Tribler-lab

14 years of "ledger" experience

Dr. Johan Pouwelse
associate professor
Founder blockchain-lab.org
j.a.pouwelse@tudelft.nl

TUDelft

Tribler-lab

Why: monopolisation of the digital economy

How: craft public critical digital infrastructure

What: blockchain-based self re-enforcing trust

Lesson for today:
Blockchain Engineering is being 95% less productive
(or cheat with central servers)

Outline

- Centralisation of economy and Big Tech
- Blockchain 1.0 (Cryptocurrency) **bitcoin**
- Blockchain 2.0 (Smart contracts) ethereum
- *Blockchain 3.0 (TrustChain) ? ? ?* Tribler
  - *TUDelft 2007 distributed ledger*
  - *Trustchain*

TUDelft *Blockchain Lab*
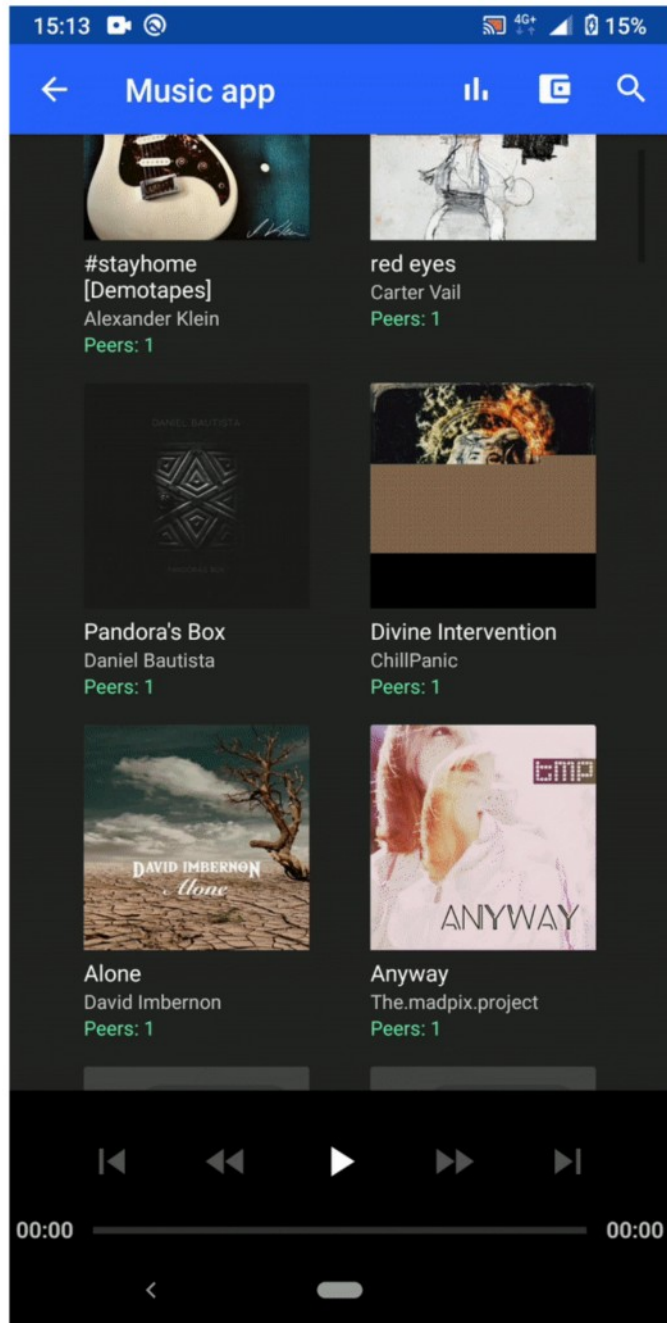
Key example for today

What is the 2nd music platform?

Music streaming subscribers 2020

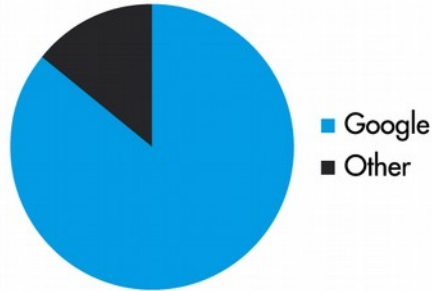| App	Subscribers
Spotify	165 million
Apple Music	88 million
Amazon Music	70 million
YouTube Premium	50 million
Deezer	7 million
Pandora	6 million
Tidal	3 million

Concentration in manufacturing

Number and Percentage of U.S. Manufacturing Industries in which Largest Four Companies Accounted for at Least 50 Percent of Shipment Value in Their Industries, 1947-2007
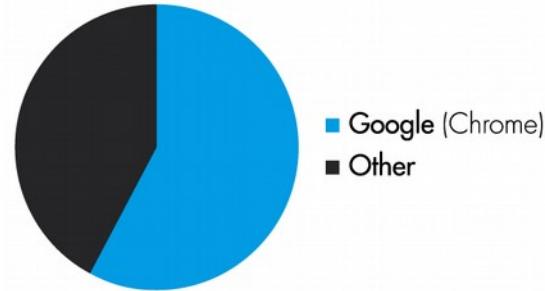
GLOBAL MARKET SHARE BY COMPANY (2017)

Internet search

- Google
- Other

Web browsers

- Google (Chrome)
- Other

Cloud hosting

- Amazon (Amazon Web Services)
- Microsoft
- Other
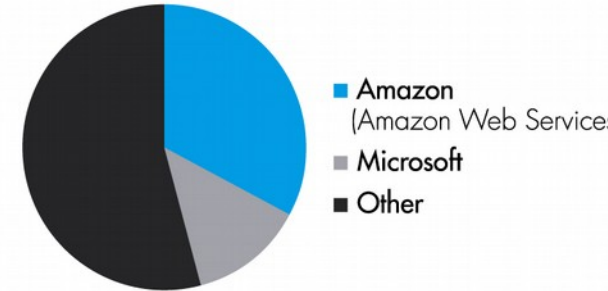
Desktop operating systems

- Microsoft (Windows)
- Apple (OSX)
- Other
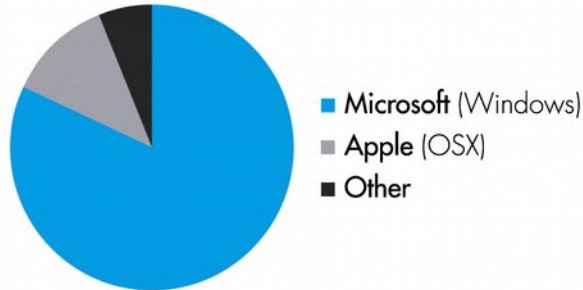
Mobile operating systems

- Google (Android)
- Apple (iOS)
- Other

Online ad revenue

- Google
- Facebook
- Other
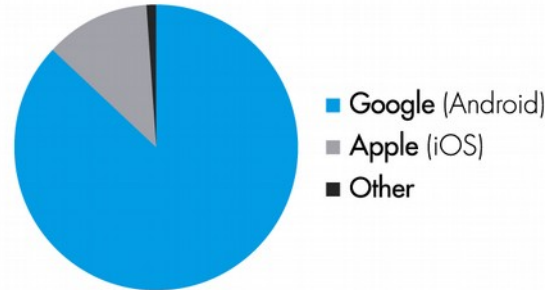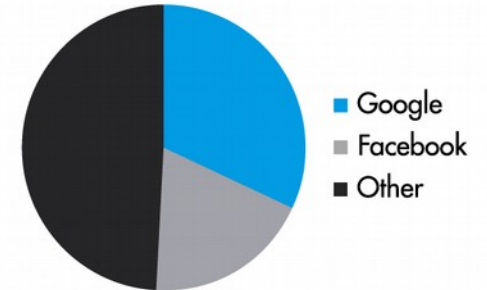
Sources: Synergy Research, CNBC, Statista (Bloomberg, Gartner, StatCounter, eMarketer.)

https://mitsloan.mit.edu/ideas-made-to-matter/will-regulating-big-tech-stifle-innovation

REVENUE SPENT ON R&D BY COMPANY (2017)

Company

Company	R&D Spending
Amazon	~$16B
Alphabet	~$13.9B
Intel	~$12.7B
Samsung	~$12.7B
Volkswagen	~$12.1B
Microsoft	~$12B
Roche	~$11.4B
Merck	~$10.1B
Apple	~$10B
Novartis	~$9.6B
Toyota	~$9.3B
Johnson & Johnson	~$9.1B
General Motors	~$8.1B
Pfizer	~$7.9B
Ford	~$7.3B
Daimler	~$6.9B
Oracle	~$6.8B
Cisco	~$6.3B
Honda	~$6.2B
Facebook	~$5.9B

$5B $6B $7B $8B $9B $10B $11B $12B $13B $14B $15B $16B
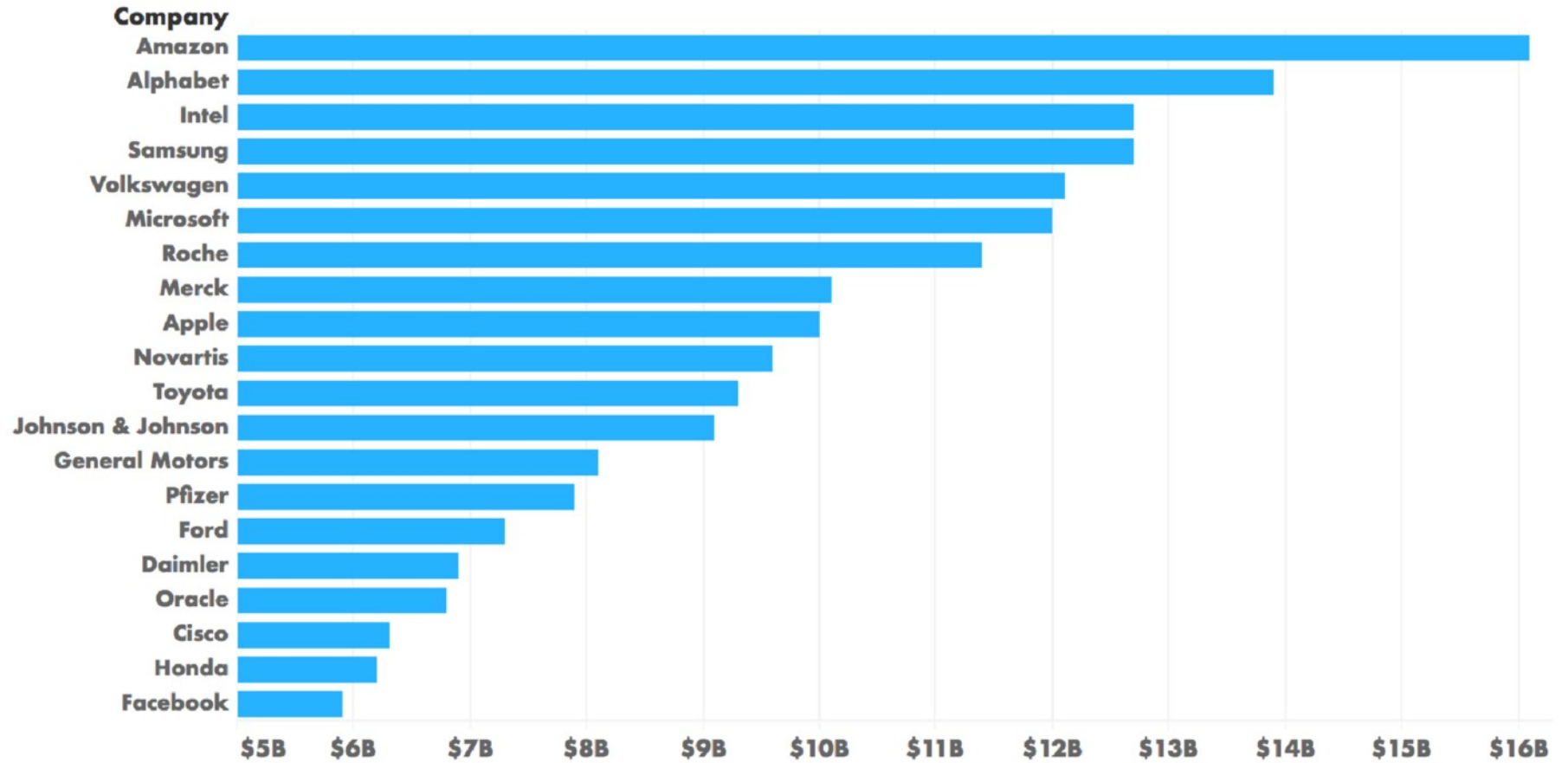
Source: Statista

TUDelft blockchain research **dream:** re-decentralise our economy

FOX NEWS LIVE

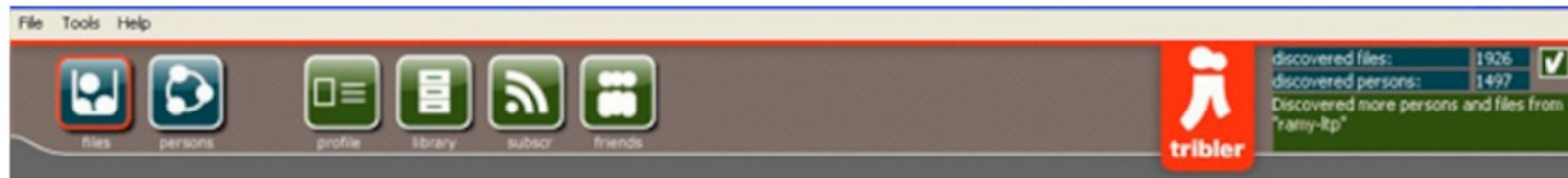U.S.   Politics   Media   Opinion   More ⋮   🔍 Watch TV

Hot Topics

TECH · Published February 10, 2012 · Last Update November 4, 2015

Forget Megaupload! Researchers call new file-sharing network 'invincible'

By | News Corp Australian Papers

TUDelft early work

- 1999: "Musicbrainz.org",
  - 2 years pre-Wikipedia.org
  - "a single code base for different distributed public writable databases"
    `https://www.usenix.org/conference/2000-usenix-annual-technical-conference/`
    `presentation/open-information-pools`
- 2007: "Creating and Maintaining Relationships in Social Peer-to-Peer Networks"
- 2007: "bandwidth as a currency", BBC News
- 2008: widgets / Distributed Apps / Smart contracts

2008: P2P Widgets

Distribute Python code

Share with strangers

Votes by strangers

Trust that?

Search Files

search

Family Filter:ON

ShoutBox Widget

Name	Shout
stage1	Very nice! Me too :-)
PCstefanie	I'm fine, enjoying these new Tribler features!
stage1	How are you all doing?
stage1	hello Shoutbox users!

Very nice! Me too :-)   Shout

Hot Torrents

No	Torrent		Popularity
1	Th	E...	17821
2	Wa		16883
3	Kn		11335
4	Tru	i	9669
5	Va		7571
6	Pu		6790
7	Th	r...	6113
8	Th	G	3343

Best Tribe Contributors

No	Peer	Up
1	unknown peer	3 TB
2	unknown peer	445 GB
3	unknown peer	399 GB
4	Alka-PC	125 GB
5	unknown peer	83 GB
6	unknown peer	82 GB
7	unknown peer	59 GB
8	firefly-PC	52 GB

2007: TUDelft & Harvard: bandwidth-as-a-currency

Blockchain-lab.org

Three generations ?

- Blockchain 1.0 (Cryptocurrency)
- Blockchain 2.0 (Smart contracts)
- *Blockchain 3.0 (TrustChain) ? ? ?*

bitcoin

ethereum

Tribler

Blockchain 1.0: Bitcoin

- Proposed in 2007 by Satoshi Nakamoto (pseudonym)
- Your public key is your wallet address
- With the private key, you can sign transactions
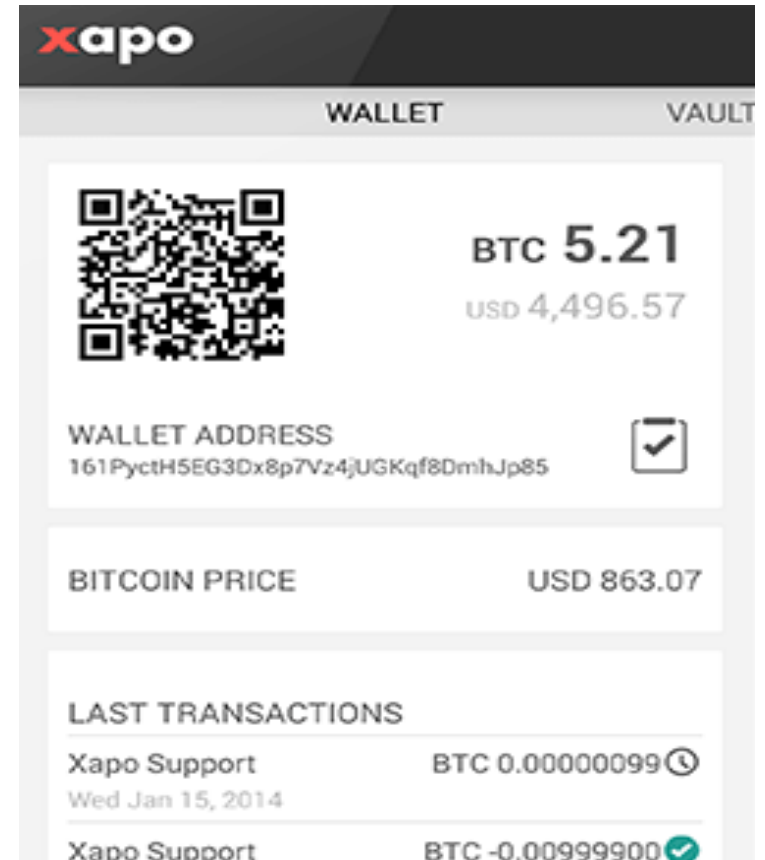
Blockchain 2.0: Ethereum

- Founded in 2014

- Nodes in the network execute **smart contracts**
  - Executed within the Ethereum Virtual Machine
  - Written in the Solidity scripting language

- Ether, the "fuel" of the network
  - Every computing step that transforms the state consumes some ether

Example of a smart contract

```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;          // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        if (balanceOf[msg.sender] < _value) throw;         // Check if the sender has enough
        if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
        balanceOf[msg.sender] -= _value;                   // Subtract from the sender
        balanceOf[_to] += _value;                          // Add the same to the recipient
    }
}
```

OPINION | TECH

Smart Contracts Are Still Way Too Dumb

They've proven good mainly at helping people lose money.

By Elaine Ou

💬 2   November 16, 2017, 8:00 AM GMT+1

Blockchain 3.0

Gossip of ledger updates

No mining
No double spending prevention

Tribler

- Science: trustworthy public critical infrastructure prevent monopolisation of our digital economy
- European "Youtube", based on Bittorrent
- Ledger-based cooperative system
  - Internet-Deployed since Feb 2006
  - 2.1M Tribler installs, 28k MAU
- **Github.com/Tribler/tribler**

"Researchers have created invincible file sharing software", Fox News, Feb 10 2012

The Tribler Open S...

https://www.openhub.net/p/tribler

BLACKDUCK | **Open HUB**

Follow @ OH   ProfJohanPouwelse

PROJECTS   **PEOPLE**   **ORGANIZATIONS**   **TOOLS**   **BLOG**

Projects ▾   Search...

Tribler

⚙ Settings | ⚑ Report Duplicate

High Activity

5

I Use This!

🕐 Analyzed 8 days ago. based on code collected 10 days ago.

Project Summary

Tribler is a social community that facilitates filesharing and a/v streaming through a peer-to-peer (p2p) network.

Tags

streaming   p2p   bittorrent   python   social

In a Nutshell, Tribler...

... has had 17,810 commits made by 114 contributors
representing 191,295 lines of code

... is mostly written in Python
with an average number of source code comments

... has a well established, mature codebase maintained by a very large development team
with decreasing Y-O-Y commits

... took an estimated 49 years of effort (COCOMO model)
starting with its first commit in September, 2005
ending with its most recent commit 11 days ago

Quick Reference

Project Links: 🔗 Homepage
  🔗 Download

Code Locations: (7 Locations)

Licenses: LGPL

Similar Projects: WebTorrent   jestery

  Deluge   Bittornado

Managers: ProfJohanPouwelse

2

bbc **Search**

Results   860

Channels   1070

Downloads   6

Videoplayer

▸ Sort by   ▸ File type   File size: 0.00 KB   83.18 GB

🔍 Filter results

channel AaBbCc
Latest Update: 27-04-2015   Torrents: 96   Popularity: ⭐☆☆☆☆

channel The Pirate Bay   **Visit channel**
Latest Update: 30-04-2015   Torrents: 7724   Popularity: ⭐⭐⭐⭐⭐   Associated torrents: 18

`25418 users marked this channel as one of their favorites.`

BBC.Storyville.2015.Indias.Daughter.1080p.HDTV.x264.AAC.M
Size: 1.56 GB   File type: Video Files   Health: ▮▮▮▮

BBC.Timeshift.The.Nations.Railway.The.Golden.Age.Of.British.Rail.720p.HDTV.x264.AAC.MVGroup.org.mp4
Size: 1.31 GB   File type: Other   Health: ▮▮▮▮

BBC.Rhod.Gilberts.Work.Experience.Series5.4of4.RAF.Fighter.Pilot.720p.HDTV.x264.AAC.MVGroup.org.mkv
Size: 652.30 MB   File type: Video Files   Health: ▮▮▮▮

channel ===>>> EZTV <<<===
Latest Update: Today 15:48   Torrents: 8630   Popularity: ⭐⭐⭐⭐⭐   Associated torrents: 7

BBC.Rhod.Gilberts.Work.Experience.Series5.3of4.Hotelier.720p.HDTV.x264.AAC.MVGroup.org.mkv
Size: 606.40 MB   File type: Video Files   Health: ▮▮▮▮

BBC.James.Brown.Mr.Dynamite.720p.HDTV.x264.AAC.MVGroup.org.mkv   **Stream**   **Download**
Size: 1.61 GB   File type: Video Files   Health: ▮▮▮▮

BBC.Reputations.1996.Albert.Speer.The.Nazi.Who.Said.Sorry.576p.HDTV.x264.AAC.MVGroup.org.mkv
Size: 684.77 MB   File type: Video Files   Health: ▮▮▮▮

BBC.Soillse.2015.U455.Mystery.of.the.Lost.Submarine.PDTV.x264.AAC.MVGroup.org.mkv
Size: 604.26 MB   File type: Video Files   Health: ▮▮▮▮

channel Things and stuff

Torrent details | Files | Trackers

Name   BBC.James.Brown.Mr.Dynamite.720p.HDTV.x264.AAC.MVGroup.org.mkv
Type   Video
Uploaded   Unknown
Filesize   1.61 GB in 1 file(s)
Health   13 seeders, 0 leechers (current)

No thumbnail available

Upload thumbnail

Family filter ☐   ▼ 0.0 KB/s ▲ 0.0 KB/s   338.2GB

Problem of trust and cooperation

Elinor Ostrom - 2009 nobel prize,
"*The Struggle to Govern the Commons*",
Science, Vol. 302, 2003

Why be a relay and help others be anonymous?
Why be a seed and help other download?
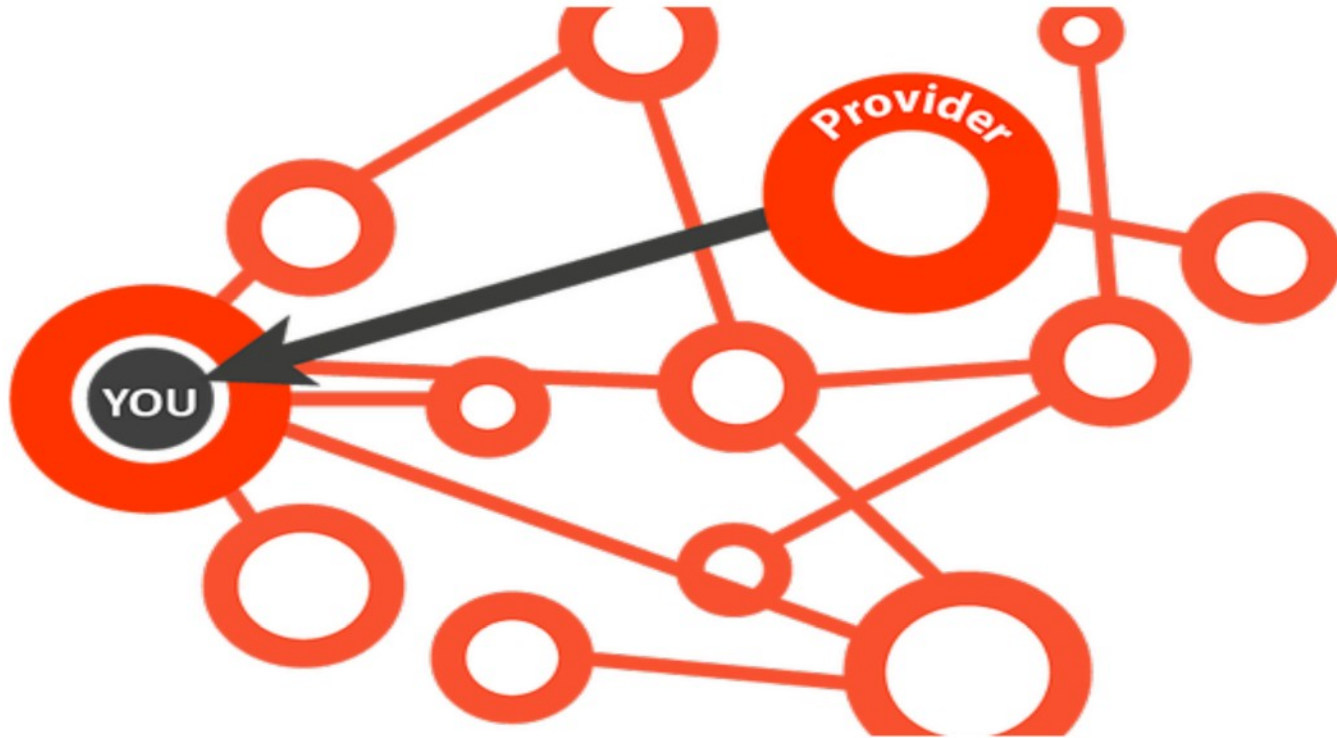Why be a contributor in Wikipedia?
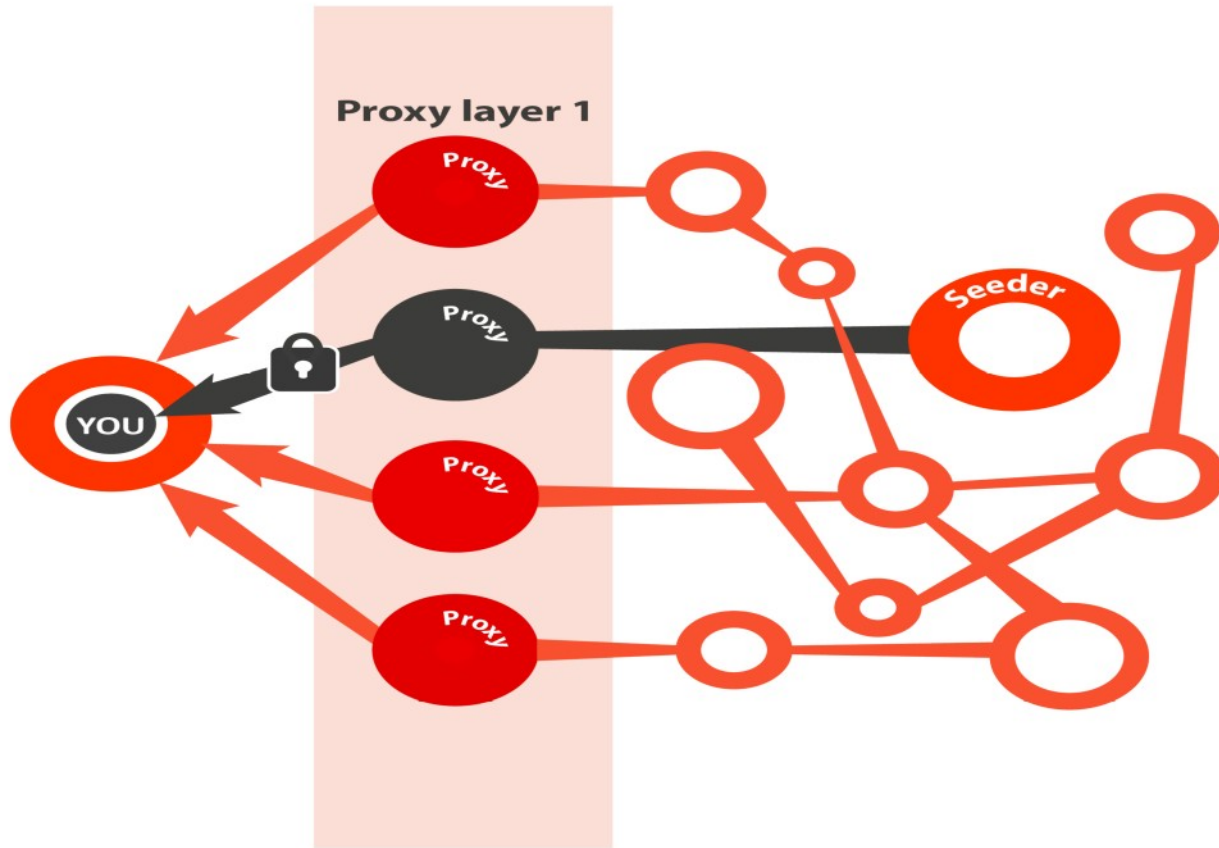Why be good and pay taxes?
Solution: *credits*
bandwidth-as-currency

Show that human trust can work at scale (a billion),
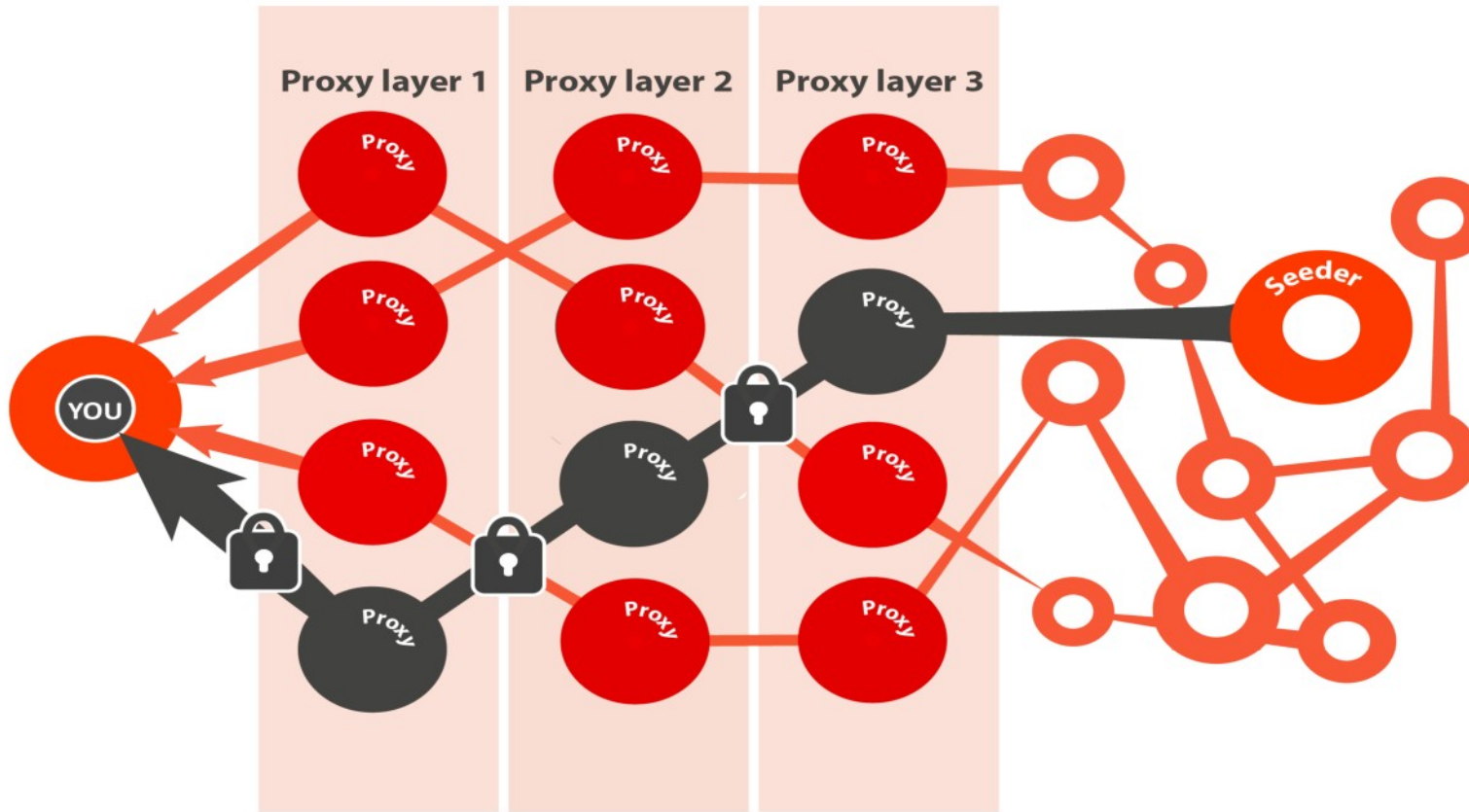prove that we can overcome freeriding, fraud and deception
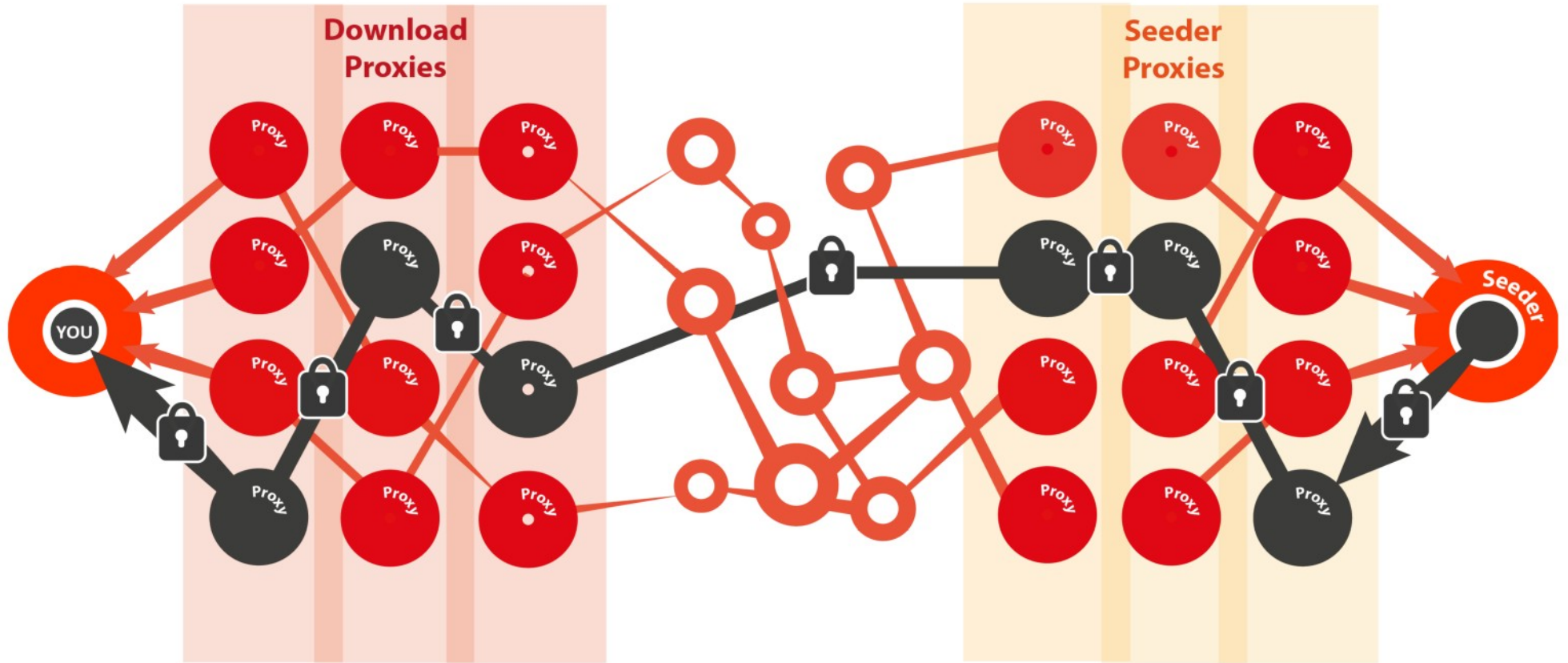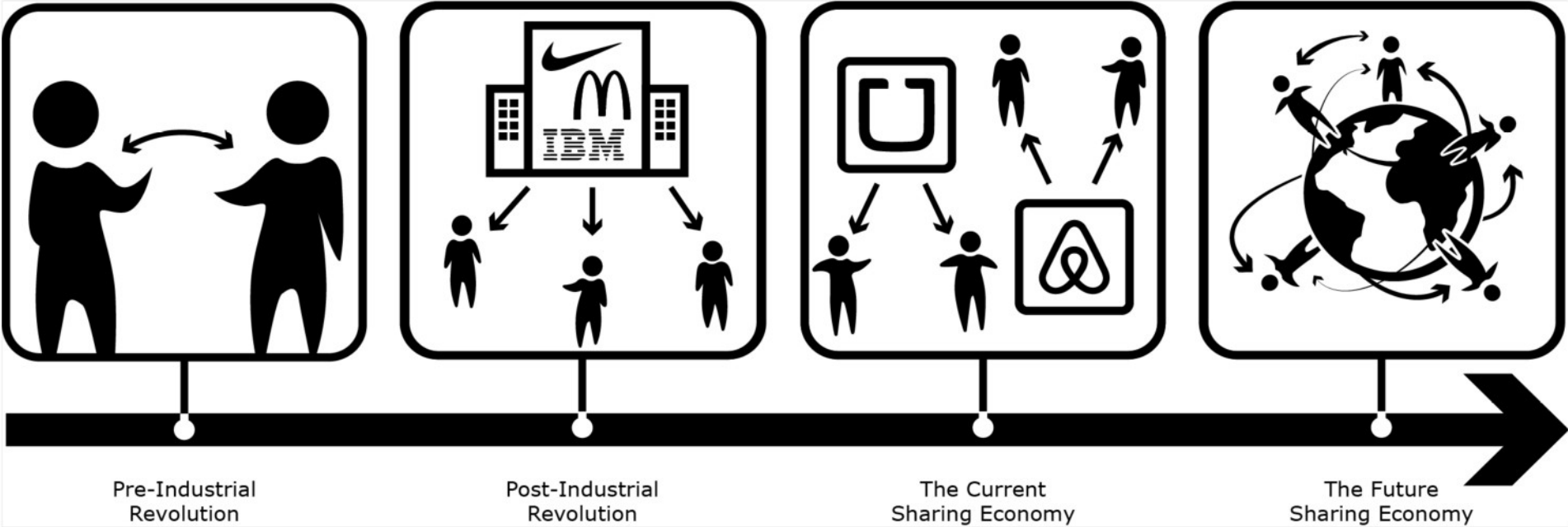
Privacy with proxies

Privacy with proxies

Privacy with proxies

Privacy with proxies

$$1 \text{ GB private} = 2 \text{ GB } P_1 + 2 \text{ GB } P_2 + 2 \text{ GB } P_3 + 2 \text{ GB } P_4 + \ldots + 1 \text{ GB provider} = 13 \text{ GB}$$

Evolution of trust

Pre-Industrial Revolution

Post-Industrial Revolution

The Current Sharing Economy

The Future Sharing Economy

Lock-in: reputation "owned" by single company

UBER

airbnb

TUDelft

generic reputation system

3

Bartercast: early distributed ledger (2007)

- ledger for bandwidth exchanges
  - Uploaded and downloaded bytes
  - Unbounded scalability
  - Incentive compatible
  - Has no global consensus
  - Insecure: free to lie
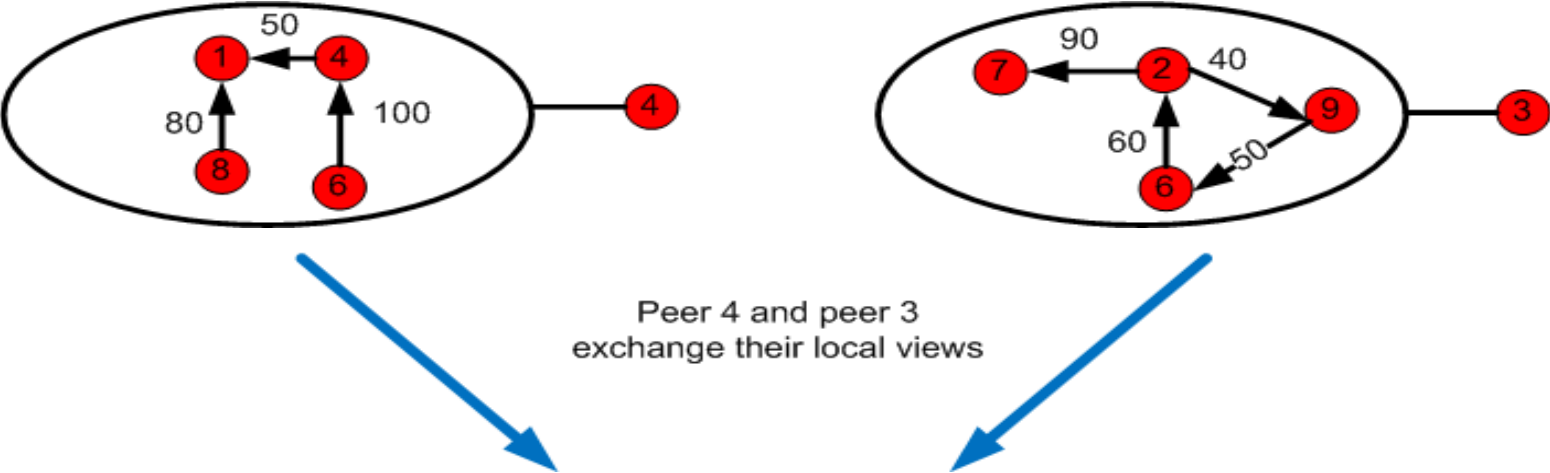- Solve freeriding, superior to T4T
- 2007: initial Bartercast deployment
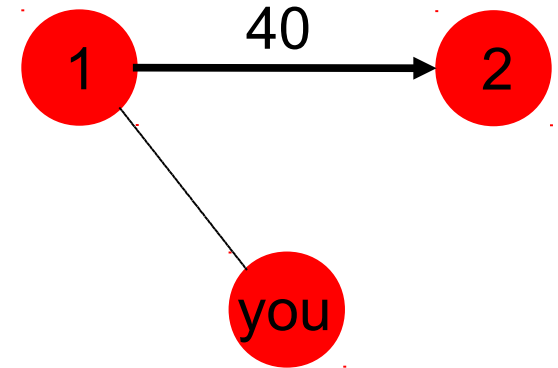
rely on voluntary reports
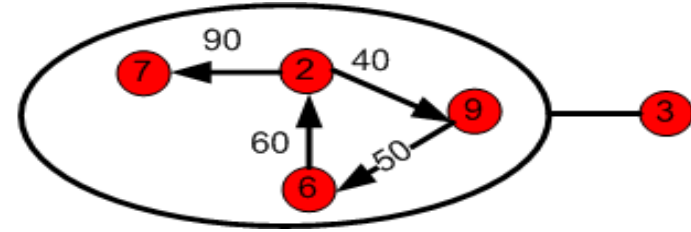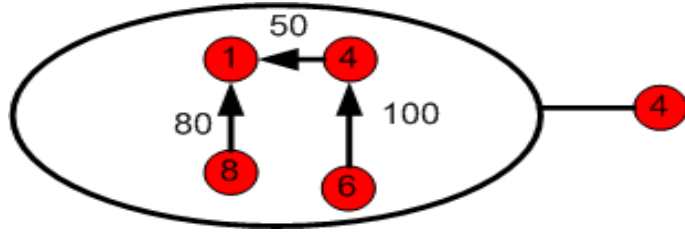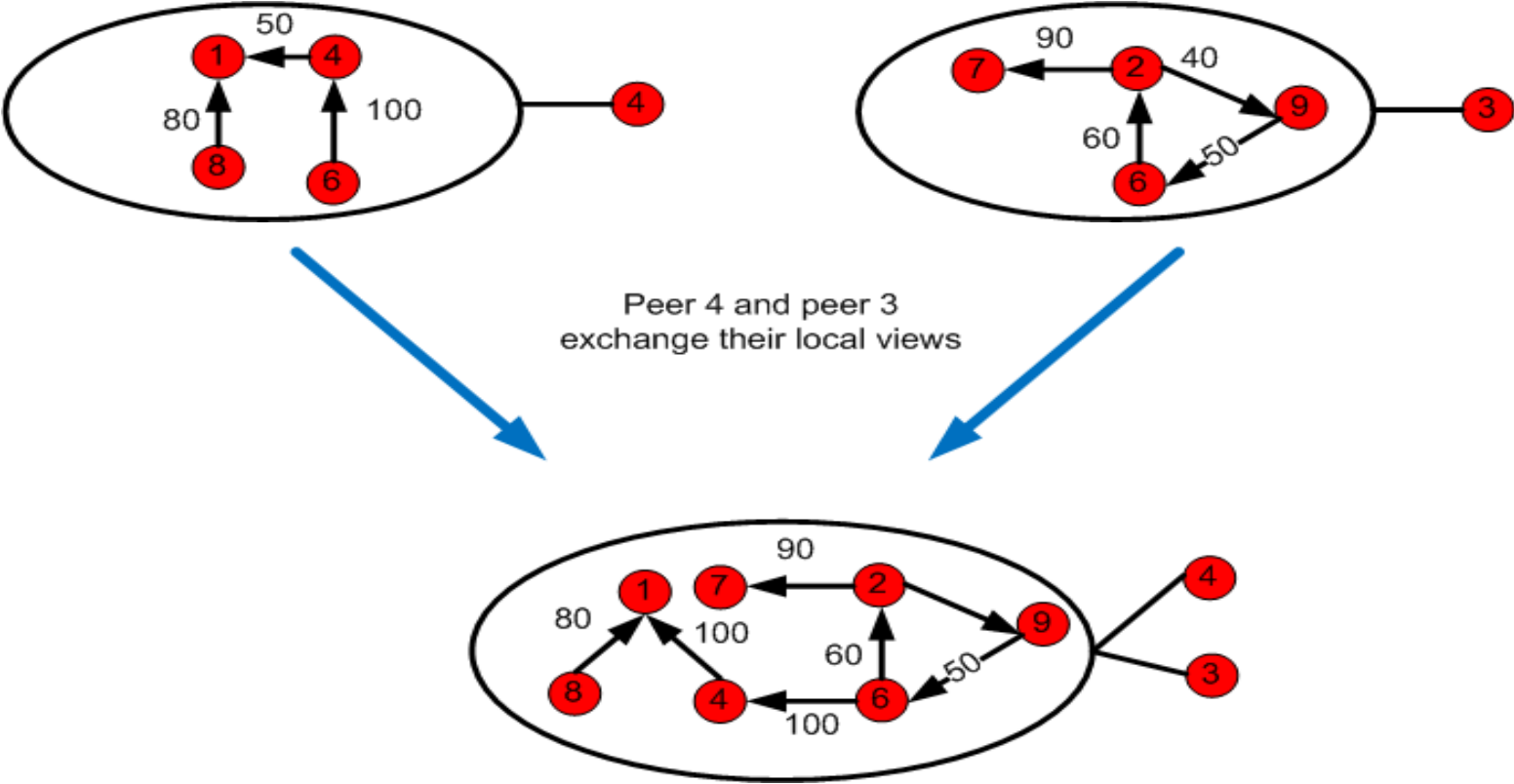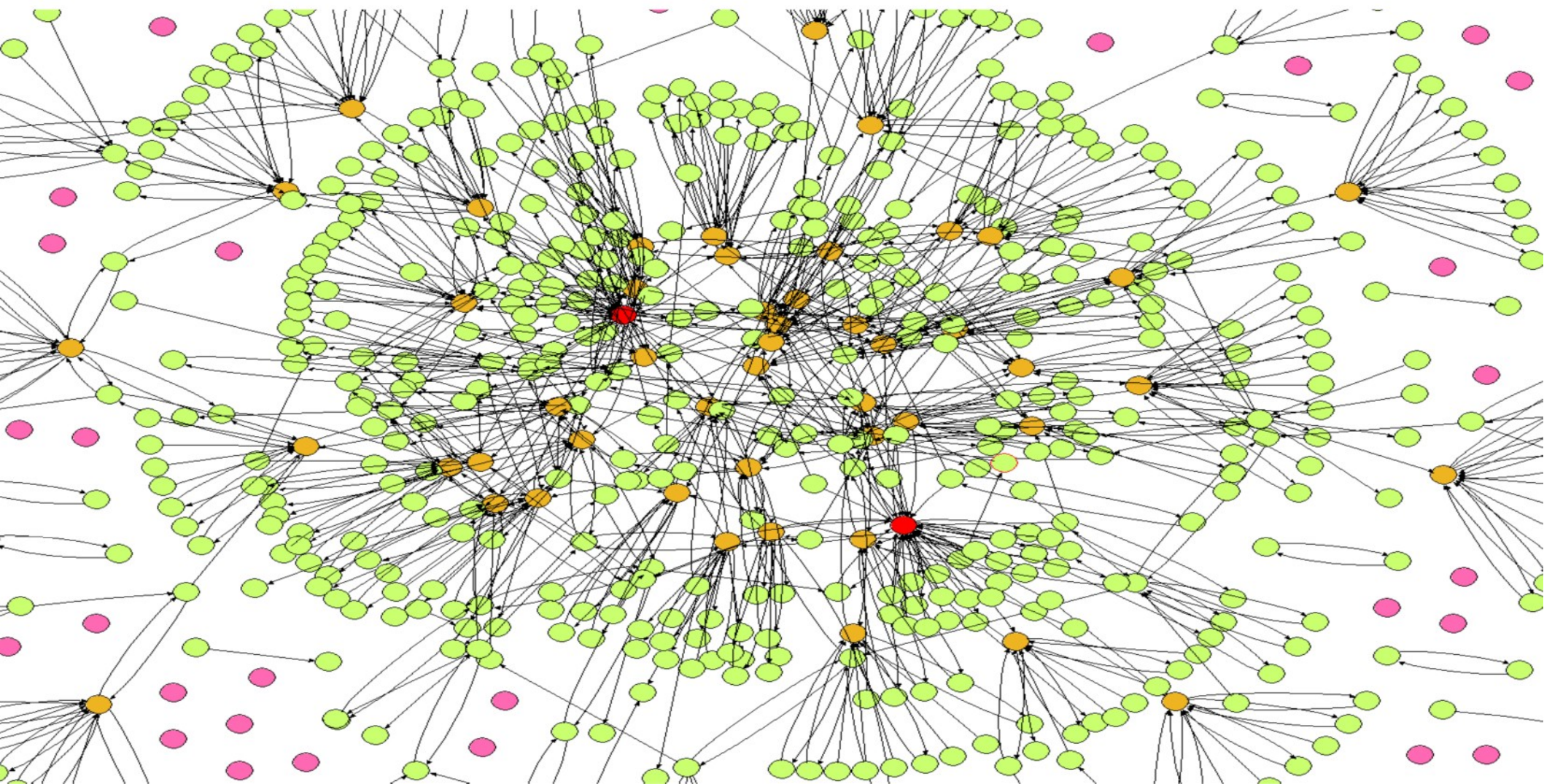
Bartercast: Information Exchange

Bartercast: Information Exchange

Peer 4 and peer 3
exchange their local views

Bartercast: Information Exchange

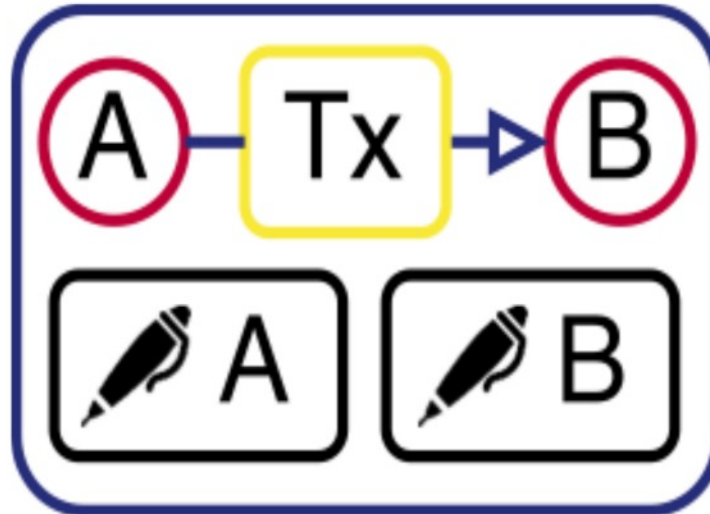Peer 4 and peer 3 exchange their local views

Bartercast: Internet-deployment
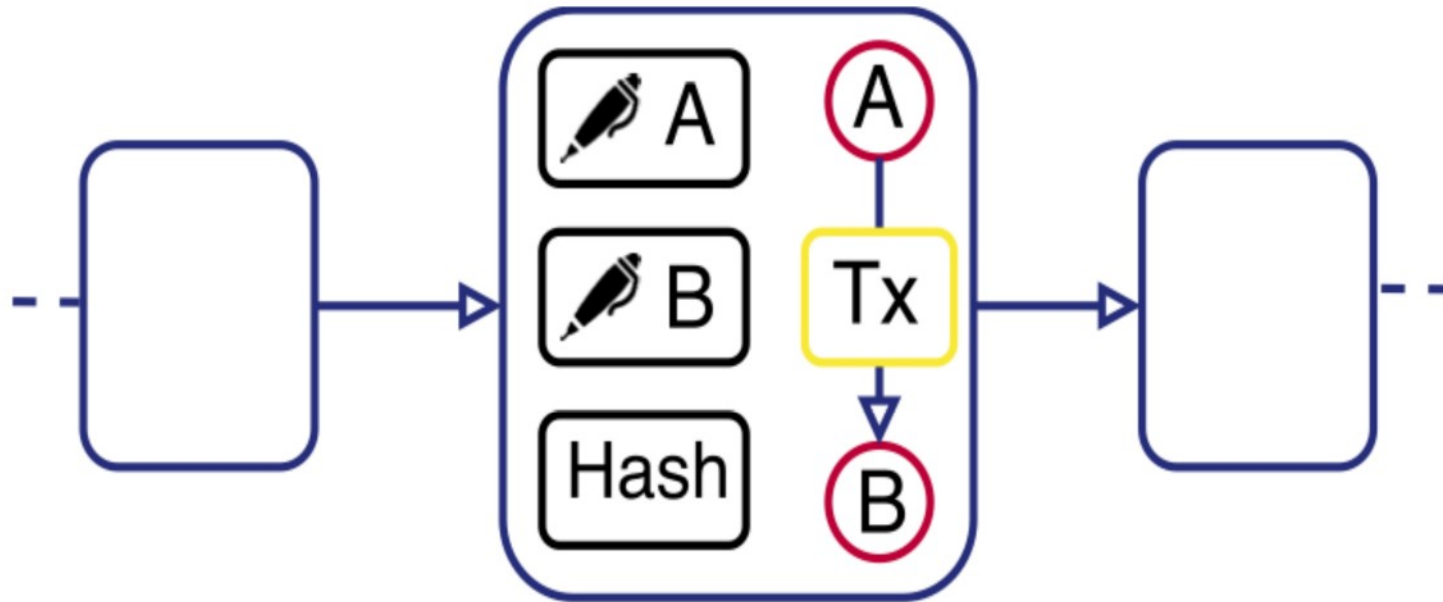
Trustchain (2012)

Transaction

- Consider a transaction between two users
- Both users sign the transaction
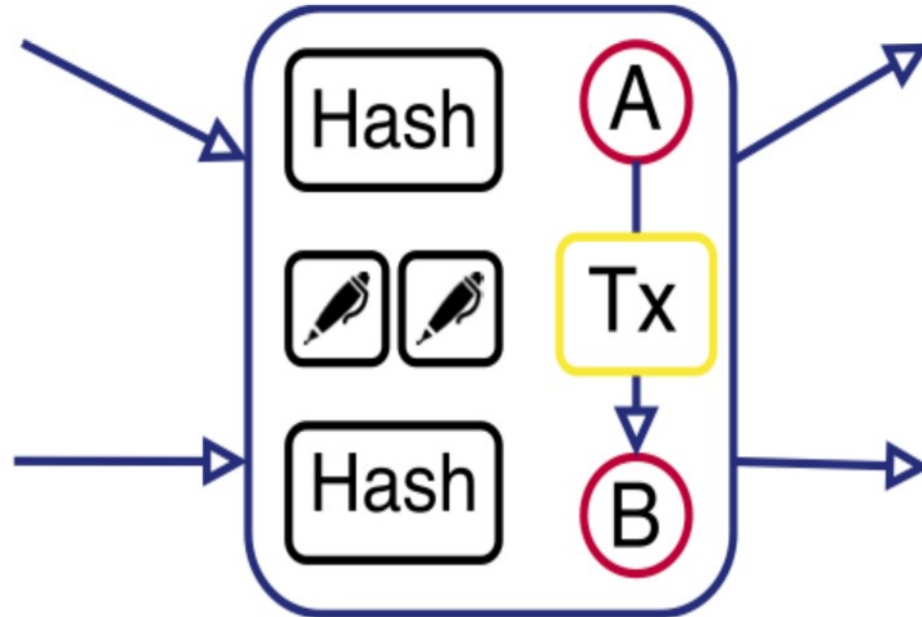 - Using any secure signing algorithm

TU Delft

Transaction Chaining

- We can chain these transactions together
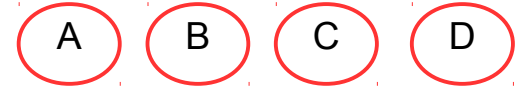- Each user keeps track of his own transaction history

Improving Security

- We add an additional pointer to each block
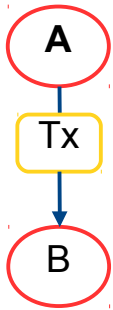 - Points towards a block in the chain of the transaction counterparty
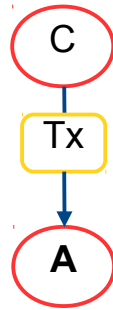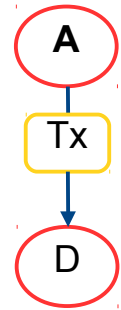
Chaining transactions

A   B   C   D

Tx units:
 - TorCoin (Lira, GoldStar, Par..)
 - BittorrentSeeding
 - Bandwidth credits

A
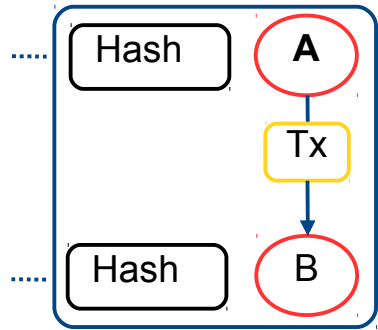↓ Tx
B

C
↓ Tx
A

A
↓ Tx
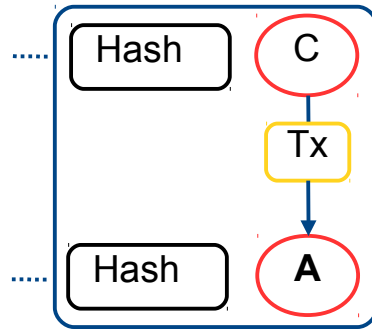D

Tx = A gives 10 units   Tx = A takes 35 units   Tx = A gives 25 units
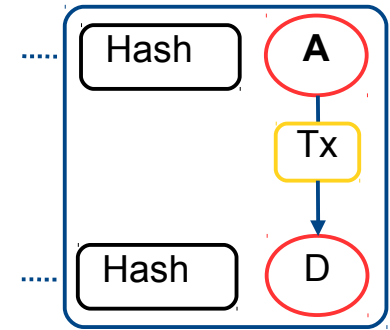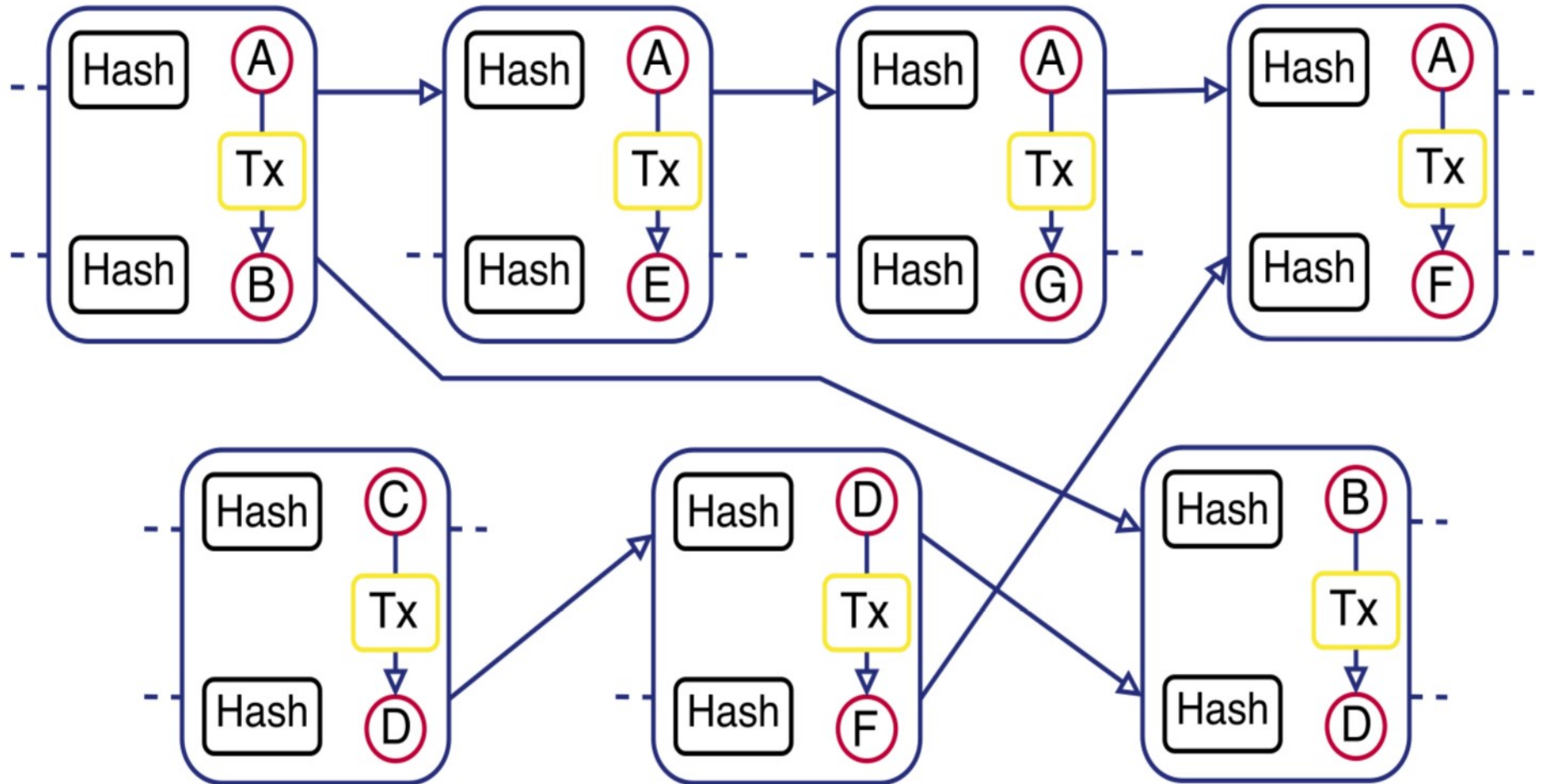
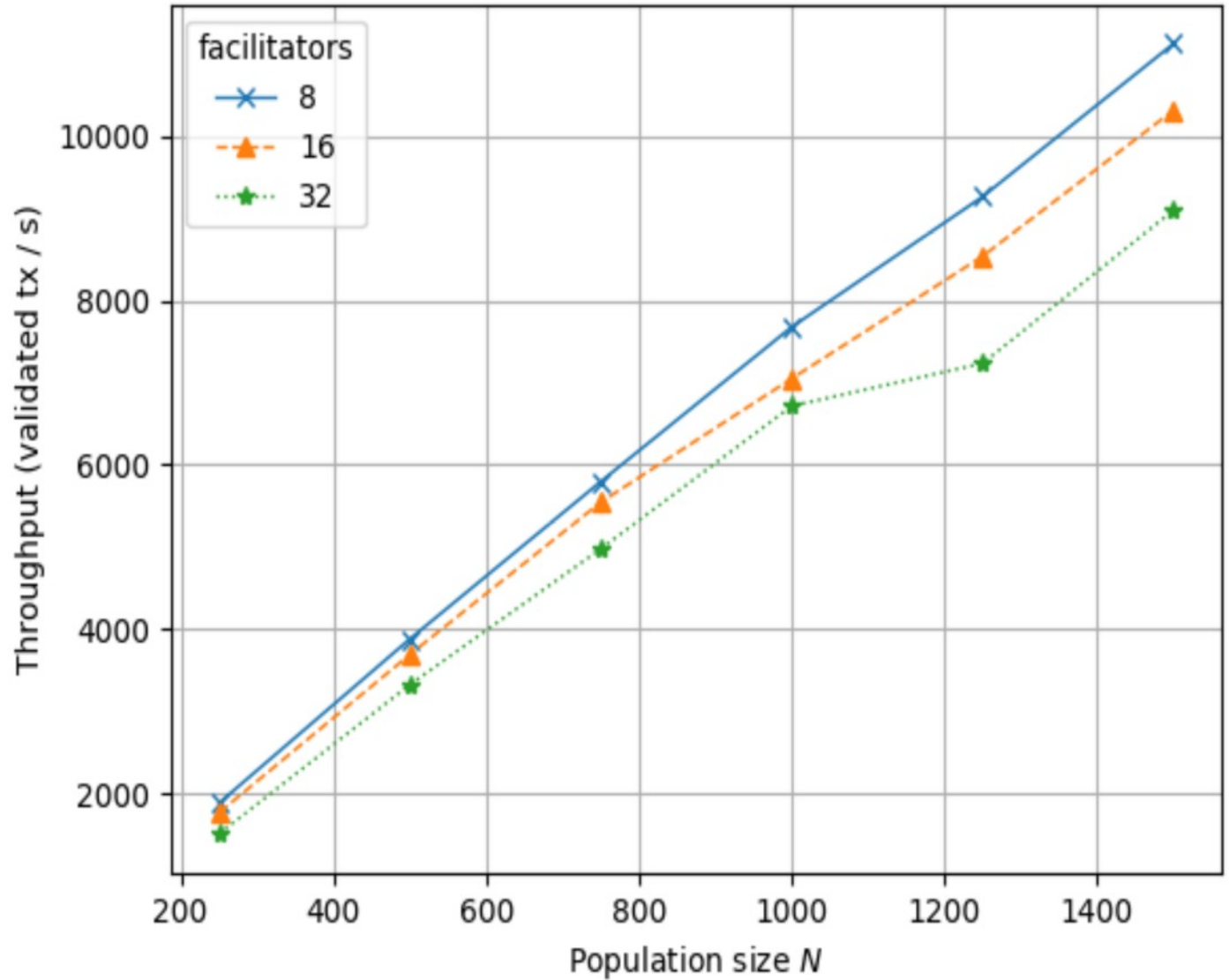# Ledger counting

Tx = A gives 10 units

Tx = A takes 35 units

Tx = A gives 25 units

Tx + Tx + Tx = 10 + -35 + 25 = 0 units

4

Entangled Chains

10,000 tps

https://github.com/Tribler/tribler/issues/
2457

Real TrustChain

4

Sector-specific Business Logic
Logistics, Energy, Finance, Real Estate, Retail, ...

Decentralized Market

Conditional Payments or Smart Contracts

Real-time Clearance and Settlement
Internet-of-Money

Legally valid signatures, electronic business transactions

Trustworthiness and Reputation
Distributed Temporal Pagerank

Blockchain Layer
TrustChain

Scalable Consensus

Self-Sovereign Identity
IPv8

Physical Unclonable Functions

Biometric-based Authentication

4

Decentralized market (in Beta)

- **Goal:** design, deploy and evaluate a decentralized, blockchain-regulated market for general asset trading
  - Assets: Bitcoin, credits, stocks, euros etc.

- Ask/bid creation and dissemination

- Transactions on the blockchain (TradeChain)

- (Scalable) reputation mechanism

https://github.com/Tribler/tribler/issues/2559

Decentralized market (in Beta)

Tribler

Search for your favorite content
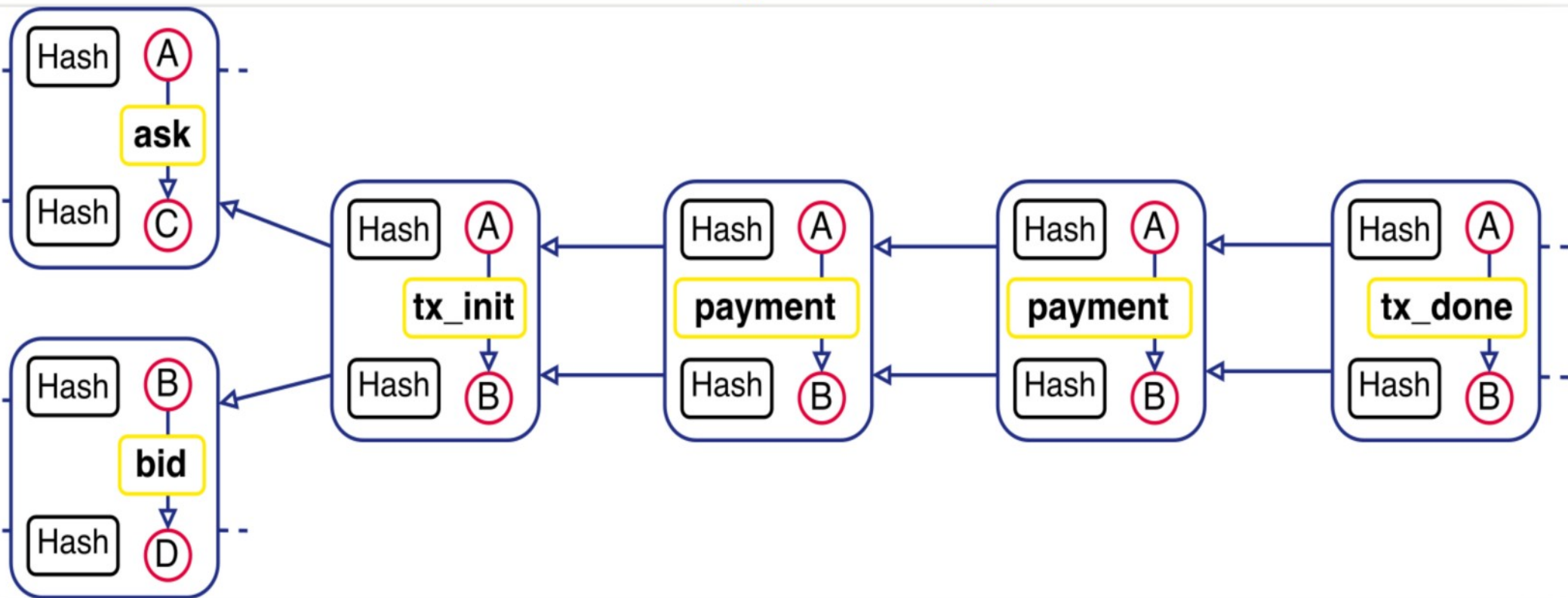
- Home
- Search results
- Discovered
- My Channel
- Subscriptions
- Downloads
- Video Player
- Debug

Market

| 0.000126 Bitcoin | 1000 Dummy 1 | 0 Reputation | 1000 Dummy 2 |

Currency: DUM1 / DUM2

BUYING

Volume	Price
20.0 DUM1	22.0 DUM2

SELLING

Volume	Price
23.0 DUM1	23.0 DUM2

Buy DUM1 for DUM2

Sell DUM1 for DUM2

Trader ID   12c406358ba05e5883a75da3f009477e4ca699a9
Order Number   1
Price   22.0 DUM2
Quantity   20.0 DUM1
Time created   2017-05-13 10:42:44

Current release: credit mining

Self-replicating code

Goal: create code that looks alive

- Python code which can buy VPS servers

- Earn coins by working as Tor-like relay

- Sell Tribler bandwidth coins on market

- Each month clone children with mutation

- Thesis title "PlebNet: Botnet for good"

https://github.com/Tribler/tribler/issues/
2925

DOWN	UP	NAME	IP	HOSTER	TIME
412947 MB	410050 MB	Gordana-Koski	185.185.24.134	linevast	55s
200863 MB	197809 MB	Loretta-Fiore	185.185.24.133	linevast	40s
38192 MB	37671 MB	Alejandra-Morcillo	185.82.23.164	linevast	58795s
28559 MB	28047 MB	Rudolf-Holubova	185.82.23.209	linevast	58737s
8712 MB	8179 MB	David-Cik	46.105.169.23	ccihosting	45s
1597 MB	1331 MB	Alvin-Christensen	185.185.27.13	linevast	56s
328 MB	2 MB	Srine-Mathiasen	178.32.53.129	pulseservers	-65s

Critical infrastructure with self-governance

scientific challenge: foundations of trust

(a) System model

(b) Conflict at gullible and traitor nodes
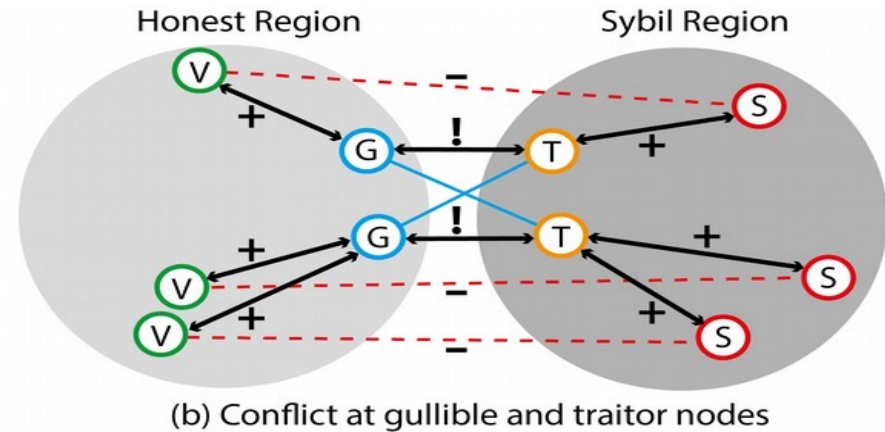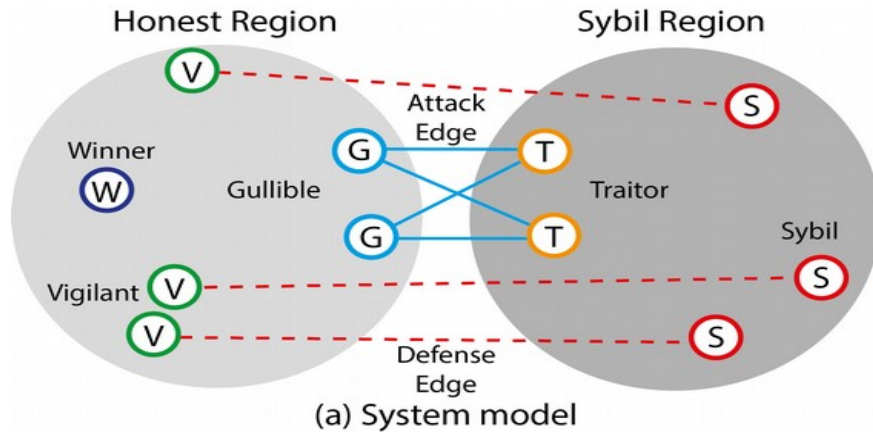
Outcome: fully autonomous economic entities, independent of creator, only temporary leaders, no dependence on any single machine
New class of distributed systems: nobody owns them

"Leveraging trust and distrust for sybil-tolerant voting in online social media", Privacy and Security in Online Social Media, 2012

kotlin-ipv8/TrustChainTu ×   +

github.com/Tribler/kotlin-ipv8/blob/master/doc/TrustChainTutorial.md

XPS13 ⊕ Declare ✔ MapleTA ⚡ SVN central ⊕ Reservation S... MSP Study Planning $ EXAM ◆ Unspent Outp... ⚡ brightspace ⚡ THESIS ⊕ Start OsirisD ◢ FlexDelft »

Load TrustChain overlay

First, we initialize IPv8 in a similar way as described in the overlay tutorial.

`TrustChainCommunity.Factory` requires two compulsory arguments: TrustChainSettings defining protocol parameters, and the persistence storage implementing TrustChainStore interface. The following snippet can be used to configure the overlay with the default settings and the SQLite store implementation:

```kotlin
val settings = TrustChainSettings()
val driver = AndroidSqliteDriver(Database.Schema, this, "trustchain.db")
val store = TrustChainSQLiteStore(Database(driver))
val randomWalk = RandomWalk.Factory()
val trustChainCommunity = OverlayConfiguration(
    TrustChainCommunity.Factory(settings, store),
    listOf(randomWalk)
)
```

As previously the Overlay Configuration should be passed to IPv8Configuration which is subsequently used to

Thesis: Artist Investment Token #6714
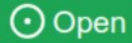
⊙ Open   **synctext** opened this issue on Jan 10 · 9 comments

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

5
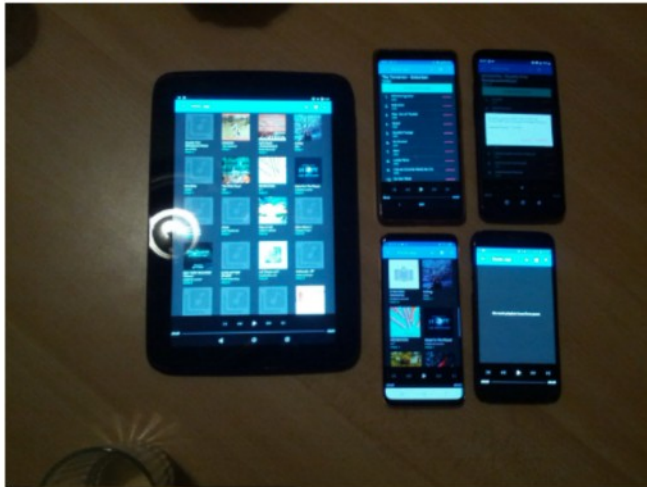
Blockchain Engineering - class of 2022 - Team FROST #6788

⊙ Open   **synctext** opened this issue 3 days ago · 0 comments

synctext commented 3 days ago · edited ▾   Member   ☺ •••
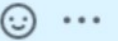
Focus: multi-signature transactions using FROST algorithm

Re-use the existing source code, as inside this WIP PR. See work by Martijn. How functional is this Kotlin code? Missing parts?
Could Trustchain+IPv8 help with overlay topology for 1+ million users scalability?
We have Taproot somewhat integrated in Superapp. Taproot.tribler.org documentation `const val REG_TEST_FAUCET_IP =`
`"131.180.27.224"` , the call itself and documentation here

Application: the Internet-deployed MusicDAO by Delft students enables music streaming and Bitcoin donations. Future step is to
integrate FROST for enabling collective music investment decisions

Grading and outcome: a *merged* pull request on the Superapp, readme addition to the repo, and some operational code. We do
not ask you to solve hard scientific problems within this course, but that you spend 5 x 5 ECTS wisely.

☺   👍 5

https://github.com/Tribler/tribler/issues/6788

5

2022: decentralised Google

i3 | Search

Findwise i3 Version 1.2
html
The below list illustrates the components that combined makes up version 1.2 of Findwise i3.

Original score: 3,44
Total nb of clicks: 20
Nb of clicks by dev: 15
Nb of clicks by sales: 5

Support contract template i3
docx
The following document describes ...

Original score: 3,43
Total nb of clicks: 180
Nb of clicks by dev: 8
Nb of clicks by sales: 172

i3 sales presentation Powerpoint
pptx
i3_presentation.pptx

Original score: 3,43
Total nb of clicks: 123
Nb of clicks by dev: 16
Nb of clicks by sales: 107

Customer X i3 proposal
pptx
$omething

Original score: 3,42
Total nb of clicks: 58
Nb of clicks by dev: 2
Nb of clicks by sales: 56

Findwise i3 Intelligence, Information and Integration.
html
Findwise i3 is an intelligent way to integrate information. The knowledge and experience of 10 years' search technology projects...

Original score: 2,67
Total nb of clicks: 9
Nb of clicks by dev: 1
Nb of clicks by sales: 8

How do I check IndexSvc logs? Slack i3 channel
msg
{fw.home}/logs

Original score: 2,17
Total nb of clicks: 23
Nb of clicks by dev: 23
Nb of clicks by sales: 0

SolrConfigXml - Wiki
html

Original score: 0,87
Total nb of clicks: 73
Nb of clicks by dev: 72

5

github.com/Tribler/tribler/wiki

Topic and open Github issue	Researcher
PageRank-like trust model with Sybil-attack resilience, math foundation	Pim Otte
Blockchain-regulated marketplace to bid/ask/cancel bandwidth credits	Martijn de Vos
Blockchain enhancement: self-reinforcing trust with collection of credit records based on live edge traversal	Pim Veldhuisen
Blockchain: earn credits with anonymous seeding and detect investments	Ardhi Putra
Blockchain: detect freeriders, refuse service; anon compatible	Ewout Bongers
Fast anonymous streaming with Tor-like onion routing	Quinten Stokkink
Blockchain-regulated markets and fault-tolerance	Bas ijzendoorn
initial Sybil attack survey	Kelong Cong
Scalability: donating TeraBytes to crowdsourcing projects	Wouter Smit
Crowdsourcing and investments	Bart Gout
Attack-resilient social media on mobile devices, using LibTribler	Paul Brussee
Dissemination videos to millions of people in seconds without servers on Android	Chengxin Ma
Adversarial search: blockchain-based spam resilience in Youtube-like systems	Jelle Licht
Connecting banks to decentral markets through PSD2 open APIs	Kypianou
re-use our decentral market platform for real-world business case, crowdsourcing real-estate	4 bsc thesis students
Understanding the impact of latency from Tor-like tunnels on Libtorrent throughput	Van Den Heuvel and Van Deursen

Reflection: 23 years of focus on building trust

- 1999: "Open Information Pools"

- 2007: primitive distributed ledger

- 2017: blockchain-lab.org

- 2030: (re-)organise our economy?