Lamden: un cadre pour le développement rapide et le déploiement de technologies blockchain.

Stuart Farmer[[1]](#footnote-1)

Mario Hernandez[[2]](#footnote-2)

James Munsch[[3]](#footnote-3)

Le développement de l'application blockchain est inutilement difficile, en partie en raison de la nouvelle technologie, mais aussi pour certaines limitations imposées sur le statu quo actuel de la façon dont les blockchains sont utilisées aujourd'hui. Dans cet article, nous discutons les problèmes liés aux implémentations de blockchains actuelles et une solution à ces problèmes. Nous présentons Lamden: un progiciel de développement qui comprend un générateur de blockchain, des outils de collaboration communautaire et une communication chaîne-chaîne indépendante pour créer de vastes réseaux d'applications de blockchain qui peuvent transférer tout actif à travers eux.

**Mots-clés:** décentralisation, crypto-monnaie, systèmes distribués.

# Motivation

Au cours des dernières années, nous avons vu un afflux de technologies blockchains frapper le marché. Ces technologies sont considérées comme un moyen de mettre fin aux systèmes bancaires et financiers centralisés. Cependant, ces blockchains reposent sur des systèmes défectueux qui ne tiennent pas compte de l'application de ces technologies dans l'espace d'infrastructure actuel. En conséquence, la technologie blockchain est séparée des systèmes financiers traditionnels et, de ce fait, elle est irrégulièrement entravée en atteignant son but final.  
Le projet Lamden est un effort pour créer des outils de développement de logiciels qui augmentent l'adoption massive de la technologie blockchain, de sorte que l'infrastructure peut révolutionner les systèmes de marché et provoquer une innovation réaliste sur les marchés.

Dans notre livre blanc, nous offrons nos critiques sur l'état actuel des marchés et sur la façon dont nous prévoyons d'améliorer cet espace.

**Problèmes avec les implémentations**

**blockchain actuelles**

Il existe de nombreux défauts fondamentaux avec l'architecture blockchain qui l'empêche de devenir une technologie traditionnelle. Ceux existent du côté de l'utilisateur ainsi que du côté du développeur / fournisseur de services. Les domaines dans lesquels nous améliorons les implémentations de blockchain actuelles sont mis en évidence.

**Les frais de transaction**

Tout d'abord, examinons le problème avec les frais de transaction du point de vue de l'utilisateur final. La clé du succès dans le cryptoespace est l'adoption massive de Bitcoin sur le marché international. Au moment de l'écriture, les frais de transaction moyens pour une transaction Bitcoin sont d'environ 6%. Par rapport aux systèmes centralisés tels que PayPal, Mastercard et Visa, Bitcoin est environ deux fois plus cher.

Il convient de noter que les fondamentaux de la crypto’monnaie sont les raisons pour lesquelles les utilisateurs se sentent justifiés avec cet écart. La nature décentralisée de la propriété l'emporte sur les coûts supplémentaires. Cependant, sur une échelle macroéconomique, l'efficacité des coûts l'emporter sur l'allure fondamentale.

"Mais qu'en est-il d'Ethereum? Leurs frais de transaction ne sont que de 0,3%! "

Bien que cela soit vrai, Ethereum n'a pas été conçue comme un réseau de transfert de valeur comme Bitcoin, mais plutôt un réseau de contrats intelligents pour permettre des progiciels sans confiance et décentralisés. Nous devons nous rappeler que les utilisateurs paient plutôt le nombre d'opérations qui se produisent sur la chaîne et que ce nombre d'opérations continue d'augmenter à mesure que des contrats intelligents de plus en plus complexes sont déployés.

Un point de vente majeur d'Ethereum était la possibilité d'ajouter des contrats intelligents comme des «bibliothèques» qui fonctionnent de la même manière que les frameworks d'autres piles de développement de logiciels, qui automatise les opérations et les processus, de sorte que les utilisateurs ne doivent pas les réécrire encore et encore. Ainsi, nous pouvons supposer en toute sécurité que, au fil du temps, à mesure que des contrats intelligents plus complexes sont réalisés et que plus de bibliothèques sont intégrées, le coût de l'interaction avec la chaîne de blocage Ethereum principale. Ce mécanisme, en chargeant les développeurs sur les opérations, désintègre l'innovation et les systèmes de contrat intelligents complexes qu'Ethereum doit être un succès à long terme.

**Chaînes gonflées**

En continuant avec le modèle Ethereum, car le Ledger est public, tout le monde peut déployer les contrats intelligents qu'ils souhaitent. En conséquence, même si la chaîne de bloc n'est que de deux ans, la taille d'un nœud complet est de 242 Gb, ce qui est encore plus grand que la taille actuelle d'un nœud complet Bitcoin d'environ 152 Gb. Le fait d'installer un nœud complet, ou au moins une chaîne légère qui est encore autour de 20Gb de données, est une barrière d'entrée élevée pour quelqu'un qui veut simplement se débrouiller dans un développement de contrats intelligents.

Comparez le temps nécessaire pour synchroniser complètement un nœud avec le temps qu'il faut pour installer Python, Node.js ou tout autre environnement de programmation pour commencer à fouiller. L'inconvénient et la taille du téléchargement sont inviolables pour la plupart des développeurs et des entreprises, sans parler de l'utilisateur moyen curieux de la technologie blockchain.

**Transactions par Seconde (Évolutivité)**

Les chaînes de blocs modernes ont un taux de débit notoirement faible, ce qui entraîne une ralentissement des temps de transaction et une accumulation de transactions en attente pour s'accumuler. Il s'agit d'un remplacement inacceptable pour les systèmes financiers actuels qui traitent des millions de transactions par jour.

Par exemple, Bitcoin a un rendement de 3 transactions par seconde. De même, Ethereum possède seulement 15 transactions par seconde. En comparaison, PayPal a publié une étude de cas en mai 2015 où ils ont pu créer un taux de rendement de plus d'un milliard de transactions par jour. Cela se traduit par environ 11 600 transactions par seconde.

Cela dissuade les entreprises qui traitent des actifs dans une structure de base de données à haut rendement traditionnelle pour sacrifier la capacité aux bénéfices d'une maintenance record.

**Efficacité de minage et des ressources**

Une autre barrière à l'adoption en masse est la fonction de hachage arbitraire que les plates-formes de minage effectuent pour «prouver le travail». Ces machines absorbent des quantités massives de ressources dans les coûts de l'énergie qui n'ont aucun sens pour l'utilisateur standard de l'entreprise. Alors qu'il s'agit d'une approche de la distribution de jetons et de pièces de monnaie sur une chaîne principale, elle ne se traduit pas par le contexte commercial où les ressources en capital sont optimisées. Un traitement inefficace n'a aucun sens pour l'entreprise moderne et, par conséquent, ces types de fonctions de hachage inutiles empêchent une adoption généralisée.

**Intégration et Adoption**

Le logiciel Blockchain est très nouveau et les ressources en capital humain sont rares. Il requiert une personne très hautement technique et spécialisée pour consulter et développer des applications blockchain. Par rapport à d'autres types de bases de données dans un contexte d'entreprise, la mise en place d'un blockchain prend beaucoup de temps et coûte cher.

Alors que la plupart des systèmes de base de données modernes suivent un paradigme de développement et de déploiement similaire, les blockchains sont tellement différentes qu'il n'existe actuellement pas de solution pour transformer le processus de développement en quelque chose qui ressemble à d'autres systèmes de base de données sur le marché.

En outre, les environnements de développement, les gestionnaires de paquets, les suites de test, l'environnement d'intégration continu, etc. qui existent pour presque toutes les autres plates-formes technologiques existantes n'existent pas pour le logiciel blockchain. Cela empêche les organisations d'intégrer cette technologie dans leur flux de travail actuel.

**Migration, Mises à Jour et Vérification Future**

Pour de nombreux intéressés dans les technologies blockchains pour leurs entreprises, le manque de capacité à migrer des données vers une nouvelle chaîne, ou à mettre à jour à un moment qui est le mieux pour une entreprise, est un piège. Les personnes intéressées par les systèmes mainchain et ledger public dépendent de fondations pour libérer de nouveaux codes ou de la communauté décentralisée où il y a peu d'autorité ou de certitude pour le résultat. En outre, essayer de différents systèmes pour voir ce qui fonctionne le mieux pour une organisation est encombrant.

# La Solution

Le Projet Lamden propose la création d'une suite d'outils de développement qui permet le développement et le déploiement rapides de systèmes blockchain privés qui imitent le processus de développement moderne présenté dans des piles technologiques telles que Node.js ou Python qui fournissent une pléthore d'outils faciles à utiliser. et une documentation robuste, et des communautés de soutien très populaires.

Le projet est divisé en trois sections, Saffron, Flora et Clove, qui ajoutent chacun une couche à l‘objectif final de fournir des chaînes de blocs hypertextes pour le développeur pour tester, expérimenter et déployer à travers un réseau d'autres systèmes blockchain.

Saffron est l'outil générateur de déploiement de chaînes privées sur un réseau interne sans tracas. Flora est un référentiel central pour les paquets et modèles de contrats intelligents, les services de nommage de chaînes privées et la découverte de blockchains. Clove est le réseau qui gère les processus de swap de canaux de paiement entre chaînes et facilite la communication entre les applications de blocchains sur le réseau d'une manière qui reste sans confiance et décentralisée.

**Saffron: Un outil générateur**

Au lieu d'avoir un seul réseau principal qui souffre des problèmes mentionnés ci-dessus, la rupture des blockchains dans des cas d'utilisation individuelle et leur interaction s'impose lorsque cela s'avère nécessaire pour résoudre de nombreux problèmes avec un faible taux d'adoption de blockchains. Par exemple, une organisation aurait sa propre blockchain pour leur propre application Web. Cela leur permet d'avoir un contrôle total sur la technologie qu'ils utilisent et de consacrer leurs propres ressources informatiques à l'exécution de cette chaîne de blocblockchain, plutôt que de gaspiller les efforts sur une chaîne principale. En outre, le «gaz» dans le cas d'une chaîne Ethereum peut être éliminé et la difficulté d'un réseau peut être réduite à un niveau plus raisonnable, permettant ainsi des transactions gratuites dans leur application. Cela rend une blockchain plus comme un serveur web qu'une chaîne traditionnelle et peut alors être utilisée pour remplacer et mettre à niveau les structures de base de données existantes en interne.

**Motivation pour un Consensus Indépendant**

Ce qui fait que la technologie blockchain fonctionne, c'est le fait que les mineurs sont des acteurs indépendants qui vérifient les transactions qui se produisent, de sorte qu'il est presque impossible d'injecter de fausses informations dans la chaîne. Cependant, dans les contextes traditionnels, les mineurs sont récompensés en crypto-monnaie par rapport aux frais de transaction. Parce que les transactions sont gratuites sur le protocole de Lamden, un mécanisme de récompense différent doit être instillé afin que les mineurs soient toujours motivés à effectuer une vérification indépendante des transactions.

Il est possible de créer une preuve de travail, une preuve de mise en jeu et tout autre programme gratifiant en utilisant des contrats intelligents. De cette façon, un contrat intelligent peut être appelé à calculer la récompense et le destinataire, et récompenser tout type d'actif sur la chaîne. Au lieu de simplement la monnaie native de la chaîne (qui est initialement Ether), des jetons ERC20 ou des implémentations nouvelles de cryptoasset peuvent également être récompensés, offrant encore plus de personnalisation aux chaînes privées. Et parce que les transactions et le gaz sont gratuits sur les réseaux, appeler un contrat d'un bloc, par exemple, n'est pas coûteux.

pragma solidity ^0.4.15;  
  
contract RewardedAsset {  
 string public constant symbol = "AU";  
 string public constant name = "Digital Gold";  
 uint8 public constant decimals = 0;  
 uint256 \_totalSupply = 1000000000;  
 uint8 public reward = 10;  
 uint256 lastBlock;  
  
 address public owner;  
 mapping(address => uint256) balances;  
 mapping(address => mapping (address => uint256)) allowed;  
  
 function disperseRewards (bool success) onlyOwner() {  
 if (lastBlock < block.number) {  
 \_totalSupply += reward;  
 balances[block.coinbase] += reward;  
 lastBlock = block.number;  
 }  
 }

}

**Outil Générateur**

Saffro prend des files d'attente de conception à partir d'autres outils CLI (interface de ligne de commande) de gestion de paquets tels que pip, yeoman et npm pour générer des blockchains privées comme leurs propres projets de développement. La génération à travers le CLI pris est aussi simple que 'Saffron init'. Grâce à cette application CLI, vous pourrez interagir avec la chaîne dans une API simplifiée qui résume la plupart des complexités des technologies blockchains de votre part.

La technologie blockchain initiale que nous mettons en œuvre est Ethereum, de sorte que les développeurs pourront initialiser ces chaînes, créer des comptes, des blocs de mine et déployer des contrats dans une instance sous-traitée de geth, le client d'Ethereum écrit en Go.

En abstraction des principaux composants d'interaction loin de geth dans un outil CLI, nous sommes en mesure de fournir un service API RESTful pour interagir avec ces chaînes privées. Une API RESTful permet à des blockchains d'interagir à travers l'Internet dans n'importe quelle interface de langage de programmation. Si un langage de programmation prend en charge les requêtes HTTP, ils pourront interagir avec les chaînes privées générées par Lamden. Cela permet l'intégration dans n'importe quelle pile de technologie et nous permet de créer des bibliothèques pour de nombreux frameworks de langue modernes tels que Swift pour le développement iOS, Java pour le développement Android, et même intégré aux applications C pour Internet de choses.

En outre, Saffron fournira un serveur local avec un explorateur Ethereum blockchain qui peut être confronté au public afin que la communauté élargie puisse surveiller et voir l'activité sur la chaîne.

Un service Web pour gérer la chaîne à partir d'une interface Web graphique similaire à Parse sera également inclus dans la boîte.

Des instances déployables optionnelles de IPFS / IPNS et Tor.

**Déploiement**

Après le développement d'une chaîne privée, une organisation souhaitera empiler et déployer celle-ci de manière intégrée dans ses piles techniques internes. Pour ce faire, Saffron exporte des fichiers Docker pour un déploiement rapide.

**Architecture**

Au-delà de la création d'une instance de chaîne privée, Saffron contient les méthodes nécessaires pour accepter les transactions de canaux de paiement et interagir avec la chaîne Lamden plus grande. Ainsi, Saffron doit être considéré comme un type d'interface. Chaque instance de Lamden Wrapper doit se conformer adéquatement à un ensemble de protocoles de surveillance et d'interaction pour garantir que la chaîne est sans confiance et que les transactions peuvent être confirmées indépendamment.

Si le composant Saffron peut atteindre ces fonctionnalités, le pilote blockchain interne ne doit pas être basé sur Ethereum. Dans le futur, Saffron soutiendra des technologies de chaînes de blocs arbitraires telles que Bitcoin, Litecoin, Zcash, Monero, Neo, Tezos, Eos et plus, pour autant qu'elles puissent supporter les chaînes de paiement de manière sans confiance. Même les nouvelles technologies blockchains qui adhèrent au protocole wrapper seront prises en charge, créant ainsi un réseau d'interconnexion bloc-bloc-bloc-blocs entièrement personnalisé.

Le Wrapper finira par supporter toute technologie blockchain tant qu'elle adhérera à certaines spécifications afin qu'elle puisse interagir avec Clove. Ce futur attribue le système Lamden afin que, peu importe les technologies existantes à l'avenir, il y aura toujours un réseau pour interagir avec eux. Cela résout également le problème de la migration des blockchains, car les entreprises et les applications peuvent passer aux derniers projets et à la technologie blockchain lorsqu'ils se retrouvent sur la concurrence.

**Flora: Gestionnaire de paquets décentralisés et dépôts publics**

Mis à part la simple génération de blockchains, le principal moteur de l'adoption de la technologie n'est pas le principal cas d'utilisation de la technologie de base, mais plutôt les communautés environnantes et les ensembles de caractéristiques créés par elles. Vous pouvez le voir avec la communauté Ethereum et plus avec les nouveaux systèmes de contrats intelligents qui commencent à stimuler l'innovation. Leurs mécanismes de crypto-monnaie ne sont pas ce qui les distingue de Bitcoin ou Litecoin. Au lieu de cela, c'est la communauté de développement entourant et développant des applications de contrats intelligents qui permettent une adoption plus large.

De même, les référentiels de paquets qui permettent aux utilisateurs de tirer des paquets de la communauté dans son ensemble, de les commenter et même de développer pour eux solidifient une base de capital intellectuel qui mène à la réussite du projet et une plus grande innovation dans le domaine.

Flora a pour but d'héberger un dépôts de paquets décentralisés, un système d'espace de noms et un outil de découverte pour que les développeurs de chaînes Lamden puissent se connecter avec d'autres développeurs, se défendre de leurs innovations et conduire à un état supérieur de crypto-monnaie.

**Gestionnaire de paquets publics**

pragma solidity ^{{solidity\_version}};  
  
contract {{contract\_name}} {  
 string public constant symbol = "{{symbol}}";  
 string public constant name = "{{asset\_name}}";  
 uint8 public constant decimals = 18;  
 uint256 \_totalSupply = {{total\_supply}};  
  
 address public owner;  
 mapping(address => uint256) balances;  
 mapping(address => mapping (address => uint256)) allowed;  
   
   
...  
  
  
{  
 'solidity\_version':'0.4.15',  
 'contract\_name':'Testcoin',  
 'symbol':'TST',  
 'asset\_name':'Testcoin',  
 'total\_supply':'1000000'  
}

Comme d'autres suites de développement, Lamden a la possibilité de créer des paquets de contrats intelligents. À l'aide d'un système de modélisation de macro, nous pouvons résumer des types communs de contrats de Solidité tels que les jetons ERC20, les services Ethereum Name et l'échange décentralisé d'Etherdelta, les intégrer à des contrats qui ne font qu'un ensemble d'arguments et permettent le déploiement dans les chaînes privées aussi simple que d'exécuter 'hpm install ens' à partir d'une console CLI, ou d'envoyer une requête API pour faire la même chose dans le tableau de bord administratif inclus dans Saffron. Cela supprime les maux de tête du redéploiement des contrats intelligents couramment utilisés et permet l'emballage d'applications intelligentes très complexes pour une distribution rapide.

Au fur et à mesure que plus blockchains sont ajoutées au Wrapper, le support de leurs langues contractuelles sera également ajouté au Hub. Les développeurs peuvent télécharger leurs propres contrats pour soutenir la communauté. L'interaction avec le Hub sera au-dessus du système de fichiers interplanétaires (IPFS) afin que tous les services restent distribués et décentralisés.

**Service de répertoire des noms**

Les chaînes devront communiquer entre elles pour exécuter des canaux de paiement. Pour ce faire, un service de nommage doit être mis en œuvre. Ce service de nommage attribue un nom commun et une paire de clés à chaque chaîne afin que d'autres chaînes puissent les découvrir et leur signer des demandes de transaction.

En outre, les utilisateurs pourront rechercher et découvrir de nouvelles applications blockchain. Il s'agit de chaînes privées développées avec Saffron qui ont été reliées à Clove. Chacune de ces chaînes pourra s'inscrire à un nom et compléter un profil sur son service qui peut inclure des liens vers des sites de marketing, des informations de connexion pour les mineurs, et toute autre chose qui amènerait les utilisateurs à des informations plus précieuses sur leur service. Ce nom sera utilisé pour localiser et envoyer des informations à travers Clove pour les transactions de paiement, l'interaction avec les chaînes et l'utilisation générale du jeton natif Lamden.

Nous avons également exploré les options d'utilisation du Token pour que d'autres développeurs puissent enregistrer leurs modules sur lesquels les métriques d'utilisation pourraient générer des liquidités symboliques entre les membres de la communauté des développeurs.

**Clove: Routeur Anonyme Permettant l'Interfaçage Chaîne-Chaîne**

Le principal exploit technologique du projet Lamden est son grand registre cryptographique et son système de routage qui relie les chaînes privées. Au lieu de recréer une chaîne entièrement nouvelle et plutôt de se concentrer sur les chaînes privées distribuées uniquement liées par une infrastructure de routage, nous pouvons éviter le blocage de la chaîne, la nécessité de «synchroniser» avec le réseau avant d'interagir avec lui, d'augmenter les coûts de transaction et de garantir une plate-forme à l'épreuve du futur qui durera des années, indépendamment des améliorations supplémentaires apportées à la technologie générale de blockchains.

**Routage**

Clove est principalement l'infrastructure qui relie les chaînes privées sur un protocole commun, tout comme un réseau téléphonique. Le Ledger s'occupe de l'interaction entre toutes les chaînes et fournit un ensemble commun d'options d'interface pour que les chaînes puissent être traitées de la même manière dans les environnements de programmation informatique et les plates-formes pour une intégration plus poussée loin de Flora.

Une valeur ajoutée principale de Clove est l'absence de frais de transaction. En échange des avantages de la connexion à Flora et de l'exposition d'une chaîne privée à l'ensemble de la collectivité qui augmente l'adoption publique, une chaîne privée consacre une certaine quantité de puissance informatique au Ledger. Étant donné que le Ledger est absent des fonctions de hachage difficiles, et sert simplement d'intermédiaire pour traiter des paquets d'informations entre les chaînes. La charge informatique pour connecter et diffuser des informations est comparable à un serveur Web moderne, plutôt qu'un mineur à blocs standard. Les fournisseurs d'applications Blockchain exposent un seul point d'entrée public à l'IPFS et au cluster informatique distribué pour les transactions entrantes et se connectent au nœud Ledger public pour les transactions sortantes.

**Canaux de paiement pour les transactions en chaîne transversale**

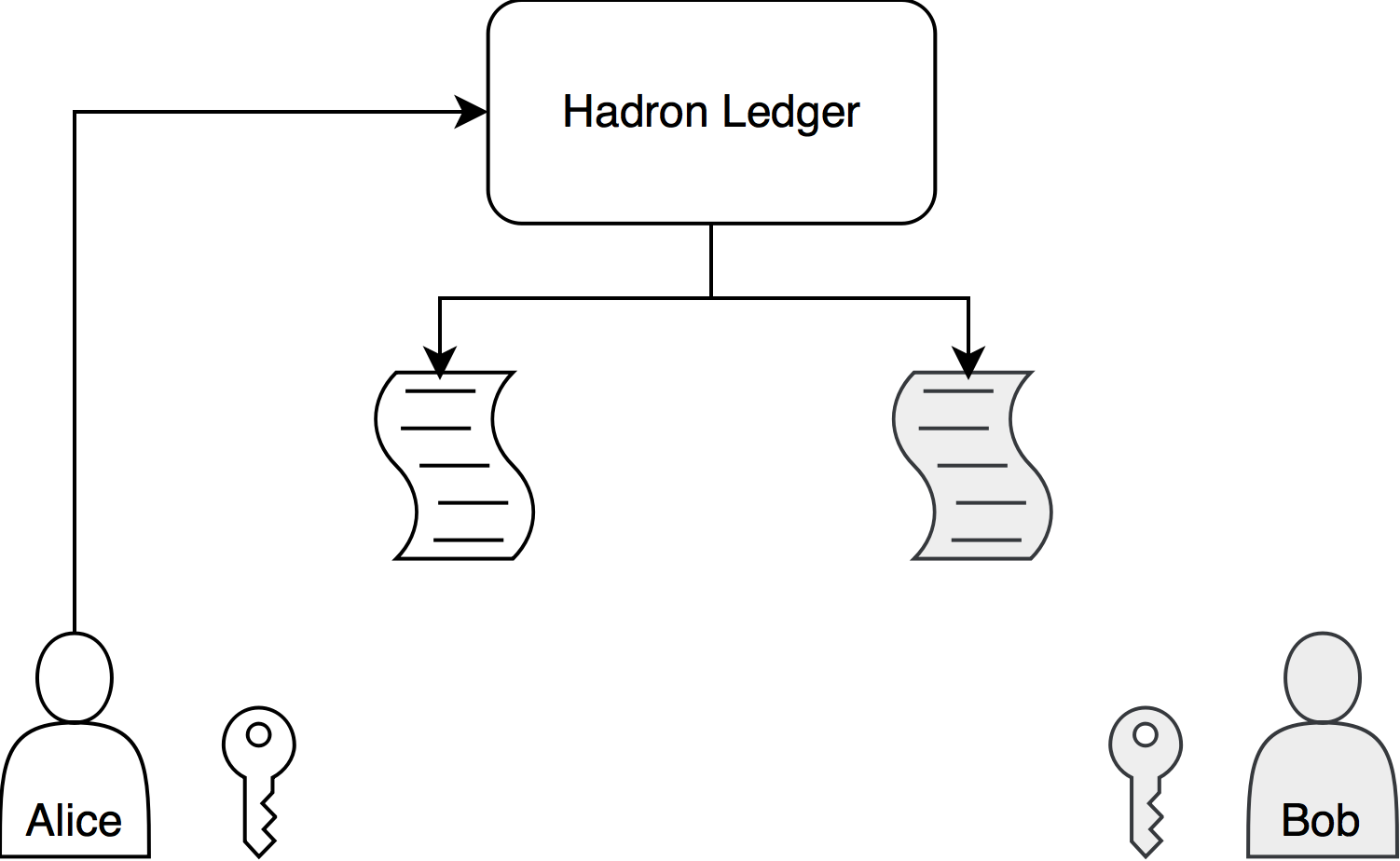
Tout en conservant un système sans confiance et décentralisé, il faut qu'un système de paiements en chaîne transversele existe afin que les applications blockchains puissent interagir librement. C'est le principal attrait de Clove. Pour ce faire, le Ledger met en place des canaux de paiement inspirés de Lightning Network pour fournir une méthode sûre et décentralisée d'échange de fonds à travers les blockchains. Les transactions commencent à partir de chaînes privées et utilisent le Ledger comme service public pour la gestion des envois de fonds sécurisés et garantis de chaîne en chaîne.

Le Ledger est un service public qui distribue le travail de déploiement de contrats intelligents et de vérification d'identité pour les transferts de chaîne à chaîne entre les participants connectés au réseau principal. Les chaînes privées sont libres de mettre en œuvre leurs propres méthodes pour transférer des fonds les uns aux autres, mais le Ledger public est vérifiable par consensus des participants sur le réseau plus large, ce qui donne un sentiment de confiance accru aux transactions en chaîne croisée.

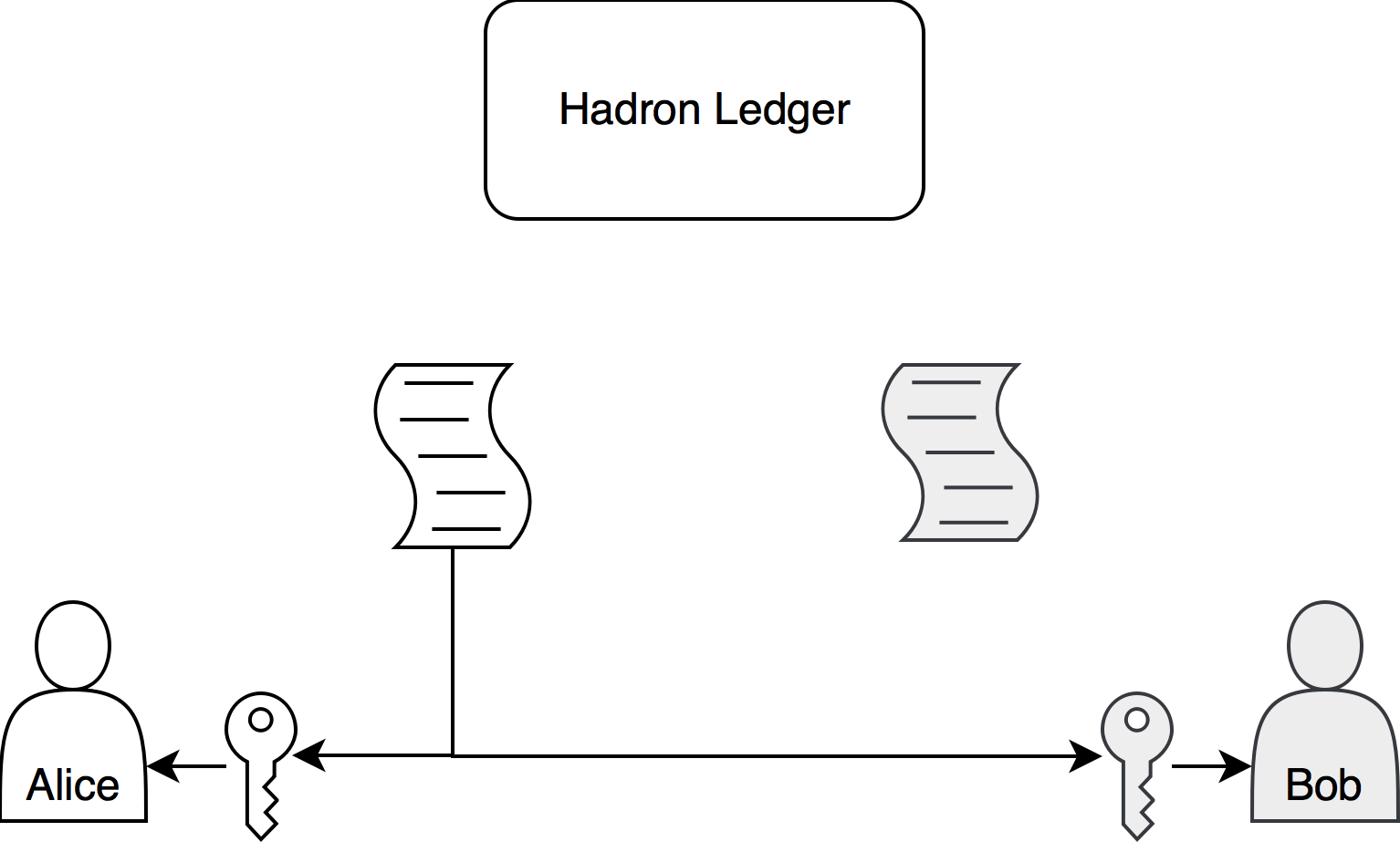
Les canaux de paiement sont représentés dans le code de contrat intelligent Solid Solid qui fonctionne sur chaque blockchain privée. Lorsqu'un utilisateur souhaite lancer un échange, il envoie une demande à la fois le service Clove et la chaîne à laquelle ils souhaitent échanger en décrivant les termes de leur transfert attendu. La demande comprend l'adresse de l'expéditeur et du destinataire sur les deux chaînes, ainsi que la valeur de l'élément qui est échangé. Par exemple, une charge utile ressemblerait à ceci:

{  
 Private-chain-1 : {  
 Sender-address : 0x000,  
 Receiver-address: 0x000,  
 Amount: 100,  
 Token-contract-address (optional): 0x000  
 }  
 Private-chain-2 : {  
 Sender-address : 0x000,  
 Amount: 1000,  
 Token-contract-address (optional): 0x000  
 }  
}

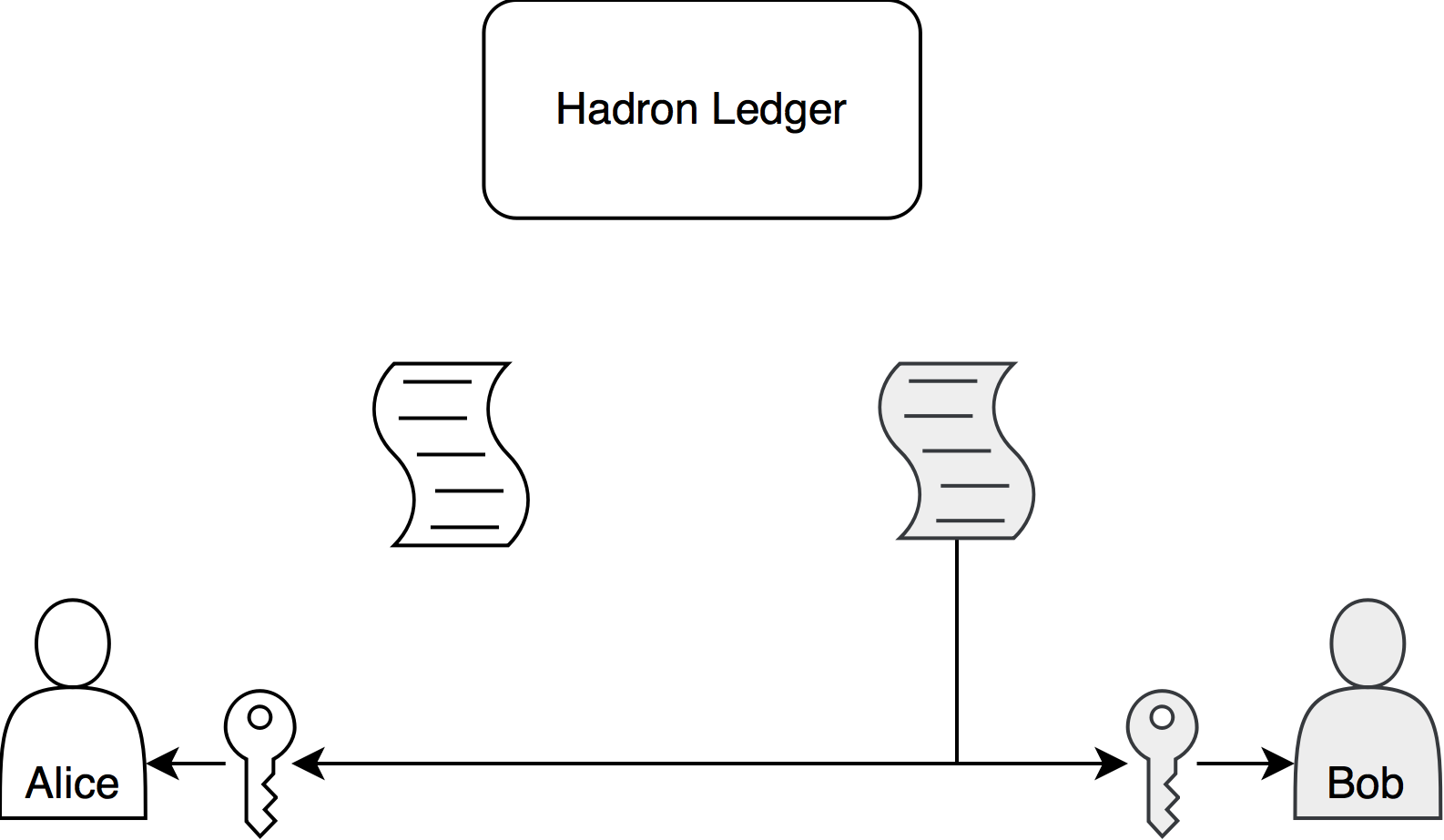
Lorsque le cluster informatique reçoit cette charge utile, le cluster compilera le code de contrat Solidity dans un bytecode qui doit être déployé sur chaque chaîne dans le prochain bloc. Les bytecodes des chaînes opposées sont envoyés l'un à l'autre et signés avec une clé d'identifiant publique afin qu'ils puissent vérifier de manière indépendante que le code de contrat correct a bien été déployé dans le prochain bloc de la chaîne.



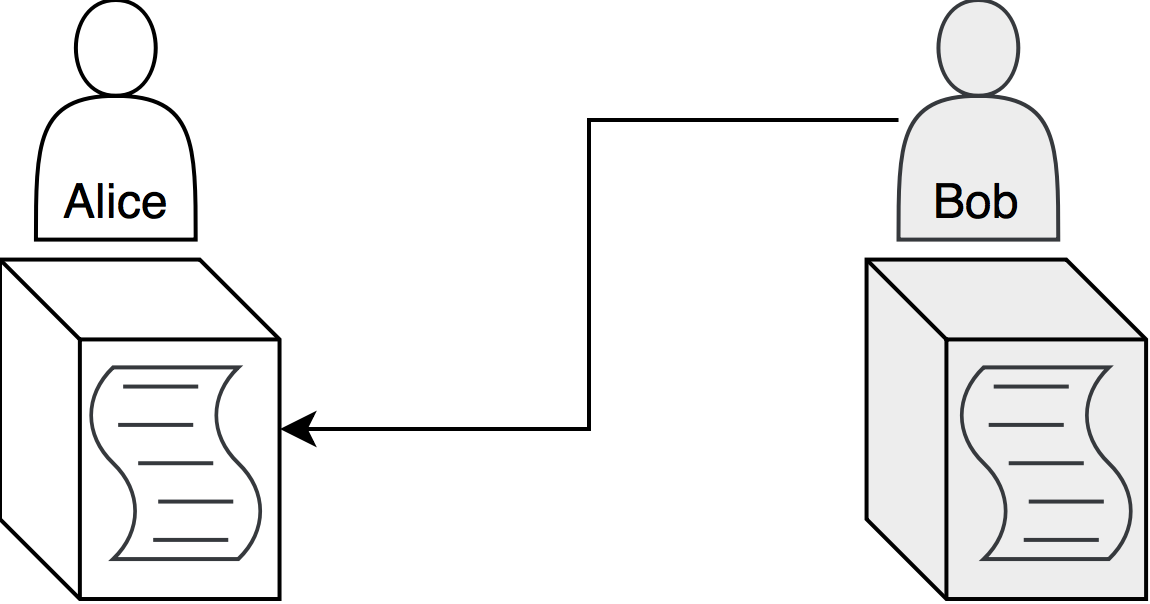
*Alice commence un échange en envoyant un message au Ledger. Le Ledger prend alors les exigences de swap et les compile dans le Bytecode de Solidité à déployer sur chaque chaîne.*



*Le bytecode est signé avec la clé publique de chaque chaîne et envoyé aux deux parties. Alice déploie son contrat. Bob conserve une copie pour vérifier plus tard.*



Le même se produire pour Bob.

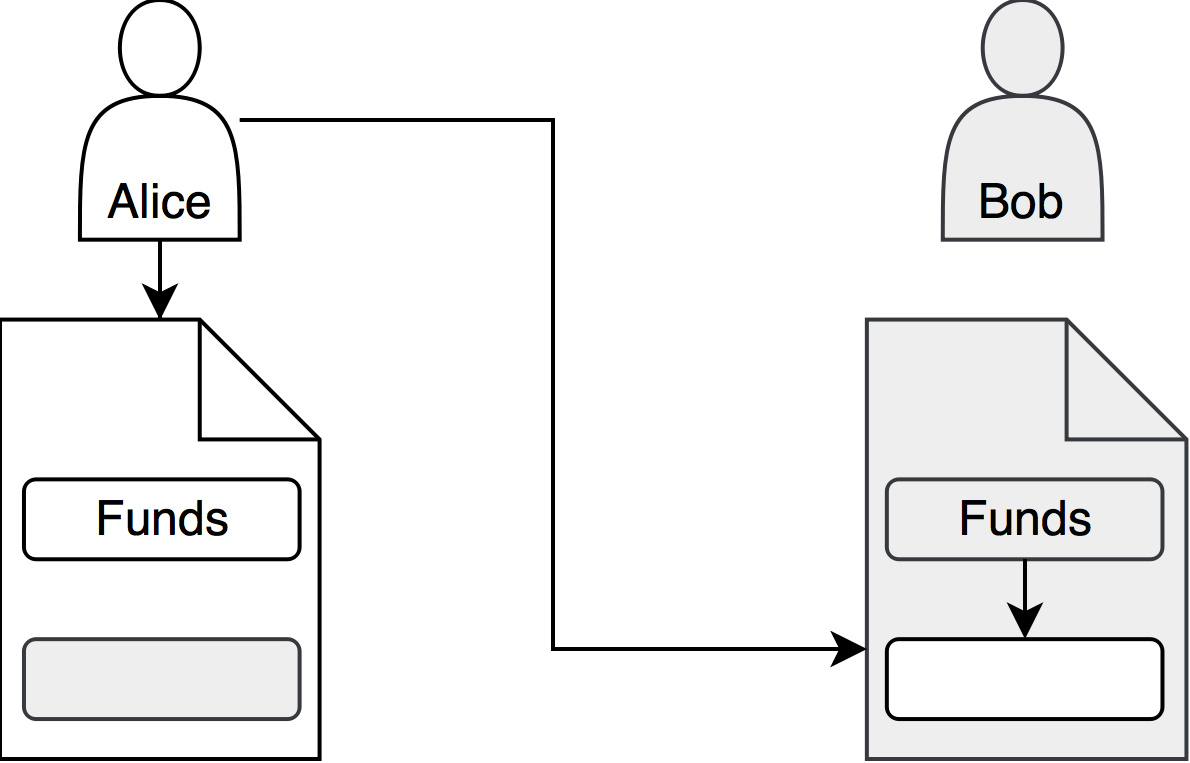


*En supposant qu'il s'agisse d'un échange acceptable, les deux chaînes déploient le contrat et vérifient si l'autre partie a fait la même chose en recherchant le bytecode sur le dernier bloc. Si cela ne s'est pas produit, la chaîne ne doit pas respecter ses obligations et la transaction revient sans perte de fonds.*

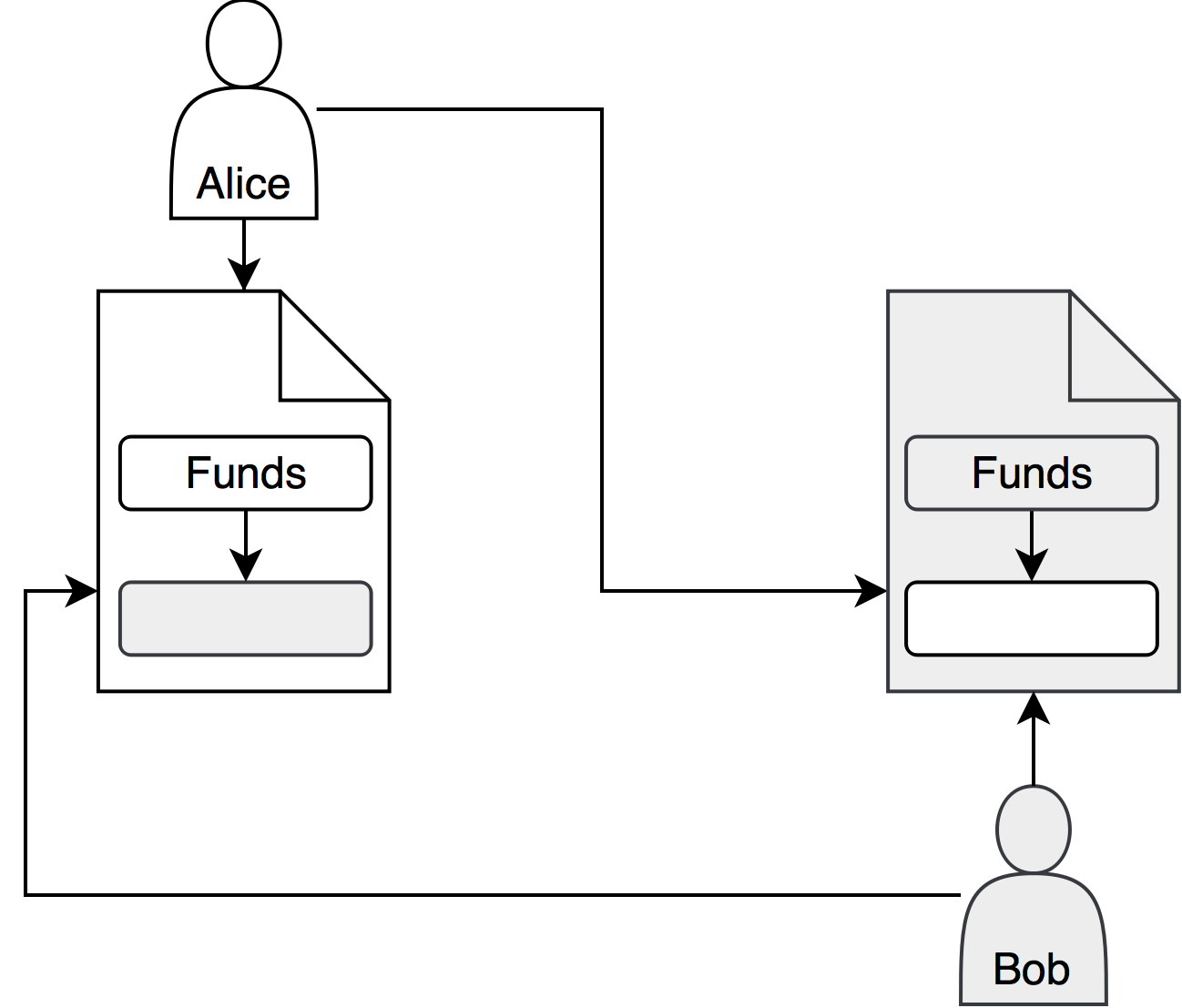
Si la chaîne d'origine ne parvient pas à déployer son contrat alors que la chaîne destinataire se déroule, le contrat sur la chaîne destinataire s'autodétruira et renverra les fonds à leur compte. Sur le revers, si l'initiateur établit un contrat, mais le destinataire n'accepte pas les termes, le contrat d'origine sera détruit, ils recevront leurs fonds verrouillés.

En supposant que les deux parties sont intéressées à poursuivre le swap, elles doivent ensuite respecter les obligations convenues sur les chaînes des autres, qui exécute régulièrement le canal de paiement.

Pour s'assurer que les paiements ont été envoyés en temps opportun, chaque chaîne peut "ping" ses contrats qui invoque une méthode de verrouillage temporel. Si le contrat comporte trop de blocs derrière le délai convenu, on suppose que l'autre partie ne va pas finaliser le canal de paiement et que le contrat est détruit. Cette incitation de la partie adverse à respecter ses obligations parce qu'elles risquent de perdre leurs fonds. Il inciterait également l'auteur à faire valoir son contrat le plus tôt possible, car dans la situation où l'auteur a reçu des fonds sur la chaîne adverse mais pas sur leur chaîne, ils peuvent renvoyer leurs fonds à eux-mêmes et en effet ont gagné "gratuitement" des actifs sur la chaîne opposée parce que le verrouillage du temps avait expiré sur leur propre pour réclamer les actifs.



*La meilleure option économique d'Alice est de soumettre les fonds et de résoudre son propre contrat le plus tôt possible, car si Bob agit devant elle, Alice perdra ses fonds. À l'inverse, Alice pourrait également profiter si Bob décidait de ne pas échanger ses fonds. C'est aussi dans le meilleur intérêt d'Alice de résoudre son contrat le plus tôt possible*



*Le meilleur scénario pour les deux parties est donc de résoudre le canal de paiement sur la chaîne opposée et de résoudre le contrat sur leur propre chaîne le plus tôt possible. En ajoutant des incitations économiques pour ce faire, le réseau bénéficie de transferts rapides en chaîne à chaîne.*

# Exemple de Flux de Travail

Tout d'abord, vous installez un outil Saffron conçu pour développer des blockchains. Vous exécuterez 'saffron init' dans un répertoire de projet et générerez une chaîne. À partir de là, vous installez les paquets dont vous avez besoin pour votre application à l'aide de Flora ou notre gestionnaire de paquets nommé 'textttflora.' Disons que vous souhaitez ajouter un nouvel élément ERC20. Exécutez 'flore d'installation erc20' dans le répertoire du projet, et un nouveau jeton sera généré. Pour déployer les contrats sur la chaîne, exécutez 'saffron start', puis 'saffron déployez tout'.

De là, vous pouvez accéder au tableau de bord administratif si vous souhaitez interagir graphiquement avec votre blockchain. Vous pouvez installer des paquets à partir d'ici, ajouter des comptes, voir des transactions, etc. etc. beaucoup comme Etherscan ou un autre logiciel d'exploration de blocs. Vous disposerez également de Remix et d'autres outils de développement de contrats intelligents.

À partir de ce dorsal, vous pouvez télécharger de nouveaux contrats que vous développez pour Flora. Vous pouvez également connecter votre chaîne à Clove pour interagir avec d'autres applications blockchain. Pour ce faire, vous allez héberger un noeud IPFS et vous connecter au cluster informatique distribué en tant que serveur. Vous pouvez ensuite interagir avec d'autres blockchains indépendantes en tant qu'utilisateur, ou pour implanter des swaps chaîne-chaîne. Vous pouvez lancer des swaps avec le jeton natif Tau hors de la boîte avec toutes les blockchains.

Maintenant, vous pouvez intégrer votre autre logiciel au sommet du blockchain, comme une interface utilisateur publique, des transferts automatiques entre chaînes, une interaction avec un contrat intelligent, et même une interaction avec des contrats personnalisés que vous déployez sur d'autres chaînes sur Clove. Tout est possible avec le projet Lamden.

**Maintenance de l'Architecture du Système Distribué et Sans Confiance**

Alors que les chaînes privées de Lamden sont construites à partir d'Ethereum qui est un protocole distribué et sans confiance, le reste des systèmes Lamden pourrait être développé à l'aide d'une architecture centralisée serveur-client centralisée. Cependant, bien qu'il s'agisse potentiellement d'une méthode d'exécution plus facile, le protocole HTTP standard est vulnérable aux attaques DDOS, à l'échec du serveur et à la propriété centralisée des données qui sacrifient les droits des collaborateurs du projet.

Ainsi, le projet sera déployé sur le protocole IPFS pour établir un véritable système pair à pair distribué et sans confiance.

**Lamden Tau, un atout numérique agnostique**

Bien que les canaux de paiement sur les chaînes privées contribuent à faciliter la communication application-application, il devrait également être éloigné des utilisateurs impliqués dans le projet Lamden, à part un hôte de chaîne ou un développeur pour participer facilement et utiliser les applications de bloc-blocs sur Flora. Ainsi, nous proposons un actif d'agnostique connu sous le nom de 'Lamden Tau'. Tau est un atout numérique qui sert l'atout universel de la plate-forme elle-même, disponible pour le commerce par les utilisateurs du système qui veulent utiliser une monnaie qui utilise toutes les chaînes privées. La communication avec la chaîne Tau sort de la boîte pour les développeurs de Lamden, de sorte qu'ils n'ont pas à établir des relations indépendantes avec d'autres chaînes privées pour commencer à transférer des actifs les uns aux autres. De cette façon, les développeurs peuvent commencer à intégrer un marché de la monnaie numérique et échanger immédiatement dans leurs applications blockchains. En offrant une monnaie numérique natif hors de la boîte à tous les utilisateurs de Lamden, Tau augmente le taux d'adoption des chaînes privées, car plus d'individus peuvent participer avec la demande provenant de la communauté Lamden.

**Vente des Jetons (Événement de Diffusion des Jetons)**

Le projet Lamden sera financé par un événement Token Distribution (Diffusion des Jetons) du Lamden Tau. Ces Lamden Tau seront disponibles à l'achat sur la chaîne principale Ethereum sous la forme d'un jeton ERC20. Ledit Lamden Tau sera alors disponible pour échanger sur la chaîne de Lamden lors d'un processus cérémonieux qui signifie la réalisation historique de la communication chaîne-chaîne sur Clove.

D'autres détails sur l'événement de Diffusion de Jetons sont inclus dans les documents organisationnels.

# Conclusion

L'objectif du projet Lamden est de fournir une suite d'outils qui facilite le développement rapide et le déploiement des blockchains pour la population générale des développeurs. En modélisant nos outils basés sur les outils les plus populaires utilisés par les développeurs d'aujourd'hui, nous pouvons capturer une base large et enthousiaste de développeurs qui veulent s'impliquer dans le blockchain, mais ne peuvent pas surmonter les obstacles initiaux.

De plus, en fournissant une communauté centralisée, l'innovation peut prospérer et s'appuyer sur elle-même, conduisant à des technologies plus récentes et plus importantes et à l'accélération de l'industrie dans son ensemble.

Enfin, grâce à Clove, nous sommes en mesure de relier tous ces projets ensemble sur un seul système de routage qui facilite les transactions de swap afin que les chaînes privées puissent conserver les avantages de l'autogestion et profiter encore d'un écosystème plus vaste d'applications exceptionnelles.

1. stuart@lamden.io [↑](#footnote-ref-1)
2. mario@lamden.io [↑](#footnote-ref-2)
3. james@lamden.io [↑](#footnote-ref-3)