AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EFMD EQUIS ACCREDITED

Evolution of the Bitcoin Address Graph An Exploratory Longitudinal Study

Erwin Filtz[1], Axel Polleres[1], Roman Karl[2], Bernhard Haslhofer[2]

[1]Vienna University of Economics and Business

[2]Austrian Institute of Technology

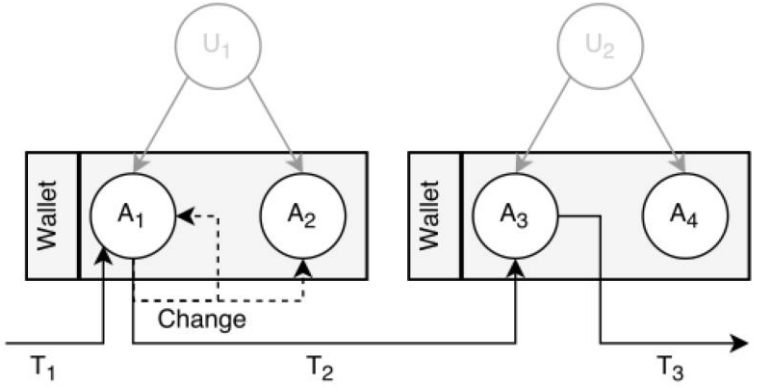
IDSC 2017, Salzburg, Austria

Bitcoin

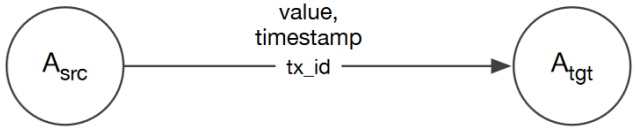
- Decentralized, unregulated currency
- Based on cryptographic technologies → „cryptocurrency“
- All transactions are available in a public ledger called blockchain
- Longitudinal study of the Bitcoin address graph
  - January 2009 – August 2016
  - Changes in structure over time
  - Identification of real-world actors
  - Transaction behavior of users

Analyzing Bitcoin as a Graph

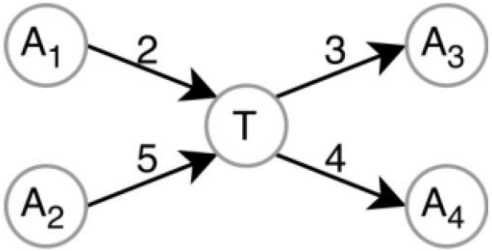
- Entities:
  - Addresses *A*,
  - Transactions *T*,
  - Users *U*



- Bitcoin address graph
  - Node: address
  - Edge: transaction
  - Nodes and edges can carry additional information
  - Monotonously growing

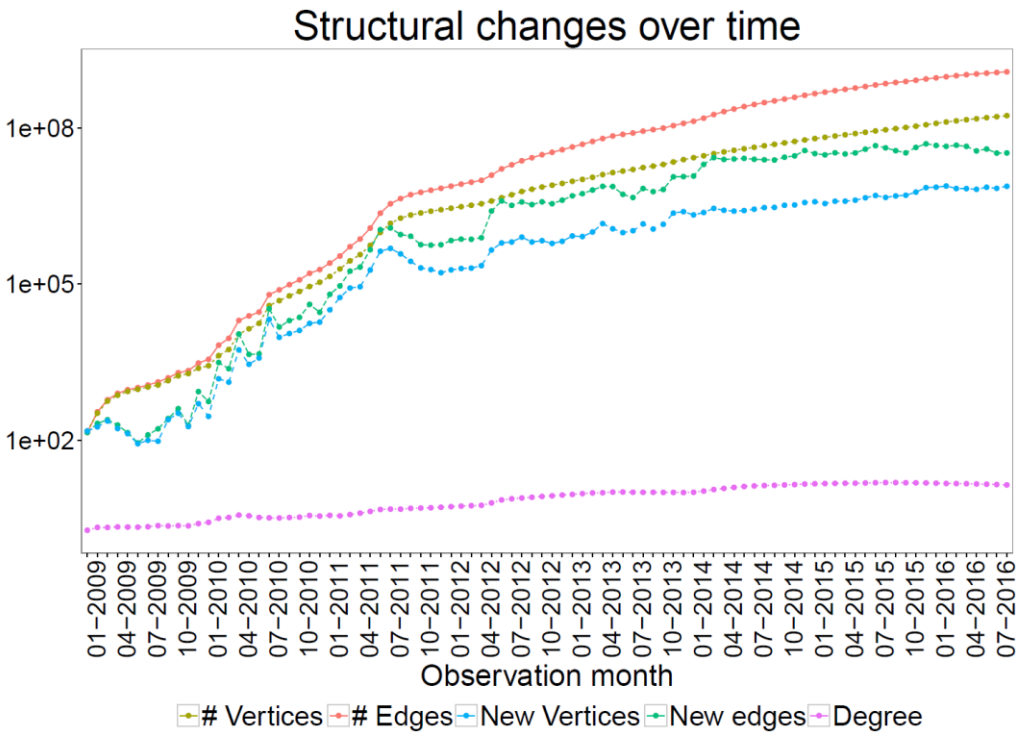


- Bitcoin flow
  - Exact allocation of flows not possible



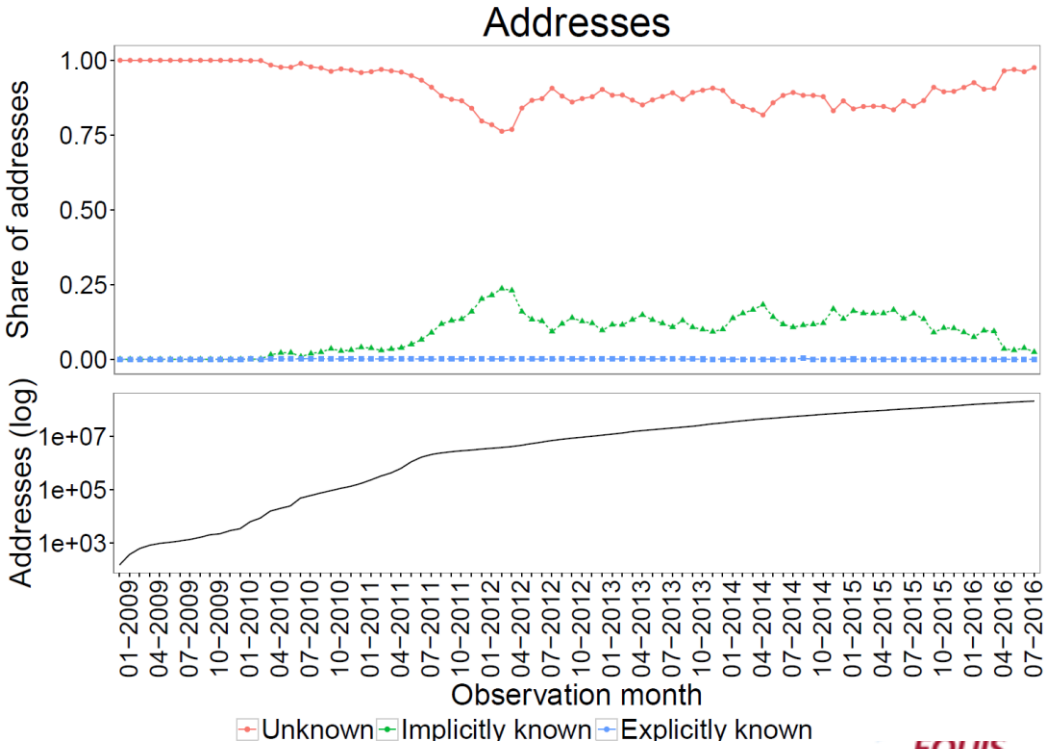
Structural analysis

- Degree distribution
  - High degree nodes are of special interest (marketplace, casino,…)
  - Majority of addresses has a low degree
- Nodes and edges
  - Cumulative number of nodes / edges
  - Users create new addresses for each transaction
  - Increased usage of Bitcoin



Real-world actors

- Transactions are anonymous by design
- User clusters based on same input heuristic
- We differentiate three user groups:
  - Unknown addresses
    No contextual information
  - Explicitly known addresses
    Additional information avbl
    extracted from the web
  - Implicitly known addresses
    appear in a cluster with
    explicitly known addresses



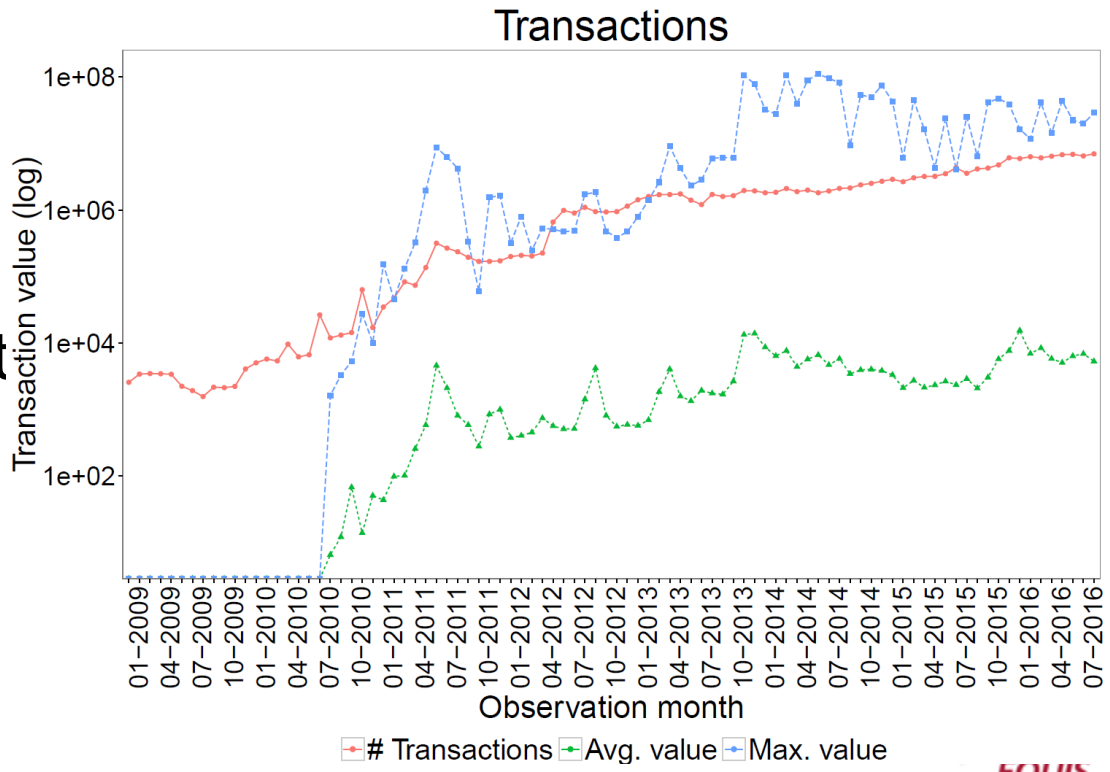
Real-world actors

- Decreasing fraction of known addresses might be caused by:
  - Newly generated addresses with no tags available
  - Increased awareness of end users to preserve anonymity
  - Increased usage of Bitcoin mixing services

- Bitcoin is designed to allow anonymous payments
- Degree of anonymity depends on the user‘s needs
  - Organizations looking for donations
  - Business model
  - Illegal activities

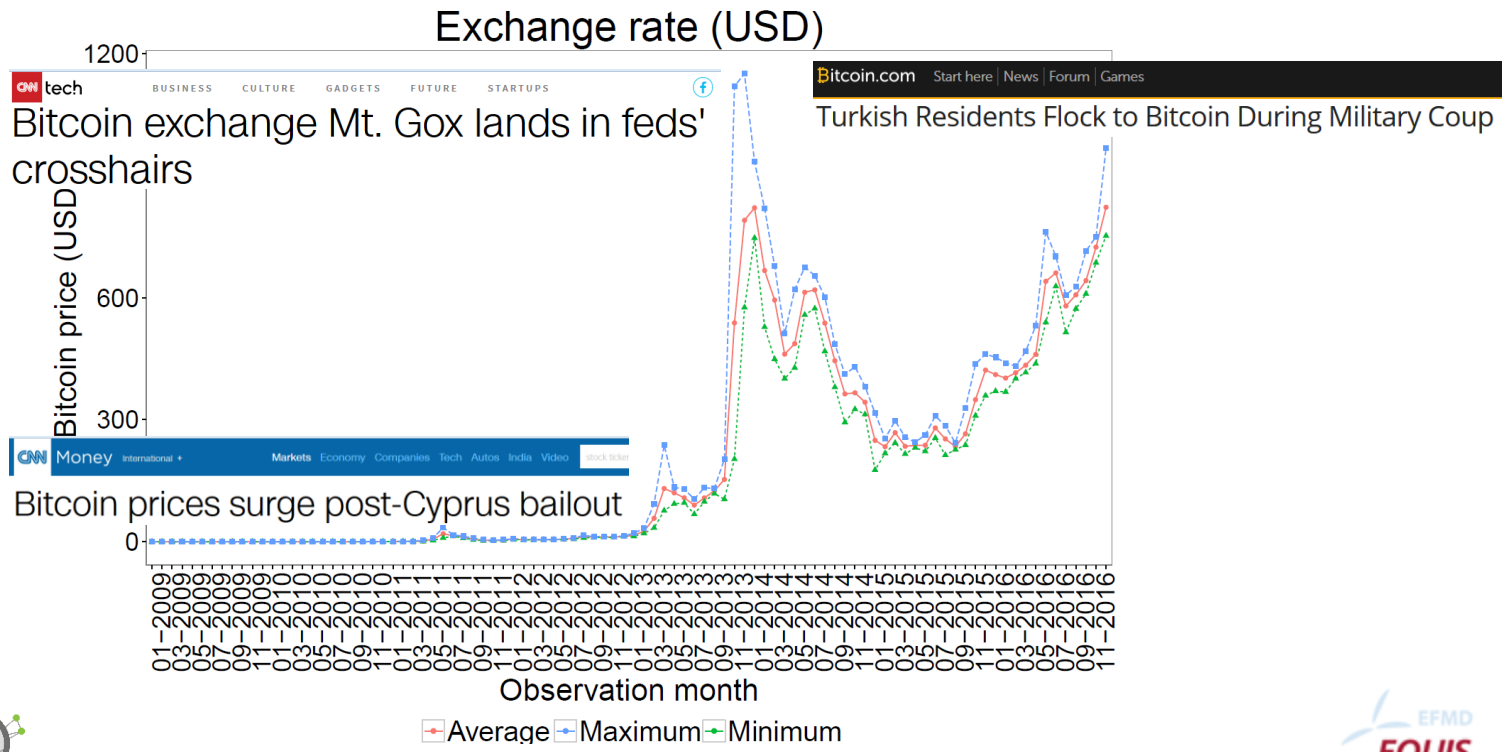
Transaction behavior

- Increasing number of transactions in the first years
- Steady for the last four years
- Reasons:
  - „new technology"
  - „Let's try it out"
  - Adopting to Bitcoin
- New vendors accept Bitcoin for payment
- Illegal activities



Exchange rate

- Exchange rate remains steady for the first years
- Influence of real world events?



Bitcoin as savings account?

- Is Bitcoin used to substitute a savings account?
- Activity period between first and last transaction on address and entity level

Metric	Address based	Entity based
Avg. used in transactions (incoming)	2.25	10.5
Avg. used in transactions (outgoing)	1.75	3.7
Avg. Activity time (days)	12	15
Median activity time (days)	< 1	< 1

Conclusion

- Bitcoin address graph shows a highly-skewed degree distribution, high degree addresses are often NPO or gaming sites
- The address graph is continuously expanding with a stable degree distribution
- Clustering techniques allow classification of users, but external information is required for deanonymization
- Real-world events have an influence on Bitcoin exchange rate

Thank you!
Questions?