# Upgrading Bitcoin: Segregated Witness

Dr. Johnson Lau

Bitcoin Core Contributor

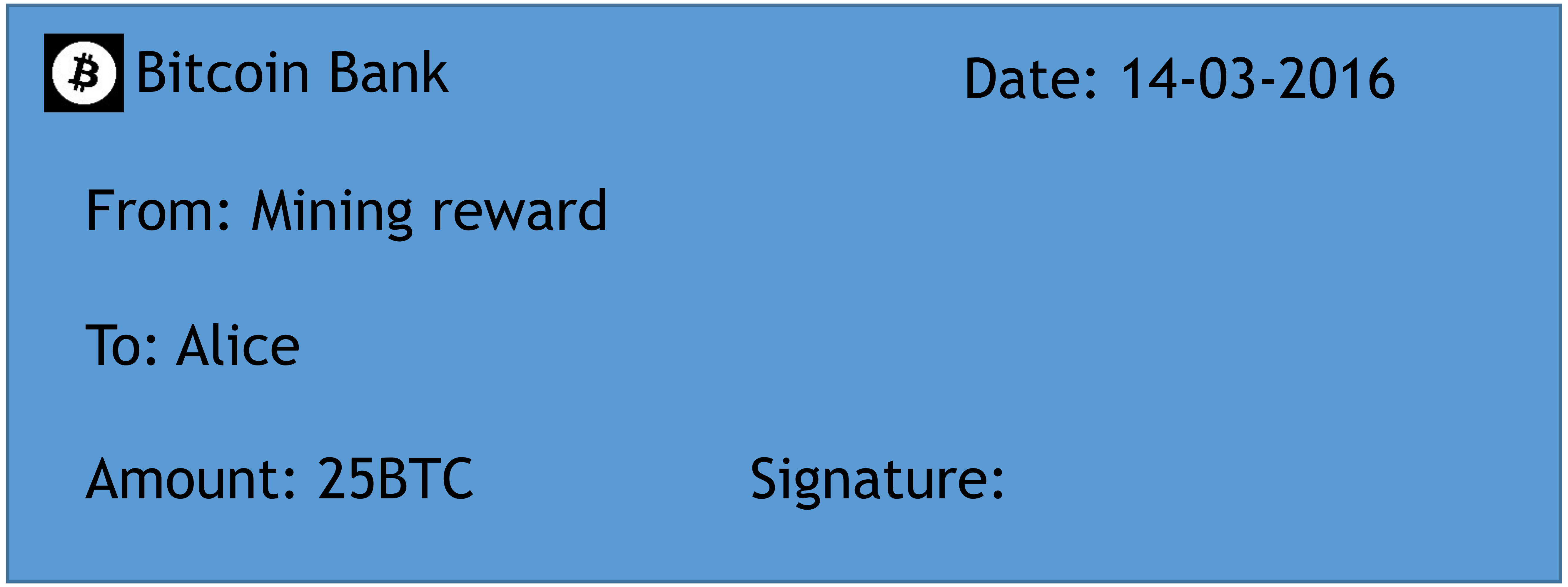
Co-author of Segregated Witness BIPs 141-143

16-March-2016

# Topics

- A short introduction to Bitcoin transactions
- What is transaction malleability and why it is bad
- Segregated witness as the solution
- Bonus of deploying segregated witness
- User experience
- Safety issues of deploying segregated witness

# Bitcoin Transaction is like a cheque



Bitcoin Bank

Date: 14-03-2016

From: Mining reward

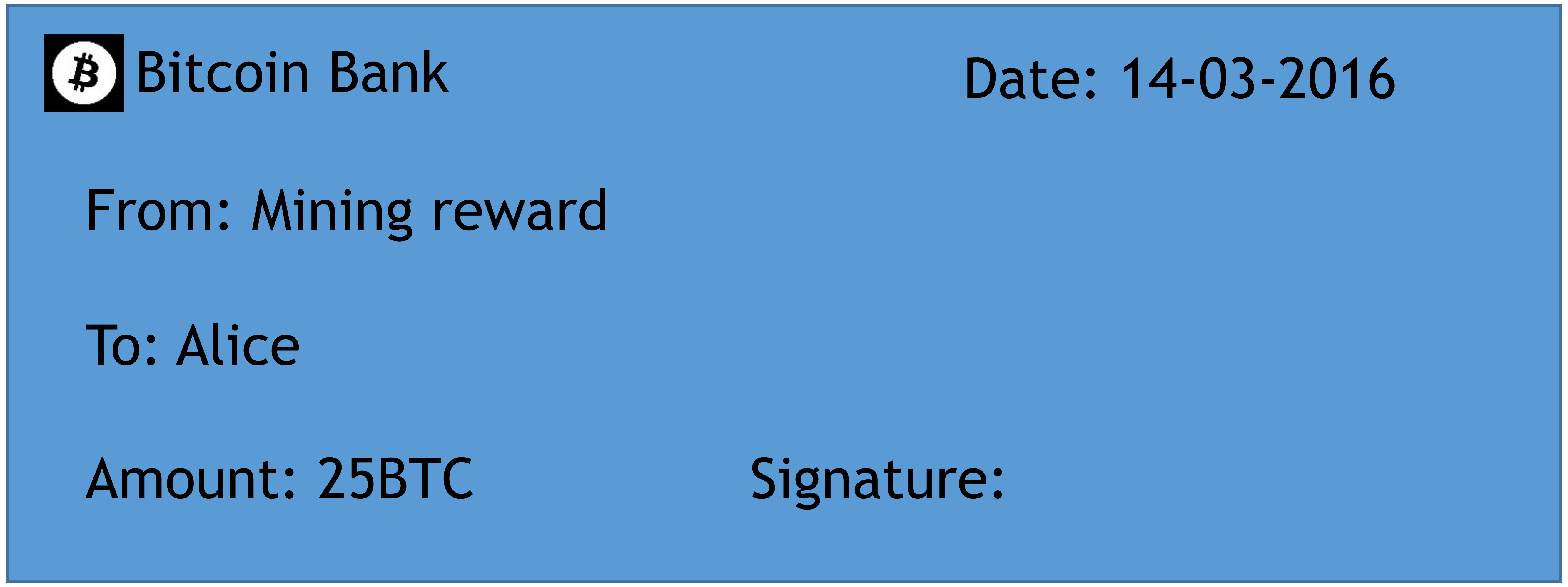
To: Alice

Amount: 25BTC

Signature:

Alice: 25 BTC

# Bitcoin Transaction is like a cheque



Bitcoin Bank

Date: 14-03-2016

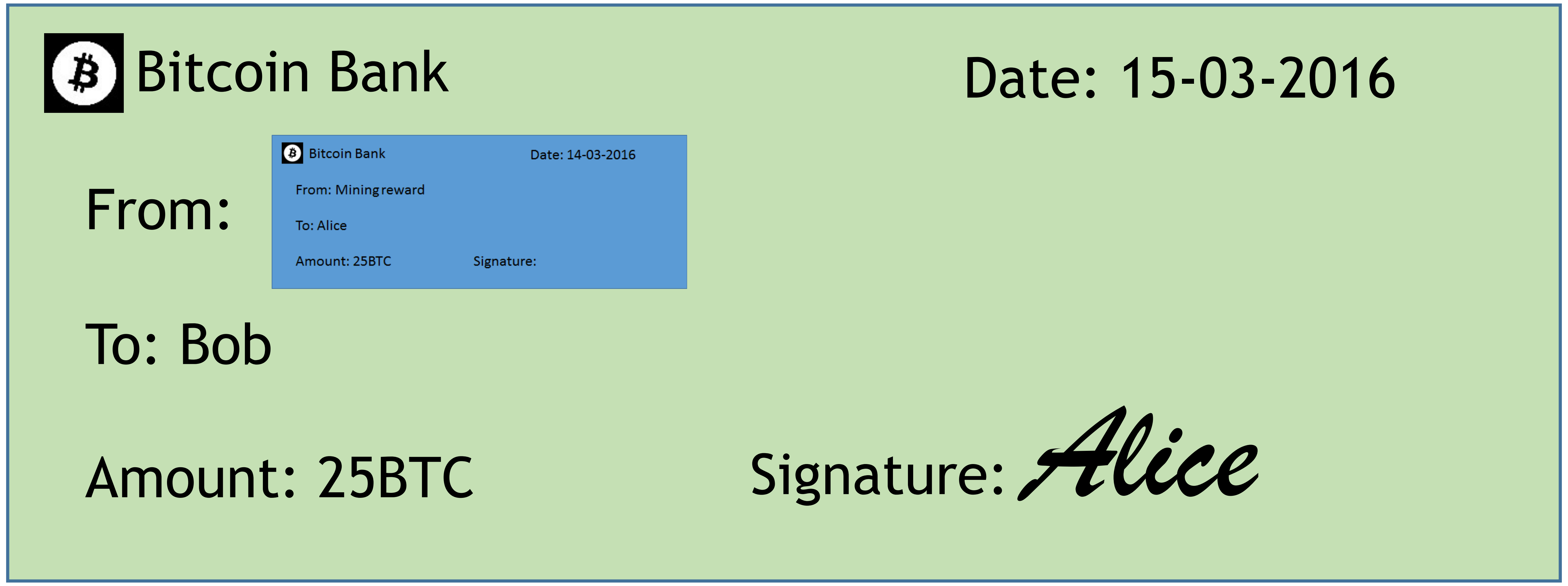
From: Mining reward

To: Alice

Amount: 25BTC

Signature:

Alice: 25 BTC



Bitcoin Bank

Date: 15-03-2016

From:

Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC

Signature:

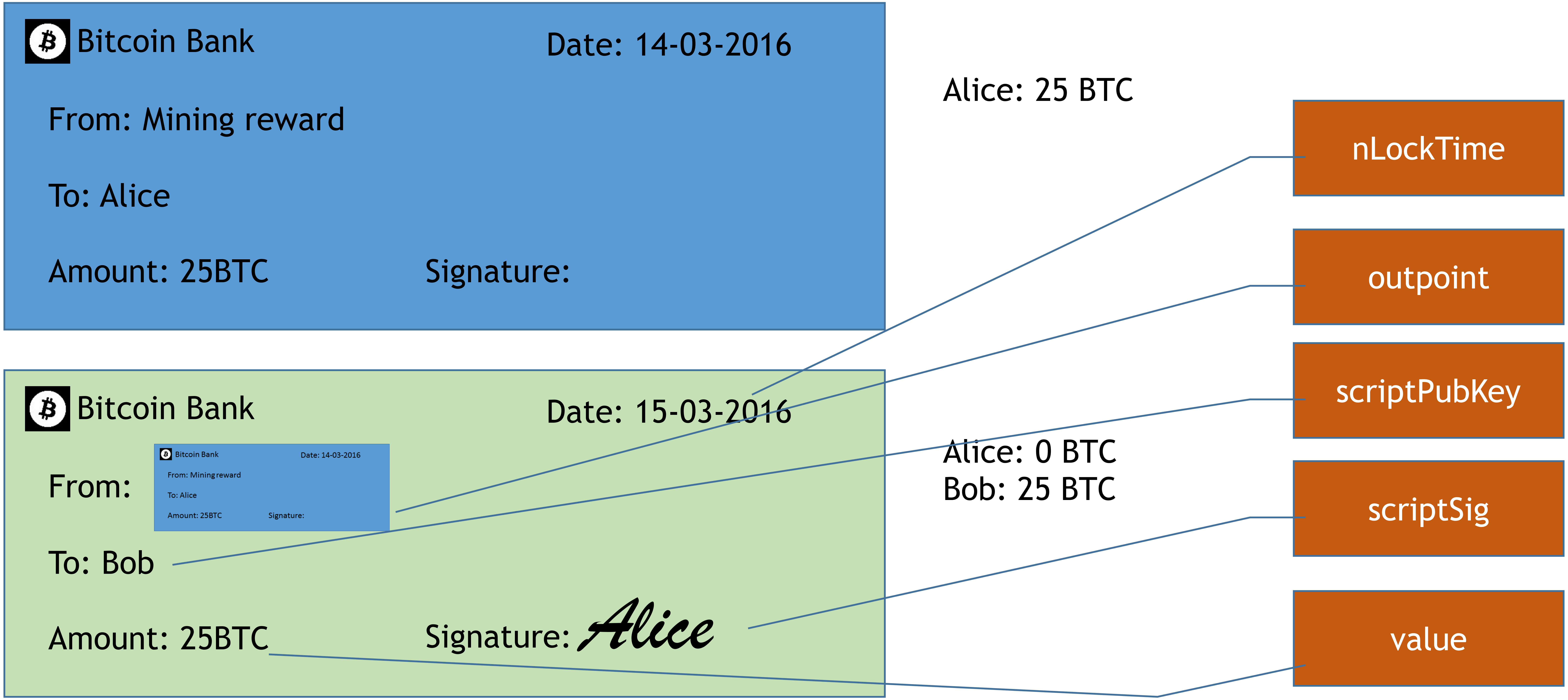
To: Bob

Amount: 25BTC

Signature: Alice

Alice: 0 BTC
Bob: 25 BTC

# Bitcoin Transaction is like a cheque



Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC

Signature:

Alice: 25 BTC

Bitcoin Bank

Date: 15-03-2016

From:

Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC

Signature:

To: Bob

Amount: 25BTC

Signature: Alice

Alice: 0 BTC
Bob: 25 BTC

nLockTime

outpoint

scriptPubKey

scriptSig

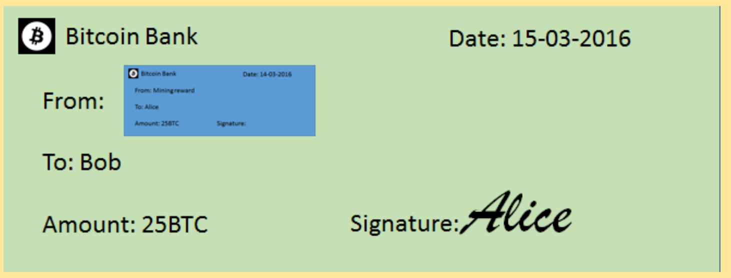
value

# Passing on

Bitcoin Bank

Date: 18-03-2016

From:



Bitcoin Bank

Date: 15-03-2016

From:

Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC

Signature:

To: Bob

Amount: 25BTC

Signature: Alice

To: Carl

Amount: 24.99BTC

Signature: Bob

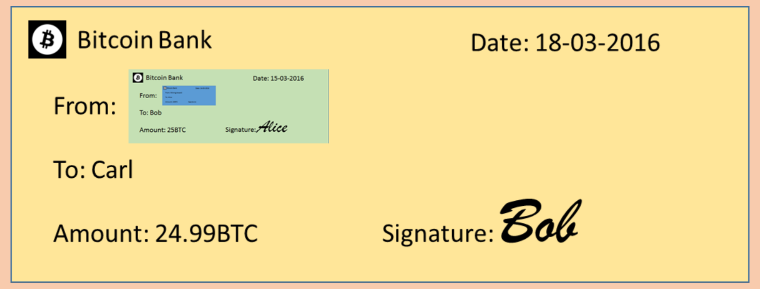
Alice: 0 BTC
Bob: 0 BTC
Carl: 24.99 BTC

Fee: 0.01 BTC

Bitcoin Bank

Date: 13-03-2016

From:



Bitcoin Bank

Date: 18-03-2016

From:

Bitcoin Bank

Date: 15-03-2016

From:

To: Bob

Amount: 25BTC

Signature: Alice

To: Carl

Amount: 24.99BTC

Signature: Bob

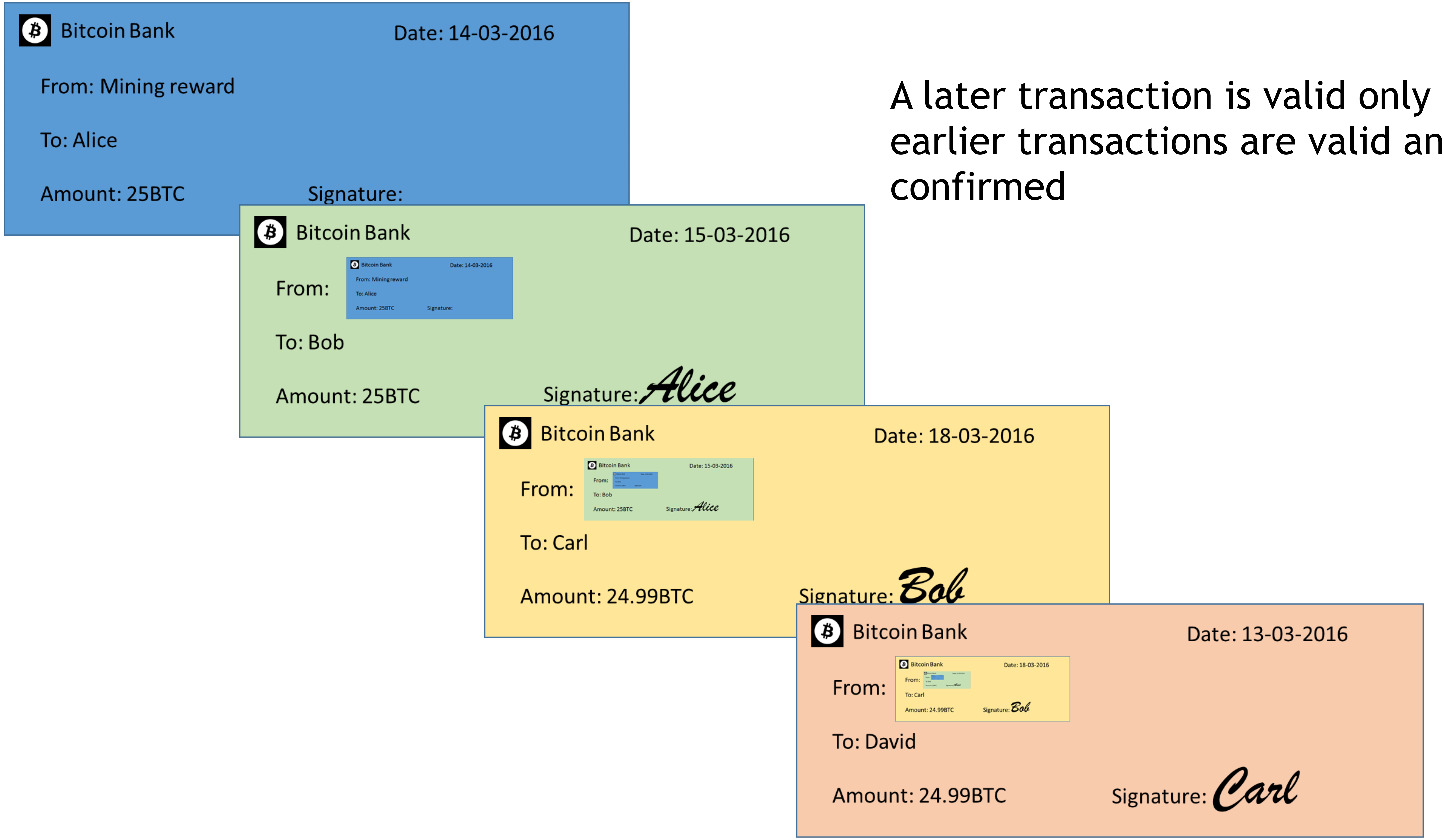
To: David

Amount: 24.99BTC

Signature: Carl

Alice: 0 BTC
Bob: 0 BTC
Carl: 0 BTC
David: 24.99 BTC

# A chain of transactions



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

Bitcoin Bank Date: 15-03-2016

From:

To: Bob

Amount: 25BTC Signature: Alice

Bitcoin Bank Date: 18-03-2016

From:

To: Carl

Amount: 24.99BTC Signature: Bob

Bitcoin Bank Date: 13-03-2016

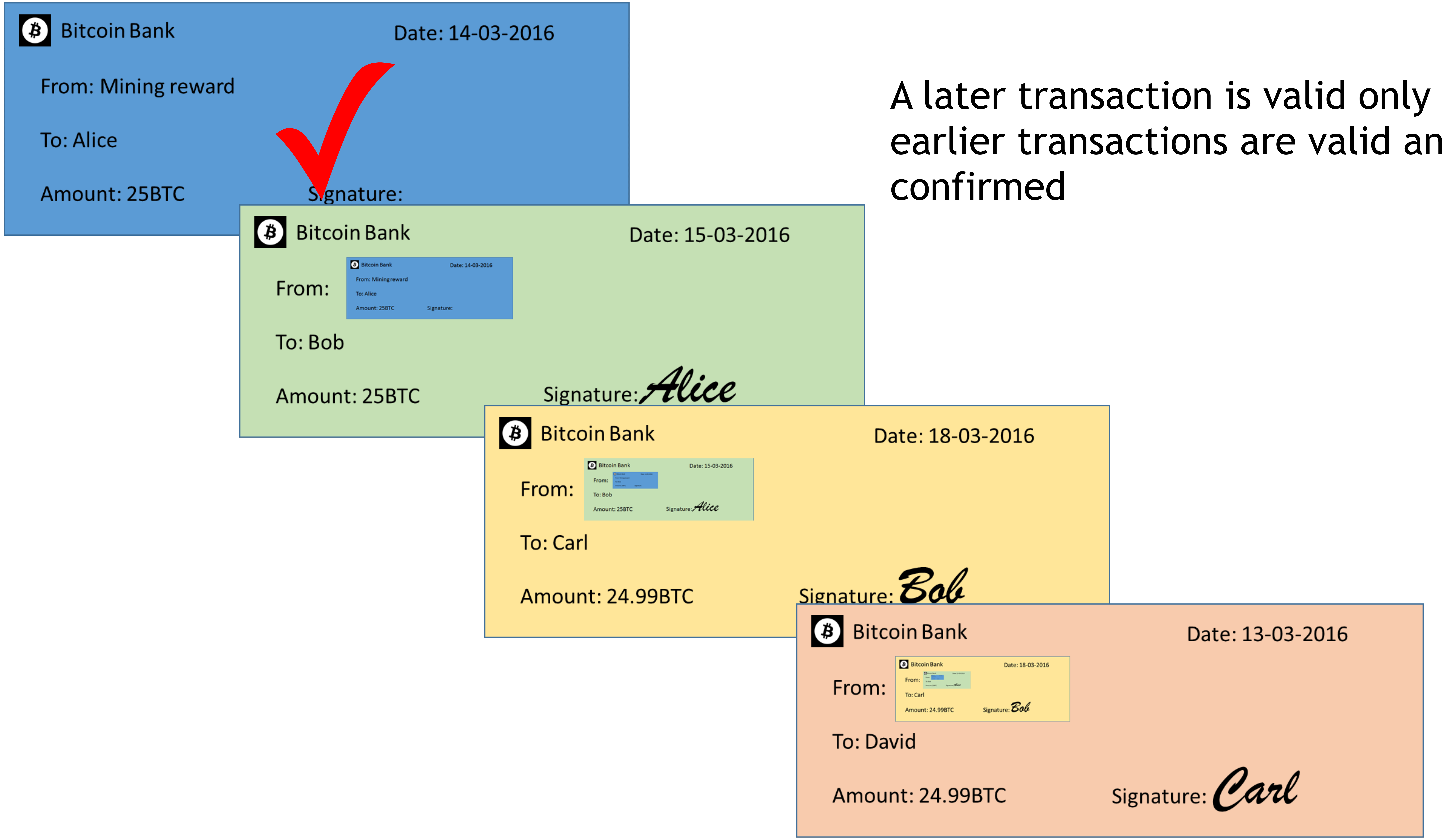
From:

To: David

Amount: 24.99BTC Signature: Carl

A later transaction is valid only if the earlier transactions are valid and confirmed

# A chain of transactions



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Alice Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

Bitcoin Bank Date: 18-03-2016

From: Bitcoin Bank Date: 15-03-2016 From: To: Bob Amount: 25BTC Signature: Alice

To: Carl

Amount: 24.99BTC Signature: Bob

Bitcoin Bank Date: 13-03-2016

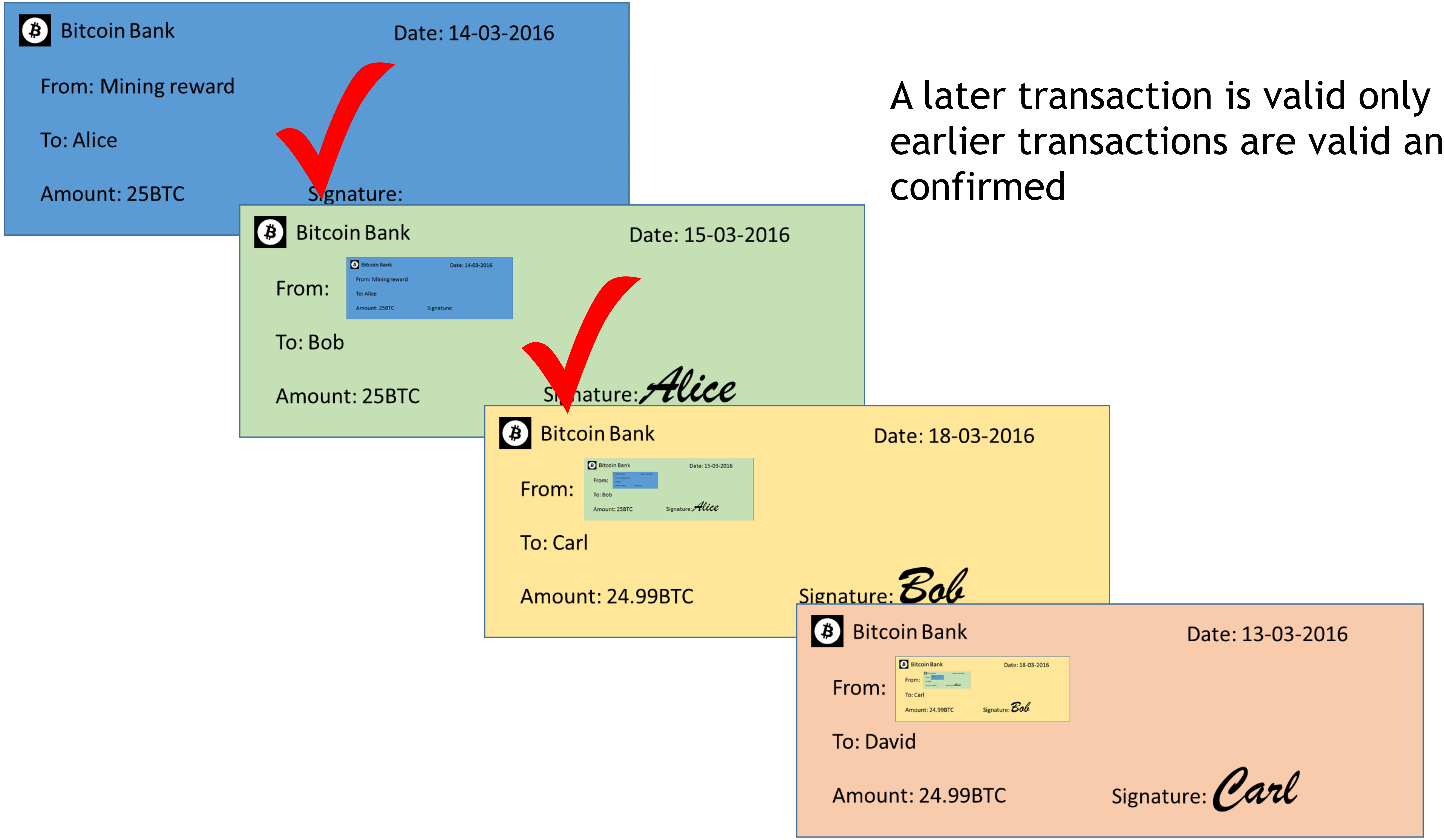
From: Bitcoin Bank Date: 18-03-2016 From: To: Carl Amount: 24.99BTC Signature: Bob

To: David

Amount: 24.99BTC Signature: Carl

A later transaction is valid only if the earlier transactions are valid and confirmed

# A chain of transactions



Bitcoin Bank
Date: 14-03-2016
From: Mining reward
To: Alice
Amount: 25BTC
Signature:

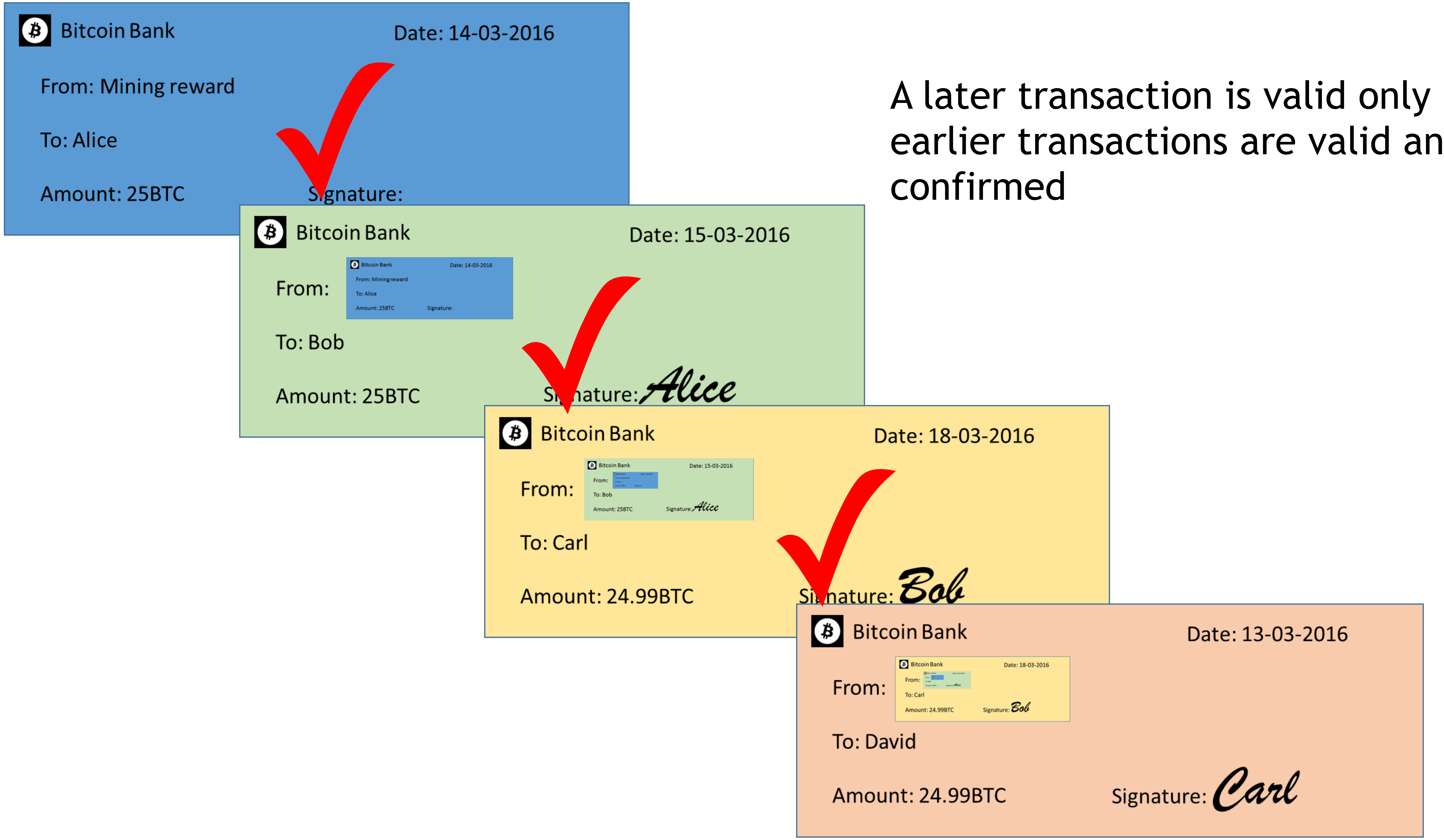
Bitcoin Bank
Date: 15-03-2016
From:
Bitcoin Bank
Date: 14-03-2016
From: Mining reward
To: Alice
Amount: 25BTC
Signature:
To: Bob
Amount: 25BTC
Signature: Alice

Bitcoin Bank
Date: 18-03-2016
From:
Bitcoin Bank
Date: 15-03-2016
From:
To: Bob
Amount: 25BTC
Signature: Alice
To: Carl
Amount: 24.99BTC
Signature: Bob

Bitcoin Bank
Date: 13-03-2016
From:
Bitcoin Bank
Date: 18-03-2016
From:
To: Carl
Amount: 24.99BTC
Signature: Bob
To: David
Amount: 24.99BTC
Signature: Carl

A later transaction is valid only if the earlier transactions are valid and confirmed

# A chain of transactions



Bitcoin Bank
Date: 14-03-2016
From: Mining reward
To: Alice
Amount: 25BTC
Signature:

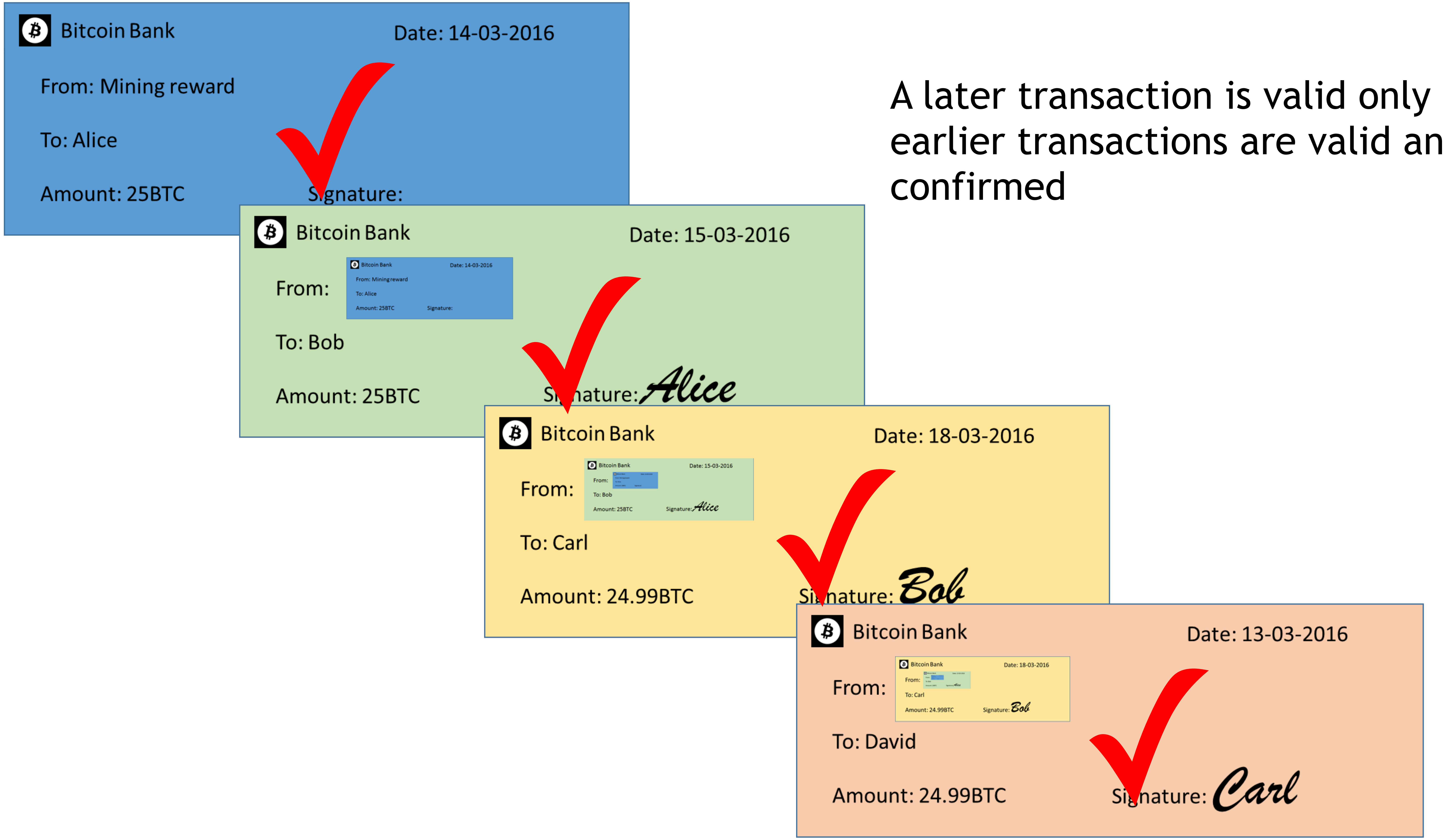
Bitcoin Bank
Date: 15-03-2016
From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Alice Amount: 25BTC Signature:
To: Bob
Amount: 25BTC
Signature: Alice

Bitcoin Bank
Date: 18-03-2016
From: Bitcoin Bank Date: 15-03-2016 From: To: Bob Amount: 25BTC Signature: Alice
To: Carl
Amount: 24.99BTC
Signature: Bob

Bitcoin Bank
Date: 13-03-2016
From: Bitcoin Bank Date: 18-03-2016 From: To: Carl Amount: 24.99BTC Signature: Bob
To: David
Amount: 24.99BTC
Signature: Carl

A later transaction is valid only if the earlier transactions are valid and confirmed

# A chain of transactions



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

Bitcoin Bank Date: 18-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

To: Bob

Amount: 25BTC Signature: Alice

To: Carl

Amount: 24.99BTC Signature: Bob

Bitcoin Bank Date: 13-03-2016

From:

Bitcoin Bank Date: 18-03-2016

From:

To: Carl

Amount: 24.99BTC Signature: Bob

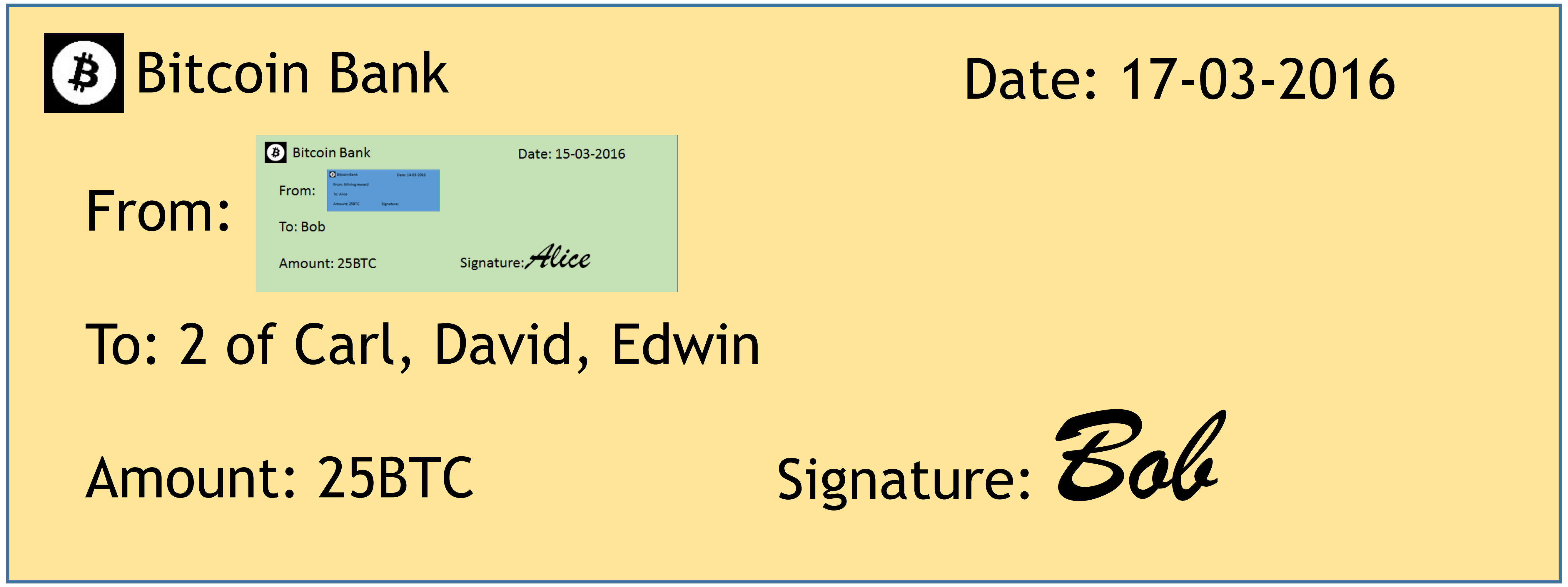
To: David

Amount: 24.99BTC Signature: Carl

A later transaction is valid only if the earlier transactions are valid and confirmed

# Bitcoin transactions are very flexible

m-of-n multi-signature
e.g. 2-of-3 multi-sig



Bitcoin Bank Date: 17-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

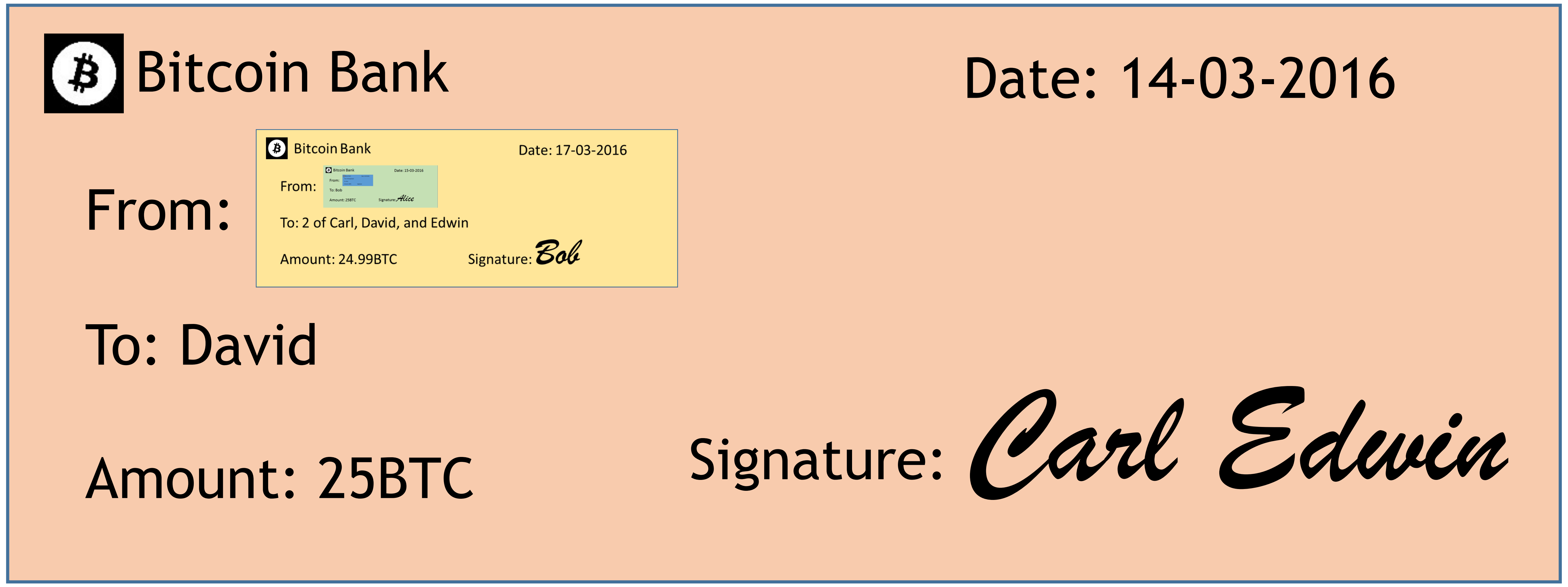
Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

To: 2 of Carl, David, Edwin

Amount: 25BTC Signature: Bob



Bitcoin Bank Date: 14-03-2016

From:

Bitcoin Bank Date: 17-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

To: Bob

Amount: 25BTC Signature: Alice

To: 2 of Carl, David, and Edwin

Amount: 24.99BTC Signature: Bob

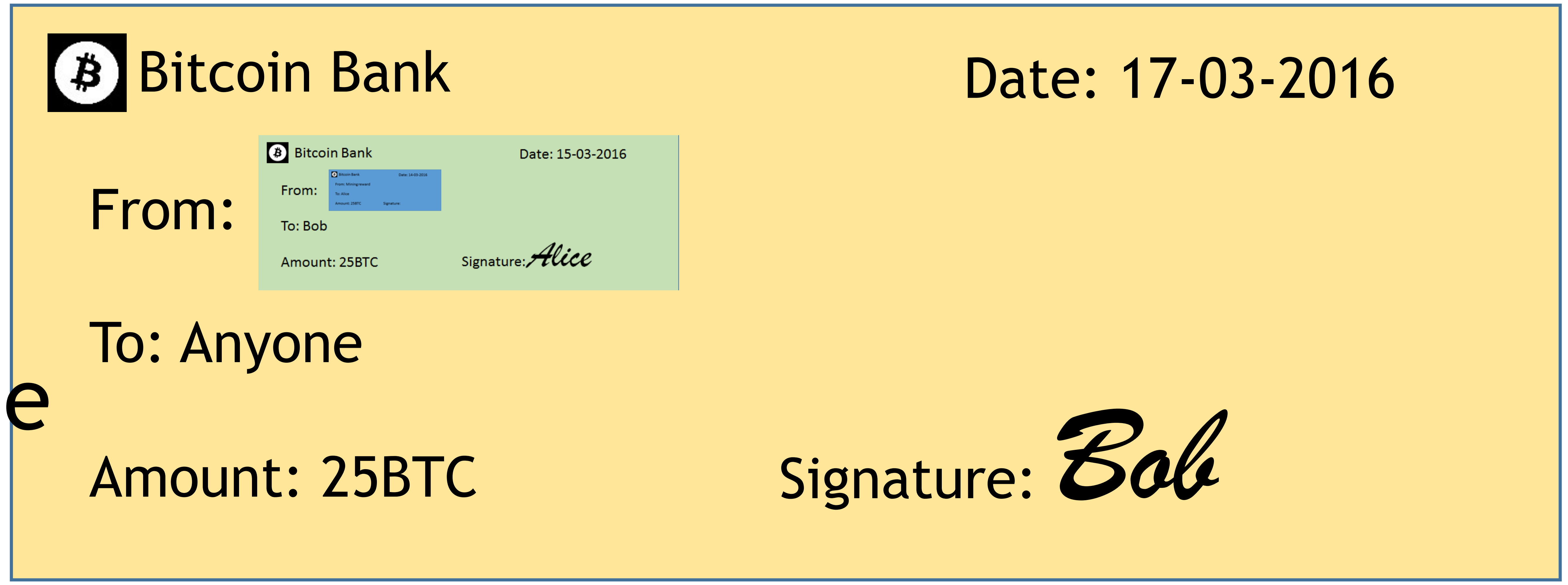
To: David

Amount: 25BTC Signature: Carl Edwin

# Bitcoin transactions are very flexible

“Anyone-can-spend”

Payable to bearer cheque



Bitcoin Bank Date: 17-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

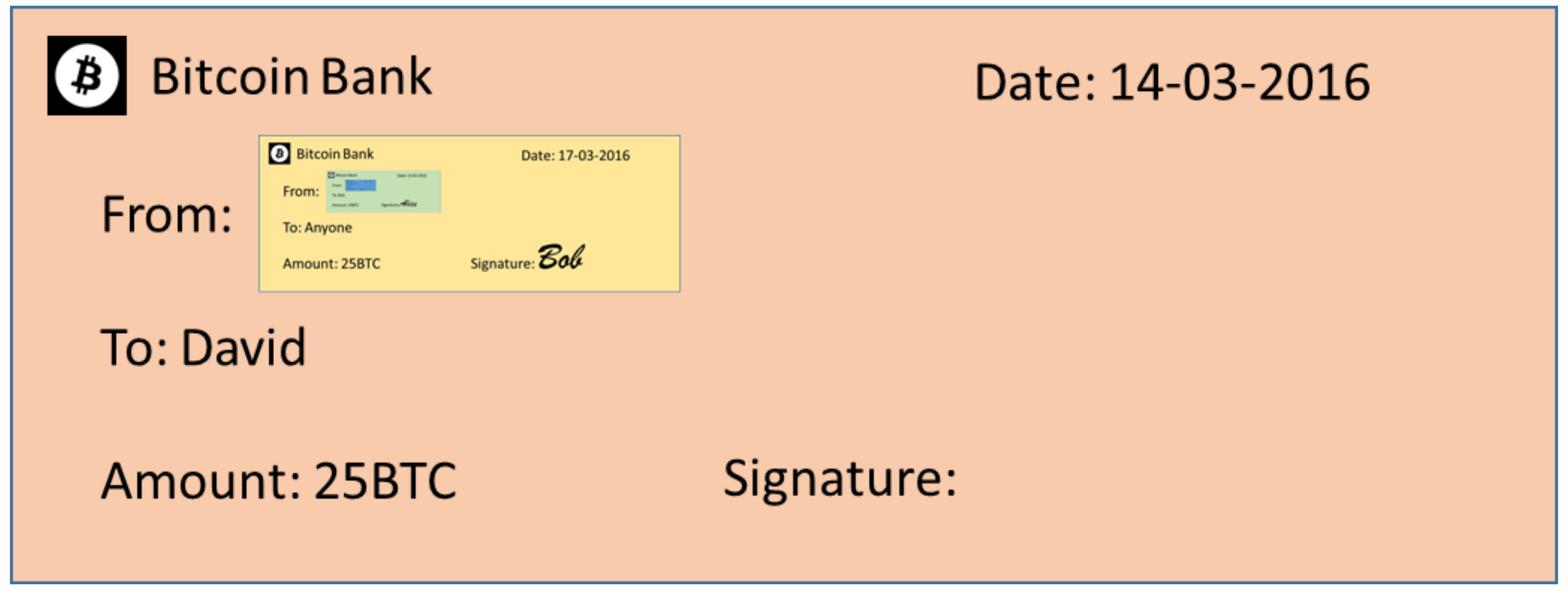
Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

To: Anyone

Amount: 25BTC Signature: Bob



Bitcoin Bank Date: 14-03-2016

From:

Bitcoin Bank Date: 17-03-2016

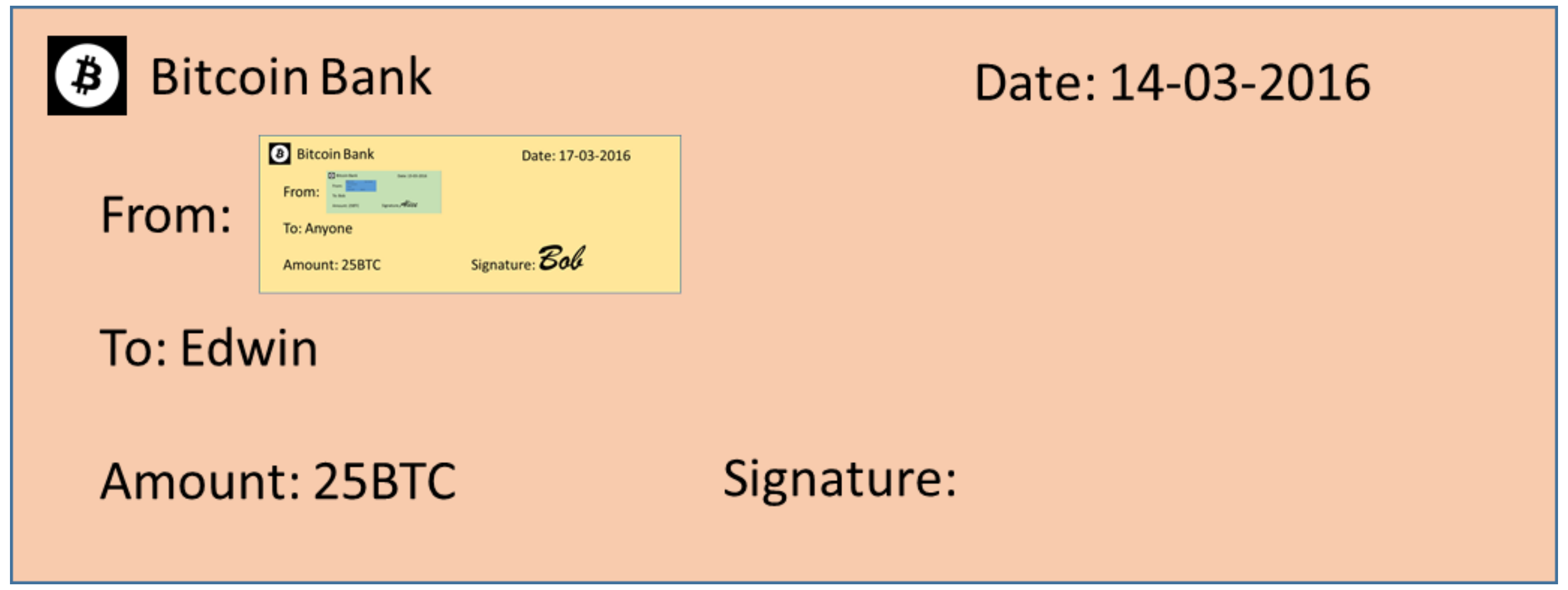
From:

To: Anyone

Amount: 25BTC Signature: Bob

To: David

Amount: 25BTC Signature:



Bitcoin Bank Date: 14-03-2016

From:

Bitcoin Bank Date: 17-03-2016

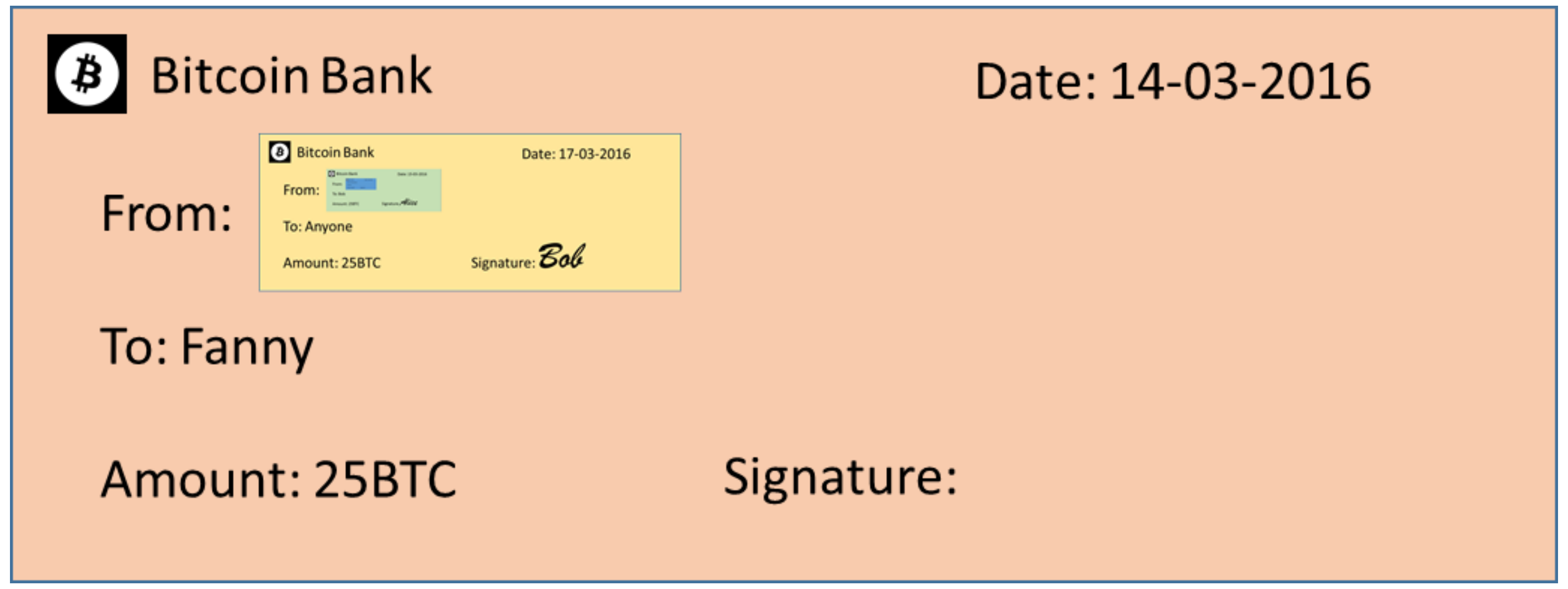
From:

To: Anyone

Amount: 25BTC Signature: Bob

To: Edwin

Amount: 25BTC Signature:



Bitcoin Bank Date: 14-03-2016

From:

Bitcoin Bank Date: 17-03-2016

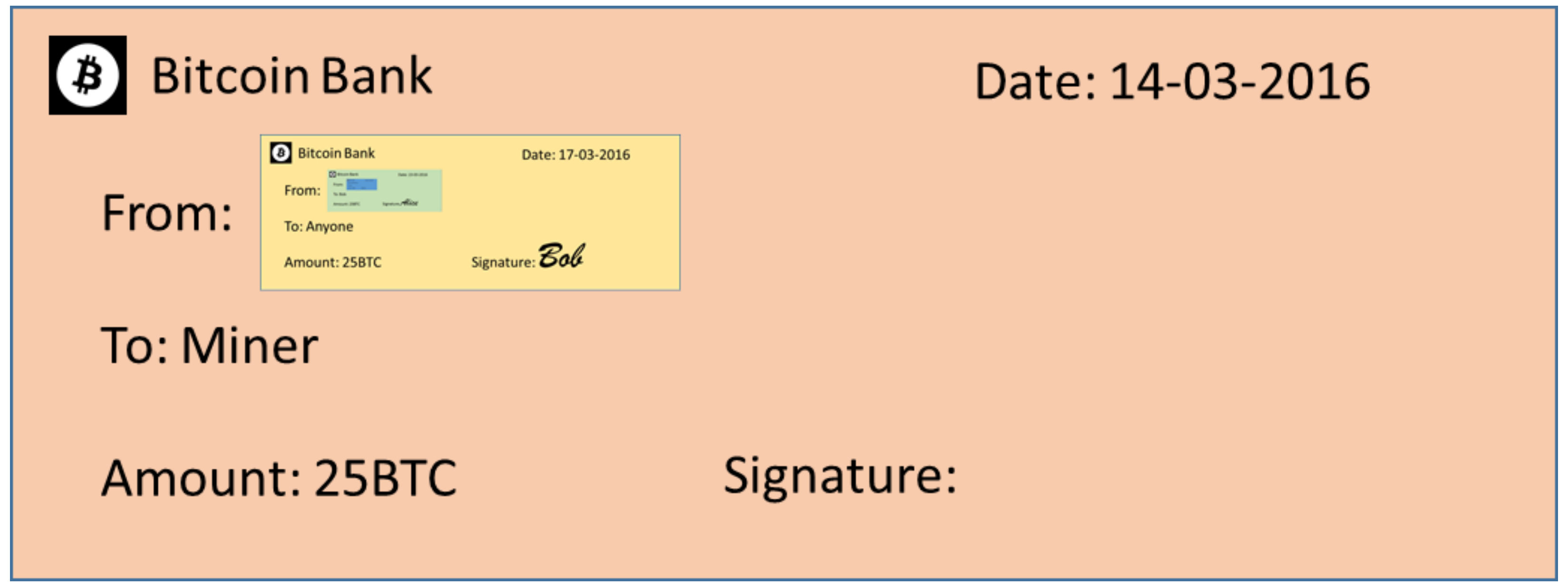
From:

To: Anyone

Amount: 25BTC Signature: Bob

To: Fanny

Amount: 25BTC Signature:



Bitcoin Bank Date: 14-03-2016

From:

Bitcoin Bank Date: 17-03-2016

From:

To: Anyone

Amount: 25BTC Signature: Bob

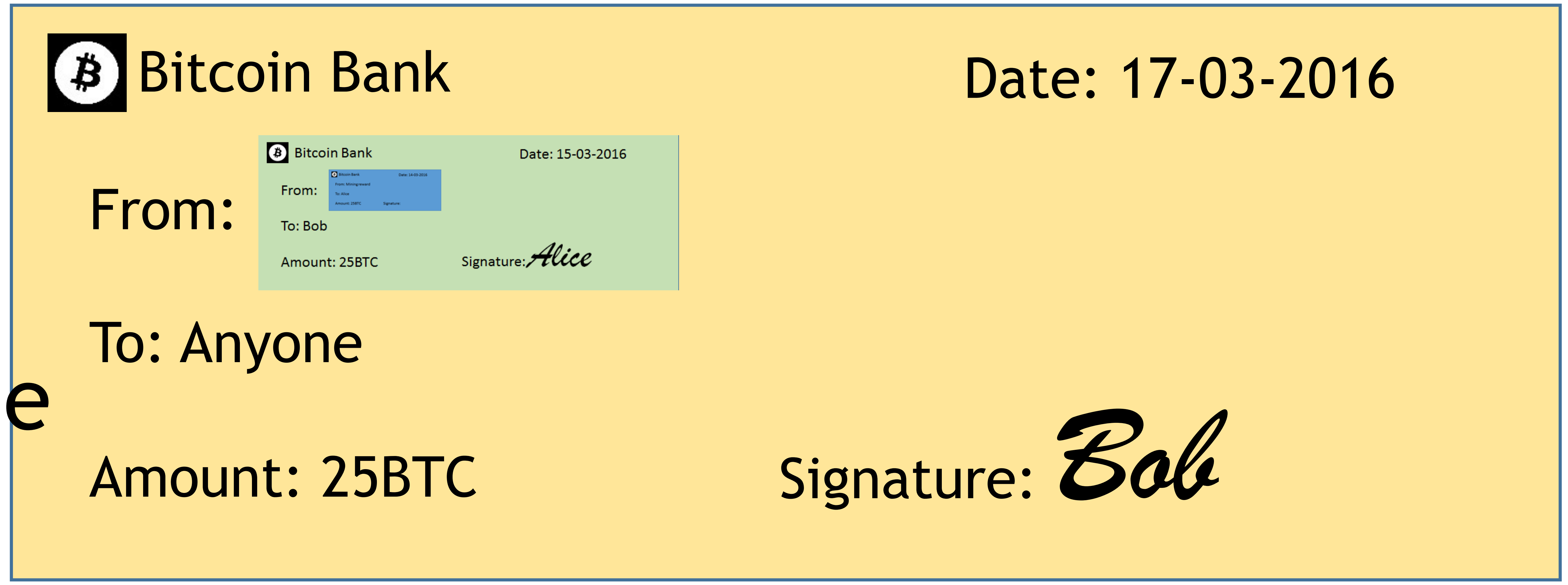
To: Miner

Amount: 25BTC Signature:

# Bitcoin transactions are very flexible

"Anyone-can-spend"

Payable to bearer cheque



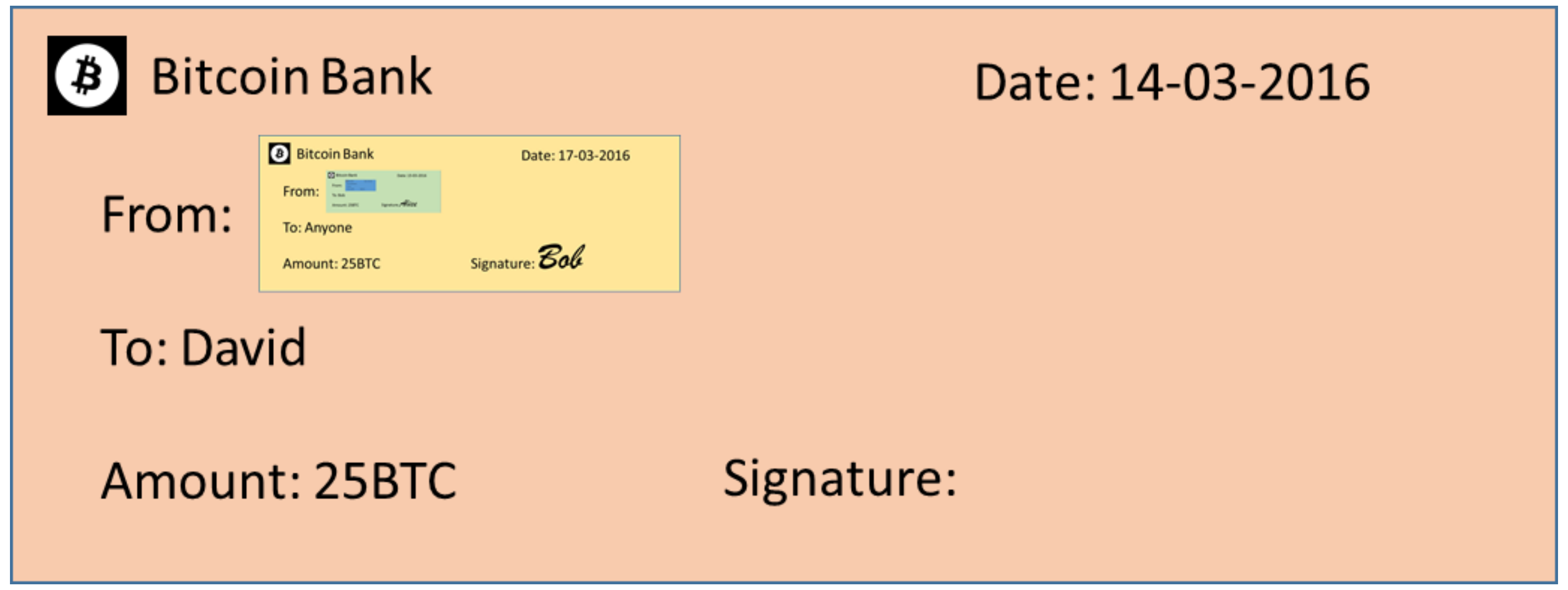
Bitcoin Bank Date: 17-03-2016

From:

> Bitcoin Bank Date: 15-03-2016
>
> From:
>
> To: Bob
>
> Amount: 25BTC Signature: Alice

To: Anyone

Amount: 25BTC Signature: Bob



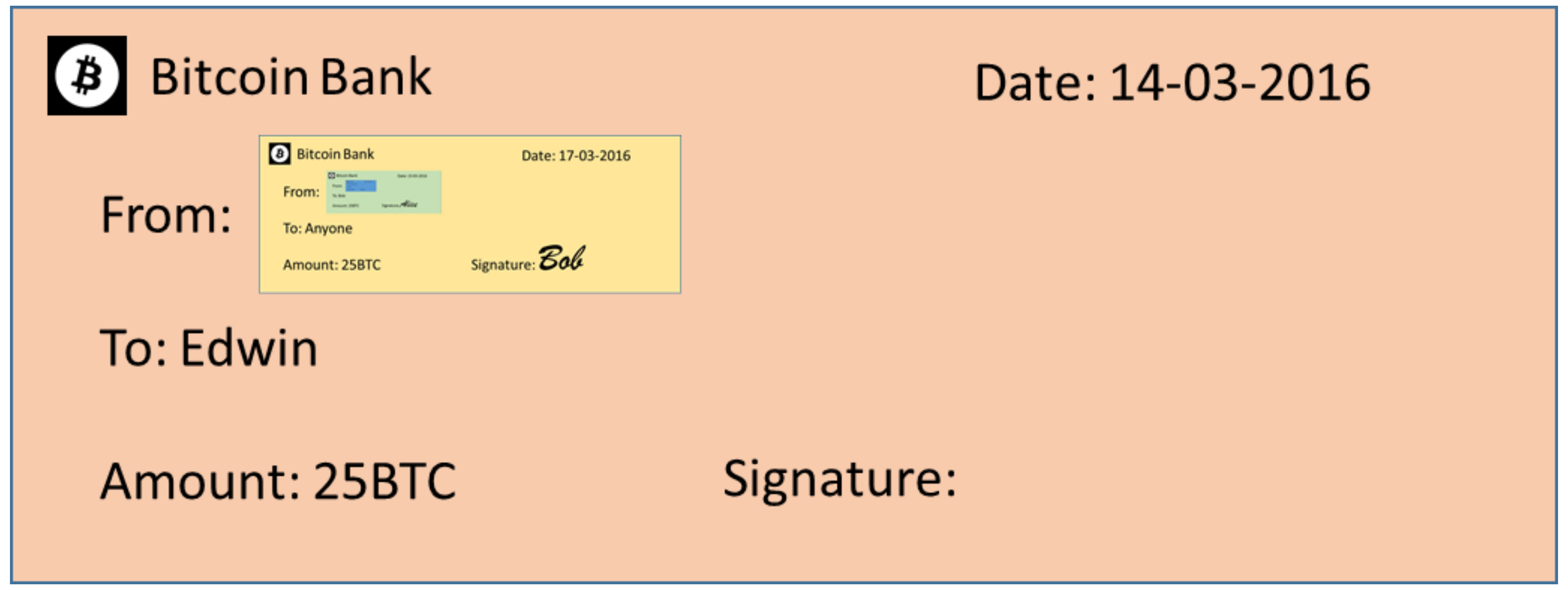
Bitcoin Bank Date: 14-03-2016

From:

> Bitcoin Bank Date: 17-03-2016
>
> From:
>
> To: Anyone
>
> Amount: 25BTC Signature: Bob

To: David

Amount: 25BTC Signature:



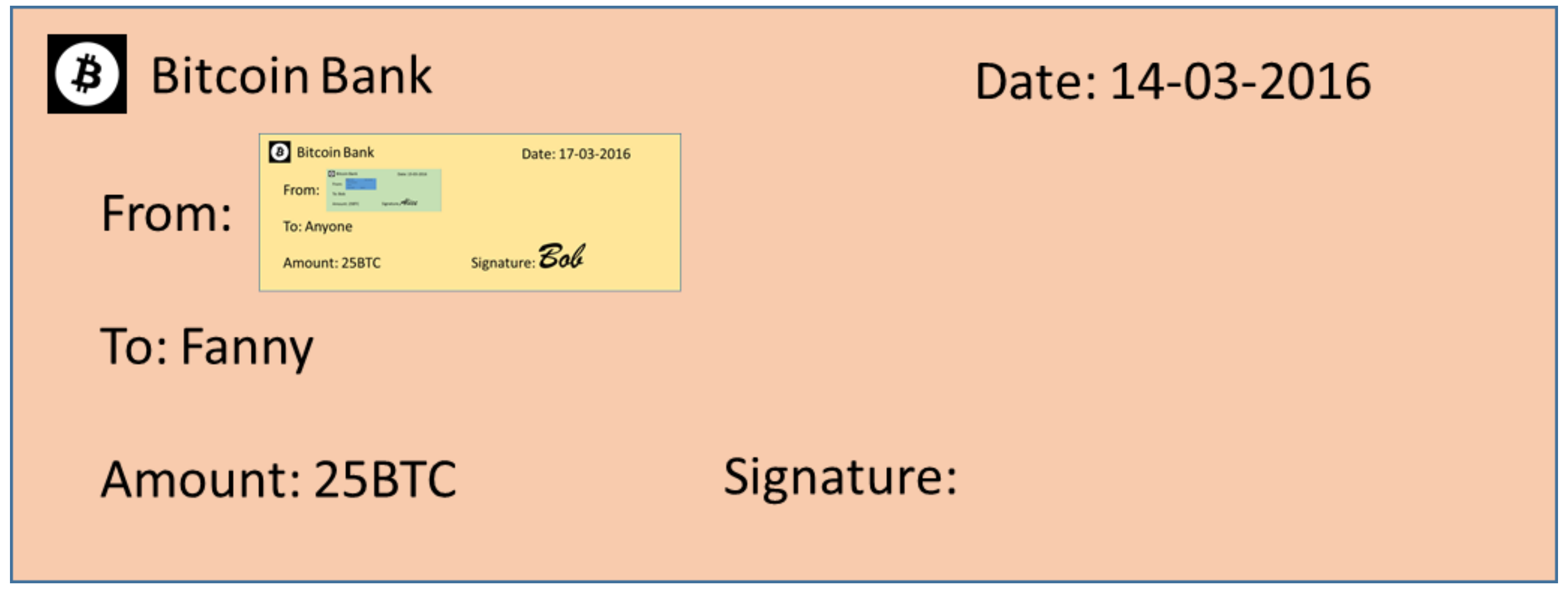
Bitcoin Bank Date: 14-03-2016

From:

> Bitcoin Bank Date: 17-03-2016
>
> From:
>
> To: Anyone
>
> Amount: 25BTC Signature: Bob

To: Edwin

Amount: 25BTC Signature:



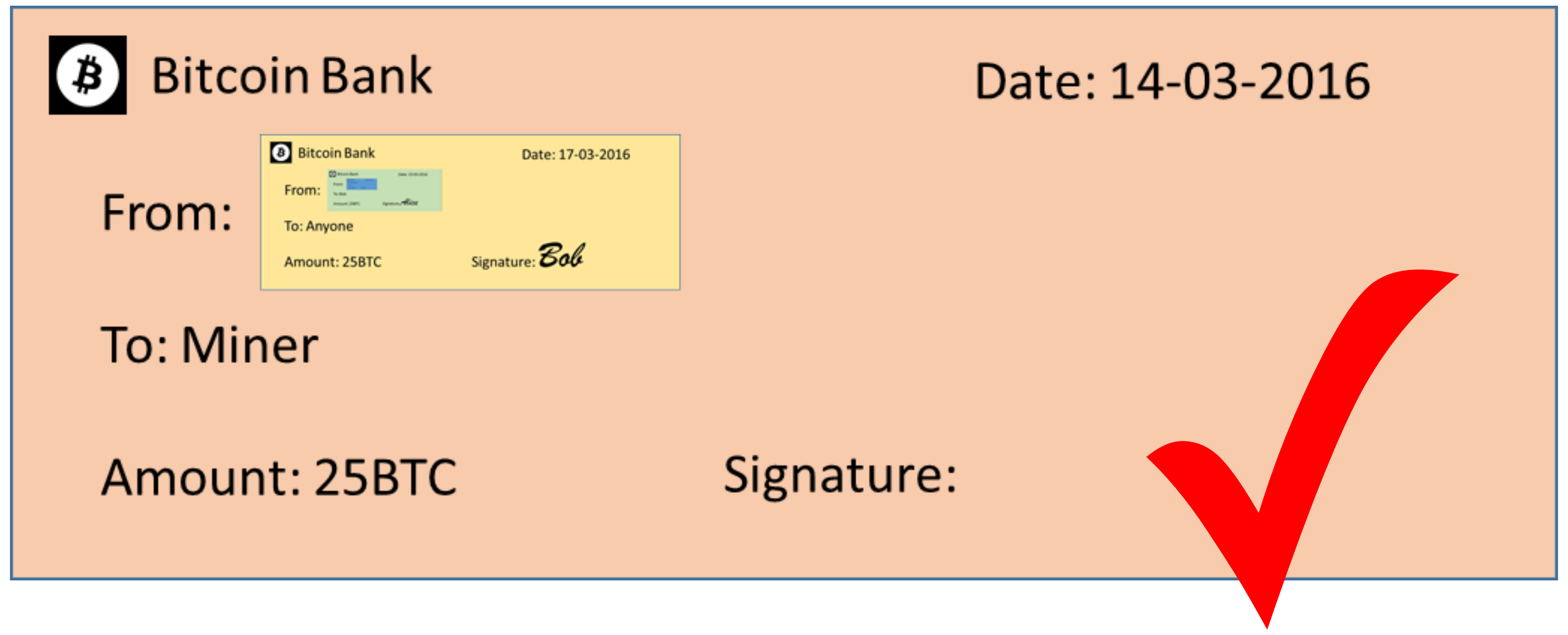
Bitcoin Bank Date: 14-03-2016

From:

> Bitcoin Bank Date: 17-03-2016
>
> From:
>
> To: Anyone
>
> Amount: 25BTC Signature: Bob

To: Fanny

Amount: 25BTC Signature:



Bitcoin Bank Date: 14-03-2016

From:

> Bitcoin Bank Date: 17-03-2016
>
> From:
>
> To: Anyone
>
> Amount: 25BTC Signature: Bob

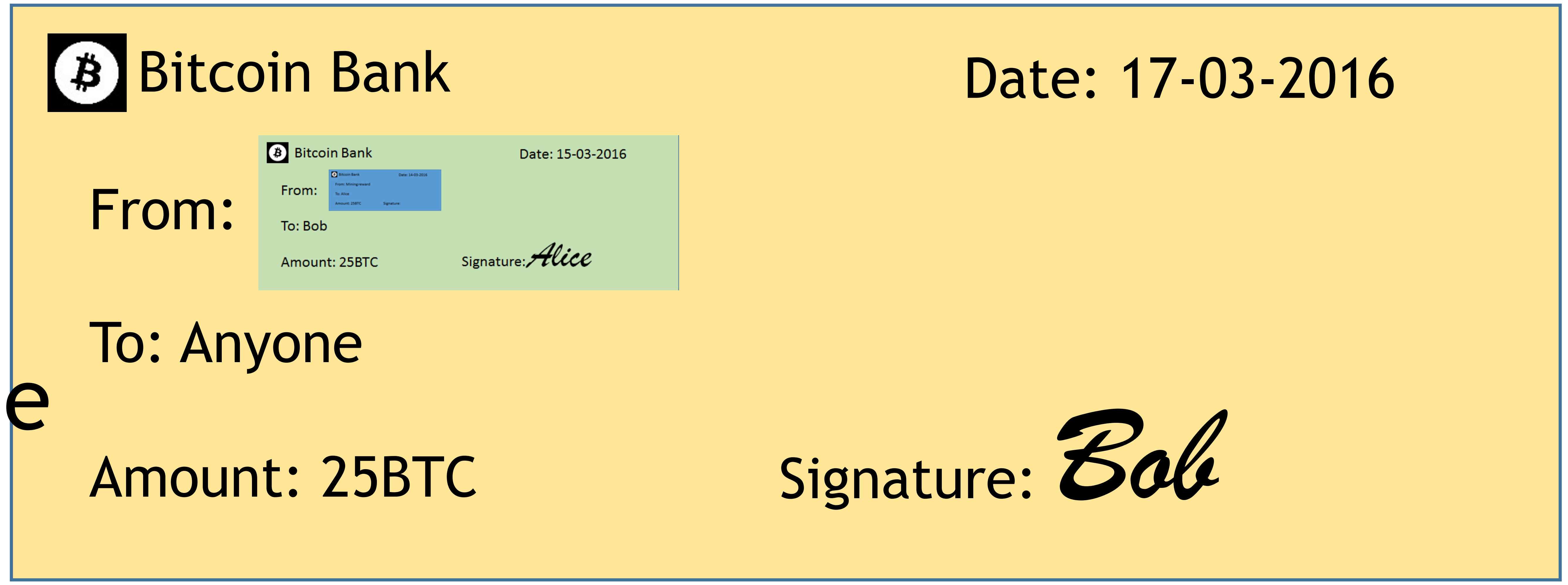
To: Miner

Amount: 25BTC Signature: ✓

# Bitcoin transactions are very flexible

“Anyone-can-spend”

Payable to bearer cheque



Bitcoin Bank

Date: 17-03-2016

From:

Bitcoin Bank

Date: 15-03-2016

From:

To: Bob

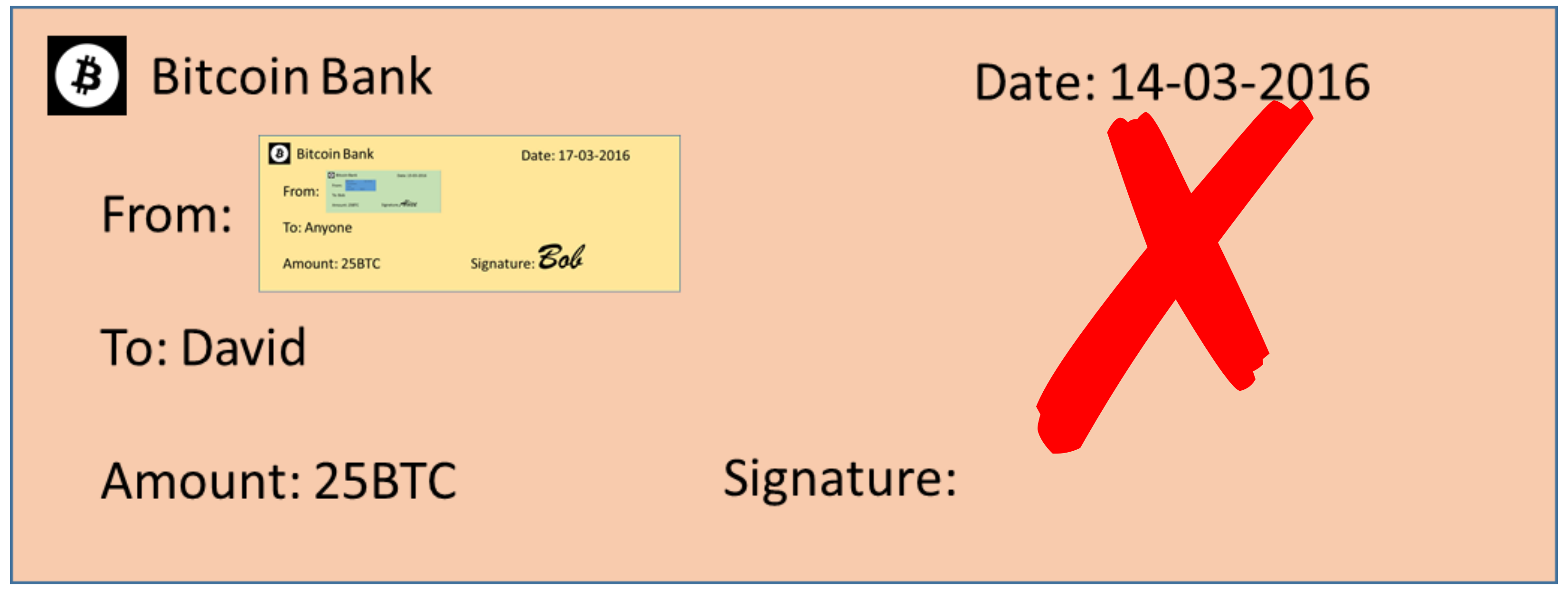
Amount: 25BTC

Signature: Alice

To: Anyone

Amount: 25BTC

Signature: Bob



Bitcoin Bank

Date: 14-03-2016

From:

Bitcoin Bank

Date: 17-03-2016

From:

To: Anyone

Amount: 25BTC

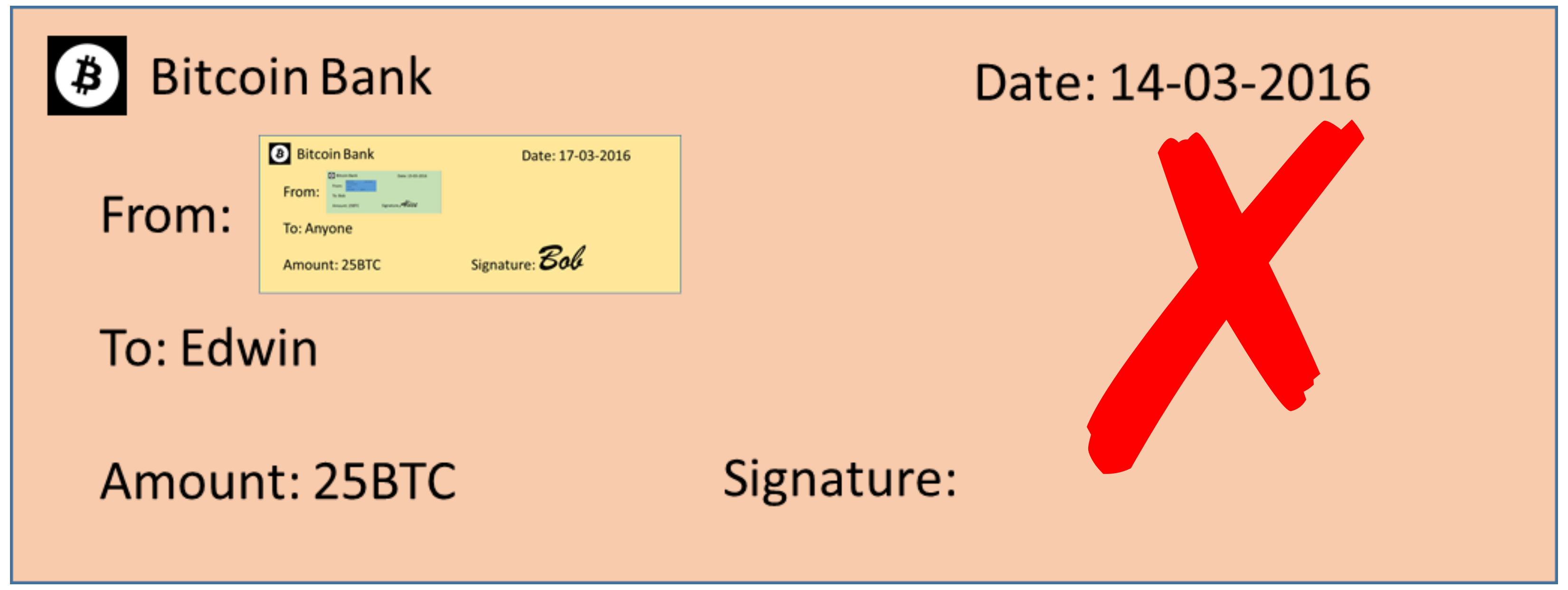
Signature: Bob

To: David

Amount: 25BTC

Signature:

✗



Bitcoin Bank

Date: 14-03-2016

From:

Bitcoin Bank

Date: 17-03-2016

From:

To: Anyone

Amount: 25BTC

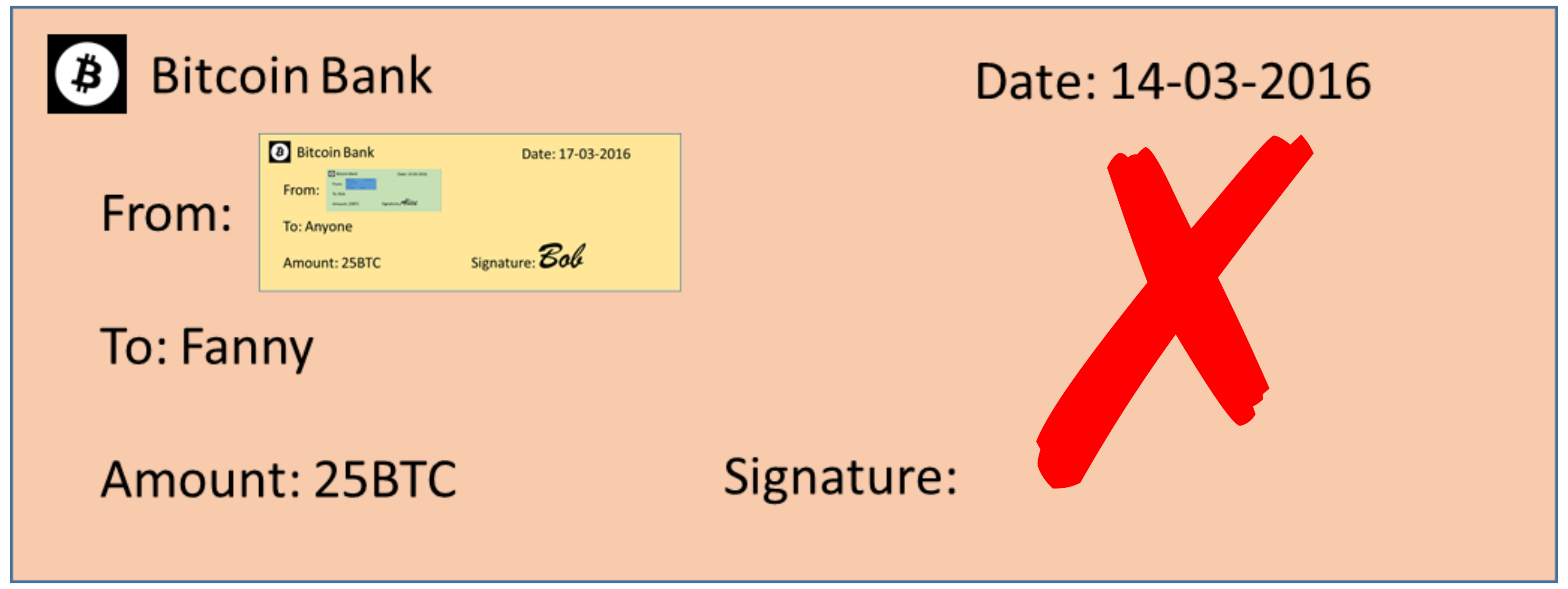
Signature: Bob

To: Edwin

Amount: 25BTC

Signature:

✗



Bitcoin Bank

Date: 14-03-2016

From:

Bitcoin Bank

Date: 17-03-2016

From:

To: Anyone

Amount: 25BTC

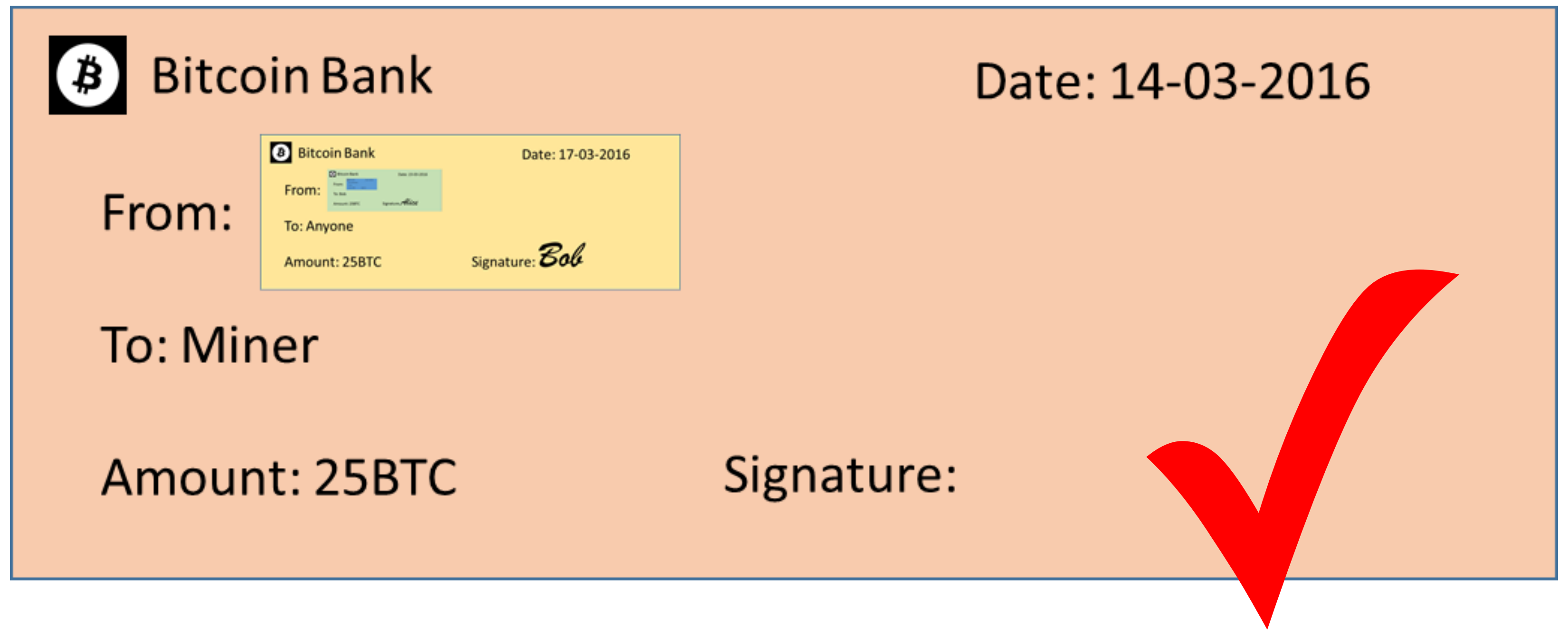
Signature: Bob

To: Fanny

Amount: 25BTC

Signature:

✗



Bitcoin Bank

Date: 14-03-2016

From:

Bitcoin Bank

Date: 17-03-2016

From:

To: Anyone

Amount: 25BTC

Signature: Bob

To: Miner

Amount: 25BTC

Signature:

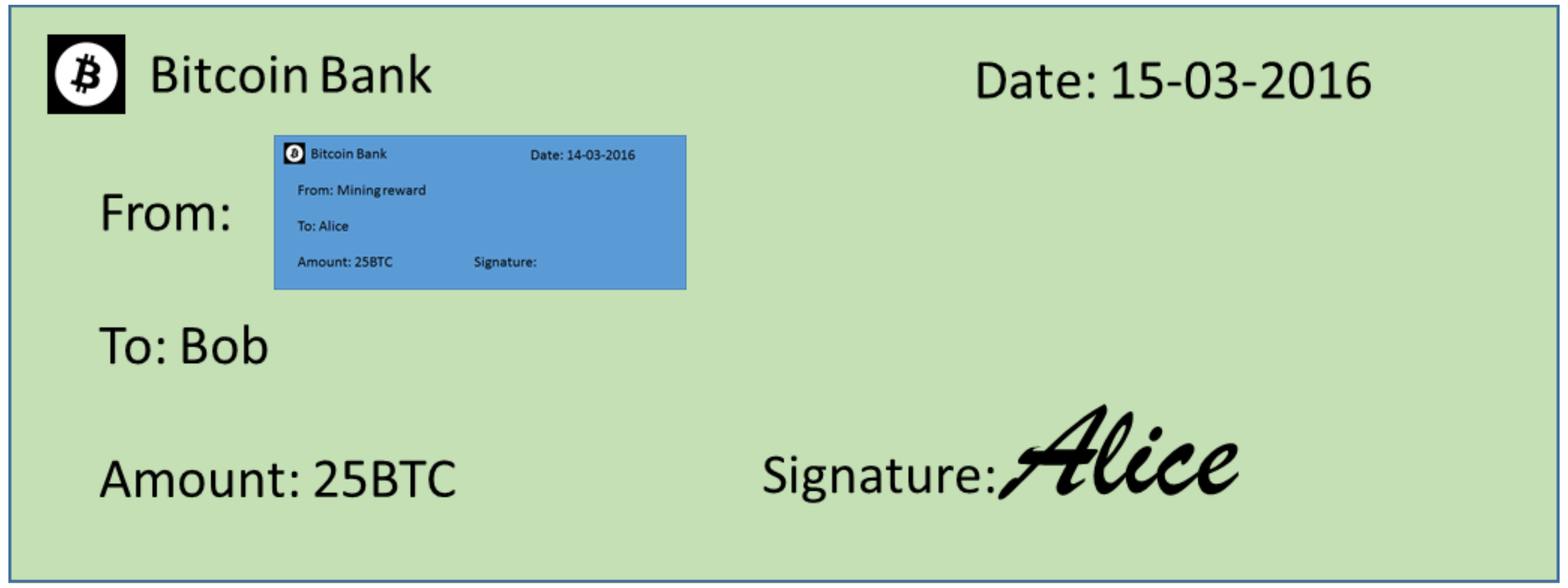
✓

# Transaction malleability

- The transaction ID may be changed by the payer or any other people before the transaction is confirmed by a miner
  - The “appearance” of a cheque may be changed by the payer or any other people before the cheque is confirmed by the Bitcoin Bank
- Malleability by the payer (Double spending)
  - Malicious or legitimate
  - NOT fixable. The payer will always have the ability to change the txid until the tx is confirmed -> Unconfirmed tx is not safe unless you really trust the payer
- Malleability by any other people (Involuntary)
  - Signature malleability
  - Possible due to the mathematical property of the digital signature, and the flexibility of Bitcoin script language

# Signature malleability

All the following cheques are valid but not more than one might be confirmed



Bitcoin Bank

Date: 15-03-2016

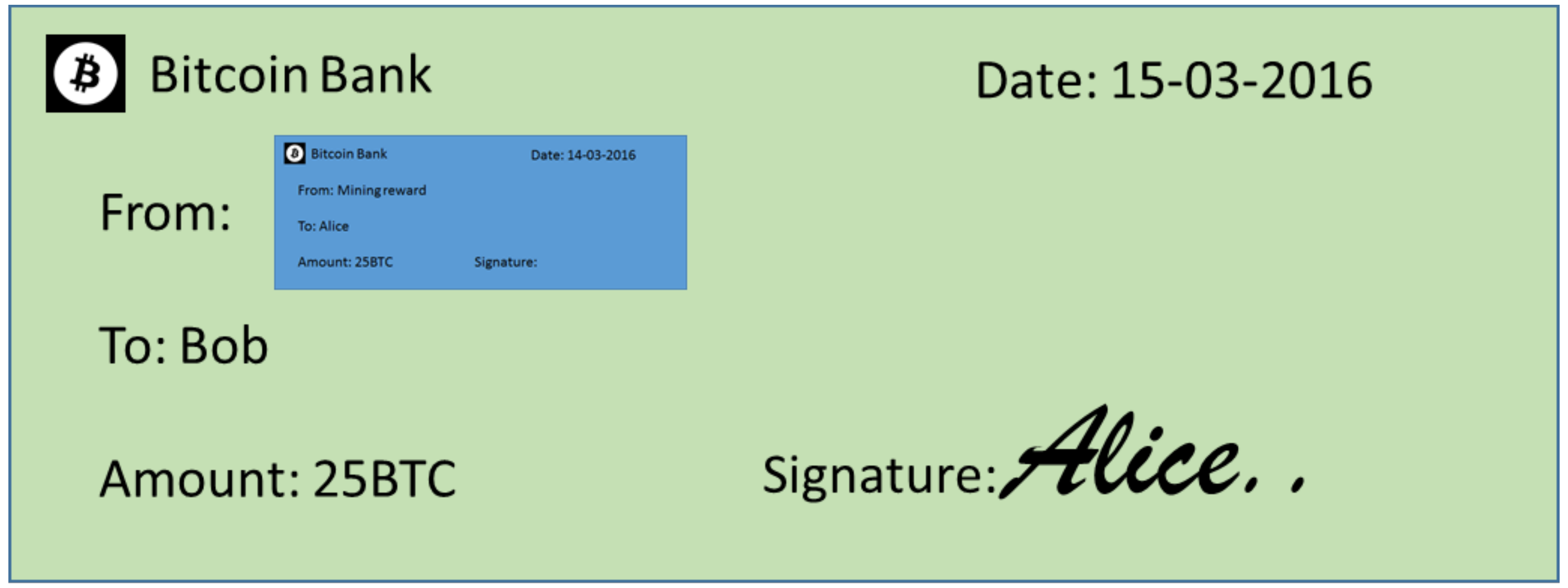
From:

Bitcoin Bank Date: 14-03-2016
From: Mining reward
To: Alice
Amount: 25BTC Signature:

To: Bob

Amount: 25BTC

Signature: Alice



Bitcoin Bank

Date: 15-03-2016

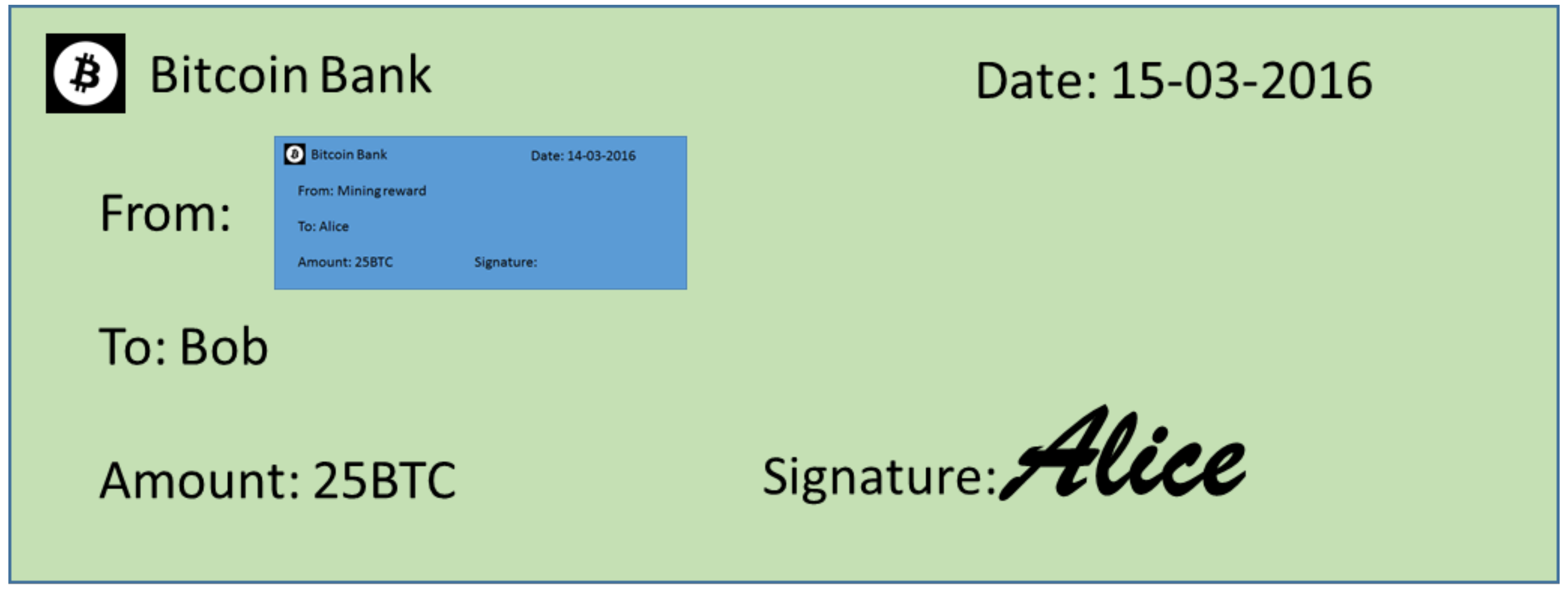
From:

Bitcoin Bank Date: 14-03-2016
From: Mining reward
To: Alice
Amount: 25BTC Signature:

To: Bob

Amount: 25BTC

Signature: Alice, ,



Bitcoin Bank

Date: 15-03-2016

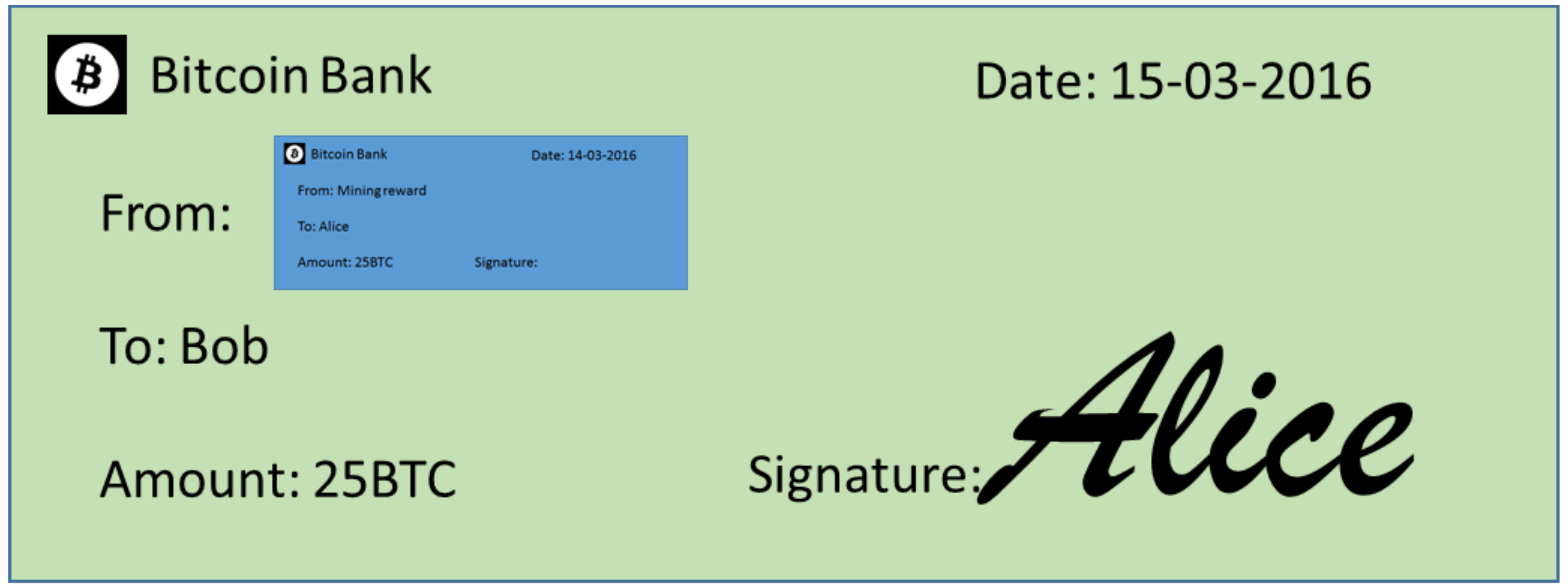
From:

Bitcoin Bank Date: 14-03-2016
From: Mining reward
To: Alice
Amount: 25BTC Signature:

To: Bob

Amount: 25BTC

Signature: Alice



Bitcoin Bank

Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016
From: Mining reward
To: Alice
Amount: 25BTC Signature:

To: Bob

Amount: 25BTC

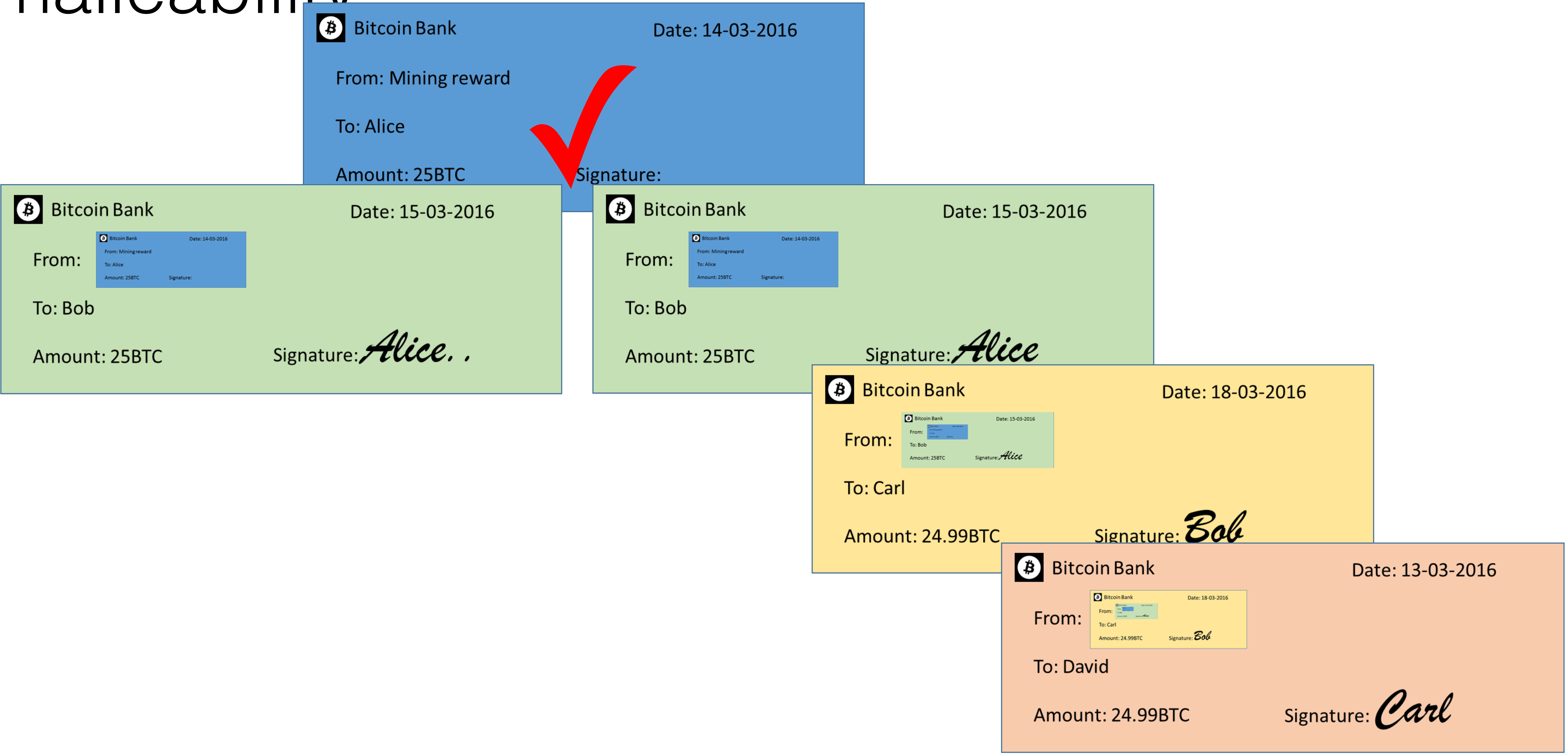
Signature: Alice

# Why transaction malleability is bad?

1. The Tx ID is not final until the transaction is confirmed
   - Tx ID usually won't change in traditional banking system
   - MtGox blamed tx malleability for loss of 850,000BTC
2. A chain of unconfirmed transactions is not safe
   - If the TxID of an earlier transaction in a chain is changed and confirmed, all subsequent transactions in the chain become invalid
3. It is not possible to construct a chain of transactions, without first signing an earlier transaction in the chain
   - To buy an apartment, you have to irreversibly pay the deposit BEFORE you sign ANY contract

- Even if you fully trust your counterparty, the problems 1 and 2 still persist due to involuntary malleability.

# Breaking unconfirmed tx chain with tx malleability



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Alice Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice. ,

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Alice Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

Bitcoin Bank Date: 18-03-2016

From: Bitcoin Bank Date: 15-03-2016 From: To: Bob Amount: 25BTC Signature: Alice

To: Carl

Amount: 24.99BTC Signature: Bob

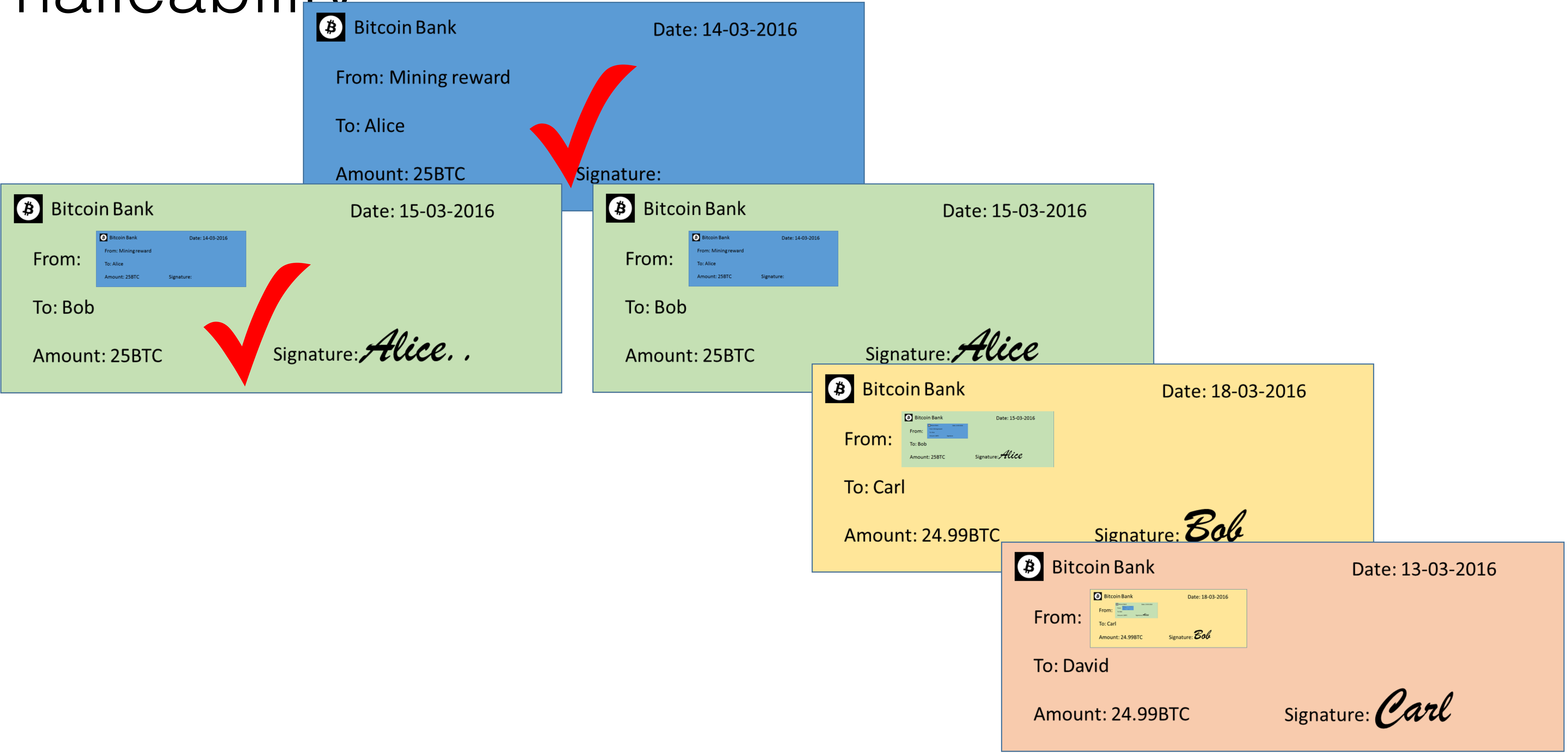
Bitcoin Bank Date: 13-03-2016

From: Bitcoin Bank Date: 18-03-2016 From: To: Carl Amount: 24.99BTC Signature: Bob

To: David

Amount: 24.99BTC Signature: Carl

# Breaking unconfirmed tx chain with tx malleability



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Alice Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice. ,

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Alice Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

Bitcoin Bank Date: 18-03-2016

From: Bitcoin Bank Date: 15-03-2016 From: To: Bob Amount: 25BTC Signature: Alice

To: Carl

Amount: 24.99BTC Signature: Bob

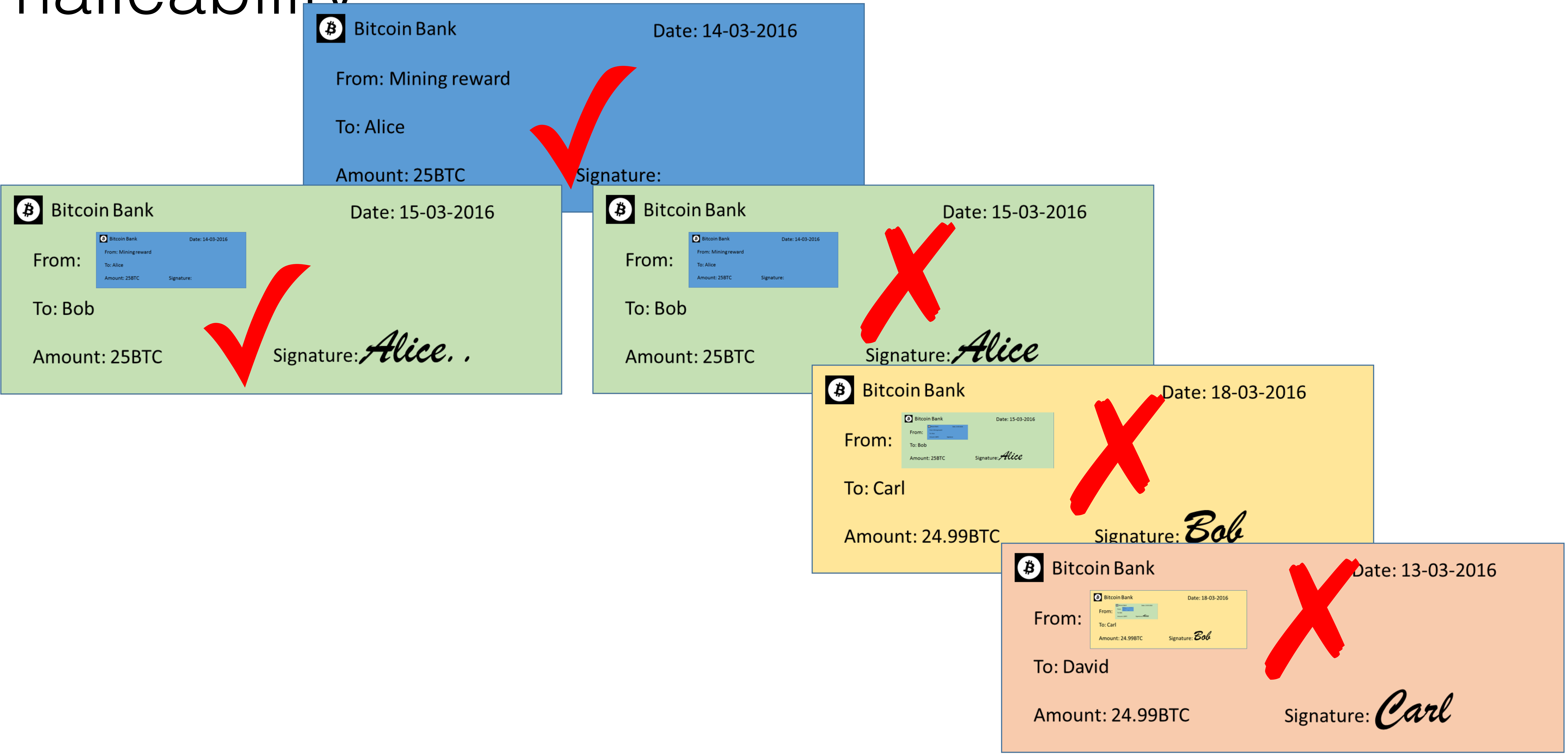
Bitcoin Bank Date: 13-03-2016

From: Bitcoin Bank Date: 18-03-2016 From: To: Carl Amount: 24.99BTC Signature: Bob

To: David

Amount: 24.99BTC Signature: Carl

# Breaking unconfirmed tx chain with tx malleability



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

✓

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Alice Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice. ,

✓

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Alice Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

✗

Bitcoin Bank Date: 18-03-2016

From: Bitcoin Bank Date: 15-03-2016 From: To: Bob Amount: 25BTC Signature: Alice

To: Carl

Amount: 24.99BTC Signature: Bob

✗

Bitcoin Bank Date: 13-03-2016

From: Bitcoin Bank Date: 18-03-2016 From: To: Carl Amount: 24.99BTC Signature: Bob

To: David

Amount: 24.99BTC Signature: Carl

✗

# Creating a chain of transactions

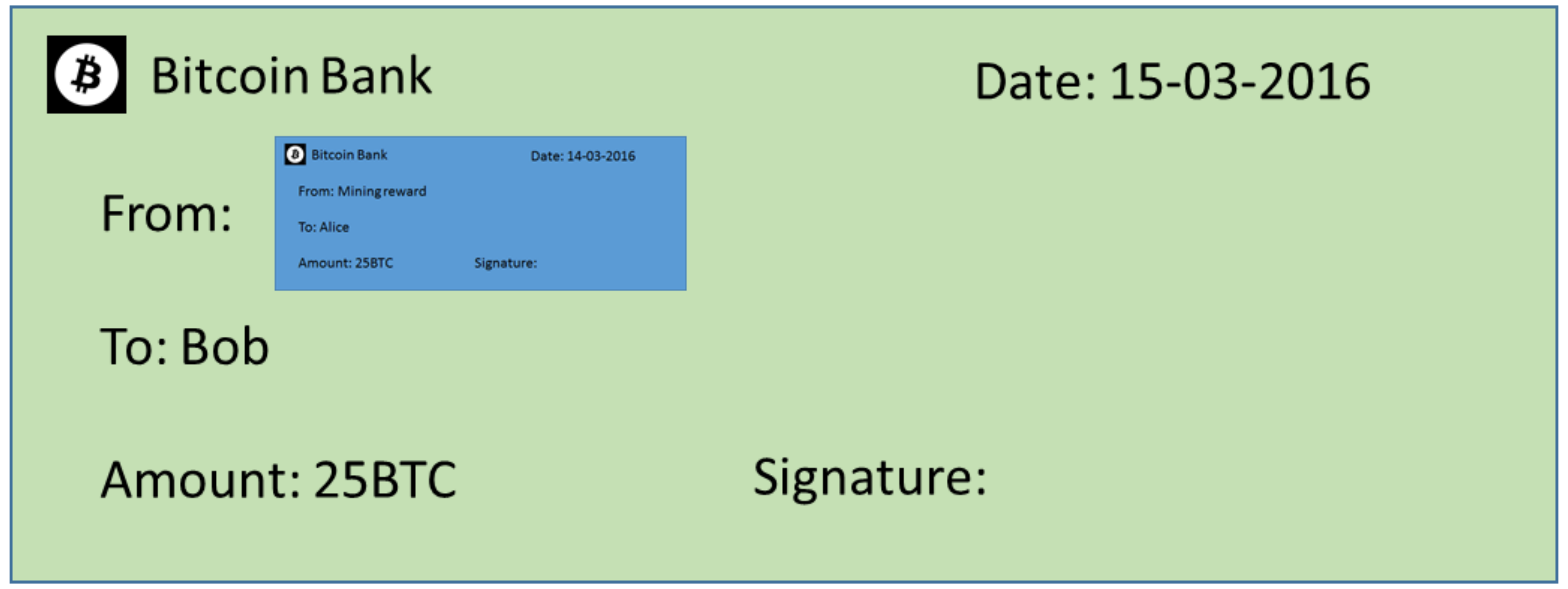
Scenario: Alice is paying 25BTC to Bob, but only if Bob agrees to pay 24.99BTC to Carl later.

Could she do it safely?

# Creating a chain of transactions

## Method 1

- Alice creates the green cheque but not sign it



Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

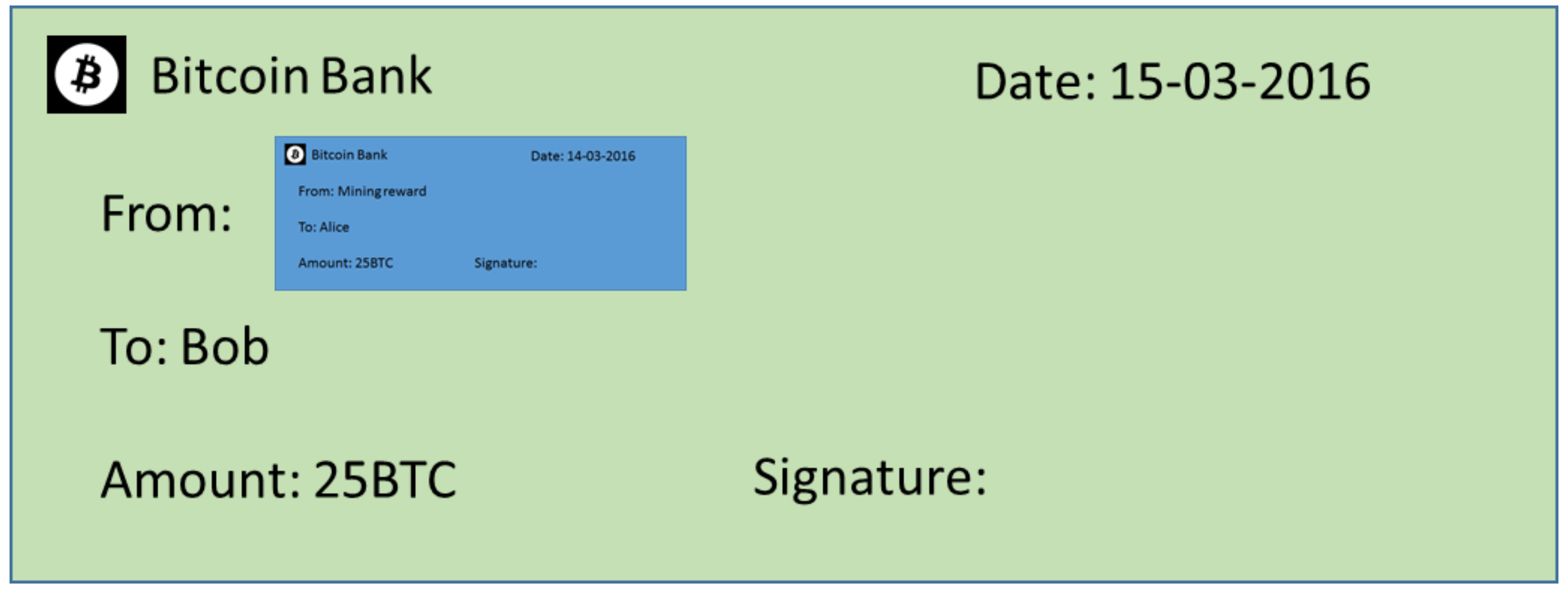
To: Bob

Amount: 25BTC Signature:

# Creating a chain of transactions

## Method 1

- Alice creates the green cheque but not sign it
- Bob creates the yellow cheque and signs it



Bitcoin Bank

Date: 15-03-2016

From:

Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Alice

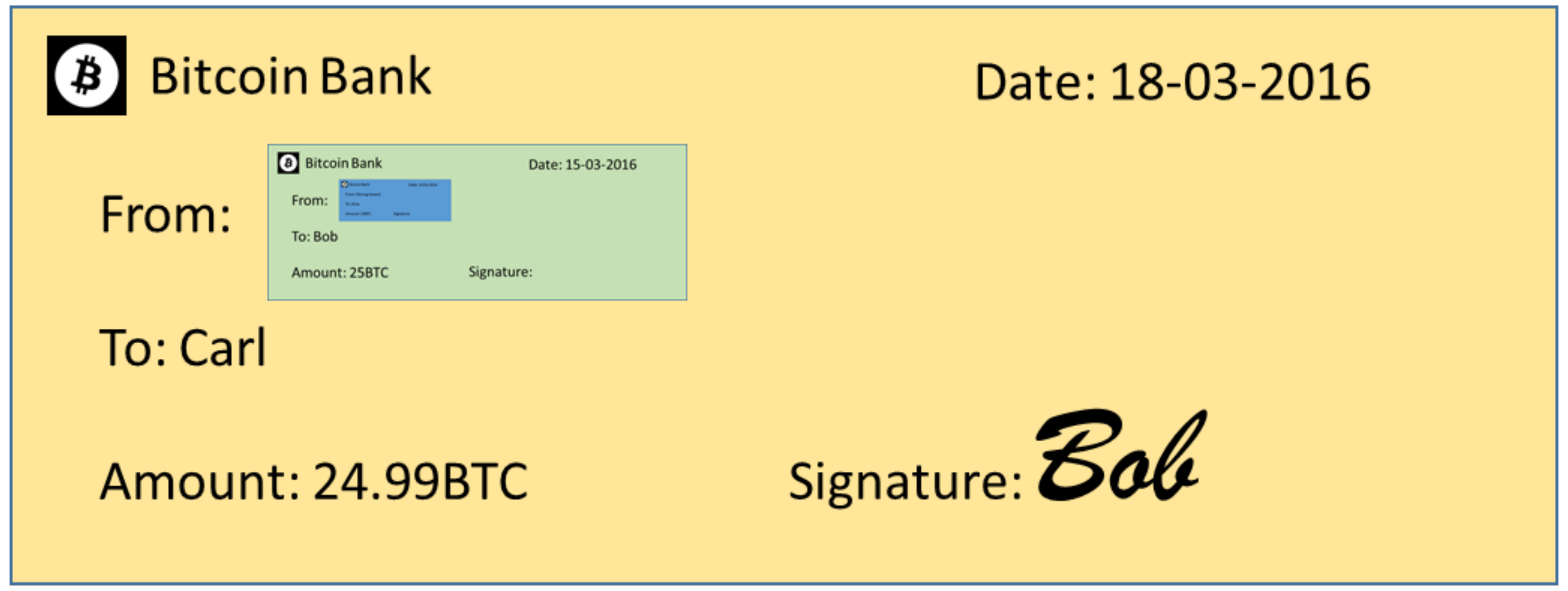
Amount: 25BTC

Signature:

To: Bob

Amount: 25BTC

Signature:



Bitcoin Bank

Date: 18-03-2016

From:

Bitcoin Bank

Date: 15-03-2016

From:

To: Bob

Amount: 25BTC

Signature:

To: Carl

Amount: 24.99BTC

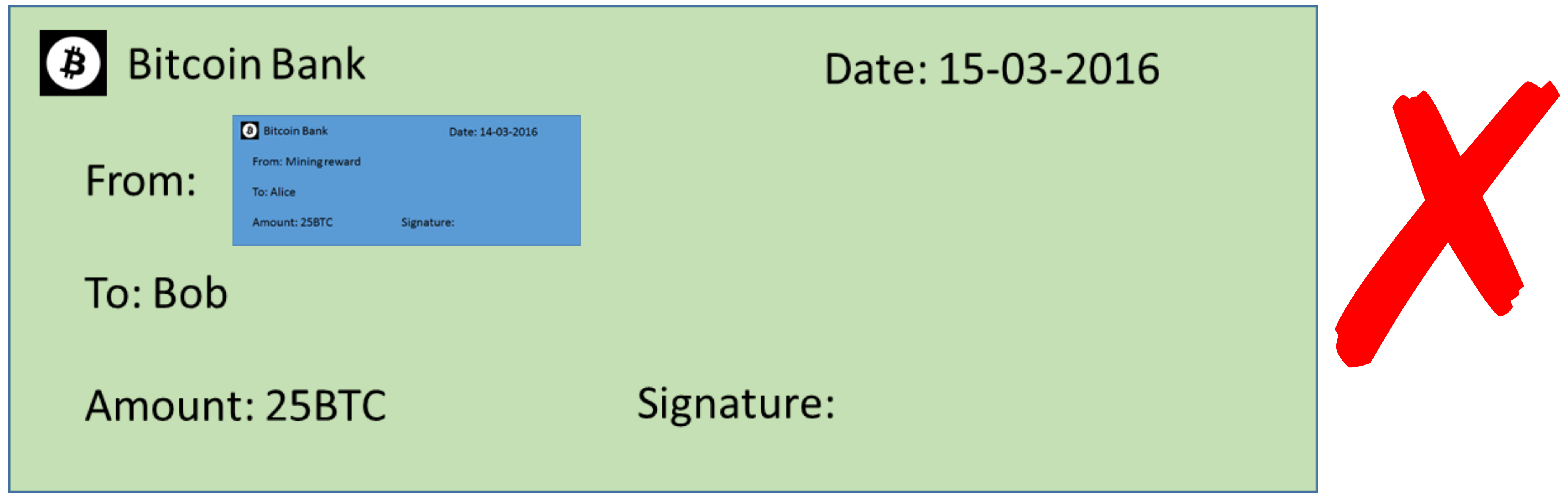
Signature: Bob

# Creating a chain of transactions

## Method 1

- Alice creates the green cheque but not sign it
- Bob creates the yellow cheque and signs it

- Since the green cheque has no signature and is invalid, the yellow cheque is also invalid



Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

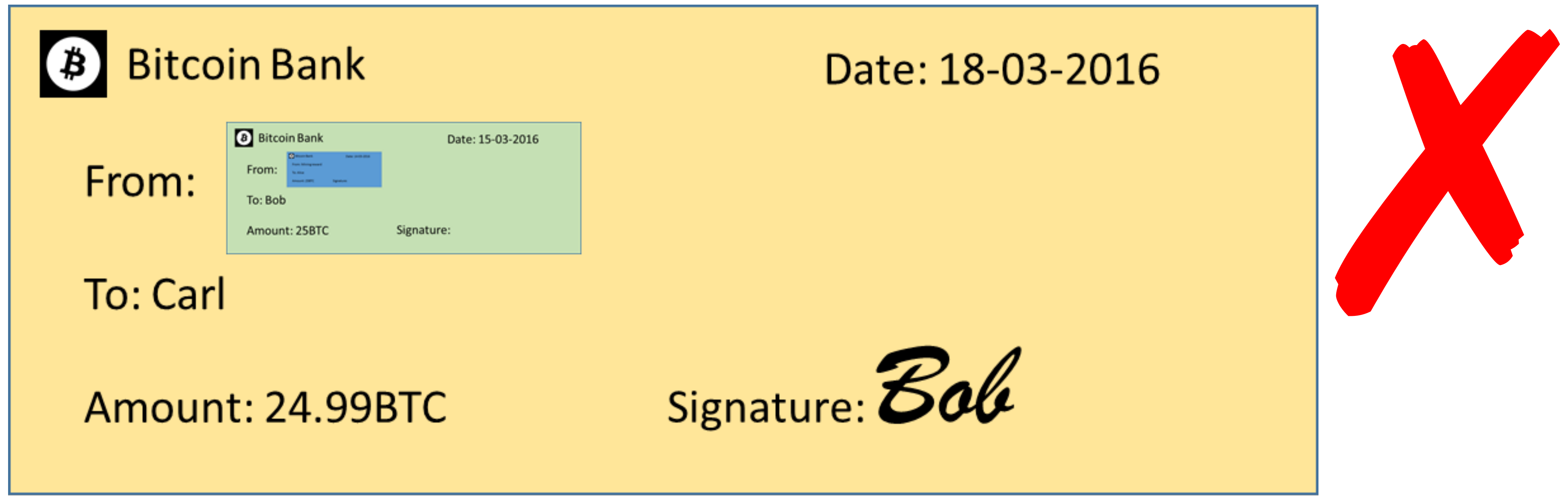
To: Alice

Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature:

✗



Bitcoin Bank Date: 18-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

To: Bob

Amount: 25BTC Signature:

To: Carl

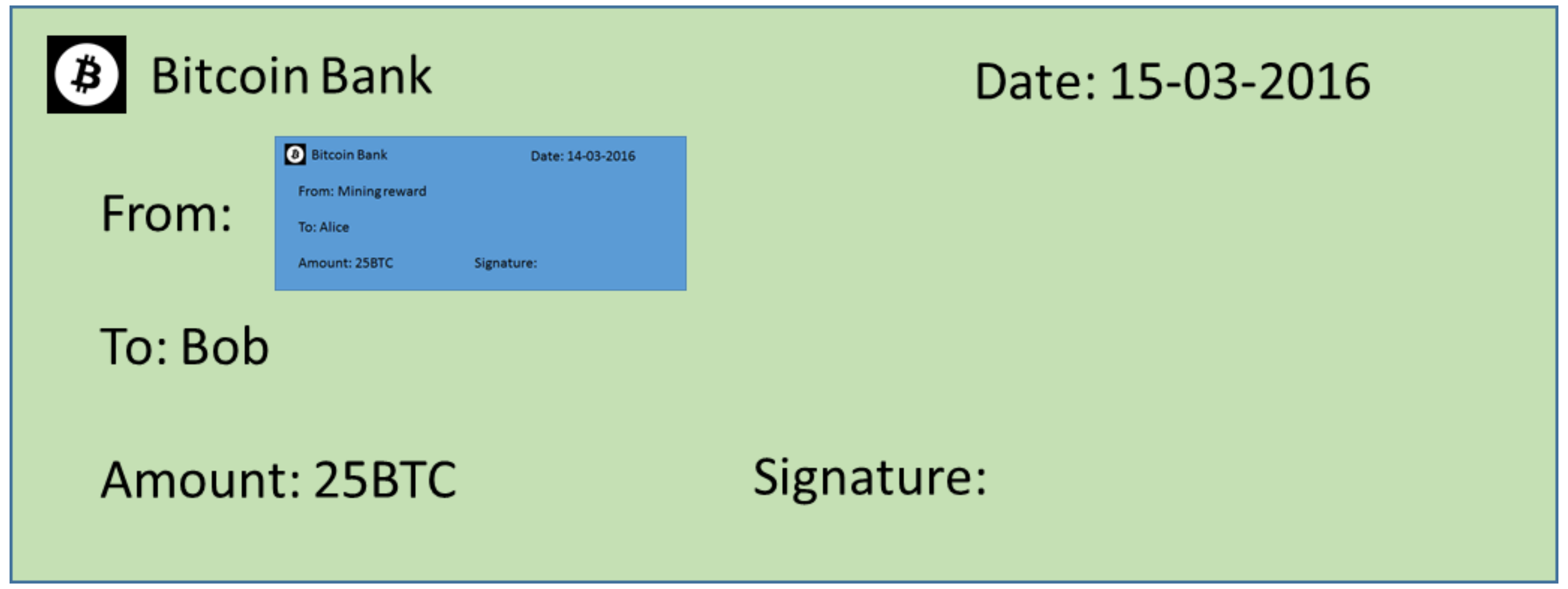
Amount: 24.99BTC Signature: Bob

✗

# Creating a chain of transactions

## Method 2

- Alice creates the green cheque but not sign it (invalid)



Bitcoin Bank

Date: 15-03-2016

From:

Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC

Signature:

To: Bob

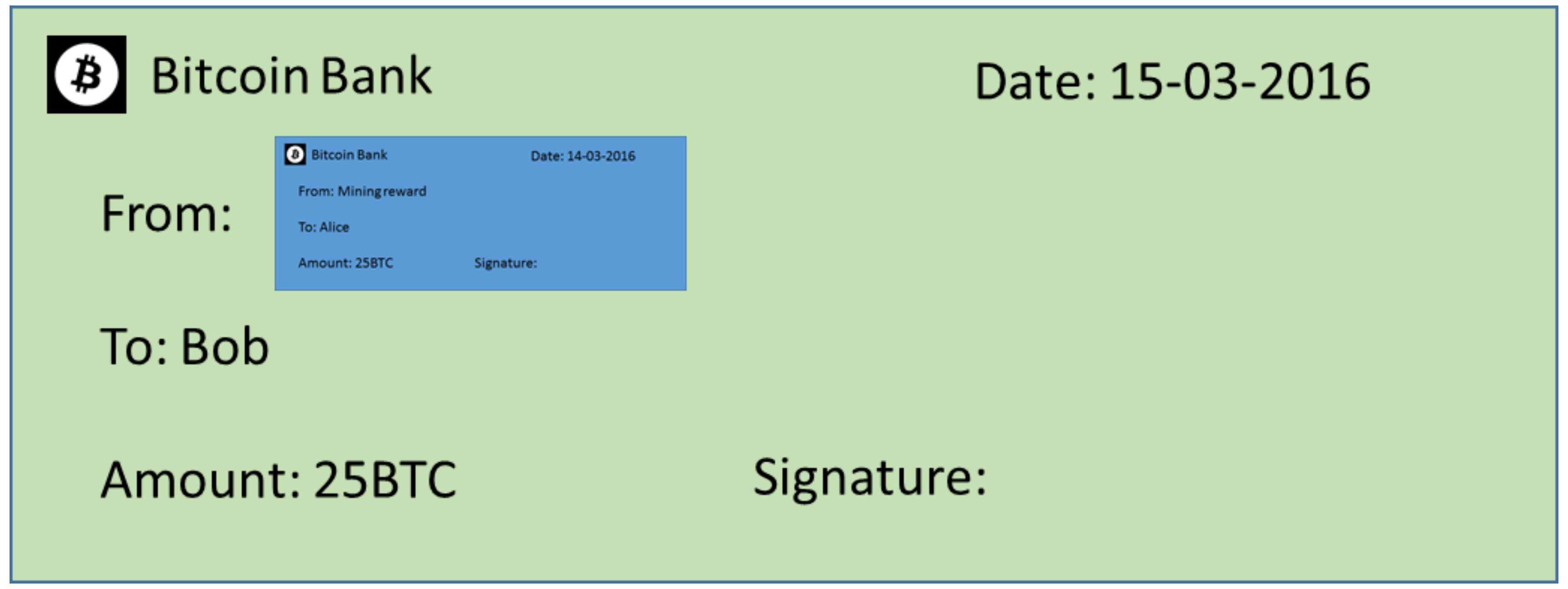
Amount: 25BTC

Signature:

# Creating a chain of transactions

## Method 2

- Alice creates the green cheque but not sign it (invalid)
- Bob creates the yellow cheque and signs it (invalid)



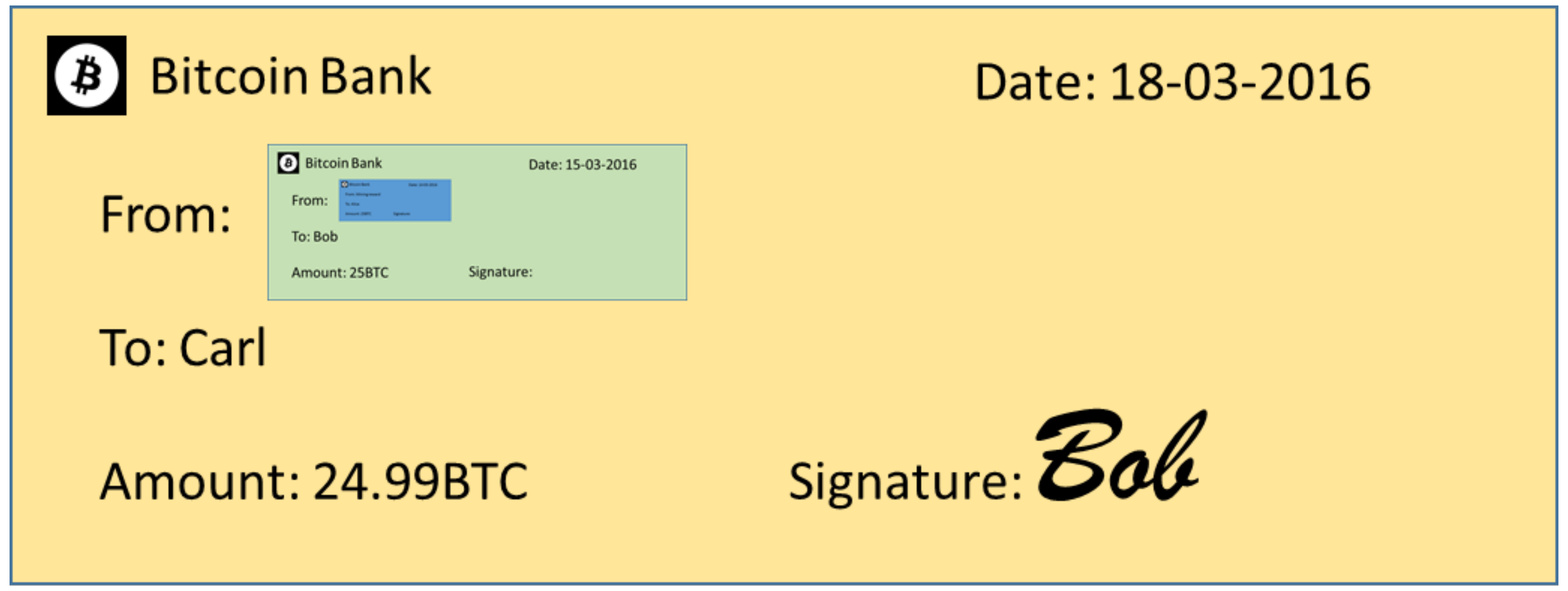
Bitcoin Bank Date: 15-03-2016

From:

> Bitcoin Bank Date: 14-03-2016
>
> From: Mining reward
>
> To: Alice
>
> Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature:



Bitcoin Bank Date: 18-03-2016

From:

> Bitcoin Bank Date: 15-03-2016
>
> From:
>
> To: Bob
>
> Amount: 25BTC Signature:

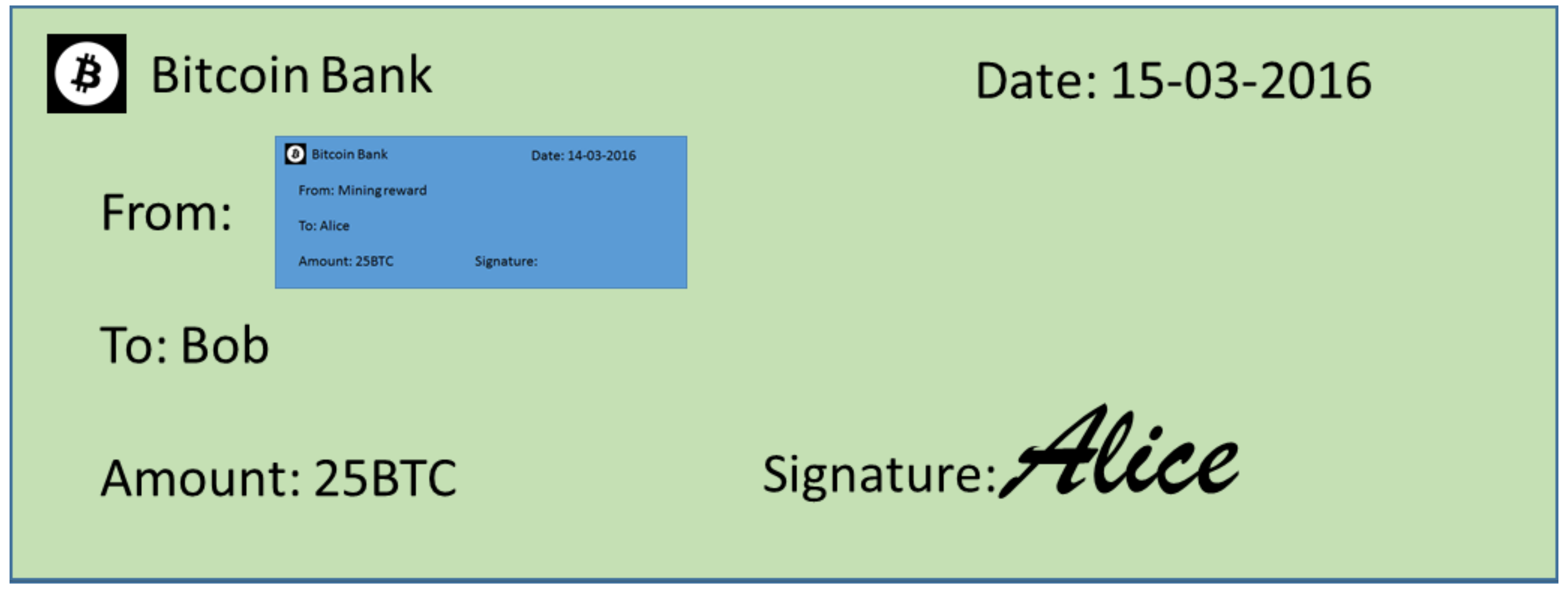
To: Carl

Amount: 24.99BTC Signature: Bob

# Creating a chain of transactions

## Method 2

- Alice creates the green cheque but not sign it (invalid)
- Bob creates the yellow cheque and signs it (invalid)
- Alice signs the green cheque (valid)



Bitcoin Bank

Date: 15-03-2016

From:

Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC

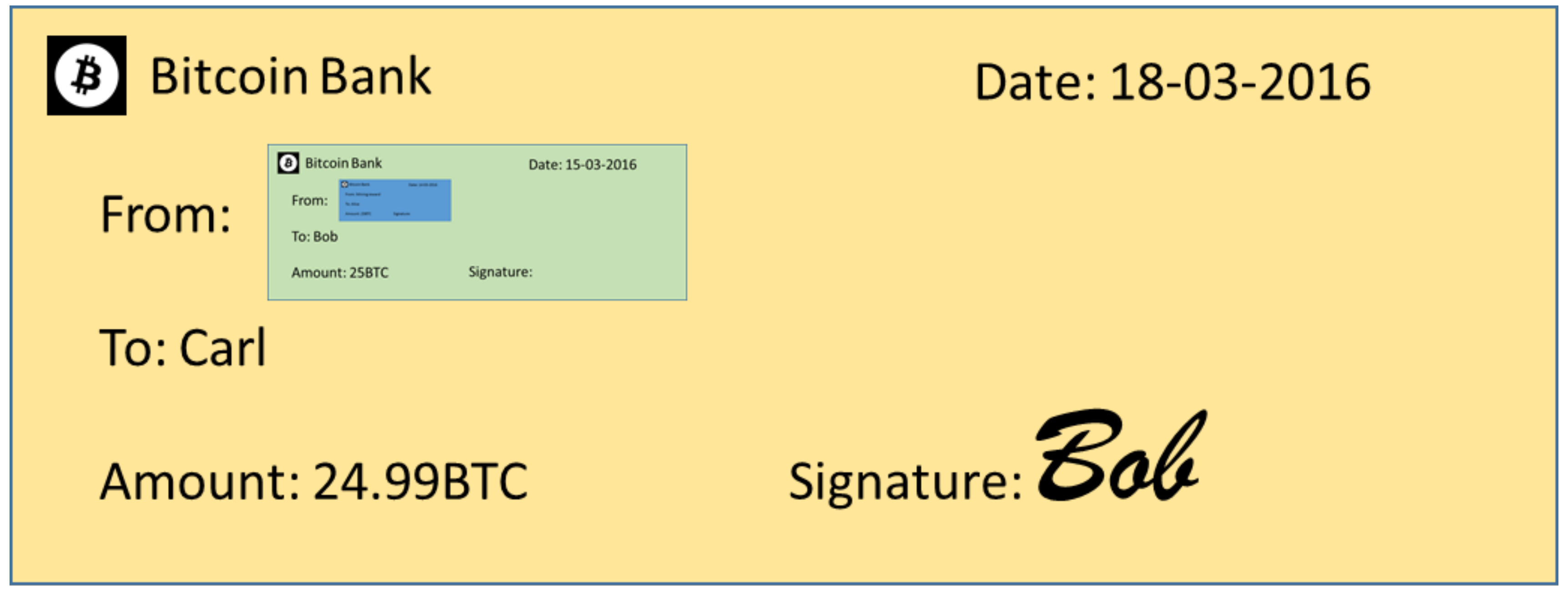
Signature:

To: Bob

Amount: 25BTC

Signature: Alice

✓



Bitcoin Bank

Date: 18-03-2016

From:

Bitcoin Bank

Date: 15-03-2016

From:

To: Bob

Amount: 25BTC

Signature:

To: Carl

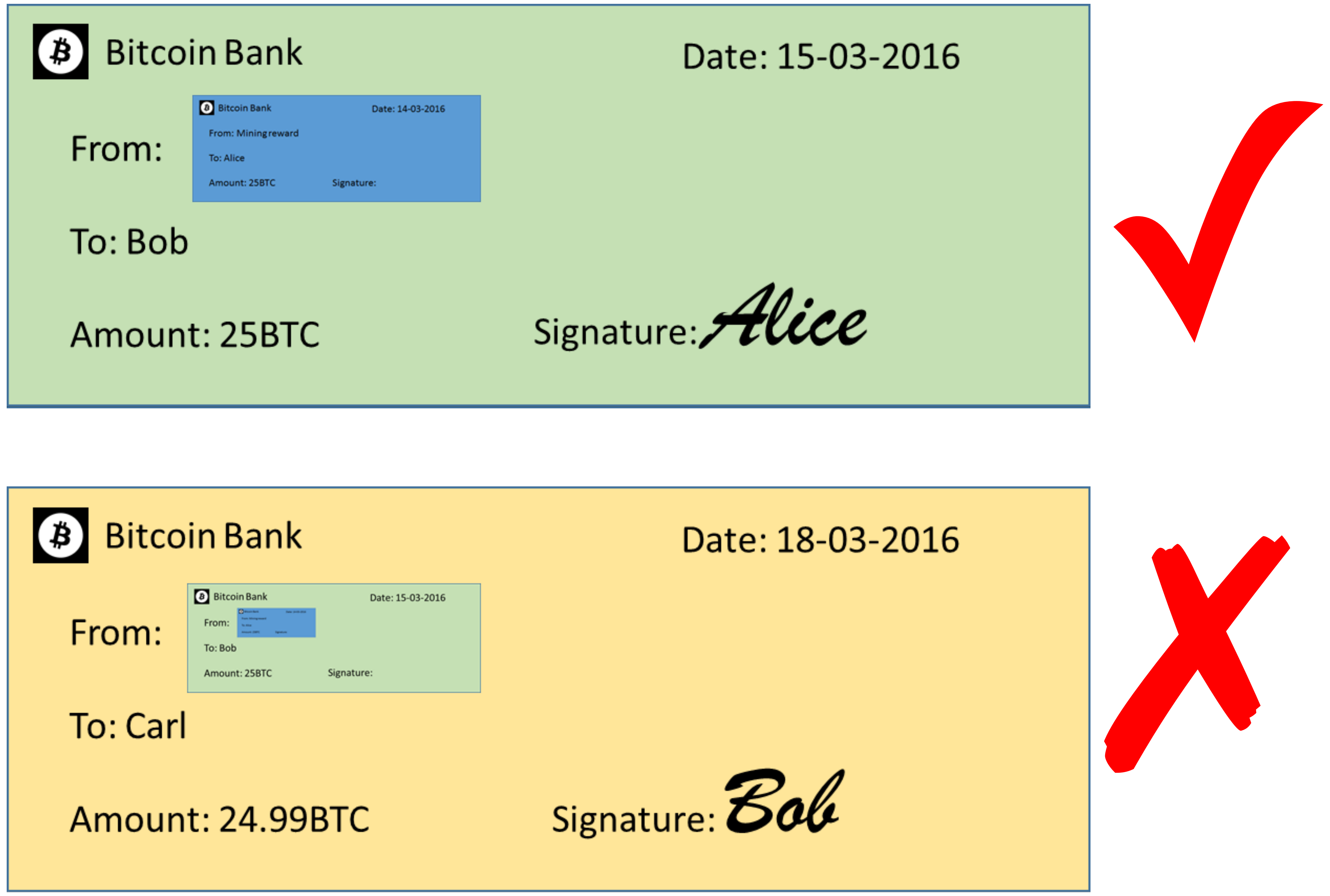
Amount: 24.99BTC

Signature: Bob

# Creating a chain of transactions

## Method 2

- Alice creates the green cheque but not sign it (invalid)
- Bob creates the yellow cheque and signs it (invalid)
- Alice signs the green cheque (valid)
- The yellow cheque is still invalid since it is based on the unsigned green cheque



Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

✓

Bitcoin Bank Date: 18-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

To: Bob

Amount: 25BTC Signature:

To: Carl

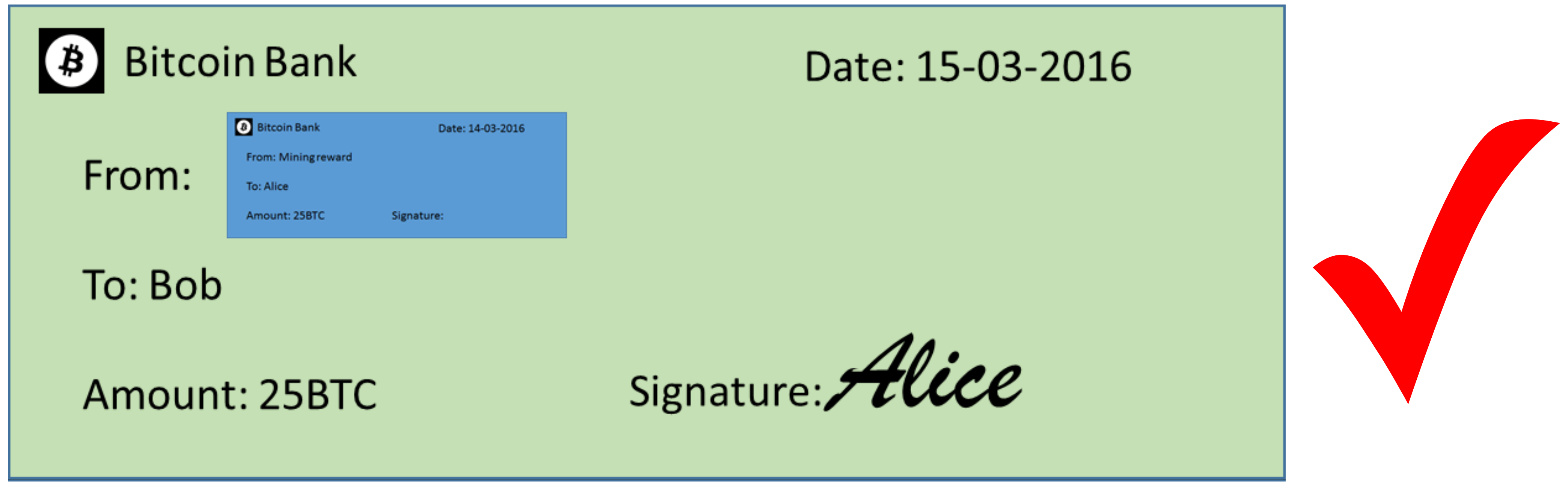
Amount: 24.99BTC Signature: Bob

✗

# Creating a chain of transactions

## Method 3

- Alice creates the green cheque and sign it (valid)
- Bob may just take the money and run away



Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

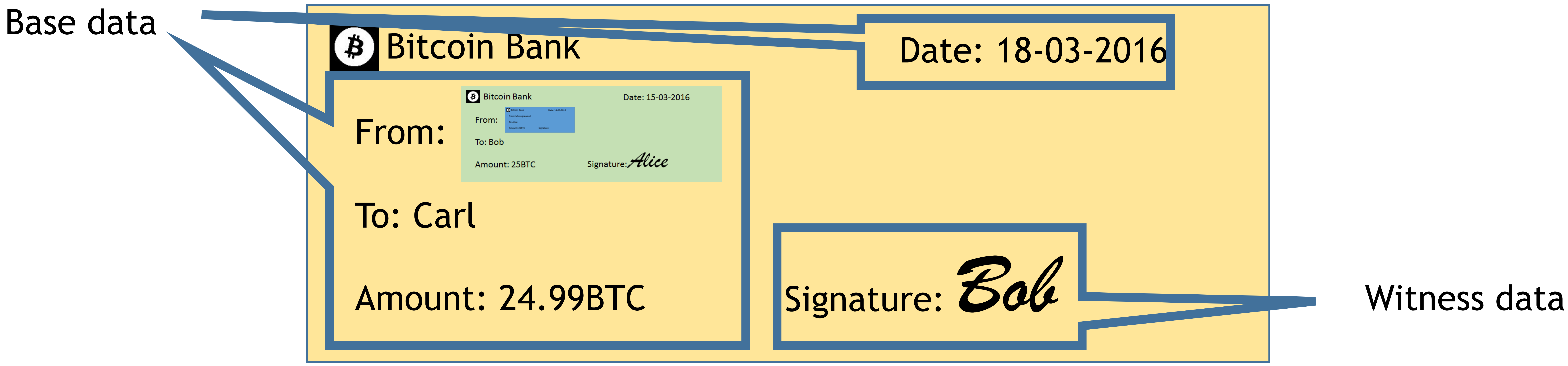
Amount: 25BTC Signature:

To: Bob

Amount: 25BTC Signature: Alice

# Solution to involuntary malleability : Segregated witness

- Proposed by Pieter Wuille
- Transaction could be divided in the 2 parts:
  - Base data: where the money comes and goes
  - Witness data: information to verify the correctness of the base data (signature)
- Segregated witness: separating base data and witness data



Bitcoin Bank

Date: 18-03-2016

From:

Bitcoin Bank

Date: 15-03-2016

From:

Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC

Signature:

To: Bob

Amount: 25BTC

Signature: Alice

To: Carl

Amount: 24.99BTC

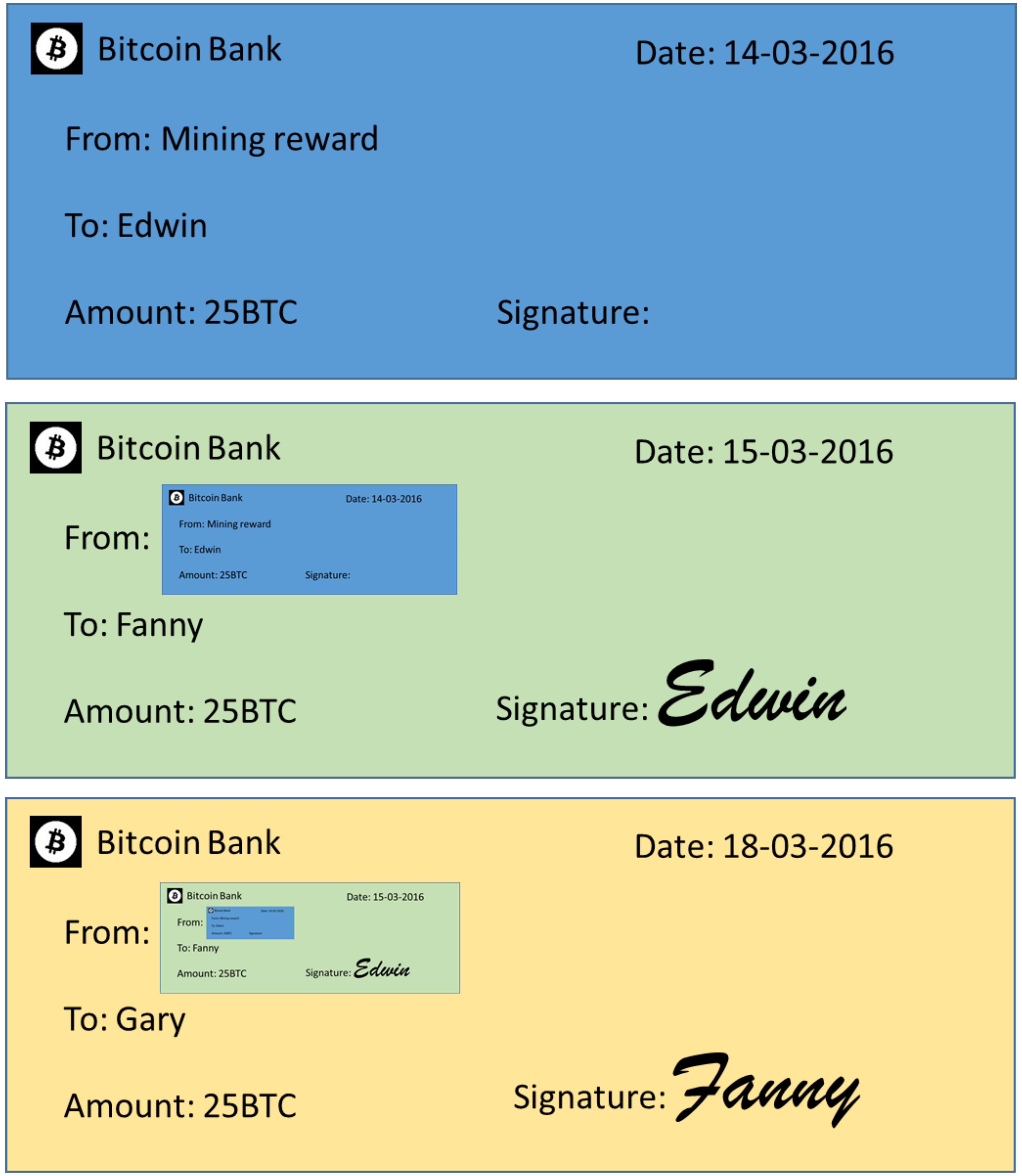
Signature: Bob

# New rules introduced by SegWit

- Instead of paying to “Alice”, we pay to “Anyone (segwit Alice)”
- When Alice wants to spend the money, she MUST NOT sign on the cheque.
- Instead, Alice signs on a separate paper and attach it to the cheque
  - For people who enforce the new rules, they will verify the signature as they know the money actually belongs to “segwit Alice”, not “Anyone”
- If the signature field on the cheque is not exactly blank, people who enforce the new rules will reject the cheque
  - Involuntary malleability becomes impossible

- For people who do not know the new rules…
  - The cheque is valid because the money was sent to “Anyone” and did not require any signature to spend
  - They don’t understand “segwit Alice” and will just ignore it
  - They will not see the real signature

## Without segwit



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Edwin

Amount: 25BTC Signature:

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Edwin Amount: 25BTC Signature:

To: Fanny

Amount: 25BTC Signature: Edwin

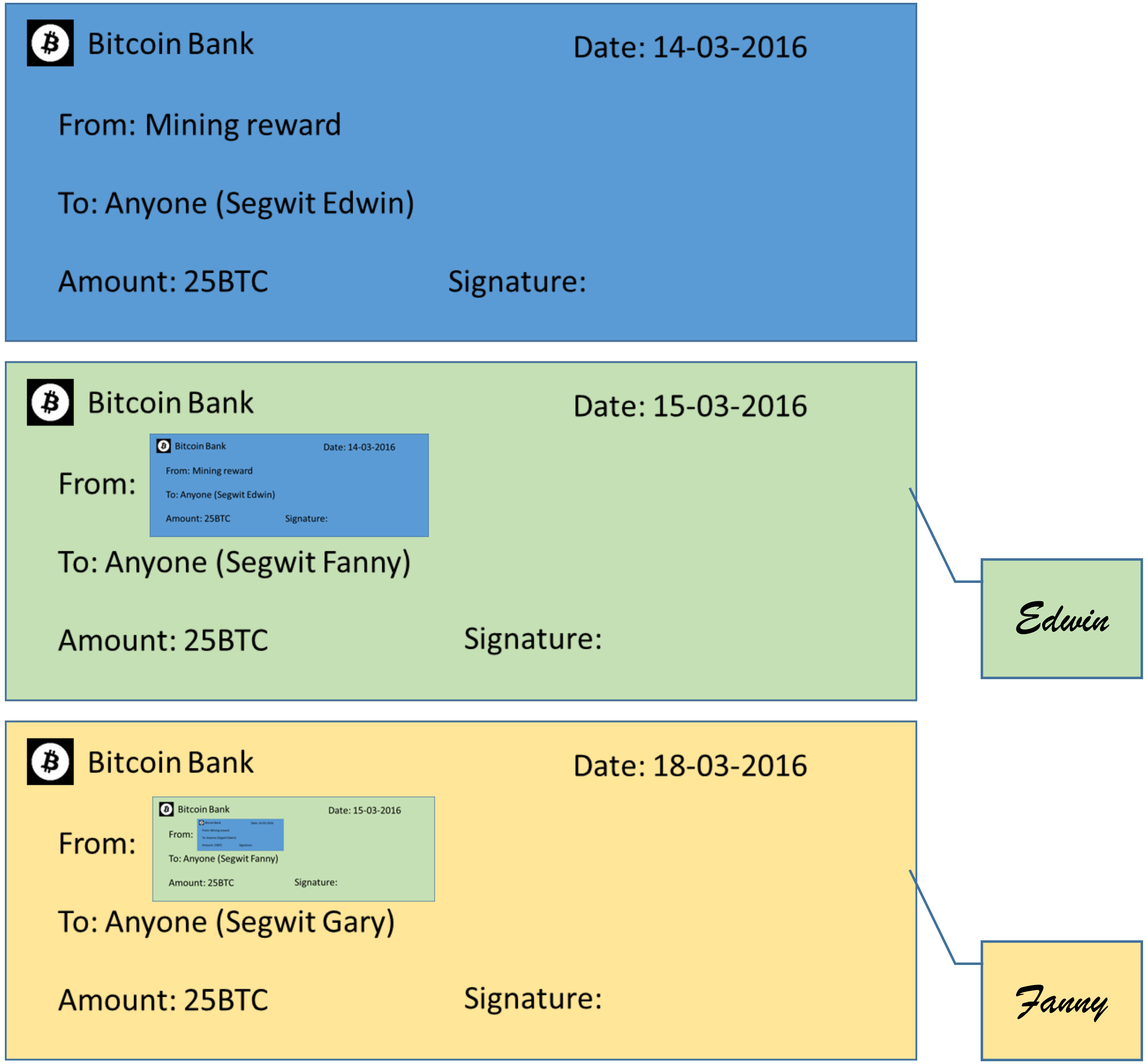
Bitcoin Bank Date: 18-03-2016

From: Bitcoin Bank Date: 15-03-2016 From: To: Fanny Amount: 25BTC Signature: Edwin

To: Gary

Amount: 25BTC Signature: Fanny

## With segwit



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Anyone (Segwit Edwin)

Amount: 25BTC Signature:

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Anyone (Segwit Edwin) Amount: 25BTC Signature:

To: Anyone (Segwit Fanny)

Amount: 25BTC Signature:

Edwin

Bitcoin Bank Date: 18-03-2016

From: Bitcoin Bank Date: 15-03-2016 From: To: Anyone (Segwit Fanny) Amount: 25BTC Signature:

To: Anyone (Segwit Gary)

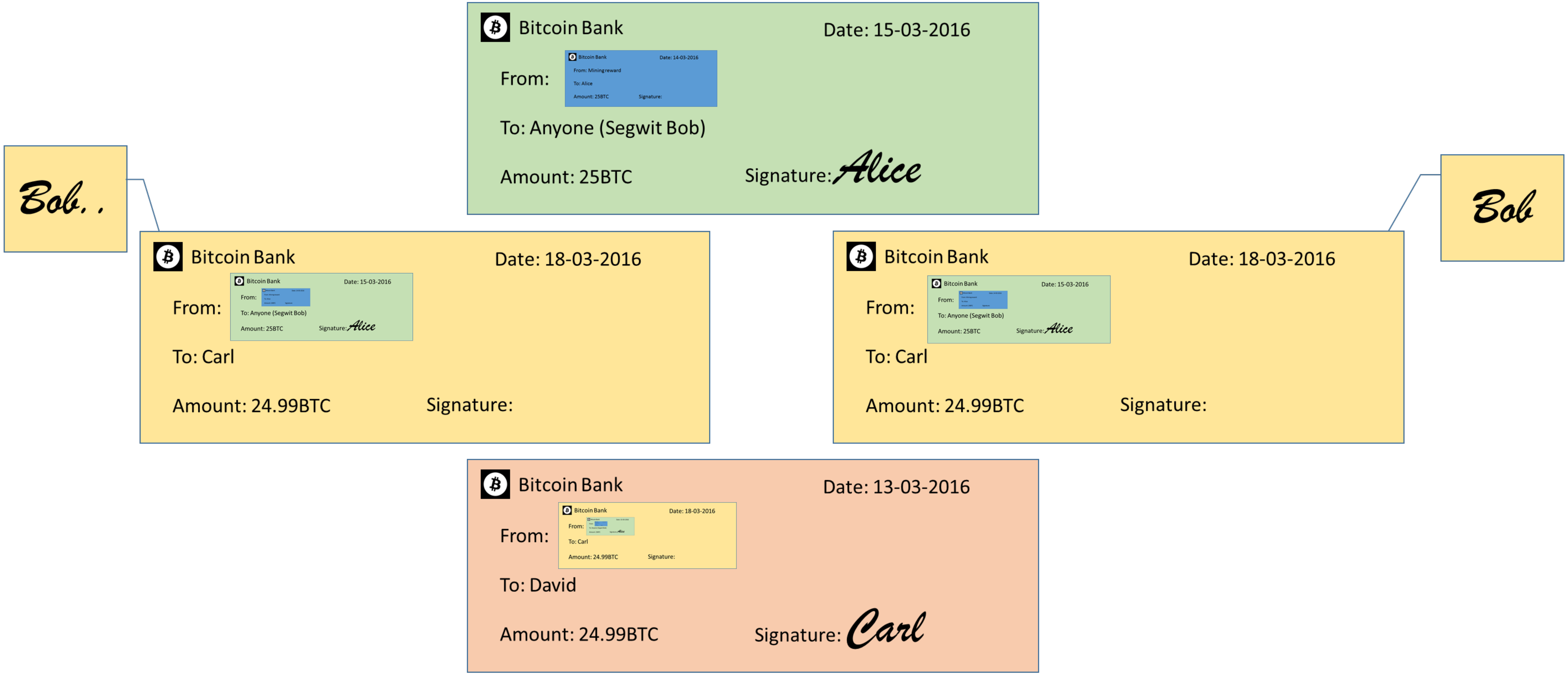
Amount: 25BTC Signature:

Fanny

# Segregated witness

- Two types of malleability
  - Signature malleability
  - Double spending
- With segwit, signature malleability becomes irrelevant
  - The cheque itself still looks the same (the TxID is not changed)
- Double spending becomes the only type of transaction malleability
  - Not fixable: unconfirmed txs are always unsafe
  - Use multi-signature to prevent unexpected double spending by the counterparty
- A transaction chain could be constructed without first signing an earlier transaction in the chain

# Signature malleability won’t break the tx chain



Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Alice

Amount: 25BTC Signature:

To: Anyone (Segwit Bob)

Amount: 25BTC Signature: Alice

Bob. ,

Bitcoin Bank Date: 18-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

To: Anyone (Segwit Bob)

Amount: 25BTC Signature: Alice

To: Carl

Amount: 24.99BTC Signature:

Bob

Bitcoin Bank Date: 18-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

To: Anyone (Segwit Bob)

Amount: 25BTC Signature: Alice

To: Carl

Amount: 24.99BTC Signature:

Bitcoin Bank Date: 13-03-2016

From:

Bitcoin Bank Date: 18-03-2016

From:

To: Carl

Amount: 24.99BTC Signature:

To: David

Amount: 24.99BTC Signature: Carl

# Creating a chain of transactions with segwit

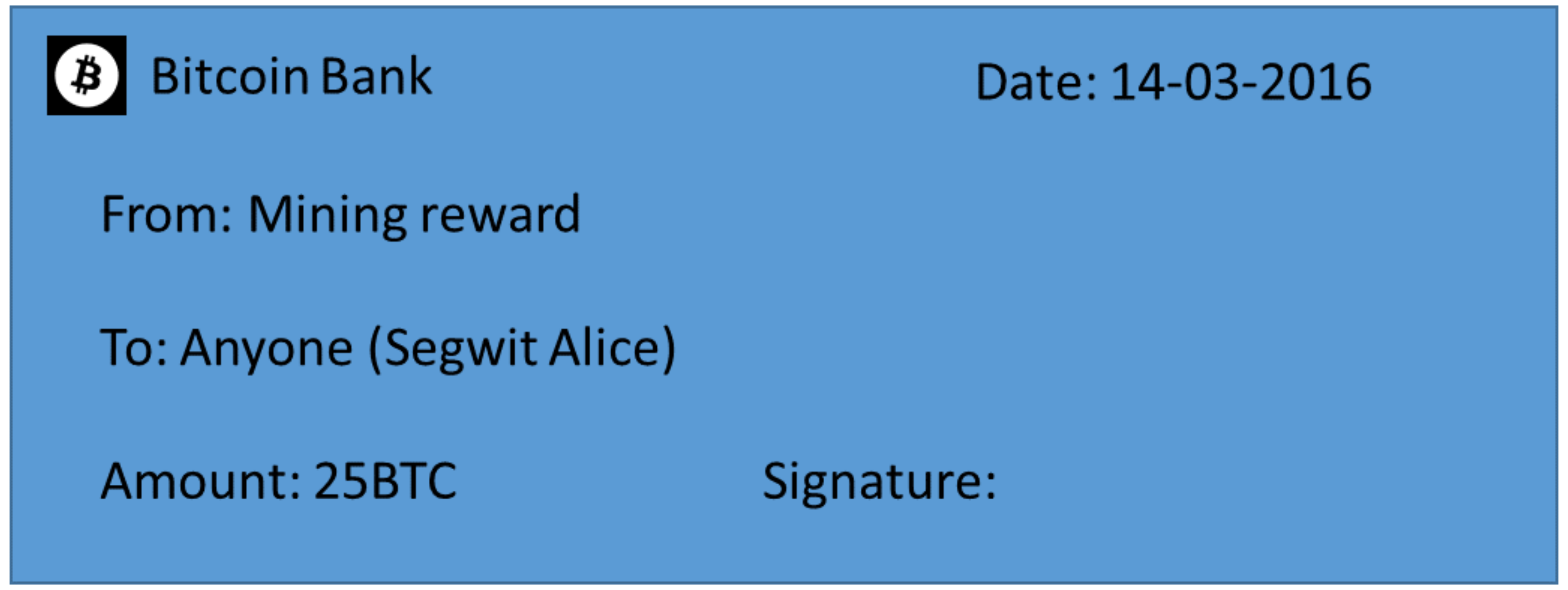
Scenario: Alice is paying 25BTC to Bob, but only if Bob agrees to pay 24.99BTC to Carl later.

However, Alice worries that Bob will just take the money and refuse to send to Carl

Use segwit and 2-of-2 multisig

# Creating a chain of transactions with segwit

1. Alice has 25BTC in a segwit address, already confirmed



Bitcoin Bank

Date: 14-03-2016

From: Mining reward

To: Anyone (Segwit Alice)

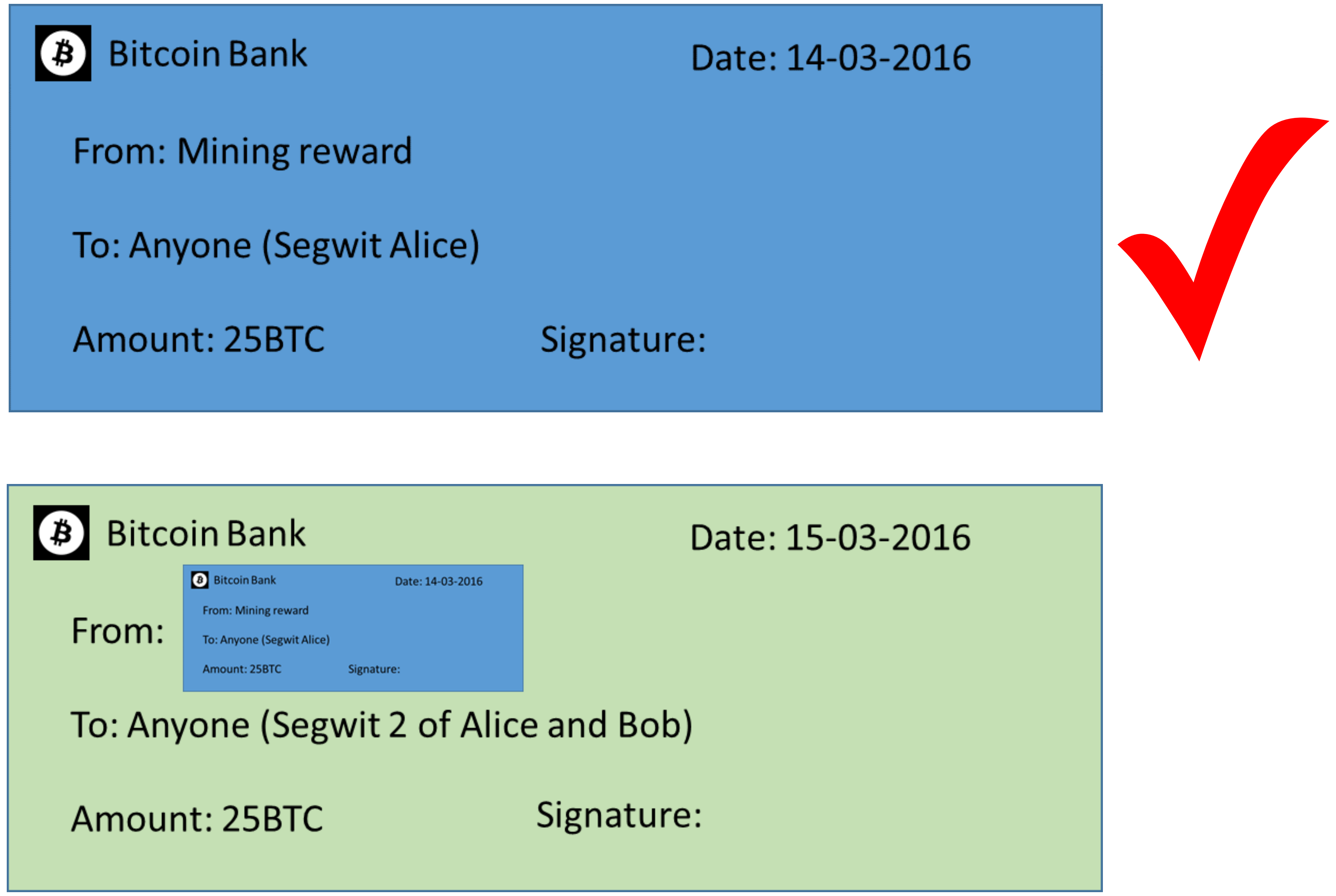
Amount: 25BTC

Signature:

✓

# Creating a chain of transactions with segwit

1. Alice has 25BTC in a segwit address, already confirmed
2. Alice creates the green cheque, sending 25BTC to “Segwit 2 of Alice and Bob”, but do NOT attach a signature



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Anyone (Segwit Alice)

Amount: 25BTC Signature:

✓

Bitcoin Bank Date: 15-03-2016

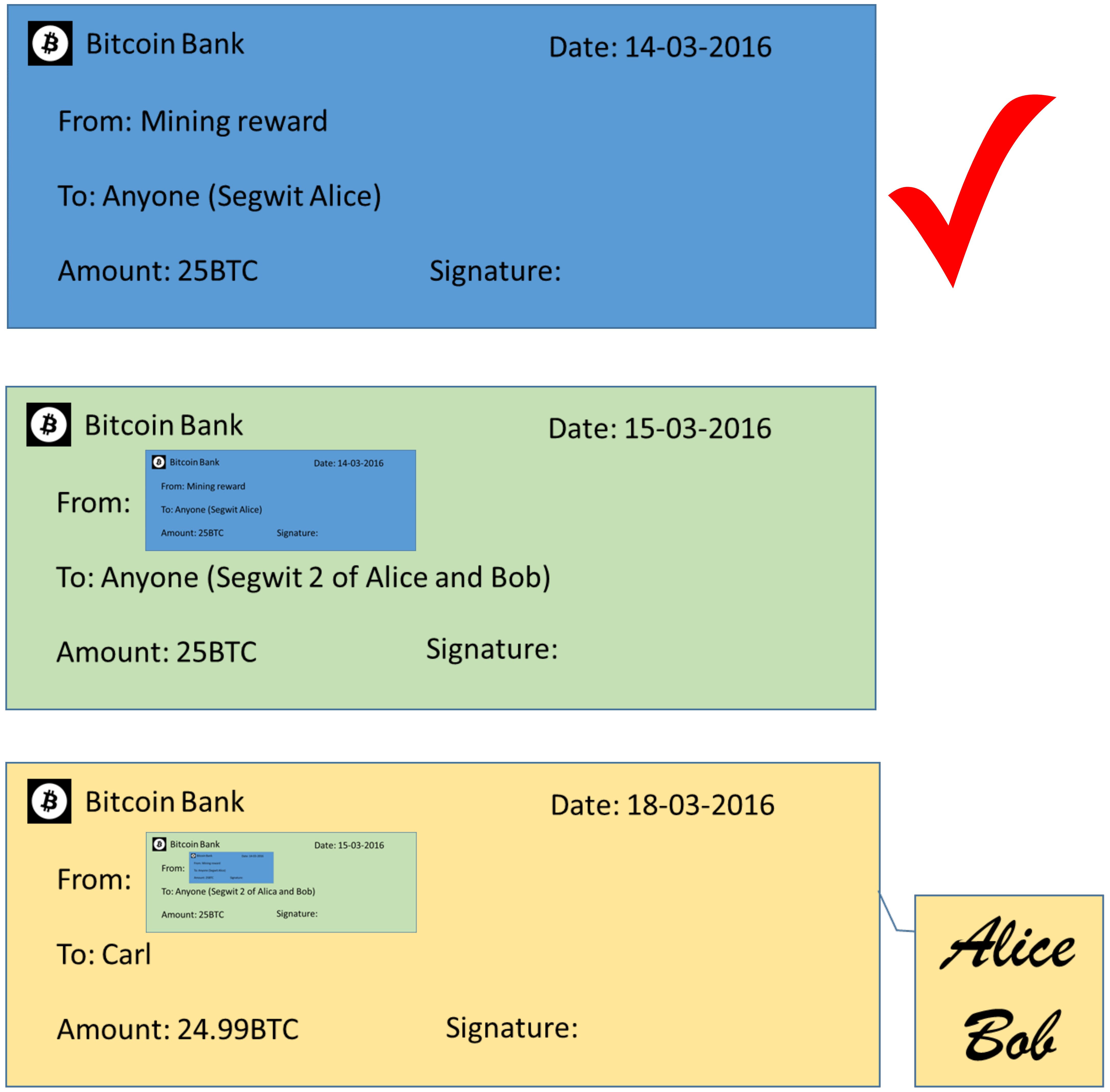
From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Anyone (Segwit Alice) Amount: 25BTC Signature:

To: Anyone (Segwit 2 of Alice and Bob)

Amount: 25BTC Signature:

# Creating a chain of transactions with segwit

1. Alice has 25BTC in a segwit address, already confirmed
2. Alice creates the green cheque, sending 25BTC to “Segwit 2 of Alice and Bob”, but do NOT attach a signature
3. Based on the green cheque, Alice and Bob create the yellow cheque, sending 24.99BTC to Carl, and sign it.
   - The yellow cheque is invalid at this moment since the green check has not signature attached



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Anyone (Segwit Alice)

Amount: 25BTC Signature:

✓

Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Anyone (Segwit Alice)

Amount: 25BTC Signature:

To: Anyone (Segwit 2 of Alice and Bob)

Amount: 25BTC Signature:

Bitcoin Bank Date: 18-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

To: Anyone (Segwit 2 of Alica and Bob)

Amount: 25BTC Signature:

To: Carl

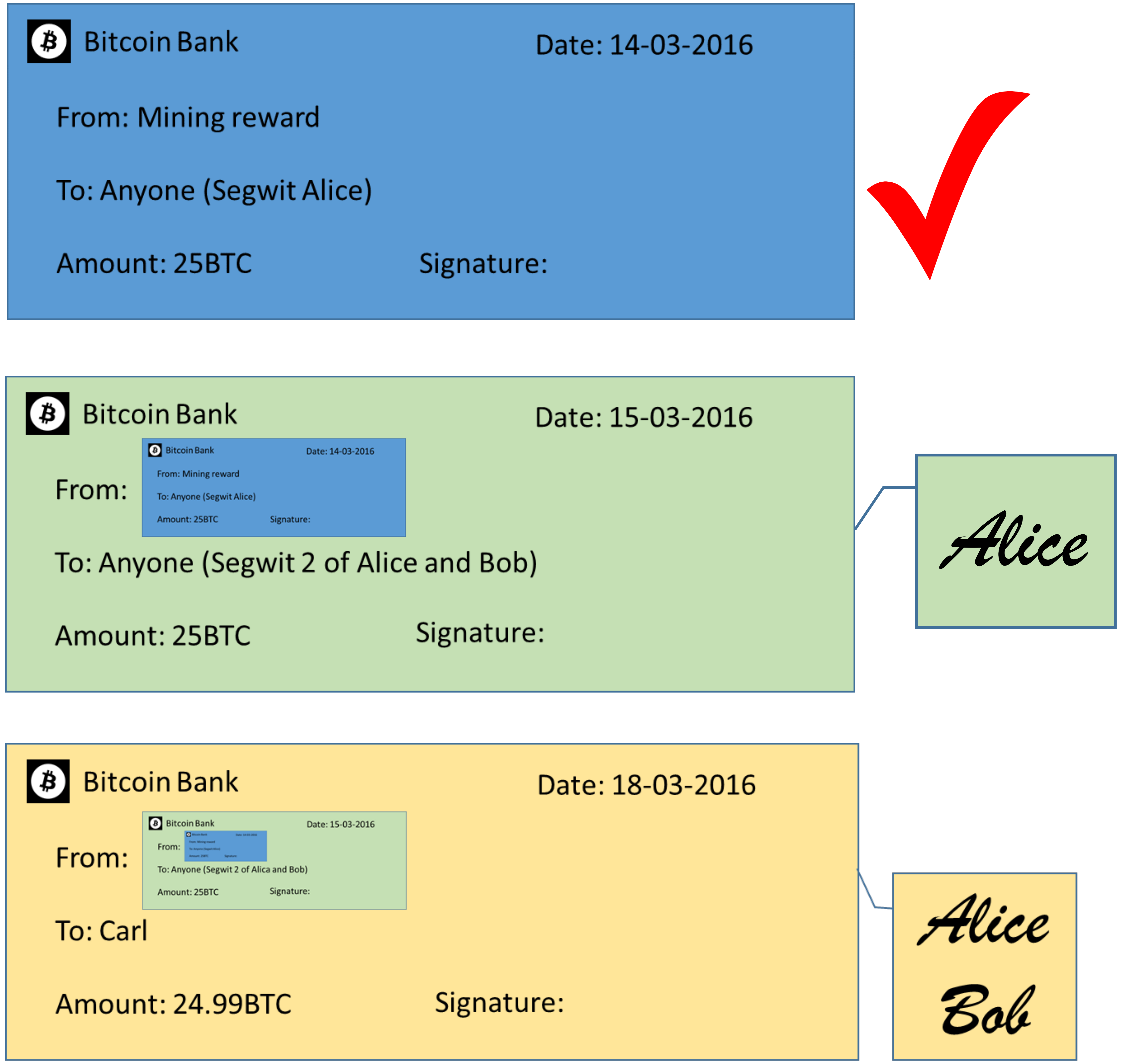
Amount: 24.99BTC Signature:

Alice

Bob

# Creating a chain of transactions with segwit

1. Alice has 25BTC in a segwit address, already confirmed
2. Alice creates the green cheque, sending 25BTC to “Segwit 2 of Alice and Bob”, but do NOT attach a signature
3. Based on the green cheque, Alice and Bob create the yellow cheque, sending 24.99BTC to Carl, and sign it.
   - The yellow cheque is invalid at this moment since the green check has not signature attached
4. After the yellow cheque has Bob’s signature attached, Alice signs the green cheque
   - Both green and yellow cheques become valid



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Anyone (Segwit Alice)

Amount: 25BTC Signature:

✓

Bitcoin Bank Date: 15-03-2016

From: Bitcoin Bank Date: 14-03-2016 From: Mining reward To: Anyone (Segwit Alice) Amount: 25BTC Signature:

To: Anyone (Segwit 2 of Alice and Bob)

Amount: 25BTC Signature:

Alice

Bitcoin Bank Date: 18-03-2016

From: Bitcoin Bank Date: 15-03-2016 From: To: Anyone (Segwit 2 of Alica and Bob) Amount: 25BTC Signature:

To: Carl

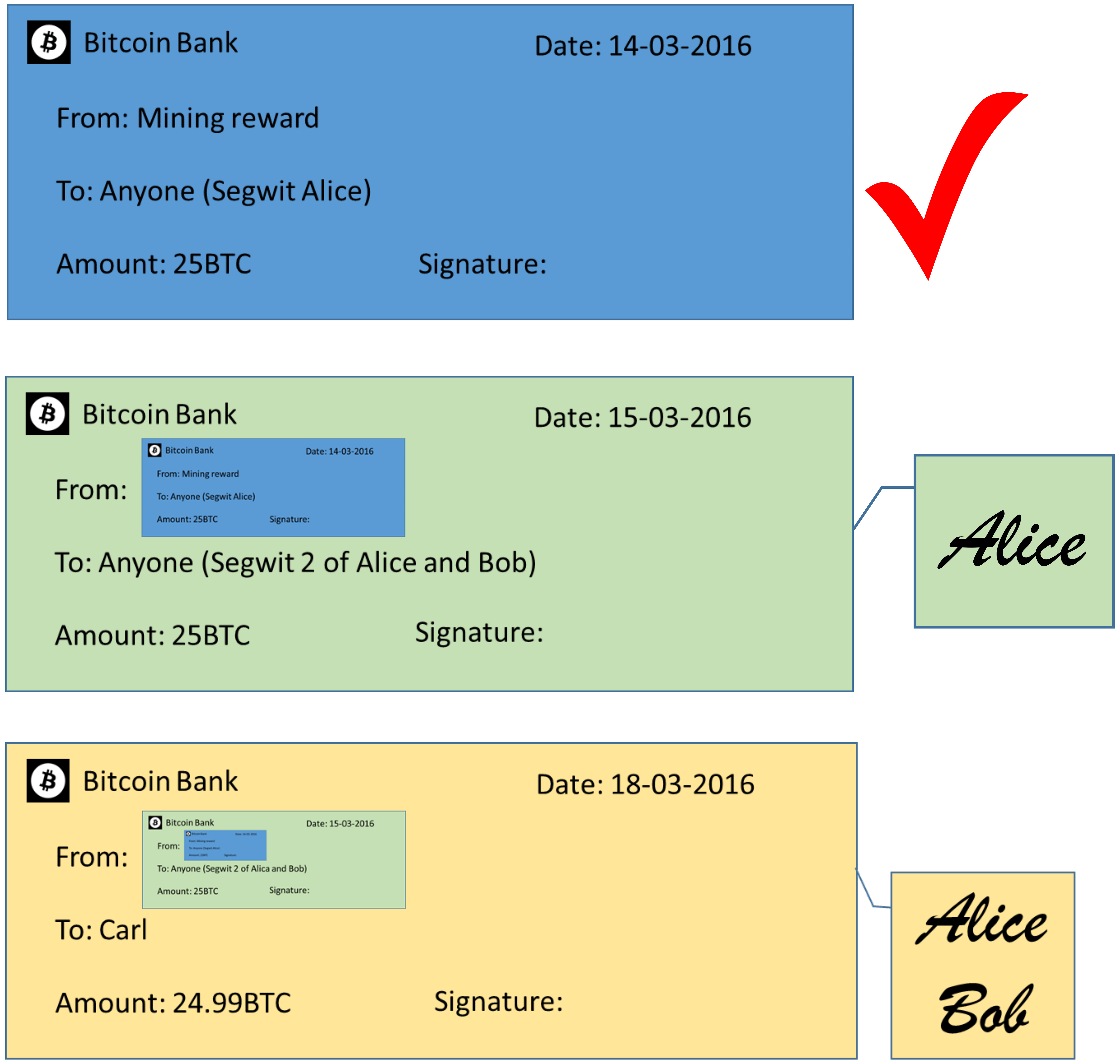
Amount: 24.99BTC Signature:

Alice

Bob

# Creating a chain of transactions with segwit

1. Alice has 25BTC in a segwit address, already confirmed
2. Alice creates the green cheque, sending 25BTC to “Segwit 2 of Alice and Bob”, but do NOT attach a signature
3. Based on the green cheque, Alice and Bob create the yellow cheque, sending 24.99BTC to Carl, and sign it.
   - The yellow cheque is invalid at this moment since the green check has not signature attached
4. After the yellow cheque has Bob’s signature attached, Alice signs the green cheque
   - Both green and yellow cheques become valid
5. Bonus: If both Alice and Bob agree, they can sign another cheque, dated before 18-03-2016, sending the money to another person



Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Anyone (Segwit Alice)

Amount: 25BTC Signature:

✓

Bitcoin Bank Date: 15-03-2016

From:

Bitcoin Bank Date: 14-03-2016

From: Mining reward

To: Anyone (Segwit Alice)

Amount: 25BTC Signature:

To: Anyone (Segwit 2 of Alice and Bob)

Amount: 25BTC Signature:

Alice

Bitcoin Bank Date: 18-03-2016

From:

Bitcoin Bank Date: 15-03-2016

From:

To: Anyone (Segwit 2 of Alica and Bob)

Amount: 25BTC Signature:

To: Carl

Amount: 24.99BTC Signature:

Alice

Bob

# Bonus of segregated witness

- Increasing the maximum block size from 1MB to effectively 1.75-4MB
  - Since the witness data is not visible to existing software, it won't be counted in the block size limit
  - Allow more transactions in a block
- Existing transaction format still works in the same way as before
  - Upgrade is mandatory for miners only
  - Non-upgraded wallets will keep functioning (no malleability protection)
  - Seamlessly sending money between upgraded and non-upgraded wallets
  - Upgraded wallets will enjoy ~50% discount in transaction fee due to the use of the cheaper space for witness data

# Bonus of segregated witness

- Transmission and storage of witness data becomes optional
  - Base data alone is enough for telling the full history of transactions
  - Witness data is needed only if a wallet wants to validate transactions
    - Most light wallets do not validate transactions
  - Witness data long time ago may be removed, assuming no one would challenge its validity
  - Some archival network nodes may still keep witness data

# Bonus of segregated witness

- Fully enabling smart contracts
  - Many smart contracts require chains of multi-signature transactions
  - Lightning Network: instant confirmation with very low cost

- Introduction of new script system becomes much easier
  - BIP143: to be deployed with segregated witness (BIP141)
    - Bug fix for transaction validation
    - Fee calculation becomes much easier for hardware wallets / cold wallets
  - Future
    - Efficient signature system, e.g. Schnorr signature
    - Compressing long and conditional scripts: Merklized abstract syntax tree (MAST)

# Bonus of segregated witness

- Introduction of fraud proof system
  - Bitcoin White Paper: *“(SPV wallets) accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency”*
  - Compact fraud proof is currently not possible in some situations
    - Excessive minting
    - Excessive block size
    - Spending of a non-existing input
  - Extra witness data can be committed that allows short proofs of block invalidity that light wallets can quickly verify

# User experience

- If you do not upgrade your wallet:
  - You can receive payment from any wallets, upgraded or not, through 1-initial or 3-initial addresses (without any benefit of segwit)
  - You can pay a non-upgraded wallet, through an 1-initial or 3-initial address (without any benefit of segwit)
  - You can pay an upgraded wallet, through a 3-initial address
    - You won't enjoy any benefit of segwit
    - The payee will enjoy the benefit of segwit when they spend the bitcoin later

- If you upgrade your wallet:
  - You can receive payment from any wallets, upgraded or not, through 3-initial addresses
  - ~50% transaction fee discount (relative to non-upgraded wallet) is expected when you spend your bitcoin, depending on the proportion of witness data
    - Multisig tx will enjoy more discount
    - Tx with many inputs but a few outputs will enjoy more discount

# Safety issues in the deployment of SegWit

- It is a softfork:
  - Upgrade is mandatory for miners (mining pools) only
  - As long as vast majority of miners enforce the new rules, sustained blockchain split is not possible
  - We have profound experience of deploying softfork: BIPs16, 34, 66, 65
  - This is not the first time we change the meaning of some anyone-can-spend scripts (BIP16)
- Testing and peer reviewing
  - Segwit has been tested in sidechains for > 6 months
  - Bitcoin segregated witness testnet (“segnet”) has been running since December 2015

# Technical details: BIP141

- A traditional 1-initial address represents a scriptPubKey like this:
  - OP_DUP OP_HASH160 <20-byte-public-key-hash> OP_EQUALVERIFY OP_CHECKSIG
- With the same public key hash, the equivalent segwit scriptPubKey is:
  - OP_0 <20-byte-public-key-hash>
  - “P2WPKH”: Pay-to-witness-public-key-hash
  - In the original script language, this scriptPubKey is anyone-can-spend, since it does not contain any functional code, and the last push is non-zero
- To spend P2WPKH:
  - The scriptSig must be exactly empty
  - The witness must contain exactly 2 items: signature and public key
- We also define P2WSH (Pay-to-witness-script-hash) which allows arbitrarily complex scripts, similar to P2SH (pay-to-script-hash, BIP16)
  - See BIP141 for details

# Technical details: BIP141

- Commitment of witness data
  - Witness data is committed as a Merkel Root in one of the outputs of the coinbase transaction.
  - The commitment is recorded in a scriptPubKey of the coinbase transaction. It must be at least 38 bytes, with the first 6-byte of 0x6a24aa21a9ed, followed by the 32-byte commitment hash
  - If there are more than one scriptPubKey matching the pattern, the one with highest output index is assumed to be the commitment.
  - Extra space is reserved for commitments required by future softforks.

- Witness data discount
  - A 75% discount is given to the witness data
  - Block size limit: base data size + (witness data size / 4) ≤ 1MB

# Technical details: BIP143

- There are at least 2 weaknesses in the original signature verification algorithm:

- The verification time grows quadratically, instead of linearly, as the number of signature operations increase.
  - A normal 1 MB block should take 2 seconds to verify
  - A 1MB transaction with 5569 signature operations may take 25 seconds to verify; a 2MB transaction may take > 10 minutes

- The algorithm does not involve the amount of Bitcoin being spent by the input.
  - Offline transaction signing device ("cold wallet") are unable to calculate the exact amount being spent and the transaction fee
  - A cold wallet must acquire the full transaction being spent, just for calculation of fee
  - Difficult for lightweight, air-gapped wallet.

- BIP143 introduces a new signature verification algorithm to segwit transactions to solve these problems

# Technical details: BIP144

- A new serialization format is defined
- Non-segwit transaction must use the original serialization format
- Segwit transaction use the new format when witness data is included

Transaction ID: nVersion | inputs | outputs | nLockTime

Witness ID: nVersion | 0x00 | flags | inputs | outputs | witness | nLockTime

# Technical details: BIP142 (deferred)

- There are 2 ways for using segwit:
  - Native segwit (more efficient)
  - Segwit in P2SH (less efficient as it requires extra base data space)
- BIP142 defines new address format for native segwit use
  - Not deployed in the initial release for segwit
- “Segwit in P2SH” allows non-upgraded wallets pay to upgraded wallets through 3-initial addresses
- Native segwit is still possible without BIP142
  - BIP70 Payment Protocol
  - Raw transactions (dangerous!!!)

# BIP62: an incomplete fix

- “Dealing with malleability” by Pieter Wuille
- Canonical signature approach: Limiting the way people may sign a transaction
    - For involuntary signature malleability only
    - Voluntary signature malleability / double-spending is not fixable
- It is an incomplete fix, because
    - New mathematical malleability might be found in the future and bring us back to the square one
    - It fixes malleability in only some common cases
    - In the case of an m-of-n multisig, ANY 1 of the n people may change the Tx ID without the consent of other people (due to voluntary signature malleability)
    - It is still not possible to construct a chain of txs, without first signing an earlier tx in the chain