Digital Currencies

Paolo Tasca

Deutsche Bundesbank[1]
CFS, Goethe University
London School of Economics
University College London
ECUREX Research

SUERF/Liberales Institut/University of Zurich
CASH ON TRIAL

November 5, 2015

[1]The statements reflect the personal views of the speaker and do not necessarily coincide with the position of the Deutsche Bundesbank.

1. Bitcoin Protocol. Nuts and Bolts
2. Bitcoin as Payment Network
3. Bitcoin as Currency
4. Groups of Interest. Investors
5. Distribution of Income and Wealth
6. Take-home Message

What are Digital Currencies ?

- *Satoshi Nakamoto*'s paper "Bitcoin: A Peer-to-Peer Electronic Cash System" (`http://nakamotoinstitute.org/`)
- Based on decentralised/distributed peer-validated time-stamped ledgers (instead of trust-based centralised ledgers) publicly/privately[a] auditable.
- Uses cryptography to verify indentities/transactions, and to expand the monetary base at a constant pace.

[a] Eg., Ripple, Hyperledger.

Combination between
distributed ledger technology and **cryptography**:
BLOCKCHAIN TECHNOLOGY


INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA
The Economist
Our guide to America's best colleges
Turkey votes to the sound of bombs
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
OCTOBER 31ST–NOVEMBER 6TH 2015
Economist.com
The trust machine
How the technology behind bitcoin could change the world
IN BLOCKCHAIN WE TRUST

What are Digital Currencies ?

- Digital Currencies are **money** expressed as a string of bits sent as a message in a network where nodes verify the authenticity of the message via different mechanisms (e.g., PoW, PoS, PoB).
- A digital currency is not only money:
  - **payment system**.
  - ...and something more.
- Digital Currencies differ among each others by:
  - Consensus protocol (synchronous[a] or asynchronous[b]).
  - Rewarding mechanisms (money supply mechanism)

---

[a] Such as Hyperledger.
[b] Such as Bitcoin.

Why Blockchain technology is important ?

It allows for a trustworthy record of transactions among anonymous in all those cases where the following operational structures are in place:

- intermediation;
- clearing and settlement;
- record system;
- rating or voting system;
- databases;
- distributed storage, authentication, anonymisation of private information;
- rewarding and punishing-incentive schemes;
- transaction traceability schemes;
- refereeing, arbitration or notarization.

How the Bitcoin protocol works ?

Money as a string of bits sent as a **message** in a network that verifies the authenticity of the message via a proof-of-work / proof-of-stake mechanism.

1. Alice (**A**) want to give to Bob (**B**) one BTC (**BTC**).
   A will:
   1. write a message: "I, A, am giving B one BTC with **serial number** 123456";
   2. sign the message with a **private cryptographic key**;

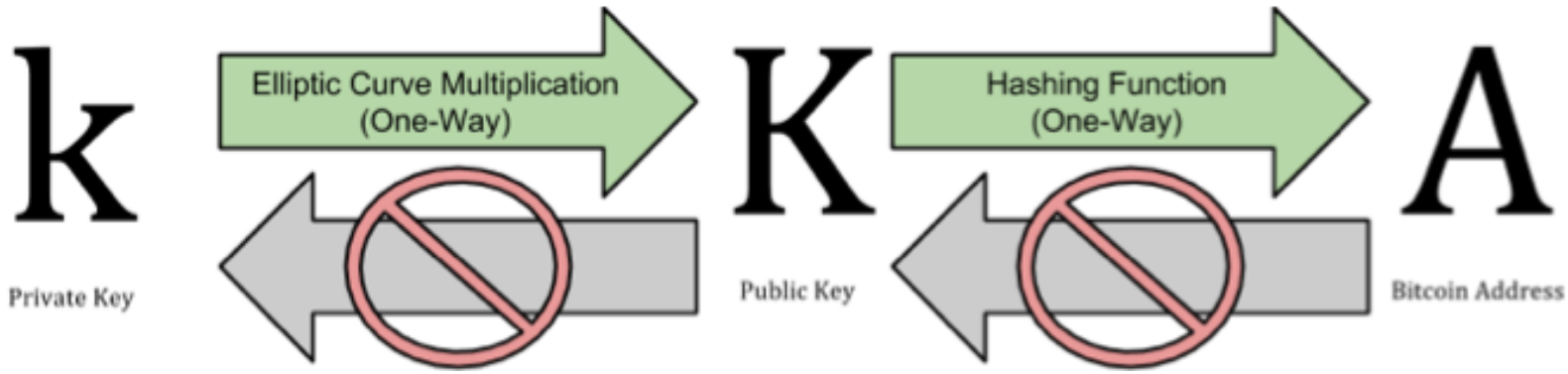


Figure: Generation of BTC address

Private key, Signature, Public Key

- **K** is used to receive BTCs.
- **k** is used to sign transactions to spend BTCs. The signature is different each time, but created from the same **k**.
- Ownership and control over **k** is the root of user control over all funds associated with the corresponding BTC address.
- Mathematical relationship between **K** and **k** that allows **k** to be used to generate signatures on messages. This signature can be validated against **K** without revealing **k**.
- Through the presentation of the **K** and signature everyone in the network can verify and accept the transaction as valid, confirming that the person transferring the BTCs owned them at the time of the transfer.

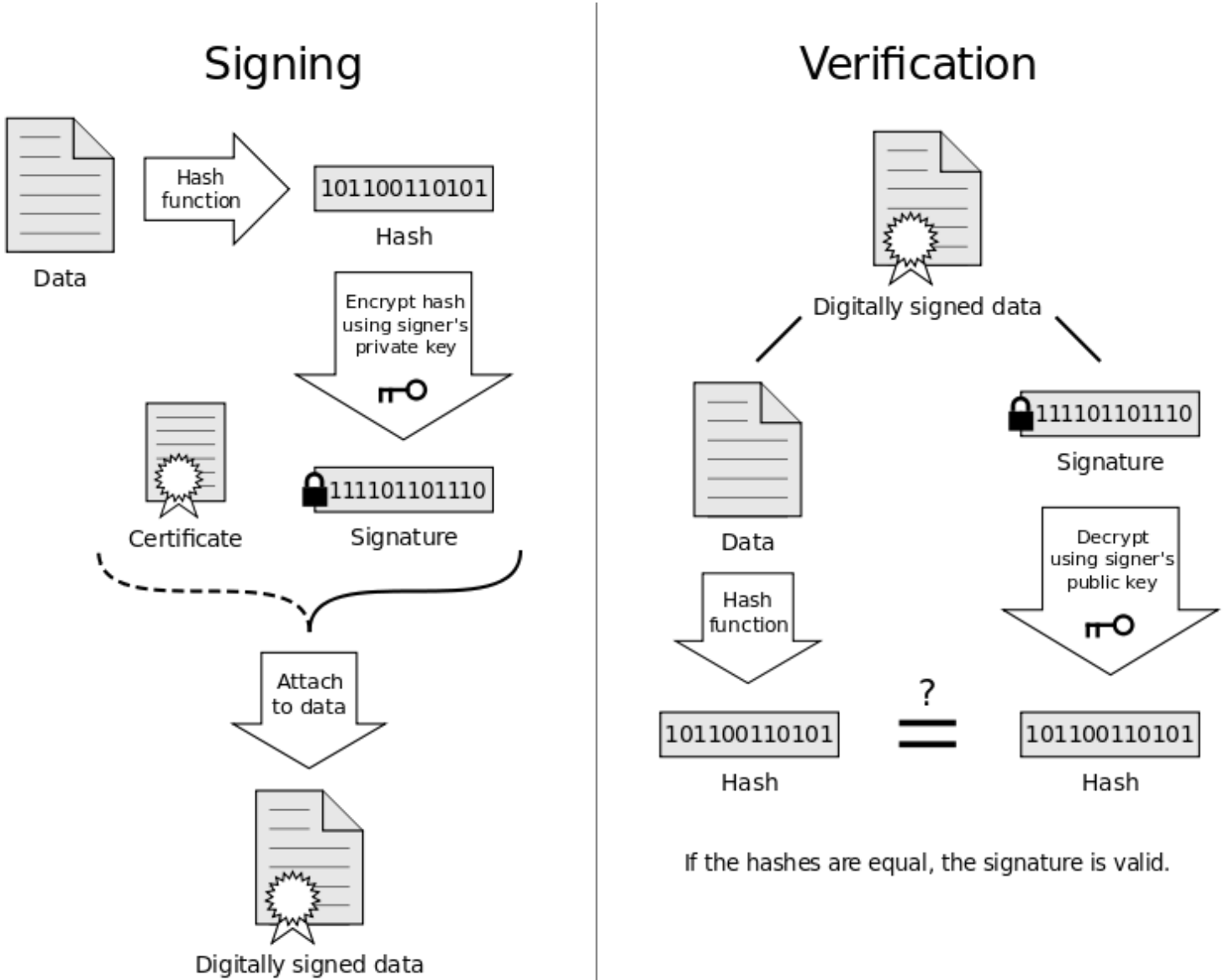


Figure: Digital Signature.

Problem: We need a trusted source of serial numbers generator

Solution: Every node in the network collectively composes a "decentralised" bank that book keeps a unique public ledger called blockchain[a] by:

- provides serial numbers for BTCs;
- keeps track of who has which BTCs;
- verifies that transactions really are legitimate.
- register in the ledger the passages of messages between users.

[a] Every node with a desktop BTC client has an updated copy of the blockchain in its computer.

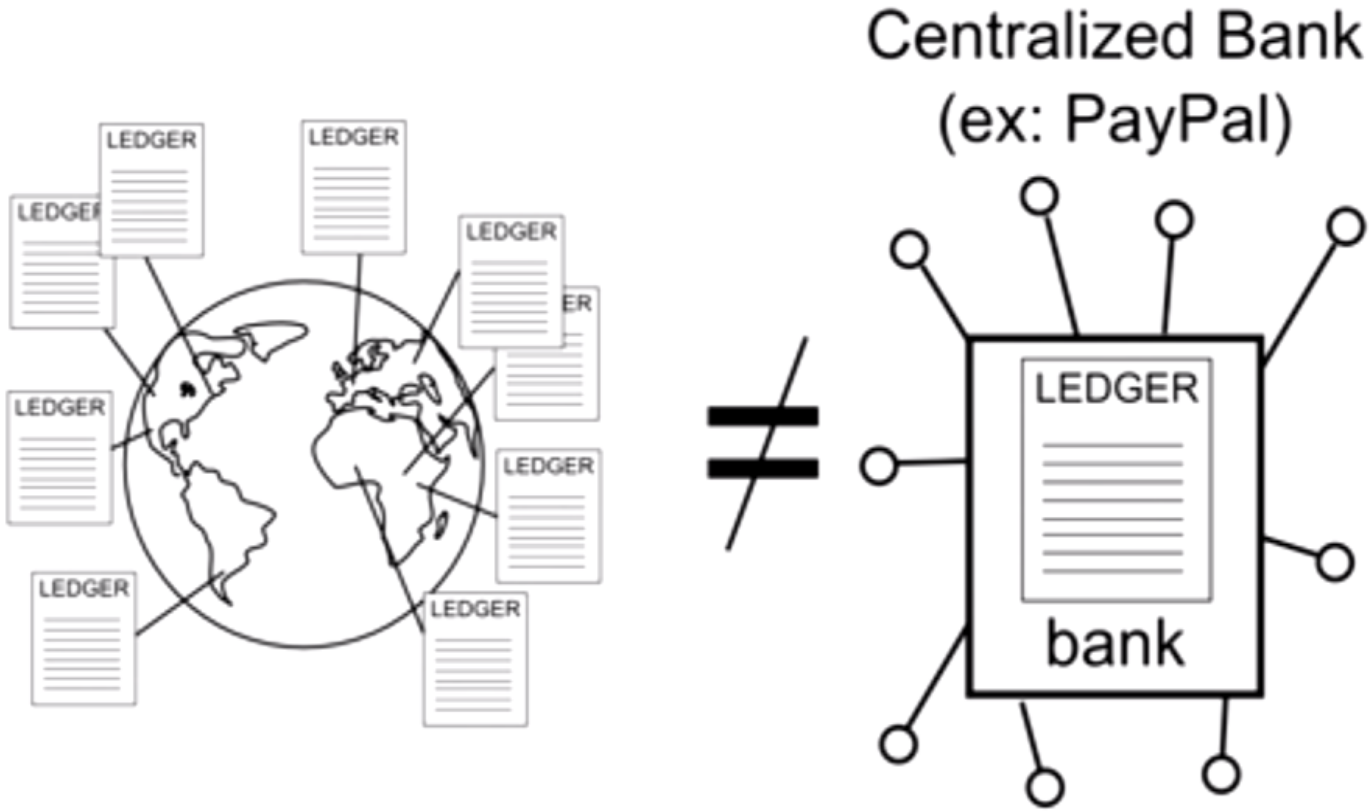


Figure: The blockchain is a decentralised Ledger that works as *Cash-flow Balance* instead of an account Balance. The blockchain contains all the history of all transactions (time-stamped) ever occurred in the Bitcoin network.

2 B – with his copy of the blockchain – does a sanity check that the BTC with serial number 123456 belongs indeed to A;

3 B will broadcast the signed string of bits to the entire network.

4 Other nodes in the network will collectively **verify** whether A holds one BTC with serial number 123456.

- 4.1 David (**D**) receives the message "I, A, am giving B one BTC with serial number 123456" and queue it together with other messages recently received that must to be digested (pending transactions of the last 10 mins not yet approved by the network). Together they form a **transaction block**.
- 4.2 With his copy of the blockchain and the public keys, D can verify that each transaction in his block is valid.
- 4.3 D must solve an NP-hard computational puzzle before to broadcast to the network the validity of the transactions: Proof-of-work principle.

Proof-of-work. Mining is a competition to approve transactions

D needs to compute new hash values based on the combination of:

- the previous hash value;
- the new transaction block;
- a *nonce*.

such that the new hash value start with a given number $\leq$ *Target*. The Target is automatically adjusted to ensure that a BTC block takes, on average, about ten minutes to validate.

A miners chance of winning the competition is roughly equal to the proportion of the total computing power that they control. Therefore, specific hardware has been produced.

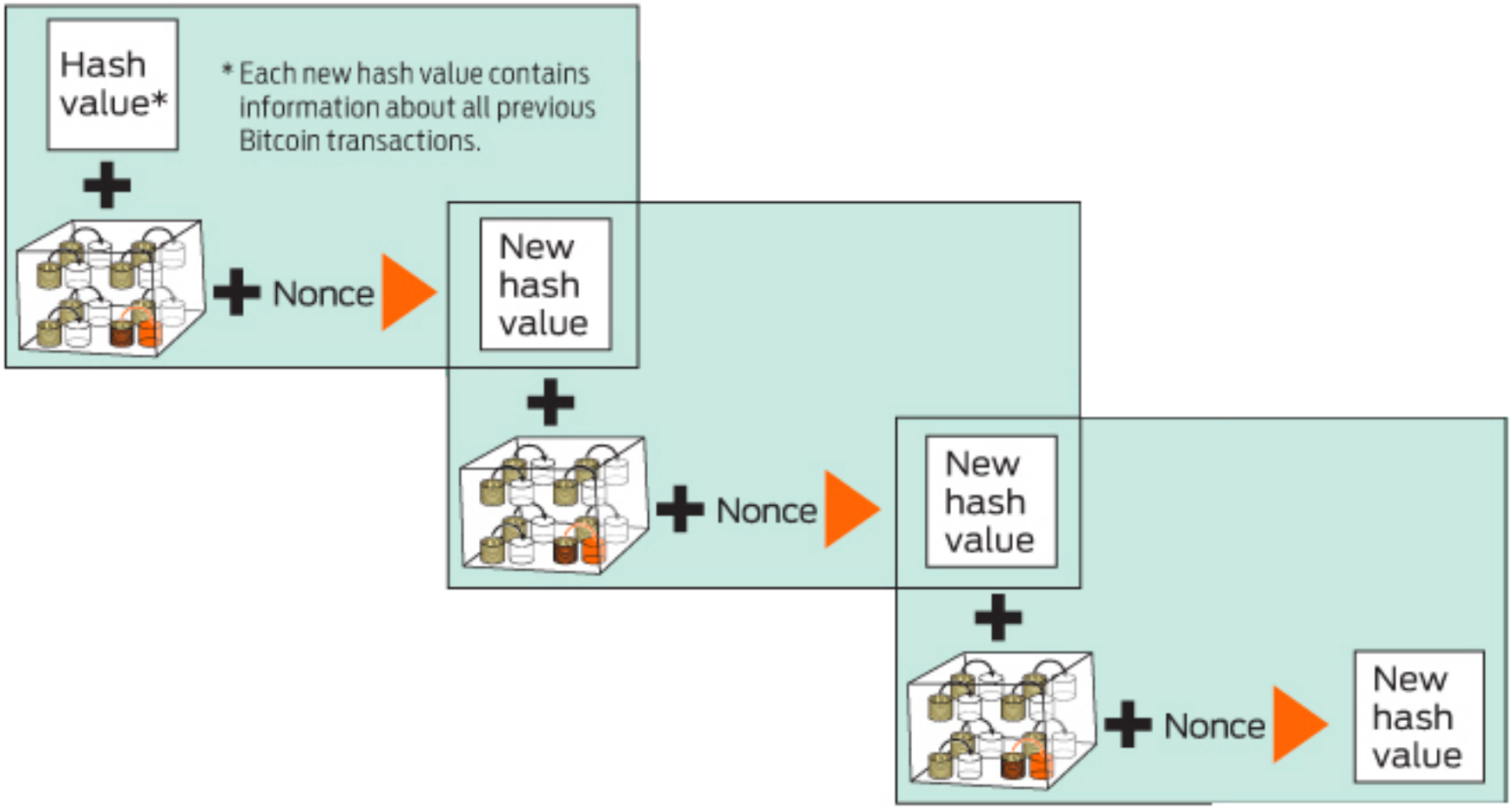


Figure: Any transaction of X BTCs from A to B must refer to previous transactions (Inputs) with which A received at least X BTCs. The verification process checks indeed if the inputs allow A to transfer X BTCs to B.

5 If D finds the suitable *nonce*, he will broadcast the message "Yes, A owns BTC 123456, it can now be transferred to B" together with the other transactions in the transaction block and the nonce (s.t. the network can check-test).

6 Everyone updates their blockchain to show that BTC 123456 now belongs to B, and the transaction is complete.

7 each transaction block contains a "**coinbase**" transaction that pays 25 BTCs (as for now) to the winning-miner to a newly address created on D name.

Bitcoin as Payment Network. Network Expansion

The average amount transferred per Bitcoin transaction is larger than in any other major 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.[2]

[2] 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. Network Expansion

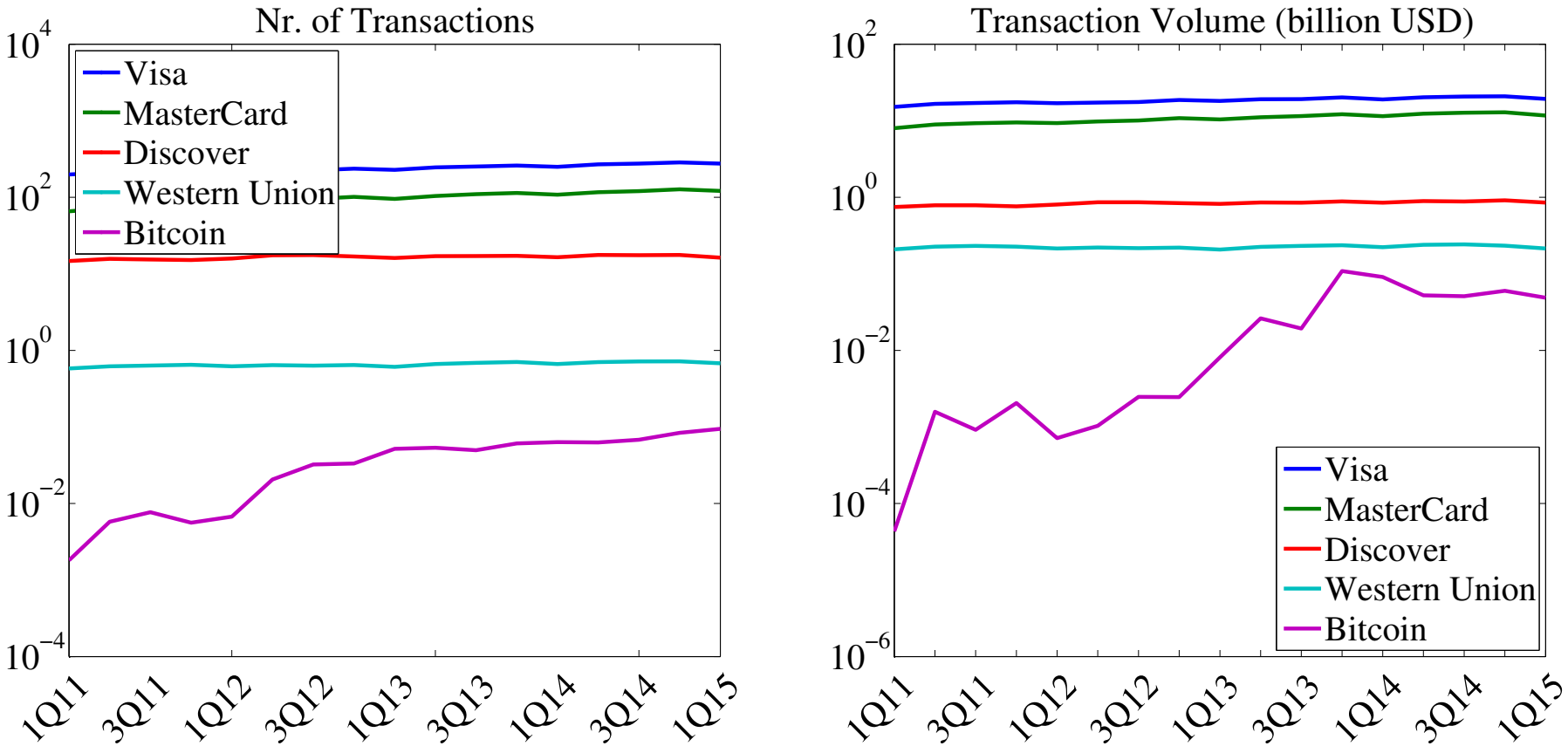


Figure: Comparison between different payment networks. Left: Average (log) number of daily transactions. Right: Average (log) amount of daily transactions in USD. Data source: Bitcoin blockchain, VISA, MasterCard, Discover, Western Union performance reports. Period: 1Q2011 to 1Q2015. Internal calculation.

Bitcoin as Payment Network. Network Expansion

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. Network Expansion

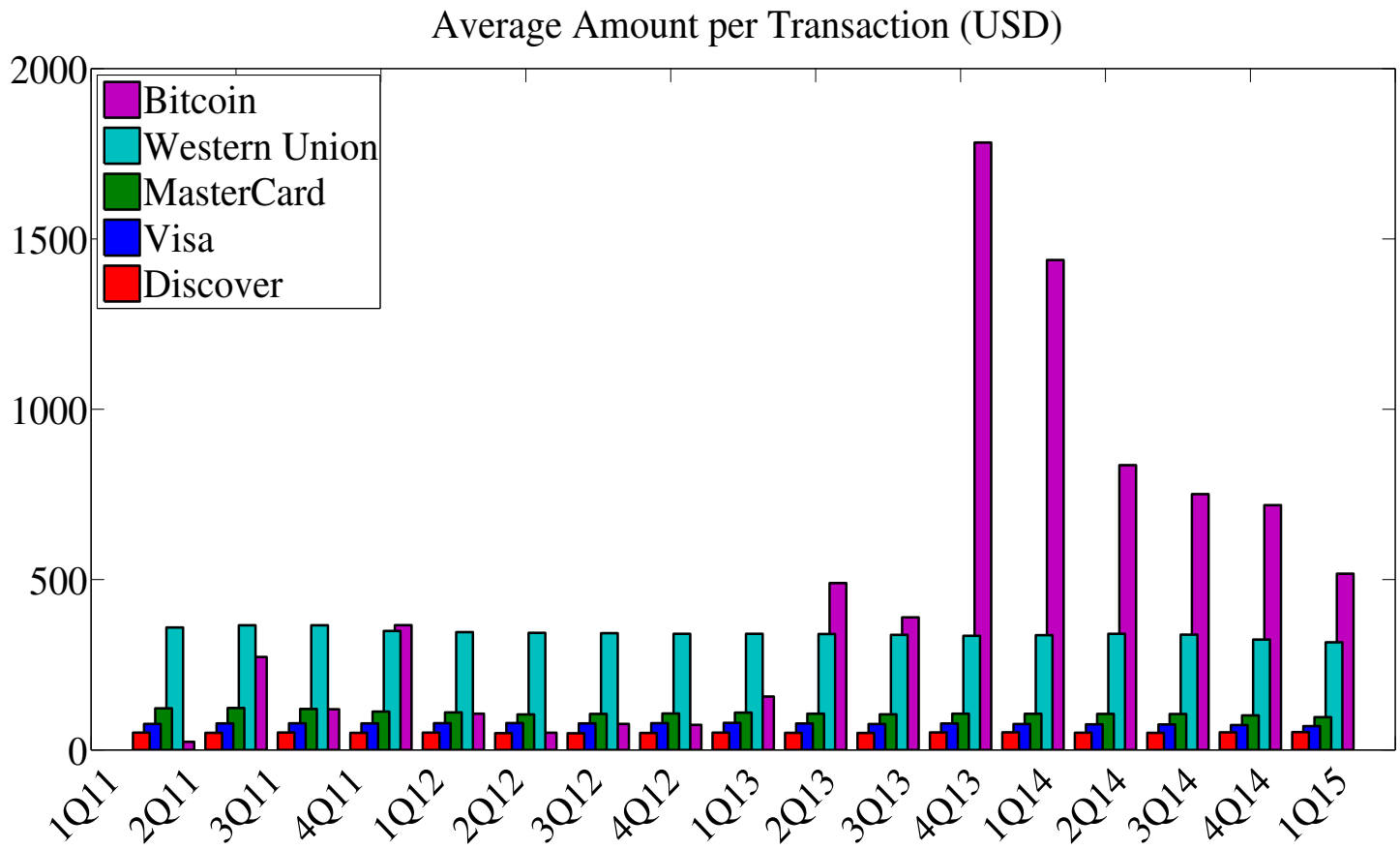


Figure: Comparison between different payment networks. Average daily USD amount per transaction from 1Q2011 to 1Q2015. Data source: Bitcoin blockchain, VISA, MasterCard, Discover, Western Union performance reports. Internal calculation.

Bitcoin as Currency. Network Expansion

The relative capitalisation of Bitcoin with regard to other digital currencies is receding in favour of Ripples.

- Until mid-2014, Bitcoin dominated the digital currency market by covering up to **95%** of its total volume.
- Since the 2nd part of 2014, the Bitcoin dominant position has been eroded by Ripple, which now covers about **10%** of the total market capitalisation.
- Even though Bitcoin remains dominant on the digital currency market, the relative currency strength of Bitcoin has **decreased** – on average –, compared to that of the other (almost) existing 500 digital currencies.

Bitcoin as Currency. Network Expansion

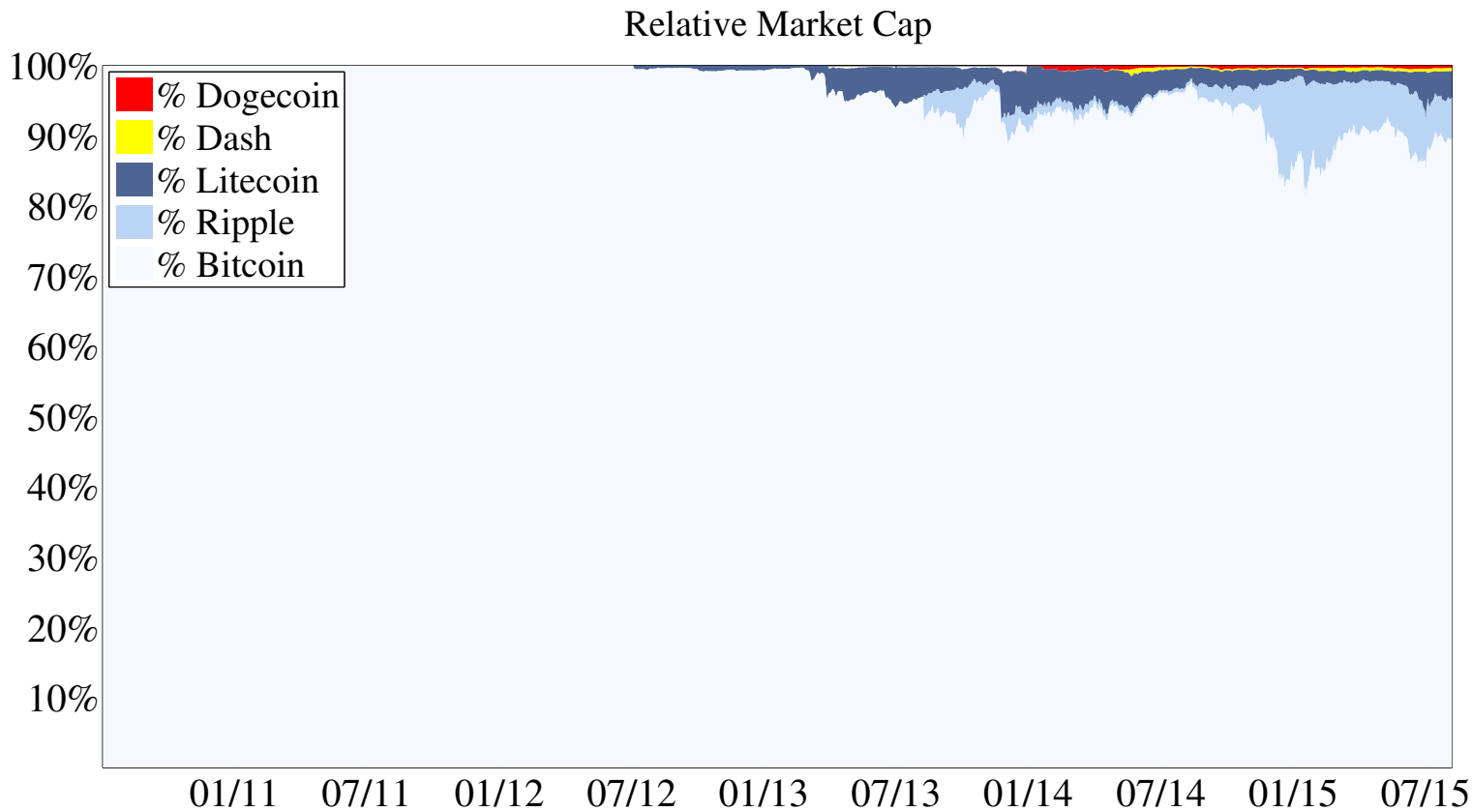


Figure: Relative market capitalisation of Bitcoin, Ripple, Litecoin, Dash, Dogecoin. Data source : Coinmarketcap. Internal calculation.

Bitcoin as Currency. Currency Competition

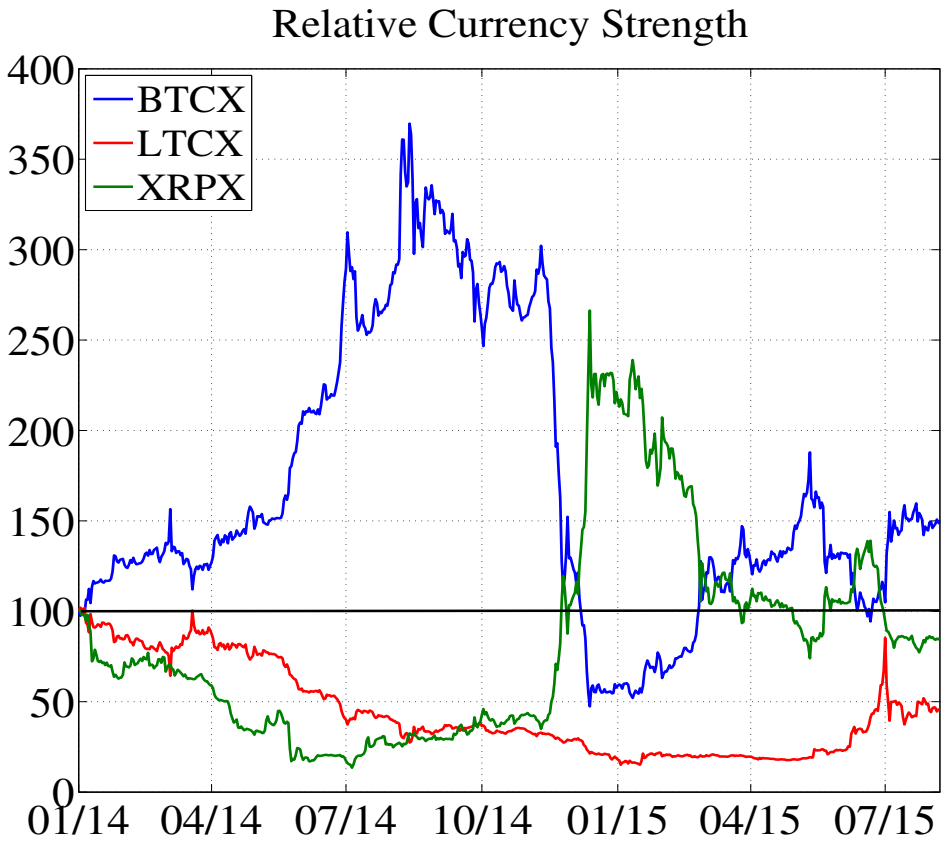


Figure: Comparison between relative index strengths. Ba= 100 on 01.01.2014 (BTCX, LTCX, XRPX). Internal calculation.

Bitcoin as Currency. Currency Competition

- 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.

Currency competition expressed in currency strength indices

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

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

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

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.

Groups of Interest. Investors

Bitcoin startups raised almost USD 1 billion in three years with an annual investment growth rate of about 150%

- Capital investments in Bitcoin-related startups is a recent trend that started in 1Q 2012.
- Since 1Q 2012, the Bitcoin industry represents the **fastest growing sector** for capital investment.
- Within the Bitcoin sector, the **Mining** and **Payment & Remittance** industries drove the funding race.
- 21 Inc alone covered over half of the capital raised by the Mining industry and Coinbase one third of the capital raised by the whole Payment & Remittance industry.

Groups of Interest. Investors

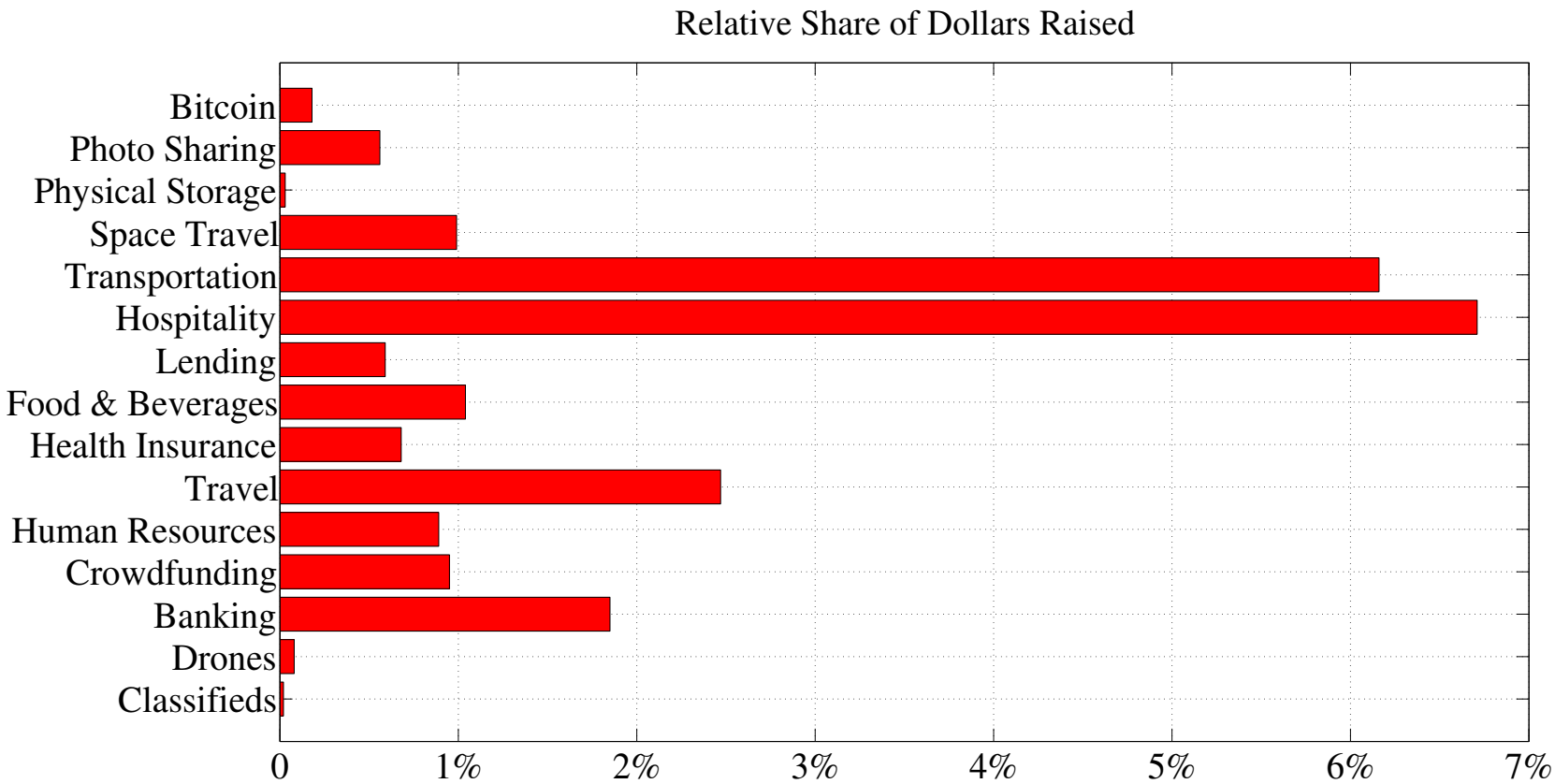


Figure: Relative Capital investment into different startup businesses during the period mid-2012 till mid-2015. Data source: Mattermark. Internal calculation.

Groups of Interest. Investors

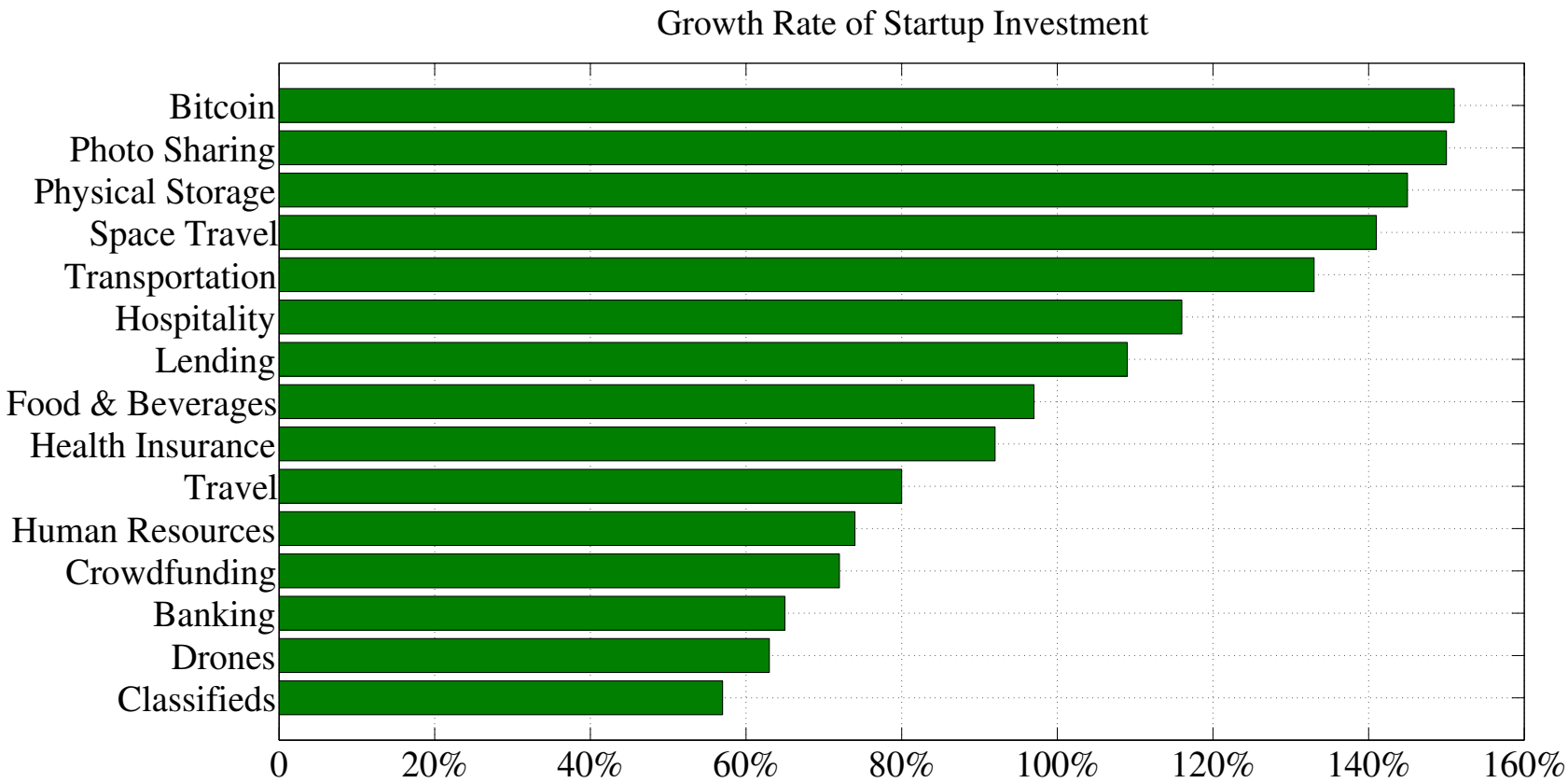


Figure: Relative rate of growth of capital investment into different startup businesses during the period mid-2012 till mid-2015. Data source: Mattermark. Internal calculation.

Groups of Interest. Investors

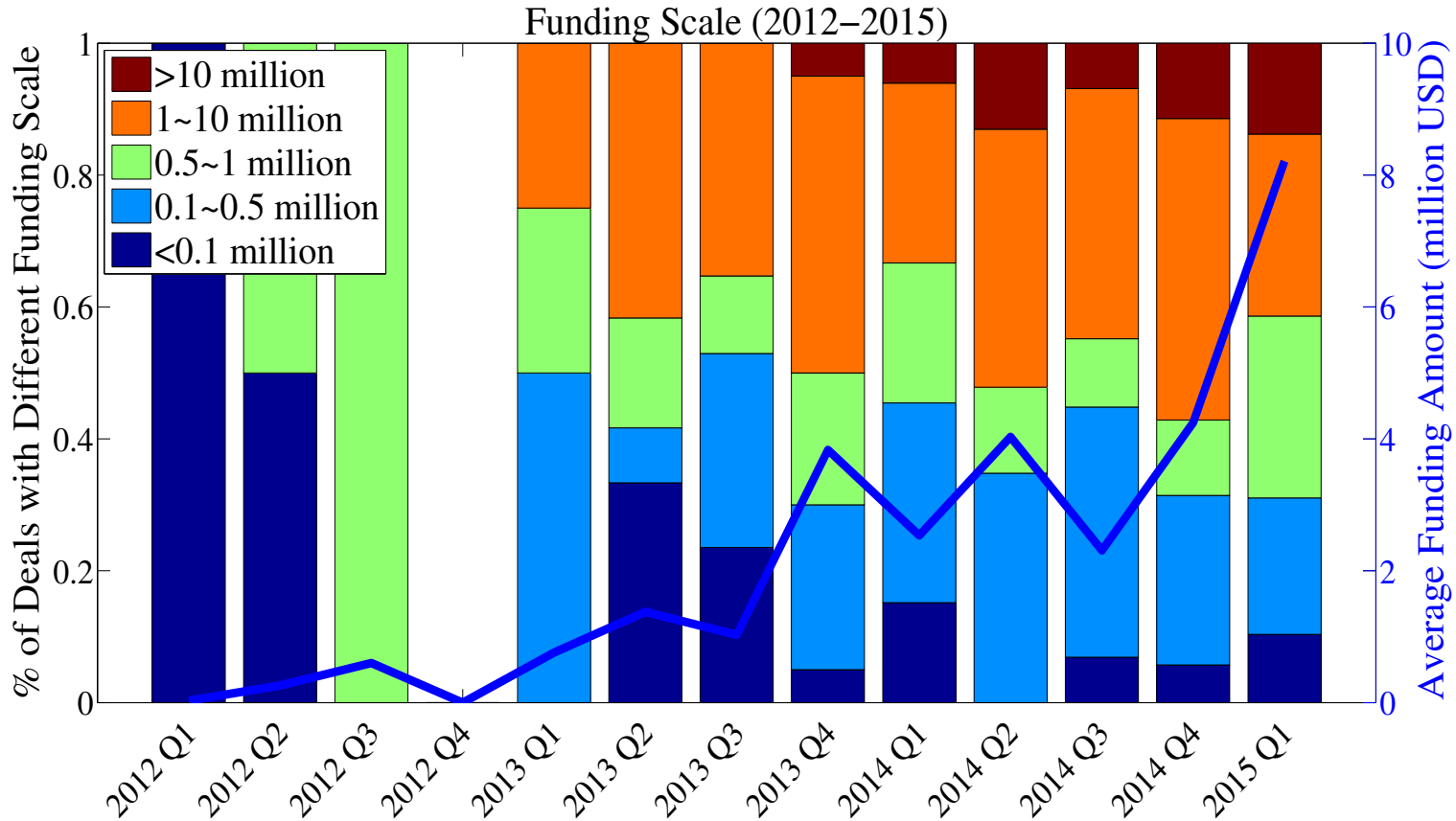


Figure: Bar chart: Percentage of deals in different funding scales, from Q1/2012 to Q1/2015. Line chart: Average funding amount per deal in each quarter. Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

Groups of Interest. Investors

Capital Market	**Payment and Remittance**	**Financial Services**	**Blockchain Application**	**Mining Industry**	**Miscellaneous**
Exchange	Payment	Accounting	Smart Contracts	Mining Solutions	Bitcoin Faucet
Derivatives	Remittance	Security	Blockchain API	Mining Pool	Tipping
Commodity	Wallet	ATM			Messaging
Institutional Trading		Market and			
Crowdfunding and		Data Analysis			
Crypto Equity					

Table: Classification of business categories in the Bitcoin industry.

Groups of Interest. Investors

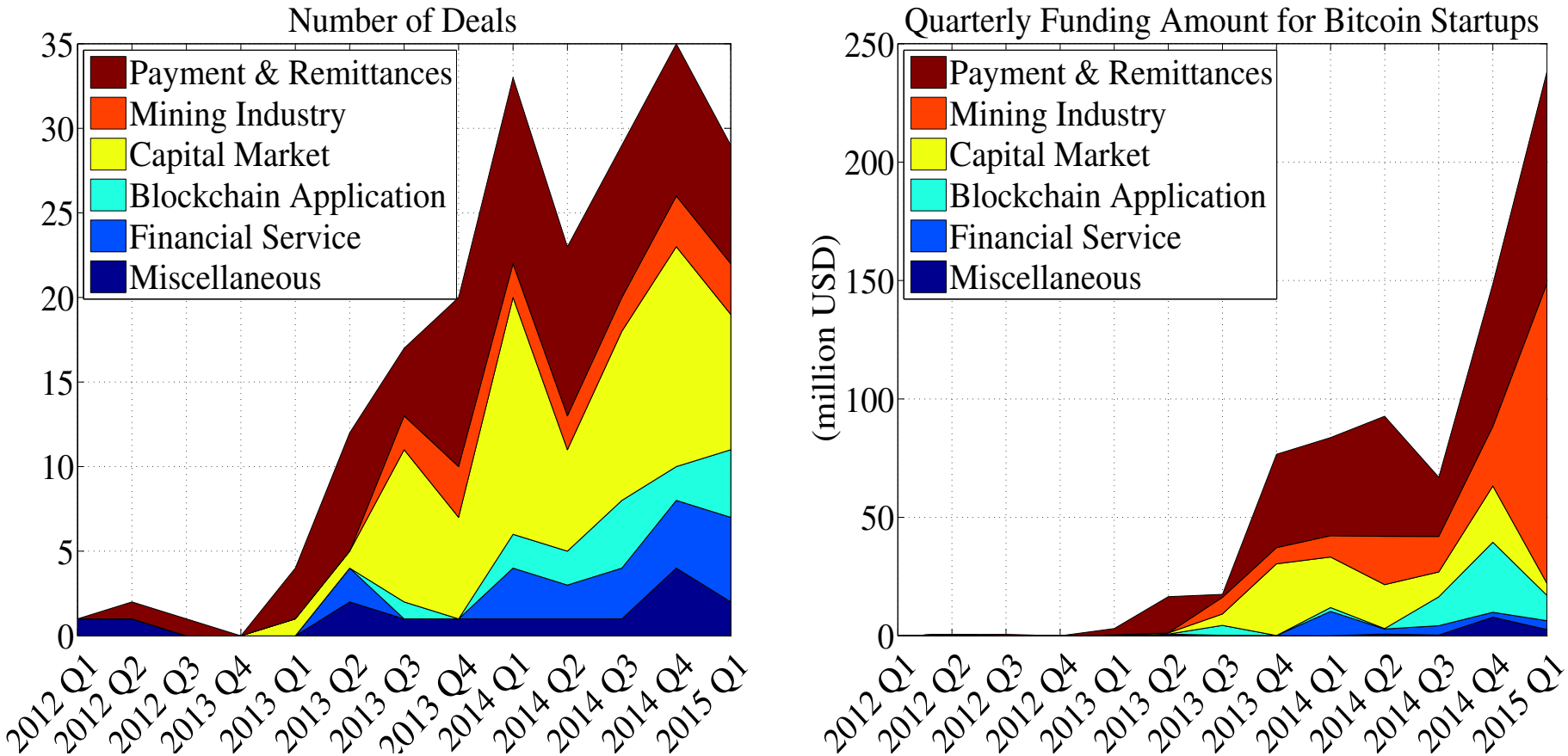


Figure: Left: Quarterly number of deals for startups in different Bitcoin industries. Right: Quarterly funding amount for startups in different Bitcoin industries. Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

Groups of Interest. Investors

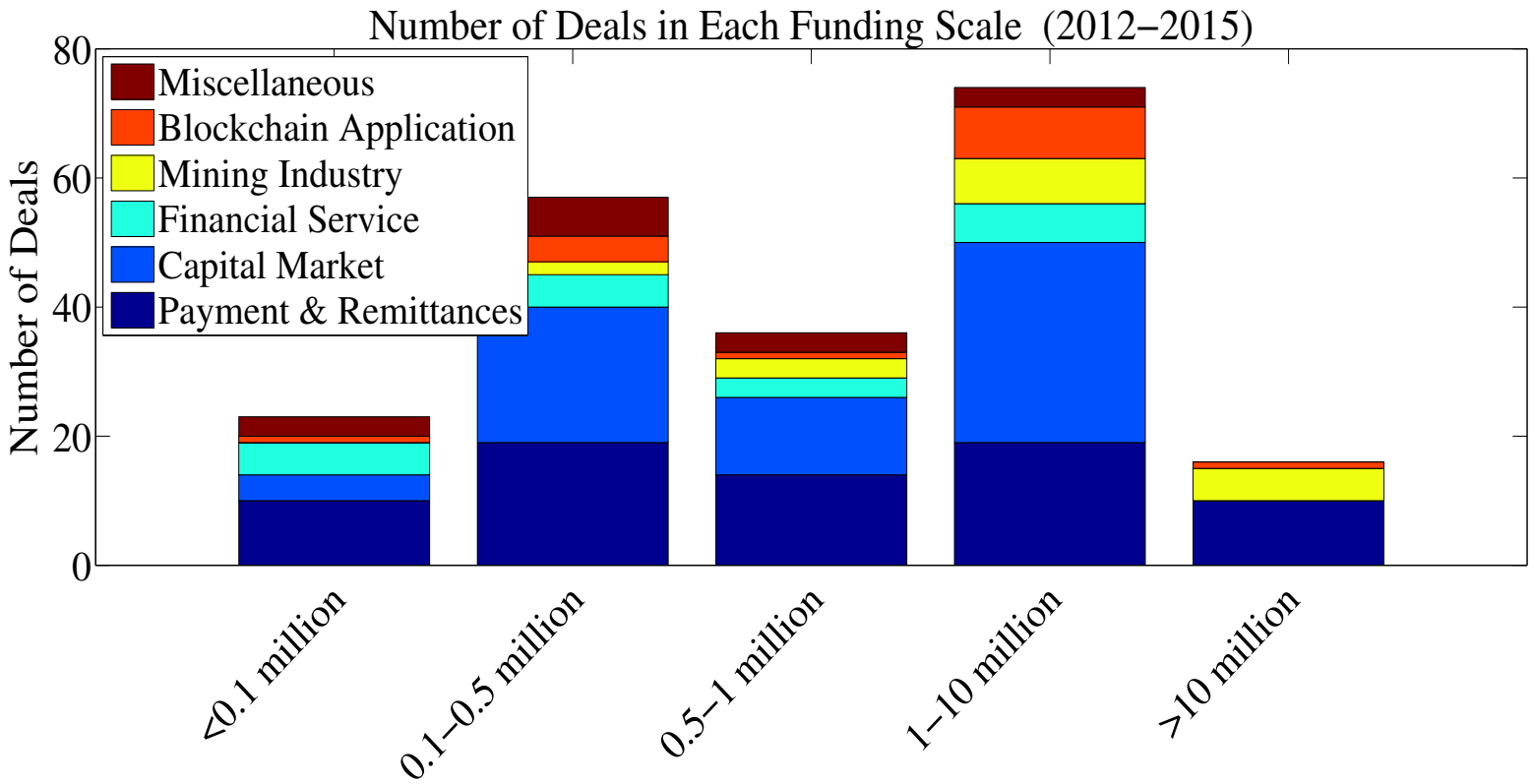


Figure: Number of deals in each funding scale (Q1/2012 to Q1/2015). Deals in each funding scale are further divided into business categories. Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

Groups of Interest. Investors

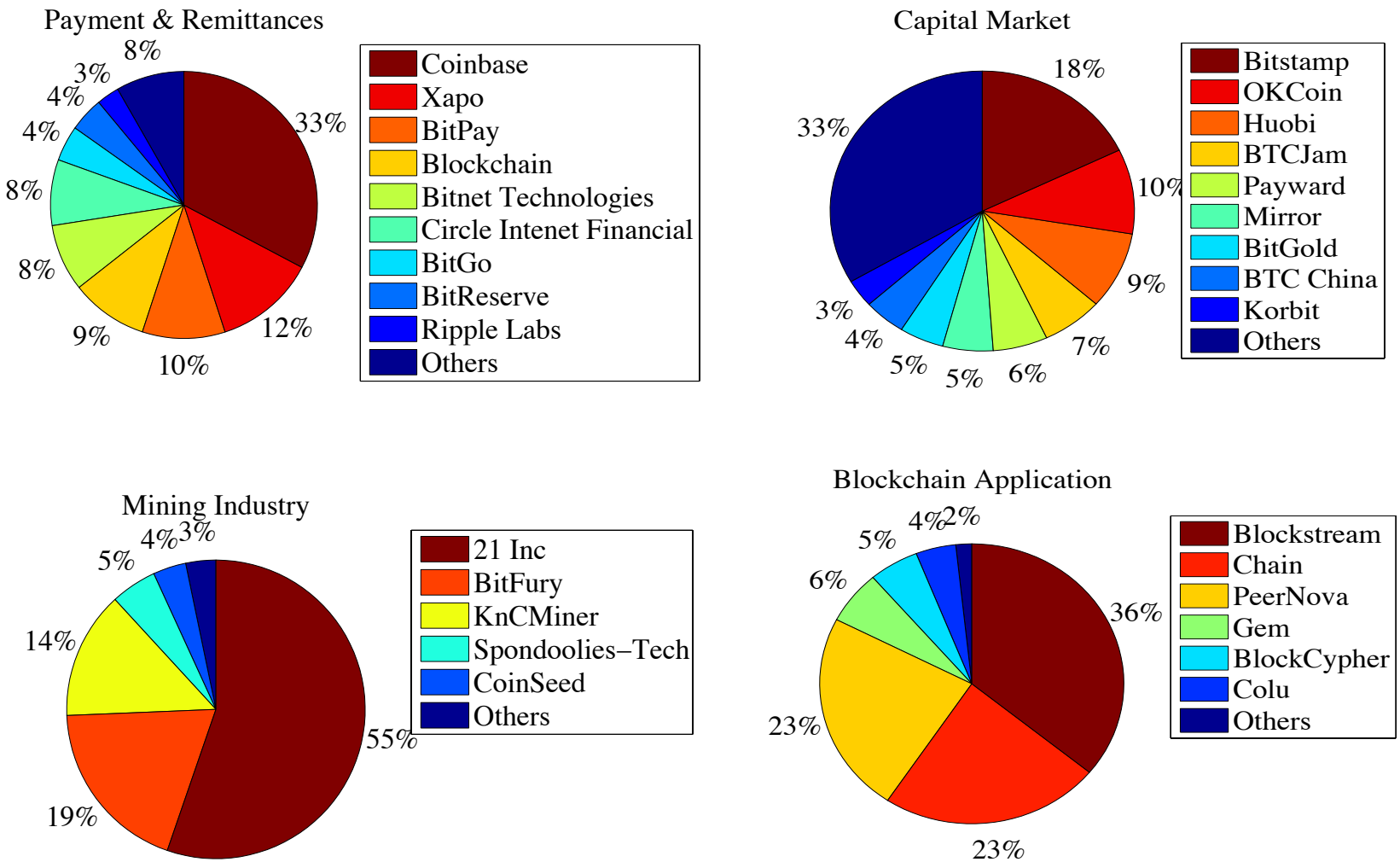


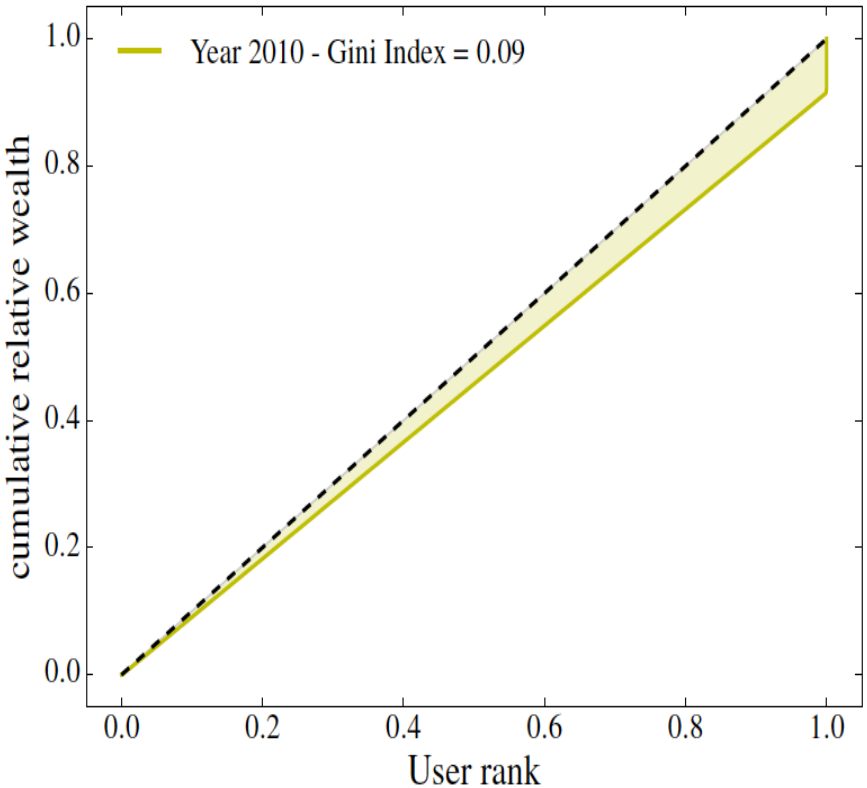
Figure: Funding distribution among startups within main categories (Q1/2012 – Q1/2015).
Data source: Bitangel, Cbinsight, Coinfilter, Coindesk, Crunchbase. Internal calculation.

Distribution of Income and Wealth.

The wealth distribution in the Bitcoin ecosystem is highly unequal,and this inequality is growing.

- The inequality of the distribution of Bitcoins amongst addresses, summarised by the Gini coefficient grew **from 0.09 in 2010 to 0.99 in 2015**.
- 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 Bitcoin mining market is under control by 5 to 7 major mining pools.
- During the period 2013-2015, the cumulative market share of the largest 10 pools relative to the total market hovered in the **70% – 80%** range.

Distribution of Income and Wealth. Users



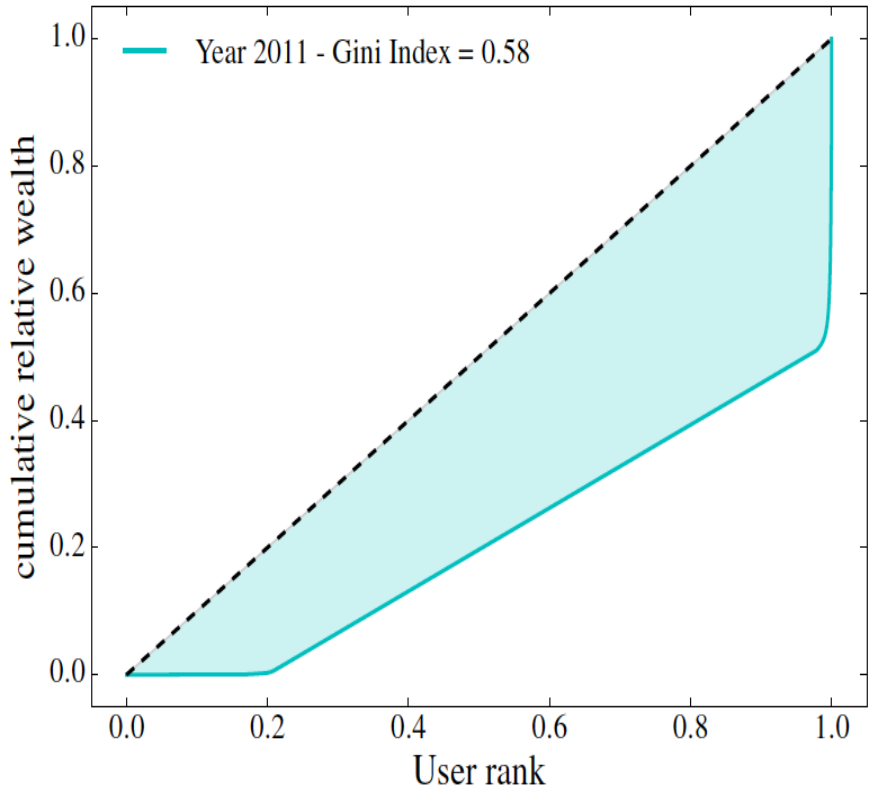
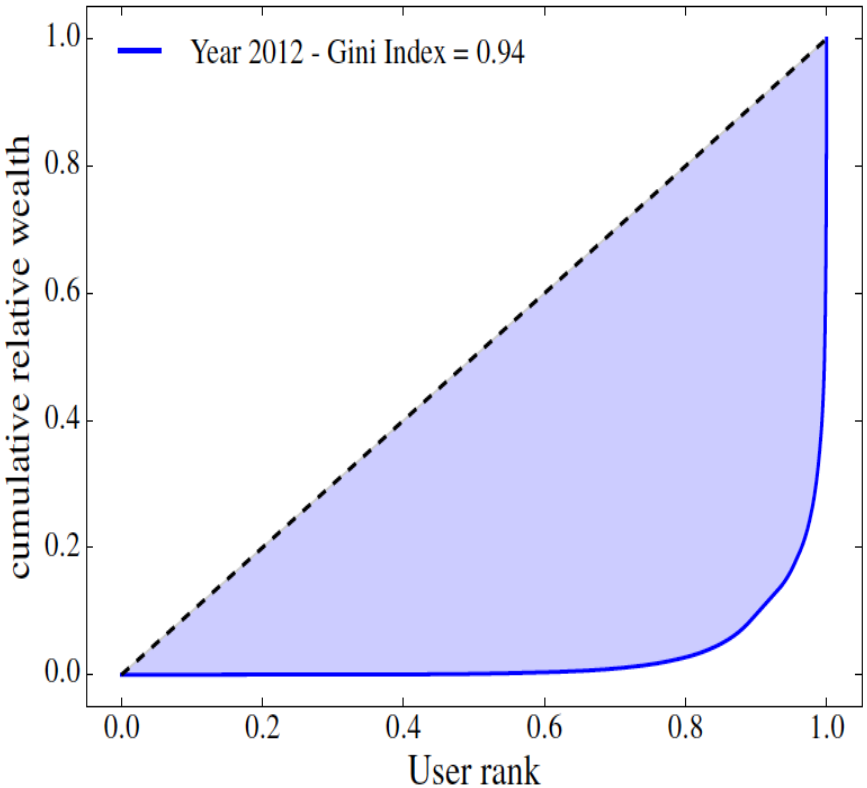


Figure: Lorenz Curve and Gini Coefficient for the Bitcoin Economy. Percentile of addresses sorted by wealth wrt to the percentile of the wealth own.

Distribution of Income and Wealth. Users



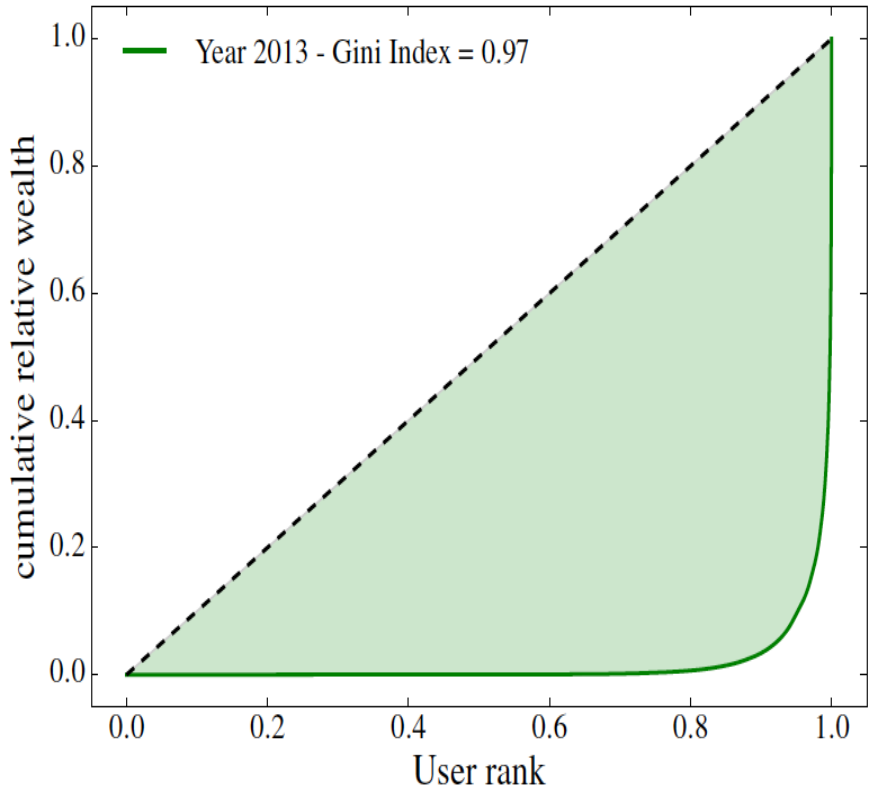
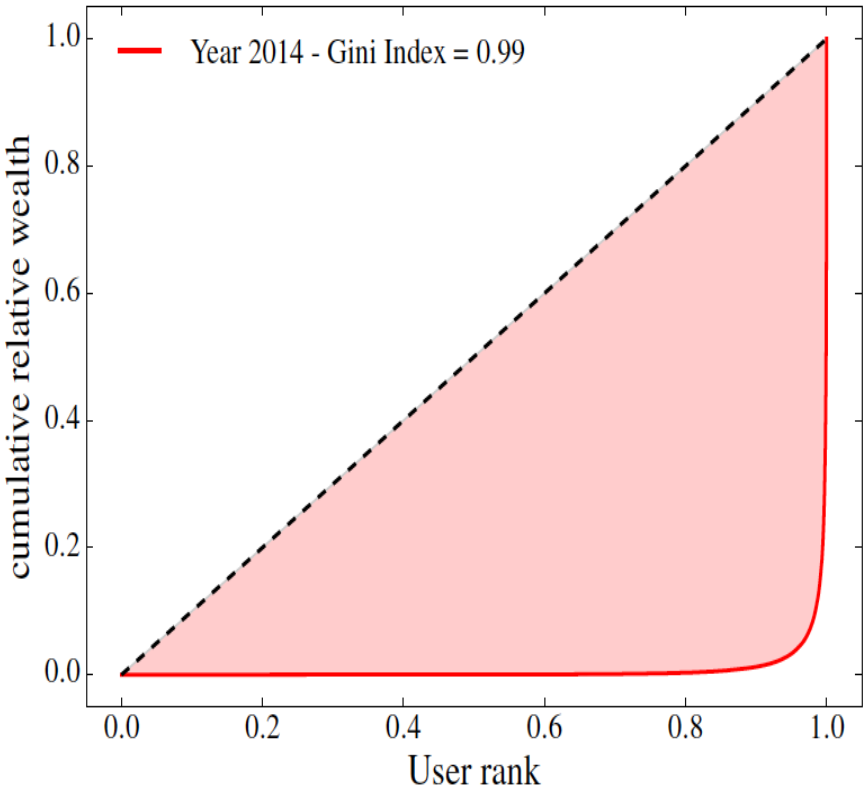


Figure: Lorenz Curve and Gini Coefficient for the Bitcoin Economy. Percentile of addresses sorted by wealth wrt to the percentile of the wealth own.

Distribution of Income and Wealth. Users



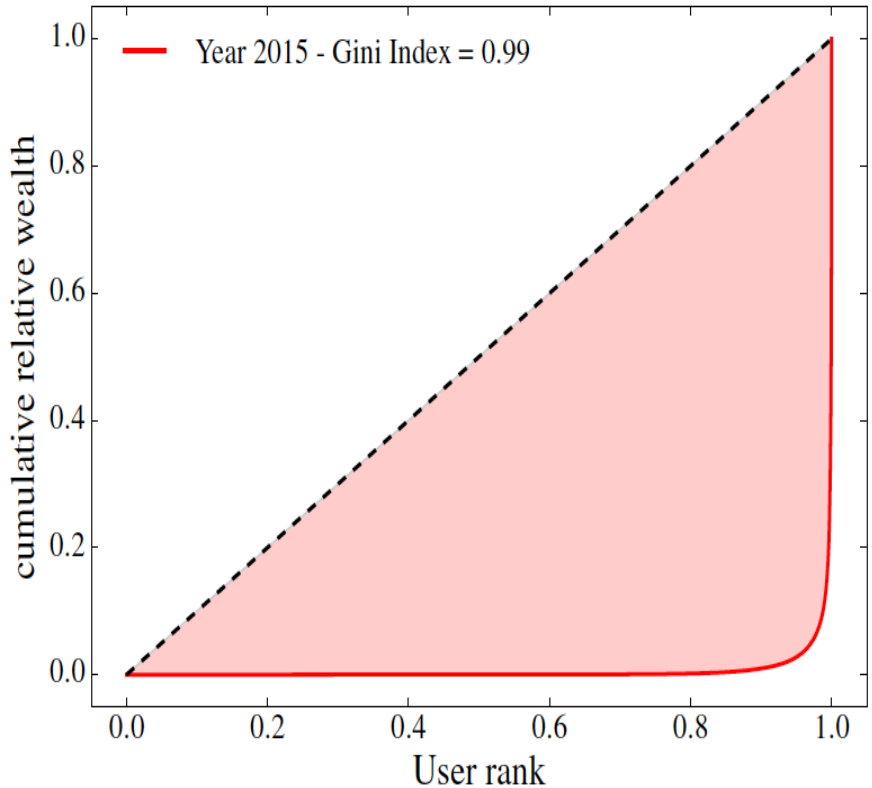


Figure: Lorenz Curve and Gini Coefficient for the Bitcoin Economy. Percentile of addresses sorted by wealth wrt to the percentile of the wealth own.

Distribution of Income and Wealth. Users

The Gini coefficient (G) is an inequality index of income or wealth.[3]

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.

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

Distribution of Income and Wealth. Users

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 $i = 1, ..., n$:

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

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

Distribution of Income and Wealth. Users

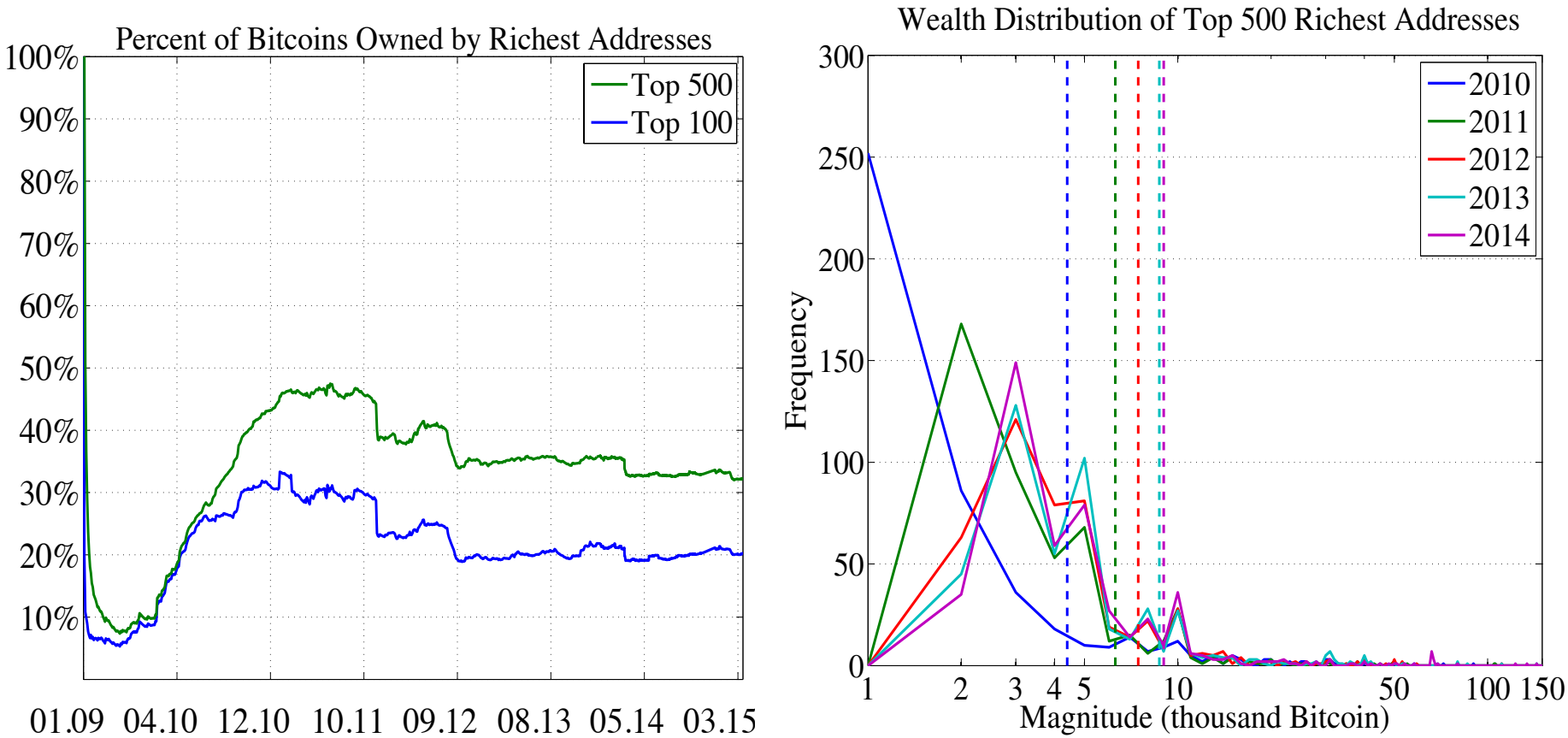
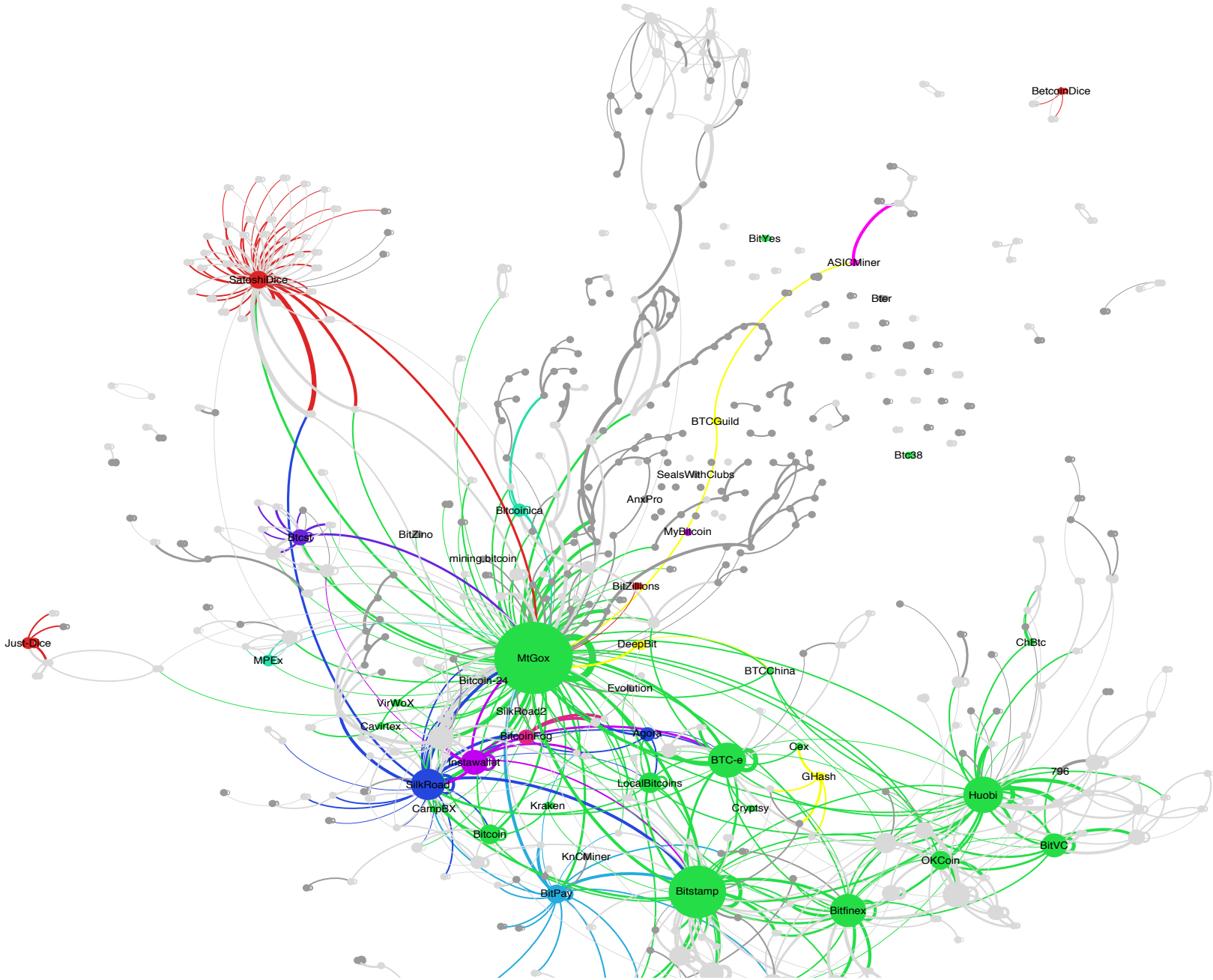
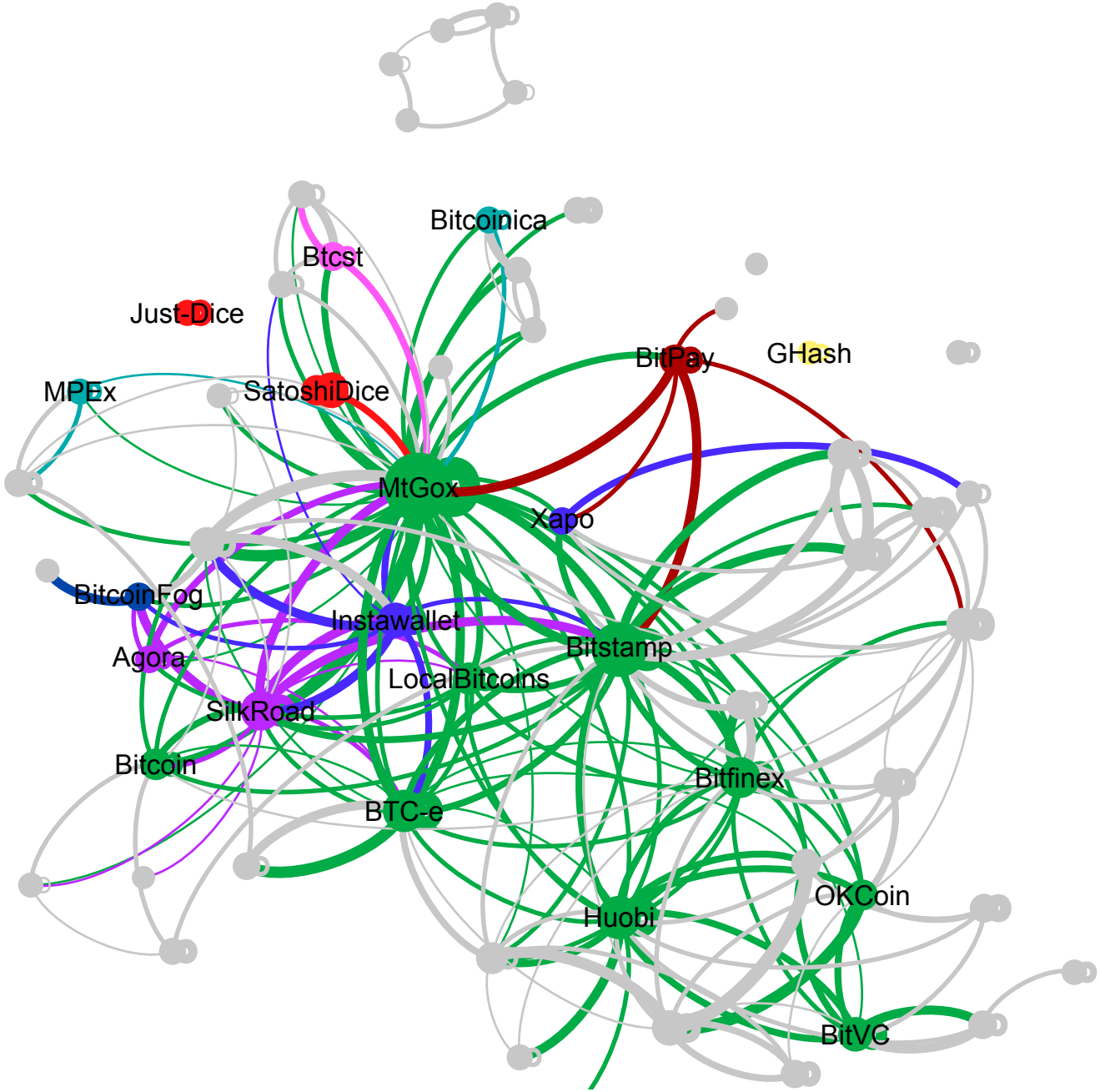


Figure: Left: Relative wealth of the top 100 and 500 richest Bitcoin addresses. Right: Wealth distribution among the top 500 richest Bitcoin addresses (with x-axis log-transformed). Data source: Bitcoin blockchain. Internal calculation.

Distribution of Income and Wealth. Users



Distribution of Income and Wealth. Users



Distribution of Income and Wealth. Users

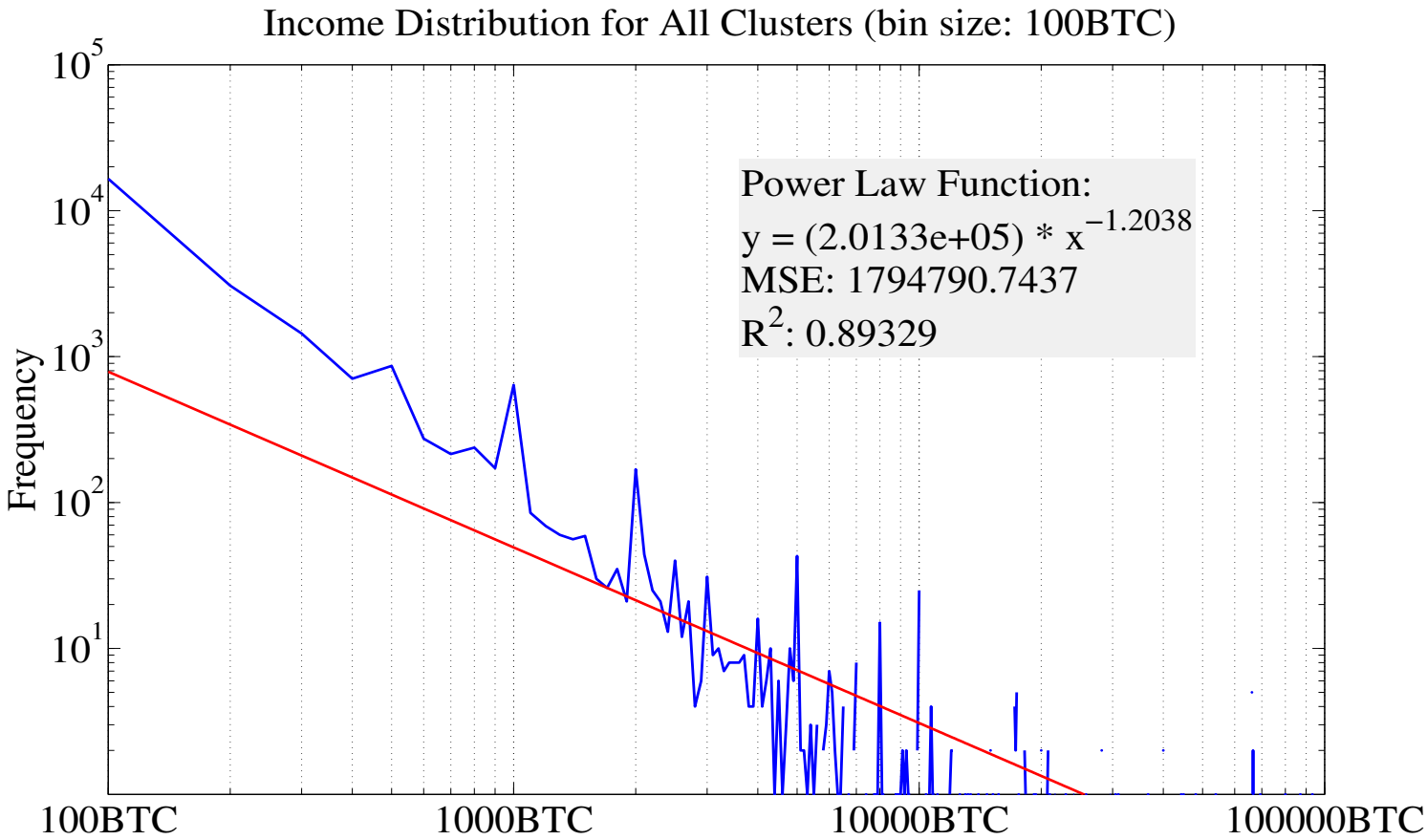
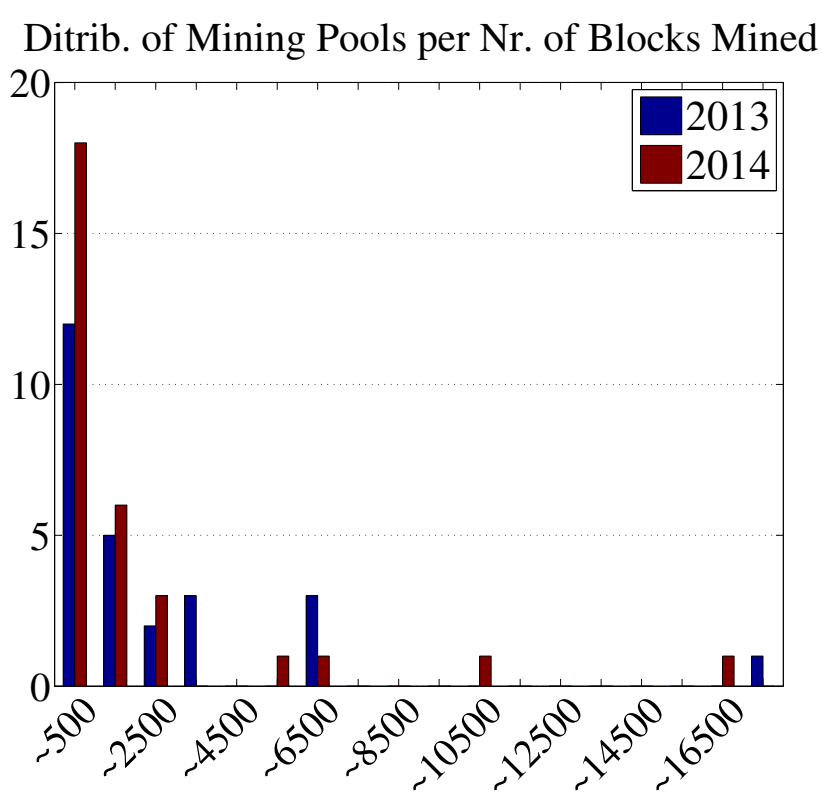


Figure: Income distribution for all clusters. Data source: Bitcoin Core parsed from the 3rd of January 2009 until the 8th of May 2015. Total nr. addresses: 75,191,953. Total nr. clusters (contains at least addresses): **30,708,660** (9,847,999 $\geq$ 2 nodes) and 4,810,342 with non-zero balance. Total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

Distribution of Income and Wealth. Miners



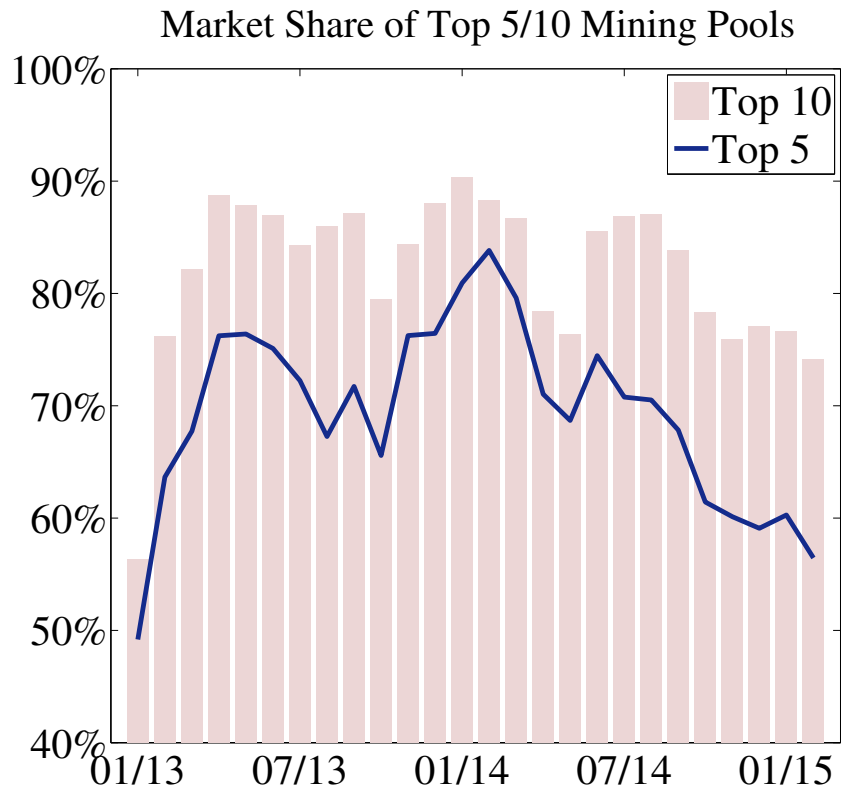


Figure: Left: Distribution of mining pools per number of blocks. Right: Market share of top 5 and 10 mining pools. Data source: Blocktrail. Internal calculation.

Distribution of Income and Wealth. Miners

- Ghash.IO hashing power was close to "51% attack" for several times.

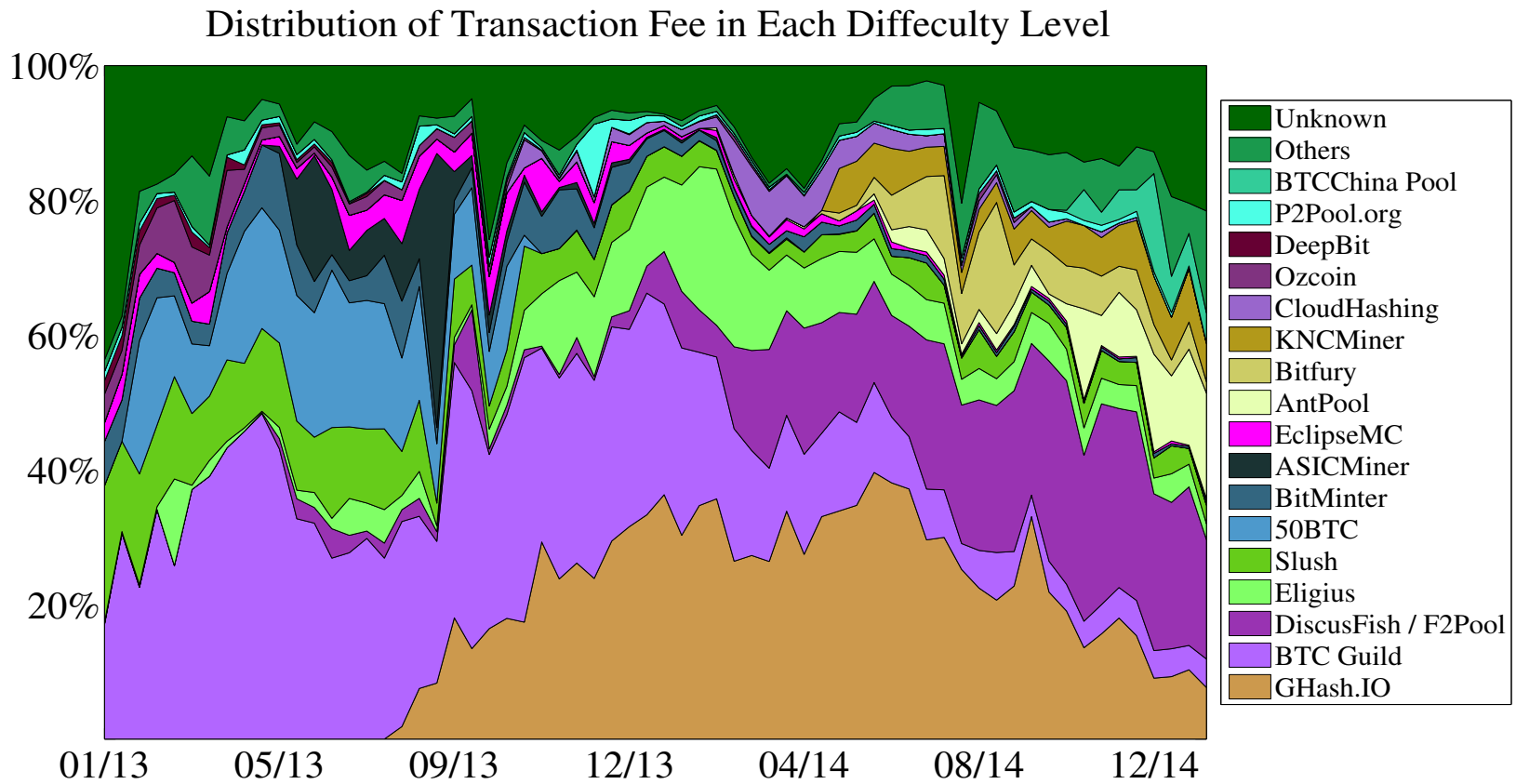


Figure: Top 17 mining pools (out of 40) per relative amount of fees earned. In each difficulty level, transaction fees collected by each mining pool are summed up and compared to the total fees earned and collected by the market. Period: From January 2013 to February 2015. Data source: Blocktrail. Internal calculation.

Distribution of Income and Wealth. Miners

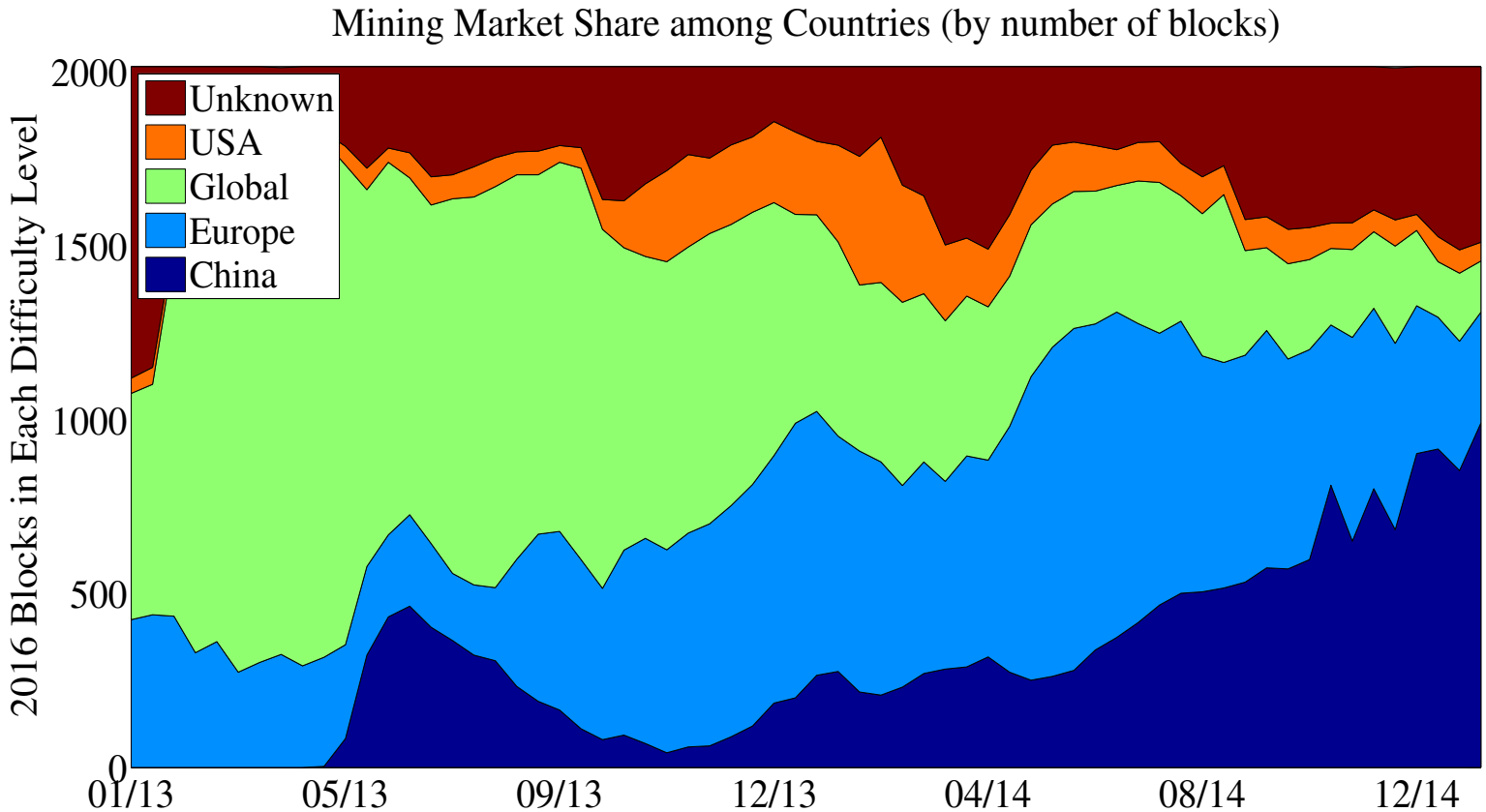


Figure: Top mining activity per country. Mining pools are classified per country of operation. Many mining pools operate in different countries (e.g, BTC Guild and BitMinter run their mining operation in both USA and Europe), so they are classified as "Global". Period: from January 2013 to February 2015. Data source: Blocktrail, Bitcoin Wiki (comparison of mining pools). Internal calculation.

Take-Home Message

1. The average amount transferred per Bitcoin transaction is larger than in any other major payment network.
2. The relative capitalisation of Bitcoin with regard to other digital currencies is receding in favour of Ripple's.
3. China is the largest country in the world per: (1) number of active Bitcoin clients; (2) mining capacity; (3) volume of Bitcoins exchanged via electronic trading platforms.
4. Bitcoin startups raised almost USD 1 billion in three years with an annual investment growth rate of about 150%.
5. In Jan. 2015 the Bitcoin volume exchanged on electronic trading platforms reached 50% of the total number of Bitcoins ever mined at that time.
6. During the year 2014, the transaction costs in digital currencies dropped significantly.
7. The year 2014 saw fewer incidences and less arbitrage opportunities than the previous years. In effect, the digital currency market is becoming more efficient.
8. The wealth distribution in the Bitcoin ecosystem is highly unequal, and this inequality is growing.
9. The Mining industry is consolidating as an oligopoly.