Perm Summer School 2017

Bitcoin Blockchain technology

Mihail Nikulin, Co-founder & CTO, Lykke

What is money?

Copy protection consensus

Consensus based on top of proof of existence

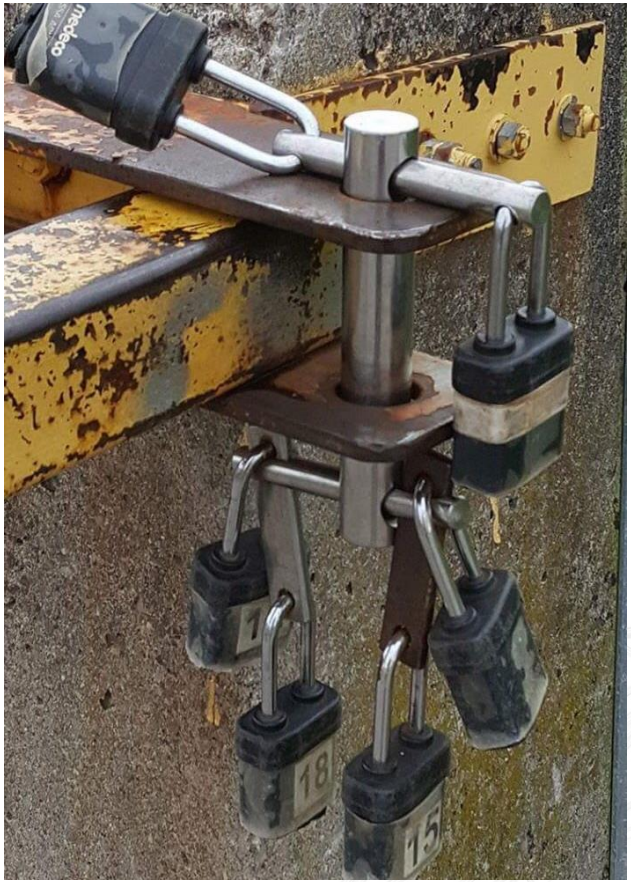
Mining is burning electricity

Colored Coins

	BTC/ETH/Some tokens	Colored coins/Some tokens
Issuer	undefined	Companies, Individuals
Issuance limit	limited	Unlimited
Price	Defined by market	Linked to the real asset
Market risk	Yes	No
Counterparty risk	No (???)	Issuer
Protocol risk	Miners/Smartcontract	Counterparties/Smartcontract

Any centralized service is to be hacked

MultiSig wallet is needed

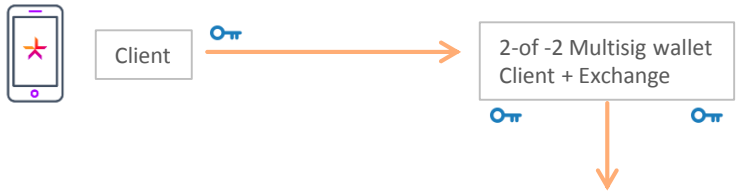


MultiSig wallets

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



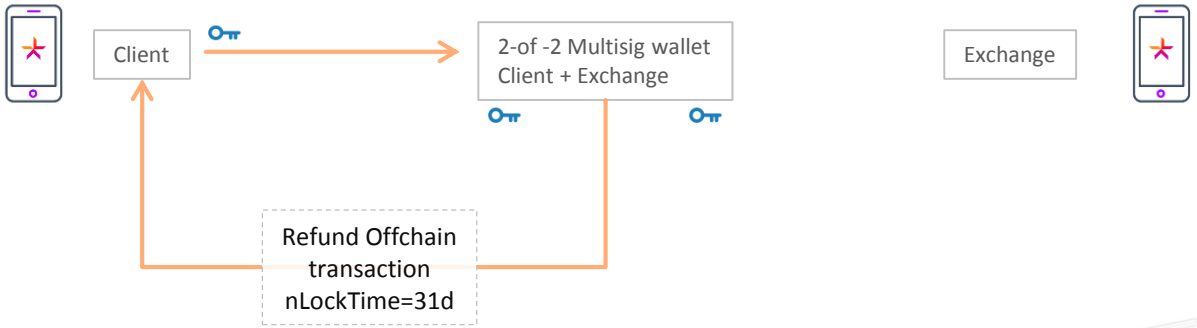
MultiSig wallets advantages

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

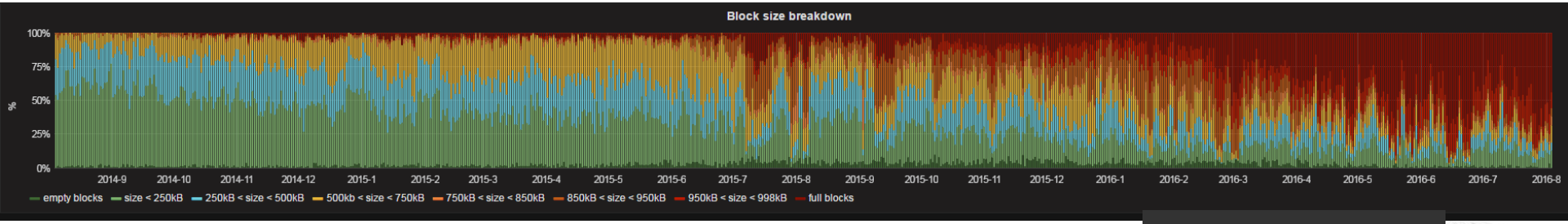
Bitcoin Scaling Issues

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 (!)

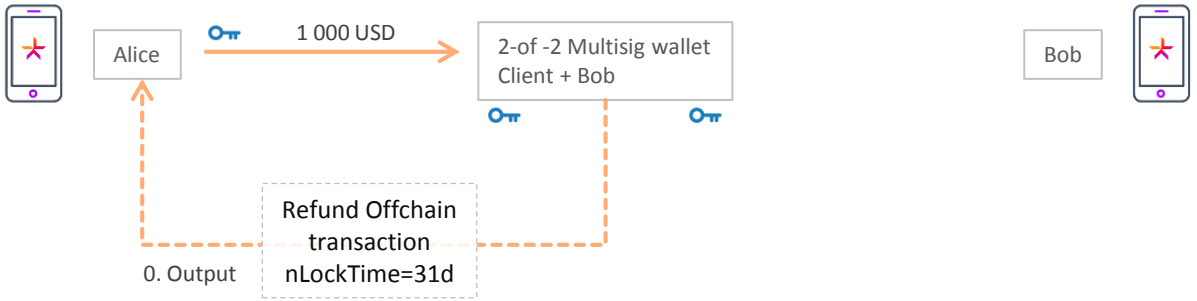
1 Billion people doing 2 transaction per day:

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

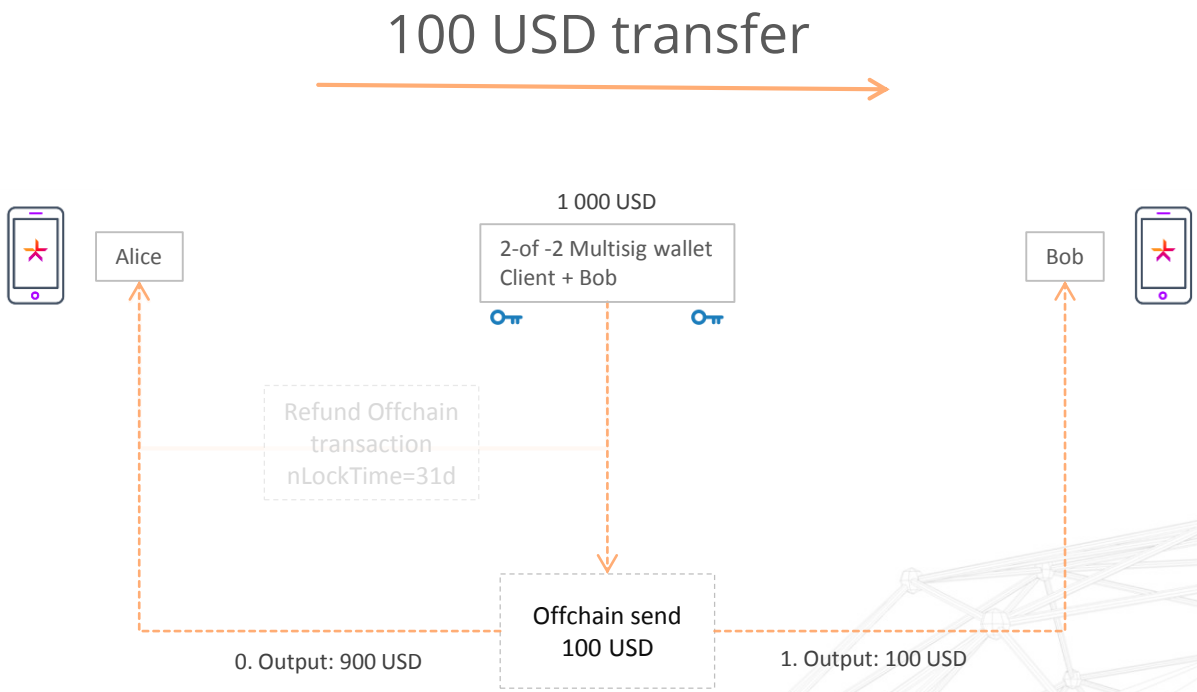
Bigger block = Centralization

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

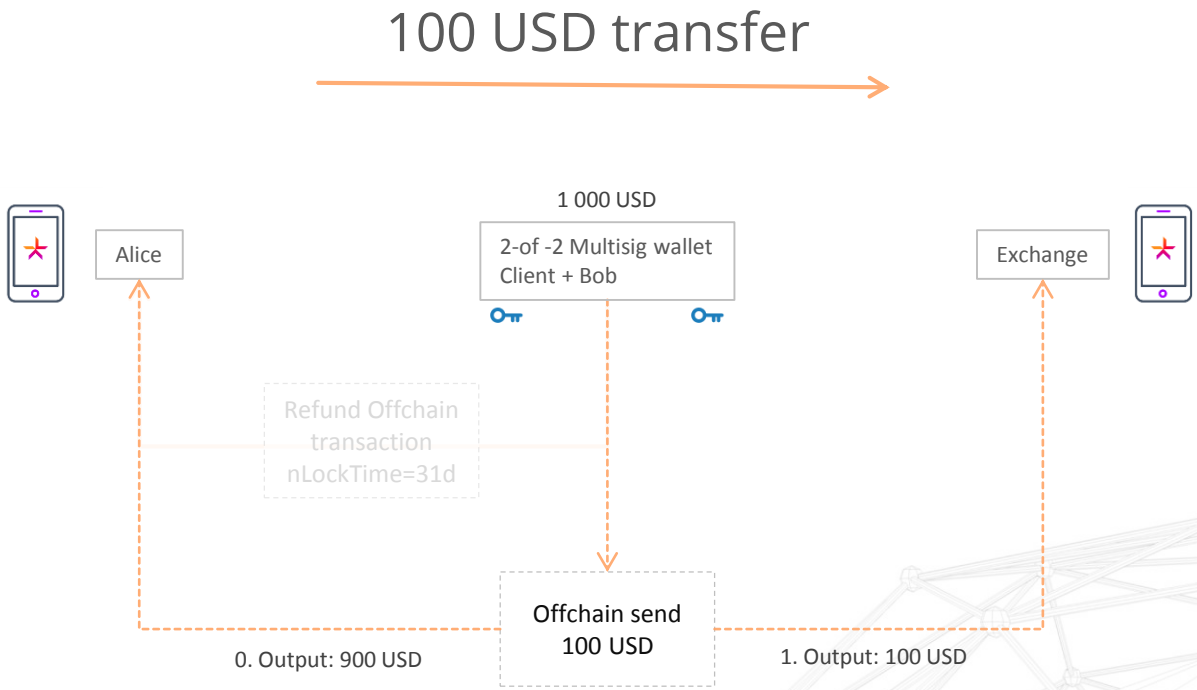
Bitcoin Scaling With Offchain Payment Channels



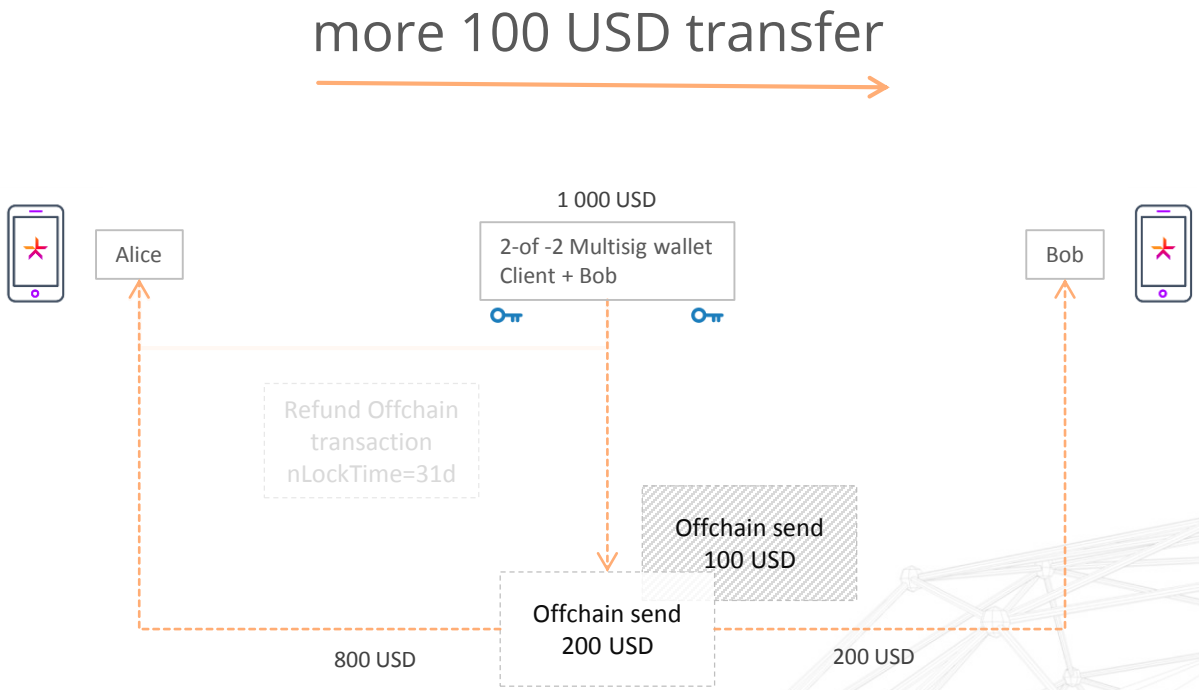
Bitcoin Scaling With Offchain Payment Channels



Bitcoin Scaling With Offchain Payment Channels

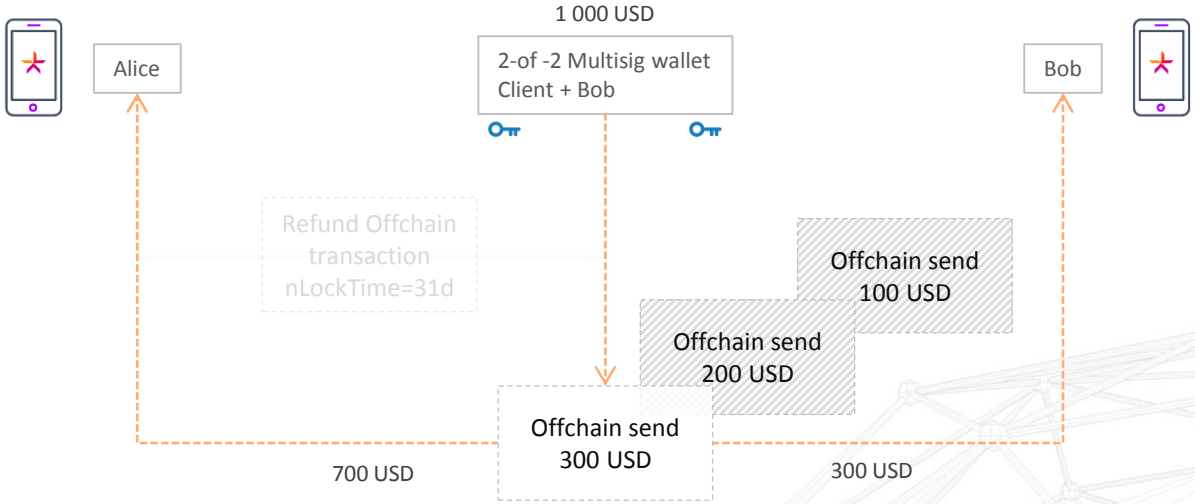


Bitcoin Scaling With Offchain Payment Channels

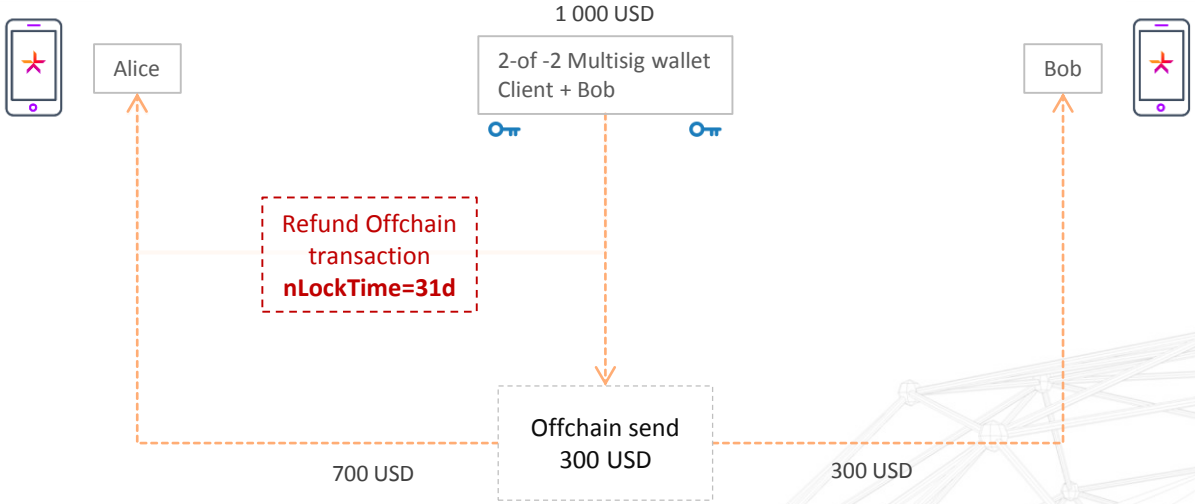


Bitcoin Scaling With Offchain Payment Channels

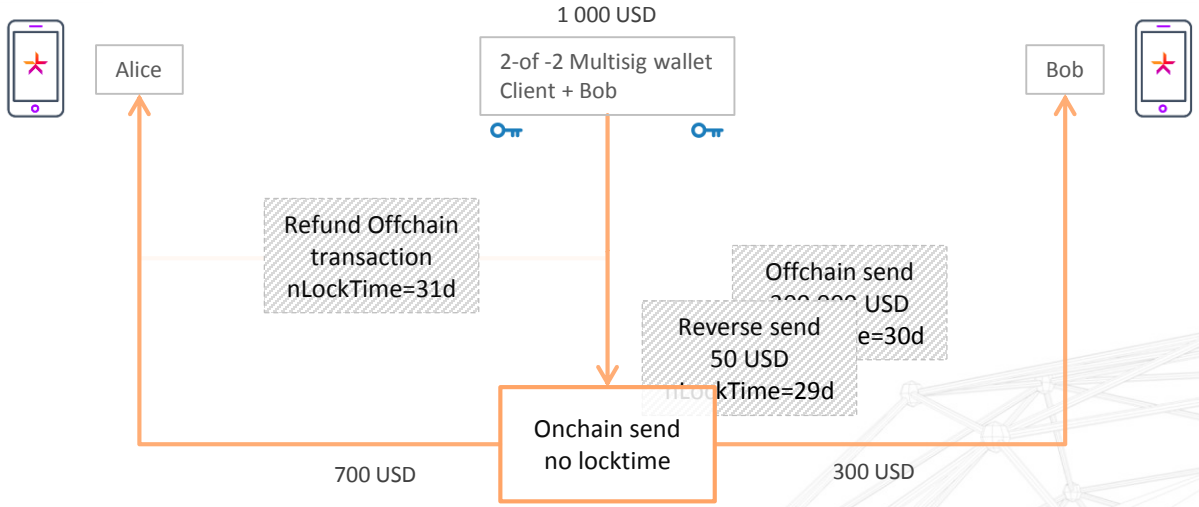
and more 100 USD transfer



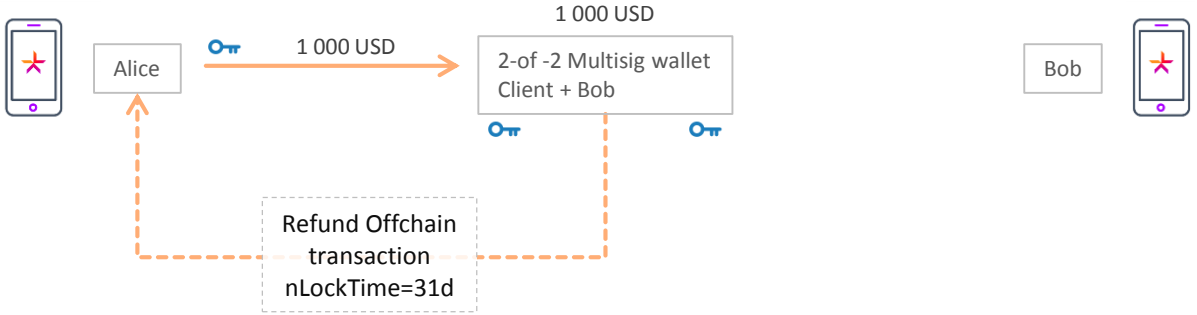
Bitcoin Scaling With Offchain Payment Channels



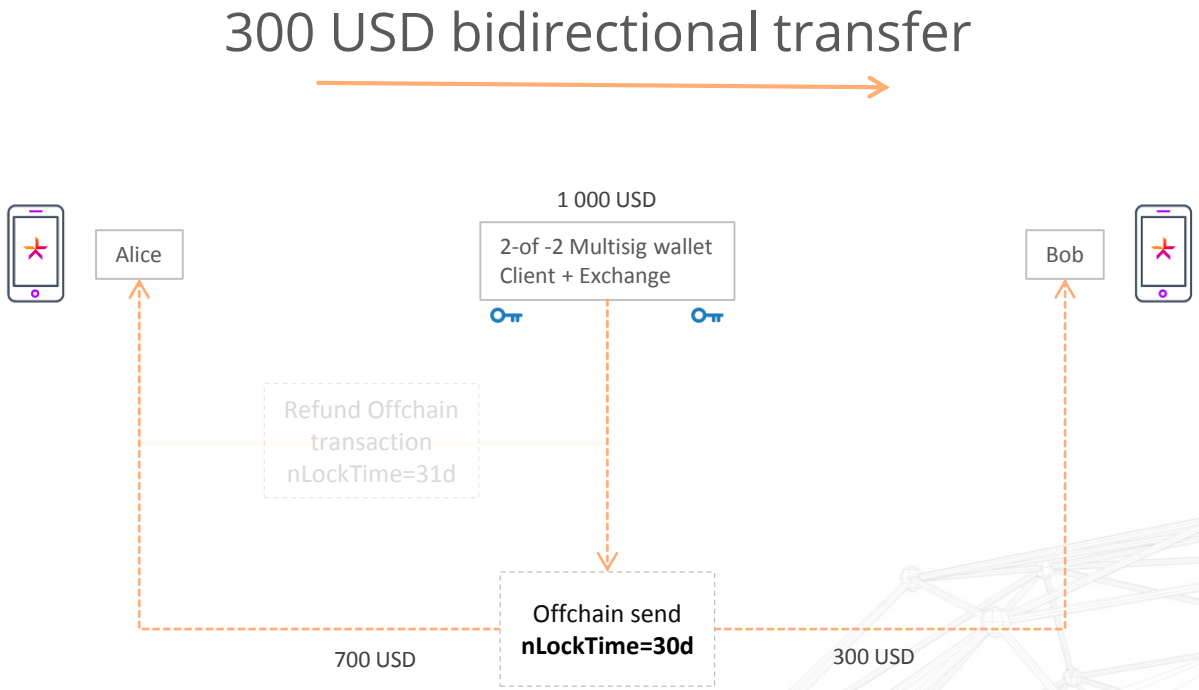
Closing Payment Channel



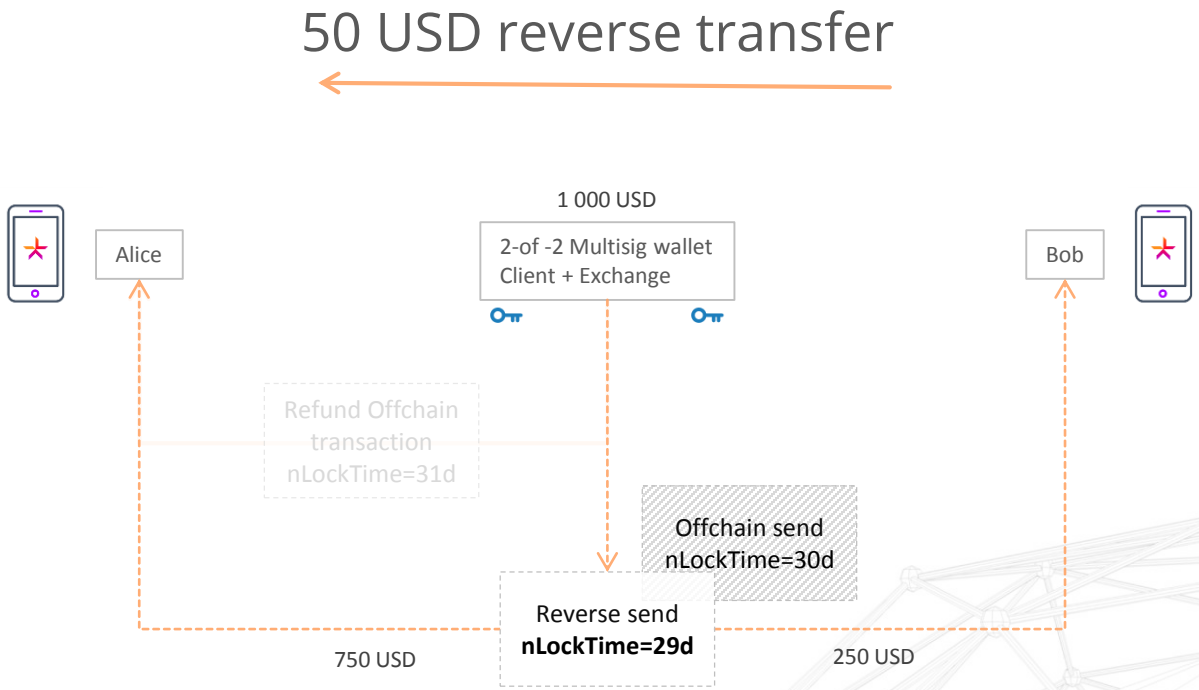
Bidirectional Payment Channel



Bidirectional Payment Channel

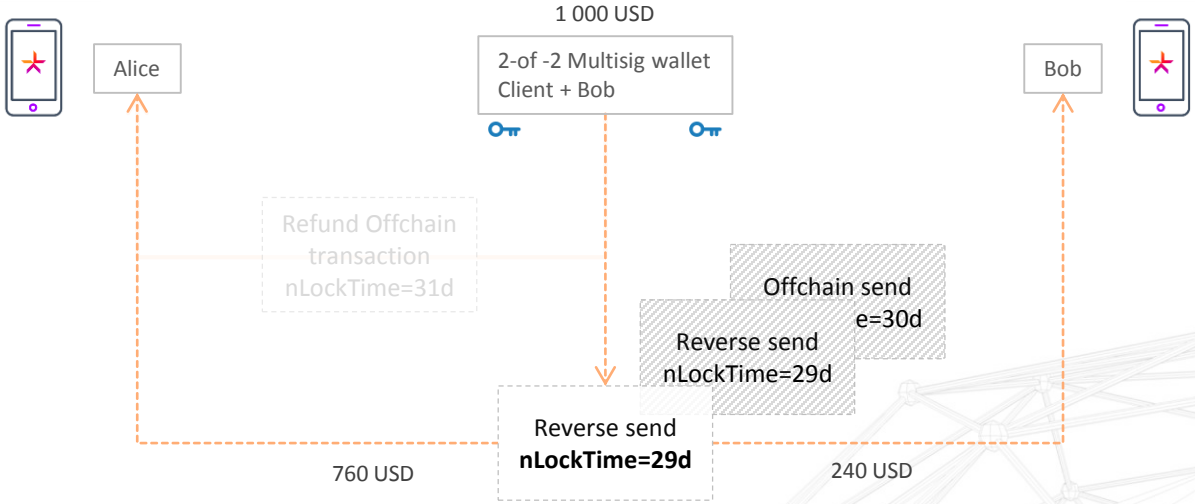


Bidirectional Payment Channel

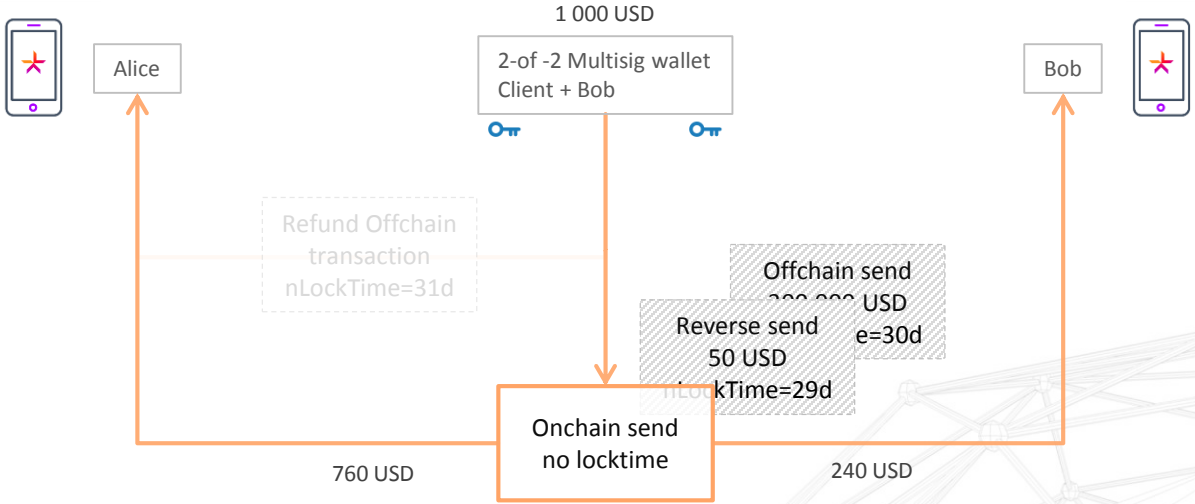


Bidirectional Payment Channel

10 USD reverse transfer

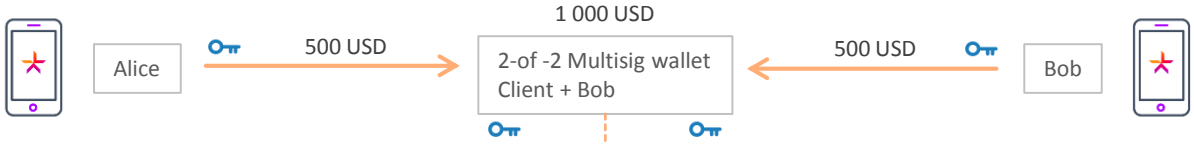


Closing Bidirectional Payment Channel



Infinite Bidirectional Payment Channel

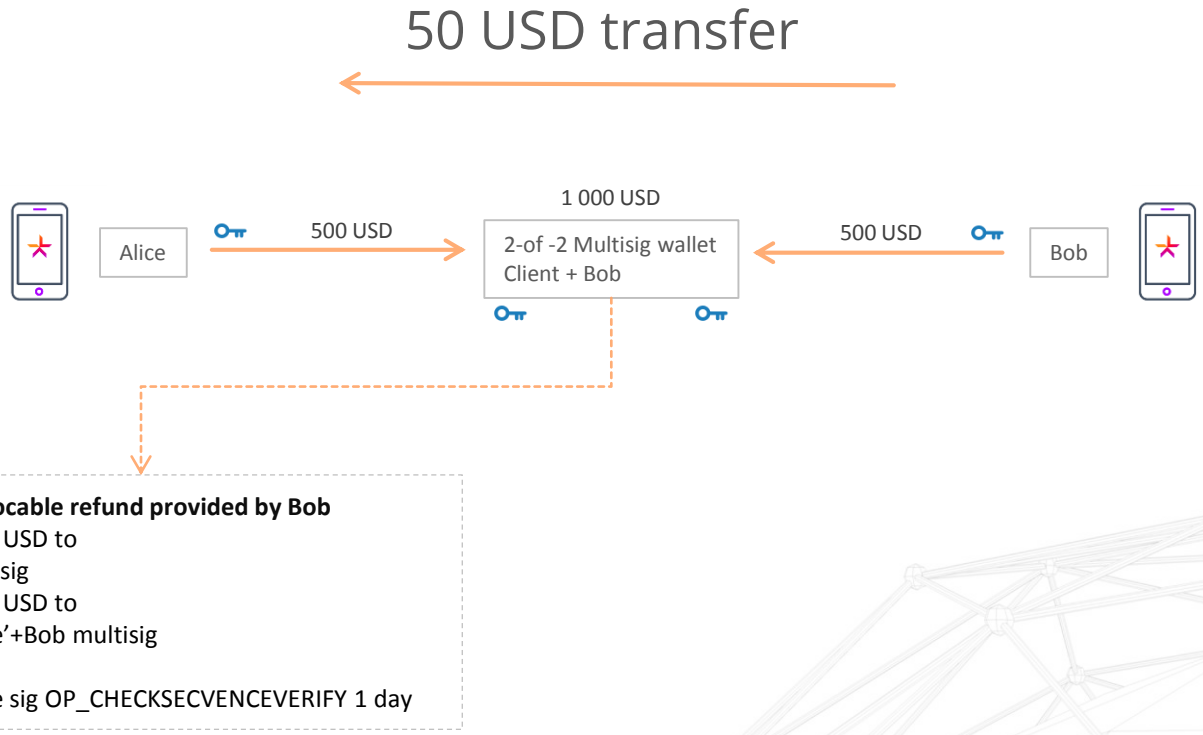
OP_CHECKSECVENCEVERIFY (BIP-0112) relative lock-time is available on Bitcoin blockchain from May 2016



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



Infinite Bidirectional Payment Channel

Revoced refund provided by Bob

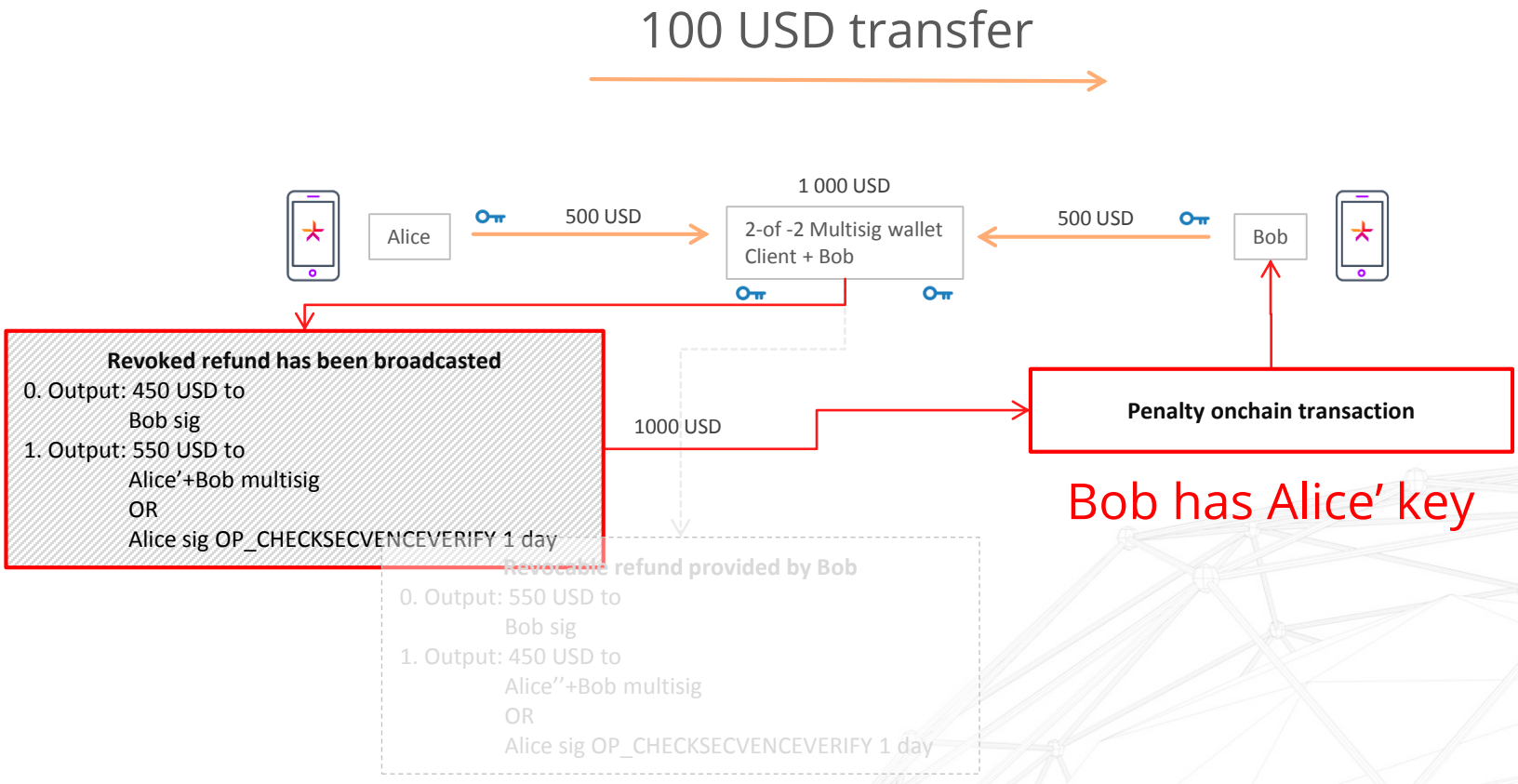
0. Output: 450 USD to
   Bob sig
1. Output: 550 USD to
   Alice'+Bob multisig
   OR
   Alice sig OP_CHECKSECVENCEVERIFY 1 day

Revocable refund provided by Bob

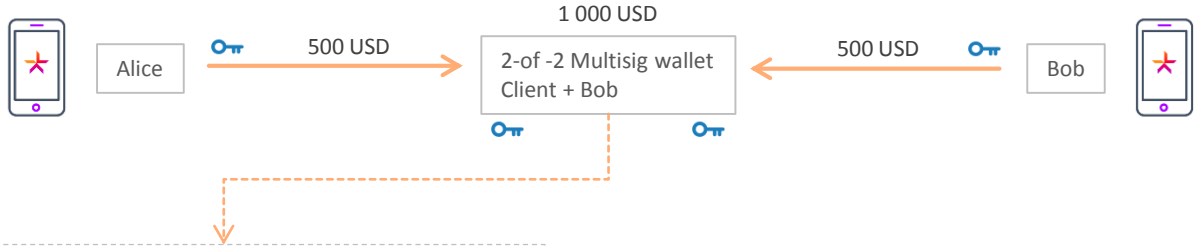
0. Output: 550 USD to
   Bob sig
1. Output: 450 USD to
   Alice''+Bob multisig
   OR
   Alice sig OP_CHECKSECVENCEVERIFY 1 day

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

Penalty Channel Transaction



Mirrored Refunds for Payment Channel

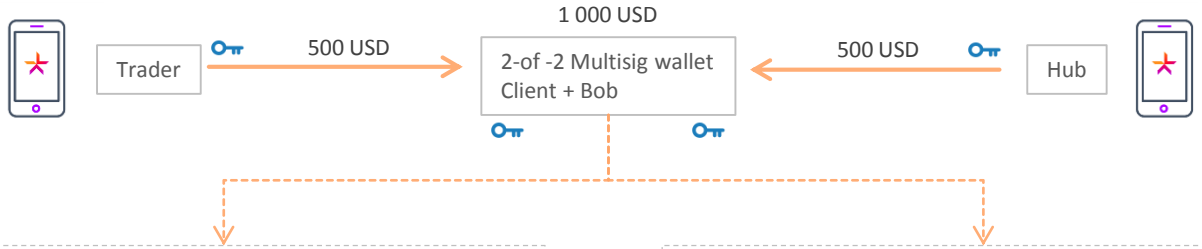


Revocable refund provided by Bob

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



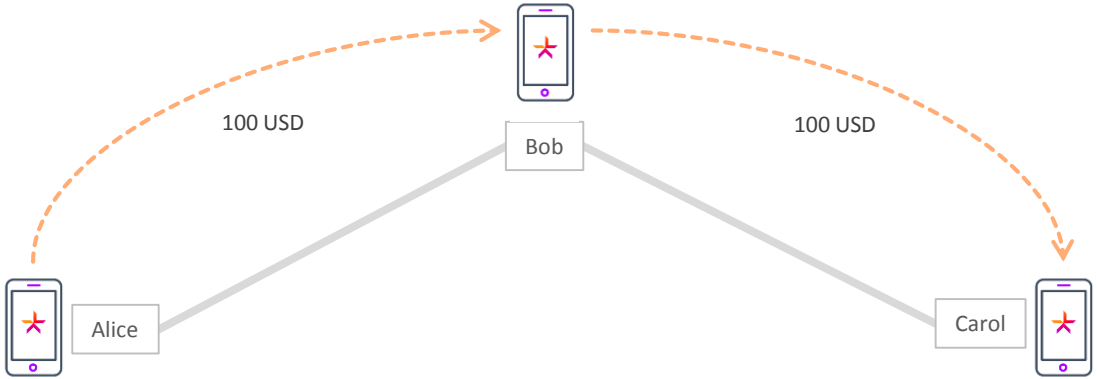
Revocable refund provided by Hub

0. Output: 500 USD to
   Hub sig
1. Output: 500 USD to
   Trader'+Hub multisig
   OR
   Trader sig OP_CHECKSECVENCEVERIFY 1 day

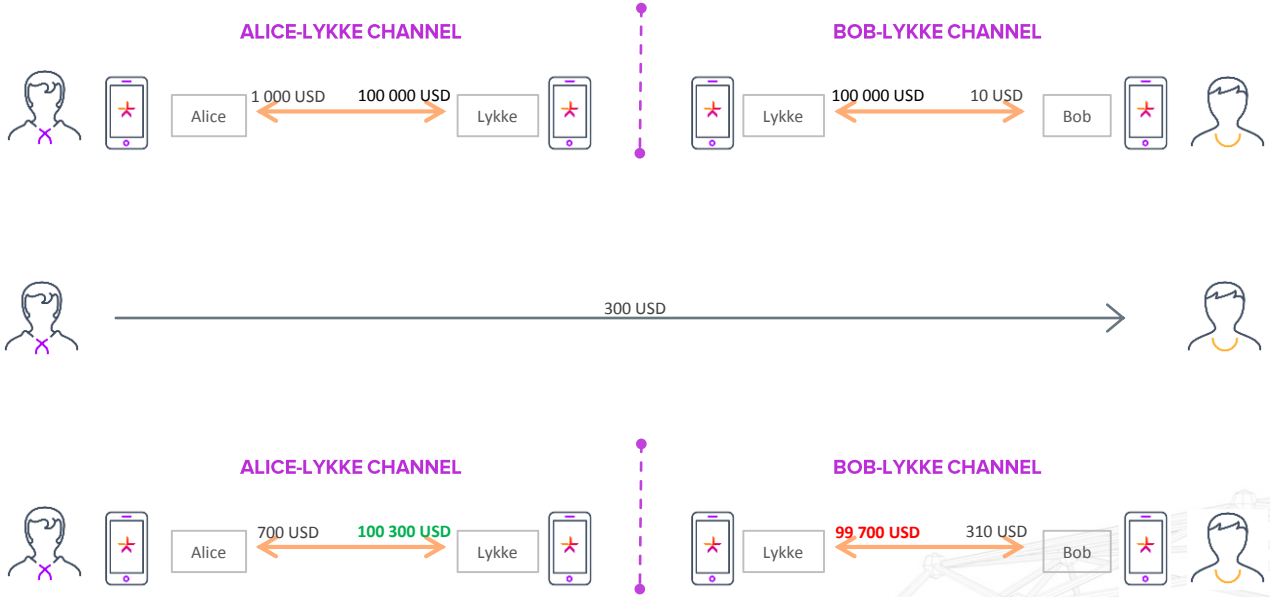
Revocable refund provided by Trader

0. Output: 500 USD to
   Trader sig
1. Output: 500 USD to
   Trader+Hub' multisig
   OR
   Hub sig OP_CHECKSECVENCEVERIFY 1 day

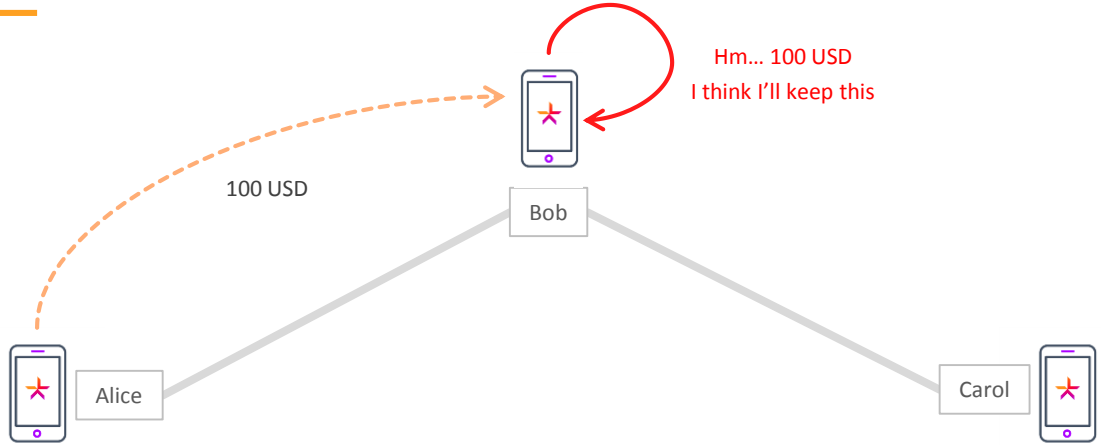
3 Party Channels



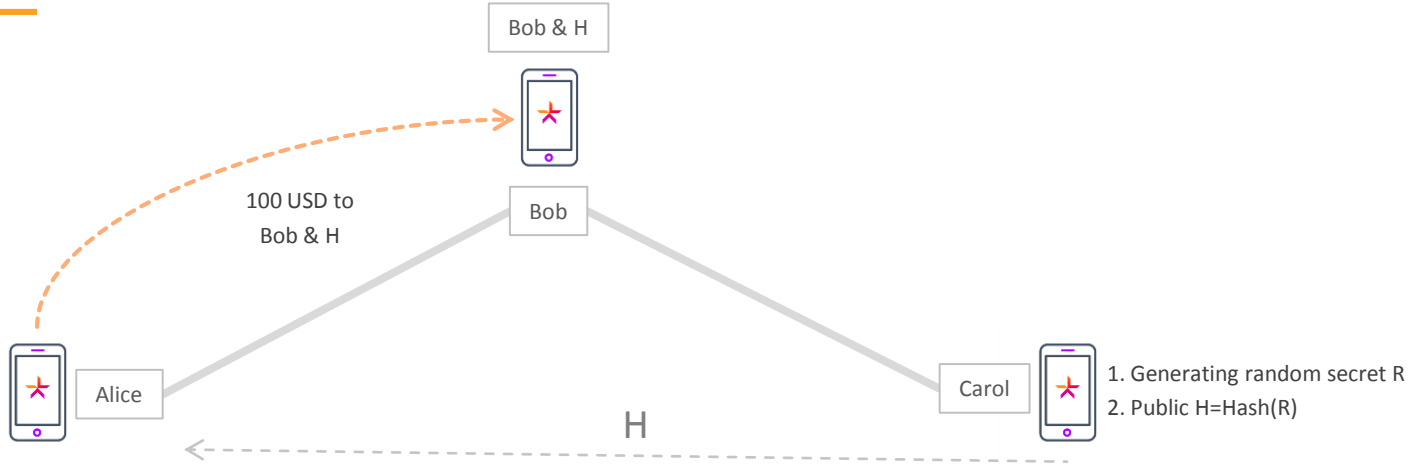
Offchain payments



3 Party Channels – Trust Issue



3 Party Channels – Hash Locks

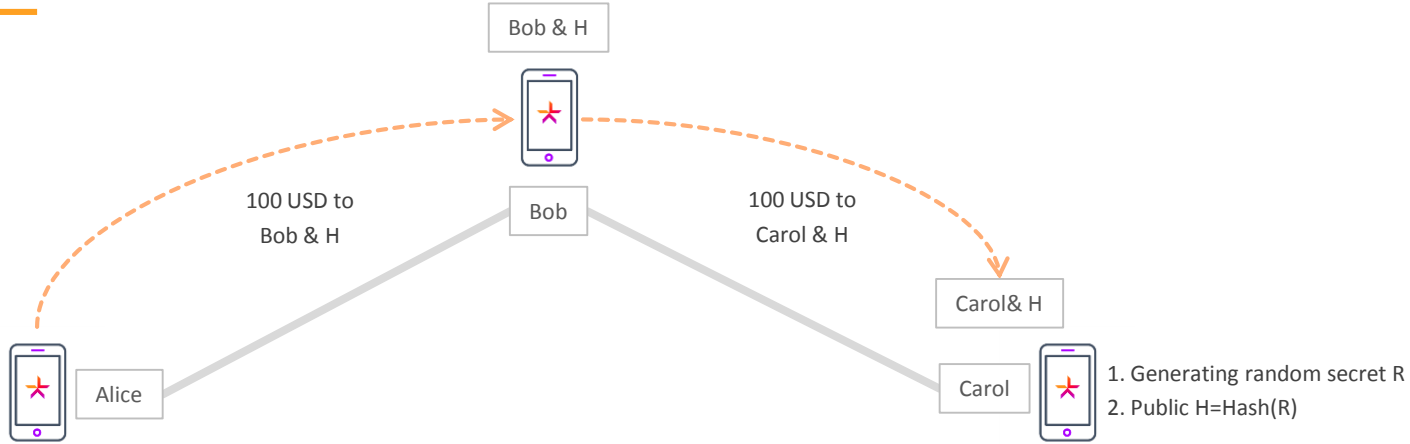


Hash-Locked contracts:

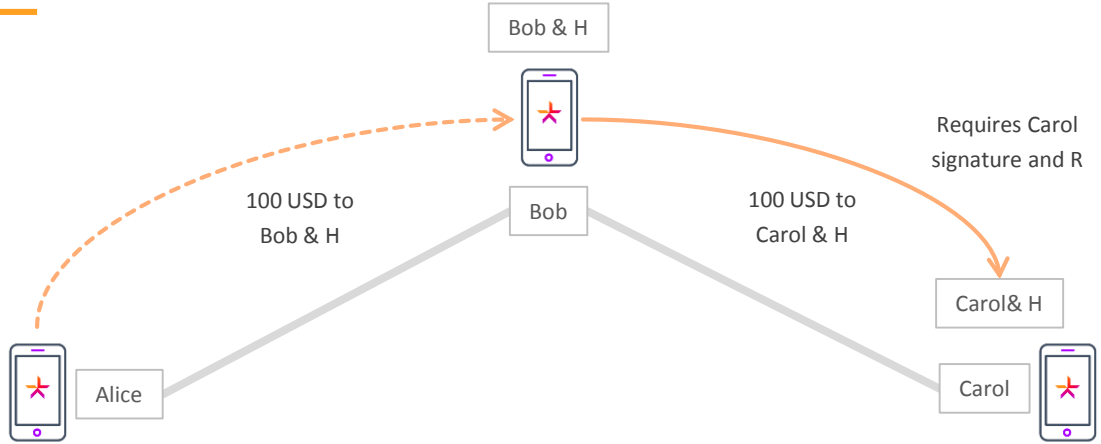
1. Using one-way hash functions – Alice can prove that she sent funds to Carol off-chain
2. Alice pays to Contract (output: Bob & H)

Bob needs to know R to spend the funds.

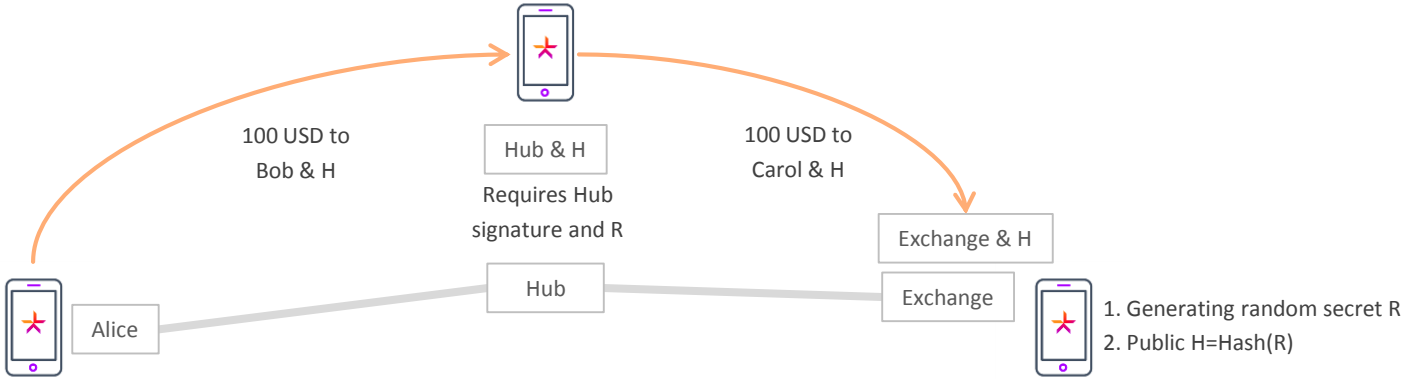
3 Party Channels – Hash Locks



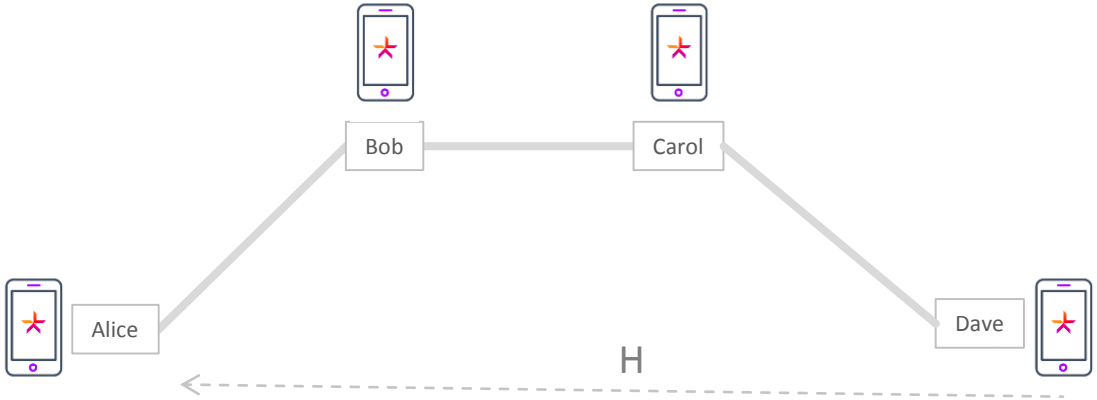
3 Party Channels – Hash Locks



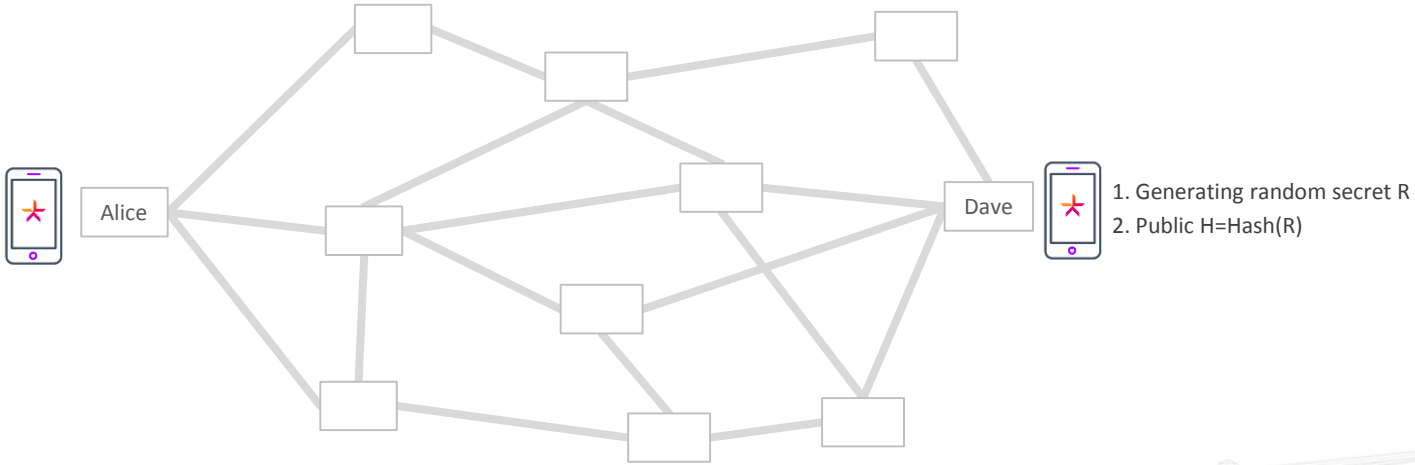
3 Party Channels – Hash Locks



3+ Party Channels



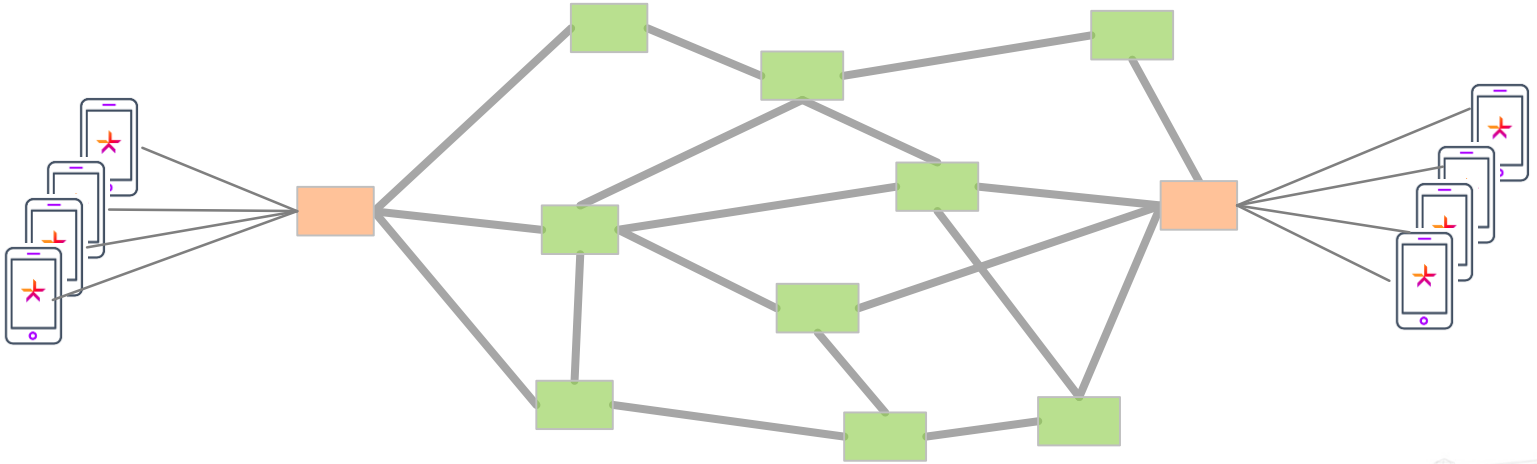
Lightning Network



Alice wants to pay to Dave.
Dave says:

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

Lightning Network Topology



Offchain Settlement

BTC CHANNELS SNAPSHOT – 04 JUL 2017

Multisignature address	Client	Liquidity Hub
34i3ozADy8yknSPow4hfZevVUHE1gDEBMt	0.03073017	37.16926983
37zGsNecseFBYUEt2Q79vq5R4RJDsAjR7G	2.20091438	26.38003815
3GAkHd3dZhowFHqzQgmWGtCdKa1LDfQ9wT	6.75324318	22.24675682
35RgpgT11WJRW8vSqCTvny66eipGgYKWwz	2.53595479	17.46404521
3CN3UqxgZybCsEitdkMp8YUVmLaSweYvYH	0.00604847	14.99395153
…	…	…
3BFHeiYAo3BeGmzagQCzDobguVp7i6D5iR	0.00002917	0
3B73AV9i9EiVyuYYyTEWV55M3NfnTbjrpR	0.00002892	0
TOTAL in 2249 ‘BTC’ CHANNELS	**726.5220753**	**1104.964189**

Offchain Settlement Statistics

NUMBER OF OPERATIONS 28 JUN 2017 – 04 JUL 2017

Operation	ONCHAIN	OFFCHAIN	TOTAL
BUY SETTLEMENTS	1140	1991	3131
SELL SETTLEMENTS	163	2176	2339
BLOCKCHAIN CASH OUT (BTC, LKK)	520	-	520
CASHIN (fiat…)	104	414	518
BLOCKCHAIN CASHIN (BTC, LKK)	289	-	289
HUB'S CHANNEL WITHDRAWALS	76	-	76
CASHOUT (fiat…)	0	65	65
	2292	**4646**	**6938**

Offchain Settlement Statistics

NUMBER OF OPERATIONS 28 JUN 2017 – 04 JUL 2017

Asset	ONCHAIN	OFFCHAIN	TOTAL
BTC	1249	642	1891
USD	156	1498	1654
LKK	622	760	1382
CHF	40	722	762
EUR	33	422	455
TIME	35	222	257
LKK1Y	81	167	248
SLR	25	82	107
GBP	16	78	94
HCP	28	25	53
JPY	2	23	25
HKD	0	3	3
XAU	2	0	2
XPT	1	0	1
XAG	0	1	1
RUB	1	0	1
RRB	0	1	1
ILS	1	0	1
TOTAL	**2292**	**4646**	**6938**

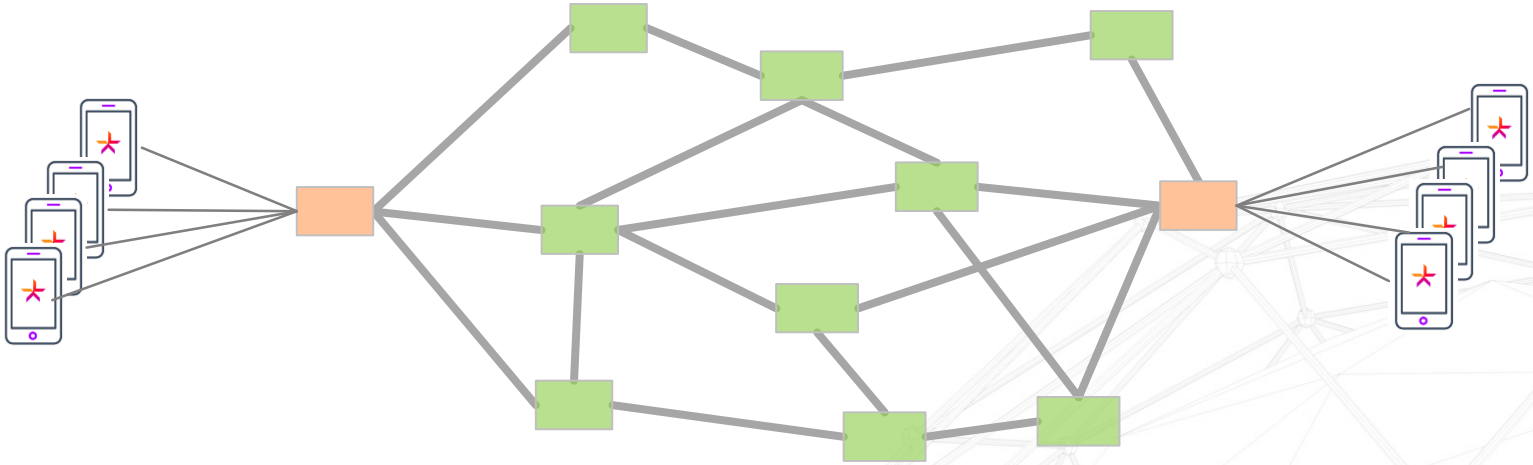
Offchain Settlement Statistics

NUMBER OF OPERATIONS 28 JUN 2017 – 04 JUL 2017

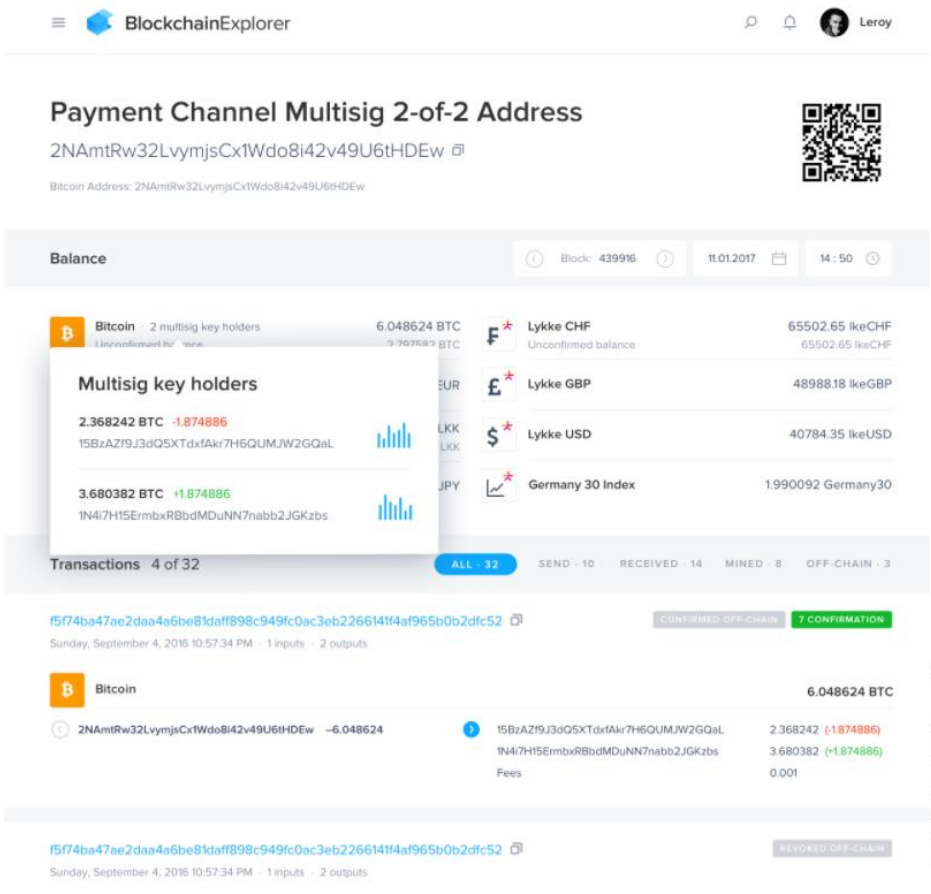
Asset	BUY SETTLEMENT OFFCHAIN	BUY SETTLEMENT ONCHAIN	SELL SETTLEMENT OFFCHAIN	SELL SETTLEMENT ONCHAIN
BTC	291	461	351	5
USD	533	26	654	68
LKK	340	497	420	25
CHF	362	11	316	15
EUR	181	11	194	6
TIME	106	11	76	21
LKK1Y	59	78	94	1
SLR	51	21	15	0
GBP	34	5	37	6
HCP	19	13	6	15
JPY	12	1	11	1
HKD	1	0	2	0
XAU	0	2	-	-
XPT	0	1	-	-
XAG	1	0	-	-
RUB	0	1	-	-
RRB	1	0	-	-
ILS	0	1	-	-
TOTAL	**1991**	**1140**	**2176**	**163**

Offchain Fees

1. Offchain Fees
2. Onchain fees (closing 2000 channels takes ~8 BTC)
3. Interest rates for lending Bitcoins



Offchain Settlement ToDo List



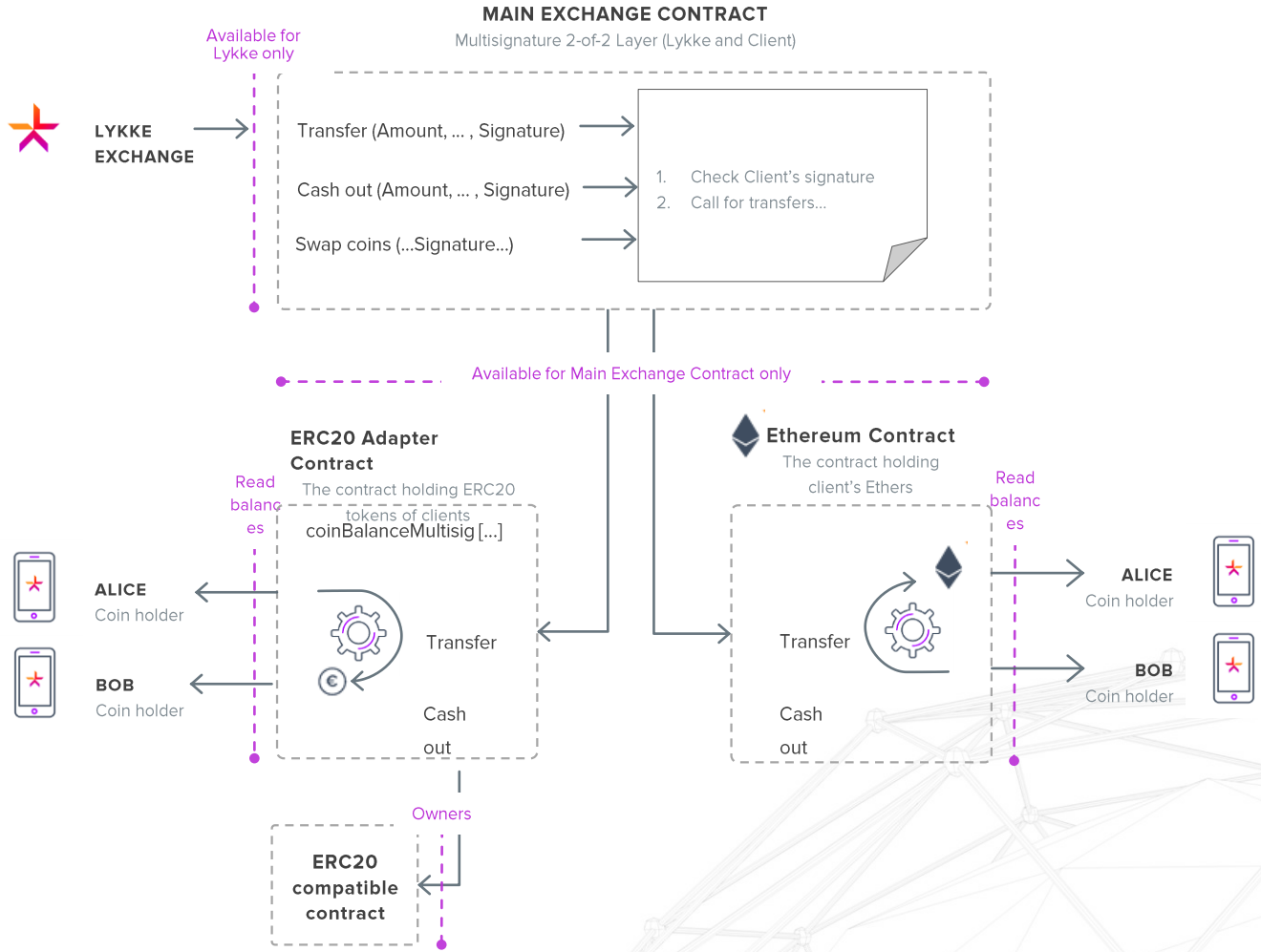
1. Public offchain transaction history

2. Offchain coinholders structure

3. Public commitment transactions

4. Public service for the channels monitoring`

Ethereum multisig


MAIN EXCHANGE CONTRACT
Multisignature 2-of-2 Layer (Lykke and Client)
Available for Lykke only
LYKKE EXCHANGE
Transfer (Amount, ... , Signature)
Cash out (Amount, ... , Signature)
Swap coins (...Signature...)
1. Check Client's signature
2. Call for transfers...
Available for Main Exchange Contract only
ERC20 Adapter Contract
The contract holding ERC20 tokens of clients
coinBalanceMultisig [...]
Read balances
ALICE
Coin holder
BOB
Coin holder
Transfer
Cash out
Ethereum Contract
The contract holding client's Ethers
Read balances
Transfer
Cash out
ALICE
Coin holder
BOB
Coin holder
Owners
ERC20 compatible contract

MultisigWithdrawal function

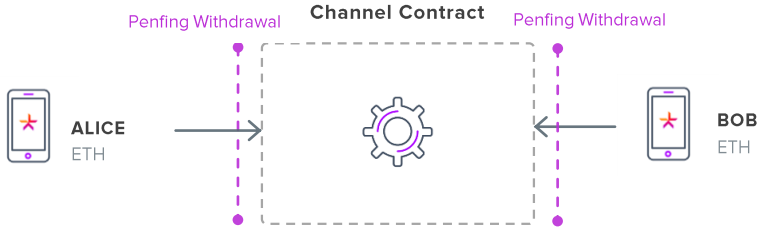
```
function Withdraw(
                    …
                    address from,
                    address to,
                    amount,
                    client's signature

                                ) onlyowner

    …

    hash = sha3(… address from, address to, amount);

    CheckClientSign(hash, client's signature);

    MakeWithdrawal(…);
```

MultisigWithdrawal function

```
function Withdraw(
                    …
                    address from,
                    address to,
                    amount,
                    client's signature

                                ) onlyowner

        …

        hash = sha3(… address from, address to, amount);

        CheckClientSign(hash, client's signature);

        MakeWithdrawal(…);
```

Can not be changed

StateChannel contract



function PendingChannelClose(

channel id
channel state id,
address1 to,
address2 to,
amount1,
amount2,
penalty2 hash,
client1 signature
client2 signature
)

Private key backup

Private Key Backup Issue

1. Digital key converted to 12 words

Risk: Client may loose the paper backup

2. The key is stored on Lykke server

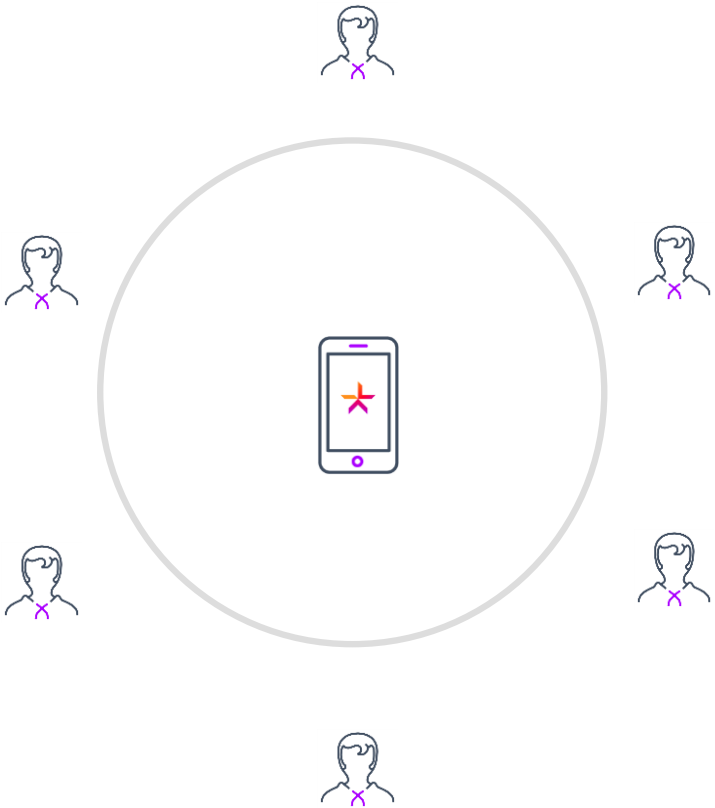
It is protected by the encryption client’s password so Lykke’s staff can’t steal it.

Risk: The client can forget his / her password.

3. The key is stored on client’s device

Risk: The device can be wiped, stolen or broken.

Social Backup (competition finished)



1. Request for backup are to be send to trustees (relatives and friends) using personal contacts (sms or emails)
2. Parts of the private key distributed over the trustees
3. Trustee would need to install the LykkeWellet to save the backup

Social Backup Recovery

1. sms
2. email
3. selfie