Welcome to Blockchain Engineering

- how to **engineer** blockchain technology
- No written exam
- Project-based: 5 students

You will learn that blockchain is 95% engineering on top of sophisticated APIs and only 5% validation, crypto and creating trust.

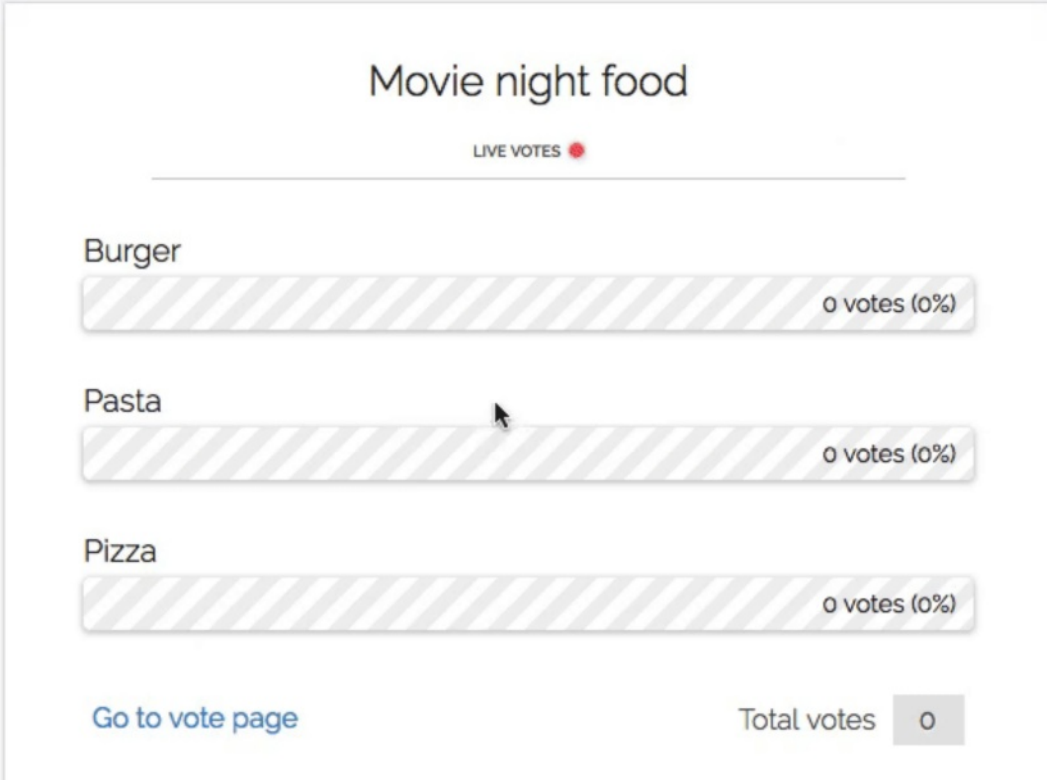
Project-based course

- Enroll by email on a project
  (Brightspace instructions)
- Deadline enrollment: 20Feb 11:59am (Noon)
- Brightspace → GITHUB list of projects
- Weekly meetings with advisors
- Work towards an operational prototype

  WARNING: no running code, no passing grade

Schedule for today 8:45 – 10:30-ish

- This introduction
- 3 On-chain democracy projects + Hyperledger health project
- 9:30 - 10:30 questions + group formation



Blockchain Engineering - class of 2024 #7691

Edit New issue

Open 5 tasks **synctext** opened this issue on Nov 14, 2023 · 1 comment

synctext commented on Nov 14, 2023 • edited Member

<ongoing editing, will be finalised before class kickoff 14Feb 2024> 2023 edition: #7100 {Tiktok class project}

Class schedule (DRAFT)

On-campus lectures location: DELFT CAMPUS - Drebbelweg-Instruction Room 4 (35.1.170)

Week	Description
3.1	course outline slides and presentation of available projects and formation of teams (each 5 students)
(14Feb)	8:45 - 9:45 : present all available projects
	9:45 - 10:30 : self-organise and form teams of 4-5 students. Professors available for questions
3.2	Networking foundations for chains (Bulat)
	IPv8 simulator
3.3	Introduction to blockchains, Bitcoin, ledger technology, and DAO (slides) by (Can: TU Delft & IOTA Foundation)
	short 10 minute introduction to Superapp (Rowdy)
3.4	Consensus models and algorithms (Jeremie)

Assignees
synctext

Labels
type: MSc course work

Projects
None yet

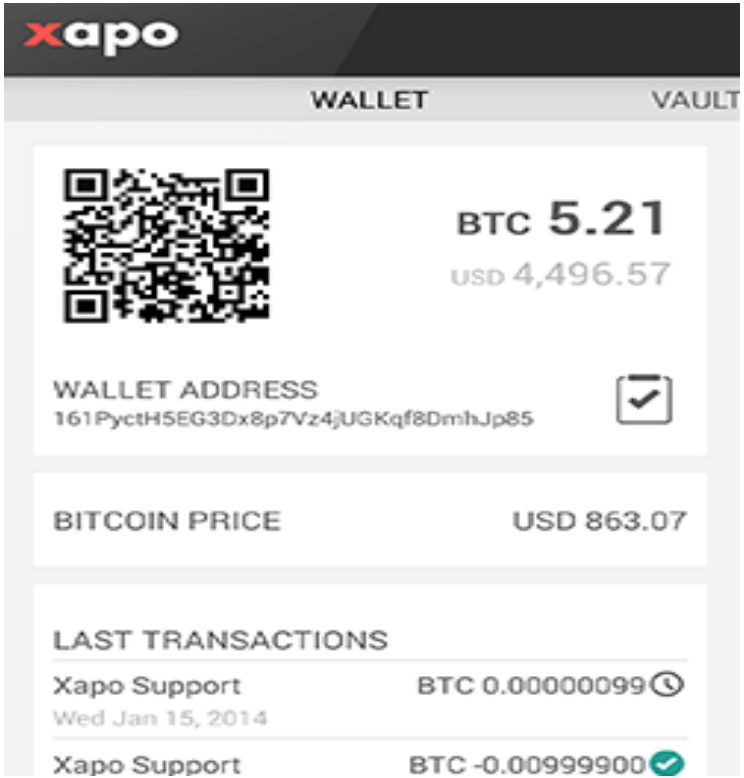
Milestone
No milestone

Development
Create a branch for this issue or link a pull request.

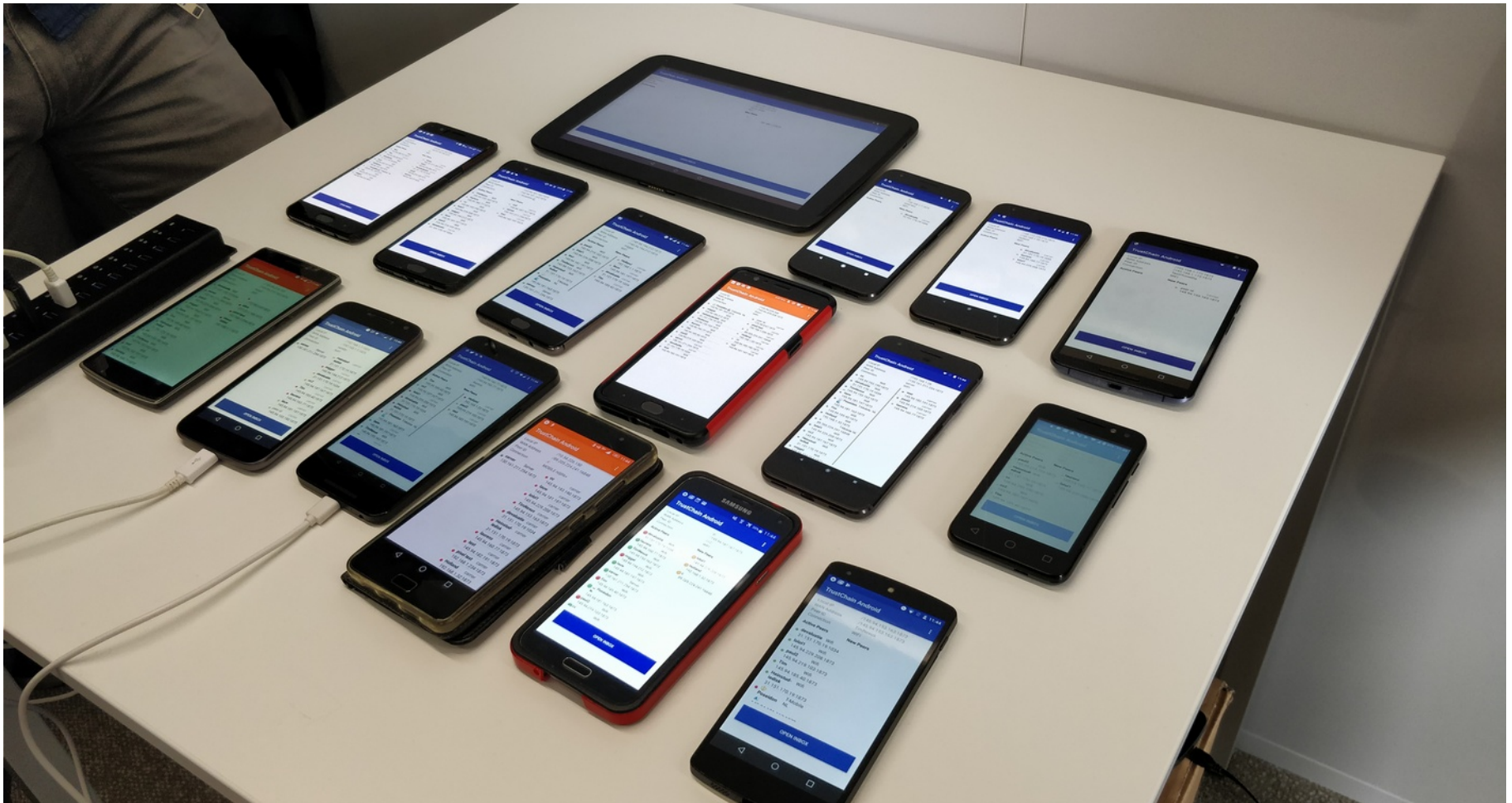
Notifications Customize
Unsubscribe
You're receiving notifications because you're watching this repository.

In this course: Bitcoin (1)

- Proposed in 2007 by Satoshi Nakamoto (pseudonym)
- Your public key is your wallet address
- With the private key, you can sign transactions



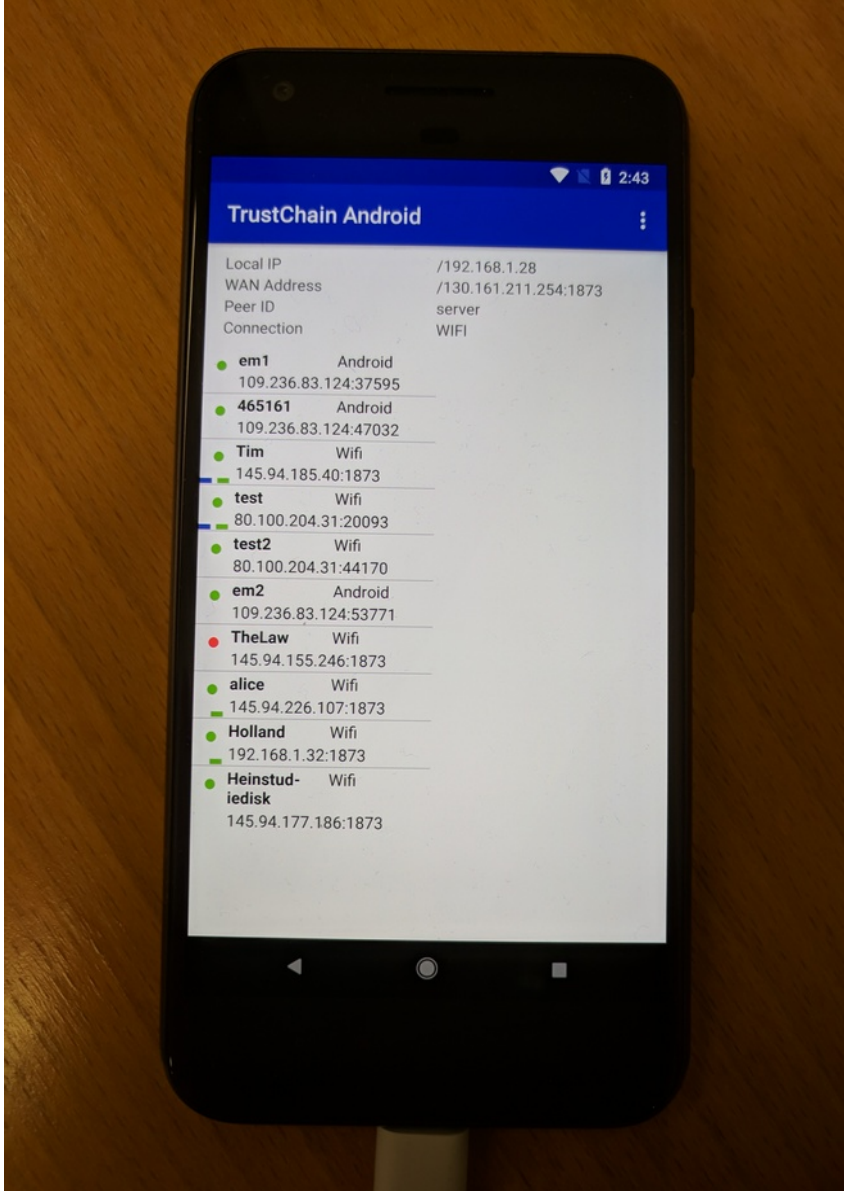
In this course (2.1) phone-to-phone



In this course (2.2) phone overlay of “billions”?

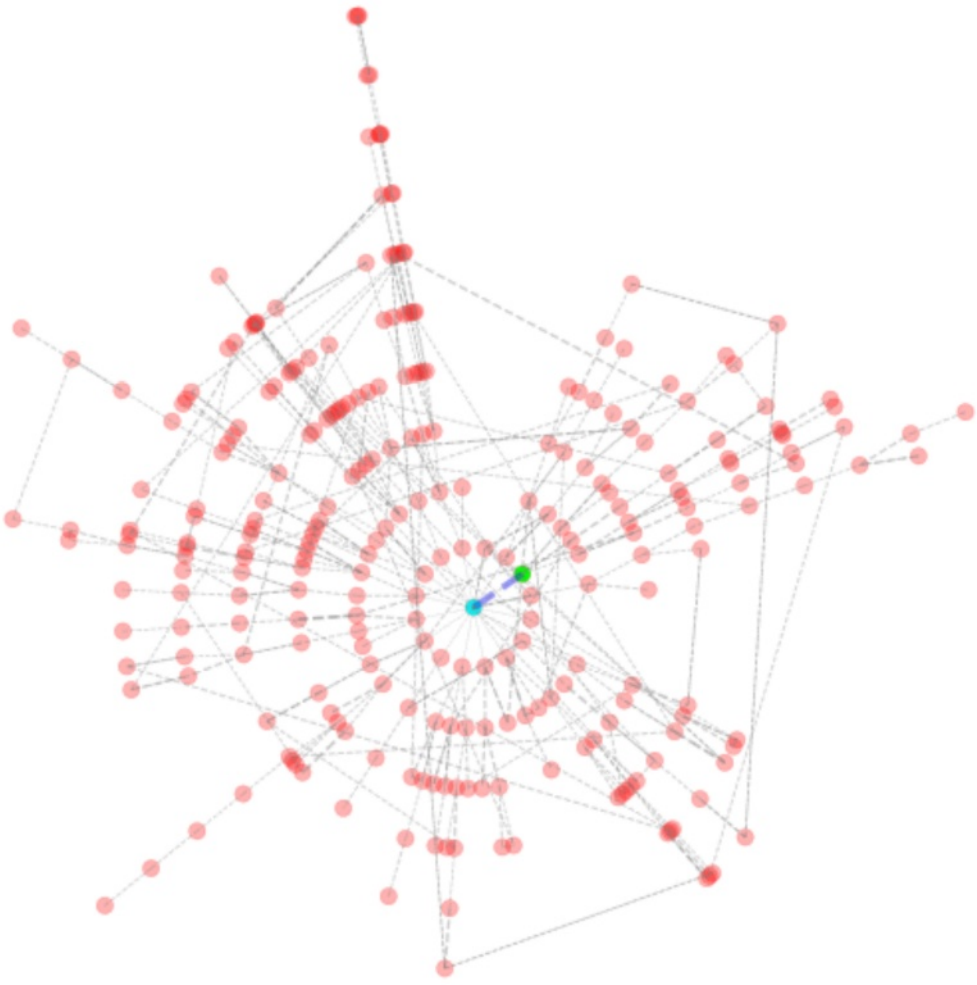
- No servers
- No laptops
- No Javascript
- “IPv8”

https://github.com/Tribler/

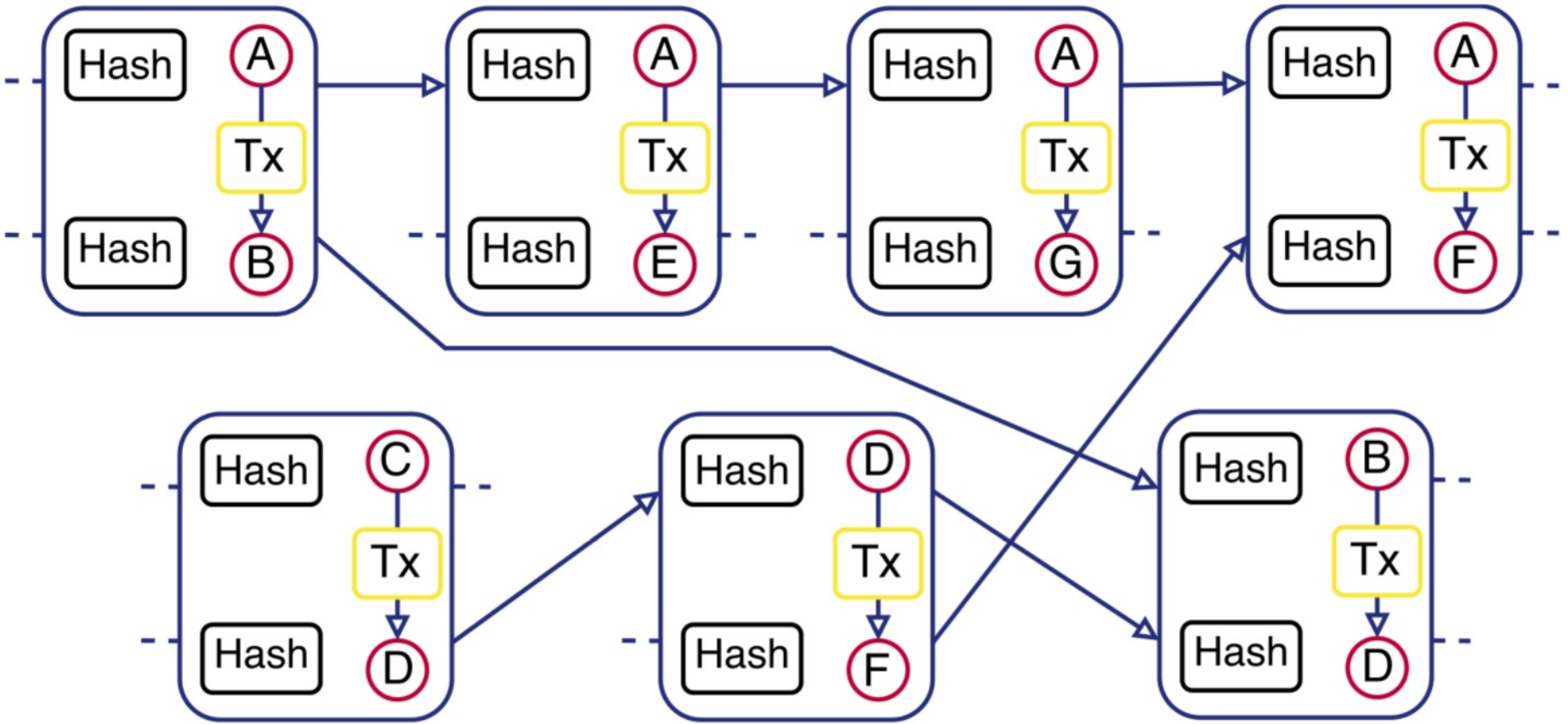


In this course (2.3): magic sparkle of **trust**

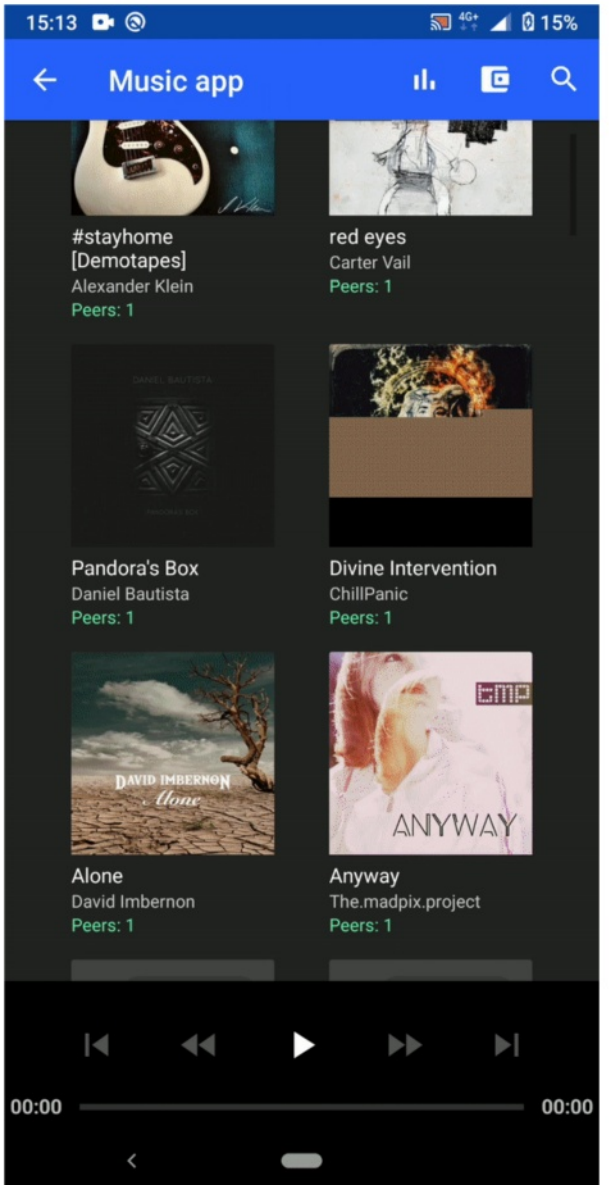
- Generic mechanism to create trust
- Remember who helped you “trustchain”
- Gossip with others
- Build graph



In this course (2.4): Trustchain – by TUDelft



In this course (3): Superapp - by TUDelft



Thesis: Artist Investment Token #6714

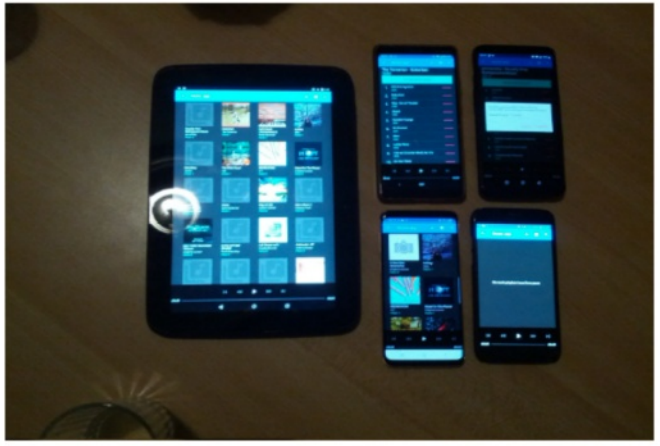
Open **synctext** opened this issue on Jan 10 · 9 comments

synctext commented on Jan 10 • edited ▾ Member ☺ ···

Thesis: replace music industry with open source code, including the investment part.

Wealth has accumulated with a select few: the investing class. The rest of the world belongs to the worker class. Digital technology is breaking the monopoly on investing. We prove the viability of our ideas with an Internet-deployment focused on an industry that operates purely digitally and has deep rooted monopolistic culture: the music industry.

Prior work: Tribler/trustchain-superapp#45



https://github.com/Tribler/tribler/issues/6714

Unstoppable disruption

1. 1991 – Linux: Open OS
2. 2001 – Bittorrent: "shared drive"
3. 2009 – Bitcoin: money, no banks
4. 2012 – Decentralised AI
5. 2025 – Tribler: online democracy

$$\sum_{i=1}^{t} f_i(\bar{w}^{(i)}) - f_i(w^\star) \leq$$
$$\leq -\frac{\lambda t}{2}\|w^{(t+1)} - w^\star\|^2 + \frac{G^2}{2\lambda}\sum_{i=1}^{t}\frac{1}{i} \leq \frac{G^2(log(t)+1)}{2\lambda},$$

In this course (4): Tribler

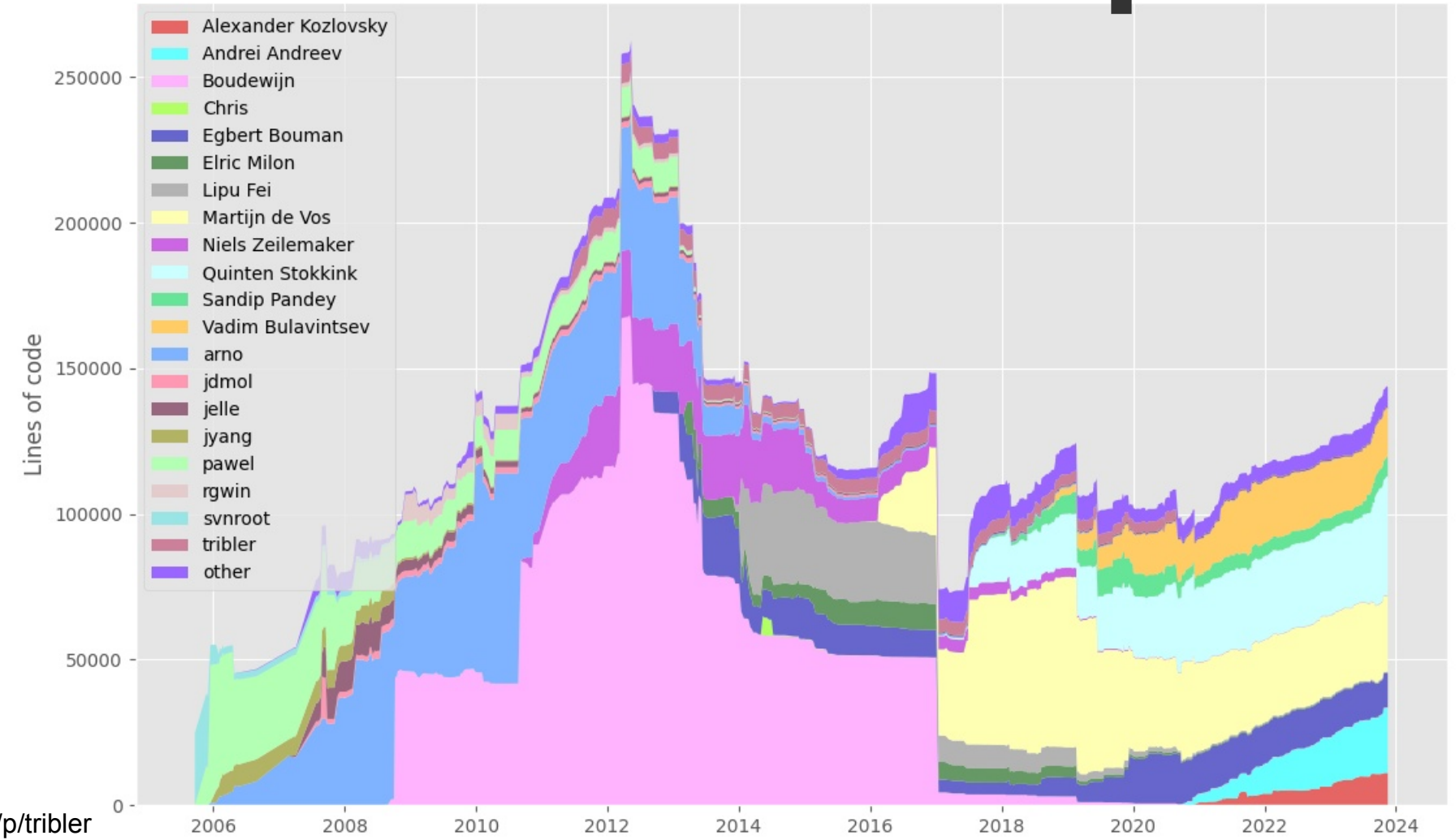
- Our academic, experimental playground (since 2005)
- Fully decentralised *trustworthy* software
- “Decentralised tiktok/Youtube”

trustworthy search | spam filtering | freeriding prevention | streaming | metadata enrichment

token economy | decentralised marketplace | social networking | crowdsourcing | tagging

Over: **2.4 million** downloads

Tribler: 306 developers



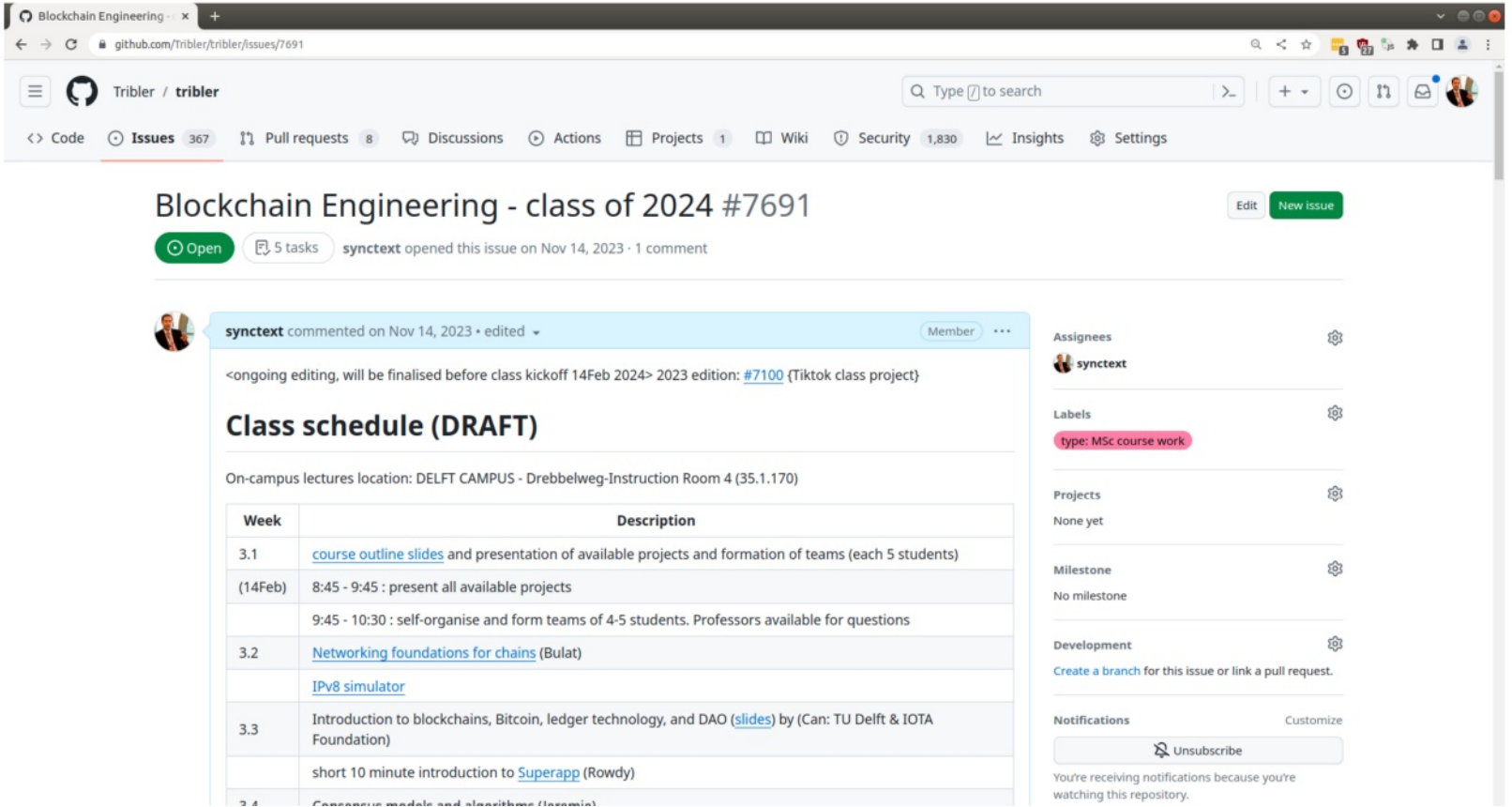
https://openhub.net/p/tribler

Class of 2024

end of intro

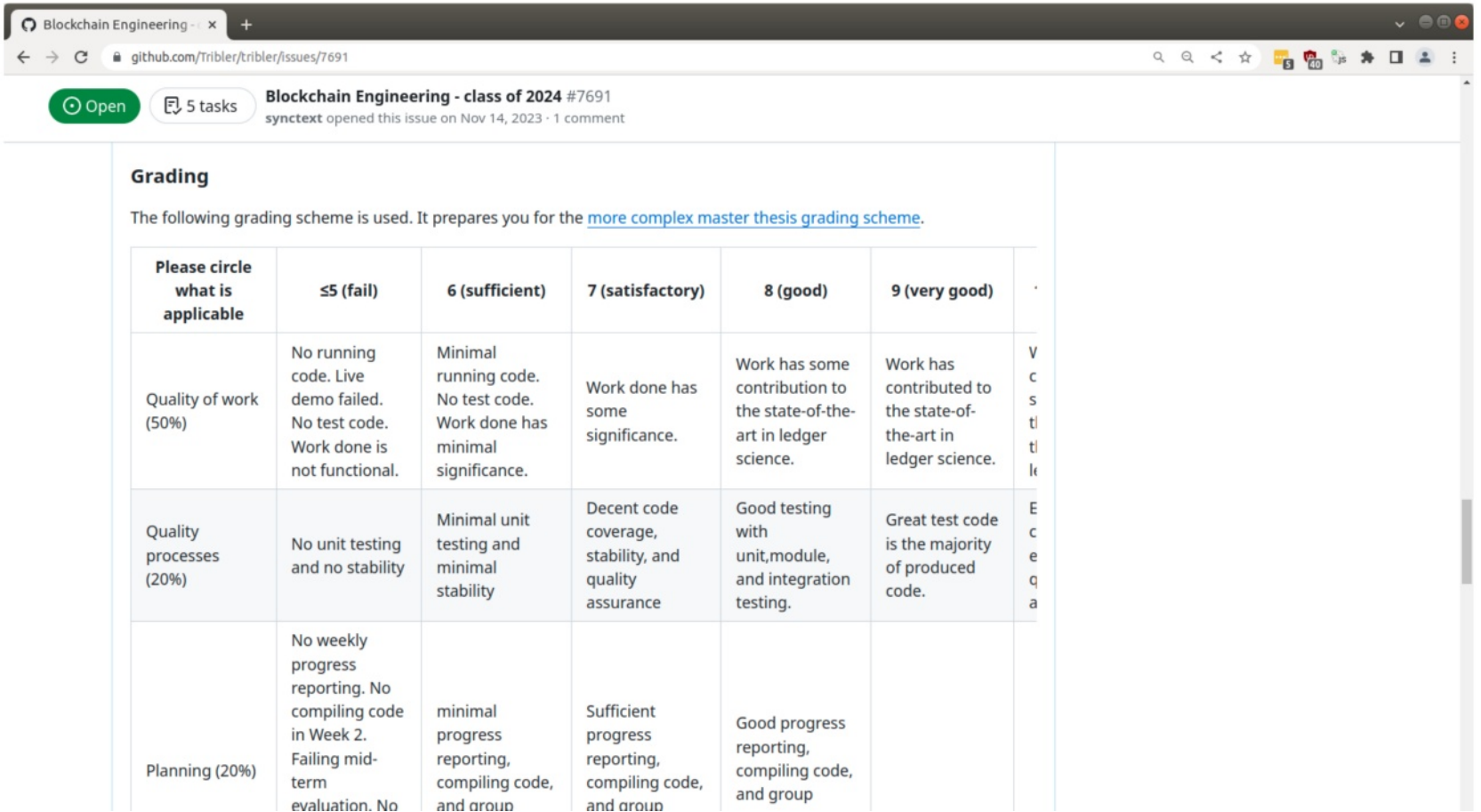
Class of 2024

github.com/Tribler/tribler/issues/7691



Class of 2024 - Grading

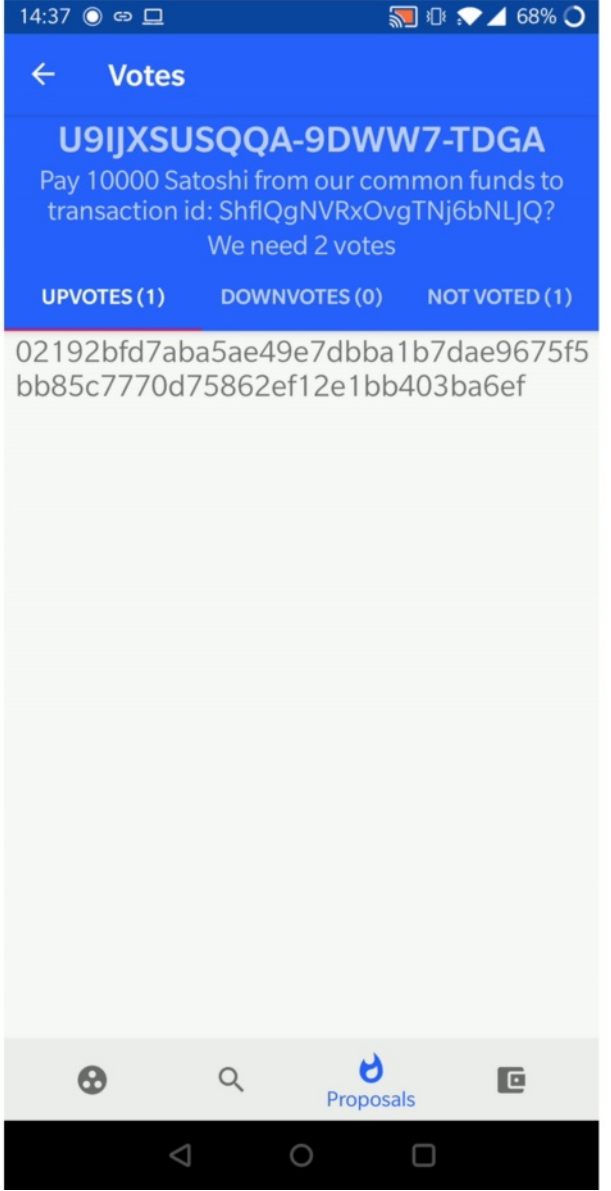
github.com/Tribler/tribler/issues/7691



Goals after 10 weeks:

- You had fun and learned
- You have running code
- Ready for msc thesis

Lab goal: Fix Society



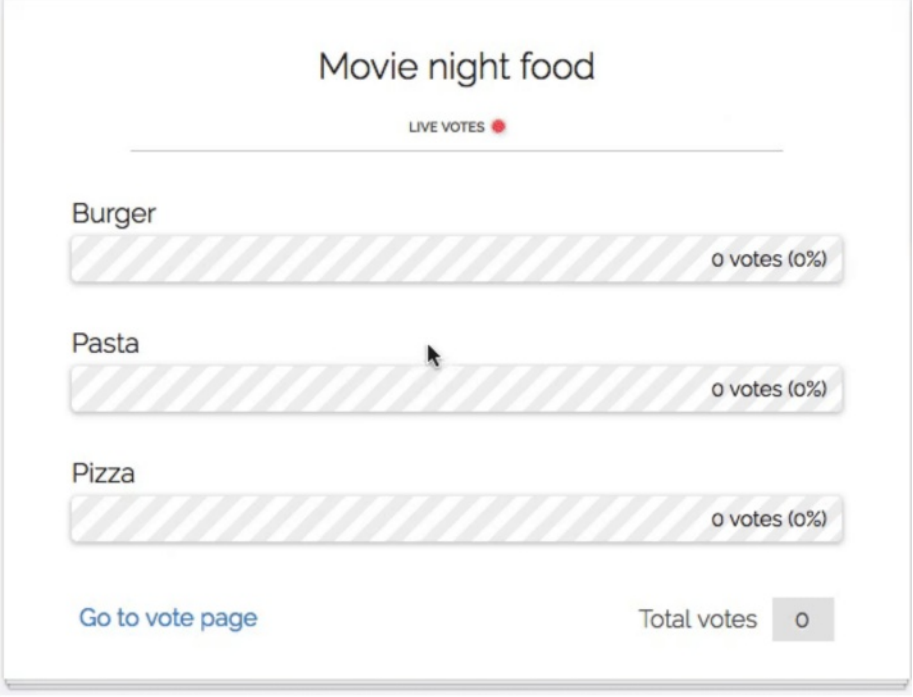
- Ready for msc thesis

(Digital Euro, EU passport, DAO democracy, distributed AI..)

Lab goal: Fix Society

On-chain Democracy (1)

- Determine how easy/hard it is to create democracy
- Anybody can contribute to deliberation, democratic decision making, and self-governance
- Design principles: permissionless innovation, scalability, and censorship resilience



On-chain Democracy (2)

- Anybody can vote and influence the top proposal for new features
- Bounty market. Open market for developers to compete on new features
- Features are checked for security,quality, and performance.
- **(unsolved)** voting by fake identities
- **(unsolved)** voting by a billion people
- **(unsolved)** self-evolving systems

Democracy-1: Blockchain networking

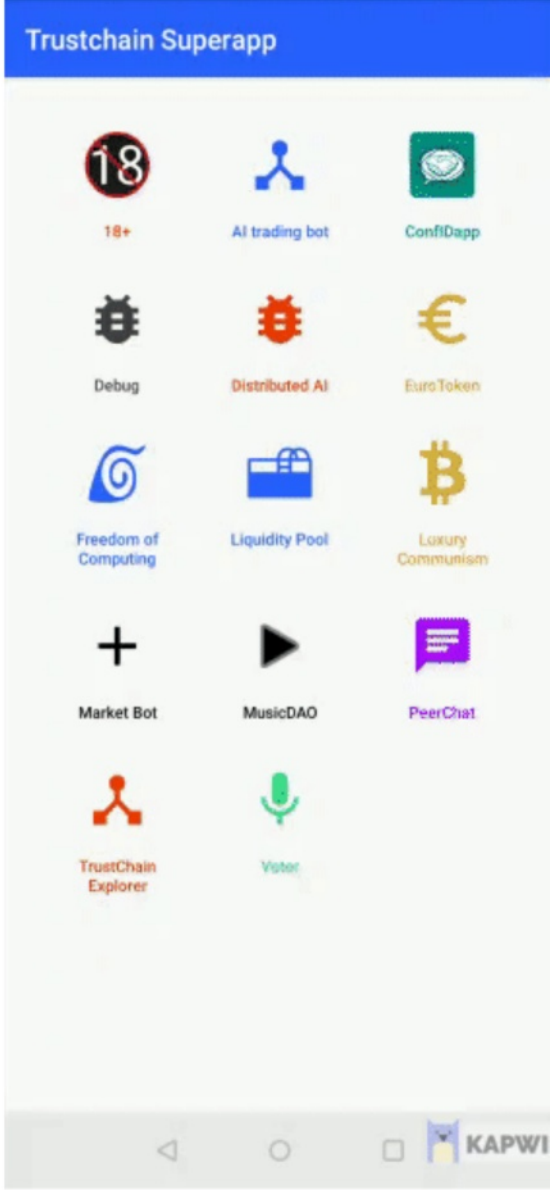
- Replay historical voting rounds on live network.
- Re-use existing ready-to-go datasets with DAO votes.
- Create ledger-based transaction blocks and share votes
- Binary transfer of bulk votes using QUIC.
- Focus on a single number: blockchain-data bits transfer
- **FIX and craft hardened code**

Democracy-2: Crypto Core

- Analyse existing running code with multi-sig, taproot, Schnorr signatures, and threshold voting
- Analyse existing code running with 4 laptops. Add new debug dashboard of connected IPv4, last-response-time..
- Identify the exact location of security vulnerabilities such as lack of message signing, lack of pre-commitment..
- **FIX and craft hardened code**

Democracy-3:
self-evolving blockchain

- Kickstarter chain: ledger-based system with internal competitive market for mutation
- Democratic decisions for "*good*" mutations.
- Code and system upgrade using plugins. Bypasses censorship by Google Store
- Re-produce prior problems such as connectivity of peers, DHT lookup, bounty…
- **FIX and craft hardened code**



Health-1: European Health Data Space *(team from Zeki Erkin @Cybersecurity)*

- Enable health data to be used for research & other purposes
- Network, consisting of regulators, medical data providers and research institutions, uses a permissioned blockchain (Hyperledger Indy)
- Query medical data and track responses, PKI infra, modular design, data exchange, proof of transactions
- Examples: the number of (medical) devices in a certain area, the average age of people using such devices, etc.

Schedule for today 8:45 – 10:30-ish

- ~~This introduction~~
- ~~teams for Democracy 1..3 and Health-1~~

- 9:30 - 10:30 questions + group formation

HOMEWORK: compile the skeleton