



# AXELAR, LA PLATEFORME DE COMMUNICATION INTER-BLOCKCHAINS ACCESSIBLE À TOUS

Analyses et Dossiers

09 novembre 2021 à 19h00 par **Morgan Phuc**



## Comment protéger vos profits en Bull Market : quelques

L'un des tout premiers conseils que l'on donne souvent à un débutant dans l'univers des cryptomonnaies et du trading en général, c'e

Le 30 avril 2021 à 19h00

**Axelar est une plateforme de communication *cross-chain*. Dédiée aux développeurs blockchain, aux programmeurs d'applications décentralisées, et bien sûr aux utilisateurs finaux de ces dernières, elle permet à différentes blockchains de communiquer entre elles facilement, grâce à un ensemble d'outils dédiés.**

Axelar est un réseau **ouvert à tous**. Dans cet article, nous étudierons comment il s'articule, et quels sont ses avantages par rapport aux solutions d'interopérabilité existantes.

## AXELAR ET SON ÉQUIPE

Axelar est un projet cofondé par **Sergey Gorbunov** et **Georgios Vlachos**, deux membres fondateurs d'Algorand. L'[équipe de développement](#) est composée d'ingénieurs hautement qualifiés dans des domaines divers et variés : interopérabilité des blockchains, sécurité des systèmes et des réseaux, cryptographie... Les membres d'Axelar ont ainsi presque tous travaillé dans différents projets de l'écosystème crypto, comme **Ethereum** ou **MakerDAO**.

L'équipe d'Axelar est soutenue par de [nombreux acteurs de l'industrie](#), comme Polychain Capital, Coinbase Ventures, Binance et bien d'autres. Fondée en **2020**, l'entreprise a tout d'abord levé **3,75 millions de dollars** en *seed*; puis elle a clôturé une série A de **25 millions** en juillet 2021.



*Sergey Gorbunov, cofondateur d'Axelar*

## LES CHALLENGES DE L'INTEROPÉRABILITÉ

### LES SOLUTIONS EXISTANTES

L'interopérabilité entre les blockchains est un des plus grands **défis de la crypto-industrie**. Alors que de nombreuses plateformes de smart contracts bénéficient d'une adoption grandissante, il existe peu de solutions permettant de les **connecter les unes aux autres**.

Seuls les **systèmes centralisés** permettent de bénéficier d'une **interopérabilité scalable**. Bien qu'efficaces, ils présentent des points uniques de défaillance, et ne correspondent pas à l'idéal de décentralisation recherché par la communauté crypto. Il existe des **hubs** comme **Cosmos** ou **Polkadot**, conférant une grande interopérabilité entre les différentes *sidechains* qui s'y connectent;

cependant, il faut obligatoirement passer par des **technologies externes** pour passer d'un hub à l'autre. De plus, la **pluralité des langages de programmation** rend la tâche difficile.

Il en est de même pour les **ponts** (*bridges*) permettant de « tokéniser » un actif d'une chaîne à une autre. Ces systèmes souffrent d'un manque de scalabilité, et requièrent des **efforts d'intégration** particulièrement lourds pour les développeurs.

L'interopérabilité est donc un **challenge** tant pour les **développeurs de plateformes** que pour les **développeurs d'applications**. Il est très difficile pour une dApp de communiquer d'une blockchain A à une blockchain B. C'est dans ce contexte qu'Axelar propose une **suite logicielle complète**, permettant d'assurer facilement cette **interopérabilité cross-chain**.



## LA COMMUNICATION *CROSS-CHAIN* VUE PAR AXELAR

La **problématique** est donc la suivante : comment permettre à des réseaux très différents, ayant leurs langages de programmation propres, de communiquer sans friction et de façon scalable ? Bien évidemment, la sécurité de ces protocoles de communication doit être sans faille.

Les propriétés recherchées par l'équipe d'Axelar quant à leur plateforme *cross-chain* sont les suivantes :

- Une **intégration *plug and play*** : il s'agit de réduire le travail d'intégration au minimum pour les développeurs ;
- Le **routage *cross-chain*** : toutes les fonctions de découverte des adresses et de routage doivent permettre de faciliter la communication inter-chaînes ;
- Les **mise à jour** des différentes blockchains doivent être prises en charge avec le minimum d'efforts ;

- Un **langage uniforme** pour les applications : le protocole assurant le verrouillage, le déverrouillage, le transfert d'actifs et la communication inter-applications doit être simple à appréhender.

Bien entendu, ces protocoles doivent être **sûrs**. Tout d'abord, afin d'avoir un haut degré de **décentralisation**, le réseau Axelar doit être **ouvert**. Ensuite, le niveau de **sécurité** doit garantir l'**intégrité** des **actifs** et de l'**état** des différentes chaînes. Enfin, le réseau de communication *cross-chain* doit être **accessible** avec un haut degré de **disponibilité** (*liveness*).



## COMMENT FONCTIONNE AXELAR ?

### LES DIFFÉRENTS PROTOCOLES DU RÉSEAU AXELAR

Le réseau Axelar repose sur deux protocoles essentiels : le **CGP** et le **CTP**.

#### *Cross-Chain Gateway Protocol (CGP)*

Le protocole CGP est utilisé pour **connecter de multiples blockchains autonomes**. C'est le CGP qui s'occupe de router les données entre ces différentes blockchains. Il s'agit d'un protocole **agnostique** : en effet, peu importe le mécanisme de consensus des blockchains, ou le langage de programmation de leurs smart contracts. De même, une blockchain n'a pas besoin de connaître l'état des autres pour communiquer.

Il suffit de configurer un **compte portail** (*gateway account*) sur Axelar pour rejoindre le réseau. Les comptes de ce type sont ensuite gérés de façon collective par un **ensemble décentralisé de nœuds** gérant CGP. Ces nœuds contrôlent les paquets de données arrivant sur les *gateways*. Une fois qu'ils ont défini comment seront traitées ces données, elles sont routées et envoyées aux *gateways* de destination.

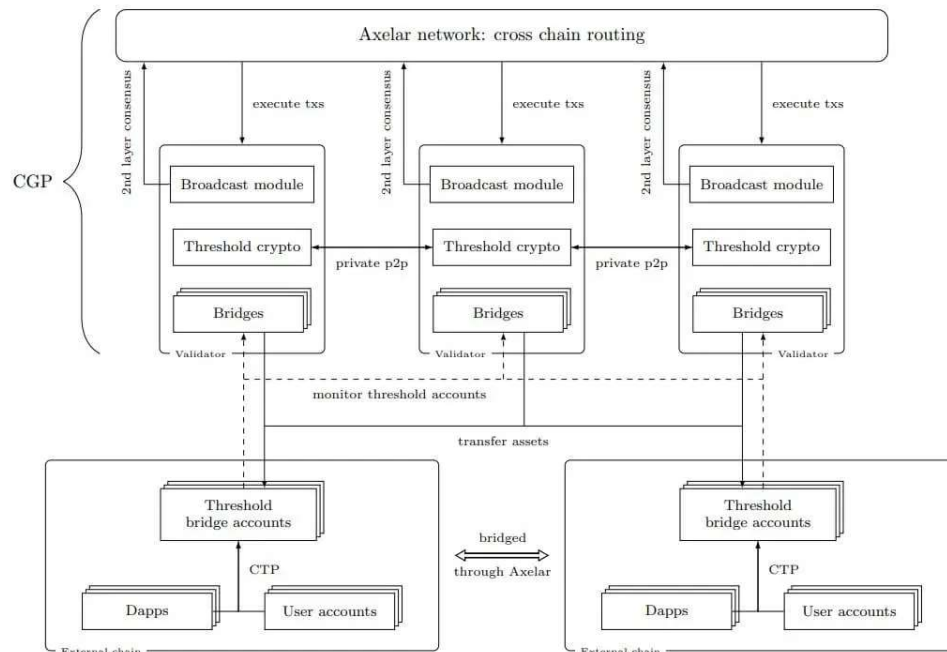
Le CGP peut **finaliser les blocs de n'importe quelle chaîne** grâce au consensus des nœuds, qui s'exécute sur une **couche secondaire**. Ainsi, tout type de blockchain peut être connecté au réseau : mécanismes de consensus probabilistes tout comme consensus à finalité immédiate.

### ***Cross-Chain Transfer Protocol (CTP)***

Ce protocole est exécuté au niveau de la **couche applicative**. Il est donc au-dessus des protocoles de routage (CGP). Le **CTP** permet aux développeurs de **connecter** leurs applications décentralisées à **n'importe quelle chaîne**, puis d'envoyer leurs **requêtes cross-chain**. Il est possible d'interagir avec des dApps de n'importe quelle blockchain grâce à des **appels API**, à la façon des requêtes HTTP :

- **Verrouillage, déverrouillage** ou **transferts d'actifs** entre deux adresses, quelles que soient les plateformes blockchain considérées ;
- Exécution de **requêtes cross-chain entre les dApps**. Par exemple, un smart contract sur Ethereum peut faire un appel API afin de mettre à jour l'état d'un smart contract sur Solana ;
- Mise en place d'**appels à seuil de déclenchement**. Par exemple, une dApp sur Solana peut effectuer un appel pour mettre à jour l'état d'un smart contract sur Ethereum si une valeur-cible est atteinte.





*Routage inter-chaînes sur le réseau Axelar*

## LES AVANTAGES D'AXELAR

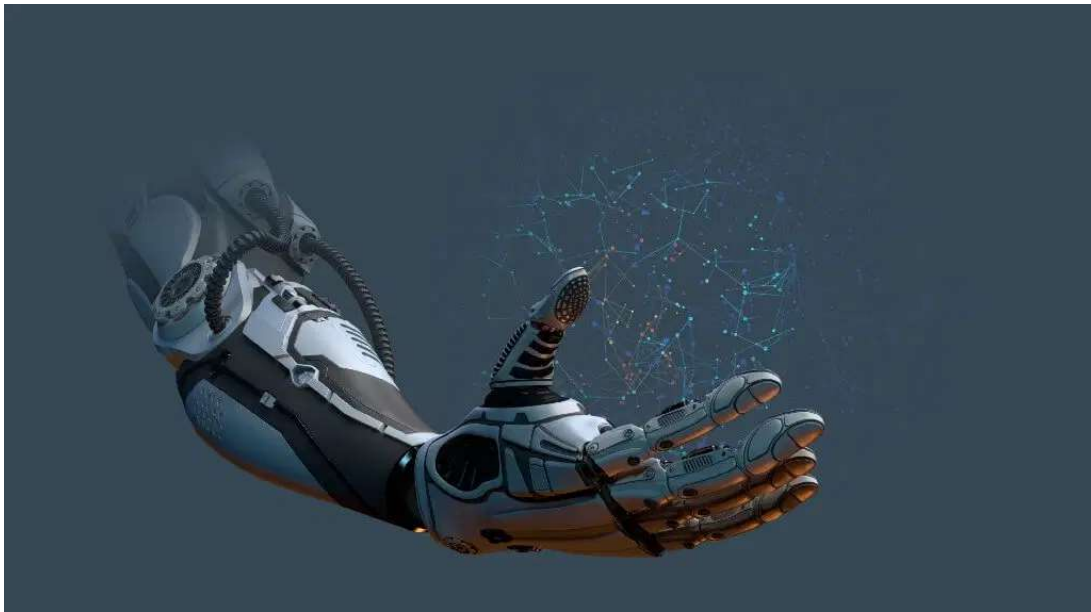
La plateforme Axelar sera **gouvernée par ses utilisateurs**, qui pourront voter pour deux types de propositions :

- Premièrement, l'ajout d'une nouvelle blockchain sur le réseau ;
- Deuxièmement, l'ajout de nouveaux protocoles de niveau applicatif au réseau et à ses protocoles de routage et de livraison.

L'ambition est de taille : déployer un **réseau d'interopérabilité cross-chain scalable et sécurisé**. Axelar permettra d'augmenter grandement la **liquidité** et la **mobilité** des actifs numériques, de **connecter** différentes communautés crypto jusqu'alors fragmentées, de déployer des **applications décentralisées** sur de **multiples chaînes** et simplifier leur **expérience utilisateur**.

## CONCEPTION DU RÉSEAU AXELAR

La plateforme **Axelar** est donc un ensemble d'outils dédiés à la **communication inter-blockchains**. Son point fort est que les développeurs n'ont pas besoin d'intégrations compliquées pour connecter une blockchain au réseau. Une simple **API** permet d'interagir avec n'importe quelle chaîne.



## Les nœuds validateurs

Il faut donc des **nœuds validateurs** pour **maintenir** le réseau Axelar et **sécuriser** sa blockchain. Le mécanisme de consensus utilisé est la **preuve d'enjeu déléguée** (*delegated proof of stake* ou **DPoS**). Ce sont les utilisateurs qui élisent les validateurs en déléguant leur *stake*. Le **pouvoir de vote** des validateurs est **proportionnel** à leur *stake*.

Les validateurs doivent exécuter le **logiciel client** de chaque blockchain connectée au réseau Axelar afin de connaître son **état**. Il n'est pas nécessaire de maintenir un nœud complet (une version légère du client suffit). Ils vont alors s'accorder sur l'état de chaque blockchain connectée au réseau. Une fois l'état de ces blockchains (Bitcoin, Ethereum, Stellar, etc.) connu, il est **enregistré** sur la **blockchain d'Axelar**.

## Signatures à seuil (*threshold signatures*)

Axelar permet donc de connaître l'état de toutes les blockchains connectées à son réseau à n'importe quel moment. C'est ce qui permet d'établir des **ponts** (*bridges*) entre ces blockchains et d'effectuer des opérations *cross-chain*.

Afin d'exécuter une **opération cross-chain**, comme un transfert d'actif, les nœuds doivent collectivement **approuver** l'opération. Ils



vont donc co-signer les transactions correspondantes. Le **seuil** requis est de **80 %**.

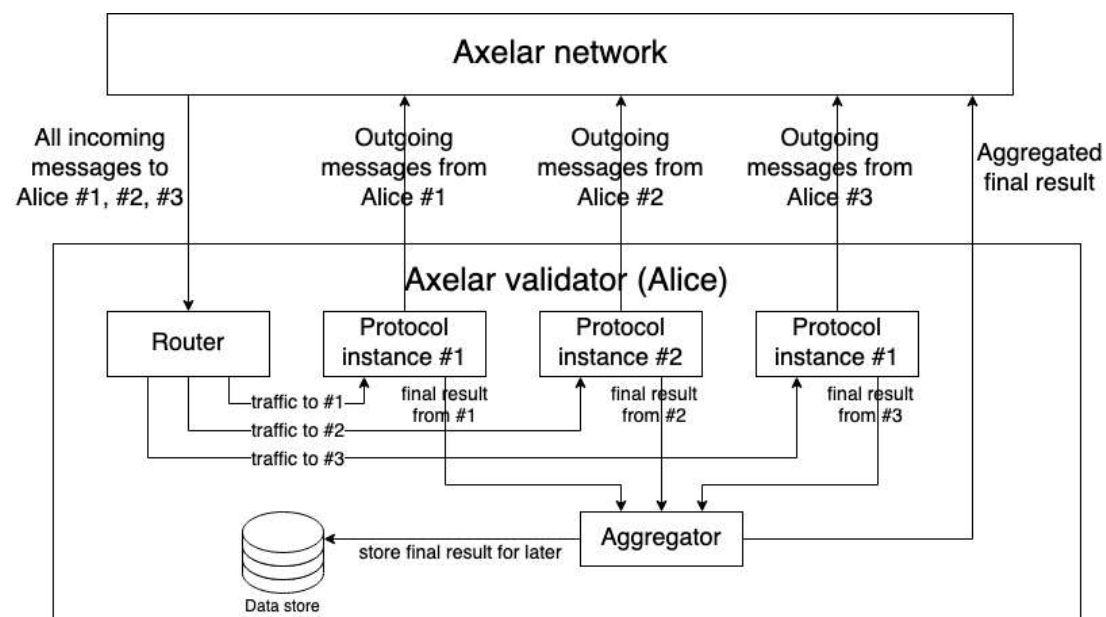
On peut ainsi définir Axelar comme un **oracle décentralisé cross-chain en lecture/écriture** (*decentralized crosschain read/write oracle*).

## LA SÉCURISATION DU RÉSEAU

La **sécurité** d'Axelar Network repose sur son algorithme de consensus, mais aussi sur le schéma des signatures. Le **consensus** utilisé est un **BFT** (*Byzantine Fault Tolerant*). Il est **partiellement synchrone** (un compromis entre synchrone et asynchrone), et tolère jusqu'à un tiers d'acteurs malicieux.

### Les signatures à seuil

Le mécanisme de signature permet à  $n$  parties de partager une **clef secrète**. N'importe quel sous-ensemble de  **$t + 1$  (ou plus)** parties peut alors collaborer et produire une signature. Cependant, il est **impossible** pour un sous-ensemble de  **$t$  (ou moins)** participants de produire une signature, ou d'obtenir une quelconque information quant à la clef secrète.



*Architecture des signatures à seuil sur Axelar (prenant en compte le poids du stake du validateur).*

Ce mécanisme présente plusieurs **propriétés intéressantes** :

- Il est **sécurisé contre une majorité malhonnête** (c'est-à-dire qu'il est résistant même si la majorité des n parties est malicieuse) ;
- Afin d'optimiser la charge des communications entre les parties, il utilise un **système de pré-signature** : une partie du travail de signature est effectué hors-ligne ;
- Il est impossible d'entraver la production des signatures pour des acteurs malhonnêtes (**robustesse**) ;
- Le réseau peut **détecter les acteurs malicieux** (et les punir).

## Résistance à la collusion

Au sein de sa **couche réseau**, Axelar repose sur divers mécanismes pour assurer sa sécurité. Il faut avoir à l'esprit que l'**interopérabilité** des blockchains engendre de **nouveaux vecteurs d'attaques**. Par exemple, les validateurs d'une certaine chaîne pourraient tenter de forger de fausses preuves (de l'état de la blockchain) pour voler des fonds sur une autre chaîne.

Afin de prévenir ce type d'attaques, Axelar a mis en place un **seuil de sécurité de 90 %** : les validateurs devraient alors quasiment tous colluder pour essayer de voler des fonds verrouillés. Cela suppose donc une **disponibilité maximale** des nœuds. Cependant, cela ne fait pas tout : en cas de problème (un trop grand nombre de validateurs hors-ligne, par exemple, qui entraînerait un arrêt du réseau), il faut des **mécanismes de repli (*fall-back*)** solides.

Le système mis en place par Axelar repose sur une **clé de déverrouillage d'urgence**, partagée entre des milliers de parties, comme la communauté d'une chaîne donnée. Cette clef permet ainsi de récupérer les fonds verrouillés en cas d'arrêt du réseau.

La **décentralisation** du réseau et des mécanismes de *fall-back* doit être **maximale** pour garantir le **meilleur niveau de sécurité**. Il n'y a pas de limites au nombre de validateurs sur le réseau Axelar (c'est une bonne chose pour le schéma des signatures à seuil). De plus, un **second ensemble** d'utilisateurs peut prendre le relai en cas d'arrêt du réseau dans le cas où le premier mécanisme de *fall-back* s'avère insuffisant.

Pour résumer, la **sécurité** du réseau repose sur un seuil très élevé de validateurs et sur une **décentralisation** maximale des parties assurant le **mécanisme de restauration**. Quant à la **gouvernance** d'Axelar, les utilisateurs pourront voter pour les blockchains qui seront connectées au réseau. Un **fonds d'urgence** est également disponible en cas d'imprévu, également soumis à la gouvernance des utilisateurs.

## CONCLUSION

**Le développement et l'adoption à grande échelle des nombreuses blockchains de l'industrie passera par des solutions de communication simples d'utilisation et universelles. Axelar se présente comme la couche de communication inter-chaînes ultime. Elle devrait permettre aux développeurs d'intégrer facilement de multiples chaînes pour leurs applications décentralisées, d'accéder aux liquidités de ces différents réseaux**

**ainsi que de toucher un maximum d'utilisateurs. L'avenir des cryptos est multi-chaînes.**

N'hésitez pas à visionner l'interview de Sergey Gorbunov, réalisée par Sami, en marge du Mainnet 2021 !

## RESSOURCES

- Le [site web](#) d'Axelar
- Le [whitepaper](#)
- [Discord](#)
- [Telegram](#)
- [Twitter](#)
- [YouTube](#)
- [LinkedIn](#)

## POUR ALLER PLUS LOIN

Bitcoin le 5 janvier 2022 - L'horizon écarlate des 40 000\$

Pépité crypto : Cosmos prêt à ATOM-iser de nouveaux sommets ?

Les paiements en cryptomonnaies bientôt sur AirBnB ? Le grand patron lance un pavé dans la mare

Samsung signe avec Cardano (ADA) pour planter 2 millions

d'arbres à Madagascar

Les prévisions explosives pour Bitcoin du patron de Nexo

Le géant du gaming Square Enix dévoile ses ambitions crypto pour 2022

Le DOGE de la colère - Mozilla déclenche la colère de sa communauté

DeFi, NFT, Ethereum 2... Coinbase anticipe les cartons crypto de 2022

## Morgan Phuc

Cofounder @ 8Decimals - Journal du Coin / BitConseil / Trading du Coin

> Plus d'articles de l'auteur(e)

## Entrez dans la cour des grands du trading de cryptos : nos

Afin de vous familiariser avec le trading de produits dérivés, nous vous proposons une entrevue complète de FTX et son interface de trading. Rappel : le

Le 16 févr. 2021 à 19h00

# Dans la même catégorie

---

**Taxation et  
régulation de Bitcoin  
et des crypto-actifs  
en France en 2022,  
l'heure du bilan**

Le **03 janv. 2022** à 10h00

---

**Guerre civile de  
Bitcoin : L'influence  
de l'User Activated  
Soft Fork (UASF)**

Le **02 janv. 2022** à 09h00

---

**Bitcoin et  
cryptomonnaies : Les  
10 thèses  
d'investissements de  
Messari pour 20**

Le **01 janv. 2022** à 14h00

---

**EPNS : un système de  
notifications pour le  
Web 3.0**

Le **23 déc. 2021** à 19h00

---

**Minute Régulation  
#4 : La  
réglementation de  
Bitcoin et des  
cryptomonnaies**

Le **19 déc. 2021** à 14h00

---

**Bitcoin et la guerre  
des blocs :  
l'impossible  
compromis sur la  
scalabilité**

Le **19 déc. 2021** à 09h00

---

**Le FOMO, pire  
ennemi de  
l'investisseur crypto -  
10 règles pour mieux  
le combattre**

Le **18 déc. 2021** à 09h00

---

**Guide : des  
transactions crypto  
plus rapides et moins  
chères grâce à  
Alchemy**

Le **12 déc. 2021** à 14h00



# RECEVEZ UN CONDENSÉ D'INFORMATION CHAQUE JOUR

Adresse email

Suivant

Toute l'actualité des cryptomonnaies, analyses, vidéos et guides.

Copyright © 2017-2022 8Decimals - Tous droits réservés.  
Contact | Mentions légales | Politique de confidentialité