

# Cryptocurrency Innovations: EcoMobiCoin for Green Behavior & LCoin for Local Economies

Pascal Lafourcade



30 August 2024



CHAIRE  
**CYBERCNI**  
Sécurité des infrastructures critiques



# Sumerians around 3,500 BC



# What is money?

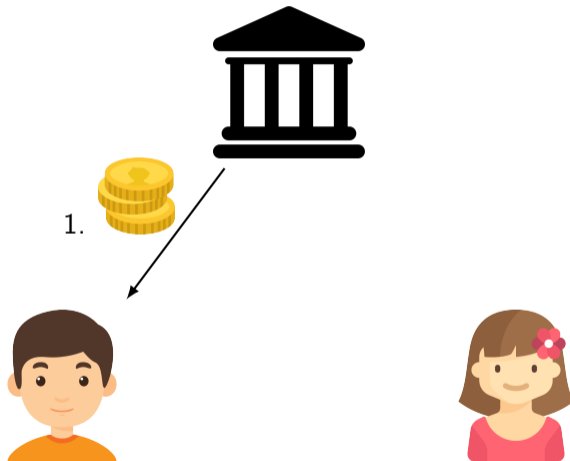


- ▶ Intermediary and means of exchanging goods and services between individuals
- ▶ Reserve of value
- ▶ Unit of account

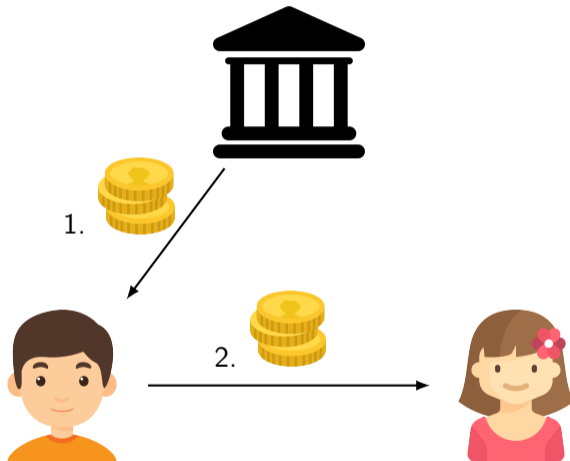
# Several currencies



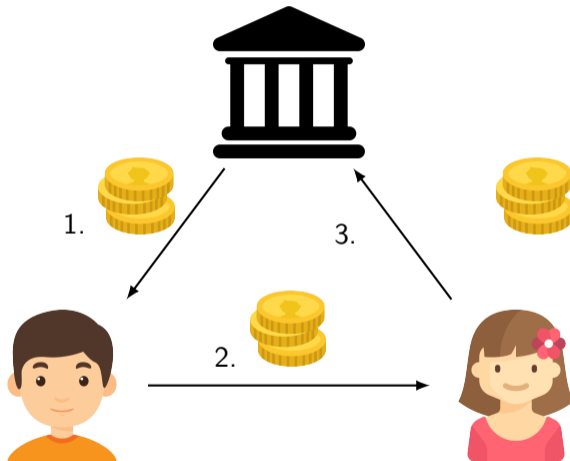
# Principe : Central Bank



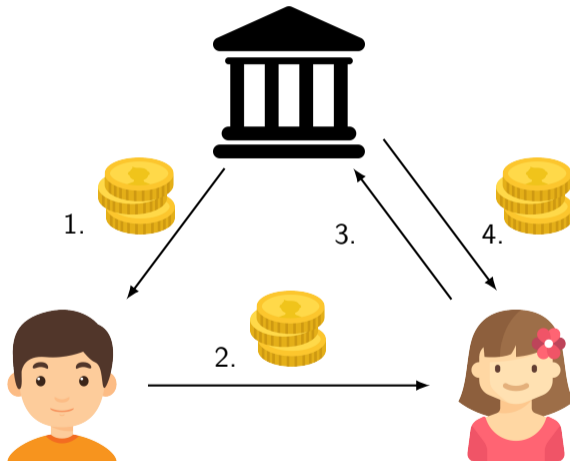
# Principe : Central Bank



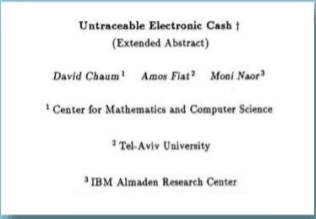
# Principe : Central Bank



# Principe : Central Bank



# 1988 : DigiCash




Untraceable Electronic Cash †  
(Extended Abstract)

David Chaum<sup>1</sup> Amos Fiat<sup>2</sup> Moni Naor<sup>3</sup>

<sup>1</sup> Center for Mathematics and Computer Science  
<sup>2</sup> Tel-Aviv University  
<sup>3</sup> IBM Almaden Research Center

CRYPTO 1988

*DigiCash*<sup>™</sup>

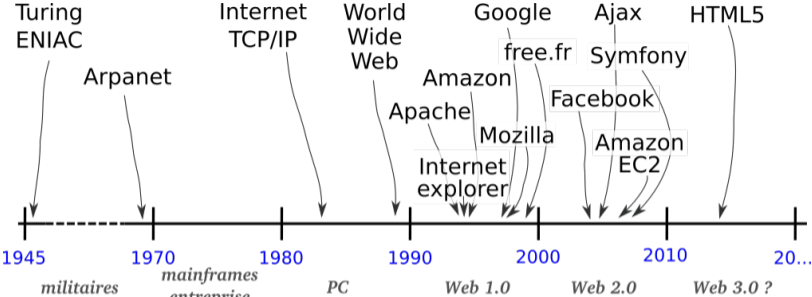


David Chaum

- ☺ Preserves privacy
- ☹ Using cryptographic primitives
- ☹ Always requires a third party (bank)



# A visionary idea ahead of its time



## ▶ Monney

1. Intermediary and means of exchanging goods and services between individuals
2. Reserve of value
3. Unit of account

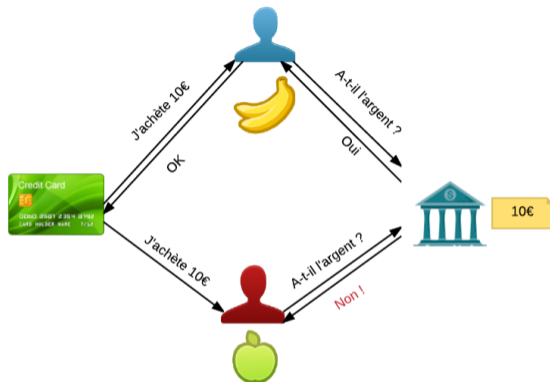
## ▶ Crypto-currency: electronic money, without a Third Party

4. Respect for privacy
5. Non-Falsifiable
6. Avoid double spending

# Properties: Unforgeable



# Properties: Avoir double spending



► identification of cheater

► “presumption of innocence”



# Properties: Privacy preserving

- ▶ Weak anonymity: no identification of a buyer
- ▶ Strong anonymity: no traceability of a buyer



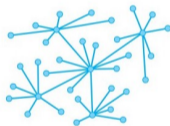
# Bitcoin 2009



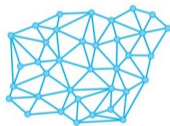
## ► Decentralised and distributed



Système centralisé



Système décentralisé



Système distribué



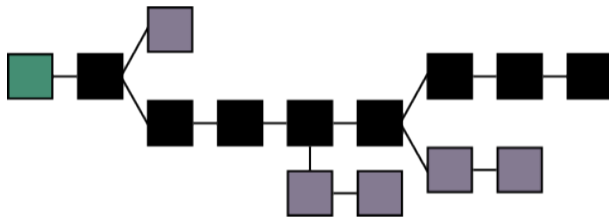
21 millions BTC

# Distributed then Unstoppable

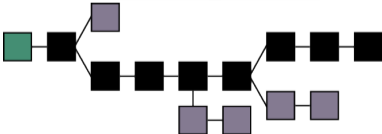




# Infalsifiable



# Auditable



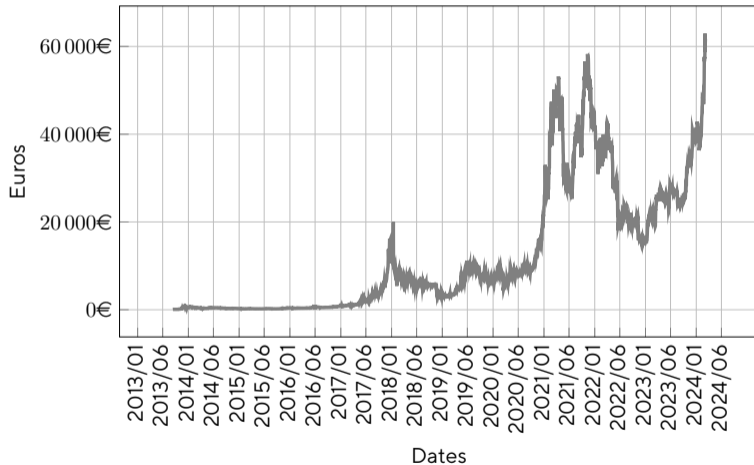
# Bitcoin in 2008 by Satoshi Nakamoto

1 BTC  $\approx$  61 257 € 24 July 2024

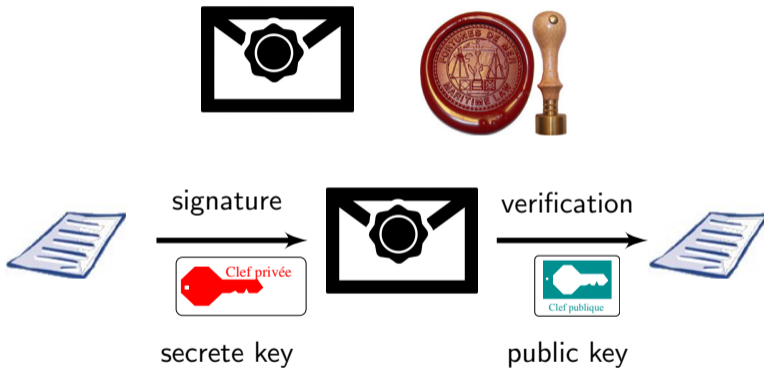


1	BTC = 1 Bitcoin	
0,01	BTC = 1 cBTC	= 1 centiBitcoin (ou bitcent)
0,001	BTC = 1 mBTC	= 1 milliBitcoin
0,000 001	BTC = 1 $\mu$ BTC	= 1 microBitcoin
0,000 000 01	BTC = 1 Satoshi	

# Bitcoin



# Signature



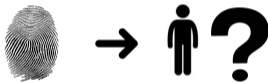
RSA:  $m^d \bmod n$

# Hash Functions (RIPEMD-160, SHA-256, SHA-3)



## Properties

- ▶ Pré-image resistance



- ▶ Seconde Pré-image resistance



- ▶ Collision resistance



# Bitcoin

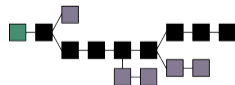
- ▶ Total number of bitcoins is **finite**

21 millions BTC

- ▶ Use a **PKI**
- ▶ Account number:

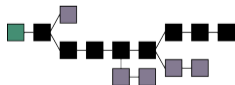
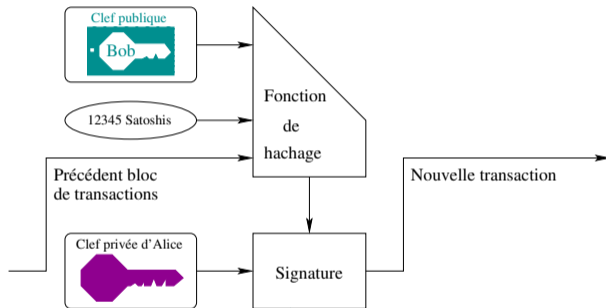
$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$

- ▶ All transactions are **public**
- ▶ **Blockchain**: a peer-to-peer system that guarantees the validity of transactions.



# How to make a transaction?

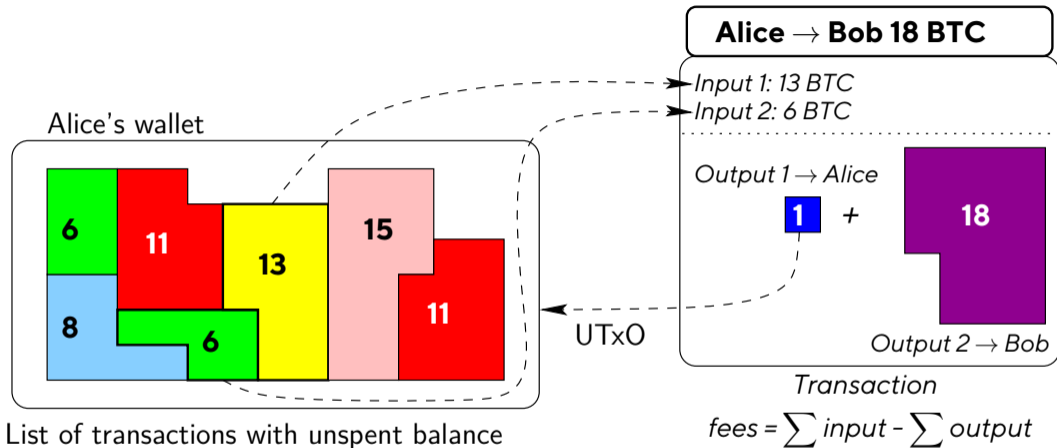
Alice gives 12345 Satoshis to Bob.



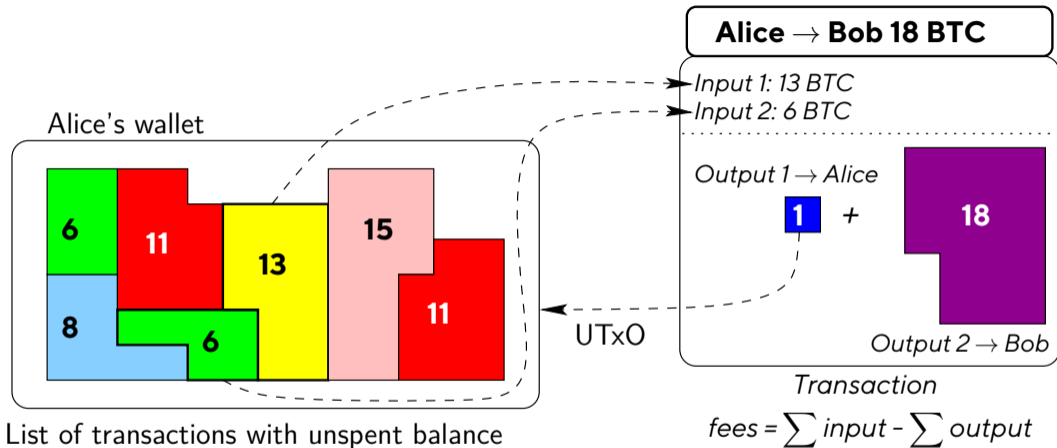
Unspent Transaction Output UTXO



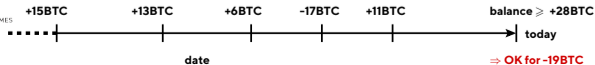
# Pay 18 BTC with coins



# Pay 18 BTC with coins



▶ Only bitcoins owned can be spent



# How to mine Bitcoins?



# How to mine Bitcoins?



“Minera” valid transaction for bitcoins



# Mine Bitcoins

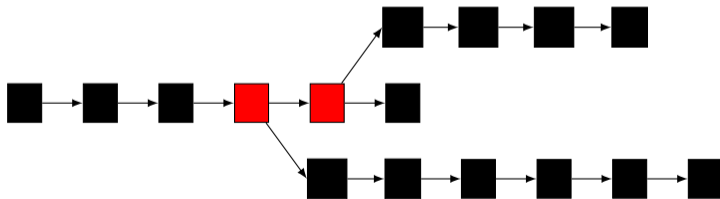
- ▶ Valid = solve **hash target**
- ▶ Reward initially of 50 BTC for one validation
- ▶ Divided by 2 every 210000 validations

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



# Blockchain Infalsifiable

$$\begin{aligned} & \text{SHA256}(C, A, 1, \text{SHA256}(C, B, 9, \text{SHA256}(A, B, 3, 424210))) \\ = & \text{SHA256}(C, A, 1, \text{SHA256}(C, B, 9, 458237)) \\ = & \text{SHA256}(C, A, 1, 936127) \\ = & 458237 \end{aligned}$$





# Mine: Hash target

Target for the block 816 377 (Feb 2024)

0000000000000000000000004819400



Find  $n$  such that

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

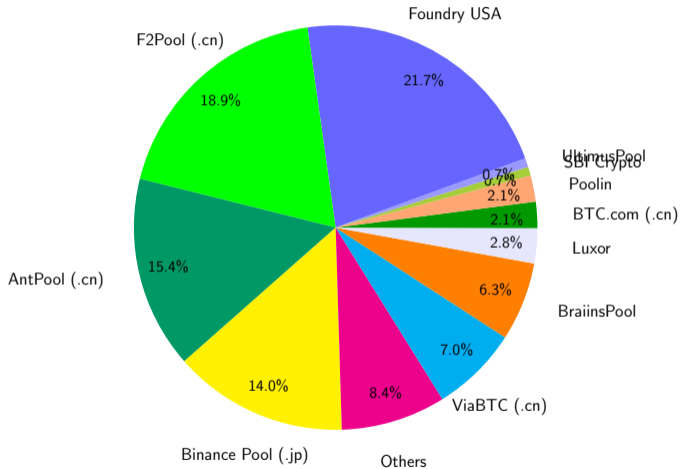
At least 18 zéros for  $x$

Strategy: brute force

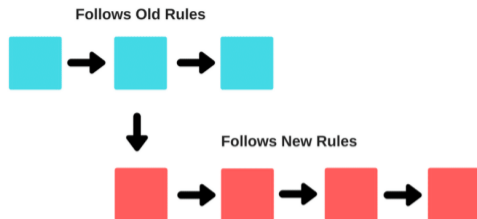
Test all possible values of  $n$



# Farms of miners: sharing rewards



# Soft Fork

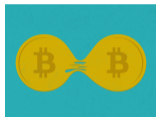


The primary difference between a soft fork and hard fork is that it is not backward compatible

## Code modifications:

- ▶ Correction of bugs
- ▶ Consensual improvements

# Hard Fork



**Bitcoin Blockchain, 1 MByte**

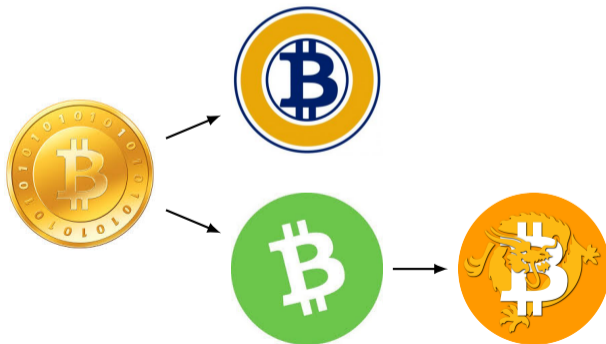


**Bitcoin Cash Blockchain,  
8 MByte**



# Hard Fork History

- ▶ Bitcoin Cash for Bitcoin (1 August 2017 at block 478558)
- ▶ Bitcoin Gold for Bitcoin (24 October 2017 at block 491407)
- ▶ Bitcoin SV (Satoshi Version) for Bitcoin Cash (15 November 2018 at block 556766)



# Hard Fork History

Logo	Fork Name	Fork Symbol	Blockchain	Fork Date	Fork Block	Coin Distribution
	Bitcoin Zero	BZX	Bitcoin	Sunday, September 26, 2016	0	1 BZX = 1 BTC = 1 BZX
	Moss Bitcoin	MBC	Bitcoin	Wednesday, May 25, 2016	525000	1 BTC = 1000 MBC
	Classic Bitcoin	CBTC	Bitcoin	Sunday, April 01, 2016	516025	1 BTC = 1000 CBTC
	Bitcoin Life	BTC.L	Bitcoin	Tuesday, January 30, 2016	0	1 BTC = 1 BTC.L
	Bitcoin Atom	BTA	Bitcoin	Wednesday, January 24, 2016	558889	1 BTC = 1 BTA
	Bitcoin Interest	BCI	Bitcoin	Monday, January 22, 2016	565863	1 BTC = 1 BCI
	BitcoinTV	BT.V	Bitcoin	Sunday, January 21, 2016	559250	1 BTC = 1 BT.V
	Bitcoin Smart	BCS	Bitcoin	Sunday, January 21, 2016	559250	1 BTC = 100 BCS
	Bitcoin Floodum	BTR	Bitcoin	Wednesday, January 16, 2016	0	1 BTC = 1 BTR
	Bitcoin Private	BTP	Bitcoin	Monday, January 01, 2016	0	1 BTC = 250 = 1 BTP
	Bitcoin All	BTA	Bitcoin	Monday, January 01, 2016	0	1 BTC = 1 BTA
	Bitcoin Pizza	BPA	Bitcoin	Monday, January 01, 2016	501886	1 BTC = 1 BPA
	BitcoinDay	BCD	Bitcoin	Sunday, December 31, 2017	501886	1 BTC = 100 BCD
	Bitcoin One	BCO	Bitcoin	Sunday, December 31, 2017	501949	1 BTC = 1 BCO
	Bitcoin Uranium	BUA	Bitcoin	Sunday, December 31, 2017	0	1 BTC = 1 BUA
	Quantum Bitcoin	QBTC	Bitcoin	Thursday, December 28, 2017	0	1 BTC = 10BTC
	Bitcoin SegWizX et1	BZX	Bitcoin	Thursday, December 28, 2017	501461	1 BTC = 1 BZX
	Bitcoin File	BFI	Bitcoin	Wednesday, December 27, 2017	501225	1 BTC = 1000 BFI
	Bitcoin God	BGD	Bitcoin	Wednesday, December 27, 2017	501225	1 BTC = 1 BGD
	Bitcoin Top	BTT	Bitcoin	Tuesday, December 26, 2017	501116	1 BTC = 1 BTT

Logo	Fork Name	Fork Symbol	Blockchain	Fork Date	Fork Block	Coin Distribution
	Bitcoin Nova	BTN	Bitcoin	Monday, December 25, 2017	501000	1 BTC = 1 BTN
	Lightning Bitcoin	LBTC	Bitcoin	Tuesday, December 19, 2017	498660	1 BTC = 1 LBTC
	Bitcoin Stake	BTC.S	Bitcoin	Tuesday, December 19, 2017	498660	1 BTC = 100 BTC.S
	Bitcoin Faith	BTF	Bitcoin	Tuesday, December 19, 2017	500000	1 BTC = 1 BTF
	Bitcoin World	BTW	Bitcoin	Sunday, December 17, 2017	499777	1 BTC = 1000 BTW
	United Bitcoin	UB	Bitcoin	Tuesday, December 13, 2017	496777	1 BTC = 1 UB
	Bitcoin Hut	BTH	Bitcoin	Tuesday, December 12, 2017	496448	1 BTC = 100 BTH
	BitcoinX	BCX	Bitcoin	Tuesday, December 12, 2017	496880	1 BTC = 1000 BCX
	Super Bitcoin	SBTC	Bitcoin	Tuesday, December 12, 2017	496880	1 BTC = 1 SBTC
	Bitcoin Silver	BTSI	Bitcoin	Friday, December 01, 2017	0	1 BTC = 1 BTSI
	Bitcoin Nano	BTN	Bitcoin	Friday, December 01, 2017	501488	1 BTC = 1000 BTN
	Bitcoin Diamond	BDD	Bitcoin	Friday, November 24, 2017	496480	1 BTC = 10 BDD
	Bitcoin	BTX	Bitcoin	Thursday, November 02, 2017	0	1 BTC = 0.5 BTX
	Bitcoin Gold	BTC.G	Bitcoin	Tuesday, October 16, 2017	491407	1 BTC = 1 BTC.G
	Bitcoin	BTX	Bitcoin	Tuesday, August 01, 2017	476558	1 BTC = 1 BTX
	OK BTC	OKBTC	Bitcoin	Tuesday, August 01, 2017	496880	1 BTC = 1 OKBTC
	Bitcoin Galactic	BCHG / B	Bitcoin	Tuesday, August 01, 2017	476558	1 BTC = 1 BCHG / B
	Bitcoin Cash	BCH	Bitcoin	Tuesday, August 01, 2017	476559	1 BTC = 1 BCH

# 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



ETHEREUM

12 secondes



## Proof of Stake Lightning Network

# Outline

Bitcoin

Blockchain

EcoMobiCoin

LCoin

Conclusion

# Plan

Bitcoin

Blockchain

EcoMobiCoin

LCoin

Conclusion

## The St Lawrence

Incorporated by Letters Patent

Capital \$80000 in

Shares

First issue of 405

We the undersigned do hereby subscribe in the Capital Stock of the St Lawrence Starch and Co. Ltd and our assigns promise and agree to pay the full amount of the said shares and in such manner and amount as by the

## Starch Company (Limited)

under "The Companies Act"

800 Shares of \$100 each.

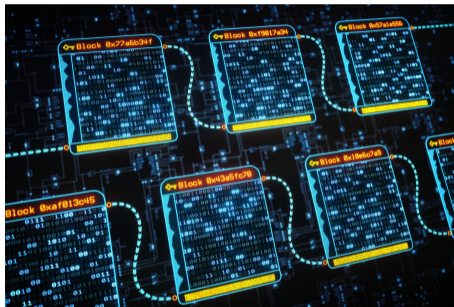
Liability

Shares \$40,500.

for the number of shares set opposite our respective names in the Stock Book of the said Company (Limited) and we do each for himself and himself to pay the full amount of the said respective shares as shown in the said Stock Book and the balance at such time as the Directors or Provisional Directors of the said Company may

Date	Subscribers	Shares	Residence	No of Shares	Remarks	Witness	Amount
1859 Apr 29	Robt. Kilgour	100	Toronto	One Hundred		Atkinson	\$10,000 <sup>00</sup>
Nov 29	Chas. Hutchinson	100	Toronto	One Hundred		Atkinson	\$10,200 <sup>00</sup>
Nov 29	Joseph Milne	100	Toronto	One Hundred		H. Atkinson	\$10,000 <sup>00</sup>
Dec 5	John Gray	100	Cardinal	One Hundred		Marion Gray	\$10,200 <sup>00</sup>
" 5	James Macleod	100	Cardinal	One Share		Marion Gray	\$-100 <sup>00</sup>

# Blockchain

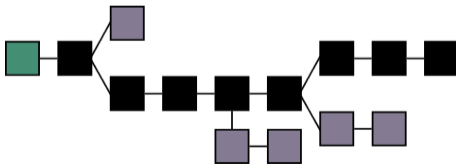


Registre distribué, sécurisé, infalsifiable

# Miners valid all transactions



Update a distributed ledger



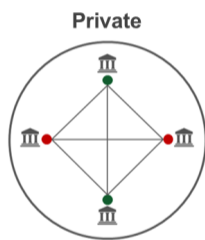
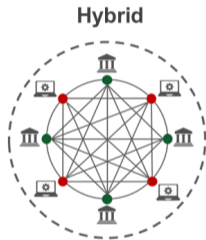
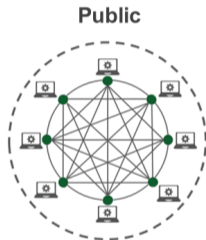
Unstoppable, Infalsifiable, Auditable

# Miners decisions

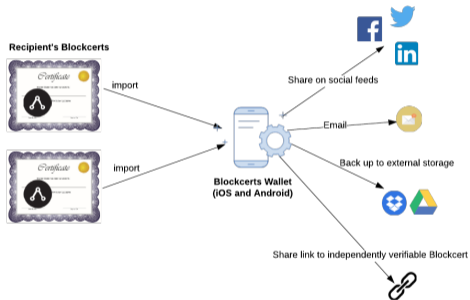




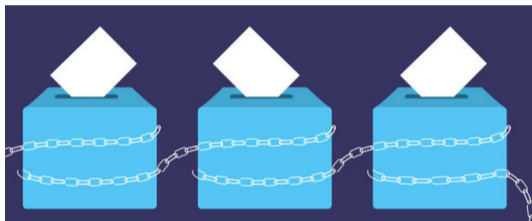
# Blockchain Private vs Public



# Blockchain Application : MIT Diploma



# Blockchain Applications: Verify Your Vote, DABSTERS



## Properties

Universal Verifiability, Individual Verifiability, Privacy, Receipt-Freeness, Prevent Double Vote, Vote and Go, ...

# Blockchain Applications: Auction



## Properties

Universal Verifiability, Individual Verifiability, Privacy, Receipt-Freeness, Prevent Double Spending, Non-Repudiation ...

# Plan

Bitcoin

Blockchain

EcoMobiCoin

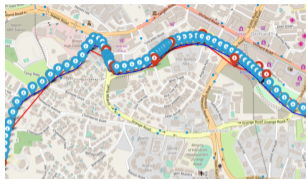
LCoin

Conclusion

## Quels types de transports consomment le plus de CO2 ?



# EcoMobiCoin Proof of Behavior



# EcoMobiCoin Temporal Demurage

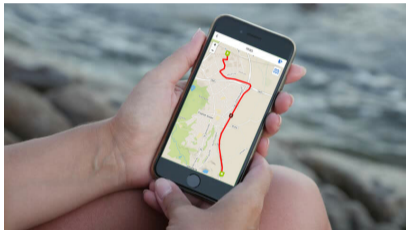




# Ephemeral PoB



# 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)

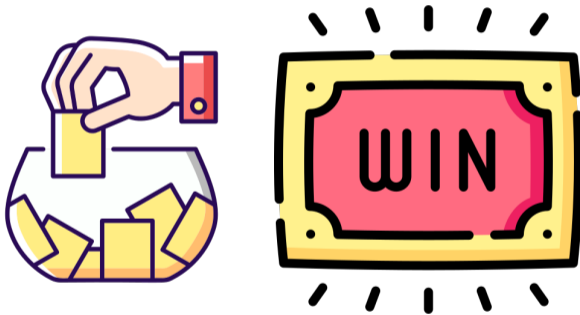


- ▶ Alice wants to prove to Bob that  $y = x^{2^T}$
- ▶ Bob picks a random large prime  $p$
- ▶ Alice finds  $q$  and  $r$  such that :  $2^T = qp + r$ ,  $0 \leq r < p$  and sends  $\pi = x^q$
- ▶ Bob Computes  $r = 2^T \bmod p$  and accepts if  $\pi^p x^r = y$

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

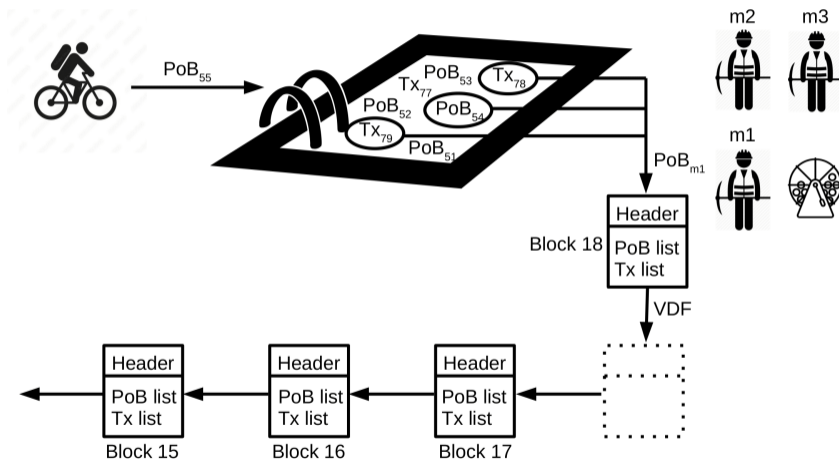
# Lottery for miners

VDF(PoB) gives proof of computation time

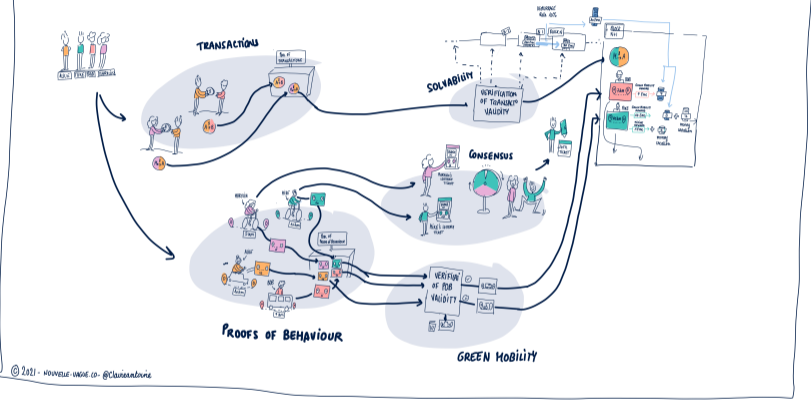


The faster wins !

# Blockchain Mining



# ECOMOBICOIN PRINCIPLES



<https://ecomobitcoin.limos.fr>





# Plan

Bitcoin

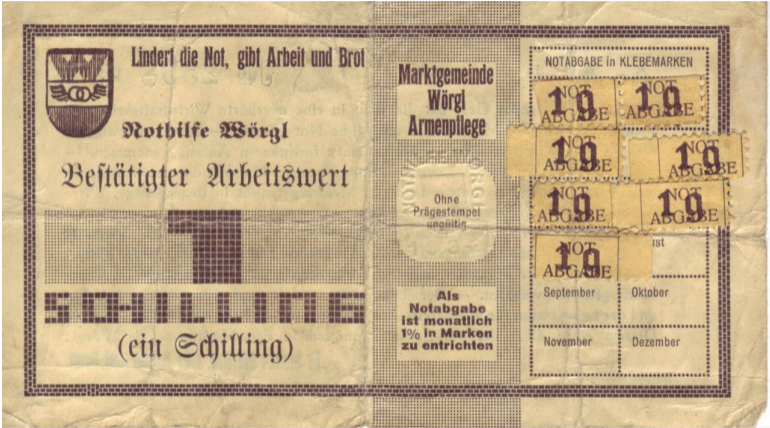
Blockchain

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

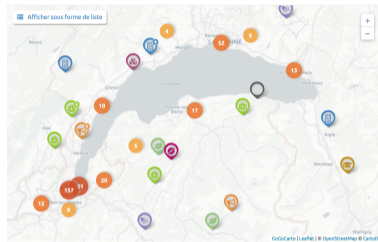
CC-BY-NC-SA www.lagedefaire-lejournal.fr



# Local Currency



# Léman: Local Cryptocurrency



Using blockchain (Proof of Work)



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

# Our idea I: Restricted Area

**Proximity certificate** delivered by Affiliated Local Shops



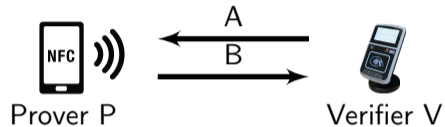
Proof that Alice and Bob are simultaneously in the “same” location



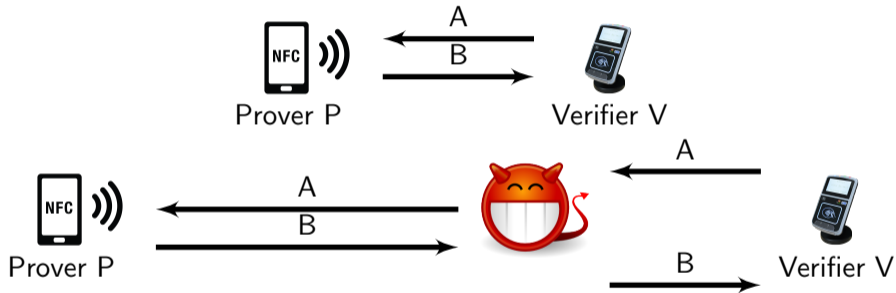
Distance Bounding Protocol



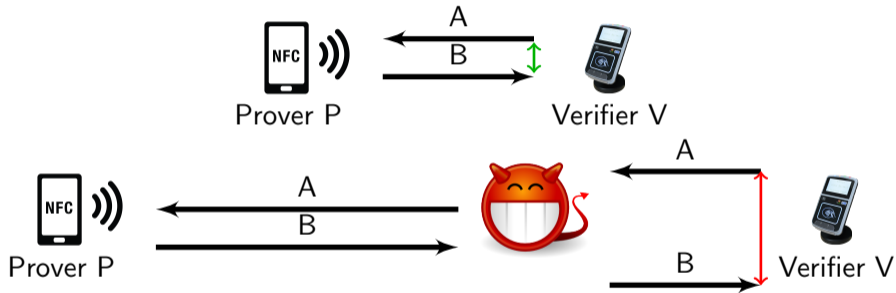
# Distance Bounding



# Distance Bounding



# Distance Bounding





Solution: distance bounding (Brands and Chaum, 1991)

# Our idea I: Geographic Demurrage



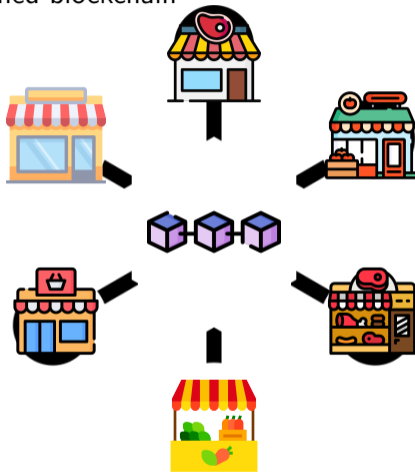
2 options :  $2^2 = 4$  possibilities

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



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

Permissioned blockchain



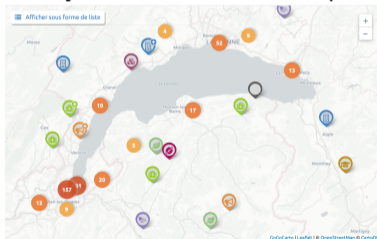
Miners = Affiliated Shops

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: X Restricted Area ✓ Geographical Demurrage

Coins have Point of Attachment (PoA) and a timestamp

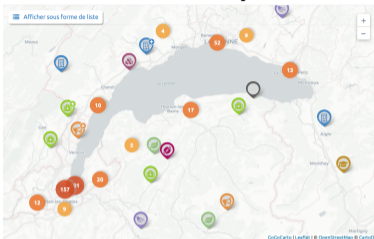


Value : Proportional to the distance



# 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



# Plan

Bitcoin

Blockchain

EcoMobiCoin

LCoin

Conclusion

# Conclusion



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

EcoMobiCoin & LCoin

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

# Thanks for your attention

## Questions ?

