BLOCKCHAIN

EXPLAINER

Cryptography 101

#CRYPTOGRAPHY
#SECURITY
#PUBLICKEY

Cryptography is a method of securing data and communications in the presence of third parties in order to protect it, either during communication, or while it is stored.

Overview

General Practice

Plaintext (unencrypted data) is encrypted using a cipher (mathematical algorithm used to encrypt and decrypt data securely). This produces cipher-text (unreadable encrypted data).

Types

Symmetric-Key Cryptography: The same key is used to both encrypt and decrypt the data.

- **Most used symmetric-key cipher:** Advanced Encryption Standard (AES), which the NSA has approved for use in the encryption of classified information.
- **Pros:** Symmetric crypto is generally believed to be more highly quantum resistant than asymmetric (Public-Key). It's also stronger because it enables (but doesn't require) the user to use a key that is at the same length as the plaintext (rather than using prime factorization), meaning that it is nearly uncrackable.
- **Cons:** Difficult to use for the type of communication needed for blockchain. Two parties cannot share their encryption key securely, and giving away the key to another user compromises the security of what that key protects.

Public-Key Cryptography: Uses separate keys for encryption and decryption. A user generates a pair of keys that are mathematically linked. One key is public and used for encryption, while the other key is private and used for decryption.

- **Goal:** Public-key cryptography ensures that communications being sent are kept confidential during transit. The algorithm linking the keys is designed so that it will be infeasible for an attacker to derive the private key from the given public key.
- **Use:** Using this method, anyone can download a person's shared public key and use it to encrypt messages to send back to him. Once encrypted, this message can only be decrypted with the linked private key.
- **Process:**
  - A mathematically-linked public and private key is created
  - The public key is shared while the private key is kept secret
  - A message (data/transaction) is encrypted with the public key
  - The message is sent to the recipient electronically where it can be decrypted with the private key

Digital Signature

Goal

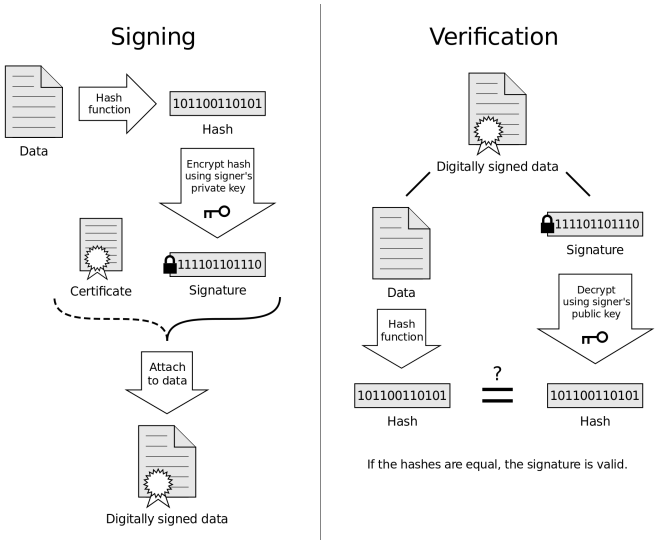
Provides authentication, data integrity, and non-repudiation.

What is it?

Digital signatures are **based on public-key cryptography.**

A digital signature is created by combining the user's private key with the data he wishes to sign into a mathematical algorithm (encrypted hash).

This algorithm is unique to the data, and any change in the data will result in a different value. This allows others to validate the integrity of the data by using the signer's public key to decrypt the algorithm. If it matches, it authenticates the digital signature. If the public key does not match, the data has either been tampered with or the signature was created with a non-corresponding private key.



Sources: https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/
https://www.cryptomathic.com/news-events/blog/how-digital-signatures-and-blockchains-can-work-together