1INDF activité 3 : transactions

Nom:	Groupe:	Date:

Le but de la troisième activité est de comprendre comment effectuer des transactions sur une chaîne de blocs.

3.1 Théorie

Comme dans l'activité 1, le **mineur** désigne l'entité qui effectue les calculs de la PoW pour insérer un nouveau bloc dans la chaîne de blocs.

Le **nœud** désigne l'entité qui gère les transactions, vérifie la validité des nouveaux blocs et des transactions, maintient une copie locale de la chaîne de blocs et envoie les paramètres à un mineur pour miner un nouveau bloc.

Les **transactions** permettent de transférer la cryptomonnaie d'un **payeur**, qui émet la transaction, à un **destinataire,** qui reçoit la cryptomonnaie associée à la transaction. La transaction consiste en un montant de cryptomonnaie dont la propriété passe du payeur au destinataire.

Dans une chaîne de blocs, aucune cryptomonnaie ne circule réellement ; c'est simplement l'**adresse** à laquelle la cryptomonnaie est associée qui change. Chaque acteur de la chaîne de blocs (mineurs, nœuds, payeurs et destinataires) possède une adresse unique dans la chaîne de blocs ; ces adresses sont équivalentes à un numéro de compte bancaire, mais elles restent anonymes.

Une fois que le payeur et le destinataire se sont mis d'accord sur le montant de la transaction, le payeur émet une transaction et la signe. Toutes les transactions sont partagées entre les nœuds de la chaîne de blocs dans une zone d'attente appelée **mempool**. Les mineurs choisissent les transactions qu'ils souhaitent insérer dans un bloc. Pour qu'une transaction devienne effective, elle doit être insérée dans un bloc faisant partie de la fourche la plus longue ; les transactions insérées dans les blocs des autres chaînes ne seront pas exécutées.

Important : la chaîne de bloc garantit que la cryptomonnaie est transférée de l'adresse du payeur à celui du vendeur, mais n'a aucune influence sur le monde réel.

La même transaction peut être choisie par plusieurs mineurs, mais c'est seulement le mineur dont le bloc est finalisé qui recevra les frais de transaction en récompense pour son travail.

La récompense pour le minage d'un bloc est aussi gérée par une transaction ; elle est insérée par le mineur dans son propre bloc.

Frais de transaction

Pour convaincre les mineurs d'inclure sa transaction dans un nouveau bloc, le payeur inclut dans sa transaction des **frais de transaction** (« fee » dans Bitcoin ou « gas » dans Ethereum), qui seront payés au mineur si le bloc dans lequel la transaction est insérée est finalisée. Le montant des frais de transaction peut varier entre 0 et l'infini. Les mineurs gagnent davantage de cryptomonnaie en insérant les transactions avec les frais les plus élevés dans les nouveaux blocs qu'ils calculent ; ainsi plus les frais sont élevés, plus la probabilité que la transaction soit choisie puis incluse dans un bloc est élevée.

Validation des transactions

Avant d'insérer une transactions un nouveau bloc, le nœud doit impérativement vérifier validité de la transaction :

- si les informations inclues sont fausses ou mal écrites, ou si le payeur n'a pas les fonds, la transaction est écartée ;
- si les informations inclues sont justes et que le payeur a assez de fond, les transactions sont transférées dans la zone d'attente des transactions, appelée **mempool** (memory pool).

  Attention : une transaction affichée dans le mempool ne garantit pas qu'elle soit valide.

Important : si un bloc contient une transaction qui s'avère invalide, alors le bloc en entier est rejeté, y compris les transactions valides. Dans Ethereum, une punition est infligée au mineur fautif, qui perd des ethers. Il est donc essentiel que les transactions soient vérifiées par les nœuds avant d'être inclues dans les blocs.

Si un bloc est confirmé dans la chaîne de blocs, les transactions qu'il contient deviennent effectives, et la cryptomonnaie associée au montant de la transaction passe de l'adresse du payeur à celle du destinataire, et celle associée aux frais de transaction passe à l'adresse du mineur. Les transactions sont inscrites dans la chaîne de blocs et deviennent **irréversibles** et **immuables**.

Confirmation et finalisation

Lorsqu'un nouveau bloc est inséré dans la chaîne de blocs, les transactions qu'il contient sont **confirmées**, mais ne sont pas encore **finalisées**. En effet, il n'est pas garanti que le nouveau bloc fasse partie de la fourche la plus longue.

Les transactions insérées dans un bloc finalisé sont exécutées :

- la récompense est créditée au mineur
- le montant de chaque transaction est soustrait du solde du payeur, et crédité au solde du destinataire
- les frais de transactions sont soustraits du solde du payeur, et crédités au mineur

Dans Bitcoin, les blocs ne sont jamais finalisés, mais sont reconnus comme tels sur la base du calcul de la probabilité qu'un bloc fasse partie de la fourche la plus longue ; en général, il faut attendre au moins une heure après qu'un bloc soit inséré dans la chaîne Bitcoin avant de le considérer comme étant finalisé. A partir de ce moment, il devient très improbable que le bloc se retrouve dans une fourche qui sera abandonnée ultérieurement. Cette **période de latence** est considérée comme une faiblesse de Bitcoin.

Dans Ethereum, un bloc est considéré comme finalisé, et les autres blocs éliminés, lorsque deux époques de 32 blocs ont été ajoutés à la chaîne dont fait partie le bloc.

Solde d'un utilisateur

La chaîne de blocs garde la trace de toutes les transactions, mais ne traite aucune information concernant les utilisateurs. Pour connaître le solde d'un utilisateur, les nœuds analysent toutes les transactions de la chaîne de blocs et calculent le solde selon les crédits et les débits inscrits. Ce calcul sert à vérifier le solde avant de valider une transaction, et fait partie des services

gratuits que doivent fournir les nœuds du réseau, afin que les utilisateurs puissent consulter le solde de cryptomonnaie qu'ils possèdent à tout moment.

3.2 BlocNote

Dans BlocNote, les transactions comportent les informations suivantes:

1. le numéro du noeud du payeur,
2. le numéro du noeud du destinataire,
3. le montant de la transaction ; dans notre activité, le montant se situe entre 1 et 99 R$.
4. le montant des frais de transaction ; dans notre activité, les frais de transactions se situent entre 0 et 9 R$.

Par exemple, le nœud 5 achète une paire de ski au nœud 7 pour 35 R$; il ajoute à la transaction des frais de 3 R$.

Payeur	Destinataire	Montant de la Tx	Frais de Tx
5	7	35	3

→ 57353

Le nœud 4 paye le nœud 8 un montant de 7 R$ pour déneiger le devant de sa maison; il ajoute à la transaction des frais de 1 R$.

Payeur	Destinataire	Montant de la Tx	Frais de Tx
4	8	7	1

→ 48071

Les transactions de récompense comportent les informations suivantes:

1. le numéro du noeud du payeur est « 0 » car la cryptomonnaie est créée dans la chaîne de blocs,
2. le numéro du noeud-mineur,
3. le montant de la récompense, soit 10 R$.
4. les frais de transaction sont de 0 R$, puisque le mineur insère la transaction dans son propre bloc.

Par exemple, le nœud 3 met la transaction suivante dans chacun de ses blocs :

Payeur	Destinataire	Montant de la Tx	Frais de Tx
0	3	10	0

→ 03100

Blocs

Le blocID et la Pow sont obtenus de la même façon que dans l'activité 1, mais en plus du blocID et de la Pow, les blocs contiennent maintenant au minimum la transaction de récompense, et possiblement une ou deux transaction(s) supplémentaires.

Exemple : le mineur 3 enchaîne un nouveau bloc au

BlocID = 3520

bloc-parent 520.

- le blocID est 3520 ;
- la PoW est 0b110111000000;
- la transaction de récompense est 03100 ;
- il en profite pour passer deux transactions affichées dans le mempool : 57353 et 48071.

PoW = 0b110111000000			
Tx			
payeur	dest.	montant	frais
0	3	10	0
5	7	35	3
4	8	07	1

Si ce bloc est finalisé (i.e. fait partie de la fourche la plus longue à la fin de l'activité),

- le nœud 3 recevra 14 R$ (10 R$ de récompense et 3R$ + 1 R$ de frais de transaction),
- le nœud 5 payera 38 R$ (35 R$ au nœud 7 et 3 R$ de frais de transaction),
- le nœud 7 recevra 35 R$,
- le nœud 4 payera 8 R$ (7 R$ au nœud 8 et 1 R$ de frais de transaction),
- et le nœud 8 recevra 8 R$.

3.3 Activité

Les règles et le but sont les mêmes que celles de l'activité 1, à quelques différences près :

- les groupes de 4 élèves jouent à la fois les rôles de payeur, de destinataire, de nœud et de mineur. Les transactions se font entre nœuds ;
- chaque bloc contient de une à trois transactions, dont obligatoirement la transaction de récompense, et 0, 1 ou 2 transactions choisies dans la mempool ;
- les nœuds doivent vérifier la validité des transactions avant de les inclure dans les blocs.

Matériel :

- panneau d'affichage (tableau blanc et aimants, ou panneau en liège et punaises, ou poster et scotch) pour la chaîne de blocs
- un tableau « mempool » (tableau blanc et aimants, ou panneau en liège et punaises, ou poster et scotch) pour afficher les transactions

Tableau d'affichage des transactions (mempool)

Payeur	Destina.	Montant	Frais
7	3	10	2

Payeur	Destina.	Montant	Frais
6	3	47	4

Payeur	Destina.	Montant	Frais
8	4	11	3

Payeur	Destina.	Montant	Frais
5	7	35	3

Payeur	Destina.	Montant	Frais
3	5	54	7

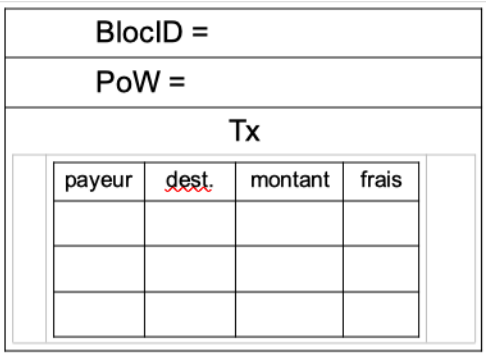
Payeur	Destina.	Montant	Frais
7	5	56	9

Payeur	Destina.	Montant	Frais
4	8	07	1

Payeur	Destina.	Montant	Frais
8	5	22	4

Payeur	Destina.	Montant	Frais
4	7	33	1

- feuillets représentant les blocs :



- papier brouillon (pour les calculs), crayon, calculatrice

3.3.1 Variante 1

But : effectuer le plus de transactions possible.

Dans cette variante, il est possible d'insérer des transactions concernant la cryptomonnaie de n'importe quel nœud. Par exemple, le nœud 6 peut insérer la transaction 35081, qui signifie que le nœud 3 transfère 8 R$ au nœud 5, et le nœud 6 empoche 1 R$ de frais de transaction.

1. les mineurs calculent le blocID et la PoW des nouveaux blocs comme dans l'activité 1 ;
2. chaque bloc contient en plus au minimum la transaction de récompense, et possiblement une ou deux autres transactions ;

   Pour les premiers blocs, tant qu'aucune cryptomonnaie n'est encore disponible, les mineurs n'insèrent que la transaction de récompense dans les blocs.

   Dès que de la cryptomonnaie est en circulation, les mineurs doivent obligatoirement ajouter des transactions dans leurs blocs.
3. les nœuds choisissent les transactions qu'ils souhaitent insérer dans des blocs parmi les transactions affichées dans le mempool ;

   Pour cette première version, les nœuds peuvent dépenser toute la cryptomonnaie disponible dans la chaîne, même celle qui appartient à d'autres nœuds.
4. Avant d'insérer une transaction dans un bloc, le nœud doit vérifier sa validité :
   i. identifier l'adresse du payeur de la transaction ;
   ii. analyser la chaîne de blocs pour identifier toutes les transactions concernant cette adresse ;
   iii. comptabiliser toutes ces transactions afin de vérifier si le solde du payeur est suffisant pour couvrir le montant et les frais de la transaction.
      - si le payeur n'a pas assez de R$, la transaction est éliminée, et une autre transaction est choisie dans le mempool ;
      - si le payeur a assez de R$, la transaction est insérée dans le futur bloc.

   Important : il n'est pas nécessaire de comptabiliser toutes les transactions associées à une adresse dans toutes les chaînes de la chaîne de blocs, mais que pour la fourche dans laquelle le nouveau bloc sera inséré.

   Attention ! Si une seule transaction est fausse, le bloc en entier est rejeté.

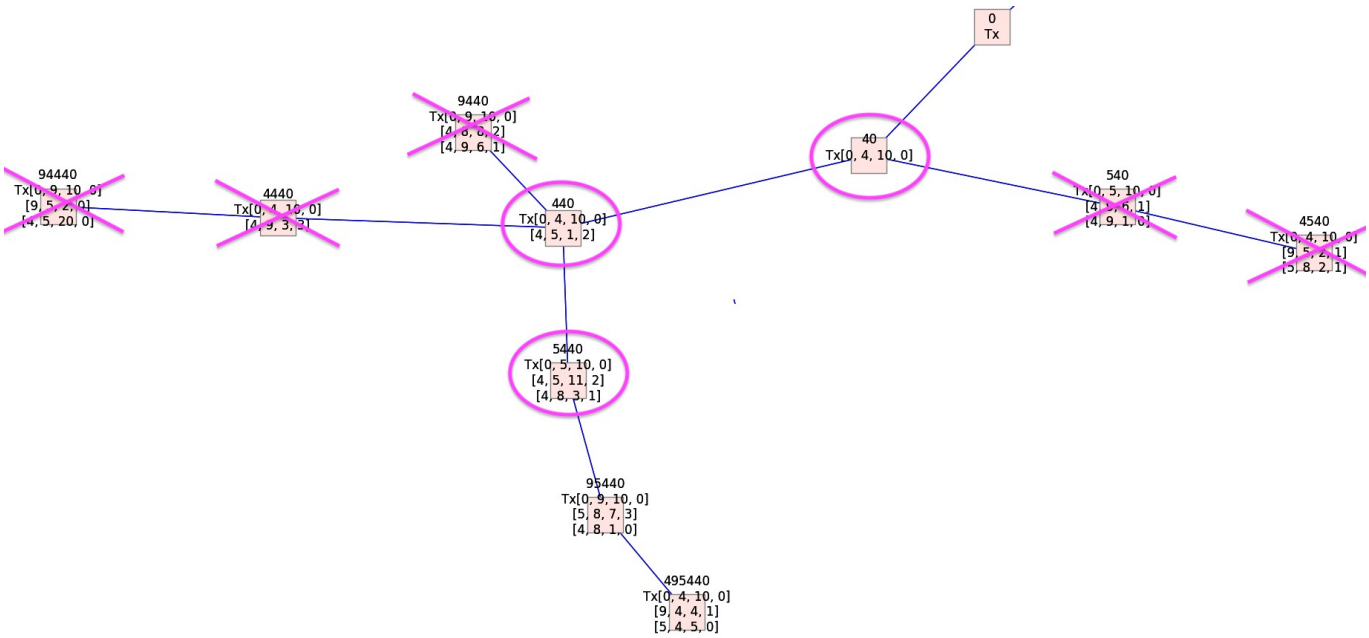
Notons que si le vendeur et l'acheteur sont inversés dans la transaction, et que celle-ci est confirmée par un bloc inséré dans la chaîne de blocs, la transaction est irréversible.

5. À la fin de l'activité, les nœuds analysent la chaîne de blocs la plus longue pour comptabiliser le solde de chaque nœud.

3.3.2 Variante 2

Dans cette activité, si deux blocs sont enchaînés à la suite d'un bloc, ce bloc est finalisé et les transactions insérées dans ce bloc sont exécutées. Les autres blocs au même niveau que le bloc finalisé sont éliminés, ce qui permet de simplifier l'analyse de la chaîne de blocs et d'éviter de perdre trop d'énergie sur des fourches stériles.

Par exemple, dans la chaîne de blocs montrée ci-dessous, le bloc 40 a été finalisé lorsque les blocs 4540, 9440, 4440 et 5440 ont été enchaînés. Par la suite, le bloc 440 a été finalisé par les blocs 94440 et 95440, puis le bloc 5440 a été finalisé par le bloc 495440. A ce moment, les blocs 540, 4540, 9440, 4440 et 94440 sont éliminés car ils ne font pas partie de la fourche où se trouvent les blocs finalisés, il n'est donc plus possible d'y enchaîner des blocs.



Un exemple complet est donné dans la section 3.5.2.

3.3.2 Variante 3

Dans cette variante, il n'est plus possible de dépenser la cryptomonnaie appartenant à un autre nœud.

Déroulement :

1. Le payeur et le destinataire doivent d'abord s'entendre sur le mondant de la transaction ;
2. le vendeur prépare la transaction et la signe pour autoriser le transfert de sa cryptomonnaie à l'adresse du destinataire

Payeur	Destinataire	Montant de la Tx	Frais de Tx
5	7	35	3

→ 57353

Signature du payeur : ……..……...

3. le vendeur met ensuite la transaction dans le mempool, et le reste de l'activité se déroule comme dans la variante 1.

3.3.2 Variante 4

Pour encourager la circulation de la cryptomonnaie, le nœud gagnant est celui qui aura transféré le plus de cryptomonnaie. Le score d'un nœud à la fin de l'activité correspond à la somme de tous les R$ qu'il aura transférés à d'autres nœuds, de laquelle est déduit son solde.

Par exemple, si le nœud 4 a transféré un total de 472 R$, mais qu'à la fin du jeu il a un solde de 121 R$, son score sera de 351 R$.

3.4 A retenir

Dans une vraie chaîne de blocs, les transactions doivent être signées par le payeur, ce qui empêche un utilisateur d'insérer des transactions sans l'accord du payeur. Ces signatures sont authentifiées grâce à la cryptographie, ce qui rend ces signatures indélébiles, ne permet qu'au propritaire d'avoir accès à sa cryptomonnaie, et empêche un acheteur de se rétracter.

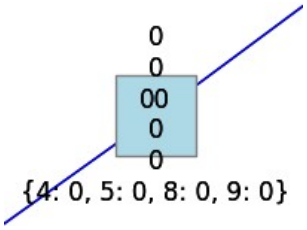
La chaîne de blocs pérennise le registre des transactions, mais ne calcule pas le solde de cryptomonnaie que chaque utilisateur possède. Etant donné que le registre est public, n'importe quelle entité (utilisateur, nœud, plateforme d'échange, ...) peut l'analyser pour en extraire les informations nécessaires pour calculer le solde correspondant à une adresse.

3.5 Exemple complet

L'exemple de l'activité 1 est repris, mais cette fois avec les transactions.Chaque bloc comprend 6 lignes:

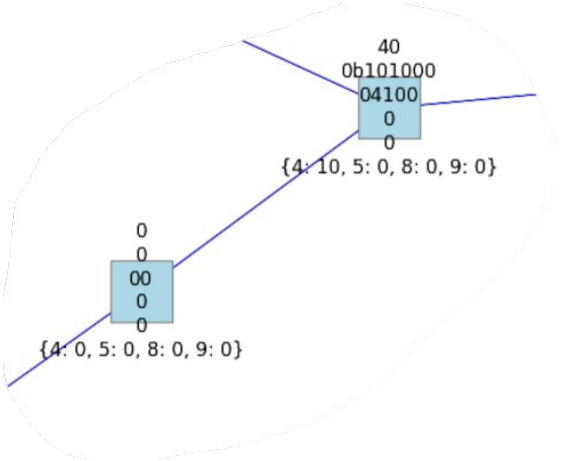
1. numéro du bloc
2. PoW
3. transaction de récompense
4. transaction 1
5. transaction 2
6. solde des noeuds après l'enchaînement du bloc.

0) Toutes les chaînes commencent par le bloc-genèse, dont le blocID, la PoW et les transactions sont 0. Le solde de tous les nœuds est de 0.



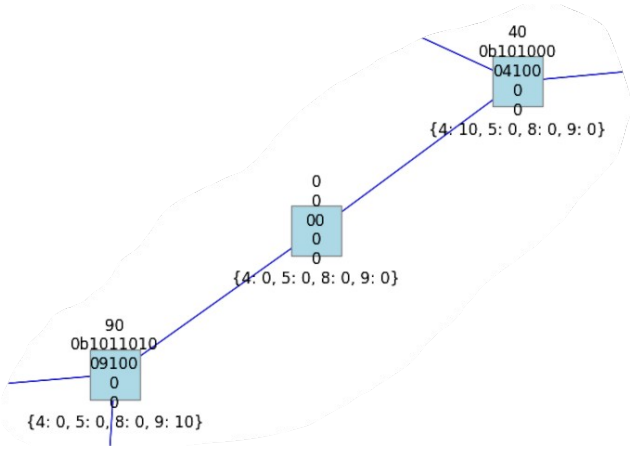
1) Le noeud 4 enchaîne un bloc au bloc-genèse, le blocID est donc 40. Le solde de tous les nœuds étant de 0, seule la transaction de récompense « 04100 » est insérée.

Si ce bloc est finalisé, le solde du nœud 4 sera de 10 R$, le solde des autres nœuds de 0.

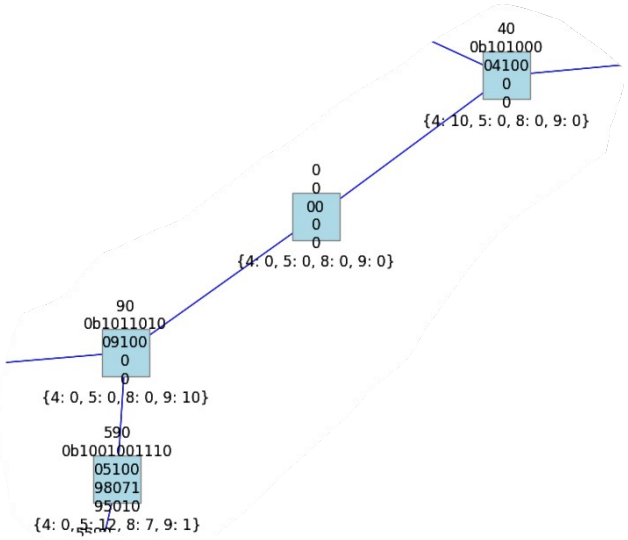


2) Le noeud 9 enchaîne aussi un bloc au bloc-genèse, le blocID est donc 90. Le solde de tous les nœuds étant de 0, seule la transaction de récompense « 09100 » est insérée.

Si ce bloc est finalisé, le solde du nœud 9 sera de 10 R$, le solde des autres nœuds de 0.



3) Le noeud 5 enchaîne un bloc au bloc 90, le blocID est donc 590.



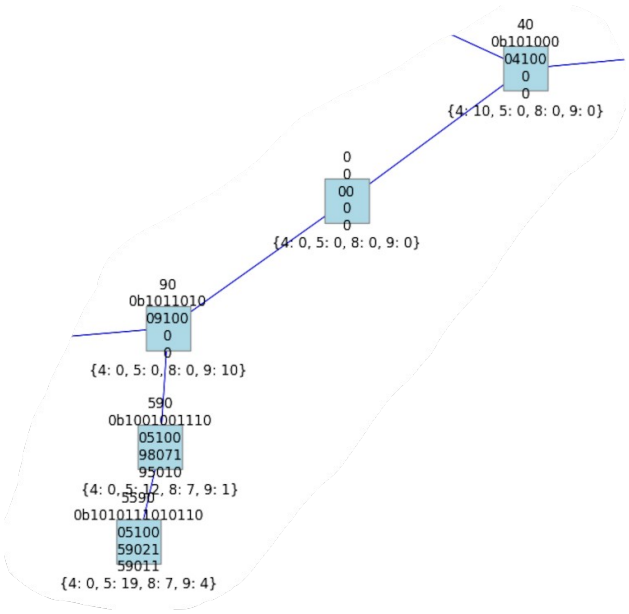
Cette fois, 10 R$ sont disponibles, donc en plus de la récompense, deux transactions sont insérées :

- 98071 : le nœud 9 paye 7 R$ au nœud 8, et paye aussi 1 R$ de frais de transaction ;
- 95010 : le nœud 9 paye 1 R$ au nœud 5, mais sans frais de transaction.

Si ce bloc est finalisé,

- le nœud 5 reçoit 12 R$ (10 R$ récompense, 1 R$ frais de transaction, et 1 R$ du nœud 9) ;
- le nœud 9 n'a plus que 1 R$, car il a dépensé 9 R$ (7 R$ au nœud 8, 1R$ de frais de transaction et 1 R$ au nœud 5)
- le nœud 8 a reçu 7 R$;
- le nœud 4 n'a toujours rien.

4) Le noeud 5 enchaîne un bloc au bloc 590, le blocID est donc 5590.



Dans cette chaîne, 20R$ ont été créés, donc en plus de la récompense, deux transactions sont insérées dans le nouveau bloc :

- 59021 : le nœud 5 paye 2 R$ au nœud 9, avec 1 R$ de frais de transaction ;
- 59011 : le nœud 5 paye 1 R$ au nœud 9, avec 1 R$ de frais de transaction.

Si le bloc est finalisé,

- le nœud 5 paye 5 R$ (2 R$ + 1 R$ au nœud 9, 2 R$ de frais) mais reçoit 12 R$ (10 R$ récompense, 2 R$ frais). Son solde précédent étant de 12 R$, il est maintenant de 19 R$.
- Le nœud 9 reçoit 3 R$ du nœud 5, son solde précédent étant de 1 R$, il a maintenant 4 R$.
- Les soldes des nœuds 4 et 8 ne changent pas.

5) Le noeud 9 enchaîne un bloc au bloc 40, le blocID est donc 940.

Dans cette chaîne, seulement 10 R$ ont été créés. En plus de la récompense, une transaction est insérée dans le nouveau bloc :

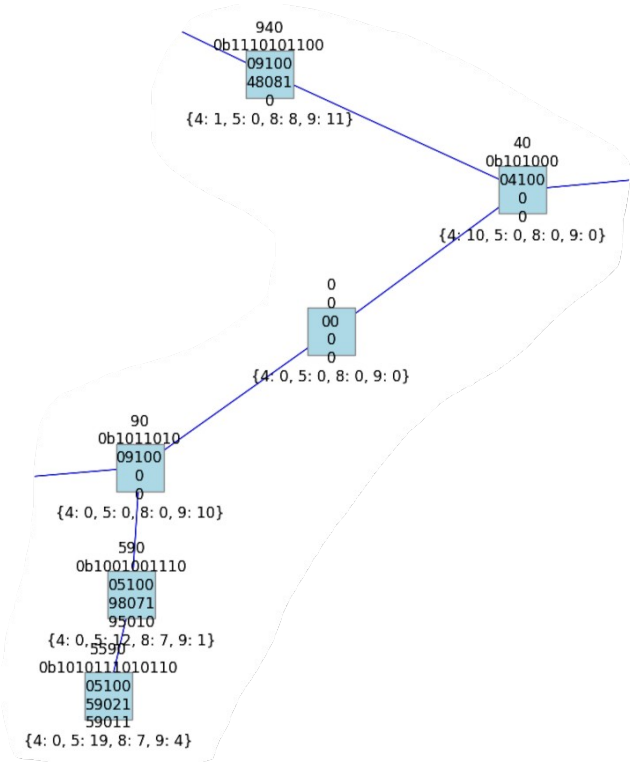
- 48081 : le nœud 4 paye 8 R$ au nœud 8, et paye 1 R$ de frais de transaction.

Si le bloc est finalisé,

- le nœud 9 reçoit 11 R$ (10 R$ de

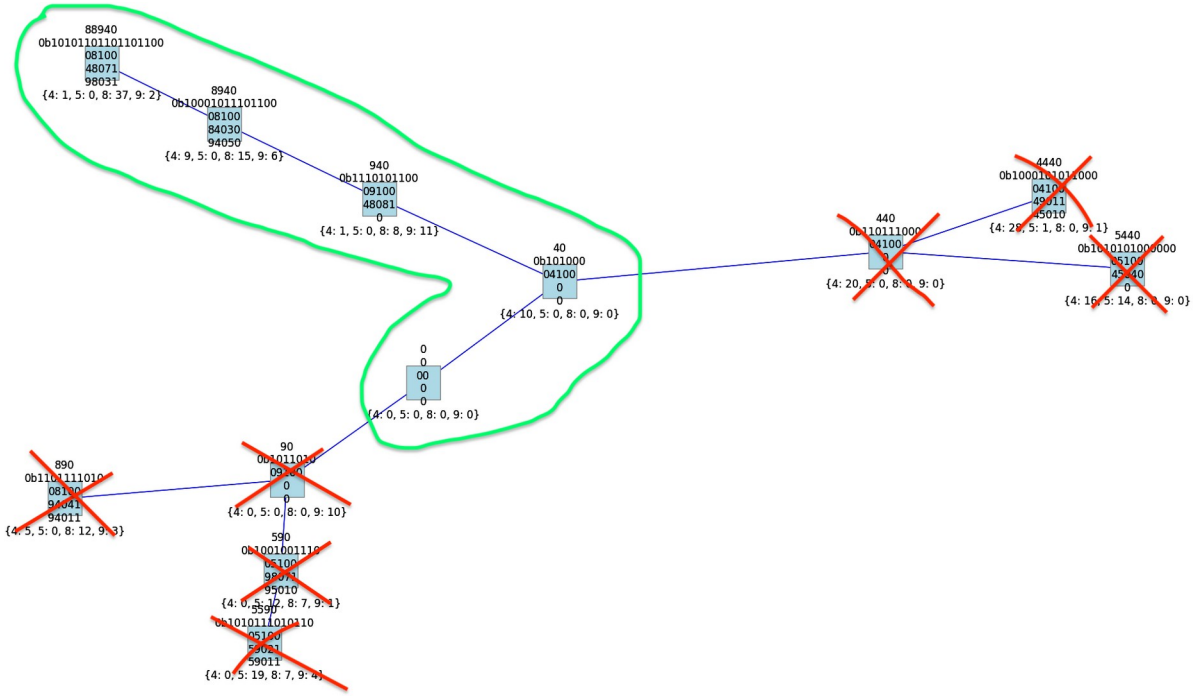
récompense, 1 R$ de frais) ;

- le nœud 4 paye 9 R$ (8 R$ au nœud 8 et 1 R$ de frais). Son solde précédent étant de 10 R$, il lui reste 1 R$;
- le nœud 8 reçoit 8 R$ du nœud 4 ;
- le solde du nœud 5 reste à 0.



Les blocs 890, 440, 8940, … sont ensuite enchaînés de la même façon, en calculant à chaque fois les soldes des nœuds pour s'assurer qu'ils ont les fonds pour honorer les transactions.

A la fin de l'activité, seule la chaîne la plus longue compte, et seules les transactions confirmées par les blocs 40-540-8540-88540 vont permettre la création de R$ (pour les récompenses) et le transfert de R$ entre les utilisateurs. L'activité se termine donc avec un solde de 1 R$ pour le nœud 4, 0 R$ pour le nœud 5, 37 R$ pour le nœud 8 et 2 R$ pour le nœud 9.



Le registre de cette chaîne de blocs est le suivant :

BlocID	PoW	Tx1	Tx2	Tx3
0	0	0	0	0
40	0b101000	04100	0	0
90	0b1011010	09100	0	0
590	0b1001001110	05100	98071	95010
5590	0b1010111010110	05100	59021	59011
940	0b1110101100	09100	48081	0
890	0b1101111010	08100	94041	94011
440	0b110111000	04100	0	0
8940	0b10001011101100	08100	84030	94050
88940	0b10101101101101100	08100	48071	98031
5440	0b1010101000000	05100	45040	0
4440	0b1000101011000	04100	49011	45010

Comme expliqué dans l'activité 1, le registre de la chaîne de blocs ne donne pas le solde de chaque noeud. Pour calculer le solde, il faut remonter la chaîne jusqu'au bloc-genèse et comptabiliser les transactions. Dans le tableau ci-dessous, les données du registre ont été réorganisées par chaîne.

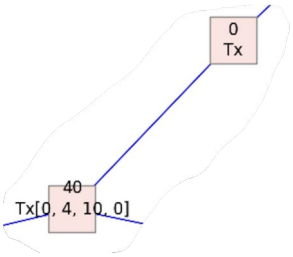
BlocID	PoW	Tx1	Tx2	Tx3	Solde
0	0	0	0	0	{4: 0, 5: 0, 8: 0, 9: 0}
40	0b101000	04100	0	0	{4: 10, 5: 0, 8: 0, 9: 0}
940	0b1110101100	09100	48081	0	{4: 1, 5: 0, 8: 8, 9: 11}
8940	0b10001011101100	08100	84030	94050	{4: 9, 5: 0, 8: 15, 9: 6}
88940	0b10101101101101100	08100	48071	98031	{4: 1, 5: 0, 8: 37, 9: 2}
0	0	0	0	0	{4: 0, 5: 0, 8: 0, 9: 0}
90	0b1011010	9100	0	0	{4: 0, 5: 0, 8: 0, 9: 10}
890	0b1101111010	8100	94041	94011	{4: 5, 5: 0, 8: 12, 9: 3}
0	0	0	0	0	{4: 0, 5: 0, 8: 0, 9: 0}
90	0b1011010	09100	0	0	{4: 0, 5: 0, 8: 0, 9: 10}
590	0b1001001110	05100	98071	95010	{4: 0, 5: 12, 8: 7, 9: 1}
5590	0b1010111010110	5100	59021	59011	{4: 0, 5: 19, 8: 7, 9: 4}
0	0	0	0	0	{4: 0, 5: 0, 8: 0, 9: 0}
40	0b101000	04100	0	0	{4: 10, 5: 0, 8: 0, 9: 0}
440	0b110111000	04100	0	0	{4: 20, 5: 0, 8: 0, 9: 0}
5440	0b1010101000000	05100	45040	0	{4: 16, 5: 14, 8: 0, 9: 0}
0	0	0	0	0	{4: 0, 5: 0, 8: 0, 9: 0}
40	0b101000	04100	0	0	{4: 10, 5: 0, 8: 0, 9: 0}
440	0b110111000	04100	0	0	{4: 20, 5: 0, 8: 0, 9: 0}
4440	0b1000101011000	04100	49011	45010	{4: 28, 5: 1, 8: 0, 9: 1}

3.5.2 Exemple complet, variante 2 (finalisation après deux niveaux)

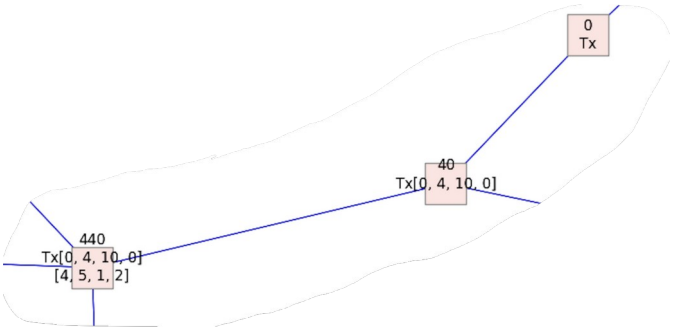
Cet exemple montre l'évolution d'une chaîne de blocs dont les blocs sont finalisés lorsque deux blocs sont enchaînés à sa suite.

1) Un premier bloc 40 est enchaîné au bloc-genèse, 2) le bloc 440 est enchaîné au bloc 40.

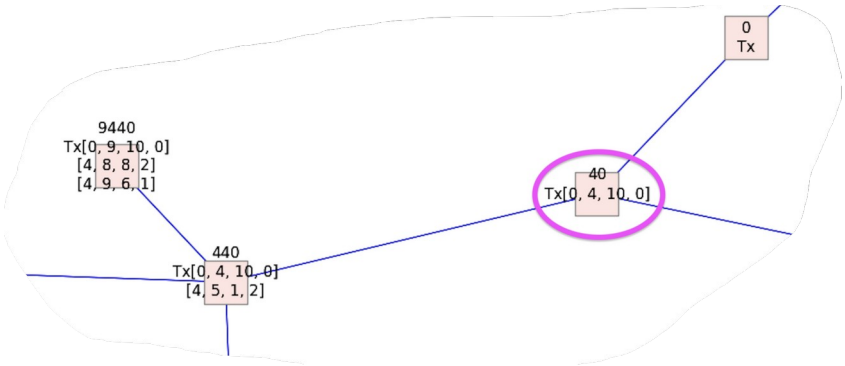
1)



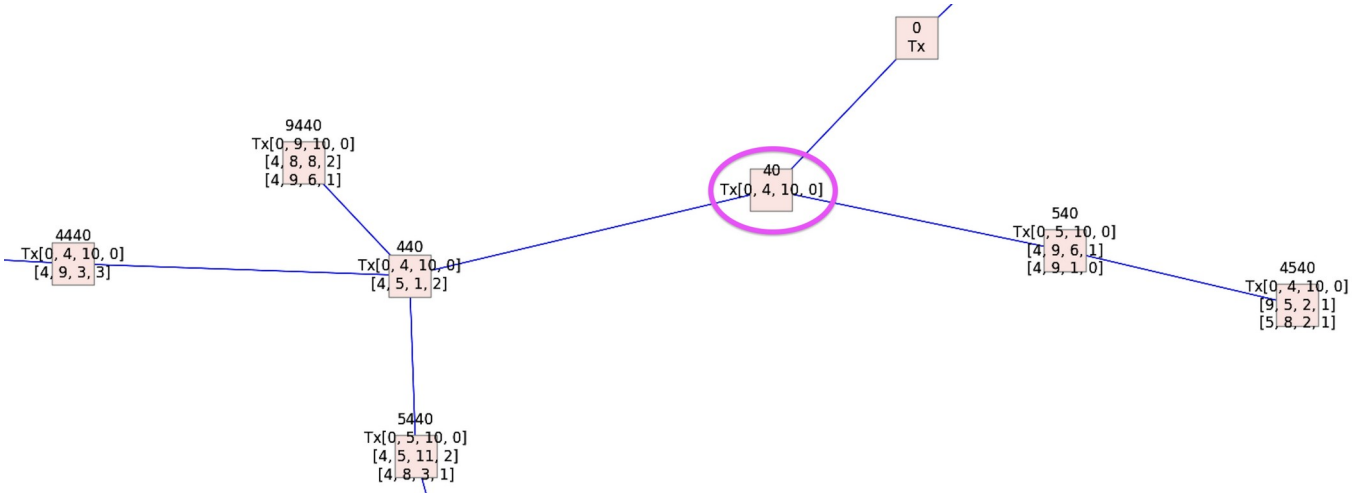
2)



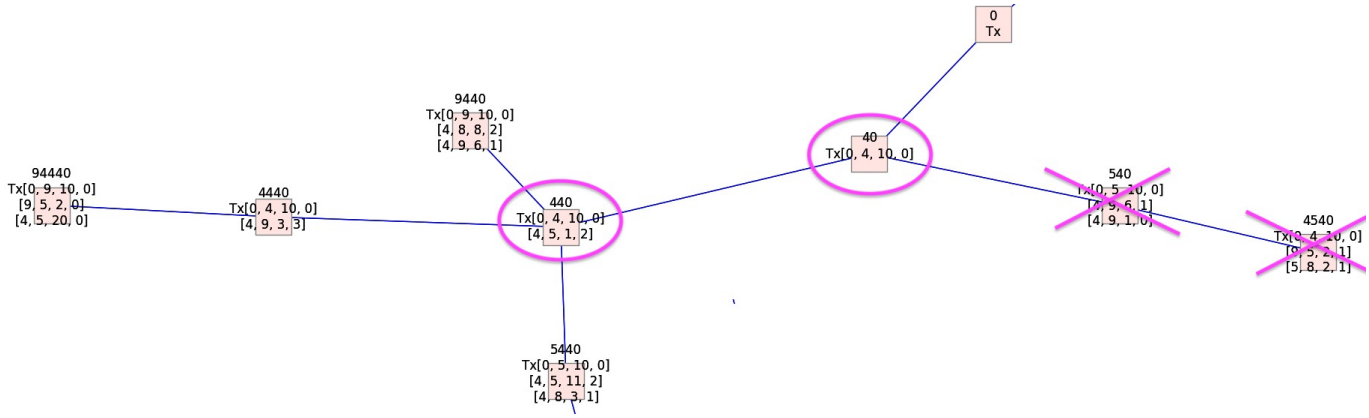
3) Lorsque le bloc 9440 est enchaîné au bloc 440, le bloc 40 est finalisé, car deux blocs le suivent :



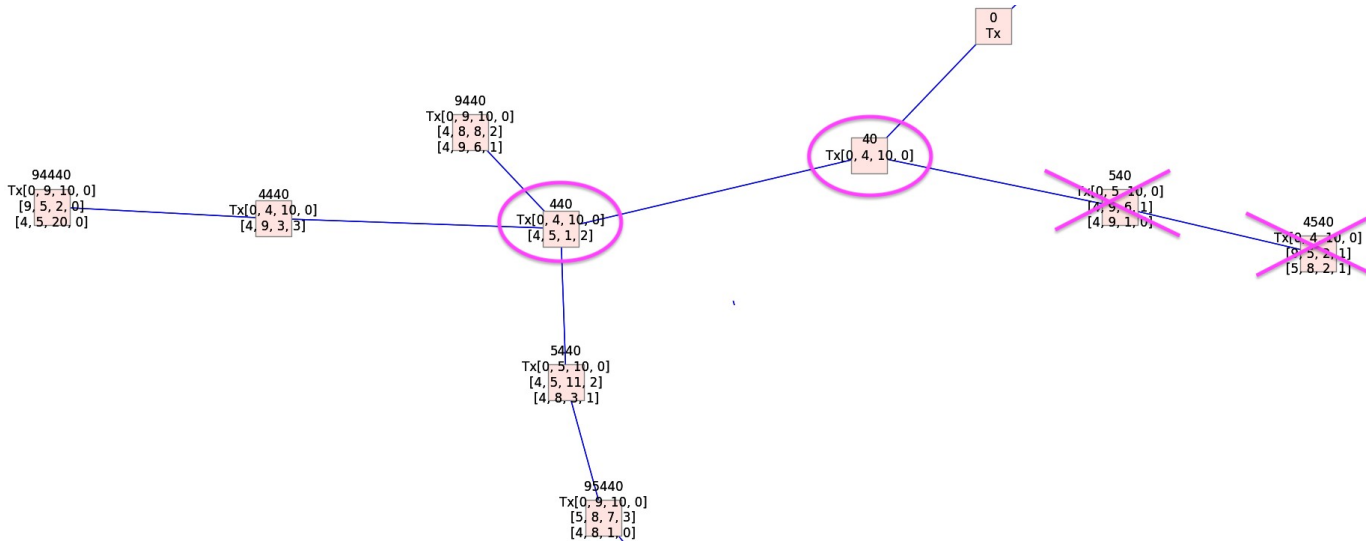
4) Les blocs 4440, 5440 et 4540 sont enchaînés, mais ils sont tous à deux niveaux du bloc 40, donc aucun autre bloc n'est finalisé :



5) Lorsque le bloc 94440 est enchaîné sur le bloc 4440, le bloc 440 est finalisé car deux blocs le suivent. Le bloc 540 est éliminé car il ne fait pas partie de la fourche où les blocs 40 et 440 sont finalisés, et par conséquent le bloc 4540 est lui aussi éliminé.



6) Le bloc 95440 est enchaîné au bloc 5440, mais aucun autre bloc n'est finalisé car il est au même niveau que le bloc 94440.



7) Lorsque le bloc 4 enchaîne le bloc 495440 sur le bloc 95440, alors le bloc 5440 est finalisé, et les blocs 9440, 4440 et 94440 sont éliminés.