Criptografía

Arbol de Merkle

El bloque inicial se llama root o génesis. Calcula de forma anidada los distintos hash. Si se cambia un bit de un bloque, cambia su hash y por lo tanto la información del siguiente y todos los hashes de todos los que le siguen.

- Medio eficiente para generar una estructura distribuida de datos
- Seguridad y resistencia a alteraciones de datos
- Alto nivel de rendimiento de transmisión de datos
- Computacionalmente poco costoso y eficiente a la hora de crear, procesar y verificar información.
- Permiten disección, descomposición de un árbol de Merkle en sus componentes individuales para hacer búsquedas de verificación más rápidas.

Funciones hash

Se una función computable mediante un algoritmo x→H(x) que convierte la netrada en una cadena fija y pequeña de bits:

- Barato
- Compresión
- Sirven como identificadores de documentos, dificilmente corruptibles
- Uniforme
- determinista
- no reversible.

De blockchain pre-cuántica a post-cuántica

- La fortaleza de los criptosistemas de clave pública contra ataques de computación clásica se ha estimado tradicionalmente mediante el sistema de Nivel de Seguridad de Bit.
- Este nivel se define como el esfuerzo requerido por una computadora clásica para realizar un ataque de fuerza bruta.
- el coste de romper criptosistemas de 80-bits con computadores clásicos están estimados entre decena de miles y cientos de millones de dólares
- Sin embargo:
    - Las curvas elípticas de 160-bits pueden romperse con un computador cuántico de 1000 qbits
    - RSA de 1024 bits necesitaría 2000 qbits
- Esta amenaza afecta a todos los sistemas que dependen de la factorización de enteros o curvas elípticas entre otros.

Algoritmo de Shor

- Se usa para encontrar los factores primos de un número entero en tiempo polinómico
- Mientras que los algoritmos clásicos tienen complejidad exponencial para factorizar números grandes
- El algoritmo cuántico que se utiliza par abiscar en una secuencia no ordenada de datos con N componentes en un tiempo O(N^1/2) y con una necesidad adicional de espacio de almacenamiento de O(logN)
- Se usa para búsquedas en bases de datos no estructurados y, en el caso de la cirptografía, para romper sistemas basados en hash.

Amenaza cuántica

- Muchos criptosistemas han sido comprometidos o impactados de forma significativa por los ataques cuánticos que usan Shor y Grover