Free Software Economics

Hellekin Wolf, Jaromil Jaromil, Radium Radium, Christian Grothoff

FREE SOFTWARE ECONOMICS

Fifteen years ago, in his seminal article *Code Is Law* *(http://harvardmagazine.com/2000/01/code-is-law-html)*, Lawrence Lessig identified a problematic: *"The most important contexts of regulation in the future will affect Internet commerce: where the architecture does not enable secure transactions."* Today, European free software researchers are implementing innovative solutions to address this and other issues that will shape digital economics in the near future.

We argue that beyond regulation, code embeds politics. We'll introduce two projects we think will transform not only how we conduct economic transactions online, but which also hold the potential to radically change the global balance of economic power.

Freecoin is a social digital currency based on the blockchain technology of Bitcoin but which relies on a "social proof of work" instead of the original brute-force algorithmic proof of work used in Bitcoin. Freecoin was developed by the Dyne Foundation, a free culture foundry based in the Netherlands, and now a European Research Network. Freecoin is Project no. 610349 in the FP7 - CAPS framework, under the Decentralised Citizens ENgagement Technologies (D-CENT) project.

GNU Taler is the Taxable Anonymous Libre Economic Reserve, a new electronic payment system under development at Inria, the French National Institute for Information and Automation Research, and the Technical University of Munich (TUM). It aims at delivering an online and offline payment solution for various established currencies such as Euro, U.S. Dollar, or even electronic currencies such as Freecoin.

Together they implement a unique electronic solution for mainstream economics beyond payment. They were specifically designed with social values addressing the shortcomings of both early electronic currencies such as Bitcoin, enabling a variety of local currencies to work together, extending transactions to non-monetary domains such as distributed storage, and drastically limiting the criminal use of money. Their combined approaches unfold a many-to-many platform suitable for daily use from global micro-payments to local social currencies.

Bitcoin was the first digital currency to appear on the Internet. It implements a distributed and authenticated public ledger called the blockchain, whose mode of operation is based on decentralized consensus. The blockchain replaces the bank: it uses cryptographic techniques to regulate the emission of coins and verify transactions between peers.

The design of Bitcoin has definitive shortcomings: first of all it's very volatile. By the time this article was finished, its value was down to USD 402.7 after reaching USD 479 earlier during the day. As all finalized Bitcoin transactions appear in the blockchain, the whole market is transparent, and a coin's history can be used to connect identities to addresses. To avoid double spending, no bitcoin transaction can be reversed, which means the buyer is not protected against fraud from the seller, nor addressing errors. By design, Bitcoin rewards early adopters. Finally, the proof of work requires a significant amount of computing power which translates into high energy costs.

freecoin

Freecoin *(http://freecoin.ch/)* is a set of tools that let people run a reward scheme that is transparent and auditable by other organizations. Designed for participatory and democratic organizations willing to incentivize participation it is, unlike centralized banking databases, a social currency that is reliable, simple, and resilient. Technical and design elements shape a way to legitimize the bottom-up process using audit of cryptographic blockchain technologies such as decentralized storage, ubiquitous wallets, and ad-hoc social remuneration systems.

The Freecoin project insists on the need to strengthen the democratic debate necessary to consolidate and preserve the management of economic transactions, especially those with a social orientation, inside the local monetary circuit. It focuses on complementary currency design to allocate and distribute credit created among engaged members, using a reputation as risk management system.

Citizens can collectively define their social needs using a participatory deliberation based on "social sustainability": without participation, local monetary circuits run the risk to remain too little, too dependent on the local political cycles, too far from the real demand that may be expressed by the local economic system. Choices need to be informed with social objectives and ethical criteria to properly allocate resources and investments.

The Freecoin / D-CENT project is an experiment in digital social currency design that aims at solving two problems: (1) the vulnerability of centralized information systems, whose integrity can be jeopardized by compromising a few points of failure, and (2) the management of digitally distributed trust to make sure that different organizations which may not share trust can agree and verify the integrity of a transaction history, even in the absence of the other organization.

1) *Complementary currency governance systems*: with a minimalistic reinterpretation of the blockchain technology, the Freecoin Toolchain is a toolkit for community members to easily access and decide on the features of their currency system by using a decentralized governance structure - essentially, bringing back human intervention to oppose the high-frequency trading algorithms (Durbin, 2010). A system for collective deliberation on the decisions regarding digital currency will allow users to engage in collective monetary policy-making.

2) *Distributed trust management systems:* reputation is the basis for trust and decision-making. Putting together trust and the blockchain, the Freecoin Toolchain allows for the design and prototyping of systems aimed at managing social currency in a community, i.e. reputation in a decentralized fashion. The use of micro-endorsements allows the even spreading of risk among participants, and the rewarding of the best political contributions (similar to the participatory budgeting in Iceland). In a municipality, the use of those credits as loyalty scheme vouchers lowers the risk to promote proposals that go against the common interest of the citizenry.

The issuance of new coins is a technology-driven mechanism based on a consensus algorithm that neutralizes counterfeiting. However, this may also be seen as a departure from an active and critical engagement among humans and machines, whereby the creation of money in the system is motivated by social interactions for the com-

mon good, rather than by exclusively hashing cycles and shortsighted money-making. Therefore, the task of the Freecoin / D-CENT research is to redefine Bitcoin's 'proof of work' and the reward of a blockchain system, to devolve power into the hands of people through a democratic decision process. The outcome of this shift in design is twofold: (1) people engage in transactions that have real world desirable impact that they produce and collectively construct; (2) new participants can enjoy an egalitarian economic environment by avoiding the undesirable condition of structural advantage by early adopters of a currency. At the same time, this allows complete democratic oversight of transaction history and collective deliberation on social currency system rules of engagement and reward.

The Freecoin project is licensed as Affero GNU General Public License version 3 or later to make sure that all uses, commercial or non-commercial, will provide access to the source code, be it modified or not.

gnu taler

At IETF 93, Edward Snowden said via videoconference: "I think one of the big things that we need to do, is we need to get away from true-name payments on the Internet. The credit card payment system is one of the worst things that happened for the user, in terms of being able to divorce their access from their identity." So while obviously some people do not care much about their privacy, we do think that many will heed his words once a viable alternative exists. Identity theft, fraud, convenience and efficiency gains are other reasons why consumers or merchants are likely to be excited about adopting Taler.

While our initial market is likely to be technological enthusiasts with a focus on privacy, we believe that the technology is applicable in general for all payments (in online stores and physical stores) assuming sufficient engineering effort (integration, ease of use, etc.) is put behind it.

However, as the receivers of funds are not anonymous and can be audited and taxed by the state, Taler's market does not include tax evasion, money laundering, human

trafficking and any other forms of illegal trade that have ballooned the popularity of Bitcoin.

Existing payment systems, including BitCoin, use cryptography to authenticate the user making the payment. In contrast, Taler uses cryptography to secure the value and validity of the payment. As a result, identity theft is no longer a problem for customers using Taler, and merchants also do not have to worry about the theft of sensitive customer information. Naturally, customers may reveal their identity (i.e. for shipping), but they are not forced to by the payment system. In contrast to previous research designs, Taler provides stronger assurances for the customer's privacy (including better than BitCoin, where transactions are linkable). We are also the first electronic payment system of this type that supports giving change (i.e. pay 5 EUR with a 100 EUR coin and get 95 EUR in electronic change) with these privacy assurances. Taler can even provide refunds to customers without violating their anonymity. At the same time, transaction costs are several orders of magnitude cheaper than those with BitCoin-technologies. At scale, we expect transaction costs to be lower than those for existing credit cards, as expenses from fraud by consumers, merchants or identity theft are prevented by the cryptographic protocol.

Unlike BitCoin, Taler does not introduce a new currency but merely provides digital representations of existing currencies (such as EUR, USD or even BTC), eliminating the risk from currency fluctuations introduced by payment systems that introduce a new currency, such as BitCoin, AltCoins, Stellar or Ripple.

Our system consists of various components operated by different groups. The mint creating the digital coins is mostly finished and just undergoing additional testing and audits. The mint is also the most complex part of the design. Even after this is finished, we still need to integrate the mint with the banking system of each respective country to perform wire transfers. This is a one-time expense per banking system. For the customers, we need to ensure that the "wallet" application works well for their respective platform. Our initial implementation is for Firefox, ports to other browsers and native apps for mobile phones will require more work. The wallet is simpler than the mint, but still non-trivial especially if we want to make it easy to use and nice to look at.

Finally, each merchant will require some modifications to their business logic to integrate the new payment system. While these modifications are way smaller and easier than the mint or the wallet, there are of course many more businesses platforms than browsers or banking systems. Hence, while the work for an individual store should be tiny, this will be a major effort. We are trying to document our protocol and prototypes and will provide reference implementations in various languages to facilitate this integration.

GNU Taler is free software released under the terms of the GNU General Public License version 3 or later.

by Hellekin, with Jaromil and Radium, of Dyne.org (http://www.dyne.org) / D-CENT (http://dcentproject.eu/) project, and Christian Grothoff, INRIA Rennes, maintainer of GNU Taler (https://taler.net).