BitConeView: Visualization of Flows in the Bitcoin Transaction Graph

IEEE Symposium on **Visualization for Cyber Security**

G. Di Battista[1] · V. Di Donato[1] · M. Patrignani[1]
M. Pizzonia[1] · V. Roselli[1] · R. Tamassia[2]

[1] Department of Engineering
Roma Tre University

[2] Department of Computer Science
Brown University

Outline

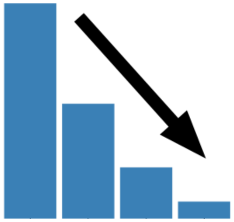
- Background on Bitcoin
- Bitcoin anonymity
- BitConeView: Requirements
- BitConeView: key concepts and metaphors
- Experiments
- Evaluation
- Conclusions and ongoing work

Background

Peer-to-peer
transactions

No need
for third parties

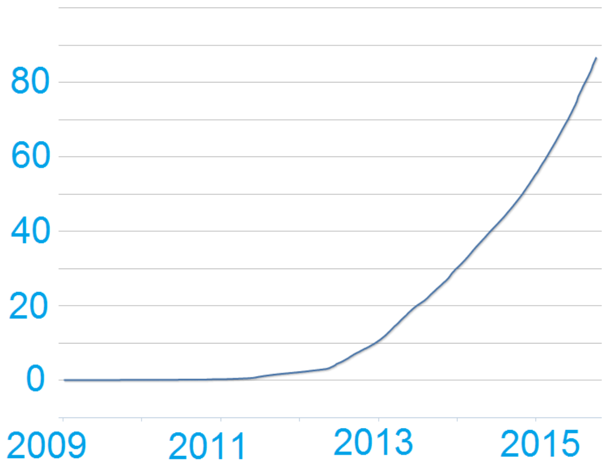
Worldwide
payments



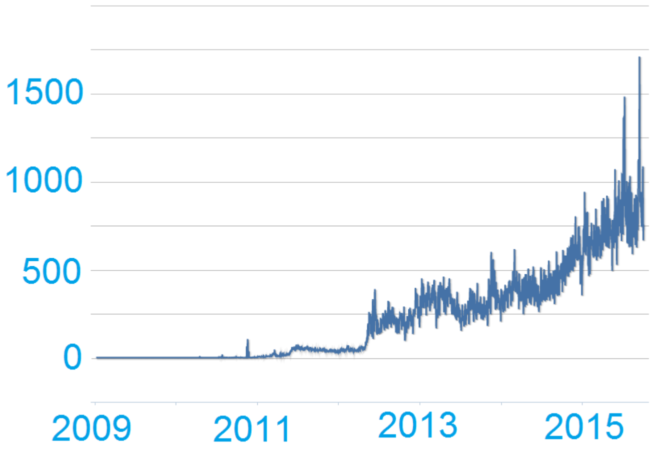
Low
processing fees

- 2008 S. Nakamoto. **Bitcoin: A peer-to-peer electronic cash system**. Whitepaper on a popular cryptography mailing list
- 2009 released the first **bitcoin software** that launched the network and the first units of the bitcoin cryptocurrency

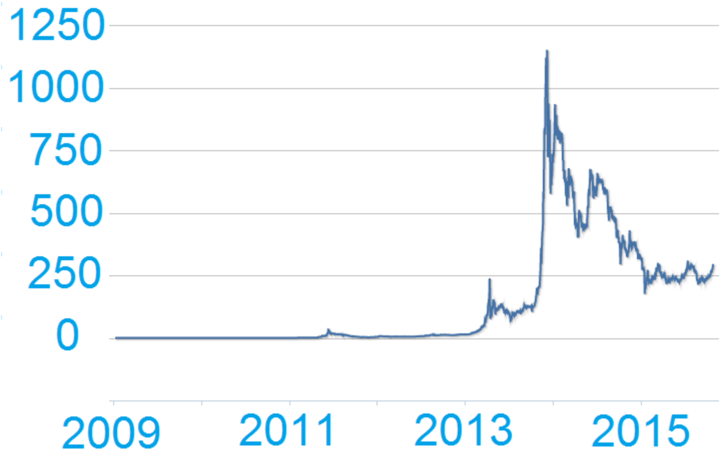
The numbers



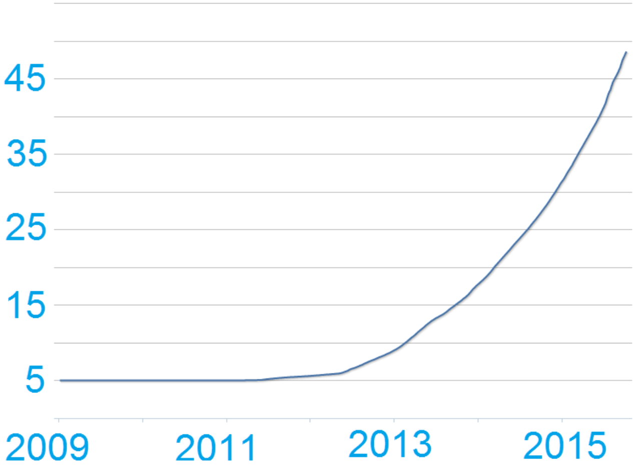
Total # Txs (M)



Avg # ~every 10 min

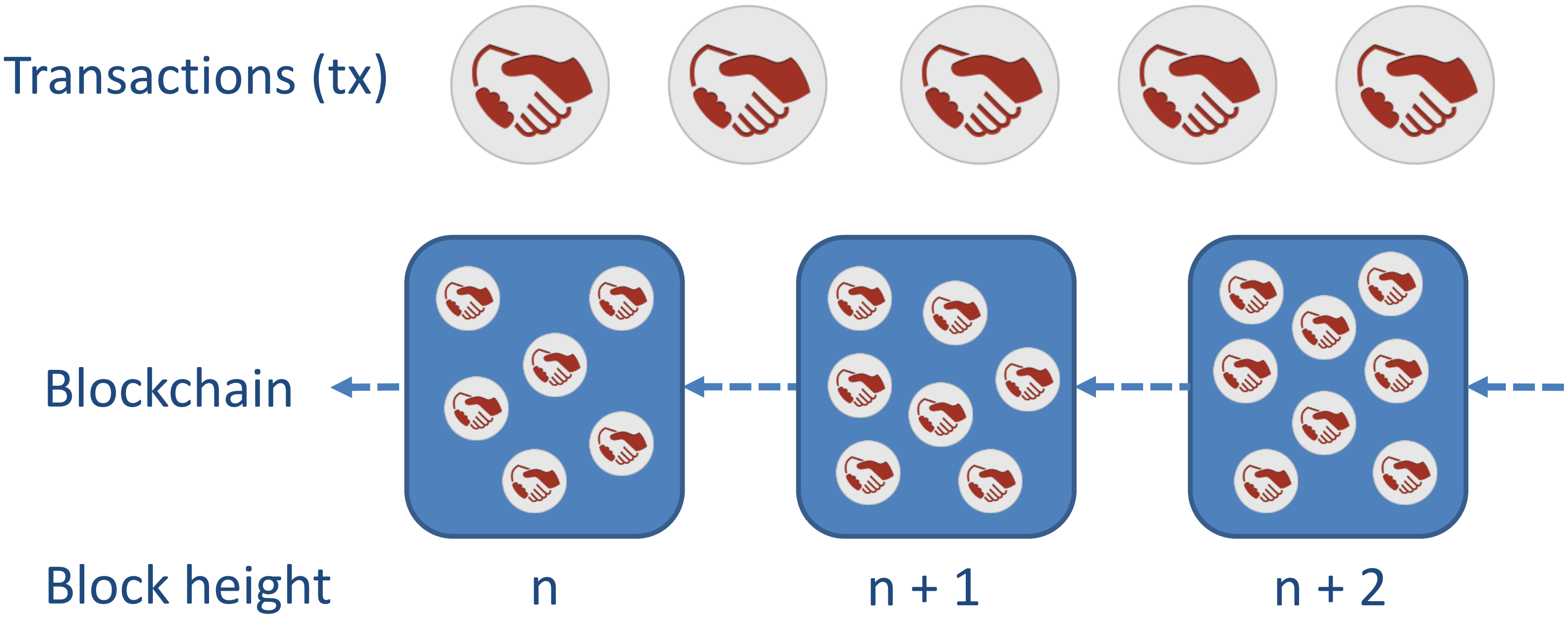


Market price (USD)



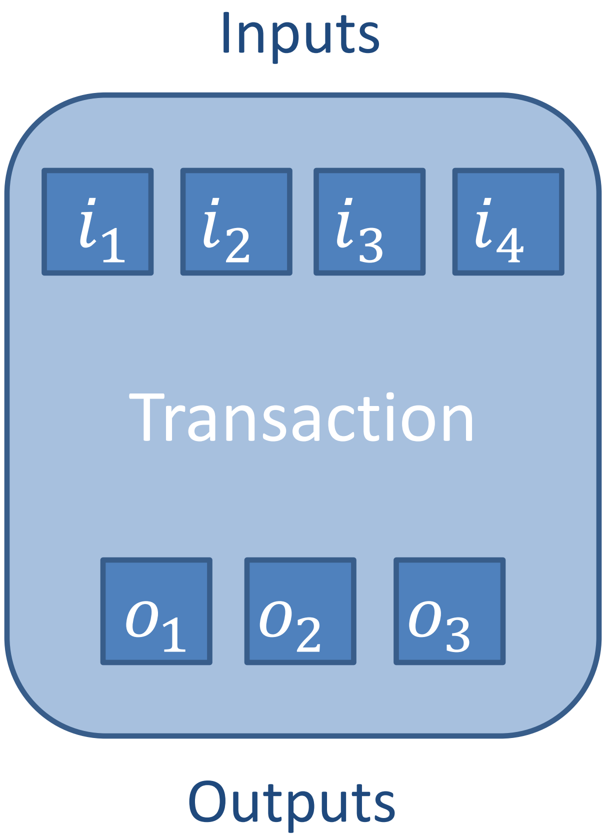
Blockchain size (GB)

Background



- Bitcoins are trasferred by means of **Transactions (Txs)**
- All transactions are recorded in a public ledger called **Blockchain**

Background



Inputs

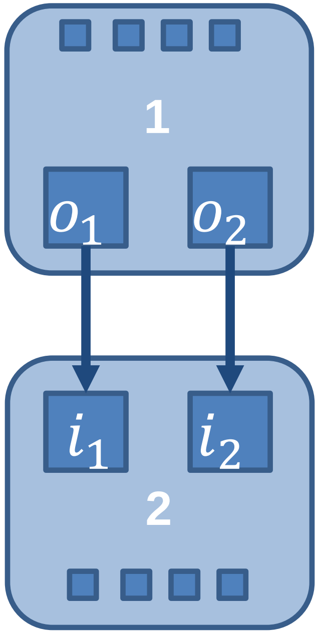
	ADDRESS	AMOUNT
i_1	1AspUk7FPS2k6dW4JEBTSyESdyfnChvrce	4 BTC
i_2	5FypDr7RP42k6dWFJEdTtrESSWfnPOha1cr	2 BTC
i_3	13K3pHeqzmzEVUVsYiFVG1tQsrwbSQoatx	3 BTC
i_4	1KoeyaqRfVcNUZD22kAahcma4GXNRbT7c	2 BTC

Outputs

	ADDRESS	AMOUNT
o_1	1KoeyaqRfVcNUZD22kAahcma4GXNRbT7c	1 BTC
o_2	1Kis3otnx9bYEHj55iRBWW5ZsvvEdJraEk	6 BTC
o_3	1KoeyaqRfVcNUZD22kAahcma4GXNRbT7c	4 BTC

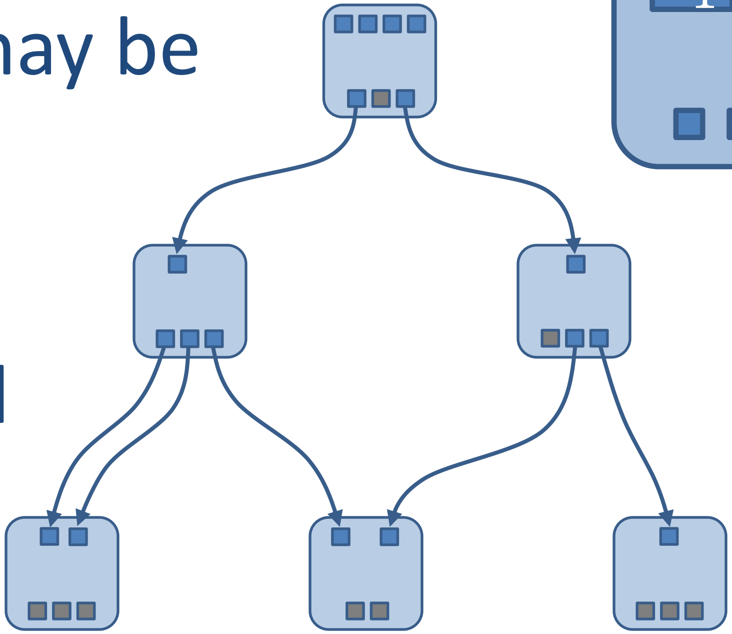
Background

- Once a tx has been processed, the only way to spend its outputs is to use them as inputs for other txs



  n.b. some outputs may be unspent (UTXOs)

- Txs define a directed acyclic multi-graph



Bitcoin anonymity

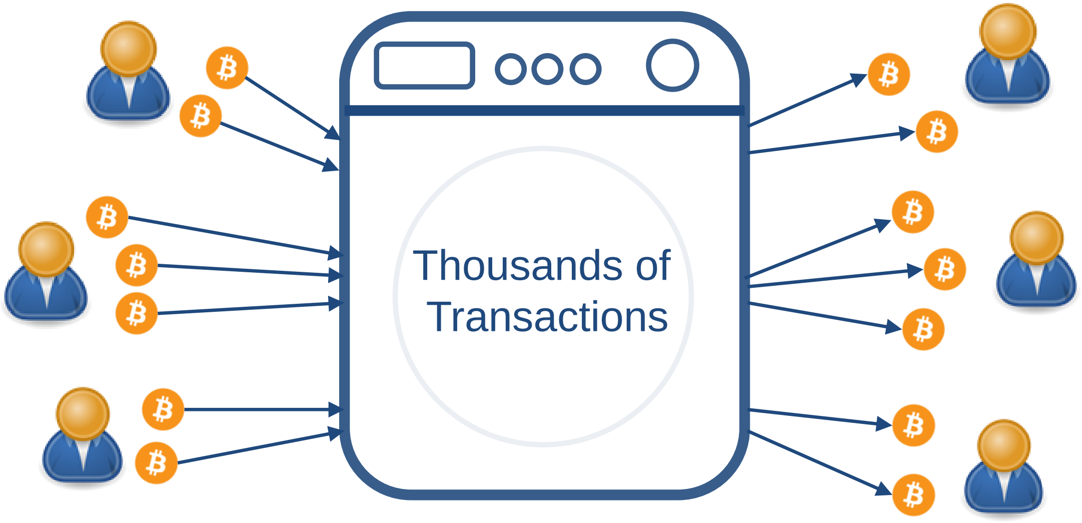
Bitcoin is not *always* anonymous

- Identity behind Bitcoin addresses is revealed
  - during a purchase for delivery purposes
  - when buying USD at exchanges

- Third parties may be able to
  - track your future transactions
  - trace your previous activity

Mixing and Laundering

- Mixing services to improve anonymity
  - BitLaundry
  - Bitcoin Fog
  - Bitcoin Mixer
  - Bitcomix
  - BitSafe
  - …



- Side effect
  - Mixing services facilitate money laundering

BitConeView: Requirements

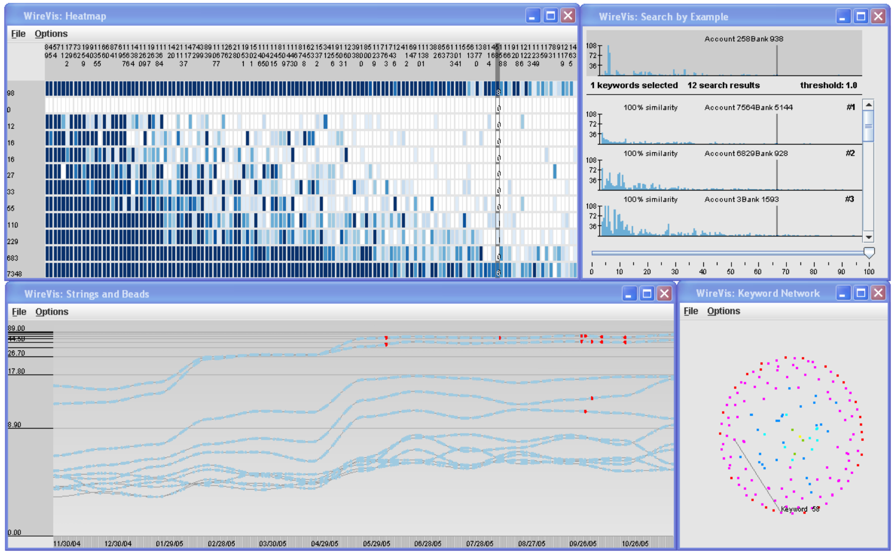
- Starting from one (or more) transaction(s)
  - Follow Bitcoins over time
  - Reveal flow patterns of interest
    - Accumulation, distribution, mixing
  - Understand when Bitcoins are mixed up
    - Understand the *degree of mixing* of Bitcoins over time
  - Evaluate effectiveness of mixing websites

State of the Art: tx-graph analysis

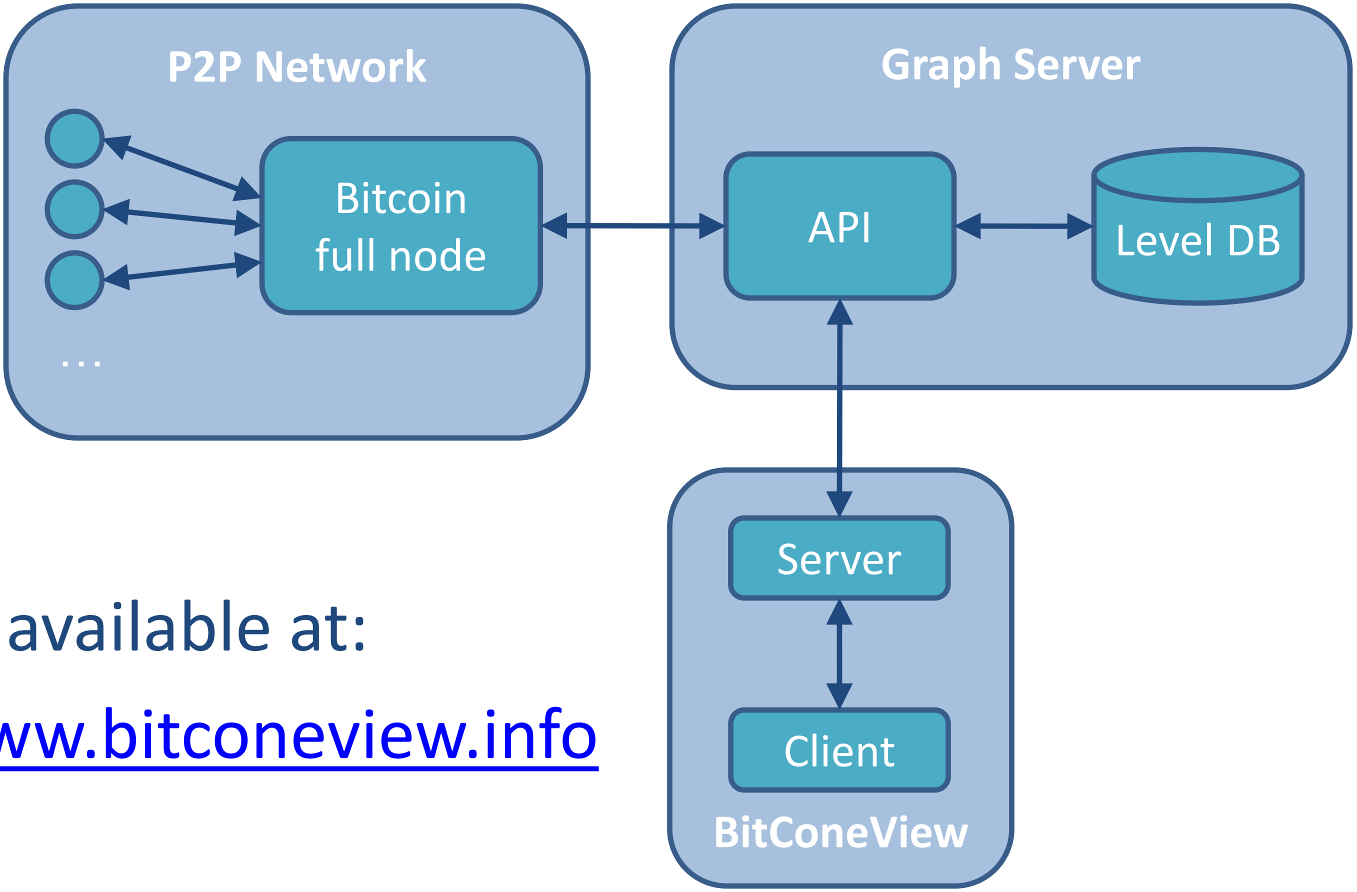
- Several papers on the analysis of the tx-graph
  - [Meiklejohn et al., 2013]
  - [Reid and Harrigan, 2013]
  - [Ron and Shamir, 2013]
- Some include drawings of subgraphs of interest
  - Laboriously created by hand or
  - Generated with standard force directed graph drawing tools that often yield to cluttered layouts

State of the Art: fraud detection

- Financial fraud detection literature
  - [Chang et al., 2007]: A visual analytics system for discovering suspicious (traditional) bank wire transactions by providing multiple coordinated visualizations



BitConeView: System Architecture and prototype

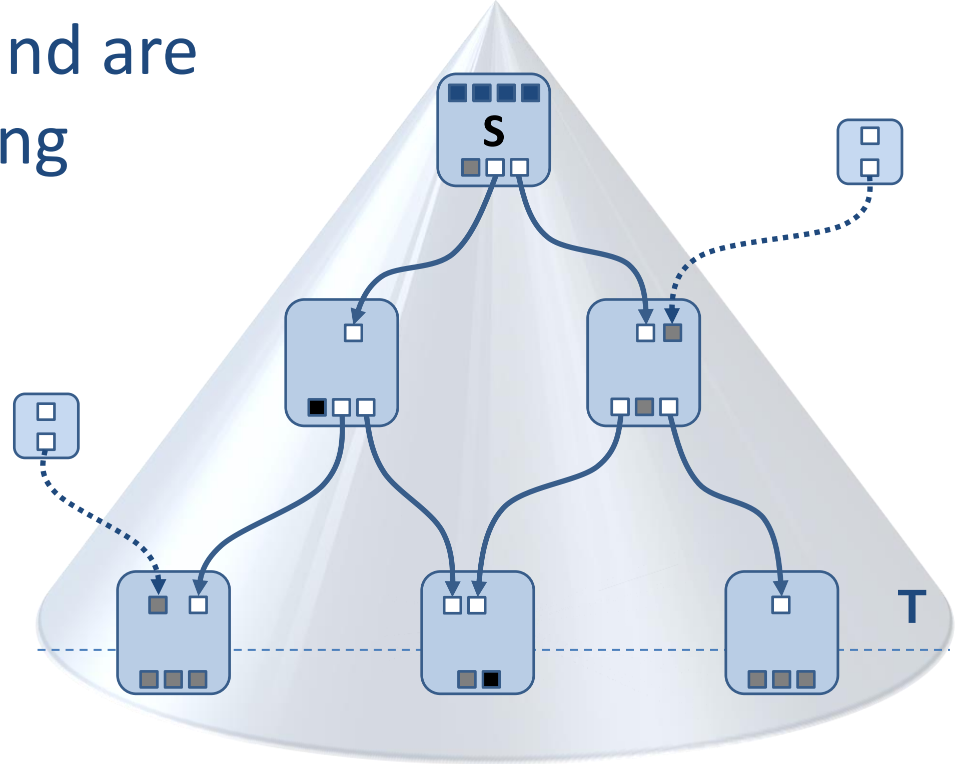


- DEMO available at:

http://www.bitconeview.info

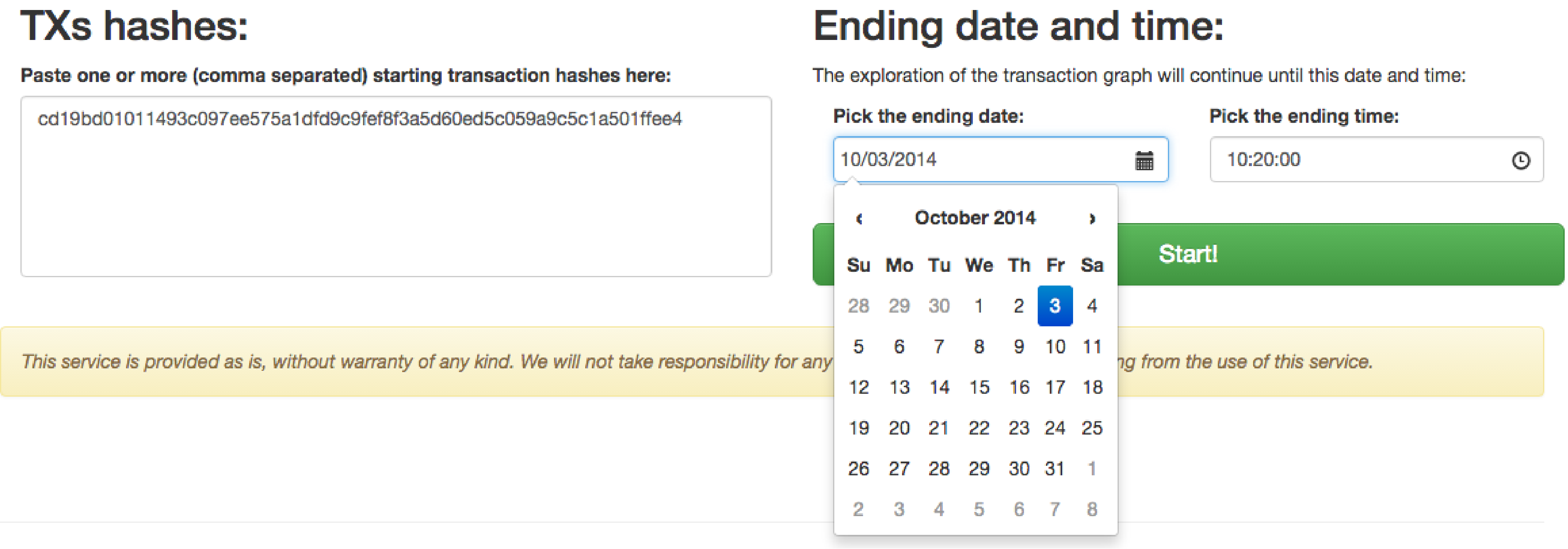
BitConeView: Some key concepts

- The *BitCone* or *cone* of a transaction **S** is the subgraph reachable from **S** within a given time limit **T**
- *Intruders* are (grey) inputs coming from outside the cone and are responsible for the mixing
- *UTXOs* may be unspent
    - at time **T** (grey)
    - at present time (black)
- Other (white) outputs are spent



BitConeView: inputs

- One starting tx **S** through its 64 digits hash
- An ending date (time limit **T**)



TXs hashes:

Paste one or more (comma separated) starting transaction hashes here:

cd19bd01011493c097ee575a1dfd9c9fef8f3a5d60ed5c059a9c5c1a501ffee4

Ending date and time:

The exploration of the transaction graph will continue until this date and time:

Pick the ending date: 10/03/2014

Pick the ending time: 10:20:00

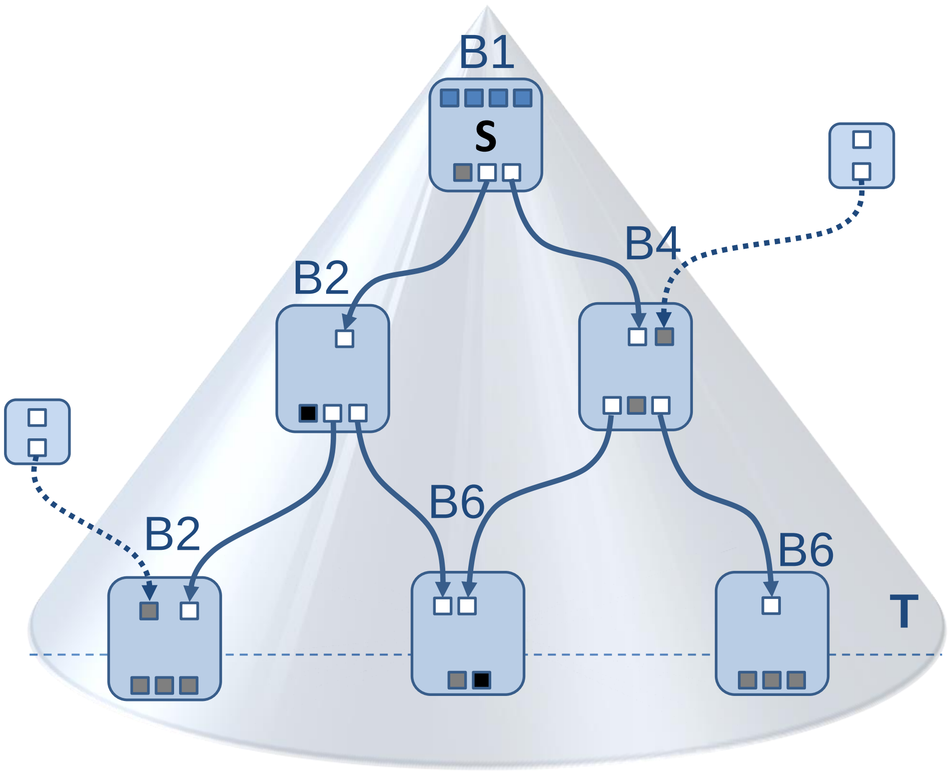
‹ October 2014 ›

Su	Mo	Tu	We	Th	Fr	Sa
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

This service is provided as is, without warranty of any kind. We will not take responsibility for any *ng from the use of this service.*

BitConeView

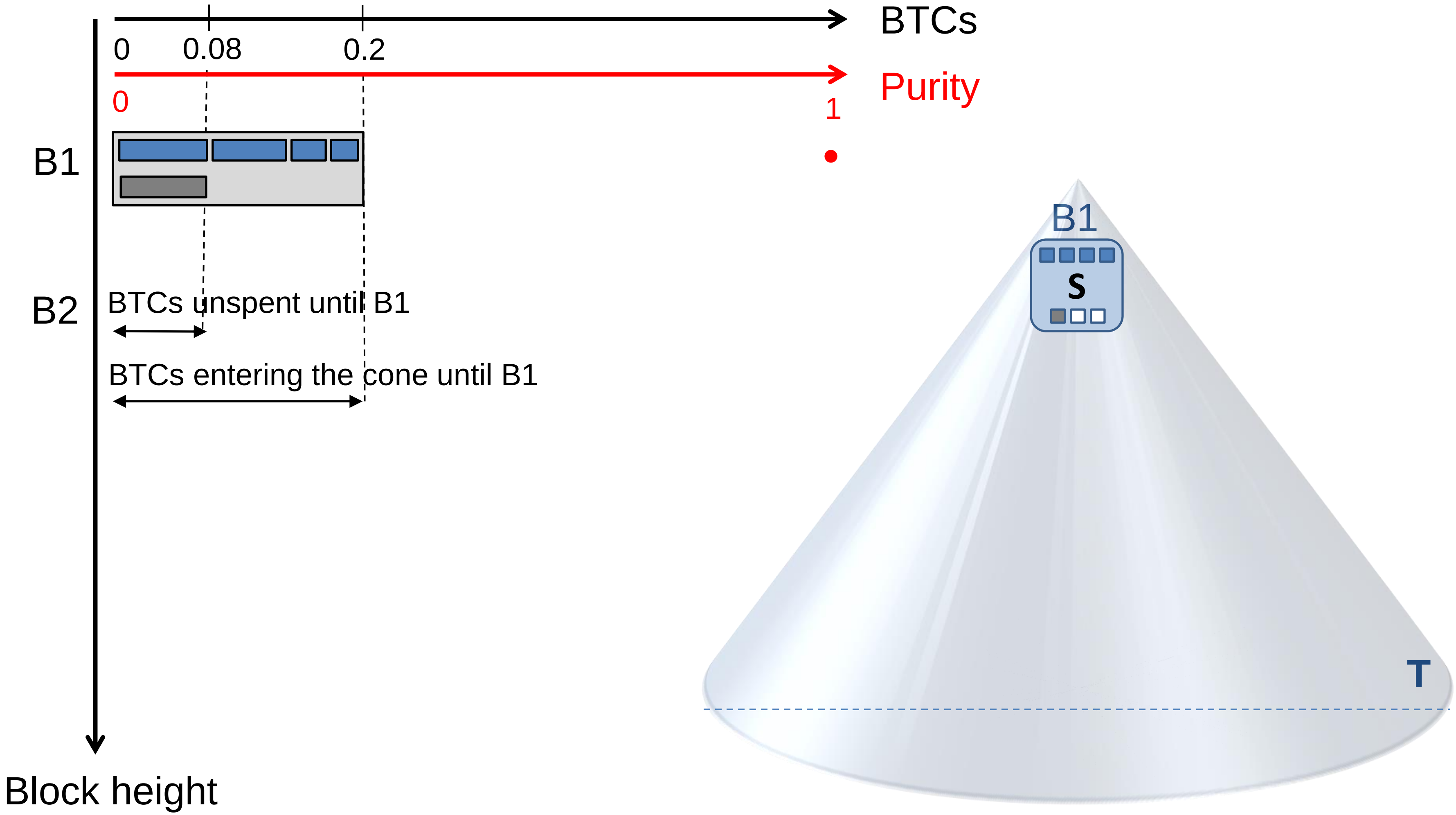
- The system will start computing cone(**S**, **T**):



- But it will not draw it as is

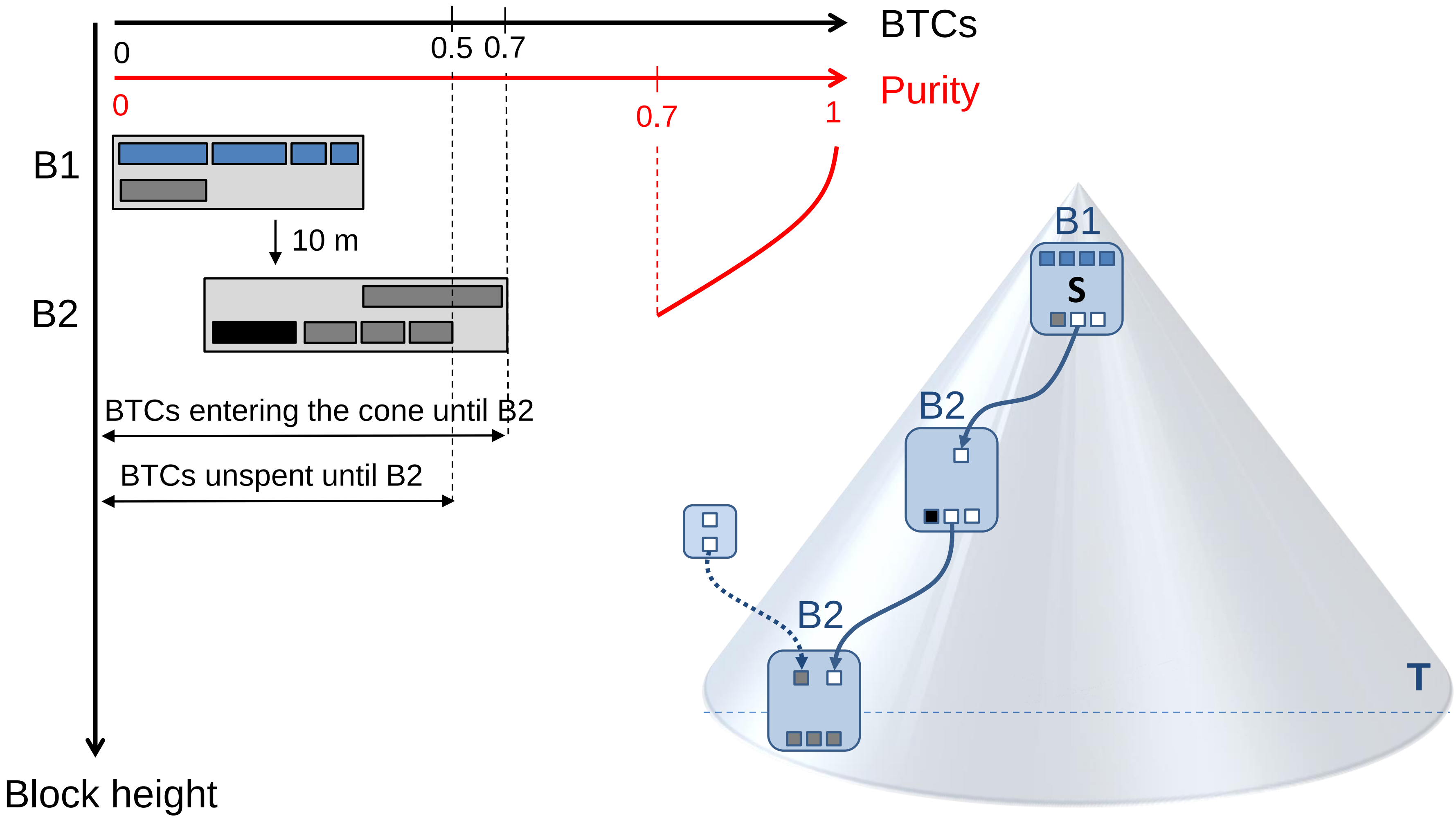
BitConeView

- Inputs of starting tx, and UTXO



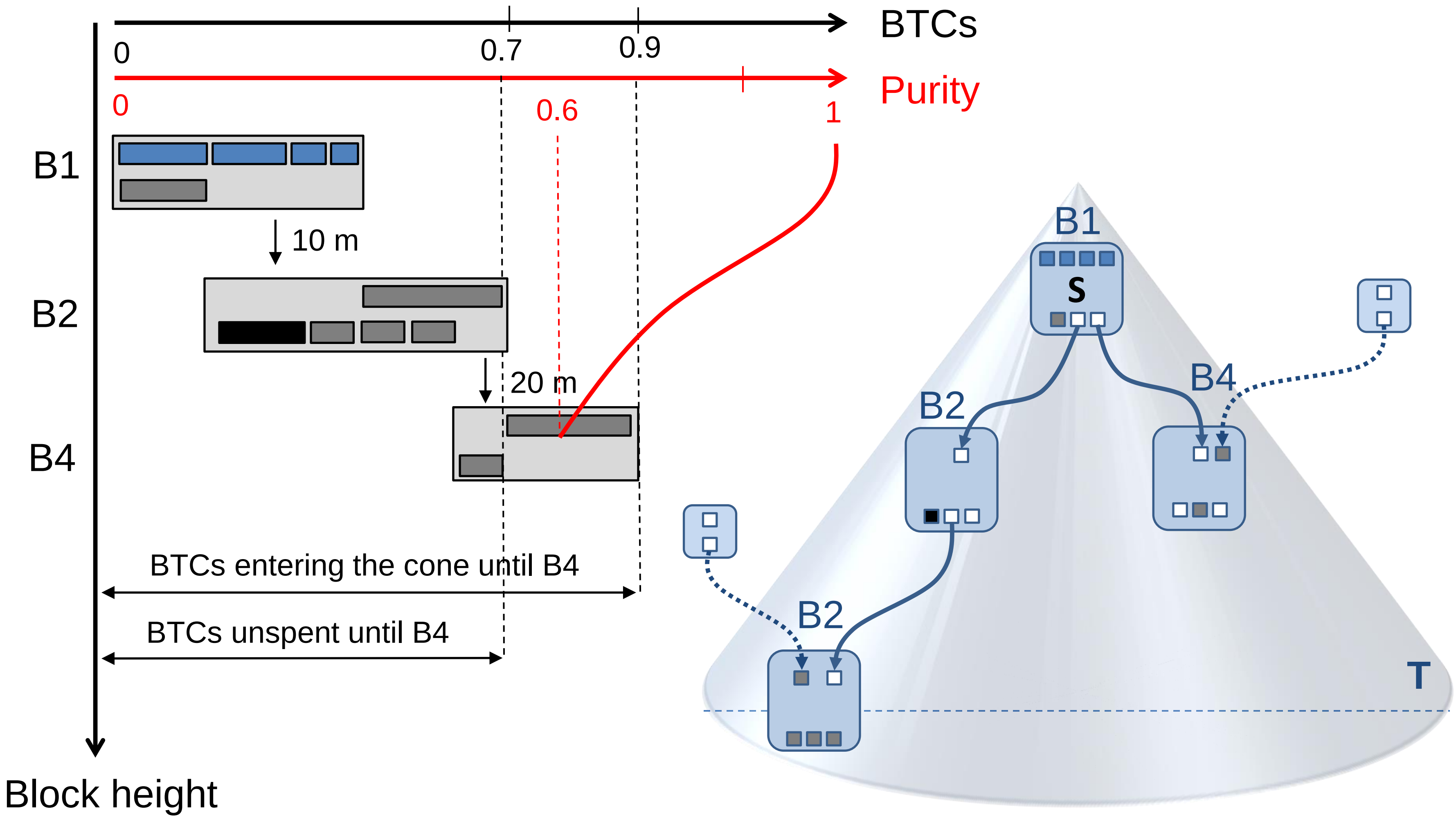
BitConeView

- Intruders and UTXOs (unspent up to T or never-spent)



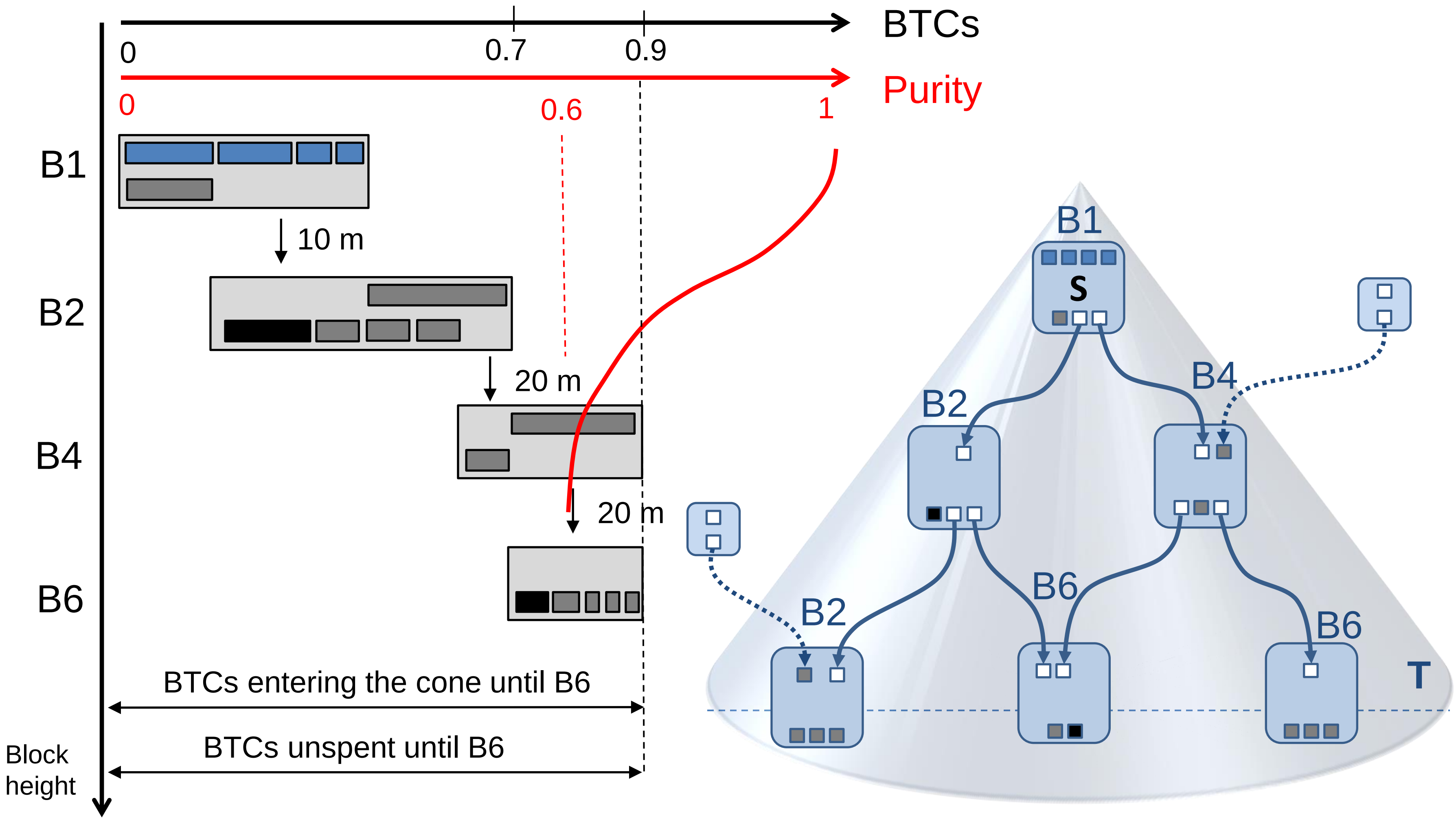
BitConeView

- Another intruder and another UTXO (unspent up to T)



BitConeView

- No intruders, more unspent outputs

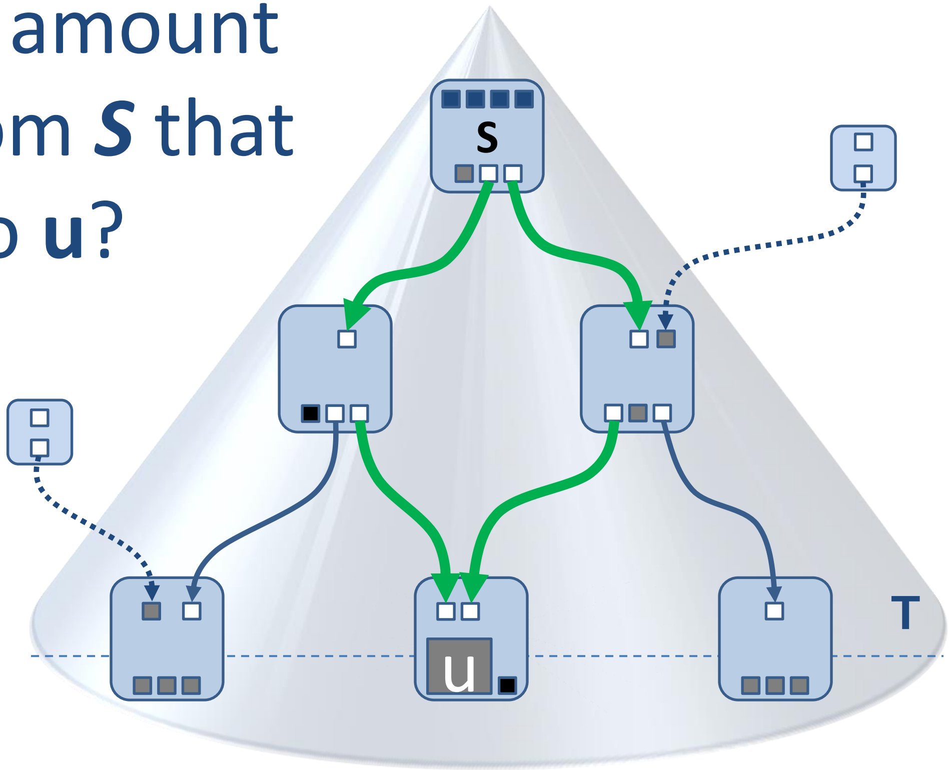


BitConeView

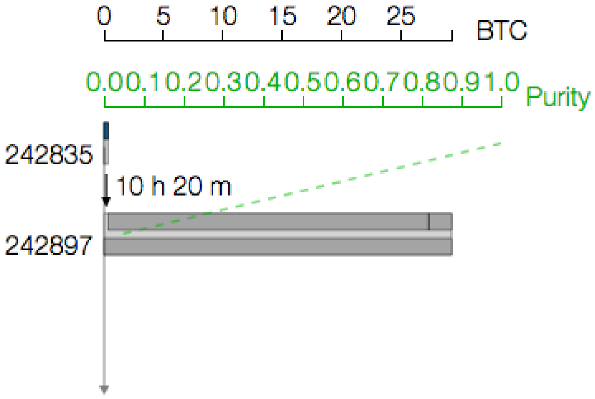
[USAGE VIDEO]

BitConeView: *Transfer Analysis*

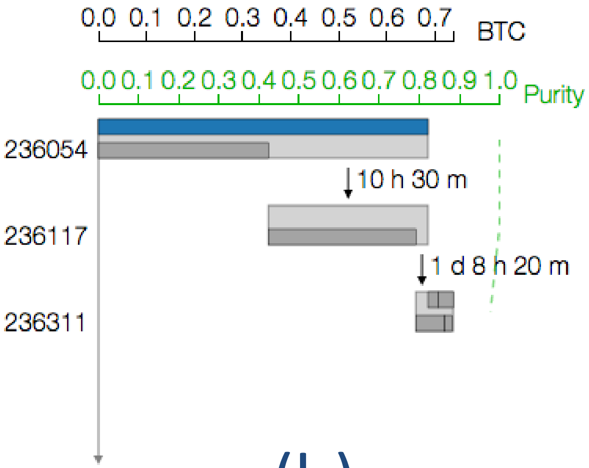
- We also defined a *Transfer Analysis* tool
- given the starting tx **S** and the UTXO **u**
- What is the maximum amount of the BTCs coming from ***S*** that could be transferred to **u**?
- May the two txs be connected?
- Consider the tx-graph as a flow network!



Experiments with BitLaundry



(a)



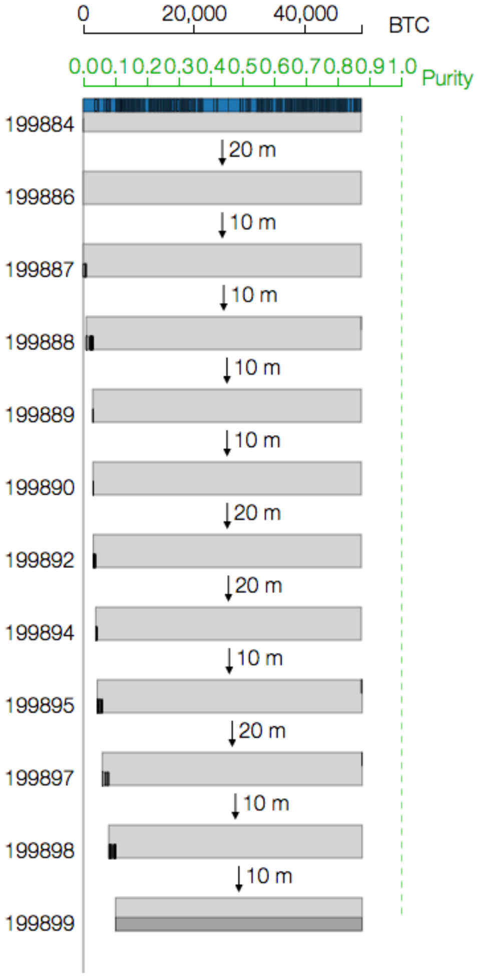
(b)

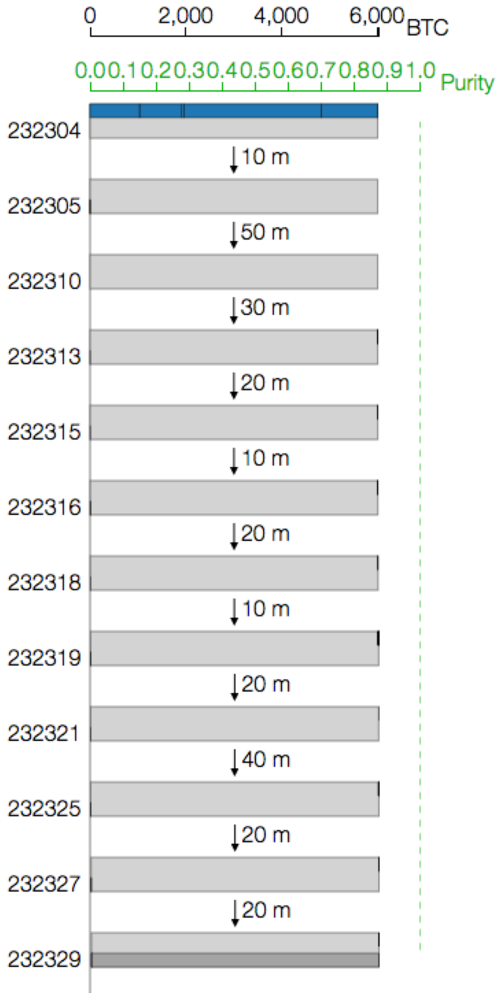
- Starting txs from [Moser et al. 2013]
- (a) the injected Bitcoins are mixed after ~10 h
- (b) BitLaundry is less effective

Experiments with Bitcoin Fog

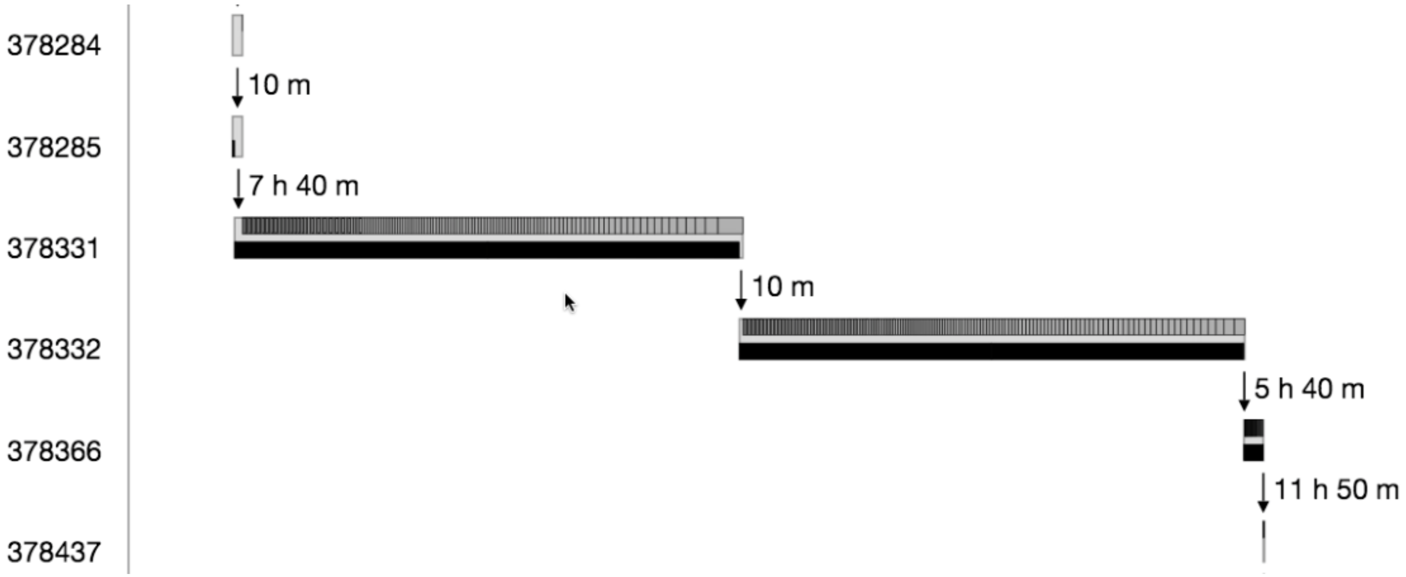
- [Moser et al. 2013]
- BTCs used as payout by mixing services often come from txs that are part of long chains in which each tx distributes small amounts of BTCs
- At the apex of the chains is common to find very large txs that bundle Bitcoins

40,000 BTCs > 10M USD!





Accumulation pattern



- *~150 inputs in txs falling in the same block*
- *1 final transaction bundling 1000 Bitcoins*
- *Twice!*

Evaluation

- Informal usability study (9 users, 2 experts)
  - Six engineers in the 30–35 age range
  - Three detectives of an Italian Investigation Division in the 40–50 age range
- 30 minute tutorial on Bitcoin
- Demonstration of BitConeView on some examples answering questions
- Let the users play themselves with the interface exploring real-world data

Evaluation

Question topic	Avg. Score (1-5)
Understand usage of Bitcoins	3.67
Understand mixing processes	4.22
Understand money laundering activity	3.78
Usefulness of the concept of purity	3.67
Usefulness of the Transfer Analysis	3.44

- Users were asked to fill out forms
  - Six questions with a score from one to five
- Good feedbacks overall
  - Effectiveness in showing mixing processes

Conclusions

- Conclusions
  - We presented a system for the **visual analysis** of flows in the Blockchain
  - We introduced the concept of **purity** of Bitcoins
  - We analyzed many real **money laundering** processes
  - We evaluated the system by means of a **usability study**

Ongoing work

- Scalability of the visualization
- Drill-down feature to explore the subgraph within a given block
- Support blockchains of different types of cryptocurrencies
- Integration with blockchain exploration platforms?

Questions?