Blockgraph : une Structure de Type Blockchain Tolérante aux Partitions pour les MANET

Nom et acronyme du projet : Blockchain pour réseau Mesh - B4Mesh
Porteur du projet : Guy Pujolle, President de Green Communications
Contact du porteur: guy.pujolle@green-communications.fr
Consortium : Geen Communications, Sorbonne Université et Squad
Instrument de financement : DGA-RAPID
Dates de début et fin de projet : 01/06/2019 - 31/10/2021
Plage de TRL associées aux innovations : TRL3 - TRL6

Auteurs :
David A. Cordova M, Pedro B. Velloso, Alexandre Guerre,
Thi-Mai-Trang Nguyen, Guy Pujolle, Khaldoun Al Agha, Guillaume Dua

***Résumé*—Le Blockgraph est une nouvelle structure de blockchain dans laquelle les blocs sont interconnectés sous la forme d'un graphe au lieu d'une chaîne. Blockgraph a été conçu pour permettre l'utilisation de la blockchain dans les réseaux mobiles adhoc et les réseaux maillés en traitant le problème de la partition du réseau due à la mobilité des nœuds.**

***Mots clés*—blockchain, réseaux maillés, MANET, systèmes distribués**

I. Introduction

La blockchain est une relativement nouvelle technologie qui fournit une base de données sécurisée de forme distribuée ; ce qui permet de stocker des transactions d'une manière inviolable, permettant une haute disponibilité et auditabilité. Les dernières années ont montré que non seulement les cryptomonnaies peuvent bénéficier des avantages de la blockchain. Des nouvelles applications émergent chaque année dans toute sorte de domaine comme c'est le cas du vote électronique pour la gouvernance [1], la traçabilité des données dans le domaine de la santé [2], ou bien encore le prélèvement des données dans l'IoT [3]. Néanmoins, les blockchains dites traditionnelles ont été conçues pour être utilisées sous un réseau muni d'une infrastructure capable de garantir la complète connectivité du réseau. Dit autrement, les blockchains traditionnelles ne sont pas capables de faire face à des réseaux mobiles sans infrastructure. En raison des changements de topologie, les nœuds du réseau peuvent se diviser en différents partitions ou bien se fusionner en une seule partition. Les applications qui reposent sur le concept des réseaux mobiles ad hoc (MANET) tel que les réseaux pour des opérations militaires, les réseaux de véhicules ou les réseaux de drones, y sont concernées. Il est donc impossible d'utiliser une blockchain traditionnelle dans ces scénarii. Dans ce contexte, nous avons proposé une nouvelle solution pour adapter la technologie blockchain aux MANET afin de doter ces réseaux, des propriétés et possibilités qu'offrent la blockchain. Cette nouvelle technologie nous l'avons appelé Blockgraph.

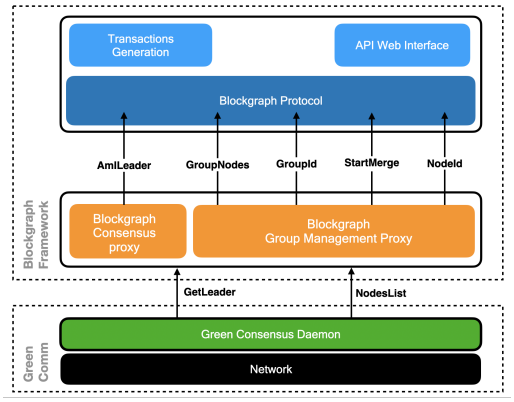

Fig. 1. L'architecture et interfaces du système Blockgraph utilisant le consensus de Green Communications

II. Blockgraph

Le blockgraph est un réseau dit permissioned et tokenless, où les nœuds participant au réseau sont pre-validés et autorisés à participer au réseau et où il n'existe pas une unité de base pour le transfert de valeur. Cependant, elle est utilisée comme un moyen de disséminer de l'information tout en gardant les avantages en matière d'immuabilité, d'inviolabilité et de sécurité. L'idée principale consiste à représenter la blockchain comme un Graph Orienté Acyclique (DAG), dans lequel chaque partition indépendante génère sa propre blockchain correspondant à une seule branche du graphe. Par conséquent, un split correspond à de nouvelles ramifications dans le Blockgraph, tandis qu'un merge correspond à la jonction de deux ou plusieurs branches en une seule. L'innovation de notre solution repose principalement sur deux concepts. Tout d'abord, la capacité d'un bloc pour référencer un, deux ou plusieurs blocs parents, ce qui permet l'existence d'une structure en forme de DAG. Ces blocs, nous les appelons des blocs de merge. La procédure de merge permet la création d'un bloc de merge en identifiant les fusions des partitions réseaux

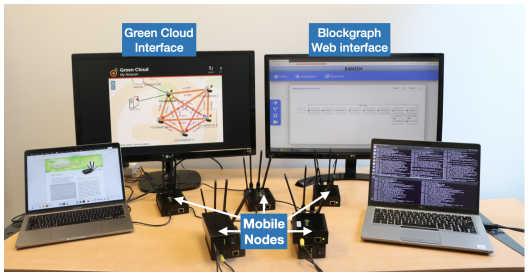

Fig. 2. Testbed

et la synchronisation du Blockgraph par les nœuds participant à la fusion. Ainsi, notre protocole est capable de maintenir une base de données distribuée en présence de changements de topologie.

Le système est composé de trois modules différents. L'algorithme de consensus, en charge de s'accorder sur un seul nœud capable de créer un nouveau bloc ; le système de gestion des groupes, responsable du suivi de la topologie du réseau et de la création d'une communauté des nœuds participant au consensus, et le protocole Blockgraph, qui est responsable de la gestion de la structure de données du Blockgraph, ainsi que toutes les différentes fonctions menant à cet objectif. Les détails de notre protocole sont présentés dans [4].

III. Développement et preuve de concept

Pour démontrer la faisabilité de notre solution, nous avons d'abord implémenté notre solution dans le simulateur à événements discrets NS3. Ce simulateur réseau nous a permis de réaliser des nombreuses études de performances qui nous ont permis de mieux caractériser notre solution. Notamment, nous avons obtenu des résultats sur le débit des transactions par secondes que notre système est capable de supporter avec un certain nombre de conditions qui peuvent seulement être évaluées à travers des simulations. Ensuite, nous avons passé à la phase d'implémentation. Notre testbed est composé de cinq routeurs mesh de faible puissance déployés dans le laboratoire LIP6 comme le montre la figure 2. Le démon blockgraph est embarqué dans chaque routeur mesh. Au démarrage, les routeurs se connectent entre eux pour rejoindre le réseau Blockgraph et créent le bloc de genèse tout en commençant à émuler la génération de transactions. Pour la validation du concept de Blockgraph, nous créons une partition réseau en prenant deux routeurs mesh loin des autres routeurs jusqu'à ce que le réseau soit entièrement divisé en deux groupes. Une partition réseau est composée de trois routeurs mesh et l'autre de deux autres routeurs. Nous laissons les deux partitions réseau séparées l'une de l'autre assez longtemps pour que les deux partitions réseau puissent générer de nouveaux blocs. Nous revenons ensuite avec ces deux routeurs pour observer le processus de merge. La visualisation du Blockgraph dans le routeur 1 est montrée dans la figure 3. On peut voir que le Blockgraph commence par le bloc 0 (bloc genesis) puis il y a deux blocs validés dans le même groupe (Gr 26). Après le split, le réseau est divisé en deux groupes et chaque groupe

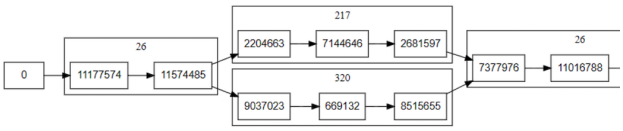

Fig. 3. Blockgraph visualization

continue à générer des blocs. Chaque branche correspond à une partie du Blockgraph maintenu par chaque groupe. Lorsque nous revenons avec les deux routeurs en mouvement, il y a une fusion de deux réseaux (Gr 217 et 320), en un seul réseau composé des cinq nœuds comme au début de la démonstration. Nous pouvons observer dans la figure 3 que le bloc de fusion (block-id = 7377976) est connecté à deux blocs précédents (2681597 et 8515655) par les hachages de ces blocs.

IV. Conclusion

Nous avons conçu un nouveau type de technologie de grand livre distribué (DLT), capable d'adapter sa structure de données en fonction de la topologie et de la mobilité de noeuds. Nous avons caractérisé les performances du block-graph à travers des nombreuses simulations, ce qui nous a permis d'améliorer et optimiser notre système. Finalement, nous avons mis en oeuvre un prototype de Blockgraph en utilisant des routeurs mesh. Cette implémentation nous a permis de valider notre système Blockgraph en étant la première structure de données capable d'apporter aux applications MANET les garanties et propriétés de la blockchain.

Références

[1] F. . Hjálmarsson, G. K. Hreiarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[2] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[3] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 618-623, doi: 10.1109/PERCOMW.2017.7917634.

[4] D. Cordova, A. Laube, T. -M. -T. Nguyen and G. Pujolle, "Block-graph: A blockchain for mobile ad hoc networks," 2020 4th Cyber Security in Networking Conference (CSNet), 2020, pp. 1-8, doi: 10.1109/CSNet50428.2020.9265532.