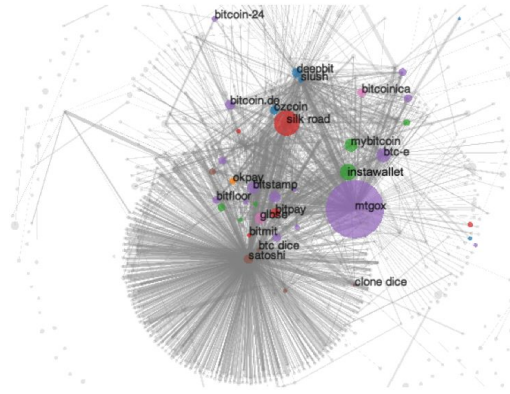


Blockchain: what it is and why it matters

Laura Ricci
Damiano Di Francesco Maesa

6/4/2022

damiano.difrancesco@unipi.it



Bitcoin user's graph analysis

Graph models

Different models possible for the same blockchain data

- Address graph: nodes are addresses, edges are payments between them
- Users graph: nodes are addresses clusters, edges are payments between the addresses inside the clusters
- Simple Transactions graph: nodes are transactions, edges indicate outputs used as inputs between transactions
- Addresses-Transactions graph: bipartite, nodes are either addresses or transactions, edges are payments between a transaction to an address or vice versa

All multigraphs

Graph models

Trustful Transactions Graphs

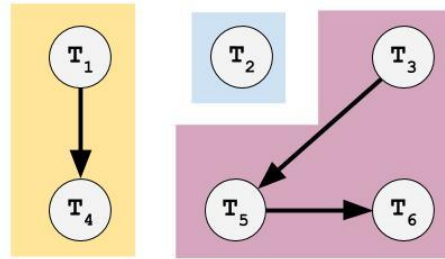
Transactions List 7

Block b

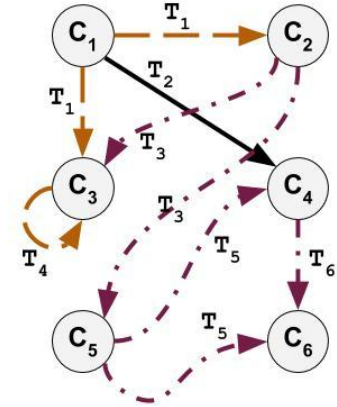
timestamp
blockId

T1: $\{ \{ (101, c1, 10) \}, \{ (200, c2, 5), (201, c3, 5) \} \}$
T2: $\{ \{ (123, c1, 10) \}, \{ (202, c4, 10) \} \}$
T3: $\{ \{ (134, c2, 5) \}, \{ (203, c5, 2), (204, c3, 3) \} \}$
T4: $\{ \{ (201, c3, 5), (145, c3, 10) \}, \{ (205, c3, 15) \} \}$
T5: $\{ (203, c5, 2) \}, \{ (206, c6, 1), (207, c4, 1) \}$
T6: $\{ (207, c4, 1) \}, \{ (208, c6, 1) \}$

H_b



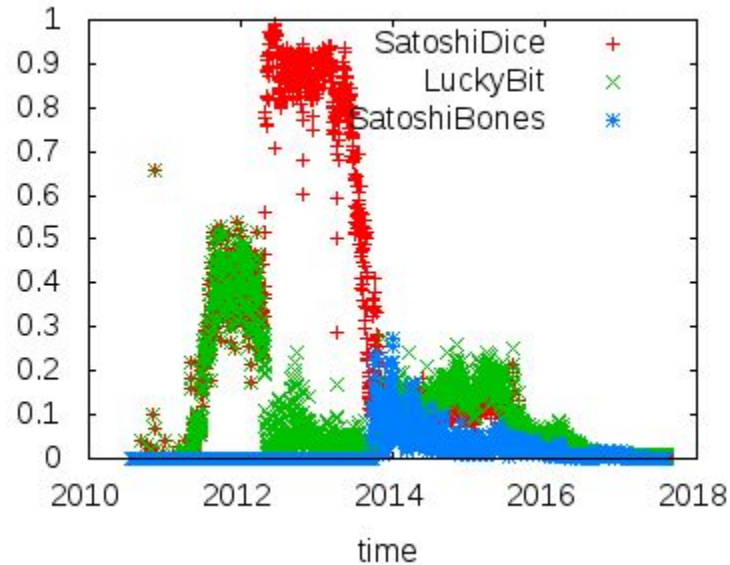
G_T



Graph models

Trustful Transactions Graphs

Percentage of TTGs containing at least one cluster of three considered betting services.



Users Graph

Weighted directed multigraph

E.g. until 2017-08-10 18:03 GMT

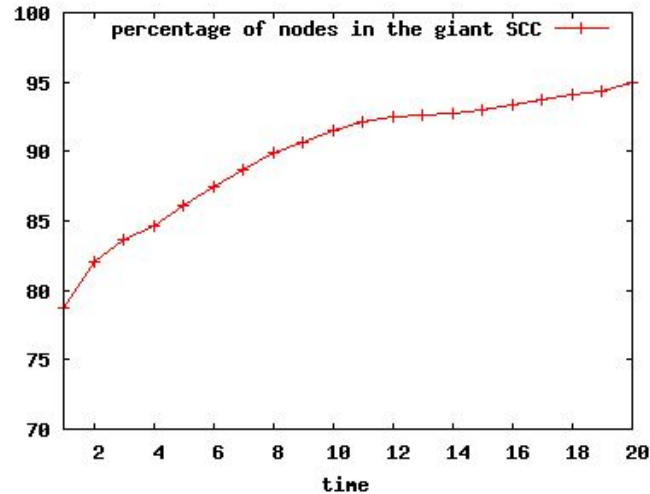
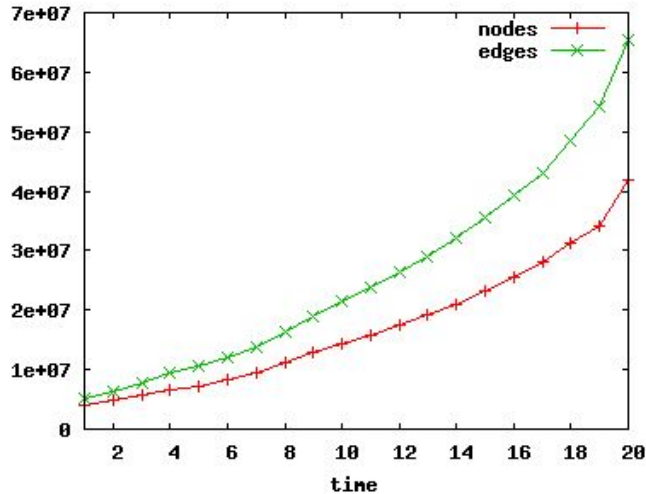
- 293,798,168 Addresses
- 245,410,081 Transactions
- 139,962,731 Nodes
- 666,229,139 Edges (354,715,071 unique, non self loops)

E.g. **until 2015-12-23 09:40:52 GMT**

- 113,221,083 Addresses
- 99,602,440 Transactions
- 46,144,246 Nodes
- 294,705,549 Edges

Users Graph

Densification, distance analysis, degree distribution, clustering coefficient and several centrality measures



TIME t	SNAPSHOT
1	Tue Jan 01 00:00:00 GMT 2013
2	Sun Feb 24 07:41:02 GMT 2013
3	Fri Apr 19 15:22:04 GMT 2013
4	Wed Jun 12 23:03:06 GMT 2013
5	Tue Aug 06 06:54:08 GMT 2013
6	Sun Sep 29 14:25:10 GMT 2013
7	Fri Nov 22 22:06:12 GMT 2013
8	Thu Jan 16 05:47:14 GMT 2014
9	Tue Mar 11 13:28:16 GMT 2014
10	Sun May 04 21:09:18 GMT 2014
11	Sat Jun 28 04:50:20 GMT 2014
12	Thu Oct 14 20:12:24 GMT 2014
13	Tue Dec 08 03:53:26 GMT 2014
14	Mon Dec 08 03:53:26 GMT 2014
15	Sat Jan 31 11:34:28 GMT 2015
16	Thu Mar 26 19:15:30 GMT 2015
17	Wed May 20 02:56:32 GMT 2015
18	Mon Jul 13 10:37:34 GMT 2015
19	Sat Sep 05 18:18:36 GMT 2015
20	Wed Dec 23 9:40:52 GMT 2015

Users Graph

Densification, distance analysis, degree distribution, clustering coefficient and several centrality measures

Harmonic	Indegree	Degree
Mt. Gox	Mt.Gox	Mt.Gox
2477299	BTC-e.com1	LocalBitcoins.com
LocalBitcoins.com	LocalBitcoins.com	2477299
Cex.io	AgoraMarket	BTC-e.com1
FaucetBOX.com	SilkRoadMarketplace	AgoraMarket
26638073	2477299	SilkRoadMarketplace
MoonBit.co	BitPay.com1	BitPay.com1
19860816	BTC-e.com2	BTC-e.com2
Poloniex.com	BitPay.com2	Cryptsy.com
Bittrex.com	Cryptsy.com	BitPay.com2

Rich Get Richer

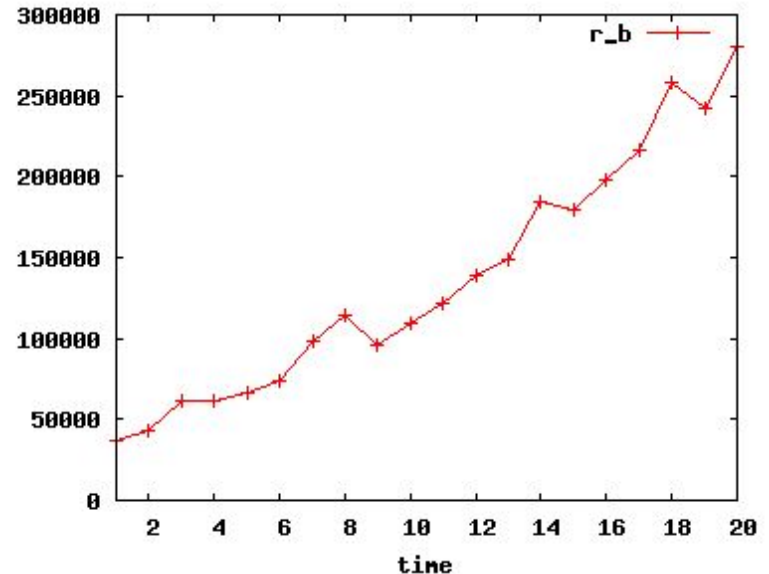


Rich get Richer:



The richest users at time t are richer than the richest users at time $t' < t$

$$r_b^t = \frac{\sum_{u \in B_k^t} b^t(u)/k}{\sum_{u \in V^t} b^t(u)/|V^t|}$$



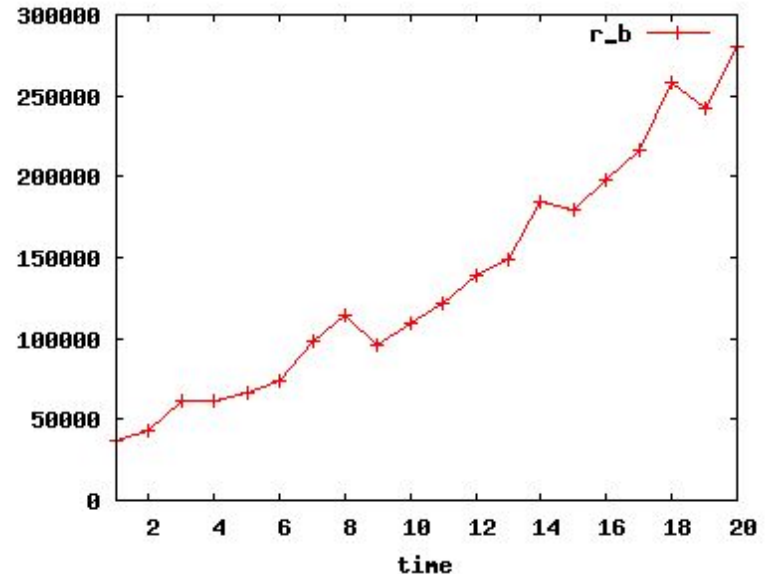
Rich get Richer:



The richest users at time t are richer than the richest users at time $t' < t$

$$r_b^t = \frac{\sum_{u \in B_k^t} b^t(u)/k}{\sum_{u \in V^t} b^t(u)/|V^t|}$$

↓

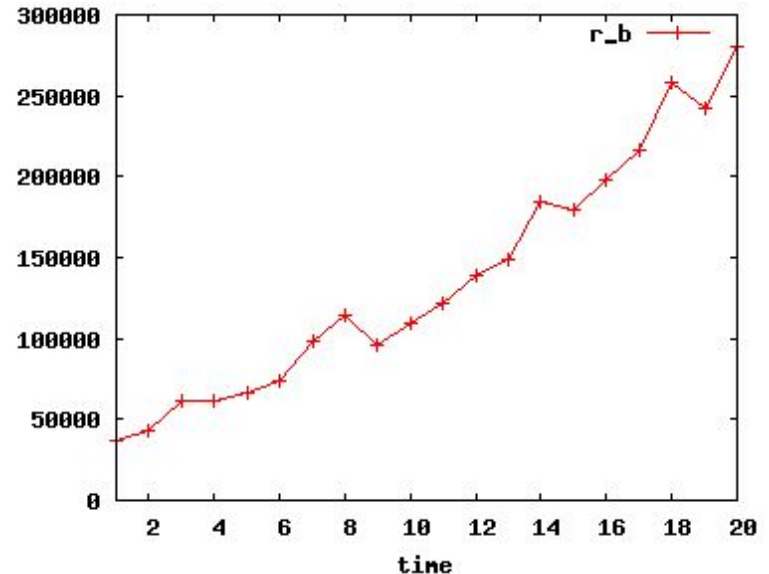


Rich get Richer:



The richest users at time t are richer than the richest users at time $t' < t$

$$r_b^t = \frac{\sum_{u \in B_k^t} b^t(u)/k}{\sum_{u \in V^t} b^t(u)/|V^t|}$$

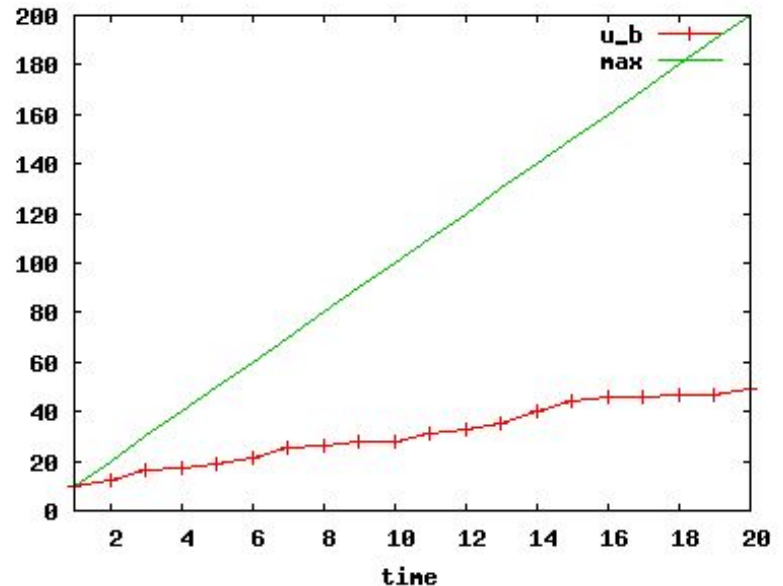


Rich get Richer:



The richest users at a certain time t tend to remain the richest at time $t' > t$

$$u_b^t = \left| \bigcup_{i=1}^t B_k^i \right|$$

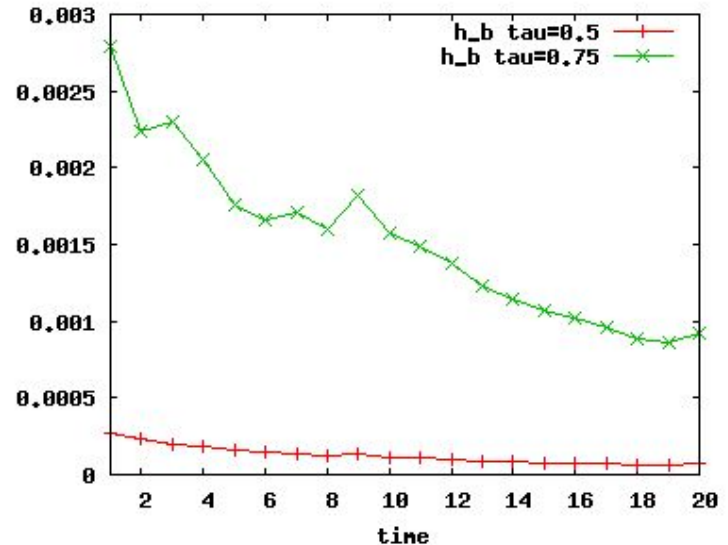


Rich get Richer:



The richness gets more concentrated with the progression of time

$$h_b^t = \min \left\{ k : \frac{\sum_{u \in B_k^t} b^t(u)}{\sum_{u \in V^t} b^t(u)} > \tau \right\} / |V^t|$$

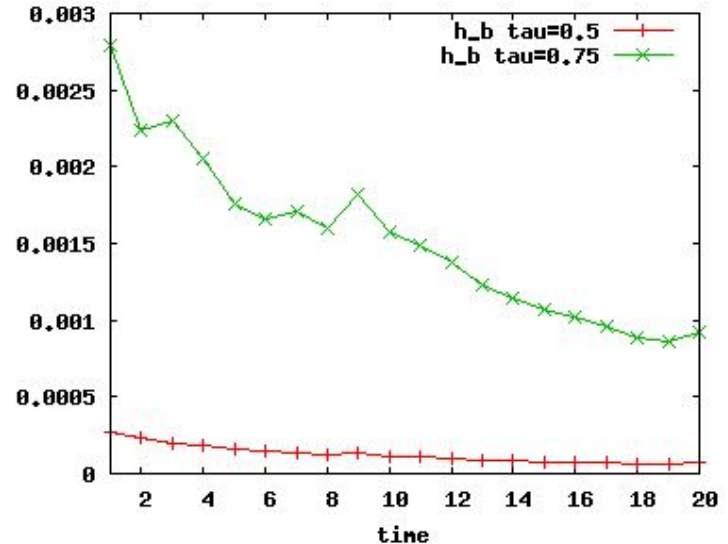


Rich get Richer:



The richness gets more concentrated with the progression of time

$$h_b^t = \min \left\{ k : \frac{\sum_{u \in B_k^t} b^t(u)}{\sum_{u \in V^t} b^t(u)} > \tau \right\} / |V^t|$$



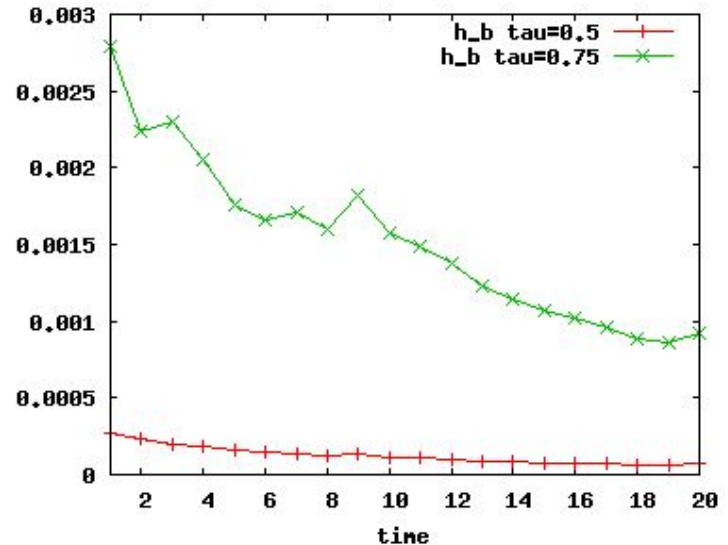
Rich get Richer:



The richness gets more concentrated with the progression of time

$$h_b^t = \min \left\{ k : \frac{\sum_{u \in B_k^t} b^t(u)}{\sum_{u \in V^t} b^t(u)} > \tau \right\} / |V^t|$$

↓



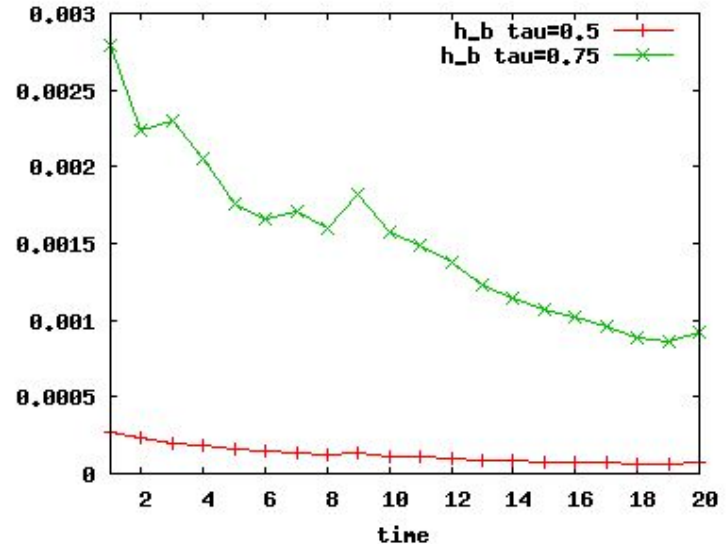
Rich get Richer:



The richness gets more concentrated with the progression of time

$$h_b^t = \min \left\{ k : \frac{\sum_{u \in B_k^t} b^t(u)}{\sum_{u \in V^t} b^t(u)} > \tau \right\} / |V^t|$$

↓

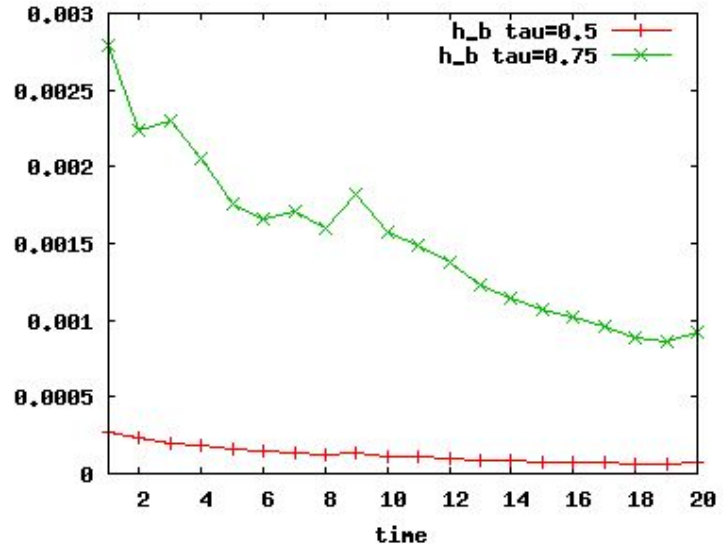


Rich get Richer:



The richness gets more concentrated with the progression of time

$$h_b^t = \min \left\{ k : \frac{\sum_{u \in B_k^t} b^t(u)}{\sum_{u \in V^t} b^t(u)} > \tau \right\} // |V^t|$$

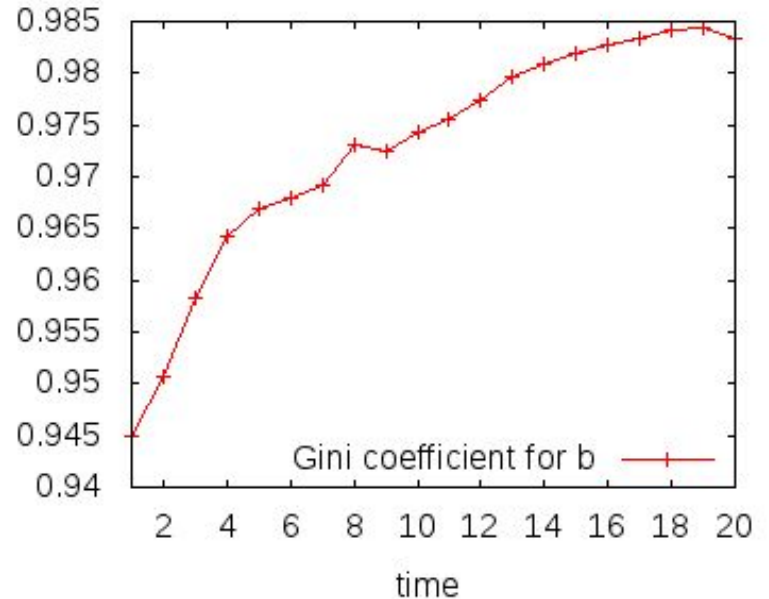


Rich get Richer:



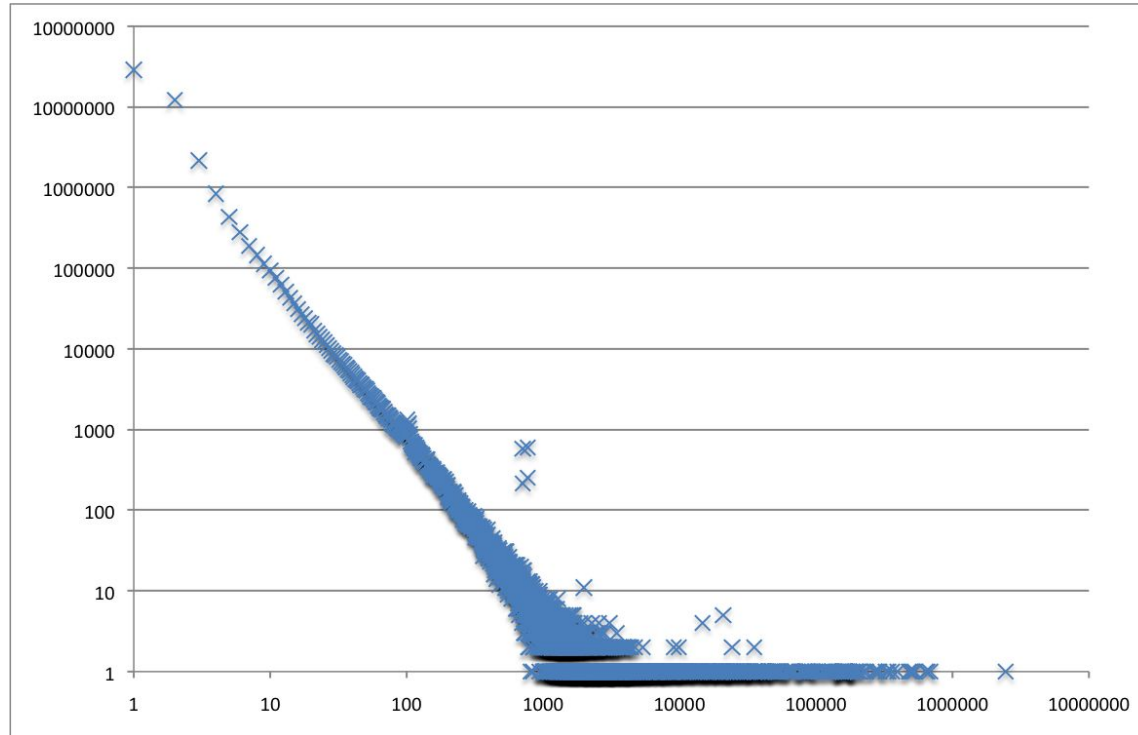
Gini coefficient

$$G = \frac{2 \sum_{i=1}^n i x_i}{n \sum_{i=1}^n x_i} - \frac{n+1}{n}$$

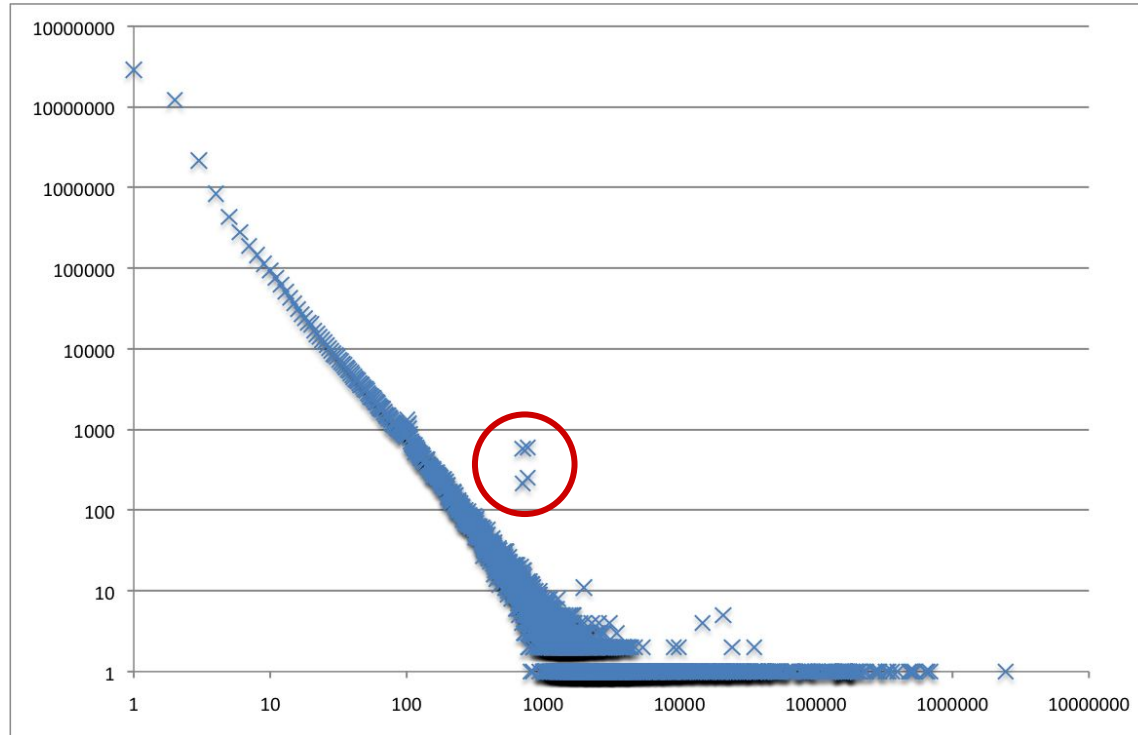


Small World Anomalies

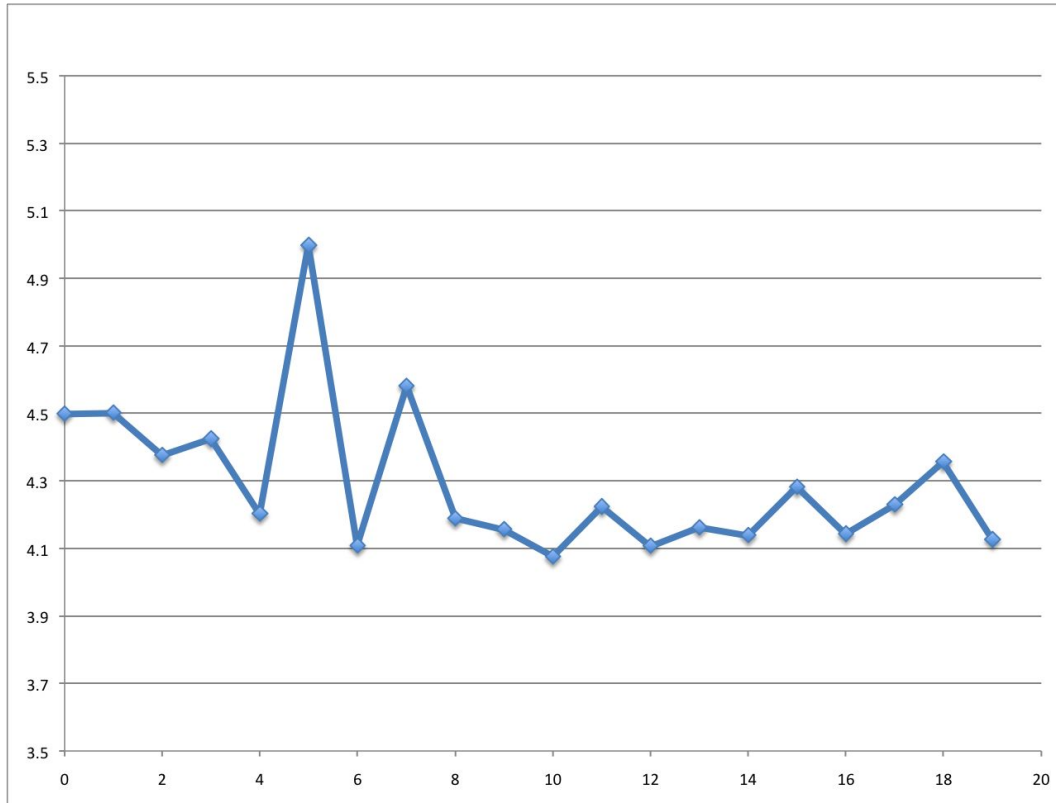
Indegree Distribution



Indegree Distribution



Average Distance

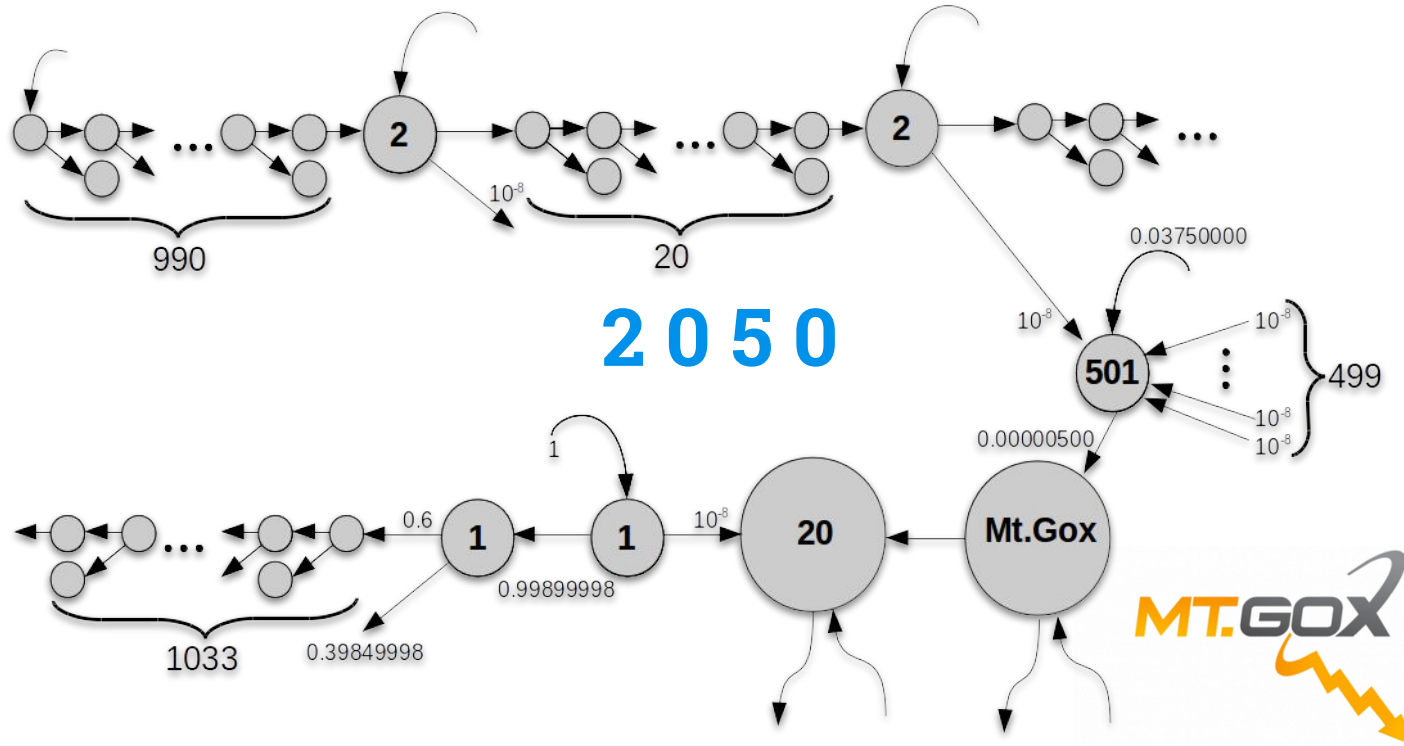


Diameter

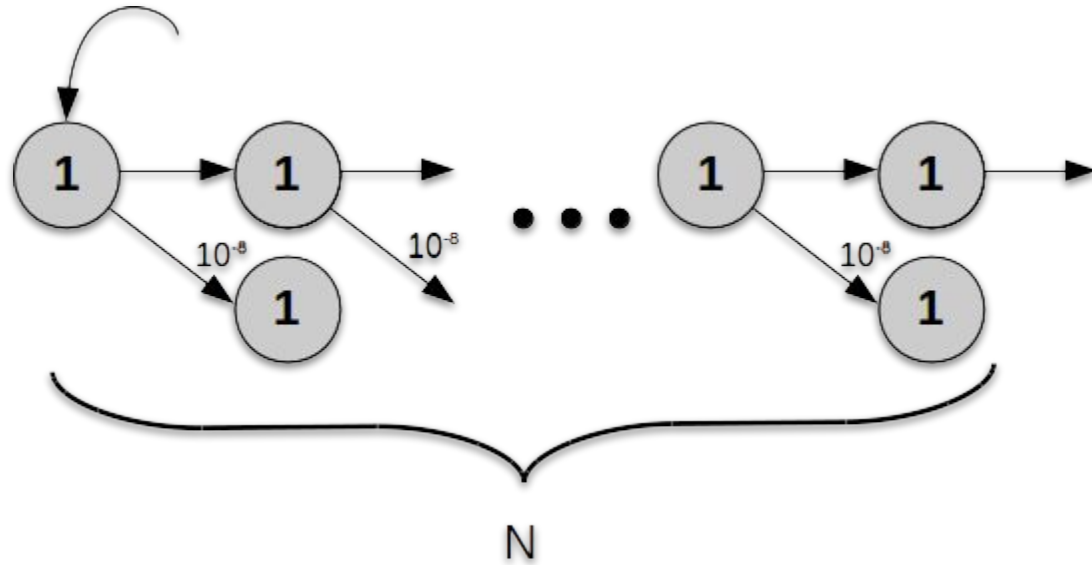
2 0 5 0

Diameter

CLUSTER
SIZE



Diameter



Detecting Patterns



An interesting transaction

35dead89c059e846e2013
a06a70cd84a7ba0f80da7
741c283d6efd573e0a7319

13h8bRdWGLCDNkDR8Pyf6jw3wM3q4EwbTF (0.0929742 BTC - Output)



1G8zjUzeZBUpeC...	(Jay_Pal) - (Unspent)	0.00001 BTC
14bFbRFJQXZTPG...	(aronm) - (Unspent)	0.00001 BTC
1C3NNQ6Y7Qa7Q...	(Jambo) - (Spent)	0.00001 BTC
1DhFR2vR6w17BV...	(arly) - (Unspent)	0.00001 BTC
14B3GFdIBZqxgNp...	(arekb) - (Unspent)	0.00001 BTC
1MAVvk5dcd3v9m8...	(Jameson) - (Unspent)	0.00001 BTC
19V4iTPAYUPT7Lx...	(aredk) - (Unspent)	0.00001 BTC
143SikKpjzwhBy5Z...	(Jan) - (Unspent)	0.00001 BTC
12ZyGLi2ps2Agpy8...	(ak0b) - (Unspent)	0.00001 BTC
1PxBSHEZ3EbyZ4...	(ake262144) - (Unspent)	0.00001 BTC
1KseGadiZnuFoHo...	(alidi) - (Unspent)	0.00001 BTC
1JadeSJWfvCuMA...	(Jade-) - (Unspent)	0.00001 BTC
1JALLENn5SAy4F...	(allen) - (Unspent)	0.00001 BTC
1GsNNdHjYFSf5mBgHRwqJe3zLEYfMcHYTA	- (Spent)	0.0912558 BTC
1BgKdr9cZc2yFpX...	(akers1976) - (Unspent)	0.00001 BTC
1EPY398Xk6cgqP...	(abberwok) - (Unspent)	0.00001 BTC
19QkqAza7BHFTu...	(ackjack) - (Unspent)	0.00001 BTC
1jackkHHCLixryJF...	(ackmaninov) - (Unspent)	0.00001 BTC
17iqSDHshYLthDv...	(acoder) - (Unspent)	0.00001 BTC
1CXwyYjrc8Vock5...	(acroe) - (Unspent)	0.00001 BTC
16jVo7Vj7QdZ4Ap...	(ziHostik) - (Unspent)	0.00001 BTC
1FzcqrNwbXgkDk...	(ixne) - (Unspent)	0.00001 BTC
1MZVFA1VZmYTP...	(bixi) - (Unspent)	0.00001 BTC
1BSGbFq4GBr3uck...	(JA37) - (Unspent)	0.00001 BTC
1aombYbEygW4u...	(yeman) - (Unspent)	0.00001 BTC
1FkN3XYsvuNdd2l...	(J.) - (Unspent)	0.00001 BTC
1DbQYvpXSVB7G...	(tsybitsy) - (Unspent)	0.00001 BTC
1CmUQsc87rByVi...	(temine) - (Unspent)	0.00001 BTC
19e3fcoLTu8YVFA...	(bica) - (Unspent)	0.00001 BTC
1Lhfrdmq563mZxY...	(vanish) - (Unspent)	0.00001 BTC
18ZcRwarkP4akcT...	(itsASpark) - (Unspent)	0.00001 BTC

An interesting transaction

35dead89c059e846e2013
a06a70cd84a7ba0f80da7
741c283d6efd573e0a7319

13hBbRdWGLCDNkDR8Pyf6jw3wM3q4EwbTF (0.0929742 BTC - Output)



1G8zjUzeZBUpeC...	(Jay_Pal) - (Unspent)	0.00001 BTC
14bFbRFJQXZTPG...	(aronm) - (Unspent)	0.00001 BTC
1C3NNQ6Y7Qa7Q...	(Jambo) - (Spent)	0.00001 BTC
1DhFR2vR6w17BV...	(arly) - (Unspent)	0.00001 BTC
14B3GFdIBZqxgNp...	(arekb) - (Unspent)	0.00001 BTC
1MAVvk5dcd8v9m8...	(Jameson) - (Unspent)	0.00001 BTC
19V4ITPAYUPT7Lx...	(aredk) - (Unspent)	0.00001 BTC
143SikKpjzwhBy5Z...	(Jan) - (Unspent)	0.00001 BTC
12ZyGLi2ps2Agpy8...	(ak0b) - (Unspent)	0.00001 BTC
1PxBSHEZ3EbyZ4...	(ake262144) - (Unspent)	0.00001 BTC
1KseGadiZnuFoHo...	(alidi) - (Unspent)	0.00001 BTC
1JadeSJWfvCuMA...	(Jade-) - (Unspent)	0.00001 BTC
1GsNNdHjYFSf5mBgHRwqJe3zLEyIMcHYTA	(Spent)	0.0912568 BTC
1EPY398Xk6cgqP...	(jabberwok) - (Unspent)	0.00001 BTC
19QkqAza7BHFTu...	(jack(jack)) - (Unspent)	0.00001 BTC
1jackkHHCLixryJF...	(jackmaninov) - (Unspent)	0.00001 BTC
17iqSDHshYLthDv...	(acoder) - (Unspent)	0.00001 BTC
1CXwyYjrc8Vock5...	(acroe) - (Unspent)	0.00001 BTC
16jVo7Vj7QdZ4Ap...	(ziHostik) - (Unspent)	0.00001 BTC
1FzcqrNwbXgkDk...	(ixne) - (Unspent)	0.00001 BTC
1MZVFA1VZmYTP...	(bipixi) - (Unspent)	0.00001 BTC
1BSGbFq4GBr3uck...	(JA37) - (Unspent)	0.00001 BTC
1aombYbEygW4u...	(lyeman) - (Unspent)	0.00001 BTC
1FkN3XYsvuNdd2l...	(J.) - (Unspent)	0.00001 BTC
1DbQYvpXSVB7G...	(tsybitsy) - (Unspent)	0.00001 BTC
1CmUQsc87rByVi...	(temine) - (Unspent)	0.00001 BTC
19e3fcoLTu8YVFA...	(bica) - (Unspent)	0.00001 BTC
1Lhfrdmq563mZxY...	(vanish) - (Unspent)	0.00001 BTC
18ZoRwarkP4akcTl...	(itsAspark) - (Unspent)	0.00001 BTC

An interesting transaction

35dead89c059e846e2013
a06a70cd84a7ba0f80da7
741c283d6efd573e0a7319

13hBbRdWGLCDNkDR8Pyf6jw3wM3q4EwbTF (0.0929742 BTC - Output)

Fee 0.0007184 BTC

41.8% of the total value actually spent

1G8zjUzeZBUpeC...	(Jay_Pal) - (Unspent)	0.00001 BTC
14bFbRFJQXZTPG...	(aronm) - (Unspent)	0.00001 BTC
1C3NNQ6Y7Qa7Q...	(Jambo) - (Spent)	0.00001 BTC
1DhFR2vR6w17BV...	(arly) - (Unspent)	0.00001 BTC
14B3GFdIBZqxgNp...	(arekb) - (Unspent)	0.00001 BTC
1MAVvk5dcd3v9m8...	(Jameson) - (Unspent)	0.00001 BTC
19V4ITPAYUPT7Lx...	(aredk) - (Unspent)	0.00001 BTC
143SikKpjzwhBy5Z...	(Jan) - (Unspent)	0.00001 BTC
12ZyGLi2ps2Agpy8...	(ak0b) - (Unspent)	0.00001 BTC
1PxBSHEZ3EbyZ4...	(ake262144) - (Unspent)	0.00001 BTC
1KseGadiZnuFoHo...	(alidi) - (Unspent)	0.00001 BTC
1JadeSJWfvCuMA...	(Jade-) - (Unspent)	0.00001 BTC
1GsNNdHjYFSf5mBgHRwqJe3zLEYfMcHYTA	- (Spent)	0.0912568 BTC
1EPY398Xk6cgqP...	(jabberwok) - (Unspent)	0.00001 BTC
19QkqAza7BHFTu...	(jackjack) - (Unspent)	0.00001 BTC
1jackkHHCLxryJF...	(jackmaninov) - (Unspent)	0.00001 BTC
17iqSDHshYLthDv...	(acoder) - (Unspent)	0.00001 BTC
1CXwyYjrc8Vock5...	(acroe) - (Unspent)	0.00001 BTC
16jVo7Vj7QdZ4Ap...	(ziHostik) - (Unspent)	0.00001 BTC
1FzcqrNwbXgkDk...	(ixne) - (Unspent)	0.00001 BTC
1MZVFA1VZmYTP...	(bipixi) - (Unspent)	0.00001 BTC
1BSGbFq4GBr3uck...	(JAS7) - (Unspent)	0.00001 BTC
1aombYbEyygW4u...	(lyeman) - (Unspent)	0.00001 BTC
1FkN3XYsvuNdd2l...	(J.) - (Unspent)	0.00001 BTC
1DbQYvpXSVB7G...	(tsybitsy) - (Unspent)	0.00001 BTC
1CmUQsc87rByVi...	(temine) - (Unspent)	0.00001 BTC
19e3fcoLTu8YVFA...	(bica) - (Unspent)	0.00001 BTC
1Lhfrdmq563mZxY...	(vanish) - (Unspent)	0.00001 BTC
18ZoRwarkP4akcTl...	(itsAspark) - (Unspent)	0.00001 BTC

Classification

Transaction with:

- only one input
- all outputs with same amount except for change

Generic Pseudo Spam

$t = (\text{In}, \text{Out}, \text{InAmount}, \text{Fees})$

- $|\text{In}| = 1$
- $|\text{Out}| \geq 3$
- $|\{(o, b) \in \text{Out} : b = a\}| \leq 1$, for some $a \in \mathbb{R}$

Chain them through change addresses

Artificial Transactions

Artificial transactions: the transaction purpose is to obtain some kind of side effect outside the blockchain rather than to transfer value between addresses

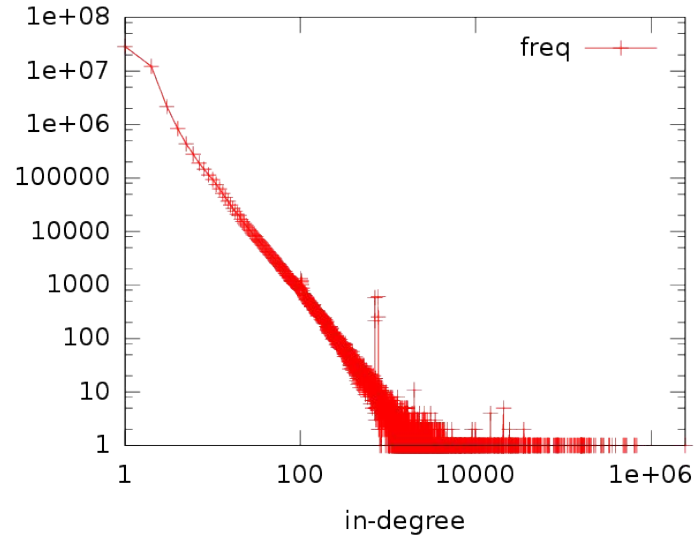
Blind trust: GPS -chains change outputs are spent much faster than average
spending block wait 88 vs 2413

Artificial Transactions

Possible interpretations:

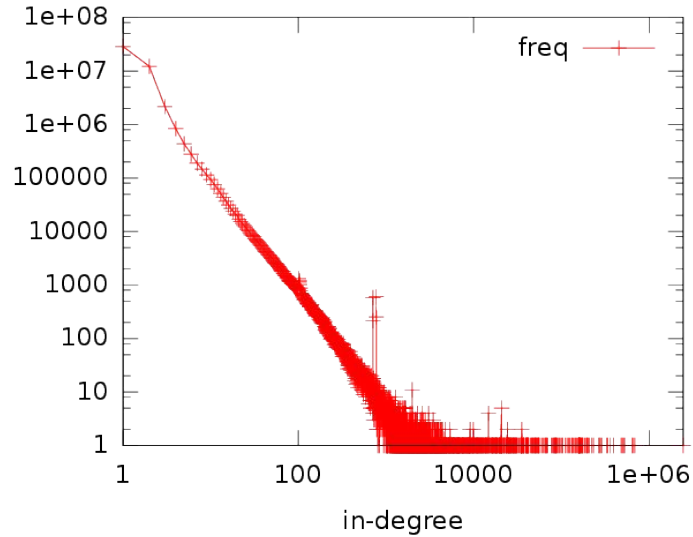
- Attack on users pseudonymity by increasing heuristic rules effectiveness
- UTXO spam attack (flooding attack of July 2015)
- Live spam advertising campaign through **vanity addresses**, e.g.
1**Sochi**WwFFySPjQoi2biVftXn8NRPCSQC, 1**Enjoy**1C4bYBr3tN4sMKxvJDqG8NkdR4Z

GPSchains pruning

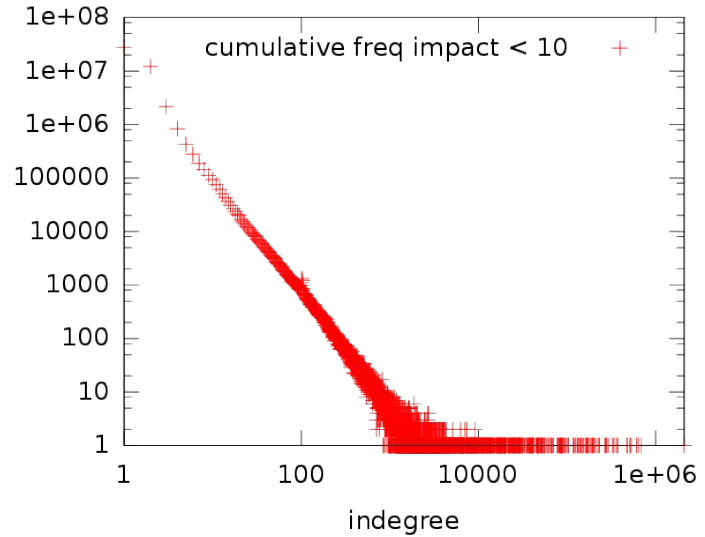


2050

GPSchains pruning

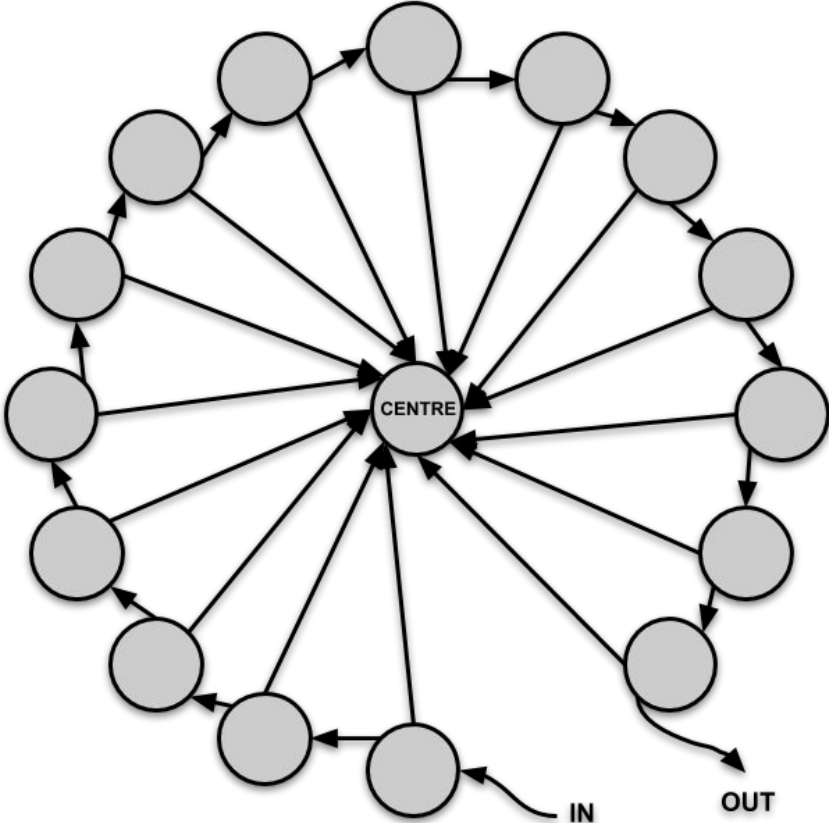


2050

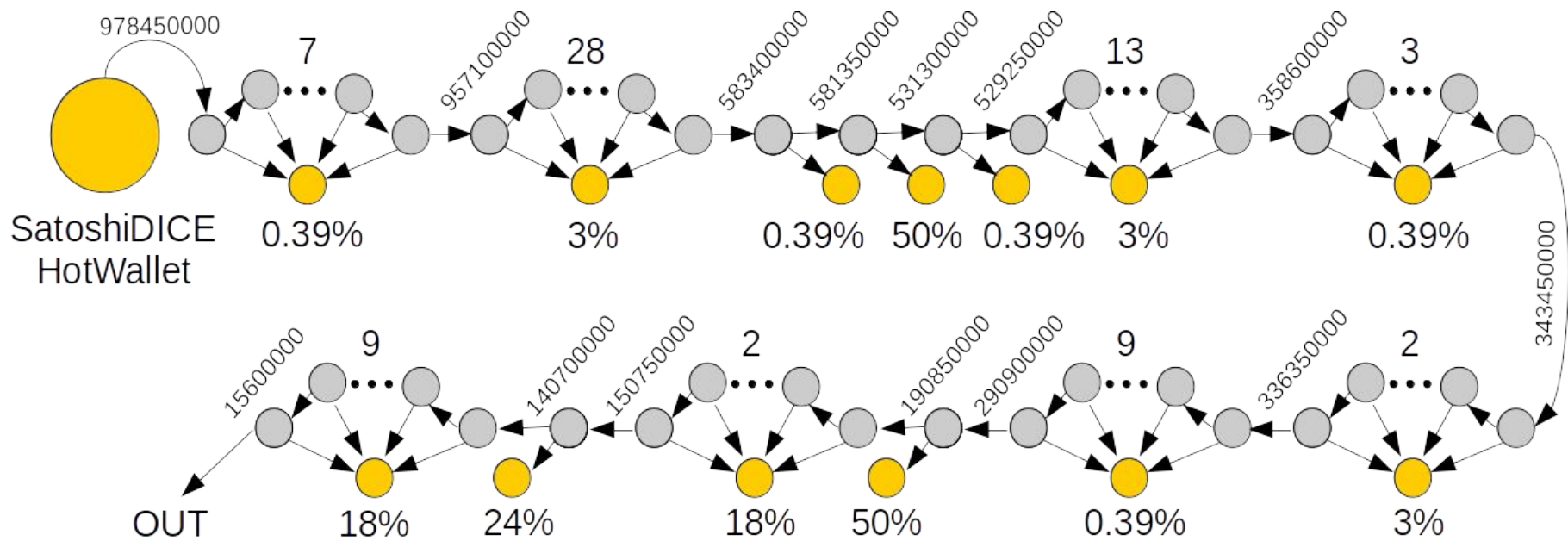


9 (575)

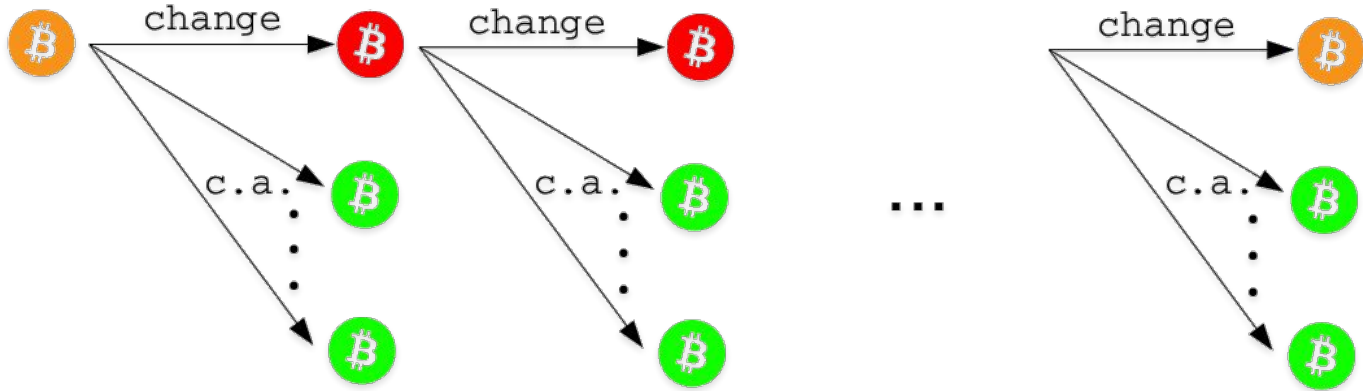
Wheels



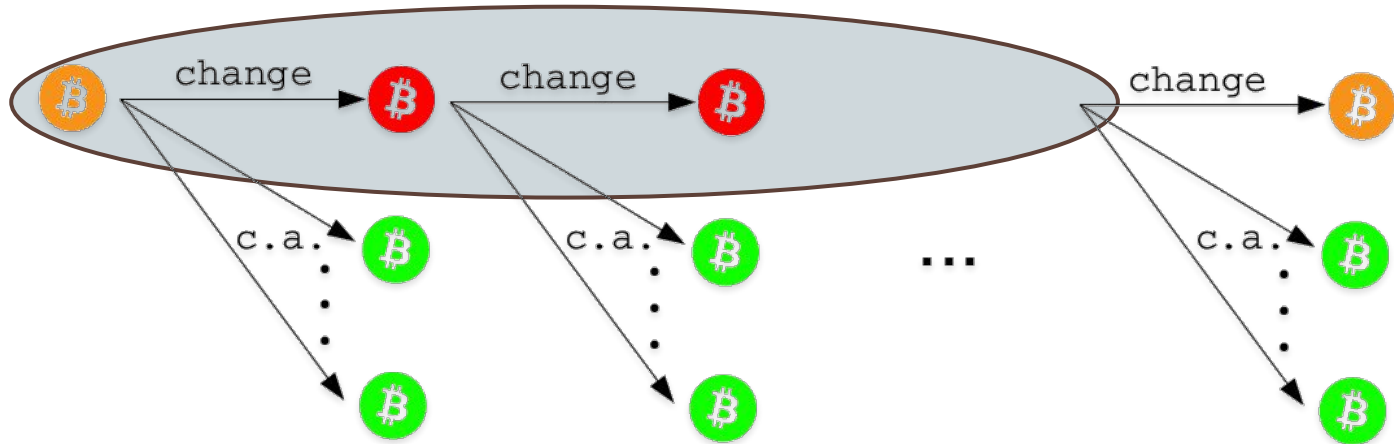
Wheels

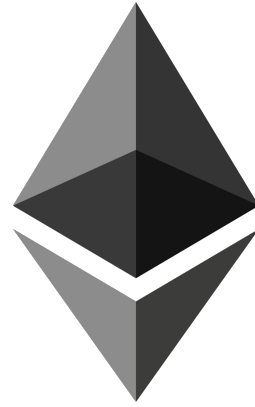


Chain Heuristic

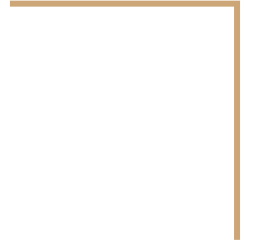
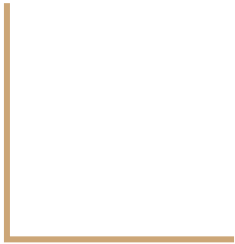


Chain Heuristic





Ethereum economies



Ethereum tokens

Ethereum allows for layered economies (isolated or connected) through smart contracts.

Fungible or non fungible tokens:

- fungible tokens induce fully layered economies (with fixed rules) on top of ether exchanges.

Fungible means that all tokens are identical and interchangeable (they carry no attached info).

ERC-20 standard (Ethereum Request for Comments 20)

ERC-20

function name() public view returns (string)

function symbol() public view returns (string)

function decimals() public view returns (uint8)

function totalSupply() public view returns (uint256)

function balanceOf(address _owner) public view returns (uint256 balance)

function transfer(address _to, uint256 _value) public returns (bool success)



**function transferFrom(address _from, address _to, uint256 _value) public returns
(bool success)**

function approve(address _spender, uint256 _value) public returns (bool success)

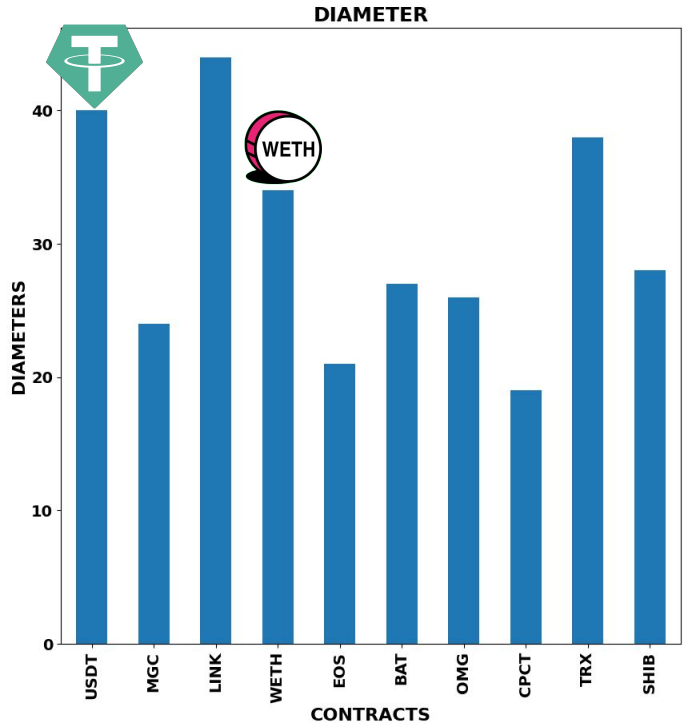
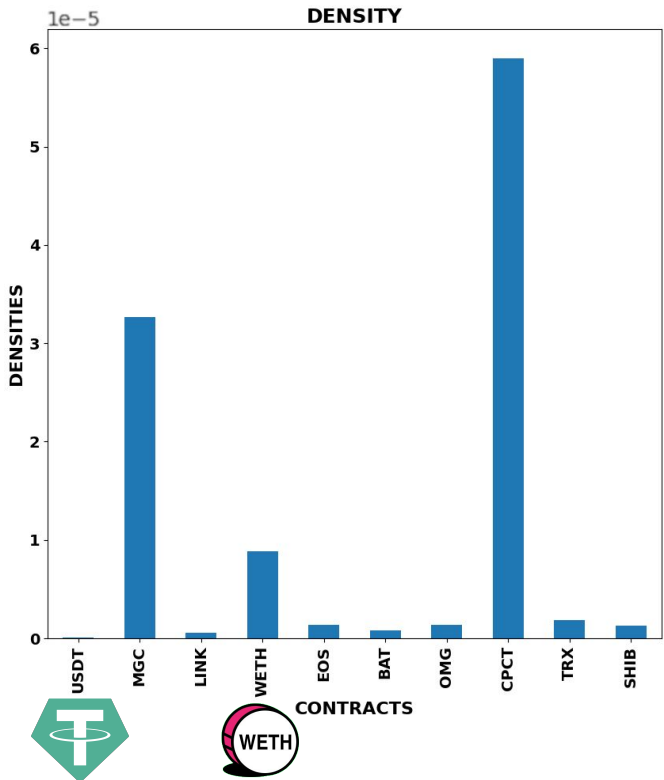
function allowance(address _owner, address _spender) public view returns (uint256
remaining)

ERC-20 analysis

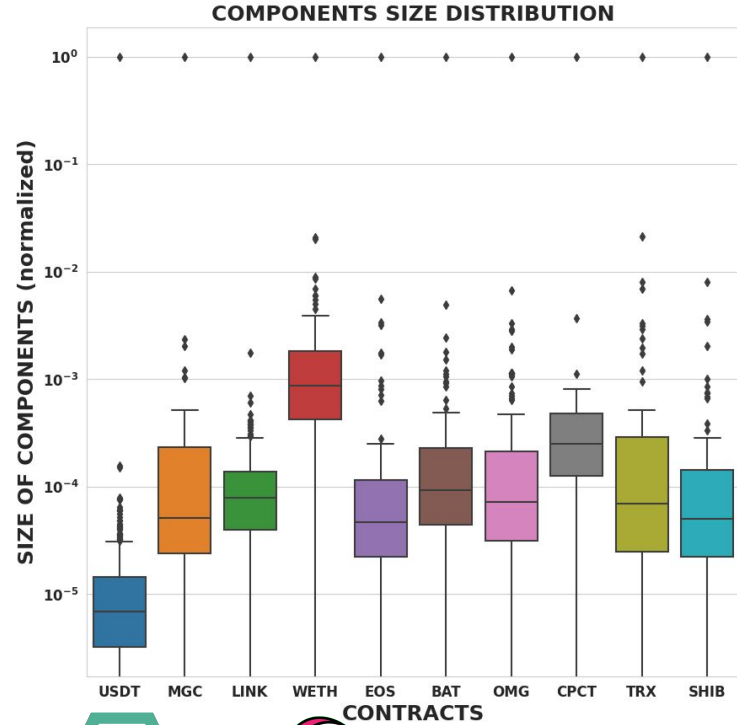
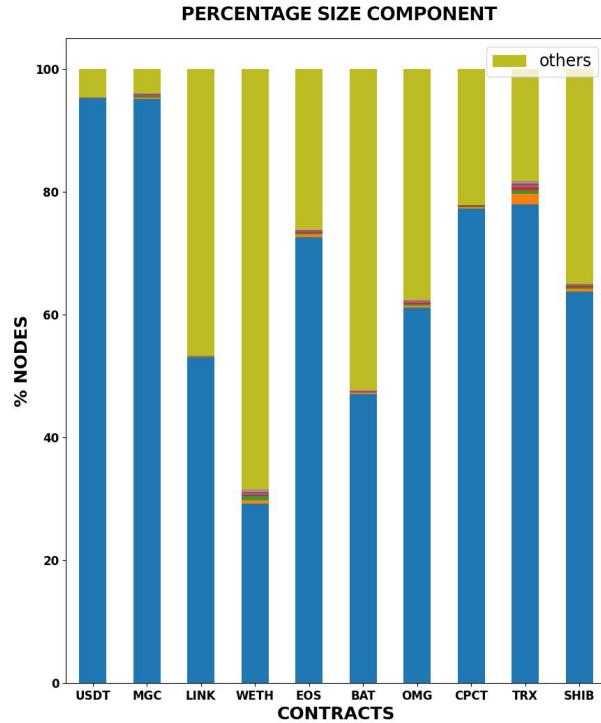
10 most popular (by number of transactions) ERC-20 smart contracts on the Ethereum blockchain (until November 2021).

Token	Transactions	Nodes	Edges	Multi-edges %		
USDT	112 938 770	33 364 482	53 046 857	25	stable	
MGC	9 088 327	724 078	8 563 420	4.3	wallet	
LINK	4 926 783	3 428 016	3 164 252	11.4	oracles	
WETH	3 082 172	169 083	126 784	23.5	Wrapped eth	
EOS	2 970 111	1 556 393	1 651 465	22	Crypto	
BAT	2 732 230	2 036 665	1 718 097	11	Advertisement	
OMG	2 527 799	1 379 525	1 333 777	17.2	Crypto	
CPCT	2 229 775	72 274	154 101	56.7	Crypto IoT	
TRX	2 084 274	1 305 033	1 583 982	10.2	Crypto TRON	
SHIB	1 922 519	1 398 040	1 255 602	15.5	Crypto Doge	

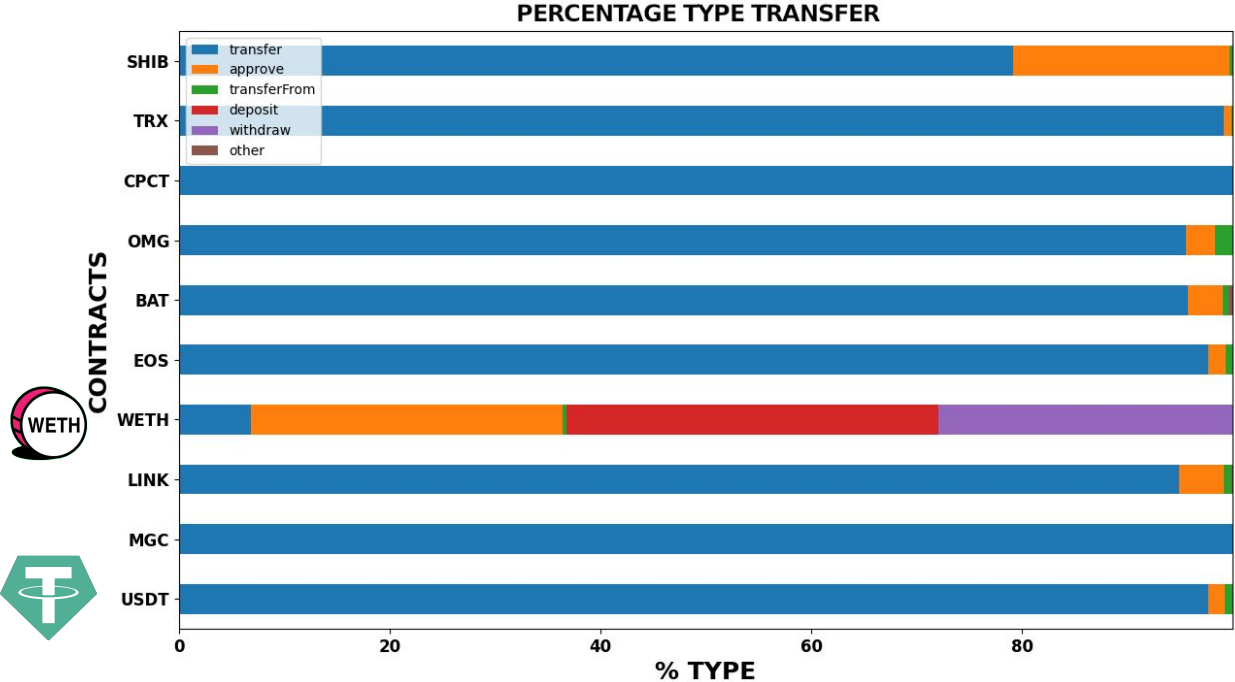
ERC-20 analysis



ERC-20 analysis

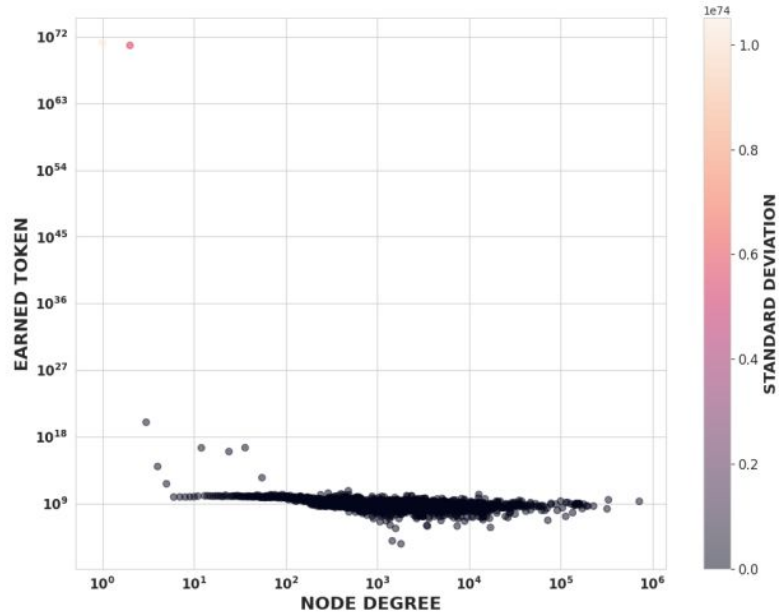
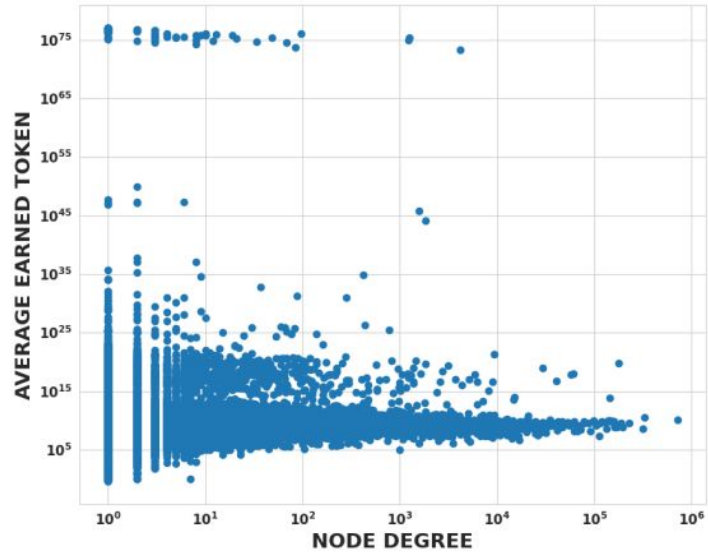


ERC-20 analysis



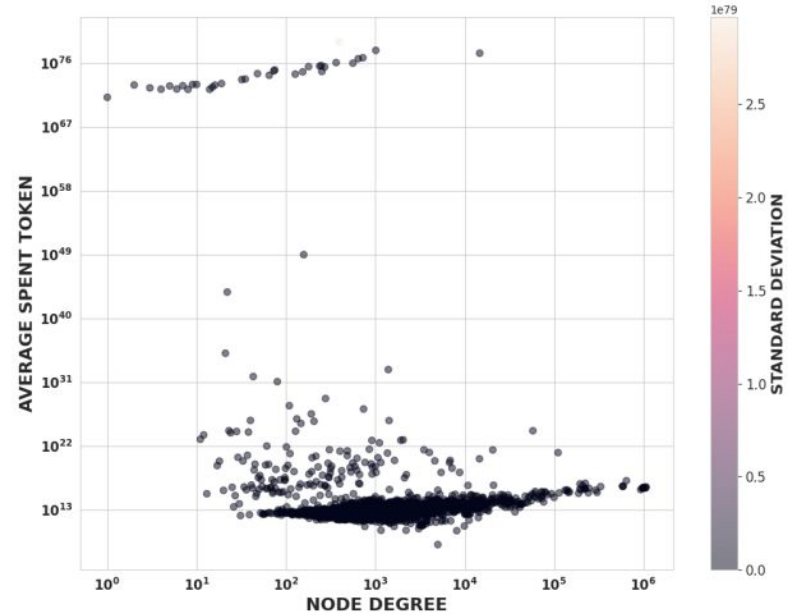
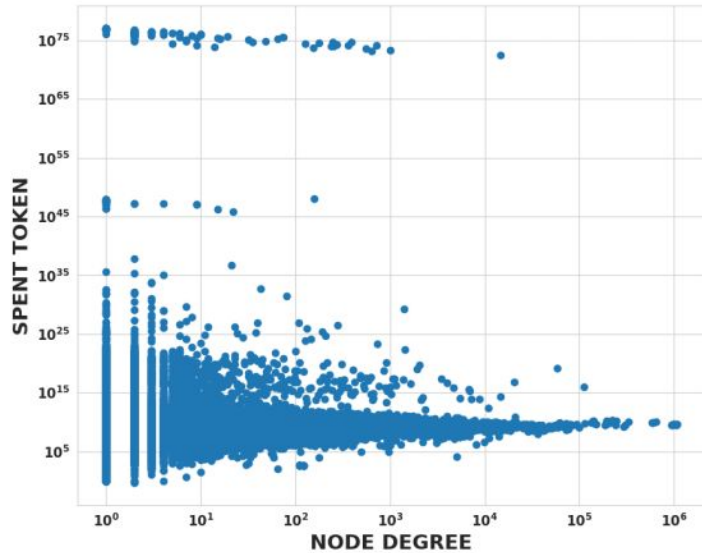
ERC-20 analysis

USDT earned



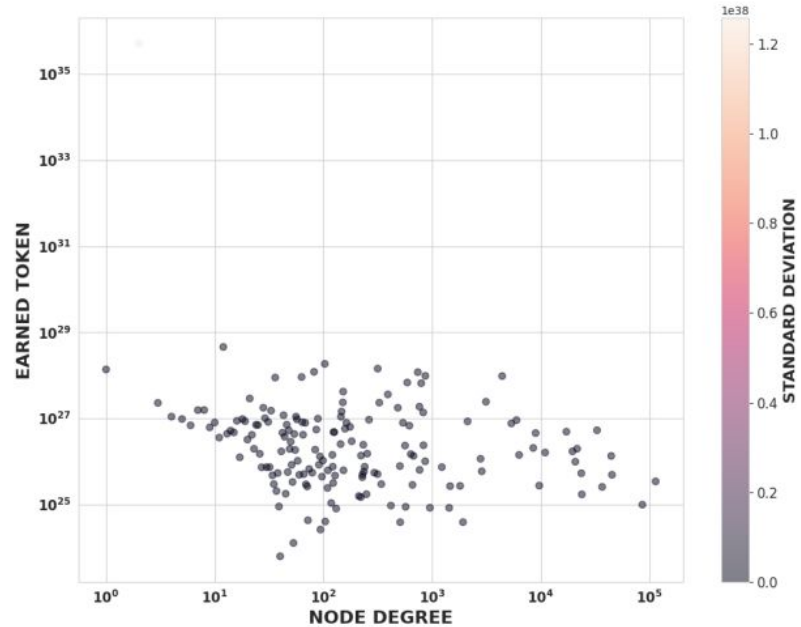
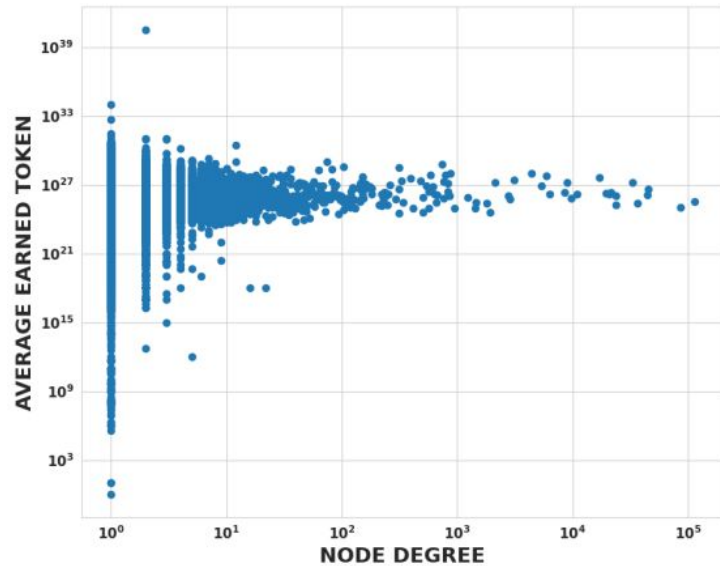
ERC-20 analysis

USDT spent



ERC-20 analysis

SHIB earned



Take home message

Huge data publicly readable and ready to be analysed.

Different layers to be read on the same data.

Mining the data, not just for consensus!



