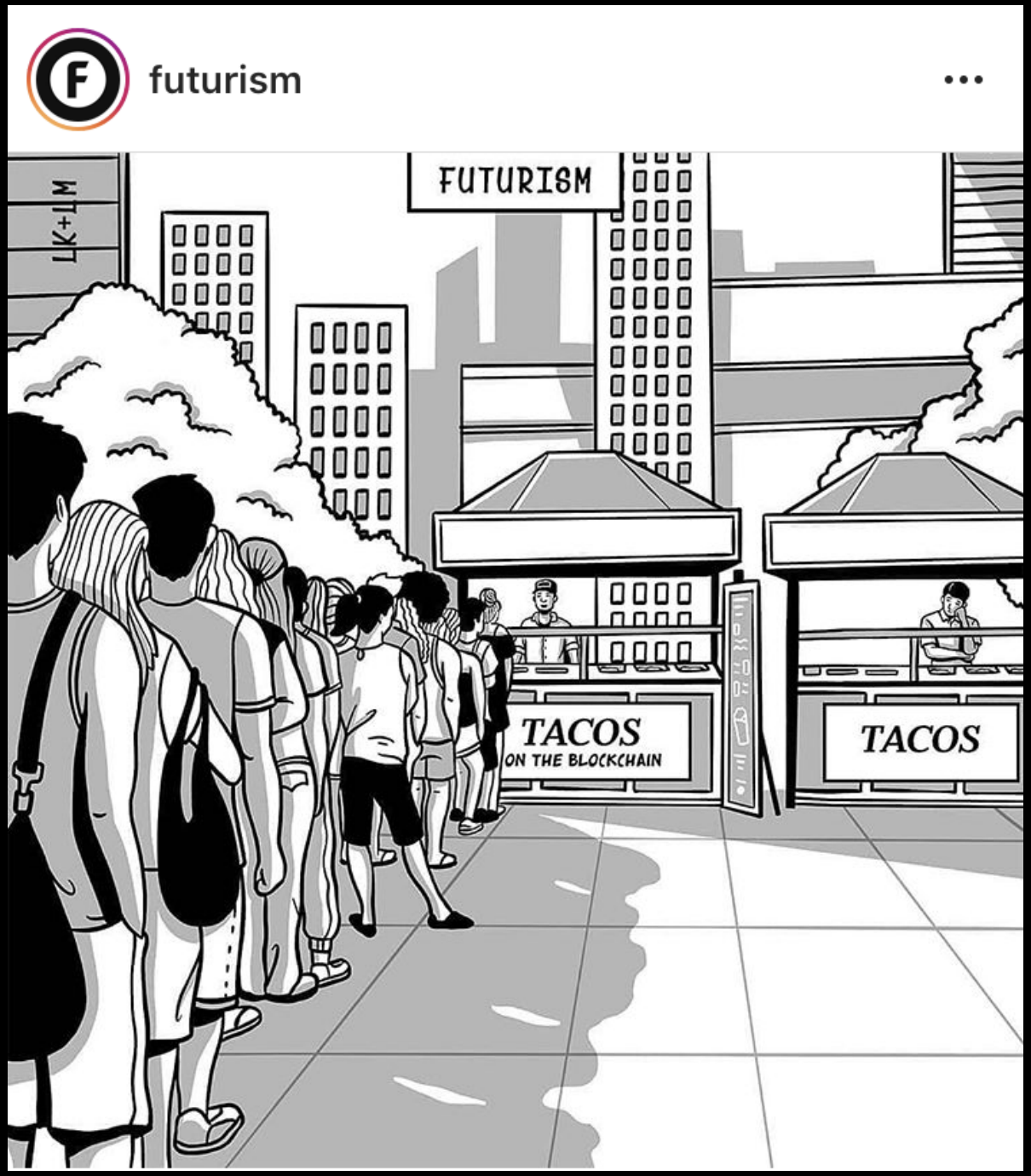
CNBC

BITCOIN CRIME WAVE

Treasury crackdown as Bitcoin is used by to buy drugs, guns and launder illegal

now intends to crackdown and regulate the

sex, drugs, rock-n-roll


futurism
FUTURISM
LK+LM
TACOS
ON THE BLOCKCHAIN
TACOS

This talk is not about Bitcoin

This talk is not about Bitcoin

It’s about blockchains.

This talk is not about Bitcoin

It’s about blockchains.

And why this area needs real, scientific research


Hello World!
timing
crashes
omission
Byzantine
Now solve consensus
Classical Adversary

Modern Adversary

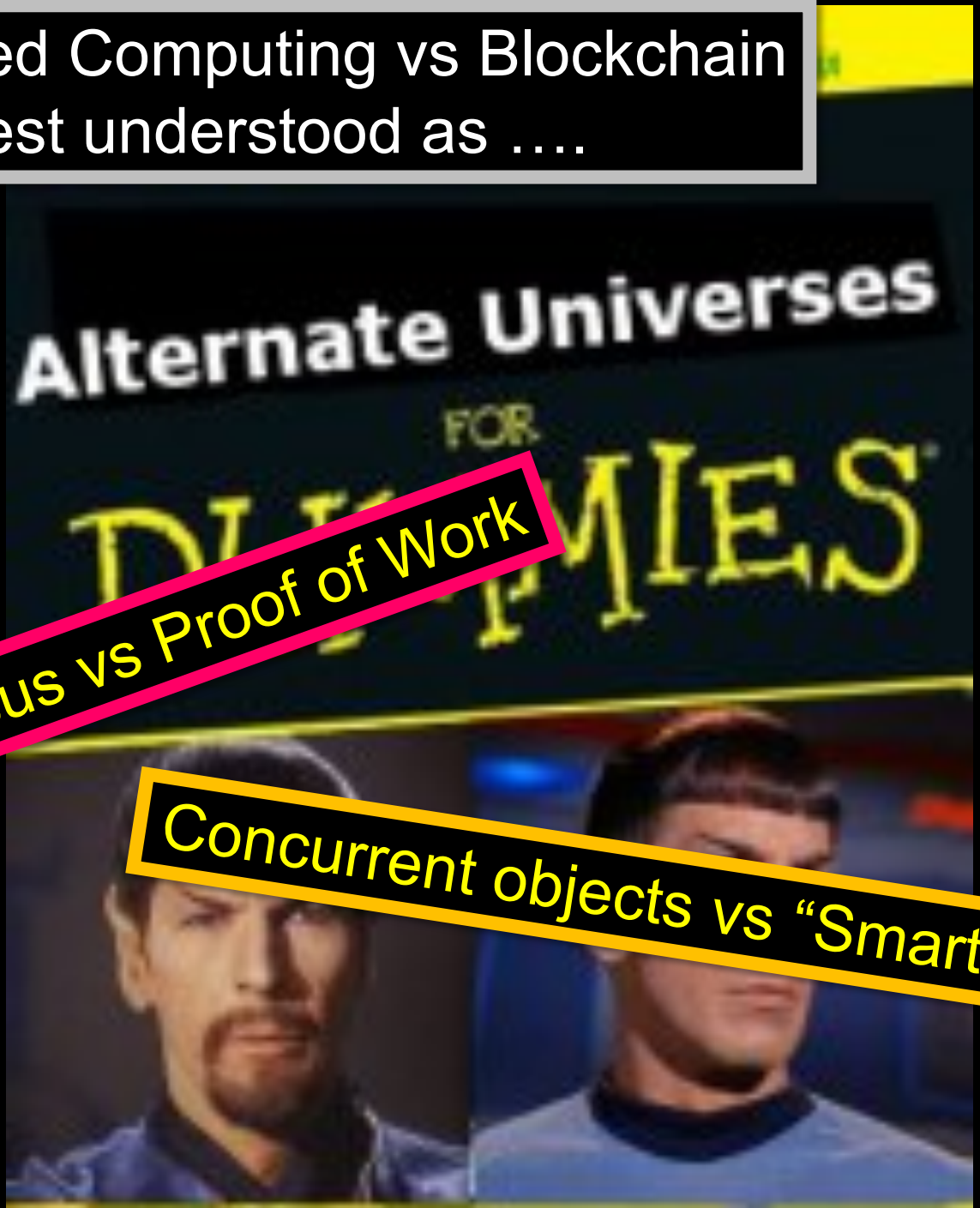
Real innovation usually intrudes from outside a community …

Would this paper have been accepted to a mainstream DC conference in 2008?

Now multi-billion dollar industry

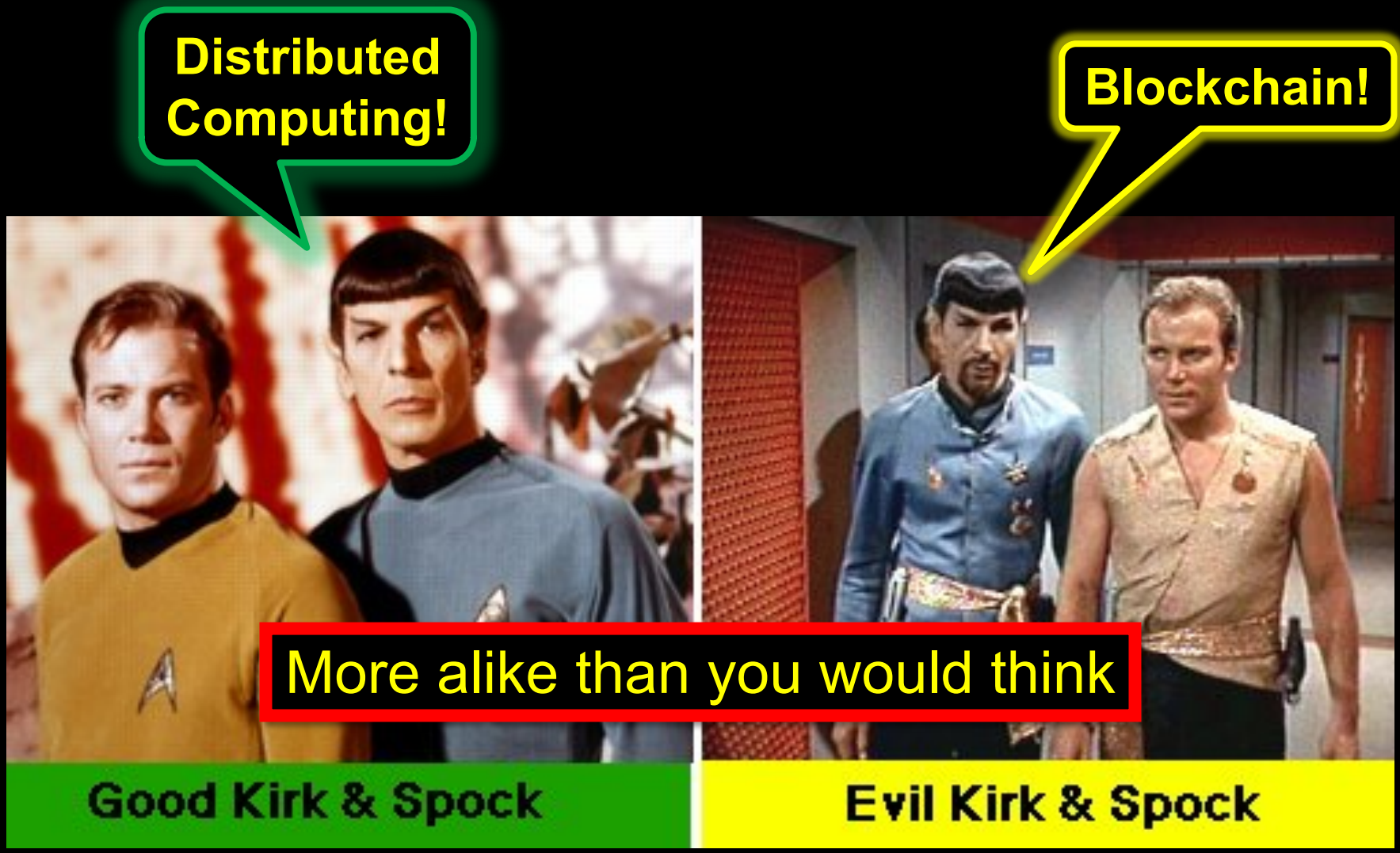
What relation to distributed computing?

Distributed Computing vs Blockchain best understood as ….

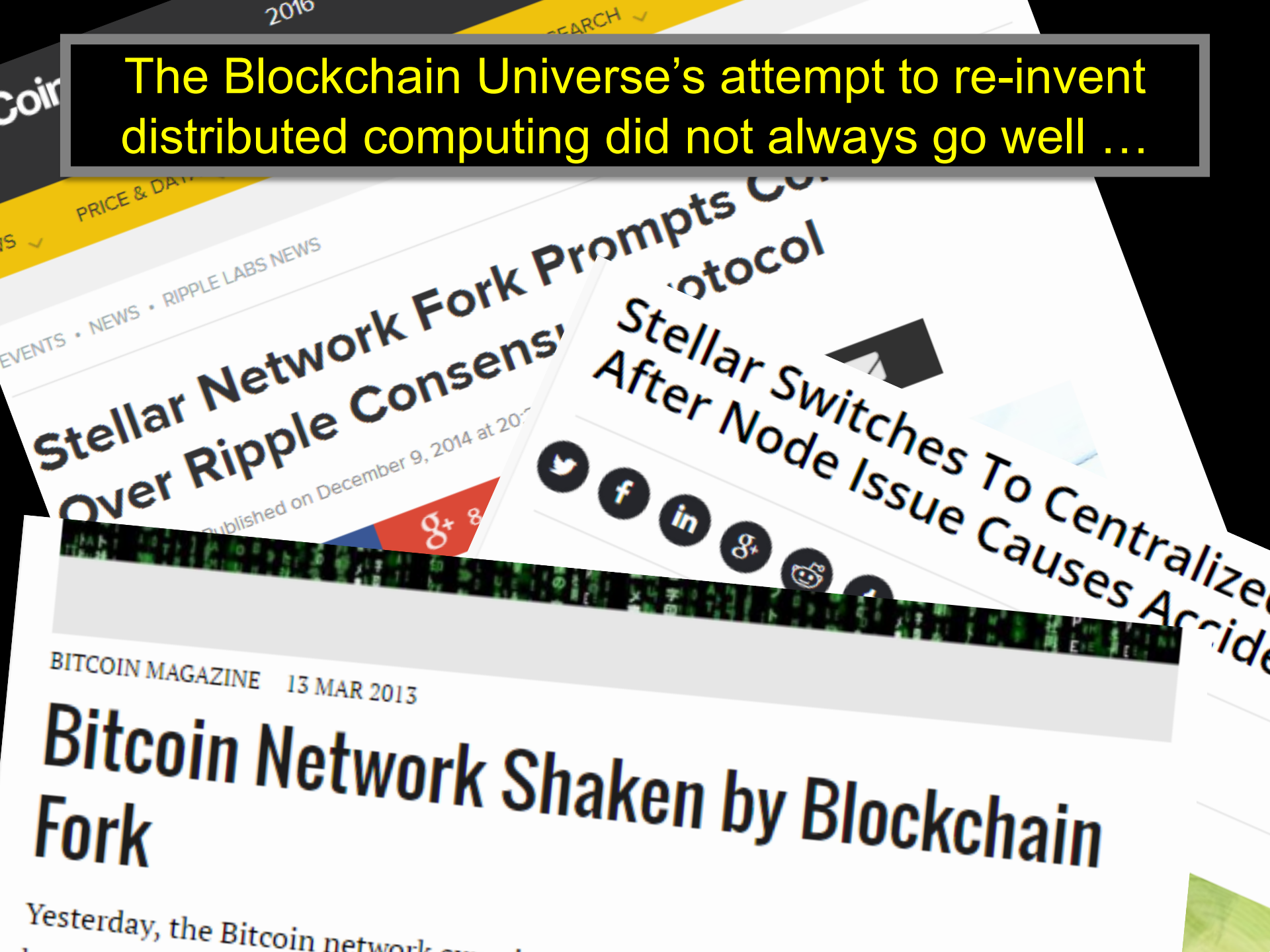


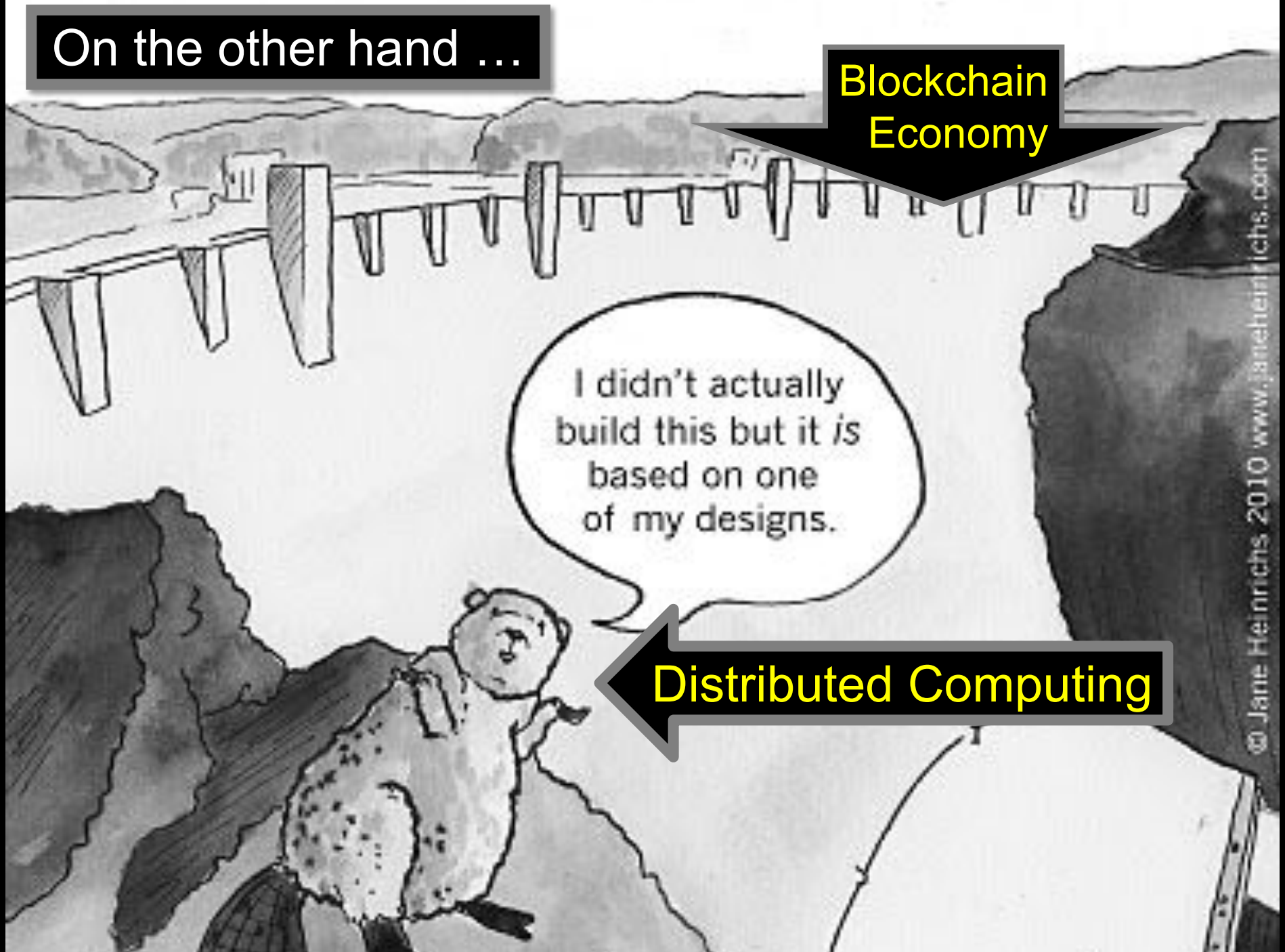
Consensus vs Proof of Work

Concurrent objects vs “Smart Contracts”


Distributed Computing!
Blockchain!
More alike than you would think
Good Kirk & Spock
Evil Kirk & Spock

The Blockchain Universe's attempt to re-invent distributed computing did not always go well …




On the other hand …
Blockchain Economy
I didn't actually build this but it *is* based on one of my designs.
Distributed Computing
© Jane Heinrichs 2010 www.janeheinrichs.com

Abstraction: Distributed Ledger

Cash

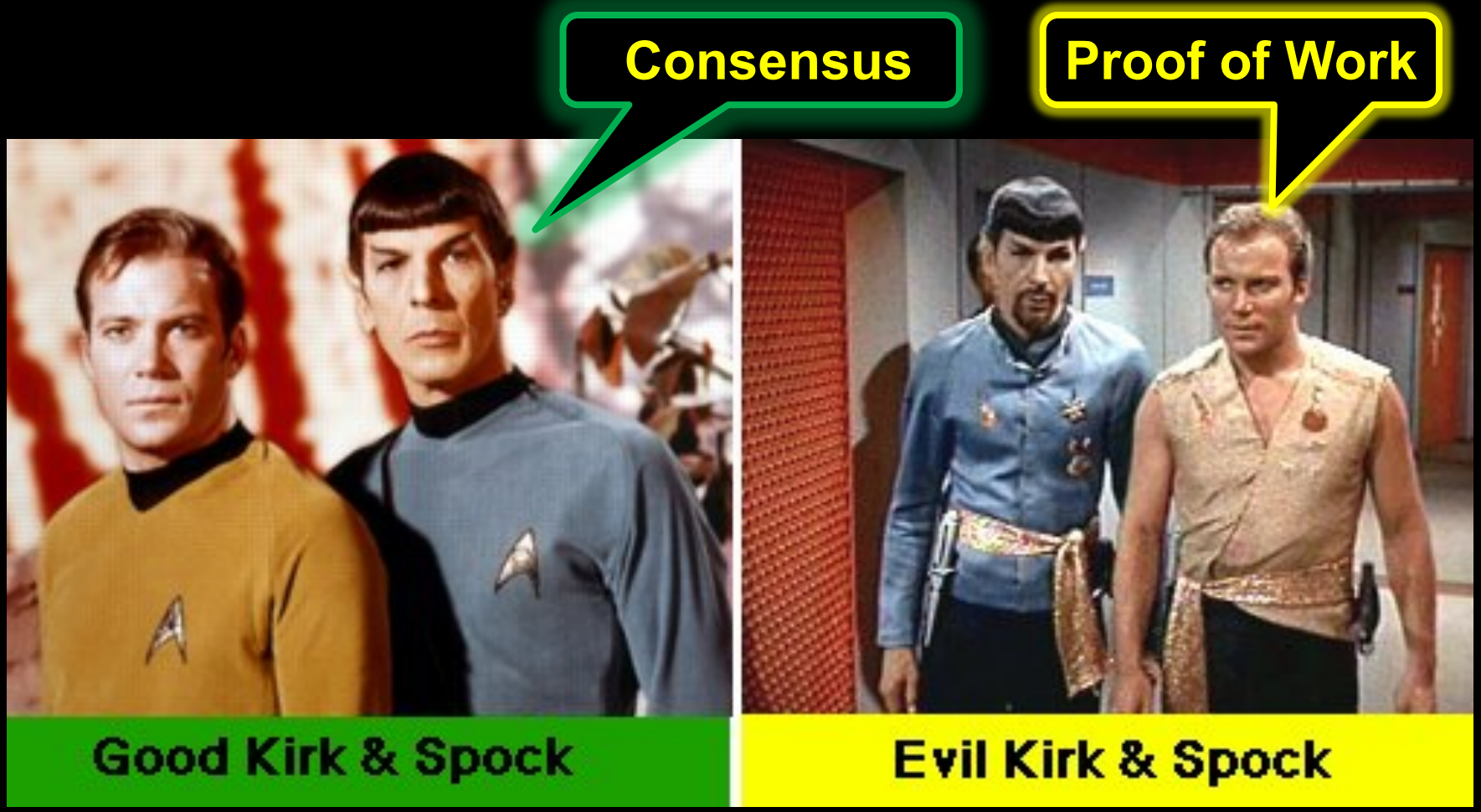
Date	Description	Increase	Decrease	Balance
Jan. 1, 20X3	Balance forward			$ 50,000
Jan. 2, 20X3	Collected receivable	$ 10,000		60,000
Jan. [illegible]	Cash sale	5,000		65,000
Jan. 5, 20X3	Paid rent		7,000	58,000
Jan. 7, 20X3	Paid salary		[illegible]	55,000
Jan. [illegible]	Cash sale	4,000		59,000
Jan. 8, 20X3	Paid bills		2,000	57,000
Jan. 10, 20X3	Paid tax		1,000	56,000
Jan. 12, 20X3	Collected receivable	7,000		63,000

Append-only list of events

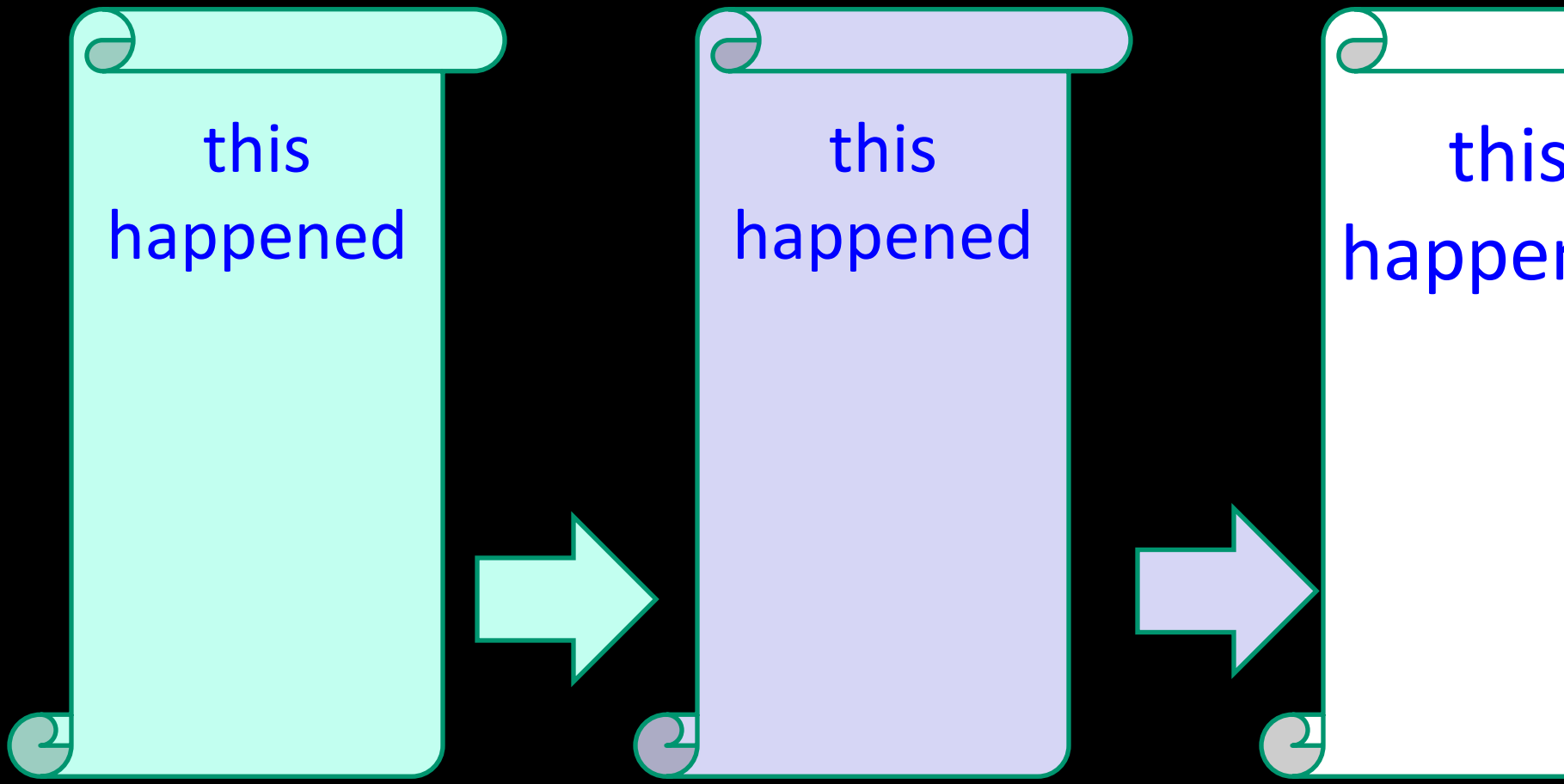
Not just financial

Everyone agrees on content

Tamper-proof!


Consensus
Proof of Work
Good Kirk & Spock
Evil Kirk & Spock

Literally

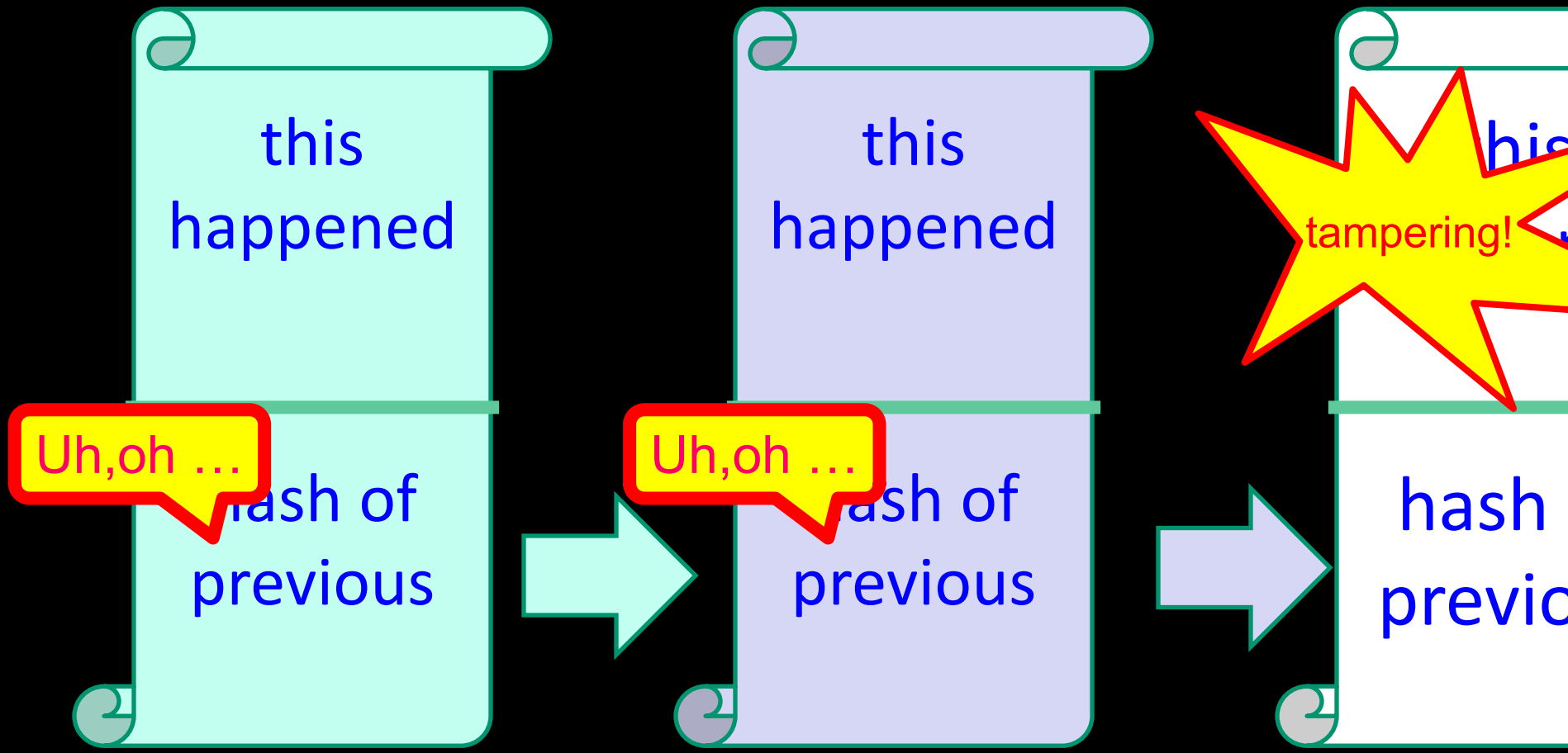


Cryptographic Hash Functions

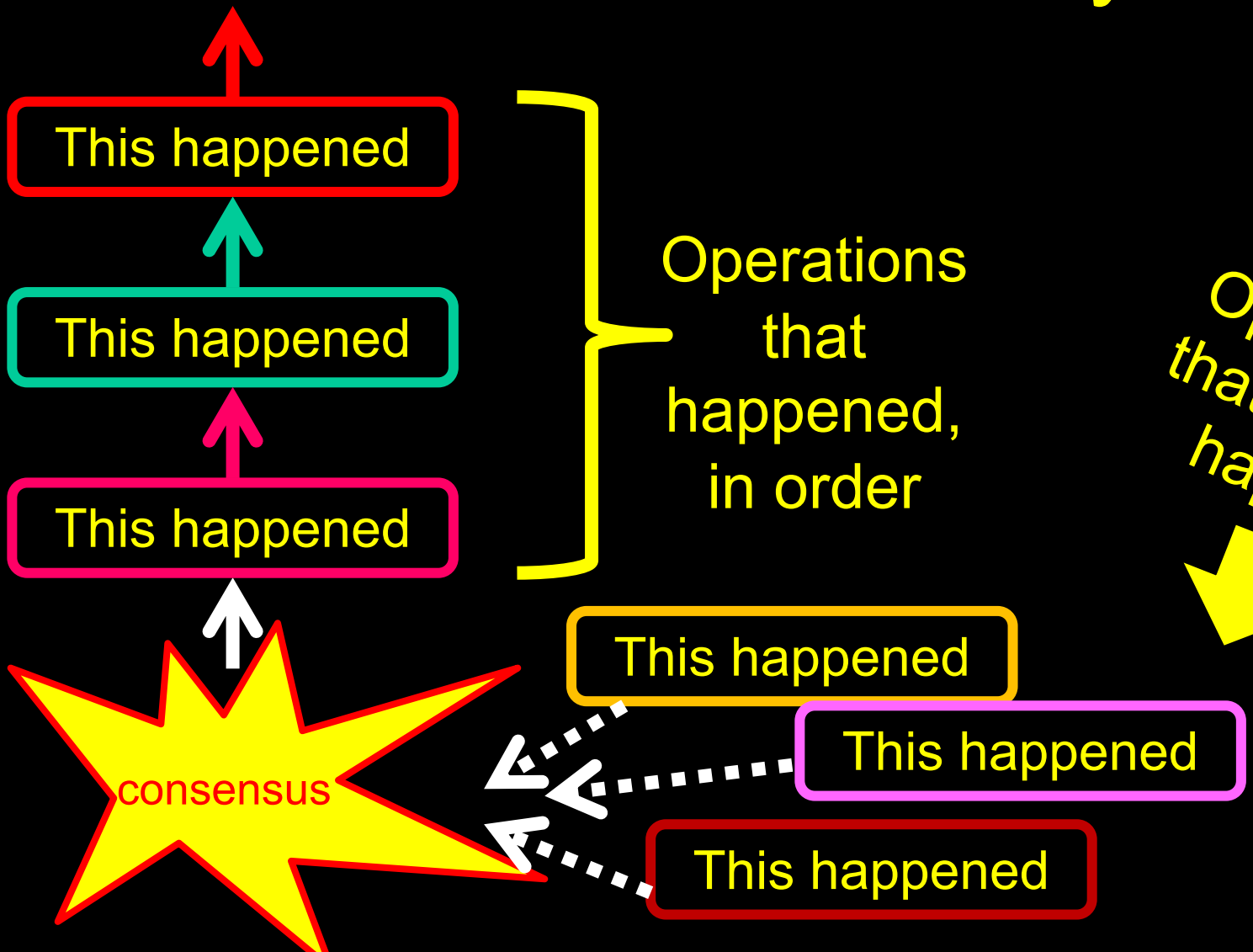
Easy

Hard

More Literally



Even More Literally



MOTHERBOARD

BLOCKCHAINS | By Daniel Oberhaus | Aug 27 2018, 4:19pm

Th s Oldest Blockchain Has Been Hiding In the N w Y k Times Since 1995

Hash documents

Store documents on server …

Every day, publish hashs to …

This really gives a new meaning to the “paper

The New York Times Lost & Found

NOTICES & LOST AND FOUND

(5100-5102)

Universal Registry Entries:
Zone 2 -

dS8492cgVOFAoP9kvE1XzMOrQ
HgEwzkVbVafNvIkUz99qvq8/ME
p5v9EFSG8XxzMBaIGQQ==

Zone 3 -

JnFCg+HCmvhj8GmmUP7VZna71
NgZup/RfuKUQNzCHWXMuqLK
durxHQV5pSHLqBGPRIv+mg==

These base64-encoded values represent the combined fingerprints of all digital records notarized by Surety between 2009-06-03Z 2009-06-09Z.

www.surety.com 571-748-5800

Alice has a frozen yogurt business

Her business is in trouble

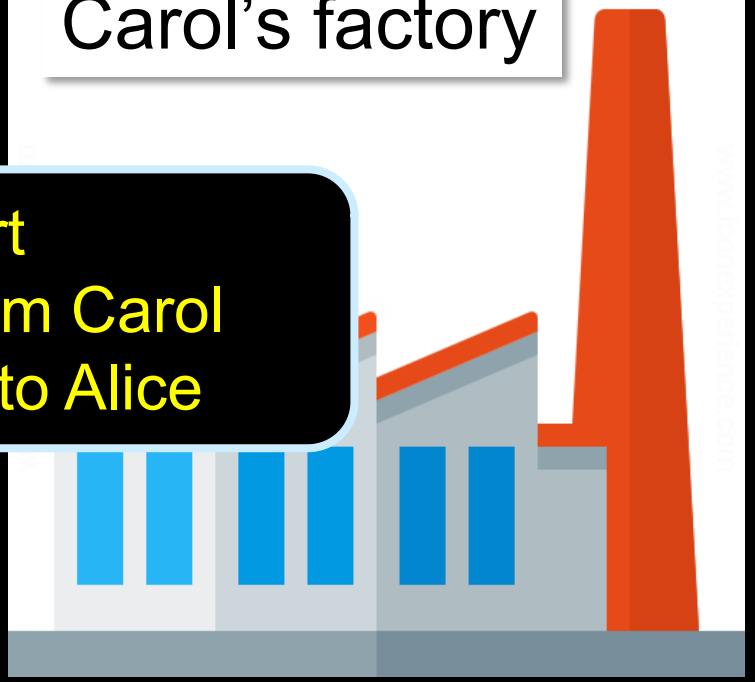
Shipments arrive melted

Alice's Supply Chain

Bob's truck

What Bob said!

Carol's factory



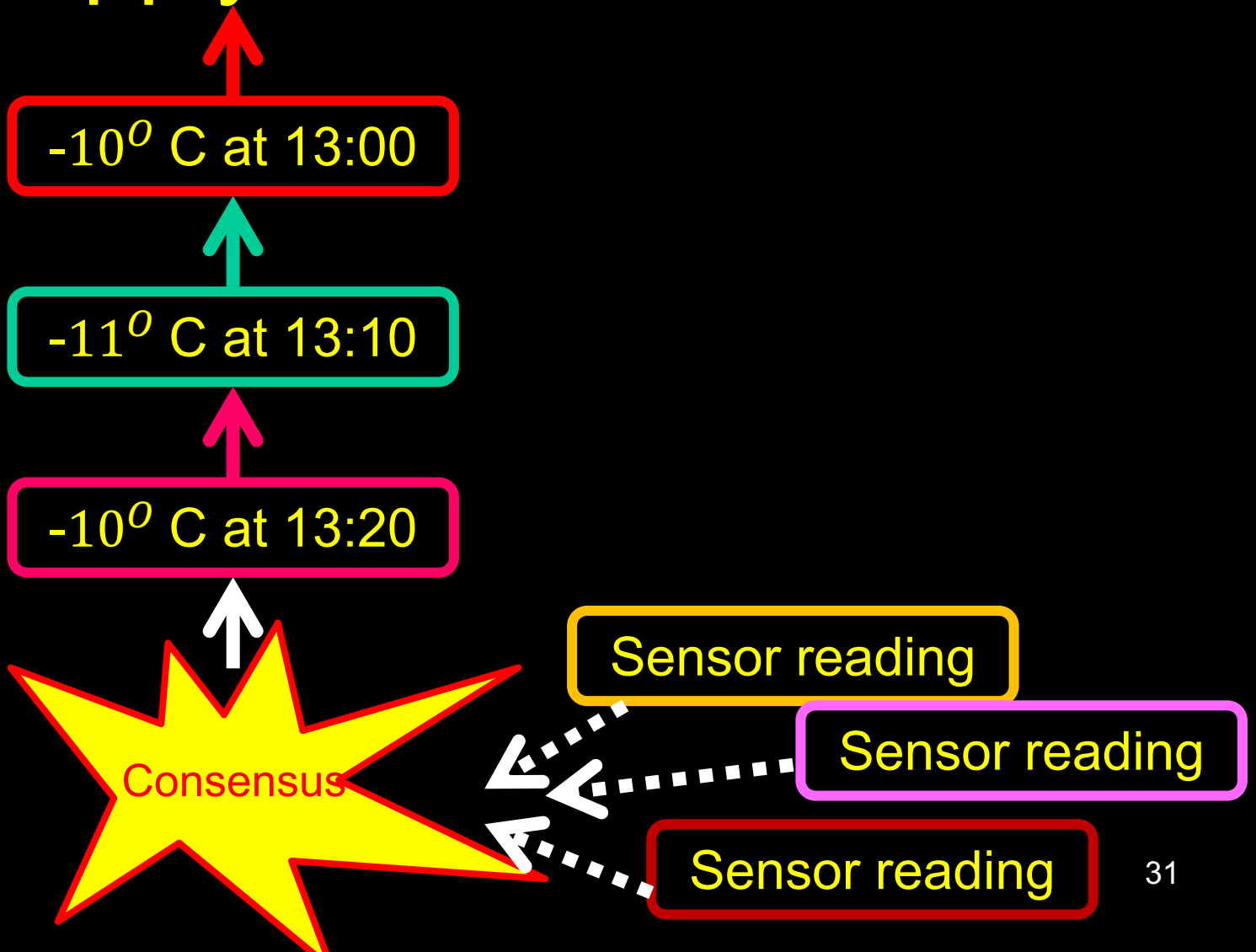
1. I never transported that yogurt
2. It was melted when I got it from Carol
3. It was OK when I delivered it to Alice

Ledger in Cloud

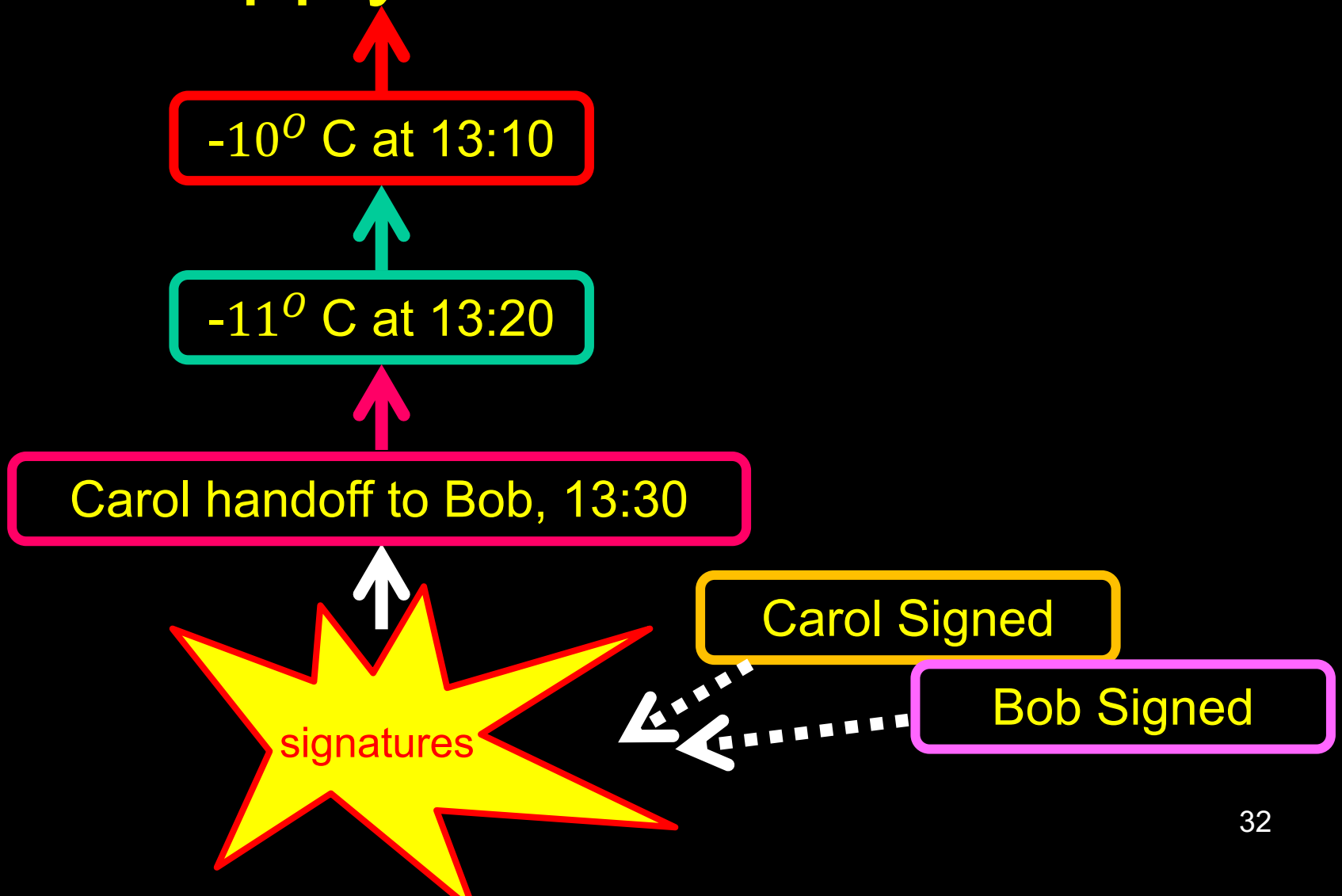
Bob and Carol

Sensors

Supply Chain Blockchain



Supply Chain Blockchain



Alice sells her frozen yogurt business…

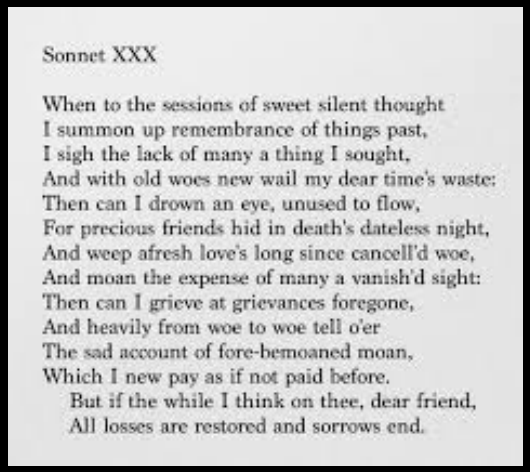
And decides to open a restaurant

But rents are high and VCs are greedy …

So she decides to raise money by …

Discount meals when restaurant opens

Alice's public key



Sonnet XXX

When to the sessions of sweet silent thought
I summon up remembrance of things past,
I sigh the lack of many a thing I sought,
And with old woes new wail my dear time's waste:
Then can I drown an eye, unused to flow,
For precious friends hid in death's dateless night,
And weep afresh love's long since cancell'd woe,
And moan the expense of many a vanish'd sight:
Then can I grieve at grievances foregone,
And heavily from woe to woe tell o'er
The sad account of fore-bemoaned moan,
Which I new pay as if not paid before.
But if the while I think on thee, dear friend,
All losses are restored and sorrows end.

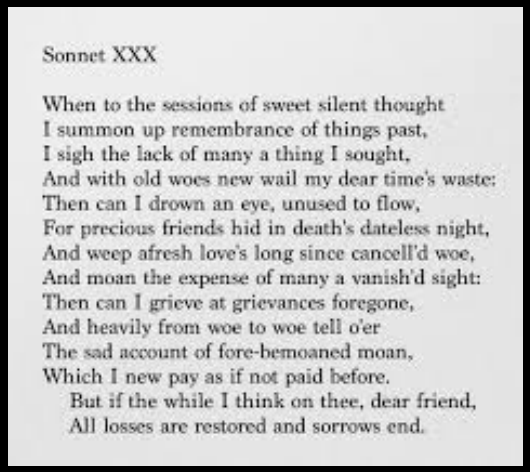
encrypt

decrypt

Alice's private key

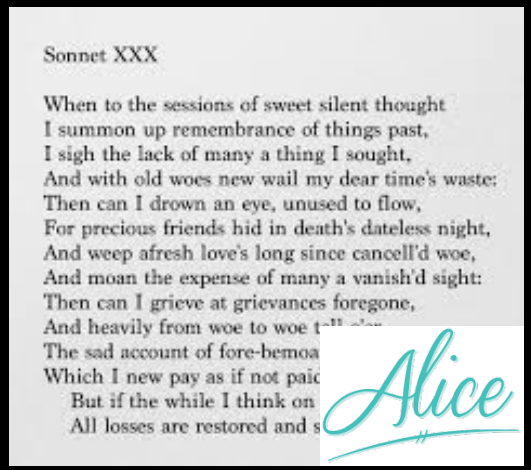
Only Alice can read

Alice's private key



encrypt

decrypt



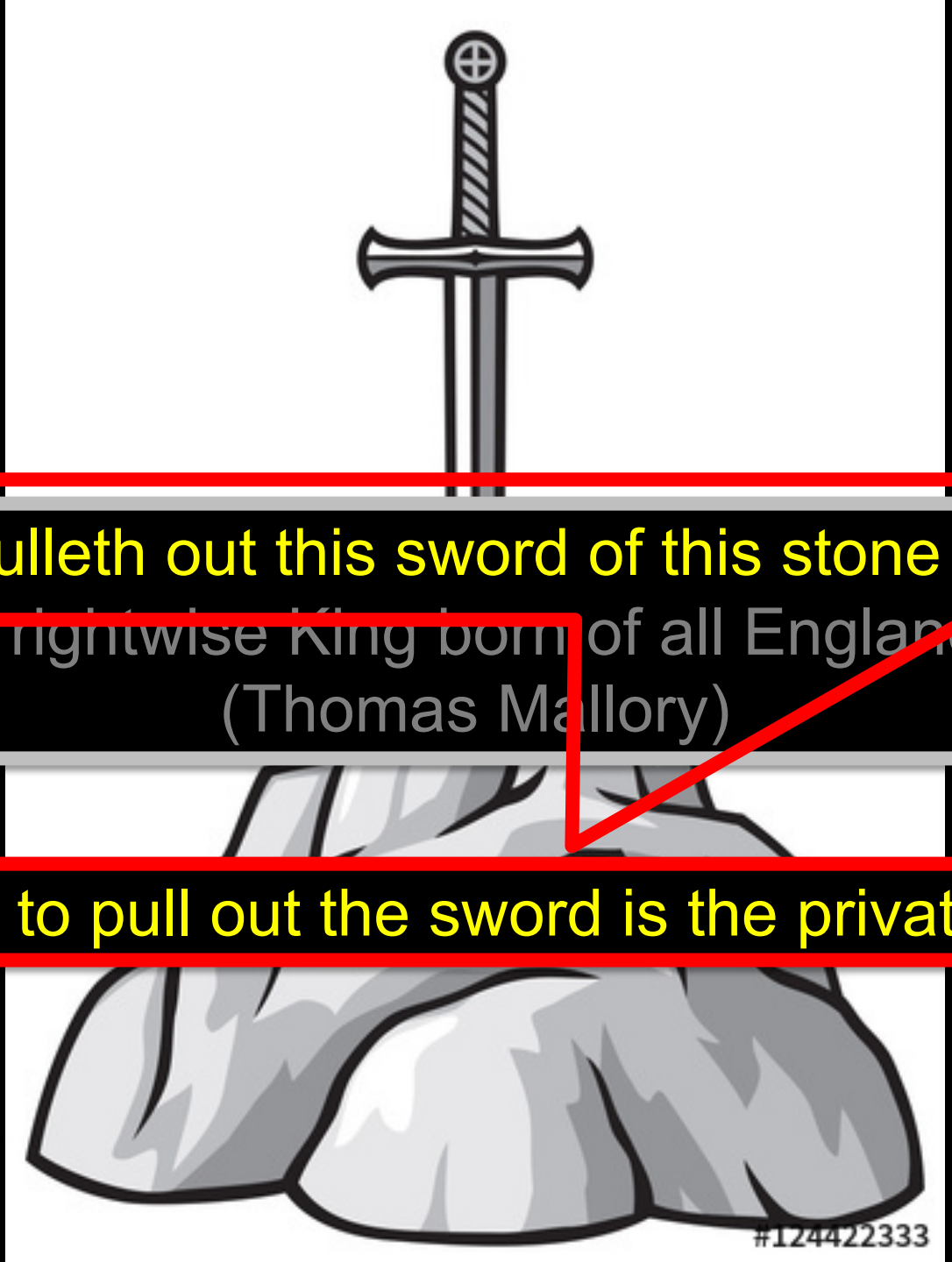
Alice's public key

Only Alice can sign

"Whoso pulleth out this sword of this stone and anvil is rightwise King born of all England"
(Thomas Mallory)

"Whoso pulleth out this sword of this stone and anvil is rightwise King born of all England"
(Thomas Mallory)

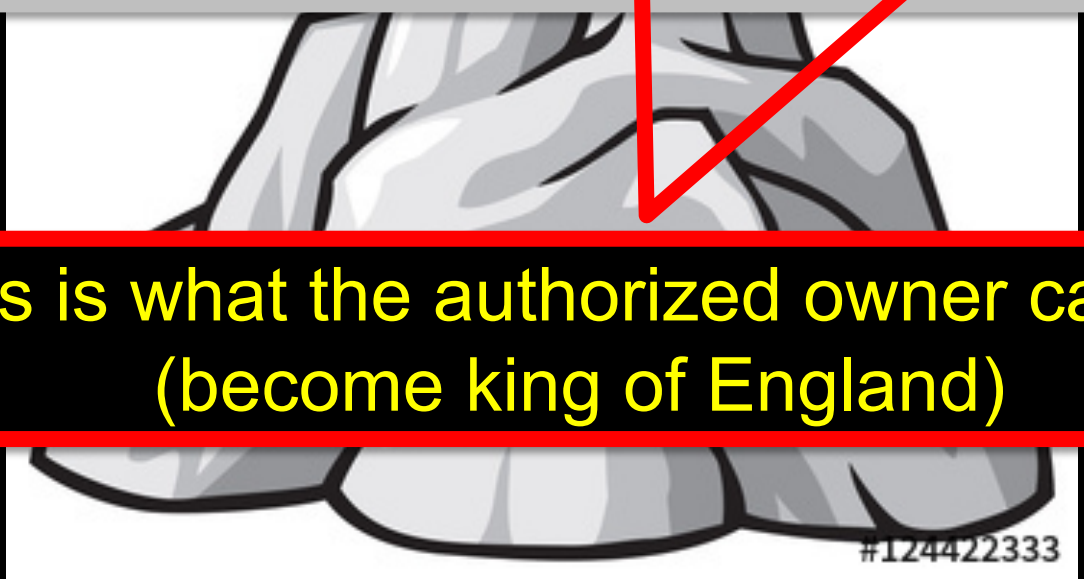
The sword is the public key



"Whoso pulleth out this sword of this stone and anvil is rightwise King born of all England"
(Thomas Mallory)

Ability to pull out the sword is the private key

"Whoso pulleth out this sword of this stone and anvil is rightwise King born of all England"
(Thomas Mallory)



This is what the authorized owner can do (become king of England)

I, The Ledger …

Anyone who knows the *private* key matching the following *public* key owns one of Alice's *cryptocoupons*: …

I, The Ledger …

Anyone who knows the *private* key matching the following *public* key owns one of Alice's *cryptocoupons*: …

Being on the ledger makes this entry authoritative

I, The Ledger …

Anyone who knows the *private* key matching **the following *public* key** owns one of Alice's *cryptocoupons*: …

The public key allows owner to be recognized

I, The Ledger …

Anyone who knows the *private* key matching the following *public* key owns one of Alice's *cryptocoupons*: …

Knowledge of this private key conveys ownership

I, The Ledger …

Anyone who knows the *private* key matching the following *public* key … owns one of Alice's *cryptocoupons*:

This is what the authorized owner can do (establish ownership)

Spending a Coupon

I, the owner of the *private* key matching the 1st *public* key listed below do hereby transfer ownership of that coupon to the owner of the private key matching the 2nd public key: …

Spending a Coupon

I, the owner of the *private* key **matching the 1st *public* key listed below** do hereby transfer ownership of that coupon to the owner of the private key matching the 2nd public key: …

The public key allows owner to be recognized

Spending a Coupon

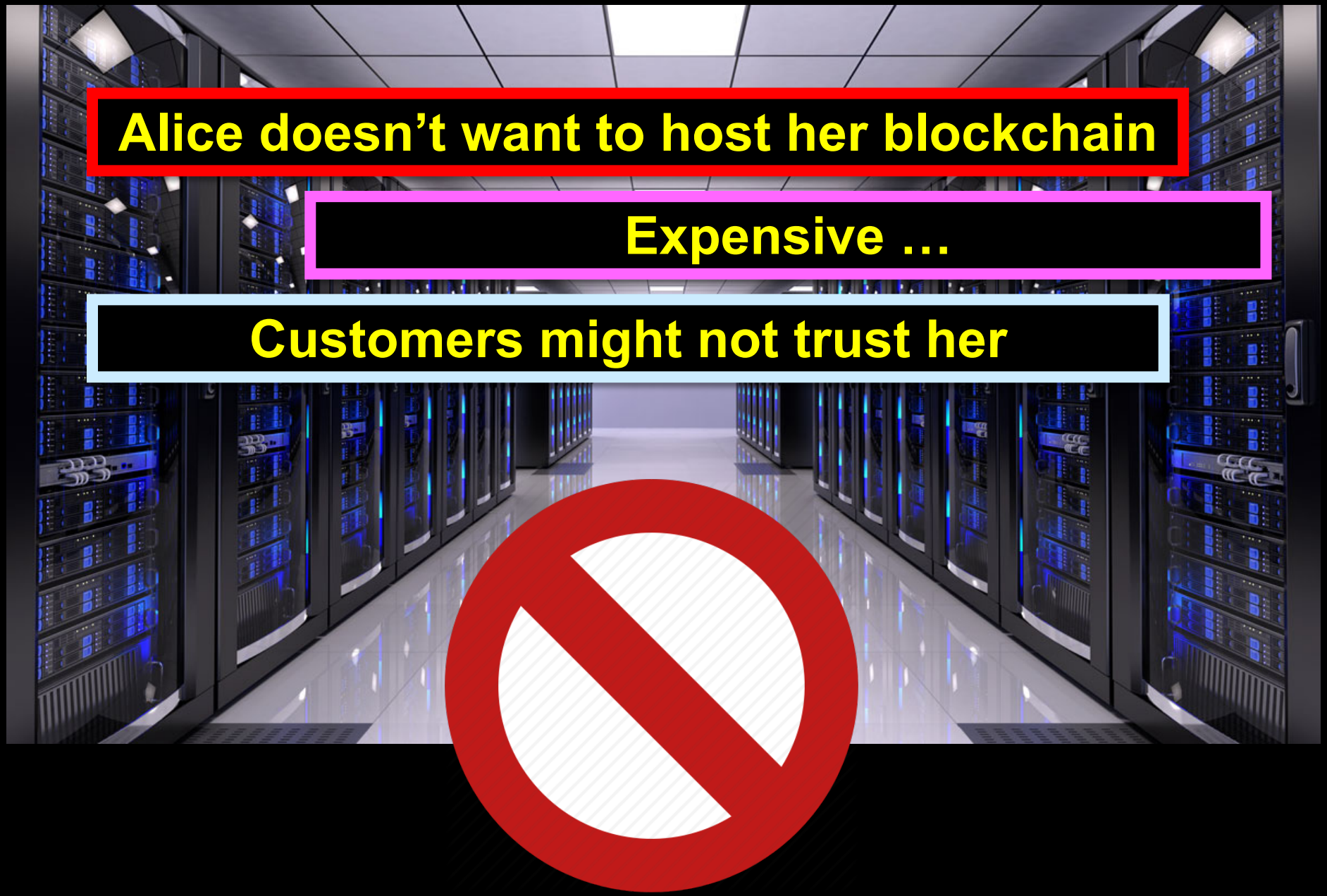
I, the owner of the *private* key matching the 1st *public* key listed below do hereby transfer ownership of that coupon to the owner of the private key matching the 2nd public key: …

Knowledge of this private key conveys ownership

Spending a Coupon

I, the owner of the *private* key matching the 1st *public* key listed below do hereby transfer ownership of that coupon to the owner of the private key matching the 2nd public key: …

This is what the authorized owner can do (transfer ownership to another public key)


Alice doesn’t want to host her blockchain
Expensive …
Customers might not trust her

The Genius of Blockchains

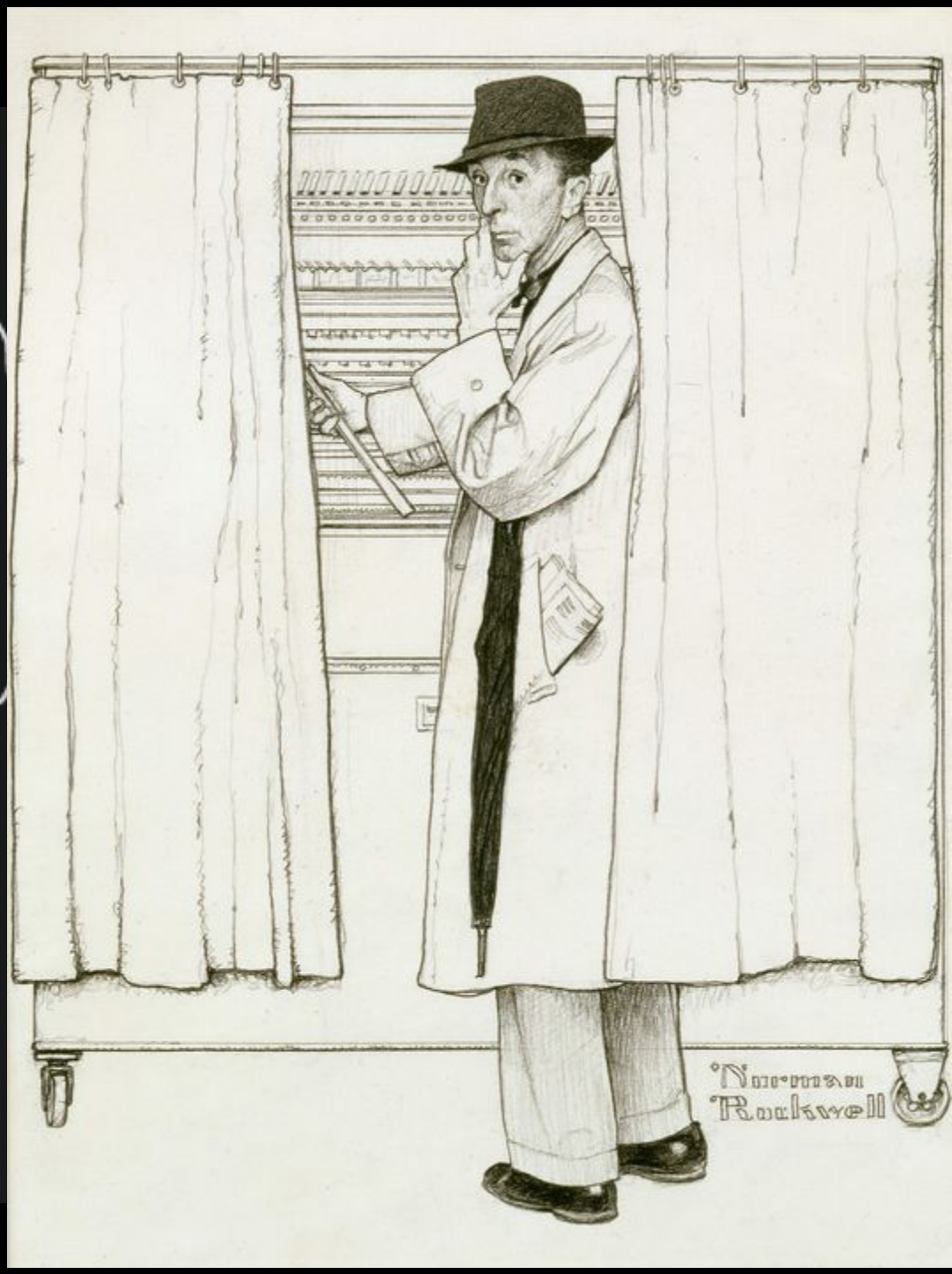
Who Controls the Blockchain?

Centralized

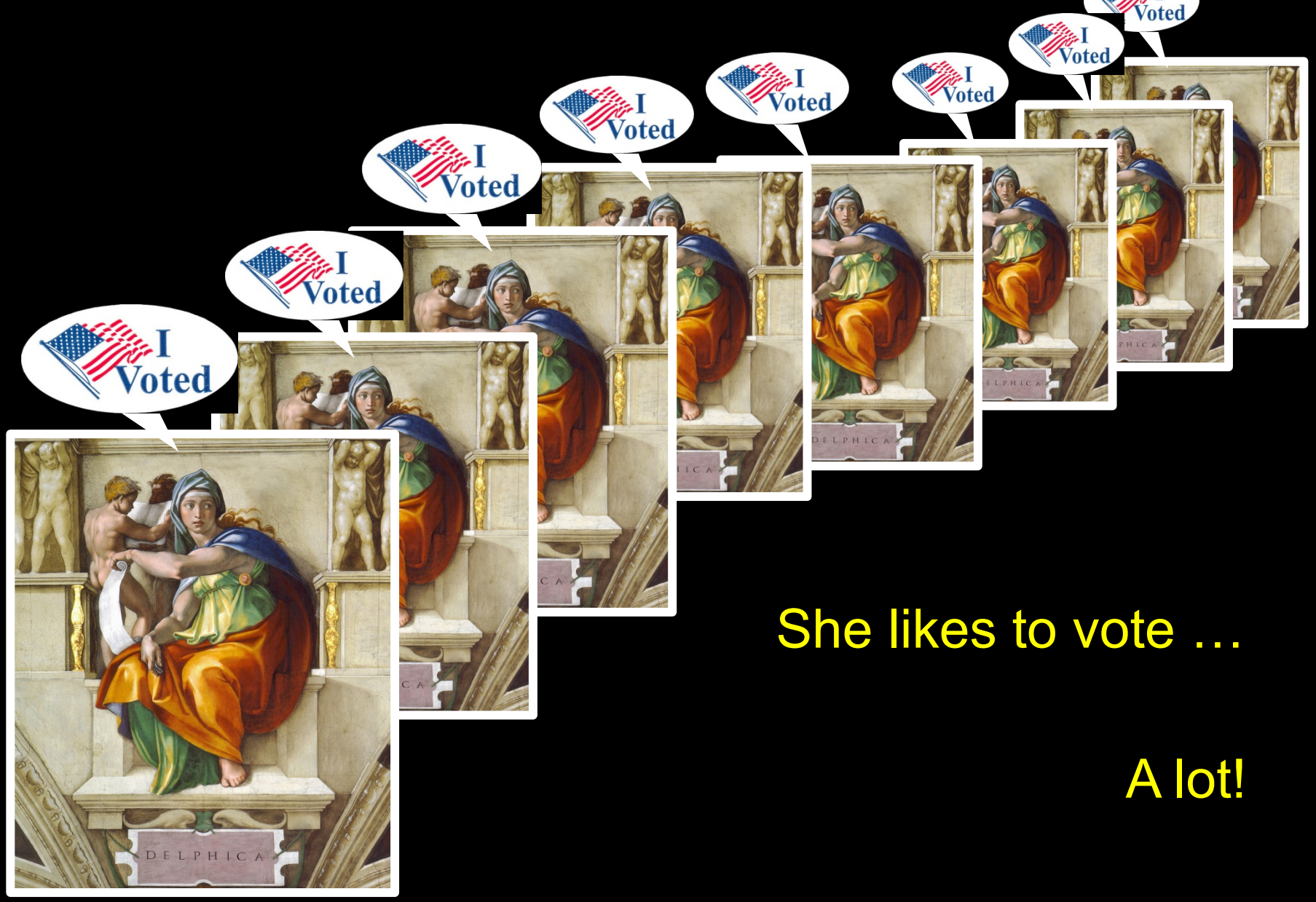
Decentralized

oh, wait …


Distributed
Consensus
requires voting!
GOOD


Norman
Rockwell

Oh yeah? Meet my friend, the Delphic Sibyl …

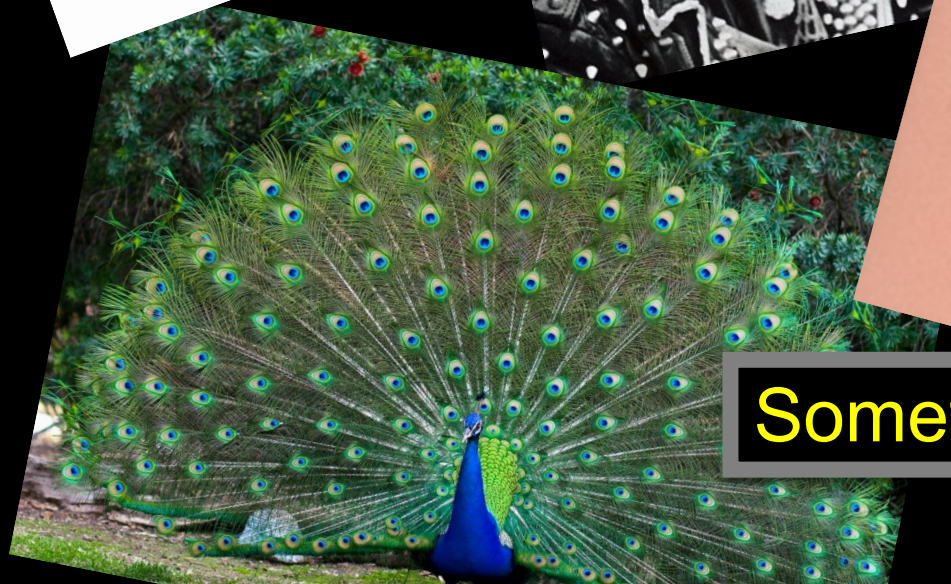


She likes to vote …

A lot!

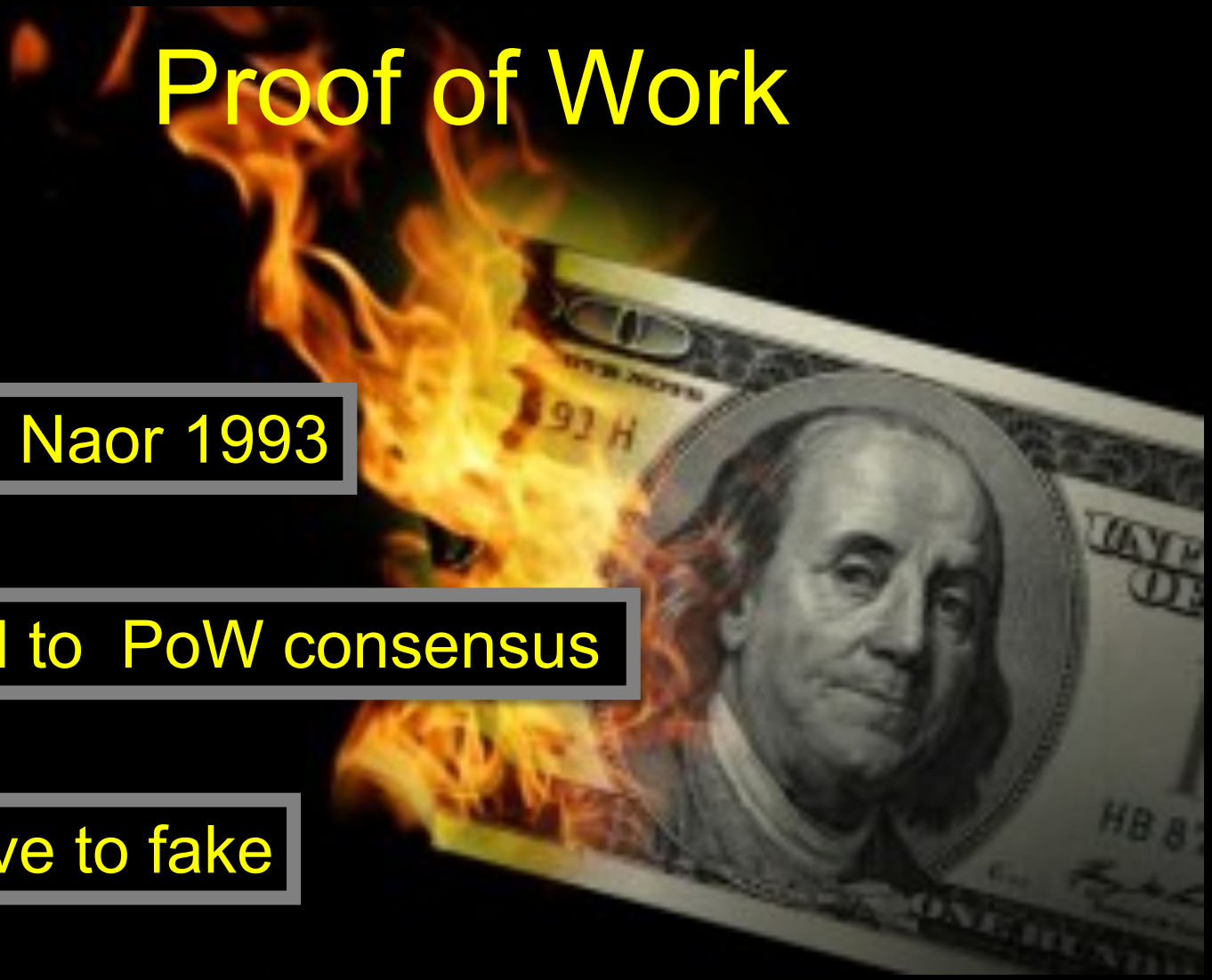
Need a signal that's hard to fake!

The solution: Costly signaling ….



Something hard to fake.

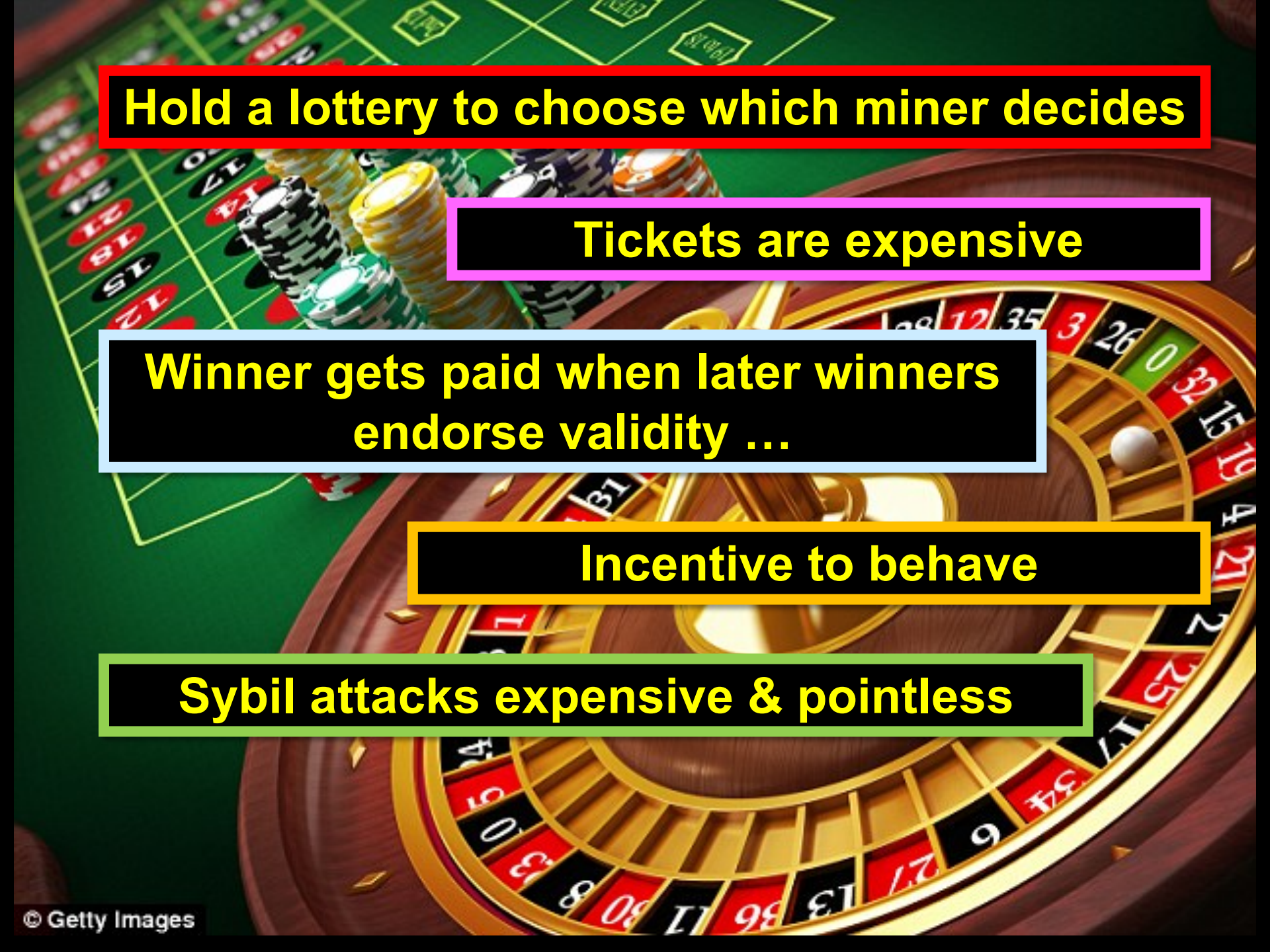
Proof of Work

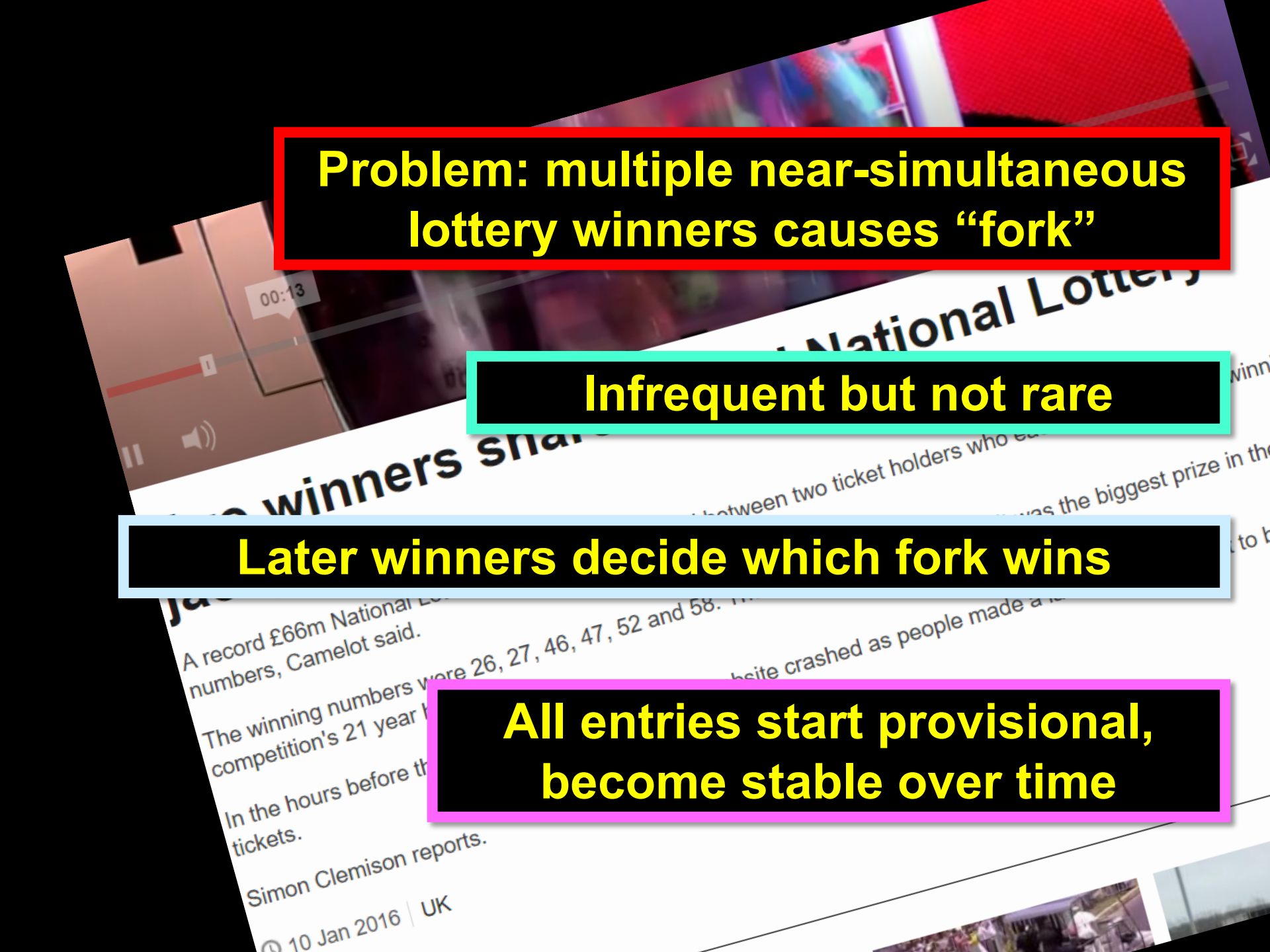


Dwork & Naor 1993

Adapted to PoW consensus

Expensive to fake


Hold a lottery to choose which miner decides
Tickets are expensive
Winner gets paid when later winners endorse validity …
Incentive to behave
Sybil attacks expensive & pointless
© Getty Images

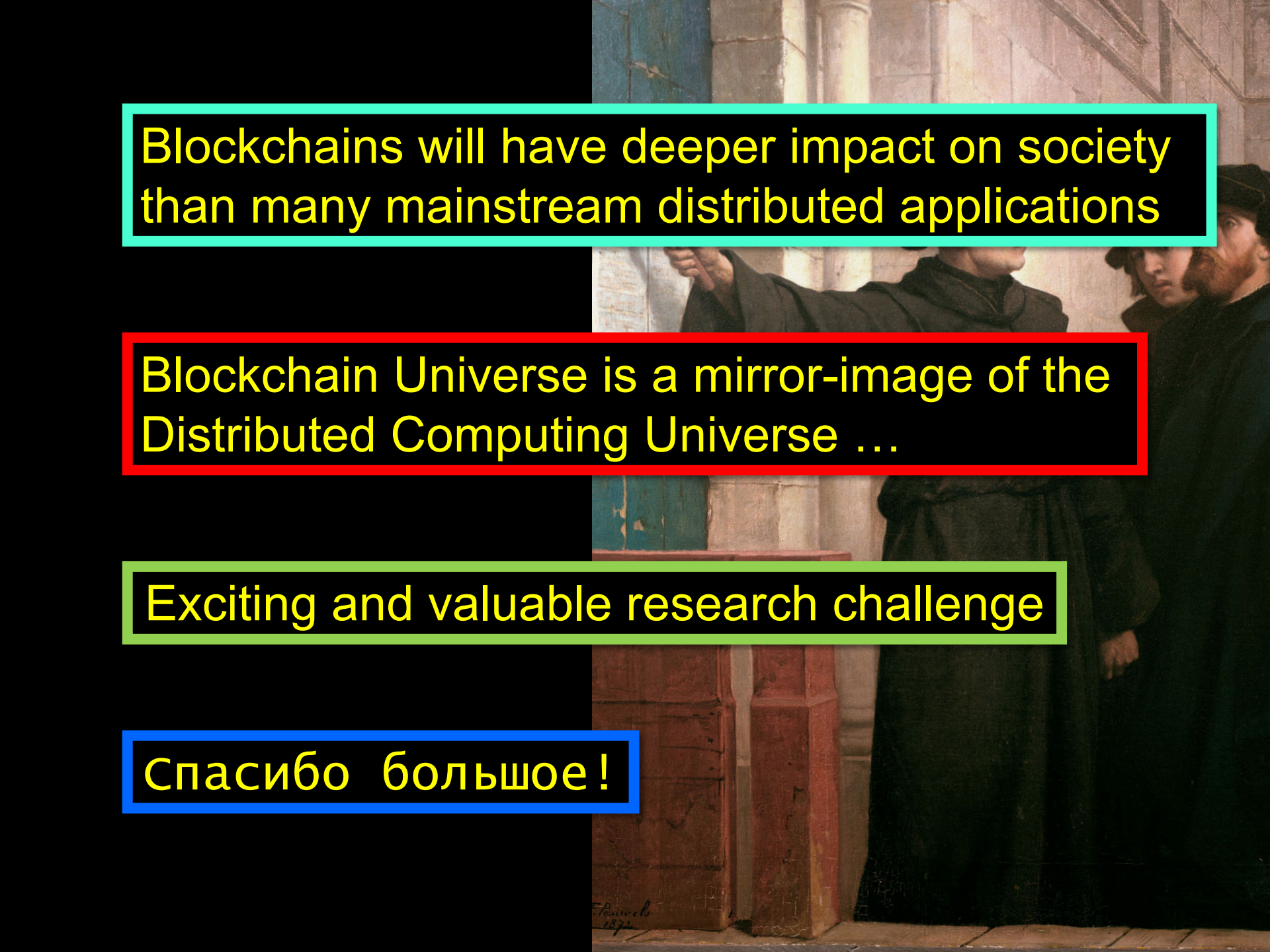

Problem: multiple near-simultaneous lottery winners causes “fork”
Infrequent but not rare
Later winners decide which fork wins
All entries start provisional, become stable over time
00:13
National Lotter
winners sha
between two ticket holders who
was the biggest prize in th
A record £66m National
numbers, Camelot said.
The winning numbers were 26, 27, 46, 47, 52 and 58.
competition's 21 year
In the hours before th
tickets.
bsite crashed as people made a
Simon Clemison reports.
10 Jan 2016 | UK

Consensus establishes a unique winner!

PoW Consensus might pick multiple winners every now and then

Consensus, once reached, is permanent!


PoW consensus emerges only over time



Blockchains will have deeper impact on society than many mainstream distributed applications

Blockchain Universe is a mirror-image of the Distributed Computing Universe …

Exciting and valuable research challenge

Спасибо большое!