lab10 - Support #37

Didi's Log

06.01.2017 10:44 - didi

Status:	Ongoing	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour

Description

Log of activities not associated otherwise and random observations

History

#1 - 06.01.2017 10:49 - didi

Chief economist of Bank of England's *nostra culpa*:

> narrow models ignored *irrational behaviour*.

Relating to lack of or wrong predictions related to financial crisis and Brexit consequences. source.
Yeah, really? What about calling it *human behaviour* instead of *irrational behaviour*?
I'd say that economists behave irrationally, not being able to adapt their models in the face of overwhelming evidence.

#2 - 06.01.2017 10:52 - didi

Environmental cost of rare-earth mining, Baotou, Inner Mongolia.
Major demand comes from electric cars (I guess batteries), but also phones and other electronic devices.

#3 - 06.01.2017 15:34 - didi

Tools For Thought (1985). Retrospective futurism.

> It is important that we realize today that those skills of tomorrow will have little to do with how to operate computers and a great deal to do with how to use augmented intellects, enhanced communications, and amplified imaginations.
>
> Hackers *try to create a mental lever.*
>
> ...using computers to create leverage for human intellect, the way wheels and dynamos create leverage for human muscles.
> Babbage: Invention of the *penny post* (flat rate - independent of distance).

TODO: Read it!

#4 - 07.01.2017 00:09 - didi

uPort
Ethereum based Identity Management.

A *proxy contract* represents the persistent identity. This is transparent to invoked contracts, because contracts and accounts share the address space. The contract code is minimal, because it needs to remain the same for a stable identity.

A *controller contract* handles access control to the proxy contract. Can be updated without losing the identity.

A *recovery quorum contract* implements identity recovery. Works for example by having 2 out of 3 previously registered parties (e.g. friends) signing a new key.

A *registry contract* maintains cryptographic bindings between a uPort identifier and the off-chain data attributes associated with it.

uPort can generate *attestations* which is kind of signed data fragments.
It's also possible to create *linked profiles*, e.g. between uPort and a Twitter account. An attestation proofs that the user owns the uPort identity. This attestation includes the URL of a tweet which includes the uPort identity (pub key?), proofing that the user also controls the Twitter account.

Selective disclosure makes it possible to share profile attributes in encrypted form by encrypting them with a public key of the receiver before transmitting.

Developer libs (JS):
https://github.com/ConsenSys/uport-persona
https://github.com/ConsenSys/uport-lib

For mobile support, an App is in development.

The aspects of being without password and using n of m quorum for recovery are similar to zeropass. Instead of using a server, uPort is Blockchain based.

#5 - 07.01.2017 01:02 - didi

Oraclize makes it possible to fetch data from the outside world into a smart contract.
It supports various datasources, including arbitrary web APIs and IPFS.
Quite interesting is the datasource computation which allows to use an IPFS hosted Dockerfile (+ arbitrary to operate upon). Execution can then be then triggered from a smart contract (timeout ~5 minutes).

Oraclize uses TLSNotary to proof integrity of the delivered data.

The Ethereum integration works like this:
The smart contracts issues a query to a data source, e.g.
oraclize_query("URL", "json(https://www.therocktrading.com/api/ticker/BTCEUR).result.0.last");
This issues an Ethereum event which the oraclize server listens for. After fetching the data, this server issues an Ethereum transaction to the same contract, invoking
function __callback(bytes32 myid, string result).

Pricing: Oraclize currently charges $0.01 per request.

#6 - 12.01.2017 00:40 - didi

Difference between Money and Currency.

Etymology:
Money is derived either from the Latin *monere* (remind, warn, instruct) or the Greek *moneres* (alone, unique).
It's believed to originate from the temple of Juno Moneta in Rome where the mint was located.
Currency is derived from the Latin currens (running) - circulating.

Definition:
Money is any item or verifiable record that is generally accepted as payment for goods and services and repayment of debts in a particular country or socio-economic context.
It's historically an emergent *market phenomen.*
**Currency*: system of money (monetary units) in common use

There are varying definitions and the difference is not always very clear (especially in everyday use of the words), but generally speaking, money is the abstract concept and currency the materialized form of it.

#7 - 13.01.2017 13:36 - didi

Idee: Mietersyndikat
Vorbild: https://www.syndikat.org/
Kurzbeschreibung: Mieter zahlen Miete nicht direkt, sondern in einen Topf.
Aus dem gemeinsamen Topf werden Objekte gekauft (gehebelt durch Bankkredit, der durch das jeweilige Projekt abgesichert ist).
Die Mietzahlungen gehen in Kredit-Tilgung.

Erweiterungsidee:
Gezahlte Mieten werden 1:1 mit Token belohnt. D.h. Mieter A zahlt 500€, erhält dafür 500 Token (monatlich).
Die Token sind anfangs wertlos.
Wenn im Laufe der Zeit Überschuss im gemeinsamen Topf anfällt, wird dieser dafür verwendet, auf einer eigens dafür eingerichteten Börse Token zurückzukaufen. Somit steigen die Token langsam im Wert. Vorteil gegenüber Mietreduktion: Mieter können je nach Bedarf die Mietreduktion direkt "mitnehmen" oder aber den Überschuss im Projekt investiert lassen (mit Aussicht auf Wertsteigerung, die gegen eine obere Grenze strebt).
Die Token könnten auch eine andere Funktionen übernehmen, z.B. Gewichtung von Stimmrechten.

There's already something in Austria:
https://habitat.servus.at
https://gemeinsam-bauen-wohnen.org

#8 - 13.01.2017 15:43 - didi

TODO: write brief summary of https://hcpp.cz/

#9 - 14.01.2017 01:12 - didi

Etherex seems to be abandoned - probably in favour of Maker Market.

#10 - 14.01.2017 03:01 - didi

The distinction between currency and voucher is quit blurred, isn't it? I mean, if you don't or can't enforce one-time use of a voucher, it becomes currency.
Apropos blurry: I comprehend Bitcoins UXTO concept as a strange middle-thing between book money and (variable sized) coins? (context: Vitaliks pro/con regarding UXTO)

#11 - 16.01.2017 19:35 - didi

Flood Project / Hypercoin:
ERC-20 compatible token with integrated ICO-platform. Further, hypercoins can be *connected*, such a connection essentially creates an Exchange (without 3rd party, not even a 3rd party smart contract).

#12 - 18.01.2017 02:05 - didi

TODO: project def:
transparentes Grundbuch:
fetch whole Grundbuch data (how? see Grundstücksdatenbank)
visualized it:

- as interactive map: mouseover or click shows owner of parcel
- list of owners, ordered by
  - area (may be by category, e.g. agricultural, urban, ...)
  - estimated market value

Also see schweden-integriert-blockchain-beim-grundbuchamt

#13 - 18.01.2017 03:28 - didi

TODO: research
EU introduced (?) legislation requiring all user data collecting entities to offer tools/API for data export. By 2018?
This should open up a lot of opportunity for integration. Integrate everything!

Banks will soon also be required to offer APIs.

#14 - 18.01.2017 03:59 - didi

todo:
cryptoeconomicon summary and share with Thomas: https://www.youtube.com/watch?v=-oJas0jq5YY

#15 - 18.01.2017 04:00 - didi

Todo: Gleichzeitige Ungleichzeitigkeiten summary (complexity research)

#16 - 25.01.2017 20:36 - didi

Ad Komplexität:

- Professor Kruse. z.B. Wie reagieren Menschen auf Komplexität?
- Gleichzeitige Ungleichzeitigkeiten von Manfred Füllsack (Uni Graz). TODO: Summary

#17 - 25.01.2017 22:43 - didi

Eigentum

Eigentum als Fundament der bürgerlichen Gesellschaft von Karl-Heinz-Brodbeck.
Grundlegend: Eigentum am eigenen Körper. War nicht immer so. z.B. Leibeigenschaft. In China nahmen angeblich (citation needed) manche Herrscher Teile ihres Hofstaats selbst mit in den Tod.
Verhältnis zwischen Besitz und Eigentum:
Eigentum ist anerkannter Besitz.

Eine Übersicht über Eigentumstheorien findet sich auf Wikipedia.

- Platon formuliert einen Anspruch auf Eigentum für gewisse Berufsstände, z.B. Handwerker und Bauern. Andererseits sollen die *Wächter* kein Eigentum haben, weil dies keinen Nutzen für die Gemeinschaft bringen würde. Das geht soweit, dass selbst ihr Wohnraum für die Öffentlichkeit zugägnlich sein soll.
- Aristoteles sieht Eigentum als Mittel zum Zweck (Ziel des menschlichen Lebens: *das Gute*), es entspringt der Vernunft, weil Eigentum größere Sorgfalt bewirkt und dem Leistungsprinzip förderlich ist. Weitere praktische Gründe: erleichtert Konfliktvermeidung, schafft Rechtssicherheit.
- Römer: verschiedene Formen von Eigentum. Für Cicero entsteht Eigentum durch Okkupation. Konzept des Immissionsverbots bereits vorhanden.
- Mittelalter: Bei den Germanen Allmende. Also see Tragik der Allmende
- John Locke begründet das Recht auf Eigentum mit dem *Selbsterhaltungsrecht*. Eigentum an einer natürlichen Ressource entsteht, wenn sie mit eigener Arbeit vermischt wird (z.B. Bearbeitung eines Stücks Land). Er hebt gleichzeitig hervor, dass dieser Anspruch nur soweit geht wie der eigene Bedarf: *As much as any one can make use of to any advantage of life before it spoils, so much he may by his labour fix a Property in: Whatever is beyond this, is more than his share, and belongs to others. Nothing was made by God for Man to spoil or destroy*. Locke erkennt auch, dass diese Limitierung durch Verderblichkeit von Geld ausgehebelt wird, weil dieses nicht verderblich ist, und dass daraus verstärkt Ungleichverteilung entsteht.
- Rousseau hält Eigentum gleichzeitig für "das heiligste von allen Bürgerrechten" und als Ursache für viele Übel, die sich vor allem aus Ungleichheit ergeben. Er billigt demokratisch beschlossene Verteilungsmaßnahmen, z.B. progressive Steuern. Und: *„Der erste, der ein Stück Land eingezäunt hatte und dreist sagte: 'Das ist mein' und so einfältige Leute fand, die das glaubten, wurde zum wahren Gründer der bürgerlichen Gesellschaft.*

TODO: weitere...

#18 - 26.01.2017 00:27 - didi

Leaving the banking system today (migrate to BTC):

- Blog about it
- Reddit thread about it
- Cashila: BTC -> SEPA and SEPA -> BTC. SEPA receiving takes place via a shared bank account on a czech bank, association to a cashila user is done via a reference number to be set by the sender. Integrated in Mycelium wallet.
- bit2me allows BTC to cash conversion. Currently works in Spain and Romanian. Workflow: send BTC to a given address, then you get a code (via SMS) which can be used to retrieve cash from an ATM.
- bitwala allows sending BTC to SEPA and SWIFT and offers a cheap (prepaid) credit/debit card (VISA). The card holds fiat currency, which means when charging BTC it's immediately converted to fiat at the current rate.
- xapo debit card is associated to a xapo (remote) wallet, which means conversion to fiat is done at the moment of a card transaction.

- bitwage combines a Bitcoin bridge between currencies/countries (low fees, fast transactions), (team) invoice management and job mediation.

#19 - 04.02.2017 18:11 - didi

Antonopolous on *Streaming Money*.
Essence: With automation and near zero transaction cost (payment channels), the charachter of money will change, like happened to the character of information.
E.g. why are salaries paid monthly? Not daily, hourly, per second?
Payments may be transformed into streams.

#20 - 07.02.2017 18:18 - didi

Ideas forwarded by Thomas:

- Decentralized drug intolerance checks (TODO: are ZKPs helpful? How does this currently work? Can something be learned from Watson Health?)
- Decentralized private storage (chunked, encrypted). Minebox like, but max. user friendly

-> Privacy box

#21 - 12.02.2017 16:05 - didi

I took a look at the Polkadot Paper.
My understanding after reading some chapters:
It's an abstraction above existing (and future) blockchains, having itself a Blockchain (named *relay-chain*) at it's core (probably an instance of Ethereum).
It envisions a consensus algo which is something between Proof of Authority and (Nominated) Proof of Stake.
Integrated Blockchains (and similar data structures) are integrated as *parachains* (parallelised chains).
Polkadot allows cross-parachain interaction, e.g. an Ethereum contract could *send* a transaction to Bitcoin and vice versa.
Polkadot is a proposal for how to decouple consensus and state transition.

It defines 4 roles: Collator, Fisherman, Validator and Nominator.
Collators propose blocks of parachains. Fisherman look for misbehaving validators and get bounties for such discoveries. Validators form consensus (as known in PoS), Nominators add weight to Validators of their choice.

My unqualified opinion:
Looking at the status quo of Blockchains, I have some doubts about how useful this could be.
It somehow looks a bit like a bet against Ethereum. E.g. in the preliminary analysis it also takes a look at Casper (section 2.2.3), noting that it's complex, hard to introduce (hard fork) and needs to be seen if/how it will work out. Also, while focusing on the scalability aspect, it barely mentions the sharding option / plans of Ethereum.
The aspect of integration of public and non-public chains looks like a valid point.
Also, the paper acknowledges that integration as imagined would be challenging/limited with the Bitcoin blockchain as it is (currently deployed Bitcoin protocol).

While there's obviously a lot of different Blockchains out there, I'd argue that Bitcoin and Ethereum stand out, having achieved significant network effect. Some kind of integration was already done, e.g. with btcrelay.

If Ethereum's scaling plans work out, I don't see why its public instance couldn't fulfill the role of the "mother of all Blockchains" itself.

#22 - 19.02.2017 00:16 - didi

Digital Roadmap Austria
Simple vs easy

Edcon resources (also see related tweets:
etherisc
Swarm (hosted on Swarm). Also see tutorial video. Swarm hosted bulletin board.

#23 - 19.02.2017 01:17 - didi

On DAOs. Blog series.
Blockchain is a stateful protocol. Smart contracts are protocol extensions.
DAOs overcome national regulation, instate international rules.
Preliminary token sale allows for financing building (dev, marketing, ...) the actual DAO.
Voting tokens holders govern, can get paid a small fee for that service.

About dfinity: moved to #61.

#24 - 28.02.2017 20:10 - didi

Meteor
REPL: meteor shell
Output a collection (example): Machines.find().fetch()

Meteor uses a Mongo DB on the server and a Minimongo DB (in memory) on the client.
They are synced with the DDP protocol (Distributed Data Protocol).
Generally, the server needs to publish exposed collections and the client to subscribe to it.
In this project there is no such code, probably because the autopublish package is still included (it's supposed to be removed in releases).

I wonder if the file BIM_global.js being in both server and client context is needed / a good idea.
According to the meteor guide there should be nothing in the global context.
server/main.js and client/main.js are the entry points. They should include only code imports/startup.

#25 - 03.03.2017 15:57 - didi

Elevate Festival

Algorithmic Fate 1933/2016 compared how technology was used in the 30ies and now.
Back then, for a while IBM created punch-cards containing personal information (profiles) incl. family relationships, helping to identify Jews.
Today, IBM Watson processes data related to immigrants (e.g. social profiles) to calculate a *terrorist score*.

Human Obsolescence & Data Basic Income: The Institute of human obsolescence conjectures: Most of physical human labor has already become obsolete, cognitive labor is following (AI). However data generated by humans is still valuable.
Art project: The *body suit* uses heat generated by the body to mine cryptocurrency. Seems inspired by the Matrix :-)
Next project: How about this deal: Basic income in return of data produced?

Upload yourself: The artist Lars Holdhus will upload his genome as torrent (150GB).
He thinks China is far ahead regarding experimenting with genoms. BGI wants to *sequence the world*. Political tool.
CRISP genome editing.

Smart for a reason

In an urban setting, a lot is shared. Sharing is our evolved response to interdependence. Neoliberalism threatens that.
Sharing is the key to smart city.
Seoul and Amsterdam leaders. Sharing cities apply experience, not commercial and technological *solutions*.
Bridging social capital.
Commercial sharing solutions sideline the social vision. Local regulation and governance needed. Commercial sharing not egalitarian.
Social urbanism examples:
Cheonggyecheon is an example for (restored) public commons.
Porto Allegre: participative budgeting.
Belo Horizonte: food.
Sharing as relational process, not transactional one.

Rent the runway
Toy libraries.

Freetown Christiana in CPH. Alternative currency.
Repair cafes.
Occupy movement has created new institutions (incl. currency).

Book Sharing Cities.

https://en.wikipedia.org/wiki/Sidewalk_Labs
Larry Page talked about taking over infrastructure provision of a city (existing or from scratch).
Model: Dubai and Singapore.
Failure of imagination.

#26 - 03.03.2017 17:09 - didi

Run Ethereum private chain:

create a genesis file, then initialize the chain:
geth --datadir .eth-test init genesis.json
then start a node:
geth --datadir .eth-test --testnet --networkid 1357 --nodiscover
The testnet param causes geth to operate in a subdir *testnet* of the datadir.

Consecutive nodes need to do the same, the genesis file needs to match.
On the second node, manually add the first one as peer in geth console with
admin.addPeer(<enode>)

Of course at least one node needs to mine for the chain to progress. Add --mine --minerthreads 1.

An explanation of the genesis file can be found here.
Example which also premines to an account:

```
{
    "nonce": "0x0045004400430042",
    "timestamp": "1463868000",
    "parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "extraData": "0x476c6f72696669656420706c61696e206f6c6420656c656374696f6e",
    "gasLimit": "0xFFFFFFFF",
    "difficulty": "1000000",
    "mixhash": "0x0000000000000000000000000000000000000000000000000000000000000000",
    "coinbase": "0x3333333333333333333333333333333333333333",
    "alloc": {
        "ae4a95287aaa216c5361db6810d06f28de956c4d": {
                "balance": "6382507000000000000"
        }
    }
}
```

#27 - 05.03.2017 22:53 - didi

Thought about money:
Cryptocurrency with fixed supply a la Bitcoin (and most others) are inherently prone to speculation.
Crypto-currency with a Proof-of-Work which is bound to actual value creation (as e.g. Solarcoin or [[lab:BikeCoin]]) should be less susceptible to that.
Government controlled money represented in crypto coins will probably be the most stable choice for the foreseeing future.

Also see #49, Dezentrales_Geld.

#28 - 07.03.2017 14:11 - didi

Did letsencrypt renew for die-unendlich-wahl.at. Required nginx to be stopped (for the standalone variant to work).

#29 - 09.03.2017 00:47 - didi

Clojure resources:
https://www.cis.upenn.edu/~matuszek/Concise%20Guides/Concise%20Clojure.html
http://www.4clojure.com
https://clojure.org/reference
https://www.rosettacode.org
https://www.tutorialspoint.com/clojure/

#30 - 12.03.2017 03:16 - didi

Ethereum Roadmap
Metropolis (ETA: 3-6 months)
Abstraction:

- Separate consensus, logic and data
- Support for different consensus protocols, account security (other algos, e.g. Lamport signature), scalability (?). Make it easier to build custom Blockchain configs. zk-snarks (Project Alchemy)

Serenity (?)
Switch to PoS (based on Casper)
More abstraction, e.g. UTXO based token support, advanced contract execution (e.g. self paying contract), unification of user accounts and contract accounts.
Sharding

Ethereum core devs meeting 3.3.
They discussed the Ropsten Spam issue, without a clear decision about what to do. Gavin was not there, but one other Parity guy. No mention of PoA.
Regarding switch to PoS: Vitalik explained the option of a gradual switch over: initially PoS in a kind of parallel, simulated way, then hybrid with varying weights until pure PoS.
They also discussed the issue of gas cost rising with Eth price going up and if/how the gasprice should go down to compensate for it.
It became clear that there's currently no consensus on how to deal with gasprice. The difficulty is to not open the door to spam attacks when making it flexible. Currently the clients seem to implement different transaction relay policies.

#31 - 12.03.2017 18:25 - didi

Liberation of Audible audiobooks:
Prerequisites: python and ffmpeg
audible-activator retrieves the activation key (the 8 digit string printed at the end). Uses selenium to scrape the info via Chrome.
audible-converter converts the aax files to m4a files, keeping metadata (chapters and cover). It requires the activation key retrieved before as param.
audible-downloader downloads all audiobooks from the personal library, again via Selenium/Chrome. Was broken for me, managed to work around it.
Note: there's aa and aax file formats (all proprietary and with DRM). aax has higher bitrate.

#32 - 12.03.2017 21:46 - didi

Claim of Bitcoin consuming as much electricity as Ireland.
Source from 2014, with Bitcoin being at ~380€.
It claims Ireland needs ~3 GW, which is consistent with wikipedia (latest value from 2013).

Since there was a block reward halving since and bitcoin value is about 3x, power consumption is now probably ~50% higher.

The paper assumes a electricity cost of 0.10 US dollars per kWh and speculates a lot about efficiency of different mining equipments.

I think the assumed cost is way too high (see this chart and equipment efficiency isn't really relevant. What may be relevant is the cost of equipment (considering the limited amount of time it can be used efficiently). Other then that, the equation should be simple: take the lowest energy price, calculate the block reward per time according to the current exchange rate -> get the energy burned.

With 1 BTC = 1000€ there's ~ 1000€ * 12,5 * 6 = 75.000€ to be gained per hour.
With 0,04 Cent / kWh (I think mining farms may be below, but lets add something for HW cost), that puts the consumed energy at ~1,9 GW.
This assumes only rational agents and absence of speculation.
Somebody speculating on rising Bitcoin value may well mine for a slight loss. Bitcoin price and consumed power are for sure correlated, but only in the long term, as the hashpower change (or not) during the last halving showed. It's probably a bit comparable to the relation of stock prices with company performance.

#33 - 14.03.2017 11:15 - didi

Reddit thread about fiat on the Blockchain:
With discussion if Decentralized Capital is a sane approach.

#34 - 15.03.2017 17:04 - didi

Simple made easy

#35 - 15.03.2017 17:21 - didi

Fullmoon meeting at madcity:
I presented Bitcoin and Ethereum.
Met with Andi. Does some game dev as a hobby (example, was interested in using crypto tokens for games.
Andreas Zobl of [Das Lastenrad](http://das-lastenrad.at/, dustmap) was also there. TODO: visit him.

#36 - 20.03.2017 17:24 - didi

YouTube liberation:
In reference to this talk's tree metaphor at 31:34, that's what we could do:
Enhance YouTube players with the ability to (automatically) pin watched videos to IPFS and register the hash somewhere.
Could be done e.g. via a Greasemonkey script or 3rd party players like NewPipe.
Ideally, we get explicit consent of the video uploader / owner. E.g. by (semi-)automatically sending them a request whenever such a pinning occurs, such that they can give permission with a simple click. That click could trigger publishing of the hash into a public, searchable database. Voilà, decentralized YouTube.

#37 - 20.03.2017 23:20 - didi

Important argument for decentralization (inspired by this YT comment:
On a small scale, the impact of personal decisions becomes visible. This makes the decision to behave in a way more aligned with personal values even in the face of increased cost or inconvenience (but mostly it's mainly about the cognitive effort to change behaviour) easier.
Can be a powerful antidote to the widely spread "my impact is so small on the global scale it's not even worth trying" excuse.
It can also lead to a form of social pressure and thus needs to be handled carefully.

#38 - 24.03.2017 00:06 - didi

Conversation with Thomas:
lab10.coop is probably best bootstrapped with a token sale based on own projects.
What projects should this be based on? What's a good narrative? What target group should we focus?
Minebox is a positive example for a story easy to explain.

The freedombox model could be the basis for such a narrative. E.g. self own your digital identity. Restore it with a click if for whatever reason your box breaks down. Recovery based on social trust network instead of password or 3rd party delegate.
Can we add a killer use case based on ZKP?

The intermodal travel system may be bootstrappable on a local level. E.g. take a set of cities (like Graz and Vienna) and offer at least one path. For example train + bike sharing. Or car2go. This model can be extended to different region, e.g. add a set of cities in France, no need to already offer a path between the Austrian and French region. As soon as air transport is added, the critical mass threshold is much bigger.
The system needs to be open such that transport providers can attach themselves without talking to us. Needs built-in reputation system acting as quality control. Legal constraints however need to be ensured.

Private car sharing based on cooperative model: May also have huge potential.
The storyline could be: get rid of your car while keeping the advantages. What are the fears? Should there be an optional "instant guarantee"?
Should we partner with https://carsharing247.com/ or similar? Could also be good for a crowdsale. Coop tokens (the same those dedicating their cars get).

#39 - 24.03.2017 21:22 - didi

Conversation with Nejc:
Seems quite interested in the collective idea, would like to participate. Meeting currently difficult, probably on 6th.
TODO: Send him some info about what's currently going on.

Conversation with Thomas:
We should build a website for lab10.coop. Target audience: Potential members.
The site should clearly differentiate from usual ones.
We could build on some metaphors of https://ar.al/.
May be designed to challenge visitors: Issues are known, here a framework for building solutions is created. Would you help?
Yes -> proposals ranging from becoming a member to just self-educate on issues.
Example for "different" website: the VC site with cmdline interface (TODO: link).

Legal:
Tokens would qualify as currency. Schenkungssteuer when giving out. No capital tax when "sold" after > 1 year.
Alternatives: options and futures. Those have no effect on Sozialversicherung.
Tokens: How is the value determined for tax purpose? The coop may provide an Exchange which converts it to FIAT with a fixed rate. This is a kind of anchor value, not too dissimilar from the nominal value of Stammkapital (shares) of classic for profit companies. (?)
There may or may not be secondary markets trading it higher.

Options: Stiftung (in CH?), DAO (2.0).

Token sales should probably be project specific. Idea: Have caps for the project, but allow overfunding, excess capital going to the collective (not bound to the project). Allows communication to remain simple (about the specific project), but potentially leveraging attention to also learn about the underlying coop.

Model may be an intermediate thing of ICO and Kickstarter. Example Freedombox: Initially sold only for lab10 tokens. Thus investing in the project can be seen as an option for the product (on Kickstarter it's not an option, but a future), at the same time the token remains convertible. May be used for other projects or sold.
Successful ICOs don't necessarily require a dedicated Blockchain. See e.g. Ethereum based Tokens. Mostly App tokens, but not only (->DAO).

Idea: Patenschaft (sponsorship/mentorship) of specific projects. Candidate projects are nicely presented and explained. Outsiders are invited to "adopt" them. Can e.g. imply financing and being a public mentor of the project. May be attractive for wealthy / high profile people with motivations beyond wealth increase.

Slogan for the coop: Rebuilding from the bottom up.

#40 - 03.04.2017 22:28 - didi

Flash thought while browsing bountysource.com (similar one: commiteth.com):
Pro: (open source) devs get paid for useful contributions. Lowers pressure to earn money in other ways.
Con: Economic incentive undermines intrinsic motivation (citation needed, but not hard to find)

Probably "solvable" by cognitively decoupling the devs from the bounties. E.g. hide explicit mentions of value and currency. The bounty may still influence the order of listings and probably be expressed visually (e.g. color gradients visualizing the value of the bounty). Similarly, payouts should not require any explicit action of devs. The should just stick to their normal workflow, as if there were no bounty. Some kind of community process may ensure that this isn't abused by those offering bounties (and not paying them out as promised).
It may be abstracted even further e.g. by a platform not doing per issue payout, but doing bookkeeping in the background and periodically paying out contributors, keeping payout amount and solved issues correlated in the mid and long term.

#41 - 06.04.2017 20:17 - didi

Ropsten had a revival - ropsten.etherscan.io.

Aragon (*unstoppable companies*) published Alpha 0.3 - featuring *bring your own token*. Found in Rchain's Slack channel community governance - quoting jimscarver: *This looks like a gold mine for rchain governance. They have done a good part of what divvy has been planning. There are other governance contracts I am reviewing but these look great so far as a potential bases for the rchain community governance.*

RChain uses a special kind of namespace logic (ex nihilo logic) for allowing a kind of sharding with arbitrary strength (subset of nodes). Rhchain architecture doc.

Differential privacy allows to really anonymize datasets (in contrast to pseudonymization) before handing them out e.g. for research. This is achieved by randomizing part of the data (e.g. 25%). That makes it much more difficult to de-anonymize individuals while keeping retaining the possibility to derive meaningful statistical information (the error introduced reduces accuracy, but not the results itself if calculated properly).

#42 - 08.04.2017 19:48 - didi

Identity

Definitions from Wikipedia:
We start from an *entity*, which is for example a physical person. An entity can have several identities, e.g. an account in an online shop, an account in a online game. An identity is composed of a set of (personalized) attributes. An identity usually belongs to a single entity. Seeviz.
It's normal for an entity to have multiple identities, online and also offline (e.g. driver's license, bank account, ...).
Attributes can be known, unknown, permanent (e.g. DNA) or mutable (e.g. hair color).
Identities are often correlated to rights, obligations, permissions.
Companies often think in terms of *Identity management architecture* (IMA), which can also include aspects like automatic provisioning of permissions based on a role, single sign on etc.

From en wiki:
In IT, the topic is also known as *Identity and access management* (IAM).

#43 - 12.04.2017 23:03 - didi

Qtum:
Tech Whitepaper
They are dishonest when writing that Ethereum has no light wallet and not mentioning the Raiden network.
... aims at producing a variation of Bitcoin with Ethereum Virtual Machine (EVM) compatibility.
Claims that the Ethereum account model poses a scalability bottleneck.
For context, Vitalik's thoughts about UTXO vs Accounts: link.
Short summary:

- UTXO has indeed potential scalablity advantages due to possible parallel execution of transactions
- Doing stateful (as in most smart contracts) transactions is very complicated
- Ethereum may one day support both models with currency abstraction

They want to start from a Bitcoin fork.

#44 - 12.04.2017 23:07 - didi

Quick test of Qubes OS 3.2:
I installed it on a T410s. Needed to disable VT-d (in BIOS) in order to get the graphical installer working (context. Without VT-d, networking isn't isolated, which slightly degrades security.

Couldn't figure out how to connect to a WiFi. Ethernet worked immediately.
Browsing showed a bit of scroll lagging. Otherwise performance seemed ok.
Audio working. Didn't try USB.
YouTube video can't be full-screened (trying so somehow broke the window rendering).

#45 - 13.04.2017 02:13 - didi

The IP of h1 (5.9.14.80) was listed on Spamhouse: https://www.spamhaus.org/query/ip/5.9.14.80 in the CBL list.
Hetzner notified me about it.

Was easy to remove.
However I'm not sure what triggered it. Looking at the mail logs:

```
Apr 13 02:05:30 redmine postfix/smtp[31280]: BB71C1005F5: to=<didi@d10r.net>, relay=in1-smtp.messagingengine.com[66.111.4.74]:25, delay=106, delays=0.15/0/106/0, dsn=4.0.0, status=deferred (host in1-smtp.messagingengine.com[66.111.4.74] refused to talk to me: 421 Client host [5.9.14.80] blocked using internal list; Mutating HELO parameter, use a consistent one. Expected removal in 5.6 days)
```

So, Fastmail still refuses to accept the mail. Looks like it doesn't like changing domains for the same IP, which is to may knowledge not forbidden by the spec.

And:

```
Apr 10 08:36:55 redmine postfix/smtp[29683]: 0CB7F100038: to=<thomas.zeinzinger@optinna.com>, relay=optinna-com.mail.protection.outlook.com[213.199.154.170]:25, delay=5.6, delays=0.18/0.01/0.18/5.2, dsn=5.7.1, status=bounced (host optinna-com.mail.protection.outlook.com[213.199.154.170] said: 550 5.7.1 Service unavailable, Client host [5.9.14.80] blocked using Spamhaus. To request removal from this list see http://www.spamhaus.org/lookup.lasso (AS16012611) [DB5EUR01FT033.eop-EUR01.prod.protection.outlook.com] (in reply to RCPT TO command))
```

In March, Fastmail reported this:

```
Mar 21 16:00:37 redmine postfix/smtp[2484]: 7FDAE100027: host in1-smtp.messagingengine.com[66.111.4.75] refused to talk to me: 451 4.7.1 <redmine.d10r.net>: Helo command rejected: Too many different HELO strings from this IP (7 > 6), try again and use consistent HELO strings
```

So, always using lab10.io as sender domain may fix this.

I added an SPF DNS (* TXT) record for lab10: "v=spf1 a ptr". Which allows all IPs for all subdomains which match.

Still unsure that triggered the entry in spam blacklist. Did Fastmail report this?
Opened a ticket with them.

Tool for constructing SPF record: http://www.spfwizard.net/
Tool for analyzing SPF entry of domain: https://mxtoolbox.com/spf.aspx

#46 - 13.04.2017 03:29 - didi

gitlab install according to this guide.
Proxied through h1 as usual.

Many settings are in https://code.lab10.io/admin/application_settings (I couldn't figure out how to navigate there through the UI).

Normal workflow when changing a config outside UI:
Edit /etc/gitlab/gitlab.rb
Run gitlab-ctl reconfigure.
Afterwards it seems to frequently happen that a service is down.
Check with gitlab-ctl status, start all with gitlab-ctl once.

Info about CI

#47 - 13.04.2017 03:36 - didi

sovrin is a blockchain focused on identity.
Here is a brief comparison with uPort.
It's based on the DID spec (also used by uPort).

Announcement by the Foundation president (who also wrote the book Digital Identity.

Uses the evernym ledger.

Context:

- #37-42
- http://www.weboftrust.info/papers.html
- https://en.wikipedia.org/wiki/Identity_management
- https://de.wikipedia.org/wiki/PRIME
- https://de.wikipedia.org/wiki/FIDIS

#48 - 20.04.2017 00:02 - didi

Gitlab intro

Was initially developed using Ruby, later switch to Go (now mixed codebase).

Code chances are usually applied using **merge requests**.
Those are collaborative and offer a lot of interactivity. E.g. possibility to comment specific lines of code.
Permissions configurable per branch. E.g. protected branches may allow only approved merge requests.

The free tier (see comparison has most features we're interested in.
Missing: LDAP, advanced issue management (e.g. . Those are in Enterprise Starter ($3.25 per user per month).
The Enterprise versions are focused on process features and support.

CI is integrated via the **Pipeline** module.
Defined in file .gitlab-ci.yml in root dir of a repo (can differ by branch).

Contains:
Jobs:

- collection of tasks
- independent / parallelizable
- can expose artifacts Stages:
- defined at the top of the .gitlab-ci config file
- jobs are assigned to stages, all jobs of a stage are run in parallel
- next stage starts after all jobs of prev stage finished

Runners are defined by URL. It should be possible to have runners behind NAT as they can initiate a connection to the gitlab server.

Integrated **Mattermost**. Integrates neatly (similar to Slack).

Supports *Smart commits* with integrated Issue Tracker.

Sonarqube integration should be possible

Issues
reordering in cardboard view now possible
no nesting
no direct relations (but mention in comment)
no "blocked by"
labels, otherwise flat structure
has filtering
ordering?
no (/rudimentary) time tracking
no cloning

Snippets (gists)

github integration:
import into gitlab possible
keeping in sync not
push to github possible via pipeline

TODO: True that gitlab allows only one repo per project?

#49 - 20.04.2017 00:12 - didi

About federated identity. Complicated shit. Time to get rid of it.

#50 - 26.04.2017 09:30 - didi

https://theinformationageblog.wordpress.com/2017/02/21/elastico-a-new-scalable-blockchain-protocol-proposal/
Elastico by National University of Singapore

TODO...

#51 - 26.04.2017 10:05 - didi

About micro finance: The Antinomies of 'Financial Inclusion': Debt, Distress and the Workings of

The dichotomies of financial inclusion/exclusion and formal/informal finance doesn't hold on a closer look.
The paper examines the *2010 Andhra Pradesh microfinance crisis* and shows how microfinance initiatives can lead to outcomes such as predatory lending, redistribution from the poor to the rich etc.

#52 - 26.04.2017 10:31 - didi

I started reading (more exactly: listening to Ayn Rand.
Anthem:
Essentially society collapses due to collectivist behaviour and descends into a new dark age, with most skills (including handling electricity) are lost.
The words *I*, *my*, *mine* are forgotten / banned. The main character / narrator references itself as *we*.
It ends with the protagonist escaping, finding a house from the sunken civilization and re-discovering the mentioned words in books.

The story is an endless damnation of collectivism and praise of individualism.

Related:
Classification of social behaviours
Most interesting finding for me: Altruism is inverted Egoism.

#53 - 26.04.2017 10:58 - didi

About insect brains
Intelligence not so much dependent on brain size, but on connections. Ants are especially interesting (as already observed by Darwin).

#54 - 26.04.2017 13:15 - didi

Linuxtage talk
Example: ccc.
Under the hood: Ethereum: Gas concept, VM, create token.

#55 - 29.04.2017 10:37 - didi

About alternative currencies:

- http://www.fairventure.de/infothek/item/203-margrit-kennedy-zukunft-geld
- http://monneta.org/

#56 - 03.05.2017 12:53 - didi

Hint from epigenetics:
Early life (-1 - 1 year) circumstances act as a kind of genetic configuration.
Default trust level is also affected. In a friendlier environment, more trust makes sense (cooperative game theory).
Probably the past decades of high living standard (at least in parts of the world) led to a population configured for high default trust and thus high vulnerability in non-cooperative environments - may be somewhat related to the Snowflake phenomena.

#57 - 05.05.2017 14:46 - didi

About filter bubbles: https://mobile.nytimes.com/2017/03/03/arts/the-battle-over-your-political-bubble.html

#58 - 15.05.2017 16:47 - didi

Sonnengeld

Fixe Menge
Narrativ: Geldmenge = nachhaltig produzierte (oder produzierbare?) Energie
Problem Hayek-Geld: Lässt sich nicht auf Marktweg in Umlauf bringen.
Ähnlich Solarcoin (aber darüber hinausgehend): Schöpfung durch Produktion von regenerativer Energie

#59 - 22.05.2017 10:34 - didi

Vitalik about coordination problems as a tool:
This is the essence of engineering decentralized instutitions: it is about strategically using coordination problems to ensure that systems continue to satisfy certain desired properties.

Two levels of *light clients*:
1) (Almost) guarantee to be on the right (e.g. heaviest) chain. Specific details state can be checked via Merkle trees.
2) *Nearly fully verifying*: Additionally checks that rules are followed. Works in combination with fishermen - a kind of whistleblowers which broadcast *fraud proofs* if they see something fishy going on. The concept (by Gavin) was first mentioned here and is explained in greater detail in the Polkadot Paper (section 4.4).

#60 - 22.05.2017 11:04 - didi

Consensus algos

Casper (source):
Deposit + penalty based PoS.
Anyone can join as validator by submitting a deposit.
Hybrid design:
Every 100th block is a checkpoint.
Active validators can send *prepare* and *commit* messages on checkpoints.

> = 2/3 commits mean *finalized*.

Slashing conditions: if doing something it shouldn't, a validator gets deposits deleted.
Hybrid fork choice rule:
a) prefer finalized checkpoints
b) prefer checkpoints that are close to being finalized (2/3 prepares, some commits)
c) take PoW longest chain

Dynamic validator sets:

After leaving, a validator needs to wait for 4 months until deposit recovery

Impl:
Casper contract
Standalone daemon (python) work in progress

#61 - 22.05.2017 12:05 - didi

Algorand
Paper Reddit
Cryptographic sortition.

Video: Fast and furious byzantine agreement.
Agreement, Consistency.
Comms model: Complete syncrhronous network
complete: (fixed number of participants)
Synch: Rounds

Adversarial Model:
infinite computing power
can currupt
controls and coordinates all bad players
sees all messages

Old goads:
Byzantine Agreement with O(n) bad players and (1) rounds
Theorem: you need t+1 rounds to get rid of t bad players deterministically
Ben-Or: O(sqrt(n)) bad plyers in O(1) rounds probabilistically
Rabin:n/4 bad players in expected O(1) rounds via a common coin provided by an external trusted party
...
Feldman Micali: n/3 bad players in expected O(1) rounds via a (very) complex protocol

Today: Cryptographic BA with < n/3 bad players in expected 6 trivial rounds
Assumption: every player i has a public key PKi for a VRF (?).
There is a random string R independent of PKi's.
Signature is deterministic.
Random oracle: H(SIGi(m)) unique random string for i and m

Rounds:
Qr = H(R,r)
At each round there is a quantity that is unique to that round and random.
Exchange of message:
Receive br-1, send br
Goal: After every message there's probability of >= 1/3 of agreement (if not already the case at start of round)
Once in agreement, it's stable

Receive: br-1 and SIGj(Qr) from each *willing* j (willing: probably only good players)
Local decision:
If #(0) > 2n/3 then br = 0
If #(1) > 2n/3 then br = 1
Else hash the signatures, select the smallest one: randr = min H(SIGj(Qr)). Then take the lsb of it: br = lsb(randr)
Send br

Effect of the else branch:
The player didn't receive a 2/3 majority. Thus "randomly" selects one of the received signatures and takes the last bit.

Player replaceability: if you shoot people, it still works.

#62 - 29.05.2017 20:28 - didi

About **Casper** from its Gitter channel:
Validators need to register for staking, requires an ETH deposit.
In order to allow nodes not online 24/7 to participate, there's a login/logout mechanism (sending a message). The logged in state is stored in the state (1 bit per validator and block if I understand correctly).
If logged in and not participating, there's a slight penalty. That's implemented with a negative interest rate (probably 8% annually) which is applied to all deposits by default.
An *epoch* is 100 blocks (~23 mins).

Both Algorand and the dfinity BLS are mentioned and discussed.
Mindmap

Vitalik is working on a new doc on Casper: link

In discussion: validator set is determined by auction (cheapest validators are selected).
Validator set doesn't change frequently. Light clients know it.
Validator selection for block creation round robin or prescribed partial order.

Timing candidates:
~6s per block, ~6m per epoch.

I wonder: isn't it easy to (D)DoS the validator supposed to create the next block?

#63 - 07.06.2017 16:29 - didi

Stratis
A Bitcoin implementation in C#. Plan to switch from PoW to PoS (source).
Qt Wallet (fork of a fork of the Novacoin wallet).
Focused on presenting to the business community with focus on .NET / C#.
See use cases.

#64 - 30.06.2017 14:29 - didi

On ICOs:
Epicenter episode (covers Bancor and other recent ones)
Coinlist - an approach to be Sec compliant, will be first used for the Filecoin (IPFS) ICO. Forbes article.
Vitalik's Opinion

Continuous token model - PoC implementation "Ethernalsale"

#65 - 12.07.2017 20:47 - didi

Resources about cooperation:

http://isites.harvard.edu/fs/docs/icb.topic426436.files/five_rules.pdf
https://en.wikipedia.org/wiki/The_Evolution_of_Cooperation
https://en.wikipedia.org/wiki/Competitive_altruism

#66 - 14.07.2017 02:03 - didi

Solidity:

https://github.com/ConsenSys/smart-contract-best-practices