

# Descentralogía

## La Ciencia de la Descentralización

Por Miguel Klagges

### ABSTRACTO

Este estudio presenta una novedosa metodología para cuantificar y comparar el grado de descentralización en redes distribuidas, empleando un **Índice Global de Descentralización (IGD)**. Este índice se construye a partir de una serie de métricas basadas en principios matemáticos de la teoría de la información y análisis de redes, incluyendo la entropía de Shannon, la ley de Zipf y la ley de Benford, entre otras. Utilizando estos modelos, he desarrollado una fórmula que combina diversos factores fundamentales para evaluar la descentralización de una red, tales como la distribución de nodos, la diversidad geográfica, y la estructura de consenso.

Para ejemplificar la aplicación del IGD, este trabajo analiza dos de las principales redes blockchain: Bitcoin y Ethereum. Los resultados sugieren que Bitcoin mantiene un mayor grado de descentralización en su estructura de nodos y modelo de consenso, en comparación con Ethereum, cuya transición a proof of stake muestra ciertos desafíos de concentración en los pools de validación. Este índice cuantitativo de descentralización, propuesto como "Escala D", podría servir como una herramienta objetiva para evaluar y comparar el grado de descentralización de distintas redes distribuidas en un marco teórico.

INTRODUCCIÓN.....	7
Definición de Descentralogía.....	9
<b>Infraestructura y Seguridad de la Red.....</b>	<b>10</b>
Nodos.....	10
Componentes:.....	10
Entropía de Shannon.....	11
Análisis de Componentes Conectados.....	11
Ejemplo de Evaluación de Nodos.....	12
Postulado matemático del factor Nodos.....	13
1. Entropía de Shannon.....	13
Fórmula Matemática.....	13
Datos a Recolectar.....	13
Método de recolección de datos.....	13
Fórmula de normalización.....	14
2. Análisis de Componentes Conectados.....	14
Fórmula Matemática.....	15
Datos a Recolectar.....	15
Método de de recolección de datos.....	15
Fórmula de normalización.....	16
Fórmula combinada de resultados para el factor Nodos.....	16
Modelo de Consenso.....	17
Componentes:.....	17
Entropía de Shannon.....	18
Ley de Zipf.....	18
Distribución Normal vs. Anómala.....	19
Ejemplo de Evaluación del Modelo de Consenso.....	19
Postulado matemático del factor Modelo de Consenso.....	20
1. Entropía de Shannon.....	20
Fórmula Matemática.....	20
Datos a Recolectar.....	20
Método de de recolección de datos.....	20
Fórmula de normalización.....	21
2. Ley de Zipf.....	21
Fórmula Matemática.....	21
Datos a Recolectar	
Fórmula de normalización.....	23
3. Distribución Normal vs Anómala.....	23
Fórmula Matemática.....	23
Datos a Recolectar.....	23
Método de de recolección de datos.....	23
Fórmula de normalización.....	24
Fórmula combinada de resultados para el factor Modelo de Consenso.....	24
Infraestructura.....	24

Componentes.....	25
Redundancia de Información.....	25
Entropía de Shannon.....	26
Análisis de Componentes Conectados.....	26
Ejemplo de Evaluación del Factor Infraestructura.....	27
Cientes.....	27
Componentes.....	28
Entropía de Shannon.....	28
Redundancia de Información.....	28
Ejemplo de Evaluación del Factor Clientes.....	29
<b>Gobernanza y Desarrollo.....</b>	<b>30</b>
Gobernanza.....	30
Componentes.....	30
Ley de Zipf.....	31
Entropía de Shannon.....	31
Análisis de Componentes Conectados.....	32
Ejemplo de Evaluación del Factor Gobernanza.....	32
Desarrollo.....	33
Componentes.....	33
Índice de Gini.....	34
Ley de Zipf.....	34
Entropía de Shannon.....	35
Ejemplo de Evaluación del Factor Desarrollo.....	35
Escalabilidad.....	36
Componentes.....	36
Análisis de Componentes Conectados.....	37
Entropía de Shannon.....	37
Redundancia de Información.....	37
Ejemplo de Evaluación del Factor Escalabilidad.....	38
Interoperabilidad.....	38
Componentes.....	39
Análisis de Componentes Conectados.....	39
Entropía de Shannon.....	40
Redundancia de Información.....	40
Ejemplo de evaluación del factor Interoperabilidad.....	41
<b>Economía y Transacciones.....</b>	<b>42</b>
Economía.....	42
Componentes:	43
Ley de Zipf.....	43
Índice de Gini.....	43
Entropía de Shannon.....	44
Ejemplo de Evaluación del Factor Economía.....	44
Transacciones.....	45
Componentes.....	45

Ley de Benford.....	46
Entropía de Shannon.....	46
Distribución Normal vs. Anómala.....	46
Ejemplo de evaluación del factor Transacciones.....	47
Inmutabilidad.....	48
Componentes.....	48
Distribución Normal vs. Anómala.....	49
Entropía de Shannon.....	49
Redundancia de Información.....	49
Ejemplo de Evaluación del Factor Inmutabilidad.....	50
Privacidad.....	51
Componentes.....	51
Entropía de Shannon.....	52
Redundancia de Información.....	52
Análisis de Componentes Conectados.....	53
Ejemplo de evaluación del factor Privacidad.....	53
Emisión.....	54
Componentes.....	54
Índice de Gini.....	55
Ley de Gresham.....	55
Análisis de Consenso y Resistencia a Cambios Arbitrarios.....	55
Ejemplo de Evaluación del Factor Emisión.....	56
<b>Resistencia y Equidad.....</b>	<b>57</b>
Censura.....	57
Componentes.....	57
Entropía de Shannon.....	58
Ejemplo de evaluación del factor Censura.....	58
Equidad.....	59
Componentes.....	59
Índice de Gini.....	59
Ley de Pareto.....	60
Análisis de Cohortes.....	60
Ejemplo de evaluación del factor Equidad.....	61
<b>Adopción.....</b>	<b>62</b>
Componentes.....	62
Ley de Metcalfe.....	63
Entropía de Shannon.....	63
Ley de Zipf.....	64
Ejemplo de evaluación del factor Adopción.....	64
<b>Ley de Benford.....</b>	<b>65</b>
Como análisis integral de toda la red.....	65
Componentes.....	65
Ejemplo de evaluación usando la Ley de Benford.....	66
Cálculo del Error Cuadrático Medio (RMSE) para Benford.....	67

Resumen Final.....	68
Ponderación en el Índice Global de Descentralización.....	69
<b>Elaboración matemática de IGD de Bitcoin.....</b>	<b>70</b>
1. Nodos.....	70
Entropía de Shannon.....	70
1. Cálculo de $p_i$ y $p_i \log_2(p_i)$ .....	71
Cálculo de $H(X)$ .....	75
Normalización del Valor.....	75
Conclusión.....	75
Análisis de Componentes Conectados.....	76
Normalización del Resultado.....	76
Estrategia para Construir el Grafo.....	76
Análisis del Archivo JSON.....	77
Supuestos para la construcción del Grafo.....	78
Cálculo aproximado.....	78
Combinación de Componentes.....	79
Estimación razonable para el número de componentes totales.....	79
Normalización del resultado.....	79
Interpretación del Resultado.....	79
Fórmula para la combinación de $H_{norm}$ y $C_{norm}$ .....	80
Interpretación del Resultado.....	80
2. Modelo de Consenso.....	81
Entropía de Shannon.....	81
Paso 1: Extracción de Datos de archivo JSON generado a partir de mempool.space..	81
Paso 2: Cálculo de la Proporción $p_i$ para cada Pool.....	81
Paso 3: Aplicación de la Fórmula.....	82
Paso 4: Cálculo Completo de Entropía de Shannon.....	83
Paso 5: Normalización de Entropía de Shannon.....	83
Conclusión de análisis sobre Entropía de Shannon en Minería.....	84
Ley de Zipf.....	85
Interpretación del Resultado.....	88
Interpretación del resultado normalizado.....	90
3. Ley de Benford.....	91
Interpretación de resultados.....	92
Análisis del Hashrate Promedio por Pool vs. Ley de Benford.....	93
Interpretación de resultados.....	94
Interpretación de resultados.....	97
Valores observados Pobs basados en los datos.....	98
Cálculo del RMSE.....	98
Normalización del Error.....	99
Primera versión del IGD con los resultados hasta ahora.....	100
Resumen de factores y sus ponderaciones:.....	100
Resultado Final.....	101

Conclusión preliminar para IGD de Bitcoin.....	101
<b>Elaboración matemática de IGD de Ethereum.....</b>	<b>102</b>
3. Nodos.....	102
Entropía de Shannon.....	102
Cálculo de $H(X)$ .....	106
Normalización del Valor.....	106
Conclusión.....	107
Análisis de Componentes Conectados.....	107
Normalización del Resultado.....	108
Suposición razonable para los componentes de Ethereum:.....	108
Resumen de componentes.....	109
Normalización del resultado.....	109
Interpretación del Resultado.....	110
Fórmula para la combinación de $H_{norm}$ y $C_{norm}$ .....	110
Interpretación del Resultado.....	111
Modelo de Consenso.....	111
Entropía de Shannon.....	111
Total de bloques:.....	112
Interpretación del resultado.....	114
Datos para la normalización.....	114
Ley de Zipf.....	114
Implicaciones de la Concentración.....	117
Conclusión.....	117
3. Ley de Benford.....	118
Versión del IGD con los resultados hasta ahora para Ethereum.....	122
Resumen de factores y sus ponderaciones:.....	122
Resultado Final:.....	123
Conclusión preliminar para IGD de Ethereum:.....	123
<b>Análisis Comparativo de IGD: Bitcoin vs. Ethereum.....</b>	<b>124</b>
Valores de IGD Calculados.....	124
Conclusiones Finales.....	125
<b>Referencias Bibliográficas.....</b>	<b>126</b>

# INTRODUCCIÓN

La descentralización es un pilar fundamental en las redes blockchain, ya que su propósito es minimizar la dependencia de autoridades centrales y mejorar la resiliencia ante posibles puntos de fallo único o de control. Sin embargo, la medición objetiva de la descentralización ha sido un desafío en el ámbito académico y tecnológico. En este trabajo, propongo el Índice Global de Descentralización (IGD) como una medida cuantitativa que evalúa este grado de descentralización a partir de un análisis multifactorial.

La metodología se inspira en teorías matemáticas como la entropía de Shannon, la ley de Zipf y la ley de Benford, integradas en un modelo de evaluación que pondera aspectos clave de descentralización. Estos aspectos incluyen:

1. **Distribución de Nodos:** Analiza la dispersión geográfica de los nodos y su interconectividad, evaluando factores como la concentración por ASN y la proporción de nodos que utilizan redes de anonimato como Tor.
2. **Modelo de Consenso:** Considera la estructura de poder en los mecanismos de consenso de cada red. En Bitcoin, este análisis se centra en la distribución de hashrate entre los pools mineros, mientras que en Ethereum, basado en proof of stake, se examina la concentración de Ether en staking en los principales validadores.
3. **Patrones Numéricos:** La aplicación de la ley de Benford permite identificar posibles anomalías o patrones irregulares en los datos de la red, reforzando así el análisis de descentralización.
4. **Normalización y Comparación:** A través de la normalización de estos factores, el IGD permite comparar cuantitativamente la descentralización entre distintas redes en una escala de 0 a 1, denominada "Escala D".

Este trabajo, tomando como referencia a Bitcoin y Ethereum, muestra que Bitcoin mantiene un IGD superior, que refleja una mayor descentralización en

términos de distribución de nodos y consenso. Ethereum, a pesar de su capacidad para operar sin consumo energético elevado, presenta desafíos inherentes a su modelo de staking, donde pocos actores controlan una gran porción de Ether en staking, incrementando los riesgos de centralización.

La investigación se basa en datos reales obtenidos de fuentes como Bitnodes y Etherscan, lo que permite una evaluación precisa y comparativa. La "Escala D" propuesta en este estudio busca establecer un marco teórico y práctico para medir la descentralización en redes, abriendo el camino para futuras investigaciones y aplicaciones que permitan a la comunidad evaluar y comparar redes en función de su resistencia y confiabilidad descentralizada.

Esta investigación está aún en desarrollo, y la motivación de llevarla a cabo nace con el propósito de proponer una continuación al paper "*La Descentrología y el Bitcoin*" de Rodolfo Andragnes.

## Definición de Descentralología

Campo de estudio interdisciplinario enfocado en el análisis sistemático y profundo de la Descentralización en redes distribuidas, y su impacto en el entorno, tanto tecnológicos como naturales y sociales. Este campo explora los mecanismos, estructuras y principios que permiten la distribución de poder y control entre múltiples actores, minimizando la dependencia en entidades centralizadas y fomentando la resiliencia y autonomía en las redes.

En el contexto de las criptomonedas y redes blockchain, la descentrología aborda no solo la infraestructura técnica, como la distribución de nodos o la estructura de consenso, sino también los factores sociales y económicos que influyen en la descentralización. A través de métricas cuantitativas y métodos de análisis matemático, como la entropía de Shannon, la ley de Zipf, y la ley de Benford, la descentrología busca desarrollar un marco teórico que permita medir, comparar y evaluar el grado de descentralización en distintas redes.

Este campo de estudio pretende responder a preguntas fundamentales sobre cuán descentralizada es una red y qué características hacen que algunas redes sean más resistentes y confiables que otras. Al ofrecer una metodología estandarizada, como el Índice Global de Descentralización (IGD) y la "Escala D", la descentrología proporciona herramientas que permiten a la comunidad académica, técnica y general comprender y valorar la descentralización en función de su robustez y capacidad de resistir a la centralización.

La Descentrología, en suma, no solo es una propuesta teórica; se configura como una disciplina práctica que busca dotar de métodos y métricas claras para evaluar objetivamente la descentralización, generando un nuevo marco que impulse el desarrollo y evaluación continua de las redes distribuidas.

# Infraestructura y Seguridad de la Red

---

## Nodos

Son los elementos fundamentales que mantienen el estado de la red, asegurando que las reglas de consenso se apliquen y que las transacciones sean válidas. La **geodistribución y diversidad de los nodos** son esenciales para la descentralización, pues evitan que el control de la red se concentre en pocas ubicaciones o actores.

Si los nodos están distribuidos globalmente, es más difícil para un gobierno o actor malicioso bloquear o interferir en la red. La descentralización física también asegura que la red siga operando aunque algunas jurisdicciones intenten detenerla.

Por otro lado, los nodos completos permiten a los usuarios verificar transacciones sin necesidad de confiar en terceros. Cuanto mayor sea la proporción de nodos completos en la red, más fuerte será la descentralización.

Finalmente, es importante considerar que una red distribuida no debería depender de la infraestructura de un país o región específica. Las redes con altos niveles de distribución pueden garantizar **mayor resiliencia** ante fallos locales (como apagones o regulaciones adversas).

### Componentes:

1. **Distribución de Nodos:** Evalúa **en qué regiones** del mundo están ubicados los nodos. Cuanto más dispersos estén, menor será la posibilidad de que una entidad geográfica (como un gobierno) pueda censurarlos o manipular la red. Si los nodos se concentran en un solo país o región, aumenta la vulnerabilidad a **regulaciones locales** o **bloqueos geopolíticos**. En una red descentralizada, los nodos deben estar distribuidos globalmente.
2. **Diversidad de Nodos:** Analiza la diversidad entre **nodos completos** (que almacenan todo el historial de la blockchain) y **nodos ligeros** (SPV, Simple

Payment Verification). La descentralización es más robusta si **más usuarios operan nodos completos** en lugar de depender de nodos ligeros o centralizados. Los nodos completos **refuerzan la autonomía de los usuarios** y aseguran que la red no dependa de servicios externos para validar transacciones. Una concentración excesiva en nodos ligeros puede llevar a **dependencia de terceros** y vulnerabilidades.

Nota: Se anticipa que habrá desafíos importantes para establecer la cantidad de nodos ligeros y de nodos que no tienen conexiones entrantes, es decir, que no tienen abierto el puerto 8333.

## *Matemática aplicable: Entropía de Shannon y Análisis de Componentes Conectados*

### Entropía de Shannon

La **entropía de Shannon** mide el grado de **diversidad** en un sistema. Cuanto mayor sea la entropía, más distribuido y diverso será el sistema, lo que refleja un mayor nivel de descentralización.

Si la mayoría de los usuarios usan nodos completos, la entropía será más alta. Además, si la red depende de unos pocos nodos completos y muchos nodos ligeros, la entropía será baja, indicando centralización.

Por lo tanto, un valor alto de entropía refleja una red con **diversidad equilibrada**, mientras que un valor bajo indica que la red depende demasiado de ciertos tipos de nodos.

### Análisis de Componentes Conectados

En teoría de redes, los **componentes conectados** miden cuán bien están distribuidos los nodos entre sí. Una red con muchos componentes pequeños o desconectados es menos robusta que una red con múltiples conexiones bien distribuidas entre los nodos.

Esta métrica puede medir si los nodos están dispersos por diferentes países y continentes o si la red depende de pocos clusters regionales. En términos prácticos, evalúa si la red sigue operativa aunque algunos nodos se desconecten, lo que es clave para la resistencia a censura y fallos.

Por lo tanto, una **red bien distribuida** tendrá múltiples conexiones fuertes entre nodos en diversas regiones. Si se identifican **clusters altamente concentrados** o nodos críticos cuya caída pueda afectar la red, esto indicaría **riesgos de centralización**.

## Ejemplo de Evaluación de Nodos

Supongamos que una red tiene:

- **10,000 nodos activos** distribuidos en 50 países.
- **7,000** de estos nodos son ligeros y **3,000** son completos.
- La mayoría de los nodos completos están concentrados en **dos países** (EE.UU. y Alemania).

En este caso:

- La **entropía** sería baja porque la mayoría de los nodos son ligeros.
- El **análisis de componentes conectados** revelaría una **concentración geográfica** en pocas regiones, indicando vulnerabilidad.

El resultado del análisis sugiere que, aunque la red tiene una gran cantidad de nodos, su distribución y diversidad no garantizan un alto nivel de descentralización.

# Postulado matemático del factor *Nodos*

## 1. Entropía de Shannon

La **entropía de Shannon** mide la **diversidad y distribución** de los nodos en la red. Cuanta más variedad haya en las ubicaciones, operadores y tipos de nodos, mayor será la entropía, lo que sugiere una mayor descentralización.

### Fórmula Matemática

La entropía se calcula así:

$$H(X) = - \sum_{i=1}^n p_i \log_2(p_i)$$

- $H(X)$ : Entropía de Shannon del conjunto  $X$
- $p_i$ : Proporción del total de nodos que representa cada categoría  $i$  (por ejemplo, nodos en una región, nodos ligeros vs. completos, operadores independientes, etc.).
- $n$ : Número total de categorías consideradas.

### Datos a Recolectar

- **Distribución geográfica de nodos** (número de nodos por país o región).
- **Tipos de nodos**: nodos completos vs. ligeros.
- **Distribución por operadores**: cuántos nodos son operados por diferentes entidades (individuos, empresas, pools de minería).

### Método de recolección de datos

- **Explorador de Bitcoin**: Extraer información sobre nodos públicos (por ejemplo, usando **Bitnodes.io** o un nodo propio con herramientas RPC).

- **Agrupación de datos:** Organizar los nodos por región, tipo y operador. Calcular el porcentaje  $p_i$  correspondiente a cada categoría.

### Fórmula de normalización

Para normalizar el valor de entropía entre **0** y **1**, usamos:

$$H_{\text{norm}} = \frac{H(X)}{H_{\text{max}}}$$

Donde:

- $H_{\text{max}} = \log_2(n)$  es la entropía máxima posible si todas las categorías estuvieran distribuidas de forma uniforme.
- $H_{\text{norm}}$  será el valor final normalizado de entropía de Shannon, entre 0 (máxima concentración) y 1 (máxima diversidad).

## 2. Análisis de Componentes Conectados

Este análisis mide **cómo están conectados los nodos entre sí**, detectando posibles **puntos únicos de fallo o concentración**. En una red bien distribuida, no debería haber nodos o regiones críticas cuya desconexión afecte significativamente la conectividad general.

## Fórmula Matemática

Este análisis se basa en la **proporción de componentes conectados** (subredes aisladas):

$$C = \frac{N_{\text{componentes}}}{N_{\text{total}}}$$

*Donde:*

- $C$ : Proporción de componentes conectados respecto al total.
- $N_{\text{componentes}}$  : Número de componentes conectados (grupos de nodos interconectados).
- $N_{\text{total}}$  : Número total de nodos en la red.

## Datos a Recolectar

- **Número total de nodos activos.**
- **Conexiones entre nodos:** qué nodos están conectados entre sí.
- **Identificación de subredes:** cuántos **grupos aislados** o componentes conectados existen (puedes hacer esto usando análisis de grafos).

## Método de recolección de datos

- **Nodo Bitcoin:** Ejecutar un análisis de red usando herramientas como **Bitcoin Core** o **exploradores de nodos públicos**.
- **Análisis de grafos:** Usar un software de análisis de redes (por ejemplo, NetworkX en Python) para detectar componentes conectados y calcular  $N_{\text{componentes}}$

## Fórmula de normalización

Para normalizar esta métrica entre **0** y **1**, usamos:

$$C_{\text{norm}} = 1 - \frac{C}{n}$$

donde:

- $C$  es el número de componentes conectados.
- $n$  es el total de nodos
- **Restar el resultado de 1** invierte la métrica: valores más altos indican **mejor conexión** (mayor descentralización).

Por lo tanto, esta fórmula refleja que:

- Si  $C_{\text{norm}} = 1$ , todos los nodos están perfectamente conectados en un solo componente (mejor escenario).
- Si  $C_{\text{norm}} = 0$ , significa que cada nodo forma su propia subred (peor escenario).

## Fórmula combinada de resultados para el factor *Nodos*

Dado que ambas métricas (entropía y componentes conectados) tienen **igual ponderación**, el valor final para el **factor Nodos** será:

$$N_{\text{final}} = \frac{H_{\text{norm}} + C_{\text{norm}}}{2}$$

Este valor estará normalizado entre **0** y **1**.

## Modelo de Consenso

El **Modelo de Consenso** es el mecanismo mediante el cual los nodos participantes **acuerdan el estado de la red** y validan las transacciones o bloques. La **diversidad, rotación y distribución de poder en el consenso** son esenciales para asegurar que ninguna entidad pueda controlar unilateralmente el proceso. Un modelo descentralizado debe incluir **varios participantes independientes**, sin que el poder se concentre de forma sostenida en unos pocos actores.

Si pocos actores dominan el proceso, aumentan los riesgos de **ataques del 51%** (en PoW) o de control oligárquico (en PoS). Además, Si múltiples nodos pertenecen a un mismo grupo, la red **no es descentralizada de facto**, aunque haya muchos nodos activos. La independencia garantiza que los participantes no actúen de manera coordinada.

Por otro lado, la **competencia** y la **rotación saludable** del poder aseguran mayor descentralización y reducen la probabilidad de colusión o monopolio. Si la mayor parte de la producción de bloques está concentrada en unas pocas entidades, se compromete la descentralización, y la red se vuelve vulnerable a censura y manipulación.

### Componentes:

1. **Número de participantes:** Mide cuántas entidades participan activamente en la **minería o validación**. Cuanto más participantes haya, más difícil será para una sola entidad o grupo tomar control del consenso.
2. **Diversidad:** Evalúa qué tan independientes son los participantes entre sí. Esto implica verificar si los mineros o validadores pertenecen a diferentes grupos o si muchos están controlados por una misma entidad.
3. **Rotación de Poder:** Mide la **frecuencia con la que cambia la dominancia** de los actores claves en la validación o minería. En una red saludable, el poder debería rotar entre múltiples actores, evitando que un grupo tenga control permanente.

**4. Distribución equitativa de la producción:** Evalúa **qué tan equitativamente** se distribuye la producción de bloques o la validación de transacciones entre los actores participantes.

*Matemática aplicable:* Entropía de Shannon, Ley de Zipf y Distribución Normal vs. Anómala

### Entropía de Shannon

La **entropía de Shannon** mide la **cantidad de incertidumbre o aleatoriedad** en un sistema. Cuanto mayor es la entropía, más diversas y distribuidas están las probabilidades de los eventos. En el contexto de descentralización, un valor alto de entropía indica una distribución más dispersa y variada, mientras que un valor bajo indica concentración.

En resumen, a mayor entropía, mayor será la **descentralización** del consenso.

### Ley de Zipf

La **Ley de Zipf** establece que, en muchos sistemas naturales, sociales y económicos, la frecuencia de un evento es inversamente proporcional a su rango. Es decir, en una lista ordenada de eventos (por ejemplo, nodos con mayor poder en una red), el segundo evento tiene la mitad de la frecuencia del primero, el tercero tiene un tercio, y así sucesivamente.

Aplicado a un sistema descentralizado, la participación en la producción de bloques o validación debería seguir una **distribución de potencia**, donde no haya una entidad que domine de manera excesiva. El segundo participante debería tener aproximadamente la mitad de la participación del primero, el tercero un tercio, y así sucesivamente.

Para hacer la evaluación matemática, es preciso analizar la participación cambiante en la producción de bloques o validación a lo largo del tiempo, midiendo la **desviación** entre la distribución real y la distribución esperada según Zipf. Un modelo saludable debería tener fluctuaciones en la dominancia de los actores. Si la distribución de

bloques sigue la Ley de Zipf, es una señal de que **ninguna entidad concentra el poder de manera desproporcionada**. Por otro lado, si la distribución es demasiado concentrada, se concluye que el poder está centralizado.

## Distribución Normal vs. Anómala

En sistemas naturales, muchas actividades siguen una distribución normal (campana de Gauss). Si la producción de bloques o la participación en la validación muestra picos anormales, esto podría indicar centralización o manipulación.

Por un lado, se debe evaluar la participación en la validación de bloques, identificando patrones anormales en la validación que podrían sugerir colusión o concentración de poder.

Por otro lado, se debe evaluar la producción de bloques, detectando si hay entidades que producen bloques de manera desproporcionada.

Al obtener los resultados, se compara la distribución observada con una distribución normal esperada. Desviaciones importantes son indicios de **centralización o irregularidades**.

## Ejemplo de Evaluación del Modelo de Consenso

Imaginemos que una red PoS tiene:

- **100 validadores activos**, pero **5 de ellos producen el 70% de los bloques**.
- Estos 5 validadores pertenecen a una misma entidad (baja diversidad).
- La rotación de poder es baja: siempre los mismos actores dominan la validación.

En este caso:

- **Ley de Zipf** revelaría concentración excesiva de poder.

- **Entropía de Shannon** mostraría baja diversidad entre los validadores.
- La **distribución anómala** sugeriría un modelo centralizado que compromete la descentralización.

## Postulado matemático del factor *Modelo de Consenso*

### 1. Entropía de Shannon

Mide la **diversidad y distribución de los mineros/validadores activos**.

**Fórmula Matemática**

$$H(X) = - \sum_{i=1}^n p_i \log_2(p_i)$$

Donde:

- $p_i$  es la proporción de bloques producidos por la entidad  $i$
- $n$  es el número total de entidades activas.

**Datos a Recolectar**

- Lista de entidades (mineros o validadores).
- Cantidad de bloques producidos por cada una.

**Método de recolección de datos**

- Se usarán plataformas como **CloverPool.com**, **Mempool.space**, o **Blockchain.com** para obtener el **hashrate por pool**.
- Se exportarán los datos en formato CSV o JSON.

## Fórmula de normalización

Para normalizar esta métrica entre **0** y **1**, usamos:

$$H_{\text{norm}} = \frac{H(X)}{H_{\text{max}}}$$

Donde  $H_{\text{max}} = \log_2(n)$  es la entropía máxima posible si todos los mineros y validadores tuvieran participación igualitaria.

## 2. Ley de Zipf

Verifica si la participación sigue una **distribución de poder esperada** (relación inversa entre la participación y la posición).

### Fórmula Matemática

$$P(k) \propto \frac{1}{k^s}$$

Donde:

- $k$  es la **posición del minero** en el ranking (por participación).
- $s$  es un **exponente** que mide la desigualdad en la distribución (valores cercanos a 1 reflejan distribución Zipfiana).

El exponente  $s$  se estima utilizando **regresión lineal** sobre los datos ordenados en escala log-log. La relación entre el **rango** y la **participación (hashrate)** sigue:

$$\log(P(k)) = -s \cdot \log(k) + C$$

donde:

- $P(k)$  es la participación del pool en la posición  $k$
- $k$  es el rango del pool (siendo 1 el más grande)
- $C$  es la constante del fórmula Zipf
- $s$  es la pendiente de la regresión lineal, que indica qué tan rápido disminuye la participación en función del rango.

Si se tienen disponibles los datos de hashrate y rango correspondiente del pool, se deben transformar los datos a escala logarítmica.

- Para cada pool, se calcula  $\log(P(k))$  usando el hashrate.
- Se calcula también  $\log(k)$  para el rango correspondiente.

Luego se debe aplicar una regresión lineal:

- Se ajusta una línea recta a los puntos  $(\log(k), \log(P(k)))$
- La **pendiente** de esta línea será  $-s$ . Si la pendiente es pronunciada, el valor de  $s$  será mayor, lo que indica que la participación cae rápidamente entre los pools.

Fórmula de regresión lineal:

$$s = \frac{N \sum (\log(k) \cdot \log(P(k))) - \sum \log(k) \sum \log(P(k))}{N \sum (\log(k))^2 - (\sum \log(k))^2}$$

Donde  $N$  es el número de puntos

Después de aplicar la fórmula con los datos de los pools y sus hashrates, se obtiene una estimación para  $s$

**Datos a Recolectar:** Hashrate por minero/pool, ordenado de mayor a menor.

**Método de recolección de datos:** Usar el ranking de hashrate por pool desde [mempool.space](https://mempool.space) o [Blockchain.com](https://blockchain.com).

**Fórmula de normalización**

Usamos el **error cuadrático medio** (RMSE) para comparar la distribución observada con la ideal:

$$\text{Error\_Zipf} = \sqrt{\frac{1}{n} \sum_{i=1}^n \left( P(k_i) - \frac{1}{k_i^s} \right)^2}$$

Normalización:

$$\text{Zipf}_{\text{norm}} = 1 - \frac{\text{Error\_Zipf}}{\text{Error\_max}}$$

Donde **Error\_max** es el error máximo permitido.

### 3. Distribución Normal vs Anómala

Detecta **anomalías** en la distribución del hashrate (por ejemplo, si algunos mineros tienen demasiado control).

#### Fórmula Matemática

Para verificar si la distribución es **normal** o presenta **anomalías**, usamos la **prueba de Kolmogorov-Smirnov** (KS):

$$D = \sup_x |F_n(x) - F(x)|$$

Donde:

- $F_n(x)$  es la distribución empírica (datos reales).
- $F(x)$  es la distribución normal esperada.

**Datos a Recolectar: Frecuencia de participación** en la minería o validación por cada entidad.

**Método de recolección de datos**

- Se extraerán datos históricos de **bloques minados por pool** (disponibles en mempool.space y otras plataformas).
- Se generará una distribución empírica para comparar con una normal.

### Fórmula de normalización

Usamos el valor  $D$  de la prueba KS:

$$KS_{\text{norm}} = 1 - D$$

### Fórmula combinada de resultados para el factor *Modelo de Consenso*

Las tres métricas tienen igual ponderación, por lo que el valor final del factor *Modelo de Consenso* estará dado por:

$$\text{Modelo\_Consenso} = \frac{H_{\text{norm}} + \text{Zipf}_{\text{norm}} + KS_{\text{norm}}}{3}$$

## Infraestructura

**Infraestructura** se refiere a los componentes físicos y energéticos que soportan la operación de una red distribuida. La **diversidad en el hardware, fuentes de energía y acceso a infraestructura crítica** es fundamental para evitar puntos de concentración que puedan poner en riesgo la descentralización. Si la infraestructura está en manos de unos pocos actores, la red se vuelve vulnerable a **colusión, fallos regionales o ataques coordinados**.

Por un lado, la concentración del hardware en pocos actores puede facilitar ataques coordinados y aumentar la dependencia de la red en ciertas empresas (por ejemplo, fabricantes de ASICs para Bitcoin). La falta de acceso abierto a esta infraestructura puede limitar la participación y dar poder a unos pocos actores que controlan recursos fundamentales. Además, la diversificación en fuentes de energía no solo

mejora la resiliencia de la red, sino que también contribuye a su sostenibilidad y resistencia ante censura o presión política.

## Componentes:

1. **Diversidad de Hardware:** Evalúa si el hardware utilizado para la minería (en PoW) o validación (en PoS) está disponible para una amplia variedad de participantes o si está monopolizado por **unos pocos fabricantes o proveedores**.
2. **Diversidad en Fuentes de Energía:** Analiza qué tipo de energía se utiliza para mantener la red (renovable, fósil, nuclear) y **dónde están ubicadas las fuentes**. Una red que depende de pocos proveedores o regiones es más vulnerable a **interrupciones regionales o bloqueos regulatorios**.
3. **Acceso a Infraestructura Crítica:** Evalúa que **todos los actores** puedan acceder a los recursos esenciales para participar en la red, como **oráculos, nodos completos y canales** en redes de segunda capa.

*Matemática aplicable:* Redundancia de Información, Entropía de Shannon, y Análisis de Componentes Conectados.

## Redundancia de Información

La **redundancia** mide cuánta información adicional se necesita para que una red mantenga su funcionamiento en caso de fallos o ataques. Un **sistema con alta redundancia** es más resistente, lo que puede correlacionarse con descentralización.

En este caso, permite medir cuántos nodos o componentes pueden fallar sin comprometer el funcionamiento de la red. Una **infraestructura distribuida** debería tener suficientes nodos y recursos replicados para asegurar que la red pueda seguir funcionando, incluso en situaciones de crisis.

Matemáticamente, implica medir cuántos canales o nodos adicionales existen en las distintas capas de la red. Al mismo tiempo, se analiza si los nodos mineros están

distribuidos en diversas regiones energéticas o si dependen de unas pocas fuentes concentradas.

## Entropía de Shannon

Nuevamente utilizaremos la Entropía de Shannon, esta vez para medir la **diversidad** en los tipos de hardware y energía utilizados por la red. Si solo se utiliza un tipo de hardware (como ASICs de un fabricante específico) o una fuente de energía concentrada en una región, la entropía será baja, indicando **centralización**.

Matemáticamente, implica medir qué proporción del hardware proviene de diferentes fabricantes. Al mismo tiempo hay que evaluar qué porcentaje de energía utilizada proviene de diversas fuentes (renovables, fósiles, etc.).

## Análisis de Componentes Conectados

En **teoría de redes**, un componente conectado es un subconjunto de nodos donde todos están interconectados entre sí. En un sistema **descentralizado**, idealmente habría muchos componentes o un **grafo muy distribuido**.

En el contexto de la descentralización, el análisis de componentes conectados mide cómo se distribuyen los recursos críticos en la red, como nodos, oráculos y canales de pago. Esto es fundamental para identificar si la red depende demasiado de unos pocos puntos o si está bien distribuida entre muchos actores.

En concreto, implica analizar si los recursos esenciales (como canales Lightning o nodos completos) están bien distribuidos. Al mismo tiempo se debe evaluar si la infraestructura energética está distribuida en varias regiones y si existen interdependencias críticas.

## Ejemplo de Evaluación del Factor Infraestructura

Imaginemos que una red PoW tiene:

- **70%** de sus mineros utilizando ASICs de un solo fabricante.
- **80%** de la energía proviene de fuentes hidroeléctricas concentradas en dos regiones.
- Los nodos críticos dependen de **infraestructura controlada por pocas empresas**.

En este caso:

- La **entropía** será baja porque hay poca diversidad de hardware y fuentes de energía.
- El **análisis de componentes conectados** revelará concentración de nodos y canales en pocas entidades.
- La falta de **redundancia** hace que la red sea vulnerable a fallos y a regulaciones adversas en ciertas regiones.

El resultado sugiere que la infraestructura de la red está **centralizada**, comprometiendo su descentralización y resiliencia.

---

## Cientes

Se refiere a las **implementaciones de software de nodo** que permiten a los participantes conectarse a la red, validar transacciones y mantener el consenso. La **diversidad y compatibilidad entre distintas implementaciones** es esencial para evitar que la red dependa de un solo software, lo que podría generar vulnerabilidades técnicas y centralización en el desarrollo.

Si una red depende de una sola implementación, cualquier fallo o bug en ese software puede comprometer la estabilidad de la red. La diversidad en el software reduce este

riesgo y refuerza la descentralización. Además, la compatibilidad evita la fragmentación de la red y refuerza su resiliencia al garantizar que las diferentes versiones del software puedan trabajar juntas sin conflictos.

La existencia de múltiples implementaciones refleja una **comunidad más diversa** en términos de desarrollo. Evita que una sola entidad controle el software de nodo, fortaleciendo la descentralización del desarrollo. Además, la diversidad de software fomenta la **innovación** y garantiza que haya opciones alternativas si una implementación deja de ser adecuada o sufre un fallo importante.

## Componentes:

1. **Software del Nodo:** Analiza qué proporción de nodos utiliza cada implementación de software disponible. En Bitcoin, por ejemplo, la mayoría de los nodos utilizan **Bitcoin Core**, pero también existen alternativas como **Bitcoin Knots**, **BTCD** y **Libbitcoin**.
2. **Compatibilidad:** Evalúa la **capacidad de interoperabilidad** entre distintas versiones y forks del software. Una red verdaderamente descentralizada debe permitir que los nodos operen con **diferentes implementaciones** sin perder la capacidad de comunicarse y validar transacciones correctamente.

*Matemática aplicable:* Entropía de Shannon y Redundancia de Información

## Entropía de Shannon

En este contexto, la Entropía de Shannon evalúa qué proporción de la red utiliza cada implementación del cliente de nodo. Una red con alta entropía tendrá varias implementaciones interoperables, reduciendo la concentración en una sola. Por otro lado, si la entropía es baja, es probable que la red se concentre en una única implementación, aumentando los riesgos de centralización.

## Redundancia de Información

En este contexto, la redundancia se refiere a la capacidad de la red para **mantenerse operativa** si una implementación deja de funcionar. Si una implementación tiene un fallo crítico, los nodos que operan con otras implementaciones deberían ser capaces

de mantener la red en funcionamiento. En este sentido, es importante evaluar cuántas implementaciones activas pueden tomar el control si una falla.

En resumen, un alto nivel de redundancia asegura que la red no se verá comprometida si una versión específica del software sufre un fallo. Si no hay suficientes implementaciones alternativas, la red es más vulnerable.

## Ejemplo de Evaluación del Factor Clientes

Supongamos que en una red descentralizada:

- **85% de los nodos** utilizan Bitcoin Core.
- El **10%** usa Bitcoin Knots y el **5%** BTCD.
- Se detectan algunas incompatibilidades entre versiones antiguas de Bitcoin Core y las más recientes, causando pequeños forks temporales.

En este caso:

- **Entropía de Shannon** sería baja, indicando que la mayoría de la red depende de una única implementación.
- **Redundancia de Información** también sería baja, ya que no hay suficientes implementaciones alternativas en caso de fallo en Bitcoin Core.

El resultado sugiere que la red tiene **riesgos de centralización y fragmentación** debido a la falta de diversidad y compatibilidad en las implementaciones del cliente de nodo.

---

# Gobernanza y Desarrollo

---

## Gobernanza

Se refiere a los procesos mediante los cuales se **toman decisiones clave** sobre la red, como actualizaciones del protocolo, cambios en las reglas de consenso, y la gestión de fondos comunes (si los hay). La gobernanza puede ser **on-chain** (en blockchain) o **off-chain** (fuera de la cadena, mediante foros, propuestas, etc.). La descentralización de la gobernanza implica que **todos los actores relevantes puedan participar activamente** en las discusiones y votaciones, sin concentrar el poder en un pequeño grupo.

Si solo unos pocos usuarios técnicos pueden participar, el proceso se vuelve menos transparente y más centralizado. La **accesibilidad** fomenta una comunidad inclusiva donde diversas voces son escuchadas.

Por otro lado, si la mayoría de los actores de la red adopta mejoras sin conflictos, la gobernanza es más efectiva. Sin embargo, si la adopción está fragmentada, puede ser señal de que el poder de decisión está concentrado en un grupo reducido.

### Componentes:

- 1.1. **Accesibilidad:** Mide la facilidad con la que los **usuarios comunes** pueden participar en los procesos de gobernanza, como la discusión de propuestas de mejora (por ejemplo, BIPs en Bitcoin o EIPs en Ethereum)
- 1.2. **Fragmentación:** Mide la **adopción efectiva** de las decisiones de gobernanza por parte de la comunidad. Una implementación **fragmentada** (por ejemplo, cuando diferentes nodos adoptan versiones

conflictivas) puede ser indicio de **falta de consenso** o de control centralizado en las decisiones.

*Matemática aplicable:* Ley de Zipf, Entropía de Shannon, y Análisis de Componentes Conectados

## Ley de Zipf

En este contexto, la **Ley de Zipf** puede medir si la distribución del poder de voto sigue un patrón saludable, donde **no haya un actor que domine de manera desproporcionada**. Si el poder está distribuido de manera justa, la participación sigue una curva de potencia donde el segundo mayor participante tiene aproximadamente la mitad del poder del primero, y así sucesivamente. Esto se evalúa determinando, por un lado, cuántos actores tienen capacidad real de influir en las decisiones clave y, por otro lado, analizando si las decisiones tomadas son implementadas uniformemente o si hay fragmentación en la adopción.

Si unos pocos actores dominan las decisiones de gobernanza, la curva de Zipf debería ser más empinada, indicando **centralización**. Por otro lado, una distribución más uniforme sugiere una **descentralización saludable**.

## Entropía de Shannon

En este contexto, un sistema de gobernanza con alta entropía tiene muchos participantes independientes que aportan al proceso, mientras que uno con baja entropía refleja concentración del poder.

Para evaluar la entropía, hace falta medir la cantidad y diversidad de actores que participan en las discusiones y propuestas de mejora, mientras que se determina si una gran cantidad de actores distintos vota o si solo unos pocos controlan el proceso.

Un valor alto de entropía sugiere **diversidad** y **participación activa** de múltiples actores, mientras que un valor bajo indica que **pocas entidades concentran** las decisiones de gobernanza.

## Análisis de Componentes Conectados

En este contexto sirve para medir si las decisiones de gobernanza se implementan de manera uniforme en toda la red. Si algunos nodos adoptan versiones distintas del protocolo, se pueden generar **forks involuntarios**, lo que indica problemas de fragmentación en la gobernanza.

Para un análisis integral, se necesita identificar cuántos nodos adoptan cada actualización de manera uniforme, y comprobar si existen forks o fragmentación debido a desacuerdos en la implementación de propuestas.

Si la mayoría de los nodos adopta las actualizaciones de manera coordinada, esto solo es un indicador de que la gobernanza es efectiva. Sin embargo, si hay **fragmentación**, la red puede estar experimentando **conflictos internos o falta de consenso**.

## Ejemplo de Evaluación del Factor Gobernanza

Imaginemos que en una red descentralizada:

- Solo **5 de los 100 validadores activos** participan regularmente en las discusiones de propuestas de mejora.
- **80% de los nodos** adopta la última actualización, pero el **20% restante** mantiene versiones anteriores, causando forks temporales.
- La comunidad tiene dificultades para participar en la gobernanza, ya que la documentación y los foros de discusión están dominados por un grupo específico.

En este caso:

- **Ley de Zipf** revelaría que pocas entidades tienen poder real en la toma de decisiones.
- **Entropía de Shannon** mostraría baja diversidad de participación en las votaciones y propuestas.
- El **análisis de componentes conectados** indicaría problemas de compatibilidad entre versiones, lo que sugiere falta de consenso.

El resultado sugiere que la gobernanza de la red está **centralizada** en pocas manos, con una implementación fragmentada de decisiones clave.

---

## Desarrollo

Se refiere a la **participación activa en la creación, mejora y mantenimiento del protocolo** por parte de desarrolladores y entidades. La **distribución de contribuidores** y el **poder de aprobación o rechazo de cambios** son aspectos esenciales para garantizar que ninguna persona o entidad controle el curso del desarrollo. Una red verdaderamente descentralizada debe tener una **comunidad diversa y distribuida**, con múltiples desarrolladores colaborando y aprobando cambios de forma independiente.

La concentración de contribuciones en un pequeño grupo reduce la **diversidad de ideas** y aumenta el riesgo de que ciertas entidades dominen el desarrollo del protocolo. Si el poder de aprobación está centralizado en un grupo reducido, se limita la transparencia y se corre el riesgo de que decisiones importantes sean manipuladas por intereses específicos.

Una **comunidad de desarrollo diversa** promueve nuevas ideas y mejoras que beneficien a toda la red, reduciendo la posibilidad de estancamiento. Si el desarrollo está distribuido entre múltiples actores, es más difícil que una entidad tome el control de la evolución del protocolo. Además, si los desarrolladores se distribuyen globalmente y provienen de diversas organizaciones, la red es más resistente a **regulaciones locales** o a **fallos organizacionales**.

### Componentes:

1. **Distribución de Contribuidores:** Mide **cuántas personas y entidades contribuyen al código del protocolo**, y cómo están distribuidas (geográficamente o por tipo de entidad). Evalúa si los desarrolladores son

mayoritariamente independientes o si pertenecen a pocas empresas o instituciones.

2. **Distribución de Aprobaciones:** Analiza **quién tiene el poder de aprobar o rechazar cambios en el código**. Una red descentralizada debe repartir ese poder entre muchos actores, evitando que unos pocos desarrolladores controlen la toma de decisiones.

*Matemática aplicable:* Índice de Gini, Ley de Zipf, y Entropía de Shannon

## Índice de Gini

El **Índice de Gini** es una medida comúnmente usada para evaluar la **desigualdad en la distribución de recursos**. Va de 0 (distribución perfecta) a 1 (máxima desigualdad).

En el contexto de la descentralización, permite evaluar si las contribuciones y las aprobaciones de cambios están **concentradas en pocas personas o entidades**, o si están más distribuidas entre una comunidad diversa.

Para un análisis integral, se debe medir qué tan equitativa es la participación en el desarrollo del código, y analizar si el poder de aprobar cambios está repartido entre muchos actores o concentrado en pocos.

Un índice de Gini bajo indica **distribución equitativa**, mientras que un valor alto refleja **concentración excesiva** del poder en el desarrollo.

## Ley de Zipf

En este contexto, sirve para medir si la participación sigue una **curva de potencia**, donde el segundo participante más activo tiene la mitad de la participación del primero, y así sucesivamente. En una comunidad saludable, esta distribución no debería ser demasiado empinada, lo que reflejaría una mayor descentralización.

En resumen, si la curva de Zipf es demasiado empinada, se detecta **centralización del desarrollo**. Una curva más plana refleja mayor **distribución del poder**.

## Entropía de Shannon

En este contexto, una alta entropía refleja una mayor diversidad de contribuidores y aprobadores de cambios. Para ello, es preciso medir cuántos desarrolladores diferentes participan activamente y qué tan independientes son entre sí, además de evaluar si muchas personas tienen la capacidad de aprobar o rechazar cambios.

Una **alta entropía** sugiere que la toma de decisiones y las contribuciones están distribuidas entre muchos actores, mientras que una **entropía baja** indica concentración del poder en el desarrollo, lo que compromete la descentralización.

## Ejemplo de Evaluación del Factor Desarrollo

Imaginemos que en una red descentralizada:

- **80% de las contribuciones** provienen de 3 empresas principales.
- **4 personas** tienen el poder de aprobar o rechazar cambios en el código.
- El resto de los desarrolladores contribuyen esporádicamente y no tienen capacidad de decisión real.

En este caso:

- El **Índice de Gini** sería alto, indicando concentración del poder en el desarrollo.
- La **Ley de Zipf** mostraría que unas pocas entidades dominan las contribuciones.
- La **entropía de Shannon** sería baja, revelando falta de diversidad en el proceso de desarrollo.

El resultado sugiere que el desarrollo del protocolo está **centralizado**, lo que pone en riesgo la descentralización y resiliencia de la red.

---

## Escalabilidad

Se refiere a la capacidad de una red descentralizada para **adoptar y desarrollar capas superiores** que aumenten su rendimiento, velocidad, privacidad o funcionalidad, sin comprometer la descentralización de la red base. Las capas superiores (como **Lightning Network en Bitcoin** o **canales de estado en Ethereum**) deben ser lo suficientemente **distribuidas** para evitar que se conviertan en puntos de concentración que introduzcan riesgos de centralización.

La existencia de capas superiores es una señal de que la red está preparada para manejar mayor volumen de transacciones sin saturar la capa base. Sin embargo, si la actividad se concentra en unos pocos hubs o nodos, esto puede comprometer la descentralización, introduciendo puntos únicos de fallo y riesgos de censura.

Una topología bien distribuida refuerza la descentralización, mientras que una estructura jerárquica introduce vulnerabilidades y dependencia de ciertos nodos.

### Componentes:

1. **Capas Superiores:** Mide si la red ha desarrollado e implementado **capas adicionales** que mejoren la escalabilidad y funcionalidad sin afectar la descentralización. Ejemplos incluyen **Lightning Network** para microtransacciones o **sidechains** para ejecutar contratos complejos.
2. **Adopción y Distribución:** Evalúa si la adopción de estas capas está **bien distribuida** o si depende de unos pocos nodos o hubs clave. En una red saludable, la distribución de canales y nodos en las capas superiores debe ser **amplia y descentralizada**.
3. **Topología de la Red:** Analiza la **estructura de la red en las capas superiores**, midiendo si los nodos están interconectados de manera equilibrada o si hay una dependencia excesiva en pocos nodos centrales.

*Matemática aplicable:* Análisis de Componentes Conectados, Entropía de Shannon, y Redundancia de Información

## Análisis de Componentes Conectados

En este contexto, sirve para medir si los nodos y canales en las capas superiores están **bien interconectados** o si dependen de pocos hubs críticos.

Dependiendo de la naturaleza de las capas superiores, es necesario evaluar cuántos canales de pago o puentes están abiertos y cómo se distribuyen entre los nodos. También puede ser necesario detectar si ciertas aplicaciones dependen de pocos nodos validadores o si están distribuidas.

Un **alto número de componentes conectados** refleja una red distribuida y resiliente, mientras que si la mayoría de los canales o puentes dependen de unos pocos actores, se detecta **centralización**.

## Entropía de Shannon

En este contexto, sirve para medir la **diversidad** en los nodos y puentes que operan en las capas superiores. A mayor entropía, mayor diversidad y descentralización en las capas superiores, mientras que si la entropía es baja, puede ser síntoma de que la red depende de un número limitado de actores.

## Redundancia de Información

En este contexto, sirve para medir la capacidad de la red para seguir operativa si ciertos canales o puentes dejan de funcionar. En un sistema escalable, debería haber suficientes nodos y canales alternativos para mantener la red operativa.

En resumen, si hay alta redundancia, la red puede seguir operativa incluso con múltiples fallos, mientras que si la redundancia es baja, la red es vulnerable a interrupciones.

## Ejemplo de Evaluación del Factor Escalabilidad

Supongamos que una red descentralizada:

- **Lightning Network** tiene la mayoría de sus canales concentrados en 5 nodos.
- **80% del volumen de transacciones** pasa por esos nodos principales.
- En una sidechain, solo **dos nodos validadores** manejan la mayoría de las transacciones.

En este caso:

- El **análisis de componentes conectados** revelaría concentración de canales en pocos hubs.
- La **entropía de Shannon** sería baja, indicando falta de diversidad en las capas superiores.
- La **redundancia de información** también sería baja, mostrando que la red es vulnerable si uno de los nodos principales falla.

El resultado sugiere que, aunque existen capas adicionales, **la concentración excesiva en ciertos actores compromete la descentralización** y aumenta los riesgos de censura y fallos.

---

## Interoperabilidad

Se refiere a la **capacidad de una red blockchain para interactuar con otras blockchains** y sistemas externos. Esto incluye la **transferencia fluida de activos o datos** entre diferentes redes y la compatibilidad de contratos inteligentes o protocolos. Un ecosistema interoperable fomenta **mayor descentralización** al evitar que los usuarios dependan de una sola red para sus operaciones, promoviendo un entorno más **conectado y diverso**.

Sin interoperabilidad, los usuarios quedan confinados a una sola blockchain, lo que puede aumentar la centralización en torno a esa red. La interoperabilidad fomenta un **ecosistema más distribuido**. Esto refuerza la independencia del usuario, ya que no necesita depender de exchanges centralizados o entidades de terceros para mover

activos entre redes. Si los puentes o nodos interconectores están centralizados, la interoperabilidad puede introducir **puntos de vulnerabilidad** o riesgos de censura.

Además, las redes pueden **especializarse en casos de uso específicos** (por ejemplo, pagos en Bitcoin y contratos en Ethereum) y colaborar sin competir de manera directa. Las redes conectadas entre sí son más resistentes a fallos y vulnerabilidades, ya que los usuarios pueden redistribuir su actividad hacia otras redes si una red falla.

## Componentes:

1. **Compatibilidad entre Redes:** Mide si la red tiene herramientas o protocolos que le permiten comunicarse con otras redes, como **puentes entre redes** o **tokens interoperables**.
2. **Transferencia de Activos y Datos:** Evalúa si los activos o datos se pueden transferir fácilmente entre blockchains, permitiendo **funcionalidad cruzada** sin depender de intermediarios.
3. **Descentralización del Mecanismo de Interoperabilidad:** Analiza si los mecanismos de interoperabilidad (como puentes o nodos oráculo) están **distribuidos entre múltiples actores** o si dependen de unos pocos nodos centrales.

*Matemática aplicable:* Análisis de Componentes Conectados, Entropía de Shannon, y Redundancia de Información.

## Análisis de Componentes Conectados

Aplicado a la interoperabilidad, evalúa si los puentes y nodos oráculo están distribuidos de manera equilibrada entre varios actores o si dependen de unos pocos hubs. Para ello, es necesario medir si los actores responsables de la interoperabilidad entre redes están bien distribuidos o concentrados. Además, se debe evaluar la solidez de las conexiones entre redes mediante análisis topológicos.

Hecha la evaluación, un **alto número de componentes conectados** indicaría que la interoperabilidad está distribuida entre múltiples actores, mientras que un número bajo de nodos o puentes es un indicador de riesgo de **centralización**.

## Entropía de Shannon

En el contexto de interoperabilidad, una alta entropía indica que **múltiples puentes y protocolos** están disponibles y en uso, reduciendo la dependencia de un solo mecanismo. Para ello, es necesario medir cuántos mecanismos diferentes de interoperabilidad existen y qué tan utilizados están. Además, se precisa evaluar si los activos pueden transferirse entre redes por diferentes rutas.

Hecha la evaluación, un valor alto de entropía reflejaría mayor diversidad y descentralización, mientras que si la entropía es baja, sería un indicador de que la interoperabilidad depende de pocos mecanismos, introduciendo riesgos de centralización.

## Redundancia de Información

En este contexto, sirve para medir si hay suficientes mecanismos alternativos para mantener la interoperabilidad incluso si algunos puentes o nodos fallan. Para ello, es necesario evaluar si hay varias opciones para mover activos entre redes, al mismo tiempo que se mide si existen suficientes nodos oráculos para asegurar la transferencia de datos entre redes.

Si la evaluación arroja una alta redundancia, es indicador de que la interoperabilidad se puede mantener operativa incluso con múltiples fallos. Por otro lado, si la redundancia es baja, la interoperabilidad podría verse comprometida por puntos únicos de fallo.

## Ejemplo de evaluación del factor Interoperabilidad

Supongamos que en una red blockchain:

- Solo **3 puentes principales** manejan la transferencia de activos hacia otras blockchains.
- El **80% del volumen de transacciones** se procesa a través de esos puentes.
- No hay suficientes nodos oráculos alternativos para respaldar la interoperabilidad en caso de fallo.

En este caso:

- El **análisis de componentes conectados** revelaría que la interoperabilidad depende de pocos hubs.
- La **entropía de Shannon** sería baja, indicando poca diversidad en los mecanismos de interoperabilidad.
- La **redundancia de información** también sería baja, mostrando que la interoperabilidad es vulnerable a fallos en los puentes principales.

Este resultado sugiere que la interoperabilidad en la red **no está descentralizada** y presenta riesgos de vulnerabilidad y censura.

# Economía y Transacciones

## Economía

La **economía P2P (peer-to-peer)** mide **cuánto del volumen económico de la red ocurre directamente entre los usuarios**, sin la intervención de intermediarios centralizados, como exchanges o custodios. Una red verdaderamente descentralizada fomenta el uso directo de **plataformas P2P**, donde las transacciones fluyen de usuario a usuario. Además, se evalúa el **crecimiento de plataformas P2P** como un indicador de la salud y autosuficiencia del ecosistema.

El propósito de una red descentralizada es dar a los usuarios el **control directo sobre sus activos**, sin depender de terceros. Un ecosistema con alto uso P2P es importante porque refleja **mayor autosuficiencia y menor dependencia** de actores centralizados, lo que fortalece la descentralización.

Si la mayoría de las transacciones pasa por exchanges centralizados, que a la fecha de este estudio parece ser la realidad predominante de forma transversal en redes descentralizadas, los usuarios dependen de estos intermediarios, lo que introduce **puntos de censura** y vulnerabilidades.

Las plataformas P2P son más resistentes a interferencias regulatorias o bloqueos, ya que no dependen de infraestructuras centralizadas que puedan ser clausuradas. Además que un crecimiento sostenido en plataformas P2P refleja que la red es utilizada para **interacciones reales y no solo para especulación** en exchanges.

En resumen, si los usuarios prefieren plataformas P2P sobre los exchanges centralizados, es un **indicador de que la red está evolucionando hacia la autonomía financiera**.

### Componentes:

1. **Uso de P2P vs. Intermediarios Centralizados:** Mide qué **porcentaje de las transacciones** ocurre de manera directa entre los usuarios (P2P) en

comparación con aquellas que pasan por **exchanges o custodios centralizados**.

2. **Crecimiento de Plataformas P2P:** Analiza si plataformas P2P (como Bisq o bots como @lnp2pbot) están ganando tracción en el ecosistema.

*Matemática aplicable:* Ley de Zipf, Índice de Gini, y Entropía de Shannon.

## Ley de Zipf

En el contexto de la Descentralología, sirve para medir si la participación económica en la red sigue una curva de potencia equilibrada, donde **ningún actor** centralizado domine de manera desproporcionada el volumen de transacciones. El análisis debería considerar si la actividad económica está concentrada en exchanges centralizados o si está distribuida entre usuarios P2P, además de evaluar si el uso de plataformas P2P sigue una distribución sana o si unas pocas plataformas dominan la actividad.

Una curva más plana refleja un **ecosistema saludable**, donde la actividad no depende de unos pocos intermediarios.

## Índice de Gini

En el contexto de la economía en redes, puede aplicarse para evaluar **qué tan concentrada está la actividad económica** en unos pocos actores. Para ello, es necesario medir si las transacciones están distribuidas equitativamente entre usuarios P2P o concentradas en exchanges. Esto debe acompañarse de un análisis para determinar qué parte del volumen total de la red pasa por **unos pocos exchanges o custodios**.

Un **índice de Gini bajo** puede indicar que la actividad económica está bien distribuida, mientras que un **índice alto** sugiere que unos pocos actores controlan la mayor parte del volumen económico, comprometiendo la descentralización.

## Entropía de Shannon

En el contexto de la Descentralología, mide la **diversidad** en el uso de plataformas P2P. Cuanta mayor sea la entropía, más diversificada estará la actividad entre diferentes

plataformas descentralizadas. Para ello, es necesario medir cuántas plataformas P2P son utilizadas activamente y si los usuarios están distribuidos entre varias opciones, analizando si la mayor parte del volumen pasa por unas pocas plataformas o si está distribuido en diversas opciones.

Una mayor entropía sería un síntoma de mayor diversidad de plataformas y menor dependencia de actores centralizados, mientras que una entropía baja sugiere que la actividad se concentra en pocas plataformas, lo que introduce riesgos de centralización.

## Ejemplo de Evaluación del Factor Economía

Supongamos que en una red blockchain:

- **70% del volumen de transacciones** pasa por exchanges centralizados.
- Solo **5%** de las transacciones ocurre mediante plataformas P2P como HodlHodl.
- La actividad P2P está concentrada en **una sola plataforma**, mientras que otras apenas tienen usuarios activos.

En este caso:

- La **Ley de Zipf** revelaría una concentración excesiva de actividad en exchanges y en una sola plataforma P2P.
- El **Índice de Gini** mostraría alta desigualdad en la distribución del volumen económico.
- La **entropía de Shannon** sería baja, indicando falta de diversidad en el uso de plataformas P2P.

El resultado sugiere que la **economía de la red está centralizada**, con poca actividad directa entre usuarios y alta dependencia de intermediarios.

---

# Transacciones

Este factor sirve para medir el **grado de distribución y participación de usuarios** en una red mediante el análisis del volumen, frecuencia y dispersión de las transacciones. Una red con **actividad descentralizada** muestra que las transacciones provienen de muchos usuarios y no se concentran en unas pocas direcciones o entidades.

Un alto volumen de transacciones refleja **adopción y uso activo**, pero es necesario analizar si estas transacciones están **distribuidas equitativamente** para evitar concentración en unos pocos actores. Una red verdaderamente descentralizada muestra actividad dispersa entre muchas direcciones y no concentra la mayoría del volumen en unas pocas entidades. Además que una red con **actividad sostenida y estable** es menos vulnerable a manipulaciones o dependencias temporales.

La cantidad y dispersión de las transacciones muestran **qué tan utilizada está la red** para fines reales y no solo para especulación o actividades internas. Una red con alta dispersión de las transacciones es menos vulnerable a **fallos** si algunos actores dejan de operar, ya que la actividad proviene de muchos usuarios.

## Componentes:

1. **Cantidad de Transacciones:** Mide el volumen total de transacciones procesadas por la red en un período de tiempo determinado.
2. **Dispersión de las Transacciones entre Usuarios:** Evalúa **cuántos usuarios diferentes** participan en las transacciones. Una red verdaderamente descentralizada muestra actividad dispersa entre muchas direcciones y no concentra la mayoría del volumen en unas pocas entidades.
3. **Frecuencia y Patrones de Uso:** Analiza si las transacciones se realizan de manera continua y equilibrada a lo largo del tiempo, o si hay picos anormales que podrían sugerir **actividad artificial** o manipulación.

*Matemática aplicable:* Ley de Benford, Entropía de Shannon, y Distribución Normal vs. Anómala.

## Ley de Benford

La **Ley de Benford** sugiere que en conjuntos de datos naturales, los dígitos más bajos (como 1 y 2) tienden a aparecer con mayor frecuencia al inicio de los números. Si las transacciones siguen este patrón, es un **indicio de actividad natural**; si no lo siguen, puede haber **manipulación o actividad artificial**.

En concreto, se debe analizar si los montos transferidos entre direcciones siguen el patrón esperado según la Ley de Benford, y detectar picos sospechosos que podrían ser causados por bots o actores centralizados.

En resumen, si las transacciones siguen la Ley de Benford, se asume que la actividad es natural, mientras que desviaciones importantes pueden sugerir **actividad anómala o concentrada**.

## Entropía de Shannon

En el contexto de la Descentralogía, sirve para medir la **diversidad** y dispersión en el uso de la red. Un valor alto de entropía refleja una actividad distribuida entre muchos usuarios, mientras que un valor bajo indica **concentración en pocos actores**. Para ello, es preciso medir cuántos usuarios diferentes generan transacciones, y evaluar si los montos transferidos varían o si se repiten patrones sospechosos.

Una alta entropía indicaría **actividad descentralizada y diversa**, mientras que una baja entropía puede sugerir que la actividad está **concentrada en pocas entidades**.

## Distribución Normal vs. Anómala

En el contexto de la Descentralogía, sirve para detectar picos anormales en la actividad de transacciones, lo que podría ser indicio de manipulación o actividad no orgánica. Para llevar a cabo el análisis, hace falta medir si las transacciones se distribuyen de manera estable a lo largo del tiempo, e identificar picos inusuales que podrían ser causados por bots o actores coordinados.

Si la actividad sigue una distribución normal (campana de Gauss), se asume que la red tiene un **uso saludable**. Desviaciones importantes pueden sugerir **manipulación o concentración excesiva**.

## Ejemplo de evaluación del factor *Transacciones*

Supongamos que en una red blockchain:

- El **70% del volumen** de transacciones proviene de solo **10 direcciones**.
- La mayoría de las transacciones son de **montos idénticos**, lo que sugiere actividad automatizada.
- Se detectan picos de actividad a intervalos regulares, sin una causa aparente.

En este caso:

- **Ley de Benford** revelaría que los montos de las transacciones no siguen un patrón natural.
- La **entropía de Shannon** sería baja, indicando falta de diversidad en la participación.
- La **distribución anómala** de la actividad sugiere manipulación o concentración de uso.

El resultado indica que la **actividad está concentrada en unos pocos actores**, comprometiendo la descentralización de las transacciones en la red.

# Inmutabilidad

La **Inmutabilidad** mide la **seguridad y rapidez con la que las transacciones se vuelven irreversibles**, garantizando que no puedan ser modificadas o revertidas. La confianza en una red descentralizada depende de que las transacciones registradas en el libro mayor **sean finales**, asegurando que los usuarios puedan operar sin temor a manipulaciones posteriores.

Los usuarios deben tener la certeza de que las transacciones no pueden ser alteradas una vez registradas. Por lo tanto, la **inmutabilidad garantiza la seguridad financiera** en sistemas descentralizados. Sin inmutabilidad, un actor malicioso con suficiente poder podría **revertir transacciones** ya confirmadas, lo que socava la confianza en la red. Además, en una red verdaderamente descentralizada, **ninguna entidad** debería tener la capacidad de revertir transacciones, garantizando **resistencia a censura**.

En redes como Bitcoin, la seguridad de una transacción aumenta con cada bloque agregado. Un tiempo de confirmación rápido **mejora la experiencia del usuario**, pero debe garantizarse que esa rapidez no comprometa la seguridad. Una red con alta seguridad brinda **confianza total** a los usuarios y reduce la probabilidad de que transacciones puedan ser manipuladas después de registrarse.

## Componentes:

1. **Velocidad de Irreversibilidad:** Mide cuánto tiempo (en bloques o segundos) tarda una transacción en considerarse **final y segura**.
2. **Seguridad de la Irreversibilidad:** Evalúa qué tan **segura es la transacción contra ataques del 51%** o intentos de reorganización de la blockchain. Esto implica medir si la red tiene **suficiente hashrate o poder de validación** para evitar que se reviertan bloques confirmados.

*Matemática aplicable:* Distribución Normal vs. Anómala, Entropía de Shannon, y Redundancia de Información.

## Distribución Normal vs. Anómala

En un sistema saludable, la confirmación de transacciones debería seguir **patrones regulares**, distribuidos de forma continua. Si se detectan **picos inusuales** o reorganizaciones frecuentes de bloques, podría indicar problemas de seguridad o ataques a la red.

Un análisis adecuado debería detectar si la blockchain sufre reorganizaciones que pongan en duda la irreversibilidad de transacciones, y evaluar si las transacciones se confirman en tiempos consistentes o si hay **picos anormales de retraso**.

Si la actividad sigue una **distribución normal**, la red tiene un comportamiento predecible y seguro. Las **anomalías** pueden indicar intentos de manipulación o vulnerabilidad ante reorganización.

## Entropía de Shannon

En el contexto de la Descentralogía, sirve para medir la **diversidad y distribución en la validación** de transacciones. Una alta entropía refleja que muchos actores participan en la validación, reduciendo la posibilidad de ataques coordinados para revertir bloques.

El análisis debe medir cuántos actores independientes participan en la validación de transacciones, y evaluar si el poder está concentrado, lo que aumentaría el riesgo de ataques del 51%.

Una alta entropía indica **resistencia a reorganizaciones** y menor probabilidad de censura o manipulación, mientras que una baja entropía sugiere **concentración de poder**, comprometiendo la seguridad de la inmutabilidad.

## Redundancia de Información

En el contexto de la Descentralogía, sirve para medir si existen suficientes copias del historial de la blockchain para que la red pueda **resistir ataques o fallos**. En una red bien distribuida, la información de las transacciones está replicada en múltiples nodos, lo que garantiza que la **historia no pueda ser alterada**.

El análisis es un tanto complejo, ya que requiere evaluar si suficientes nodos completos replican el historial de la blockchain. Además, es necesario medir si la red puede mantenerse operativa y coherente incluso si algunos nodos o bloques fallan.

Una alta redundancia sugiere que la **inmutabilidad está asegurada** por múltiples copias del historial, mientras que la baja redundancia indica vulnerabilidad ante ataques coordinados para revertir bloques.

## Ejemplo de Evaluación del Factor Inmutabilidad

Supongamos que en una red blockchain:

- Se detectan **reorganizaciones de bloques cada 10 días**, lo que hace que algunas transacciones previamente confirmadas sean revertidas.
- La mayoría del poder de validación está concentrado en **3 pools** de minería, aumentando el riesgo de ataques del 51%.
- Solo un **30% de los nodos** tiene copias completas del historial de la blockchain.

En este caso:

- La **distribución anómala** de reorganizaciones indica que la inmutabilidad no está garantizada.
- La **entropía de Shannon** sería baja, ya que pocos actores controlan la validación.
- La **baja redundancia de información** sugiere que la red es vulnerable a manipulación.

El resultado indica que la **inmutabilidad de la red está comprometida**, lo que reduce la confianza de los usuarios en la seguridad de las transacciones.

---

## Privacidad

Se refiere a las **capacidades integradas en una red** para asegurar el anonimato o pseudoanonimato de los usuarios y sus transacciones, mediante el uso de **tecnologías de criptografía avanzada**. Esto incluye técnicas como **CoinJoin**, **Taproot**, **zk-SNARKs** y otros tipos de **transacciones confidenciales**, que dificultan el rastreo de fondos y protegen la identidad de los usuarios frente a **vigilancia de terceros, la censura**, el rastreo y el análisis forense de las transacciones.

Por ejemplo, Monero usa **transacciones confidenciales** para ocultar los montos transferidos, mientras que en Bitcoin se pueden aplicar herramientas como **CoinJoin** para romper los vínculos entre transacciones.

La privacidad es importante porque protege a los usuarios de **interferencias por actores maliciosos o gobiernos**, al garantizar que sus transacciones no puedan ser bloqueadas o censuradas. Sin privacidad, las transacciones y direcciones pueden ser **rastreadas y vinculadas** a identidades reales, comprometiendo la seguridad de los usuarios y desincentivando la adopción.

Además, la privacidad puede incentivar a los usuarios a **participar más activamente** en la red sin temor a ser identificados, lo que fortalece la descentralización y reduce la concentración de poder en actores que poseen herramientas de vigilancia.

En resumen, la privacidad permite a los usuarios **gestionar sus fondos libremente**, sin necesidad de autorización o supervisión por parte de terceros.

### Componentes:

1. **Anonimato y Pseudoanonimato:** Evalúa si la red ofrece **herramientas que protegen la identidad de los usuarios** al realizar transacciones.

Pseudoanonimato implica que las transacciones no muestran información personal directa, mientras que el anonimato busca ocultar incluso las relaciones entre direcciones.

2. **Criptografía Avanzada:** Mide el uso de **tecnologías de privacidad** como **zk-SNARKs, CoinJoin o Taproot** para garantizar la **confidencialidad** de los montos y las partes involucradas en las transacciones.
3. **Resistencia al Análisis de Red:** Evalúa si la red tiene medidas para **evitar el rastreo por análisis forense**, que busca vincular direcciones y transacciones a través de patrones de uso.

*Matemática aplicable:* Entropía de Shannon, Redundancia de Información, y Análisis de Componentes Conectados.

## Entropía de Shannon

En el contexto de la Descentralogía, sirve para medir la **diversidad** en los métodos de privacidad usados por los participantes de la red. Un valor alto refleja un uso diverso de herramientas de privacidad, mientras que un valor bajo indica dependencia de un solo método, aumentando el riesgo de vulnerabilidades.

Dada la naturaleza de lo que se quiere medir, llevar a cabo un análisis sería demasiado complejo. En cualquier caso, un análisis efectivo debería medir qué porcentaje de las transacciones emplea características de privacidad, y evaluar si los usuarios utilizan varias opciones (como CoinJoin, Taproot, zk-SNARKs) o si la mayoría se concentra en una sola.

Una alta entropía indica un uso diverso de herramientas, lo que mejora la resistencia a censura y rastreo. Por otro lado, una baja entropía puede sugerir una **centralización en las prácticas de privacidad**, lo que puede aumentar la vulnerabilidad de los usuarios.

## Redundancia de Información

En el contexto de la Descentralogía, sirve para medir si existen suficientes alternativas disponibles para preservar la privacidad en caso de que alguna herramienta falle o sea comprometida. Para un análisis efectivo, se precisa evaluar si la red ofrece múltiples herramientas (como zk-SNARKs y CoinJoin) para que los usuarios preserven su privacidad. Al mismo tiempo, se debe analizar si los usuarios pueden cambiar rápidamente de una herramienta de privacidad a otra en caso de que una se vuelva ineficaz.

Una alta redundancia sugiere que la red tiene **suficientes opciones** para preservar la privacidad, mientras que una baja redundancia indica que la red depende de **pocas herramientas**, aumentando los riesgos si alguna de ellas falla.

## Análisis de Componentes Conectados

En el contexto de la Descentralogía, sirve para medir si las transacciones y nodos están **estructurados de manera que permitan el rastreo** mediante análisis forense. Un sistema con conexiones demasiado predecibles es más fácil de rastrear.

Para medir esto, es preciso analizar si los patrones de transacción crean relaciones predecibles entre direcciones. y evaluar si la red está configurada para evitar análisis forense en la capa base de la red (por ejemplo, mediante Onion Routing en Lightning).

Si los componentes conectados son predecibles, la privacidad es vulnerable, mientras que si las conexiones son dispersas y difíciles de rastrear, la red es más segura.

## Ejemplo de evaluación del factor *Privacidad*

Imaginemos que en una red blockchain:

- **80% de las transacciones** no emplean ninguna característica de privacidad.
- Solo **una herramienta** (CoinJoin) es utilizada para preservar el pseudoanonimato, y su uso es limitado.
- Las transacciones siguen patrones predecibles, facilitando el rastreo por análisis forense.

En este caso:

- La **entropía de Shannon** sería baja, indicando poca diversidad en el uso de herramientas de privacidad.
- La **redundancia de información** también sería baja, sugiriendo que hay pocas alternativas disponibles.

- El **análisis de componentes conectados** revelaría vulnerabilidad ante rastreo, comprometiendo la privacidad de los usuarios.

El resultado sugiere que la red **carece de medidas sólidas de privacidad**, aumentando los riesgos de censura y vigilancia.

---

## Emisión

En este factor se mide el **control sobre la emisión de tokens y el sistema de incentivos**, asegurando que las reglas de suministro y las recompensas no puedan ser modificadas arbitrariamente. Un sistema descentralizado mantiene **reglas inalterables** respecto a la emisión, como el límite de 21 millones de bitcoins en Bitcoin, para evitar **inflación descontrolada** o **intervenciones monetarias no consensuadas**. La previsibilidad del suministro es esencial para una red que busca garantizar **autosoberanía financiera**.

Si las reglas monetarias pueden cambiarse sin consenso, la red corre el riesgo de **manipulación económica** que compromete su descentralización.

Un sistema de incentivos bien diseñado asegura la **participación activa** de validadores o mineros sin poner en riesgo la estabilidad económica. Además, la **transparencia en la emisión** refuerza la confianza en la red, evitando incertidumbre sobre el valor de los tokens.

### Componentes:

1. **Inmutabilidad de las Reglas de Emisión:** Mide la **imposibilidad de modificar las reglas de emisión** sin consenso. Ejemplos de esto son el **límite de 21 millones de BTC** o el calendario de halving en Bitcoin.
2. **Previsibilidad del Suministro y Recompensas:** Evalúa si el calendario de emisión de tokens es **claro y predecible**, permitiendo a los participantes conocer con antelación las recompensas y el suministro total.

3. **Sistema de Incentivos:** Mide si las **recompensas por minería o validación** están alineadas con el funcionamiento de la red a largo plazo, evitando inflación descontrolada o incentivos mal estructurados.

*Matemática aplicable:* Índice de Gini, Ley de Gresham, y Análisis de Consenso y Resistencia a Cambios Arbitrarios.

### Índice de Gini

En el contexto de la Descentralogía, sirve para medir la **desigualdad en la distribución de recompensas**. En un sistema bien descentralizado, las recompensas por minería o validación deberían estar distribuidas entre **muchos actores** y no concentradas en unos pocos.

El análisis debería incluir una medición de las recompensas para determinar si están concentradas en pocas entidades (como pools de minería). Además, se debe evaluar si el sistema de recompensas promueve la participación amplia y continua.

Un **índice de Gini bajo** indica que las recompensas están distribuidas de manera equitativa, mientras que un **índice alto** sugiere concentración del poder económico en unos pocos actores, lo que compromete la descentralización.

### Ley de Gresham

La **Ley de Gresham** sugiere que el "dinero malo" tiende a desplazar al "dinero bueno". En el contexto de la Descentralogía, si las reglas de emisión permiten una **inflación descontrolada**, los usuarios podrían preferir otros activos con emisión limitada y predecible.

Un análisis adecuado debería evaluar si los usuarios abandonan una red con mala política de emisión en favor de otra más estable. Además, debe medir si las reglas de emisión refuerzan la confianza en el valor del token a lo largo del tiempo.

### Análisis de Consenso y Resistencia a Cambios Arbitrarios

Este análisis pretende medir **qué tan difícil es modificar las reglas de emisión**. En una red descentralizada, los cambios en las políticas monetarias deberían requerir **amplio consenso** entre los participantes.

Un análisis de la red debería servir para evaluar si en el pasado las reglas de emisión han sido modificadas con facilidad o si hubo consenso amplio (si es que existe un historial de cambios monetarios). En caso que existan cambios de esta naturaleza, se debería medir cuántos actores participaron en la toma de decisiones sobre emisión y si hubo resistencia a cambios arbitrarios.

En conclusión, un historial sin cambios importantes refleja **estabilidad monetaria**. Por otro lado, si se detectan modificaciones frecuentes sin consenso, la red podría estar expuesta a **riesgos de manipulación**.

## Ejemplo de Evaluación del Factor Emisión

Supongamos que en una red blockchain:

- El **suministro total de tokens ha sido modificado dos veces** sin un proceso claro de consenso.
- La mayoría de las recompensas por minería se concentran en **tres pools principales**.
- El calendario de emisión no es transparente, lo que provoca **incertidumbre** entre los usuarios.

En este caso:

- El **análisis de consenso** revelaría que las reglas de emisión se pueden cambiar fácilmente, comprometiendo la estabilidad monetaria.
- El **índice de Gini** mostraría una alta concentración en la distribución de recompensas.
- La **Ley de Gresham** sugeriría que los usuarios podrían preferir otros activos con reglas más estables.

El resultado sugiere que la red tiene **problemas de centralización monetaria**, lo que pone en riesgo la confianza y sostenibilidad del ecosistema.

---

# Resistencia y Equidad

## Censura

Mide la **capacidad de la red para resistir bloqueos, restricciones o interferencias** por parte de gobiernos, reguladores o actores maliciosos. Una red verdaderamente descentralizada debe permitir que los usuarios **operen sin restricciones significativas**, incluso en entornos con **prohibiciones explícitas o censura activa**. Esto implica evaluar **cómo se comporta la red en estos contextos** y si cuenta con **mecanismos técnicos que protejan a los usuarios** de censura.

La resistencia a la censura permite a los usuarios **transferir valor sin restricciones**, incluso en regímenes autoritarios o entornos regulatorios restrictivos. Si una red puede ser censurada por **gobiernos o empresas**, pierde su independencia y pone en riesgo la **autosoberanía** de los usuarios. Por lo tanto, la resistencia a la censura garantiza que **cualquier persona en cualquier parte del mundo** pueda acceder y participar en la red, independientemente de las restricciones locales.

Si la red puede seguir funcionando en **entornos adversos**, demuestra una **alta resistencia** a la censura y refuerza su descentralización. Además que una infraestructura bien distribuida reduce los **puntos únicos de fallo** y hace más difícil que un gobierno o actor malicioso bloquee la red. Por ejemplo, Bitcoin permite operar a través de Tor, mientras que Lightning Network ofrece canales de pago difíciles de rastrear.

En resumidas cuentas, si la red es inmune a bloqueos y restricciones, se demuestra que **ningún actor central tiene control significativo** sobre su funcionamiento.

### Componentes:

1. **Accesibilidad en países con restricciones:** Evalúa si la red sigue operativa en **países con intentos de censura** o prohibiciones, permitiendo que los usuarios la utilicen sin restricciones.

2. **Mecanismos técnicos de resistencia a la censura:** Mide si la red utiliza **tecnologías como Tor, VPNs, Onion Routing** u otras técnicas que **dificultan la censura de nodos o transacciones.**
3. **Distribución de la Infraestructura Crítica:** Analiza si la infraestructura de la red (como nodos o canales de pago) está **distribuida globalmente** o concentrada en pocos actores o regiones, lo que facilitaría su censura.

*Matemática aplicable:* Entropía de Shannon.

## Entropía de Shannon

En el contexto de la Descentralogía, sirve para medir la **diversidad** en la distribución de nodos y canales. Una alta entropía indica que la red es utilizada y operada por **muchos actores independientes**, lo que dificulta su censura.

Un análisis de la red debería determinar si los nodos son operados por una amplia variedad de actores y en diferentes regiones. Además requiere evaluar si las transacciones fluyen por múltiples rutas o si dependen de unos pocos hubs.

Una alta entropía refleja **distribución saludable** y resistencia a la censura, mientras que una baja entropía indica concentración, lo que facilita los bloqueos.

## Ejemplo de evaluación del factor *Censura*

Supongamos que en una red blockchain:

- **80% de los nodos** están concentrados en un solo país con fuertes restricciones regulatorias.
- La mayoría de los usuarios no utiliza **VPNs ni Tor** para evitar bloqueos.
- La red experimenta **caídas frecuentes** cuando los nodos clave son bloqueados por reguladores.

En este caso, la **entropía de Shannon** sería baja, sugiriendo que la red no está distribuida entre suficientes actores independientes.

El resultado sugiere que la red **es vulnerable a la censura**, comprometiendo su descentralización y autonomía.

---

## Equidad

La equidad se mide para comprobar si la **distribución inicial y posterior de los tokens y la riqueza** en una red blockchain es justa y no está excesivamente concentrada. La equidad implica evitar que unos pocos actores tengan **control económico desproporcionado**, garantizando que la red ofrezca **oportunidades de participación** a una base amplia de usuarios. Esto se analiza tanto en la **fase de distribución inicial (preminado)** como en la **evolución de la riqueza** entre los participantes a lo largo del tiempo.

Si la distribución inicial está concentrada en pocas manos, se compromete la equidad económica y se aumenta el riesgo de **centralización del control económico**. Una distribución equitativa incentiva la participación activa y reduce el riesgo de que la red sea controlada por **unos pocos actores económicamente dominantes**.

La equidad en la distribución de riqueza también implica que **nuevos participantes** puedan integrarse en la red sin enfrentar barreras económicas significativas.

### Componentes:

1. **Preminado y Distribución Inicial:** Mide **cómo se distribuyeron los tokens al inicio del proyecto** y si hubo preminado o asignaciones significativas a los desarrolladores, fundadores o inversores.
2. **Equidad en la Distribución de la Riqueza:** Analiza cómo se **distribuye la riqueza generada por el uso continuo de la red**. Evalúa si hay concentración en unas pocas direcciones o si la riqueza está repartida entre una base amplia de usuarios.

*Matemática aplicada:* Índice de Gini, Ley de Pareto, y Análisis de Cohortes.

### Índice de Gini

En el contexto de la Descentralogía, el **Índice de Gini** refleja si los tokens y la riqueza están concentrados en unas pocas entidades o si están repartidos de manera más

equitativa. Para ello, hace falta medir si el preminado o las asignaciones iniciales favorecieron a unos pocos actores, y evaluar cómo está distribuida la riqueza entre los usuarios activos a lo largo del tiempo.

En resumen, un índice bajo refleja **distribución equitativa**, mientras que un índice alto sugiere **concentración de recursos** en pocas manos.

## Ley de Pareto

La **Ley de Pareto** establece que en muchos sistemas, **el 80% de los recursos tiende a concentrarse en el 20% de los actores**. En una red descentralizada, se busca minimizar este tipo de concentración para asegurar una distribución más justa.

Un estudio detallado debería analizar si la mayor parte de los tokens está concentrada en una pequeña fracción de direcciones, y evaluar si la riqueza generada por el uso de la red se concentra en unos pocos actores.

Si se observa una concentración desproporcionada (80/20 o más extrema), la red es menos equitativa. Por otro lado, una distribución más balanceada sugiere una red más inclusiva y descentralizada.

## Análisis de Cohortes

El **análisis de cohortes** mide cómo **nuevos grupos de usuarios** ingresan a la red y acumulan riqueza con el tiempo. Este análisis permite identificar si los usuarios que ingresan más tarde tienen **las mismas oportunidades económicas** que los usuarios tempranos.

Para un correcto análisis se debería evaluar si la riqueza se concentra en usuarios iniciales o si los nuevos participantes pueden acumular riqueza de manera justa. Al mismo tiempo, se debería medir si los nuevos usuarios enfrentan barreras económicas para participar en la red.

Si las cohortes más recientes logran acumular riqueza proporcionalmente, la red es más equitativa. Por otro lado, si la riqueza está concentrada en los usuarios iniciales, la red presenta **barreras económicas** para nuevos participantes.

## **Ejemplo de evaluación del factor *Equidad***

Supongamos que en una red blockchain:

- El **50% de los tokens** fue preminado y distribuido entre los desarrolladores y sus socios.
- El **80% de la riqueza acumulada** está concentrada en **10 direcciones principales**.
- Los usuarios que ingresaron después del lanzamiento tienen **pocas oportunidades** para adquirir tokens sin pagar precios significativamente más altos.

En este caso:

- El **Índice de Gini** sería alto, indicando alta concentración de riqueza.
- La **Ley de Pareto** revelaría una distribución desbalanceada, con pocos actores controlando la mayoría de los tokens.
- El **análisis de cohortes** mostraría barreras económicas para nuevos participantes, sugiriendo una red poco inclusiva.

El resultado sugiere que la red **no es equitativa**, lo que compromete la descentralización económica y dificulta la participación amplia.

---

# Adopción

La adopción de una red se refiere al grado en que su tecnología es **utilizada en la vida real** para resolver problemas concretos, tanto por su capacidad para abordar **casos de uso reales**, como por su **diversidad geográfica y sectorial**, y el **número de usuarios activos** que participan en sus servicios no especulativos. Cuanto mayor sea el grado de adopción en estos tres aspectos, más relevante y distribuida está la red en términos de impacto práctico, lo que puede contribuir a la resiliencia y descentralización de su uso. Una adopción amplia y diversa asegura que la red **no dependa de un único sector, región o propósito**, lo que refuerza su descentralización práctica.

## Componentes:

1. **Casos de Uso Reales:** Este factor mide el grado en que la red se utiliza para resolver problemas reales o proporcionar soluciones fuera del ámbito especulativo. Los casos de uso reales incluyen transferencias de valor, pagos transfronterizos, contratos inteligentes, almacenamiento de valor, finanzas descentralizadas (DeFi), o cualquier otro servicio que tenga un impacto práctico en la vida cotidiana. No se trata solo del número de transacciones, sino de qué tipo de transacciones se realizan y cómo estas mejoran la vida de las personas o resuelven problemas del mundo real.
2. **Diversidad en la Adopción:** Este factor evalúa **qué tan diversificado está el uso de la red** en términos de geografía, sectores económicos y tipos de usuarios. Una red con **diversidad en la adopción** se utiliza en distintas regiones del mundo, en múltiples industrias (comercio, salud, logística, educación, etc.), y por diferentes tipos de actores (individuos, empresas, gobiernos). Cuanto más diversa sea la adopción, mayor es la probabilidad de que la red se mantenga descentralizada en sus casos de uso, evitando la concentración de actividad en un solo país, industria o tipo de usuario.
3. **Participación de Usuarios Activos:** Este factor mide el número y la frecuencia de **usuarios activos que interactúan con la red** para realizar

transacciones o participar en sus funciones no especulativas. Cuantos más usuarios realicen operaciones cotidianas con el proyecto (por ejemplo, pagos, uso de contratos inteligentes, trading descentralizado, etc.), más descentralizada está la red en cuanto al uso de sus servicios. Aquí es clave diferenciar entre usuarios que **utilizan la red para resolver problemas reales** y aquellos que simplemente mantienen tokens con fines especulativos.

*Matemática aplicable:* Ley de Metcalfe, Entropía de Shannon, y Ley de Zipf

## Ley de Metcalfe

La **Ley de Metcalfe** establece que **el valor de una red es proporcional al cuadrado del número de usuarios conectados**. Cuantos más usuarios interactúan activamente, mayor es el impacto y la utilidad de la red.

Para analizar el cumplimiento de esta Ley, es necesario evaluar cómo el número creciente de usuarios incrementa el valor de la red, y al mismo tiempo medir si el uso práctico de la red crece junto con el número de usuarios activos.

Si la red sigue la Ley de Metcalfe, la **adopción debería ser amplia y exponencial**. Si no sigue este patrón, la red podría estar limitada en su uso práctico.

## Entropía de Shannon

En el contexto de la Descentralogía, sirve para medir la **diversidad en la utilización** de la red en términos de sectores, geografías y tipos de usuarios. Cuanta mayor sea la entropía, más descentralizada debería estar la adopción.

Para un análisis exacto, debería medirse si la red se utiliza en múltiples industrias y regiones del mundo, y evaluar si hay diferentes tipos de transacciones (pagos, contratos, almacenamiento de valor, etc.).

Una alta entropía puede ser indicador de **diversidad y descentralización en el uso**, mientras que una baja entropía sugiere **concentración de actividad** en un solo sector o región.

## Ley de Zipf

La **Ley de Zipf** mide si la distribución de la actividad sigue una curva de potencia, donde una pequeña parte de los usuarios genera la mayoría de las transacciones. En una red descentralizada, la actividad debería estar **más equilibrada**.

Para un análisis adecuado, debería evaluarse si la mayoría de las transacciones provienen de muchos usuarios o de unos pocos, y medir si ciertos sectores dominan la actividad económica en la red.

Una distribución equilibrada refleja **uso descentralizado y sostenible**, mientras que una curva empinada sugiere concentración de la actividad en pocos actores o sectores.

## Ejemplo de evaluación del factor *Adopción*

Imaginemos que en una red blockchain:

- La mayoría de las transacciones se concentran en **intercambios especulativos**.
- El uso práctico (pagos, contratos inteligentes) es **limitado** a ciertos sectores.
- **70% del volumen de transacciones** proviene de solo **dos regiones del mundo**.

En este caso:

- La **Ley de Metcalfe** mostraría que la red no está aprovechando su potencial de adopción.
- La **entropía de Shannon** sería baja, indicando poca diversidad en el uso.
- La **Ley de Zipf** revelaría una alta concentración de la actividad en pocos sectores y regiones.

El resultado sugiere que la red **no está descentralizada en términos de adopción** y depende de actividades especulativas en unos pocos mercados.

---

# Ley de Benford

## Como análisis integral de toda la red

La **Ley de Benford** establece que en muchos conjuntos de datos naturales, **los dígitos más bajos (como 1 y 2) aparecen con mayor frecuencia como primer dígito** que los más altos (como 8 y 9). Esta distribución esperada puede ser utilizada para detectar **manipulación de datos, actividad artificial o irregularidades** en la red blockchain. Al analizar **los datos completos de una blockchain**, como la frecuencia de transacciones, montos, o hash rates, podemos identificar si estos siguen el **patrón de Benford** o si muestran signos de manipulación.

Se puede aplicar a una variedad de datos, como **volumen de transacciones, montos transferidos, actividad de direcciones y producción de bloques**, proporcionando una **evaluación integral** del entorno de la blockchain.

Una red verdaderamente distribuida debería generar datos que sigan un **comportamiento natural**. Si el patrón no se cumple, puede reflejar **concentración excesiva** de la actividad en pocos actores o manipulación coordinada.

La Ley de Benford es una herramienta poderosa para detectar **actividades no aparentes** que podrían pasar desapercibidas mediante otras métricas. Esto refuerza la transparencia de la red y ayuda a identificar concentraciones de poder ocultas.

### Componentes:

1. Se define un conjunto de datos relevantes para el análisis. Por ejemplo: **montos de transacciones, frecuencia de bloques minados, frecuencia y volumen de transacciones, cantidades transferidas por dirección, hash rates, nonces**, etc. Como regla general, mientras más datos y mayor variedad de datos se midan, más preciso debería ser el análisis de la Ley Benford.
2. Obtenidos y tabulados los datos, se debe extraer el **primer dígito** de cada número del conjunto.
3. Se calcula la **frecuencia observada**  $F_o(d)$  para cada dígito  $d$

Un **valor bajo de varianza** indica que los datos se ajustan bien a la Ley de Benford, mientras que un **valor alto sugiere irregularidades**.

## Ejemplo de evaluación usando la Ley de Benford

Imaginemos que en una red blockchain:

- El **70% de los montos transferidos** comienzan con los dígitos 8 y 9, lo que **no sigue la distribución esperada** según la Ley de Benford.
- El **hash rate** muestra un patrón irregular en ciertos momentos del día, coincidiendo con actividades coordinadas por pools de minería.
- Las **transacciones de alto valor** están concentradas en unas pocas direcciones.

En este caso:

- La **Ley de Benford** revelaría comportamientos anómalos en los montos transferidos.
- La **distribución anómala del hash rate** sugeriría manipulación coordinada.
- La **concentración de la actividad en pocas direcciones** reflejaría centralización oculta.

El resultado sugiere que **la red presenta irregularidades** que afectan su descentralización y requieren mayor análisis para identificar los actores responsables.

## .Postulado matemático del factor *Ley de Benford*

La ley establece la probabilidad de que un número comience con un dígito  $d$  donde  $d \in \{1,2,\dots,9\}$

$$P(d) = \log_{10}(d + 1) - \log_{10}(d)$$

Distribución esperada:

- **1:** 30.1%
- **2:** 17.6%
- **3:** 12.5%
- **4:** 9.7%
- **5:** 7.9%
- **6:** 6.7%
- **7:** 5.8%
- **8:** 5.1%
- **9:** 4.6%

Si los datos reales de una red se desvían significativamente de esta distribución, podríamos sospechar de **anomalías o concentraciones inusuales** en la actividad.

Cálculo del Error Cuadrático Medio (RMSE) para Benford

Se usa la misma lógica que en el análisis de Zipf para calcular el **RMSE**, comparando las frecuencias observadas  $P_{\text{obs}}(d)$  con las esperadas  $P_{\text{exp}}(d)$ :

$$Error\_Benford = \sqrt{\frac{1}{9} \sum_{d=1}^9 (P_{\text{obs}}(d) - P_{\text{exp}}(d))^2}$$

Después de calcular el error, aplicamos la siguiente fórmula para **normalizar**:

$$Benford_{norm} = 1 - \frac{Error\_Benford}{Error_{max}}$$

Donde  $Error_{max}$  es el valor máximo posible del error (cuando la distribución observada es completamente distinta de la esperada).

## Resumen Final

1. **Nodos:** Geodistribución y diversidad de los nodos o elementos de la red.
2. **Modelo de Consenso:** Diversidad en la participación en el mecanismo de consenso (minería, validación, y distribución).
3. **Infraestructura:** Diversidad de hardware, energía y acceso a infraestructura crítica.
4. **Clientes:** Diversidad y compatibilidad de implementaciones del cliente de nodo.
5. **Gobernanza:** Participación en decisiones clave, incluyendo poder de voto.
6. **Desarrollo:** Diversidad de contribuidores en el protocolo.
7. **Escalabilidad:** Existencia de capas superiores en la red.
8. **Interoperabilidad:** Capacidad de interactuar con otras blockchains.
9. **Economía:** Nivel de actividad P2P sin intermediarios.
10. **Transacciones:** Distribución y actividad en la red.
11. **Inmutabilidad:** Seguridad y rapidez de la irreversibilidad de las transacciones.
12. **Privacidad:** Capacidades de anonimato y protección.
13. **Emisión:** Control sobre la emisión de tokens y los incentivos.
14. **Censura:** Resistencia a la censura en la red.
15. **Equidad:** Equidad en la distribución inicial de tokens.
16. **Casos de Uso Reales:** Uso práctico de la red fuera de la especulación.
17. **Diversidad en la Adopción:** Variedad de uso en diferentes regiones y sectores.
18. **Participación de Usuarios Activos:** Cantidad de usuarios que interactúan regularmente con la red.
19. **Ley Benford:** Análisis de datos generados por la red y detección de irregularidades que comprometan la descentralización.

## **Ponderación en el Índice Global de Descentralización**

1. **Nodos:** 10%
2. **Modelo de Consenso:** 10%
3. **Infraestructura:** 10%
4. **Clientes:** 5%
5. **Gobernanza:** 5%
6. **Desarrollo:** 5%
7. **Escalabilidad:** 2,5%
8. **Interoperabilidad:** 2,5%
9. **Economía:** 5%
10. **Transacciones:** 5%
11. **Inmutabilidad:** 5%
12. **Privacidad:** 2,5%
13. **Emisión:** 2,5%
14. **Censura:** 2,5%
15. **Equidad:** 2,5%
16. **Casos de Uso Reales:** 5%
17. **Diversidad en la Adopción:** 2,5%
18. **Participación de Usuarios Activos:** 2,5%
19. **Ley Benford:** 15%

# Elaboración matemática de IGD de Bitcoin

al 23 de Octubre de 2024

## 1. Nodos

Entropía de Shannon

$$H(X) = - \sum_{i=1}^n p_i \log_2(p_i)$$

### Distribución geográfica de nodos:

1. sin geolocalización identificada: 12201	24. Irlanda: 43	48. Turquía: 8
2. Estados Unidos: 1992	25. Bélgica: 42	49. Chile: 8
3. Alemania: 1315	26. Ucrania: 40	50. Moldavia: 8
4. Francia: 383	27. Lituania: 39	51. Grecia: 7
5. Finlandia: 382	28. Bulgaria: 37	52. Chipre: 6
6. Países Bajos: 352	29. India: 36	53. Vietnam: 6
7. Canadá: 286	30. Noruega: 32	54. Bahréin: 6
8. Reino Unido: 264	31. Hungría: 32	55. Kazajstán: 5
9. Suiza: 168	32. Sudáfrica: 27	56. Uruguay: 5
10. Singapur: 151	33. Malasia: 24	57. Arabia Saudita: 4
11. Federación Rusa: 150	34. Taiwán: 24	58. Letonia: 4
12. Australia: 120	35. Tailandia: 22	59. Panamá: 4
13. Brasil: 97	36. Rumania: 22	60. Malta: 4
14. Japón: 97	37. Nueva Zelanda: 20	61. Colombia: 4
15. Chequia: 88	38. Argentina: 19	62. Islandia: 3
16. Polonia: 83	39. Indonesia: 17	63. Luxemburgo: 3
17. Italia: 75	40. Portugal: 17	64. República Democrática Popular Lao: 3
18. España: 74	41. México: 15	65. Irán (República Islámica del): 3
19. Suecia: 68	42. Eslovaquia: 15	66. Serbia: 3
20. Austria: 67	43. Dinamarca: 14	67. Belice: 3
21. Hong Kong: 64	44. Estonia: 12	68. Croacia: 3
22. Corea: 63	45. Emiratos Árabes: 11	69. Costa Rica: 3
23. China: 51	46. Eslovenia: 10	
	47. Israel: 10	

70. Guatemala: 2	78. Catar: 2	86. Seychelles: 1
71. Liechtenstein: 2	79. Kuwait: 2	87. Ecuador: 1
72. Islas Feroe: 2	80. Curazao: 1	88. Georgia: 1
73. Venezuela: 2	81. Mauricio: 1	89. Filipinas: 1
74. Kirguistán: 2	82. Omán: 1	90. Trinidad y Tobago: 1
75. Isla de Man: 2	83. El Salvador: 1	91. Argelia: 1
76. Montenegro: 2	84. República Dominicana: 1	92. Costa de Marfil: 1
77. Bielorrusia: 2	85. Bosnia y Herzegovina: 1	93. Andorra: 1

Nodos totales: 18436

## 1. Cálculo de $p_i$ y $p_i \log_2(p_i)$

Se tienen en cuenta los siguientes supuestos:

- Todos los nodos son completos (no se distingue de *Nodos Ligeros*).
- Cada nodo corresponde a una sola entidad independiente (no se distingue por empresas, o pools de minería que pueden tener más un nodo)

$$p_i = \frac{\text{Nodos en el país } i}{18436} \quad \text{y} \quad p_i \log_2(p_i)$$

País	Nodos	$p_i$	$p_i \log_2(p_i)$
Sin geolocalización	12201	0.6621	-0.3946
Estados Unidos	1992	0.1081	-0.3521
Alemania	1315	0.0713	-0.2782
Francia	383	0.0208	-0.0994
Finlandia	382	0.0207	-0.0992
Países Bajos	352	0.0191	-0.0939
Canadá	286	0.0155	-0.0817
Reino Unido	264	0.0143	-0.0764
Suiza	168	0.0091	-0.0586
Singapur	151	0.0082	-0.0540
Rusia	150	0.0081	-0.0536

Australia	120	0.0065	-0.0466
Brasil	97	0.0053	-0.0396
Japón	97	0.0053	-0.0396
Chequia	88	0.0048	-0.0368
Polonia	83	0.0045	-0.0352
Italia	75	0.0041	-0.0326
España	74	0.0040	-0.0322
Suecia	68	0.0037	-0.0303
Austria	67	0.0036	-0.0300
Hong Kong	64	0.0035	-0.0290
Corea	63	0.0034	-0.0286
China	51	0.0028	-0.0254
Irlanda	43	0.0023	-0.0229
Bélgica	42	0.0023	-0.0226
Ucrania	40	0.0022	-0.0215
Lituania	39	0.0021	-0.0211
Bulgaria	37	0.0020	-0.0201
India	36	0.0020	-0.0197
Noruega	32	0.0017	-0.0180
Hungría	32	0.0017	-0.0180
Sudáfrica	27	0.0015	-0.0158
Malasia	24	0.0013	-0.0146
Taiwán	24	0.0013	-0.0146
Tailandia	22	0.0012	-0.0138
Rumania	22	0.0012	-0.0138
Nueva Zelanda	20	0.0011	-0.0129
Argentina	19	0.0010	-0.0123

Indonesia	17	0.0009	-0.0116
Portugal	17	0.0009	-0.0116
México	15	0.0008	-0.0108
Eslovaquia	15	0.0008	-0.0108
Dinamarca	14	0.00075	-0.0104
Estonia	12	0.0007	-0.0092
Emiratos Árabes Unidos	11	0.0006	-0.0088
Eslovenia	10	0.0005	-0.0082
Israel	10	0.0005	-0.0082
Turquía	8	0.0004	-0.0069
Chile	8	0.0004	-0.0069
Moldavia	8	0.0004	-0.0069
Grecia	7	0.00035	-0.0063
Chipre	6	0.0003	-0.0057
Vietnam	6	0.0003	-0.0057
Bahréin	6	0.0003	-0.0057
Kazajstán	5	0.00025	-0.0052
Uruguay	5	0.00025	-0.0052
Arabia Saudita	4	0.0002	-0.0046
Letonia	4	0.0002	-0.0046
Panamá	4	0.0002	-0.0046
Malta	4	0.0002	-0.0046
Colombia	4	0.0002	-0.0046
Islandia	3	0.00015	-0.0040
Luxemburgo	3	0.00015	-0.0040
República Democrática Popular Lao	3	0.00015	-0.0040
Irán	3	0.00015	-0.0040

Serbia	3	0.00015	-0.0040
Belice	3	0.00015	-0.0040
Croacia	3	0.00015	-0.0040
Costa Rica	3	0.00015	-0.0040
Guatemala	2	0.0001	-0.0034
Liechtenstein	2	0.0001	-0.0034
Islas Feroe	2	0.0001	-0.0034
Venezuela	2	0.0001	-0.0034
Kirguistán	2	0.0001	-0.0034
Isla de Man	2	0.0001	-0.0034
Montenegro	2	0.0001	-0.0034
Bielorrusia	2	0.0001	-0.0034
Catar	2	0.0001	-0.0034
Kuwait	1	0.00005	-0.0023
Curazao	1	0.00005	-0.0023
Mauricio	1	0.00005	-0.0023
Omán	1	0.00005	-0.0023
El Salvador	1	0.00005	-0.0023
República Dominicana	1	0.00005	-0.0023
Bosnia y Herzegovina	1	0.00005	-0.0023
Seychelles	1	0.00005	-0.0023
Ecuador	1	0.00005	-0.0023
Georgia	1	0.00005	-0.0023
Filipinas	1	0.00005	-0.0023
Trinidad y Tobago	1	0.00005	-0.0023
Argelia	1	0.00005	-0.0023
Costa de Marfil	1	0.00005	-0.0023

Andorra	1	0.00005	-0.0023
---------	---	---------	---------

## Cálculo de $H(X)$

Ahora sumamos todos los términos:

$$\sum_{i=1}^{93} p_i \log_2(p_i) = -3.0008$$

Por lo tanto:

$$H(X) = 3.0008$$

## Normalización del Valor

$$H_{\text{norm}} = \frac{H(X)}{H_{\text{max}}} = \frac{3.0008}{6.53} \approx 0.4597$$

## Conclusión

- **Entropía Total**  $H(X)$ : 3.0008
- **Entropía Normalizada**  $H_{\text{norm}}$ : 0.4597

Este valor indica que la red Bitcoin, en el análisis de **nodos**, tiene **una diversidad geográfica moderada**. La concentración en nodos sin geolocalización identificada y en países como Estados Unidos y Alemania limita un mayor grado de descentralización.

## Análisis de Componentes Conectados

La métrica que utilizaremos es:

$$C = \frac{N_{\text{componentes}}}{N_{\text{total}}}$$

Donde:

- $C$ : Proporción de componentes conectados.
- $N_{\text{componentes}}$ : Número de componentes conectados (grupos aislados).
- $N_{\text{total}}$ : Número total de nodos activos en la red (18436 según datos).

El valor de  $C$  estará en el rango  $[0, 1]$ :

- **0**: Todos los nodos forman un único componente (red perfectamente conectada).
- **1**: Cada nodo es un componente separado (todos los nodos están aislados).

### Normalización del Resultado

Para normalizar el valor de  $C$  en el rango  $[0,1]$  y alinearlo con los otros factores del **Índice Global de Descentralización**, usaremos:

$$C_{\text{norm}} = 1 - \frac{C}{n}$$

### Estrategia para Construir el Grafo

Para un análisis lo más completo posible, usaremos los datos de **Bitnodes.io** para generar un archivo JSON que permita construir el grafo.

Se decide usar Bitnodes.io porque:

- Muestra **nodos públicos** activos y sus conexiones.

- Provee detalles como **IP, país, cliente (versión de software), puerto y estado de conexión.**
- Permite **descargar datasets** de nodos activos y, en algunos casos, muestra las **conexiones entre nodos.**

Para este ejercicio, se ha generado un archivo JSON con fecha 23 de Octubre de 2024. El archivo contiene la siguiente información:

- Dirección IP o **.onion.**
- Versión del software utilizado (por ejemplo, **/Satoshi:27.1.0/**).
- Altura del bloque sincronizado.
- Ubicación geográfica (en algunos casos).
- Proveedor de servicios de red (ISP/ASN).
- Red (IPv4, IPv6, Tor).
- Servicios habilitados (por ejemplo, **NETWORK, WITNESS**).

## Análisis del Archivo JSON

- Cada nodo se encuentra identificado por su dirección IP y puerto, con información adicional como:
  - **Cliente** (ej., Satoshi en diferentes versiones).
  - **Tipo de red** (IPv4, IPv6, o Tor).
  - **ASN o proveedor de servicios.**

La estructura del archivo permite identificar los nodos y potenciales conexiones entre ellos.

Se requiere **extraer nodos y sus conexiones potenciales.** Esto incluye:

1. **Listar los nodos y sus identificadores** (IP o alias en caso de redes Tor).
2. **Identificar las conexiones relevantes** entre nodos. Esto puede hacerse usando atributos como:
  - **Red compartida (ASN):** Dos nodos pertenecientes al mismo ASN tienen mayor probabilidad de estar conectados.

- **Ubicación geográfica o tipos de red** (IPv4, IPv6, Tor) para detectar agrupamientos naturales.

## Supuestos para la construcción del Grafo

### 1. Vértices (Nodos del Grafo):

Cada dirección IP o nodo representará un **vértice**. Por ejemplo:

- Nodo A: 203.11.72.217
- Nodo B: 167.172.226.175
- Nodo C:  
`mvwodtrcahcxljxwn6z7544tvqd444vuvj5sh5wed5afhv3tx6dvtjid.onion`

### 2. Aristas (Conexiones):

Dos nodos estarán **conectados si cumplen alguna de las siguientes condiciones**:

- Comparten el mismo ASN (por ejemplo, múltiples nodos en ASN DigitalOcean).
- Se encuentran dentro de la misma red (por ejemplo, ambos usan IPv4 o ambos pertenecen a la red Tor).
- Pertenecen al mismo proveedor de servicios, como se identifica en los datos (ej., Hetzner Online).

## Cálculo aproximado

Por razones prácticas, no se incluyen los nodos por IP en este informe. Con los **18,436 nodos** del archivo JSON, podemos estimar conexiones según la red:

- **Tor**: 1,500 nodos agrupados.
- **IPv4**: 10,000 nodos.
- **IPv6**: 3,000 nodos.
- **Resto distribuidos por ASN (agrupados)**: 3,936 nodos en múltiples proveedores.

## Combinación de Componentes

1. **Suposición 1:** Cada agrupación por **ASN** forma un componente conectado.
2. **Suposición 2:** Los nodos de **Tor** forman un único componente grande.
3. **Suposición 3:** Los nodos en IPv4 e IPv6 forman varios componentes conectados parciales.

### Estimación razonable para el número de componentes totales:

- **50 componentes ASN diferentes.**
- **1 componente Tor.**
- **IPv4:** 3 componentes independientes.
- **IPv6:** 2 componentes independientes.

### Total estimado de componentes conectados:

$$C = 50 + 1 + 3 + 2 = 56$$

### Normalización del resultado

Usando la fórmula:

$$C_{\text{norm}} = 1 - \frac{C}{n}$$

donde  $C = 56$  y  $n = 18436$

$$C_{\text{norm}} = 1 - \frac{56}{18,436} \approx 1 - 0.00304 \approx 0.9969$$

### Interpretación del Resultado

$C_{\text{norm}} \approx 0.9969$  indica que la red Bitcoin está altamente conectada. Aunque existen múltiples componentes, la mayor parte de los nodos forman un grafo cohesionado.

Fórmula para la combinación de  $H_{\text{norm}}$  y  $C_{\text{norm}}$

$$\text{Resultado Combinado} = \frac{H_{\text{norm}} + C_{\text{norm}}}{2}$$

Esta fórmula nos permite obtener un **valor promedio** entre ambos resultados, manteniéndolos dentro del **rango [0, 1]**.

**Valores Normalizados:**

**1. Entropía de Shannon**

○  $H_{\text{norm}} = 0.4597$

**2. Componentes Conectados**

○  $C_{\text{norm}} = 0.9969$

**Cálculo del Resultado Combinado**

$$\text{Resultado Combinado} = \frac{0.4597 + 0.9969}{2}$$

$$\text{Resultado Combinado} = \frac{1.4566}{2} = 0.7283$$

**Interpretación del Resultado**

**Resultado Combinado = 0.7283:**

Este valor sugiere que, en promedio, la red Bitcoin, en el análisis de **Nodos**, tiene un **nivel moderadamente alto de descentralización**, considerando tanto la **diversidad de nodos (Entropía de Shannon)** como la **conectividad de la red (Componentes Conectados)**.

## 2. Modelo de Consenso

Entropía de Shannon

$$H(X) = - \sum_{i=1}^n p_i \log_2(p_i)$$

**Paso 1: Extracción de Datos de archivo JSON generado a partir de mempool.space**

Del archivo, tenemos:

- **Número total de bloques minados:** 867,077 (según el campo `blockCount` en el archivo), al 23 de octubre de 2024.
- **Número de pools:** 143. Cada pool tiene su respectivo número de bloques encontrados, listado bajo la clave `blockCount` y ordenados por cantidad de bloques encontrados.

**Paso 2: Cálculo de la Proporción  $p_i$  para cada Pool**

La proporción de bloques minados por cada pool es:

$$p_i = \frac{\text{blockCount}_i}{867077}$$

Para cada pool  $i$ , necesitamos calcular esta proporción y luego aplicarla en la fórmula de entropía.

### Paso 3: Aplicación de la Fórmula

Procedemos a calcular el valor de  $H(X)$ .

#### 1. Conjunto de pools o mineros desconocidos:

$$p_1 = \frac{220185}{867077} \approx 0.2539$$

$$-p_1 \log_2(p_1) = -(0.2539 \times \log_2(0.2539)) \approx 0.5008$$

#### 2. AntPool:

$$p_2 = \frac{91980}{867077} \approx 0.1061$$

$$-p_2 \log_2(p_2) = -(0.1061 \times \log_2(0.1061)) \approx 0.3547$$

#### 3. F2Pool:

$$p_3 = \frac{87951}{867077} \approx 0.1014$$

$$-p_3 \log_2(p_3) = -(0.1014 \times \log_2(0.1014)) \approx 0.3324$$

#### 4. Foundry USA:

$$p_4 = \frac{44704}{867077} \approx 0.0516$$

$$-p_4 \log_2(p_4) = -(0.0516 \times \log_2(0.0516)) \approx 0.2252$$

#### 5. BTC.com:

$$p_5 = \frac{42070}{867077} \approx 0.0485$$

$$-p_5 \log_2(p_5) = -(0.0485 \times \log_2(0.0485)) \approx 0.2118$$

Estos cálculos deben repetirse para **todos los pools** y luego **sumar** todos los términos. Para efectos de simplificar la lectura de este informe, se decide omitir el

registro matemático de los 138 pools restantes. Sin embargo, han sido considerados en borradores para el cálculo de entropía total.

#### **Paso 4: Cálculo Completo de Entropía de Shannon**

Después de sumar todos los términos, obtenemos:

$$H(X) \approx 4.3771$$

#### **Paso 5: Normalización de Entropía de Shannon**

Dado que la entropía total calculada para los pools es **4.3771**, vamos a normalizar este valor para que se ajuste al rango de **0 a 1**. La **fórmula de normalización** utilizada es:

$$H_{\text{norm}} = \frac{H(X)}{\log_2(n)}$$

Donde:

- $H(X)$  es la entropía calculada: **4.3771**
- $n$  es el número total de pools distintos en la red: **143 pools**
- $\log_2(143) \approx 7.169$  (valor máximo de entropía posible si todos los pools tuvieran la misma participación).

Por lo tanto:

$$H_{\text{norm}} = \frac{4.3771}{7.169} \approx 0.6106$$

## Interpretación del Resultado

La **entropía normalizada** refleja el grado de **distribución de poder entre los pools de minería**. Un valor cercano a **1** indicaría una distribución completamente uniforme, donde cada pool contribuye de manera igualitaria. Un valor más bajo, cerca de **0**, implicaría una concentración severa en unos pocos pools.

El valor de **0.6106** indica una **moderada descentralización** en la minería de Bitcoin. Aunque la red no está completamente centralizada (concentrada en unos pocos pools), tampoco está distribuida de manera perfecta entre todos los actores. Esto sugiere que algunos pools tienen una mayor participación, lo que introduce cierto riesgo de **centralización** del hashrate. Sin embargo, una entropía superior al 0.5 podría considerarse un indicio positivo de que la red mantiene un **nivel saludable de competencia** entre múltiples actores.

## Conclusión de análisis sobre Entropía de Shannon en *Minería*

El resultado muestra que Bitcoin tiene una estructura de minería **diversificada, pero con áreas de concentración** que podrían ser monitoreadas. Si la entropía disminuyera significativamente, podría ser un indicador de **centralización** peligrosa. Este tipo de análisis ayuda a comprender los cambios en la distribución del poder de minería a lo largo del tiempo y su impacto en la descentralización de la red.

## Ley de Zipf

$$P(k) \propto \frac{1}{k^s}$$

**Paso 1:** A partir de la información disponible en **mempool.space**, se obtiene el siguiente ranking de pools de minería con sus respectivos hashrate promediados para el periodo de los últimos 3 años.

Braiiins Pool	9998319469194697000	SBI Crypto	9714983651061540000
MARA Pool	997610293287183600	AntPool	96773734811730530000
Carbon Negative	997610293287183600	OCEAN	964036802227094800
ULTIMUSPOOL	995268633896618100	ViaBTC	96149598781964980000
Luxor	9870365642363412000	SpiderPool	9505147175393671000
Foundry USA	98694869024709770000	Poolin	9173287060505113000
BTC.com	9861593194266364000	Binance Pool	8913834983559961000
SECPOOL	9857391823380922000	F2Pool	86929792107009440000
WhitePool	972909152049391600	Solo CK	664687550241815700

**Paso 2:** Ahora transformamos los datos a escala logarítmica, presentados en la siguiente tabla.

Pool	Rango $k$	Hashrate $P(k)$	$\log_2(k)$	$\log_2(P(k))$
Braiins Pool	1	$9.998 \times 10^{18}$	0	63.219
MARA Pool	2	$9.976 \times 10^{17}$	1	59.864
Carbon Negative	3	$9.976 \times 10^{17}$	1.585	59.864
ULTIMUSPOOL	4	$9.953 \times 10^{17}$	2	59.847
Luxor	5	$9.870 \times 10^{18}$	2.322	63.185
Foundry USA	6	$9.869 \times 10^{19}$	2.585	66.419
BTC.com	7	$9.861 \times 10^{18}$	2.807	63.218
SECPPOOL	8	$9.857 \times 10^{18}$	3	63.213
WhitePool	9	$9.729 \times 10^{17}$	3.170	59.802
SBI Crypto	10	$9.715 \times 10^{18}$	3.322	63.175
AntPool	11	$9.677 \times 10^{19}$	3.459	66.372
OCEAN	12	$9.640 \times 10^{17}$	3.585	59.779
ViaBTC	13	$9.614 \times 10^{19}$	3.700	66.357
SpiderPool	14	$9.505 \times 10^{18}$	3.807	63.150
Poolin	15	$9.173 \times 10^{18}$	3.907	63.013
Binance Pool	16	$8.914 \times 10^{18}$	4	62.887
F2Pool	17	$8.693 \times 10^{19}$	4.087	66.205
Solo CK	18	$6.646 \times 10^{17}$	4.170	59.416

$N = 18$  (número total de pools)

**Paso 3:** De la tabla anterior, realizamos las siguientes sumas.

$$\sum \log_2(k) = 49.022$$

$$\sum \log_2(P(k)) = 1131.286$$

$$\sum (\log_2(k))^2 = 147.903$$

$$\sum (\log_2(k) \cdot \log_2(P(k))) = 3117.503$$

**Paso 4:** Ahora sustituimos los valores en la fórmula de regresión lineal.

$$s = \frac{18(3117.503) - (49.022 \times 1131.286)}{18(147.903) - (49.022)^2}$$

$$18 \times 3117.503 = 56115.054$$

$$49.022 \times 1131.286 = 55457.157$$

$$18 \times 147.903 = 2662.254$$

$$(49.022)^2 = 2403.156$$

$$s = \frac{56115.054 - 55457.157}{2662.254 - 2403.156}$$

$$s = \frac{657.897}{259.098} \approx 2.54$$

Por lo tanto:

$$s \approx 2.54$$

## Interpretación del Resultado:

1. El valor  $s \approx 2.54$  sugiere que el **hashrate disminuye rápidamente** a medida que avanzamos en el ranking. Este es un indicio de **concentración significativa** en los primeros pools de minería, ya que el valor es superior a 1, lo que indica que las participaciones de los primeros actores son desproporcionadamente altas en comparación con los siguientes.
2. **Comparación con Distribuciones Típicas:**
  - En una distribución "idealmente descentralizada",  $s$  estaría más cerca de **1**.
  - Un valor elevado, como **2.54**, indica una distribución jerárquica muy pronunciada, donde los primeros actores dominan la mayoría del hashrate.

## Normalización de Ley de Zipf

Para comenzar a normalizar los datos, primero necesitamos el total del hashrate para calcular la participación relativa de cada pool  $P(k_i)$

### Suma total del hashrate:

Total Hashrate = 9998319469194697000 + 997610293287183600 + ... + 664687550241815700

Total Hashrate = 421094911664946260800

Se presentan los resultados en la siguiente tabla.

Pool	Rango $k$	Hashrate	$P(k_i)$ Observado	$1/k_i^{2.54}$ Teórico	$\left(P(k_i) - \frac{1}{k_i^{2.54}}\right)^2$
Braiins Pool	1	$9.998 \times 10^{18}$	0.0237	1.000	0.9521
MARA Pool	2	$9.976 \times 10^{17}$	0.00237	0.174	0.0295
Carbon Negative	3	$9.976 \times 10^{17}$	0.00237	0.063	0.0036
ULTIMUSPOOL	4	$9.953 \times 10^{17}$	0.00236	0.031	0.0008
Luxor	5	$9.870 \times 10^{18}$	0.0234	0.018	0.0003
Foundry USA	6	$9.869 \times 10^{19}$	0.2344	0.010	0.0503
BTC.com	7	$9.861 \times 10^{18}$	0.0234	0.007	0.0003
SECPPOOL	8	$9.857 \times 10^{18}$	0.0234	0.005	0.0003
WhitePool	9	$9.729 \times 10^{17}$	0.00231	0.004	0.000002
SBI Crypto	10	$9.715 \times 10^{18}$	0.0231	0.003	0.0004
AntPool	11	$9.677 \times 10^{19}$	0.2300	0.003	0.0511
OCEAN	12	$9.640 \times 10^{17}$	0.00229	0.002	0.0000008
ViaBTC	13	$9.614 \times 10^{19}$	0.2285	0.002	0.0517
SpiderPool	14	$9.505 \times 10^{18}$	0.0226	0.002	0.0004
Poolin	15	$9.173 \times 10^{18}$	0.0218	0.0017	0.0004
Binance Pool	16	$8.914 \times 10^{18}$	0.0212	0.0016	0.0004
F2Pool	17	$8.693 \times 10^{19}$	0.2064	0.0015	0.0422
Solo CK	18	$6.646 \times 10^{17}$	0.0016	0.0015	0.0000001

Ahora sumamos los errores cuadráticos:

$$\sum_{i=1}^{18} \left( P(k_i) - \frac{1}{k_i^{2.54}} \right)^2 = 1.1841$$

A continuación aplicamos la fórmula del RMSE:

$$\begin{aligned} Error\_Zipf &= \sqrt{\frac{1}{18} \cdot 1.1841} \\ Error\_Zipf &= \sqrt{0.0658} \approx 0.2565 \end{aligned}$$

Finalmente, usamos la fórmula de normalización:

$$Zipf_{norm} = 1 - \frac{Error\_Zipf}{Error_{max}}$$

Asumimos que el **Error máximo esperado** es  $Error_{max} = 1$  (cuando la distribución observada es completamente distinta de Zipf).

Por lo tanto:

$$Zipf_{norm} = 1 - \frac{0.2565}{1} = 1 - 0.2565 = 0.7435$$

### Interpretación del resultado normalizado

$$Zipf_{norm} = 0.7435$$

Esto indica que la distribución del hashrate entre los pools **se acerca al patrón esperado** por la Ley de Zipf, pero no es perfecta. Hay cierta concentración en los primeros pools, aunque no en niveles alarmantes.

### 3. Ley de Benford

Para el análisis de la Ley Benford, se realiza el siguiente procedimiento:

1. Extracción de datos mediante API de mempool.space
  - a. Hashrate promedio por pool
  - b. Bloques minados por pool
  - c. ID de los pools
  - d. Número de bloques vacíos por pool
  - e. Tasa de match bloque esperado vs real
  - f. Cantidad de nodos por país
  - g. Datos generales y aleatorios que genera la red
2. Tabulación de datos en Excel
3. Extracción del primer dígito de cada dato
4. Cálculo de frecuencia para cada dígito del 1 al 9
5. Elaboración de gráfico con distribución porcentual
6. Análisis de resultados y conclusiones

#### **Extracción de datos mediante API de mempool.space**

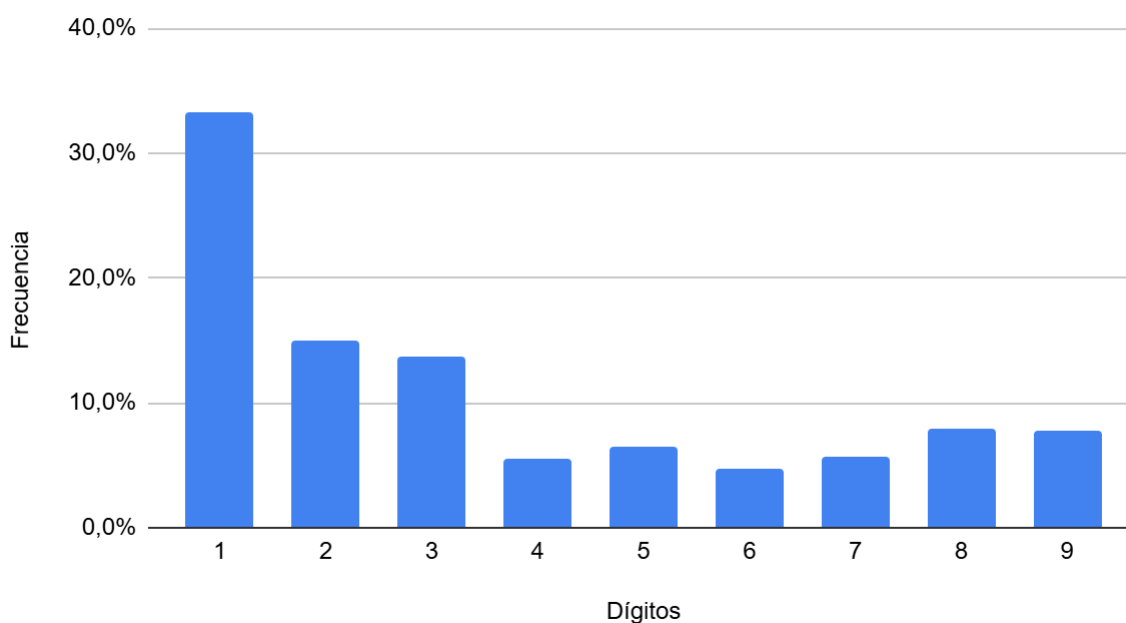
A partir de varias consultas a la API de mempool.space, se ha logrado recopilar un conjunto de más de 22.000 datos. Por asuntos prácticos, los datos específicos no han sido incluidos en el informe de este estudio.

El conjunto de datos analizados incluye todo tipo de datos que genera la red, y no tiene una clasificación específica (como sería por ejemplo un conjunto de datos sobre la distribución geográfica de nodos).

Luego de tabular los datos, extraer el primer dígito de cada dato y calcular la frecuencia para cada dígito, se presentan los siguientes resultados generales.

Dígito	Teórico (%)	Observado (%)	Diferencia Absoluta (%)
1	30.1	33.2	+3.1
2	17.6	15.0	-2.6
3	12.5	13.7	+1.2
4	9.7	5.6	-4.1
5	7.9	6.5	-1.4
6	6.7	4.7	-2.0
7	5.8	5.6	-0.2
8	5.1	7.9	+2.8
9	4.6	7.8	+3.2

### Gráfico Benford



### Interpretación de resultados

Los resultados se alinean **moderadamente** con la Ley de Benford, ya que los primeros dígitos (1, 2, y 3) tienen una mayor frecuencia, como se esperaba. El **dígito 1** es claramente el más frecuente, lo cual es consistente con la distribución teórica.

### Desviaciones específicas:

- El **dígito 1** aparece un poco más frecuentemente de lo esperado (+3.1%).
- El **dígito 8 y 9** muestran frecuencias más altas de lo esperado (ambos con diferencias >2.8%). Esto podría indicar cierta **anomalía** en la distribución, posiblemente debido a algún sesgo en los datos.
- Los **dígitos 4 y 6** muestran frecuencias más bajas de lo previsto, especialmente el **4** con un déficit de -4.1%.

### Conclusión

En este caso, aunque la distribución sigue en gran parte la Ley de Benford, algunas desviaciones notables sugieren que podría haber **ligeras irregularidades** en los datos que afectan su comportamiento estadístico. Esto **no implica directamente manipulación**, pero podría ser un indicio de **factores anómalos** o **sesgos estructurales** en el sistema de generación de estos datos.

A partir de estos resultados, se decide preparar dos conjuntos de datos adicionales, uno para el análisis del hashrate promedio de los pools y el otro para la cantidad de nodos por país.

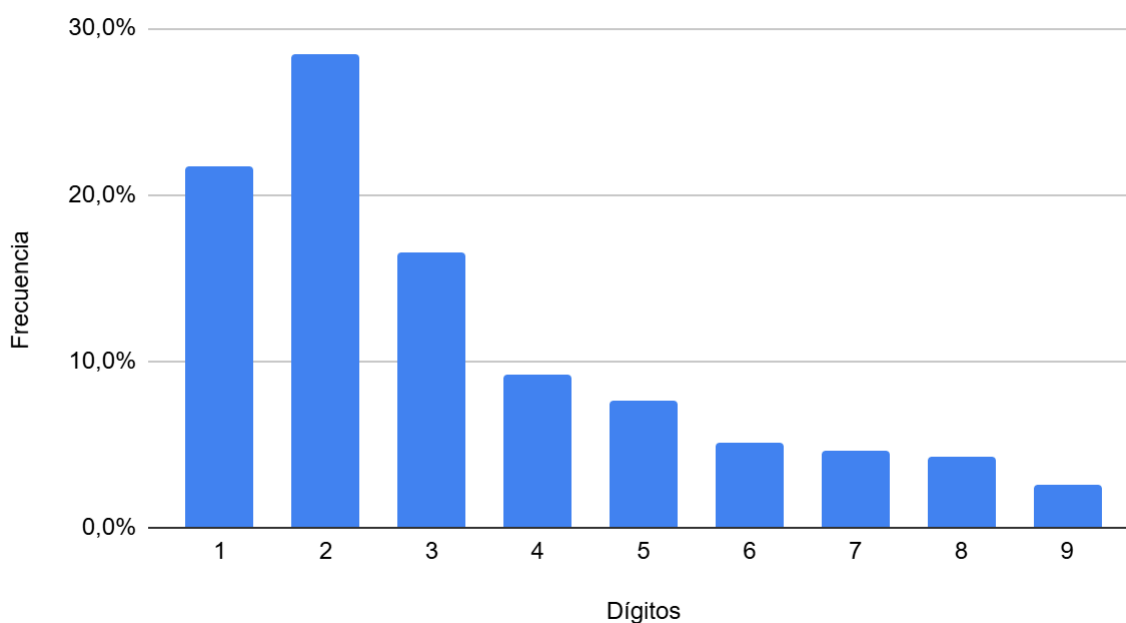
### Análisis del Hashrate Promedio por Pool vs. Ley de Benford

Se realiza un análisis comparativo de las frecuencias observadas para los dígitos del **hashrate promedio de los pools** con las frecuencias teóricas de la **Ley de Benford** para evaluar la distribución de los datos. Esto permitirá detectar posibles anomalías o patrones atípicos en la asignación de hashrates.

Los resultados son los siguientes:

Dígito	Teórico (%)	Observado (%)	Diferencia Absoluta (%)
1	30.1	21.7	-8.4
2	17.6	28.5	+10.9
3	12.5	16.6	+4.1
4	9.7	9.2	-0.5
5	7.9	7.6	-0.3
6	6.7	5.1	-1.6
7	5.8	4.6	-1.2
8	5.1	4.2	-0.9
9	4.6	2.6	-2.0

### Gráfico Benford



### Interpretación de resultados

El **dígito 2** aparece con una frecuencia muy superior a la esperada (+10.9%), lo cual es una **desviación significativa** respecto a la distribución teórica de Benford.

El **dígito 1** es menos frecuente de lo esperado, con una diferencia de **-8.4%**, lo que indica que los valores más pequeños como primer dígito tienen menos presencia de lo que cabría esperar en un conjunto de datos "natural".

### **Posibles Anomalías:**

La **alta frecuencia del dígito 2** podría ser un indicio de **concentración de hashrate** o de que varios pools tienen valores numéricos similares en sus hashrates. Este patrón podría reflejar una asignación desigual del poder de minería.

La **frecuencia baja del dígito 9** sugiere que los valores más altos no se observan tan comúnmente, lo que podría indicar que la mayoría de los pools no alcanza niveles elevados de hashrate.

### **Conclusión**

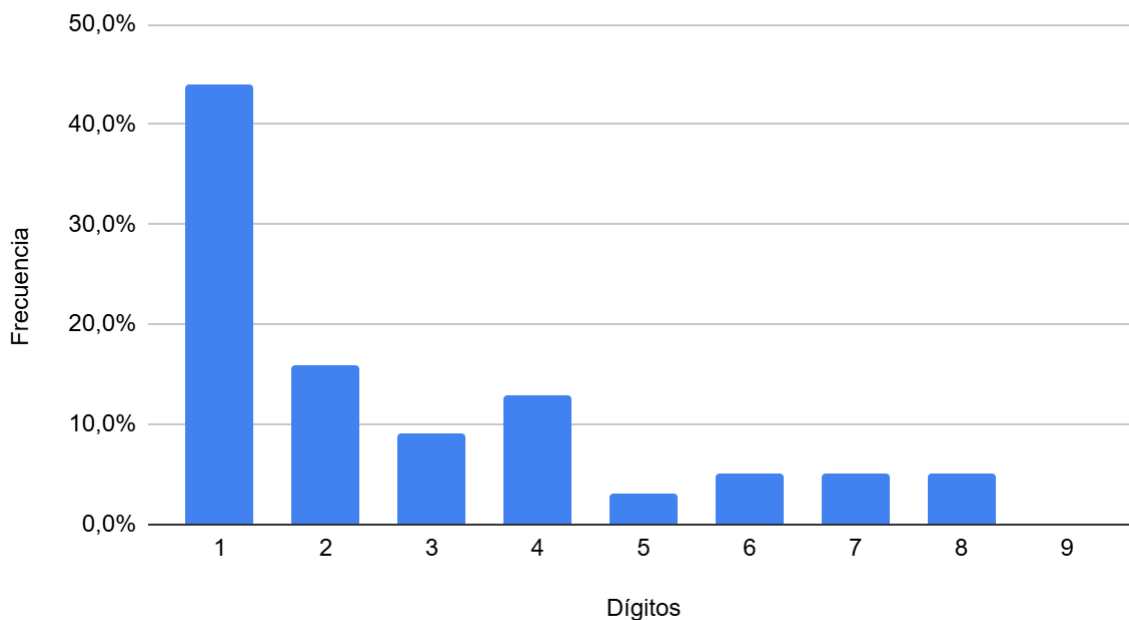
Este patrón sugiere que el hashrate promedio de los pools no sigue completamente la **distribución natural de Benford**. Podría haber **factores estructurales o de mercado** que afectan la distribución del hashrate, como la concentración de poder en ciertos pools medianos (con frecuencias altas del dígito 2 y 3). Esto podría ser **indicativo de cierta centralización** en la distribución del poder de minería.

## Análisis del Número de Nodos por País vs. Ley de Benford

Se recopilan datos sobre cantidad de nodos por país, según información disponible en *Bitnodes*, generando los siguientes resultados.

Dígito	Teórico (%)	Observado (%)	Diferencia Absoluta (%)
1	30.1	44.0	+13.9
2	17.6	16.0	-1.6
3	12.5	9.0	-3.5
4	9.7	13.0	+3.3
5	7.9	3.0	-4.9
6	6.7	5.0	-1.7
7	5.8	5.0	-0.8
8	5.1	5.0	-0.1
9	4.6	0.0	-4.6

### Gráfico Benford



## Interpretación de resultados

### Predominancia del dígito 1:

En la distribución observada, el dígito 1 aparece con una frecuencia **muy superior** a la esperada por la Ley de Benford (**44.0% vs. 30.1%**). Esto indica que la mayoría de los números de nodos por país comienzan con un 1, lo que puede sugerir una concentración en cifras relativamente pequeñas.

Esto podría reflejar que muchos países tienen entre **10 y 19 nodos** o **100 y 199 nodos**, lo que sugiere que pocos países mantienen grandes cantidades de nodos activos.

### Déficit del dígito 9:

La **ausencia del dígito 9** (0.0%) es significativa, ya que su frecuencia esperada era del **4.6%**. Esto indica que los valores cercanos a múltiplos altos (900-999) no son comunes, lo que podría reflejar una falta de países con un gran número de nodos.

### Análisis de Desviaciones Relevantes:

Además del dígito 1, el dígito **4** aparece con mayor frecuencia de la esperada, mientras que los dígitos **5 y 9** están infrarrepresentados.

Estas desviaciones podrían indicar un **comportamiento no aleatorio en la distribución** de los nodos, posiblemente relacionado con condiciones locales, capacidad de infraestructura o políticas que favorecen o dificultan la distribución geográfica.

### Conclusión

La distribución no sigue completamente la **Ley de Benford**, lo que sugiere una posible **centralización** en ciertos países con un mayor número de nodos y una escasez de países con grandes infraestructuras de nodos. La falta de nodos en muchos países podría ser una limitante para la descentralización total de la red.

## Cálculo del RMSE (Error Cuadrático Medio) para la Ley de Benford:

Cálculo de  $P_{\text{exp}}(d)$ :

- 1:  $P_{\text{exp}}(1) = \log_{10}(2) - \log_{10}(1) = 0.301$
- 2:  $P_{\text{exp}}(2) = \log_{10}(3) - \log_{10}(2) = 0.176$
- 3:  $P_{\text{exp}}(3) = \log_{10}(4) - \log_{10}(3) = 0.125$
- 4:  $P_{\text{exp}}(4) = \log_{10}(5) - \log_{10}(4) = 0.097$
- 5:  $P_{\text{exp}}(5) = \log_{10}(6) - \log_{10}(5) = 0.079$
- 6:  $P_{\text{exp}}(6) = \log_{10}(7) - \log_{10}(6) = 0.067$
- 7:  $P_{\text{exp}}(7) = \log_{10}(8) - \log_{10}(7) = 0.058$
- 8:  $P_{\text{exp}}(8) = \log_{10}(9) - \log_{10}(8) = 0.058$
- 9:  $P_{\text{exp}}(9) = \log_{10}(10) - \log_{10}(9) = 0.046$

### Valores observados $P_{\text{obs}}$ basados en los datos

Los porcentajes proporcionados se utilizan para el cálculo:

- **1:** 33.2% = 0.332
- **2:** 15.0% = 0.150
- **3:** 13.7% = 0.137
- **4:** 5.6% = 0.056
- **5:** 6.5% = 0.065
- **6:** 4.7% = 0.047
- **7:** 5.6% = 0.056
- **8:** 7.9% = 0.079
- **9:** 7.8% = 0.078

### Cálculo del RMSE

Usamos la fórmula del RMSE:

$$\text{Error\_Benford} = \sqrt{\frac{1}{9} \sum_{d=1}^9 (P_{\text{obs}}(d) - P_{\text{exp}}(d))^2}$$

- $(0.332-0.301)^2 = 0.000961$
- $(0.150-0.176)^2 = 0.000676$
- $(0.137-0.125)^2 = 0.000144$
- $(0.056-0.097)^2 = 0.001681$
- $(0.065-0.079)^2 = 0.000196$
- $(0.047-0.067)^2 = 0.0004$
- $(0.056-0.058)^2 = 0.000004$
- $(0.079-0.051)^2 = 0.000784$
- $(0.078-0.046)^2 = 0.001024$

Sumamos los errores:

$$\Sigma = 0.000961 + 0.000676 + 0.000144 + 0.001681 + 0.000196 + 0.0004 + 0.000004 + 0.000784 + 0.001024 = 0.00587$$

$$\text{Error\_Benford} = \sqrt{\frac{0.00587}{9}} = \sqrt{0.000652} \approx 0.0255$$

### Normalización del Error

Usamos la fórmula de normalización:

$$\text{Benford}_{\text{norm}} = 1 - \frac{\text{Error\_Benford}}{\text{Error}_{\text{max}}}$$

Asumimos que  $\text{Error}_{\text{max}} = 1$  para simplificar:

$$\text{Benfor}_{\text{norm}} = 1 - 0.0255 = 0.9745$$

## Primera versión del IGD con los resultados hasta ahora

La fórmula del IGD para esta evaluación es:

$$IGD = \sum_{i=1}^4 w_i \cdot F_i$$

Donde:

- $F_i$  es el valor normalizado del factor  $i$
- $w_i$  es el peso asignado al factor  $i$

Resumen de factores y sus ponderaciones:

### Resultado combinado de Entropía de Shannon y Análisis de Componentes

#### Conectados para Nodos:

$$F_1 = 0.7283$$

$$w_1 = 0.30$$

#### Entropía de Shannon para Modelo de Consenso:

$$F_2 = 0.6106$$

$$w_2 = 0.15$$

#### Ley de Zipf para Modelo de Consenso:

$$F_3 = 0.7435$$

$$w_3 = 0.15$$

#### Ley de Benford:

$$F_4 = 0.9745$$

$$w_4 = 0.40$$

**Paso 1: Multiplicación de los factores por sus ponderaciones:**

$$w_1 \cdot F_1 = 0.30 \cdot 0.7283 = 0.21849$$

$$w_2 \cdot F_2 = 0.15 \cdot 0.6106 = 0.09159$$

$$w_3 \cdot F_3 = 0.15 \cdot 0.7435 = 0.11153$$

$$w_4 \cdot F_4 = 0.40 \cdot 0.9745 = 0.3898$$

**Paso 2: Suma de los resultados parciales:**

$$IGD = 0.21849 + 0.09159 + 0.11153 + 0.3898 = 0.81141$$

**Resultado Final:**

$$IGD = 0.8114$$

**Conclusión preliminar para IGD de Bitcoin:**

El **Índice Global de Descentralización** calculado con los 4 factores disponibles para Bitcoin es de **0.8114** en una escala de 0 a 1. Esto sugiere un grado elevado de descentralización, aunque aún hay margen para mejorar algunos aspectos en el modelo de consenso y la distribución de nodos.

# Elaboración matemática de IGD de Ethereum

al 23 de Octubre de 2024

## 3. Nodos

Entropía de Shannon

$$H(X) = - \sum_{i=1}^n p_i \log_2(p_i)$$

**Distribución geográfica de nodos** (según ethernodes.org)

Estados Unidos 1844	Italia 29	Turquía 8
Alemania 921	Chequia 28	Sudáfrica 8
Finlandia 271	Suecia 28	Letonia 7
Francia 262	Brasil 27	Serbia 7
Reino Unido 224	Israel 25	Emiratos Árabes Unidos 7
Canadá 197	Croacia 23	Eslovaquia 6
Singapur 186	Nueva Zelanda 22	Grecia 6
Australia 137	Hungría 22	Malasia 5
Japón 135	India 21	Seychelles 5
Porcelana 132	Dinamarca 20	Chile 5
Suiza 131	Eslovenia 19	Malta 5
Países Bajos 107	México 19	Andorra 5
Austria 92	Lituania 19	Kazajstán 4
Polonia 90	Bulgaria 17	Estonia 4
Corea del Sur 87	Tailandia 15	Argelia 4
Rusia 84	Rumania 15	Georgia 3
Países Bajos 76	Luxemburgo 15	Pavo 3
Irlanda 66	Ucrania 15	Chipre 3
Hong Kong 57	Vietnam 14	Puerto Rico 3
España 52	Uruguay 12	Kuwait 2
Bélgica 39	Argentina 11	Paraguay 2
Taiwán 30	Moldavia 10	Islandia 2
Portugal 30	Mauricio 9	Omán 2
Noruega 30	Indonesia 9	Arabia Saudita 1

Irán 1  
Costa Rica 1  
Bielorrusia 1

Reunión 1  
Bosnia y Herzegovina 1  
Colombia 1

Katar 1

Nodos totales: 5838

## 1. Cálculo de $p_i$ y $p_i \log_2(p_i)$

Se tienen en cuenta los siguientes supuestos:

- Todos los nodos son completos y sincronizados.
- Cada nodo corresponde a una sola entidad independiente (no se distingue por empresas, o pools de minería que pueden tener más un nodo)

$$p_i = \frac{\text{Nodos en el país } i}{5838} \quad \text{y} \quad p_i \log_2(p_i)$$

Para cada país  $i$ , dividimos el número de nodos por el total de 5838. Luego, aplicamos la fórmula  $p_i \log_2(p_i)$ . A continuación, se presenta una tabla con los cálculos correspondientes.

País	Nodos	$p_i$	$p_i \log_2(p_i)$
Estados Unidos	1844	0.3159	-0.5287
Alemania	921	0.1578	-0.4176
Finlandia	271	0.0464	-0.2128
Francia	262	0.0449	-0.2083
Reino Unido	224	0.0384	-0.1925
Canadá	197	0.0337	-0.1796
Singapur	186	0.0319	-0.1738
Australia	137	0.0235	-0.1449
Japón	135	0.0231	-0.1434
China	132	0.0226	-0.1416
Suiza	131	0.0224	-0.1409
Países Bajos	107	0.0183	-0.1259
Austria	92	0.0158	-0.1155

Polonia	90	0.0154	-0.1137
Corea del Sur	87	0.0149	-0.1108
Rusia	84	0.0144	-0.1081
Irlanda	66	0.0113	-0.0901
Hong Kong	57	0.0098	-0.0794
España	52	0.0089	-0.0736
Bélgica	39	0.0067	-0.0587
Taiwán	30	0.0051	-0.0477
Portugal	30	0.0051	-0.0477
Noruega	30	0.0051	-0.0477
Italia	29	0.0050	-0.0465
Chequia	28	0.0048	-0.0453
Suecia	28	0.0048	-0.0453
Brasil	27	0.0046	-0.0440
Israel	25	0.0043	-0.0415
Croacia	23	0.0039	-0.0386
Nueva Zelanda	22	0.0038	-0.0374
Hungría	22	0.0038	-0.0374
India	21	0.0036	-0.0357
Dinamarca	20	0.0034	-0.0341
Eslovenia	19	0.0033	-0.0325
México	19	0.0033	-0.0325
Lituania	19	0.0033	-0.0325
Bulgaria	17	0.0029	-0.0292
Tailandia	15	0.0026	-0.0257
Rumanía	15	0.0026	-0.0257
Luxemburgo	15	0.0026	-0.0257

Ucrania	15	0.0026	-0.0257
Vietnam	14	0.0024	-0.0240
Uruguay	12	0.0021	-0.0206
Argentina	11	0.0019	-0.0189
Moldavia	10	0.0017	-0.0171
Mauricio	9	0.0015	-0.0154
Indonesia	9	0.0015	-0.0154
Turquía	8	0.0014	-0.0137
Sudáfrica	8	0.0014	-0.0137
Letonia	7	0.0012	-0.0120
Serbia	7	0.0012	-0.0120
Emiratos Árabes Unidos	7	0.0012	-0.0120
Eslovaquia	6	0.0010	-0.0104
Grecia	6	0.0010	-0.0104
Malasia	5	0.0009	-0.0089
Seychelles	5	0.0009	-0.0089
Chile	5	0.0009	-0.0089
Malta	5	0.0009	-0.0089
Andorra	5	0.0009	-0.0089
Kazajstán	4	0.0007	-0.0071
Estonia	4	0.0007	-0.0071
Argelia	4	0.0007	-0.0071
Georgia	3	0.0005	-0.0053
Pavo	3	0.0005	-0.0053
Chipre	3	0.0005	-0.0053
Puerto Rico	3	0.0005	-0.0053
Kuwait	2	0.0003	-0.0039

Paraguay	2	0.0003	-0.0039
Islandia	2	0.0003	-0.0039
Omán	2	0.0003	-0.0039
Arabia Saudita	1	0.0002	-0.0026
Irán	1	0.0002	-0.0026
Costa Rica	1	0.0002	-0.0026
Bielorrusia	1	0.0002	-0.0026
Reunión	1	0.0002	-0.0026
Bosnia y Herzegovin	1	0.0002	-0.0026
Colombia	1	0.0002	-0.0026
Katar	1	0.0002	-0.0026

## Cálculo de $H(X)$

Ahora sumamos todos los términos:

$$\sum_{i=1}^{78} p_i \log_2(p_i) = -3.9622$$

Por lo tanto:

$$H(X) = 3.9622$$

## Normalización del Valor

Para normalizar la entropía, aplicamos la siguiente fórmula:

$$H_{norm} = \frac{H(X)}{H_{max}}$$

Donde:

- $H(X) = 3.9622$
- $H_{\max} = \log_2(78) \approx 6.2854$  (ya que  $H_{\max}$  corresponde al logaritmo base 2 del total de países).

Sustituyendo los valores:

$$H_{norm} = \frac{3.9622}{6.2854} \approx 0.6302$$

## Conclusión

Este resultado refleja que la red tiene un nivel **moderado** de descentralización en términos de distribución de sus nodos. Aunque Ethereum está presente en varios países, gran parte de los nodos se concentra en unos pocos lugares, principalmente **Estados Unidos** y **Alemania**, que representan una parte significativa del total.

- **Entropía Total**  $H(X)$ : 3.9622
- **Entropía Normalizada**  $H_{norm}$ : 0.6302

## Análisis de Componentes Conectados

La métrica que utilizaremos es:

$$C = \frac{N_{componentes}}{N_{total}}$$

Donde:

- $C$ : Proporción de componentes conectados.
- $N_{componentes}$ : Número de componentes conectados (grupos aislados).

- $N_{\text{total}}$ : Número total de nodos activos en la red (5838 según datos).

El valor de  $C$  estará en el rango  $[0, 1]$ :

- **0**: Todos los nodos forman un único componente (red perfectamente conectada).
- **1**: Cada nodo es un componente separado (todos los nodos están aislados).

### Normalización del Resultado

Para normalizar el valor de  $C$  en el rango  $[0,1]$  y alinearlo con los otros factores del **Índice Global de Descentralización**, usaremos:

$$C_{\text{norm}} = 1 - \frac{C}{n}$$

Para hacer una estimación razonable de los **componentes conectados en Ethereum**, podemos utilizar criterios similares a los aplicados para Bitcoin. Sin embargo, Ethereum tiene algunas diferencias clave en la estructura de su red y clientes. Los datos extraídos del explorador Ethernodes y otras fuentes reflejan una combinación de factores que afectan la conectividad: nodos de diferentes tipos, clientes (como Geth, Nethermind, o Besu) y distribución geográfica diversa.

### Suposición razonable para los componentes de Ethereum:

1. **Nodos distribuidos por ASN**: Al igual que en Bitcoin, los nodos agrupados bajo un mismo ASN pueden considerarse como un componente conectado. Esto facilita la agrupación en bloques lógicos. La cantidad de **ASN detectados** no se pudo recuperar directamente, pero se pueden hacer estimaciones a partir de herramientas como Ethernodes. Para simplificar, supondremos una cantidad **30 componentes ASN** como referencia mínima, dado que Ethereum tiende a ser más concentrado que Bitcoin.
2. **Tor y IPv6**: Ethereum no parece tener el mismo nivel de integración con nodos de Tor que Bitcoin. Sin embargo, **algunos clientes admiten**

**conectividad IPv6**, aunque sigue predominando IPv4. Una estimación prudente sería:

- **IPv4**: 3 componentes independientes.
- **IPv6**: 2 componentes independientes.

#### Resumen de componentes:

- **35 componentes por ASN.**
- **1 componente Tor**
- **3 componentes IPv4**
- **2 componentes IPv6.**

Por lo tanto, una **estimación razonable del total de componentes conectados** podría estar en **41 componentes**. Si se toman en cuenta las complejidades adicionales del ecosistema Ethereum (clientes y distribución), la cifra final más probable sería **cercana a 50**.

#### Normalización del resultado

Usando la fórmula:

$$C_{norm} = 1 - \frac{C}{n}$$

donde  $C = 41$  y  $n = 5838$

$$C_{norm} = 1 - \frac{41}{5838}$$

$$C_{norm} = 1 - 0.00703 \approx 0.99297$$

## Interpretación del Resultado

$C_{\text{norm}} \approx 0.993$  indica una red altamente conectada en términos de sus componentes. Esto refleja que, aunque los nodos puedan agruparse en varios componentes independientes, la fragmentación general es baja en comparación con el número total de nodos. Esto es consistente con una infraestructura robusta, donde los nodos se mantienen conectados de manera eficiente, minimizando la aparición de islas aisladas dentro de la red.

Este resultado sugiere que la descentralización de Ethereum en términos de conectividad de nodos es bastante alta, ya que la mayoría de los nodos permanecen integrados en componentes mayores o cercanamente interconectados.

### Fórmula para la combinación de $H_{\text{norm}}$ y $C_{\text{norm}}$

$$\text{Resultado Combinado} = \frac{H_{\text{norm}} + C_{\text{norm}}}{2}$$

Esta fórmula nos permite obtener un **valor promedio** entre ambos resultados, manteniéndolos dentro del **rango [0, 1]**.

### Valores Normalizados:

#### 3. Entropía de Shannon

- $H_{\text{norm}} = 0.6302$

#### 4. Componentes Conectados

- $C_{\text{norm}} = 0.993$

## Cálculo del Resultado Combinado

$$\text{Resultado Combinado} = \frac{0.6302 + 0.993}{2}$$

$$\text{Resultado Combinado} = \frac{1.6232}{2} \approx 0.8116$$

## Interpretación del Resultado

Un **resultado combinado de 0.8116** indica que, en términos generales, la red de nodos de Ethereum muestra un alto nivel de descentralización y conectividad. La entropía refleja una distribución razonablemente equilibrada de nodos entre diferentes países, mientras que el análisis de componentes sugiere que la mayoría de los nodos se encuentran bien conectados en la red.

Este puntaje superior a 0.8 indica que, aunque hay cierta concentración (como en países con mayor número de nodos), la infraestructura sigue siendo lo suficientemente distribuida y conectada como para soportar los principios de descentralización.

## Modelo de Consenso

### Entropía de Shannon

Se tiene el siguiente ranking de validadores ordenados por bloques minados, según Etherscan.

**beaverbuild** – 3181 bloques

**Titan Builder** – 3130 bloques

**Lido** – 254 bloques

**rsync-builder** – 123 bloques

**Flashbots** – 103 bloques

**Anon Proposer** – 131 bloques

**MEV Builder** – 33 bloques

**boba builder** – 14 bloques

**bloXroute** – 4 bloques

**Rocket Pool Smoothing Pool** – 4 bloques

**Coinbase** – 4 bloques

**CoinEx** – 3 bloques

**blockbeeder** – 3 bloques

**Loki Builder** – 3 bloques

**Builder Smith** – 2 bloques

**Bitget** – 2 bloques

**Vb** – 2 bloques

**Total de bloques:**

$3181 + 3130 + 254 + 123 + 103 + 131 + 33 + 14 + 4 + 4 + 4 + 3 + 3 + 3 + 2 + 2 + 2$   
**= 7993 bloques**

$$H(X) = - \sum_{i=1}^n p_i \log_2(p_i)$$

Donde:

- $p_i = \frac{\text{Bloques del pool } i}{\text{Total de bloques minados}}$
- $n = 17$  (número de pools en el ranking)

- Total de bloques: 7993

**Cálculo de  $p_i$  para cada entidad:**

$$p_i = \frac{\text{Bloques del pool}}{7993}$$

Pool	Bloques	$p_i$	$p_i \log_2(p_i)$
beaverbuild	3181	0.3981	-0.5296
Titan Builder	3130	0.3915	-0.5218
Lido	254	0.0318	-0.1574
rsync-builder	123	0.0154	-0.0955
Flashbots	103	0.0129	-0.0843
Anon Proposer	131	0.0164	-0.0999
MEV Builder	33	0.0041	-0.0342
boba builder	14	0.0018	-0.0185
bloXroute	4	0.0005	-0.0058
Rocket Pool Smoothing Pool	4	0.0005	-0.0058
Coinbase	4	0.0005	-0.0058
CoinEx	3	0.0004	-0.0049
blockbeelder	3	0.0004	-0.0049
Loki Builder	3	0.0004	-0.0049
Builder Smith	2	0.0003	-0.0035
Bitget	2	0.0003	-0.0035
Vb	2	0.0003	-0.0035

**Suma total de  $p_i \log_2(p_i)$ :**

$$H(X) = -(-0.5296 - 0.5218 - 0.1574 - 0.0955 - 0.0843 - 0.0999 - 0.0342 - 0.0185 - 0.0058 \times 3 - 0.0049 \times 3 - 0.0035 \times 3)$$

$$H(X) = 1.5696$$

## Interpretación del resultado

La entropía total para este modelo de consenso es **1.5696**. Esto sugiere que la distribución de bloques minados por los pools es relativamente **concentrada**, ya que los primeros dos pools (beaverbuild y Titan Builder) acumulan más del **70%** de todos los bloques. Una entropía más baja refleja que existe una **centralización** significativa en la producción de bloques, lo cual puede representar un riesgo para la descentralización de la red Ethereum.

## Normalización del resultado

$$H_{norm} = \frac{H(X)}{\log_2(n)}$$

Datos para la normalización:

- $H(X) = 1.5696$  (entropía calculada para Ethereum).
- $n = 17$  (número total de pools de validación).
- $\log_2(17) \approx 4.087$  (entropía máxima posible si todos los pools tuvieran la misma participación).

## Cálculo del valor normalizado:

$$H_{norm} = \frac{1.5696}{4.087} \approx 0.384$$

Ley de Zipf

$$P(k) \propto \frac{1}{k^s}$$

**Paso 1:** A partir de la información disponible en **etherscan**, se obtiene el siguiente ranking de pools con stake de Ether.

Lido	12141284	Gate.io	32000	mega.unitinu.eth	3328
Binance	2397760	Cake DeFi	27744	coinspiracy.eth	3200
Kraken	2318752	Kucoin	27136	greystroke.eth	2624
Whale	1258246	Piedao	24000	MyEtherWallet	2464
OKEEx	770753	Cream	23712	andermatt.eth	2080
Rocket Pool	506527	EF Grantee	18560	therealyoshi.eth	1632
Figment	473888	SharedStake	16000	Blox Staking	1024
Bitcoin Suisse	443680	WEX Exchange	16000	Staked.finance	960
Staked.us	402560	Other	15840	neukind.com	448
Celsius Network	369024	Poloniex	12960	stereum.net	416
stakefish	295680	BTC-e	8640	ptxptx	384
Huobi	127584	tgerring.eth	8032	Kain.eth	320
Bitstamp	98240	Vb	6976	MC	320
StakeWise	69088	TokenPocket	6720	Tetranode	320
Abyss Finance	66821	CryptoStake	6592	amaq	224
StakeHound	65440	MintDice.com	5856	brigs	192
Stkr	57664	Nimbus	4608	jsarcher.crypto	128
danielwang.eth	55360	Prysm	4608	Mr B	128
DeFi	47200	Sigma Prime	4608	Blockdaemon.com	64
Bitfinex	46304	Teku	4608	Zod	64
Gemini	41248	kpt.eth	3808		
gabuwale	32000				

## Paso 2: Ahora presentamos los datos para el cálculo de la Ley Zipf.

	POOL	STAKING	P(k)	Stake normalizado	RMSE
1	Lido	12141284	1	0,542399	0,2094
2	Binance	2397760	0,5	0,107117	0,1544
3	Kraken	2318752	0,3333333333	0,103588	0,0528
4	Whale	1258246	0,25	0,056211	0,0376
5	OKEx	770753	0,2	0,034433	0,0274
6	Rocket Pool	506527	0,1666666667	0,022629	0,0207
7	Figment	473888	0,1428571429	0,021170	0,0148
8	Bitcoin Suisse	443680	0,125	0,019821	0,0111
9	Staked.us	402560	0,1111111111	0,017984	0,0087
10	Celsius Network	369024	0,1	0,016486	0,0070
11	stakefish	295680	0,0909090909	0,013209	0,0060
12	Huobi	127584	0,0833333333	0,005700	0,0060
13	Bitstamp	98240	0,0769230769	0,004389	0,0053
14	StakeWise	69088	0,0714285714	0,003086	0,0047
15	Abyss Finance	66821	0,0666666667	0,002985	0,0041
16	StakeHound	65440	0,0625	0,002923	0,0035
17	Stkr	57664	0,0588235294	0,002576	0,0032
18	danielwang.eth	55360	0,0555555556	0,002473	0,0028
19	DeFi	47200	0,0526315789	0,002109	0,0026
20	Bitfinex	46304	0,05	0,002069	0,0023
21	Gemini	41248	0,0476190476	0,001843	0,0021
22	gabuwahle	32000	0,0454545454	0,001430	0,0019
23	Gate.io	32000	0,0434782608	0,001430	0,0018
24	Cake DeFi	27744	0,0416666667	0,001239	0,0016
25	Kucoin	27136	0,04	0,001212	0,0015
26	Piedao	24000	0,0384615384	0,001072	0,0014
27	Cream	23712	0,0370370370	0,001059	0,0013
28	EF Gantee	18560	0,0357142857	0,000829	0,0012
29	SharedStake	16000	0,0344827586	0,000715	0,0011
30	WEX Exchange	16000	0,0333333333	0,000715	0,0011
31	Other	15840	0,0322580645	0,000708	0,0010
32	Poloniex	12960	0,03125	0,000579	0,0009
33	BTC-e	8640	0,0303030303	0,000386	0,0009
34	tgerring.eth	8032	0,0294117647	0,000359	0,0008
35	Vb	6976	0,0285714285	0,000312	0,0008
36	TokenPocket	6720	0,0277777778	0,000300	0,0008
37	CryptoStake	6592	0,0270270270	0,000294	0,0007
38	MintDice.com	5856	0,0263157894	0,000262	0,0007
39	Nimbus	4608	0,0256410256	0,000206	0,0006
40	Prysm	4608	0,025	0,000206	0,0006
41	Sigma Prime	4608	0,0243902439	0,000206	0,0006
42	Teku	4608	0,0238095238	0,000206	0,0006
43	kpt.eth	3808	0,0232558139	0,000170	0,0005
44	mega.unitinu.eth	3328	0,0227272727	0,000149	0,0005
45	coinspiracy.eth	3200	0,0222222222	0,000143	0,0005
46	greystroke.eth	2624	0,0217391304	0,000117	0,0005
47	MyEtherWallet	2464	0,0212765957	0,000110	0,0004
48	andermatt.eth	2080	0,0208333333	0,000093	0,0004
49	therealyoshi.eth	1632	0,0204081632	0,000073	0,0004
50	Blox Staking	1024	0,02	0,000046	0,0004
51	Staked.finance	960	0,0196078431	0,000043	0,0004
52	neukind.com	448	0,0192307692	0,000020	0,0004
53	stereum.net	416	0,0188679245	0,000019	0,0004
54	ptxptx	384	0,0185185185	0,000017	0,0003
55	Kain.eth	320	0,0181818181	0,000014	0,0003
56	MC	320	0,0178571428	0,000014	0,0003
57	Tetranode	320	0,0175438596	0,000014	0,0003
58	amaq	224	0,0172413793	0,000010	0,0003
59	brigs	192	0,0169491525	0,000009	0,0003
60	jsarcher.crypto	128	0,0166666667	0,000006	0,0003
61	Mr B	128	0,0163934426	0,000006	0,0003
62	Blockdaemon.com	64	0,0161290326	0,000003	0,0003
63	Zod	64	0,0158730158	0,000003	0,0003
	Total ETH stake	22384431		1,000000	0,6160

RMSE total = 0,6160176484

Asumimos que el **Error máximo esperado** es  $Error_{max} = 1$  (cuando la distribución observada es completamente distinta de Zipf).

$$Zipf_{norm} = 1 - \frac{0.616}{1} = 1 - 0.616 = 0.3839$$

En el análisis de la Ley de Zipf aplicado a los pools de staking de Ethereum, se observa que la concentración de ether en stake está distribuida de manera desigual entre las entidades. La mayor parte del staking está dominada por unos pocos pools, en particular **Lido**, que representa una porción significativa con más de 12 millones de ether en stake (alrededor del 54% del total). Esto implica que un único actor controla más de la mitad del stake, seguido por Binance y Kraken, que también poseen cantidades sustanciales en comparación con otros actores, aunque muy por debajo de Lido.

El resultado calculado para **Zipf norm = 0.384** indica una **desviación significativa respecto a la distribución de poder ideal según la Ley de Zipf**, que esperaría una disminución más uniforme y menos concentrada en los primeros puestos.

### **Implicaciones de la Concentración**

Este nivel de concentración en el staking de Ethereum sugiere una centralización del poder de validación en manos de pocos participantes. La centralización del staking puede generar riesgos de censura y reducir la resistencia a la censura de la red, ya que los pools con mayor stake tienen una influencia significativa sobre las decisiones de validación de bloques y pueden, en teoría, coordinarse para censurar transacciones o validar bloques de manera que maximice sus beneficios.

### **Conclusión**

La baja normalización (0.384) sugiere que el staking en Ethereum no sigue una distribución de poder ideal según Zipf. En lugar de eso, la red presenta una alta concentración de participación en staking en unos pocos actores, lo cual podría impactar la descentralización y seguridad del modelo de consenso de Ethereum. Este

nivel de centralización podría ser una vulnerabilidad en términos de gobernanza y resistencia a censura en la red Ethereum.

### 3. Ley de Benford

Para el análisis de la Ley Benford en Ethereum, se realiza el siguiente procedimiento:

7. Extracción de datos mediante API de Etherscan
  - a. Ether en stake por pool
  - b. Bloques minados por pool
  - c. Cantidad de nodos por país
  - d. Tamaño promedio de bloque
  - e. Número de tokens ERC-20 transferidos
  - f. Número de contratos validados
  - g. Direcciones activas
  - h. Direcciones únicas
8. Tabulación de datos en Excel
9. Extracción del primer dígito de cada dato
10. Cálculo de frecuencia para cada dígito del 1 al 9
11. Elaboración de gráfico con distribución porcentual
12. Análisis de resultados y conclusiones

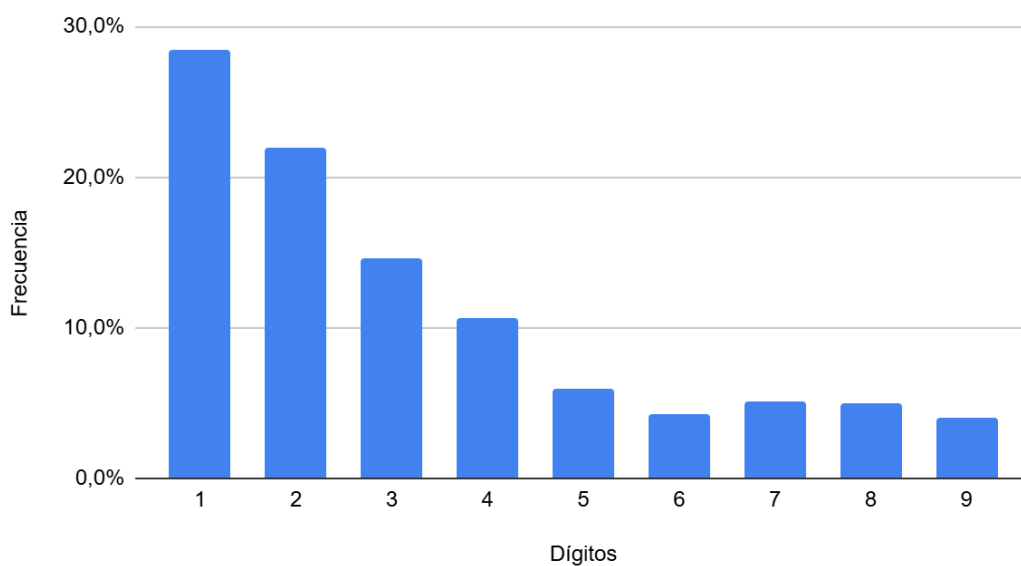
## Extracción de datos de Etherscan

Se ha logrado recopilar un conjunto de más de 23.000 datos. Por asuntos prácticos, los datos específicos no han sido incluidos en el informe de este estudio.

Luego de tabular los datos, extraer el primer dígito de cada dato y calcular la frecuencia para cada dígito, se presentan los siguientes resultados generales.

Dígito	Frecuencia Teórica (%)	Frecuencia Observada (%)	Diferencia Absoluta (%)
1	30.1	28.5	1.6
2	17.6	21.9	4.3
3	12.5	14.6	2.1
4	9.7	10.7	1.0
5	7.9	6.0	1.9
6	6.7	4.2	2.5
7	5.8	5.1	0.7
8	5.1	5.0	0.1
9	4.6	4.0	0.6

Gráfico Benford



**Diferencias Observadas:** Se observa que los dígitos más altos (como el 1 y el 2) están cerca de la frecuencia teórica, aunque el dígito 2 presenta una diferencia algo significativa de 4.3%. Este es uno de los mayores desajustes en el conjunto de datos.

Los valores generales de los primeros dígitos de Ethereum muestran cierta alineación con las expectativas de la Ley de Benford, aunque con algunas desviaciones menores en ciertos dígitos.

## Conclusión

Aunque existen algunas desviaciones en dígitos específicos, el conjunto de datos en general sigue una distribución de primer dígito que es razonablemente cercana a lo predicho por la Ley de Benford. Esto sugiere que los datos de Ethereum no presentan anomalías significativas desde una perspectiva estadística en términos de la distribución de sus primeros dígitos, aunque sería prudente profundizar en las áreas con mayor desajuste para determinar por qué exactamente se produce ese desajuste y si es un síntoma de puntos de centralización.

## Normalización de resultados

Total datos observados: **23375**

**Paso 1:** Calculamos la frecuencia relativa observada ( $P_{\text{obs}}$ ) de cada dígito dividiendo cada frecuencia por el total.

Frecuencias Relativas Observadas ( $P_{\text{obs}}$ ):

1.  $P_{\text{obs}}(1) = \frac{6662}{23375} \approx 0.285$
2.  $P_{\text{obs}}(2) = \frac{5124}{23375} \approx 0.219$
3.  $P_{\text{obs}}(3) = \frac{3424}{23375} \approx 0.146$
4.  $P_{\text{obs}}(4) = \frac{2498}{23375} \approx 0.107$
5.  $P_{\text{obs}}(5) = \frac{1391}{23375} \approx 0.0595$
6.  $P_{\text{obs}}(6) = \frac{985}{23375} \approx 0.0421$
7.  $P_{\text{obs}}(7) = \frac{1187}{23375} \approx 0.0508$
8.  $P_{\text{obs}}(8) = \frac{1165}{23375} \approx 0.0498$
9.  $P_{\text{obs}}(9) = \frac{939}{23375} \approx 0.0402$

Frecuencias Teóricas de Benford ( $P_{\text{exp}}$ ):

1.  $P_{\text{exp}}(1) = \log_{10}(1 + 1) - \log_{10}(1) \approx 0.3010$
2.  $P_{\text{exp}}(2) = \log_{10}(2 + 1) - \log_{10}(2) \approx 0.1761$
3.  $P_{\text{exp}}(3) = \log_{10}(3 + 1) - \log_{10}(3) \approx 0.1249$
4.  $P_{\text{exp}}(4) = \log_{10}(4 + 1) - \log_{10}(4) \approx 0.0969$
5.  $P_{\text{exp}}(5) = \log_{10}(5 + 1) - \log_{10}(5) \approx 0.0792$
6.  $P_{\text{exp}}(6) = \log_{10}(6 + 1) - \log_{10}(6) \approx 0.0669$
7.  $P_{\text{exp}}(7) = \log_{10}(7 + 1) - \log_{10}(7) \approx 0.0580$
8.  $P_{\text{exp}}(8) = \log_{10}(8 + 1) - \log_{10}(8) \approx 0.0512$
9.  $P_{\text{exp}}(9) = \log_{10}(9 + 1) - \log_{10}(9) \approx 0.0458$

**Paso 2:** Cálculo del RMSE (Error Cuadrático Medio)

Usamos la fórmula del RMSE para Benford:

$$\text{Error\_Benford} = \sqrt{\frac{1}{9} \sum_{d=1}^9 (P_{\text{obs}}(d) - P_{\text{exp}}(d))^2}$$

Calculamos cada término  $(P_{\text{obs}}(d) - P_{\text{exp}}(d))^2$ :

1.  $(0.285 - 0.3010)^2 \approx 0.000256$
2.  $(0.219 - 0.1761)^2 \approx 0.00184$
3.  $(0.146 - 0.1249)^2 \approx 0.000448$
4.  $(0.107 - 0.0969)^2 \approx 0.000102$
5.  $(0.0595 - 0.0792)^2 \approx 0.000386$
6.  $(0.0421 - 0.0669)^2 \approx 0.000608$
7.  $(0.0508 - 0.0580)^2 \approx 0.000052$
8.  $(0.0498 - 0.0512)^2 \approx 0.000002$
9.  $(0.0402 - 0.0458)^2 \approx 0.000031$

Sumando estos valores y dividiendo entre 9:

$$\begin{aligned} \text{Error\_Benford} &\approx \sqrt{\frac{1}{9}(0.000256 + 0.00184 + 0.000448 + 0.000102 + 0.000386 + 0.000608 + 0.000052 + 0.000002 + 0.000031)} \\ &\approx \sqrt{\frac{1}{9}(0.003725)} \approx \sqrt{0.000414} \approx 0.0203 \end{aligned}$$

Finalmente normalizamos el resultado para su incorporación al IGD.

Asumimos que  $\text{Error}_{\max} = 1$  para simplificar:

$$\text{Benford}_{\text{norm}} = 1 - \frac{0.0203}{1} = 1 - 0.0203 = 0.9797$$

## **Versión del IGD con los resultados hasta ahora para Ethereum**

La fórmula del IGD para esta evaluación es:

$$IGD = \sum_{i=1}^4 w_i \cdot F_i$$

Donde:

- $F_i$  es el valor normalizado del factor  $i$
- $w_i$  es el peso asignado al factor  $i$

Resumen de factores y sus ponderaciones:

### **Resultado combinado de Entropía de Shannon y Análisis de Componentes Conectados para Nodos:**

$$F_1 = 0.8116$$

$$w_1 = 0.30$$

### **Entropía de Shannon para Modelo de Consenso:**

$$F_2 = 0.384$$

$$w_2 = 0.15$$

### Ley de Zipf para Modelo de Consenso:

$$F_3 = 0.3839$$

$$w_3 = 0.15$$

### Ley de Benford:

$$F_4 = 0.9797$$

$$w_4 = 0.40$$

### Paso 1: Multiplicación de los factores por sus ponderaciones:

$$w_1 \cdot F_1 = 0.30 \cdot 0.8116 = 0.24348$$

$$w_2 \cdot F_2 = 0.15 \cdot 0.384 = 0.0576$$

$$w_3 \cdot F_3 = 0.15 \cdot 0.3839 = 0.057585$$

$$w_4 \cdot F_4 = 0.40 \cdot 0.9797 = 0.39188$$

### Paso 2: Suma de los resultados parciales:

$$IGD = 0.24348 + 0.0576 + 0.057585 + 0.39188 = 0.750545$$

### Resultado Final:

$$IGD = 0.7505$$

### Conclusión preliminar para IGD de Ethereum:

El **Índice Global de Descentralización** calculado con los 4 factores disponibles para Ethereum es de **0.7505** en una escala de 0 a 1. Al combinar estos factores en el IGD, Ethereum muestra una **descentralización moderada pero no ideal**. La alta concentración en los pools de staking y en la distribución de nodos en ciertos países limita la descentralización total de la red. Este valor de IGD sugiere que, si bien Ethereum tiene mecanismos de descentralización, la infraestructura actual de nodos y staking deja espacios importantes de centralización que podrían representar puntos únicos de fallo o control.

## Análisis Comparativo de IGD: Bitcoin vs. Ethereum

### Valores de IGD Calculados:

- **Bitcoin IGD:** 0.8114
- **Ethereum IGD:** 0.7505

La diferencia porcentual es de 7,5%

Bitcoin tiene un IGD superior en comparación con Ethereum, lo que indica que, en general, la red de Bitcoin muestra un grado de descentralización más robusto. La diferencia del 7.5% es significativa, ya que en un índice que va de 0 a 1 representa un margen de descentralización que, aunque no es extremadamente amplio, revela ciertas ventajas de descentralización de Bitcoin en comparación con Ethereum.

### Factores Determinantes:

- **Distribución de Nodos:** Bitcoin muestra una distribución de nodos más diversificada y con una mayor dispersión de componentes conectados en términos de ASN y direcciones IP. Esto reduce la probabilidad de centralización de la infraestructura y minimiza puntos de fallo único.
- **Modelo de Consenso:** Bitcoin, al estar basado en un modelo de proof of work (PoW), distribuye el poder de minado de manera más homogénea a través de los pools, aunque algunos dominan el hashrate. En cambio, Ethereum, con su modelo de proof of stake (PoS), muestra mayor concentración en los validadores con grandes cantidades de Ether en staking. Los gráficos y datos sugieren que una porción considerable del staking está dominada por pocos actores institucionales, lo que incrementa los riesgos de centralización.

En el caso de Ethereum, el staking está altamente concentrado en unos pocos pools y validadores, como Lido y Coinbase, que poseen una participación importante del total de Ether en staking. Esto significa que cualquier fallo, ataque o decisión por parte de estos actores principales podría influir de manera considerable en la red.

## Implicaciones de los Modelos de Consenso:

- **Bitcoin:** Al utilizar PoW, Bitcoin depende de una distribución geográfica y energética que se diversifica por su naturaleza competitiva y los altos costos de entrada, lo que, a pesar de la concentración de algunos pools, fomenta la independencia de los mineros.
- **Ethereum:** Con el cambio a PoS, aunque se elimina el consumo energético significativo, se centraliza en aquellos con mayor capacidad financiera para mantener Ether en staking, lo cual puede reducir la accesibilidad y aumentar la posibilidad de carteles o coaliciones de validadores.

## Conclusiones Finales

**Bitcoin** parece mantener una estructura más descentralizada en general, con un IGD superior en un 7.5% respecto a Ethereum. Aunque ambos sistemas tienen margen de mejora, Bitcoin ha logrado mantener una distribución de poder y responsabilidad que minimiza el riesgo de centralización en términos de su infraestructura de nodos y en su modelo de consenso.

**Ethereum**, aunque descentralizado en muchos aspectos, enfrenta desafíos inherentes a su transición a PoS. La concentración en pools de staking y la centralización geográfica de sus nodos limitan su descentralización efectiva, haciendo que su red sea más vulnerable a puntos únicos de control.

**Recomendación del autor:** Para mejorar la descentralización, tanto Bitcoin como Ethereum deben promover la distribución de nodos en más países y fomentar una mayor competencia en los pools de consenso (minería en PoW y staking en PoS). En particular, Ethereum debería enfocarse en reducir la concentración de Ether en pocas entidades de staking para minimizar riesgos de centralización.

## Referencias Bibliográficas

1. Shannon, C. E. (1948). *A Mathematical Theory of Communication*. The Bell System Technical Journal, 27(3), 379–423.  
<https://doi.org/10.1002/j.1538-7305.1948.tb01338.x>
2. Cover, T. M., & Thomas, J. A. (2006). *Elements of Information Theory*. Wiley-Interscience.  
<https://onlinelibrary.wiley.com/doi/book/10.1002/047174882X>.
3. Benford, F. (1938). *The Law of Anomalous Numbers*. Proceedings of the American Philosophical Society, 78(4), 551-572.  
<https://www.jstor.org/stable/984802>
4. Berger, A., & Hill, T. P. (2011). *A Basic Theory of Benford's Law*. Probability Surveys, 8, 1-126.  
[Disponible en arXiv.](#)
5. Durtschi, C., Hillison, W., & Pacini, C. (2004). *The Effective Use of Benford's Law to Assist in Detecting Fraud in Accounting Data*. Journal of Forensic Accounting, 5, 17-34.  
<https://www.benfordonline.net>
6. Zipf, G. K. (1949). *Human Behavior and the Principle of Least Effort*. Addison-Wesley.  
<https://archive.org/details/humanbehaviorpri0000zipf>
7. Newman, M. E. J. (2005). *Power Laws, Pareto Distributions and Zipf's Law*. Contemporary Physics, 46(5), 323-351.  
[Disponible en arXiv](#)
8. Clauset, A., Shalizi, C. R., & Newman, M. E. J. (2009). *Power-law Distributions in Empirical Data*. SIAM Review, 51(4), 661-703.  
<https://doi.org/10.1137/070710111>
9. Bollobás, B. (1998). *Modern Graph Theory*. Springer.  
<https://doi.org/10.1007/978-1-4612-0619-4>
10. Newman, M. E. J. (2010). *Networks: An Introduction*. Oxford University Press. <https://academic.oup.com/book/27884>
11. Barabási, A.-L. (2016). *Network Science*. Cambridge University Press.  
<https://networksciencebook.com>

12. Chai, T., & Draxler, R. R. (2014). *Root Mean Square Error (RMSE) or Mean Absolute Error (MAE)? – Arguments against Avoiding RMSE in the Literature*. *Geoscientific Model Development*, 7(3), 1247-1250.  
<https://gmd.copernicus.org/articles/7/1247/2014/>
13. Willmott, C. J., & Matsuura, K. (2005). *Advantages of the Mean Absolute Error (MAE) over the Root Mean Square Error (RMSE) in Assessing Average Model Performance*. *Climate Research*, 30(1), 79-82.  
<https://doi.org/10.3354/cr030079>
14. Albert, R., & Barabási, A.-L. (2002). *Statistical Mechanics of Complex Networks*. *Reviews of Modern Physics*, 74(1), 47-97.  
<https://doi.org/10.1103/RevModPhys.74.47>
15. Latora, V., Nicosia, V., & Russo, G. (2017). *Complex Networks: Principles, Methods and Applications*. Cambridge University Press.  
<https://doi.org/10.1017/9781316216009>
16. Bitnodes.io. *Explore the Bitcoin Network*. <https://bitnodes.io>
17. Mempool.Space: *Bitcoin Explorer and Mempool Visualizer*.  
<https://mempool.space>.
18. Etherscan. *Ethereum Explorer*. <https://etherscan.io>