A Deep Dive into Bitcoin Mining Pools

An Empirical Analysis of Mining Shares

Matteo Romiti [1] Aljosha Judmayer [2]
Alexei Zamyatin [2, 3] Bernhard Haslhofer [1]

June 3, 2019

[1] Austrian Institute of Technology

[2] SBA Research

[3] Imperial College London

Introduction

Why do we care about miners?

Introduction

Why do we care about miners?

- Miners decide which transactions to include in a block

Introduction

Why do we care about miners?

- Miners decide which transactions to include in a block
- Miners decide which blocks to include in the chain

Introduction

Why do we care about miners?

- Miners decide which transactions to include in a block
- Miners decide which blocks to include in the chain
- Miners are rewarded with new coins and transaction fees

Introduction

Why do we care about miners?

- Miners decide which transactions to include in a block
- Miners decide which blocks to include in the chain
- Miners are rewarded with new coins and transaction fees
- Miners secure the network (Proof-of-Work algorithm)

Introduction

Why do we care about miners?

- Miners decide which transactions to include in a block
- Miners decide which blocks to include in the chain
- Miners are rewarded with new coins and transaction fees
- Miners secure the network (Proof-of-Work algorithm)
- Miners can attack the network (e.g., double-spend)

Introduction

What about Mining Pools?

Introduction

What about Mining Pools?

- Solo mining is not profitable anymore

Introduction

What about Mining Pools?

- Solo mining is not profitable anymore
- Miners join pools for steadier revenues

Introduction

What about Mining Pools?

- Solo mining is not profitable anymore
- Miners join pools for steadier revenues
- Pools compete to create blocks and claim the rewards

Introduction

What about Mining Pools?

- Solo mining is not profitable anymore
- Miners join pools for steadier revenues
- Pools compete to create blocks and claim the rewards
- Pool managers coordinate work and rewards among members

Introduction

What about Mining Pools?

- Solo mining is not profitable anymore
- Miners join pools for steadier revenues
- Pools compete to create blocks and claim the rewards
- Pool managers coordinate work and rewards among members
- Miners can join multiple pools (Cross-Pool Mining)

Introduction

Research Questions

Introduction

Research Questions

1. How did the mining centralization evolve? How decentralized is Bitcoin mining now?

Introduction

Research Questions

1. How did the mining centralization evolve? How decentralized is Bitcoin mining now?
2. How does a pool distribute the rewards? How can we detect payments to pool members?

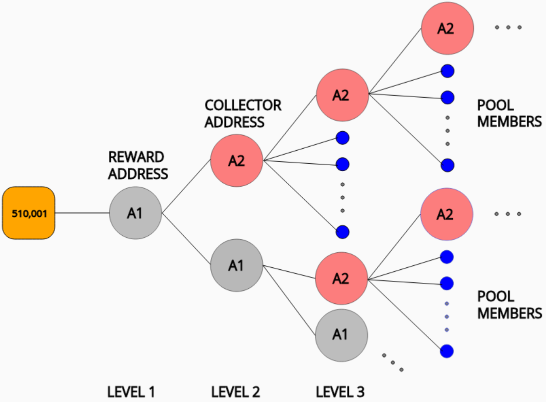
Introduction

Research Questions

1. How did the mining centralization evolve? How decentralized is Bitcoin mining now?
2. How does a pool distribute the rewards? How can we detect payments to pool members?
3. How decentralized is a mining pool? What do we know about pool members?

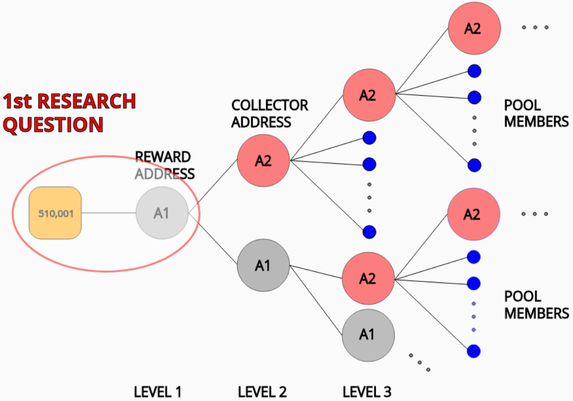
Background

Background — Coinbase Flow



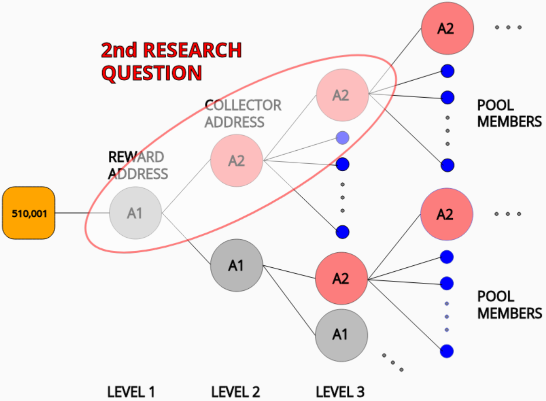
Example of a coinbase flow

Background — Coinbase Flow



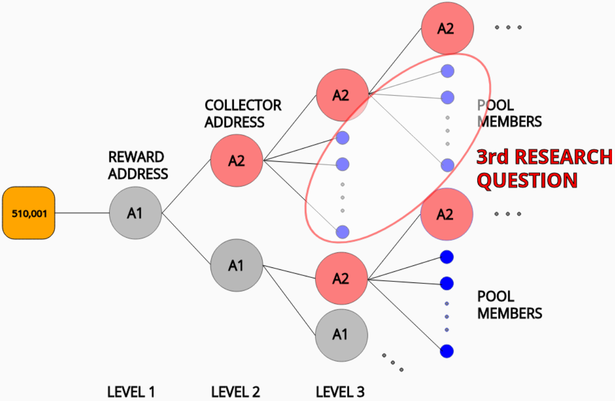
Example of a coinbase flow

Background — Coinbase Flow



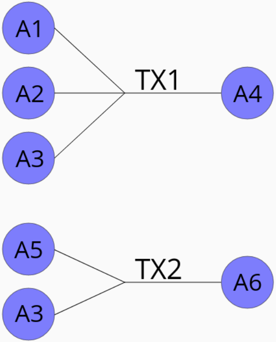
Example of a coinbase flow

Background — Coinbase Flow



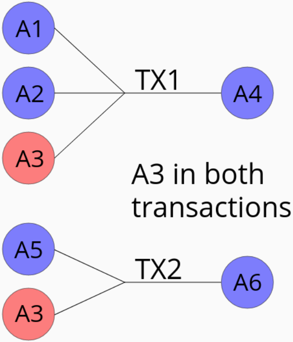
Example of a coinbase flow

Background — Multiple-Input Clustering Heuristic



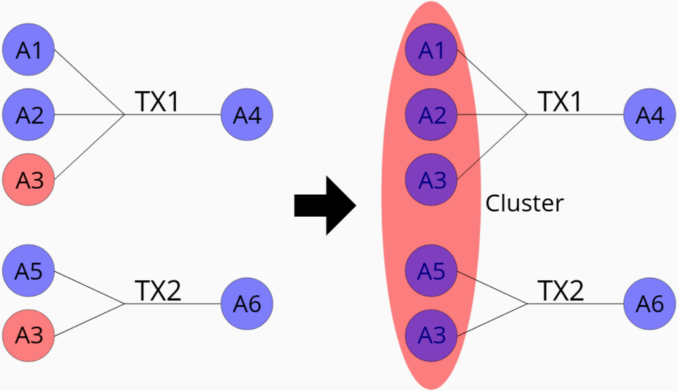
Multiple-input clustering heuristic

Background — Multiple-Input Clustering Heuristic



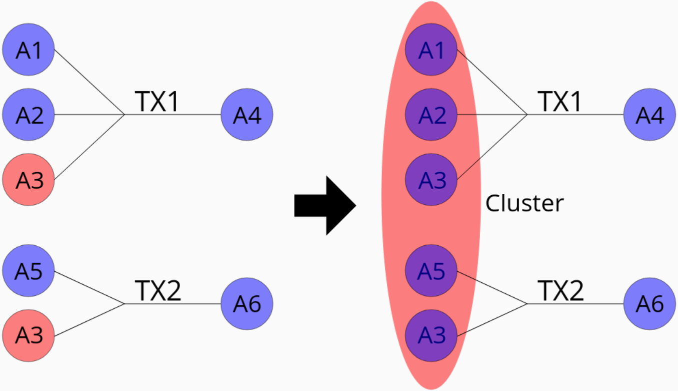
Multiple-input clustering heuristic

Background — Multiple-Input Clustering Heuristic



Multiple-input clustering heuristic

Background — Multiple-Input Clustering Heuristic



GRAPHSENSE

How did the mining centralization evolve? How decentralized is Bitcoin mining now?

Block Attribution — Data Sources

We combined different publicly-available data sources:

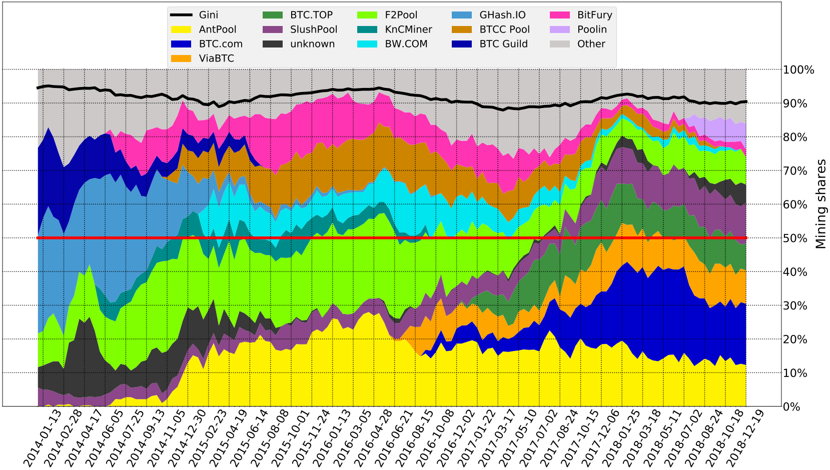
- Blocktrail API (till block 514239, March 2018)
- Blockchain.info Github repository
- BTC.com Github repository
- GraphSense
- Coinbase markers manually retrieved

Block Attribution — Conflicts

684 attribution conflicts out of 556400 blocks (0.0012%)

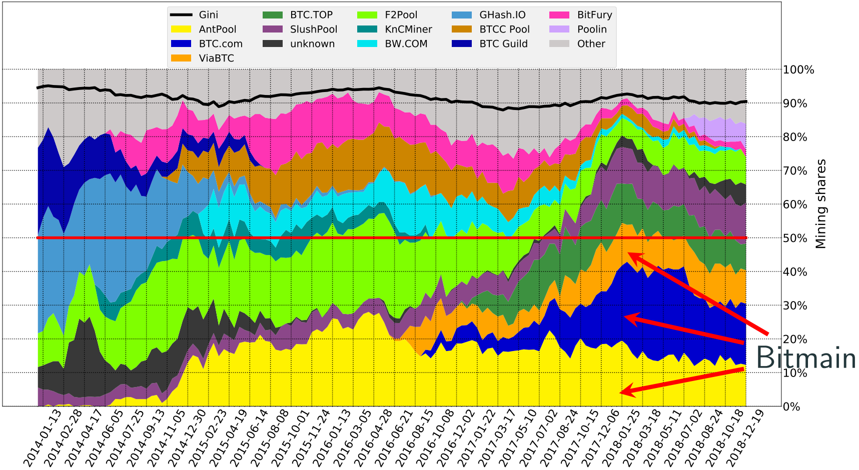
Miner 1	Miner 2	#Conflicts
BTC.TOP	CANOE	338
Bixin	TangPool	142
BTC.com	Waterhole	113
BTC.TOP	WAYI.CN	81

Block Attribution — Mining Shares

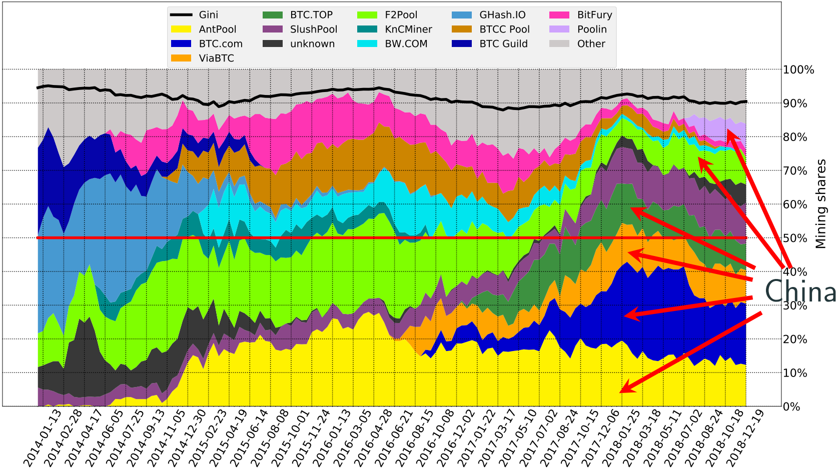


Evolution of mining pools’ shares (2013-12-21 to 2018-12-19)

Block Attribution — Mining Shares



Block Attribution — Mining Shares

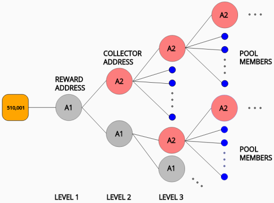


China

How does a pool distribute the rewards? How can we detect payments to pool members?

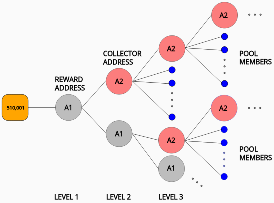
Payout Patterns — Data Sources

- Coinbase flows from Blockchain.info API

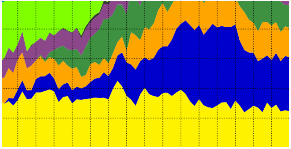


Payout Patterns — Data Sources

- Coinbase flows from Blockchain.info API

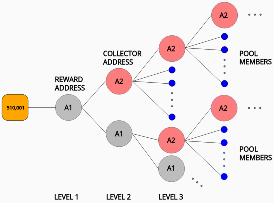


- Focus on BTC.com, AntPool and ViaBTC

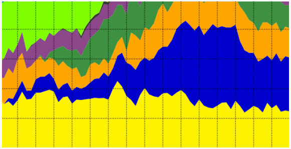


Payout Patterns — Data Sources

- Coinbase flows from Blockchain.info API

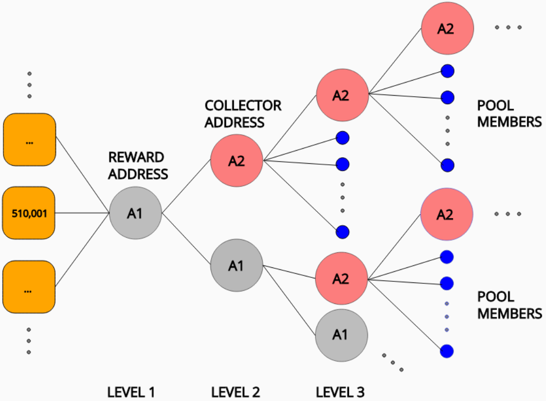


- Focus on BTC.com, AntPool and ViaBTC



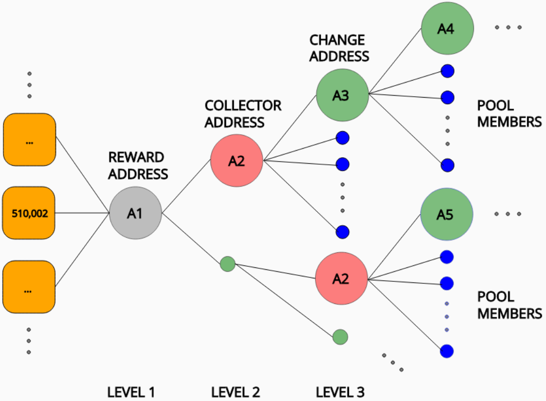
- From block 510,000 to 514,032

Payout Patterns — BTC.com



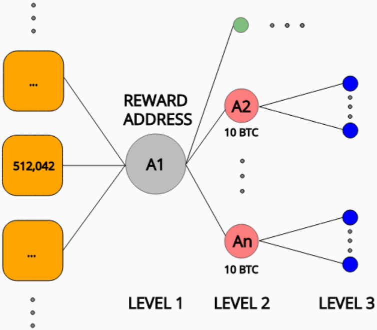
BTC.com payout pattern between block 510,000 and 514,032

Payout Patterns — AntPool



AntPool payout pattern between block 510,000 and 514,032

Payout Patterns — ViaBTC



ViaBTC payout pattern observed between block 510,000 and 514,032

Payout Patterns — Results

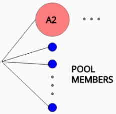
Statistics of data retrieved between block 510,000 and 514,032

Pool	Mined Blocks	Txs Found	BTC Coverage	Address Reuse Index
BTC.com	1,020	225	92%	9.8
AntPool	617	408	30%	1.4
ViaBTC	457	104	75%	7.0

How decentralized is a mining pool? What do we know about pool members?

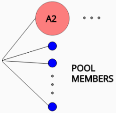
Pools Members — Data Sources

- Payout transactions (BTC.com, AntPool and ViaBTC)

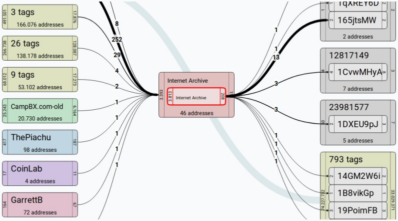


Pools Members — Data Sources

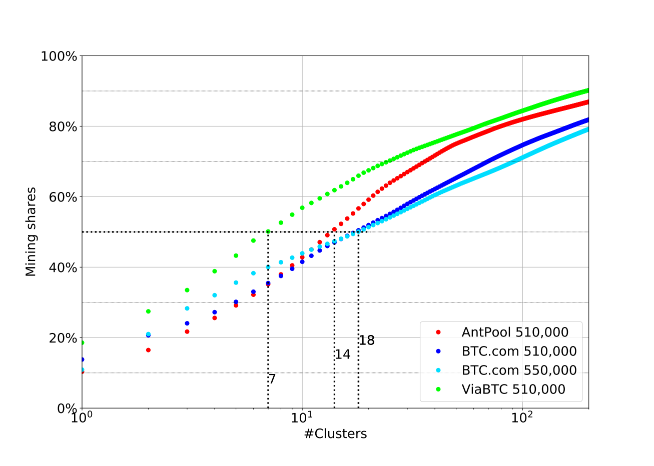
- Payout transactions (BTC.com, AntPool and ViaBTC)



- GraphSense (Clustering and Tags)

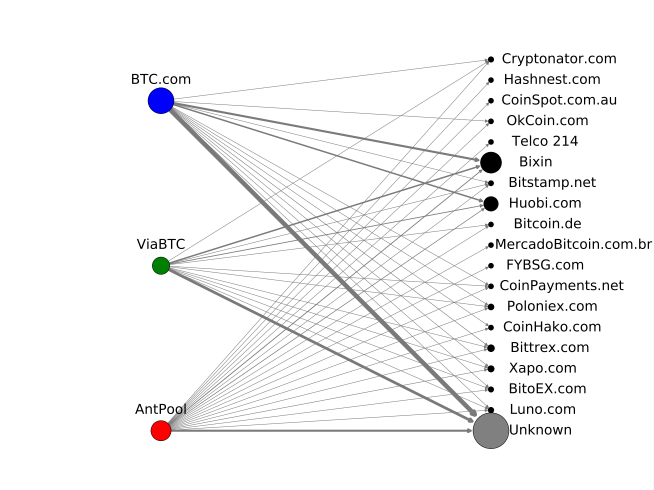


Pools Members — Pool Centralization



Cumulative sum of mining shares over clusters for each pool

Pools Members — Cross-Pool Mining



Distribution of mining rewards among top members

Pools Members — Main Entities

Cross-pool mining between block 510,000 and 514,032. W: wallet provider, E: exchange service, P: mining pool, M: unknown mining entity

		BTC.com			AntPool			ViaBTC			
Entity/Actor	Service	BTC	%BTC	#Addr.	BTC	%BTC	#Addr.	BTC	%BTC	#Addr.	Total BTC
Unknown	?	8930.39	**74.07**	13286	1682.25	**72.09**	8888	2877.02	**67.17**	4845	13489.67
Bixin	W+E+P	1663.75	13.80	1061	241.28	10.34	546	795.36	18.57	476	2700.39
Huobi.com	E	808.64	6.71	964	142.04	6.09	759	225.50	5.27	322	1176.19
Bittrex.com	E	83.71	0.69	348	29.56	1.27	251	43.36	1.01	177	156.63
Xapo.com	W	26.96	0.22	94	70.75	3.03	64	5.79	0.14	33	103.50
Poloniex.com	E	42.65	0.35	381	11.52	0.49	268	19.97	0.47	139	74.15
Luno.com	W+E	36.59	0.30	258	4.06	0.17	104	4.39	0.10	60	45.04
Bitstamp.net	E	8.94	0.07	57	3.55	0.15	38	3.91	0.09	22	16.39
Cryptonator.com	W+E	5.75	0.05	80	0.70	0.03	41	2.70	0.06	33	9.15

Conclusion

Conclusion

1. Mining centralization has followed a cyclical pattern so far

Conclusion

1. Mining centralization has followed a cyclical pattern so far
2. Three to four mining pools control 51% of mining

Conclusion

1. Mining centralization has followed a cyclical pattern so far
2. Three to four mining pools control 51% of mining
3. Bitmain and China play a key role in the mining industry

Conclusion

1. Mining centralization has followed a cyclical pattern so far
2. Three to four mining pools control 51% of mining
3. Bitmain and China play a key role in the mining industry
4. Major pools follow specific patterns to distribute mining rewards

Conclusion

1. Mining centralization has followed a cyclical pattern so far
2. Three to four mining pools control 51% of mining
3. Bitmain and China play a key role in the mining industry
4. Major pools follow specific patterns to distribute mining rewards
5. Major pools show centralization tendencies (50% of the identified BTC goes to 18 or less members)

Conclusion

1. Mining centralization has followed a cyclical pattern so far
2. Three to four mining pools control 51% of mining
3. Bitmain and China play a key role in the mining industry
4. Major pools follow specific patterns to distribute mining rewards
5. Major pools show centralization tendencies (50% of the identified BTC goes to 18 or less members)
6. Miners are active across multiple pools

Conclusion

1. Mining centralization has followed a cyclical pattern so far
2. Three to four mining pools control 51% of mining
3. Bitmain and China play a key role in the mining industry
4. Major pools follow specific patterns to distribute mining rewards
5. Major pools show centralization tendencies (50% of the identified BTC goes to 18 or less members)
6. Miners are active across multiple pools
7. Miners use exchanges and wallet services to receive payouts

Future work

Future work

- Classification of entities and collaborative tag sharing
- Improve heuristics to find more payments and extend work to other pools
- IP-network traffic measurements

Links

- **Slides**: `https://github.com/MatteoRomiti/WEIS_Deep_Dive_slides`
- **Graphsense**: `https://graphsense.info/`
- **Code**: `https://github.com/MatteoRomiti/Deep_Dive_BTC_Mining_Pools`

Appendix

Block Attribution — Results

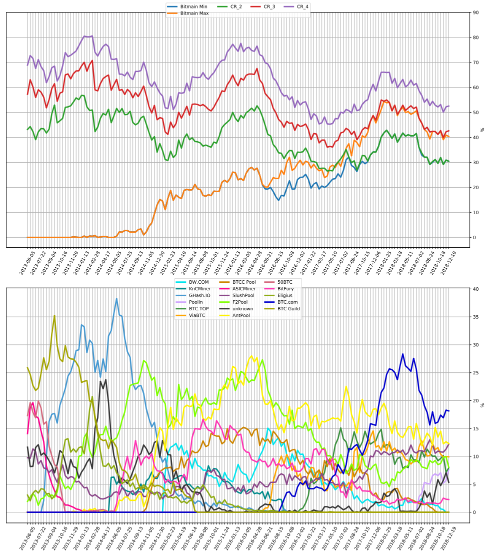


Figure 1: Concentration indeces and mining shares.

Pools Members — Cross-Pool Unknown Mining

Table 1: Cross-pool mining of the ten largest unknown mining clusters sorted by total amount of BTC received by the three pools in the time period between block 510,000 and 514,032 ($\sim$ 4 weeks).

	BTC.com		AntPool		ViaBTC			
Cluster ID	BTC	%BTC	BTC	%BTC	BTC	%BTC	Mined BTC	Total BTC Received
327539880	409.34	3.40	122.10	5.23	258.55	6.04	789.99	521,939
324067473	295.02	2.45	90.44	3.88	189.15	4.42	574.61	3,756,583
350822682	244.77	2.03	9.29	0.40	182.92	4.27	436.98	110,566
350824718	244.67	2.03	65.65	2.81	46.20	1.08	356.52	112,680
333653856	153.02	1.27	54.02	2.31	83.60	1.95	290.63	130,680
372448840	181.10	1.50	33.64	1.44	55.73	1.30	270.48	882,713
234254928	93.31	0.77	27.18	1.16	58.68	1.37	179.17	905,101
249123673	15.63	0.13	0.40	0.02	107.23	2.50	123.26	6,812,938
349962609	8.67	0.07	39.01	1.67	19.74	0.46	67.41	1,173,892
311503667	38.94	0.32	7.47	0.32	7.77	0.18	54.18	486,338

Payout Patterns — Methodology

Algorithm 1 Find payout patterns in BTC.com, AntPool and ViaBTC.

```
for each pool do
    for each mined block do
        get coinbase flow of block
        compute number of addresses at each step of the coinbase flow
        save results
    plot data and look for common patterns among flows
```

Payout Patterns — Methodology

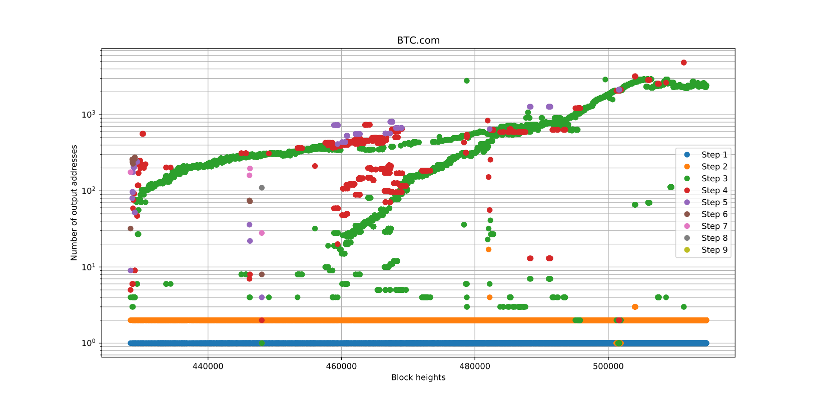


Figure 2: Payout trend for BTC.com

Pools Members — Cross-Pool Mining

Cross-pool mining between block 510,000 and 514,032

Pool 1	Pool 2	Addresses in common	Clusters in common	BTC from Pool 1	BTC from Pool 2
BTC.com	AntPool	537 (1.58%)	434 (3.2%)	664.3 (5.5%)	176.8 (7.6%)
AntPool	ViaBTC	115 (0.54%)	196 (2.4%)	11.1 (0.47%)	102.6 (2.4%)
ViaBTC	BTC.com	250 (0.91%)	267 (2.3%)	175.4 (4.1%)	174.1 (1.4%)