Blockchains: Peering Through the Hype

Elaine Ou
Qcon London
March 8 2017

Blockchains and Distributed Ledgers

- Some Blockchain History
  - Crypto Anarchy
  - Early Distributed Ledgers
- Bitcoin Blockchain
  - Threat Model
  - What Makes a Blockchain Secure
  - What is a Bitcoin
- Programmable Ledgers
  - Smart Contracts
- Blockchain Use Cases

Intro to Crypto Anarchy

Set and Enforce Self-Defined Rules

- A system that relies on authority is expensive and inconsistent
    - Trusted third party may not be trustworthy
    - Vending machine vs human vendor
- Disintermediate financial authority
    - Private money (vs central bank)
    - Peer-to-peer transactions (vs third-party payment processors)
- Remove the ability for anyone to seize control
    - Decentralization
    - Encryption for privacy, access control

Threat Model

- Counterparty, who might try to cheat you
- Government, which might try to stop you
- Anyone else, who might be coerced by the first two

- A little trust goes a long way. The less you use, the further you'll go.

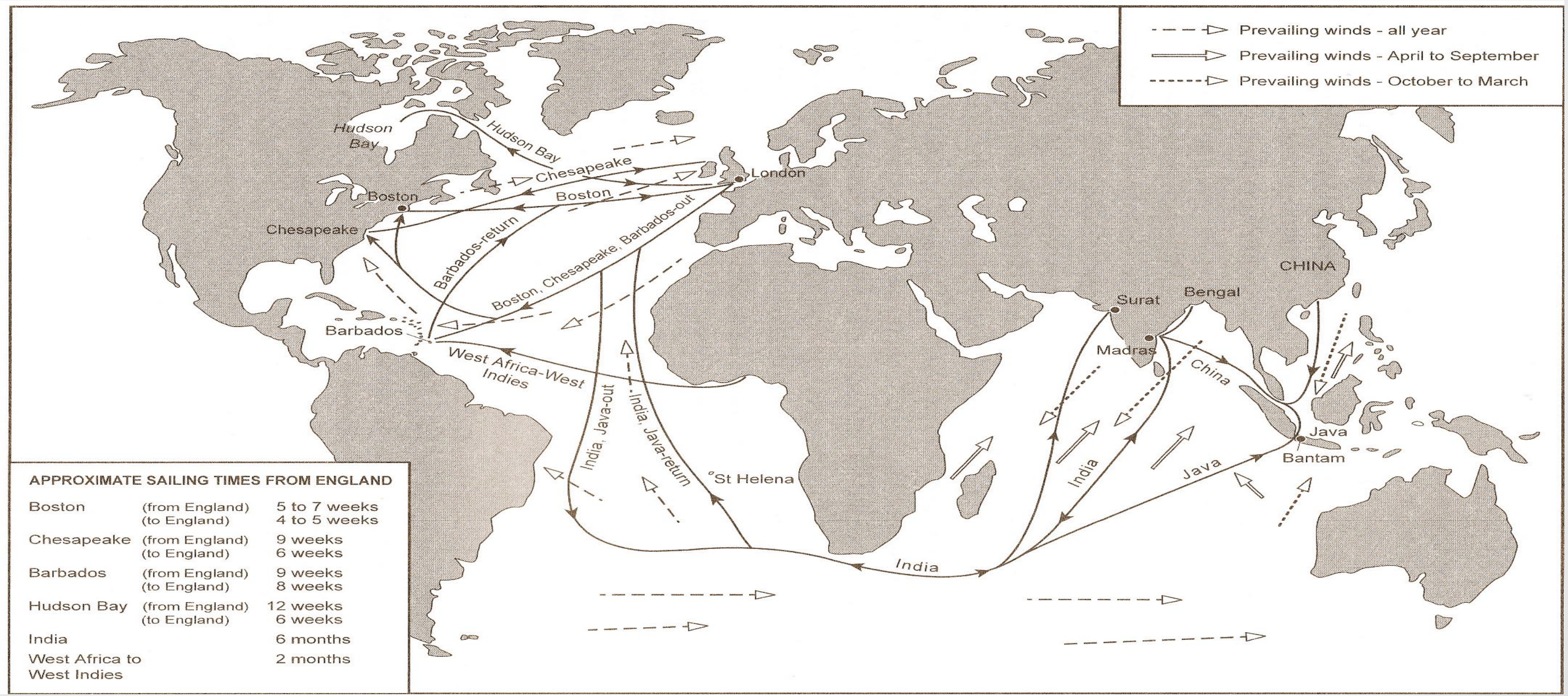
Replacing the Role of Government

- A rule is only as good as its enforceability
- Things a central authority should do
  - Protect property rights
  - Enforce contractual obligations
- Use technology as a substitute for government
  - Maintain secure asset registries using digital signatures
  - Self-enforcing contracts

Secure Asset Registries with Minimal Trust

British East India Company, 17th Century

Distributed Ledgers are Hard



APPROXIMATE SAILING TIMES FROM ENGLAND

Boston	(from England) (to England)	5 to 7 weeks 4 to 5 weeks
Chesapeake	(from England) (to England)	9 weeks 6 weeks
Barbados	(from England) (to England)	9 weeks 8 weeks
Hudson Bay	(from England) (to England)	12 weeks 6 weeks
India		6 months
West Africa to West Indies		2 months

Replication and Synchronization: Fault-Tolerant Distributed Ledgers

How do we build secure distributed ledgers in the digital world?

Tuesday September 1st 1835

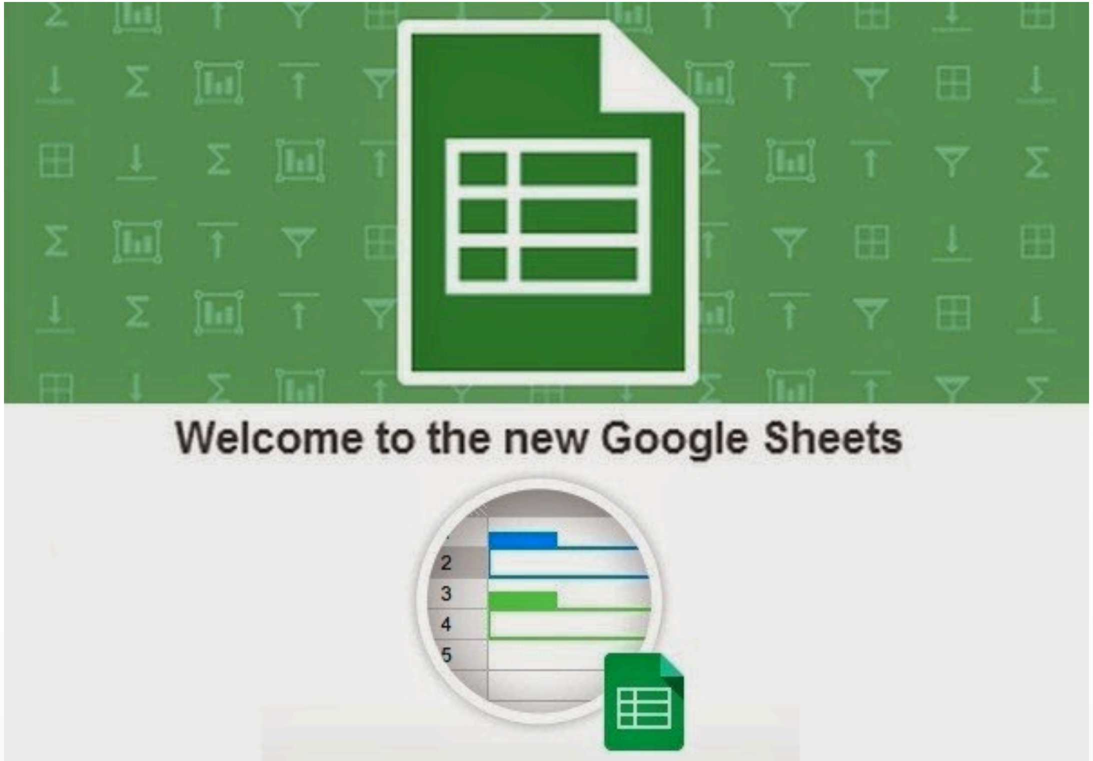
Wednesday October 14th 1835

- All the physical world problems, plus…
- Information is cheap to copy
  - Fake news can flood out real news
  - (In the physical world, phantom ships can't deliver fake records)
- Information is easy to edit
  - Forged records
  - Double-entry bookkeeping prevented edits

The Blockchain Solution

Protecting the Integrity of Data

How About a Shared Spreadsheet?

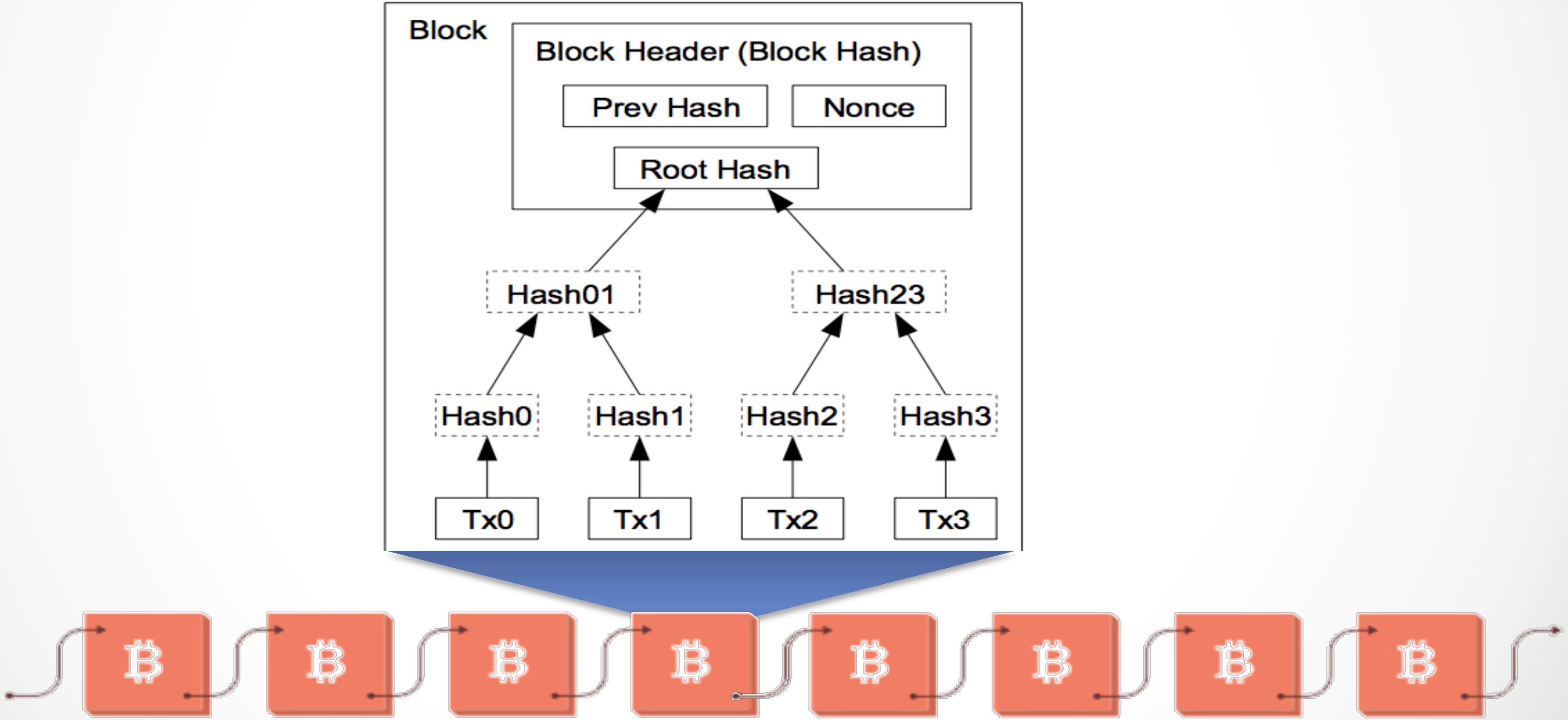


Threat Model

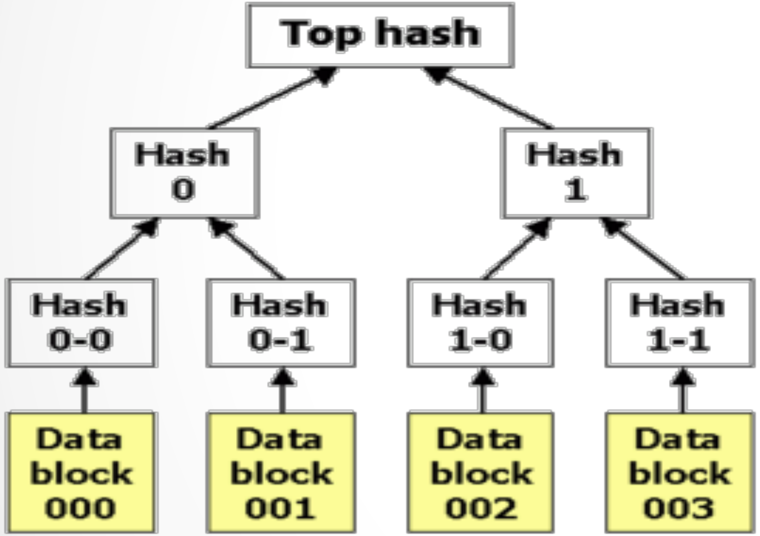
- Counterparty, who might try to cheat you
- Government, which might try to stop you
- Anyone else, who might be coerced by the first two

- If none of those are part of your threat model, use a shared spreadsheet.

Bitcoin Blockchain

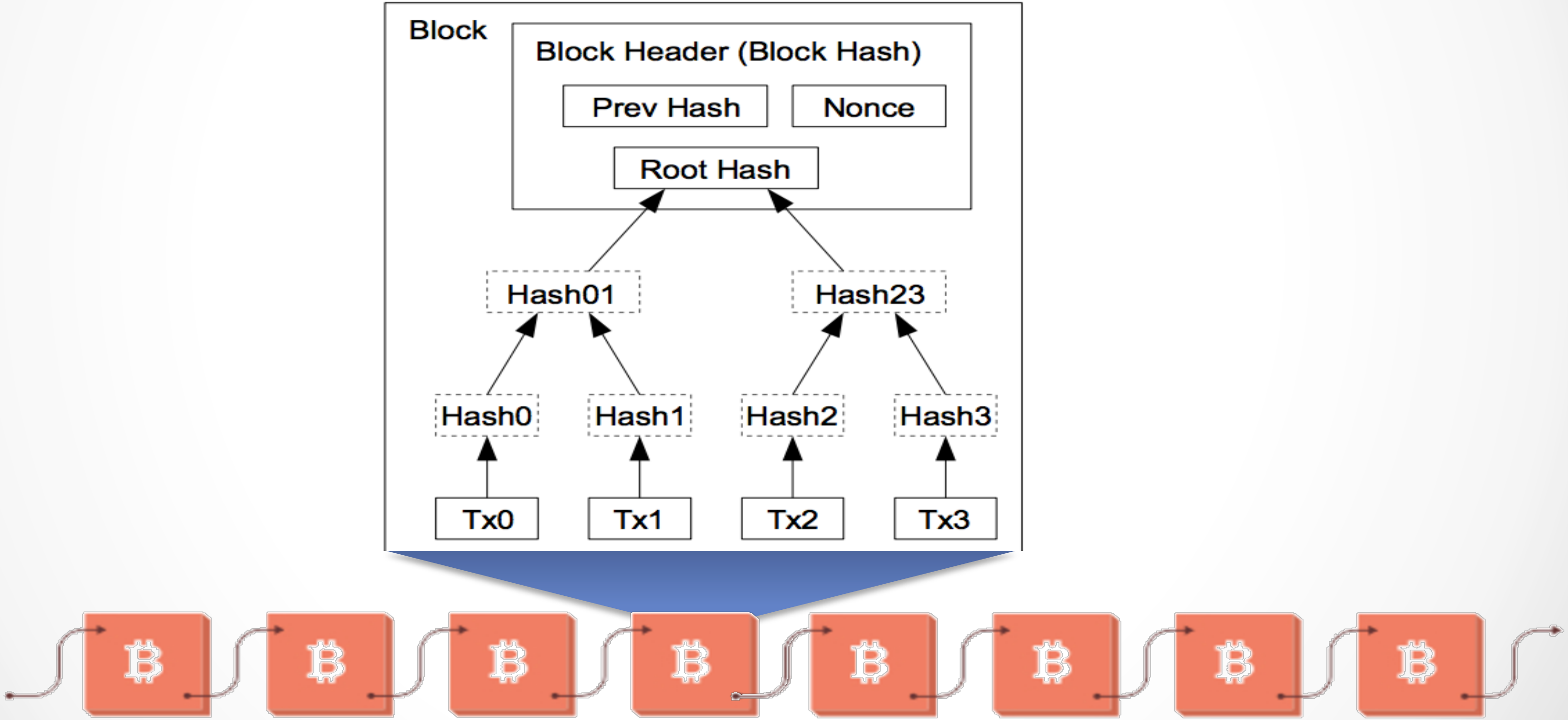


Merkle Trees



- Set of ledger entries
  - Transaction data: eg, Alice pays Bob
- Non-leaf nodes labeled with hash of child nodes
- Hash trees are used to verify that data are unaltered

Bitcoin Blockchain

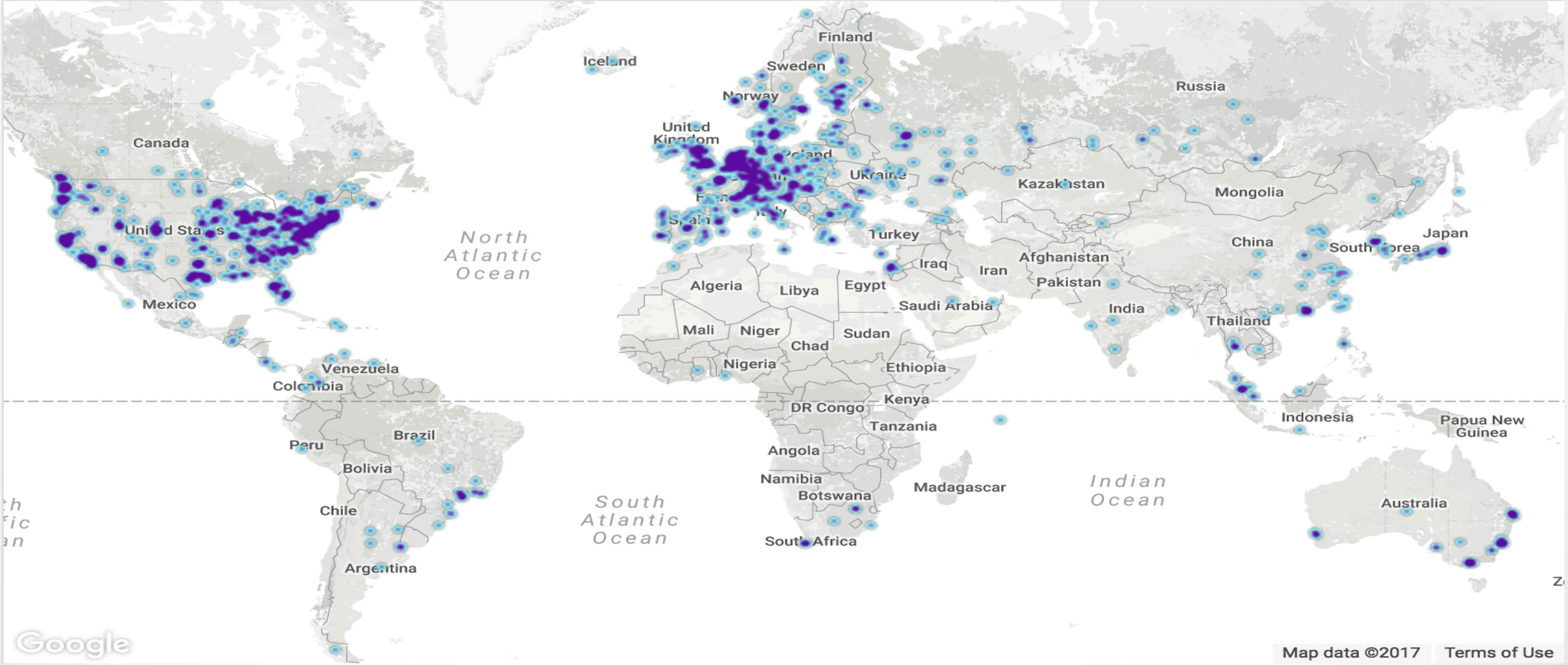


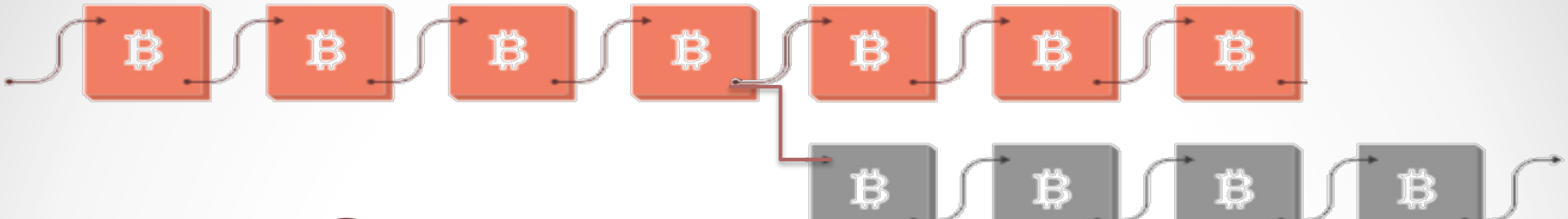
Censorship-Resistance

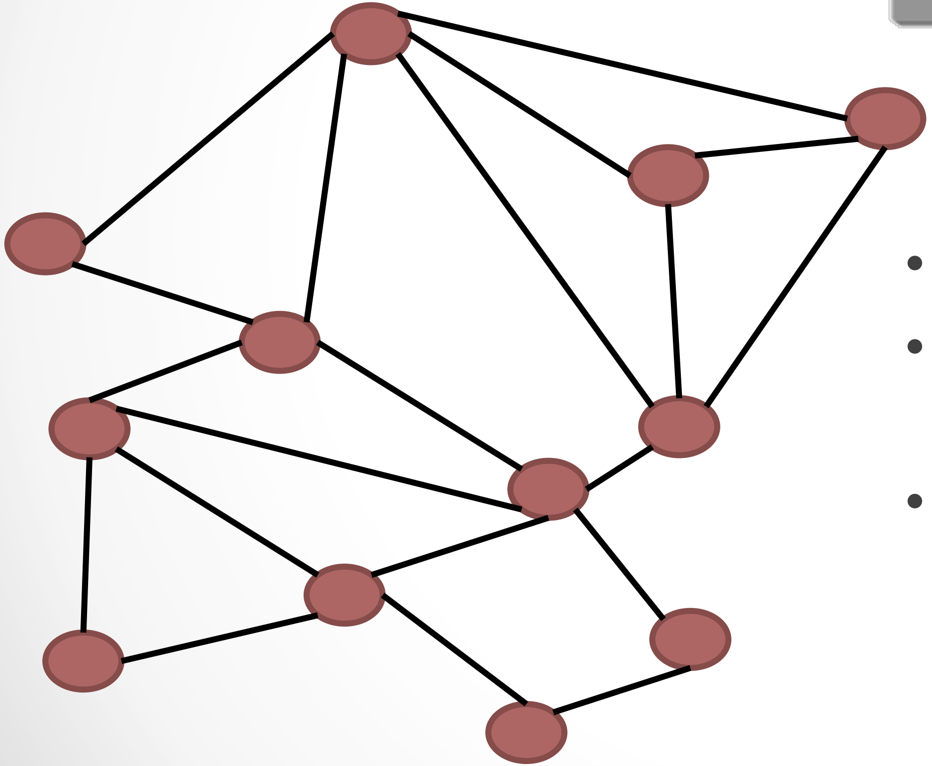
- Attempts at Digital Money
    - DigiCash: Anonymous cash
        - refused to comply with regulators, bankrupt
    - E-Gold: Gold-backed digital money
        - shut down, prosecuted, fined
    - Liberty Reserve: Private currency
        - shut down, founder in prison
    - PayPal: Private currency
        - caved to regulators

- Solution: Decentralize it

Bitcoin Network







- Nodes submit new blocks
- Nodes check every block received, drop if invalid
- Longest blockchain is valid, but a bad node can attempt to create a longer chain

Public Network Problems

- Longest blockchain is valid
- BUT! On the internet, no one knows you’re a sockpuppet

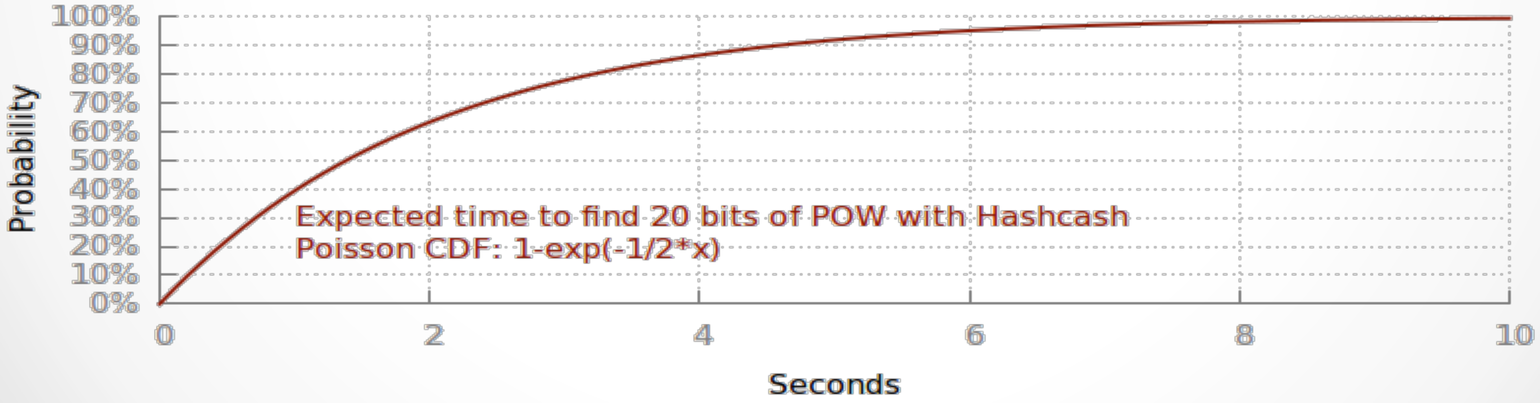
Proof of Work

- New blocks must contain proof of work
  - Require participant to complete a computational challenge to signal honesty
- Proof
  - Unforgeable: Sacrifice something to produce it
  - Easily verified
- Useful for:
  - Deterring Denial of Service attacks
  - Prevent spam
  - Encourage valid blocks
  - Store of value

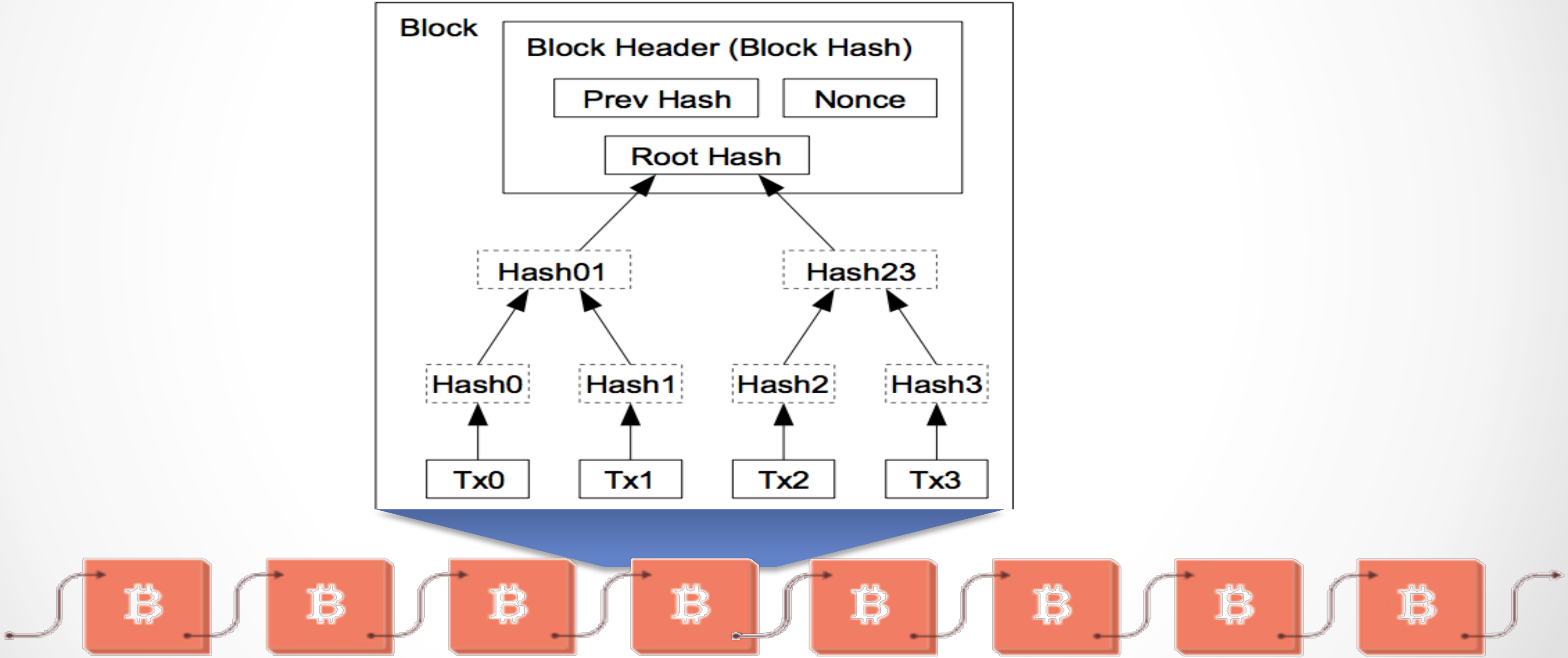
Proof of Work

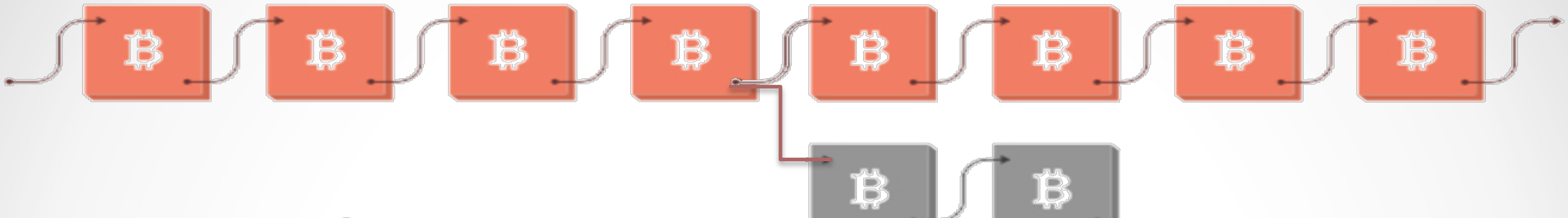
- Cryptographic hashes are hard to invert, easy to verify
- Hashcash: Use brute force to find a hash result with a certain number of leading 0s

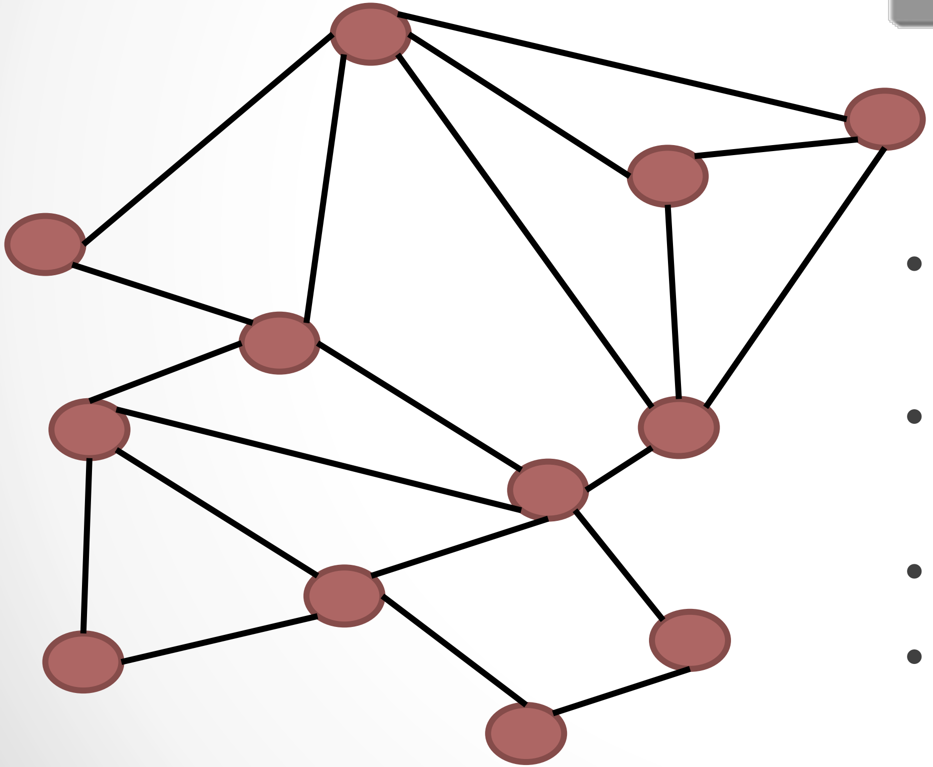
```
SHA256(SHA256(block_header, rand)) = “0000…”
```



Work is Expensive (10 mins)
Validation is Cheap



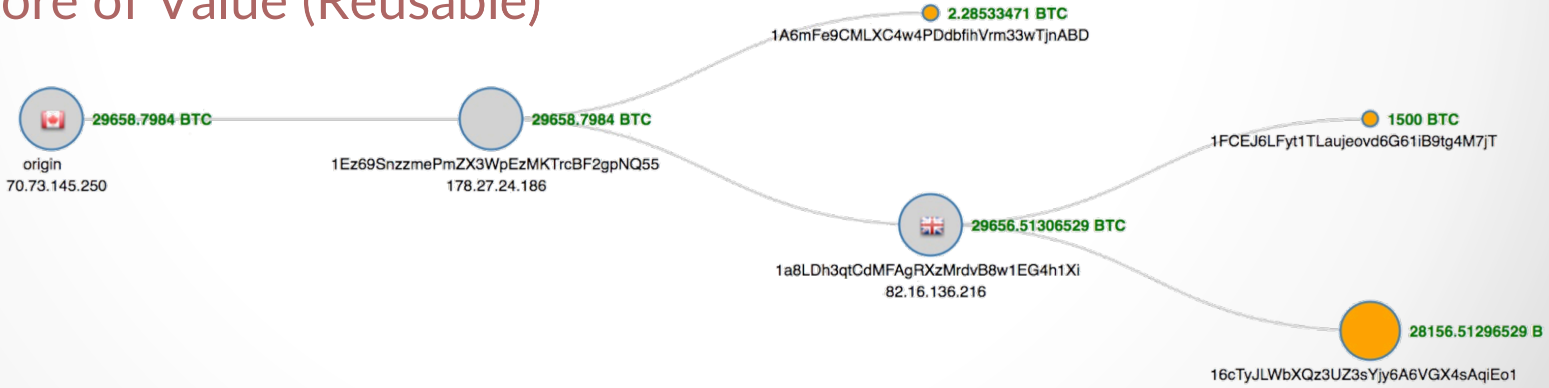




- Proof of Work randomizes block submitter
- Every block validated by every node
- Invalid blocks are dropped
- Longest chain is valid

What is a Bitcoin?

- Each block has a block reward transaction
  - “Bitcoin Mining”
- Proof of Work
  - Unforgeable, Easily verified
  - Store of Value (Reusable)


29658.7984 BTC
origin
70.73.145.250
29658.7984 BTC
1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55
178.27.24.186
2.28533471 BTC
1A6mFe9CMLXC4w4PDdbfihVrm33wTjnABD
29656.51306529 BTC
1a8LDh3qtCdMFAgRXzMrdvB8w1EG4h1Xi
82.16.136.216
1500 BTC
1FCEJ6LFyt1TLaujeovd6G61iB9tg4M7jT
28156.51296529 B
16cTyJLWbXQz3UZ3sYjy6A6VGX4sAqiEo1

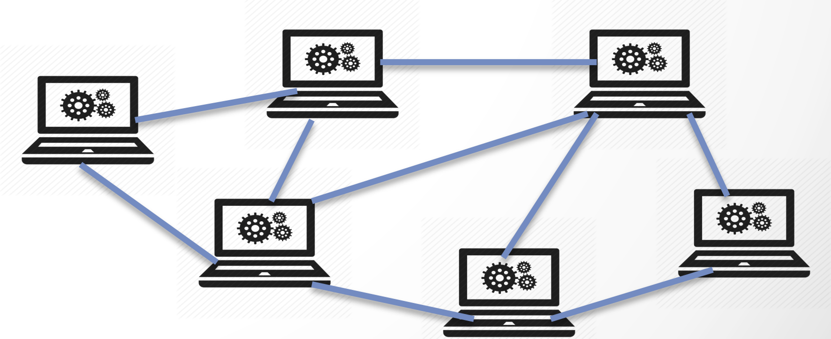
Programmable Ledgers

• • •

Smart Contracts

Smart Assets on the Blockchain

- Spreadsheets do more than store numbers – they can perform calculations
- Blockchain assets can be programmable
  - Bitcoin already has simple functions available
- We are already replicating ledgers. Now replicate computations as well



Bitcoin Script

- There are no bitcoins. Only transaction histories.
- Encumbrance
  - Instructions recorded with each transaction that describe how to spend the output

	Debit (input)	Credit (output)
Coinbase	100	
Alice		100 🔒
Alice	100	
Bob		100 🔒
Bob	100	
Elaine!!!		100

Bitcoin Script

- OP_CHECKSIG <public key> <signature>
  - Each Bitcoin address is a public key
  - Owner signs transaction with private key
  - Is the signature valid for the public key?
- OP_CHECKMULTISIG OP_3 <public key1> <public key2> <public key3> OP_2 <signature1> <signature2>
  - Now we need 2 signatures out of the 3 public keys
  - Escrow

Smart Contracts

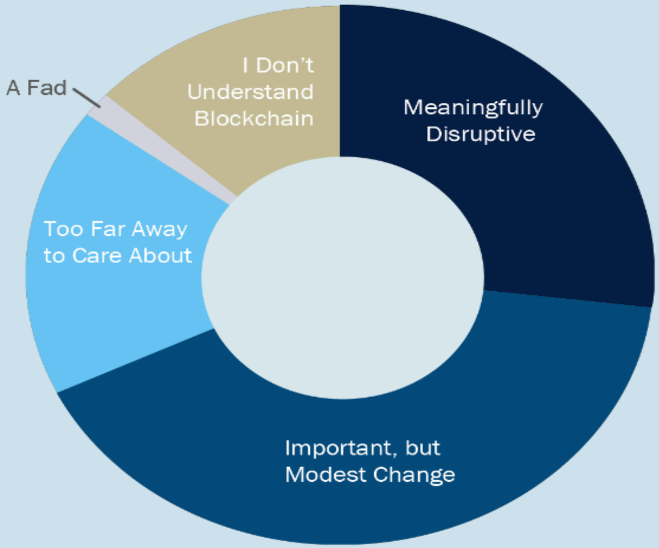
- Self-enforcing agreements that automate the exchange of value
- Ethereum
  - Turing-complete smart contracts platform
  - Software applications run on all nodes across network
- Potential applications
  - Gambling
  - Crowdfunding tokens
  - Voting
  - Decentralized Autonomous Organization
  - Financial instruments with cash flows

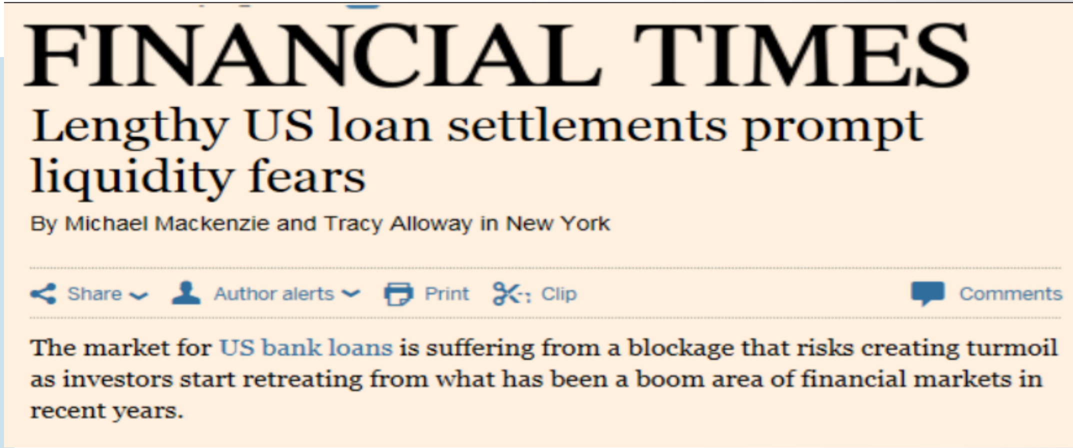
How Blockchains Will Save Billions of Dollars for Financial Institutions

…

(just kidding)

How disruptive will blockchain be?




FINANCIAL TIMES

Lengthy US loan settlements prompt liquidity fears

By Michael Mackenzie and Tracy Alloway in New York

The market for US bank loans is suffering from a blockage that risks creating turmoil as investors start retreating from what has been a boom area of financial markets in recent years.

COSTS

Reduce costs of paying a middle man or running a back-office with manual processes.

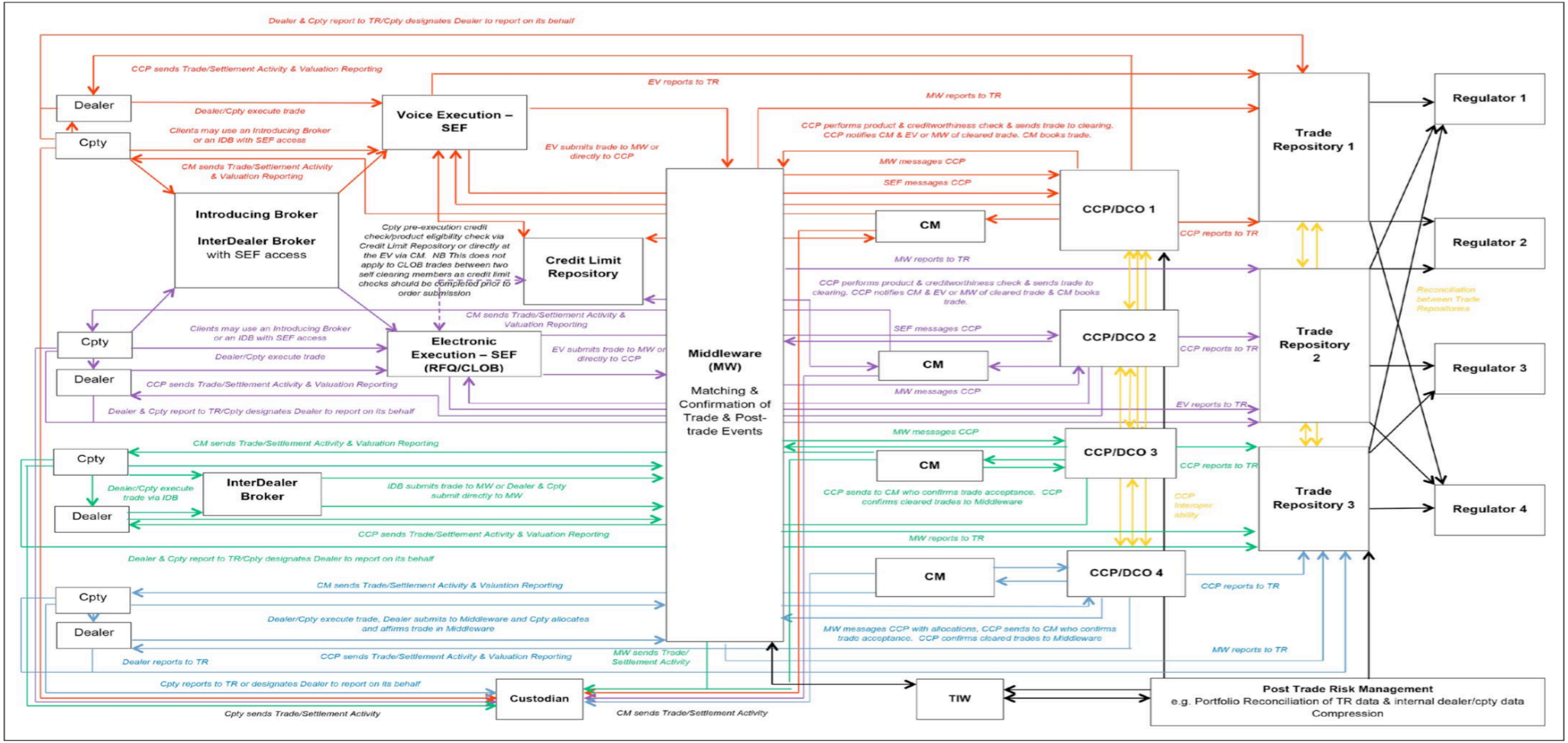
CAPITAL

Settlement risk is minimized with automation, which reduces the collateral and counterparty risk.

SPEED

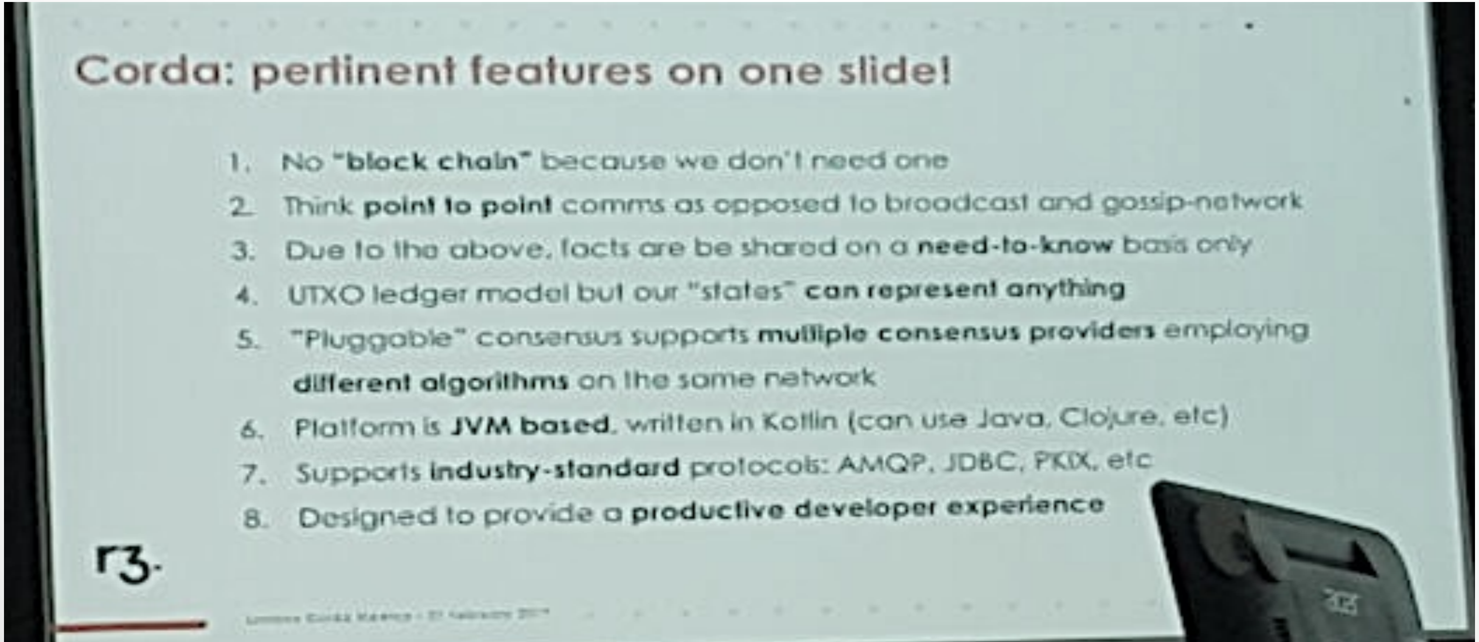
Simply put, T+3 or even sometimes T+30 could go to T+0.

Derivatives Processing Workflow


Dealer & Cpty report to TR/Cpty designates Dealer to report on its behalf
CCP sends Trade/Settlement Activity & Valuation Reporting
EV reports to TR
MW reports to TR
Dealer
Cpty
Dealer/Cpty execute trade
Clients may use an Introducing Broker or an IDB with SEF access
CM sends Trade/Settlement Activity & Valuation Reporting
Voice Execution – SEF
EV submits trade to MW or directly to CCP
CCP performs product & creditworthiness check & sends trade to clearing. CCP notifies CM & EV or MW of cleared trade. CM books trade.
MW messages CCP
SEF messages CCP
Trade Repository 1
Regulator 1
Introducing Broker
InterDealer Broker with SEF access
Cpty pre-execution credit check/product eligibility check via Credit Limit Repository or directly at the EV via CM. NB This does not apply to CLOB trades between two self clearing members as credit limit checks should be completed prior to order submission
Credit Limit Repository
CCP/DCO 1
CM
CCP reports to TR
MW reports to TR
Regulator 2
CCP performs product & creditworthiness check & sends trade to clearing. CCP notifies CM & EV or MW of cleared trade & CM books trade.
Reconciliation between Trade Repositories
CM sends Trade/Settlement Activity & Valuation Reporting
Clients may use an Introducing Broker or an IDB with SEF access
Cpty
Electronic Execution – SEF (RFQ/CLOB)
Dealer/Cpty execute trade
Dealer
EV submits trade to MW or directly to CCP
Middleware (MW)
Matching & Confirmation of Trade & Post-trade Events
SEF messages CCP
CCP/DCO 2
CM
CCP reports to TR
Trade Repository 2
Regulator 3
CCP sends Trade/Settlement Activity & Valuation Reporting
MW messages CCP
Dealer & Cpty report to TR/Cpty designates Dealer to report on its behalf
EV reports to TR
CM sends Trade/Settlement Activity & Valuation Reporting
MW messages CCP
Cpty
CCP/DCO 3
CM
CCP reports to TR
Dealer/Cpty execute trade via IDB
InterDealer Broker
IDB submits trade to MW or Dealer & Cpty submit directly to MW
Dealer
CCP sends to CM who confirms trade acceptance. CCP confirms cleared trades to Middleware
CCP Interoper ability
Trade Repository 3
Regulator 4
CCP sends Trade/Settlement Activity & Valuation Reporting
MW reports to TR
Dealer & Cpty report to TR/Cpty designates Dealer to report on its behalf
CM sends Trade/Settlement Activity & Valuation Reporting
CM
CCP/DCO 4
Cpty
CCP reports to TR
Dealer/Cpty execute trade, Dealer submits to Middleware and Cpty allocates and affirms trade in Middleware
MW messages CCP with allocations, CCP sends to CM who confirms trade acceptance. CCP confirms cleared trades to Middleware
Dealer
MW reports to TR
Dealer reports to TR
CCP sends Trade/Settlement Activity & Valuation Reporting
MW sends Trade/ Settlement Activity
Cpty reports to TR or designates Dealer to report on its behalf
Custodian
TIW
Post Trade Risk Management
e.g. Portfolio Reconciliation of TR data & internal dealer/cpty data
Compression
Cpty sends Trade/Settlement Activity
CM sends Trade/Settlement Activity

Blockchains for Banks

- ~~Proof of Work~~
- ~~Public Network~~



Corda: pertinent features on one slide!

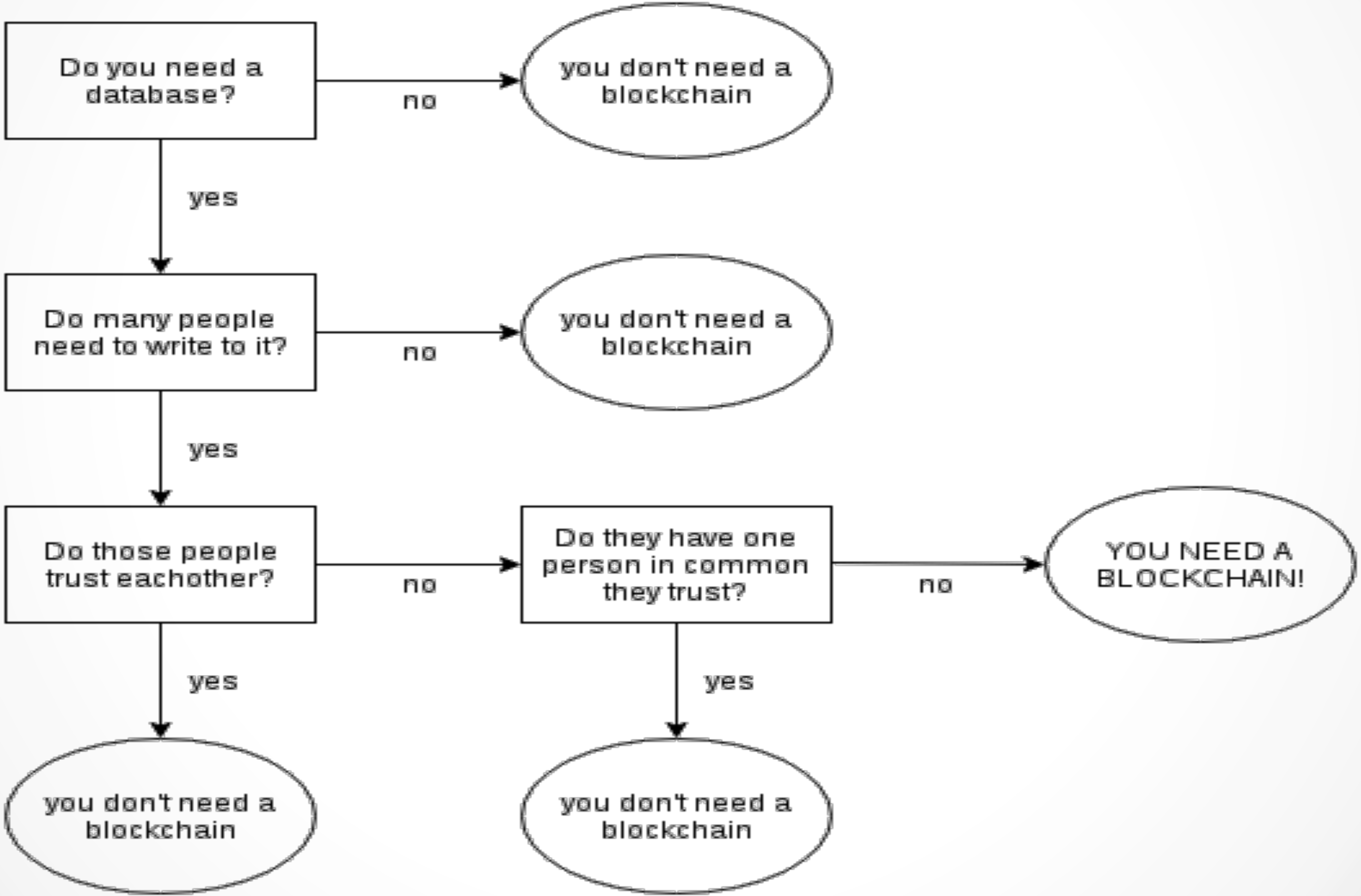
1. No "**block chain**" because we don't need one
2. Think **point to point** comms as opposed to broadcast and gossip-network
3. Due to the above, facts are be shared on a **need-to-know** basis only
4. UTXO ledger model but our "states" **can represent anything**
5. "Pluggable" consensus supports **multiple consensus providers** employing **different algorithms** on the same network
6. Platform is **JVM based**, written in Kotlin (can use Java, Clojure, etc)
7. Supports **industry-standard** protocols: AMQP, JDBC, PKIX, etc
8. Designed to provide a **productive developer experience**

r3.

[illegible]

Do you need a blockchain?

Do you need a blockchain?



Do you need a database?

no

you don't need a blockchain

yes

Do many people need to write to it?

no

you don't need a blockchain

yes

Do those people trust eachother?

yes

you don't need a blockchain

no

Do they have one person in common they trust?

yes

you don't need a blockchain

no

YOU NEED A BLOCKCHAIN!

Disintermediation of Authority

- Track and transfer digital asset ownership
- Financial instruments
- Management of identity or credentials
  - DNS
  - Reputation
- Distributed cloud storage market
- Timestamps
  - Future proof of current information
  - (Like anagrams for scientific discoveries)

Information Management

- Electronic Data Interchange
  - Access control for medical records
  - Shared information for supply chain management
- Provenance of goods
  - Track farm to table
- Many more possibilities
  - The technology is still young!

Conclusion

- Blockchains can provide security from:
  - Counterparty, who might try to cheat you
  - Government, which might try to stop you
  - Anyone else, who might be coerced by the first two

- Technology can create a way for people to set and enforce their own rules

Thank you.

Elaine Ou
elaine@globalfinancialaccess.com