

# Ebay without Ebay

Oleg Andreev  
@oleganza  
oleganza@gmail.com

February 13, 2014

**Bitcoin is:**

# Bitcoin is:

All-or-nothing ledger

# Bitcoin is:

All-or-nothing ledger

Decentralized

# Bitcoin is:

All-or-nothing ledger

Decentralized

Programmable

**Bitcoin is:**

**Bitcoin is:**

Everyone sees everything

# Bitcoin is:

Everyone sees everything

Everyone executes code



# Bitcoin is:

Everyone sees everything

Everyone executes code

Everyone validates txs

Every teenager:

# Every teenager:

2001: can make a webpage

# Every teenager:

2001: can make a webpage

2010: can make a mobile app

# Every teenager:

2001: can make a webpage

2010: can make a mobile app

2014: can make a contract



**Alice**



**Bob**



Alice



Bob



iPod



Alice

\$100



Bob



iPod





Alice

\$100



Bob



iPod



Alice

\$100



Bob



iPod

ebay



Alice

\$100



Bob



iPod



Alice

ebay

\$100



Bob



iPod



ebay

\$100



Alice



Bob



iPod

ebay

\$100



Alice



Bob



iPod

ebay



Alice



iPod

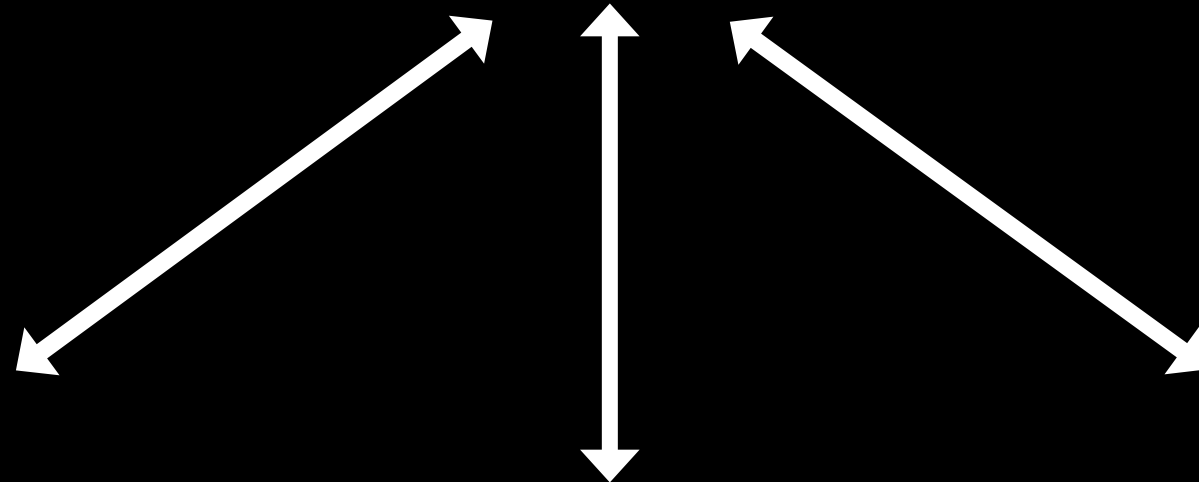


Bob

\$100



ebay



Alice

Bob





Alice

\$100



Bob



iPod



Alice

\$100



Bob



iPod

\$200



Alice

\$100

\$200



Bob



iPod

\$200



Alice

\$100



Bob



iPod



\$200



Alice

\$100



Bob



iPod

\$200

\$200



Alice

\$100



Bob



iPod



Alice

\$100



Bob



iPod



\$200  
\$200



Alice



Bob

\$100



iPod



\$200  
\$200



Alice



iPod



Bob

\$100

\$200  
\$200



Alice



iPod



Bob

\$100

\$200

\$200



Alice



iPod



Bob

\$100





Alice



iPod

\$200



Bob

\$100

\$200



# 1 transaction

## 2 inputs locked by 2 keys



\$200



\$200

2

AlicePubKey

BobPubKey

2

CHECKMULTISIG



\$200



\$200

2

AlicePubKey

BobPubKey

2

CHECKMULTISIG

Signatures required



\$200



\$200

2

AlicePubKey

BobPubKey

2

CHECKMULTISIG



Signatures required



\$200



\$200

2

AlicePubKey

BobPubKey

2

CHECKMULTISIG

Keys used

Signatures required

Alice Public Key



\$200

2

AlicePubKey

BobPubKey

2

CHECKMULTISIG

\$200



Keys used

Signatures required

Alice Public Key



\$200

2

AlicePubKey  
BobPubKey

\$200

2

CHECKMULTISIG



Keys used

Bob's Public Key

Alice and Bob must agree on how money is being spent



\$200



\$200

2

AlicePubKey

BobPubKey

2

CHECKMULTISIG

To unlock money both signatures must be present

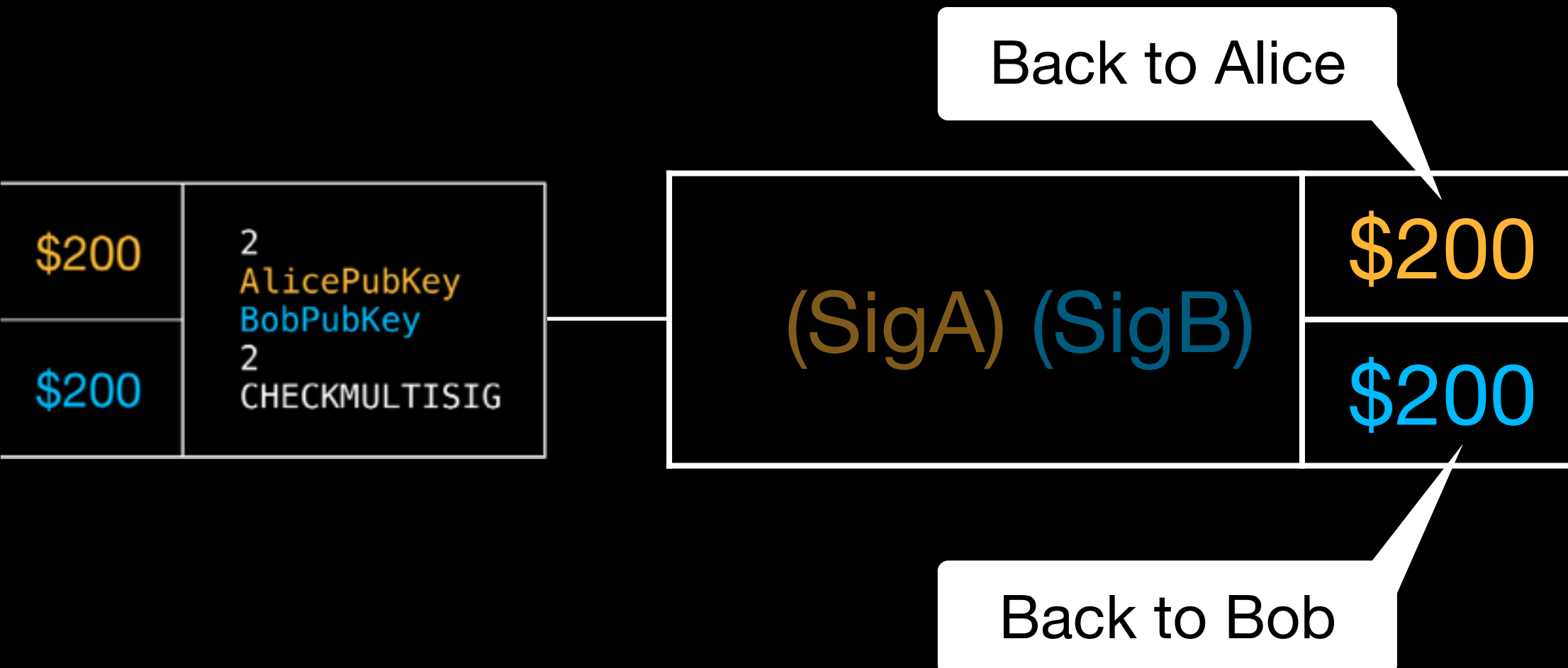


To unlock money both signatures must be present

Back to Alice



To unlock money both signatures must be present





Alice



iPod

SigA SigB



Bob

\$100



Alice has both signatures and sends the unlock transaction





Alice



iPod

SigA SigB



Bob

\$100



Alice



iPod

SigA SigB

\$200  
\$200

**Problem:**  
Alice can unlock  
\$200 any time she  
wants, but Bob  
cannot.



Bob

\$100

**Anti-troll measure**



MLAD





# Mutually



Mutually  
Assured



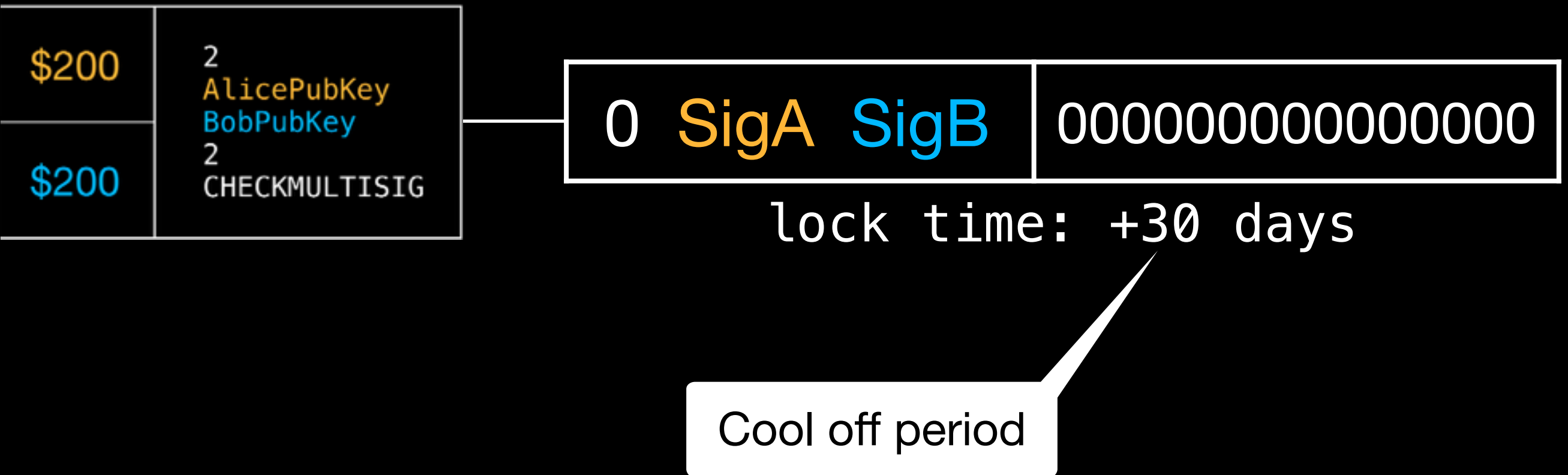
# Mutually Assured Destruction



Before starting business, Alice and Bob  
sign transaction that destroys all funds



Before starting business, Alice and Bob sign transaction that destroys all funds







Alice



iPod

SigA SigB



Bob

\$100



Alice



Bob



iPod

\$100

SigA SigB

**Payment + Unlock  
in one transaction**

\$400



Alice



iPod



Bob

\$100

\$100  
\$300



Alice



iPod



Bob

\$100



\$100

\$300



Alice



iPod



Bob

\$100





Alice



iPod

\$100



Bob

\$100

\$300

\$400



Alice



iPod

SigA



Bob

\$100

SigB

\$400



Alice



iPod



Bob

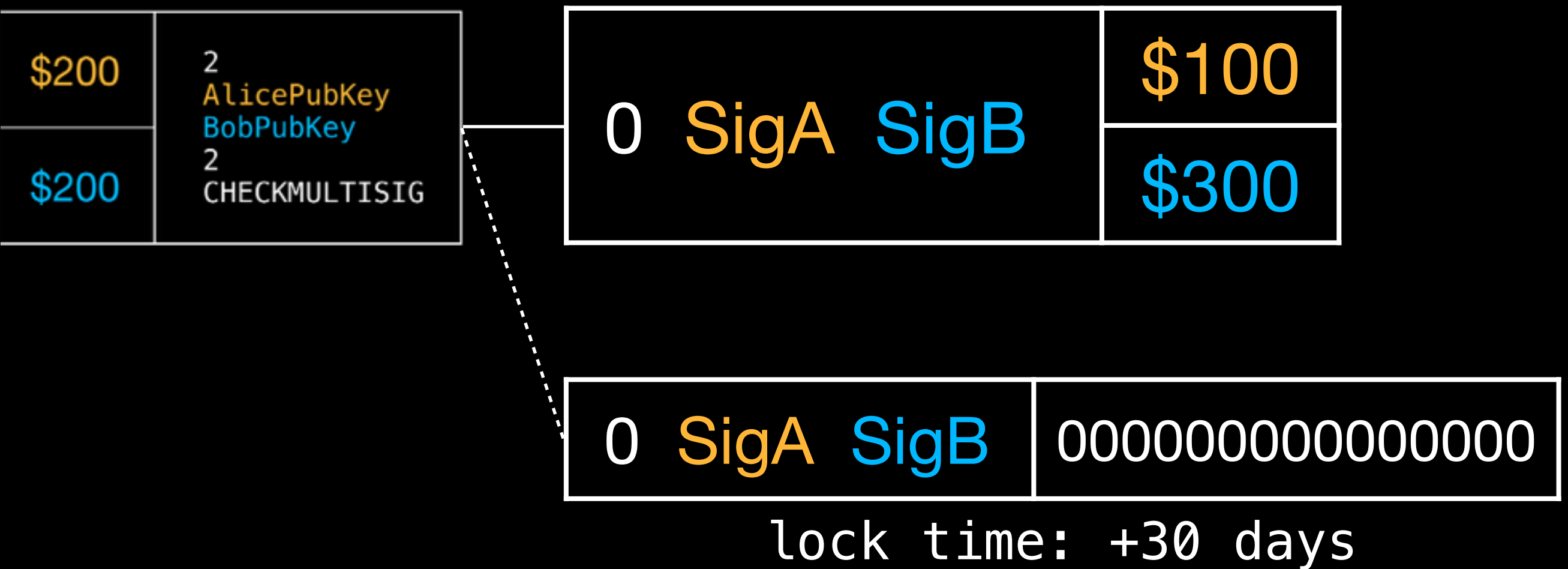
\$100

SigA SigB

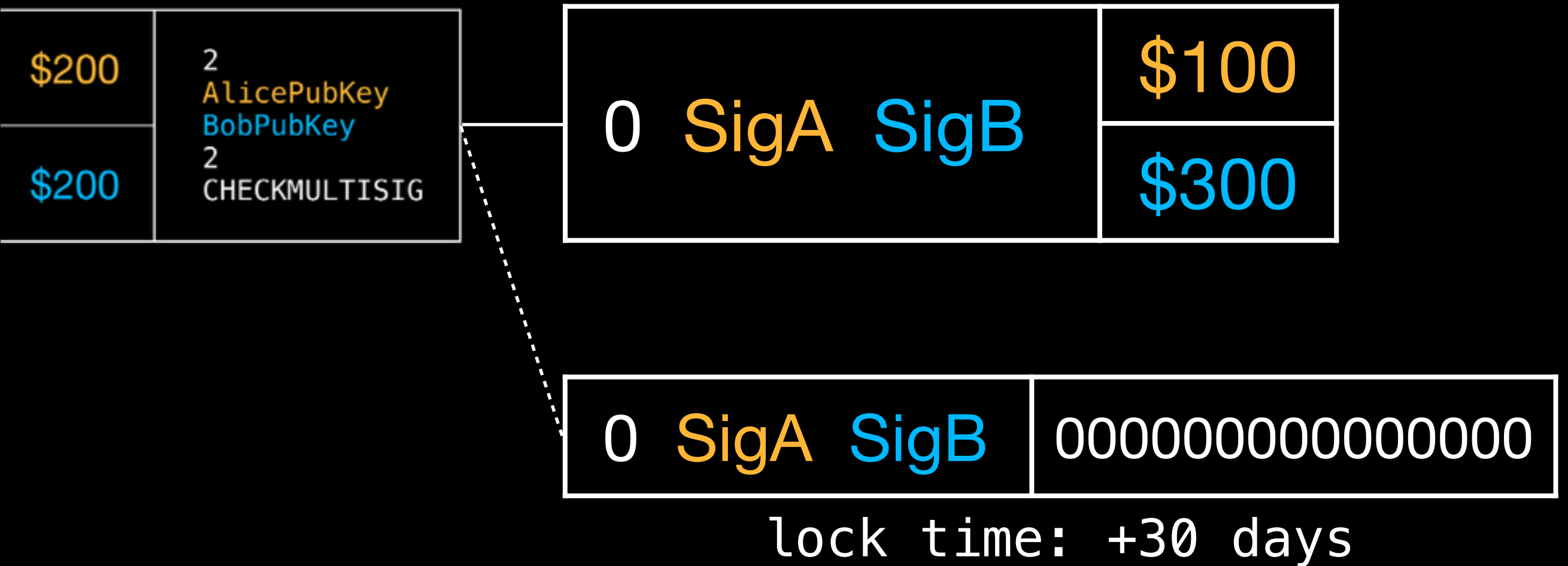
Alice pays and unlocks at the same time



Bob is motivated to unlock \$300 to not allow Alice to destroy his \$200



Once one tx is in blockchain,  
another one becomes invalid



Once one tx is in blockchain,  
another one becomes invalid





# Protocol:

# Protocol:

Alice and Bob choose keys.

# Protocol:

Alice and Bob choose keys.

They lock money with 2-of-2 multisig script.

# Protocol:

Alice and Bob choose keys.

They lock money with 2-of-2 multisig script.

They sign a +30d timelocked destruction tx.

# Protocol:

Alice and Bob choose keys.

They lock money with 2-of-2 multisig script.

They sign a +30d timelocked destruction tx.

Bob sends the product.

# Protocol:

Alice and Bob choose keys.

They lock money with 2-of-2 multisig script.

They sign a +30d timelocked destruction tx.

Bob sends the product.

Alice pays and unlocks money.

# Protocol:

Alice and Bob choose keys.

They lock money with 2-of-2 multisig script.

They sign a +30d timelocked destruction tx.

Bob sends the product.

Alice pays and unlocks money.

If money is not unlocked in time, either party can destroy money.



# Use cases:

# Use cases:

## Anonymous markets

# Use cases:

Anonymous markets

Freelance contracts

# Use cases:

Anonymous markets

Freelance contracts

Autonomous agents



<http://oleganza.com/bitcoin-epita-2014.pdf>