Crypto-economic Design: A Proposed Agent-Based Modelling Effort

Dave Babbitt, Northwestern University
Joel Dietz, University of Pennsylvania

A crypto-economy is an economic system which is 1) not defined by geographic location, political structure or legal system, and 2) uses cryptographic techniques to constrain behaviour (in place of using trusted third parties). Economic agents in these systems can be human-controlled clients and autonomous organizations or contracts. Prices of transacted goods and services in these economies are expressed in a built-in money-like informational commodity (a "crypto-currency") and all transactions are recorded on a public ledger.

They are important because they eliminate "bridging" social capital - the building of connections between heterogeneous groups - as a necessary precondition for successful economic development (Schuller, Baron, & Field, 2000). You no longer have to trust your valuables to strangers.

Crypto-economies have more than a need for software and security testing - they need to have their economies tested. Adding to the complexity of crypto systems (that a crypto-economy is based on) is the fact that exchanging value necessarily involves economic considerations. Therefore they must be analysed not only for computational soundness and security, but also for economic soundness (Poelstra, 2014). That is, they must be designed so that incentives are aligned with the goal of strengthening the security of the system and not inadvertently weakening it.

Agent-Based Modelling (ABM) often results in what is called "weak emergence" - appearance of new properties not fully reducible to that of the micro-properties on which it supervenes, but derivable only by simulation (Bedau, 1997). It is this weak emergence and the relative ease of capturing salient aspects of the actual system that allows development of crypto-economy-specific test scaffolding.

To capture salient aspects of crypto-economic systems we can categorize economic agents into "speculators", "miscreants", and "altruists". And open code sources of crypto-currencies can be written almost character for character into the agents built for the test, adding pauses in place of the cryptographic calculations. The cycle of enthusiasm and strong feeling around the adoption of the new economy can be incorporated as an institutional arrangement.

Speculators, for instance, can be modelled as standard profit-seeking economic agents. The altruists and malicious are harder agents to model. The altruists can be modelled with information cascades, where an agent observes the actions of others and then — despite possible contradictions in its own private information signals — engages in the same acts. As theoretical security holes are discovered, miscreants can be modelled as exploiting them.

Economic analysis of crypto-economies exposes various public goods issues that typically happen to a communal effort in danger of being lobbied by special interest groups. These public goods issues include 1) the financial incentives for operating a centralized mining pool, 2) the
centralization of infrastructure without the benefits of centralization (i.e., lower transaction costs, efficiencies of scale), and 3) the lack of financial incentives for working as a developer.

The first economists to study Bitcoin have attempted to discover what individual incentives exist without the use of agent-based models (ABMs). We conclude that these issues would’ve been readily apparent ("low hanging fruit") with the use of ABMs and that if you run an economic simulation of the design ahead of time, you will at least have a model-based exploration method to find the big issues.

Works Cited


