A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Authors :-
Sarah Meiklejohn
Grant Jordan
Damon McCoy
Stefan Savage
Marjori Pomarole
Kirill Levchenko
Geoffrey M. Voelker

Introduction

-> Online virtual currency

-> Cryptographic protection and P2P protocol

-> Anonymity, Scalable, irrevocable

-> Law-enforcement w.r.t. bitcoin

In This Paper

-> Flow of bitcoin, Use of bitcoin, Extent of Traceability

-> Based on Availability Bitcoin block chain

-> Labeling and clustering public keys

Background

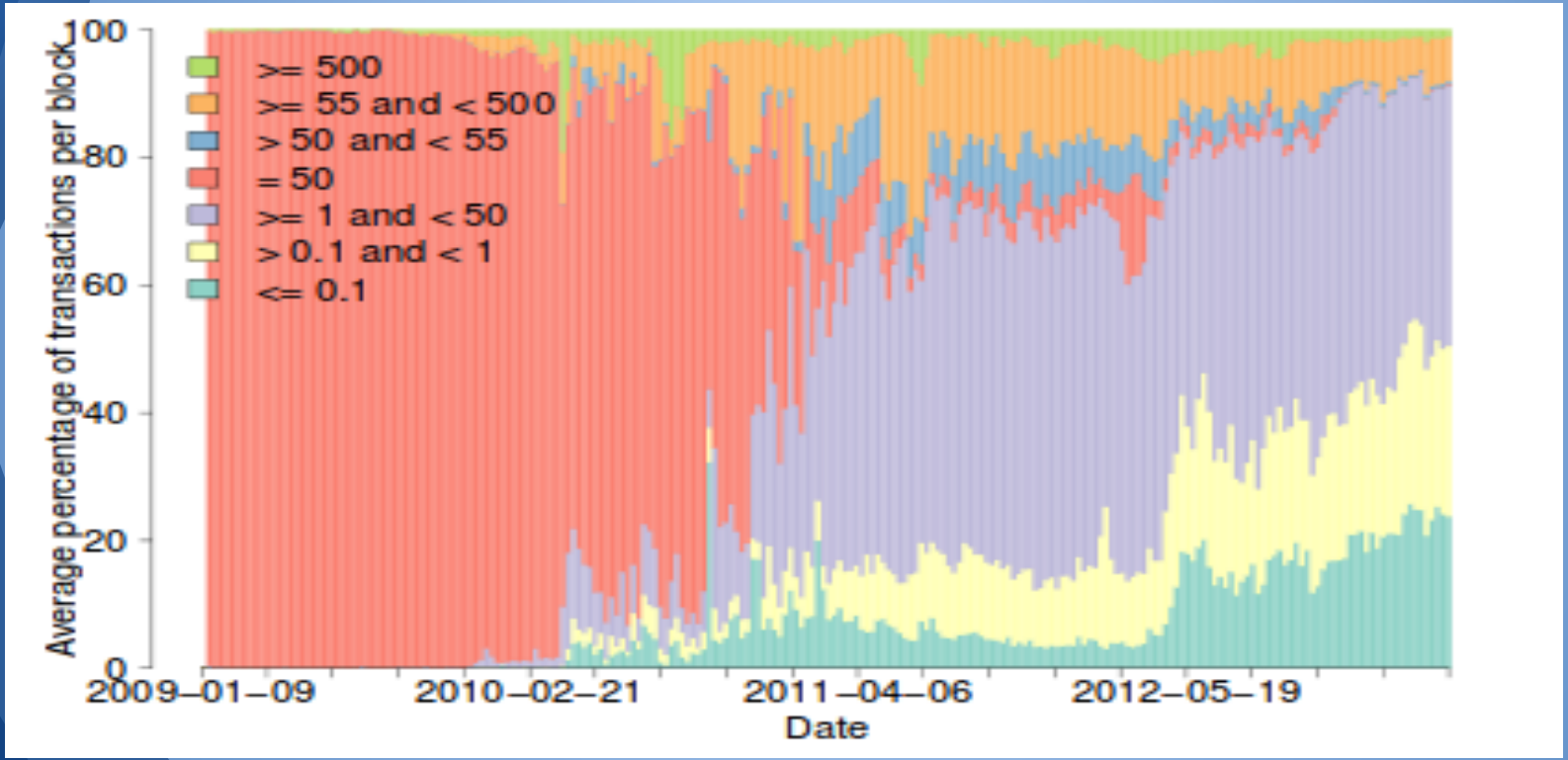
Bitcoin Protocol

-> Owners are identified by a public key(eg PK_a , PK_b)

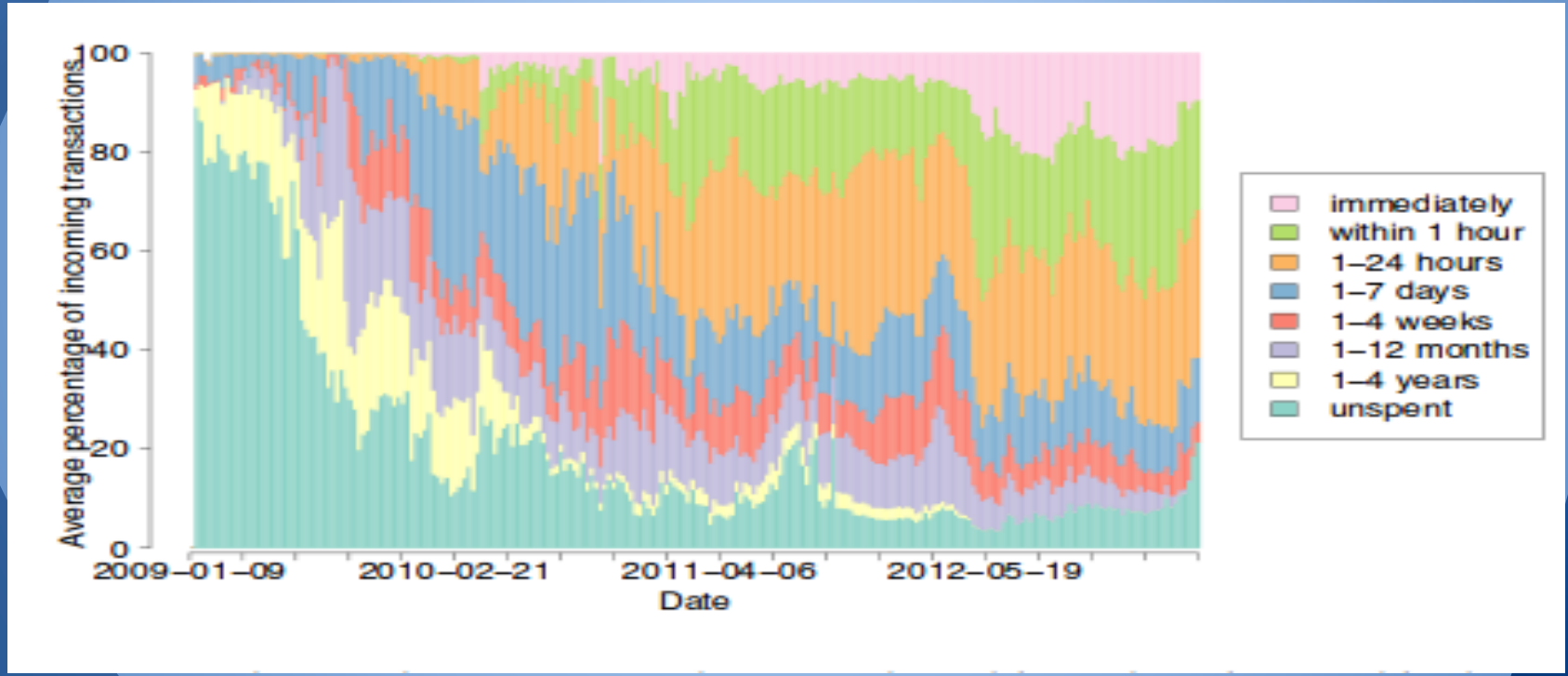
-> Sign SHA256[(received bitcoins transaction, PK_b)] using SK_a

-> blocks and block chain (double spending)

Transaction Trend with respect to amount (value)



Bitcoin spent trend with respect to time



Data Collection

Own Transactions

-> 344 transactions with different services
Mining, Wallets, Exchanges(Mt Gox), Vendors, Gambling(Satoshi Dice), etc.

Other Transaction Sources

-> blockchain.info/tags

-> Collected 5000 tags

Account Clustering Heuristics

-> Address control and account ownership

-> Transaction graph and public key graph

-> Heuristic-1 and Heuristic-2

-> The Impact of change address

-> Refining Heuristic-2

Transaction Graph - G: (V,E)

V: set of transaction $\{t_1, t_2, t_3, .., t_n\}$

E: set of directed edges $\{e_1, e_2, .., e_m\}$

$e_x = (t_1, t_2)$ => output of t_1 is used in input of t_2

In degree: $d^+_{tx}(t)$: the number of inputs for the transaction

Out degree: $d^-_{tx}(t)$: the number of outputs for the transaction

Public key Graph - G: (V,E)

V: set of public keys $\{pk_1, pk_2, pk_3, .., pk_n\}$

E: set of directed edges $\{e_1, e_2, .., e_m\}$

$e_x = (pk_1, pk_2)$ => flow of money from pk_1 to pk_2

In count: $d^+_{addr}(pk)$: # pk has been output in a transaction

Out count: $d^-_{addr}(pk)$: # pk has been input in a transaction

Heuristic-1

If two(or more) addresses are inputs to the same transaction, they are controlled by the same user.

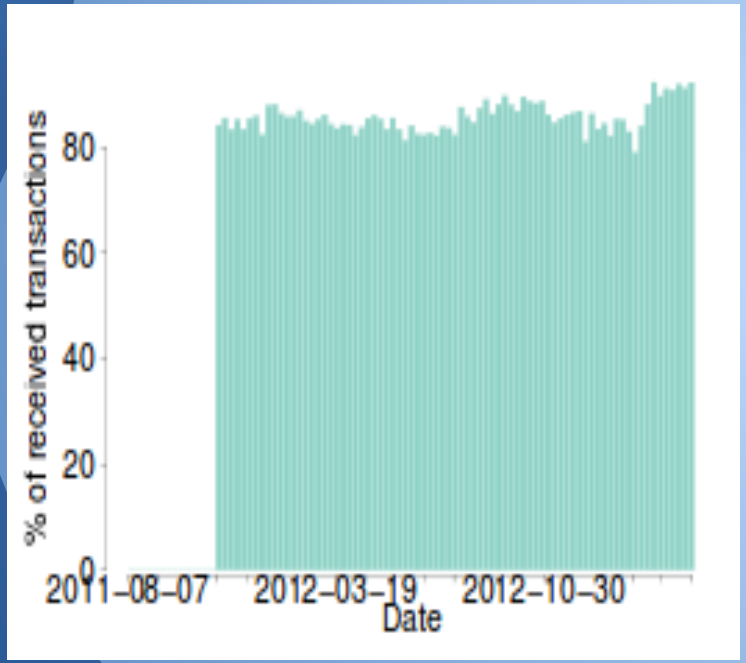
Heuristic-2

The one time change address is controlled by the same user as the input addresses.

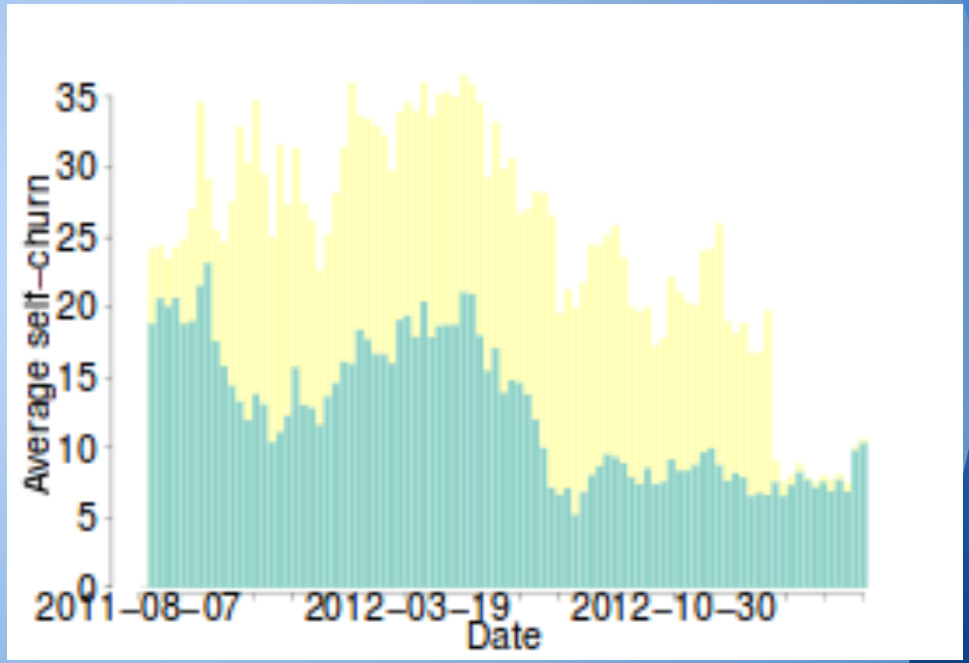
what is change address?

what is one time change address?

Impact of change addresses

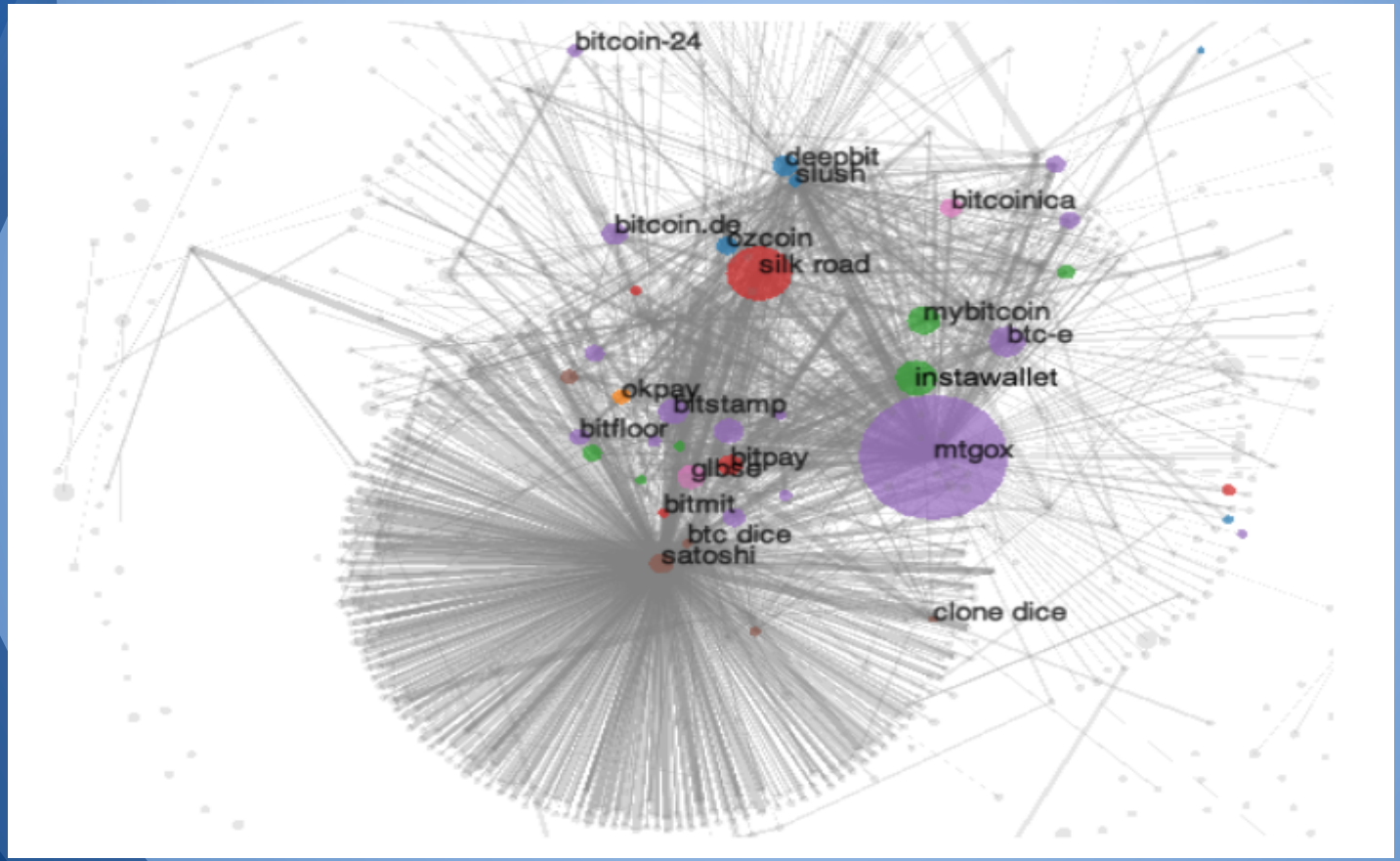


Deepbit

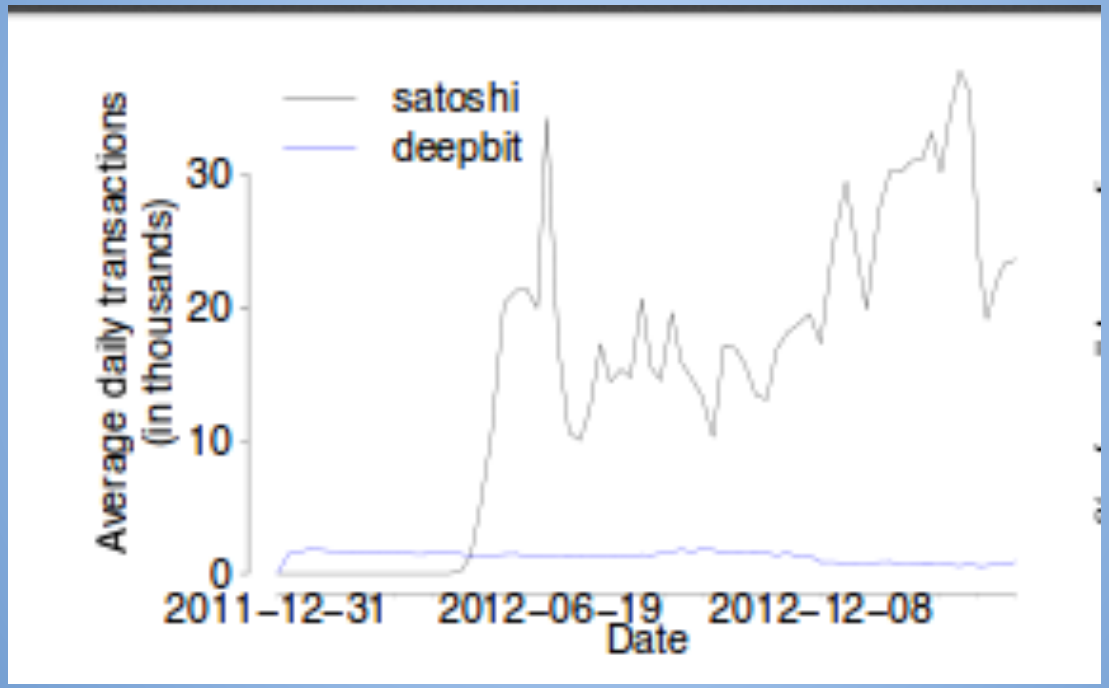


Mt Gox

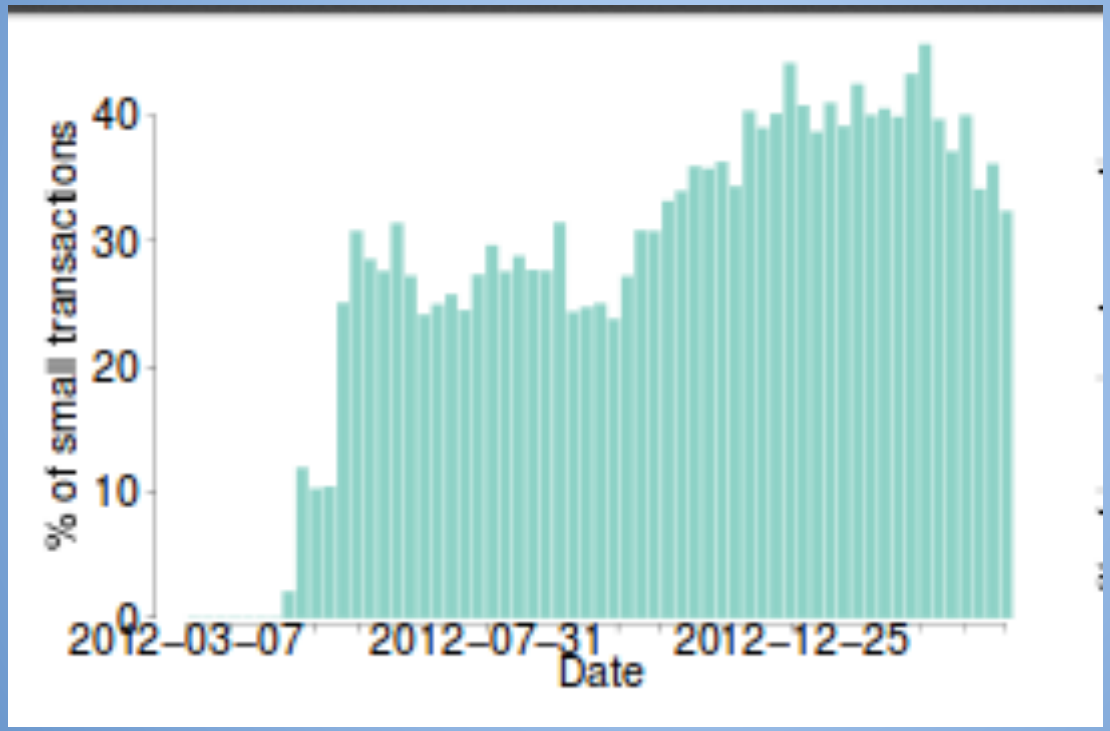
User Network visualization



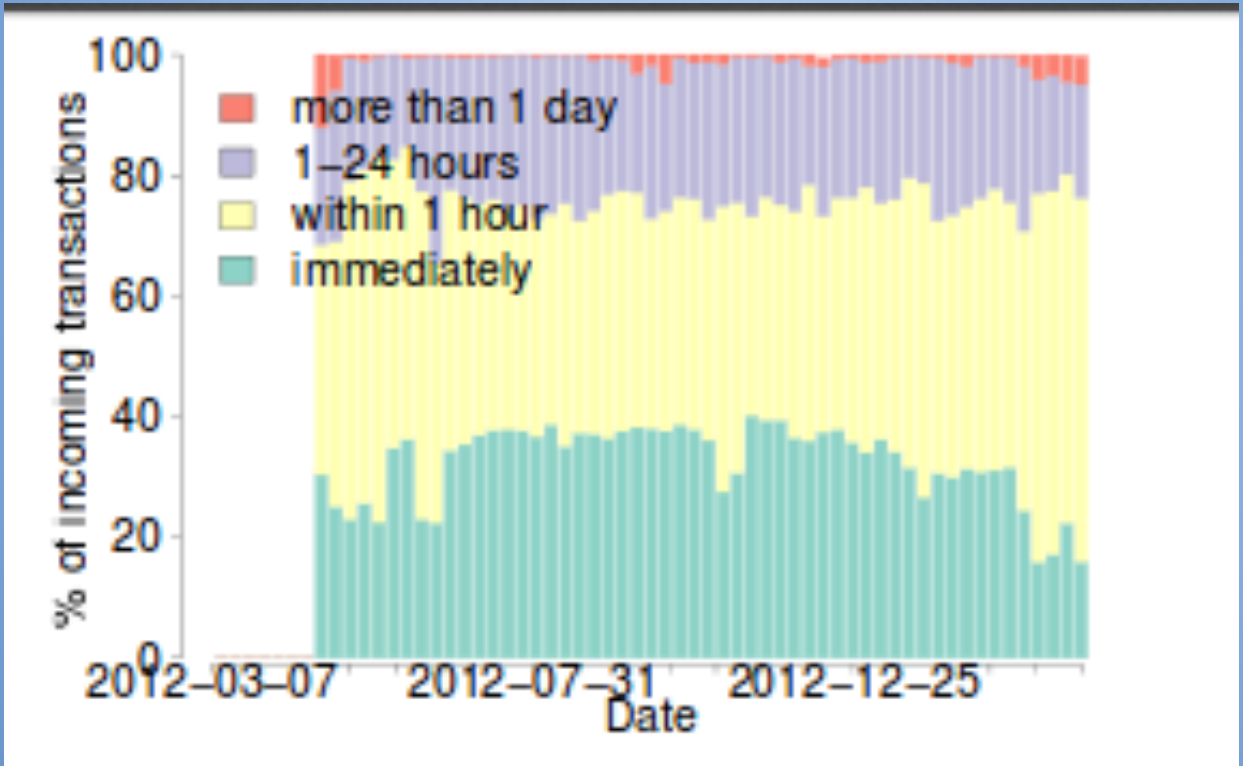
Effect of popular services (Satoshi Dice)



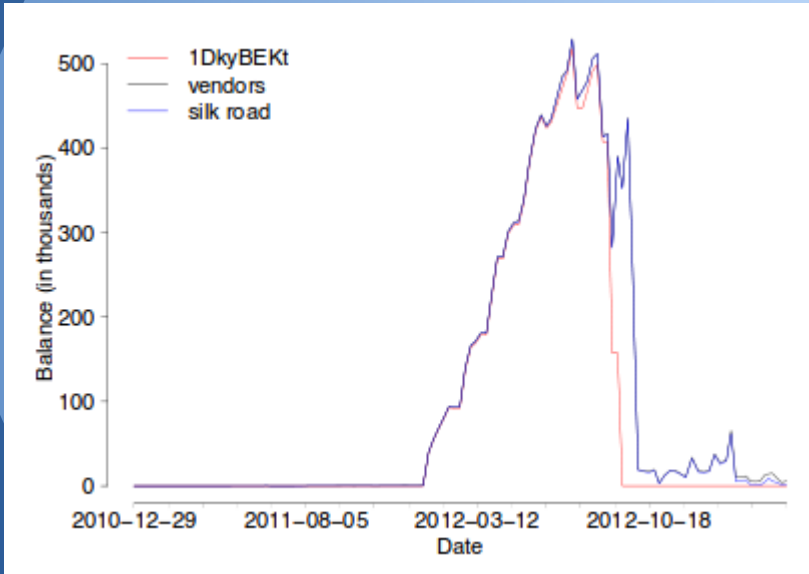
Satoshi Dice



Satoshi Dice



Tracking id: 1DkyBEKt



	First		Second		Third	
Service	Peels	BTC	Peels	BTC	Peels	BTC
Bitcoin-24			1	2	3	124
Bitcoin Central					2	2
Bitcoin.de					1	4
Bitmarket					1	1
Bitstamp			5	97	1	1
BTC-e					1	250
CA VirtEx	1	3	1	10	3	22
Mercado Bitcoin					1	9
Mt. Gox	11	492	14	70	5	35
OKPay	2	151			1	125
Instawallet	7	39	5	135	2	43
WalletBit	1	1				
Bitzino					2	1
Seals with Clubs	1	8				
Coinabul			1	29		
Medsforbitcoin	3	10				
Silk Road	4	28			5	102

Tracking Theft

A: Aggregations

S: Split

F: Folding

P: Pealing

Theft	BTC	Date	Movement	Exchanges?
MyBitcoin	4019	Jun 2011	A/P/S	Yes
Linode	46,648	Mar 2012	A/P/F	Yes
Betcoin	3171	Mar 2012	F/A/P	Yes
Bitcoinica	18,547	May 2012	P/A	Yes
Bitcoinica	40,000	Jul 2012	P/A/S	Yes
Bitfloor	24,078	Sep 2012	P/A/P	Yes
Trojan	3257	Oct 2012	F/A	No

Conclusion

-> Developed clustering heuristics and Analysed the currency flow

-> Analysing the gap between actual and potential anonymity

Thanks...