THE GRAPH STRUCTURE OF BITCOIN

Damiano Di Francesco Maesa[1], Andrea Marino[2],
Laura Ricci[2]

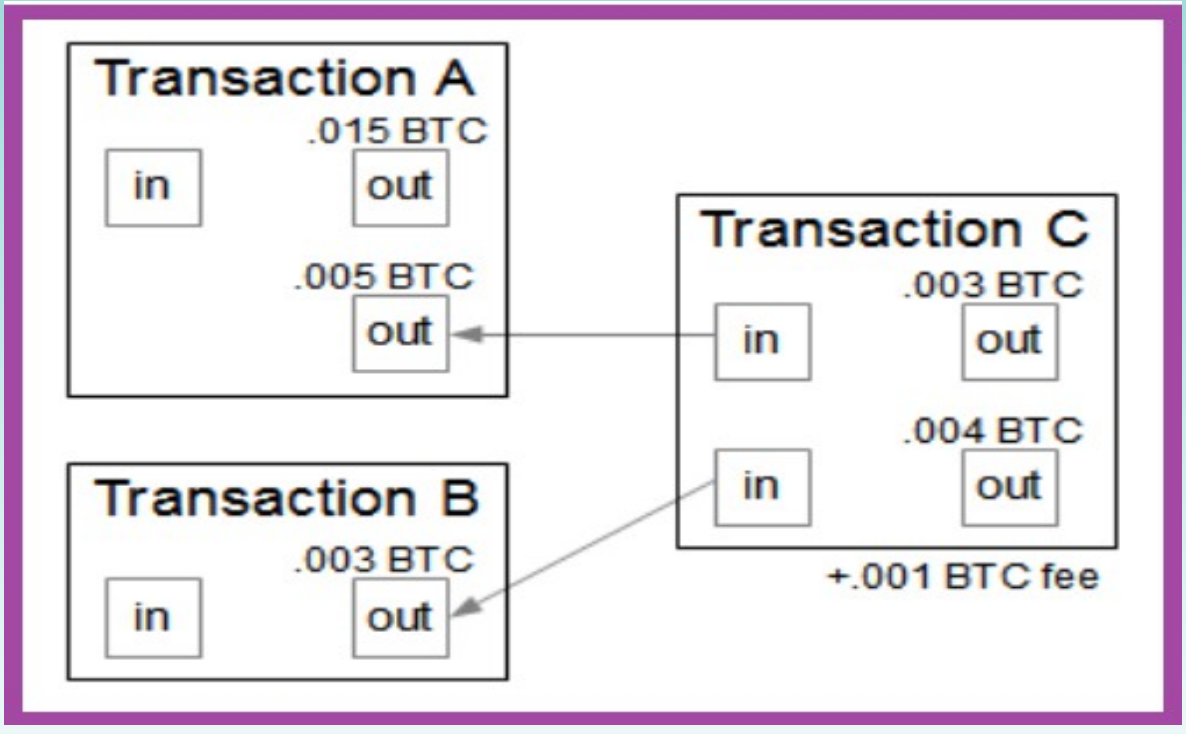
[1]Dep .of Computer Science and Technology, University of Cambridge
[2]Dep. of Computer Science, University of Pisa

DLT 2019: 2nd Distributed Ledger Technology Workshop
Pisa – February 2019

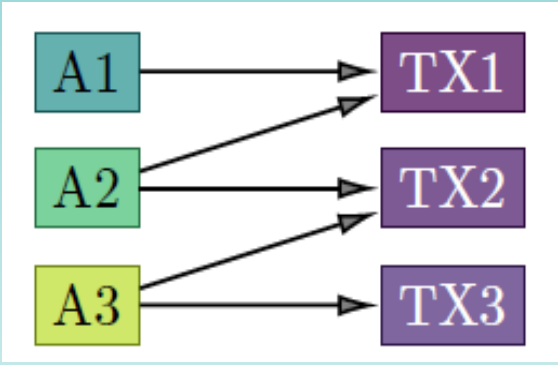
OVERVIEW

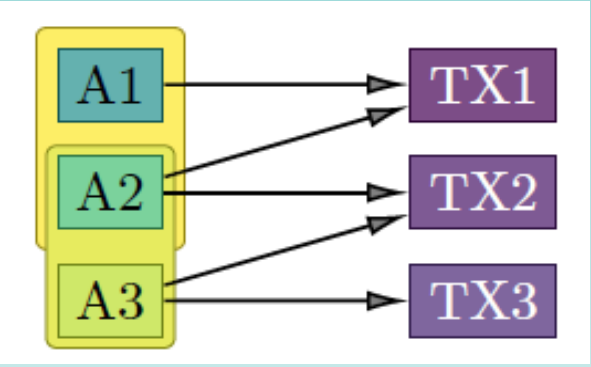
- main goals of our work:
  - analyze the bow tie graph structure, originally attributed to the Web, in the case of the Bitcoin users graph.
  - link the connectivity structure of the Bitcoin users graph to the economical activity of its nodes.
- characteristics of the Bitcoin users graph:
  - nodes augmented with balance
  - edges
    - weighted with the Bitcoin value exchanged.
    - paired with the temporal time stamp of creation

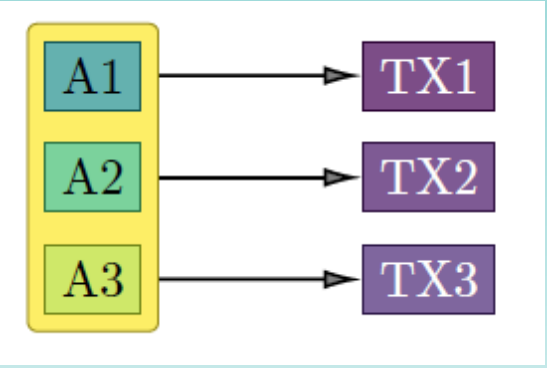
THE STRUCTURE OF BITCOIN TRANSACTIONS



THE COMMON INPUT HEURISTICS







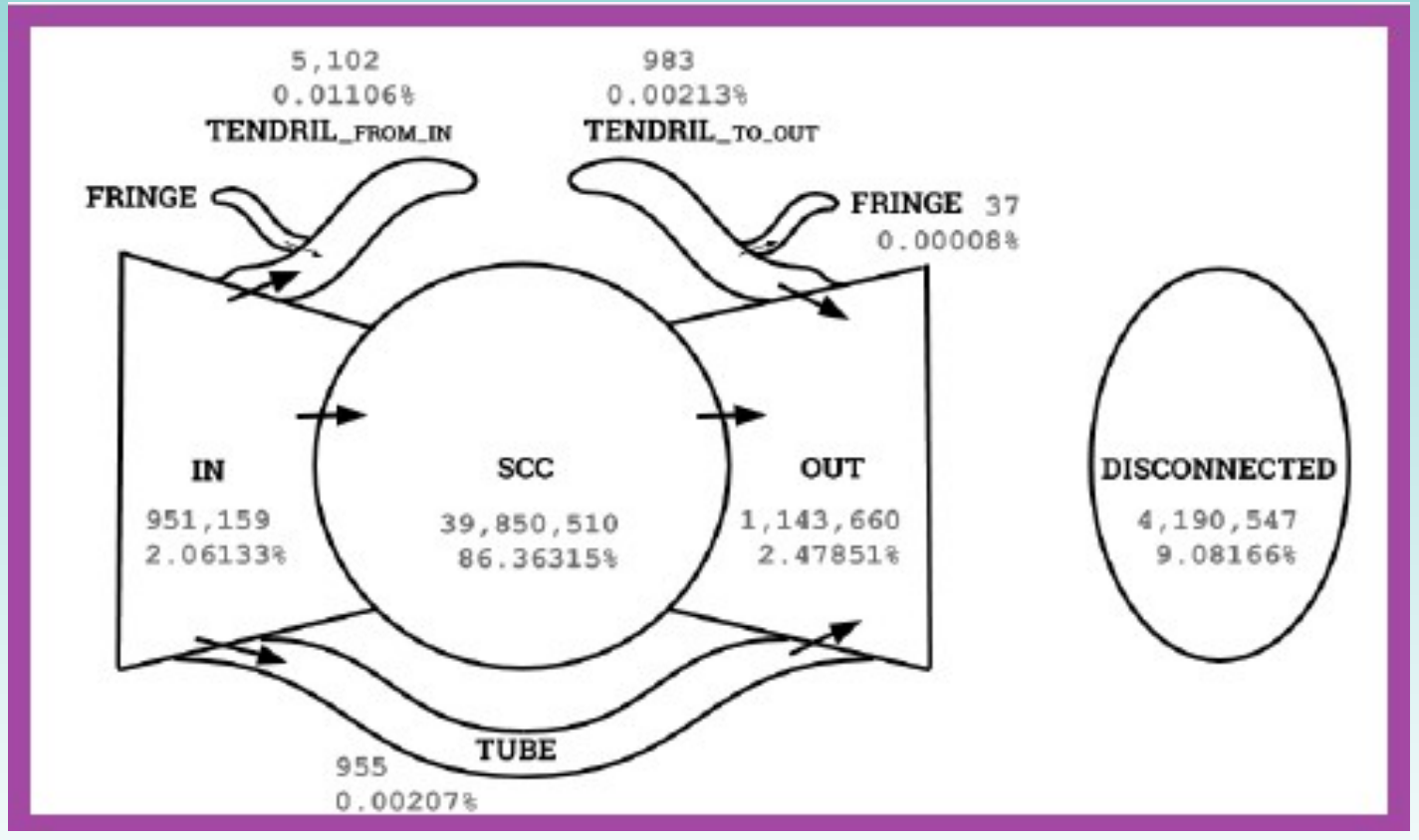
If a Bitcoin transaction spends unspent transaction outputs belonging to different addresses

- common input heuristics: assume that the issuer of the transaction is the owner of all of the associated addresses
- trasform the address graph into the users graph

THE USERS GRAPH

- Clustering algorithm
  - builds a graph G where an edge exists between the 2 addresses A1 and A2 if and only if they appear as input of the same transaction
  - find the connected components of G
  - linear complexity
- Users graph
  - nodes are cluster
  - an arc from cluster C1 to C2 exists whether there exists a transaction from an address of C1 to an address of C2.

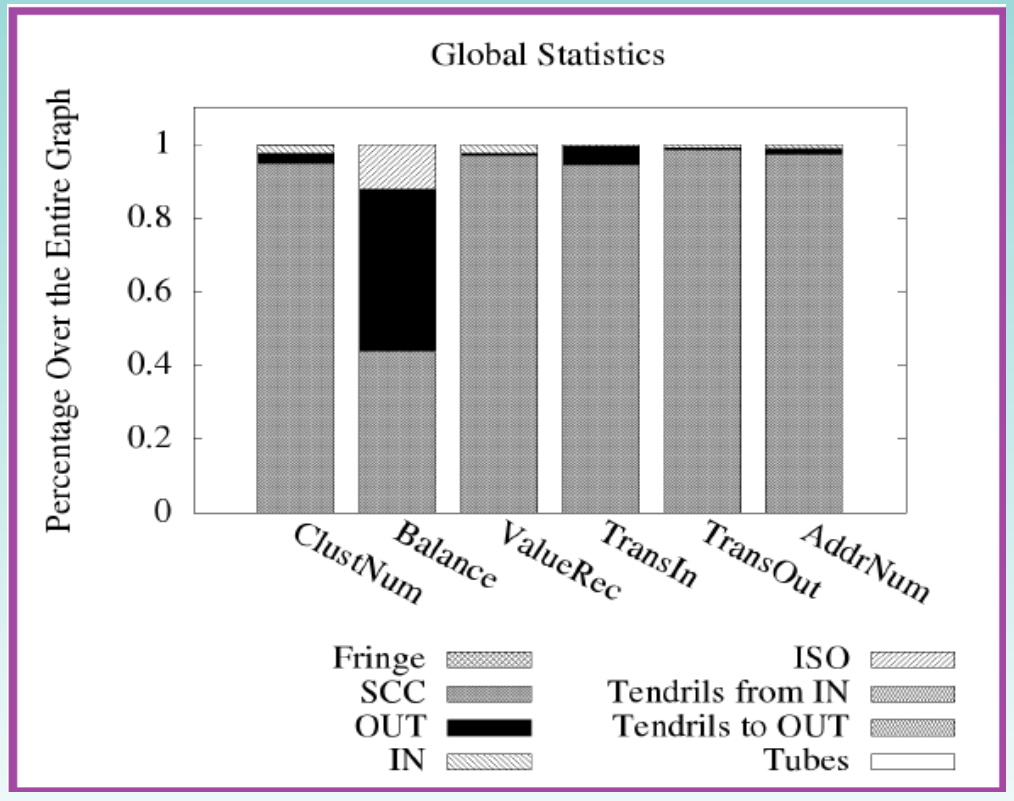
THE BOW TIE STRUCTURE OF THE USERS GRAPH



ECONOMICAL INTERPRETATION OF THE GRAPH

- our goal:
  - linking the bow tie structure to the economical activity of the nodes
- metrics used to characterize the components of the bow tie
  - AddrNum: number of addresses in a cluster.
  - Balance
  - ValueRec: sum of the payment received
  - TransIn: number of payments received (including coinbase)
  - TransOut: number of payments done

ECONOMICAL INTERPRETATION OF THE GRAPH

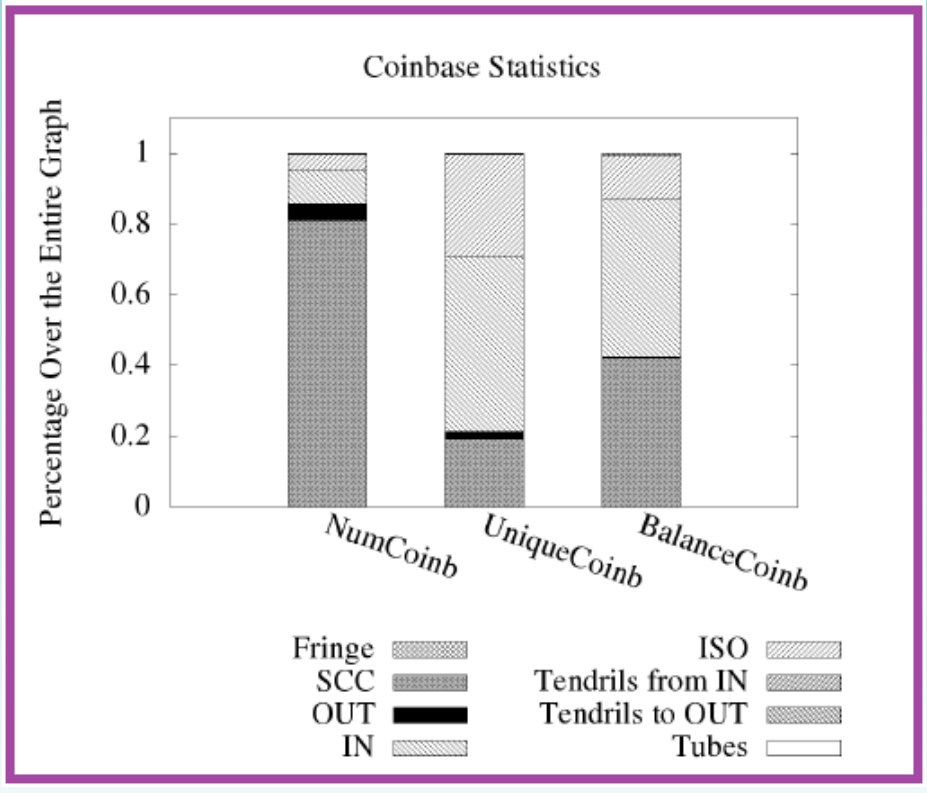


- In the SCC
  - a sensibly large number of addresses
  - dominates all metrics, but not current balance
  - high discrepancy between the current balance and total value received by clusters
  - large part of the balance credited to clusters in OUT
- SCC contains the really active clusters of the economy.

COINBASE TRANSACTIONS

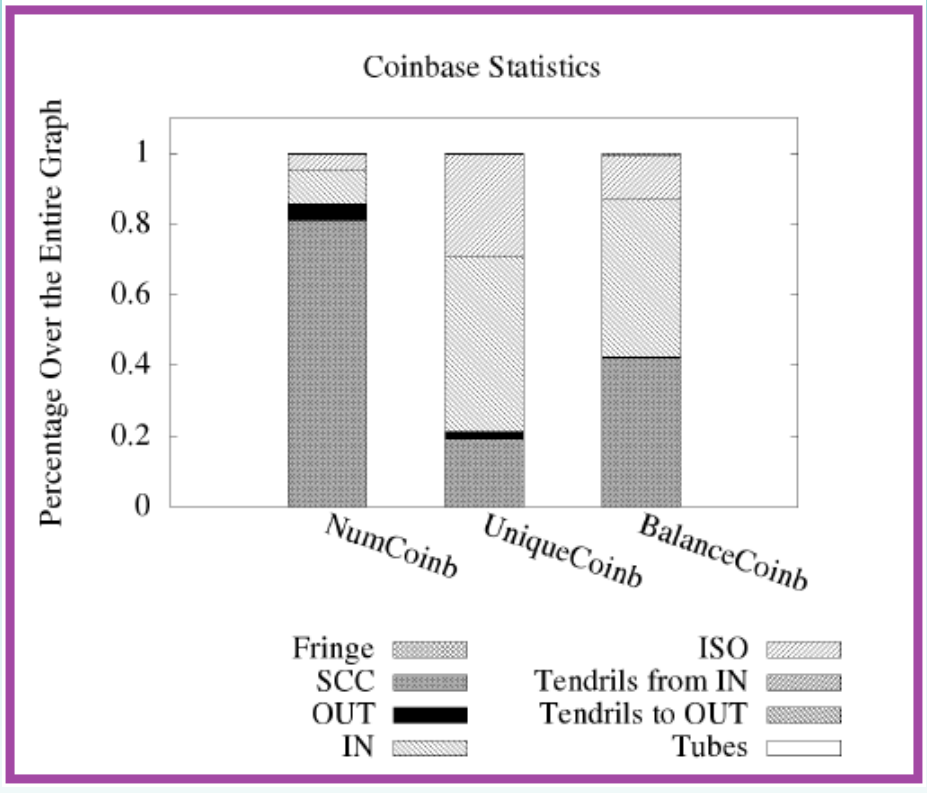
- the Proof of Work requires an important computational effort
- the resources dedicated to PoW are expensive
  - an incentive mechanism is defined to reward miners
- a reward is collected by the miner finding a block
  - sum of all fees of the transactions contained in the block, plus a fixed amount
  - reward is credited to the miner through a special coinbase transaction
- miners can be located in the bow tie through the analysis of the coinbases.

ANALYSIS OF THE COINBASE TRANSACTIONS



- NumCoinbase
  - number of payments received from coinbase transactions,
- UniqueCoinBase
  - number of clusters that received at least one payment from a coinbase transaction
- BalanceCoinBase
  - total value received from coinbase transactions,

ANALYSIS OF THE COINBASE TRANSACTIONS

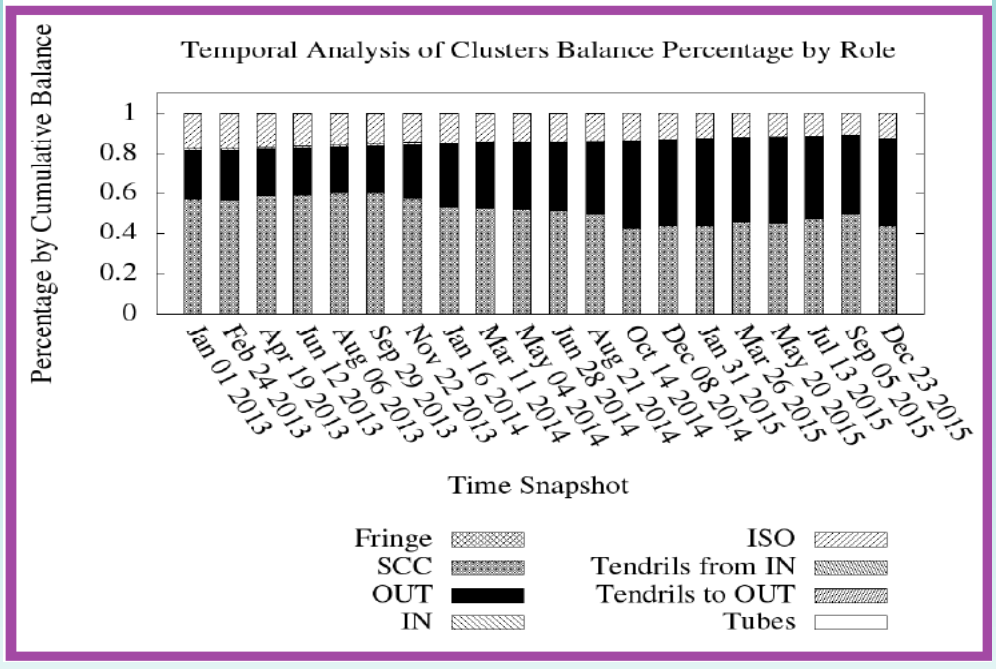


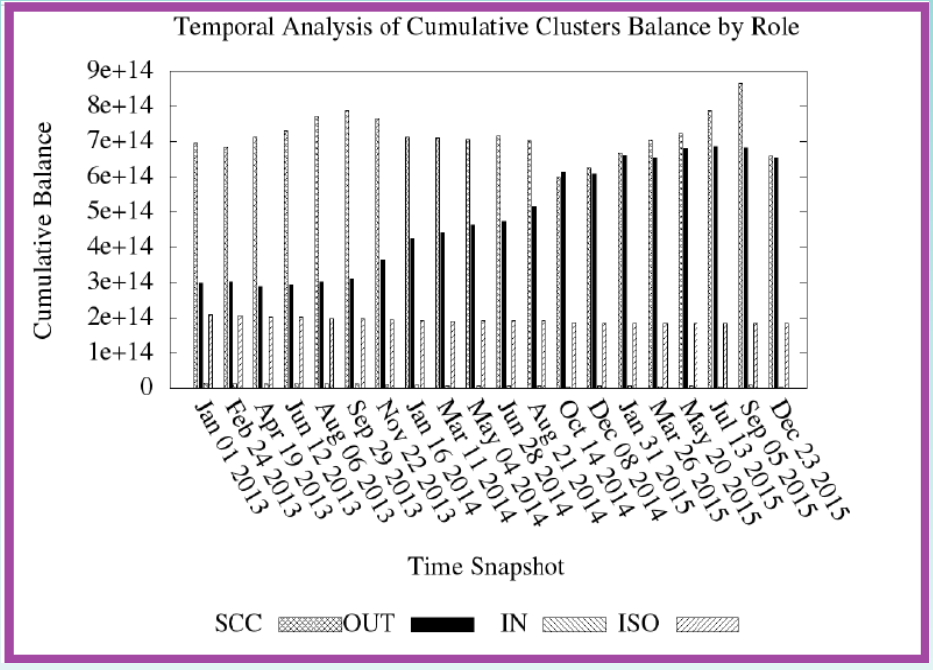
- clusters that have received at least one coinbase transaction mainly belong to IN
- IN nodes
  - corresponds mainly to miners
  - obtain new bitcoin as mining rewards
  - spend them inside the "SCC economy"

TEMPORAL ANALYSIS OF THE BOW TIE

- studying the evolution of the bow tie components
  - the blockchain includes the entire history of the Bitcoin system
- divide the timespan of our dataset in 20 temporal snapshots
  - all equal in duration (2 months) except the first one.
  - from january 2013 to december 2015
- older graph is a subgraph of a newer one, but nodes may change their roles in the bow tie

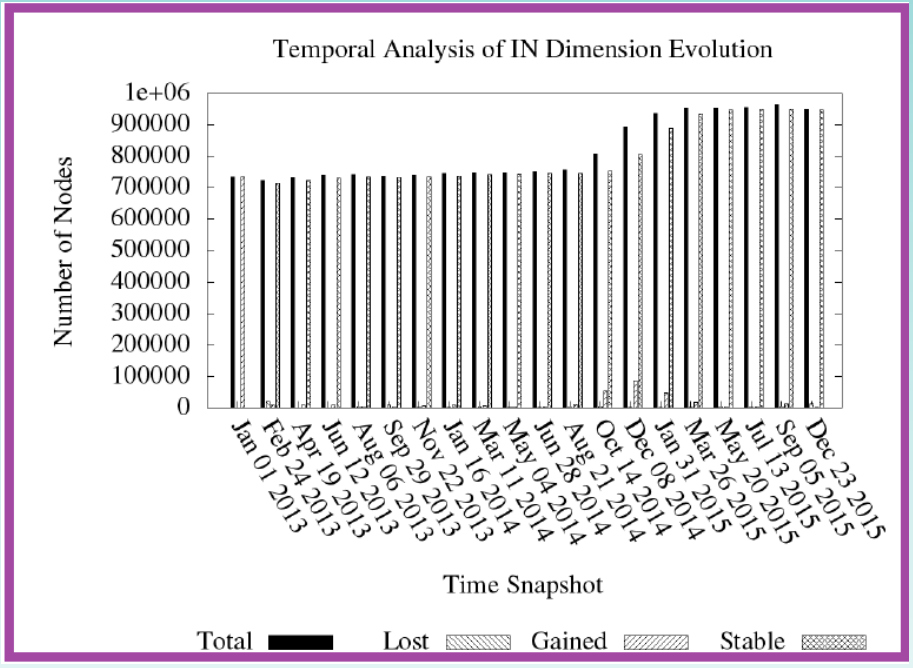
TEMPORAL ANALYSIS OF CLUSTER BALANCE

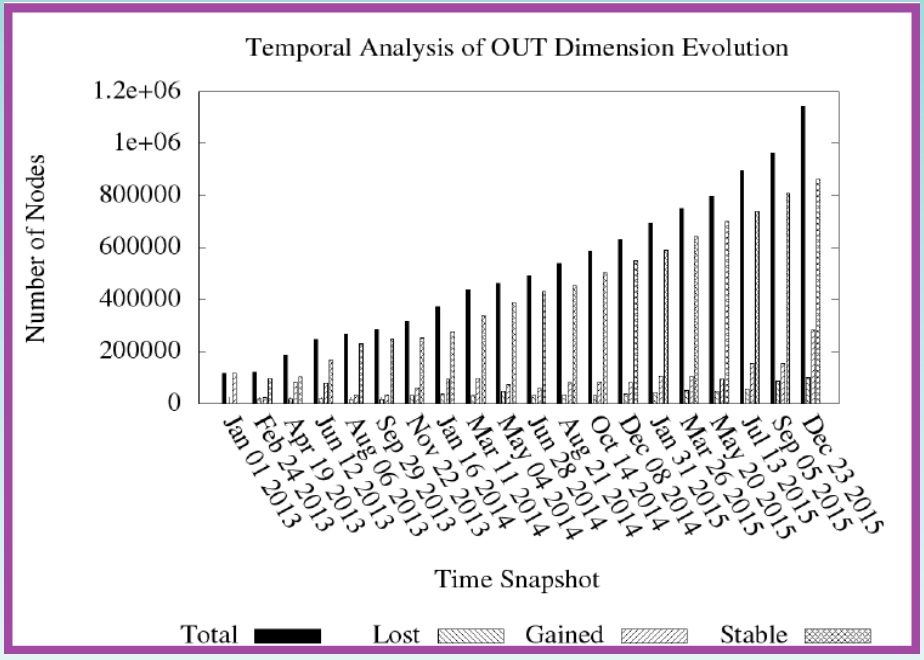




- cumulative current balance of the SCC component remains stable
- cumulative current balance of OUT increases over time.

EVALUATION OF THE TEMPORAL STABILITY





- IN is temporally stable and a few nodes leave this component
- OUT continuously grows over time: the number of nodes that join is higher than the non negligible number of nodes that leaves.

CONCLUSIONS

- most economical exchanges performed by clusters in SCC.
- current balance mostly contained in OUT.
  - current balance of the SCC remains somewhat stable, while the cumulative current balance of OUT increases over time.
- more and more value actually passes and is used by the nodes in the SCC, but is temporary stored in the OUT component
  - values in OUT: currently unspent outputs/ cold storage
- most miners contained in IN and these miners receive higher rewards with respect to those in SCC

FUTURE WORKS

- more sophisticated deanonymization techniques to discover the economical meaning of the nodes in the bow tie.
- perform the same analysis for the graph obtained from the Ethereum blockchain
  - comparing the economies of the two cryptocurrencies.