COINsolidation

Algoritmos oneCKey (one Consolidated private Key) y CUA (Consolidated Universal Address).

By Guillermo Vidal
vidal@coinsolidation.org
www.coinsolidation.org / www.coinsolidation.io

Resumen: Un algoritmo para consolidar la llave privada de direcciones de diferentes blockchains, utilizadas en la actualidad en el área financiera (criptomonedas), aplicaciones y sectores diversos. Proponemos dos algoritmos el primero que llamamos **oneCKey** (**one C**onsolidated prívate **Key**) se aplique para consolidar llaves privadas (Una llave privada para Ndirecciones de diferentes tecnológicas blockchain). Lo anterior se usa para crear sistemas más eficientes en administración de llaves privadas. Este sistema se en conjuntos de series para ser, la primera Serie A1 o serie "Génesis" aplicamos oneCKey en los blockchains Bitcoin y Ethereum una relación de 1:2 (una llave privada para generar dos direcciones) y posteriormente tendremos Series AX y BX donde habrá relaciones de 1: N (una llave privada para N-direcciones). Usamos otro algoritmo llamado **CUA** (**C**onsolidated **U**niversal **A**ddress) para la creación de direcciones universales que llamaremos direcciones consolidadas. El algoritmo CUA se desglosa en tres tipos de consolidación de direcciones las cuales son; **CUA** "Consolidated Universal Address" una dirección formada de Criptomoneda con Criptomoneda, **DAC** "Direct Address Consolidated" una dirección formada de Token con Token y la **HAC** "Hibric Address Consolidated" una dirección formada de Token con Criptomoneda.

INTRODUCCION.

Actualmente 2021 se tiene una tendencia al uso de sistemas blockchain en diferentes sectores como financiero (criptomonedas) y emergentes tanto públicos como privados. En las diferentes tecnologías de blockchain se manejan la generación de sus propias direcciones de uso común para las operaciones de depósitos de sus activos correspondientes y cada dirección administra sus activos de forma independiente por medio de su llave privada única referenciada a una sola dirección de depósito pública, en la actualidad se tiene solamente una relación 1:1 (una dirección para depósito referenciada a una sola y única llave privada para transferencias de activos) por lo que la administración de varias direcciones se ve complicada al tener siempre una cantidad de N-direcciones para depósito de activos referenciadas a N-llaves privadas de transferencia de activos, una relación N:N. Donde N es la cantidad de direcciones creadas por un usuario en diferentes criptomonedas, siempre se cumple esta relación de N: N.

Por otra parte, también consideremos que la administración se complica para las llaves privadas de igual forma con la relación N: N, es decir un usuario que tenga N direcciones de depósito tendrá de manera directamente proporcional N llaves privadas para administrar. Al aplicar el algoritmo oneCKey se creará una relación de 1: N, una relación de una llave privada para varias direcciones de depósito de diferentes tecnologías blockchain (consolidamos las llaves privadas a solo una que administrará N direcciones de depósito). Por ultimo también se tiene la necesidad de que cada usuario al querer desear realizar un deposito o una transferencia de activos necesita saber la dirección destino, la propuesta es aplicar el segundo algoritmo llamado CUA – "Consolidated Universal Address", una dirección que consolida dos o más tecnologías blockchain dando como resultado una sola dirección.

Todo lo anterior debe estar funcionando con los sistemas de criptografía que actualmente usa cada criptomoneda, al consolidar la llave primaria se utiliza la validación y la criptografía actual de cada blockchain nativo de la criptomoneda a usar, así cuando se desarrolle cada serie con relación 1: N+1 se aplicara los mismos protocolos de criptografía y hash actuales, esto es consolidación en seguridad.

Después de realizar un estudio sobre el basto mundo de las criptomonedas más importantes y sobresalientes del mercado, hemos encontrado que hay dos tendencias fundamentales para la generación de direcciones y llaves privadas. Las dos curvas de criptografía usado tipo ECC (*Elliptic curve cryptography)* que cubren el 95% de las criptomonedas actuales "más sobresalientes", son: I. La Curva criptográfica secp256k1 usado por Bitcoin y Ethereum. (**Series A**).

II. La Curva criptográfica Ed25519 tiene una tendencia a ser usada Es una de las curvas ECC más rápidas y no está cubierta por ninguna *patente*. (**Series B**).

Ejemplo:

Name	Type	Signing alg	Curve	Hash	Address encoding	Address hash
Bitcoin	UTXO	ECDSA	secp256k1	SHA-256	base58, bech32	SHA-256, RIPEMD-160
Ethereum	account	ECDSA	secp256k1	Keccak-256 *	none (just hex) *	last 20B of Keccak-256 *
XRP	account	ECDSA *	secp256k1 *	first half of SHA-512	base58 with different alphabet *	SHA-256, RIPEMD-160
Litecoin	UTXO	ECDSA	secp256k1	SHA-256 *	base58, bech32	SHA-256, RIPEMD-160
EOS	account	ECDSA	secp256k1	SHA-256	none *	none *
Bitcoin Cash	Same as Bitcoin *					
Stellar	account	EdDSA	ed25519	SHA-256 and SHA-512 in EdDSA *	base32	none
Binance Coin	Ethereum ERC-20 token *					
Tether	Bitcoin Omni layer / Ethereum ERC-20 token					
TRON	UTXO	ECDSA	secp256k1	SHA-256	base58	last 20 bytes of Keccak-256 *
Cardano	UTXO	EdDSA	ed25519	none and SHA-512 in EdDSA *	base58	none
Monero	UTXO *	*it's complicated**	ed25519	Keccak-256 *	base58	Keccak-256 *
IOTA	UTXO	Winternitz one time signature scheme	-	Curl, Kerl *	none	Kerl
Dash	UTXO	ECDSA	secp256k1	SHA-256 *	base58	SHA-256, RIPEMD-160
Maker	Ethereum ERC-20 token					
NEO	account	ECDSA	secp256r1	SHA-256	base58	SHA-256, RIPEMD-160
Ontology	account	ECDSA	nist256p1	3x SHA-256	base58	SHA-256, RIPEMD-160
Ethereum Classic	Same as Ethereum					
NEM	account	EdDSA	ed25519	none and Keccak-256 in EdDSA *	base32	Keccak-256, RIPEMD-160
Zcash	UTXO	ECDSA, zk-SNARKs *	secp256k1, Jubjub *	SHA-256	base58, bech32	SHA-256, RIPEMD-160
Tezos	account	EdDSA, ECDSA *	ed25519, secp256k1, secp256r1	BLAKE2 and SHA-512 in EdDSA *	base58	BLAKE2

COINSOLIDATION

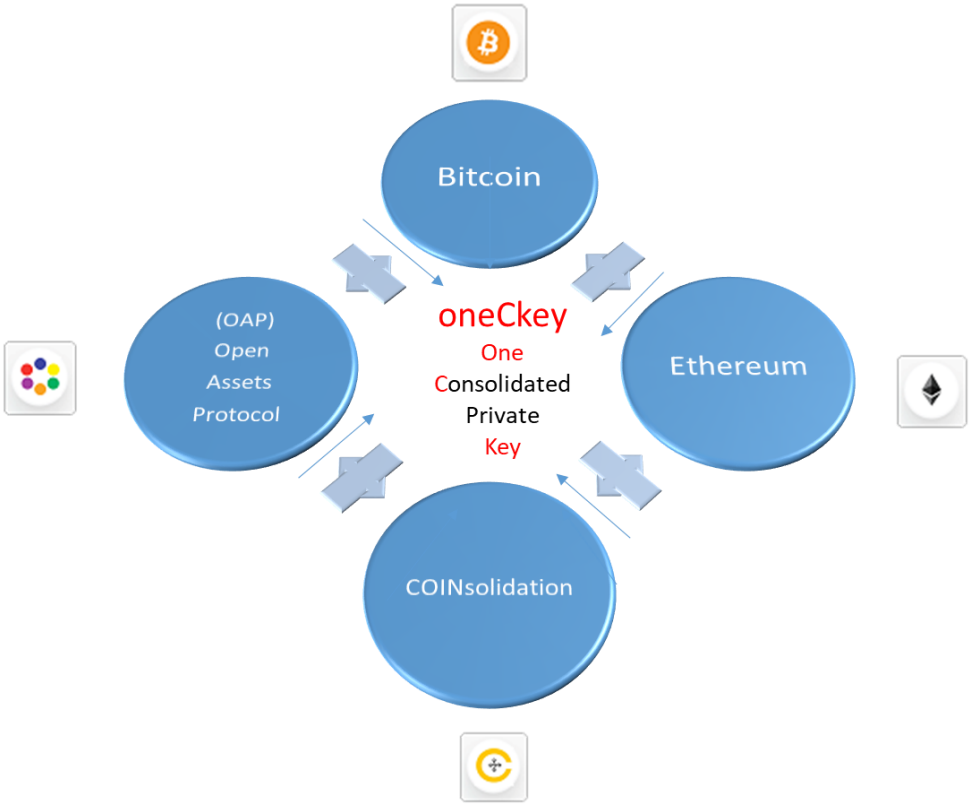
Criptografía para Serie A o Serie "Génesis".

La serie A o serie "Génesis" es la primera consolidación de llaves privadas. Esta serie está formada por la consolidación de las 2 principales criptomonedas y 2 Tokens (Bitcoin, Ethereum, OAP y COINsolidation).

La criptografía aplicada en ambos casos es ECDSA (*Elliptic Curve Digital Secure Algorithm*) que es la que utilizan actualmente en su generación de llaves públicas y privadas tanto Bitcoin como Ethereum.

La generación de la llave privada consolidada integrada por ambos blockchain Bitcoin y Ethereum se puede aplicar en los siguientes casos (3 opciones).

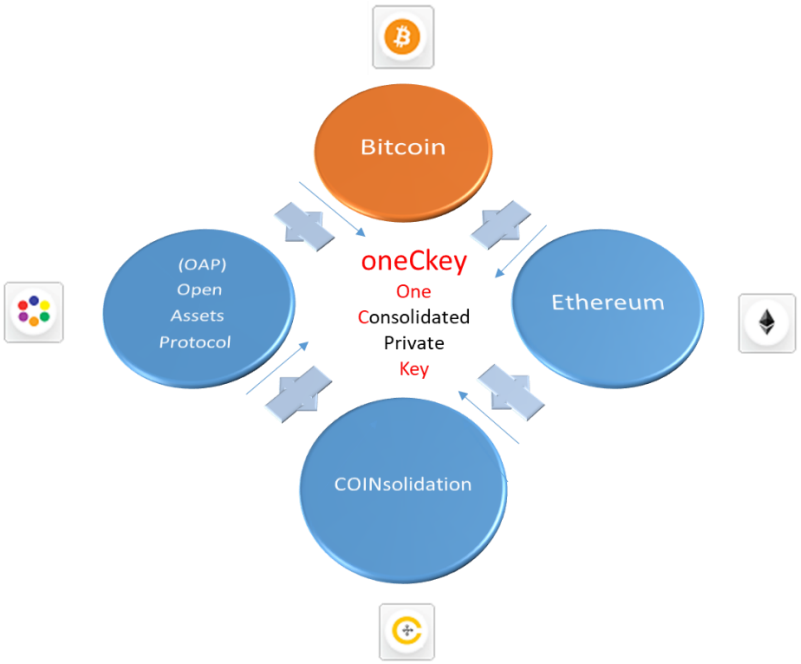
1.- Generación de una llave privada consolidada a partir de QRNG (*Quantum Random Number Generator*)



Generamos un numero aleatorio de una fuente QRNG, proponemos la generación del uso mecánica ópticacuántico mediante una foto con formato RAW para producir la suficiente entropía. Esto se realiza usando el lente del Smartphone, aplicamos hash (SHA254) y hacemos la conversión a hexadecimal para crear la llave privada consolidada, esta la aplicamos el algoritmo oneCKey-secp256k1 para generar las respectivas direcciones de depósito en cada blockchain Bitcoin y Ethereum. Aplicamos a la dirección Bitcoin formato del protocolo OAP (Open Assets Protocol) para generar un ExoToken. Usando oneCKey nos dará una sola llave privada para dos diferentes direcciones de depósito de diferentes blockchain como son Bitcoin y Ethereum, así como la generación de un Token OAP (Open Assets Protocol) para ser usado por el usuario según sus intereses, abriendo una posibilidad de ampliar sus perspectivas de negocios.

OINSOLIDATION

2.- Generación de una llave privada consolidada a partir de una dirección de Bitcoin existente. Se aplica la llave privada Bitcoin al algoritmo oneCKey-secp256k1 para generar una dirección Ethereum y aplicamos a dirección Bitcoin formato del protocolo OAP (Open Assets Protocol) para generar ExoToken.



Ejemplo:

Llave privada Bitcoin existente (en esta aplicamos oneCKey para crear otras direcciónes):

28a0f97c6921e43872eb0640af41a54b9bde57c71cf4efe0db9d829f8b2cf645

Dirección Bitcoin:

18XmTwfTeurjKQ8i1rEQT1DAx8BDjdR96A

Dirección Ethereum:

0x9c789b22758c85f456dca3ac02e1fb00a059a4e

Dirección OAP (Open Assest Protocol) basada en la anterior dirección Bitcoin.

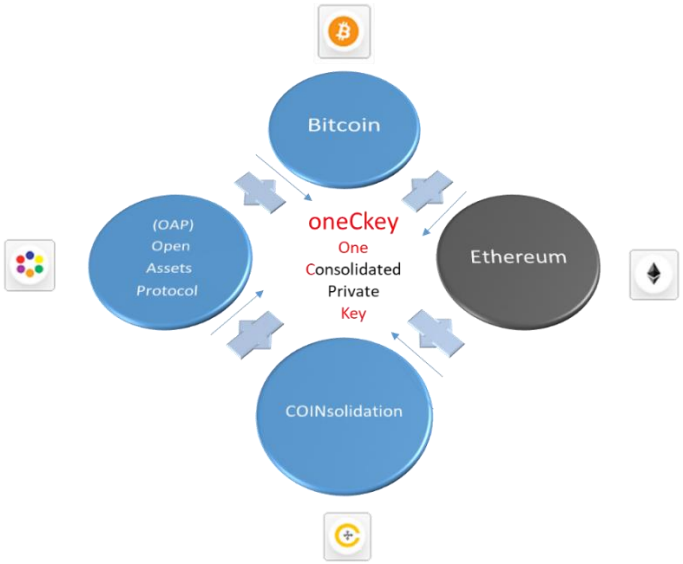
akJVei7Uo8PkRBeJ54ULb6s7kHjMPhs8UjG

Dirección Token COINsolidation:

0x9d08c0ac0f2fdf078c883db6fa617b15776e4b41

3.- Generación de una llave privada consolidada a partir de una dirección de Ethereum existente. Se aplica la llave privada Ethereum al algoritmo oneCKey-secp256k1 para generar dirección Bitcoin y aplicamos a dirección Bitcoin formato del protocolo OAP (Open Assets Protocol) para generar ExoToken.

.



Criptografía para Serie A1.

Donde interviene un total de 5 criptomonedas y 2 Tokens.

En este caso tendremos 5 opciones para crear la oneCKey, podemos usar cada llave privada ya existente de las diferentes criptomonedas soportadas.

COINSOLIDATION

Criptografía para Serie A2.

Ejemplo: Si tomamos la llave privada de DASH aplicando oneCKey generaremos 5 direcciones basadas en la llave privada de DASH y los dos Tokens también dependerán de esta. Una relación de 1:7 (1 llave privada consolidada para 7 direcciones).

Llave privada de DASH (aplicamos oneCKey para crear otras direcciones).

20ba723de1fdeee66e927e30fdb3ada74ae23bfdb370da378f301ce4dbf27312

Dirección DASH:

XtAGtBbnzykDSwoWUSjgQUF4gG1h3uyYKW

Dirección Bitcoin:

1JUS3vwu3GXdJ1CvcZRTYwZGqvRzwT7FEk

Dirección Ethereum:

0x9d4a5854955c8e498e61eaaae7d3846917381f5b

Dirección OAP:

akUSKJ6mEWkRKAFNHfBXeCoTrBXcAyavXnS

Dirección COINsolidation Token:

0x9d08c0ac0f2fdf078c883db6fa617b15776e4b41

Dirección Litecoin

LchPK9Fj7vmgYou5nhQkpxd348oHAJ3aSu

Dirección Dogecoin:

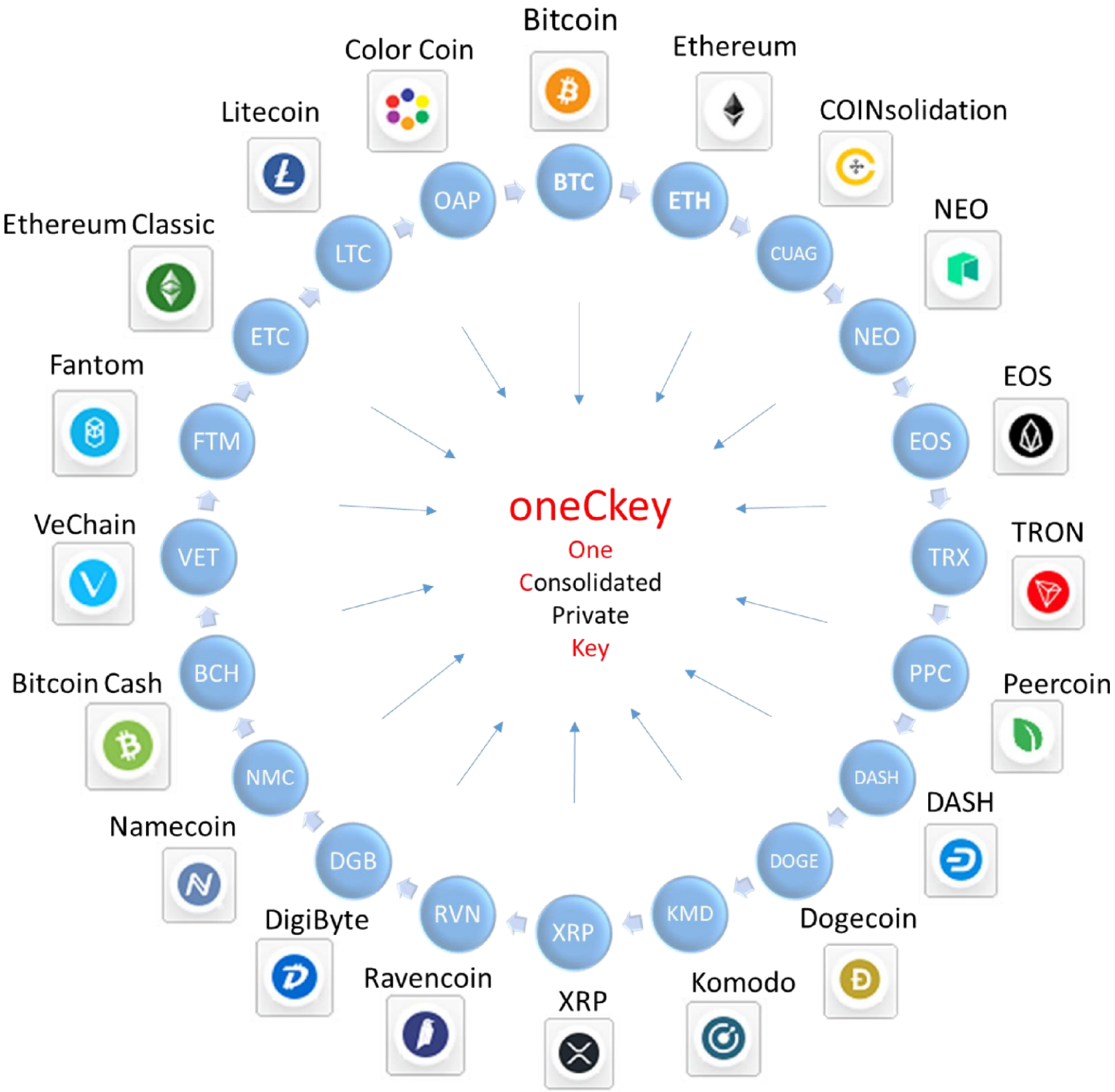
DNcXbBtYLgRuq1PXM9R26hisj4AJGJj4pT

Lo anterior podemos aplicarlo de la misma forma para cualquier dirección ya existente de las criptomonedas antes mencionadas y soportadas por oneCKEY en la serie B. Nos da como resultado una llave privada para usarla en 5 criptomonedas y 2 Tokens.

OINSOLIDATION

Criptografía para Serie A3.

La serie A3 se aplica a 18 criptomonedas y 2 Tokens. Lo que sería una relación 1: 20 (una llave privada consolidada para uso común en 20 direcciones).



Lo anterior podemos aplicarlo de la misma forma para cualquier dirección ya existente de las criptomonedas antes mencionadas y soportadas por oneCKEY en la serie A3.

Ejemplo: A la llave privada de Bitcoin aplicando oneCKey generaremos 18 direcciones con una sola llave privada y dos Tokens de esta. Una relación de 1:20 (una llave privada consolidada para 20 direcciones).

Llave privada de Bitcoin (aplicamos oneCKey para crear otras direcciones).

d2783ceae51a0c74fb733640f7128092dba3093605232b2b76fb102dca092d69

1. Dirección Bitcoin:
   1N67xWPN9F1sEMXparSpzT24erp5F2p6LK
   https://www.blockchain.com/explorer

2. Dirección Ethereum:
   0x91efb31bcd0bd12a088f9625344bbe92c1543bc3 https://etherscan.io/

3. Dirección COINsolidation:
   0x9d08c0ac0f2fdf078c883db6fa617b15776e4b41 https://etherscan.io/

4. Dirección Wallet EOS:
   5KQykH8ssQkwsmUWffvrbgsMRf5wh8iHofZGvkHou5h1HYCqJYp

5. Dirección TRON:
   TPGr8Vp78vNcfhSvnpp7EnucaBKEBXns7h (*The account is not activated.)*
   https://trx.tokenview.com/

6. Dirección Peercoin:
   PVgJ7UnDCAW4DCCavvmMfLzLGbyxJ4HRpP
   https://blockbook.peercoin.net/

7. Dirección DASH:
   Xwmxnm3G6xETPJ8QSjm3qyhrVCPmECp3dt
   https://explorer.dash.org/insight/

8. Dirección Dogecoin:
   DSEDVmL1Sev9mMiRKSSPYDBfXzYNYadkdV
   https://blockchair.com/dogecoin

9. Dirección Komodo:
   RWNK32Gek4pSJMu242Rx5yMGR8GfprvY69 https://kmdexplorer.io/

10. Dirección XRP:
    r4afxWP49Er1NMXF2iSFzTpheiFnEpFaLK (*The account is not activated.)*
    https://bithomp.com/explorer/

11. Dirección Ravencoin:
    RWNK32Gek4pSJMu242Rx5yMGR8GfprvY69

https://ravencoin.network/

12. Dirección DigiByte:
    DSEDVmL1Sev9mMiRKSSPYDBfXzYNYadkdV
    https://digibyteblockexplorer.com/

13. Dirección Namecoin:
    NHfVA9tM4d7RktnKrfmQCyAyP6D8AQ2rA5
    https://www.cryptoground.com/namecoin-block-explorer

14. Dirección Bitcoin Cash:
    1N67xWPN9F1sEMXparSpzT24erp5F2p6LK (New format to see explorer site)
    https://explorer.bitcoin.com/bch New format address:
    bitcoincash:qrn49p6cy49tzgatt9gz9xz3gf8qxwl9tu800hul9m

15. Dirección VeChain:
    0x91efb31bcd0bd12a088f9625344bbe92c1543bc3 https://explore.vechain.org

16. Dirección Fantom:
    0x91efb31bcd0bd12a088f9625344bbe92c1543bc3
    https://explorer.fantom.network/

17. Dirección Ethereum Classic:
    0x91efb31bcd0bd12a088f9625344bbe92c1543bc3
    https://etcblockexplorer.com/

18. Dirección Litecoin:
    LgK5DihCDuFvVADykzS8GU5ps5BMGWfCXX
    https://blockchair.com/litecoin

19. Dirección Color coin:
    akY41CgChciuZ6bhBdUZ1eJvdzTzF9Sizv3 https://blockchainexplorer.lykke.com/

20. WIF (Wallet Import Format) - NEO use secp256r1, Do not use secp256k1).
    Para obtener dirección importar WIF sitio: https://neotracker.io/wallet/open-wallet usa WIF como Private Key.

    WIF (Wallet Import Format) NEO:
    L4GqU2DmXVryD5JRwgphv6yF9q6pQ93FAyBTJE5BzshaFnwXPB4H
    Dirección NEO:
    AKkcm37QeMxZpFfRrrLGeqFRgkFzMPH9Gn
    https://neotracker.io/

21. Dirección ExoCrypto:
    Exo41CgChciuZ6bhBdUZ1eJvdzTzF9Sizv3 https://exoCrypto.com

Resumen de cryptomonedas soportadas y clasificadas por las dos curvas ECC. (secp256k1 & Ed25519)

COINSOLIDATION

Serie A3 (secp256k1) – Ready

1. Bitcoin*
2. OAP***
3. Ethereum**
4. COINsolidation***
5. XRP
6. NEO
7. EOS
8. TRON
9. Dash
10. Bitcoin Cash*
11. Ethereum Classic**
12. Litecoin
13. Dogecoin
14. VeChain**
15. DigiByte
16. Fantom**
17. Ravencoin
18. Komodo
19. Peercoin
20. Namecoin

(*) Criptomonedas Bitcoin con la misma dirección ya que el algoritmo para generarlas es el mismo únicamente cambia el blockchain que es diferentes para las transacciones de cada una.
(**) Criptomonedas Ethereum con la misma dirección ya que el algoritmo para generarlas es el mismo únicamente cambia el blockchain que es diferentes para las transacciones de cada una.
(***) Tokens generados y dependientes de la llave primaria consolidada.

Roadmap Serie A4 incluye Serie A3 + Zcash, Binance BNB, Filecoin, Tether, Tezos, Cosmos, Zilliqa y Avalanche. Q4-2021

Roadmap inicia Serie B1 con Curve Ed25519. (Polkadot, Cardano, Monero, Stellar,Algorand, IOTA, Elrong, Algorand, y Waves) liberación Q42021.

Serie B1 (Ed25519) –Q42021

1. Polkadot
2. Cardano
3. Monero
4. COINsolidation***
5. Stellar
6. Algorand
7. IOTA
8. Elrong
9. Decred
10. Nano
11. Horizen
12. Siacoin
13. Stacks
14. Lisk
15. Qtum
16. Waves 17. ….Others.

NOTA: Pueden variar los cripto-activos de cada serie dependiendo del comportamiento del mercado de criptomonedas puede la lista ser modificada, según la liquidez de cada activo.

Seguridad implementada en oneCKey, algoritmos PQC - (Post-Quantum Cryptography) embebido en el repositorio donde se almacena la llave consolidada generada de forma local en cada Smartphone o en su caso una llave ya existente introducida por el usuario.

Para la codificación segura de la oneCKey hemos implementado una combinación de algoritmos de seguridad PQC compuesta con: AES-CGM + chacha20poly1305.

Chacha20poly1305: https://tools.ietf.org/html/rfc7539
AES-CGM: https://tools.ietf.org/html/rfc5288

U = operador de aplicación de algoritmos PQC.

Cifrado de oneCKey = U (AES-CGM (chacha20poly1305 (OneCKey)))

Aplicamos Mini PQC software para android con operador; Insert DB SQLite en (A).

https://github.com/openqbit-diy/MiniPQC

Calculo de AES-CGM para soportar ataques con computación cuántica.

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required	Time Required to Break System	Quantum-Resilient Replacement Strategies
AES-GCM	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} yrs 1.97×10^{22} yrs 2.29×10^{32} yrs	
RSA	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,290 4,338 8,434	2.56×10^6 6.2×10^6 1.47×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete -log problem	Asymmetric encryption	256 386 512	128 192 256	Shor's algorithm	2,330 3,484 4,719	3.21×10^6 5.01×10^6 7.81×10^6	10.5 hours 37.67 hours 95 hours	Move to NIST-selected PQC algorithm when available
SHA256	Bitcoin mining	N/A	72	Grover's algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iteration	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from passwordbased authentication

Algoritmo CUA creación direcciones consolidadas.

Actualmente las fusiones de empresas están al día, ya sea por un bien económico, tecnológico o de mercado.

Presentamos el primer modelo de fusión de criptoactivos o crypto-tokens basado en un algoritmo para crear una dirección consolidada que se usa y genera en el ambiente de COINsolidation.

Creamos tres tipos de direcciones consolidadas.

- **CUA** (Consolidated Universal Address) esta se usa para consolidar y crear un nuevo ExoToken (activo) para ser usado por el usuario. La combinación sera Cryptocurrency con Cryptocurrency. En el caso de la CUA se tiene la primera serie creada llamada CUAG (Coinsolidated Universal Address Genesis).
- **HAC** (Hibric Address Consolidated) se usa cuando necesitamos consolidar una direccion referente a una cryptocurrency y/o token y una direccion normal de tranferencia de activos.
- **DAC** (Dual Address Consolidated) esta se usa para administrar y consolidar dos direcciones normales de Token un mismo blockchain o de dos diferentes tecnologias, son direcciones simples de tranferencia de activos referidos a Token-Token.

Empecemos por ver las ventajas de la CUA.

Una dirección CUA está formada por la dirección del token COINsolidation (dirección estática) y un token adicional conocido como “Colored Coin” (dirección variable). En este caso podemos ver que las direcciones CUA siempre estarán formados por direcciones de algún tipo de combinación de activo (Criptomonedas o tokens).

En nuestro caso cuando consolidamos el token COINsolidation y un token OAP lo conoceremos como la “CUA génesis” o CUAG (Consolidated Universal Address Génesis).

El token COINsolidation esta creado en el blockchain Ethereum y usa el standard ERC20 (Ethereum Request for Comments 20).

El token “Colored coin” está basado y creado en el blockchain de Bitcoin y usa el standard Open Assest Protocol (OAP).

Empecemos a revisar cual es el potencial y beneficio de consolidar direcciones.

- Para los usuarios que creen una CUA se podrá crear un token (OAP) que puede personalizar el usuario creador de la CUA, el usuario tendrá la posibilidad de tener su propio token o crypto activo para que lo pueda usar en la creación, soporte o expansión de su(s) negocios, de una forma simple y sencilla tendrá un activo en el mundo de los crypto-tokens.

- Para las empresas que creen una CUA podrán tener un token (OAP) que podrán usar para crear valor en su cadena de suministros o usar el activo en transacciones de liquidez basadas en el soporte económico de sus activos y pasivos de la empresa.

- Para las cryptomonedas y tokens existentes al crear una CUA, podrán usar su dirección que identifica su activo y al consolidarla con el token (OAP) podrán crecer su demanda ofreciendo a sus inversionistas actuales y futuros su propio token para sus usuarios.

OINSOLIDATION

Nuestras direcciones universales consolidadas CUA (Consolidated Universal Address) son creadas utilizando el siguiente algoritmo:

Paso 1.- Seleccionamos las direcciones en Bitcoin y Ethereum.

Dirección Bitcoin – (BTC). – dirección A1

1Hjx3CanChCytqVz7vek1SSvN1momghJ42

Dirección Ethereum – (ETH) – dirección A2

0x9d08c0ac0f2fdf078c883db6fa617b15776e4b41

Paso 2.- Se obtiene el SHA512(address String-Texto) de cada dirección quitando el primer elemento de cada dirección y se toma de SHA512 los dos caracteres situados en los lugares 120 al 121 de cada hash operación simbolizada con "U". Números verificadores.

U(SHA512(**Hjx3CanChCytqVz7vek1SSvN1momghJ42**)) = **bf**

U(SHA512(**x9d08c0ac0f2fdf078c883db6fa617b15776e4b41**)) = **28**

Paso 3.- Se toma el primer elemento (carácter) de cada dirección empezando por la dirección con menor tamaño en número de elementos y se obtiene la cadena "10".

A10[0] = 1

A20[0] = 0

Paso 3.- Se les obtiene el SHA512 sin los elementos del paso 3 y se toman solo los cuatro caracteres situados en el lugar 120 al 123.

U(SHA512(**Hjx3CanChCytqVz7vek1SSvN1momghJ42**x9d08c0ac0f2fdf078c883db6fa617b15776e4b41)) = **140c**

Paso 4.- Se concatenan los caracteres de cada dirección uno a uno iniciando por la dirección que tenga menos caracteres que la componga, en caso de tener la misma cantidad de caracteres la concatenación puede iniciar de cualquier dirección.

Address 1 = A10[0], A11[1], A12[2], A13[3], A14[4]……..A1N[n], A1N+1[n+1].

Address 2 = A20[0], A21[1], A22[2], A23[3], A24[4]……..A2N[n], A2N+1[n+1].

Concatenación de direcciones:

A10[0] + A20[0] + A10[1] + A20[1] + A11[2] + A22[2] + …. A1N+1[n+1] + A2N+2[n+1].

**Últimos caracteres que no se puedan concatenar se ponen al principio de la cadena y el paso 3 se anexa al final de la cadena concatenada.

776e4b41 Hxj9xd30C8acn0CahcC0yft2qfVdzf70v7e8kc18S8S3vdNb16mfoam6g1h7Jb4125 **10**

Paso 4.- Se agrega al principio el número de caracteres la cadena que NO se pudieron concatenar en el paso 4.

8776e4b41Hxj9xd30C8acn0CahcC0yft2qfVdzf70v7e8kc18S8S3vdNb16mfoam6g1h7Jb412510

Paso 5.- Se agrega al inicio de la cadena dos enteros verificadores XX que nos ayudaran a verificar si la diferencia de las cadenas (resta) la de mayor tamaño menos la menos, siempre debe de dar un numero entero positivo este par de enteros nos apoyara para evitar errores en la concatenación. En caso de que sea la diferencia sea menor o igual a "9" el numero verificador será "00" en caso de ser mayor a "9" la diferencia se marcar en estos dos dígitos.

En nuestro caso de la generación entre Bitcoin y Ethereum siempre los dos dígitos verificadores serán "00".

008776e4b41Hxj9xd30C8acn0CahcC0yft2qfVdzf70v7e8kc18S8S3vdNb16mfoam6g1h7Jb412510

Paso 6.- Se concatenan los dos pares de verificadores del paso 2 de cada dirección al principio de la cadena resultado del paso 3 en el mismo orden A1 + A2.

bf28008776e4b41Hxj9xd30C8acn0CahcC0yft2qfVdzf70v7e8kc18S8S3vdNb16mfoam6g1h7Jb412510

Paso 7.- Se integra al final de la cadena los 4 dígitos del SHA512 del paso 3.

bf28008776e4b41Hxj9xd30C8acn0CahcC0yft2qfVdzf70v7e8kc18S8S3vdNb16mfoam6g1h7Jb412510**140c**

Paso 8.- Se integra la identificación de **CUA** (Consolidated Universal Address "Genesis") Dirección Universal Consolidada al inicio de la dirección creada en el paso 5.

CUAfd55008776e4b41Hxj9xd30C8acn0CahcC0yft2qfVdzf70v7e8kc18S8S3vdNb16mfoam6g1h7Jb412510140c

En el caso de la consolidación de direcciones Bitcoin y Ethereum dará una dirección formada por **90 caracteres hexadecimales.