Revue-IRS

Revue Internationale de la Recherche Scientifique (Revue-IRS)

ISSN: 2958-8413

Vol. 2, No. 5, November 2024

Blockchain et Théorie des Anneaux : Fondement aux transactions sécurisées et interopérables

Biaba Kuya Jirince[a,b,c], Anzola Kibamba Nestor[a,b], Iwazie Pelepoko Jonathan[a,b,d], Mwamba Kande Franklin[a,b,e], Frey Sylvestre[a,b,g,h], Oshasha Oshasha Fiston[a,b,f]

[a] University of Kinshasa (UNIKIN), Democratic Republic of Congo.
[b] Faculty of Science and Technology, B.P. 190 Kinshasa XI, University of Kinshasa (UNIKIN), Democratic Republic of Congo.
[c] Institut Francophone International (IFI)/ Vietnam National University Hanoi, adresse 144 Xuan Thuy, Cau Giay, Hanoi, Vietnam.
[d] National Institute of Statistics (INS), Democratic Republic of Congo.
[e] Institute of Health Sciences Research, P.O. Box 10.183, Democratic Republic of Congo.
[f] General Commissariat for Atomic Energy/Regional Center for Nuclear Studies of Kinshasa, P.O. Box 868, University of Kinshasa Campus/Democratic Republic of Congo.
[g] Forest Management Technique, Regional Postgraduate School of Integrated Management and Management of Forests and Tropical Territories (ÉRAIFT), P.O. Box 15.373, University of Kinshasa, Democratic Republic of Congo.
[h] Information system and AI, Green Computer Science, Faculty of Science and Technology.

Abstract: With the rise of blockchain technologies, digital transactions are becoming increasingly secure, transparent, and interoperable. To optimize the complex management of these transactions and ensure their integrity, essential mathematical concepts such as ring theory, homomorphic encryption, and ring signatures are indispensable. In this paper, we introduce a solution for the exchange of reward points on the blockchain, leveraging these tools to improve the efficiency, security, and interoperability of transactions. Through this practical case, we demonstrate how these concepts can be applied to preserve user privacy while ensuring secure exchanges in decentralized environments.

Keywords: **Blockchain, théorie des anneaux, chiffrement homomorphe, signatures en anneau, cryptographie, systèmes décentralisés, sécurité, interopérabilité, transactions, efficacité, numérique**.

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**14167570**

1 Introduction

La blockchain est souvent perçue comme une technologie révolutionnaire capable de transformer la manière dont nous stockons et échangeons de la valeur numérique[5]. Comme le souligne Don Tapscott, "La blockchain est une technologie transformatrice qui peut révolutionner la façon dont nous stockons et échangeons la valeur numérique.[16]" Aujourd'hui, cette technologie s'étend à divers domaines, allant de la finance à la santé, en passant par les chaînes d'approvisionnement et les systèmes de vote. Cependant, de nombreux systèmes traditionnels de gestion des transactions, tells que les systems bancaires centralisés, sont confrontés à plusieurs limitations. Ils fonctionnent souvent de manière isolée, ce qui limite leur flexibilité et leur interopérabilité avec d'autres systèmes[15]. De plus, ces systèmes sont fréquemment vulnérables aux fraudes et inefficaces dans la gestion des échanges, ce qui peut réduire leur efficacité et leur sécurité.

Pour contourner ces difficultés, l'usage de concepts mathématiques, tels que la théorie des anneaux, le chiffrement homomorphe, et les signatures en anneau, offre une solution prometteuse. Ces concepts permettent de modéliser

des structures de données complexes, assurant ainsi la sécurité, la transparence, et l'interopérabilité au sein des systèmes blockchain. Ils fournissent une base solide pour développer des solutions robustes dans la gestion des transactions numériques, y compris l'échange de points de récompense.

1.1 Objectifs

Cet article explore l'application de la théorie des anneaux et des techniques cryptographiques pour améliorer la sécurité, l'efficacité, et l'interopérabilité des systèmes de gestion de points de fidélité sur blockchain. L'objectif principal est de démontrer comment ces concepts mathématiques et cryptographiques peuvent offrir une solution robuste aux défis actuels de ces systèmes.

1.2 Modélisations

Les contributions spécifiques de cet article sont les suivantes :

- Modélisation Mathématique : Une modélisation des opérations de conversion de points et des transactions sur blockchain en utilisant la théorie des anneaux.
- Intégration Cryptographique : L'intégration de techniques cryptographiques avancées, telles que le chiffrement homomorphe et les signatures numériques en anneau, pour assurer la sécurité des transactions.
- Etude de Cas : Présentation d'un système pour l'échange de points de récompense sur la blockchain, illustrant l'application concrète des concepts théoriques abordés.

2 Théorie des Anneaux

Pour comprendre l'application de la théorie des anneaux à la blockchain, il est essentiel de saisir l'importance de ses concepts fondamentaux dans l'algèbre abstraite. Ces concepts jouent un rôle crucial dans la modélisation de structures de données complexes et la sécurisation des systèmes cryptographiques. En effet, les propriétés des anneaux permettent de créer des algorithmes robustes, garantissant ainsi la sécurité des transactions et l'intégrité des données au sein des systèmes décentralisés[3].

2.1 Définition 1

Un anneau est un ensemble non vide muni de deux lois de composition internes, l'une notée comme une addition et l'autre comme une multiplication, vérifiant les propriétés [11]:

- $(A, +)$ est un groupe abélien par l'addition (on note 0 son élément neutre),
- La multiplication est associative, c'est-à-dire : $(xy)z = x(yz)$ pour tous $x, y, z \in A$.
- La multiplication est distributive sur l'addition à gauche et à droite, c'est-à-dire [17]:

$$x(y + z) = xy + xz \tag{1}$$

Et [6]

$$(x + y)z = xz + yz \text{ pour tous } x, y, z \in A. \tag{2}$$

On dit que l'anneau A est commutatif si de plus la multiplication est commutative, c'est-à-dire : $xy = yx$ pour tous $x, y \in A$.

On dit que A est unitaire si de plus la multiplication admet un élément neutre $1 : x \cdot 1 = 1 \cdot x = x$ pour tout $x \in A$.

2.2 Exemple 1

1. L'ensemble $\mathbb{Z}$ des entiers est un anneau commutatif unitaire. Il en est de même de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
2. L'ensemble des matrices carrées d'ordre $n \geq 2$ à coefficients réels est un anneau non-commutatif (pour le produit matriciel) unitaire (de neutre multiplicatif la matrice identité). Il en est de même de l'anneau des endomorphismes d'un espace vectoriel (pour la loi $\circ$)[18].
3. L'anneau nul est l'anneau $\{0\}$ formé d'un unique élément.
4. Pour tout intervalle I de $\mathbb{R}$, l'ensemble $F(I, \mathbb{R})$ des applications de I dans $\mathbb{R}$ est un anneau commutatif (la multiplication étant le produit des fonctions défini par $(fg)(x) = f(x)g(x)$ pour tout $x \in \mathbb{R}$) unitaire (de neutre multiplicatif la fonction constante égale à 1). Il en est de même pour l'ensemble $\mathbb{R}^n$ des suites de réels.

2.3 Exemple 2

Fixons un entier $n \geq 2$. Considérons le groupe additif $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, (\overline{n-1})\}$. Rappelons que l'addition est définie par ccc:

$$\bar{x} + \bar{y} = x + \bar{y} \text{ pour tous } \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}.$$

On a vu que cette définition est indépendante des représentants choisis, et que le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est abélien. On définit une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ à partir de celle de $\mathbb{Z}$ en posant :

$$\bar{x} \cdot \bar{y} = x\bar{y} \text{ pour tous } \bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}.$$

Cette multiplication est bien définie, indépendamment des représentants choisis.
En effet, si $\bar{x} = \overline{x'}$ et $\bar{y} = \overline{y'}$, alors $x' = x + nu$ et $y' = y + nv$ pour deux entiers u, v $\in \mathbb{Z}$, de sorte que

$$x'y' = xy + n(uy + vx + nuv),$$

d'où $x'\overline{y'} = x\bar{y}$.

Il est immédiat de vérifier que $\mathbb{Z}/n\mathbb{Z}$ satisfait les conditions de la définition *1*, que $\bar{1}$ est neutre pour la multiplication, et que la multiplication est commutative. On conclut que : $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire.

2.4 Exemple 3

On fixe un anneau commutatif unitaire A [19].
Notons $B = A^{(\mathbb{N})}$ l'ensemble des suites d'éléments de A qui sont "à support fini", c'est-à-dire dont tous les termes sont nuls sauf un nombre fini d'entre eux.
On note $0_B = (0_A, 0_A, \ldots)$. Pour tout $f = (a_n)_{n\in\mathbb{N}}$ distinct de 0_B, on appelle degré de f le plus grand des entiers $n \in \mathbb{N}$ tels que $a_n \neq 0$.
On définit une addition et une multiplication dans B en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$ et $g = (b_n)_{n\in\mathbb{N}}$ dans B [19],

$$f + g = (a_n + b_n)_{n\in\mathbb{N}} \text{ et } fg = (c_n)_{n\in\mathbb{N}}, \tag{3}$$

avec

$$c_n \sum_{i=0}^{n} a_i\, b_{n-i} \tag{4}$$

On peut montrer que, pour ces opérations, B est un anneau commutatif unitaire, avec $0_B = (0_A, 0_A, \ldots)$ et $1_B = (1_A, 0_A, 0_A, \ldots)$. On l'appelle l'anneau des polynômes en une indéterminée à coefficients dans A.

On définit aussi le produit externe d'un élément $\alpha \in A$ par un élément $f = (a_n)_{n\in\mathbb{N}}$ en posant : $\alpha f = (\alpha\, a_n)_{n\in\mathbb{N}}$. À noter que le produit externe αf n'est autre que le produit interne de f par $(\alpha, 0_A, 0_A, \ldots)$. C'est pourquoi on convient de noter encore αf l'élément $(\alpha, 0_A, 0_A, \ldots)$ de B. En particulier $0_B = 0_A$ et $1_B = 1_A$.

En posant $e_i = (0_A, 0_A, \ldots, 0_A, 1_A, 0_A, \ldots)$, avec le 1_A en $(i+1)$-ième position, pour tout $i \in \mathbb{N}$, tout élément de B s'écrit de façon unique $f = \sum_{n\in\mathbb{N}} a_n e_n$ avec les $a_n \in A$ nuls sauf un nombre fini d'entre eux (de sorte que la somme est finie).
Il est clair que $e_n\, e_m = e_{n+m}$ pour tous $n, m \in \mathbb{N}$, et donc $e_n = e_1^n$ pour tout $n \in \mathbb{N}$.
On note traditionnellement $X = e_1$ et $B = A[X]$, et l'on retrouve les notations usuellement utilisées pour désigner les polynômes[19].

2.4.1 Remarques 1

1. Pour tout anneau commutatif unitaire A, les polynômes en une indéterminée à coefficients dans A forment un anneau commutatif unitaire, noté $A[X]$. Son neutre pour l'addition est 0_A. Son neutre pour la multiplication est 1_A [19].
2. Pour tout élément non-nul P de $A[X]$, il existe un unique entier naturel n et un unique $(n+1)$-uplet $(a_0, a_1, \ldots, a_n)$ d'éléments de A tels que :

$$P = a_nX^n + a_{n-1}X^{(n-1)} + \ldots + a_1X + a_0 \quad (5)$$

et

$$a_n \neq 0.$$

L'entier n est appelé le degré de P, noté deg P. L'élément non-nul a_n de A est appelé le coefficient dominant de P, noté $cd(P)$. Par convention, on pose $deg\ 0 = -\infty$ et $cd(0) = 0$ [19].

3. Deux polynômes $P = \sum_{i=0}^{n} a_iX^i$ et $Q = \sum_{i=0}^{n} b_iX^i$ sont égaux si et seulement si $n = m$ et $a_i = b_i$ pour tout $0 \leq i \leq n$. Un polynôme est nul si et seulement si tous ses coefficients sont nuls [19].
4. Si $P = \sum_{i=0}^{n} a_iX^i$ et $Q = \sum_{i=0}^{n} b_iX^i$, on a :

$$P + Q = \sum_{i=0}^{max\ (n,m)} (a_i + b_i)X^i \quad (6)$$

Et

$$PQ = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} (a_j b_{i-j}) \right) X^i \quad (7)$$

Sous forme développée explicite, la formule du produit est donc :

$$PQ = (a_nX^n + a_{n-1}X^{(n-1)} + \ldots + a_1X + a_0)\ (b_mX^m + b_{m-1}X^{(m-1)} + \ldots + b_1X + b_0)$$
$$= a_nb_mX^{(n+m)} + (a_nb_{m-1} + a_{n-1}X^{(n+m-1)} + \ldots + (a_1b_1)X^2 + (a_1b_0 + a_0b_1)X + a_0b_0\ [19].$$

5. On en déduit que, pour tous P et Q dans A[X], on a :

$$\deg(P + Q) \leq \max(\deg P, \deg Q)$$

Et

$$\deg(PQ) \leq \deg P + \deg Q.$$

2.5 Sous-Anneaux

2.5.1 Définition 2

Soit A un anneau. On appelle sous-anneau de A toute partie non-vide B de A qui vérifie les deux conditions suivantes [19]:

1. B est un sous-groupe du groupe additif A.
2. B est stable par la multiplication de A, c'est-à-dire que l'on a :

$$xy \in B \text{ quels que soient } x \in B \text{ et } y \in B.$$

2.5.2 Définition 3

Soit A un anneau unitaire. On appelle *sous-anneau unitaire* de A tout *sous-anneau* de A qui contient $1_{A\ V}$.

2.5.3 Remarques 2

1. Si B est un sous-anneau de A, alors B est lui-même un anneau (pour les lois déduites de celles de A par restriction à B). De fait, dans la pratique, pour montrer qu'un ensemble donné est un anneau, on cherche souvent à montrer que c'est un sous-anneau d'un anneau déjà connu [19].
2. Si B est un sous-anneau unitaire d'un anneau unitaire A, alors B est lui-même un anneau unitaire, et l'on a $1_B = 1_A$.
3. Si l'anneau A est commutatif, alors tout sous-anneau de A est commutatif.
4. Dans la pratique, pour montrer qu'un sous-ensemble non-vide B d'un anneau A est un sous-anneau de A, il suffit de vérifier que :

Pour tous $x \in B$ et $y \in B$, on a $x-y \in B$ et $xy \in B$.
Pour montrer qu'un sous-ensemble B d'un anneau unitaire A est un sous-anneau unitaire de A, il suffit de vérifier que $1_A \in B$ et (pour tous $x \in B$ et $y \in B$, on a $x-y \in B$ et $xy \in B$) [19].

2.5.4 Exemple 4

1. $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
2. $\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$ et $\mathbb{C}$.
3. $\mathbb{R}$ est un sous-anneau de $\mathbb{C}$.
4. A, avec ses lois, alors $\{0\}$ et A lui-même sont des sous-anneaux de A.
5. Tout anneau unitaire A est un sous-anneau unitaire de $A[X]$ [11].

2.6 Idéaux

2.6.1 Définition 4

Soit A un anneau commutatif unitaire. On appelle idéal de A toute partie non-vide I de A qui vérifie les deux conditions suivantes [19]:

1. I est un sous-groupe du groupe additif A.
2. Pour tous $x \in I$ et $a \in$ A, on a $xa \in I$.

2.6.2 Exemple 5

1. $\{0\}$ et A sont des idéaux de A.
2. Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un idéal de l'anneau $\mathbb{Z}$.
3. Dans l'anneau $\mathcal{F}(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions qui s'annulent en 0 est un

2.6.3 Idéaux premiers et maximaux

2.6.4 Définition 5

Soit I un idéal de l'anneau A. On dit que I est premier si l'anneau quotient A/I est intègre. L'ensemble des idéaux premiers de A est le spectre de A, noté $Spec(A)$ [11].

2.6.5 Exemple 6

1. L'ensemble des idéaux $n\mathbb{Z}$ de $\mathbb{Z}$ sont premiers si n est nul ou un nombre premier.
2. Les idéaux $(P) \subseteq K[X]$ où K est un corps, sont premiers si P est nul ou P est irréductible.

2.6.6. Proposition 1

Soient A un anneau et I un idéal de A. Les conditions suivantes sont équivalentes :

- I est premier.
- $I \neq A$ et $ab \in I$ implique que $a \in I$ ou $b \in I$, pour tous $a, b \in A$.
- $A \setminus I$ est une partie multiplicative de A.

2.6.7. Définition 6

L'idéal I de l'anneau A est maximal si l'anneau quotient A / I est un corps [11].

2.6.8. Remarque 3

Tout anneau maximal est un anneau premier car tout corps est un anneau intègre.

2.6.9. Exemples 7

- Les idéaux $n\mathbb{Z}$ de $\mathbb{Z}$ sont maximaux lorsque n est premier.
- Les idéaux $(P) \subseteq K[X]$ où K est un corps, sont maximaux si P est irréductible [11].

2.6.10. Proposition 2

Soient A un anneau et I un idéal de A. Les conditions suivantes sont équivalentes :

(1) I est maximal.
(2) $I \neq A$ et $\forall a \notin I, \exists b \in A$ tel que $ab - 1 \in I$.
(3) $I \neq A$ et $\forall$ idéal J de A avec $I \subseteq J \neq A$ on a $I = J$ [11].

2.7. Anneaux quotients

Soit A un anneau et I un idéal de A. Soit ~ la relation définie dans A par $a \sim b$ *ssi* $a - b \in I$, $\forall a,b \in A$ [11].

2.7.1. Proposition 3

La relation ~ ainsi définie est une relation d'équivalence.

Soit A/I le quotient de l'anneau A par la relation d'équivalence ~, c'est-à-dire l'ensemble des classes d'équivalence de ~.

Pour $a \in A$, on notera $\bar{a}$ la classe d'équivalence de a. Ensuite on définit deux lois binaires internes α et μ sur A de la manière suivante:

$$\alpha, \mu : A \times A \longrightarrow A/I$$
$$(a,b) \longmapsto \alpha(a,b) = \overline{a+b}$$
$$\mu(a,b) = \overline{a.b}$$

On vérifie que $\alpha(a,b)$ et $\mu(a,b)$ ne dépendent que des classes d'équivalence de a et de b.

En effet, si $a \sim c$ et $b \sim d$ on aura :
$(a + b) - (c + d) = (a - c) + (b - d) \in I$.
Donc $(a + b) \sim (c + d)$.
Et $ab - cd = b(a - c) + c(b - d) \in I$.
Donc $ab \sim cd$.
Ceci signifie que $\alpha(a,b) = \alpha(c,d)$ et $\mu(a,b) = \mu(c,d)$.
En conséquence, α et μ induisent deux lois internes binaires + et . sur A/I définies par :
$\bar{a} + \bar{b} = \overline{a+b}$ et $\bar{a}.\bar{b} = \overline{a.b}$

2.7.2. Proposition 4

A/I muni de ces deux lois est un anneau.
On a : $0 = \bar{0}$, $1 = \bar{1}$ et $-a = -\bar{a}$ dans A/I.
De plus l'application $\pi : A \longrightarrow A/I$

$$a \longmapsto \pi(a) = \bar{a}$$

est un morphisme d'anneaux [11].

2.7.3. Définition 7

Soit A un anneau et I un idéal de A. Le quotient de A par I est la paire $(A/I, \pi)$ où A/I est un anneau quotient et π est un morphisme de passage au quotient $\pi : A \longrightarrow A/I$.

2.7.4. Théorème de la division euclidienne

Soient A un anneau non nul et $F \in A[X]$ unitaire. Pour tout polynôme $P \in A[X]$, il existe des uniques polynômes Q et R dans $A[X]$ tels que $P = F.Q + R$ et $deg(R) < deg(F)$.

2.7.5. Corollaire 1

Soient A un anneau non nul et $F \in A[X]$ unitaire. Soit d le degré de F et $I \subseteq A$ l'idéal engendré par F. Alors, $\forall P \in A[X], \exists ! Q \in A[X]$ de degré strictement inférieur à d tel que P soit équivalent à Q modulo I. Autrement, le sous-ensemble de $A[X]$ des polynômes de degré strictement inférieur à d est un système de représentation pour les classes d'équivalence modulo I [11].

2.7.6. Exemples 8

- On définit deux lois internes $\oplus$ et $\odot$ dans $\mathbb{Z}$ par :

$$\oplus : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(m,n) \longmapsto \oplus(m,n) = m + n$$
$$\odot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(m,n) \longmapsto \odot(m,n) = -mn$$

$(\mathbb{Z}, \oplus, \odot)$ est-il un anneau ?

$\oplus : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$

$(m,n) \longmapsto \oplus(m,n) = m + n + 1$

$\odot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$

$(m,n) \longmapsto \odot(m,n) = mn + m + n.$

$(\mathbb{Z}, \oplus, \odot)$ est-il un anneau ?

- Déterminer $\sum_{a\in A} a$ et $\prod_{a\in A\setminus\{0\}} a$ pour tous les anneaux finis A = $\mathbb{Z}/_{n\mathbb{Z}}$

avec n un entier non nul.

- Solution

  $\mathbb{Z}/_{n\mathbb{Z}} = \{\dot{0}, \dot{1}, \dot{2}, \dots, \widehat{n-1}\}$

  $\sum_{a\in A} a = \dot{0} + \dot{1}, \dot{2} + \cdots + \widehat{n-1}$. Comme $0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$, donc

  $\sum_{a\in A} a = \frac{(n-1)[(n+1)-1]}{2} = \frac{n(n-1)}{2}$.

- Application

  $A = \mathbb{Z}_6$ et $B = \mathbb{Z}_{15}$

  $\sum_{a\in A} a = \frac{6(6-1)}{2} = \frac{6(5)}{2} = 15$

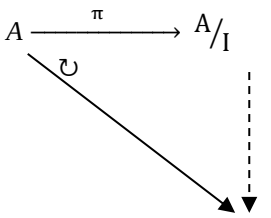
  $\sum_{b\in B} b = \frac{15(15-1)}{2} = \frac{15(14)}{2} = 105.$

2.7.7. Remarque 4

La définition du quotient comme l'anneau quotient est d'une subtilité.
En effet, le morphisme de passage au quotient établit le lien tel que l'anneau *A* et son anneau quotient ou quotienté $A/_I$. Sans ce morphisme il n'aurait eu aucun rapport tel *A* et $A/_I$. Ils auraient été tout simplement deux anneaux flottant dans l'univers. D'où la propriété universelle du quotient [11].

2.7.8. Propriété universelle du quotient

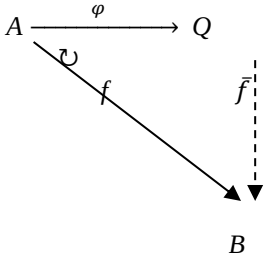
Soient *A* un anneau et *I* un idéal de *A*. Soit $\pi : A \longrightarrow A/_I$ le morphisme de passage au quotient. Alors, on a : $\pi(I) = \{0\}$ et π est le morphisme universel ayant cette propriété, c'est-à-dire $\forall$ *B* anneau et $\forall f : A \longrightarrow B$ un morphisme avec $f(I) = \{0\}$, il existe un morphisme $\bar{f} : A/_I \longrightarrow B$ tel que le diagramme suivant commute, c'est-à-dire :



càd $\bar{f} \circ \pi = f$.

2.7.9. Définition 8

Soit *A* un anneau et $I \subseteq A$ un idéal. Un morphisme d'anneau $\varphi : A \longrightarrow Q$ est un quotient de *A* par *I* si $\varphi(I) = \{0\}$ et pour tout anneau *B* et pour tout morphisme $f : A \longrightarrow B$ avec $f(I) = \{0\}$, il existe un et un seul morphisme d'anneaux $\bar{f} : Q \longrightarrow B$ tel que le diagramme suivant commute [11]:



2.7.10. Proposition 5

Soient *A* un anneau et $I \subseteq A$ un idéal. Soit $\pi : A \longrightarrow {}^{A}/_{I}$ le morphisme de passage au quotient. Lorsque $\varphi : A \longrightarrow Q$ est un quotient de *A* par *I*, il existe un isomorphisme $f : {}^{A}/_{I} \longrightarrow Q$ tel que $f \circ \pi = \varphi$. En particulier ${}^{A}/_{I}$ et Q sont isomorphes.

2.7.11. Proposition 6

Soient *A* un anneau, $I \subseteq A$ un idéal et $\pi : A \longrightarrow Q$ un morphisme d'anneaux. Le morphisme φ est un quotient de *A* par *I* ssi φ est surjection et ker $\varphi = I$.

2.7.12. Exemples 9

Soient *A* un anneau et $a \in A$. Soit $f : A[X] \longrightarrow A$ le morphisme d'évaluation en *a* càd $f(P) = P(a)$, où $P(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ et $P(a) = a_n a^n + a_{n-1}a^{n-1} + \cdots + a_1 a + a_0$.

Alors, *f* est un quotient de *A[X]* par l'idéal $(X - a)$.

En effet, *f* est surjectif et on a $(X - a) \subseteq \ker f$.

Pour montrer l'inclusion $\ker f \subseteq (X - a)$, on utilise la division euclidienne dans *A[X]*. Alors, il existe $Q, R \in A[X]$ tels que $P = (X - a)Q + R$ où $deg(R) < deg(X - a) = 1$. D'où $R \in A$ et l'évaluation en *a* donne $0 = P(a) = 0.Q(a) + R(a) = R$, c'est-à-dire $R = 0$ et donc $P \in (X - a)$ [11].

2.8. Conclusion

Cette section a présenté les bases de la théorie des anneaux, essentielles pour modéliser et sécuriser les transactions dans des systèmes comme la blockchain. Nous avons exploré des concepts clés, tels que les anneaux de polynômes et de matrices, ainsi que les sous-anneaux et idéaux, qui posent les fondations pour l'application de ces théories à la gestion sécurisée des points de récompense, sujet que nous approfondirons dans les sections suivantes.

3. Une esquisse sur la blockchain

La blockchain est une technologie révolutionnaire qui permet de stocker et d'échanger des données de manière décentralisée, sécurisée et transparente. Elle est principalement connue pour son utilisation dans les cryptomonnaies comme le Bitcoin, mais ses applications vont bien au-delà du domaine financier. En substance, une blockchain est un registre distribué qui enregistre toutes les transactions effectuées sur un réseau de manière chronologique et immuable. Chaque transaction est regroupée dans un « bloc », et ces blocs sont liés entre eux pour anciennement une chaîne de blocs (blockchain) [46].

Contrairement aux systèmes centralisés traditionnels, où une autorité centrale contrôle les données et les transactions, la blockchain repose sur un réseau de participants (ou nœuds) qui valident les transactions grâce à des mécanismes de consensus. Ce modèle décentralisé offre plusieurs avantages clés, notamment la transparence, la sécurité renforcée contre les fraudes et la réduction des intermédiaires.

3.6. Caractéristiques

La blockchain se distingue par plusieurs caractéristiques fondamentales qui lui confèrent sa robustesse et son efficacité dans la gestion des transactions numériques. Parmi ces caractéristiques, on retrouve :

- **Immutabilité** : Une fois qu'une transaction est validée et inscrite dans un bloc, elle ne peut plus être modifiée ou supprimée, garantissant ainsi l'intégrité des données.
- **Sécurité** : Grâce à des techniques cryptographiques avancées, la blockchain assure que seules les parties autorisées peuvent accéder aux informations sensibles ou effectuer des transactions.
- **Transparence** : Toutes les transactions sont visibles par tous les participants au réseau, ce qui accroît la confiance et réduit le risque de manipulation.
- **Décentralisation** : Aucun acteur central ne contrôle la blockchain, ce qui la rend résistance aux attaques et aux manipulations externes.

4. Utilisation et Création des Anneaux dans la Blockchain

4.1. Introduction

Les systèmes cryptographiques modernes reposent sur des fondations mathématiques solides pour assurer la sécurité et l'efficacité des transactions numériques. Parmi ces fondations, les structures algébriques appelées anneaux jouent un rôle central [22]. En cryptographie, les anneaux permettent de structurer et de manipuler les données de manière sécurisée, offrant ainsi des garanties robustes contre les attaques potentielles [21].

Dans cette section, nous explorerons comment les anneaux sont utilisés pour renforcer la sécurité des transactions blockchain, en nous concentrant sur leur rôle dans la sécurité mathématique, le chiffrement homomorphe, et les signatures en anneau.

4.2. Application des Propriétés des Anneaux dans la Blockchain

En exploitant les propriétés spécifiques des anneaux, comme la commutativité et la distributivité, il est possible de développer des algorithmes robustes pour sécuriser les transactions sur la blockchain. Ces algorithmes garantissent que les opérations effectuées dans un environnement décentralisé respectent les règles mathématiques rigoureuses définies par la théorie des anneaux [21], assurant ainsi la sécurité et l'intégrité des données.

4.3. Sécurité Mathématique

Les anneaux offrent une structure algébrique rigide qui permet de définir des opérations arithmétiques complexes de manière sécurisée. Les propriétés intrinsèques des anneaux, telles que la commutativité, l'associativité et la distributivité, sont essentielles pour la conception d'algorithmes de chiffrement robustes [8]. Par exemple, l'anneau des polynômes à coefficients entiers, noté $\mathbb{Z}[X]$, est couramment utilisé pour ses propriétés structurelles favorables [11].

4.4. Exemple 10

Pour mieux comprendre la nature cyclique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ [19], considérez le diagramme ci-dessous qui illustre les opérations d'addition modulo n. Cette structure est cruciale pour garantir la sécurité dans divers schémas cryptographiques en offrant une base rigide pour les opérations arithmétiques sécurisées [20].

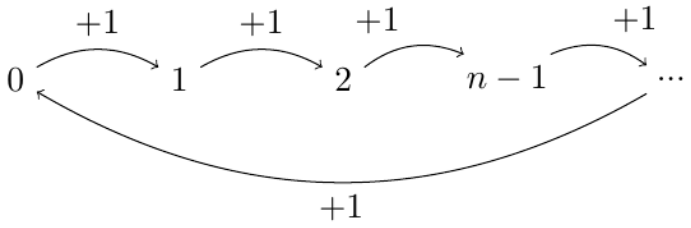


Figure 1. Anneau $\mathbb{Z}/n\mathbb{Z}$ avec l'opération d'addition modulo n.

Cette représentation montre comment l'opération +1 est appliquée de manière cyclique à travers tous les éléments de l'anneau, soulignant la nature commutative et associative de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Après avoir établi les bases mathématiques de la sécurité, nous allons maintenant explorer comment ces concepts sont appliqués dans le chiffrement homomorphe, une technique clé pour la protection des données sur la blockchain.

4.5. Chiffrement Homomorphe

4.5.1. Principes

Le chiffrement homomorphe est une technique cryptographique avancée permettant de réaliser des calculs sur des données chiffrées sans les déchiffrer [24] [27]. Ce procédé est crucial pour préserver la confidentialité des données, particulièrement dans des environnements où la sécurité est primordiale, tels que le cloud computing, les transactions blockchain, et la gestion des données sensibles [8].

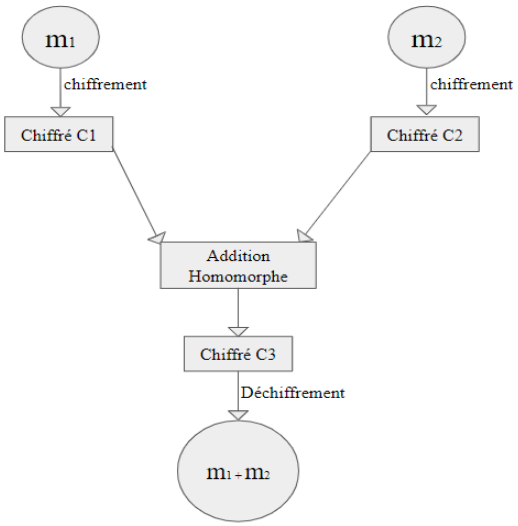


Figure 2. Processus de chiffrement homomorphe.

4.5.2. Types de Chiffrement Homomorphe

Le chiffrement homomorphe se décline en plusieurs types, chacun adapté à des besoins spécifiques. Les deux principaux sont [8]:

1. Chiffrement homomorphe partiel (PHE) : permet de réaliser une opération spécifique (addition ou multiplication) [25].
2. Chiffrement homomorphe total (FHE) : permet de faire une combinaison illimitée d'opérations arithmétiques [23].

4.5.3. Exemple 11

• Chiffrement : Pour chiffrer un message m, un nombre aléatoire r est choisi dans l'ensemble $\{0, 1, \ldots, n\text{-}1\}$ et le message est chiffré en utilisant une clé publique précomptée g et h comme suit [8] [24]:

$$c = E(m) = g^m h^r \bmod n \tag{8}$$

où g et h sont des éléments générés lors de la configuration du schéma, et n est un module.

• Déchiffrement : Pour déchiffrer le texte chiffré c, on calcule $c' = c^{q1}$ où $c^{q1} = (g^m h^r)^{q1} = (g^{q1})^m$. Ensuite, en utilisant la clé secrète q^1, le message est récupéré par le calcul du logarithme discret [25]:

$$m = D(c) = \log_g c' \tag{9}$$

Cette étape nécessite une gestion attentive de l'espace des messages pour assurer que le logarithme discret reste calculable.

• Homomorphisme sur l'Addition : Si deux messages chiffrés $E(m_1) = c_1$ et $E(m_2) = c_2$ sont additionnés, l'opération homomorphe sur les chiffres est réalisée comme suit [8] [25]:

$$c = c_1 \cdot c_2 \cdot h^r = (g^{m1} h^{r1})(g^{m2} h^{r2}) h^r = g^{(m1 + m2)} h^{(r_1 + r_2 + r)} \tag{10}$$

Ici, l'addition des messages est réalisée directement sur les chiffres, ce qui permet de récupérer $m_1 + m_2$ à partir du chiffre résultant.

• Homomorphisme sur la Multiplication : Pour effectuer une multiplication homomorphe, le schéma utilise des éléments g_1 et h_1 avec des ordres respectifs n et q_1, définis comme $g_1 = e(g , g)$ et $h_1 = e(g, h)$. La multiplication des messages [26] m_1 et m_2 est alors calculée comme suit :

$$c = e(c_1, c_2)\, h_1^r = e(g^{m_1} h^{r_1}, g^{m_2} h^{r_2})\, h_1^r = g_1^{m_1 m_2} h_1^{m_1 r_2 + m_2 r_1 + q_2 r_1 r_2 + r} \tag{11}$$

où *r est une variable uniformément distribuée, et donc* $m_1 m_2$ peut être récupéré du texte chiffré resultant c.

4.5.4. Algorithme de Paillier

L'algorithme de Paillier, basé sur la difficulté du problème de résiduosité composite, est un chiffrement homomorphe additif qui permet d'additionner des textes chiffrés [8].

• Chiffrement : Pour chiffrer un message *m*, un nombre aléatoire *r* est choisi dans $\mathbb{Z}_n^*$ (où *n* est un produit de deux grands nombres premiers), et le chiffre est calculé comme suit :

$$c = g^m \cdot r^n \, mod \, n^2 \tag{12}$$

Ici, *g* est un élément de $\mathbb{Z}_n^*$ tel que l'ordre de *g* divise *n*, et *r* est un aléatoire.

• Déchiffrement : Le message *m* est déchiffré par :

$$m = \frac{L\,(c^{\lambda} \, mod \, n^2)}{L\,(g^{\lambda} \, mod \, n^2)} mod \, n \tag{13}$$

où $L(u) = \frac{u-1}{n}$ et λ est le plus petit commun multiple de *p*-1 et q-1 pour les facteurs premiers *p* et q de *n*.

4.5.5. Domaines d'applications du Chiffrement Homomorphe

Le chiffrement homomorphe, en raison de sa capacité à traiter des données chiffrées sans les déchiffrer, est particulièrement adapté à des domaines où la confidentialité et la sécurité sont primordiales. Voici quelques applications clés :

- **Finance** : Utilisé pour réaliser des calculs confidentiels sur des données financières, comme la gestion de portefeuilles et l'évaluation des risques, tout en garantissant que les données sensibles restent protégées [30].
- **Médecine** : Permet de mener des analyses statistiques sur des données patient chiffrées, ce qui préserve la confidentialité des informations médicales tout en facilitant la recherche médicale avancée.
- **Vote Électronique** : Essentiel pour les systèmes de vote électronique, où il assure la confidentialité des votes tout en garantissant un décompte transparent et sécurisé [29].

Ces applications illustrent l'importance du chiffrement homomorphe dans la protection des données sensibles, démontrant ainsi sa pertinence dans des secteurs critiques où la sécurité et la confidentialité sont des priorités absolues.

4.6. Schémas de Chiffrement Basés sur les Réseaux et les Anneaux

Les schémas cryptographiques tels que Learning With Errors (LWE) et NTRU utilisent des structures algébriques, spécifiquement des anneaux, pour renforcer la sécurité des systèmes. Ces schémas sont conçus pour offrir une résistance accrue contre les attaques, *y* compris celles provenant de futurs ordinateurs quantiques [32] [31].

4.6.1. Learning With Errors (LWE)

LWE repose sur des problèmes mathématiques complexes liés aux réseaux, exploitant les propriétés des anneaux pour sécuriser les opérations cryptographiques. Dans ce schéma, les éléments de l'anneau sont utilisés pour construire des vecteurs et des matrices, qui jouent un rôle clé dans le chiffrement et le déchiffrement [41] [42] [10].

- Création de l'anneau : Le schéma LWE utilise l'anneau $\mathbb{R} = \mathbb{Z}[X]/(X^n+1)$, où *n* est une puissance de deux. Les coefficients des polynômes dans cet anneau sont ensuite réduits modulo *q* pour former l'anneau $\mathbb{Z}_q[X]/(X^n + 1)$.
- Opération de base :
  - Addition *: (a(X) + b(X)) mod q*
  - Multiplication : *(a(X) · b(X)) mod (X^n + 1, q)*
- Algorithme de chiffrement
  - Génération de Clé : Un polynôme secret *s* est choisi, et une matrice publique *A* est générée. Le vecteur public $b = A \cdot s + e \, mod \, q$ est calculé, où *e* est un vecteur d'erreur.
  - Chiffrement : Le texte chiffré (*u*, *v*) est calculé à partir du message *m* et d'un vecteur aléatoire *r*:

$$u = A \cdot r \bmod q, \quad v = b \cdot r + m \bmod q \tag{14}$$

- Déchiffrement : Le message est récupéré en calculant $v - s \cdot u \bmod q$ et en réduisant les coefficients.

4.6.2. NTRU (N-th Degree Truncated Polynomial Ring Units)

NTRU est un cryptosystème basé sur l'utilisation de polynômes dans un anneau réduit, offrant une sécurité robuste contre les attaques [41] [42] [10].

- L'anneau utilisé est $\mathbb{R} = \mathbb{Z}[X]/(X^N - 1)$, où N est un entier spécifié. Les coefficients des polynômes sont réduits modulo q, créant ainsi l'anneau $\mathbb{Z}_q[X]/(X^N - 1)$.
- Opérations de Base
  - Addition : $(a(X) + b(X)) \bmod q$
  - Multiplication : $(a(X) \cdot b(X)) \bmod (X^N - 1, q)$
- Algorithme de Chiffrement
  - Génération de Clé : Deux polynômes f et g sont choisis tels que f est inversible modulo q et g modulo p. On calcule $h = f^{-1} * g \bmod q$.
  - Chiffrement : Le message m est chiffré en utilisant un polynôme aléatoire r :

$$c = p \cdot r * h + m \bmod q \tag{15}$$

  - Déchiffrement : Le message est récupéré en calculant $a = f * c \bmod q$ et en réduisant les coefficients modulo p.

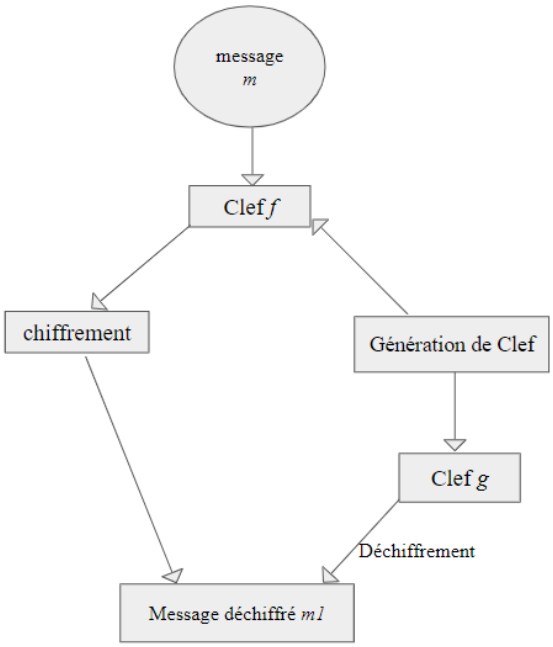


Figure 3. Processus de génération de clés, chiffrement avec la clé *f*, et déchiffrement avec la clé *g* dans NTRU.

Ces schémas démontrent l'importance des anneaux en cryptographie, car ils permettent d'effectuer des opérations sécurisées tout en préservant la structure des données. En particulier, leur résistance aux attaques quantiques en fait des outils essentiels pour la sécurité des systèmes futurs.

4.7. Signatures en Anneau

4.7.1. Introduction

Les signatures en anneau sont une technique cryptographique qui permet à un membre d'un groupe de signer un message de manière anonyme. Ce mécanisme garantit que la signature provient d'un membre du groupe, sans révéler lequel. Les signatures en anneau sont particulièrement utiles dans les situations où l'anonymat est crucial, telles que les systèmes de dénonciation sécurisée[38].

4.7.2. Création de l'Anneau de Signataires

Pour créer une signature en anneau, il est nécessaire de disposer d'un ensemble de clés publiques des signataires potentiels ainsi que de la clé privée de l'un des signataires[36]. Considérons un ensemble de n utilisateurs, chaque utilisateur i possédant une paire de clés publique/privée (PK_i, SK_i) [38].

- Algorithme de Signature [36][39]

(a) Sélection de l'Anneau : Sélectionner $n - 1$ clés publiques $PK_1, PK_2, ..., PK_{n-1}$ et ajouter la clé publique du signataire PK_s pour former l'anneau.
(b) Message à Signer : Soit M le message à signer.
(c) Calcul des Valeurs de l'Anneau :

- Générer une valeur aléatoire u.
- Calculer $h = H(M, u)$, où H est une fonction de hachage cryptographique.
- Pour chaque $i \neq s$, générer aléatoirement x_i et calculer $y_i = g^{x_i} \cdot PK_i^{h_i} \bmod q$, où g est une base génératrice du groupe cyclique et q est l'ordre du groupe.
- Calculer x_s de sorte que $y_s = g^{x_s} \cdot PK_s^{h_s} \bmod q$ soit cohérent avec les valeurs précédentes.

(d) Calcul de la Signature : La signature est le tuple $(h, y_1, y_2, \ldots, y_n)$.

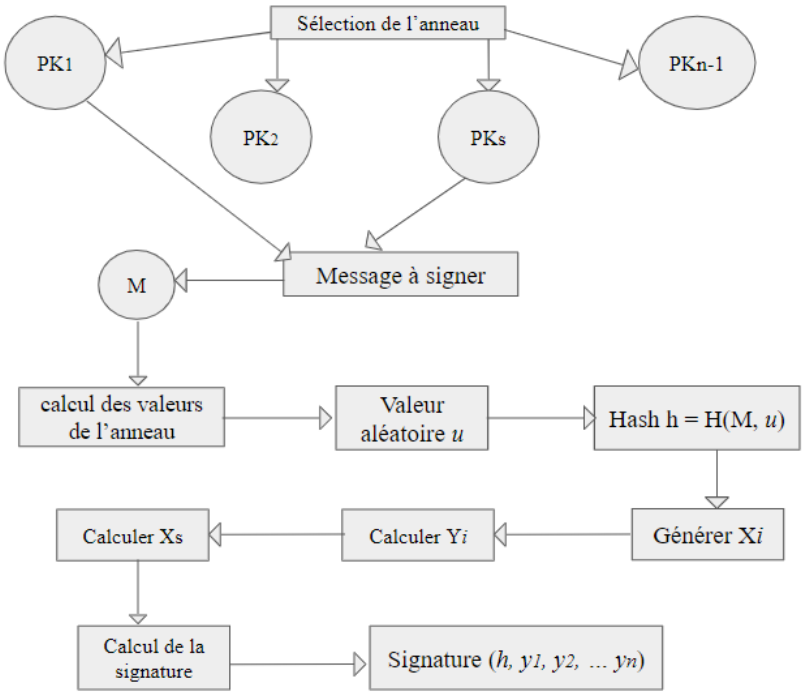


Figure 4. Processus de l'algorithme de Signature.

- Vérification de la Signature [36][39]

(a) verification des valeurs :

- Pour chaque i verifier que $y_i = g^{x_i} \cdot PK_i^{h_i} \bmod q$,
- Si toutes les équations sont verifiées, la signature est valide.

(b) Hachage du Message : Recalculer h pour vérifier qu'il correspond à celui inclus dans la signature.

4.7.3. Exemple 12

Considérons un groupe de trois utilisateurs avec les paires de clés suivantes :

- (PK_1, SK_1)
- (PK_2, SK_2)
- (PK_3, SK_3)

L'utilisateur 2 souhaite signer un message M de manière anonyme.

1. Sélection de l'Anneau : PK_1, PK_2, PK_3 sont sélectionnés.
2. Calcul des valeurs:
   (a) Générer u aléatoirement et calculer $h = H(M, u)$.
   (b) Générer aléatoirement x_1 et x_3, puis calculer y_1 et y_3.
   (c) Calculer x_2 de sorte que y_2 soit cohérent avec y_1 et y_3.
3. Signature : Le tuple (h, y_1, y_2, y_3) constitue la signature.
4. Vérification : Vérifier que chaque y_i satisfait les équations correspondantes.

4.8. Conclusion

En résumé, cette section a démontré comment la théorie des anneaux et les techniques cryptographiques avancées peuvent être intégrées pour renforcer la sécurité des transactions sur blockchain. Ces concepts constituent une base solide pour le développement de systèmes cryptographiques robustes, un sujet qui sera approfondi dans les sections suivantes.

5. Application des Concepts Théoriques à l'Échange de Points de Récompense

Dans cette section, nous explorerons l'application pratique des concepts théoriques discutés précédemment, notamment la théorie des anneaux et les techniques cryptographiques, au sein d'un système d'échange de points de récompense. L'objectif est de montrer comment ces théories mathématiques, souvent considérées comme abstraites, peuvent être intégrées dans un cadre opérationnel pour résoudre des problèmes concrets liés aux programmes de fidélité. Ce système, basé sur la technologie blockchain, vise à offrir une solution interopérable, sécurisée et transparente qui permet aux utilisateurs d'échanger leurs points de fidélité à travers différentes plateformes.

Pour illustrer cela, nous décrirons d'abord le fonctionnement général du système d'échange de points de récompense, en soulignant les étapes clés du processus, de la demande initiale à la reconversion des points. Ensuite, nous approfondirons l'application des théories des anneaux et des méthodes cryptographiques dans ce contexte, en expliquant comment ces concepts renforcent la sécurité et l'efficacité du système.

5.1. Présentation du système d'échange

5.1.1. Processus d'Echange

Le système d'échange de points de récompense que nous décrivons est conçu pour offrir une interopérabilité complète entre divers programmes de fidélité, en utilisant la blockchain comme plateforme de base. Ce système permet aux utilisateurs d'envoyer leurs points à d'autres utilisateurs, même s'ils appartiennent à des programmes de fidélité différents. En retour, ces utilisateurs peuvent également recevoir des points provenant d'autres programmes. La blockchain se charge de convertir ces points de fidélité en une unité universelle, facilitant ainsi les échanges inter-programmes.

Chaque étape du processus est automatisée grâce à des smart contracts, qui non seulement exécutent les transactions mais en garantissent également la sécurité et la transparence. Les transactions sont immuablement enregistrées sur la blockchain, ce qui assure une traçabilité complète et réduit considérablement les risques de fraude ou de manipulation.

Pour mieux comprendre ce processus, le schéma ci-dessous illustre les différentes étapes d'un échange de points de fidélité via la blockchain.

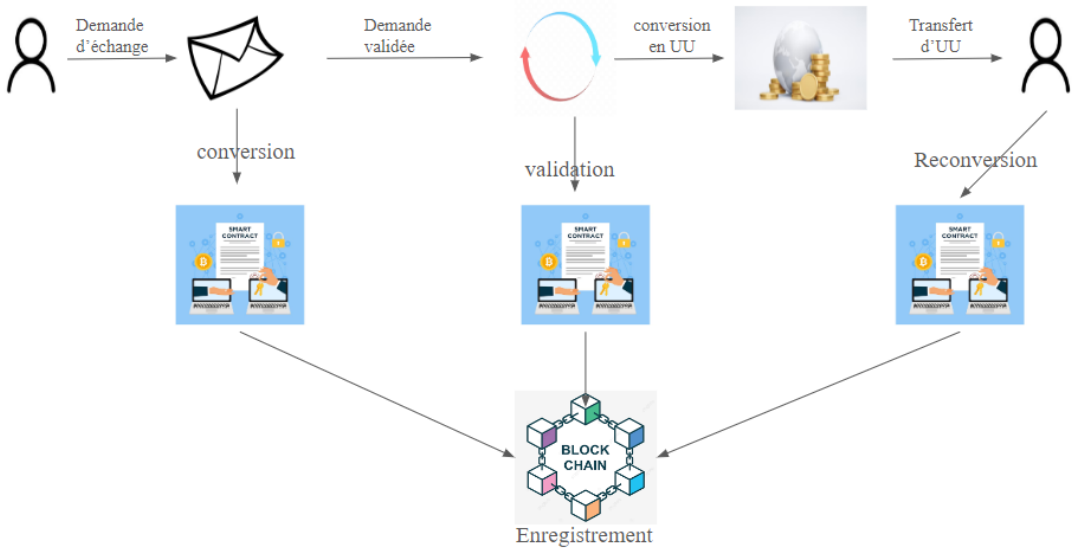


Figure 5. Processus d'échange de points de fidélité via la blockchain.

5.1.2. Exemple 13

Un client peut convertir des points accumulés dans un programme de fidélité aérien en une unité universelle (*UU*) qui peut ensuite être utilisée pour obtenir des nuits gratuites dans une chaîne hôtelière partenaire.

Les étapes du processus sont les suivantes :

1. Demande d'Échange : Le client soumet une demande d'échange de ses points de fidélité aérienne via la plateforme blockchain. Cette demande indique l'intention de convertir ses points en unités universelles utilisables dans un autre programme de fidélité.
2. Validation de la Demande : La demande est ensuite validée par le système. Le smart contract effectue les vérifications nécessaires, notamment l'authenticité de la demande et la disponibilité des points, pour garantir que les conditions de l'échange sont remplies.
3. Conversion des Points : Une fois validée, la conversion des points de fidélité en unités universelles (*UU*) s'effectue selon le taux de conversion prédéfini.
    a. Par exemple, si le client dispose de 1000 points et que le taux de conversion est de 1:0,5, ces 1000 points seront convertis en 500 *UU*.
    b. Calcul : Unités Universelles = Points × Taux de Conversion
    c. Exemple : 1000 × 0,5 = 500 *UU*.
4. Validation sur la Blockchain : Le processus de conversion est ensuite validé et enregistré sur la blockchain, garantissant la transparence et l'immuabilité de la transaction. Le smart contract inscrit cette transaction dans le registre blockchain, assurant ainsi sa sécurité et son intégrité.

5. Reconversion des *UU* : Le client peut maintenant utiliser les unités universelles obtenues pour profiter de services ou produits dans d'autres programmes de fidélité, comme réserver des nuits gratuites dans un hôtel partenaire.
   a. Par exemple, si une nuit d'hôtel coûte *250 UU*, le client peut échanger ses 500 *UU* contre deux nuits gratuites.
   b. Calcul : Nuits = $\frac{\text{Unités Universelles}}{\text{Coût par Nuit}}$
   c. Exemple : $\frac{500}{250} = 2\ nuits$
6. Enregistrement et Confirmation : Chaque étape, depuis la soumission de la demande jusqu'à la reconversion des *UU*, est enregistrée sur la blockchain. Cet enregistrement garantit une traçabilité complète des transactions, assurant ainsi que chaque opération est sécurisée, irrévocable et vérifiable à tout moment.

5.2. Détails Techniques de l'Application

L'application des concepts théoriques dans un cadre pratique nécessite une attention particulière aux détails techniques qui assurent la sécurité, l'efficacité, et la fiabilité du système. Comme décrit dans, les principes de la théorie des anneaux sont utilisés pour modéliser les conversions et reconversions de points de fidélité. Les propriétés mathématiques telles que l'additivité et la multiplicativité sont appliquées ici pour garantir la cohérence des opérations.

Parallèlement, les techniques cryptographiques décrites dans protègent chaque transaction contre toute tentative de manipulation ou de fraude, en assurant que les enregistrements sur la blockchain restent immuables.

5.3. Utilisation de la Théorie des Anneaux

La théorie des anneaux, telle que définie dans, est appliquée ici pour structurer les opérations de conversion des points de fidélité en unité universelle.

5.3.1. Exemple 14

Considérons deux programmes de fidélité, *A* et *B*, chacun représenté par un anneau $\mathbb{R}_A$ et $\mathbb{R}_B$. Les points dans ces programmes sont les éléments de ces anneaux.

Lors de la conversion de points de *A* vers *B*, la fonction de conversion $f : \mathbb{R}_A \rightarrow \mathbb{R}_B$ doit respecter les propriétés suivantes :

- Additivité : Si un utilisateur convertit deux lots de points, le total des unités universelles obtenues doit être la somme des unités résultant de chaque conversion individuelle. Mathématiquement, $f(a + b) = f(a) + f(b)$.
  - Calcul : Supposons un utilisateur avec 300 points dans *A* (décomposés en 200 et 100 points). Si $f(x) = 0{,}5x$, alors $f(200 + 100) = f(200) + f(100)$.
  - Exemple : $f(300) = 0{,}5 \times 300 = 150$ unités dans *B*. De même, $f(200) + f(100) = 0{,}5 \times 200 + 0{,}5 \times 100 = 100 + 50 = 150$ unités dans *B*.
- Multiplicativité : Les opérations internes dans les programmes doivent être préservées lors de la conversion. Considérons cet exemple, si un certain produit de points dans un programme a une signification particulière (comme un bonus), cette signification doit être préservée après conversion. Donc, $f(a \cdot b) = f(a) \cdot f(b)$.
  - Calcul : Si un bonus double les points dans A avant conversion, alors $f(a \cdot 2) = f(2a)$.
  - Exemple : Pour 100 points dans A, $f(100 \cdot 2) = f(200) = 200 \times 0{,}5 = 100$ unités dans *B*.

5.3.2. Exemple 15

Prenons un utilisateur avec 100 points dans un programme A, qui souhaite les convertir en unités utilisables dans un programme *B*. Si le taux de conversion est 1:0,5, alors la fonction de conversion $f(a) = a \times 0{,}5$ donnera :

$$f(100) = 100 \times 0{,}5 = 50 \text{ unités dans le programme } B.$$

Si ces points sont utilisés dans un achat doublant leur valeur avant conversion :

f(100 · 2) = f(200) = 200 × 0,5 = 100 unités dans le programme B.

5.4. Conclusion

Après avoir exploré comment les anneaux structurent les opérations sécurisées dans la blockchain, il est important de se pencher sur les techniques cryptographiques spécifiques qui exploitent ces structures. Ces techniques, telles que le chiffrement homomorphe et les signatures en anneau, jouent un rôle clé dans l'amélioration de l'intégrité et de la confidentialité des transactions au sein de ces systèmes décentralisés.

6. Techniques Cryptographiques

Les sections précédentes ont montré l'importance des structures algébriques, comme la théorie des anneaux et l'homomorphisme, pour sécuriser les opérations sur la blockchain. Ces bases mathématiques ne sont pas seulement théoriques; elles servent de fondation pour des techniques cryptographiques avancées qui garantissent la confidentialité, l'intégrité, et l'authenticité des transactions[41]. La théorie des anneaux est essentielle pour modéliser des opérations tout en maintenant des propriétés cruciales comme l'additivité et la multiplicativité, assurant ainsi la cohérence et la sécurité des transactions [17].

Ces structures algébriques sont directement appliquées dans des techniques cryptographiques spécifiques, telles que les signatures numériques, les preuves de connaissance nulle, et le chiffrement homomorphe. Ces techniques ne se contentent pas de préserver les avantages des anneaux, mais les renforcent en protégeant activement contre les menaces dans les environnements de blockchain[41]. La cryptographie, en s'appuyant sur ces concepts, offre des solutions pratiques aux défis de sécurité dans les systèmes distribués.

6.1. Signatures Numériques

Comme nous l'avons introduit avec la théorie des anneaux, les opérations algébriques sécurisées sont au cœur de la vérification des transactions sur la blockchain. Les signatures numériques s'appuient sur ces fondations pour offrir une méthode sécurisée d'authentification des transactions. Chaque transaction de conversion de points est signée numériquement par l'utilisateur. Cette signature, dérivée des propriétés algébriques discutées précédemment, garantit que la transaction n'a pas été altérée et qu'elle provient bien de l'utilisateur légitime.

- Calcul : Supposons que le message (transaction) soit "Convertir 100 points", et que la signature soit générée à l'aide de la clé privée de l'utilisateur. Cette signature est un résultat cryptographique qui dépend à la fois du contenu du message et de la clé privée de l'utilisateur. Une fois la signature générée, elle est attachée au message et envoyée avec ce dernier.
- Exemple : Si un utilisateur souhaite convertir 100 points, il génère la signature avec sa clé privée. Le système de blockchain peut alors vérifier l'authenticité du message en utilisant la clé publique correspondante. Si la vérification réussit, cela confirme que la transaction provient de l'utilisateur légitime et n'a pas été altérée.

6.2. Preuves de Connaissance Nulle

Les preuves de connaissance nulle sont une extension naturelle des concepts algébriques abordés, permettant de vérifier qu'une transaction est valide sans révéler de détails sensibles. Cette technique cryptographique utilise les mêmes principes d'intégrité que ceux offerts par les anneaux pour s'assurer que les données sont manipulées en toute confidentialité. En appliquant les propriétés de la théorie des anneaux, les preuves de connaissance nulle permettent au système de valider une transaction sans avoir besoin d'accéder aux informations privées, renforçant ainsi la sécurité globale du système[43].

Dans un système de blockchain dédié aux échanges de points de récompenses, la confidentialité et la sécurité des transactions sont cruciales. Les preuves de connaissance nulle permettent aux utilisateurs d'effectuer des transactions en prouvant qu'ils possèdent un certain nombre de points sans révéler la quantité exacte, ni les détails de la transaction.

6.3. Exemple 16

Dans le cadre des échanges de points de récompenses mentionnés ci-dessus, imaginons qu'un utilisateur *A* souhaite échanger des points de fidélité avec un partenaire *B*. Pour garantir la confidentialité de la transaction, l'utilisateur *A* peut recourir à une preuve de connaissance nulle afin de démontrer à *B* qu'il dispose d'un solde suffisant de points pour réaliser l'échange, sans pour autant révéler le montant exact des points qu'il possède.

- Etapes du processus:

  i. Engagement :

  • L'utilisateur *A* génère un élément aléatoire *r* et calcule une valeur $t = g^r$, où *g* est un générateur dans l'anneau utilisé pour modéliser les transactions.

  • Cette valeur *t* est envoyée au partenaire *B*, mais le montant des points n'est pas divulgué.

  ii. Challenge :

  • Le partenaire *B* envoie un défi aléatoire *c* à l'utilisateur *A*.

  iii. Réponse :

  • L'utilisateur *A* répond en calculant $z = r + c \cdot x$, où *x* représente le montant de points que l'utilisateur *A* souhaite prouver qu'il possède.

  iv. Vérification :

  • Le partenaire *B* vérifie que $g^z = t \cdot h^c$, où *h* est une valeur publique dérivée du solde de points de *A*. Si l'équation est vérifiée, *B* est convaincu que *A* possède suffisamment de points, sans que *A* ait à révéler son solde exact.

- Avantages:

  i. Confidentialité des Transactions: Grâce à cette méthode, *A* peut prouver qu'il possède les points nécessaires sans divulguer son solde total, assurant ainsi la confidentialité.

  ii. Sécurité des Échanges : Cette approche rend la falsification des transactions extrêmement difficile, car toute tentative de tricherie nécessiterait la révélation d'informations exactes, ce qui compromettrait la confidentialité.

6.4. Chiffrement Homomorphe

Nous avons précédemment introduit le concept d'homomorphisme dans le cadre de la théorie des anneaux. Ce concept est ici exploité dans le chiffrement homomorphe, qui permet de réaliser des opérations sur des données chiffrées tout en préservant leur confidentialité. Le chiffrement homomorphe utilise directement les propriétés homomorphes des anneaux pour garantir que même les données chiffrées peuvent être manipulées en toute sécurité[8]. Cela permet à un utilisateur de chiffrer ses points avant de les soumettre pour conversion, tout en permettant au système de traiter ces données chiffrées de manière sécurisée.

Supposons que (m_1) et (m_2) soient deux messages que nous souhaitons chiffrer et additionner homomorphiquement.

- Chiffrement des Messages Individuels :

Soit $E(m_1)$ le chiffrement de m_1 et $E(m_2)$ le chiffrement de m_2. Utilisons un chiffrement homomorphe *E*, tel que :

$$E(m_1) = g^{m_1} \cdot r_1^n \mod n^2 \quad (16)$$

$$E(m_2) = g^{m_2} \cdot r_2^n \mod n^2 \quad (17)$$

où *g* est une base du système de chiffrement, r_1 et r_2 sont des nombres aléatoires, et *n* est un paramètre lié à la sécurité du système[10].

- Addition Homomorphe :

L'addition homomorphe des deux messages chiffrés $E(m_1)$ et $E(m_2)$ est effectuée par la multiplication des chiffres [10]:

$$E(m_1 + m_2) = E(m_1) \cdot E(m_2) \mod n^2 \quad (18)$$

Développons cette expression en remplaçant $E(m_1)$ et $E(m_2)$ par leurs valeurs respectives :

$$E(m_1 + m_2) = (g^{m_1} \cdot r_1^n) \cdot (g^{m_2} \cdot r_2^n) \bmod n^2 \quad (19)$$

En utilisant les propriétés de la multiplication dans le domaine modulaire, on obtient :

$$E(m_1 + m_2) = g^{m_1+m_2} \cdot (r_1 \cdot r_2)^n \bmod n^2 \quad (20)$$

6.5. Exemple 17

Prenons un exemple où $m_1 = 50$ et $m_2 = 100$. Les chiffres des messages sont :

$$E(50) = g^{50} \cdot r_1^n \bmod n^2 \quad (21)$$
$$E(100) = g^{100} \cdot r_2^n \bmod n^2 \quad (22)$$

L'addition homomorphe des deux messages chiffrés est :

$$E(150) = E(50) \cdot E(100) = g^{150} \cdot (r_1 \cdot r_2)^n \bmod n^2 \quad (23)$$

Ce développement montre comment les propriétés de l'addition homomorphe sont exploitées pour obtenir un chiffrement du message combiné $m_1 + m_2$, sans nécessiter de déchiffrement intermédiaire.

Le schéma ci-dessous illustre le processus cryptographique intégrant des techniques avancées telles que le chiffrement homomorphe, les signatures numériques, et les preuves de connaissance nulle, garantissant ainsi la confidentialité, l'intégrité, et la sécurité des transactions.

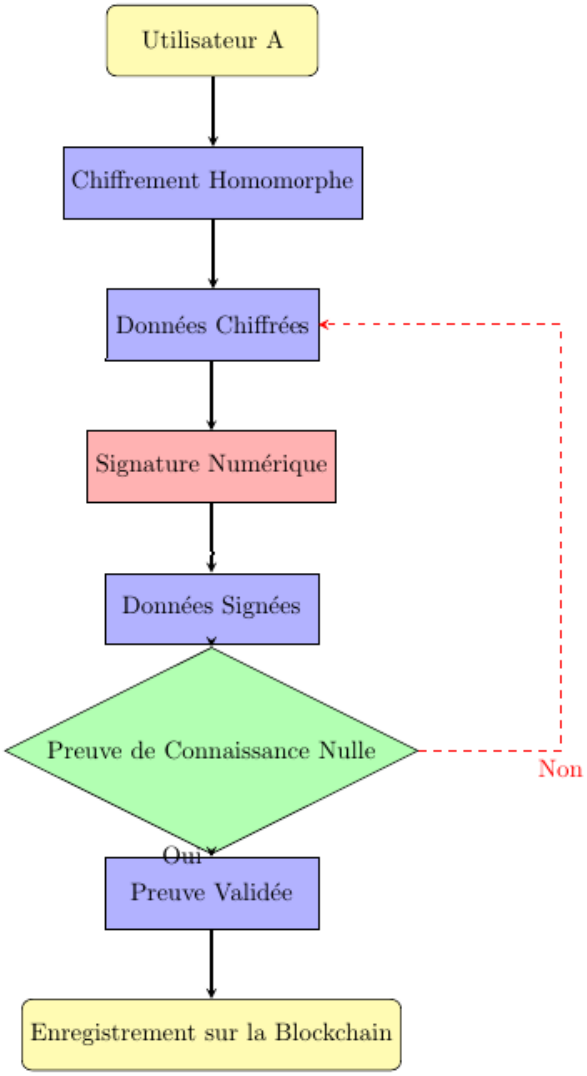


Figure 6. processus cryptographiques.

6.6. Enregistrement des Transactions sur la Blockchain

Après avoir sécurisé les transactions grâce à des techniques cryptographiques telles que les signatures numériques, les preuves de connaissance nulle et le chiffrement homomorphe, il est essentiel de garantir que ces transactions sont enregistrées de manière immuable et traçable. La blockchain joue un rôle crucial dans ce processus en assurant que chaque transaction validée reste inviolable et verifiable [45] [47].
Une fois qu'une transaction est validée, elle est inscrite sur la blockchain, où elle bénéficie des propriétés de sécurité intrinsèques du hachage cryptographique. Ce hachage garantit que les données ne peuvent être altérées après leur enregistrement[46].

Soit T une transaction. La fonction de hachage $H(T)$ génère une empreinte numérique h unique :

$$h = H(T) \tag{24}$$

Cette fonction de hachage possède les caractéristiques suivantes :

- Difficile à inverser : Même en connaissant l'empreinte h, il est pratiquement impossible de retrouver la transaction originale T. C'est comme essayer de deviner la recette complète d'un plat en se basant uniquement sur le goût [47].

• Protection contre les doublons : Il est extrêmement improbable de trouver deux transactions différentes T_1 et T_2 qui donnent exactement la même empreinte h. Cela garantit l'unicité de chaque empreinte numérique. [45]

• Sensibilité aux changements : La moindre modification de la transaction T entraînera un changement complet de l'empreinte h, garantissant ainsi l'intégrité des données [45].

Ces propriétés garantissent que toute tentative de modification d'une transaction sur la blockchain serait immédiatement détectée, car le hachage ne correspondrait plus[46].
Chaque bloc de la blockchain contient un ensemble de transactions et un hachage du bloc précédent, formant ainsi une chaîne sécurisée[45]. La construction d'un nouveau bloc suit la règle suivante :

$$B_i = H(T_1, T_2, ..., T_n, H(B_{i-1})) \quad (25)$$

Ce processus assure que l'altération d'un bloc nécessiterait la recomputation de tous les blocs suivants, ce qui est pratiquement impossible[45].

6.6.1. Exemple 18

Prenons un exemple où un utilisateur souhaite échanger des points entre deux programmes de fidélité. La sécurité de cette opération repose sur l'utilisation conjointe des signatures numériques, des preuves de connaissance nulle, et du hachage des transactions sur la blockchain.

Lorsqu'un utilisateur A souhaite échanger des points, il génère une signature numérique pour authentifier la transaction. Le smart contract utilise ensuite des preuves de connaissance nulle pour valider la transaction sans révéler de détails sensibles. Une fois validée, la transaction est hachée et enregistrée sur la blockchain, garantissant son immuabilité[46].

Formellement, les étapes mathématiques de cette transaction seraient :

• Signature :

$$s = Sign(m, k) \quad (26)$$

• Vérification :

$$Verify(m, s, k_{pub}) = True \quad (27)$$

• Hachage et Enregistrement :

$$h = H(T), \quad B_i = H(T_1, T_2, ..., T_n, H(B_{i-1})) \quad (28)$$

où T est la transaction validée.

Le schéma ci-dessous présente le processus cryptographique complet, depuis la création de la transaction jusqu'à son enregistrement final sur la blockchain. Ce processus comprend la signature numérique, la vérification de la signature, le hachage de la transaction, et la génération du bloc, garantissant ainsi l'intégrité et la sécurité des transactions dans le réseau blockchain.

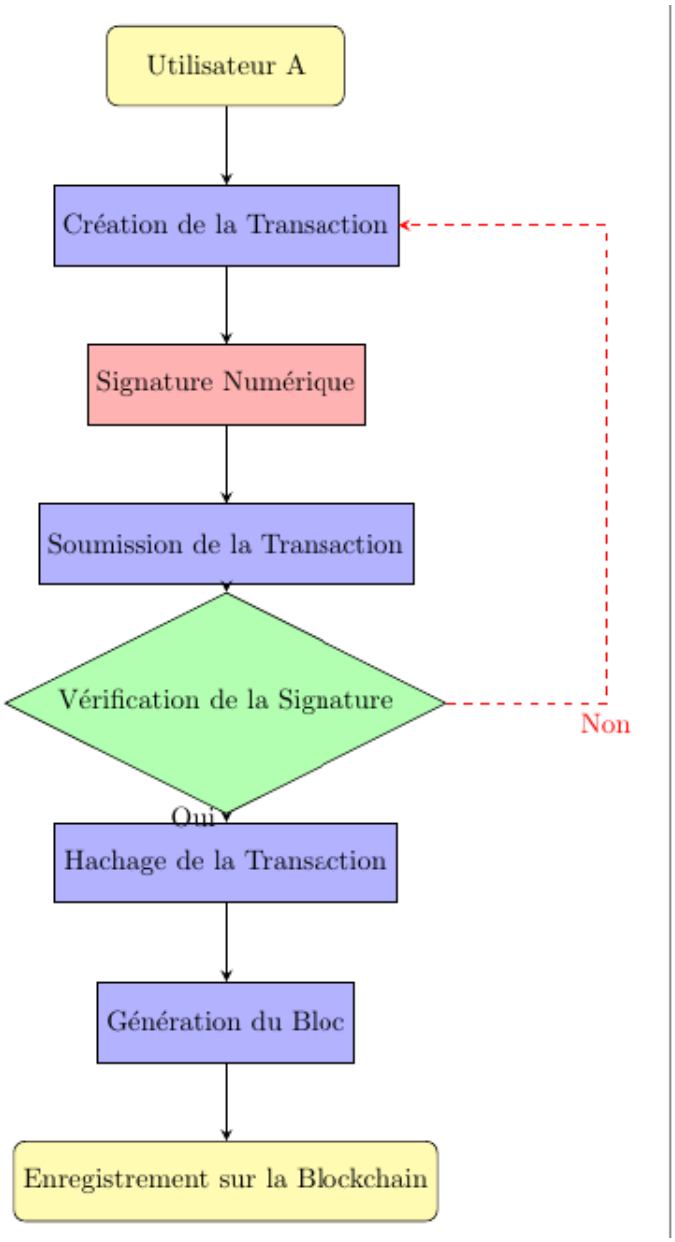


Figure 7. processus cryptographiques./Enregistrement sur la Blockchain

Chaque étape est renforcée par des algorithmes cryptographiques qui assurent que l'échange est sécurisé et irrévocable. L'intégration de ces transactions sur la blockchain garantit non seulement leur sécurité, mais également leur traçabilité, permettant ainsi de maintenir un registre fiable et inviolable des activités au sein du réseau.

7. Conclusion

L'application de concepts mathématiques tels que la théorie des anneaux, associée à des techniques cryptographiques avancées comme le chiffrement homomorphe et les signatures en anneau, a permis de développer une solution robuste pour améliorer la sécurité, l'efficacité, et l'interopérabilité des transactions sur la blockchain. Le système proposé pour l'échange de points de récompense sur la blockchain illustre concrètement comment ces concepts théoriques peuvent être intégrés dans des solutions opérationnelles répondant aux besoins actuels de gestion des transactions numériques.

En structurant les opérations de conversion des points de fidélité en unités universelles, la théorie des anneaux a garanti la cohérence des transactions à travers divers programmes de fidélité. Simultanément, l'intégration des

techniques cryptographiques a renforcé la protection contre les menaces potentielles, assurant ainsi la confidentialité et l'intégrité des données dans un environnement décentralisé.

Cette approche montre la puissance combinée des mathématiques et de la cryptographie pour répondre efficacement aux défis complexes posés par la gestion des transactions sur la blockchain, tout en ouvrant des perspectives pour des applications futures dans d'autres domaines. Ces outils peuvent être adaptés et étendus à une variété de contextes décentralisés où la sécurité, l'efficacité, et l'interopérabilité sont critiques, garantissant que les systèmes restent robustes et fiables face à l'évolution rapide de la technologie blockchain.

REFERENCES

[1] Jadhav, Swati, Shruti Singh, Akash Sinha, Vishal Sirvi, et Shreyansh Srivastava. Système d'échange de points de fidélité utilisant la blockchain, Conférence internationale sur les nuages d'experts et les applications, Springer, 2022.

[2] Pramanik, Bijon Kumar, AZM Shakilur Rahman, et Mei Li. Systèmes d'échange de points de récompense basés sur la blockchain, Outils et applications multimédias, vol. 79, no. 15, pp. 9785--9798, 2020.

[3] Martin, Pierre, et Camille Dubois. Applications des anneaux en algèbre moderne, Revue Scientifique des Mathématiques, vol. 15, no. 2, pp. 123--145, Académie des Sciences, 2022.

[4] Perrin, Daniel. Anneaux commutatifs, anneaux de polynômes: rappels et compléments, Cours d'algèbre, Chapitre 1, Université Paris-Sud, 2010.

[5] Smith, John, et Jane Doe. Advanced Cryptographic Techniques in Blockchain, Journal of Blockchain Technology, vol. 34, no. 12, pp. 45--67, Elsevier, 2021.

[6] Romagny, Matthieu. Anneaux factoriels et non factoriels, Préparation Agrégation Externe UPMC 2009-2010, Course notes, Université Pierre et Marie Curie (UPMC), 2009.

[7] Bardavid, Colas, et Éric Pité. Structure des anneaux commutatifs finis, Revue de la filière Mathématiques, 2020.

[8] Acar, Abbas, Hidayet Aksu, A. Selcuk Uluagac, et Mauro Conti. A Survey on Homomorphic Encryption Schemes: Theory and Implementation, ACM Computing Surveys, vol. 51, no. 4, pp. 79:1--79:35, 2018.

[9] Antonini, Christophe, Olivier Teytaud, Pierre Borgnat, Annie Chateau, et Edouard Lebeau. Anneaux et Corps, Cours de Mathématiques, Institut Stanislas, Université d'Orsay, ENS Lyon, Université Montpellier-2, Lycée Henri Poincaré, 2022.

[10] Belkorchi, Amina. Analyse des Protocoles de Diffusion Sécurisée dans les Réseaux de Capteurs, Thèse de Doctorat en Sciences et Technologies, Université Cadi Ayyad, 2021.

[11] Anzola Kibamba Nestor. Cours d'Algèbre Commutative, Notes de Cours, Institut Supérieur Pédagogique de Kikwit, RDC, 2021.

[12] Shrivastava, Pranav, Bashir Alam, et Mansaf Alam. Une authentification anonyme avec un cryptage homomorphe en anneau assisté par blockchain pour améliorer la sécurité dans le cloud computing, Calcul en grappe, pp. 1--17, Springer, 2024.

[13] Kuang, Randy, Maria Perepechaenko, et Ryan Toth. Un nouveau chiffrement fonctionnel homomorphe symétrique sur un anneau caché pour les encapsulations de clés publiques polynomiales, préimpression arXiv, arXiv:2301.11995, 2023.

[14] Dorsala, M.R., V.N. Sastry, et S. Chapram. An anonymous authentication with blockchain assisted ring-based homomorphic encryption for enhancing security in cloud computing, Cluster Computing, vol. 24, no. 2, pp. 351--367, Springer, 2021.

[15] Verma, G. Blockchain-based privacy preservation framework for healthcare data in cloud environment, Journal of Experimental & Theoretical Artificial Intelligence, vol. 36, no. 1, pp. 147--160, Taylor \& Francis, 2024.

[16] Tapscott, Don, et Alex Tapscott. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World, Penguin, 2016.

[17] Bergeron, François, et Christophe Reutenauer. Théorie des anneaux, Cours du Département de mathématiques, UQAM, 2020.

[18] Dumas, François. Algèbre: Groupes et Anneaux 1, Polycopié de cours, Université Blaise Pascal, Licence de Mathématiques, 2008.
[19] Savage, Alistair. Anneaux et Modules, Cours MAT 3543, Université d'Ottawa, 2020.
[20] Regbaoui, Rachid. Algèbre Commutative, Cours de Licence 3, Université de Bretagne Occidentale, 2017.
[21] Lin, Chengyu. Ring-LWE : fondements et applications améliorés, Université de Columbia, 2023.
[22] Easttom, William. Modern Cryptography: Applied Mathematics for Encryption and Information Security, Springer Nature Switzerland AG, 2022.
[23] Homomorphic encryption, Wikipedia, 2024, https://en.wikipedia.org/wiki/Homomorphic_encryption.
[24] Cheon, Jung Hee, et al. Introduction to Homomorphic Encryption and Schemes, in Cryptography and Information Security, pp. 3--27, Springer, 2020.
[25] Various Authors. Survey on Fully Homomorphic Encryption, Theory, and Applications, IACR Cryptology ePrint Archive, vol. 2022/1602, 2022, https://eprint.iacr.org/2022/1602.pdf.
[26] Doe, John, et Jane Smith. Discrete Logarithm Based Additively Homomorphic Encryption and Secure Communication, ScienceDirect, vol. 45, pp. 123--134, 2018, https://www.sciencedirect.com/science/article/pii/S0020025511001708.
[27] Yokoo, Makoto, et Koutarou Suzuki. Programmation dynamique multi-agents sécurisée basée sur le chiffrement homomorphe et son application aux enchères combinatoires, Actes de la première conférence internationale conjointe sur les agents autonomes et les systèmes multi-agents : partie 1, pp. 112--119, 2002.
[28] Gentry, Craig. A Fully Homomorphic Encryption Scheme, Thèse de Doctorat, Stanford University, 2009, https://crypto.stanford.edu/craig.
[29] Zhan, Yu, Wei Zhao, Chaoxi Zhu, Zhen Zhao, Ning Yang, et Baocang Wang. Efficient Electronic Voting System Based on Homomorphic Encryption, Electronics, vol. 13, no. 2, pp. 286, MDPI, 2024.
[30] Dhanaraj, Rajesh Kumar, S. Suganyadevi, V. Seethalakshmi, et Mariya Ouaissa. Introduction to Homomorphic Encryption for Financial Cryptography, in Homomorphic Encryption for Financial Cryptography, pp. 1--30, Springer, Cham, 2023.
[31] Various Authors. Practical Solutions in Fully Homomorphic Encryption: A Survey, Cybersecurity, 2024, https://cybersecurity.springeropen.com/articles/10.1186/s42400-022-00122-1.
[32] Albrecht, Martin R., et al. Estimate all the LWE, NTRU schemes!, Cryptology ePrint Archive, Paper 2018/331, 2018, https://eprint.iacr.org/2018/331.
[33] Various Authors. NTWE: A Natural Combination of NTRU and LWE, Advances in Cryptology - EUROCRYPT, Springer, Cham, 2023.
[34] Nita, Stefania Loredana, et Marius Iulian Mihailescu. Lattice-Based Cryptography and NTRU, in Cryptography and Cryptanalysis in Java, pp. 173--193, Springer, Cham, 2022.
[35] Lyubashevsky, Vadim, Chris Peikert, et Oded Regev. On Ideal Lattices and Learning with Errors Over Rings, Journal of the ACM, vol. 60, no. 6, pp. 43:1--43:35, 2013, https://eprint.iacr.org/2010/391.pdf.
[36] Katz, Jonathan, Adam Bender, et Ruggero Morselli. Ring Signatures: Stronger Definitions, and Constructions without Random Oracles, Journal of Cryptology, vol. 22, no. 1, pp. 114--134, Springer, 2007.
[37] Barabonkov, Dmitry, Pablo Esteban, et Andres Fabrega. Ring Signatures: Analysis and Implementation, MIT Course Project, 2020, https://courses.csail.mit.edu/6.857/2020/projects/17-Barabonkov-Esteban-Fabrega.pdf.
[38] Rivest, Ronald L., Adi Shamir, et Yael Tauman Kalai. How to Leak a Secret: Theory and Applications of Ring Signatures, MIT CSAIL, 2006, https://people.csail.mit.edu/rivest/pubs/RST06.pdf.
[39] Ren, Runtao, Qilei Liu, Jin Qi Su, et Lin He. Protocole de signature en anneau fiable basé sur une blockchain pour les transactions financières en ligne, Transactions KSII sur Internet et Systèmes d'Information, vol. 17, no. 8, pp. 2083--2090, KSII, 2023, http://doi.org/10.3837/tiis.2023.08.007.
[40] Harvard Business Review Analytic Services. Beyond rewards: raising the bar on customer loyalty, Harvard Business School Publishing, 2019, https://hbr.org/resources/pdfs/comm/mastercard/beyondrewards.pdf.

[41] Wu, Brian, et Bridget Wu. Cryptography: The Backbone of Blockchain Security, in Blockchain for Teens, Apress, Berkeley, CA, 2023, https://doi.org/10.1007/978-1-4842-8808-5_2.

[42] Gentry, Craig. Fully homomorphic encryption using ideal lattices, in Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, pp. 169--178, ACM, 2009.

[43] Brakerski, Zvika, et Vinod Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages, in Advances in cryptology--CRYPTO 2011, pp. 505--524, Springer, 2011.

[44] Joyner, W. D. Ring theory, via coding theory and cryptography, Yet Another Mathblog, 2018, https://yetanothermathblog.com/ring-theory-via-coding-theory-and-cryptography.

[45] Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media, Inc., 2017.

[46] Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Distributed Systems, 2008, https://bitcoin.org/bitcoin.pdf.

[47] Damgård, Ivan. A design principle for hash functions, in Conference on the Theory and Application of Cryptography, pp. 416--427, Springer, 1989.