Merchant Sharing Theory

Laurent Fournier

Merchant Sharing Theory

Laurent FOURNIER – {laurent.fournier@cupfoundation.net}

November 22, 2013

Abstract

This paper is the first attempt to formalize a new field of *economics*; studding the *Intangibles Goods* available on the *Internet*. We are taking advantage of the *digital world*'s specific rules to propose a theory of TRADING & SHARING unified. A function based money is created as a world-wide currency; ⊔ (pronounced /kʌp/). We argue that our system discourage speculation activities while it makes easy captured taxes for governments. The implementation removes the today's *paywall* on the *Internet* and provides a simple-to-use, open-source, free-of-charge, highly-secure, person-to-person, privacy-respectful, digital payment tool for citizens, using standard smart-phones with a strong authentication. Next step will be the propagation of the network application and we expect many shared benefits for the whole economics development.

keywords: Economics, Internet, Intangible Good, Sharing, Trading, Money, Digital Signature, Payment, Currency, Exchange rate, Cultural Piracy, Copyright, Paywall, Peer-to-peer.

1 Introduction

SHARING and TRADING seem first conflicting in our everyday physical experience of *Tangibles Goods* (TG). When we share something, it's usually free of charge and there is no declared ownership. People are involved in a strong relationship, as friends. On the contrary, buying an object defines explicitly the owner and exclude other people from having or using the good. Trading means that the seller is dispossessed of the good against a financial reward, after a ONE-TO-ONE instantaneous relationship. Furthermore, the buyer and the seller may be completely anonymous from each other.
Is a *Merchant Sharing Theory* likely to be impossible?
Well, the *digital* world carried by the *Internet* is following different rules than the physical world. Our purpose here is to show that over the *Internet*, SHARING and TRADING are not only compatibles, but have tremendous advantages to be associated. The following theory introduces a breakthrough in the **economics** domain, making new potentially growing markets and new business opportunities. Since *Internet* is very young compared to the history of merchant exchange, all applications and all consequences of this theory are not yet well evaluated, but all the technologies are available for a generalized primary usage. Our proposal opens a new and exciting field of research and investigation.

2 Theory construction

Axiom 1 *An* **Intangible Good**[1] *(*IG*) is a virtual object having a significant* **value** *for a set of individuals, and a* **null** *margin cost.*

Only the **Internet** is able to save and to publish an IG. Any file can be duplicated on any network node at no cost. End users are investing themselves in terminal computers, phones, storage devices, so the marginal cost for the producer of an IG is null. Any tangible good (TG) may have a very low margin cost with large scale mass production, but this cost is never null. Internet also store data for private communications, without any value in public publishing. This data is not considered as an IG.

Creator: The *creator* of an IG is one individual or a group of individuals using high skills and spending time to create the IG. This work deserve a direct or indirect financial reward for the creator.

[1] see fr.wikipedia.org/wiki/Bien_immateriel

Customer: A *customer* of an IG in one individual owning a sufficient amount of money to acquire the right to *use* that IG any time all his life, on any device[2], without any DRM[3] attached nor advertising.

Transaction: (Figure **??**) For a given IG, Internet allows to define a ONE-TO-MANY temporal relation $\mathcal{F}_c(i,t)$ between the *creator* and the effective i *customers*. As soon as the IG is published, customers are free to choose the time for buying the IG, without the creator agreement. In the same IG relation, any new buyer, in position i, time t, may spend a *price* $\mathcal{P}_i^t$, making for the creator an *income* $\mathcal{I}_i^t$ and for the $i-1$ previous j buyers as a *refund* $\mathcal{R}_{ij}^t$. Unlike for a TG transaction requiring transportation and transformations, no intermediate actor is requested in the pure digital IG transaction, thus no additional fee is required in IG relation. So the following equation states:

$$\forall i \in \mathbb{N}^* \qquad \mathcal{P}_i^t = \mathcal{I}_i^t + \sum_{j=1}^{j\leq i} \mathcal{R}_{ij}^t$$

Starting from now, the time parameter t is skipped because our main proposal is time independent, but we do not exclude to define in next developments a time dependent solution, specially for time valuated IG like for flash paper news.

Hypothesis 1 *The price $\mathcal{P}_i$ is only dependent of the position i of the buyer in the list (eventually the time of the buying action), but never dependent of buyer personal features/data or buyer financial capabilities.*

Hypothesis 2 *For a given* IG *and knowing that the margin cost is null while the production cost is finite. It is a fair principle to bound the cumulative income $\mathcal{T}_i$ with a fixed value, $\mathcal{T}_\infty$, chosen by the creator and known universally.*

$$\forall i \in \mathbb{N}^* \qquad \mathcal{T}_i = \sum_{k=1}^{k\leq i} \mathcal{I}_k \qquad \lim_{i\to\infty} \mathcal{T}_i = \mathcal{T}_\infty$$

Then we have:

$$\lim_{i\to\infty} \mathcal{P}_i = 0 \tag{1}$$

Hypothesis 3 *For a given* IG*, the price function $\mathcal{P}_i$ is decreasing. If two customers ask to buy the same* IG *at the same time, the displayed price has to be higher than the effective price.*

$$\forall i \in \mathbb{N}^* \qquad \mathcal{P}_i' \leq 0$$

Hypothesis 4 *For a given* IG *and for any purchase number i, the refunding values $\mathcal{R}_{ij}$ for $j < i$ are equal.*

$$\forall i \in \mathbb{N}^* \qquad \forall j < i \qquad \mathcal{R}_{ij} = \mathcal{R}_i$$

Then we can verify the equations:

$$\mathcal{P}_i = \mathcal{I}_i + (i-1)\mathcal{R}_i \tag{2}$$
$$\mathcal{T}_i = i\mathcal{P}_i \tag{3}$$
$$\mathcal{I}_i = \mathcal{T}_i - \mathcal{T}_{i-1} \tag{4}$$

Theorem 1 *At the same time, all i buyers had payed, including the refunds, the very same price to get the same* IG*. This price is equal to $\mathcal{P}_i$.*

[2]This right is referenced as the "mobiquity" right.

[3]Digital Right Management

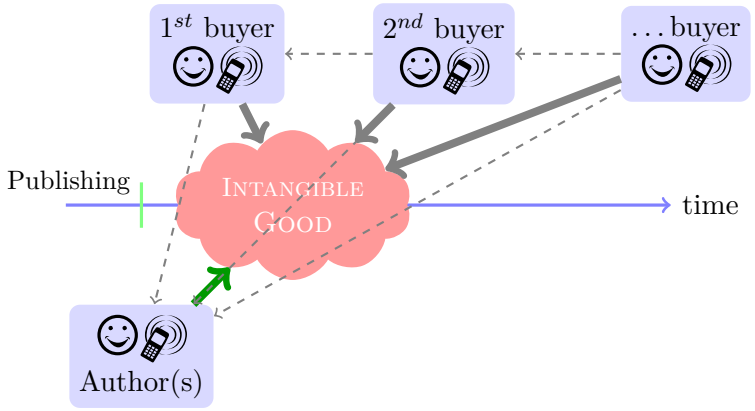

Figure 1: Intangible Good; a perpetual *many-to-many*, relation.

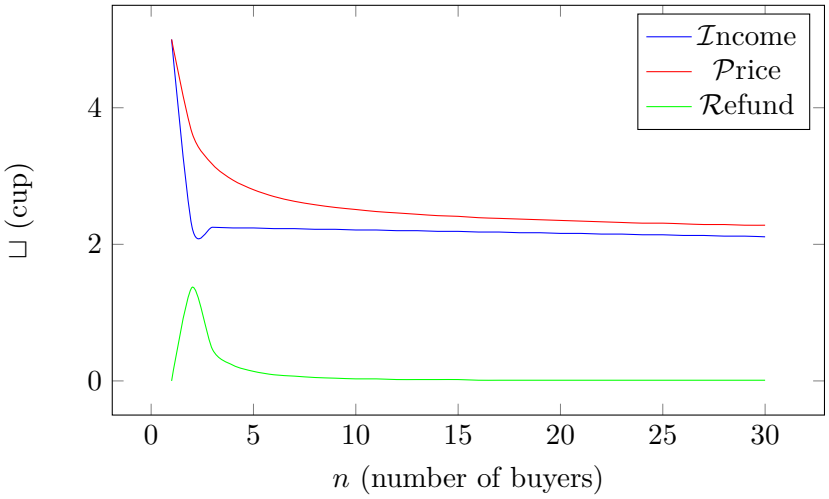

Figure 2: Income, Price and Refund values for a 5⊔1000 IG and $\xi = 0.3$.

Theorem 2 *For an* IG *given by its creator with initial price* $\mathcal{P}_1$ *and a limit cumulative income* $\mathcal{T}_\infty$*, It exists a solution satisfying previous hypothesis.*

The previous hypothesis can be summerized in the less formalized principle of FAIRNESS:

Principle 1 *Creator cumulative income of an* IG *is bounded while every time, all buyers pay the very same price down to zero.*

We seen that IG transactions follows rules not as simple as for the physical world where only a ONE-TO-ONE relation occurs. We used to use the equation $\mathcal{P} = \mathcal{I} + \sum_i f_i$. The f_i are fees taken by intermediaries for transportation and transformation and are subject to speculation. Prices, incomes are scalars and refund is null for tangibles goods. However, for IG, its price is a function and the relation is a little more complex to manage the automatic refund. We introduced a breakthrough in traditional economics exchange.
The next section proposes a function solution family with "smooth" variations. This family requires only one tuning parameter $\xi \in [0, 1]$ called speed parameter.

3 The exponential family

For an IG sold at the first price $\mathcal{P}_1$ and expecting an income $\mathcal{T}_\infty$, the three related computed values are:

- $\mathcal{P}_i$ the price a buyer has to pay the good in position i
- $\mathcal{I}_i$ the additional income to the creator for a purchase in position i, $\mathcal{T}_i$ is the cumulative income.

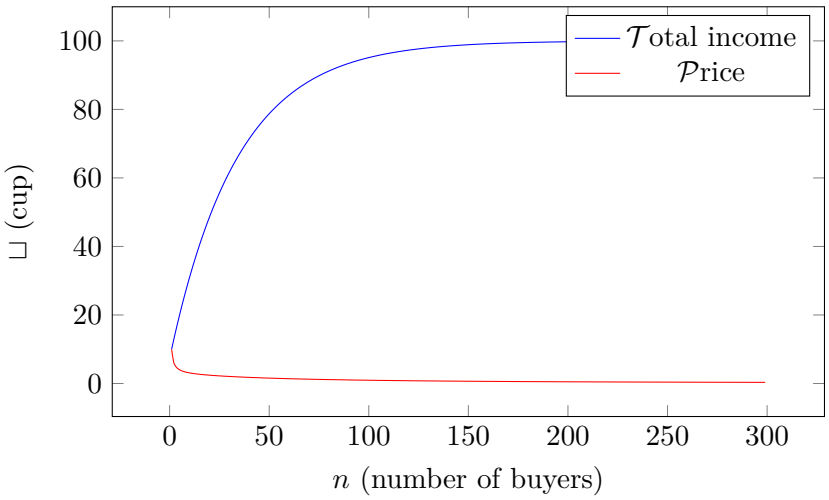

Figure 3: Income and Price evolution of a 1⊔100 IG for $\xi = 0.25$.

- $\mathcal{R}_i$ the refunding value given to all previous $(i-1)$ consumers of the same good

A piece linear model solution exists but we present here the exponential based solution. For this model, with a speed parameter $\xi \in [0, 1]$ selected by the creator, and with:

$$\lambda = \left(\frac{\mathcal{T}_\infty - \mathcal{P}_1}{\mathcal{T}_\infty - 2\mathcal{P}_1}\right)^\xi$$

we have $\mathcal{I}_1 = \mathcal{P}_1$, $\mathcal{R}_1 = 0$ and $\forall i > 1$ and (*Figure* **??**):

$$\mathcal{P}_i = \frac{\mathcal{T}_\infty + (\mathcal{P}_1 - \mathcal{T}_\infty)\lambda^{1-i}}{i} \tag{5}$$

$$\mathcal{I}_i = (1-\lambda)(\mathcal{P}_1 - \mathcal{T}_\infty)\lambda^{1-i} \tag{6}$$

$$\mathcal{R}_i = \frac{\mathcal{T}_\infty + \lambda^{1-i}\left(1 + i(\lambda - 1)\right)(\mathcal{P}_1 - \mathcal{T}_\infty)}{i(i-1)} \tag{7}$$

The total income (*Figure* **??**) is:

$$\mathcal{T}_i = \mathcal{T}_\infty + (\mathcal{P}_1 - \mathcal{T}_\infty)\lambda^{1-i} \tag{8}$$

$\mathcal{P}_i$, $\mathcal{I}_i$ and $\mathcal{R}_i$ are decreasing while $\mathcal{T}_i$ is increasing and we check that:

$$\lim_{i\to\infty} \mathcal{P}_i = 0 \qquad \lim_{i\to\infty} \mathcal{T}_i = \mathcal{T}_\infty$$

3.1 The numerical rounding issue

The implementation of the solution over the Internet raises a numerical rounding issue for the money. There is computational benefits to use integers instead of floating point. We argue that the paradigm shifting require to introduce a new money/currency, noted with the SQUARECUP symbol: ⊔[4], dedicated to IG, with main features:

- ⊔ is vector based; $(\mathcal{P}_1, \mathcal{T}_\infty, \xi)$ or function based but not scalar based unlike € or $.
- ⊔ is an universal/international currency dedicated to *intangible goods* of the Internet, world-wide by construction.
- ⊔ is from design integer based, with a unit value around 10 cents; the smaller price to get a significant IG. The exchange rate value is explained in section 5.

[4] pronounced /kʌp/

- ⊔ is not sensitive to speculation actions... see section 6 for details on this point.

For integer computation, the full transaction has to remain well balanced. As soon as the cumulative income approach the expected value, all entities (price, income, refund, become very small, so we must select the more suited rounding policy. An admissible solution is to round first the income $\mathcal{I}_i$ and second the refund value $\mathcal{R}_i$, then compute the price as:

$$\mathcal{P}_i = \mathcal{I}_i + (i-1)\mathcal{R}_i$$

This way, all the money given by a new coming customer is shared between the creator and the previous buyers.
We may find two interesting values:

No refunding threshold : the value i_{nr} for which: $\forall i \geq i_{nr} \qquad \mathcal{R}_i = 0$

Public domain threshold : the value i_{pd} for which: $\forall i \geq i_{pd} \qquad \mathcal{I}_i = \mathcal{P}_i = \mathcal{R}_i = 0$

It is obviously verified that $i_{nr} < i_{pd}$ and as the ⊔ money is integer based, we have:

$$i_{pd} = \mathcal{T}_\infty \tag{9}$$

The first i_{pd} customers had paid 1⊔ and all the other get the IG for free.

4 No paywall

Beyond the idea that *Internet* pushing and speeding-up trading of *tangibles goods*, it remains today a *paywall* on the Net. The current main payment systems; *VISA, Mastercard, PayPal...* are in the same time too complex, poorly secure, and very expensive for any citizen (merchant or customer). This is particularly unfortunate for IG creators who can't publish their work directly on the Net, on their own server, just because they do not have access to an automatic, in the Net stack, free payment system to get their incomes. *One click* payment attends to fix that paywall but raises privacy issues as we see for *Google-wallet* or *iTunesStore*. We argue that a distributed, open-source, free of charge solution is technically possible and it would promote a new peer-to-peer publishing, instead of concentration on huge intermediary private platforms. This digital payment system called Ping-Pong-Cash is fully adapted to ⊔ trading for IG but also provides great usage for traditional trading of TG, using € or $ currencies.
Authentication is a key point for digital payment. That's why our system requires a three ways authentication:

- Something you carry (phone, card, usb stick...)
- Something you know (PIN, passphrase...)
- Something on you (bio-metric data)

The smartphone is likely the best device to enable this strong autentication. It store a locally generated private key while the public key is readable universally on a Ditributed Hash Table DHT. A transaction is simply a message digitally signed by the buyer. The selected digital signature algorithm is ECDSA with the *P521* NIST eliptic curve[5]. Private key usage is protected by AES 256 symetric encryption. Any user who buy an IG received an encrypted URL, when decrypted, downloads the full file.

[5] `http://www.nsa.gov/ia/_files/nist-routines.pdf`

5 Exchange rate proposal

The ⊔ money is not created from scratch, it is more considered as a *unit* computed value based on a shared formula. The ⊔ currency is then convertible with most local currencies in the World. Let define as $\mathcal{C}$ the finite subset of n currencies not including the ⊔. r_{ij}^t is the exchange rate between the currency i and currency j at discrete date t. Each currency i has a known volume v_i in the world and v is the total volume. Volumes are supposed stable during long time periods. The trivial solution for fixing $r_{\sqcup k}^t$ for any currency k would have been to sum all current exchange rates for currencies in $\mathcal{C}$ weighted by their respective volume v_i as:

$$\forall t \in \mathbb{N}, \forall k \in \mathcal{C} \qquad r_{\sqcup k}^t = \frac{1}{v} \sum_{i=0}^{i<n} v_i r_{ik}^t$$

As it as been set for the ECU in 1999[**?**] for introducing the Euro. This definition would not minimize the time variation of the exchange rate with other currency, making an opportunity to engage speculation with such currency. To fix this issue, we consider that exchange rates are given each day, so t' means the day after t. Let select randomly a currency k in $\mathcal{C}$ and we are facing the problem of defining the exchange rate $r_{\sqcup k}$ between ⊔ and k. One has to select an initial value $r_0 = r_{\sqcup k}^0$ at the date of birth for the international currency.

We proposes a recursive algorithm that computes $r_{\sqcup k}^{t'}$ knowing $r_{\sqcup k}^t$ for a given currency k but all other exchange rates with other currencies i are immediately computed with:

$$r_{\sqcup i}^t = r_{\sqcup k}^t r_{ki}^t \qquad \forall t \in \mathbb{N} \qquad \forall i \in \mathcal{C}$$

Let define the value:

$$\mathcal{V} = \min_{r_{\sqcup k}^{t'}} \left(\sum_{i=0}^{i<n} v_i \left| 1 - \frac{r_{\sqcup i}^{t'}}{r_{\sqcup i}^t} \right| \right)$$

This value $\mathcal{V}$ can be written:

$$\mathcal{V} = \min_{r_{\sqcup k}^{t'}} \left(\sum_{i=0}^{i<n} v_i \left| 1 - \frac{r_{ki}^{t'}}{r_{ki}^t r_{\sqcup k}^t} r_{\sqcup k}^{t'} \right| \right) = \min_{r_{\sqcup k}^{t'}} \left(\sum_{i=0}^{i<n} \left| a_i r_{\sqcup k}^{t'} + b_i \right| \right)$$

with a_i and b_i known constants.
The previous multi pieces linear equation has one solution (Figure **??**) satisfying: $\exists j \in \mathcal{C}, r_{\sqcup k}^{t'} = -b_j/a_j$
For such currency j that minimize the value $\mathcal{V}$, we have:

$$r_{\sqcup k}^{t'} = \frac{r_{kj}^t}{r_{kj}^{t'}} r_{\sqcup k}^t$$

If:

$$\mathcal{V}_i = \sum_{i \neq j} v_i \left| 1 - \frac{r_{\sqcup i}^{t'}}{r_{\sqcup i}^t} \right|$$

then j is such that $\mathcal{V} = \min(\mathcal{V}_i)$
The algorithm simply computes the $\mathcal{V}_i$ for all currencies of $\mathcal{C}$ and find the j currency that does not change its rate between t and t'. The currency solution j is always independent of the selected currency k used at first reference.
Let now define the value function:

$$\mathcal{V} = \sum_{i=0}^{i<n} v_i \left(1 - \frac{r_{\sqcup i}^{t'}}{r_{\sqcup i}^t} \right)^2$$

This polynomial function of degree two has a unique minimum for:

$$\forall k \in \mathcal{C} \qquad r_{\sqcup k}^{t'} = \left(\frac{\sum_{i=0}^{i<n} \frac{r_{ki}^{t'}}{r_{ki}^t} v_i}{\sum_{i=0}^{i<n} \left(\frac{r_{ki}^{t'}}{r_{ki}^t} \right)^2 v_i} \right) r_{\sqcup k}^t = \mathcal{K}_k^{tt'} . r_{\sqcup k}^t$$

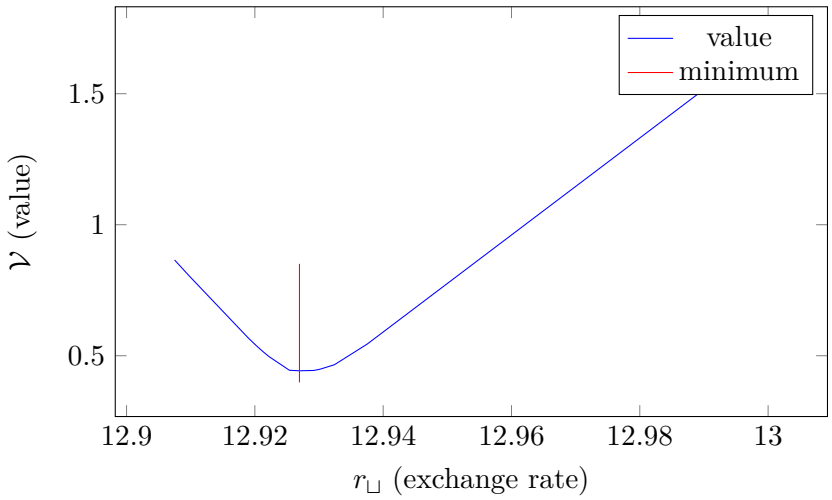

Figure 4: Value function for $r^t_{\sqcup\$} = 13$, then minimum reach for $r^{t'}_{\sqcup\$} = 12.9269511038$.

Knowing exchange rates between all currencies in $\mathcal{C}$ for all days from an initial date, one can compute the $\mathcal{K}^{tt'}_k$ delta coefficient and then exchange rate with $\sqcup$ for all those days, starting with a fixed initial value. Our proposal for the most used currency in the set:

$$\mathcal{C} = \{\text{USD}, \text{EUR}, \text{JPY}, \text{GSP}, \text{AUD}, \text{CHF}, \text{CAD}, \text{HKD}, \text{SEK}, \text{NZD}, \text{SGD}, \text{KRW}, \text{NOK}, \text{MXN}, \text{INR}\}$$

with their respective volume value[**?**]:

$$v = \{849, 391, 190, 129, 76, 64, 53, 24, 22, 16, 15, 15, 13, 13, 9\}$$

6 Speculation

The exchange rate for $\sqcup$ as defined in the previous section protects the currency from speculation attacks. There are mainly five reasons for that resistance:

- As an international currency, available all over the Internet, there is no need for currency exchange. The ratio is the most stable from the set $\mathcal{C}$ of reference currencies, so any fluctuation of $\sqcup$ means that other currencies has changed. However, the algorithm is fully deterministic knowing the daily exchange rates between currencies in $\mathcal{C}$ and one exchange with $\sqcup$ the day before. Authorities or human evaluation cannot change the new exchange rate. Anybody in the world can compute it to get the same result.

- Any *Intangible Good* is sold on the Internet in $\sqcup$ at the same price whatever the development level of the population. Then, there is no local market places with different prices and possible speculation gains.

- $\sqcup$ exchange with other currencies are subject to support a selling and buying tax going to the government or financial authority in charge of the foreign currency. For instance to exchange \$ into € using $\sqcup$, one has to pay a tax to EEC for buying $\sqcup$ from € and a tax for the USA for selling $\sqcup$ into \$. As we see, there is no advantage for traders to use $\sqcup$ between currencies on the market exchange.

- $\sqcup$ is dedicated to *Intangible Good* exchange and the transaction is atomic (money in $\sqcup$ against the URL of the good). There is not a double transaction like in the tangible world (Figure **??**). Any undervalued or overvalued transaction using $\sqcup$ is immediately suspect and may hide another illegal transaction. Transactions without a real intangible good are only allowed for the same individual to change local currency into $\sqcup$ in order to buy cultural goods or for an artist earning $\sqcup$ to change them into the local currency. It is not allowed for one person to $\sqcup$ from another

Figure 5: Trading difference between Intangible Good (IG) and Tangible Good (TG).

person against euros for instance. There should always exists an intangible good published over the Internet by the seller.

- ⊔ economics follows different rules than the classical economics for tangible goods. The mechanism of refunding of previous buyers when new buyers are coming makes ⊔ the first functional or non scalar currency. Those different rules makes more clear the necessity to define a new currency. It could have been possible to computes transaction following the fair intangible good principle using euro, but then people would have to carefully make the difference between euros for tangible goods, without refunding and euros for intangible goods with refunding and bound income. Some sellers of cultural goods on the Internet may have use the same currency name to sell without refunding and without bound income, an clearly unfair transaction.

7 Conclusion

In *economics*, this paper proposed a new paradigm dedicated to *Intangible Good* TRADING fully consistent with SHARING. Thanks to the *Internet* to make the theory possible and verifiable in real life. We introduced the ⊔ convertible, functional money, we shown the resistance against speculation and we argued on the need to deploy as soon as possible a easy-to-use, free-of-charge, open-source, distributed, secure digital payment system for person-to-person exchanges, both for IG and for TG. Next study will detail the network architecture and the peer-to-peer node design, including cryptographic primitives.

References

[1] Task force sur l'Union économique et monétaire *De l'Écu à l'Euro: fixation des taux de change*. 1999.

[2] L. Fournier *Economics for Intangible Goods*. arXiv.org 2012.

[3] Wikipedia *Foreign exchange market*. 2013.

[4] P. Jorion *L'argent mode d'emploi*. Fayard, 2009.

[5] A. Testart *Critique du don, Étude sur la circulation non marchande*. Paris: Syllepse, 2007.