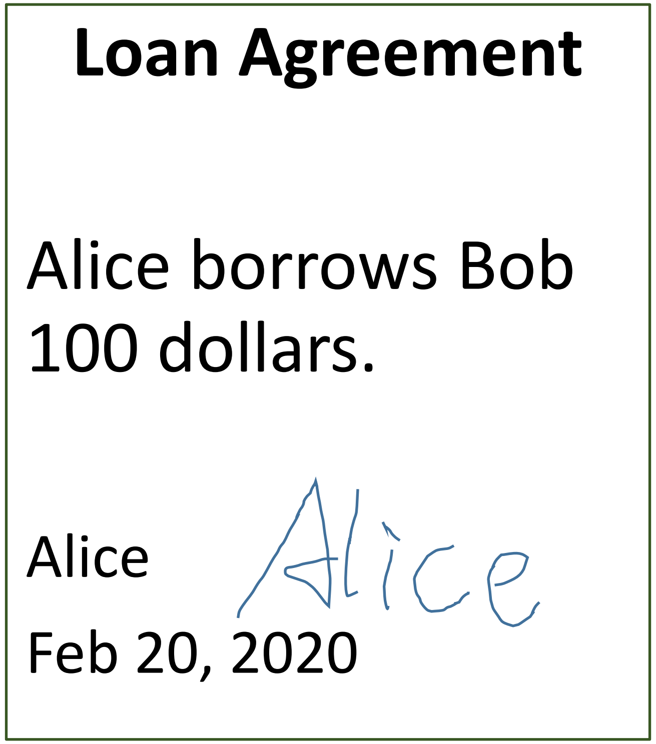
Digital Signature

Shusen Wang

Is this digital agreement safe?



Loan Agreement

Alice borrows Bob 100 dollars.

Alice Alice

Feb 20, 2020

Is this digital agreement safe?

Loan Agreement

Alice borrows Bob 100 dollars.

Alice Alice

Feb 20, 2020

Forged document

Loan Agreement

Alice borrows Bob 10000 dollars.

Alice

Feb 20, 2020

Is this digital agreement safe?

Loan Agreement

Alice borrows Bob 100 dollars.

Alice Alice

Feb 20, 2020

Copy the signature

Forged document

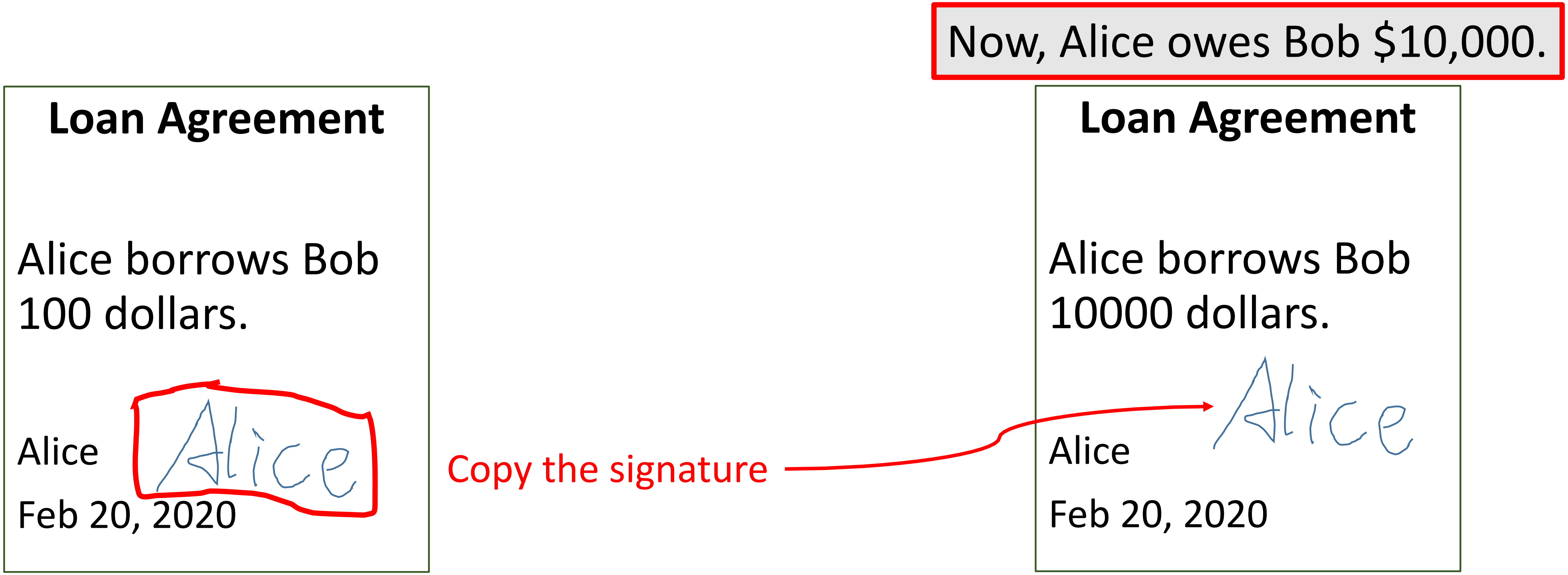
Loan Agreement

Alice borrows Bob 10000 dollars.

Alice

Feb 20, 2020

Is this digital agreement safe?



Loan Agreement

Alice borrows Bob 100 dollars.

Alice Alice

Feb 20, 2020

Copy the signature

Now, Alice owes Bob $10,000.

Loan Agreement

Alice borrows Bob 10000 dollars.

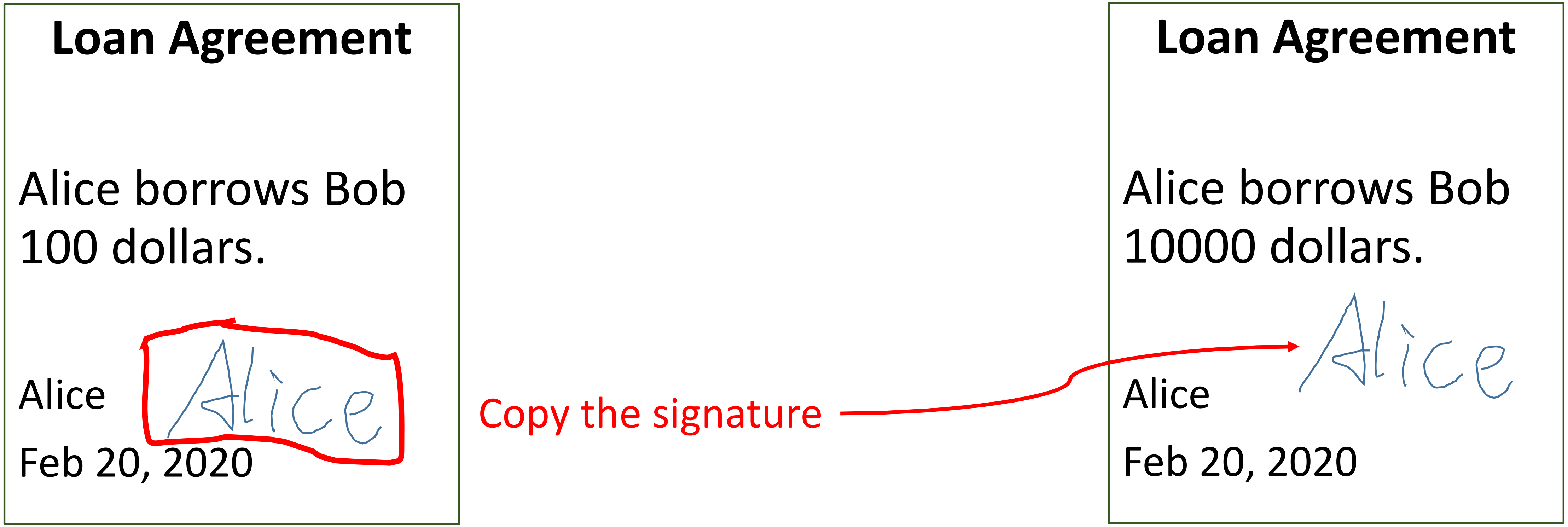
Alice Alice

Feb 20, 2020

Is this digital agreement safe?

Question: How to protect the integrity of document?

Now, Alice owes Bob $10,000.



Loan Agreement

Alice borrows Bob 100 dollars.

Alice Alice

Feb 20, 2020

Copy the signature

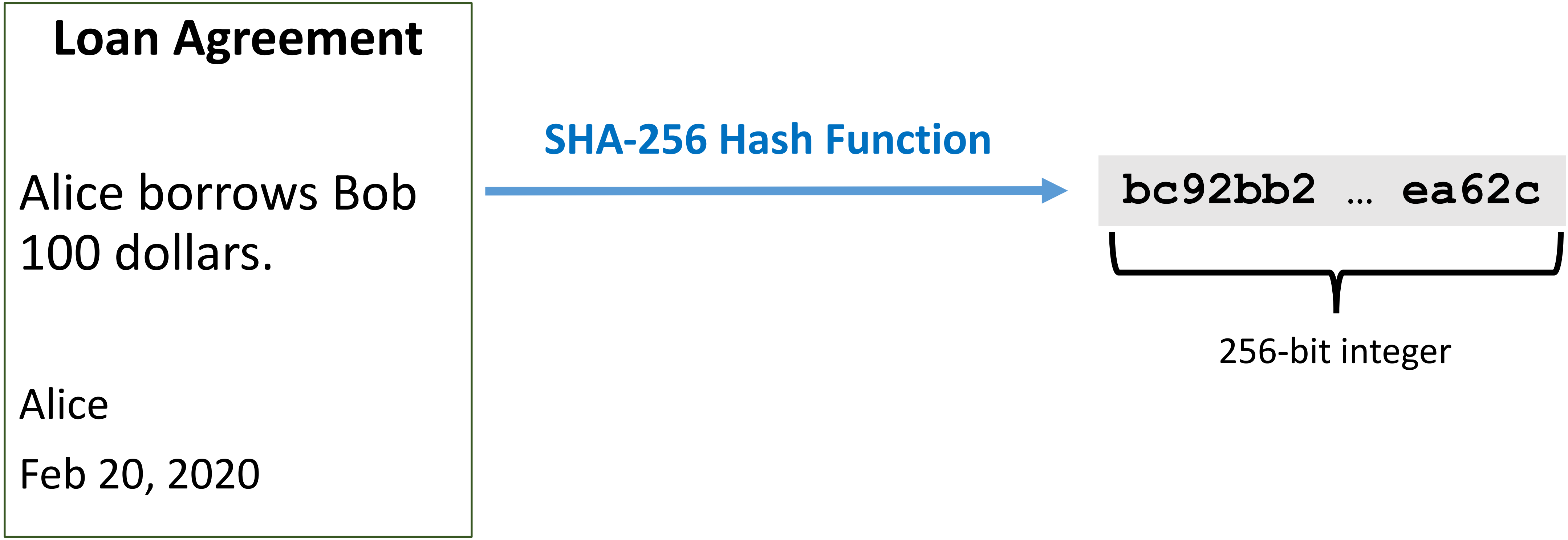
Loan Agreement

Alice borrows Bob 10000 dollars.

Alice Alice

Feb 20, 2020

Hashing as checksum



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

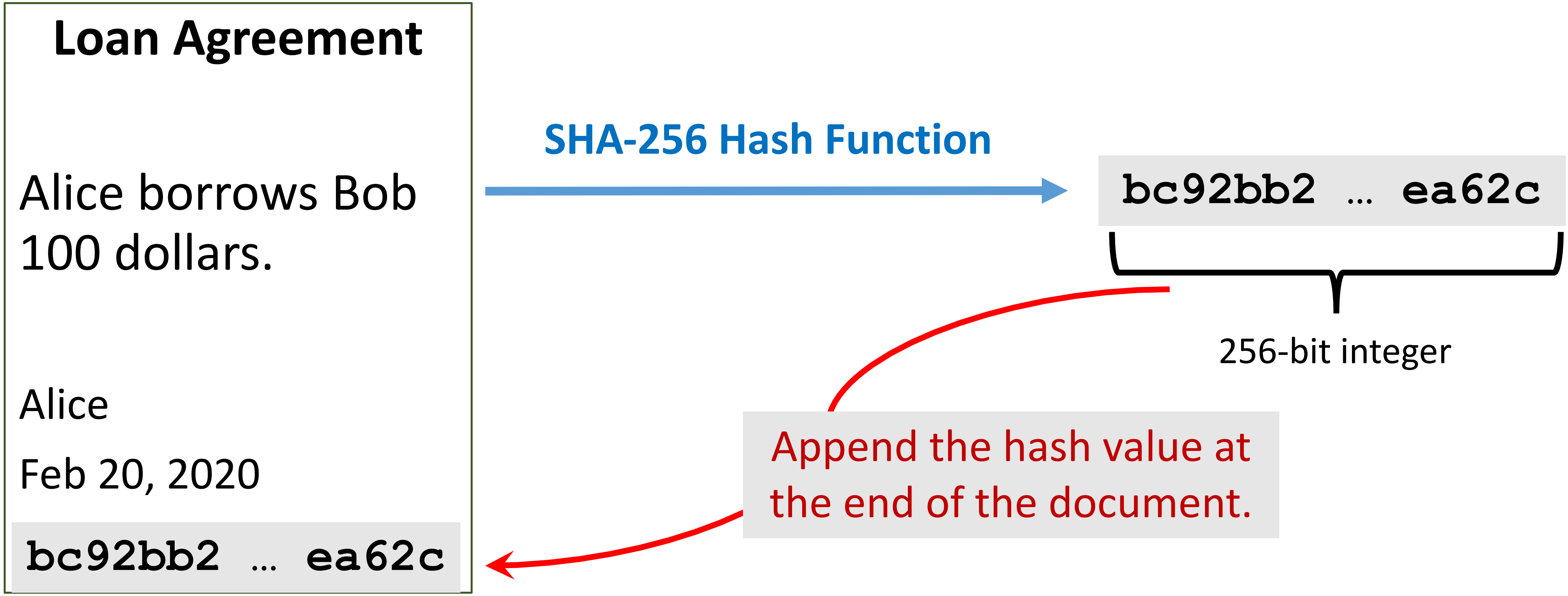
Feb 20, 2020

SHA-256 Hash Function

`bc92bb2 … ea62c`

256-bit integer

Hashing as checksum



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

`bc92bb2 … ea62c`

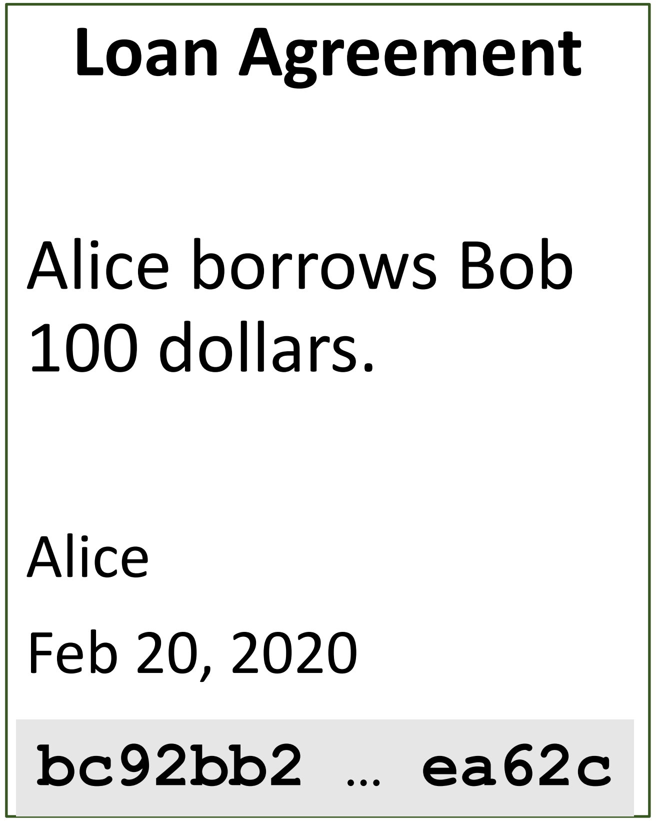
SHA-256 Hash Function

`bc92bb2 … ea62c`

256-bit integer

Append the hash value at the end of the document.

Hashing as checksum



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

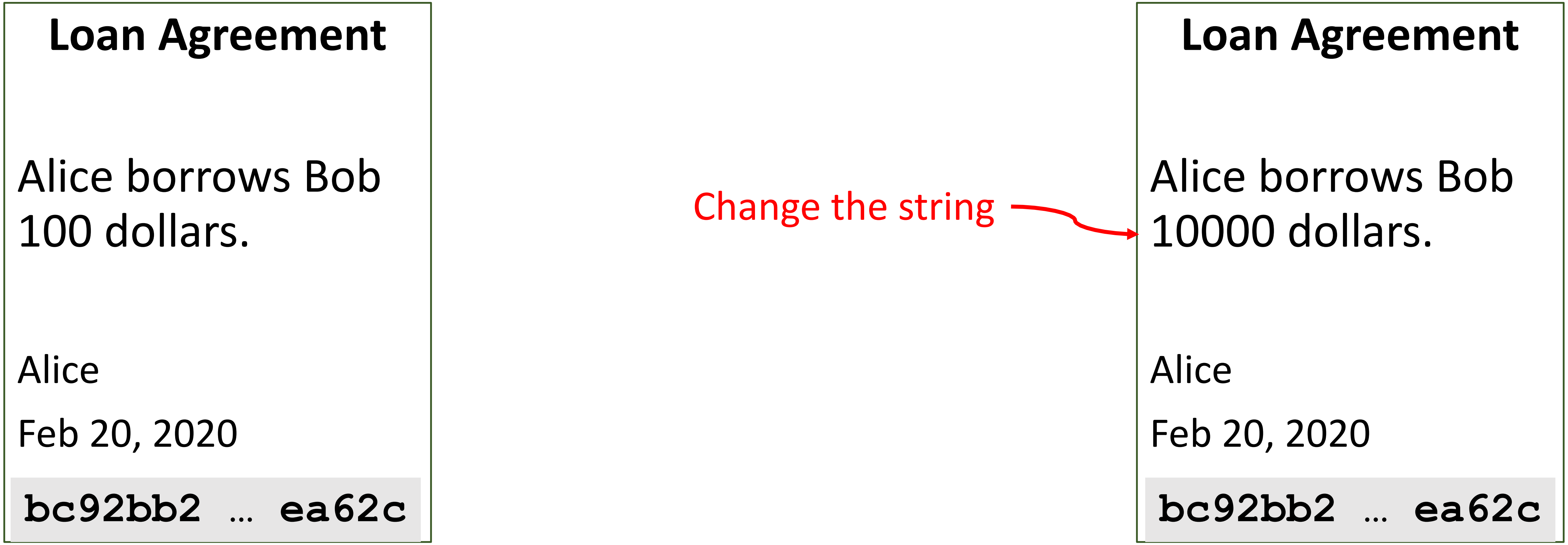
Feb 20, 2020

`bc92bb2 … ea62c`

- If anything in the document is changed, then the hash values will not match.

- **Question:** Can Bob forge a loan agreement?

Hashing as checksum



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

`bc92bb2 … ea62c`

Change the string

Loan Agreement

Alice borrows Bob 10000 dollars.

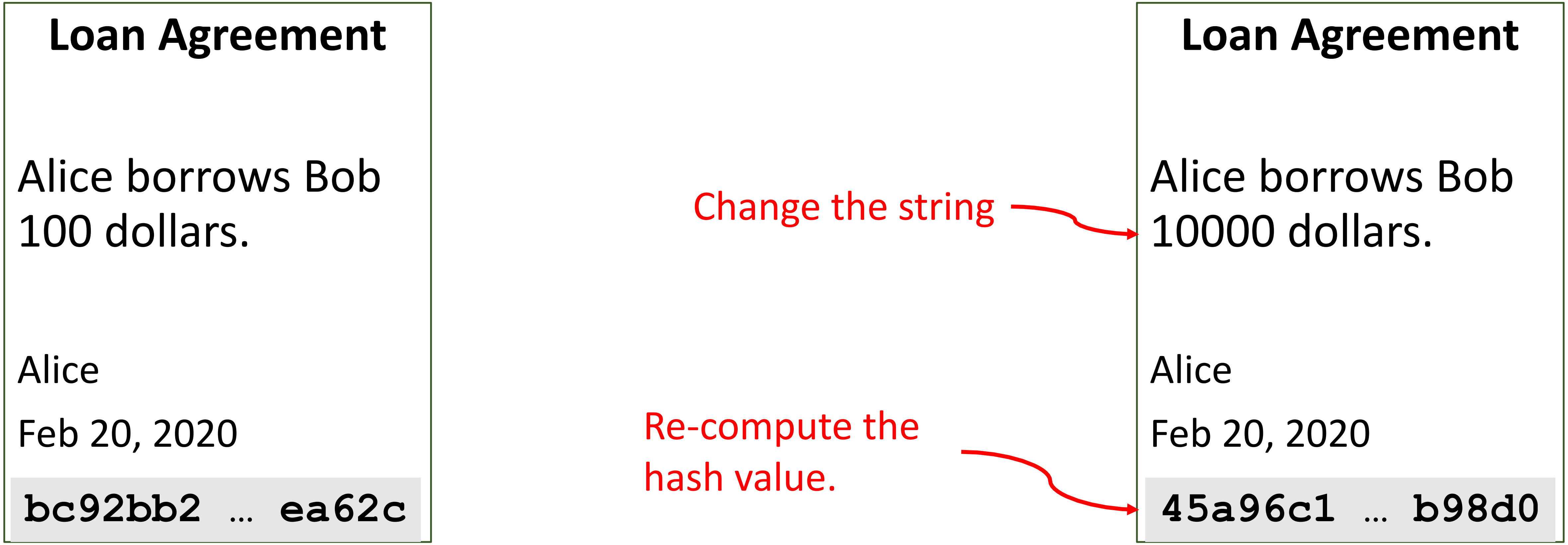
Alice

Feb 20, 2020

`bc92bb2 … ea62c`

Hashing as checksum

Hashing itself is not enough!



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

`bc92bb2 … ea62c`

Change the string

Re-compute the hash value.

Loan Agreement

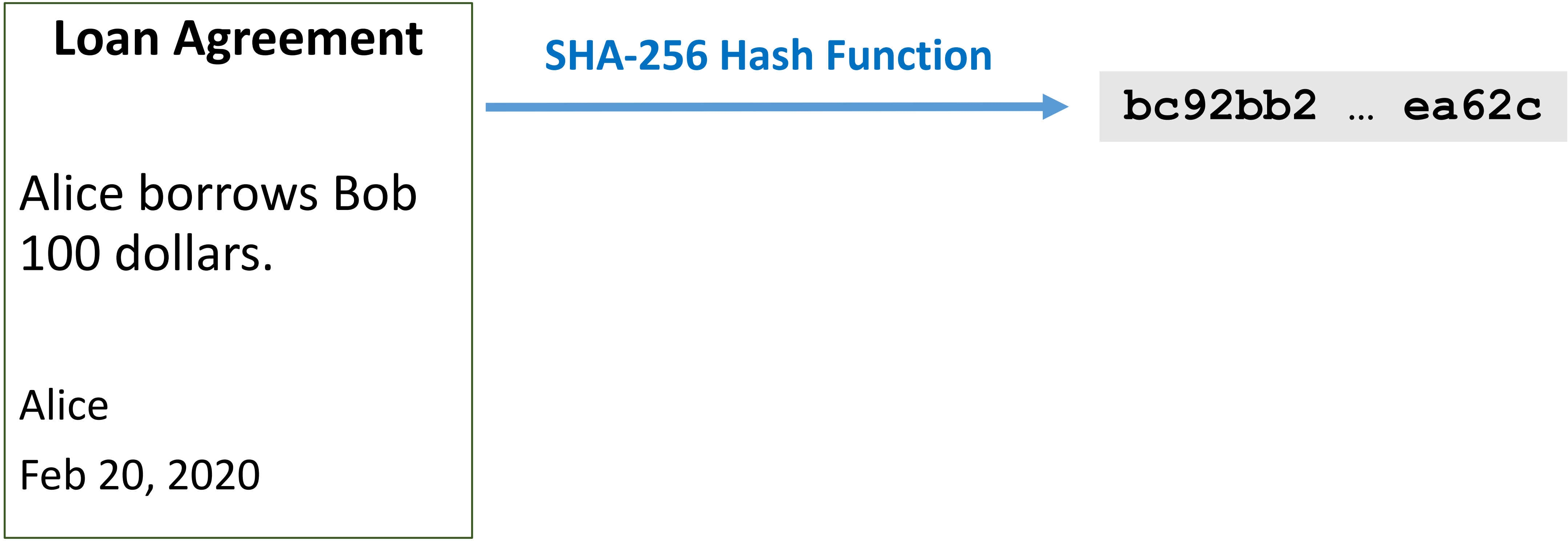
Alice borrows Bob 10000 dollars.

Alice

Feb 20, 2020

`45a96c1 … b98d0`

Digital Signature: Hashing + Encryption



Loan Agreement

Alice borrows Bob 100 dollars.

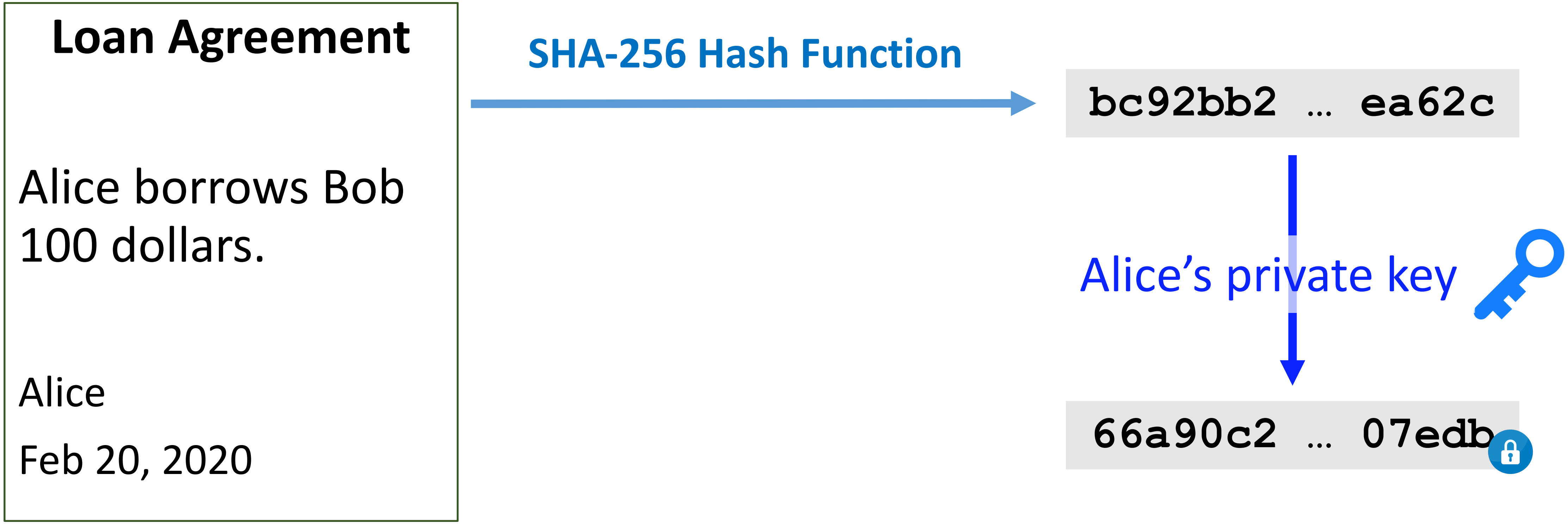
Alice

Feb 20, 2020

SHA-256 Hash Function

`bc92bb2 … ea62c`

Digital Signature: Hashing + Encryption



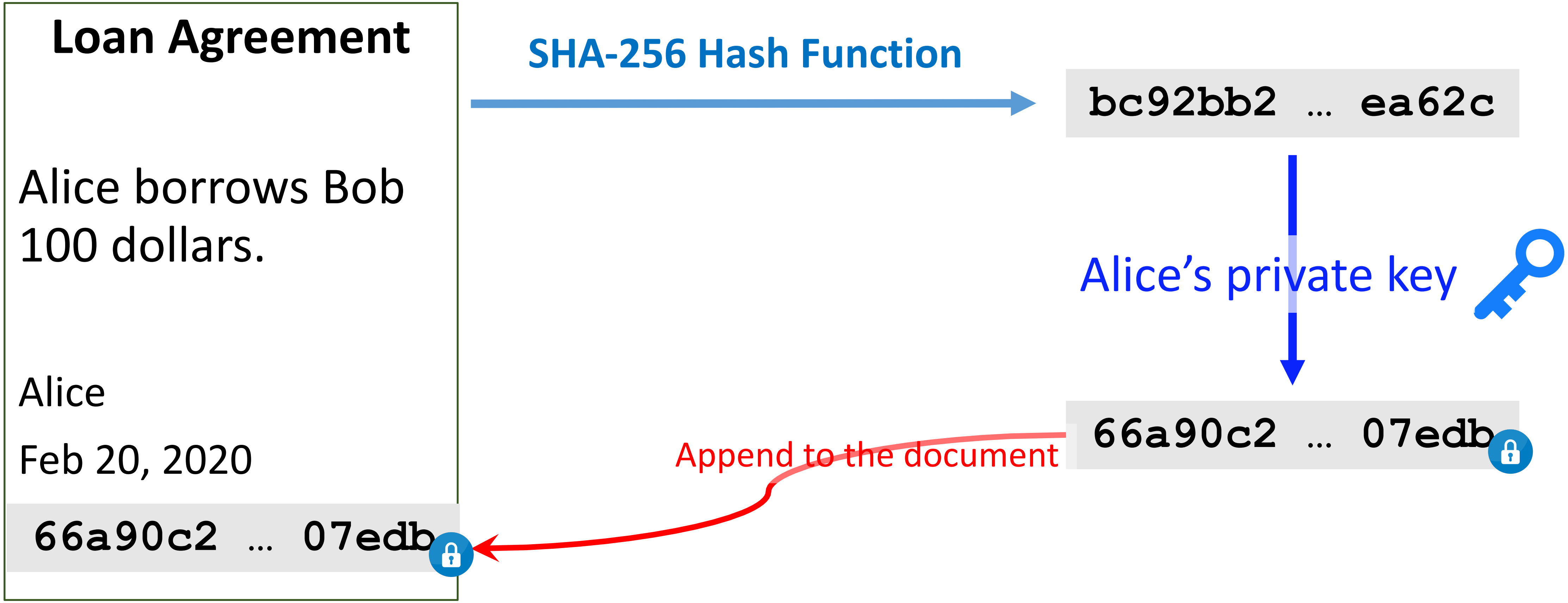
Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

Digital Signature: Hashing + Encryption



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

66a90c2 … 07edb

SHA-256 Hash Function

bc92bb2 … ea62c

Alice’s private key

66a90c2 … 07edb

Append to the document

Digital Signature: Hashing + Encryption

Loan Agreement

Alice borrows Bob 100 dollars.

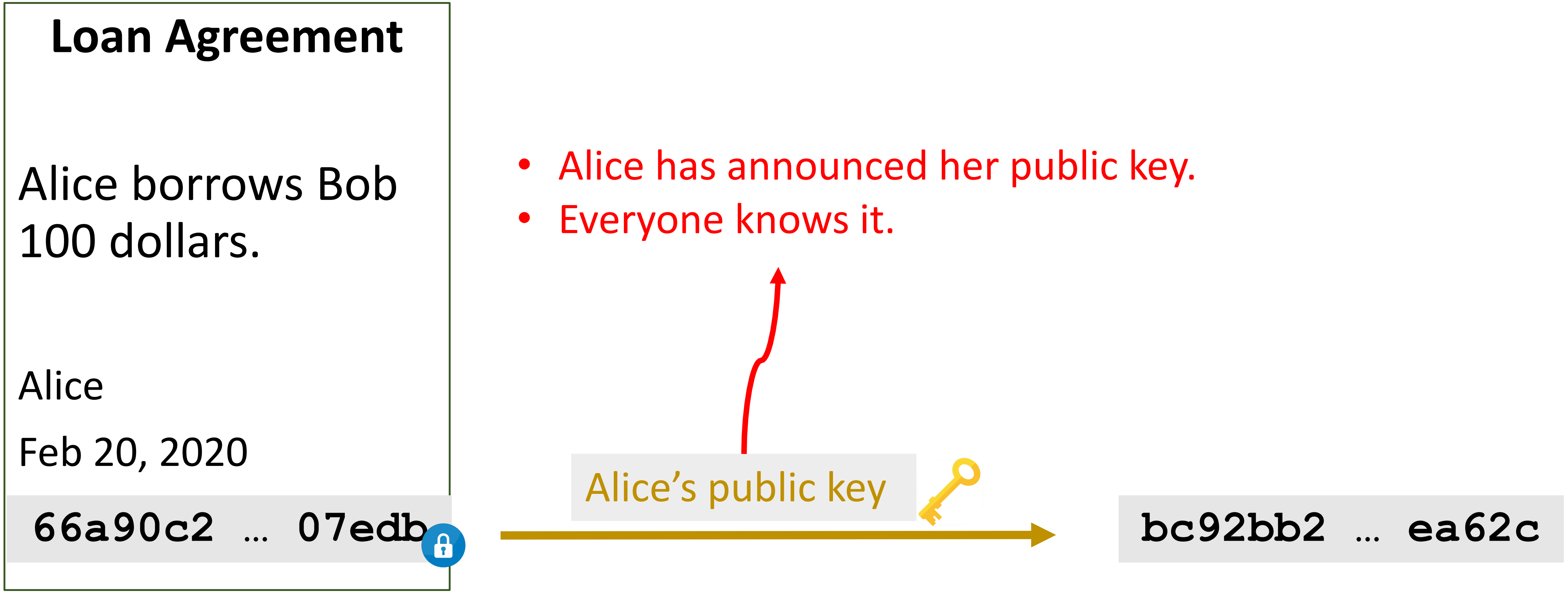
Alice

Feb 20, 2020

`66a90c2 … 07edb`

This is called digital signature.

Verity the authenticity



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

`66a90c2 … 07edb`

- Alice has announced her public key.
- Everyone knows it.

Alice’s public key

`bc92bb2 … ea62c`

Verity the authenticity

Loan Agreement

Alice borrows Bob 100 dollars.

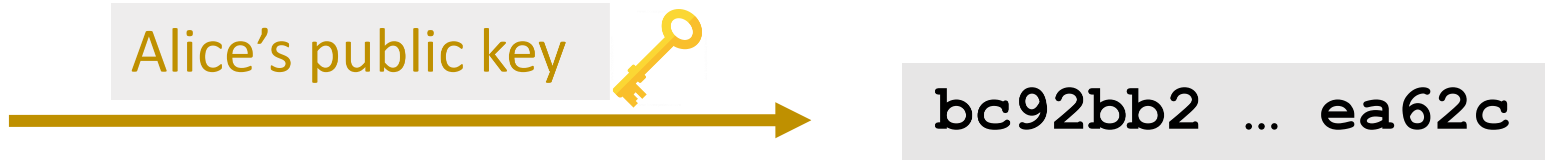
Alice

Feb 20, 2020

`66a90c2 … 07edb`

Properties of RSA algorithm

- $D\big(E(\text{messge})\big) = \text{message}.$



Verity the authenticity

Loan Agreement

Alice borrows Bob 100 dollars.

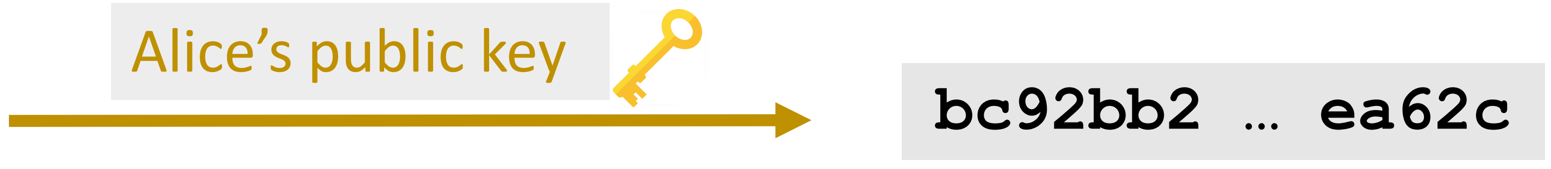
Alice

Feb 20, 2020

`66a90c2 … 07edb`

Properties of RSA algorithm

- $D\left(E(\text{messge})\right) = \text{message}.$
- $E\left(D(\text{messge})\right) = \text{message}.$

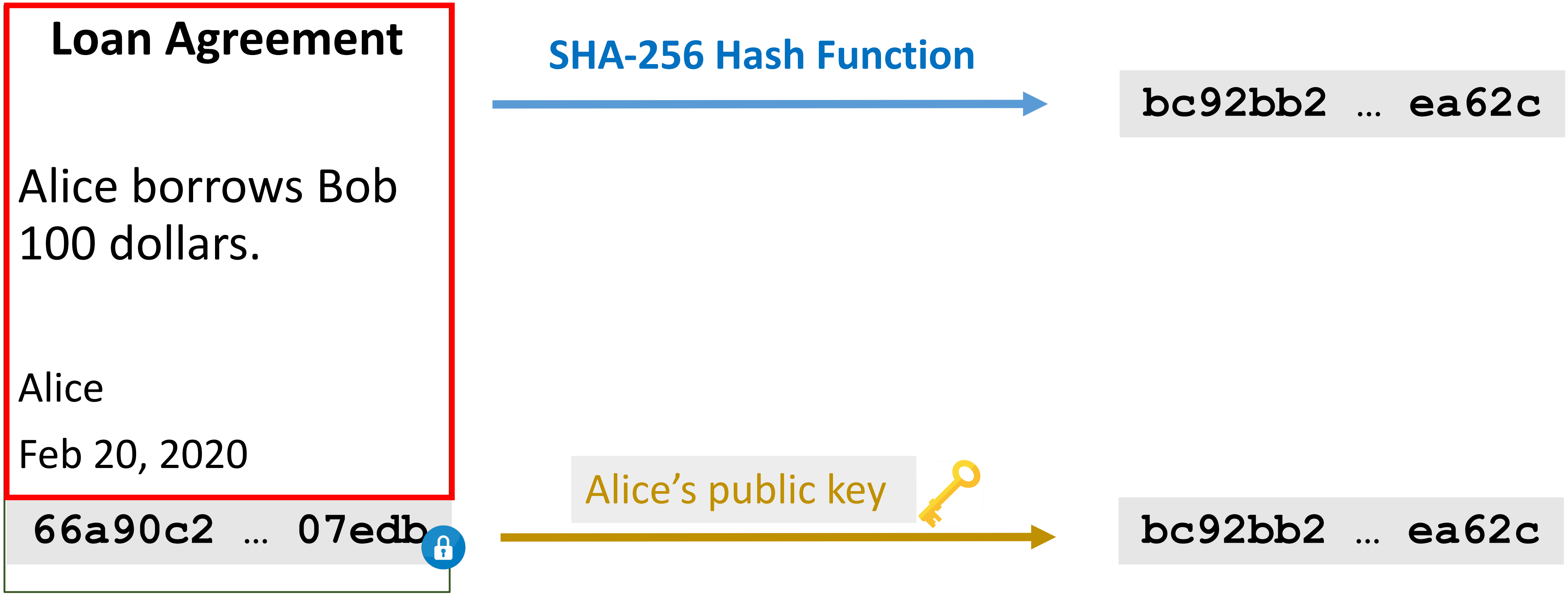


Alice's public key

`bc92bb2 … ea62c`

The original hash value

Verity the authenticity



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

66a90c2 … 07edb

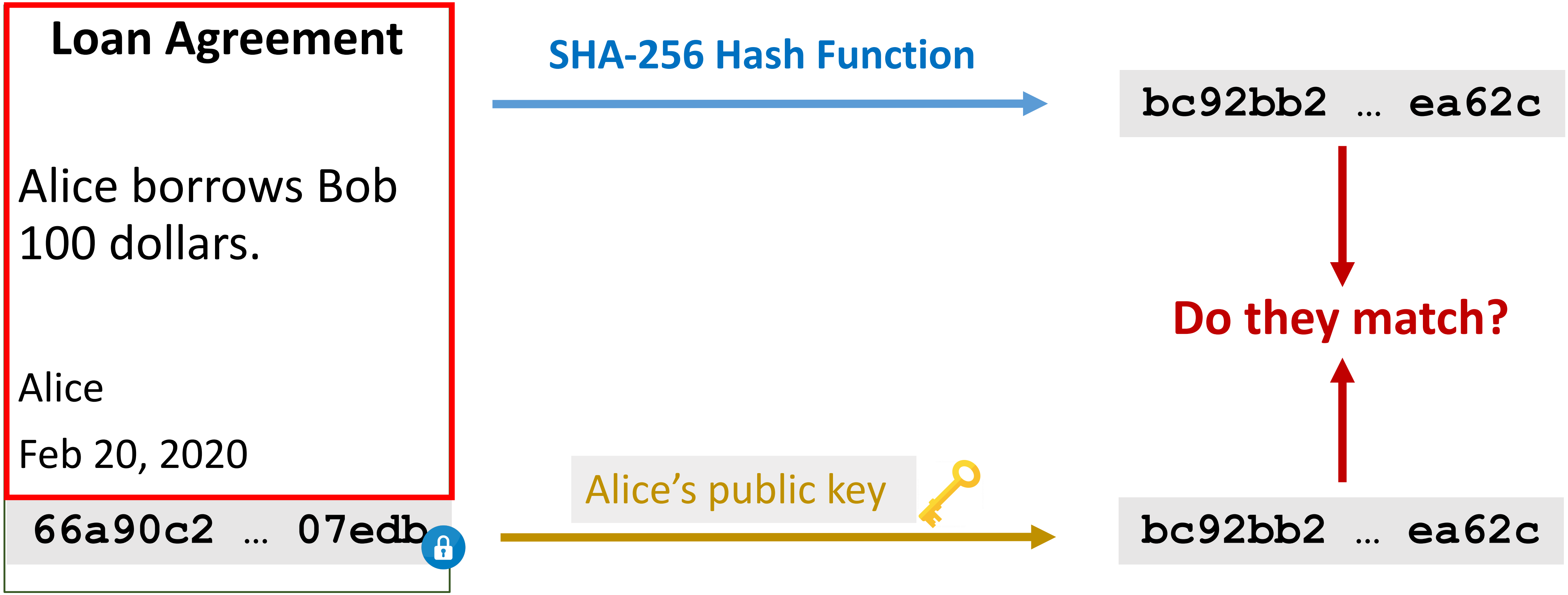
SHA-256 Hash Function

bc92bb2 … ea62c

Alice’s public key

bc92bb2 … ea62c

Verity the authenticity



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

66a90c2 … 07edb

SHA-256 Hash Function

bc92bb2 … ea62c

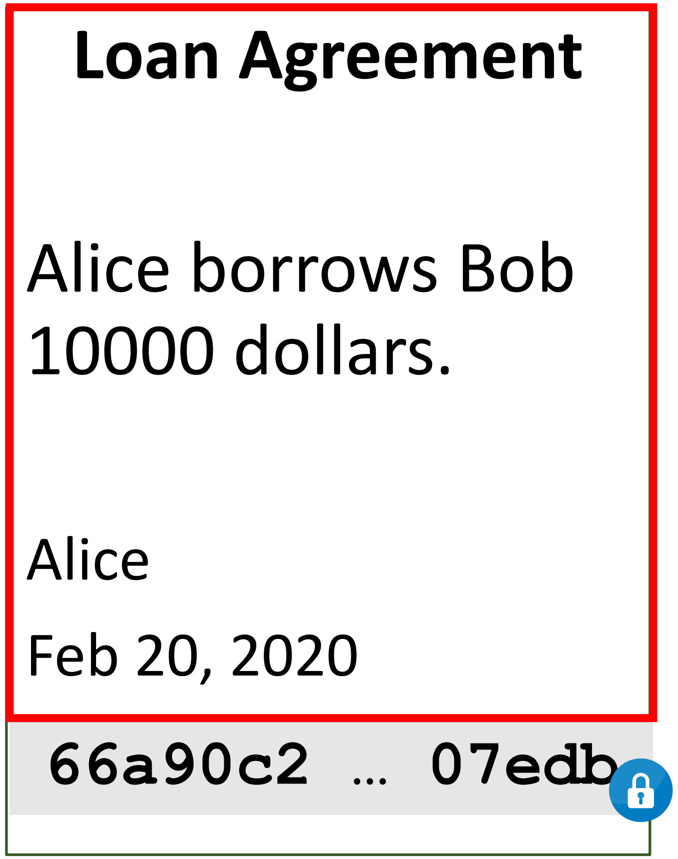
Do they match?

Alice’s public key

bc92bb2 … ea62c

Verity the authenticity

Forged document



Loan Agreement

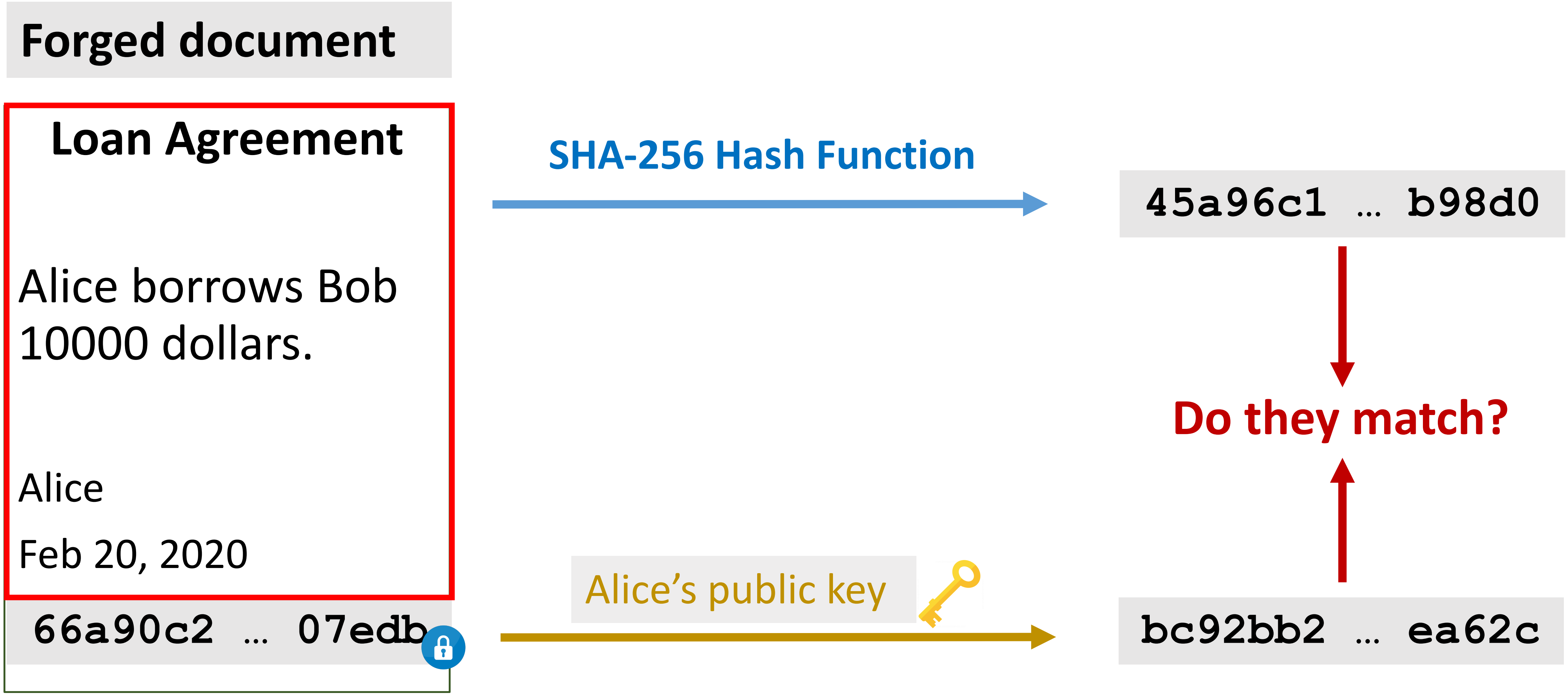
Alice borrows Bob 10000 dollars.

Alice

Feb 20, 2020

`66a90c2 … 07edb`

Verity the authenticity



Forged document

Loan Agreement

Alice borrows Bob 10000 dollars.

Alice

Feb 20, 2020

66a90c2 … 07edb

SHA-256 Hash Function

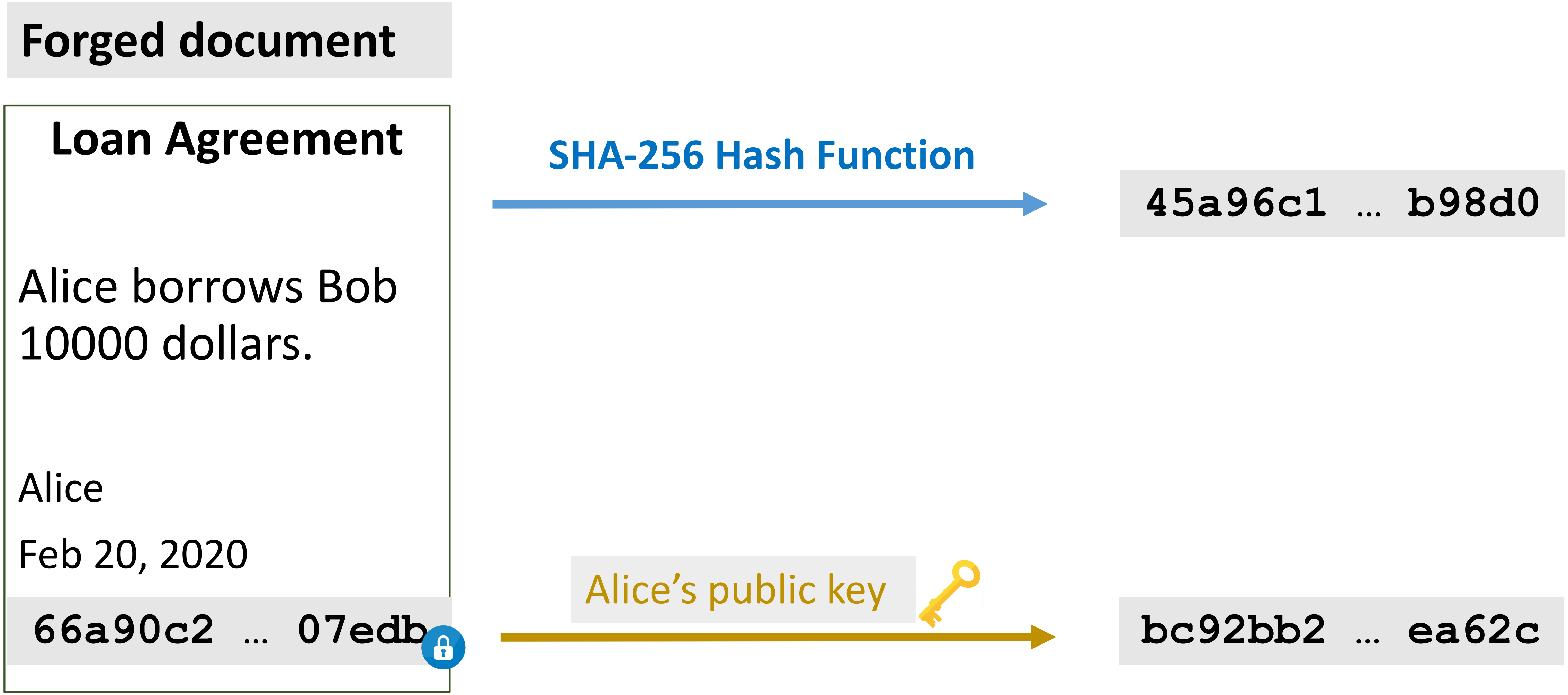
45a96c1 … b98d0

Do they match?

Alice's public key

bc92bb2 … ea62c

How to forge a document that looks authentic?



Forged document

Loan Agreement

Alice borrows Bob 10000 dollars.

Alice

Feb 20, 2020

66a90c2 … 07edb

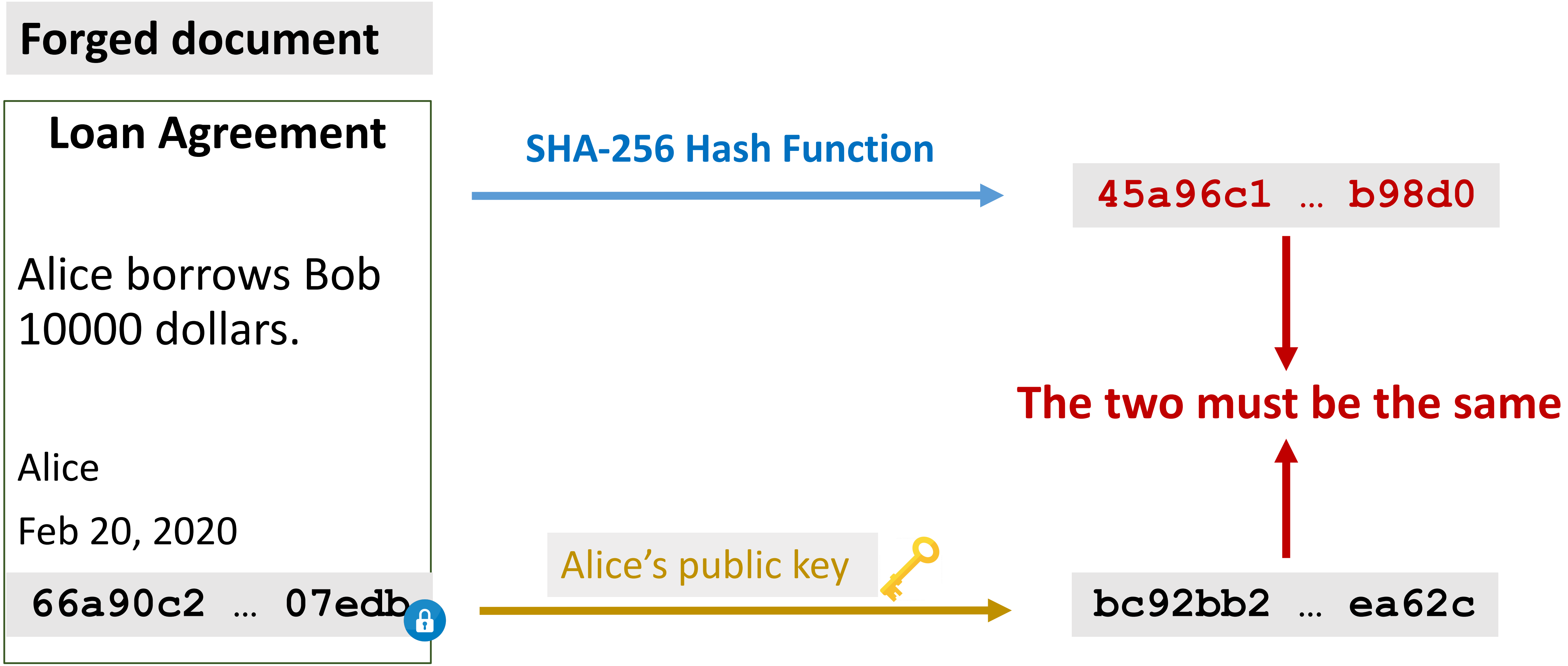
SHA-256 Hash Function

45a96c1 … b98d0

Alice’s public key

bc92bb2 … ea62c

How to forge a document that looks authentic?



Forged document

Loan Agreement

Alice borrows Bob 10000 dollars.

Alice

Feb 20, 2020

`66a90c2 … 07edb`

SHA-256 Hash Function

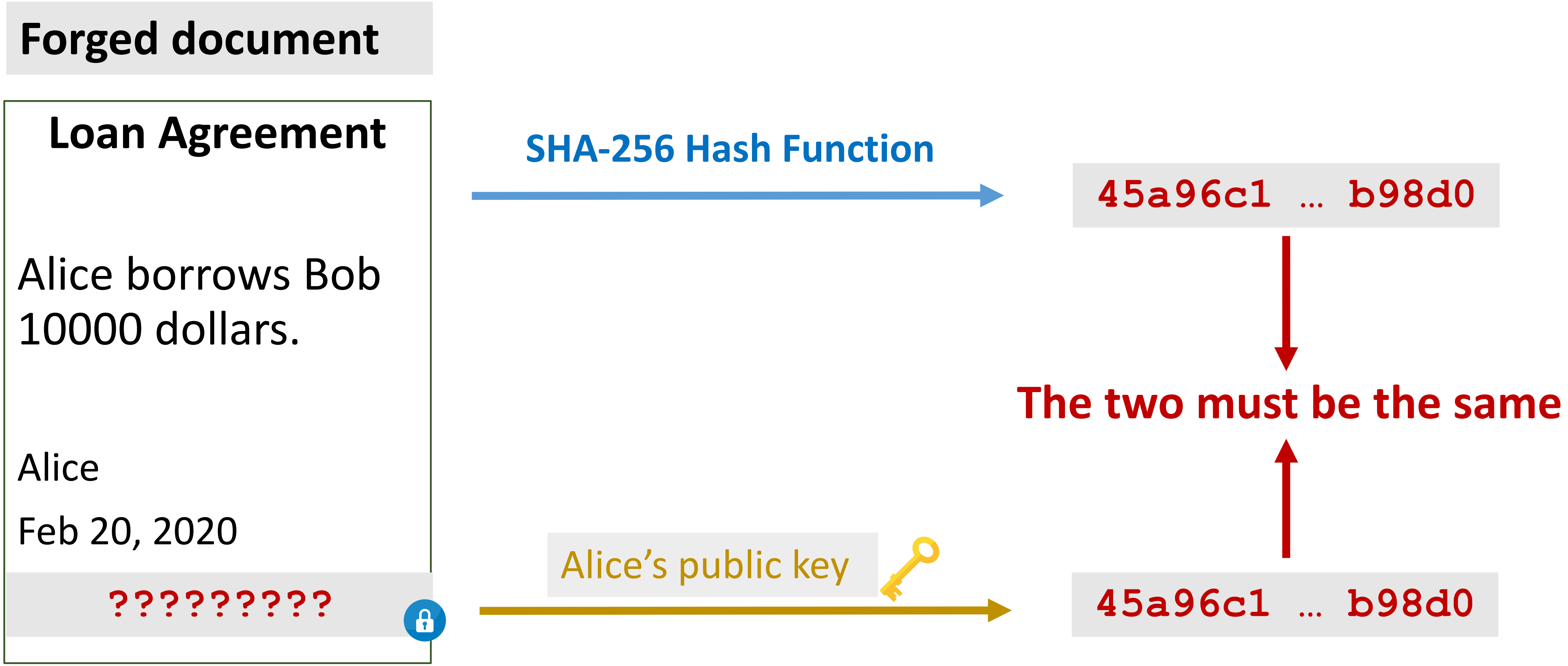
`45a96c1 … b98d0`

The two must be the same

Alice’s public key

`bc92bb2 … ea62c`

Option 1: Modify the digital signature



Forged document

Loan Agreement

Alice borrows Bob 10000 dollars.

Alice

Feb 20, 2020

?????????

SHA-256 Hash Function

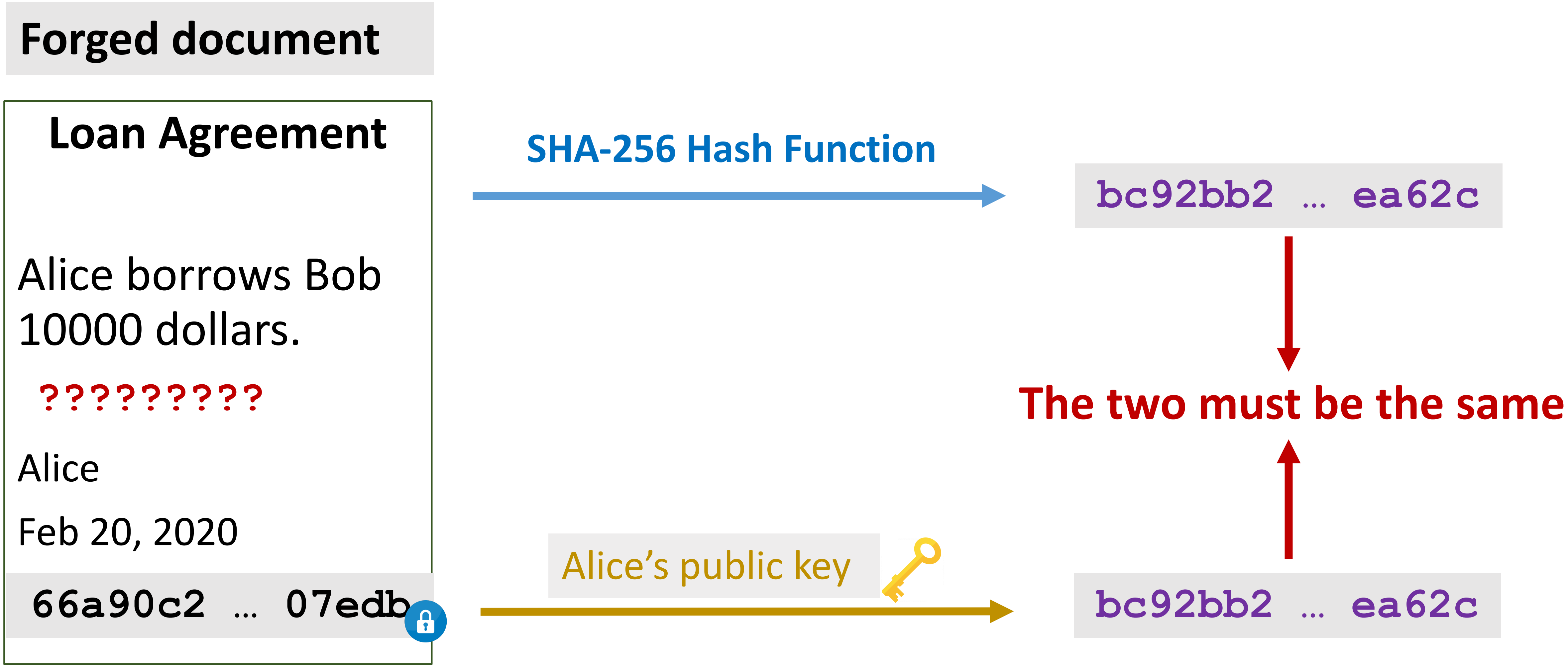
45a96c1 … b98d0

The two must be the same

Alice's public key

45a96c1 … b98d0

Option 2: Modify the file content



Forged document

Loan Agreement

Alice borrows Bob 10000 dollars.

?????????

Alice

Feb 20, 2020

`66a90c2 … 07edb`

SHA-256 Hash Function

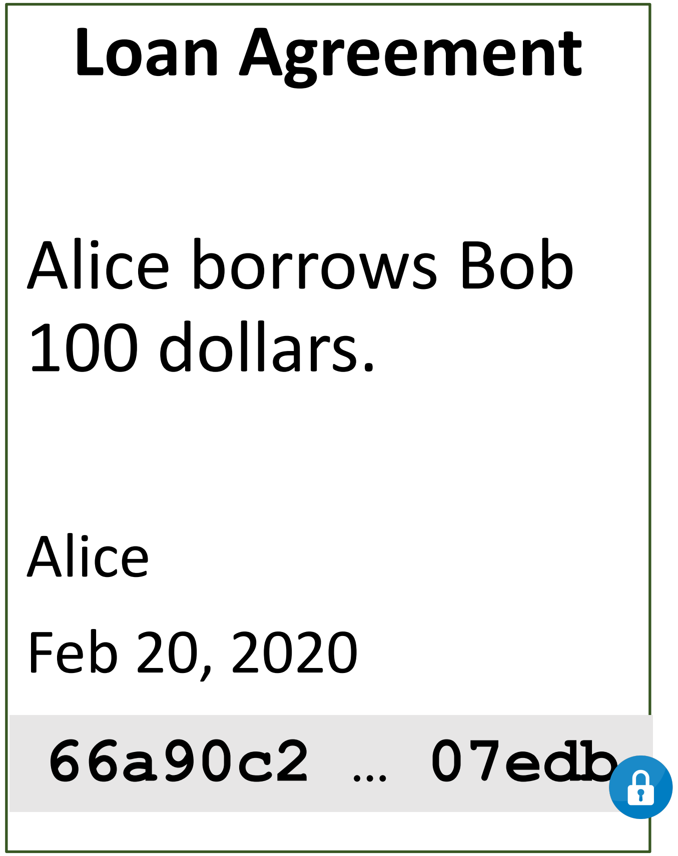
`bc92bb2 … ea62c`

The two must be the same

Alice’s public key

`bc92bb2 … ea62c`

Digital signature is safe



Loan Agreement

Alice borrows Bob 100 dollars.

Alice

Feb 20, 2020

`66a90c2 … 07edb`

- Changing anything in the document will cause hash value mismatch.
- Forging digital signature and creating hash collision are impractical.

Thank You!