

RESUMEN DE LA INVENCION

La invención proporciona una solución implementada por computadora para controlar acceso a un recurso relacionado con computadora tal como, por ejemplo, una billetera digital; en una o más modalidades, la billetera puede implementarse al utilizar una cadena de bloques tal como la cadena de bloques de Bitcoin pero la invención no está limitada con respecto a esto; el uso de la invención durante la configuración inicial de la billetera puede permitir operaciones subsecuentes tal como transacciones de billetera para manejarse en una forma segura sobre un canal inseguro tal como Internet; un método de conformidad con una modalidad de la invención puede comprender los pasos de dividir un elemento de verificación (tal como una clave privada en un par de criptografía asimétrica) en una pluralidad de acciones; determinar un secreto común en dos o más nodos en una red; y utilizar el secreto común para transmitir al menos una acción del elemento de verificación entre los dos o más nodos; las acciones pueden dividirse de manera que ninguna acción por sí misma es suficiente para llegar al elemento de verificación; esto significa que ninguna parte almacena toda la clave privada, proporcionando seguridad mejorada de la clave; se requieren dos o más acciones para restaurar la clave; las acciones se restauran en ubicaciones separadas de las cuales es una ubicación independiente de respaldo o de almacenamiento seguro; si una de las otras acciones se vuelve no disponible, la acción puede recuperarse del respaldo para asegurar que la clave (y de esa forma el recurso controlado) aún es accesible; para asegurar transmisión segura de la(s) acción(es), se genere el secreto común en dos modos diferentes independientemente uno de otro y entonces se utiliza para generar una clave de encriptación; la clave de encriptación puede utilizarse para encriptar al menos una acción del elemento de verificación, o un mensaje que lo comprende, para asegurar que la(s) acción(es) se transmite(n) de manera segura.