Bitcoin visualization project

Jean-Daniel Fekete

Petra Isenberg

Christoph Kinkeldey

www.aviz.fr

Goal: Understanding Bitcoin Activity

- Bitcoin is a fashionable topic
- But nobody really knows what is going on
  - Money laundering?
  - Illegal transactions?
  - Normal transactions?
  - Saving/investment?
- We want to provide exploration and visualization tools to make sense of Bitcoin

Focus on Simple Transactions

Normally, transactions are:

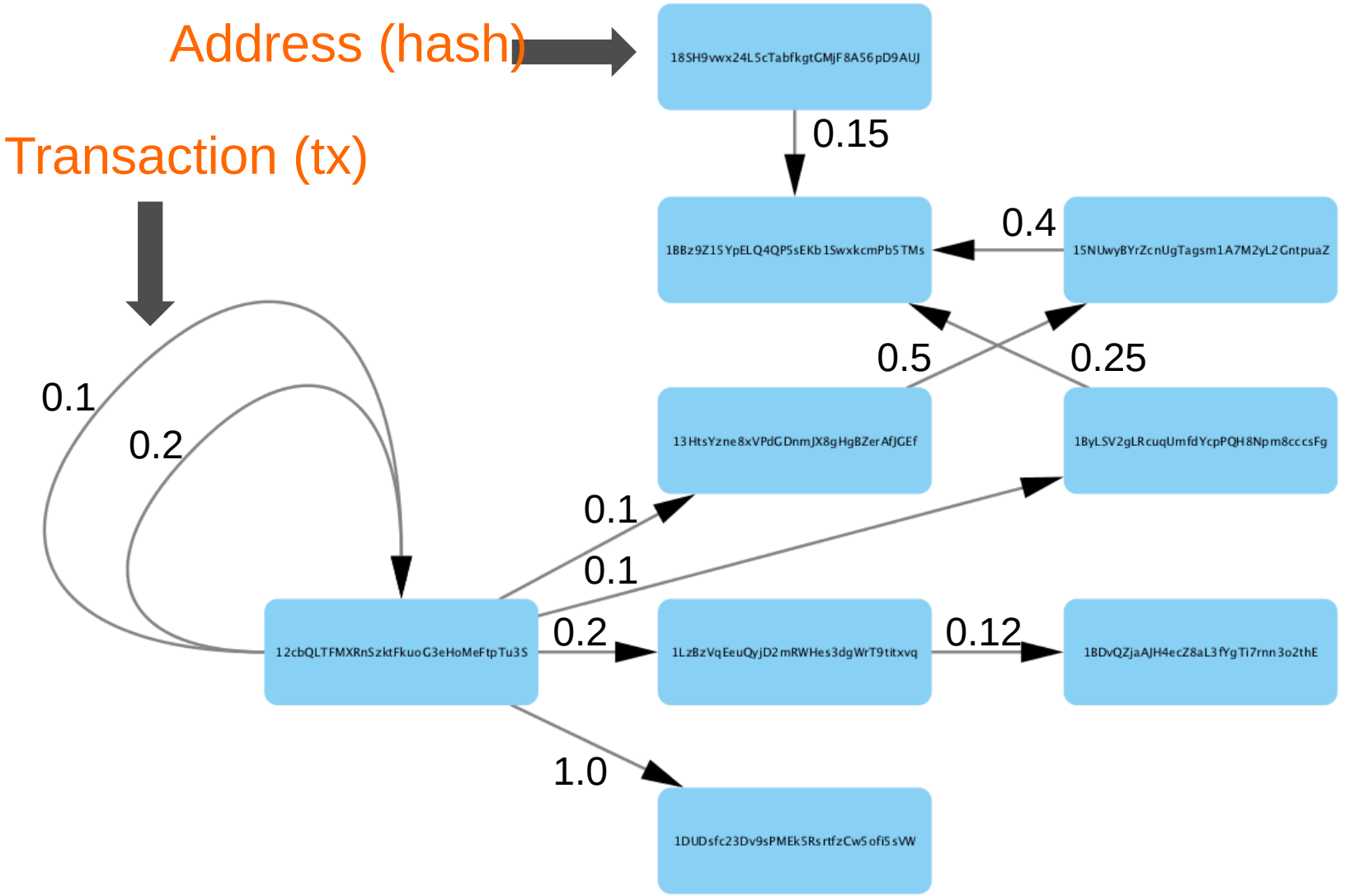
- Multiple inputs (addresses), amount, multiple outputs, time

But really, what we want:

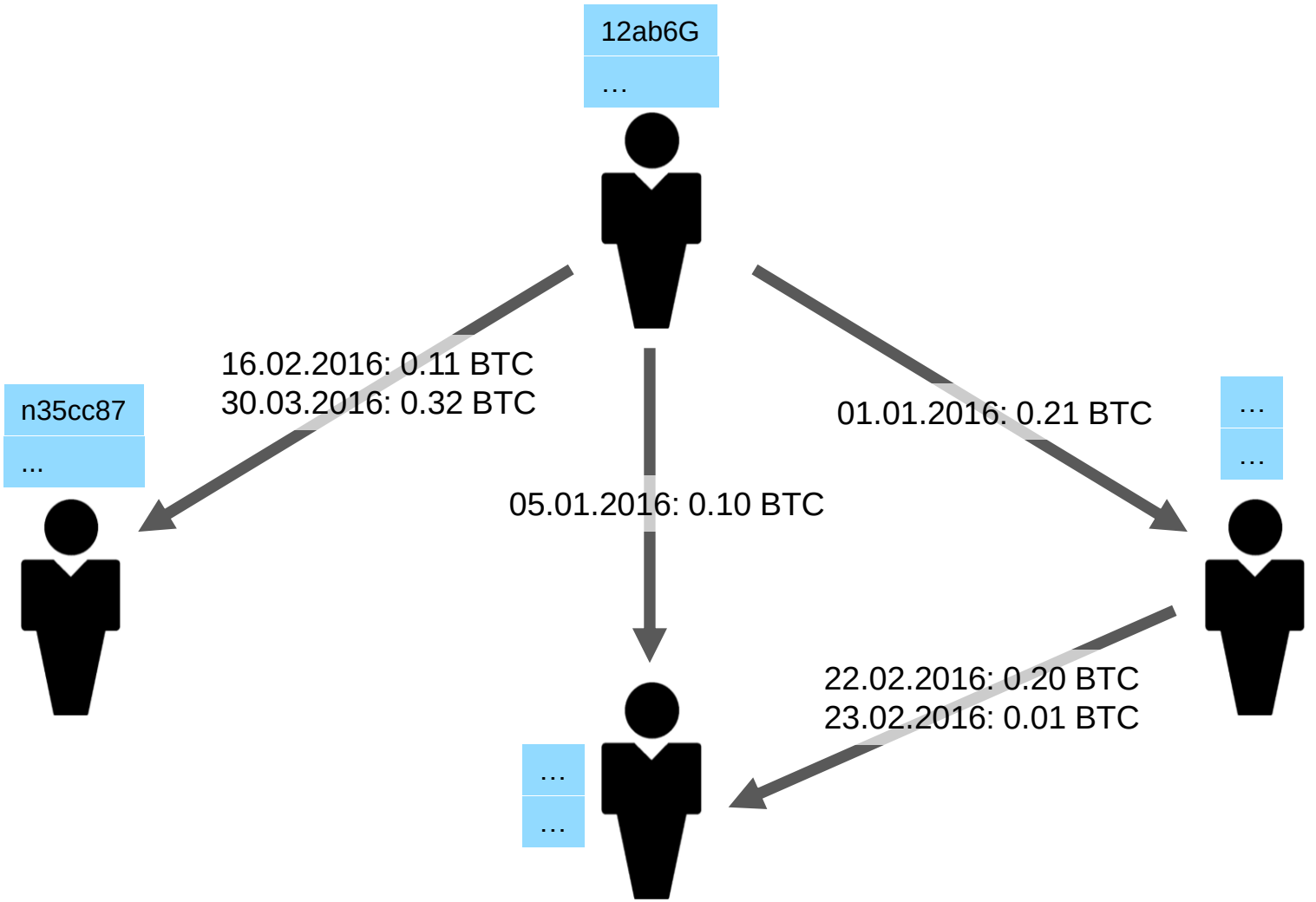
- One input entity, amount, one output entity, time

- Initial **clustering** of addresses into entities

What we have...


Address (hash)
Transaction (tx)
18SH9vwx24L5cTabfkgtGMjF8A56pD9AUJ
0.15
1BBz9Z15YpELQ4QP5sEKb1SwxkcmPb5TMs
0.4
15NUwyBYrZcnUgTagsm1A7M2yL2GntpuaZ
0.5
0.25
13HtsYzne8xVPdGDnmJX8gHgBZerAfJGEf
1ByLSV2gLRcuqUmfdYcpPQH8Npm8cccsFg
0.1
0.2
0.1
0.1
12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S
0.2
1LzBzVqEeuQyjD2mRWHes3dgWrT9titxvq
0.12
1BDvQZjaAJH4ecZ8aL3fYgTi7rnn3o2thE
1.0
1DUDsfc23Dv9sPMEk5RsrtfzCw5ofi5sVW

What we want


12ab6G
…
16.02.2016: 0.11 BTC
30.03.2016: 0.32 BTC
n35cc87
...
05.01.2016: 0.10 BTC
01.01.2016: 0.21 BTC
…
…
22.02.2016: 0.20 BTC
23.02.2016: 0.01 BTC
…
…

What is an entity?

n35cc87

12ab6G

Z2axO0

addresses

?

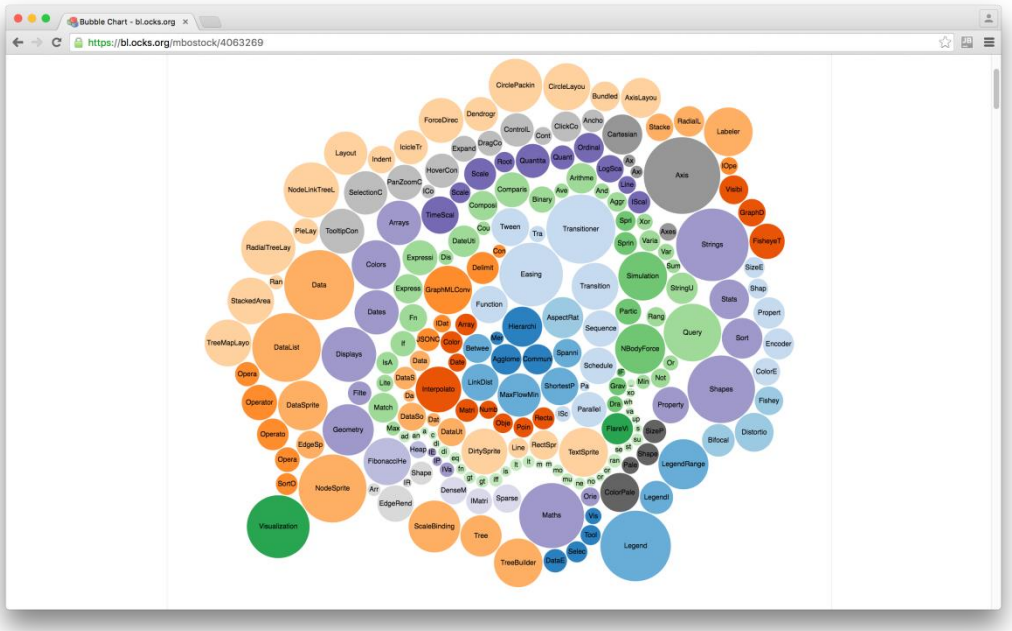
?

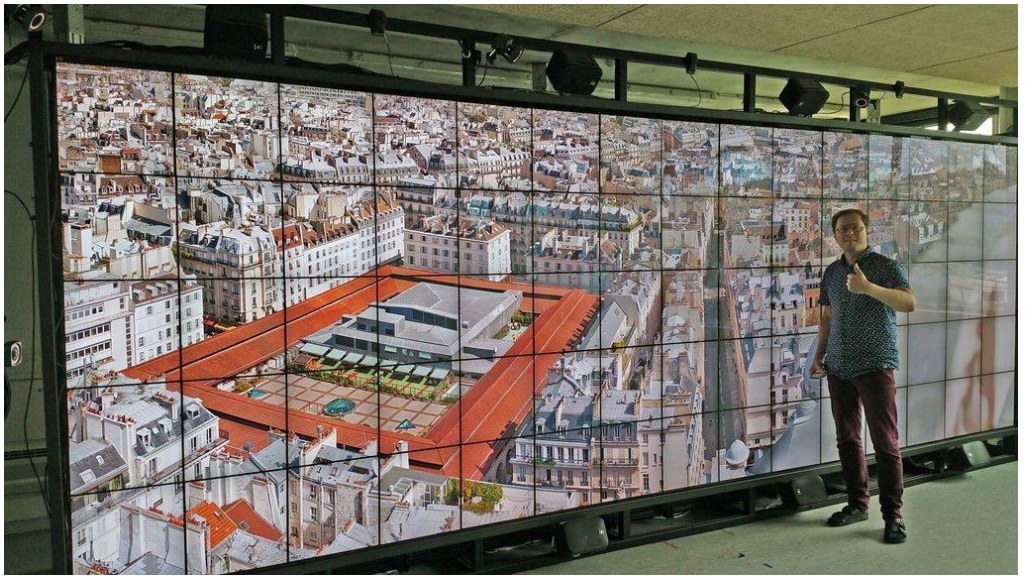
“entity”

Back to Ledger (anonymous?)

https://en.wikipedia.org/wiki/Ledger#/media/File:Hauptbuch_Hochstetter_vor_1828.jpg

Visualization of Transactions





Web-based

Wall display

What is visualization?

- Not (only) pretty images
- Not (only) a method for communication
- A method for **data exploration**
- Good visualizations use essential properties of our perception system
  - To read data quickly, effortlessly, and without error

Visualization for Who?

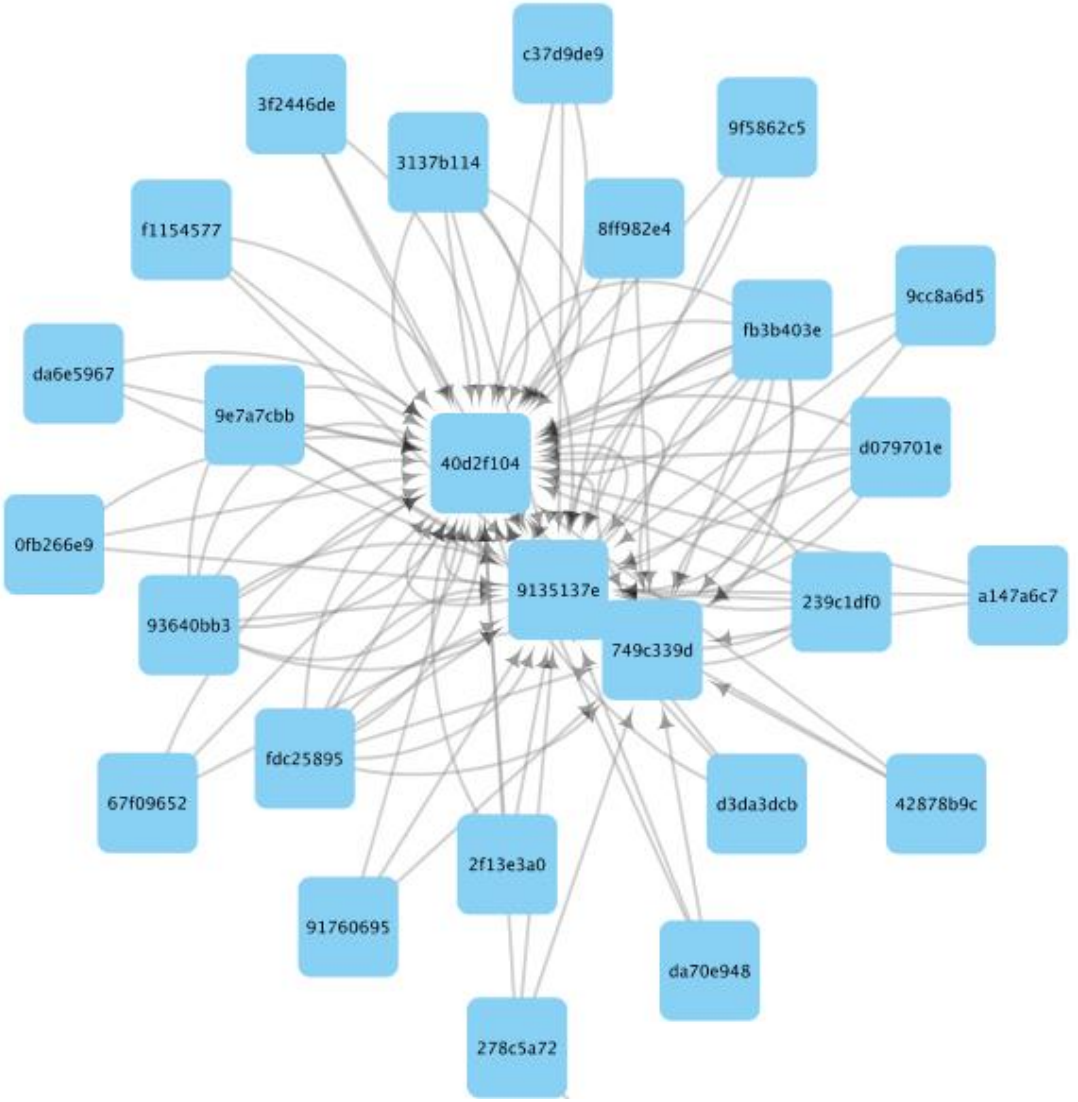
- Blockchain infrastructure
  - Blockchain debugging
  - Miners
- Regulators
  - Policy makers
  - Intelligence/hackers
- Humanities
  - **Economists**
  - Sociologists
  - Historians

Structure of Transactions

	txid	time	cluster_from	cluster_to	amount
2	4676433ef4f496c09943cf71d3d6f764513a2fadebf3764e87eca835cc	1281663660	46302	46355	0.5
3	4676433ef4f496c09943cf71d3d6f764513a2fadebf3764e87eca835cc	1281663660	46302	46301	47.6
4	ff5d515b813a14407fdcb4a0ea37d67ff567a62ab65d2f4494f4ac47ae	1280058451	38420	35149	0.02
5	ff5d515b813a14407fdcb4a0ea37d67ff567a62ab65d2f4494f4ac47ae	1280058451	38420	38418	14.3
6	9a4c518d51abaf61fc0fb497d129cce0157aa808433b06bd3421a933	1285545525	61113	61112	0.05
7	9a4c518d51abaf61fc0fb497d129cce0157aa808433b06bd3421a933	1285545525	61113	60925	0.01
8	86aaef7c081ab3ebe5890acecbce4d4a8fc1e79f67106c8bb7db8c592	1290815935	94147	93360	100
9	8564106cedfcaceafeca65303b22ed4401bb757dfab2853cb88701f57	1290259094	91025	91025	0.01
10	5a0a274b52c6174758b5e4e8927ee1eaf9aa64ebe04aa1d23e341be	1290334796	91426	91426	0.01
11	dce8c13fc1aaf3ab09f316bbace88440844114a7ac599276b53291e3	1290230901	91025	91025	0.01
12	c44f8f75cc8bc4d56a331f80ce538f2df99f58f90a8cca7bb5fa7002dcf4	1280522594	41827	1MW7GCMjNVuNK1LGhJce9trzm2X8kqsa6	0.05
13	c44f8f75cc8bc4d56a331f80ce538f2df99f58f90a8cca7bb5fa7002dcf4	1280522594	41827	41826	11.66
14	7a1d1a4e75879ba3dc49a171f38b093f201a2e08a90ca4f1a3a3ae78	1290639276	89981	92684	0.01
15	b907f296b204bd57a85fb5d0ad33cfcc9ffad4620c2993932e26e4cbe	1290119158	90683	90683	0.06
16	f396a0c85b37d286b1091de046cbcfe71ef4a6138767d40ce4b66553	1292902664	105759	106248	0.14
17	bb9095c1c9380003c9255548cad3ff095020e9479950e6770726be50	1290230901	91025	91025	0.01
18	7054e6c4050c6bca89493e57ce8022b6a5ee3993f046680c2942246	1279123980	29039	29038	47.47
19	7054e6c4050c6bca89493e57ce8022b6a5ee3993f046680c2942246	1279123980	29039	14932	0.01
20	f35873f2e08ac4cc5772e8fc65c3d5cf21dcca178fcf0fdb4ccb3894dac6	1289918731	89796	89796	50
21	be1318e17c29d350c358f229ee12b7bac171df3978449dd53dc24804	1290663587	92684	89981	0.01
22	3db95621435157804f2acc6ed7cd87b51c7a3c7bb5010351b3613b7	1290197259	90872	90872	0.01
23	54dbdc7de3fe2120b213fc23db8504a6c0acd09a57cca258f8fcac987	1290686120	92977	92943	0.3
24	592f89e5f9e4b1c3484d4a0b61851fa32539b25109fdd8854a8681d2	1285197478	59211	59216	0.01
25	592f89e5f9e4b1c3484d4a0b61851fa32539b25109fdd8854a8681d2	1285197478	59211	59241	0.07
26	d262482a313a7b861f6ba0c8c9a415ead8f63b1928dd94c5c02f0f7b2	1292196361	100891	1AZSQqSTSwSogJspcgjvzsrCvKmAsf42rT	40
27	d262482a313a7b861f6ba0c8c9a415ead8f63b1928dd94c5c02f0f7b2	1292196361	100891	105619	157.05
28	a51d714185330094cdee94eb222e77f3d745b643b58ed9c2948c3c5	1292617513	103766	17JqxTkVA1nadbMmjahAwSVBfdsqbTnC6q	0.05
29	a51d714185330094cdee94eb222e77f3d745b643b58ed9c2948c3c5	1292617513	103766	103778	380.06
30	68c980bce88f76281cde7962be5f674b5d3c09e12fb026ac97a187c25	1290332745	91424	91424	0.01
31	16714a4d0cfea9de8e330a1c17aa854be4eefff2ec78169c09d069586	1285749818	63857	63856	103.78
32	16714a4d0cfea9de8e330a1c17aa854be4eefff2ec78169c09d069586	1285749818	63857	20161	0.05
33	08b4fcf2ea7caaac26198cc15102928bdba6a5b6c88491cd516ad9d7	1290307628	91426	91426	0.01
34	b2c26c96528e1fdd00f912989cf7210943ce1924229af830b380cd69c	1290627826	89981	92684	0.01
35	82f21dd60849babcfacde494f539ff8817bdc9c45acf4bcad3c8422925	1290231279	91024	91024	0.01
36	a884b115fb474f85fc85dd1b8d92c5781de1addc60afe2808161f3765	1285898018	64660	64659	0.745

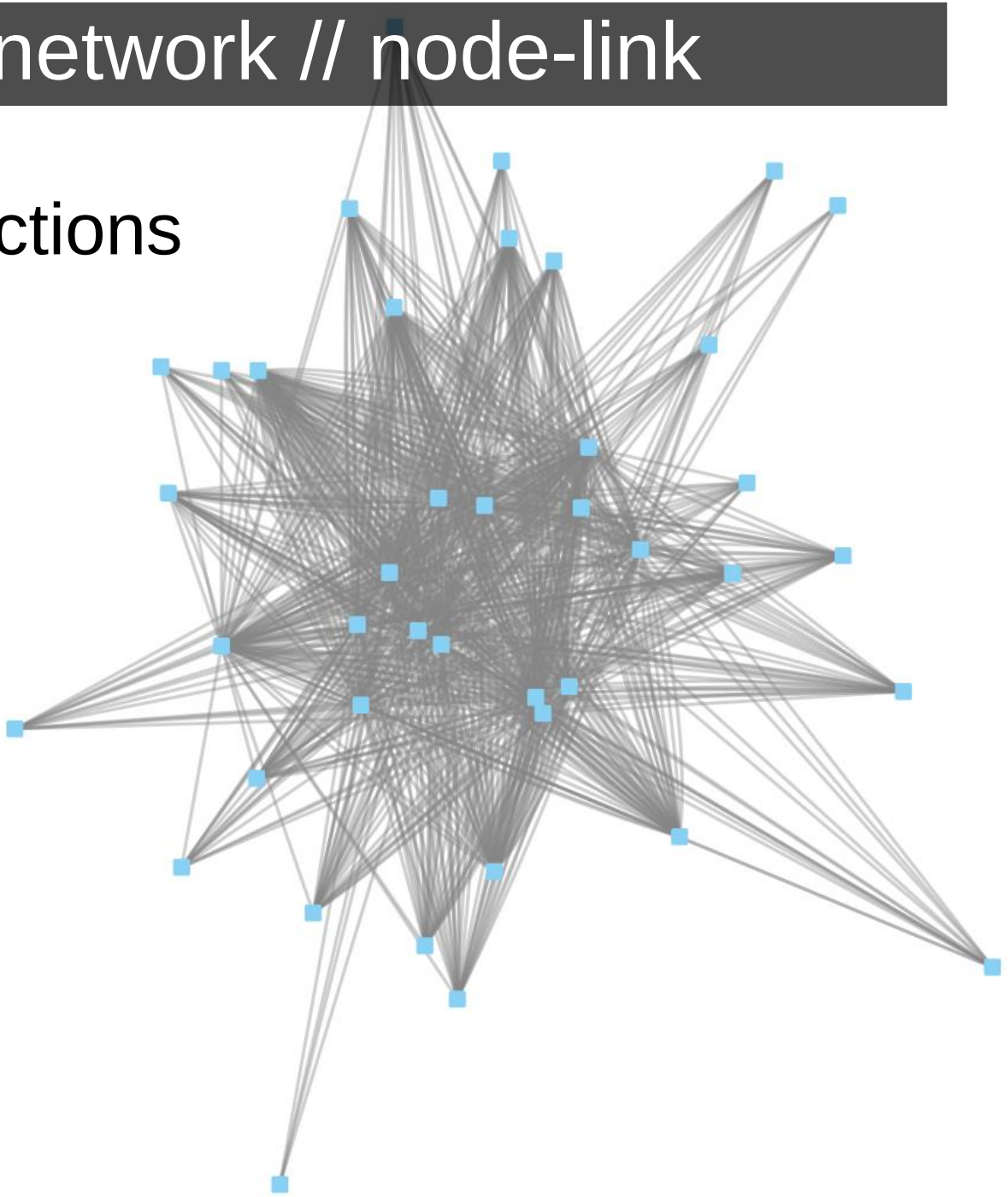
Transaction network // node-link

Nodes: transactions
Edges: flows



Transaction network // node-link

Nodes: transactions
Edges: flows

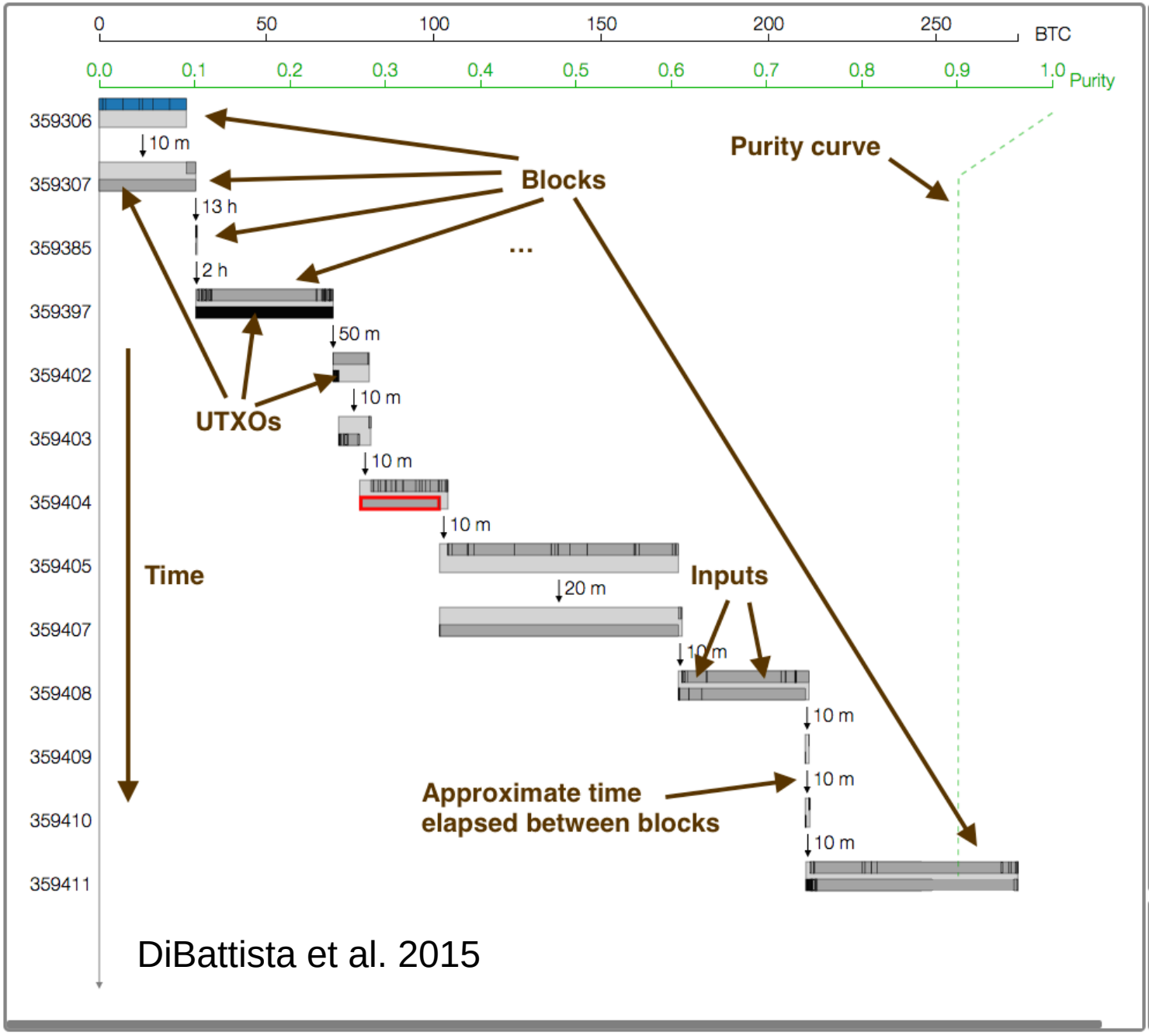


Sources:

- 4ff027f936f4b2741230507ea51b756a518df1fe057e4049fbd6122feb692069 (26.01049401 BTC)

Info:

- Starting Date: Thu, 04 Jun 2015 00:33:21 GMT
- Ending Date: Thu, 04 Jun 2015 18:20:00 GMT



DiBattista et al. 2015

Money in circulation:

UTXOs (BTC) and their Purity	Inputs (BTC)
71.17232234 P: 0.000	37.00000000
58.91451609 P: 0.000	31.27317994
41.00000000 P: 0.000	22.09255839
30.79549192 P: 0.000	14.10000000
28.84515384 P: 0.901	14.00000000
23.37623762 P: 0.000	12.00000000
3.85505000 P: 0.000	11.00000000
2.88506066 P: 0.000	10.30000000
2.75500000 P: 0.000	9.91001165
1.33600000 P: 0.000	5.40440000
1.01120573 P: 0.000	5.16000000
0.81630000 P: 0.000	5.00000000
0.63725059 P: 0.000	5.00000000
0.57966819 P: 0.000	5.00000000
0.54668000 P: 0.000	5.00000000
0.50283462 P: 0.000	4.55161305
0.49439113 P: 0.000	3.85505000
0.47601571 P: 0.000	3.62633663
0.29532432 P: 0.000	3.40737406
0.29004218 P: 0.000	3.00000000
0.27849860 P: 0.000	2.84615384
0.27395985 P: 0.000	2.75500000
0.25526793 P: 0.000	2.36309640
0.25132335 P: 0.000	2.00892683
0.21100000 P: 0.000	1.86200000
0.19468242 P: 0.000	1.80000000
0.18953738 P: 0.000	1.77422932
0.18900000 P: 0.000	1.71742612
0.17582502 P: 0.000	1.61287129
0.17262652 P: 0.000	1.43605911
0.16440186 P: 0.000	1.42170000
0.16218916 P: 0.000	1.37678049
0.16135205 P: 0.000	1.33600000
0.16074681 P: 0.000	1.33511100
0.16046419 P: 0.000	1.30948156

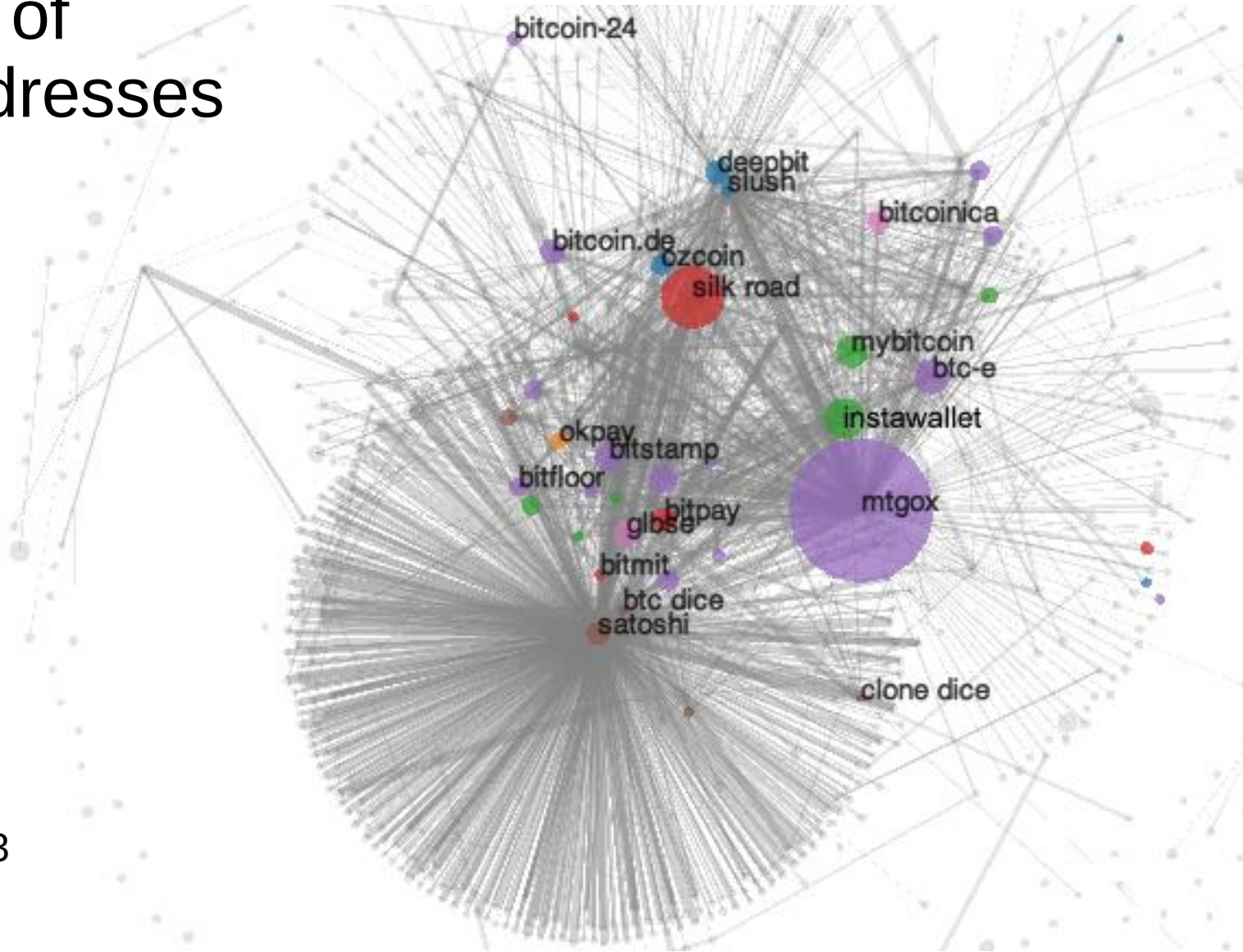
Transfer Analysis:

M.T.M. to selected UTXO: 0.01001535 BTC
Percentage w.r.t the selected UTXO: 0.04 %
Percentage w.r.t. sources inputs: 0.04 %

M.T.M: Maximum transferable money from the sources

Heuristics

Visualization of clustered addresses



Meiklejohn et al. 2013

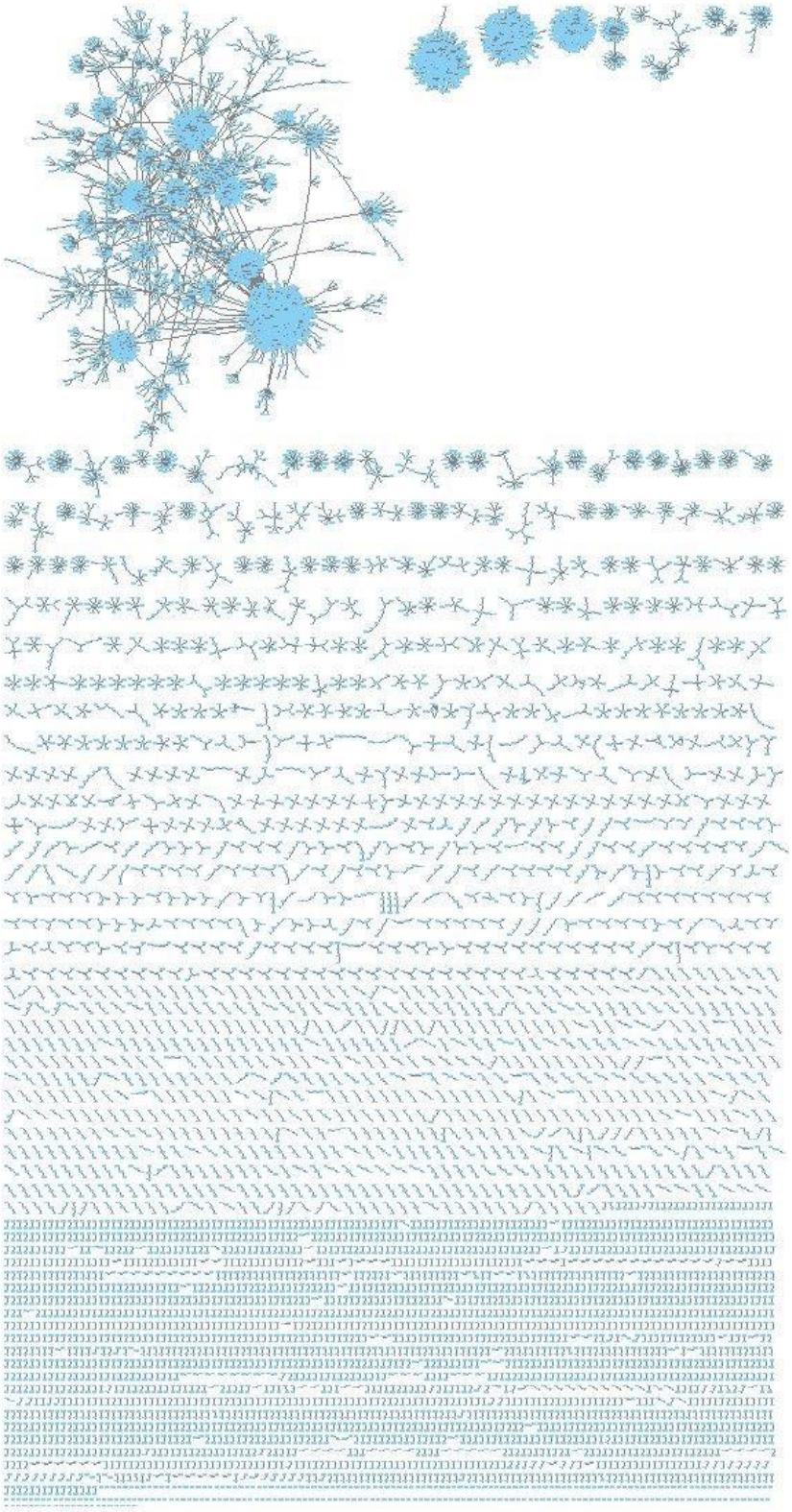
Nodes: addresses
Edges: flows

McGinn Dan, Birch David, Akroyd David, Molina-Solana Miguel, Guo Yike, and Knottenbelt William J. **Visualizing Dynamic Bitcoin Transaction Patterns** Big Data. June 2016, 4(2): 109-119. doi:10.1089/big.2015.0056.

FIG. 4. **(A)** High-resolution (8k) visualization of a standard block; **(B)** detail of both a low (small node) and a high (large node) value transaction, **(C)** known and linked Bitcoin addresses, **(D)** a payout system, and **(E)** a highly associated disconnected component believed to be a coin-tumbling service to move amounts rapidly between addresses, obfuscating the source and destination of funds.

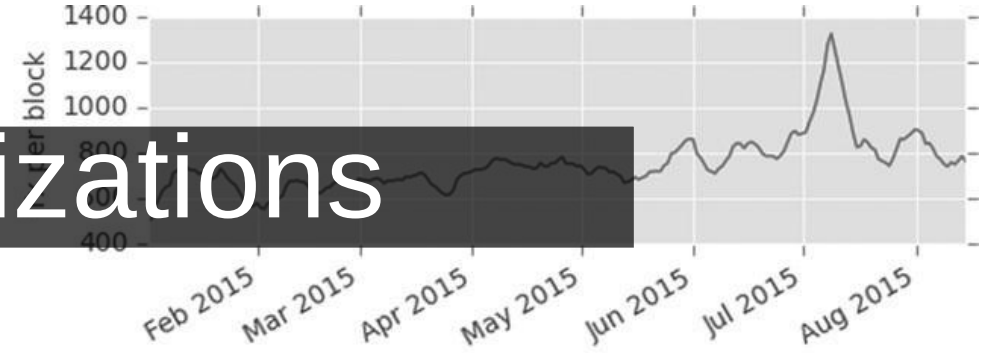
Transaction network

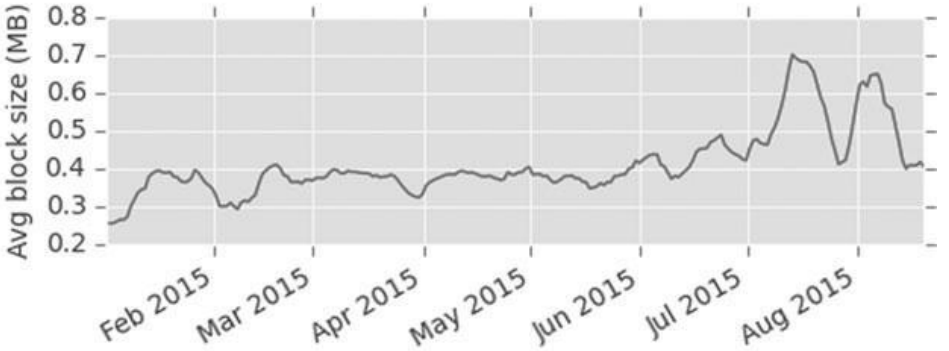
Nodes: **addresses**
Edges: transactions

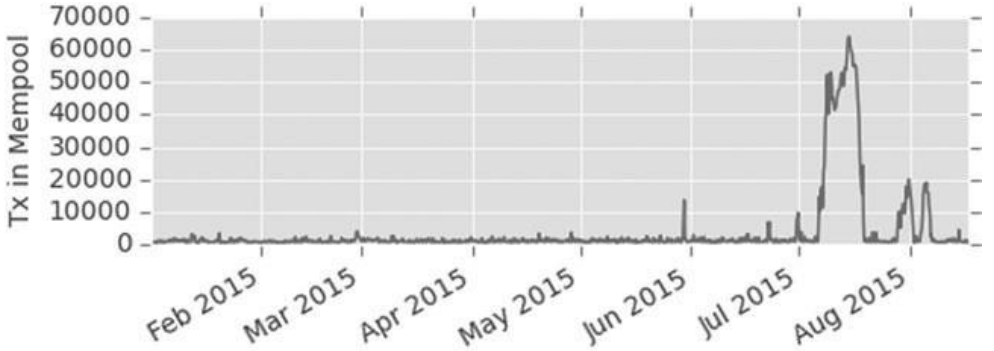


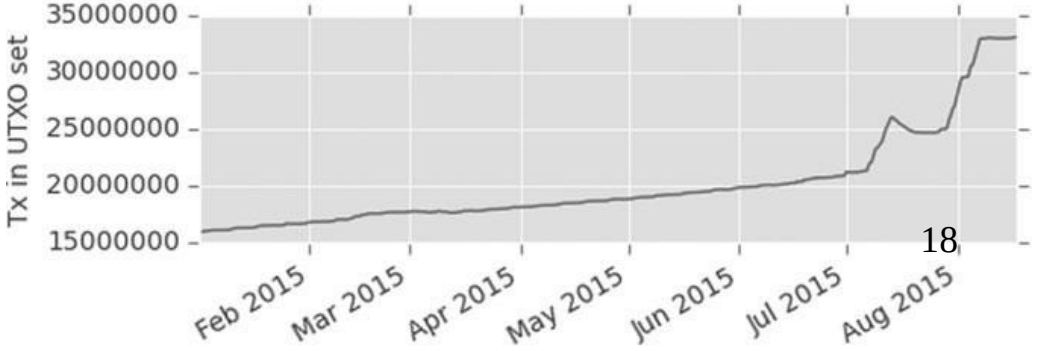
Summary of Visualizations

- Not understandable
- Not scalable
- So people use aggregated statistics





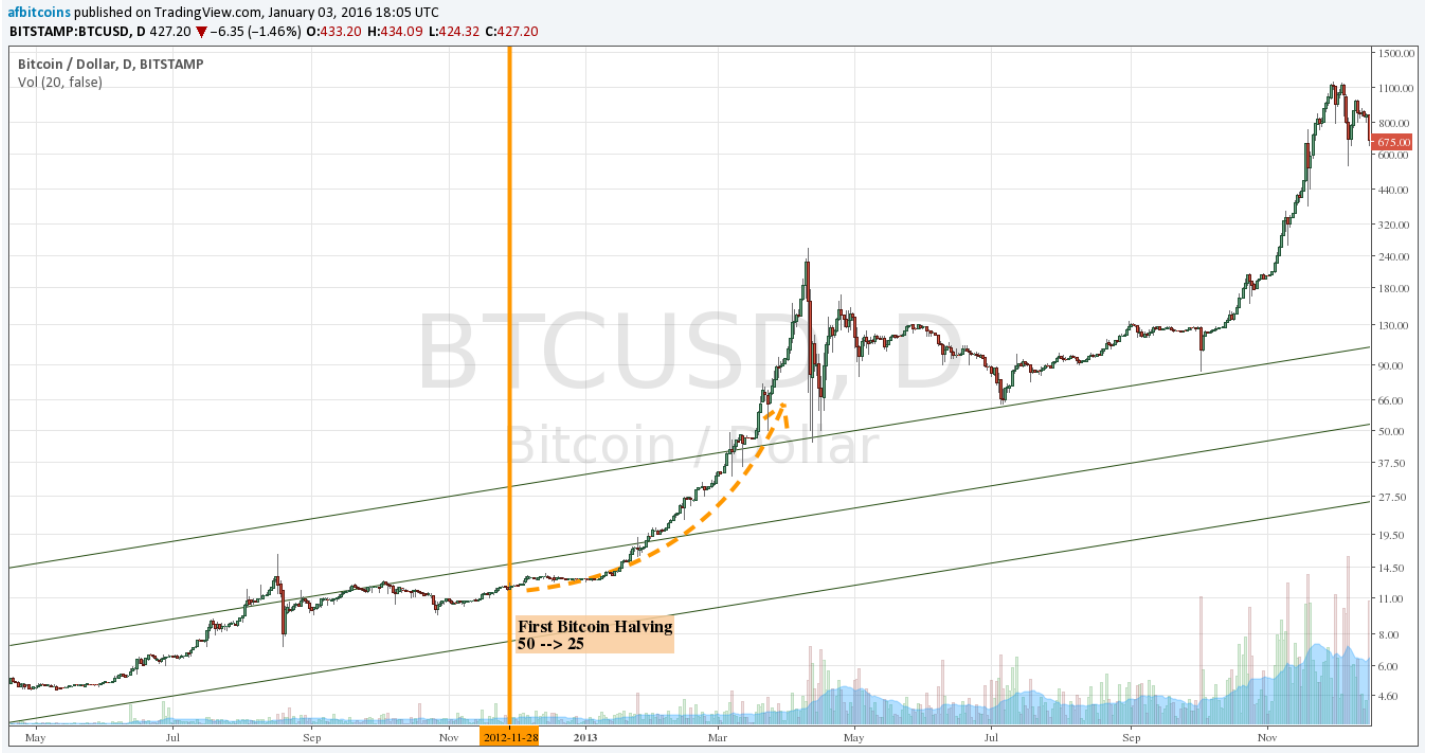




Analysis of Bitcoin Events

Some high-level analyses can still be done

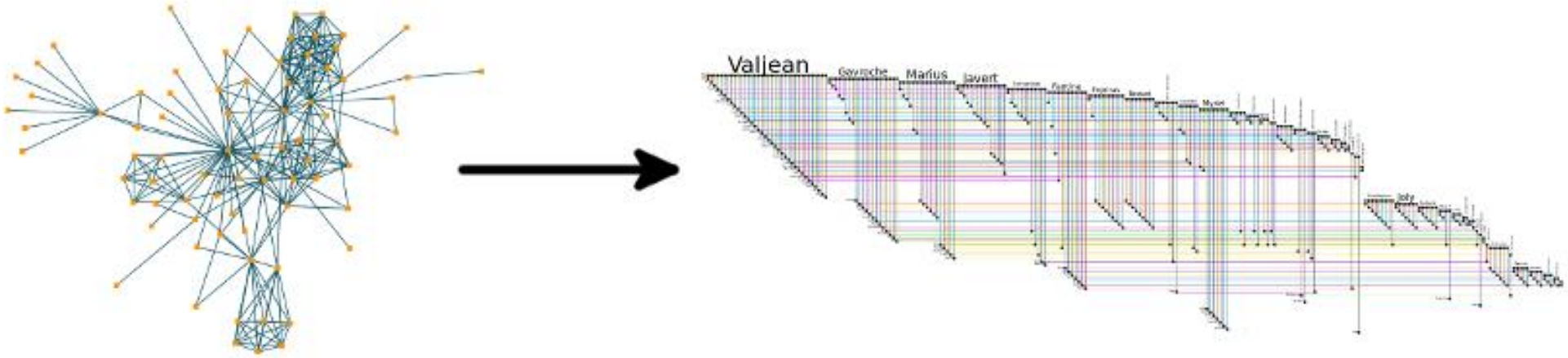
- Internal, e.g., halving day
- External, e.g., stock market crash



https://www.deepdotweb.com/2016/01/06/bitcoin-price-analysis-6-january-2016/

Scalable Visualization

- Change visualization technique
  - Biofabric http://www.biofabric.org/
- Categorize transactions
- Manage multiple scales



http://www.biofabric.org/gallery/pages/SuperQuickBioFabric.html

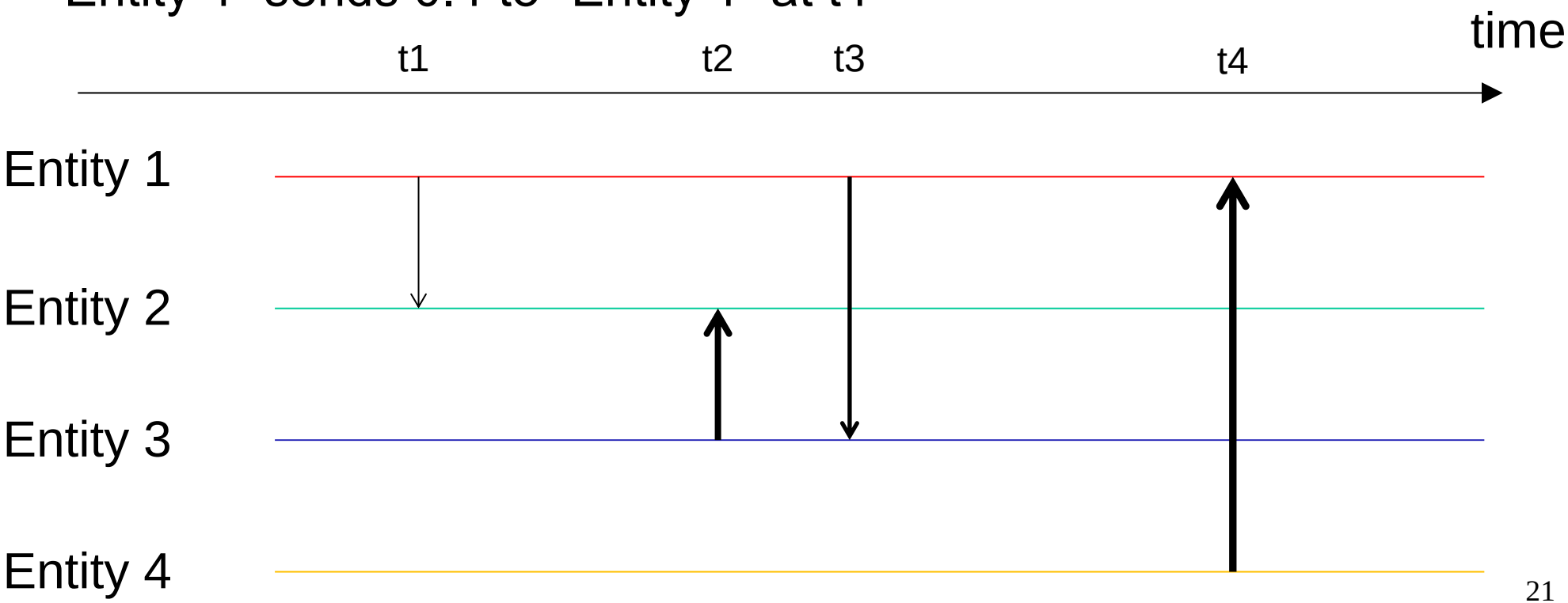
Visualization of Transactions

"Entity 1" sends 0.1 to "Entity 2" at t1

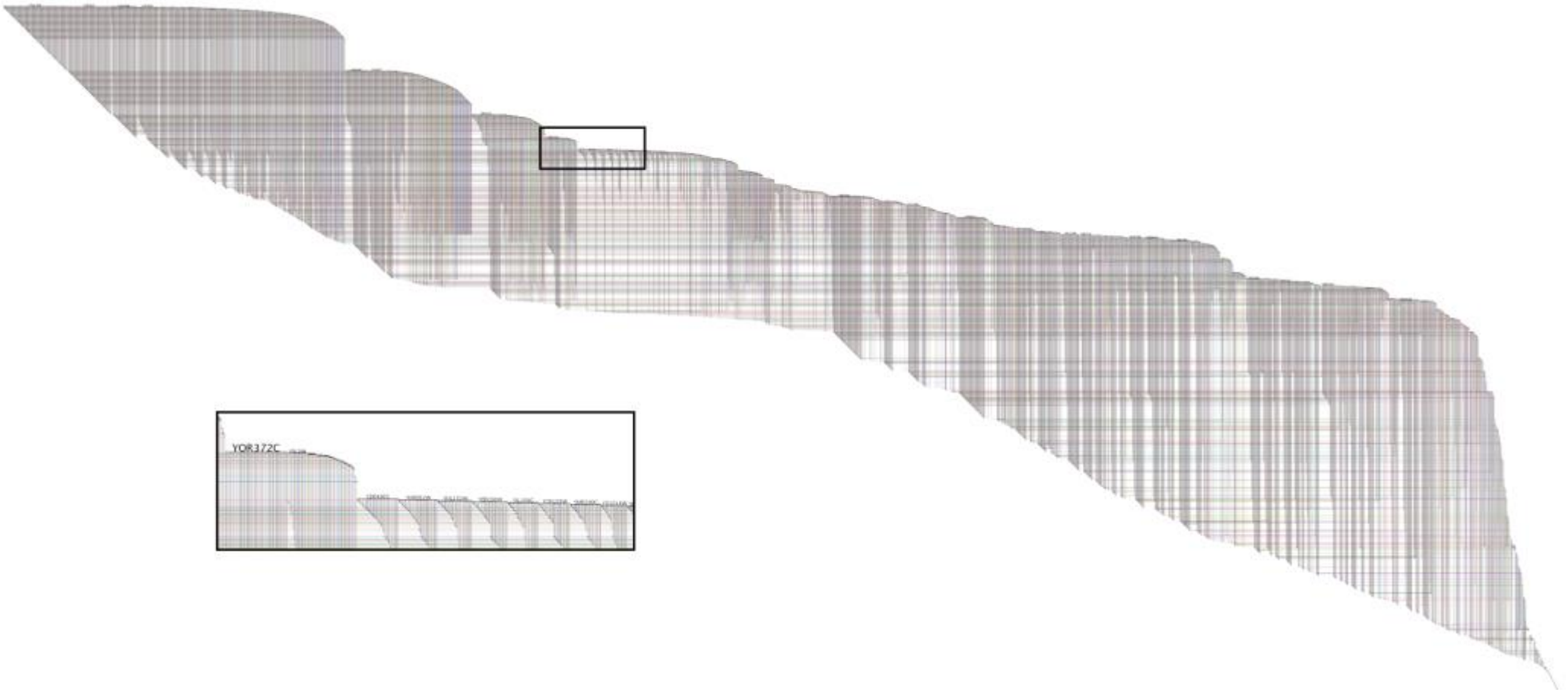
"Entity 3" sends 0.5 to "Entity 2" at t2

"Entity 1" sends 0.3 to "Entity 3" at t3

"Entity 4" sends 0.4 to "Entity 1" at t4

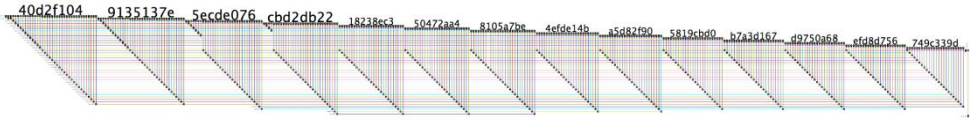


BioFabric Scales to 10^5



Ordering, Filtering and Aggregating

- Reordering transactions
- Reordering entities by
  - Time
  - Category of entity
- Filtering
  - Time
  - Category
- Aggregating
  - Transactions by time inter.
  - Amounts by category



Current work

- Clustering ➔ entities
  - heuritistic: “input addresses of a transaction belong to same entity”
- Categorize entities by activity
  - dead/tester, investor, merchant, miner, …

  ➔Visualize categories over time

- If you can help, we would be thrilled!