encointer - An Ecological, Egalitarian and Private Cryptocurrency and Self-Sovereign Identity System

Alain Brenzikofer
alain@encointer.org

***Abstract*—*encointer* proposes a new blockchain based cryptocurrency with an ecological consensus mechanism using trusted execution environments and an egalitarian money supply policy where money issuance is done by individuals attending randomized pseudonym key signing events.**

***Index Terms*—cryptocurrency, macroeconomics, identity management, location awareness, privacy, energy efficiency**

I. Motivation

A. Economics

With the appearance of Bitcoin [1] in 2008, a big socio-economic experiment took off. The nature of money itself was widely debated. Bitcoin adopts a hard-coded nominally inflatonary monetary policy saturating at a fixed supply. Rapid adoption made Bitcoin a real deflationary currency, which it will remain if successful. Early adopters made a fortune. Because of its deflationary nature, bitcoin favors accumulation of capital for the few. Wealth increases without work.

The monetary policy followed by central banks issuing national fiat money on the other hand often follows the goal of price stability, aiming at a moderate inflation goal in the order of 1-2%. Issuance of money is appointed to banks who give credit to companies who employ workers who consume goods and thereby make companies profitable and raise the GDP. A process that alledgedly benefits everyone. As Thomas Piketty shows in [20], it doesn't benefit every one equally.

encointer aims at turning this logic upside-down and issue money where humans provably do an effort as opposed to where the capital already is. The provable effort a person has to make to benefit from *encointer* issuance is attending to pseudonym key signing parties that happen at regular intervals at high sun all over the world within small randomized groups of people [2]. The *encointer* issuance therefore represents a global *conditional* basic income for every person attending the key signing event. It is not to be confused with helicopter money which distributes money *unconditionally*.

These *encointer* ceremonies are at the same time the basis of a self-sovereign identity claim of individuality (SSICI): One person can only maintain one individuality claim because ceremonies are designed to make it impossible to attend two ceremonies physically as they happen in different places concurrently. SSICI supports the standard for decentralized self-sovereign identity defined in [3].

B. Unpermissioned Consensus

Bitcoin and many other cryptocurrencies use an energy-hungry consensus mechanism called proof of work (PoW). While PoW has been the key idea that made Bitcoin possible in the first place, it is not ecologically sustainable. Moreover, it failed it's goal of decentralization as mining has become centralized by a single company in a single country.

Peercoin [4] introduced the first proof-of-stake (PoS) cryptocurrency in 2012. Until today, PoS is not academically respected as a sound consensus mechanism [5]. While PoW makes a compromise on energy efficiency, PoS makes the compromise of benefitting the rent-seeking wealthy.

Accepting that there's always a compromise to make, *encointer* introduces dPoET; a permissionless version of proof-of-elapsed-time (PoET) [6], relying on trusted execution environments (TEE). PoET requires trust in vendor attestation services. Currently, there are few TEE vendors on the market (i.e. Intel SGX [7], ARM trust zone [8] used by AMD, Qualcomm and others) but there are also open-source hardware initiatives that might one day diversify the attestation trust.

C. Private Smart Contracts

In 2015 Ethereum [15] was introduced, bringing turing-complete smart contracts to the blockchain. Ethereum now serves as a platform for many decentralized applications (DApps) and has become the major ecosystem for ICO's. While enabling publicly verifyable smart contracts, there is no way to process private data on Ethereum in trustless manner. Public unpermissioned validation of smart contracts is only possible with a minimum of public inputs. Support for zk-SNARKS has been added to the etheremun virtual machine with the metropolis hard-fork, yet this only enables to verify zero knowledge proofs that have been generated off-chain. It is therefore possible to hide the payload of a smart contract call, but as you have to call the contract by means of a public transaction, your pseudonym is leaking. Quorum [16], an Ethereum fork, approaches privacy by delegating smart contract validation to a small group of permissioned validators using a BFT consensus and allowing Zcash-style shielded transactions to hide your pseudonym when calling a private smart contract. Such setups do not allow GDPR-compliant [17] DApps. The reasoning is the following: In order for the DApp to comply with GDPR, the Dapp has to be run by a single operator having users opting into his privacy terms. The operator would then have to run all private contract validators by himself. Such centralization would render the use of blockchain meaningless.

encointer enables private, decentralized DApps. As the internal state of a TEE is not leaking, they offer a way to run

smart contracts with private, encrypted inputs while still offering verifyability. This has been demonstrated by Hyperledger Sawtooth Private Data Objects (PDO) [18]. PDO's allow to take state and execution of smart contracts off chain, thereby also improving scalability as compared to Ethereum.

D. Transaction Privacy

Bitcoin transactions are pseudonymous but not anonymous. It has been shown that identities of transacting parties can be revealed [21]. Aiming at transaction privacy, Monero was introduced in 2014, employing the CryptoNote protocol [10]. Receiving funds in Monero means scanning every block for transactions to oneself. This task can only be taken out by full nodes as delegating it would leak private information.

Zcash was introduced in 2016 empoying the Zerocash protocol [12] using zk-SNARKS to hide sender, receiver and value from third parties. Generating SNARKS to send funds is a computationally heavy process, limiting its usability for mobile and IoT devices.

For both Monero and ZCash, privacy comes at the price of large transaction size, letting the blockchain grow quickly. Beeing equipped with private smart contracts using PDO [18], *encointer* only stores tx hashes onchain.

E. Scalability

Because of it's block size limit, Bitcoin can only reach about 4-7 transactions per second onchain. In order to tackle Bitcoin's scalability issues, Lightning Network payment channels [13] were introduced in 2015 and demonstrated in 2017. Scalability is achieved by bilaterally treating transactions off-chain with the option to settle the last balance at any time on-chain. Teechan [14] was introduced in 2017, implementing payment channels in TEE's.

encointer takes transactions and smart contract execution off-chain altogether. Only one hash per transaction and per contract state change must be stored onchain. The latest state is shared among validators but only the hash of that state needs to be onchain. This improves scalability by an order of magnitude and delays the need for second layer solutions. If needed, a solution similar to Teechan would fit well into the *encointer* concept as a payment channel solution.

F. Governance

Decentralized blockchain governance has in the past been tried by various means. In the case of Bitcoin, a balance of power bewteen miners and coin holders decides about the future of the protocol, which lead to multiple chain forks in the past, hurting the ecosystem and dividing development teams.

PoS blockchains delegate governance to their whales. Who has more coin has more say. This poses a conflict of interest i.e. in the case of deciding the future nominal inflation.

As *encointer* has an anti-sybil attack measure in place (SSICI), a one-person-one-vote (1p1v) scheme could be implemented. However, there is a conflict of interest as well because low-wealth individuals are expected to vote in favor of higher inflation as they directly benefit in the short term due to their role as money issuers in *encointer* .

encointer suggests a novel approach to blockchain governance, delegating blockchain governance to a swiss cooperative holding the *encointer* trademark. Cooperative membership is open to anyone staking the equivalent of X CHF. The cooperative suggests protocol updates in advance, including changes of nominal inflation rate, tx tax burn rate, block size limit. Suggestions by the cooperative can be blocked by a referendum vote requiring a majority of 2/3 of stake and 2/3 majority of 1p1v voters. Balloting happens onchain anonymously. The 2/3 majority threshold for referendums allows the cooperative to react quickly to changing circumstances but still provide decentralization, given large opposition.

If the *encointer* cooperative should fail to suggest necessary changes, the community may suggest changes as well. They also require a majority of 2/3 of stake and 2/3 majority of 1p1v voters.

II. Monetary Policy

Unlike Bitcoin, *encointer* doesn't have a hard-capped supply. The more people are joining the ecosystem, the more money is issued. The value of one *encointer* is therefore tied to the willingness of people to spend time to attend key signing parties. As median wages vary greatly between nations but *encointer* is a global unit of account, it is expected and intended that ceremonies are more economically attractive to attend in low-wage countries. Also, the possibility of obtaining a digital identity might be especially beneficial in developing countries where people might own a mobile phone but not a state-issued ID.

Nominally deflationary factors are

- loss of private key or password necessary to unlock funds
- party deposits burned because of no-show

The total coin supply $M0$ after K parties with N_i total participants for party i can be expressed as

$$M0 = \sum_{i=0}^{K} N_i - T \cdot b - D \tag{1}$$

where T is the total value transacted and b is the tx tax (being burned). D being the total of burned party deposits.

Exponential community growth causes exponential growth of money supply. If community participation should one day saturate, money issuance will be constant and inflation rate will therefore decrease over time.

With such a policy in place, no early adoper should expect to get rich by hoarding *encointer* as adoption drives inflation.

III. Ceremonies

A. Preparation

Key signing ceremonies will be scheduled every 42 days and will happen at high sun. At least 24h in advance, participant a creates a registration transaction for ceremony i containing

$K_{a,i}^{pub}$	one-time public key derived from his/her DID
$S_{s,j}$	a ring signature proving ceremony $j < i$ was attended with group s last time. The ring consisting of all participants of ceremony j at location $L_{s,j}$.

$L'_{a,i}$	his/her anticipated approximate position as a geohash [19]
$r_{a,i}$	acceptable distance range to meetingpoint in [km]
$n^{min}_{a,i}$	minimum number of counterparties
$d_{a,i}$	minimum deposit for counterparties
$S(tx)$	a deposit in *encointer* to be redeemed after attendance

The system then tries to find randomized matching counterparties. A ceremony can take place if all of the following conditions are met:

- at least 3 attendees with overlapping acceptable range
- at least 2/3 of all participants haven't met at the last ceremony already

24h before the ceremony, the system defines the location anchors $\hat{L}_{s,i}$ for all groups s. It will maximize the distance between any two location anchors subject to individual acceptable ranges. The group is then free to agree on any meeting place $L_{s,i}$ within a range and a tolerance range $r_{s,i}$ by setting up a private chat provided by the *encointer* app. Meeting time $T_{s,i}$ is set precisely to high sun for $\hat{L}_{s,i}$ longitude.

No ceremonies with more than 10 people will be scheduled to make sure every attendee can remember who he/she already signed with.

B. Ceremony Procedure

Key signing must begin within $\Delta t_{s,i}$ after $T_{s,i}$. No latecomers may be accepted.

$$\Delta t_{s,i} = \frac{min\left(dist\left(L_{s,i}, Lk, i\right)\right)}{v_{max}} \forall k \in S \tag{2}$$

Where $v_{max} = 300km/h$ is a *encointer* parameter set to make it impractical to attend two adjacent ceremonies, even when using a helicopter.

Attendees attest the physical presence of all counterparties with their own reputation.

C. Ceremony Scalability

The most densely inhabitated city is Manila with $43'000/km^2$ [25]. With a limit of 10 people per ceremony and a participation of 100% , 4300 ceremonies would take place per km^2. Each ceremony would be allowed an area of $232m^2$ and the tolerance range would be $r_{s,i} \approx 15m$. This is impractical as such a small range might be inaccessible to the public. $\delta_T s, i$ would be as low as $180ms$, which is achievable by automated witnessing over i.e. bluetooth. To avoid trespassing attempts, a group s may file a relocation request with $\hat{L}'_{s,i}$ signed by at least 2/3 of members in s.

D. Claim of Individuality

Attending one ceremony supplies the individual with a proof-of-personhood. It doesn't prove that one individual maintains exactly one id. More than half of all ceremonies must be attended in order to get a valid SSICI claim and be eligible for coin issuance

E. Attacks and Mitigation

1) Illegit Videoconference: People may try to meet virtually instead of physically.

2) Surrogates: An adversary might pay other people to attend ceremonies on behalf of identities controlled by the adversary. The effect is similar to people renting out their identity. This can't be prevented by means of a pseudonym party.

3) Social Engineering: Attendees might talk others into signing more than one pseudonym. Bribery could happen too.

4) Systematic No-Show: a meeting might become invalid if too many participants don't show up. No shows are punished by burning the deposit.

5) Threats to Personal Safety: As ceremony members need to meet in person, all risks involved with human encounters apply. These risks are reduced by randomizing participants and by the minimal group size of 3 persons. Participants are advised to choose public places for ceremonies. Threats by non-participants who want to hurt the *encointer* ecosystem are mitigated if group s keeps their exact meeting point private.

F. mutual-signing off-shore bot communities

The above rules allow many unconnected communities to grow independently all over the world which accelerates adoption. This opens an attack vector of an adversary creating virtual communities in the middle of the pacific where no real person will likely ever show up. In order to disincentivize self-signing bot communities, ceremony rewards are frozen until isolated community members join the genesis community. It might still be necessary to combine this graph-theoretical measure with additional proofs of personhood taken out during the ceremony, like live chat Turing tests with participants of other ceremonies.

IV. dPoET Consensus

The major technical innovation of Bitcoin is its use of PoW to avoid double spends in a decentralized digital cash scheme. The higher the cost of a double spend attack, the more secure the Bitcoin blockchain. The security of Bitcoin relies on mining power. Miners invest in infrastructure and energy as long as this remains profitable. Mining power therefore depends on the real value of miner income being proportional to Bitcoin exchange rate.

PoS blockchain security on the other hand relies on game theory. Gaining control over the majority of stake to attack a PoS chain would destroy the real value of that stake, hurting the attacker most. PoS blockchain security therefore is proportional to its total market capitalization. A yet unsolved issue with PoS is the *nothing-at-stake* dilemma [5] which may cause uncontrollable forks.

PoET has similar security properties like PoW as it is just an energy-efficient replacement for PoW to elect the validator who may write the next block to the blockchain. Each validator TEE samples a uniform random number $u \in [0..1)$ and waits for an exponentially distributed wait time defined by:

$$t = -\frac{ln(1-u)}{\lambda} \tag{3}$$

λ has to be adjusted to validator population size to reach a defined average block time, similar to Bitcoin's difficulty adjustment.

Everyone with a supported TEE hardware can join the validator set and gets equal probability of being selected to generate the next block. Therefore, the 51% (double spend) attack applies to PoET as well. The difference is just that it's not 51% of PoW mining power but 51% of TEE devices in the network.

encointer makes such an attack very expensive by demanding that every validator must be linked to a unique person. Every person may run at most one validator.

Each *encointer* validator node waits a random time before generating a new block according to PoET. It then assembles transactions into a block including a PoET and broadcasts the block to the network.

In bitcoin, all nodes believe in the blockchain accumulating the most PoW since genesis. In *encointer* , nodes believe in the blockchain accumulating the highest PoET difficulty $\sum_i \frac{1}{\lambda_i}$. We call this consensus algorithm *democratic proof of elapsed time* (dPoET)

A. Settlement Finality

Like PoW, dPoET only delivers probabilistic transaction finality.

V. Trusted Execution Environment Security

TEE's aim to provide the necessary guarantees for secure remote computation. They should provide integrity and confidentiality guarantees when executing software on a computer maintained by an untrusted party. The most recent TEE's rely on software attestation, a process that guarantees the user that she's communicating with a known piece of code running inside a secure container inside a genuine trusted hardware by means of a manufacturer signature.

As criticized in [7], manufacturers seem to follow a security by obscurity principle not disclosing design internals necessary for a proper security review. Their *in dubio contra reum* analysis of Intel SGX shows vulnerabilities to cache timing and sidechannel attacks. ARM TrustZone on the other hand is only an IP core and design details are left to the manufacturer, equally reluctant to disclose details.

Since at least the post-Snowden era, one also has to be concerned about manufacturers being forced by their state to introduce deliberate backdoors. Even if open-source CPUs like OpenPower [24] might soon feature TEE's, one would still have to trust the manufacturer not to tamper with the design.

While all this is disturbing, it should be put in perspective. Information security is a never-ending race. All blockchain solutions are software running by large part on Intel CPU's. While hardware wallets may give us some comfort concerning our funds private keys, there's no guarantee on confidentiality when considering sidechannel attacks.

The *encointer* cooperative will follow developments closely and maintain an up to date list of accepted TEE manufacturers' attestation keys. Even if the author is not satisfied with today's TEE's security guarantees, he considers the ecological downsides of PoW to be much more severe for society as a whole and therefore proposes to make heavy use of TEE's for *encointer* .

VI. Proportional Transaction Fees

Bitcoin transactions may pay a fee to the miner including the transaction in his block. Because Bitcoin has a hard cap on block size, a market develops for fees and miners choose the best-paying transactions to fill a block. This effect prevents micropayments undermining adoption in developing countries. While IOTA [22] and Nano [23] have zero transaction fees they must use a small PoW as a measure against spam transactions. Even though small, PoW limits the possibilities to use mobile or IoT devices to send transactions.

encointer suggests yet another way: Each transaction must show a PoET of 0.5 seconds as an anti-spam measure. Nowadays, even mobile devices feature a TEE and are therefore able to provide a PoET. Requiring a TEE to send transactions comes with a nice side benefit: The TEE can be used as a hardware wallet for private keys, effectively mitigating the weakest link in blockchain security by solving the safekeeping of private keys for hot wallets.

Still, validator nodes need an incentive for *encointer* to benefit from a large decentralized network of validators. In the spirit of the Tobin Tax [9] it seems beneficial to the *encointer* ecosystem to charge a proportional transaction fee in the order of 0.1% to incentivize validator nodes to process transactions. In the presence of indirect block size limitations like TEE memory size, a proportional fee may still inhibit micropayments as validators might select high-value transactions with priority. That is left to be solved when we get there.

encointer targets a balance of power among multiple TEE vendors as it is unlikely that different vendors collude or show the same vulnerabilities. Such a balance of power must be incentivized in order to take place. One possible incentive would be to burn a fraction of tx fees that is proportional to the network share of the validor's TEE's vendor. Minority TEE's would earn more fees than majority TEE's.

VII. Privacy

A. Private Transactions

Private transactions in *encointer* are based on the idea of Hyperledger Sawtooth's *Private Data Objects* [18]. Fig 1 shows how transactions are processed in encrypted form. Alice creates a transaction to Bob and encrypts it with the shared verifier key K_V^{pub}. She then appends a PoET P_{ET} and sends the tx to the network. If her device has no TEE, she can delegate the PoET to any third party, whereby she only shares the encrypted tx with the PoET provider.

The validator retrieves the most recent $state_{t-1}$ (i.e. from IPFS [26]), assembles transactions from its mempool and sends everything to its TEE. The TEE is able to dectypt the data to process the clearing. It then writes hashes of a transaction to the new block together with the hash of the encrypted new $state_t$ and a signature, proving which validator

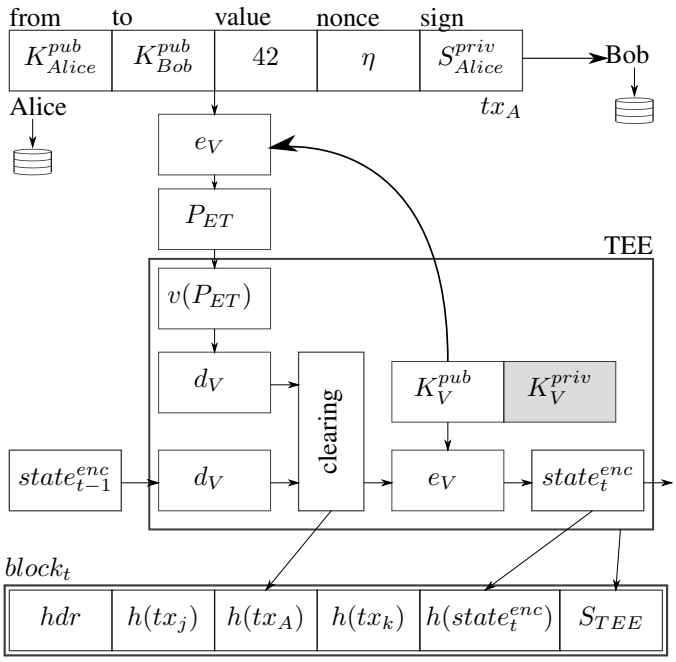

Fig. 1. simplified private transaction scheme

created the block. The new block only contains hashes, so no private information is leaking.

In order for Bob to know he received funds, Alice sends him the plaintext tx_A over a private messaging channel. Bob can then hash it and scan the blockchain for $h(tx_A)$. Both Alice and Bob then must make sure to store tx_A securely and redundantly as they can't retrieve their wallet balance by scanning the blockchain.

The shared private key K^{priv}_V is known to all registered validators. Whenever the validator set changes, a new key K^{priv}_V has to be established among all validators' TEEs.

B. Private Smart Contracts

The concept of private transactions explained above can be extended to allow private execution of generic smart contracts.

In order to

VIII. *encointer* Cooperative

encointer cooperative is a not-for-profit cooperative under swiss law. Its purpose is to govern the *encointer* ecosystem. It fulfills the following tasks

- community bootstrapping
- protocol updates
- define tx tax rate
- maintain list of accepted TEE attestation service keys

All changes are subject to a referendum by the community.

A. Community Bootstrapping

In order to establish liquidity and value for the *encointer* token quickly, *encointer* will run a one-way exchange allowing users to exchange their *encointer* for some established cryptocurrency tbd.A minimum ceremony participation of 2 out of the last 3 will be required. The exchange will be funded with a tbd amount per ceremony by the *encointer* cooperative, funded by donations. The amount you get per *encointer* depends on how many *encointer* will be traded.

To bootstrap a community in a new region, a minimum of 9 participants is needed because of ceremony rules defined in III-A.

IX. Conclusion

A novel cryptocurrency system has been introduced in conceptual detail. Main contributions are

- A new definition of trustless pseudonym key signing parties incentivized by *encointer* tokens.
- A novel consensus algorithm dPoET, combining PoET with a self-sovereign identity claim of individuality (SSICI) to achieve decentralization of power by ecological means
- A novel global egalitarian approach to monetary policy

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf, 2008

[2] Bryan Ford. Pseudonym Parties: An Offline Foundation for Online Accountability, 2008

[3] K. Wagner, B. Nmethi, E. Renieris, P. Lang, E. Brunet, E. Holst. Self-sovereign Identity: A position paper on blockchain enabled identity and the road ahead, https://www.bundesblock.de/wp-content/uploads/2018/10/ssi-paper.pdf, 2018

[4] Sunny King, Scott Nadal. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012

[5] Andrew Poelstra. "Distributed Consensus from Proof of Stake is Impossible"

[6] Hyperledger. PoET 1.0 Specification. https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html

[7] V. Costan S. Devadas. Intel SGX Explained. Tech. rep., Cryptology ePrint Archive, 2016.

[8] Introducing ARM TrustZone. https://developer.arm.com/technologies/trustzone

[9] J. Tobin. The New Economics One Decade Older. The Eliot Janeway Lectures on Historical Economics in Honour of Joseph Schumpeter, Princeton University Press, 1972

[10] Nicolas van Saberhagen, CryptoNote v 2.0, https://cryptonote.org/whitepaper.pdf, 2014

[11] B. Bnz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, Greg Maxwell. Bulletproofs: Short Proofs for Confidential Transactions and More, IEEE S&P 2018

[12] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin, proceedings of the IEEE Symposium on Security & Privacy (Oakland) 2014, 459-474, IEEE, 2014

[13] Poon, Joseph. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, 2015

[14] J. Lind, I. Eyal, P. Pietzuch, E. Gn Sirer. Teechan: Payment Channels Using Trusted Execution Environments

[15] Vitalik Buterin, Gavin Wood, Joseph Lubin. Ethereum Whitepaper, https://github.com/ethereum/wiki/wiki/White-Paper, 2014

[16] JP Morgan Chase. Quorum. https://github.com/jpmorganchase/quorum

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, Vol. L119 (4 May 2016), pp. 1-88

[18] Hyperledger Sawtooth Private Data Objects. https://github.com/hyperledger-labs/private-data-objects

[19] Gustavo Niemeyer. Geohash. https://geohash.org

[20] Thomas Piketty. Capital in the Twenty-First Century, 2013

[21] Fergal Reid. An Analysis of Anonymity in the Bitcoin System, Security and Privacy in Social Networks, 2012

[22] Serguey Popov. The Tangle, http://iotatoken.com/IOTA_Whitepaper.pdf, 2016
[23] Colin LeMahieu. Nano: A Feeless Distributed Cryptocurrency Network, 2016
[24] https://openpowerfoundation.org/
[25] https://en.wikipedia.org/wiki/List_of_cities_by_population_density, sampled Nov. 2018
[26] Juan Benet. IPFS - Content Addressed, Versioned, P2P File System. 2014