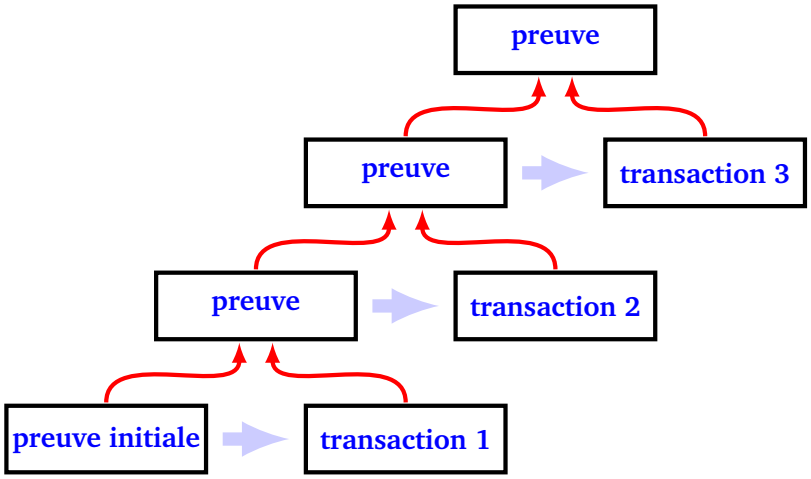
Bitcoin

- La monnaie *bitcoin* est une monnaie dématérialisée.
- Les transactions sont enregistrées dans un grand livre de compte appelé *blockchain*.
- Imaginons un groupe d'amis qui souhaitent partager les dépenses du groupe de façon la plus simple possible.
- Au départ tout le monde dispose de 1000 *bitcoins* et on note au fur et à mesure les dépenses et les recettes de chacun.
- On note sur le livre de compte la liste des dépenses/recettes, par exemple :
  — « Amir a dépensé 100 *bitcoins* »
  — « Barbara a reçu 45 *bitcoins* »
  — etc.
- Il suffit de parcourir tout le livre pour savoir combien chacun a reçu ou dépensé depuis le début.

Blockchain

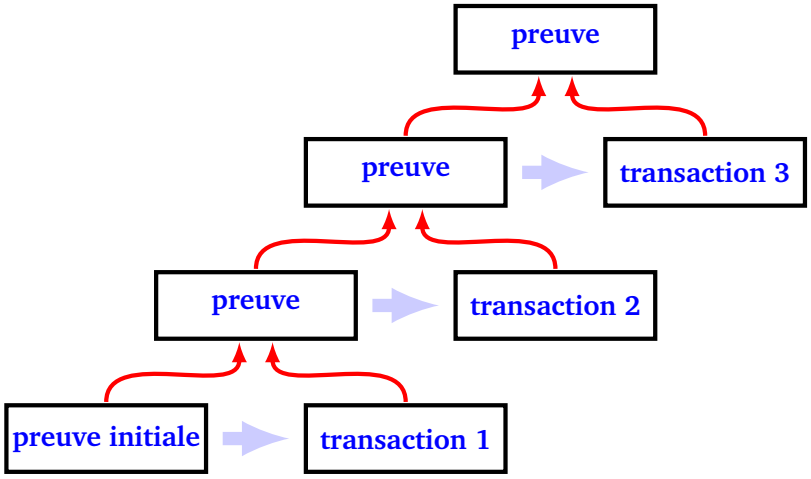
Pour éviter que quelqu'un ne vienne truquer le livre de compte, après chaque transaction on ajoute dans le livre une certification construite à partir d'une preuve de travail.

1. On commence par une preuve de travail quelconque. Pour nous ce sera `[0,0,0,0,0,0]`.
2. On écrit la première transaction (par exemple `"Amir -100"`).
3. On calcule et on écrit dans le livre une preuve de travail, qui va servir de certificat. C'est une liste (par exemple `[56,42,10,98,2,34]`) obtenue après beaucoup de calculs prenant en compte la transaction précédente et la précédente preuve de travail.
4. À chaque nouvelle transaction (par exemple `"Barbara +45"`), quelqu'un calcule une preuve de travail pour la dernière transaction associée à la précédente preuve. On écrit la transaction, puis la preuve de travail.



Preuve de travail

- Une preuve de travail est la résolution d'un problème difficile, mais où il est facile de vérifier que la solution obtenue est correcte.
- Comme les sudokus par exemple : il suffit de dix secondes pour vérifier qu'une grille est remplie correctement, par contre il a fallu plus de dix minutes pour le résoudre.



Fonction de hachage

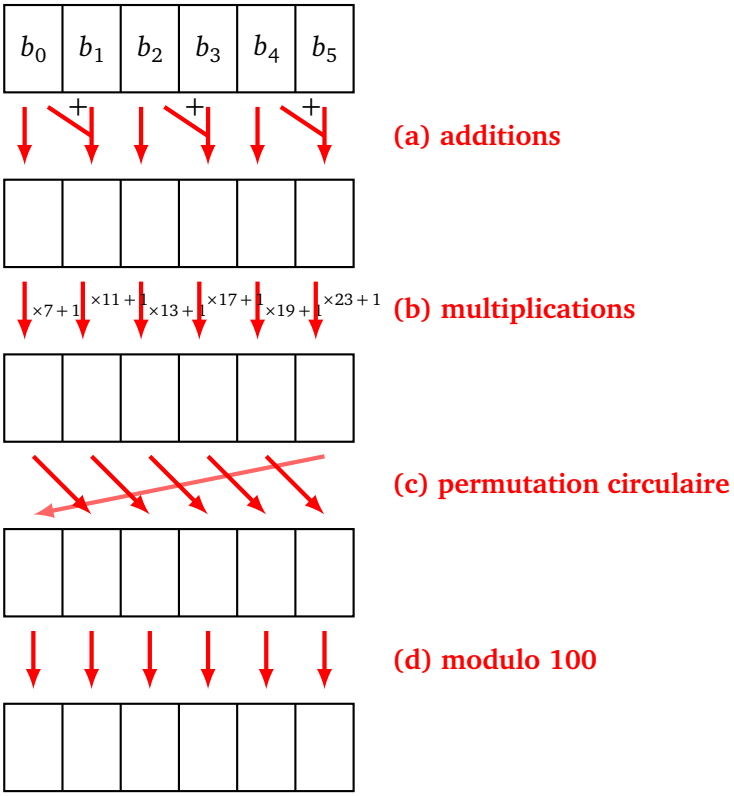
- À partir d'un long message nous calculons une courte empreinte.
- Il est difficile de trouver deux messages différents ayant la même empreinte.
- Ici notre message est une liste d'entiers (entre 0 et 99) de longueur un multiple quelconque de $N = 6$.
- Son empreinte (ou *hash*) sera une liste de longueur $N = 6$.
- Exemple : `[1, 2, 3, 4, 5, 6, 1, 2, 3, 4, 5, 6]` a pour empreinte :
  `[10, 0, 58, 28, 0, 90]`
- Exemple : `[1, 1, 3, 4, 5, 6, 1, 2, 3, 4, 5, 6]` a pour empreinte :
  `[25, 14, 29, 1, 19, 6]`

L'idée est de mélanger les nombres par bloc de $N = 6$ entiers, puis de combiner ce bloc au suivant et de recommencer, jusqu'à obtenir un seul bloc.

Un tour

Pour un bloc $[b_0, b_1, b_2, b_3, b_4, b_5]$ de taille $N = 6$, *faire un tour* consiste à faire les opérations suivantes :

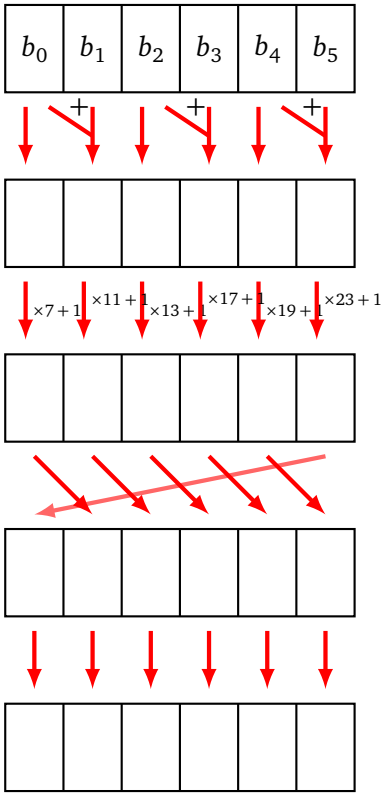
1. On additionne certains entiers :
$$[b'_0, b'_1, b'_2, b'_3, b'_4, b'_5] = [b_0, b_1 + b_0, b_2, b_3 + b_2, b_4, b_5 + b_4]$$
2. On multiplie ces entiers par des nombres premiers (dans l'ordre $7, 11, 13, 17, 19, 23$) et on rajoute 1 :
$$[b''_0, b''_1, b''_2, b''_3, b''_4, b''_5] = [7 \times b'_0 + 1, 11 \times b'_1 + 1, 13 \times b'_2 + 1, 17 \times b'_3 + 1, 19 \times b'_4 + 1, 23 \times b'_5 + 1]$$
3. On effectue une permutation circulaire (le dernier passe devant) :
$$[b'''_0, b'''_1, b'''_2, b'''_3, b'''_4, b'''_5] = [b''_5, b''_0, b''_1, b''_2, b''_3, b''_4]$$
4. On réduit chaque entier modulo 100 afin d'obtenir des entiers entre 0 et 99.



Partant du bloc $[0,1,2,3,4,5]$, on a donc successivement :

1. additions : $[0,1,2,5,4,9]$
2. multiplications : $[7\times 0+1, 11\times 1+1, 13\times 2+1, 17\times 5+1, 19\times 4+1, 23\times 9+1] = [1,12,27,86,77,208]$
3. permutation : $[208,1,12,27,86,77]$
4. réduction modulo 100 : $[8,1,12,27,86,77]$

Vérifie que le bloc $[1,1,2,3,4,5]$ est transformé en $[8,8,23,27,86,77]$.



Dix tours

Pour bien mélanger chaque bloc, itère dix fois les opérations précédentes. Après 10 tours :

- le bloc $[0, 1, 2, 3, 4, 5]$ devient $[98, 95, 86, 55, 66, 75]$,
- le bloc $[1, 1, 2, 3, 4, 5]$ devient $[18, 74, 4, 42, 77, 42]$.

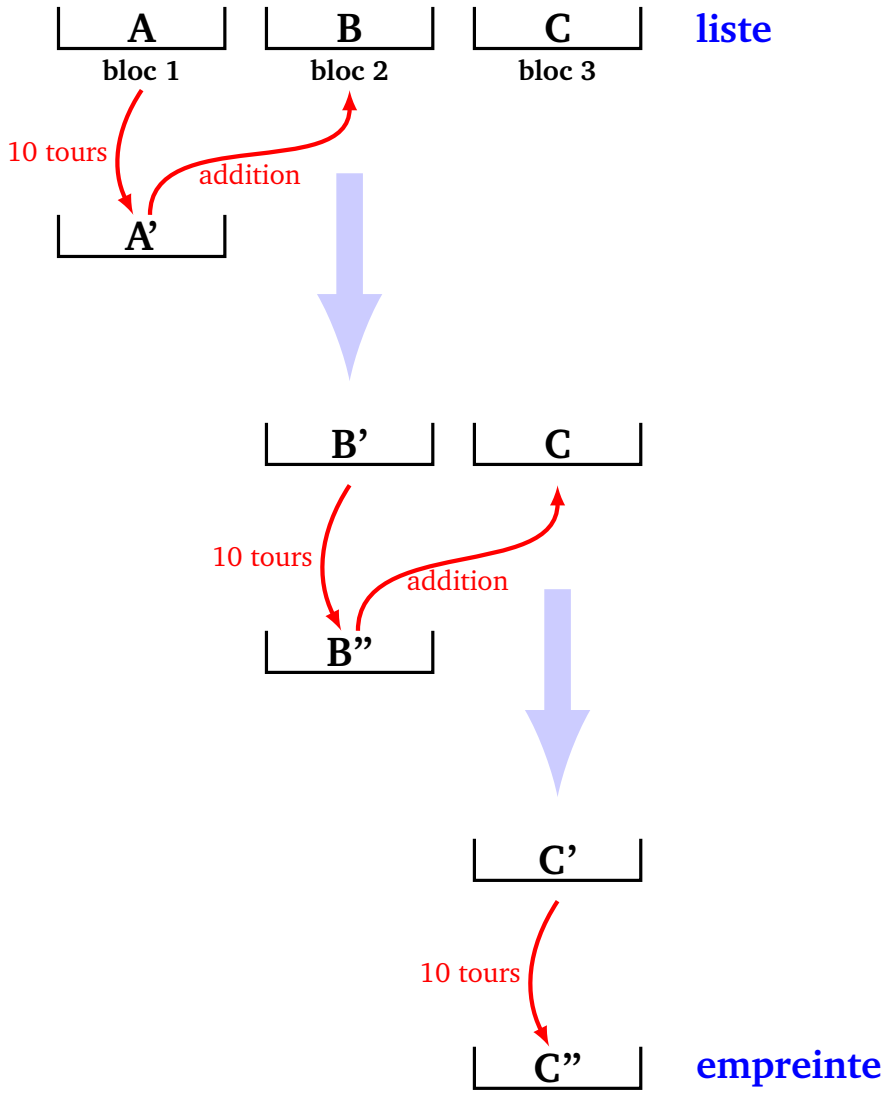
Deux blocs proches sont transformés en deux blocs très différents !

Hachage d'une liste

Partant d'une liste de longueur un multiple de $N = 6$, on la découpe en blocs de longueur 6 et on calcule l'empreinte de cette liste selon l'algorithme suivant :

- On extrait le premier bloc de la liste, on effectue 10 tours de mélange.
- On ajoute terme à terme (et modulo 100), le résultat de ce mélange au second bloc.
- On recommence en partant du nouveau second bloc.
- Lorsqu'il ne reste plus qu'un bloc, on effectue 10 tours de mélange, le résultat est l'empreinte de la liste.

Voici le schéma d'une situation avec trois blocs : dans un premier temps il y a trois blocs (A,B,C) ; dans un second temps il ne reste plus que deux bloc (B' et C) ; à la fin il ne reste qu'un bloc (C") : c'est l'empreinte !



Exemple avec la liste $[0, 1, 2, 3, 4, 5, 1, 1, 1, 1, 1, 1, 10, 10, 10, 10, 10, 10]$.

- Le premier bloc est $[0, 1, 2, 3, 4, 5]$, son mélange à 10 tours est $[98, 95, 86, 55, 66, 75]$.
- On ajoute ce mélange au second bloc $[1, 1, 1, 1, 1, 1]$.
- La liste restante est maintenant $[99, 96, 87, 56, 67, 76, 10, 10, 10, 10, 10, 10]$.
- On recommence. Le nouveau premier bloc est $[99, 96, 87, 56, 67, 76]$, son mélange à 10 tours vaut $[60, 82, 12, 94, 6, 80]$, on l'ajoute au dernier bloc $[10, 10, 10, 10, 10, 10]$ pour obtenir (modulo 100) $[70, 92, 22, 4, 16, 90]$.
- On effectue un dernier mélange à 10 tours pour obtenir l'empreinte : $[77, 91, 5, 91, 89, 99]$.