

REIVINDICACIONES MODIFICADAS

1. Un método para registrar una transacción de datos que comprende, en un dispositivo asociado con una primera entidad mientras se produce una primera transacción de datos entre la primera entidad y una segunda entidad:
 - determinar primeros datos iniciales;
 - determinar segundos datos iniciales mediante la combinación de al menos los primeros datos iniciales y el registro de la primera transacción de datos;
 - generar un primer resumen (hash) mediante la función de resumen (hashing) de los segundos datos iniciales, en donde el primer resumen comprende un historial de transacciones de datos que involucran a la primera entidad donde la generación del primer resumen es contemporánea a la realización de la primera transacción de datos; y
 - almacenar simultáneamente el registro de la primera transacción de datos y el primer resumen contra el registro de la primera transacción de datos en una memoria.
2. El método de la reivindicación 1, en donde los primeros datos iniciales comprenden un resumen inicial.
3. El método de la reivindicación 2, en donde el resumen inicial es el resultado de realizar una función de resumen de un registro de una transacción de datos previa que involucra a la primera entidad.
4. El método de la reivindicación 2, en donde el resumen de inicio comprende un resumen aleatorio.
5. El método de la reivindicación 4, en donde el resumen aleatorio comprende al menos una firma del dispositivo, la fecha y/o la hora en que se generó el resumen aleatorio.

6. El método de cualquiera de las reivindicaciones precedentes, en donde proporcionar segundos datos iniciales comprende además la combinación de una primera prueba de conocimiento cero y una segunda prueba de conocimiento cero con los primeros datos iniciales y el registro de la primera transacción de datos, en donde:

la primera prueba de conocimiento cero comprende probar que el resumen inicial comprende el resumen verdadero de la transacción de datos anterior que involucra a la primera entidad; y

la segunda prueba de conocimiento cero comprende probar que un segundo resumen comprende el resumen verdadero de una transacción de datos anterior que involucra a la segunda entidad.

7. El método de la reivindicación 6, en donde proporcionar segundos datos iniciales comprende además combinar una tercera prueba de conocimiento cero con los primeros datos iniciales, el registro de la primera transacción de datos, la primera prueba de conocimiento cero y la segunda prueba de conocimiento cero.

8. El método de la reivindicación 7, en donde la tercera prueba de conocimiento cero se genera a partir de datos aleatorios.

9. El método de la reivindicación 7, en donde la tercera prueba de conocimiento cero es una repetición de la primera prueba de conocimiento cero o la segunda prueba de conocimiento cero.

10. El método de la reivindicación 7, en donde la tercera prueba de conocimiento cero se construye utilizando un segundo registro de la primera transacción de datos que corresponde a la segunda prueba de conocimiento cero.