The Future of Bitcoin

Decentralize everything!

- The block chain as a vehicle for decentralization
- Routes to block chain integration
- What can we decentralize?
- When is decentralization a good idea?
The Future of Bitcoin

- The block chain as a vehicle for decentralization
- Routes to block chain integration
- What can we decentralize?
- When is decentralization a good idea?

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.

Transfer

signed by A
Pay to pk_B: H(·)

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?

The Future of Bitcoin

• The block chain as a vehicle for decentralization
• Routes to block chain integration
• What can we decentralize?
• When is decentralization a good idea?
### 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 \( \sum \text{(inputs)} \geq \text{output} \)
- Each funder signs only her own input and the output

\[ \text{2 participants, 1 output, 1000 units} \]

\[ \text{Each funder signs their own input and the output.} \]
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

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

- Single mandatory intermediary
- Multiple competing intermediaries
- “Threshold” of intermediaries
- No intermediary
### Improving Security

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

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

### A generic Decentralization Template

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

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

The Future of Bitcoin

- The block chain as a vehicle for decentralization
- Routes to block chain integration
- What can we decentralize?
- When is decentralization a good idea?
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

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 $A$

Decentralized version:
$E$ is a 2-out-of-3 multi-sig address controlled by $A$, $B$, $C$
Levels of (De)centralization

- Single mandatory intermediary
- Multiple competing intermediaries
- "Threshold" of intermediaries
- No intermediary

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
Example of DAO: The DAO

- Decentralized Autonomous Organization
- Exists as a set of contracts among people
- Contracts reside on the Ethereum blockchain
- Does not have a physical address, nor people in formal management rules
- Power directly in hands of owners, not directors and fund managers
- Completely transparent: everything done by code, which anyone can see and audit, on GitHub.

Example of DAO: The DAO (2)

- DAO intended as “a hub that disperses funds to projects”.
- Investors receive voting rights by means of a digital share token.
- To interact with real-world legal structures, The DAO established a Swiss-based company,DAO.Link
- Swiss law allows it to “take money from an unknown source as long as you know where it’s going.”
- June 2016: The DAO subjected to a $50M hack due to a weakness in the code.
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
The Future of Bitcoin

- The block chain as a vehicle for decentralization
- Routes to block chain integration
- What can we decentralize?
- When is decentralization a good idea?

What are we 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