Bitcoin fundamentals

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

October 22, 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:

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

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.

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 is SHA-256: it produces a digest of size 256 bits. The important proprety of cryptographic hashes is that the design is made such that the creation of a hash is efficient but hard to recover the original message. If h is the hash function x the message and y the hash we have:

$$h(x) = y \tag{5}$$

$h(x)$ is easy to compute but $h^{-1}(y)$ is hard.

Transaction and coins

A transaction is represented by a hash. An electronic coin is represented by a chain of digital signatures ?. If Alice, represented by the public private key pair $(a, a^{'})$, want to transfer a coin to Bob, represented by $(b, b^{'})$. Her coin is represented by the chain $\{t_0, t_1, .., t_n\}$, which is ordered and n is finite, where t_n is the last transaction made for this coin. Each transaction $t_i \forall i \leq n$ is a hash. To perform the transaction Alice must sign, using here private key $a^{'}$, a hash composed of the transaction t_n and Bob's public key b. This will add a new transaction t_{n+1} to the coin. We can verify using Alice's public key a that Bob's is the new owner of the coin. This is the method proposed to verify the ownership of a coin.

Block chain

A block is a file that contains multiple transactions, recorded permanently ?. A block contains also a block header, a 256 bits hash, used to the following block to create generate its own hash. The blockchain is a ledger of all recorded blocks. The miners, the computers that do the (proof-of-)work to approve the transactions, add a new blocks in the blockchain in a chronological order. Those new block records, once added to the Bitcoin blockchain, can never be removed or modified.

Double-spending

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. To be able to find a solution to this problem, we need a *central* authority to acknowledge each transaction. Bitcoin uses a peer-to-peer network, a distributed application meaning that the data are not stored in a central server but in multiple computers that form the p2p network, and a proof-of-work system called hashcash ?. Using a p2p network provides a decentralized authority to approve the transactions and the proof-of-work provides a system that makes it hard to rebuild a block therefor hard to modify an approved transaction.

Proof-of-work

Each blocks is minted using the hashcash cost-fuction algorithm. A cost-function should be easy to verify but hard to compute, and the computation difficulty is parameterisable ?.

Let b_n the hash of the last block in the blockchain. We want to create a new block b_{n+1}. Bitcoins uses hashcash as follow: each block hash requires a number of 0 bits at the beginning. To build this hash, concatenated the previous block hash and a nonce, a 32 bits numbers that is incremented. This concatenation is hashed using hashcash-SHA-256 and the result must be a new 256 bits hash starting with the required number of 0. This new hash must be lower than the previous block hash: $b_{n+1} < b_n$.

1 Address

Address is the public private key. Bad reuse because no anonymousity.

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