La richesse des réseaux cryptographiques

Première Proposition de Modèle Economique pour le Réseau Elrond

Elrond Team - v0.3.2
lucian.todea@elrond.com
Last update: 30 Sep. 2020

Traduction en langue Française
Dernière mise à jour de la traduction: 9 Nov. 2020

Crédits de traduction et relecture
(contributeurs Elrond France)

Clément A. (t.me/Myrayke)
Michel B. (t.me/Maxtrax75),
Yan Delcroix. (t.me/kryptchioyaya)
Kevin Lallement (t.me/edareisz)
Pascal Landeau (t.me/poussette)
Olivier. Lefevre (t.me/olivier_lefevre)
Philippe Martin (t.me/darkmanipulat)

Avertissement

Rien dans ce document ou sur le site elrond.com ne constitue une offre de vente ou la sollicitation d'une offre d'achat de jetons. Elrond publie ce document uniquement pour recevoir des retours et commentaires du public. Rien dans ce document ne doit être traité ou lu comme une garantie ou une promesse du développement de l'activité, des services ou du jeton d'Elrond, ou encore de l'utilité ou de la valeur du jeton. Ce document et le site Web elrond.com décrivent les plans actuels, qui pourraient changer à sa discrétion, et dont le succès dépendra de nombreux facteurs indépendants de la volonté d'Elrond, incluant les facteurs basés sur le marché ainsi que ceux des industries des données et de la crypto-monnaie, entre autres. Toute déclaration concernant des événements futurs est basée uniquement sur l'analyse d'Elrond des problèmes décrits dans ce document ou sur le site Web elrond.com. Cette analyse peut s'avérer incorrecte.
Elrond eGold (eGLD) n'intègre aucun lien avec l'or physique ou les instruments dérivés de l'or. eGLD n'est pas un «stablecoin» et peut être volatile et/ou perdre de la valeur. Aucune recommandation n'est faite ici quant à l'opportunité d'acheter eGLD; nonobstant, n'achetez pas eGLD si vous ne pouvez pas supporter la perte de la totalité du prix d'achat.

Préface

Pourquoi le capitalisme est-il actuellement sous tension ? Pourquoi les banques centrales ont-elles l'air si fragiles? Est-il possible d'aller au-delà du capitalisme et de trouver une meilleure approche? Le capitalisme peut-il se court-circuiter lui-même? [3] Pouvons-nous construire une alternative plus robuste, voire résiliente, où les systèmes "trop gros et voué à l'échec" ne sont plus présents? [21]

À travers Elrond, nous proposons une vision audacieuse pour un monde post-capitaliste, fournissant un nouveau modèle économique et un nouveau langage spécifiquement conçu pour l'ère de l'information.

Cet article décrit comment la monnaie native de la blockchaîne publique Elrond sera créée et frappée de manière algorithmique, pour maintenir les avantages en adéquation avec la santé et la sécurité du réseau à long terme. Cet article offre un aperçu temporaire des principes économiques régissant le réseau Elrond, tels qu'ils se présentent au moment de la rédaction.

Le jeton Elrond, eGold (eGLD), aura une durée d'amorçage prévue d'environ trois à cinq ans. Le jeton Elrond est inséparable du réseau Elrond, et donc intrinsèque à celui-ci. Des cas d'utilisation prévus d'eGold incluent la mise en gage (staking), la délégation, les paiements, les frais de location de stockage et de déploiement de contrats intelligents, ainsi que la récompense des validateurs qui contribuent aux performances, à la stabilité et à la sécurité du réseau.

Au cours des premières années, notre objectif sera de positionner Elrond en tant que service public mondial au sein de l'écosystème Internet, offrant une architecture de blockchain hautement évolutive, efficace et interopérable, avec une économie croissante basée sur ses jetons eGold natifs. Toutes les activités au sein du réseau, telles que le traitement des transactions, l'exécution de contrats intelligents, la fourniture de services tels que le jalonnement ou l'exécution d'un nœud de validation, seront alimentées par notre jeton natif. Les startups et les grandes entreprises pourront créer des applications décentralisées sur le réseau d'Elrond ou intégrer Elrond dans le cadre de leur solution d'infrastructure pour les produits et services.

Dans cette première phase, l'accès à un flux de valeur récurrent généré par le réseau est conditionné par la possession du token eGold, en tant qu'actif natif du réseau Elrond.

Après cette première période, nous prévoyons qu'eGold se prêtera naturellement, provisoirement, à devenir une monnaie ou un jeton de paiement, complétant les devises conventionnelles grâce à son mécanisme programmatique flexible. Cela signifie qu'eGold deviendra probablement un moyen d'échange efficace pour divers biens et services, puisque ses détenteurs pourront envoyer et recevoir eGold directement, mondialement et avec peu de frais via des transactions.

Une fois Elrond devenu un écosystème mondial prospère et un service public, on peut s'attendre à ce que le jeton devienne une solide réserve de valeur, en raison de la combinaison d'incitations programmables et des puissants effets de réseau sous-jacents régissant les architectures de la blockchaîne. Sa qualité en tant que réserve de valeur sera fonction des incitations économiques sous-jacentes amplifiées par l'adoption dans le monde réel, une transition conditionnelle définie vers un modèle économique déflationniste et une confiance accrue dans le réseau Elrond.

Le réseau Elrond, quant à lui, est une plate-forme de blockchaîne basée sur la preuve d'enjeu où un ensemble de validateurs, qui ont mis en gage un collatéral eGold, produisent des blocs en atteignant un consensus. Les validateurs sont récompensés par des eGold pour leur travail et ce collatéral. Cependant, si

un validateur décide de s'écarter intentionnellement des instructions du protocole, il risque de perdre une partie de son collatéral eGold mis en gage en raison de la sanction-couperet(slashing). L'ensemble des nœuds élus comme validateurs et leur affectation aux fragments change constamment (à chaque époque, soit environ une fois par jour, sur la base d'un processus d'enchères qui sera activé après le lancement de Mainnet), et ce nombre est limité en fonction des besoins courants du réseau en termes de sécurité et de débit.

Tous les détenteurs d'eGold peuvent participer indirectement aux mise en gage(staking) en déléguant leurs eGold à des validateurs existants, généralement des validateurs professionnels (prestataires de staking en tant que service), qui choisissent d'accepter des délégations. Un détenteur d'eGold désigne le candidat validateur en qui il a confiance et met un peu d'eGold en gage pour soutenir sa délégation. Si un ou plusieurs de leurs candidats sont élus validateurs à une époque, ils partageront avec eux toutes récompenses ou punitions économiques, proportionnelles à leur participation déléguée. Déléguer l'eGold est une manière d'investir son eGold, et de contribuer à la sécurité du système. Plus le montant total d'eGold mis en gage est élevé, plus la sécurité du système est élevée, grâce au montant croissant de la mise qui serait nécessaire à un adversaire pour que ses nœuds soient élus comme validateurs.

Nous visons donc à avoir à tout moment plus de 50% de l'approvisionnement en circulation mis en jeu.

Comment contribuer et donner vos retours

Cet article est la première ébauche publique du modèle économique d'Elrond. Les particuliers et les entreprises qui contribuent à cet article opèrent dans un environnement dynamique où de nouvelles idées et des facteurs de risque émergent continuellement. Ainsi, nous sommes constamment à la recherche de commentaires, avec de nouvelles hypothèses qui pourraient remettre en question et améliorer certaines parties de notre modèle. Nous encourageons ceux qui souhaitent contribuer à faire part de leurs commentaires sur le Forum d'Elrond.

Table des matières

1. Contexte

Il y a environ 70000 ans, les premiers humains modernes ont fait un saut évolutif important connu sous le nom de Révolution Cognitive. C'est cette révolution qui a permis aux Homo Sapiens de développer des capacités de réflexion et de communication particulièrement sophistiquées, qui, peut-être étonnamment, les amènent à devenir le prédateur dominant et le plus redoutable de la planète. [1]

Le développement du langage a été, sans aucun doute, l'un des facteurs les plus importants de l'ascension de l'Homo Sapiens. La langue a aidé à créer une compréhension commune entre les membres d'un groupe, facilitant la communication et l'échange d'informations et d'idées. Par conséquent, la confiance, la coopération et la coordination sont apparues comme des outils de plus en plus utiles et nécessaires, mettant à l'échelle des communautés primitives pour la première fois. Ainsi, les tribus ont créé des villages, qui se sont ensuite transformés en villes, puis certains se sont transformés en États-nations. Aujourd'hui, les États-nations ont été progressivement remplacés par le village mondial moderne hyper-connecté.

Les humains sont des animaux sociaux et tout au long de l'histoire, nous avons toujours vécu en communauté. Au début, la confiance et les transferts étaient plus sociaux, personnels et directs. Ensuite, ils sont devenus institutionnels, impersonnels et indirects (pensez aux intermédiaires) aux niveaux local et mondial. Mais pour chaque transition, de nouveaux outils et structures ont dû être inventés et appliqués, les anciens montrant leurs limites à chaque changement d'échelle.

L'aube de la révolution technologique annonçait une augmentation rapide du rythme des progrès. Le matériel, en particulier les transistors et les microprocesseurs, est devenu le poste budgétaire mondial majeur, la loi de Moore soulignant une tendance exponentielle que nous allions connaître. Les logiciels, pour la plupart propriétaires au début, ont ensuite capturé notre imagination, car il est devenu clair qu'ils consumaient sur le monde. Le mouvement open source a propulsé le logiciel au niveau supérieur, créant de nouveaux outils et normes permettant d'étendre la collaboration à l'échelle mondiale.

De plus, il est maintenant clair que nous sommes à l'aube d'un changement de paradigme majeur en matière de données et de confidentialité. Alors que les gens se réveillent en découvrant la valeur et les utilisations surprenantes de ce paradigme, nous prévoyons que de nouveaux outils permettront bientôt à chacun de collecter, gérer et monétiser ses données privées comme il le souhaite. De nouvelles lois nous donneront la propriété de ce qui aurait dû être des droits inaliénables, ce qui marquera la transition du féodalisme des données vers des marchés de données ouverts, permettant un échange productif fondé sur la propriété souveraine des données.

Si Internet était avant tout une question de collaboration et de numérisation du contenu, la prochaine vague technologique majeure devra apporter de nouveaux mécanismes de coordination et économiques qui peuvent évoluer à l'échelle mondiale, renforcer la propriété numérique des données et des biens et offrir un modèle de travail pour régir tout cela. C'est précisément là que Elrond entre en jeu.

1.1 L'argent programmable

Les humains ont inventé l'argent et l'écriture pour faciliter l'échange de valeur et d'informations. Ainsi, il est devenu plus facile d'effectuer des transactions économiques et potentiellement plus difficile de commettre une fraude. Les échanges économiques ont permis aux communautés de se développer, mais à mesure qu'elles grandissaient, il devenait de plus en plus difficile de les coordonner. Ainsi, nous avons développé des lois pour réguler les comportements des institutions et assurer leurs respect.

Aujourd'hui, de nouvelles technologies nous permettent d'étendre les échanges économiques au niveau mondial d'une manière différente et bien meilleure. Les réseaux décentralisés sécurisés par cryptographie ont introduit une forme de monnaie programmable avec des propriétés particulièrement précieuses qui gagnent en popularité.

Parmi les propriétés les plus importantes figurent les suivantes :

- Actifs de capitalisation
- Support d'échange: non censurable, bon marché et rapide
- Réserve de valeur: résistante aux saisies et à la censure, non souveraine
- Vie privée: anonymat à la demande, pseudo-anonymat et confidentialité
- Programmable via des contrats intelligents(logiciel), permettant une gamme de services financiers (décentralisés) (DeFi): instruments financiers pour dérivés, titrisation et tokenisation d'actifs, prêt, séquestre, hypothèque, assurance, mise en gage, délégation, garantie et bien d'autres.

Compte tenu des propriétés ci-dessus, nous pensons que la monnaie programmable est un marché encore balbutiant de plusieurs milliards de dollars. L'argent programmable facilitera un meilleur alignement des intérêts et permettra de nouveaux mécanismes pour capter la valeur, mais nous devons veiller à éviter de commettre les mêmes erreurs que dans les économies traditionnelles.

En prenant un peu de recul, l'impact d'Elrond visera à aller au-delà de l'argent, permettant progressivement aux données, à l'identité et à la propriété d'être transformées en actifs numériques via la tokenisation.

1.2 Crypto-économies

Définitions

La crypto-économie peut être décrite avec justesse comme l'utilisation de mesures incitatives et de la cryptographie dans la conception de réseaux décentralisés. Ce n'est pas un sous-domaine de l'économie, mais plutôt une application de la cryptographie qui prend en compte la théorie des jeux.
La théorie des jeux est la modélisation mathématique de l'interaction stratégique entre des agents rationnels (et irrationnels). La conception de mécanismes, en revanche, est un sous-domaine de la théorie des jeux, souvent appelée théorie des jeux inversés, car nous partons d'un résultat souhaité à l'esprit et travaillons à rebours pour concevoir un jeu qui en fait la promotion. Un jeu où des joueurs rationnels et intéressés produiront le résultat souhaité.

Donc, si la théorie des jeux consiste à choisir les meilleurs mouvements dans un jeu donné, la conception du mécanisme consiste à créer un jeu qui tient compte des mouvements que vous désirez.

Pour résumer, la crypto-économie se compose de deux éléments: la cryptographie qui est la partie du mécanisme assurant l'intégrité des mouvements passés, et l'économie qui est la partie du mécanisme garantissant que tous les acteurs effectuent les bons mouvements futurs.

Les garanties de sécurité économique de tout réseau cryptographique dépendent en partie de la solidité de ses hypothèses et de la façon dont les gens réagissent aux incitations économiques. Cependant, il convient de noter que la conception de mécanismes n'est pas une panacée et que la crypto-économie ne peut pas être appliquée dans le vide. Il y a une limite à la capacité de compter sur des incitations pour façonner de manière prévisible les comportements futurs.

Création d'un modèle
Plusieurs aspects sont pris en compte lors de la création d'un modèle économique crypto:

- Comportement souhaité de la part de tous les acteurs
- Des incitations économiques telles que des récompenses et des frais pour les acteurs qui se comportent bien, mais aussi des sanctions pour tout acteur qui pourrait avoir des motivations non désirées par rapport aux comportements souhaités
- Règles économiques (comme la notation, les sanctions ou les couperets(slashing)) qui découragent des comportements spécifiques: messages de protocole invalides, échec de production, omission des messages de protocole, action équivoque et autres.

Les aspects économiques des incitations mises en œuvre doivent tenir compte du fait que, quelle que soit la valeur monétaire d'un jeton particulier, il existe des facteurs qui influencent la bonne santé du système, à savoir:

- l'inflation doit être suffisamment faible pour ne pas «taxer» les détenteurs de jetons, mais suffisamment importante pour couvrir leurs coûts d'engagement (nœuds de fonctionnement)
- la masse monétaire mise en jeu doit être suffisamment importante pour qu'il y ait suffisamment d'entités distinctes et qu'une collusion soit peu probable, mais suffisamment petite pour que la vitesse de la monnaie ne soit pas affectée (MV=PQ)

Comme on peut le voir, la crypto-économie est la règle du jeu, mais comment changer les règles après leur mise en œuvre? La réponse est la gouvernance. La gouvernance est le pouvoir de changer les règles, et à mesure que le jeu devient plus précieux, la gouvernance devient le méta-jeu qui peut maintenir ou détruire cette valeur.

1.3 Gouvernance

Les réseaux décentralisés sécurisés par cryptographie fournissent une couche neutre de décentralisation, d'immuabilité, de confidentialité et de confiance. Les contrats intelligents peuvent ainsi être utilisés à la fois pour organiser des élections électroniques justes certifiées conformes ou pour faire des achats.

Compte tenu de leurs implications importantes et de grande portée, la conception d'un mécanisme de gouvernance efficace pour les systèmes décentralisés est une tâche ardue. De simples extrapolations de modèles de gouvernance du monde réel se révèlent naïves, et de nombreux réseaux crypto mourront probablement en raison d'une gouvernance défectueuse une fois que leur réseau atteindra une valeur suffisamment élevée pour qu'une gamme d'attaques décisives soit justifiée.

Ainsi, la gouvernance nécessite un examen séparé et approfondi. Le modèle de gouvernance d'Elrond sera présenté dans un article qui sera publié ultérieurement, après le lancement officiel du réseau Elrond. Auparavant, Elrond utilisera une solide approche de gouvernance hors chaîne pour garantir une vitesse et une efficacité maximales.

1.4 Termes et composants organisationnels

Une définition claire est nécessaire, pour les termes utilisés décrivant les différents acteurs et actions à l'intérieur du modèle économique d'Elrond.

Utilisateurs et participants au réseau

Toute partie, individu, entité, entreprise, blockchaîne ou réseau qui utilise, développe, crée ou interagit avec n'importe quel aspect du réseau Elrond. Les utilisateurs sont identifiés par une adresse de compte unique (dérivée de leur paire de clés publique-privée principale stockée dans un portefeuille).

Détenteurs de jetons.
Utilisateurs détenteurs de jetons eGold natifs, à utiliser sur le réseau Elrond pour soumettre des transactions signées pour des transferts de valeur, l'exécution de contrats intelligents ou pour fournir des liquidités.

Développeurs d'application
Les utilisateurs qui développent des contrats intelligents et / ou des applications qui reposent sur des contrats intelligents pour fournir des services. Les développeurs ont besoin d'un compte pour déployer des contrats intelligents sur le réseau.

Groupe de consensus
Pour qu'un bloc soit proposé et validé, un nombre spécifique de nœuds (*numNodesConsensus*) est sélectionné au hasard parmi tous les nœuds éligibles (*eligibleNodesPerShard*) assignés à un fragment pour former le groupe de consensus à chaque tour (*blockTime*). Le groupe de consensus a la responsabilité d'engager des blocs dans ce fragment, à chaque tour. Au début de chaque tour, un nouveau groupe de consensus est sélectionné. Le groupe de consensus dans le fragment Metachain est configuré de sorte que *numNodesConsensus = eligibleNodesPerShard*, faisant effectivement de tout le fragment Metachain le groupe de consensus. Ceci est motivé par les exigences de sécurité élevées de la métachaîne.

Noeuds
Dispositifs (ordinateurs ou serveurs) exécutant le logiciel (le client Elrond) et relayant les messages reçus de leurs pairs. Ils peuvent être soit des validateurs (participant activement à la sécurisation du réseau), soit des observateurs (membres passifs du réseau pouvant servir d'interface de lecture et de relais) et peuvent être soit des nœuds complets (avoir l'historique complet de la blockchain), soit des nœuds légers (uniquement garder 2 époques de l'histoire de la blockchaîne). Un nœud est sur la liste des nœuds éligibles si plusieurs exigences sont remplies: une note supérieure à un seuil spécifique, a remporté un emplacement de nœud dans l'enchère de sélection (lorsque l'enchère sera activée), a été affecté à un fragment, etc.

Type de noeuds	Participants	Non-Participants (Observateurs)
Complet	Nœud gardant une trace de chaque transaction dans le réseau et mettant également un collatéral eGold en gage pour participer au mécanisme de consensus (validateur)	Nœud conservant un enregistrement de chaque transaction qui se produit dans son fragment. Pas de collatéral mis en gage et donc ne propose ni ne signe de blocs.
Léger	Nœud qui a un enjeu (tout comme un validateur) et ne conserve que les enregistrements des transactions dans la ou les époques les plus récentes	Pas d'engagement et garde seulement 2 époques d'historique de la blockchaîne

Validateurs
Les validateurs sont des nœuds - des ordinateurs sur le réseau Elrond qui traitent les transactions et sécurisent le réseau en participant au mécanisme de consensus, tout en gagnant des récompenses grâce au

protocole et aux frais de transaction. Afin de faire partie du réseau Elrond, un validateur doit engager une garantie sous la forme de jetons eGold, qui sont mis en place pour aligner les incitations des validateurs sur le bon fonctionnement du réseau. Les validateurs risquent de perdre une partie ou la totalité de leur mise s'ils s'écartent des instructions du protocole ou s'entendent pour perturber le réseau. Pour qu'un nœud puisse devenir un validateur, il doit figurer sur la liste des nœuds éligibles.

Proposant de bloc
Le rôle de proposant de bloc est désigné pour le premier nœud de validation sélectionné (via un processus aléatoire et impartial) dans le groupe de consensus. Le proposant de bloc est le validateur qui propose le bloc suivant, que le reste du groupe de consensus doit vérifier et approuver.

Récompenses de bloc
La blockchaîne récompensera les nœuds de validation pour leur collatéral eGold engagé. La récompense peut être de deux types: une partie des frais de transaction et une nouvelle émission d'eGold (également appelée frappe ou inflation). Les détenteurs d'eGold qui ne mettent pas leur eGold en gage en étant un validateur ou en déléguant leur eGold à un validateur, ne recevront aucune des récompenses de bloc.

Fragments ou partitions
À tout moment, le réseau se compose d'un certain nombre de fragments, chaque fragment contenant un sous-ensemble de toutes les adresses et leur état associé, y compris les adresses de compte d'utilisateur et les adresses de contrat intelligent. Chaque fragment exécute sa propre blockchaîne, mais tous les fragments sont connectés via la métachaîne.

Métachaîne
Une blockchaîne fonctionnant en parallèle et de manière synchrone avec les fragments, utilisée pour notariser les blocs validés par les fragments et également pour la communication entre les fragments. Tous les validateurs éligibles de la métachaine participent à son consensus. Au lieu de choisir un groupe de consensus, la source aléatoire est utilisée uniquement pour choisir un producteur de bloc. Le producteur de blocs Metachain compose un métablock qui se compose d'informations d'en-têtes de partition et d'en-têtes de minibloc, dont chacun doit être confirmé par au moins un bloc de partition dans sa partition correspondante. Le proposant du bloc Metachain crée également le bloc «début d'époque» si nécessaire. La métachaine est également responsable de l'engagement / du désengagement / de l'emprisonnement (changements dans la configuration du validateur) et de la sanction-couperet.

Pérennisation du protocole
La pérennisation du protocole a pour but d'augmenter la sécurité et la valeur du réseau à court, moyen et long terme. Les spécificités de la gouvernance et de la gestion de la trésorerie du protocole seront présentées dans le document de gouvernance. D'ici là, la trésorerie du protocole sera sous le contrôle et la supervision de l'équipe Elrond Core.

Organe de gouvernance du protocole
Une organisation autonome décentralisée auto-organisée, supervisée par une fondation à but non lucratif.

Plus d'informations sur les aspects techniques sont détaillées dans le livre blanc .(https://elrond.com/assets/files/elrond-whitepaper.pdf) qui décrit en détail l'architecture du protocole Elrond
(NDT:traduction en langue française:
https://github.com/elrond-fr/livre-blanc/raw/master/Elrond_Whitepaper_FR.pdf)

2. Validateurs

Afin de sécuriser le réseau, Elrond utilisera un modèle de preuve d'enjeu.

Contrairement aux systèmes Proof-of-Work (PoW), Elrond n'a pas besoin de machines pour résoudre les équations de blocs. Au lieu de cela, toute la puissance de calcul du réseau est utilisée pour les transactions réelles, par conséquent, avec Proof-of-Stake, l'économie d'énergie est substantielle. De plus, Elrond ne nécessite pas de GPU ou de puces spécialisées pour prendre en charge le réseau: vous pouvez contribuer et prendre en charge le réseau en utilisant le matériel que vous avez déjà (s'il répond aux exigences minimales: processeur double, processeur compatible SSE4 et x64, 4 Go de RAM, 80 Go de disque dur).

Dans les systèmes Proof-of-Work (PoW) où un mineur remporte tout (récompense de bloc + frais de transaction), il n'y a qu'un seul moyen d'améliorer vos chances de succès: augmenter votre puissance de hachage. Cela conduit à trois résultats: i) il devient peu rentable pour les appareils de petite / faible puissance de participer, ii) la mise en commun massive des ressources devient souhaitable et iii) la spécialisation du matériel devient nécessaire.

En revanche, le système Proof-of-Stake (PoS) ne repose pas sur des récompenses pour la sécurisation du réseau, mais plutôt sur des pénalités. Les validateurs mettent de l'argent («dépôts de garantie») en gage et sont indemnisés pour le blocage de leur capital et les frais de maintenance du nœud. La majeure partie du coût occasionné en allant à l'encontre des règles provient de sanctions qui sont des centaines ou des milliers de fois plus importantes que les récompenses qu'un attaquant pourrait obtenir entre-temps. Donc, si dans le PoW les mineurs sont en concurrence les uns avec les autres, dans le PoS, les validateurs collaborent les uns avec les autres.

De cette manière, un réseau PoS est beaucoup plus économe en ressources, plus évolutif et plus inclusif pour maintenir un réseau blockchaîne public décentralisé (sans autorité centrale). En regardant les chiffres rassemblés dans les premiers réseaux PoS et les deux plus grands réseaux PoW (Bitcoin et Ethereum), nous pouvons voir que l'argent dépensé pour l'infrastructure est d'un ordre de grandeur plus petit dans PoS que dans PoW (environ 10% des récompenses au lieu de 100%).

Par conséquent, avec Elrond, il n'y a pas de minage. Au lieu de cela, les validateurs gagnent des jetons pour faire un travail utile. L'un des aspects les plus importants que nous avions à l'esprit lors de la conception du réseau Elrond était l'obtention de garanties d'équité pour tous les participants du réseau. Dans le cas des validateurs, nous avons conçu Elrond pour être résistant à la concentration des ressources et pour assurer une répartition égale et équitable des récompenses en fonction du travail effectué par tous les validateurs, qu'ils soient petits ou grands.

Les participants au réseau apportent de la valeur au réseau. Plus il y a de validateurs, plus de collatéral eGold est mis en gage et plus la sécurité et la décentralisation du réseau sont élevées. Étant donné que les réseaux partitionnés tels que Elrond nécessitent un nombre minimal de validateurs pour former plusieurs fragments bien sécurisés, nous avons développé un client de validation qui fonctionne sur du matériel grand public standard sans exigence de configurations complexes et longues.

2.1 Sélection des validateurs

L'un des principaux objectifs que nous avions à l'esprit lorsque nous avons conçu le protocole Elrond était une évolutivité élevée. Nous y parvenons en partitionnant le réseau en fragments, ce qui permet le traitement parallèle des blocs. Plus de validateurs signifie que plus de fragments peuvent être créés, de sorte que le réseau peut traiter plus de transactions et est donc évolutif. Ceci étant, nous devons prendre en compte le fait que le nombre de validateurs et de fragments doit correspondre étroitement aux besoins effectifs du réseau à un instant donné (y compris - jusqu'à un certain point - une augmentation soudaine de l'utilisation). Étant donné qu'un trop grand nombre de fragments signifie que le protocole sous-utilise les ressources et que les coûts sont plus élevés que nécessaire, nous devrions viser à ce que tous les fragments aient une charge d'environ 50% (*targetShardLoad*).

C'est pourquoi nous prévoyons un lancement progressif du réseau principal, où le nombre de nœuds est limité à un nombre spécifique (*numNodes*). Cette limite peut augmenter, à la fois avec la progression des phases et avec les besoins du réseau, en gardant un équilibre entre sécurité, décentralisation, efficacité et besoins attendus du réseau, notamment en termes de débit, de disponibilité des données et de stockage.

Il y aura un nombre limité de noeuds par fragment (*nodesPerShard*), donc le nombre de noeuds (*numNodes*) augmentera proportionnellement au nombre de fragments dont le réseau a besoin pour le traitement et le stockage. Ainsi, un nombre minimum de 3 fragments (plus la métachaîne) est formé pour que la réorganisation des fragments à la fin de l'époque fasse sens.

Il y aura un prix de réserve minimum prédéfini pour le nœud, pour établir un *nodePrice* plancher. Le prix minimum de réserve du noeud peut être un montant fixe en eGold ou indexé sur un montant fixe en USD.

Afin d'amorcer le Mainnet Elrond, à la Genèse, nous avons déployé un système d'engagement et de délégation fermé. Cela signifiait un no-in et no-out temporaire pour les validateurs ou les délégataires. Le processus d'amorçage a été conçu pour atteindre une vitesse d'échappement et rassembler une communauté suffisamment grande autour du réseau Elrond. Un autre objectif que nous avions à l'esprit était de créer des moyens de dissuasion économiques prohibitifs contre les attaques réseau, en garantissant que plus l'offre est verrouillée dans l'engagement, plus les coûts d'attaque sont importants pour les acteurs malveillants .

Au moment de la genèse, le Mainnet a été amorcé avec un engagement fixe par nœud, 2500 eGLD et un nombre fixe de validateurs: 2169, formant 3 fragments et une métachaîne.

Le passage de cette période de bootstrap à un modèle de croissance durable se fera par étapes.

- Les phases 1 et 2 permettront aux validateurs et aux délégataires de se mettre en file d'attente afin que le nombre de nœuds reste fixe ou supérieur à un certain seuil, tout en permettant aux nouveaux membres de la communauté de patienter en déléguant ou en engageant leurs jetons eGLD et permettre de réserver une place dans cette file d'attente. Ces files d'attente permettront également aux délégataire et aux validateurs existants de retirer leur mise s'ils le souhaitent, les remplaçant ainsi par les premières réservations en file d'attente.

- Les phases 3 et 4 comprendront des fonctionnalités telles que: l'augmentation du nombre total de nœuds, la possibilité d'engager plus de 2500 eGLD par nœud, la délégation ouverte avec un nouveau

contrat intelligent de délégation de système grâce auquel tout le monde peut recevoir et accepter des délégations, et un nouveau système d'enchères amélioré (soft) . La transition vers les phases 3 et 4 inclura également, très probablement, notre premier vote communautaire en chaîne (on-chain).

2.2 Notation des validateurs

Comme pour tout réseau décentralisé et sans autorisation, nous nous attendons à voir la participation de nombreux validateurs, de différents horizons, utilisant différentes spécifications matérielles, configurations d'infrastructure, connexions Internet, bande passante, etc. Cela conduira à des performances différentes en termes de disponibilité, temps de réponse, temps de calcul, etc. Si ces variations sont acceptables et attendues, plus le réseau est décentralisé, plus il devient clair que des actions spécifiques sont plus souhaitables, tandis que d'autres ne le sont pas. Gardez à l'esprit que lorsque nous discutons de la notation, nous nous référons en général au temps de fonctionnement et aux performances du matériel / de la configuration (se manifestant par le nombre de blocs proposés et signés avec succès), et non au comportement et aux actions contre le protocole, qui sont couverts par la section 2.3 Sanction-couperet "slashing" (double signature, action équivoque, etc.).

Grâce au mécanisme de notation, nous récompensons les performances souhaitées (telles que la disponibilité et la proposition correcte d'un bloc), mais nous pénalisons également les actions indésirables affectant les performances du réseau (telles que les propositions de bloc manquantes). Plus la note d'un nœud est élevée, plus les chances d'être sélectionné en tant que validateur de consensus dans un tour sont élevées (ce qui implique d'avoir la possibilité de gagner des récompenses). À l'inverse, plus la note est basse (mais au-dessus d'un seuil de notation *ratingThreshold* de valeur pré-configurée), plus les chances d'être sélectionné comme validateur sont faibles. La récompense ou la pénalité est effectuée simplement par une augmentation ou une diminution de la note du nœud, donc aucune sanction-couperet n'est impliqué.

La notation d'un nœud est une valeur entière comprise entre 0 et 100 inclus. Toutes les évaluations sont stockées par la métachaine, qui suit l'activité des nœuds tour après tour, et à la fin d'une époque, la métachaine ajuste les évaluations en conséquence. Chaque nœud rejoint le réseau avec le même *startRating* initial, qui est conservé et ajusté époque après époque.

La table 1 présente quantitativement la manière dont l'évaluation d'un nœud augmente ou diminue ses chances d'être sélectionné comme validateur de consensus (sujet à changement dans le temps lorsque davantage de données seront disponibles).

Table 1

Intervalle de notation	Modificateur de chance
0-10	-100%
10-20	-20%
20-30	-15%
30-40	-10%
40-50	-5%
50-60	0%
60-70	+5%

70-80	+10%
80-90	+15%
90-100	+20%

Un nœud de validation peut augmenter sa note de deux manières:

1) Maintenir un bon niveau de signature des blocs proposés. Chaque fois qu'un nœud est choisi pour être un validateur de consensus, sa note sera implicitement augmentée par la valeur *validatorRatingIncrease*, entrainant un bon niveau de signature de bloc.
2) Proposer un bloc valide lorsqu'il est sélectionné pour être le proposant du bloc (i.e: le leader du consensus). Un bloc valide entraînera une augmentation de la note du proposant de bloc de la valeur *proposerRatingIncrease*.

Pour qu'un nœud soit éligible pour recevoir *validatorRatingIncrease* lors de sa sélection pour le consensus, il doit avoir signé un pourcentage minimum de blocs sur la dernière séquence continue de *numValidatedBlocksRange* pour laquelle il a été validateur (le comptage à l'époque précédente est autorisé). Le pourcentage de blocs signés doit être égal ou supérieur à la valeur de *signedBlocksThreshold*. La raison derrière cette approche est le fait que pour qu'un bloc proposé soit validé, seules ⅔ +1 signatures sont nécessaires. Nous nous attendons à ce qu'un nœud ait sa signature présente sur au moins certains blocs sur un laps de temps (ou un nombre de blocs) spécifique, suffisamment long, afin d'augmenter sa note de validation. Cette limite doit être suffisamment élevée, nous n'encourageons donc pas les nœuds parasites qui ne signent pas réellement des blocs, mais ne font que proposer des blocs lorsqu'ils se trouvent être des proposants de bloc. D'un autre côté, les nœuds qui sont toujours lents et qui ne sont pas en mesure d'envoyer leur signature pour les blocs dans le temps requis cesseront, à un moment donné, de recevoir une augmentation de notation pour avoir été sélectionnés dans un groupe de consensus, car leur pourcentage de blocs signés sera tombé en dessous du *signedBlocksThreshold*. De plus, dans cette situation, ils pourraient commencer à perdre des points de notation (à mettre en œuvre ultérieurement).

Le modèle de notation est ainsi conçu pour encourager au maximum les nœuds productifs, soit comme validateurs, soit comme proposants. L'une des principales préoccupations de conception concerne la durée dont aurait besoin un nœud idéal pour atteindre la note maximale, après avoir rejoint le réseau. Cette durée est nommée *HoursToMaxRatingFromStartRating* et correspond au nombre de secondes attendu nécessaire à un nœud pour atteindre progressivement la note maximale (*maxRating*) dans des conditions idéales, à partir de la valeur de notation initiale, *startRating*. La valeur de *HoursToMaxRatingFromStartRating* sera probablement configurée pour être égale à quelques jours.

À partir de *HoursToMaxRatingFromStartRating*, le modèle définit les fonctions *avgValidatorRatingPerRound(·)* et *avgProposerRatingPerRound(·)*, qui expriment le nombre moyen de points de notation gagnés par un nœud idéal, par tour, lorsqu'il est sélectionné comme validateur et comme proposant, respectivement. Ces fonctions dépendent du *HoursToMaxRatingFromStartRating* précédemment mentionné, ainsi que de la topologie du fragment, de la configuration du groupe de consensus et de l'*importanceRatingRatio*, une proportion fixe définie comme:

$$importanceRatingRatio = \frac{avgProposerRatingPerRound(\cdot)}{avgValidatorRatingPerRound(\cdot)}$$

Cette proportion équilibre le nombre de points de notation gagnés par les validateurs par rapport aux proposants, une nécessité étant donné qu'il est beaucoup plus susceptible d'être sélectionné comme validateur dans un tour, plutôt que comme proposant. Pour les proposants de bloc, il est souhaitable que la

contribution globale à la notation du *proposerRatingIncrease* total attribué à une époque soit idéalement la même que le total du *validatorRatingIncrease* attribué. Les définitions exactes de *avgValidatorRatingPerRound(·)* et *avgProposerRatingPerRound(·)* sont actuellement en développement, car elles dépendent du modèle choisi pour l'algorithme de sélection du consensus.

Les valeurs de *validatorRatingIncrease* et *proposerRatingIncrease* peuvent être exprimées comme suit:

$$validatorRatingIncrease = \frac{(maxRating - startRating)}{avgValidatorRatingPerRound(\cdot)}$$

$$proposerRatingIncrease = \frac{(maxRating - startRating)}{avgProposerRatingPerRound(\cdot)}$$

La volonté actuelle est de maintenir à la fois *validatorRatingIncrease* et *proposerRatingIncrease* à des valeurs constantes. Pour y parvenir, les définitions de *avgValidatorRatingPerRound(·)* et *avgProposerRatingPerRound(·)* doivent être ajustées en conséquence, car elles modifient la notation d'un nœud, ce qui à son tour altère sa probabilité d'être sélectionné pour le consensus. Comme expliqué précédemment, cela affecte alors la notation, formant une boucle de rétroaction contrôlée. Des alternatives non constantes pour *validatorRatingIncrease* et *proposerRatingIncrease* sont également envisagées par l'équipe.

Outre l'augmentation de sa note, un validateur pourra voir sa note diminuée s'il ne parvient pas à proposer un bloc valide lorsqu'il est sélectionné comme proposant de bloc, quelle que soit la raison de l'échec. Chaque fois qu'un proposant de bloc ne remplit pas son rôle, sa note sera ajustée avec la pénalité suivante:

$$proposerRatingDecrease = -4 \cdot proposerRatingIncrease$$

Un validateur qui est hors ligne ou qui ne peut pas ou ne veut pas produire ou signer de nouveaux blocs verra sa note diminuer beaucoup plus rapidement qu'elle n'aurait augmenté. Cela peut être encore accéléré si davantage de nœuds ont leur note inférieure à *ratingThreshold*.

Lors de la phase de mise en œuvre , il appartient d'éviter de pénaliser les proposants de bloc honnêtes après un tour malveillant (1 bloc avant) en différant le bloc.

La métachaîne sélectionne son groupe de consensus différemment. Alors que la sélection du proposant de bloc est en effet la même que dans les autres des fragments, tout nœud qui n'est pas le proposant de bloc devient automatiquement un validateur de consensus. Cela s'explique par le fait que le groupe de consensus dans la métachaîne est configuré pour avoir la taille du fragment entier, ce qui augmente la sécurité. Afin de maintenir la cohérence avec les autres fragments, la métachaîne remplace la définition de *validatorRatingIncrease* par *validatorRatingIncreaseMeta*:

$$validatorRatingIncreaseMeta = \frac{(maxRating - startRating)}{avgValidatorRatingMetaPerRound(\cdot)}$$

Les attributions de notation et les pénalités pour les proposants de bloc dans la métachaîne restent les mêmes que dans les fragments:

$$proposerRatingIncreaseMeta = \frac{(maxRating - startRating)}{avgProposerRatingPerRound(\cdot)}$$

$$proposerRatingDecrease = -4 \cdot proposerRatingIncreaseMeta$$

Afin d'accélérer l'élimination des nœuds potentiellement hors ligne, nous mettrons en œuvre une pénalité qui augmente à chaque échec consécutif à proposer un bloc lorsqu'il est choisi comme proposant. Cette valeur est le *proposerPenaltyGrowth* (dans la configuration de Genesis, elle s'appelle "*consecutiveMissedBlocksPenalty*" et peut être définie différemment sur les fragments et la métachaîne; la valeur par défaut est actuellement de 1,1, augmentation de 10% de *proposerRatingDecrease*), configurée de manière à ce qu'un nœud qui échoue constamment à proposer des blocs lorsqu'il est sélectionné en tant que proposant de bloc verra sa note sera réduite en dessous du seuil de notation *(ratingThreshold)* en approximativement 10 heures, ce qui le rend inéligible pour participer à l'enchère ou au processus suivant de sélection de validateur. De plus, un nœud qui échoue à proposer tous les blocs (lorsqu'il est sélectionné comme proposant de bloc) au cours d'une époque, ne sera éligible à aucune récompense au titre de cette époque.

Pour qu'un nœud avec une note inférieure au *ratingThreshold* soit reconsidéré pour être remis sur la liste des validateurs éligibles, une transaction spéciale unJail (*resetRating*) doit être envoyée à la métachaîne et validée. Afin d'encourager l'inclusion de la transaction *resetRating*, le nœud doit inclure un *resetRatingFee* dans le cadre de sa transaction, que se verra attribuer le proposant de bloc qui l'inclut. La ligne de pensée actuelle est de faire en sorte que le montant de resetRatingFee soit au moins égal à la moyenne des récompenses gagnées par un validateur au cours de la dernière époque. Lors du Genesis, cela a été configuré à 0,1% du *nodePrice* et il n'y a pas de transaction de réinitialisation effective, mais une transaction *unJail* (seulement si le nœud est déjà emprisonné) qui permet la réinitialisation.

Notez que nous ne sanctionnons(slashing) pas un validateur dont la note a chuté en dessous de *ratingThreshold*. Toutefois, les nœuds avec une note inférieure à *ratingThreshold* ne gagnent plus de récompenses et ne sont plus considérés comme éligibles pour faire partie des groupes de consensus. De plus, à la fin de l'époque, ils seront également automatiquement expulsés du pool de reconduction pour la prochaine sélection de validateur si le nombre minimum de nœuds par fragment n'a pas été atteint.

Un validateur est incité à conserver une note de nœud au-dessus de *ratingThreshold*, pour conserver l'opportunité de faire partie du pool de validateurs, sinon cela entraînera la perte de récompenses pendant au moins 2 époques. De plus, conserver une note élevée augmente les chances d'un validateur d'être sélectionné dans un groupe de consensus.

La définition exacte du modèle statistique de notation est en cours d'élaboration et est fortement liée à l'algorithme de sélection par consensus, qui, comme décrit précédemment, utilise la notation d'un nœud pour augmenter ou diminuer sa probabilité d'être sélectionné.

Dans l'implémentation actuelle, l'algorithme de sélection par consensus peut être modélisé à l'aide d'une distribution basée sur la distribution hypergéométrique centrale multivariée. Des algorithmes alternatifs et leurs implémentations sont également en cours d'étude.

Une simulation, basée sur certaines hypothèses initiales et des valeurs configurées, peut être vue ici: https://docs.google.com/spreadsheets/d/1DzeeJvLvS5H7XrH24QURyYQJ9QqyaUG5yzUDwyl5yY4/edit#gid=267148288.

2.3 Sanction-couperet(slashing)

Les actions entreprises par les validateurs, telle que l'exécution d'autres clients ou de code modifié à partir du client officiel, peuvent être préjudiciables au fonctionnement du réseau, et nécessitent donc des mesures punitives dans le cadre d'un système PoS. La sécurité d'un système PoS est assurée par des incitations sous forme de récompenses et de pénalités. En exigeant que les validateurs mettent “leur peau en jeu” via une mise en gage d’eGold verrouillé, ils seront fortement découragé à agir de manière malveillante étant donné la menace qui pèse sur leur mise en gage.

Dans le réseau Elrond, l'ensemble du processus de sanction peut être décrit à travers un processus de déclencheurs pouvant impliquer différents acteurs:

1. Détection
2. Signalement
3. Vérification
4. Effet

La **détection (1)** est effectuée par un nœud qui a accès au bloc qu'un validateur malveillant crée / signe, et peut vérifier l'exactitude de ce bloc. Il peut s'agir de n'importe quel nœud du fragment sur lequel l'action malveillante a été effectuée. Étant donné que tous les nœuds du fragment traitent tous les blocs produits, cela signifie que tout nœud d'un fragment (validateur ou observateur) peut détecter les actions indésirables définies. Cela permet à tout nœud exécutant le code officiel d'Elrond, de détecter et de fournir des preuves de l'action indésirable observée, de vérifier la validité des preuves fournies et d'être récompensé si une telle preuve a été validée. Les nœuds qui détectent et fournissent la preuve des actes répréhensibles sont appelés des **pêcheurs** (ou challenger).

Il y aura un commutateur d'option supplémentaire pour les validateurs, pour activer ou désactiver le rôle pêcheur / challenger, ce qui nécessitera la configuration d'une clé privée valide associée à un portefeuille contenant des fonds.

Le **signalement (2)** d'une action malveillante observée se fera via une transaction spéciale (il peut être nécessaire d'avoir 2 transactions avec un schéma de validation afin d'éviter les attaques frontales). La valeur transférée dans une telle transaction sera dissuasive pour éviter de générer de faux défis. La raison d'utiliser les transactions comme défis est double: le mécanisme devrait empêcher le spamming et garantir une récompense, étant donné que la validation de ces défis nécessitera une consommation de bande passante non négligeable (transferts de données pour les preuves) et du temps de traitement.

La structure d'une telle transaction est similaire à celle d'un appel normal de contrat intelligent et est détaillée ci-dessous:

- **sender** – adresse du portefeuille de l'opérateur du nœud
- **destination** – adresse fixe pour le contrat intelligent du protocole de couperet(slashing)
- **gas price** – le prix du gaz
- **gas limit** – la limite de gaz
- **value** – valeur fixe non triviale pour tout défi (à déterminer ultérieurement)
- **data** – paramètres pour le contrat intelligent de vérification - quelle fonction appeler et ses paramètres. La fonction appelée doit être la fonction de preuve de l'action malveillante

observée, et les paramètres les données requises pour la vérification (par exemple, les données d'en-tête, les données de bloc, les preuves de merkle, etc.)

Le prix du gaz et la limite de gaz doivent être fixés pour que le protocole du contrat intelligent prenne en compte le chemin le plus long (preuve la plus complexe d'un scénario).

Comme mentionné précédemment, le rapporteur d'une situation défavorable / malveillante sera appelé «Pêcheur» - car il recherche des activités malveillantes, ou «Challenger» - car il conteste toute situation défavorable qu'il découvre. Le pêcheur, comme mentionné précédemment, peut être soit un validateur dans le réseau Elrond, soit simplement un nœud d'observateur.

Cela signifie que le pêcheur n'a besoin d'aucune participation dans le réseau, mais a toujours besoin d'un portefeuille et de jetons Elrond suffisants pour lancer des défis. Dans le cas où le défi est démontré valide selon les preuves fournies, la valeur transférée via la transaction de défi est retournée à l'expéditeur, ainsi que 50% du montant confisqué aux acteurs malveillants démasqués. Les autres 50% pourront éventuellement être brûlés afin de dissuader d'éventuelles attaques et d'éviter la collusion.

La **vérification (3)** de tout défi sera effectuée par les nœuds de la métachaîne. Le défi est émis via une transaction qui transfère un montant d'eGold, il sera donc exécuté à l'intérieur d'un fragment et inclus dans un bloc. Les transactions de défi sont également référencées dans l'en-tête du bloc, de sorte que la métachaîne puisse effectuer la vérification.

Le même défi peut provenir de plusieurs pêcheurs du système en même temps, il y aura donc un moyen d'identifier le même défi provenant de plusieurs rapporteurs. Cela pourrait être fait en fonction du champ de données de défi qui est propre à chaque défi.

Il ne devrait pas y avoir deux types de défis qui peuvent être vérifiés sur le même bloc, s'il y en avait, alors le plus dommageable devrait être retenu pour ouvrir droit à récompense.

La notarisation d'une telle contestation produira un **effet (4)** de couperet(slashing) pour un ou plusieurs validateurs si la contestation est effectivement validée, selon le type d'action contradictoire qui a été signalée: dans certains cas, tous les signataires d'un bloc invalide sont sanctionnés; dans d'autres cas, seul le producteur de blocs ou un sous-ensemble de validateurs d'un groupe de consensus. Si le défi n'est pas validé par les nœuds de la Metachaîne, alors le challenger perd la valeur transférée via la transaction de défi et le gaz associé pour valider le défi.

Une fois qu'un fragment traite un bloc de la Metachaîne qui a notarié une transaction de défi validée, le challenger devrait recevoir en retour la valeur transférée ainsi qu'un pourcentage (montant à décider) de la ou des mises confisquées, tandis qu'une autre partie pourrait être donnée en récompense aux nœuds de métachaine. Pour les défis marqués comme invalides par la métachaîne, le fragment n'aurait pas besoin de faire autre chose, car le coût du défi aurait déjà été transféré.

Nous définissons comme étant des mauvais comportements ou des comportements malveillants les actions qui peuvent être prouvées par cryptographie:

- Double signature d'un bloc à la même hauteur
- Signature d'un bloc à la suite d'une transition d'état invalide.

Il reste deux approches supplémentaires pour la phase de mise en œuvre et pour les recherches futures:

- Nous pourrions envisager d'augmenter progressivement le montant confisqué, à mesure que le temps passe et que le réseau devient plus mature.
- Nous pourrions envisager d'augmenter le montant confisqué(slashed) en fonction du nombre d'autres validateurs sanctionnés en même temps, afin de décourager davantage les actions coordonnées de plusieurs acteurs malveillants.

2.4 Récompenses de mise en gage

Les récompenses de mise en gage, la possibilité d'être sanctionné (slashing), ou d'augmenter/diminuer la note d'un nœud, sont un ensemble d'incitations qui encouragent les détenteurs de jetons et les validateurs à sécuriser le réseau Elrond. En échange de la sécurité, les validateurs peuvent augmenter leur part relative de détention de jetons dans le réseau.

Nous pensons que la finalité des récompenses de mise en gage n'est pas de fournir un flux de revenus en soi aux détenteurs de jetons. En fait, la justification économique de la mise en gage n'est pas tant de recevoir une récompense ("rendement"), mais plutôt d'affirmer clairement aux validateurs que la mise en gage augmente leur intérêt relatif (par le montant d'eGold détenu) dans le réseau, et contribue également à une appréciation significative des jetons.

Dans cette optique, il est préférable de considérer le taux d'inflation comme un taux de dilution des détenteurs de jetons. En tant que tel, la mise en gage est le meilleur moyen d'accroître à la fois vos avoirs en jetons et votre intérêt pour le réseau Elrond.

Voici comment les récompenses seront versées chez Elrond :

Il y aura un montant minimum garanti de récompense par an. Le montant minimum garanti de la récompense proviendra des frais, tandis que le reste proviendra de l'inflation. Le taux d'inflation maximum par an, si les frais sont nuls, est donc de :

Modèle d'émission eGold d'Elrond

Années	JETONS TOTAL MAX EMISSION ANNUELLE	TAUX MAX EMISSION %	EMISSION ANNUELLE MAX A AJOUTER	Transaction par sec. (TPS) Pour zero emission	Stock à écouler
	20,000,000.00				
Année 1	22,169,025.00	10.845130%	2,169,025.00	**1375.586631**	1375.586631
Année 2	24,109,733.00	9.703538%	1,940,707.00	**1230.788305**	1230.788305
Année 3	25,822,122.00	8.561945%	1,712,388.00	**1085.989346**	1085.989346
Année 4	27,306,192.00	7.420352%	1,484,070.00	**941.1910198**	941.1910198
Année 5	28,561,944.00	6.278760%	1,255,751.00	**796.3920599**	796.3920599
Année 6	29,589,377.00	5.137167%	1,027,433.00	**651.5937341**	651.5937341
Année 7	30,388,492.00	3.995574%	799,114.00	**506.7947742**	506.7947742
Année 8	30,959,288.00	2.853982%	570,796.00	**361.9964485**	361.9964485
Année 9	31,301,766.00	1.712389%	342,477.00	**217.1974886**	217.1974886
Année 10	31,415,926.00	0.570796%	114,159.00	**72.39916286**	72.39916286

Si la somme cumulée des frais pendant une année est supérieure aux récompenses minimales garanties, le taux d'inflation devient nul et les récompenses distribuées seront supérieures aux récompenses minimales garanties. Dans le cas contraire, le total des frais ne fera que réduire l'inflation du montant correspondant. En adoptant cette approche, nous avons créé les prémisses de la transition vers un système monétaire déflationniste.

Comme les récompenses sont fixées au départ, le montant distribué à chaque validateur sera proportionnel à son nombre total de nœuds et à leur note. Alors que la notation est davantage sous le contrôle du validateur, le nombre de nœuds est sous le contrôle de la gouvernance du protocole. Au moment de la genèse, le réseau Elrond sera amorcé avec 2169 nœuds qui formeront une métachaîne et 3 fragments (ceci inclut les listes d'attente des fragments, contenant 142 nœuds chacun). Cette configuration sera suffisante pour atteindre environ 15 000 TPS et les niveaux de sécurité et de décentralisation souhaités.

Nous reconnaissons qu'à terme, le nombre de fragments et de nœuds pourrait devoir être augmenté, afin d'équilibrer la charge sur les fragments et de créer davantage d'infrastructures pour soutenir un débit plus élevé.

Nous pensons que lorsque les besoins ci-dessus se feront ressentir, les récompenses supplémentaires nécessaires pour un nouveau fragment avec 400 nœuds éligibles + nœuds en attente, seront partiellement "financées" par une augmentation des frais (déjà en cours et encore accélérée par le nouveau fragment), de manière à éliminer la nécessité d'une augmentation de l'inflation. Nous avons donc plafonné le taux d'inflation, afin d'éviter que l'augmentation ne dépasse le taux maximum défini pour l'année. Idéalement, tout nouveau fragment devrait être activé lorsque le montant des frais dépasse les récompenses minimales garanties dans un rapport de $1/N_{sh}$, où N_{sh} est le nombre total de fragments existants.

Au prix de 0,00005 eGold par transaction, il semble que pour un TPS compris entre 5000 et 7000, des frais suffisants soient générés pour justifier un fragment supplémentaire sans effet sur l'inflation. Pour chaque exigence de 2000 TPS supplémentaires, un fragment supplémentaire peut être ajouté sans effet sur

l'inflation, tout en maintenant la charge sur les fragments en dessous de 50%. Bien que d'autres tests en conditions réelles et davantage de données soient nécessaires, c'est ainsi que les choses ont été modélisées au moment de la rédaction du présent document.

Voici le calculateur pour les validateurs que nous avons utilisé pour le lancement du réseau Elrond (Genesis) :
https://docs.google.com/spreadsheets/d/1moHSRVAPeFyVnnx6psHmsUbTUrIBibXyopJAZ5o4zWs/edit#gid=1905747724

2.5 Calcul et distribution des récompenses

Les récompenses sont distribuées à la fin de chaque époque selon les règles suivantes : 10% des frais d'un bloc sont reçus par le proposant du bloc, tandis que les 90% restants sont versés dans une réserve de frais, *TotalFeesToBeDistributed*. Pour plus d'informations sur les frais, veuillez vous reporter à la section 3 correspondante..

À la fin de l'époque, un calcul sera effectué pour déterminer combien de nouveaux jetons doivent être frappés. Ce nombre est établi en calculant la récompense totale à distribuer (*TotalRewardsToBeDistributed*) en fonction de l'inflation maximale possible (*maxPossibleInflation)*, et le nombre de blocs produits par chaque fragment, moins le total des frais cumulés (*TotalAccumulatedFees*) par tous les fragments pendant cette période. Sur le montant total des récompenses à distribuer (*TotalRewardsToBeDistributed)*, 10 % seront transférés à l'adresse du fonds de pérennisation du protocole. Voir la section 4 pour plus de détails sur ce fonds.

Lorsque le nombre de fragments est modifié, les récompenses par bloc sont calculées en fonction du nouveau nombre de fragments. Si le temps du tour est modifié, les récompenses par bloc sont calculées en fonction du nouveau tour. Le calcul du *RewardPerBlock* est effectué à la fin de l'époque et ajouté au bloc du début de l'époque par les proposants du bloc, vérifié par tous les validateurs.

A la fin de chaque époque :

a. *MinTotalRewardsToBeDistributed* est égal au nombre total de blocs produits par tous les fragments + métachaîne multiplié par *RewardsPerBlock.*
b. Pour chaque bloc produit à chaque tour dans chaque fragment, 10 % de la somme des frais de transaction de ce bloc vont directement au proposant de ce bloc, mais seulement après que 10 % aient été réservés pour assurer la pérennité du protocole.
c. Les 90 % restants des frais de transaction de tous les fragments sont regroupés et ajoutés à un fonds commun, appelé *TotalFeesToBeDistributed*, libellé en nombre de jetons eGold.
d. *TotalAccumulatedFees* est égal à *TotalFeesToBeDistributed* + tous les frais allant directement au proposants de blocs.
    i. si *TotalAccumulatedFees* < *MinTotalRewardsToBeDistributed* alors *MinTotalRewardsToBeDistributed* - *TotalAccumulatedFees* tokens sont créées et ajoutés à la réserve de compensation du validateur pour un total de *TotalRewardsToBeDistributed = MinTotalRewardsToBeDistributed*
    ii. si *TotalAccumulatedFees* > *MinTotalRewardsToBeDistributed* alors aucun token additionnel n'est créé et *TotalRewardsToBeDistributed = MinTotalRewardsToBeDistributed + (TotalAccumulatedFees - MinTotalRewardsToBeDistributed).*

iii. Un montant de 10% de la valeur des récompenses totales à distribuer est transféré à l'adresse du fonds assurant la pérennité du protocole.

iv. Les 90% restants du *TotalRewardsToBeDistributed* sont répartis entre tous les validateurs (sur l'ensemble des fragments, y compris les validateurs de la métachaîne) qui ont agi en tant que membres du groupe de consensus.

e. À partir du *TotalRewardsToBeDistributed*, nous calculons le *RewardsPerBlock* et le *RewardsPerBlockPerNode* en fonction du nombre de validateurs éligibles à cette époque et du nombre total de blocs produits à cette époque.

f. Le nouveau proposant de bloc de la métachaîne du nouveau bloc de début d'époque distribue les récompenses (frais de transaction et jetons émis, le cas échéant) dans le métabloc de début d'époque.

g. Le processus de distribution est déterministe, tous les validateurs de la métachaîne créent les mêmes récompenses et doivent arriver à la même conclusion :

i. Itérer les statistiques du validateur et exporter les données suivantes pour chaque clé publique du BLS : nombre d'occurrences de sélection dans les blocs achevés, nombre d'occurrences en tant que leader, total des droits accumulés et adresse de la récompense.

ii. Lors de l'itération de toutes les clés publiques du BLS, le processus ajoute le *RewardsPerBlockPerNode* * *NumSelectedInSuccesfullBlocks* + *TotalAccumulatedFees* à l'adresse de récompense pour cette clé BLS publique

iii. Pour chaque adresse de récompense, une transaction de récompense est créée à partir de la métachaîne vers les fragments.

iv. Les fragments ajouteront la valeur des transactions de récompenses au solde des comptes.

2.6 Désengagement(Unstaking) et détachement(Unbonding)

Désengagement

Si un validateur souhaite effectuer un retrait de son gage, il lance une transaction qui indique qu'il veut désengager un certain nombre de nœuds, avec la clé publique BLS de chaque nœud pour paramètre. La transaction est générée par le validateur et envoyée vers la métachaîne.

À la fin de l'époque, lorsque les nœuds sont redistribués aléatoirement, ceux qui se sont désengagés pendant l'époque qui vient de s'achever seront redistribués en premier.

- Si le nœud ne peut pas être redistribué, alors il doit "rester et continuer à valider". Si le nœud décide de se mettre hors ligne, sa notation diminue et à un moment donné, il sera en dessous du *ratingThreashold*, ce qui le rendra inéligible pour participer au processus de sélection ou d'enchères suivant. Un nœud en-dessous du *ratingThreashold* ne peut pas être désengagé tant que sa notation n'est pas supérieure au *ratingThreshold* (voir transaction *resetRating*. de réinitialisation de la notation).
- S'il y a plus de nœuds en cours de désengagement dans un fragment que le nombre de nœuds dans la liste d'attente, la métachaîne calcule un ordre de redistribution et seuls les premiers nœuds en attente de la liste sont retirés.

Si un validateur initialise un désengagement, puis décide à la même époque de se rétracter, il peut envoyer une nouvelle transaction et son désengagement sera annulé.

Les informations relatives au désengagement sont sauvegardées dans le contrat d'engagement du validateur. La transaction de ré-engagement est identique à la soumission initiale, la seule différence est qu'il n'y a pas besoin de renvoyer la *valeur*.

Détachement
Le délai de détachement effectif est fixé à 10 jours, après quoi le nœud pourra récupérer ses fonds précédemment engagés.

Pendant la période de détachement:

- Si le nœud mène des activités malveillantes, il est toujours sanctionnable(slashable). Il peut s'agir d'attaques telles que (voir la section 2.3 sur la sanction-couperet) :
    - Attaques à longue portée
    - Non-exécution des activités de validation requises

- Il est possible que la période de détachement d'un nœud ne se termine jamais si tous les nœuds du système sont partis et qu'il n'y a pas assez de nœuds pour faire fonctionner un seul fragment. Cependant, cela ne peut pas se produire en pratique, car Elrond fournira des nœuds pour au moins la métachaîne et un fragment au prix minimum du nœud de réserve. De cette manière, nous garantissons un mécanisme à sécurité intégrée où Elrond est l'opérateur de nœud de dernier recours.

À la fin de la période de détachement, le validateur envoie une transaction demandant à récupérer le collatéral mis en gage pour chacun des nœuds qu'il choisit de retirer.

La requête *unBond* est traitée par les nœuds de la métachaîne uniquement si la période avant séparation est terminée pour chaque nœud concerné par le désengagement. Si la période de détachement n'est pas terminée, tout le gaz est consommé.

2.7 Délégation

Comme tout le monde ne pourra pas être validateur et avoir son propre noeud. Ceux voulant quand même participer, peuvent déléguer leurs eGold aux validateurs et fournisseurs de services pour pouvoir partager les récompenses avec eux.

Lors de la phase de démarrage du réseau Elrond, la société Elrond exploitera un certain nombre de nœuds. Les membres de la communauté pourront déléguer leur participation à Elrond en tant que fournisseur de services au cours des premiers mois. En outre, Elrond a un certain nombre de partenaires qui fourniront des services professionnels pour gérer de grandes infrastructures ; ces partenaires ainsi que Elrond auront besoin d'un modèle de contrat intelligent de délégation pour commencer.

Les exigences générales pour un tel contrat seront de distribuer les récompenses générées par les validateurs, vers les membres de la communauté qui ont mis leurs jetons en gage par le biais du contrat. La distribution doit tenir compte du moment où les récompenses doivent être remises aux membres inscrits et du montant des frais de service.

De plus amples informations sur la délégation en général, la délégation à la genèse, et le modèle de contrat intelligent pour la délégation, fourni par Elrond à titre indicatif, seront annoncées ultérieurement dans une autre publication ou par un article posté sur medium.com.

3. Les frais

Un flux de valeur durable pour le réseau peut provenir des frais de transaction et de l'inflation des actifs. Étant donné que le succès du réseau se reflète dans l'adoption et l'utilisation qui généreront des frais de transaction, le modèle économique pourra financer la croissance et le maintien du réseau sans avoir besoin d'inflation.

Le calcul et la distribution des récompenses et des honoraires sont effectués à la fin de l'époque, ajoutés au début de l'époque suivante par les proposants de blocs, et vérifiés par tous les validateurs.

Pour tous les blocs produits à chaque tour, par chaque shard, 10% des frais de transaction du bloc vont directement au proposant du bloc. Les 90% restants de tous les frais de transaction d'un bloc sont ajoutés dans un pool et sont distribués à tous les validateurs à la fin de l'époque. Seul le proposant de bloc prend 10% des frais du bloc actuel.

Après avoir examiné les simulations initiales, nous avons décidé que les frais de transaction commenceront à 0,00005 eGold par transaction.

3.1 Transactions et frais des contrats intelligents

Les frais de transaction sont calculés comme suit :

1. Opérations de transfert de valeurs :

$$(moveBalanceGas + storePerByteGas * len(txData\ field)) * GasPrice$$
$$GasPrice >= minGasPrice$$

2. Transactions avec les contrats intelligents :

$$(moveBalanceGas + storePerByteGas * len(txData\ field)) * GasPrice + (actual\ smart\ contract\ processing\ gas) * GasPrice$$

Le proposant de bloc approprié les calculeras directement pendant le processus de consensus.

Les frais de transaction sont calculés à l'aide d'un modèle de gaz. Celui-ci prend en considération : la quantité de ressources utilisées par transaction, ce qui comprend:

i. CPU
ii. Bande passante
iii. Stockage

Cette liste fournit 584 opérations et leur quantité de gaz associée qui seront utilisées sur Genesis (sous réserve de modifications ultérieures). Les 584 opérations sont uniquement du gaz. L'unité de mesure provient de *gasPrice*. Il existe un prix minimum du gaz dans le système, en-deçà duquel les opérations ne

sont pas exécutées. Le *gasPrice* peut être fixé par l'utilisateur. Les frais réels de la transaction sont calculés en appliquant *gasPrice* * *gasLimit*. Le *gasPrice* contient l'unité actuelle qui est 10^{-18} eGold. Les frais sont calculés en fonction du prix du gaz consommé (*consumedGas* * *gasPrice*).

Pour tout bloc donné dans chaque fragment, les frais de transaction inclus dans le bloc sont agrégés (voir la section 2.4 Récompense de mise en gage). Jusqu'à la fin de l'époque (à ce moment là les frais de transaction regroupés sont distribués aux agents appropriés), les frais de transaction ne sont contrôlés par aucun agent et sont stockés sous forme d'informations dans l'en-tête metaBlock, inaccessibles aux nœuds de chaque fragment.

Chaque transaction doit spécifier la quantité de gaz dont elle a besoin dans le cadre des données de transaction. Pendant qu'un producteur de blocs crée un bloc, il exécutera chaque transaction en déduisant le gaz consommé et en remboursant le gaz restant. Si une transaction spécifie suffisamment de gaz pour l'exécution mais des fonds insuffisants pour le transfert réel, alors l'exécution consommera le gaz donné mais la fonction de déplacement de solde (ou appel de contrat intelligent) ne provoquera aucun changement de solde en raison d'un solde insuffisant (le nonce du compte sera augmenté et la transaction sera ajoutée à la chaîne de bloc comme une transaction non valide)

Pour toute transaction, ce montant peut être calculé par une surestimation (mais pas plus de 10x) de la consommation prévue de gaz, grâce au retour du montant inutilisé au payeur, une fois toutes les transactions terminées. Si une transaction ne relie pas suffisamment de gaz pour exécuter une fonction requise, la transaction se terminera prématurément et échouera, mais facturera toujours le gaz utilisé.

Pour toute transaction qui spécifie moins de *gasLimit* comme indiqué dans la section 3.1, formule 1, le système rejettera cette transaction et ne notarisera donc pas la transaction (pas même comme une transaction ayant échoué).

Les travaux à venir exploreront la possibilité d'ajuster les frais en fonction de la charge sur l'ensemble du réseau, de sorte que, par exemple, tant que la charge est inférieure à 50%, nous ayons un prix du gaz minimal, mais lorsque la charge dépasse 50%, le prix du gaz augmente. Afin d'éviter la manipulation du prix du gaz par la tenue de transactions, un délai d'expiration sera fixé à chaque transaction. Par la suite, à la fin de chaque époque, une réorganisation des fragments pourrait être déclenchée, de sorte que les contrats intelligents et les dApps soient déplacés vers d'autres fragments afin de rééquilibrer la charge par fragment et de la ramener à moins de 50%.

3.2 Frais de stockage

Le stockage doit être considéré séparément du calcul ou de la bande passante, car chaque transaction de contrat intelligent qui nécessitera un stockage sur tous les validateurs à l'avenir, n'est pas seulement soumise à des frais uniques lors de l'exécution de la transaction, mais également à un coût de stockage.

Elrond introduira un loyer public pour les transactions de contrats intelligents, où il y aura un prix fixe pour chaque octet à stocker (à l'avenir, ce prix fixe pourra être ajusté via la gouvernance), un prix qui sera payé périodiquement. Le prix public du loyer est appliqué uniquement aux contrats intelligents et non aux comptes de solde normal. Nous allons également introduire un mécanisme pour effacer temporairement l'état d'un compte (qui n'est pas en mesure de payer le loyer), pour mettre le compte en veille prolongée et le restaurer lorsque nécessaire.

3.3 Frais de développement et monétisation

Afin d'accélérer considérablement l'adoption par les développeurs, nous fournirons aux développeurs une solution intégrée de monétisation du protocole. Ainsi, 30% des frais directement associés à une dApp, iront au développeur. Ainsi, lors du traitement d'une transaction de contrat intelligent, 30% des frais de cette transaction seront ajoutés au solde du contrat intelligent.

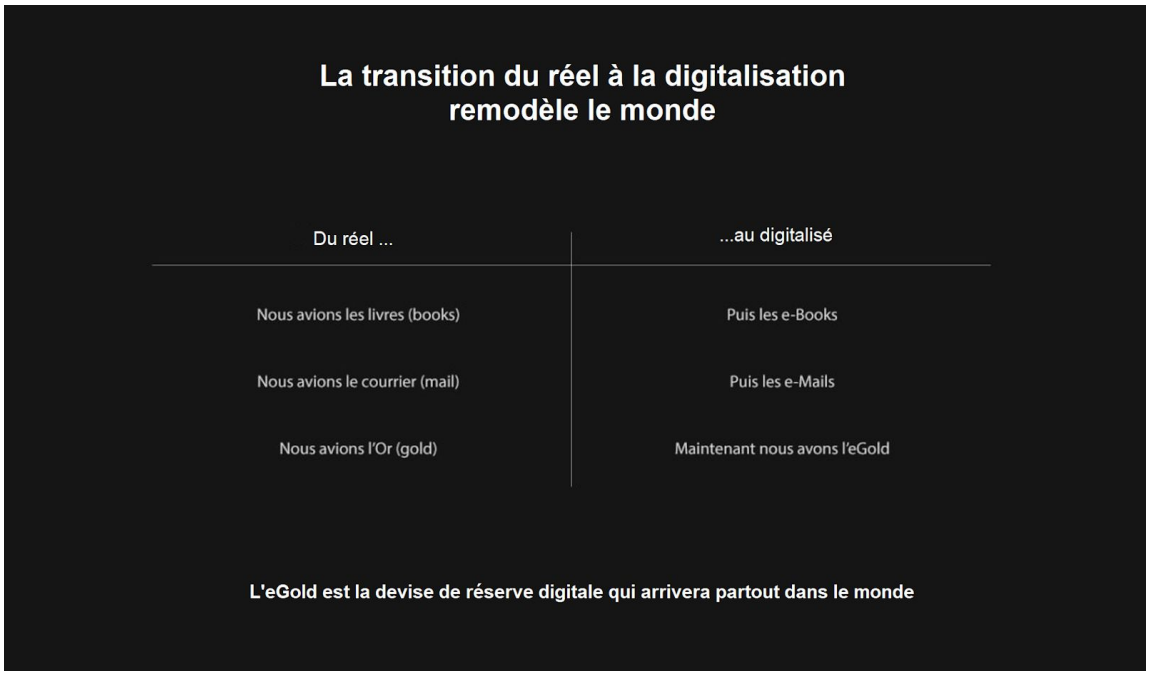
4. eGold

Le jeton Elrond eGold natif ouvre une nouvelle phase de croissance pour l'économie d'Elrond. C'est une étape naturelle vers l'activation des services Elrond natifs tels que le jalonnement et la délégation, et les options DeFi natives.

4.1 Aperçu global

Ci-après une vue globale des caractéristiques les plus importantes de l'eGold

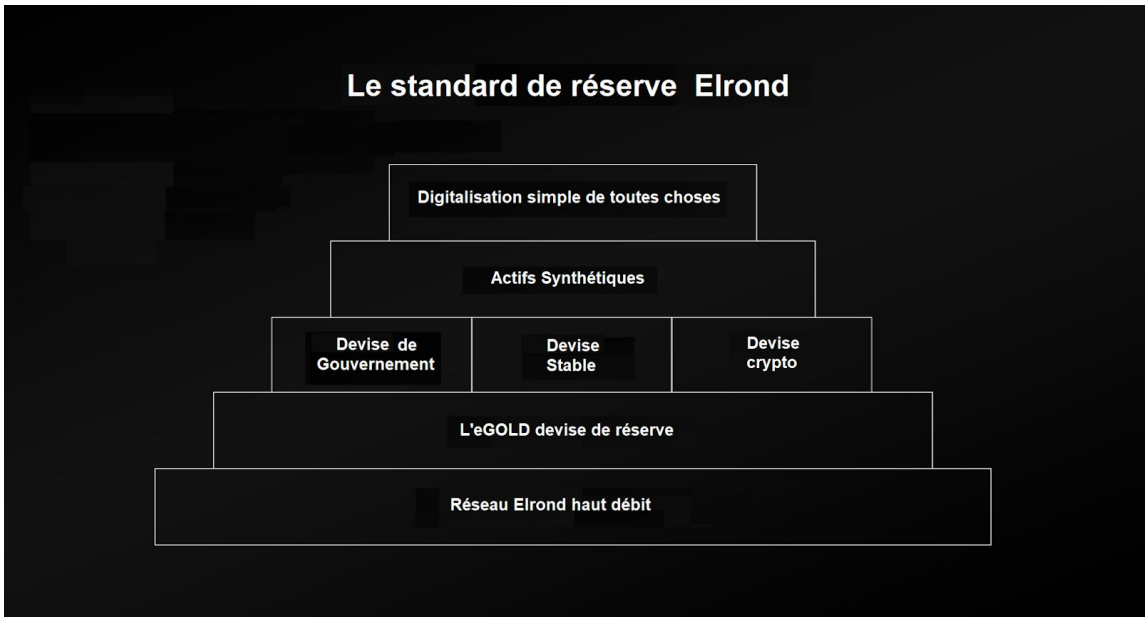
a) **La monnaie eGold est conçue pour la simplicité et l'adoption mondiale**
La complexité est l'obstacle le plus important à l'adoption dans le monde réel - essayez d'expliquer Bitcoin ou Ethereum à des gens normaux et vous voyez immédiatement ce que nous voulons dire. Afin d'atteindre le prochain milliard de personnes, nous avons complètement repensé la monnaie Elrond, en capturant son essence dans une métaphore universellement attrayante et puissante.



b) **La monnaie eGold est conçue comme une norme de réserve numérique et une solide réserve de valeur**
Un nouveau modèle économique a été défini pour positionner eGold comme le jeton central du réseau, fondamental pour tous les usages internes d'Elrond. Ce jeton est conçu pour optimiser les paramètres qui se prêtent à la création d'une solide réserve de valeur, similaire à l'or, mais avec des mécanismes et des fonctionnalités qui vont bien au-delà de ceux de l'or.

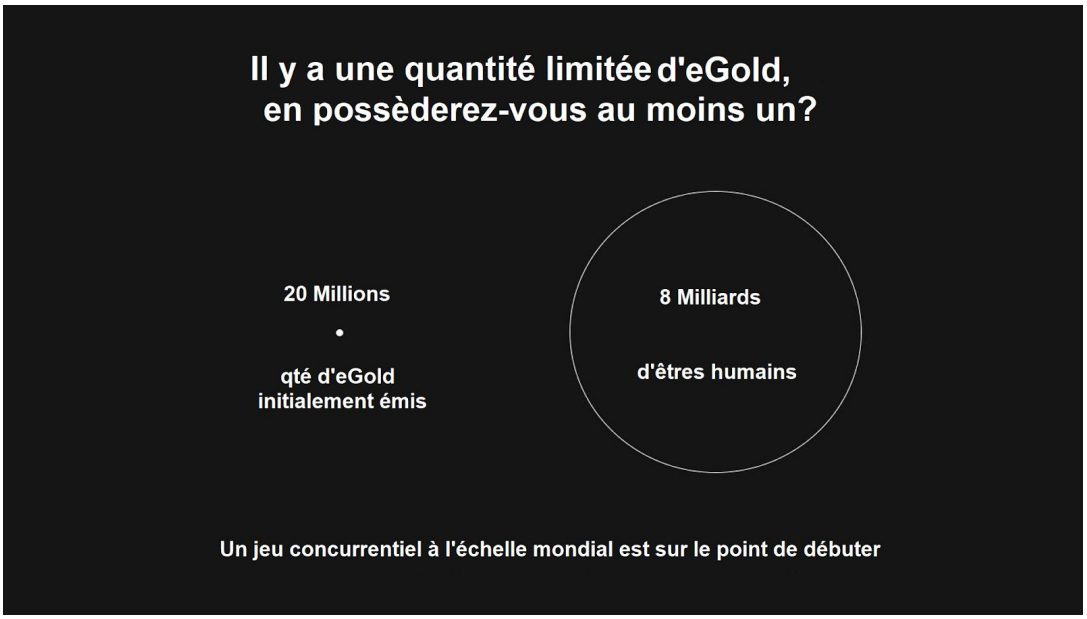
En activant un nouvel ensemble de tickers avec un “e” pour préfixe, comme eGLD, nous rendons les choses simples et intuitives à comprendre, mais peut-être mieux encore, permettons un chemin de dérivation flexible et cohérent basé sur le préfixe E, compatible avec l’ajout d'un ensemble illimité de nouvelles devises en plus de la réserve eGold.

Cette conception repose sur l'hypothèse que Elrond est compatible à la fois avec les monnaies des gouvernements locaux et d'autres crypto-monnaies, qui pourront à terme tirer parti du réseau à large bande passante d'Elrond pour offrir un transfert de valeur mondiale à leurs communautés locales. En fait, nous avons l'intention d'intégrer de nombreux nouveaux jetons, tels que des pièces stables, des actifs synthétiques et des monnaies fiduciaires locales.



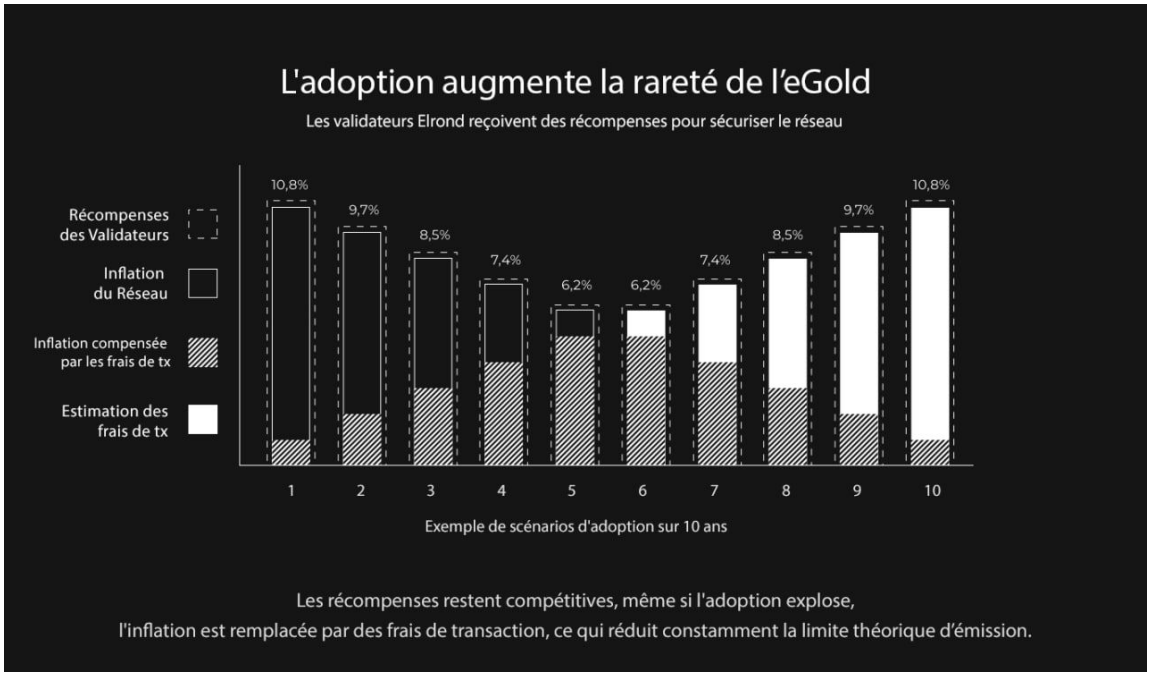
c) La rareté intégrée pour renforcer la valeur et la demande

Il n'y a que 20 millions d'eGold au moment de la Genèse en regard de 8 milliards d’être humains. Cela signifie qu'il y a une offre très limitée de seulement 0,0025 eGold par personne. Cela déclenche une course à l’accumulation, car posséder quelques milliers d'eGold aujourd’hui pourrait être comme posséder quelques milliers de Bitcoin en 2010.



d) Une forte incitation à l'engagement(staking) pour un validateur associée à une limite d'offre maximale

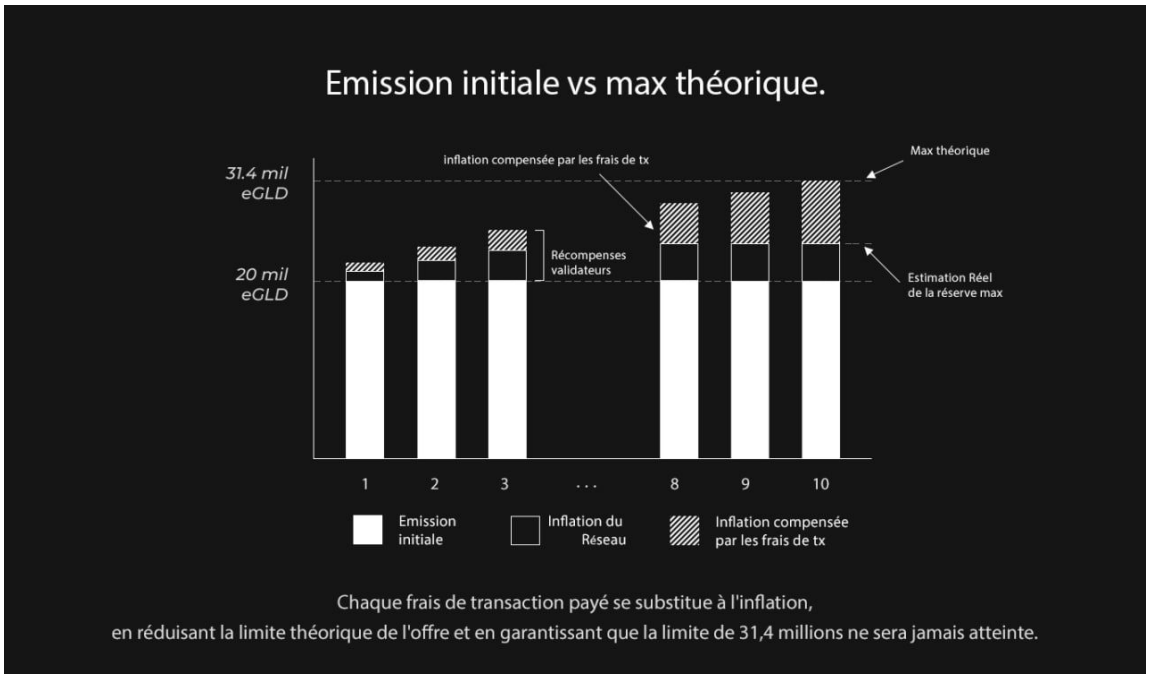
Les validateurs sont fortement incités à sécuriser le réseau Elrond. Au début, ces incitations au jalonnement proviennent d'une nouvelle offre émise chaque année, mais à mesure que l'adoption commence, l'inflation (NDT:l'émission de nouveau jeton) est remplacée par des frais de transaction pour couvrir les récompenses de mise en gage. De plus, contrairement à la plupart des autres réseaux blockchaîne où la nouvelle émission est infinie et non plafonnée, dans l'éco-système Elrond cette somme est plafonnée à une limite d'approvisionnement théorique de 31 415 926 eGold qui peut être atteinte sur 10 ans.



e) L'adoption réduit cette inflation théorique et augmente la rareté

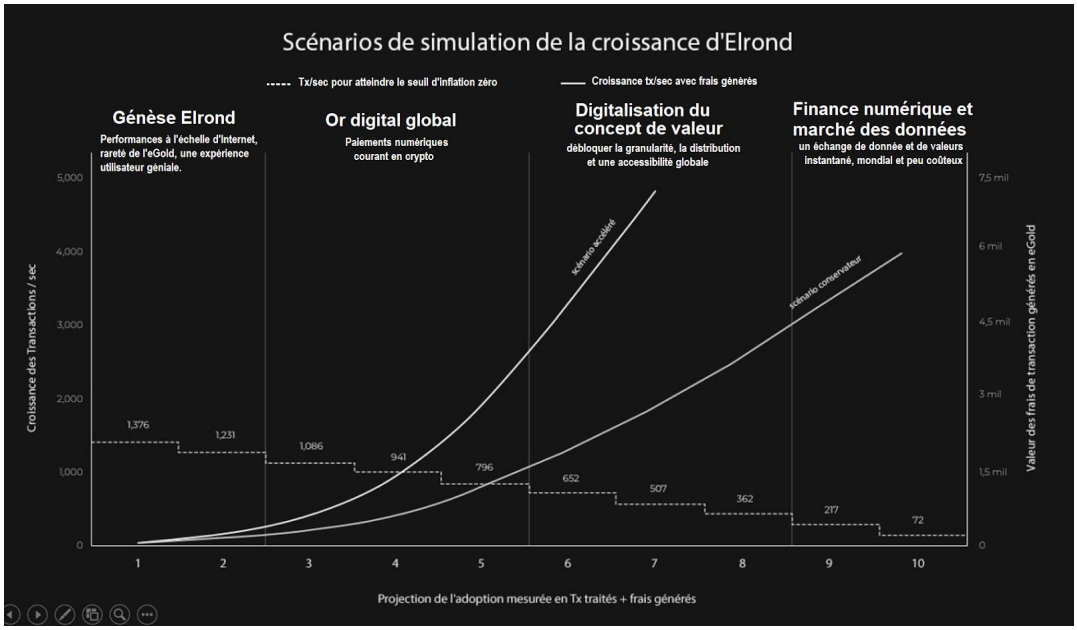
L'une des caractéristiques les plus puissantes du modèle économique d'Elrond est que chaque frais de transaction payé réduit la limite théorique en remplaçant l'inflation (NDT:l'émission) par des frais,

rendant ainsi eGold plus rare, garantissant que la limite d'offre maximale de 31,4 millions ne sera jamais atteinte.



f) Un modèle d'adoption durable qui développe l'ensemble de l'économie eGold et renforce la déflation

Elrond offre sans doute l'un des modèles d'adoption les plus solides de l'espace blockchain, grâce à la capacité du réseau de passer immédiatement à un modèle entièrement déflationniste via n'importe quel scénario d'adoption. En effet, le seuil d'inflation zéro visible dans l'image ci-dessous montre que, puisque moins de 10% de la capacité du réseau est nécessaire pour franchir le seuil, avec une adoption suffisante, Elrond peut dépasser ce seuil et créer une valeur significative pour tous les participants du réseau.



4.2 Propriétés des devises et de l'eGold

Il existe deux types de devises qui ont été utilisées récemment dans le monde: les devises représentatives, où chaque pièce ou billet peut être directement échangé contre un montant spécifié d'une marchandise; et les monnaies fiduciaires, émises par un gouvernement, non adossées à une marchandise, mais opérant plutôt selon une foi partagée entre les individus et les gouvernements, ces monnaies continuent à être acceptées et utilisées comme moyen d'échange ou de paiement.

Toute devise dans le monde est considérée comme une réserve de valeur, si elle peut maintenir de manière fiable sa valeur relative au fil du temps sans se déprécier. En plus d'être une bonne réserve de valeur, toute monnaie robuste doit également satisfaire à certaines caractéristiques liées à l'utilité, à la rareté, à la divisibilité, à la transportabilité, à la durabilité et à la contrefaçon.

L'eGold est un nouveau type de monnaie numérique avec des propriétés uniques qui se prêtent à la création d'une solide réserve numérique de valeur.

Propriétés	OR Physique (Ressource)	Fiat (Dollars US)	eGold (Elrond)
Fongibilité (Interchangeable)	élevé	élevé	Très élevé
Transportabilité	Moyen	élevé	Très élevé
Durabilité	élevé	Moyen	Très élevé
Divisibilité	Faible	Moyen	Très élevé
Sureté (empêcher la contrefaçon)	Moyen	Moyen	élevé
Rareté (Qté prédictible)	Moyen	Faible	Très élevé
Non-Souveraineté (Indépendant des états)	élevé	Faible	Très élevé
Résistance à la censure	Moyen	Faible	Très élevé
Programmabilité (Intelligent)	Faible	Faible	Très élevé

a) Utilité

Une monnaie doit avoir une utilité pour être efficace. Les individus doivent pouvoir échanger de manière fiable des unités de la monnaie contre des biens et des services. C'est l'une des principales raisons pour lesquelles les devises se sont développées en premier lieu: afin que les participants à un marché puissent éviter d'avoir à troquer directement des marchandises. L'utilité nécessite également que les devises soient facilement déplacées d'un endroit à un autre. Les métaux précieux et les produits de base onéreux ne satisfont pas facilement à cette exigence.

Peut-être que le plus grand avantage de la monnaie eGold est qu'il s'agit du jeton natif alimentant l'une des architectures de blockchaîne les plus avancées, traitant à son lancement plus de 15000 transactions par seconde, avec une capacité de mise à l'échelle pouvant dépasser des centaines de milliers de transactions par seconde. Ainsi, étant numérique, eGold est un moyen supérieur d'échange et de transfert de valeur, se prêtant à des transferts d'argent rapides, mondiaux et rentables.

b) Rareté

La clé du maintien de la valeur d'une monnaie est son approvisionnement. Une masse monétaire trop importante pourrait entraîner une flambée des prix des biens, entraînant un effondrement économique.

Dans l'écosystème Elrond, l'offre commence à 20 000 000 et affiche une augmentation temporaire prévisible de l'offre pour inciter à la sécurité du réseau via des récompenses de mise en gage (staking). L'offre maximale définie ne peut excéder 31 415 926 sur une période de 10 ans. Cependant, ce plafond théorique diminuera en fait avec chaque transaction traitée et les frais générés. Ainsi, plus l'adoption est forte, plus l'offre d'eGold sera réduite.

c) **Divisibilité**

Les devises réussies sont divisibles en unités incrémentielles plus petites. Pour qu'un système de monnaie unique fonctionne comme moyen d'échange pour tous les types de biens et de valeurs au sein d'une économie, il doit avoir la flexibilité associée à cette divisibilité. La monnaie doit être suffisamment divisible pour refléter avec précision la valeur de chaque bien ou service disponible dans l'ensemble de l'économie.

L'eGold a un degré de divisibilité beaucoup plus élevé que la plupart des monnaies fiduciaires du monde entier. Un eGold est divisible jusqu'à 18 décimales. Si le prix de l'eGold continue d'augmenter au fil du temps, sa grande divisibilité garantit qu'avec de minuscules fractions d'un seul eGold, les gens pourront toujours l'utiliser dans les transactions quotidiennes.

d) Transportabilité

Dans une économie, les devises doivent être facilement transférées entre les participants pour être utiles. En termes de monnaie fiduciaire, cela signifie que les unités de monnaie doivent être transférables au sein de l'économie d'un pays particulier ainsi qu'entre les nations via l'échange.

Contrairement aux monnaies fiduciaires, où le processus de transfert d'argent peut prendre des jours et entraîner des frais importants, tant qu'il y a Internet, eGold peut être transféré n'importe où dans le monde, en un instant, et à un coût 100 fois inférieur aux options actuellement disponibles. Grâce à sa cotation sur les plus grandes bourses, eGold peut être facilement échangé contre presque toutes les devises.

e) Durabilité

La durabilité est un enjeu majeur pour les monnaies fiduciaires sous leur forme physique. Un billet d'un dollar, bien que solide, peut encore être déchiré, brûlé ou rendu inutilisable.

Tout comme une monnaie doit être durable, elle doit également être difficile à contrefaire pour rester efficace. Sinon, des parties malveillantes pourraient facilement perturber le système monétaire en l'inondant de faux billets, ce qui aurait un impact négatif sur la valeur de la monnaie.

Les moyens de paiement numériques ne sont pas exposés à ces dommages physiques de la même manière. Pour cette raison, eGold a une valeur considérable. Il ne peut pas être détruit de la même manière qu'un billet d'un dollar peut l'être, même s'il peut être perdu. Si un utilisateur perd sa clé cryptographique, l'eGold dans le portefeuille correspondant peut être effectivement inutilisable de manière permanente. Cependant, l'eGold lui-même ne sera pas détruit et continuera d'exister dans les enregistrements de la blockchain.

f) Contrefaçon

Grâce à la sécurité intégrée robuste de son système de blockchaîne décentralisé, eGold est incroyablement difficile à contrefaire. Cela exigerait essentiellement de corrompre une partie non négligeable des participants au réseau et exigerait un coût de plus en plus élevé et dissuasif. La seule façon de créer un eGold contrefait serait d'exécuter ce que l'on appelle une attaque à double dépense.

Cela se réfère à une situation dans laquelle un utilisateur «dépense» ou transfère le même eGold dans deux ou plusieurs endroits différents, créant effectivement un enregistrement en double. Bien que ce ne soit pas un problème avec un billet en monnaie fiduciaire - il est impossible de dépenser le même billet d'un dollar en deux ou plusieurs transactions distinctes - c'est théoriquement possible avec les monnaies numériques. Ce qui rend improbable une double dépense sur la blockchaîne Elrond, c'est le coût croissant et prohibitif des ressources nécessaires pour l'exécuter.

Vous trouverez ci-dessous un aperçu du modèle d'émission de l'eGold:

Elrond eGold supply model

YEARS	MAX TOTAL SUPPLY	MAX ISSUANCE RATE %	MAX YEARLY SUPPLY TO BE ADDED	TX/S TO ZERO ISSUANCE	STOCK TO FLOW
	20,000,000.00				
Year 1	22,169,025.00	10.845130%	2,169,025.00	1375.586631	1375.586631
Year 2	24,109,733.00	9.703538%	1,940,707.00	1230.788305	1230.788305
Year 3	25,822,122.00	8.561945%	1,712,388.00	1085.989346	1085.989346
Year 4	27,306,192.00	7.420352%	1,484,070.00	941.1910198	941.1910198
Year 5	28,561,944.00	6.278760%	1,255,751.00	796.3920599	796.3920599
Year 6	29,589,377.00	5.137167%	1,027,433.00	651.5937341	651.5937341
Year 7	30,388,492.00	3.995574%	799,114.00	506.7947742	506.7947742
Year 8	30,959,288.00	2.853982%	570,796.00	361.9964485	361.9964485
Year 9	31,301,766.00	1.712389%	342,477.00	217.1974886	217.1974886
Year 10	31,415,926.00	0.570796%	114,159.00	72.39916286	72.39916286

5. Pérennité du protocole

L'adresse du fonds de pérennisation du protocole recevra 10% du total des récompenses générées, afin de fournir les ressources et les fonds nécessaires pour développer, maintenir et promouvoir le protocole Elrond.

Travaux à venir

Une voie prometteuse pour les travaux à venir examinera l'utilisation d'un jeton algorithmique stable pour les frais et l'utilisation de l'enjeu comme garantie pour l'émission du jeton stable.

En activant un nouvel ensemble de tickers avec un “e” pour préfixe, comme eGLD, nous rendons les choses simples et intuitives à comprendre, mais mieux encore, permettons un chemin de dérivation flexible et cohérent basé sur le préfixe E, compatible avec l’ajout d'un ensemble illimité de nouvelles devises sur le réseau Elrond.

Par ailleurs, eGold, en plus d'être bloqué dans la mise en gage et la délégation, pourrait servir à stabiliser la valeur des actifs stabilisés d'Elrond, devenant ainsi une composante de réserve. La réserve pourrait consister en un panier de crypto-monnaies qui aide le protocole à réduire l'offre de futurs actifs stables d'Elrond.

Cet article est la première ébauche publique du modèle économique d'Elrond. Les particuliers et les entreprises qui contribuent à cet article opèrent dans un environnement dynamique où de nouvelles idées et des facteurs de risque émergent continuellement. Ainsi, nous sommes constamment à la recherche de commentaires, avec de nouvelles hypothèses qui pourraient remettre en question et améliorer certaines parties de notre modèle. Nous encourageons ceux qui souhaitent contribuer, à faire part de leurs commentaires sur le Forum d'Elrond.

Constantes and formules

Nom	Valeur	Formule / commentaires
initialSupply	20,000,000	
maxPossibleInflation		<table><tr><th>Year</th><th>Inflation</th></tr><tr><td>1</td><td>10.845130%</td></tr><tr><td>2</td><td>9.703538%</td></tr><tr><td>3</td><td>8.561945%</td></tr><tr><td>4</td><td>7.420352%</td></tr><tr><td>5</td><td>6.278760%</td></tr><tr><td>6</td><td>5.137167%</td></tr><tr><td>7</td><td>3.995574%</td></tr><tr><td>8</td><td>2.853982%</td></tr><tr><td>9</td><td>1.712389%</td></tr><tr><td>10</td><td>0.570796%</td></tr><tr><td>11</td><td>0.000000%</td></tr></table>
numNodes	2169	
eligibleNodesPerShard	400	
nodesPerShard	542.5	*Le Fragment 0 (Shard 0) sera assigné pour prendre un noeud supplémentaire*
waitingNodesPerShard	142.5	*nodesPerShard - eligibleNodesPerShard*
numNodesConsensus	63	
eligibleNodesMeta	400	
numNodesConsensusMeta	400	
targetShardLoad	50%	

epochLength	86,400 seconds	
blockTime	6 seconds	
numBlocksPerEpoch	14,400	*epochLength ÷ blockTime*
validatorPerEpoch	2232 times	*numBlocksPerEpoch × (numNodesConsensus ÷ eligibleNodesPerShard)*
blockProposerPerEpoch	36 times	*validatorPerEpoch × (1 ÷ numNodesConsensus)*
nodePrice	2500 eGold	*(1)*
validatorRatingIncrease	0,00367	*(4)*
$validatorRatingIncrease_{metachain}$	0,00075	*(7)*
proposerRatingIncrease	0,23148 pour les fragments et 0.303030 pour meta	*(5)*
blockProposerRatingNegativePct	TBC	*(6)*
importanceRatingRatio	1	*(3)*
startRating	50.00001	
maxRating	100	
ratingThreshold	10	
HoursToMaxRatingFromStartRating	72h pour les fragments et 55h pour la metachaine	
resetRating	50.00001	
resetRatingFee		*0.1% du nodePrice*

Annexes

- Livre blanc d'Elrond (Original en anglais), (Traduction française)
- Calendrier d'émission du jeton eGOLD
- Calculette de mise en gage
- Coût du gaz pour les opérations
- Notation des validateurs Elrond par les pairs.

Réferences

1. *Sapiens: A Brief History of Humankind - by Yuval Noah Harari*

2. *Value Capture & Quantification: Cryptocapital vs Cryptocommodities*
   https://www.placeholder.vc/blog/2019/4/26/value-capture-and-quantification-cryptocapital-vs-cryptocommodities

3. *Towards Post-Capitalism*
   https://medium.com/econaut/towards-post-capitalism-7679d2831408

4. *Theory of Games and Economic Behavior - by John von Neumann, Oskar Morgenstern*

5. *A Brief Introduction to the Basics of Game Theory - by Matthew O. Jackson*

6. *Mechanism Theory - by Matthew O. Jackson*

7. *Essentials of Game Theory - by Kevin Leyton-Brown*

8. *Game Theory - by Fudenberg, Drew and Tirole, Jean*

9. *Cryptonetworks as Emerging Economies (Done Right?)*
   https://a16z.com/2019/02/11/cryptonetworks-economies-governance-capital-access-risk-capital

10. *Crypto, the Future of Trust*
    https://a16z.com/2018/12/16/future-trust-crypto-summit-2018/

11. *Programmable money*
    https://medium.com/@ElectricCapital/programmable-money-79e16dc7bfca

12. *Voting, Security, and Governance in Blockchains*
    https://a16z.com/2019/02/09/voting-blockchains-governance-security-cryptoeconomics/

13. *A Crash Course in Mechanism Design for Crypto Economic Applications*
    https://medium.com/blockchannel/a-crash-course-in-mechanism-design-for-cryptoeconomic-applications-a9f06ab6a976

14. *Vitalik Buterin. Blockchain resource pricing*
    https://github.com/ethereum/research/blob/master/papers/pricing/ethpricing.pdf

15. *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*
    https://ethereum.github.io/yellowpaper/paper.pdf

16. *On Inflation, Transaction Fees and Cryptocurrency Monetary Policy*
    https://blog.ethereum.org/2016/07/27/inflation-transaction-fees-cryptocurrency-monetary-policy/

17. *The Truth About Staking Yields*
    https://blog.chorus.one/the-truth-about-staking-yields/

18. *Elrond: A Highly Scalable Public Blockchain via Adaptive State Sharding and Secure Proof of Stake - Technical whitepaper https://elrond.com/assets/files/elrond-whitepaper.pdf*

19. *Antifragile: Things That Gain from Disorder - by Nassim Nicholas Taleb*