LeMagIT
L'informatique pour et par les pros
TechTarget
E-handbook
Contenu PRO+

# Quelle blockchain privée choisir ?

## Dans ce guide



## Introduction.

Parler de *la* blockchain n'a pas grand sens tant les options technologiques pour les déploiements privés (c'est à dire entre acteurs d'un consortium qui se connaissent en amont) sont diverses et variées.

Dans ce dossier spécial, Damien Lecan, ex-M. Blockchain de SQLI, décortique les spécificités *des* principales blockchains privées pour y voir plus clair.

Ce tour d'horizon n'est pas exhaustif mais il couvre les technologies de registres distribués les plus connues et les plus répandues. Et il vous permettra en tout cas d'y voir beaucoup plus clair avant de choisir celle qui convient le mieux au PoC que vous aurez identifié.

Dans ce guide



# L'essentiel sur Hyperledger, la superstar de la blockchain privée

**Damien Lecan,** Space Elephant

**Soutenue par la Linux Fondation et par IBM, Hyperledger est taillée dès l'origine spécialement pour les entreprises, exclusivement pour un contexte de blockchain de consortium.**

Hyperledger est la blockchain la plus complète et la plus adaptable des blockchains privées. Elle est taillée dès l'origine spécialement pour les entreprises.

Ses Smart Contracts, nommés « chaincodes » sont codés principalement dans le langage de programmation Go, mais peuvent l'être aussi en Java ou JavaScript (Node.js).

Le déploiement de cette blockchain est néanmoins très complexe. L'ensemble des composants qu'il faut mettre en œuvre pour qu'un seul nœud soit opérationnel nécessite beaucoup d'ingénierie et de configuration.

**Dans ce guide**



Hyperledger est en effet constitué de composants que l'on peut (et doit) assembler à sa guise. Chacun nécessite de savoir les choisir selon son contexte, les paramétrer et les utiliser.

Certains composants sont indispensables, comme le choix de l'algorithme de consensus, le protocole de communication ou le stockage des données.

C'est le cas du composant d'identité, qui peut reposer sur une infrastructure de génération de clefs (PKI). Toute la sécurité d'Hyperledger reposerait sur ces clefs. Or, la PKI est en elle-même une activité complète à déployer en entreprise à laquelle se dédient des entreprises spécialisées (Keynectis/OpenTrust).

## Flexibilité et complexité

La Ultra-flexible, Hyperledger stocke les données de l'état de la blockchain préférentiellement dans les bases de données NoSQL Google LevelDB ou CouchDB. Cela implique de choisir un moteur de stockage - et donc de faire une étude avec les DBA (administrateurs de base de données) selon les besoins du projet blockchain, les licences existantes, les compétences internes, la scalabilité souhaitée, etc. Pour simplifier ce choix, Hyperledger fournit

## Dans ce guide



néanmoins, en mode développement, des "quickstarts" dans lesquels LevelDB est packagé.

Autre difficulté, le moteur de Smart Contract « chaincode » est un composant système à part entière. D'un point de vue architecture, le nœud en lui-même est chargé de gérer toutes les connexions réseau avec les autres nœuds. Les instances de Smart Contract, elles, sont des composants qui vont être déployés autour de ce nœud dans des conteneurs Docker exclusivement. Hyperledger exige donc d'avoir également des compétences dans ce domaine.

Un autre composant précise le type de consensus (preuve de travail par exemple, même si elle n'a pas grand sens dans un consortium, ou preuve personnalisée à l'envie). Ce moteur concourt à la gestion de la confidentialité des données entre les nœuds - qui est elle-même personnalisable de manière très poussée et très fine dans un module dédié. La personnalisation du consensus est potentiellement illimitée et nécessite une phase de spécification et de conception particulière.

Hyperledger est de loin la blockchain la plus complète du marché - ce qui explique que IBM a pu faire un Roadshow et multiplier les PoC (preuves de concept) dans des industries très différentes (SACEM, MAERSK, Wallmart, etc.).

Mais que l'on ne s'y trompe pas. Cette liberté à un prix - technologique et financier.

## Dans ce guide



La complexité inhérente à cette liberté fait que Hyperledger est aussi la blockchain de choix des grandes ESN et des intégrateurs... qui peuvent facturer du service.
Certains projets débutés sur Hyperledger - justement parce qu'elle est une blockchain robuste, sécurisée, capable de répondre à tous les cas métiers - ont été migrés sur d'autres blockchains à cause de cette complexité. C'est le cas d'un grand constructeur automobile qui, après 6 mois de projet, a jeté l'éponge pour revenir à un choix plus pragmatique, Ethereum.

Reste que Hyperledger est aujourd'hui LA blockchain de référence et que son adaptabilité a séduit des éditeurs comme SAP ou Oracle.

Indépendamment du code - open source - d'Hyperledger auquel il contribue, IBM propose des outils d'administration et de sécurité packagés pour piloter la mise en production et l'exploitation (haute disponibilité, quel nœud est ok, quel nœud est HS, etc.) sur son Cloud Bluemix.

Bref, Hyperledger joue les premiers rôles dans la Blockchain, mais elle demande beaucoup de compétences pour mener à bien les projets.

Dans ce guide



# Ethereum & Quorum : les cousines anti-Hyperledger

**Damien Lecan,** Space Elephant

**Face à la complexité de Hyperledger, Ethereum et Quorum jouent la carte de la simplicité. Au prix, évidemment, d'un compromis fonctionnel.**

Ethereum est le plus grand challenger d'Hyperledeger dans la blockchain privée. Plus simple, elle séduit des entreprises dont certaines sont rebutées par la complexité et les (trop) grandes possibilités de personnalisation d'Hyperledger.

Quorum, conçue par JP Morgan, essaye de garder cette simplicité tout en palliant certaines lacunes fonctionnelles d'Ethereum.

## Ethereum : l'anti-Hyperledger

Face Ethereum est une blockchain simple. La plus simple même pour un contexte de consortium. Mais cela a un prix. Ethereum est quasiment clef en main mais ne permet évidemment pas les personnalisations d'Hyperledger.

## Dans ce guide



A l'origine, Ethereum est une blockchain publique qui motorise l'altcoin Ether. Plus exactement, il s'agit d'un protocole de Blockchain. Plusieurs clients open source ont implémenté ce protocole pour miner cette monnaie. Les plus connus sont Eth en C++, Parity en Rust et Geth en Go. C'est l'un d'entre eux (Geth) qui s'est développé pour s'adapter au contexte des blockchains privées avec le soutien de la Fondation Ethereum (à ne pas confondre avec la Enterprise Ethereum Alliance, dont l'objectif est de développer des standards blockchain adaptés à l'entreprise et pas directement des produits).

Le déploiement d'Ethereum sur un nœud de blockchain privé a gardé l'esprit originel de simplicité de la blockchain publique. Il suffit de télécharger le binaire du client pour son système d'exploitation directement depuis le site officiel Ethereum. Les paramétrages sont volontairement limités : pas question ici de choisir un moteur de stockage, pas de PKI et les Smarts Contracts tournent dans l'Ethereum Virtual Machine qui est incluse dans le moteur de base d'Ethereum.

Il faut évidemment spécifier les caractéristiques de la blockchain privée, définir le Génésis (le bloc « 0 » de la blockchain), mais cette étape est commune à toutes les autres blockchains. Un projet peut au final commencer très rapidement.

Revers de cette simplicité, Ethereum a une richesse fonctionnelle bien inférieure à celle d'Hyperledger. Notamment, la gestion des droits (qui peut voir quelle transaction ? Qui peut faire quoi dans le registre ?).

## Dans ce guide



Celle-ci se fera presque exclusivement dans un Smart Contract - et non dans un composant de base. Le résultat tient souvent du « bricolage » et les possibilités sont bien plus faibles que dans Quorum ou dans Hyperledger. Il n'est par exemple pas possible de cacher totalement certaines transactions à certains acteurs et pas à d'autres dans Ethereum.

En preuve de travail, la vitesse de validation des blocs n'est pas non plus paramétrable. Elle est figée à un toutes les 14 secondes, que ce soit dans un déploiement à deux nœuds ou dans un à 10.000 nœuds.

Quant aux outils de monitoring et de supervision disponibles, ils sont limités. Une entreprise séduite par Ethereum devra certainement envisager de développer elle-même ses tableaux de bord spécifiques pour la production.

Côté consensus, Ethereum supporte aussi bien la preuve de travail (PoW) que la preuve d'autorité (PoA, Proof-Of-Authority – plusieurs implémentations sont disponibles selon le client utilisé) plus adaptée à la blockchain privée. Avec la PoA, des « autorités » choisies sécurisent la blockchain et sont explicitement autorisées créer des nouveaux blocks et se surveillent mutuellement.

Avec ses forces et malgré ses faiblesses, Ethereum « tourne » parfaitement et a fait ses preuves dans un contexte public, beaucoup plus exigeant qu'un contexte de consortium.

En France, les atouts de cette blockchain ont été choisis par Carrefour pour son projet de traçabilité alimentaire.

## Quorum : Ethereum augmenté

Lancée par JP Morgan, Quorum est une blockchain qui reprend les bases d'Ethereum pour en combler (certaines) lacunes.

La gestion de la confidentialité des transactions de chaque participant par exemple y est nettement plus poussée. Avec Quorum, il est par exemple possible de masquer le contenu d'une transaction en les rendant « privée ».

Au contraire d'Ethereum, Quorum ne supporte pas la PoW, mais propose des algorithmes de consensus spécifiques (Raft et Istambul BFT par exemple).

JP Morgan propose aussi des outils de déploiement de cluster de nœuds Quorum en open source, mais les outils d'administration restent assez succincts.

Côté défaut, Quorum n'est pas (encore) disponible de manière packagée, comme on pourrait l'attendre dans un contexte entreprise sécurisé. Il faut télécharger le code source puis le compiler soi-même. Ce qui rend son adoption, son évolutivité et ses mises à jour délicates au fil du temps. Autre point faible, il y a mécaniquement un écart de version avec Ethereum.

## Dans ce guide



En clair, d'un point de vue fonctionnel, Quorum est plus riche et plus adaptée à un contexte de consortium qu'Ethereum, mais pour la mise en production et le déploiement, elle est plus compliquée.

Malgré cela, son potentiel est aussi très important. JP Morgan devrait en effet bientôt séparer cette activité. La banque souhaiterait gérer Quorum comme une entreprise à part entière. On peut donc espérer des développements supplémentaires et, rapidement, un mode de déploiement plus simple.

A noter que comme Quorum augmente, mais ne remplace pas, les fonctionnalités d'Ethereum (Geth), il existe une portabilité entre les deux blockchains (la seule portabilité entre blockchain aujourd'hui).

Dans ce guide



# Projet Casper : Ethereum en route vers la Preuve d'Enjeux

**Philippe Ducellier** journaliste

**Les développeurs d'Ethereum ont publié la première implémentation de « Proof of Stake » dans leur blockchain publique. Elle doit remplacer d'ici deux ans la Preuve de Travail, jugée trop gourmande en énergie. Deux des principaux clients Ethereum testent ce code.**

C'est une petite révolution dans le monde des Blockchains publiques. Ethereum a commencé le projet de passer de la preuve de travail (Proof of Work) - au cœur de la blockchain Bitcoin - à la preuve d'enjeu (Proof of Stake).

## Consensus et « Preuve de »

Bien La « Preuve de » est une partie importante de l'étape clef, appelée « consensus », dans des échanges décentralisés via une blockchain.

Le consensus est le processus qui permet de valider les nouvelles transactions en vérifiant, de manière consensuelle entre les membres de la blockchain, qu'elles sont bien correctes.

Ce consensus se compose d'une part de la validation des données (c'est à dire vérifier que le débiteur possède bien les fonds en analysant les lignes précédentes du registre) et d'autre part du choix du nœud/membre qui aura la charge de cette validation et de l'écriture du nouveau bloc.

Imaginez dix personnes qui ne se connaissent pas dans une pièce : on en choisit une - par un algorithme connu de tous - qui vérifie les transactions puis qui les écrit dans un registre. Une fois qu'elle a terminé, elle demande aux neuf autres de relire son travail et de le contresigner. Se pose alors une question : comment choisir la personne dans la pièce qui va valider les transactions ?

Les « Preuves de » apportent une solution.

## Limites de la Preuve de Travail

Avec la Preuve de Travail (PoW pour Proof of Work), les nœuds qui souhaitent valider les transactions rentrent en compétition dans un concours de force brute. En clair, il s'agit d'une loterie - et non d'un puzzle mathématique.

« La PoW est une loterie payante », expliquait récemment Damien Lecan, ex Monsieur Blockchain de SQLI et nouveau CTO de Space Elephant. « Avoir plus de puissance permet d'augmenter ses chances de trouver un résultat le premier. Mais il y a une forte composante aléatoire dans le fait de trouver le bon "hash". [...] Par analogie, vous pouvez acheter beaucoup de tickets de Loto

pour augmenter vos chances de gagner à chaque tirage, mais sans être sûr de gagner le gros lot ».

La PoW a été un coup de génie du créateur du Bitcoin. Elle a rendu la falsification coûteuse et a permis la rémunération des « mineurs ». Mais elle a aussi deux gros défauts : la lenteur (relative) et surtout la débauche gargantuesque d'énergie (on compare aujourd'hui celle du Bitcoin à la consommation de pays entiers).

## Intérêt de la Preuve d'Enjeux (Proof of Stack)

Une des alternatives à la Preuve de Travail est la Preuve d'Enjeux (ou PoS pour Proof of Stake).

Avec la preuve d'enjeux, les nœuds qui possèdent le plus d'actifs sont prioritaires dans la validation des transactions.

Le principe est que les acteurs qui ont le plus d'intérêts impliqués (c'est à dire qui possèdent les plus gros « tas » - « stack » en anglais - d'actifs) sont les mieux placés pour s'assurer honnêtement que tout se passe bien dans la blockchain, car dans le cas contraire, leurs actifs se dévalueraient rapidement suite à une perte de confiance des membres.

Avec la PoS, la débauche d'énergie est résolue. Un algorithme - auditable et ouvert - évalue les « mineurs » prioritaires en fonction de données objectives issues de la blockchain elle-même.

## Ethereum en route vers la PoS

Début mai, l'équipe de développeurs d'Ethereum a annoncé la sortie officielle du code de la toute première version de Casper Friendly Finality Gadget (FFG v0.1). « Casper » étant le nom du projet d'Ethereum pour remplacer la PoW par une nouvelle PoS.

Le passage de l'une à l'autre se fera progressivement. Dans une première phase, les deux types de « validateurs » (ceux choisis par force brute et d'autres en fonction de leurs actifs impliqués) cohabiteront.

Le choix de devenir un « validateur » dans cette période de transition impliquera plusieurs contraintes pour le nœud volontaire.

Vitalik Buterin, le créateur d'Ethereum, explique qu'il faudra envoyer un dépôt de 1500 Ethers (soit au cours où est écrit cet article : 680.000 $), être suffisamment en ligne et de voter activement.

Un barème de récompense / pénalité sanctionnera les différents comportements. Les bons élèves pourront gagner jusqu'à 5% de leur mise par

## Dans ce guide



an. Les autres pourront perdre de 5 à 10% de leurs actifs. Voire pire s'ils tentent de corrompre le registre (avec la perte totale de leurs actifs).

Ce barème, qui n'est pas encore définitif, n'entrera en vigueur que lorsque les clients Ethereum auront intégré Casper. Ce qui n'est pas encore le cas. Mais deux des principaux clients Ethereum - Parity et Geth (ce deuxième étant à la base de la version privée d'Ethereum) - ont d'ores et déjà fait savoir qu'ils avaient commencé à tester ce code.

La phase de consensus hybride PoW - PoS devrait durer environ deux ans.

Dans ce guide



# L'essentiel sur Ripple : la Blockchain ultra-spécialisée (et ambigüe)

**Damien Lecan,** Space Elephant

**Ripple est une blockchain atypique. Dédiée exclusivement à la gestion des paiements, elle motorise une crypto-monnaie tout en étant disponible pour des déploiements privés.**

L'essor Ripple est une blockchain de consortium très à part. Première différence avec ses concurrentes Ethereum ou Hyperledger : elle est contrôlée par une seule entreprise et non par une fondation aux membres multiples.

Deuxième particularité : elle est spécialisée dans le paiement.

## Spécialisée et mature

L'essor La variété de ses fonctionnalités est donc « réduite » mais elle est ultra-efficace et très rapide dans son domaine précis - micro-paiement, échanges internes dans une entreprise, de la compensation entre établissements - ce qui en fait une solution plébiscitée par les banques et par les institutions financières. Mais elle ne fait que cela.

Autre spécificité : elle existe depuis 2012, d'abord sous le nom initial d'OpenCoin, puis de Ripple en 2015, ce qui lui donne la plus grande maturité des blockchain privées.

Comme elle est sous le contrôle d'une seule société, Ripple ne crée en revanche pas la même confiance par son code (ce qui est le cas des blockchains classiques dont le principe est de transférer la confiance des acteurs vers le logiciel) mais, de manière plus traditionnelle, par un contrat passé entre les clients et le prestataire Ripple.

## Complexe et chère

Dernières caractéristiques, Ripple est complexe dans son paramétrage et ses personnalisations possibles en fonction du contexte de déploiement. Ses outils d'administration et de monitoring révèlent en revanche la maturité du produit et son succès en entreprise.

En résumé, il y a du travail de conception, d'architecture pour mettre une Blockchain Ripple en route. On reste néanmoins loin de la complexité d'un Hyperledger.

Enfin Ripple est cher. Les mauvaises langues diront que c'est d'ailleurs cette difficulté et ce prix élevé qui ont attiré les banques - pour qui tout ce qui est sérieux rime avec onéreux.

## Ambiguïté entre la blockchain Ripple et la monnaie Ripple

A bien noter : Ripple est aussi le nom d'une crypto-monnaie qui porte le même nom (XRP).

Cet altcoin est bien motorisé par le même code de blockchain, avec un algorithme de consensus qui ressemble à la Preuve d'Autorité (PoA ou Proof of Authority), où les transactions sont validées par des nœuds connus rassemblés dans une liste, sous contrôle de Ripple.

Mais cette blockchain repose sur une infrastructure partagée et publique qui n'a strictement rien à voir avec les blockchains Ripple déployées sur l'infrastructure des architectures privées dans le cadre de consortiums.

## Une blockchain robuste

Ce Ripple public montre en tout cas la capacité de cette blockchain à gérer un grand nombre de nœuds, massivement distribués, pour réaliser des millions de transactions.

UBS, Santander, American Express, et en France le Crédit Agricole utilisent Ripple.

## Dans ce guide

Dans ce guide



# Corda (R3) : ne l'appelez surtout pas « Blockchain »

**Damien Lecan,** Space Elephant

**Réponse des banques aux blockchains des acteurs technologiques, ce registre distribué est prometteur. Mais plusieurs points invitent à rester prudent sur une offre qui, par ailleurs, refuse le terme de Blockchain.**

Historiquement, Corda est une réponse d'un consortium de banques (R3) aux blockchains comme Hyperledger, Ethereum et Quorum ou Ripple. Leur idée était qu'elles ne pouvaient pas laisser une technologie au potentiel aussi disruptif pour leurs métiers dans les mains de tiers.

La philosophie de Corda est la même que celle d'Hyperledger même si elle a, de fait, moins de fonctionnalités et que la gouvernance du projet fonctionne moins bien que celle de la Linux Foundation.

Les banques ne sont en effet pas habituées à gérer des communautés sur le modèle des fondations open-source. Ni à faire du logiciel.

Résultat, le projet a pris beaucoup temps pour sortir une blockchain qui soit utilisable, s'est peut-être un peu dispersé en prospectant d'autres secteurs

## Dans ce guide



métier (assurance, santé, énergie …) et surtout a induit de la confusion dans ses utilisateurs potentiels en refusant de se qualifier de « blockchain ».

Même les membres de R3 se sont mis à utiliser d'autres blockchains !

JP Morgan, par exemple, était initialement dans R3 avant de lancer Quorum (tout en participant au développement de Hyperledger).

Techniquement, Corda est codée avec le langage de programmation moderne Kotlin (qui s'exécute avec la machine virtuelle Java), les smart-contracts pouvant être écrits en Kotlin ou en Java.

Ce n'est pas le seul choix atypique fait par R3. Le consensus par exemple, est différent des traditionnels Preuves de travail (Proof of Works, PoW) et Preuve d'autorité (Proof of Authority). Il repose sur la notion de service de notaire, qui est chargé de contrôler et de signer les transactions dans le réseau. Chaque service est paramétré avec son propre algorithme de consensus (RAFT, BFT ou autre) et peut cohabiter avec d'autres sur le même réseau, pour répartir la charge et améliorer la vitesse de traitement des transactions.

Résultat : Corda est une solution de choix, mais elle est atypique, et ne possède pas, par ailleurs, de caractéristiques clefs que n'auraient pas d'autres solutions, en particulier une taille critique d'utilisateurs qui garantirait sa pérennité.

## Dans ce guide



On ne saurait trop recommander la prudence et attendre pour voir l'évolution de cette offre open source en fonction de l'implication de sa communauté et des membres de l'association R3.

Mi-mai 2018, les banques HSBC et ING ont indiqué qu'elles avaient réalisé la première opération de financement de négoce international (lettre de crédit) en conditions réelles, pour la société Cargill, en utilisant Corda.

## Dans ce guide



# Accéder à plus de contenu exclusif PRO+

Vous avez accès à cet e-Handbook en tant que membre via notre offre PRO+ : une collection de publications gratuites et offres spéciales rassemblées pour vous par nos partenaires et sur tout notre réseau de sites internet.

L'offre PRO+ est gratuite et réservée aux membres du réseau de sites internet TechTarget.

**Profitez de tous les avantages liés à votre abonnement sur: http://www.lemagit.fr/eproducts**

Images; Fotolia

## Dans ce guide





Cyrille Chausson | *Rédacteur en Chef*
TechTarget
22 rue Léon Jouhaux, 75010 Paris
www.techtarget.com