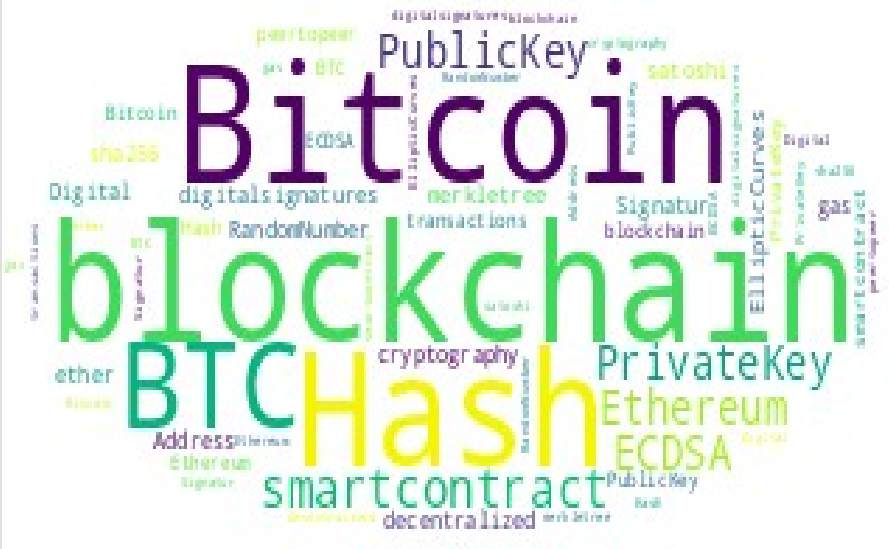


Blockchain Terminology explanation

K. A. Draziotis

Download from https://tinyurl.com/msesyeva

Written with Libreoffice

Key words

When we are learning about blockchain technology, we read very often some terms , such as:

- blockchain
- private keys, public keys,
- digital signatures,
- hash functions,
- bitcoin address,
- wallet,
- merkle trees,
- mining,
- nonce, etc.

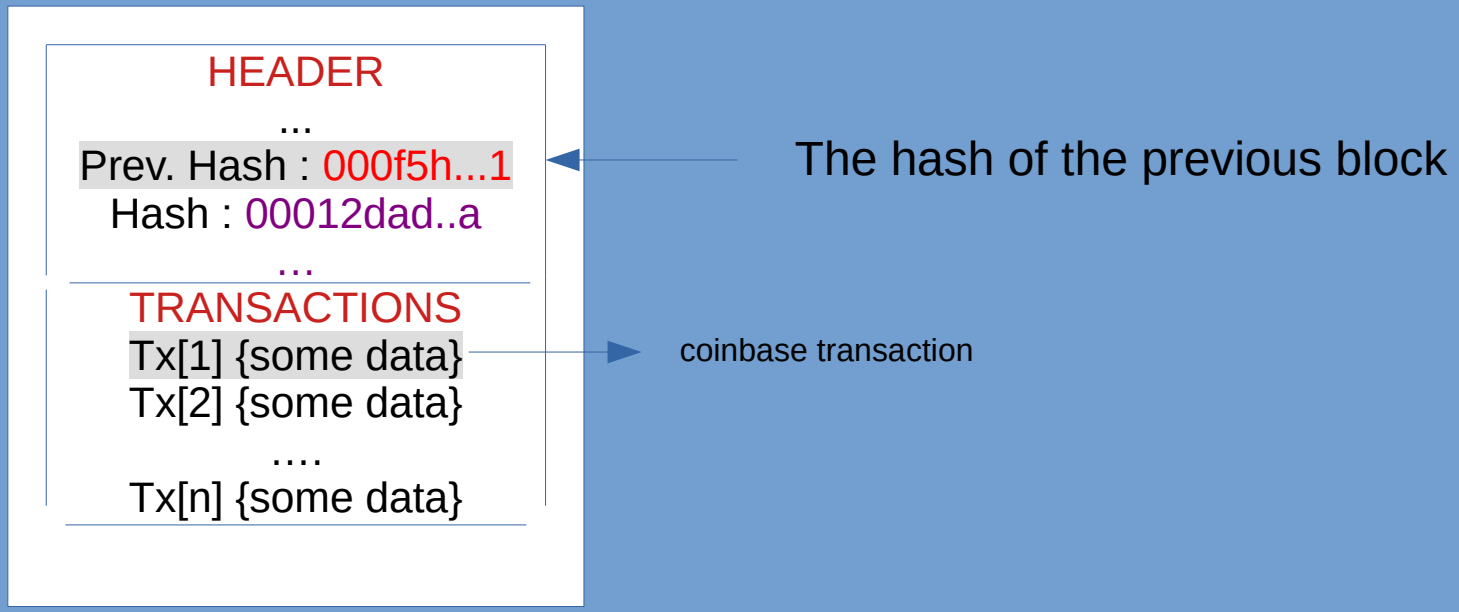
What is a "blockchain"?

1st definition : timestamped append-only log

- Fun fact : Satoshi does not invent blockchain. Stuart Haber. His 1991 paper "How to Time-Stamp a Digital Document", with W. Scott Stornetta, is one of the most important paper for the developing of cryptocurrencies.

2nd definition : distributed database or ledger that is shared among the nodes of a computer network.

A block in a blockchain



For instance :

```
        return
a = print_bitcoin_block(761670)
#print("mining date:",str(a.day)+'/'+str(a.month)+'/'+str(a.year))
```

```
mining date: 4/11/2022
{
    "blocks": [
        {
            "bits": 386376745,
            "block_index": 761670,
            "fee": 815035,
            "hash": "00000000000000000001dbb7b237f576b6885252d81c89a0d815272d1c167fae",
            "height": 761670,
            "main_chain": true,
            "mrkl_root": "e70a1afb0af2948a5a8520e264ebe326b9725030293c13ee3b186e762a7be758",
            "n_tx": 180,
            "next_block": [
                "00000000000000000005d8e2d059d4edf48b3b46d69160d81504527405e49e9"
            ],
            "nonce": 3500027787,
            "prev_block": "00000000000000000000267a68c6ac5a0b9dbdeeceadbdfa7debb3b2fba193161",
            "size": 64415,
            "time": 1667549618,
```

Public keys/Private keys

In blockchain we use Public key cryptography, in fact we are using digital signatures.

- Digital signatures have public and private keys.
- So, what is a private key?

  - You can think it as a large random number which is kept private. We do not disclose it to anyone. A large number is, say, a number with ~256 bits or ~76 decimal digits.
- Now, the chances someone else generates the same private key is negligible.

Public keys/Private keys

- This very long number is generated in practice by our wallet. There is no need our wallet to be online. You can generate it, offline. Wallet, has a suitable software to generate a long random number.
- This process is similar to the precedure of flipping a fair coin.

Public/Private keys

Now, what is a Public key?

- A public key is generated by the private key.

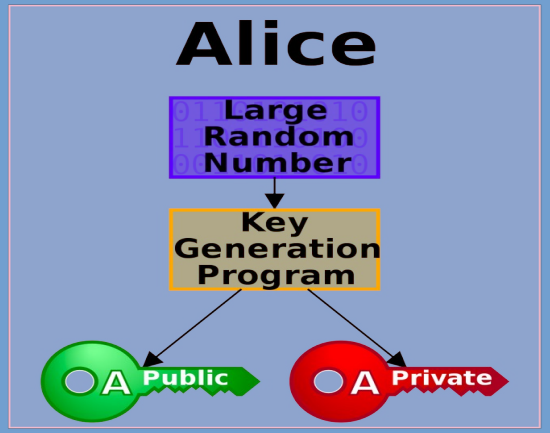
  In Bitcoin and Ethereum the public key is generated using multiplication over an elliptic curve. In fact if k is the private key i.e. a long random integer number, then the public key is k*G, where G is a generator of an elliptic curve.
- The protocol that we use in blockchain (at least in Bitcoin/Etherreum) is called ECDSA.

Public/Private keys

- This pair of keys is used to digitally sign our transactions.
- So, we are using them to generate suitable data that append our original document.
- We sign our transactions with our private key, and anyone that has our public key can verify it with a secure way.

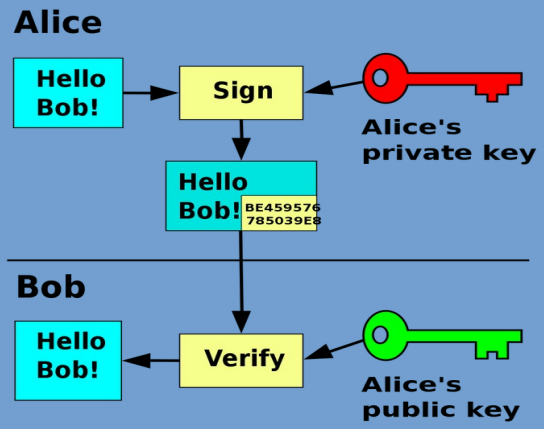
Digital signatures

1st step



Public domain image

2nd step



CC BY-SA 4.0

Bitcoin address

- To understand what is a bitcoin address, we have to understand, except digital signatures, what is a hash function.
- A hash function is something like a fingerprint.
- Fingerprints among persons are almost always different, the same for hash function of some data.
- So, if we feed a hash function with some data, the hash function will return us a “unique” fingerprint of the data.

sha256 hash function

```
[~]:$ echo -n "welcome to OK! thess"|sha256sum
7762e2e3a839ea9f380784a97e2f1315189271754466fa48e687071328bb9e2e  -
[~]:$
```

```
[~]:$ echo -n "welcome to OK thess"|sha256sum
c3bfa2157fdf905522ff012e179c57e2851408c1acfba8f5f35c189878155cac  -
```

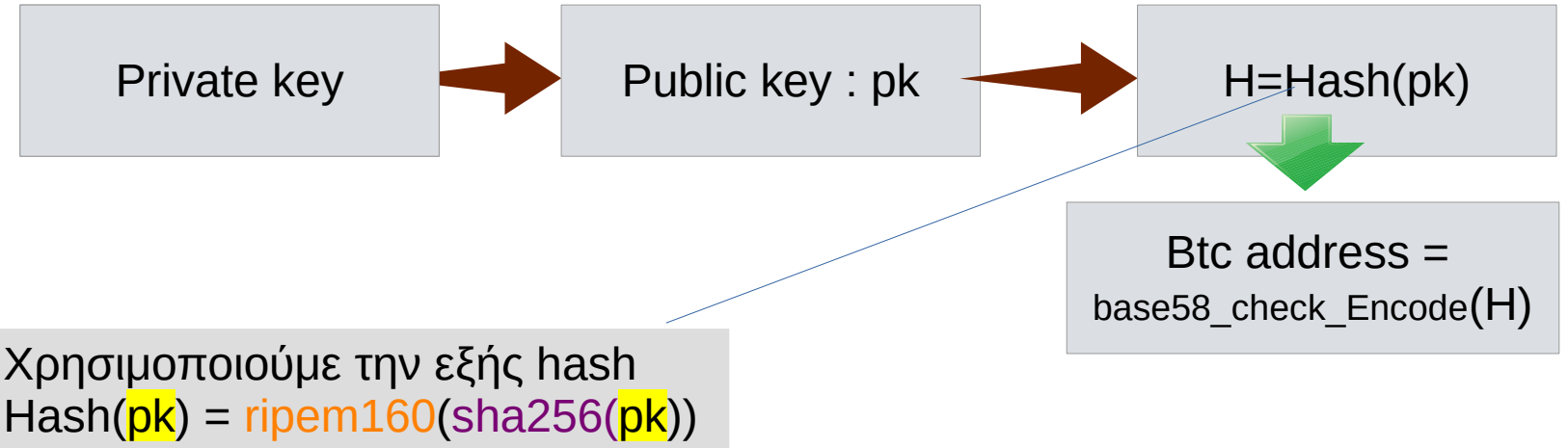
```
[~]:$ echo -n "welcome to OK! thes"|sha256sum
628e610dba76011b8c3b15a47330194f5df451e26c8e2a35686027580eff44c5  -
```

sha256 hash function

Basic properties of all hash functions
- Determenistic
- efficient

Some properties of cryptographic secure hash functions :
- avalance effect
- one way
- collision free

Bitcoin Addresses



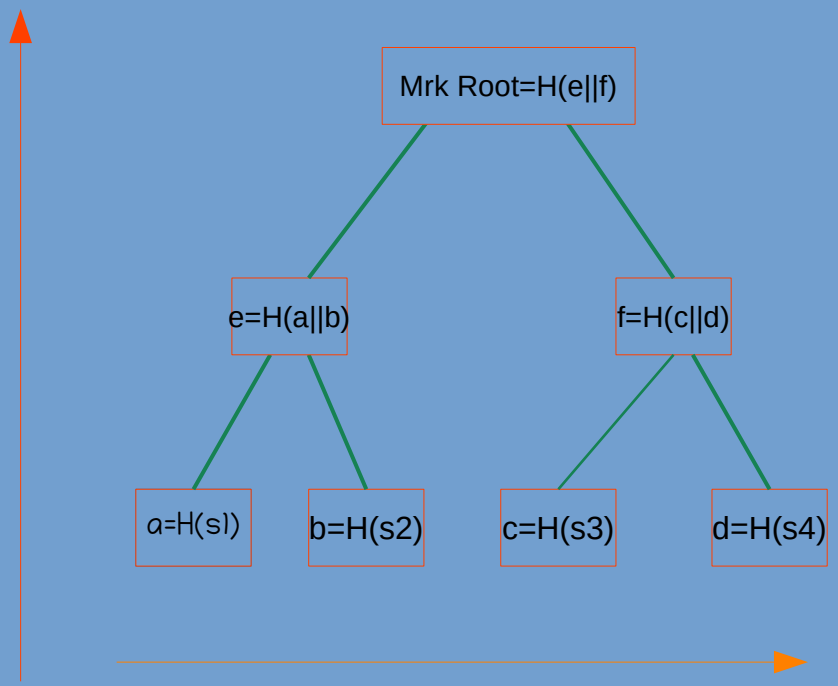
Χρησιμοποιούμε την εξής hash
Hash(pk) = ripem160(sha256(pk))

[1] Bitcoin addresses
[2] Base58check_encoding

How can someone send us btc?

- We have to provide a valid btc address, generated with the previous algorithm.
- Then, it is very easy someone to send us bitcoins using our address. In fact, this procedure is created from a wallet.

Merkle root



Allow us to make integrity check to a large number of transactions with a memory efficient way

Thank you!