Demurrage and geolocation for local and crypto-currencies.

Cybersecurity MSc *research* project proposal.

Contacts:	Jean-Guillaume.Dumas@univ-grenoble-alpes.fr, tel: 0 457 421 732.
	Pascal.Lafourcade@udamail.fr, Ariane.Tichit@uca.fr
Laboratoires:	Jean Kuntzmann (LJK), IMAG - CS 40700
	700 avenue centrale, 38058 Grenoble. ljk.imag.fr
	Collaboration with cerdi.org and limos.isima.fr
Earnings:	Standard by the LJK.

Demurrage is the cost associated with owning or holding currency over a given period. It is sometimes referred to as a carrying cost of money. For commodity money such as gold, demurrage is the cost of storing and securing the gold. For paper currency, it can take the form of a periodic tax, such as a stamp tax, on currency holdings. Demurrage is sometimes cited as economically advantageous, usually in the context of complementary currency systems.

One of the objectives of local currencies is, among other things, to promote local economies. Unfortunately, one of the problem that arises then is the definition of what is considered local. For purely practical and legal reasons, local currencies usually therefore define their area of use according to federal limits such as a "département" in France. However, this seems to be a rather restrictive and not particularly pertinent definition. Indeed, for certain areas close to a border, it could be more coherent to use the local currency of the neighboring area.

Now, crypto-currencies are dematerialized by nature. This may make it possible to implement a consistent definition of locality. For instance, it should be possible to combine a cumulative geolocation principle and a demurrage to ensure an incentive for local consumption.

Many questions arises, among them, what about buyer and sellers localities, notions of privacy if transactions are public, security of geolocation data, management of the demurrage rate (see for instance Freicoin at freico.in), etc.

Thus, the first goal of this MSc research project is to define a model for demurring crypto-currencies either based on time, on location or on both; then to propose a distributed management of this demurrage and finally to develop a prototype implementation using recently developed blockchain or byzantine consensus technologies.

References

- Ariane Tichit, Pascal Lafourcade, Vincent Mazenod. Les monnaies virtuelles dcentralises sont-elles des outils d'avenir ? 2017. hal.archives-ouvertes.fr/halshs-01467329
- Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. 2017. ia.cr/2017/454
- Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In IEEE Symposium on Security and Privacy, IEEE Computer Society Press, p. 459-474. 2014.
- Iddo Bentov, Charles Lee, Alex Mizrahi, Men Rosenfeld. Proof of Activity: Extending Bitcoin: A Proof of Work via Proof of Stake. In Proceedings of the 9th Workshop on the Economics of Networks, Systems and Computations. 2014.