

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

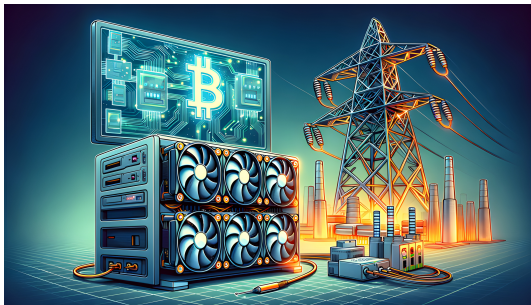
FIC 2024



Bitcoin = Proof of Work



Energyvore



Highly energy consuming in 2023

Proof of Work

- ▶ Useless computations



Other crypto-monnaies

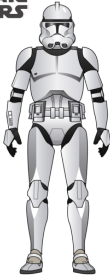


Classification I : Domy



Classification II : Clones of Bitcoin

STAR
WARS



STANDARD



6TH AIRSPEED CORPS
41ST CLONING



501ST LEGION



7TH SKY CORPS
21ST AIRBORNE



99TH ASSAULT
BATTALION



107TH STAR CORPS



CLONE
TROOPER

Classification III : More useful

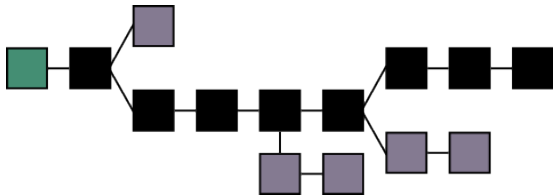
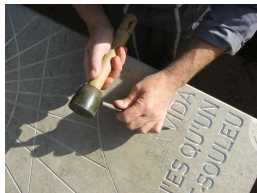


Classification IV : Other Proofs



Rich get richer !

Roles of Miners



Contributions

Proof of Behavior

- ▶ Paradigm shift
- ▶ Incentivization of green behaviors
- ▶ EcoMobiCoin

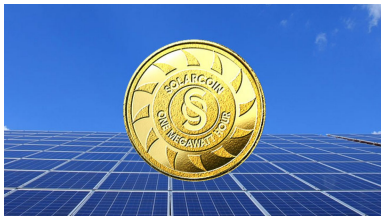


LCoin

- ▶ Geographical demurage
- ▶ Proof of Location

Related Work

- ▶ SolarCoin



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

- ▶ MobiCoin



Outline

Motivations

Proof of Behavior

EcoMobiCoin

LCoin

Conclusion

Outline

Motivations

Proof of Behavior

EcoMobiCoin

LCoin

Conclusion

Proof of Behavior (PoB)

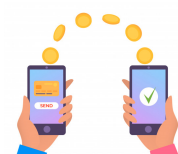


- ▶ No specialized hardware required for mining
- ▶ Anyone behavior helps to generate coins
- ▶ No waste of computational power

Proof of Behavior (PoB)

- ▶ Public blockchain
- ▶ Decentralization

3 actors



User



Prover



Verifier

Users



Provers



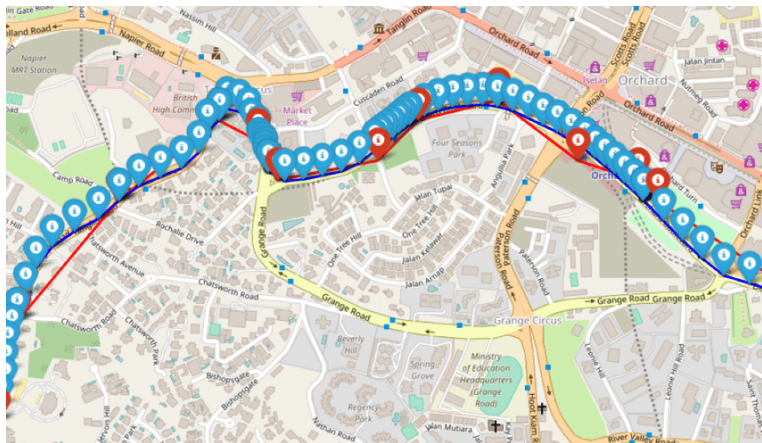
Who realize PoB



Verifiers (Miners)



Who verify PoBs and transactions



Miners have to perform PoB

Outline

Motivations

Proof of Behavior

EcoMobiCoin

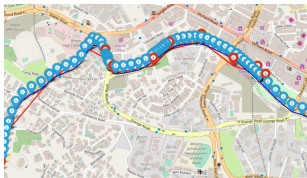
LCoin

Conclusion

Quels types de transports consomment le plus de CO2 ?



EcoMobiCoin Proof of Behavior



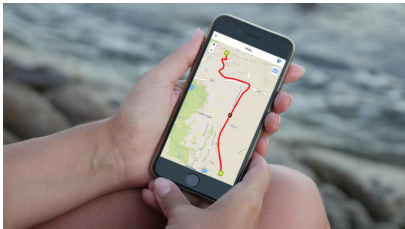
EcoMobiCoin Temporal Demurage



Ephemeral PoB

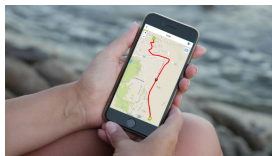


Prover Reward = Distance



Verifier Reward

- ▶ PoB is required



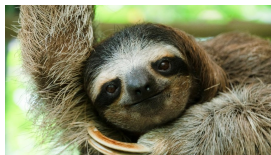
- ▶ Check transactions
- ▶ Mining = play Lottery



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 $h(h(\dots h(x)\dots))$
- ▶ Pietrzak 2019 : Simple Verifiable Delay Functions
- ▶ Wesolowski 2019 : Efficient Verifiable Delay Functions

Efficient Verifiable Delay Functions (VDF)



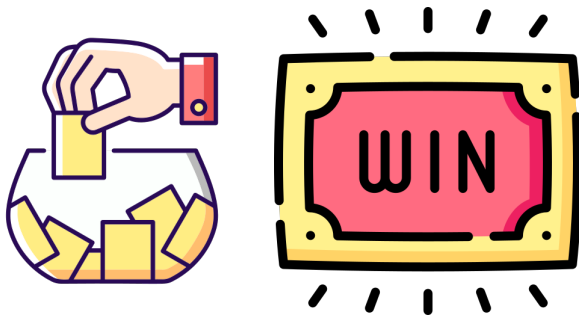
- ▶ Alice wants to prove to Bob that $y = x^{2^T}$
- ▶ Bob picks a random large prime p
- ▶ Alice finds q and r such that : $2^T = qp + r$, $0 \leq r < p$ and sends $\pi = x^q$
- ▶ Bob Computes $r = 2^T \bmod p$ and accepts if $\pi^p x^r = y$

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

Proposed by Benjamin Wesolowski at Eurocrypt 2019

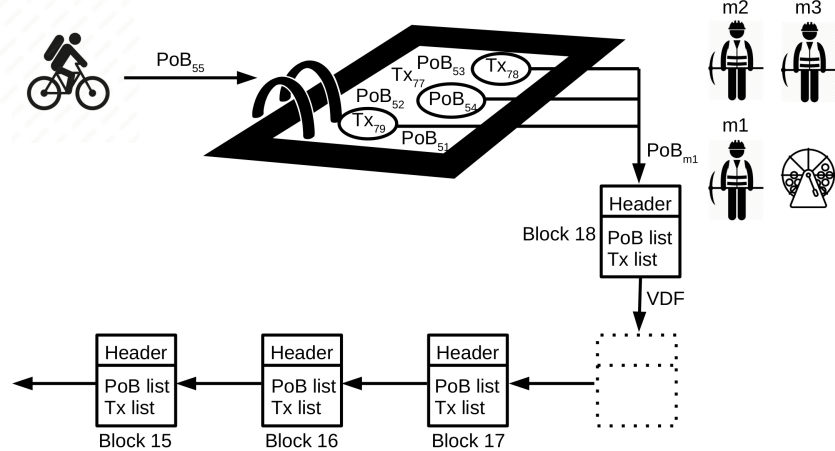
Lottery for miners

VDF(PoB) gives proof of computation time

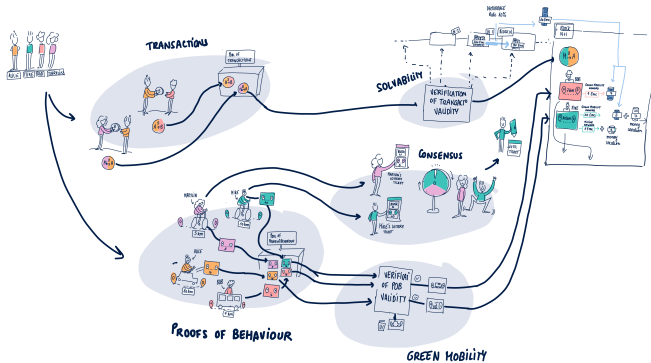


The faster wins !

Blockchain Mining



ECOMOBICOIN PRINCIPLES



© 2021 - HOUVELLE-VOIE CO - @ChloéAntoine

<https://ecomobitcoin.limos.fr>



Outline

Motivations

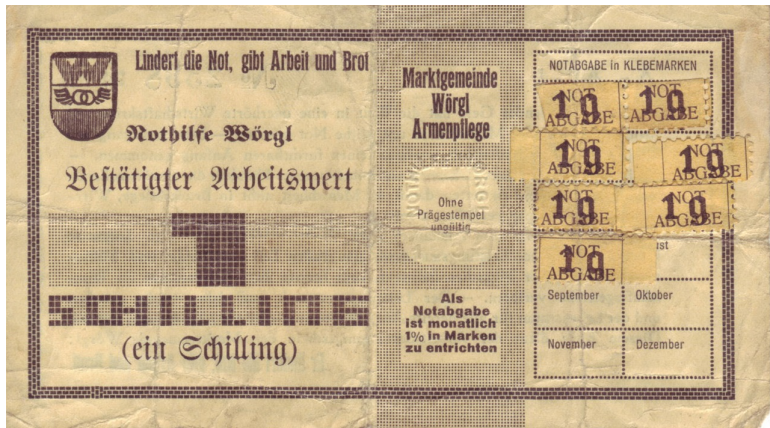
Proof of Behavior

EcoMobiCoin

LCoin

Conclusion

Local Currency in Wörgl, Austria



Temporal Demurrage

Temporal Demurrage: Ticket Restaurant, France

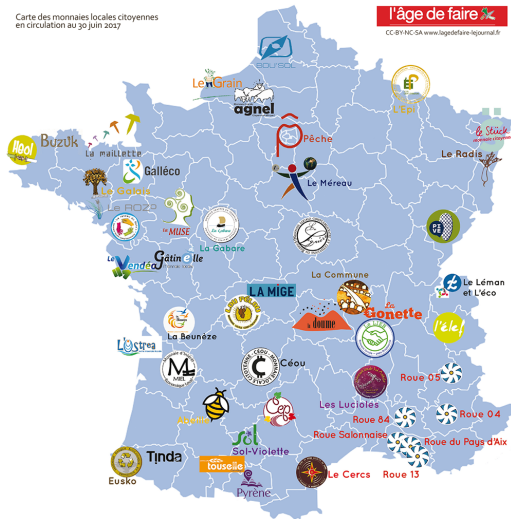


French Local Currencies

Carte des monnaies locales citoyennes
en circulation au 30 juin 2017

l'âge de faire

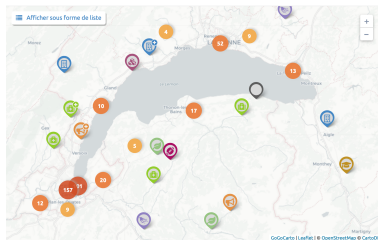
CC-BY-NC-SA www.lagedefaire-lejournal.fr



Local Currency



Léman: Local Cryptocurrency



Using blockchain (Proof of Work)

Our idea I: Restricted Area

Proximity certificate delivered by Affiliated Local Shops



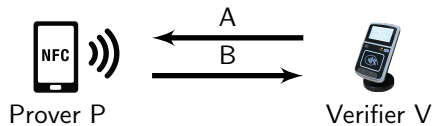
Proof that Alice and Bob are simultaneously in the “same” location



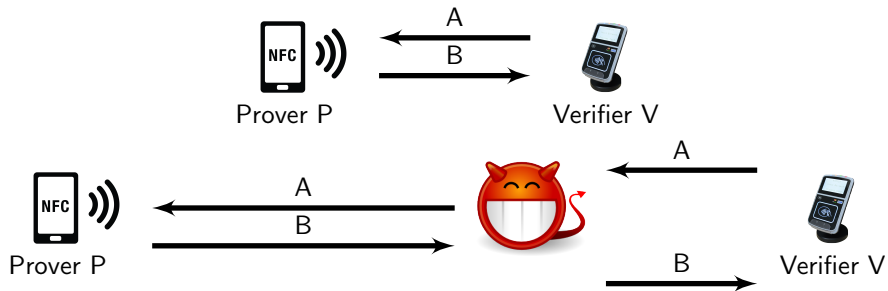
Distance Bounding Protocol

Limited duration of Proximity certificate

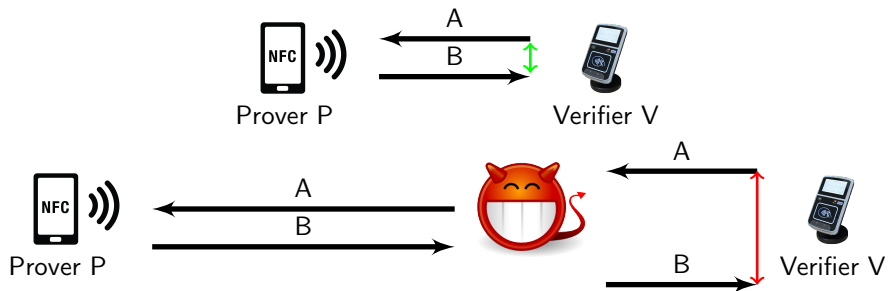
Distance Bounding



Distance Bounding



Distance Bounding





Solution: distance bounding (Brands and Chaum, 1991)

Our idea I: Geographic Demurrage



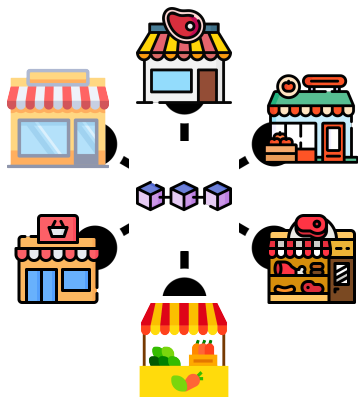
2 options : $2^2 = 4$ possibilities

	 Restricted Area	 Geographical Demurrage
Simple	X	X
Restricted	✓	X
LCoin	X	✓
Perfect	✓	✓



Simple: X Restricted Area X Geographical Demurrage

Permissioned blockchain



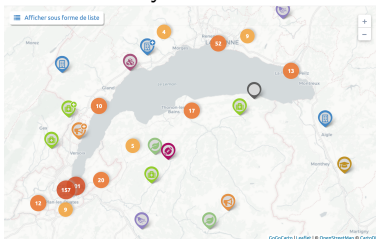
Miners = Affiliated Shops

Unrestricted Area & Trust in Affiliated Shops

Restricted: ✓ Restricted Area ✗ Geographical Demurrage



Proximity certificate delivered by Affiliated Local Shops using DB



Limited duration

Proof of local expenses

LCoin: ✗ Restricted Area ✓ Geographical Demurrage

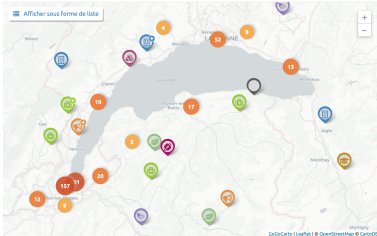
Coins have Point of Attachment (PoA) and a timestamp



Value : Proportional to the distance

Perfect: ✓ Restricted Area ✓ Geographical Demurrage

Proximity certificate delivered by Affiliated Local Shops using DB



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



Outline

Motivations

Proof of Behavior

EcoMobiCoin

LCoin

Conclusion

Conclusion



- ▶ Proof of Behavior
- ▶ Geographic Demurrage
- ▶ Proof of Attachment

EcoMobiCoin & LCoin

<https://ecomobicoin.limos.fr/>

Thanks for your attention

Questions ?

Les
**BLOCK
CHAINS**

EN 50 QUESTIONS

Comprendre le fonctionnement et les enjeux
de cette technologie innovante



pascal.lafourcade@uca.fr