Loughborough University

Alistair Milne

Discussion of Andrea Canidio "Financial Incentives for Open Source Development: the case of Blockchain"

Bank of Finland/ CEPR conference,
Money in the Digital Age, 12th-13th June 2018

Set up 1

- Three players engage in a ‘protocol’:

1. The developer with an initial cash holding A_0
2. A mass of risk-neutral price-taking investors
3. A mass of users.

- The development lasts $\tau \leq T$ periods, after which the developer exits the game, users and investors remain
- Transactions using the protocol for $t > \tau$ must be conducted using a protocol specific token with a market price p (this is the “blockchain” element of the paper).

Set up 2

- In period $t_0 \leq T$ chosen by the developer initial coin offering (ICO) creating M of these tokens. Monetary value of transactions using the protocol depends on the cumulative past effort and investment:

$$V_\tau = \sum_{s=1}^{\tau} f(e_s, i_s)$$

- There is also 'speculative' demand for tokens, with investors, not users, holding a proportion γ of all tokens. This implies that the price of tokens (determined by user demand) $t \geq T$ is given by

$$p = \frac{V}{(1-\gamma)M}$$

Set up 3

- In each period the developer decides effort e_t, investment i_t, consumption c_t and token holding $Q_t \leq M$ determining cash holdings:

$$A_t = A_{t-1} - i_t - c_t + (Q_{t+1} - Q_t)p_t \geq 0$$

(inequality because no access to credit),

- maximising undiscounted expected utility, linear in consumption, quadratic in effort:

$$\sum_{s=t}^{T} \left(c_s - \frac{1}{2}e_s^2\right)$$

Solution for 'rich developer' A_0 large

- Solution for rich developer (prop 1) mixed strategy, holding all tokens but developer cashing out at $\tau = t < T$ with probability

$$\alpha_t = (1-\gamma)\frac{\frac{1}{2}e^*(M)^2 + i^*(M)}{f\left(e^*(M), i^*(M)\right)}$$

- with the associated price of the tokens increasing over time:

$$p_t = \frac{V_t + (1-\alpha_t)(T-t)f\left(e^*(M), i^*(M)\right)}{(1-\gamma)M}$$

- but this solution turns out to be "off equilibrium" collapses (prop 2) to the ICO taking place either in $T-1$ with the developer holding all tokens until T or in T with all tokens sold.

Solution for 'poor developer' A_0 small

- Explored for the case of $T = 3$ and investment a binary choice of $i \in \{0,1\}$ with
$$f(e,i) = g(e)i$$

- two cases: ICO in period $t = 2$ or $t = 1$. f $a > 2$ then the ICO is held at $t = 2$, otherwise at $t = 1$ i.e. ICO is delayed as long as possible while financing investment period 1 (Proposition 6).

- If $A_2 - i_2 \leq 1$ then multiple equilibria (two different mixed strategy equilibria) are possible (Proposition 4). An 'anti-coordination' or expectations problem

"*If investors expect the developer to develop the software in the future, this expectation should be priced into the token's current price. But if this is the case, then the developer is strictly better off by selling all his tokens, which allows him to "cash in" on the future development without doing any. On the other hand, if investors expect no development to occur, the price of the token will be low.*"

Comments 1 – technical/ presentational

- This draft is a bit of a struggle to read (took me four hours to write my five summary slides)
- Maths untidy – please make reader's life easier !
  - e.g. c_t redundant, $e^*(t)$ not $e^*(M)$, A_0 not a, γ also (?) redundant
- Focus more on the economics in model presentation
  - Separate more clearly results from technical development and proofs (latter might go in an appendix)
  - My advice start with simplest case (three periods, binary investment choice). Only later, separate section, generalise
- Is this really multiple equilibrium? Is problem not that of pre-commitment, without this only low price equilibrium?

Comment 2: real world relevance?

- ICOs in practice *not* often linked to use of protocol
  - Example Ripple's XTM
  - Most / many ICOs seem to be scams, a way of escaping investor protection regulation, or just fraud (example "Onecoin")
  - Real world ICO similar to your model (I cannot find one)?
- Blockchain itself may be failing
  - Milne and Mainelli (2016). Essentially a shared databased.
    - Absence of trusted third party just an implementation detail. Adds relatively little when applied in regulated finance.
  - Example: "pausing" of the DTCC blockchain project for repo.
- Generic problem – technical solutions looking for application
  - Applies to developers and to economists !!

Comment 3 (my work, loosely related)

- Cryptographic technology and full reserved banking

  Milne (2017), “Cryptocurrencies from an Austrian perspective”, SSRN
  - Record keeping role of monitoring transaction on ledger not in commercial banks
  - Commercial bank liquidity/ money creation through securitisation onto this ledger
- *and* (coming soon) quantity based monetary policy
  - Misunderstanding of the zero-lower bound
    - An expectational problem (negative interest rates do not help)
    - Is problem interest rate rather than quantity based monetary rule? We do not solve problem of debt overhang undermining demand through creating more debt.
  - We need to encourage more reliance on the non-portfolio channels of monetary policy, via transactions/ precautionary not portfolio demand,
    - Requires breaking close substitution between money and govt bonds
    - Technology can perhaps solve this e.g. penalty on non-circulated money
    - Also – make gov bonds but *not* money defaultable.
- Money in the digital age is a public policy challenge: improving financial architecture, will not happen through market mechanisms

Thank you!

Alistair Milne
a.k.l.milne@lboro.ac.uk

Loughborough University

Inspiring Winners Since 1909