La Blockchain Aptos Infrastructure Web3 Evolutive, Sécurisée et Scalable

16 août 2022
v1.0
Traduit par KBCONSULTING45

Table des matières

Executive Summary

L'essor des blockchains en tant que nouvelle infrastructure Internet a conduit les développeurs à déployer des dizaines de milliers d'applications décentralisées à des rythmes de croissance rapide.
Malheureusement, l'utilisation de la blockchain n'est pas encore omniprésente en raison de pannes fréquentes, de coûts élevés, de limitations de débit et de nombreuses préoccupations en matière de sécurité.
Pour permettre une adoption massive à l'ère du web3, l'infrastructure blockchain a besoin de suivre la voie de l'infrastructure cloud en tant qu'infrastructure fiable, évolutive, rentable et doit continuer l'amélioration de la plate-forme pour la création d'applications largement utilisées.
Nous présentons la blockchain Aptos, conçue en tant que blockchain avec pour principes clés l'évolutivité, la sécurité et la fiabilité pour relever ces défis.
La blockchain Aptos a été développée au cours des trois dernières années par plus de 350 développeurs à travers le monde [1].
Elle offre des innovations nouvelles dans le consensus, la conception de contrats intelligents, la sécurité du système, la performance et la décentralisation.
La combinaison de ces technologies fournira un élément fondamental pour démocratiser le Web3.

• Tout d'abord, la blockchain Aptos intègre nativement et utilise en interne le langage Move pour la rapidité et l'exécution sécurisée des transactions [2].
The Move Prover, un vérificateur formel pour les contrats intelligents écrit en Move, fournit des garanties supplémentaires pour les invariants contractuels et leur comportement.
Cet accent mis sur la sécurité permet aux développeurs de mieux protéger leurs applications contre les entités malveillantes.
• Deuxièmement, le modèle de données Aptos permet une gestion flexible des clés et des options de conservation hybrides.
Ceci, en plus de la transparence des transactions avant la signature et des protocoles clients légers pratiques offrant une expérience utilisateur plus sûre et plus fiable.
• Troisièmement, pour atteindre un débit élevé et une faible latence, la blockchain Aptos exploite un pipeline et une approche modulaire pour les étapes clés du traitement des transactions.
Plus précisément, la diffusion des transactions, l'ordonnancement des métadonnées par bloc, l'exécution de transactions parallèles, le stockage par lots, et la certification du grand livre fonctionnent simultanément.
Cette approche tire pleinement partie de tous les éléments physiques disponibles, améliore l'efficacité matérielle et permet une exécution hautement parallèle.
• Quatrièmement, contrairement à d'autres moteurs d'exécution parallèle qui brisent l'atomicité des transactions en exigeant la connaissance initiale des données à lire et à écrire, la blockchain Aptos n'amène pas ces limitations pour les développeurs.
Elle peut soutenir efficacement l'atomicité en arbitrant des transaction complexes, permettant un débit plus élevé et une latence plus faible pour les applications du monde réel et ainsi simplifier le développement.

• Cinquièmement, la conception de l'architecture modulaire Aptos prend en charge la flexibilité du client et est optimisée pour les mises à niveau fréquentes et instantanées. De plus, pour déployer rapidement de nouvelles innovations technologiques et prendre en charge de nouveaux cas d'utilisation web3, la blockchain Aptos fournit un protocole de gestion des changements on-chain.

• Enfin, la blockchain Aptos expérimente de futures initiatives pour aller au-delà de la performance individuelle du validateur : sa conception modulaire et son moteur d'exécution parallèle prennent en charge le partitionnement interne d'un validateur, de plus le partitionnement d'état homogène offre un potentiel d'évolutivité horizontal du débit sans ajouter de complexité supplémentaire pour les opérateurs de nœuds.

1 Introduction

Dans la version Web2 d'Internet, des services tels que la messagerie, les médias sociaux, la finance, les jeux, les achats, et le streaming audio/vidéo sont fournis par des entreprises centralisées qui contrôlent l'accès direct aux données utilisateur (par exemple, Google, Amazon, Apple et Meta).
Ces entreprises développent des infrastructures en utilisant des logiciels spécifiques aux applications optimisés pour des cas d'utilisation ciblés et tirant parti des infrastructures cloud pour déployer ces applications aux utilisateurs.
L'infrastructure cloud permet d'accéder à des services d'infrastructures virtualisées et/ou physiques, tels que les machines virtuelles louées (VM) et le matériel bare metal fonctionnant dans les centres de données du monde entier (par exemple, AWS, Azure et Google Cloud).
Par conséquent, construire des services internet web2 qui peuvent convenir à l'utilisation simultanée de milliards d'utilisateurs n'a jamais été aussi faciles qu'aujourd'hui.
Toutefois le web2 exige que les utilisateurs accordent une confiance aveugle aux entités centralisées, une exigence qui est devenue de plus en plus préoccupante pour notre société.
Pour lutter contre cette préoccupation, une nouvelle ère Internet a commencé : le Web3.
Dans la version Web3 d'Internet, les blockchains ont émergé pour fournir des registres décentralisés et immutables qui permettent aux utilisateurs d'interagir avec les uns avec les autres de manière sûre et fiable, le tout sans nécessiter de tiers de confiance tels que des intermédiaires et des entités centralisées.
Semblable à la façon dont les services et applications Internet web2 s'appuient sur l'infrastructure cloud en tant que socle, les applications décentralisées peuvent utiliser les blockchains comme une couche d'infrastructure décentralisée pour atteindre des milliards d'utilisateurs à travers le monde.
Cependant, malgré l'existence de nombreuses blockchains aujourd'hui, l'adoption généralisée du web3 n'a pas encore eu lieu [3].
Alors que la technologie continue de faire progresser l'industrie, les blockchains existantes sont peu fiables, imposent des frais de transaction élevés pour les utilisateurs, ont des limitations de débit, souffre de hacks réguliers entrainant des pertes dues à des problèmes de sécurité et ne peuvent pas prendre en charge la réactivité en temps réel.
Par rapport à la façon dont le cloud d'infrastructure a permis aux services web2 d'atteindre des milliards de personnes, les blockchains n'ont pas encore « activées » le web3 pour faire de même.

2 La vision d'Aptos

La vision d'Aptos est de fournir une blockchain qui peut apporter l'adoption grand public du web3 et renforcer un écosystème d'applications décentralisées pour résoudre les problèmes des utilisateurs du monde réel.
Notre mission est de faire progresser l'état de l'art en matière de fiabilité, de sécurité et de performance de la blockchain en fournissant un système flexible et modulaire d'architecture blockchain.
Cette architecture devrait prendre en charge des mises à niveau fréquentes, une adoption rapide des derniers progrès technologiques et la prise en charge en première instance des cas d'utilisation nouveaux et émergents.
Nous envisageons un réseau décentralisé, sécurisé et évolutif régi et exploité par la communauté qui l'utilise.
Lorsque les demandes d'infrastructure augmentent à travers le monde, les ressources de calcul d'une blockchain évoluent horizontalement et verticalement pour répondre à ces besoins. Au fur et à mesure que de nouveaux cas d'utilisation et des progrès technologiques surviennent, le réseau doit être mis à niveau fréquemment et de manière transparente sans interrompre les utilisateurs.
Les préoccupations en matière d'infrastructure devraient passer au second plan.
Les développeurs et les utilisateurs auront accès à de nombreuses options différentes pour la récupération des clés, la modélisation des données, les normes de contrats intelligents, les compromis d'utilisation des ressources, la confidentialité et la composabilité.
Les utilisateurs savent que leurs actifs sont sécurisés, toujours disponibles et peuvent être accessible avec des frais presque à prix coûtant.
N'importe qui peut effectuer des transactions en toute sécurité, facilement et immuablement avec des personnes et sans tiers de confiance à travers le monde.
Les blockchains seront aussi omniprésentes que l'infrastructure cloud.
Pour arriver à cela, des avancées technologiques significatives doivent être réalisées.
A travers nos expériences de construction, de développement, de progression et de déploiement de la blockchain Diem (le prédécesseur de la blockchain Aptos) au cours des trois dernières années, il a été prouvé qu'un réseau peut continuellement mettre à niveau ses protocoles sans perturber ses clients [4].
Le réseau principal Diem a été déployé sur plus d'une douzaine d'opérateurs de nœuds avec plusieurs fournisseurs de portefeuille au début de l'année 2020.
Au cours de l'année suivante, notre équipe a publié deux mises à niveau majeures.
Cela a modifié le protocole de consensus et le cœur du framework.
Les deux mises à niveau se sont terminées sans temps d'arrêt pour les utilisateurs.
Avec la blockchain Aptos, nous avons apporté une série d'améliorations radicales à la pile technologique tout en intégrant des mises à niveau sûres, transparentes et fréquentes en tant que caractéristique principale inspirée par la blockchain Diem.
En particulier, nous mettons en évidence de nouvelles méthodes de traitement des transactions (comme décrit à la section 7) et de nouvelles approches en matière de décentralisation et de gouvernance des réseaux.

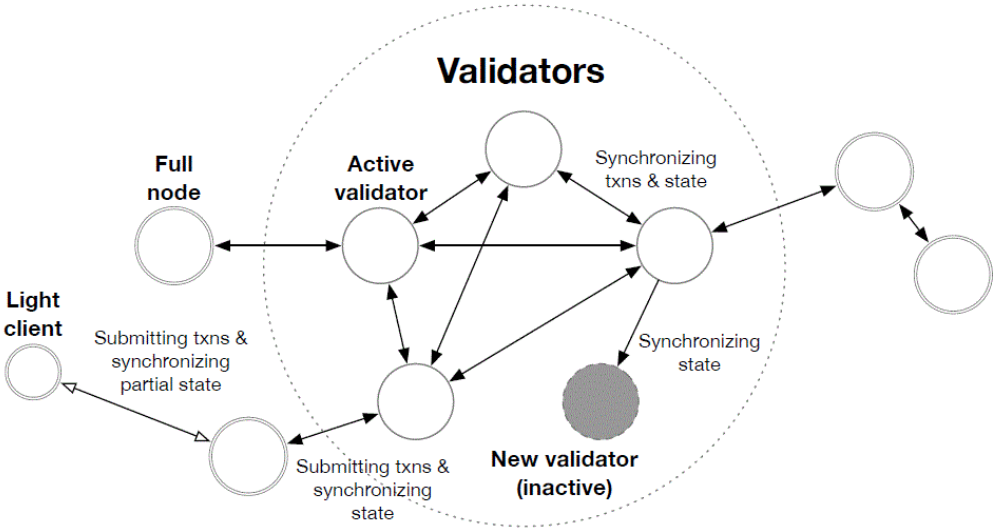

Figure 1: Components of the Aptos ecosystem.

Au fur et à mesure que la blockchain Aptos continue de s'améliorer et de croître, nous publierons des versions actualisées de ce livre blanc avec la dernière itération de nos protocoles et de nos choix de conception.
Dans le reste du présent document, nous décrivons l'état actuel de la blockchain Aptos ainsi que les plans futurs.

3 Vue d'ensemble

La blockchain Aptos, comme le montre la figure 1 ci-dessus, est composée d'un ensemble de validateurs qui reçoivent conjointement les transactions des utilisateurs et les traitent à l'aide d'un consensus byzantin tolérant aux pannes (BFT) et d'un mécanisme de preuve d'enjeu.
Les détenteurs de jetons verrouillent ou mettent en jeu des jetons dans les validateurs qu'ils ont sélectionnés. Pour chaque validateur le poids des votes par consensus est proportionnel au montant qui y est verrouillé.
Un validateur peut être actif et participer au consensus.
De même, un validateur peut également être inactif s'il n'a pas suffisamment de jeton verrouillés (stakés) pour participer, il tourne ainsi hors de l'ensemble des validateurs et choisit d'être hors ligne tout en se synchronisant à l'état de la blockchain, ou est réputé ne pas participer au protocole de consensus en raison de mauvaises performances historiques.
Les clients sont représentés par toute partie du système qui doit soumettre des transactions ou interroger l'état et l'historique de la blockchain.
Les clients peuvent choisir de télécharger et de vérifier les preuves signées par le validateur des données interrogées.
Les nœuds complets (ou fullnode) sont des clients qui répliquent l'état de la transaction et de la blockchain à partir des validateurs ou de d'autres nœuds complets (fullnode) du réseau.
Ils peuvent choisir d'élaguer l'historique des transactions et l'état de la blockchain comme souhaité pour récupérer de l'espace de stockage.
Les clients légers (light clients) gèrent uniquement l'ensemble actuel de validateurs et peuvent interroger partiellement l'état de la blockchain en toute sécurité, généralement à partir de nœuds complets.
Les portefeuilles sont un exemple courant de client léger.
Pour répondre aux besoins d'une infrastructure web3 sûre, rapide, fiable et évolutive pour une adoption généralisée, la blockchain Aptos est construite sur les principes de conception de base suivants :

- Exécution rapide et sécurisée ainsi qu'auditabilité simple et analysabilité mécanique via un nouveau langage de programmation de contrat intelligent, Move [5].
  Move est issu du prédécesseur de la blockchain Aptos (Diem) et continue de progresser via l'évolution de ce projet.

• Débit extrêmement élevé et faible latence grâce à une approche du traitement des transactions par lots, canalisée et parallélisée.
• Nouveau traitement de transaction parallèle qui prend en charge efficacement l'atomicité avec un arbitrage des transactions complexes via Block-STM, contrairement aux moteurs d'exécution parallèle existants qui nécessitent de connaitre à l'avance l'emplacement des données à lire et à écrire.
• Optimisations pour les performances et la décentralisation au travers de la rapidité, de l'importance des jetons stakés et du suivi de la réputation des validateurs.
• Évolutivité et configurabilité en tant que principes de conception de base pour adopter de nouveaux cas d'utilisation et les dernières technologies.
• Conceptions modulaires qui permettent des tests rigoureux au niveau des composants et une modélisation appropriée aux menaces ainsi qu'un déploiement transparent, le tout garantissant des opérations hautement sécurisées et fiables.
• Évolutivité horizontale du débit tout en préservant la décentralisation, avec un concept de partitionnement de première classe exposé aux utilisateurs et natif au modèle de programmation et de données.

La section 4 explique comment les développeurs interagissent avec Move dans la blockchain Aptos.
La section 5 décrit le modèle de données logique.
La section 6 détaille comment la blockchain Aptos permet une expérience utilisateur sécurisée grâce à de solides méthodes de vérification.
La section 7 décrit les principales innovations en matière de performance autour du pipelining, du batching (traitement par lots), et de la parallélisation.
La section 8 détaille diverses options permettant aux différents clients de synchroniser l'état avec d'autres nœuds.
La section 9 décrit nos plans en matière d'appropriation et de gouvernance communautaires.
Enfin, la section 10 discute des orientations de performance futures tout en maintenant la décentralisation.

4 La langue Move

Move est un nouveau langage de programmation de contrats intelligents qui met l'accent sur la sécurité et la flexibilité.
La blockchain Aptos utilise le modèle objet de Move pour représenter l'état de son registre (voir Section 5.5) et utilise le code Move (modules) pour encoder les règles des transitions d'état.
Les utilisateurs soumettent des transactions qui peuvent :

- Être publiées sur de nouveaux modules
- Mettre à niveau des modules existants
- Exécuter des fonctions d'entrée définies dans un module
- Ou contenir des scripts qui peuvent interagir directement avec les interfaces publiques des modules.

L'écosystème Move contient un compilateur, une machine virtuelle et de nombreux autres outils de développement.
Move s'inspire du langage de programmation Rust, qui rend explicite la propriété des données dans le langage via des concepts comme les types linéaires.
Move met l'accent sur la rareté, la préservation et l'accès aux contrôle des ressources.
Les modules Move définissent la durée de vie, le stockage et le modèle d'accès de chaque ressource.
Cela garantit que des ressources comme Coin :

- Ne sont pas produites sans informations d'identification appropriées
- Ne peuvent pas être dépensées deux fois
- Et ne disparaissent pas.

Move exploite un vérificateur de bytecode pour garantir la sécurité du type et de la mémoire, même en présence de code non approuvé.
Pour vous aider à écrire du code fiable, Move inclut un vérificateur formel, le Move Prover [6], capable de vérifier l'exactitude fonctionnelle d'un programme Move par rapport à une spécification donnée, formulée dans le langage de spécification intégré dans Move.

Au-delà des comptes d'utilisateurs et du contenu du compte correspondant, l'état du grand livre contient également la configuration on-chain de la blockchain Aptos.
Cette configuration réseau inclut l'ensemble des actifs des validateurs, les propriétés de staking et la configuration de divers services au sein de la blockchain Aptos.
La prise en charge par Move de la mise à niveau des modules et de la programmabilité complète permet une configuration transparente, modifie et prend en charge les mises à niveau de la blockchain Aptos elle-même. (Les deux ensembles de mises à niveau ont été exécuté plusieurs fois sans temps d'arrêt sur un réseau principal privé).
L'équipe Aptos a encore amélioré Move avec la prise en charge de cas d'utilisation web3 plus larges.
Comme mentionné plus loin dans la section 5.5, la blockchain Aptos permet un contrôle précis des ressources. Non seulement elle prend en charge la parallélisation de l'exécution, mais elle permet également d'atteindre un coût quasi fixe associé à l'accès et au déplacement des données.
De plus, la blockchain Aptos permet un contrôle fin des ressources qui permet d'obtenir des ensembles de données à grande échelle (par exemple, des collections massives de NFT) dans un seul compte.
De plus, Aptos prend en charge les comptes partagés ou autonomes qui sont représentés entièrement on-chain.
Cela permet aux organisations autonomes décentralisées (DAO) complexes de partager des comptes en collaboration et d'utiliser ces comptes comme conteneurs pour une collection hétérogène de ressources.

5 Modèle de données logique

L'état du grand livre de la blockchain Aptos représente l'état de tous les comptes.
L'état du grand livre est versionné à l'aide d'un entier 64 bits non signé correspondant au nombre de transactions exécutées du système.
N'importe qui peut soumettre une transaction à la blockchain Aptos pour modifier l'état du registre.
Pour toute exécution d'une transaction, une sortie de transaction est générée.
Une sortie de transaction contient zéro ou plusieurs opérations pour manipuler l'état du grand livre (appelés jeux d'écriture), un vecteur d'événements résultants (voir Section 5.1.1), la quantité de gaz consommée et l'état de la transaction exécutée.

5.1 Transactions

Une transaction signée contient les informations suivantes :

- Authentificateur de transaction : l'expéditeur utilise un authentificateur de transaction qui inclut une ou plusieurs signatures numériques pour vérifier qu'une transaction est authentifiée.
- Adresse de l'expéditeur : l'adresse du compte de l'expéditeur.
- Charge utile : la charge utile fait référence à une fonction d'entrée existante on-chain ou contient la fonction à exécuter en tant que bytecode intégré (appelé script).
  En outre, un ensemble d'arguments d'entrée est codé dans des tableaux d'octets. Pour une transaction d'égal à égal, les entrées contiennent les informations et le montant qui leur a été transféré.
- Prix du gaz (dans la devise / unités de gaz spécifiées) : Il s'agit du montant que l'expéditeur est prêt à payer par unité de gaz pour exécuter la transaction. Le gaz est un moyen de payer pour le calcul, la mise en réseau et le stockage.
  Une unité de gaz est une mesure abstraite du calcul sans valeur réelle inhérente.
- Quantité maximale de gaz : La quantité maximale de gaz est le maximum d'unités de gaz que la transaction est autorisée à consommer avant d'avorter. Le compte doit avoir au moins le prix du gaz multiplié par la quantité maximale de gaz ou la transaction sera rejetée lors de la validation.
- Numéro de séquence : Le numéro de séquence de la transaction. Cela doit correspondre au numéro de la séquence stocké dans le compte de l'expéditeur lors de l'exécution de la transaction. Une fois la transaction réussie, le numéro de séquence du compte est incrémenté pour empêcher les attaques par relecture.

• Délai d'expiration : Un horodatage après lequel la transaction cesse d'être valide.
• Chain id : Identifie la blockchain pour laquelle cette transaction est valide, offrant une protection supplémentaire pour que les utilisateurs évitent les erreurs de signature.

A chaque version i, le changement d'état est représenté par le trio (Ti ,O_i , S_i), contenant respectivement la transaction, la sortie de transaction et l'état du grand livre qui en résulte.
Étant donné une fonction déterministe nommée Appliquer, l'exécution de la transaction T_i avec l'état du grand livre S_{i-1} produit la sortie de transaction O_i et un nouvel état du grand livre S_i.
C'est-à-dire Appliquer(S_{i-1}, T_i) → ⟨O_i, S_i⟩.

5.1.1 Événements

Les événements sont émis lors de l'exécution d'une transaction.
Chaque module Move peut définir ses propres événements et sélectionner quand émettre ces événements lors de l'exécution.
Par exemple, lors d'un transfert de pièces, les comptes de l'expéditeur et du destinataire émettront respectivement SentEvent et ReceivedEvent.
Ces données sont stockées dans le registre et ce dernier peut être interrogé via un nœud Aptos.
Chaque événement enregistré a une clé unique et la clé peut être utilisée pour interroger les détails de l'événement.
Plusieurs événements émis vers la même clé d'événement produisent des flux d'événements, une liste d'événements, chacun contenant un nombre croissant séquentiellement commençant à 0, un type et des données.
Chaque événement doit être défini par un certain type.
Il peut y avoir plusieurs événements définis par le même type ou des types similaires, en particulier lors de l'utilisation de génériques.
Les événements ont des données associées.
Pour les développeurs de modules Move, le principe général doit inclure toutes les données nécessaires pour comprendre les modifications apportées aux ressources sous-jacentes avant et après l'exécution de la transaction qui a modifié les données et émis l'événement.
Les transactions peuvent uniquement générer des événements et ne peuvent pas lire les événements.
Cette conception permet à l'exécution de la transaction d'être uniquement une fonction de l'état actuel et des entrées de transaction, et non des informations historiques (p. ex., événements générés précédemment).

5.2 Comptes

Chaque compte est identifié par une valeur unique de 256 bits appelée adresse de compte.
Un nouveau compte est ajouté à l'état du grand livre (voir Section 5.5) lorsqu'une transaction envoyée à partir d'un compte existant appelle la fonction Move create_account(addr).
Cela se produit généralement lorsqu'une transaction tente d'envoyer des jetons Aptos à une adresse de compte qui n'a pas encore été créée.
Pour plus de commodité, Aptos prend aussi en charge une fonction transfert (de, à, montant) qui crée implicitement un compte s'il n'existait pas déjà avant le transfert.

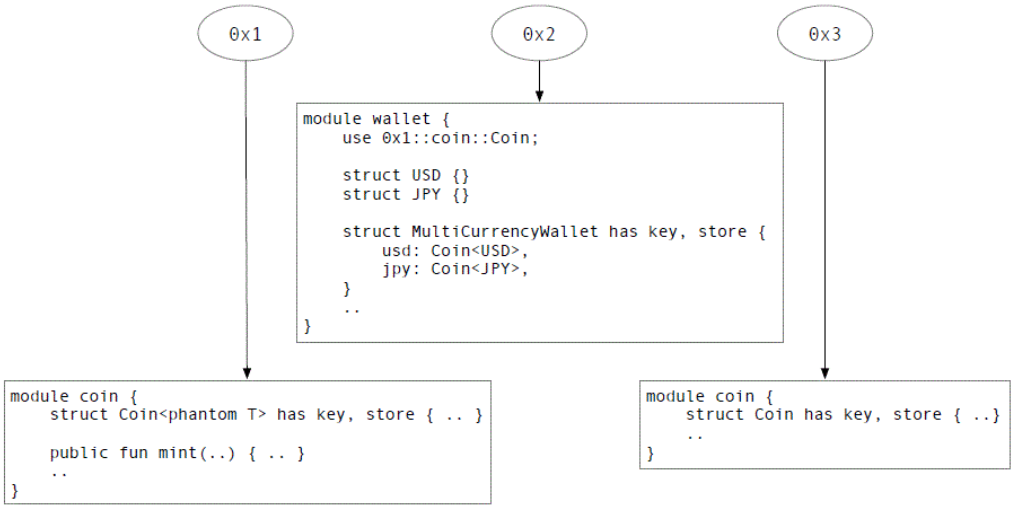

Figure 2: Example on-chain Move modules.

Pour créer un nouveau compte, un utilisateur génère d'abord une paire clé-clé de signature : (vk, sk).
Puis génère le nouveau compte.
L'adresse d'un schéma de signature donné est dérivée à l'aide du hachage cryptographique H de la vérification de la clef publique vk concaténée avec l'identificateur de schéma de signature (ssid) : où addr = H(vk, ssid).
Une fois le nouveau compte créé à d'adresse addr, l'utilisateur peut signer les transactions à envoyer à partir de addr, en utilisant la clé de signature privée sk. L'utilisateur peut également faire pivoter sk, soit de manière proactive changer sk ou pour répondre à un compromis possible. Cela ne changera pas l'adresse du compte, car l'adresse du compte n'est dérivée qu'une seule fois, lors de sa création à partir de la vérification de la clé publique.
La blockchain Aptos ne lie pas les comptes à une identité réelle.
Un utilisateur peut en créer plusieurs en générant plusieurs paires de clés.
Les comptes contrôlés par le même utilisateur n'ont pas de lien inhérent les uns avec les autres. Cependant, un seul utilisateur peut toujours gérer plusieurs comptes dans un seul portefeuille pour gestion simple des actifs.
Cette flexibilité fournit un pseudonyme aux utilisateurs pendant que nous expérimentons des primitives préservant la confidentialité pour les versions futures.
Plusieurs comptes appartenant à un seul utilisateur ou à un ensemble d'utilisateurs fournissent également des canaux pour augmenter la simultanéité d'exécution, comme décrit à la Section 7.4.

5.3 Les modules MOVE

Un module Move contient un bytecode Move qui déclare les types de données (structs) et les procédures.
Il est identifié par l'adresse du compte où le module est déclaré avec un nom de module.
Par exemple, l'identificateur du premier module de devise de la figure 2 est 0x1::coin.
Un module peut dépendre d'autres modules on-chain, comme le montre le module de portefeuille de la figure 2, permettant la réutilisation du code.
Un module doit être nommé de manière unique dans un compte, c'est-à-dire que chaque compte peut déclarer au plus un module avec n'importe quel nom donné. Par exemple, le compte à l'adresse 0x1 de la figure 2 n'a pas pu déclarer un autre module nommé coin.
D'autre part, le compte à l'adresse 0x3 pourrait déclarer un module nommé coin et l'identifiant de ce module serait 0x3::coin.
Notez que 0x1::coin::Coin et 0x3::coin::Coin sont des types distincts et ne peuvent pas être utilisés de manière interchangeable ni partager un code de module commun.
En revanche, 0x1::coin::Coin<0x2::wallet::USD> et 0x1::coin::Coin<0x2::wallet::JPY> sont des instanciations différentes du même type générique qui ne peuvent pas être utilisées de manière interchangeable mais peuvent partagées du code de module commun.
Les modules sont regroupés en packages situés à la même adresse.

Un propriétaire de cette adresse publie le package on-chain dans son ensemble, y compris le bytecode et les métadonnées du package.
Les métadonnées du package déterminent si un package peut-être mis à niveau ou s'il est immuable.
Pour un package évolutif, des contrôles de compatibilité sont effectués avant que la mise à niveau ne soit autorisée : aucune fonction de point d'entrée existante ne doit être modifié et aucune ressource ne peut être stockée en mémoire.
Cependant, de nouvelles fonctions et ressources peuvent être ajoutés.
Le framework Aptos, composé des bibliothèques de base et de la configuration de la blockchain Aptos, est défini comme un ensemble de modules pouvant faire l'objet d'une mise à niveau régulière (voir la section 9.2).

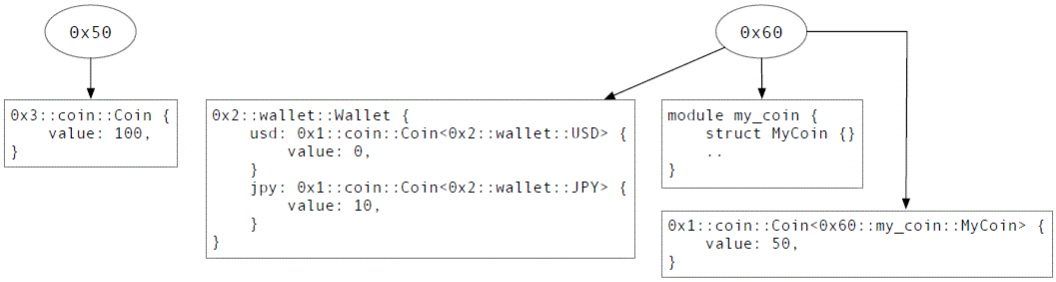

Figure 3: Example on-chain data.

5.4 Ressources

À l'instar des modules, les adresses de compte peuvent également être associées à des valeurs de données.
Au sein de chaque adresse du compte, les valeurs sont saisies par leurs types, avec au plus une valeur de chaque type appartenant au compte.
La figure 3 en est un exemple. L'adresse 0x50 contient une valeur unique, avec 0x3::coin::Coin étant le type entièrement qualifié.
0x3 est l'adresse où le module de pièces est stocké, coin est le nom du module et Coin est le nom du type de données.
Les valeurs des types génériques sont également autorisées avec différentes instanciations traitées comme des types distincts.
Ceci est essentiel pour l'extensibilité, permettant à différentes instanciations de partager le même code fonctionnel.
Les règles de mutation, de suppression et de publication d'une valeur sont codées dans le module qui définit le type de données.
Les règles de sécurité et de vérification de Move empêchent d'autres codes ou entités de créer directement, modifier ou supprimer des instances de types de données définis dans d'autres modules.
Avoir au plus une valeur de niveau supérieur de chaque type sous une adresse peut à première vue sembler limitatif.
Cependant, ce n'est pas un problème dans la pratique car les programmeurs peuvent définir des types de wrapper avec d'autres données en tant que champs internes, évitant ainsi toute limitation.
La structure de Wallet de la figure 3 est un exemple de la façon d'utiliser des types de wrapper.
Il convient également de noter que tous les types de données ne peuvent pas être stockés on-chain.
Pour que les instances de données soient qualifiées en tant que valeurs de niveau supérieur, le type de données doit avoir la capacité Key.
De même, la capacité Store est requise pour les valeurs imbriquées.
Les types de données avec les deux capacités sont également appelés ressources.

5.5 État du grand livre

Du point de vue de la machine virtuelle Move (Move VM), chaque compte se compose d'un ensemble de valeurs et valeurs clés de la structure de données.
Ces structures de données sont appelées entrées de table et sont stockées dans le format BCS (Binary Canonical Serialization Format).
Cette disposition des données permet aux développeurs d'écrire des contrats intelligents (smart contracts) qui peuvent fonctionner efficacement sur de petites quantités de données, répliquées sur un grand nombre de comptes, ainsi que sur de grandes quantités de données stockées dans un petit nombre de comptes.
Les modules MOVE sont stockés de la même manière que les données de compte, mais sous un espace de noms indépendant.
L'état de genèse du grand livre définit l'ensemble initial de comptes et leur état associé lors de l'initialisation de la blockchain.
Au lancement, la blockchain Aptos sera représentée par un seul état de registre. Cependant, au fur et à mesure que l'adoption augmente et la technologie se développe, Aptos augmentera le nombre de partitions pour augmenter le débit (c'est-à-dire activer plusieurs états de registre) et prendre en charge les transactions qui déplacent ou accèdent à des ressources entre des partitions.
Chaque état du grand livre conservera toutes les ressources on-chain pour la partition spécifique et fournira le même modèle de compte avec la granularité adéquate des valeurs de clé offrant des coûts quasi fixes pour l'accès au stockage.

6 Une expérience utilisateur sûre

Pour toucher des milliards d'internautes, l'expérience utilisateur web3 doit être sûre et accessible. Dans les sections ci-dessous, nous décrivons plusieurs innovations fournies par la blockchain Aptos qui travaillent dans ce but.

6.1 Protection de la viabilité des transactions

La signature d'une transaction signifie que le signataire autorise la transaction à être validée et exécutée par la blockchain.
Occasionnellement, les utilisateurs peuvent signer des transactions involontairement ou sans tenir pleinement compte de toutes les façons dont leurs transactions pourraient être manipulées.
Pour réduire ce risque, la blockchain Aptos limite la viabilité de chaque transaction et protège le signataire d'une validité illimitée.
Il y a actuellement trois protections différentes fournies par la blockchain Aptos :

- Le numéro de séquence de l'expéditeur
- Un délai d'expiration de la transaction
- Un identificateur de chaîne désigné.

• Le numéro de séquence d'une transaction ne peut être validé qu'une seule fois pour le compte de chaque expéditeur.
Par conséquent, les expéditeurs peuvent observer que si le numéro de séquence du compte courant est supérieur ou égale au numéro de séquence d'une transaction t, alors soit t a déjà été validé, soit t ne sera jamais validé (car le numéro de séquence utilisé par t a déjà été consommé par une autre transaction).
• « L'heure » de la blockchain avance avec une précision et une fréquence élevée (généralement inférieures à la seconde), comme détaillé au point 7.3.1.
Si « l'heure » de la blockchain dépasse « l'heure » d'expiration de la transaction t, alors de même, soit t a déjà été validé, soit t ne sera jamais validé.
• Chaque transaction a un identifiant de chaîne désigné pour empêcher les entités malveillantes de rejouer des transactions entre différents environnements de blockchain (par exemple, sur un réseau de test et un réseau principal).

6.2 Gestion des clés basée sur les déplacements

Comme indiqué à la section 5.2, les comptes Aptos prennent en charge la rotation des clés, une fonctionnalité importante qui peut aider à réduire :

- Les risques associés à la compromission de clés privées
- Les attaques de longue portée
- Les avancées futures qui pourraient transformer les algorithmes cryptographiques existants.

En outre, les comptes Aptos sont également suffisamment flexibles pour permettre de nouveaux modèles hybrides de sécurité.
Dans l'un de ces modèles, un utilisateur peut déléguer la possibilité de faire pivoter la clé privée du compte pour un ou plusieurs dépositaires et autres entités de confiance.
Un module Move peut alors définir une stratégie qui permet à ces entités approuvées de faire pivoter la clé dans des circonstances spécifiques.
Par exemple, les entités peuvent être représentées par une clé multi-sig « k-out-of-n » détenue par de nombreuses parties de confiance et offrir des services de récupération de clé pour éviter la perte de clé utilisateur (par exemple, 20% de Bitcoin est actuellement enfermé dans des comptes irrécupérables [7]).
De plus, alors que de nombreux portefeuilles prennent en charge divers schémas de récupération de clés tels que :

- La sauvegarde de clés privées sur l'infrastructure cloud
- Le calcul multipartite
- Et à la récupération sociale,

ils sont généralement mis en œuvre sans prise en charge de la blockchain (c'est-à-dire off chain).
Par conséquent, chaque portefeuille doit implémenter sa propre clé de gestion d'infrastructure et les opérations connexes deviennent opaques pour les utilisateurs.
En revanche, la fonctionnalité de gestion de la clé de la couche blockchain Aptos offre une transparence totale de toutes les clés liées et simplifie la mise en œuvre d'un portefeuille avec une gestion riche des clés.

6.3 Transparence de la transaction préalable à la signature

Aujourd'hui, les portefeuilles offrent très peu de transparence sur les transactions qu'ils signent.
Par conséquent, les utilisateurs sont souvent assez simplement amenés à signer des transactions malveillantes qui peuvent entrainer le vol de fonds et avoir des effets dévastateurs.
Cela est vrai même pour les blockchains qui nécessitent d'énumérer toutes les données de la chaîne auxquelles accèdent chaque transaction.
Par conséquent, peu de mesures de protection des utilisateurs sont actuellement en place, ce qui les rend vulnérables à une grande variété d'attaques.
Pour y remédier, l'écosystème Aptos fournit des services de pré-exécution des transactions : une mesure de précaution qui décrit aux utilisateurs (sous une forme lisible par l'homme) les résultats de leurs transactions antérieures avant la signature.
L'association avec un historique connu d'attaques antérieures et de contrats intelligents malveillants vous aidera à réduire la fraude.
En outre, Aptos permet également aux portefeuilles de dicter des contraintes sur les transactions pendant leur exécution.
La violation de ces contraintes entraînera l'interruption des transactions, afin de protéger davantage les utilisateurs d'applications malveillantes ou d'attaques d'ingénierie sociale.

6.4 Protocoles clients légers pratiques

S'appuyer uniquement sur les certificats TLS/SSL des fournisseurs d'API pour établir la confiance entre les blockchains, les clients et les serveurs ne protègent pas suffisamment les clients.
Même en présence de certificats valides, les portefeuilles et les clients n'ont aucune garantie quant à l'authenticité et à l'intégrité des données présentées.

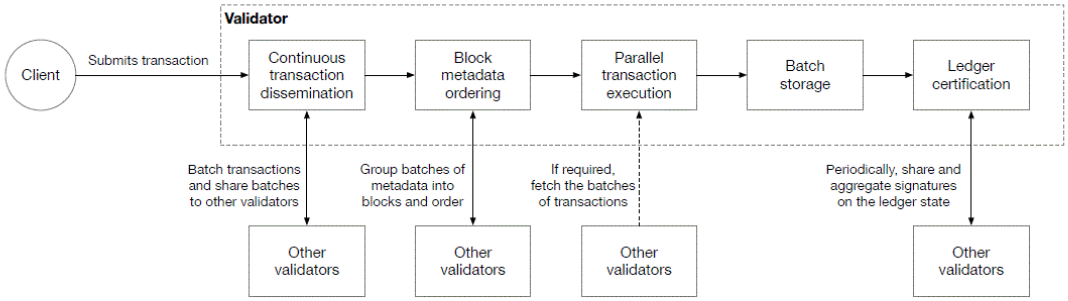

Figure 4: The transaction processing life cycle. All stages are completely independent and are individually parallelizable.

Toutes les étapes sont complètement indépendantes et sont parallélisables individuellement.
Par conséquent, les fournisseurs d'API peuvent renvoyer des données de blockchain incorrectes ou malveillantes, tromper les tiers et effectuer des attaques à double dépense.
Pour éviter cela, Aptos fournit des preuves d'état et des protocoles de vérification client légers qui peuvent être utilisés par des portefeuilles et des clients pour vérifier la validité des données présentées par un serveur tiers non fiable.
De plus, en tirant parti des preuves d'état basées sur l'horodatage de la section 7.6.2, les clients légers peuvent toujours assurer des limites strictes sur la « fraîcheur » de l'état du compte (par exemple, en quelques secondes) et n'avoir besoin que de suivre les modifications de la configuration du réseau (changements d'époque) ou utilisation de points de contrôle approuvés actuels (waypoints) pour rester à jour [8].
En combinant des horodatages à haute fréquence et des preuves d'état peu coûteuses, la blockchain Aptos offre des garanties de sécurité accrues aux clients.
En outre, les nœuds Aptos exposent également des interfaces de stockage riches et hautes performances qui peuvent être optimisées pour établir des preuves d'abonnements ciblant des données et des comptes spécifiques on-chain.
Cela peut être exploité par des clients légers pour conserver un minimum de données vérifiables sans avoir besoin d'exécuter un nœud complet ou traiter un nombre important de transactions.

7 Pipelining, traitement par lots (batch) et traitement parallèle des transactions

Pour optimiser le débit, augmenter la simultanéité et réduire la complexité de l'ingénierie, le traitement des transactions sur la blockchain Aptos est divisée en étapes distinctes.
Chaque étape est complètement indépendante et individuellement parallélisable, ressemblant à des architectures de processeurs modernes et super scalables.
Non seulement cela offre des avantages significatifs en termes de performances, mais permet également à la blockchain Aptos d'offrir de nouveaux modes d'interaction validateur-client.
Par exemple :

- Les clients peuvent être avertis lorsque des transactions spécifiques ont été incluses dans un lot de transactions persistantes
  Les transactions persistantes et valides sont très susceptibles d'être validées de manière imminente.
- Les clients peuvent être informés lorsqu'un lot de transactions persistantes a été commandé. Ainsi, pour réduire la latence de détermination des sorties de transaction exécutées, les clients peuvent choisir d'exécuter les transactions localement plutôt que d'attendre que les validateurs terminent l'exécution à distance.
- Les clients peuvent choisir d'attendre l'exécution certifiée de la transaction par les validateurs et d'exécuter la synchronisation d'état sur les résultats attestés (p. ex., voir rubrique 8).

La conception modulaire d'Aptos facilite la vitesse de développement et prend en charge des cycles de libération plus rapides, car les modifications peuvent être ciblées sur des modules individuels, au lieu d'une architecture monolithique unique.
De même, la conception modulaire fournit également un chemin structuré vers la mise à l'échelle des validateurs au-delà d'une seule machine, fournissant un accès à des ressources de calcul, de réseau et de stockage supplémentaires.
La figure 4 montre le cycle de vie des transactions et les différentes étapes de traitement.

7.1 Traitement par lots

Le traitement par lots est une optimisation importante de l'efficacité qui fait partie de chaque phase opérationnelle dans la blockchain Aptos.
Les transactions sont regroupées en lots par chaque validateur durant la diffusion de la transaction, et les lots sont combinés en blocs via le consensus.

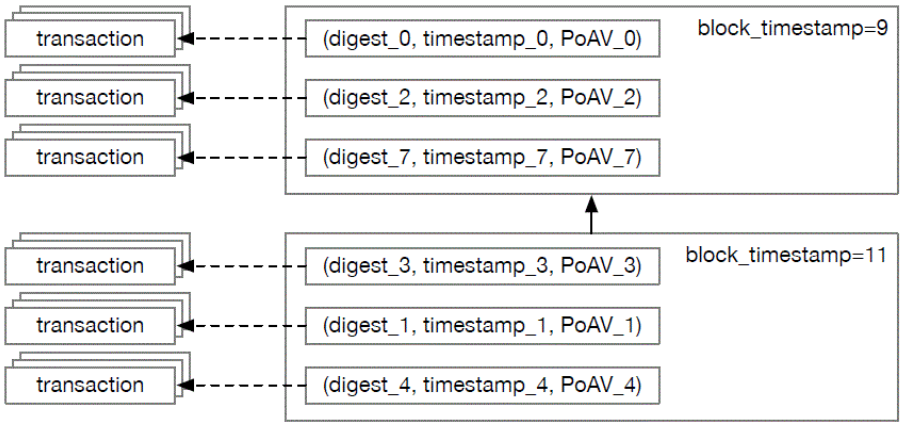

Figure 5: Block metadata ordering occurs independently from transaction dissemination.

L'exécution, le stockage et les phases de certification du grand livre fonctionnent également par lots pour offrir des possibilités de réorganisation, de réduction des opérations (p. ex., le calcul en double ou la vérification de signature) et l'exécution parallèle.
Le regroupement des transactions en lots peut induire de petites périodes de latence, par exemple, attendre 200 millisecondes pour accumuler un lot de transactions avant d'effectuer la diffusion.
Cependant, le traitement par lots est facilement configurable par rapport à une période d'attente maximale et à la taille maximale du lot, ce qui permet au réseau décentralisé d'optimiser automatiquement la latence et l'efficacité.
Le traitement par lots permet également d'optimiser les frais en hiérarchisant les transactions et permet d'éviter les attaques involontaires par déni de service (DoS) de clients trop zélés.

7.2 Diffusion continue des transactions

Selon l'aperçu principal de Narwhal & Tusk [9], la diffusion des transactions dans la blockchain Aptos est découplée du consensus.
Les validateurs se transmettent en continu des lots de transactions les uns aux autres en utilisant simultanément toutes les ressources réseau disponibles.
Chaque lot distribué par un validateur v est persistant, et une signature sur le résumé du lot est renvoyée à v.
Si l'on suit les pré requis du consensus défini au point 7.3, toute signature pondérée au poids de 2 f + 1 sur le lot constitue une preuve de disponibilité (PoAv).
Une telle preuve garantit qu'au moins les f +1 validateurs honnêtes pondérés selon leur poids (défini par quantité de jetons staké) ont enregistré le lot, et ainsi tous les validateurs honnêtes seront en mesure de récupérer ce lot avant l'exécution.
Des lots de transactions persistants à l'infini peuvent ouvrir un vecteur d'attaque DoS en entrainant les validateurs à manquer de stockage et se bloquer.
Pour éviter cela, chaque lot de transactions a un horodatage associé.
L'horodatage sur le lot permet un ramassage efficace des « garbage collector » pour chaque validateur.
De plus, un mécanisme de quota séparé par validateur est conçu pour empêcher les validateurs de manquer d'espace de stockage même dans les circonstances les plus extrêmes, comme lors d'attaques byzantines potentielles.
Les lots aussi ont des contraintes de dimensionnement qui sont validées avant l'accord pour persister dans un stockage stable.
Finalement plusieurs optimisations pour dédupliquer et mettre en cache les transactions réduisent les coûts de stockage et garantissent la performance d'intégration avec le moteur d'exécution parallèle.

7.3 Bloquer l'ordre des métadonnées

Une fausse idée commune consiste à penser que le consensus est lent et que débit et latence constituent donc le principal goulot d'étranglement pour la blockchain.
L'une des innovations clés de la blockchain Aptos est de découpler le désaccord des tâches connexes telles que la diffusion des transactions, les transactions（l'exécution/le stockage) et la certification du grand livre de la phase de consensus.
En découplant la diffusion des transactions de la phase consensus l'ordonnancement peut se faire avec une très faible bande passante (métadonnées de bloc et preuves uniquement), ce qui entraîne des débits de transaction élevés et une latence minimisée.
Aujourd'hui, la blockchain Aptos tire parti de la dernière itération de DiemBFTv4 [10], un protocole de consensus BFT de confiance et réactif.
Le consensus dans le cas commun ne nécessite que deux voyages sur le réseau (avec des temps d'aller-retour généralement inférieurs à 300 millisecondes à travers le monde) et s'ajuste dynamiquement aux validateurs défectueux par le biais d'un mécanisme de réputation de leader [11].
Le mécanisme on-chain de réputation des leaders promeut les validateurs qui ont validé avec succès des blocs dans une fenêtre et rétrograde les validateurs qui ne participent pas.
Ce nouveau mécanisme améliore considérablement les performances dans des environnements décentralisés, fournit une infrastructure adaptée pour des incitations appropriées, et minimise rapidement l'impact des validateurs défaillants sur le débit et la latence.

DiemBFTv4 garantit la vitesse de synchronisation partielle et assure la sécurité en asynchrone lorsque la mise totale du validateur est supérieure ou égale à 3f +1 avec jusqu'à f validateurs défectueux pondérés en fonction de la mise.
DiemBFTv4 a été largement testé sur plusieurs itérations depuis 2019 avec des dizaines d'opérateurs de nœuds et un écosystème multiwallet.
Nous expérimentons également des recherches récentes (par exemple, Bullshark [12]) et d'autres protocoles qui s'appuient sur l'historique des blocs et la communication associée pour déterminer l'ordonnancement et la finalité des blocs de métadonnées.
Un bloc de consensus et une proposition d'horodatage sont émis par un leader et approuvés par d'autres validateurs, comme illustré à la figure 5.
Notez que chaque bloc de consensus contient uniquement les lots de métadonnées et des preuves.
Les transactions réelles ne sont pas requises dans le bloc, car le PoAV garantit que les lots de transactions seront disponibles à la phase d'exécution après la commande (voir section 7.2).
Les validateurs peuvent voter la proposition d'un leader après avoir vérifié que la preuve et les critères de métadonnées de bloc sont remplis (p. ex., horodatage de la proposition ≤ délai d'expiration du bloc).

7.3.1 Temps de la blockchain

La blockchain Aptos adopte un horodatage physique approximatif, convenu, pour chaque bloc proposé et par conséquent, toutes les transactions au sein de ce bloc.
Cet horodatage permet de nombreux cas d'utilisation.
Par exemple :

- Logique dépendante du temps dans les contrats intelligents. Par exemple, un développeur aimerait encoder que toutes les offres sur une vente aux enchères doivent être reçues avant midi le jeudi.
- Comme les oracles publient des données on-chain, un horodatage précis et fiable sur la chaîne est nécessaire pour corréler les événements et gérer les retards à partir de données réelles.
- Les clients peuvent discerner à quel point ils sont à jour par rapport à la blockchain.
Pour des raisons de sécurité, pour éviter les données périmées et les attaques à longue portée, un client doit avoir accès à un horodatage lorsque l'état du compte a été mis à jour.
- L'audit de la blockchain avec un horodatage fiable fournit une forte corrélation avec les événements off-chain tels que s'assurer que les paiements légalement appliqués répondent aux exigences attendues.
- L'expiration de la transaction est basée sur l'horodatage le plus récent validé. Comme mesure de protection supplémentaire pour les transactions client, les clients peuvent sélectionner une heure d'expiration pour une transaction, comme décrit à la section 6.1.

La blockchain Aptos fournit les garanties suivantes en ce qui concerne les horodatages pour toutes les transactions à l'intérieur d'un bloc :

- Le temps augmente de manière monotone dans la blockchain. Autrement dit, si bloc B1 < bloc B2, alors « B1.Temps » < « B2.Temps ».
- Si un bloc de transactions est convenu avec l'horodatage T, alors au moins f + 1 validateurs honnêtes ont décidé que T appartient au passé. Un validateur honnête ne votera sur un bloc que lorsque l'horloge du sien sera ≥ horodatage T. Voir la section 7.2.
- Si un bloc de transactions a un quorum de signatures consensuelles avec un horodatage T, le validateur ne servira pas un tel bloc à d'autres validateurs tant que sa propre horloge ne sera pas ≥ horodatage T.

L'horodatage le plus récent est mis à jour sur chaque bloc validé et utilisé comme horodatage pour toutes transactions dans ce bloc. Lorsque le réseau est synchrone, un bloc de transactions est validé à chaque aller-retour réseau et fournit une mise à jour rapide et une horloge très fiable.
L'ordre dans des blocs de transactions peut être déterminé avec une granularité plus fine si vous le souhaitez.

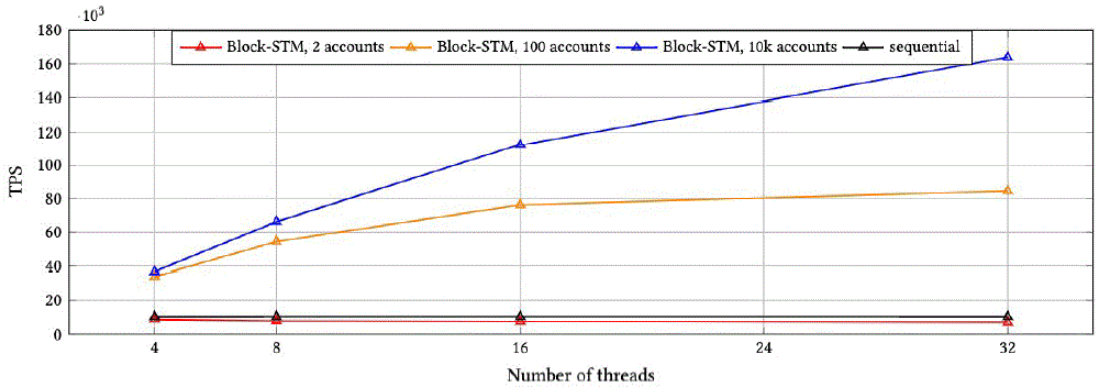

Figure 6: Block-STM (component-only) benchmarks comparing the number of physical cores with different levels of contention.

7.4 Exécution de transactions parallèles

Une fois les métadonnées de bloc de consensus ordonnées, les transactions peuvent être exécutées par n'importe quel validateur, nœud complet ou client.
Au moins 2f +1 validateurs pondérés en fonction du nombre de token stakés ont véritablement persisté dans les transactions le lot proposé.
Étant donné que la diffusion des transactions est continue, d'autres validateurs honnêtes recevront le lot de transactions au fil du temps.
Si un validateur honnête n'a pas reçu les transactions pour le lot en cours au moment où il atteint le stade d'exécution, il peut les télécharger à partir des 2f + 1 validateurs pondérés en fonction du nombre de token stakés, sachant qu'au moins f + 1 validateurs pondérés par le montant staké sont honnêtes (≥ à la moitié de la mise pondérée PoAV des signataires).
Un objectif important pour toute blockchain est de permettre autant d'exécution parallèle que possible.
La blockchain Aptos fait progresser cette composante à partir du modèle de données et du moteur d'exécution.

7.4.1 Modèle de données parallèles

Le modèle de données Move prend en charge en mode natif l'adressage global des données et des modules.
Les transactions qui n'ont pas de conflits de chevauchement dans les données et les comptes peuvent s'exécuter en parallèle.
Compte tenu de la conception par pipeline utilisée par la blockchain Aptos, réorganiser un groupe de transactions peut réduire le nombre de conflits, améliorant ainsi la simultanéité.
Même lorsque les transactions modifient le même ensemble de valeurs on-chain, une grande partie de l'exécution des transactions du processus peut toujours être parallélisée.
La blockchain Aptos introduit un nouveau concept, « l'écart d'écriture », qui décrit une modification de l'état du compte plutôt que l'état du compte modifié (par exemple, incrément d'un entier plutôt que simplement déterminer la valeur finale).
Tout le traitement des transactions peut être réalisé en parallèle, puis les écarts d'écritures sont appliqués dans l'ordre correct pour les valeurs en conflit afin d'assurer des résultats déterministes.
Au fil du temps, la blockchain Aptos continuera d'améliorer le modèle de données de manière à améliorer la simultanéité et également améliorer l'ergonomie, ce qui la rend plus naturelle pour les développeurs pour créer, modifier et composer des valeurs on-chain.
Move offre la flexibilité nécessaire pour effectuer ces améliorations à la fois au niveau du « level » du langage et également grâce à des fonctionnalités spécifiques à la plate-forme.

7.4.2 Moteur d'exécution parallèle

Le moteur d'exécution parallèle Block-STM détecte et gère les conflits pour un ensemble ordonné de transactions et permet un contrôle d'accès simultané de confiance ceci afin de permettre un parallélisme maximal pour un ordonnancement particulier donné [13].
Les lots de transactions sont exécutés en confiance, en parallèle et validés après l'exécution.
Les validations infructueuses conduisent à des réexécutions.
Block-STM utilise une structure de données multi-versions pour éviter les conflits de double écriture.
Toutes les écritures sont stockées au même emplacement avec leurs versions, qui contiennent leurs ID de transaction et le nombre de fois que l'écriture de la transaction a été réexécutée en toute confiance.
Lorsque la transaction tx lit un emplacement de mémoire, elle obtient à partir de la structure de données multi-version la valeur écrite à cet emplacement par la transaction la plus récente qui apparaît avant tx dans l'ordre prédéfini, ainsi que la version associée.
Block-STM est déjà intégré à la blockchain Aptos.
Pour comprendre le plein potentiel de Block-STM en termes de performance, nous avons mené des expériences avec des transactions Move non triviales en peer-to-peer (c.-à-d. 8 lectures et 5 écritures par transaction) via un benchmark isolé, en exécution uniquement (et non de bout en bout) sur une base de données en mémoire.
Dans la figure 6, nous présentons nos résultats d'exécution Block-STM.
Chaque bloc contient 10k transactions et le nombre de comptes déterminent le niveau de conflits et de contention.
En cas de faible contention, Block-STM atteint une accélération de 16 fois par rapport à une exécution séquentielle avec 32 threads, alors qu'en cas de forte contention, Block-STM atteint une accélération de plus de 8 fois supérieure.
Unique en comparaison des autres moteurs d'exécution parallèle dans l'espace blockchain, Block-STM est capable d'extraire le parallélisme inhérent à toute charge de travail, dynamiquement et en toute transparence (sans aucune action de l'utilisateur).
En comparaison des environnements d'exécution parallèles qui nécessitent une connaissance préalable des emplacements de données à lire ou à écrire, le STM peut prendre en charge simultanément des transactions plus complexes.
Cette propriété conduit à moins de transactions mais plus d'efficacité, réduit les coûts et réduit la latence pour les utilisateurs.
Peut-être le plus important, la division d'une transaction atomique en plusieurs petites transactions brise la sémantique du tout ou rien d'une transaction unique avec des résultats d'état complexes.
Le jumelage de la sémantique de transaction expressive avec l'exécution parallèle dans Block-STM permet aux développeurs d'avoir le meilleur des deux mondes.
Notez que l'étape d'ordonnancement des métadonnées de bloc n'empêche pas de réorganiser les transactions dans la phase d'exécution parallèle.
Les transactions peuvent être réorganisées sur un ou plusieurs blocs pour optimiser la simultanéité d'accès lors de l'exécution parallèle. La seule exigence est que la réorganisation doit être pour tous les validateurs honnêtes.
L'optimisation de l'exécution parallèle ainsi que l'ajout de randomisation pour la réorganisation augmentent les performances et potentiellement découragent les techniques dites de valeur extractible maximale (MEV) pour une réorganisation rentable des transactions du validateur.
Les stratégies résistantes aux MEV « commander puis révéler » peuvent également être incorporées dans cette conception de type pipeline.
Block-STM et le réordonnancement des transactions sont des techniques complémentaires pour augmenter l'exécution parallèle.
Ils peuvent être combinés avec des indices d'accès aux transactions en lecture/écriture pour une meilleure complémentarité.

7.5 Stockage par lots

La phase d'exécution parallèle se traduit par des jeux d'écriture pour toutes les transactions d'un groupe.
Ces jeux d'écriture peuvent être stockés en mémoire pour une vitesse d'exécution maximale, puis utilisé comme cache pour le bloc ou le jeu suivant de blocs à exécuter.
Toute écriture qui se chevauche ne doit être écrite qu'une seule fois dans un stockage stable.
Si un validateur échoue avant de stocker les jeux d'écriture en mémoire, il peut simplement reprendre l'exécution parallèle à partir de la phase d'ordonnancement des métadonnées du bloc.
Le découplage des jeux d'écriture du stockage par lot, de l'exécution parallèle, garantit que l'exécution parallèle peut fonctionner efficacement.
En résumé, le traitement par lots des jeux d'écriture réduit le nombre d'opérations de stockage et tire parti d'opérations d'E/S plus efficaces et plus importantes.
La quantité de mémoire réservée à la mise en cache du jeu d'écriture peut être configurée manuellement par machine et fournit un mécanisme de contrepoids naturel.
La granularité des lots peut être différente de celle des blocs d'exécution parallèle si vous souhaitez les optimiser pour des environnements d'E/S et de mémoire spécifique.

7.6 Certification du grand livre

A ce stade du pipeline, chaque validateur individuel a calculé le nouvel état d'un bloc de transactions validé.
Toutefois, pour prendre en charge efficacement les clients légers vérifiés et la synchronisation d'état, la blockchain Aptos implémente la certification du grand livre concernant son historique ainsi que son état.
Une différence clé pour la blockchain Aptos est que la certification du grand livre n'est pas sur le chemin critique du traitement des transactions et peut même être exécuté complètement hors bande si vous le souhaitez.

7.6.1 Certification de l'historique du grand livre

Un validateur ajoute les transactions avec leur sortie d'exécution à un fichier global de structure des données authentifiées du grand livre.
Une partie de l'output d'une transaction constitue le jeu d'écriture d'état, composé des modifications faites à l'état global accessible par Move.
L'authentificateur court de cette structure de données établi une liaison avec l'historique du grand livre, qui comprend le lot de transactions nouvellement exécuté.
Similaire à l'exécution d'une transaction, la génération de cette structure de données est déterministe.
Chaque validateur signe l'authentificateur court dans sa nouvelle version de la base de données.
Les validateurs partagent leur récent ensemble d'authentificateurs courts signés les uns avec les autres, les agrègent collectivement en quorum signés et partagent les quorums signés des authentificateurs courts avec les autres.
À l'aide de cette signature collective, les clients peuvent s'assurer qu'une version de base de données représente l'intégralité de l'historique du grand livre valide et irréversible selon les propriétés BFT du protocole.
Les clients peuvent interroger n'importe quel validateur (ou tout réplica tiers de la base de données, tel qu'un nœud complet) pour lire une base de données et vérifiez le résultat à l'aide de l'authentificateur et d'une preuve des données demandées.

7.6.2 Certification périodique de l'État

L'intégralité de l'état global accessible par Move peut être résumée par un authentificateur court à n'importe quel endroit dans l'historique, semblable à un résumé de l'historique du grand livre.
En raison de la nature d'accès aléatoire à l'état global (contrairement à l'historique du grand livre qui est en annexe uniquement), le coût de maintenance de cette authentification est important.
Néanmoins, lors de la mise à jour de la structure de données dans un lot important, nous pouvons calculer la mise à jour en parallèle et également exploiter tout chevauchement entre les parties qui doivent être mises à jour quand chaque valeur d'état individuel change.
La blockchain Aptos ne certifie délibérément que périodiquement l'état global pour réduire la duplication des mises à jour partagées.
Pendant les intervalles configurés et déterministes, le réseau émet des points de contrôle d'état des transactions qui incluent l'authentificateur d'état global dans le cadre de leur sortie.
Ces versions sont notées points de contrôle d'état.
Plus l'écart entre deux points de contrôle est grand, plus l'amortissement du coût de la mise à jour de la structure de données authentifiée par état et par transaction est faible.
Avec les points de contrôle d'état, on peut lire n'importe quelle valeur d'état en toute confiance sans avoir à stocker l'ensemble des états.
Cette fonctionnalité est utile pour des applications telles que la synchronisation incrémentale des états, le partitionnement du stockage entre les validateurs, les nœuds de validation sans état et les clients légers à stockage limité.
Cependant, étant donné que les points de contrôle d'état sont périodiques, obtenir une preuve d'une version spécifique de l'état du grand livre nécessite soit l'exécution de transactions supplémentaires pour les alternances d'état manquantes, soit une inclusion d'une preuve à partir de l'historique du grand livre authentifié.
Les points de contrôle d'état sont liés aux versions de transaction spécifiques dans l'historique du grand livre, donc liés à l'horodatage associé aux lots de transactions mentionnés à la section 7.
Avec l'horodatage, un client léger peut évaluer l'ancienneté d'une preuve de valeur d'état.
Sans horodatage, un client léger ne peut assurer la validité de la preuve d'un état antérieur qui pourrait être lointaine dans le passé, ce qui fournit peu d'assurance sur la pertinence.
En outre, les horodatages pour les preuves d'état sont nécessaires pour suivre l'historique d'accès et aussi à des fins d'audit du type : calcul du solde horaire moyen des jetons dans une réserve de jetons.
Les points de contrôle d'état peuvent être dérivés d'un point de contrôle d'état précédent et d'alternances d'état dans les sorties de transaction.
Par conséquent, les points de contrôle d'état persistants vers un stockage stable n'ont pas besoin d'être sur le chemin critique pour le traitement des transactions.
En outre, des effets de dosage bénéfiques existent également en cas de points de contrôle d'état persistent.
La mise en cache des points de contrôle d'état récents (ou plutôt du delta entre eux) et le deversement des points de contrôle d'état périodiques vers un stockage stable peut réduire considérablement la consommation de bande passante pour le stockage.
La façon dont les points de contrôle sont choisis pour être conservés n'affecte pas le calcul de la structure de données authentifiées.
Par conséquent, il s'agit d'un choix par nœud : Les opérateurs de nœud peuvent configurer le compromis approprié entre la capacité de mémoire et la bande passante pour le stockage.

8 Synchronisation des états

La blockchain Aptos vise à fournir un système à haut débit et à faible latence pour tous les participants à l'écosystème.
En conséquence, la blockchain doit offrir un protocole de synchronisation d'état efficace pour diffuser, vérifier et conserver les données blockchain aux clients légers, aux nœuds complets et aux validateurs [14].
De plus, le protocole de synchronisation doit également être tolérant aux contraintes de ressources et à l'hétérogénéité au sein du réseau, en tenant compte des différents utilisateurs et cas d'utilisation.
Par exemple, il doit permettre l'archivage pour les nœuds complets afin de vérifier et conserver l'ensemble de l'historique et de l'état de la blockchain, tout en permettant aux clients légers de suivre efficacement un petit sous-ensemble de l'état de la blockchain Aptos.
Pour permettre d'appliquer cette propriété, la blockchain Aptos exploite l'historique du grand livre authentifié et les preuves d'état certifiées (voir Section 7.6.1) offertes par les validateurs, nœuds complets et autres réplicateurs pour fournir un protocole de synchronisation flexible et configurable.
Plus précisément, les participants au réseau peuvent sélectionner différentes stratégies de synchronisation à optimiser en fonction de leurs cas d'utilisation et de leurs exigences.
Par exemple, dans le cas de nœuds complets, Aptos permet plusieurs stratégies de synchronisation, y compris la possibilité de traiter toutes les transactions depuis le tout début ou d'ignorer complètement l'historique de la blockchain et de synchroniser uniquement le dernier état de la blockchain à l'aide de waypoints.
Dans le cas des clients légers, des stratégies consistent à inclure la synchronisation d'états partiels de la blockchain : par exemple des comptes ou des valeurs de données spécifiques, et permet la lecture des états vérifiés : par exemple, la récupération du solde du compte vérifié.
Dans tous les cas, Aptos permet aux participants de configurer la quantité et l'ancienneté des données à récupérer, traiter et conserver.
En adoptant une approche flexible et configurable de la synchronisation d'état, Aptos peut s'adapter à une grande variété d'exigences des clients et continuer à offrir de nouvelles stratégies de synchronisation plus efficaces à l'avenir.

9 Propriété communautaire

La blockchain Aptos sera détenue, exploitée et gouvernée par une communauté large et diversifiée.
Un jeton Aptos natif sera utilisé pour : les frais de transaction et de réseau, le vote de gouvernance sur le protocole, les mises à niveau et les processus on-chain/off-chain, et la sécurisation de la blockchain via un modèle de preuve d'enjeu.
Une description complète de l'économie des jetons Aptos suivra dans une prochaine publication.

9.1 Frais de transaction et de réseau

Toutes les transactions Aptos ont un prix unitaire de gaz (spécifié dans les jetons Aptos) qui permet aux validateurs de prioriser les transactions de la plus haute valeur dans le réseau. De plus, à chaque étape du process, il existe de multiples possibilités d'écarter les transactions de faible valeur (permettant à la blockchain de fonctionner efficacement lorsque le système en a la capacité).
Au fil du temps, des frais de réseau seront déployés pour assurer que les coûts d'utilisation de la blockchain Aptos sont proportionnels aux coûts réels du matériel déployé, sa maintenance et le fonctionnement des nœuds.
De plus, les développeurs auront la possibilité de concevoir des applications avec différents compromis de coûts entre la puissance de calcul, le stockage et la mise en réseau.

9.2 Gouvernance du réseau

Chaque changement et amélioration significatif de fonctionnalité sur la blockchain Aptos passera par plusieurs phases, y compris la proposition, la mise en œuvre, les tests et le déploiement.
Cette structure crée des opportunités permettant aux parties concernées et aux parties prenantes de fournir des commentaires, de partager leurs préoccupations et de faire des suggestions.
La phase finale représentée par le déploiement est généralement réalisée en deux étapes.
Tout d'abord, une version logicielle avec les nouvelles fonctionnalités sera déployée sur chaque nœud, et ensuite la fonctionnalité sera activée, par exemple, via un indicateur de fonctionnalité ou une variable de configuration on-chain.
Chaque déploiement de logiciel par les opérateurs de nœud doit être rétro compatible afin de garantir que le nouveau le logiciel est interopérable avec les versions prises en charge.
Le processus de déploiement d'une nouvelle version du logiciel peut s'étendre sur plusieurs jours, pour tenir compte des opérateurs dans différents fuseaux horaires et de tout problème externe.
Une fois qu'un nombre suffisant de nœuds a été mis à niveau, l'activation de la nouvelle fonctionnalité peut être déclenchée par un point de synchronisation, tel qu'une hauteur de bloc annoncée ou un changement d'époque.
En cas d'urgence (par exemple, lorsque le temps d'arrêt est inévitable), l'activation peut être manuelle et forcée via un changement à opérer par les opérateurs de nœuds, et dans le pire des cas, un hard fork sur le réseau.
Par rapport à d'autres blockchains, la blockchain Aptos encode sa configuration on-chain.
Chaque validateur a la capacité de se synchroniser avec l'état actuel de la blockchain et de sélectionner automatiquement la configuration correcte (par exemple, le protocole de consensus et la version du framework Aptos) en fonction de la configuration actuelle basée sur les valeurs sur la chaîne.
Les mises à niveau de la blockchain Aptos sont transparentes et instantanées grâce à cette fonctionnalité.
Pour fournir flexibilité et configurabilité au processus d'activation, la blockchain Aptos soutient la gouvernance on-chain pour laquelle les détenteurs de jetons peuvent voter en fonction de leur balance de jetons.
Les protocoles de vote on-chain sont publiques, vérifiables et peuvent être instantanés.
La gouvernance on-chain peut également prendre en charge l'activation de résultats non binaires sans déploiement de logiciels.
Par exemple, les paramètres du protocole d'élection des chefs de file on-chain peuvent être modifiés avec une gouvernance on-chain alors que le point de synchronisation ne serait pas en mesure de gérer les modifications dynamiques, car toutes les modifications doivent être connus à l'avance.
La gouvernance on-chain peut au fil du temps être déployée sur l'ensemble du processus de gestion des mises à niveau.
À titre d'exemple :

1. Les détenteurs de jetons votent on-chain sur la transition vers un nouveau système de signature résistant au quantique.
2. Les développeurs implémentent et vérifient le nouveau schéma de signature et créent une nouvelle version du logiciel.
3. Les validateurs mettent à niveau leur logiciel vers la nouvelle version.
4. Les détenteurs de jetons votent on-chain pour activer le nouveau schéma de signature, la configuration sur la chaîne est mise à jour et la modification prend effet.

En tant que projet open source, la blockchain Aptos dépendra des commentaires de la communauté et utilisera la gouvernance on-chain pour gérer les processus appropriés.
L'activation de la mise à niveau off-chain peut toujours être exigées sous certaines conditions, mais seront réduites au minimum au fil du temps.

9.3 Consensus sur la preuve d'enjeu

Pour participer à la validation des transactions sur la blockchain Aptos, les validateurs doivent avoir une quantité minimum requise de jetons Aptos stakés.
Les montants stakés ont un poid proportionnel à la mise 2f + 1 PoAv pondéré pendant la diffusion de la transaction, il en va de même pour le poid des votes et la sélection des leaders pendant les ordre des blocs de métadonnées.
Les validateurs décident de la répartition des récompenses pour eux et leurs stakers respectifs.
Les stakers peuvent sélectionner n'importe quel nombre de validateurs dans lesquels miser leurs jetons pour un partage des récompenses convenu à l'avance. À la fin de chaque époque, les validateurs et leurs stakers respectifs recevront leurs récompenses via les modules Move on-chain.
Tout opérateur de validation avec une participation suffisante peut rejoindre librement la blockchain Aptos.
Tous les paramètres, y compris la mise minimale requise, peut être définie par les processus d'activation sur la chaîne décrite dans la Section 9.2.

10 Performances

Comme mentionné dans la section 7, la blockchain Aptos est capable d'atteindre un débit optimal avec un matériel performant grâce à son pipeline de traitement des transactions parallèle, optimisé par lots et modulaire.
De nouvelles innovations, telles que les mises à niveau de consensus, les écritures des écarts (delta), les choix de transaction et la mise en cache du chemin critique continuera d'augmenter le débit et d'améliorer l'efficacité au fil du temps.
Aujourd'hui, le débit de la blockchain est généralement mesuré en transactions par seconde.
Cependant, étant donné le large éventail de coûts et de complexité entre les transactions et les infrastructures, c'est une méthode imprécise de comparaison des systèmes.
La latence des transactions est tout autant imprécise que l'envoi du point de départ et du point d'arrivée pour l'exécution de la transaction varient d'une expérience à l'autre.
En outre, certains systèmes nécessitent a priori une connaissance des entrées et des sorties de transaction et forcent les transactions logiques à être divisées en transactions plus petites et moins complexes.
Fractionner les résultats d'une transaction entraine une mauvaise expérience utilisateur et impacte artificiellement la latence et le débit sans tenir compte de ce que le développeur essaie d'accomplir.
En revanche, l'approche Aptos consiste à permettre aux développeurs de librement construire sans limites et de mesurer le débit et la latence à partir d'une utilisation réelle des cas plutôt que des transactions synthétiques.
La blockchain Aptos continuera d'optimiser les performances des validateurs individuels, de même que l'expérimentation avec des techniques de mise à l'échelle qui via l'ajout plus de validateurs au réseau.
Les deux directions ont des compromis.
Toute blockchain avec des capacités d'exécution parallèle peut prendre en charge une concurrence supplémentaire nécessitant un matériel plus puissant ou même de structurer chaque validateur comme un cluster de machines individuelles.
Cependant, il existe des limites pratiques au nombre de validateurs globaux qui est proportionnel au coût et à la complexité pour les opérateurs de validation.
L'essor et la popularité des bases de données sans serveur dans les services cloud illustrent comment quelques entités sont capables de déployer et de maintenir efficacement ces types de systèmes distribués complexes.

10.1 Sharding d'état homogène

Initialement, la blockchain Aptos sera lancée avec un seul état de registre.
Au fil du temps, le réseau Aptos adoptera une approche unique de l'évolutivité horizontale tout en maintenant la décentralisation.
Cela se produira via plusieurs états de registre partitionnés, chacun offrant une API homogène et un concept de partitionnement de première classe.
Le jeton Aptos sera utilisé pour les frais de transaction, le staking et la gouvernance sur tous les Shards.
Les données peuvent être transférées entre les Shards par un pont homogène.
Les utilisateurs et les développeurs peuvent choisir leurs propres schémas de partitionnement en fonction de leurs besoins.
Par exemple, les développeurs peuvent proposer une nouvelle partition ou un nouveau cluster d'utilisateurs au sein de partitions existantes pour obtenir des connexions intra-partition.
En outre les partitions peuvent avoir des caractéristiques systèmes différentes.
Une partition peut être optimisée pour le calcul avec des disques SSD, et une autre pourrait être optimisé via des disques de grande capacité avec de faibles performance de calcul.
En fournissant de la flexibilité matérielle entre les différentes partitions, les développeurs peuvent tirer parti des caractéristiques systèmes appropriés à leurs applications.
En résumé, le partitionnement d'état homogène offre le potentiel d'évolutivité horizontale du débit, permet aux développeurs de programmer avec un seul état universel sur les partitions et permet aux portefeuilles d'intégrer facilement des données partitionnées pour leurs utilisateurs.
Cela offre également des avantages significatifs en termes de performances via la simplicité d'une plate-forme unique unifiée de contrats intelligents Move.

Références

[1] « Aptos-core », 2022. [En ligne]. Disponible: https://github.com/aptos-labs/aptos-core
[2] « Move », 2022. [En ligne]. Disponible: https://github.com/move-language/move
[3] D. Matsuoka, C. Dixon, E. Lazzarin et R. Hackett. (2022) Présentation du rapport 2022 sur l'état de la cryptographie. [En ligne]. Disponible: https://a16z.com/tag/state-of-crypto-2022/
[4] Z. Amsden, R. Arora, S. Bano, M. Baudet, S. Blackshear, A. Bothra, G. Cabrera, C. Catalini, K. Chalkias, E. Cheng, A. Ching, A. Chursin, G. Danezis, G. D. Giacomo, D. L. Dill, H. Ding, N. Doudchenko, V. Gao, Z. Gao, F. Garillot, M. Gorven, P. Hayes, J. M. Hou, Y. Hu, K. Hurley, K. Lewi, C. Li, Z. Li, D. Malkhi, S. Margulis, B. Maurer, P. Mohassel, L. de Naurois, V. Nikolaenko, T. Nowacki, O. Orlov, D. Perelman, A. Pott, B. Proctor, S. Qadeer, Rain, D. Russi, B. Schwab, S. Sezer, A. Sonnino, H. Venter, L. Wei, N. Wernerfelt, B. Williams, Q. Wu, X. Yan, T. Zakian et R. Zhou, « La blockchain libra », 2019. [En ligne]. Disponible: https://developers.diem.com/papers/the-diem-blockchain/2020-05-26.pdf
[5] S. Blackshear, E. Cheng, D. L. Dill, V. Gao, B. Maurer, T. Nowacki, A. Pott, S. Qadeer, D. R. Rain, S. Sezer, T. Zakian et R. Zhou, « Move: A language with programmable resources », 2019. [En ligne]. Disponible: https://developers.diem.com/papers/diem-move-a-language-with-programmableresources/18/06/2019.pdf
[6] D. Dill, W. Grieskamp, J. Park, S. Qadeer, M. Xu et E. Zhong, « Fast and reliable formal verification » des contrats intelligents avec le prouveur de déménagement », dans Outils et algorithmes pour la construction et l'analyse de Systems, D. Fisman et G. Rosu, Eds. Cham: Springer International Publishing, 2022, pp. 183-200.
[7] N. Popper. (2021) Les mots de passe perdus verrouillent les millionnaires hors de leur fortune bitcoin. [En ligne]. Disponible: https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html
[8] The Diem Team, « State synchronization and verification of committed information in a système avec reconfigurations », 2020. [En ligne]. Disponible: https://github.com/aptos-labs/aptoscore/blob/main/documentation/tech-papers/lbft-verification/lbft-verification.pdf
[9] G. Danezis, L. Kokoris-Kogias, A. Sonnino et A. Spiegelman, « Narwhal and tusk: A dag-based » mempool and efficient bft consensus », dans Actes de la dix-septième Conférence européenne sur Systèmes informatiques, ser. EuroSys '22. New York, NY, États-Unis: Association for Computing Machinery, 2022, p. 34 à 50. [En ligne]. Disponible: https://doi.org/10.1145/3492321.3519594
[10] The Diem Team, « Diembft v4: State machine replication in the diem blockchain », 2021. [En ligne]. Disponible: https://developers.diem.com/papers/diem-consensus-state-machine-replication-in-the-diemblockchain/17/08/2021.pdf
[11] S. Cohen, R. Gelashvili, L. Kokoris-Kogias, Z. Li, D. Malkhi, A. Sonnino et A. Spiegelman, « Soyez conscients de vos dirigeants », CoRR, vol. abs/2110.00960, 2021. [En ligne]. Disponible: https://arxiv.org/abs/2110.00960
[12] A. Spiegelman, N. Giridharan, A. Sonnino et L. Kokoris-Kogias, « Bullshark: Dag bft protocols made pratique », dans Actes de la 20e Conférence sur la sécurité informatique et des communications (CCS), ser. CCS '22. Los Angeles, CA, États-Unis: Association for Computing Machinery, 2022.
[13] R. Gelashvili, A. Spiegelman, Z. Xiang, G. Danezis, Z. Li, Y. Xia, R. Zhou et D. Malkhi, « Block-stm: Mettre à l'échelle l'exécution de la blockchain en transformant la malédiction de l'ordre en une bénédiction de performance », 2022. [En ligne].
Disponible: https://arxiv.org/abs/2203.06871
[14] J. Lind, « L'évolution de la synchronisation d'état : le chemin vers plus de 100 000 transactions par seconde avec des sous-secondes latence à aptos », 2022. [En ligne]. Disponible: https://medium.com/aptoslabs/52e25a2c6f10