Lecture 11

The future of Bitcoin?

Decentralize everything!

Lecture 11.1:

The block chain as a vehicle for decentralization

Motivating example: smart property

Step 1: car controlled by a cryptographic key

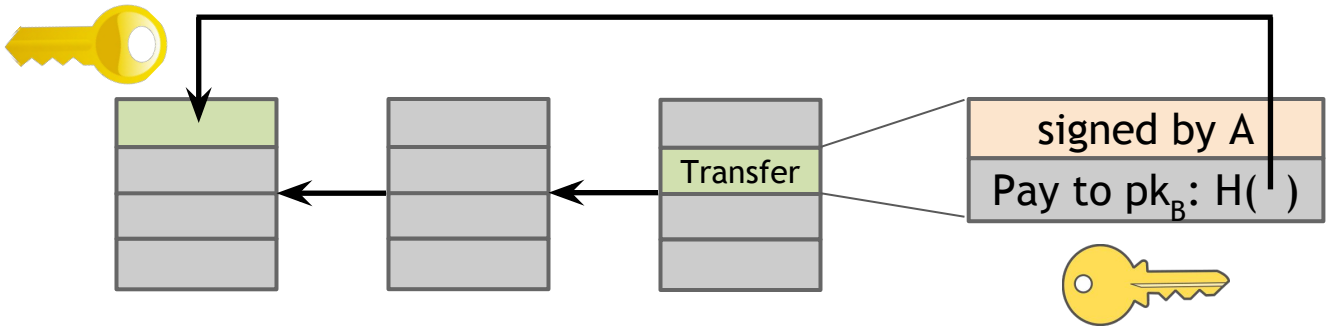
Car has public key hard-coded

Activated upon receiving message signed by corresponding private key

Motivating example: smart property

Step 2: public key is dynamically updated based on Bitcoin block chain

Alice owns the car because she controls private key of green Tx output

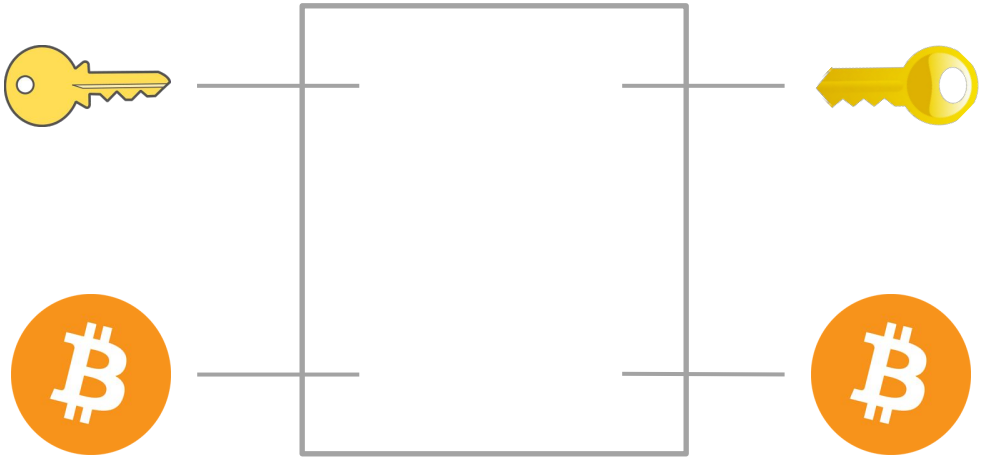


Now Bob's key activates car

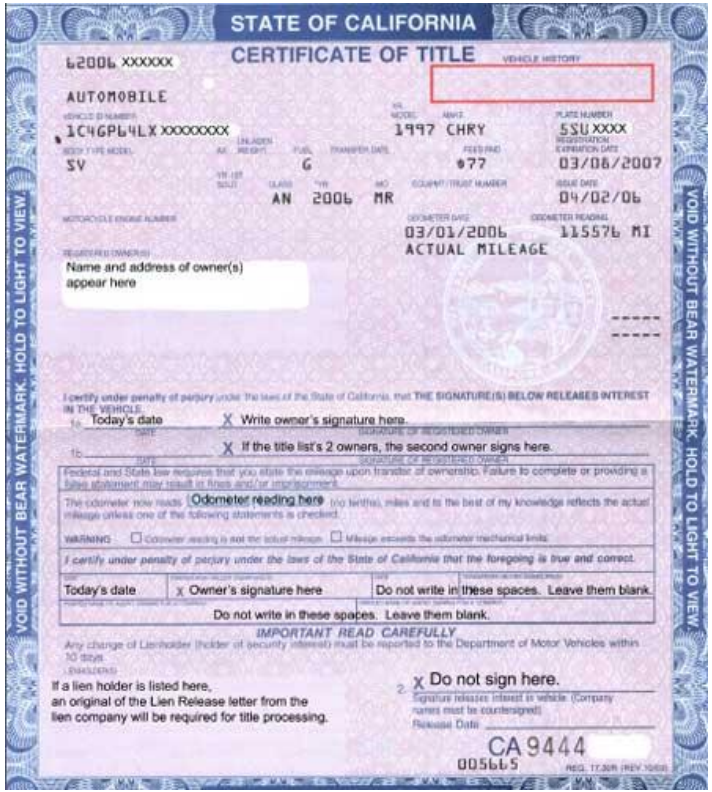
Motivating example: smart property

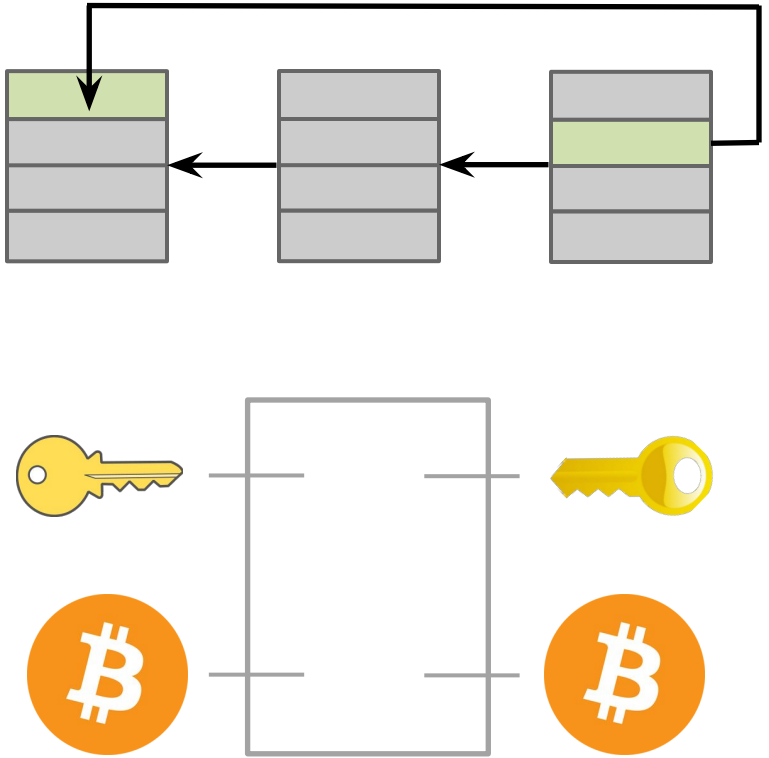
Step 3: Create a single transaction that combines Bob's payment to Alice and Alice's ownership transfer to Bob

Alice and Bob sign separately, then broadcast



Decentralized property ownership





Representation and atomicity

Representation:

How to encode complex transactions into the block chain?

Atomicity:

How to couple the actions of the various parties?

Questions

- What else can we decentralize this way?
- Can these be done on Bitcoin or do they require a separate block chain?
- Are there alternatives to atomicity?
- Is it a good idea to do commerce like this?

Lecture 11.2:

Routes to block chain integration

Route 1: Directly on Bitcoin

Advantage:

easy to deploy

Disadvantages:

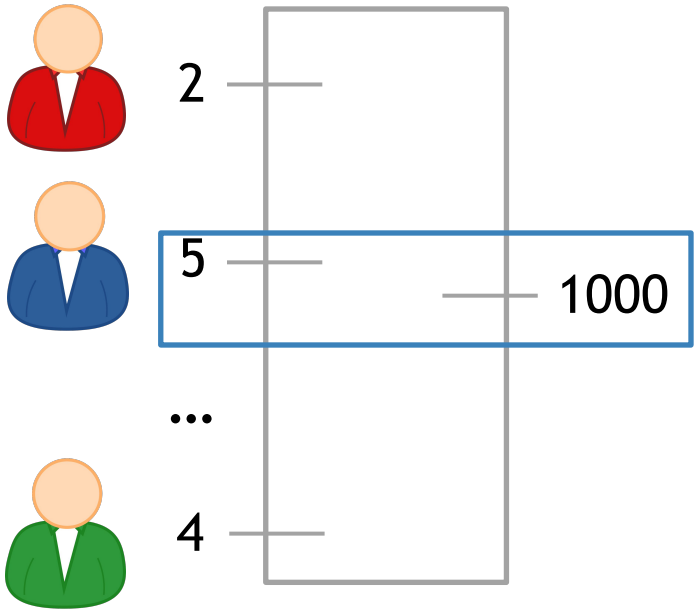
limited representation and atomicity

Example: crowd funding

Single Tx with arbitrary number of inputs and 1 output

Spendable only if
Σ(inputs) ≥ output

Each funder signs only her own input and the output



Example: pay for proof

- Alice knows x such that $H(x) = c$
- Bob would like to pay Alice in exchange for x
- Bob's Payment should be atomically coupled with Alice's publication of x on block chain

Possible but unwieldy

Route 2: Embedding

Recall: Colored coins

Similar to representation of car ownership, but relies on entire history

Recall: Mastercoin

Route 2: Embedding

Advantages:

- Complex representations possible
- Security of Bitcoin block chain

Disadvantages:

- Limited scripting and atomicity
- Results in unwanted Tx’s in block chain

Route 3: Side chains

Recall:

merge-mined, 1-1 pegged Bitcoin testbed

Advantage:

Avoids polluting the block chain

Disadvantage:

Requires Bitcoin modifications

Route 4: Altcoins

Example: Ethereum

- General framework for ledger-based consensus
- Turing-complete scripts
- Pay for miner computation using “gas”

Which approach to use?

Conceptually, any of the four can implement smart property

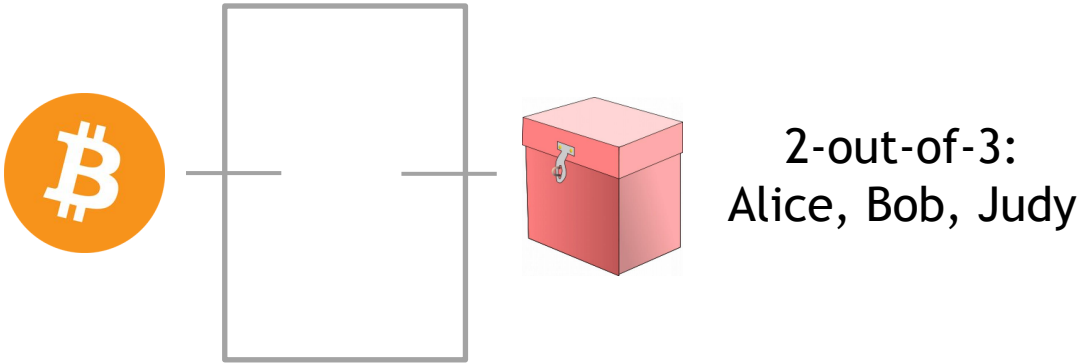
Differences in power and flexibility

Practical differences, e.g: SPV feasibility

Back to the car sale example

What about a dispute?

Recall: 2-out-of-3 escrow



2-out-of-3:
Alice, Bob, Judy

Comparison to legal remedy

Advantage(?):

Alice and Bob have freedom to choose mediator Judy

→ competition between intermediaries

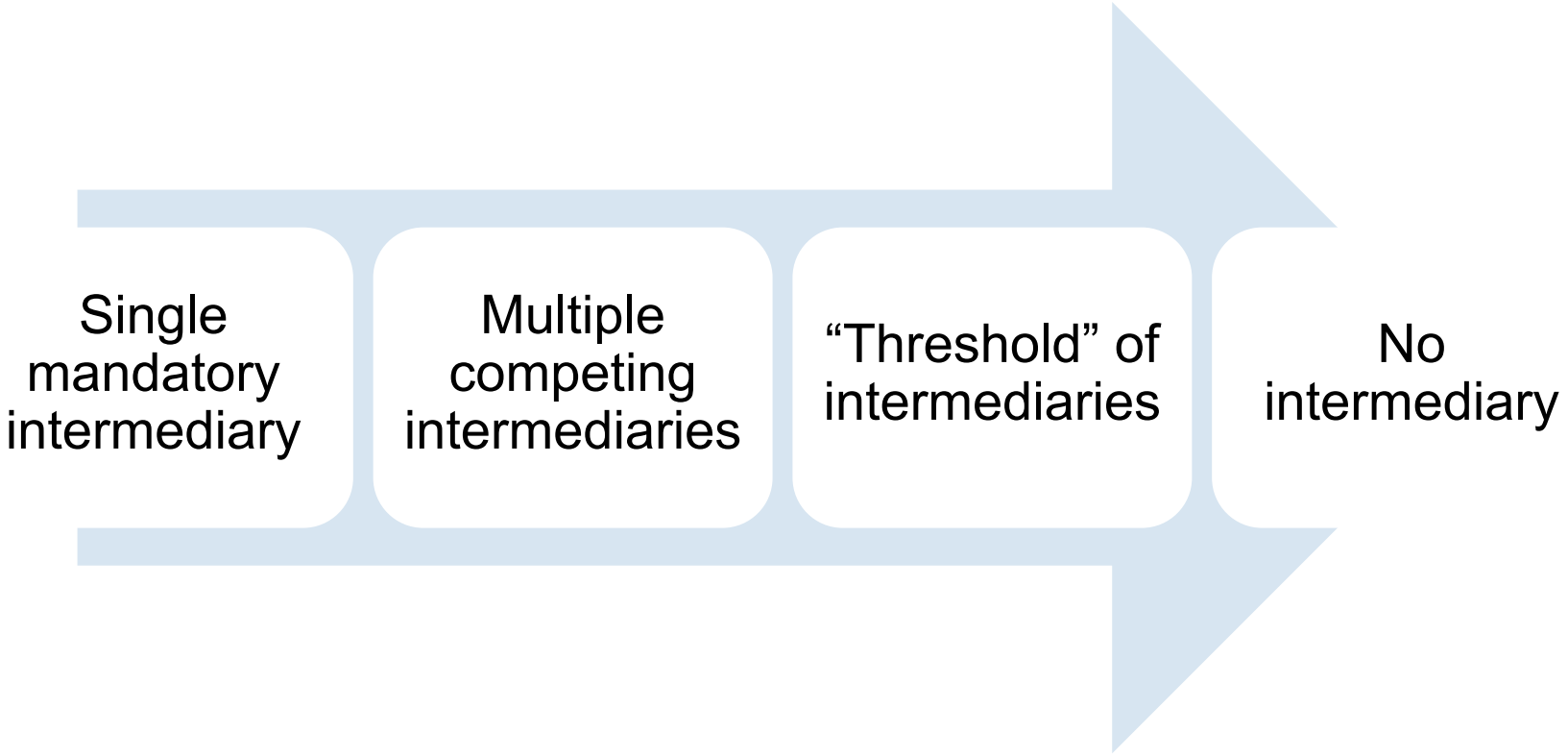
Disadvantage:

Funds tied up during mediation

Competing intermediaries

Recall: decentralized prediction market achieved by allowing anyone to start a market

Levels of (de)centralization



Improving security

- Reputation
- Escrow & dispute mediation
- Atomic exchange
- Trusted hardware

} Seen so far

Limitations due to lack of real-world enforcement:
no debt or punitive measures

Security: vocabulary

~~Trust minimization~~

Lack of trust is (unfortunate) starting point, not a goal!

A generic decentralization template

- What is being decentralized
- Type of block chain integration
- Level of decentralization
- How security is achieved

} Seen so far

Allows succinctly representing almost any proposal for block chain based decentralization

Example: smart property

Decentralizes	property ownership and trading
in the sense of	disintermediation
using	Bitcoin
via	atomicity

Example: decentralized prediction markets

Decentralizes	prediction markets
in the sense of	competition
using	an Altcoin
via	atomicity

Example: StorJ

“Agent” that lives in the cloud

Pay to store a file for fixed period (say 1 day)

Has other aspects such as reproduction (ignore for now)

Example: StorJ

Decentralizes	file storage and retrieval
in the sense of	competition
using	Bitcoin
via	reputation

Example: Zerocoin

Decentralizes	mixing
in the sense of	disintermediation
using	an Altcoin
via	atomicity

Lecture 11.3:

What can we decentralize?

1. Purely digital things

- Name mapping
- Storage
- Pay for proof
- Random number generation
- Lotteries

2. Things that can be represented digitally

- Real-world currencies
- Stocks
- Other assets

3. Property ownership and trade

Smart property and atomic exchange

4. Complex contracts

- Crowd funding
- Financial derivatives
  Requires price data feed unless
  underlying asset is traded on block chain

5. Markets and auctions

Centralized markets:

- Used bike store — buys your bike, sells it later
- EBay — matches participants, routes payments
- PayPal — processes payments, (some) dispute mediation
- Craigslist — matches participants

How to decentralize markets

Payment	Bitcoin
Transfer of goods	smart property, atomicity
Dispute handling	escrow
Matching participants	??

Decentralized matching

- Broadcast partially complete transaction to P2P network
- Counterparty finds it, completes, signs, broadcasts

Variant: use block chain instead of P2P network

Variant: auction

Counterparty can’t complete directly, must return to auction creator

Variant: double auction (order book)

- Both sides simultaneously broadcast partial transactions
- Miners match orders, keep bid-ask spread (Avoids miner front-running)

6. Data feeds

Recall:

data feeds allow arbiters to assert facts about the world into the block chain

Examples:

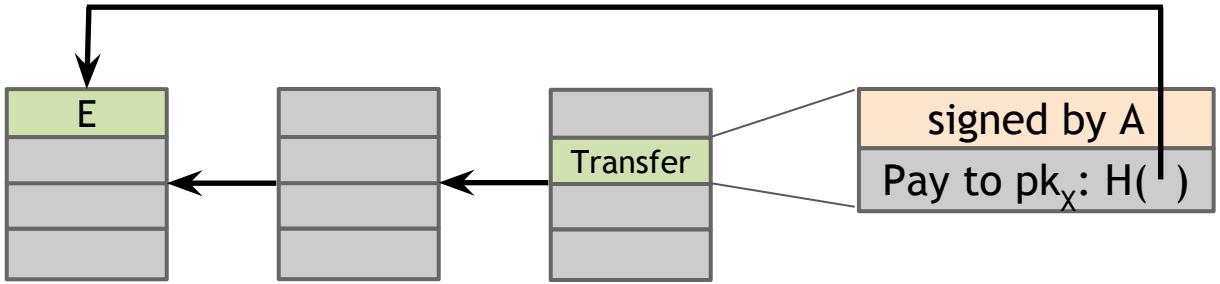
price movements, outcomes of events…

Big incentives to lie!

Decentralization by voting

Centralized version:
Tx corresponds to event E with outcomes X, Y, Z

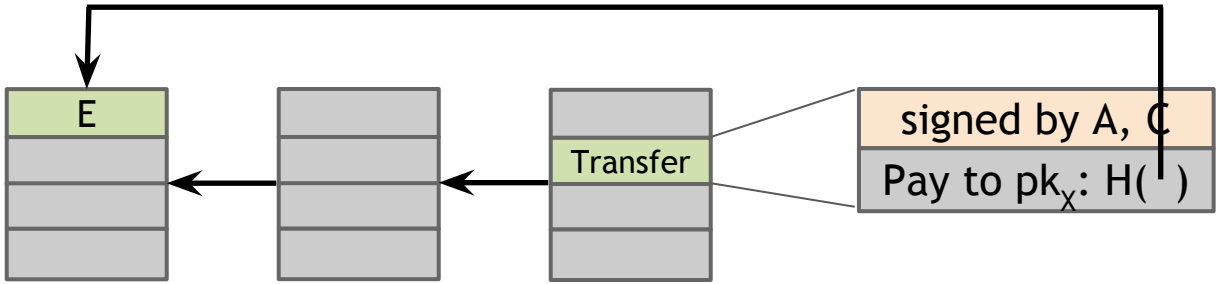
Transfer to pk_X if outcome X happens
Signed by arbiter A



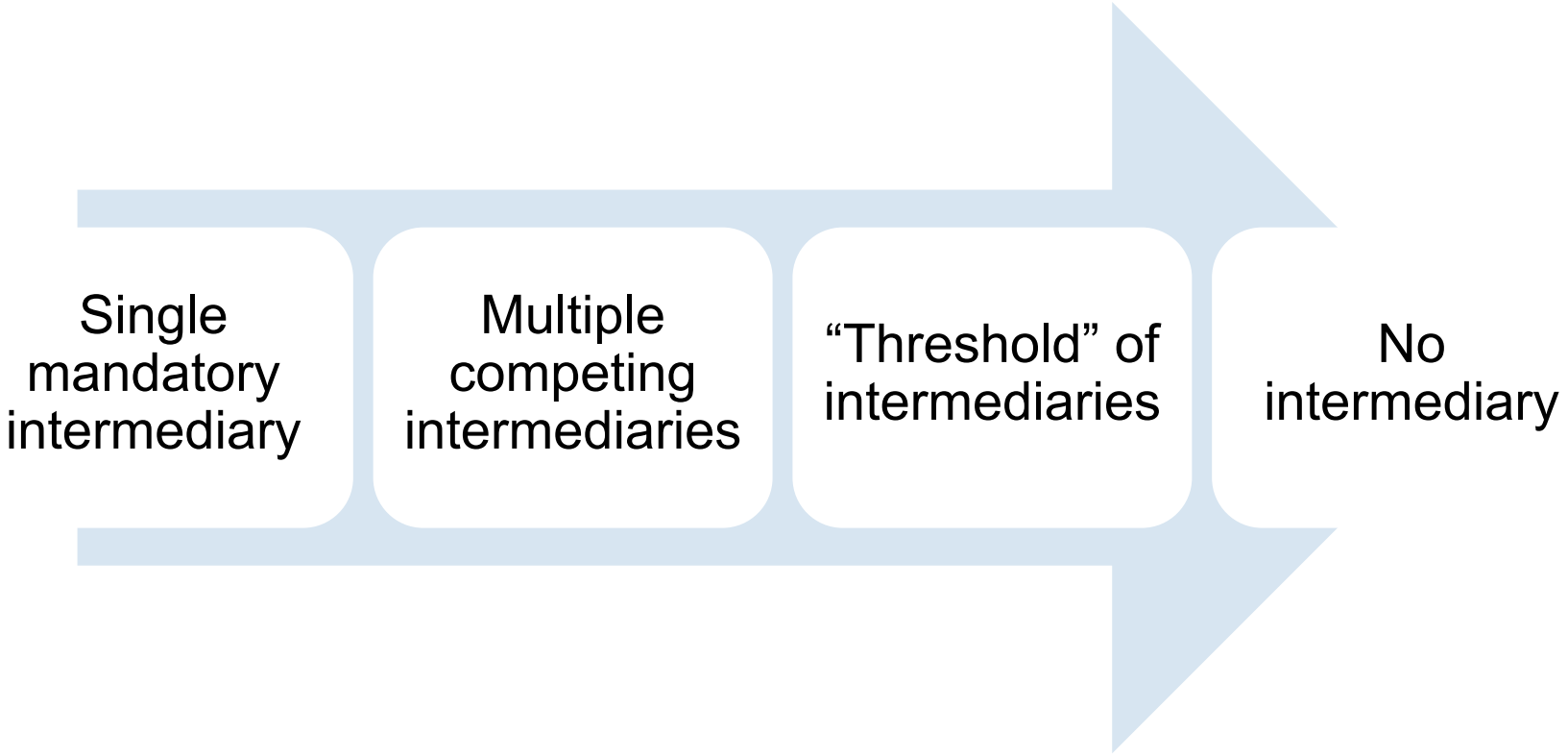
Decentralization by voting

Decentralized version:

E is a 2-out-of-3 multi-sig address controlled by A, B, C



Levels of (de)centralization



7. Autonomous agents

Key features

- Contracts
- Data feeds
- Voting as a way to change the rules
- Some variants: reproduction

Challenges

- Keeping private state
- Hostile takeover

Autonomous agents: terminology

~~Decentralized Autonomous Corporation~~

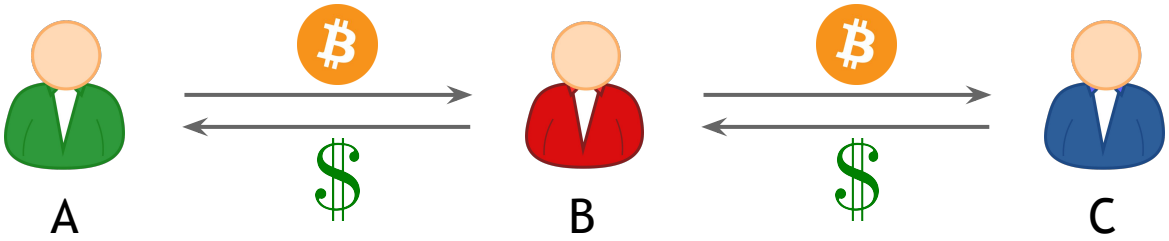
Preserves few of the salient features of corporations

8. Exchanges

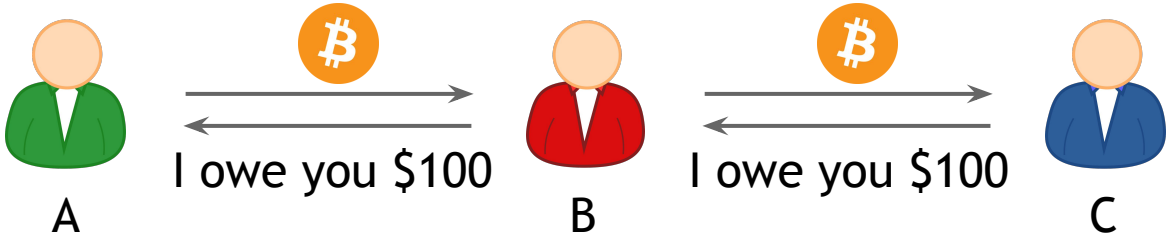
The problem:

- Alice would like USD for BTC
- Carol would like BTC for USD
- They don’t trust each other

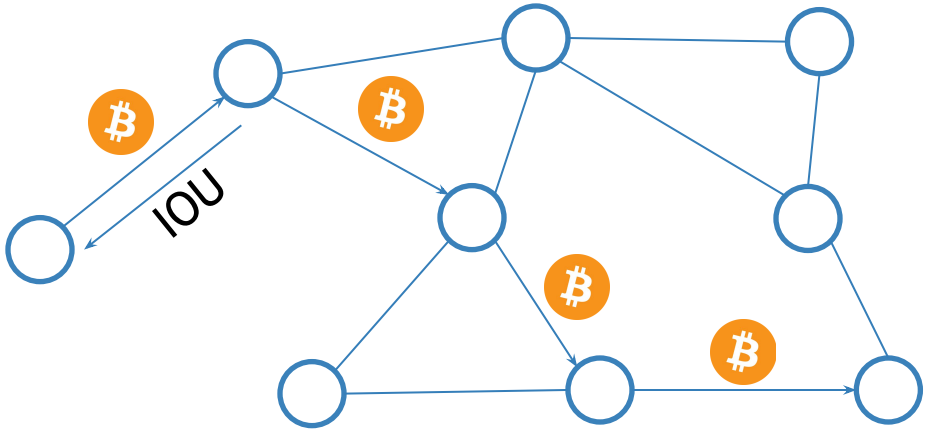
Luckily, they have a mutual friend Bob



Let’s make this more efficient



And scale it up



Pairs of friends pre-declare how much debt they're willing to extend

Triangular debt cancellation means actual settlement may be rare

Ripple

Decentralizes	currency exchange
in the sense of	disintermediation
using	an Altcoin
via	transitive trust

Lecture 11.4:

When is decentralization a good idea?

What we're really talking about:

Technological alternatives to human institutions — legal, social and financial

Recall: Cypherpunk roots

Back to the car example

What are the problems with car ownership and trade?

- Security (theft)
- Disputes about sale terms

What happens in a smart property model?

Security is complex

Preventive, detective and corrective controls

Real-world solution relies on law enforcement

Bitcoin security

Unsolved problem for the foreseeable future

Software security is partly a human problem

Excessive reliance can cause serious problems
Loss of key → car turns into brick?

Dispute mediation is complex

Fundamentally a human problem

Real-world solution:
court system, especially small-claims courts

Crowd funding security

Also fundamentally a human problem

Entrepreneur can take the money and run

Smart property model

- Didn’t solve existing (social) problems
- In fact, made them harder to solve
- Introduced new problems

Possible benefits of smart property

- Efficiency for small transactions
- Anonymity & privacy
- Freedom to choose mediator

Crypto and the state

The state is one way to scale society past small groups where everyone trusts each other

Crypto is another

Dismantling the state is not an option

How can the two work together?

The big opportunity

- Find compelling use-cases for decentralization
- Integrate into existing systems
- Co-opt legal and regulatory practices

Next steps

Assignments, eventually

Message boards, research groups