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



- 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)

Initial Coin Offerings are now a reality

■ ~\$8B

Cryptocurrency ICO Stats 2017



Totals raised are grouped by the ICO closing date and are valued using BTC exchange rate at that time. Data correct on 7th September 2017 14:00 UTC

What is different?

1. Multiple trading protocols are possible

User-facing exchange mask

t Et	ther Delt a	a 🔳 🗆	BNT -					Chat	🗐 🗐 He	elp 🗸 🌘	🕽 Tokens 👻	🖹 Smar	t Contract 👻	🖄 English	 Select 	account 👻
BALANCE				ORDER BOOI	ĸ		PRICE CHART						TRADES			
Deposit	With	hdraw	Transfer		506.452	7.597	Pric	e			Depth		BN	T/ETH	BNT	ETH
Please select	an account us	ing the account	drondown in		10.000 10.000	0.150 0.140							0.0080		9.969	0.0802
		per right.	. al op a official in		10.000	0.135							0.0089	10490个	90.052	0.802
					10.000	0.130							0.0080		92.851	0.743⊡
					500.000	6.250							0.0060	000024	0.239	0.002
					1000.000	12.400	0.0135							00000 ~ 00000 ~	2.066 10.000	0.026⊡ 0.123⊡
					270.000	3.348							0.0125	00000	39.000	0.123
					10.000	0.123							Note: Eth	erDelta will o	nly show recent t	
					123.000	1.513			-				Note. Lui		ily show recent t	ansacuons.
					10.000	0.119	0.0120									
					3500.000	41.580										
				0.011800000	10.000	0.118	-									
				BNT/ETH	BNT	ETH	_									
				0.008000000	407.149 10.031	3.257	0.0105									
				0.008000000	10.031 250.000	0.080 1.950										
				0.007800000	2200.000	15.620										
				0.007020000	200.000	1.404										
				0.006670000	250.000	1.667	0.0090				_					
				0.006660000	150.000	0.999	_									
				0.003010000	1200.000	3.612										
				0.001900000	1000.000	1.900										
VOLUME				0.001780000	1000.000	1.780	0.0075									
VOLONIE				0.001100000	5000.000	5.500	00:00	04-00	00.00	0.00 04	:00 05:00	06:00				
Pair	Daily	Bid	Offer	0.000900000	1000.000	0.900	00:00	01:00	02:00 0	03:00 04	:00 05:00	06:00				
ZRX/ETH	7341374	0.001830000	0.001600000	0.000800000	1000.000	0.800										
CDT/ETH	17985448	0.000441000	0.000490000	0.000400000	1000 000	0 100										
PPT/ETH	114323	0.015410000	0.015700000	NEW ORDER			MY TRANSACTIC	אוכ								
DNT/ETH	3552638		0.000548000	Buy	Se	-										
VERI/ETH	2386		0.424999999	Cay			Trades		Orders	\$	Fu	nds				
STX/ETH	93923		0.008000000	BNT	Amount to	hund						NT/ETH				
IXT/ETH	477267		0.001588000		Amount to	buy	Transaction		·							
CAT/ETH	101786		0.005100000				Note: E	EtherDelta w	vill only sho	ow recent t	ransactions.					
PLR/ETH	969024		0.000560000	BNT/ETH	Price											
TIX/ETH	312178 294595		0.001800000													
XRL/ETH DENT/ETH	294595 99743738		0.001500000 0.000004999	ETH	Total											
PAY/ETH	99743738 26977		0.000004999													
ADX/ETH	67897		0.0011938990	Expires	10000											
OMG/ETH	11103		0.025000000													
OAX/ETH	24291		0.007000000		Buy											
CVC/ETH	77575		0.001800000													
EOS/ETH	19693	0.004600100	0.004990000													

Fully Decentralized, "OTC", Peer-to-Peer Exchange





The Protocol for Trading Tokens



WHITEPAPER

What is different?

2. High Level of Transparency

See transactions *between "addresses" (="IDs")*

Etherscan		HOME			ddress / Txhas	sh / Block / Tok CHART	en / Ens MISC	GO
TOKEN Bancor						Home / Tok	enTracker /	Bancor
okenTracker Summary							Reputation	ok 🐽
otal Supply: 78	,119,117.3153 BNT (\$193,860),401.53)	Contract Address: 0x1f573d6fb3f13d689ff844b4ce37794d79a7ff1c					
alue per Token: \$2	.4816 @ 0.008665 Eth (-7.61%	6)	Token Decimals:	18				
oken Holders: 12	842 addresses		Official Links:	0 2 2 0	* ¥ ₿			
	580 Iders Read Smart Contra	act Comments	Search/Filter By:	Enter Token Ac	ddress or TxHa	sh Apply		
o.Of.Transfers: 79	Iders Read Smart Contra	act Comments	Search/Filter By:	Enter Token Ac	First Prev		92 Next	_ast
o.Of.Transfers: 79 Token Transfers Token Ho J.F. A Total of 79580 events fou	Iders Read Smart Contra		То	Enter Token Ac	First Prev	Page 1 of 15 antity	92 Next	ast
o.Of.Transfers: 79 Token Transfers Token Ho IF A Total of 79580 events fou TxHash	Iders Read Smart Contra nd Age	From	То		First Prev Qua	Page 1 of 15 antity	92 Next	_ast
o.Of.Transfers: 79 Token Transfers Token Ho IF A Total of 79580 events fou TxHash 0xc68e75284311c4	Iders Read Smart Contra nd Age 2 mins ago	From 0x3b0899f81f2dc9d	To Ox1f573d6 Ox060001	6fb3f13d6	First Prev Qua 144 77.1	Page 1 of 15 antity 3	92 Next	Last
o.Of.Transfers: 79 Token Transfers Token Ho J.F. A Total of 79580 events fou TxHash 0xc68e75284311c4 0x6b7f845687265d	Iders Read Smart Contra nd Age 2 mins ago 4 mins ago	From 0x3b0899f81f2dc9d 0x5concentionnac	To 0x1f573d6 0x3b0899f	6fb3f13d6	First Prev Qua 144 77.1	Page 1 of 15 antity 3 72585794 .43420543	92 Next	_ast
o.Of.Transfers: 79 Token Transfers Token Ho J.F. A Total of 79580 events fou TxHash 0xc68e75284311c4 0x6b7f845687265d 0x7b51a5654fdc7d	Iders Read Smart Contra nd Age 2 mins ago 4 mins ago 4 mins ago	From 0x3b0899f81f2dc9d 0x5c5r 52r9bf9f4ac	To 0x1f573d6 ↓ 0x3b0899f ↓ 0x3b0899f	6fb3f13d6 186666108 1881f2dc9d	First Prev Qua 144 77.1 650 9.98	Page 1 of 15 antity 3 72585794 .43420543	92 Next	Last
D.Of.Transfers: 79 Foken Transfers Token Ho IF A Total of 79580 events fou TxHash 0xc68e75284311c4 0x6b7f845687265d 0x7b51a5654fdc7d 0xaf41da965d47f7c	Iders Read Smart Contra nd Age 2 mins ago 4 mins ago 4 mins ago 4 mins ago	From 0x3b0899f81f2dc9d 0xccorrocrobiorrac 0xccorrocrobiorrac 0x5e575279bf9f4ac 0x3107c141c57c20	To 0x1f573d6 ↓ 0x3b0899f ↓ 0x3b0899f ↓ 0xcbe27c5 ↓ 0x1f573d6	6fb3f13d6 166665108 1f81f2dc9d 50302e33	First Prev Qua 144 77.1 650 9.99 412	Page 1 of 15 antity 3 72585794 0.43420543 5	92 Next I	Last

What is different? 3. You can tell who owns what

TOKEN Bancor Home / TokenTracker / Bancor Reputation OK TokenTracker Summary Contract Address: 0x1f573d6fb3f13d689ff844b4ce37794d79a7ff1c Total Supply: 78,119,117.3153 BNT (\$193,860,401.53) 18 \$2.4816 @ 0.008665 Eth (-7.61%) Token Decimals: Value per Token: Token Holders: 12842 addresses Official Links: 0 🛛 C 🖸 🋠 y B No.Of.Transfers: 79580 Search/Filter By: Apply Enter Token Address or TxHash **Token Transfers** Token Holders Read Smart Contract Comments TokenHolders Chart Page 1 of 257 Next Last First A total of 12842 Token Holders found Rank Address Quantity Percentage 0x5894110995b8c8401bd38262ba0c8ee41d4e4658 20.3103% 15865957 1 2 0x79e7ccb8e7a61ad4781c98864c40e380bb10dd26 14312616.4803711 18.3218% 3 0xad04835b1129c08be6093d683d725ff82cd24036 10539657.098791 13.4920% 10.0536% 4 0x7af1362060ec77ca30be2508cce10169210393ee 7853648.22 5 0xfbb1b73c4f0bda4f67dca266ce6ef42f520fbb98 4227754.51610493 5.4120% 6 0x7bb42206cddc93380ed1115d15fb1e65a1d754fc 1312102.22092 1.6796% 7 0x0c43eb0b18774a15bca2e639ba470796147b8d24 1207481.05212123 1.5457% 8 0x31fc2dbe295a8570b69c09c5aaec33459fc1a1b3 750000 0.9601% 9 0x696618b03604354787b631695bfc9d14c203360a 659100.152343954 0.8437% 10 0x86842054dd8802519dc7dcc458dc9311c1434639 426100 0.5455%

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/ ho small investors $ho \leq 1/2$
 - trade with probability ρ at "public" price
 - each period, mass 1 wants to buy, mass 1 wants to sell
- Infinitely many trading periods

our results need not be

plicable 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

$$p(q) = rac{\kappa\sigma^2}{N} \; (-I+q) \equiv rac{\ell}{2} (q-I)$$

• 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 ρq
- Linear *mining/validation* cost:
 - pay γq 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 $P + \ell/2 imes Q$
 - 2. LP to LT: "sell you Q at price $\gg p$?"
- Front-runner pays validation costs.

Idea:

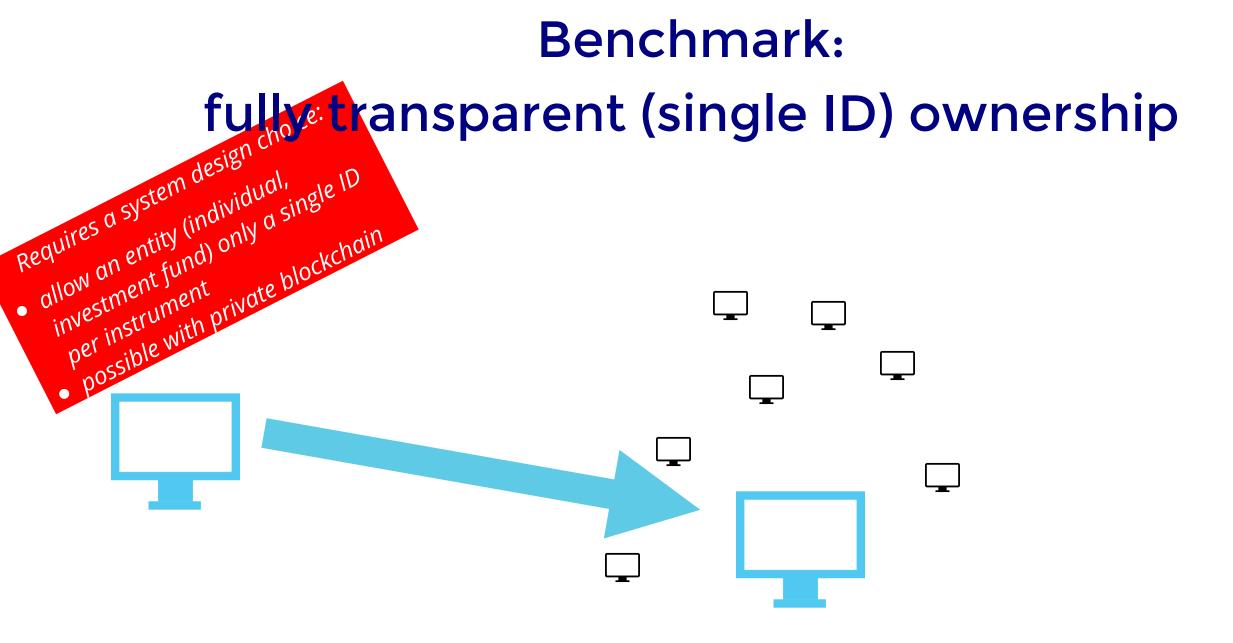
keep "risk" of transparency within trading model

4.3

 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)



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).

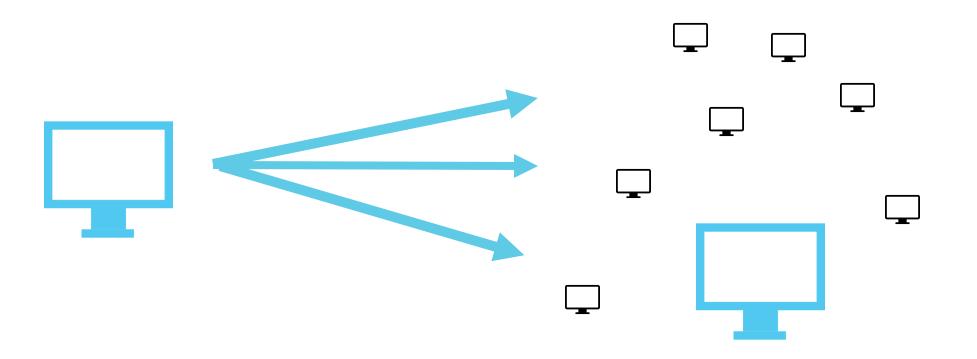
Repeated setting:

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 frontrunning 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



Equilibrium

- The optimal mass of IDs to contact is independent of the intermediary's inventories/public price.
- Mass *x** depends on:
 - ρ: probability of small traders accepting the offer
 - ℓ : the (il-)liquidity of the intermediated market
 - c: complexity/data processing costs.

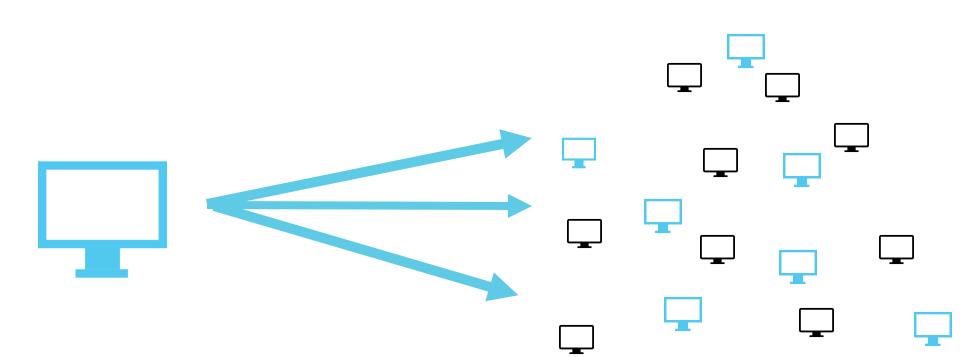
$$x^* = \max\{0, rac{\ell
ho}{\ell
ho^2+c} - rac{
ho\gamma}{\ell
ho^2+c}\}$$

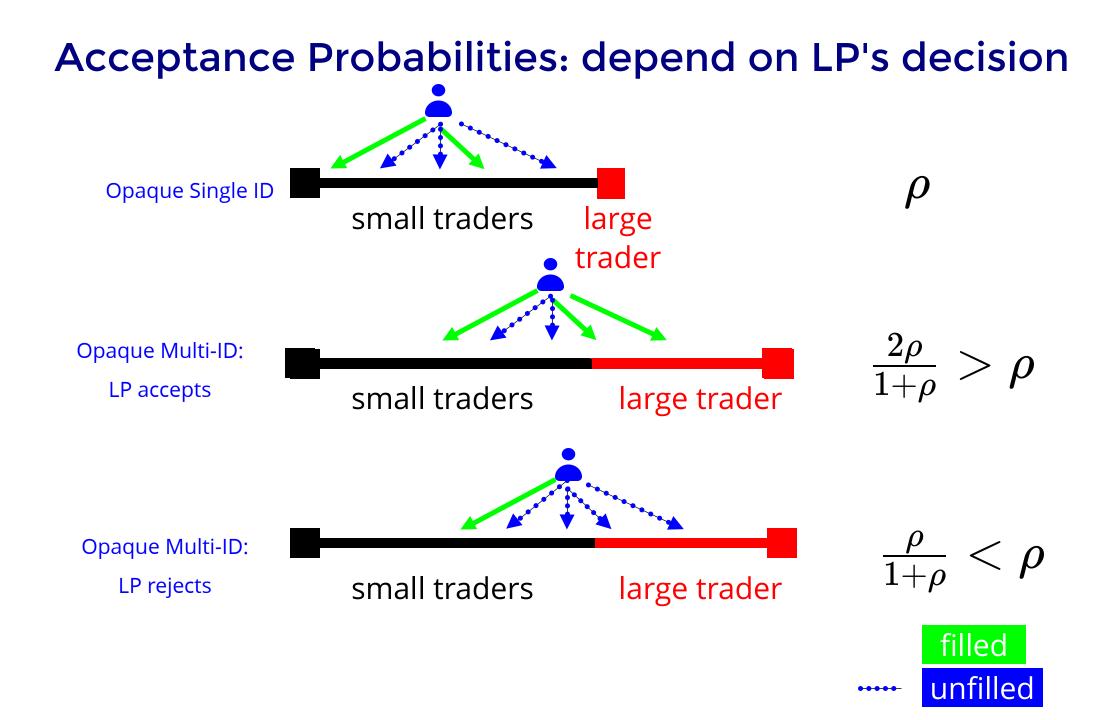
• When the validation cost is not too large, $\gamma<\ell$, the liquidity trader trades with both continuum & intermediaries

Closest and native to "public" blockchains:

- anyone can participate anonymously
- can create as many accounts as l want
- described by Ethereum founder as simple solution to achieve privacy
- private
 blockchains can
 choose to
 organize like this

Opaque multi-ID ownership





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 front run • incurs validation fee when frontrunning

Equilibrium & More

Result 1: There exists an equilibrium with no frontrunning 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.

Equilibrium & More

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, nontransparent ledger with single IDs:
 - **public blockchain privacy solution** has higher aggregate welfare
 - but does not necessarily lead to higher payoffs for large investors.