P/SA

A financially accountable watching network

Patrick McCorry

@paddypisa

RESEARCH INSTITUTE.
Ethereum Community Fund
ethereum foundation grants
BINANCE_X

P/SA

A financially accountable watching network

Patrick McCorry

@paddypisa

RESEARCH INSTITUTE.
Ethereum Community Fund
ethereum foundation grants
BINANCE_X

P/SA

A financially accountable watching network

~~Patrick McCorry~~

~~@paddypisa~~

RESEARCH INSTITUTE.

Ethereum Community Fund

ethereum foundation grants

BINANCE_X

P/SA

A financially accountable watching network

~~Patrick McCorry~~

Sergi Delgado

~~@paddypisa~~

@sr_gi

RESEARCH INSTITUTE.

Ethereum Community Fund

ethereum foundation grants

BINANCE_X

P/SA

A financially accountable watching network

~~Patrick McCorry~~

Sergi Delgado

~~@paddypisa~~ @sr_gi

RESEARCH INSTITUTE.

Ethereum Community Fund

ethereum foundation grants

BINANCE_X

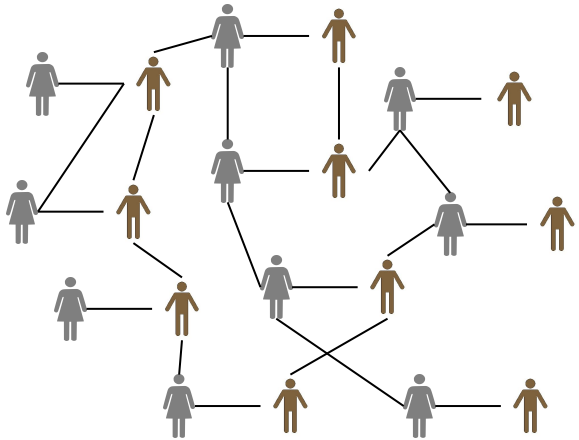
WHY IS OFF-CHAIN EXCITING?

P/SA

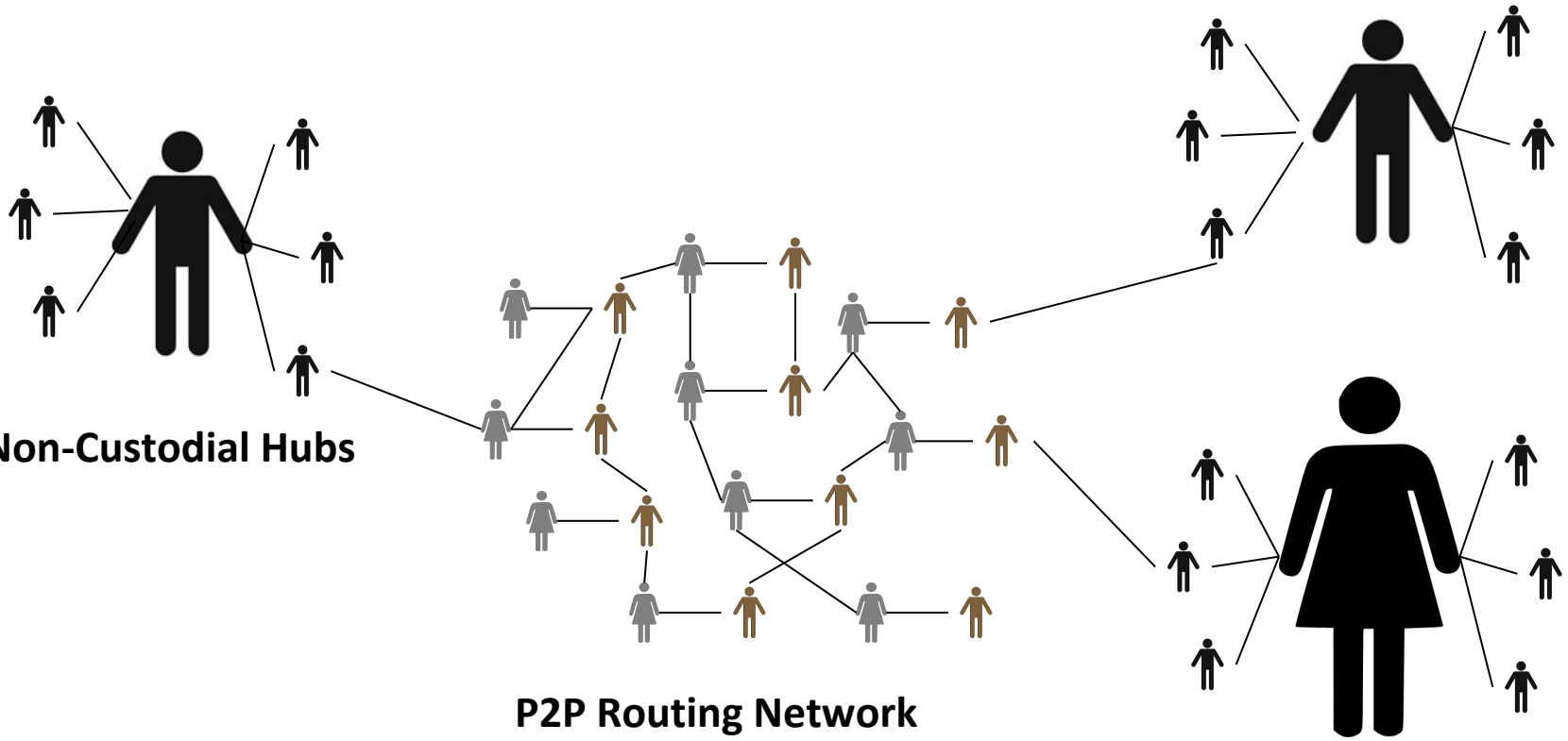
Bypass all blockchain latency and fees
While still retaining non-custodial security guarantees

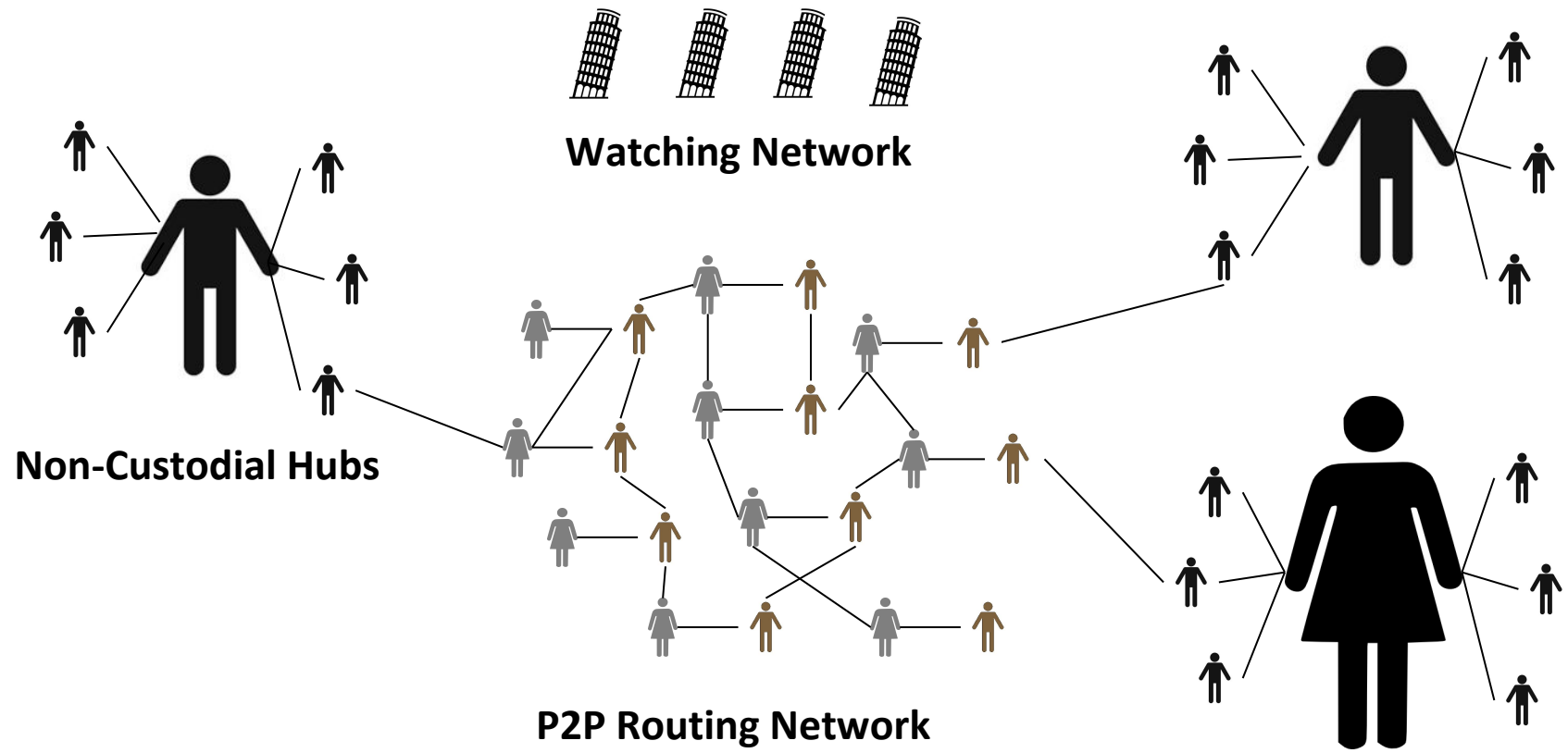
Only scaling solution that will exceed 10k tps
99% of transactions are LOCAL and never reach the global network

But what does an “off-chain network” look like?



P2P Routing Network


Non-Custodial Hubs
P2P Routing Network


Watching Network
Non-Custodial Hubs
P2P Routing Network

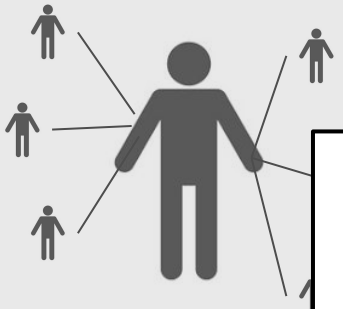
Watching Network

Non-Custodial Hubs

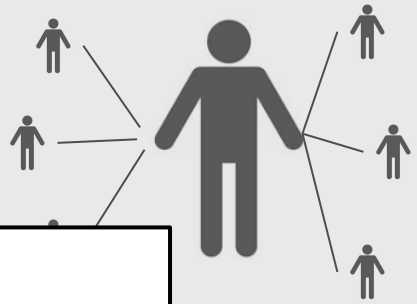
P2P Routing Network

Settlement System and
Root of Trust of all Layer 2

Watching Network

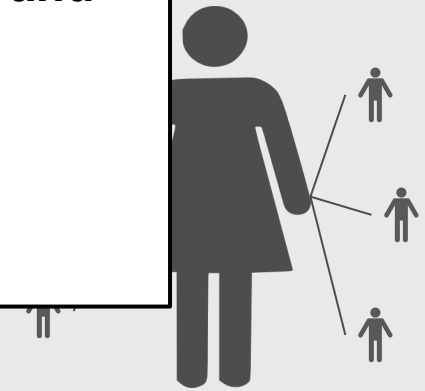


Non-Custodial Hu



Open-source, global, permissionless and non-custodial financial system.

It is coming…



P2P Routing Network

Settlement System and
Root of Trust of all Layer 2

P/SA RESEARCH

LIQUIDITY·NETWORK

STARKWARE

LIGHTNING

RAIDEN

L4

ARWEN

connext

eclairmobile

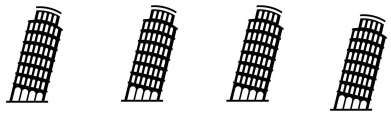
Lightning Network Bitcoin wallet

Blockstream

pg Plasma Group

Settlement System and
Root of Trust of all Layer 2

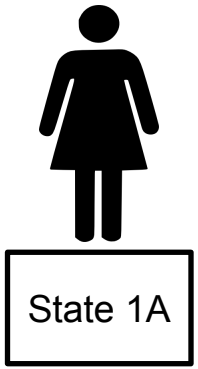
We'll "briefly" talk about how replace-by-revocation works **before deep-diving into the watching network**

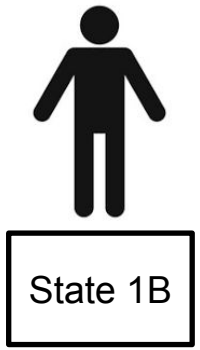


Watching Network

What does a lightning channel look like? (replace-by-revocation)

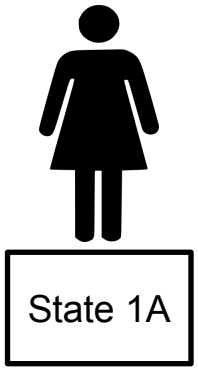
Alice and Bob always have a transaction (“state”) that only they can broadcast to trigger a dispute

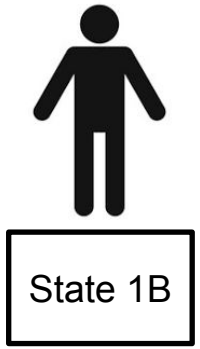




What does a lightning channel look like? (replace-by-revocation)

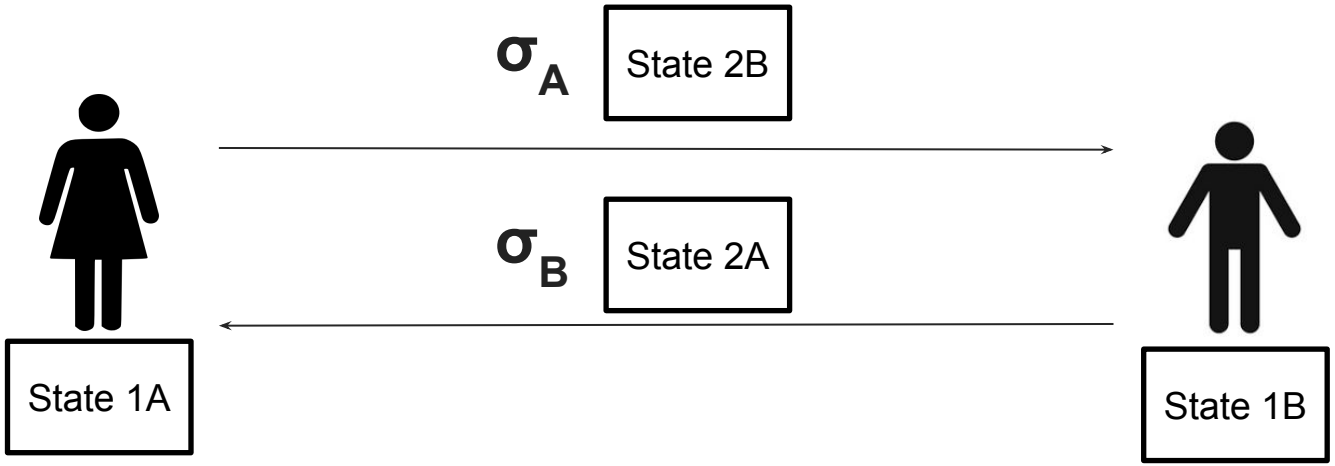
`Authorising a payment is a two-step process`





What does a lightning channel look like? (replace-by-revocation)

1. Both parties authorise a new state
(a transaction only the counterparty can broadcast)



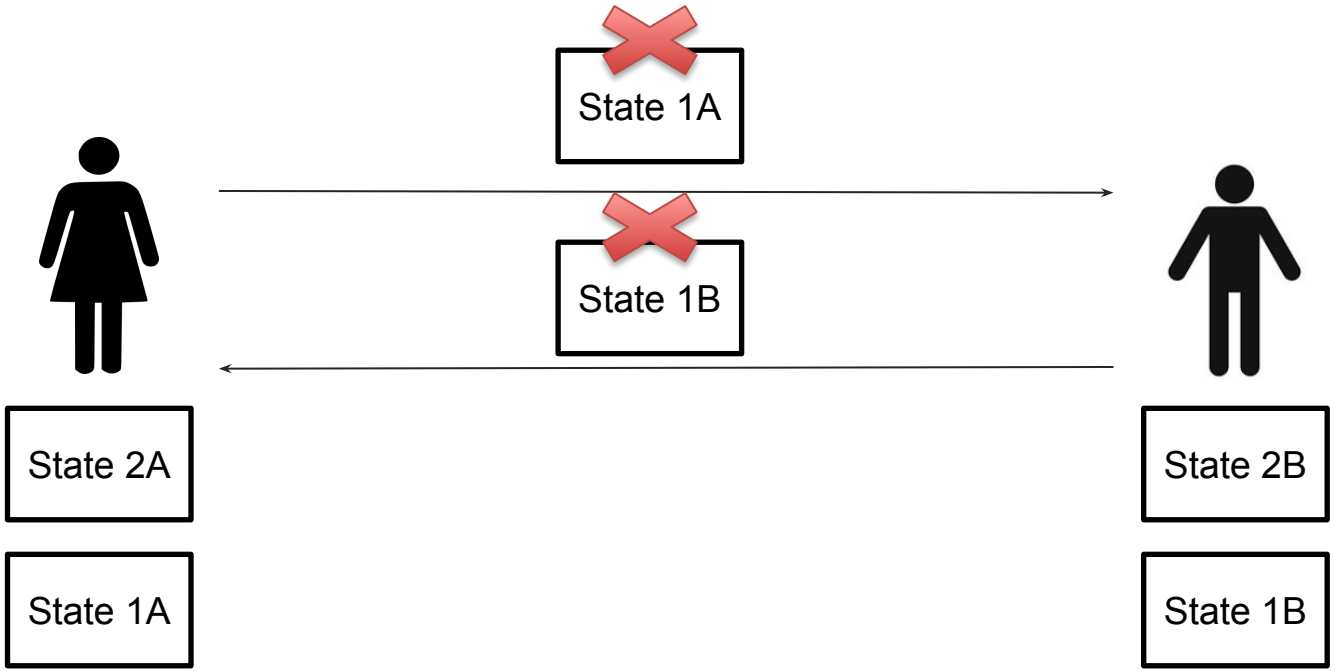
What does a lightning channel look like? (replace-by-revocation)

Either State 1 or State 2 can be broadcast…

Second step revokes old balance and confirms the new one

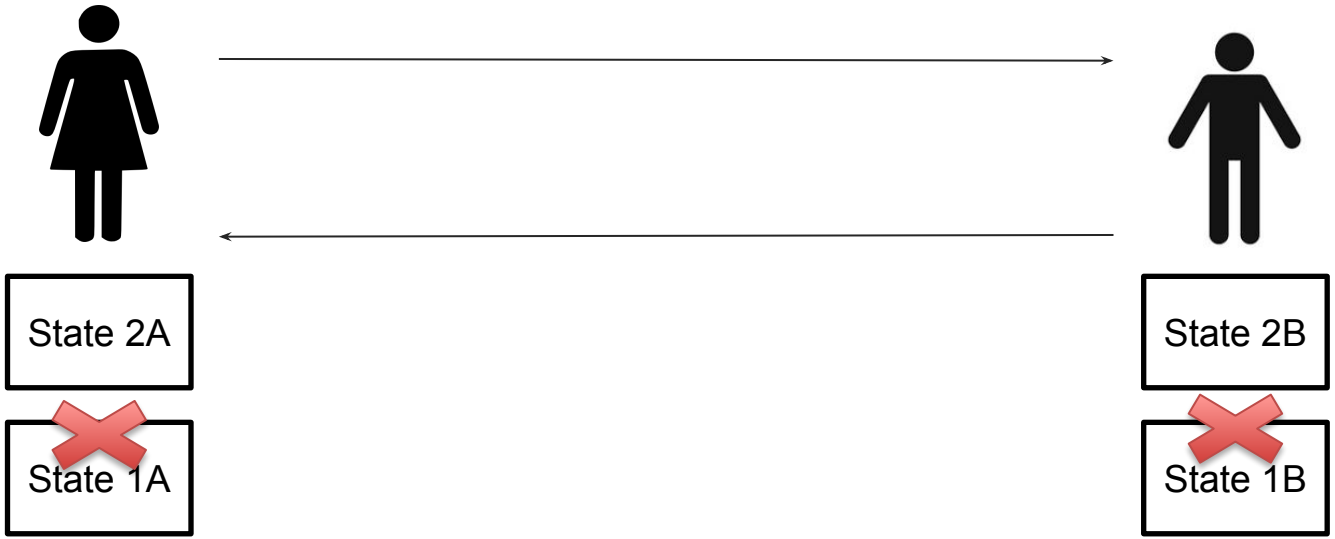
What does a lightning channel look like? (replace-by-revocation)

2. Both parties will “revoke” the old state
(i.e. share preimage of hash)



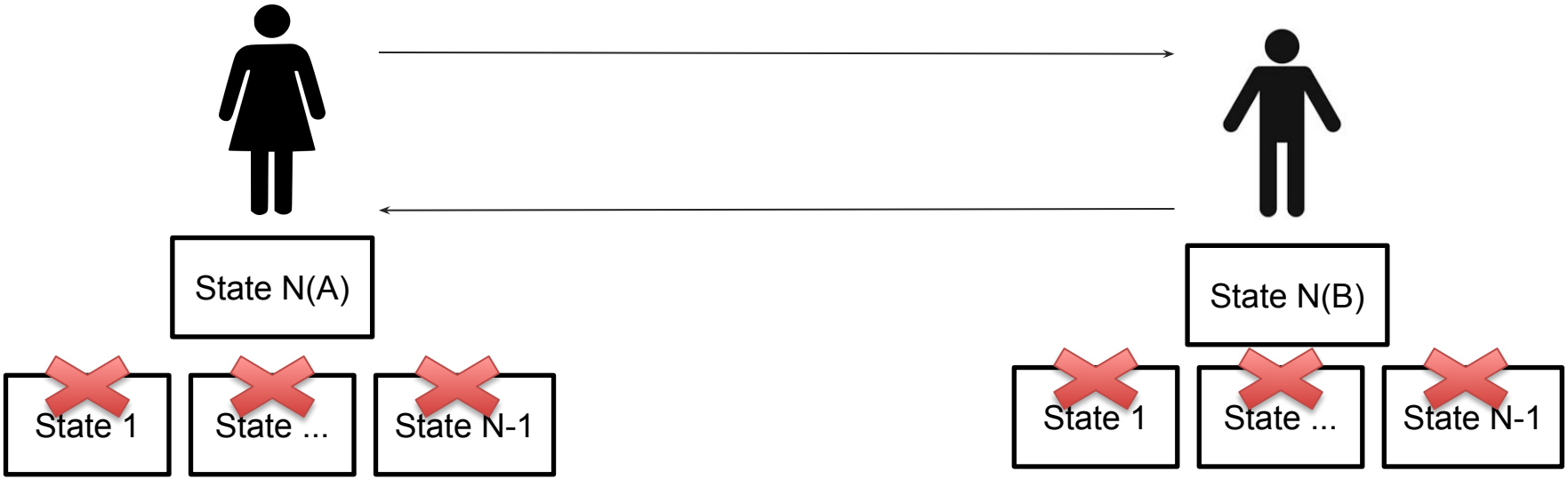
What does a lightning channel look like? (replace-by-revocation)

Complete!
Both parties can always broadcast the latest state

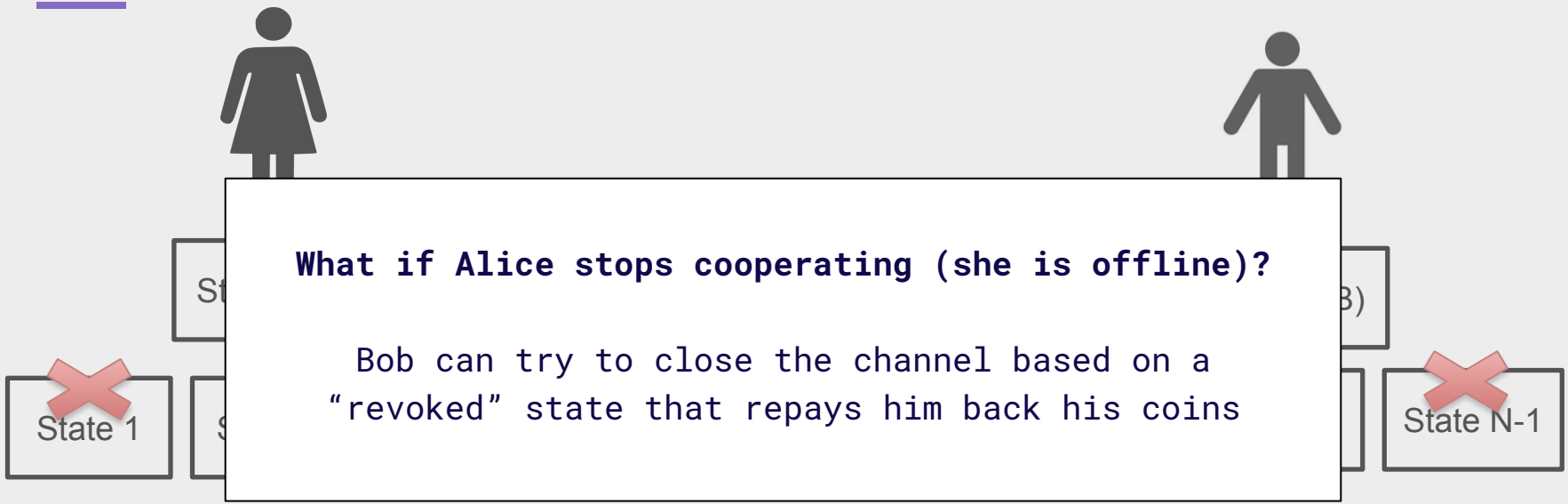


What does a lightning channel look like? (replace-by-revocation)

… and a growing list of revoked states… as we will see,
this will be problematic...



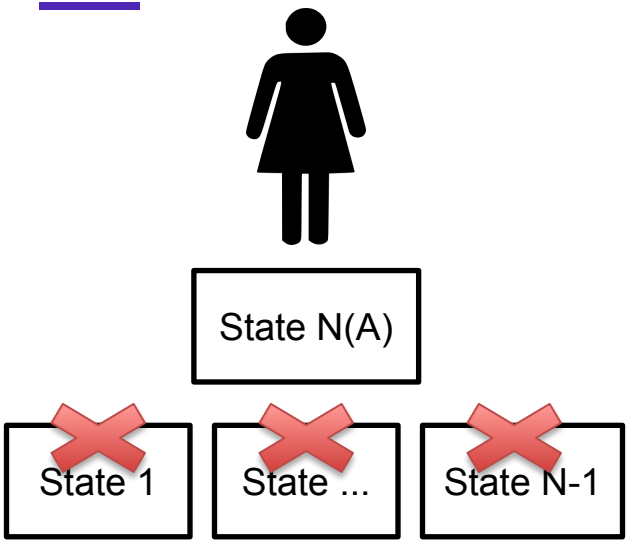
What does a lightning channel look like? (replace-by-revocation)

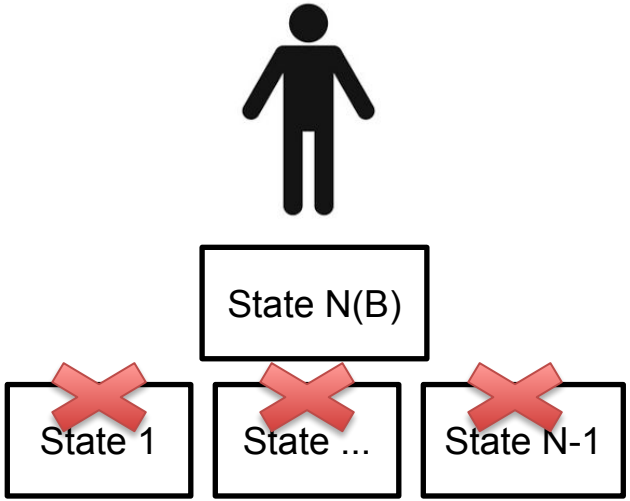


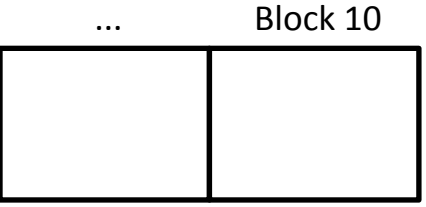
What if Alice stops cooperating (she is offline)?

Bob can try to close the channel based on a “revoked” state that repays him back his coins

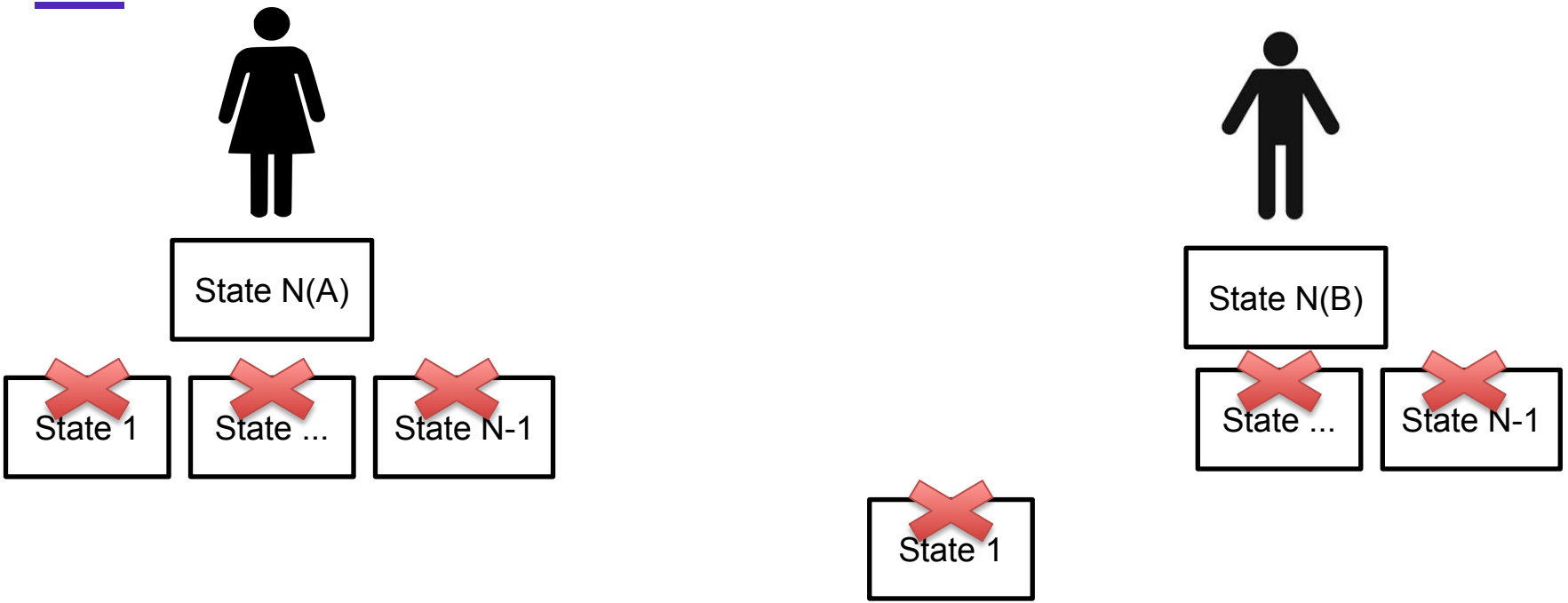
What does a lightning channel look like? (replace-by-revocation)



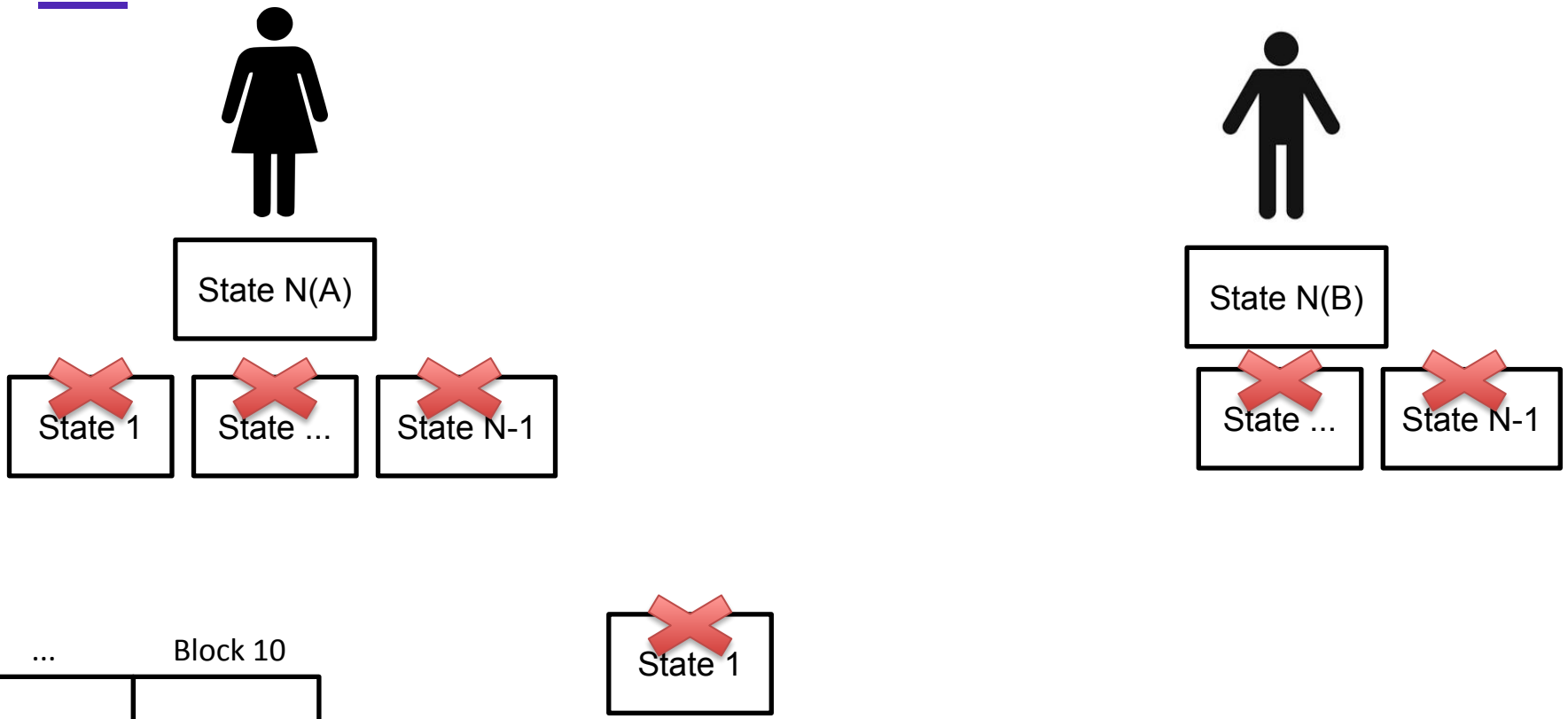




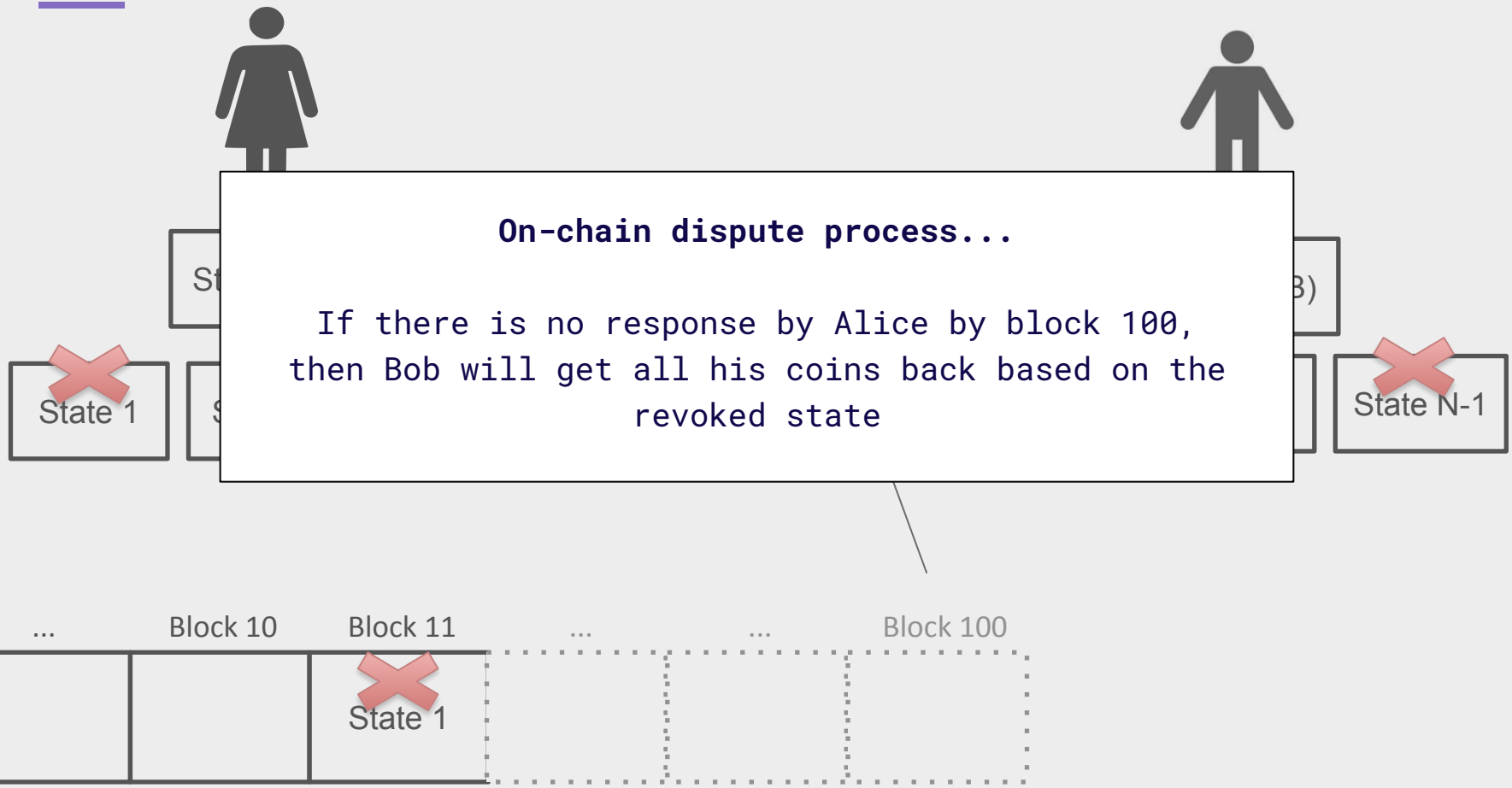
What does a lightning channel look like? (replace-by-revocation)



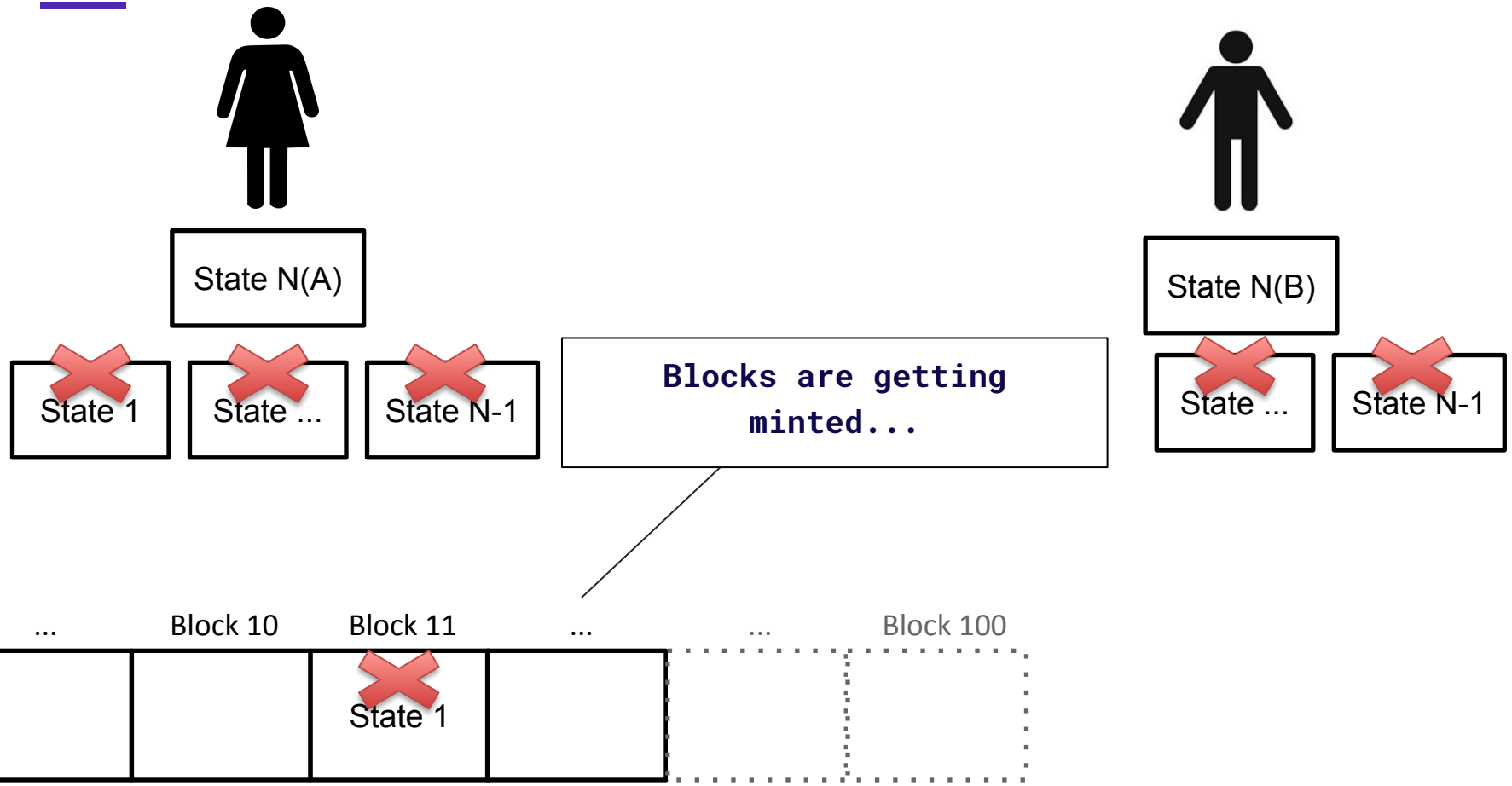
What does a lightning channel look like? (replace-by-revocation)



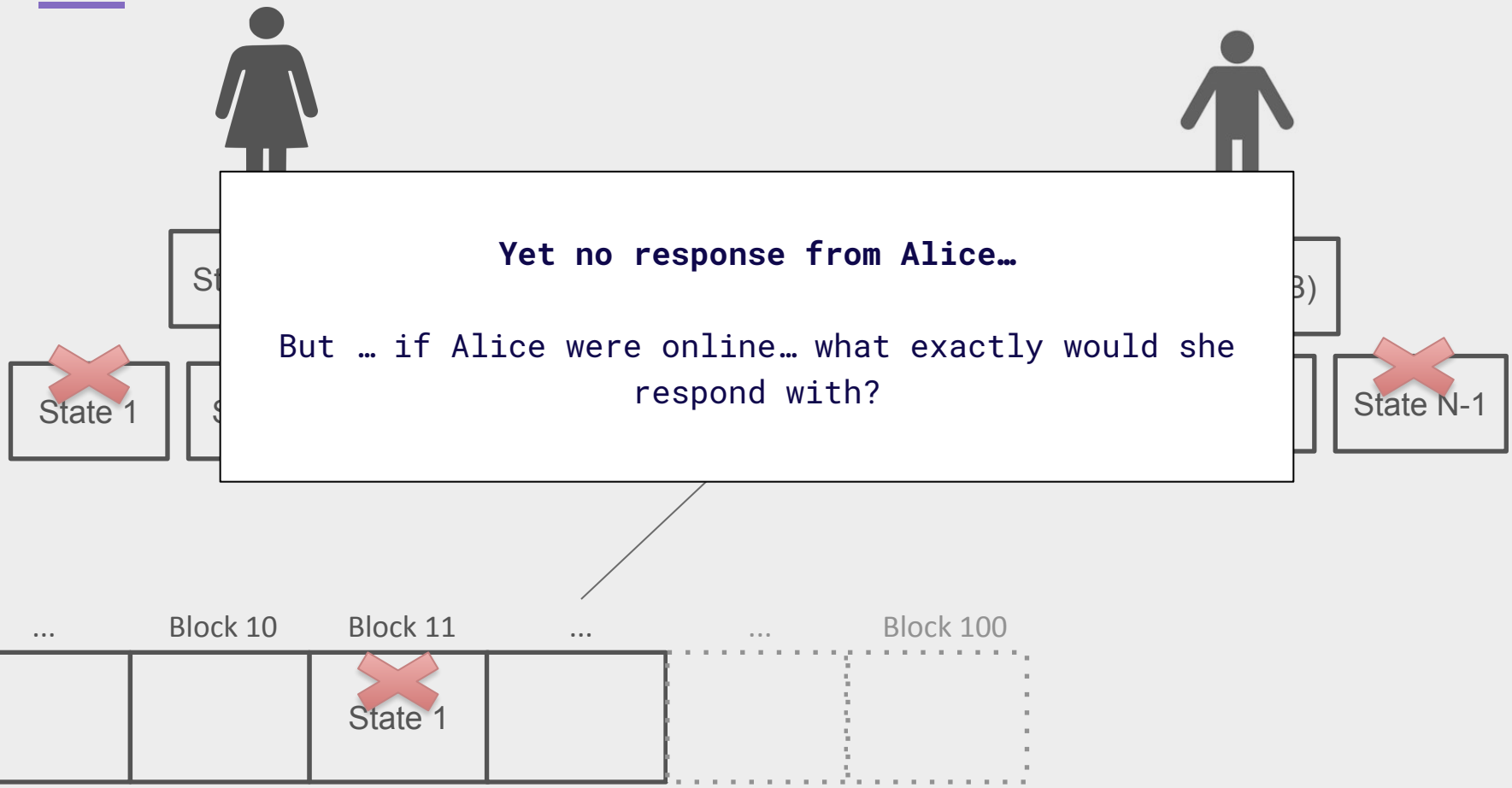
What does a lightning channel look like? (replace-by-revocation)



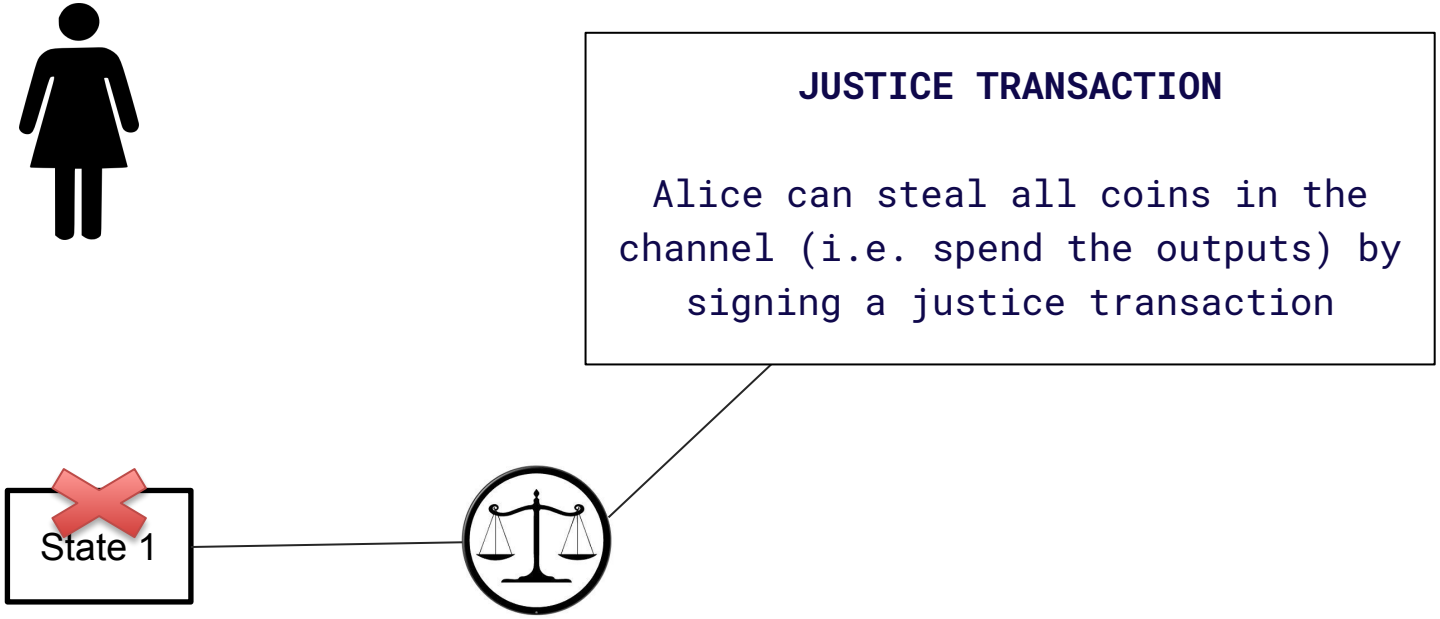
What does a lightning channel look like? (replace-by-revocation)



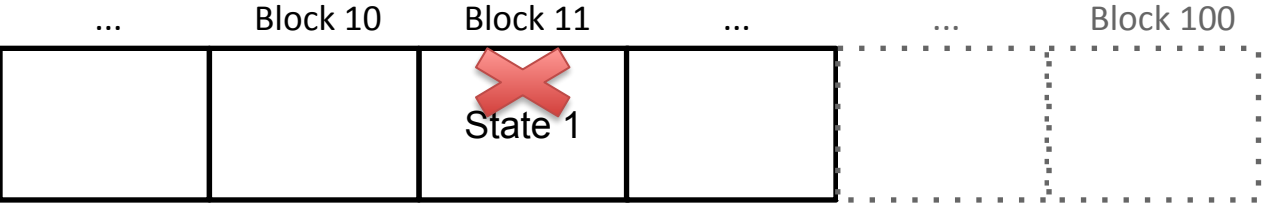
What does a lightning channel look like? (replace-by-revocation)



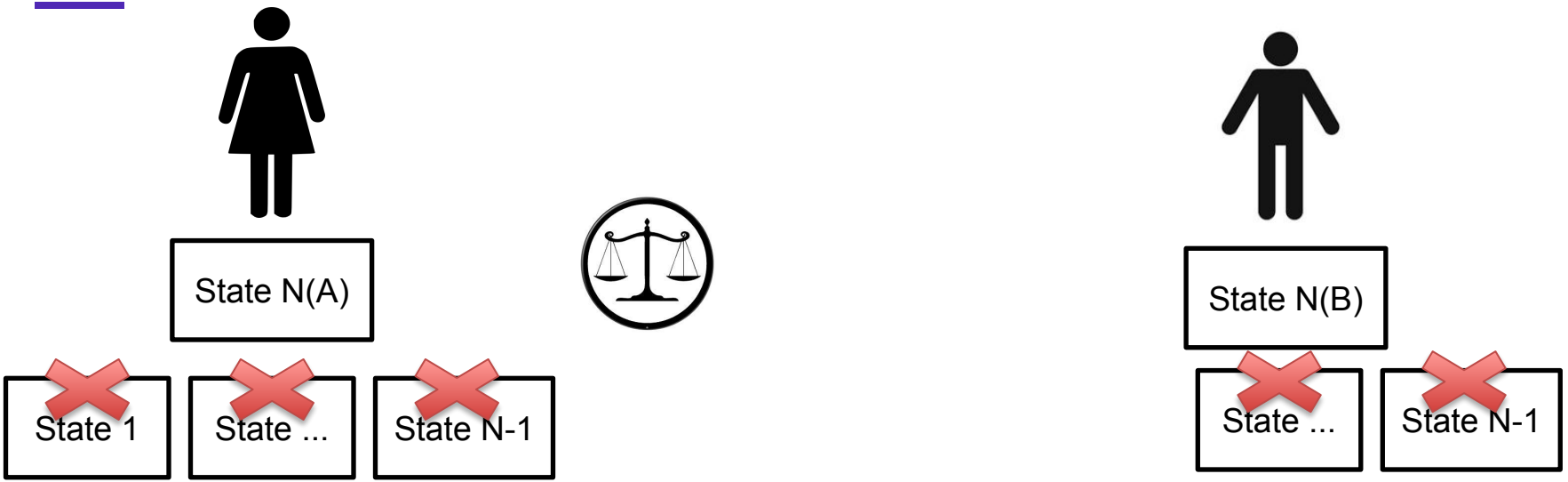
What does a lightning channel look like? (replace-by-revocation)

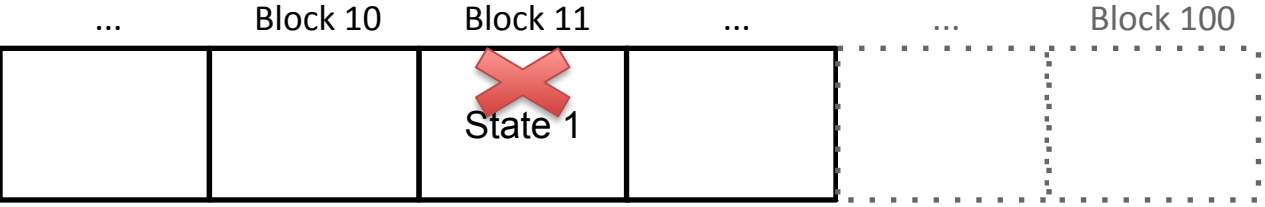


What does a lightning channel look like? (replace-by-revocation)

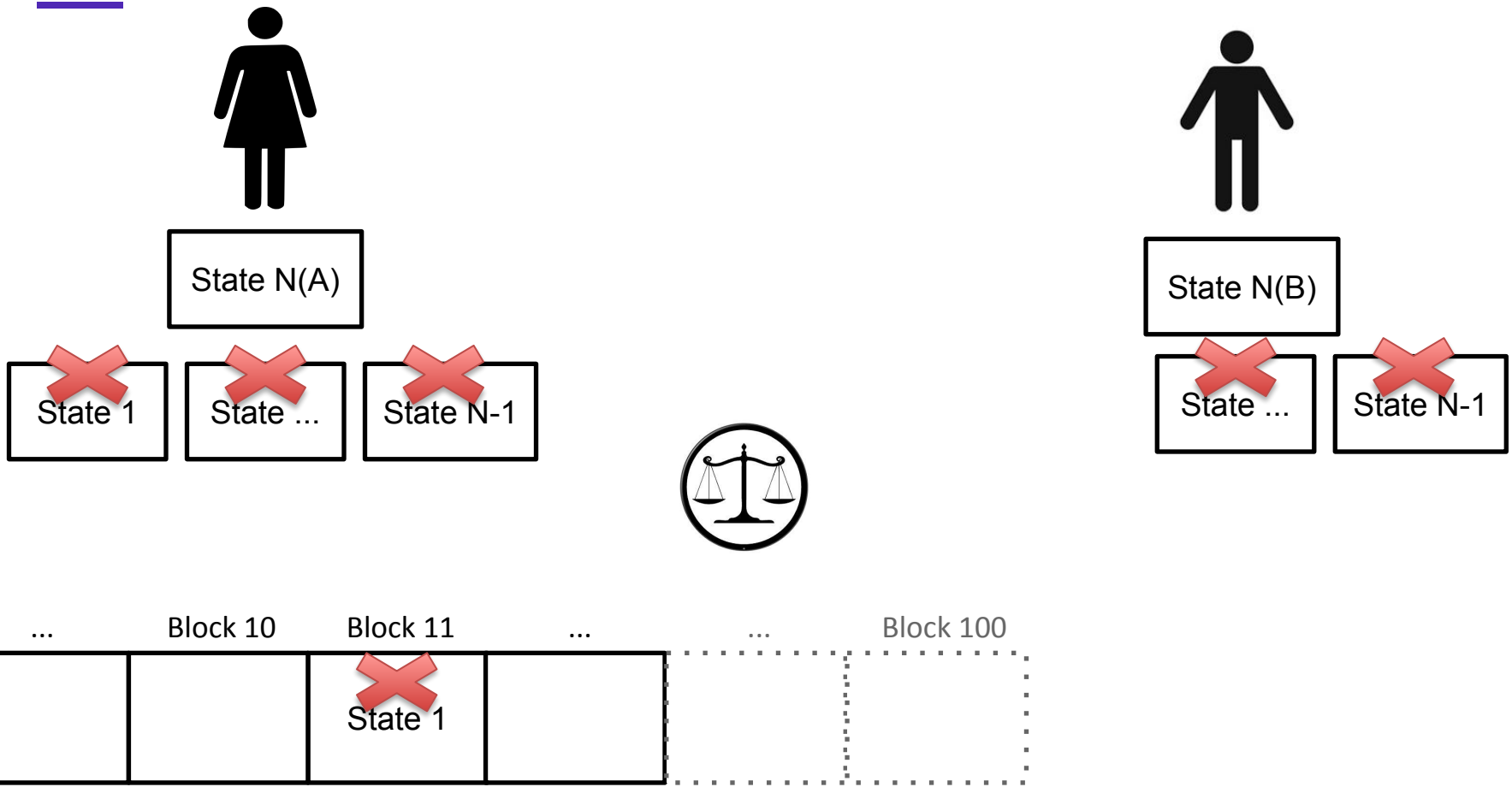


What does a lightning channel look like? (replace-by-revocation)

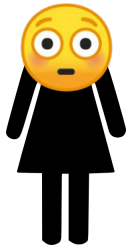


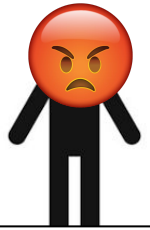


What does a lightning channel look like? (replace-by-revocation)



What does a lightning channel look like? (replace-by-revocation)





State N(A)

State 1

State ...

Alice wins!

Her JUSTICE TRANSACTION was accepted into the blockchain before the dispute process expired!

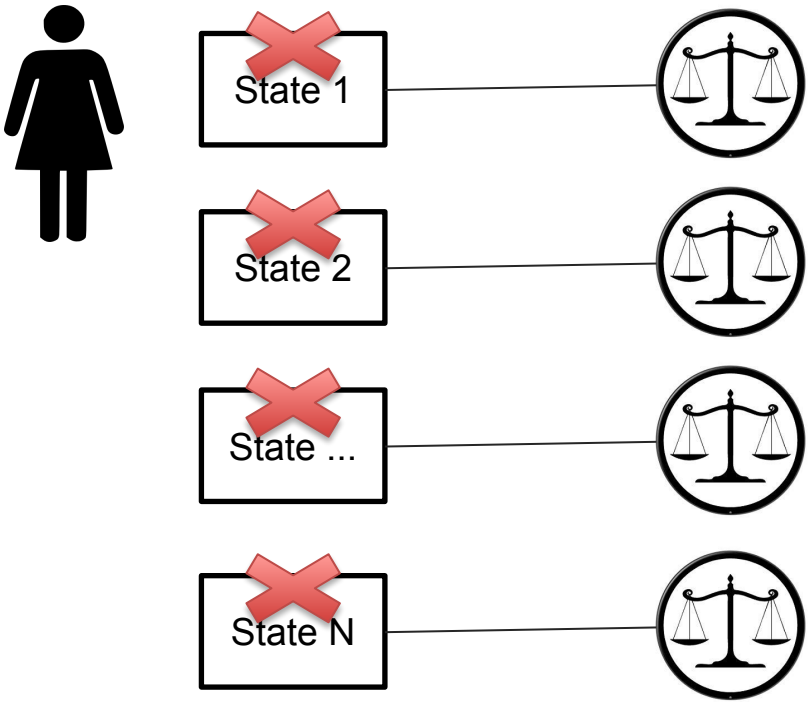
She punished Bob for trying to cheat **by taking all coins in the channel**

... Block 10 Block 11 ... ... Block 100

State 1

FAQ: Can Alice just keep a pre-signed justice tx around?

FAQ: Can Alice just keep a pre-signed justice tx around?



Why?

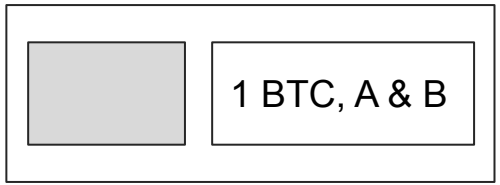
Bob has a LIST of REVOKED transactions that only HE can broadcast….

She must be ready to prove any of them are invalid…

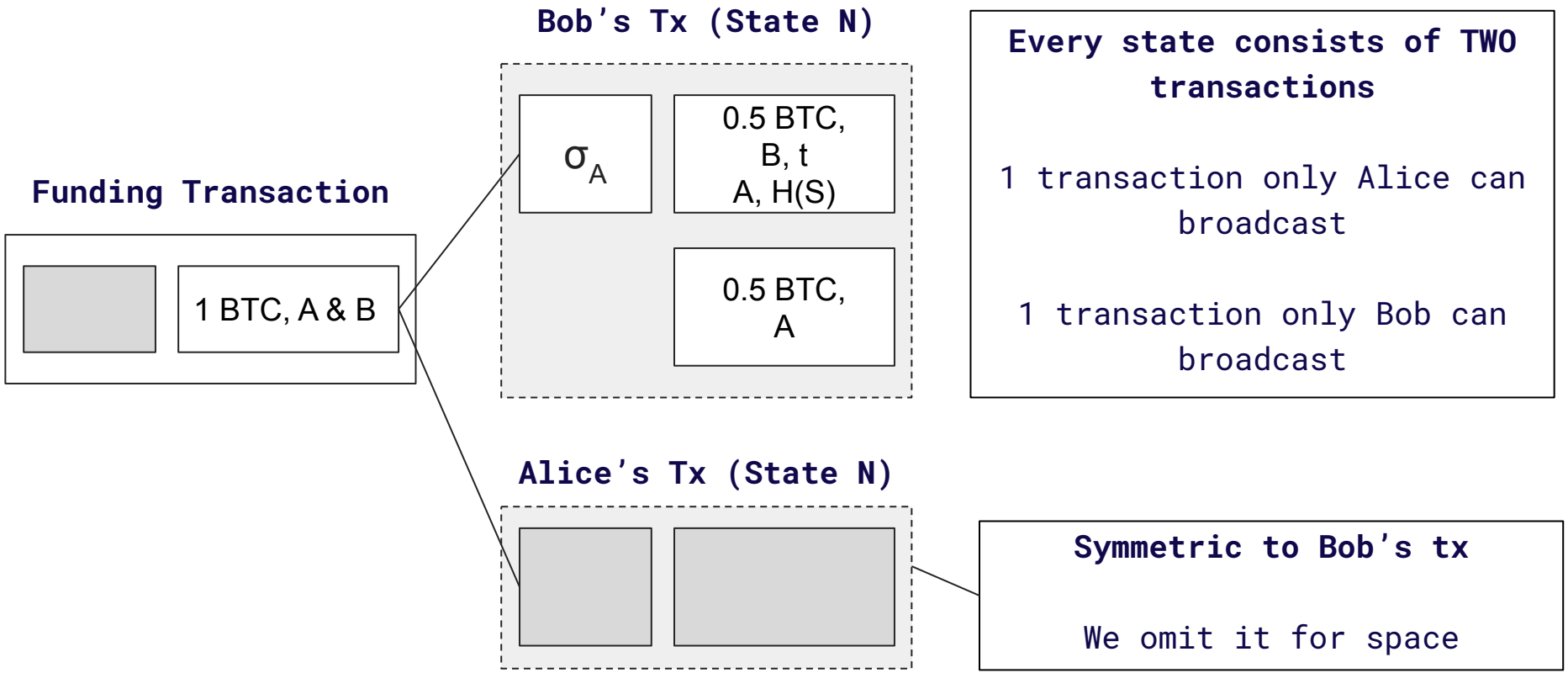
Remember, UTXO!

FAQ: Under the hood - what does it look like (roughly speaking)

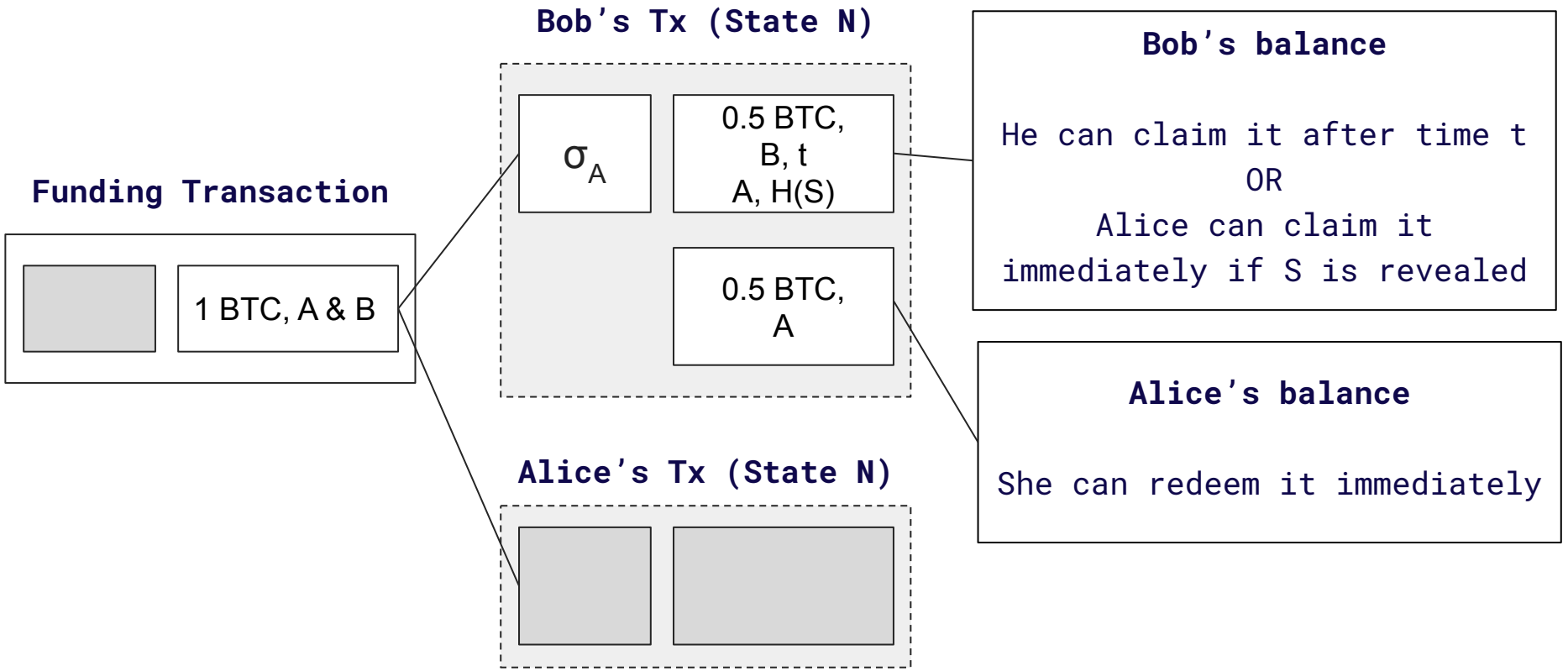
Funding Transaction



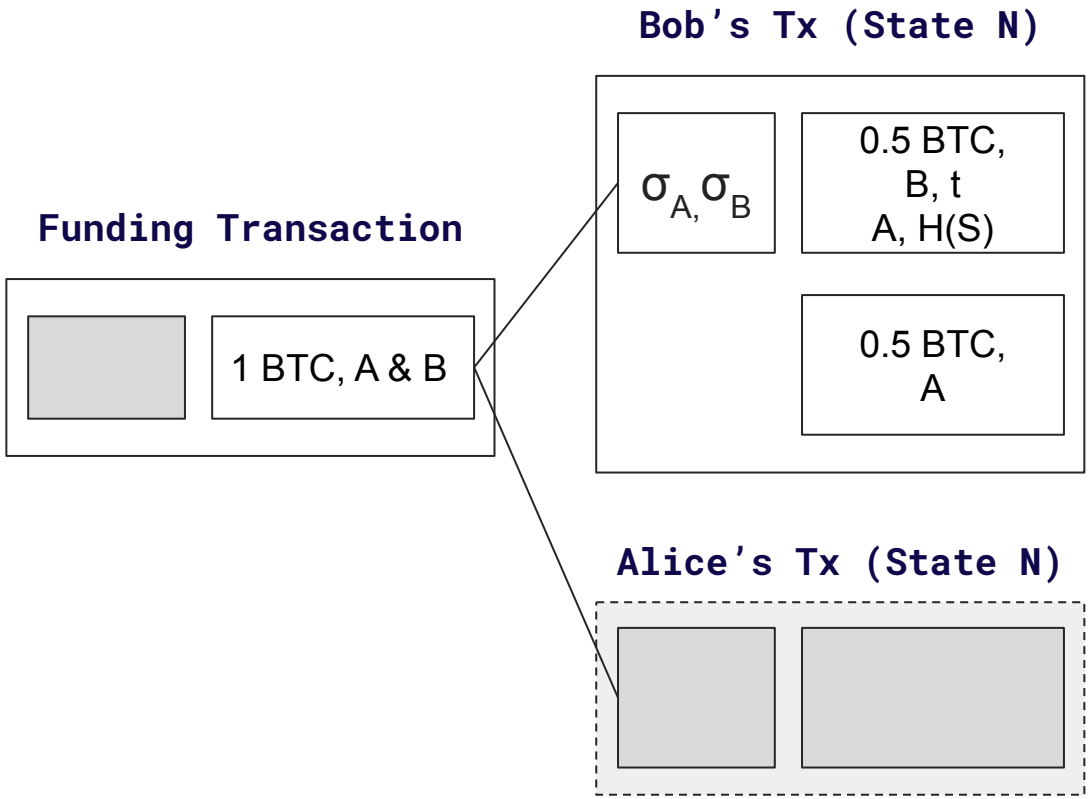
FAQ: Under the hood - what does it look like (roughly speaking)



FAQ: Under the hood - what does it look like (roughly speaking)



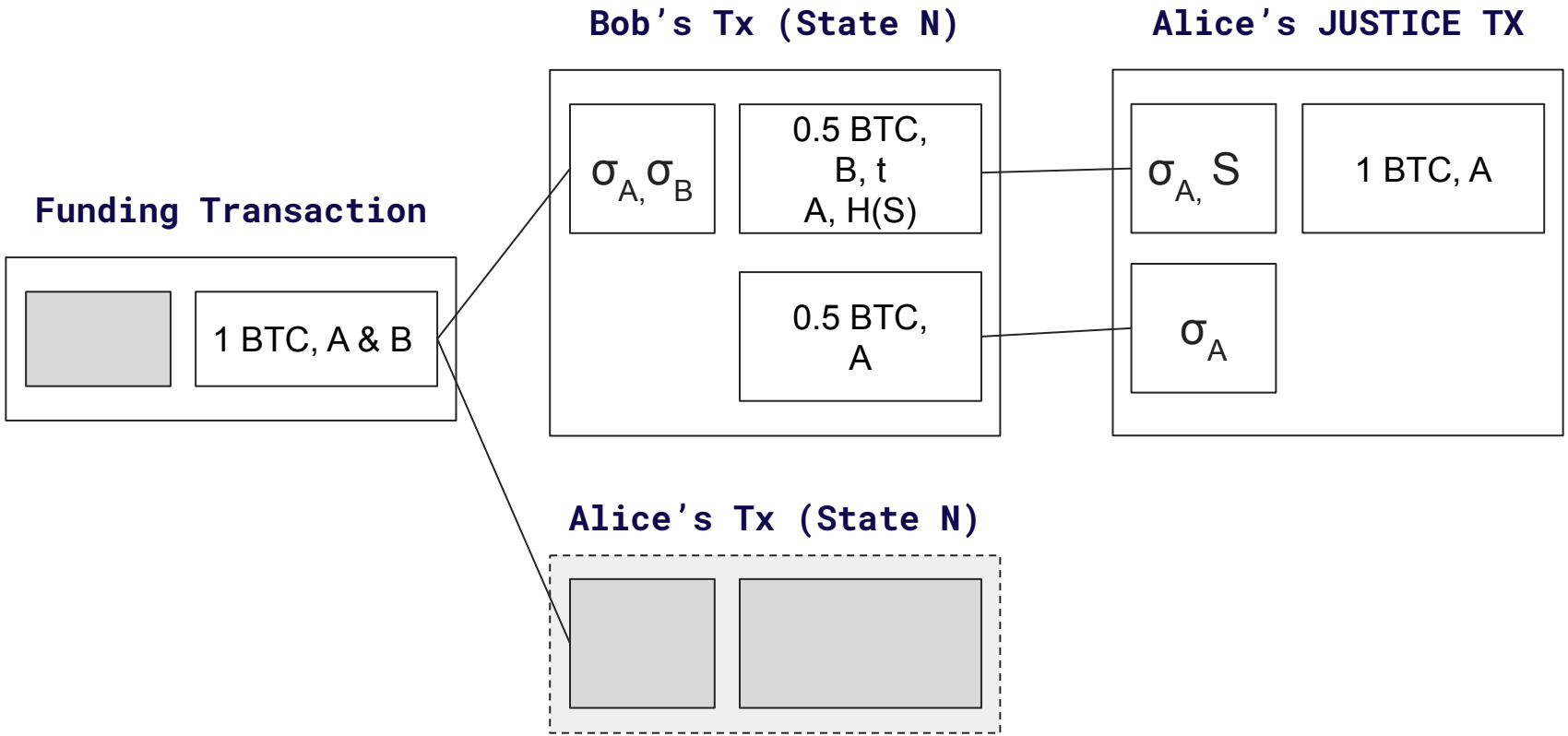
FAQ: Under the hood - what does it look like (roughly speaking)



Bob broadcasts it

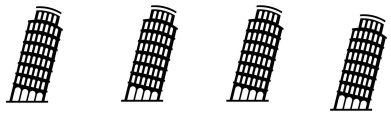
He can just sign and broadcast it at any time… to trigger the dispute period (up to time t)

FAQ: Under the hood - what does it look like (roughly speaking)



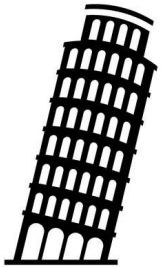
Now we know how Lightning Channels (replace-by-revocation) roughly works…

Let’s better understand this watching network



Watching Network

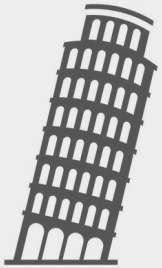
Monitor (Tadge) @ Scaling Bitcoin ‘16



Leaning Watchtower

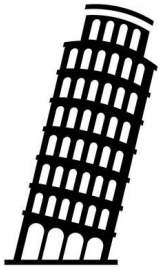
Monitor (Tadge) @ Scaling Bitcoin ‘16

But what does she send to the watchtower?

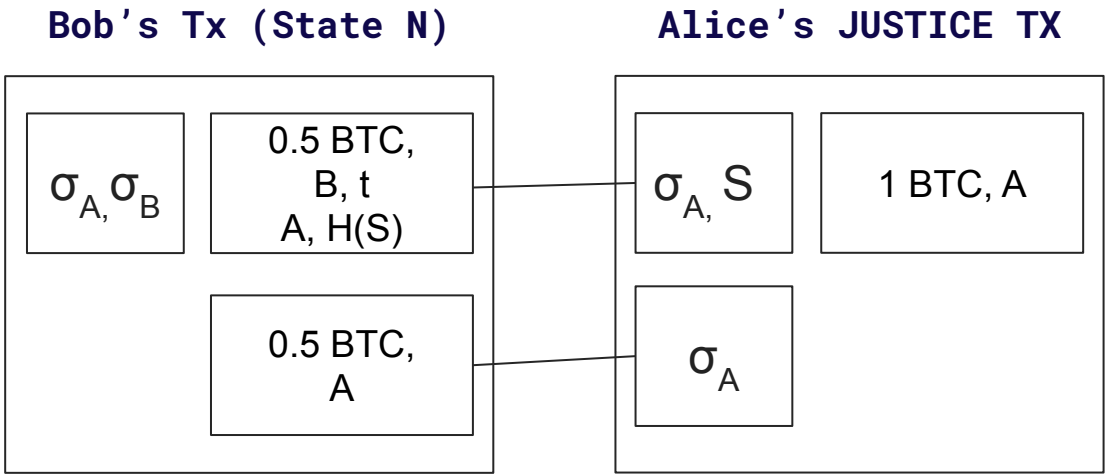


Leaning Watchtower

Monitor (Tadge) @ Scaling Bitcoin ‘16



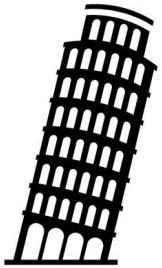
Leaning Watchtower



Monitor (Tadge) @ Scaling Bitcoin ‘16

Tx Locator
Let’s watching service find transaction when dispute is triggered

Encryption Key
Used to encryption Justice Transaction, only discoverable when a dispute is triggered



Leaning Watchtower

Bob’s TX (State N)

TXID [32 bytes]

TxLocator = [16:0]
Encryption Key = [16:32]

4410c8d14ff9f87ceeed1d65cb58e7c7b2422b2d7529afc675208ce2ce09ed7d

TxLocator

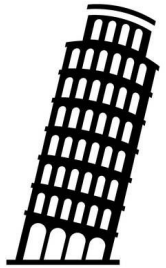
Encryption Key

Monitor (Tadge) @ Scaling Bitcoin ‘16

Encrypted Justice Transaction

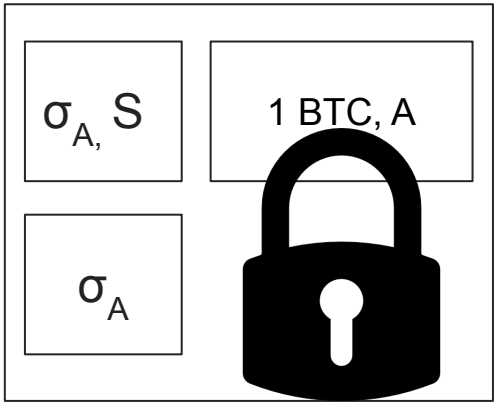
Alice encrypts the pre-signed justice transaction

It can ONLY be decrypted by watchtower if there is a dispute (or if bob leaks the key)



Leaning Watchtower

Encrypted Justice TX



Bob’s TX (State N)

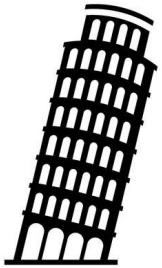
TXID [32 bytes]

TxLocator = [16:0]
Encryption Key = [16:32]

Monitor (Tadge) @ Scaling Bitcoin ‘16

Send to the Watching Service

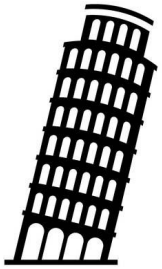
TxLocator & Encrypted Justice Transaction



Leaning Watchtower

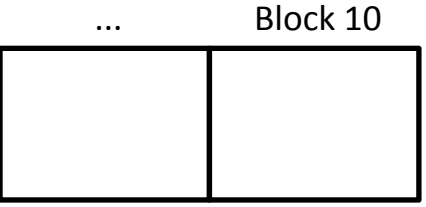
TxLocator & Encrypted Justice Transaction

Monitor (Tadge) @ Scaling Bitcoin ‘16

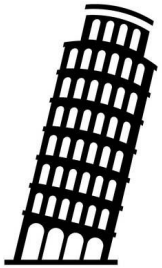


Leaning Watchtower

```
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice
```

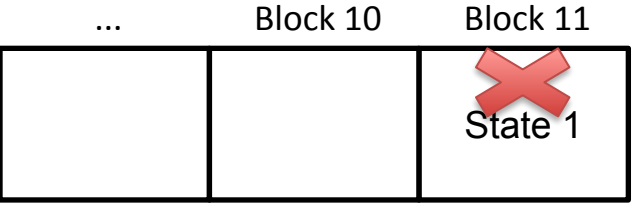


Monitor (Tadge) @ Scaling Bitcoin ‘16



Leaning Watchtower

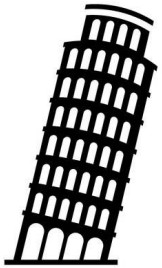
```
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice
```



Monitor (Tadge) @ Scaling Bitcoin ‘16

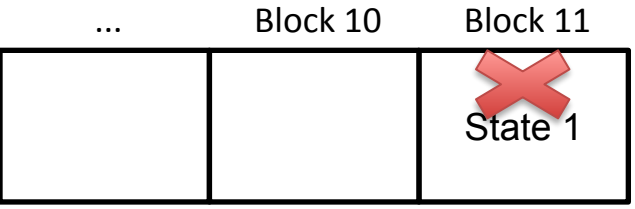
Watching Service - 5 Steps

1. Extract Transaction ID
2. Compute TxLocator + Key
3. Find “encrypted blob”
4. Decrypt it!
5. Broadcast to the network



Leaning Watchtower

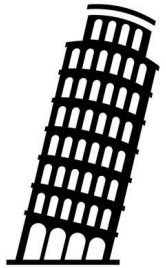
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice



Monitor (Tadge) @ Scaling Bitcoin ‘16

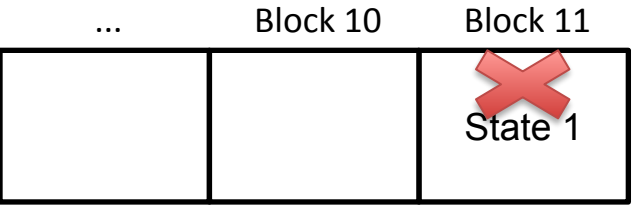
Watching Service - 5 Steps

1. Extract Transaction ID
2. Compute TxLocator + Key
3. Find “encrypted blob”
4. Decrypt it!
5. Broadcast to the network



Leaning Watchtower

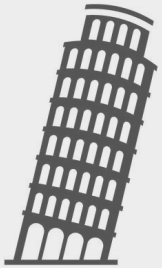
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice



Monitor (Tadge) @ Scaling Bitcoin ‘16

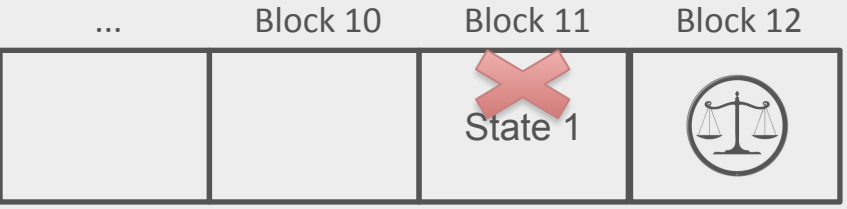
Watching Service - 5 Steps

Let’s look at the good, bad and the ugly



Leaning Watchtower

TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice



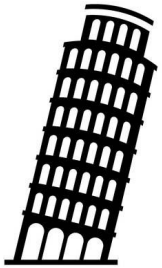
Monitor - THE GOOD

Channel-Privacy

We don’t know anything about channel until dispute.
(Can also send us junk)

Responder, not trigger

We CANNOT trigger any disputes! Only respond if the counterparty tries to cheat.



Leaning Watchtower

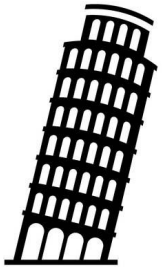
Simple Protocol

Just store encrypted blob and watch blockchain to retrieve decryption key.

Monitor - THE GOOD, BAD

Channel-Privacy	O(N) Storage	Responder, not trigger
We don't know anything about channel until dispute. (Can also send us junk)	Watching service must store a justice transaction for EVERY new state update.	We CANNOT trigger any disputes! Only respond if the counterparty tries to cheat.

Congestion BIG problem	Simple Protocol
Watching service only has a pre-signed transaction and very very awkward to bump fees.	Just store encrypted blob and watch blockchain to retrieve decryption key.

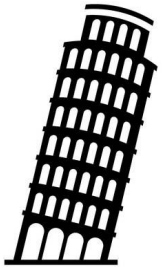


Leaning Watchtower

Monitor - THE GOOD, BAD, AND THE UGLY

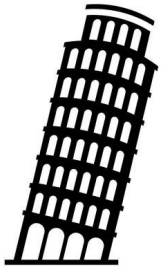
Channel-Privacy We don't know anything about channel until dispute (Can also send us junk)	**O(N) Storage** Watching service must store a justice transaction for EVERY new state update.	**Responder, not trigger** We CANNOT trigger any disputes! Only respond if the counterparty tries to cheat.

Congestion BIG problem Watching service only has a pre-signed transaction and very very awkward to bump fees	**Simple Protocol** Just store encrypted blob and watch blockchain to retrieve decryption key	**HOPES FOR AVAILABILITY** Hire hundreds of watchers and only 1 is rewarded. **What if they don't respond?** Tough luck.

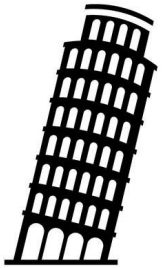


Leaning Watchtower

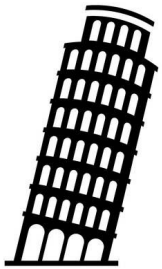
View of how a “watching network” might work so far



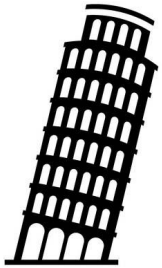
Leaning Watchtower



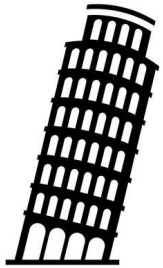
Leaning Watchtower



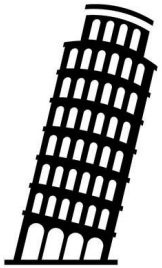
Leaning Watchtower



Leaning Watchtower



Leaning Watchtower



Leaning Watchtower

Hire multiple watchtowers

And hope one responds!
Goal for “Monitor” was CHANNEL Privacy

Reward Policy?

Only the one watchtower who gets their respective justice tx in the blockchain **will get rewarded**

WatchTower @ BPASE'18

σ_A, σ_B, i^*

Signatures

State version

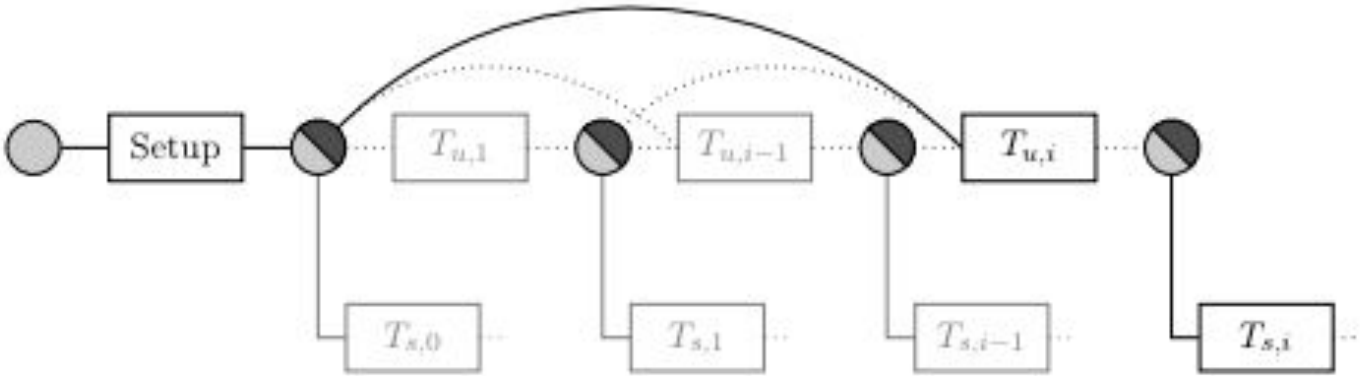
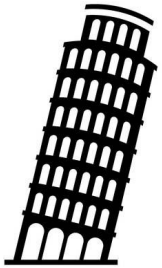


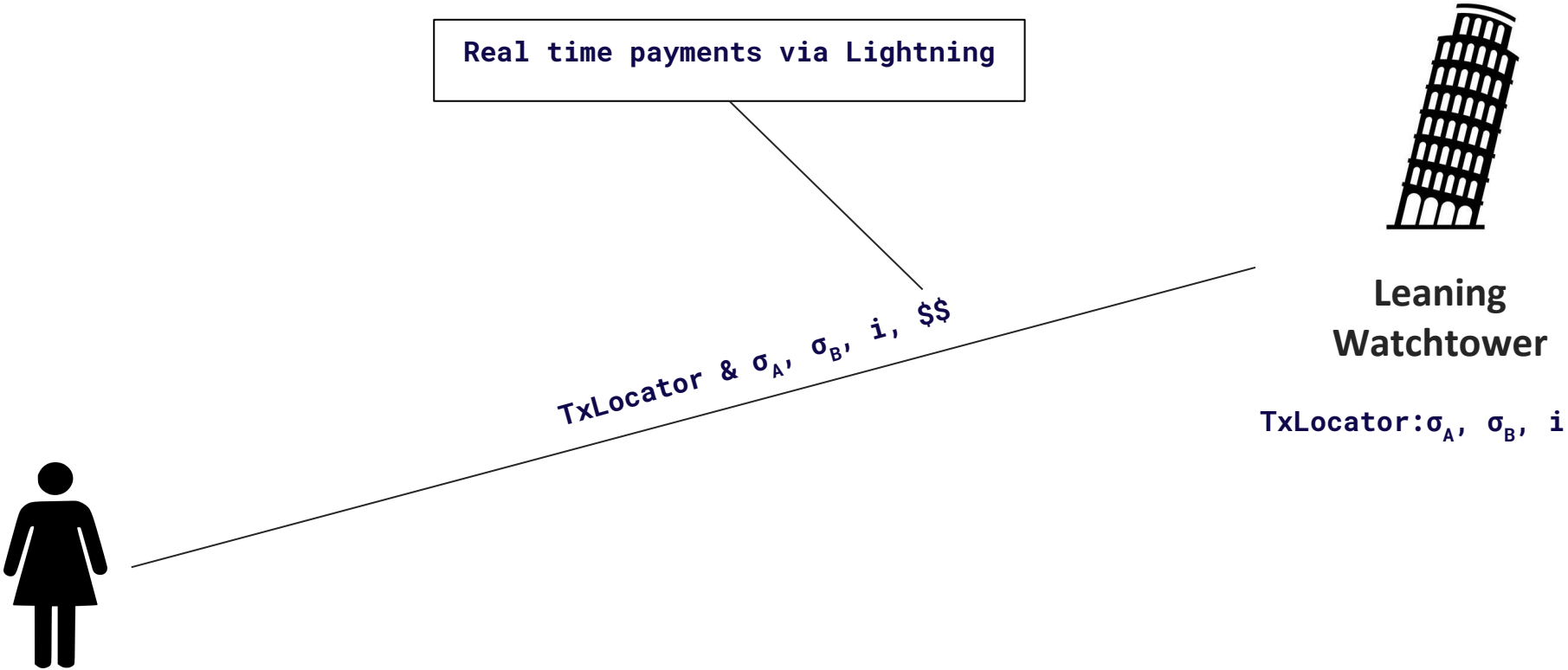
Figure 5: Overview of the off-chain protocol.



Leaning Watchtower

*The actual construction is slightly different, it commits to the "version, randomness" which is revealed, but this is easier to explain.

WatchTower @ BPASE'18

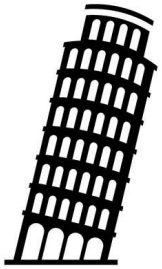


*The actual construction is slightly different, it commits to the "version, randomness" which is revealed, but this is way easier to explain.

WatchTower @ BPASE'18

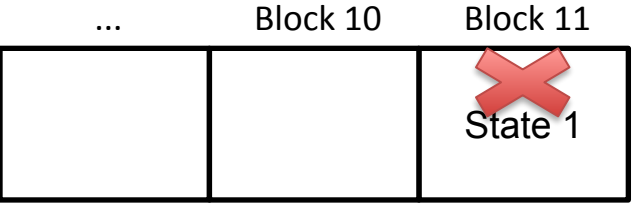
Watching Service - 5 Steps

1. Extract Transaction ID
2. Look up the latest "i" received
3. Broadcast it!



Leaning Watchtower

TxLocator:σ_A, σ_B, i

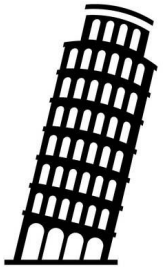


WatchTower @ BPASE'18

Watching Service - 5 Steps

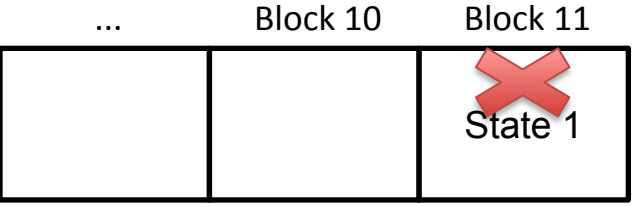
1. Extract Transaction ID
2. Look up the latest "i" received
3. Broadcast it!

σ_A, σ_B, i



Leaning Watchtower

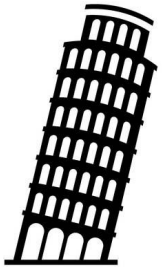
TxLocator:σ_A, σ_B, i



WatchTower @ BPASE'18

Watching Service - 5 Steps

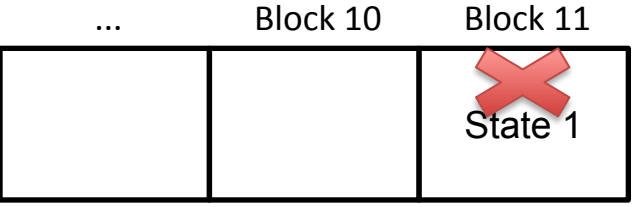
1. Extract Transaction ID
2. Look up the latest "i" received
3. Broadcast it!



Leaning Watchtower

TxLocator:σ_A, σ_B, i

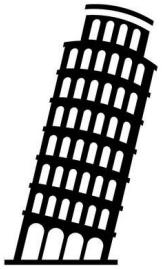
σ_A, σ_B, i



WatchTower @ BPASE'18

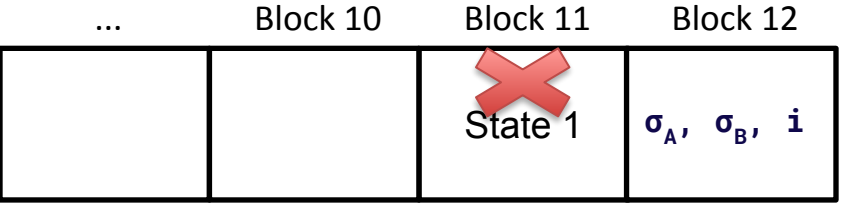
Watching Service - 5 Steps

1. Extract Transaction ID
2. Look up the latest "i" received
3. Broadcast it!



Leaning Watchtower

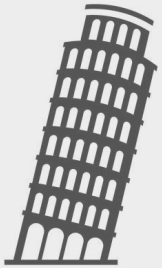
TxLocator:σ_A, σ_B, i



WatchTower @ BPASE'18

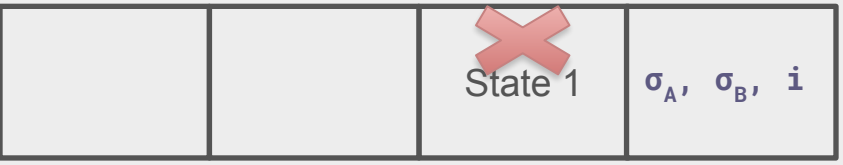
Watching Service - 5 Steps

Let's look at the good, bad and the ugly



Leaning Watchtower

…cator:σ_A, σ_B, i



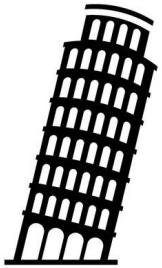
WatchTower - THE GOOD

Verifiable Job

No longer store junk. We know it is a useful job.

Separates TX + State

We are broadcasting the “latest state” and not necessarily a Bitcoin transaction. Cleaner solution.



Leaning Watchtower

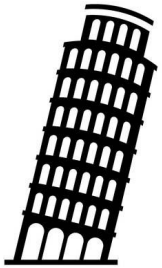
O(1) Storage

Only store the job with the largest version.

WatchTower - THE GOOD, BAD

Verifiable Job	Accountability? No	Separates TX + State
No longer store junk. We know it is a useful job.	No evidence a watch tower was hired and if they don't do their job, no way to prove it.	We are broadcasting the "latest state" and not necessarily a Bitcoin transaction. Cleaner solution.

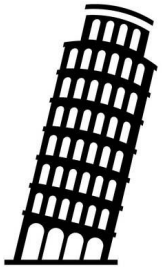
No financial deterrent	O(1) Storage
We need to rely on the reputation of a watching service (or hire multiple) since no skin-in-the-game	Only store the job with the largest version.



Leaning Watchtower

WatchTower - THE GOOD, BAD, AND THE UGLY

Verifiable Job No longer store junk. We know it is a useful job.	**Accountability? No** No evidence a watch tower was hired and if they don't do their job, no way to prove it.	**Separates TX + State** We are broadcasting the "latest state" and not necessarily a Bitcoin transaction. Cleaner solution.
No financial deterrent We need to rely on the reputation of a watching service (or hire multiple) since no skin-in-the-game	**O(1) Storage** Only store the job with the largest version.	**Consensus Upgrade** We need a new OP_CODE for eltoo to work, so we don't get the benefits of watchtower.

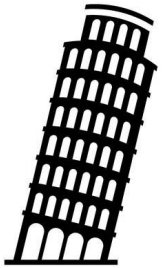


Leaning Watchtower

PISA @ Scaling Bitcoin ‘19

We don’t care too much about the underlying payment channel construction.

It can be replace-by-revocation (today)
or replace-by-version (eltoo).



Leaning Watchtower

Monitor-style Jobs	Eltoo-style Jobs	Outpost-style Jobs
TxLocator + Encrypted TX	TxLocator & Authorised State Version	TxLocator + Decryption Key

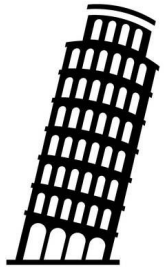
PISA @ Scaling Bitcoin ‘19

On-chain evidence

If PISA doesn’t respond, clear on-chain evidence.

Signed Receipt

An acknowledgement that PISA accepted a job

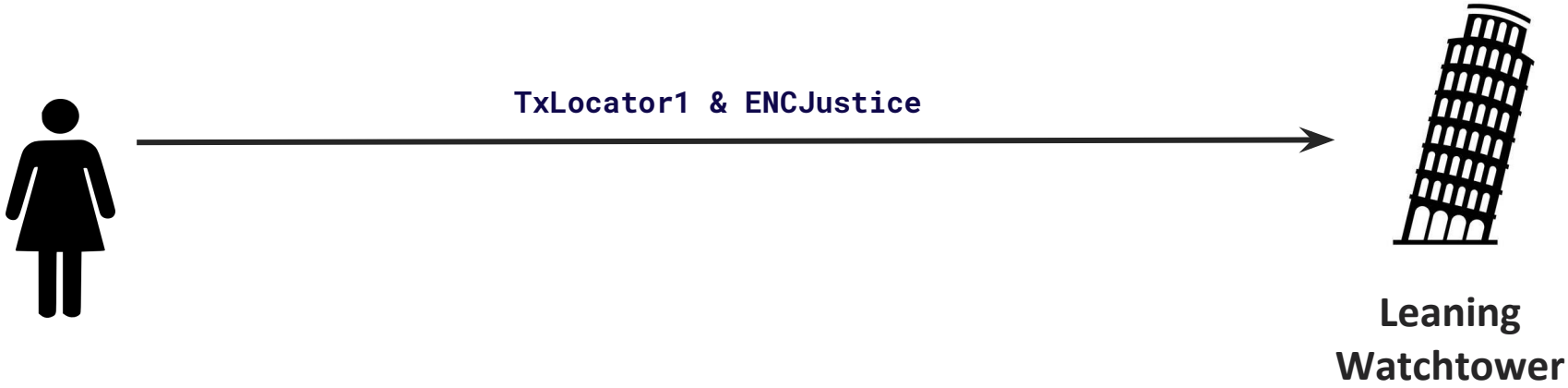


Leaning Watchtower

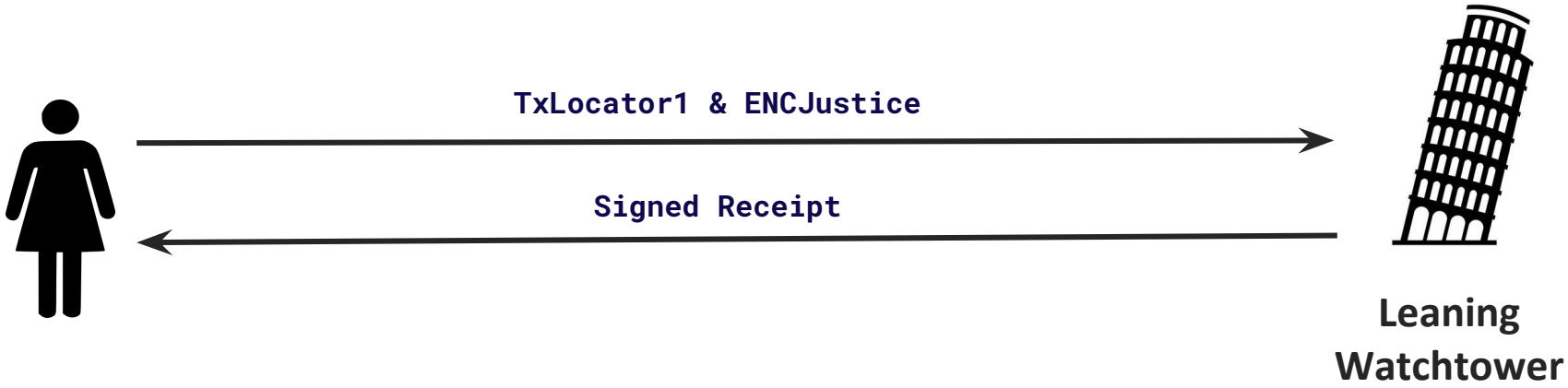
Requires a new OPCODE to support SPV Proof, parsing receipt & covenants

PISA Contract with security deposit

PISA (Monitor) @ Scaling Bitcoin ‘19



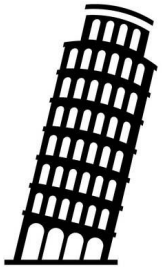
PISA (Monitor) @ Scaling Bitcoin ‘19



PISA (Monitor) @ Scaling Bitcoin ‘19

TxLocator1 & ENCJustice

Signed Receipt



Leaning Watchtower

In-depth Signed Receipt

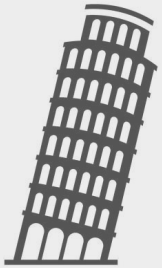
Encrypted Justice: ENCJustice
Transaction Locator: TxLocator1
Appointment Start: Block 10
Appointment Expiry: Block 500
Minimum Dispute Period: 50 blocks
Signature by PISA: σ_{PISA}

PISA (Monitor) @ Scaling Bitcoin ‘19

BONUS POINTS - Fair real-time payments

We can use a simple HTLC transfer to guarantee fair exchange of signed receipt + payment over the lightning network.

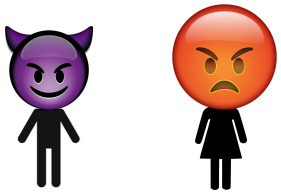
Just put H(R) in receipt and PISA reveals “R” to redeem HTLC payment.



Leaning Watchtower

Encr
Tran
Appointment Start: Block 10
Appointment Expiry: Block 500
Minimum Dispute Period: 50 blocks
Signature by PISA: σ_{PISA}

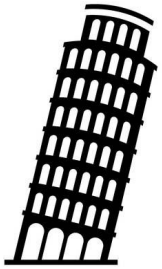
Monitor (Tadge) @ Scaling Bitcoin ‘16



Scenario

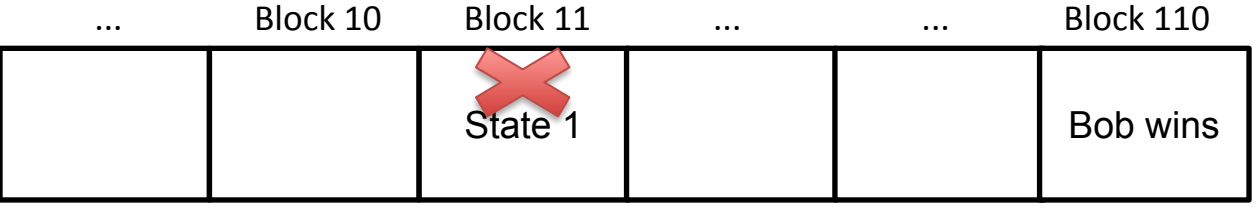
Bob triggered a dispute,
PISA failed to respond,
Bob gets the coins.

How can Alice prove wrongdoing?



Leaning Watchtower

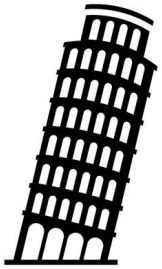
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice



Monitor (Tadge) @ Scaling Bitcoin ‘16

In-depth Signed Receipt

Encrypted Justice: ENCJustice
Transaction Locator: TxLocator1
Appointment Start: Block 10
Appointment Expiry: Block 500
Minimum Dispute Period: 50 blocks
Signature by PISA: σ_{PISA}

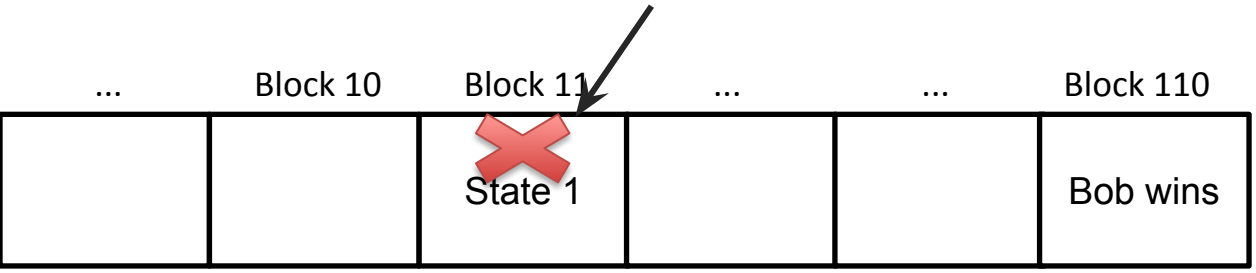


Leaning Watchtower

TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice

Anyone can verify the “dispute details” via blockchain:

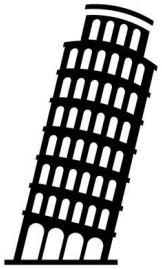
- TxLocator1 FOUND
- Dispute triggered between block 10 and 500
- Assume for now dispute time is >50 blocks



Monitor (Tadge) @ Scaling Bitcoin ‘16

In-depth Signed Receipt

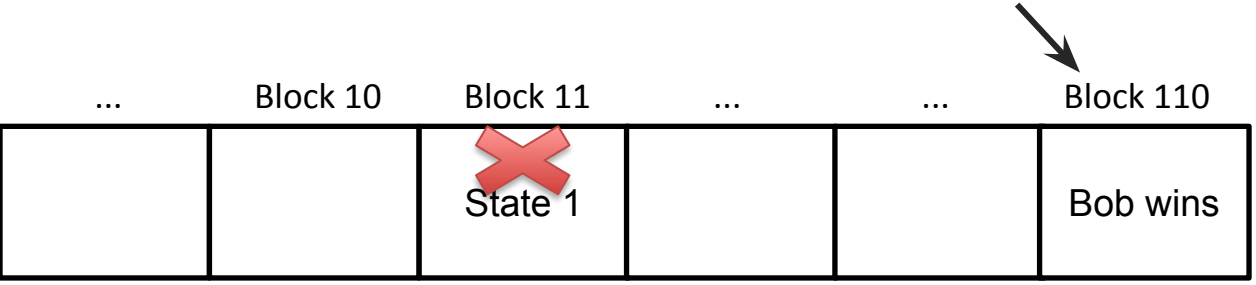
Encrypted Justice: ENCJustice
Transaction Locator: TxLocator1
Appointment Start: Block 10
Appointment Expiry: Block 500
Minimum Dispute Period: 50 blocks
Signature by PISA: σ_{PISA}



Leaning Watchtower

Anyone can decrypt ENCJustice and verify:

- Valid justice transaction
- Not included in the blockchain at all

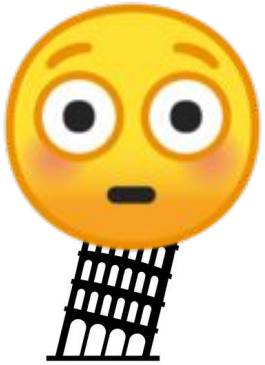


TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice

Monitor (Tadge) @ Scaling Bitcoin ‘16

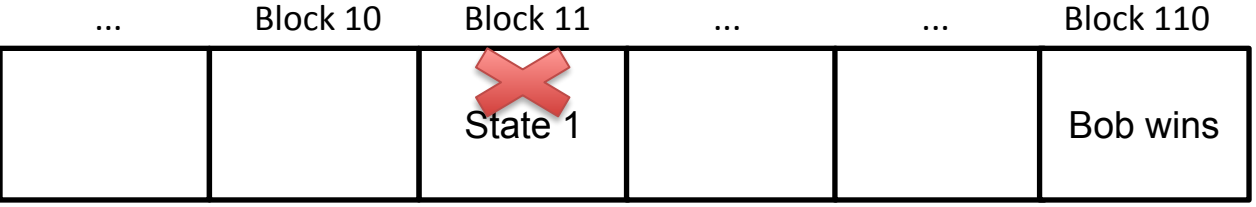
Reputational Accountability, not Financial
Publicly verifiable that PISA accepted the job and failed to do its duty by the customer.

With a consensus upgrade, the evidence of SPV proof for dispute + Bob’s spend transaction, could be used to slash/refund customer.



Leaning Watchtower

TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice

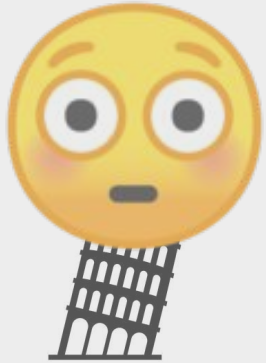


Monitor (Tadge) @ Scaling Bitcoin ‘16

Reputational Accountability, not Financial

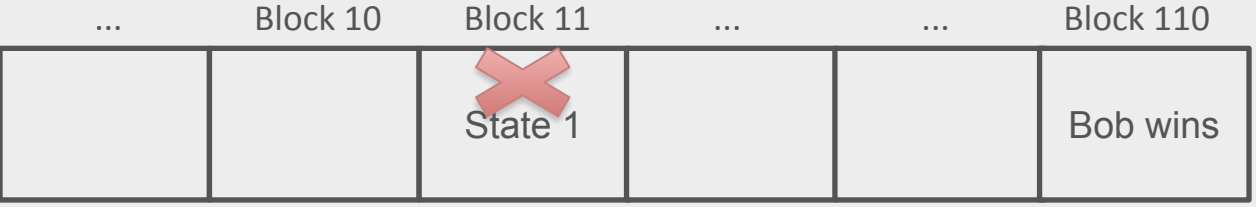
Publicly verifiable that PISA accepted the job and

Let’s look at the good, bad and the ugly



Leaning Watchtower

TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice



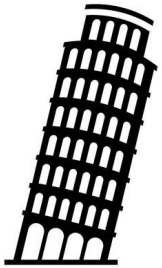
PISA - THE GOOD

Channel-Privacy

By re-using the Monitor protocol, PISA doesn't know what channel is being watched!

Accountability

We can prove to anyone that a PISA-tower cheated.



Leaning Watchtower

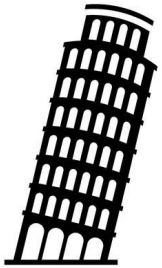
Simple Protocol

Adopting a signed receipt for different channel constructions is relatively straight-forward.

PISA - THE GOOD, BAD

Channel-Privacy	O(1) OR O(N) Storage	Accountability
By re-using the Monitor protocol, PISA doesn't know what channel is being watched!	Depends on the underlying channel construction (or if ENCJustice is stored on-chain via OUTPOST)	We can prove to anyone that a PISA-tower cheated.

Security Deposit hard	Simple Protocol
While there is "skin in the game", it may be under-collateralized. Provisions (2015) can help.	Adopting a signed receipt for different channel constructions is relatively straight-forward.

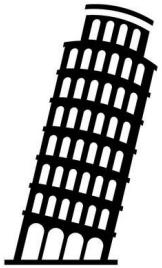


Leaning Watchtower

PISA - THE GOOD, BAD, AND THE UGLY

Channel-Privacy	O(1) OR O(N) Storage	Accountability
By re-using the Monitor protocol, PISA doesn't know what channel is being watched!	Depends on the underlying channel construction (or if ENCJustice is stored on-chain via OUTPOST)	We can prove to anyone that a PISA-tower cheated.

Security Deposit hard	Simple Protocol	Consensus Upgrade
While there is "skin in the game", it may be under-collateralized. Provisions (2015) can help.	Adopting a signed receipt for different channel constructions is relatively straight-forward.	We need a new OP_CODE for the slashing condition. Very likely, will not get into Bitcoin soon.



Leaning Watchtower

Watching Networks for Bitcoin (no forks)

No financial deterrent	**Channel-Privacy**	**O(N) Storage/Updates**	**Reputation Accountability via Signed Receipt**
No way for the blockchain to self-enforce that via slashing.	By re-using the Monitor protocol, PISA doesn't know what channel is being watched!	Depends in Monitor or Outpost. O(N) implies we need N-1 encrypted blobs, **so it leaks number of transfers.**	We can prove to anyone that a PISA-tower cheated.

Watching Networks for Bitcoin (no forks)

No financial deterrent No way for the blockchain to self-enforce that via slashing.	**Channel-Privacy** By re-using the Monitor protocol, PISA doesn't know what channel is being watched!	**O(N) Storage/Updates** Depends in Monitor or Outpost. O(N) implies we need N-1 encrypted blobs, **so it leaks number of transfers.**	**Reputation Accountability via Signed Receipt** We can prove to anyone that a PISA-tower cheated.
Fair exchange payment + job via offchain tx PISA can be hired via the lightning network. Not knowing which channel hired it.	Watching Networks for Bitcoin (no forks)		**TX + State Intertwined == bumping fee is HARD** PISA can't sign state & broadcast it, must get a "pre-signed" justice tx.

No financial deterrent

No way for the blockchain to self-enforce that via slashing.

Channel-Privacy

By re-using the Monitor protocol, PISA doesn't know what channel is being watched!

O(N) Storage/Updates

Depends in Monitor or Outpost. O(N) implies we need N-1 encrypted blobs, **so it leaks number of transfers.**

Reputation Accountability via Signed Receipt

We can prove to anyone that a PISA-tower cheated.

Fair exchange payment + job via offchain tx

PISA can be hired via the lightning network. Not knowing which channel hired it.

Watching Networks for Bitcoin (no forks)

TX + State Intertwined == bumping fee is HARD

PISA can't sign state & broadcast it, must get a "pre-signed" justice tx.

Consensus upgrades required

A lot of problems can be fixed. We, as a community, must seriously consider them.

Responder, not trigger

We CANNOT trigger any disputes! Only respond if the counterparty tries to cheat.

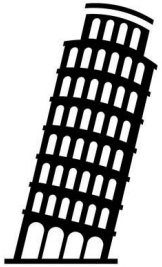
No Verifiable Jobs (May store junk)

Important that PISA is paid up-front for storing "blobs" and not via bounties.

Simple Protocol

Encrypting and decrypting blobs is straight forward, but reducing O(N) storage "constant" is ugly.

PISA - Final word about “watchers” and their emerging role



Responder of LAST resort

Financial Liability & Insurance

Watchers take on the “financial liability” for users who go offline.

The “cost” of a watcher is some function of financial liability, number of updates & number of channels watched.

What can a watchtower do?

Protect hubs against crashes + dos attacks by responding to malicious customer closures

What can a watchtower NOT do?

Protect hubs against insider threats, theft of signing keys, etc.

PISA - WHERE ARE WE NOW?

PRIVATE TEST

We have a working basic PISA implementation.

Signed Receipt BOLT

Coming soon to a wallet near you!

(after guinea pigs try out our demo)

Do you want to try out our watchtower?

Please contact us!


@sr_gi


@paddypisa


@PisaResearch

https://pisa.watch