What’s new in Lykke exchange development

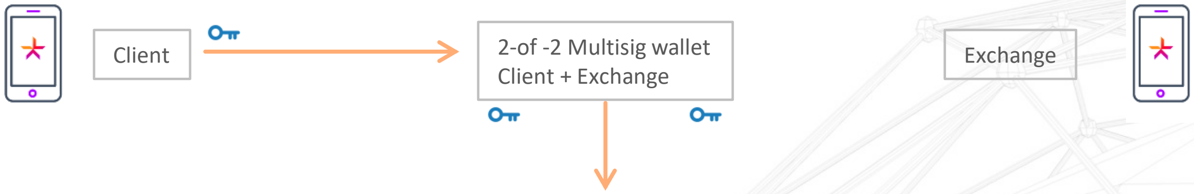
- Ethereum integration
- Ethereum vs Bitcoin crosschain settlement
- Scaling Bitcoin – offchain settlement
- Ethereum offchain

MultiSig wallets

Multisignature wallets are used to deposit client's coins. The exchange does not take possession of the traded coins.

2-of-2 Multisig address requires two signature to spend coins from it:

- Client's signature
- Exchange signature



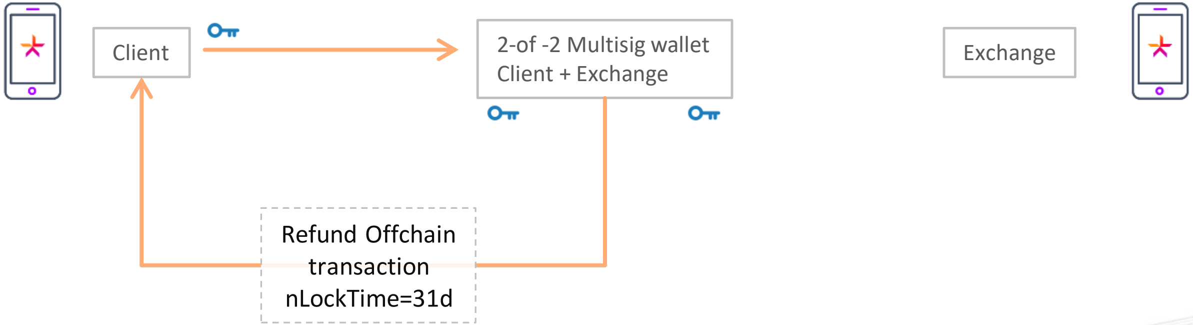
MultiSig wallets advantages

MultiSig wallet provides the following advantages:

- Coins flow control – Exchange signature required for each transaction
- Client identification (KYC) – registered clients only are allowed to trade
- Coins safety – even if exchange is compromised clients will not lose their coins

MultiSig wallets refunds

To guarantee funds recovery from the MultiSig wallet Exchange provides offchain «refund transaction»



Refund transaction can be broadcasted after 31 days

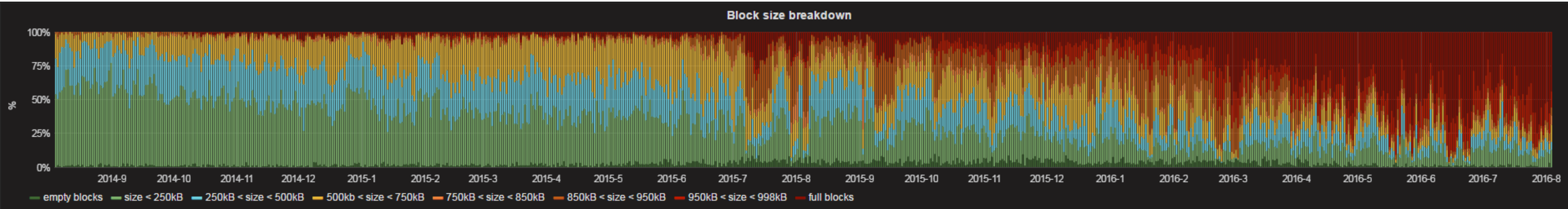
Bitcoin Scaling Issues

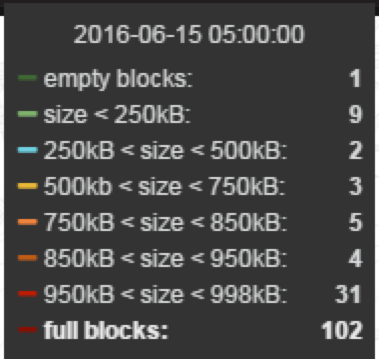
1 Mb blocks:

7 transactions per second (250 bytes/transaction)

220 mln transaction per year(!)

Not enough for city, let alone the world





2016-06-15 05:00:00

empty blocks:	1
size < 250kB:	9
250kB < size < 500kB:	2
500kb < size < 750kB:	3
750kB < size < 850kB:	5
850kB < size < 950kB:	4
950kB < size < 998kB:	31
full blocks:	**102**

Bitcoin Scaling Issues

1 Billion transaction per day requires:

1.6 GB blocks

87 Tb/Year

Centralization (!)

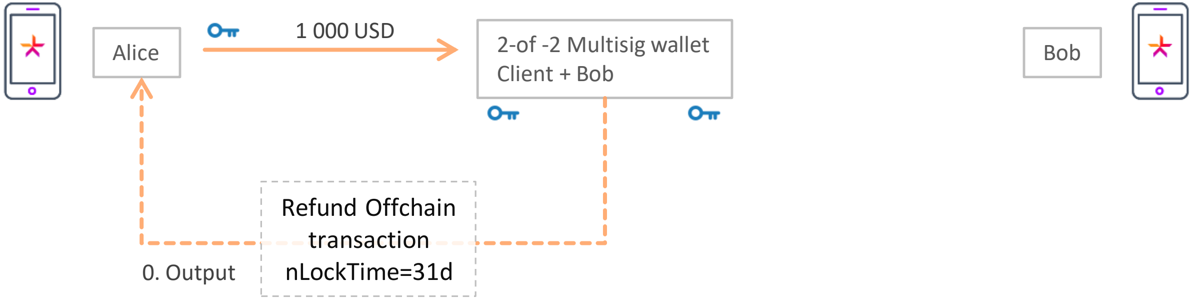
1 Billion people doing 2 transaction per day:

- 24 GB block
- 3.5 Tb/Day
- 1.27 Pb/Year

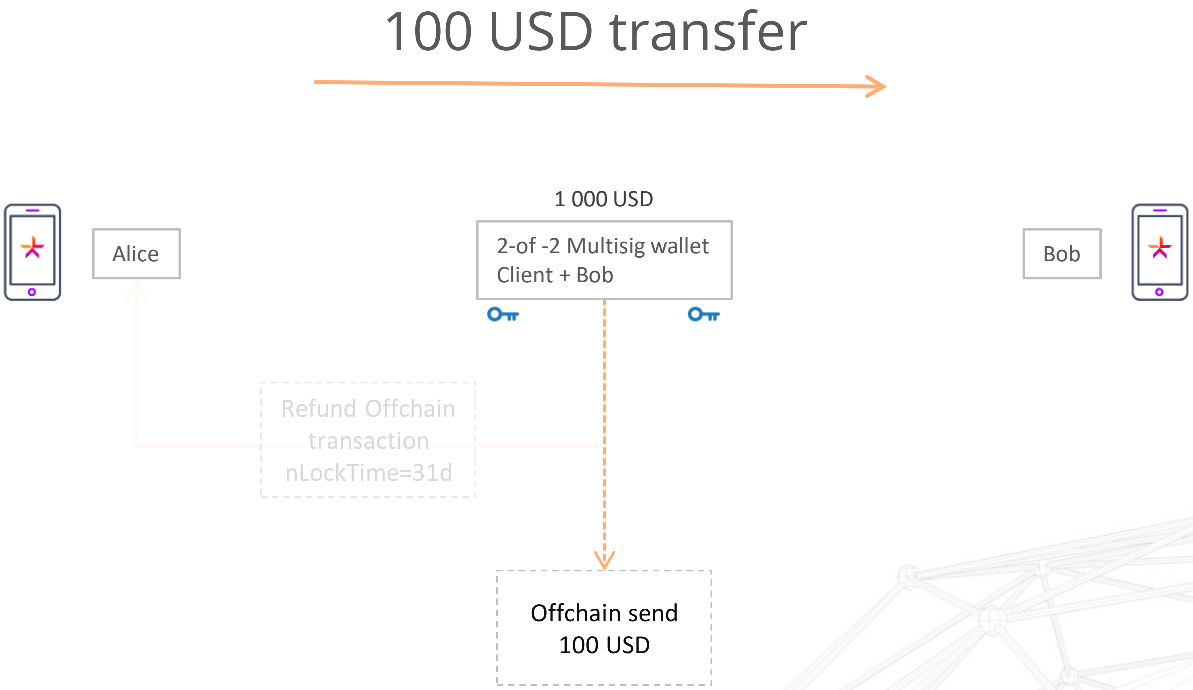
Bigger block = Centralization

- Very few full nodes
- Very few miners
- De facto inability to validate blockchain

Bitcoin Scaling With Offchain Payment Channels

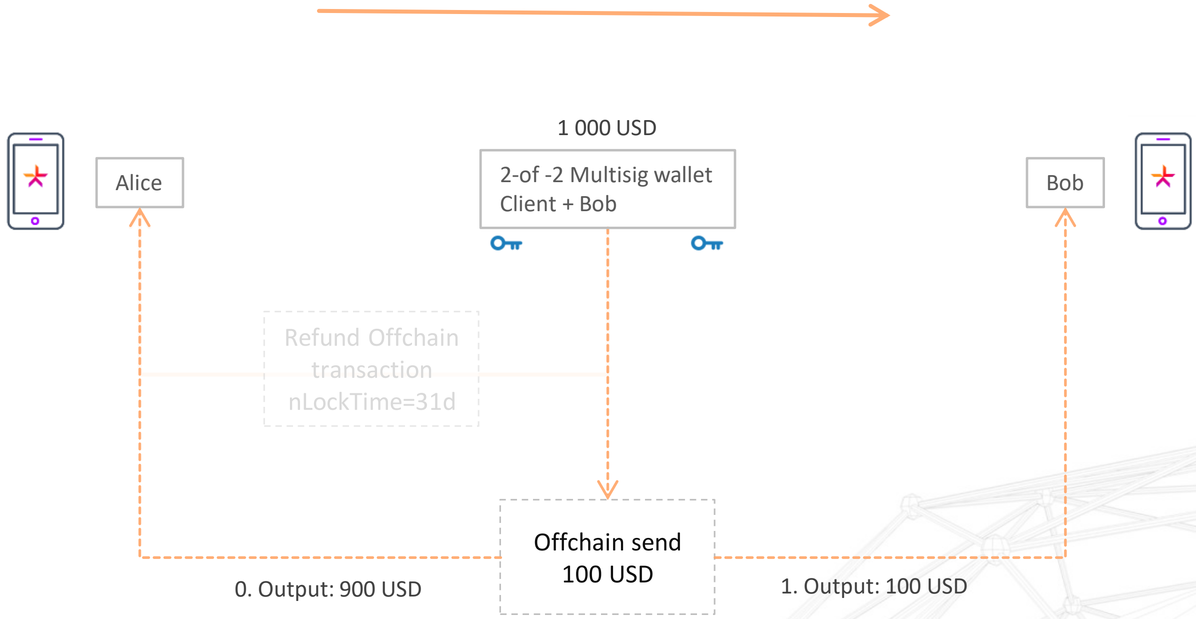


Bitcoin Scaling With Offchain Payment Channels



Bitcoin Scaling With Offchain Payment Channels

100 USD transfer



1 000 USD

2-of -2 Multisig wallet
Client + Bob

Alice

Bob

Refund Offchain
transaction
nLockTime=31d

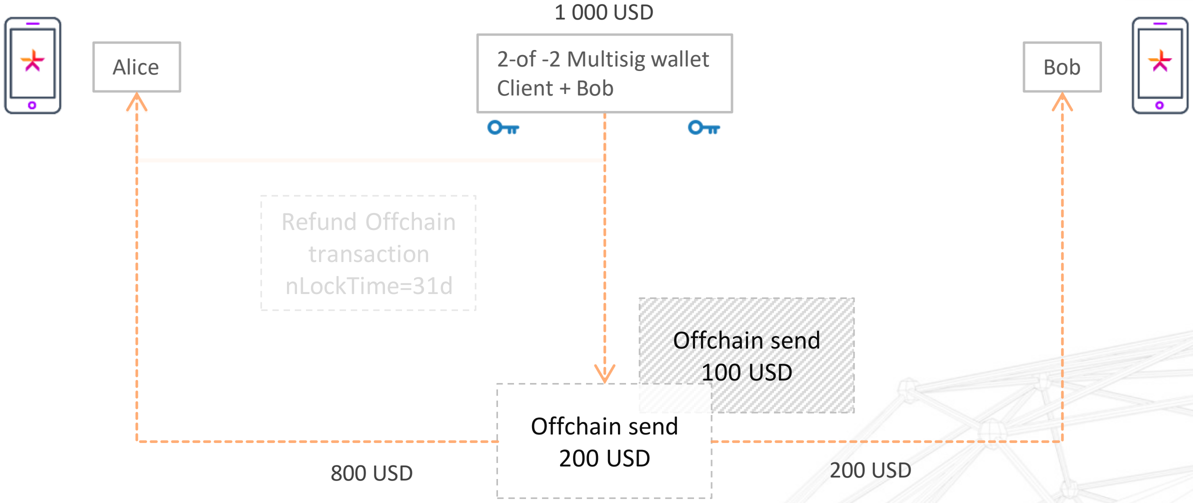
Offchain send
100 USD

0. Output: 900 USD

1. Output: 100 USD

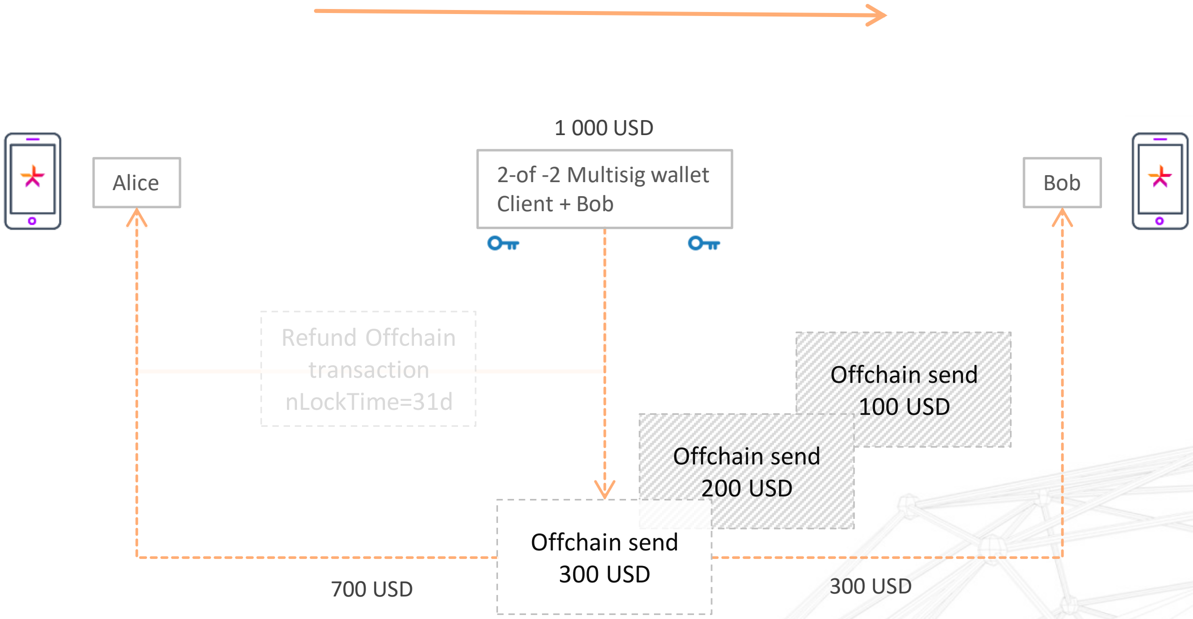
Bitcoin Scaling With Offchain Payment Channels

more 100 USD transfer

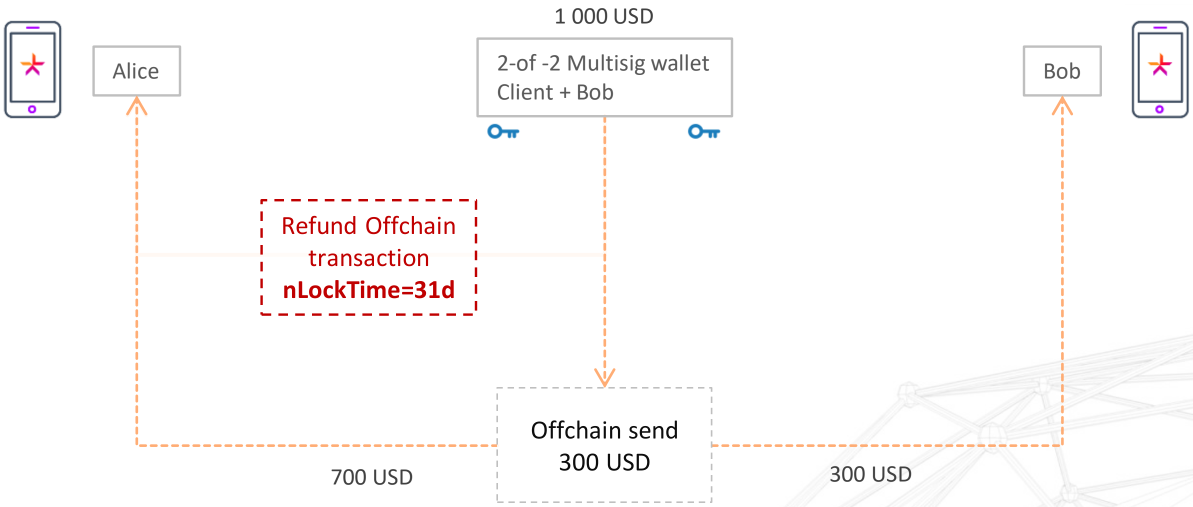


Bitcoin Scaling With Offchain Payment Channels

and more 100 USD transfer



Bitcoin Scaling With Offchain Payment Channels



1 000 USD

2-of -2 Multisig wallet
Client + Bob

Alice

Bob

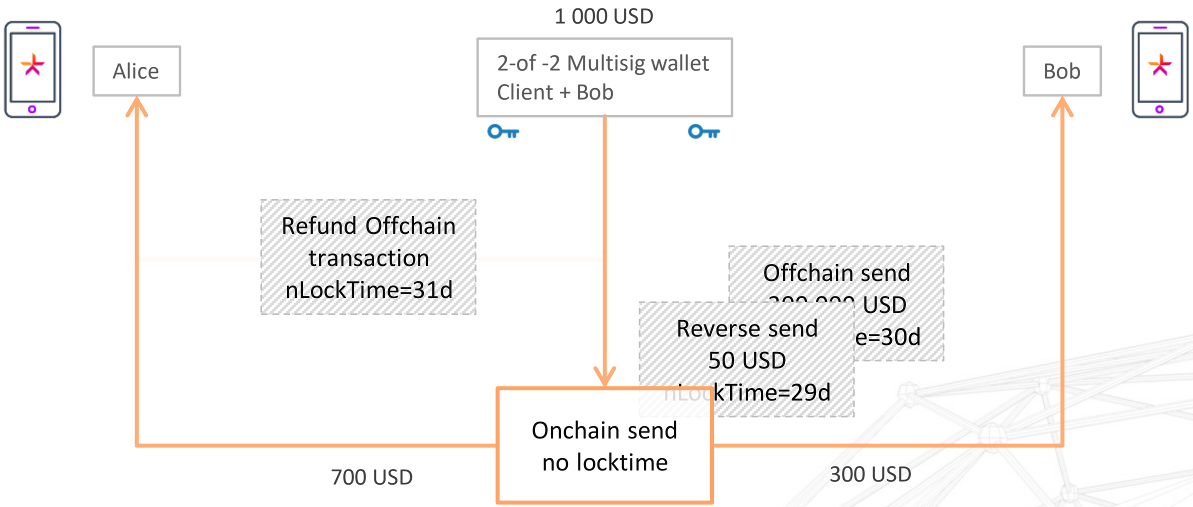
Refund Offchain transaction
nLockTime=31d

Offchain send
300 USD

700 USD

300 USD

Closing Payment Channel



1 000 USD

2-of -2 Multisig wallet
Client + Bob

Alice

Bob

Refund Offchain
transaction
nLockTime=31d

Offchain send
200 000 USD
e=30d

Reverse send
50 USD
nLockTime=29d

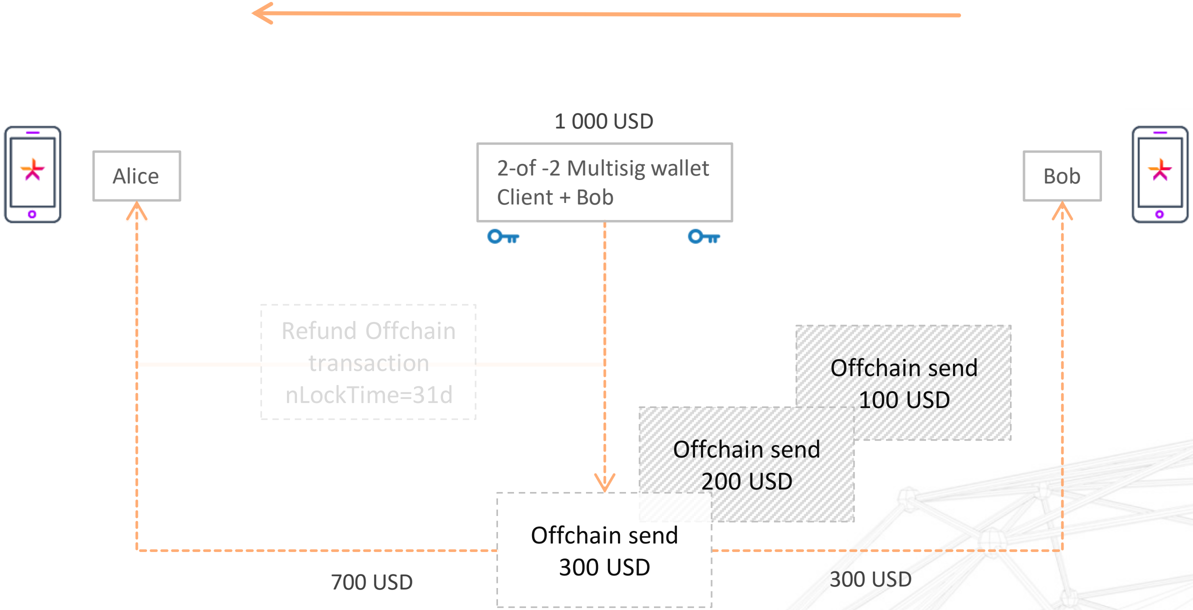
Onchain send
no locktime

700 USD

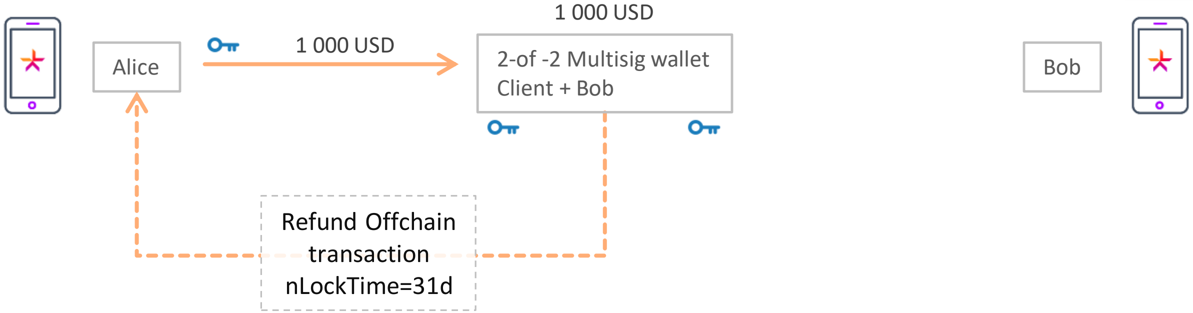
300 USD

Bidirectional Payment Channel

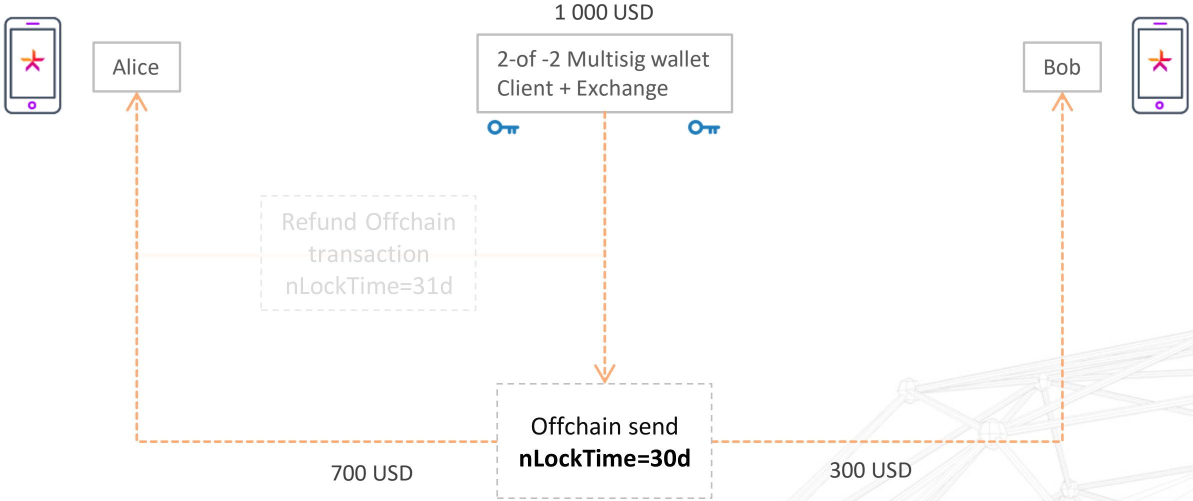
How to transfer in the opposite direction?



Bidirectional Payment Channel

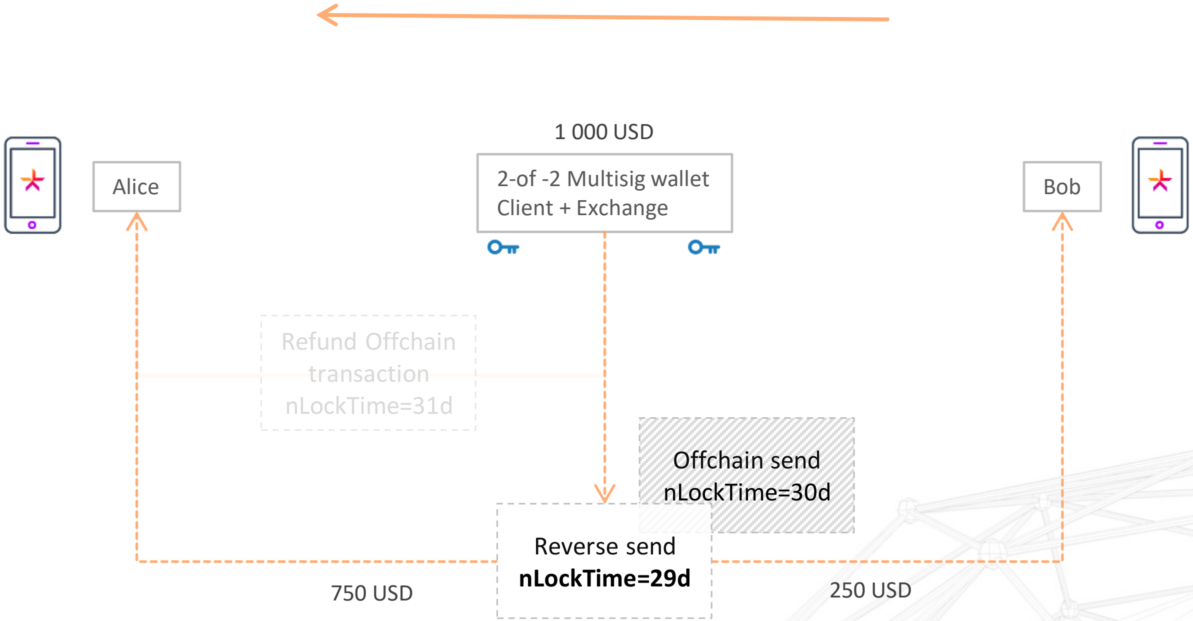


Bidirectional Payment Channel



Bidirectional Payment Channel

50 USD reverse transfer



1 000 USD

2-of -2 Multisig wallet
Client + Exchange

Alice

Bob

Refund Offchain transaction nLockTime=31d

Offchain send nLockTime=30d

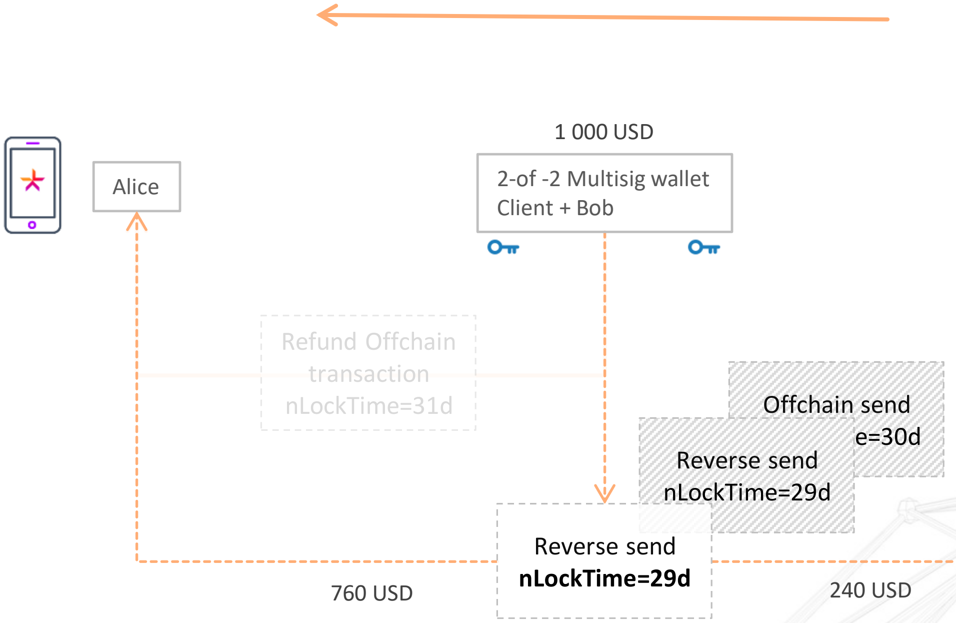
Reverse send
nLockTime=29d

750 USD

250 USD

Bidirectional Payment Channel

10 USD reverse transfer



1 000 USD

2-of -2 Multisig wallet
Client + Bob

Alice

Bob

Refund Offchain
transaction
nLockTime=31d

Offchain send
e=30d

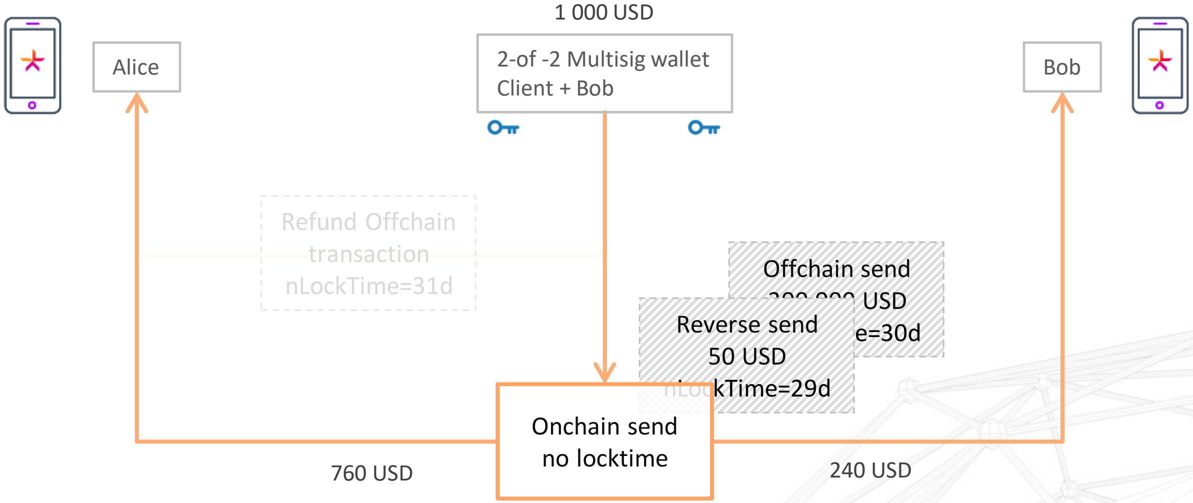
Reverse send
nLockTime=29d

Reverse send
nLockTime=29d

760 USD

240 USD

Closing Bidirectional Payment Channel



Alice

1 000 USD

2-of -2 Multisig wallet
Client + Bob

Bob

Refund Offchain
transaction
nLockTime=31d

Offchain send
200 000 USD
e=30d

Reverse send
50 USD
nLockTime=29d

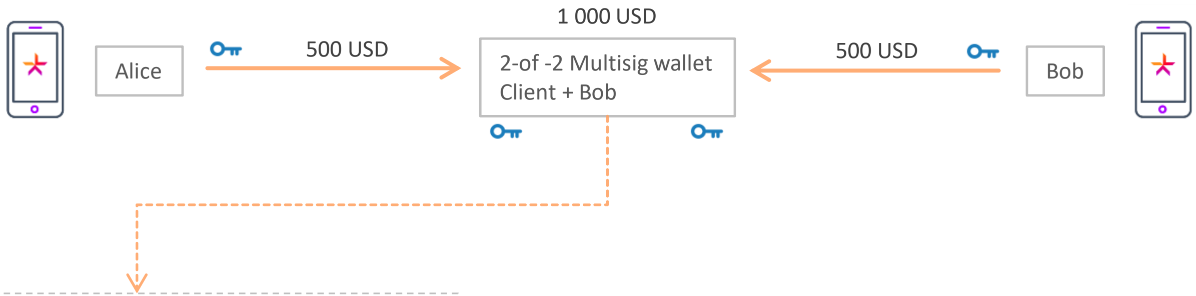
Onchain send
no locktime

760 USD

240 USD

Infinite Bidirectional Payment Channel

OP_CHECKSECVENCEVERIFY (BIP-0112) relative lock-time is available on Bitcoin blockchain from May 2016

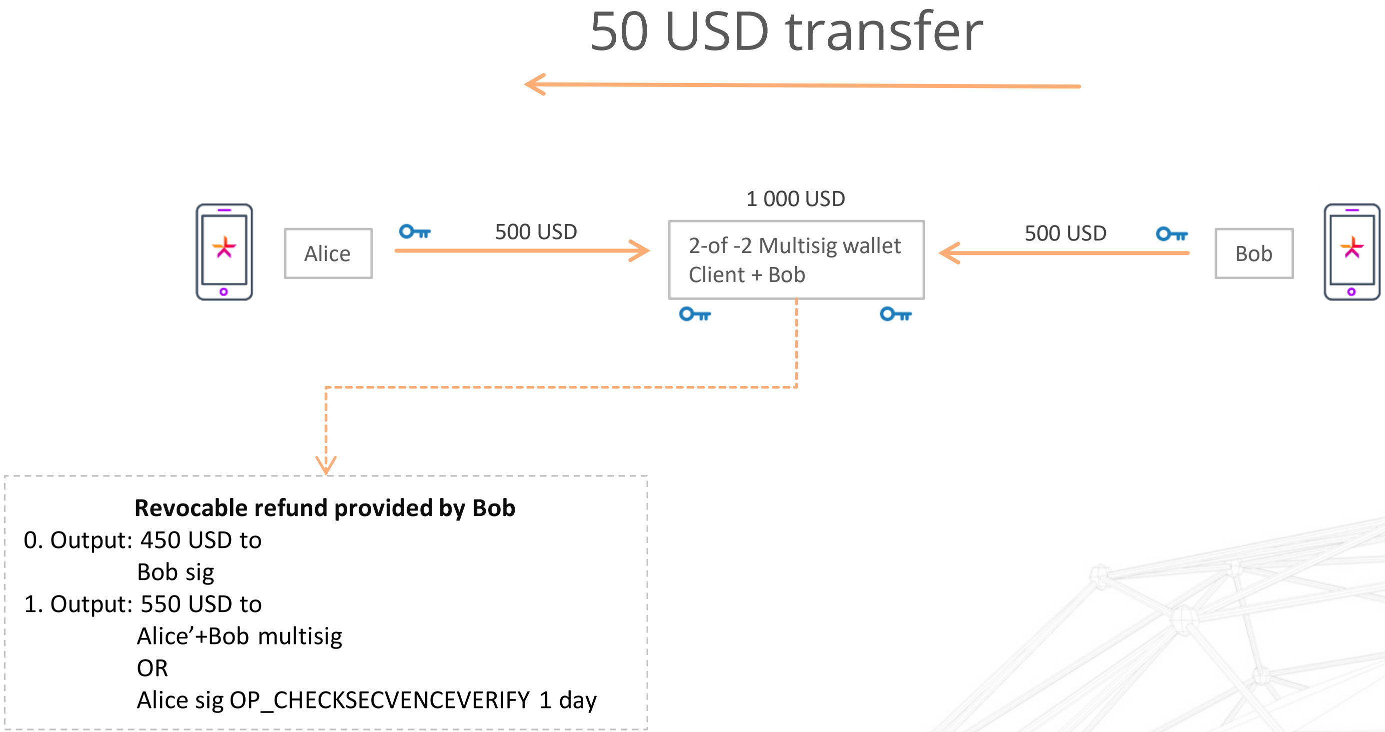


Revocable refund provided by Bob

0. Output: 500 USD to
Bob sig

1. Output: 500 USD to
Alice’+Bob multisig
OR
Alice sig OP_CHECKSECVENCEVERIFY 1 day

Infinite Bidirectional Payment Channel



50 USD transfer

Alice

500 USD

1 000 USD

2-of -2 Multisig wallet
Client + Bob

500 USD

Bob

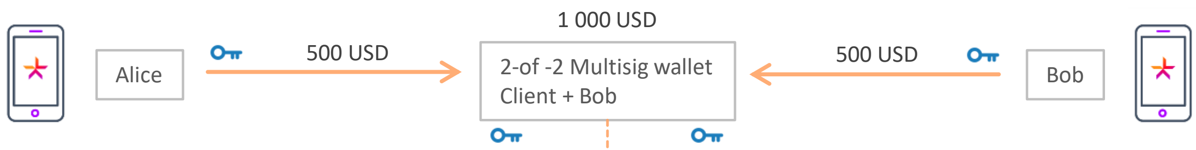
Revocable refund provided by Bob

0. Output: 450 USD to
Bob sig

1. Output: 550 USD to
Alice’+Bob multisig
OR
Alice sig OP_CHECKSECVENCEVERIFY 1 day

Infinite Bidirectional Payment Channel

100 USD transfer



Revoced refund provided by Bob

0. Output: 450 USD to
   Bob sig
1. Output: 550 USD to
   Alice’+Bob multisig
   OR
   Alice sig OP_CHECKSECVENCEVERIFY 1 day

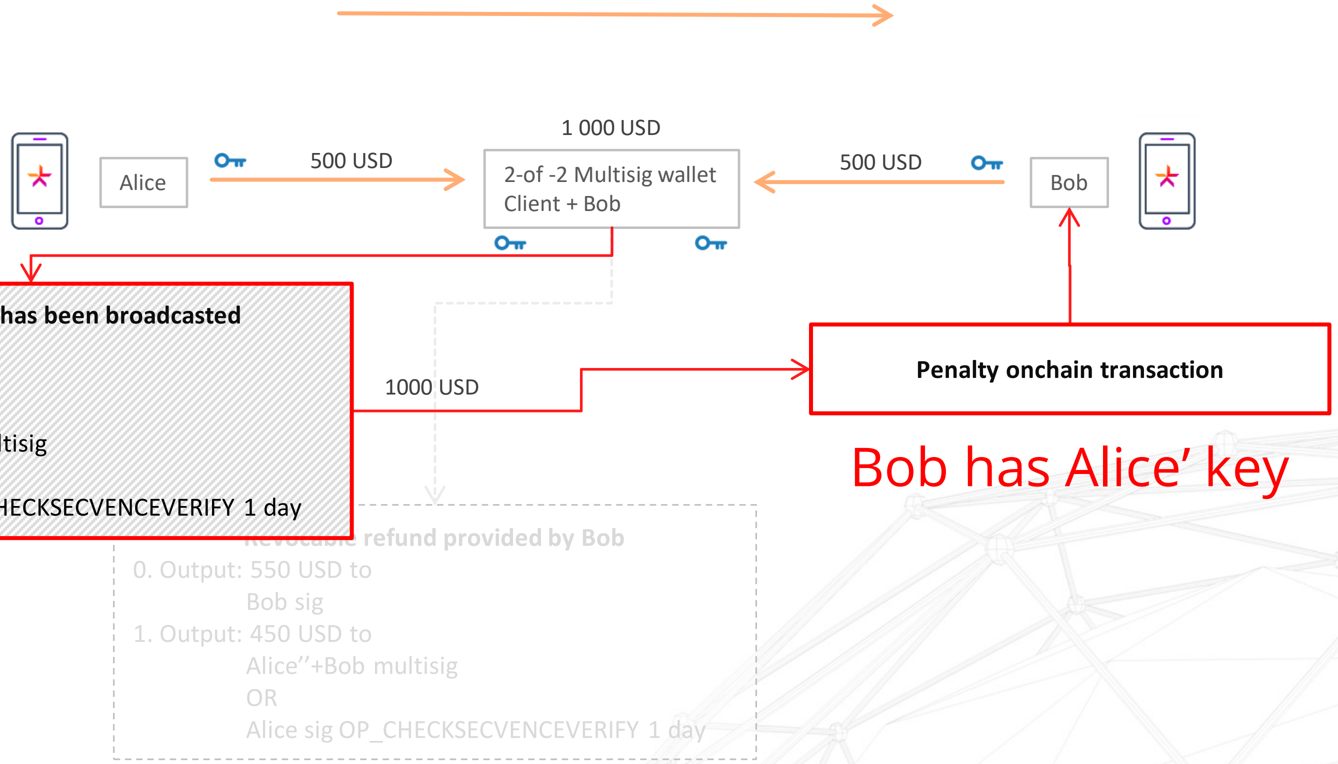
Revocable refund provided by Bob

0. Output: 550 USD to
   Bob sig
1. Output: 450 USD to
   Alice’’+Bob multisig
   OR
   Alice sig OP_CHECKSECVENCEVERIFY 1 day

How Alice can assure Bob that previous transaction will never be broadcasted?

Penalty Channel Transaction

100 USD transfer



Revoked refund has been broadcasted

0. Output: 450 USD to
   Bob sig
1. Output: 550 USD to
   Alice’+Bob multisig
   OR
   Alice sig OP_CHECKSECVENCEVERIFY 1 day

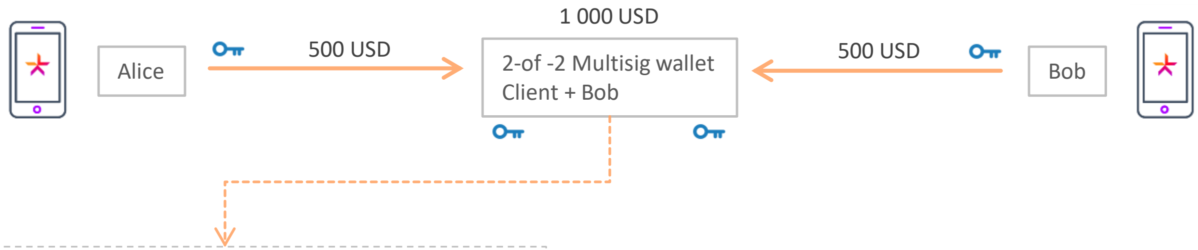
Penalty onchain transaction

Bob has Alice’ key

Revocable refund provided by Bob

0. Output: 550 USD to
   Bob sig
1. Output: 450 USD to
   Alice’’+Bob multisig
   OR
   Alice sig OP_CHECKSECVENCEVERIFY 1 day

Mirrored Refunds for Payment Channel



Alice

500 USD

1 000 USD

2-of -2 Multisig wallet
Client + Bob

500 USD

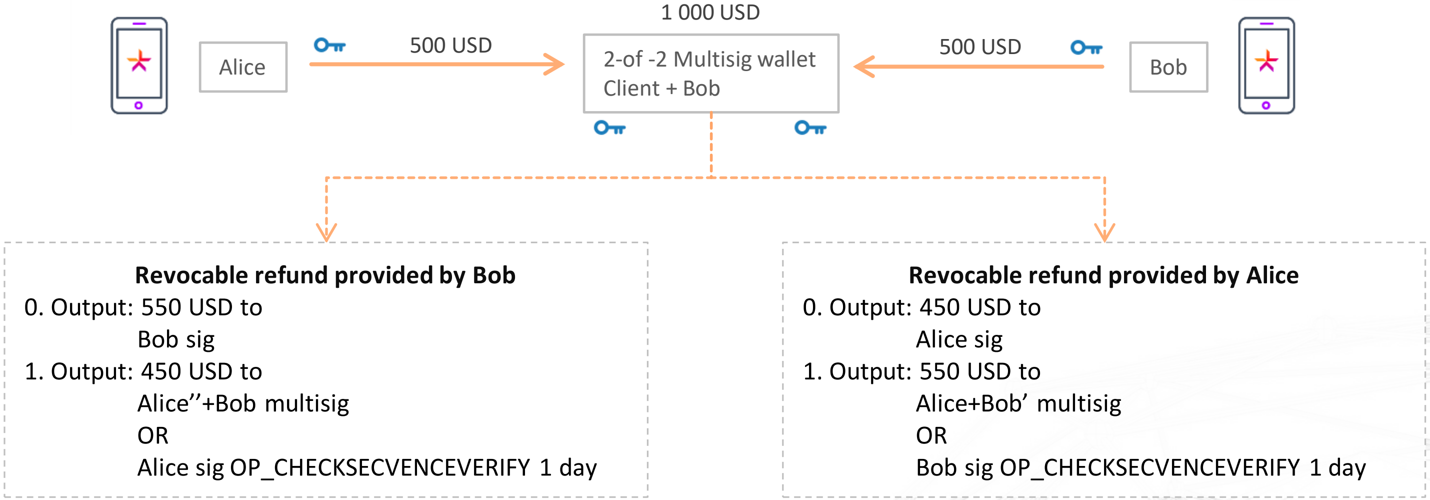
Bob

Revocable refund provided by Bob

0. Output: 550 USD to
   Bob sig
1. Output: 450 USD to
   Alice’’+Bob multisig
   OR
   Alice sig OP_CHECKSECVENCEVERIFY 1 day

How can Bob close the channel?

Mirrored Refunds for Payment Channel



Alice

500 USD

1 000 USD

2-of -2 Multisig wallet
Client + Bob

500 USD

Bob

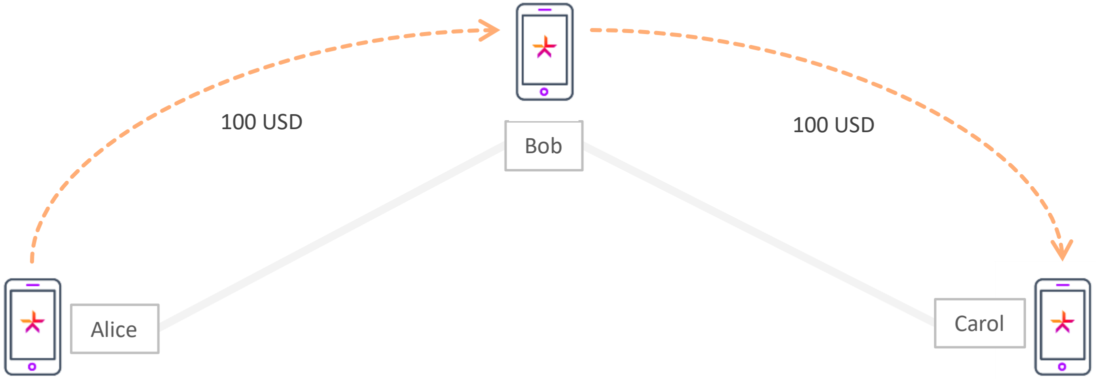
Revocable refund provided by Bob

0. Output: 550 USD to
Bob sig
1. Output: 450 USD to
Alice''+Bob multisig
OR
Alice sig OP_CHECKSECVENCEVERIFY 1 day

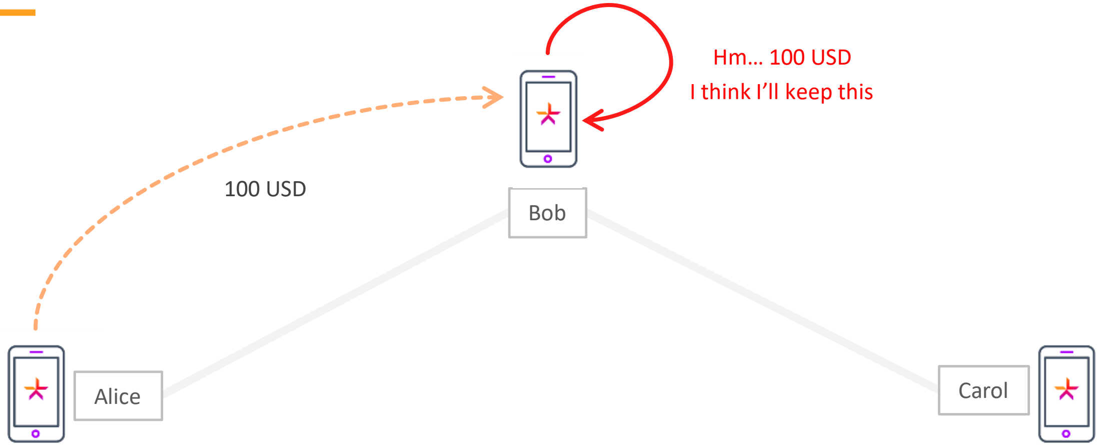
Revocable refund provided by Alice

0. Output: 450 USD to
Alice sig
1. Output: 550 USD to
Alice+Bob' multisig
OR
Bob sig OP_CHECKSECVENCEVERIFY 1 day

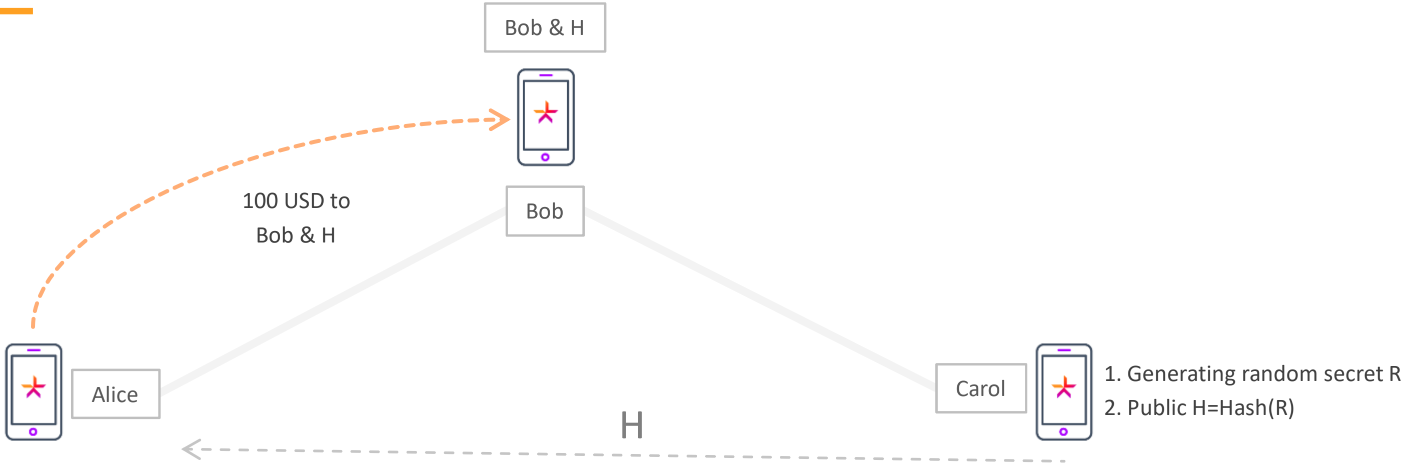
3 Party Channels



3 Party Channels – Trust Issue



3 Party Channels – Hash Locks



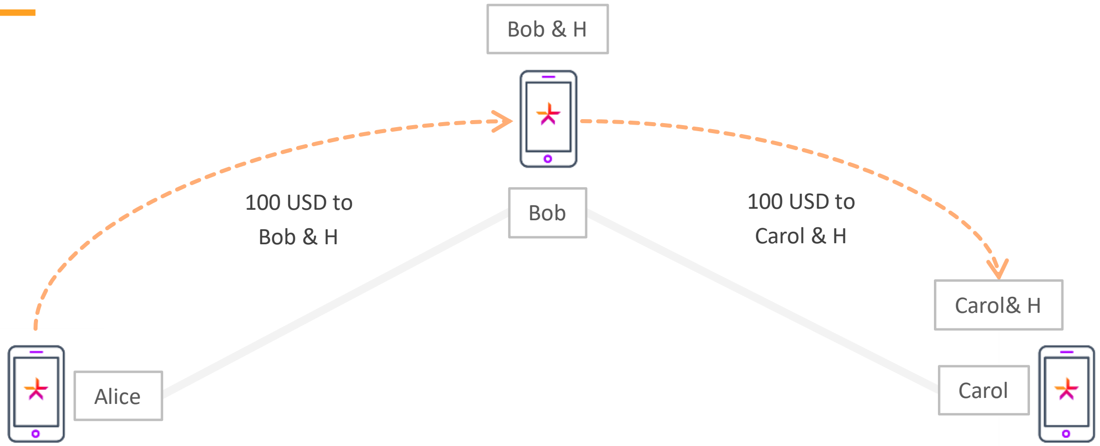
1. Generating random secret R
2. Public H=Hash(R)

Hash-Locked contracts:

1. Using one-way hash functions – Alice can prove that she sent funds to Carol off-chain
2. Alice pays to Contract (output: Bob & H)

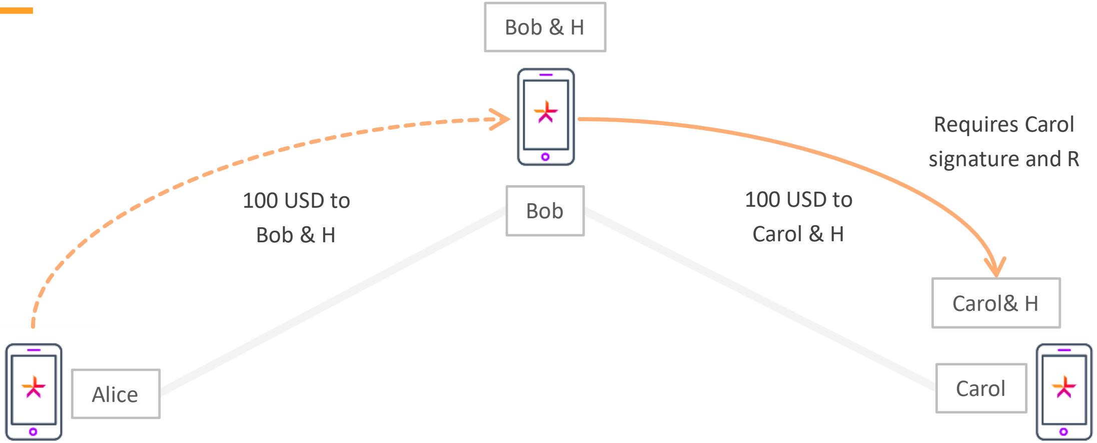
Bob needs to know R to spend the funds.

3 Party Channels – Hash Locks

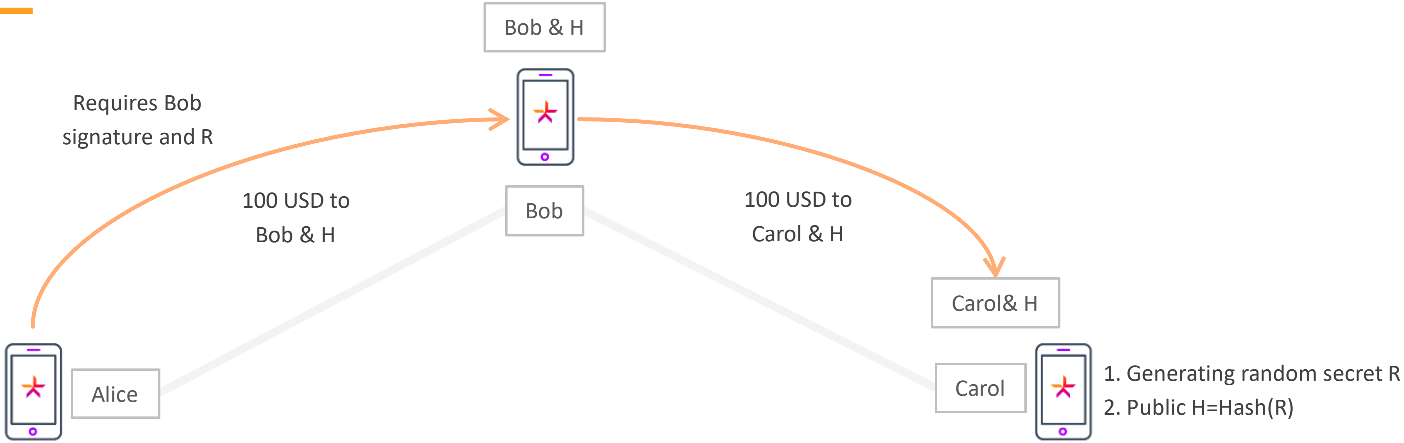


1. Generating random secret R
2. Public H=Hash(R)

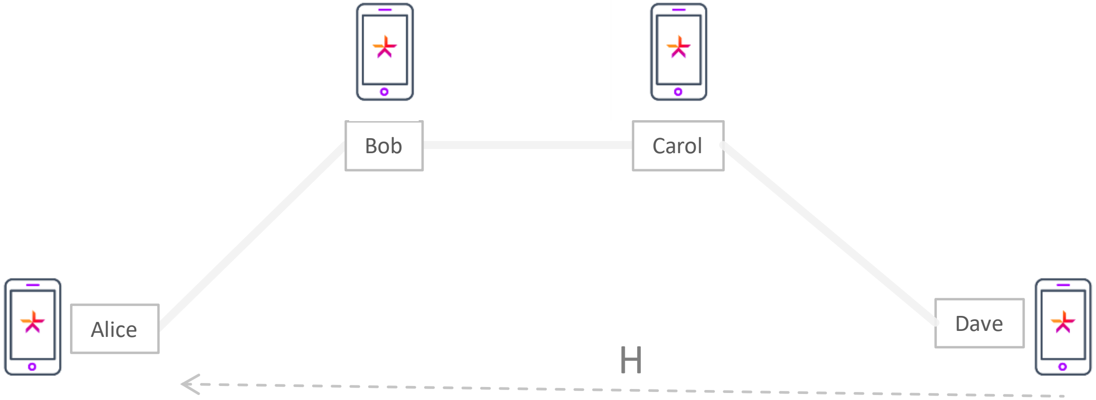
3 Party Channels – Hash Locks



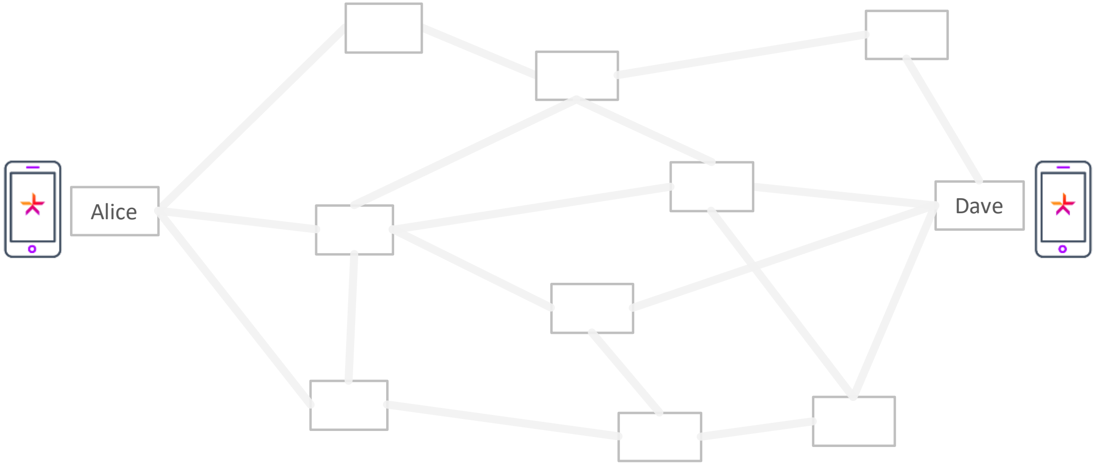
3 Party Channels – Hash Locks



3+ Party Channels



Lightning Network



1. Generating random secret R
2. Public H=Hash(R)

Alice wants to pay to Dave.
Dave says:

1. Here is my H
2. If you know R consider payment fulfilled