Expertos del Protocolo

Clase 3

Librería de Satoshi

₿4OS

</bitcoin for open source>

CLASS OVERVIEW

1. Hashes
2. Wallets
   - Keys
   - Independent / Deterministic / HD
   - Descriptors
   - Seeds & Passphrases
   - Keys derivation
3. Blockchain
   - Estructura de bloque
   - Merkle trees

B4OS

Hashes

Hashes -> Camino de ida

Principales características

- Determinístico: misma entrada, misma salida
- Irreversible: teniendo un hash, no podemos calcular origen
- Tamaño de salida fijo, sin importar la entrada
- Efecto avalancha: pequeños cambios, diferente resultado
- Nos permite obtener una "huella digital"

- Recordar: sha256 -> 256 bits -> 32 bytes -> 64 caracteres hexa

https://emn178.github.io/online-tools/sha256.html

B4OS

Wallets y Keys

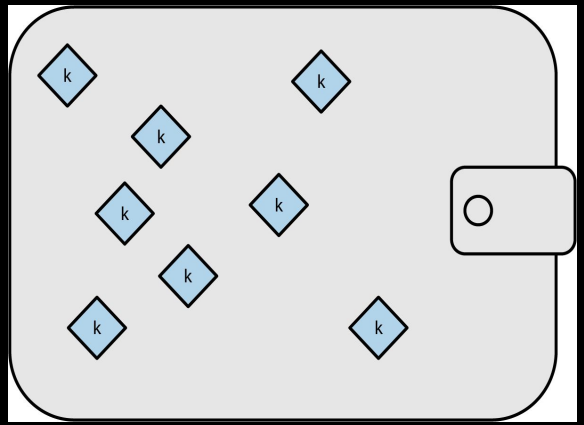
Generando llaves

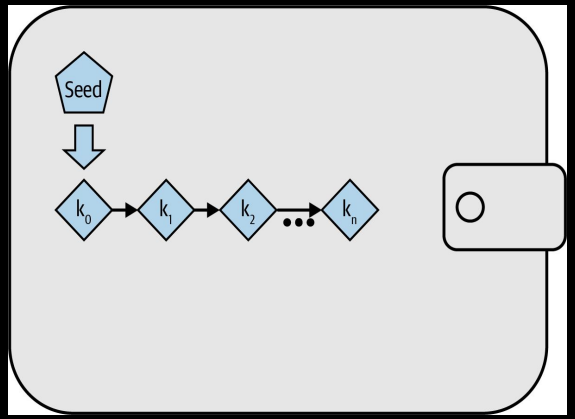
Llave privada: número aleatorio del cual se puede obtener una llave pública

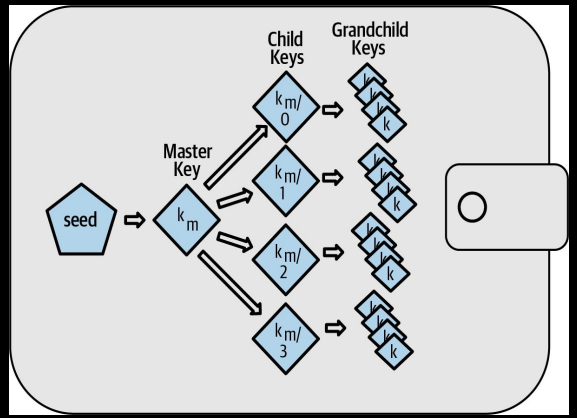
Independientes

Determinísticas

Determinísticas Jerárquicas







Derivation Paths y Descriptors

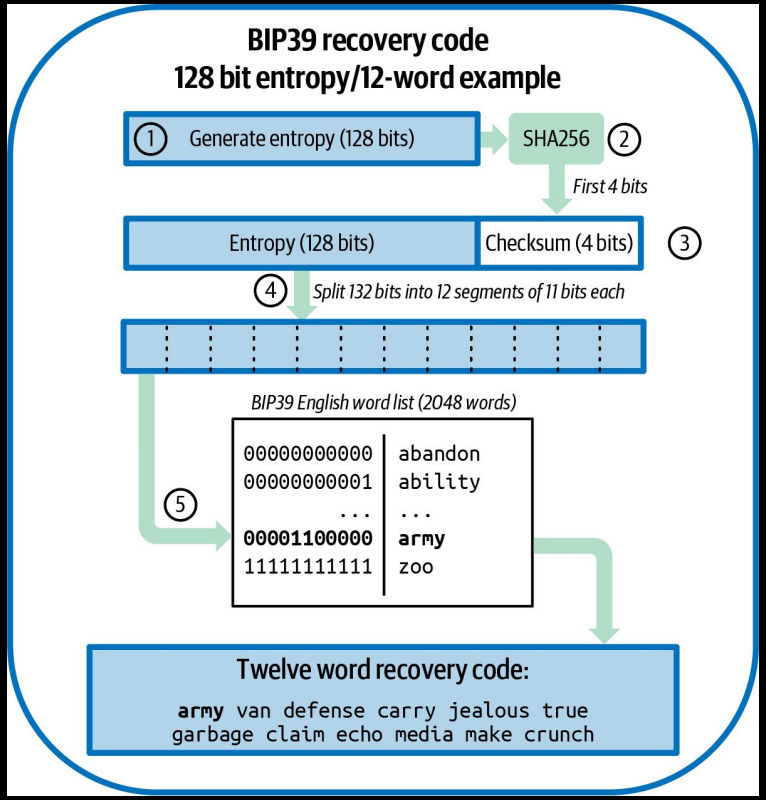
Información sensible en cuanto a privacidad. No pone en riesgo los fondos

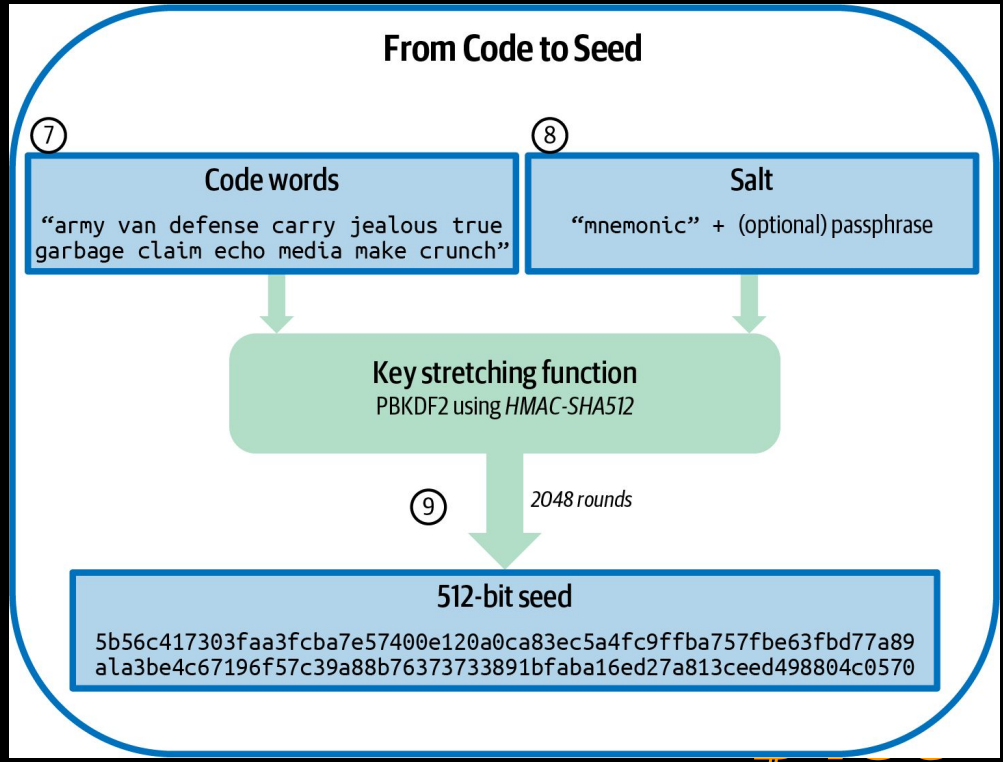
Implicit script paths defined by various BIPs

Standard	Script	BIP32 path
BIP44	P2PKH	`m/44'/0'/0'`
BIP49	Nested P2WPKH	`m/49'/1'/0'`
BIP84	P2WPKH	`m/84'/0'/0'`
BIP86	P2TR Single-key	`m/86'/0'/0'`

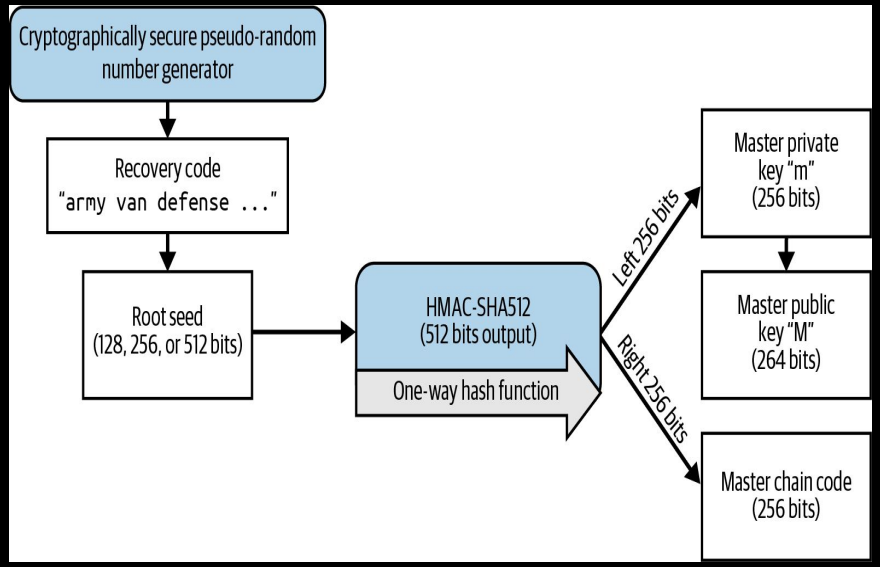
Descriptor	Explanation
`pkh(02c6…9ee5)`	P2PKH script for the provided public key
`sh(multi(2,022f…2a01,03ac…ccbe))`	P2SH multisignature requiring two signatures corresponding to these two keys
`pkh([d34db33f/44'/0'/0']xpub6ERA…RcEL/1/*)`	P2PKH scripts for the BIP32 `d34db33f` with the extended public key (xpub) at the path `M/44'/0'/0'`, which is `xpub6ERA…RcEL`, using the keys at `M/1/*` of that xpub

Mnemonic phrase, seed y ***Passhprase***



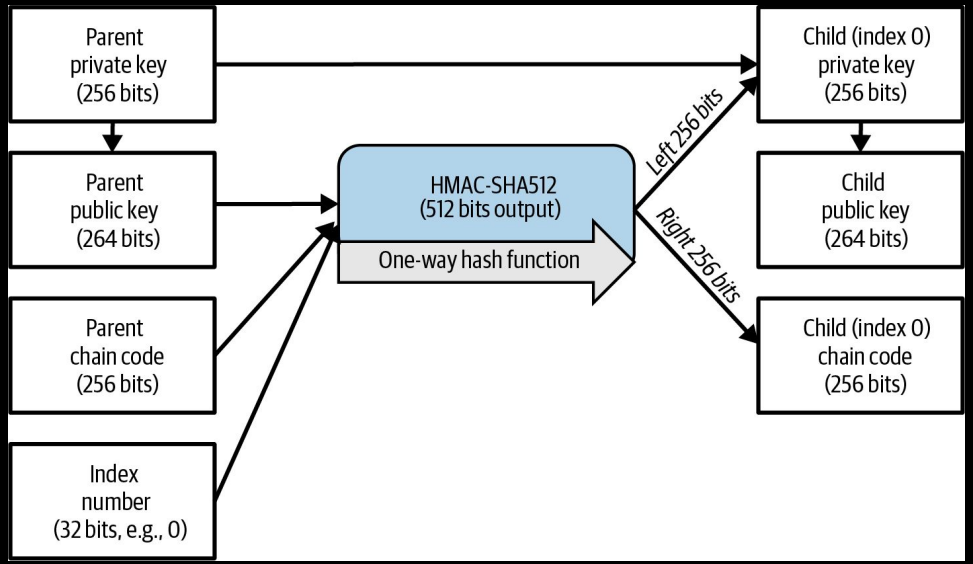


Hierarchical Deterministic Key Generation

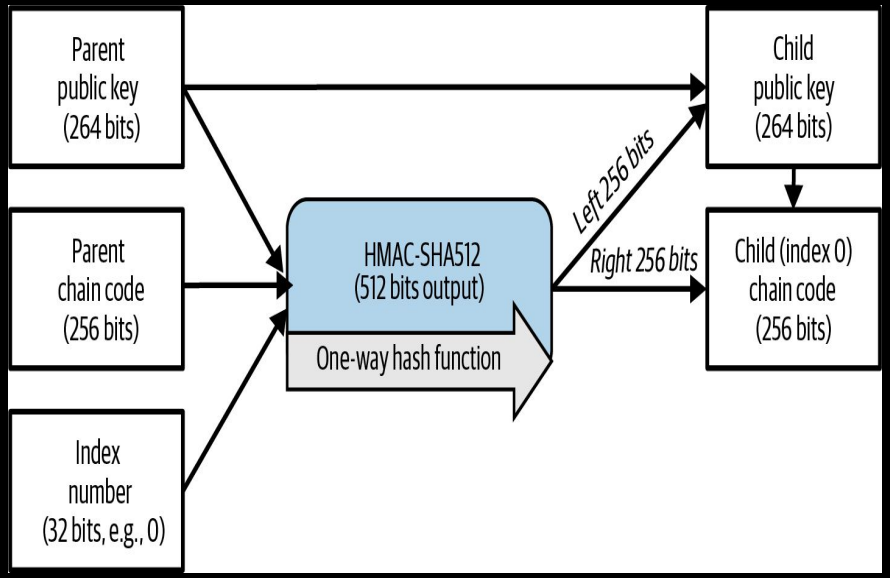


Master Private key from seed

Child Private key from Master Private Key

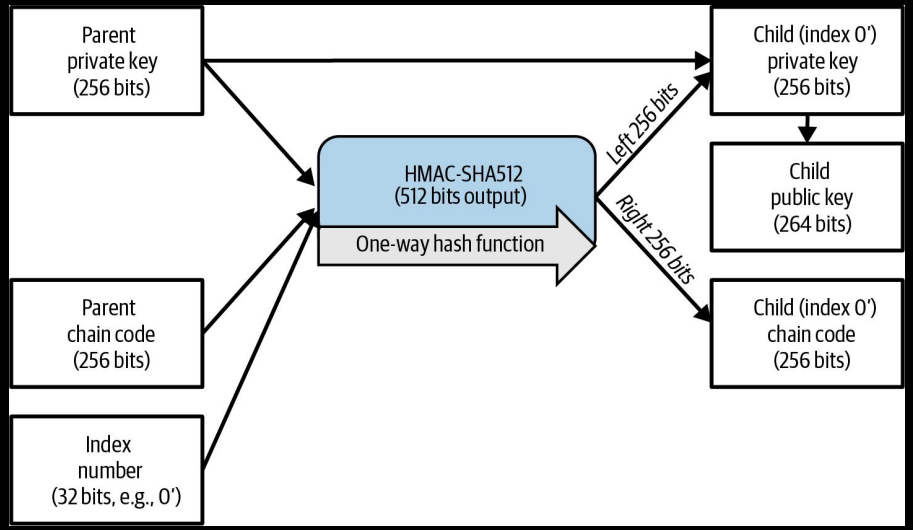


Hierarchical Deterministic Key Generation



Deriving child public Key

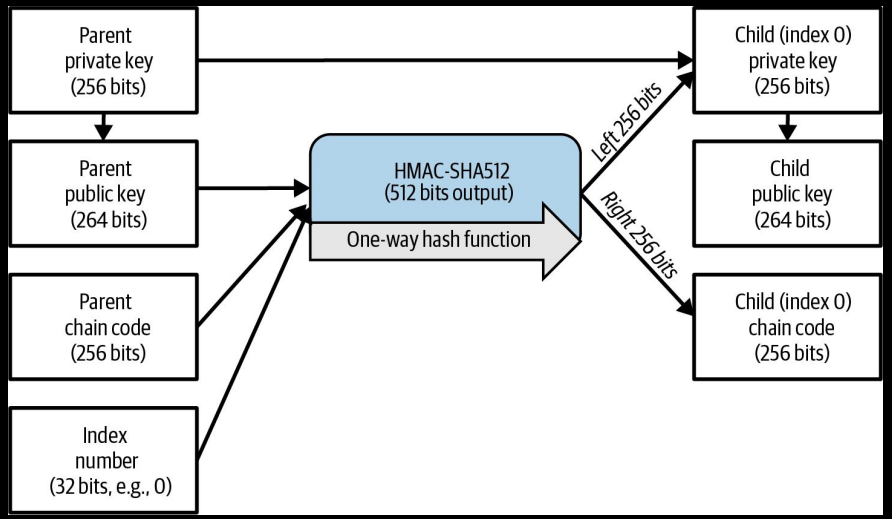
Hardened Private Key



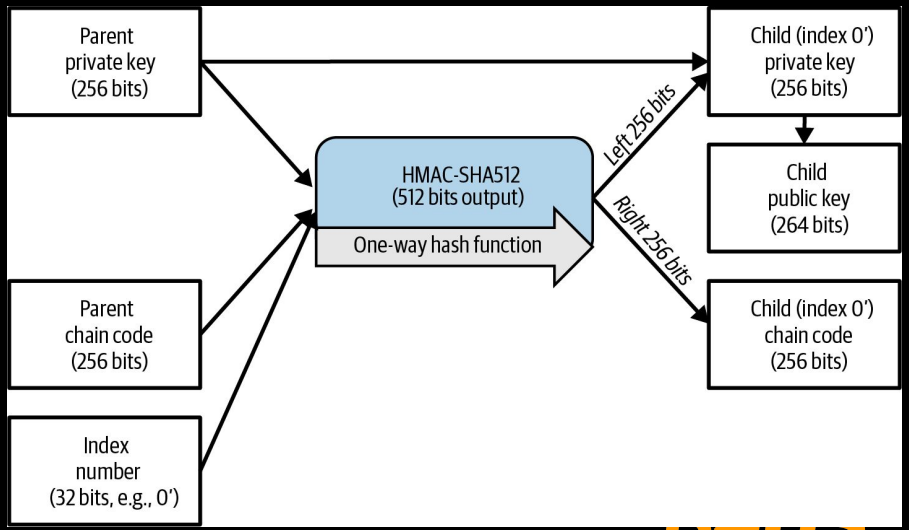
Non Hardened Vs. Hardened

Resumen: usar siempre Hardened.... a menos que sepas por que prefieres usar la otra

Non Hardened



Hardened



Blockchain

B4OS

Estructura de un bloque

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1–3 bytes (compactSize)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Encabezado del bloque

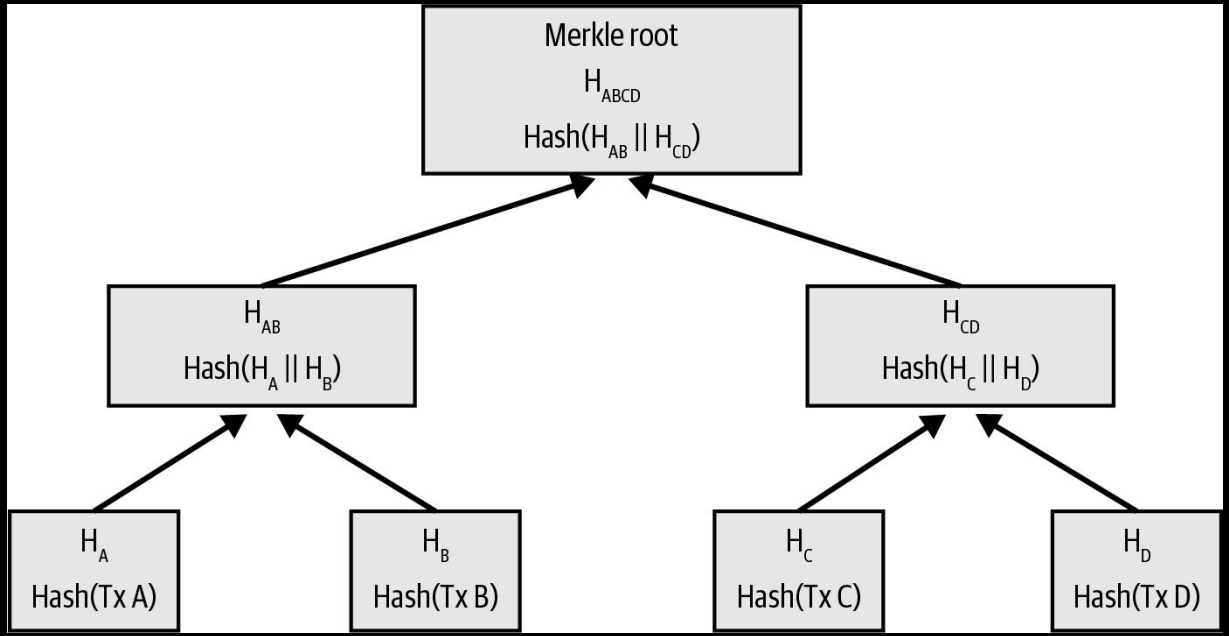
Size	Field	Description
4 bytes	Version	Originally a version field; its use has evolved over time
32 bytes	Previous Block Hash	A hash of the previous (parent) block in the chain
32 bytes	Merkle Root	The root hash of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (Unix epoch time)
4 bytes	Target	A compact encoding of the proof-of-work target for this block
4 bytes	Nonce	Arbitrary data used for the proof-of-work algorithm

Merkle Trees

B4OS

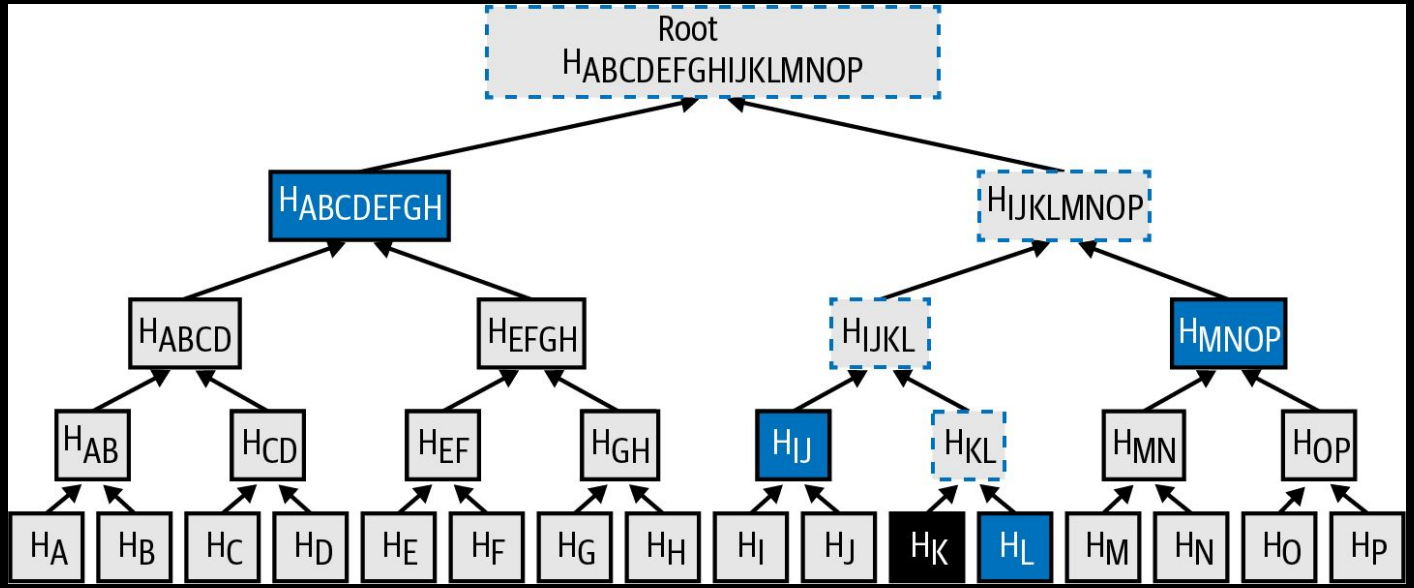
Calcular Merkle tree

Bitcoin usa el hash double-sha256



Comprobar información en el árbol

Podemos hacerlo sin conocer el resto de transacciones



B4OS

Preguntas y Dudas

B4OS

libreriadesatoshi.com & b4os.dev

B4OS