# Decentralized Payment System

**Shusen Wang**

# Centralized Payment System

## Bank’s Database:

| User | Balance |
|---|---|
| Alice | 300 |
| Bob | 500 |
| Chris | 60 |
| ⋮ | ⋮ |

# Centralized Payment System

## Bank’s Database:

| User | Balance |
|---|---|
| Alice | 300 |
| Bob | 500 |
| Chris | 60 |
| ⋮ | ⋮ |

## Transaction:

| | |
|---|---|
| From: | Alice |
| To: | Bob |
| Amount: | 50 |

# Centralized Payment System

## Bank’s Database:

| User | Balance | |
|---|---|---|
| Alice | 300 | −50 |
| Bob | 500 | +50 |
| Chris | 60 | |
| ⋮ | ⋮ | |

## Transaction:

| | |
|---|---|
| From: | Alice |
| To: | Bob |
| Amount: | 50 |

# Centralized Payment System

## Bank’s Database:

| User | Balance |
|---|---|
| Alice | 250 |
| Bob | 550 |
| Chris | 60 |
| ⋮ | ⋮ |

## Transaction:

| | |
|---|---|
| From: | Alice |
| To: | Bob |
| Amount: | 50 |

# Decentralized Payment System

# Decentralized Payment System

Alice

| User | Balance |
|---|---|
| Alice | 300 |
| Bob | 500 |
| Chris | 60 |
| ⋮ | ⋮ |

Bob

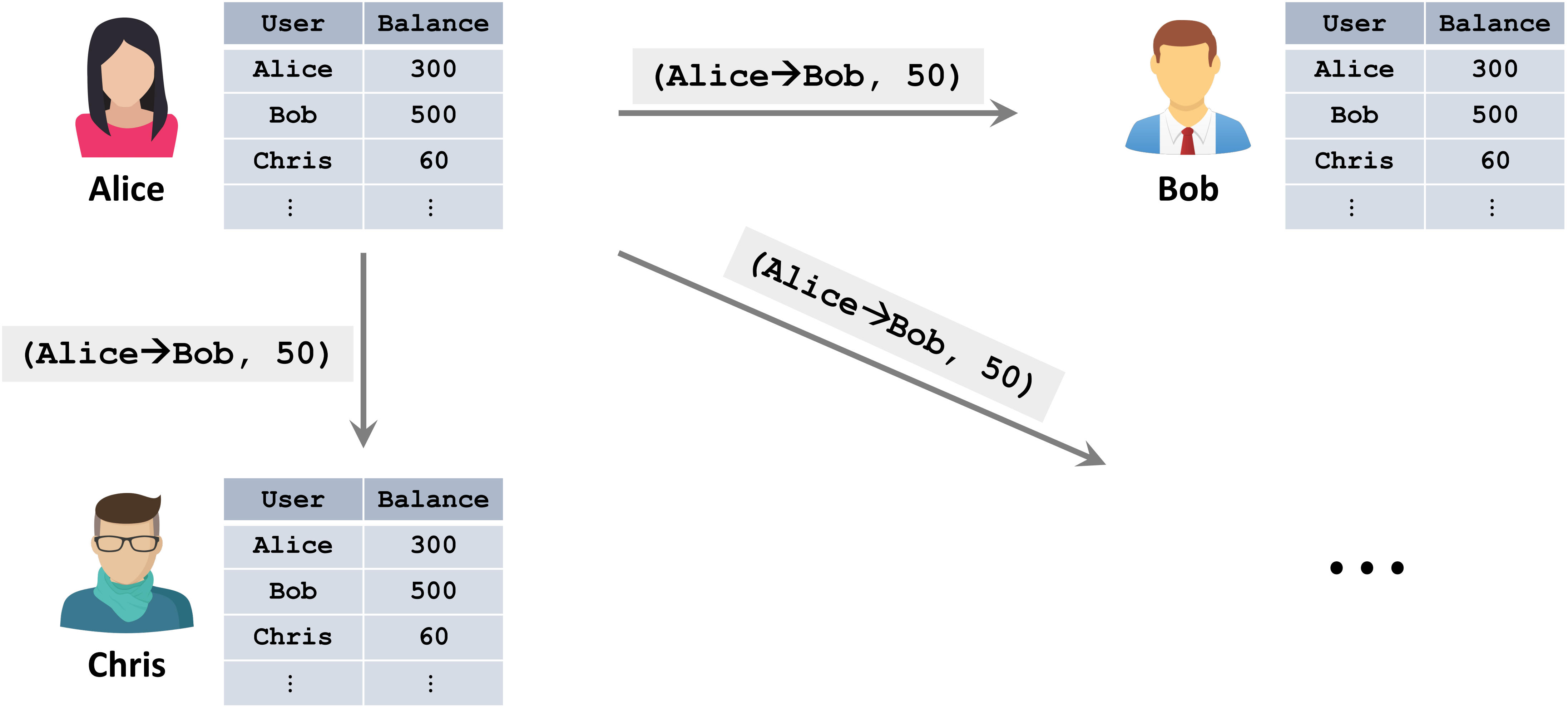
| User | Balance |
|---|---|
| Alice | 300 |
| Bob | 500 |
| Chris | 60 |
| ⋮ | ⋮ |

Chris

| User | Balance |
|---|---|
| Alice | 300 |
| Bob | 500 |
| Chris | 60 |
| ⋮ | ⋮ |

• • •

# Alice transfers $50 to Bob



Alice

| User | Balance |
|---|---|
| Alice | 300 |
| Bob | 500 |
| Chris | 60 |
| ⋮ | ⋮ |

Bob

| User | Balance |
|---|---|
| Alice | 300 |
| Bob | 500 |
| Chris | 60 |
| ⋮ | ⋮ |

Chris

| User | Balance |
|---|---|
| Alice | 300 |
| Bob | 500 |
| Chris | 60 |
| ⋮ | ⋮ |

# Alice transfers $50 to Bob

Alice

| User | Balance | |
|---|---|---|
| Alice | 300 | -50 |
| Bob | 500 | +50 |
| Chris | 60 | |
| ⋮ | ⋮ | |

Bob

| User | Balance | |
|---|---|---|
| Alice | 300 | -50 |
| Bob | 500 | +50 |
| Chris | 60 | |
| ⋮ | ⋮ | |

Chris

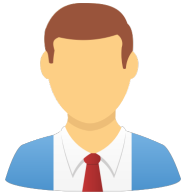
| User | Balance | |
|---|---|---|
| Alice | 300 | -50 |
| Bob | 500 | +50 |
| Chris | 60 | |
| ⋮ | ⋮ | |

• • •

# Alice transfers $50 to Bob

Alice

| User | Balance |
|---|---|
| Alice | 250 |
| Bob | 550 |
| Chris | 60 |
| ⋮ | ⋮ |



Bob

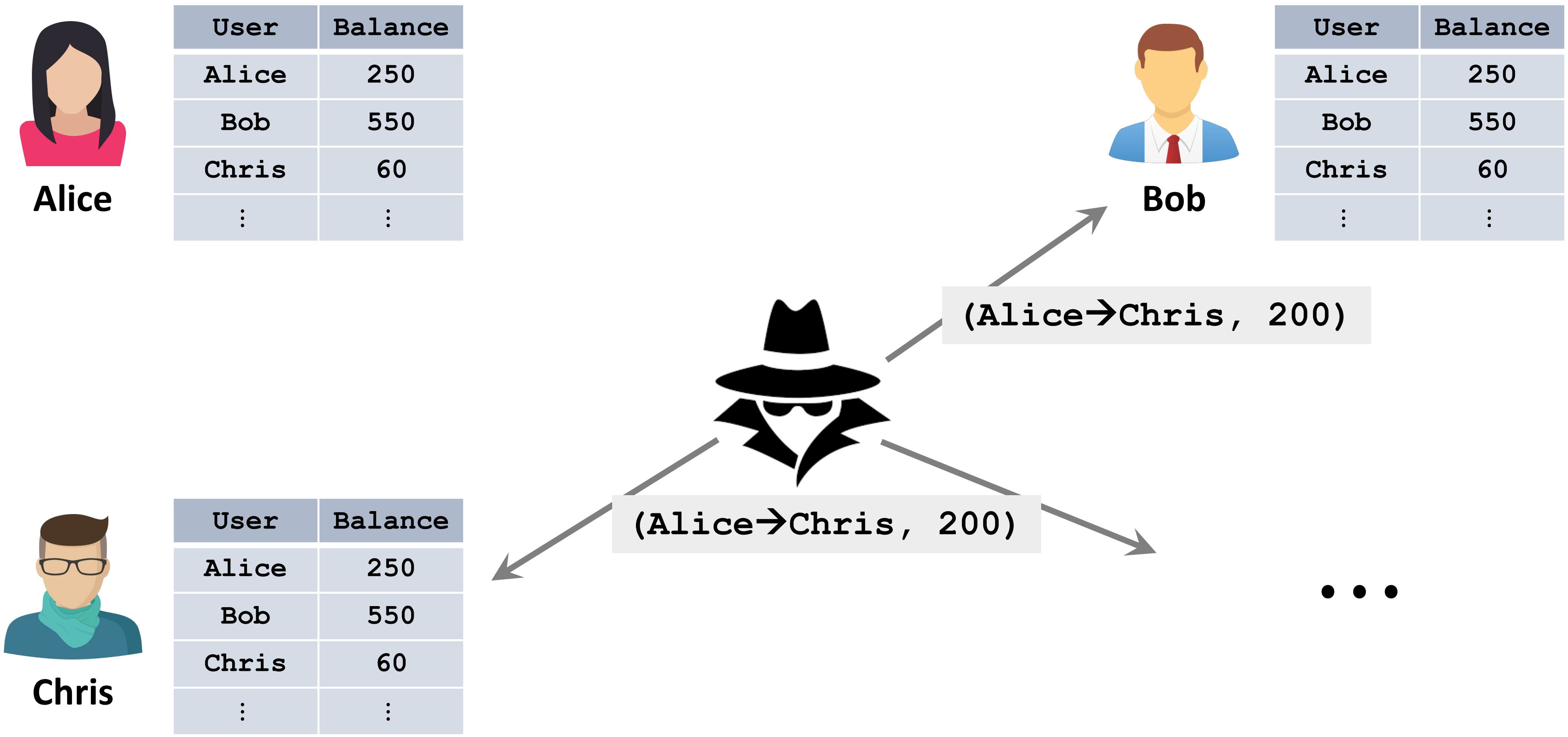
| User | Balance |
|---|---|
| Alice | 250 |
| Bob | 550 |
| Chris | 60 |
| ⋮ | ⋮ |

Chris

| User | Balance |
|---|---|
| Alice | 250 |
| Bob | 550 |
| Chris | 60 |
| ⋮ | ⋮ |

• • •

# How to verify the authenticity?



Alice

| User | Balance |
|---|---|
| Alice | 250 |
| Bob | 550 |
| Chris | 60 |
| ⋮ | ⋮ |

Bob

| User | Balance |
|---|---|
| Alice | 250 |
| Bob | 550 |
| Chris | 60 |
| ⋮ | ⋮ |

Chris

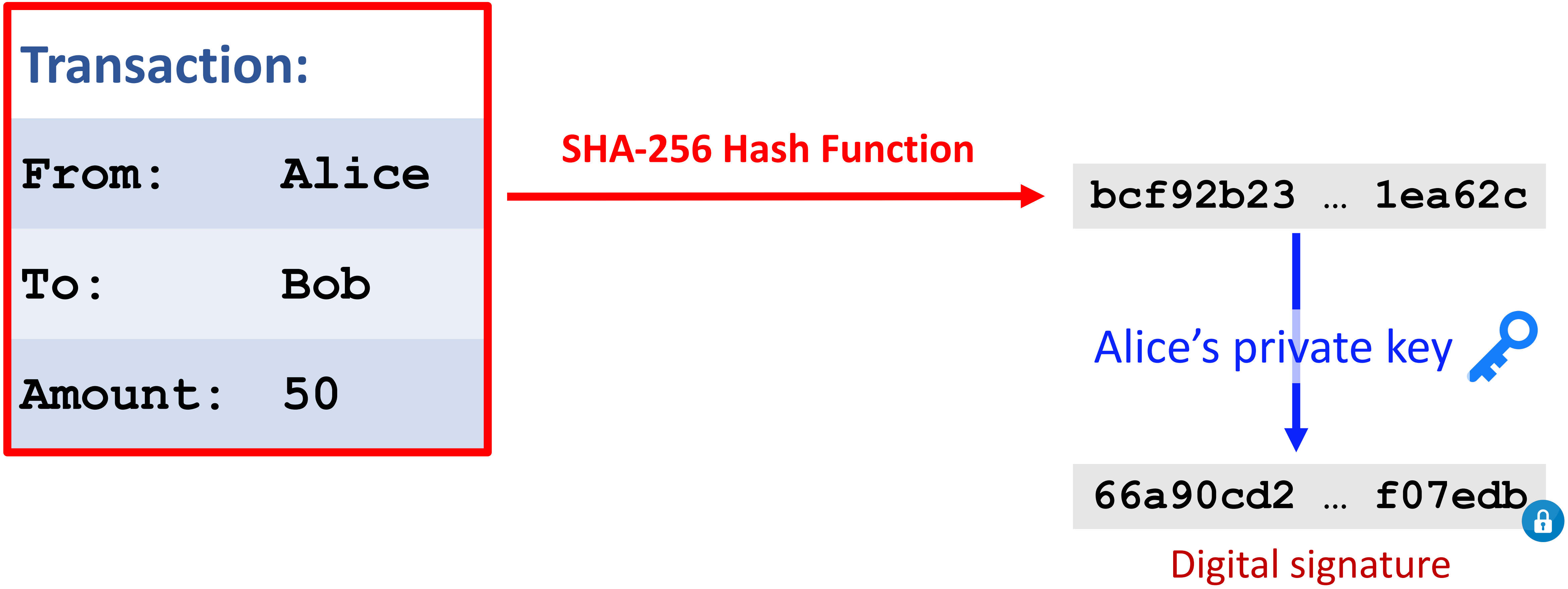
| User | Balance |
|---|---|
| Alice | 250 |
| Bob | 550 |
| Chris | 60 |
| ⋮ | ⋮ |

(Alice→Chris, 200)

(Alice→Chris, 200)

• • •

# Use Digital Signature



Transaction:

| | |
|---|---|
| From: | Alice |
| To: | Bob |
| Amount: | 50 |

SHA-256 Hash Function

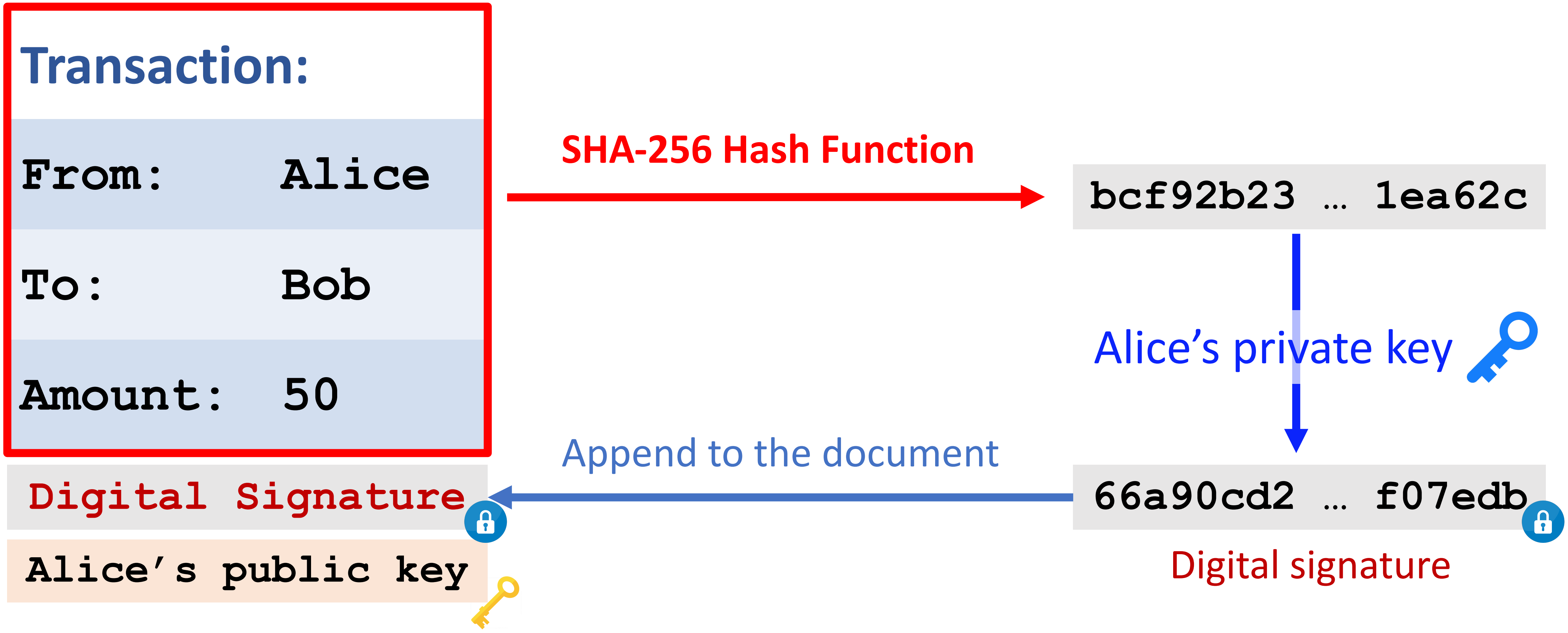
`bcf92b23 … 1ea62c`

Alice’s private key

`66a90cd2 … f07edb`

Digital signature

# Use Digital Signature



Transaction:

| | |
|---|---|
| From: | Alice |
| To: | Bob |
| Amount: | 50 |

Digital Signature

Alice's public key

SHA-256 Hash Function

bcf92b23 … 1ea62c

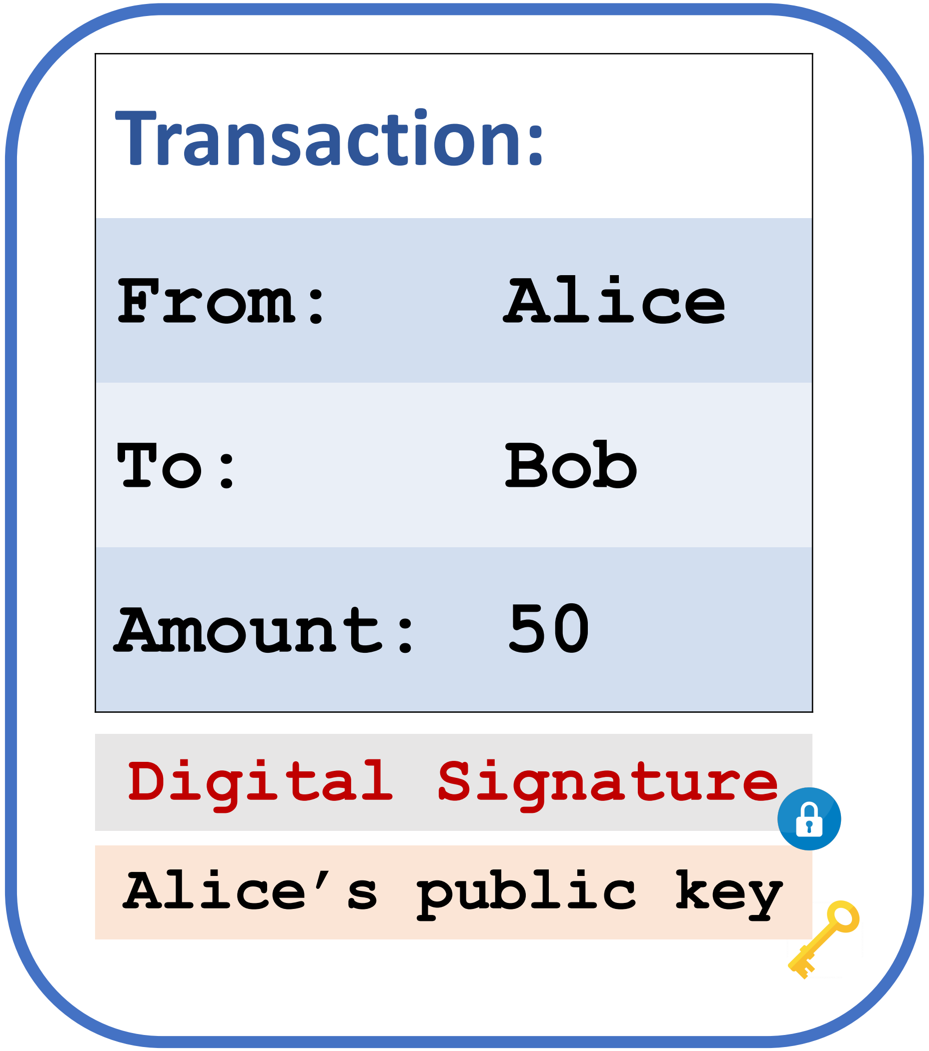
Alice's private key

66a90cd2 … f07edb

Digital signature

Append to the document

# Use Digital Signature



**Transaction:**

| | |
|---|---|
| From: | Alice |
| To: | Bob |
| Amount: | 50 |

Digital Signature

Alice's public key

- Use digital signature to ensure the authenticity of a message.
- Alice's public key is known to everyone.
- Others can verify the authenticity using Alice's public key.

# Use Digital Signature

## Transaction:

| | | |
|---|---|---|
| From: | ~~Alice~~ | Alice’s Public Key |
| To: | ~~Bob~~ | Bob’s Public Key |
| Amount: | 50 | |

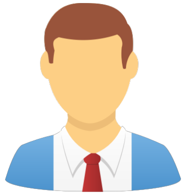
Digital Signature

# Ledger: Transaction History

# Decentralized Ledger

Alice

| ~~User~~ | ~~Balance~~ |
|---|---|
| ~~Alice~~ | ~~300~~ |
| ~~Bob~~ | ~~500~~ |
| ~~Chris~~ | ~~60~~ |
| ⋮ | ⋮ |



Bob

| ~~User~~ | ~~Balance~~ |
|---|---|
| ~~Alice~~ | ~~300~~ |
| ~~Bob~~ | ~~500~~ |
| ~~Chris~~ | ~~60~~ |
| ⋮ | ⋮ |

Chris

| ~~User~~ | ~~Balance~~ |
|---|---|
| ~~Alice~~ | ~~300~~ |
| ~~Bob~~ | ~~500~~ |
| ~~Chris~~ | ~~60~~ |
| ⋮ | ⋮ |

• • •

# Decentralized Ledger

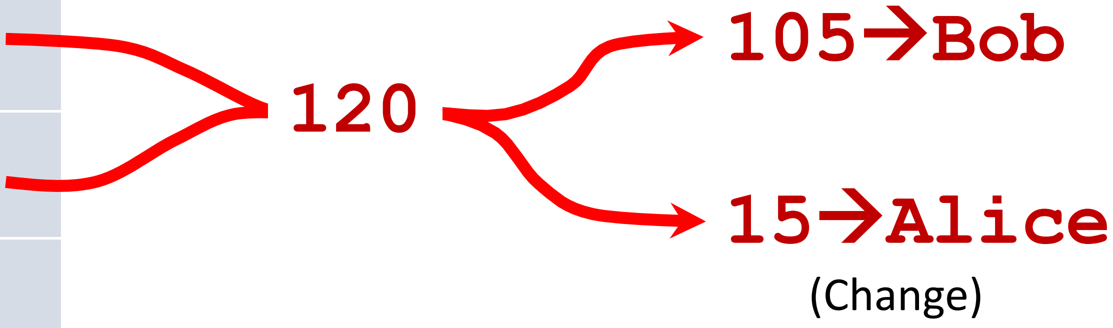
| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| ⋮ | ⋮ | ⋮ |

# Decentralized Ledger

| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| ⋮ | ⋮ | ⋮ |

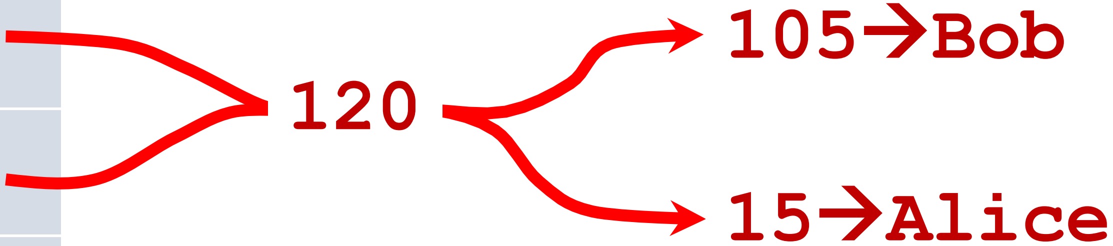
# Decentralized Ledger

| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| ⋮ | ⋮ | ⋮ |



# Decentralized Ledger

| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| Alice | Bob | 105 |
| Alice | Alice | 15 |



120

105→Bob

15→Alice

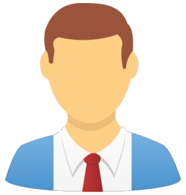
# How do you send money?

1. Search your history to find all of your unspent income.
2. Write down:
   - previous transactions (source),
   - recipients (their public keys),
   - values (amount).
3. Add digital signature.
4. Publicly announce the transaction.

# Everyone update their ledgers

Alice

| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| Alice | Bob | 105 |
| Alice | Alice | 15 |



Bob

| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| Alice | Bob | 105 |
| Alice | Alice | 15 |

Chris

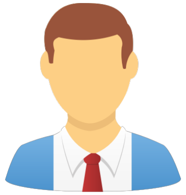
| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| Alice | Bob | 105 |
| Alice | Alice | 15 |

• • •

# How to guarantee consensus?

Alice

| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| Alice | Bob | 105 |
| Alice | Alice | 15 |



Bob

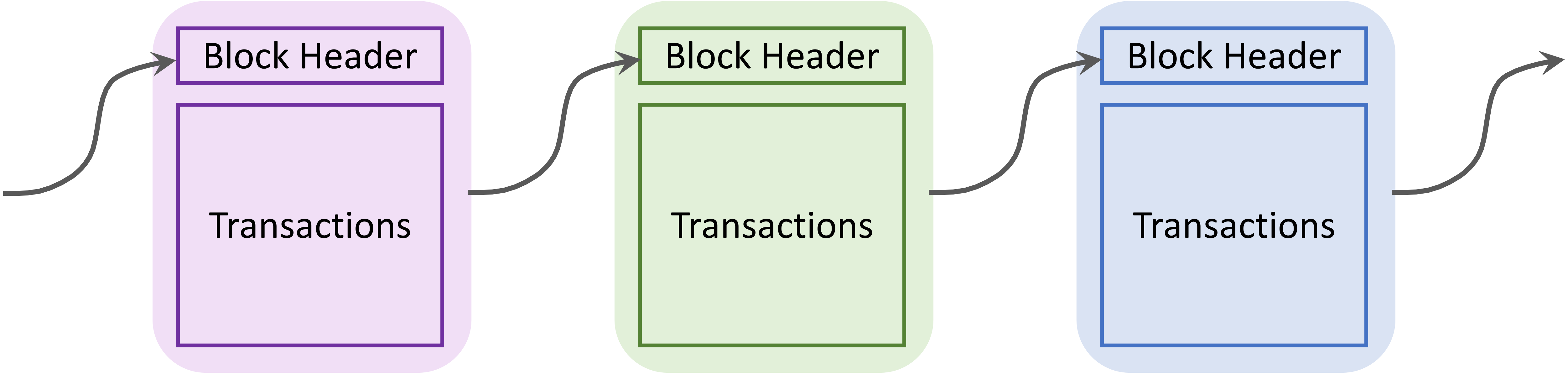
| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| Alice | Bob | 105 |
| Alice | Alice | 15 |

Chris

| From | To | Amount |
|---|---|---|
| ⋮ | ⋮ | ⋮ |
| System | Alice | 100 |
| Chris | Alice | 20 |
| System | Bob | 100 |
| System | Alice | 100 |
| Alice | Bob | 105 |
| Alice | Alice | 15 |

• • •

# Solution: Blockchain



# Thank You!