

Proof of Behavior

Pascal Lafourcade



Africacrypt 2025
Rabat, Tunisia

Outline

Bitcoin

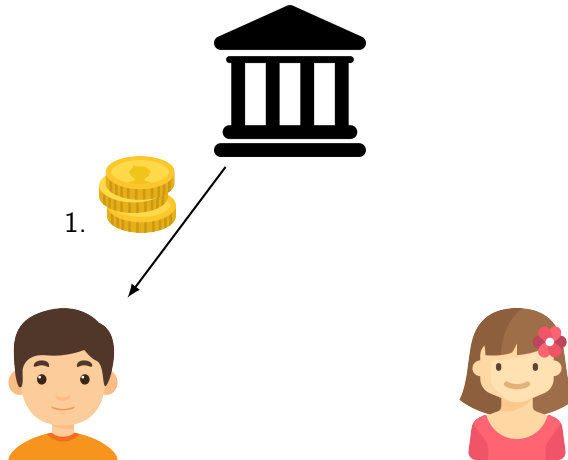
Proof of Behavior

EcoMobiCoin

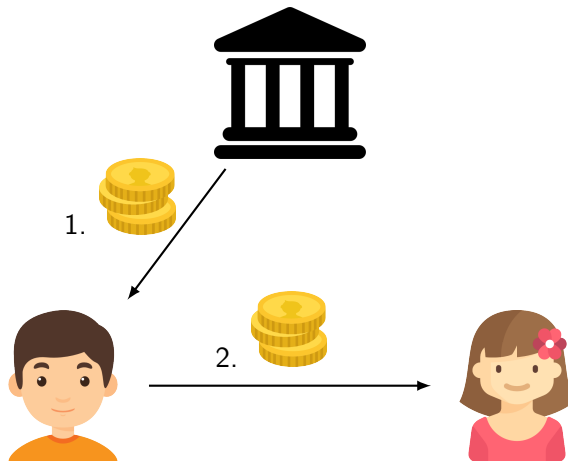
LCoin

Conclusion

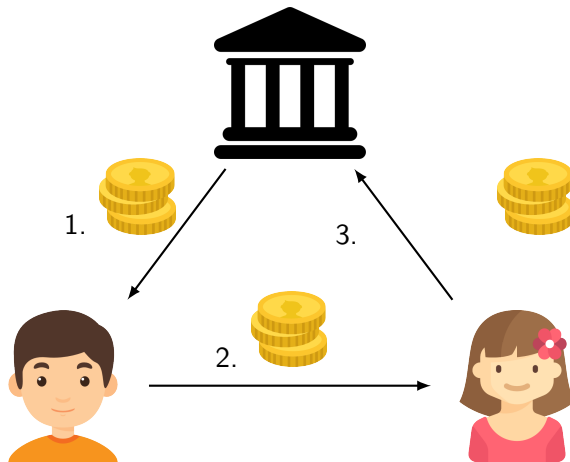
Central Bank



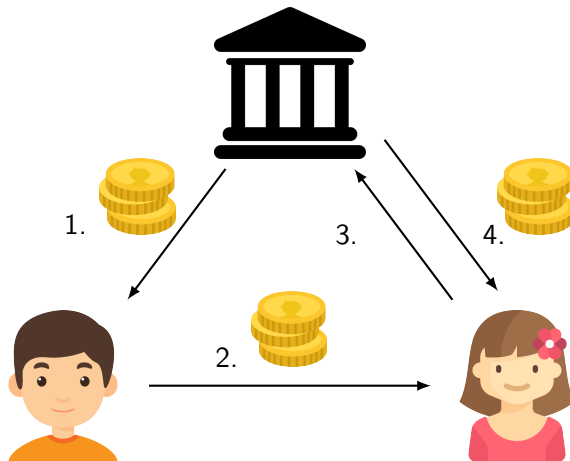
Central Bank



Central Bank



Central Bank



1988 : Digtcash

Untraceable Electronic Cash †
(Extended Abstract)

David Chaum¹ Amos Fiat² Moni Naor³

¹ Center for Mathematics and Computer Science

² Tel-Aviv University

³ IBM Almaden Research Center

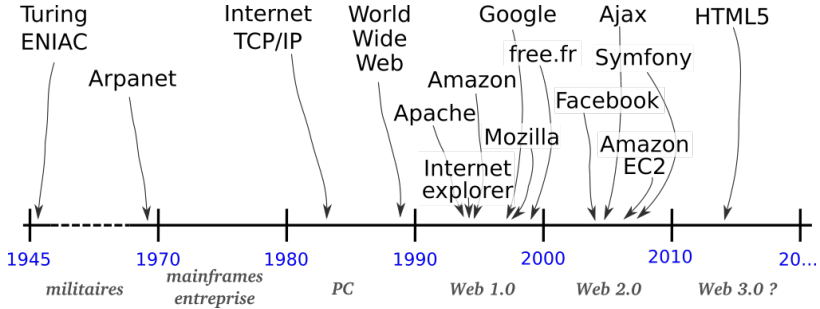


David Chaum

CRYPTO 1988

DigiCash™

Not ready !



LIMOS

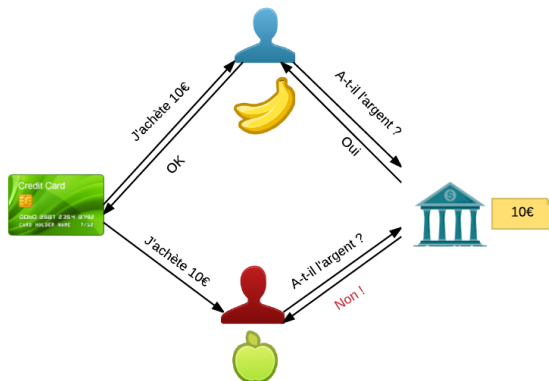
LABORATOIRE D'INFORMATIQUE,
DE MODELISATION ET D'OPTIMISATION DES SYSTEMES



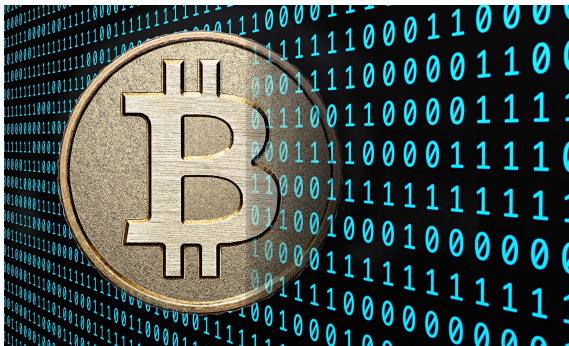
Property : Unforgeable



Property : Avoid double spending



Bitcoin 2009



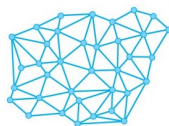
► Crypto-currency decentralised and distributed



Système centralisé



Système décentralisé



Système distribué

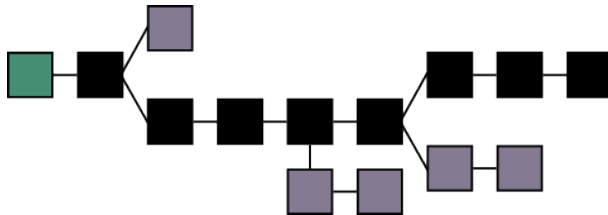


21 millions BTC

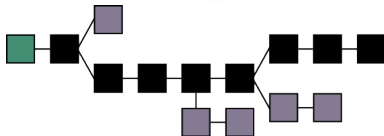
Unstopable



Infalsifiable



Auditable



Bitcoin

2009 by Satoshi Nakamoto

1 BTC $\approx$ 104 257 € 14 july 2025

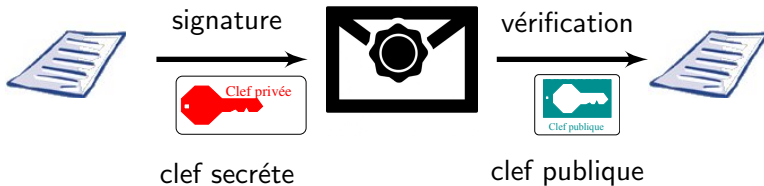


1	BTC = 1 Bitcoin	
0,01	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
0,001	BTC = 1 mBTC	= 1 milliBitcoin
0,000 001	BTC = 1 μ BTC	= 1 microBitcoin
0,000 000 000 000 000 001	BTC = 1 Satoshi	



LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Signature



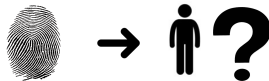
ECDSA

Hash Function (RIPEMD-160, SHA-256, SHA-3)



Security Properties

- ▶ Pré-image



- ▶ Second Pré-image

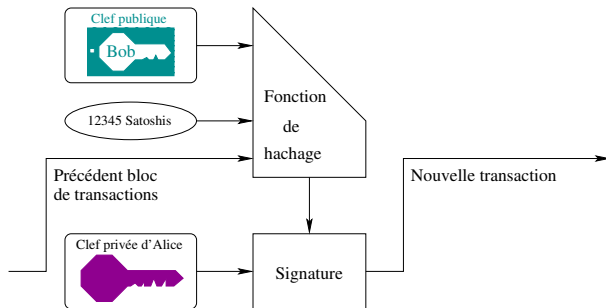


- ▶ Collision



A transaction

Alice gives 12345 Satoshis to Bob.



Unspent Transaction Output UTXO

Mining Bitcoins



Mining Bitcoins



“Miners” valid transactions to generate bitcoins



Mining

- ▶ Valid = solve hash target
- ▶ Reward 50 BTC for one validation
- ▶ Divided by 2 every 210000 validations

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



Miner : Objectif de hachage

Target for the block 816 377 (February 2024)

[illegible]

Find n such that

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

Broken Cryptography which Impacts ?

- ▶ Hash function SHA256
 - ▶ Collision $\Rightarrow$ Steal and destroy coins
 - ▶ Second pre-image $\Rightarrow$ Double spend and steal coins
 - ▶ Pre-image $\Rightarrow$ Complete failure of the blockchain
- ▶ RIPEMD160 : Repudiate payments
- ▶ Signature ECDSA : Selective forgery $\Rightarrow$ Steal coins from public key

When The “Crypto” in Cryptocurrencies Breaks: Bitcoin Security Under Broken Primitives Ilias Giechaskiel, Cas Cremers, Kasper Rasmussen. 2017

IOTA : S-box ¹

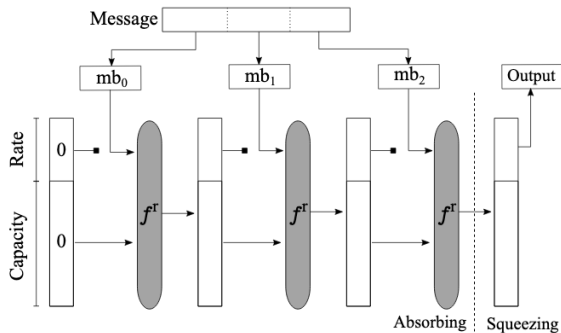


Fig. 1. The Curl-P construction.

¹ *Cryptanalysis of Curl-P and Other Attacks on the IOTA Cryptocurrency* by Ethan Heilman, Neha Narula, Garrett Tanzer, James Lovejoy, Michael Colavita, Madars Virza, and Tadge Dryja

AES 256 en Hexa

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Curl-P-27

	-1	0	1
-1	1	1	-1
0	0	-1	1
1	-1	0	0

Traceable



Traceable



MONERO



CASH

Snark

Limitations



10 minutes = 1 block



Size of the transactions 1 Mo

Limitations



10 minutes = 1 block



Size of the transactions 1 Mo



Lightning Network



LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES



ETHEREUM

12 secondes

Energyvore



LIMO

Source
U.S. Energy Information Administration, [Country Data](#), 2019 est. (or most recent available year)

Outline

Bitcoin

Proof of Behavior

EcoMobiCoin

LCoin

Conclusion

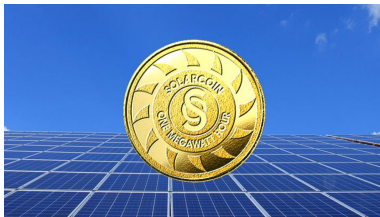
Proof of Behavior

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



Related Work

► SolarCoin



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

► MobiCoin



Proof of Behavior (PoB)

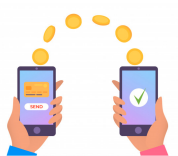


- ▶ No specialized hardware required for mining
- ▶ Anyone behavior helps to generate coins
- ▶ No waste of computational power

Proof of Behavior (PoB)

- ▶ Public blockchain
- ▶ Decentralization

3 actors



User



Prover



Verifier

Users



Provers



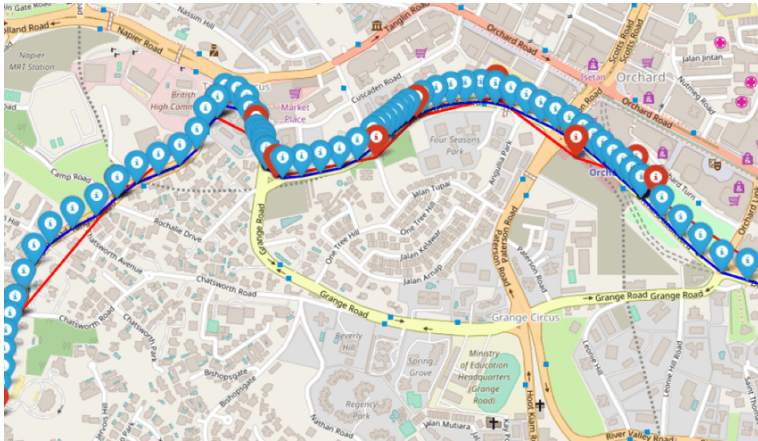
Who realize PoB



Verifiers (Miners)



Who verify PoBs and transactions



LIMOS

LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Miners have to perform PoB

Outline

Bitcoin

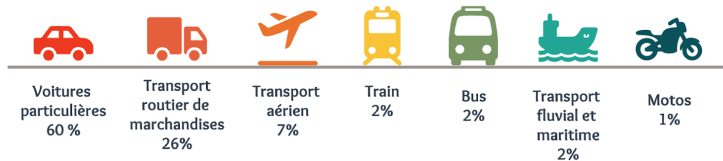
Proof of Behavior

EcoMobiCoin

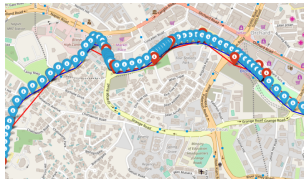
LCoin

Conclusion

Quels types de transports consomment le plus de CO2 ?



EcoMobiCoin Proof of Behavior



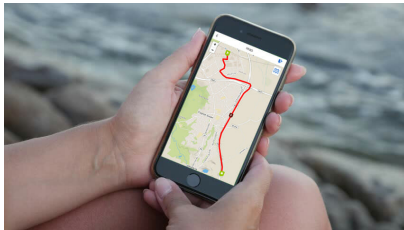
EcoMobiCoin Temporal Demurage



Ephemeral PoB

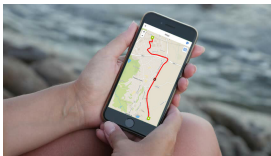


Prover Reward = Distance



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)



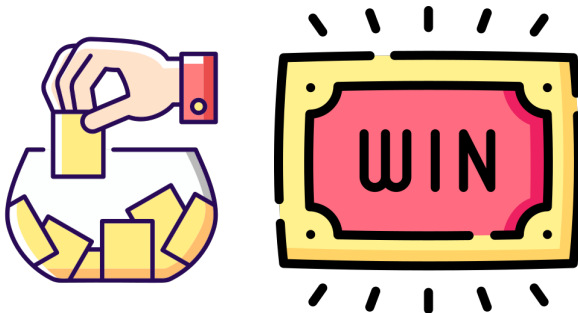
- ▶ Alice wants to prove to Bob that $y = x^{2^T}$
- ▶ Bob picks a random large prime p
- ▶ Alice finds q and r such that : $2^T = qp + r$, $0 \leq r < p$ and sends $\pi = x^q$
- ▶ Bob Computes $r = 2^T \bmod p$ and accepts if $\pi^p x^r = y$

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

Proposed by Benjamin Wesolowski at Eurocrypt 2019

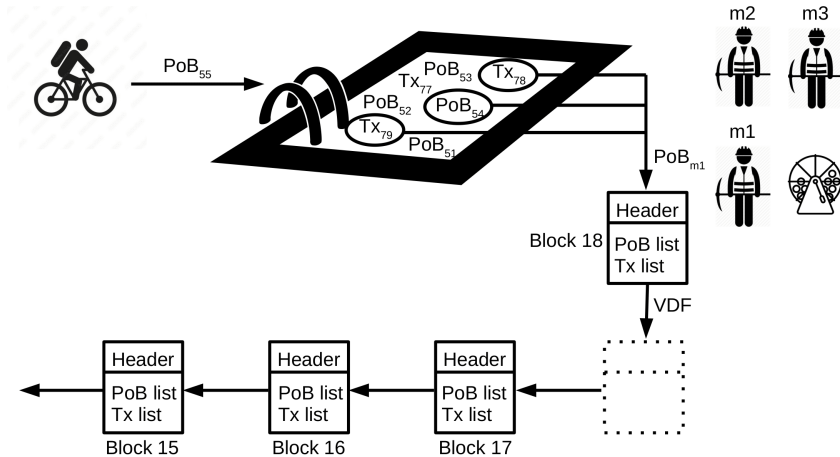
Lottery for miners

VDF(PoB) gives proof of computation time



The faster wins !

Blockchain Mining



Outline

Bitcoin

Proof of Behavior

EcoMobiCoin

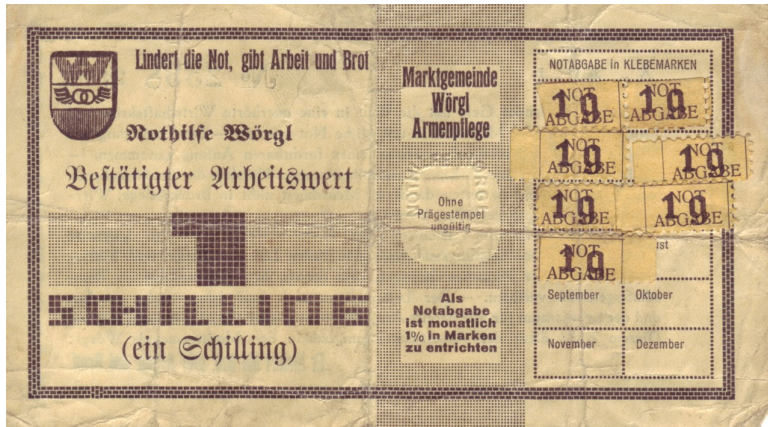
LCoin

Conclusion

LCoin

- ▶ Geographical demurage
- ▶ Proof of Location

Local Currency in Wörgl, Austria



Temporal Demurrage

Temporal Demurrage: Ticket Restaurant, France



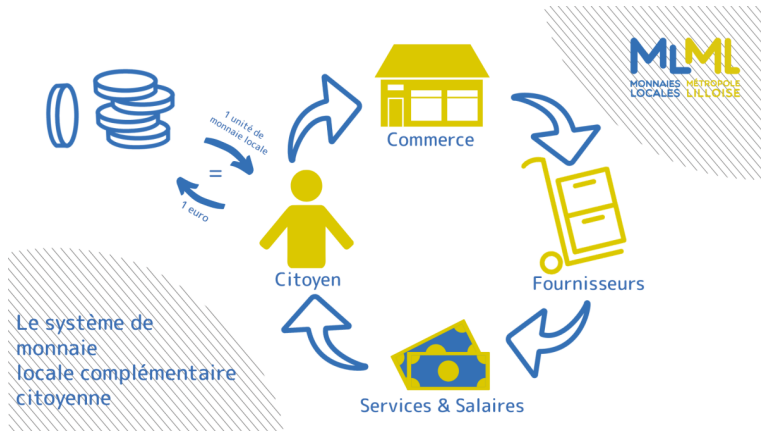
French Local Currencies



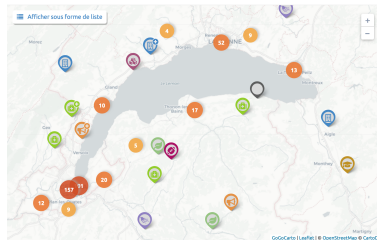
l'âge de faire ✂

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

Local Currency



Léman: Local Cryptocurrency



Using blockchain (Proof of Work)



LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Our idea I: Restricted Area

Proximity certificate delivered by Affiliated Local Shops



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

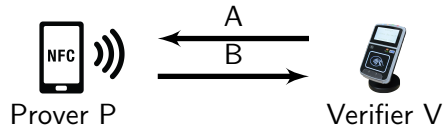


The LIMOS logo, featuring the word "LIMOS" in a stylized blue font with binary code (0s and 1s) integrated into the letters.

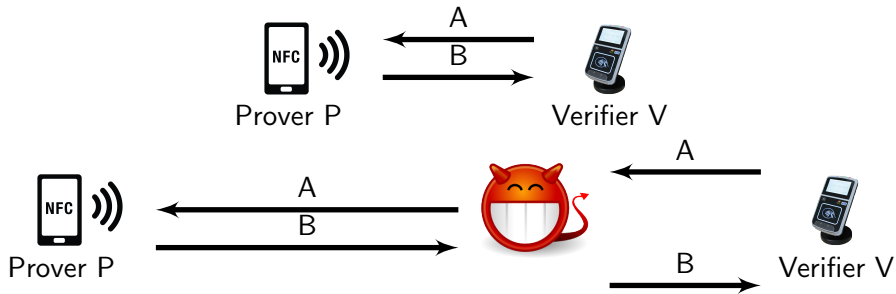
LABOR
DE MO

Distance Bounding Protocol

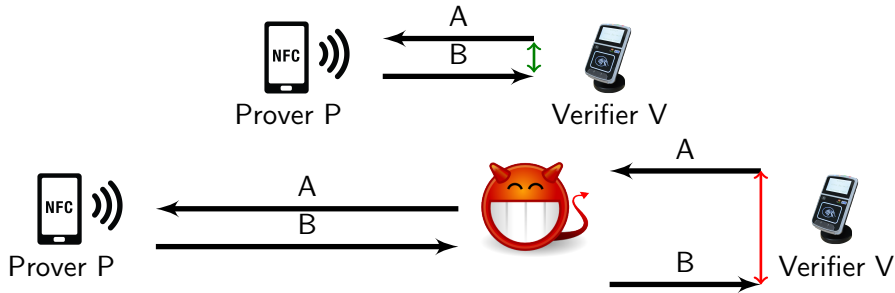
Distance Bounding



Distance Bounding



Distance Bounding



Our idea I: Geographic Demurrage



2 options : $2^2 = 4$ possibilities

	 Restricted Area	 Geographical Demurrage
Simple	<i>X</i>	<i>X</i>
Restricted	<i>D</i>	<i>X</i>
LCoin	<i>X</i>	<i>D</i>
Perfect	<i>D</i>	<i>D</i>



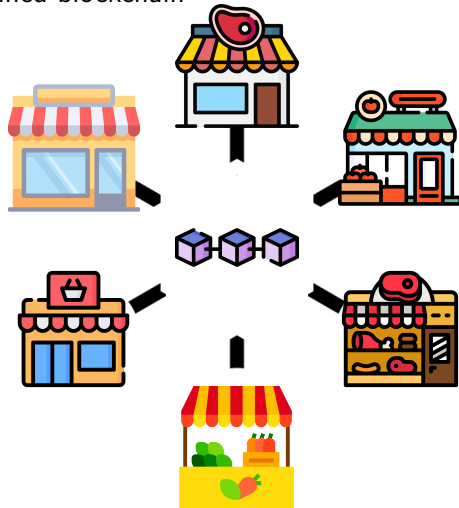
Simple: X Restricted Area X Geographical Demurrage

Permissioned blockchain



LIMOS

LABORATOIRE D'INFORMATIQUE,
DE MODELISATION ET D'OPTIMISATION DES SYSTEMES

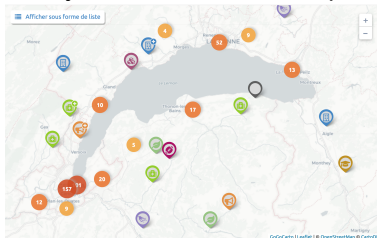


Miners = Affiliated Shops

Restricted: *D* Restricted Area *X* Geographical Demurrage



Proximity certificate delivered by Affiliated Local Shops using DB



Limited duration

Proof of local expenses



LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

LCoin: X Restricted Area D Geographical Demurrage

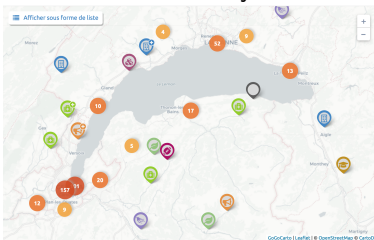
Coins have Point of Attachment (PoA) and a timestamp



Value : Proportional to the distance

Perfect: *D* Restricted Area *D* Geographical Demurrage

Proximity certificate delivered by Affiliated Local Shops using DB



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



Outline

Bitcoin

Proof of Behavior

EcoMobiCoin

LCoin

Conclusion

Conclusion



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

EcoMobiCoin & LCoin

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

Thanks for your attention
Questions ?

Les
**BLOCK
CHAINS**

EN 50 QUESTIONS

Comprendre le fonctionnement et les enjeux
de cette technologie innovante

