Foundations of Blockchain

Cryptographic Primitives and Wallets

Matteo Nardelli

October, 2023

Key Cryptographic Functions

Hash Functions

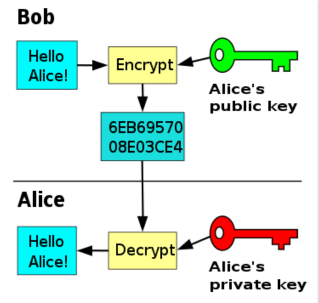
- A hash function H accepts a variable-length block of data M as input and produces a fixed-size hash value $h = H(M)$;
- Good hash function: large set of inputs will produce outputs that are evenly distributed and apparently random;
- **Data integrity**: A change to any bit in M results, with high probability, in a change to the hash value.
- SHA-256 is the most extensively used hash function in blockchains.
    - sha256(hello world!) = 7509e5bda0c762d2bac7f90d758b5b2263fa01ccbc542ab5e3df163be08e6ca9
    - Suffers from length extension attack , i.e., that sha256(m_1) that can be used to compute sha256($m_1||m_2$);
    - Bitcoin uses double SHA-256 to prevent this.

Asymmetric Key Cryptography

- Leverages a (secret) **private key** and a **public key**;
- Both the keys can be used to encrypt data, obtaining different applications. The other key is then used to decrypt the data.

Encryption/decryption:

- When message encrypted with public key;
- Usually slower than symmetric key encryption (e.g., AES);

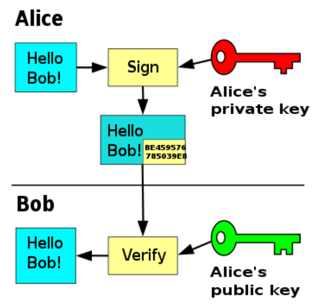


Asymmetric Key Cryptography

- Leverages a (secret) **private key** and a **public key**;
- Both the keys can be used to encrypt data, obtaining different applications. The other key is then used to decrypt the data.

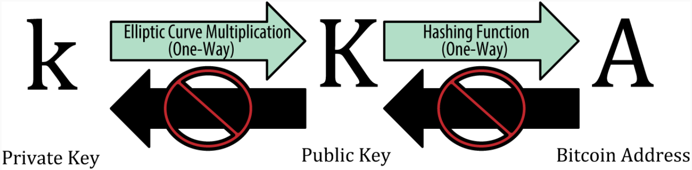
Digital signature:

- When message encrypted with private key;
- Provides non-repudiation property;
- Popular Schemes: DSA, ECDSA, and Schnorr (based on the difficulty of computing discrete logarithms).



Addresses

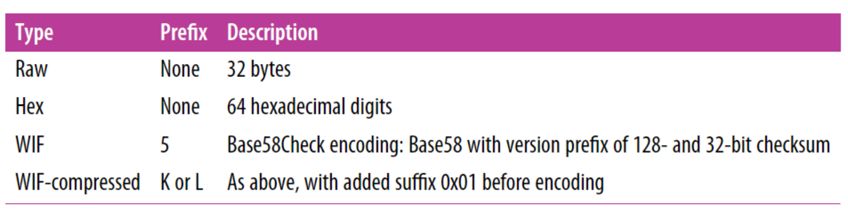
- The private key (k) is a number, usually picked at random.
- From k, a one-way cryptographic function generates a public key (K).
- From K, a one-way cryptographic hash function generates an address (A).
  - An address is used to receive money (e.g., can be represented as a QR-code);
  - In BitCoin, $A = RIPEMD160(SHA256(K))$; then, encoded as Base58Check to help human readability, e.g., `1PRTTaJesdNovgne6Ehcdu1fpEdX7913CK`;
  - Addresses can be used without authorization: they are not stored in the blockchain until their first usage;



Key Format

- Both private and public keys can be represented in a number of different formats.
- WIF: Wallet Import Format (read more)

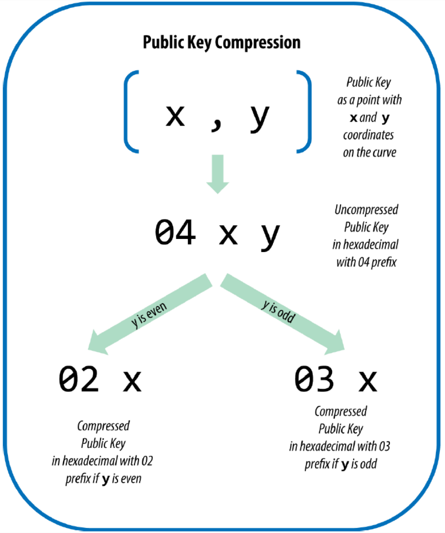
Private Key encoding:



Type	Prefix	Description
Raw	None	32 bytes
Hex	None	64 hexadecimal digits
WIF	5	Base58Check encoding: Base58 with version prefix of 128- and 32-bit checksum
WIF-compressed	K or L	As above, with added suffix 0x01 before encoding

Key Format

Public keys are usually presented in either compressed or uncompressed way.



Public Key Compression
x , y
Public Key as a point with x and y coordinates on the curve
04 x y
Uncompressed Public Key in hexadecimal with 04 prefix
y is even
y is odd
02 x
03 x
Compressed Public Key in hexadecimal with 02 prefix if y is even
Compressed Public Key in hexadecimal with 03 prefix if y is odd

Wallets

Wallet

A wallet:

- Does not physically hold cryptocurrencies;
- Stores pairs of public-private keys;
- Provides digital signatures that authorize transactions;
- Additional features: view balance, receive funds, user-interface, encodes addresses e.g., in QR codes, avoid address reuse;

Wallet

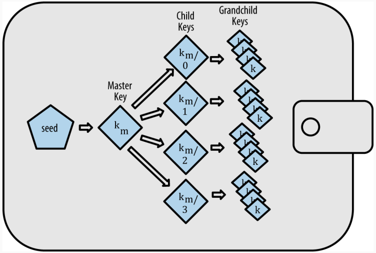
A wallet:

- Does not physically hold cryptocurrencies;
- Stores pairs of public-private keys;
- Provides digital signatures that authorize transactions;
- Additional features: view balance, receive funds, user-interface, encodes addresses e.g., in QR codes, avoid address reuse;
- **Deterministic wallet** can derive a *sequence* of private-public keys from a master key (or, *seed*);
    - Using different addresses (hence, public key) for each transaction can help improving privacy;

Hierarchical Deterministic Wallet

A Hierarchical-deterministic (HD) wallet:

- derives a *tree* of private-public keys from a master key;
- allows to generate a new key pair for each crypto transaction to enhance privacy and security;
- Reference standard for HD wallet: BIP-32;
- The tree root (i.e., the master key) can be (deterministically) derived from a *seed*;
- The seed can be a sequence of words, called *mnemonic*: BIP-39;

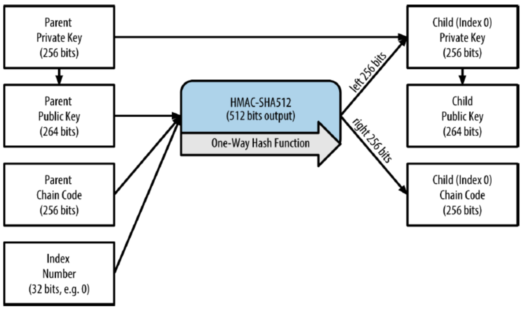


HD Wallet: Child Private Key Derivation

The child key derivation functions are based on a one-way hash function that combines:

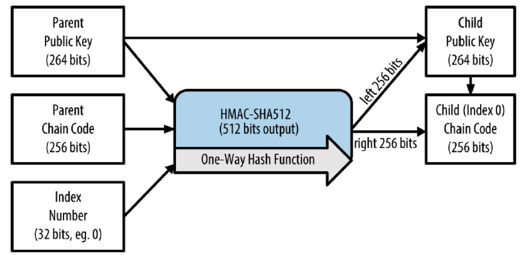
- A parent private or public key (ECDSA uncompressed key);
- A seed called a chain code (256 bits);
- An index number (32 bits)

See BIP-32 for further details.



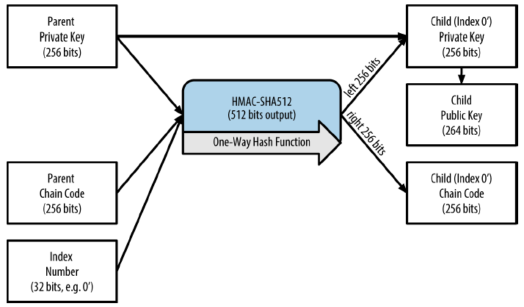
HD Wallet: Child Public Key Derivation

- A very useful characteristic of HD wallets is the ability to **derive public child keys from public parent keys**, *without* having the private keys.
- This gives us **two ways** to derive a child public key: either from the child private key, or directly from the parent public key.



HD Wallet: Hardened Derivation

- Since the extended pubkey contains the chain code, if a child private key is known, it can be used to derive all the other child private keys.
- To counter this risk, HD wallets use an alternative hardened derivation, which breaks the relationship between parent public key and child chain code.



The hardened derivation function uses the parent private key to derive the child chain code, instead of the parent public key.

Wallet: Hot and Cold

Hot Wallet:

- Connected to the Internet (e.g., web-based, mobile, desktop wallets);
- Vulnerable to hacking and online attacks;
- Easy to use;
- Best suited to beginners.

Cold Wallet:

- Kept offline (e.g., paper and hardware wallets);
- Reduced exposure to attacks;
- More expansive;
- Best suited to store crypto over a long period of time.

Wallet: Custodial and Non-custodial

Custodial Wallet:

- A 3rd party (*custodian*) controls of private keys and access to funds;
- Less secure (stored online);
- Less personal responsibility but requires **trust** in the custodian;
- Backups in place (key recovery is easy);
- May require Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) procedures;
- More user-friendly.

Non-Custodial Wallet:

- Users have complete control of their keys;
- More secure (keys held offline);
- Users are wholly responsible for keeping private keys secure;
- No KYC or AML procedures;
- Less user-friendly.

Matteo Nardelli