Der Reichtum von Krypto-Netzwerken

Erster wirtschaftlicher Modellvorschlag für Elrond Network

Elrond Team - v0.3.2

lucian.todea@elrond.com

Zuletzt aktualisiert: 15. November 2020

Deutsche Übersetzung (deutsches Team) Oktober 2020

Credits: .@WolfgangRueckerl, @Alfadirson , @Runkosx3, @Nathanael, @Bodhi1976

Zuletzt aktualisiert : 15.11.2020

Haftungsausschluss

Nichts in dieser Abhandlung oder auf der Website elrond.com ist ein Angebot zum Verkauf oder eine Aufforderung zur Abgabe eines Kaufangebots für irgendwelche Tokens. Elrond veröffentlicht dieses Dokument ausschließlich, um Feedback und Kommentare von der Öffentlichkeit zu erhalten. Nichts in diesem Dokument darf als Garantie oder Versprechen für die Entwicklung des Geschäfts, der Dienstleistungen oder des Tokens von Elrond oder für den Nutzen oder Wert des Tokens behandelt oder verstanden werden.

In diesem Dokument und auf der Website elrond.com werden aktuelle Pläne skizziert, die sich nach eigenem Ermessen ändern können und deren Erfolg von vielen Faktoren abhängt, die außerhalb der Kontrolle von Elrond liegen, einschließlich marktbasierter Faktoren und Faktoren innerhalb der Daten- und Kryptowährungsbranche, unter anderem. Alle Aussagen über zukünftige Ereignisse basieren ausschließlich auf Elronds Analyse der in diesem Papier oder auf der Website elrond.com beschriebenen Themen. Diese Analyse kann sich als falsch erweisen.

Elrond eGold (eGLD) beinhaltet keine Verbindung zu physischem Gold oder Gold-Derivat-Instrumenten. eGLD ist keine "stabile Währung" und kann volatil sein und/oder an Wert verlieren. Hierin wird keine Empfehlung hinsichtlich der Ratsamkeit des Kaufs von eGLD gegeben; dennoch sollten Sie eGLD nicht kaufen, wenn Sie den Verlust des gesamten Kaufpreises nicht tragen können.

Vorwort

Warum steht der Kapitalismus jetzt unter Stress? Warum sehen die Zentralbanken so zerbrechlich aus? Ist es möglich, über den Kapitalismus hinauszugehen und einen besseren Ansatz zu finden? Kann der Kapitalismus sich selbst verknappen? [3] Können wir eine robustere oder sogar antifragile Alternative aufbauen, wo die "too big to fail"-Systeme nicht mehr vorhanden sind? [21]
Mit Elrond schlagen wir eine mutige Vision für eine postkapitalistische Welt vor, die ein neues Wirtschaftsmodell und eine neue, speziell für das Informationszeitalter entwickelte Sprache bietet.

Dieses Dokument skizziert, wie die native Währung der öffentlichen Elrond-Blockchain geschaffen und algorithmisch geprägt werden soll, um die Anreize im Einklang mit der langfristigen Gesundheit und Sicherheit des Netzwerks aufrechtzuerhalten. Dieses Dokument bietet eine vorläufige Momentaufnahme der ökonomischen Prinzipien, die das Elrond-Netzwerk zum Zeitpunkt der Abfassung dieses Dokuments regeln.

Der Elrond-Token, eGold (eGLD), wird eine erwartete Bootstrapping-Dauer von etwa drei bis fünf Jahren haben. Der Elrond-Token ist untrennbar mit dem Elrond-Netzwerk verbunden und somit diesem inhärent. Einige der vorgesehenen Anwendungsfälle von eGold umfassen Staking, Delegierung, Zahlungen, Gebühren für Aufbewahrungsmiete und für den Einsatz intelligenter Verträge sowie die Belohnung der Validierer, die zur Leistung, Stabilität und Sicherheit des Netzwerks beitragen.

In den ersten Jahren werden wir uns darauf konzentrieren, Elrond als globales öffentliches Versorgungsunternehmen innerhalb des Internet-Ökosystems zu etablieren, das eine hochskalierbare, effiziente und interoperable Blockchain-Architektur anbietet, mit einer wachsenden Wirtschaft, die auf den nativen eGold-Token aufbaut. Alle Aktivitäten innerhalb des Netzwerks, wie z.B. die Verarbeitung von Transaktionen, das Ausführen intelligenter Verträge, die Bereitstellung von Dienstleistungen wie das Staking oder das Betreiben eines Validator-Nodes, werden von unserem nativen Token gespeist werden. Sowohl Start-ups als auch Großunternehmen werden in der Lage sein, dezentralisierte Anwendungen auf dem Elrond-Netzwerk aufzubauen oder Elrond als Teil ihrer Infrastrukturlösung für Produkte und Dienstleistungen zu integrieren.

In dieser ersten Phase wird der Zugang zu einem wiederkehrenden Wertstrom, der vom Netzwerk generiert wird, durch den Besitz des eGold-Tokens als systemeigenes Asset des Elrond-Tokens bedingt.

Nach dieser ersten Periode erwarten wir, dass sich eGold natürlich vorübergehend auch als Währung oder Zahlungsmittel eignen wird, das dank seines flexiblen programmatischen Mechanismus die herkömmlichen Währungen ergänzt. Dies bedeutet, dass eGold wahrscheinlich ein effizientes Tauschmittel für verschiedene Waren und Dienstleistungen werden wird, da seine Besitzer in der Lage sein werden, eGold direkt, weltweit und kostengünstig über Transaktionen zu versenden und zu empfangen.

Sobald sich Elrond zu einem florierenden globalen Ökosystem und öffentlichen Elrond-Blockchain entwickelt hat, könnte man erwarten, dass das Token zu einem robusten Wertaufbewahrungsmittel wird, da sich die programmierbaren Anreize und die starken Netzwerkeffekte, die den Blockchain-Architekturen zugrunde liegen, verstärken. Seine Qualität als Wertaufbewahrungsmittel hängt von den zugrundeliegenden wirtschaftlichen Anreizen ab, die durch die Übernahme aus der realen Welt, den definierten bedingten Übergang zu einem deflationären Wirtschaftsmodell und das gewachsene Vertrauen in das Elrond-Netzwerk verstärkt werden.

Das Elrond-Netzwerk hingegen ist eine Proof-of-stake-basierte Blockchain-Plattform, bei der eine Reihe von Validatoren, die eGold gestaked haben, Blöcke produzieren, indem sie einen Konsens erzielen. Die Validatoren werden für ihre Arbeit belohnt und haben eGold gestapelt. Wenn ein Validierer jedoch beschließt, absichtlich von den Protokollanweisungen abzuweichen, verliert er einen Teil seines eingesetzten eGold durch Slashing. Der Bestand an Nodes, die als Validatoren gewählt werden, und ihre Zuordnung zu den Shards ändert sich ständig (in jeder Epoche, d.h. etwa einmal pro Tag, auf der Grundlage eines Auktionsprozesses, der nach dem Start des Mainnet aktiviert wird), und diese Anzahl ist je nach den aktuellen Bedürfnissen des Netzwerks in Bezug auf Sicherheit und Durchsatz begrenzt.

Eine beliebige Anzahl von eGold-Inhabern kann indirekt am Staking teilnehmen, indem sie ihr eGold an bestehende Validierer, in der Regel professionelle Validierer (Staking-as-a-Service-Provider), delegieren, die sich dafür entscheiden, Delegationen zu akzeptieren. Ein eGold-Inhaber gibt an, welchen Validierungskandidaten er vertraut, und setzt etwas eGold zur Unterstützung seiner Delegation ein. Wenn einer oder mehrere ihrer Kandidaten in einer Epoche als Validatoren gewählt werden, teilen sie mit ihnen alle wirtschaftlichen Belohnungen oder Sanktionen, proportional zu ihrem delegierten Anteil. Das Delegieren von eGold ist eine Möglichkeit, sein eGold zu investieren und zur Sicherheit des Systems beizutragen. Je größer der Gesamteinsatz an eGold ist, desto höher ist die Systemsicherheit, da ein Gegner immer mehr Einsatz benötigt, um Knotenpunkte als Validatoren zu wählen.

Wir streben daher an, dass jederzeit mehr als 50% der zirkulierenden Versorgung gestaked werden.

Wie Sie beitragen und Feedback geben können

Dieses Dokument ist der erste öffentliche Entwurf des Elrond-Wirtschaftsmodells. Die Personen und Unternehmen, die zu diesem Dokument beitragen, arbeiten in einem dynamischen Umfeld, in dem ständig neue Ideen und Risikofaktoren entstehen. Daher sind wir ständig auf der Suche nach Feedback mit neuen Annahmen, die Teile unseres Modells in Frage stellen und verbessern könnten. Wir ermutigen diejenigen, die einen Beitrag leisten möchten, ihr Feedback über das Github von Elrond abzugeben. Github.

Inhaltsverzeichnis

1. Kontext

Vor etwa 70.000 Jahren machte der frühneuzeitliche Mensch einen bedeutenden Evolutionssprung durch, der als kognitive Revolution bekannt ist. Diese Revolution ermöglichte es dem Homo Sapiens, einzigartig hochentwickelte Denk- und Kommunikationsfähigkeiten zu entwickeln, die ihn vielleicht überraschenderweise zum dominierenden und furchterregendsten Raubtier der Erde werden ließen. [1]

Die Entwicklung der Sprache war zweifellos einer der maßgeblichsten Faktoren für den Aufstieg des Homo Sapiens. Die Sprache trug zur Schaffung eines gemeinsamen Verständnisses zwischen den Mitgliedern einer Gruppe bei und erleichterte die Kommunikation und den Austausch von Informationen und Ideen. Folglich erwiesen sich Vertrauen, Zusammenarbeit und Koordination als immer nützlichere und notwendigere Werkzeuge, die erstmals primitive Gemeinschaften skalierten. So schufen die Stämme Dörfer, die sich später in Städte und einige dann in Nationalstaaten verwandelten. Heute sind die Nationalstaaten nach und nach durch das moderne, hyper-verbundene globale Dorf abgelöst worden.

Menschen sind soziale Tiere, und im Laufe der Geschichte haben wir immer in Gemeinschaften gelebt. Am Anfang waren Vertrauen und Transfers eher sozial, persönlich und direkt. Dann ging es über zu institutionellen, unpersönlichen und indirekten (man denke an Zwischenhändler) sowohl auf lokaler als auch auf globaler Ebene. Doch für jeden Übergang mussten neue Instrumente und Strukturen erfunden und angewandt werden, da die alten bei jeder Veränderung des Umfangs ihre Grenzen zeigten.

Der Anbruch der technologischen Revolution kündigte einen raschen Anstieg des Fortschrittstempos an. Hardware, insbesondere Transistoren und Mikroprozessoren, wurde zum ersten großen Meilenstein, und das Mooresche Gesetz unterstrich einen exponentiellen Trend, den wir erleben würden. Software, anfangs meist proprietär, eroberte als nächstes unsere Vorstellungskraft, als klar wurde, dass sie die Welt auffraß. Die Open-Source-Bewegung brachte Software auf die nächste Stufe und schuf neuartige Werkzeuge und Standards, die die Zusammenarbeit weltweit skalieren konnten.
Darüber hinaus ist jetzt klar, dass wir an der Schwelle zu einem großen Paradigmenwechsel in Bezug auf Daten und Privatsphäre stehen. Wenn die Menschen aufwachen und ihren überraschenden Wert und Nutzen entdecken, gehen wir davon aus, dass neue Instrumente es bald jedem ermöglichen werden, seine privaten Daten nach Belieben zu sammeln, zu verwalten und zu monetarisieren. Neue Gesetze werden uns das Eigentum an den eigentlich unveräußerlichen Rechten einräumen, und dies wird den Übergang vom Datenfeudalismus zu offenen Datenmärkten markieren und einen produktiven Austausch ermöglichen, der auf souveränem Datenbesitz aufbaut.

Wenn es im Internet nur um Zusammenarbeit und die Digitalisierung von Inhalten ging, muss die nächste große Technologiewelle neuartige Koordinations- und Wirtschaftsmechanismen hervorbringen, die global skalierbar sind, den digitalen Besitz von Daten und Gütern durchsetzen und ein Arbeitsmodell für all dies bieten. Und genau hier kommt Elrond ins Spiel.

1.1 Programmierbares Geld

Die Menschen haben Geld und Schrift erfunden, um den Austausch von Werten und Informationen zu erleichtern. Dadurch wurde es einfacher, wirtschaftliche Transaktionen durchzuführen, und potenziell schwieriger, wirtschaftlichen Betrug zu begehen. Der wirtschaftliche Austausch ermöglichte es den Gemeinschaften zu wachsen, aber je größer sie wurden, desto schwieriger wurde es, sie zu koordinieren. So entwickelten wir Gesetze, um das Verhalten zu regulieren und Institutionen, um deren Einhaltung zu gewährleisten.

Heute sind neue Technologien entstanden, die es uns ermöglichen, den wirtschaftlichen Austausch auf globaler Ebene auf eine andere und weitaus bessere Weise zu skalieren. Kryptographisch gesicherte dezentrale Netzwerke haben eine Form von programmierbarem Geld mit besonders wertvollen Eigenschaften eingeführt, die erheblich an Zugkraft gewinnen.

Die wichtigsten Eigenschaften unter diesen sind:

- Kapitalvermögen
- Tauschmittel: unaufhaltsam, billig und schnell
- Wertaufbewahrung: beschlagnahme- und zensurresistent, nicht souverän
- Datenschutz: Anonymität auf Anfrage, Pseudoanonymität und Vertraulichkeit
- Programmierbar durch intelligente Verträge, die eine Reihe von (dezentralisierten) Finanzdienstleistungen (DeFi) ermöglichen: Finanzinstrumente für Derivate, Verbriefung und Tokenisierung von Vermögenswerten, Kreditvergabe, Treuhand, Hypothek, Versicherung, Absteckung, Delegation, Besicherung und viele andere.

Angesichts der oben genannten Eigenschaften glauben wir, dass programmierbares Geld ein Markt von mehreren Milliarden Dollar ist, der noch in den Kinderschuhen steckt. Programmierbares Geld wird eine bessere Abstimmung der Anreize erleichtern und neue Mechanismen zur Werterfassung ermöglichen, aber wir sollten darauf achten, nicht dieselben Fehler zu machen wie in traditionellen Volkswirtschaften.

Die Wirkung von Elrond-Token wird über Geld hinausgehen und schrittweise die Umwandlung von Daten, Identität und Eigentum in digitale Werte durch Tokenisierung ermöglichen.

1.2 Kryptoökonomie

Definitionen

Die Kryptoökonomie lässt sich treffend als die Verwendung von Anreizen und Kryptographie beim Entwurf verteilter Netzwerke beschreiben. Sie ist kein Teilgebiet der Ökonomie, sondern vielmehr ein Bereich der angewandten Kryptographie, der die Spieltheorie berücksichtigt.
Spieltheorie ist die mathematische Modellierung der strategischen Interaktion zwischen rationalen (und irrationalen) Agenten. Das Design von Mechanismen hingegen ist ein Teilgebiet der Spieltheorie, das oft als umgekehrte Spieltheorie bezeichnet wird, weil wir mit einem gewünschten Ergebnis vor Augen beginnen und rückwärts arbeiten um ein Spiel zu entwerfen, das dieses Ergebnis fördert. Ein Spiel, bei dem rationale, eigennützige Spieler ein gewünschtes Ergebnis erzielen.

Wenn es in der Spieltheorie also darum geht, die besten Züge in einer bestimmten Partie zu wählen, geht es beim Mechanismusdesign darum, eine Partie zu schaffen, die die von Ihnen gewünschten Züge berücksichtigt.

Zusammenfassend lässt sich sagen, dass die Kryptoökonomie aus zwei Komponenten besteht: der Kryptographie, die der Teil des Mechanismus ist, der die Integrität vergangener Schritte sicherstellt, und der Ökonomie, die der Teil des Mechanismus ist, der sicherstellt, dass alle Akteure die richtigen zukünftigen Schritte unternehmen..

Die wirtschaftlichen Sicherheitsgarantien eines jeden Kryptonetzwerks hängen zum Teil von der Stärke seiner Annahmen ab, also davon, wie die Menschen auf wirtschaftliche Anreize reagieren. Es sei jedoch darauf hingewiesen, dass die Gestaltung der Mechanismen kein Allheilmittel ist und dass die

Kryptoökonomie nicht in einem Vakuum angewendet werden kann. Es gibt eine Grenze, wie sehr wir uns auf Anreize verlassen können, um zukünftiges Verhalten vorhersagbar zu gestalten.

Erstellen eines Modells
Bei der Erstellung eines kryptoökonomischen Modells werden mehrere Aspekte berücksichtigt:

- gewünschtes Verhalten aller Akteure
- wirtschaftliche Anreize wie Belohnungen und Gebühren für die sich gut benehmenden Akteure, aber auch Strafen für jeden Akteur, der möglicherweise falsche Anreize in Bezug auf das gewünschte Verhalten gesetzt hat
- wirtschaftliche Regeln (wie Bewertung, Strafen oder Kürzungen), die von bestimmten Verhaltensweisen abschrecken: ungültige Protokollnachrichten, Nichtproduktion, Auslassung von Protokollnachrichten, Äquivokation und andere.

Die wirtschaftlichen Aspekte der Anreize, die umgesetzt werden, müssen berücksichtigen, dass es unabhängig vom Geldwert eines bestimmten Tokens Faktoren gibt, die das Wohlergehen des Systems beeinflussen, nämlich/

- die Inflation sollte klein genug sein, um die Token-Inhaber nicht zu "besteuern", aber groß genug, um ihre Einsatzkosten (laufende Nodes) zu decken
- die Geldmenge, die gestaked wird, sollte groß genug sein, damit es genügend verschiedene Einheiten gibt, so dass eine Kollusion unwahrscheinlich ist, aber klein genug, damit die Geldumlaufgeschwindigkeit nicht beeinträchtigt wird (MV=PQ)

Wie man sieht, ist die Kryptoökonomie die Spielregel, aber wie ändert man die Regeln, nachdem sie in Kraft gesetzt wurden? Die Antwort lautet Führung. Führung (Governance) ist die Macht, die Regeln zu ändern, und wenn das Spiel wertvoller wird, wird Governance zum Metaspiel, das diesen Wert erhalten oder zerstören kann.

1.3 Führung (Governance)

Kryptographisch gesicherte verteilte Netzwerke bieten eine neutrale Ebene der Dezentralisierung, Unveränderbarkeit, Privatsphäre und Vertrauen. Intelligente Verträge können daher sowohl für die Durchführung nachweislich fairer elektronischer Wahlen als auch für deren Kauf verwendet werden.

Angesichts ihrer bedeutenden und weitreichenden Implikationen ist die Gestaltung eines wirksamen Governance-Mechanismus für dezentralisierte Systeme eine anstrengende Aufgabe. Bloße Extrapolationen von Governance-Modellen aus der realen Welt erweisen sich als naiv, und viele Kryptonetzwerke werden wahrscheinlich aufgrund fehlerhafter Governance sterben, sobald ihr Netzwerk einen ausreichend hohen Wert erreicht hat, um eine Reihe entscheidender Angriffe zu rechtfertigen.

Daher erfordert die Governance eine separate, eingehende Betrachtung. Das Elrond-Governance-Modell wird in einem zukünftigen Dokument skizziert werden, das zu einem späteren Zeitpunkt nach der offiziellen Einführung des Elrond-Netzwerks veröffentlicht werden soll. Vor diesem Zeitpunkt wird Elrond einen robusten Off-Chain-Governance-Ansatz anwenden, um maximale Geschwindigkeit und Effizienz zu gewährleisten.

1.4 Begriffe und organisatorische Komponenten

Für die Begriffe, die zur Beschreibung der verschiedenen Akteure und Maßnahmen innerhalb des Elrond-Wirtschaftsmodells verwendet werden, ist eine klare Definition erforderlich.

Benutzer oder Netzwerk-Teilnehmer
Jede Partei, Einzelperson, Einheit, Unternehmen, Blockchain oder Netzwerk, die einen beliebigen Aspekt des Elrond-Netzwerks nutzt, entwickelt, schafft oder mit ihm interagiert. Benutzer werden durch eine eindeutige Kontoadresse identifiziert (abgeleitet von ihrem öffentlich-privaten Hauptschlüsselpaar, das in einer Wallet gespeichert ist).

Token-Inhaber
Benutzer, die Inhaber von nativen eGold-Token sind, die im Elrond-Netzwerk verwendet werden, um unterzeichnete Transaktionen für Werttransfers, intelligente Vertragsabwicklung oder zur Bereitstellung von Liquidität einzureichen.

Anwendungsentwickler
Benutzer, die intelligente Verträge und/oder Anwendungen entwickeln, die sich bei der Bereitstellung von Dienstleistungen auf intelligente Verträge stützen. Entwickler benötigen ein Konto, um intelligente Verträge im Netzwerk bereitstellen zu können.

Konsensus-Gruppe
Damit ein Block vorgeschlagen und bestätigt werden kann, wird eine bestimmte Anzahl von Nodes (numNodesConsensus) nach dem Zufallsprinzip aus allen in Frage kommenden Shards (eligibleNodesPerShard) ausgewählt, die während jeder Runde (blockTime) einem Shard zugeordnet werden, um die Konsensgruppe zu bilden. Die Konsensgruppe trägt die Verantwortung dafür, während jeder Runde Blöcke in diesem Shard zu binden (blockTime). Zu Beginn jeder Runde wird eine neue Konsensgruppe ausgewählt. Die Konsensgruppe im Metachain-Shard ist so konfiguriert, dass numNodesConsensus = eligibleNodesPerShard, was effektiv dazu führt, dass die gesamte Metachain den Shard der Konsensgruppe bildet. Dies ist durch die hohen Sicherheitsanforderungen der Metachain motiviert.

Nodes
Geräte (Computer oder Server), auf denen die Software (der Elrond-Client) läuft und die Nachrichten von anderen Peers weiterleiten. Sie können entweder Validatoren (die aktiv an der Sicherung des Netzwerks teilnehmen) oder Beobachter (passive Mitglieder des Netzwerks, die als Lese- & Weiterleitungsschnittstelle fungieren können) sein und können entweder Full (haben den gesamten Verlauf der Blockchain) oder Light-Nodes (behalten nur 2 Epochen des Blockchain-Verlaufs) sein. Eine Node steht auf der Liste der in Frage kommenden Node, wenn mehrere Voraussetzungen erfüllt sind: eine Bewertung über einem bestimmten Schwellenwert, der Gewinn eines Node-Slots in der Auswahl-Auktion (wann die Auktion aktiviert wird), die Zuweisung zu einem Shard, usw.

Node Varianten	Teilnehmende	Nichtteilnehmende (Beobachter)
Full	Eine Node, die über jede	Eine Node, die jede Transaktion, die jemals

	Transaktion im Netzwerk Buch führt und auch eGold einsetzt, um am Konsensmechanismus teilzunehmen (auch Validator)	stattgefunden hat, in ihren Shards aufzeichnet. Setzt nicht ein und schlägt daher keine Blöcke vor oder unterzeichnet sie.
Light	Eine Node, die einen Anteil hat (so wie ein Validator) und nur die Aufzeichnungen von Transaktionen der letzten Epoche(n) führt	Kein Stake-Anteil und hält nur 2 Epochen des Blockchain-Verlaufs

Validatoren

Validatoren sind Nodes - Computer im Elrond-Netzwerk, die Transaktionen verarbeiten und das Netzwerk sichern, indem sie am Konsensmechanismus teilnehmen und gleichzeitig Belohnungen aus dem Protokoll und Transaktionsgebühren erhalten. Um Teil des Elrond-Netzwerks zu werden, muss ein Validator eine Sicherheit in Form von eGold-Tokens hinterlegen, die gestaked werden, um die Anreize der Validatoren mit dem korrekten Funktionieren des Netzwerks in Einklang zu bringen. Validatoren verlieren einen Teil oder ihren gesamten Anteil, wenn sie von den Anweisungen des Protokolls abweichen oder anderweitig Absprachen treffen, um das Netzwerk zu stören. Ein Node kann nur dann ein Validator werden, wenn er auf der Liste der in Frage kommenden Nodes steht.

Blockantragsteller

Die Rolle des Blockantragstellers wird dem ersten ausgewählten (durch einen unvoreingenommenen, zufälligen Prozess) Validierungsshard in der Konsensgruppe zugewiesen. Der Blockvorschlagende ist der Validierer, der den nächsten Block vorschlägt, den der Rest der Konsensgruppe überprüfen und genehmigen muss.

Block Belohnungen

Die Blockchain belohnt die Validator-Shards für ihr eingesetztes eGold. Die Belohnung kann aus zwei Arten bestehen: einem Teil der Transaktionsgebühren und der Neuemission von eGold (auch Prägung oder Inflation genannt). Elrond-Inhaber, die ihr eGold nicht staken, indem sie ein Validator sind oder ihr eGold an einen Validator delegieren, erhalten keine der Blockprämien.

Shards

Das Netzwerk besteht zu jedem beliebigen Zeitpunkt aus einer Reihe von Shards, wobei jeder Shard eine Teilmenge aller Adressen und den zugehörigen Status enthält, einschließlich der Adressen von Benutzerkonten und intelligenten Verträgen (smart Contracts). Jeder Shard betreibt eine eigene Blockchain, aber alle Shards sind über die Metachain miteinander verbunden.

Metachain

Eine Blockchain, die parallel und synchron zu den Shards läuft und für die notarielle Beglaubigung der von den Shards begangenen Blöcke sowie für die Kommunikation zwischen den Shards verwendet wird. Alle berechtigten Validierer in der Metachain nehmen an ihrem Konsens teil. Anstatt eine Konsensgruppe zu wählen, wird die Zufallsquelle nur zur Auswahl eines Blockproduzenten verwendet. Der Metachain-Blockproduzent setzt einen Metablock zusammen, der aus Shard-Header-Informationen und Miniblock-Headern besteht, von denen jeder durch mindestens einen Shardblock in seinem relevanten Shard bestätigt werden muss. Der Vorschlagende des Metachain-Blocks erstellt bei Bedarf auch den "Start-of-Epoch"-Block. Die Metachain ist auch für den Stack/Unstake/Unjail (Änderungen in der Validator-Konfiguration) und das Slashing verantwortlich.

Protokoll Nachhaltigkeit
Die Nachhaltigkeit des Protokolls hat den Zweck, die Sicherheit und den Wert des Netzwerks kurz-, mittel- und langfristig zu erhöhen. Die Besonderheiten der Governance (Führung) und der Verwaltung der Protokollkasse werden in dem Governance-Dokument vorgestellt. Bis dahin wird die Protokollkasse unter der Kontrolle und Aufsicht des Elrond-Kernteams stehen.

Protokoll-Verwaltungsorgan
Eine selbstorganisierte, dezentralisierte, autonome Organisation, die von einer gemeinnützigen Stiftung überblickt wird.

Weitere Einzelheiten zu den technischen Aspekten sind im Whitepaper (https://elrond.com/assets/files/elrond-whitepaper.pdf) beschrieben, das den Aufbau des Elrond-Protokolls im Detail beschreibt.

2. Validatoren

Um das Netzwerk zu sichern, wird Elrond ein "Proof of Stake"-Modell verwenden.

Im Gegensatz zu Proof-of-Work (PoW)-Systemen benötigt Elrond keine Maschinen zur Lösung von Rätseln. Stattdessen wird die gesamte Rechenleistung des Netzwerks für die eigentlichen Transaktionen genutzt, so dass mit dem Proof-of-Stake die Energieeinsparung erheblich ist. Darüber hinaus benötigt Elrond keine GPUs oder Spezialchips zur Unterstützung des Netzwerks: Sie können mit der bereits vorhandenen Hardware zum Netzwerk beitragen und es unterstützen (wenn sie die Mindestanforderungen erfüllt: Dual-CPU, SSE4- und x64-fähige CPU, 4 GB RAM, 80 GB HDD).

Bei Proof-of-Work (PoW)-Systemen, bei denen ein Miner alles nimmt (Blockbelohnung + Transaktionsgebühren), gibt es nur eine Möglichkeit, Ihre Erfolgschancen zu verbessern: Erhöhen Sie Ihre Hash-Power. Dies führt zu drei Ergebnissen: I) es wird unwirtschaftlich, dass kleine Geräte mit geringer Leistung teilnehmen, II) eine massenhafte Zusammenlegung von Ressourcen wird wünschenswert, und III) eine Spezialisierung der Hardware wird notwendig.

Im Gegensatz dazu stützt sich der Proof-of-Stake (PoS) nicht auf Belohnungen für die Sicherung des Netzwerks, sondern auf Strafen. Die Validatoren setzen Geld ("Kautionen") ein und werden für die Bindung ihres Kapitals und die Kosten für die Instandhaltung einer Node entschädigt. Der größte Teil der Kosten, wenn gegen die Regeln verstoßen wird, entsteht durch Strafen, die hundert- oder tausendmal größer sind als die Belohnungen, die ein Angreifer in der Zwischenzeit erhalten könnte. Wenn also im PoW die Miner miteinander konkurrieren, arbeiten im PoS die Validierer miteinander zusammen.

Auf diese Weise ermöglicht ein PoS-Netzwerk eine wesentlich ressourceneffizientere, skalierbarere und umfassendere Art und Weise der Aufrechterhaltung eines genehmigungsfreien Blockchain-Netzwerks. Ein Blick auf die Zahlen, die in den frühen PoS-Netzwerken und den beiden größten PoW-Netzwerken (Bitcoin und Ethereum) gesammelt wurden, zeigt, dass das für die Infrastruktur ausgegebene Geld am PoS um eine Größenordnung kleiner ist als am PoW (etwa 10% der Belohnungen statt 100%).

In Elrond gibt es also kein Mining. Stattdessen verdienen die Validatoren Tokens für nützliche Arbeit. Einer der wichtigsten Aspekte, den wir bei der Gestaltung des Elrond-Netzwerks im Auge hatten, war die Gewährleistung von Fairness für alle Netzwerkteilnehmer. Im Falle der Validatoren haben wir Elrond so

konzipiert, dass es der Konzentration von Ressourcen widersteht und eine gleichmäßige und faire Verteilung der Belohnungen auf der Grundlage der von allen Validatoren, ob groß oder klein, geleisteten Arbeit gewährleistet ist.

Die Teilnehmer des Netzwerks bringen einen Mehrwert für das Netzwerk. Je mehr Validatoren, desto mehr eGold steht auf dem Spiel und desto größer ist die Sicherheit und Dezentralisierung des Netzwerks. Angesichts der Tatsache, dass Shard-Netzwerke wie Elrond eine notwendige Anzahl von Validatoren benötigen, um mehrere gut gesicherte Shards zu bilden, haben wir einen Validator-Client entwickelt, der auf durchschnittlicher Verbraucher-Hardware läuft, ohne dass komplexe Setups und langwierige Konfigurationen erforderlich sind.

2.1 Auswahl der Validatoren

Eines der Hauptziele, das wir beim Entwurf des Elrond-Protokolls im Auge hatten, war eine hohe Skalierbarkeit. Dies erreichen wir durch die Partitionierung des Netzwerks in Shards, die eine parallele Verarbeitung von Blöcken ermöglicht. Mehr Validatoren bedeuten, dass mehr Shards erstellt werden können, so dass das Netzwerk mehr Transaktionen verarbeiten kann und somit skalierbar ist. In diesem Sinne müssen wir berücksichtigen, dass die Anzahl der Validatoren und Shards den aktuellen Bedürfnissen des Netzwerks (einschließlich - bis zu einem gewissen Grad - einer plötzlichen Zunahme der Nutzung) entsprechen sollte. Da zu viele Shards bedeuten, dass das Protokoll die Ressourcen zu wenig nutzt und die Kosten höher sind als nötig, sollten wir anstreben, dass alle Shards eine Auslastung von etwa 50% haben (*targetShardLoad*).

Deshalb planen wir eine stufenweise Einführung des Mainnets, bei der die Anzahl der Nodes auf eine bestimmte Anzahl (numNodes) begrenzt ist. Diese Grenze kann sich sowohl mit dem Phasenverlauf als auch mit den Bedürfnissen des Netzwerks erhöhen, wobei ein Gleichgewicht zwischen Sicherheit, Dezentralisierung, Effizienz und den erwarteten Bedürfnissen des Netzwerks, insbesondere in Bezug auf Durchsatz, Datenverfügbarkeit und Speicherung, gewahrt werden muss..

Es wird eine begrenzte Anzahl von Nodes pro Shard geben, so dass numNodes proportional mit der Anzahl der Shards wachsen wird, die das Netzwerk zur Verarbeitung und Speicherung benötigt. So wird eine Mindestanzahl von 3 Shards (plus Metachain) gebildet, so dass die Reorganisation der Shards am Ende der Epoche sinnvoll ist.

Der NodePrice, d.h. die Höhe des für den Betrieb eines Nodes erforderlichen Einsatzes, wird durch einen Auktionsmechanismus bestimmt, der es dem Markt ermöglicht, das optimale Sicherheits-/Belohnungsverhältnis zu bestimmen.

Die Anzahl der in Epoche ei+2 verfügbaren Validatornode-Slots wird wie folgt bestimmt:

- Jeder Shard wird eine Anzahl von berechtigten Validierungsnodes OptN haben. Die Anzahl der Validierungsnodes pro Shard ist eine feste Zahl, die derzeit auf 400 festgelegt ist. Sie wird zur Entstehungszeit festgelegt. Diese Anzahl ist für alle Shards gleich. Die Metachain kann sich unterscheiden, da sie einen bestimmten Konfigurationswert hat. All dies wird zur Genesis-Zeit von der Genesis-Konfiguration aus festgelegt.
- Wenn $N_{sh,i+2}=2$ dann beträgt die netzwerkweite Anzahl der Validierer in Epoche ei+2 2*optN. Wenn $N_{sh,i+2}>2$ dann ist die netzwerkweite Anzahl der Validierer in Epoche ei+2 $(N_{sh,i+2}+1)$*optN, was bedeutet, dass sich die Anzahl der Shards pro Epoche um 1 ändert.

Diese Validator-Slots werden mit Hilfe des Auktionsmechanismus zugewiesen. Jeder Node-Betreiber, der mit seinen Nodes als Validierer teilnehmen (oder weiterhin teilnehmen) möchte, reicht eine unterzeichnete Transaktion beim Auction Smart-Contract ein, die sein Gebot repräsentiert. Wenn der Node-Betreiber später seinen Anteil oder die Anzahl der von ihm ausgeführten Validatoren aktualisieren möchte, sendet er eine weitere Transaktion mit einem aktualisierten Gebot an den intelligenten Auktionsvertrag.

Die Biettransaktion enthält:

- $stake_v$, der Gesamtbetrag der von diesem Node-Betreiber zugesagten Beteiligung, angegeben durch den Wert der Transaktion selbst.
- $nodes_v$, die Anzahl der Validator-Nodes, zu deren Betrieb sich der Betreiber verpflichtet, sowie die eindeutigen öffentlichen BLS-Schlüssel, Pk, für jeden von ihnen.
- *rewardAddress,* die Adresse des Kontos, an das die von jedem Node in $nodes_v$ verdienten Belohnungen geschickt werden. Unabhängig von der Anzahl der Nodes in der BLS-Schlüsselliste des Gebots gibt es eine einzige Reward-Empfängeradresse für alle Nodes.
- *maxNodePrice* (optional), der maximale Preis, den der Betreiber nach eigenen Angaben für einen einzelnen Node bezahlen wird. Das bedeutet, dass der Validator nicht bereit ist, mehr als diese Zahl für den Betrieb eines Nodes einzusetzen. Am Ende der Auktion, am Ende der Epoche, wird der *nodePrice* für die Epoche ei+2 berechnet. Jedem Node-Betreiber, dessen *maxNodePrice* unter dem berechneten *nodePrice* liegt, werden alle seine Nodes herausgenommen. Es gibt keine andere Beziehung zwischen den genannten Variablen.
- *proposalFee,* legt fest, wie viel von der Belohnung der nächsten Epoche an den Blockvorschlagenden gegeben wird, der die Nodes des Betreibers einschließt (zu diskutieren und vielleicht zu einem späteren Zeitpunkt hinzuzufügen).

Die intelligenten Verträge mit Einsätzen (Staking) und Auktionen befinden sich in der Metachain. Die beiden Verträge arbeiten zusammen und speichern die von den Knotenbetreibern eingereichten Gebote, so dass pro Betreiber ein Gebot abgegeben werden kann: Jedes Gebot wird unter der Kontoadresse gespeichert, von der aus die Transaktion eingereicht wurde (nicht zu verwechseln mit der RewardAddress innerhalb des Gebots selbst).

Darüber hinaus werden in den intelligenten Verträgen für Einsätze (Staking) und Auktionen auch die Kontoadressen der erfolgreichen Gebote für die Epochen e_i, e_{i+1} und e_{i+2} sowie die öffentlichen BLS-Schlüssel, die ausgewählt wurden, gespeichert.

Zu Beginn jeder Epoche wird der Validator-Auswahlmechanismus unter Berücksichtigung des zuletzt eingereichten Angebots der Node-Betreiber ausgelöst. Der Auswahlmechanismus weist dann die Validator-Slots für Epoche e_{i+2} den Nodes der bietenden Betreiber zu.

Der Prozess läuft wie folgt ab:

1. Zuerst muss festgelegt werden, welche Nodes an der Auktion teilnehmen dürfen:
    a. Nodes der Betreiber, die noch nicht unstaked sind
    b. Nodes, deren Rating über dem Mindest-*RatingThreshold* liegt. Wenn das Rating eines Nodes unter diesen Schwellenwert fällt, wird er vom Staking-Smart-Kontrakt inhaftiert. Solche Transaktionen müssen von niemandem unterzeichnet werden, da sie das Ergebnis deterministischer Berechnungen sind, d.h. sie werden von allen Validierern der Metachain identisch erstellt.

2. Zweitens muss der Wert von *nodePrice* berechnet werden, d.h. der Betrag, der für jeden validierenden Node während der Epoche e_{i+2} eingesetzt wird. Dieser Wert hängt von den aktuell registrierten Geboten ab (entweder neu von Betreibern abgegebene Gebote oder Gebote, die implizit aus den vorherigen Epochen übernommen wurden) und von der Gesamtzahl der Nodes, die am Auktionsprozess teilnehmen dürfen, wie unter (1) beschrieben. Die folgenden Gleichungen beschreiben die Berechnung des *nodePrice*, der als der höchste Wert definiert ist, für den eine ausreichende Anzahl von Nodes von ihren Betreibern eingesetzt werden kann. Dies bedeutet, dass *nodePrice* die Beziehung erfüllen muss

$$nodeCount(Bids,\ nodePrice)\ \geq\ numNodes\,,$$

wobei die Funktion *nodeCount* wie folgt definiert ist:

$$nodeCount(Bids,\ nodePrice) = \sum_{bid\ \in\ Bids} min\left(bid.nodes,\ floor\left(\frac{bid.stake}{nodePrice}\right)\right)$$

Es ist zu erkennen, dass *nodeCount* mit steigendem *nodePrice* abnimmt, was einfach bedeutet, dass je teurer die Nodes sein müssen, desto weniger Nodes als Validatoren in der Epoche e_{i+2} gewählt werden können. Aus diesem Grund muss *nodePrice* niedrig genug gehalten werden, um mehr Validatoren als die erforderliche Anzahl Nodes zuzulassen, aber hoch genug, um nur die Nodes der am höchsten zahlenden Bieter auszuwählen. Der endgültige Wert von *nodePrice* wird daher sein:

$$nodePrice = max\left(\{price\ :\ nodeCount(Bids,\ price)\ \geq\ numNodes\}\right)$$

3. Als nächstes wird die Gesamtzahl der vorgeschlagenen Validierer über alle Gebote der Node-Betreiber betrachtet:
    - Die Situation wenn $\sum_{bidv\in Bids} bid.nodes < numNodes$ kann, per Design, nicht passieren, unabhängig vom *nodePrice*. Die Genesis wird korrekt gestartet, wenn die Anzahl der Nodes gleich oder höher als numNodes ist. Darüber hinaus ist es für keinen Betreiber eines Nodes möglich, ein Unstake durchzuführen, wenn die Gesamtzahl der vorgeschlagenen Validierer gleich oder kleiner als *numNodes* ist. Das Zusammenführen von Shards muss zuerst erfolgen (und damit die Anzahl der *numNodes* verringern), bevor ein *Unstake* wieder möglich ist.
    - If $\sum_{bid\in Bids} bid.nodes = numNodes$, dann wird jeder Node-Betreiber genau die Anzahl von Nodes ausführen, die er in seinem Angebot vorgeschlagen hat.
    - If $\sum_{bid\in Bids} bid.nodes > numNodes$, dann wird die Menge an eGold, die jeder Node-Betreiber in seinen Geboten abgibt, bewertet, und jeder Node-Betreiber erhält die Anzahl der Validator-Slots proportional zum Betrag, den er bietet, im Verhältnis zum Gesamtbetrag der Gebote aller. Wenn es mehrere Validierer gibt, die sich mit demselben Gebot qualifizieren und nicht alle ausgewählt werden können, dann wird bei der Auswahl die Bewertung der einzelnen Nodes berücksichtigt, um zwischen ihnen zu unterscheiden (höhere Bewertungen werden bevorzugt). Wenn eine Auswahl immer noch nicht möglich ist, können sie schließlich nach dem Zufallsprinzip ausgewählt werden.

- Jeder Node-Betreiber, dem mindestens ein Validator-Slot zugeteilt wird, setzt den nodePrice multipliziert mit der Anzahl der zugeteilten Slots ein. Eingesetztes eGold bleibt in dem SC der Auktion.
- Jeder Betrag, der über diesen eingesetzten Betrag hinaus geboten wird, kann vom Bieter jederzeit abgerufen werden. Wenn er den Überschuss zurückziehen möchte, kann er dies durch eine "Abruf-Transaktion" tun. In diesem Fall wird das Gebot für die nächste Epoche ohne den zurückgezogenen Betrag berechnet. Wenn die Transaktion "Abruf" nicht eingereicht wird, wird der Überschuss nicht beansprucht und das vorherige Gebot bleibt wie bisher.

Kurz gesagt, die Höhe des Einsatzes bestimmt die Anzahl der Validator-Slots, die einem Betreiber für seine Nodes zugewiesen werden. Wenn ein Validierer das 5-fache des für einen Knoten erforderlichen Einsatzes (Staking) hat (d.h. das 5-fache des berechneten *nodePrice*), dann muss er 5 Nodes ausführen. Dieser Ansatz schafft Anreize für professionelle Staking-as-a-Service-Provider, um eine gute Infrastruktur aufrechtzuerhalten und bietet gleichzeitig vielen Validatoren einen Anreiz, nur ein oder zwei Nodes zu kontrollieren, ohne dass komplizierte Setups erforderlich sind, wodurch das Feld ausgeglichen wird und die durchschnittliche Verbraucher-Hardware eine faire und ausreichende Belohnung erhält.

Es wird einen vordefinierten Mindestreserve-Nodepreis geben, so dass der Nodepreis nicht unterschritten werden kann. Der Mindestreserve-Nodepreis kann ein fester Betrag in eGold sein oder an einen festen Betrag in USD gebunden sein.

Um das Elrond Mainnet zu unterstützen, haben wir bei Genesis ein geschlossenes Staking und Delegationssystem eingeführt. Dies bedeutete ein vorübergehendes No-in und No-out für Validatoren oder Delegierte. Der Bootstrapping-Prozess wurde so konzipiert, dass eine möglichst schnelle Abwicklung erreicht und eine ausreichend große Gemeinschaft um das Elrond-Netzwerk versammelt werden konnte. Ein weiteres Ziel, das wir im Auge hatten, war die Schaffung einer unerschwinglichen wirtschaftlichen Prävention gegen Angriffe auf das Netzwerk, wobei wir sicherstellen wollten, dass die Angriffskosten für böswillige Akteure umso höher sind, je größer das für das Staking gesperrte Angebot ist.

Bei Genesis wurde das Mainnet mit einem festen Einsatz (Stake) pro Node, 2500 eGLD und einer festen Anzahl von Validatoren gebootet: 2169, die 3 Shards und eine Metachain bildeten.

Der Übergang von dieser Bootstrapping-Phase zu einem nachhaltigen Wachstumsmodell wird in Phasen erfolgen.

- Phase 1 und 2 ermöglichen Validatoren und Delegatoren Warteschlangen, so dass die Anzahl der Nodes fest oder über einem bestimmten Schwellenwert bleibt, während neue Gemeinschaftsmitglieder der Warteschlange beitreten können, indem sie ihre eGLD-Token delegieren oder staken und einen Platz in der Warteschlange reservieren. Diese Warteschlangen ermöglichen es auch bestehenden Delegatoren und Validatoren, ihren Einsatz zurückzuziehen, wenn sie dies wünschen, und sie so durch die ersten, die in der Warteschlange reserviert wurden, zu ersetzen.
- Phase 3 und 4 werden Funktionen beinhalten wie: Erhöhung der Gesamtzahl der Nodes, die Möglichkeit des Staking von mehr als 2500 eGLD pro Node, offene Delegation mit einem neuen Systemdelegations-Smart Contract, durch den jeder Delegationen empfangen und annehmen kann, und ein neues und verbessertes (weiches) Auktionssystem. Der Übergang zu Phase 3 und 4 wird sehr wahrscheinlich auch unsere erste gemeinschaftliche Abstimmung auf der Blockchain beinhalten.

2.2 Bewertungen der Validierer

Wie bei jedem dezentralisierten und genehmigungslosen Netzwerk erwarten wir die Teilnahme vieler Validierer von verschiedenen Standorten aus, die unterschiedliche Hardware-Spezifikationen, Infrastruktur-Einrichtungen, Internet-Verbindungen, Bandbreite usw. verwenden. Dies wird zu unterschiedlichen Leistungen in Bezug auf Betriebszeit, Reaktionszeit, Rechenzeit usw. führen. Diese Unterschiede sind zwar akzeptabel und zu erwarten, aber je dezentraler das Netzwerk ist, desto deutlicher wird, dass bestimmte Aktionen wünschenswerter sind, während andere Aktionen nicht wünschenswert sind. Denken Sie daran, dass wir uns bei der Erörterung der Bewertung im Allgemeinen auf die Betriebszeit und die Hardware-/Setup-Leistung beziehen (die sich als die Anzahl der erfolgreich vorgeschlagenen und unterzeichneten Blöcke manifestiert) und nicht auf das Verhalten und die Aktionen gegen das Protokoll, die durch den Schrägstrich-Abschnitt abgedeckt werden (Doppelsignierung, Äquivokation usw.).

Durch den Bewertungsmechanismus belohnen wir erwünschte Leistungen (z.B. Betriebszeit und korrekter Vorschlag eines Blocks), aber wir bestrafen auch unerwünschte Aktionen, die die Leistung des Netzwerks beeinträchtigen (z.B. fehlende Blockvorschläge). Je höher die Bewertung einer Node, desto höher ist die Chance, in einer Runde als Konsensvalidator ausgewählt zu werden (was die Möglichkeit impliziert, Belohnungen zu erhalten). Umgekehrt ist die Chance, als Validierer ausgewählt zu werden, umso geringer, je niedriger das Rating (aber über einem konfigurierten Wert ratingThreshold) liegt. Die Belohnung oder Bestrafung erfolgt lediglich durch eine Erhöhung oder Verringerung des Node-Ratings, so dass es sich nicht um eine Kürzung handelt.

Die Bewertung einer Node ist ein ganzzahliger Wert zwischen 0 und 100, einschließlich. Alle Bewertungen werden von der Metachain gespeichert, die die Aktivität der Nodes Runde für Runde verfolgt, und am Ende einer Epoche passt die Metachain die Bewertungen entsprechend an. Jede Node tritt dem Netzwerk mit dem gleichen anfänglichen Start-Rating bei, das von Epoche zu Epoche weitergeführt und angepasst wird.

Tabelle 1 stellt quantitativ dar, wie das Rating einer Node seine Chance, als Konsensusvalidierer ausgewählt zu werden, erhöht oder verringert (vorbehaltlich zeitlicher Änderungen, wenn mehr Daten zur Verfügung stehen).

Tabelle 1

Bewertungsintervall	**Zufalls-Modifikator**
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%

Eine Validator-Node kann seine Bewertung auf zwei Arten erhöhen:

1) Aufrechterhaltung einer guten Bilanz bei der Unterzeichnung vorgeschlagener Blöcke. Immer wenn eine Node als Konsens-Validierer ausgewählt wird, wird ihr Rating implizit um den Wert *validatorRatingIncrease* erhöht, sofern ein guter Blockunterzeichnungsnachweis vorliegt.
2) Vorschlagen eines gültigen Blocks, wenn er als Blockvorschlagsteller (d.h. als Konsensführer) ausgewählt wird. Ein gültiger Block führt dazu, dass das Rating des Blockantragstellers um den Wert *proposerRatingIncrease* erhöht wird.

Damit eine Node bei ihrer Auswahl für den Konsens *validatorRatingIncrease* erhalten kann, muss sie einen Mindestprozentsatz von Blöcken aus der letzten fortlaufenden Sequenz von *numValidatedBlocksRange* unterzeichnet haben, für die sie als Validator tätig war (Zählen in die vergangene Epoche ist erlaubt). Der Prozentsatz der unterzeichneten Blöcke muss gleich oder größer als der Wert von *signedBlocksThreshold* sein. Der Grund für diesen Ansatz ist die Tatsache, dass für die Validierung eines vorgeschlagenen Blocks nur ⅔ +1 Signaturen erforderlich sind. Wir gehen davon aus, dass eine Node ihre Signatur zumindest auf einigen Blöcken in einem bestimmten, ausreichend langen Zeitrahmen (oder einer bestimmten Anzahl von Blöcken) vorhanden ist, um ihre Bewertung für die Validierung zu erhöhen. Diese Grenze muss hoch genug sein, so dass wir keine Trittbrettfahrer-Node ermutigen, die nicht wirklich Blöcke signieren, sondern nur Blöcke vorschlagen, wenn sie zufällig Blockvorschlagsteller sind. Auf der anderen Seite werden Nodes, die durchweg langsam sind und nicht in der Lage sind, ihre Signatur für Blöcke in der erforderlichen Zeit zu senden, irgendwann keine Rating-Erhöhung für die Auswahl in einer Konsensgruppe mehr erhalten, weil ihr Prozentsatz an signierten Blöcken unter den *signedBlocksThreshold* fällt. Außerdem könnten sie in dieser Situation anfangen, Rating-Punkte zu verlieren (die zu einem späteren Zeitpunkt umgesetzt werden sollen).

Das Bewertungsmodell ist also darauf ausgerichtet, produktive Nodes so weit wie möglich zu fördern, entweder als Validierer oder als Antragsteller. Ein primäres Designanliegen ist die Frage, wie lange eine Node nach ihrem Beitritt zum Netzwerk braucht, um die maximal mögliche Bewertung zu erreichen. Diese Dauer wird als HoursToMaxRatingFromStartRating bezeichnet, und es handelt sich um die erwartete Anzahl von Sekunden, die eine Node benötigt, um allmählich das maximal mögliche Rating (maxRating) unter idealen Bedingungen zu erreichen, beginnend mit dem anfänglichen Ratingwert, startRating. Der Wert von HoursToMaxRatingFromStartRating wird wahrscheinlich so konfiguriert, dass er ein paar Tage beträgt.

Ausgehend von *HoursToMaxRatingFromStartRating* definiert das Modell die Funktionen *avgValidatorRatingPerRound*(·) und *avgProposerRatingPerRound*(·), die die durchschnittliche Anzahl der von einem idealen Node pro Runde erzielten Bewertungspunkte ausdrücken, wenn er als Validierer bzw. als Vorschlagender ausgewählt wird. Diese Funktionen hängen von den oben genannten *HoursToMaxRatingFromStartRating* ab, sowie von der Shard-Topologie, der Konsensusgruppenkonfiguration und dem *importanceRatingRatio*, einem festen Verhältnis, bezeichnet als:

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

Dieses Verhältnis gleicht die Anzahl der Bewertungspunkte aus, die Validierer und Antragsteller erhalten haben, was notwendig ist, da es viel wahrscheinlicher ist, in einer Runde als Validierer und nicht als Antragsteller ausgewählt zu werden. Für Block-Antragsteller ist es wünschenswert, dass der Gesamtbeitrag zur Bewertung der gesamten in einer Epoche vergebenen Proponenten-Rating-Zunahme idealerweise mit der Summe der vergebenen Validator-Rating-Zunahme übereinstimmt. Die genauen Definitionen von

avgValidatorRatingPerRound(·) und *avgProposerRatingPerRound*(·) befinden sich derzeit in der Entwicklung, da sie von dem für den Konsens-Auswahlalgorithmus gewählten Modell abhängen.

Die Werte für *validatorRatingIncrease* und *proposerRatingIncrease* können wie folgt ausgedrückt werden:

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

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

Die derzeitige Absicht besteht darin, sowohl *validatorRatingIncrease* als auch *proposerRatingIncrease* auf konstanten Werten zu halten. Um dies zu erreichen, müssen die Definitionen von *avgValidatorRatingPerRound*(·) und *avgProposerRatingPerRound*(·) entsprechend angepasst werden, da sie das Rating eines Node verändern, was wiederum seine Wahrscheinlichkeit verändert, für den Konsens ausgewählt zu werden. Wie bereits erläutert, wirkt sich dies dann auf das Rating aus und bildet eine kontrollierte Rückkopplungsschleife. Nicht konstante Alternativen für *validatorRatingIncrease* und *proposerRatingIncrease* werden vom Team ebenfalls in Betracht gezogen.

Abgesehen davon, dass sein Rating erhöht wird, wird das Rating eines Validierers verringert, wenn er bei der Auswahl als Blockvorschlagssteller keinen gültigen Block vorschlägt, unabhängig vom Grund des Scheiterns. Jedes Mal, wenn ein Blockantragsteller seine Rolle nicht erfüllt, wird sein Rating mit der folgenden Strafe angepasst:

$$proposerRatingDecrease = -4 \cdot proposerRatingIncrease$$

Bei einem Validierer, der offline ist oder nicht in der Lage oder willens ist, neue Blöcke zu produzieren oder zu unterschreiben, wird seine Bewertung viel schneller sinken als die Rate steigt. Dies kann weiter beschleunigt werden, wenn mehr Nodes ihr Rating unter *ratingThreshold* haben.

Es liegt an der Umsetzungsphase, ehrliche Block-Antragsteller nach einer böswilligen Runde (1 Block vorher) nicht durch Verzögerung des Blocks zu bestrafen.

Der Metachain Shard wählt seine Konsensgruppe anders aus. Während die Auswahl des Block-Antragstellers tatsächlich dieselbe ist wie bei den übrigen Shards, wird jeder Node, der nicht der Block-Antragsteller ist, automatisch zum Konsensvalidator. Dies geschieht, weil die Konsensgruppe im Metachain-Shard so konfiguriert ist, dass sie die Größe des gesamten Shards hat, was die Sicherheit erhöht. Um die Konsistenz mit den anderen Shards zu wahren, ersetzt die Metachain die Definition von *validatorRatingIncrease* durch *validatorRatingIncreaseMeta*:

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

Rating-Belohnungen und Strafen für Block-Antragsteller in der Metachain bleiben die gleichen wie bei den Shards:

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

$$proposerRatingDecrease = -4 \cdot proposerRatingIncreaseMeta$$

Um die Eliminierung potenziell Offline-Nodes zu beschleunigen, werden wir eine Strafe einführen, die mit jedem aufeinanderfolgenden Versäumnis, einen Block vorzuschlagen, erhöht wird, wenn wir als Antragsteller ausgewählt werden. Dieser Wert ist der PropositionerPenaltyGrowth (in der Genesis-Konfiguration heißt er "consecutiveMissedBlocksPenalty" und kann für Shards und Meta unterschiedlich eingestellt werden; die Standardeinstellung ist derzeit 1,1, 10% Erhöhung des PropositionerRatingDecrease), der so konfiguriert ist, dass ein Node, der ständig keine Blöcke vorschlägt, wenn er als Blockvorschlagsteller ausgewählt wird, sein Rating in etwa 10 Stunden unter den RatingThreshold absinken lässt, so dass er nicht an der nächsten Auktion teilnehmen kann. Darüber hinaus wird ein Node, der während einer Epoche nicht alle Blöcke vorschlägt (wenn er als Blockvorschlagsteller ausgewählt wird), während dieser Epoche nicht für Belohnungen in Frage kommen.

Damit ein Node mit einem Rating unter dem zu überprüfenden *RatingThreshold* wieder auf die Liste der berechtigten Validierer gesetzt werden kann, muss eine spezielle unJail-Transaktion (*resetRating*) an die Metachain gesendet und validiert werden. Um einen Anreiz für die Aufnahme der *resetRating*-Transaktion zu schaffen, muss der Node eine *resetRatingFee* als Teil seiner Transaktion aufnehmen, die dem Blockvorschlagenden, der sie aufnimmt, zugesprochen wird. Die derzeitige Denkweise besteht darin, den Betrag der *resetRatingFee* so zu gestalten, dass er mindestens den durchschnittlichen Belohnungen entspricht, die ein Validierer in der letzten Epoche verdient hat. Bei Genesis wurde dies auf 0,1% des *NodePrice* konfiguriert, und es gibt keine tatsächliche Reset-Transaktion, aber durch *unJail* (wenn nur die Node bereits inhaftiert ist) kann ein Reset durchgeführt werden.

Bitte beachten Sie, dass wir einen Validator, dessen Rating unter den Schwellenwert gefallen ist, nicht kürzen. Dennoch erhalten Validatoren mit einem Rating unter einem bestimmten Schwellenwert keine weitere Belohnung und können nicht mehr als Teil von Konsensusgruppen betrachtet werden. Darüber hinaus werden sie am Ende der Epoche automatisch aus dem Rollover-Pool für die nächste Validator-Auswahl-Auktion ausgeschlossen, wenn die Mindestanzahl von Nodes pro Shard nicht erreicht wurde.

Der Anreiz für einen Validator, ein Node-Rating über den Schwellenwert zu halten, besteht darin, dass ein Versäumnis, dies zu tun, ihn die Möglichkeit kostet, Teil des Validator-Pools zu werden, und das führt dazu, dass er für mindestens 2 Epochen Belohnungen verliert. Darüber hinaus erhöht das Beibehalten eines hohen Ratings die Chancen eines Validators, in einer Konsensgruppe ausgewählt zu werden.

Die genaue Definition des statistischen Modells für das Rating wird derzeit entwickelt und ist eng mit dem Konsensus-Auswahlalgorithmus verbunden, der, wie bereits beschrieben, das Rating einer Node verwendet, um seine Wahrscheinlichkeit, ausgewählt zu werden, erhöht oder verringert.

Unter der gegenwärtigen Implementierung kann der Konsensus-Auswahlalgorithmus mit einer Verteilung modelliert werden, die auf der multivariaten zentralen hypergeometrischen Verteilung basiert. Alternative Algorithmen und ihre Implementierungen werden derzeit ebenfalls erforscht.

Eine Simulation, die auf einigen anfänglichen Annahmen und konfigurierten Werten basiert, kann hier eingesehen werden:
https://docs.google.com/spreadsheets/d/1DzeeJvLvS5H7XrH24QURyYQJ9QqyaUG5yzUDwyl5yY4/edit#gid=267148288.

2.3 Slashing (Bestrafung)

Von Validierern ergriffene Maßnahmen, wie der Betrieb anderer Clients oder modifizierte Codes des offiziellen Clients, können dem Betrieb des Netzwerks schaden und erfordern daher einige Strafmaßnahmen im Rahmen eines PoS-Systems. Die Sicherheit eines PoS-Systems wird durch Anreize in Form von Belohnung und Strafe zusammengehalten. Von Validatoren wird verlangt, das sie eGLD hinterlegen. Diesen Einsatz könnten sie aufs Spiel setzen und verlieren, wenn sie böswillig handeln. Damit wäre ihr wirtschaftlicher Wert in Gefahr ist.

Im Elrond-Netzwerk lässt sich der gesamte Prozess des Slashings durch einen Prozess von Auslösern beschreiben, die verschiedene Akteure haben können:

1. Erkennung/Entdeckung/Nachweis
2. Bericht(erstattung)
3. Überprüfung
4. Aus(wirkung)

Die Erkennung (1) erfolgt durch eine Node, die Zugriff auf den Block hat, den ein böswilliger Validierer erstellt/signiert, und der die Richtigkeit dieses Blocks überprüfen kann. Dies kann jede Node im Shard sein, an dem die böswillige Aktion durchgeführt wurde. Da alle Nodes im Shard alle erzeugten Blöcke verarbeiten, bedeutet dies, dass jeder Node in einem Shard (Validierer oder Beobachter (Observer)) die definierten schädlichen Aktionen erkennen kann. Dies ermöglicht es jedem Node, der den offiziellen Elrond-Code ausführt, die beobachteten unerwünschten Wirkungen zu erkennen und nachzuweisen, die Gültigkeit der vorgelegten Nachweise zu überprüfen und im Falle einer Validierung eines solchen Nachweises dafür belohnt wird. Die Nodes, die Fehlverhalten erkennen und Beweise dafür liefern, werden Fischer (oder Herausforderer) genannt.

Es wird einen zusätzlichen Optionsschalter für Validierer geben, um die Rolle des Fishermen (Herausforderer) zu aktivieren oder zu deaktivieren, was die Konfiguration eines gültigen privaten Schlüssels erfordert, der mit einer Wallet verbunden ist, die Gelder enthält.

Die Meldung (2) einer beobachteten böswilligen Aktion erfolgt durch eine spezielle Transaktion (es könnten 2 Transaktionen mit einem Commit-Decover-Schema erforderlich sein, um Front Running-Angriffe zu verhindern). Der übertragene Wert in einer solchen Transaktion wird nicht trivial und für die Generierung falscher Herausforderungen unerschwinglich sein. Der Grund für die Verwendung von Transaktionen als Challenges ist ein doppelter: Der Mechanismus soll Spamming verhindern und eine Belohnung sicherstellen, da die Validierung solcher Challenges einen nicht-trivialen Bandbreitenverbrauch (Datentransfers für den Beweis) und Verarbeitungszeit erfordert.

Die Struktur einer solchen Transaktion ähnelt der eines normalen intelligenten Vertragsabschlusses und wird im Folgenden näher erläutert:

- Absender – Wallet Adresse des Node-Betreibers
- **Ziel** – feste Adresse für den Slashing Protokoll Smart Contract
- Gaspreis – der Gaspreis
- Gasgrenzwert – der Gasgrenzwert
- **Wert** – fester nicht-trivialer Wert für jede Herausforderung (wird später entschieden)

- **Daten** – Parameter für die Überprüfung *SmartContract* - welche Funktion aufzurufen ist und ihre Parameter. Die aufgerufene Funktion sollte die Prüffunktion für die beobachtete böswillige Handlung sein, und die Parameter die erforderlichen Daten für die Verifikation (z.B. Headerdaten, Blockdaten, Merkle-Proofs etc.).

Der Gaspreis und die Gasgrenze sollten für den protokollarisch intelligenten Vertrag so festgelegt werden, dass der längste Weg berücksichtigt wird (komplexester Nachweis eines Szenarios).

Wie bereits erwähnt, wird der Reporter einer ungünstigen/bösartigen Situation "Fishermen" genannt - da er nach bösartigen Aktivitäten fischt, oder "Herausforderer" - da er jede ungünstige Situation, die er findet, herausfordert. Der *Fishermen* kann, wie bereits erwähnt, entweder ein Validator im Elrond-Netzwerk oder einfach ein *ObserverNode* sein.

Das bedeutet, dass der *Fishermen* keine Beteiligung an dem Netzwerk benötigt, aber dennoch eine Wallet und genügend Elrond-Token benötigt, um Herausforderungen zu stellen. Falls sich die Anfechtung anhand der vorgelegten Beweise als gültig erweist, wird der durch die Anfechtungstransaktion überwiesene Wert an den Absender zurückerstattet, zusammen mit den 50 % des geschmälerten Betrags von dem/den gefundenen böswilligen Akteur(en). Die restlichen 50% des geschmälerten Betrags werden als verbrannt betrachtet, um mögliche Angriffe abzuschrecken und Absprachen zu verhindern.

Die **Verifizierung (3)** jeder Herausforderung wird von den Metachain-Nodes durchgeführt. Die Herausforderung wird durch eine Transaktion ausgegeben, die eine Menge eGold überträgt, so dass sie innerhalb eines Shards ausgeführt und in einen Block aufgenommen wird. Die Challenge-Transaktionen werden auch im Block-Header referenziert, so dass die Verifizierung durch die Metachain durchgeführt werden kann.

Die gleiche Herausforderung kann von mehreren *Fishermen* im System zur gleichen Zeit kommen, so dass es eine Möglichkeit gibt, die gleiche Herausforderung von mehreren Reportern kommend zu identifizieren. Dies könnte anhand des Challenge-Datenfeldes erfolgen, das für jede Herausforderung einzigartig ist.

Es sollte nicht zwei verschiedene Arten von Herausforderungen geben, die im selben Block verifiziert werden können. Wenn es zwei verschiedene Arten von Herausforderungen gibt, dann sollte die schädlichste für die Rückgabe von Belohnungen in Betracht gezogen werden.

Die notarielle Beurkundung einer solchen Anfechtung hat für einen oder mehrere Validierer einen Bestrafungsseffekt (Slashing) (4) zur Folge, wenn die Anfechtung tatsächlich validiert wird, abhängig von der Art des kontradiktorischen Verfahrens, das gemeldet wurde: in einigen Fällen werden alle Unterzeichner eines ungültigen Blocks bestraft, in anderen Fällen nur der Blockhersteller oder eine Untergruppe von Validierern aus einer Konsensusgruppe. Wenn die Anfechtung nicht durch die Metachain-Node validiert wird, hat der Anfechter den durch die Anfechtungstransaktion übertragenen Wert und das zugehörige Gas zur Validierung der Anfechtung verloren.

Sobald ein Shard einen Metachain-Block bearbeitet, der eine validierte Challenge-Transaktion notariell beglaubigt hat, würde der Herausforderer den übertragenen Wert und einen Prozentsatz (Betrag noch zu entscheiden) des/der gestrichenen Einsatzes/Einsätze zurückerhalten, während ein weiterer Teil als Belohnung an die Metachain-Nodes gegeben werden könnte. Für die von der Metachain als ungültig markierten Challenges müsste der Shard nichts weiter tun, da die Kosten für die Challenge bereits übertragen wurden.

Wir definieren Fehlverhalten oder böswilliges Verhalten als die Handlungen, die kryptografisch nachgewiesen werden können:

- Doppelte Unterzeichnung eines Blocks auf gleicher Höhe
- Signieren eines Blocks mit einem nicht gültigen Zustandsübergang

Es gibt zwei weitere Ansätze, die für die Implementierungsphase und für die zukünftige Forschung übrig bleiben:

- Wir könnten in Betracht ziehen, die gekürzte Summe allmählich zu erhöhen, nachdem etwas Zeit vergangen ist und das Netzwerk reifer wird.
- Wir könnten erwägen, den gekürzten Betrag auf der Grundlage der Anzahl anderer Validierer, die gleichzeitig gekürzt wurden, zu erhöhen, so dass wir koordinierte Aktionen durch mehrere böswillige Akteure weiter erschweren.

2.4 Belohnungen für das Staken

Belohnungen mit Einsätzen, die Möglichkeit der Kürzung oder der Erhöhung/Verminderung einer Node-Bewertung sind eine Reihe von Anreizen, die Token-Inhaber und Validierer dazu ermutigen, sich das Elrond-Netzwerk zu sichern. Als Gegenleistung für die Sicherheit können die Validatoren ihren relativen Anteil an Token-Beständen im Netzwerk erhöhen.

Wir sind der Meinung, dass die Staking-Belohnungen nicht existieren um den Token-Besitzern per se eine Einnahmequelle zu bieten. Tatsächlich besteht die wirtschaftliche Begründung für das staken nicht darin, eine Belohnung ("Ertrag") zu erhalten, sondern den Validatoren klar zu versichern, dass das Staken ihren relativen Anteil (durch die Menge des eGold-Eigentums) am Netzwerk erhöht und auch zu einer erheblichen symbolischen Wertschätzung beiträgt.

In diesem Sinne ist es besser, die Inflationsrate stattdessen als eine Verdünnungsrate der Token-Inhaber zu betrachten. Daher ist das staken der beste Weg, um Ihren token und Ihr Interesse am Elrond-Netzwerk zu vergrößern.

So werden die Belohnungen in Elrond gezahlt:

Es wird einen garantierten Mindestbetrag pro Jahr geben. Der garantierte Mindestbetrag der Belohnung wird sich aus den Gebühren ergeben, während der Rest aus der Inflation resultiert. Die maximale Inflationsrate pro Jahr, wenn die Gebühren 0 betragen, ist also:

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

Wenn die kumulative Summe der Gebühren während eines Jahres höher ist als die garantierten Mindestbelohnungen, wird die Inflationsrate null und die verteilten Belohnungen sind höher als die garantierten Mindestbelohnungen. Andernfalls wird die Inflationsrate durch die Gesamtgebühren lediglich um den entsprechenden Betrag gesenkt. Mit diesem Ansatz haben wir die Voraussetzungen für den Übergang zu einem deflationären Währungssystem geschaffen.

Da die Belohnungen zu Beginn festgelegt werden, wird der Betrag, der an jeden Validator verteilt wird, proportional zu seiner Gesamtzahl von Nodes und deren Bewertung sein. Während die Bewertung eher unter der Kontrolle des Validators steht, ist die Anzahl der Nodes unter der Kontrolle der Leitung des Protokolls. Zur Entstehungszeit wird das Elrond-Netzwerk mit 2169 Nodes gebootet, die eine Metachain und 3 Shards bilden werden (dies schließt die Wartelisten der Shards ein, die jeweils 142 Knoten enthalten). Dieser Aufbau wird ausreichen, um etwa 15.000 TPS und den gewünschten Grad an Sicherheit und Dezentralisierung zu erreichen.

Wir erkennen an, dass mit der Zeit die Anzahl der Shards und Nodes möglicherweise erhöht werden muss, um die Last auf den Shards auszugleichen und mehr Infrastrukturunterstützung für einen höheren Durchsatz zu schaffen.

Wir gehen davon aus, dass, wenn die oben genannten Bedürfnisse entstehen, die zusätzlichen Belohnungen, die für einen neuen Shard mit 400 in Frage kommenden Nodes + wartenden Nodes benötigt werden, teilweise durch eine Erhöhung der Gebühren "finanziert" werden (was bereits geschieht und durch den neuen Shard weiter beschleunigt wird), so dass die Notwendigkeit einer Inflationssteigerung entfällt. Daher haben wir die Inflationsrate gedeckelt, um zu verhindern, dass der Anstieg über den festgelegten Höchstsatz pro Jahr hinausgeht. Im Idealfall sollte jeder neue Splitter aktiviert werden, wenn die Höhe der Gebühren die garantierten Mindestbelohnungen im Verhältnis 1/Nsh übersteigt, wobei Nsh die Gesamtzahl der vorhandenen Shards ist.

Bei einer Gebühr von 0,00005 eGold pro Transaktion scheint es, dass für ein TPS zwischen 5000-7000 genügend Gebühren anfallen, um einen zusätzlichen Shard ohne Auswirkung auf die Inflation zu

rechtfertigen. Für jede Anforderung von zusätzlichen 2000 TPS kann ein zusätzlicher Shard ohne Auswirkung auf die Inflation hinzugefügt werden, wobei die Belastung der Shards unter 50% gehalten wird. Obwohl weitere Tests in der realen Welt und mehr Daten erforderlich sind, wurden die Dinge zum Zeitpunkt des Verfassens dieses Artikels auf diese Weise modelliert.

Hier ist der Rechner für Validatoren, den wir für die Einführung des Elrond-Netzwerks (Genesis) verwendet haben:
https://docs.google.com/spreadsheets/d/1moHSRVAPeFyVnnx6psHmsUbTUrIBibXyopJAZ5o4zWs/edit#gid=1905747724

2.5 Berechnung und Verteilung von Belohnungen

Die Belohnungen werden am Ende der Epoche nach den folgenden Regeln verteilt: 10% der Gebühr eines Blocks gehen an den Antragsteller des Blocks, während der Rest von 90% in einen Gebührenpool, GesamtzahlDerZuVerteilendeGebühren, fließt. Weitere Informationen zu den Gebühren finden Sie in Abschnitt 3 der Gebührenordnung.

Am Ende der Epoche wird eine Berechnung durchgeführt, um festzustellen, wie viele neue Tokens geprägt werden müssen. Diese Zahl wird ermittelt, indem die GesamtzahlDerZuVerteilendenBelohnungen gemäß MaximalenInflationMöglichkeit und der Anzahl der von jedem Shard produzierten Blöcke abzüglich der von allen Shards während dieser Epoche GesamtzahlDerAkkumuliertenGebühren berechnet wird. Von der GesamtzahlDerZuVerteilendenBelohnungen werden 10% an die Protokoll-Nachhaltigkeitsadresse überwiesen. Siehe Abschnitt 4 für Einzelheiten zu diesem Fonds.

Wenn die Anzahl der Shards geändert wird, werden die Belohnungen pro Block entsprechend der neuen Shard-Zahl berechnet. Wenn die Rundenzeit geändert wird, dann werden die Belohnungen pro Block entsprechend der neuen Rundenzeit berechnet. Die Berechnung des BelohnungProBlock erfolgt am Ende der Epoche und wird von den Antragstellern des Blocks zum Block zu Beginn der Epoche hinzugefügt und von allen Validierern überprüft.

Am Ende jeder Epoche:

a. *MinGesamtzahlDerZuVerteilendenBelohnungen ist gleich der Gesamtzahl der Blöcke, die von allen Shards + Metachain produziert wurden, multipliziert mit BelohnungProBlock.*
b. Für jeden Block, der in jeder Runde in jedem Shard produziert wird, gehen 10% der Summe der Transaktionsgebühren dieses Blocks direkt an den Antragsteller dieses Blocks, aber erst nachdem 10% an die Nachhaltigkeit des Protokolls gehen.
c. Die anderen 90% aller Transaktionsgebühren aus allen Shards werden zusammengefasst und zu einem Pool, GesamtzahlDerZuVerteilendeGebühren genannt, der in der Anzahl der eGold-Token angegeben ist, addiert.
d. *GesamtzahlDerAkkumuliertenGebühren ist gleich GesamtzahlDerZuVerteilendeGebühren+ alle Gebühren, die direkt an die Antragsteller des Blocks gehen.*
    i. If *TotalAccumulatedFees* < *MinTotalRewardsToBeDistributed* then *MinTotalRewardsToBeDistributed* - *TotalAccumulatedFees* tokens are minted and added to the validator compensation pool for a total of *TotalRewardsToBeDistributed* = *MinTotalRewardsToBeDistributed*
    ii. If *TotalAccumulatedFees* > *MinTotalRewardsToBeDistributed* then no additional tokens are minted and *TotalRewardsToBeDistributed* =

MinTotalRewardsToBeDistributed + (TotalAccumulatedFees - MinTotalRewardsToBeDistributed).

iii. Vom Wert von GesamtzahlDerZuVerteilendenBelohnungen wird ein Betrag von 10% an die Nachhaltigkeit des Protokolls gehen.

iv. Die restlichen 90% der GesamtzahlDerZuVerteilendenBelohnungen werden unter allen Validierern (über alle Shards, einschließlich der Metachain-Validierer) aufgeteilt, die als Mitglieder der Konsensusgruppe fungierten

e. Aus dem GesamtzahlDerZuVerteilendenBelohnungen berechnen wir die BelohnungenProBlock und BelohnungenProBlockProNode entsprechend der Anzahl der berechtigten Validierer in dieser Epoche und der Anzahl der insgesamt in dieser Epoche produzierten Blöcke.

f. Der neue Metachain-Block, der den neuen Epochenbeginn-Block vorschlägt, verteilt die Belohnungen (Transaktionsgebühren und die geprägten Tokens, falls vorhanden) im Epochenbeginn-Metablock.

g. Der Verteilungsprozess ist ein deterministischer, alle Metachain Validierer schaffen die gleichen Belohnungen und müssen zum gleichen Ergebnis kommen:

i. Iterieren Sie die Validator-Statistikversuche und exportieren Sie die folgenden Daten für jeden öffentlichen BLS-Schlüssel: Anzahl der ausgewählten erfolgreichen Blöcke, Anzahl der Führungspositionen, kumulierte Gesamtgebühren und die Belohnungsadresse.

ii. Wenn alle öffentlichen BLS-Schlüssel iteriert werden, fügt der Prozess der Belohnungsadresse für diesen öffentlichen BLS-Schlüssel die BelohnungenProBlockProNode * NumAusgewähltImErfolgreichenBlock + GesamtzahlDerAkkumuliertenGebühren hinzu.

iii. Für jede Belohnungsadresse wird eine Belohnungstransaktion von der Metachain zu den Shards erstellt.

iv. Die Shards werden den Wert aus den Belohnungstransaktionen zu den Kontensalden hinzufügen.

2.6 Unstaking und unbonding

Unstaking

Wenn ein Validierer ein Unstake durchführen möchte, initiiert er eine Transaktion, die anzeigt, dass er eine Reihe von Nodes, einschließlich des öffentlichen BLS-Schlüssels jedes Node, unstake durchführen möchte. Die Transaktion wird vom Validierer generiert und an die Metachain gesendet.

Am Ende der Epoche, wenn die Nodes neu gemischt werden, werden diejenigen, die sich während der gerade abgeschlossenen Epoche unstaked haben, zuerst herausgemischt.

- Wenn der Node nicht herausgemischt werden kann, dann muss der Node "bleiben und arbeiten". Wenn der Node beschließt, offline zu gehen, sinkt sein Rating und irgendwann wird er unter RatingThreshold liegen, was ihn von der Teilnahme an der nächsten Auswahl oder Node-Auktion ausschließt. Ein Node unterhalb von ratingThreshold kann erst entsichert werden, wenn das Rating über ratingThreshold liegt (siehe Transaktion resetRating).
- Wenn es auf einem Shard mehr unstaking Nodes gibt als die Anzahl der Nodes in der Warteliste, berechnet die Metachain eine Reihenfolge für das Herausmischen und nur die ersten wartenden Nodes aus der Liste werden entfernt.

Wenn ein Validator ein unstaking einleitet und dann in derselben Epoche beschließt, nicht fortzufahren, kann er eine Transaktion zur erneuten re-stake senden, und seine unstaking wird annulliert.

Die unstaking Informationen werden im Validator staking smart contract gespeichert. Das re-stake ist dasselbe wie das Einreichen eines stake, der einzige Unterschied besteht darin, dass er den Wert nicht erneut senden muss.

Unbonding
Die unbond Frist ist auf 10 Tage festgelegt, nach deren Ablauf der Node seine zuvor gestapelten Gelder zurückerhalten kann.

Während der Zeit der unbonding:

- Wenn der Node böswillige Aktivitäten ausführt, ist er immer noch schrägstrichfähig. Dazu können Angriffe wie (siehe Abschnitt Slashing) gehören:
    - Angriffe aus großer Entfernung
    - Nichtausführung der erforderlichen Validierungsaktivitäten

- Es ist möglich, dass die Auflösungsphase eines Nodes niemals endet, wenn alle Nodes des Systems ausgefallen sind und es nicht genügend Nodes gibt, um einen Shard zu betreiben. Dies ist jedoch praktisch nicht möglich, da Elrond Nodes für mindestens die Metachain und einen Shard zum Mindestpreis der Node-Reserve bereitstellen wird. Auf diese Weise gewährleisten wir einen ausfallsicheren Mechanismus, bei dem Elrond der Nodebetreiber der letzten Instanz ist.

Am Ende der unbond Periode sendet der Validator eine Transaktion, in der er das unstaked Geld für jeden der Node anfordert, die er unstaken möchte.

Die Anforderung zur unBond wird von den Metachain Nodes nur dann verarbeitet, wenn das unbond für jeden einzelnen Node abgeschlossen ist. Wenn die unbond Periode nicht abgeschlossen ist, wird das gesamte Gas verbraucht.

2.7 Delegieren

Da nicht jeder ein Validierer sein und einen Node betreiben kann, können diejenigen, die sich noch beteiligen wollen, ihre Beteiligung an andere Validierer oder an die Beteiligung als Dienstleister delegieren und die Belohnungen unter ihnen aufteilen.

In der Bootstrapping-Phase von Elrond Network wird Elrond als Unternehmen eine Reihe von Nodes betreiben. Die Mitglieder der Gemeinschaft werden in den ersten Monaten ihre Anteile als Dienstleister an Elrond delegieren können. Darüber hinaus verfügt Elrond über eine Reihe von Partnern, die professionelle Dienstleistungen für den Betrieb großer Infrastrukturen anbieten werden; diese Partner sowie Elrond werden zu Beginn ein smart contract für die Delegation benötigen.

Die allgemeine Anforderung an einen solchen contract besteht darin, die von den Validatoren generierten Belohnungen an die Gemeindemitglieder zu verteilen, die ihre Token durch den contract gestakt haben. Bei der Verteilung muss darauf geachtet werden, wann die Belohnungen an die registrierten Mitglieder ausgegeben werden und wie hoch die Dienstleistungsgebühr ist.

Weitere Informationen über Delegieren im Allgemeinen, Delegieren bei der Entstehung und die smart contract für Delegieren, die von Elrond als Leitfaden zur Verfügung gestellt wird, werden später in einem anderen Papier oder einem anderen Medium bekannt gegeben.

3. Gebühren

Ein nachhaltiger Wertstrom für das Netzwerk kann sich aus Transaktionsgebühren und der Inflation von Vermögenswerten ergeben. Da sich der Erfolg des Netzwerks in der Annahme und Nutzung widerspiegelt, die Transaktionsgebühren erzeugen wird, wird das Wirtschaftsmodell in der Lage sein, das Wachstum und die Aufrechterhaltung des Netzwerks ohne die Notwendigkeit einer Inflation zu finanzieren.

Die Berechnung und Verteilung der Belohnungen und Gebühren erfolgt am Ende der Epoche und wird von den Antragstellern des Blocks zum Beginn der Epoche hinzugefügt und von allen Validierern überprüft.

Für alle Blöcke, die in jeder Runde von jedem Shard produziert werden, gehen 10% der Blocktransaktionsgebühren direkt an den Blockanbieter. Die restlichen 90% aller Transaktionsgebühren eines Blocks werden in einem Pool addiert und am Ende der Epoche an alle Validierer verteilt. Allein der Blockanmelder erhält 10% der Gebühren des aktuellen Blocks.

Nach Prüfung der ersten Simulationen haben wir beschlossen, dass die Transaktionsgebühren mit 0,00005 eGold pro Transaktion beginnen werden.

3.1 Transaktions- und smart contract Gebühren

Transaktionsgebühren werden wie folgt berechnet:

1. Wertübertragungstransaktionen:

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

2. 2. Smart contract Transaktionen

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

Der entsprechende Blockanbieter wird sie während des Konsensprozesses direkt berechnen.

Die Transaktionsgebühren werden mit Hilfe eines Gasmodells berechnet. Dabei wird Folgendes berücksichtigt: die Menge der pro Transaktion verwendeten Ressourcen, einschließlich:

i. CPU
ii. Bandbreite
iii. Lagerung

Diese Liste enthält 584 Betriebe und die dazugehörige Gasmenge, die bei Genesis eingesetzt werden (Änderungen in der Zukunft vorbehalten). Die 584 Arbeitsgänge sind ausschließlich Gas. Die Bezeichnung kommt von GasPrice. Es gibt einen Mindest-Gaspreis im System, unter dem die Transaktionen nicht

ausgeführt werden. Der GasPrice kann vom Benutzer festgelegt werden. Die tatsächliche Gebühr der Transaktion wird über gasPrice * gasLimit berechnet. Der gasPrice enthält die tatsächliche Stückelung, die derzeit 10e-18 eGold beträgt. Die Gebühr wird über den consumendGas * gasPrice berechnet.

Für jeden Block in jedem Shard werden die im Block enthaltenen Transaktionsgebühren aggregiert (siehe Abschnitt Belohnungen für das staken). Bis zum Ende der Epoche (zu diesem Zeitpunkt werden die gepoolten Transaktionsgebühren an die entsprechenden Agenten verteilt) werden die Transaktionsgebühren von keinem Agenten kontrolliert und als Information im metaBlock-Header gespeichert, auf den die Nodes in jedem Shard nicht zugreifen können.

Jede Transaktion muss die benötigte Gasmenge als Teil der Transaktionsdaten angeben. Während ein Blockproduzent einen Block erstellt, führt er jede Transaktion aus, wobei das verbrauchte Gas abgezogen und das verbleibende Gas zurückerstattet wird. Wenn eine Transaktion genügend Gas für die Ausführung, aber nicht genügend Mittel für den tatsächlichen Transfer angibt, dann verbraucht die Ausführung das gegebene Gas, aber die Move-Saldo-Funktion (oder intelligenter Vertragsaufruf) verursacht keine Saldoänderung aufgrund von unzureichendem Saldo (das Konto nonce wird erhöht und die Transaktion wird der Blockchain als ungültige Transaktion hinzugefügt).

Für jede Transaktion kann dieser Betrag durch eine Überschätzung (jedoch nicht mehr als das 10-fache) des erwarteten Gasverbrauchs berechnet werden, da der nicht verbrauchte Betrag an den Zahler zurückgegeben wird, nachdem alle Transaktionen abgeschlossen sind. Wenn eine Transaktion nicht genügend Gas zur Ausführung einer erforderlichen Funktion enthält, wird die Transaktion vorzeitig abgebrochen und fehlschlagen, aber dennoch verbrauchtes Gas in Rechnung gestellt.

Für jede Transaktion, die weniger GasLimit spezifiziert, wie in Abschnitt 3.1, Formel 1, angegeben, wird das System diese Transaktion zurückweisen und die Transaktion nicht notariell beglaubigen (auch nicht als gescheiterte Transaktion).

Künftige Arbeiten werden die Möglichkeit untersuchen, die Entgelte auf der Grundlage der Auslastung des gesamten Netzes anzupassen, so dass wir beispielsweise, solange die Auslastung unter 50 % liegt, einen Mindestpreis pro Gas haben, aber wenn die Auslastung über 50 % geht, steigt der Gaspreis. Um eine Manipulation des Gaspreises durch das Halten von Transaktionen zu vermeiden, wird für jede Transaktion eine Verfallszeit festgelegt. Anschließend könnte am Ende jeder Epoche eine Reorganisation der Shards ausgelöst werden, so dass smart contracts und dApps auf andere Shards verschoben werden, um die Last pro Shard wieder auszugleichen und auf unter 50% zurückzuführen.

3.2 Lagergebühren

Die Lagerung sollte getrennt von der Berechnung oder der Bandbreite betrachtet werden, da für jede smart contract Transaktion, die künftig die Lagerung über alle Validierer hinweg erfordert, nicht nur eine einmalige Gebühr bei der Ausführung der Transaktion, sondern auch Lagerungskosten anfallen.

Elrond wird eine staatliche Miete für smart contract Transaktionen einführen, bei der es für jedes zu lagerndes Byte einen Festpreis gibt (in Zukunft kann dieser Festpreis über die Governance angepasst werden), der periodisch gezahlt wird. Der staatliche Mietpreis wird nur für smart contracts und nicht für normale Bilanzkonten angewandt. Wir werden auch einen Mechanismus einführen, um den Zustand eines Kontos (das nicht in der Lage ist, die Miete zu zahlen) vorübergehend zu bereinigen, das Konto in den Winterschlaf zu versetzen und es bei Bedarf wiederherzustellen.

3.3 Developers fees and monetization

Um die Akzeptanz bei den Entwicklern erheblich zu beschleunigen, werden wir ihnen eine integrierte Protokoll-Monetarisierungslösung zur Verfügung stellen. So gehen 30% der Gebühren, die direkt mit einer dApp verbunden sind, an den Entwickler. Bei der Verarbeitung eines smart contract werden also 30% der Gebühren aus dieser Transaktion dem Saldo des smart contract hinzugefügt.

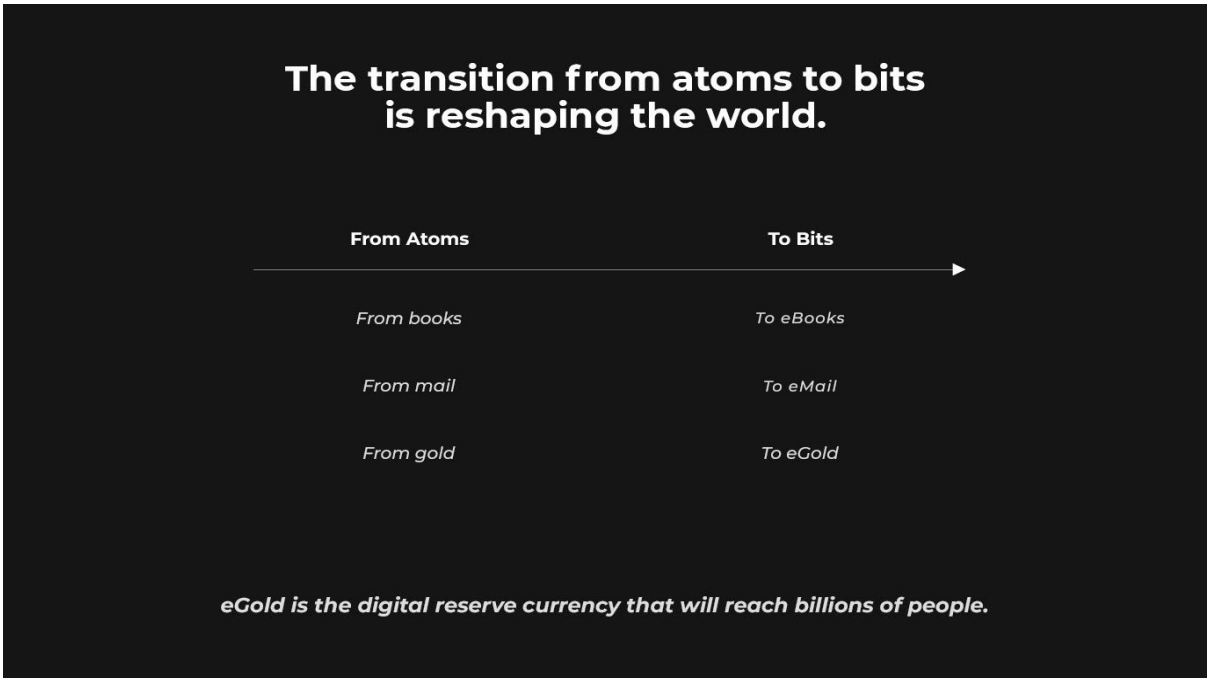
4. eGold

Der systemeigene Elrond-eGold- Token eröffnet eine neue Wachstumsphase für die Elrond-Wirtschaft. Es ist ein natürlicher Schritt zur Ermöglichung systemeigener Elrond-Dienstleistungen wie Absteckung und Delegation sowie DeFi-Optionen.

4.1 Überblick

Hier finden Sie einen Überblick über die wichtigsten eGold-Grundlagen:

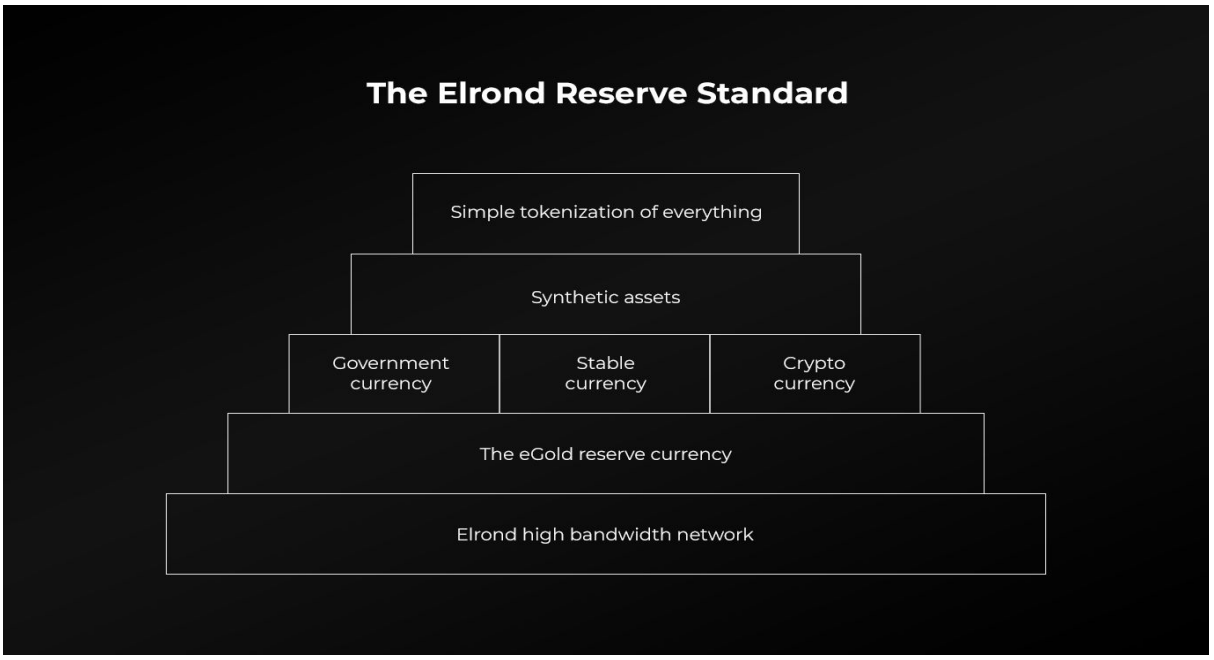
a) **Die Währung eGold ist auf Einfachheit und weltweite Einführung ausgelegt**
Komplexität ist das wichtigste Hindernis für die Einführung in der realen Welt - versuchen Sie, Bitcoin oder Ethereum normalen Menschen zu erklären, und Sie sehen sofort, was wir meinen. Um die nächste Milliarde Menschen zu erreichen, haben wir die Elrond-Währung völlig neu überdacht und ihre Essenz in eine universell ansprechende und kraftvolle Metapher gefasst.



b) **Die eGold-Währung ist als digitaler Reservestandard und robuster Wertespeicher konzipiert**
Es wurde ein neues Wirtschaftsmodell definiert, um eGold als Kernnetzwerk-Token zu positionieren, das für den gesamten internen Gebrauch von Elrond grundlegend ist. Dieses Token ist so konzipiert, dass es Parameter optimiert, die sich zur Schaffung eines robusten Wertespeichers eignen, ähnlich wie Gold, aber mit einer Mechanik und Funktionalität, die weit über die von Gold hinausgeht.

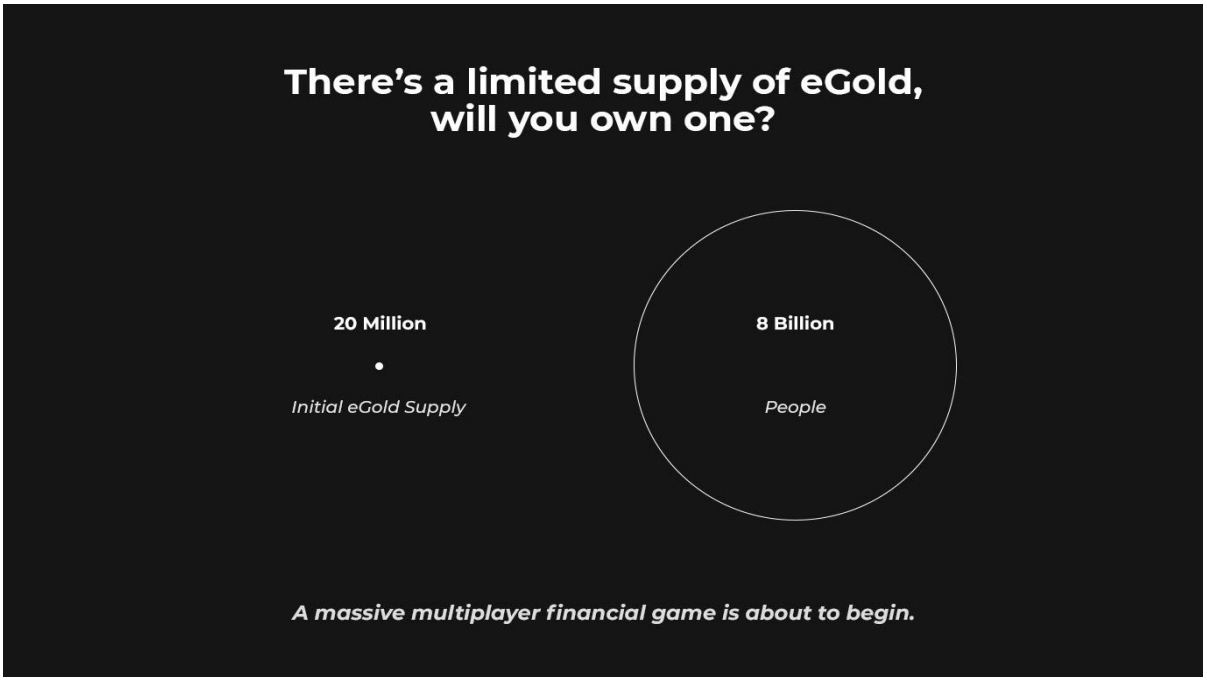
Indem wir einen neuen Satz von Tickern mit einem e als Präfix ermöglichen, wie z.B. eGLD, machen wir die Dinge einfach und intuitiv verständlich, aber vielleicht noch besser, ermöglichen wir einen flexiblen und kohärenten Ableitungspfad auf der Grundlage des E-Präfix, der mit der Auflistung einer unbegrenzten Anzahl neuer Währungen zusätzlich zur eGold-Reserve kompatibel ist.

Eingebettet in diesen Entwurf ist die Prämisse, dass Elrond sowohl mit lokalen Regierungswährungen als auch mit anderen Krypto-Währungen kompatibel ist, die schließlich in der Lage sein werden, Elronds Netzwerk mit hoher Bandbreite zu nutzen, um ihren lokalen Gemeinschaften einen globalen Werttransfer anzubieten. Tatsächlich beabsichtigen wir, viele neue Token, wie stable coins, synthetische Vermögenswerte und lokale Fiat-Währungen, an Bord zu nehmen.



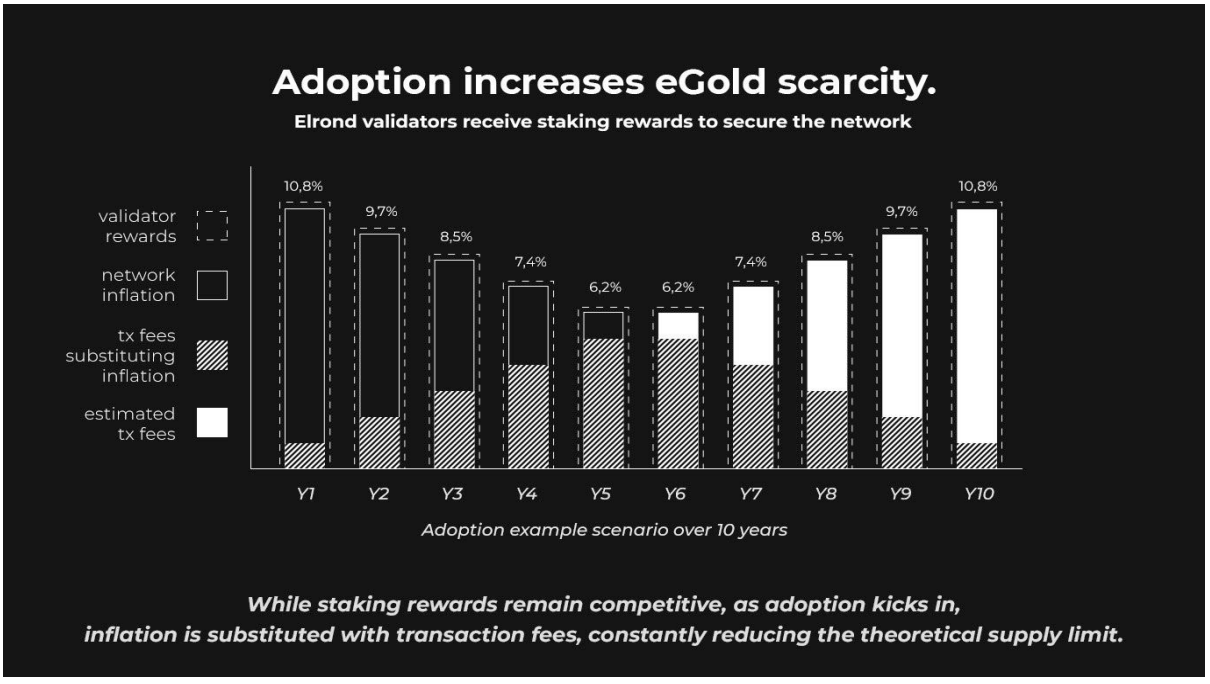
c) Eingebaute Knappheit zur Stärkung von Wert und Nachfrage

Bei Genesis gibt es nur 20 Mil anfänglich eGold im Vergleich zu 8 Bil Personen. Dies bedeutet, dass es ein sehr begrenztes Angebot von nur 0,0025 eGold pro Person gibt. Dies setzt ein Wettrüsten um die Akkumulation in Gang, da der Besitz von ein paar tausend eGold jetzt dem Besitz von ein paar tausend Bitcoin im Jahr 2010 gleichkommen könnte.



d) Starke staking Anreize für die Annahme von Validatoren, gepaart mit einer maximalen supply

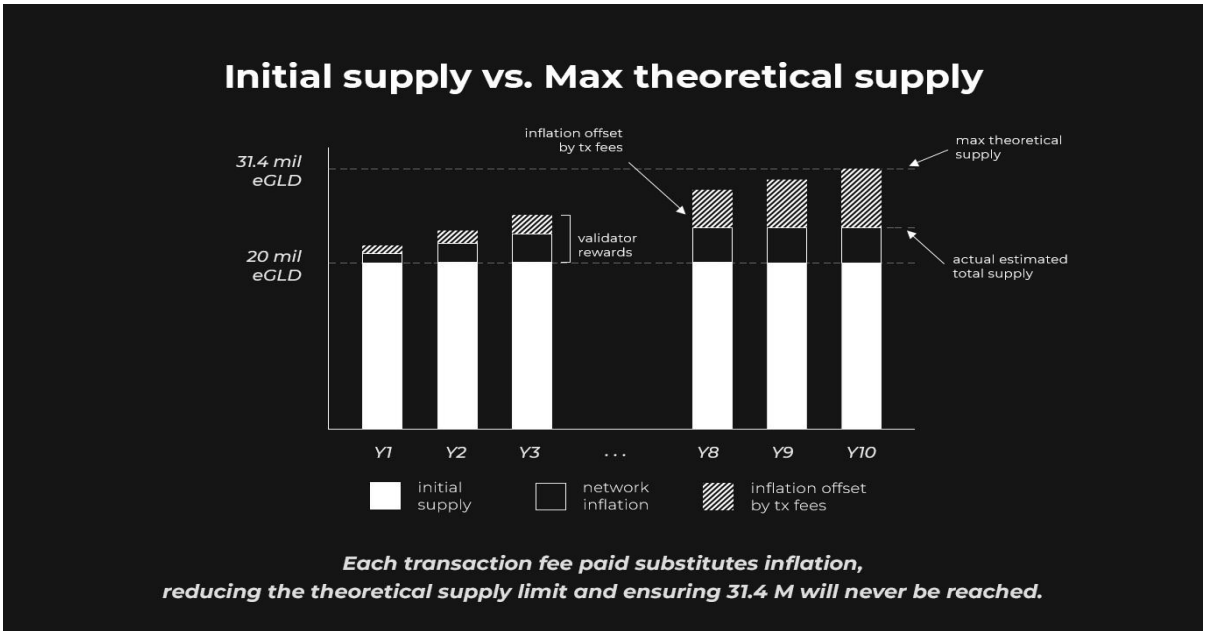
Es gibt starke staking Anreize für Validierer, das Elrond-Netz zu sichern. Zunächst werden diese Anreize durch jährlich neu herausgegebene Angebote geschaffen, aber sobald die Adoption einsetzt, wird die Inflation durch Transaktionsgebühren ersetzt, um die Belohnungen für das staking zu decken. Im Gegensatz zu den meisten anderen Blockchain Netzwerken, bei denen die Neuausgabe unbegrenzt und ohne Deckelung erfolgt, ist diese Summe bei Elrond auf eine theoretische supply von 31.415.926 eGold begrenzt, die über 10 Jahre erreicht werden kann.



e) Adoption reduziert diese theoretische Inflation und erhöht die Knappheit

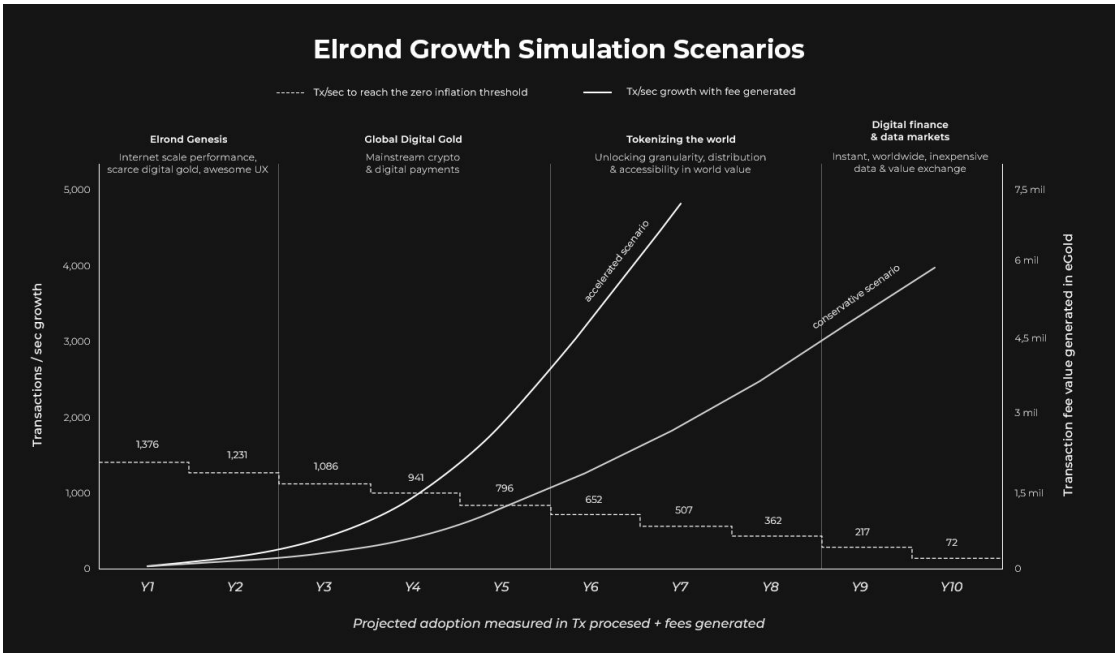
Eines der mächtigsten Merkmale des Elrond-Wirtschaftsmodells besteht darin, dass jede bezahlte Transaktionsgebühr die theoretische Grenze reduziert, indem die Inflation durch Gebühren ersetzt wird,

wodurch eGold knapper wird und sichergestellt wird, dass die maximale Liefergrenze von 31,4 Millionen niemals erreicht wird.



f) Ein nachhaltiges Adoptionsmodell, das die gesamte eGold-Wirtschaft wachsen lässt und die Deflation verstärkt

Elrond bietet wohl eines der stärksten Adoptionsmodelle im Blockchainraum, da das Netzwerk in der Lage ist, über jedes Adoptionsszenario sofort in ein vollständig deflationäres Modell überzugehen. Die im Bild unten sichtbare Nullinflationsschwelle zeigt in der Tat, dass Elrond, da weniger als 10% der Netzwerkkapazität benötigt werden, um die Schwelle zu überschreiten, bei ausreichender Adoption diese Schwelle überschreiten und einen erheblichen Wert für alle Netzwerkteilnehmer schaffen kann.



4.2 Eigenschaften von Geld und eGold

Es gibt zwei Arten von Währungen, die in letzter Zeit auf der ganzen Welt verwendet werden: repräsentative Währungen, bei denen jede Münze oder Banknote direkt gegen eine bestimmte Menge einer Ware eingetauscht werden kann, und Fiat-Währungen, die von einer Regierung ausgegeben werden und die nicht durch eine Ware gedeckt sind, sondern durch den gemeinsamen Glauben zwischen Einzelpersonen und Regierungen funktionieren, dass die Währung weiterhin akzeptiert und als Tausch- oder Zahlungsmittel verwendet wird.

Jede Währung auf der ganzen Welt wird als Wertaufbewahrungsmittel gezählt, wenn sie ihren relativen Wert im Laufe der Zeit verlässlich und ohne Abwertung beibehalten kann. Eine robuste Währung ist nicht nur ein gutes Wertaufbewahrungsmittel, sondern muss auch bestimmte Eigenschaften in Bezug auf Nützlichkeit, Knappheit, Teilbarkeit, Transportfähigkeit, Haltbarkeit und Fälschbarkeit erfüllen.

eGold ist eine neue Art digitaler Währung mit einzigartigen Eigenschaften, die sich zur Schaffung eines robusten digitalen Wertespeichers eignen..

Money properties	Gold (Resource)	Fiat (US Dollars)	eGold (Elrond)
Fungibility (Interchangeable)	High	High	Very High
Portability	Medium	High	Very High
Durability	High	Medium	Very High
Divisibility	Low	Medium	Very High
Security (Cannot be counterfeited)	Medium	Medium	High
Scarcity (Predictable Supply)	Medium	Low	Very High
Non-Sovereignity (State independence)	High	Low	Very High
Censorship Resistance	Medium	Low	Very High
Programmability *(Smart)*	Low	Low	Very High

a) Dienstprogramm

Eine Währung muss einen Nutzen haben, um effektiv zu sein. Einzelpersonen müssen in der Lage sein, Einheiten der Währung zuverlässig gegen Waren und Dienstleistungen zu tauschen. Dies ist einer der Hauptgründe, warum sich Währungen überhaupt erst entwickelt haben: damit die Teilnehmer eines Marktes vermeiden konnten, direkt mit Waren handeln zu müssen. Nützlichkeit erfordert auch, dass Währungen leicht von einem Ort zum anderen bewegt werden können. Belastende Edelmetalle und Waren erfüllen diese Bedingung nicht ohne weiteres.

Der vielleicht größte Vorteil der eGold-Währung ist, dass es sich um den nativen Token handelt, der eine der fortschrittlichsten Blockchain-Architekturen antreibt, die beim Start mehr als 15.000 Transaktionen pro Sekunde verarbeitet, mit einer Kapazität, die Hunderttausende pro Sekunde übersteigen kann. Da

eGold digital ist, ist es ein überlegenes Mittel zum Austausch und zur Übertragung von Werten, das sich für schnelle, weltweite und kosteneffektive Geldtransfers eignet.

b) Knappheit

Der Schlüssel für die Werterhaltung einer Währung ist ihre Bereitstellung. Eine zu große Geldmenge könnte die Preise für Güter in die Höhe schnellen lassen und zu einem wirtschaftlichen Zusammenbruch führen.

In Elrond beginnt das Angebot bei 20.000.000 und weist einen vorhersehbaren vorübergehenden Anstieg des Angebots auf, um die Netzsicherheit durch Belohnungen beim staken zu erhöhen. Die definierte Maximalversorgung darf 31.415.926 über einen Zeitraum von 10 Jahren nicht überschreiten. Diese theoretische Obergrenze wird jedoch mit jeder abgewickelten Transaktion und den anfallenden Gebühren tatsächlich sinken. Je stärker die Akzeptanz, desto kleiner wird also das eGold-Angebot werden.

c) **Teilbarkeit**

Erfolgreiche Währungen sind in kleinere inkrementelle Einheiten teilbar. Damit ein einheitliches Währungssystem als Tauschmittel für alle Arten von Gütern und Werten innerhalb einer Volkswirtschaft funktionieren kann, muss es über die mit dieser Teilbarkeit verbundene Flexibilität verfügen. Die Währung muss ausreichend teilbar sein, so dass sie den Wert jeder Ware oder Dienstleistung, die in der gesamten Wirtschaft zur Verfügung steht, genau widerspiegelt.

Elrond hat ein viel größeres Maß an Teilbarkeit als die meisten Fiat-Währungen auf der ganzen Welt. Ein eGold ist durch 18 Dezimalstellen teilbar. Wenn der Elrond im Laufe der Zeit weiter im Preis steigt, sorgt die große Teilbarkeit des Elrond dafür, dass die Menschen mit winzigen Bruchteilen eines einzigen Elrond immer noch an den alltäglichen Transaktionen teilnehmen können.

d) Transportfähigkeit

Währungen müssen leicht zwischen den Teilnehmern einer Volkswirtschaft transferiert werden können, um nützlich zu sein. In Fiat-Währungen ausgedrückt bedeutet dies, dass Währungseinheiten sowohl innerhalb der Wirtschaft eines bestimmten Landes als auch zwischen Nationen durch Tausch transferierbar sein müssen.

Im Gegensatz zu Fiat-Währungen, bei denen der Prozess der Geldüberweisung Tage dauern kann und mit erheblichen Gebühren verbunden ist, kann eGold, solange es Internet gibt, überall auf der Welt, in einem Augenblick und zu 100x geringeren Kosten als die derzeit verfügbaren Optionen überwiesen werden. Da eGold an den größten Börsen notiert ist, kann es leicht in fast jede Währung umgetauscht werden.

e) Haltbarkeit

Die Haltbarkeit ist ein wichtiges Thema für Fiat-Währungen in ihrer physischen Form. Ein Dollarschein ist zwar stabil, kann aber dennoch zerrissen, verbrannt oder anderweitig unbrauchbar gemacht werden.

So wie eine Währung dauerhaft sein muss, muss sie auch schwer zu fälschen sein, um wirksam zu bleiben. Andernfalls könnten böswillige Parteien das Währungssystem leicht stören, indem sie es mit gefälschten Scheinen überfluten und dadurch den Wert der Währung negativ beeinflussen.

Digitale Zahlungsformen sind nicht in gleicher Weise anfällig für diese physischen Schäden. Aus diesem Grund hat eGold einen enormen Wert. Es kann nicht auf die gleiche Weise zerstört werden wie eine Dollarnote, obwohl es verloren gehen kann. Wenn ein Benutzer seinen oder ihren kryptographischen Schlüssel verliert, kann das eGold in der entsprechenden Brieftasche (Wallet) effektiv dauerhaft unbrauchbar sein. Das eGold selbst wird jedoch nicht vernichtet und bleibt in den Aufzeichnungen auf der Blockchain weiter bestehen.

f) Fälschungssicherheit

Dank der robusten eingebauten Sicherheit seines dezentralisierten Blockchain-Systems ist eGold unglaublich schwer zu manipulieren. Dies zu tun, würde im Wesentlichen die Veruntreuung eines nicht trivialen Teils der Netzwerkteilnehmer erfordern und würde immer größere und unerschwinglichere Kosten verursachen. Der einzige Weg, wie man ein gefälschtes eGold herstellen könnte, wäre die Durchführung eines so genannten Double Spend-Angriffs.

Dies bezieht sich auf eine Situation, in der ein Benutzer dasselbe eGold in zwei oder mehr getrennten Einstellungen "ausgibt" oder überträgt und damit effektiv einen doppelten Datensatz erstellt. Während dies bei einem Fiat-Währungsschein kein Problem darstellt - es ist unmöglich, den gleichen Dollarschein in zwei oder mehr getrennten Transaktionen auszugeben - ist dies bei digitalen Währungen theoretisch möglich. Was eine doppelte Ausgabe in Elrond unwahrscheinlich macht, sind die steigenden und unerschwinglichen Kosten der Ressourcen, die zu ihrer Durchführung benötigt werden.
Unten sehen Sie eine Momentaufnahme des eGold-Versorgungsmodells:

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. Nachhaltigkeit des Protokolls

Die Nachhaltigkeitsadresse des Protokolls wird 10% der insgesamt generierten Belohnungen erhalten, um die notwendigen Ressourcen und Mittel für die weitere Entwicklung, Aufrechterhaltung und Förderung des Elrond-Protokolls bereitzustellen.

Zukünftige Arbeit

Eine vielversprechende Richtung für die künftige Arbeit wird die Verwendung eines algorithmischen stabilen Tokens für Gebühren und die Verwendung des Einsatzes als Sicherheit für die Ausgabe des stabilen Tokens untersuchen.

Indem wir einen neuen Satz von Tickern mit einem e als Präfix ermöglichen, wie z.B. eGLD, machen wir die Dinge einfach und intuitiv verständlich, aber vielleicht noch besser, ermöglichen wir einen flexiblen und schlüssigen Ableitungspfad auf der Grundlage des E-Präfix, der mit der Auflistung einer unbegrenzten Anzahl neuer Währungen auf dem Elrond-Netzwerk kompatibel ist.

Darüber hinaus könnte eGold, abgesehen davon, dass es in Staking und Delegation eingebunden ist, auch zur Stabilisierung des Wertes der von Elrond stabilisierten Vermögenswerte verwendet werden und so zu einer Reservekomponente werden. Die Reserve könnte aus einem Sammelbecken von Kryptowährungen bestehen, das dem Protokoll hilft, den Nachschub an künftigen stabilen Elrond-Vermögenswerten zu reduzieren.

Dieses Dokument ist der erste öffentliche Entwurf des Elrond-Wirtschaftsmodells. Die Personen und Unternehmen, die zu diesem Dokument beitragen, arbeiten in einem dynamischen Umfeld, in dem ständig neue Ideen und Risikofaktoren entstehen. Daher sind wir ständig auf der Suche nach Feedback mit neuen Annahmen, die Teile unseres Modells in Frage stellen und verbessern könnten. Wir ermutigen diejenigen, die einen Beitrag leisten möchten, ihr Feedback zum Elrond zu geben.

Konstanten und Formeln

Name	Wert	Formel/Weitere Informationen
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	*Shard 0 will be assigned to take 1 additional node*
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 for shard and 0.303030 for meta	*(5)*
blockProposerRatingNegativePct	TBC	*(6)*
importanceRatingRatio	1	*(3)*

startRating	50.00001	
maxRating	100	
ratingThreshold	10	
HoursToMaxRatingFromStartRating	72h for shards and 55h for metachain	
resetRating	50.00001	
resetRatingFee		*0.1% of the nodePrice*

Anhang

- Elrond Network Whitepaper
- Zeitplan für die Veröffentlichung von eGold Token
- Staking-Rechner
- Gas-Kosten für den Betrieb
- Peer-Rating für Elrond-Validatoren

Referenzen

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*