Bitcoin fundamentals

Hakim Boulahya
Université Libre de Bruxelles
hboulahy@ulb.ac.be

October 21, 2017

Introduction

Bitcoin is a electronic cash system in which it is possible to exchange money, in form of coins, anonymously. The transaction are recorded using cryptographic methodologies such as digital signatures and public key encryption.

It is necessary to have a structure that will verify payements to avoid coins double-spending problem. The major advancement of the Bitcoin protocol is the decentralized transaction management structure, using a peer-to-peer architecture.

Digital signatures

To define a transaction, it is necessary first to define a digitial signature. A digitial signature is a mathematical scheme process that must ensure the following three propreties: (1) the **integrity** of the signed document, *i.e.* the document cannot be modified during its transit. (2) Ensure the **authenticity** *i.e.* verifying the owner. (3) It also provides the hability to prove the **non-repudiation** of a document *i.e.* ensure that all entities that signed the document accept and confirm the document content.

Public-key encryption

A mechanism that provide the digital signature propreties is the public-key encryption system **?**. It is composed of a encryption algorithm E, a decryption algorithm D and two keys, one public key k and one private key k'. The public-key is shared to everyone, and the private-key is kept secret by the owner.

A public encryption systems must have both algorithms easy to compute, when using the keys. That means the decryption (encryption) algorithm is a

trap-door one-way function **?**, it is difficult to compute except if a trap-door *i.e.* the private (public) key k' is known.

An encryption is using the algorithm E with parameter k to return a cihpertext C from a message M:

$$E_k(M) = C \tag{1}$$

A decryption is using the algorithm D with parameter k' to return a message M from a ciphertext C:

$$D_{k'}(C) = M \tag{2}$$

It is also possible to recover from a encrypted (decrypted) message M using the private (public) key and the corresponding algorithm, formally:

$$D_{k'}(E_k(M)) = M \tag{3}$$

$$E_k(D_{k'}(M)) = M \tag{4}$$

The equation (4) provide the signature mechanism. Since only the owner can provide an output using the decryption algorithm D and the private key k', everyone can verify the signature using the public key.

1 Hash

A hash function is an algorithm that will convert an arbitrary size message into a fixed size digest. The hash function used by bitcoin **?** (sure that bitcoin uses only sha25) is SHA-256: it produces a digest of size 256 bits. For a message m a function SHA-256 h will produce a digest d of size 256 bits, formally:

$$h(m) = d \tag{5}$$

? This is too simple and not correctly explained

2 Transaction and coins

A transaction is represented by a hash digest. An electronic coin is represented by a chain of digital signatures **??**. To perform a transaction, the process of transfering a coin from an owner to another one, an owner of a coin signs a hash digest. This digest is composed of the values: (1) the next owner public key and the hash of the previous transaction. Let's define a coin c_a, a coin owned by Alice. This coin is represented by a chain of transaction. The last transaction is represented by the hash digest t_i.

This is the method proposed to verify the ownership of a coin.

How it is represented (what does it contains) ?

How it is build (hash, signature) ?

How it is linked (blockchain) ?

Transacrtion are not encrypted !! ?

3 Double-spending problem

We know how to verify the ownership of a coin, but we cannot make sure that a owner doesn't spend the same coin twice, or more.

4 Address

An address is the how an owner is represented during a transaction. It is possible to reuse an address, but it is not recommanded because it will be possible to read all transaction made with this address, this a way that can be used to identify a bitcoin user.

Same question as for the transaction

5 Peer-to-peer and blockchain

6 Timestamp

7 Proof-of-work