LEMANIA FIDUCIAIRE
Finance - Controlling - Fiscalité
Laurent BOYER
Expert Comptable
% Switch Vibration
Route de Thonon, 152 C
1222 VÉSENAZ (GE)
CHE-271.152.759
(+41) 78 310 93 97
laurent.boyer@lemania-fidu.ch

Appliquer les principes du PoW (BTC) à un projet logiciel développé en commun par 10 PME, de pays multiples et d'organisations non uniformes

A - Contexte

10 PME, situées dans des pays différents (notamment organisation, horaires, cadres juridiques et fiscaux) décident de développer en commun une application informatique. Ce mode de collaboration pose des problèmes classiques, amplifiés par l'éloignement géographique :

- absence d'autorité centrale de confiance entre des partenaires de statut équivalent
- traçabilité et preuve des contributions de chaque PME (code, données, financement, temps passé)
- protection de la propriété intellectuelle commune et individuelle
- prise de décision partagée (validation des livrables, répartition des coûts, arbitrage des litiges)
- absence de garantie technique sur le fait que l'historique du projet (code, décisions, versions) n'ait pas été modifié a posteriori par une des parties.

La blockchain, notamment le mécanisme de Proof-of-Work (PoW) lié au BTC, apporte des réponses techniques à une partie de ces problèmes :

- registre partagé
- infalsifiable
- validé sans dépendre de la confiance en une seule partie.

Cette fiche explique les principes du PoW et évalue, de façon réaliste, comment les mobiliser dans le contexte spécifique d'un consortium fermé de 10 PME identifiées qui veulent travailler ensemble sur un projet, en tâchant d'atteindre les objectifs :

- ne pas imposer 1 des 10 organisations hiérarchiques et techniques, car le but n'est pas de créer 1 groupe juridiquement constitué
- ne pas chercher 1 "dirigeant principal" s'imposant aux 9 autres
- profiter des moyens techniques, humains, financiers de chacune des 10 entités ainsi que de leur vécu & carnet d'adresses
- avancer en continu, en répartissant les tâches et en contribuant à les valider en groupe, à la manière d'une réunion de chantier validant les % d'avancement de chaque participant
- identifier + rapidement voire en temps réel les tâches posant problème car n'avançant pas au même rythme que les autres

B - Principes du PoW (issu du BTC)

Le PoW est le mécanisme de consensus qui permet au réseau BTC de valider les transactions et de sécuriser son historique sans autorité centrale. Ses règles essentielles :

- **chaque bloc de transactions est validé par des « mineurs »**, qui doivent résoudre un problème cryptographique coûteux en calcul (trouver un nonce tel que le hash du bloc soit inférieur à une cible donnée) => pour valider, un "Mineur" doit consacrer du

temps et des moyens, doit aussi se “challenger” avec les autres “Mineurs” car seul le premier valide le bloc, doit se concentrer sur la résolution du problème mathématique en utilisant ses moyens techniques et humaines ainsi que son expérience techniques, donc tout ceci constitue un travail (Work) qui sera validé (Proof of) par tous les autres (qui vont donc attester de la qualité de son travail et surtout déclarer que le “Mineur” a bien répondu aux attentes initiales et donc au problème posé)

- c**ette preuve de travail (PoW) rend la falsification a posteriori extrêmement coûteuse** : modifier un bloc oblige à refaire le calcul de tous les blocs suivants, plus vite que le reste du réseau
- **la difficulté du calcul est réajustée automatiquement** (tous les 2016 blocs, environ toutes les deux semaines) pour maintenir un rythme moyen d'un bloc toutes les 10 minutes, quel que soit le nombre de participants => le challenge reste donc difficile et les “Mineurs” se challengent sans arrêt pour se différencier et arriver à valider le ou les blocs suivants
- **chaque bloc contient l'empreinte (hash) du bloc précédent** : l'historique forme une chaîne, modifier un bloc ancien invalide tous les blocs suivants ; c'est la propriété d'immuabilité (on ne revient pas sur le passé et surtout on n’a pas le droit de changer les contraintes initiales pour “faciliter sa tâche” et livrer un réponse moins fiable et qualitative pour valider le bloc que l’on vise)
- **la « chaîne la plus longue », celle qui a demandé le plus de travail cumulé, fait foi** : c'est la règle qui départage les versions concurrentes de l'historique => on retrace donc du début à la fin de la chaîne les intervenants, leurs travaux, leurs interventions, les travaux validés par la communauté
- **le réseau est ouvert (permissionless)** : n'importe qui peut devenir mineur ou nœud de validation, sans autorisation ni identification préalable => on ne définit pas au début la liste “fermée” des participants, donc un nouveau participant peut se greffer au projet et valider un bloc (donc un travail), ce qui permet l’intégration de nouveaux participants + qualifiés ou performants ; la liste étant ouverte, on ne protège pas les participants historiques qui doivent constamment se “challenger” aux nouveaux

Ces propriétés (immuabilité, décentralisation, absence de tiers de confiance, résistance à la falsification) intéressent un consortium de PME sans hiérarchie entre elles. Mais le mécanisme a été conçu pour un réseau public, anonyme, potentiellement hostile, comptant des dizaines de milliers de participants : un contexte très éloigné de celui de 10 PME partenaires, identifiées contractuellement.

C - Transposer le PoW à un réseau de 10 PME

Appliqué tel quel à 10 PME, le PoW « pur » façon BTC présente plusieurs limites pratiques :

- un coût énergétique et matériel disproportionné pour sécuriser un registre utilisé par 10 acteurs connus => le PoW est conçu pour dissuader des attaquants anonymes et nombreux, pas pour départager 10 partenaires identifiés
- une latence inutile : un rythme d'un bloc toutes les 10 minutes est trop lent pour des opérations de gestion de projet courantes
- le PoW ne résout pas, à lui seul, la gouvernance (qui a le droit de valider quoi) : BTC n'a pas de « propriétaires » de nœuds désignés, alors qu'un consortium de PME veut précisément que chaque PME ait un droit de vote identifié.

En revanche, certaines propriétés du PoW peuvent être obtenues par ancrage sur la chaîne BTC elle-même, plutôt qu'en reproduisant tout le mécanisme :

- l'horodatage infalsifiable d'un livrable ou d'une décision, opposable à un tiers (y compris devant un juge) sans dépendre de la bonne foi d'aucune des 10 PME
- la preuve d'antériorité et de paternité d'une contribution, utile en cas de litige sur la propriété intellectuelle
- la résistance à la réécriture de l'historique par une partie qui contrôlerait un nœud.

Dans le cas de notre “Groupe” de 10 PME, il faudrait adopter, pour la gouvernance quotidienne du consortium, un mécanisme de consensus permissionné adapté à un nombre restreint de participants identifiés soit le PoA (Proof-of-Authority) et réserver le PoW à son usage le plus efficace dans ce contexte : l'ancrage périodique de l'empreinte du registre du consortium dans la blockchain BTC publique, via un service d'horodatage tel qu'OpenTimestamps. Le consortium bénéficie ainsi de la sécurité du PoW le plus robuste et

le plus décentralisé qui existe, sans en supporter le coût ni la lenteur pour ses opérations courantes.

La lenteur du process PoW est d'ailleurs un frein connu au développement du BTC en tant que monnaie Scripturale (monnaie dont les mouvements sont retracés par des écritures) courante car les mouvements sur le Registre sont complexes et lents, du fait de l'approbation impérative de tous les participants (ainsi que des clés publiques/privées).

Critère	PoW (BTC)	PoA	PBFT
Participants	Anonymes, ouverts, illimités	Identifiés et désignés (les 10 PME)	Identifiés, nombre fixe
Sécurise contre	Attaquants anonymes, nombreux	Collusion entre validateurs désignés	Jusqu'à (n-1)/3 nœuds défaillants ou malveillants
Coût énergétique	Très élevé	Négligeable	Négligeable
Vitesse de validation	≈ 10 minutes / bloc	Quelques secondes	Quelques secondes
Gouvernance intégrée	Aucune (règle de la chaîne la plus longue)	Oui — liste des validateurs = les 10 PME	Oui — vote / quorum des 10 PME
Adapté à 10 PME identifiées	Non, sauf en usage d'ancrage externe	Oui	Oui

NB : Le PBFT (Practical Byzantine Fault Tolerance, ou tolérance aux pannes byzantines pratique) est un algorithme de consensus utilisé dans les systèmes distribués et les blockchains pour s'assurer que tous les ordinateurs honnêtes du réseau se mettent d'accord sur une même vérité, même si certains participants mentent ou tombent en panne

D - Résoudre les problèmes de la PoW appliquée à un Groupe de PME

On prévoit et installe deux couches :

1/ Registre du consortium (blockchain permissionnée)

- un nœud par PME (10 nœuds), chacun opéré par la PME concernée sur son propre site ou son propre cloud, afin qu'aucune PME ne dépende de l'infrastructure d'une autre
- un consensus PoA ou PBFT : chaque transaction (validation d'un livrable, décision budgétaire, enregistrement d'une contribution) doit recueillir l'approbation d'un quorum défini contractuellement — par exemple 7 PME sur 10
- des contrats intelligents **(SMART CONTRACTS)** pour le déblocage des financements par étape (jalons du projet), la répartition des droits de propriété intellectuelle selon les contributions enregistrées, et la tenue du registre de vote du consortium
- un stockage du code et des documents volumineux hors chaîne : le registre ne conserve que l'empreinte de chaque version, ce qui le garde léger tout en garantissant l'intégrité de chaque fichier.

2/ Ancrage externe dans BTC (PoW)

- à intervalle régulier (chaque semaine, ou à chaque jalon contractuel important) l'empreinte cumulée du registre est publiée dans une transaction BTC via un service comme **Open Time stamps** (on ne crée pas de registre spécifique, on utilise celui du BTC uniquement pour l'empreinte et non pas pour le Minage)
- cette opération coûte quelques centimes par ancrage et donne à l'ensemble du registre la garantie d'immuabilité du réseau BTC : toute contestation ultérieure sur l'état du registre à une date donnée peut être vérifiée publiquement, indépendamment des 10 PME elles-mêmes.

E - Méthodologie pour une intégration de la BlockChain

- Charte de gouvernance du groupe : règles de vote, quorum, répartition de la propriété intellectuelle, procédure d'arbitrage des litiges (à valider juridiquement avant tout déploiement technique)
- Choix de la plateforme technique : par exemple Hyperledger Fabric ou un réseau Ethereum permissionné (Besu, Quorum) pour le registre du consortium ; IPFS pour le stockage ; OpenTimestamps pour l'ancrage Bitcoin
- Déploiement pilote avec 3 PME sur un périmètre limité (par exemple la seule validation des jalons), avant extension aux 10 partenaires
- Intégration avec les outils existants : les commits (instantanés) du dépôt de code (Git) sont hashés (empreinte numérique) et enregistrés automatiquement sur le registre à chaque fusion validée
- Formation des équipes techniques de chaque PME à l'exploitation de leur nœud
- Déploiement complet, audit de sécurité indépendant, puis bascule en production.

F - Points de Surveillance en Compliance (Juridique & Organisationnel)

- Droit applicable et juridiction compétente en cas de litige entre PME situées dans des pays différents : à fixer contractuellement en amont (la blockchain ne remplace pas un contrat-cadre de Groupe)
- localisation des données et conformité RGPD (ou équivalent local) si des données à caractère personnel transitent par le registre ou par des nœuds situés hors de l'UE
- la blockchain garantit l'intégrité et l'horodatage d'une information, pas sa véracité initiale : elle ne protège pas contre l'enregistrement de bonne foi d'une information déjà erronée
- redondance et continuité : prévoir la procédure applicable si une PME quitte le Groupe ou si son nœud devient indisponible, afin que le quorum de validation reste toujours atteignable
- gouvernance des mises à jour du logiciel de blockchain lui-même : qui décide, qui finance, selon quelle procédure.