THALES

Consensus protocols for Blockchain

Ambre Toulemonde

Université de Versailles Saint-Quentin-en-Yvelines and Thales DIS

RESSI 2020 – December 2020

Consensus protocols

The Byzantine Generals problem, 1982

- How to reach an agreement on a value in a distributed manner ?

Basic security properties

- Safety and Liveness

Practical Byzantine Fault Tolerance (PBFT)

- First practical consensus protocol
- Achieve liveness and safety in partial synchrony
- Small set of n participants whose at most $\lceil \frac{n-1}{3} \rceil$ may be Byzantine

Nakamoto Bitcoin protocol, 2008

Blockchain technology

- Distributed ledger or chain of blocks where a new block is added after reaching a consensus
- Data in blocks are immutable once written into the blockchain

Bitcoin Proof-of-Work consensus protocol

- Being the first who solves the hash puzzle
- New needs for consensus protocols: scalability and incentivation
- Issues : energy waste problem, fork problem, selfish strategy, etc.

Many new consensus protocols proposed in the literature

- Avoid the issues of the Bitcoin Proof-of-Work consensus protocol

PhD research

Consensus protocol using leader election protocol

- A participant is elected as leader whose role is to provide the next block of data to be added in the ledger

Contribution

- Formal model of leader election
- Security properties: uniqueness, fairness, unpredictability, forward unpredictability, liveness
  - Revisit fairness and unpredictability properties
- Security analysis of two protocols: attack or prove the security properties
  - *Single Secret Leader Election (SSLE)* of Boneh, Eskandarian, Hanzlik and Greco (2020)
  - *Algorand* of of Chen and Micali (2016)