BLAST

Alessandro Gattolin
Daniele Moro
Marco Frigerio

Blockchain Assisted Transparency:

Efficient certification of data continuity through public history

Presentation roadmap

- The problem
- The approach
- Transparency Layer
- Some problems of a single layer approach
- Blockchain Layer
- Properties recap

- Hackathon implementation

The problem

Dealing with (big) data means dealing with:

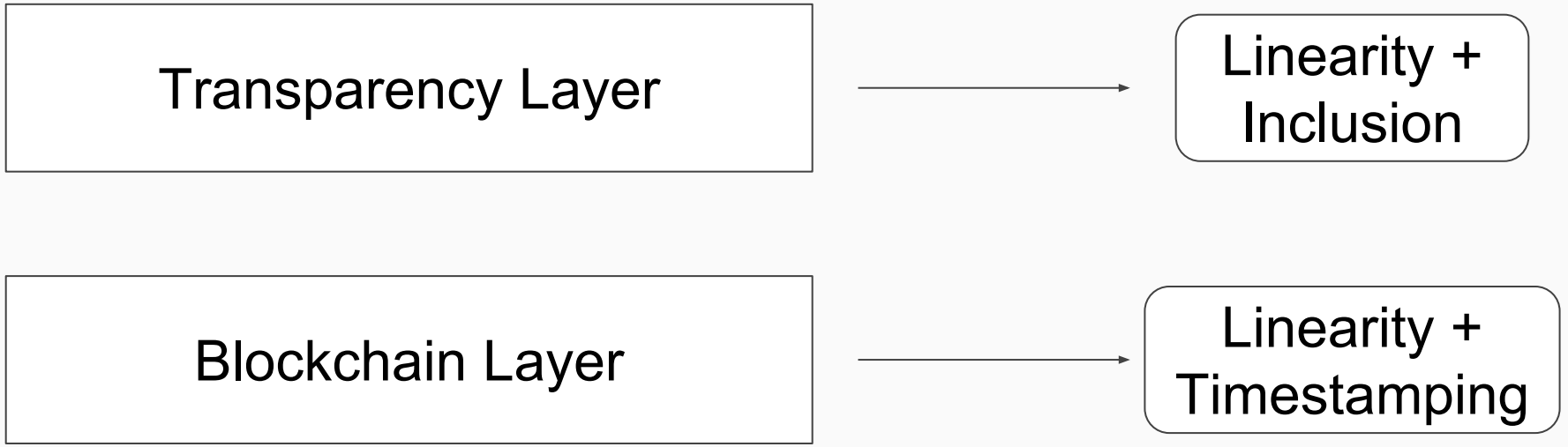
- Volume
- Variety
- Velocity and dynamicity

How to get for all the data guarantees as:

- Linearity
- Inclusion
- Timestamping

Without spending billions of dollars/euros

The approach



Transparency Layer (1): The context

(I) Define the context:

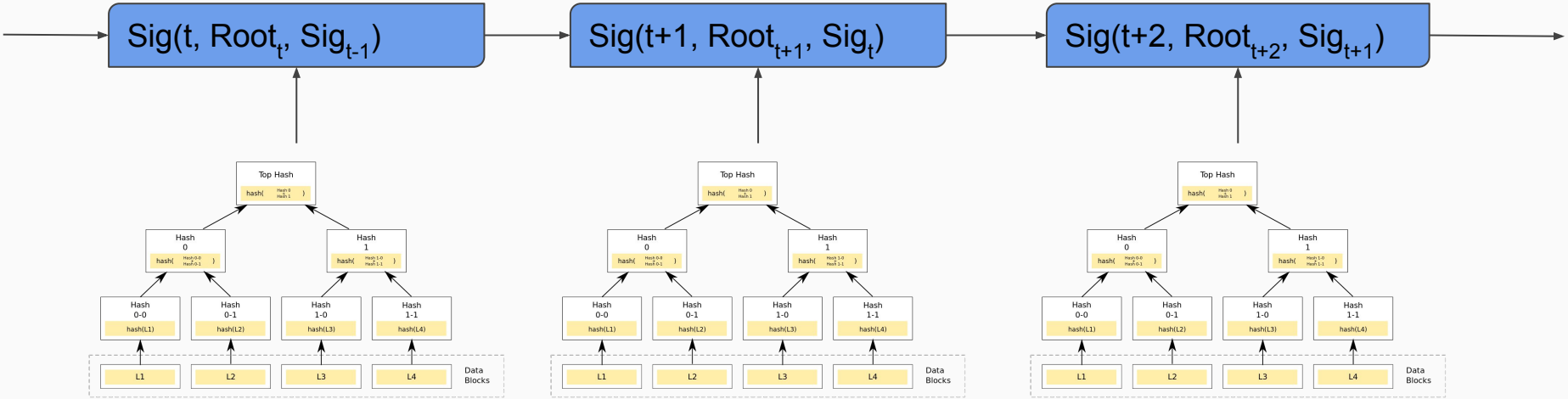
- Google Key Transparency (ID,PublicKeys pairs)
- Progress of personal career (academic, working)
- Disaster Recovery (backup history certification)
- ….

(II) Identify the representative of the context (similar to OTS Calendar server):

- He is the one in charge of the transparency layer
- He acts as a data collector

Transparency Layer (2): Data Structure

Key components: Merkle Tree, Discrete time axis, Linear history of Merkle Trees



Everything seems good...

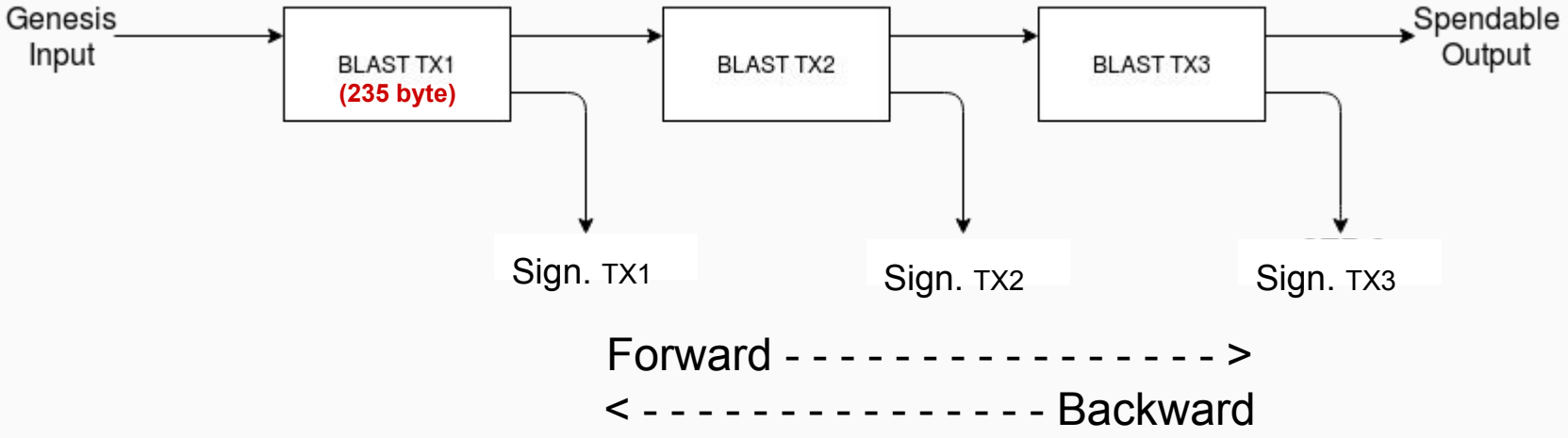
What's the problem?

Equivocation ?????

Who guarantees linearity?
What about a parallel history?
Anyone here that cares about timestamping?

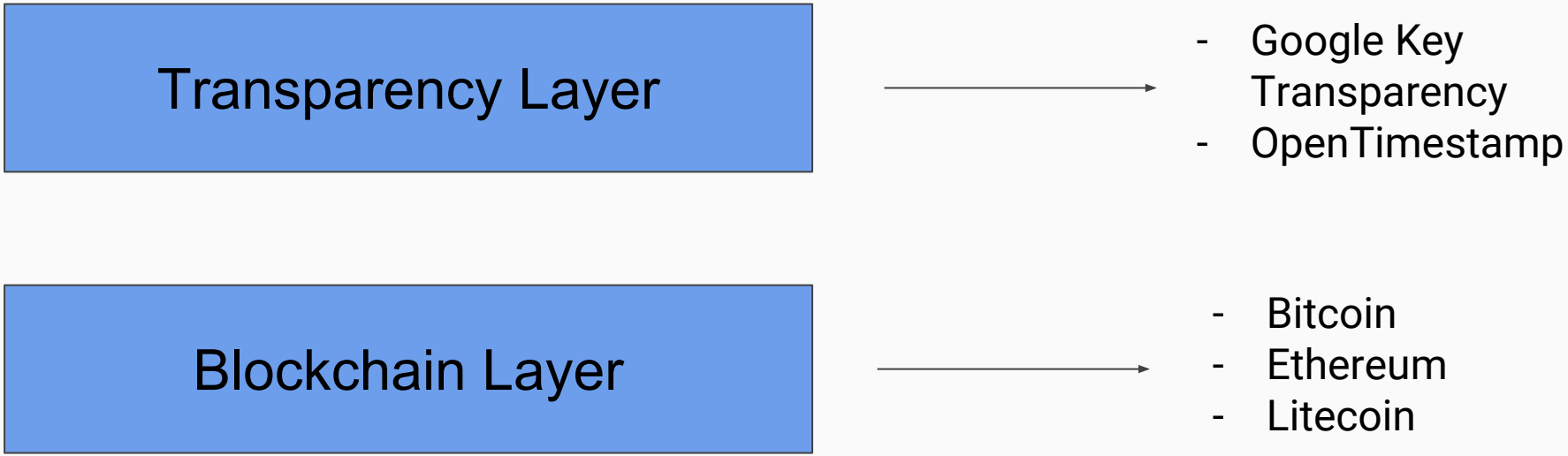
The Blockchain can do all of these

Blockchain layer

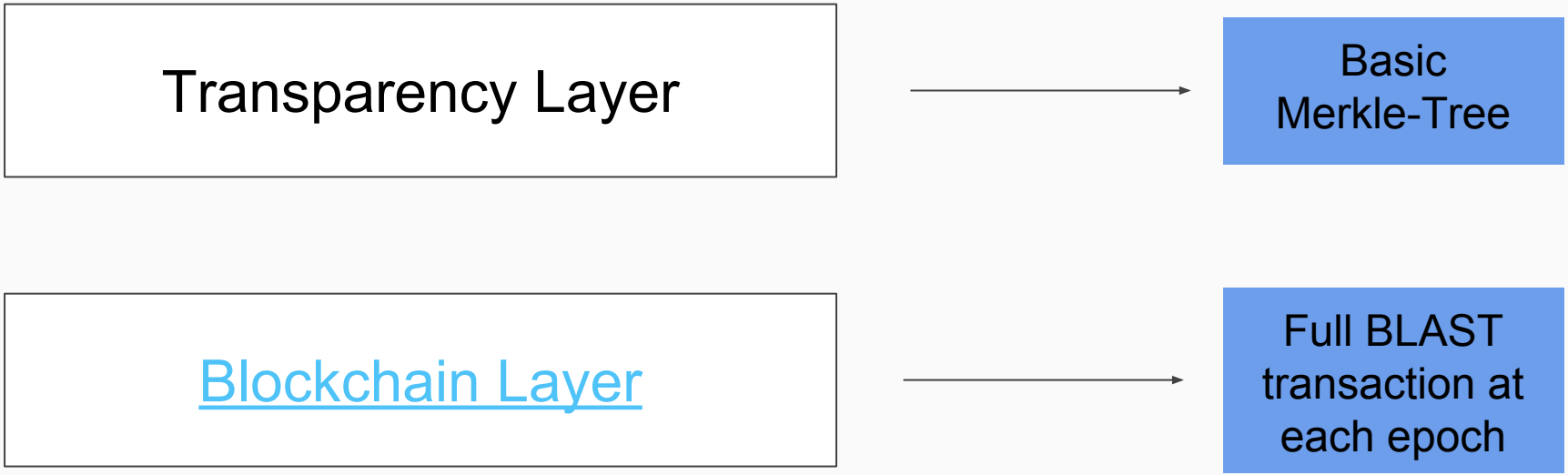


Equivocation: as hard as hard-forking

Properties Recap: No layer lock-in



Hackathon implementation



Thanks for the attention

Alessandro Gattolin
Daniele Moro
Marco Frigerio