INFO-F-405 - Homework
Fundamentals of Bitcoin

Université Libre de Bruxelles

Hakim Boulahya

October 23, 2017

Introduction

Bitcoin is a electronic cash system in which it is possible to exchange money, in form of coins. The transaction are recorded using cryptographic methods to provide a system that can ensure the privacy of the clients.

It is necessary to have a structure that will verify payements to avoid coins double-spending problem. Satoshi Nakamoto introduces in his paper[3], released in 2008, the Bitcoin protocol with an implementation of a decentralized transaction management structure, using peer-to-peer architecture and the hashcash[1] proof-of-work system.

In this paper we will define the cryptographic methods that are necessary to understand the technical mechanism of the Bitcoin system such as digital signatures, public key encryption and hash algorithms. We will also define the representation of a transaction and explain the solution proposed by Nakamoto[3] to the double-spending problem.

1 Cryptographic methods

Before describing the Bitcoin system, it is necessary to provide definitions and explain cryptographic mechanisms used by Bitcoin.

1.1 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.

1.2 Public key encryption

A mechanism that provide the digital signature propreties is the public key encryption system[4]. It is composed of an 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. It is possible to calculate the public key from the private key, but the opposite is not possible.

A public encryption system must have both algorithms easy to compute, when using the keys. That means the decryption (encryption) algorithm is a trap-door one-way function[2], 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 ciphertext 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 an encrypted (decrypted) message M using the private (public) key with the corresponding algorithm, formally:

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

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

The formula (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.

1.3 Hash

A hash function is an algorithm that will convert an arbitrary size message into a fixed size string. The result string is sometimes called a hash digest or hash. 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 it is 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.

2 Bitcoin protocol

2.1 Address

The privacy of the transfers is ensured by the Bitcoin addresses. An address is a 160 bits hash. Each address is generated using a pair of ECDSA[6] public/private key that identify an owner during a transaction. The transaction ledger is public, so it's not encouraged to

reuse an address, because it will be possible to link the transactions made by an address and build a profile of the owner of this address to identify him.

2.2 Transaction and coins

A transaction is represented by a hash. An electronic coin is represented by a chain of digital signatures[3]. Let Alice be represented by the public private key pair (a, a') and Bob be represented by (b, b'). Alice want to send a coin to Bob. 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 her private key a', a hash composed of the transaction details and Bob's public key b. This will add a new transaction hash t_{n+1}, to the coin, signed by Alice. We can verify using Alice's public key a that Bob is the new owner of the coin. This is the method proposed to verify the ownership of a coin.

2.3 Block chain

A block is a file that contains multiple transactions, recorded permanently[5]. A block contains also a block header, a 256 bits hash, used by the following block to generate its own hash. The blockchain is a ledger of all recorded blocks. The miners, the computers that do the proof-of-work (section 2.5) 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.

2.4 Double-spending

We know how to verify the ownership of a coin, but we cannot make sure that an 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. This authority timestamp all transactions and knows every transaction that are recorded in the blockchain.

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[1]. 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 therefore hard to modify an approved transaction.

Actually, it is important to note that the p2p network doesn't provide the privacy, or the anonymity. The blockchain is accessible to the public therefore all transactions are visible.

2.5 Proof-of-work

Each blocks is minted using the cost-fuction of the hashcash algorithm. A cost-function should be easy to verify but hard to compute, and the computation difficulty is parameterisable[1].

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

Conclusion

References

[1] Adam Back. *Hashcash - A Denial of Service Counter-Measure.* 2002.

[2] Whitfield Diffie and Martin E. Hellman. *New Directions in Cryptography.* 1976.

[3] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008.

[4] R. L. Rivest, A. Shamir, and L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* 1978.

[5] Bitcoin Wiki. *https://en.bitcoin.it/wiki/block*, 2017.

[6] Bitcoin Wiki. *https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm*, 2017.