Market Design with Blockchain Technology

Katya Malinova and Andreas Park
We first presented this paper in June 2016 ... 
... and for 1 year people told us that trading of blockchain "stocks" was years away.
Initial Coin Offerings are now a reality

- Available tokens for trading (Coinmarketcap)
  - August 19: 182
  - Sept 25: 257
- Capital raised from mid-2016 to date:
  - $1.3B (NYT July 27, 2017);
  - $2.5B (Coinmarketcap, Sept 26, 2017)
- Market cap (Coinmarketcap, Sept 26, 2017)
  - ~$8B
What is different?

1. Multiple trading protocols are possible

User-facing exchange mask

Fully Decentralized, "OTC", Peer-to-Peer Exchange
What is different?

2. High Level of Transparency

See transactions *between "addresses" (="IDs")*
What is different?
3. You can tell who owns what
To sum up: What is different?

1. Exchange-trading and Peer to Peer is possible
   • current world peer-to-peer -- through intermediaries
     ▪ a dealer/market maker is on one side of trade
     ▪ parties know who they are trading with
   • technology enables frictionless value transfer
2. Past transactions are visible
   • may be able to see frequent "traders"
3. Current holdings are visible
   • may be able to tell who the "whales" are

=> Informational environment changes drastically

Key: wallets/addresses = IDs but NOT = traders
Research Question

• possible ledger transparency regimes:
  ▪ visible to all
  ▪ hidden (from some)

• possible identifier-usage regimes:
  ▪ mandate single IDs per entity
  ▪ allow multiple IDs
    ◦ allows to obfuscate holdings (Buterin 2015)

How does the design of ledger transparency and identifier-usage with possible P2P interactions affect trading behavior and economic outcomes?

Who benefits and loses under which regime?
Model Ingredients

- Risky asset, value normally distributed $N(0, \sigma^2)$
- Two large investors
  - Each period one is hit with size $Q=1$ liquidity shock.
  - Other can absorb the shock at zero cost.
- Continuum of $1/\rho$ small investors $\rho \leq 1/2$
  - trade with probability $\rho$ at "public" price
  - each period, mass 1 wants to buy, mass 1 wants to sell
- Infinitely many trading periods

Disclaimer:
- no asymmetric information
- => our results need not be applicable to all asset classes
Model Ingredients: Trading and Timing

- When hit with a shock, the "liquidity trader" (LT) may:
  - trade peer-to-peer (OTC) (with small and/or large peers)
    - other large: "liquidity provider" (LP)
  - trade with a risk-averse intermediary at
    \[ p(q) = \frac{\kappa \sigma^2}{N} (-I + q) \equiv \frac{\ell}{2} (q - I) \]
    - Intermediary's inventory \( I \) "shifts" the public price
  - net-trades with intermediary = inefficient transfer of risk
- Unfilled positions clear with intermediary at end of stage game.
Model Ingredients: Costs

Direct

• Data processing/complexity to contact $q$
• Quadratic cost to contact mass $q$ of IDs:
  ▪ cost $c$ is a loss to aggregate welfare
  ▪ pay $\frac{c}{2} q^2$ and trade quantity $\rho q$
• Linear mining/validation cost:
  ▪ pay $\gamma q$ to trade with $q$ IDs

Indirect

• LT to LP: Buy quantity $Q$ at price $p$?
  1. LP buys $Q$ from intermediary and moves the "public price" $P$ to $P + \ell/2 \times Q$
  2. LP to LT: "sell you $Q$ at price $\gg p$?"
• Front-runner pays validation costs.

Idea:
• keep "risk" of transparency within trading model
• for investors, can think of other costs, e.g., stealing of investment strategies
Model Ingredients: Transparency of Ownership

1. Full transparency = common knowledge of who is large
   - assume single ID (since validation costs increase in # of IDs)
2. No transparency
   - only single ID allowed
3. No transparency (ownership cannot be inferred)
   - continuum of IDs (to obfuscate ownership)
Requires a system design choice:

- allow an entity (individual, investment fund) only a single ID per instrument
- possible with private blockchain

Benchmark: fully transparent (single ID) ownership
Options for Large Trader

Trade with small investors and intermediary

- costs:
  - complexity + validation
  - intermediation

Trade with large investor

- costs
  - reveal info about the trading needs
  - [model choice]:
    LT may get “front-run” by LP.

Single shot:
LP always extracts all surplus (or would front-run).

Repeated setting:
Front-running is punished by “grim trigger” & trade forever with small and intermediary.
The Benchmark Equilibrium

1. In a repeated game, "social norms" have bite and front-running can always be avoided.
2. LT always trades with LP.
3. LT and LP share the cost savings.
4. Price concession
   - For small discount factor (≈ infrequent interaction) price concession is necessary.
   - For large enough discount factors (≈ frequent interactions), price concession = 0 is an equilibrium.
Opaque single ID ownership
The optimal mass of IDs to contact is independent of the intermediary’s inventories/public price.

Mass $x^*$ depends on:

- $\rho$: probability of small traders accepting the offer
- $\ell$: the (il-)liquidity of the intermediated market
- $c$: complexity/data processing costs.

$$x^* = \max\{0, \frac{\ell \rho}{\ell \rho^2 + c} - \frac{\rho \gamma}{\ell \rho^2 + c}\}$$

When the validation cost is not too large, $\gamma < \ell$, the liquidity trader trades with both continuum & intermediaries.
Opaque multi-ID ownership

Closest and native to "public" blockchains:

- anyone can participate anonymously
- can create as many accounts as I want
- described by Ethereum founder as simple solution to achieve privacy
- private blockchains can choose to organize like this
Acceptance Probabilities: depend on LP's decision

- Opaque Single ID
- Opaque Multi-ID: LP accepts
- Opaque Multi-ID: LP rejects

\[
\begin{align*}
\frac{2\rho}{1+\rho} & > \rho \\
\frac{\rho}{1+\rho} & < \rho
\end{align*}
\]
Decision problem LT

submit large amount to continuum
- (small) price concession to entice larger trader (but also paid to and "wasted on" small traders)
- larger search costs

submit large amount to continuum
- no price concession
- expensive interaction with intermediary
- smaller complexity cost

Decision problem LP

accept offer
- incurs validation fee when front-running

front run
Equilibrium & More

**Result 1:** There exists an equilibrium with no front-running where

- LP accepts
- price concession = 0

provided

- the discount factor is large enough
  - = frequent interactions.
- or the intermediated market is sufficiently liquid
  - = front running not very profitable (small quantity and low price advantage)
- or validation costs are sufficiently *high*
  - = sunk cost for front-running too high.
Result 2 (numerical): For small discount (=infrequent interaction) factors, the equilibrium with no front-running where LP accept does not exist. Then:

- In equilibrium, LT offers \( p = 0 \) to the continuum, and
- LP's IDs reject the offer.

=> over-trading with intermediary

- Observation: an increase in the validation cost may curb front-running.
Comparing the designs

Observations

- Trades with intermediary => socially inefficient
  - better if large traders interact
  - otherwise: intermediary faces imbalance
- Small with large traders => complexity costs
- By construction, payoffs under the full transparency benchmark are highest.
- The trade-off for opaque regimes are:
  - complexity cost vs
  - intermediation cost
Comparing multi- vs single-ID opaque designs

• Finding 1:
  ▪ When large traders do not trade with each other, the welfare is the same in both opaque systems, irrespective of the ID-ownership setup.

• Finding 2:
  ▪ When large do trade with one another with multi-ID ownership, the welfare in this setting is higher than in the single-ID setting.
Payoffs to Large Traders

Finding 3:
For the average equilibrium stage payoffs of large traders.

1. In multi-ID, when large traders do not interact, eq. payoffs lower than in opaque single-ID.
2. In multi-ID, when large traders interact and $p=0$, eq. payoffs larger than in opaque single-ID.

Finding 4: (Numerical)
There exist parametric configurations such that large traders trade with each other at $p > 0$ in the multi-ID ownership setting, but their average equilibrium payoff in the opaque single-ID setting is higher.
Summary

1. "Back office" settlement has important front office implications!
   - with peer-to-peer there are critical design choices
     - Who can see the ledger?
     - How are virtual identities managed?

2. Findings:
   - Transparent ledger with single IDs is welfare optimal and has lowest wealth redistribution (almost by construction)
   - Between (A) public blockchain solution with multiple IDs and (B) private, non-transparent ledger with single IDs:
     - **public blockchain privacy solution** has higher aggregate welfare
     - but does not necessarily lead to higher payoffs for large investors.