Security proofs for some protocols based on blockchain technology

A. Meneghetti, A. Ottaviano Quintavalle, **M. Sala**

University of Trento

DLT Workshop - Perugia - February 1st 2018

UNIVERSITÀ DEGLI STUDI DI TRENTO

Who am I?

University of Trento

- Full Professor in Mathematics (Algebra and Cryptography)
- Laboratory of Cryptography (CryptoLabTN) Director

Italian Association of Cryptography **De Componendis Cifris**

- Acting Director

University of Trento spin-off company **Intellegit**

- Head of the Area Cyber Security and Cryptography

Overview

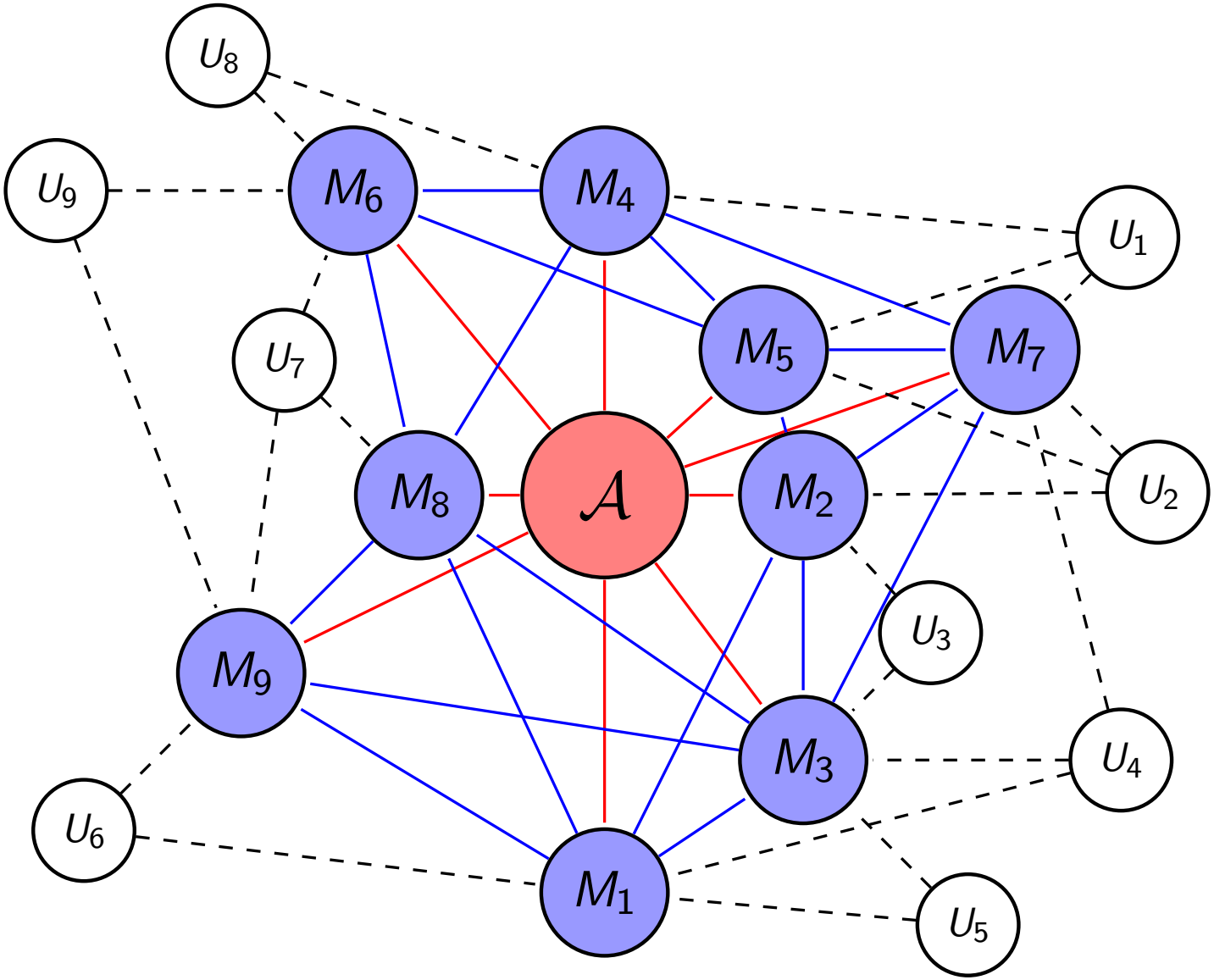
Aim

Protocol which allows data integrity verification with guaranteed:

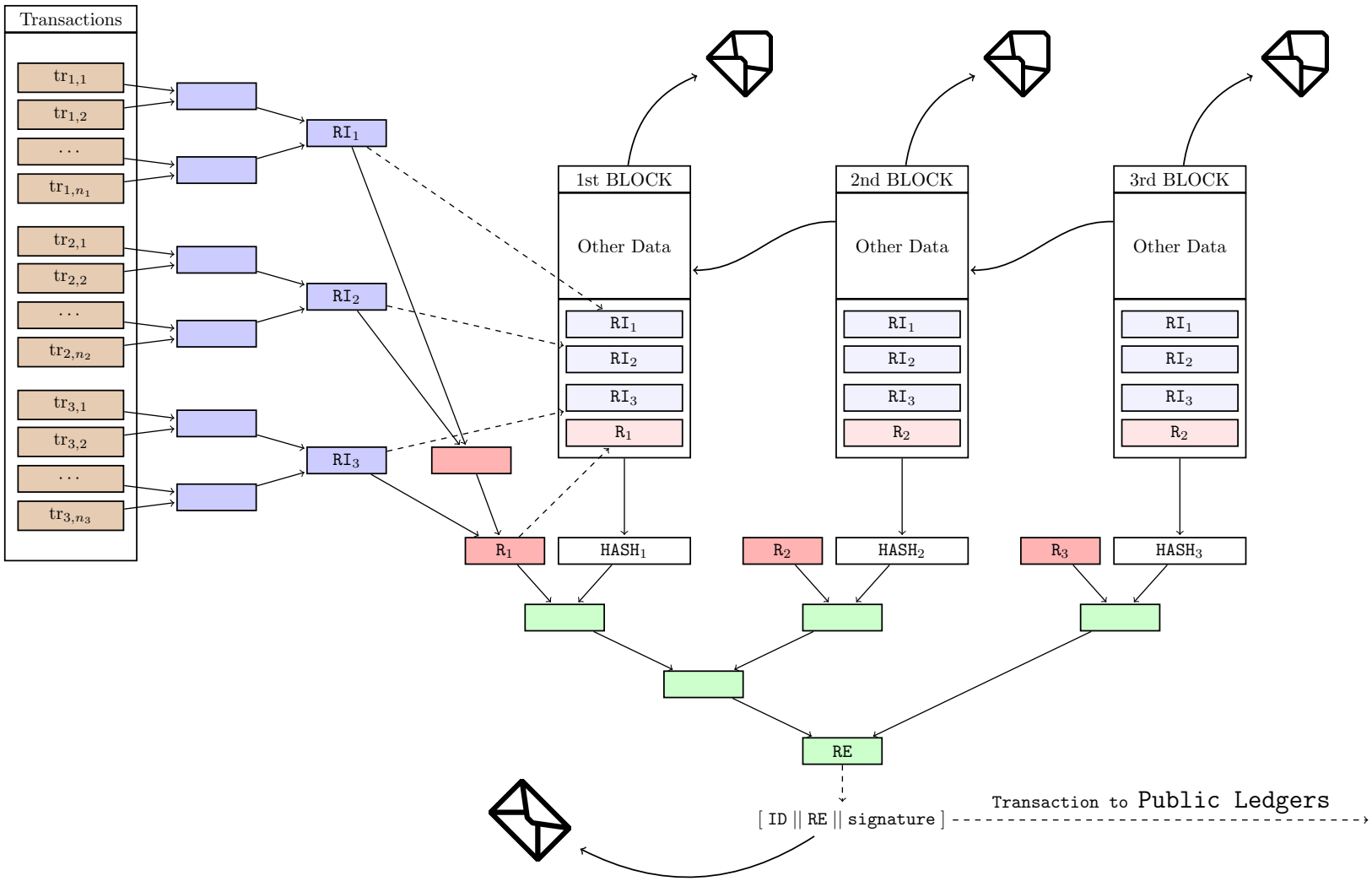
- Reliability
- Immutability
- Security

Customer: a large Italian bank

The Network



The Protocol



Security Issues

Users

- Transaction Forgery: the attacker pretend to be a valid user and send a fake transaction;
- Ghost Document: a valid user protects a new document with a previous or fake transaction.

Miner

- Transaction Forgery: modification of a valid transaction to damage a valid user;
- Receipt Forgery: creation of a fake receipt for a valid transaction from a valid user.

Security Issues

Proxy Authority

- Anchoring Failure: avoids to anchor the proxy blockchain to public distributed ledgers;
- Anchoring Forgery: creation of a fake anchor (transaction to a public ledger) or creation of fake informations on a valid anchor.

Together

- Fake Ownership: the Proxy Authority, all the miners and a malevolent user work together to steal the property of a document from an honest user.

Proof of Security

Our assumptions on the primitives:

- everyone's keys are managed by a trusted PKI;
- the public blockchain is trustworthy;
- the Hash function is collision resistant;
- the Digital Signature $d = DS(\mathrm{hash}(\mathrm{document}))$ does not allow to retrieve $\mathrm{hash}(\mathrm{document})$.

Proof of Security

- Transaction Forgery: Digital Signature
- Ghost Document: Hash function
- Receipt Forgery: either Digital Signature or Hash function
- Anchoring Failure: trusted Public Blockchain
- Anchoring Forgery: either Digital Signature or Hash function
- Fake Ownership: Digital Signature

Thank you!