DOSSIER DE RÉFÉRENCE · TECHNOLOGIE

La blockchain, expliquée *pour de bon*

Tout le monde en parle, presque personne ne sait dire ce que c'est. Ce dossier ne vend rien et n'attaque rien : c'est le document de référence de la série, du néophyte à l'expert. Ce que c'est, comment ça marche vraiment (blocs, minage, clés, contrats), ce qui tourne aujourd'hui, ce qui a échoué, et les limites que les brochures ne mentionnent jamais. À lire une fois, à garder pour toujours.

SOMMAIRE

01 Pourquoi ce dossier, et comment le lire

02 C'est quoi, une blockchain ? Le cahier de comptes du village

03 Niveau 1 · Les blocs et la chaîne : l'empreinte qui scelle tout

04 Niveau 2 · Le consensus : comment des inconnus se mettent d'accord

05 Niveau 3 · Clés, adresses, portefeuilles : posséder sans banque

06 Niveau 4 · Les smart contracts : quand le registre devient programmable

07 Ce qui tourne vraiment en 2026

08 Ce qui a été essayé, et abandonné

09 Les limites honnêtes : trilemme, énergie, oracles

10 Ce que j'en retiens · Annexes : chiffres-clés, glossaire, sources

Rédigé par Stéphane Baron, sous la supervision de Bernard Prats-Desclaux. Dossier de référence pédagogique, juillet 2026, sources publiques croisées (annexe C). Ceci n'est pas un conseil en investissement. Les chiffres cités sont datés et vérifiables.

1 Pourquoi ce dossier, et comment le lire

MODE D'EMPLOI — UN SOCLE, PAS UNE OPINION

2008	31 Md$	−99,95 %	≈ 65 %
NAISSANCE DU CONCEPT (NAKAMOTO, 31 OCT.)	D'ACTIFS RÉELS TOKENISÉS, JUILLET 2026	D'ÉNERGIE POUR ETHEREUM DEPUIS LE MERGE (2022)	DE LA VALEUR TOKENISÉE HÉBERGE SUR ETHEREUM

Les dossiers n°04 et dossier technique n°10 ont traité le bitcoin en tant qu'actif : sa sensibilité à la liquidité, puis son absence d'usage monétaire. Restait à expliquer la machine qui se trouve dessous, parce qu'on ne peut pas se faire une opinion sérieuse sur les crypto-actifs, la tokenisation ou les promesses « blockchain » d'un prospectus sans comprendre ce que le mot recouvre. Ce dossier est différent des précédents : pas de thèse à défendre, pas de produit à démonter. Un document de référence, à lire une fois en entier, puis à garder sous le coude.

Il est construit en niveaux, du plus simple au plus technique : la section 2 suffit pour ne plus jamais hocher la tête dans le vide en réunion ; les sections 3 à 6 donnent la mécanique réelle, sans mathématiques ; les sections 7 à 9 font l'état des lieux 2026, réussites, échecs et limites. Le glossaire final reprend tous les termes. Lisez jusqu'où votre curiosité vous porte : chaque niveau se suffit.

2 C'est quoi, une blockchain ? Le cahier de comptes du village

VULGARISATION — L'IDÉE EN UNE IMAGE

Imaginez un village sans banque. Pour se prêter et se payer, les habitants tiennent un grand cahier de comptes sur la place publique : « Paul doit 50 à Marie », « Jacques a payé 20 à Louise ». Tout le monde peut le lire, tout le monde peut vérifier. Problème évident : qui tient le stylo ? Si c'est Paul, il peut effacer ses dettes. Si c'est le maire, il faut lui faire confiance, et on a réinventé la banque.

La blockchain est la réponse à ce problème précis : **comment tenir un registre commun sans confier le stylo à personne**. La solution combine trois idées. Un : chaque habitant garde sa propre copie complète du cahier, en permanence synchronisée avec les autres ; falsifier une copie ne sert à rien, il faudrait les falsifier presque toutes, en même temps. Deux : les pages du cahier (les « blocs ») sont scellées les unes aux autres par un procédé cryptographique qui rend toute retouche d'une vieille page immédiatement visible. Trois : pour écrire une nouvelle page, les habitants suivent une procédure d'accord collectif (le « consensus ») qui ne suppose la confiance en personne en particulier.

Voilà l'objet, tout entier : **un registre public, répliqué, infalsifiable a posteriori, et tenu sans autorité centrale**. Tout le reste (bitcoin, ethereum, tokens, NFT, smart contracts) est construit par-dessus. Et une remarque qui économise bien des confusions : la blockchain n'est pas « le bitcoin ». Le bitcoin est la première application du procédé, comme le courrier électronique fut la première application d'internet.

> LA QUESTION QUI REMET LES IDÉES EN PLACE
>
> *Avant de s'émerveiller ou de ricaner devant un projet « blockchain », poser une seule question : y a-t-il, dans ce cas d'usage, un problème de confiance entre des acteurs qui ne peuvent ou ne veulent pas se fier à un intermédiaire central ? Si oui, l'outil a un sens. Si non, une base de données classique fera la même chose, en mille fois plus rapide et moins cher. Cette question unique explique à la fois les succès de la section 7 et le cimetière de la section 8.*

3 Niveau 1 · Les blocs et la chaîne : l'empreinte qui scelle tout

MÉCANIQUE — LE HACHAGE, OU LA CIRE À CACHETER NUMÉRIQUE

Le socle technique de tout l'édifice tient en un outil : la **fonction de hachage**. C'est un procédé mathématique qui transforme n'importe quel document en une empreinte courte, une suite de 64 caractères. Trois propriétés en font une merveille : le même document donne toujours la même empreinte ; changer une seule virgule du document change l'empreinte du tout au tout ; et il est impossible de fabriquer un document qui produirait une empreinte choisie d'avance. C'est l'empreinte digitale des données : elle identifie sans révéler, et elle trahit la moindre retouche.

La chaîne de blocs utilise cette empreinte comme cire à cacheter. Un bloc, c'est une page du cahier : un paquet de transactions, plus deux éléments décisifs. D'abord **l'empreinte du bloc précédent**, gravée dans le bloc courant : c'est le chaînage. Ensuite l'horodatage et quelques données techniques. Conséquence de ce chaînage : si un fraudeur retouche une transaction dans le bloc n°800 000, l'empreinte de ce bloc change ; or elle est gravée dans le bloc n°800 001, qui devient invalide, ce qui invalide le n°800 002, et ainsi de suite jusqu'au bout. Pour réécrire une ligne d'histoire, il faut réécrire toute l'histoire qui suit, sur la majorité des copies du réseau, plus vite que le réseau n'écrit de nouvelles pages. C'est ça, « infalsifiable » : pas impossible en théorie, mais économiquement absurde en pratique.

4 Niveau 2 · Le consensus : comment des inconnus se mettent d'accord

MÉCANIQUE — PREUVE DE TRAVAIL, PREUVE D'ENJEU

Reste la vraie difficulté, celle qui a résisté aux informaticiens pendant trente ans : qui a le droit d'écrire la page suivante, et comment empêcher un tricheur de proposer deux versions contradictoires (payer deux fois avec le même argent, la « double dépense ») ? Les blockchains publiques ont deux grandes réponses.

La preuve de travail (bitcoin) : payer l'écriture en électricité

Pour gagner le droit d'écrire un bloc, les « mineurs » font tourner des machines qui tentent des milliards de combinaisons par seconde sur un casse-tête cryptographique. Le premier qui trouve publie son bloc, les autres vérifient en une fraction de seconde (trouver est dur, vérifier est facile), et le gagnant empoche la récompense : des bitcoins neufs, plus les frais des transactions incluses. L'astuce économique est profonde : écrire coûte cher (matériel, électricité), donc tricher coûte cher. Pour imposer une fausse histoire, il faudrait durablement dépenser plus d'électricité que le reste du monde réuni (l'« attaque des 51 % »). La sécurité du registre est achetée en énergie : de l'ordre de 150 à 180 TWh par an pour le bitcoin selon les estimations de Cambridge, la consommation d'un pays comme la Pologne. C'est le prix, réel et assumé, de la confiance sans autorité.

La preuve d'enjeu (ethereum) : payer en caution

Deuxième méthode, adoptée par Ethereum lors du « Merge » du 15 septembre 2022 : remplacer la dépense d'électricité par une caution. Les « validateurs » déposent 32 ETH sous séquestre ; le protocole en tire un au sort pour écrire le bloc suivant, les autres attestent. Un validateur honnête gagne un intérêt ; un tricheur voit sa caution détruite (« slashing »). Résultat : une consommation électrique réduite de 99,95 %, contre une critique récurrente, la concentration (les gros détenteurs valident davantage et s'enrichissent en validant). Aucune des deux méthodes n'est « la bonne » : la preuve de travail achète la sécurité en énergie, la preuve d'enjeu l'achète en capital immobilisé. Deux polices d'assurance, deux primes.

5 Niveau 3 · Clés, adresses, portefeuilles : posséder sans banque

MÉCANIQUE — LA SIGNATURE QUI REMPLACE LE GUICHET

Dernière brique du socle : comment prouver que c'est bien vous, sans carte d'identité ni banquier ? Par la **cryptographie à clé publique**, un outil des années 1970 que la blockchain recycle brillamment. Chaque utilisateur possède un couple de clés mathématiquement liées : une **clé privée**, secrète, un très grand nombre tiré au hasard ; et une **clé publique**, dérivée de la première, qu'on peut montrer à tout le monde (l'« adresse » en est une version compacte). La magie : ce que la clé privée signe, la clé publique le vérifie, mais connaître la clé publique ne permet pas de retrouver la privée.

Une transaction est donc un message signé : « moi, détenteur de la clé privée de l'adresse A, transfère 0,5 unité à l'adresse B ». Le réseau vérifie la signature avec la clé publique, sans jamais voir le secret. Pas de mot de passe, pas de guichet, pas de recours. Le « portefeuille » (wallet) n'est qu'un logiciel qui garde vos clés : sur votre téléphone, sur une clé USB durcie (« hardware wallet »), ou chez un intermédiaire (une plateforme d'échange), auquel cas, notez-le bien, c'est lui qui détient les clés, et

vous ne détenez qu'une promesse. Les clients de FTX l'ont appris en novembre 2022 : « not your keys, not your coins » n'est pas un slogan, c'est du droit des faillites.

6 Niveau 4 · Les smart contracts : le registre devient programmable

MÉCANIQUE — DES PROGRAMMES QUI TIENNENT LA CAISSE

Jusqu'ici, le registre n'enregistre que des transferts : A paie B. L'apport d'Ethereum (lancé en 2015 par Vitalik Buterin, alors âgé de 21 ans) est d'avoir rendu le registre **programmable** : on peut y déposer non seulement des écritures, mais des programmes, les « smart contracts », qui s'exécutent d'eux-mêmes quand leurs conditions sont réunies. Un smart contract est un automate de caisse incorruptible : « si je reçois 100 jetons X avant le 31 décembre, je verse 105 jetons Y à l'expéditeur ; sinon je rembourse ». Une fois déployé, personne ne peut l'empêcher de s'exécuter, pas même son auteur.

C'est la brique qui a tout engendré : les **tokens** (jetons créés par simple contrat, dont les stablecoins, plus de 200 Md$ d'encours, l'usage crypto le plus réel à ce jour) ; la **DeFi** (des échanges, prêts et emprunts entièrement automatisés, sans établissement financier) ; les **NFT** (des jetons uniques attachés à un objet, dont la bulle 2021-2022 a surtout prouvé qu'un certificat d'authenticité ne vaut que ce que vaut l'objet) ; et la **tokenisation** d'actifs réels, dont on reparle à la section suivante. Deux réserves d'expert à garder en tête : un smart contract vaut ce que vaut son code (les piratages de contrats bogués se chiffrent en milliards par an, 3,4 Md$ de fonds volés en 2025 selon Chainalysis), et il ne connaît que sa blockchain : dès qu'il a besoin d'une information du monde réel, il dépend d'un « oracle », on y revient en section 9.

7 Ce qui tourne vraiment en 2026

ÉTAT DES LIEUX — LE TRI ENTRE LE RÉEL ET LA PLAQUETTE

Dix-sept ans après Nakamoto, le bilan honnête tient en quatre usages effectifs :

USAGE	ORDRE DE GRANDEUR (2026)	APPRÉCIATION
Crypto-actifs (bitcoin, ether…)	Milliers de Md$ de capitalisation	L'usage dominant : spéculation et détention (cf. dossiers n°04 et dossier technique n°10)
Stablecoins (paiement, transferts)	> 200 Md$ d'encours	L'usage de paiement réel : transferts internationaux, pays à monnaie faible ; aussi 84 % des flux illicites (Chainalysis)
Tokenisation d'actifs réels	31 Md$ (juil. 2026, +400 % en 18 mois)	En croissance rapide : fonds monétaires tokenisés (Circle USYC ≈ 3 Md$, BlackRock BUIDL ≈ 2,5 Md$), pilote DTCC en cours
Infrastructure et niches	Difficile à chiffrer	Horodatage, notarisation, registres de niche : réel mais modeste

Tableau 1 : les usages effectifs. Environ 65 % de la valeur tokenisée réside sur Ethereum. Sources : annexe C.

La tokenisation mérite un mot de plus, car c'est le dossier que la finance traditionnelle prend au sérieux : représenter sur une blockchain des actifs classiques (parts de fonds monétaires, obligations, immobilier) pour les échanger et les régler en continu, sans les délais de règlement-livraison actuels. 31 Md$ en juillet 2026, en hausse de plus de 400 % depuis début 2025, portés par BlackRock, Circle et le

pilote de règlement du DTCC attendu au second semestre. C'est petit à l'échelle de la finance mondiale (un dix-millième, à la louche), mais c'est la première fois qu'un usage blockchain croît par l'adoption d'institutions réglementées plutôt que par la spéculation. À suivre sérieusement, sans s'enflammer : on notera que l'actif tokenisé vedette est… le bon du Trésor américain. La révolution décentralisée sert pour l'instant à mieux distribuer la dette de l'État le plus central du monde. L'ironie est savoureuse.

8 Ce qui a été essayé, et abandonné

LE CIMETIÈRE — INSTRUCTIF COMME TOUS LES CIMETIÈRES

Entre 2016 et 2020, la blockchain fut promise à tout : supply chain, santé, vote, état civil, luxe, agroalimentaire. Le reflux a été discret mais massif. Trois pierres tombales valent la visite :

— **TradeLens (Maersk + IBM), 2018-2023.** LA vitrine de la « blockchain d'entreprise » : digitaliser le commerce maritime mondial. Plateforme techniquement aboutie, arrêtée en novembre 2022 (hors ligne au premier trimestre 2023), faute de « viabilité commerciale » : les concurrents de Maersk n'ont jamais voulu monter dans un système contrôlé par Maersk. La leçon est limpide : le problème n'était pas technique, il était de gouvernance, et la blockchain ne résout pas la méfiance entre concurrents quand l'un d'eux tient la plateforme.

— **Libra/Diem (Facebook/Meta), 2019-2022.** La monnaie privée mondiale annoncée en juin 2019 par un consortium mené par Facebook. Deux ans et demi de bras de fer avec les banques centrales et les parlements, un changement de nom, puis liquidation en janvier 2022, actifs vendus 182 M$ à Silvergate (banque elle-même disparue en 2023). Leçon : la monnaie est une prérogative politique ; aucune technologie n'y change rien.

— **Les consortiums « blockchain sans token ».** Des dizaines de projets bancaires et industriels (registres interbancaires, traçabilité) repliés en silence vers des bases de données classiques. La formule qui résume dix ans d'expérimentations : une blockchain privée entre acteurs qui se font déjà confiance n'est qu'une base de données lente et chère. Sans problème de confiance à résoudre, l'outil n'apporte que ses inconvénients.

9 Les limites honnêtes : trilemme, énergie, oracles

EXPERTISE — CE QUE LES BROCHURES NE DISENT JAMAIS

— **Le trilemme.** Une blockchain court après trois qualités : décentralisation, sécurité, débit. On n'en obtient jamais que deux. Bitcoin a choisi décentralisation et sécurité : 7 transactions par seconde. Les chaînes « rapides » sacrifient de la décentralisation (poignée de validateurs) ou de la sécurité. Toute promesse d'une blockchain « aussi décentralisée que bitcoin et aussi rapide que Visa » viole une loi de conception connue : c'est un signal vendeur, pas une prouesse.

— **L'énergie (preuve de travail).** 150 à 180 TWh/an pour le bitcoin. Qu'on juge ce prix justifié ou scandaleux, il est structurel : c'est l'énergie qui fait la sécurité. La preuve d'enjeu l'a réglé pour Ethereum (−99,95 %), au prix d'un autre compromis (concentration du capital validant).

— **Le problème de l'oracle.** Le registre est infalsifiable, mais aveugle : il ne sait rien du monde extérieur. Dès qu'un contrat dépend d'un fait réel (« le conteneur est arrivé », « le blé vaut 230 € »), quelqu'un doit l'écrire dans la chaîne, et ce quelqu'un peut mentir ou se tromper. La confiance chassée par la porte revient par la fenêtre. C'est LA limite conceptuelle de toutes les applications «

monde réel », traçabilité en tête : la blockchain garantit que la donnée n'a pas changé depuis son écriture, jamais qu'elle était vraie en entrant.

- **L'irréversibilité, dans les deux sens.** Pas d'annulation frauduleuse, mais pas non plus de recours en cas d'erreur, de vol de clé ou de contrat bogué (3,4 Md$ volés en 2025). L'infalsifiable protège aussi le voleur.
- **La gouvernance humaine.** Le code est neutre, ses développeurs et ses mineurs non. Les guerres de protocole (hard forks) ont montré qu'en cas de crise, ce sont des humains, réunis autour d'intérêts, qui décident quelle version de la « vérité infalsifiable » survit.

10 Ce que j'en retiens

La blockchain est une vraie invention : le premier procédé de l'histoire permettant à des inconnus de tenir un registre commun sans arbitre. Ce n'est ni une révolution universelle ni une escroquerie, c'est un outil à domaine de validité étroit : il vaut son coût là où la confiance manque et où aucun intermédiaire n'est acceptable, et il le vaut nulle part ailleurs. Dix-sept ans de terrain le confirment : les usages qui tiennent (actifs numériques, stablecoins, début de tokenisation) sont tous financiers, là où la valeur EST une écriture de registre ; les usages abandonnés voulaient enregistrer le monde physique, et le monde physique ne rentre pas dans un hachage. Pour l'investisseur, une grille tient dans une poche : devant tout projet « blockchain », chercher le problème de confiance. S'il n'y en a pas, il n'y a pas de projet, il y a un mot à la mode. Et relire la section 8 : le cimetière est le meilleur professeur.

A Annexe · Chiffres-clés

DONNÉE	VALEUR	SOURCE / DATE
Publication du document fondateur (Nakamoto)	**31 octobre 2008**	bitcoin.org
Lancement d'Ethereum (registre programmable)	**30 juillet 2015**	ethereum.org
Débit du réseau bitcoin	**≈ 7 transactions/seconde**	Caractéristique du protocole
Consommation électrique du bitcoin (preuve de travail)	**≈ 150-180 TWh/an**	Cambridge (CCAF), estimations 2025-2026
Le « Merge » d'Ethereum (passage à la preuve d'enjeu)	**15 septembre 2022, −99,95 % d'énergie**	Ethereum Foundation
Caution d'un validateur Ethereum	**32 ETH**	Protocole Ethereum
Encours des stablecoins	**> 200 Md$**	Données de place, 2026
Actifs réels tokenisés sur blockchains publiques	**31 Md$ (+400 % depuis début 2025)**	Relevés sectoriels, juillet 2026
Plus grands fonds tokenisés	**Circle USYC ≈ 3 Md$; BlackRock BUIDL ≈ 2,5 Md$**	mi-2026
Part d'Ethereum dans la valeur tokenisée	**≈ 65 %**	Relevés sectoriels, 2026
Fonds volés par piratage (contrats, plateformes)	**3,4 Md$ en 2025**	Chainalysis, Crypto Crime Report 2026
Arrêt de TradeLens (Maersk/IBM)	**Annoncé nov. 2022, hors ligne T1 2023**	Communiqué Maersk
Liquidation de Diem (ex-Libra, Meta)	**Janvier 2022, actifs cédés 182 M$**	Presse financière

B Annexe · Glossaire

Blockchain : registre de transactions public, répliqué sur de nombreux ordinateurs, organisé en blocs chaînés cryptographiquement, tenu sans autorité centrale.

Bloc : « page » du registre regroupant des transactions, l'empreinte du bloc précédent et un horodatage.

Hachage : fonction transformant toute donnée en une empreinte courte, unique en pratique et non inversible. Toute retouche de la donnée change l'empreinte.

Nœud : ordinateur du réseau conservant et vérifiant une copie du registre.

Consensus : procédure par laquelle les nœuds s'accordent sur la page suivante du registre.

Preuve de travail (PoW) : consensus du bitcoin ; le droit d'écrire s'achète en calcul (donc en électricité). Sécurité payée en énergie.

Preuve d'enjeu (PoS) : consensus d'Ethereum depuis 2022 ; le droit d'écrire s'obtient par tirage au sort parmi des validateurs ayant déposé une caution, détruite en cas de triche (« slashing »).

Minage : participation à la preuve de travail, rémunérée en unités neuves et en frais.

Attaque des 51 % : prise de contrôle de la majorité de la puissance d'écriture, seule voie théorique de falsification. Coût prohibitif sur les grandes chaînes.

Clé privée / clé publique : couple cryptographique ; la privée signe, la publique vérifie. La possession d'un actif EST la possession de la clé privée.

Portefeuille (wallet) : logiciel ou appareil conservant des clés privées. Sur une plateforme d'échange, c'est la plateforme qui détient les clés.

Smart contract : programme déposé sur la blockchain, s'exécutant automatiquement selon ses conditions, sans intervention possible une fois déployé.

Token (jeton) : unité de valeur créée par contrat sur une blockchain existante (à distinguer de la monnaie native comme l'ether).

Stablecoin : jeton conçu pour suivre une monnaie (le dollar surtout), adossé à des réserves. Principal usage de paiement crypto réel.

NFT : jeton unique et non interchangeable, attaché à un objet numérique ou physique.

DeFi : « finance décentralisée », services financiers (échange, prêt) rendus par smart contracts, sans établissement.

Tokenisation : représentation d'un actif classique (fonds, obligation, immobilier) par un jeton de blockchain, pour l'échanger et le régler en continu.

Oracle : service injectant des données du monde réel dans la blockchain. Point de confiance résiduel de tout contrat lié au réel.

Fork (embranchement) : divergence du protocole ou du registre ; un « hard fork » scinde la chaîne en deux histoires concurrentes.

Trilemme : impossibilité pratique de maximiser à la fois décentralisation, sécurité et débit.

Lightning Network : réseau de paiement de seconde couche adossé au bitcoin, à l'adoption restée marginale.

C Annexe · Sources

Satoshi Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », 31 octobre 2008 ; documentation des protocoles Bitcoin et Ethereum (ethereum.org, dont bilan énergétique du Merge).

Cambridge Centre for Alternative Finance (CCAF), indice de consommation électrique du bitcoin, estimations 2025-2026.

Relevés sectoriels de la tokenisation d'actifs réels, juillet 2026 (encours 31 Md$, +400 % depuis début 2025 ; Circle USYC ≈ 3 Md$; BlackRock BUIDL ≈ 2,5 Md$; ≈ 65 % sur Ethereum) ; annonces DTCC (pilote de règlement, S2 2026).

A.P. Møller-Maersk et IBM, communiqué d'arrêt de TradeLens, 29 novembre 2022 ; Supply Chain Dive, Computerworld (analyses).

Presse financière sur la liquidation de Diem (janvier 2022, cession à Silvergate pour 182 M$).

Chainalysis, « The 2026 Crypto Crime Report » (fonds volés 3,4 Md$ en 2025 ; stablecoins 84 % des flux illicites).

L'Investisseur Stratège, dossiers n°04 (« Bitcoin : l'épreuve de la liquidité ») et dossier technique n°10 (« À quoi sert le bitcoin ? »), juillet 2026.

Avertissement. Ce document est diffusé par L'Investisseur Stratège à des fins exclusivement informatives et pédagogiques. Il ne constitue ni un conseil en investissement, ni une recommandation d'achat ou de vente, ni une sollicitation au sens de la réglementation AMF / MAR. Les chiffres cités proviennent de sources publiques susceptibles d'être révisées. Toute décision d'investissement relève de la seule responsabilité du lecteur, invité à consulter un conseiller habilité. © 2026 L'Investisseur Stratège · investisseur.stratege@norvalgroup.com