BLOCKCHAIN TUTORIAL 6

Digital signature

BLOCKCHAIN TUTORIAL 6

Digital signature

DIGITAL SIGNATURE

- A digital signature is equivalent of a handwritten signature but it is much more secure, a handwritten signature can be faked

- A digital signature provides the recipient the following information:

    - the message was created by a known sender (**authentication**),

    - the sender cannot deny having sent the message (**non-repudiation**),

    - the message was not altered in transit (**integrity**)

DIGITAL SIGNATURE

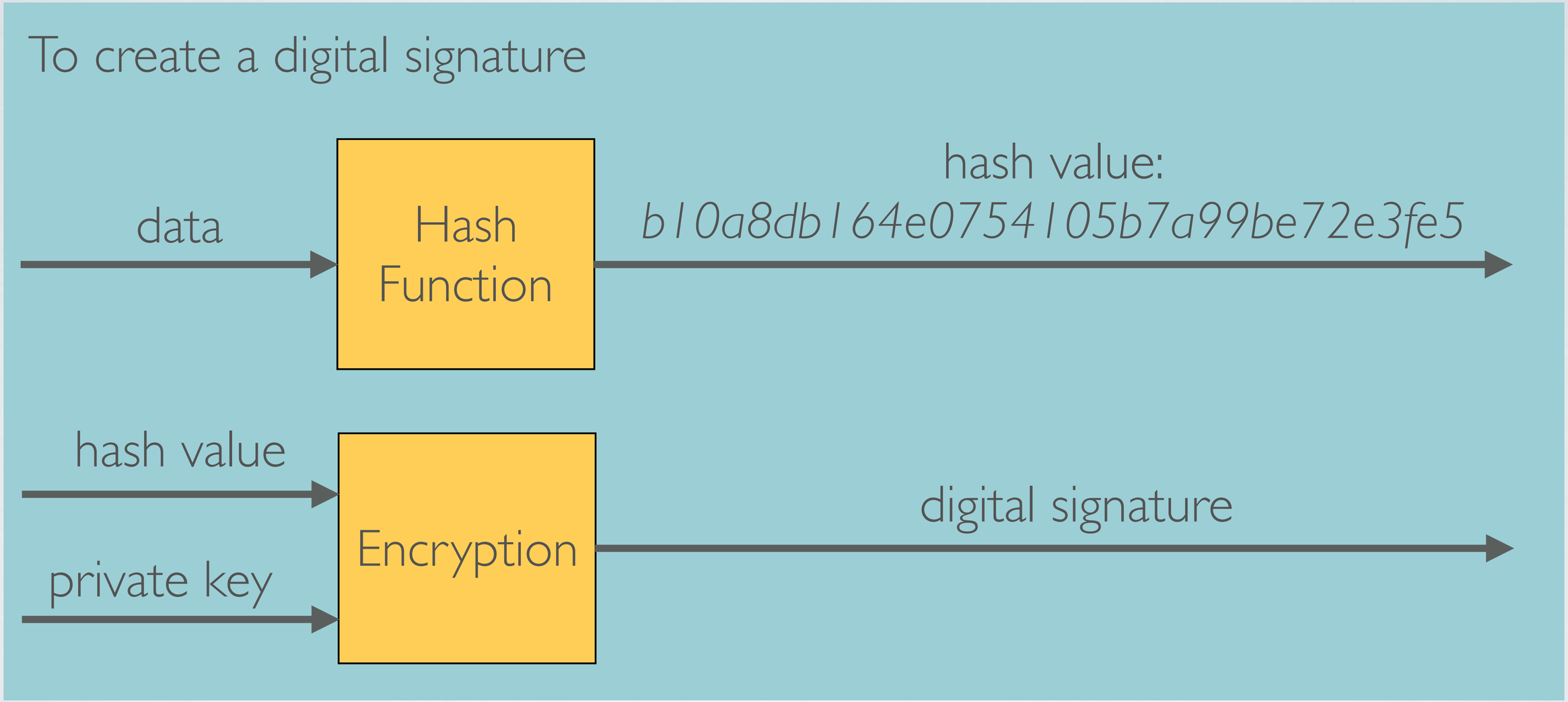
How the digital signature is created and verified:

- Alice has a document and wants to create a digital signature proofing to anyone that she is the owner of the document.
- Alice creates a digital signature:
    - First she hash the data (document, piece of text, movie file, audio file, etc)
    - Next she uses her private key to encrypt the hash.
    - The encrypted hash is called the digital signature.

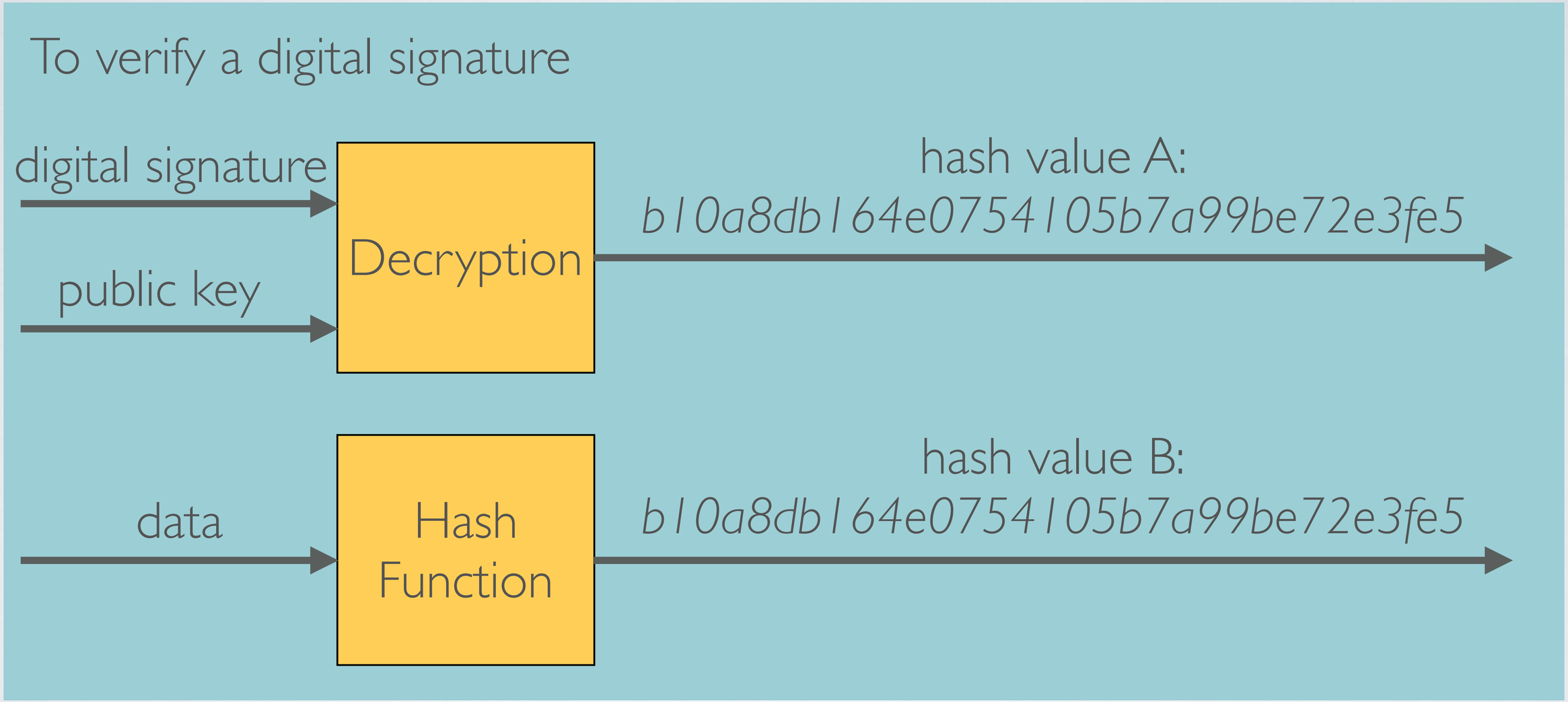
DIGITAL SIGNATURE

- Bob wants Alice document. Alice sends the document and the digital signature.
- Bob verifies the digital signature:
  - Bob decrypts the digital signature using Alice public key.
    The result is the hash value of the document (hash A)
  - Bob applies the same hash algorithm on the received document.
    The result is the hash value of the received document (hash B)
  - Bob compares both hash values (hash A, hash B)
  - If the hash values match it proofs that the document was not altered during transit and that the document is owned by Alice.

DIGITAL SIGNATURE



DIGITAL SIGNATURE



DIGITAL SIGNATURE

Alice creating a digital signature:

ENC(H(p), priv key_{alice}) = sign

Bob verifying a digital signature:

DEC(sign, pub key_{alice}) = hash val

H(p) = hash val