

Module 11

Les cryptomonnaies et la finance numérique

Comprendre les registres, les innovations et leurs limites

Qu'est-ce qui change avec la blockchain ?

1. Qu'est-ce qu'un cryptoactif ?
2. Comment fonctionne une blockchain ?
3. Les risques des cryptoactifs
4. La finance numérique de demain

Niveau lycée – Seconde à Terminale

Cours, schémas, exercices corrigés et mini-projet

Parcours personnel d'initiation ; données fictives.

Document pédagogique, ni programme officiel ni conseil personnalisé.

Table des matières

Comment utiliser le module	2
1 Chapitre 41 – Qu’est-ce qu’un cryptoactif ?	2
1.1 Distinguer trois notions	2
1.2 Un compte bancaire n’est pas un portefeuille de clés	3
1.3 Comprendre un cours et une quantité	3
1.4 Le cas particulier des stablecoins	3
2 Chapitre 42 – Comment fonctionne une blockchain ?	4
2.1 Un registre et des copies	4
2.2 Relier les blocs et valider les règles	4
2.3 Signature et secret	4
2.4 Un exemple de registre pédagogique	5
3 Chapitre 43 – Les risques des cryptoactifs	5
3.1 Volatilité et asymétrie des pourcentages	5
3.2 Clés, accès et erreurs	6
3.3 Intermédiaires et garanties	6
3.4 Fraudes et information	6
4 Chapitre 44 – La finance numérique de demain	6
4.1 Innovation de paiement ou nouvelle monnaie ?	6
4.2 Monnaies numériques de banque centrale	6
4.3 Automatisation et données	7
4.4 Énergie, inclusion et gouvernance	7
5 Étude de cas – Comparer deux services fictifs	7
6 Exercices – Chercher avant les solutions	8
7 Quiz de compréhension	10
8 Corrigés commentés	12
9 Réponses du quiz	13
10 Mini-projet – Un registre de classe, sans argent réel	15
11 Fiche de révision	15
Sources et prolongements	16

Comment utiliser le module

Un cours pour distinguer cryptoactif, compte bancaire, registre et moyen de paiement. Les exemples sont fictifs : aucune création de compte réel, transaction ou divulgation de secret n'est nécessaire.

Objectifs

- Distinguer cryptoactif, dépôt bancaire et instrument de paiement.
- Expliquer un registre, une empreinte et une validation.
- Analyser les risques techniques, économiques et de fraude.
- Évaluer une innovation selon son usage et ses droits.

Prérequis : pourcentages, proportions, lecture de tableaux et équations simples.

Un paiement sur un téléphone, un compte bancaire et un cryptoactif peuvent tous être représentés par des chiffres sur un écran. Cette ressemblance visuelle ne signifie pas qu'ils ont le même émetteur, les mêmes garanties ou la même manière de fonctionner. Nous allons distinguer l'actif, le registre qui décrit les échanges et le service utilisé pour y accéder.

Aucun exemple de ce module ne prévoit un prix futur. Les montants sont fictifs. Les repères européens sont présentés au 30 octobre 2026 ; une règle juridique doit toujours être vérifiée dans le pays et à la date concernés. L'objectif est d'expliquer une innovation et ses limites, sans inviter à acheter un produit.

1 Chapitre 41 – Qu'est-ce qu'un cryptoactif ?

1.1 Distinguer trois notions

Définition

Un cryptoactif est une représentation numérique de valeur ou de droits reposant sur des techniques cryptographiques et un registre adapté. Le terme recouvre des projets très différents. Le mot « cryptomonnaie » est courant, mais tous ces actifs ne remplissent pas les fonctions habituelles d'une monnaie.

Une unité peut servir à transférer une valeur dans un réseau sans être acceptée pour payer un loyer ou régler une dette ordinaire. Le cours en euros dépend des échanges et des anticipations, pas d'une conversion automatiquement garantie. Un nom connu ou une hausse passée ne constitue donc pas une promesse de valeur future.

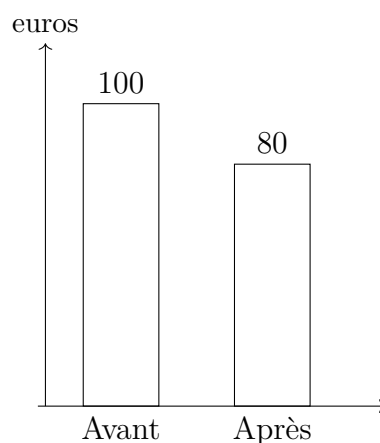
1.2 Un compte bancaire n'est pas un portefeuille de clés

Sur un compte bancaire, le client détient une créance sur un établissement. Dans une conservation personnelle de cryptoactifs, un logiciel de portefeuille sert notamment à gérer les moyens d'autoriser des opérations inscrites dans un registre. Ce n'est pas nécessairement un fichier contenant des pièces numériques détachables. Lorsque l'accès est confié à une plateforme, il faut comprendre aussi la relation avec cet intermédiaire.

1.3 Comprendre un cours et une quantité

Exemple résolu

Une unité fictive X vaut 40 €. Une quantité de 2,5 unités a une valeur affichée de $2,5 \times 40 = 100$ €, hors frais. Si le cours devient 32 €, la valeur devient 80 €, soit une perte de 20%. La quantité est inchangée ; sa valorisation en euros a baissé.



1.4 Le cas particulier des stablecoins

Un stablecoin cherche à maintenir un lien avec une référence, par exemple une monnaie. Le mécanisme peut dépendre d'actifs de réserve, de droits de remboursement et d'autres conditions. L'objectif de stabilité n'est pas une certitude : qualité et disponibilité des réserves, gestion et confiance comptent. On ne doit pas déduire du nom « stable » une garantie identique à celle d'un dépôt bancaire.

2 Chapitre 42 – Comment fonctionne une blockchain ?

2.1 Un registre et des copies

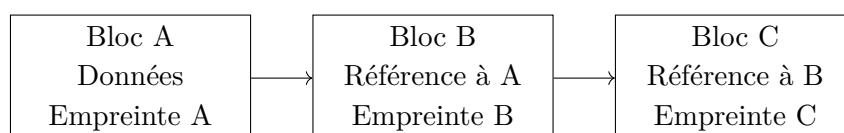
Un registre consigne des opérations selon des règles. Dans un système distribué, plusieurs participants en conservent une copie. La difficulté consiste à déterminer quel état accepter si des messages arrivent à des moments différents ou si certains participants se trompent. Partager un fichier n'est donc que le début du problème.

Définition

Une blockchain organise des informations en blocs reliés par des empreintes cryptographiques. Une empreinte est un résumé calculé à partir d'un contenu ; une modification de celui-ci conduit généralement à une empreinte différente. Ce mécanisme aide à détecter des changements, mais ne décide pas à lui seul qui a raison.

2.2 Relier les blocs et valider les règles

Chaque nouveau bloc fait référence à un état antérieur. Les participants peuvent vérifier des conditions, comme l'autorisation d'une opération et l'absence de dépense incompatible. Un mécanisme de consensus permet de s'accorder sur l'ordre ou l'état retenu. Selon le réseau, la validation et les ressources nécessaires diffèrent ; toutes les blockchains n'utilisent pas la même méthode.



Le dessin représente une liaison logique, pas le calcul réel d'une empreinte. Remplacer une ligne dans un ancien bloc modifie les vérifications qui en dépendent. Les conséquences pratiques dépendent ensuite des règles de consensus et de la puissance ou des droits des participants.

2.3 Signature et secret

Une signature numérique sert à vérifier qu'une opération a été autorisée avec une clé appropriée. La clé privée doit rester secrète ; les informations publiques permettent la vérification. Une signature valide ne prouve pas que la personne a compris les conséquences de l'opération, ni qu'un vendeur livrera un bien. La sécurité technique et la qualité de la décision sont deux sujets différents.

2.4 Un exemple de registre pédagogique

Exemple résolu

Au départ, Alice possède 10 unités et Bilal 4. Une opération autorisée transfère 3 unités d’Alice à Bilal : les soldes deviennent 7 et 7. Le total reste 14. Une deuxième opération voulant dépenser 8 unités depuis le solde d’Alice doit être refusée dans ce modèle. Aucun code réel ni clé secrète n’est nécessaire pour cet exercice papier.

Un registre peut contrôler la cohérence interne sans certifier les faits extérieurs. Si une personne y inscrit qu’un colis a été livré, la présence de cette inscription ne rend pas la livraison vraie. Ce problème explique l’importance des sources d’information et des responsabilités autour du système.

3 Chapitre 43 – Les risques des cryptoactifs

3.1 Volatilité et asymétrie des pourcentages

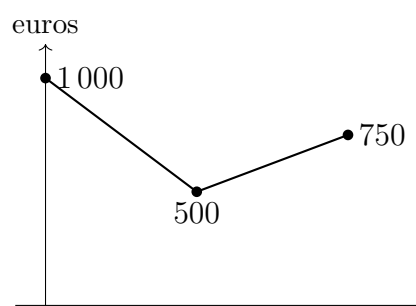
Une baisse et une hausse de même pourcentage ne s’annulent pas, car elles s’appliquent à des bases différentes. La volatilité décrit l’ampleur des variations, mais ne résume pas tous les risques. Le risque de liquidité concerne aussi la possibilité de vendre au moment souhaité et à des conditions acceptables.

Exemple résolu

Une valorisation fictive de 1 000 € baisse de 50%, puis augmente de 50% :

$$1\,000 \times 0,5 \times 1,5 = 750 \text{ €}.$$

La perte finale est de 25%. Après la première baisse, il aurait fallu une hausse de 100% pour revenir de 500 à 1 000 €.



3.2 Clés, accès et erreurs

La perte d'un secret ou d'un moyen de récupération peut empêcher d'accéder aux actifs. Une erreur d'adresse ou une autorisation mal comprise peut avoir des conséquences difficiles à annuler. Ces risques ne sont pas les mêmes qu'une simple erreur de mot de passe sur un service ordinaire. Dans un cours, on ne demande jamais de créer un portefeuille réel ou de communiquer une phrase de récupération.

3.3 Intermédiaires et garanties

Confier la conservation à un prestataire ajoute des questions : qui conserve les moyens d'accès, quels sont les frais, que se passe-t-il en cas de panne ou de défaillance ? Une autorisation réglementaire ne garantit ni le cours d'un actif ni l'absence de perte. En France et dans l'Union européenne, vérifier le statut applicable et les listes institutionnelles est une étape distincte de l'analyse économique du produit.

3.4 Fraudes et information

Une vidéo convaincante, un faux tableau de gains ou une personnalité imitée ne prouvent pas l'existence d'un placement. L'urgence, les rendements présentés comme élevés et garantis, et la demande de secrets sont des signaux d'alerte. Une vérification doit être indépendante des liens et numéros transmis dans la sollicitation. L'absence sur une liste noire ne suffit pas à établir qu'un acteur est autorisé.

4 Chapitre 44 – La finance numérique de demain

4.1 Innovation de paiement ou nouvelle monnaie ?

Une application peut rendre un paiement plus rapide sans créer une monnaie différente. Il faut identifier l'émetteur, le support, le service et les droits de l'utilisateur. Un paiement bancaire mobile peut utiliser un dépôt ordinaire ; un jeton peut relever d'une autre organisation. Le caractère numérique ne permet donc pas, à lui seul, de conclure sur les garanties.

4.2 Monnaies numériques de banque centrale

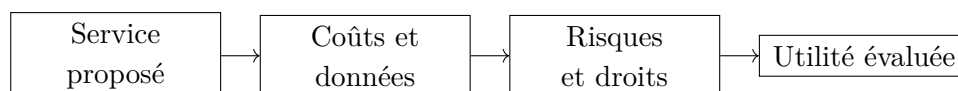
Une monnaie numérique de banque centrale désigne une forme numérique de monnaie émise par une banque centrale. Elle se distingue d'un cryptoactif privé. Les projets doivent traiter des questions d'accès, de fonctionnement hors ligne, de protection de la vie privée et de résilience. Leurs modalités et leur calendrier sont à vérifier auprès des institutions ; il ne faut pas présenter un projet comme un service déjà disponible partout.

4.3 Automatisation et données

Des programmes peuvent exécuter automatiquement certaines conditions. Cela réduit parfois des délais, mais ne supprime ni les erreurs de conception, ni les mauvaises données, ni les litiges. Une décision automatisée peut aussi reproduire des biais présents dans ses données. On examine donc les possibilités d'explication, de contrôle humain et de recours, plutôt que de supposer que l'automatisation est toujours neutre.

Exemple résolu

Un service fictif facture 0,30 € par paiement au lieu de 0,50 €. Pour 200 paiements, le coût variable passe de 100 à 60 €, soit 40 € d'écart. Mais un abonnement supplémentaire de 50 € par mois annulerait ce gain pour cet usage. L'innovation doit être évaluée par son coût complet et son utilité.



4.4 Énergie, inclusion et gouvernance

Les consommations de ressources diffèrent selon les techniques ; on évite d'attribuer une même empreinte à tous les réseaux. L'accès nécessite parfois un appareil, une connexion et des compétences. Enfin, un système distribué n'empêche pas toute concentration de pouvoir : plateformes, développeurs ou grands validateurs peuvent jouer des rôles importants. Un bilan sérieux compare les effets avec une solution de référence, sur une fonction précise.

5 Étude de cas – Comparer deux services fictifs

Une association veut collecter de petites participations, sans spéculer. Elle compare deux solutions inventées pour 100 paiements mensuels de 5 € :

	Service A	Service B
Abonnement mensuel	0	12
Frais par paiement en euros	0,25	0,08

A coûte 25 € ; B coûte $12 + 100 \times 0,08 = 20$ €. L'écart est de 5 €, mais il faut encore vérifier les délais, les conditions de remboursement, les données collectées et les personnes qui ne peuvent pas utiliser le service. Si une solution exige un actif dont le cours varie, la valeur finalement disponible peut différer du montant collecté. Le moyen technique se choisit en fonction de l'usage et des droits, pas seulement de son image de modernité.

6 Exercices – Chercher avant les solutions

Exercice 1 – Trois objets numériques

Distinguer une application bancaire, un dépôt bancaire et un cryptoactif en quatre phrases.

Exercice 2 – Valeur affichée

Une unité fictive vaut 24 €. Calculer la valeur de 3,5 unités, puis leur valeur si le cours baisse à 18 €, hors frais.

Exercice 3 – Registre papier

Alice détient 12 unités et Bilal 3. Alice transfère 5 unités à Bilal. Donner les nouveaux soldes et vérifier le total.

Exercice 4 – Une dépense impossible

Dans le modèle précédent, une opération veut ensuite transférer 9 unités depuis Alice. Pourquoi doit-elle être refusée ?

Exercice 5 – Empreinte et vérité

Une inscription indique qu'un objet a été livré. Pourquoi une empreinte cryptographique correcte ne prouve-t-elle pas la livraison ?

Exercice 6 – Baisse puis hausse

Une valeur fictive de 800 € baisse de 25%, puis augmente de 25%. Calculer la valeur finale et la perte globale.

Exercice 7 – Retrouver le départ

Après une baisse de 20%, quelle hausse permet de retrouver le niveau initial ?

Exercice 8 – Coût d'un service

A coûte 0,40 € par paiement. B coûte 10 € par mois puis 0,15 € par paiement. Comparer pour 100 paiements mensuels.

Exercice 9 – Décider sans publicité

Une plateforme affiche « réglementée, donc sans risque ». Proposer une réponse argumentée.

Exercice 10 – Un projet de collecte

Une association attend 500 €. Une solution facture 20 € de frais mais convertit ensuite la somme dans un actif qui baisse de 10%. Quelle valeur reste-t-il, si les frais sont prélevés avant la baisse ?

Exercice 11 – Recherche institutionnelle

Consulter une source officielle sur une monnaie numérique de banque centrale. Relever sa date et distinguer objectifs annoncés, décisions prises et points encore étudiés.

Exercice 12 – Oral critique

Discuter en trois minutes : « Une blockchain remplace toujours la confiance. »

7 Quiz de compréhension

Une réponse par question. Justifier avant de consulter le corrigé.

1. Un paiement numérique implique une nouvelle monnaie...
 - a) Toujours
 - b) Pas nécessairement
 - c) Uniquement pour de petits montants
2. La valeur en euros d'une quantité fixe dépend...
 - a) Du cours de l'unité
 - b) Du seul nom du portefeuille
 - c) Uniquement du délai de connexion
3. Une empreinte sert notamment à...
 - a) Détecter une modification du contenu
 - b) Garantir un bénéfice
 - c) Créer un emploi automatiquement
4. Un mécanisme de consensus traite notamment...
 - a) L'accord sur l'état retenu du registre
 - b) Le choix d'un taux de TVA
 - c) La suppression de toute règle
5. Une clé privée doit être...
 - a) Publiée pour recevoir un cours
 - b) Conservée secrète
 - c) Envoyée au professeur
6. Une baisse de 50 % puis une hausse de 50 % donne...
 - a) Le niveau initial
 - b) 75 % du niveau initial
 - c) 150 % du niveau initial
7. Le mot stablecoin garantit une valeur constante...
 - a) Oui
 - b) Non

- c) Seulement si le logo est connu
8. Une autorisation réglementaire garantit le capital. . .
- a) Oui
 - b) Non
 - c) Uniquement pour une application mobile
9. Une donnée extérieure fausse peut être inscrite dans un registre. . .
- a) Oui
 - b) Non
 - c) Jamais si elle contient un nombre
10. Pour évaluer une innovation, il faut examiner. . .
- a) Seulement son nom
 - b) Usage, coûts, risques et droits
 - c) Seulement ses abonnés

8 Corrigés commentés

Exercice 1 – Trois objets numériques

L'application est une interface ou un service. Le dépôt est une créance du client sur la banque. Un cryptoactif relève de droits et de règles propres à un réseau ou un émetteur. Une représentation numérique commune ne leur donne pas les mêmes garanties.

Exercice 2 – Valeur affichée

Avant : $3,5 \times 24 = 84$ €. Après : $3,5 \times 18 = 63$ €. La perte est de 21 €, soit 25% ; la quantité reste 3,5.

Exercice 3 – Registre papier

Alice possède $12 - 5 = 7$ et Bilal $3 + 5 = 8$. Le total est $7 + 8 = 15$, égal au total initial $12 + 3$.

Exercice 4 – Une dépense impossible

Alice ne détient que 7 unités dans l'état actuel. L'opération dépasse ce solde. Les règles de validité doivent vérifier l'état précédent, pas seulement la présence d'une ligne dans un fichier.

Exercice 5 – Empreinte et vérité

L'empreinte aide à contrôler l'intégrité du contenu. Elle n'observe pas le monde extérieur. Une information fausse peut être inscrite correctement : il faut vérifier la source et les responsabilités.

Exercice 6 – Baisse puis hausse

$800 \times 0,75 = 600$ €, puis $600 \times 1,25 = 750$ €. Perte : 50 €, soit 6,25% du départ.

Exercice 7 – Retrouver le départ

La valeur vaut 0,8 fois celle du départ. Il faut un facteur $1/0,8 = 1,25$, soit une hausse de 25%, et non 20%.

Exercice 8 – Coût d'un service

A : $100 \times 0,40 = 40$ €. B : $10 + 100 \times 0,15 = 25$ €. B est moins cher de 15 € pour cet usage, avant comparaison des autres conditions.

Exercice 9 – Décider sans publicité

L'autorisation concerne une activité et un cadre précis. Elle ne garantit pas le cours d'un actif, ni l'absence de perte ou de fraude par usurpation. Il faut vérifier l'identité, le statut exact et les caractéristiques du produit via une source indépendante.

Exercice 10 – Un projet de collecte

Après frais : $500 - 20 = 480$ €. Après baisse : $480 \times 0,90 = 432$ €. Le coût apparent des paiements ne suffit donc pas à comparer les valeurs disponibles finales.

Exercice 11 – Recherche institutionnelle

La réponse dépend du projet et de la date. Elle doit citer l'institution, identifier des objectifs et ne pas transformer une possibilité en disponibilité certaine. L'existence d'un projet ne signifie ni lancement universel ni usage obligatoire.

Exercice 12 – Oral critique

Elle peut réduire certains besoins de confiance dans la tenue du registre sous des hypothèses précises. Il reste des choix de protocole, des intermédiaires, des sources de données et des risques d'accès. Donner un exemple d'information extérieure que le registre ne vérifie pas seul.

9 Réponses du quiz

1. b). Une application peut transférer un dépôt bancaire ordinaire.
2. a). Valeur affichée = quantité $\times$ cours, avant frais.
3. a). Elle résume un contenu ; elle ne prouve pas la vérité du monde extérieur.
4. a). Plusieurs participants doivent déterminer un état commun suivant le protocole.
5. b). Un cours ne doit jamais demander un secret réel.
6. b). $0,5 \times 1,5 = 0,75$.
7. b). L'ancrage dépend d'un mécanisme et de conditions qui peuvent échouer.

- 8. **b).** Le statut du prestataire ne supprime pas le risque du produit.
- 9. **a).** La validité technique n'établit pas à elle seule la vérité de cette donnée.
- 10. **b).** Le bilan dépend du service réellement rendu et de ses conditions.

10 Mini-projet – Un registre de classe, sans argent réel

Créer sur papier un registre de transferts entre quatre personnages fictifs, puis discuter ses capacités et ses limites.

1. Attribuer des soldes initiaux dont la somme vaut 40 unités.
2. Écrire six opérations autorisées et une tentative dépassant un solde.
3. Contrôler les soldes après chaque ligne et conserver le total.
4. Inventer un fait extérieur faux et expliquer pourquoi le registre ne le vérifie pas seul.

À rendre : Un tableau de registre, un schéma de validation et une page de limites, sans compte ni transaction réelle.

11 Fiche de révision

- L'interface numérique ne définit pas la nature juridique de l'actif.
- Quantité détenue et valeur affichée sont différentes.
- Empreinte, signature et consensus ont des fonctions distinctes.
- Un registre cohérent ne certifie pas tous les faits extérieurs.
- La diversification des techniques ne supprime pas les risques de perte.
- Une innovation se juge selon son usage, son coût, ses droits et ses effets.

Les mots à maîtriser

Cryptoactif Représentation numérique de valeur ou de droits reposant sur des techniques cryptographiques et un registre.

Blockchain Registre organisant des informations en blocs liés par des empreintes.

Empreinte Résumé calculé à partir d'un contenu pour aider à en vérifier l'intégrité.

Consensus Mécanisme par lequel les participants s'accordent sur un état suivant des règles.

Clé privée Secret permettant notamment d'autoriser des opérations par signature.

Stablecoin Cryptoactif cherchant à maintenir un lien avec une référence selon un mécanisme déterminé.

Volatilité Ampleur des fluctuations de valeur sur une période.

Liquidité Possibilité d'obtenir de l'argent rapidement et à des conditions acceptables en cédant un actif.

Sources et prolongements

Ressources institutionnelles consultées le 30 octobre 2026. Les chiffres sont fictifs. Les règles dépendent du pays et de leur date.

- Banque de France — Crypto-actifs et stablecoins
Consulter la ressource officielle
- AMF — Investir en crypto-actifs : précautions pratiques
Consulter la ressource officielle
- AMF — Investir dans le bitcoin : prudence
Consulter la ressource officielle
- BCE — Questions fréquentes sur l’euro numérique
Consulter la ressource officielle