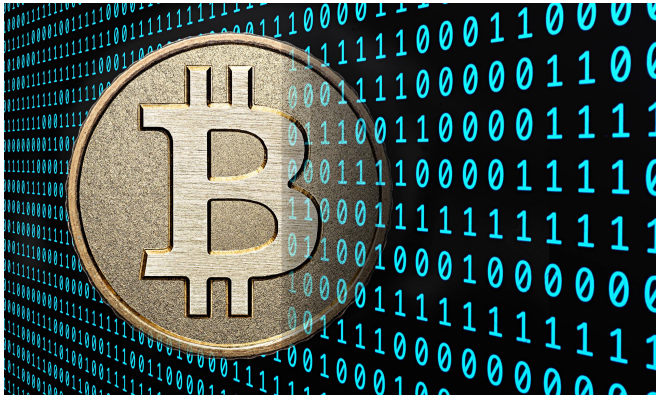
# EcoMobiCoin et Lcoin

## Cryptomonnaies pour l'éco-mobilité et les échanges locaux.

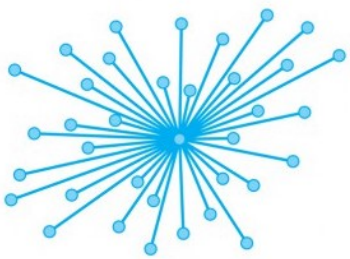
Jerôme Deschamps, Anthony Graingnic, Paul-Marie Grollemund,
Frederic Hayek, **Pascal Lafourcade**,
Kevin Thiry-Atighehchi, Ariane Tichit

Marseille, avril 2024

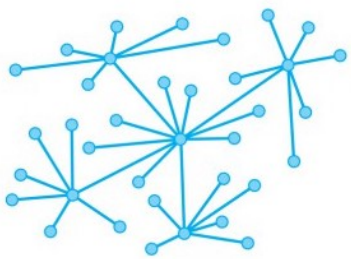
# La révolution Bitcoin 2009



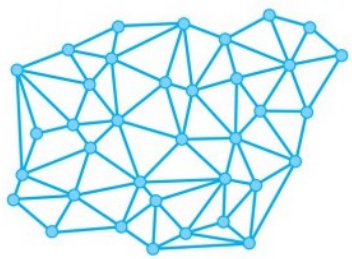

- Cryto-monnaie décentralisée et distribuée



Système centralisé



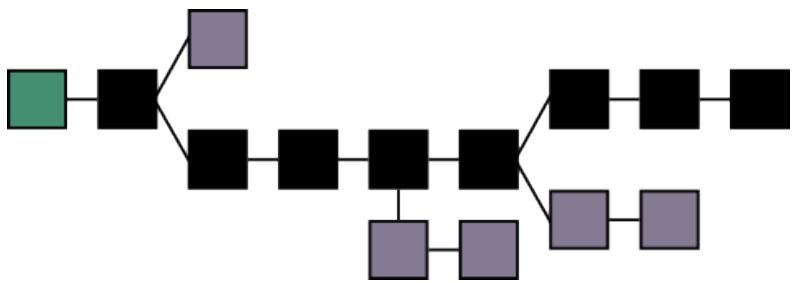
Système décentralisé



Système distribué

21 millions BTC

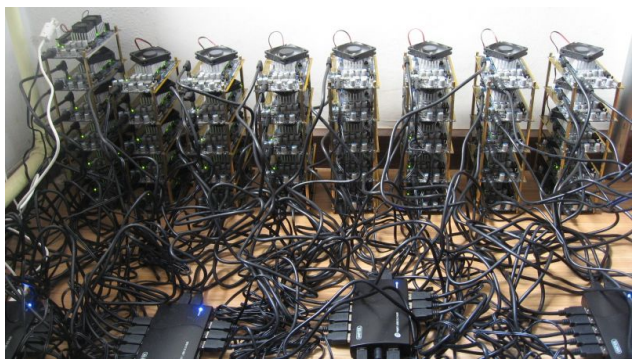
- Inarrêtable car distribuée
- Infalsifiable et auditable



# Miner des Bitcoins

# Miner des Bitcoins

Les “*mineurs*” valident les transactions contre des bitcoins



# Miner des Bitcoins

- Valider = résoudre un **objectif de hachage**
- Récompense initiale 50 BTC pour une validation
- Divisée par 2 tous les 210000 validations

$$\sum_{i=0}^{32} \frac{50}{2^i} \times 210\,000 = 21 \text{ millions BTC}$$

# Bitcoin = Proof of Work

# BitCoin Proof of Work

Target at block 816 377 is
0000000000000000000481940000000000000000000000000000000000000000

Find $n$ such that

$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, n)) = x < \textit{Target}$$

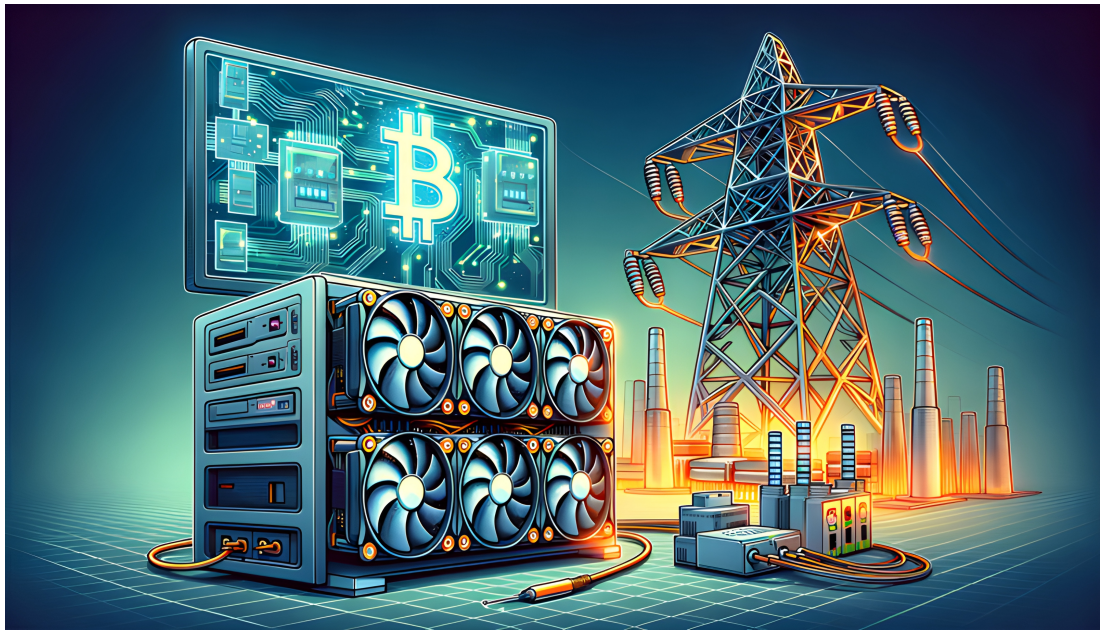
$x$ starts with at least 19 zeros

## Strategy : brute force

Try all possible values for $n$

Initial target was 00000000ffff0000000000000000000000000000000000000000000000000000

# Energyvore




Highly energy consuming in 2023

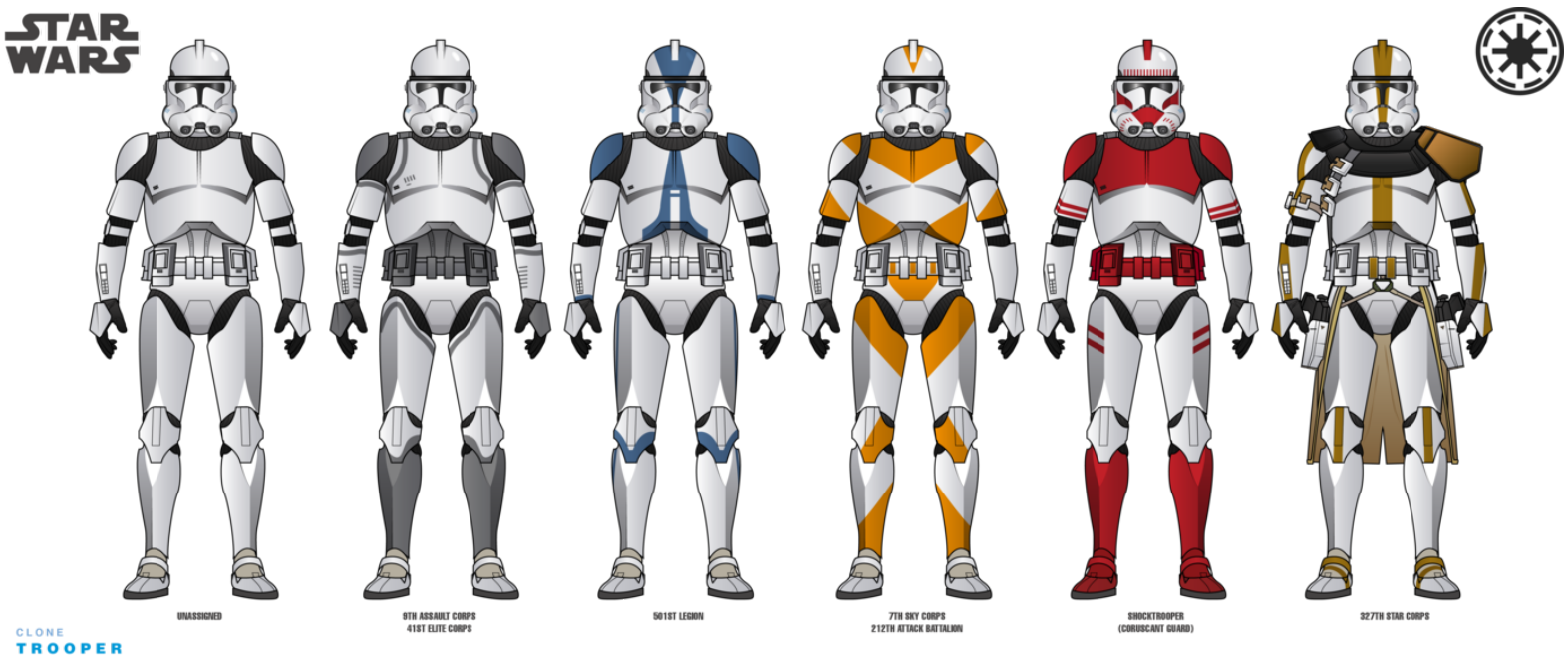
# Proof of Work

- Useless computations

# Other crypto-monnaies

# Classification I : Dumy

# Classification II : Clones of Bitcoin



# Classification III : More useful

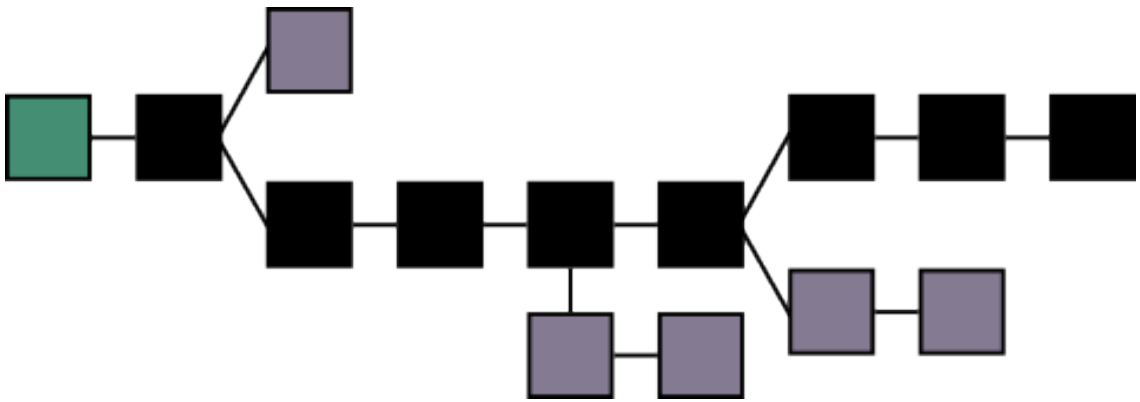


# Classification IV : Other Proofs




Rich get richer !

# Roles of Miners



# Contributions

**Proof of Behavior**

- Paradigm shift
- Incentivization of green behaviors
- EcoMobiCoin

**LCoin**

- Geographical demurage
- Proof of Location

# Related Work

- SolarCoin


*"incentivize solar electricity by rewarding the generators of solar electricity"*

- MobiCoin

16 / 53

# Outline

# Outline

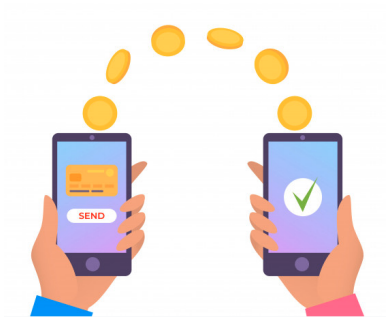
# Proof of Behavior (PoB)

- No specialized hardware required for mining
- Anyone behavior helps to generate coins
- No waste of computational power

# Proof of Behavior (PoB)

- Public blockchain
- Decentralization

3 actors

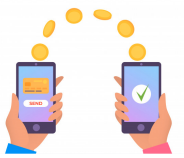



**User**

**Prover**

**Verifier**

# Users

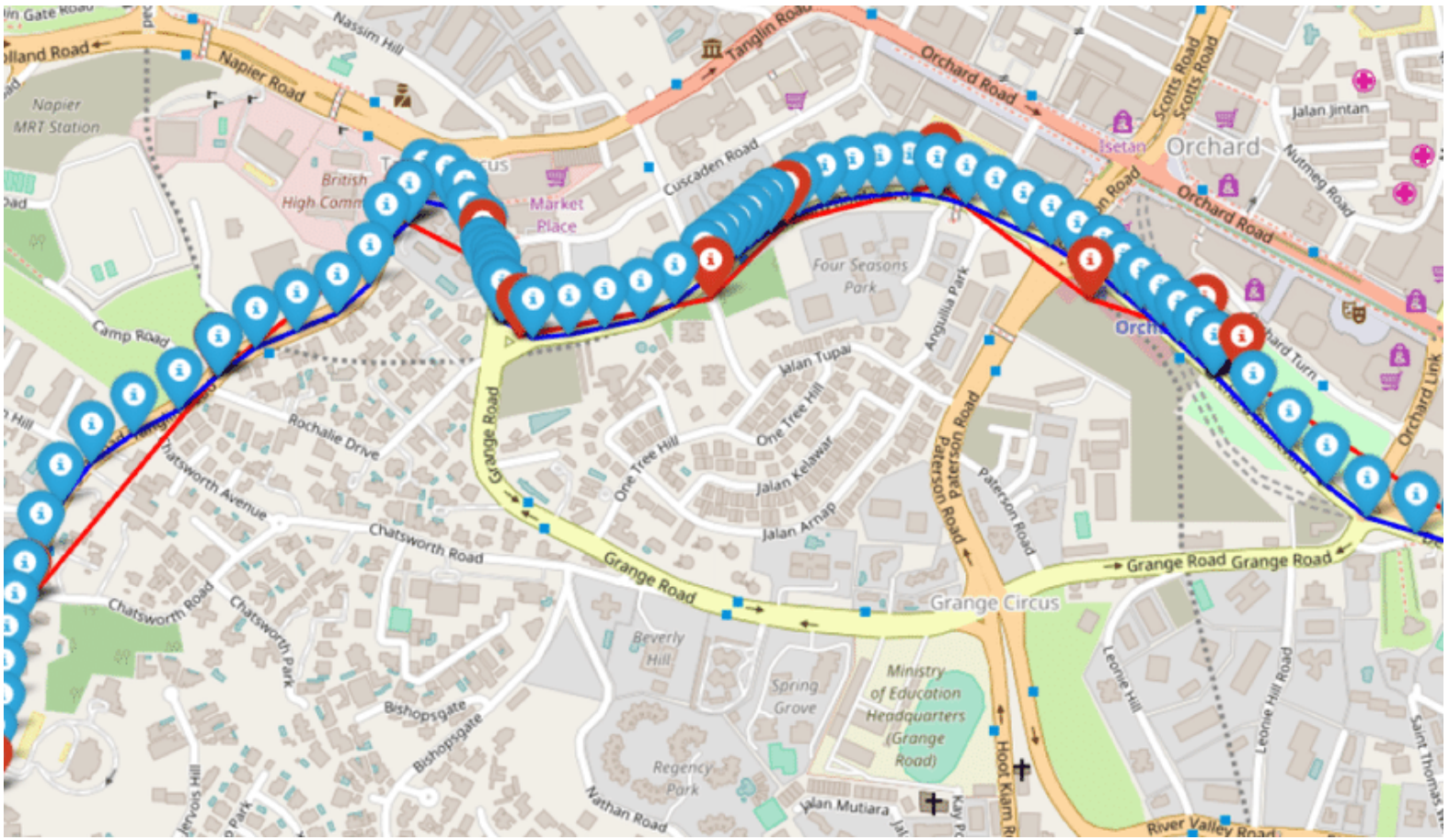


# Provers

Who realize PoB

# Verifiers (Miners)

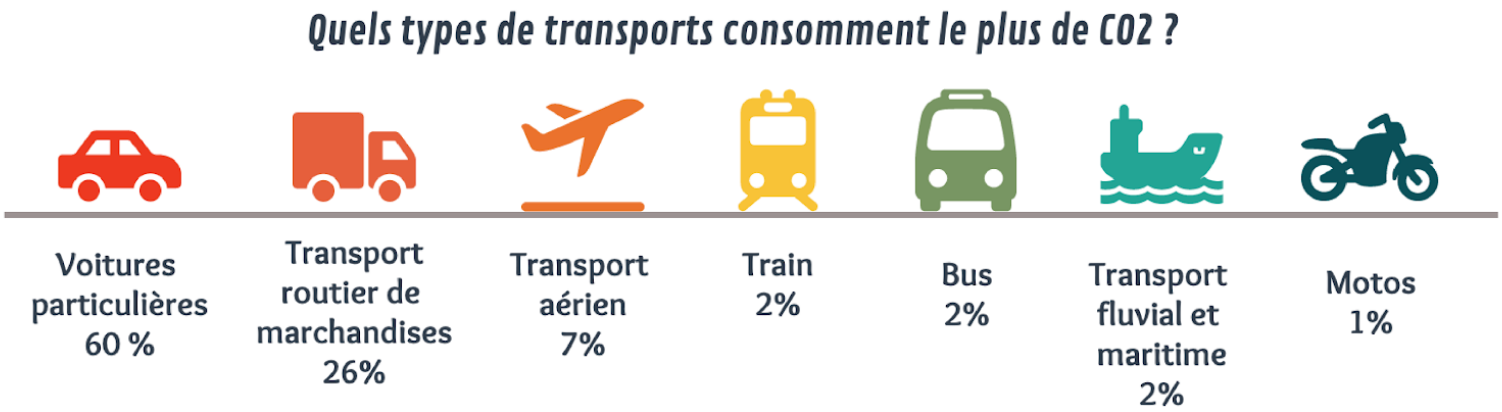
Who verify PoBs and transactions



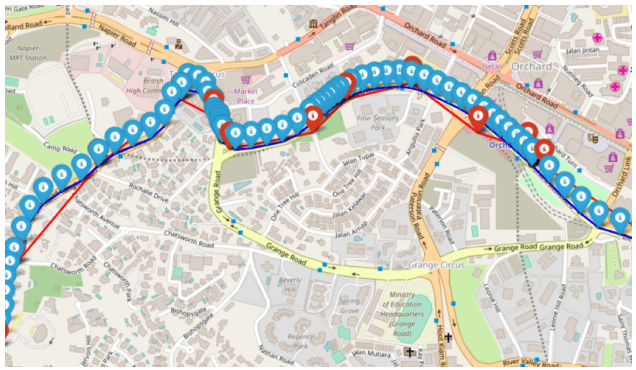

Miners have to perform PoB

# Outline

# Eco Mobility



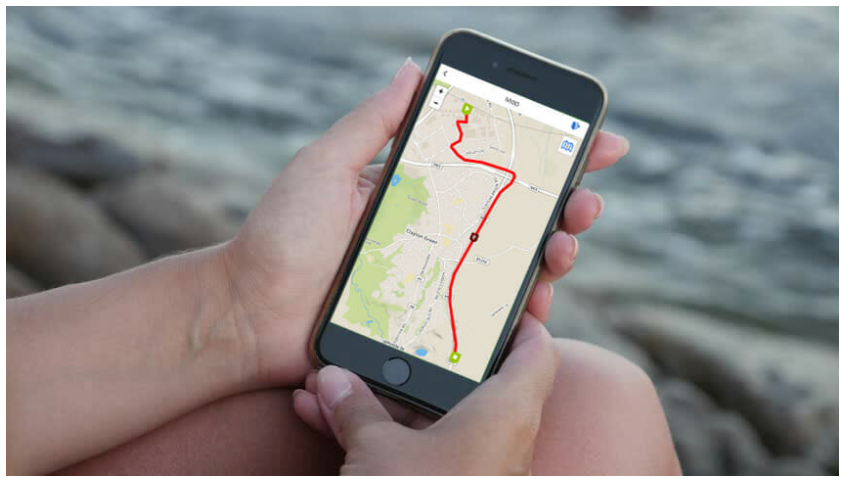
# EcoMobiCoin Proof of Behavior




# EcoMobiCoin Temporal Demurage

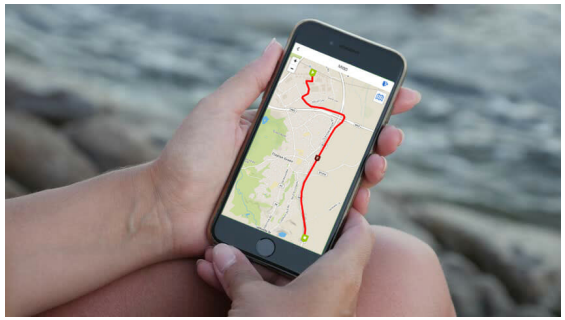
# Ephemeral PoB

# Prover Reward = Distance



# Verifier Reward

- PoB is required

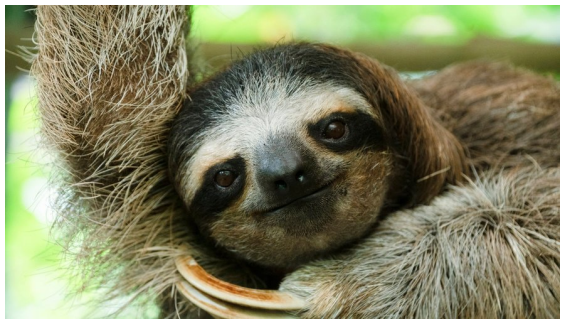


- Check transactions
- Mining = play Lottery

# Verifiable Delay Functions (VDF)

- Rivest, Shamir Wagner 1996 : Time lock Puzzle ($x^{2^T}$)
- Lenstra 2017 Sloth function
- Boneh et al. 2018 : Verifiable Delay Functions $h(h(\ldots h(x)\ldots)$
- Pietrzak 2019 : Simple Verifiable Delay Functions
- Wesolowski 2019 : Efficient Verifiable Delay Functions

# Efficient Verifiable Delay Functions (VDF)



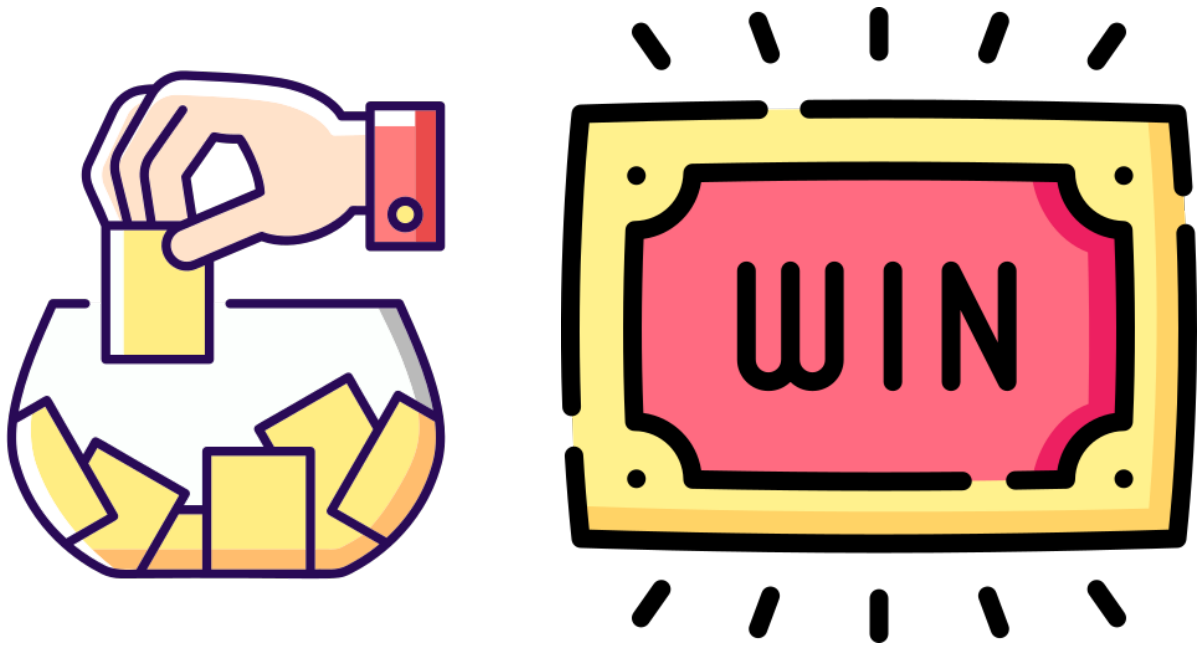
- Alice wants to prove to Bob that $y = x^{2^T}$
- Bob picks a random large prime $p$
- Alice finds $q$ and $r$ such that : $2^T = qp + r$, $0 \leq r < p$ and sends $\pi = x^q$
- Bob Computes $r = 2^T \bmod l$ and accepts if $\pi^p x^r = y$

Fiat-Shamir : Non interactive with $p = nextprime(H(x, y, T))$

Proposed by Benjamin Wesolowski at Eurocrypt 2019

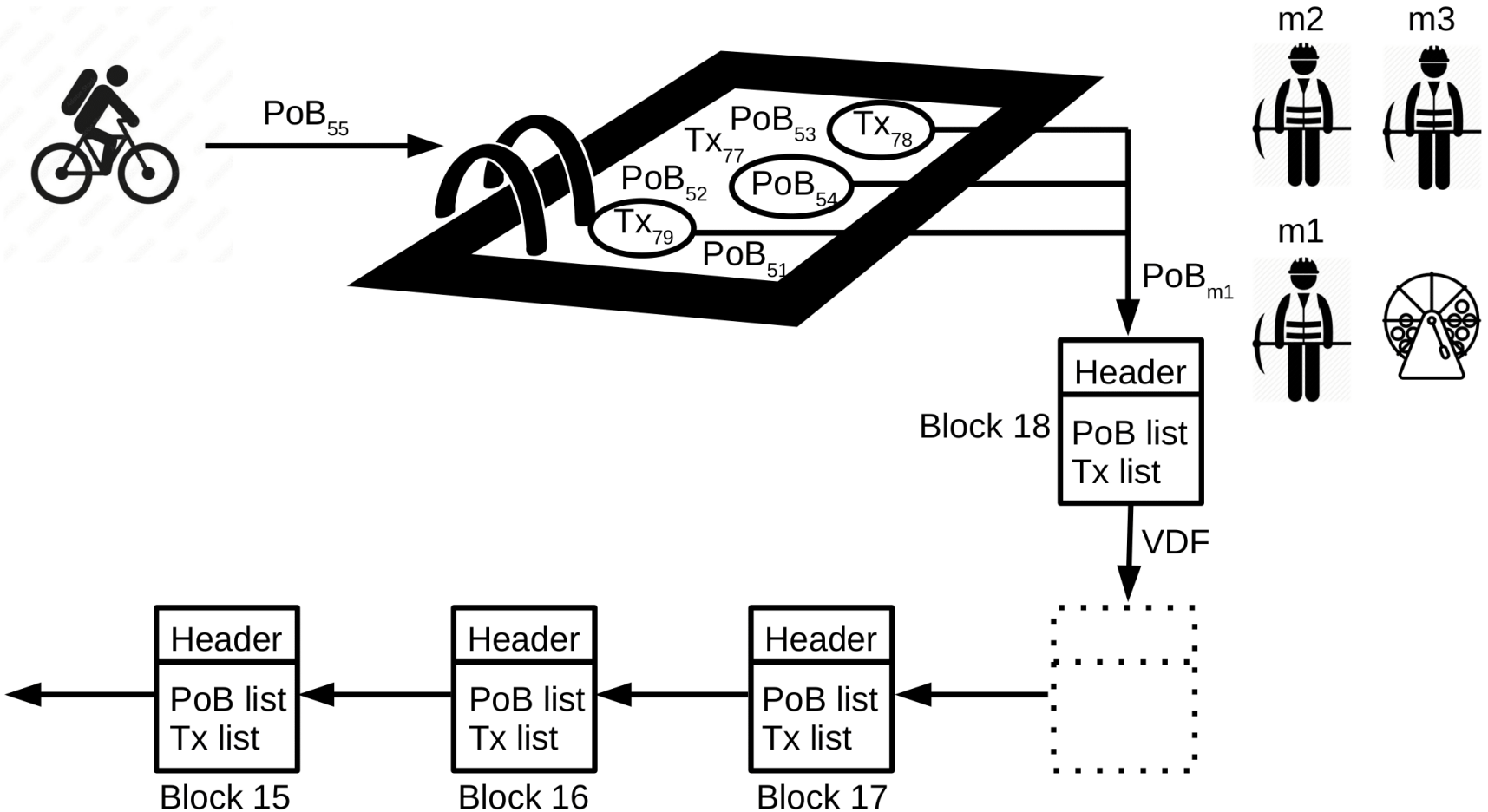
# Lottery for miners

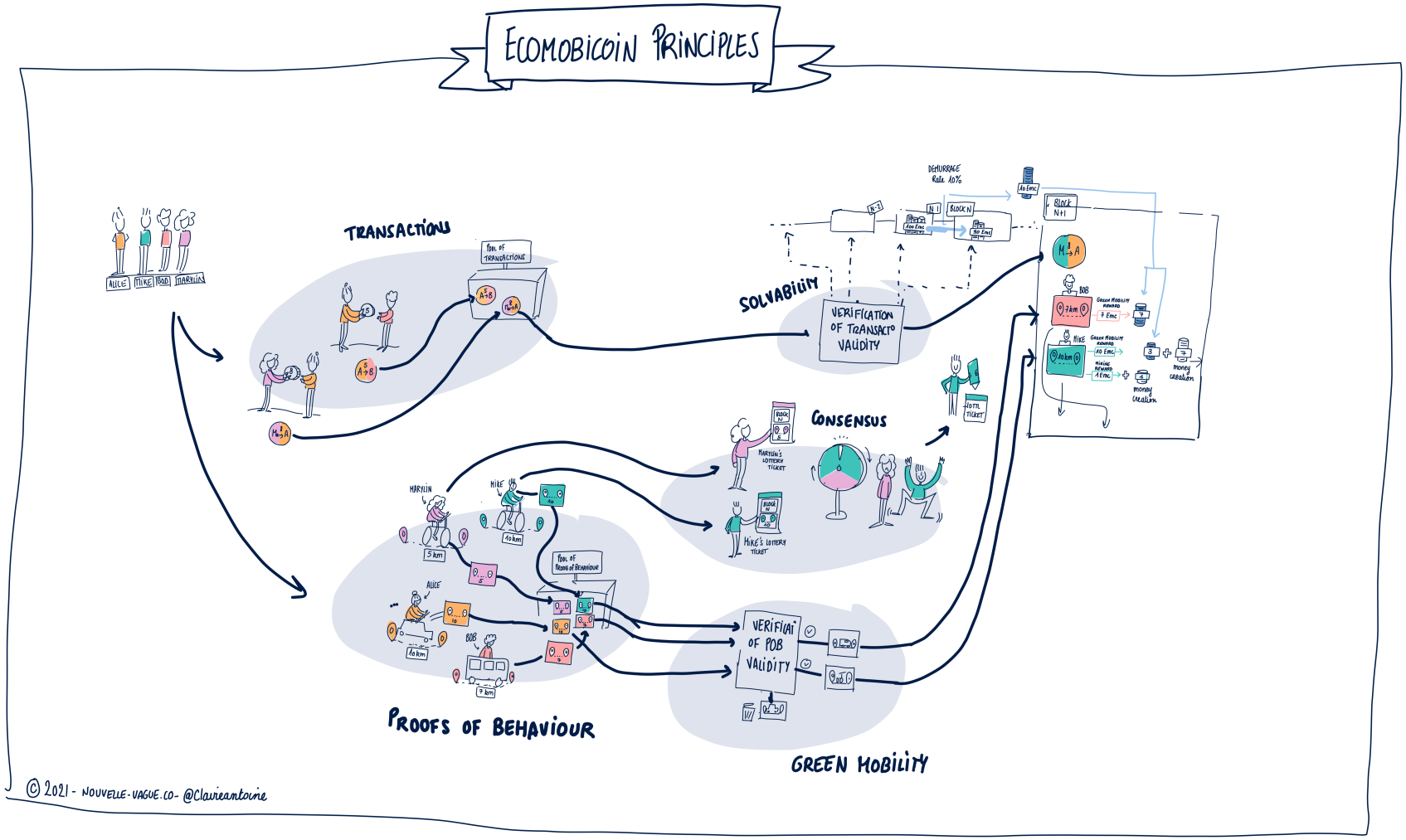
VDF(PoB) gives proof of computation time




The faster wins !

# Blockchain Mining

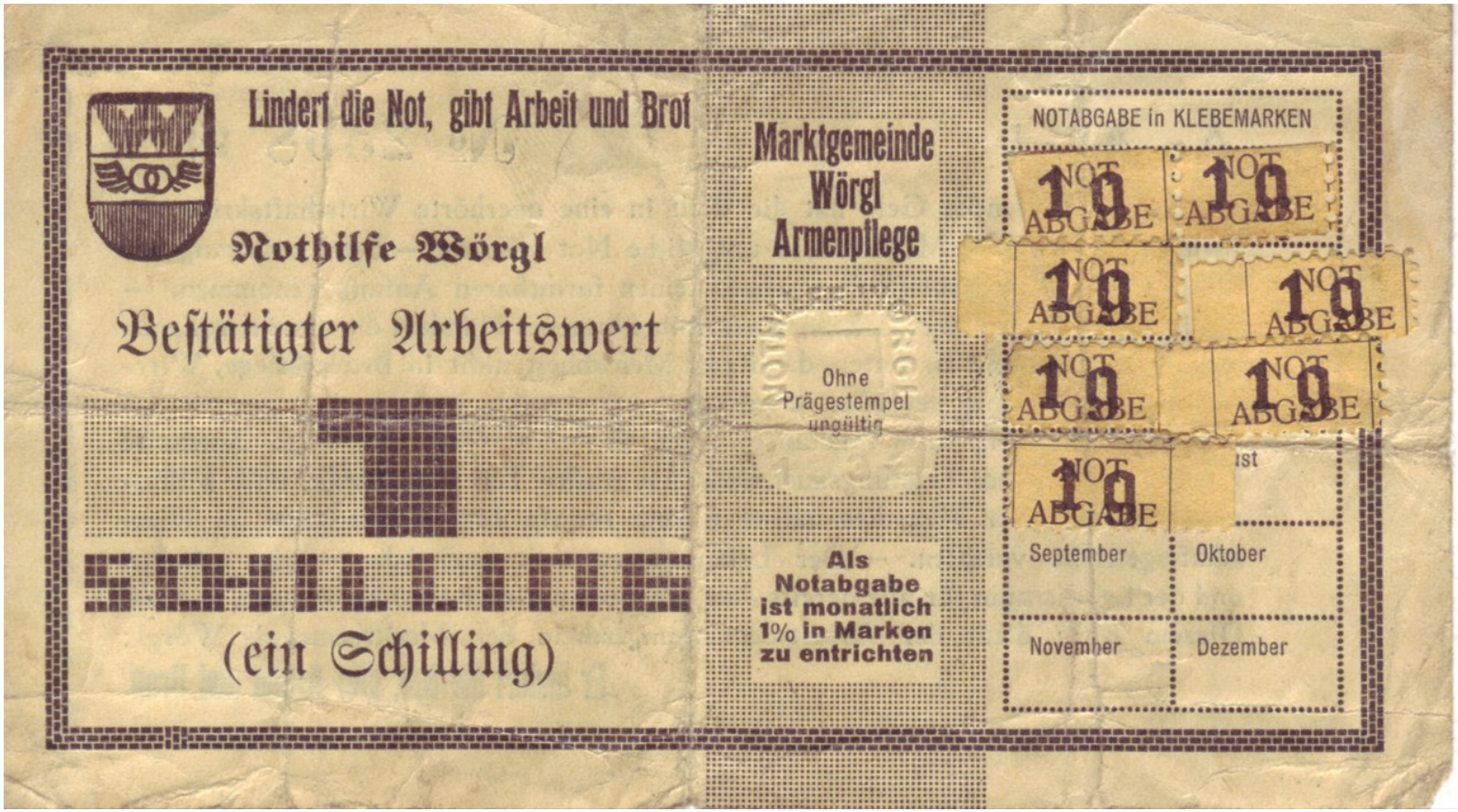





https://ecomobicoin.limos.fr

# Outline

# Local Currency in Wörgl, Austria

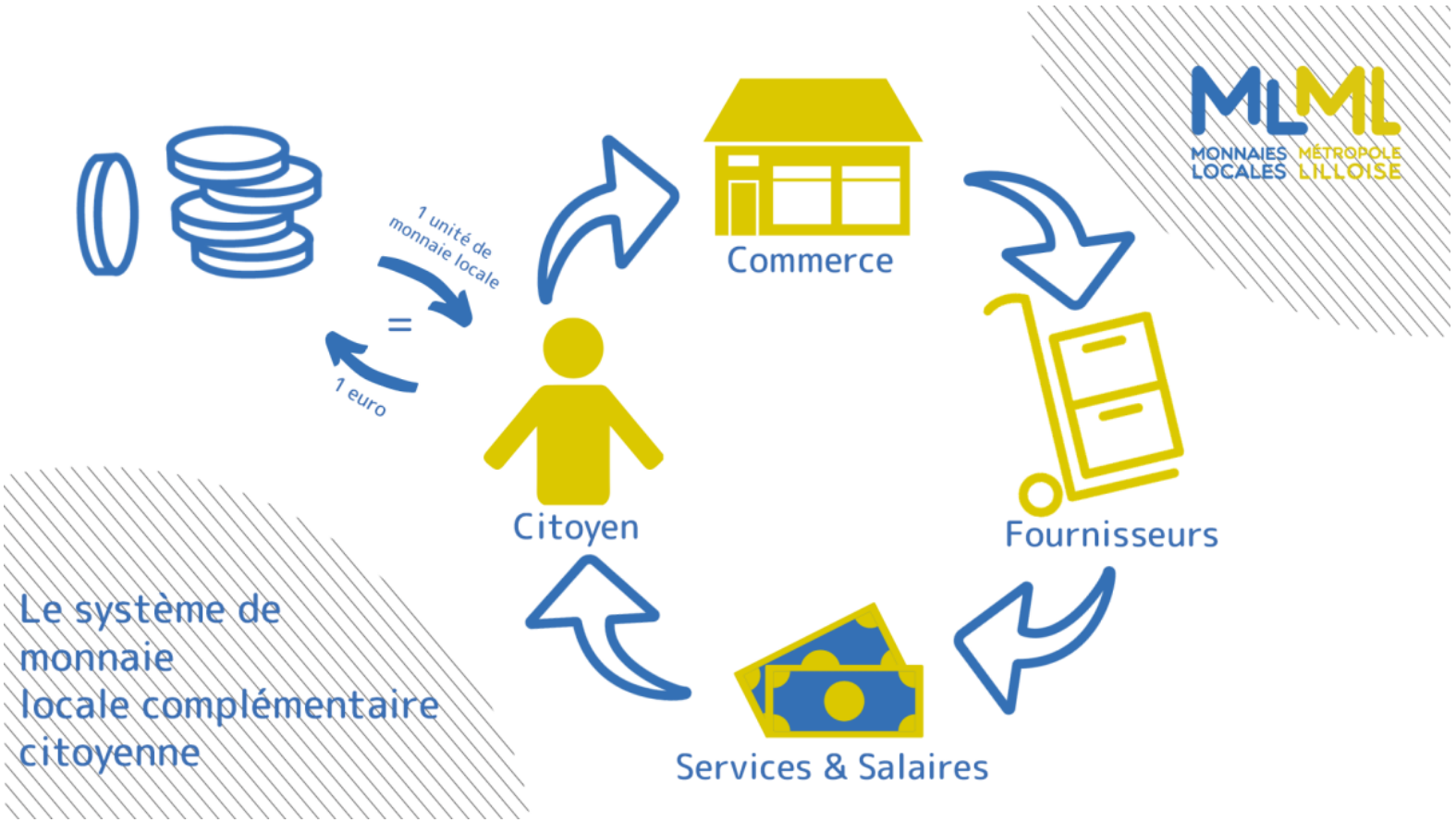



Temporal Demurrage

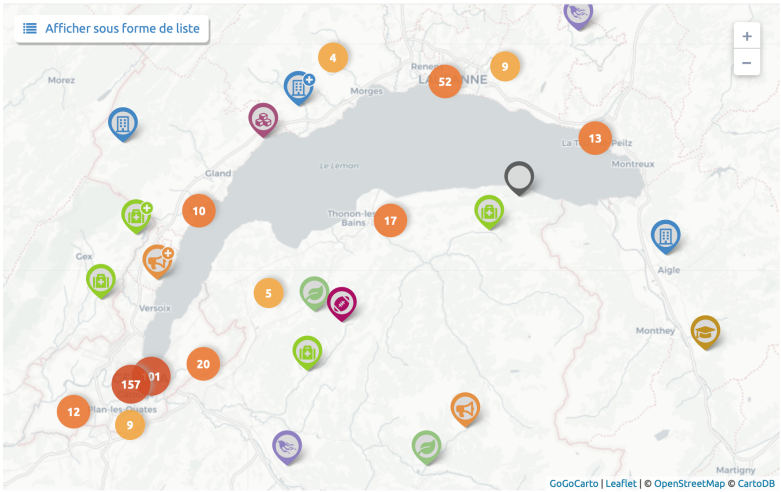
# Temporal Demurrage: Ticket Restaurant, France

# French Local Currencies

# Local Currency



# Léman: Local Cryptocurrency



Using blockchain (Proof of Work)

# Our idea I: Restricted Area

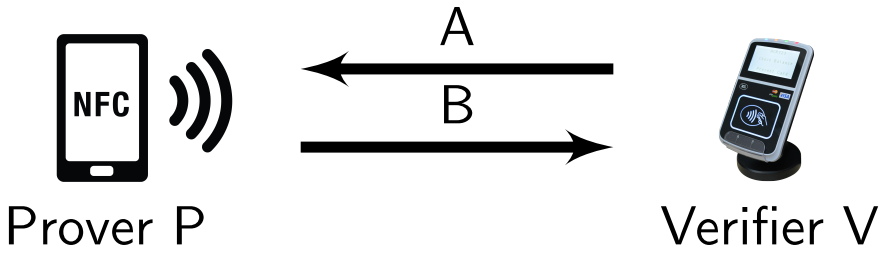
**Proxymity certificate** delivered by Affiliated Local Shops

Proof that Alice and Bob are simutaneously in the "same" location

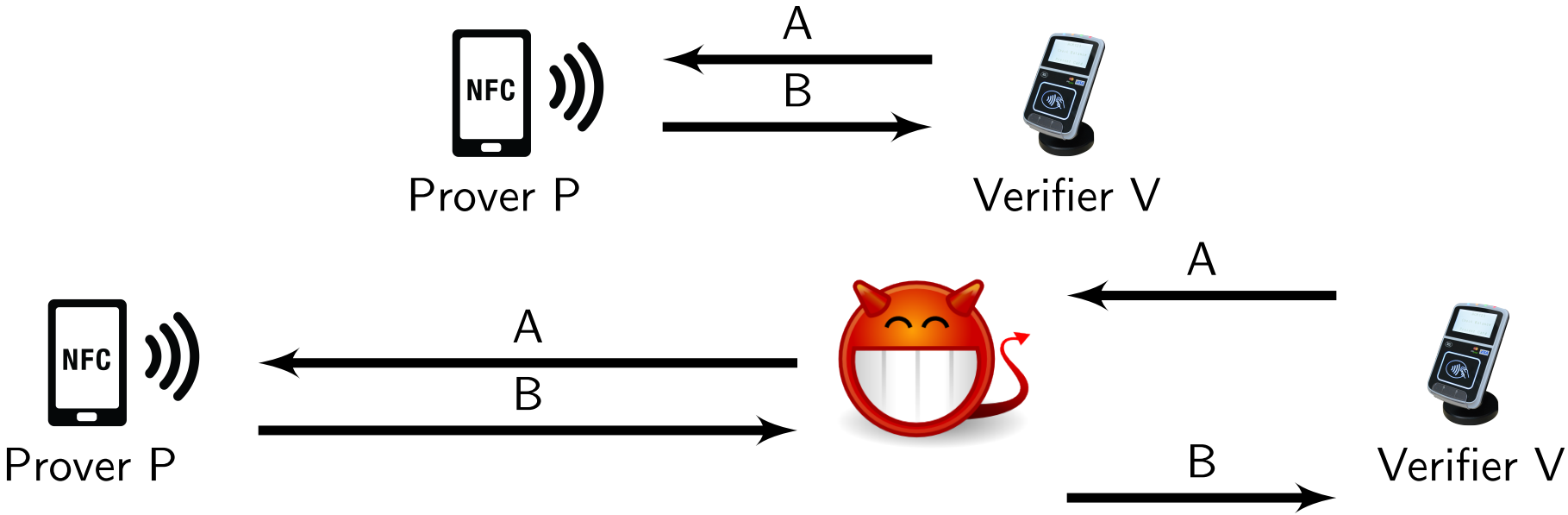
Distance Bounding Protocol

Limited duration of Proximity certificate

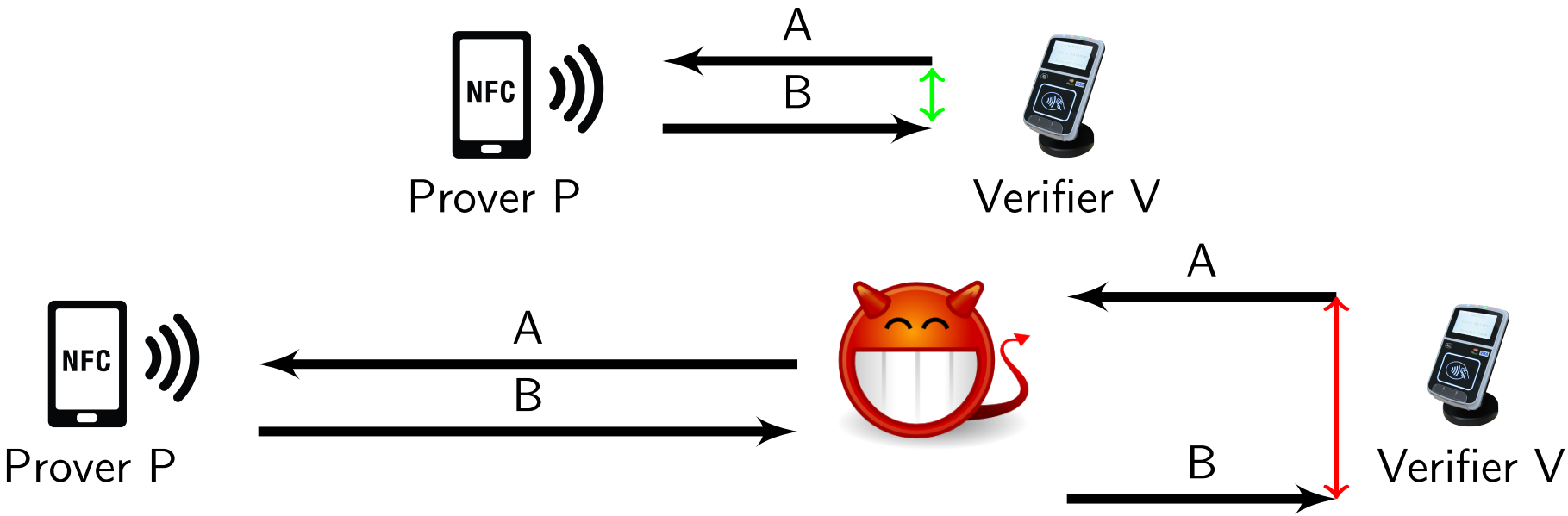
# Distance Bounding

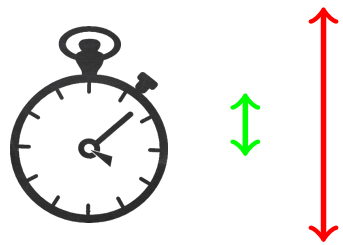


# Distance Bounding



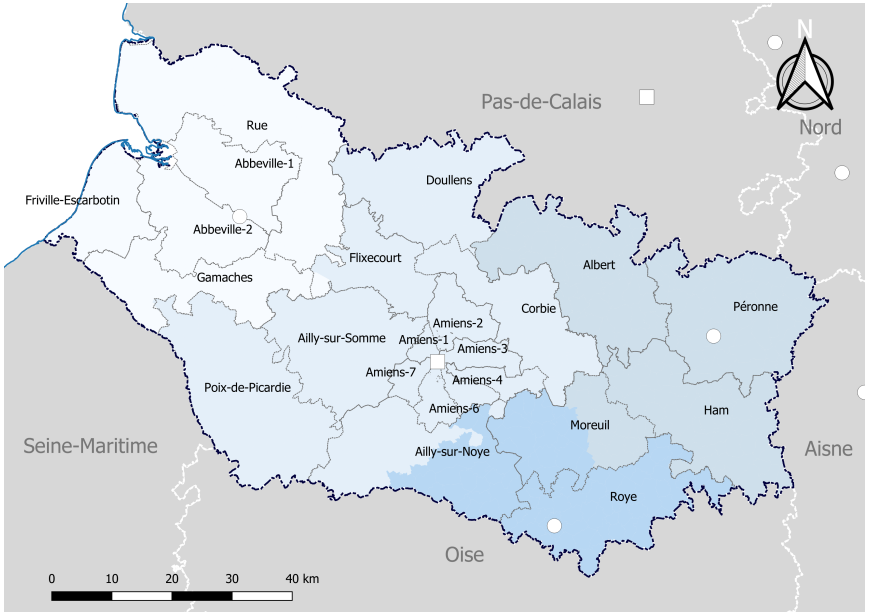
# Distance Bounding

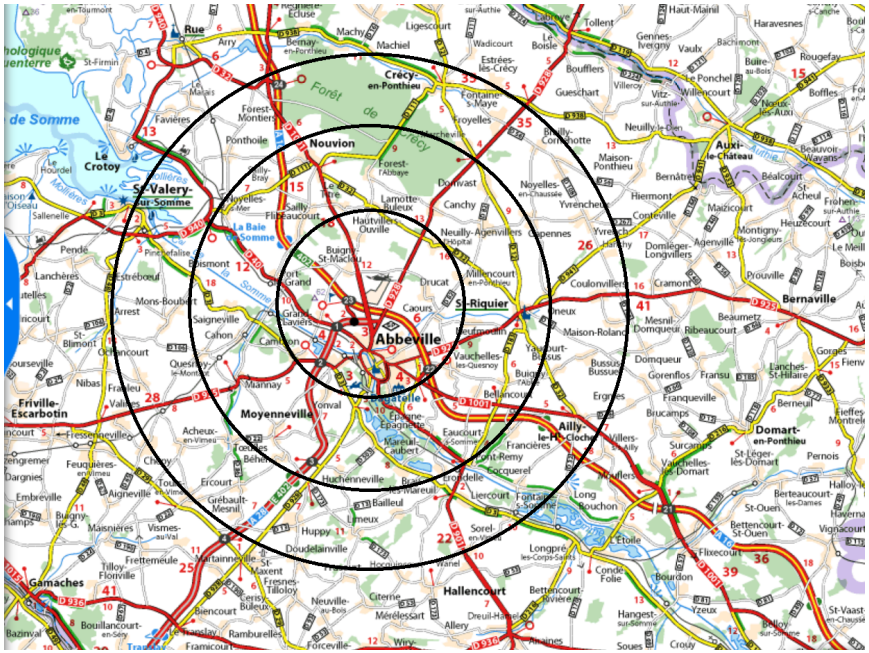


Solution: distance bounding (Brands and Chaum, 1991)

# Our idea I: Geographic Demurrage



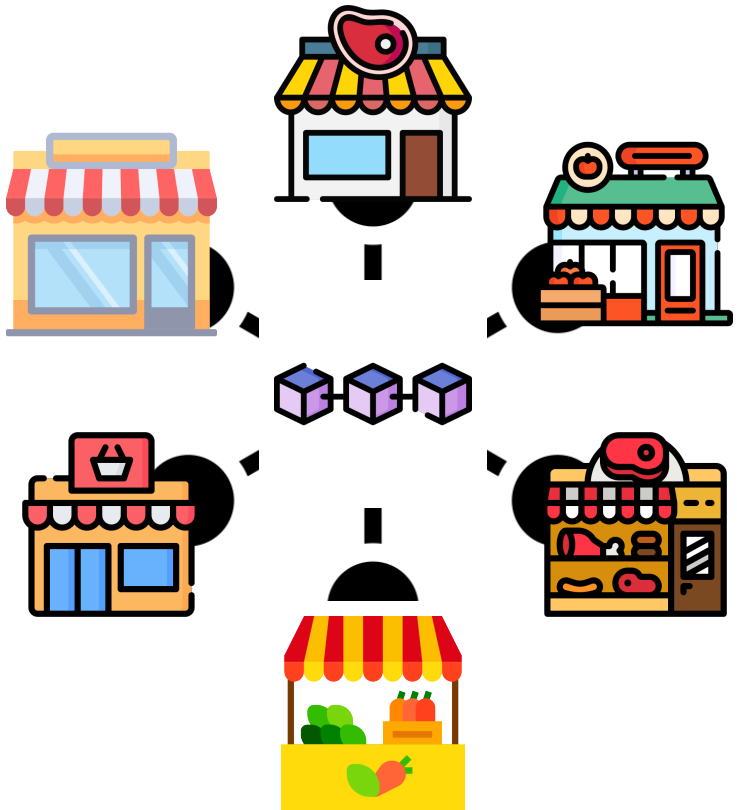



# 2 options : $2^2 = 4$ possibilities

| |  Restricted Area |  Geographical Demurrage |
|---|---|---|
| **Simple** | ✗ | ✗ |
| **Restricted** | ✓ | ✗ |
| **LCoin** | ✗ | ✓ |
| **Perfect** | ✓ | ✓ |

# **Simple**: *X* Restricted Area *X* Geographical Demurrage

Permissionned blockchain

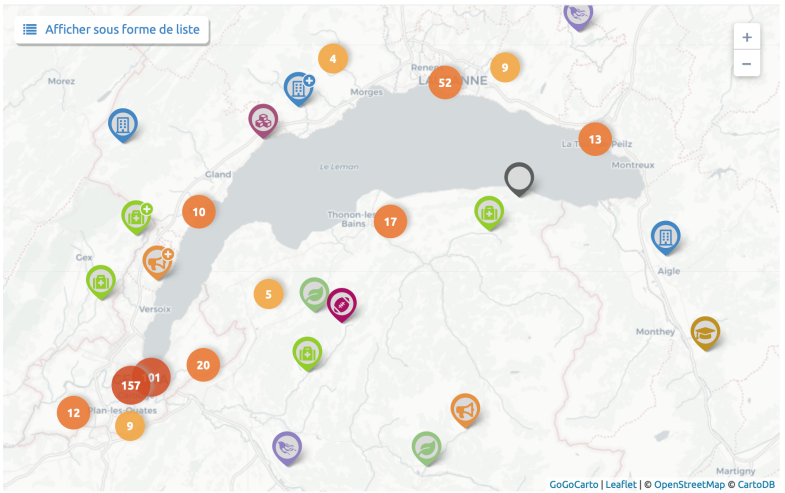



Miners = Affiliated Shops

Unrestricted Area & Trust in Affiliated Shops

# **Restricted**: ✓ Restricted Area ✗ Geographical Demurrage

Proxymity certificate delivered by Affiliated Local Shops using DB

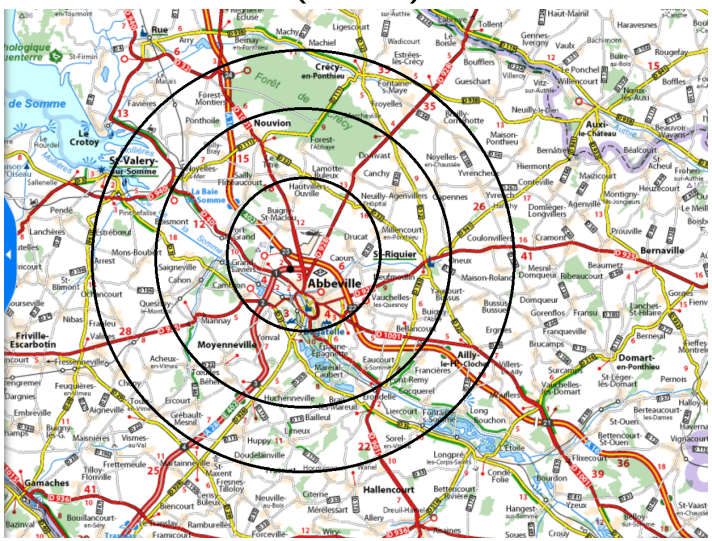



Limited duration

Proof of local expenses

# **LCoin**: ✗ Restricted Area ✓ Geographical Demurrage

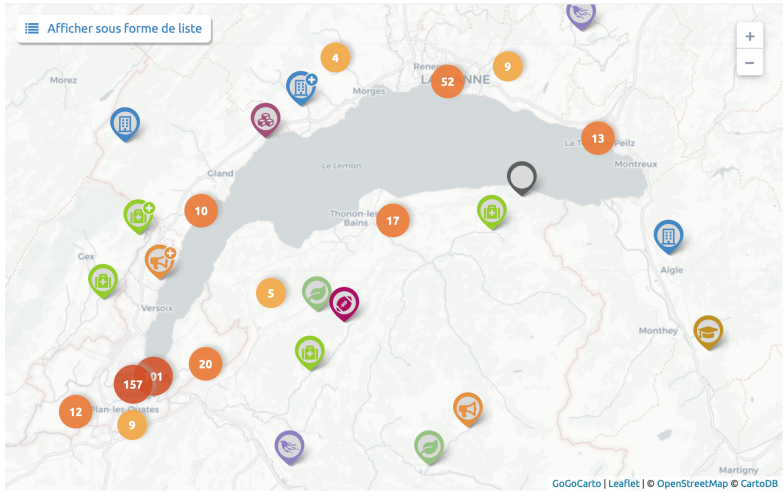
Coins have Point of Attachment (PoA) and a timestamp



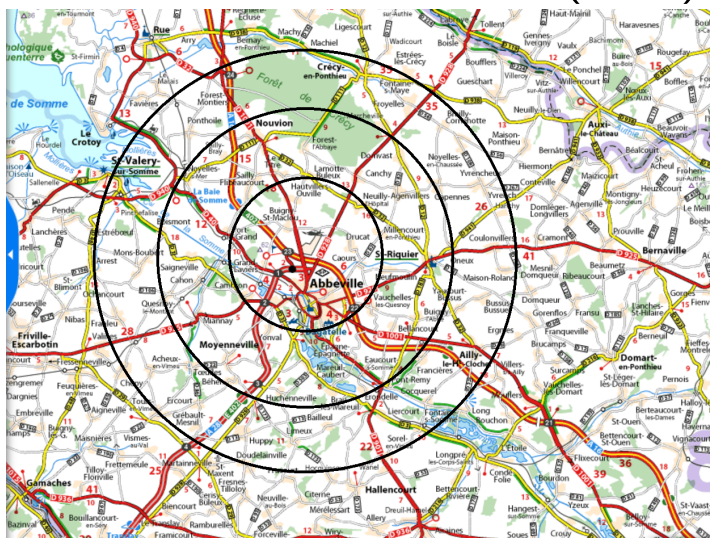

Value : Proportional to the distance

# **Perfect**: ✓ Restricted Area ✓ Geographical Demurrage

Proxymity certificate delivered by Affiliated Local Shops using DB




Value : Coins are have Point of Attachment (PoA) and a timestamp



# Outline

# Conclusion

- Proof of Behavior
- Geographic Demurrage
- Proof of Attachement

EcoMobiCoin & LCoin

`https://ecomobicoin.limos.fr/`

**Thanks for your attention**

Questions ?


pascal.lafourcade@uca.fr