

Consensus protocols from Byzantine Generals problem to Blockchain

Ambre Toulemonde



Université de Versailles Saint-Quentin-en-Yvelines and Thales DIS
ambre.toulemonde@thalesgroup.com



Consensus protocols for the Byzantine Generals Problem

> How to reach an agreement on a common action plan for the honest generals without a central authority ?

> Security properties: **Safety** and **Liveness**

Practical Byzantine Fault Tolerance (PBFT)

> First practical consensus protocol which became the reference to construct consensus protocol

> Achieve liveness and safety in partial synchrony

> Small set of n participants whose at most $\lfloor \frac{n-1}{3} \rfloor$ may be Byzantine

Nakamoto Bitcoin protocol and blockchain

> Blockchain

> **Bitcoin Proof-of-Work** consensus protocol: being the first who solves the hash puzzle

Hash(█) < target

- New needs: **scalability** and **incentivation**
- Bitcoin PoW Issues:
 - **fork problem**,

- **selfish strategy**,

- **energy waste problem, centralization in big pool, etc.**

PhD research : consensus protocols for blockchain

> Satisfying the security properties of consensus protocol and the new needs of the blockchain while avoiding the Bitcoin PoW issues

> Consensus protocols using **leader election**

Contribution

> Formal model of leader election

> Security properties of leader election protocol

- **Uniqueness**
- **Fairness**
- **Unpredictability**
- **Forward unpredictability**
- **Liveness**

> Security analysis of two leader election schemes

- **Single Secret Leader Election (SSLE)**
- **Algorand**

Single Secret Leader Election (SSLE)

> Boneh, Eskandarian, Hanzlik and Greco, 2020

> Random election of exactly one leader such that her identity remains hidden until she chooses to reveal herself

> **Contributions:** attack or prove the security properties

- Attack on the fairness property

Algorand leader election

> Chen and Micali, 2016

> Secret election of several potential leaders and a rule enables to choose one of them as leader

> **Contributions:** attack or prove the security properties

- Selfish strategy to break the forward unpredictability property