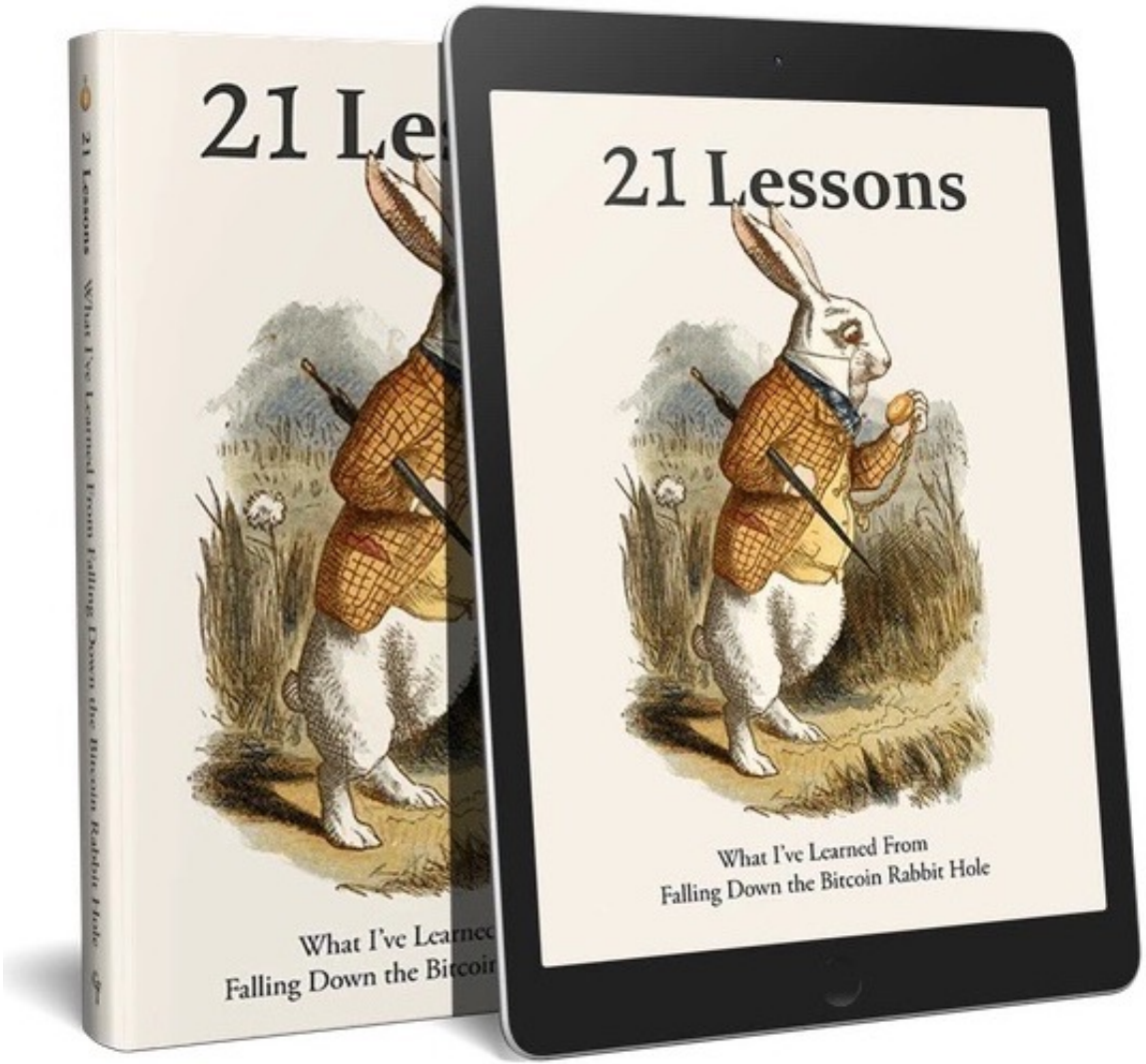
21 Lecciones

Lo Que He Aprendido
Al Caer En La
Madriguera De Bitcoin

(Por Gigi)

https://21lessons.com/



Resumen por Iván Párraga

1. Inmutabilidad y Cambio

- La naturaleza de Bitcoin es inmutable porque una vez se puso en marcha su core no se puede cambiar
- La descentralización radical fuerza a llegar a un acuerdo con todos los participantes antes de poder introducir un cambio
- Bitcoin tiene una capa social que se implementa en una capa tecnológica que es el protocolo. La capa social ha de adoptar los cambios antes que lo pueda hacer el software

2. La Escasez de la Escasez

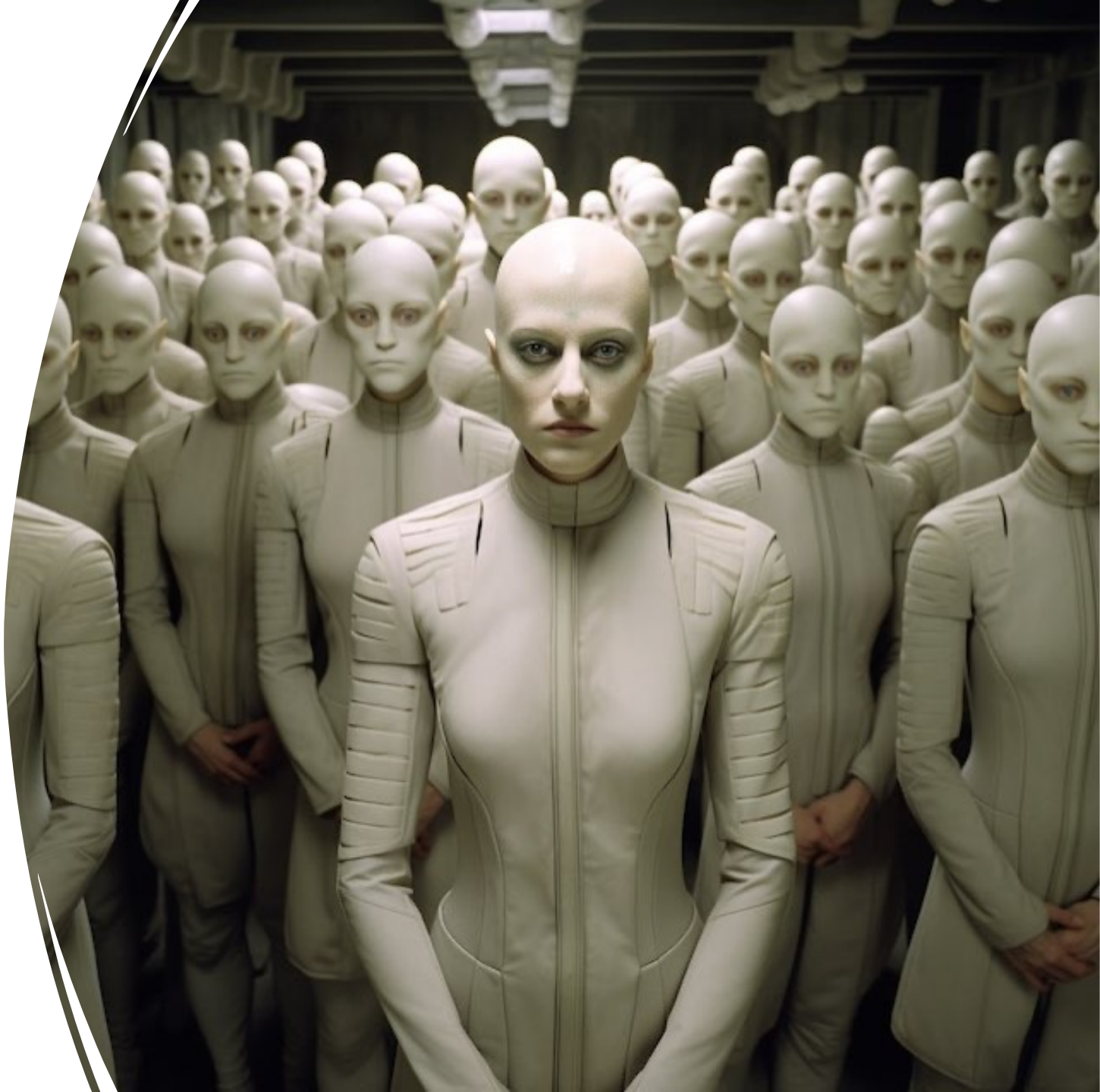
- El diseño de Bitcoin es tal que aunque su suministro sea escaso e inmodificable paradójicamente se consigue incentivando la copia del blockchain en cuantos más nodos mejor
- Es valioso porque de su escasez se deriva su propiedad como almacén de valor.
- Por la "minority rule" de Nassim Taleb, si hay una minoría intransigente que sólo acepte Bitcoin frente a otras monedas, al final la mayoría sólo aceptará Bitcoin

3. Replicación y Localización

- No existen bitcoins como entidad tecnológica
- Tan sólo existe un conjunto de cambios no gastados en las transacciones que están anotadas en un libro de cuentas (ledger) distribuido
- No tiene sentido pensar que los bitcoins están en una localización
- La clave privada permite hacer anotaciones en el libro de cuentas así que podríamos decir que la clave son los bitcoins

4. El Problema de la Identidad

- Un blockchain totalmente descentralizado, sin líder (sea este una empresa, una fundación o un dictador benevolente) tiene el reto de encontrar el mecanismo para alcanzar consensos
- Consensos con respecto a la evolución de la filosofía y la tecnología
- Cuando no hay un consenso y se produce un fork, ¿qué blockchain es el original?



5. Una Concepción Inmaculada

- El hecho que Satoshi desapareciera una vez Bitcoin superó la infancia lo convirtió en el único blockchain realmente descentralizado
- Esta descentralización garantiza que los cambios sólo pueden hacerse mediante un gran consenso y que por tanto son beneficiosos para la gran mayoría de la red
- Es el blockchain con más tiempo de funcionamiento, por tanto con más usuarios y con mayores efectos de red
- Francis Pouliot: "The value of a cryptocurrency is derived from its network effect"

6. El Poder de la Libertad de Expresión

- El Bitcoin se basa en software de código abierto, en texto y en particulares intercambiando mensajes
- Todo lo anterior son componentes de la libertad de expresión
- Una sociedad que proteja la libertad de expresión no puede censurar el Bitcoin

7. Los Límites del Conocimiento

- Hay que ser humilde y comprender que por mucho que se estudie no se puede llegar a entender todas las interioridades e implicaciones en la sociedad y la economía que una tecnología como Bitcoin puede habilitar
- Es imposible aprenderlo todo pero tenemos la obligación de educarnos

8. Ignorancia Financiera

- La mayoría de la sociedad no tiene educación financiera en parte porque el sistema educativo lo favorece
- Tenemos que ser conscientes e intentar poner remedio en la medida de nuestras posibilidades

9. Inflación

- Es el ratio al cual se crea nuevo dinero en una unidad de tiempo
- Los efectos no son inmediatos
- No afecta a todos por igual. Aquellos que están más cerca de la emisión de la nueva moneda (gobiernos, banca) se favorecen porque la pérdida de valor tarda un tiempo en producirse
- Todas las monedas de los gobiernos han acabado sucumbiendo
- El oro ha sido el dinero que ha permanecido más tiempo con un valor estable (al menos mismo orden de magnitud) porque está sometido a los límites de la física (en su stock y extracción)
- El dinero duro es aquél que conserva bien su valor a lo largo del tiempo y el espacio. El dinero blando es el que no tiene esta propiedad

10. Valor

- Los humanos valoramos aquello que es:
  - escaso,
  - difícil de producir o que requiere mucho trabajo,
  - no se puede sustituir o
  - es útil porque habilita cosas que no se podrían realizar
- Bitcoin tiene todas estas propiedades

11. Dinero

- Cualquier cosa que se usa como dinero, es dinero
- La mitad de cualquier transacción es dinero, así que aquellos que pueden emitir dinero tienen mucho poder
- El dinero actual es corrupto porque se crea del aire
- Bitcoin elimina el poder de la creación del dinero de forma pacífica

12 . La Historia y la Caída del Dinero

- El dinero fiduciario lo es por decreto, porque los gobiernos lo dicen, no por sus propiedades intrínsecas
- El dinero empezó como dinero mercancía (commodity money) hecho de materiales preciosos que tenían valor intrínseco, después surgió el dinero representativo que actuaba como una representación del dinero mercancía que estaba almacenado en algún lugar seguro y después los gobiernos rompieron el vínculo entre el dinero representativo y el dinero mecancía creando el dinero fiduciario
- Todo el dinero fiduciario es deuda porque es el mecanismo por el que los bancos centrales lo introducen en el mercado utilizando técnicas como la expansión cuantitativa
- ¿Cómo funciona la expansión cuantitativa?
  - el banco central dinero nuevo en su libro de cuentas, directamente del aire
  - el banco central entonces compra activos del mercado: deuda soberana o bien deuda privada a bancos comerciales y otras instituciones financieras
  - los bancos comerciales prestan el dinero a los ciudadanos y otras organizaciones
- La expansión cuantitativa crea inflación porque devalúa el valor de la moneda previamente existente en el mercado

13. La Locura de la Reserva Fraccional

- El sistema de reserva fraccional permite que un banco sólo deba conservar una parque muy pequeña de los depósitos y prestar el resto, lo que de manera muy rápida multiplica la cantidad de dinero disponible en el sistema
- Gracias al sistema de reserva fraccional y a la expansión cuantitativa, los bancos pueden crear dinero que no tienen

14. Dinero Duro

- El dinero duro es aquel que puede ser utilizado globalmente y que sirve como reserva de valor confiable.
- La volatilidad del Bitcoin es normal porque el mercado está todavía ajustando su precio.
- El ratio stock-to-flow es la cantidad nueva de dinero que se emite en una unidad de tiempo. A mayor dureza, menor inflación y menos se devalúa la moneda
    - El oro es la moneda con mayor dureza porque es escaso y su extracción es costosa
    - El dinero fiduciario tiene poca dureza porque los bancos centrales pueden emitir como quieran
    - Bitcoin en el largo plazo tiene dureza infinita porque su emisión está acotada y controlada algorítmicamente
- El algoritmo de emisión de Bitcoin es tal que da igual el esfuerzo que se aplique en el minado, su dificultad se ajusta al esfuerzo aplicado de manera que la emisión y el límite se mantienen como se diseñó

15. La Fortaleza Está en los Números

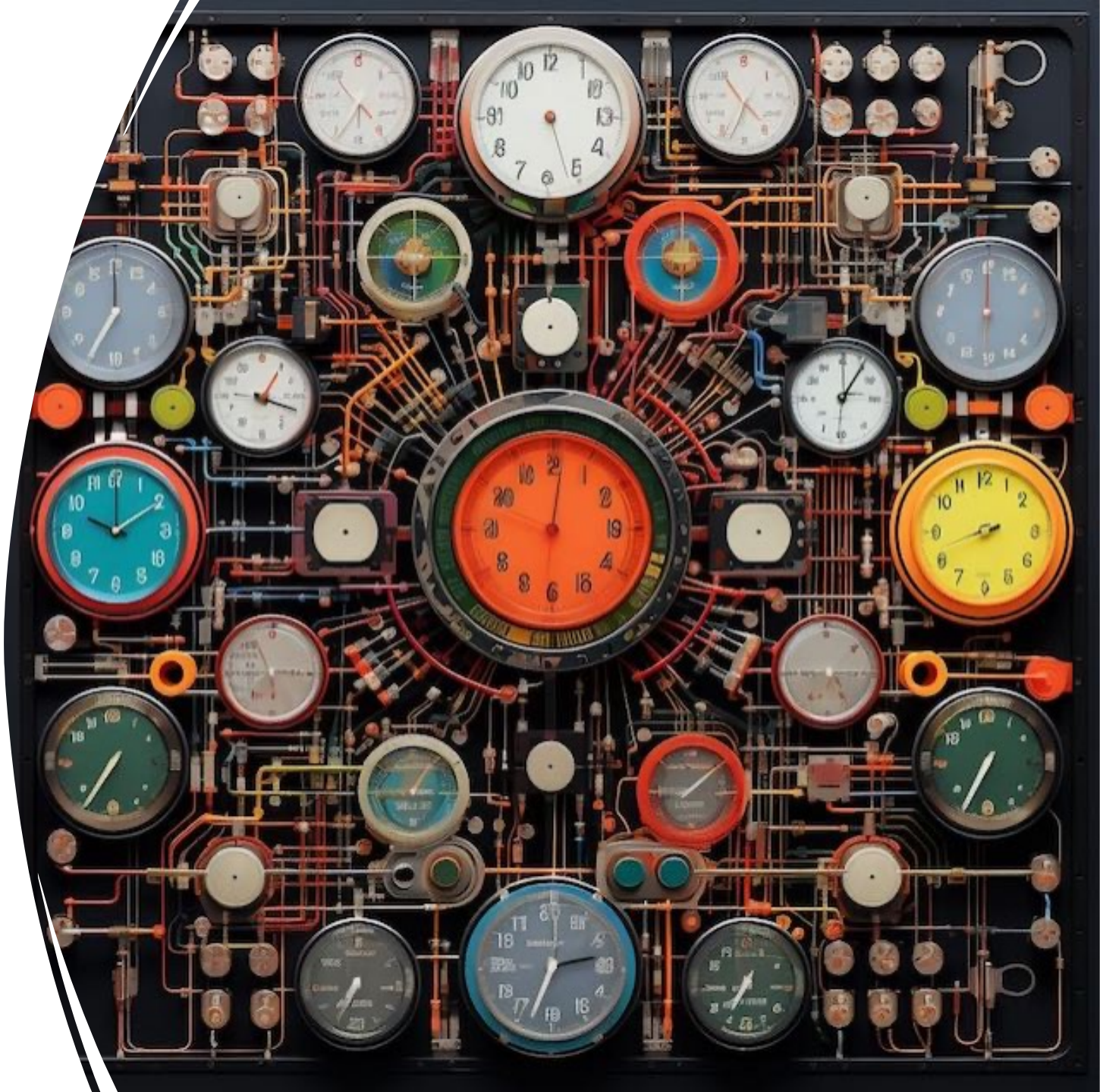
- Bitcoin se ha construido en base a grandes números y la imposibilidad de adivinarlos con fuerza bruta: criptografía fuerte
- La confianza en la seguridad de Bitcoin y su uso de la criptografía se basa en dos certezas:
  - hay una gran asimetría de esfuerzo entre encontrar soluciones y validar que dichas soluciones son correctas
  - la computación consume energía

16. Reflexiones sobre: "No Confíes, Verifica"

- En Bitcoin no se necesita confianza en una entidad central ya que su arquitectura es totalmente descentralizada
- Aún así, como en cualquier sistema informático sí se requiere confianza en el hardware y el software que se está utilizando, así como de la física y las matemáticas. A pesar de esto se sigue innovando en sistemas que también requieren menos confianza en estos campos
- En cualquier caso existen múltiples implementaciones del software y Bitcoin no tiene dependencia de un hardware en particular

17. Contar el Tiempo Cuesta Trabajo

- En un sistema totalmente descentralizado el tiempo absoluto no puede existir porque requeriría la introducción de un reloj que sería un actor centralizado que requeriría confianza y que además podría ser atacado
- El proof-of-work introduce un mecanismo que permite a todos los nodos ponerse de acuerdo sobre qué transacción va antes que otra.
- Da igual que el orden no sea cronológicamente exacto porque eventualmente se llegará a un orden consensuado e inambiguo



18. Muévete Despacio y No Rompas las Cosas

- La descentralización y la transparencia total del código y el blockchain es un factor fundamental de la seguridad de Bitcoin:
- no existe un único punto de fall
- todo el mundo puede verificar de forman independiente
- La descentralización radical hace que no sea posible forzar cambios y por tanto se requiere de consensos muy amplios
- Este mecanismo es inevitablemente lento pero minimiza la posibilidad de introducir cambios que rompan el sistema

19. La Privacidad No Está Muerta

- El anonimato en Internet no es fácil pero esforzándose se puede logra: Satoshi lo consiguió
- Aunque Bitcoin es esencialmente transparente (no hay datos encriptados), existen buenas prácticas para proteger tu identidad y hay desarrollos activos en ese sentido
- El artículo 12 de los derechos humanos reconoce el derecho a la privacidad

20. Los Cypherpunks Escriben Código

- Muchos de los principios y valores que defendían los cypherpunks se han visto implementados en Bitcoin: derecho a la privacidad, descentralización, sistemas anónimos, uso de la encriptación entre iguales.
- Satoshi, como un verdadero cypherpunk, escribió código para implementar su visión (antes de escribir el white paper)

21. Metáforas Para Entender el Futuro de Bitcoin

- Bitcoin es una tecnología exponencial que se establece la infraestructura para construir otra tecnología encima suyo. Además está construida sobre otra tecnología exponencial: Internet
- Puede que estemos en la adolescencia de Bitcoin pero n sistemas exponenciales la distancia entre la oscuridad y la obicuidad puede ser muy corta
- Bitcoin tiene múltiples efectos de red: precio, usuarios, seguridad, desarrolladores, market share y adopción como moneda global

Suscríbete a mi newsletter gratuita

“La Cadena”

para aprender más sobre Bitcoin

https://www.ivanparraga.com/la-cadena/