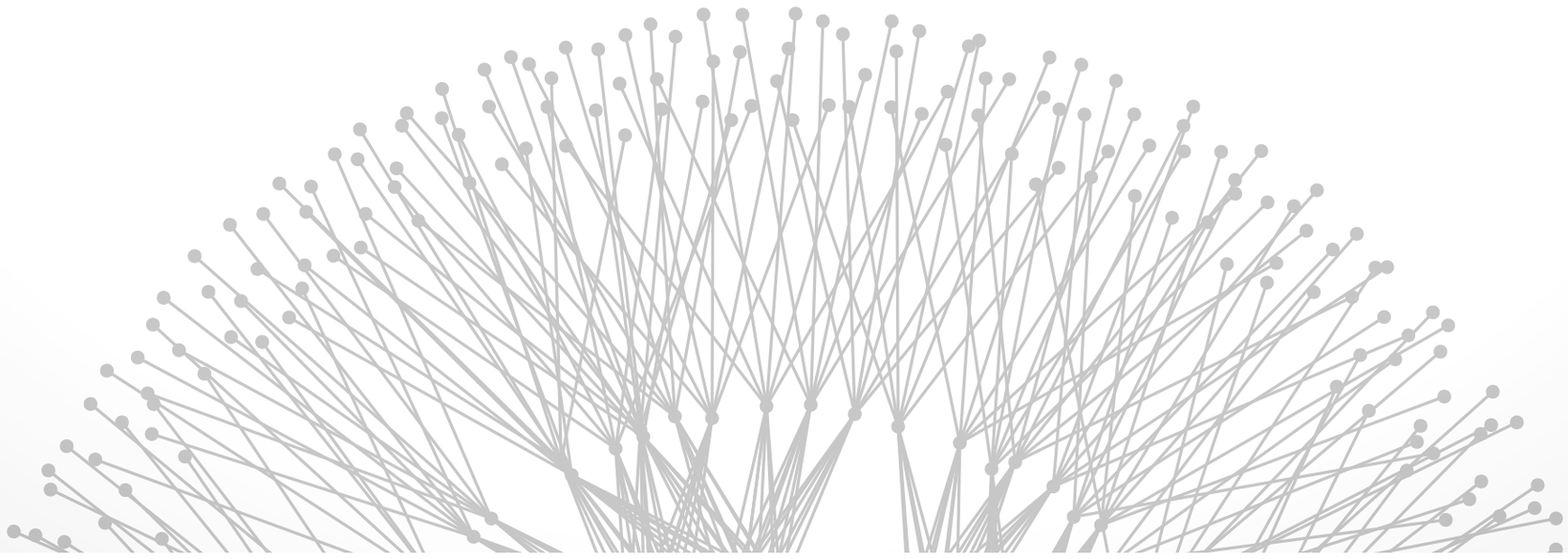
Blockchain Systems

UIUC CS 538 Fall 2017
Instructor: Mo Dong



Why are we talking about Blockchain?

An overwhelming 85% requests

There are some very interesting and important networking+system+theory challenges

Disclaimer: I hold a portfolio of cryptocurrency

Overview

What is blockchain?

Blockchain applications

What are some major challenges?

Bitcoin

The first “killer app” of blockchain

Electronic $$$

Electronic Currency System

A Key Value Store

Name	$$$
Alice	1000
Bob	300
Mo	1

Electronic Currency System

A Key Value Store

whose values are changed by transactions

Name	$$$
Alice	1000
Bob	300
Mo	1

Alice -> Mo
300

Electronic Currency System

A Key Value Store

whose values are changed by transactions

Name	$$$
Alice	700
Bob	300
Mo	301

Electronic Currency System

Today

Name	$$$
Alice	700
Bob	300
Mo	301

Electronic Currency System

Today

Centralized Banking System

Name	$$$
Alice	700
Bob	300
Mo	301

Electronic Currency System

Today

Name	$$$
Alice	700
Bob	300
Mo	301

Payment and settlement networks

Alice -> Mo
300

Build

Electronic $$$ without central authority

What’s the core of EC?

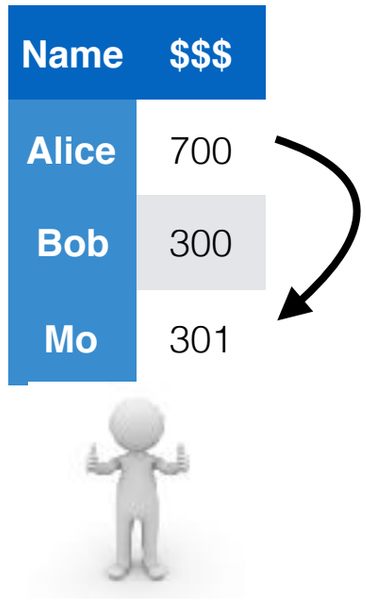
Name	$$$
Alice	700
Bob	300
Mo	301

What's the core of EC?

Essentially a consensus database or "ledger"

Name	$$$
Alice	700
Bob	300
Mo	301

What's the core of EC?

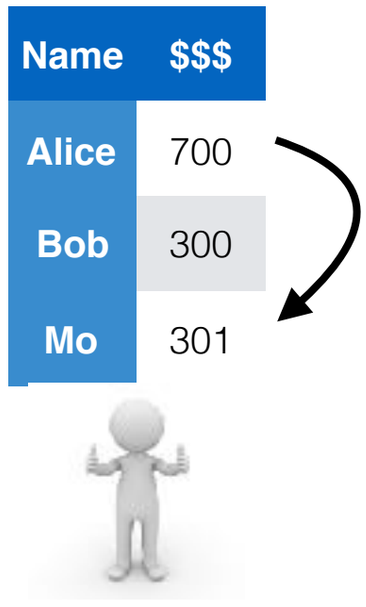


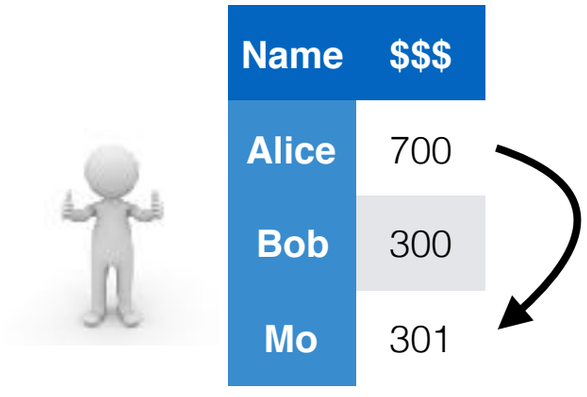
Name	$$$
Alice	700
Bob	300
Mo	301

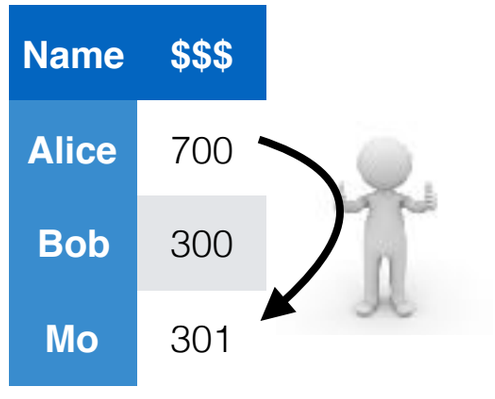
Name	$$$
Alice	700
Bob	300
Mo	301

What's the core of EC?

Large-scale Key-value Consensus Without Trust







Challenge 1: Validity of Tx

Name	$$$
Alice	700
Bob	300
Mo	301

Alice -> Mo 1

Alice

Alice -> Bob 700

Bob

Name	$$$
Alice	700
Bob	300
Mo	301

Name	$$$
Alice	700
Bob	300
Mo	301

Alice -> Mo 700

Mo

Challenge 1: Validity of Tx

Use private-public-key to sign txs

Name	$$$
Alice	700
Bob	300
Mo	301

Alice -> Mo 1

Alice

Alice -> Bob 700

Bob

Name	$$$
Alice	700
Bob	300
Mo	301

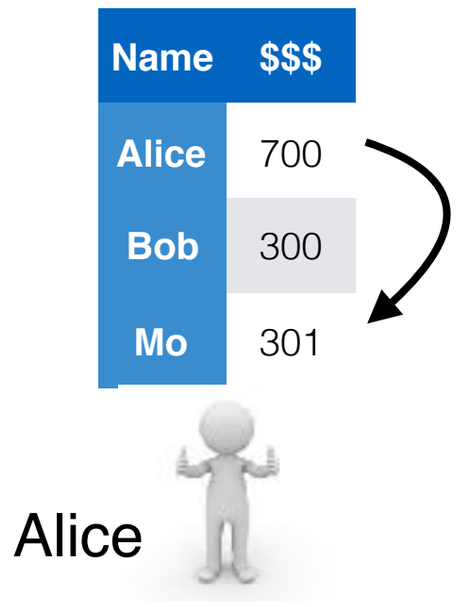
Name	$$$
Alice	700
Bob	300
Mo	301

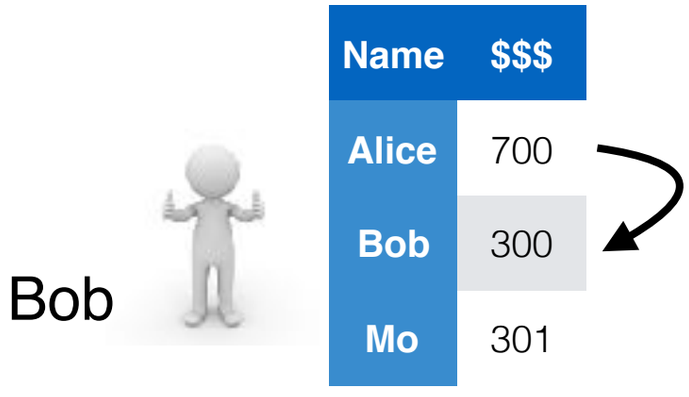
Alice -> Mo 700

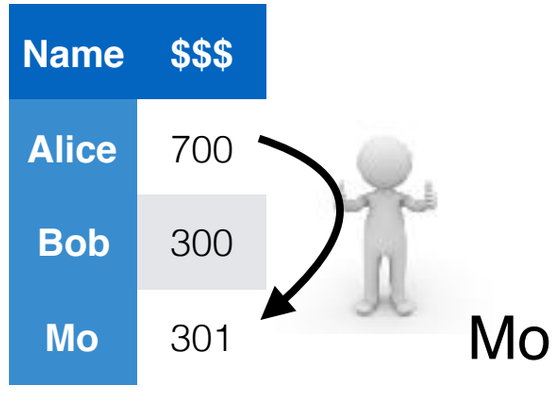
Mo

Challenge 2: IC Consensus

Paxos?Raft?



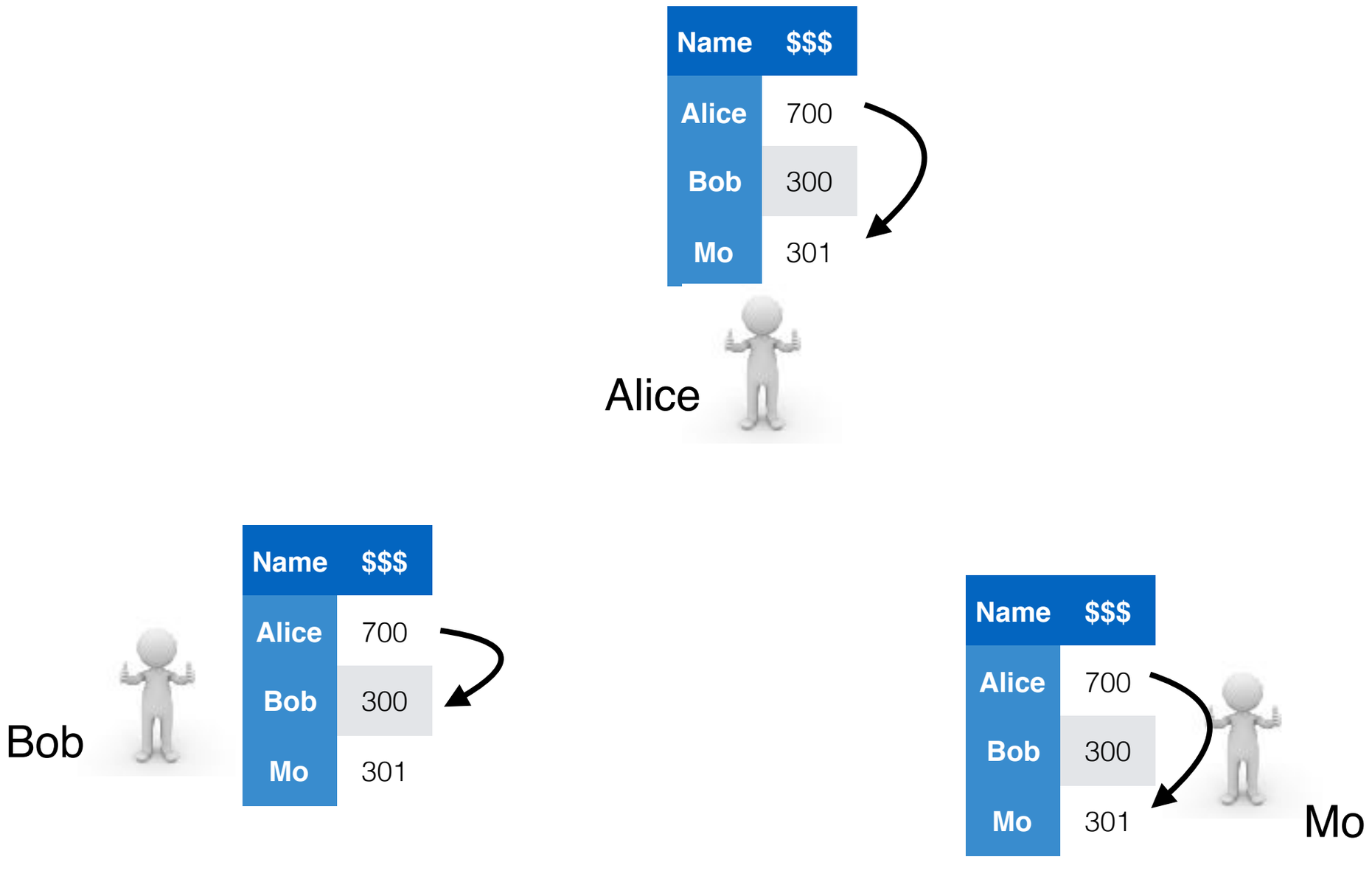




Challenge 2: IC Consensus

Paxos?Raft?

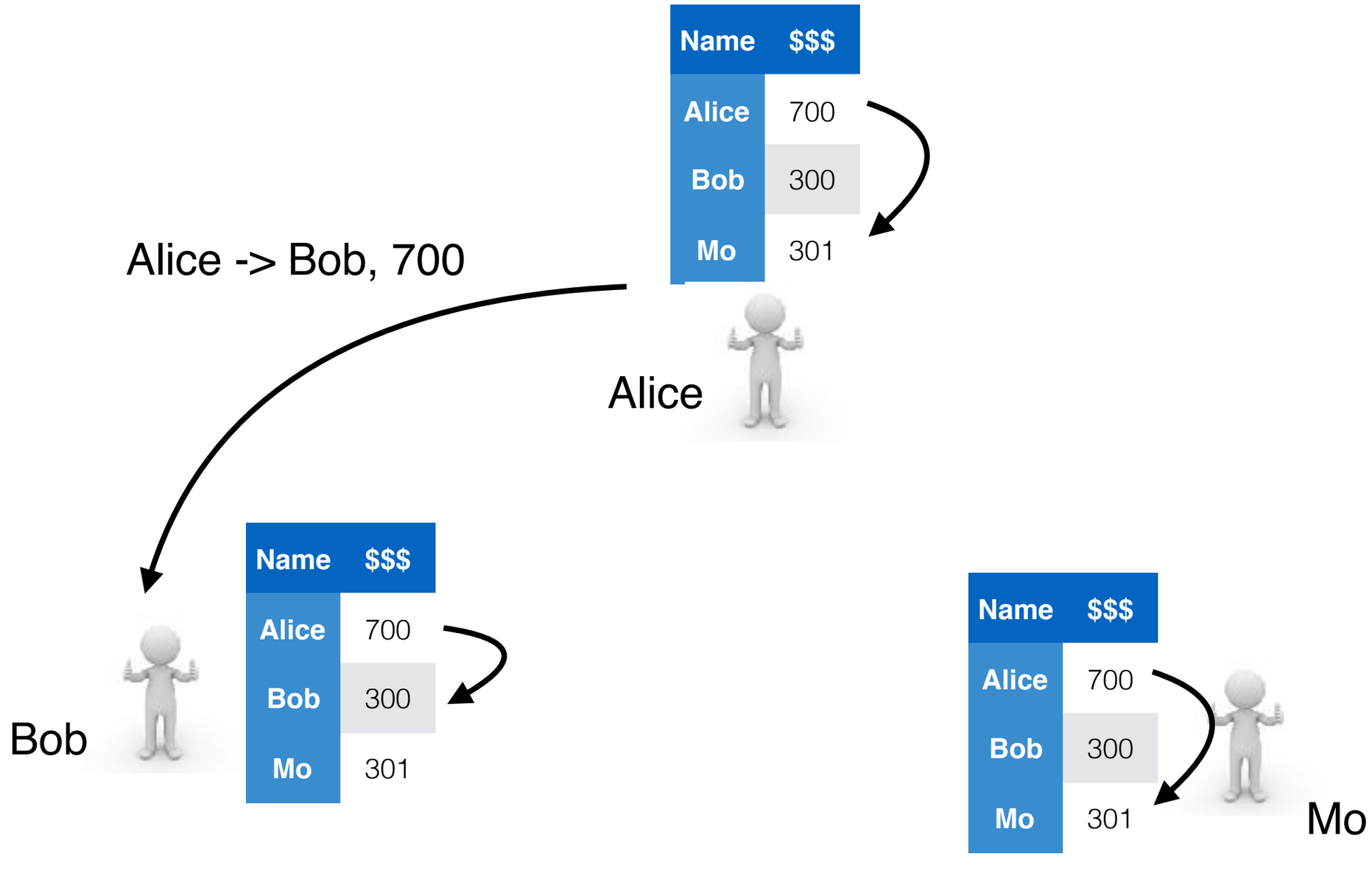
Malicious parties!



Challenge 2: IC Consensus

Paxos?Raft?

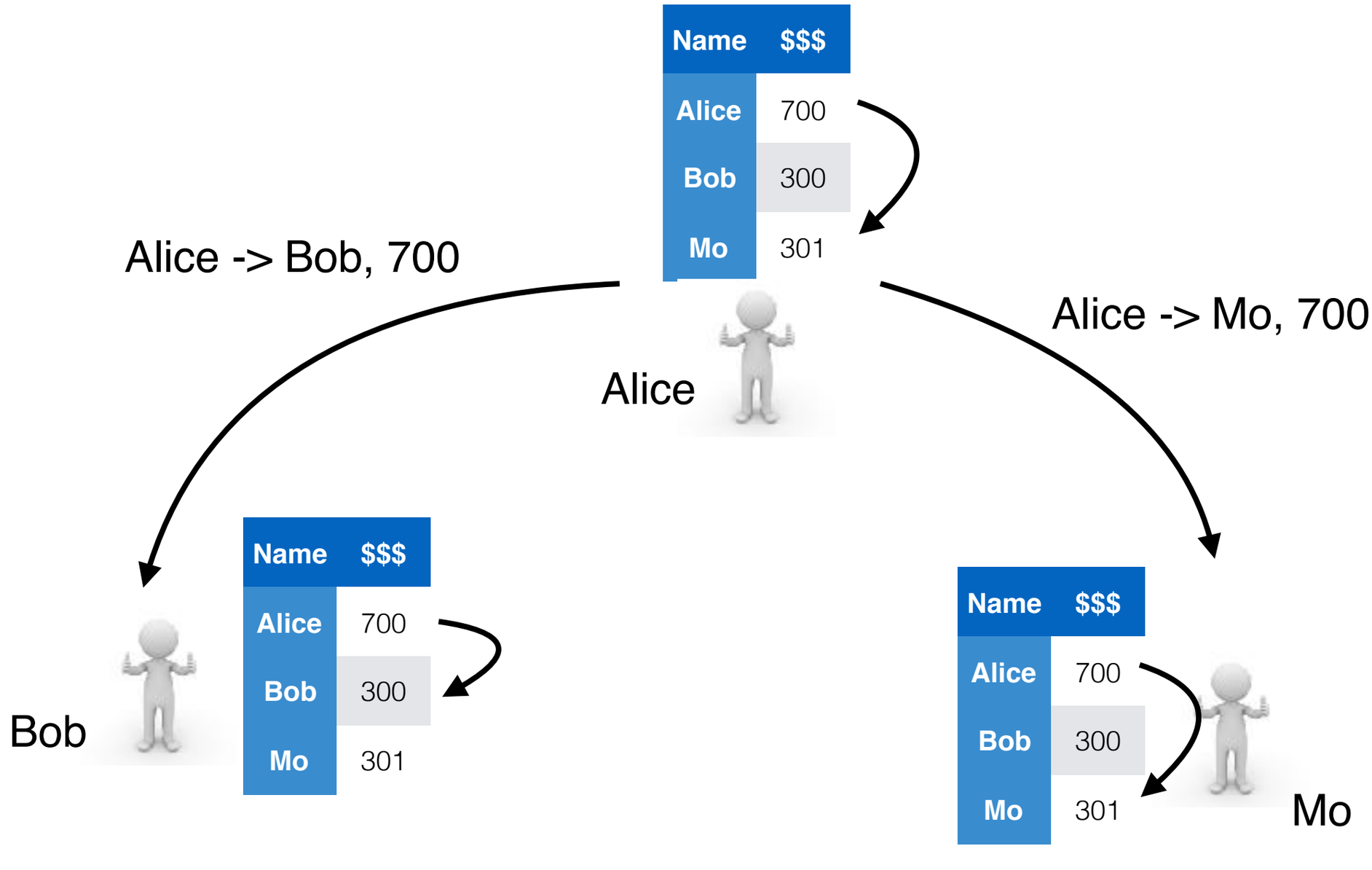
Malicious parties!



Challenge 2: IC Consensus

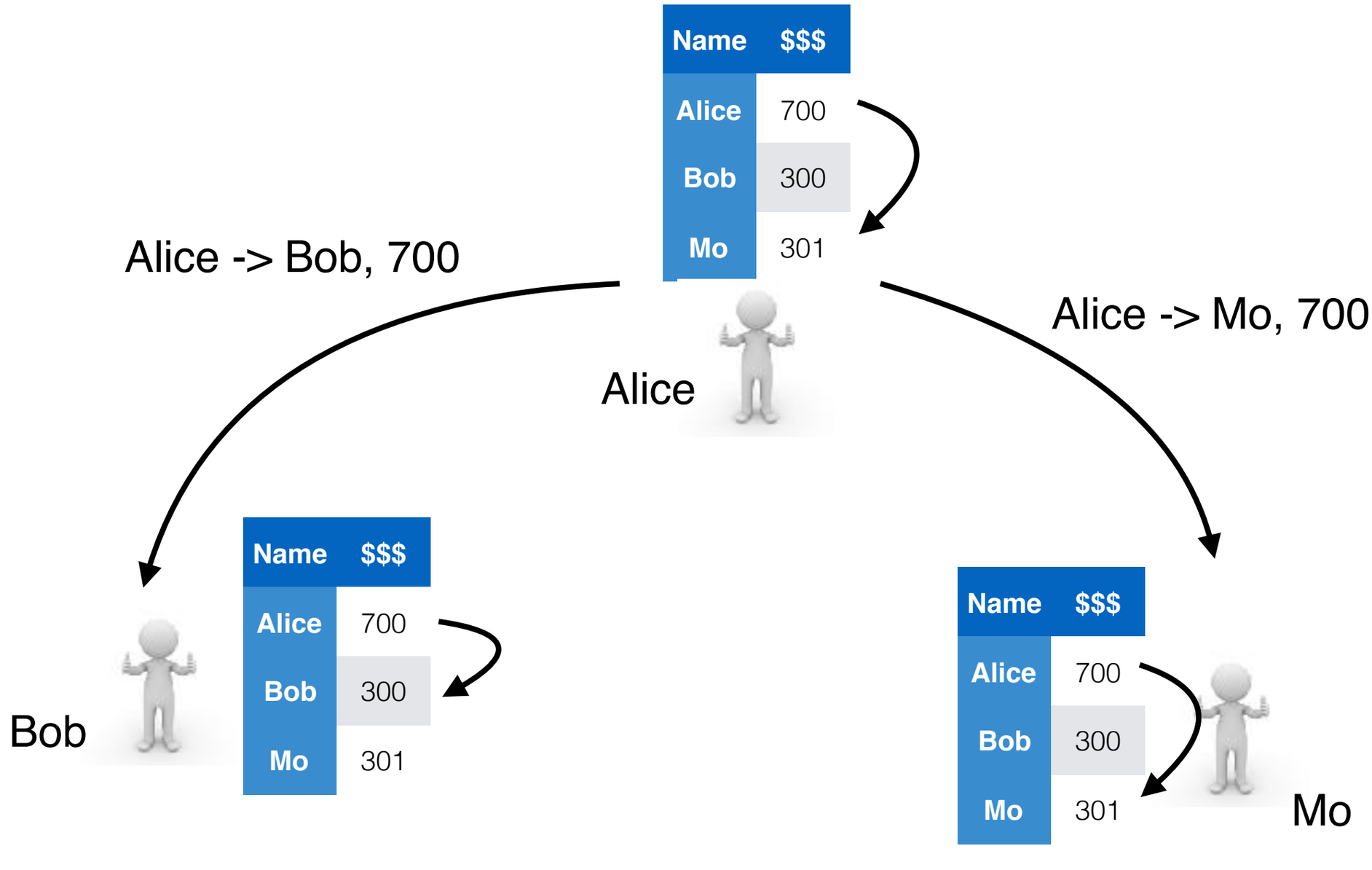
Paxos?Raft?

Malicious parties!



Challenge 2: IC Consensus

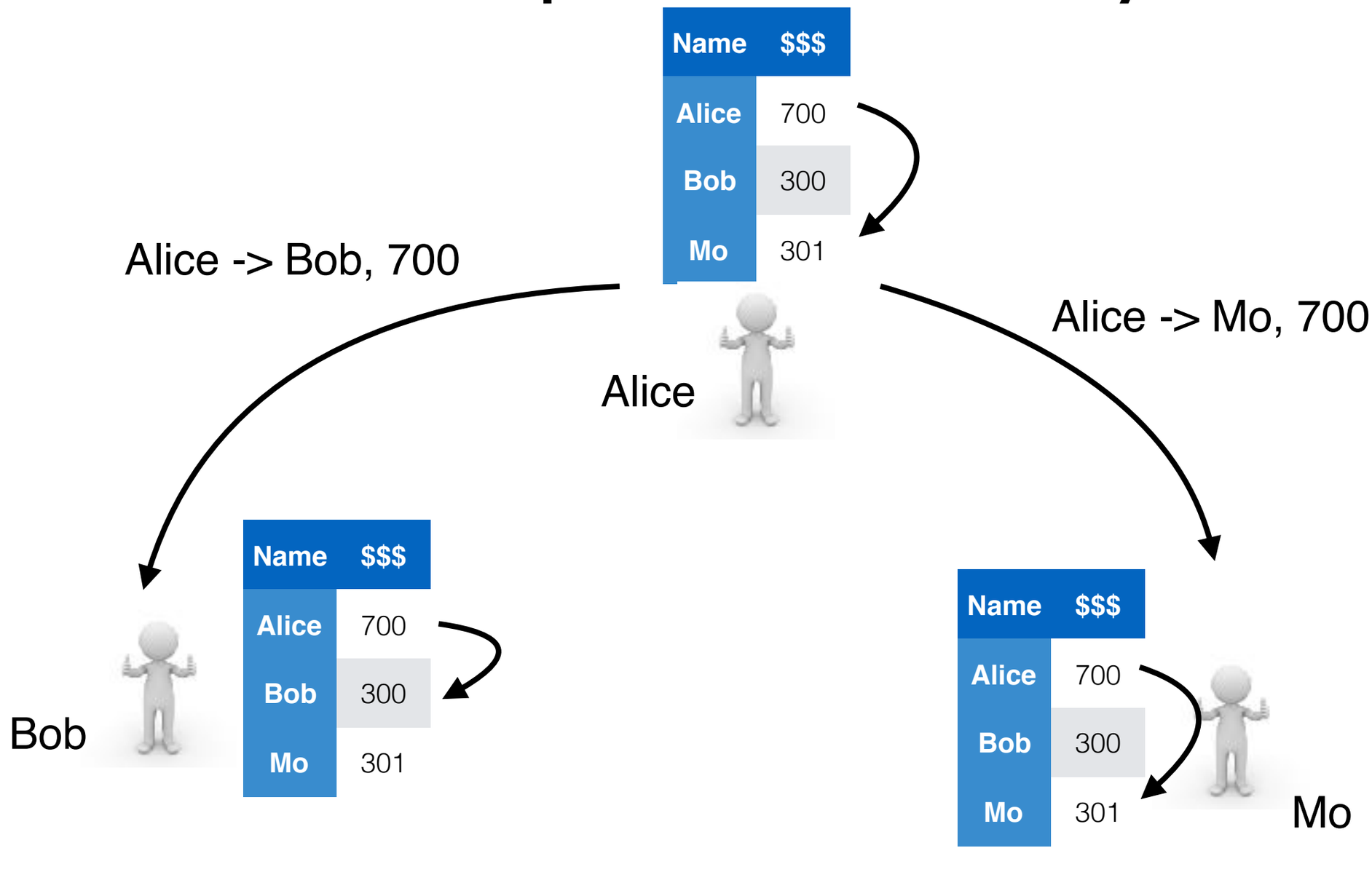
okay… PBFT?



Challenge 2: IC Consensus

okay… PBFT?

It is complicated… but, basically, closed membership limits scalability



Challenge 2: IC Consensus

Everyone just broadcast out whatever TXs s/he can sign

Alice

Name	$$$
Alice	700
Bob	300
Mo	301

Bob

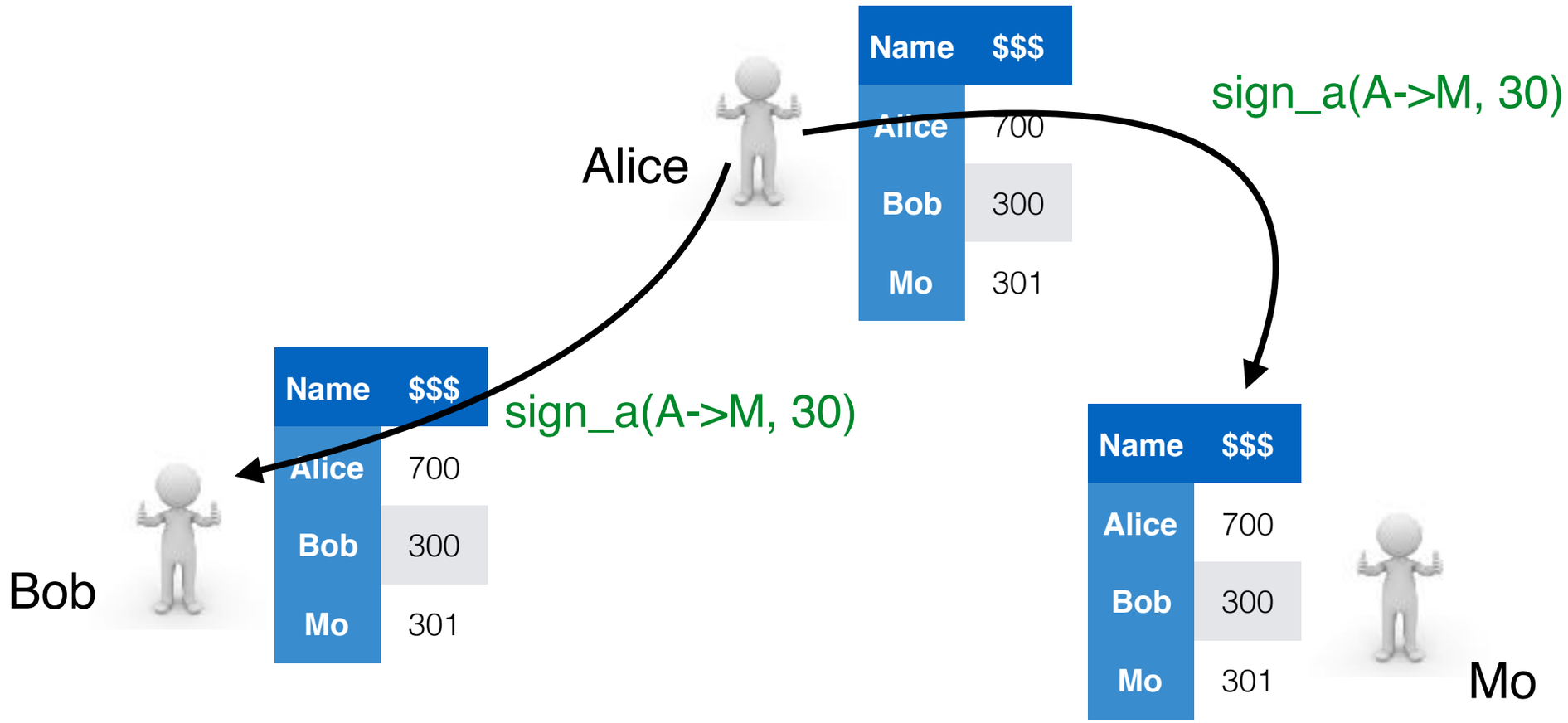
Name	$$$
Alice	700
Bob	300
Mo	301

Name	$$$
Alice	700
Bob	300
Mo	301

Mo

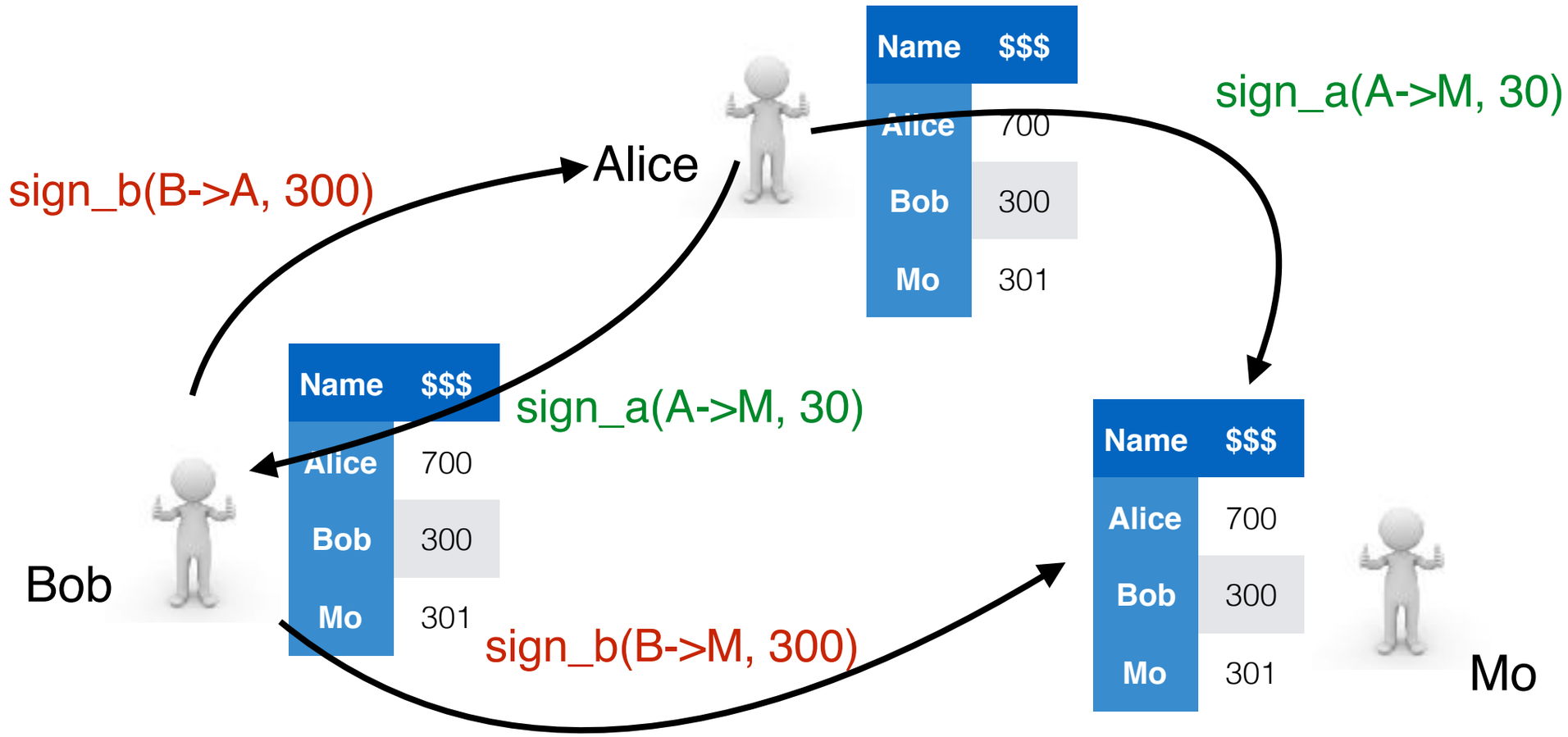
Challenge 2: IC Consensus

Everyone just broadcast out whatever TXs s/he can sign



Challenge 2: IC Consensus

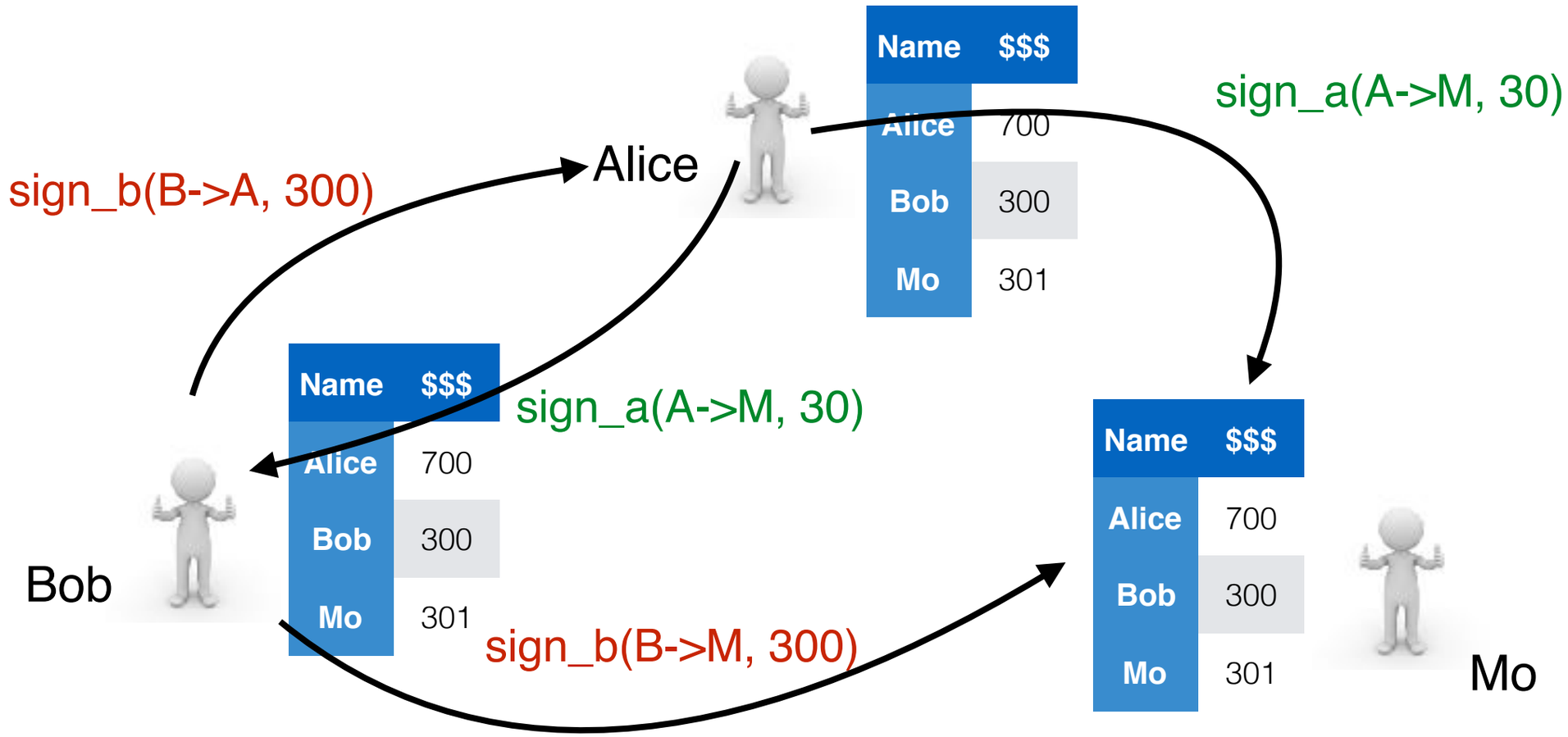
Everyone just broadcast out whatever TXs s/he can sign



Challenge 2: IC Consensus

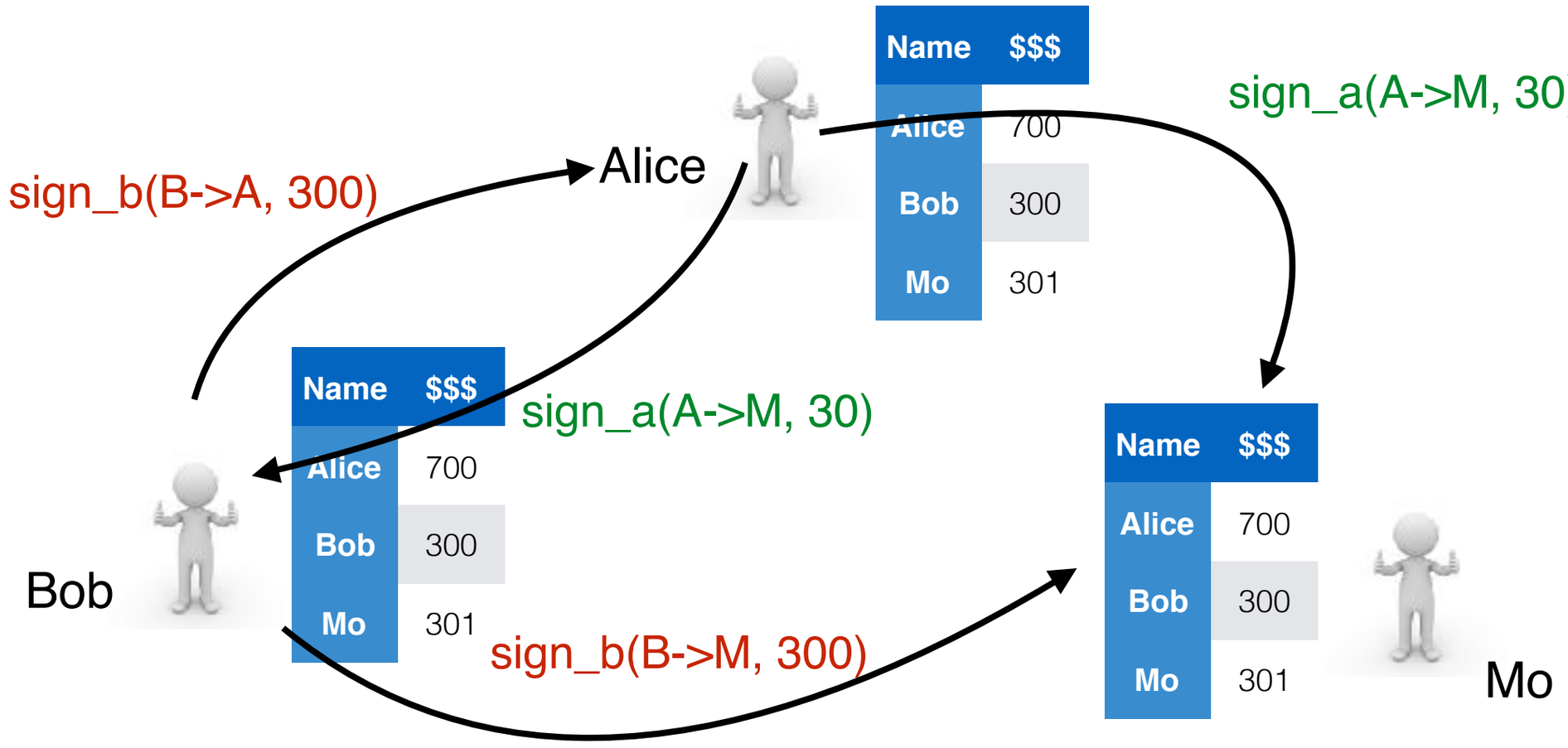
Nodes will only accept valid transactions

e.g. sign_b(B->A, 800) is not valid



Challenge 2: IC Consensus

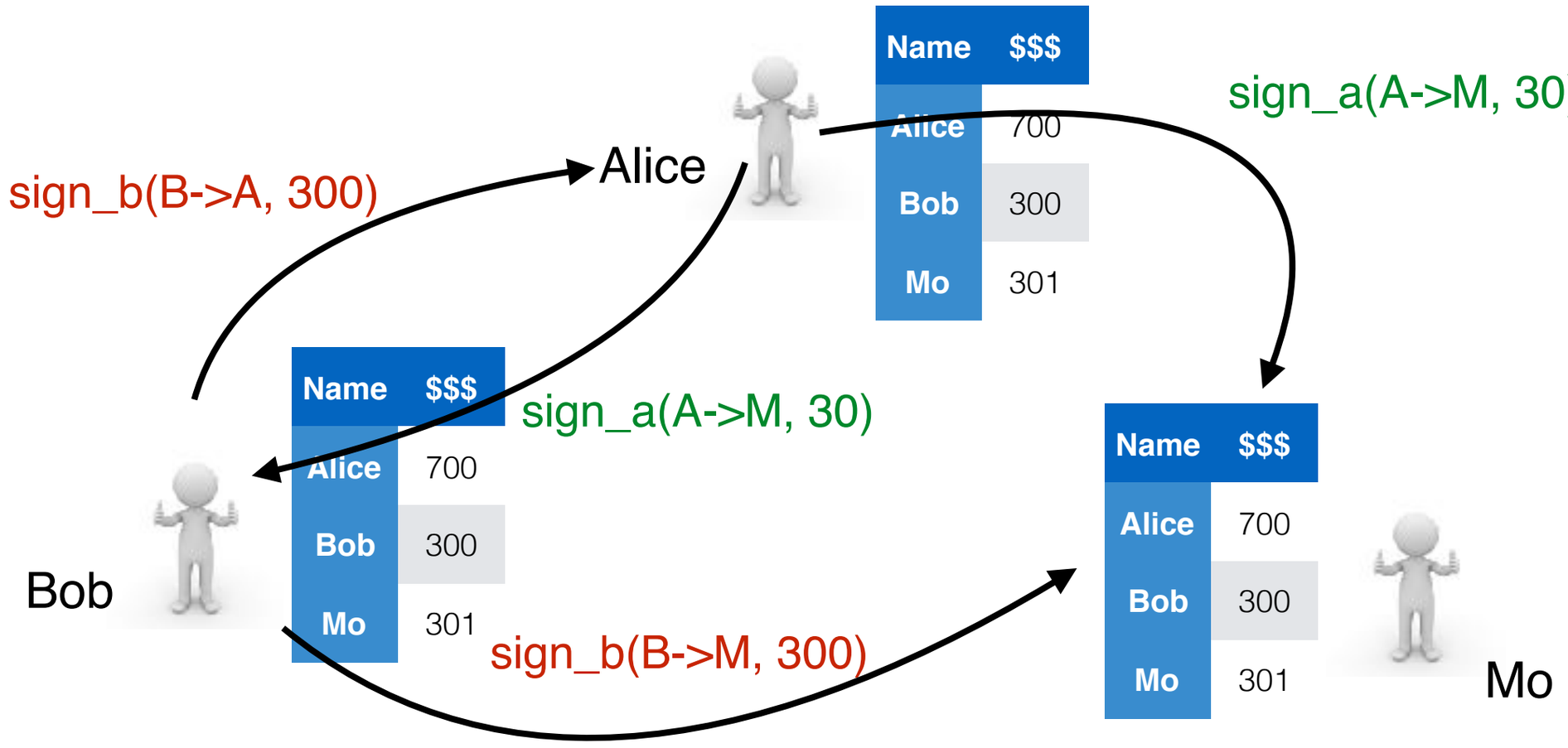
Everyone has different views



Challenge 2: IC Consensus

Everyone has different views

Who to listen?

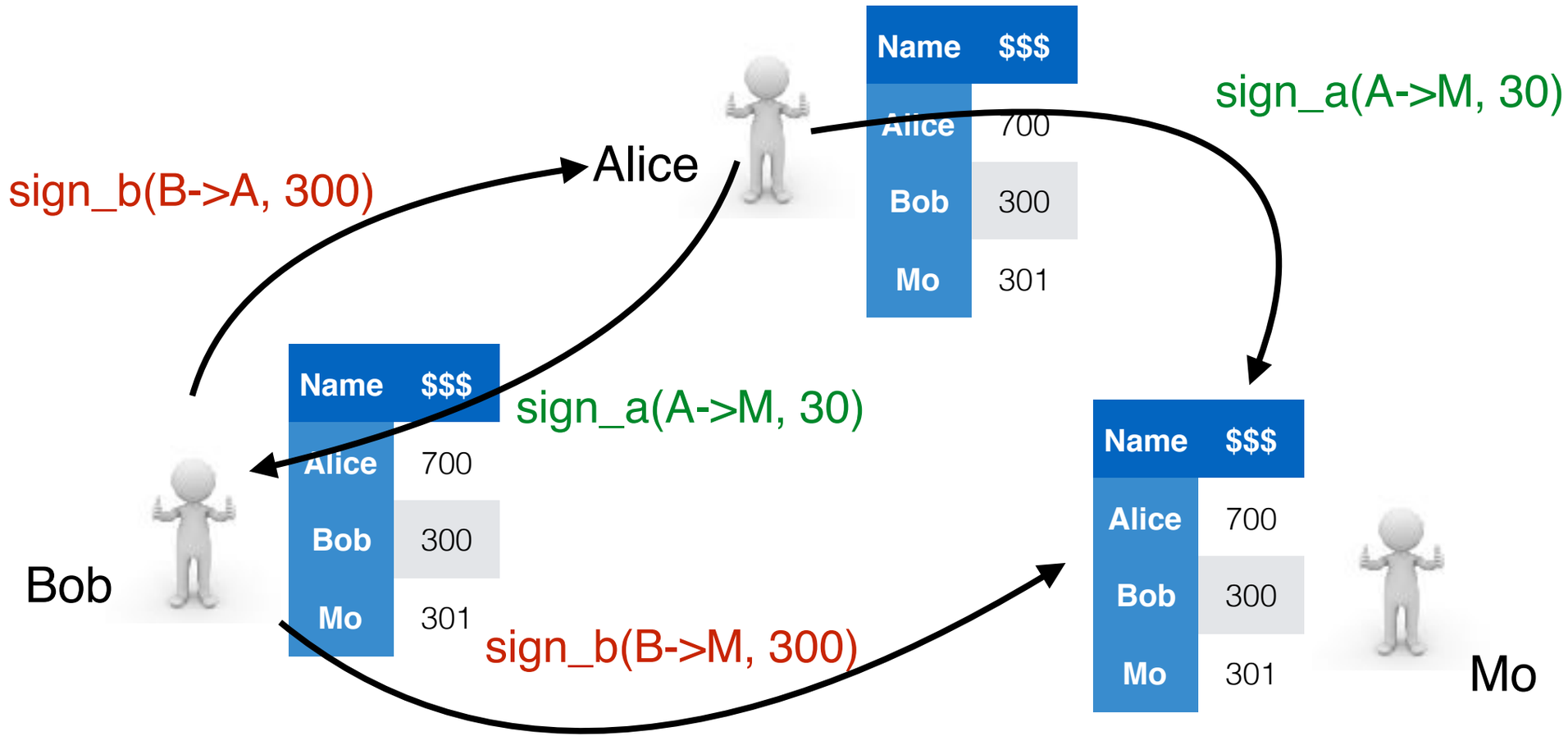


Challenge 2: IC Consensus

Everyone has different views

Who to listen?

Leader Election!



Challenge 2: IC Consensus

Who is the leader?

Alice	Bob	Mo
sign_a(A->M, 30)	sign_a(A->M, 30)	sign_a(A->M, 30)
sign_b(B->A, 300)		sign_b(B->M, 300)

Challenge 2: IC Consensus

Solve a very hard-to-compute easy-to-verify puzzle!

Alice	Bob	Mo
sign_a(A->M, 30)	sign_a(A->M, 30)	sign_a(A->M, 30)
sign_b(B->A, 300)		sign_b(B->M, 300)

Challenge 2: IC Consensus

Solve a very hard-to-compute easy-to-verify puzzle!

Alice

sign_a(A->M, 30)

sign_b(B->A, 300)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Bob

sign_a(A->M, 30)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Mo

sign_a(A->M, 30)

sign_b(B->M, 300)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Challenge 2: IC Consensus

Solve a very hard-to-compute easy-to-verify puzzle!

Alice

sign_a(A->M, 30)

sign_b(B->A, 300)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

8	2	5	4	7	1	3	9	6
1	9	4	3	2	6	5	7	8
3	7	6	9	8	5	2	4	1
5	1	9	7	4	3	8	6	2
6	3	2	5	9	8	4	1	7
4	8	7	6	1	2	9	3	5
2	6	3	1	5	9	7	8	4
9	4	8	2	6	7	1	5	3
7	5	1	8	3	4	6	2	9

Bob

sign_a(A->M, 30)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Mo

sign_a(A->M, 30)

sign_b(B->M, 300)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Challenge 2: IC Consensus

Alice "found a Block"

Alice

sign_a(A->M, 30)

sign_b(B->A, 300)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

8	2	5	4	7	1	3	9	6
1	9	4	3	2	6	5	7	8
3	7	6	9	8	5	2	4	1
5	1	9	7	4	3	8	6	2
6	3	2	5	9	8	4	1	7
4	8	7	6	1	2	9	3	5
2	6	3	1	5	9	7	8	4
9	4	8	2	6	7	1	5	3
7	5	1	8	3	4	6	2	9

Bob

sign_a(A->M, 30)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Mo

sign_a(A->M, 30)

sign_b(B->M, 300)

5	3			7				
6			1	9	5			
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Challenge 2: IC Consensus

The "newest" puzzle is based on the solution of old puzzle

Block1

Block1

Block1

Alice	Bob	Mo
TX1	TX4	~~sign_a(A->M, 30)~~
TX2	TX2	~~sign_b(B->M, 300)~~
TX3	TX7	

Challenge 2: IC Consensus

The "newest" puzzle is based on the solution of old puzzle

Block1

Alice

TX1

TX2

TX3

Block1

Bob

TX4

TX2

TX7

Mo

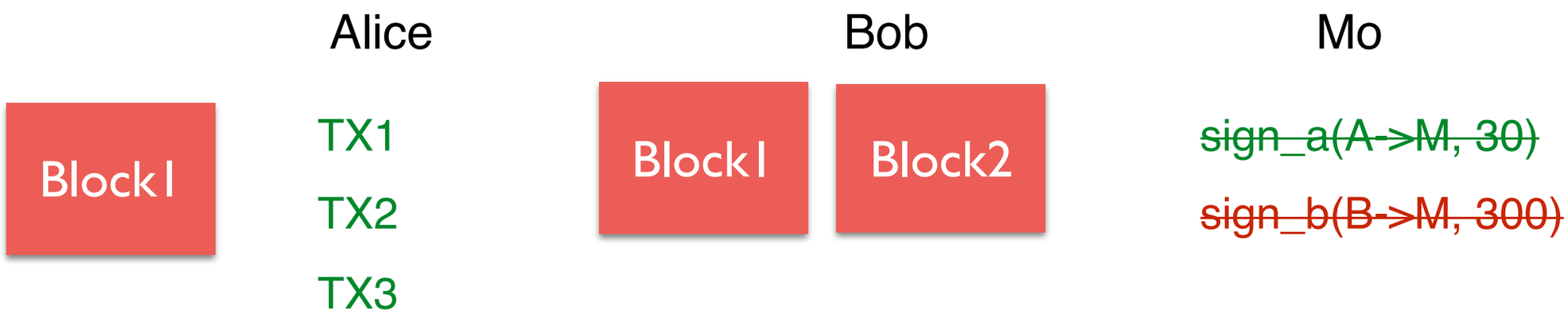
~~sign_a(A->M, 30)~~

~~sign_b(B->M, 300)~~

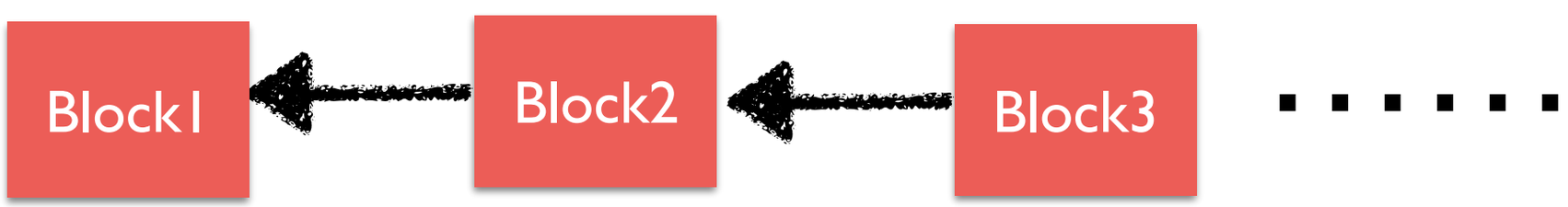
Block1

Challenge 2: IC Consensus

The "newest" puzzle is based on the solution of old puzzle

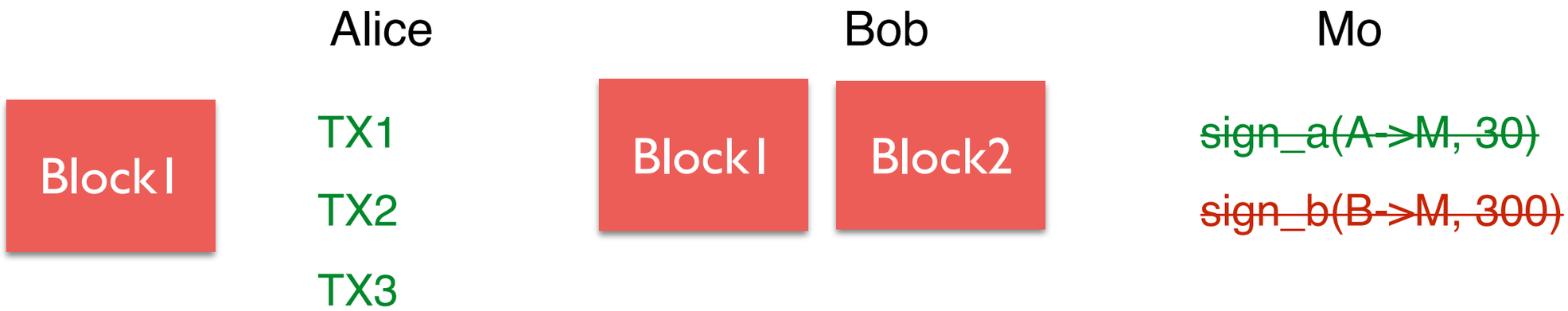


Consensus on a chain of blocks of Txs
blocks are built by solving puzzles (Mining)

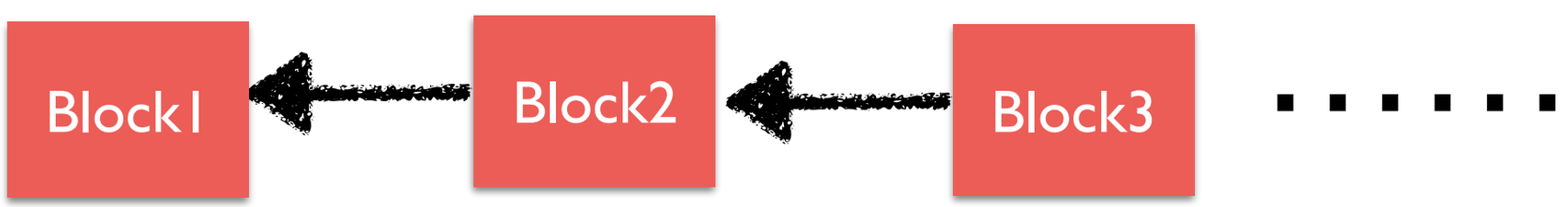


Challenge 2: IC Consensus

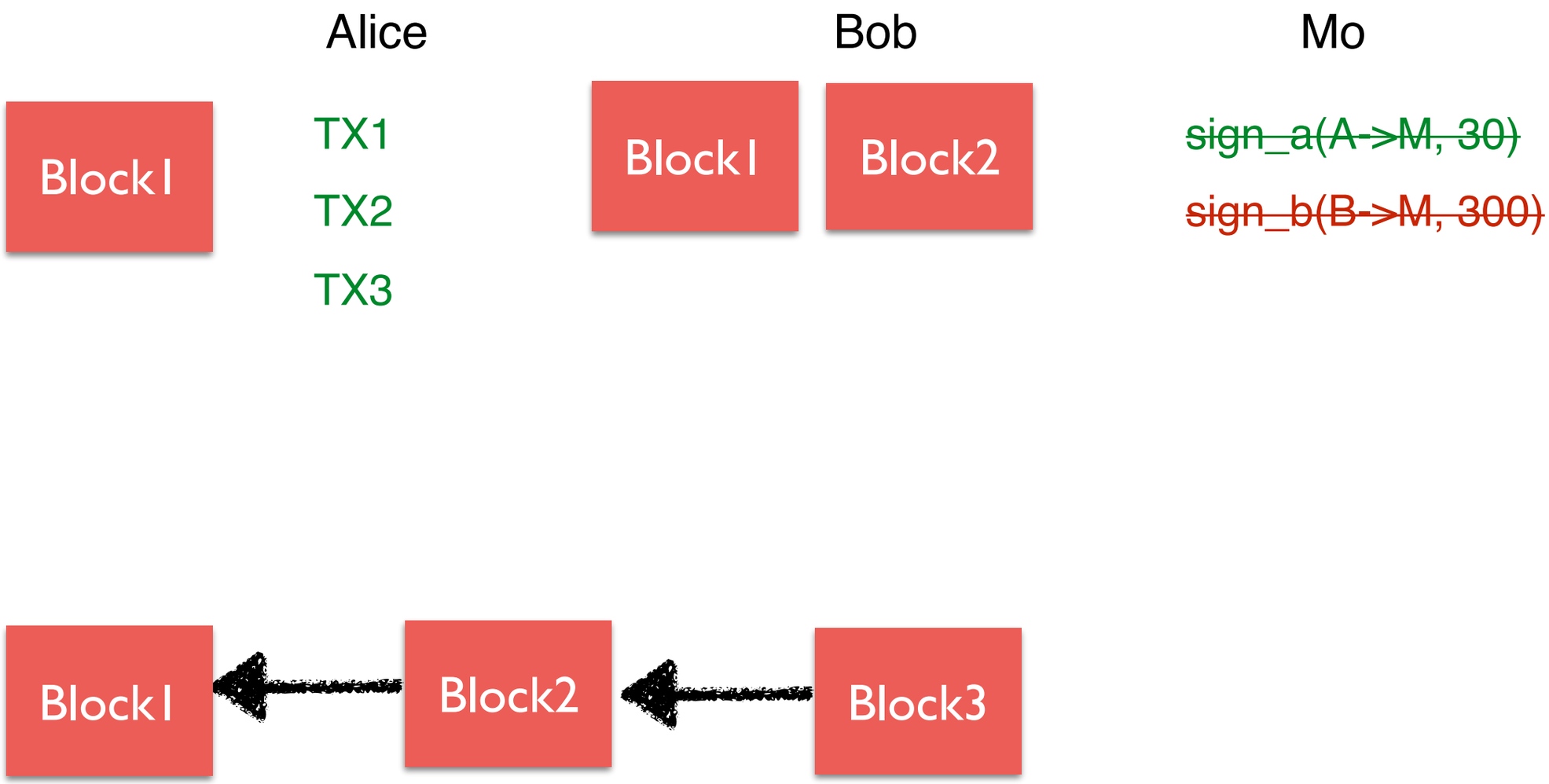
Miner Incentives: TX fees and mining reward



Consensus on a chain of blocks of Txs
blocks are built by solving puzzles (Mining)

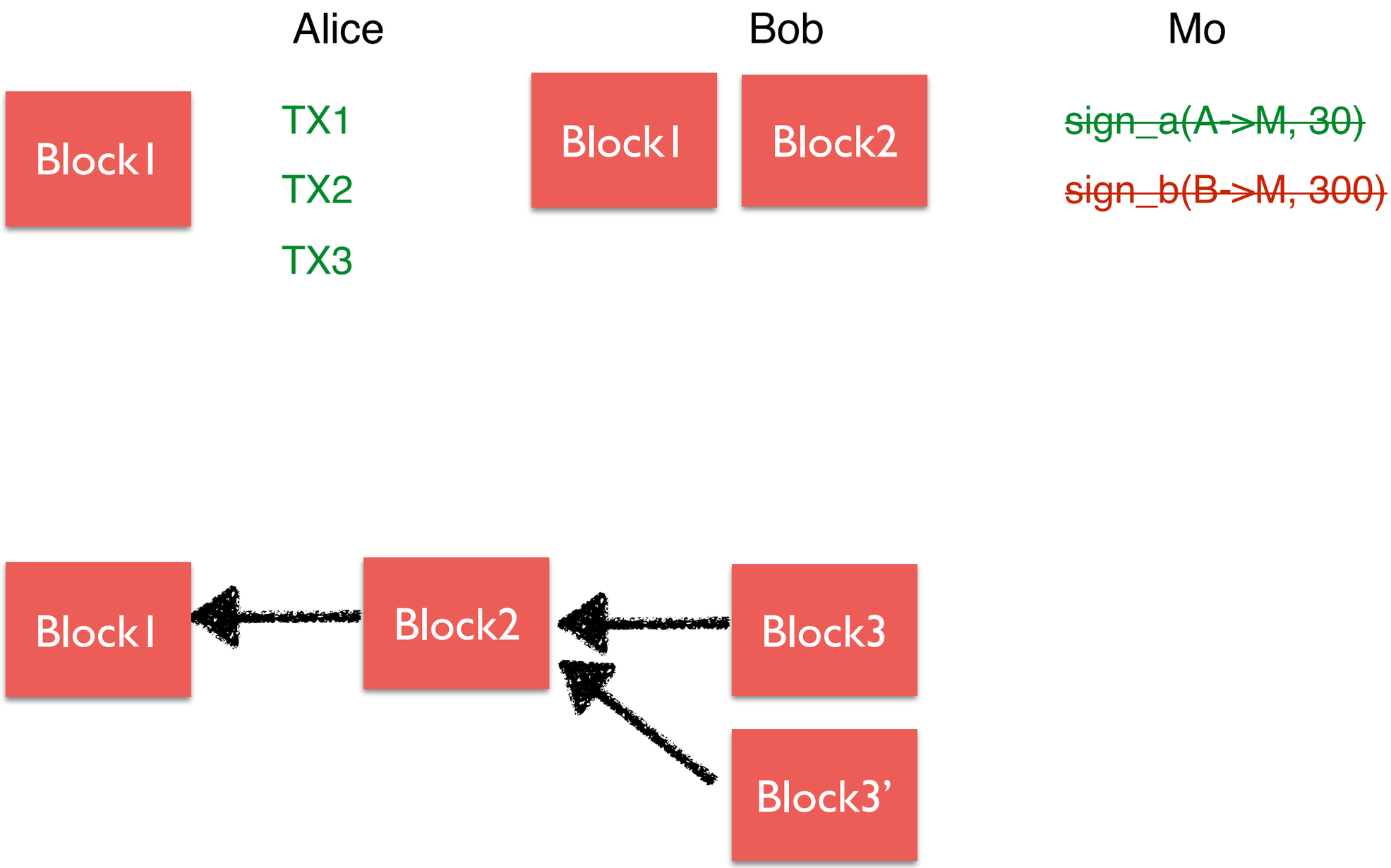


Challenge 2: IC Consensus



Challenge 2: IC Consensus

Fork of blockchain



Challenge 2: IC Consensus

Fork of blockchain

Alice

Block1

TX1

TX2

TX3

Bob

Block1

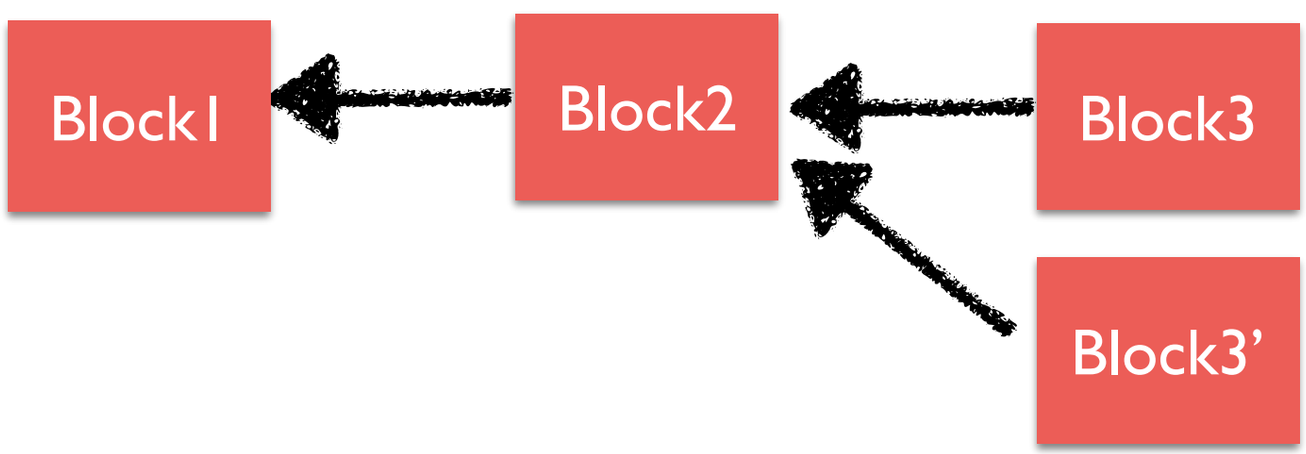
Block2

Mo

~~sign_a(A->M, 30)~~

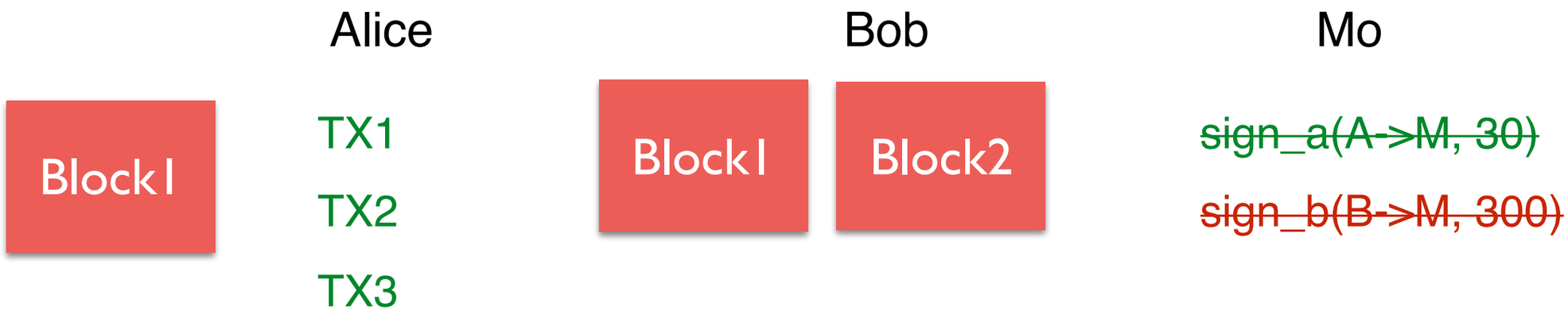
~~sign_b(B->M, 300)~~

Longest chain wins, what's the issue?

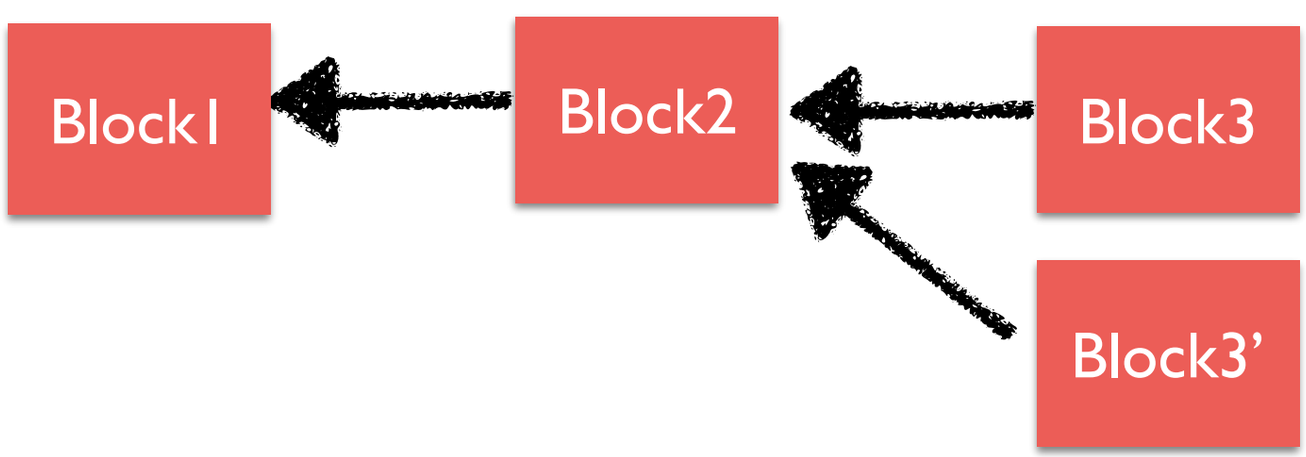


Challenge 2: IC Consensus

Fork of blockchain



50% attack, rewrite of the entire history



BTC for real

Transaction Model: UTXO

Input: Genesis

Output: 25 BTC->Satoshi

BTC for real

Transaction Model: UTXO

Input: Genesis

Output: 25 BTC->Satoshi

Input: 1[0]

Output: 5 BTC-> Mo, 20 BTC -> Satoshi

BTC for real

Transaction Model: UTXO

Input: Genesis

Output: 25 BTC->Satoshi

Input: 1[0]

Output: 5 BTC-> Mo, 20 BTC -> Satoshi

Input: 2[0]

Output: 1 BTC->Alice, 2 BTC -> Bob, 2BTC -> Mo

BTC for real

Transaction Model: UTXO

Input: Genesis

Output: 25 BTC->Satoshi

Input: 1[0]

Output: 5 BTC-> Mo, 20 BTC -> Satoshi

Input: 2[0]

Output: 1 BTC->Alice, 2 BTC -> Bob, 2BTC -> Mo

UTXO in-memory list for easy validation

BTC for real

Mining Mechanism
Proof of Work (PoW)

H(Block3, new TX, nounce) < 0x0000aef1e….

Solution

Difficulty

BTC for real

Mining Mechanism
Proof of Work (PoW)

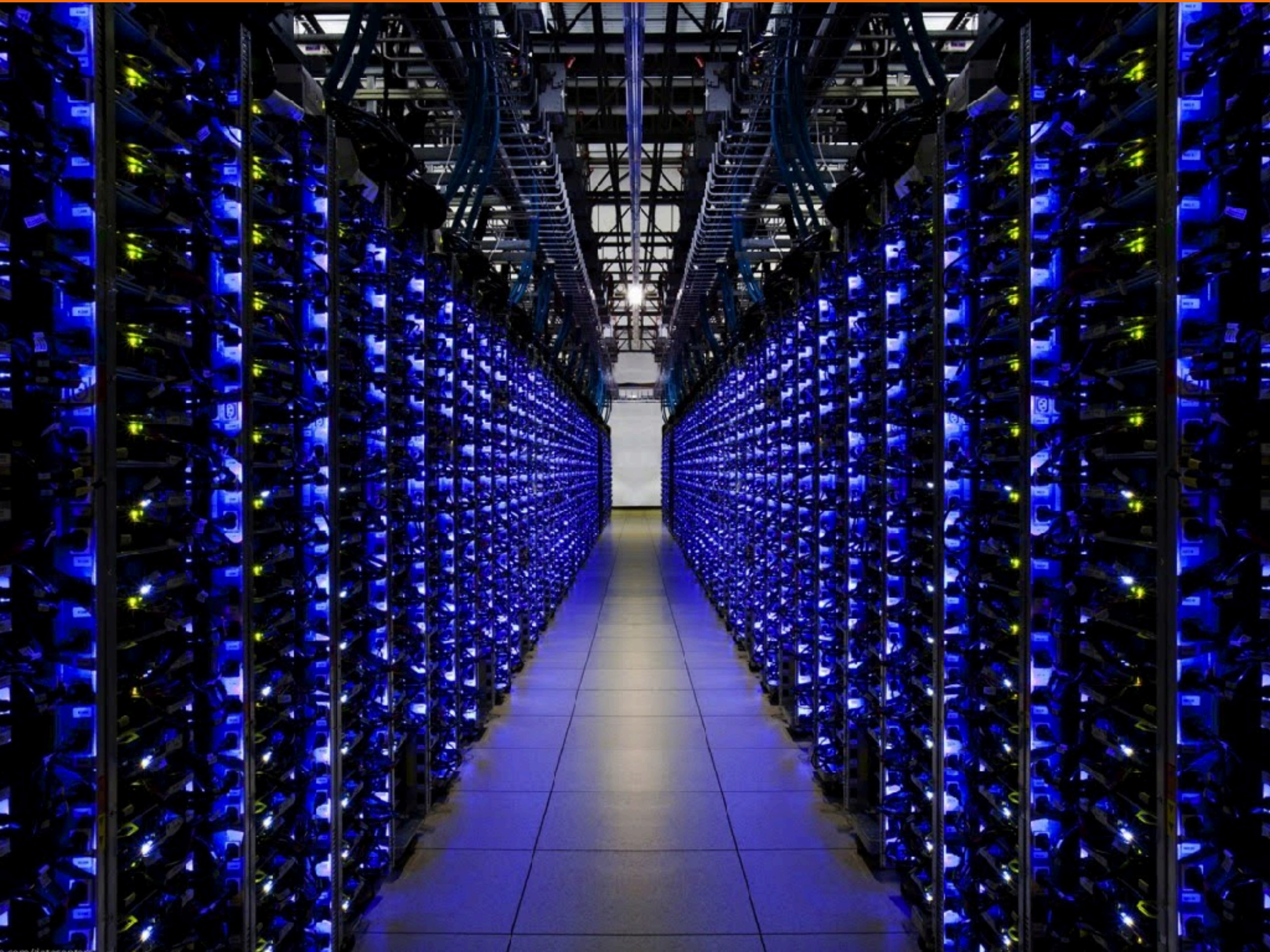
H(Block3, new TX, nounce) < 0x0000aef1e….

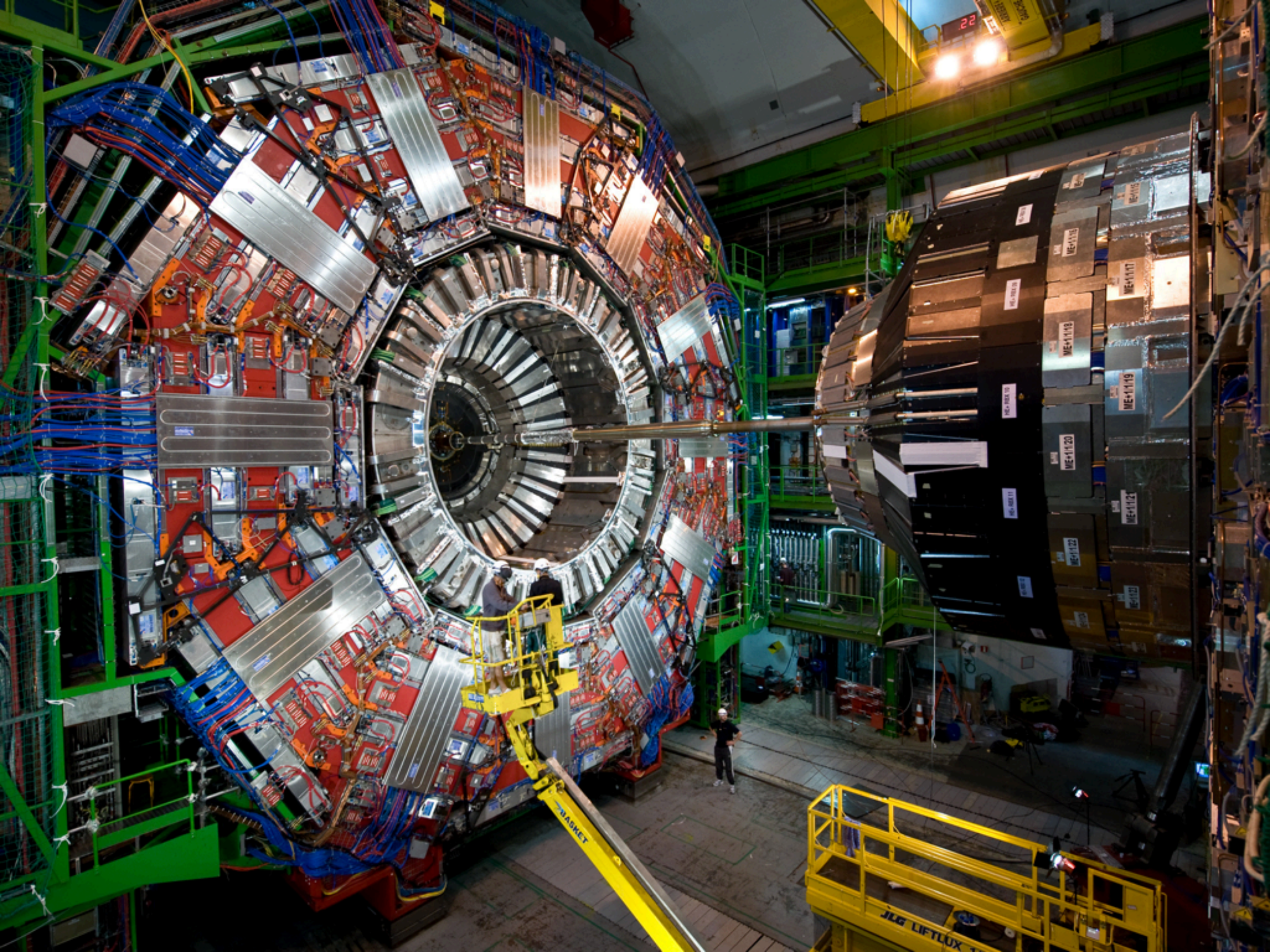
Solution

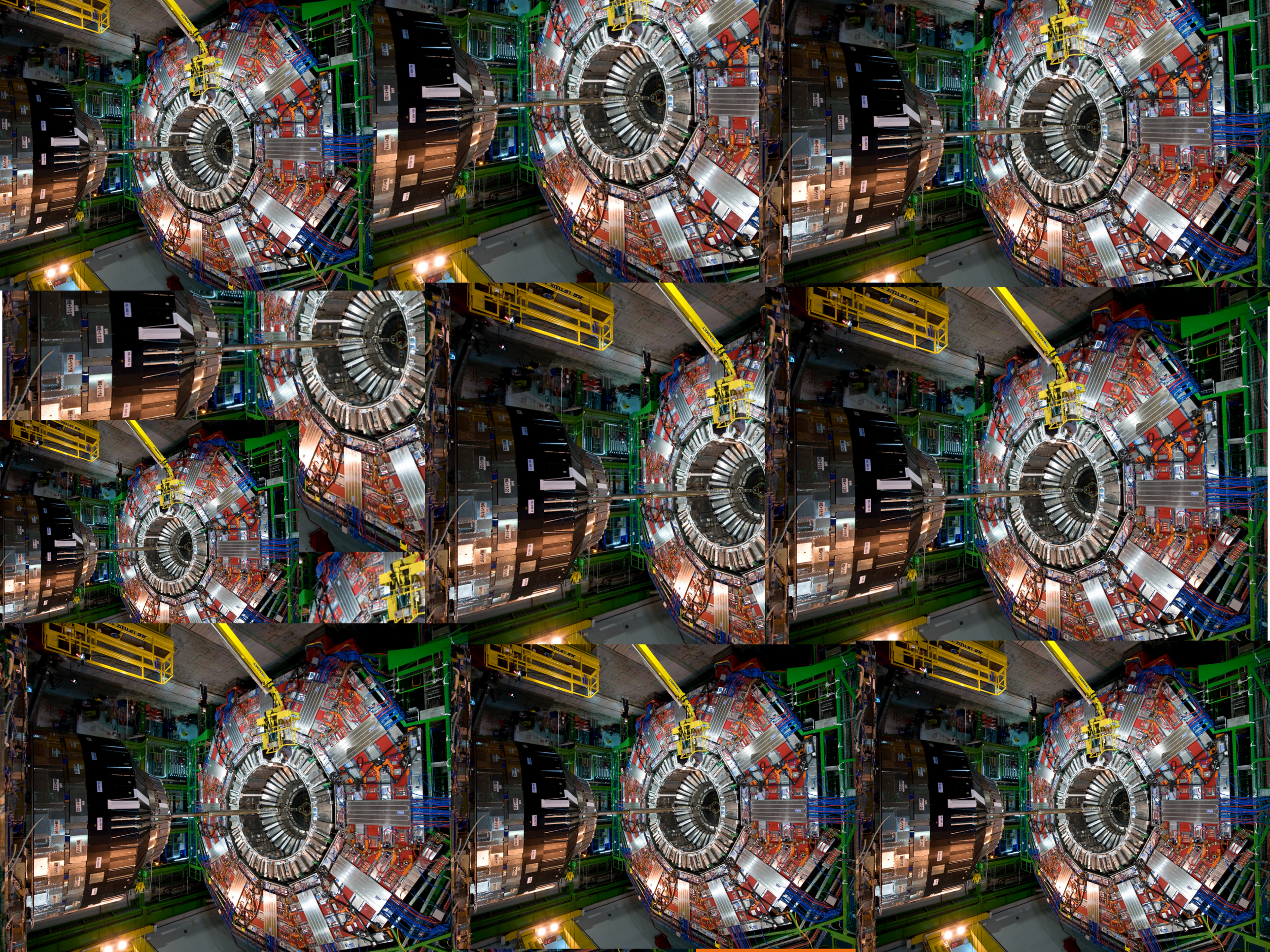
Difficulty

Control block interval


SAPPHIRE
SAPPHIRE
EVGA
1000 P

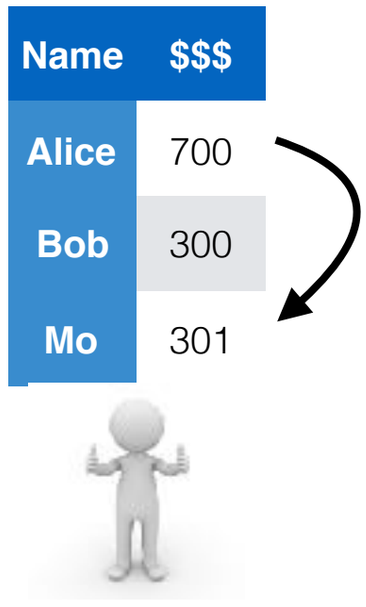


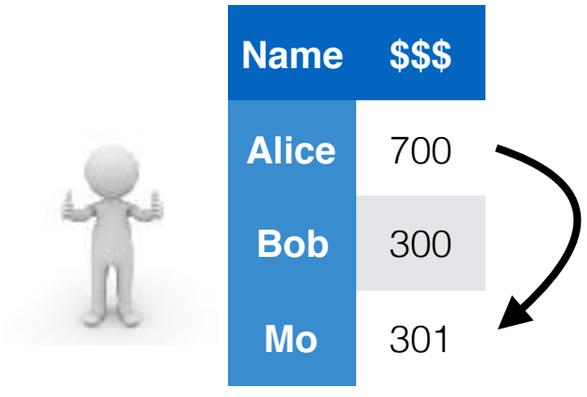

ME+1/1/17
ME+1/1/19
ME+1/1/20
JLG LIFTLUX

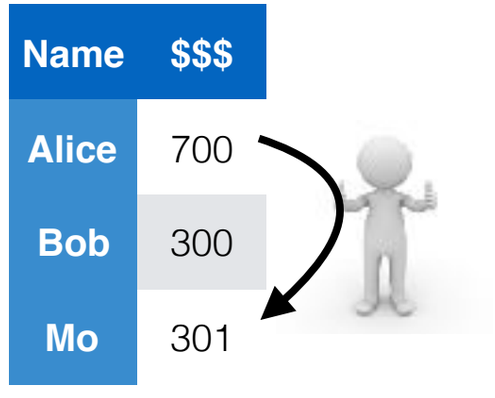


50X

Large-scale Ledger Consensus Without Trust



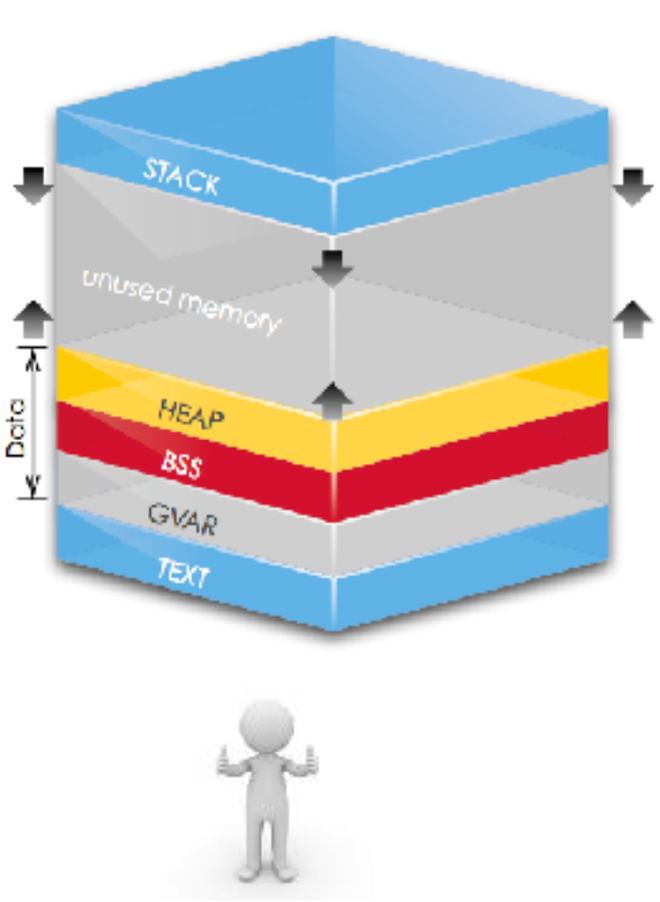


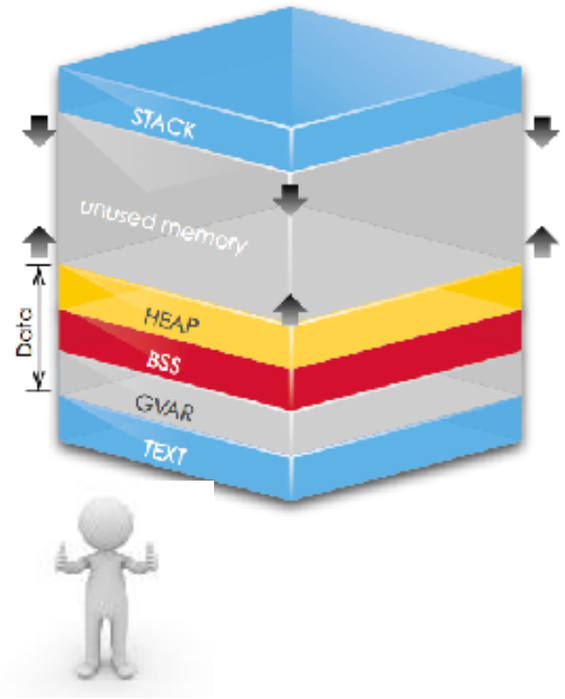


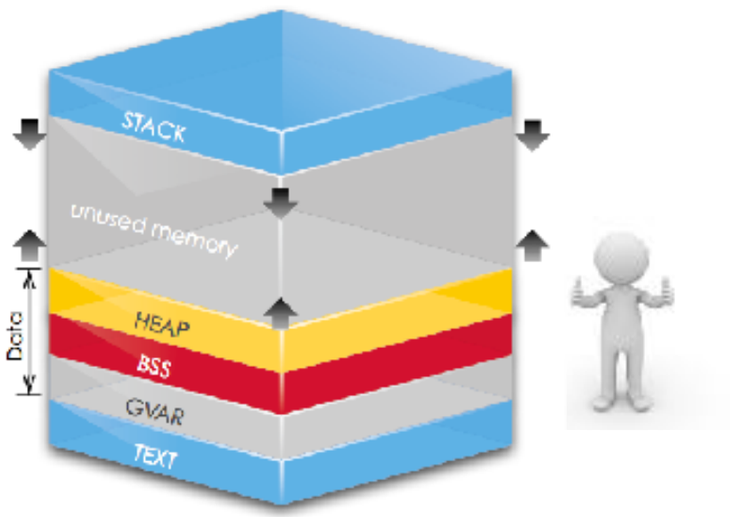
Large-scale Shared State Consensus Without Trust

Smart Contract

Large-scale VM Memory State Consensus Without Trust

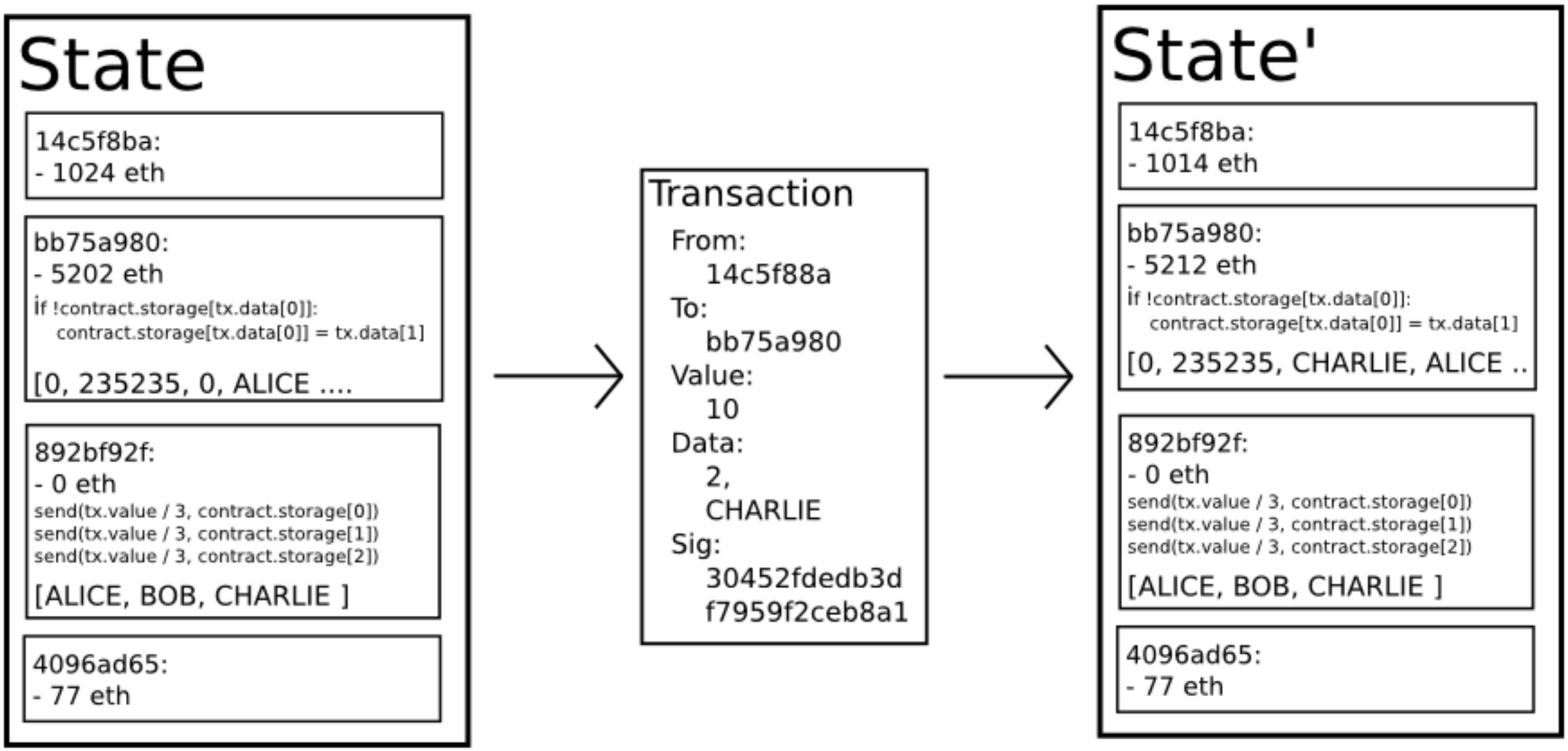






Smart Contract

Large-scale VM Memory State Consensus Without Trust



Smart Contract

What does this give us?

Smart Contract

What does this give us?

Unalterable Program

that carries out only pre-defined logics

a.k.a “smart contracts”

Blockchain Applications

Core Value Proposition

Open p2p system that achieves consensus on state without p2p trust

Launch your own currency

It's just a program that maintains a map

Name	Lunch Owed
Alice	1
Bob	2
Mo	0

Launch your own currency

It's just a program that maintains a map

Name	Lunch Owed
Alice	1
Bob	2
Mo	0

Useless?

Launch your own currency

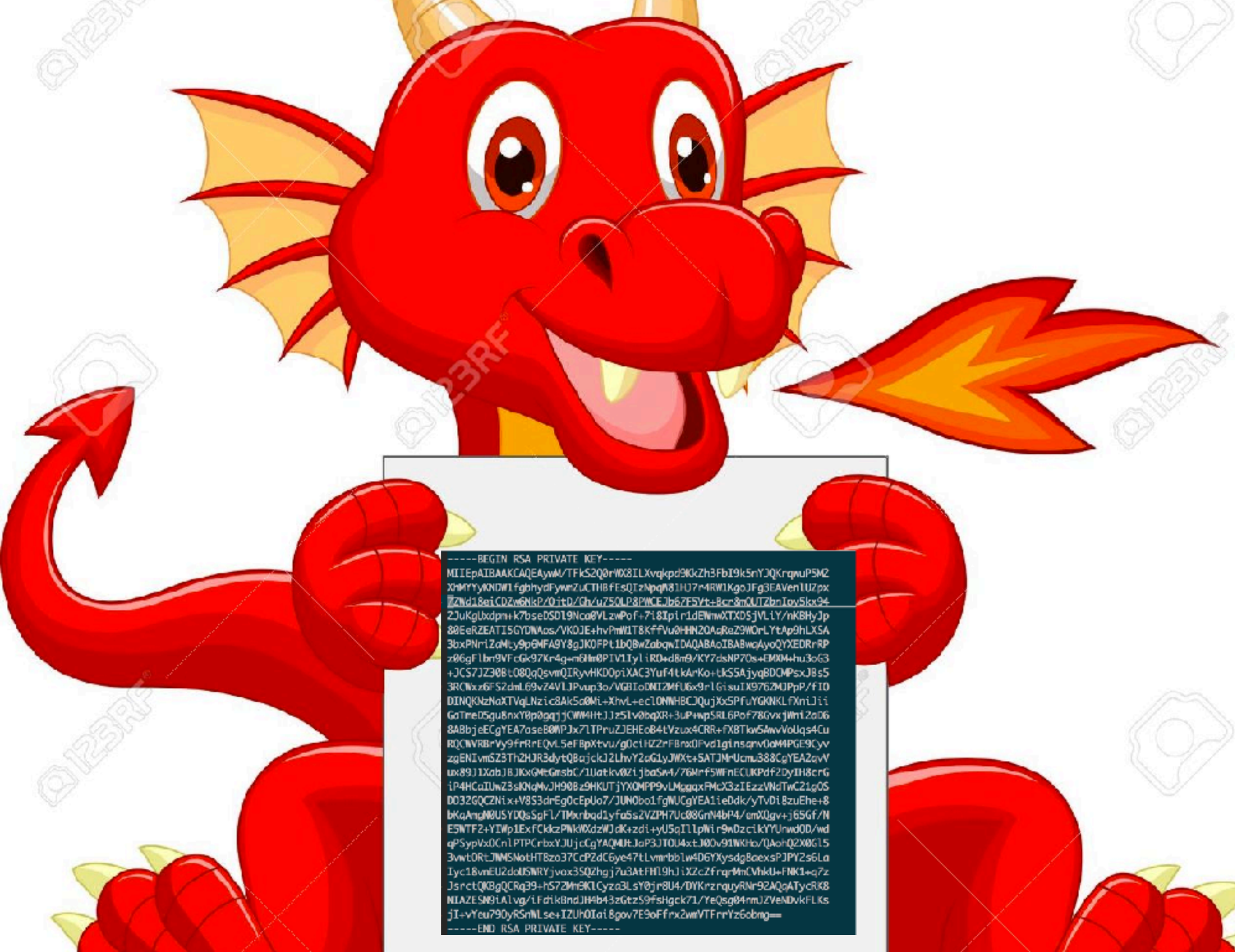
Tokenize physical properties' ownership

Launch your own currency

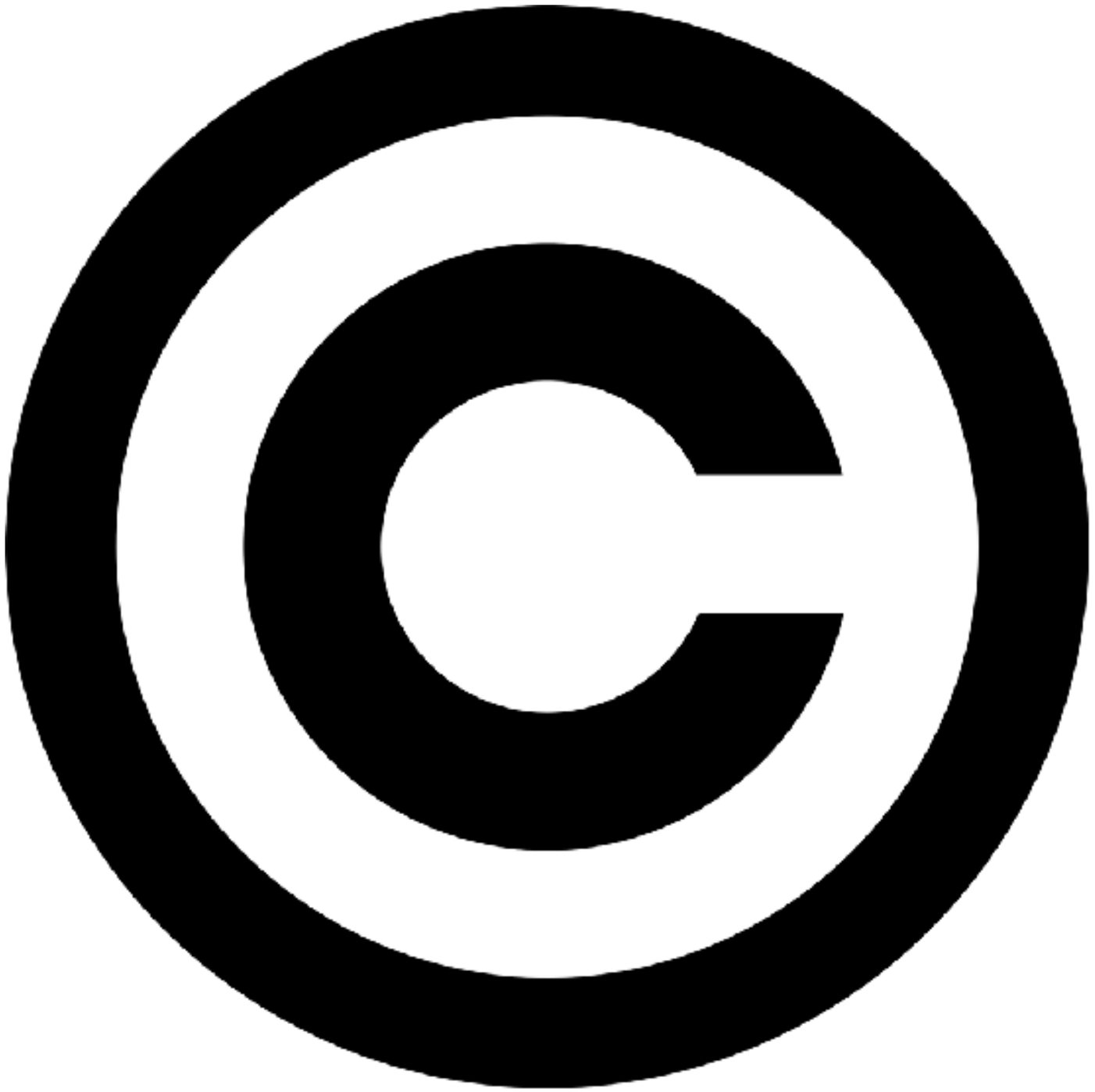
Tokenize physical properties' ownership

Gold
USD
Paintings
House
Super expensive wine


http://www.4kphoto.net/4k-dragon-fantasy-gold-human


-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAywM/TFkS2Q0rWX8ILXvqkpd9KkZh3FbI9k5nYJQKrqwuP5M2
XhMYYyKNDW1fgbhydFywrZuCTHBfEsQIzNpqW81HU7r4RW1KgoJFg3EAVen1UZpx
ZZNd18eiCDZw6NkP/QitD/Ch/u75QLP8PWCEJb67F5Yt+Bcr8mQUTZbnIqy5kx94
2JuKgUxdpn+k7bseDSD19Nca0VLzwPof+7i8Ipir1dEWmwXTXD5jVLlY/nKBHyJp
88EeRZEATI5GYDNAos/VKOJE+hvPmW1T8KffVu0HHN2QAqRaZ9WOrLYtAp9hLXSA
3bxPNriZaMcy9p6MFA9Y8gJKOFPt1bQBwZabqwIDAQABAoIBABwqAyoQYXEDRrRP
z06gFlbn9VFcGk97Kr4g+m6Hm0PIV1IyliRD+d8m9/KY7dsNP7Os+EMXM+hu3oG3
+JCS7JZ30BtO8QqQsvmQIRyvHKDOpiXAC3Yuf4tkArKo+tkS5AjyqBDCMPsxJBs5
3RCWxz6FS2dmL69vZ4VLJPvup3o/VGBIoDNI2MfU6x9rl6isuIX9762MJPpP/fID
DINQKNzNaXTVqLNzic8Ak5a0Wi+XhvL+eclONNHBCJQujXxSPfuYGKNKLfXniJii
GaTmeD5gu8nxY0p0gqjjCWW4HtJJz5lv0bqXR+3uP+wp5RL6Pof78GvxjWni2aD6
8ABbjeECgYEA7aseB0WPJx7lTPruZJEHEoB4tVzux4CRR+fXBTkw5AwvVoUqs4Cu
RQCWVRBrVy9frRrEQvL5eFBpXtvu/gOciHZ2rFBnxOFvd1ginsqrvOaM4PGE9CyV
zgENIvmSZ3Th2HJR3dytQBajckJ2LhvY2aG1yJWXt+5ATJMrUcmu388CgYEA2qvV
ux89J1XabJBJKxGMtGmsbC/1Uatkv0ZijbaSw4/76Wrf5WFnECUKPdf2DyIH8crG
iP4HCaIUwZ3sKNqMvJH90Bz9HKUTjYXOMPP9vLMgqqxFMcX3zIEzzVNdTwC21gOS
DO32GQCZNix+V8S3drEg0cEpUo7/JUNObo1fgWUCgYEA1ieDdk/yTvDi8zuEhe+8
bKqAmgN0USYDQsSgFl/TMxnbqd1yfa5s2VZPH7Uc08GnN4bP4/emXUgv+j65Gf/N
E5WTF2+YIWp1ExfCkkzPNkWXdzWJdK+zdi+yU5qIllpWir9wDzcikYYUnwdOD/wd
qPSypVxOCnlPTPCrbxYJUjoCgYAQM4tJaP3JTOU4xtJ0Ov91WKHo/QAohQ2X0Gl5
3vwtORtJWMSNotHTBzo37CdPZdC6ye47tLvmrbblw4D6YXysdgBoexsPJPY2s6La
Iyc18vmEU2doUSWRYjvox3SQZhgj7u3AtFHl9hJiXZcZfrqrMmCVhkU+FNK1+q7z
JsrctQKBgQCRq39+hS72MnEKlCyza3LsY0jr8U4/DYKrzrquyRNr92AQoATycRK8
NIAZESN9iAlvg/iFdkiBndJH4b43zGtz59fsHgck71/YeQsg04nmJZVeNDvkFLKs
jI+vYeu79OyRSnNLse+IZUhOIai8gov7E9oFfrx2wrVTFrrVz6obmg==
-----END RSA PRIVATE KEY-----

Reform copyright



Reform copyright

Reform copyright

Have an idea?

Reform copyright

Have an idea?

Write an paper

Reform copyright

Have an idea?

Write an paper

Don’t want to put on arxiv cuz of $$$

Reform copyright

Have an idea?

Write an paper

Don’t want to put on arxiv cuz of $$$

Encrypt it

Reform copyright

Have an idea?

Write an paper

Don’t want to put on arxiv cuz of $$$

Encrypt it

Put the hash of file on blockchain

Reform copyright

Have an idea?

Write an paper

Don’t want to put on arxiv cuz of $$$

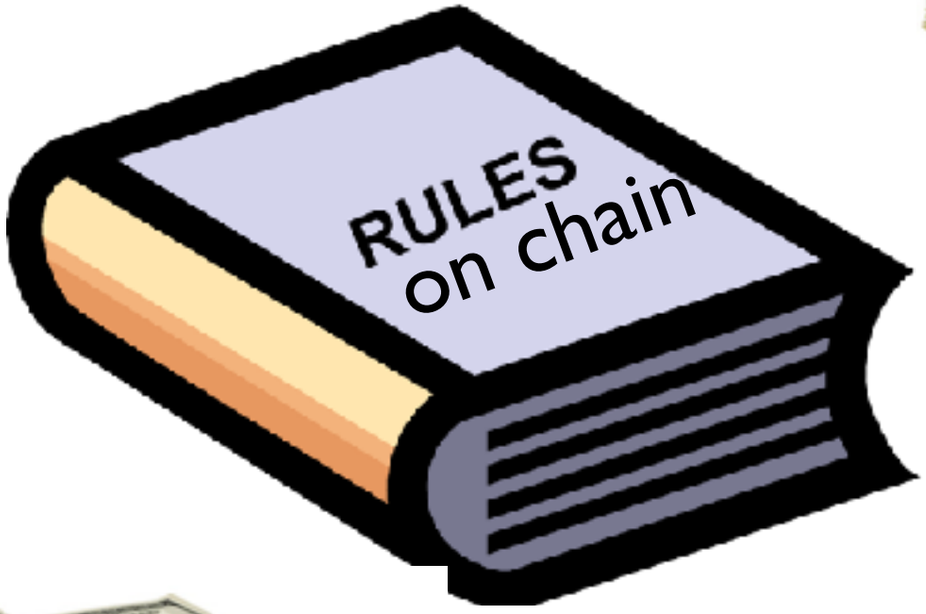
Encrypt it

Put the hash of file on blockchain

Proof of originality!

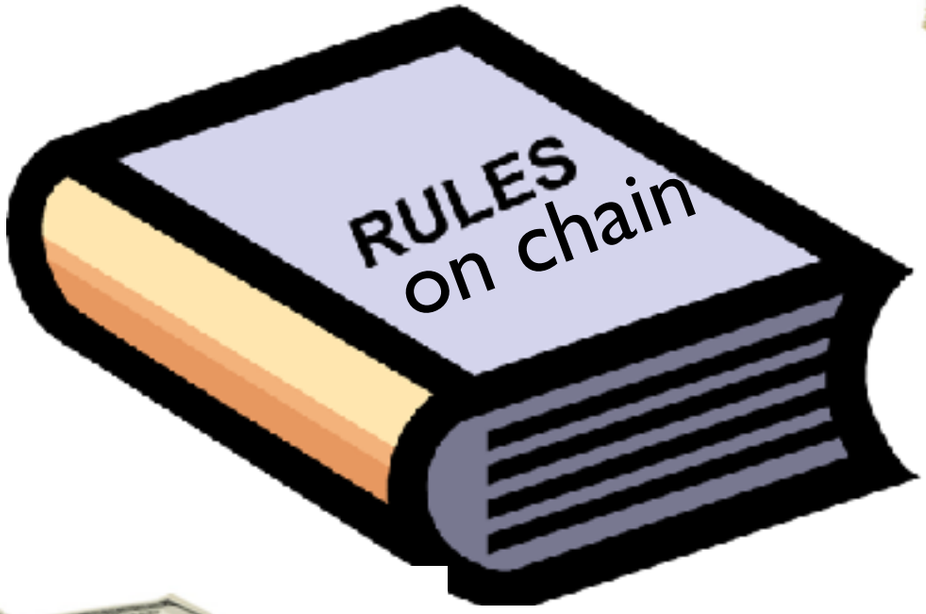
Decentralized Autonomous Organization

E.g. Crowd VC



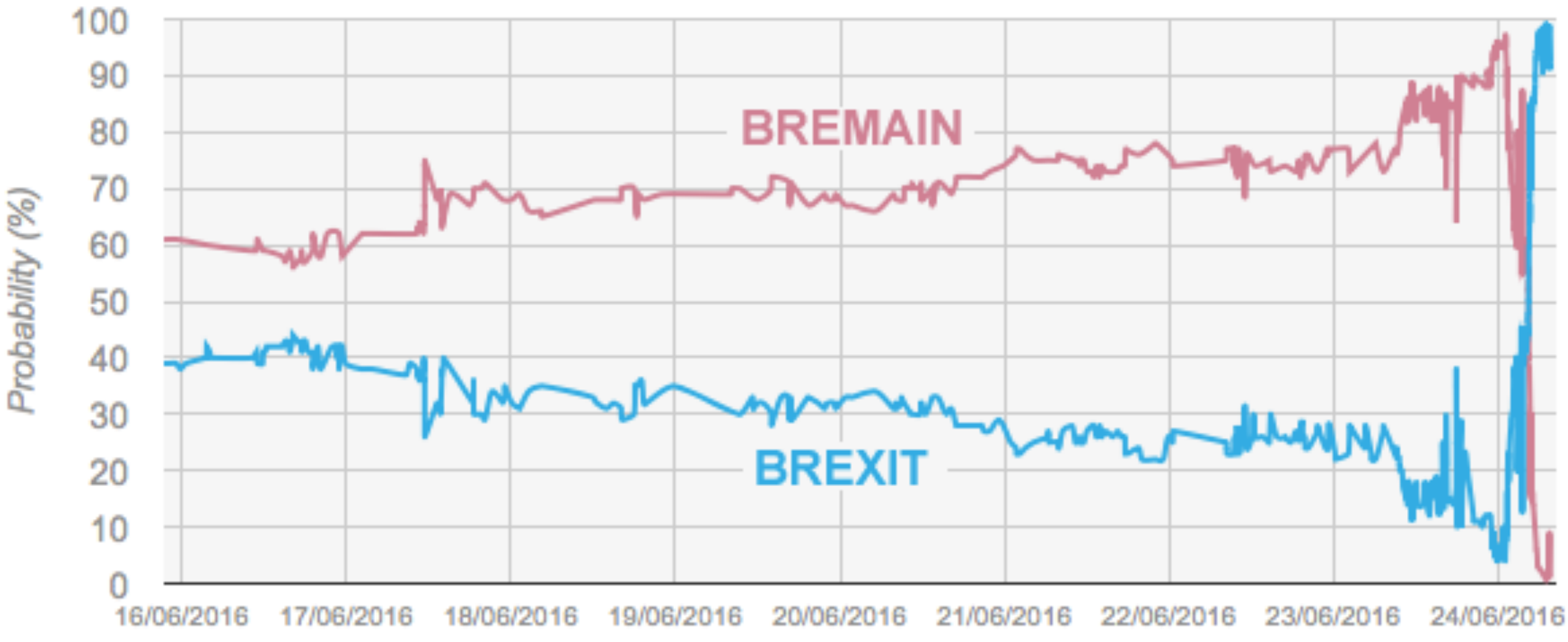
Decentralized Autonomous Organization

Vote on which
startup to invest



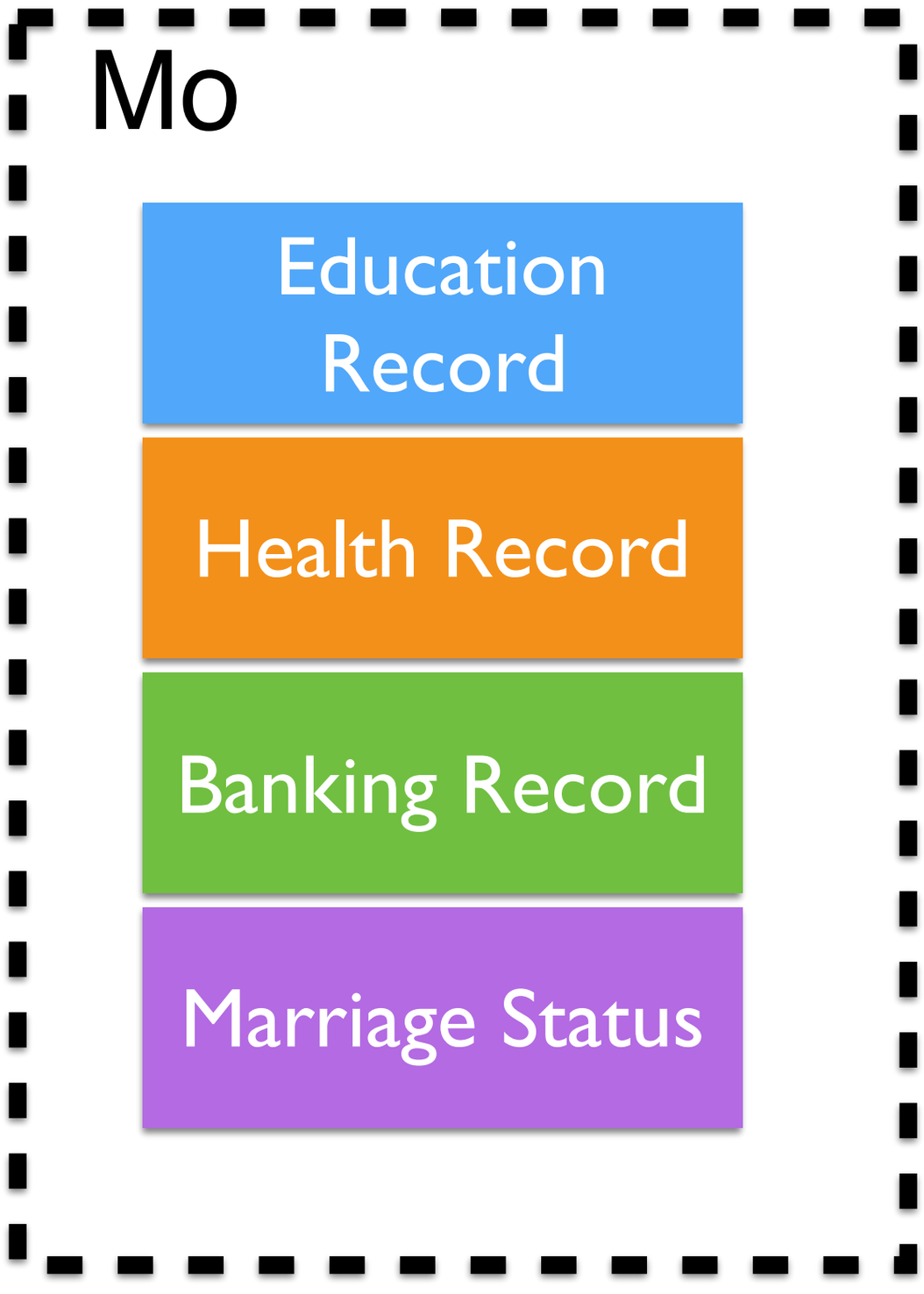
Prediction Market

Stand behind your money



I am not suggesting it is legal or illegal

Integrated ID and PII control



https://cointelegraph.com/news/kim-dotcom-explains-how-megaupload-20-will-take-bitcoin-to-the-moon

Not so fast

Technology Challenges in Blockchain

Challenges

Privacy and Confidentiality

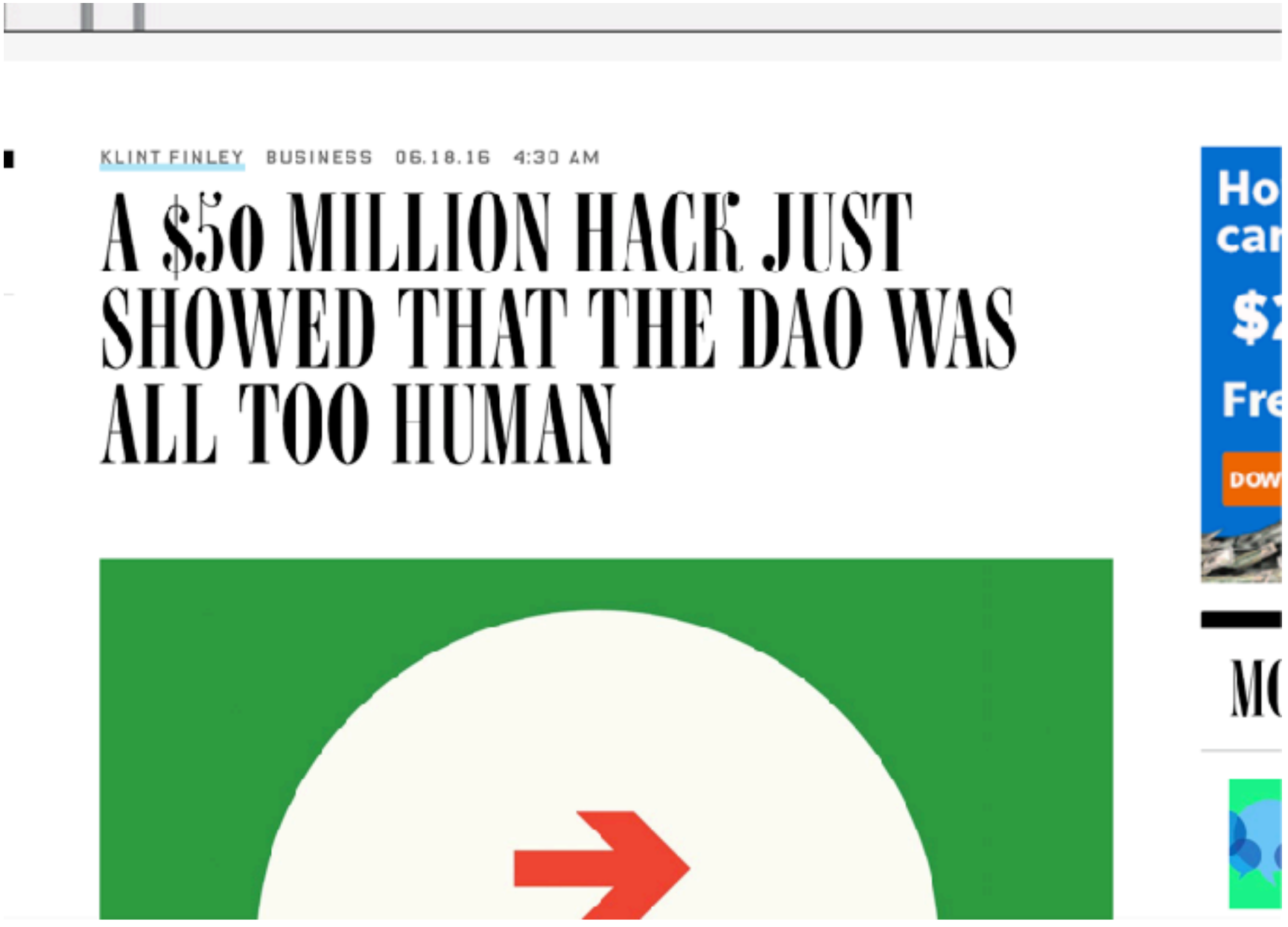
https://etherscan.io/address/
0xe7e8a4d3d0c6b43855be85f35bf86c38b370c01a

"Mixer" as a hacky solution

Privacy by construct: Zcash, Monero

Challenges

Correctness and Formal Verification



KLINT FINLEY BUSINESS 06.18.16 4:30 AM

A $50 MILLION HACK JUST SHOWED THAT THE DAO WAS ALL TOO HUMAN

Challenges

Correctness and Formal Verification

Challenges

Off-chain data injection authenticity concerns

Theresa May Calls for New Election in Britain, Seeking Stronger 'Brexit' Mandate

By STEVEN ERLANGER APRIL 18, 2017

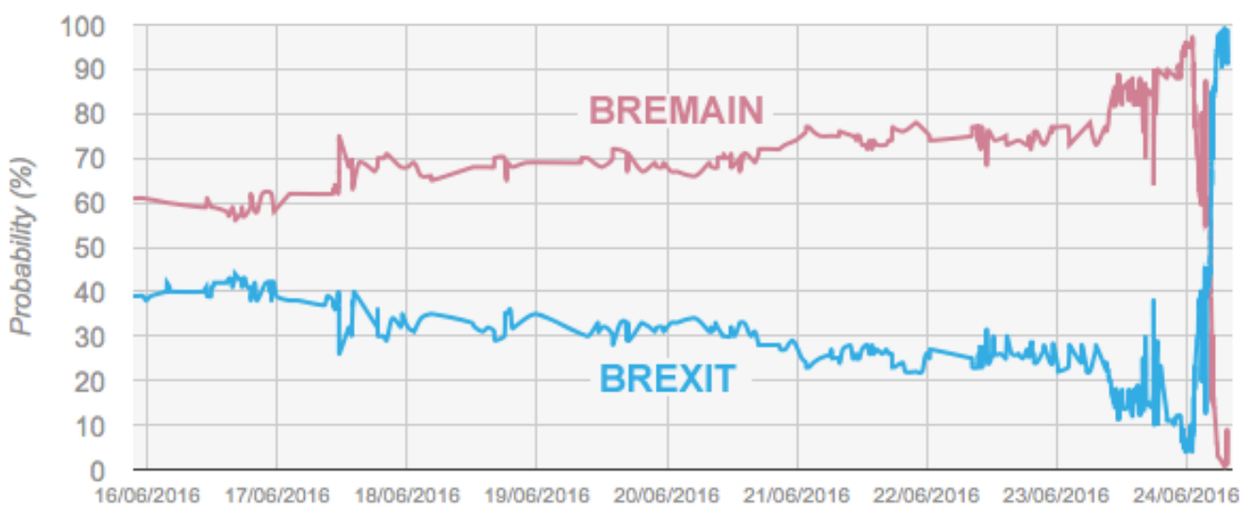
280

Prime Minister Theresa May of Britain announced on Tuesday that she would call an early election, seeking to strengthen her government's mandate while it negotiates

'Brexit': Britain's Decision to Leave the E.U.

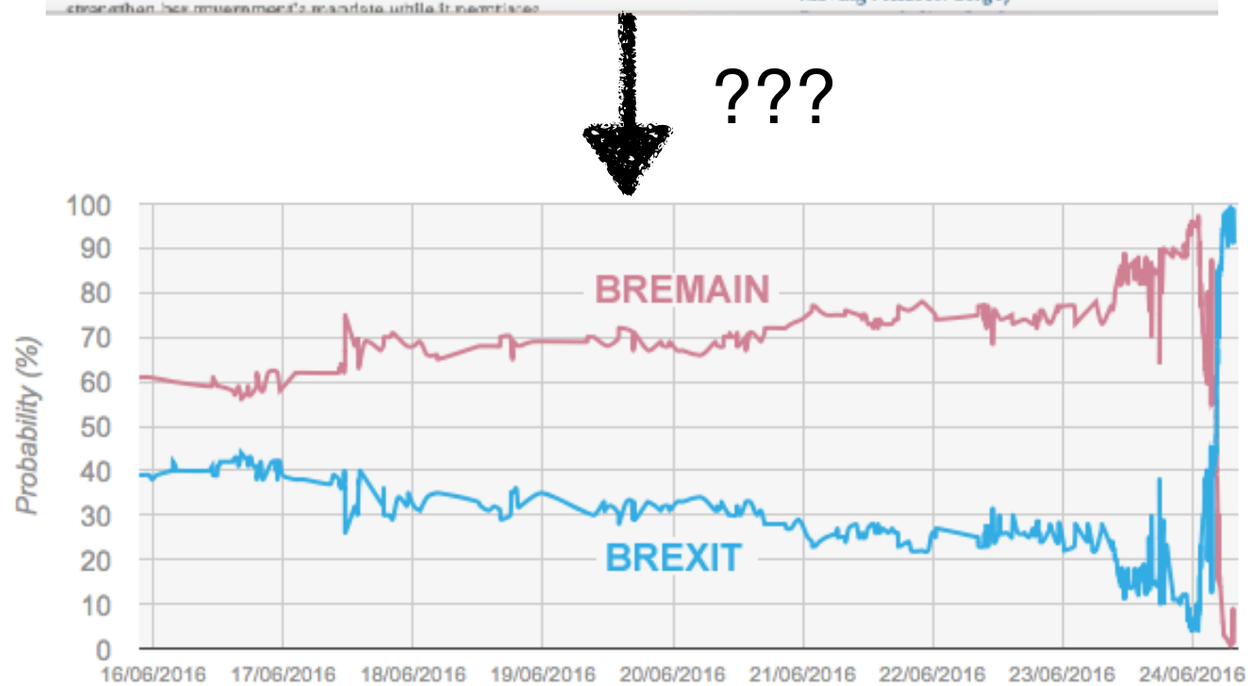
Updates on Britain's exit from the European Union

- Key Points About a Snap Election in Britain — APR 18
- Transcript of Theresa May's Address Calling for Vote — APR 18
- Will London Fall? How Dare You! — APR 13
- Britain's Uneasy Labor Market — APR 13
- Moving Pictures: Sergey — APR 11



Challenges

Off-chain data injection authenticity concerns

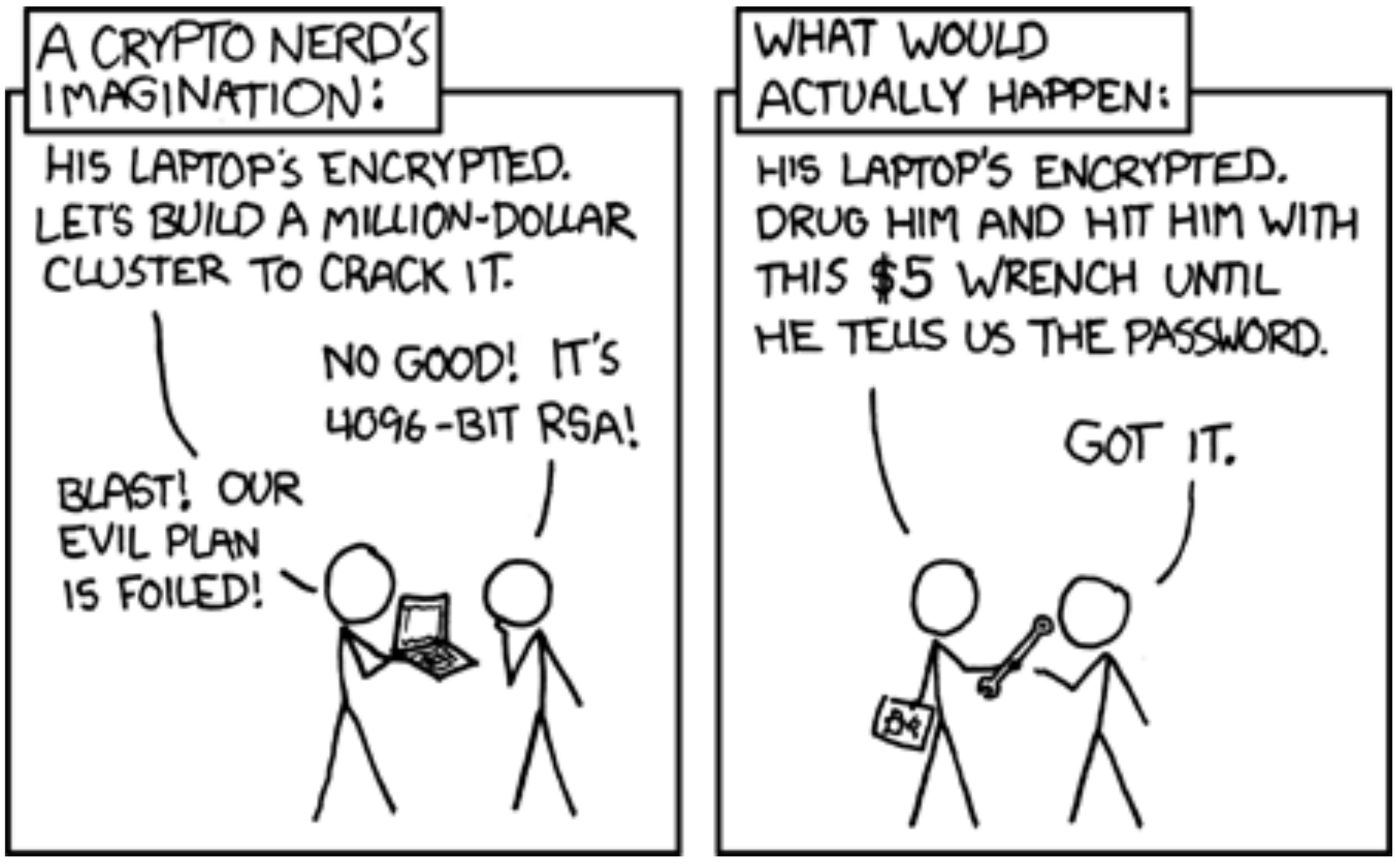


Challenges

Security

Challenges

Security



Challenges

Legalization and Regulation Risks

WOMEN@FORBES MAR 10, 2017 @ 04:20 PM 40,745

The Little Black Book of Billionaire Secrets

SEC Rejects Winklevoss Bitcoin ETF, Sending Price Tumbling

Laura Shin, CONTRIBUTOR

I cover Bitcoin, blockchain, fintech, personal finance and career FULL BIO

Opinions expressed by Forbes Contributors are their own.

On Friday, government regulators dampened the dreams of bitcoin enthusiasts, speculators and entrepreneurs Tyler and Cameron Winklevoss when it declined to approve the twins' proposal for a bitcoin

Challenges

Scalability Scalability Scalability

BTC ETH Visa

Transaction per second

Challenges

Scalability Scalability Scalability

BTC ETH Visa

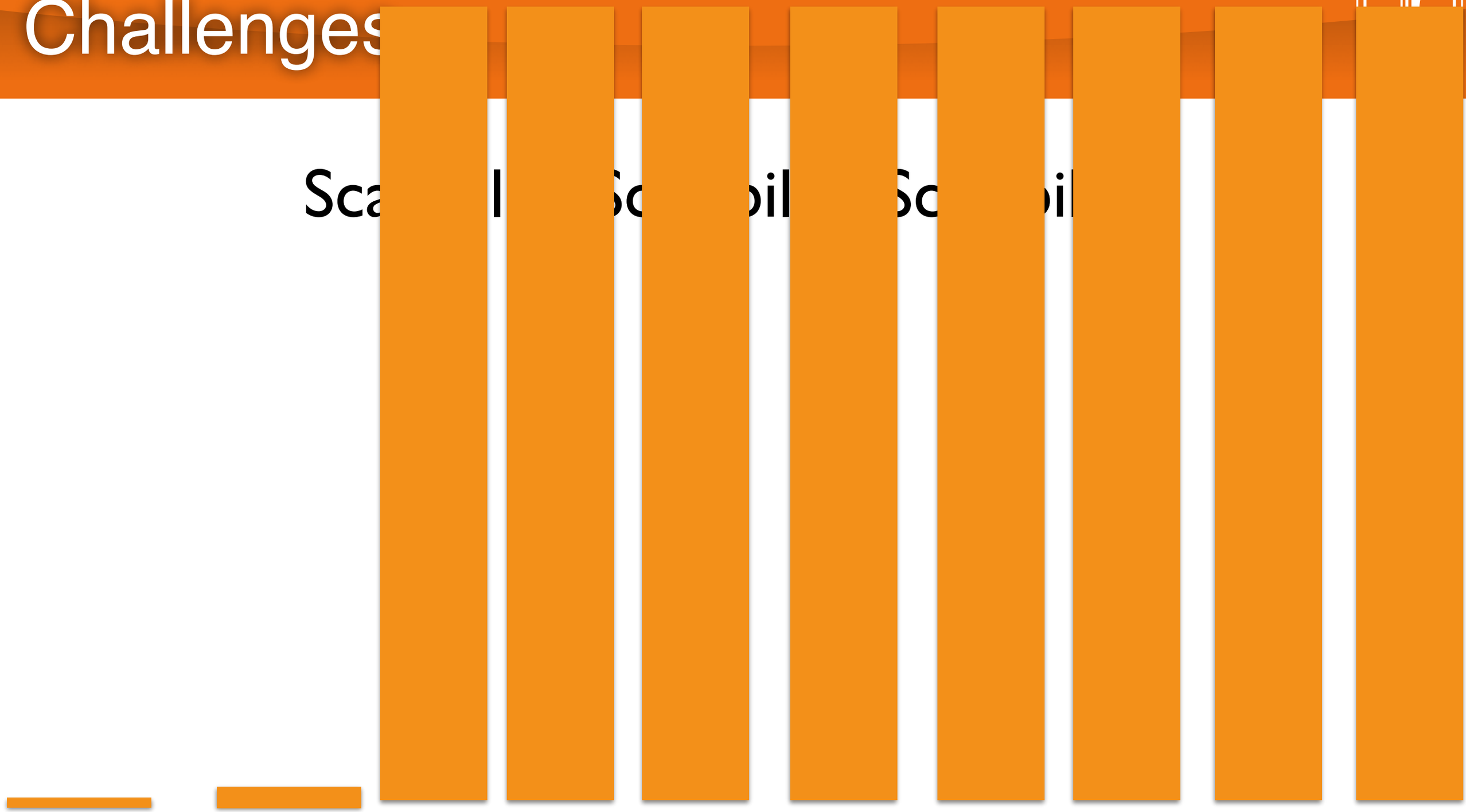
Transaction per second

Challenges

Scalability Scalability Scalability

Challenges

Sca l Sc bil Sc bil



Transaction per second

Challenges

Scalability Scalability Scalability

Why?

What are possible solutions?

Next class