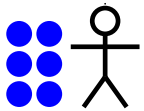
La chaîne de blocs (blockchain)

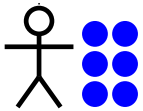
Une introduction technique simplifiée

Imaginez une économie
avec 8 individus.

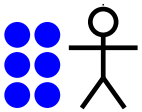
Adrienne



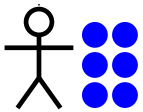
Raymonde



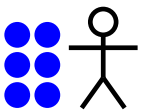
Nicholas



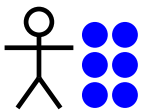
Brigitte



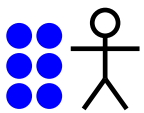
En l'absence de banque, tout le monde conserve son argent à la maison.



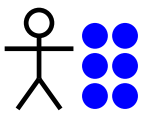
Jonathan



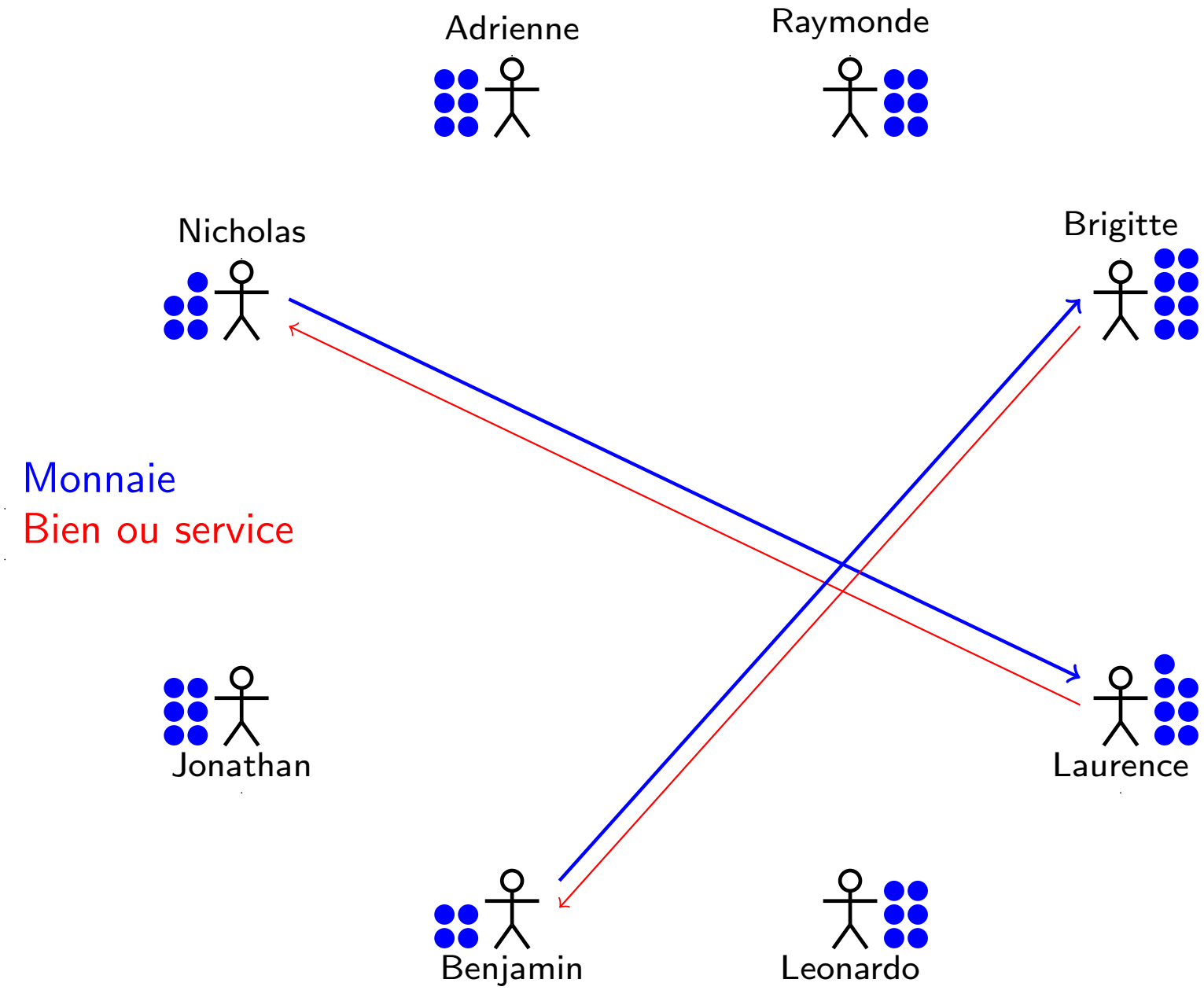
Laurence

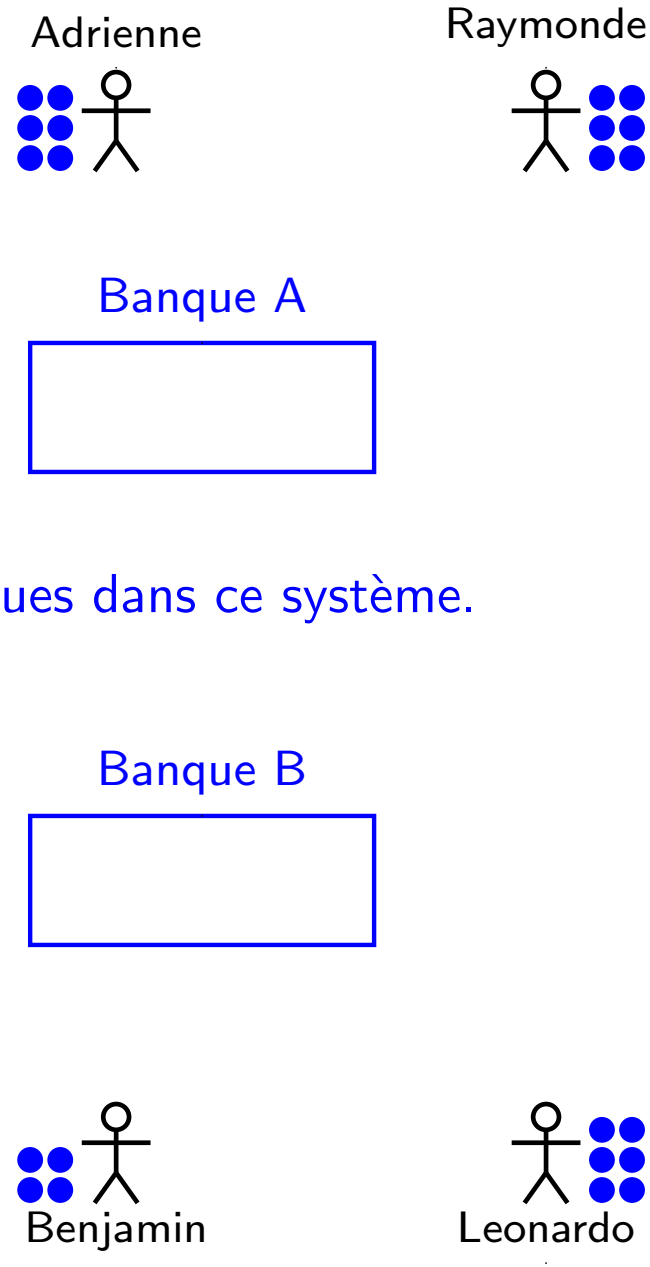


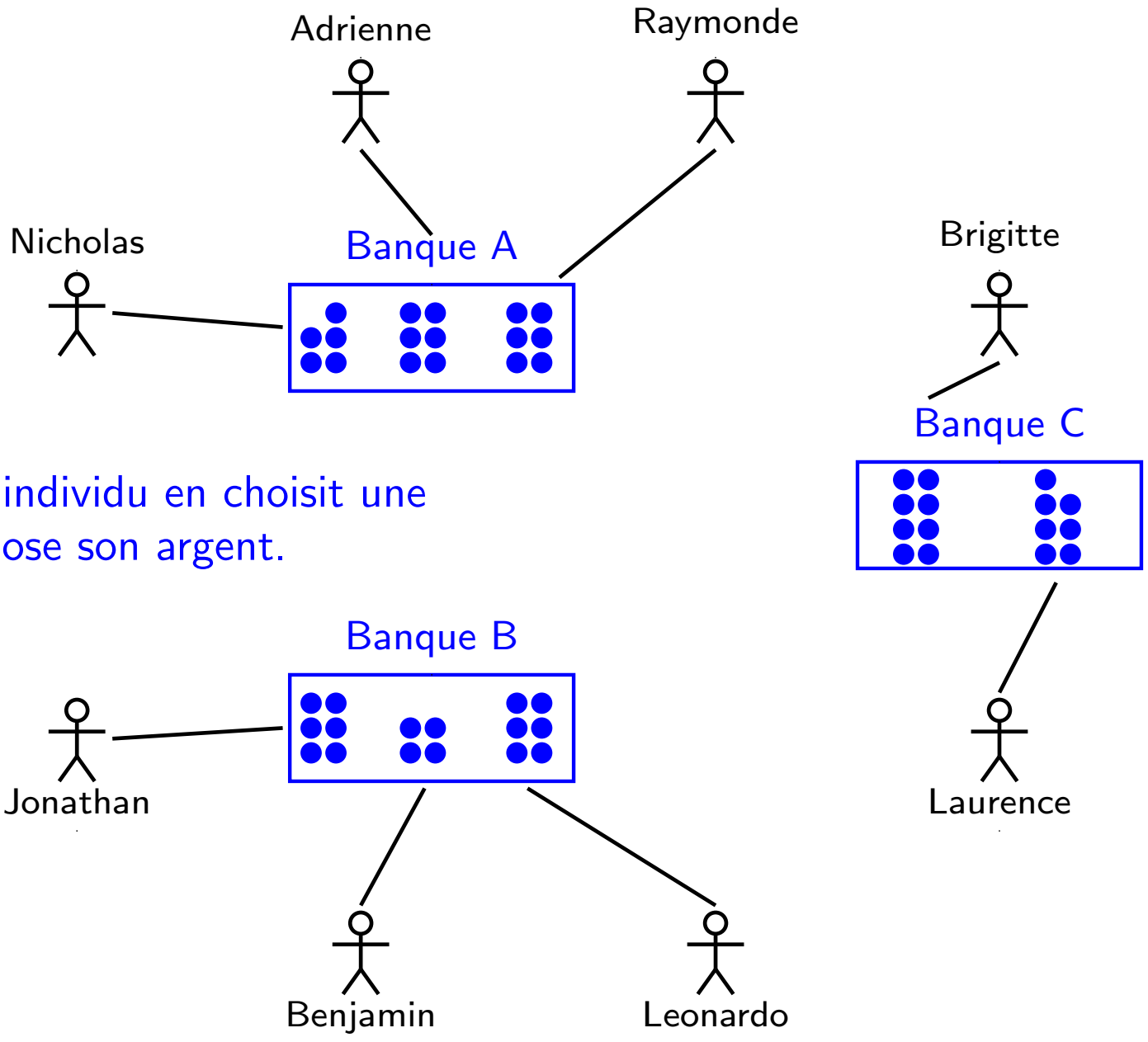
Benjamin

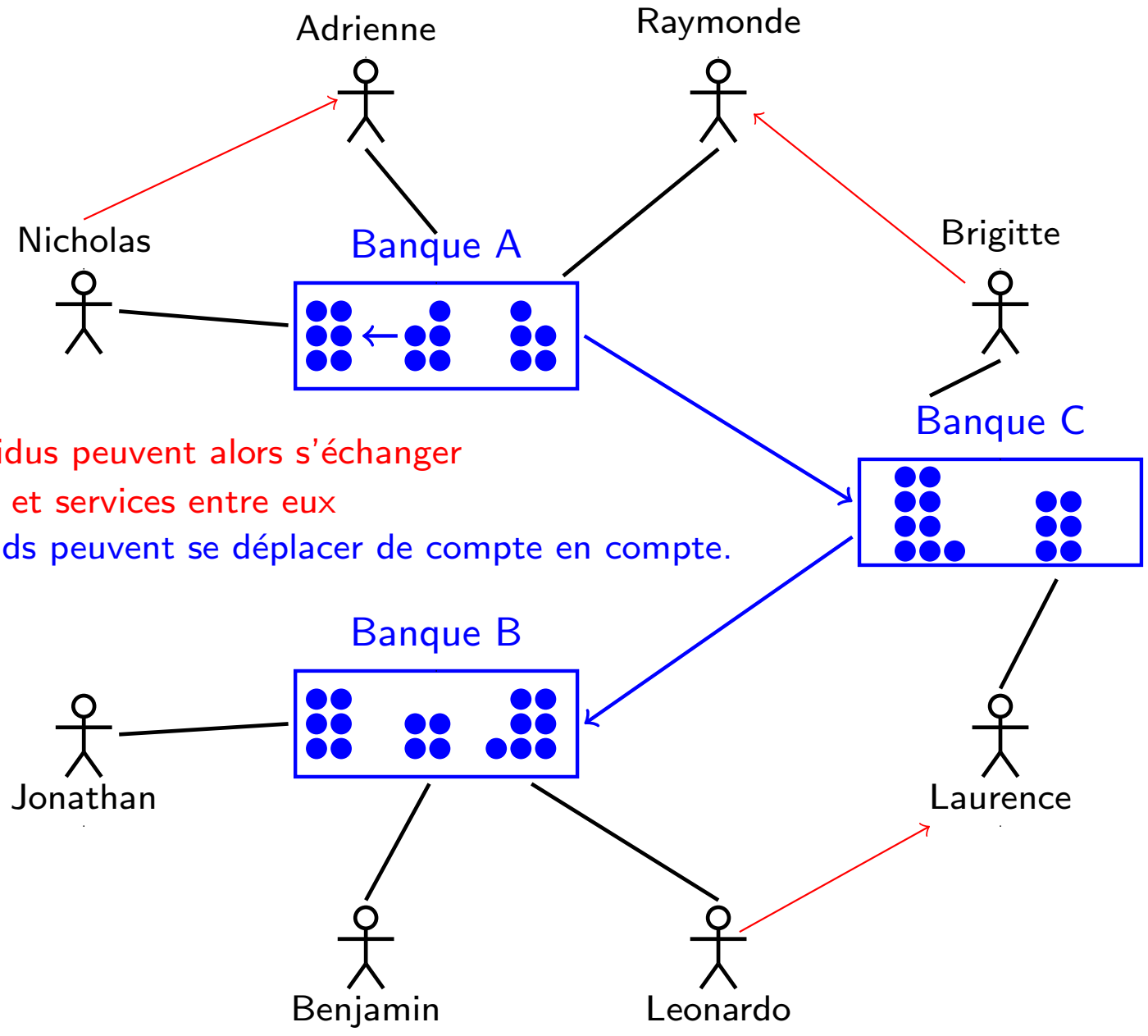


Leonardo

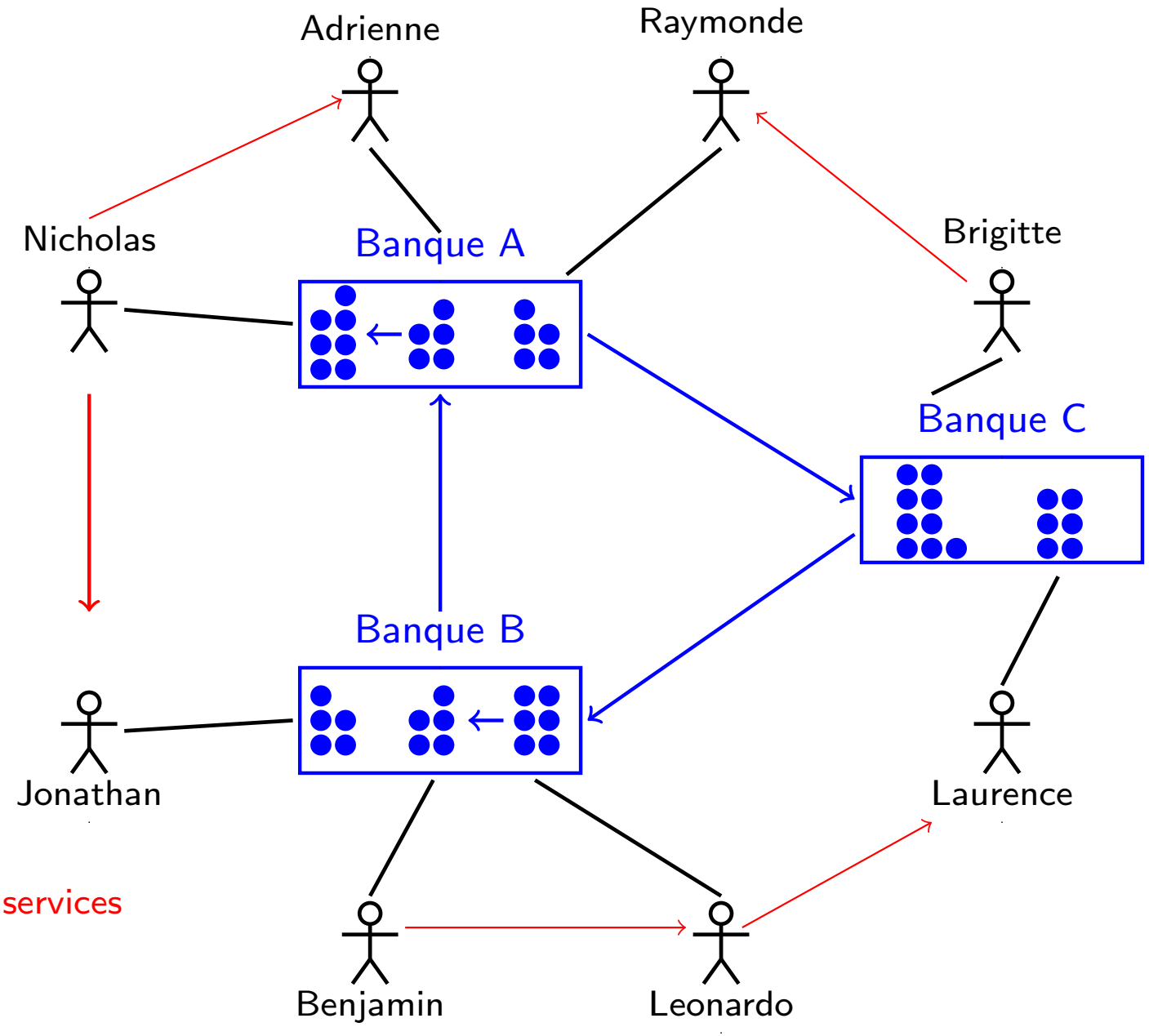

Adrienne
Raymonde
Nicholas
Brigitte
Monnaie
Bien ou service
Jonathan
Laurence
Benjamin
Leonardo

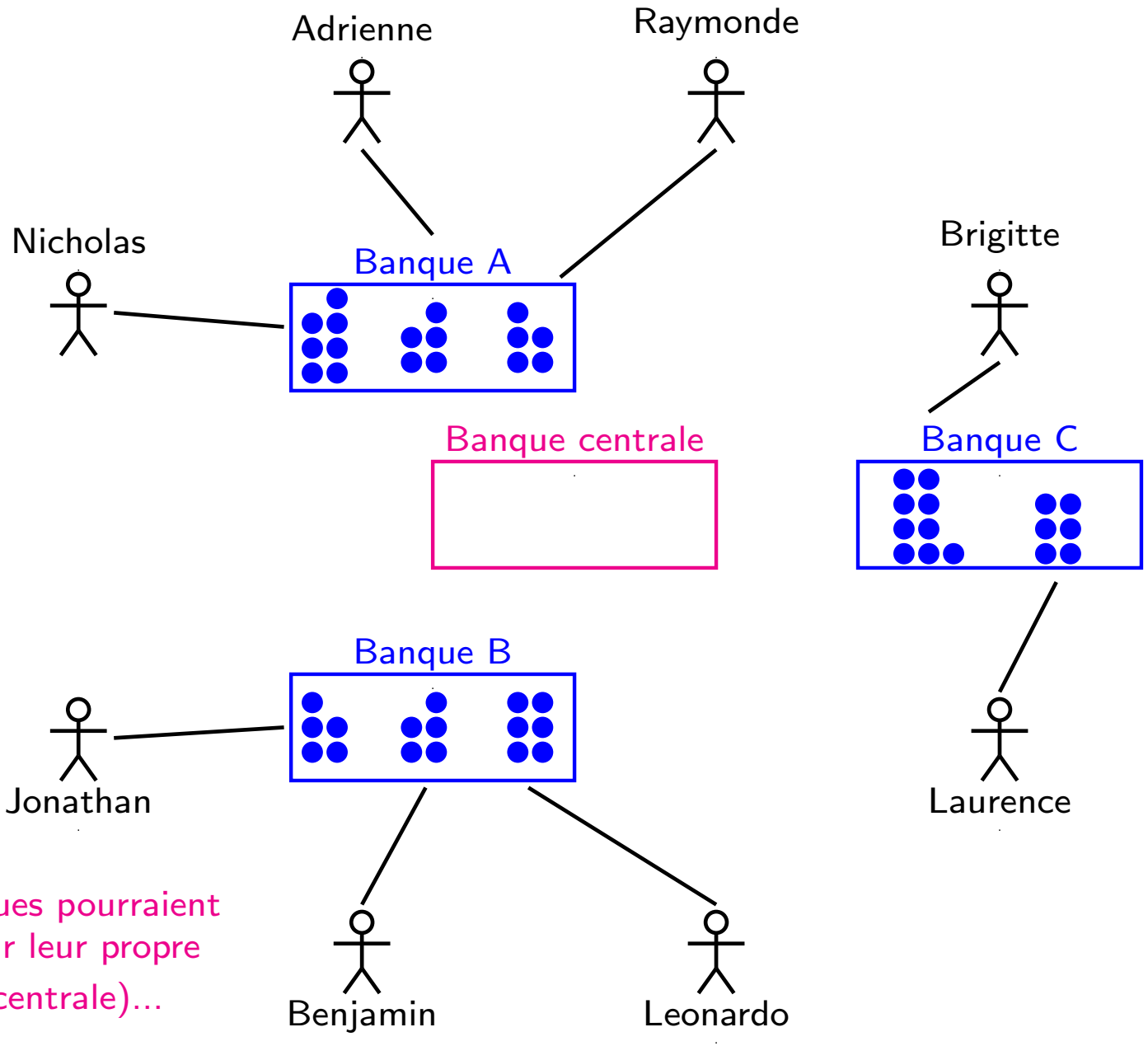

Adrienne
Raymonde
Nicholas
Banque A
Brigitte
Banque C
On introduit des banques dans ce système.
Banque B
Jonathan
Laurence
Benjamin
Leonardo


Adrienne
Raymonde
Nicholas
Banque A
Brigitte
Banque C
Chaque individu en choisit une
et y dépose son argent.
Banque B
Jonathan
Laurence
Benjamin
Leonardo

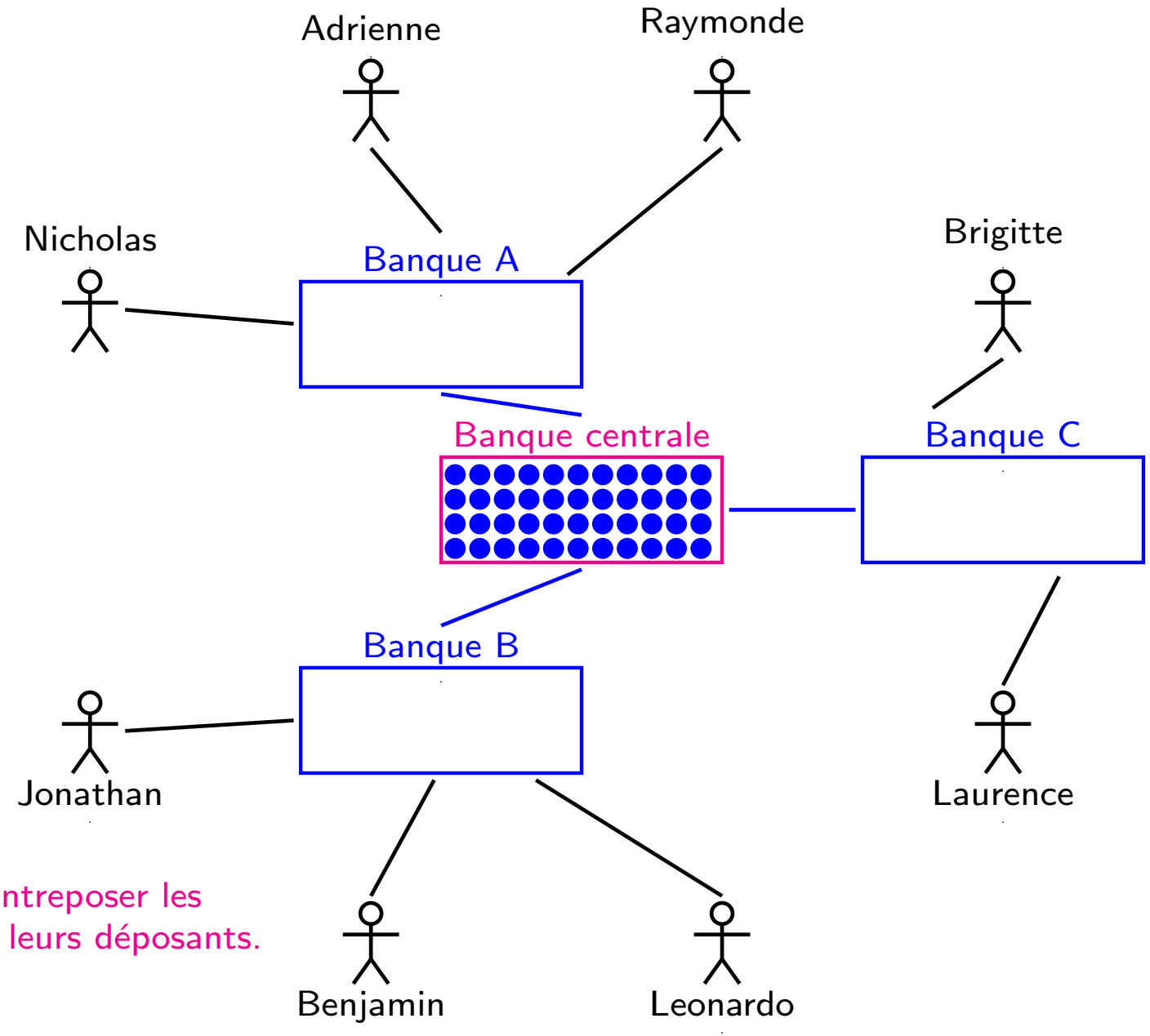


Les individus peuvent alors s'échanger
des biens et services entre eux
et les fonds peuvent se déplacer de compte en compte.

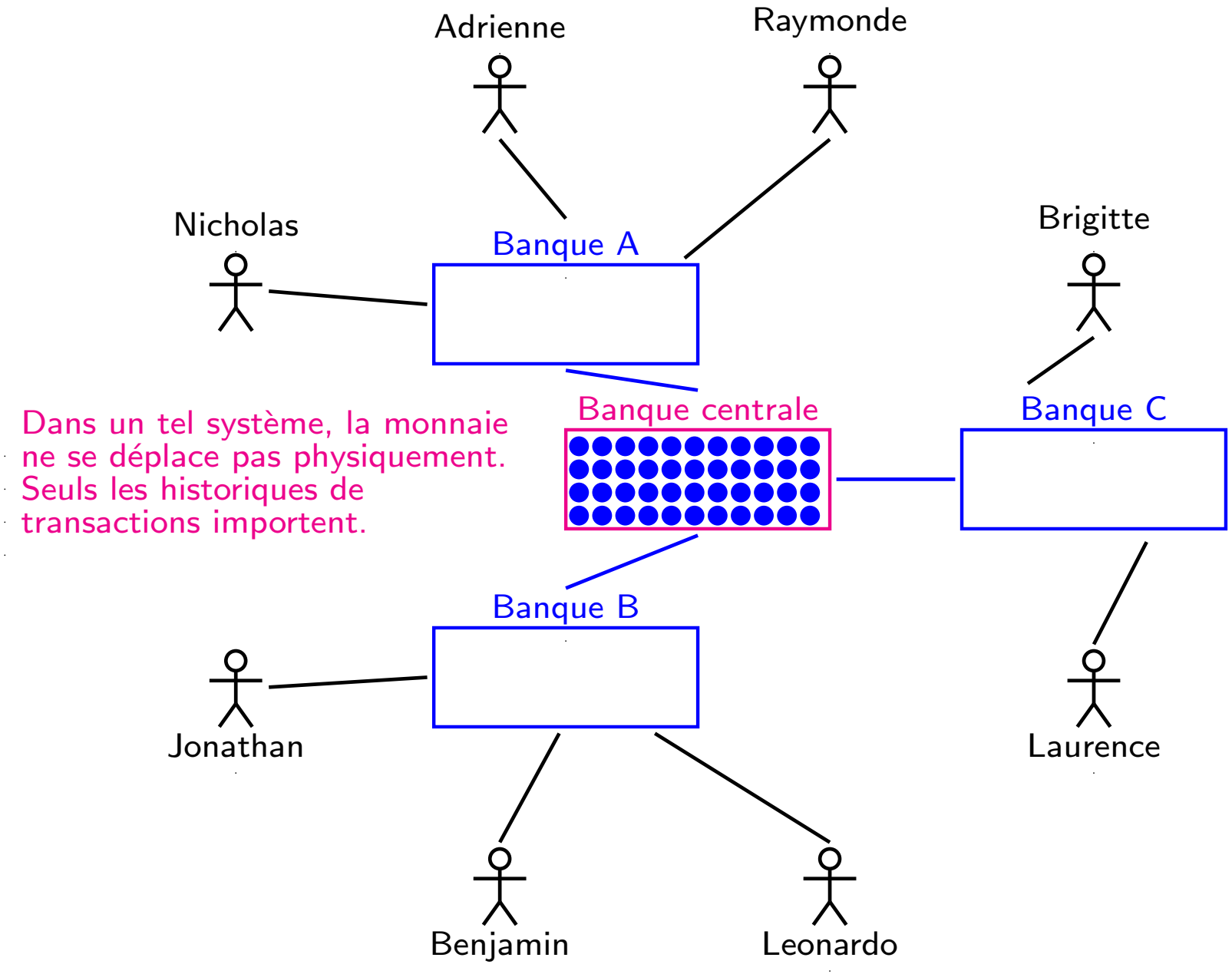

Adrienne
Raymonde
Nicholas
Banque A
Brigitte
Banque C
Banque B
Jonathan
Laurence
Benjamin
Leonardo
Biens et services
Monnaie

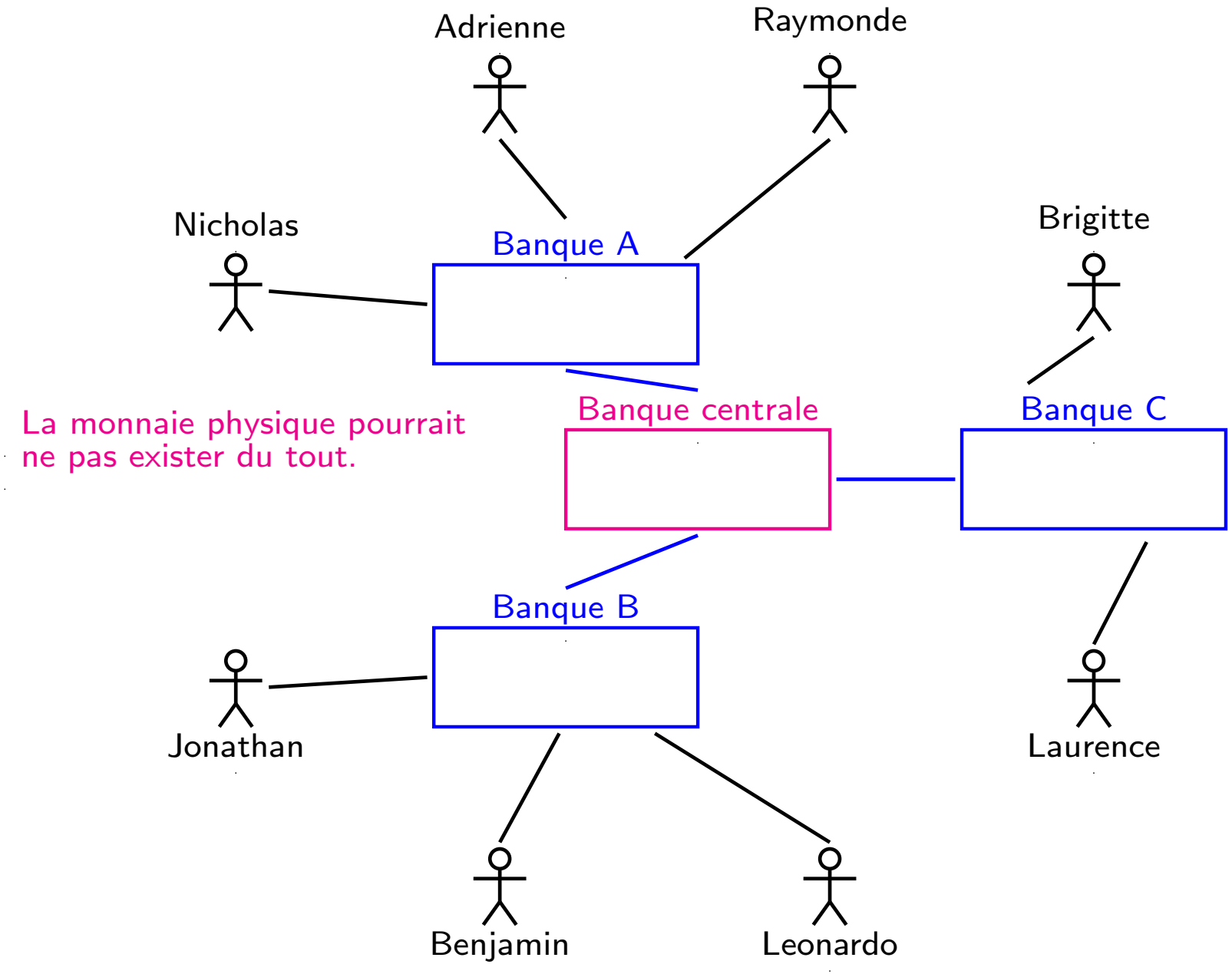


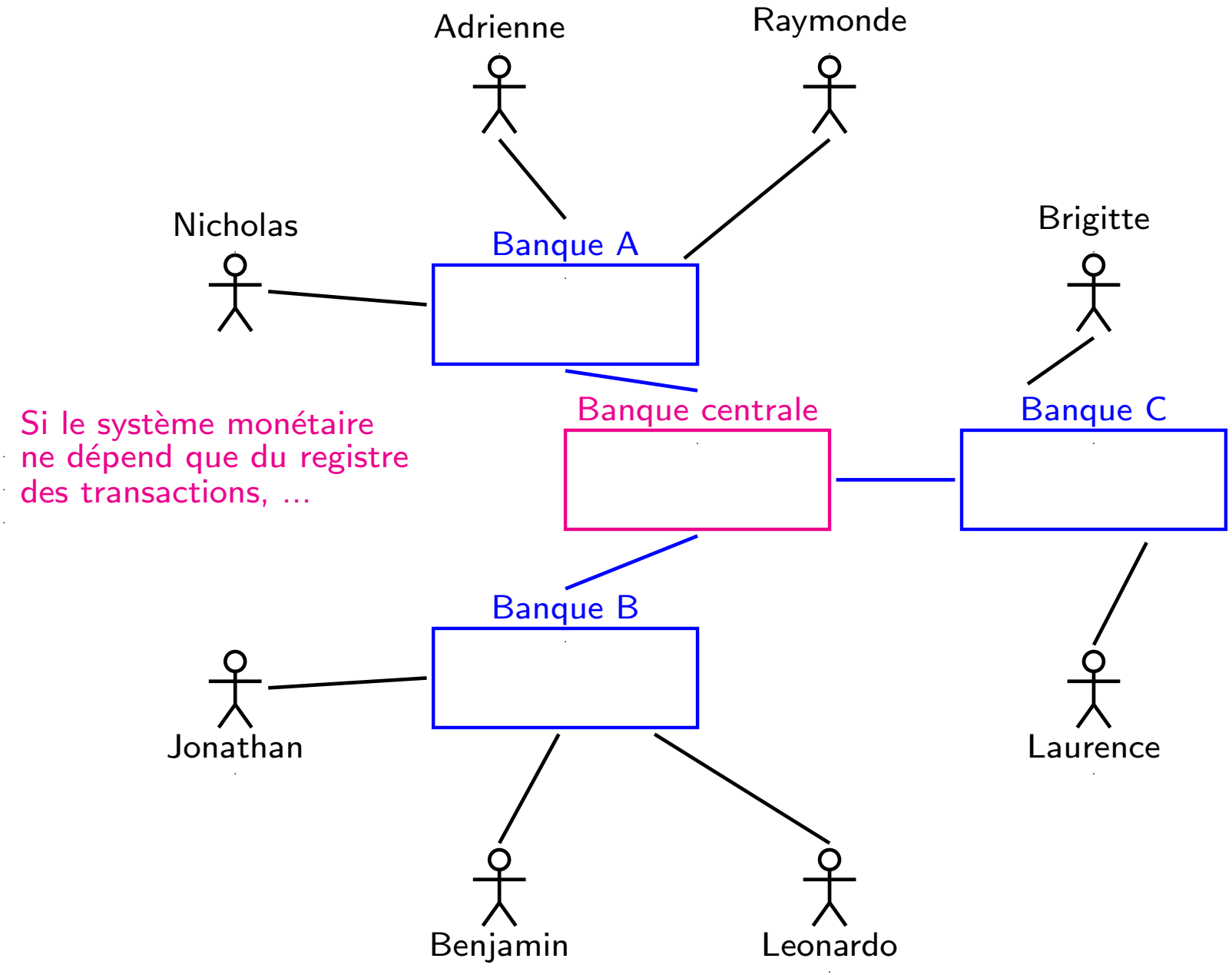
Les banques pourraient aussi avoir leur propre banque (centrale)...

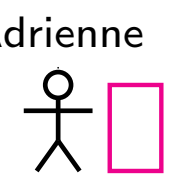


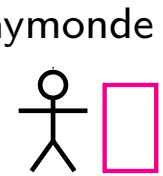
... et y entreposer les
fonds de leurs déposants.

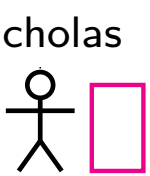

Adrienne
Raymonde
Nicholas
Banque A
Brigitte
Banque centrale
Banque C
Dans un tel système, la monnaie ne se déplace pas physiquement. Seuls les historiques de transactions importent.
Banque B
Jonathan
Laurence
Benjamin
Leonardo

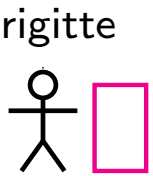

Adrienne
Raymonde
Nicholas
Banque A
Brigitte
La monnaie physique pourrait
ne pas exister du tout.
Banque centrale
Banque C
Banque B
Jonathan
Laurence
Benjamin
Leonardo


Adrienne
Raymonde
Nicholas
Banque A
Brigitte
Si le système monétaire
ne dépend que du registre
des transactions, ...
Banque centrale
Banque C
Banque B
Jonathan
Laurence
Benjamin
Leonardo

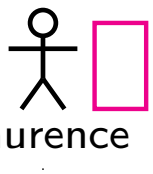


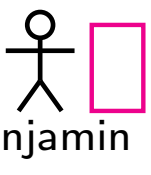


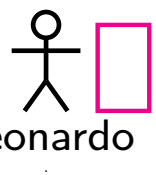


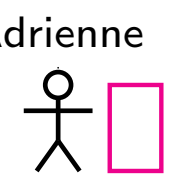


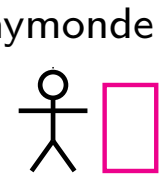
... est-il possible de décentraliser ce registre?

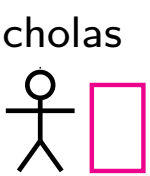


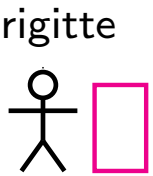




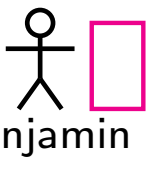


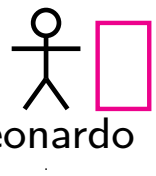


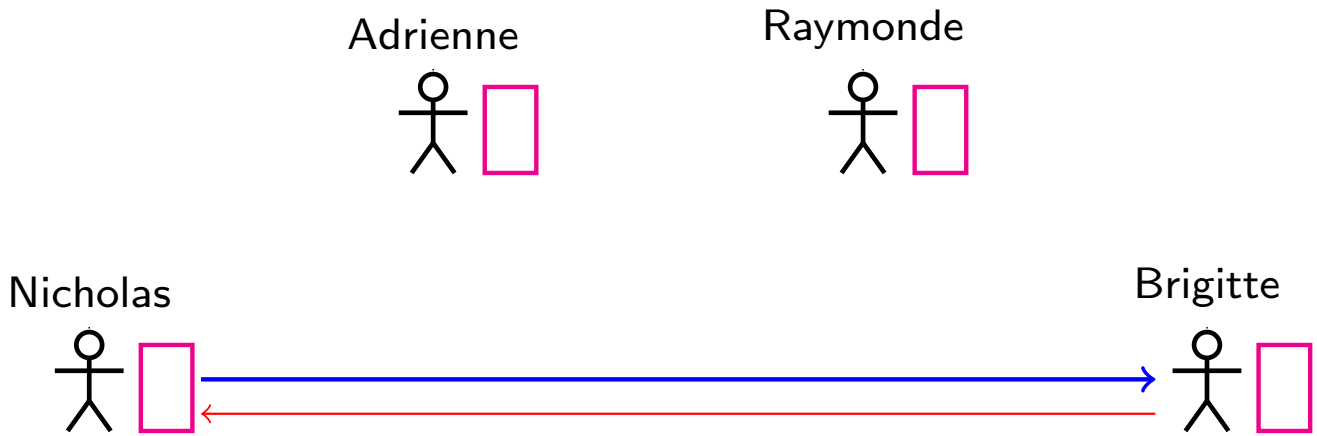




Cette situation s'apparente à la situation initiale mais, plutôt que d'avoir tout son argent dans ses poches, chacun possède une copie du registre des toutes les transactions du système.

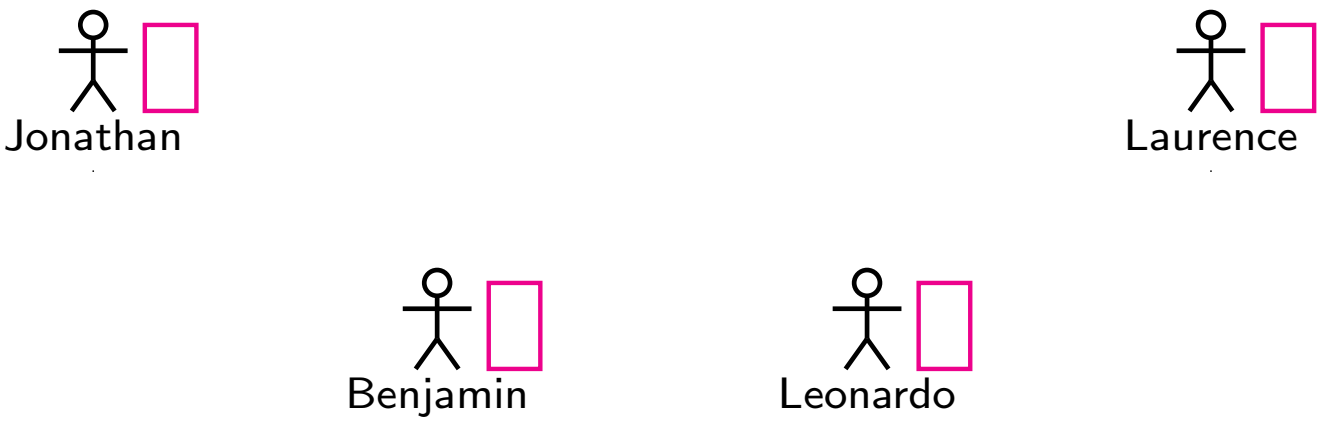


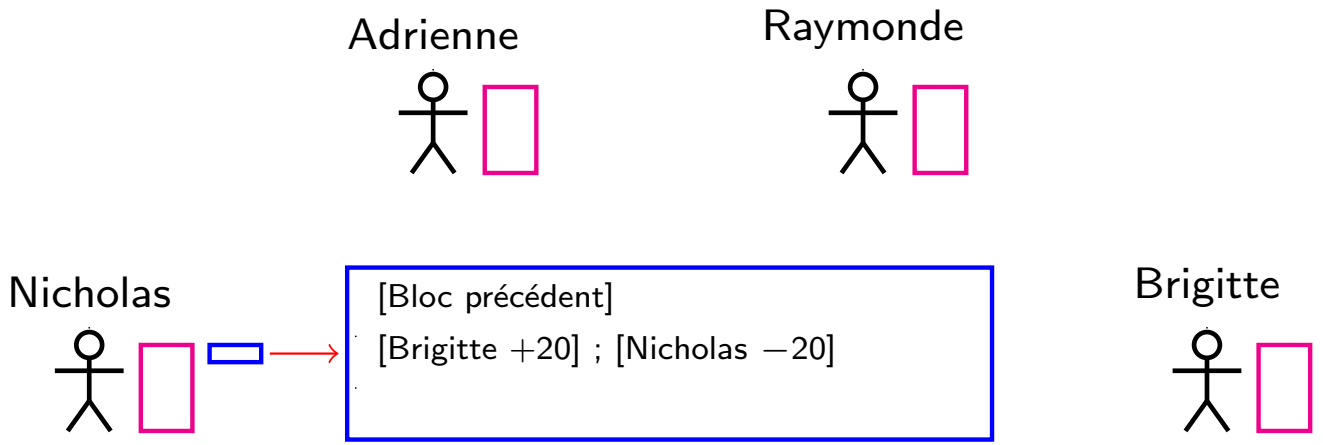




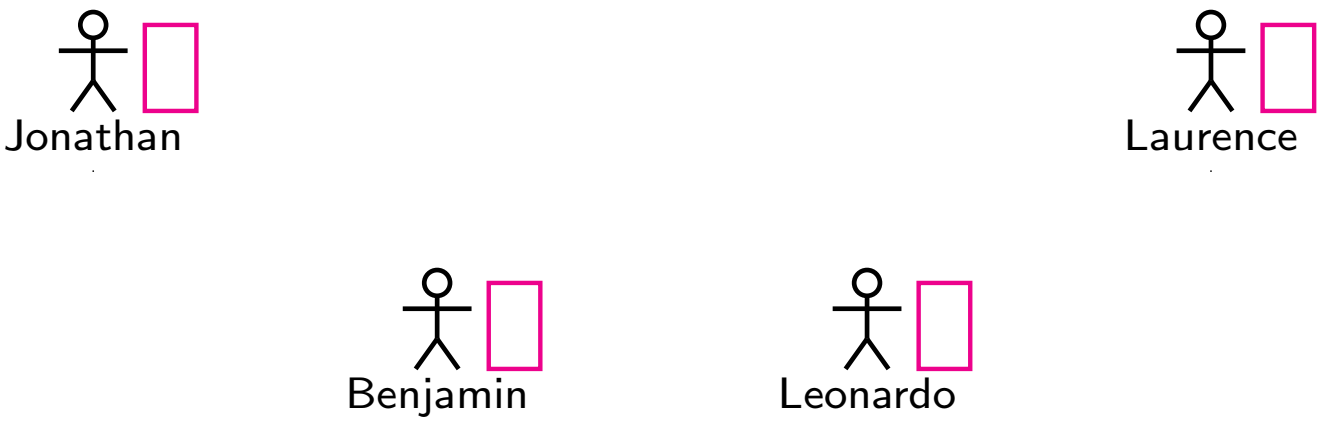
Si Nicholas désire acheter un bien ou service de Brigitte,
le registre que tous possède permet de vérifier si
Nicholas possède les “droits de dépenser” pour ce faire.

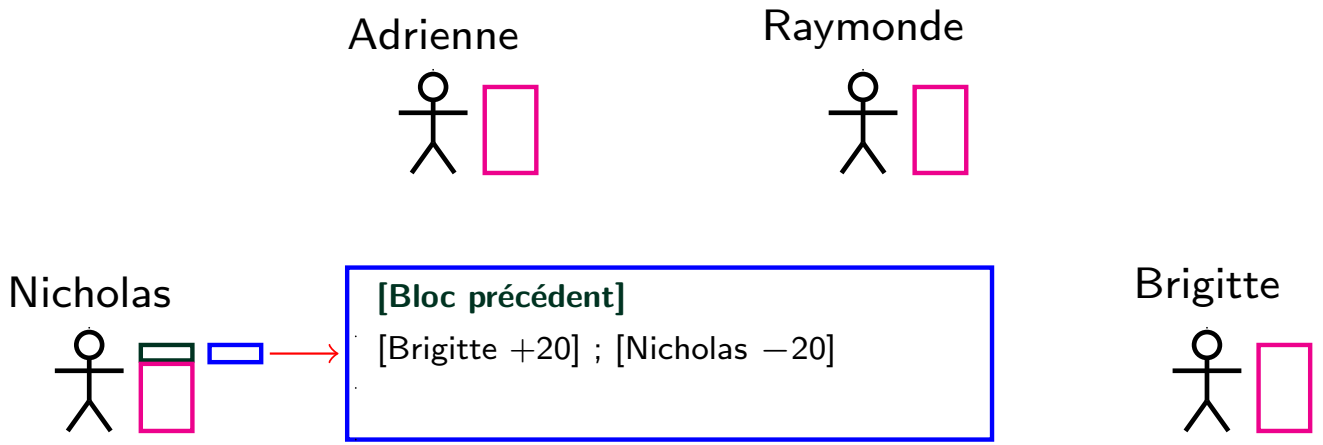
Une cryptomonnaie est un “droit de dépenser” à l’intérieur d’une “chaîne de blocs”.



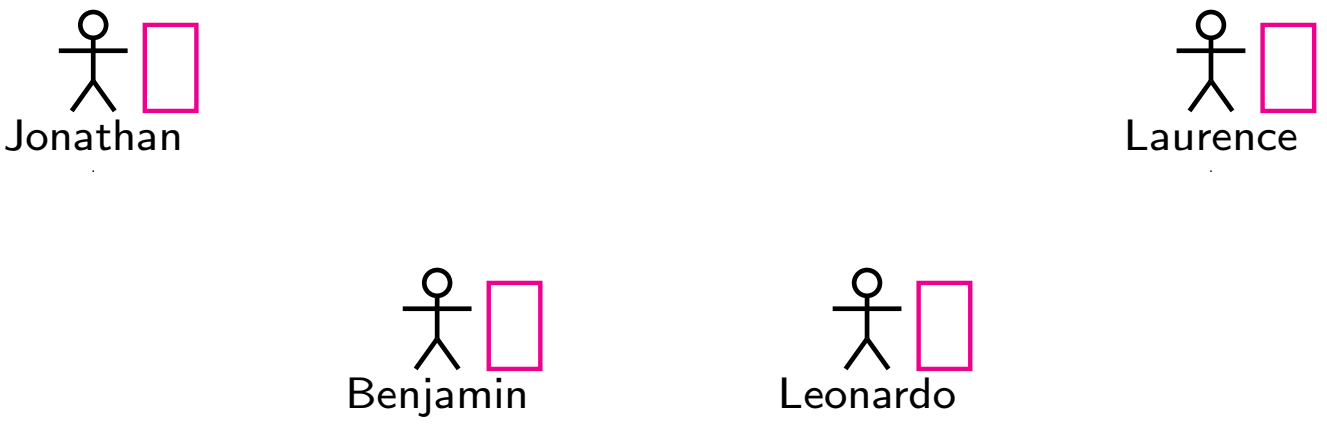


Après avoir contacté Brigitte dans le but de lui acheter un vélo
et s'être entendu avec elle pour un prix de 20 "cryptopoints"
Nicholas soumet au réseau une "permission de dépenser 20"
en metionnant que les 20 unités vont à Brigitte (bloc bleu).

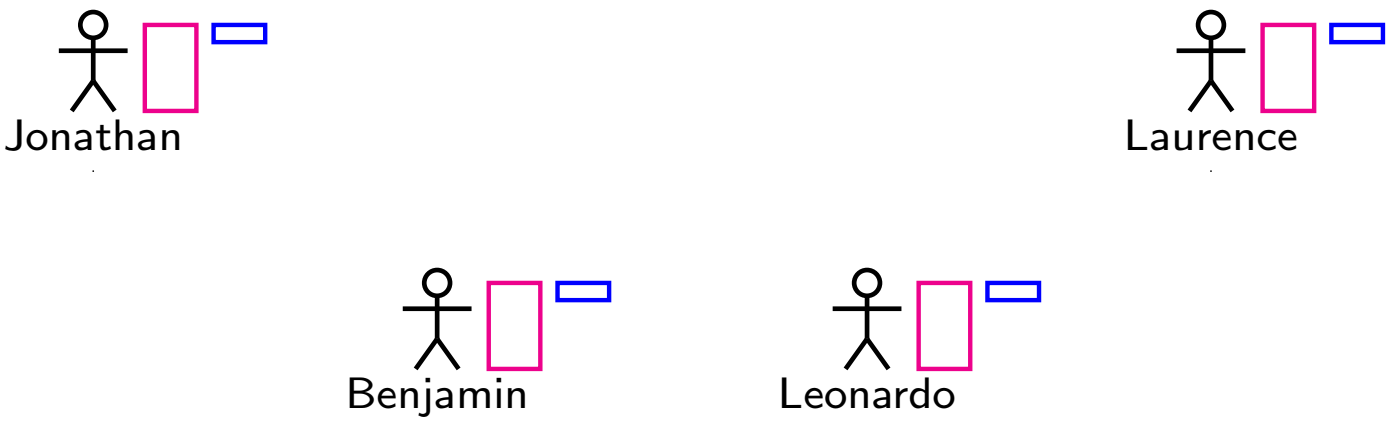


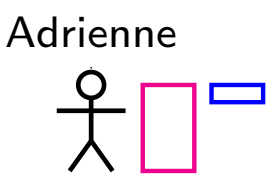


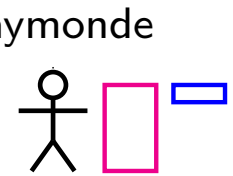
Le bloc soumis par Nicholas contient en premier lieu le hachage cryptographique du bloc au sommet de la chaîne,
le “bloc précédant” ce nouveau bloc.

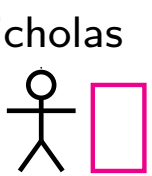


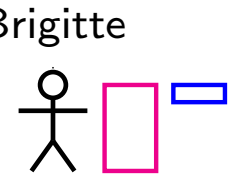
Les détenteurs de la chaîne (les “noeuds”) étudient
la “permission de dépenser 20” demandée par Nicholas
et vérifient que l’historique de transactions de Nicholas
lui donne le “droit de dépenser 20”.



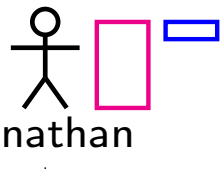


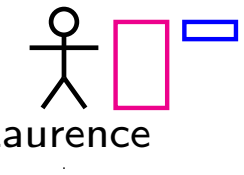


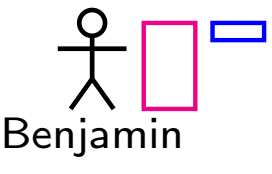


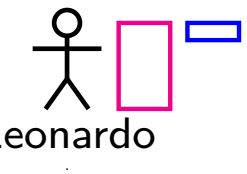


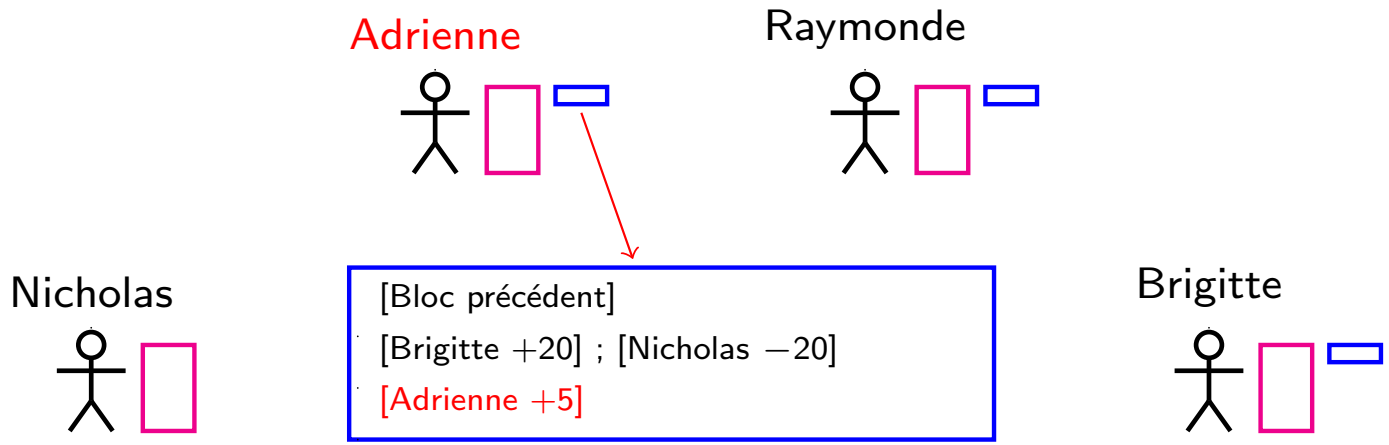
Une fois la transaction considérée valide, chaque noeud ajoute
la ligne “[Son nom +5]” à la suite de “[Brigitte +20] ; [Nicholas −20]”
et tente d’être le premier à “miner” ce nouveau bloc.
Le récompense “+5” est dictée par le protocole du réseau.



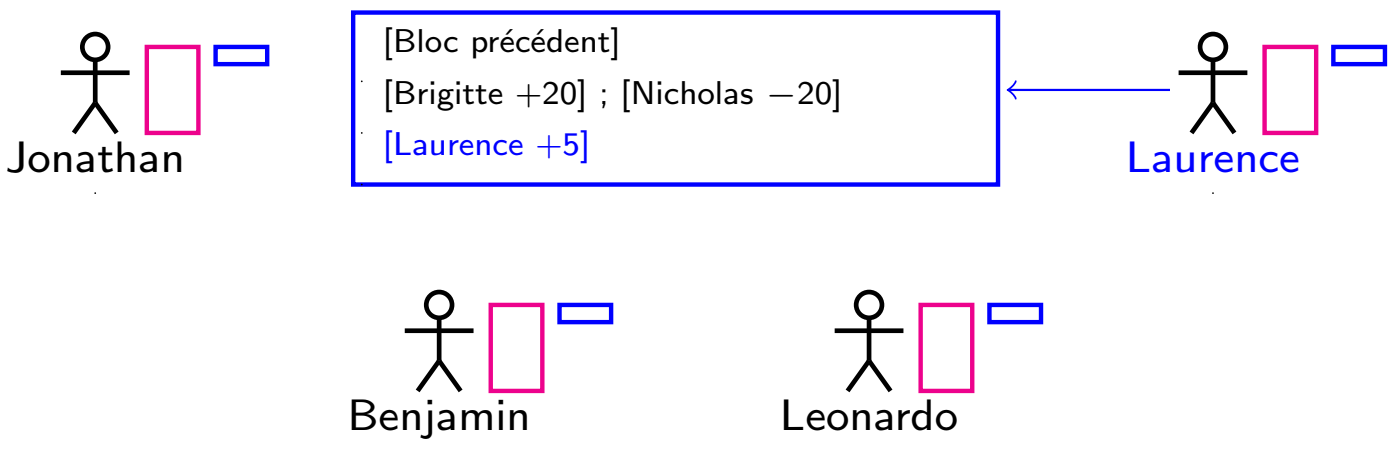




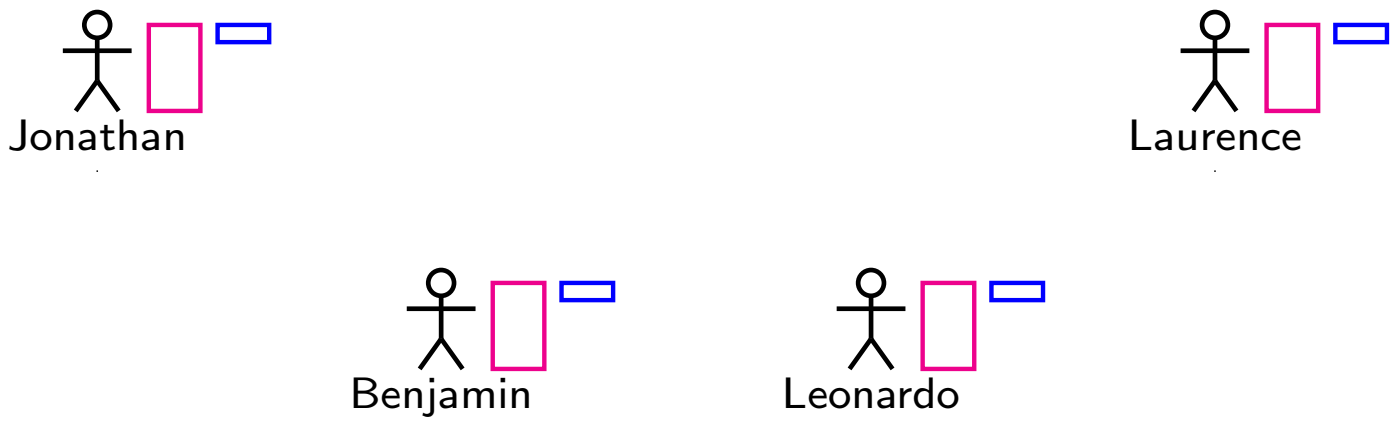


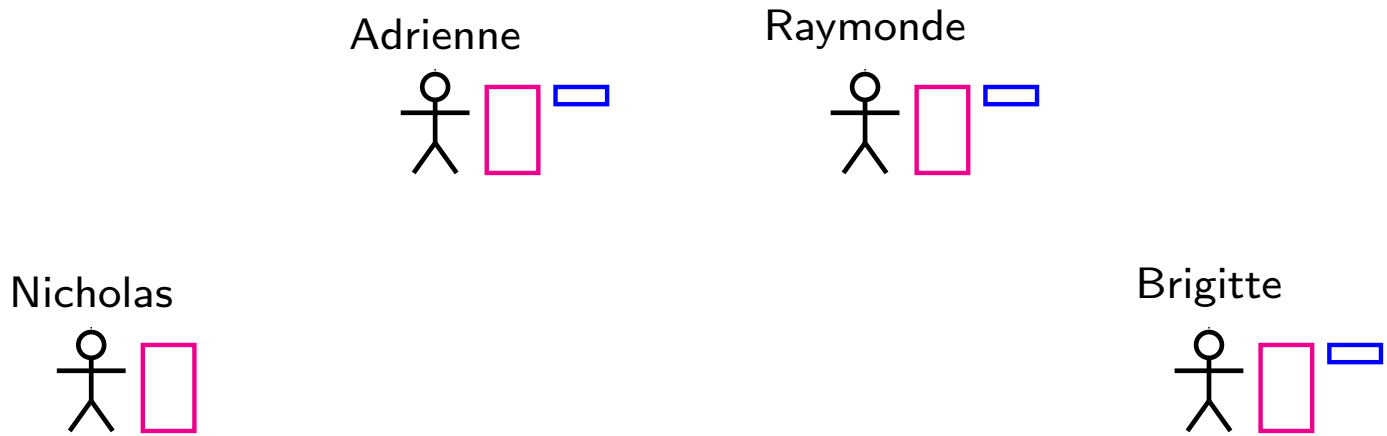


Adrienne ajoute la ligne “[Adrienne +5]” à la suite de “[Brigitte +20] ; [Nicholas −20]” dand le nouveau bloc.
Laurence ajoute la ligne “[Laurence +5]” à la suite de “[Brigitte +20] ; [Nicholas −20]” dand le nouveau bloc.

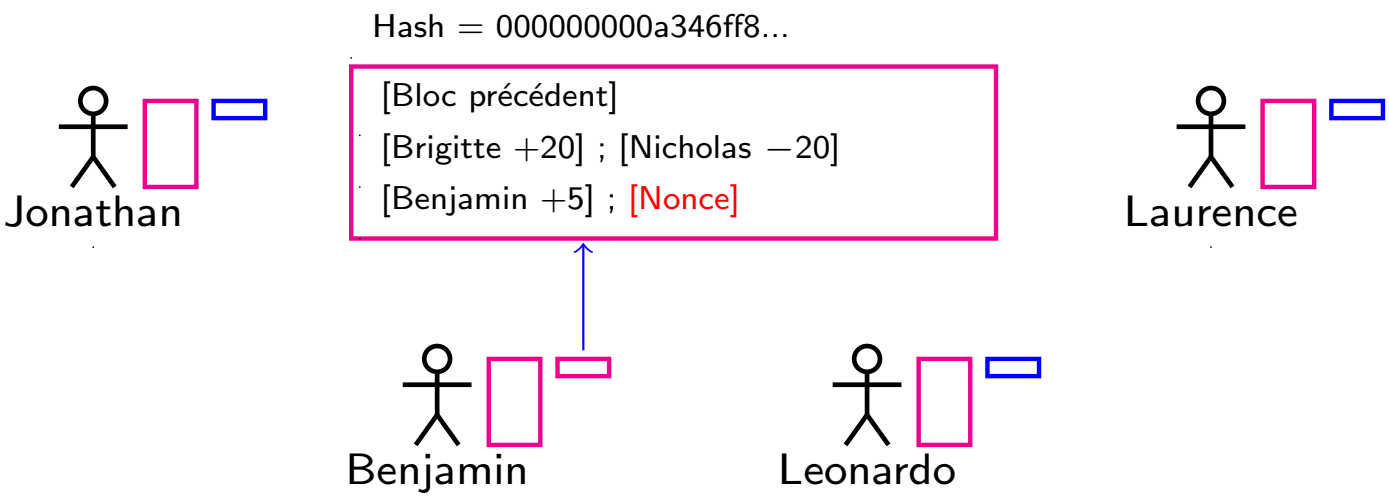


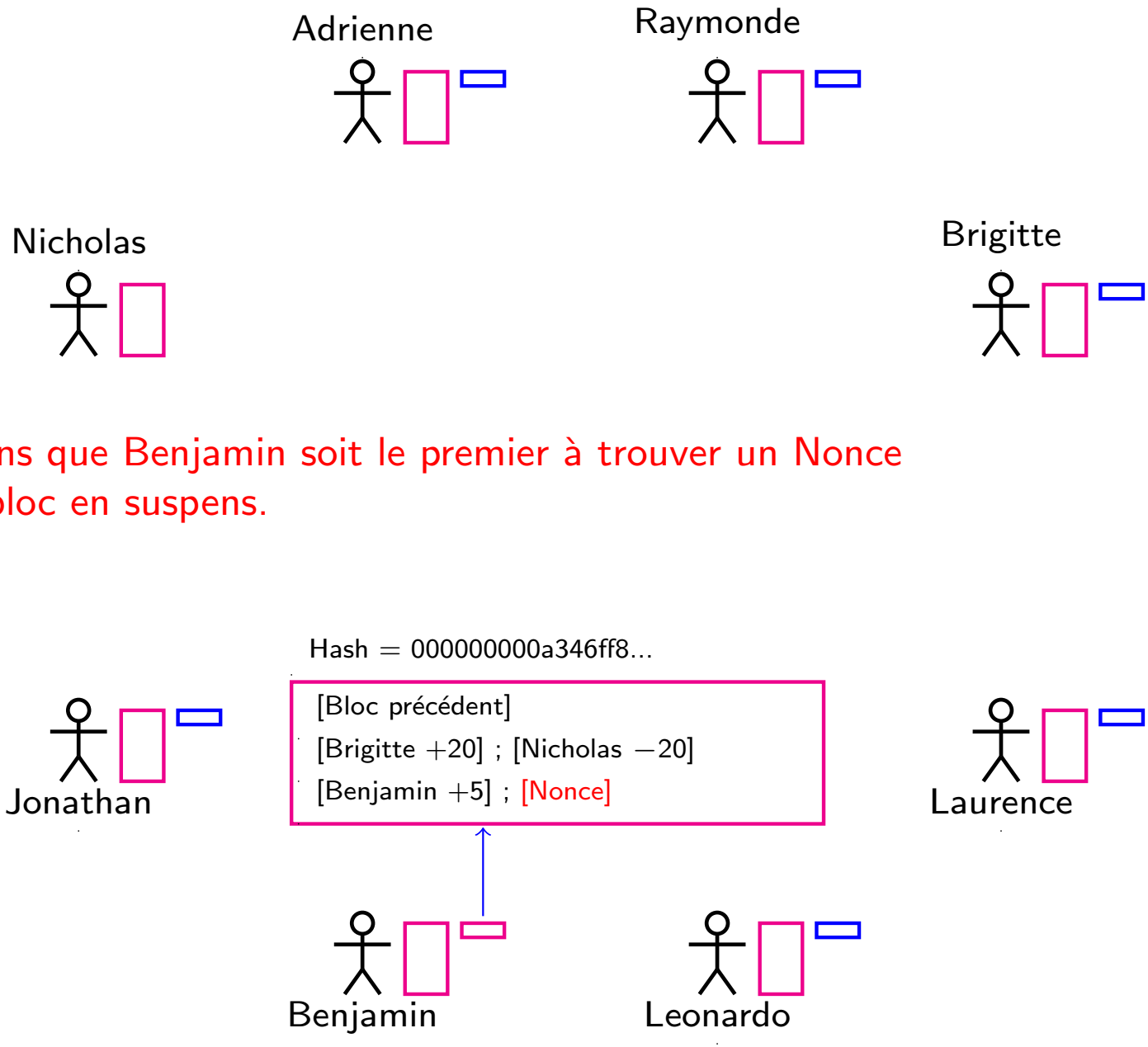
Chaque participant se met alors à “miner” son propre nouveau bloc, soit le bloc dans lequel il se voit octoyer 5 nouveaux cryptojetons. Cette opération est appelée minage dû à la création de nouveaux cryptojetons qui en résulte.



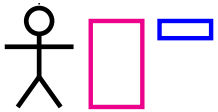


Le processus de minage consiste à ajouter un nombre ("Nonce") à la suite des informations d'un bloc de façon à ce que le hachage cryptographique (Hash) du bloc débute par le nombre de zéros requis par le protocole.

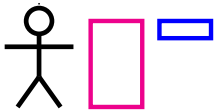



Adrienne
Raymonde
Nicholas
Brigitte
Supposons que Benjamin soit le premier à trouver un Nonce pour le bloc en suspens.
Hash = 000000000a346ff8...
[Bloc précédent]
[Brigitte +20] ; [Nicholas −20]
[Benjamin +5] ; [Nonce]
Jonathan
Laurence
Benjamin
Leonardo

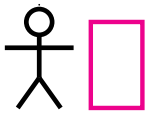
Adrienne



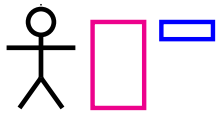
Raymonde



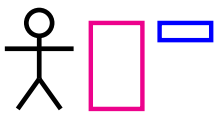
Nicholas



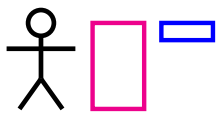
Brigitte



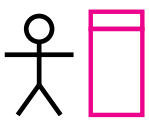
Benjamin ajoute alors le bloc miné à sa propre chaîne et annonce aux autres usagers qu'il a solutionné le problème. La chaîne de Benjamin est alors la plus longue du réseau.



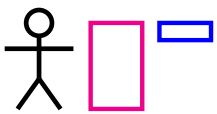
Jonathan



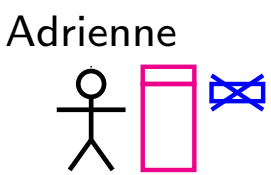
Laurence

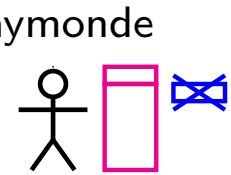


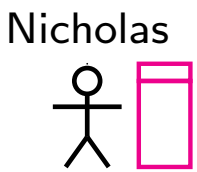
Benjamin

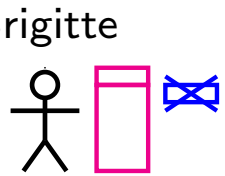


Leonardo

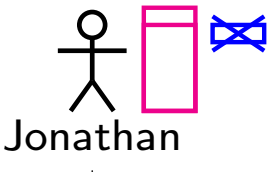


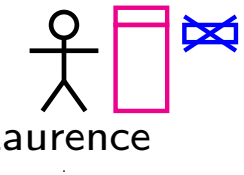


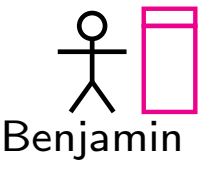


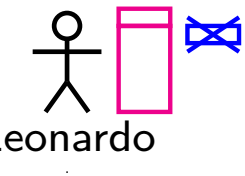


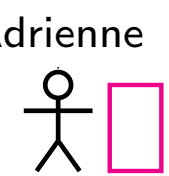
Il est alors dans le meilleur intérêt des autres usagers du réseau d'adopter la solution de Benjamin et, par le fait même, le nouveau bloc dans lequel Benjamin se voit octroyer une récompense plutôt que de s'entêter à miner leur propre solution.

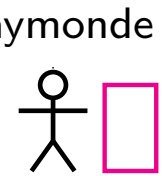


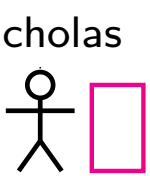


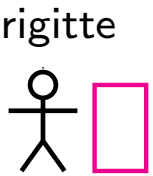




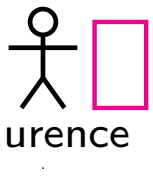


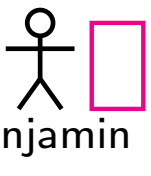


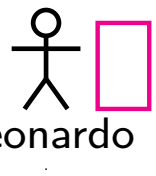




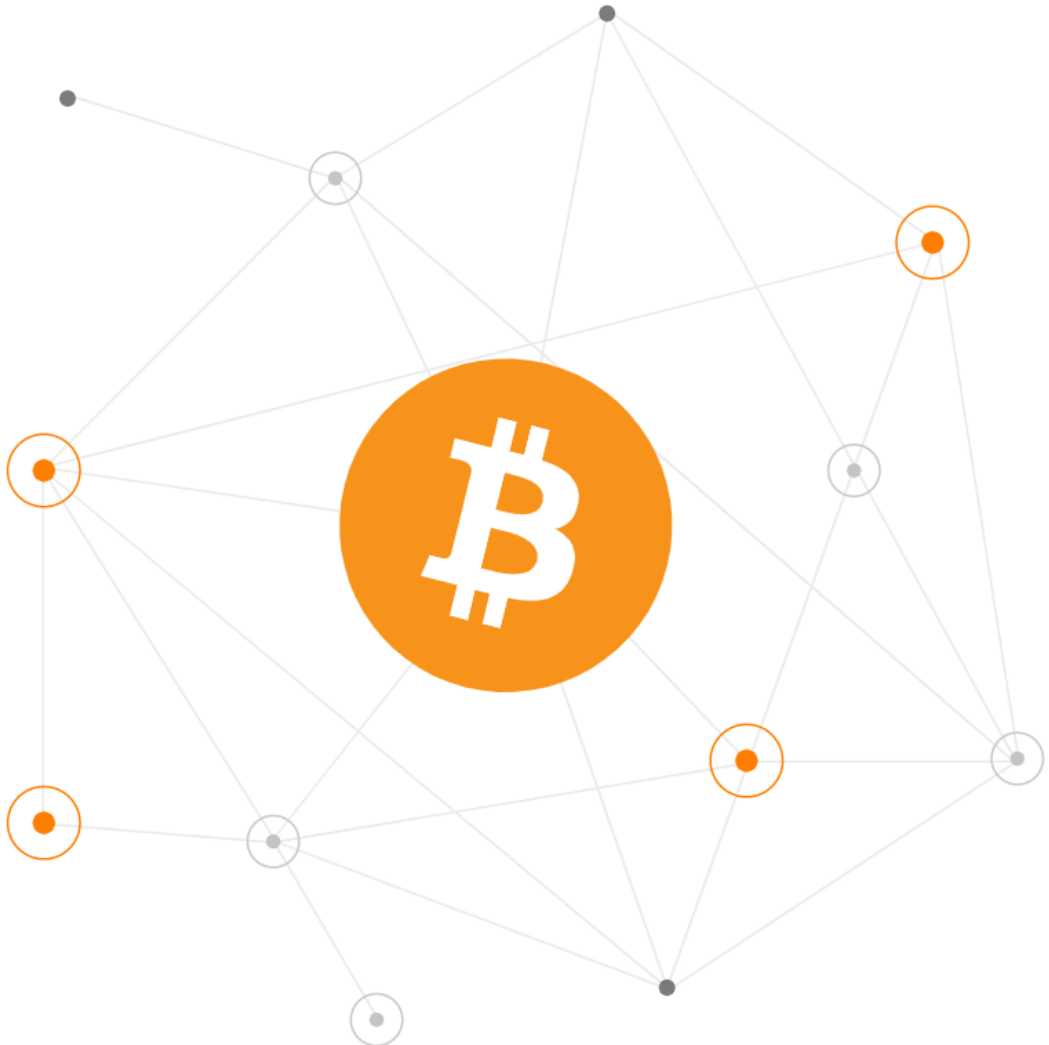
C'est ce mécanisme qui a été imaginé par Satoshi Nakamoto (2008)





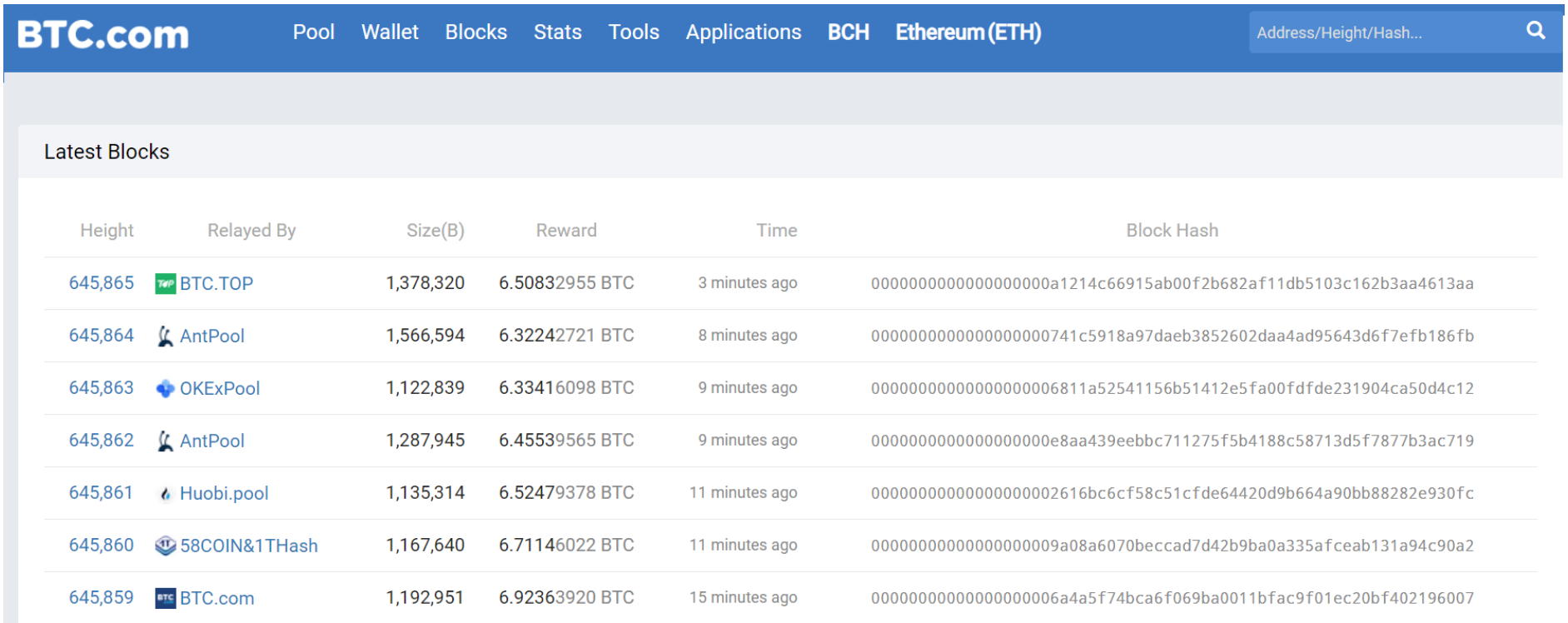


Bitcoin



Source: https://bitcoin.org/fr/

La chaîne de blocs du Bitcoin (Blockchain)



BTC.com Pool Wallet Blocks Stats Tools Applications BCH Ethereum (ETH) Address/Height/Hash...

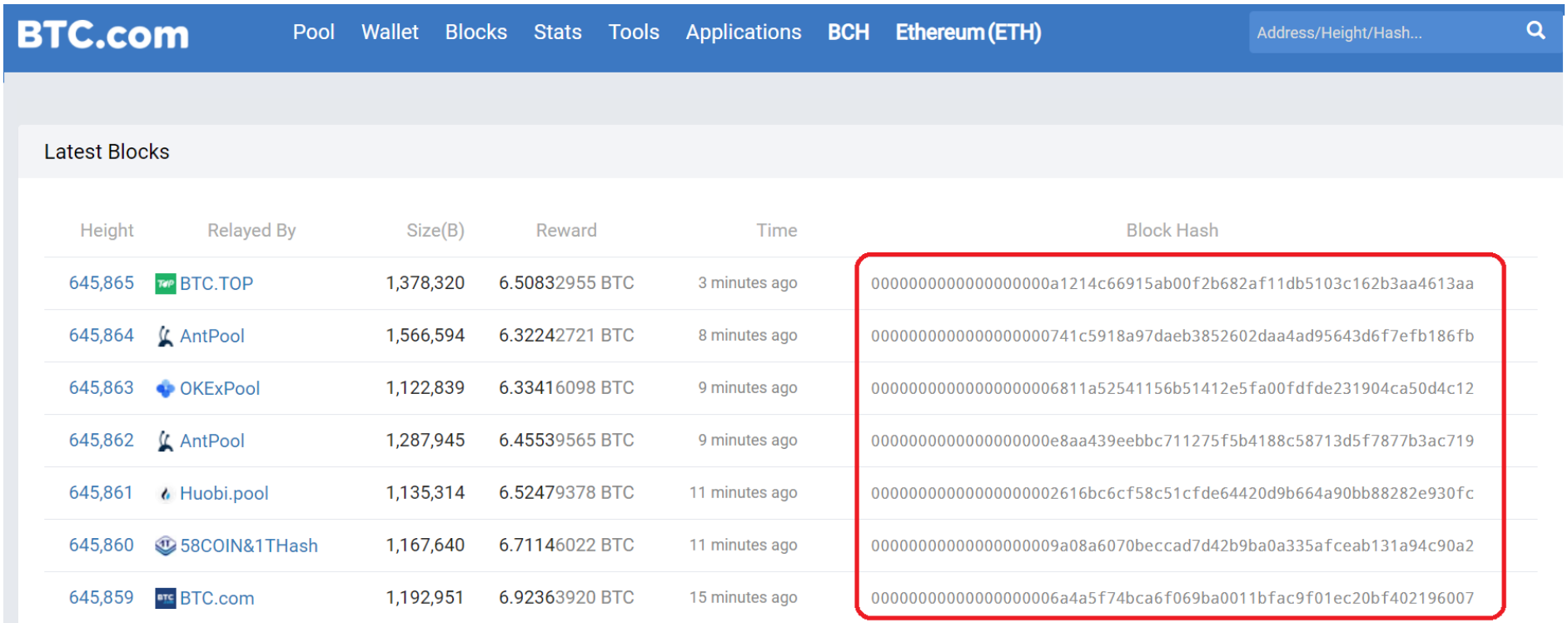
Latest Blocks

Height	Relayed By	Size(B)	Reward	Time	Block Hash
645,865	BTC.TOP	1,378,320	6.50832955 BTC	3 minutes ago	00000000000000000000a1214c66915ab00f2b682af11db5103c162b3aa4613aa
645,864	AntPool	1,566,594	6.32242721 BTC	8 minutes ago	00000000000000000000741c5918a97daeb3852602daa4ad95643d6f7efb186fb
645,863	OKExPool	1,122,839	6.33416098 BTC	9 minutes ago	00000000000000000006811a52541156b51412e5fa00fdfde231904ca50d4c12
645,862	AntPool	1,287,945	6.45539565 BTC	9 minutes ago	00000000000000000000e8aa439eebbc711275f5b4188c58713d5f7877b3ac719
645,861	Huobi.pool	1,135,314	6.52479378 BTC	11 minutes ago	00000000000000000002616bc6cf58c51cfde64420d9b664a90bb88282e930fc
645,860	58COIN&1THash	1,167,640	6.71146022 BTC	11 minutes ago	00000000000000000009a08a6070beccad7d42b9ba0a335afceab131a94c90a2
645,859	BTC.com	1,192,951	6.92363920 BTC	15 minutes ago	00000000000000000006a4a5f74bca6f069ba0011bfac9f01ec20bf402196007

Source: https://btc.com/

La chaîne de blocs du Bitcoin (Blockchain)

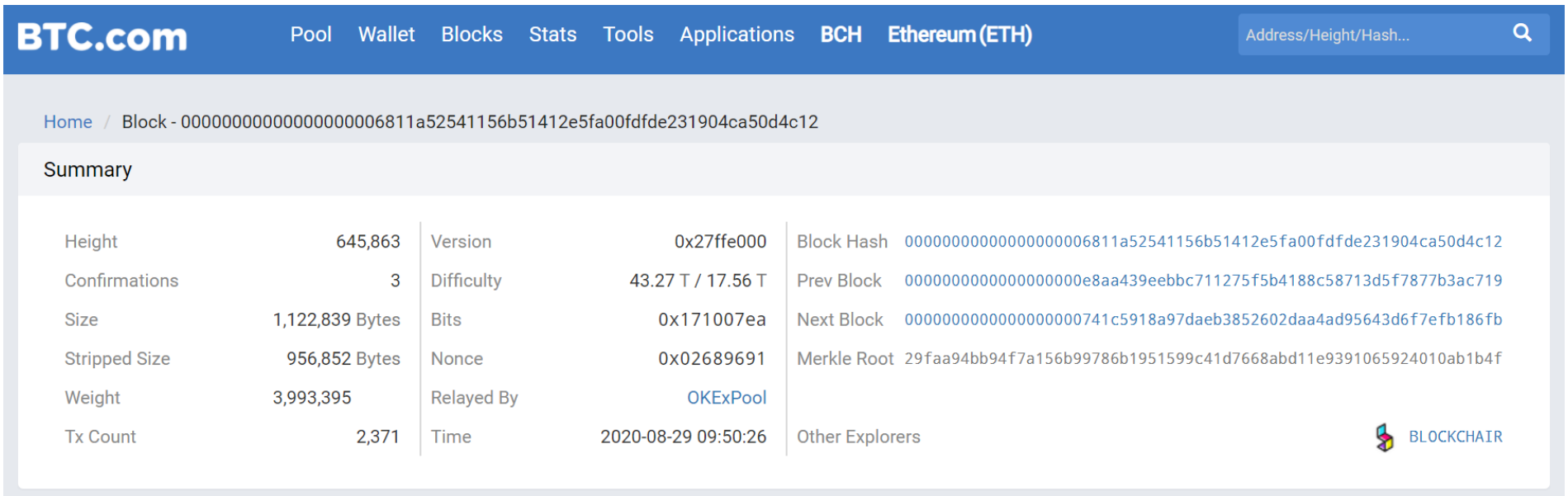
La chaîne de blocs



Source: https://btc.com/

La chaîne de blocs du Bitcoin (Blockchain)

Information contenue dans un bloc



Source: https://btc.com/

Système simplifié d'échange d'unités monétaires

Dans ce qui suit, nous allons décortiquer la mécanique d'un système très simple d'échange de monnaie basé sur une chaîne de blocs cryptographiques.

Huit individus, nommément Adrienne, Benjamin, Brigitte, Jonathan, Laurence, Leonardo, Nicholas et Raymonde, sont membres d'un réseau s'échangeant une cryptodevise appelée cryptopiastre.

Lorsque des cryptopiastres sont nouvellement émises, on indique que celles-ci proviennent du Caissier.

Système simplifié d'échange d'unités monétaires

Dans ce système d'échange, une transaction est toujours identifiée par une séquence de trois items, soient

[Usager qui envoie][Quantité de cryptopiastres][Usager qui reçoit],

où chacun des items est représenté à l'aide de huit caractères.

Puisque les noms de chacun des utilisateurs et Caissier contiennent huit lettres, ceux-ci sont inscrits tel quel dans l'énoncé d'une transaction.

Pour chaque quantité de cryptopiastres envoyée, suffisamment de zéros doivent être ajoutés devant celles-ci afin qu'elle occupe huit cases dans un message de transaction.

Système simplifié d'échange d'unités monétaires

Exemples de messages de transaction:

- Le message

  Laurence00000150Adrienne

  indique que Laurence envoie 150 cryptopiastres à Adrienne;

- Le message

  Caissier00000300Benjamin

  indique que 300 cryptopiastres nouvellement créées sont envoyées à Benjamin.

Ouverture du système

Le tableau qui suit montre les transactions qui ouvrent ce système d'échange, soit l'envoi de 1000 cryptopiastres à chacun des usagers par le Caissier.

Transactions du bloc 000

No	Texte	Description
TX01	Caissier00001000Laurence	Caissier envoie 1000 cryptopiastres à Laurence
TX02	Caissier00001000Nicholas	Caissier envoie 1000 cryptopiastres à Nicholas
TX03	Caissier00001000Adrienne	Caissier envoie 1000 cryptopiastres à Adrienne
TX04	Caissier00001000Benjamin	Caissier envoie 1000 cryptopiastres à Benjamin
TX05	Caissier00001000Raymonde	Caissier envoie 1000 cryptopiastres à Raymonde
TX06	Caissier00001000Leonardo	Caissier envoie 1000 cryptopiastres à Leonardo
TX07	Caissier00001000Brigitte	Caissier envoie 1000 cryptopiastres à Brigitte
TX08	Caissier00001000Jonathan	Caissier envoie 1000 cryptopiastres à Jonathan

Ouverture du système

La première étape de la construction de la chaîne de blocs de ce système consiste à convertir chaque message de transaction (le Texte) en un **nombre hexadécimal à 64 caractères** à l'aide de la routine **SHA-256**.

Conversion hash des transactions du bloc 000

HTX01	a0fcaf27253ce349e35178f4001d17c53fc9910de6f0d2fa115b428b62445b16
HTX02	11168f9f6918eb543f97d88a41f7af59694b71ef9980fb98a235c93314473398
HTX03	1701b5282dbd5bcf184f8d7fc9dbf348b21720a90a4a0ebc541ce282e96a8583
HTX04	dd958b84406be9a4dc3eade4b2f229846b19e37e289937ef59d189cdf4d8c02a
HTX05	82eaa24a2d2156831275c8144aa276c278973451a90616695c27014d7967e3dd
HTX06	d969f9a49b43c8265da1bbbd7bff21fedf5cb7df2ad12719d52c1fa737ea7a3d
HTX07	79a64a10687e7dba02d623e31ecdece11b7c85e3cff45f92d111b8bc188acb60
HTX08	1de237a4ffc44b780502119216e7ebf5ba1020f5bb4f86f21ce19edecdb017ad

Conversion hash (hachage cryptographique)

- Routine SHA-256 (représentée par la fonction $H(\cdot)$):

$$H(\text{Série de caractères}) \Rightarrow \text{Nombre hexadécimal à 64 caractères.}$$

  Un nombre hexadécimal est un nombre exprimé en base 16.

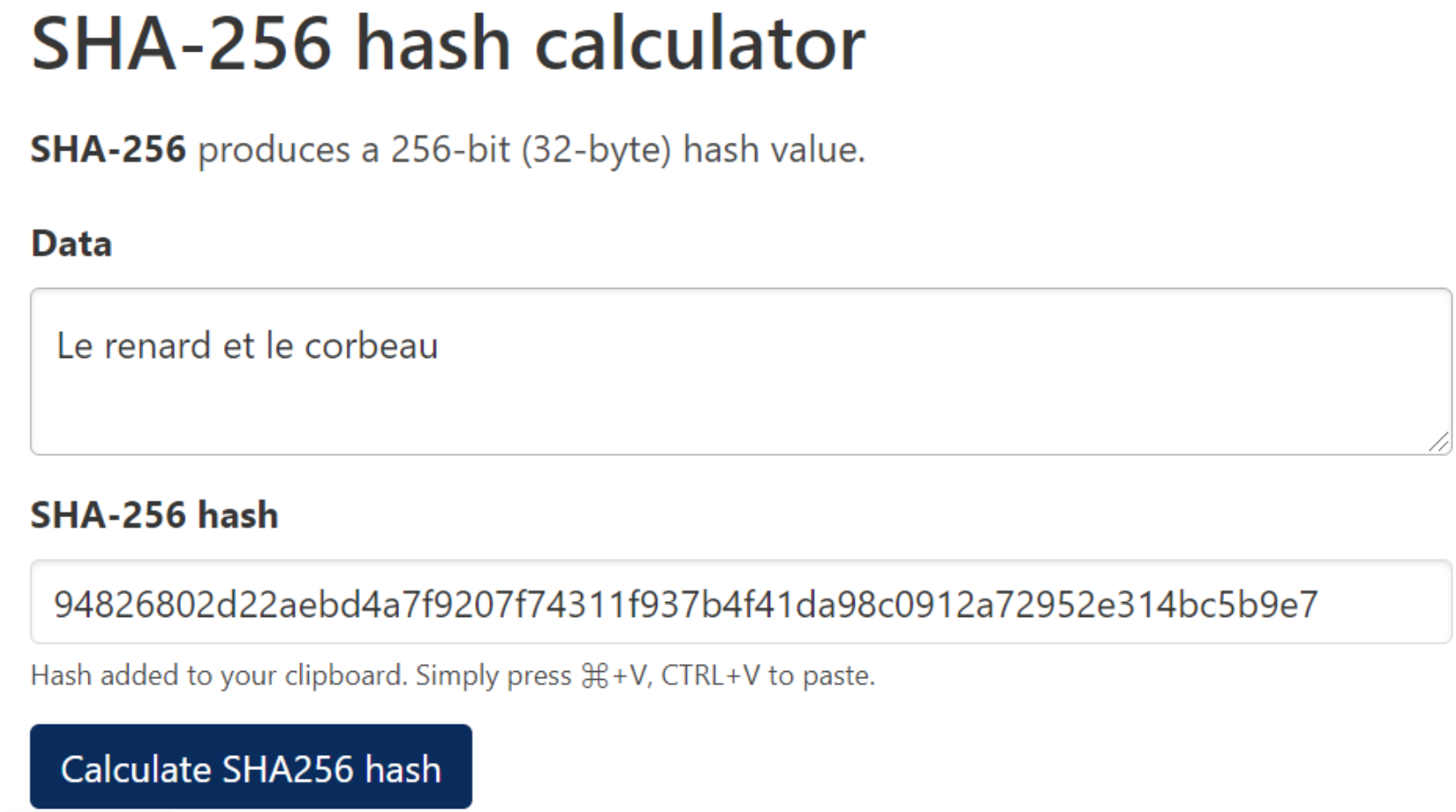
- Le hachage cryptographique est unidirectionnel mais facilement vérifiable si on connaît l'entrée d'origine:
  - Il est impossible de retracer le texte entré à partir d'une conversion hash, i.e.

$$H(\text{Série de caractères}) \not\Rightarrow \text{Série de caractères;}$$

  - Si on connaît la série exacte de caractères entrée et le nombre hexadécimal de sortie, la vérification

$$H(\text{Série de caractères}) = \text{Nombre hexadécimal}$$

    demande très peu de puissance computationnelle.



Source: https://xorbin.com/tools/sha256-hash-calculator

Hachage cryptographique (hash)–SHA-256

SHA-256 hash calculator

SHA-256 produces a 256-bit (32-byte) hash value.

Data

Le renard et le corbEau

SHA-256 hash

5fed2944734daec21da7410a19251196d8d3e916ef16559b2c835539728f4155

Hash added to your clipboard. Simply press ⌘+V, CTRL+V to paste.

Calculate SHA256 hash

Source: https://xorbin.com/tools/sha256-hash-calculator

Base 10

En base 10, le nombre 893 452 fait référence à l'opération suivante:

$$8\times10^5 + 9\times10^4 + 3\times10^3 + 4\times10^2 + 5\times10^1 + 2\times10^0$$

La représentation d'un nombre en base 10 utilise 10 caractères, soient $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

En base 10, la valeur du caractère le plus élevé utilisé est 9.

Nombres en base 2

Base 2

En base 2, le nombre 110010 fait référence à l'opération suivante:

$$1\times2^5 + 1\times2^4 + 0\times2^3 + 0\times2^2 + 1\times2^1 + 0\times2^0$$

La représentation en base 2 utilise 2 caractères, soient $\{0, 1\}$.

En base 2, la valeur du caractère le plus élevé est 1.

Base 16

En base 16, le nombre 8964 fait référence à l'opération suivante:

$$8\times16^3 + 9\times16^2 + 6\times16^1 + 4\times16^0.$$

Avec 16 comme base, les caractères utilisés doivent aller jusqu'à la valeur 15, i.e. nous avons besoin de caractères valant 10, 11, 12, 13, 14 et 15.

Les caractères 10, 11, 12, 13, 14 et 15 sont représentés par les lettres a, b, c, d, e, et f (minuscule ou majuscule).

La représentation d'un nombre en base 16 utilise 16 caractères, soient $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f\}$.

Ainsi, 45a8f en base 16 fait référence à

$$4\times16^4 + 5\times16^3 + 10\times16^2 + 8\times16^1 + 15\times16^0.$$

Base 2, base 10, base 16

Base 2	0000	0001	0010	0011	0100	0101	0110	0111
Base 10	0	1	2	3	4	5	6	7
Base 16	0	1	2	3	4	5	6	7

Base 2	1000	1001	1010	1011	1100	1101	1110	1111
Base 10	8	9	10	11	12	13	14	15
Base 16	8	9	a	b	c	d	e	f

Mécanique du hachage cryptographique

Voici une routine simplifiée de hachage cyptographique produisant un nombre hexadécimal à 8 caractères:

1. Convertir chaque caractère du texte en son code ASCII, y incluant les espaces et la ponctuation;
2. Convertir le code ASCII de chaque caractère en sa représentation binaire à 8 caractères, en ajoutant suffisamment de zéros devant chaque nombre afin qu'il occupe 8 cases;
3. Organiser les nombres binaires à 8 caractères en une matrice à 32 colonnes, en rajoutant suffisamment de zéros au besoin à la dernière ligne afin que celle-ci soit de la bonne longueur;
4. Fusionner les lignes ensemble à l'aide d'opérations binaires jusqu'à ce qu'il ne reste qu'une seule ligne;
5. Convertir la ligne finale en format hexadécimal.

Mécanique du hachage cryptographique

Nous allons appliquer notre routine simple au texte “Le chat saute.”

	Code ASCII	
Caractère	**Base 10**	**Base 2**
L	76	01001100
e	101	01100101
Espace	32	00100000
c	99	01100011
h	104	01101000
a	97	01100001
t	116	01110100
Espace	32	00100000
s	115	01110011
a	97	01100001
u	117	01110101
t	116	01110100
e	101	01100101
.	46	00101110

Mécanique du hachage cryptographique

A: Touches et nombres binaires

L	e	[Espace]	c
01001100	01100101	00100000	01100011
h	a	t	[Espace]
01101000	01100001	01110100	00100000
s	a	u	t
01110011	01100001	01110101	01110100
e	.		
01100101	00101110		

B: Nombres binaires seulement

01001100 01100101 00100000 01100011

01101000 01100001 01110100 00100000

01110011 01100001 01110101 01110100

01100101 00101110

Mécanique du hachage cryptographique

C: Matrice binaire incomplète

0100110001100101001000001100011

0110100001100001011101000010000 0

0111001101100001011101010111010 0

0110010100101110

D: Matrice binaire complète

0100110001100101001000001100011

0110100001100001011101000010000 0

0111001101100001011101010111010 0

0110010100101110000000000000000 0

Opérations sur les lignes 1 et 3	
Ligne 1:	01001100011001010010000001100011
Ligne 2:	01101000011000010111010000100000
Ligne 3:	01110011011000010111010101110100
Ligne 4:	01100101001011100000000000000000
Ligne 1 (L1):	01001100011001010010000001100011
Ligne 3 (L3):	01110011011000010111010101110100
L1 XOR L3:	00111111000001000101010100010111
Rotation de 8 bits	
L1 XOR L3:	00111111000001000101010100010111
Résultat (A1):	00000100010101010001011100111111

Mécanique du hachage cryptographique

Opérations sur les lignes 2 et 4	
Ligne 1:	01001100011001010010000001100011
Ligne 2:	01101000011000010111010000100000
Ligne 3:	01110011011000010111010101110100
Ligne 4:	01100101001011100000000000000000
Ligne 2 (L2):	01101000011000010111010000100000
Ligne 4 (L4):	01100101001011100000000000000000
L2 XOR L4:	00001101010011110111010000100000
Rotation de 8 bits	
L2 XOR L4:	00001101010011110111010000100000
Résultat (A2):	01001111011101000010000000001101

Mécanique du hachage cryptographique

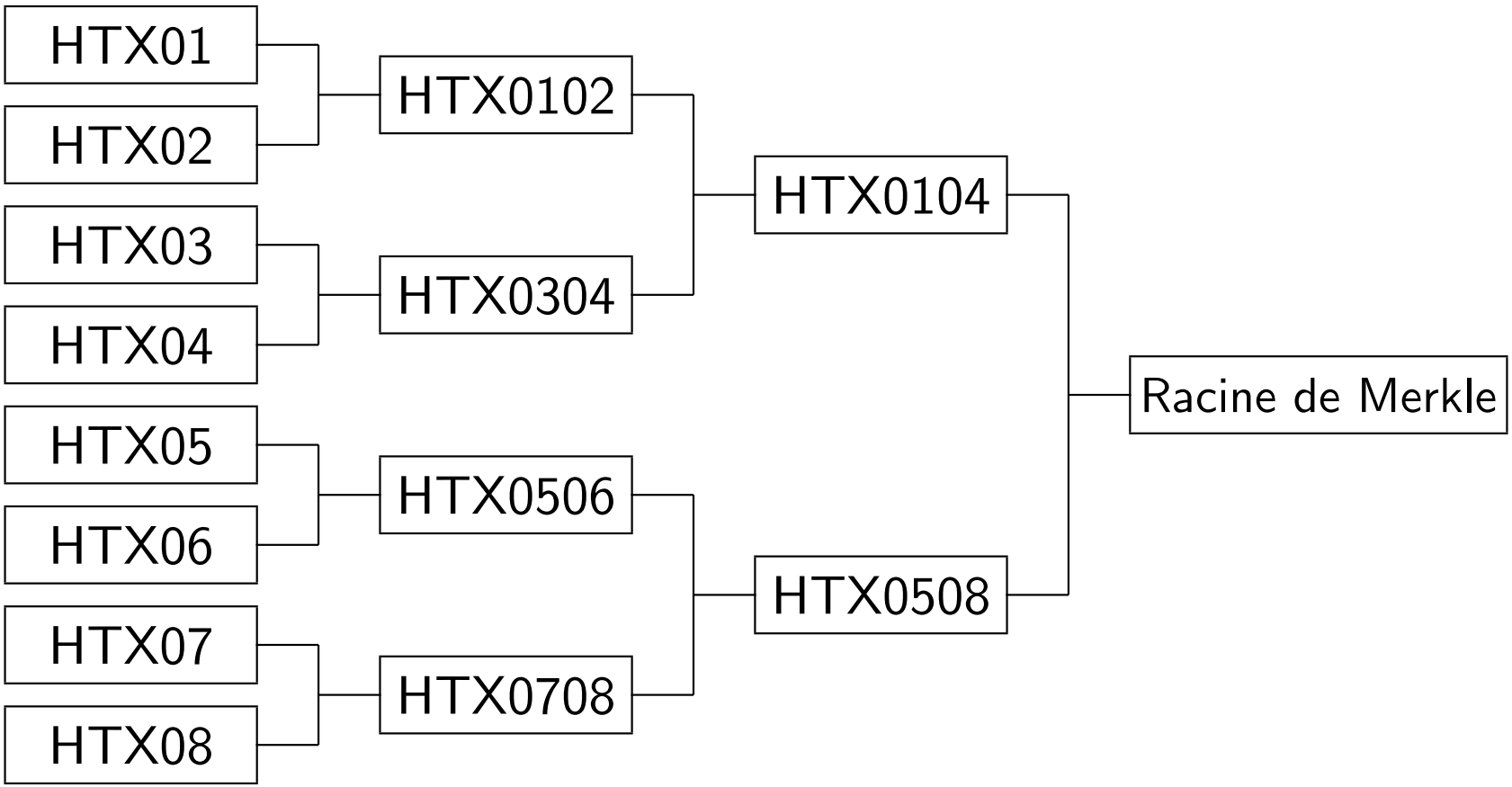
Opérations lignes A1 et A2	
A1:	00000100010101010001011100111111
A2:	01001111011101000010000000001101
A1 XOR A2:	01001011001000010011011100110010
Rotation de 8 bits	
A1 XOR A2:	01001011001000010011011100110010
Résultat (A3):	00100001001101110011001001001011

Conversion de la ligne A3 en format hexadécimal	
A3:	00100001001101110011001001001011
	0010 0001 0011 0111 0011 0010 0100 1011
	$\underbrace{0010}_{2}$ $\underbrace{0001}_{1}$ $\underbrace{0011}_{3}$ $\underbrace{0111}_{7}$ $\underbrace{0011}_{3}$ $\underbrace{0010}_{2}$ $\underbrace{0100}_{4}$ $\underbrace{1011}_{b}$
A3 hexadécimal:	**2137324b**

De retour à notre système

Conversion hash des transactions du bloc 000	
HTX01	a0fcaf27253ce349e35178f4001d17c53fc9910de6f0d2fa115b428b62445b16
HTX02	11168f9f6918eb543f97d88a41f7af59694b71ef9980fb98a235c93314473398
HTX03	1701b5282dbd5bcf184f8d7fc9dbf348b21720a90a4a0ebc541ce282e96a8583
HTX04	dd958b84406be9a4dc3eade4b2f229846b19e37e289937ef59d189cdf4d8c02a
HTX05	82eaa24a2d2156831275c8144aa276c278973451a90616695c27014d7967e3dd
HTX06	d969f9a49b43c8265da1bbbd7bff21fedf5cb7df2ad12719d52c1fa737ea7a3d
HTX07	79a64a10687e7dba02d623e31ecdece11b7c85e3cff45f92d111b8bc188acb60
HTX08	1de237a4ffc44b780502119216e7ebf5ba1020f5bb4f86f21ce19edecdb017ad

Racine de Merkle



Racine de Merkle du bloc 000

Conversion hash des transactions du bloc 000	
HTX01	a0fcaf27253ce349e35178f4001d17c53fc9910de6f0d2fa115b428b62445b16
HTX02	11168f9f6918eb543f97d88a41f7af59694b71ef9980fb98a235c93314473398
HTX03	1701b5282dbd5bcf184f8d7fc9dbf348b21720a90a4a0ebc541ce282e96a8583
HTX04	dd958b84406be9a4dc3eade4b2f229846b19e37e289937ef59d189cdf4d8c02a
HTX05	82eaa24a2d2156831275c8144aa276c278973451a90616695c27014d7967e3dd
HTX06	d969f9a49b43c8265da1bbbd7bff21fedf5cb7df2ad12719d52c1fa737ea7a3d
HTX07	79a64a10687e7dba02d623e31ecdece11b7c85e3cff45f92d111b8bc188acb60
HTX08	1de237a4ffc44b780502119216e7ebf5ba1020f5bb4f86f21ce19edecdb017ad
Fusion 2×2 des hash du bloc 000	
HTX0102	727bdccfe1d86c34e60dc8e6c4b54ad8416a394f474cfe32e8325c788128461b
HTX0304	3cd67b8cef88cf30780152c385f42ea6cb7a9ce5be49cd5fdd550ffaffcf7db0
HTX0506	dc2434da92877b9d9cd25e9ed33e2830d297ae3cafdfceb13cc19c7d6cdf4798
HTX0708	ca3244b896cbce1aa7b312737001b29090d3540cde4c7d514289e18cd91aad14
Fusion 2×2 des hash précédents	
HTX0104	6af7a1839982f3356daec7466c4bda3ec8182d7b33d70911bde3f95b1dff16aa
HTX0508	5cf37deca7abaeaea5e5b439de57dbd1aef1c200bb014523db18406b27569cd3
Racine de Merkle du bloc 000	
HTX0104	0d9fdc657f16c466b015c46953ba54f1d50ce9a9d94e54bea9fd73141f588a09

Minage de bloc

Pour inclure un bloc dans la chaîne, il faut que celui-ci soit “miné”.

Le minage d'un bloc consiste à trouver un Nonce tel que

$$H(\text{Bloc précédent}|\text{Racine de Merkle}|\text{Nonce})$$

débute par le nombre requis de zéros.

Minage de bloc

Le Nonce est un nombre hexadécimal à 8 caractères trouvé en hachant successivement

$$
\begin{aligned}
&H(\text{Bloc précédent}|\text{Racine de Merkle}|00000001)\\
&H(\text{Bloc précédent}|\text{Racine de Merkle}|00000002)\\
&H(\text{Bloc précédent}|\text{Racine de Merkle}|00000003)\\
&\vdots\\
&H(\text{Bloc précédent}|\text{Racine de Merkle}|00000009)\\
&H(\text{Bloc précédent}|\text{Racine de Merkle}|0000000a)\\
&H(\text{Bloc précédent}|\text{Racine de Merkle}|0000000b)\\
&\vdots\\
&H(\text{Bloc précédent}|\text{Racine de Merkle}|0000000f)\\
&H(\text{Bloc précédent}|\text{Racine de Merkle}|00000010)\\
&H(\text{Bloc précédent}|\text{Racine de Merkle}|00000011)\\
&\vdots
\end{aligned}
$$

jusqu'à ce que le hash obtenu débute par au moins le nombre désiré de zéros (cinq zéros dans notre exemple).

Minage de bloc

Partant des transactions et de la racine de Merkle du bloc 000, et en utilisant une séquence de 64 zéros comme bloc précédent, nous obtenons le Nonce 0009dc00:

$$H(\underbrace{0000000000000000000000000000000000000000000000000000000000000000}_{\text{...0d9fdc...}}\underbrace{\text{...657f16c466b015c46953ba54f1d50ce9a9d94e54bea9fd73141f588a090}}_{\text{0009dc00}})$$

$$= \text{00000b069faa93bb672947157065403b609ce6a09c7f9b3d7ab0b74e6a6d6981}$$

Chaîne de blocs

La chaîne de blocs suite au minage du bloc 000 est ainsi:

Bloc	Hash
000	00000b069faa93bb67294715706540 3b609ce6a09c7f9b3d7ab0b74e6a6d6981 0000000000000000000000000000000000000000000000000000000000000000

Bloc 001

Transactions du bloc 001

No	Texte	Description
TX01	Adrienne00000243Nicholas	Adrienne envoie 243 cryptopiastres à Nicholas
TX02	Brigitte00000508Benjamin	Brigitte envoie 508 cryptopiastres à Benjamin
TX03	Laurence00000467Raymonde	Laurence envoie 467 cryptopiastres à Raymonde
TX04	Caissier00000100Leonardo	Caissier envoie 100 cryptopiastres à Leonardo
Conversion hash des transactions du bloc 001		
HTX01	d1ad346c8bd6374084155447208facfd6d96325315bbdc732633e8134a5cdf2d	
HTX02	65e43f1e7a195c68df3d56134349361d3d1e48918f3271c7dfd459ac669cbfe3	
HTX03	b881b0131f6510f648b3fdcdae0ae13afc213dbb57194e04dacdcc043609e80c	
HTX04	ecfd64002bea5c38d7c03086e84f1967793636afbfa194760e141b09f60364cd	
Fusion 2×2 des hash du bloc 001		
HTX0102	00469f5badb0b115f85e136831369e5440dac2ef9e1057ffef42e8b750cdcc4f	
HTX0304	6c090828c77b7f77ae6a39baf8af28e3188b9921fb4e7d4fd281e0bfec75b75a	
Racine de Merkle du bloc 001		
HTX0104	210f9eebe13201f3bfecca54ac10fd1999eb2c8cb90dd0d09bccc8a80c6566fa	

Bloc 001

Génération du bloc 001
Bloc précédent
00000b069faa93bb67294715706540 3b609ce6a09c7f9b3d7ab0b74e6a6d6981
Racine de Merkle du bloc 001
210f9eebe13201f3bfecca54ac10fd1999eb2c8cb90dd0d09bccc8a80c6566fa
Nonce du bloc 001
0023ddbc
Bloc 001
00000b0e48cab946eec6ba2d313b8168c73bb457e8ae105107f1fbd6d4097cc5

Chaîne de blocs

Chaîne de blocs suite au minage du bloc 001

Bloc	Hash
001	00000b0e48cab946eec6ba2d313b8168c73bb457e8ae105107f1fbd6d4097cc5
000	00000b069faa93bb67294715706540 3b609ce6a09c7f9b3d7ab0b74e6a6d6981
	0000000000000000000000000000000000000000000000000000000000000000

Bloc 002

Transactions du bloc 002

No	Texte	Description
TX01	Leonardo00000043Adrienne	Leonardo envoie 43 cryptopiastres à Adrienne
TX02	Raymonde00000308Laurence	Raymonde envoie 308 cryptopiastres à Laurence
TX03	Jonathan00000121Nicholas	Jonathan envoie 121 cryptopiastres à Nicholas
TX04	Caissier00000100Benjamin	Caissier envoie 100 cryptopiastres à Benjamin
Conversion hash des transactions du bloc 002		
HTX01	576c92a3142681a132c16876edb4c8664ce1f7ee1ff8282b4d6fc37b1ab4b559	
HTX02	91e2082dafbbaad37280ee3d8a60dac9f71b93de1222b3e3385dbc9f406138d3	
HTX03	4cfed25a65f27fa9049c21f8f5d313e9fe9f51128690b856e3c7bf6a00a28cf4	
HTX04	81d65d1bc063cb2cd0ef41fd9f9619b1e6d5df1af8d5e46725ee35bd436046e1	
Fusion 2×2 des hash du bloc 002		
HTX0102	2b9f6c041023d314529d108e3d9526af10bc9b73b150977c278712db33b6d151	
HTX0304	3d87b7be3c348d449b4c68b652a1f8818c2285d5688d25ef1ee1ba0ab6527fc3	
Racine de Merkle du bloc 002		
HTX0104	abccc524735fd46a8edecdcb9d8c7f81e731c42cfb22f966d89bfd885fb8337b	

Bloc 002

Génération du bloc 002
Bloc précédent
00000b0e48cab946eec6ba2d313b8168c73bb457e8ae105107f1fbd6d4097cc5
Racine de Merkle du bloc 002
abccc524735fd46a8edecdcb9d8c7f81e731c42cfb22f966d89bfd885fb8337b
Nonce du bloc 002
00092148
Bloc 002
00000f1322a29ecd94e6a634be82df90480785d9cd2440923c59bcbbaaed1a08

Chaîne de blocs

Chaîne de blocs suite au minage du bloc 002

Bloc	Hash
002	00000f1322a29ecd94e6a634be82df90480785d9cd2440923c59bcbbaaed1a08
001	00000b0e48cab946eec6ba2d313b8168c73bb457e8ae105107f1fbd6d4097cc5
000	00000b069faa93bb67294715706540 3b609ce6a09c7f9b3d7ab0b74e6a6d6981
	0000000000000000000000000000000000000000000000000000000000000000

Bloc 003

Transactions du bloc 003

No	Texte	Description
TX01	Adrienne00000257Jonathan	Adrienne envoie 257 cryptopiastres à Jonathan
TX02	Nicholas00000111Brigitte	Nicholas envoie 111 cryptopiastres à Brigitte
TX03	Benjamin00000328Raymonde	Benjamin envoie 328 cryptopiastres à Raymonde
TX04	Caissier00000100Leonardo	Caissier envoie 100 cryptopiastres à Leonardo
Conversion hash des transactions du bloc 003		
HTX01	45fbee1ccde776b078f7b52a217987acc2f84779b3d80b6f9a1d88647271e07e	
HTX02	ad6a866a7b4911f80d58c84d56d7b33bb5c2d6dbb477d43ecf90eb353a75bfc3	
HTX03	b60f1f19761175896cc94de44fffb47e33463fbc7c85392ab397244aa51c9fcd	
HTX04	ecfd64002bea5c38d7c03086e84f1967793636afbfa194760e141b09f60364cd	
Fusion 2×2 des hash du bloc 003		
HTX0102	d1777de7884c2966e0c8cedb21cc526c69f77679434216b4dc960458bcdcff50	
HTX0304	cbaf0923da87a6d717f63f4806d969d144c22c7dac40a1f1806325fe66444ad4	
Racine de Merkle du bloc 003		
HTX0104	a3e137019817cba7bc9f88b8fe9e971d4b1b9f9b0a3e693c459173f095d9563f	

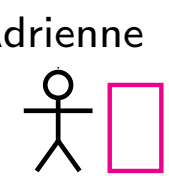
Bloc 003

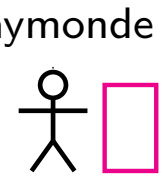
Génération du bloc 003
Bloc précédent
00000f1322a29ecd94e6a634be82df90480785d9cd2440923c59bcbbaaed1a08
Racine de Merkle du bloc 003
a3e137019817cba7bc9f88b8fe9e971d4b1b9f9b0a3e693c459173f095d9563f
Nonce du bloc 003
000a73d5
Bloc 003
0000063517a0329b74a89407dfd47708ec9c90df8a4949b3d98e0d4242c0944d

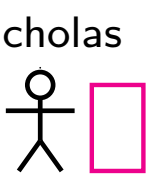
Chaîne de blocs

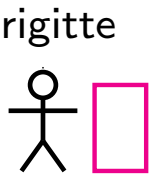
Chaîne de blocs suite au minage du bloc 003

Bloc	Hash
003	0000063517a0329b74a89407dfd47708ec9c90df8a4949b3d98e0d4242c0944d
002	00000f1322a29ecd94e6a634be82df90480785d9cd2440923c59bcbbaaed1a08
001	00000b0e48cab946eec6ba2d313b8168c73bb457e8ae105107f1fbd6d4097cc5
000	00000b069faa93bb67294715706540 3b609ce6a09c7f9b3d7ab0b74e6a6d6981
	0000000000000000000000000000000000000000000000000000000000000000

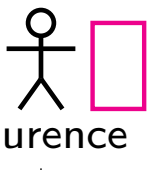


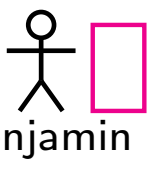


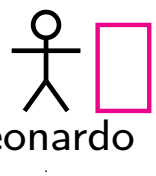


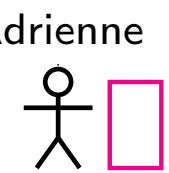


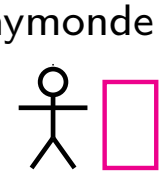
LE PRINCIPE DE LA CHAÎNE LA PLUS LONGUE

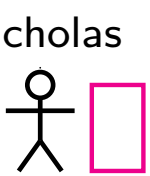


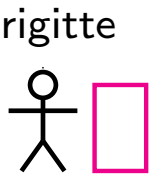




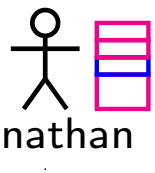


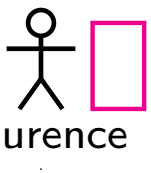


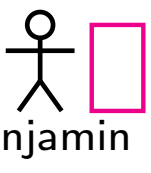


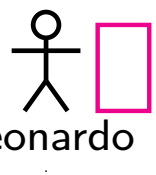


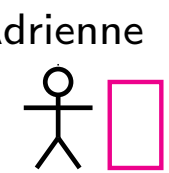
SI JOHATHAN ESSAIE DE MODIFIER (À SON AVANTAGE)
UN BLOC DE LA CHAÎNE,...

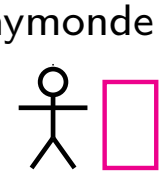


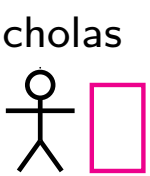


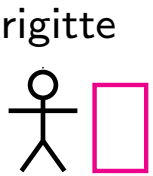




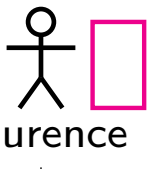


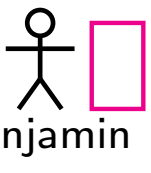


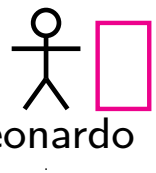


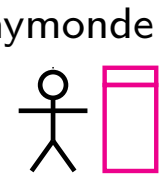


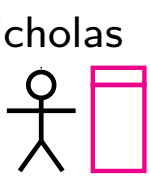
SI JOHATHAN ESSAIE DE MODIFIER (À SON AVANTAGE)
UN BLOC DE LA CHAÎNE,...
...CE BLOC ET TOUS LES BLOCS AU-DESSUS DOIVENT ÊTRE REMINÉS.

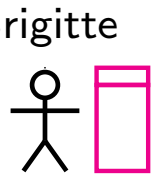




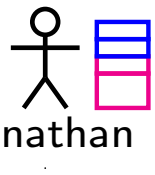


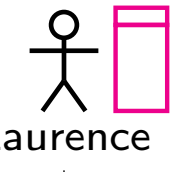


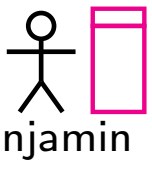


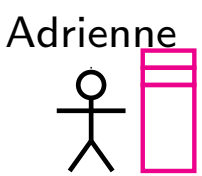


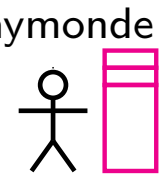
PENDANT QUE JONATHAN REMINE SA (FAUSSE) CHAÎNE,
D'AUTRES BLOCS S'AJOUTENT À LA CHAÎNE DES AUTRES.

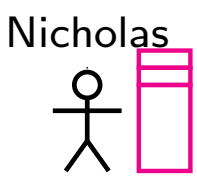


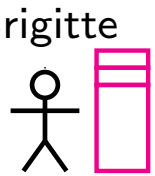




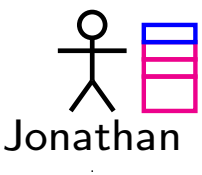


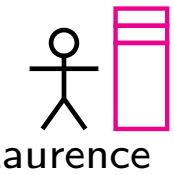


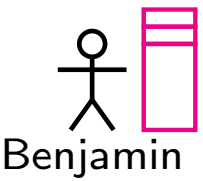


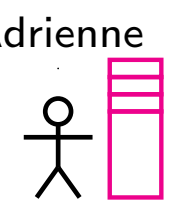


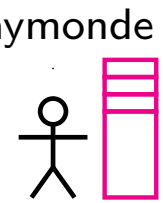
PENDANT QUE JONATHAN REMINE SA (FAUSSE) CHAÎNE,
D'AUTRES BLOCS S'AJOUTENT À LA CHAÎNE DES AUTRES.

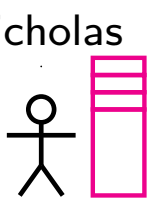


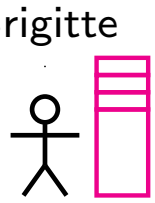




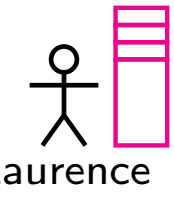


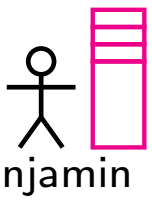


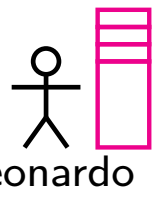




SI JONATHAN EST AUSSI RAPIDE À MINER QUE LES SEPT AUTRES USAGERS, SA CHAÎNE NE SERA JAMAIS LA PLUS LONGUE.
SI SEUL JONATHAN UTILISE SA FAUSSE CHAÎNE, CELLE-CI N'A AUCUNE VALEUR.







Soldes ou droits de dépenser

Pour connaître le solde, ou droit de dépenser, de chaque participant de notre exemple une fois le bloc 003 miné, il s'agit d'en faire le décompte à l'aide des transactions enregistrées dans la chaîne.

Transactions du bloc 000
Caissier00001000Laurence
Caissier00001000Nicholas
Caissier00001000Adrienne
Caissier00001000Benjamin
Caissier00001000Raymonde
Caissier00001000Leonardo
Caissier00001000Brigitte
Caissier00001000Jonathan

Transactions du bloc 001
Adrienne00000243Nicholas
Brigitte00000508Benjamin
Laurence00000467Raymonde
Caissier00000100Leonardo

Transactions du bloc 002
Leonardo00000043Adrienne
Raymonde00000308Laurence
Jonathan00000121Nicholas
Caissier00000100Benjamin

Transactions du bloc 003
Adrienne00000257Jonathan
Nicholas00000111Brigitte
Benjamin00000328Raymonde
Caissier00000100Leonardo

Soldes ou droits de dépenser

Si, par exemple, on désire connaître le solde de Nicholas après trois blocs, il s'agit de ressortir toutes les transactions impliquant Nicholas dans la chaîne, **additionner tous les montants des transactions où Nicholas apparaît à droite** et **soustraire tous les montants des transactions où Nicholas apparaît à gauche**.

Transactions du bloc 000
Caissier00001000Laurence
Caissier00001000Nicholas
Caissier00001000Adrienne
Caissier00001000Benjamin
Caissier00001000Raymonde
Caissier00001000Leonardo
Caissier00001000Brigitte
Caissier00001000Jonathan

Transactions du bloc 001
Adrienne00000243Nicholas
Brigitte00000508Benjamin
Laurence00000467Raymonde
Caissier00000100Leonardo

Transactions du bloc 002
Leonardo00000043Adrienne
Raymonde00000308Laurence
Jonathan00000121Nicholas
Caissier00000100Benjamin

Transactions du bloc 003
Adrienne00000257Jonathan
Nicholas00000111Brigitte
Benjamin00000328Raymonde
Caissier00000100Leonardo

Soldes ou droits de dépenser

Après trois blocs de transactions, le solde de Nicholas est ainsi de

$$1000 + 243 + 121 - 111 = 1253.$$

Transactions du bloc 000
Caissier00001000Laurence
Caissier00001000Nicholas
Caissier00001000Adrienne
Caissier00001000Benjamin
Caissier00001000Raymonde
Caissier00001000Leonardo
Caissier00001000Brigitte
Caissier00001000Jonathan

Transactions du bloc 001
Adrienne00000243Nicholas
Brigitte00000508Benjamin
Laurence00000467Raymonde
Caissier00000100Leonardo

Transactions du bloc 002
Leonardo00000043Adrienne
Raymonde00000308Laurence
Jonathan00000121Nicholas
Caissier00000100Benjamin

Transactions du bloc 003
Adrienne00000257Jonathan
Nicholas00000111Brigitte
Benjamin00000328Raymonde
Caissier00000100Leonardo

Soldes ou droits de dépenser

Usager	**Total envoyé**	**Total reçu**	**Solde**
Laurence	467	1308	841
Nicholas	111	1364	1253
Adrienne	500	1043	543
Benjamin	328	1608	1280
Raymonde	308	1795	1487
Leonardo	43	1200	1157
Brigitte	508	1111	603
Jonathan	121	1257	1136
Total			8300

Conclusion

- Une chaîne de blocs est une liste, une énumération, d'items qu'elle enregistre dans un ordre immuable.
- Chaque maillon d'une chaîne est un bloc d'informations cryptées de façon unidirectionnelle, et les maillons sont reliés entre eux en cryptant toute nouvelle information avec la valeur du bloc précédent.
- Dans un contexte de cryptodevise, une chaîne de blocs énumère l'ensemble des transactions du réseau dans l'ordre précis où elles ont eu lieu.
- Une chaîne de blocs peut ainsi être utile à entreposer tout type d'information dans un contexte où l'ordre, ou la séquence, des éléments d'information est important:
  - Dossiers médicaux, dossiers de conduite;
  - Itinéraire de marchandise;
  - Procès-verbaux, etc.