

# L'avenir de Pontem et de l'écosystème Move

19/05/2022

**Source :** [https://docs.google.com/document/d/1lrjPmdSBLuCG28kbXLICcqGuQzRXp\\_OEqIGhxVFTLY8/edit](https://docs.google.com/document/d/1lrjPmdSBLuCG28kbXLICcqGuQzRXp_OEqIGhxVFTLY8/edit)

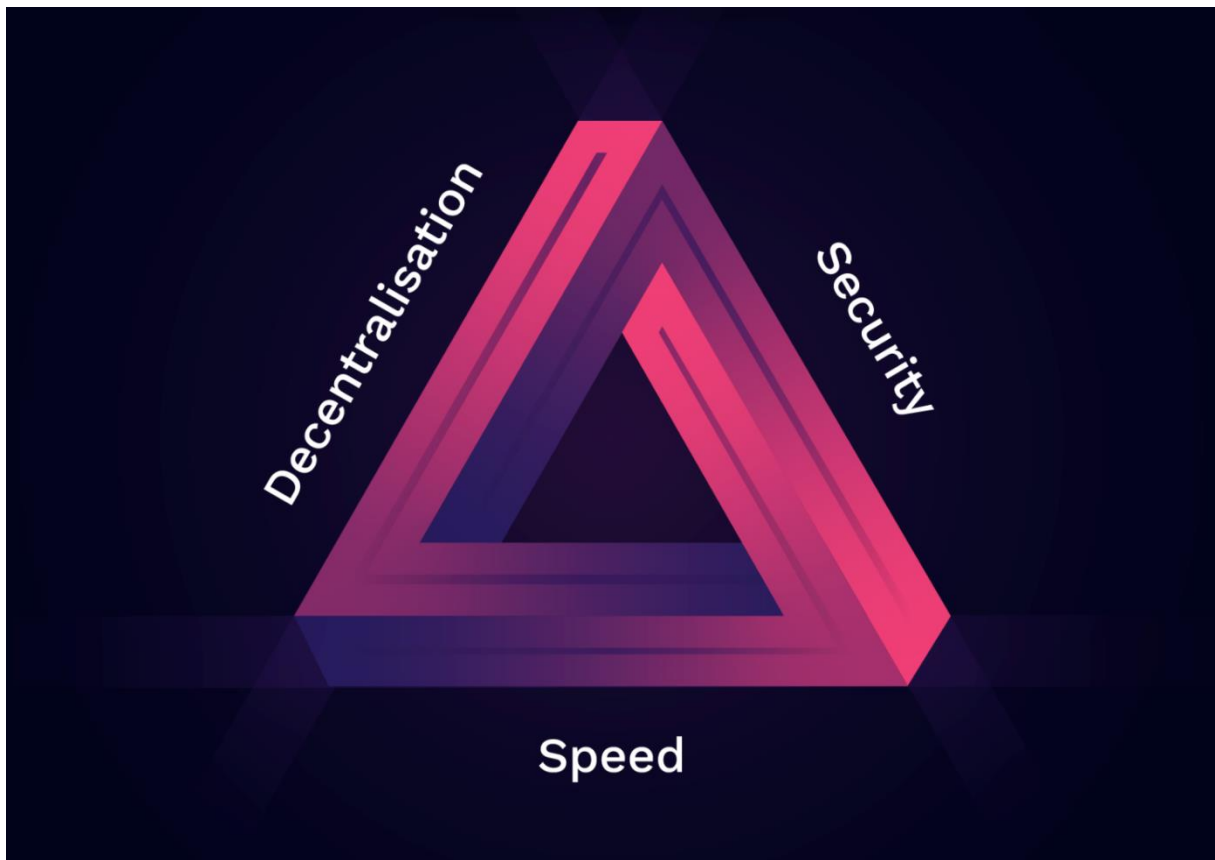


## D'où venons-nous

L'histoire des blockchains est incroyablement récente. Bien que cela semble étrange à dire pour ceux d'entre nous qui travaillent et vivent dans un monde alimenté par la crypto-monnaie, cette technologie existe depuis à peine plus d'une décennie.

Tout commence par la conception immaculée de la crypto : en 2008, le livre blanc Bitcoin de Satoshi Nakamoto est partagé via une liste de diffusion dédiée à la cryptographie. En 2011, le Litecoin et d'autres alt-coins sont apparus, apportant des améliorations itératives aux blockchains. En 2014, Ethereum a été lancé, ouvrant la voie aux contrats intelligents, permettant les NFT, la DeFi et les Play-to-earn. Quelques années plus tard, l'adoption a explosé, avec des chaînes ultra-rapides comme Solana et Avalanche qui ont mené la deuxième vague. Aujourd'hui, 14 ans à peine après le livre blanc sur le bitcoin, nous assistons à la nouvelle génération de projets L1 comme Aptos, construits avec la Move VM, et visant une adoption massive en résolvant enfin le trilemme de la blockchain : des réseaux

décentralisés, sécurisés et évolutifs. Aptos vise à faire fonctionner un système financier mondial sécurisé pour des milliards de personnes sur le Web3.



Inspirés par cette histoire, nous nous tournons vers l'avenir. Quels obstacles à l'adoption des blockchains subsistent ? Comment les blockchains vont-elles continuer à s'améliorer et à évoluer ? Quelles sont leurs utilisations futures ? Quels sont les marchés inexploités propices à l'adoption de la technologie ?

Nous avons passé les dernières années à construire des produits pour la blockchain Diem et son langage de programmation Move. Le projet Diem, lancé par Meta (en association avec Shopify et Uber), puis racheté par Silvergate Bank, a été conçu pour faciliter une intégration financière générale. Aptos, un projet créé par d'anciens ingénieurs de Diem et de Meta, reprend là où Diem s'est arrêté, en construisant une infrastructure destinée à soutenir des milliards d'utilisateurs en vue de permettre une adoption universelle. En outre, ce projet vise à réduire la population non bancarisée : les personnes ayant un accès limité ou inexistant aux outils et institutions financières. Nous continuons de croire que ces objectifs sont incroyablement importants pour faire progresser l'avenir des blockchains et les valeurs de notre secteur.

À cette fin, nous prêtons attention à deux tendances clés entremêlées dans le paysage cryptographique actuel : 1) l'adoption universelle ; et 2) l'évolutivité et la facilité d'utilisation.

L'adoption des crypto-monnaies continue de croître dans le monde entier. Cependant, la croissance ralentit sur les principaux marchés financiers comme les États-Unis et la Chine, selon Chainalysis. Dans le même temps, des pays comme le Vietnam, le Pakistan, l'Ukraine et le Kenya voient le montant de la valeur transférée sur les chaînes augmenter, surtout si l'on tient compte du pouvoir d'achat par habitant. Alors que l'engouement actuel pour le marché est dominé par les NFT, les objets de collection et les jeux play-to-earn, qui occupent une grande partie de la sphère culturelle de la crypto-monnaie, la plus grande partie de la croissance mondiale se situe en fait dans les plateformes centralisées faciles à utiliser comme Coinbase et les outils DeFi très lucratifs comme Uniswap. Pour nous, cela montre clairement la voie à suivre pour l'industrie de la blockchain : générer des outils simples et évolutifs qui utilisent les avantages inhérents à la crypto afin de transformer le contexte centralisé actuel en un nouveau système financier décentralisé qui soit ouvert, puissant et mondial.

Nous identifions trois éléments qui sont nécessaires pour poursuivre et développer cette tendance :

1. Une transparence réglementaire mondiale qui a) favorise l'innovation, b) protège les droits de propriété individuels et la vie privée, et c) est cohérente au-delà des frontières afin de faciliter les activités internationales.
2. Une combinaison complète de mécanismes financiers basés sur les crypto-monnaies, au-delà des paiements et des transactions, dont la fiabilité, la rapidité et l'accessibilité concurrencent et surpassent les outils financiers centralisés tels que Robinhood et Coinbase et les instruments financiers traditionnels tels que les actions et les obligations.
3. Des standards d'interopérabilité et de sécurité à la mesure de l'écosystème, notamment en ce qui concerne les outils, bibliothèques et frameworks de smart contract.

## Aller de l'avant

À quoi ressemblera l'avenir ? Nous imaginons un système financier interconnecté et décentralisé, accessible et utile à toute personne disposant d'un appareil mobile. Si d'importantes quantités de liquidités institutionnelles ont afflué vers les crypto-monnaies, on ne peut pas en dire autant des applications décentralisées, ou dApps. Ainsi, nous identifions un "déficit d'adoption" dans l'écosystème: les institutions financières traditionnelles ont adopté la crypto à des degrés divers en tant qu'actif d'investissement, mais ne se sont pas

pleinement engagées à déployer des contrats intelligents pour des cas d'utilisation comme la DeFi, même si les particuliers reconnaissent de plus en plus son potentiel de rendement. Cela signifie que les entreprises traditionnelles, à la fois motivées par une mission et par le profit, visant à atteindre une intégration financière générale, s'engageront plus pleinement dans la révolution DeFi. Ou bien, la DeFi remplacera les institutions qui ne s'adaptent pas au Web3. Chez Pontem, nous avons l'intention de fournir une infrastructure adaptée aux deux possibilités, car nous pensons que le monde se situera quelque part au milieu de ce spectre.

Nous pensons que la blockchain Diem, maintenant Aptos, est le projet le plus avancé techniquement pour la mission consistant à assurer une intégration financière totale. Diem visait à être incroyablement fiable, sans interruption de service entre les transactions et avec des temps de finalisation rapides et déterministes. Ils ont développé des algorithmes de consensus modernes comme HotStuff et ont également créé le langage de programmation Move. Ce dernier a été conçu pour les blockchains hautement évolutives, permettant des temps de transaction rapides et un débit élevé. Il est également conçu pour être agnostique aux blockchains, ce qui le rend idéal pour les dApps impliquant des déploiements multi-chaînes. L'utilisation du type de données natif "ressource" par Move pour les tokens plutôt que pour les smart contracts le rend plus sûr que Solidity. Les ressources Move permettent également de personnaliser facilement les propriétés des actifs. Dans l'ensemble, ces caractéristiques permettent aux développeurs de créer des applications numériques de classe mondiale et de niveau institutionnel sur Move.

Le marché des VC parie sur le succès de cette technologie. Aptos, fondée par une grande partie de l'équipe Meta qui a construit Diem, crée une nouvelle blockchain de couche 1 indépendante axée sur l'adoption massive de Web3. Des acteurs majeurs de l'industrie investissent dans la mission initiale d'apporter la crypto-monnaie à des milliards de personnes en permettant de nouveaux cas d'utilisation basés sur Move. Fort d'une expérience au sein de la société de conseil en gestion BCG et d'un rôle de direction stratégique chez Consensus, le PDG Mo Shaikh a fait participer des associés de Diem, tel que Coinbase, à la levée de fonds de 200 millions de dollars d'Aptos, menée par a16z crypto et Multicoin. Dans le cadre de sa mission visant à atteindre un milliard d'utilisateurs, Aptos donne la priorité à "la sécurité absolue, l'extensibilité et la neutralité". Ces éléments représentent les fondements essentiels à l'adoption institutionnelle et individuelle du projet.

Aptos s'appuie sur les principales innovations de Diem, notamment le Diem-BFT, un dérivé du mécanisme de consensus Hot Stuff Byzantine Fault Tolerant (BFT) utilisé par Cosmos. Avec ce mécanisme de consensus, ainsi qu'un système de vérification des blocs qui analyse la réputation des validateurs et synchronise leurs votes, Aptos peut atteindre des temps de

finalisation inférieurs à la seconde avec un débit élevé. Aptos met également l'accent sur la sécurité en couplant la VM déterministe de Move avec la gestion sécurisée des actifs de Move, les jetons étant considérés comme des types de données "ressources" natives. Cela rend l'écriture de contrats intelligents beaucoup plus sûre pour les développeurs. Des protocoles supplémentaires de rotation et de récupération des clés privées contribuent à offrir aux utilisateurs et aux développeurs la meilleure expérience possible.

L'équipe d'Aptos a également optimisé l'évolutivité et la vitesse, atteignant des débits de "130 000 transactions" en isolant et en améliorant le protocole de consensus, le pipeline d'exécution et les structures de données authentifiées. Après avoir géré l'infrastructure de données destinée à des milliards d'utilisateurs chez Meta (anciennement Facebook), le directeur technique Avery Ching et son équipe d'ingénieurs spécialisés dans la blockchain et les données sont les plus grands experts mondiaux en informatique distribuée, capables de maintenir une blockchain fiable et hautement disponible.

Nous prévoyons que le marché découvrira rapidement les avantages de la sécurité, de l'évolutivité et de la facilité d'utilisation de la Move VM. Cela conduira à une augmentation de la demande de la part des développeurs d'applications qui, à leur tour, exigeront que le langage soit intégré nativement dans les blockchains L1 sur lesquelles ils sont déjà déployés afin qu'ils puissent maintenir une base de code commune.

## Où allons-nous ?

La prochaine vague d'adoption sera menée par les entreprises. Les organisations centralisées sont très utiles pour la plupart des clients grand public qui utilisent la DeFi, car elles permettent aux utilisateurs réguliers d'externaliser certains services très importants de gestion sécurisée des clés privées et de maintenance de l'infrastructure, ce qui évite les effets externes négatifs tels que les pertes de fonds, le slashing et l'impermanent loss. Cette vague sera marquée par le détrônement de l'un des éléments les plus dominants de l'espace blockchain actuel : la machine virtuelle Ethereum. Si Ethereum et l'EVM ont des avantages, ils présentent également beaucoup d'inconvénient. La vaste communauté de développeurs qui utilise l'EVM crée un effet de réseau qui permet à de nouvelles applications numériques de se lancer rapidement, mais les problèmes d'évolutivité commencent à se faire sentir et entraînent une perte de parts de marché au profit de nouveaux entrants comme Cosmos Solana et Polkadot. Bien que les problèmes d'évolutivité soient en train d'être résolus par la dernière génération de L1, la sécurité, la fiabilité et la facilité d'utilisation restent des obstacles importants pour les institutions comme les gouvernements et les entreprises qui

veulent croire à la migration de leurs informations essentielles vers les différentes blockchains publiques formant un cloud fragmenté de calcul et de stockage décentralisés.

Le liquid staking est la manière dont des sociétés comme Kraken ont commencé à utiliser la DeFi pour le compte de leurs clients afin d'obtenir des rendements. Le staking est généralement plus sûr car il est géré par le protocole principal. Cependant, les risques de piratage des contrats intelligents doivent diminuer de manière significative pour que les entreprises se sentent à l'aise d'adopter des dApps comme les AMMs avec une liquidité suffisante pour les transactions afin de faire bénéficier à leurs clients des réductions de coûts et des récompenses du liquid stacking.

En résumé, Ethereum est risqué pour les entreprises, en grande partie à cause du langage de programmation Solidity. Même le créateur de Solidity et cofondateur d'Ethereum, Gavin Woods, souhaitait passer du langage EVM à d'autres standards comme Rust lorsqu'il a lancé Polkadot. Solidity présente de sérieux problèmes, notamment en matière de sécurité. Une fois qu'un contrat intelligent est déployé, il est immuable sans contrôle d'accès natif, ce qui signifie que les bugs et les vulnérabilités sont presque impossibles à corriger. Il est également sujet à des attaques de réentrance, ce qui a entraîné la chute de la tristement célèbre DAO en 2016. La mutabilité d'Ethereum a été mise en évidence par la naissance de l'Ethereum Classic lors d'un hard fork. Il n'est pas étonnant que les applications qui connaissent la croissance la plus rapide (mesurée par la valeur totale bloquée et les utilisateurs) se trouvent sur des blockchains plus rapides construites sur d'autres machines virtuelles, comme Fantom (Solidly), Avax (JOE) et Solana (Serum).

Il s'agit d'une partie naturelle de l'évolution de toute technologie. Ethereum a été le premier à proposer des contrats intelligents, illustrant le vaste potentiel de la technologie dans des cas d'utilisation autres que les transactions et le stockage de valeurs. Cependant, il a également été le premier martyr, car les conséquences involontaires des premières décisions de conception ont entraîné des piratages et des problèmes d'évolutivité. Aujourd'hui, de nombreuses blockchains de nouvelle génération sont apparues, apportant des solutions à ses défauts, en utilisant la gouvernance on-chain, les mécanismes de consensus par preuve d'enjeu et l'absence de hard forks.

Cela se produit avec n'importe quelle technologie ; il se trouve que les blockchains évoluent rapidement. L'internet a mis quatre ans à se développer et n'a connecté que quatre ordinateurs en 1969. Il n'a connu son essor que dans les années 1990. Aujourd'hui, 52 ans plus tard, le classement Fortune 500 est dominé par des sociétés Internet. N'oubliez pas que nous sommes à 14 ans seulement du livre blanc du bitcoin. La crypto-monnaie évolue plus rapidement que toute autre technologie dans l'histoire. Cela signifie que nous devons

permettre l'innovation à la vitesse de la lumière ou risquer de rester bloqué dans les sables du temps. Nous devons faire évoluer nos systèmes existants et en créer de nouveaux au-delà de ce que nous avons imaginé jusqu'à présent. Move est désormais à la pointe de cette évolution.

## Quelles sont les prochaines étapes pour Pontem ?

C'est dans l'écosystème florissant des infrastructures basées sur Move que Pontem possède un avantage concurrentiel. Au cours des quatre dernières années, notre équipe a développé une expertise approfondie de Move. Après avoir travaillé directement avec la technologie développée par les ingénieurs de Meta et Diem, nous savions que nous devions être les premiers à développer une machine virtuelle Move pour étendre la portée de cette technologie incroyable. Nos compétences englobent les éléments essentiels au développement de la blockchain moderne et nous pensons que nous sommes non seulement bien positionnés pour l'avenir, mais aussi dans une position unique pour le construire. Compte tenu de la position unique dans laquelle nous nous trouvons, nous allons modifier notre modèle d'entreprise pour créer les premiers produits pour la blockchain Aptos. Grâce à nos compétences et à notre expérience, nous contribuerons à la croissance, au développement de cet écosystème et à la création de valeur (à travers la pile technologique) en construisant les dApps primitives nécessaires pour que la L1 d'Aptos soit utilisée par des milliards de personnes. Nous travaillerons avec les dApps, les fournisseurs d'infrastructure et les L1 en place pour les aider à passer à la technologie Move. Lorsque nous identifierons des failles, nous développeront nous-mêmes les solutions et effectuerons des mises à jours pour rester à la pointe de l'innovation.

Nous sommes convaincus que Move est la voie à suivre, et nous soutiendrons donc les équipes qui portent le flambeau. Grâce à un partenariat avec Aptos, nous tirerons parti de notre expertise pour mettre sur le marché les premières dApps natives de Move. Nous rendrons également notre solution interopérable avec toutes les blockchains en langage Move afin de construire l'infrastructure nécessaire pour que les développeurs et les utilisateurs puissent accéder aux chaînes basées sur Move et utiliser nos protocoles sur Aptos.

Pourquoi Aptos ? Aptos n'est pas seulement la chaîne basée sur Move la plus développée, mais elle exploite également les meilleures caractéristiques de Diem, comme le protocole de consensus BFT évolutif. Les équipes d'Aptos ont également effectué des tests rigoureux sur le client Aptos Core, adopté des procédures de sécurité de compte telles que la rotation et la récupération des clés, et optimisé le pipeline d'exécution Tx pour obtenir un débit élevé et

une finalité rapide. Tout cela nous amène à penser qu'Aptos sera l'une des premières couches 1 à conquérir un milliard d'utilisateurs (si le bitcoin n'y arrive pas avant).

Nous allons d'abord construire la prochaine génération de dApps avec des expériences simplifiées rendues possibles par Aptos et Move. Cela alimentera l'adoption générale au niveau mondial pour les clients et les institutions. Nous avons l'intention de reprendre là où Diem s'est arrêté, en rejoignant les personnes qui l'ont construit pour amener le premier milliard d'utilisateurs à la blockchain. Cela représenterait un bouleversement énorme : seuls 46 millions d'Américains déclarent posséder des BTC, selon un sondage réalisé par NYDIG en 2021.

Nous avons déjà développé un fork de la machine virtuelle Move de Diem qui peut être facilement déployé sur d'autres chaînes récentes comme Polkadot, Cosmos, Avalanche, et plus encore. Notre objectif est de faire prospérer Move, nous prévoyons donc un déploiement futur au fur et à mesure que l'écosystème dApp Move mûrit et que le besoin d'environnements Move dans d'autres L1 augmente. Nous allons également étudier le développement d'une nouvelle VM Ethereum compatible avec la VM Move pour connecter les deux technologies et permettre aux développeurs de dApps de profiter de tous les avantages de Move. Cela leur permettra de migrer progressivement et prudemment, sans le risque et les frais liés à une application monolithique.

Aux autres couches 1, nous venons en paix. Notre mission est de partager le morceau à l'ensemble de l'écosystème. Ce sur quoi nous travaillons profite à tout le monde. Les améliorations apportées par la Move Virtual Machine en matière de sécurité, d'évolutivité et de facilité d'utilisation sont essentielles pour nous tous, car nous nous appuyons de plus en plus sur l'infrastructure financière blockchain. Nous avons l'intention de rendre la Move VM interopérable avec d'autres L1 et d'embarquer une nouvelle génération de développeurs blockchain qui pourront construire la prochaine vague de dApps blockchain grand public.

Nous voulons unir non seulement les parties utilisant des protocoles Move, mais aussi l'ensemble de l'écosystème blockchain en définissant des normes d'interopérabilité et de rétrocompatibilité avec Move.

Voilà où nous allons. Nous parions gros sur Move. Nous travaillons avec les personnes qui l'ont lancé pour construire un écosystème autour de lui. Move alimentera les dApps les plus performantes du monde et le futur de la finance décentralisée. Et tout cela contribue à la mission de fournir une infrastructure et une intégration financières pour tous.



# La Roadmap

Nous visons à lancer notre premier produit d'ici la fin de l'année, en même temps que le lancement du réseau principal d'Aptos. Attendez-vous à des innovations issues de nos recherches sur les AMM, EVM et portefeuilles compatibles avec Move. Nous mettrons également à jour nos outils de développement existants, tels que le navigateur Move Playground, pour qu'ils soient compatibles avec Aptos et que les développeurs puissent rejoindre Move. Nos outils constitueront un point d'entrée pour les développeurs Move et sensibiliseront les entreprises et les autres développeurs de protocoles à l'existence des produits Pontem déployés sur Aptos, grâce à des API faciles à utiliser. À long terme, notre objectif est également d'introduire Move dans les L1 comme Polkadot et Avalanche afin de faire connaître les normes de l'écosystème et de faire croître la proposition de valeur pour tous les L1 qui la soutiennent. Notre feuille de route détaillée sera bientôt publiée sur notre site Web et sur nos canaux communautaires, alors restez à l'écoute !

## FAQ

### **Que construit Pontem ?**

À court terme, nous nous concentrerons sur le déploiement des premières applications basées sur Move, comme les AMMs et le liquid staking. Nous considérons également qu'il y a une réelle opportunité de développer une machine virtuelle Ethereum compatible avec Move, ainsi que l'infrastructure et les outils nécessaires à l'interopérabilité.

Plus tard, nous déploierons notre machine virtuelle WASM Move sur des blockchains L1 populaires comme Polkadot, Cosmos et Solana afin de permettre aux applications de gérer une base de code Move sur plusieurs L1.

### **Où Pontem lancera-t-il son jeton en premier ?**

Aptos.

### **Que se passe-t-il avec le réseau de test Polkadot / Kusama ?**

Le programme de testnet incitatif se poursuivra jusqu'à la fin avril, mais les opérateurs de nœuds devront peut-être migrer à un certain moment pour tester nos nouvelles applications. Nous récompenserons tous les participants au programme de testnet incitatif soit en leur offrant les jetons NOX choisis lors du lancement sur Kusama, soit en les convertissant en

jetons qui seront lancés ultérieurement. Nous partagerons plus de détails à ce sujet dans un post à part.

### **Y aura-t-il un crowdloan sur Kusama ?**

Probablement pas cette année. Nous viserons à nous étendre à Polkadot et Kusama une fois qu'il y aura suffisamment de demande pour le Move VM en dehors d'Aptos et de Sui. Cependant, pour mettre en place ce nouveau concept de tokenomic, nous recherchons une nouvelle approche qui offrira un rendement par le biais d'une combinaison entre le liquid stacking et la bridging liquidity sur nos applications lancées dans le futur. Nous vous en dirons plus bientôt, mais pour l'instant, vous pouvez faire ce que vous voulez avec vos KSM.

### **Que va-t-il advenir du jeton Nox ?**

Nous sommes intrigués par le concept novateur qui consiste à créer un jeton distinct pour un réseau canari destiné à tester les applications. Nous pourrions donc lancer quelque chose de similaire pour les réseaux Move VM. Mais pour l'instant, nous le mettons de côté.

**Titre Tag :** L'avenir de Pontem avec Aptos

**Meta Description :** Pontem construit des dApps et des outils pour des blockchains Move rapides et évolutives.