


## Blockchain consensus for IoT

Antoine DURAND<sup>1</sup>

Gérard MEMMI<sup>2</sup>, Khalifa TOUMI<sup>1</sup>, David LEPORINI<sup>3</sup>

<sup>1</sup>IRT-SystemX, <sup>2</sup>Télécom Paris, <sup>3</sup>Atos

### 1. CONTEXT



- Blockchain could be a key enabler for large-scale, secure and autonomous IoT
- Existing research in distributed algorithms can be leveraged to improve blockchain
- Emerging algorithms does not address both scalability and resource consumption
- Blockchain protocols also present new, unfaced challenges

### 2. RESEARCH GOALS

Develop a blockchain consensus algorithm designed for IoT applications :

- Proof-of-Work algorithms are excluded
- Must handle a large count of nodes

### 3. PROPOSITION

The **Stakecube** blockchain

- ✓ The Proof-of-Stake security model is adopted to prevent Sybil attacks without Proof-of-Work
- ✓ A sharding mechanism is leveraged to make an efficient block creation procedure

The sharding structure is provided by Peercube, a Distributed Hash Table.

### 4. USE CASE

The energy marketplace is an example of an application where a blockchain is expected to solve key challenges, by allowing all kinds of energy producers and consumers to trade directly.

The implementation of the energy marketplace with Stakecube will demonstrate its viability in an IoT use-case.

### 5. EXPECTED RESULTS

An implementation of StakeCube is in progress. It is expected to :

- Validate the performance goals through the benchmarking of transaction rate and confirmation latency
- Experimentally compute optimal security parameters
- Validate compatibility with IoT devices by measuring resources usage on a Raspberry Pi Zero running the energy marketplace

### 6. FUTURE WORK

We intend to improve StakeCube by :

- Using threshold signatures to further reduce network load
- Extending the sharding mechanism to transaction storage

### REFERENCES

- Durand, A., Anceaume, E., & Ludinard, R. (2019). STAKECUBE: Combining Sharding and Proof-of-Stake to build Fork-free Secure Permissionless Distributed Ledgers. NETYS2019.
- Anceaume, E., Ludinard, R., Ravoaja, A., & Brasileiro, F. (2008, October). Peercube: A hypercube-based p2p overlay robust against collusion and churn. SASO2008.