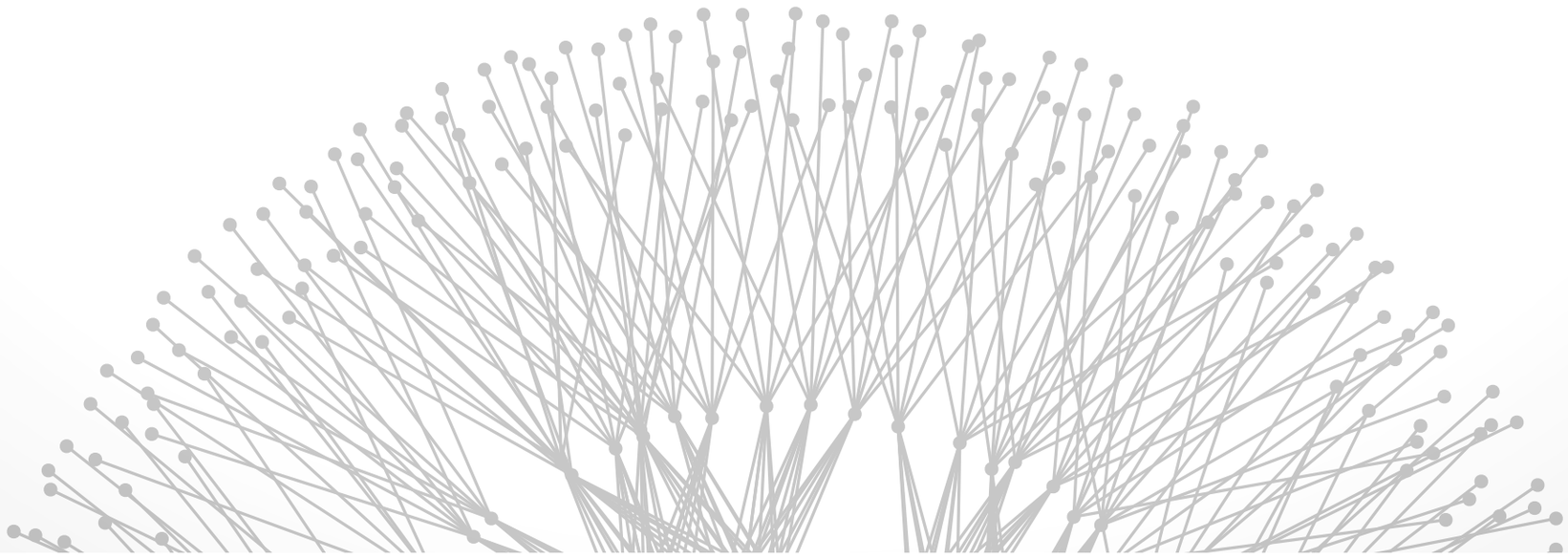
Blockchain + Networks (kinda)

UIUC CS 538 Fall 2017
Instructor: Mo Dong



Overview

Scalability challenges in blockchain systems

Payment networks and state channels

Other scalability directions and proposals

Scalability Challenge

BTC ETH Visa X 10

Transaction per second

Scalability Challenge

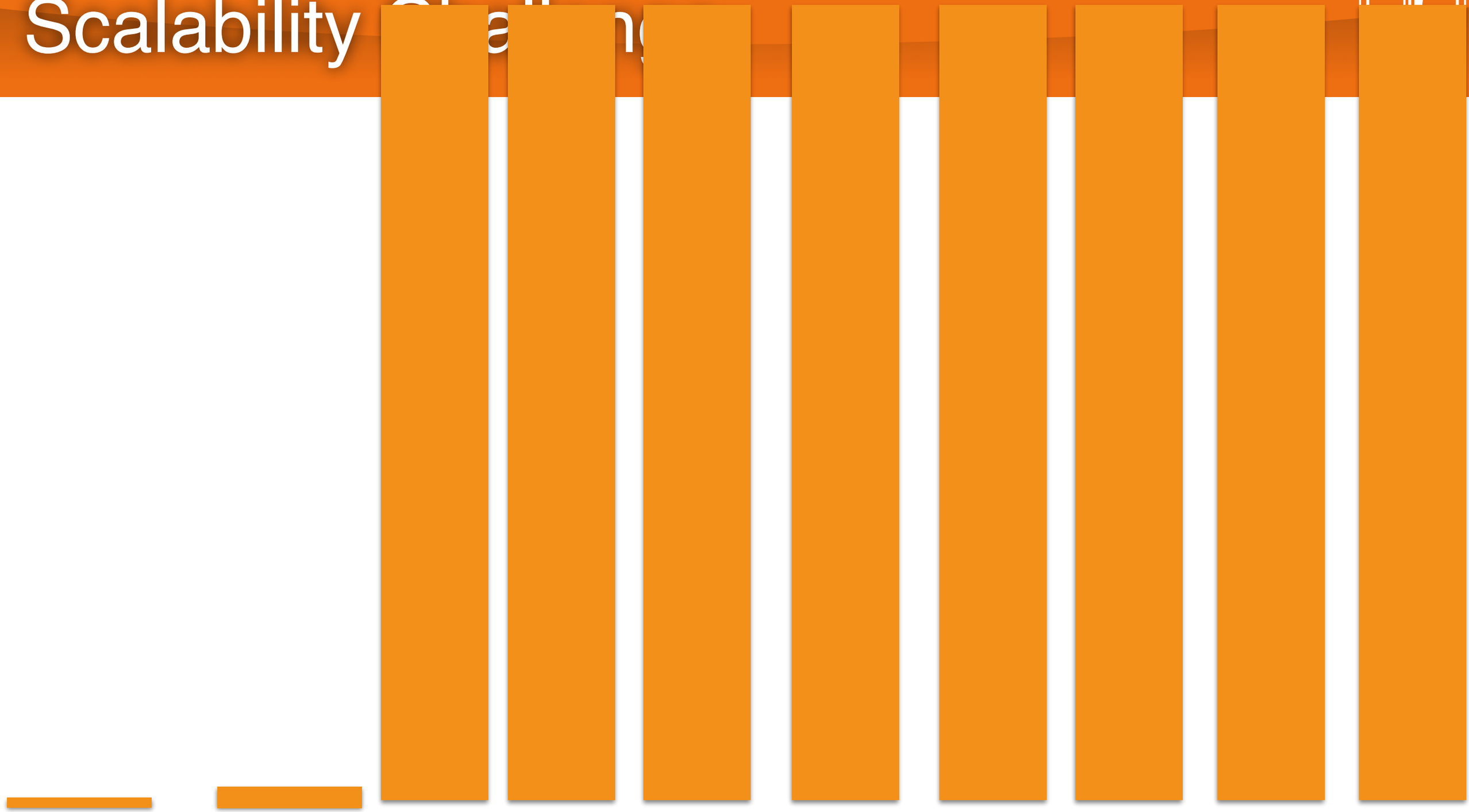
BTC ETH Visa X 10

Transaction per second

Scalability Challenge

Transaction per second

Scalability Challenge



Transaction per second

Why?

BTC as an example…

It’s a rabbit hole
but let’s dig it a little bit
until it is not fun…

BTC as an example…

It’s a rabbit hole
but let’s dig it a little bit
until it is not fun…

Scalability =

BTC as an example…

It’s a rabbit hole
but let’s dig it a little bit

until it is not fun…

Scalability =

Block size / Block Time

BTC as an example…

It’s a rabbit hole

but let’s dig it a little bit

until it is not fun…

Scalability =

Block size / Block Time

1Mb

BTC as an example…

It’s a rabbit hole
but let’s dig it a little bit

until it is not fun…

Scalability =

Block size / Block Time

1Mb 10min

Block Time

Mining Mechanism
Proof of Work (PoW)

H(Block3, new TX, nounce) < 0x0000aef1e….

Solution

Difficulty

Control block time

Block Time

Block Time

Avoid short-term fork and orphaned chain

Block Time

Avoid short-term fork and orphaned chain

- Orphan blocks make miner lose $$$

Block Time

Avoid short-term fork and orphaned chain

- Orphan blocks make miner lose $$$
- Any possible mitigation?

Block Time

Avoid short-term fork and orphaned chain

- Orphan blocks make miner lose $$$
- Any possible mitigation?
- Reward orphan! “Uncle” in Ethereum pushes down block time to ~10s

Block Time

Avoid short-term fork and orphaned chain

- Orphan blocks make miner lose $$$
- Any possible mitigation?
- Reward orphan! “Uncle” in Ethereum pushes down block time to ~10s
- Why not lower??

Block Time

Block Time

Security vs block time tradeoff

Block Time

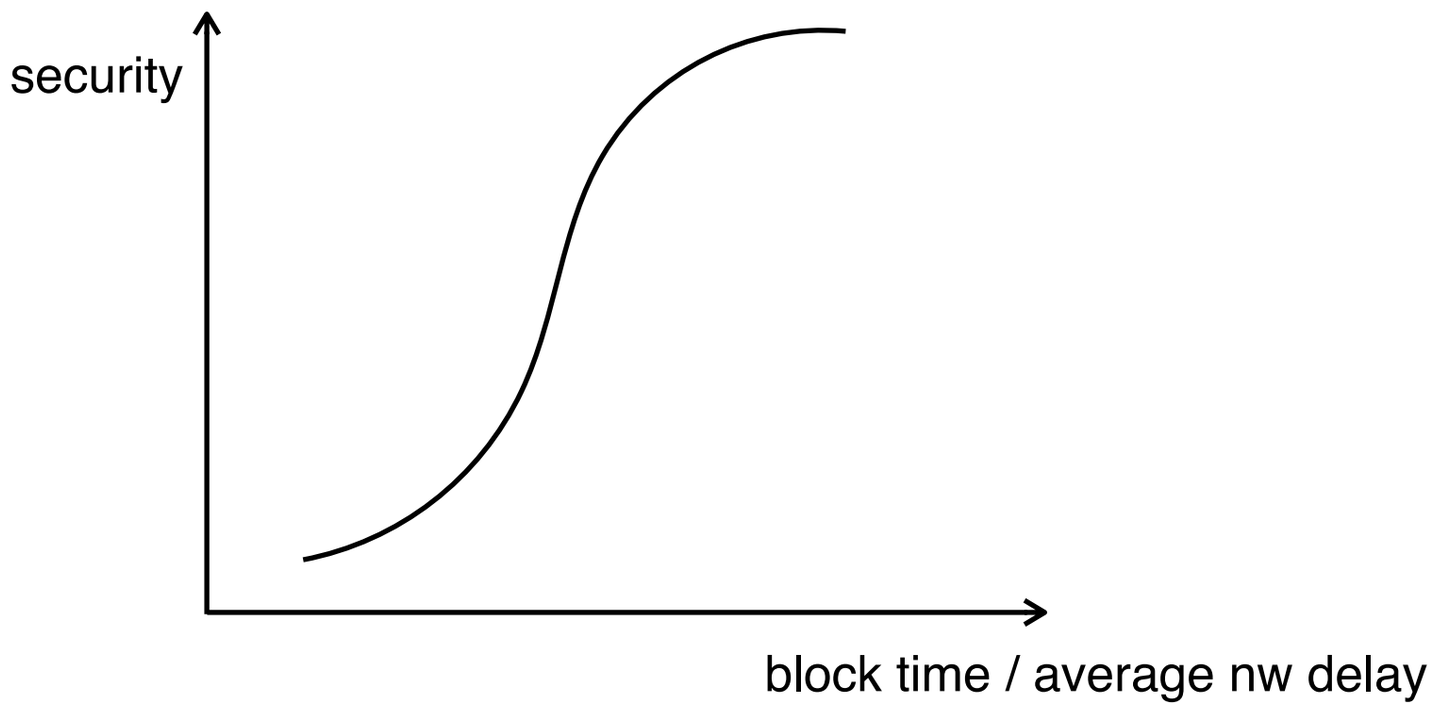
Security vs block time tradeoff

- Intuitively: the shorter the block time, the harder it is to make the valid block propagate to the majority of the network

Block Time

Security vs block time tradeoff

- Intuitively: the shorter the block time, the harder it is to make the valid block propagate to the majority of the network
- Formally, blockchain assumes synchronize network communication



Block Time

Bottom line

For POW based consensus, ~10s block time is pretty much the limit

1MB Block Size

How did we end up with 1MB blocks anyway?

1MB Block Size

How did we end up with 1MB blocks anyway?

- Once up on a time, block was BIG (32M)

1MB Block Size

How did we end up with 1MB blocks anyway?

- Once up on a time, block was BIG (32M)
- Satoshi is a(a bunch of?) really weird guy/gal/alien and one day, without explanation:

fix openssl linkage problems,

```
disable minimize to tray on Linux because it has too many problems including a CPU peg bug

git-svn-id: https://bitcoin.svn.sourceforge.net/svnroot/bitcoin/trunk@103 1a98c847-1fd6-4fd8-948a-caf3550aa51b
```

master v0.14.1 ... v0.3.10

cleanup,

```
catch some recoverable exceptions and continue
-- version 0.3.12 release

git-svn-id: https://bitcoin.svn.sourceforge.net/svnroot/bitcoin/trunk@148 1a98c847-1fd6-4fd8-948a-caf3550aa51b
```

master v0.14.1 ... v0.3.12

1MB Block Size

How did we end up with 1MB blocks anyway?

- Once up on a time, block was BIG (32M)
- Satoshi is a(a bunch of?) really weird guy/gal/alien and one day, without explanation:

```
15   class CKeyItem;
16
17 + static const unsigned int MAX_SIZE = 0x02000000;
18   +static const unsigned int MAX_BLOCK_SIZE = 1000000;
19    static const int64 COIN = 100000000;
20    static const int64 CENT = 1000000;
21    static const int COINBASE_MATURITY = 100;
1419 +    int nHeight = pindexPrev->nHeight+1;
1420 +
1421 +    // Check size
1422 +    if (nHeight > 79400 && ::GetSerializeSize(*this, SER_NETWORK) > MAX_BLOCK_SIZE)
1423 +        return error("AcceptBlock() : over size limit");
1424 +
1425 +    // Check that it's not full of nonstandard transactions
1426 +    if (nHeight > 79400 && GetSigOpCount() > MAX_BLOCK_SIGOPS)
1427 +        return error("AcceptBlock() : too many nonstandard transactions");
```

1MB Block Size

How did we end up with 1MB blocks anyway?

- Once up on a time, block was BIG (32M)
- Satoshi is a(a bunch of?) really weird guy/gal/alien and one day, without explanation:

1MB Block Size

How did we end up with 1MB blocks anyway?

- Once up on a time, block was BIG (32M)
- Satoshi is a(a bunch of?) really weird guy/gal/alien and one day, without explanation:
- Just like that, block size became 1MB

1MB Block Size

How did we end up with 1MB blocks anyway?

- Once up on a time, block was BIG (32M)
- Satoshi is a(a bunch of?) really weird guy/gal/alien and one day, without explanation:
- Just like that, block size became 1MB
- Problem is no one had a clue why….

1MB Block Size

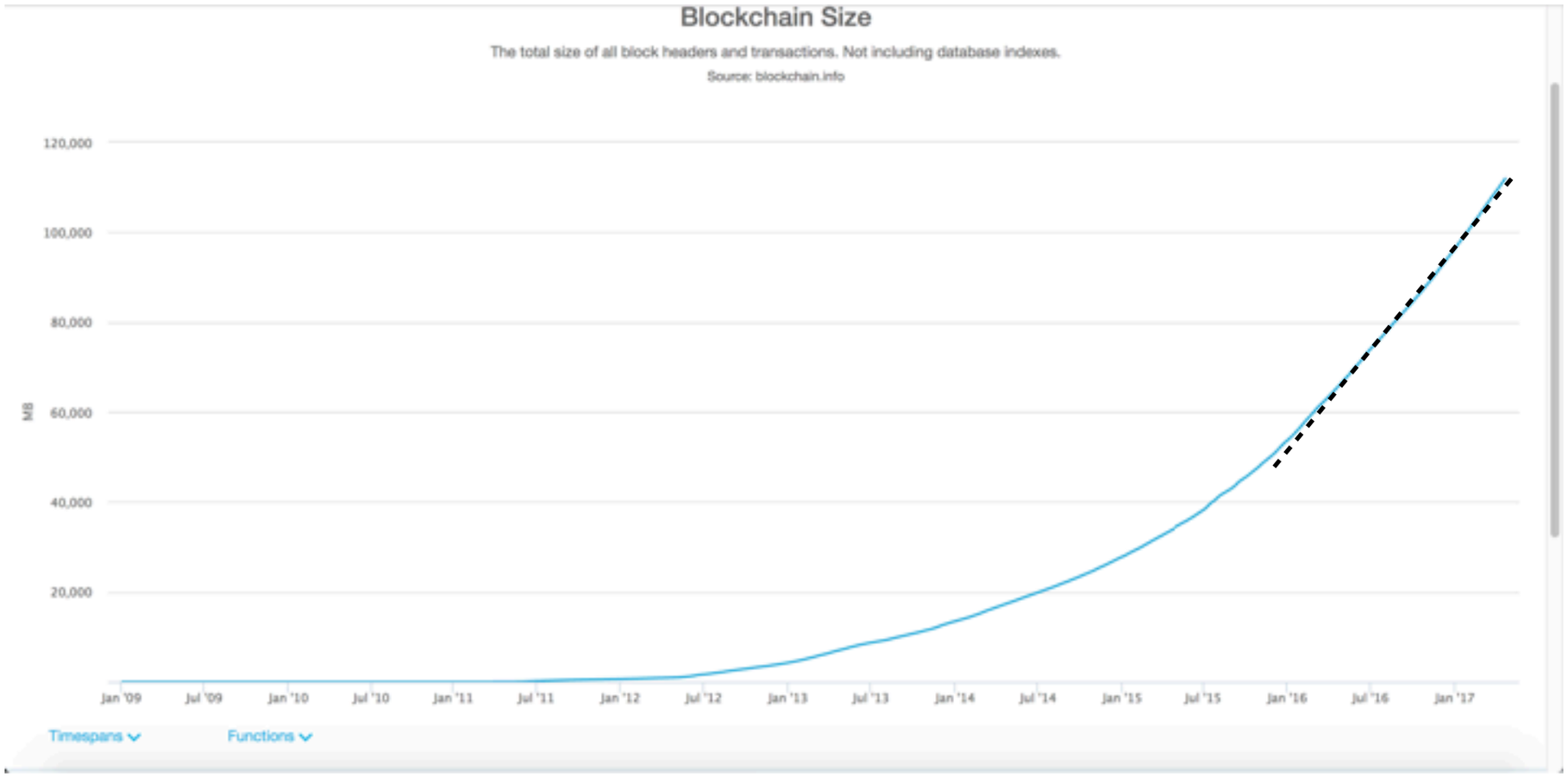
How did we end up with 1MB blocks anyway?

- Once up on a time, block was BIG (32M)
- Satoshi is a(a bunch of?) really weird guy/gal/alien and one day, without explanation:
- Just like that, block size became 1MB
- Problem is no one had a clue why….
- Let’s all guess and justify….

1MB Block Size

Possible Reasons

- Explicit growth control



1MB Block Size

Possible Reasons

- Explicit growth control for system health
  - Storage: 153G and growing
  - Compute: validation of the transactions
  - Network: bandwidth to tx and rx block data
  - Larger block require higher end hardware to run full node —> less full node in the system and therefore, less “network effect”

1MB Block Size

Possible Reasons

- Incentivize the miner
  - Bigger block = higher misc cost (network, storage, validation)
- Smaller block = more backlog and higher fee

1MB Block Size

Possible Reasons

- Security
  - Bigger block = longer propagation delays
  - Therefore bigger block = more orphan transactions
  - percentage of hash rate goes to orphan is REALLY wasted

Despite all the justifications

Block size / Block Time

1Mb 10min

https://www.facebook.com/743378802479548/photos/a.743768985773863.1073741828.743378802479548/829376217213139/?type=3&theater

Why can’t we just up the block size and see?

Hard Fork

Hard Fork

Please, refer this term from now on as “You Know What”

Hard Fork

Please, refer this term from now on as “You Know What”

Or at the very least, Hard F*rk

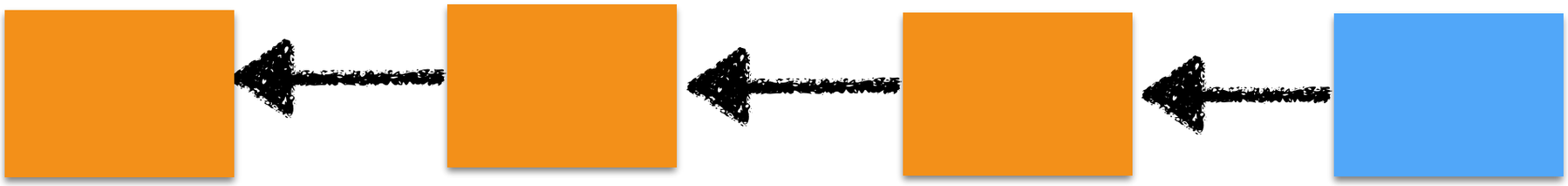
Hard F*rk

Hard F*rk

Hard F*rk

Hard F*rk

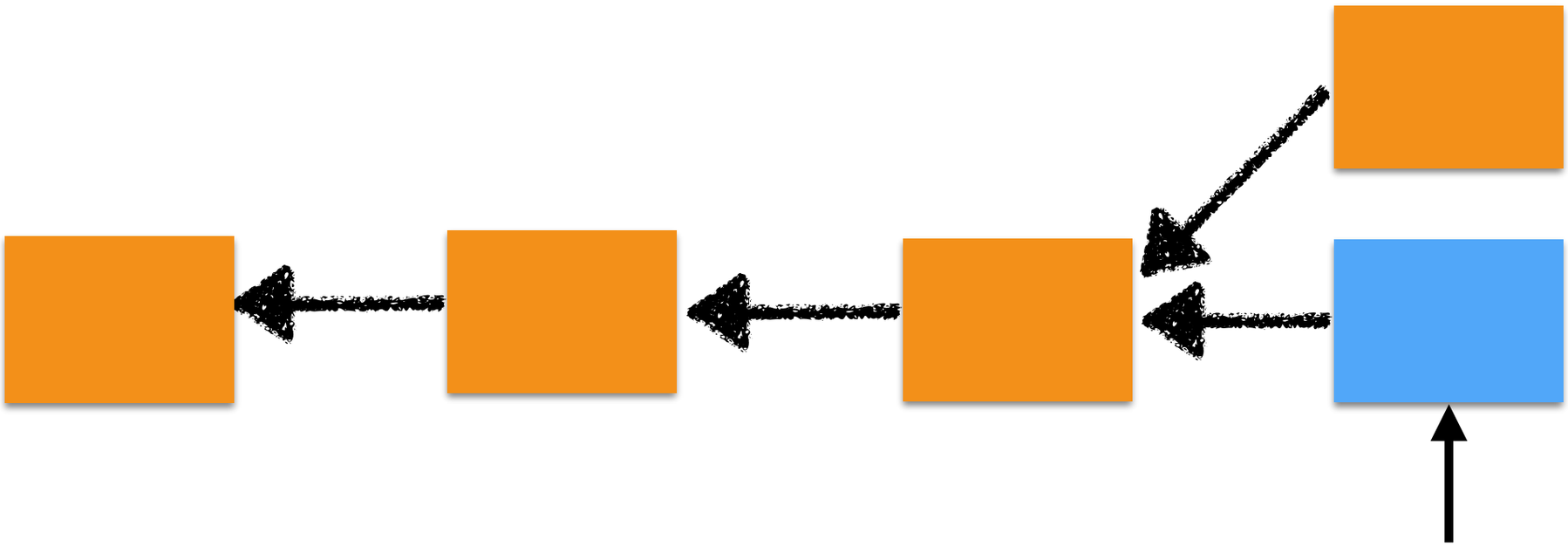
Hard F*rk



Hard F*rk

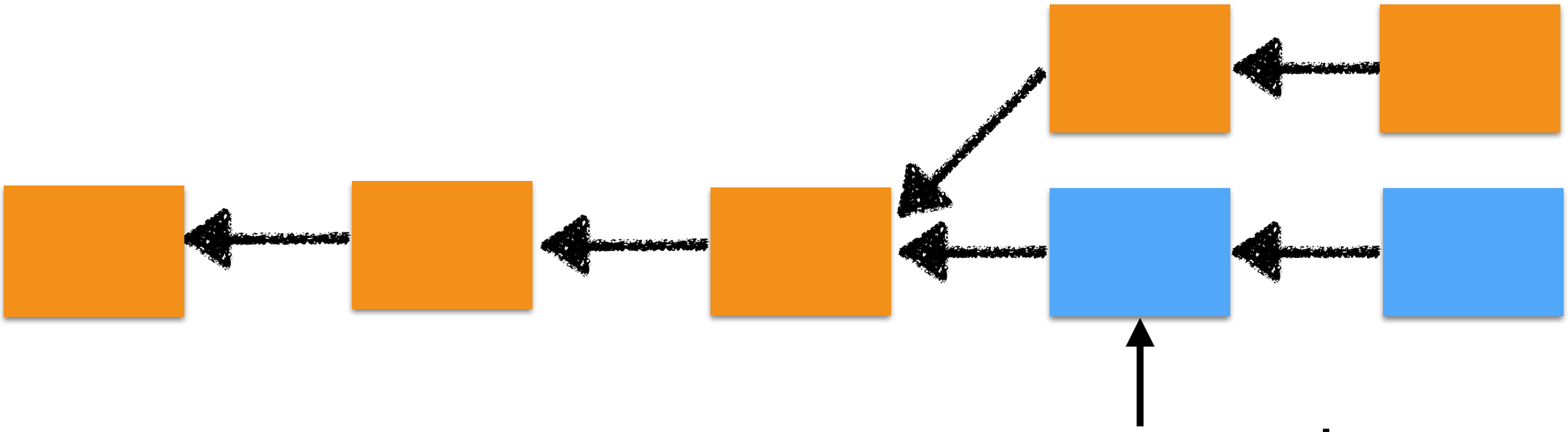
consensus rule
change
e.g. block size
change

Hard F*rk



consensus rule
change
e.g. block size
change

Hard F*rk



consensus rule
change
e.g. block size
change

Hard f*rk can cause permanent chain split

Chain split kills network effect and confidence/pure ideology of “unalterable ledger”

More practically, harm security, e.g. replay attack

Small Debate

Hard F*rk or Not?

Global Consensus without Trust

Global Consensus without Trust

Unalterable shared state

Global Consensus without Trust

Unalterable shared state

Hard to change protocol or even fix bugs

Global Consensus without Trust

Unalterable shared state

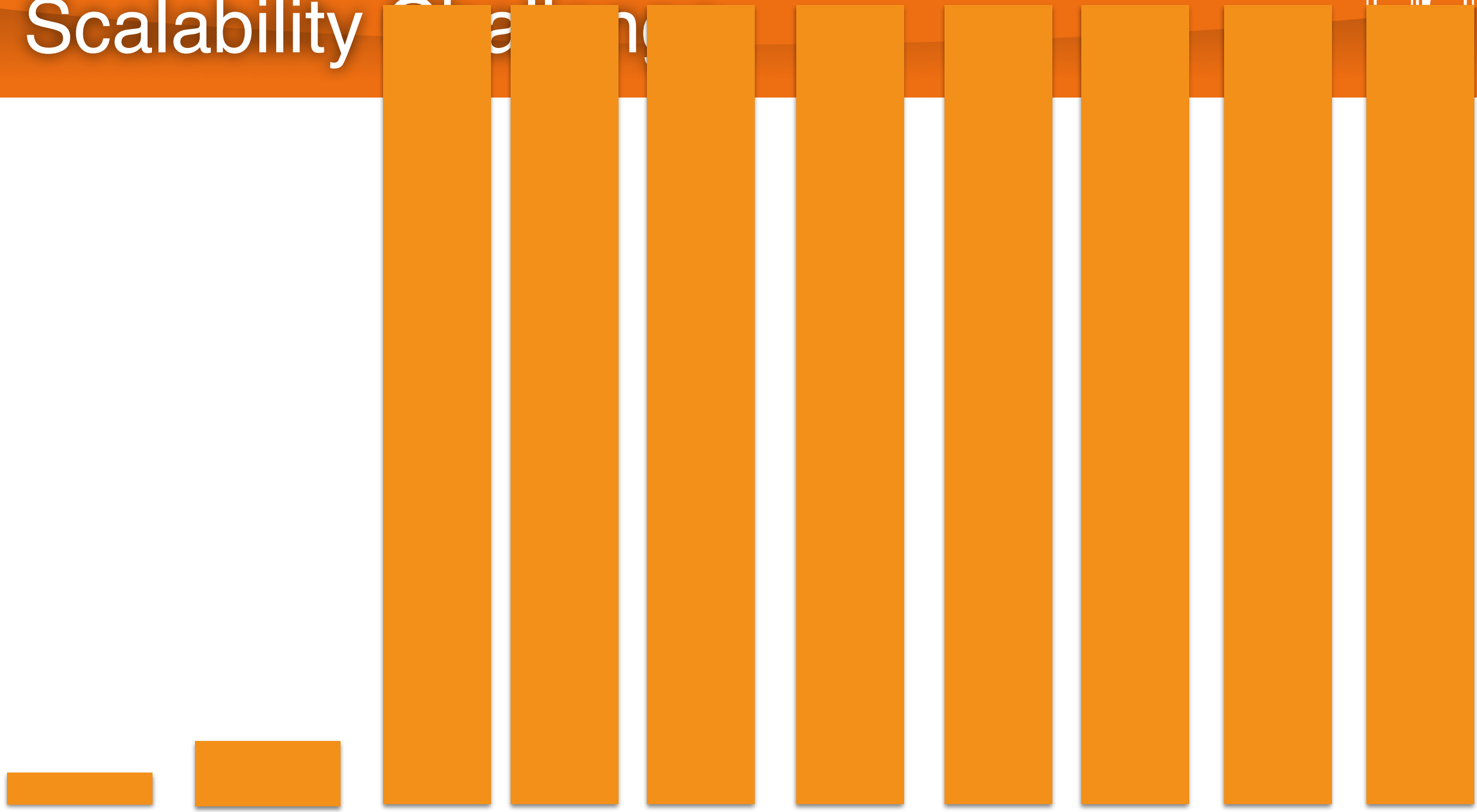
Hard to change protocol or even fix bugs

IMHO, Hard Fork is not scary at all

Forget about all these debates

So, let’s just say we put 32MB block in place (which is almost impossible)

Scalability Challenge



Transaction per second

No hope for mass adoption

Buy an ice cream, wait two hour

Transfer $10 for lunch, pay $1.5 fee

Store a 500 element hash map, pay $10

Play a chess game pay $50

Develop a smart contract? Buy 10PB SSD RAID

No hope for mass adoption

And btw, total energy consumption: O(n^2)

ALL IS LOST

Not so fast

Offchain State Channels and Networks

Repeatedly transfer small amount
of BTC without using
on-chain transaction every time

Payment Channel

Payment Channel

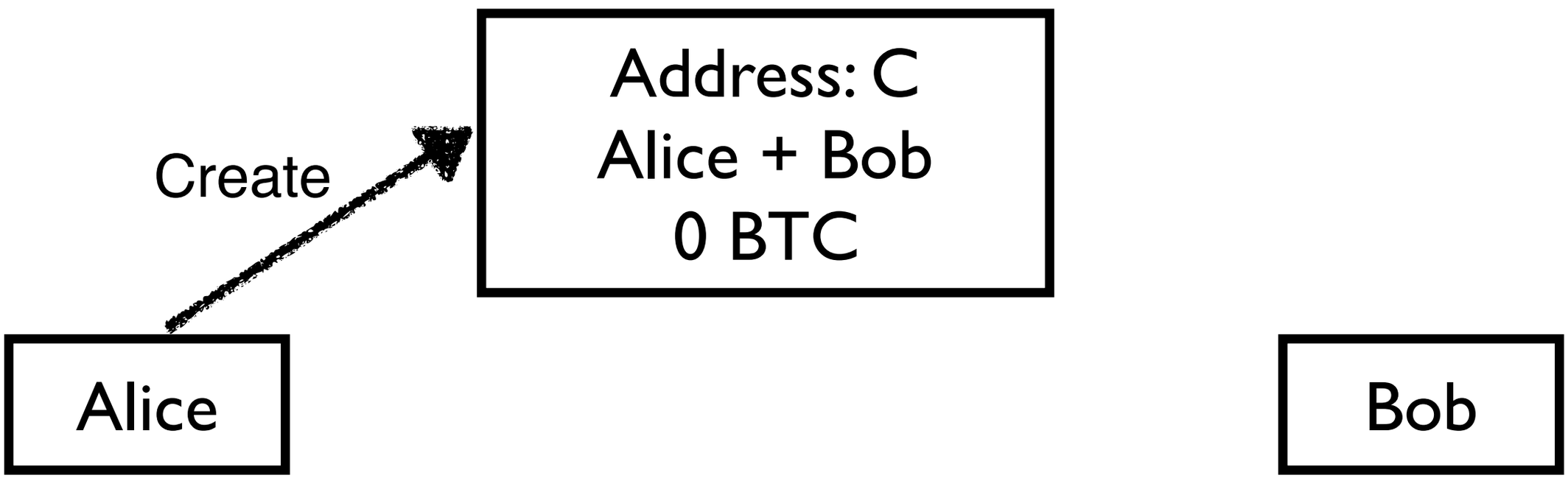
Unidirectional Channel

Alice

Bob

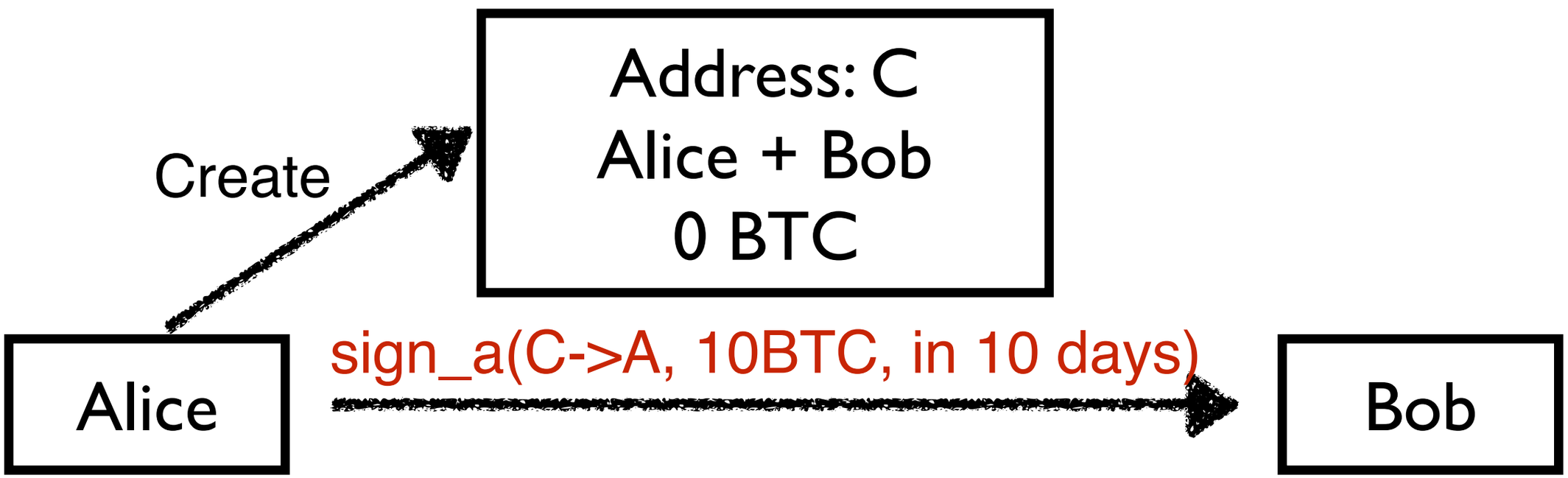
Payment Channel

Unidirectional Channel
Time-Locked Contract (TLC)



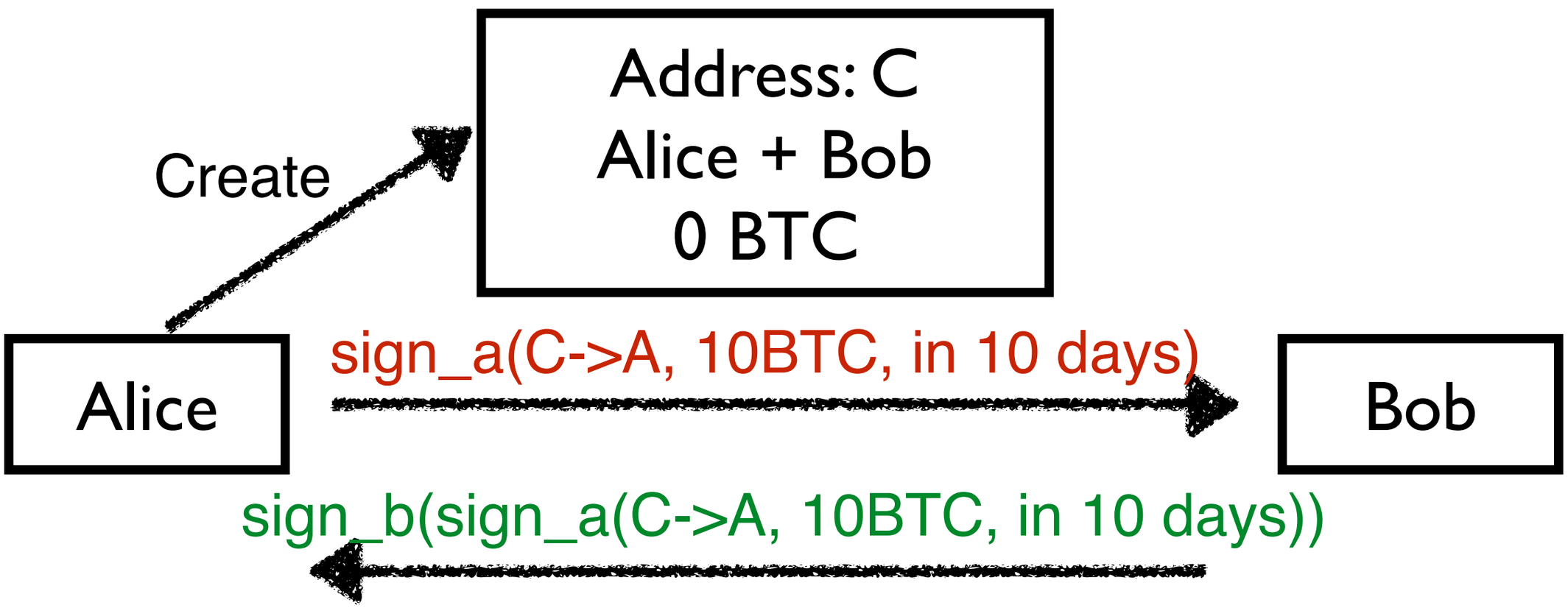
Payment Channel

Unidirectional Channel
Time-Locked Contract (TLC)



Payment Channel

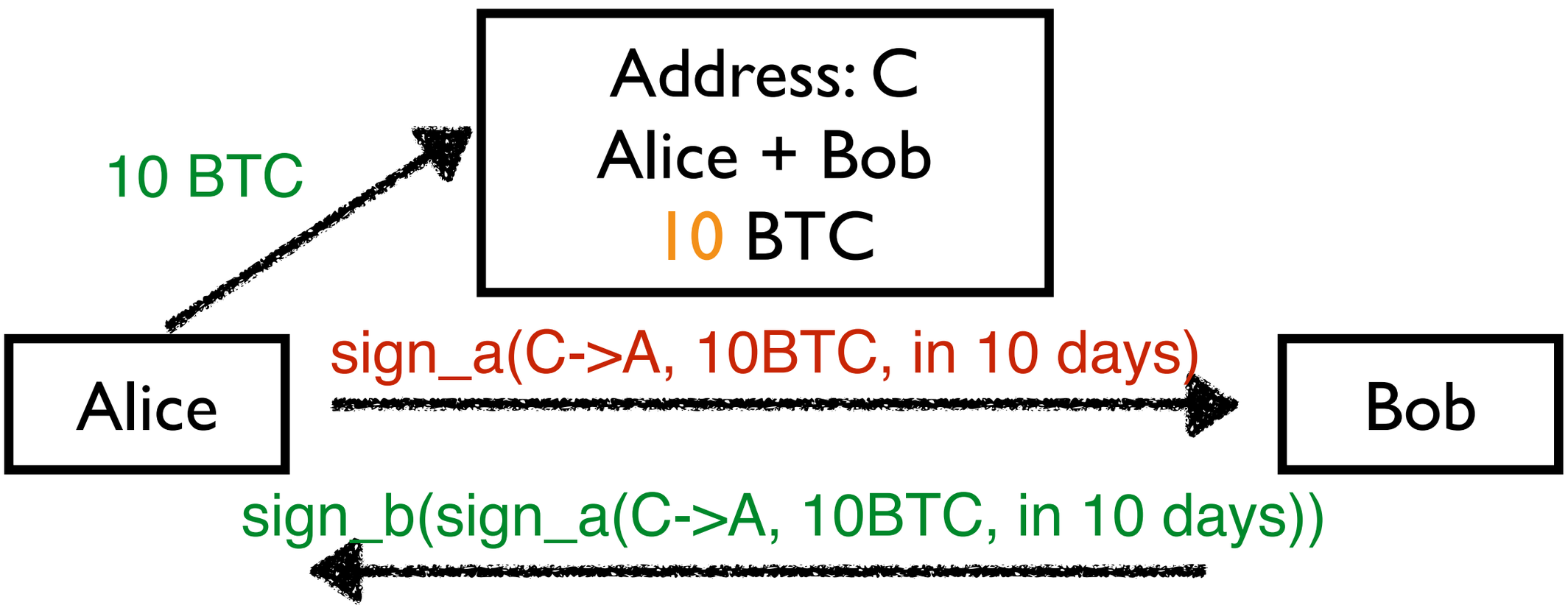
Unidirectional Channel
Time-Locked Contract (TLC)



Payment Channel

Unidirectional Channel

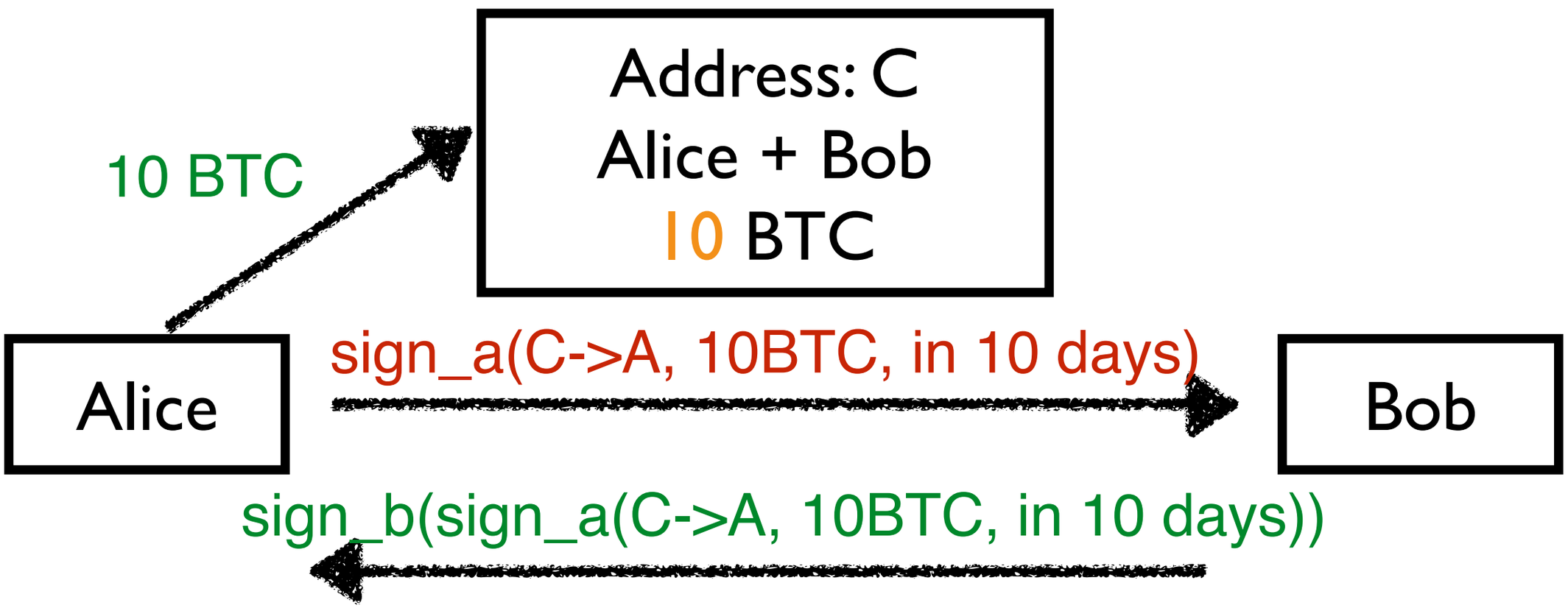
Time-Locked Contract (TLC)



Payment Channel

Unidirectional Channel

Time-Locked Contract (TLC)



2 on-chain transactions

Payment Channel

Send Bob one BTC

Address: C
Alice + Bob
10 BTC

Alice

Bob

Payment Channel

Send Bob one BTC

Address: C
Alice + Bob
10 BTC

Alice

sign_Alice
C->A, 9
C->B, 1

Bob

Payment Channel

Send Bob one BTC

Address: C
Alice + Bob
10 BTC

Send Bob
another BTC

Alice

sign_Alice
C->A, 9
C->B, 1

Bob

Payment Channel

Address: C
Alice + Bob
10 BTC

Send Bob one BTC

Send Bob another BTC

Alice

sign_Alice
C->A, 9
C->B, 1

sign_Alice
C->A, 8
C->B, 2

Bob

Payment Channel

Address: C
Alice + Bob
10 BTC

Offchain!!

Send Bob one BTC

Send Bob another BTC

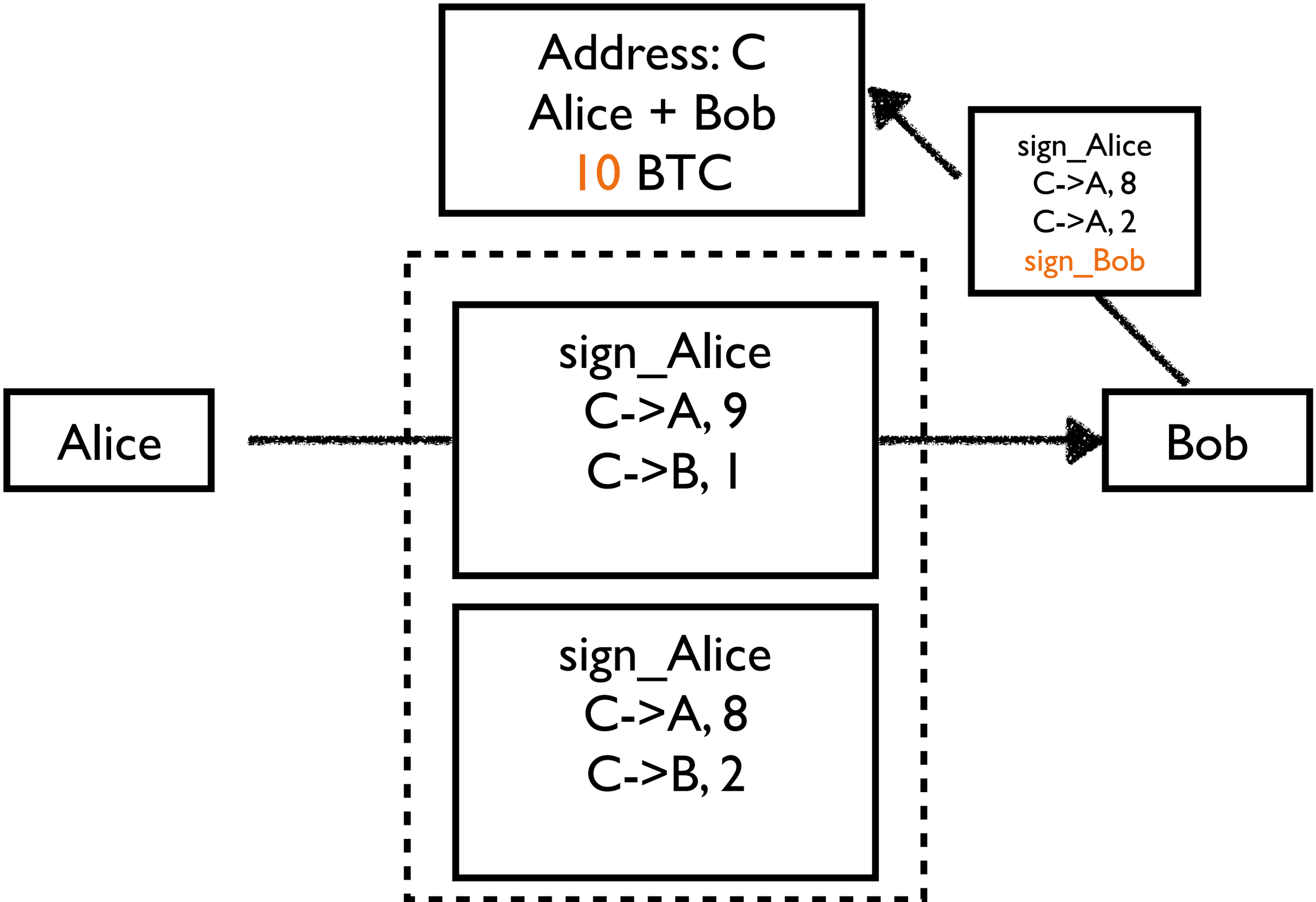
Alice

sign_Alice
C->A, 9
C->B, 1

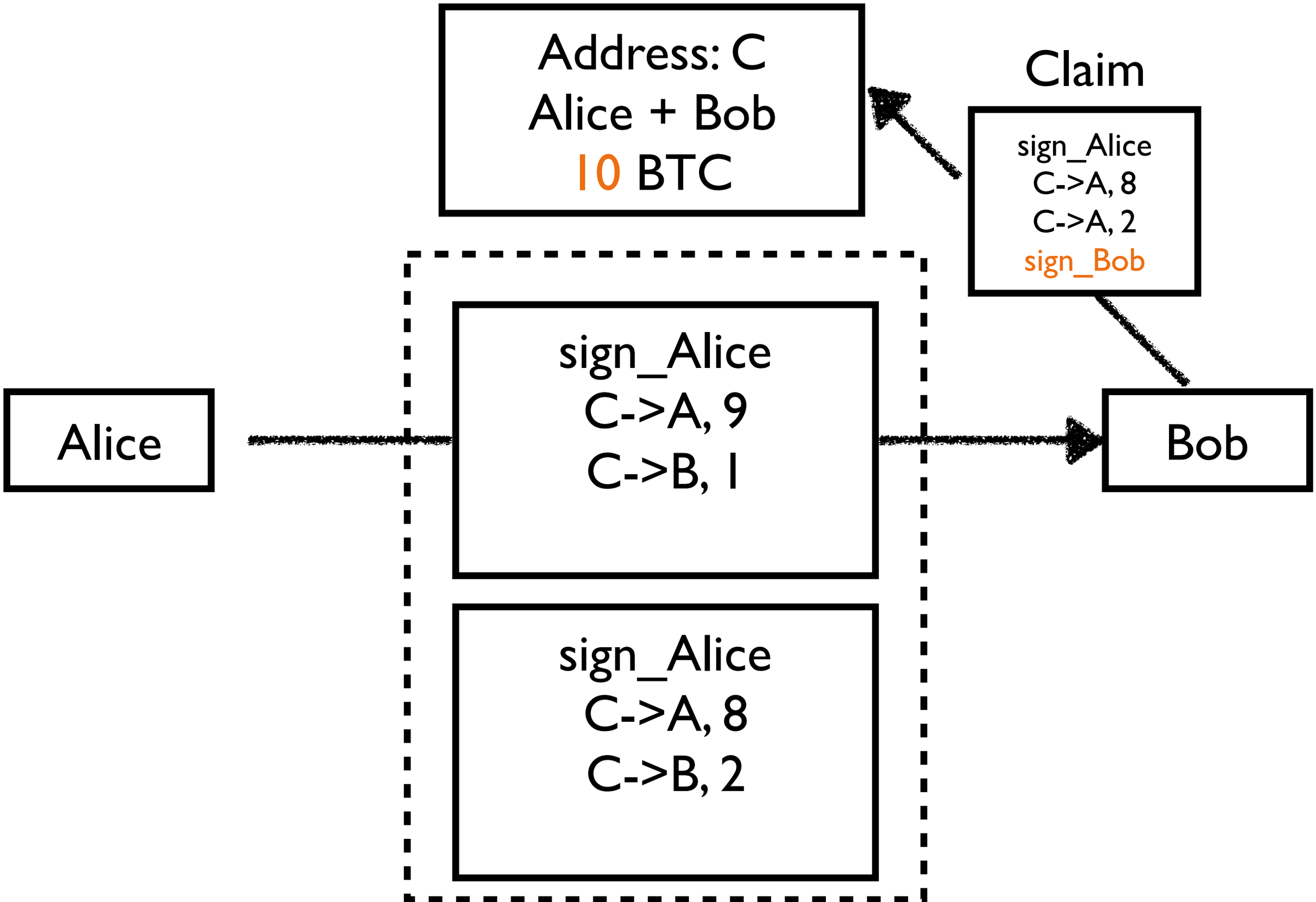
sign_Alice
C->A, 8
C->B, 2

Bob

Payment Channel

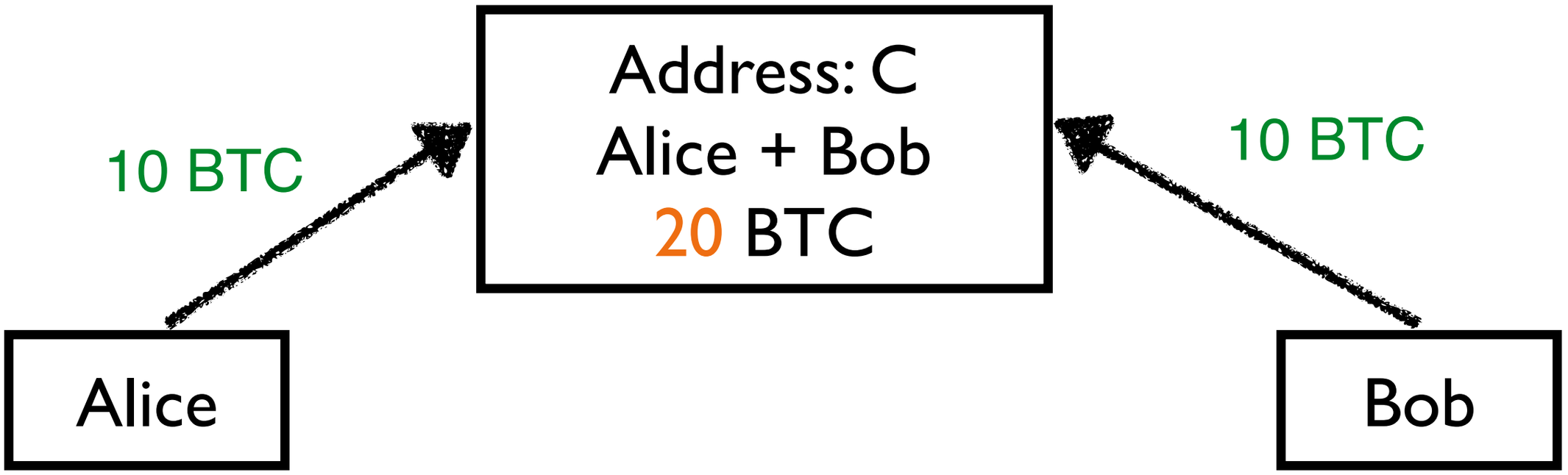


Payment Channel



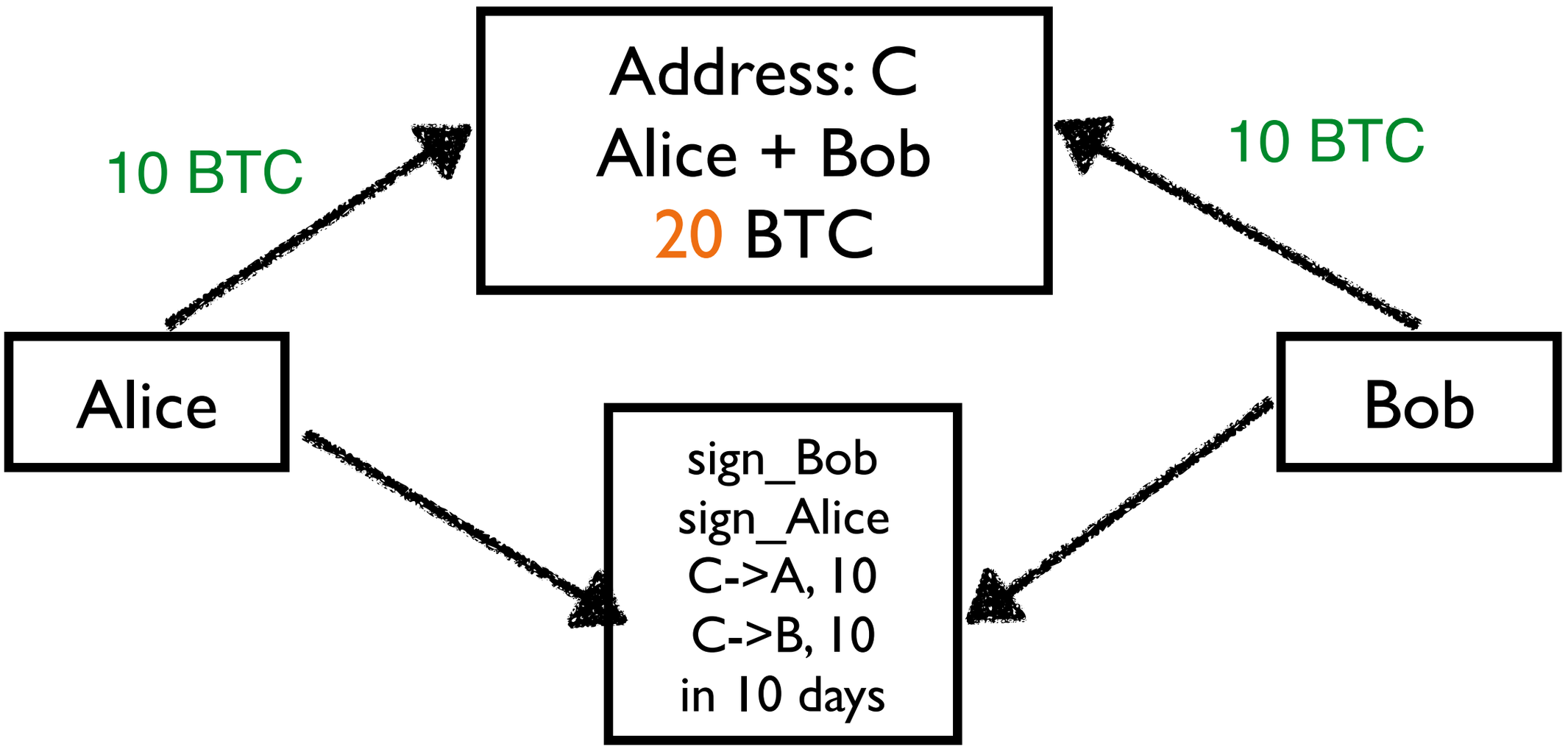
Payment Channel

Bidirectional Channel



Payment Channel

Bidirectional Channel



Payment Channel

Address: C
Alice + Bob
20 BTC

Alice

Bob

Payment Channel

Address: C
Alice + Bob
20 BTC

Alice

sign_Alice
C->A, 11
C->B, 9

Bob

Payment Channel

Address: C
Alice + Bob
20 BTC

Alice

sign_Alice
C->A, 11
C->B, 9

Bob

sign_Bob
C->A, 10
C->B, 10

Payment Channel

Address: C
Alice + Bob
20 BTC

Bob likes this more

sign_Alice
C->A, 11
C->B, 9

Alice

Bob

sign_Bob
C->A, 10
C->B, 10

Payment Channel

Address: C
Alice + Bob
20 BTC

Bob likes this more

Alice

sign_Alice
C->A, 11
C->B, 9
in 9 days(SeqNo1)

Bob

But Alice has final say

sign_Bob
C->A, 10
C->B, 10
in 8 days (SeqNo2)

Payment Channel

Address: C
Alice + Bob
20 BTC

pre

What's the down side of bi-directional channels?

sign_Bob
C->A, 10
C->B, 10
in 8 days (SeqNo)

Payment Channel

Address: C
Alice + Bob
20 BTC

pre

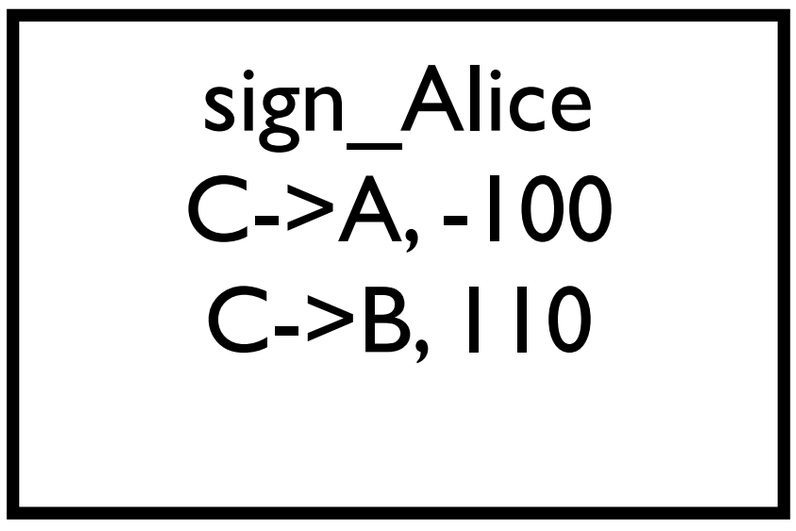
What's the down side of bi-directional channels?
Shortened lifetime of channel

sign_Bob
C->A, 10
C->B, 10
in 8 days (SeqNo)

Payment Channel

Bidirectional channel can be built using two unidirectional channels in **a single contract**

Balance can go negative in one direction



Payment Channel

Bidirectional channel can be built using two unidirectional channels in **a single contract**

Balance can go negative in individual directions, get settled later

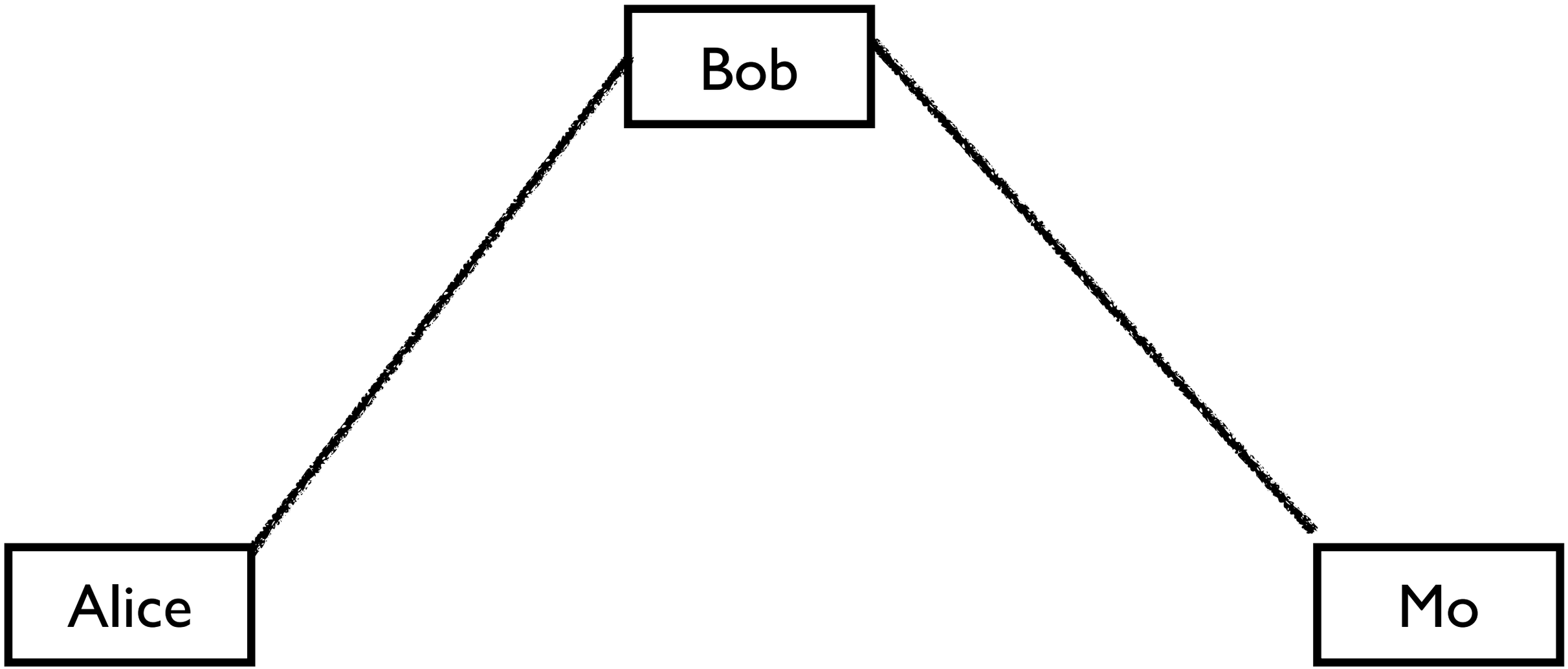
sign_Alice	sign_Bob
C->A, -100	C->A,200
C->B, 110	C->B,0

Settlement Guidelines

Do not play too close to the time lock

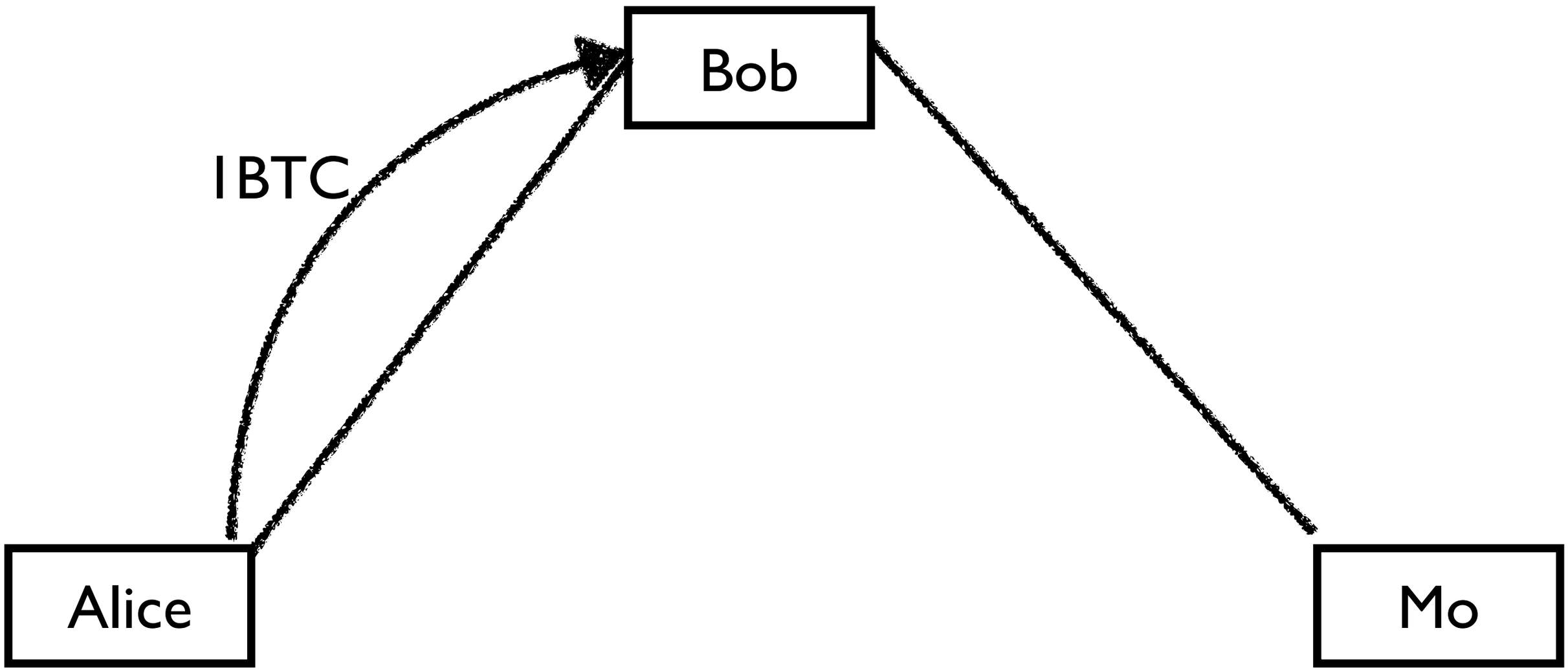
Payment Networks

Alice wants to pay Mo 1BTC



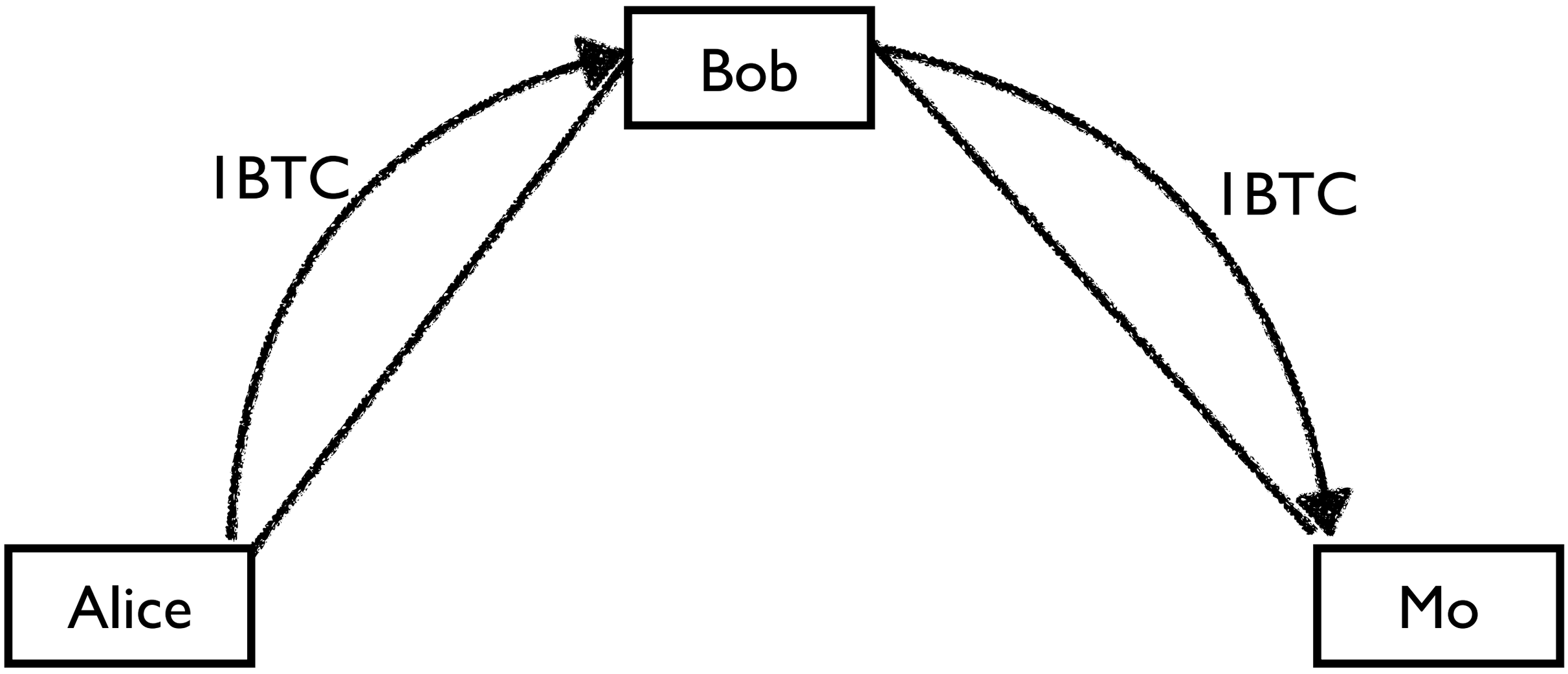
Payment Networks

Alice wants to pay Mo 1BTC



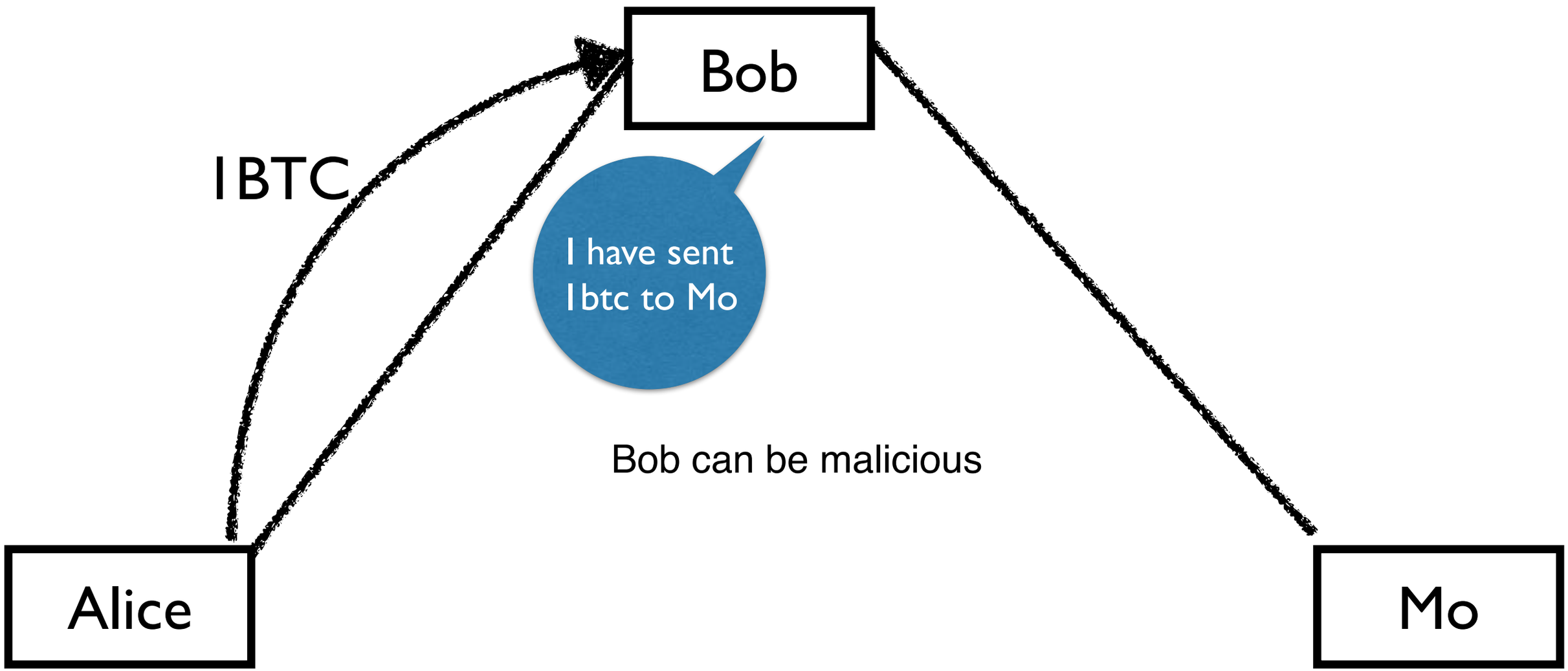
Payment Networks

Alice wants to pay Mo 1BTC



Payment Networks

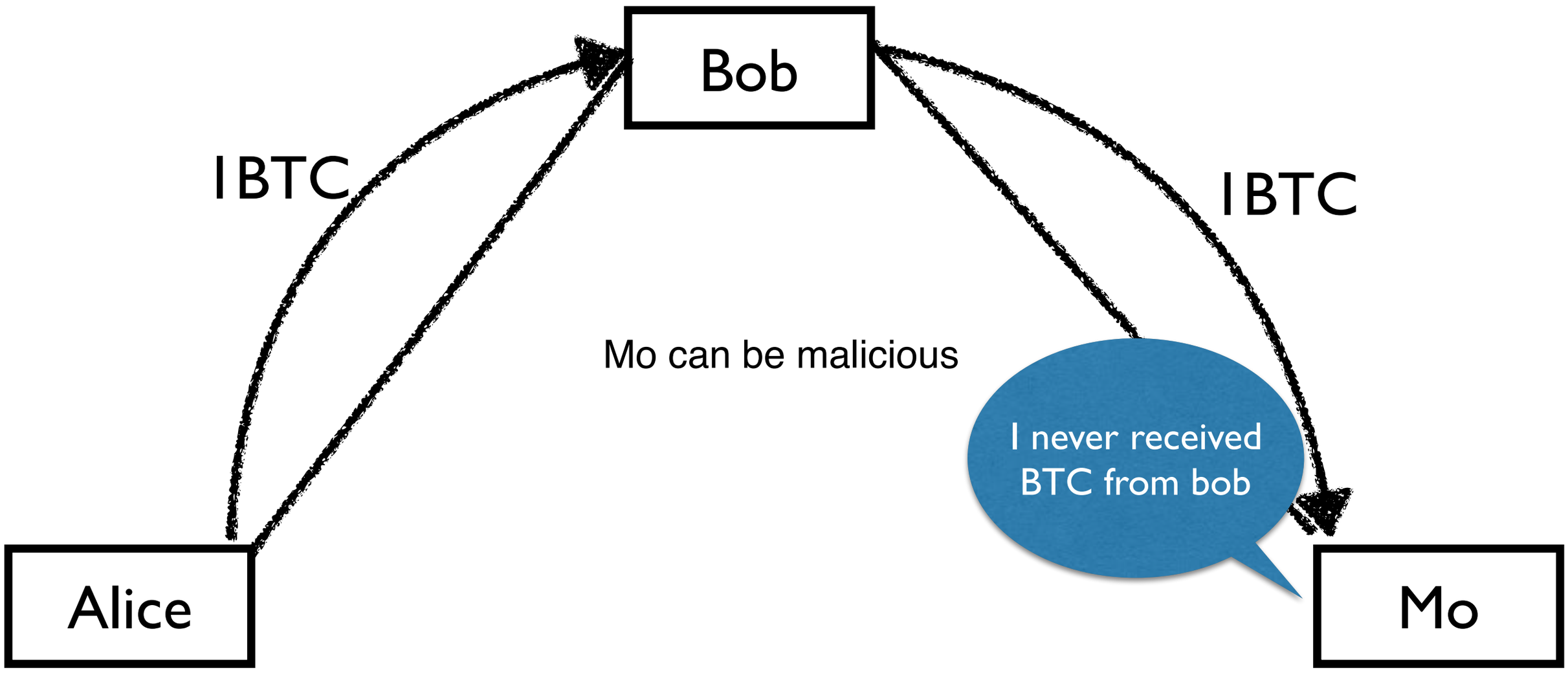
Alice wants to pay Mo 1BTC



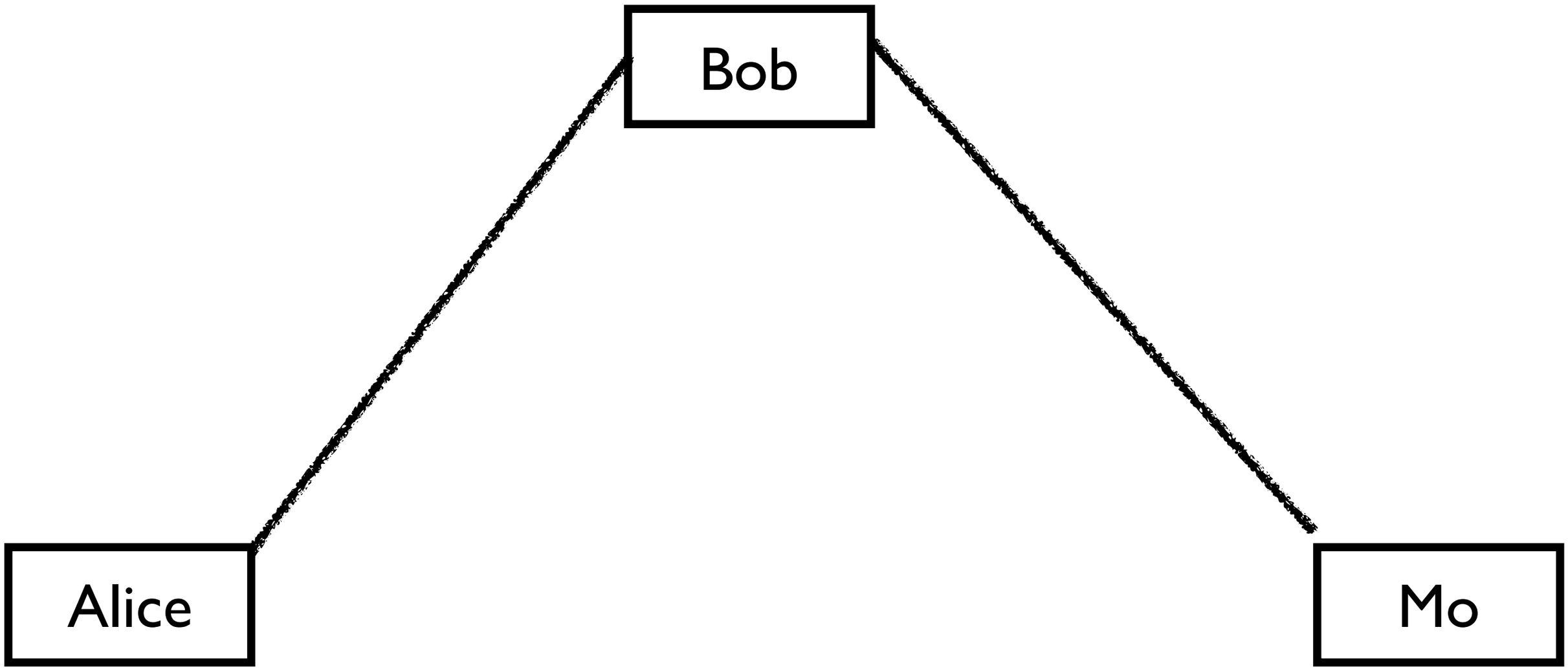
Bob can be malicious

Payment Networks

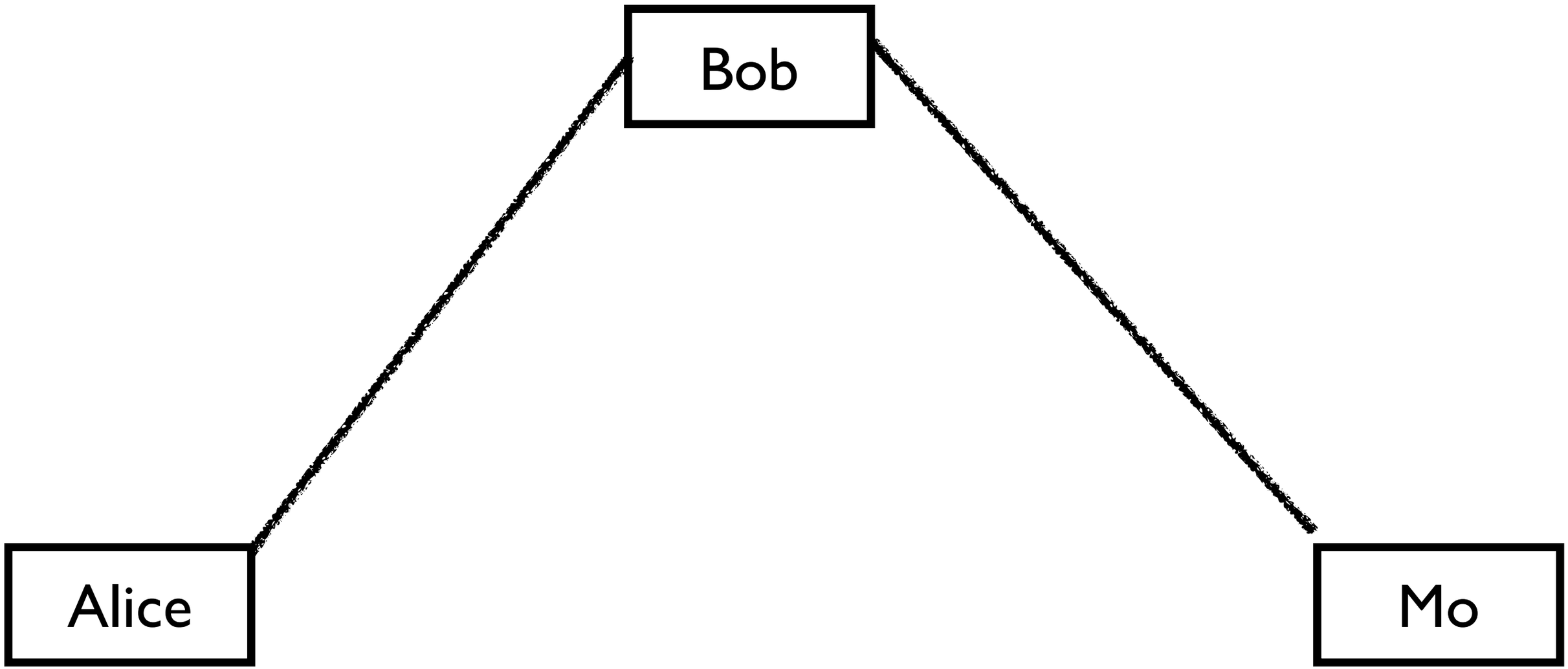
Alice wants to pay Mo 1BTC



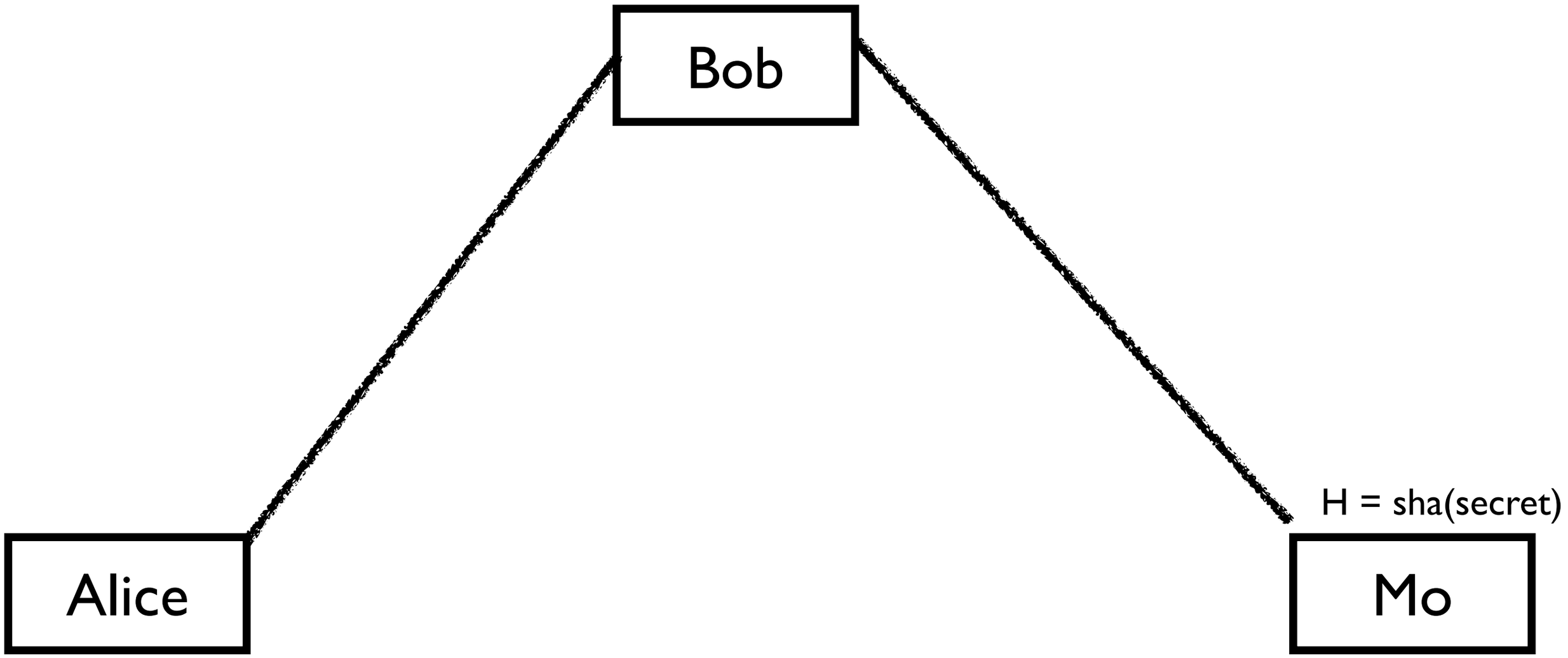
Hashed Time-locked Contract



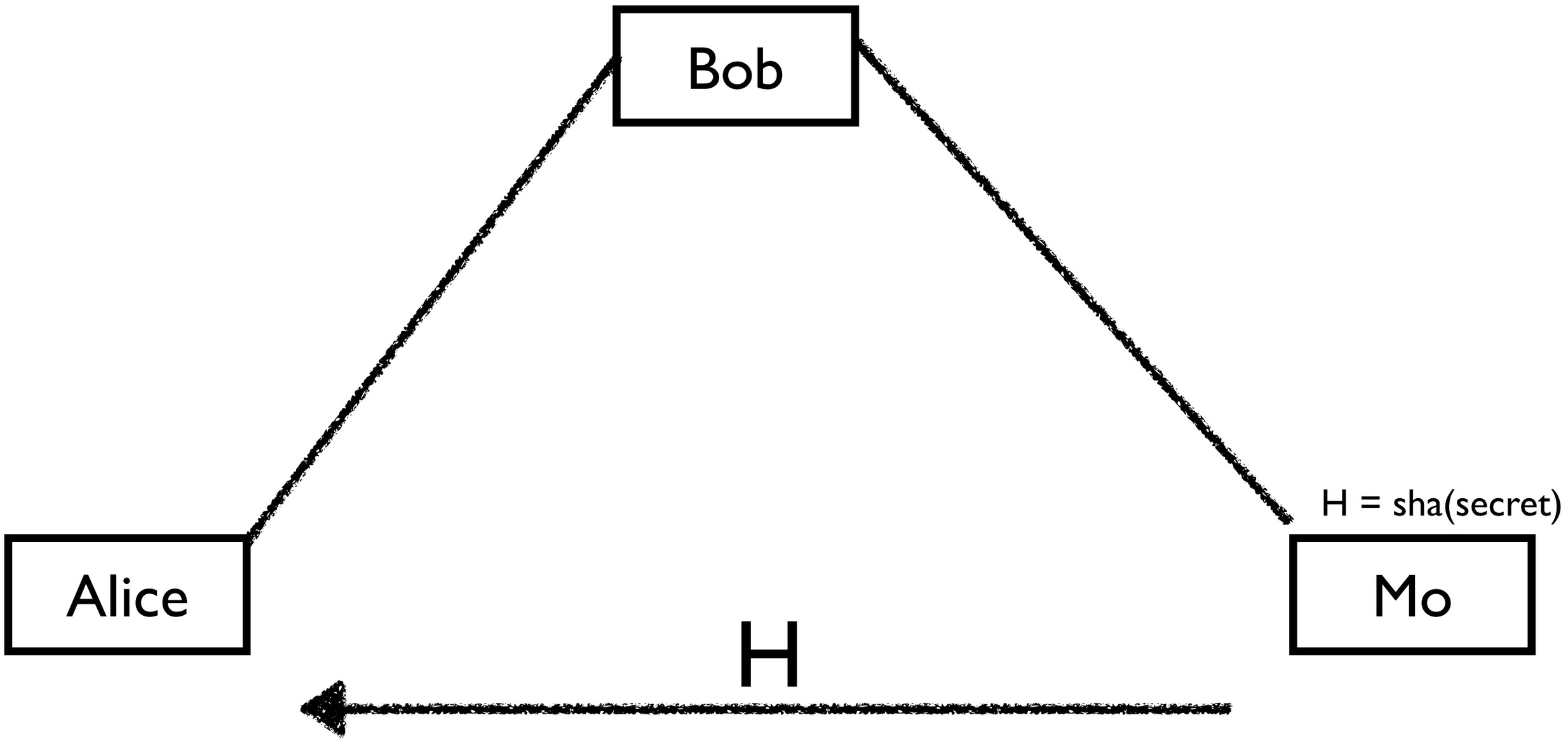
Conditional Transaction



Conditional Transaction

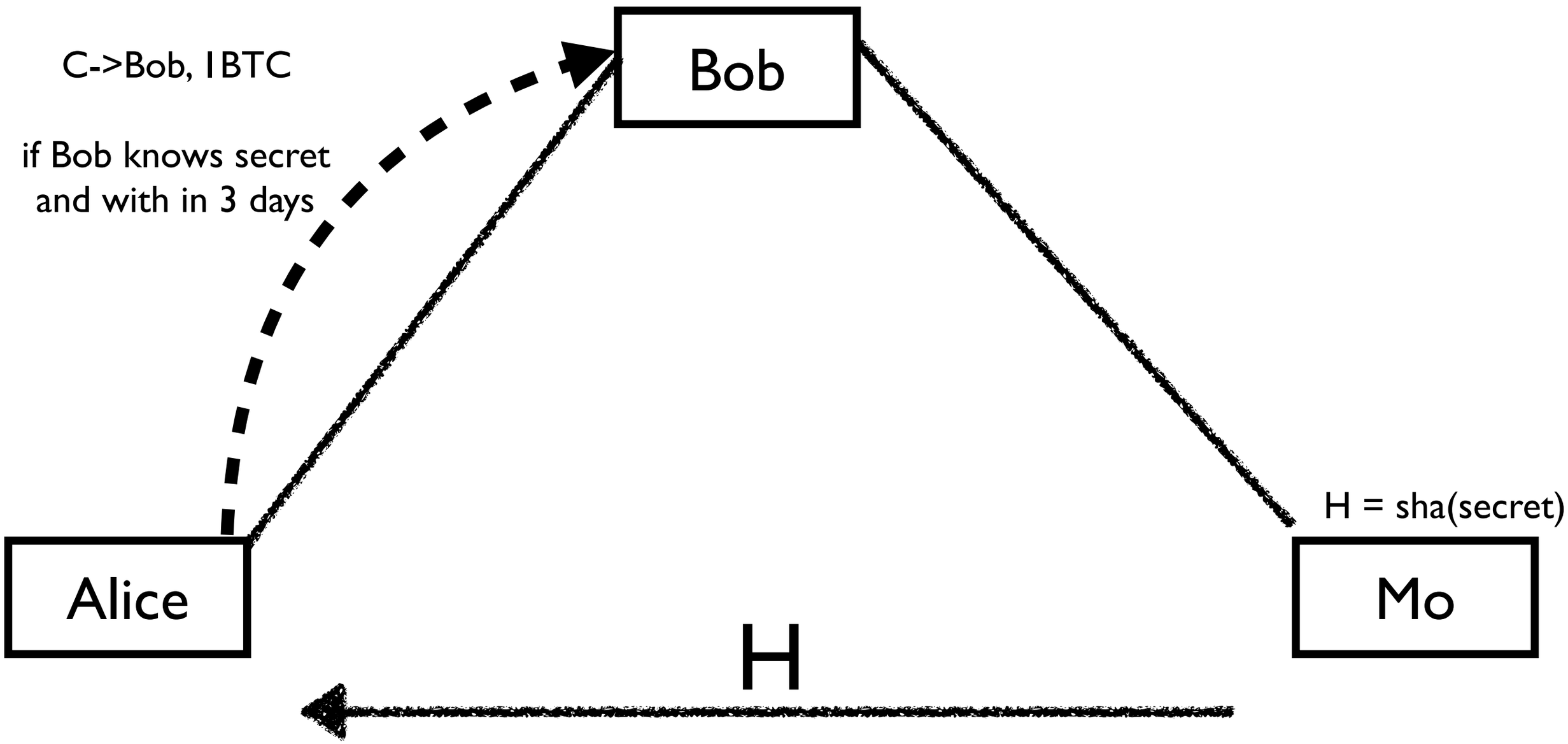


Conditional Transaction



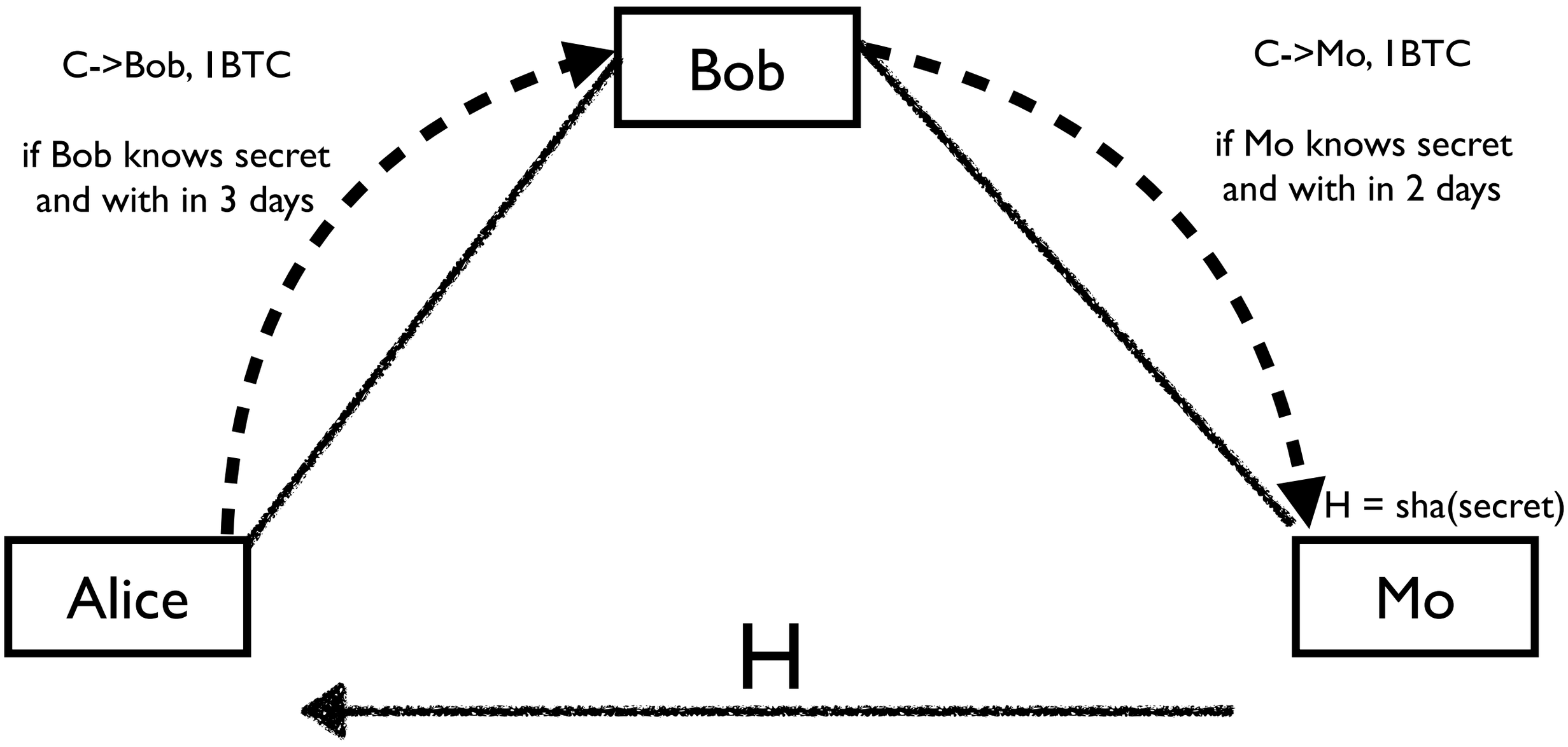
Payment Networks

Conditional Transaction



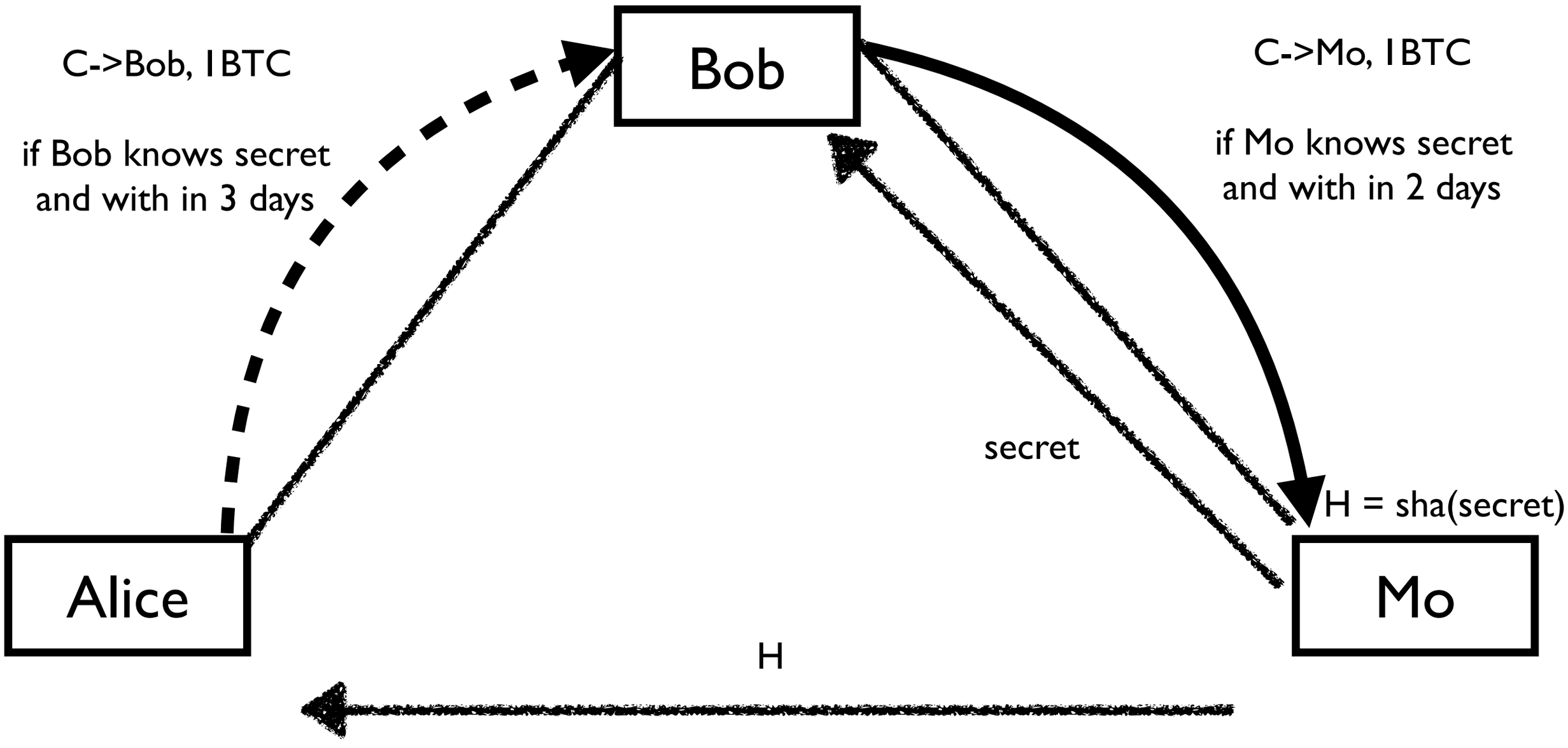
Payment Networks

Conditional Transaction



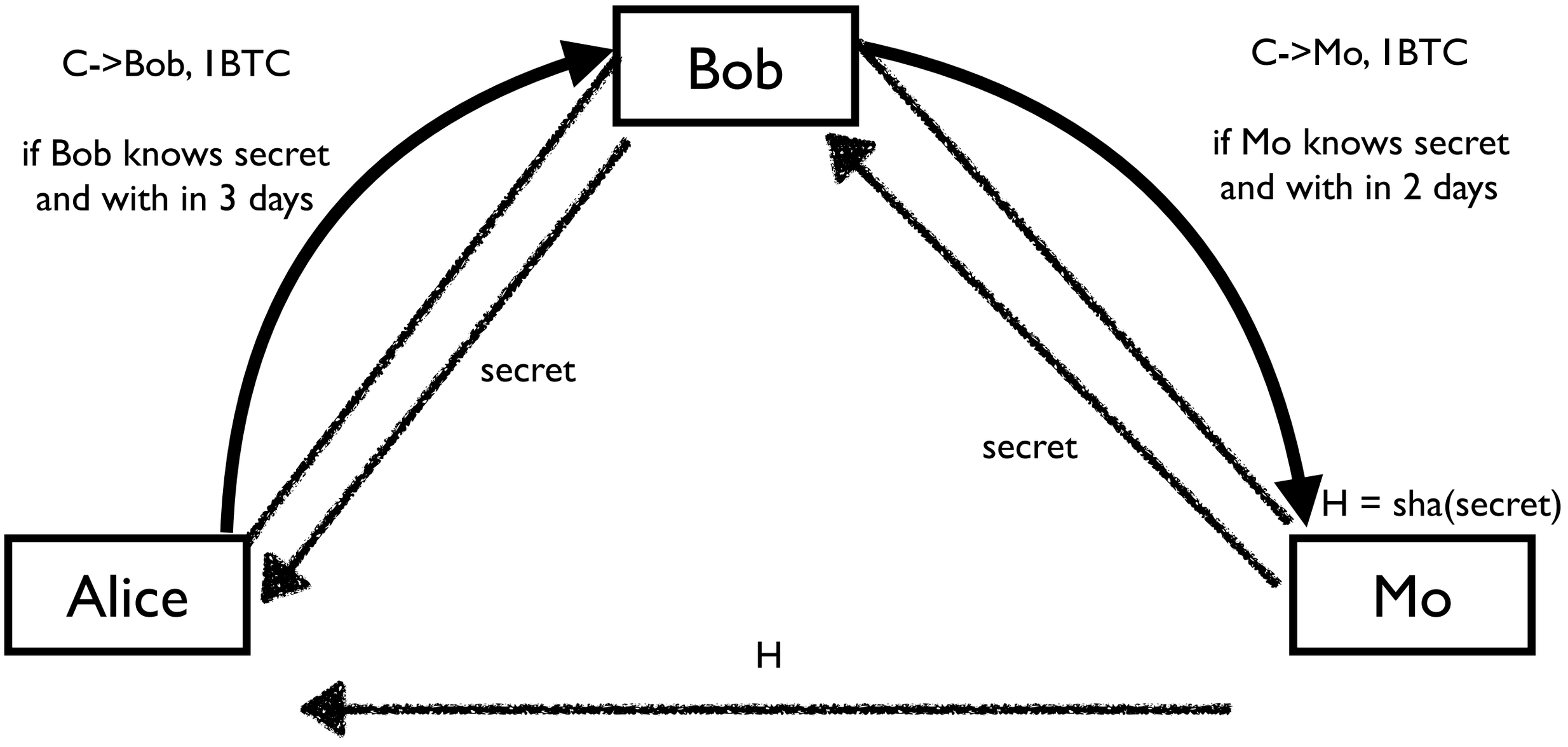
Payment Networks

Conditional Transaction



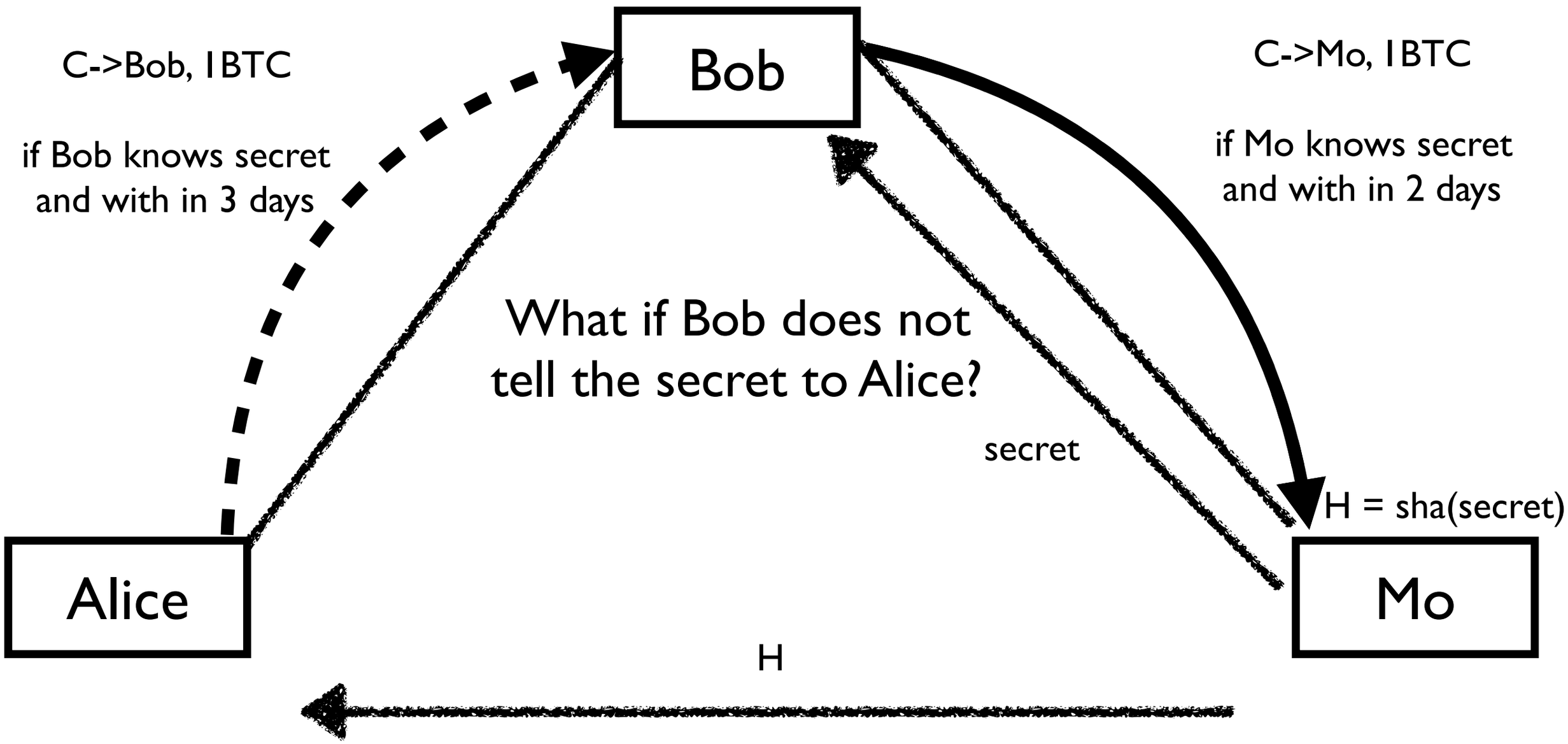
Payment Networks

Conditional Transaction



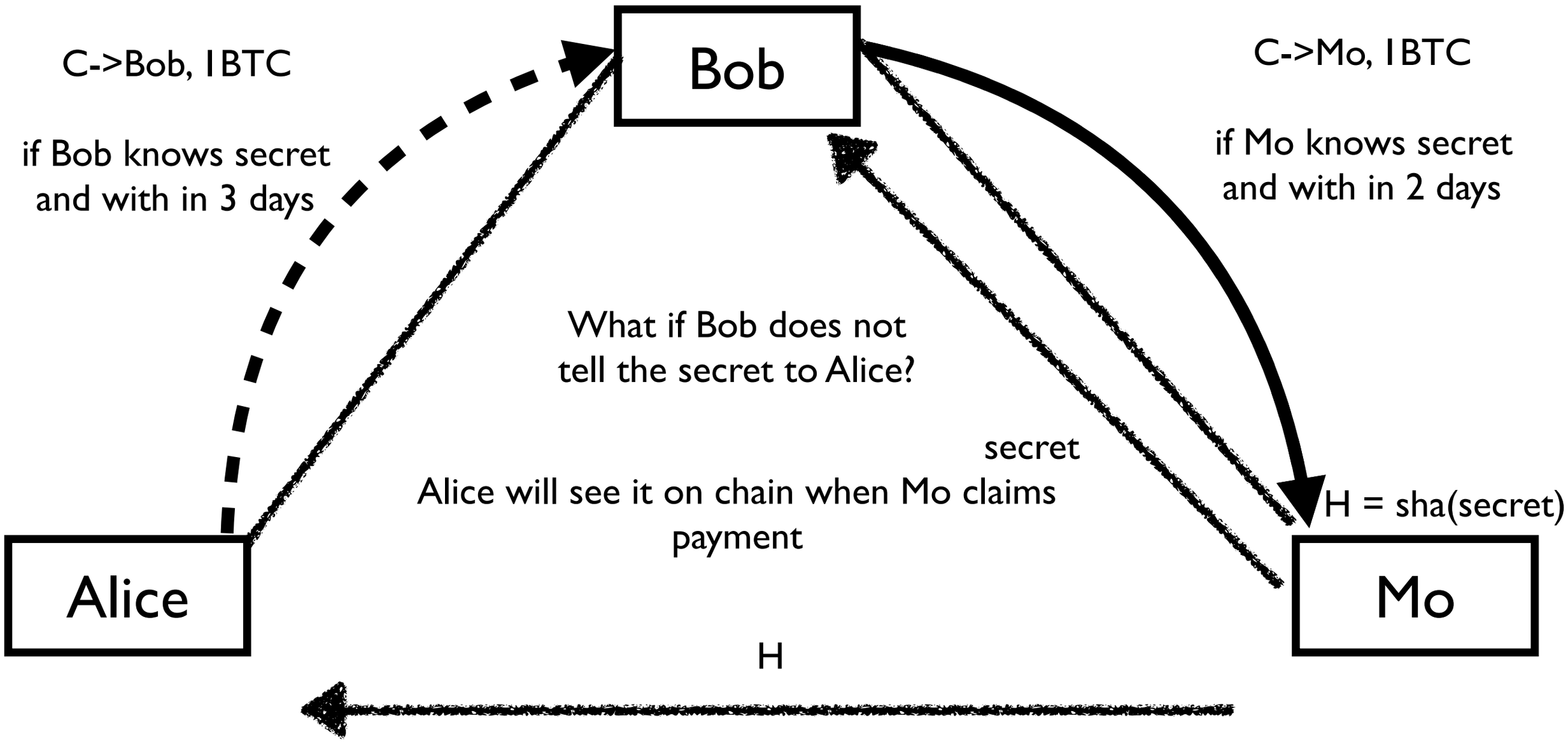
Payment Networks

Conditional Transaction



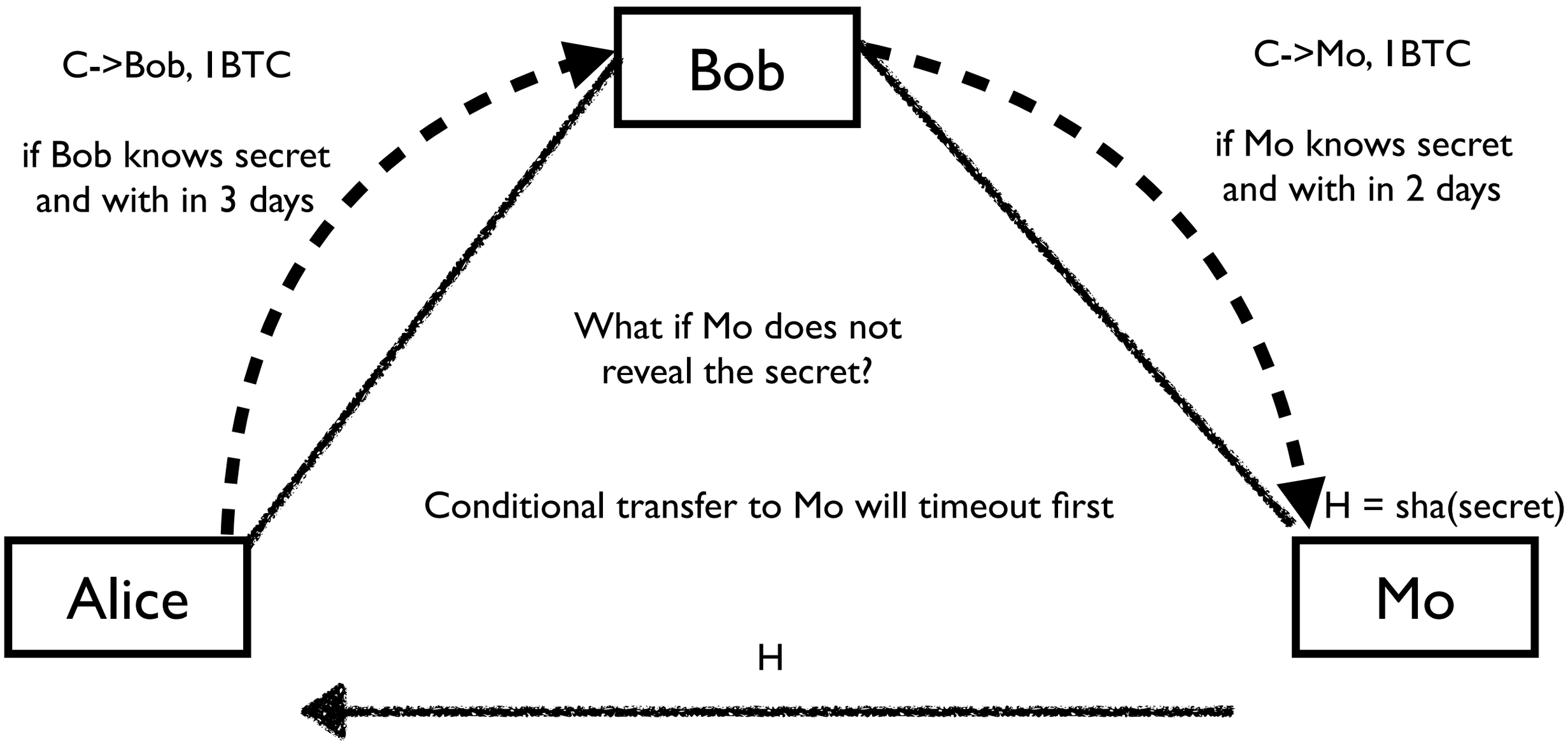
Payment Networks

Conditional Transaction



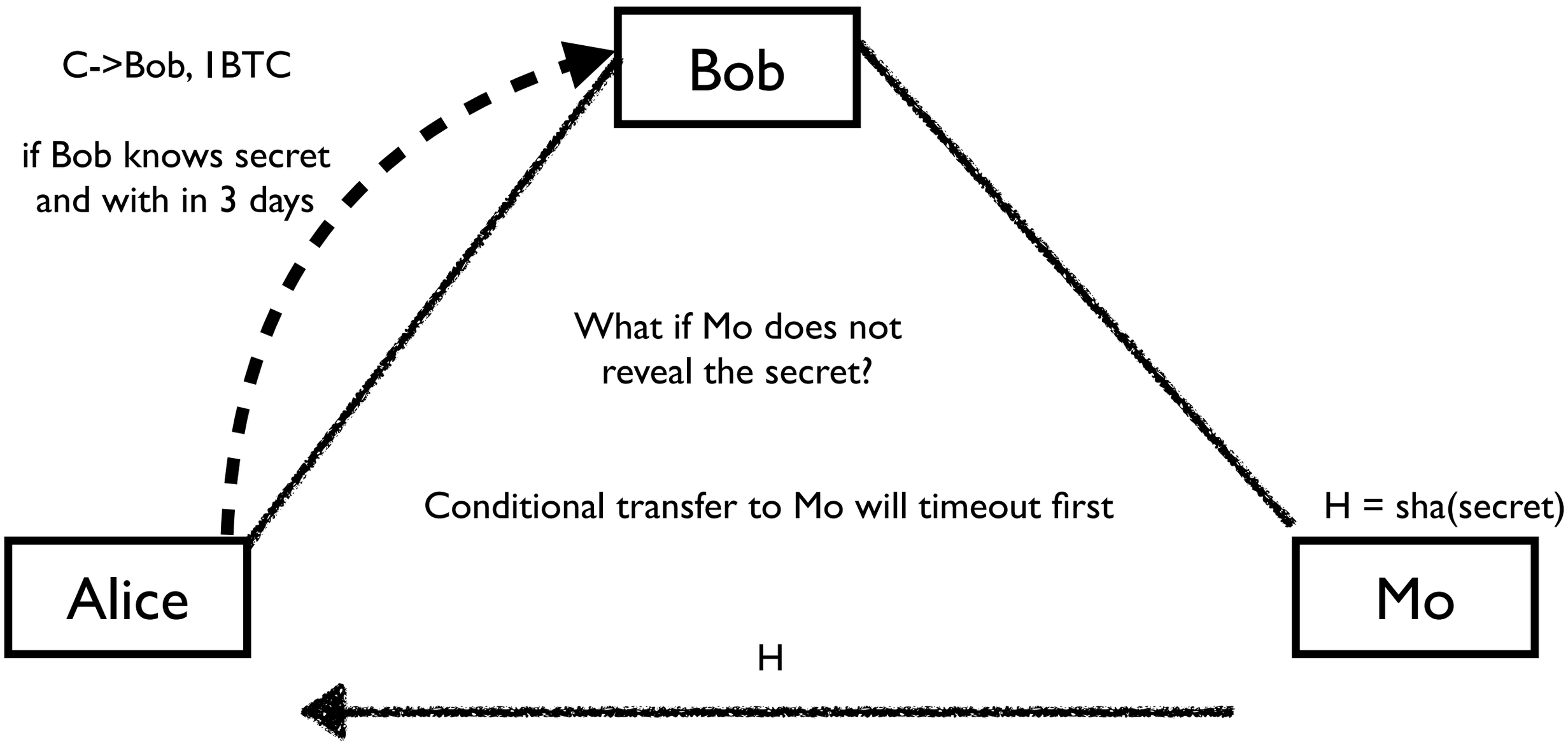
Payment Networks

Conditional Transaction

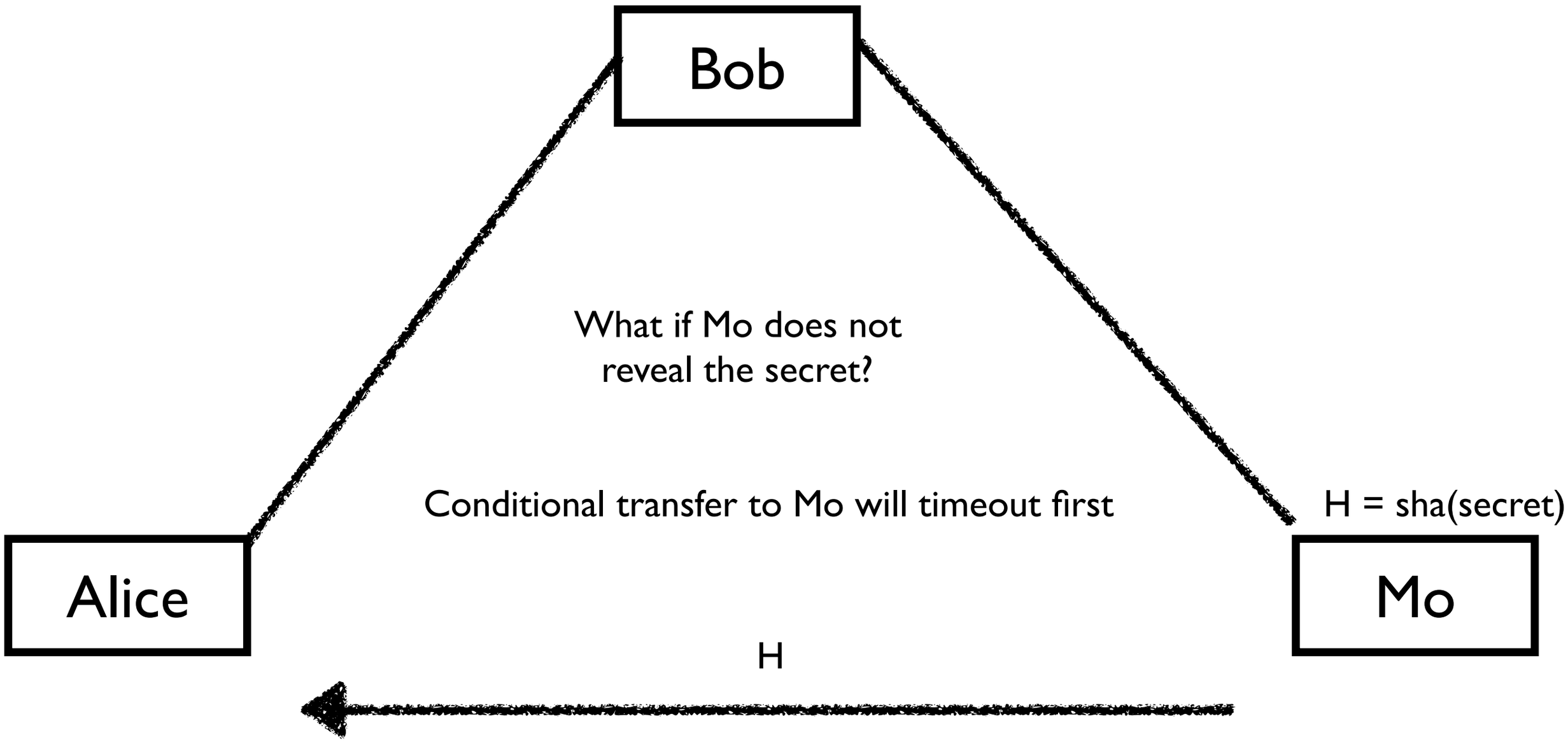


Payment Networks

Conditional Transaction



Conditional Transaction

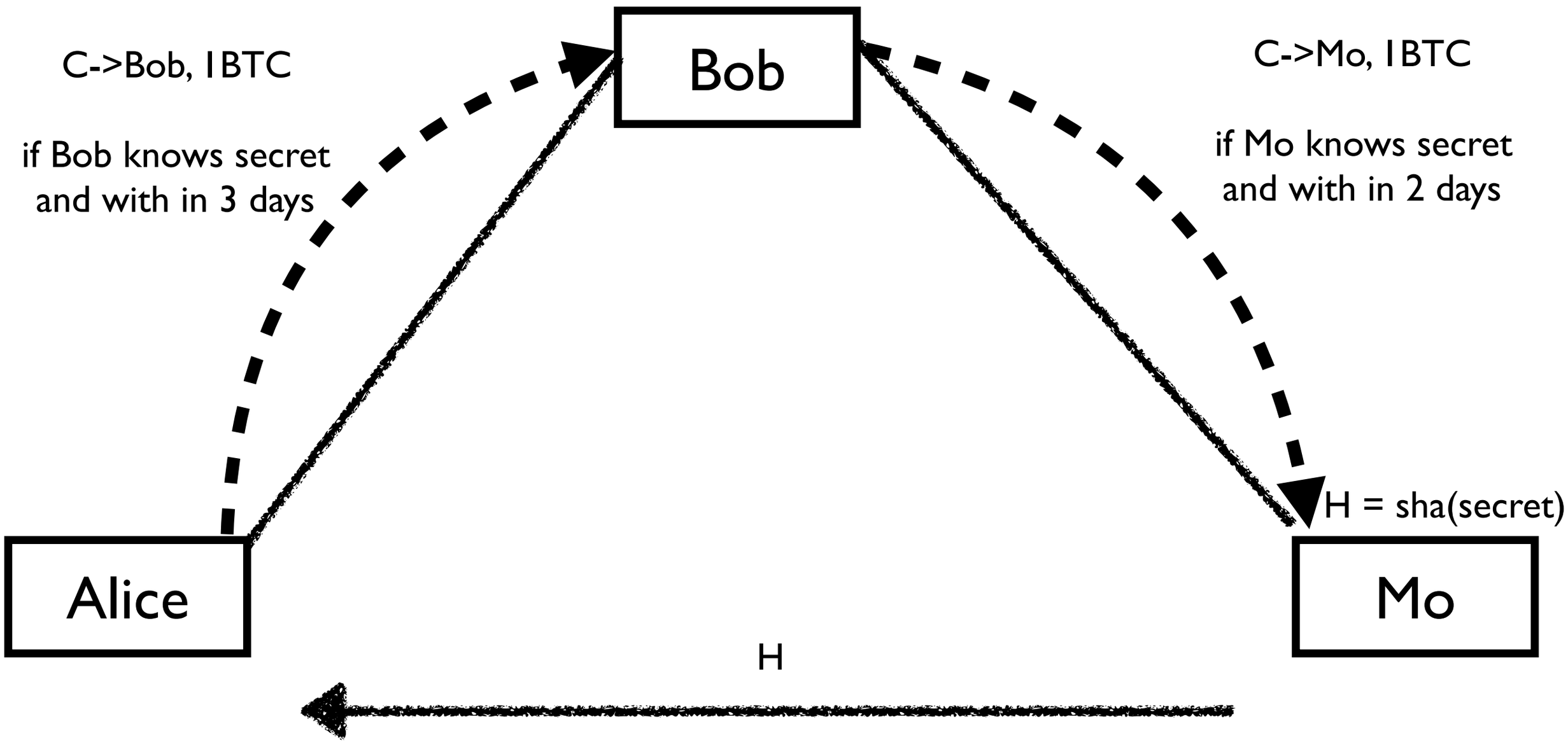


Deployment Status

BTC	ETH
Nothing at all	PoC
Requires Hard Forks	Turing Complete smart contract

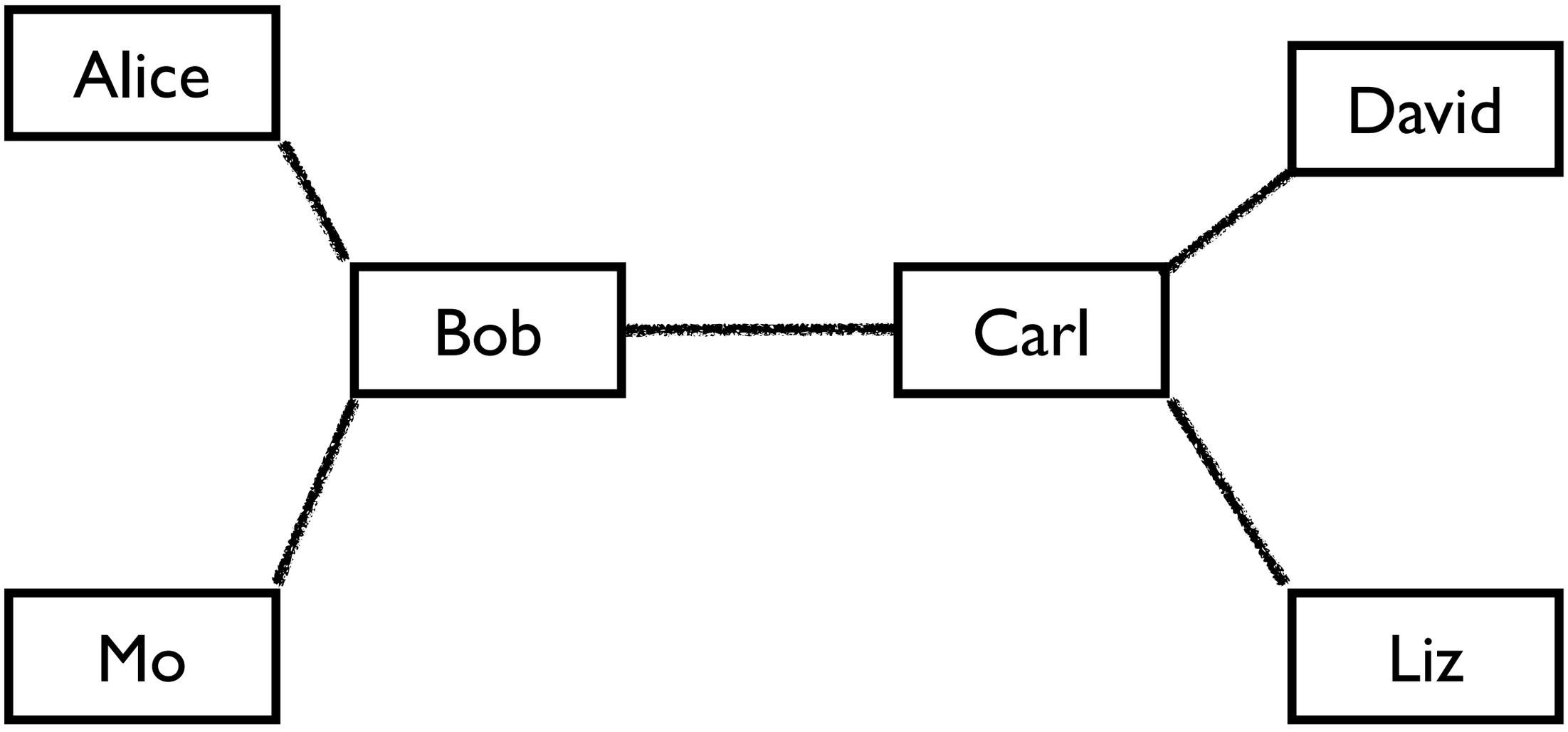
Payment Networks

What's the limitation of this?



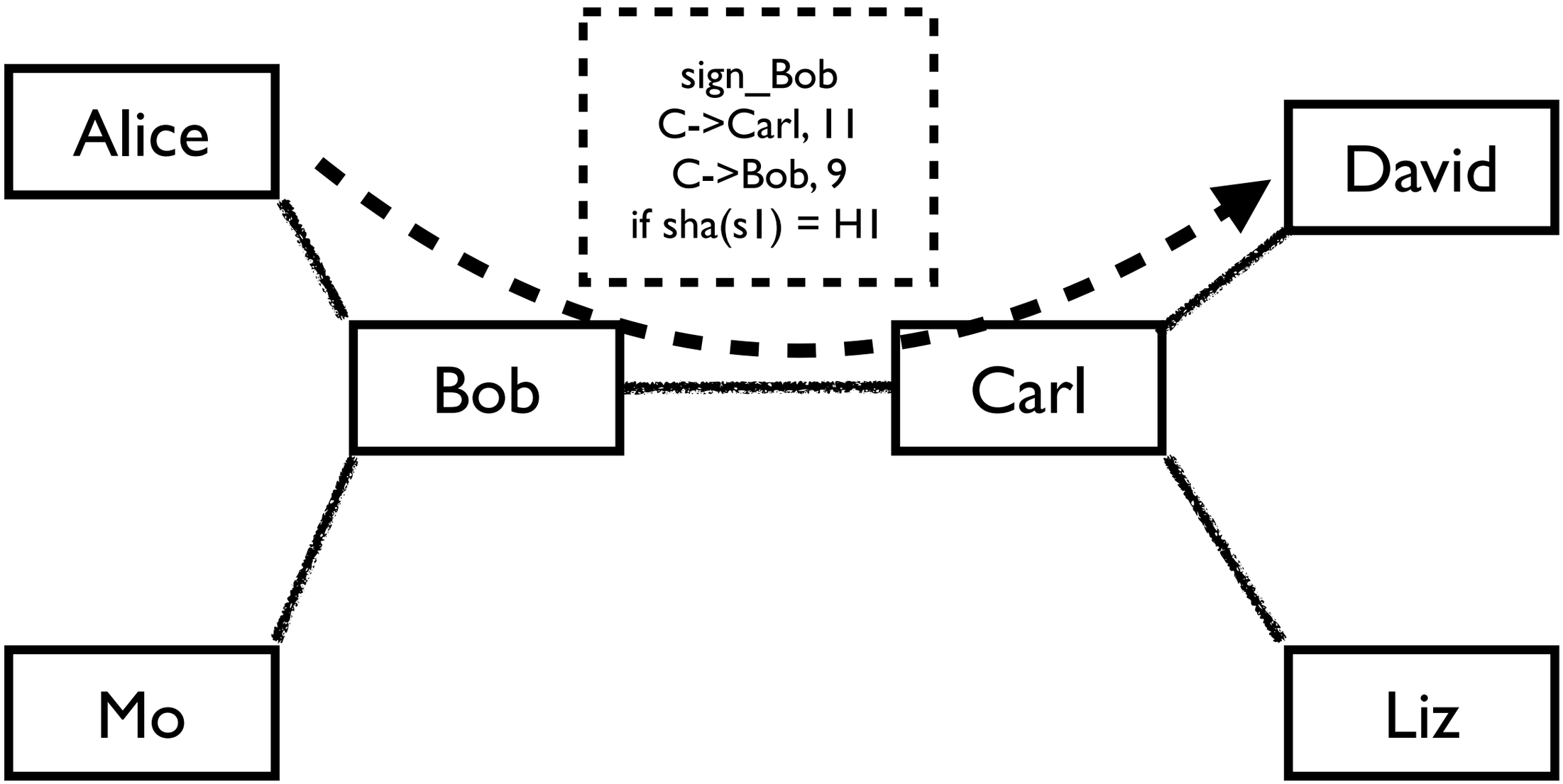
Payment Networks

What is the limitation of this?



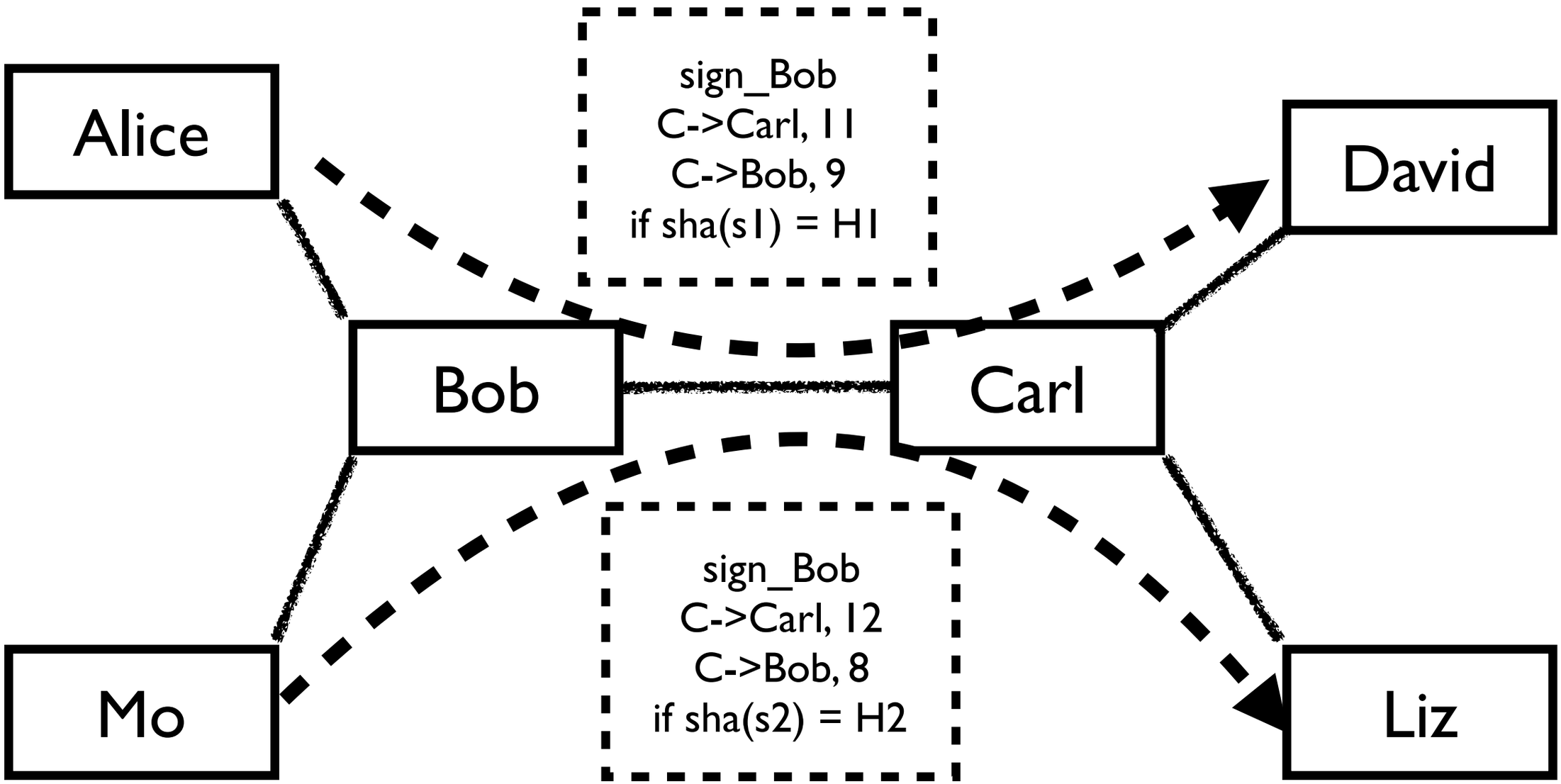
Payment Networks

What is the limitation of this?



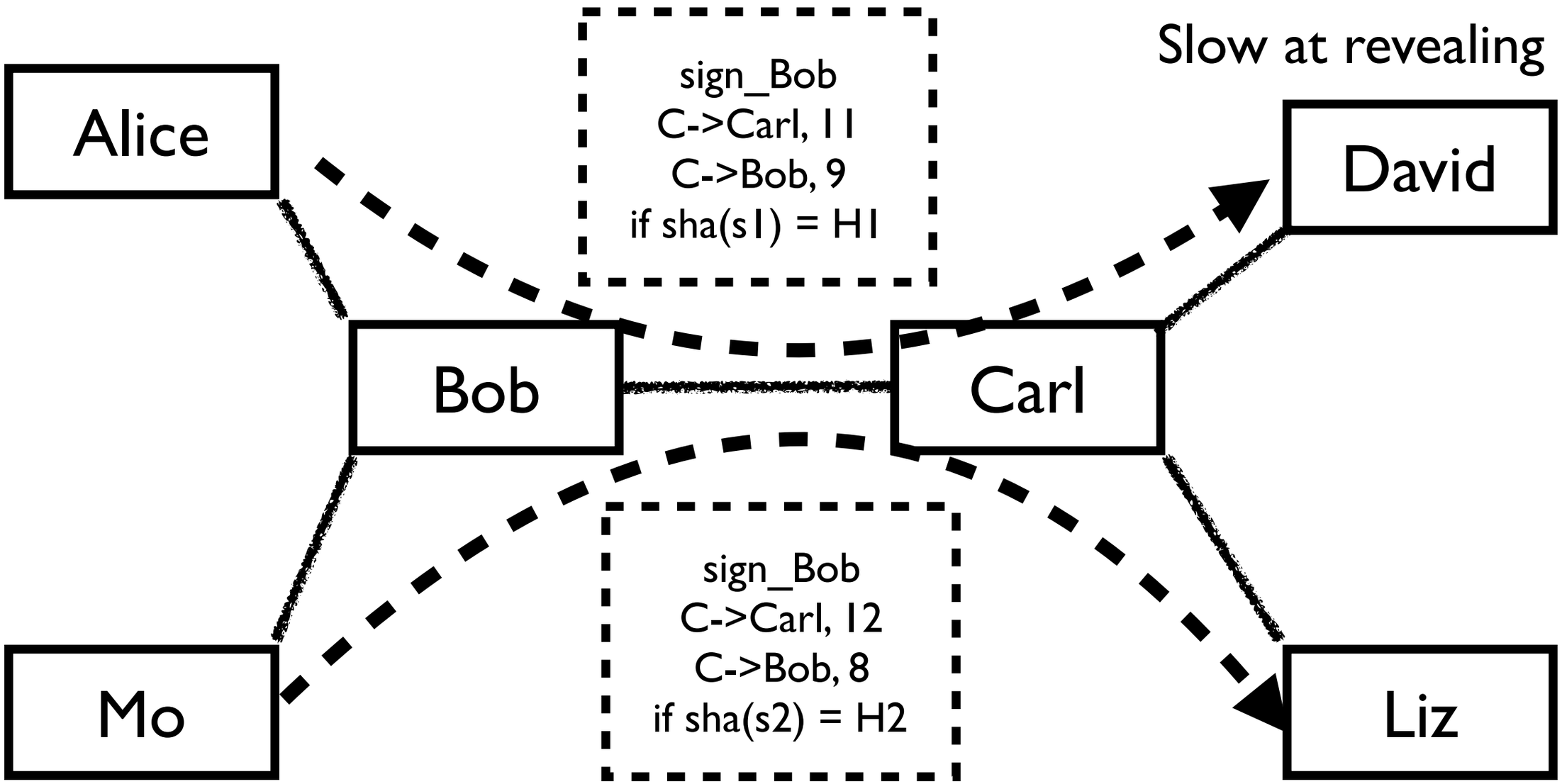
Payment Networks

What is the limitation of this?



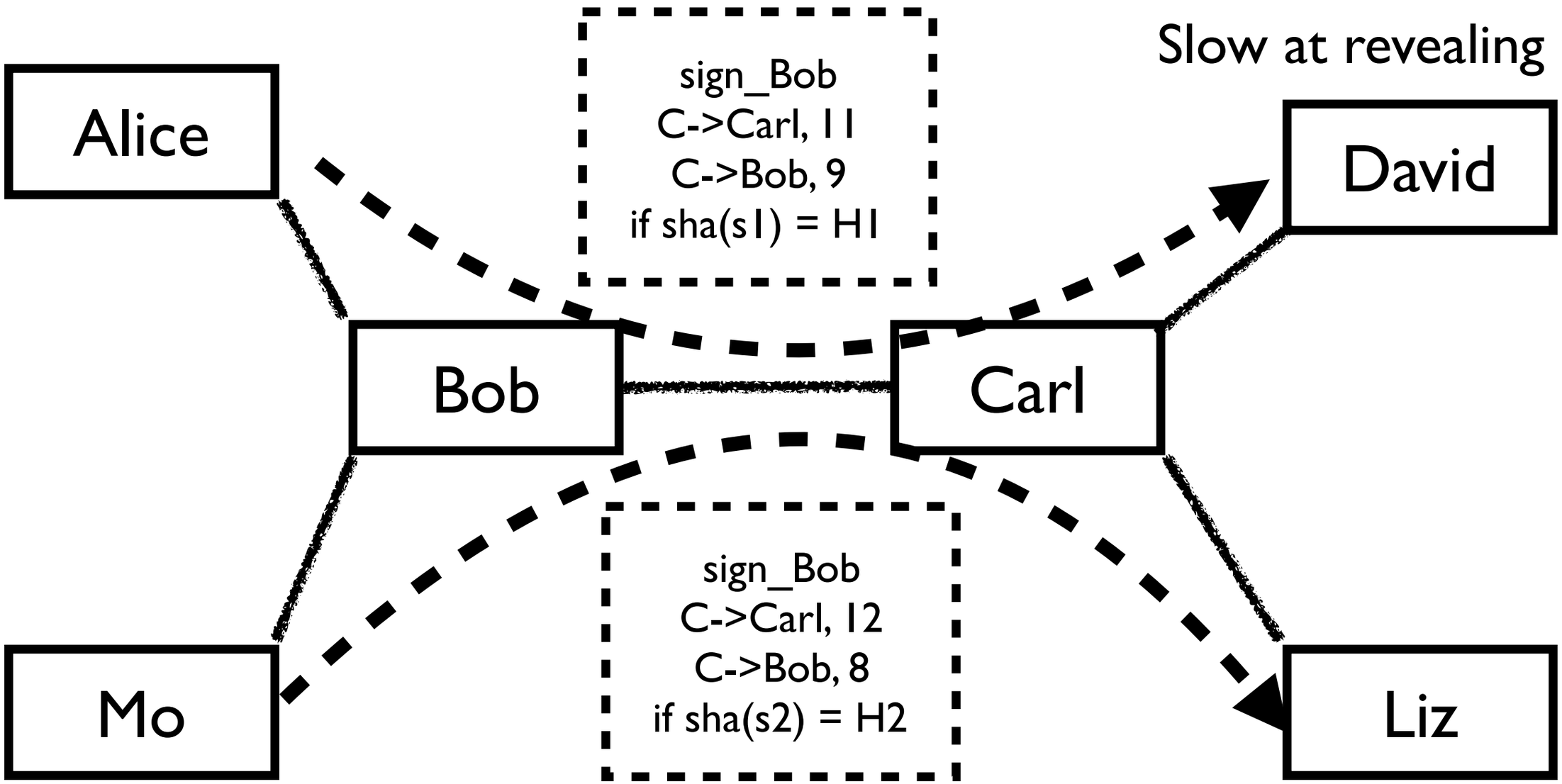
Payment Networks

What is the limitation of this?



Payment Networks

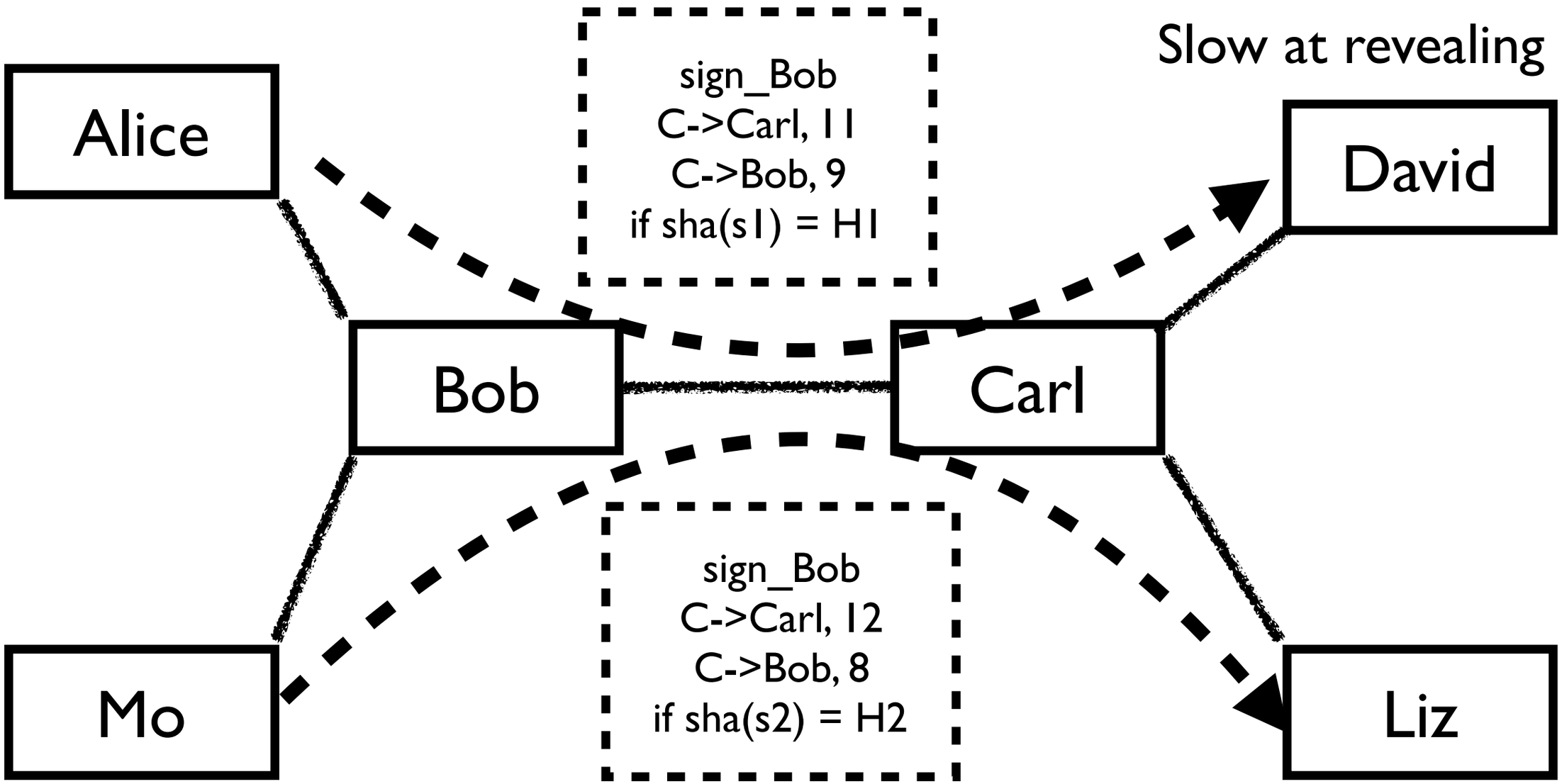
What is the limitation of this?



Security risk!

Payment Networks

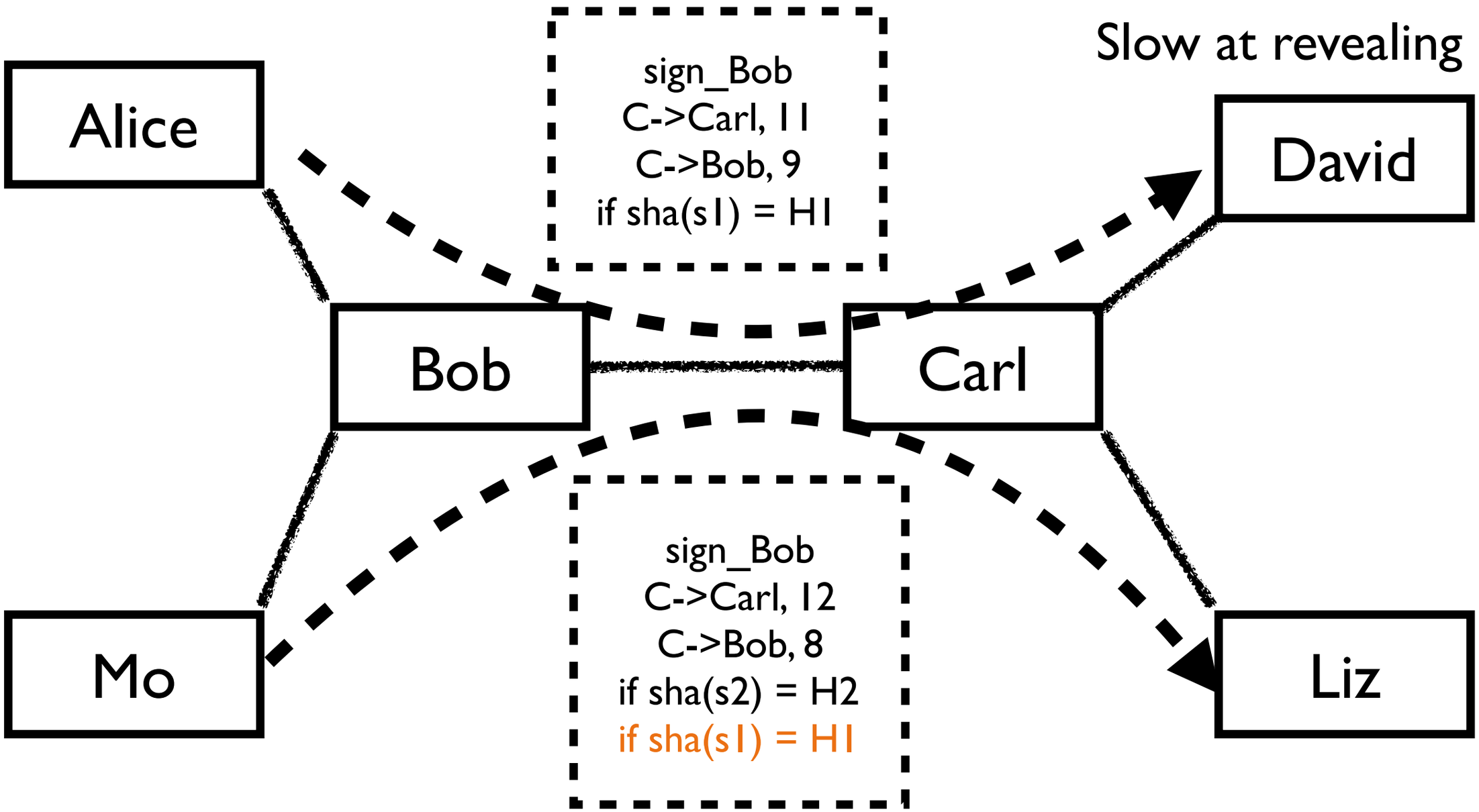
Cannot do concurrent payment!



Security risk!

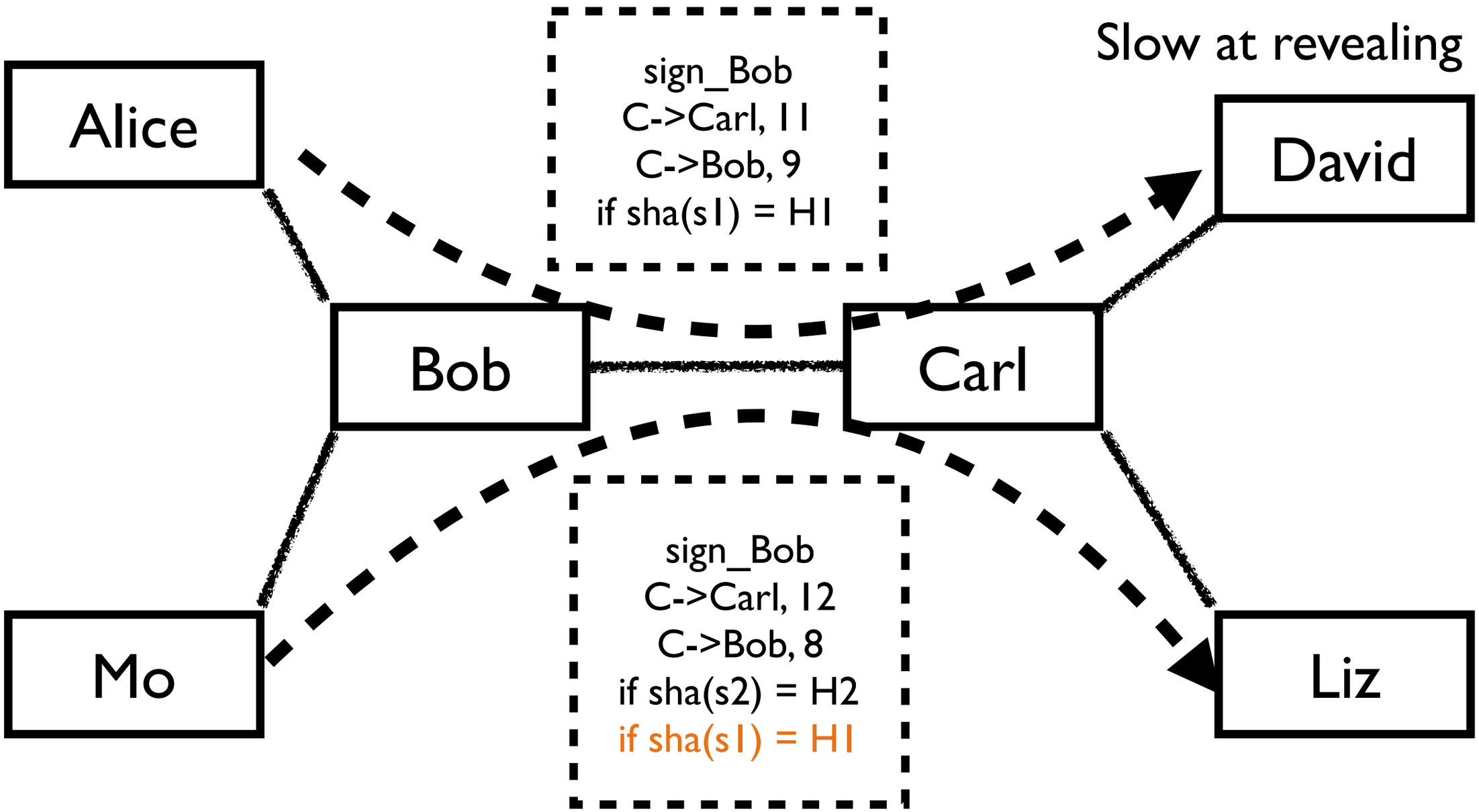
Payment Networks

Crypto researcher's solution



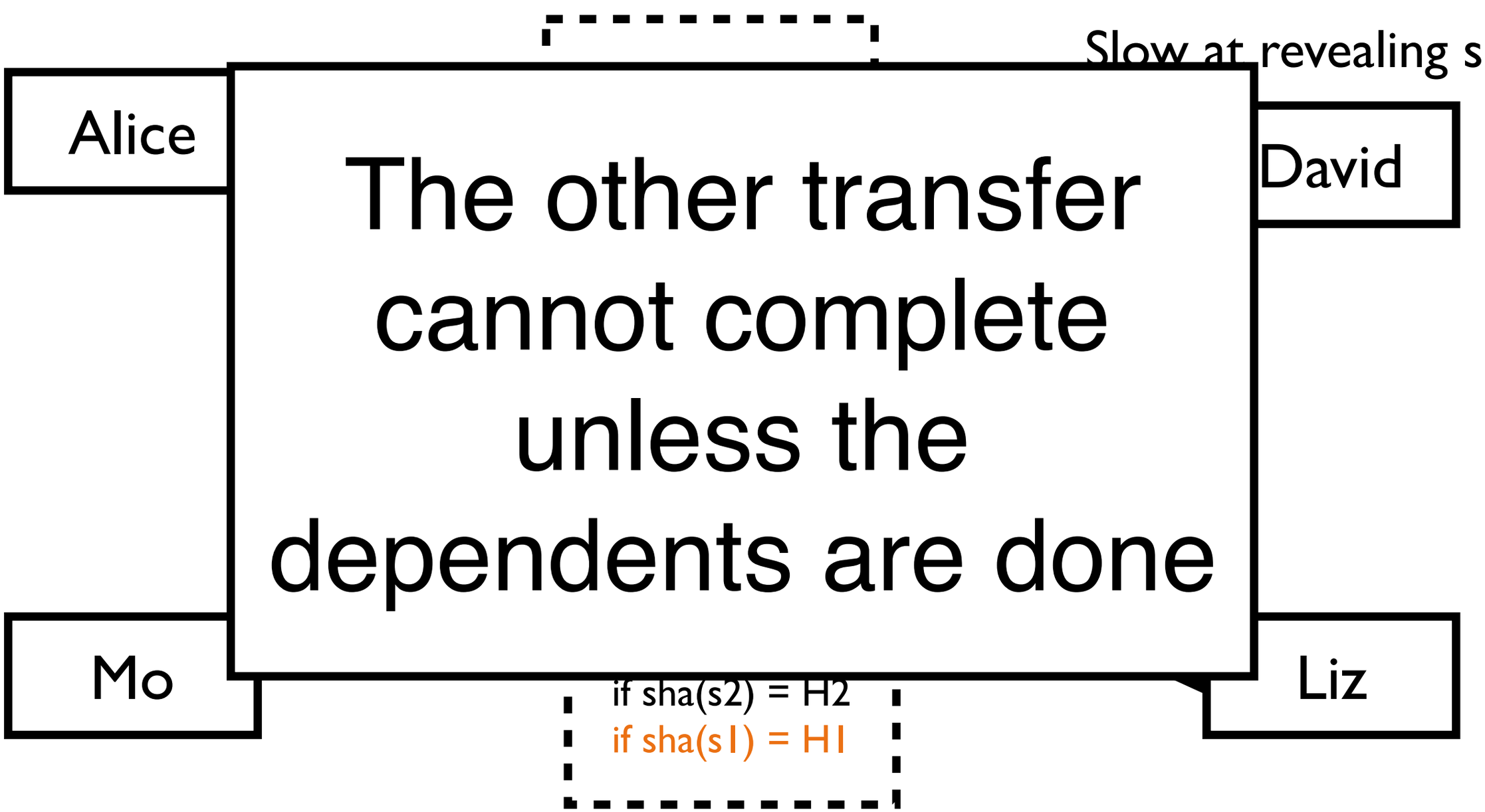
Payment Networks

Solves the safety issue, but…..



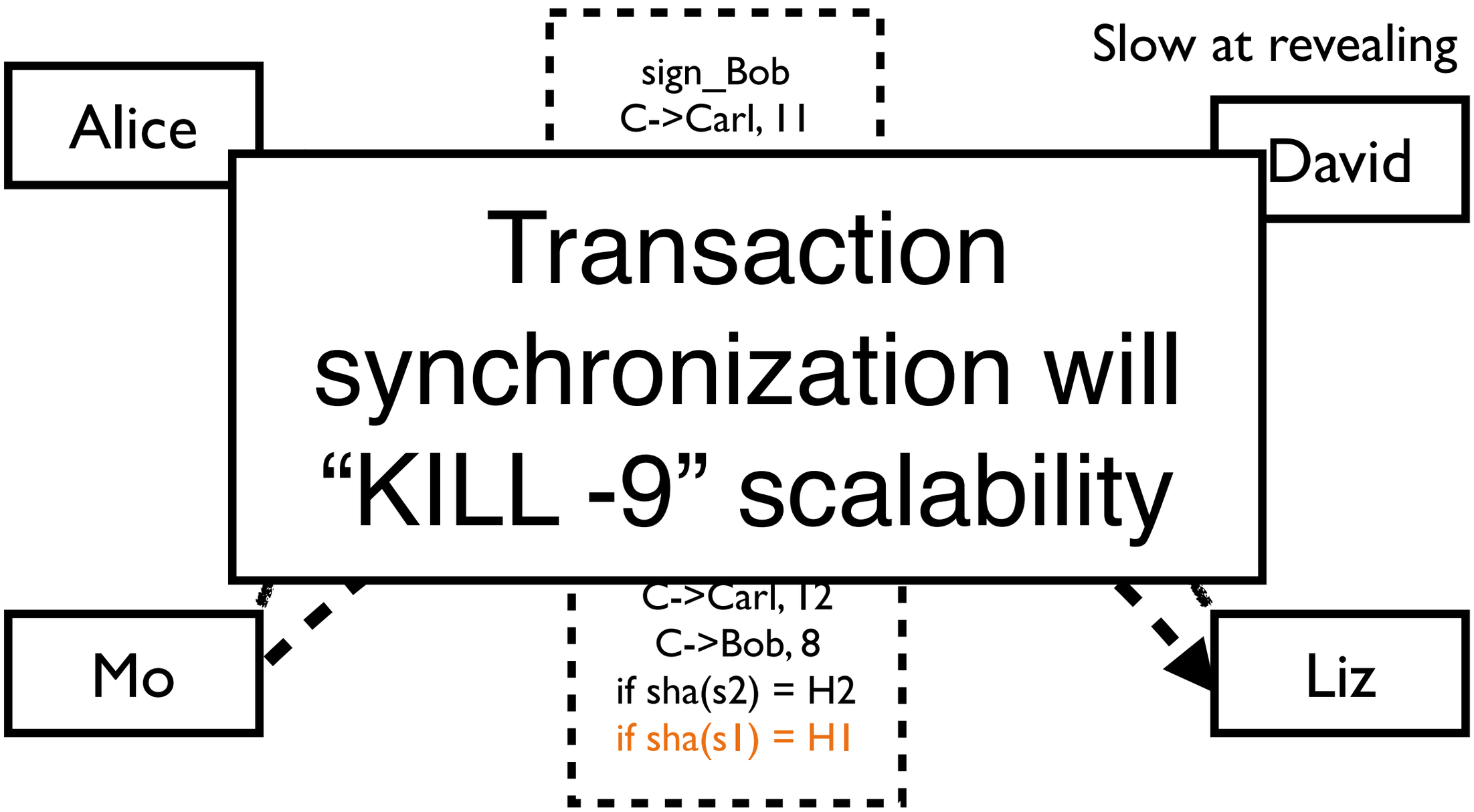
Payment Networks

Solves the safety issue, but…..



Payment Networks

Solves the safety issue, but…..



What is this?

in the view of our sharpe eyes
of
advanced networking

1920s

[Getty Images]

[US Air Force]

1920s

[Getty Images]

[US Air Force]

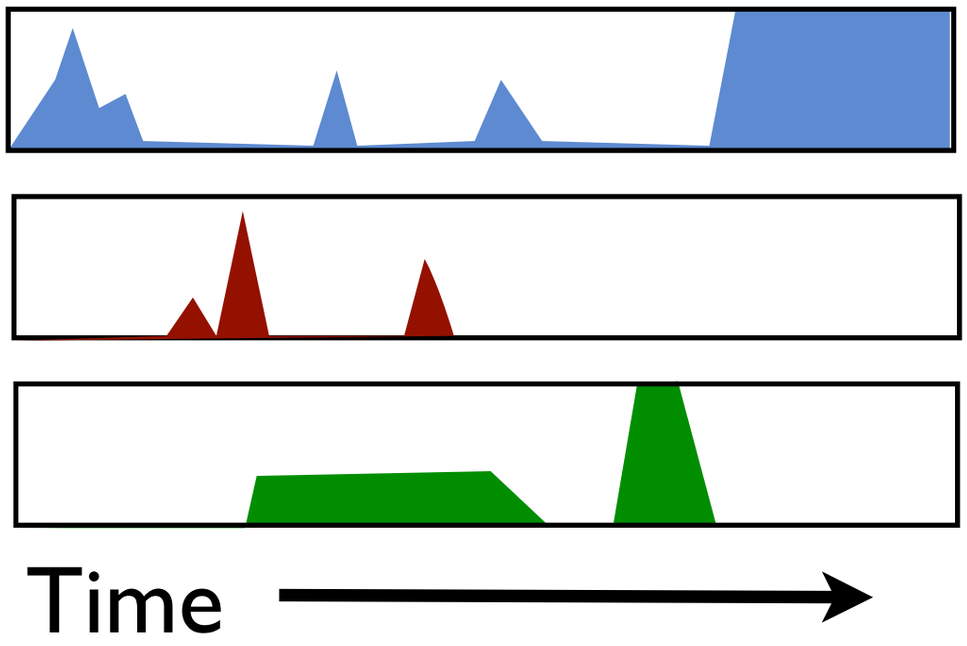
1920s

[Getty Images]

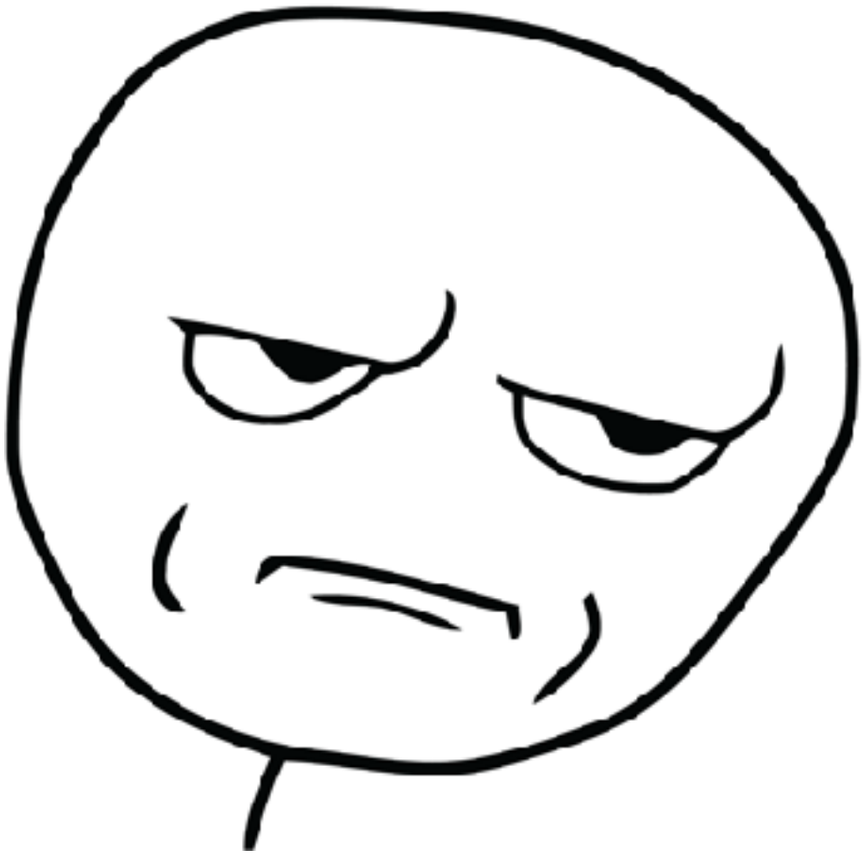
1967

[US Air Force]

Circuit switching

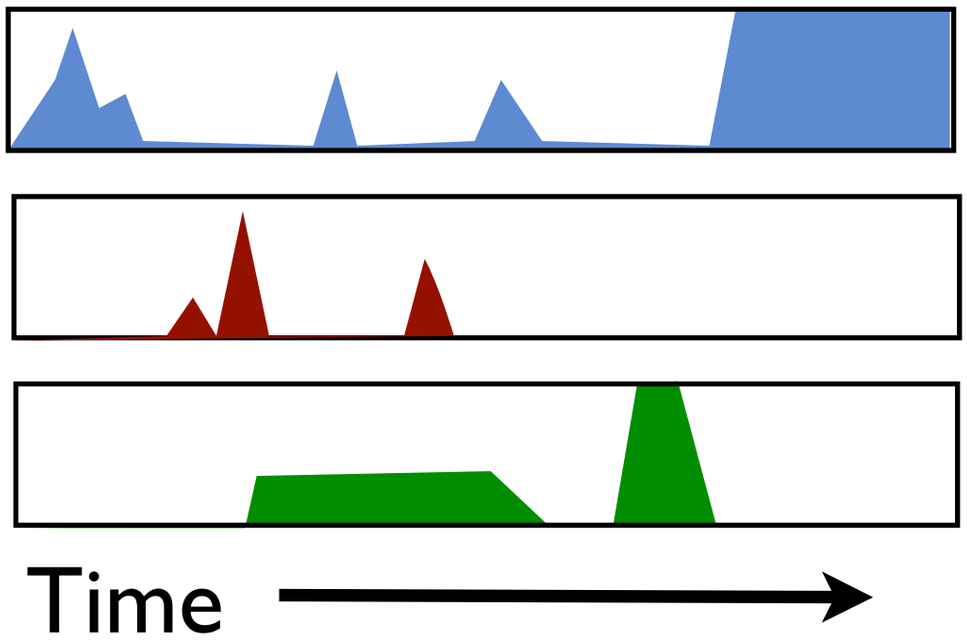


You want to build a scalable network with circuit switching in 2017?



YOU GOTTA BE KIDDING ME!

Circuit switching



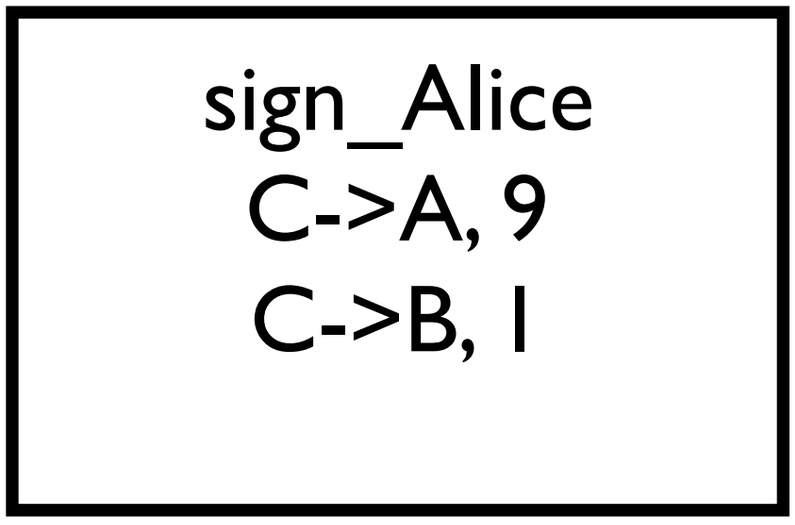
Right All the Wrong (RAW): A Networking Stack for Payment Networks (Our Active Research Projects, actively recruiting collaborators)

A limited preview

Right All the Wrong (RAW): A Networking Stack for Payment Networks (Our Active Research Projects, actively recruiting collaborators)

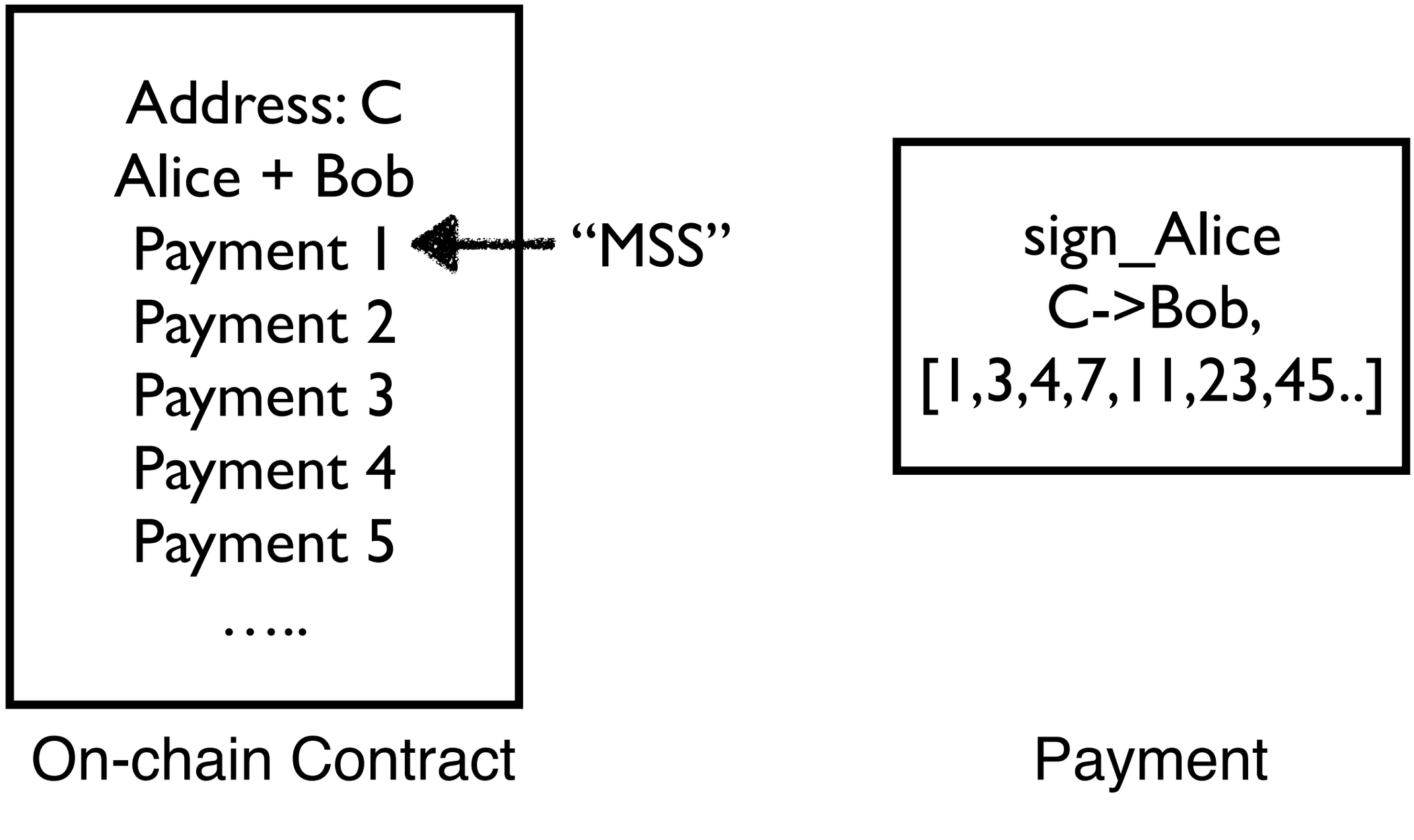
A limited preview

On-chain Contract



Payment

RAW: Packet Switching Contract



State Channel

A block chain Design Philosophy

Combine the on-chain program state settlement with frequent off-chain intermediate state transactions

Other Scalability Proposals

Proof of Stake

Sharding of Blockchain