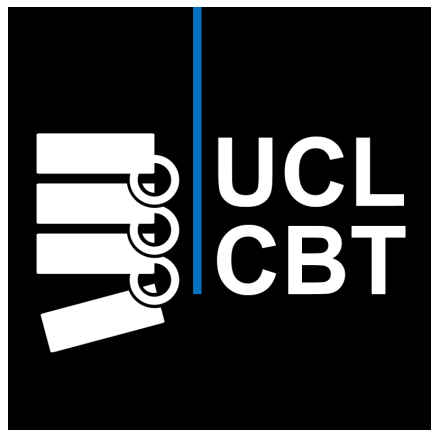
Economic Foundations of the Bitcoin Economy

Paolo Tasca

UCL Centre for Blockchain Technologies

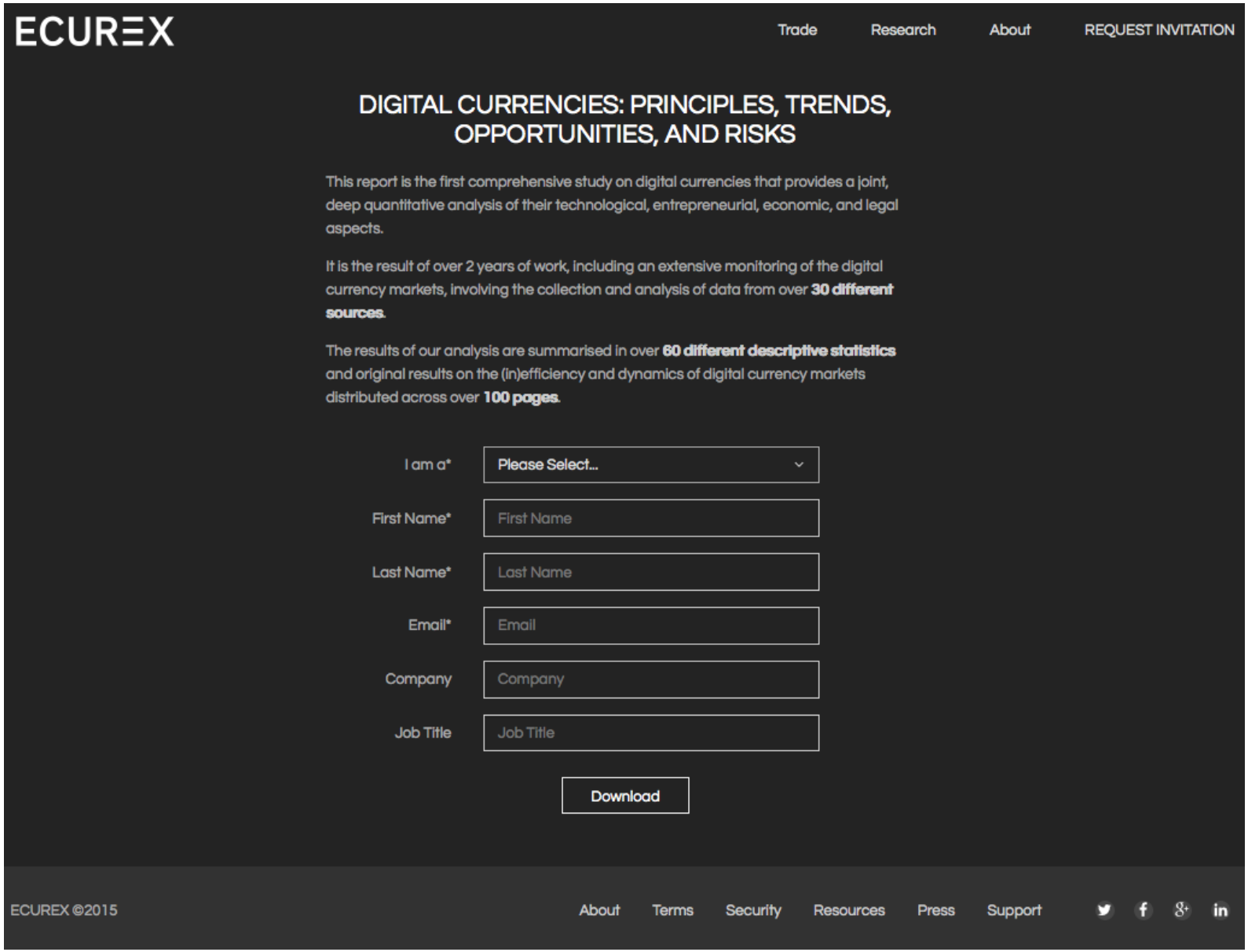


Blockchain: the Next Financial Revolution ? :: Zurich

June 16, 2016

1. Currency Competition
   - Which Type of Currency?
   - Private Currencies
   - Gresham's Law and Thyer's Law
   - Hayek Theory
   - Milton Friedman
   - Ron Paul
   - Data
2. Price Stability
3. Currency Circulation
4. Bitcoin as Payment Network

https://ecurex.com/2015report



Currency Competition

Currency Competition - Which Type of Currency?

	Private Currency	**Public/State Currency**
Fiat Currency	Ithaca Hours,[1] Time Dollars, etc..	USD, GBP, EUR, etc..
Asset-backed Currency	Liberty dollar (1998-2009)	U.S. paper currency (1863-1933)

Table: Types of currencies.

- **Fiat Currency**: Intrinsically valueless money.
- **Asset-backed Currency**: It is a commodity currency which value is based on a good, often a precious metal such as gold or silver.
- **Private Currency**: It is a currency issued by a private centralised or **decentralised** organisation.
- **Public currency**: Tax–driven money issued by Central authority in monopoly.

[1] This is a special type of labour vaucher.

Currency Competition - Which Type of Currency?

	Private Currency	**Public/State Currency**
Fiat Currency	Ithaca Hours,[2] Time Dollars, etc..	USD, GBP, EUR, etc..
Asset-backed Currency	Liberty dollar (1998-2009) Digital Currencies	U.S. paper currency (1863-1933)

Table: Types of currencies.

- **Fiat Currency**: Intrinsically valueless money.
- **Asset-backed Currency**: It is a commodity currency which value is based on a good, often a precious metal such as gold or silver.
- **Private Currency**: It is a currency issued by a private centralised or **decentralised** organisation.
- **Public currency**: Tax–driven money issued by Central authority in monopoly.

[2] This is a special type of labour vaucher.

Currency Competition - Which Type of Currency?

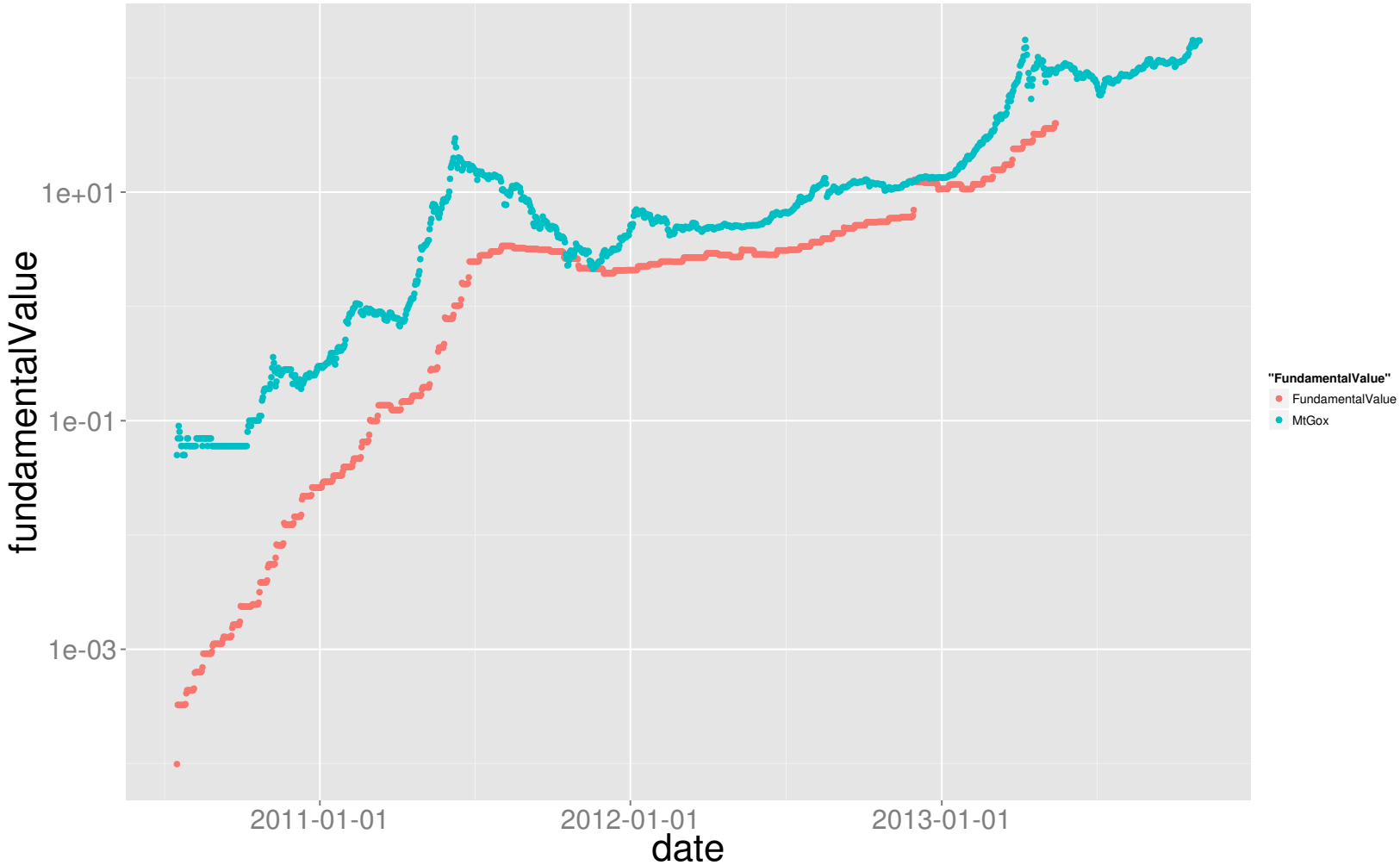


Figure: Money backed by energy.

Currency Competition - Which Type of Currency?

Algorithm:

1. Get the total (daily) hash rate from `https://bitcoinchain.info`, divide it by the (daily) number of BTC mined and adjust units to get an estimate of the number of SHA-256 hashes needed on average to mine 1 BTC.
2. Assume that a miner needs about 0.5W of power to get 1 MHash/s.[a]
3. Adjust units and assume a mean cost of 0.15$/KWh to get the lower bound estimate.

[a] This is slightly overvalued with AMD Radeon cards, largely undervalued for NVIDIA cards and of course CPU mining, which has become more or less irrelevant in 2009. This means that this calculation only holds for the period mid-2010 to beginning 2013, at which FPGA and ASICS mining is still minor compared to GPU mining.

The fundamental value becomes trustable only from about when the Radeon HD 58xx cards were introduced and became the mining standard (mid-2010-beginning 2013).

Currency Competition - Private Currencies

Irregardless of legal tender status, money refers to whatever is commonly accepted as a medium of exchange, unit of accounting and store of value:

- Today, there are over **4,000** privately issued currencies in more than 35 countries. These include commercial trade exchanges that use barter credits as units of exchange, private gold and silver exchanges, local paper money, computerised systems of credits and debits, and **digital currencies** in circulation, such as digital gold currency.
- Currently there are more than **500** digital currencies available for trading in online markets (mostly) based on the Bitcoin protocol (https://coinmarketcap.com/all.html).

Currency Competition - Gresham's Law and Thyer's Law

Gresham's Law, Sixteen century

Any circulating currency consisting of both "good" and "bad" money (both forms required to be accepted at equal value under legal tender law)[a] quickly becomes dominated by the "bad" money.

[a] **Robert Mundell**: Legal tender laws act as a form of price control. In such a case, the artificially overvalued money is preferred in exchange, because people prefer to save rather than exchange the artificially demoted one.

Dollarization in countries with weak economies and currencies may be seen as Gresham's Law operating in its reverse form (Guidotti & Rodriguez, 1992). E.g., Israel (1980s), Eastern Europe (with collapse of the Soviet bloc), South American (late 20th – early 21st century), Zimbawe multi-monetary system (since 2009).

Thyer's Law

In the absence of effective legal tender laws, Gresham's Law works in reverse. If given the choice of what money to accept, people will transact with money they believe to be of highest long-term value.

Currency Competition - Hayek Theory

The denationalisation of Money, 1976

The **denationalisation of money** is the cure for recurrent waves of depression and unemployment that have been represented as an inherent and deadly defect of capitalism.

Friedrich Hayek (Nobel Laureate, 1974)

- Instead of a national government issuing a specific currency, use of which is imposed on all members of its economy by force in the form of legal tender laws, private businesses should be allowed to issue their own forms of money, deciding how to do so on their own.

Currency Competition - Milton Friedman

- **Friedman and Schwartz (1986)** They conclude that there are in fact **NO** good economic arguments to support government monopolies of hand-to-hand currency.[a]
- **Interview to Friedman (2005) on his book "Monetary History of United States"**: "*I've always been in favor of abolishing the Federal Reserve and substituting a machine program that would keep the quantity of money going up at a steady rate*".[b]

[a] Friedman and Schwartz (1986). Has Government Any Role in Money?, *Journal of Monetary Economics* 17: 3762.

[b] `http://www.econlib.org/library/Columns/y2006/Friedmantranscript.html`

Currency Competition - Ron Paul

The Free Competition in Currency Act of 2013

Repeals the federal law establishing U.S. coins, currency, and reserve notes as legal tender for all debts, public charges, taxes, and dues

- The Free Competition in Currency Act is under discussion now.
  01/25/2013 Referred to the Subcommittee on Regulatory Reform, Commercial And Antitrust Law.
  Type of Action: Committee Consideration
  Action By: House Judiciary [3]

[3] `https://beta.congress.gov/bill/113th-congress/house-bill/77/actions`

Currency Competition - Data

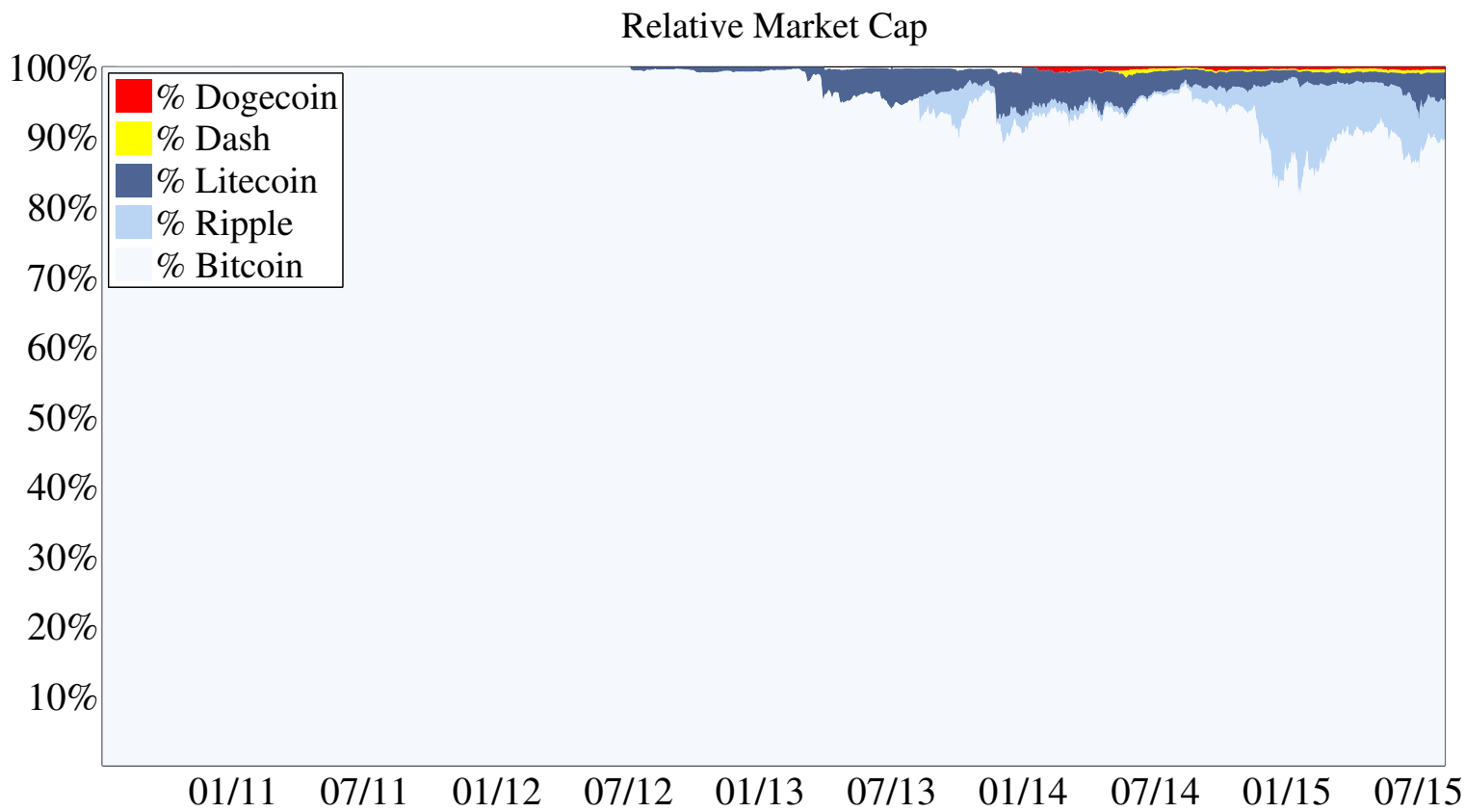


Figure: Comparison between different payment networks. Average daily USD amount per transaction from 1Q2011 to 1Q2015. Data source: Bitcoin blockchain, VISA, MasterCard, Discover, Western Union performance reports. Internal calculation.

Currency Competition - Data

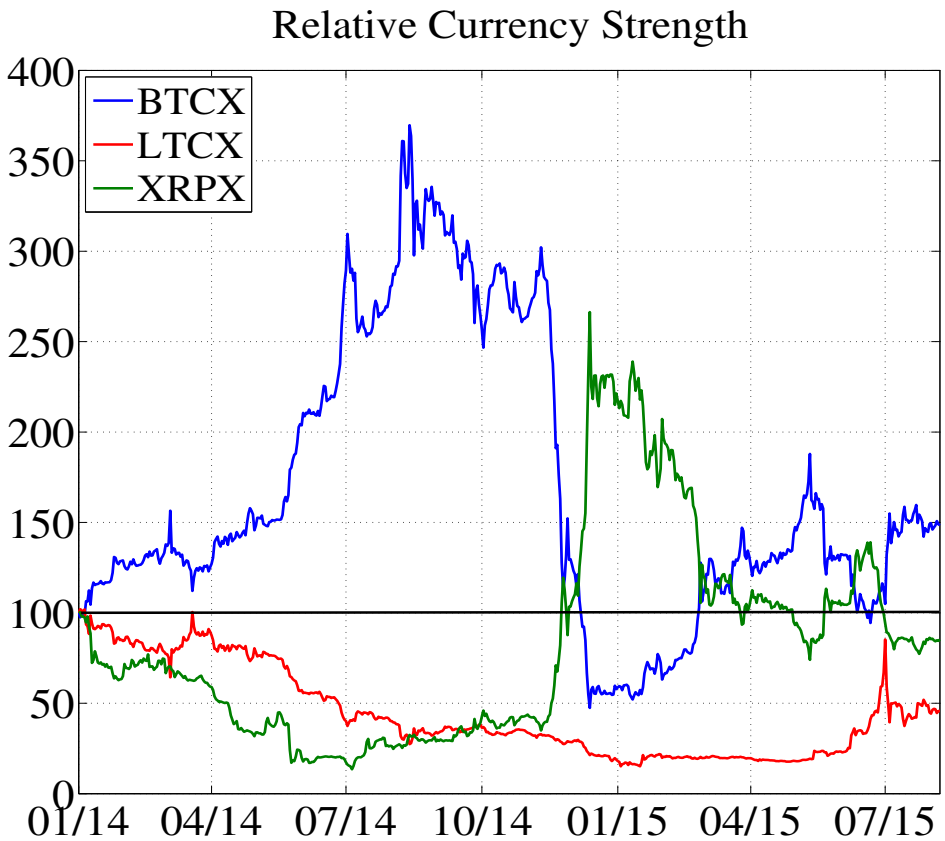


Figure: Comparison between relative index strengths. Ba= 100 on 01.01.2014 (BTCX, LTCX, XRPX). Internal calculation.

Currency Competition - Data

- BTCX: rel. strength of BTC wrt LTC and XRP, weighted by: (1) their respective rel. market cap. expressed in USD; (2) the inverse of the BTC exchange rate volatility
- LTCX: rel. strength of LTC wrt both BTC and XRP, weighted by: (1) their respective rel. market cap. expressed in USD; (2) the inverse of the LTC exchange rate volatility
- XRP: rel. strength of XRP wrt both BTC and LTC, weighted by: (1) their respective rel. market cap. expressed in USD; (2) the inverse of the XRP exchange rate volatility

$$BTCX := \Delta_{BTC} \times \text{Exp}\left\{\text{Log}\left[\frac{BTC/LTC}{\sigma\left(BTC/LTC\right)}\right](W_{BTC}) + \text{Log}\left[\frac{BTC/XRP}{\sigma\left(BTC/XRP\right)}\right](1 - W_{BTC})\right\}$$

$$LTCX := \Delta_{LTC} \times \text{Exp}\left\{\text{Log}\left[\frac{LTC/BTC}{\sigma\left(LTC/BTC\right)}\right](W_{LTC}) + \text{Log}\left[\frac{LTC/XRP}{\sigma\left(LTC/XRP\right)}\right](1 - W_{LTC})\right\}$$

$$XRPX := \Delta_{XRP} \times \text{Exp}\left\{\text{Log}\left[\frac{XRP/BTC}{\sigma\left(XRP/BTC\right)}\right](W_{XRP}) + \text{Log}\left[\frac{XRP/LTC}{\sigma\left(XRP/LTC\right)}\right](1 - W_{XRP})\right\}$$

where:

$$W_{BTC} = \left(\frac{\omega_{LTC}}{\omega_{LTC} + \omega_{XRP}}\right); W_{LTC} = \left(\frac{\omega_{BTC}}{\omega_{BTC} + \omega_{XRP}}\right); W_{XRP} = \left(\frac{\omega_{BTC}}{\omega_{BTC} + \omega_{LTC}}\right);$$

- Δ_{BTC}, Δ_{LTC} and Δ_{XRP} are normalisation factors;
- ω_{BTC}, ω_{LTC}, ω_{XRP}: market capitalisation of BTC, LTC and XRP expressed in USD.

Price Stability

Price Stability

- The Bitcoin market remains inefficient. It is characterised by high volatility, bubbles, and arbitrage opportunities.
- Risk to users remain high because of thefts, hacking, Ponzi schemes, soft/hardware malfunction.
- The year 2014 saw fewer incidences and less arbitrage opportunities than the previous years.
- The likelihood and intensity of arbitrage opportunities dramatically dropped to less than 1%.

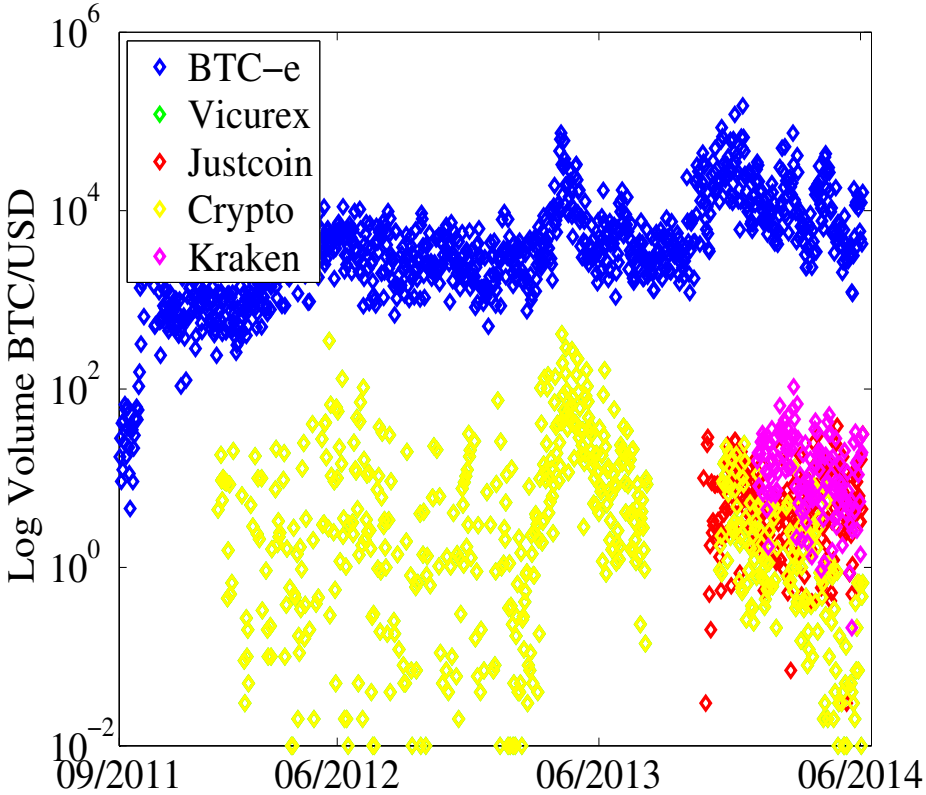
Price Stability

Arbitrage opportunities arise in presence of:

- Illiquid markets;
- Low market depth;
- Lack of market makers;
- Non-fluid exchange.

- **Test 1 (Δ^1)**: average exchange rate dispersion across platforms.
- **Test 2 (Δ^2, Δ^3)**: triangular arbitrage.

Price Stability



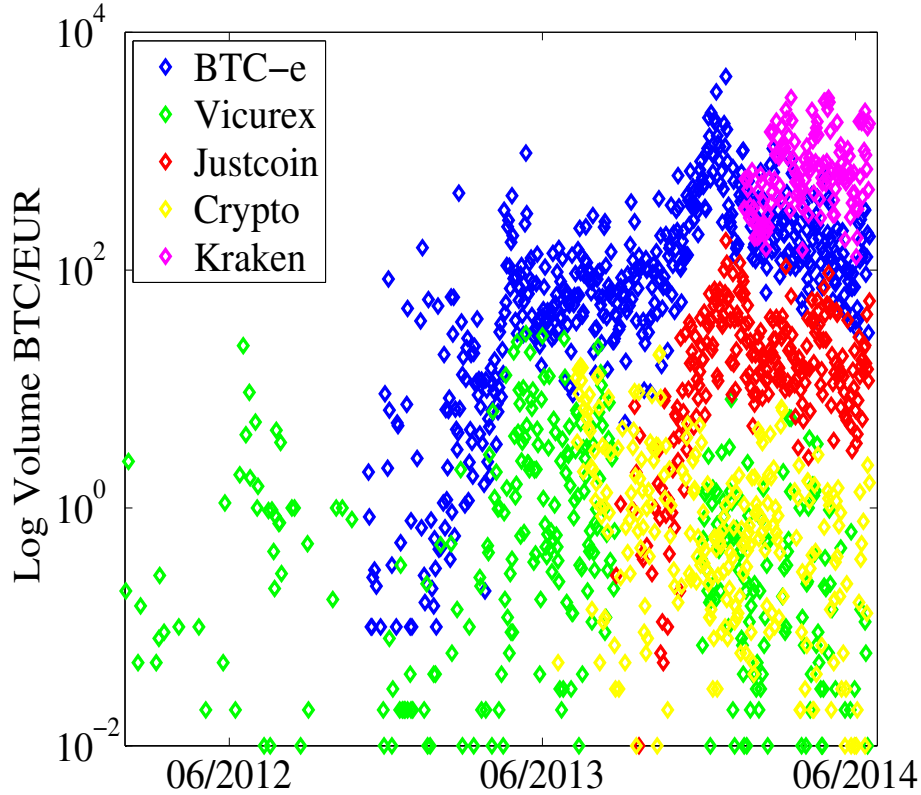


Figure: BTC daily trading volume on major trading platforms. Data source: `https://www.bitinfocharts.com` Internal calculation.

Price Stability

Test 1 In absence of arbitrage this equation must hold:

$$(\mathbf{BTC}/\mathbf{X})_{\mathbf{i}} = (\mathbf{BTC}/\mathbf{X})_{\mathbf{j}}$$

Thus, the average exchange rate dispersion (*without*) across platforms is:

$$\Delta^1 := \frac{1}{n}\sum_{i=1}^{N}\left|\frac{(BTC/X)^i}{(BTC/X)^B} - 1\right| \in [0,1].$$

i: Kraken, Vicurex, Justcoin, Crypto.
B: BTC-e
X: either USD or EUR.

Price Stability

1. Since 2011, Bitcoins volatility has been constantly decreasing

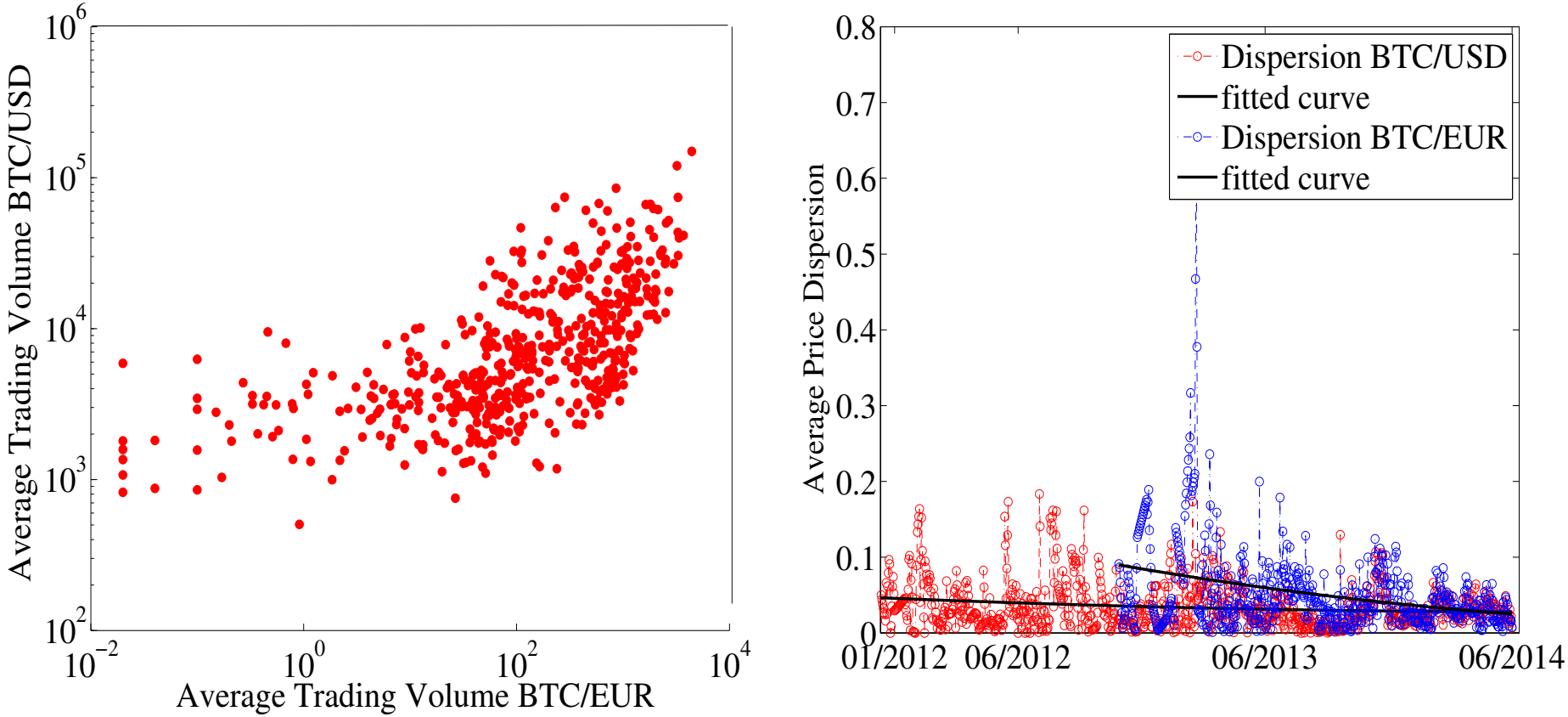


Figure: **Market Efficiency Test 1**. Left: Correlation between trading volume BTC/EUR and BTC/USD (log-log plot). Right: Average exchange rate dispersion Δ across platforms with reference BTC-e.

Price Stability

Test 2 In absence of arbitrage this equation must hold:

$$\mathbf{BTC/USD} = \mathbf{BTC/EUR} \times \mathbf{EUR/USD}$$

Thus, the average exchange rate dispersion (*within*) platforms is:

$$\begin{cases} \Delta^2 := \frac{1}{n} \sum_{i=1}^{N} \left| \frac{(BTC/EUR)^i}{(BTC/USD)^i} \times (EUR/USD) - 1 \right|, \\ \Delta^3 := \left| \Lambda \times (EUR/USD) - 1 \right|, \end{cases}$$

where:

$$\Lambda = \sum_{i=1}^{N} \left[\omega_i^{EUR} (BTC/EUR_i) \right] / \sum_{i=1}^{N} \left[\omega_i^{USD} (BTC/USD_i) \right]$$

$$\omega_i^{EUR} = \frac{\text{Volume}_i^{EUR}}{\text{Total Volume}^{EUR}}, \quad \omega_i^{USD} = \frac{\text{Volume}_i^{USD}}{\text{Total Volume}^{USD}}$$

i= BTC-e, Kraken, Vicurex, Justcoin, Crypto.

Price Stability

1. The year 2014 saw fewer incidences and less arbitrage opportunities than the previous years

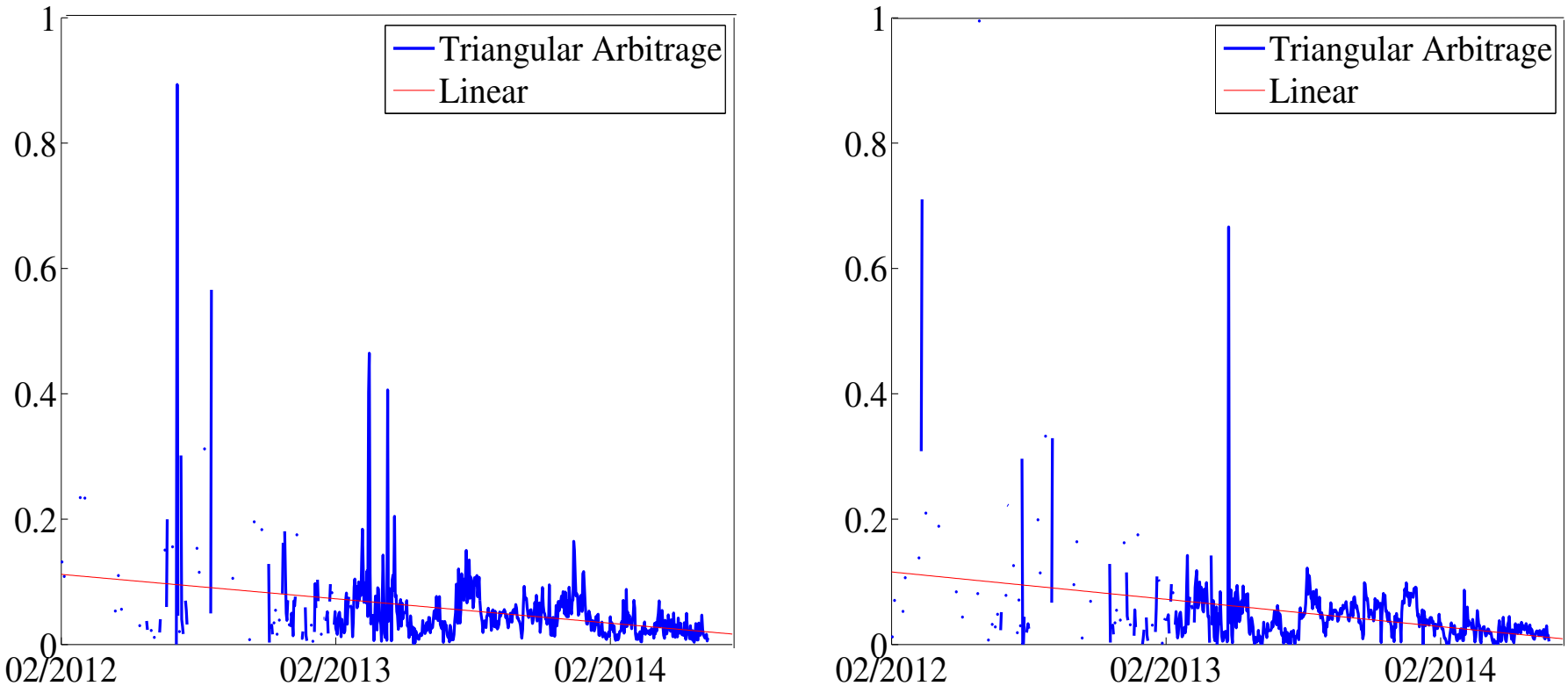


Figure: **Market Efficiency Test 2**. Average intensity of traingular arbitrage within platforms. Left: Δ^2. Right: Δ^3.

Currency Circulation

Currency Circulation

1. The inequality of the distribution of Bitcoins amongst addresses, summarised by the Gini coefficient (higher is more unequal), grew from 0.09 in 2010 to 0.99 in 2015: from quasi-perfect equality to quasi-perfect inequality.
2. This is not a "rich get richer" phenomenon. During the period 2009-2015, the top 100 richest addresses kept a constant relative wealth, totalling about 20% of the total value of the Bitcoin economy.

The increase in the inequality is the result of: (1) a socio-economic phenomenon, due to the growing popularity of Bitcoin, and (2) wallet fragmentation due to security practices such as single-use addresses and new addresses generated for change transactions.

Currency Circulation

The Gini coefficient (G) is an inequality index of income or wealth.[4]

G can be calculated from unordered size data as half of the Relative Mean Difference (RMD), which is the average absolute difference between every possible pair of values, divided by the mean size μ,

$$G = \frac{RMD}{2} \; with : RMD = \frac{MD}{\mu} \; , MD = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} |x_i - x_j|$$

- G=0: every person receives the same income;
- G=1: theoretical value for $n \to \infty$ where a single person receives 100% of the total income and the remaining people receive none

- x_i: income or wealth of person i.
- n: population size.

[4] Gini C., Variabilita' e mutabilita', 1912, reprinted in Memorie di metodologica statistica (Ed. Pizetti E, Salvemini, T). Rome: Libreria Eredi Virgilio Veschi 1955.

Currency Circulation

The Lorenz curve can be represented by a function $L(F)$ where:

- F is the cumulative portion of the population represented by the horizontal axis;
- L is the cumulative portion of the total wealth or income represented by the vertical axis.

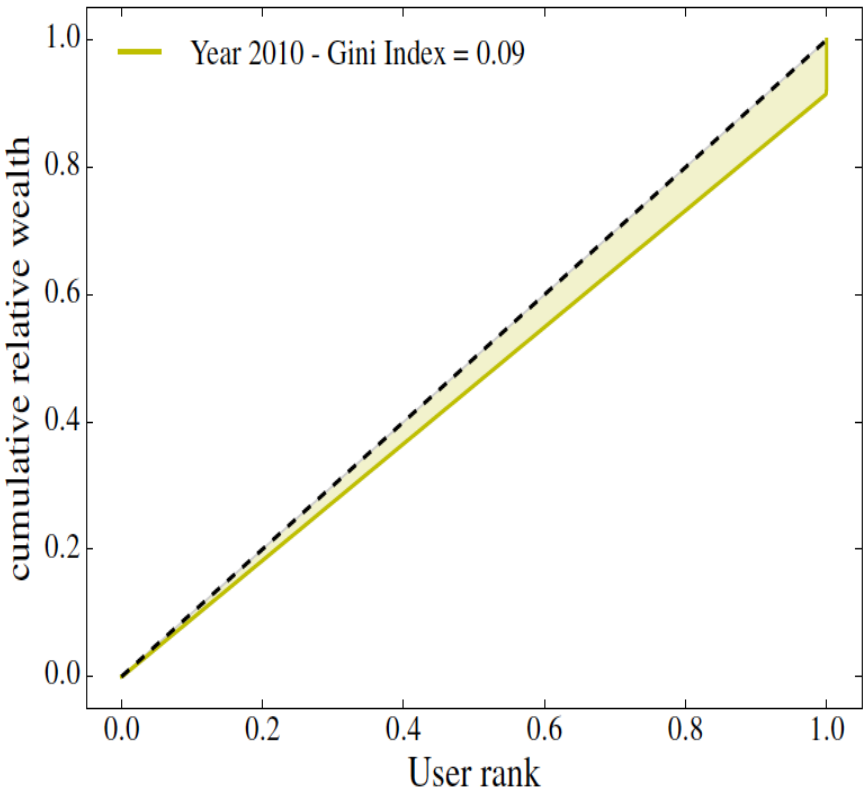
For a discrete probability function $f(y)$, let y_i, $i = 1, .., n$, be the points with non-zero probabilities indexed in increasing order $(y_i < y_{i+1})$. The Lorenz curve is the **continuous piecewise linear function** connecting the points (F_i, L_i), $i = 0, ..., n$, where $F_0 = 0$, $L_0 = 0$, and for $i = 1, ..., n$:

$$F_i = \sum_{j=1}^{i} f(y_j)$$

$$L_i = \frac{S_i}{S_n} \quad with\ S_i = \sum_{j=1}^{i} f(y_j) y_j$$

Currency Circulation

Wealth Inequality is increasing



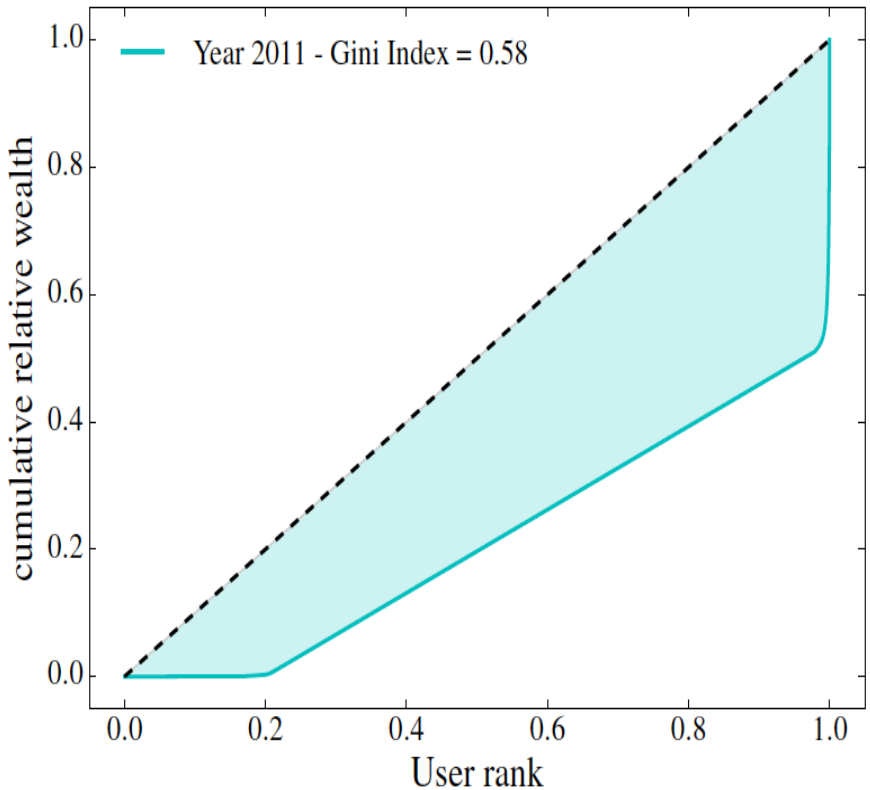
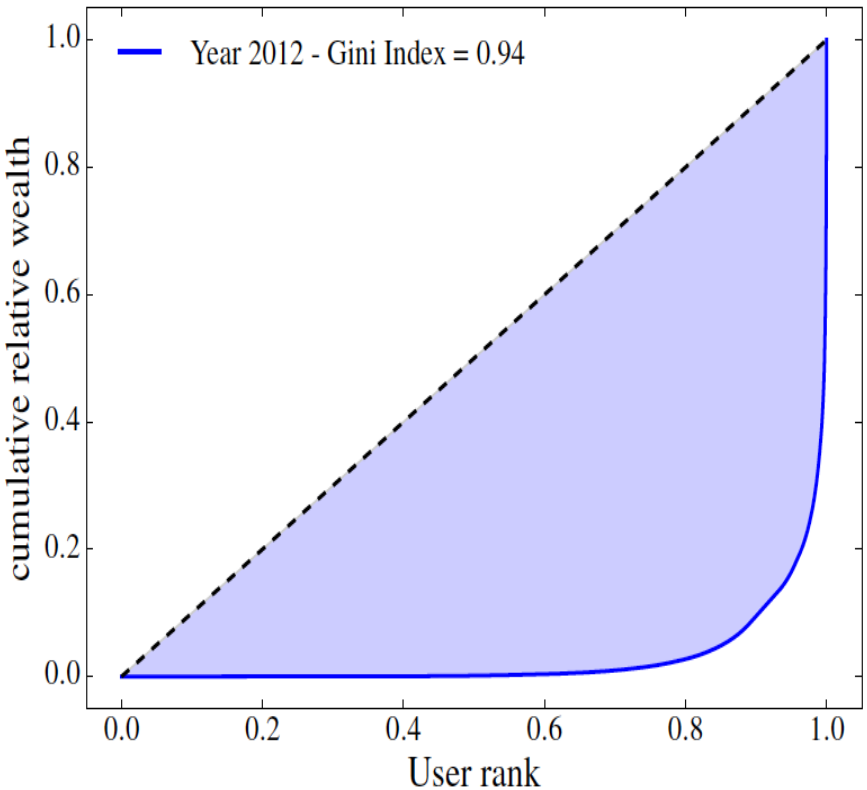


Figure: Lorenz Curve and Gini Coefficient for the Bitcoin Economy. Percentile of addresses sorted by wealth wrt to the percentile of the wealth own.

Currency Circulation

Wealth Inequality is increasing



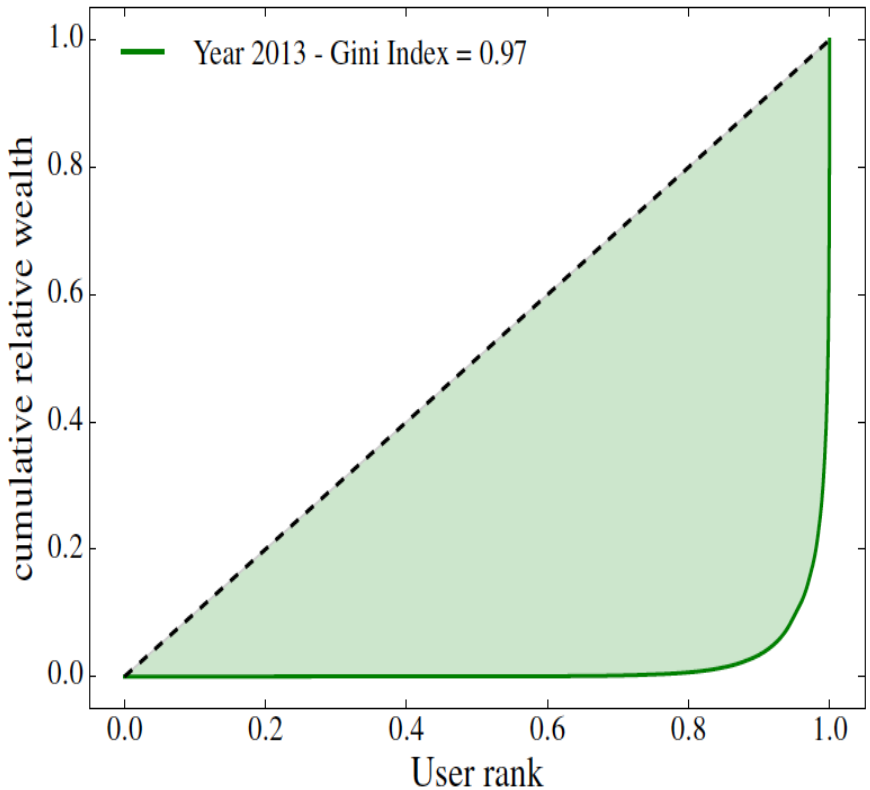
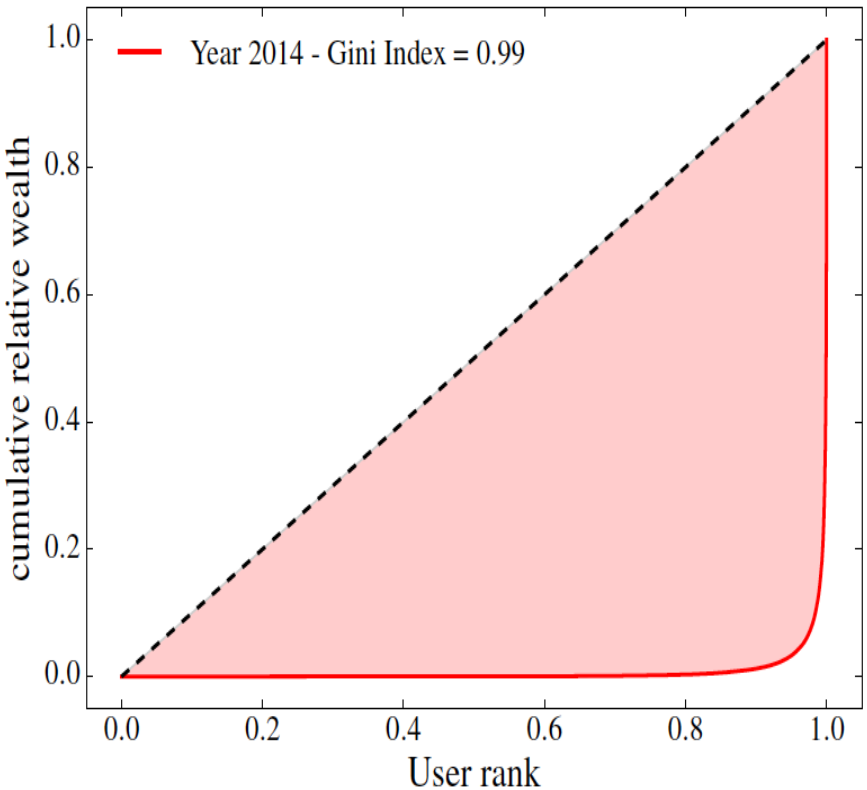


Figure: Lorenz Curve and Gini Coefficient for the Bitcoin Economy. Percentile of addresses sorted by wealth wrt to the percentile of the wealth own.

Currency Circulation

Wealth Inequality is increasing



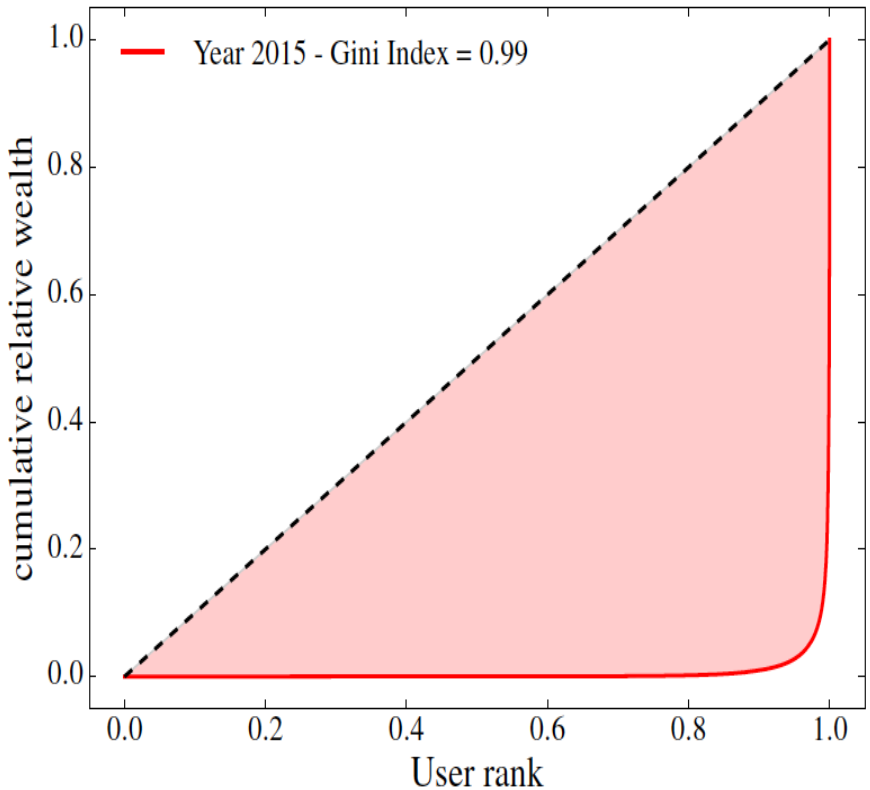


Figure: Lorenz Curve and Gini Coefficient for the Bitcoin Economy. Percentile of addresses sorted by wealth wrt to the percentile of the wealth own.

Currency Circulation

Wealth Inequality is increasing

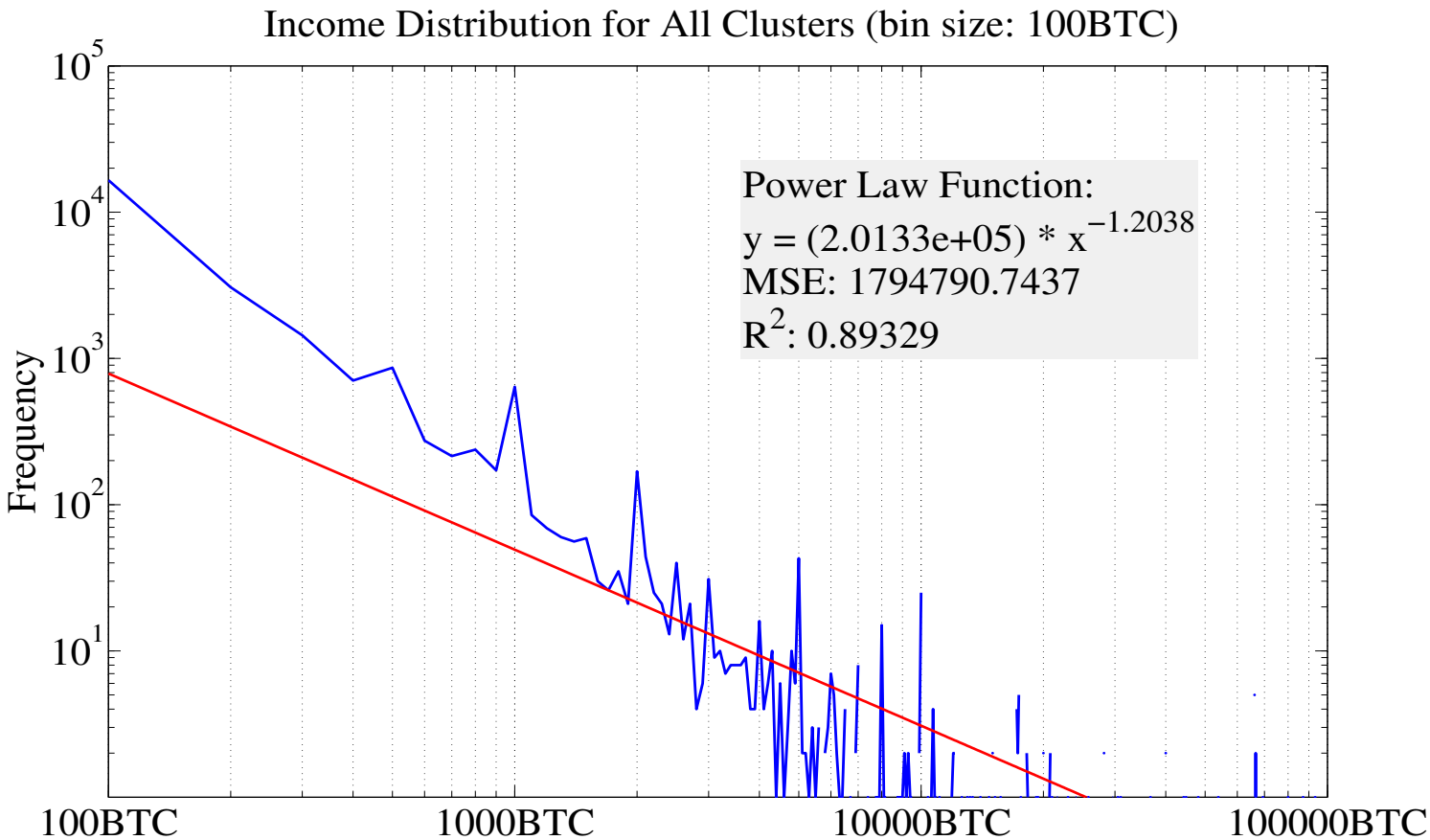
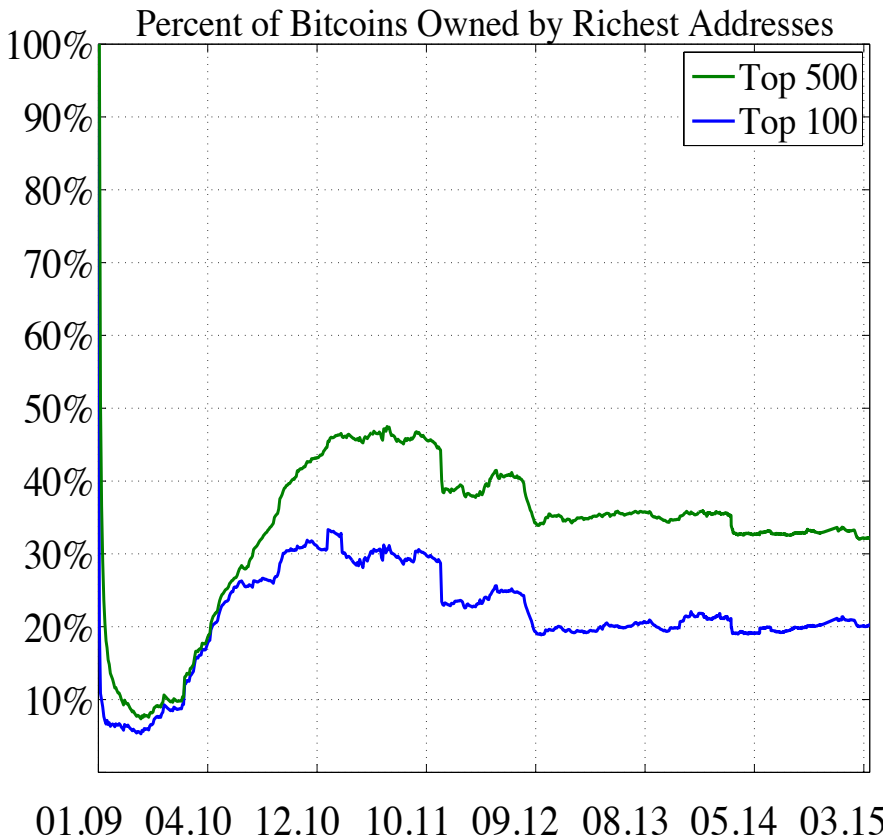


Figure: Income distribution for all clusters. Data source: Bitcoin Core parsed from the 3rd of January 2009 until the 8th of May 2015. Total nr. addresses: 75,191,953. Total nr. clusters (contains at least addresses): **30,708,660** (9,847,999 $\geq$ 2 nodes) and 4,810,342 with non-zero balance. Total TXs between clusters: 88,950,021. Internal calculation.

Currency Circulation

Wealth Inequality is increasing



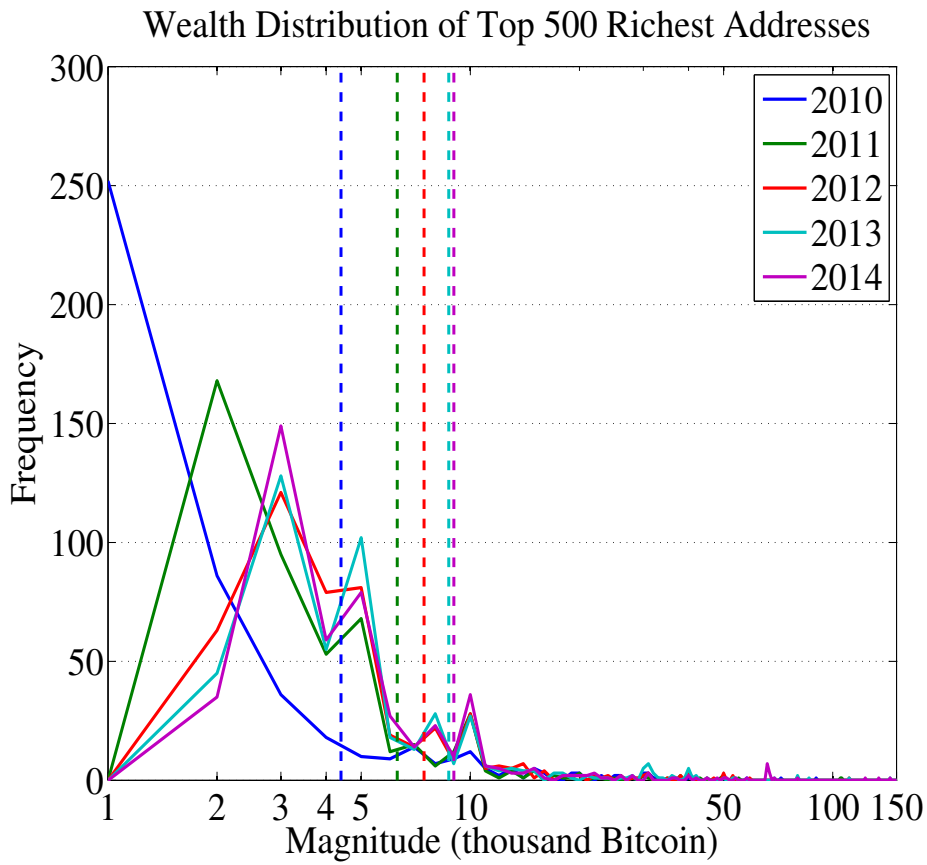


Figure: Left: Relative wealth of the top 100 and 500 richest Bitcoin addresses. Right: Wealth distribution among the top 500 richest Bitcoin addresses (with x-axis log-transformed). Data source: Bitcoin blockchain. Internal calculation.

Bitcoin as Payment Network

Bitcoin as Payment Network

During the period 2011–2015, the average amount (in USD equivalent) per transaction constantly increased, and remained larger than in the major payment networks such as Visa, Mastercard, Discover, or Western Union.

- The Bitcoin network is mostly used to remit money from user to user.[5]

[5] Studies show that the amount migrants send per transaction typically ranges between USD 100 and USD 1,000 for international remittances (e.g., Sander C., 2003);

Bitcoin as Payment Network

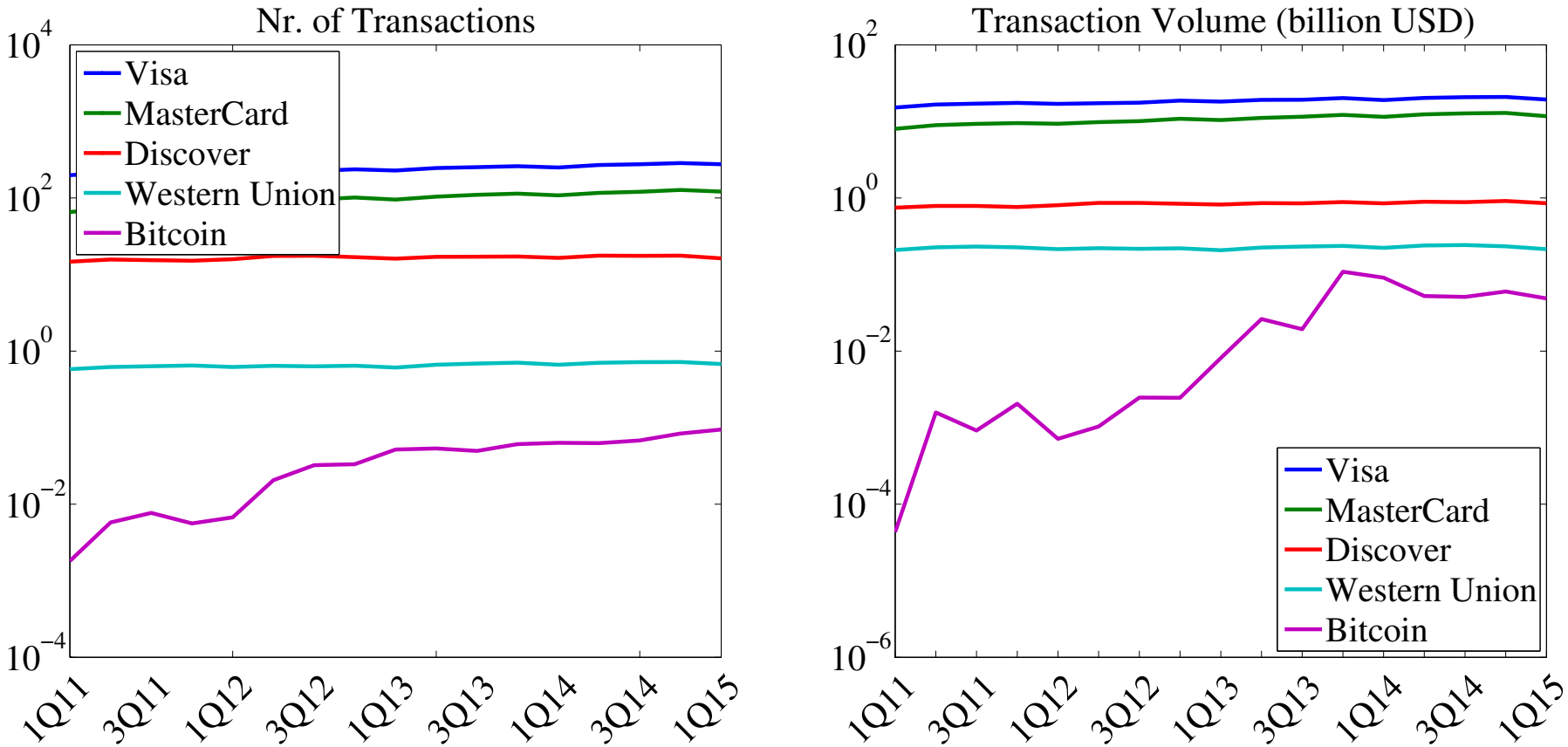


Figure: Comparison between different payment networks. Left: Average (log) number of daily transactions. Right: Average (log) amount of daily transactions in USD. Data source: Bitcoin blockchain, VISA, MasterCard, Discover, Western Union performance reports. Period: 1Q2011 to 1Q2015. Internal calculation.

Bitcoin as Payment Network

Year	VISA		MasterCard		Discover		Western Union		Bitcoin	
	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)	(Vol.)	(Tx.)
1Q11	15,153.8	198.3	8,011.0	65.6	746.5	14.7	208.8	0.6	0.04	0.002
2Q11	16,604.4	213.2	8,934.1	72.5	787.0	15.7	226.4	0.62	1.6	0.006
3Q11	17,033.0	217.7	9,285.7	77.1	787.0	15.4	231.9	0.63	0.92	0.008
4Q11	17,450.5	223.6	9,505.5	84.4	761.3	15.1	226.4	0.65	2.1	0.006
1Q12	16,934.1	215.7	9,329.7	84.8	804.3	15.8	214.3	0.62	0.7	0.007
2Q12	17,252.7	218.7	9,780.2	93.8	861.1	17.5	220.9	0.64	1.04	0.021
3Q12	17,582.4	225.3	10,087.9	95.4	860.9	17.6	216.5	0.63	2.47	0.032
4Q12	18,648.4	236.8	10,835.2	101.3	840.1	16.8	219.8	0.64	2.45	0.033
1Q13	18,120.9	227.9	10,406.6	95.1	819.2	16.1	207.7	0.61	8.12	0.052
2Q13	19,109.9	245.6	11,087.9	104.1	856.1	17.0	225.3	0.66	26.2	0.053
3Q13	19,175.8	252.1	11,494.5	109.9	850.5	17.1	231.9	0.69	19.3	0.050
4Q13	20,197.8	259.9	12,142.9	114.0	883.8	17.2	236.3	0.71	108.65	0.061
1Q14	19,011.0	249.9	11,483.5	108.2	850.4	16.5	223.1	0.66	91.01	0.063
2Q14	20,274.7	269.6	12,351.6	116.6	892.2	17.6	239.6	0.70	52.35	0.063
3Q14	20,703.3	275.9	12,714.3	120.5	881.0	17.5	242.9	0.72	51.07	0.068
4Q14	20,879.1	285.4	12,879.1	127.1	912.0	17.7	233.0	0.72	60.1	0.084
1Q15	19,263.74	275.6	11,681.32	121.3	852.32	16.3	214.29	0.68	48.80	0.094

Table: Volume in million USD (Vol.) and millions of transactions (Tx).

Bitcoin as Payment Network

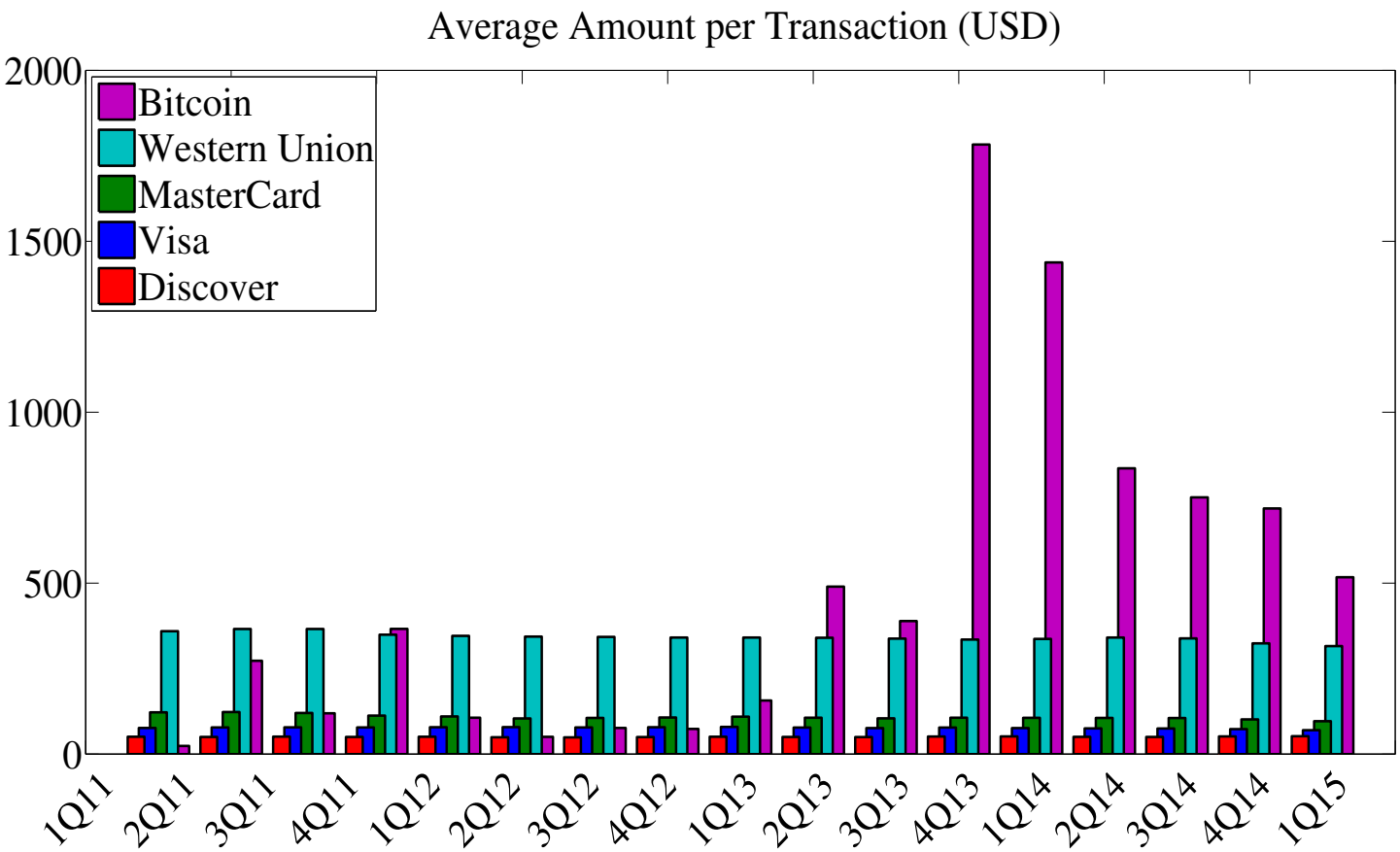


Figure: Comparison between different payment networks. Average daily USD amount per transaction from 1Q2011 to 1Q2015. Data source: Bitcoin blockchain, VISA, MasterCard, Discover, Western Union performance reports. Internal calculation.

Bitcoin as Payment Network

1. During the year 2014, the transaction costs in digital currencies dropped significantly. Throughout 2014, the average fee per Bitcoin (Litecoin) transaction decreased from about USD 20 (7) cents to USD 10 (1) cents.
2. The number of Bitcoin transactions per second remains around 7 because of block size limits.

	Network Take Rate	Transactions per second
Bitcoin	0.0%	7
Stock Exchange	0.05 USD / 100 shares	29
Card Networks	0.2%	2,000[6]
Cross Border Money Transfer	5.0%	28
EBAY	8.0%	1

[6] VISA network achieved 47,000 peak transactions per second (tps) during the 2013 holidays. (See `http://www.visa.com/blogarchives/us/2013/10/10/stress-test-prepares-visanet-for-the-most-wonderful-time-of-the-year/index.html`).

Bitcoin as Payment Network - Transaction Structure

Reasons

1. It takes about five ten minutes on average for a new transaction to find its way into a block
2. Transaction Structure is limited. One cannot transmit richer forms of information a part from the ownership of Bitcoins
3. Limited transfer conditions to specify how the ownership is proved. Smart contracts required more sophisticated languages.
4. You cannot trade safety with speed. There exists the same security guarantees for all transactions (1bn - 1) BTC.

Bitcoin as Payment Network - How to Improve the Speed ?

1. Sidechain solutions
2. Scaling Bitcoin
   - On-Chain Solutions
   - Off-Chain Solutions
3. Private Ledgers

Bitcoin as Payment Network - How to Improve the Speed ?

Sidechain solutions

1. Bitcoins are sent to a specially formed Bitcoin address. The address is specially designed so that the coins will now be out of the control of anybody. Theyre completely immobilised and can only be unlocked **if somebody can prove theyre no longer being used elsewhere**.
2. Once the immobilisation is confirm, you can send a message with a proof to another blockchain you want to use.
3. If the second blockchain has agreed to be a Bitcoin sidechain, it creates the exact same number of tokens on its own network and gives you control of them.
4. **You can now transact with those coins on that second chain**, under whatever rules that chain chooses to implement.

In the sidechain blocks may be created faster and transaction scripts can be turing complete and generally a fee is require to pay for the sidechain security.

Bitcoin as Payment Network - How to Improve the Speed ?

Sidechain solutions

We can use standard Bitcoin transaction functionality to move coins out of reach and we then prove to a second, unrelated chain, that we have done this. And later, whoever will owns them on the sidechain can do the same in reverse bY sending them back to the bitcoin network.

Bitcoin as Payment Network - How to Improve the Speed ?

Scaling Bitcoin

	Solution	Description	Pros	Cons	Further Reading
On-chain Solution	**Bitcoin Classic (hard fork)**	Increase block size from 1MB to 2 MB	Scaling in a straightforward manner	This is a **hard fork**.We are lack of experience about hard fork	https://bitcoin.org/en/bitcoin-core/capacity-increases-faq#roadmap
	Bitcoin Unlimit (hard fork)	Delete hard-coded block-size limit.Users could modify it on their own node	-	This is a **hard fork**.We are lack of experience about hard fork	http://www.bitcoinunlimited.info/
	Bitcoin XT (hard fork)	Increase Bitcoin's block-size limit from 1 megabyte to 8 megabytes, set to double every other year until it reaches 8 gigabytes	-	This is a **hard fork**.We are lack of experience about hard fork	https://bitcoinmagazine.com/articles/unlimited-classic-and-bitpay-core-bitcoin-s-new-kids-on-the-blockchain-1452705977
Off-chain Solution	**Segregated Witness (soft fork)**	Reduce the block size by moving scriptSig(60% of block size) into a segregated structure called witness	Fix scriptSig malleability	The scaling effect is limit.	https://diyhpl.us/wiki/transcripts/scalingbitcoin/hong-kong/segregated-witness-and-its-impact-on-scalability/
	Lightning Network (in developing, should be soft fork)	Payment channels between many parties in a multi-hop 'hub and spoke' model (similar to internet routing)	Reduce the load on bitcoin blockchain	Still in developing, we'll see	https://lightning.network/lightning-network-paper.pdf

Bitcoin as Payment Network - How to Improve the Speed ?

Private Ledgers

Exploit the properties of public distributed ledgers like Bitcoin but have semi-decentralised consensus mechanisms and are (generally) permissioned

- Stellar
- Ripple
- Hyperledger
- Tendermint

Bitcoin as Payment Network - How to Improve the Speed ?

Stellar

Global market place for the exchange of real assets in the form of digital credits

- Native token
- Gateways: market makers that bridge the gap between the physical and the virtual world specialized in
  - holding certain type of assets deployed on Stellar by the users
  - issue redeemable and exchangeable digital credits
  - honour the withdrawal
- Soft permission

Bitcoin as Payment Network - How to Improve the Speed ?

Ripple

Decentralized Real-Time:
1) Remittance network
2) Exchange of certificate representative of real assets
3) Gross settlement system

- Gateways to convert assets into assets into IOUs
- RPCA (synchronous) with the concept of "trusted authorities" in the UNL[7] (no mining, POW, POS)
- XRP which serves as currency bridge for less liquid pairs and use as "gas" for network maintenance[8]
- Soft permission

[7] Only the votes approved by the other members of the UNL of s are considered when determining consensus (as opposed to every node.)

[8] The fee is destroyed after having been paid.

Bitcoin as Payment Network - How to Improve the Speed ?

Hyperledger

Infrastructure for the development of innumerable interoperable ledgers operated by different parties for different purposes[a]

NOT based on:
1) Native token
2) A single public ledger. Users can deploy multiple private ledgers for sp

- No transfer fees between users within the same pool
- Immune to spamming attacks
- No mining process

[a] Local markets for particular types of assets participated by a specific set of users under ad hoc rules that serve specific needs.

Bitcoin as Payment Network - How to Improve the Speed ?

Tendermint[a]

[a] Jae Kwon. Tenderint: Cosensus without Mining.

- Tendermint Vs. Bitcoin/Ethereum consensus mechanism. Tendermint is environment friendly
- Combination of BGA and Proof of Collateral. Different from PBFT used by Hyperledger, Tendermint also works for "consortium" or "public" blockchains
- Tolerant up to n malicious nodes (n is the total number of nodes)
- About 1,000 independent validators in global network
- Transaction committed in less than 60 seconds