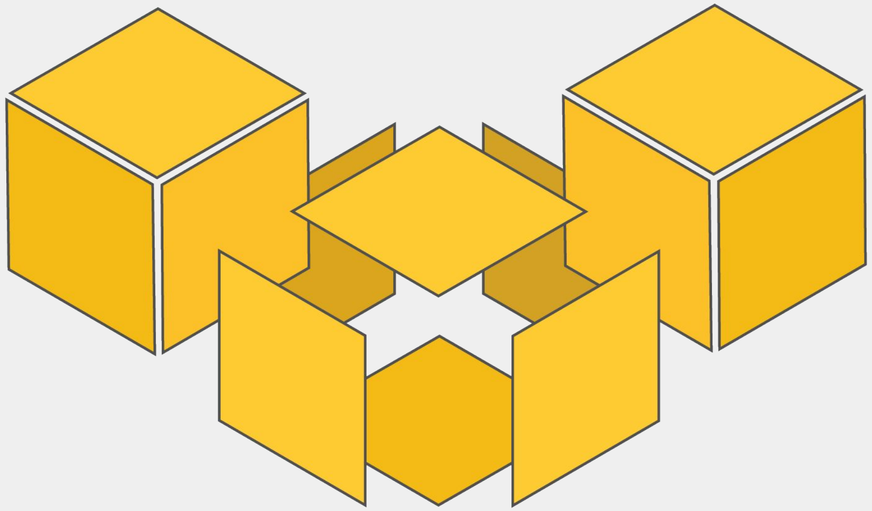


Blockchain
AT BERKELEY

Workshop 1 -
What is Blockchain?

Overview

1. Intro and Basic Concepts
2. Understanding Bitcoin and Consensus
3. Blockchain Types and Platforms
4. DOA Energy Example
5. Conclusion

Blockchain at Berkeley

Intro and Basic Concepts

Terminology

Bitcoin is the technology that started it all

- Bitcoin is a cryptocurrency

Blockchain is the technology underlying Bitcoin

- Enables distributed consensus

Community terminology

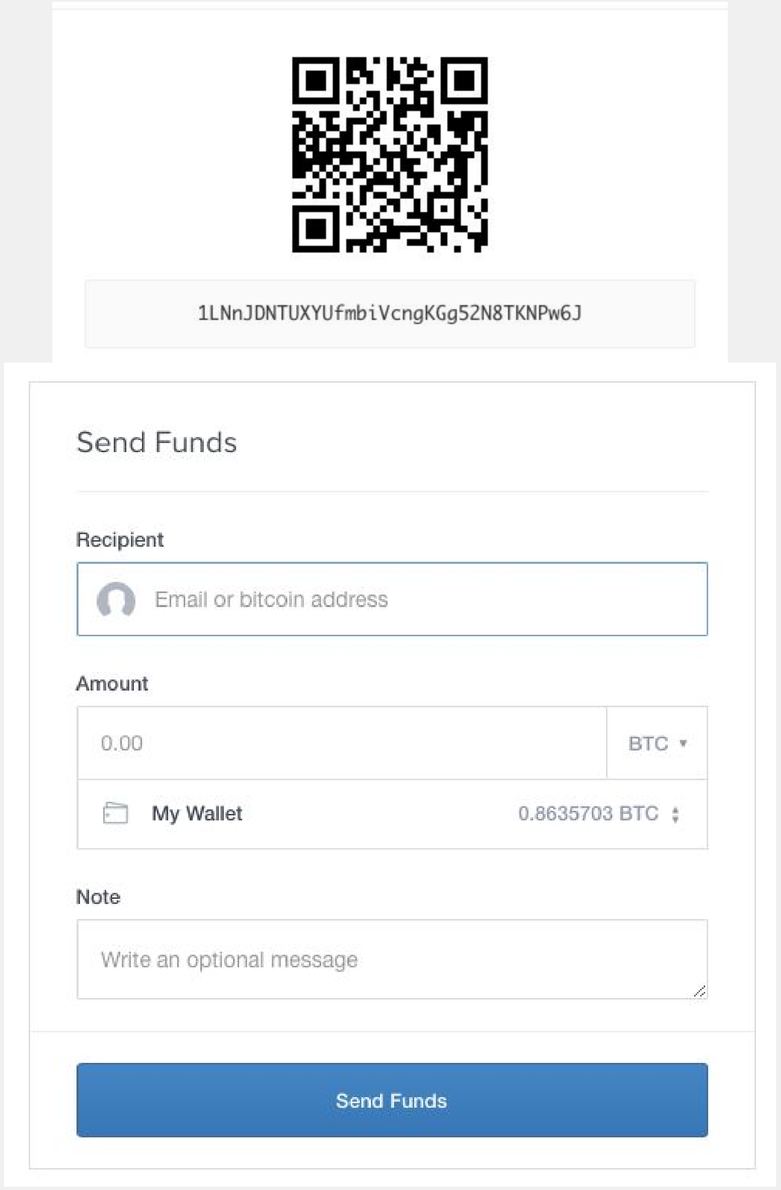
- **"crypto", "cryptocurrency"** - Bitcoin, Ethereum, more technical
- **"private blockchains", "permissioned ledgers",** or just **"blockchain"**
- "**distributed tech**" or **"decentralized tech"** - umbrella term

Blockchain at Berkeley

Understanding Bitcoin and Consensus

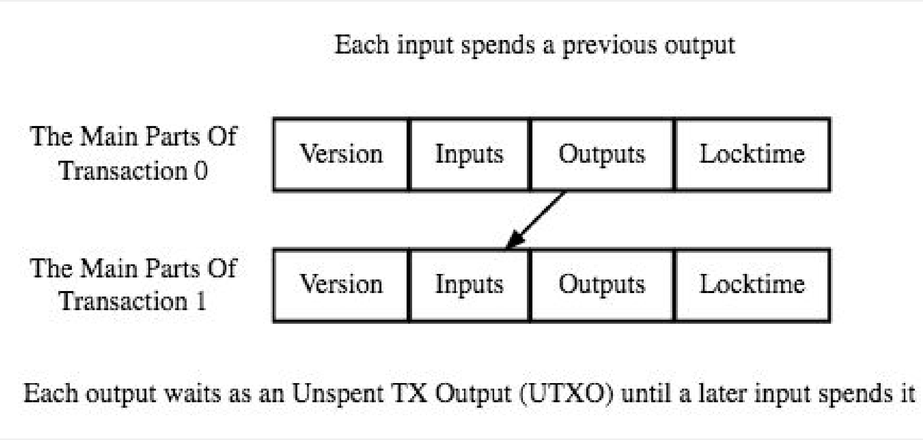
A Bitcoin Transaction - Basic Version

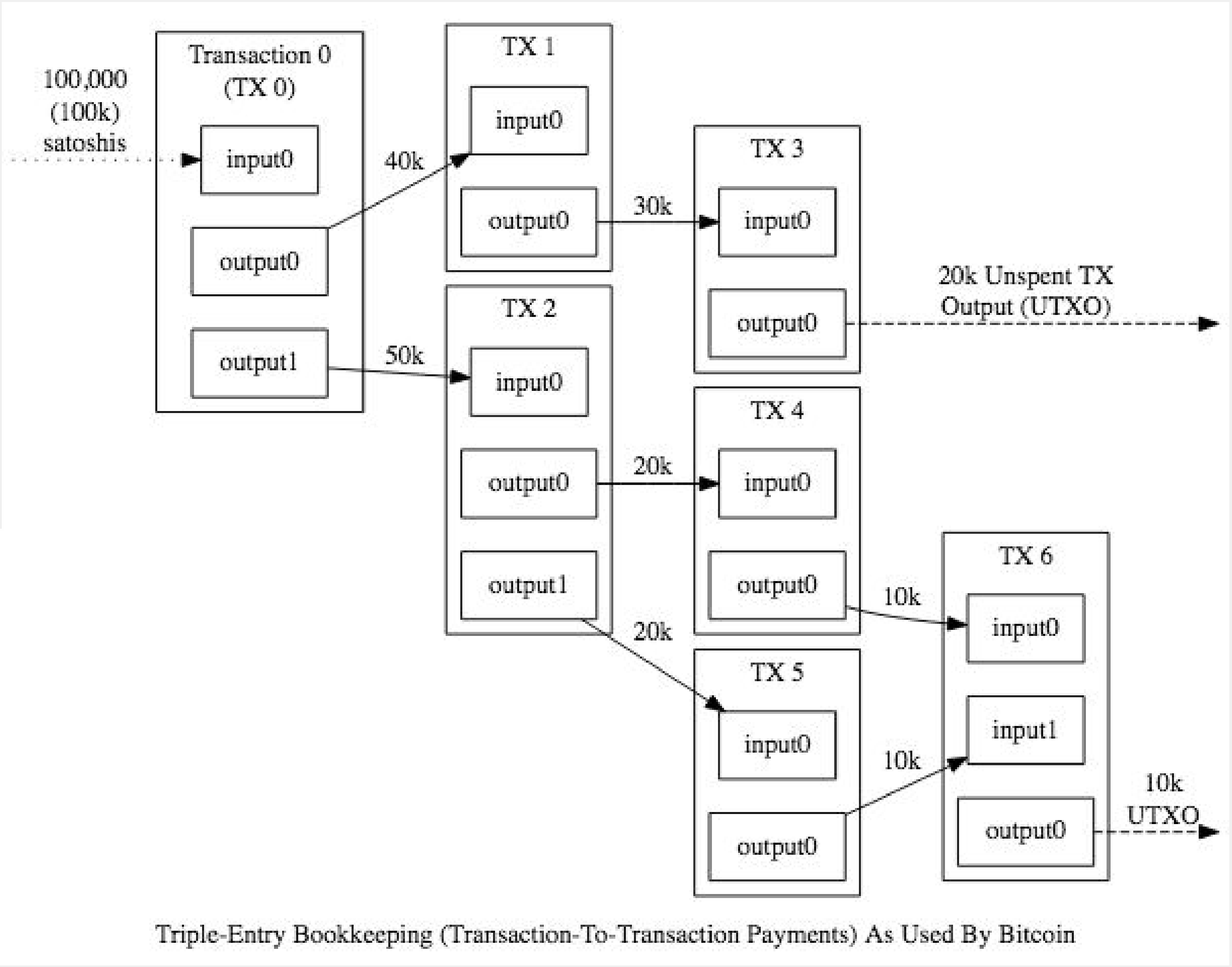
- Bitcoin exists as software
  - Transactions are conducted through wallet software
  - Wallet creation generates a Bitcoin address
- To receive money, you share your address
  - Sender specifies address and amount
- The transaction is broadcast to the network, where "miners" verify it and add it to the transaction history



Basic Concepts - Transaction

- Maps inputs addresses to output addresses
- Typical tx: one input, two outputs
- Contains signature of owner of funds





Source: [Bitcoin Developer Guide]

Transaction View information about a bitcoin transaction

447cb6623db32b5f28c94ac10551802075f053208fe995204a145197e2904bb9

3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v (44,000 BTC - Output)	3LrLWTSdd69oZVVQ6dtWaAAaBLn7N3rRjz - (Spent)	333.33328889 BTC
	3QkXtcSWJA9w77eCujnMBKDWFe7F7zwxTg - (Spent)	333.33328889 BTC
	3Qd7hXZoZ1iyXZznrbdUwUQBxHMmujdqhJ - (Spent)	333.33328889 BTC
	3ECJwvx9VgfotcUuEJMVNvmWnTGVMk179L - (Spent)	333.33328889 BTC
	3BuQmbmdce3e31GEovq5SgowLdfMgJzLDE - (Spent)	333.33328889 BTC
	3NwKLjJjzXSnBFQWokXRgBG3JeuF3bsnfE - (Spent)	333.33328889 BTC
	3GEaT8ZRXELcjMSFvGro6eZcC5S1LSLZuN - (Spent)	333.33328889 BTC
	35DVAzDtZDKAU94kFT9sxoscnuLCTxgwYc - (Spent)	333.33328889 BTC
	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v - (Unspent)	38,000 BTC
	35mwqShnStDro6uEB4bmsgbyBo8en6Byfm - (Spent)	333.33328889 BTC
	39pvSqfNcUosc8RGVWxyzKM3ny96a3uSkW - (Spent)	333.33328889 BTC
	39QNJSgQg5JnBXAtbF8ezkDn72VqWdPZPJ - (Spent)	333.33328889 BTC
	3L9qAGBQLbXkFAB2GpijnJXPScSVjuiJio - (Spent)	333.33328889 BTC
	37WSkANPVUQ8uuktf8hv671CejRtBtQ4tJ - (Spent)	333.33328887 BTC
	3EEwPZZ6pYRJSotCz9RBoVYPRnoWyGWEka - (Spent)	333.33328889 BTC
	3C4ABC7iPcAAKBh6SJXfvUSDBew3abCtw3 - (Spent)	333.33328889 BTC
	3HpQozfTzoXAsHf87m2mwJXUQ14LVtLgK4 - (Spent)	333.33328889 BTC
	337RfngTLRTpU7RT9sKWQWDdmfcdmWnugi - (Spent)	333.33328889 BTC
	3P2eoKr3vAeZhJcTzon3VFkv5r7DqSXW9G - (Spent)	333.33328889 BTC
		43,999.9992 BTC

Summary	
Size	1055 (bytes)
Received Time	2016-08-30 11:45:03
Included In Blocks	427512 (2016-08-30 11:51:09 + 6 minutes)
Confirmations	854 Confirmations
Relayed by IP	5.39.93.85 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	44,000 BTC
Total Output	43,999.9992 BTC
Fees	0.0008 BTC
Estimated BTC Transacted	333.33328887 BTC
Scripts	Hide scripts & coinbase

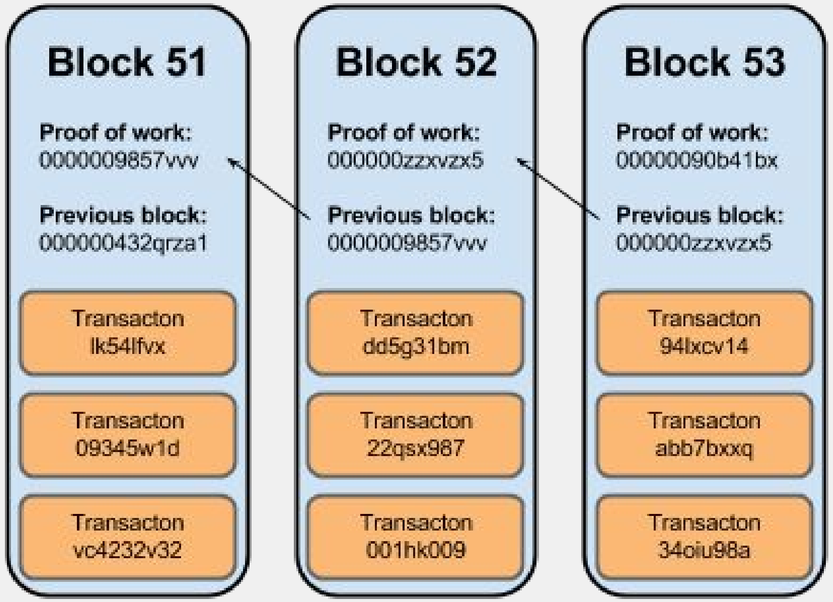
Basic Concepts - Blocks + Blockchain

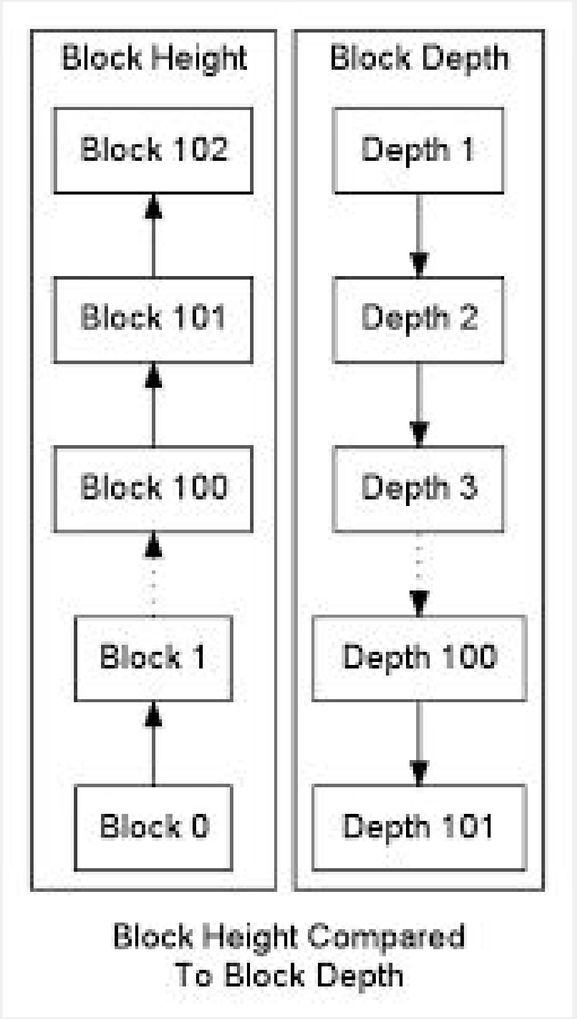
Blocks

- Contains an ordered bunch of transactions
  - Timestamps the transactions, are **immutable**
- Each block References a previous block

Blockchain

- The entire series of blocks 'chained' together



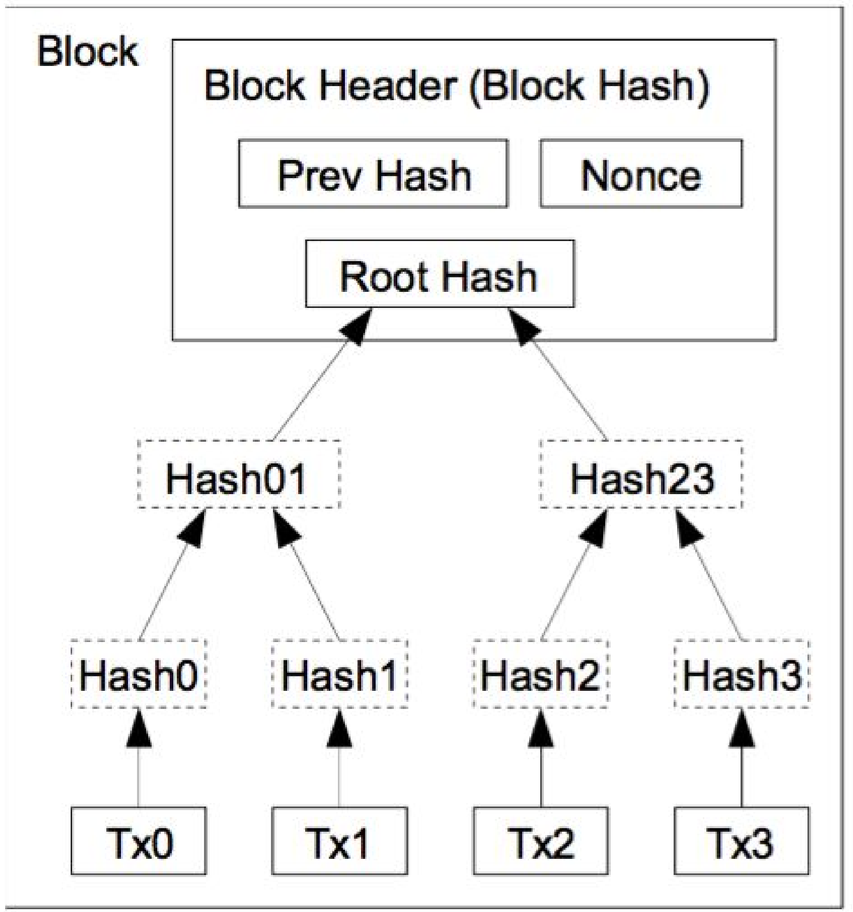


Block Height Compared To Block Depth

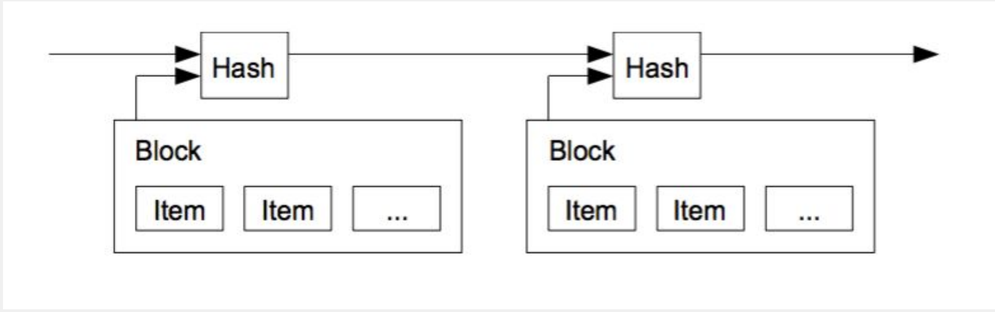
Source: Bitcoin Developer Guide

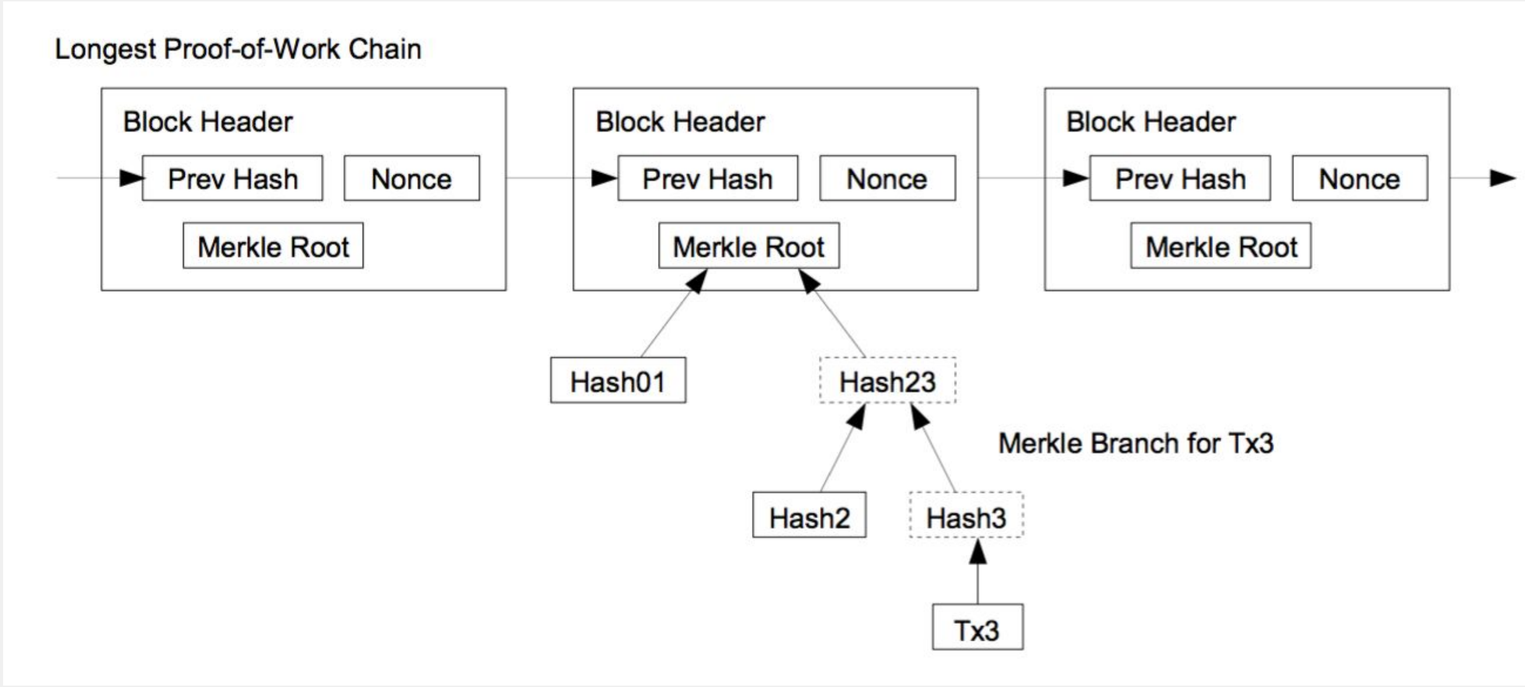
Source: Bitcoin Developer Guide

Merkle Trees



Transactions Hashed in a Merkle Tree





- Makes transaction history immutable
- PoW to add chains

Source: Nakamoto 2009

The Innovation of Satoshi Nakamoto

Bitcoin was created by Satoshi Nakamoto in 2009

- First ever decentralized, trustless system for transactions
  - A low cost financial system that only requires an internet connection
- Nakamoto solved the Double Spending problem
  - Prevent someone from spending the same asset twice
  - Solution? The blockchain + Proof-of-Work

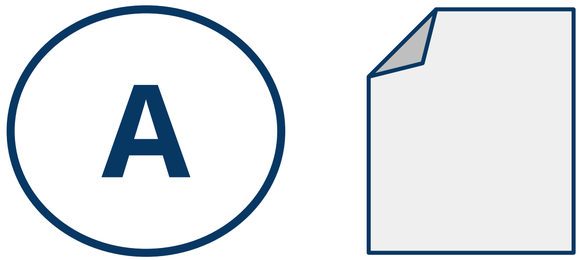
Dorian Satoshi Nakamoto
(not actually Satoshi Nakamoto)

Source: Bitcoin Developer Guide

Source: Bitcoin Developer Guide

v1

Alice writes and signs a message describing her transaction

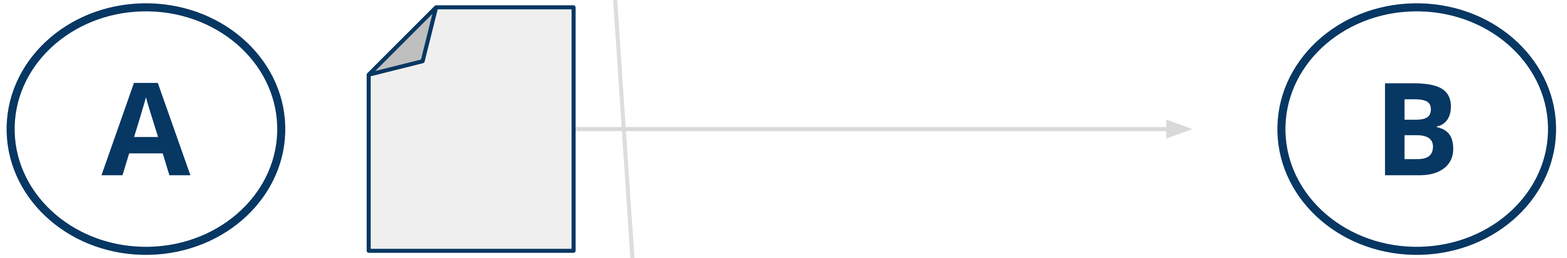


“I, Alice, am giving Bob one bitcoin.”

Slide by Viget

v1

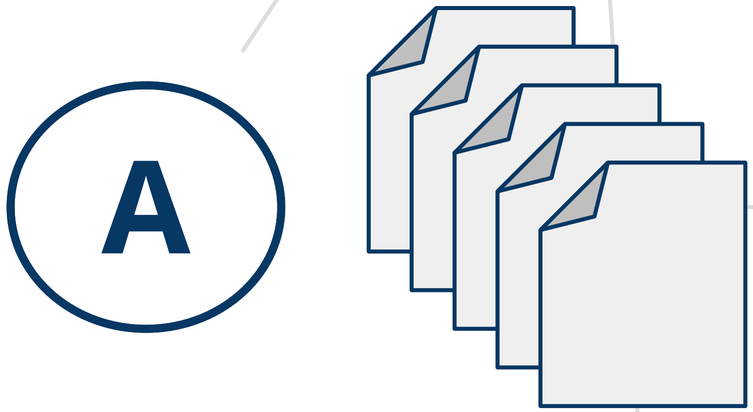
Alice sends her message to the world

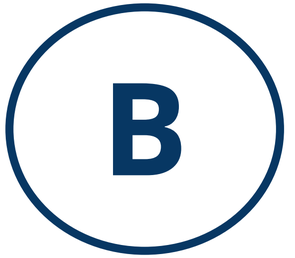


Slide by Viget

v1

Alice sends five identical messages



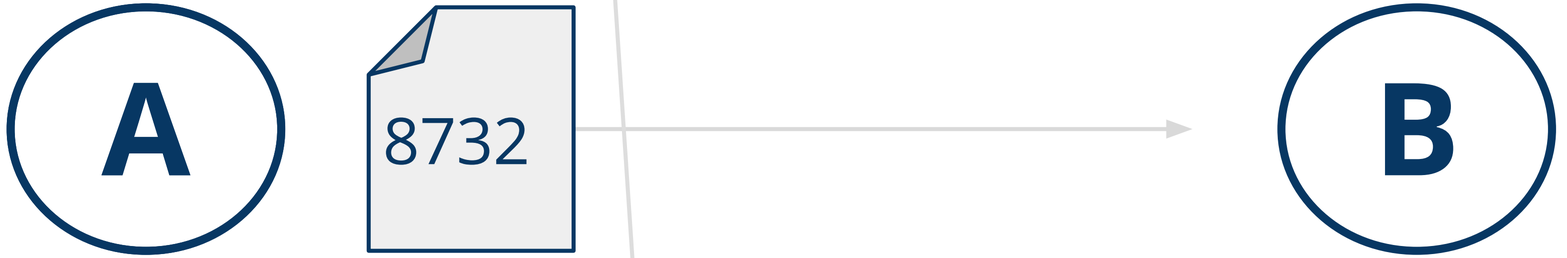


?

Slide by Viget

v2

Introducing uniquely identifiable serial numbers



Slide by Viget

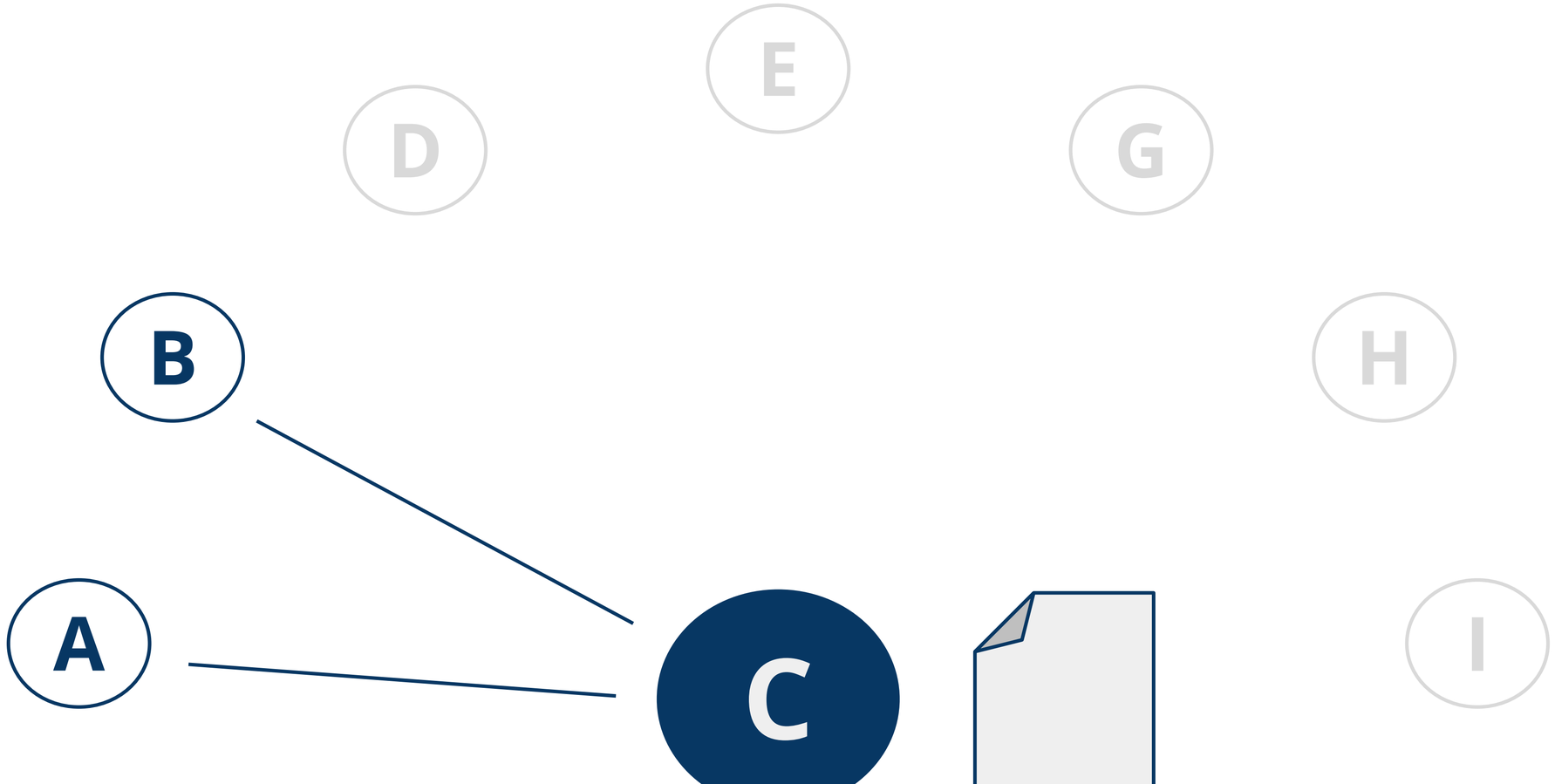
v2

Where do serial numbers come from?

?

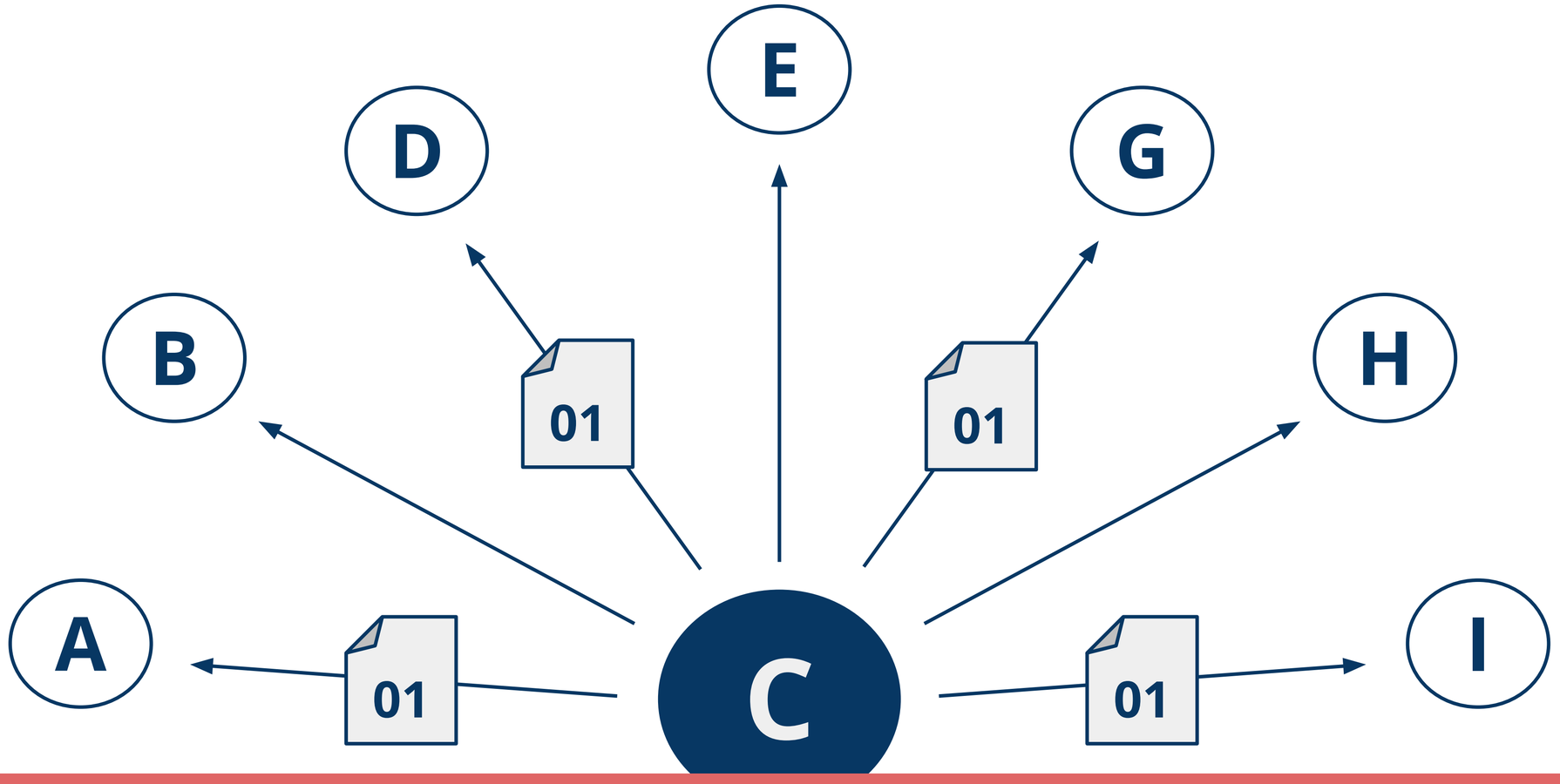
v2

A central bank manages transactions and balances



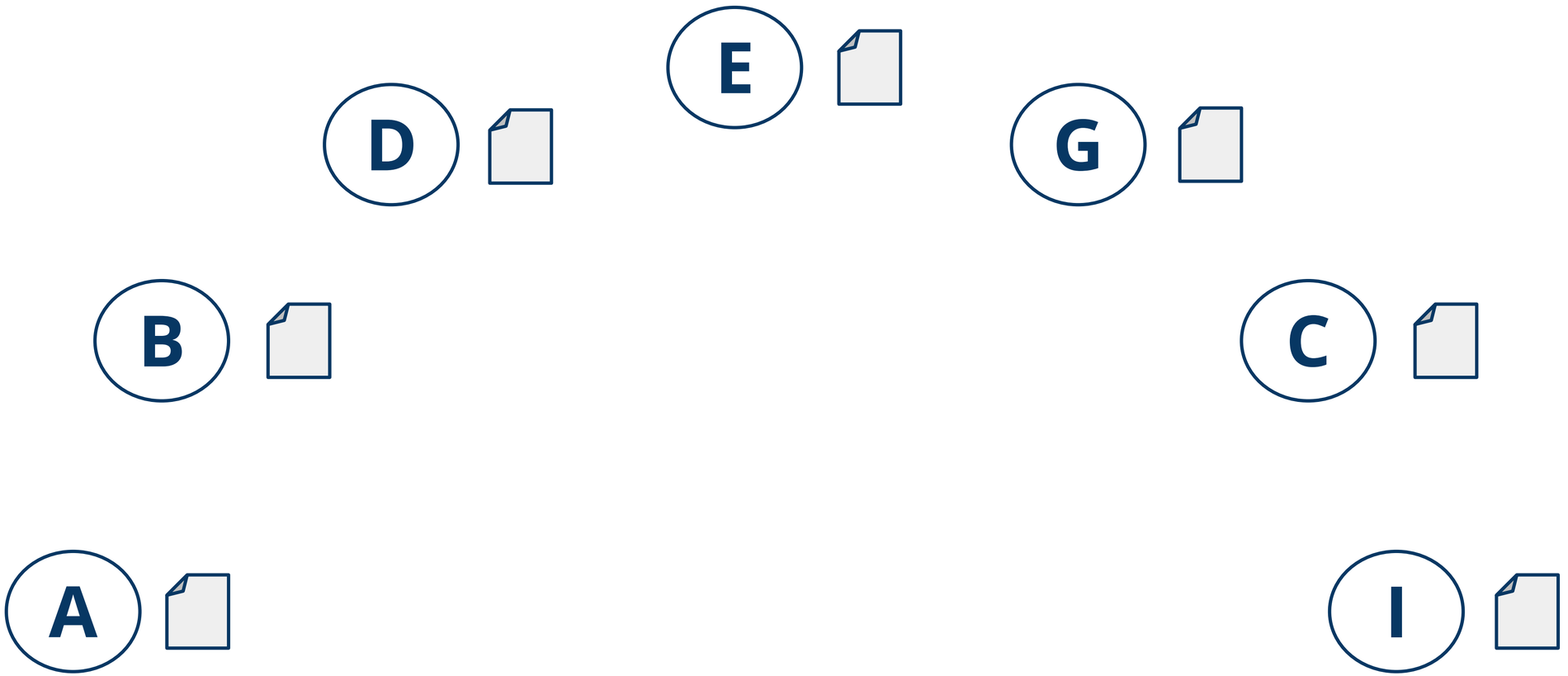
v2

Centralization



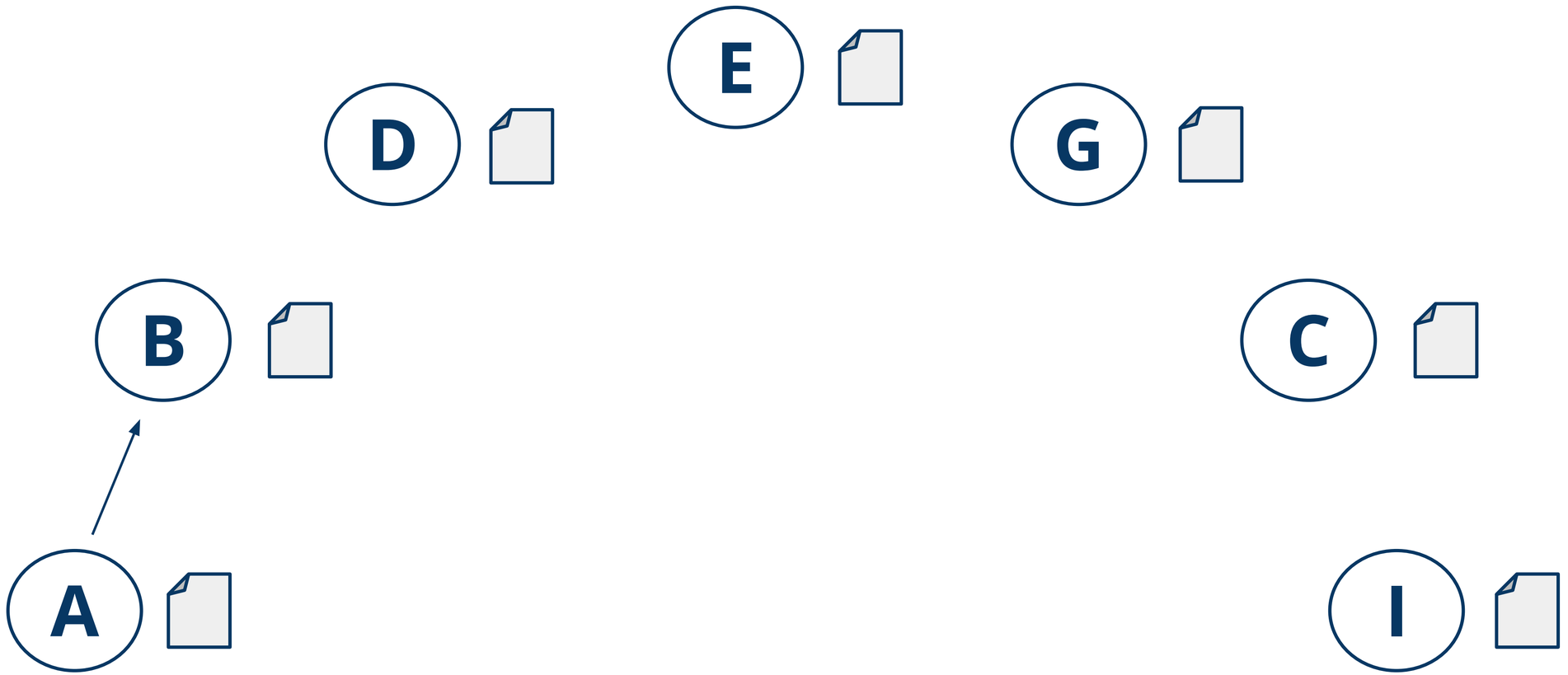
v3

Making everyone the bank



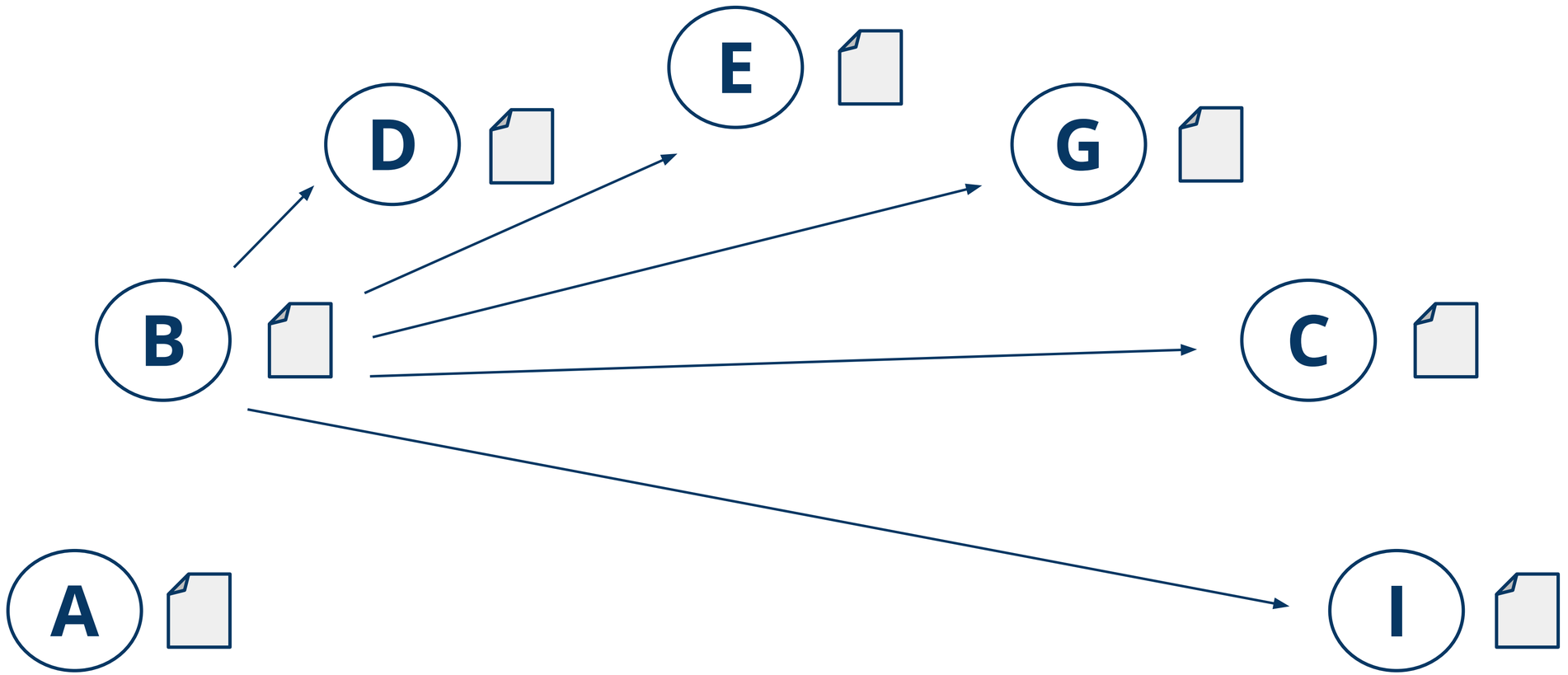
v3

Alice sends her transaction to Bob



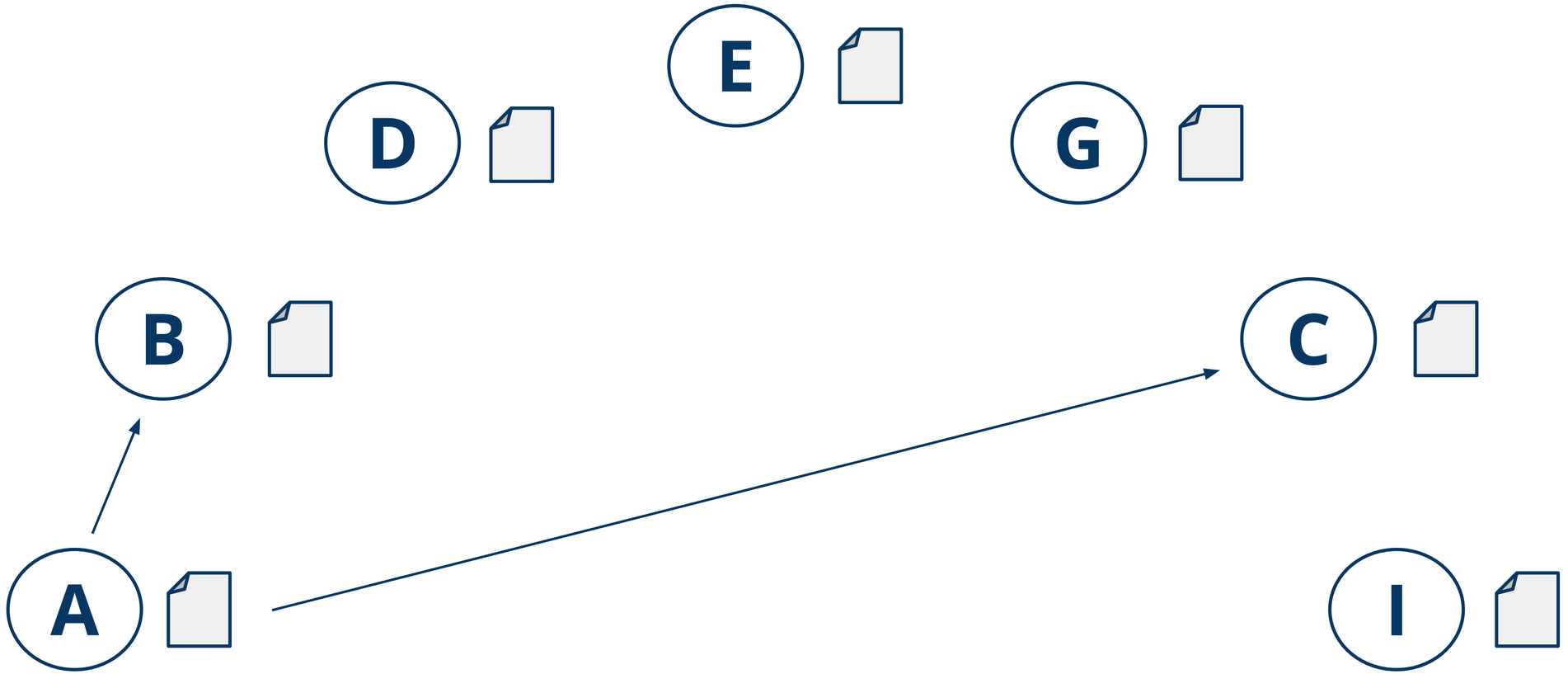
v3

Bob announces the transaction to the world



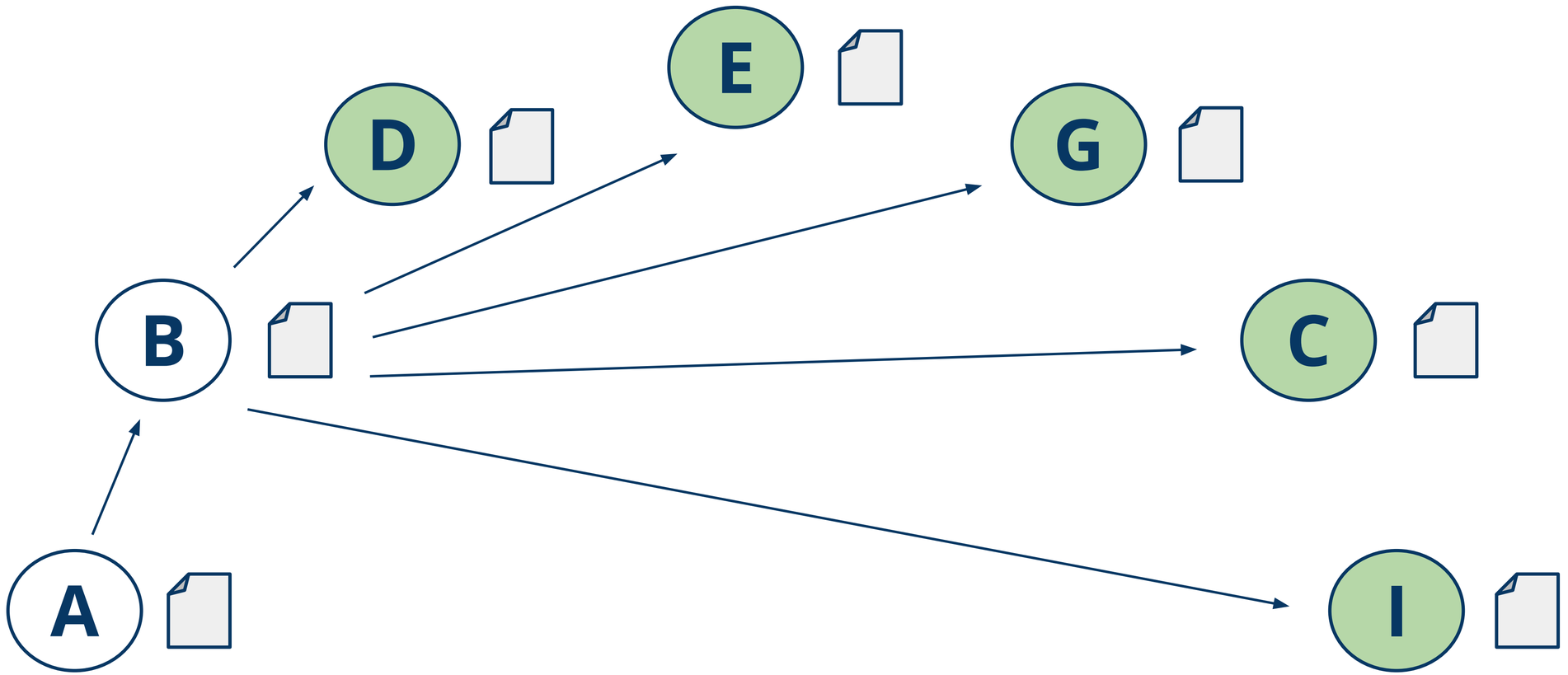
v3

Alice double spends on Bob and Charlie



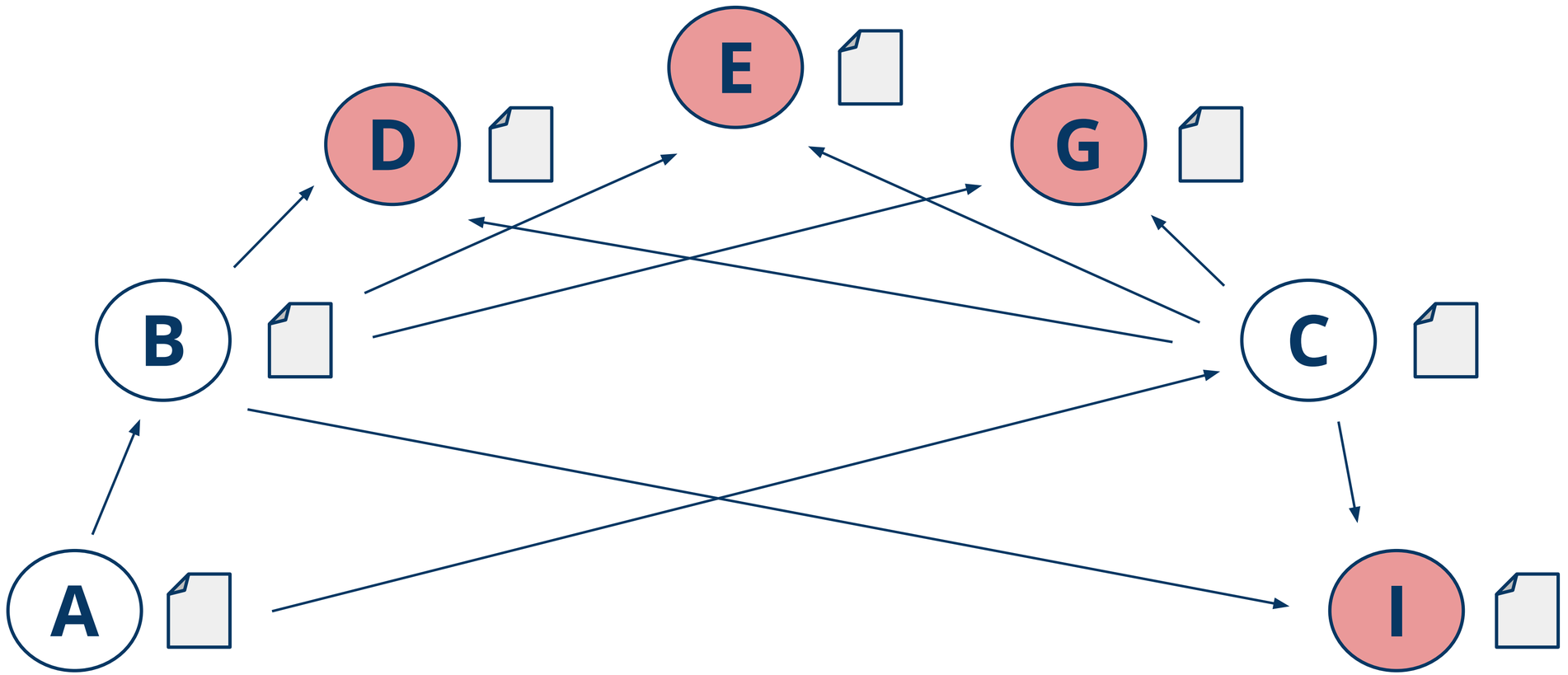
v4

Everyone verifies transactions



v4

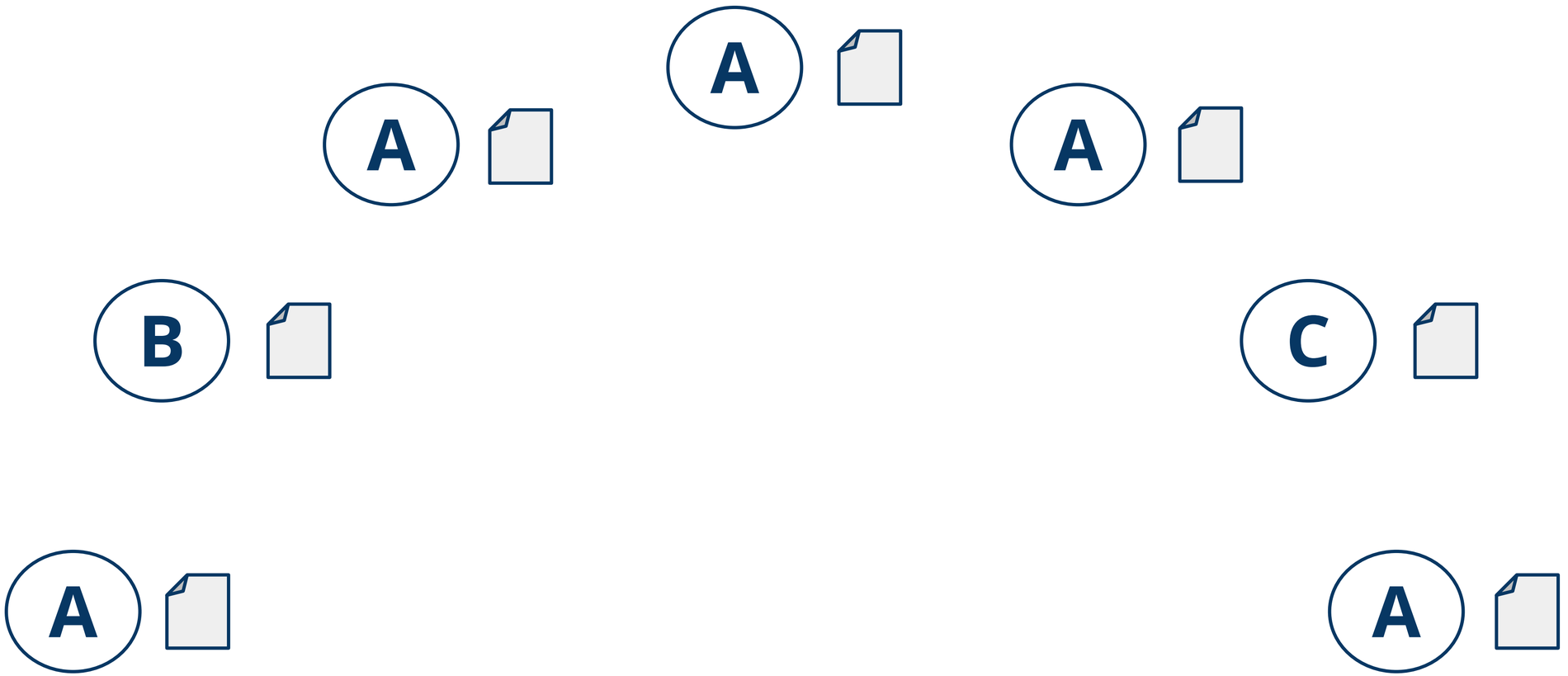
Alice is prevented from double spending



Slide by Viget

v4

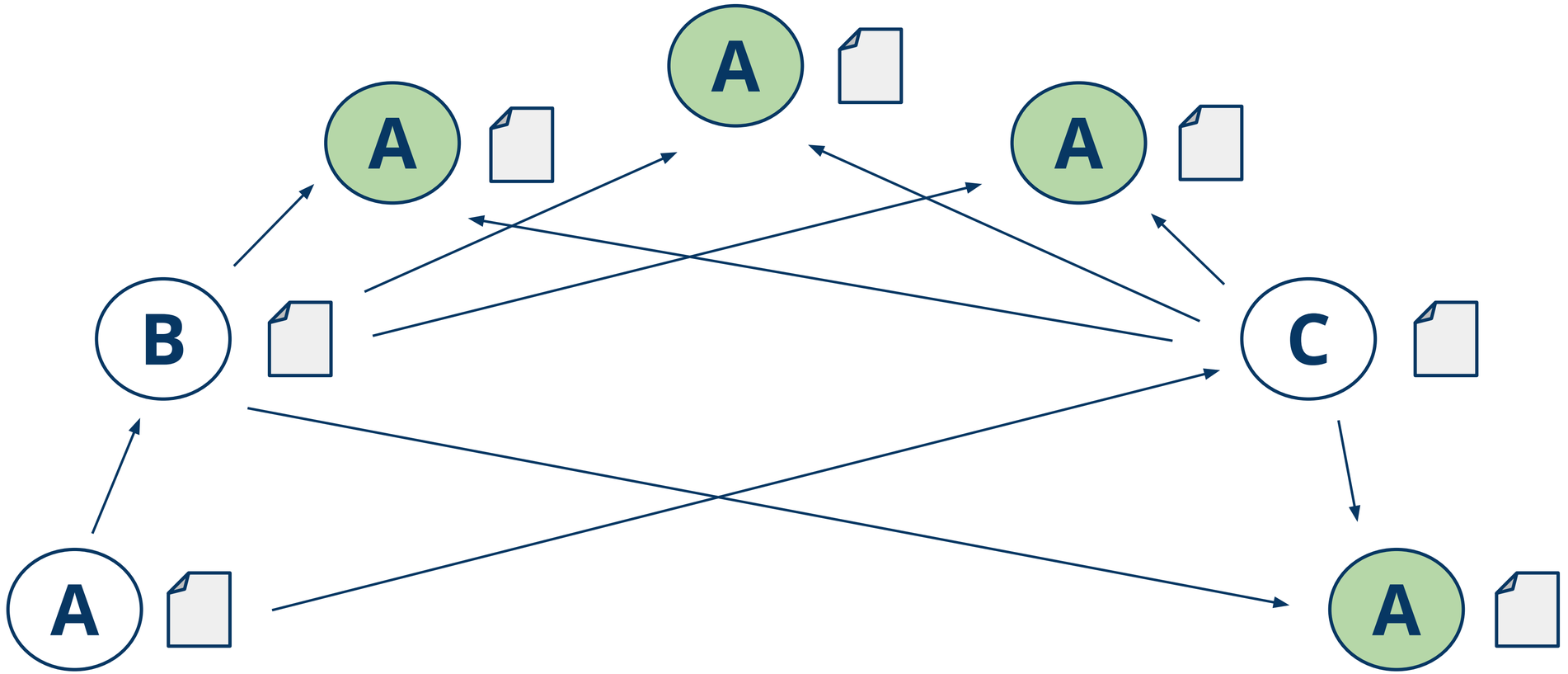
Alice sets up multiple identities



v4

Alice double spends with her multiple identities

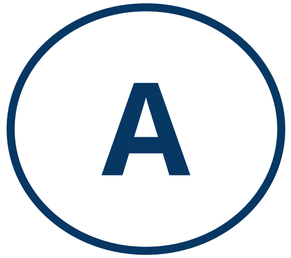
Sybil Attack: Done by creating many fake identities

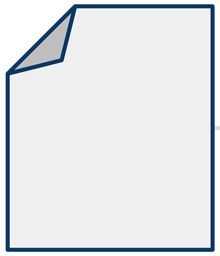


Slide by Viget

v5

Proof-of-work





v5

Pending transactions

1. I, Tom, am giving Sue one bitcoin, with serial number 3920.
2. I, Sydney, am giving Cynthia one bitcoin, with serial number 1325.
3. I, Alice, am giving Bob one bitcoin, with serial number 1234.

Slide by Viget

v5

Verifying transactions

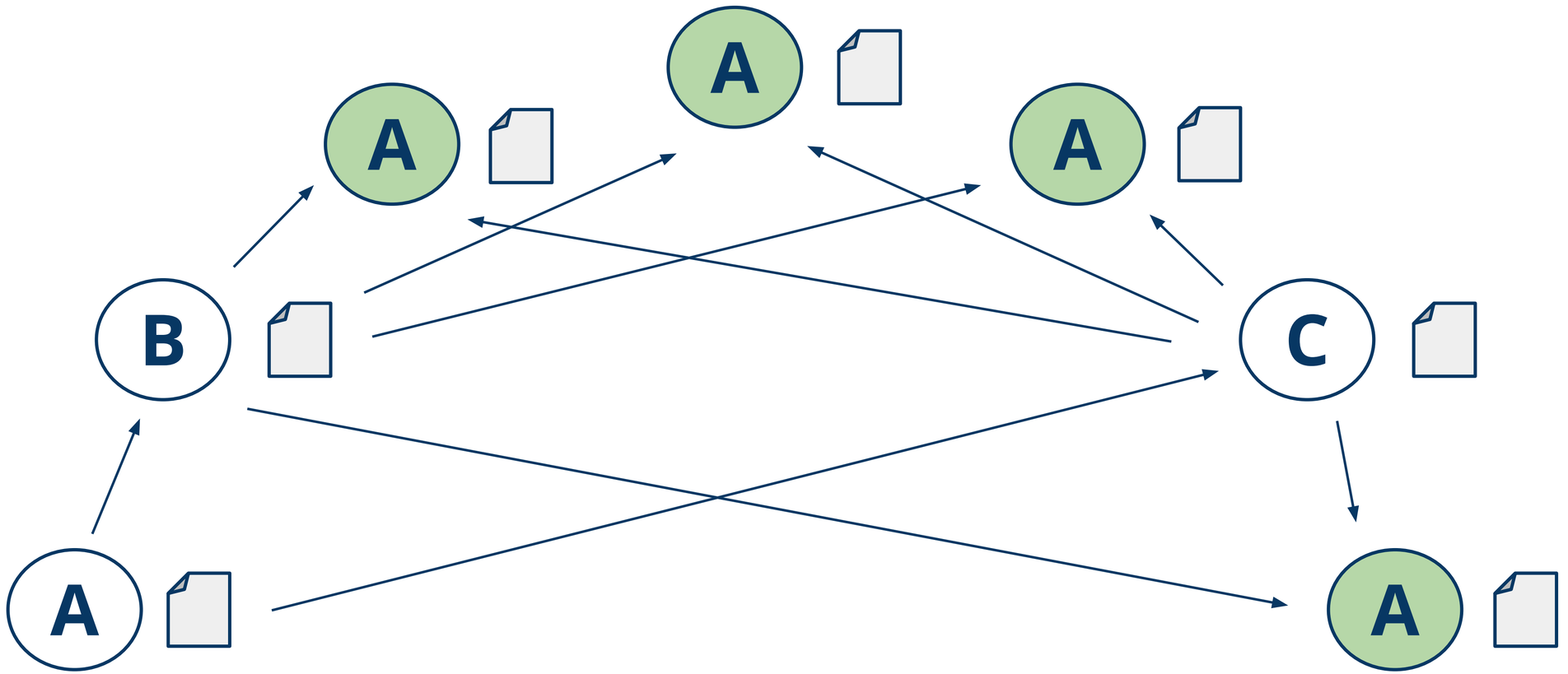
1 2 3

v5

Why the math?

v4

Alice double spends with her multiple identities



Slide by Viget

v5

Proof-of-work as a competition

Summary

Version	Major feature	Value added
1	Signed messages announced to the network	Basis of entire system
2	Serial numbers	Uniquely identifiable transactions
3	The block chain	Shared record of transactions
4	Everyone verifies transactions	Increased security
5	Proof-of-work	Prevents double spending

Bitcoin Mining

- Solution to Double Spending: Proof-of-work (PoW)
  - “Miners” continuously compete to solve a very computationally difficult problem
  - Proof of work is an example of a "Byzantine consensus algorithm"
  - Private blockchains tend to use alternative algorithms, but are not trustless

Mining functions as:

- A mining mechanism that ensures coins are distributed in a fair way
- An incentive for people to help secure the network
- Key component that enables you reach consensus in a decentralized currency

Proof-of-work is one of a plethora of consensus algorithms

Sketch of Bitcoin Mining - Finding blocks

- Finding the PoW => 'found' a block; can add block to blockchain
  - Miner who found block adds "**coinbase transaction**"
    - contains mining reward (currently 12.5 BTC)
  - Miner broadcasts block
  - Other nodes verify, then add to their own copy of the blockchain
- Timeline + stats
  - This happens roughly every 10 minutes
    - Difficulty of the problem adjusted every 2 weeks
  - Block reward halving every 4 years (recently halved on July 9th)
    - Bitcoin is in limited supply - 21 million bitcoins by 2140
      - Deflationary
  - 15.2 million bitcoins currently in circulation today
  - ~$9.6 billion market cap
  - Price is currently ~$600 per bitcoin

coinbase

Blockchain at Berkeley

Blockchain Types and Platforms

Types of Blockchain

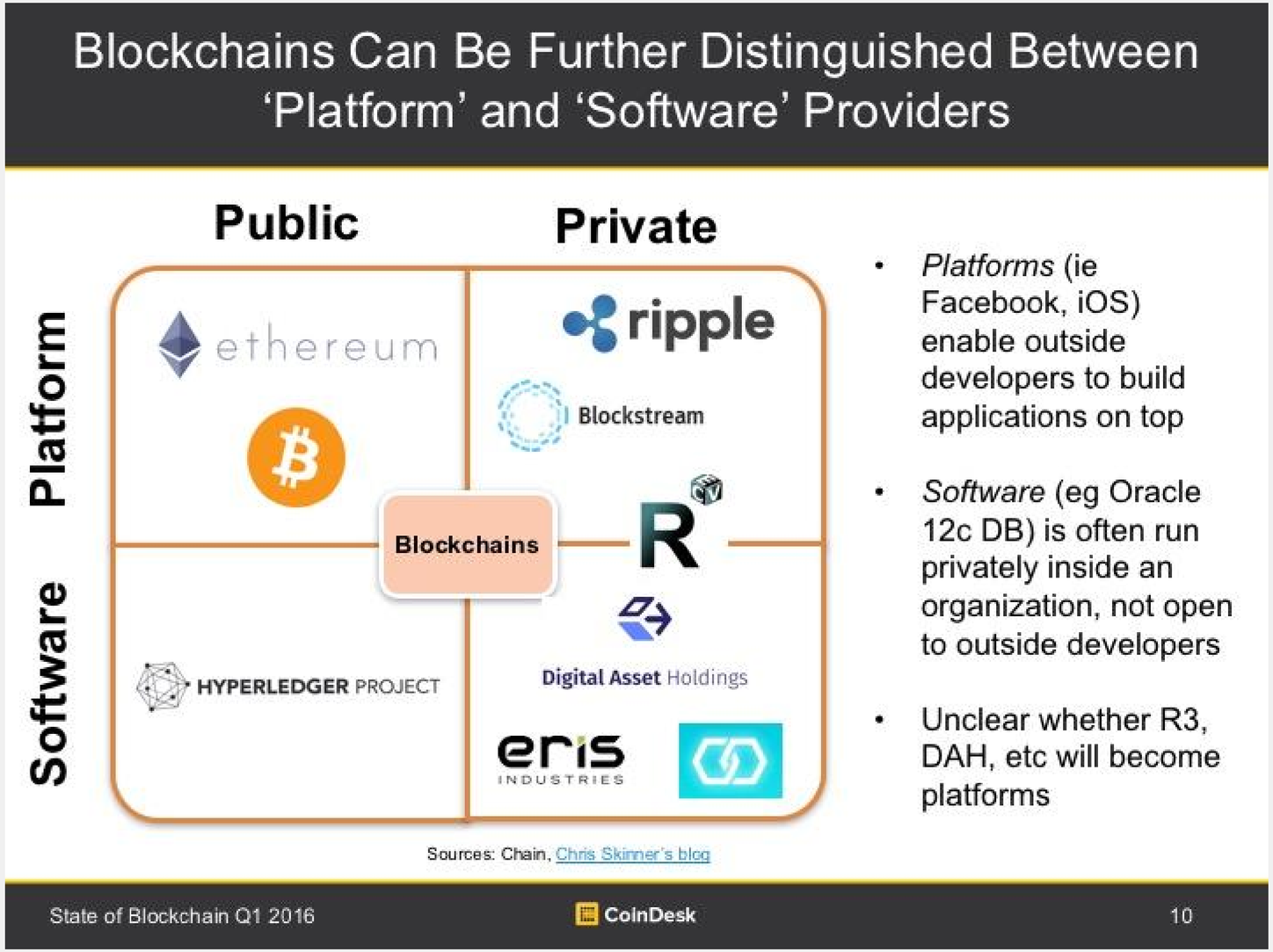
Public Blockchain - *A public blockchain is a blockchain that everybody in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and* ***anyone in the world can participate*** *in the consensus process.*

Consortium Blockchain - *A consortium blockchain is a blockchain where* ***the consensus process is controlled by a preselected set of nodes****; for example, one might imagine a consortium of 15 financial institutes, each of which operates a node and of which 10 must sign every block in order for the block to be valid.*

Fully Private Blockchain - *A fully private blockchain is a blockchain where* ***write permissions are kept centralized to one organization****. Read permissions may be public or restricted to an arbitrary extent.*

(From Vitalik Buterin: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/)

Platforms - Open vs. Private

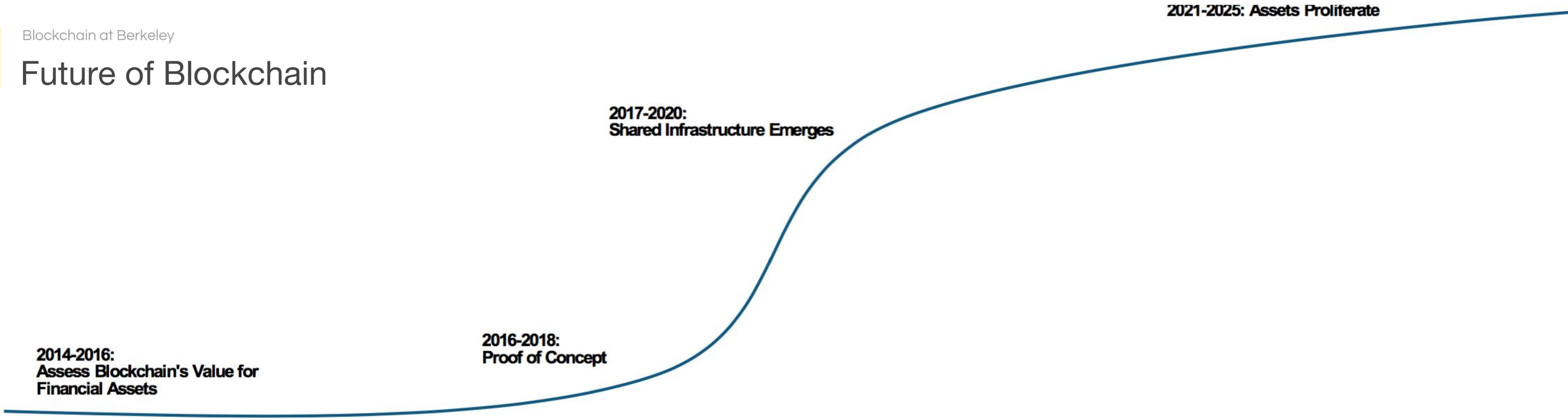


- *Platforms* (ie Facebook, iOS) enable outside developers to build applications on top
- *Software* (eg Oracle 12c DB) is often run privately inside an organization, not open to outside developers
- Unclear whether R3, DAH, etc will become platforms

Public (open) vs. Private Blockchains (Closed)

	Public	**Private**
Access	Open read/write access to database	Permissioned read/write access to database
Speed	Slower	Faster
Security	Proof-of-Work/ Proof-of-State	Pre-approved participants
Identity	Anonymous/Pseudonymous	Known identities
Asset	Native Assets	Any asset
Costs	Expensive	Cheaper

Future of Blockchain



2014-2016: Assess Blockchain's Value for Financial Assets
- Banks and other financial infrastructure intermediaries (FIIs), including Central Depositories, Exchanges, & Technology Vendors, size potential efficiencies from permissioned, shared, secure distributed ledgers
- Banks and financial infrastructure intermediaries form industry groups to discuss opportunities
- R3
- Linux Hyperledger Foundation

2016-2018: Proof of Concept
- Banks and FIIs tee up specific assets as a test case for Blockchain
- CDS
- Repo settlement
- Corporate syndicated loan settlement
- Trade finance
- International currency transfer
- Exchanges for post trade settlement

- POC Goal: Assess if Blockchain can scale and reduce costs
1) Does Tech work and scale
- Does the asset transact between buyer and seller smoothly
- Does it offer benefits beyond existing technologies on a performance, cost, speed, scale analysis
- Fails are de minimis
2) Can buyer, seller, and their 3rd parties (i.e., lawyers, auditors, regulators) validate the transaction with few human touch points, replacing teams of people
3) Does it offer benefits beyond existing technologies on a performance, cost, speed, scale analysis

- POC Tiering: Segment into most to least important assets to address
- Focus resources on most important assets, most inefficient processes
- Engage regulators, lawyers, auditors

2017-2020: Shared Infrastructure Emerges
- Proven assets adopted well beyond initial POC group
- Develop interface for external users
- Leverage APIs
- Reduce costs with fewer heads and increased mutualization of infrastructure costs

2021-2025: Assets Proliferate
- More assets move onto Blockchain as efficiencies prove out

Blockchain at Berkeley

Smart Contract Example

Smart Contracts & Property

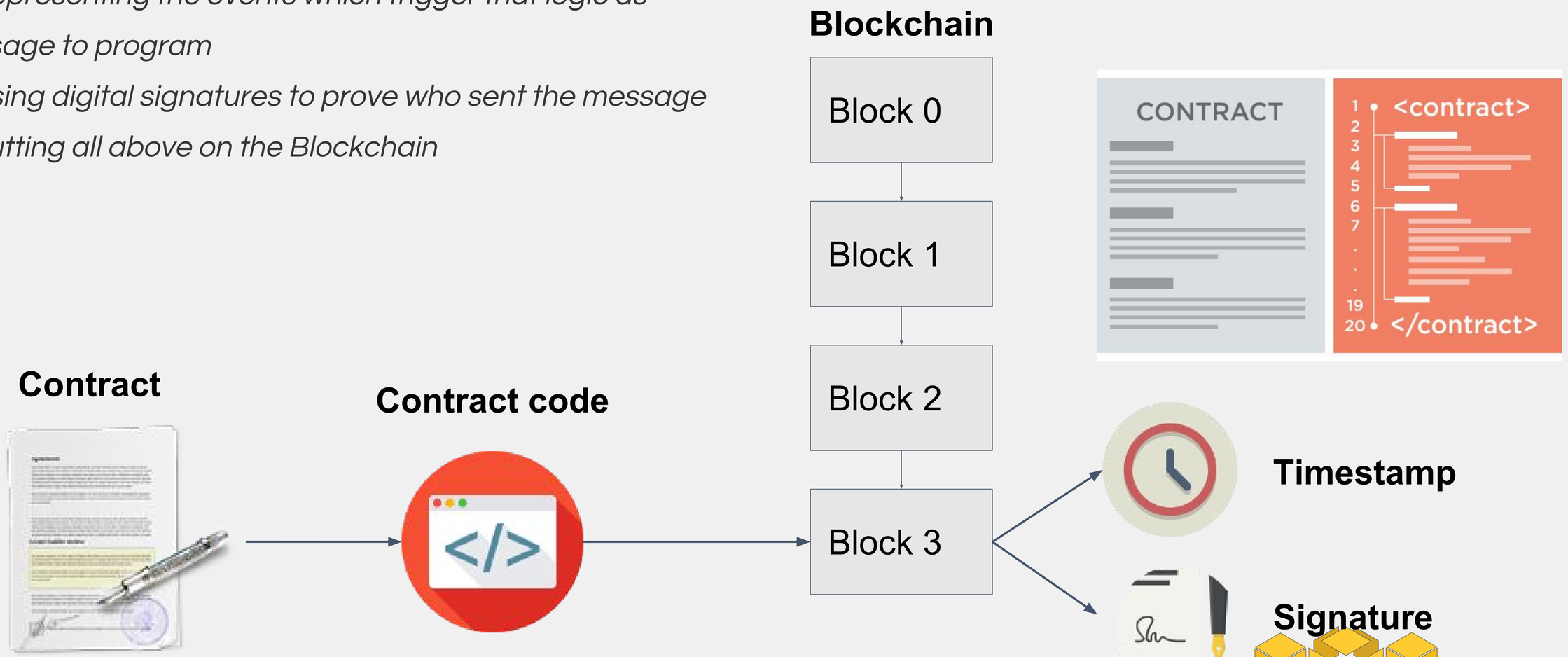
*"Smart contracts as **smart contract code**"*

(a) Expressing Business logic as a computer program

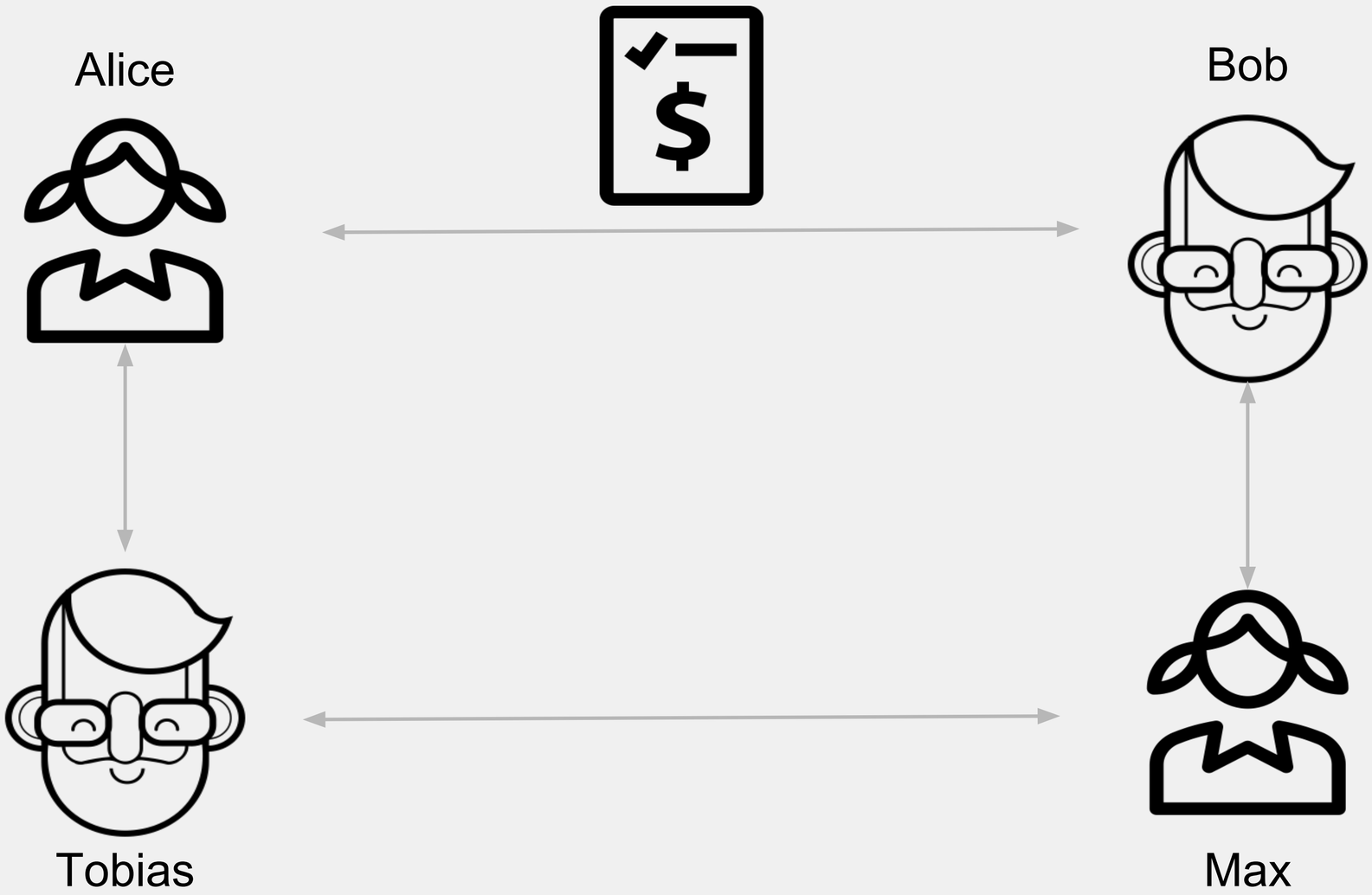
(b) Representing the events which trigger that logic as message to program

(c) Using digital signatures to prove who sent the message

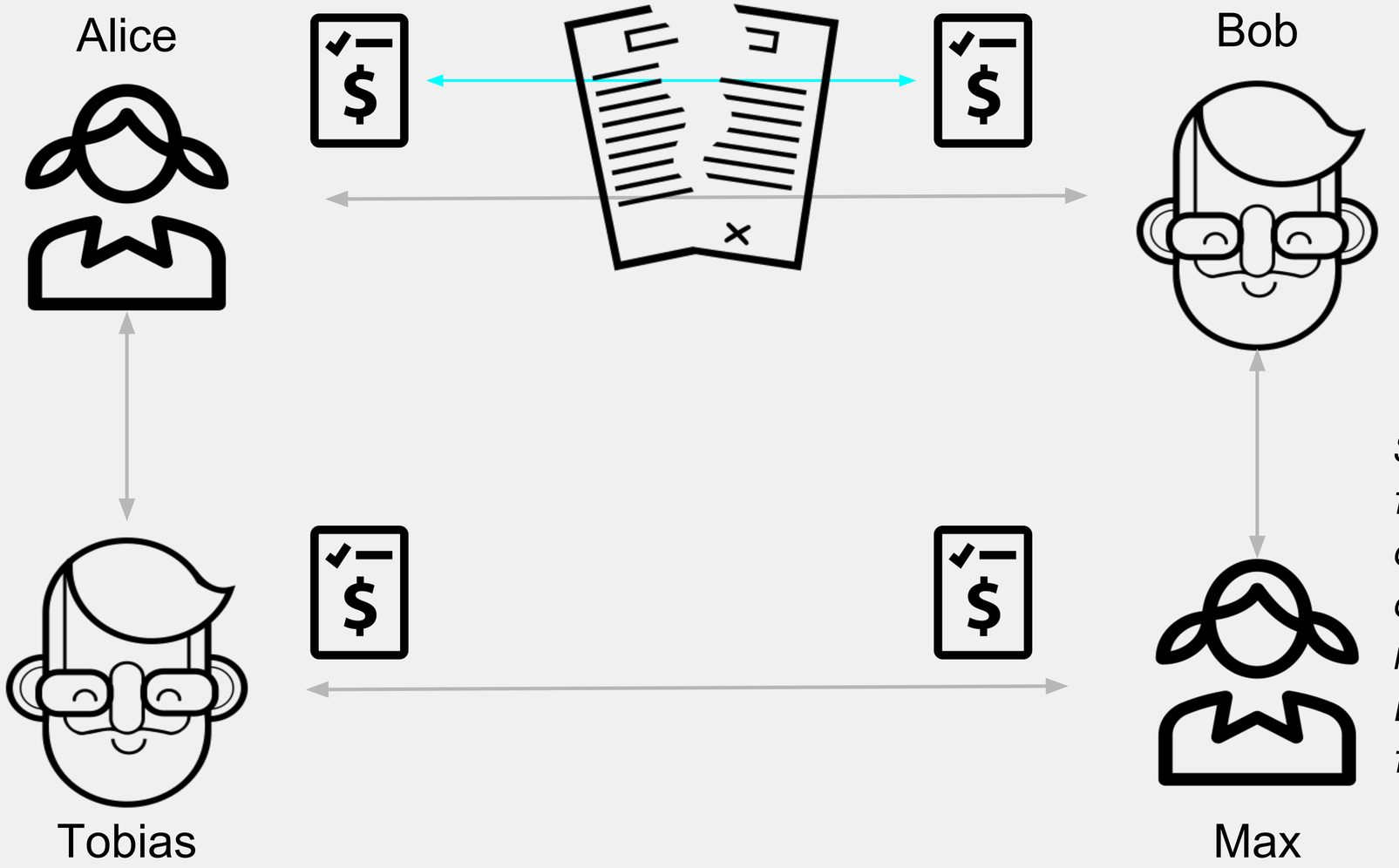
(d) putting all above on the Blockchain



Example

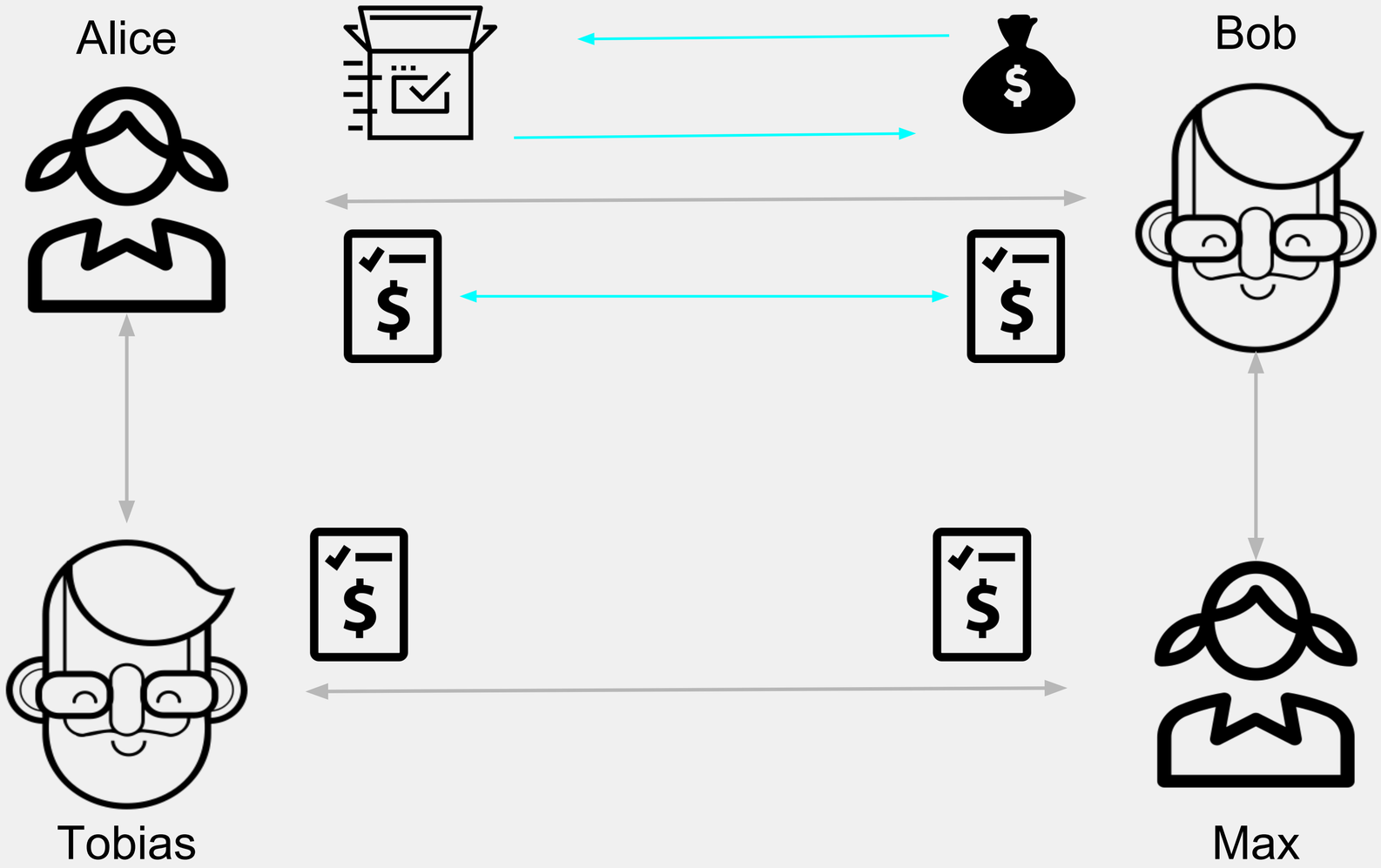


Example



So if Max wants to make a change the whole chain gets a message. Everybody needs to approve.

Example



Pro's / Con's

Pros:

- It is secure, if somebody wants to change a contract everybody gets a warning
- Self executing,
- Distributed/Decentralized
- M2M (Machine to Machine)

Cons:

- Scalability of the chain
- Difficult for legal contracts, which need human interpretation
- Computation power
- Difficult to update a smart contract

Dapps, DAOs, DACs, DASs

Decentralized applications (Dapps)

- Is an application that runs on a network in a distributed fashion with participant information securely protected and operation execution decentralized across network nodes.

Decentralized Autonomous Organizations & Corporations (DAOs & DACs)

- In a DAO/DAC, there are smart contracts as agents running on Blockchains that execute ranges of prespecified or preapproved tasks based on events and changing condition.
- Storj, Smart Contracts operated, decentralized file storage

Decentralized Autonomous Societies (DASs)

- For in the future this can be a DAS where a fleet of smart contracts, or entire ecosystems of Dapps, DAOs, DACs operating autonomously

DAO - DASH

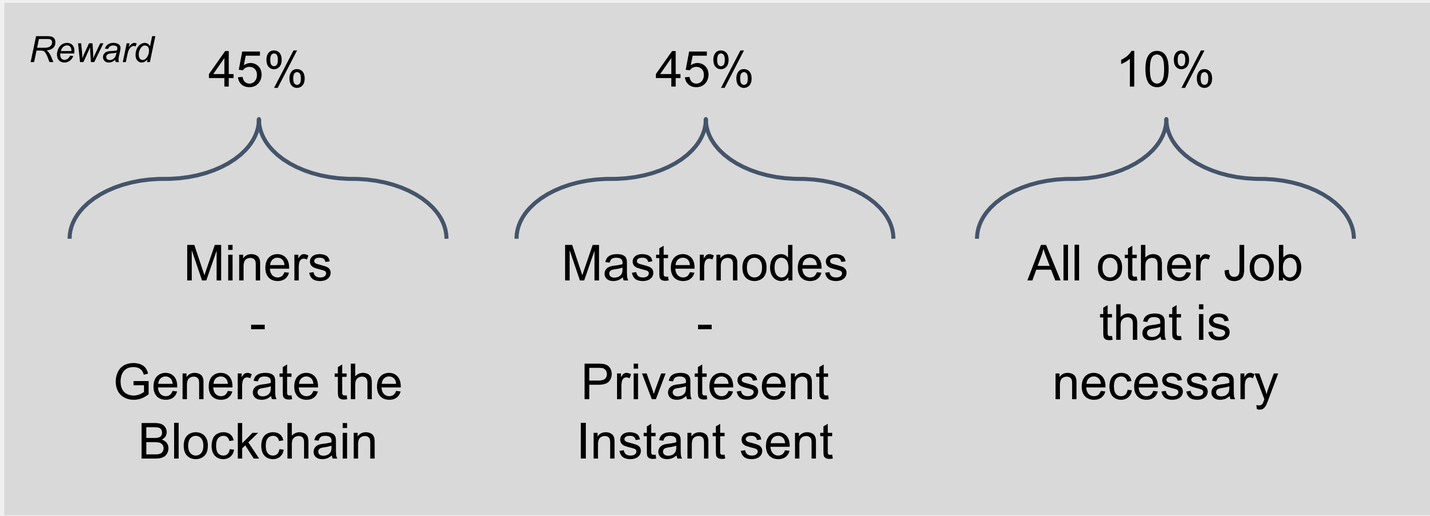
A decentralized autonomous organization (DAO), sometimes labeled a decentralized autonomous corporation (DAC), is an organization that is run through rules encoded as computer programs called smart contracts. A DAO's financial transaction record and program rules are maintained on a blockchain.

- **Dash** formerly known as **Darkcoin** and **XCoin**, rebranded in 2015
- People who communicate via a network protocol

Two principles:

1. Consensus
2. Execution

What makes it so special? →



Blockchain at Berkeley

DAO - Energy Example

Hyperledger

HYPERLEDGER PROJECT

1. Finance
   i. community of more than 50+ of the biggest banks in the world
   ii. Altoros Hyperledger Demo: Distributed Clearing Platform For Derivatives
   iii. Altoros Hyperledger Demo: Bond Issuance and Trading
   iv. HACERA: Accounts You Can Count On
   v. IntellectEU Demo: Smart Correspondent Banking

2. Healthcare (in development)
3. Supply Chain (coming)

R3 - Project (Private)

1. Software/Platform
2. Consortium of 50 of the largest banks in the world
3. Corda Project - the distributed ledger for all 50 banks

Let’s watch a video!

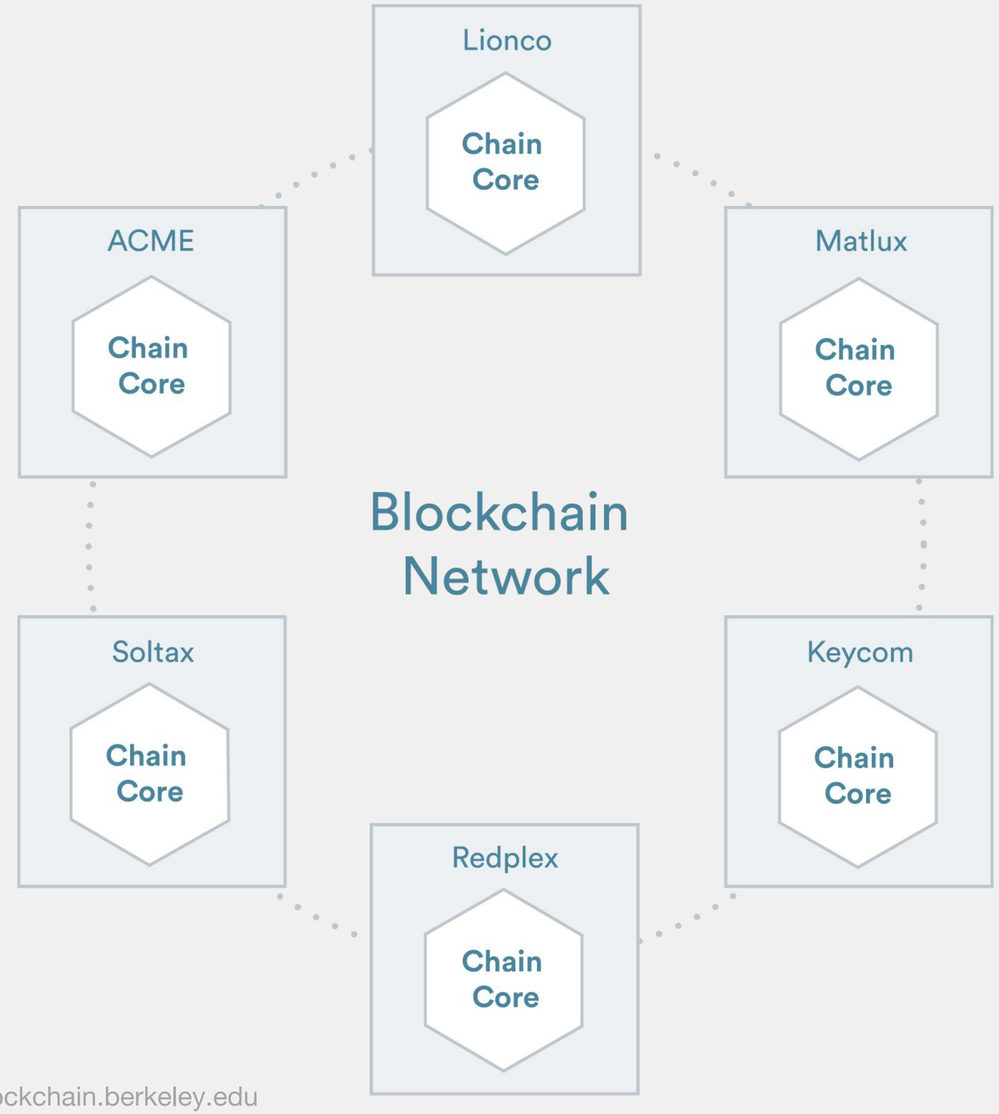
R3 - Project (Private)

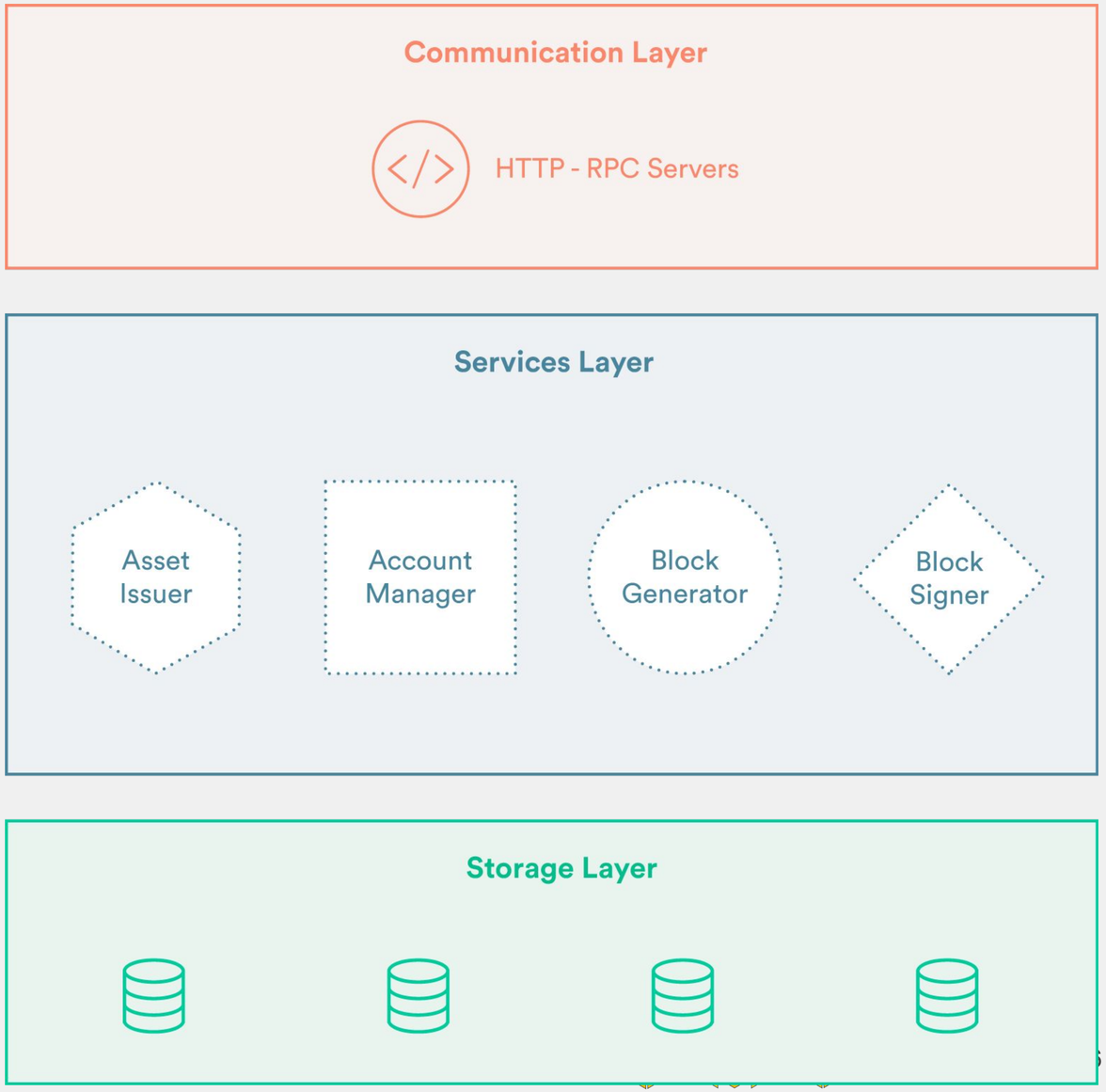
Chain.com (Private)

Delivers three different options for companies:

1. **Open Standard** - *Financial Asset registration*
2. **Chain Core** - *An enterprise-grade distributed system that powers secure, scalable, and highly available blockchain networks.*
   Enterprise software in the blockchain.
3. **Chain Sandbox** - *private blockchain network designed for rapid prototyping. It allows development teams to begin building blockchain applications in a hosted environment without deploying Chain Core on-premise.*

Chain.com (Private)

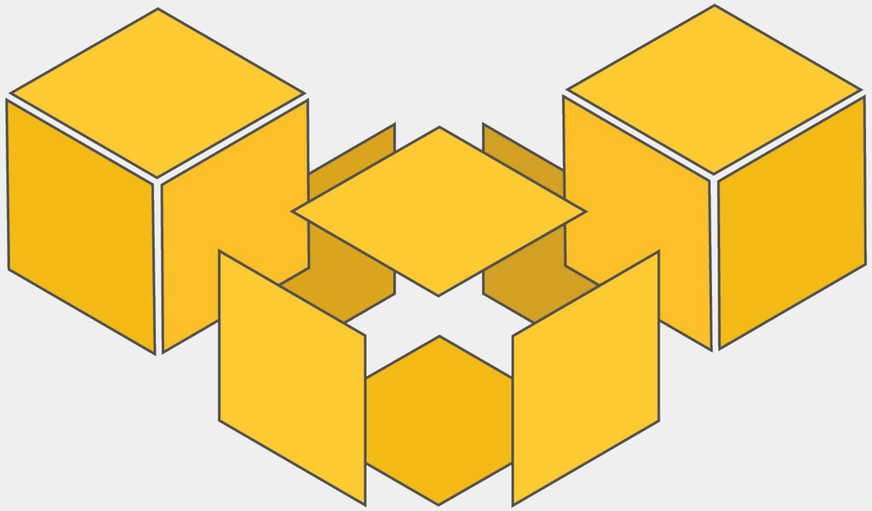




Ripple

Next week

- Please fill in this check-in form: http://www.tinyurl.com/project-bb **DUE BY MIDNIGHT**
- Expectations
- Team forming - also in the form
  - Please fill in the form and give your preference
  - Start meeting with your team this week
  - Team leaders
  - Define work structure
  - Team leaders inform Tobias & Ronen about the (scrum) meeting
    - How did it go
    - Questions
    - Can we help you?
- Dev:
  - Make a Dev environment for Ethereum and start using solidity
- Con:
  - 5 min presentation
  - Central database vs. Blockchain
  - 3 slides



Blockchain
AT BERKELEY

Thanks!

We're the world's first university-based blockchain consulting firm.

Like us on Facebook:
@Berkeleyblockchain
https://www.facebook.com/berkeleyblockchain/