P2P Economies

Enoch Peserico *
Computer Science and Artificial Intelligence Laboratory, M.I.T.
enoch@csail.mit.edu

ABSTRACT

We analyze current P2P credit systems in the light of modern economic theories, devoting particular attention to currency based ones, and argue their unsuitability to the characteristics of P2P networks. We then propose a robust, efficiently scalable barter system with *short transactions* and *wealth storage*, classically considered the two most important features of currency based economies.

Categories and Subject Descriptors: C.2.4 [Computer Communication Networks]: Distributed Systems

General Terms: Algorithms, Design, Economics

Keywords: peer, economic, incentive, currency, distributed

1. (PSEUDO-)ECONOMIES FOR P2P

(Pseudo-)economic systems are attracting increasing interest in the context of P2P and ad hoc networks, as a solution to the problem of "free riders" and as an incentive to allocate resources where they generate the greatest returns for the rest of the network. Their study is, however, still in its infancy and the proposed solutions present a number of weaknesses.

Kazaa sports one of the earliest such systems: each node advertises a "participation level" increasing with the node's uploads, and receives a proportional amount of resources from other peers. This system is vulnerable to clients that always advertise the highest participation level regardless of their actual uploads. Emule/Edonkey and Bittorent avoid this problem having each node track the resources received from other nodes, and allocate its own resources appropriately. But then each node might have to store information proportional to the number of nodes it interacted with. More importantly, this system is not *transitive*: if Alice performs a favor for Bob, and Bob for Carol, Alice cannot call in a favor from Carol. EigenTrust ([3], based on the well known PageRank algorithm) is an example of a credit system transitive but (we show) not *cohesive*: small communities end up giving more resources to larger, tightly knit communities than they receive from them, and are therefore enticed to leave the main network to form their own. The same weakness is shared by other similar systems; it also makes EigenTrust somewhat vulnerable to sybil attacks.

Systems like PeerMart [2] avoid the difficulties above by making use of a *currency*: a durable, widely accepted commodity that becomes a means to *short transactions* and *wealth storage*. With currency, transactions are short: one can trade e.g. apples for currency and currency for zucchini instead of having to spend considerable effort in search of a viable *barter path* connecting apples to zucchini - e.g. apples for beer, beer for cream, ..., wine for zucchini. Currency can also store wealth: one can trade a harvest of perishable apples for currency and at a later time currency for other goods not available or needed at the time of the harvest. Under some mild and realistic assumptions, these two features guarantee transitivity, cohesiveness and a number of other desirable properties.

Yet currency has its own problems. Using a currency exogenous to the system (e.g. the Euro) entails serious psychological, financial and legal difficulties; and exposes a vital component of the network to the vagaries of outside actors who may have no stake in the network (and may even antagonize its existence). The main difficulty with a currency endogenous to the system is instead "bootstrapping". Economic theory teaches that imposing a currency created ex nihilo on a market is effectively impossible: currency must evolve from a commodity with an initial intrinsic value in a barter economy [4]- if that commodity has certain characteristics, it becomes progressively more accepted in exchange for other commodities, eventually functioning primarily as a currency.

Unfortunately, most commodities traded on P2P networks lack one or more of the qualities of good "currency candidates". These commodities are generally either services (e.g. storage space or bandwidth or CPU cycles for a given period of time) or information (e.g. media files). Services lack the *durability* necessary to store wealth: given 1 GB of space on another peer for the next 7 days, one must either use it in that week, or lose it. Information is generally durable, but lacks *evaluability*: it is difficult to assess its value since it can be easily duplicated and thus quickly become "as common as dirt" and difficult to trade away. Finally, commodities traded on P2P networks are typically highly *heterogeneous* (e.g. while one could think of using "bytes of storage somewhere on the network" as currency, space on a high availability, high bandwidth server is quite different from the "same" space on a laptop), and heterogeneity is a well known obstacle to the adoption of a commodity as a currency [1].

2. A BARTER BASED ECONOMY

We propose a robust, scalable and efficient barter based economy for P2P which still achieves short transactions and wealth storage - classically the key features of currency.

*Part of this research was carried out at the Dep. of Information Engineering of the Univ. of Padova. Supported in part by Aeolus, Oxygen, and the Singapore/MIT alliance.

2.1 Wealth Storage

One solution to wealth storage despite perishability of commodities is to trade in promises of future commodities - these are durable (i.e. retain their value over time, until the moment they are due) even when commodities are not. E.g. one might trade today's bandwidth for CPU cycles 30 days in the future; and in 10 days retrade those CPU cycles (with 20 more days "lifetime") for some other service.

The fundamental difficulty lies in guaranteeing promises will be kept. This can be achieved under a few, realistic, assumptions; the most important being a mechanism allowing both parties engaging in barter to learn the "surplus" gained by both in the exchange (e.g. cryptographic techniques or double blind auctions). In general, a global authentication infrastructure is not needed, nor a proof of work system that forces nodes entering the system to "waste" resources so as to make identity laundering inviable.

A very simple example provides some intuition. Consider two actors A and B simultaneously bartering 1 unit of two commodities a and b. A would have been willing to give up to $1+\epsilon$ units of a for 1 of b; B's situation is symmetrical. With this initial simultaneous barter, both A and B have obtained a surplus that effectively opens a "two way credit line" with each other. Either party can now "borrow" up to an extra ϵ of the other's commodity - and the other party still experiences no overall loss even if the loan is not repayed. More importantly, either party can borrow up to $\frac{\epsilon(p(1+\epsilon)-1)}{2(1+\epsilon)}$ of the other's commodity, and assuming that trade for a quantity ϵ of the same commodities at the same rate will take place in the future with probability p, still have no incentive to "cheat" and avoid repaying the loan - even if it could immediately create a new identity at no cost! Note that this is somewhat stronger than standard tit-for-tat results.

Thus, two way credit generated by the surplus of a few initial simultaneous barter transactions can be effectively used as a durable good to store wealth. It can be traded away in a market with more than two actors, as long as a "lifeline" is kept between the two "halves" of the credit, so that cheaters can be punished by seeing their half revoked. Essentially the same results hold even in more complex utility (and utility fluctuation) models, and, with a sufficiently (but realistically) large barter surplus margin, under "noise" caused by node failures and both long and short term churn.

2.2 Short transactions

Short transactions without a single unified currency can be achieved through *barter trees*. In a basic implementation, each vertex v of the tree corresponds to a commodity $c(v)$. The vertices adjacent to v correspond to commodities for which some nodes of the network are willing to barter $c(v)$. The identity of those nodes, the current exchange rates between the corresponding commodities, and enough information to navigate the tree (i.e. to find the shortest path between any two of its vertices - information logarithmic in the number of commodities is sufficient at each node [5]) are stored together, e.g. using a distributed hash table to distribute the information over the network. Such a tree exists if there is a barter path connecting every pair of commodities (for *some* exchange rate) - were it not the case, we would simply have to deal with two or more isolated economies.

When a network node wants to barter a commodity for another (or just find the exchange rate between the two), it simply has to find and follow the path between the two corresponding vertices of the barter tree, with each edge corresponding to a barter between the commodities associated to its two vertices. Demand and supply set the exchange rate along each edge.

This basic implementation of barter trees has a number of weaknesses, mainly stemming from the fact that the root of the barter tree (and the nodes trading the respective commodity) are a bottleneck through which a large fraction of all barter has to pass. This places an excessive bandwidth load on those nodes; it also places an excessive strain on the commodity, which is unlikely to have a sufficient critical mass to avoid wide fluctuations in the exchange rate; and creates a single point of failure for the whole economy. Also, barter paths could be quite long (linear in the number of commodities in the system).

We solve all the problems above through a more sophisticated barter tree scheme, where commodities are mapped into the leaves of a complete low degree tree, and each internal vertex is associated to a *portfolio* of those commodities (or of those portfolios) associated to its children. Portfolios are managed distributedly by those network nodes associated to their commodities; with the balance of commodities in a portfolio, set by supply and demand, reflected in the balance of "power" between the nodes and in the balance of transaction bandwidth for which each node is responsible. This ensures load balancing between nodes, robustness, short (logarithmic in the number of nodes) barter paths and a relative small overhead per transaction.

3. CONCLUSIONS AND FUTURE WORK

The study of (pseudo-)economic systems to regulate networking is an area that, while steadily growing, is still very much in its infancy, and would strongly benefit from application of modern economic theory. We propose a robust barter based economy that, without the need of shared currency (and the difficulties it entails), efficiently achieves the two most desirable features of currency based economies - short transactions and wealth storage - and is thus scalable, transitive and cohesive.

A number of interesting lines of research stem from this initial work. Two of the most promising seem to be the study of stability and convergence in the presence of supply/demand fluctuations, and portfolio aggregation: what is the best strategy for aggregating (promises for future) commodities in portfolios? For further details see: *http://people.csail.mit.edu/enoch/paripari/*

4. REFERENCES

[1] G. A. Akerlof. The market for 'lemons': Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 1970.

[2] D. Hausheer. Peermart: A decentralized auction based p2p market, http://www.peermart.net.

[3] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the Twelfth International World Wide Web Conference*, 2003.

[4] M. N. Rothbard. *Man, Economy and State: A Treatise on Economic Principles*. D. Van Nostrand Co., 1962.

[5] M. Thorup and U. Zwick. Compact routing schemes. In *Proceedings of ACM SPAA*, 2001.