CRYPTOCURRENCY REGULATION ALL OR NOTHING?

Aviv Zohar

School Computer Science and Engineering

The Hebrew University of Jerusalem

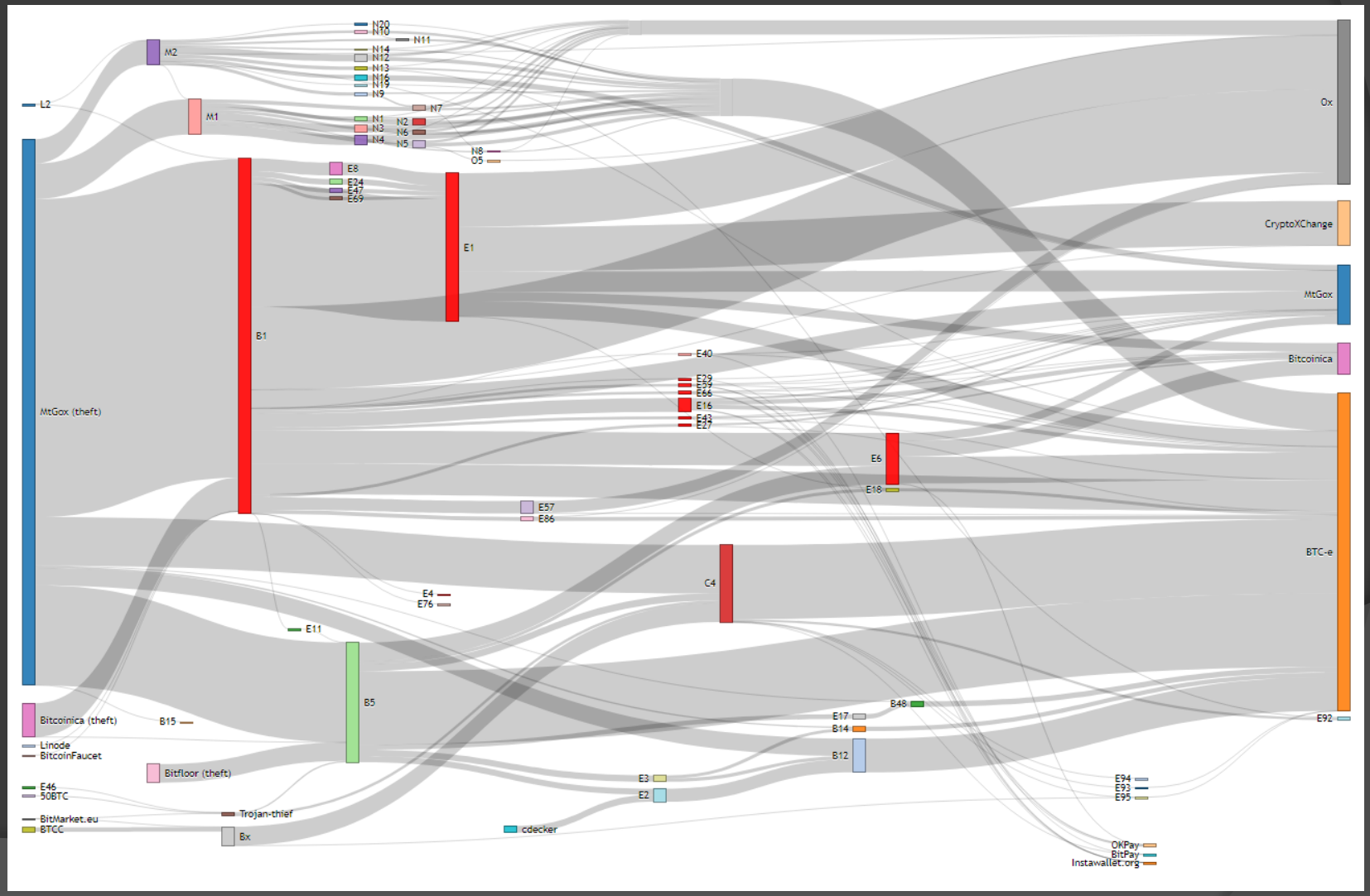
Chief scientist QED-it

- A word about ICOs:
  - From a technical standpoint, not exciting.
  - Not much more than crowdfunding.

- Main interesting aspects:
- How permissionless innovation challenges traditional systems & opens the market to wider audience.
- DAO like organizations that cannot be easily regulated.

Bitcoin's ledger is only Pseudonymous

- Funds can be tracked to some degree



Current regulation

- Bitcoin is volatile, hard to secure.
- A good amount of economic activity is of this form:
  - Person A acquires BTC at an exchange
  - Person A pays person B
  - Person B sells BTC at an exchange
- Regulation at the exchanges (KYC /AML regulations): effective
- High cost of regulation: barrier to adoption

Breakdown of current regulation

If volatility improves & wider adoption

- One can hold Bitcoins only, w/o need to convert.
- Regulation at exchanges ineffective.

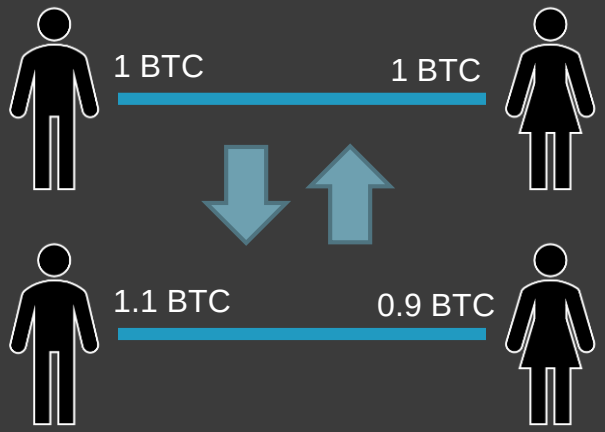
- Unclear where / how to regulate if at all. (miners too dispersed)

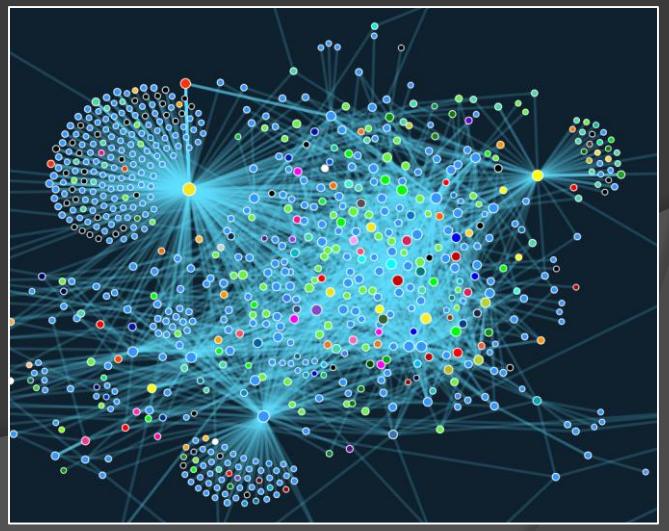
Zcash / Monero style currencies

- Use fancy cryptography
- The public ledger has **encrypted data only**.
- Encryption is **never** opened

Impossible to track funds by just looking at the ledger.

- Lightning network:
  - Payments channels that are P2P
  - Payments in different directions “cancel out”
  - Payments can be routed along several hops
  - Anonymity like TOR?





The future of cryptocurrencies is not like the present

Bitcoin has a scalability problem. 3 options:

- Cryptocurrencies fade to a meaningless phenomenon
- Bitcoin evolves to solve scale problem
- Bitcoin is replaced by a cryptocurrency that scales

Either way:

- The cryptocurrency that will become mainstream is not today's Bitcoin

A general observation

Four types of possible systems:

1. Totally open and trackable
   - Privacy problem.
2. Total privacy
   - Currently being built.
3. Private, but Gov. has “backdoor”
   - Doesn’t mesh well with global open source projects.
4. Zero Knowledge auditing: Prove compliance, but keep private
   - Hard to engineer & requires specs in advance from Gov. Probably not going to happen.

My prediction:

If cryptocurrencies gain sufficient adoption (BIG IF)

- Gov. will at some point need to choose
  - Minimal / No regulation OR:
  - Shut down public cryptocurrencies.

(A total shutdown will not succeed, but they can be suppressed from legitimate public use.)