



Sobre sistemas digitales de transferencia de valor alternativos y resistencia al cambio

En 2008, el pseudónimo de Satoshi Nakamoto publicó un artículo de nueve páginas en Internet, que no en una revista académica, introduciendo los fundamentos más actuales de la tecnología *blockchain*. Curiosamente, la palabra “blockchain” no aparece en dichas páginas. El título del artículo era “*Bitcoin: peer-to-peer electronic cash system*” (un sistema electrónico de transferencia de dinero en efectivo entre pares). Ya en 1982 David Chaum sugería un sistema de registro público y distribuido. Nakamoto recogía el espíritu de dicha propuesta y añadía “proof of work” (prueba basada en trabajo computacional) como base de su algoritmo de consenso: “la cadena de bloques más larga es la aceptada”.



Como amenazas, destaco la incertidumbre de cómo serán regulados, el aún inestable equilibrio entre la privacidad y la trazabilidad de sus transferencias, el futuro de los algoritmos criptográficos usados actualmente en el caso

del despegue de la computación cuántica, la escasa cooperación con el sistema financiero tradicional y el alto interés de la delincuencia en extraer valor de estos sistemas.

En la actualidad, aunque atravesamos un mercado ciertamente bajista, Bitcoin es el criptoactivo de mayor capitalización, seguido de Ethereum. Sólo en el *blockchain* de Ethereum existen más de 500k *tokens*. Lo más probable es que muchas de estas implementaciones *blockchain* desaparezcan o, simplemente, queden como proyectos surgidos de ideas con potencial. Sería muy ingenuo pensar que todos los criptoactivos de mayor capitalización, aunque aún sufren de una alta volatilidad, vayan a desaparecer en los próximos años.

El estudio de la ciberseguridad en *blockchain* es una de mis pasiones académicas. El diseño distribuido y descentralizado de estas cadenas de bloques hace que esta tecnología sea robusta desde el punto de vista de su disponibilidad e integridad. Sin embargo, en esta ocasión, la conocida teoría de las capas de cebolla, tan presente en la seguridad de la información, aplica completamente a todas las implementaciones *blockchain*: la seguridad en *blockchain* requiere ‘securizar’ muchas y muy diferentes capas.

Menciono dos ejemplos que confirman este hecho: la pérdida de 850k bitcoins custodiados por la plataforma de intercambio japonesa Mt. Gox en febrero de 2014. En cifras actuales, estamos hablando de un robo de decenas de billones de dólares. La falta de adecuada protección de las claves privadas de sus “wallets” (billetera) y una pésima gestión de cambios fueron dos de las causas de este incidente.

Ocho años más tarde, en 2022, el colapso de la “stablecoin” (moneda estable) Terra dejaba cerca de 45 billones de dólares por el camino. En esta ocasión, el código del “smart contract” (contrato inteligente) que regía la gobernanza de Terra tenía graves fallas de seguridad que permitían la extracción de valor de forma fraudulenta. Este abanico de causas principales es un viejo conocido de todos los que llevamos años en ciberseguridad.

Comparto en esta columna brevemente algunas de las vulnerabilidades y amenazas de las *blockchains* públicas. Como vulnerabilidades, el uso de estas cadenas de bloques es aún complejo; aunque aún se encuentran en un estado inicial de evolución, ya se observan signos de

centralización y, finalmente, su gobernanza es prácticamente dependiente de código presente en la cadena. Como amenazas, destaco la incertidumbre de cómo serán regulados estos sistemas, el aún inestable equilibrio entre la privacidad y la trazabilidad de sus transferencias, el futuro de los algoritmos

criptográficos usados actualmente en el caso del despegue de la computación cuántica, la escasa cooperación con el sistema financiero tradicional y, finalmente, el alto interés de la delincuencia en extraer valor de estos sistemas.

Aquellos lectores que quieran información adicional sobre este tema, el artículo publicado en enero de 2022, con el título ‘Modeling Bitcoin plus Ethereum as an Open System of Systems of Public Blockchains to Improve Their Resilience against Intentional Risk’, es una interesante puerta de entrada.

En definitiva, la tecnología *blockchain* es un bonito campo para aplicar ciencia con el objetivo de aumentar su seguridad. En este viaje me embarqué hace ya algunos años y en él continúo, publicando artículos científicos en los que aplico herramientas como la teoría de redes complejas y la ingeniería de sistemas para concluir con recomendaciones muy concretas que permitan el uso seguro de esta tecnología que permite la transferencia de valor digital: la seguridad de las implementaciones *blockchain* es una condición necesaria, aunque no suficiente, para la adopción generalizada de criptoactivos.

Dr. Alberto Partida
Experto en Ciberseguridad

<https://linkedin.com/in/albertopartida>

