

# BitConeView: Visualization of Flows in the Bitcoin Transaction Graph

Perugia Feb 1<sup>st</sup>, 2018

**G. Di Battista<sup>1</sup> · V. Di Donato<sup>1</sup> · M. Patrignani<sup>1</sup>  
M. Pizzonia<sup>1</sup> · V. Roselli<sup>1</sup> · R. Tamassia<sup>2</sup>**

<sup>1</sup> DEPARTMENT OF ENGINEERING  
ROMA TRE UNIVERSITY

<sup>2</sup> DEPARTMENT OF COMPUTER SCIENCE  
BROWN UNIVERSITY



# Background



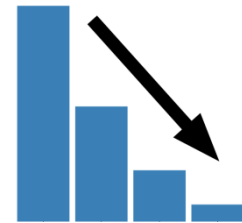
Peer-to-peer  
transactions



No need  
for third parties



Worldwide  
payments

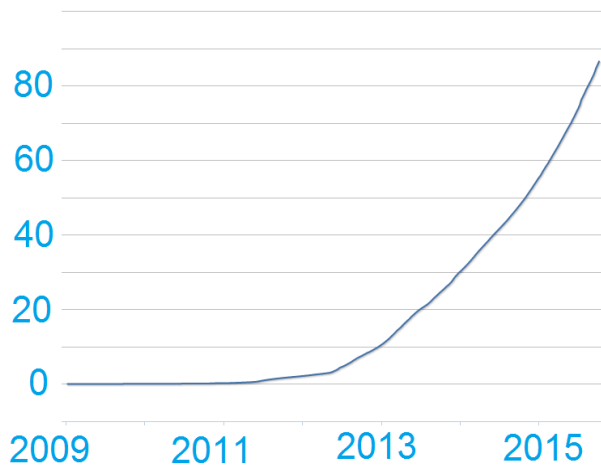


Low  
processing fees

- 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



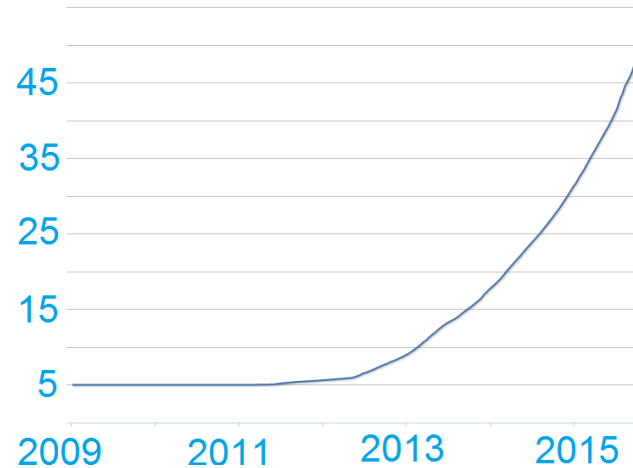
Total # Txns (M)



Avg # ~every 10 min



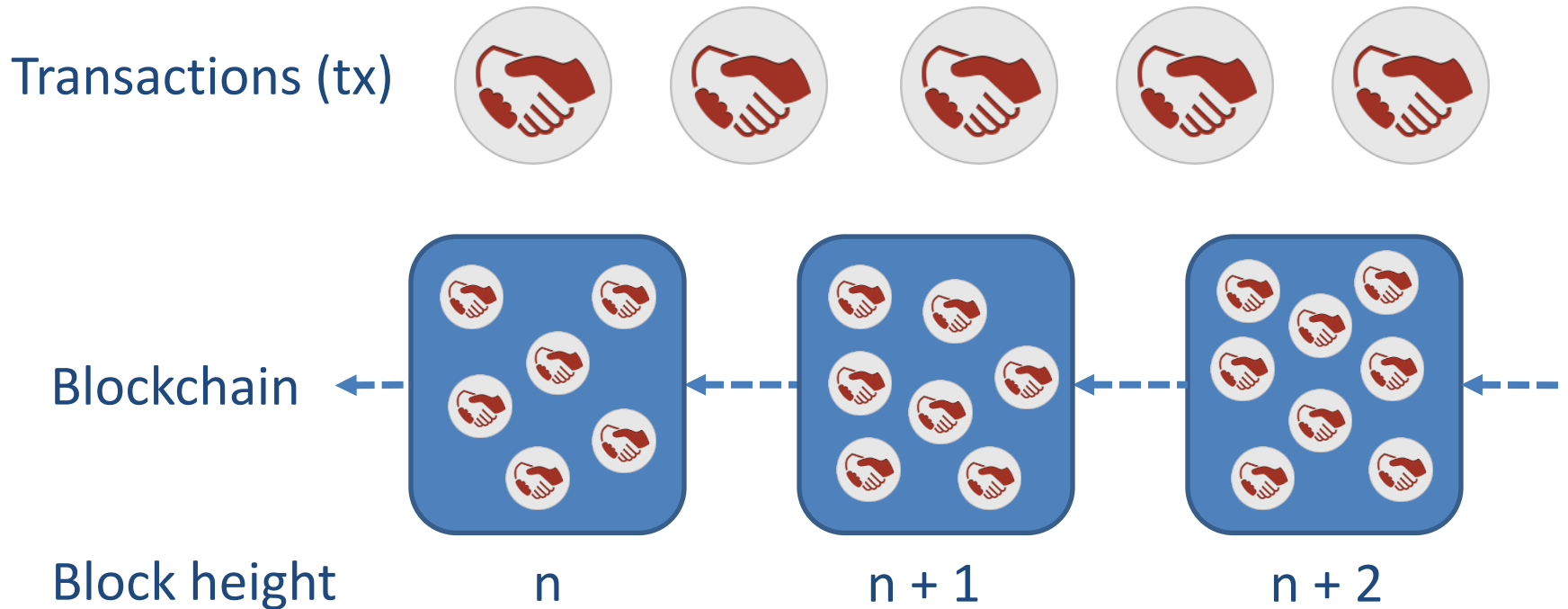
Market price (USD)



Blockchain size (GB)



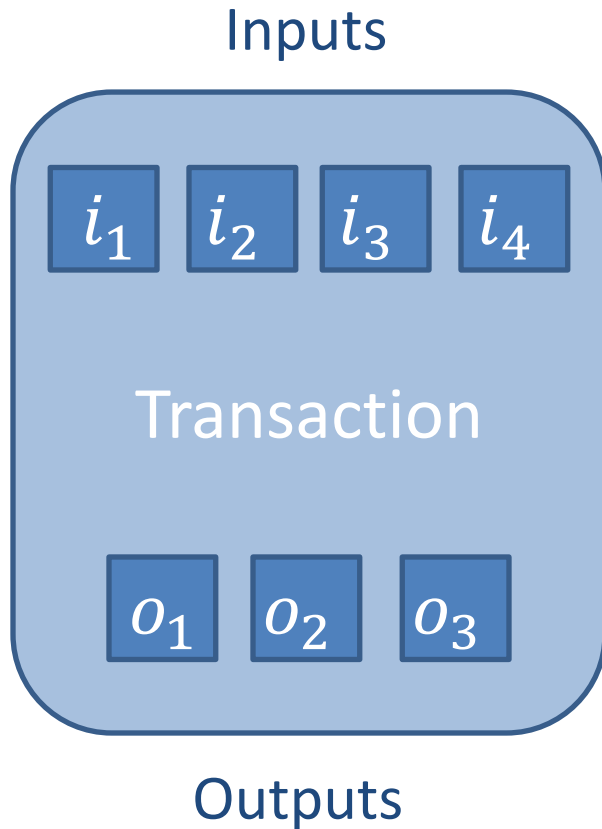
# Background



- Bitcoins are transferred 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

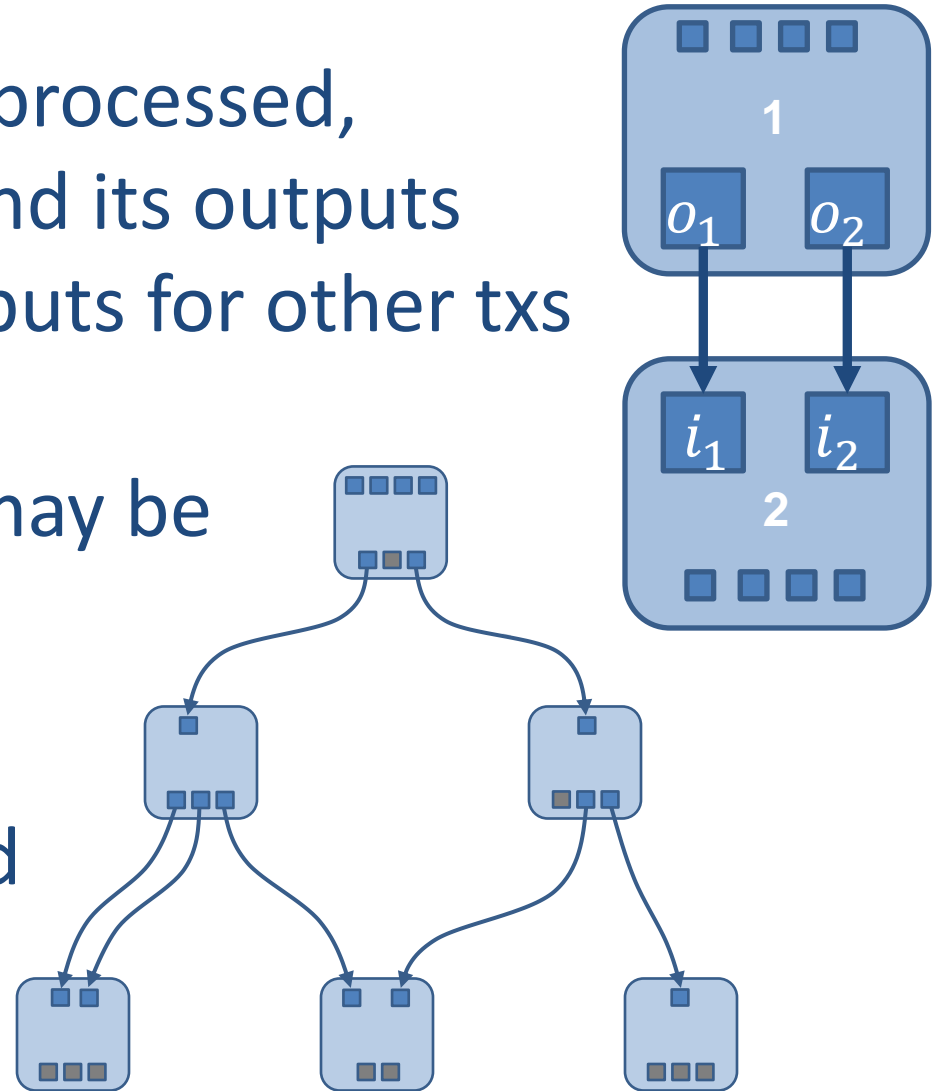


# Background

- 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

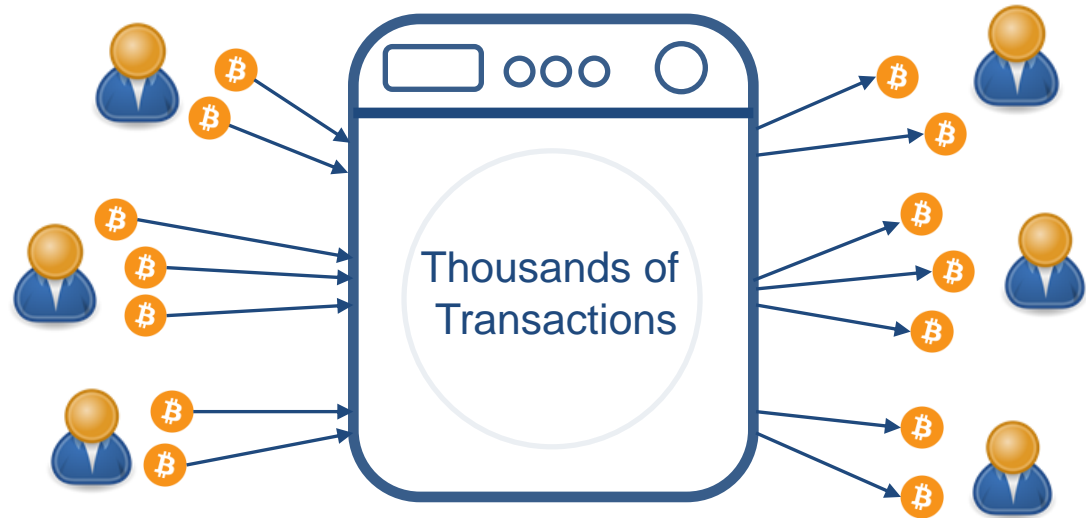
- Identity behind Bitcoin addresses is revealed
  - during a purchase for delivery purposes
  - when buying USD at exchanges
- Third parties may be able to
  - track your future transactions
  - trace your previous activity



# Mixing and Laundering

- Mixing services to improve anonymity

- BitLaundry
- Bitcoin Fog
- Bitcoin Mixer
- Bitcomix
- BitSafe
- ...



- Side effect

- Mixing services facilitate money laundering



# BitConeView: Requirements

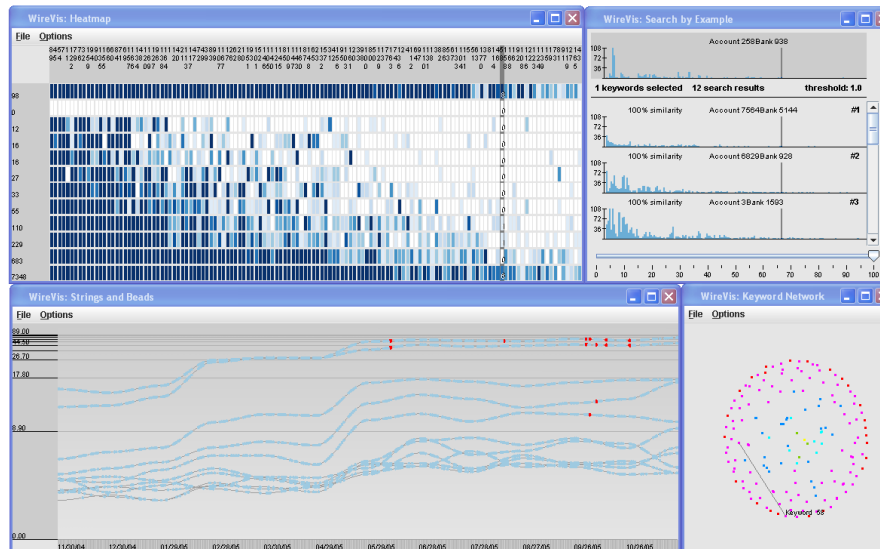
- Starting from one (or more) transaction(s)
  - Follow Bitcoins over time
  - Reveal flow patterns of interest
    - Accumulation, distribution, mixing
  - Understand when Bitcoins are mixed up
    - Understand the *degree of mixing* of Bitcoins over time
  - Evaluate effectiveness of mixing websites

# State of the Art: tx-graph analysis

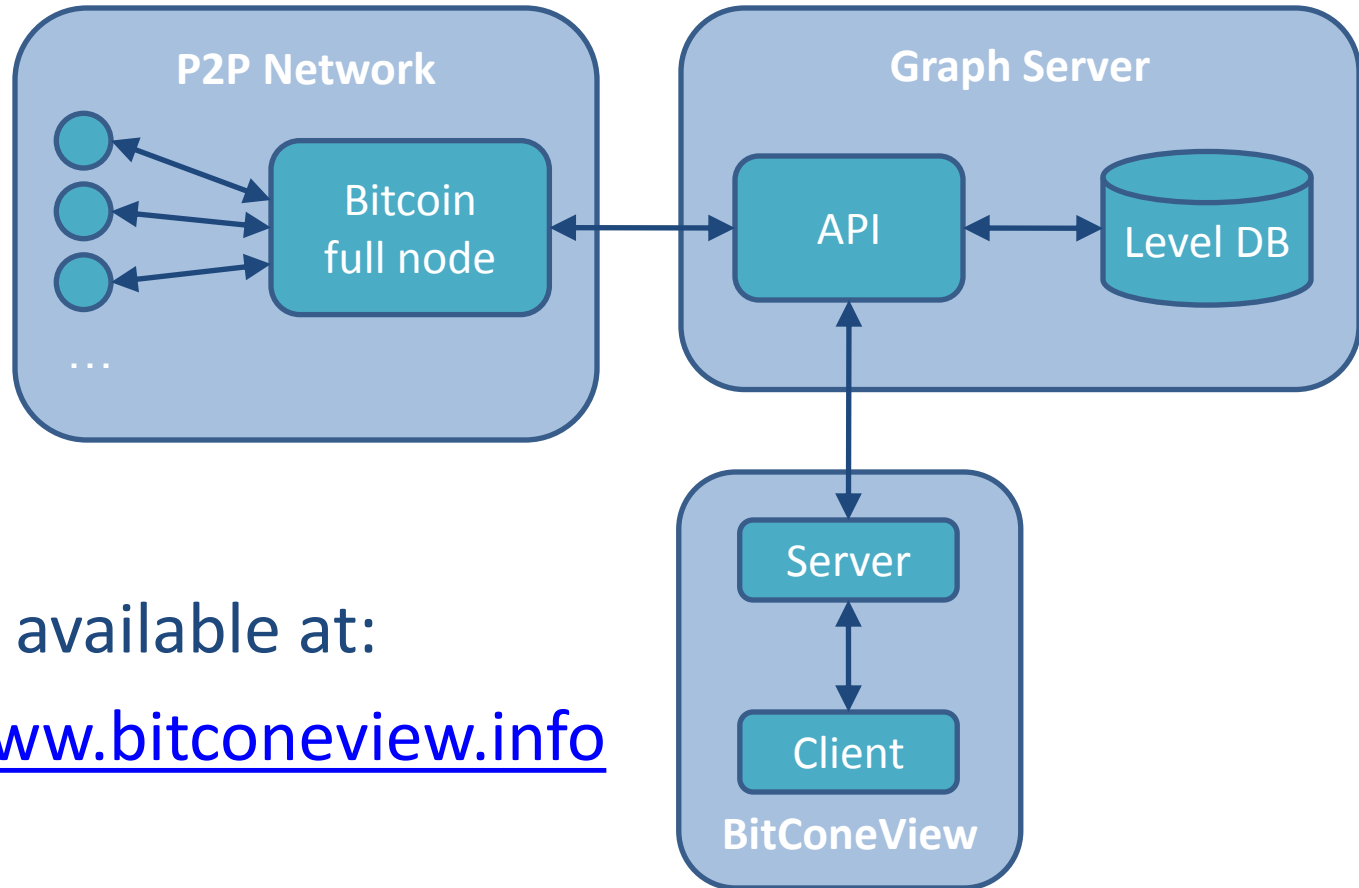
- Several papers on the analysis of the tx-graph
  - [Meiklejohn et al., 2013]
  - [Reid and Harrigan, 2013]
  - [Ron and Shamir, 2013]
- Some include drawings of subgraphs of interest
  - Laboriously created by hand or
  - Generated with standard force directed graph drawing tools that often yield to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

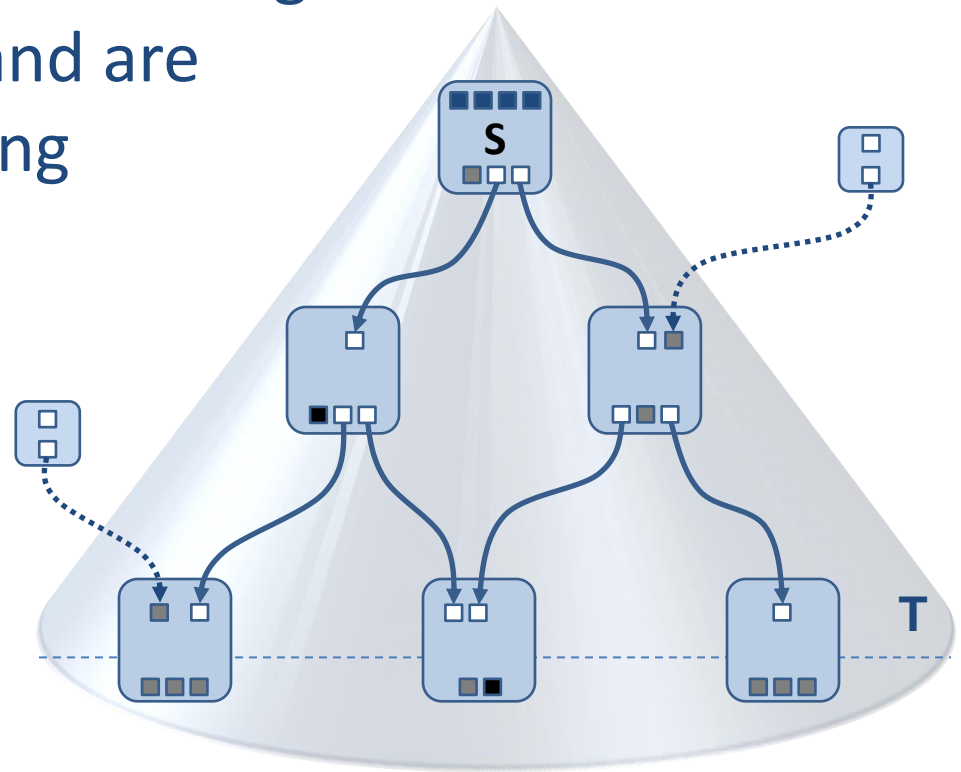


- DEMO available at:

<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:

cd19bd01011493c097ee575a1dfd9c9fef8f3a5d60ed5c059a9c5c1a501fee4

## 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

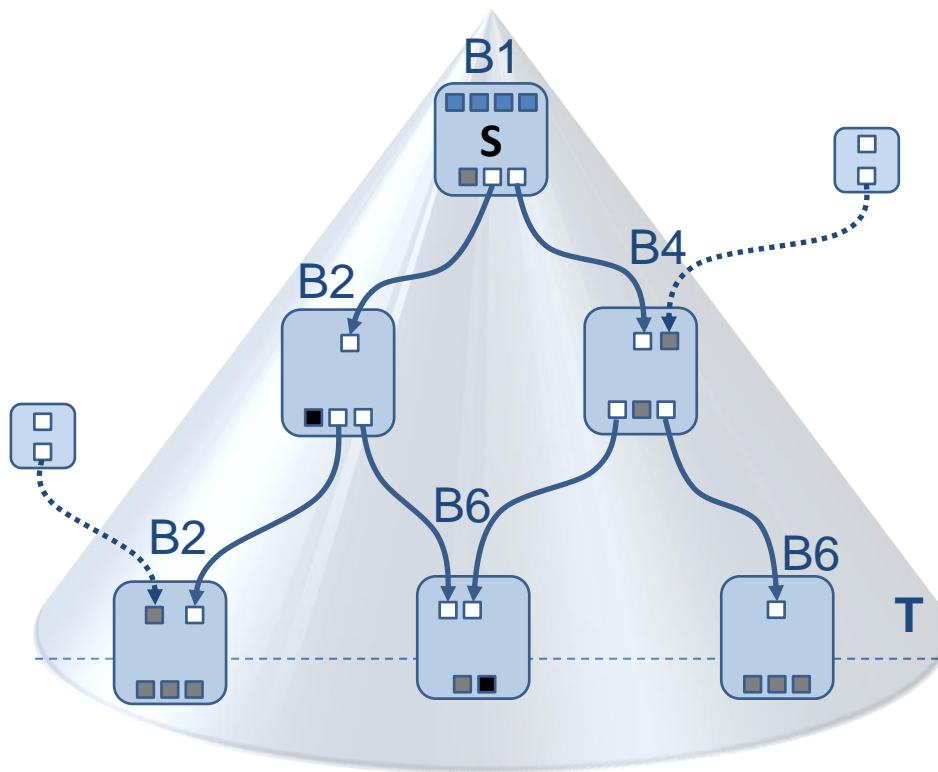
Start!

*This service is provided as is, without warranty of any kind. We will not take responsibility for any*

*ing from the use of this service.*

# BitConeView

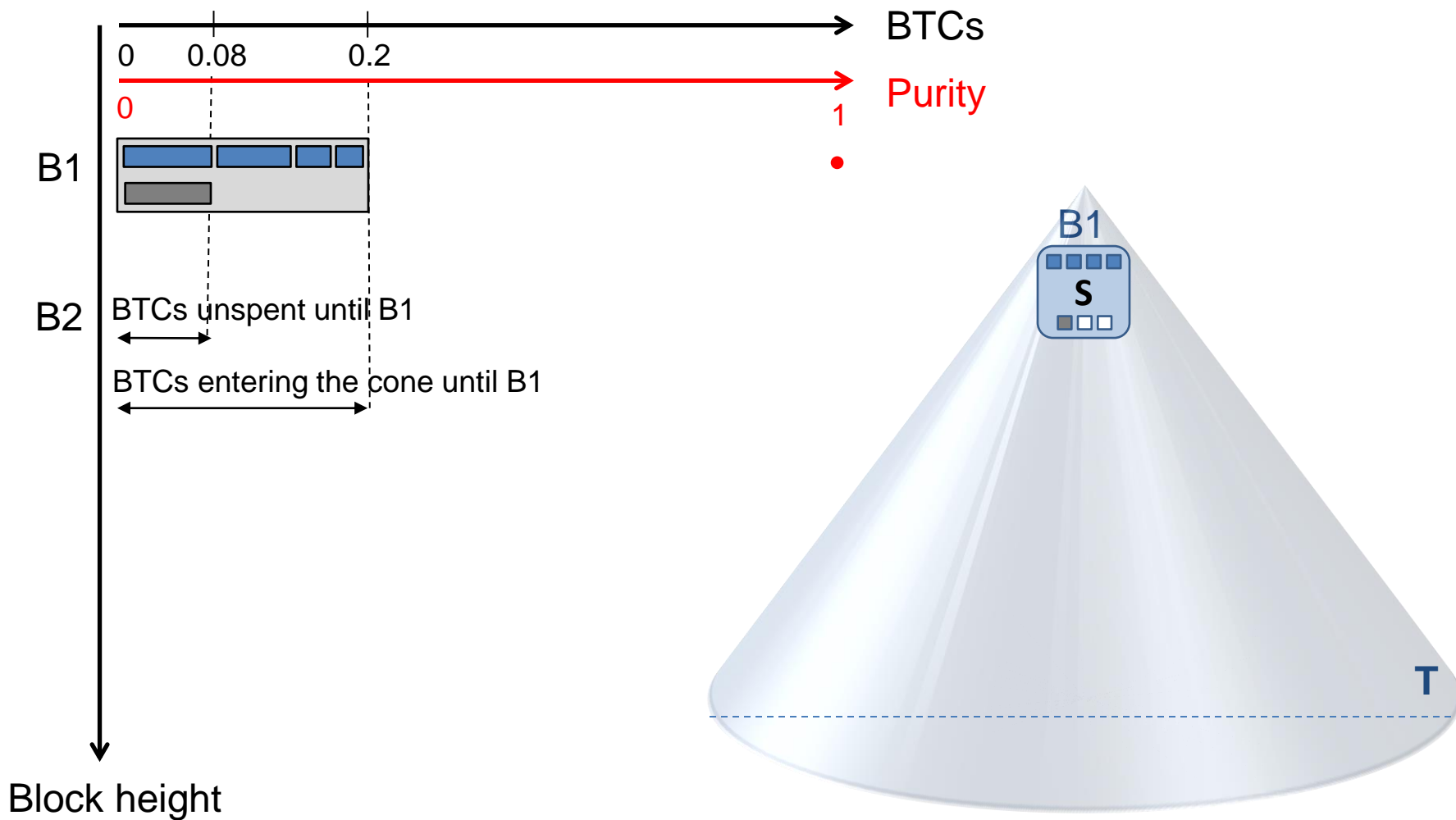
- The system will start computing cone(S, T):



- But it will not draw it as is

# BitConeView

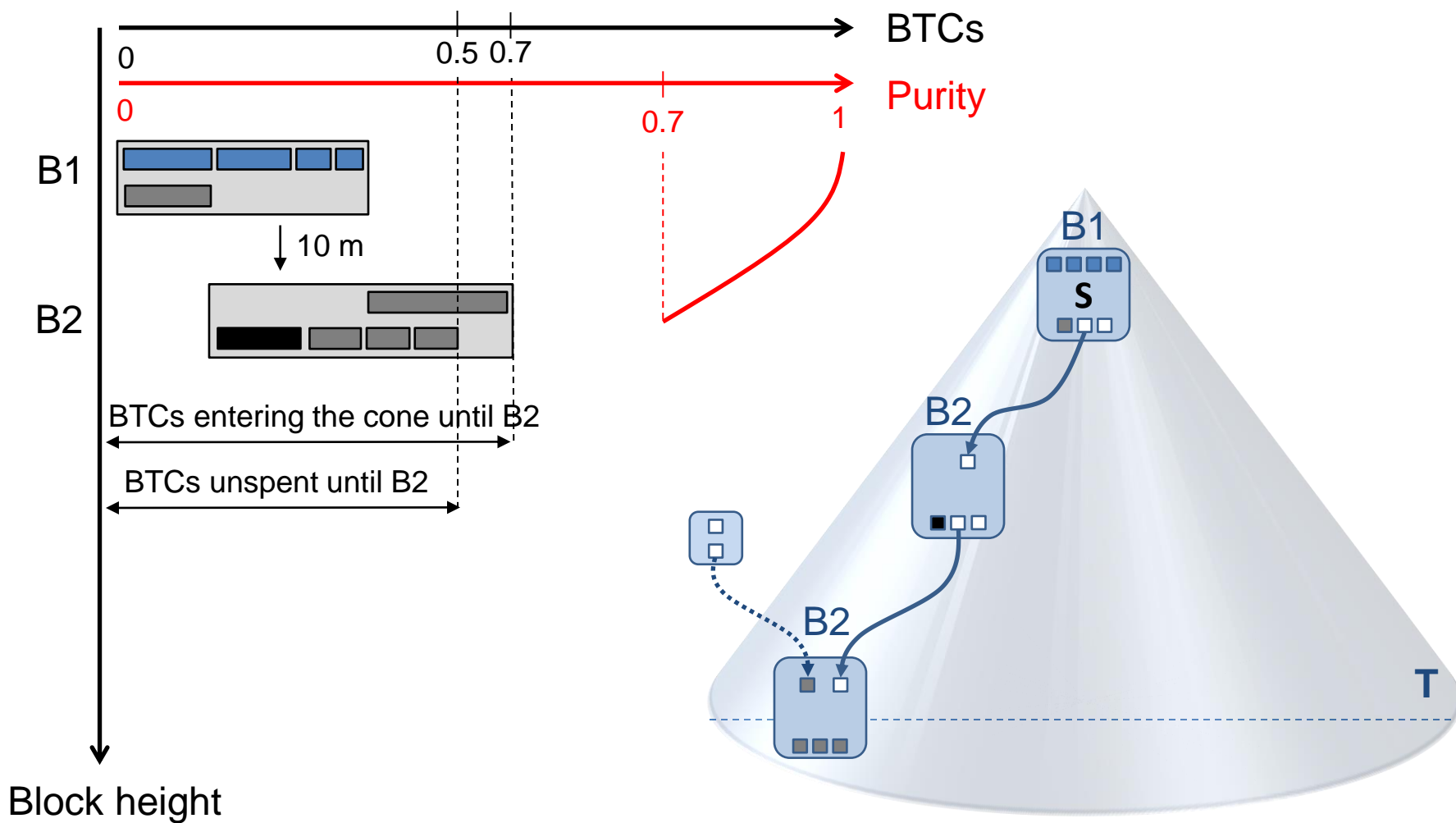
- Inputs of starting tx, and UTXO





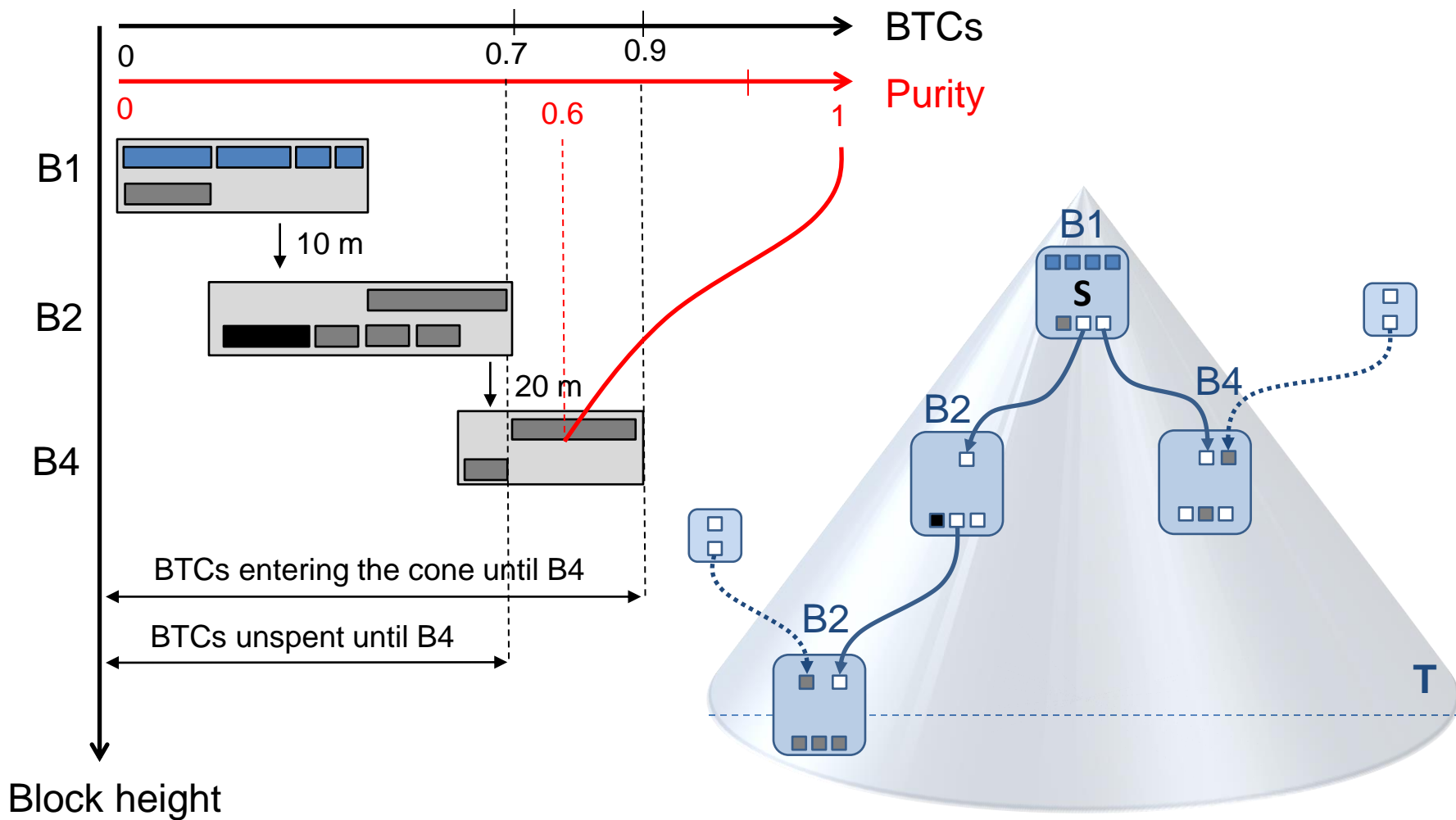
# BitConeView

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



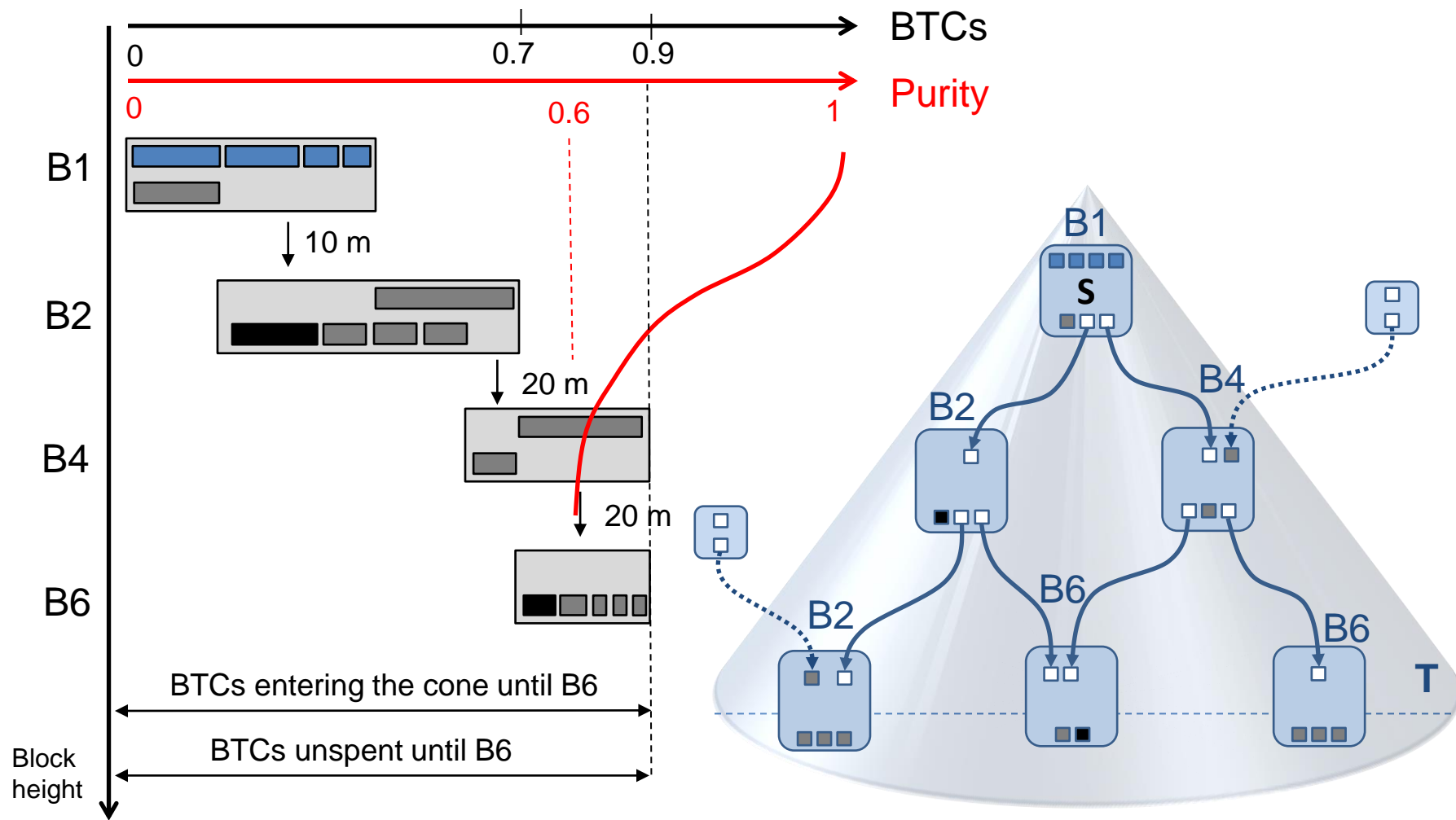
# BitConeView

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



# BitConeView

- No intruders, more unspent outputs



# Demo

[video]

Questions?