PROJECT PRESENTATION

PROJECT OBJECTIVE

- We have in a database all transactions between addresses and all transactions between actors from the beginning of bitcoin to the end of 2017 (and the rest is computing)
- Choose and obtain a small subset of this network that you consider interesting
 - Around a particular transaction (illegal activity ...)
 - About some actors
 - About a period
 -

PROJECT OBJECTIVE

- Apply tools your learned about during the class to better understand this network
- Write a report about what you learnt, and what you could learn with more time/data
 - If possible, a single Jupyter notebook with code and text
 - A separate report in PDF is also possible if relevant

PROJECT OBJECTIVE

- Recommendations:
- I recommend to limit yourself to a few thousand nodes, and less than 10.000 edges (filtering). Comparing a few graphs of this size can be relevant.
- The goal of the project is to interact!
 - Ask me if something is possible, how to do it... we are doing the project together.

DATA DESCRIPTION

SUMMARY OFTHE PROCESS

- I. Run a Bitcoin Node to download the full Blockchain
 - =>January 2021: **366 Go**
- 2. Use a tool (bitcoin-etl) to extract transactions as .json files
 - =>Until January 2018: **862G**
 - =>Total: **1.5 To**
- 3. Use co-spending heuristic to identify clusters
- 4. Use <u>walletexplorer.com</u> data to identify clusters of large actors
- 5. Create an Actor to Actor transaction records

ACTOR TO ACTOR TRANSACTION RECORDS

- Each transaction has a single actor in input
- It can have one or several actors in output.
 - Actors are identified by their names
 - Clusters are identified by a positive integer
 - Singleton addresses are identified by a negative integer
 - In the main file, we keep self-transactions, they can be removed
- Size:
 - December 2017: 768 Million transactions, 28 G
 - January 2021:TODO

SOME IDEAS

BITCOIN BLOCKCHAIN ACTIVITY TRACKING EXAMPLE

Transfer (€)

Traditional Bank

3



deposited	processed 2/10/2017		
Operations			
Account	Name	Amount	Date
available	operation	+75.00 €	2/10/2017 - 3:28 PM

2) Initial Bitcoin purchase (trading)

💿 bought	0.05423052 btc for	921.99€	average	filled	2/10/2017

"	"]	Frad	ing'	,	
---	----	------	------	---	--

🔮 sold	0.07130000 btc	for	1,059.00€	average	filled	2/22/2017
📀 bought	0.07136414 btc	for	1,008.91€	average	filled	2/18/2017
🔮 sold	0.07400000 btc	for	980.17 €	average	filled	2/18/2017
📀 bought	0.05076142 btc	for	985.00€	average	filled	2/17/2017
🔮 sold	0.02600000 btc	for	975.01€	average	filled	2/16/2017

Offchain

• How it works (probably)

3

- The exchange company owns a stock of Bitcoin
- It maintains a list of customer accounts, and how much each customer owns at time t
- When customer c1 buys btc to a customer c2, change in the internal database of the company (scripture)
 - Goal: no transaction fees, easier to manage
- The company itself certainly buy and sell on the market to ensure liquidity
 - Success=more customers who want to buy=>need to provide fresh coins
 - Need of buying/selling on the blockchain
- The company need enough reserve since customers can order bitcoin transactions from their (*virtual*) account to a *real bitcoin wallet*

1,974.99 € average

						\cap
	timestamp	sender	receiver	value	date	value_btc
619503540	1495929670	-192947146	Paymium.com	4276511	2017-05-28 00:01:10	0.042765
619622208	1495940615	35172026	Paymium.com	21408870	2017-05-28 03:03:35	0.214089
619627952	1495940615	36676998	Paymium.com	1278580	2017-05-28 03:03:35	0.012786
619641058	1495941084	320110	Paymium.com	2889754	2017-05-28 03:11:2	0.028898
619678470	1495946218	234	Paymium.com	5000000	2017-05-28 04:36:58	0.500000
61972 <mark>0</mark> 731	1495953357	21	Paymium.com	50000000	2017-05-28 06:35:57	5.000000
619724954	1495954071	Poloniex.com	Paymium.com	90000000	2017-05-28 06:47:51	0.900000
6197; 4802	1495953492	15195288	Paymium.com	563100	2017-05-28 06:38 12	0.005631
619742071	1495956403	32328334	Paymium.com	30000000	2017-05-28 07:26 <mark>4</mark> 3	3.000000
6197 1 9598	1495956760	Bit tamp.net	Paymium.com	50000000	2017-05-28 07:32 40	5.000000
6197 <mark>7</mark> 3769	1495962103	Polcniex.com	Paymium.com	5990000	2017-05-28 09:01,43	0.059900
6198 <mark>2</mark> 3537	1495968880	Poloniex.com	Paymium.com	299990000	2017-05-28 10:54 40	2.999900
6198.4805	1495969178	-193097249	Paymium.com	5000000	2017-05-28 10:59 38	0.050000
6198 <mark>3</mark> 6324	1495969665	-193098289	Paymium.com	501097	2017-05-28 11:07.45	0.005011
619859643	1495972870	Eittrex.com	Paymium.com	99900000	2017-05-28 12:01:10	0.999000
61987 <mark>)</mark> 536	1495971407	- 93116479	Paymium.com	4113900	2017-05-28 11:36:47	0.041139
619874781	1495972455	5224442	Paymium.com	1373550	2017-05-28 11:54:15	0.013735
619877.24	1495973819	-193121122	Paymium.com	365283	2017-05-28 12:16:5	0.003653
619880471	1495972455	-193122823	Paymium.com	59539	2017-05-28 11:54:15	0.000595
619880482	1495972455	-193122827	Paymium.com	58606	2017-05-28 11:54:15	0.000586
619882043	1495973387	Paymium.com	16096	620000	2017-05-28 12:09:47	0.006200
619882044	495973357	Paymium.com	222	6800000	2017-05-28 12:09:47	0.068000
		(53 to	otal)		V

0.05417748 btc

Paymium on-chain activity on 2017-05-28

5/28/2017

filled

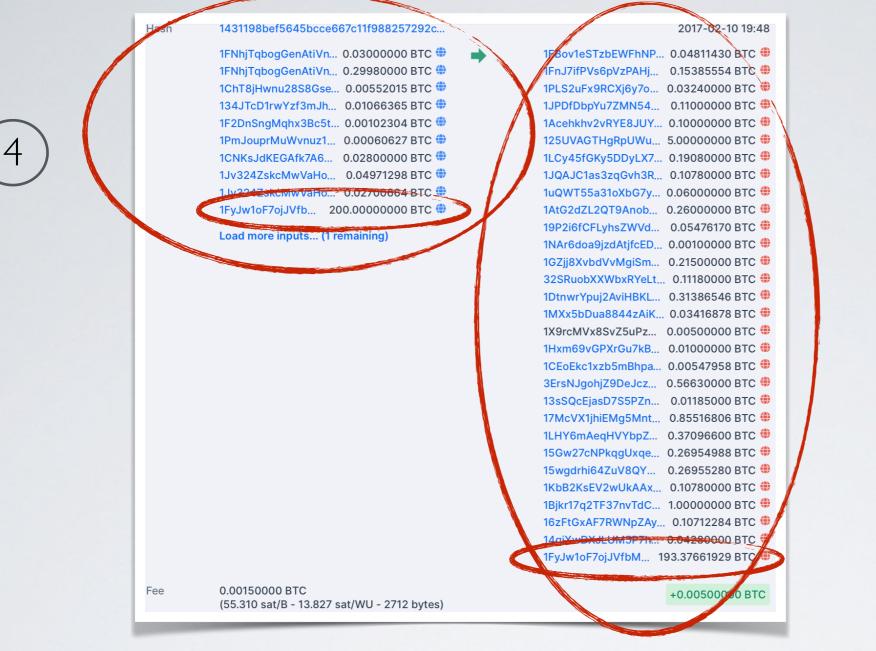
9:23GMT+1

Hard to say what it corresponds too... But my exact transaction is not there

Sending 0.005 btc from Paymium exchange to my personal wallet

4

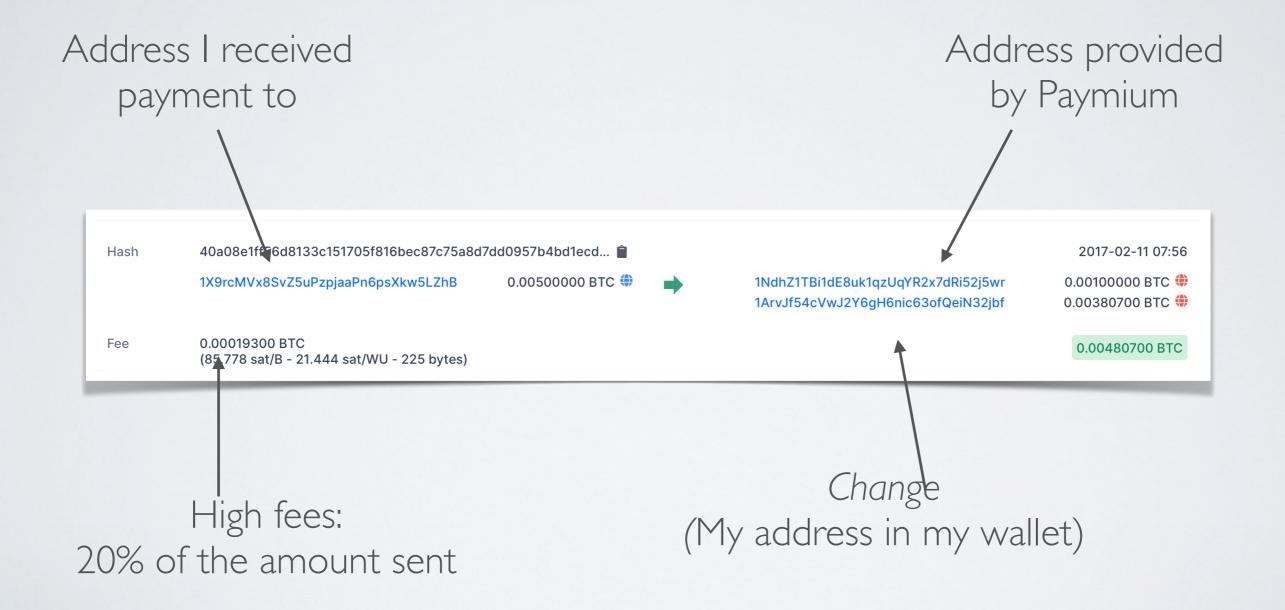
aymium	G transferred	0.00500000 btc	۲	processed	2/10/20
	Hash	1431198bef5645bcce667c11f988257292c	2017-02-10 19:48		
	Hash	1431198bef5645bcce667c11f988257292c 1FNhjTqbogGenAtiVn 0.29980000 BTC ⊕ 1FNhjTqbogGenAtiVn 0.29980000 BTC ⊕ 1GhT8jHwnu2858Gse 0.00552015 BTC ⊕ 134JTcD1rwYzf3mJh 0.01066365 BTC ⊕ 1F2DnSngMqhx3Bc5t 0.00102304 BTC ⊕ 1PmJouprMuWvnuz1 0.00060627 BTC ⊕ 1CNKsJdKEGAfk7A6 0.02800000 BTC ⊕ 1Jv324ZskcMwVaHo 0.04971298 BTC ⊕ 1Jv324ZskcMwVaHo 0.02700664 BTC ⊕ 1FyJw10F7ojJVfb 200.0000000 BTC ⊕ Load more inputs (1 remaining)	2017-02-10 19:48 1FBov1eSTzbEWFhNP 0.04811430 BTC 1FnJ7ifPVs6pVzPAHj 0.15385554 BTC 1PLS2uFx9RCXj6y7o 0.03240000 BTC 1JPDfDbpYu7ZMN54 0.11000000 BTC 1Acehkhv2vRYE8JUY 0.1000000 BTC 125UVAGTHgRpUWu 5.0000000 BTC 1LCy45fGKy5DDyLX7 0.19080000 BTC 1JQAJC1as3zqGvh3R 0.10780000 BTC 1MQWT55a310XbG7y 0.06000000 BTC 1MQVT55a310XbG7y 0.0500000 BTC 1MAr6doa9jzdAtjfcED 0.00100000 BTC 1GZjj8XvbdVvMgiSm 0.21500000 BTC 1GZj8XvbdVvMgiSm 0.21500000 BTC 1GZj8XvbdVvMgiSm 0.21500000 BTC 1DtnwrYpuj2AviHBKL 0.31386546 BTC 1X9rcMVx8SvZ5uPz 0.0050000 BTC 1X9rcMVx8SvZ5uPz 0.00547958 BTC 1X9rcMVx8SvZ5uPz 0.01185000 BTC 1X9rcMVx8SvZ5uPz 0.01185000 BTC 13sSQcEjasD7S5PZn 0.01185000 BTC 13sSQcEjasD7S5PZn 0.01185000 BTC 12srsNJgohjZ9DeJcz 0.37096600 BTC 12swgdrhi64ZuV8QY 0.26955280 BTC 15wgdrhi64ZuV8QY		
			16zFtGxAF7RWNpZAy 0.10712284 BTC 14qiXwDXJLUM5P7h 0.04280000 BTC 1FyJw1oF7ojJVfbM 193.37661929 BTC		
	Fee	0.00150000 BTC (55.310 sat/B - 13.827 sat/WU - 2712 bytes)	+0.00500000 BTC		



The exchange do not write on-chain transaction for each custom activity, but instead factorize them. It reduces individual transaction fees. Same for inputs. Note the <u>change address</u> with a large amount

Sending back **0.001** from Wallet to Paymium Exchange

5



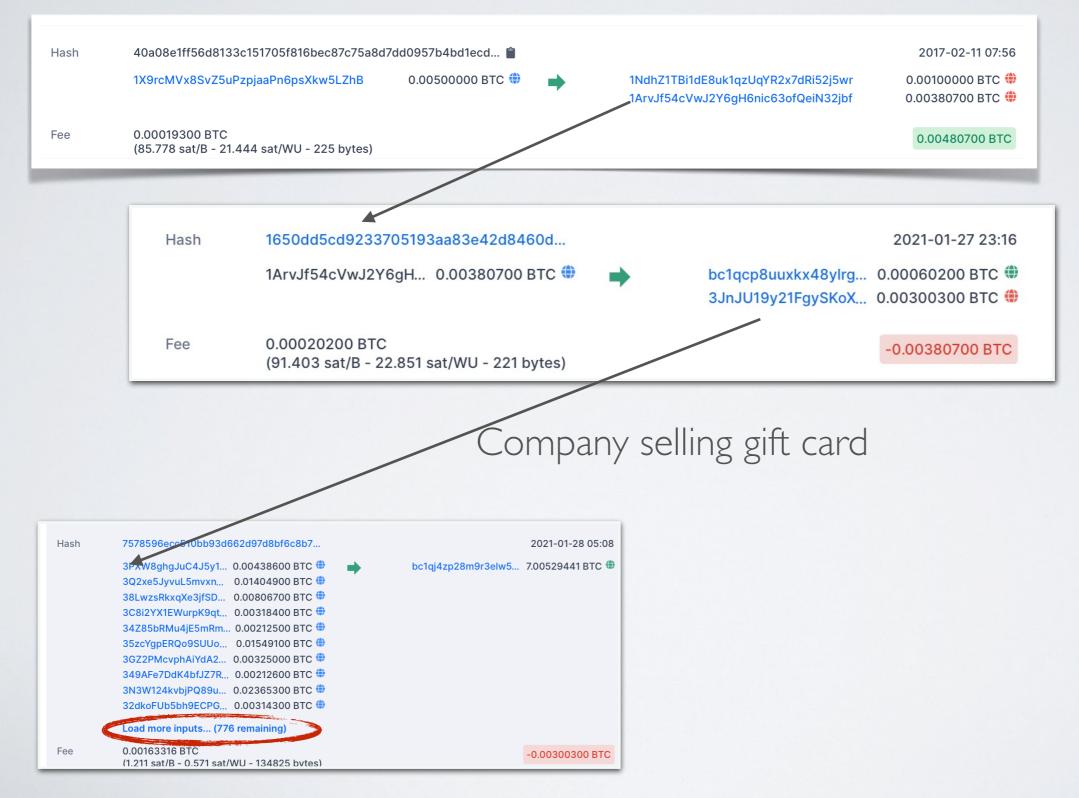
What happens with coins sent at this address?



"My" coins have been spent the same day, and not by me! =>INdh... Is not "my" address, it's paymium's address. It's just that when coins are sent to this address, Paymium *credit* my customer account of the same amount.

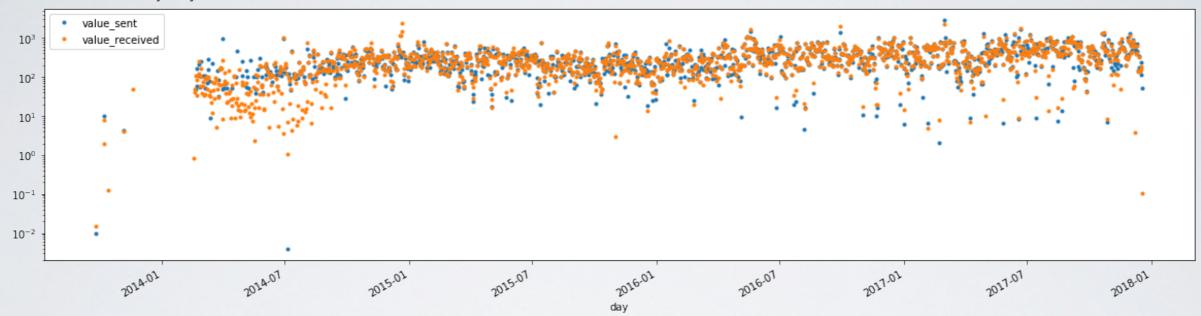
Using my wallet coins to buy some real things (Amazon gift card)

6

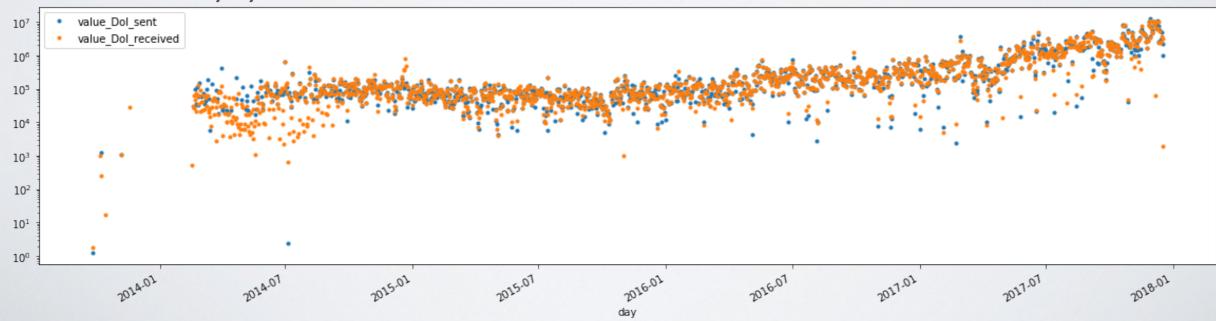


PAYMIUM ACTIVITY

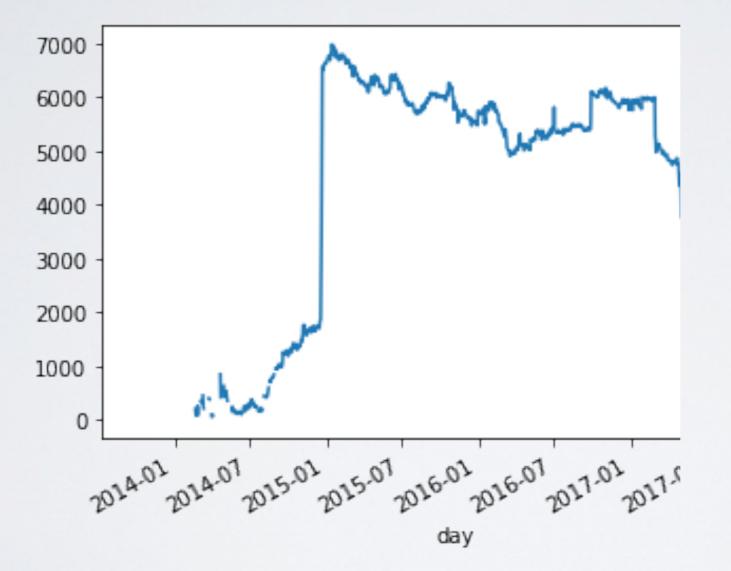
Dayly sent/received amounts in btc



Dayly sent/received amounts in \$



Cumulative of the difference between amounts received and sent (Btc owned)

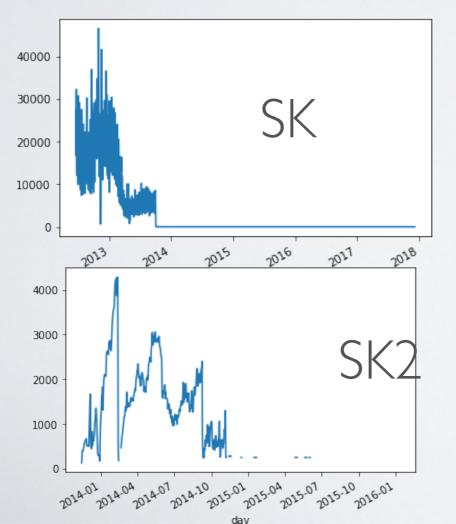


SILK ROAD

Silk Road was a website infamous for illegal product selling (drugs, etc.)

Daily transactions Amounts (btc)

Top 10 actors who Sent/Received the most to/from Silk-Road



(Mostly anonymous	ePay.info Instawallet.org Bitcoin.de-old Bitstamp.net-old 10666 89090 363 BTC-e.com-old LocalBitcoins.com-old SilkRoadMarketplace	5.057304e+05 1.785853e+05 6.506796e+04 4.965712e+04 4.130923e+04 3.998100e+04 3.533352e+04 3.511806e+04 3.451882e+04 6.393601e+06
eWallet and Mixing services)	BitcoinFog Instawallet.org ePay.info Bitstamp.net-old 2077410 89090 223978 28928788 -6337253	1.791251e+00 1.791251e+05 1.615579e+05 1.478182e+05 1.451114e+05 1.445200e+05 1.137133e+05 7.453770e+04 5.878110e+04 5.000000e+04

Some of the last transactions made by SR2... Same private Wallet, same amounts...

138077500	1415256435	SilkRoad2Market	35339862	1000000000	2014-11-06 06:47:15	2014-11-06
138081140	1415256435	SilkRoad2Market	35339862	1000000000	2014-11-06 06:47:15	2014-11-06
138081181	1415256435	SilkRoad2Market	35339862	1000000000	2014-11-06 06:47:15	2014-11-06
138081229	1415256435	SilkRoad2Market	35339862	0000000000	2014-11-06 06:47:15	2014-11-06
138081666	1415256435	SilkRoad2Market	35339862	1000000000	2014-11-06 06:47:15	2014-11-06
138081914	1415256435	SilkRoad2Market	35339862	1000000000	2014-11-06 06:47:15	2014-11-06
138081996	1415256435	SilkRoad2Market	35339862	10000000000	2014-11-06 06:47:15	2014-11-06
138082018	1415256435	SilkRoad2Market	35339862	10000000000	2014-11-06 06:47:15	2014-11-06
138082050	1415256435	SilkRoad2Market	35339862	10000000000	2014-11-06 06:47:15	2014-11-06
138082069	1415256435	SilkRoad2Market	35339862	2500000000	2014-11-06 06:47:15	2014-11-06
138082087	1415256435	SilkRoad2Market	35339862	2500000000	2014-11-06 06:47:15	2014-11-06
138082134	1415256435	SilkRoad2Market	35339862	10000000000	2014-11-06 06:47:15	2014-11-06
138082146	1415256435	SilkRoad2Market	35339862	0000000000	2014-11-06 06:47:15	2014-11-06
138082166	1415256435	SilkRoad2Market	35339862	500000000	2014-11-06 06:47:15	2014-11-06
138082206	1415256435	SilkRoad2Market	35339862	500000000	2014-11-06 06:47:15	2014-11-06
138082248	1415256435	SilkRoad2Market	35339962	10000000000	2014-11-06 06:47:15	2014-11-06

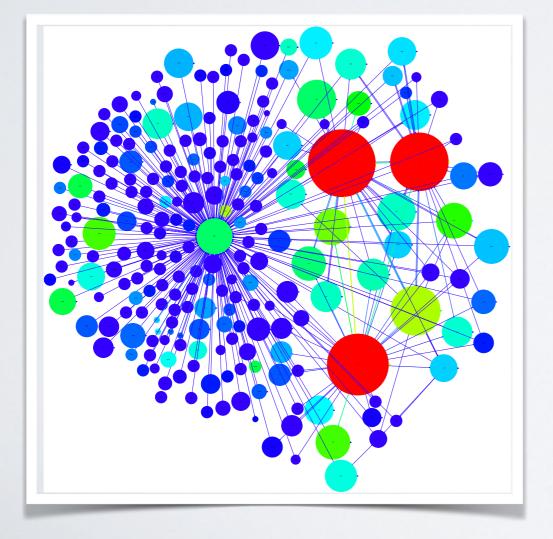
And then...

	timestamp	sender	receiver	value	date	day	PriceUSD
588090783	1492427923	35339862	-177532360	146799545224	2017-04-17 11:18:43	2017-04-17	1191.901201

EXAMPLES FROM THE SCIENTIFIC LITERATURE

EGO-CENTERED NETWORK

Wikileaks

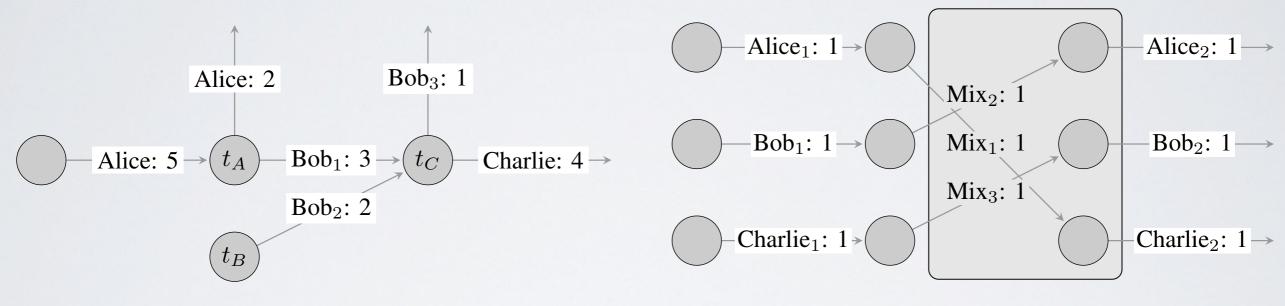


Green in the center : wikileaks

A BITCOIN THEFT



MONEY LAUNDERING



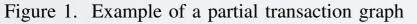
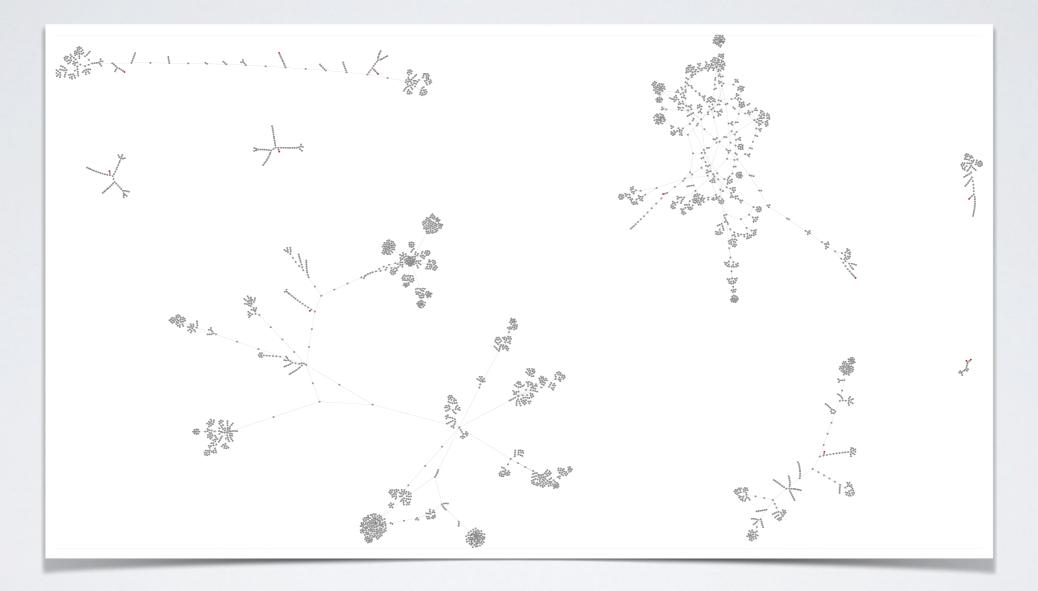


Figure 2. Block diagram of a hypothetical Bitcoin mixing service

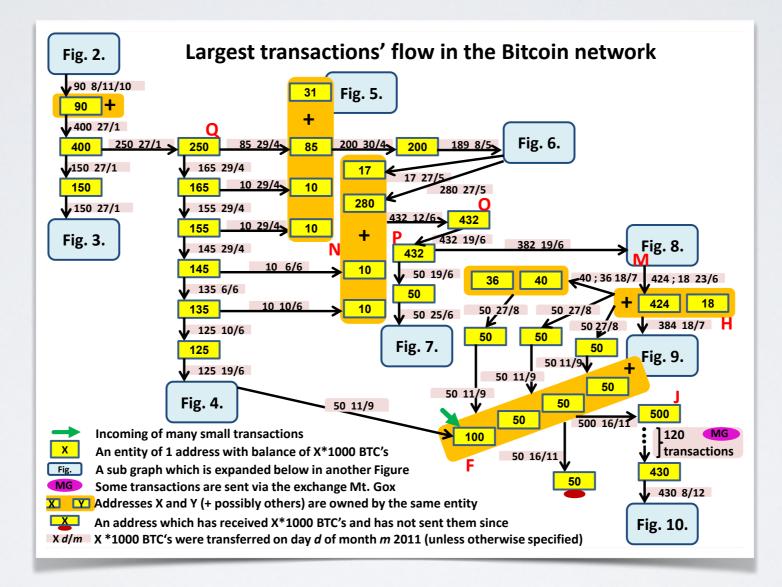
[Möser & Böhme]

MONEY LAUNDERING



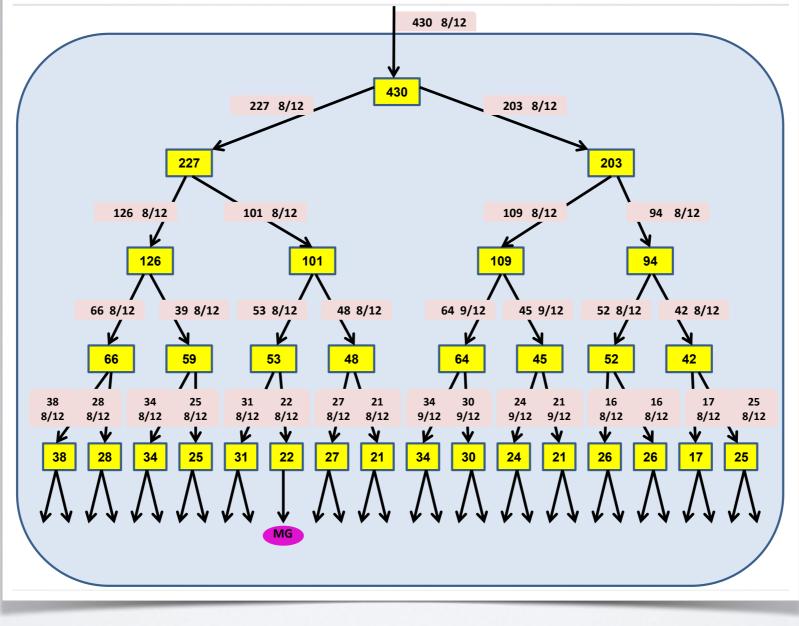
[Möser & Böhme]

EXCEPTIONAL TRANSACTIONS ANALYSIS



[Ron & Shamir]

EXCEPTIONAL TRANSACTIONS ANALYSIS



[Ron & Shamir]

ANALYSIS OF NETWORK PROPERTIES

