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
⋮	⋮

(Alice→Bob, 50)

Bob

User	Balance
Alice	300
Bob	500
Chris	60
⋮	⋮

(Alice→Bob, 50)

(Alice→Bob, 50)

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
⋮	⋮

(Alice→Chris, 200)

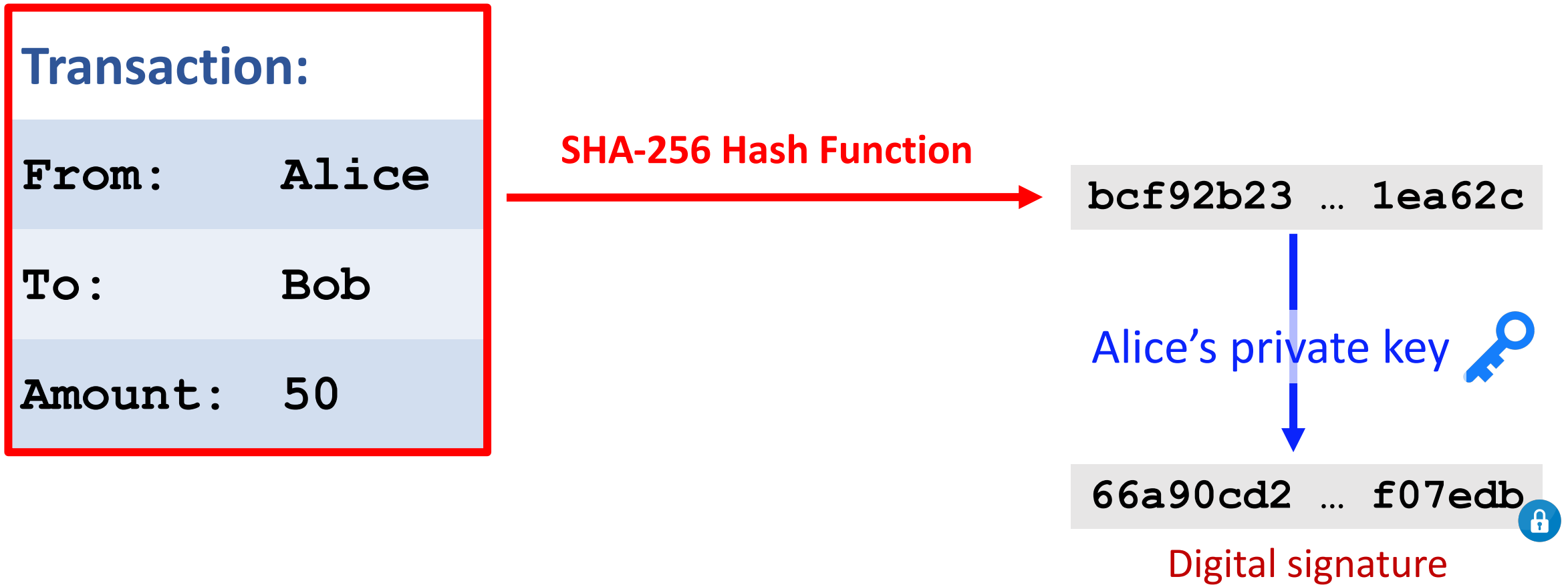
(Alice→Chris, 200)

Chris

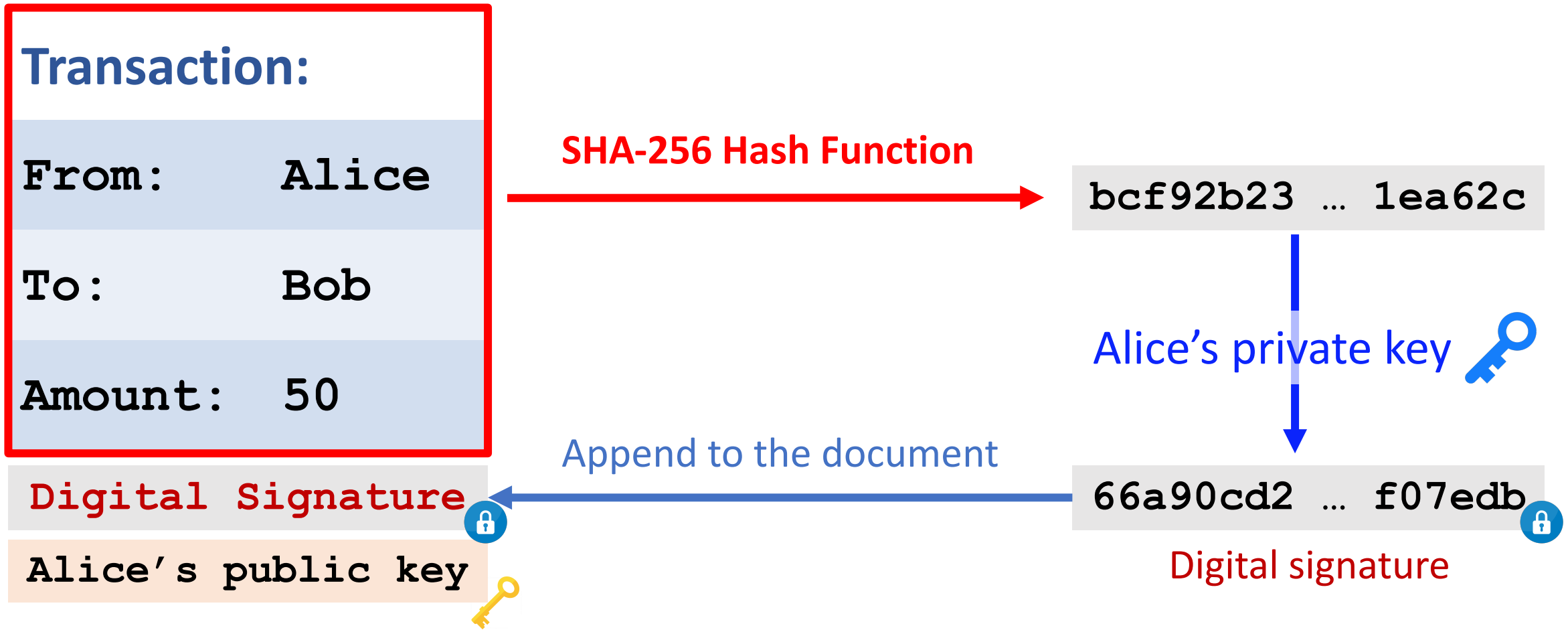
User	Balance
Alice	250
Bob	550
Chris	60
⋮	⋮

• • •

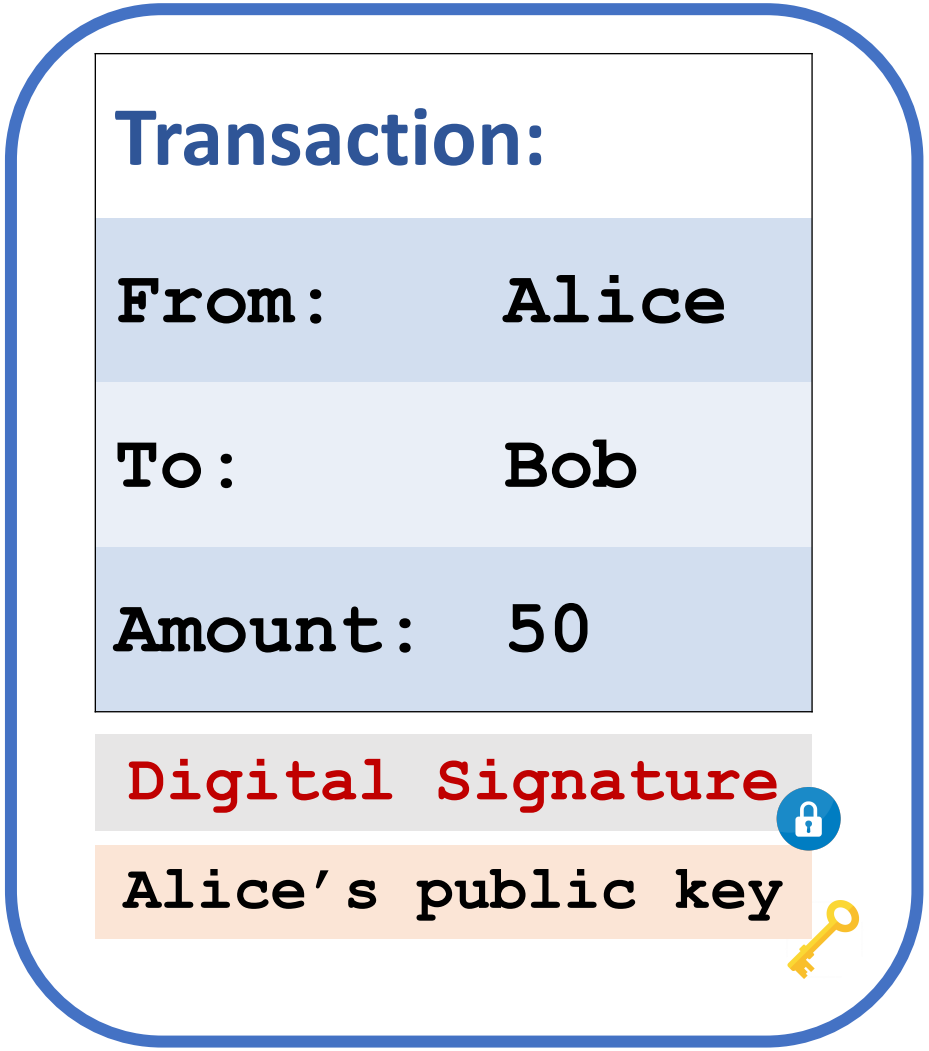
Use Digital Signature



Use Digital Signature

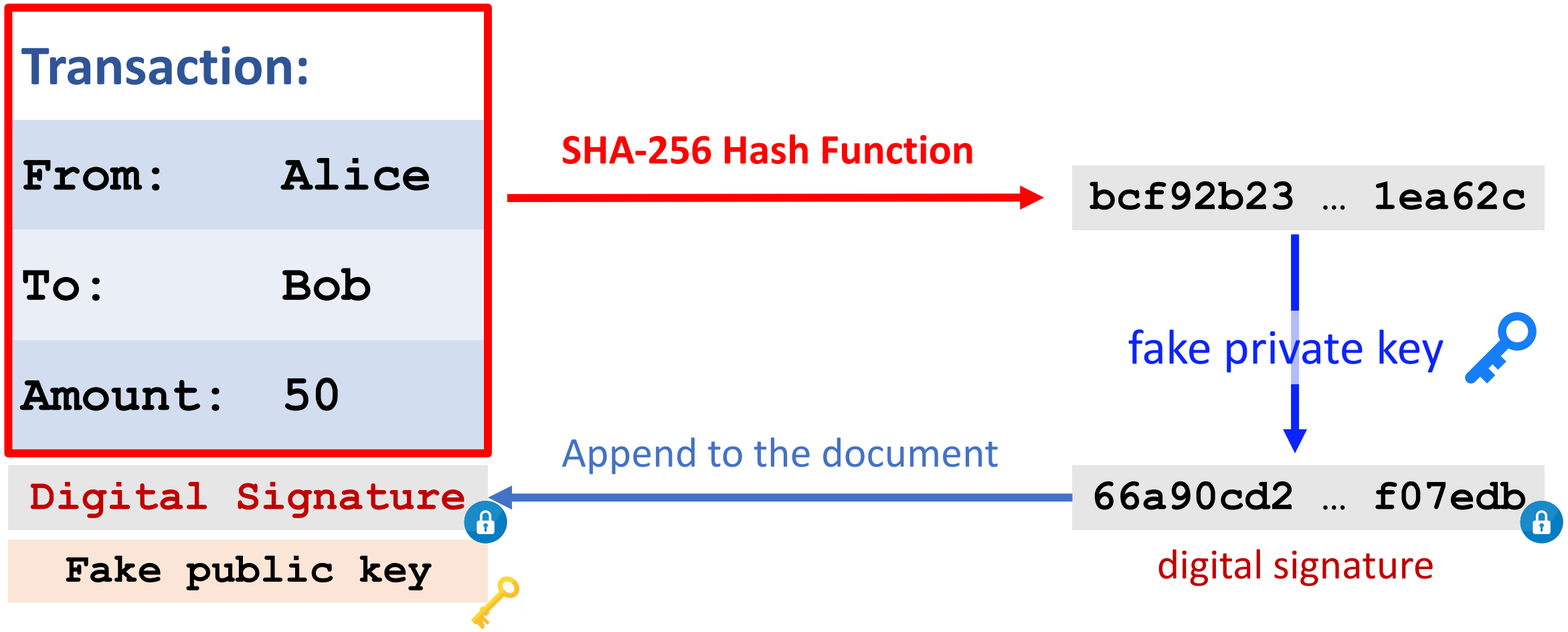


Use Digital Signature

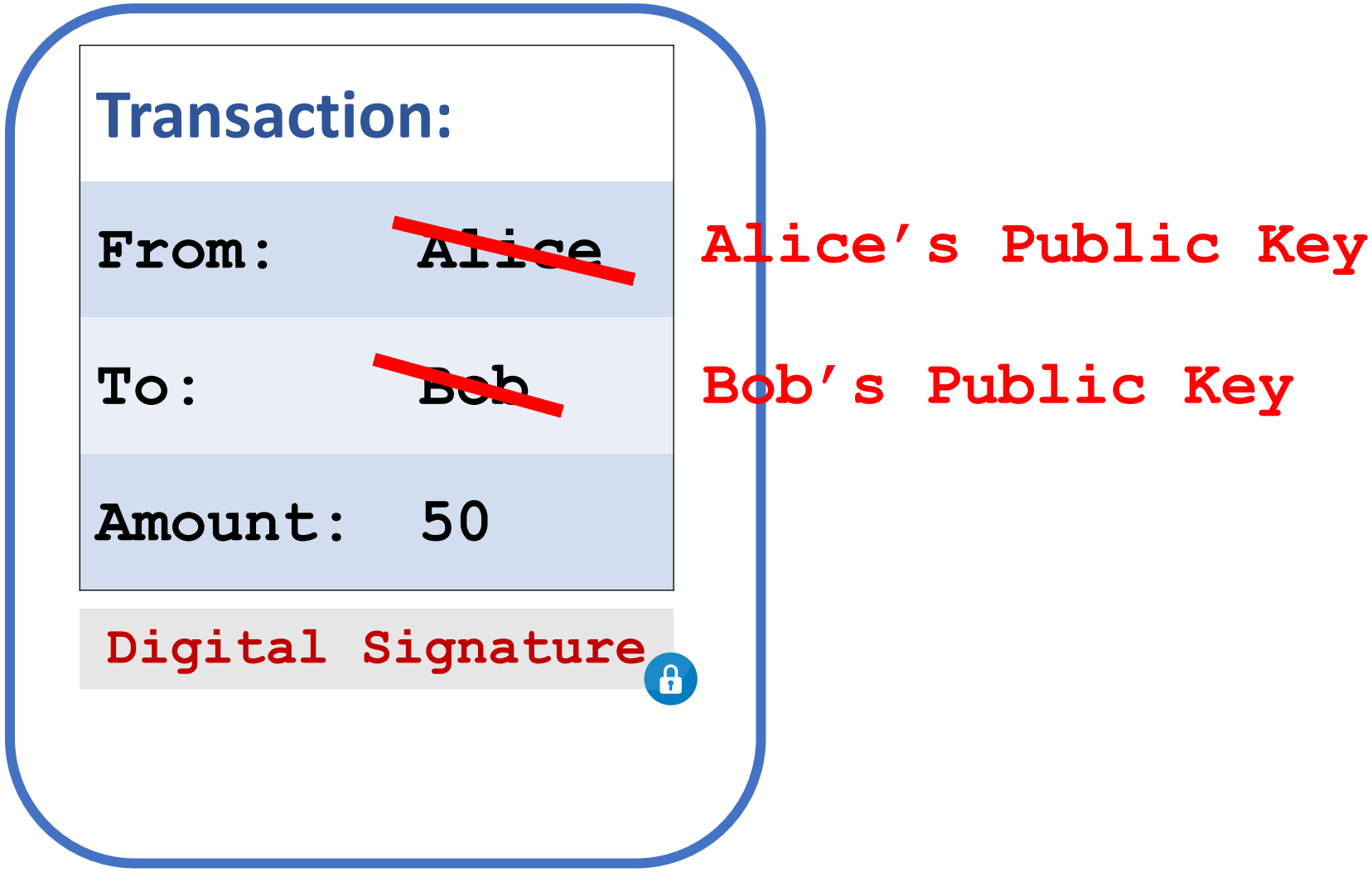


- Use digital signature to ensure the authenticity of a message.
- Alice's public key is known to everyone.
- Others can verify the authenticity using Alice's public key.

Use Digital Signature



Use Digital Signature



Ledger: Transaction History

Decentralized Ledger

Alice

User	Balance
Alice	200
Bob	500
Chris	60
⋮	⋮

Bob

User	Balance
Alice	200
Bob	500
Chris	60
⋮	⋮

Chris

User	Balance
Alice	200
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

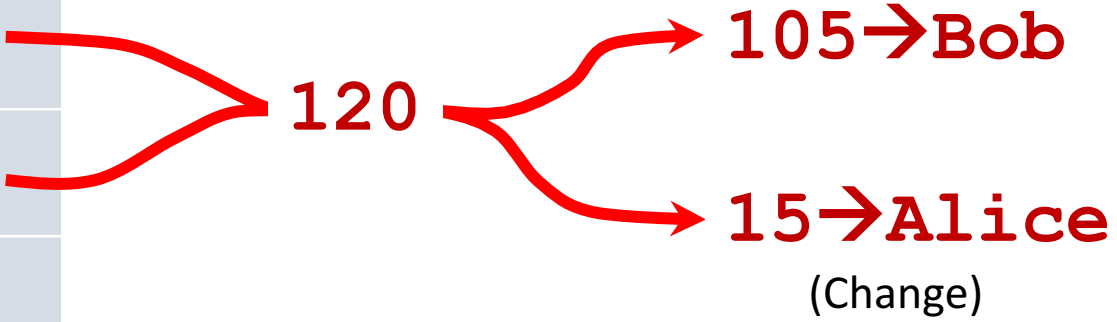
From	To	Amount
⋮	⋮	⋮
System	Alice	100
Chris	Alice	20
System	Bob	100
System	Alice	100
⋮	⋮	⋮

Alice wants to pay Bob 105 Bitcoins

Decentralized Ledger

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

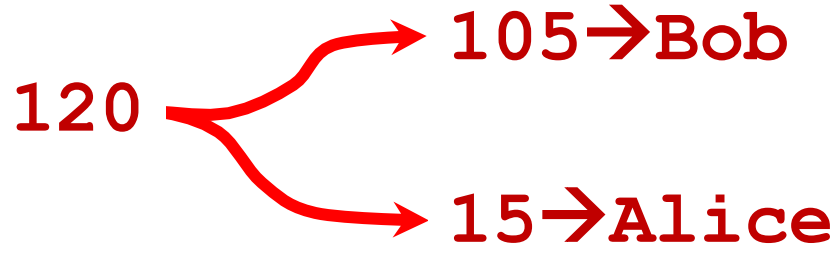
Alice wants to pay Bob 105 Bitcoins



Decentralized Ledger

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

Alice wants to pay Bob 105 Bitcoins



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

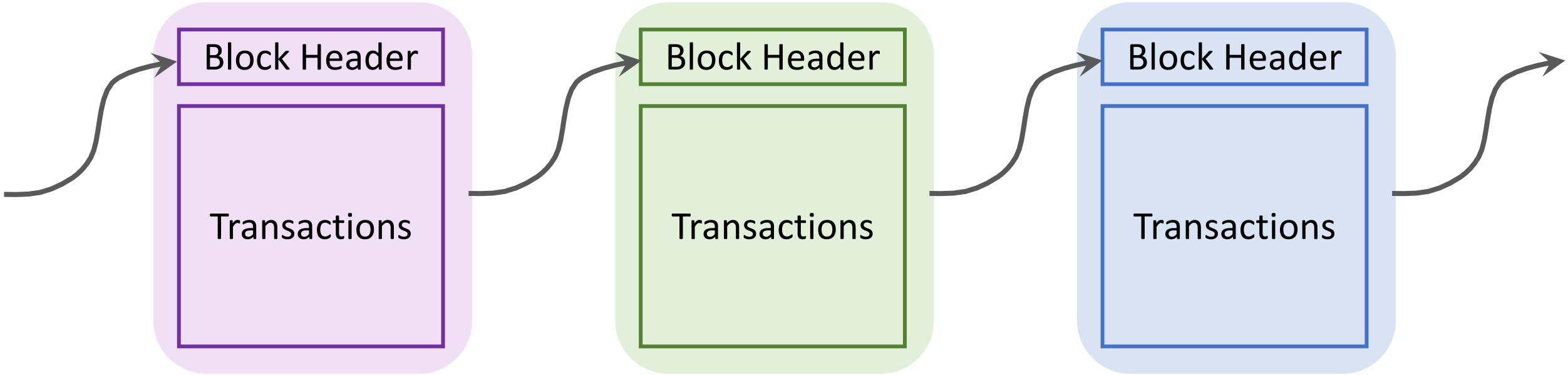
From	To	Amount
⋮	⋮	⋮
System	Alice	100
Chris	Alice	20
System	Bob	100
System	Alice	100
Alice	Bob	105
Alice	Alice	15

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!