**The Block Chain**

**Digital Signature**

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages. A valid digital signature regroups 3 principles: **authentication, non-repudiation and integrity**. The digital signatures are the standard elements of most cryptographic protocol and employ asymmetric cryptography. Example: RSA, DSA.

**1.Definition**

A digital signature consists of 3 algorithms: **A key generation** (selects a private key uniformly at random from a set of possible keys – the output is a private key and a corresponding public key); **a signing** (given a message and a private key produces a signature); and **a signature verifying** (given the message, the public key and the signature, accepts or reject the authenticity of the message).

**Two properties are required**: The authenticity of a signature generated from a message and a private key can be verified by using the public key corresponding; it should be infeasible to generate a valid signature without knowing the private key.

**2.Attacks**

1.**Key-only attack**: The attacker only has the public verification key.

2.**Known message attack**: The attacker has valid signatures from some messages not chosen by himself.

3.**An adaptive chosen message attack**: The attacker learns signatures on arbitrary messages.

1.**A total break results**: Results in recovery of the signing key.

2.**A universal forgery**: Results in ability to forge signature for any message.

3.**A selective forgery**: Results in a signature on a message of the adversary’s choice.

4.**An existential forgery**: Results in some valid message/signature pair not known to the adversary.

**3.Application of digital signatures**

**Authentication**: Digital signature can be used to authenticate the source of messages.

**Integrity:** It may be possible to change a message from the sender to the receiver. Still, it is considered to be computationally infeasible by most cryptographic hash functions to find an efficient way to modify a message and its signature to produce new message with a valid signature. Digitally signed, if any change occurs to the message after the signature, it becomes invalid.

**Non-repudiation**: After a signature, the sender can’t deny having signed it later.

**4.Additional security precautions**

1.Putting the private key on a smart card.

2.Using smart cards reader with a separate keyboard.

3.Only using digital signatures with trusted applications.

4.Using a network attached hardware security module.

5.What You See Is What You Sign (WYSIWYS)

**5.Basis prerequisites for digital signatures**

1.Quality algorithms.

2.Quality implementations.

3.Users’s software must carry the signature protocol properly.

4.The private key must remain private.

5.The public key must be verifiable.