Crypto-Economic Design: A Proposed Agent-Based Modeling Effort

Swarmfest 2014

Dave Babbitt
Masters Thesis in Predictive Analytics
Northwestern University
Evanston, IL, USA

In collaboration with:
Joel Dietz, M.A.
University of Pennsylvania
Philadelphia, PA, USA
Introduction

• We are in the process of creating agent-based models of new crypto-currency designs.
• We are doing this to gain a better understanding of the incentivizations that economic actors will have.
  – Because current ideology-based models neglect this
Overview

• Models
  – Risks
  – Methodology
• Crypto-Economy Defined
  – Smart Contracts Defined
  – DAO Defined
• Why Crypto-Economies
• Why ABMs
• Crypto-Economic Validation
  – Risks
  – ABM Candidation
• Example Crypto-Economy
  – The SWARM Model
Models for Crypto-Economies

• Goals
  - Capture currency and banking fundamentals
  - Validate Asset Management and Security Criterion

• Approaches
  - Predictive Analytics using built-in metrics
  - Analytic Game Theory
  - Agent-based models
## Model Risks

<table>
<thead>
<tr>
<th>Statistical Terminology</th>
<th>Modeling Terminology</th>
<th>Associated Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type I: rejecting $H_0$ when $H_0$ is true</td>
<td>Rejecting a valid model</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>Type II: failure to reject $H_0$ when $H_0$ is false</td>
<td>Failure to reject an invalid model</td>
<td>$\beta$</td>
</tr>
</tbody>
</table>
What is a Crypto Economy?

An economic system which is not defined by

geographic location

political structure

legal system

Source: google images
What is a Crypto Economy?

An economic system which uses cryptographic techniques to constrain behavior (in place of using trusted third parties)

Source: google images
Economic agents in these systems can be

Human-controlled clients

Autonomous organizations (Equanoms, DAOs)

Smart contracts

Source: google images, “economic agent” – Original author unknown
What are Smart Contracts?

- A smart contract is a computerized transaction protocol that executes the terms of a contract (Nick Szabo, 1994).
- Satisfies common contractual conditions:
  - Payment terms
  - Liens
  - Confidentiality
  - Enforcement
- Minimizes malicious and accidental exceptions
- Minimizes the need for trusted intermediaries

Source: google images, “smart contracts” – Original author unknown
What is a Decentralized Autonomous Organization (DAO)?

Decentralized network of narrow-AI autonomous agents

Output-maximizing production function

Divides its labor into computationally intractable tasks (which it incentivizes humans to do) and tasks which it performs itself

Source: bitcoin.wiki.it, “DAC” – Dave Babbitt
What is a DAO?

It can be thought of as a corporation run without any human involvement under the control of an incorruptible set of business rules.

Source: Bitcoin and the Three Laws of Robotics – Stan Larimer
What is a DAO?

These rules are typically implemented as publicly auditable open-source software distributed across the computers of their stakeholders.

Source: Bitcoin and the Three Laws of Robotics – Stan Larimer
What is a DAO?

A human becomes a stakeholder by buying stock in the company or being paid in that stock to provide services for the company.

Source: Bitcoin and the Three Laws of Robotics – Stan Larimer
What is a DAO?

This stock may entitle its owner to a share of the profits of the DAC, participation in its growth, and/or a say in how it is run.

Source: Bitcoin and the Three Laws of Robotics – Stan Larimer
Crypto Economy Prices and Transactions

Prices are expressed in a built-in money-like informational commodity (a "crypto-currency")

All transactions are recorded on a public ledger

Source: google images, “crypto-currency” – Original author unknown
Why are Crypto-Economies Important?

They are important because they eliminate "bridging" social capital.

The building of connections between heterogeneous groups is no longer a necessary precondition for successful economic development.

Source: google images, “bridging social capital” – Original author unknown
You no longer need a common
• Culture,
• Values, and
• Self-identification

The computerized protocol takes care of
• Power sharing and
• Common priorities

Graphic representation of the necessary and sufficient causes for bridging social capital. Direction of arrows demonstrate induction. The indicators in the green field effect the appreciation of social capital.
Why are Agent-Based Models (ABMs) Useful?

• Discovery of important details
• View of big picture
• We have discovered that Analytic Game Theorists thinking really hard about a particular crypto-economy can find about one Nash equilibria a month
• Exploring the same space in an ABM, we can theoretically find the same in about one or two days
  – When I say “we” I mean me
  – NOBODY is doing ABM in this space
Why are Agent-Based Models (ABMs) Important?

• “Bitcoin’s developers combine technical implementation proficiency with ignorance of currency and banking fundamentals.” - Brian P. Hanley

• Devs are using phrases like “you don't need to model the web to design TCP/IP” to justify not worrying about the economic aspects of their design.

• But, merely the proper setting of limits, thresholds, and costs can prevent insecurities from developing.
Validation of Crypto-Economies

Analysis and Testing

Software Reliability
- Testing must cover full complexity of software

Computational Security
- Add to that the requirements for an adversarial model

Economic Soundness
- Add to that requirements for properly incentivized actors
Double-spend Attack Risks from Small Hashrates

Incentives must simultaneously secure from attackers and process transactions

Disinflationary coins periodically half their block rewards

Hashrate halves when the block reward halves
What is True for Crypto-Economies that makes Agent-Based Modeling (ABM) Appropriate?

- Natural representation as agents
- Decisions and behaviors can be defined discretely (with boundaries)
  - Crypto-economies have a data exhaust
  - which can parameterize statistical models
  - which can be linked to process sub-models
- It’s important that crypto-actors be able to adapt and change their behavior
What is True for Crypto-Economies that makes Agent-Based Modeling (ABM) Appropriate?

- It’s important that crypto-actors learn and engage in dynamic strategic behavior
- The past is no predictor of the future
- Scaling up to arbitrary levels is important
Walk-through Modeling SWARM

- Swarm is like Kickstarter
  - But for research
  - And issuing crypto currency to represent your stake in the investment

www.swarmcorp.com
• Think of SWARM as a vending machine that accepts BTC.
• Each coin (such as RESEARCHcoin or SWARMcoin) has a price.
• All an investor has to do, is put in the bitcoins
• They get back whatever coins they’ve chosen.
So Swarm is a mix of a traditional stock exchange, a pop vending machine, Kickstarter and a hedge fund, with a splash of BTC and speculator social network thrown in the mix.
Our economic agent (shareholder in this case) uses Counterwallet to trade BTC for SWARM coin.
Shareholder Agents

Actions: Convert, Invest
Another agent to model is the one trying to raise money.

1. Build profile and fundraiser description on the website
2. Select a unique name for their coin - e.g. RESEARCH
3. Select how many coins to issue - e.g. 100 million
4. Swarm platform creates the coin on Counterparty
5. Platform retains 1% (1 million) coins
6. Platform distributes coins as dividend to SWARMcoin holders
7. Crowd-sourced Due Diligence off the Swarm network
8. Swarm initiates it’s own Due Diligence process
9. Cancer Research selects model for the VEND of the coins
   1. Linear,
   2. Logarithmic, etc.
10. COIN LAUNCHED
Fundraiser Agents

Actions: Convert, Invest
Another agent to model is the core developers themselves

- Limited number (150K, est) of devs capable of programming the blockchain
- Work on donation basis
- Assume users are like themselves
  - Anti-central banking
  - Omni-competent in private key management
# Outlining the Behavior of Our Shareholders and Fundraisers

<table>
<thead>
<tr>
<th>Agent</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWARM Platform</td>
<td>• Distributes 1% of Fundraiser’s coins as dividend to SWARMcoin holders</td>
</tr>
<tr>
<td></td>
<td>• Vends Fundraiser’s coins to market at predetermined schedule</td>
</tr>
<tr>
<td>Shareholder</td>
<td>• Uses Counterwallet to trade BTC for SWARMcoin</td>
</tr>
<tr>
<td>Investor</td>
<td>• Uses Counterwallet to trade BTC for Fundraiser’s coin</td>
</tr>
<tr>
<td>Fundraiser</td>
<td>• Builds profile on Platform</td>
</tr>
<tr>
<td></td>
<td>• Tells Platform how many coins to create</td>
</tr>
<tr>
<td></td>
<td>• Tells Platform how to vend them</td>
</tr>
</tbody>
</table>
### Possible Parameter Slider Settings

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Minimum Value</th>
<th>Maximum Value</th>
<th>Initial Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>initial-shareholder-btc</td>
<td>0.5</td>
<td>5000</td>
<td>1</td>
</tr>
<tr>
<td>Initial-investor-btc</td>
<td>0.5</td>
<td>5000</td>
<td>10</td>
</tr>
</tbody>
</table>
Emergence

"weak emergence" – the appearance of new properties not fully reducible to that of the micro-properties on which it supervenes, but derivable only by simulation (Bedau, 1997)