Veille Technologique

Dorian BARET
Teva GEITNER

INFO5
2021-2022

Abstract

Several cryptocurrencies are emerging and getting more and more important because of the potential of their use. We are presenting the Elrond blockchain which is a cryptocurrency that holds our attention for its high potential. We investigated a lot on the Elrond project descriptions and especially on the different technologies that this cryptocurrency is using like Secure Proof of Concept and Adaptive State Sharding. Elrond stands out from the crowd for many reasons. First it uses a transaction method that permits to carry out more that 100 times more transactions per second than the other cryptocurrencies. This method also extremely reduce the co2 emission, which enabled Elrond to reach more than the carbon neutrality. Finally, the Elrond environment has a huge potential and could review our monetary system or be a fantastic opportunity for many projects to be launched which is the aim of the creation of the blockchain.

Présentation

Elrond est une entreprise et une technologie blockchain conçue essentiellement pour la finance et l'utilisation en entreprise. Le réseau Elrond est une blockchain publique, elle peut être consultée et utilisée par tout le monde.

Blockchain

La blockchain est en premier lieu une technologie de stockage et transmission d'informations sans organe central de contrôle. Ainsi la blockchain permet à ses utilisateurs de partager des données sans intermédiaire.

En pratique la "*blockchain est un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs, tous également détenteurs de ce registre, et qui ont également tous la capacité d'y inscrire des données, selon des règles spécifiques fixées par un protocole informatique très bien sécurisé grâce à la cryptographie"*.

Le fonctionnement de la blockchain se repose sur plusieurs concepts :

- l'identification des utilisateurs : permis par des procédés cryptographiques
- les transactions : l'échange de données
- les noeuds : ordinateurs, organisés sous la forme d'un réseau peer-to-peer, possédant la base donnée
- les blocs : ensemble de transactions valides et en attente d'être inséré dans la blockchain, ces blocs ont une taille limitée (1Mo pour le Bitcoin)
  Une transaction ne peut être que dans un seul noeud
- les mineurs : unités de calculs permettant de récupérer et traiter un ensemble de transaction afin d'émettre des blocs sur la blockchain
  Tous les mineurs sont des noeuds mais tous les nœuds ne sont pas des mineurs.

Lorsqu'un bock est émis sur la blockchain, les nœuds le réceptionnant vont vérifier la validité du bloc (respect du protocole informatique) et revérifier la validité des transactions.
Il suffit qu'un seul nœud rejette un bloc pour que les transactions soient annulées sur l'ensemble du réseau.

DeFi

La DeFi ou Finance Décentralisée est le concept de création de valeurs financières, accessibles à tous, sans autorité de régulation (c.a.d de façon décentralisée et sans intermédiaire), instantanée, transparente.

La DeFi est un concept ancien (exemple: transaction financière de particulier à particulier) remis au goût du jour avec la technologie blockchains. On parle alors de crypto-monnaies qui sont des devises numériques décentralisées utilisant la technologie de la blockchain.

Dans le cadre de DeFi, les mineurs sont récompensés grâce aux frais de transaction payés par les utilisateurs.

Smart Contract

Les contrats traditionnels définissent les règles d'un accord entre plusieurs parties mais ne permettent pas de vérifier que les clauses soient bel et bien respectées.

Un Smart Contract fixe lui aussi les règles d'un accord tout en s'assurant le transfert d'un actif lorsque les conditions contractuelles se vérifient. Ces conditions sont vérifiées lors de la validation d'une transaction par les nœuds d'une blockchain.
En pratique, un Smart Contract est un "bout" de code. Dans le cas de la blockchain Elrond ils sont écrits en Rust, C ou C++.

Coin et Token

Le coin est un actif qui appartient à sa propre blockchain. Par exemple EGLD, Ether, Bitcoin, sont des coins qui ont été créés respectivement sur les blockchains Elrond, Ethereum, Bitcoin.
Les tokens sont créés sur des blockchains existantes. En effet grâce aux smart contracts il est possible de créer une nouvelle crypto monnaie sur une blockchain déjà existante. La blockchain la plus utilisée pour la création de tokens est Ethereum avec plus de 40000 tokens créés à partir de cette dernière. Pour l'exemple d'Ethereum, ces tokens s'appellent ERC-20.
Tout le monde peut créer son propre token personnalisé. On pourrait imaginer une utilisation telle que celle d'un festival qui voudrait avoir sa propre monnaie et permettre des transferts simplifiés.

Ce qui fait que Elrond se démarque

Particularité de la blockchain Elrond

Dans un premier temps la blockchain Elrond fournit actuellement un débit de près de 15 000 transactions à la seconde contre 7 pour le Bitcoin et 20 000 pour Visa et Mastercard.
Une des promesses de cette blockchain est qu'elle permettrait d'évoluer vers des centaines de milliers de transactions par seconde à mesure que la demande augmente. On parle de scalabilité.

Pour permettre cela, l'architecture du réseau est un peu différente des autres blockchains traditionnelles. Elle intègre une technologie nommée "Adaptive State Sharding" ou partitionnement - *ce principe est déjà utilisé pour les bases de données*. En pratique les nœuds sont divisés en sous-ensembles qui ne vont vérifier qu'une partie des transactions (appelé Network Sharding). Elle partitionne aussi les états (State Sharding) et le traitement des transactions (Transaction Sharding) afin que chaque nœud du réseau n'ait à traiter qu'une fraction de toutes les transactions.
Ainsi cela permet le traitement parallèle des transactions. Tant qu'un nombre suffisant de nœuds vérifient chaque transaction, garantissant ainsi une fiabilité et une sécurité élevées, la division d'une blockchain en shards lui permettra de traiter beaucoup plus de transactions grâce à la parallélisation, améliorant ainsi considérablement le débit et l'efficacité des transactions.

Systèmes de validations

Comparaison avec les Proof of Work - Consensus du Bitcoin

La proof of work (preuve de travail) demande aux utilisateurs d'exécuter plusieurs fois des algorithmes de hachage ou de calculer des puzzles mathématiques pour valider les transactions. Cette méthode met tous les mineurs en concurrence et le mineur qui aura effectué les calculs le plus rapidement effectue alors la validation de la transaction et recevra une récompense. Autrement dit, c'est celui qui aura la plus grande puissance de calcul qui recevra le plus de récompenses. C'est ce qui a alors donné naissance aux fermes géantes de minage de crypto-monnaies principalement en Chine.
De plus, un inconvénient important de la proof of work est que la difficulté de minage est réajustée par intervalles réguliers (tous les 2016 blocks) pour réclamer une puissance de calcul de plus en plus gourmande aux mineurs. Ceci entraîne un lourd impact énergétique et environnemental.

Secure Proof of Stake - Elrond

La méthode de Proof est utilisée pour atteindre le consensus sur la chaîne de blocs et ainsi garantir la sécurité de la blockchain.
Chaque bloc contenant un ensemble de transactions, la validation de nouveaux blocs revient à valider les nouvelles transactions arrivant sur la blockchain.
La Secure Proof of Stake est donc une méthode qui va indiquer de quelle manière sont choisis les nœuds de validation.

En effet la SPoS demande à l'utilisateur de prouver la possession de 10 egld pour Elrond, pour pouvoir prétendre à valider des transactions et ainsi avoir des récompenses.
Au début de chaque cycle de création d'un bloc, le SPoS sélectionne des validateurs en utilisant une source de hasard qui ne peut n'être ni prédite, ni influencée, ce qui représente une garantie de sécurité concernant la validation. De plus, les nœuds de validation sont aussi sélectionnés en fonction de la quantité d'Egld stockés par leur opérateur ainsi que par la note qui lui est attribuée. Cette notation repose sur le comportement passé du validateur et est mise à jour à chaque cycle encourageant la méritocratie parmi les validateurs en les incitant à maintenir un bon fonctionnement.

Ethereum souhaite dans sa mise à jour 2.0 se baser sur du Proof of Stake.
Cette méthode présente beaucoup d'avantages comparé à la Proof of Work qui est beaucoup utilisée dans le monde des crypto-monnaies.

Environnement

Elrond devient la première blockchain européenne à émission négative de carbone !
C'est un titre extrêmement dur à atteindre quand on compare les émissions de carbone que produisent les autres blockchains.
En effet, la consommation annuelle du bitcoin est actuellement estimée à environ 100 TWh par an, soit près de la totalité de la consommation électrique des Pays-Bas. C'est sans compter les déchets électroniques qu'engendre le minage du bitcoin. Il est estimé que cette crypto-monnaie génère 30.000 tonnes de déchets électroniques à l'année, ce qui revient à environ 280 grammes par transaction.
Elrond a réussi à obtenir plus que la neutralité carbone grâce à son partenariat avec la société Offsetra qui lui permet d'obtenir pour une seule transaction une compensation carbone supérieure à son émission carbone. La compensation carbon revient à contrebalancer ses propres émissions de co2 par le financement de projets de réduction d'autres émissions.
L'empreinte évaluée à 6 millions de kg de CO_2, a été compensée par le retrait d'unités de carbone équivalentes à 7,4 millions de kg de CO_2, ce qui représente un impact positif de 25 % sur l'environnement grâce à la blockchain Elrond.

Usages

Token de gouvernance (mex)

Un token de gouvernance permet de donner le droit de vote aux utilisateurs qui en détiennent.
Dans le cadre MEX (le token de gouvernance de l'Elrond), cela permet de voter les changements des règles des Smart Contracts, de choisir si un projet peut rentrer dans le launchpad.

Ecosystème

Elrond possède tout un écosystème :

- Elrond Wallet
- Maiar exchange
- Application mobile Maiar
- Launchpad

Wallet

Un wallet ou portefeuille est un procédé de stockage sécurisé de crypto-monnaies. Il peut être physique ou numérique.

Maiar Exchange

Maiar Echange est une plateforme d’échange de cryptomonnaie inter et intra blockchain.

Maiar

Maiar est une application permettant d’échanger rapidement de l’argent entre utilisateurs sans passer pour une clé publique mais plutôt en utilisant des Herotags (identifiant unique) comme actuellement avec Lydia (numéro de téléphone) ou Paypal (adresse mail)

Launchpad

Le launchpad est un incubateur de projets ayant de fortes chances d'avoir un impact durable sur le monde. Il permet notamment de le financer via l'achat d'actions par les utilisateurs de la blockchain.

Ouverture

Alors que beaucoup de cryptomonnaies sont utilisées pour faire du trading en surfant sur la mode de la blockchain, de nombreux projets avec une réelle utilité voient le jour.

Il y a par exemple la société Bitland qui a mis en place un cadastre numérique propulsé par une blockchain pour le Ghana. Cela permet de rendre infalsifiable les actes de propriété et de les rendre plus accessibles à toute la population.
Alors que de nombreux pays et organisations ont aidé à la reconstruction d'Haïti après le tremblement de terre de 2010, la problématique majeure qui s'est présentée à été d'identifier les propriétaires légitimes de milliers de parcelles. Dans un cas comme celui-ci, une telle solution aurait été intéressante.

Un autre exemple, la société Civic Power a mis en place un système de vote électronique utilisant la blockchain. Ce qui permet d'assurer l'intégrité et la traçabilité publique des votes. Par ailleurs, la mairie de Neuilly-sur-Seine a lancé un projet similaire dans la volonté de redonner envie de voter et de permettre plus de décisions populaires.

L'objectif d'Elrond est de mutualiser les services sur une blockchain performante à hauteur des enjeux actuels de la société. Les deux exemples précédents sont des projets que Elrond pourrait permettre de lancer grâce à sa blockchain.

Bibliographie

[Bercy Info, 20/09/2019, Qu'est-ce que la blockchain ?]
https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application#

[Ab Consulting, 02/05/2019, Blockchain : fonctionnement du minage]
https://www.ab-consulting.fr/blog/blockchain/minage-7-etapes

[CoinHouse, 25/09/2020,Les tokens de gouvernance vont-ils tuer la DeFi ?]
https://www.coinhouse.com/fr/blog/actualites/les-tokens-de-gouvernance-vont-ils-tuer-la-defi/

[Claire Desombre, 06/10/2020, Qu'est-ce que la DeFi, cette finance décentralisée prête à changer les règles du jeu ?]
https://www.latribune.fr/opinions/tribunes/qu-est-ce-que-la-defi-cette-finance-decentralisee-prete-a-changer-les-regles-du-jeu-858938.html

[Gauthier Phion, 10/2021, Elrond : tout ce que vous devez savoir sur cette technologie]
https://rotek.fr/elrond-tout-savoir-technologie/

[Elrond, Technologie]
https://docs.elrond.com/technology/

[Qu’es ce que la proof of work]
https://bitconseil.fr/proof-of-work-definition-explication/

[Principe du SPoS]
https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-stake/secure-proof-of-stake-spos

[les particularités d’Elrond]
https://cryptoast.fr/elrond-erd/

[Emission de carbon de la blockchain Elrond]
https://medium.com/elrondnetwork-fr/elrond-devient-la-premi%C3%A8re-blockcha%C3%AEne-europ%C3%A9enne-%C3%A0-%C3%A9mission-n%C3%A9gative-de-carbone-ouvrant-ainsi-une-f8865134f4c3*