Solving Collective Commons Problems: Future Scenarios for P2P Finance

David Hales, University of Szeged, Hungary
www.davidhales.com

Diversity in macroeconomics workshop, University of Essex, Feb 24-25th 2014.

Extended abstract of talk

There has been much recent interest in the potential of peer-to-peer (P2P) finance to support better outcomes for borrowers and lenders. More recently innovations in so-called P2P monetary systems (often based on cryptography) aim to create, it is often claimed, new forms of "money" that can be transferred between entities without requiring a trusted 3rd party.

Young Turks claim these kinds of innovative and disruptive systems may in the future replace many of the functions of banks (even central banks). Yet currently they comprise a negligible part of financial and monetary activity and raise many open issues.

In this talk I will, as a computer scientist with a background in agent-based modelling and P2P, outline the properties of existing and emerging systems, how they might be modelled, and speculate on possible future challenges and scenarios.

What is Peer-to-Peer

Firstly it is important to resolve a potential confusion. The term "peer-to-peer" (P2P) can be used in two different contexts.

P2P lending systems such as zopa.com refer to what might be better termed "person-to-person". They use traditional information systems and company structures to provide services allowing individuals to lend and borrow to and from each other. The company provides a platform. People make the deals within existing legal and contractual frameworks. I term these "first wave" systems.

P2P "money" systems such as Bitcoin refer to radically decentralised information systems with no traditional company structure or ownership. Such systems are composed purely of the software (clients) that individuals execute on their computers (peer nodes). The clients dynamically communicate to collectively provide services. In the case of Bitcoin, allowing users to perform transactions through a publicly accessible and verified shared ledger (the blockchain). I term these "second wave" systems.

Bitcoin

Bitcoin[1] is a decentralised P2P information system. It essentially supports a distributed ledger that records transactions between accounts. Transactions involve the transfer of "bitcoins" between accounts. Authorisation of a transaction from an account requires access to a private key associated with the account. Users of the Bitcoin client software can create any number of accounts with private keys stored on their client. The ledger of *all* transactions is publically available and stored in *every* client. Hence it is possible at any given time for any client to calculate the bitcoin balance of any account. This allows for a form of self-policing in which clients can block attempts to double spend.

---

[1] I do not intend to give a detailed technical description of Bitcoin. See Satoshi (2009).

Bitcoin produces and awards new bitcoin through a process termed “mining”. Essentially as part of the construction and checking of the public ledger (blockchain) new coins are awarded to those clients who participate productively. In general this means those with large computing resources earn coins. New coins are released in such a way that the total amount of coins will steadily increase until a maximum (21 million) is reached in the year 2140.

One way to view Bitcoin is as a system that creates a new kind of “base money” through an “institution” that is *mainly* algorithmically specified and controlled. Another way to view Bitcoin is as a bookkeeping innovation.

Bitcoin (and other “second wave” systems such as Bittorrent[2]) are often termed “open systems” because their source code is open for anyone to see, copy and modify. Also their protocols – that is the form and content of messages between clients – are open. This means that such systems can be seen as building blocks or services that can be easily incorporated into other software.

Many variants

Bitcoin has spawned many variants with subtly different properties[3]. Most variants differ in the way they award their respective coins and how many will be produced. Some variants “pre-mine” coins that are held and distributed by the creators. Others make them easier to mine for those who do not have access to significant hardware resources. One recent variant aims to award an equal amount of coins to every citizen of Iceland[4]. Many are “just for fun” while some are attempts to extract value from the gullible. In either case we can see the potential for “a hundred flowers to blossom”.

Socio-algorithmic group selection of variants

Interestingly *it could be argued* that this process may be sufficient to drive a kind of “cultural group selective” process in which those systems which fail will be replaced with new systems – recruiting users and value through imitation – supporting a vibrant ecology of variants (see Hales 2010 for an overview the kinds of models that might apply). In this case agents (users or people) by copying and installing a given variant client and creating or storing value within that system essentially cooperate to build the system. By hacking or moving value from the system they effectively defect reducing the utility of the system to others. By creating a new variant they offer a new choice to agents and initiate a new experiment. One could loosely compare aspects of this basic idea with the Tiebout model (1956). However this model assumes rational agents and compete information applied to a specific public goods scenario. Socio-algorithmic group selection implies myopic agents with very limited information.

Could such models be adapted to the Bitcoin variant scenarios[5]?

---

[2] A file sharing system that does not require servers (http://www.bittorrent.com).
[3] As of February 2014 over a hundred are known but only a handful appear significantly active (http://www.cryptocoincharts.info).
[4] Auroracoin.org (http://www.bbc.co.uk/news/technology-26083733).
[5] Of course, more detailed models of specific systems can be produced computationally (for example see work that compares game theory with simulation, for Bittorrent, in Rahman et al (2011)).

Recentralisation

Interestingly, due to the heavy computational demands and a certain degree of technical skill required to use Bitcoin clients, web-based "wallet services" have appeared[6]. Here the user trusts a 3rd party to look after their bitcoins reintroducing a degree of centralisation into the system. In a similar way "mining pools" have emerged which pool hardware to perform the significant amount of mining in the system reintroducing centralisation of infrastructure[7]. Also the major exchanges for Bitcoin and other variants are based on a traditional centralised model[8]. A further issue is that the complexity and need for on-going development of the Bitcoin software puts a degree of central control in the hands of the main developers. In fact when problems emerge they are required to act[9].

Is recentralisation of Bitcoin (and variants) inevitable?

Dynamic money supply

Existing variants of P2P money do not allow for the dynamic expansion and contraction of the money supply based on the needs of an economy. They specify a kind of algorithmically controlled "based money" that is either fixed or monotonically increases over time. A recent initiative aims to provide users with the ability offer credit lines in various currencies (both fiat and P2P) with others they trust (Ripple.com 2013). However, this system focuses on distributed payment and exchange rather than credit creation *per se* and relies on a centrally controlled "currency" called "ripples".

Is it possible to create a P2P system that allows users to act, effectively, as fractional reserve banks allowing them loan money into existence?

Price stability

Bitcoin currently evidences a high volatility on exchange markets. This restricts use as a payment system or unit of account. Rather it appears to have emerged as a speculative instrument.

Would it be possible to create a P2P system that could proactively attempt to stabilise such a currency using some form of distributed "open market operations"?

Distributed institutions

It has been speculated that the next wave of innovation in P2P could be characterised as Distributed Autonomous Organisations[10]. The form would depend on the kind of *governance structure* enabled by the software client and the way users exercise choices available to them. For example Namecoin (a variant of Bitcoin) provides the services of a Domain Naming System (DNS) without any central administration or control[11].

---

[6] They do not operate like banks but like safe deposit boxes (http://blockchain.info/wallet).
[7] Various pools exist some with large market share (https://blockchain.info/pools).
[8] One of the more popular exchanges: https://www.mtgox.com/
[9] For a report from the developers of a major fault on the Bitcoin network in March 2013 see: https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki
[10] https://www.ethereum.org/ethereum.html
[11] http://en.wikipedia.org/wiki/Namecoin

However, more sophisticated institutions could be created in which stakeholders could maintain shared control over transactions and other functions through joint authorisation of activities – described by computationally specified contracts. Examples could include majority vote or other processes such as, say, election of representatives.

Can the productive aspects of existing institutions be used as templates for new algorithmically enabled distributed institutions?

Conclusion

One way to view these developments and open issues, that occurs to me, is that, an interesting set of experiments are occurring that allow us to relearn some of the lessons that have historically shaped the institutions we have today. However, something is different: The speed of the evolutionary process and the new computational tools that facilitate them.

The invention of double entry bookkeeping and the joint stock company enabled new organisational forms. Could these recent developments lead to something as significant or is it a passing fad?

In either case I view these systems as a challenge to modellers. We have highly computationally specified systems evolving “in the wild”. Can we model, understand and improve them?

References

Hales, D., (2010) Rationality meets the Tribe: Recent Models of Cultural Group Selection. In Mollona, E., (ed) Computational Analysis of Firms’ Organization and Strategic Behaviour. Routledge. http://cfpm.org/~david/papers/tribe-proof-v1.pdf

Rahman, R., Vinko, T., Hales, D., Pouwelse, J. and Sips, H. (2011). Design Space Analysis for Modeling Incentives in Distributed Systems. ACM SIGCOMM 2011. http://cfpm.org/~david/papers/sigcomm2011.pdf

Ripple.com (2013) “Ripple: A Primer”. http://bit.ly/1kKByMD. [Retrieved 10/02/14]

Satoshi, N. (2009) "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf.

Tiebout, C. (1956) "A Pure Theory of Local Expenditures", Journal of Political Economy 64 (5): 416–424.