PISA

A financially accountable watching network

Patrick McCorry

PisaResearch
paddypisa

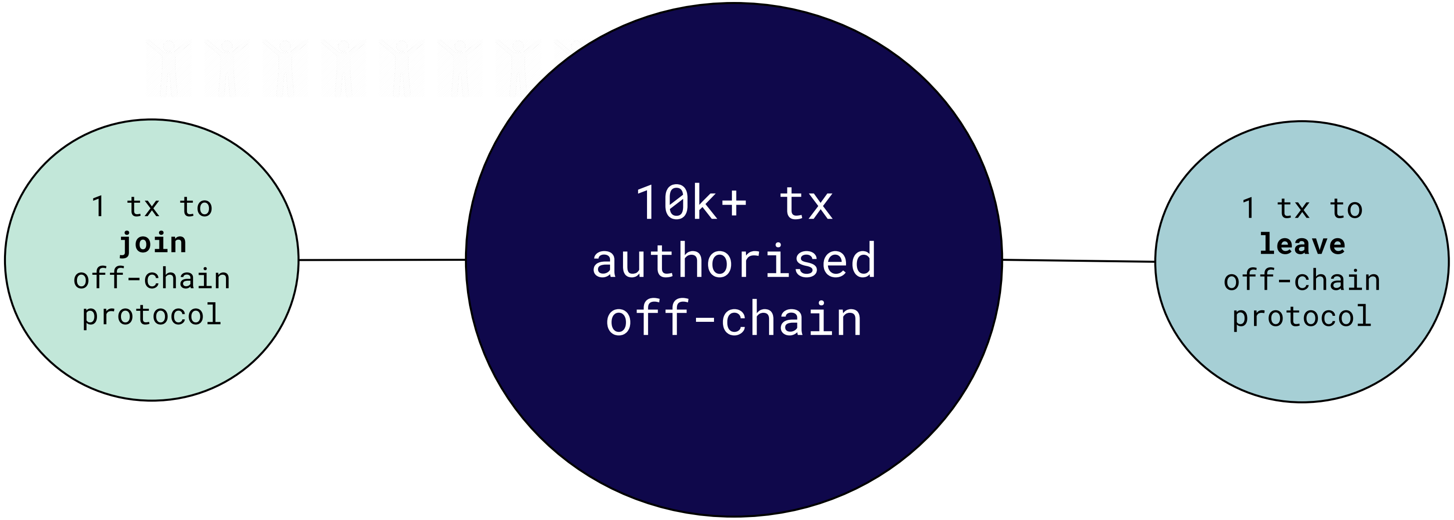
RESEARCH INSTITUTE.

Ethereum Community Fund

ethereum foundation grants

BINANCE_X

WHY IS OFF-CHAIN EXCITING?



1 tx to **join** off-chain protocol

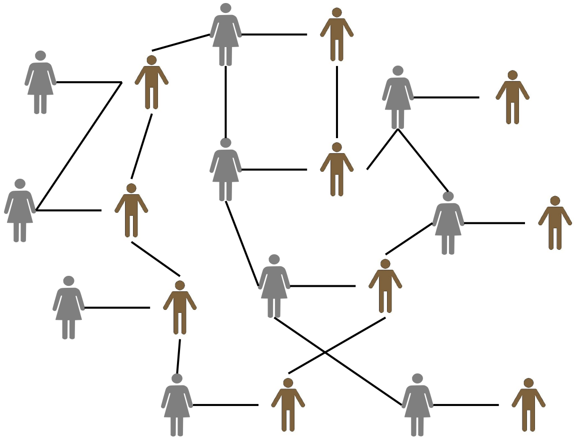
10k+ tx authorised off-chain

1 tx to **leave** off-chain protocol

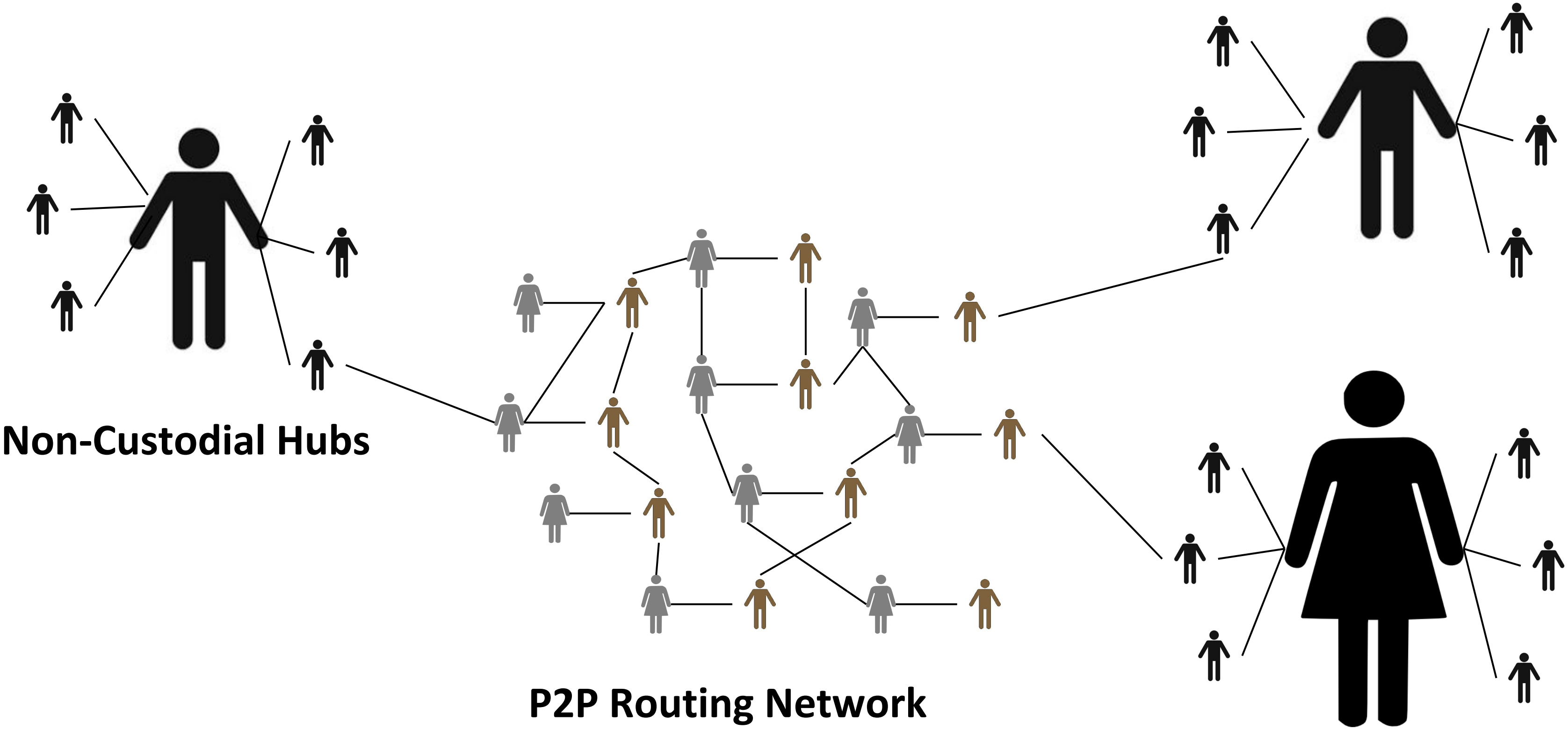
Bypass all blockchain latency and fees
While still retaining non-custodial security guarantees.

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?

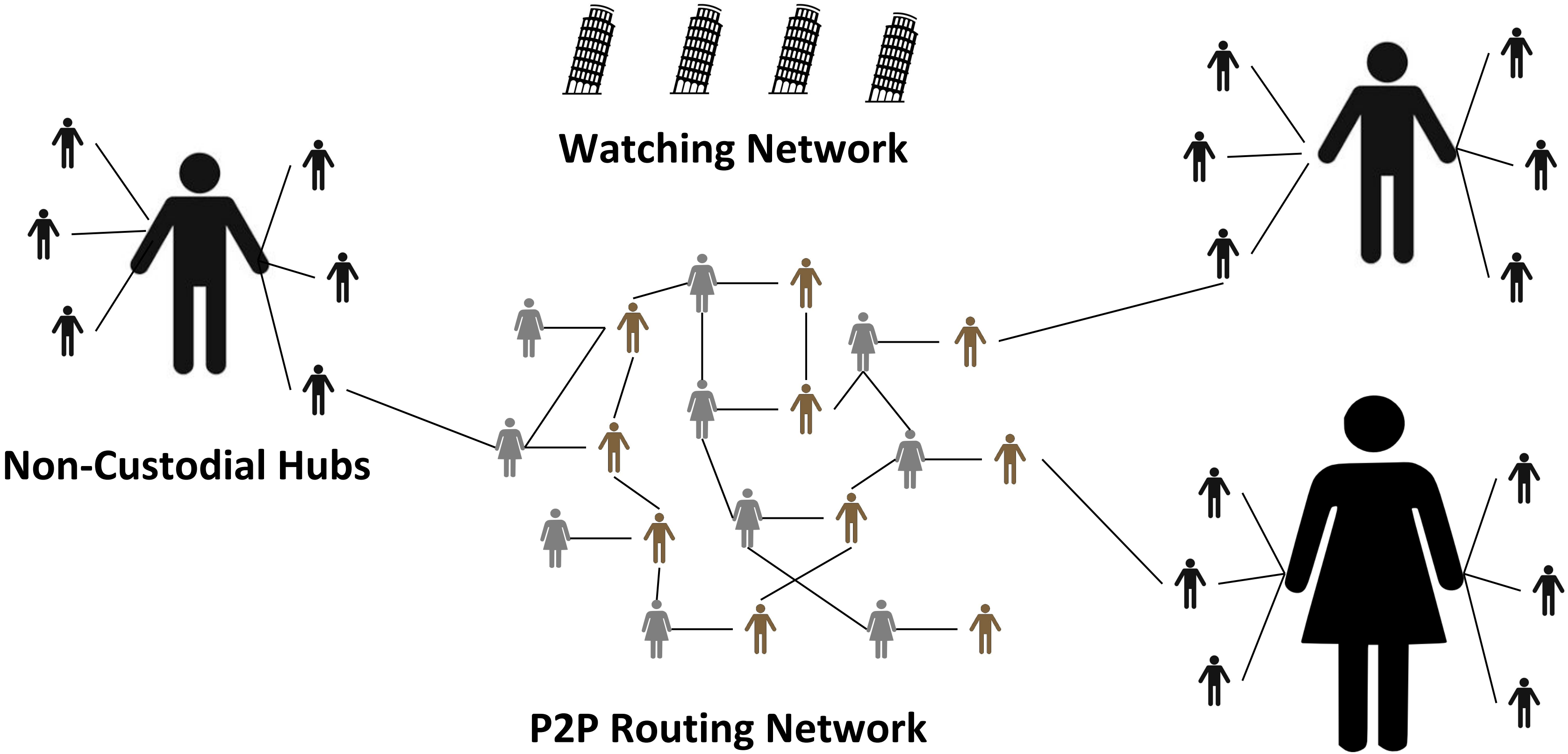


P2P Routing Network



Non-Custodial Hubs

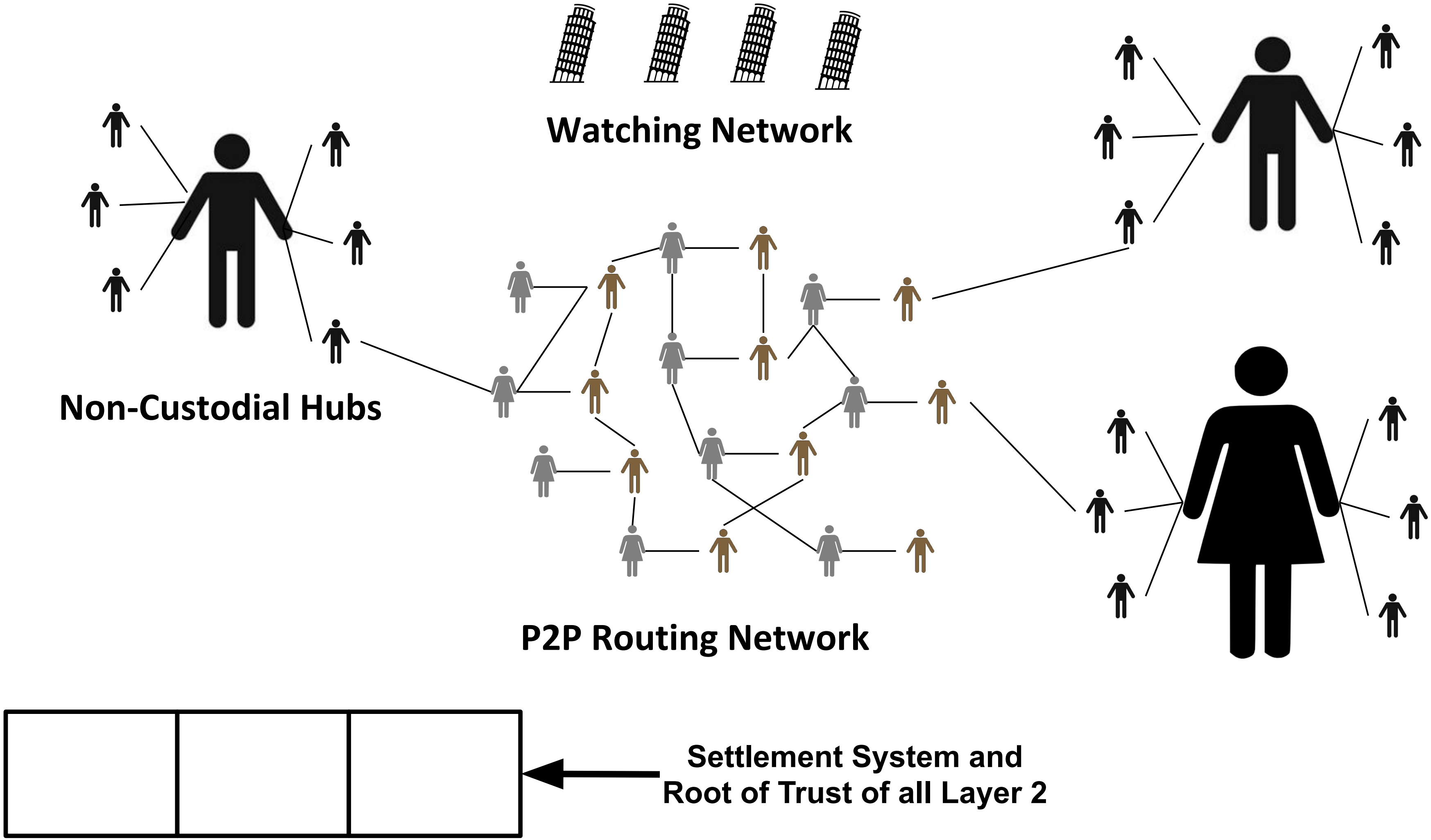
P2P Routing Network



Watching Network

Non-Custodial Hubs

P2P Routing Network

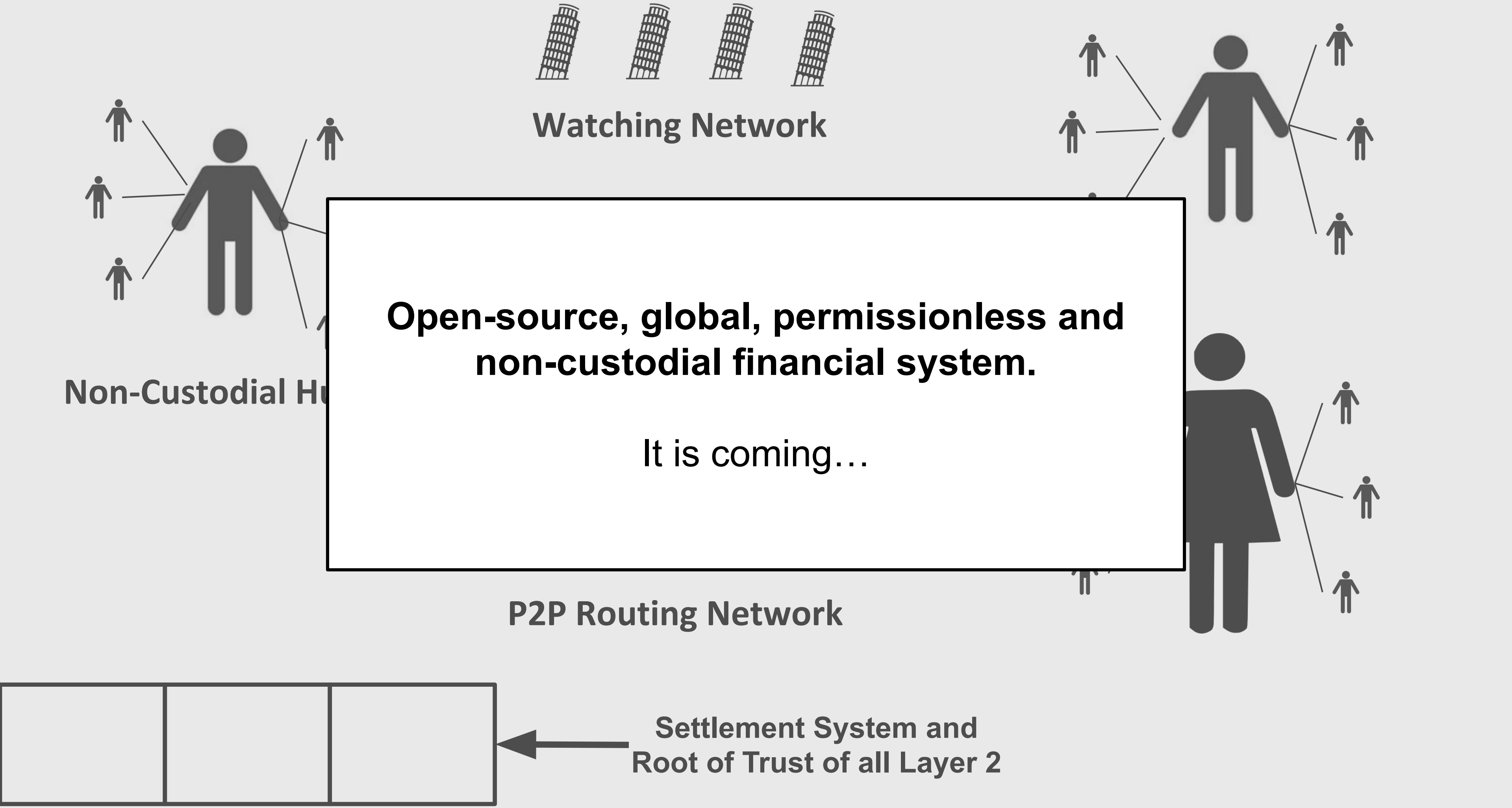


Watching Network

Non-Custodial Hubs

P2P Routing Network

Settlement System and
Root of Trust of all Layer 2



Watching Network

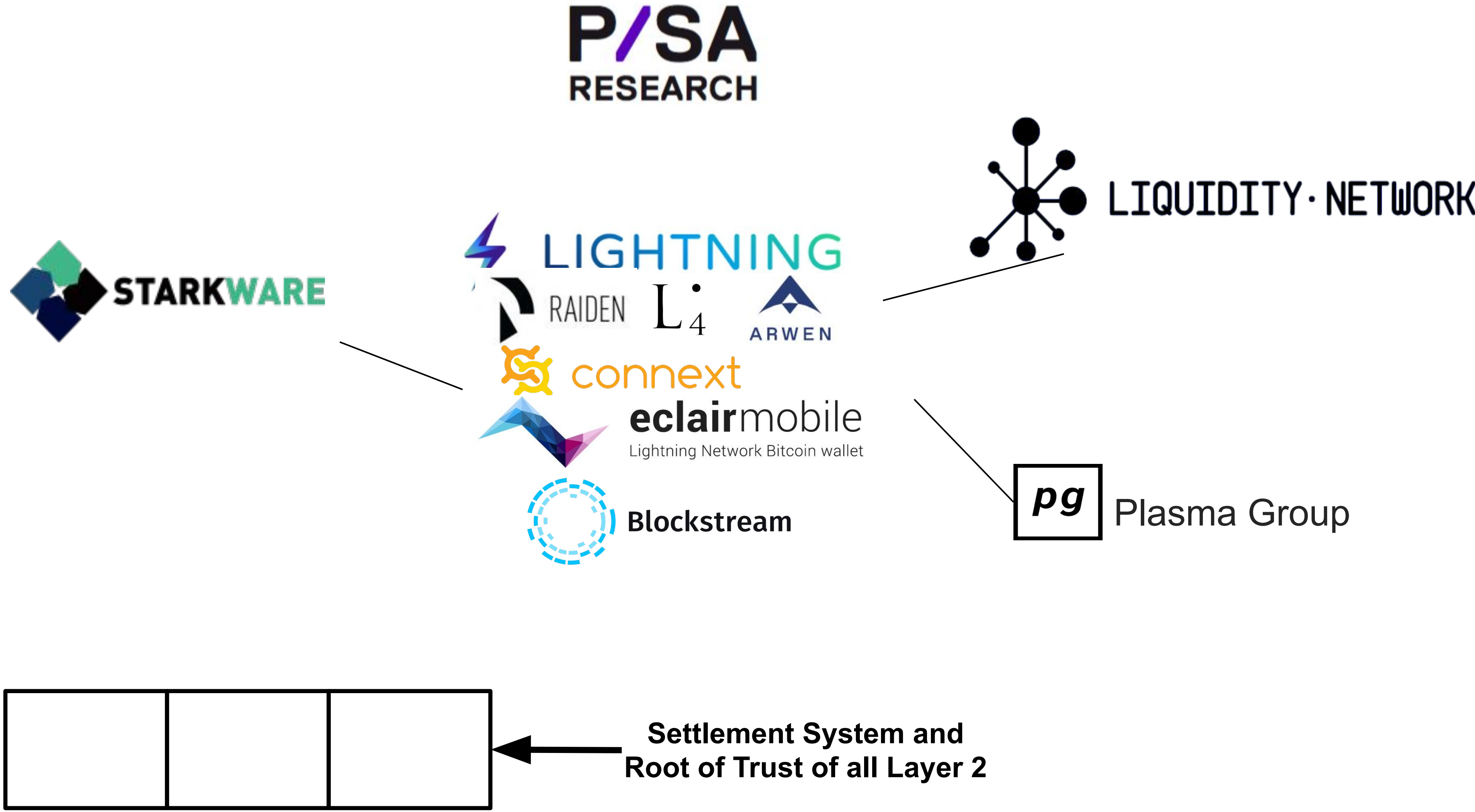
Open-source, global, permissionless and non-custodial financial system.

It is coming…

Non-Custodial Hu

P2P Routing Network

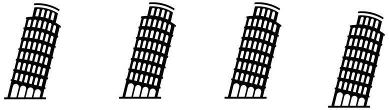
Settlement System and Root of Trust of all Layer 2



Settlement System and Root of Trust of all Layer 2

Plenty of talks about channels + plasma.

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.

State 1A

State 1B

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

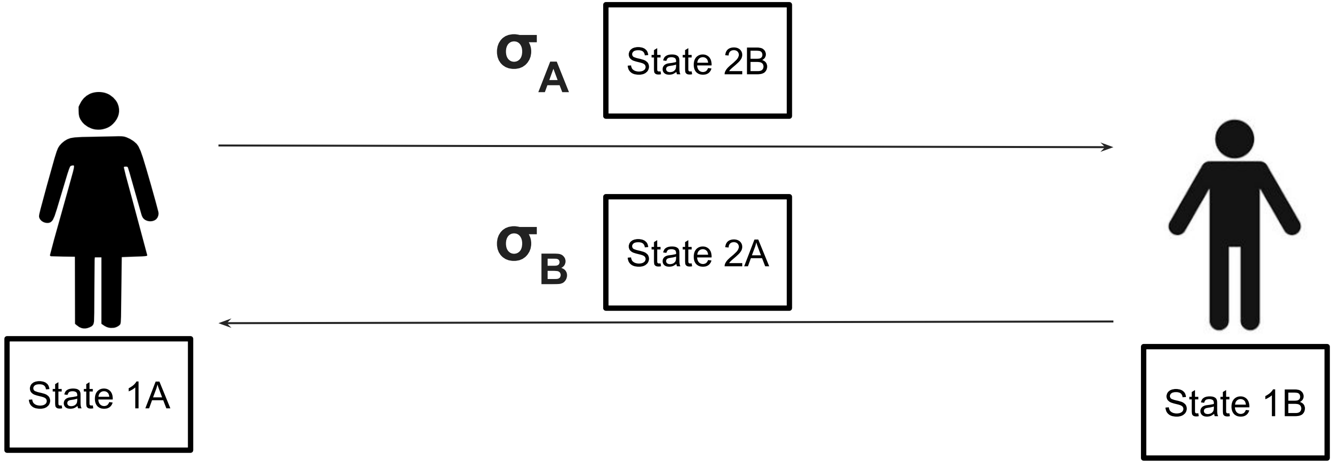
`Authorising a payment is a two-step process`

State 1A

State 1B

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.

State 2A

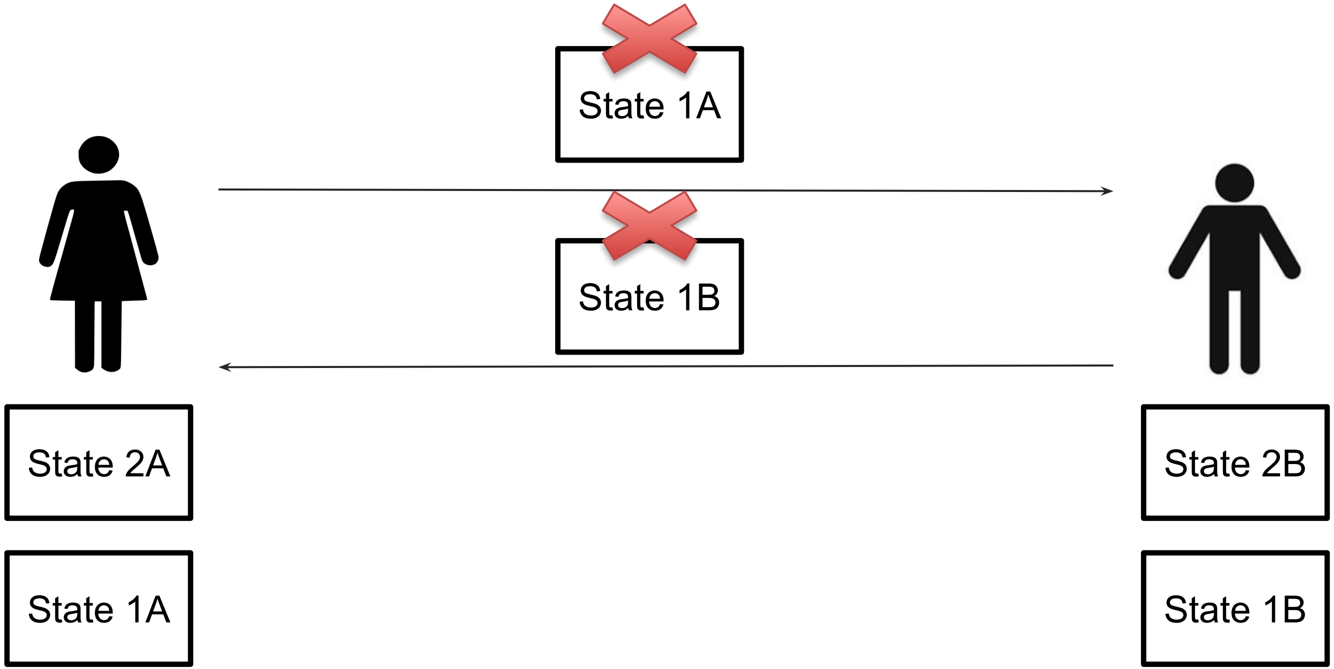
State 1A

State 2B

State 1B

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

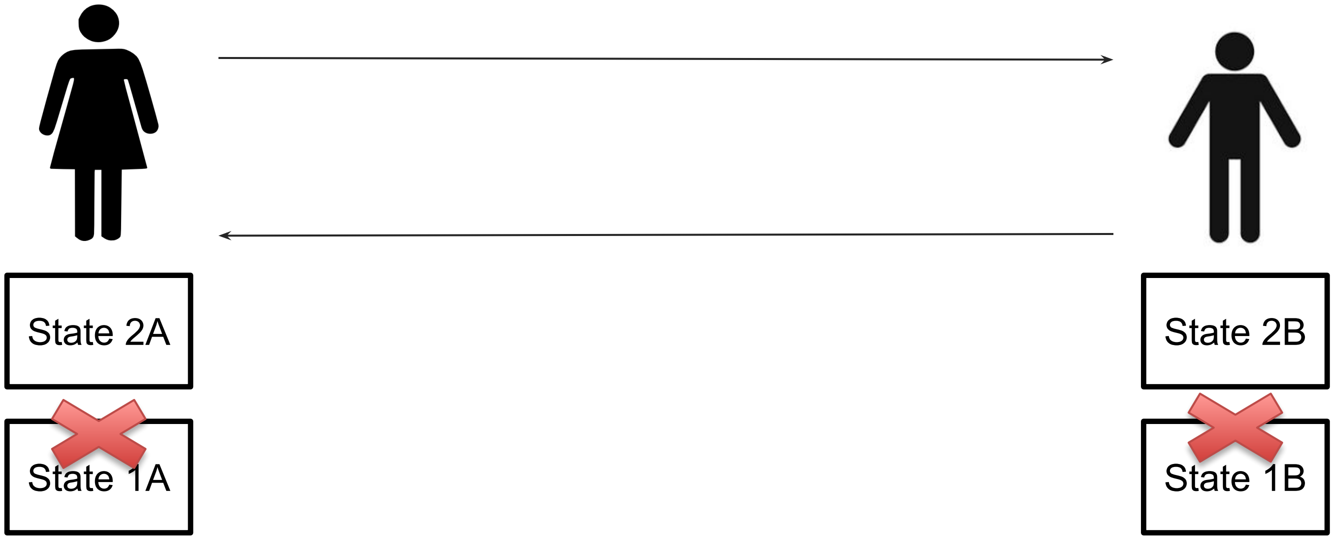
2. Both parties will “revoke” the old state
(i.e. share pre-image of hash)



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

Complete!

Both parties can always broadcast the latest state.



State 2A

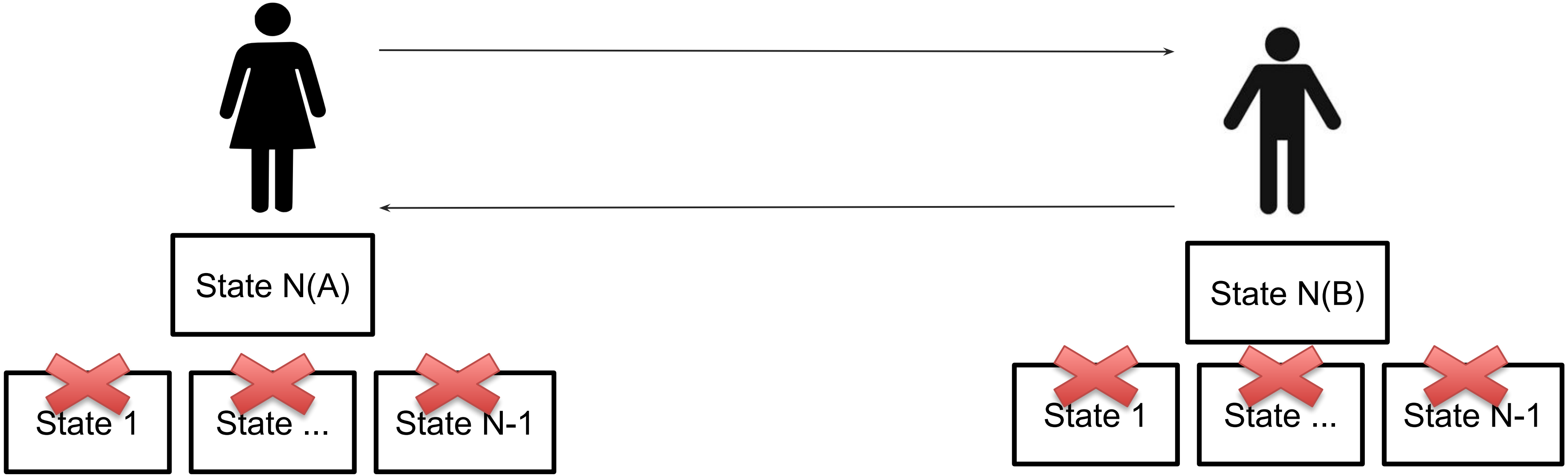
~~State 1A~~

State 2B

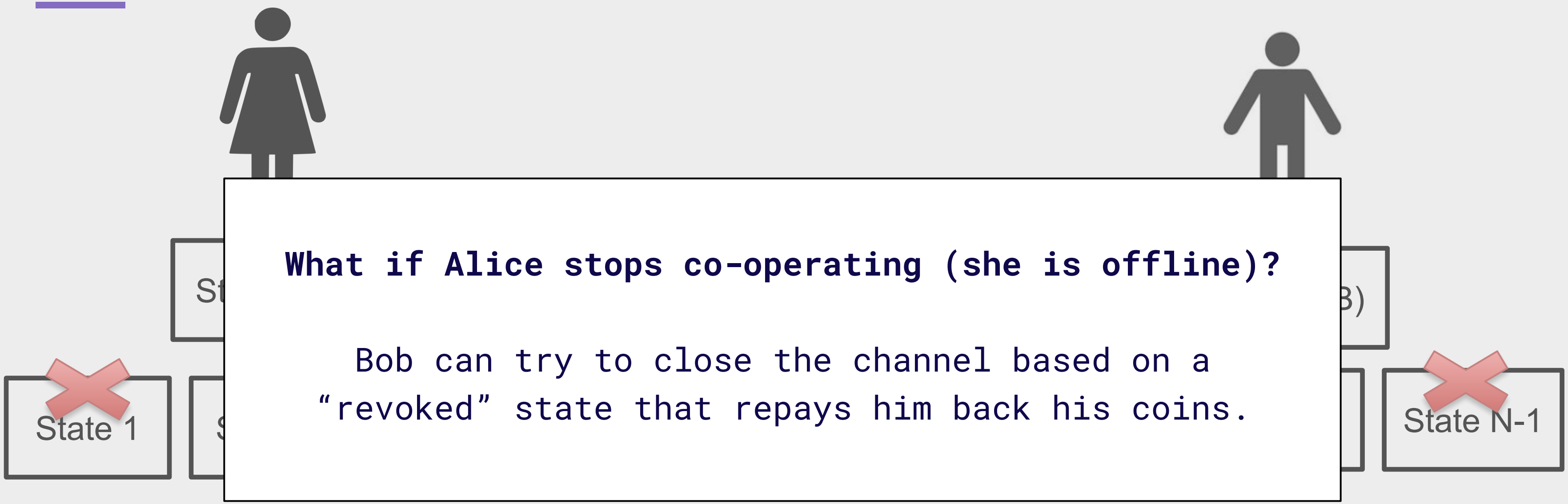
~~State 1B~~

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...



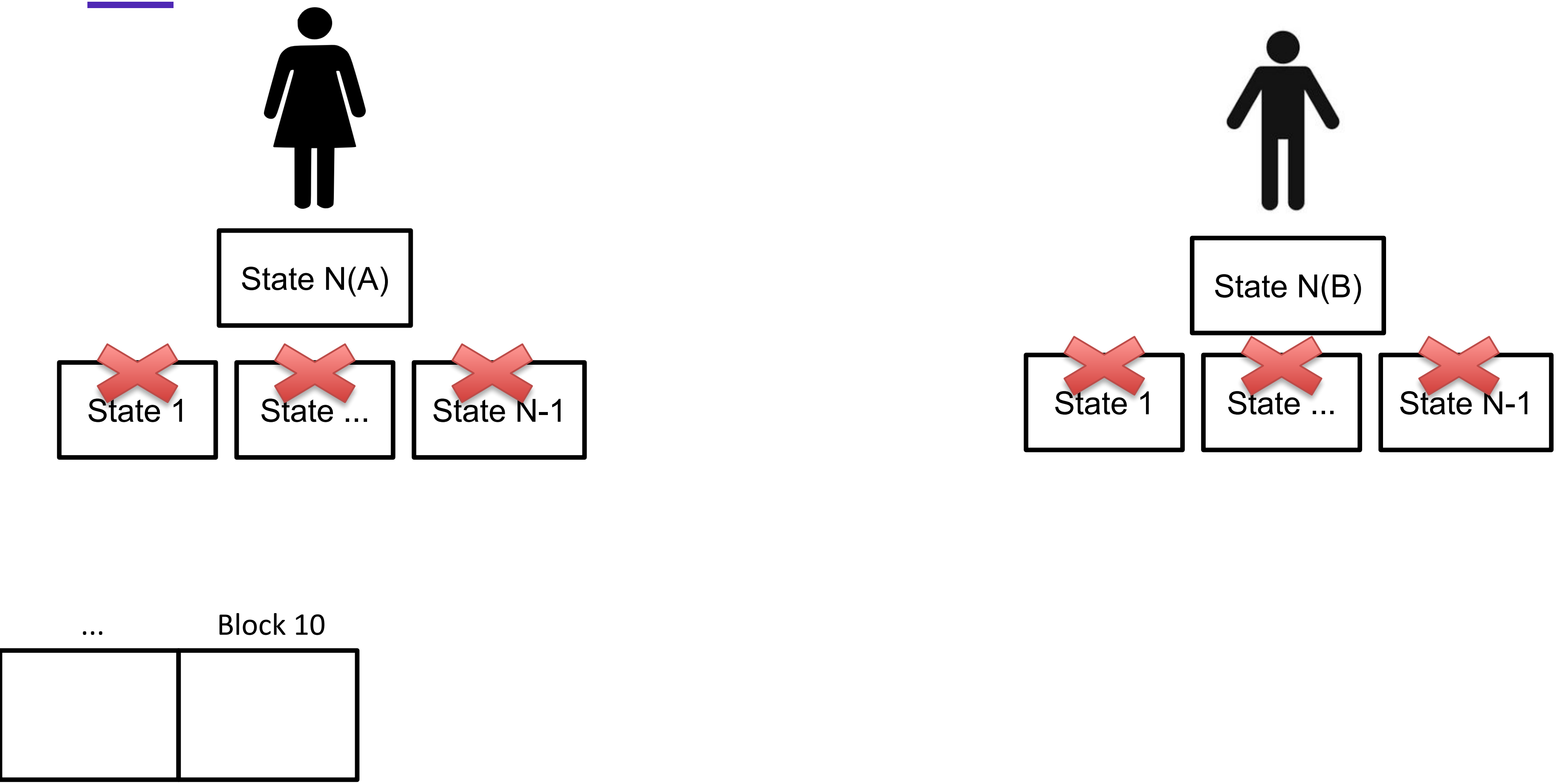
What does a lightning channel look like? (replace-by-revocation)



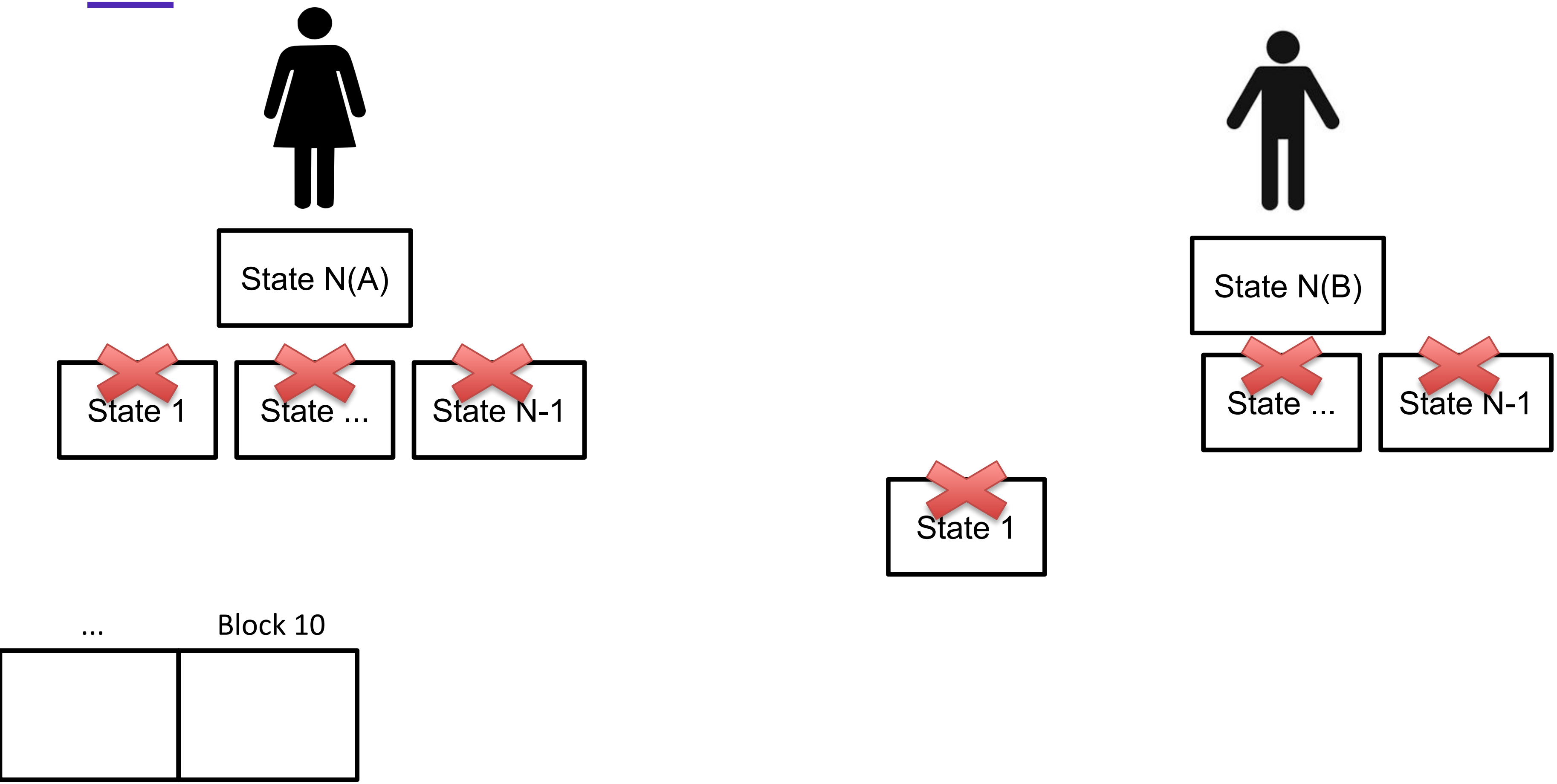
What if Alice stops co-operating (she is offline)?

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)



State N(A)

~~State 1~~

~~State ...~~

~~State N-1~~

State N(B)

~~State ...~~

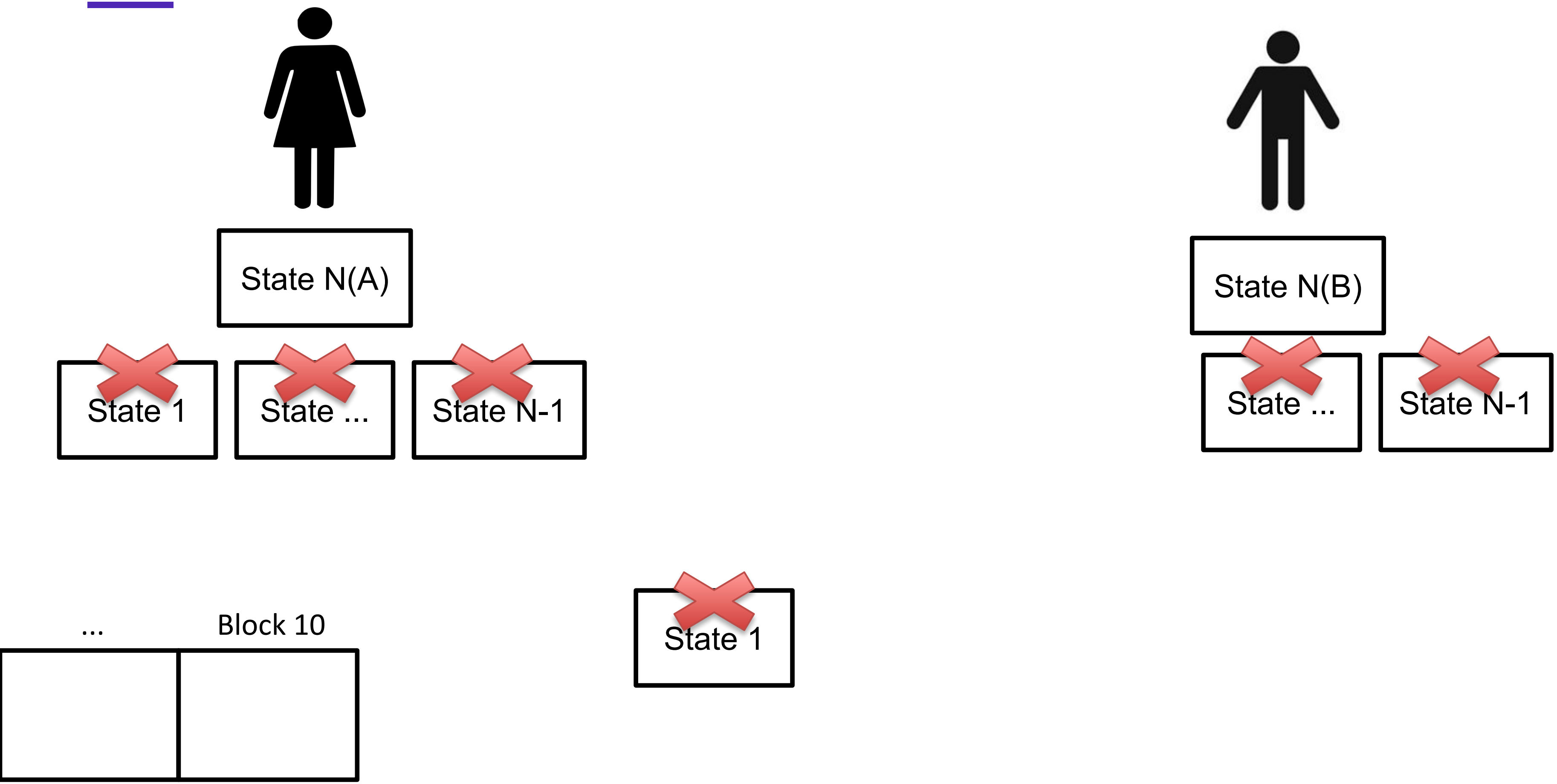
~~State N-1~~

~~State 1~~

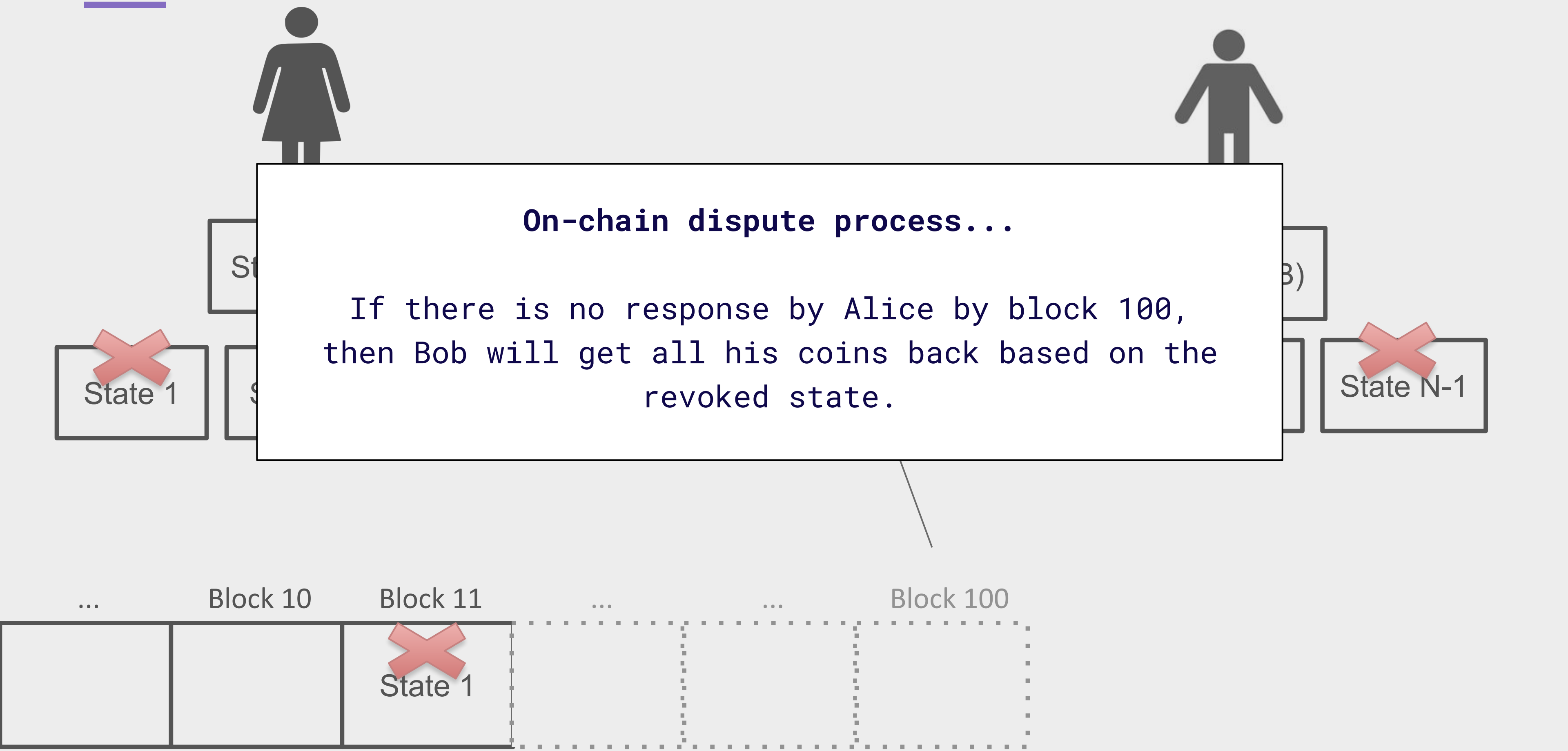
...

Block 10

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



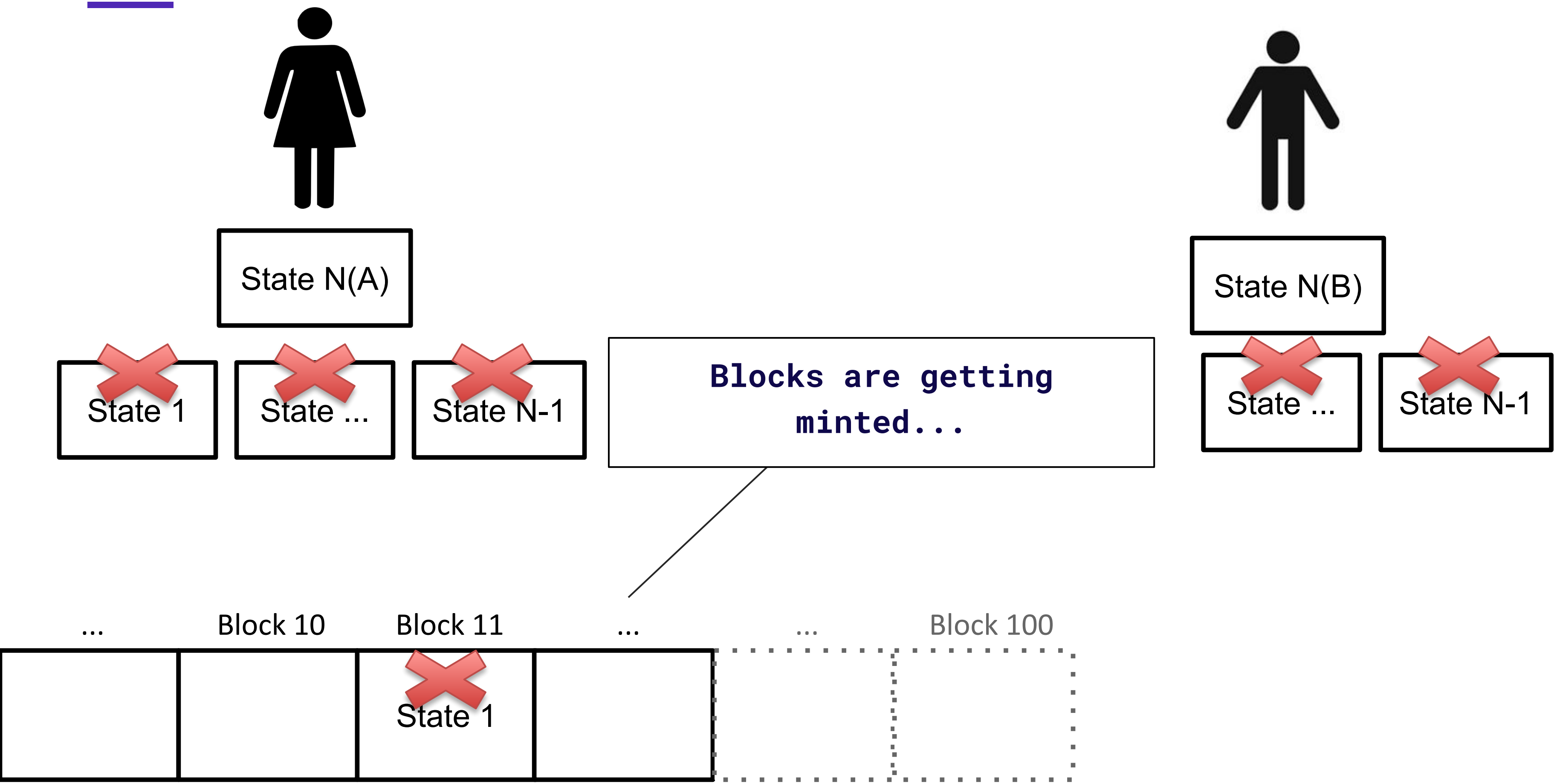
What does a lightning channel look like? (replace-by-revocation)



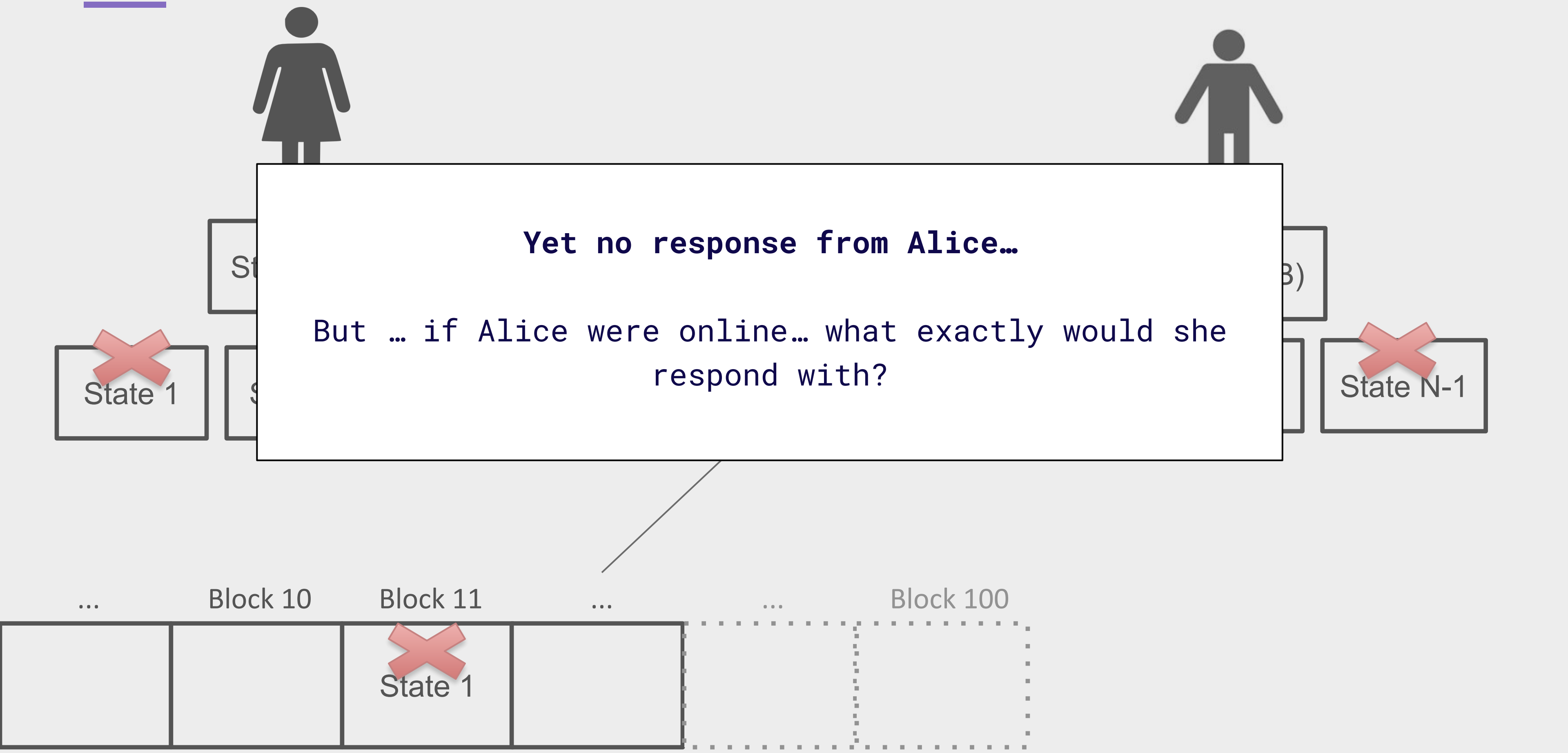
On-chain dispute process...

If there is no response by Alice by block 100, then Bob will get all his coins back based on the revoked state.

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



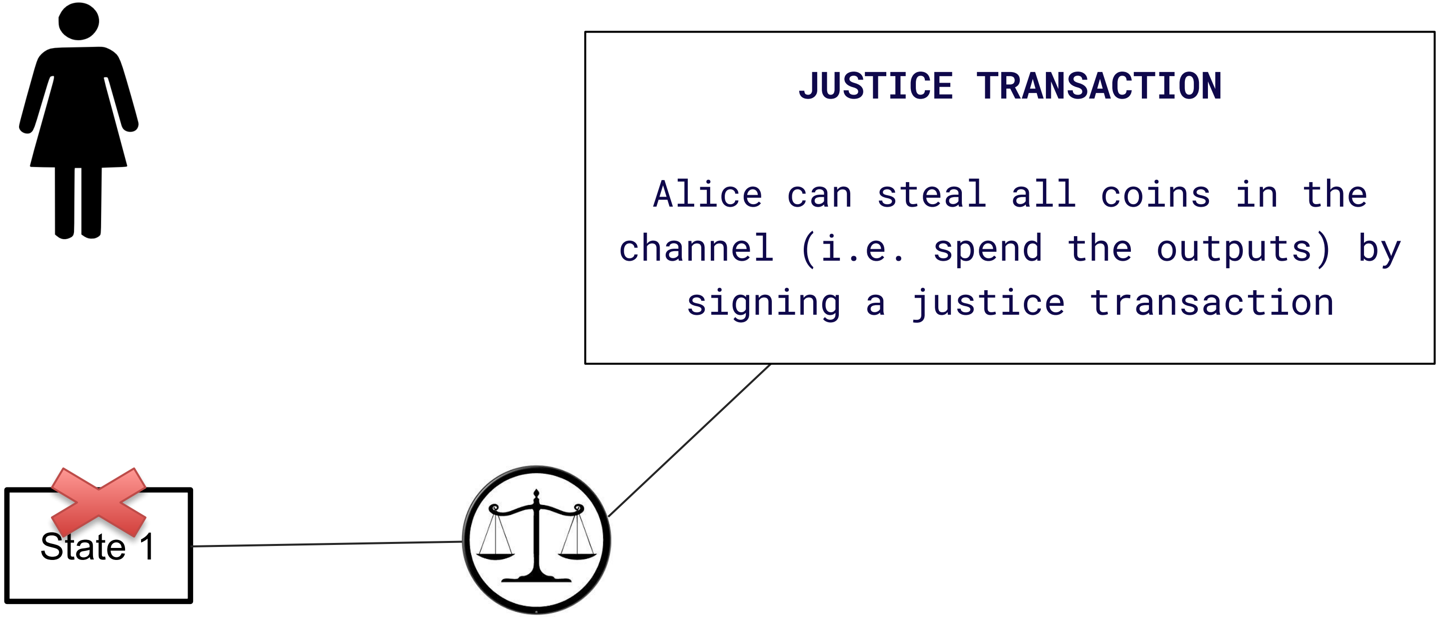
What does a lightning channel look like? (replace-by-revocation)



Yet no response from Alice…

But … if Alice were online… what exactly would she respond with?

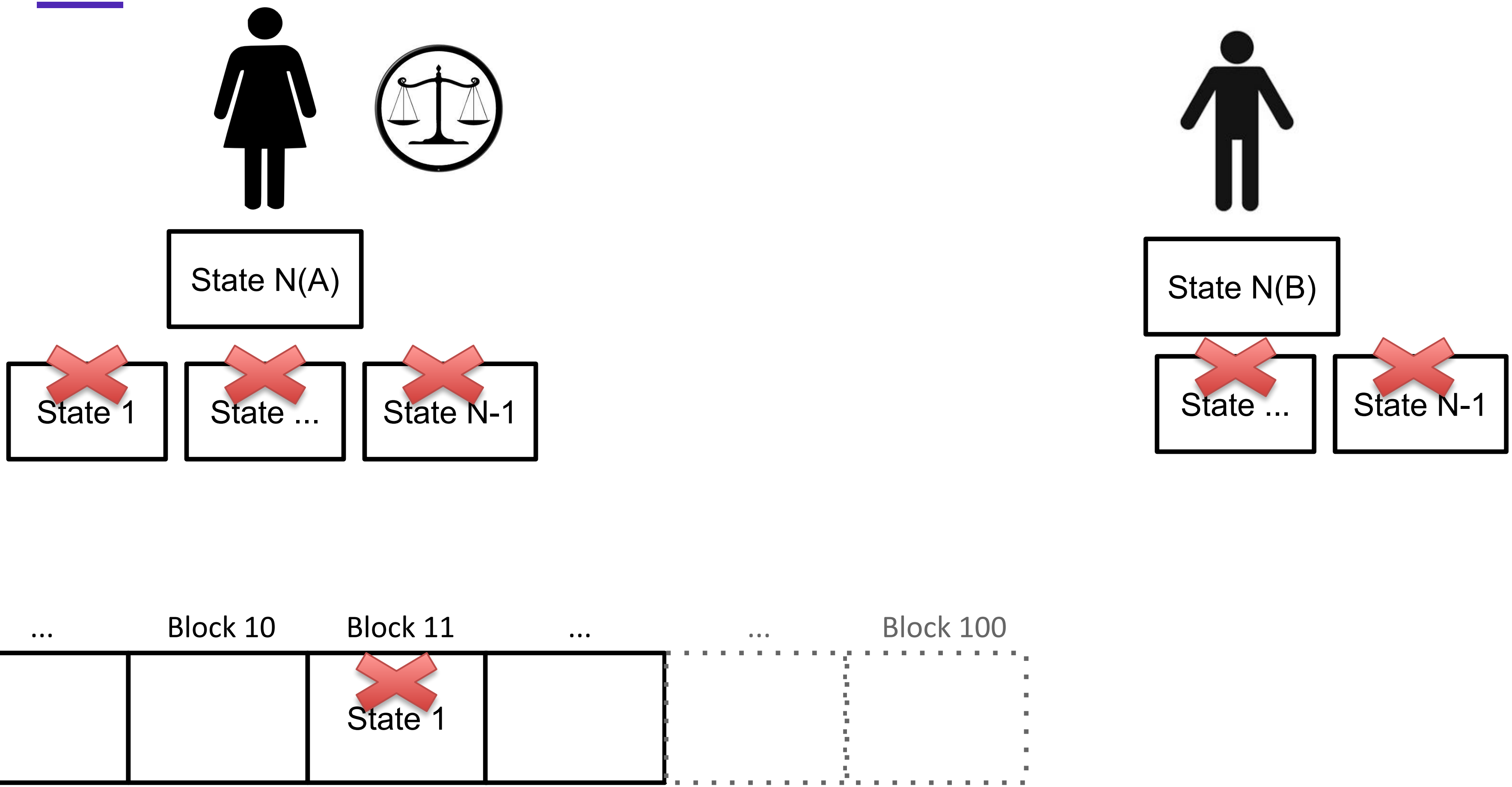
What does a lightning channel look like? (replace-by-revocation)



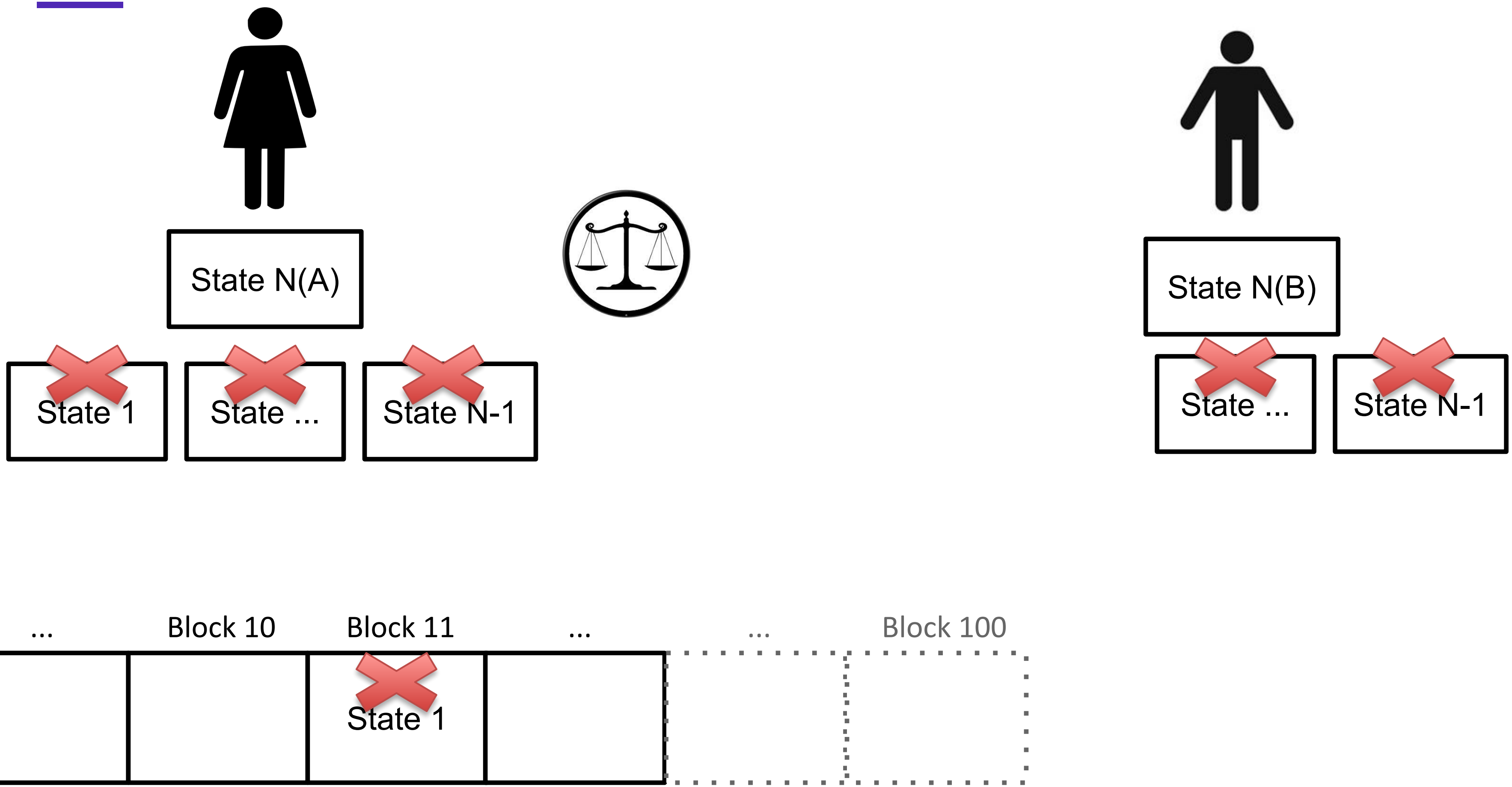
JUSTICE TRANSACTION

Alice can steal all coins in the channel (i.e. spend the outputs) by signing a justice transaction

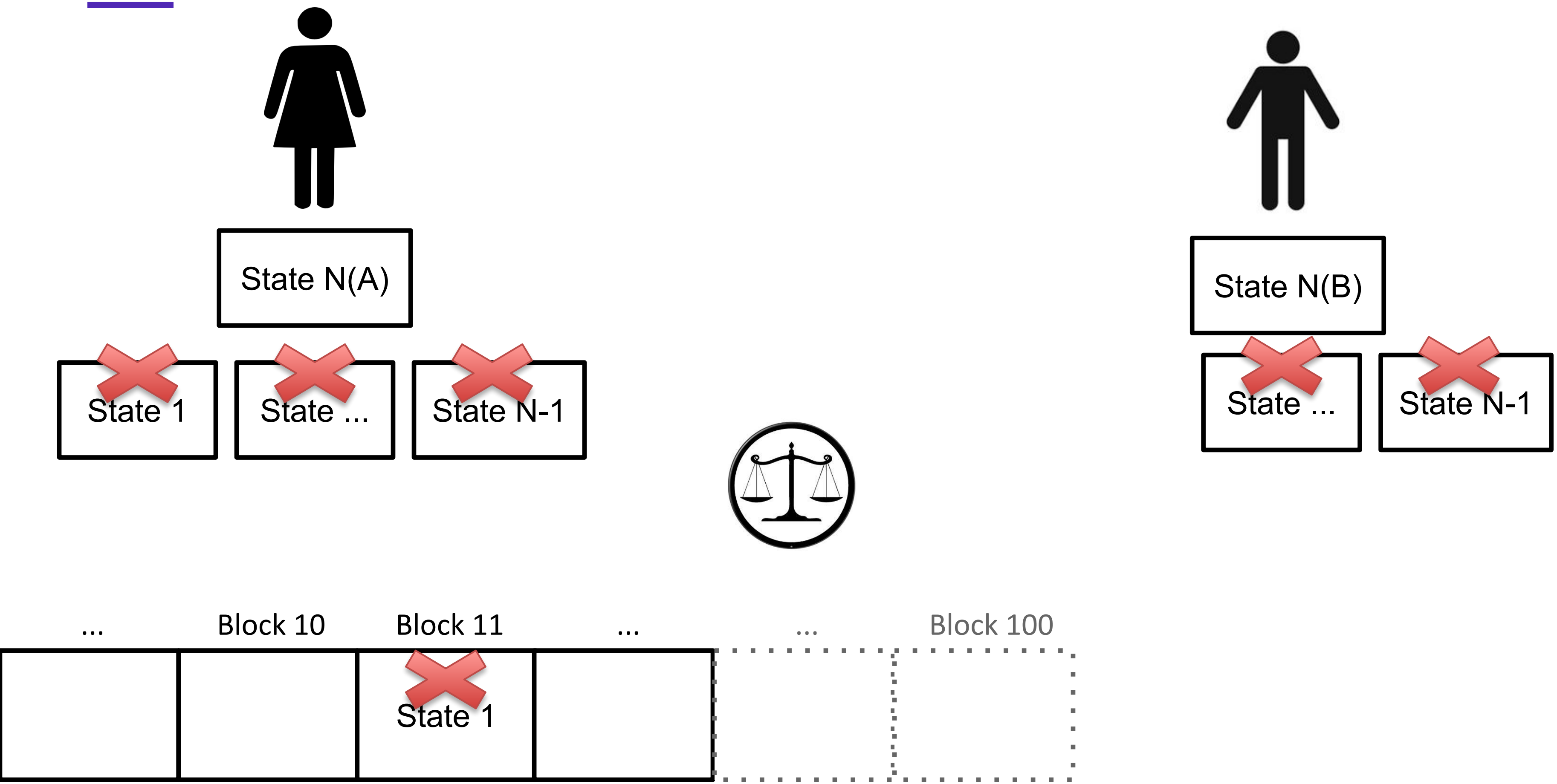
What does a lightning channel look like? (replace-by-revocation)



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 ...

State N-1

State N(B)

State ...

State N-1

...

Block 10

Block 11

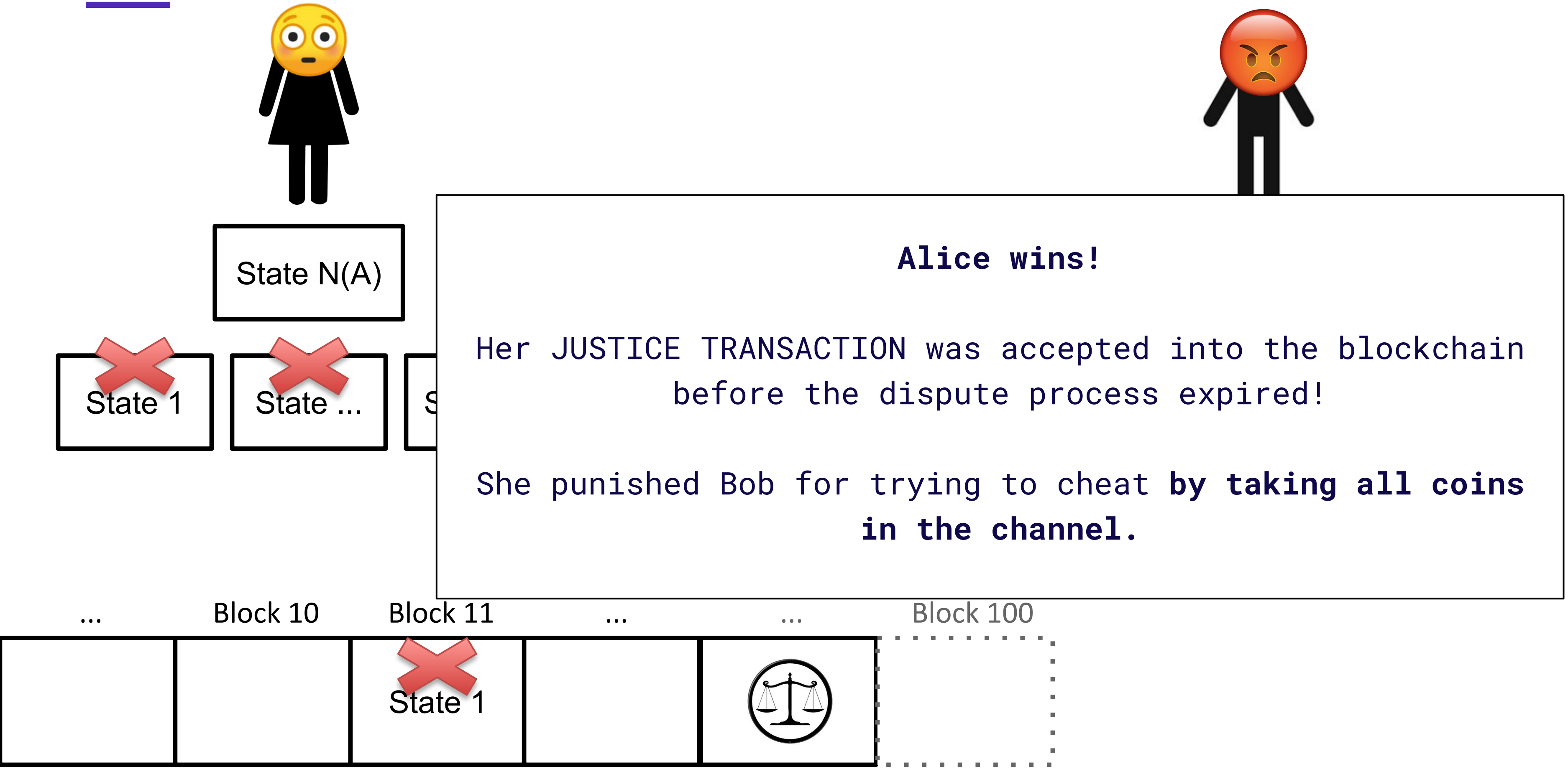
...

...

Block 100

State 1

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



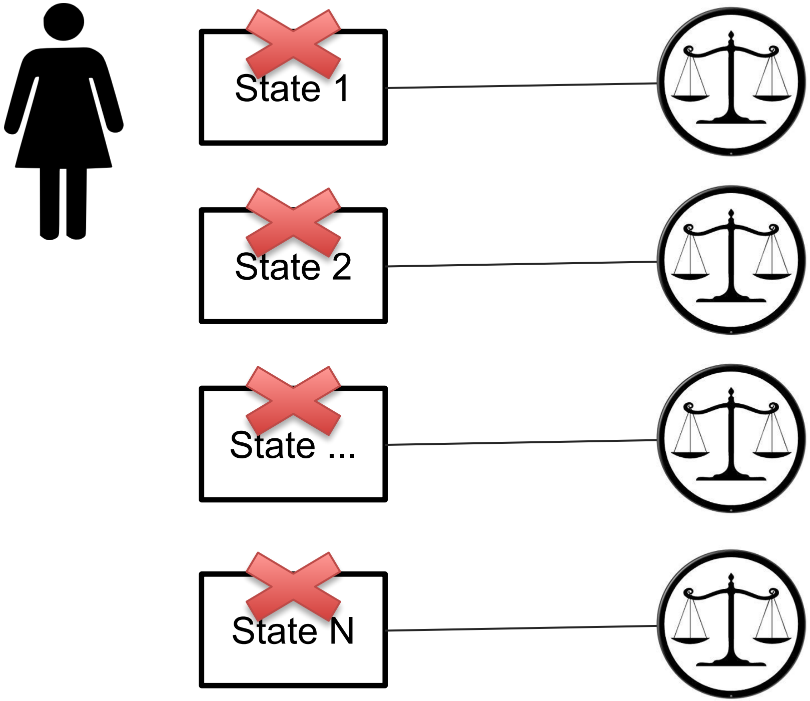
Alice wins!

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.**

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

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



Why?

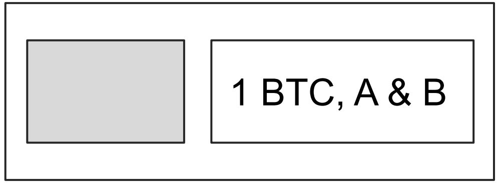
Bob has a LIST of REVOKED transactions that only HE can broadcast….

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

Remember, UTXO!

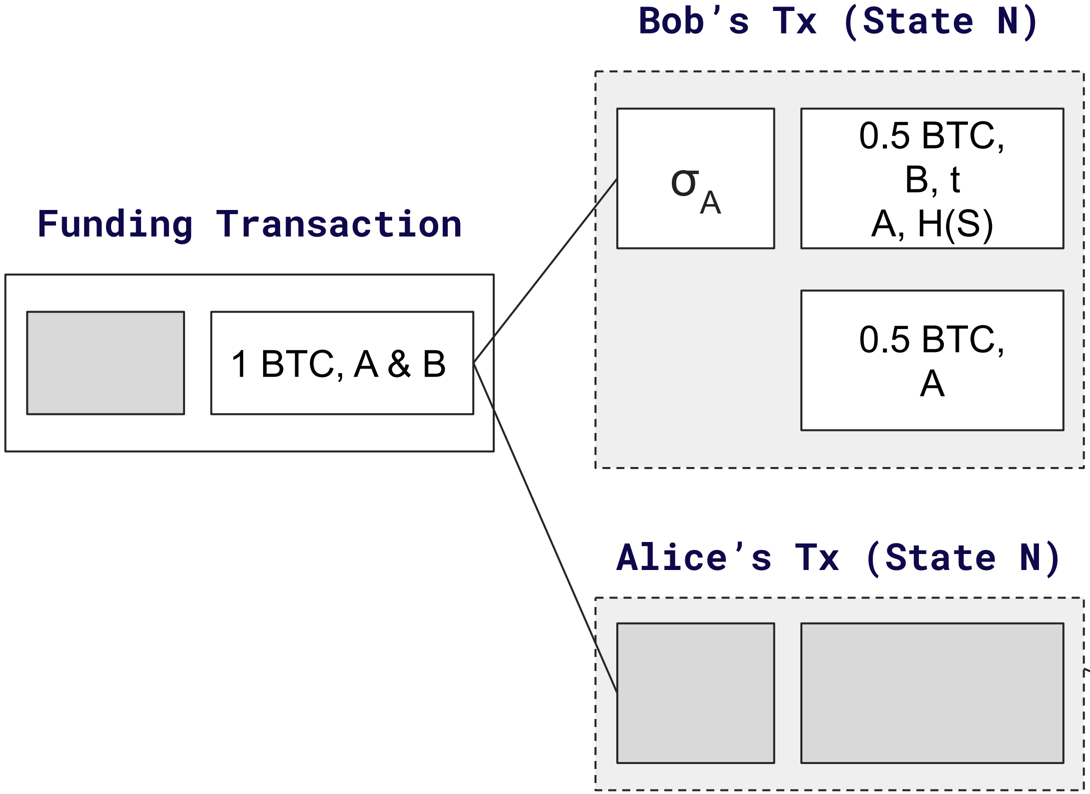
FAQ: Under the hood - what does it look like (roughly speaking)

Funding Transaction



1 BTC, A & B

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



Every state compromises of TWO transactions

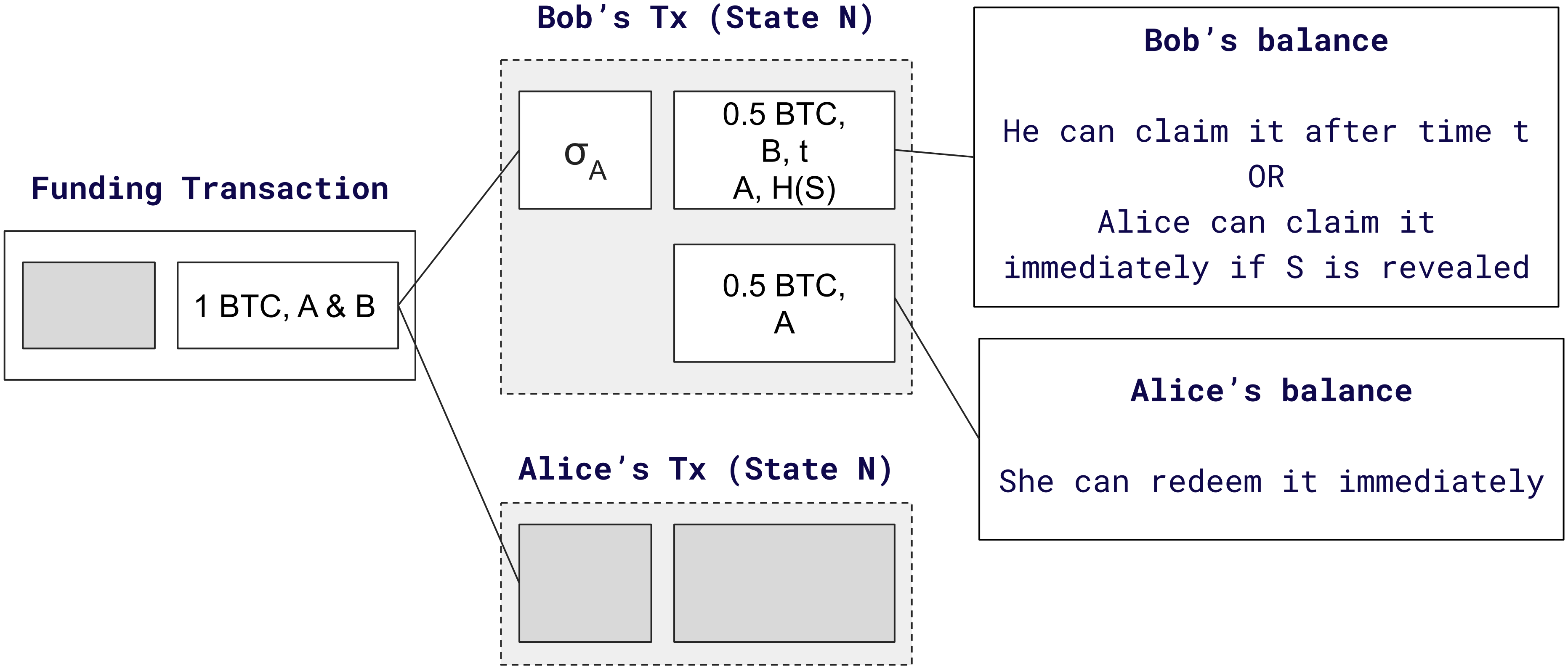
1 transaction only Alice can broadcast

1 transaction only Bob can broadcast

Symmetric to Bob's tx

We omit it for space

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



Funding Transaction

1 BTC, A & B

Bob's Tx (State N)

σ_A

0.5 BTC,
B, t
A, H(S)

0.5 BTC,
A

Alice's Tx (State N)

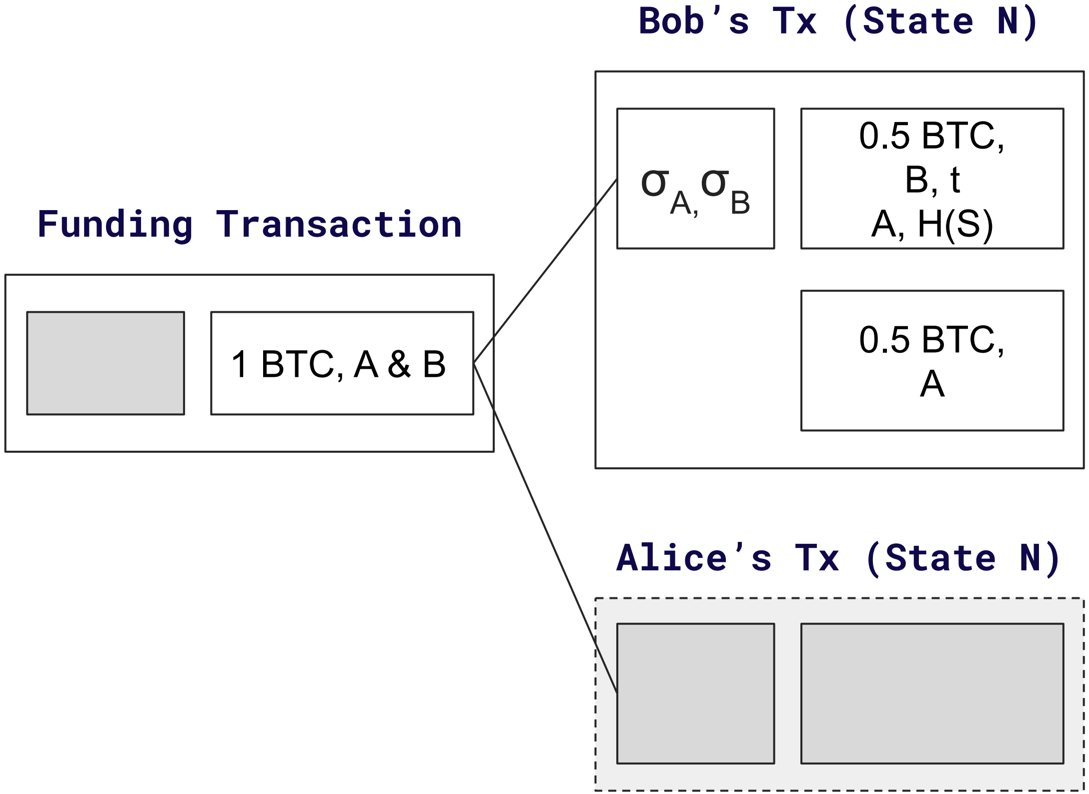
Bob's balance

He can claim it after time t
OR
Alice can claim it
immediately if S is revealed

Alice's balance

She can redeem it immediately

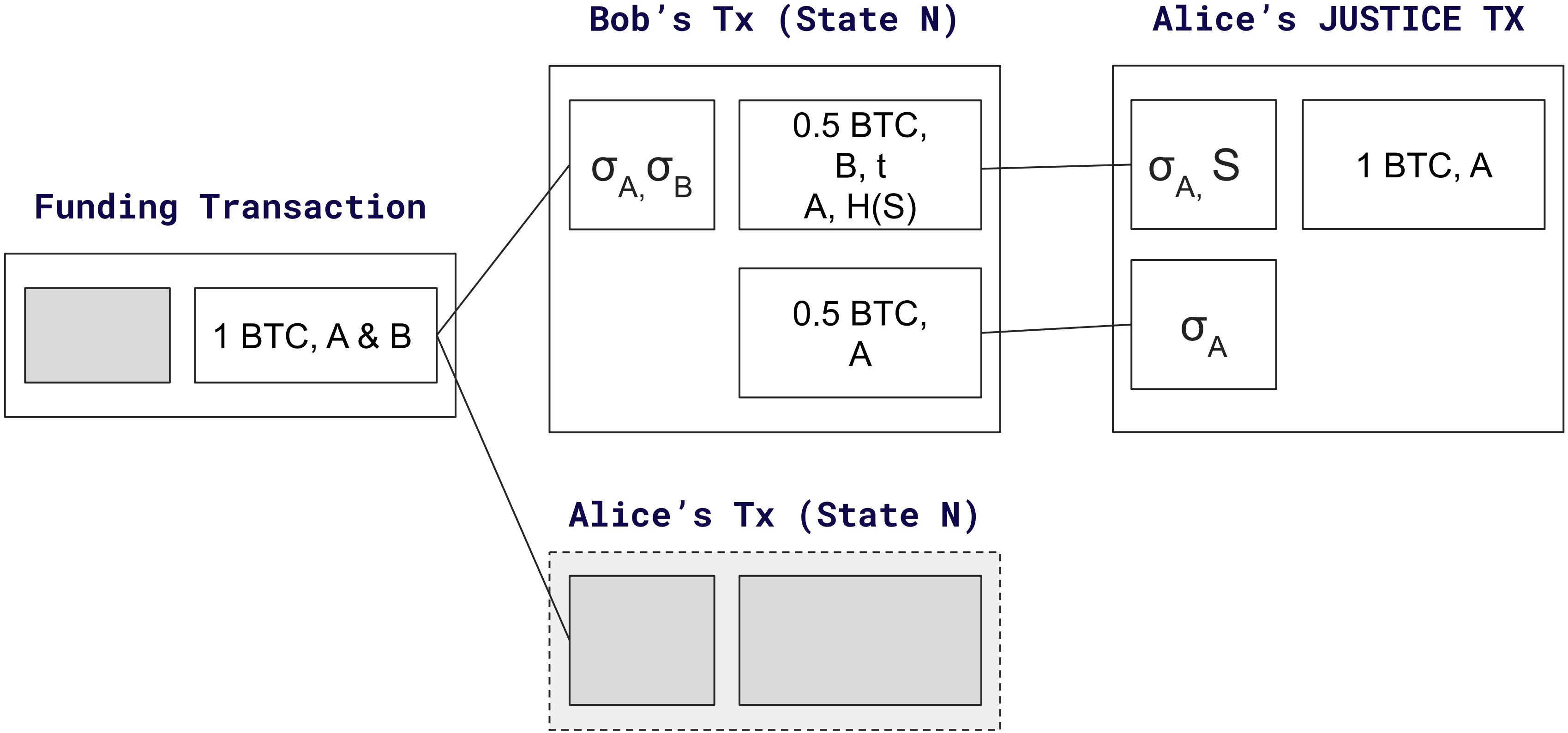
FAQ: Under the hood - what does it look like (roughly speaking)



Bob broadcasts it

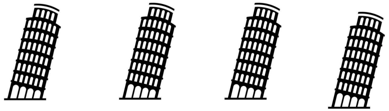
He can just sign and broadcast it at any time… to trigger the dispute period (up to time t)

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

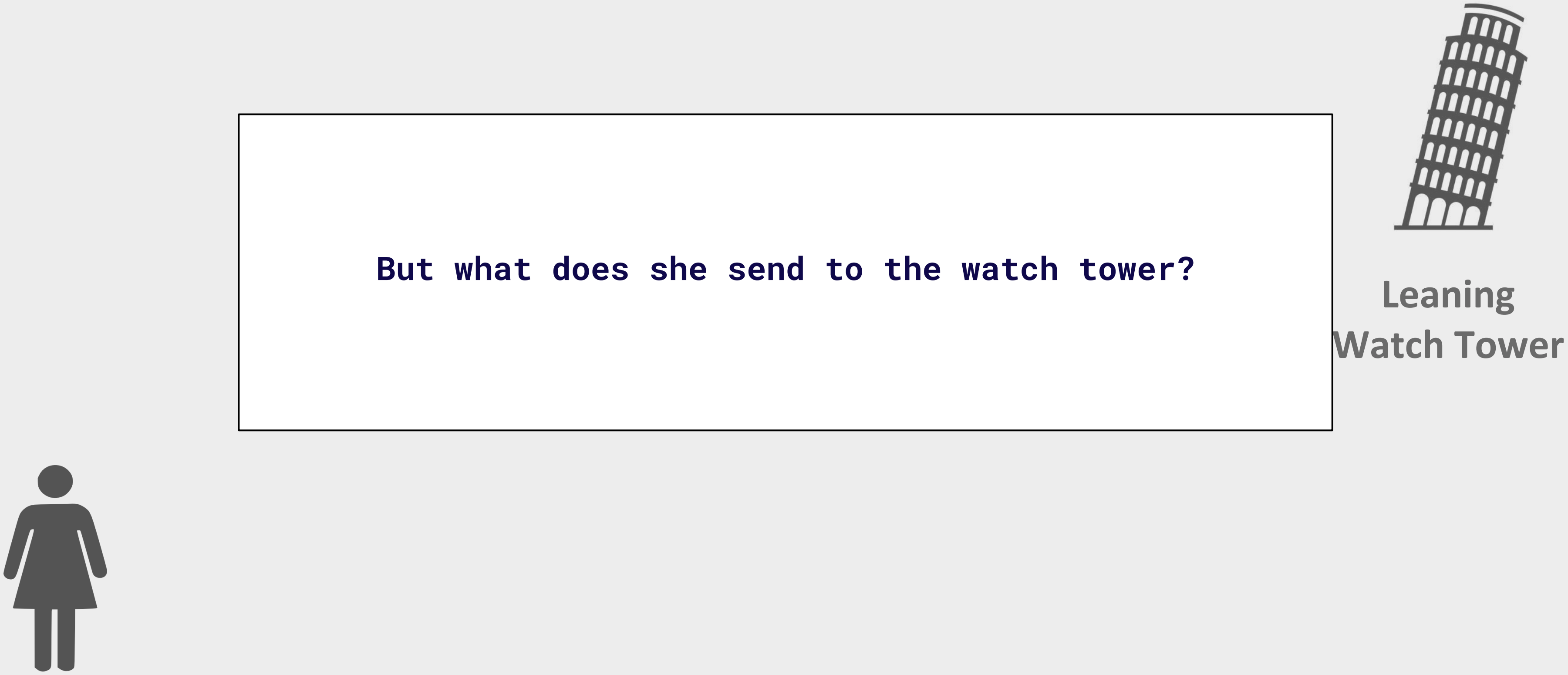


Watching Network

Monitor (Tadge) @ Scaling Bitcoin ‘16

Leaning
Watch Tower

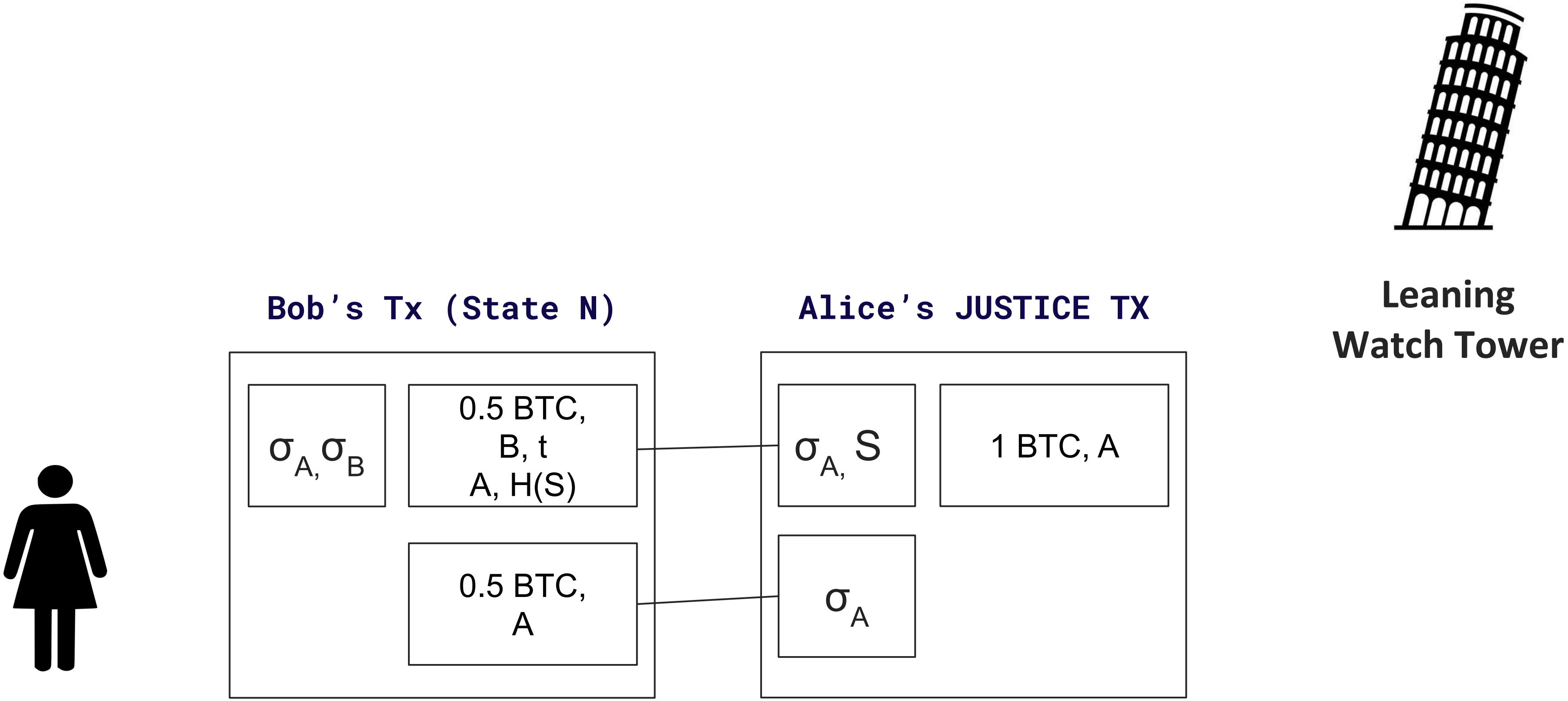
Monitor (Tadge) @ Scaling Bitcoin ‘16



But what does she send to the watch tower?

Leaning Watch Tower

Monitor (Tadge) @ Scaling Bitcoin ‘16



Leaning Watch Tower

Bob’s Tx (State N)

$\sigma_{A,}\sigma_B$

0.5 BTC,
B, t
A, H(S)

0.5 BTC,
A

Alice’s JUSTICE TX

$\sigma_{A,}$ S

1 BTC, A

σ_A

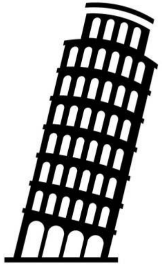
Monitor (Tadge) @ Scaling Bitcoin ‘16

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 Watch Tower

Bob’s TX (State N)

TXID [32 bytes]

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

4410c8d14ff9f87ceeed1d65cb58e7c7b2422b2d7529afc675208ce2ce09ed7d

TxLocator

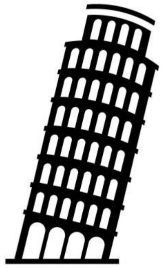
Encryption Key

Monitor (Tadge) @ Scaling Bitcoin ‘16

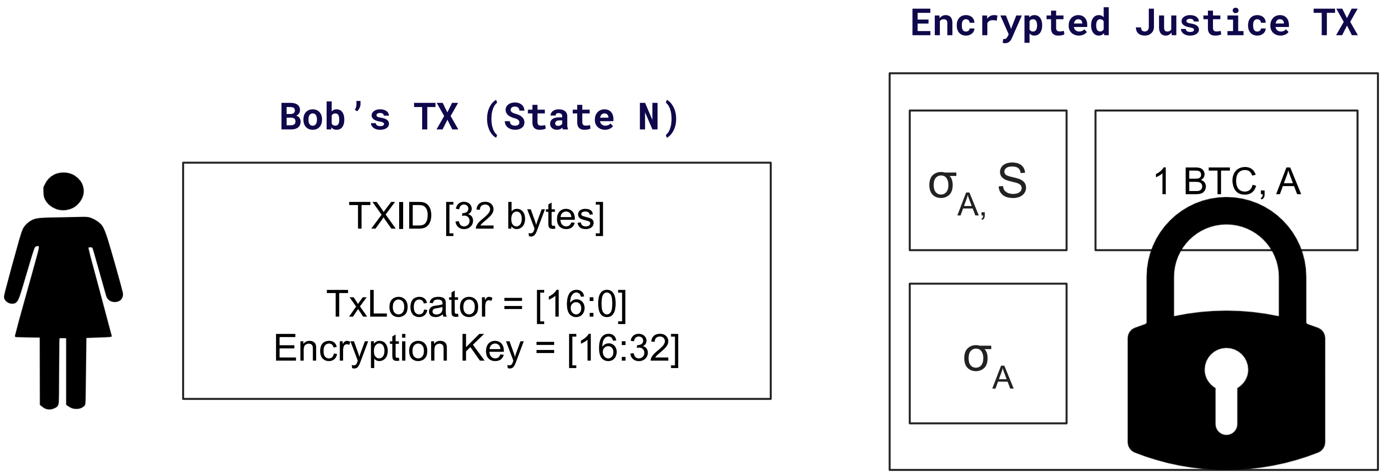
Encrypted Justice Transaction

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
Watch Tower**



Encrypted Justice TX

Bob’s TX (State N)

TXID [32 bytes]

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

$\sigma_{A,}$ S

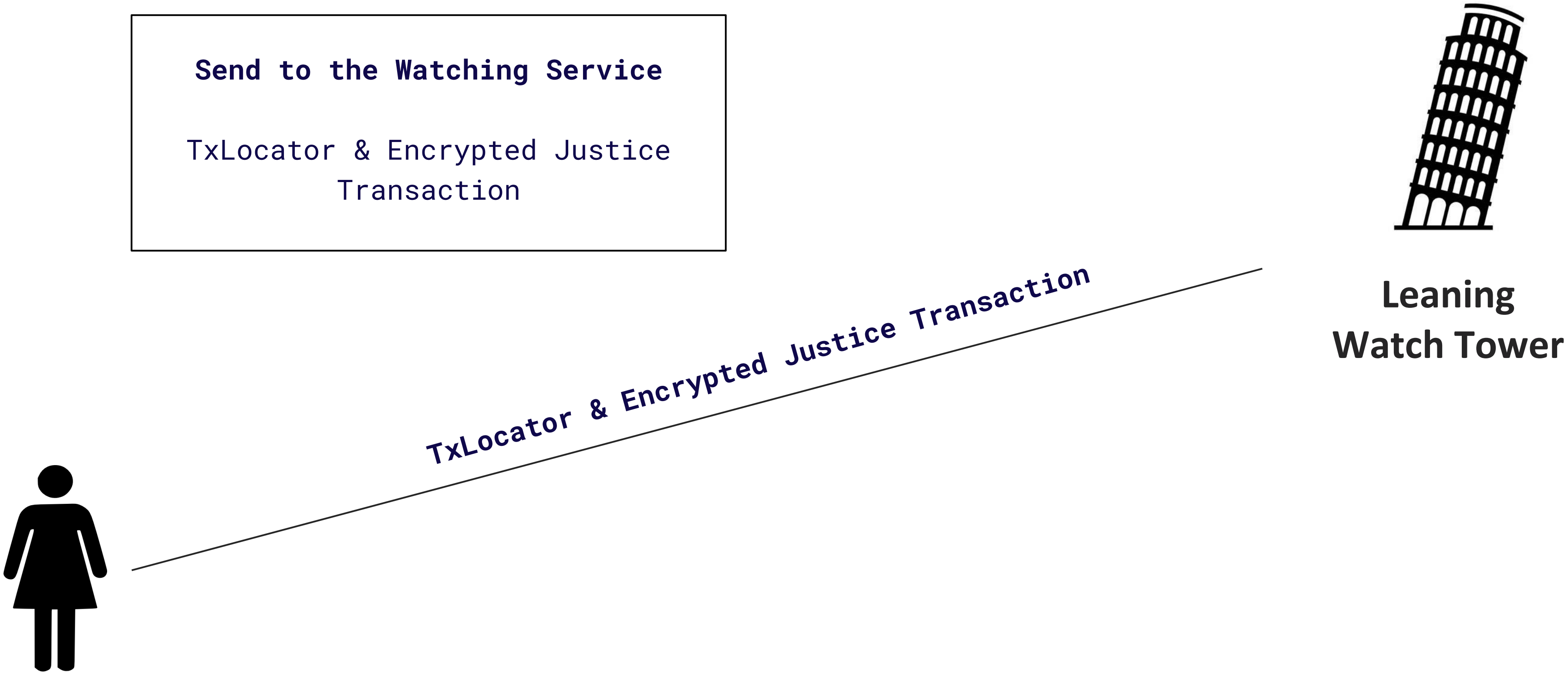
1 BTC, A

σ_A

Monitor (Tadge) @ Scaling Bitcoin ‘16

Send to the Watching Service

TxLocator & Encrypted Justice Transaction



TxLocator & Encrypted Justice Transaction

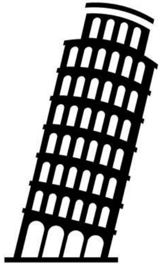
Leaning Watch Tower

Monitor (Tadge) @ Scaling Bitcoin ‘16

Leaning Watch Tower

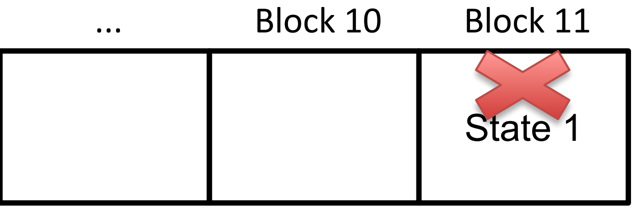
```
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice
```

Monitor (Tadge) @ Scaling Bitcoin ‘16



Leaning Watch Tower

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



...

Block 10

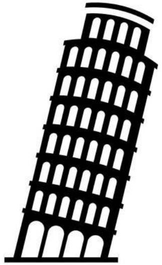
Block 11

State 1

Monitor (Tadge) @ Scaling Bitcoin ‘16

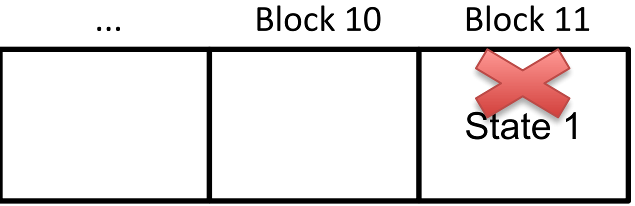
Watching Service – 5 Steps

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



Leaning Watch Tower

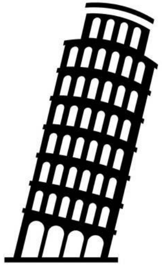
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice



Monitor (Tadge) @ Scaling Bitcoin ‘16

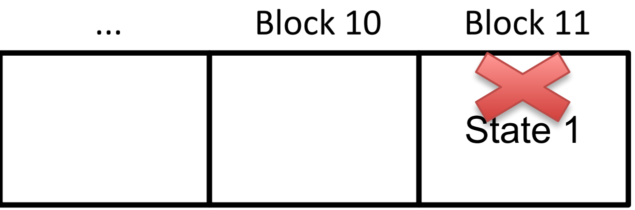
Watching Service – 5 Steps

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

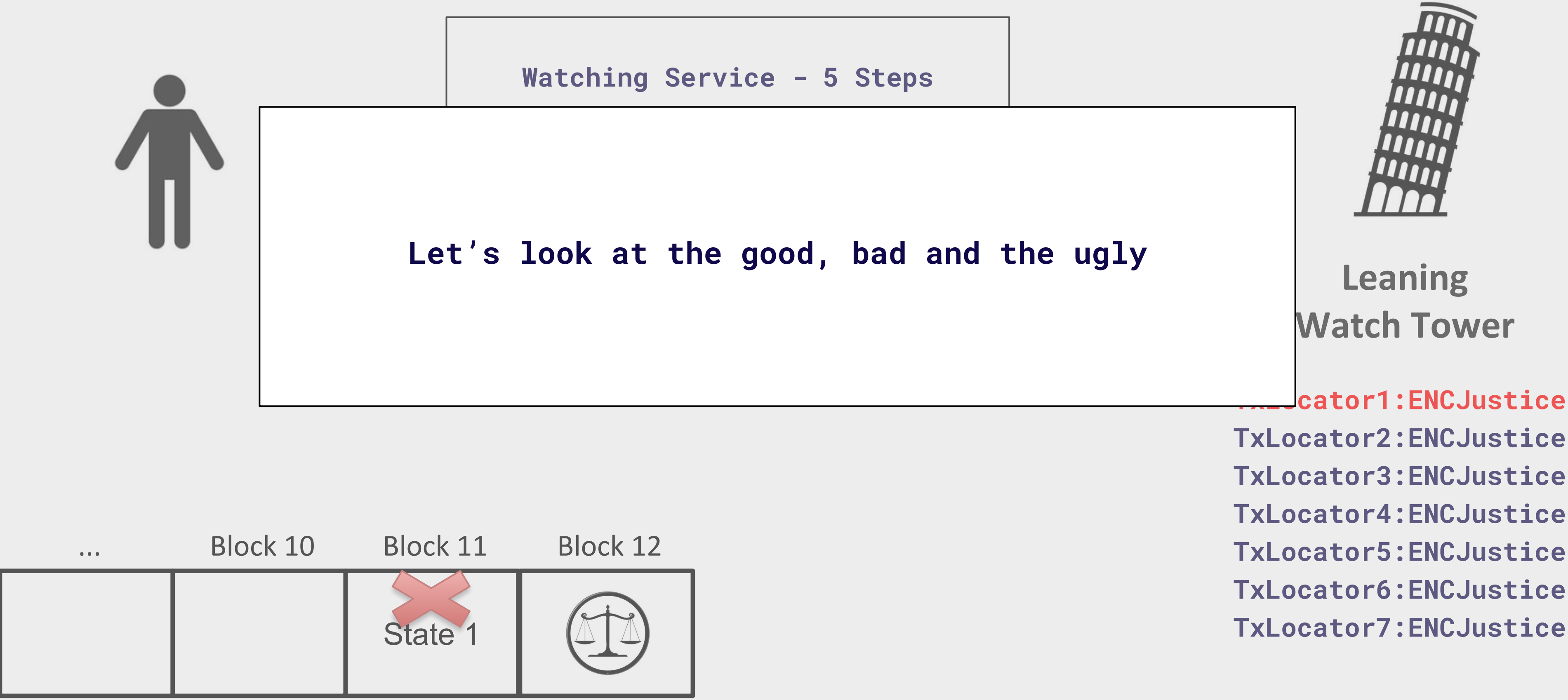


Leaning Watch Tower

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 Watch Tower

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

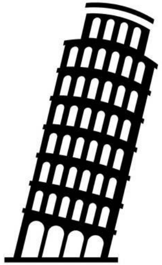
Monitor - THE GOOD

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 Watch Tower

Simple Protocol

Just store encrypted blob and watch blockchain to retrieve decryption key

Monitor - THE GOOD, BAD

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

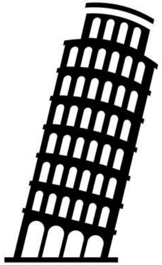
We CANNOT trigger any disputes! Only respond if the counterparty tries to cheat.

Congestion BIG problem

Watching service only has a pre-signed transaction and very very awkward to bump fees

Simple Protocol

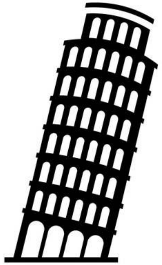
Just store encrypted blob and watch blockchain to retrieve decryption key



Leaning Watch Tower

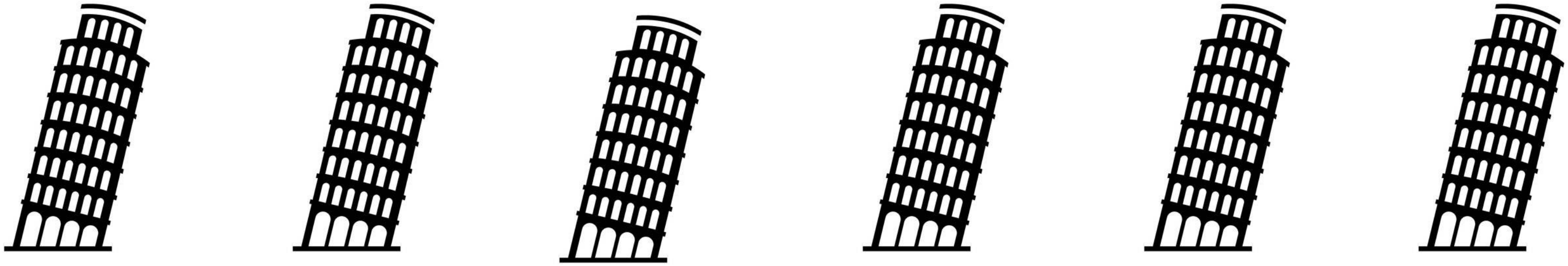
Monitor - THE GOOD, BAD, AND THE UGLY

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 Watch Tower

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



Leaning Watch Tower

Leaning Watch Tower

Leaning Watch Tower

Leaning Watch Tower

Leaning Watch Tower

Leaning Watch Tower

Hire multiple watch towers

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

Reward Policy?

Only the one watch tower who gets their respective justice tx in the blockchain **will get rewarded.**

WatchTower @ BPASE’18

$\sigma_{A,}\ \sigma_{B}$, **i***

Signatures

State version

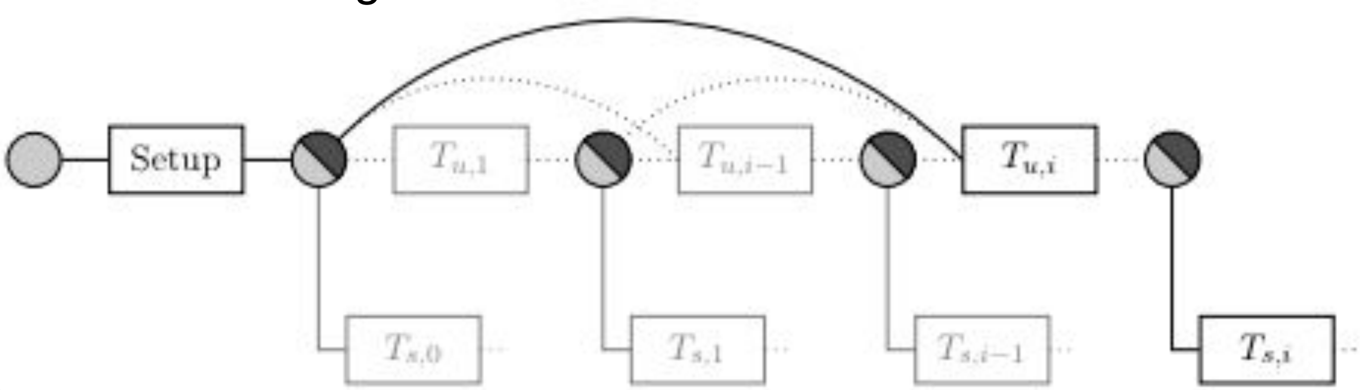
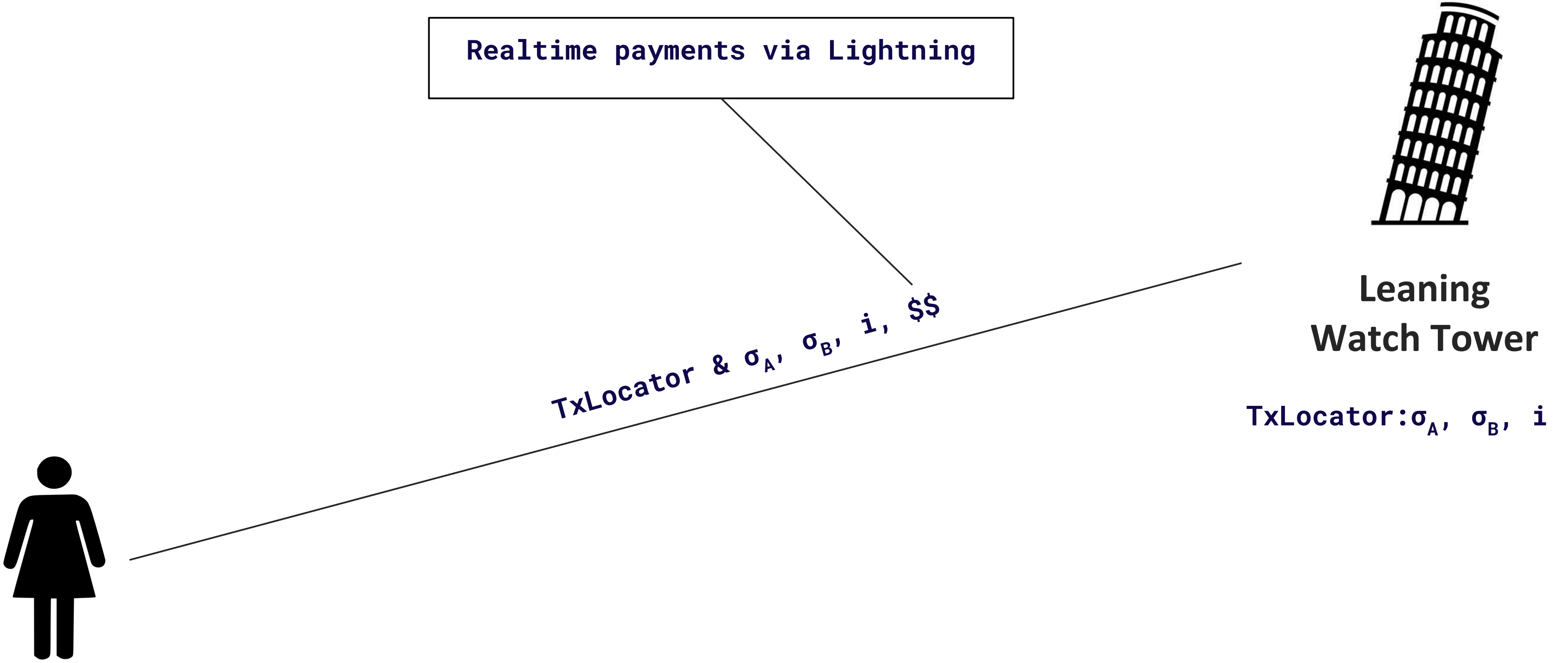


Figure 5: Overview of the off-chain protocol.

Leaning Watch Tower

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

WatchTower @ BPASE’18



Realtime payments via Lightning

TxLocator & σ_A, σ_B, i, \$\$

Leaning
Watch Tower

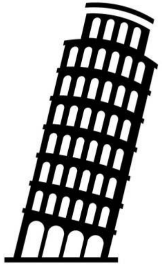
TxLocator:σ_A, σ_B, i

*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

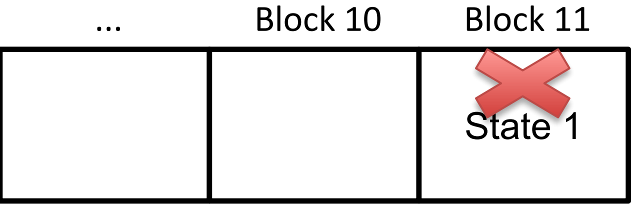
Watching Service - 5 Steps

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



Leaning Watch Tower

TxLocator:σ_A, σ_B, i



...

Block 10

Block 11

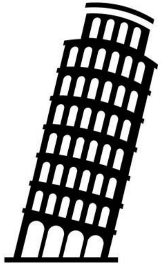
State 1

WatchTower @ BPASE’18

Watching Service - 5 Steps

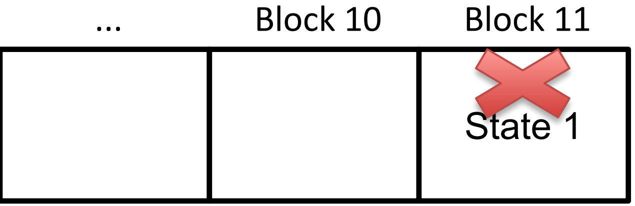
1. Extract Transaction ID
2. Look up the latest “i” received
3. Broadcast it!

σ_A, σ_B, i



Leaning Watch Tower

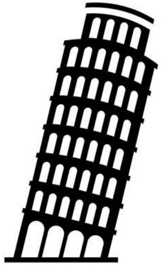
TxLocator:σ_A, σ_B, i



WatchTower @ BPASE’18

Watching Service - 5 Steps

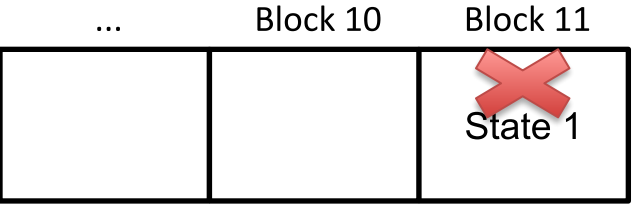
1. Extract Transaction ID
2. Look up the latest “i” received
3. Broadcast it!



Leaning Watch Tower

TxLocator:σ_A, σ_B, i

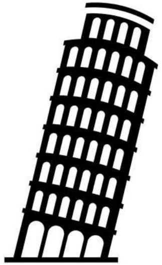
σ_A, σ_B, i



WatchTower @ BPASE’18

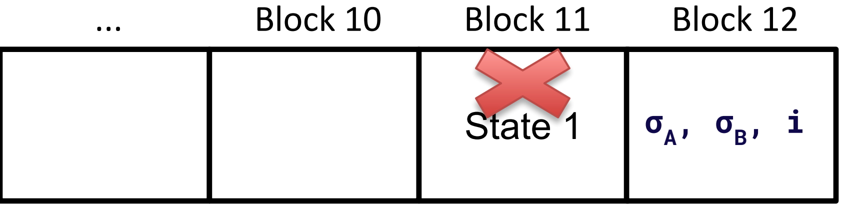
Watching Service - 5 Steps

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



Leaning Watch Tower

TxLocator:σ_A, σ_B, i



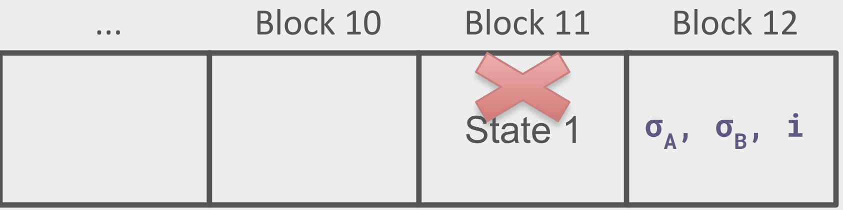
WatchTower @ BPASE’18

Watching Service - 5 Steps

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

Leaning Watch Tower

TxLocator:σ_A, σ_B, i



Watch Tower - THE GOOD

Verifiable Job

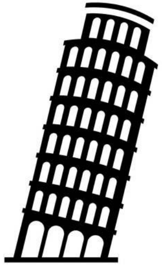
No longer store junk. We know it is a useful job.

Separates TX + State

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

O(1) Storage

Only store the job with the largest version.



Leaning Watch Tower

Watch Tower - THE GOOD, BAD

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

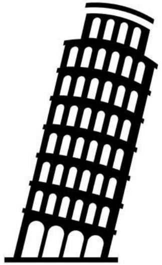
O(1) Storage

Only store the job with the largest version.

Leaning Watch Tower

Watch Tower - 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 watch tower.



Leaning Watch Tower

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 Watch Tower

Monitor-style Jobs

TxLocator +
Encrypted TX

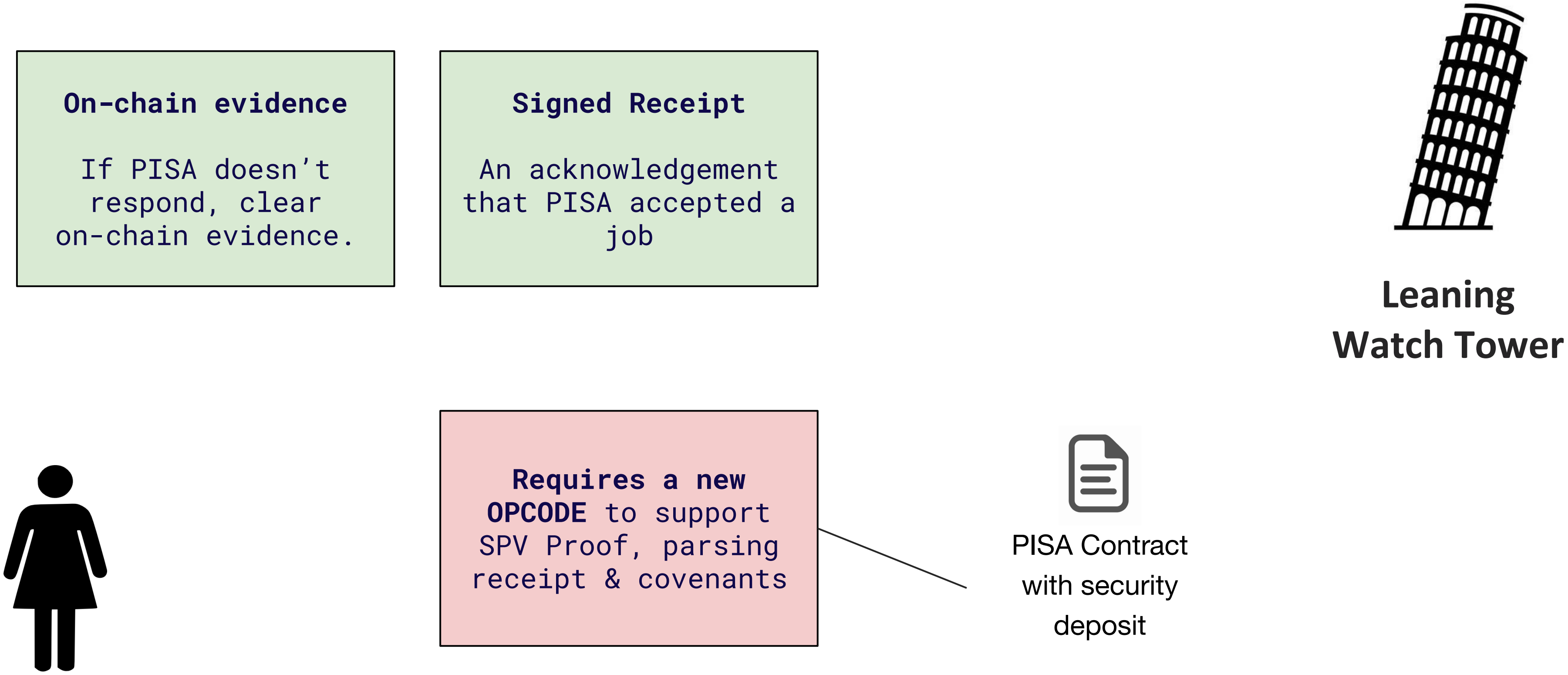
Eltoo-style Jobs

TxLocator &
Authorised State
Version

Outpost-style Jobs

TxLocator +
Decryption Key
(Find out later)

PISA @ Scaling Bitcoin ‘19



On-chain evidence

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

Signed Receipt

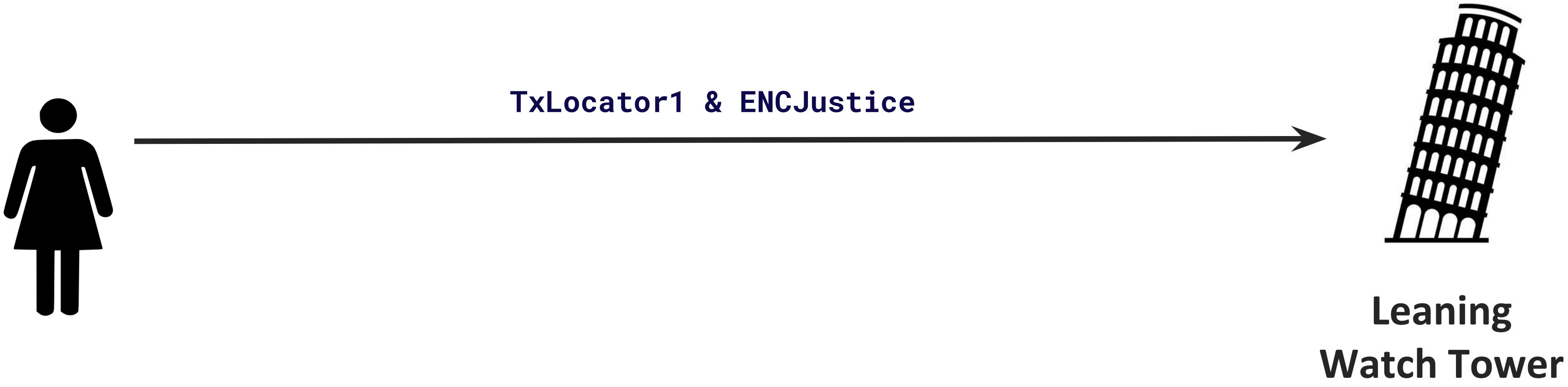
An acknowledgement that PISA accepted a job

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

PISA Contract with security deposit

Leaning Watch Tower

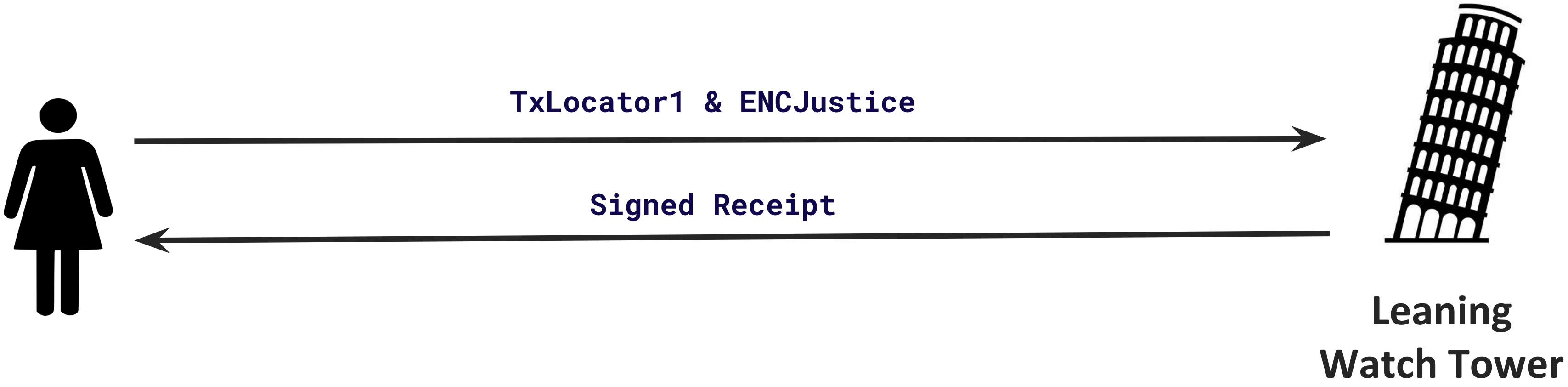
PISA (Monitor) @ Scaling Bitcoin ‘19



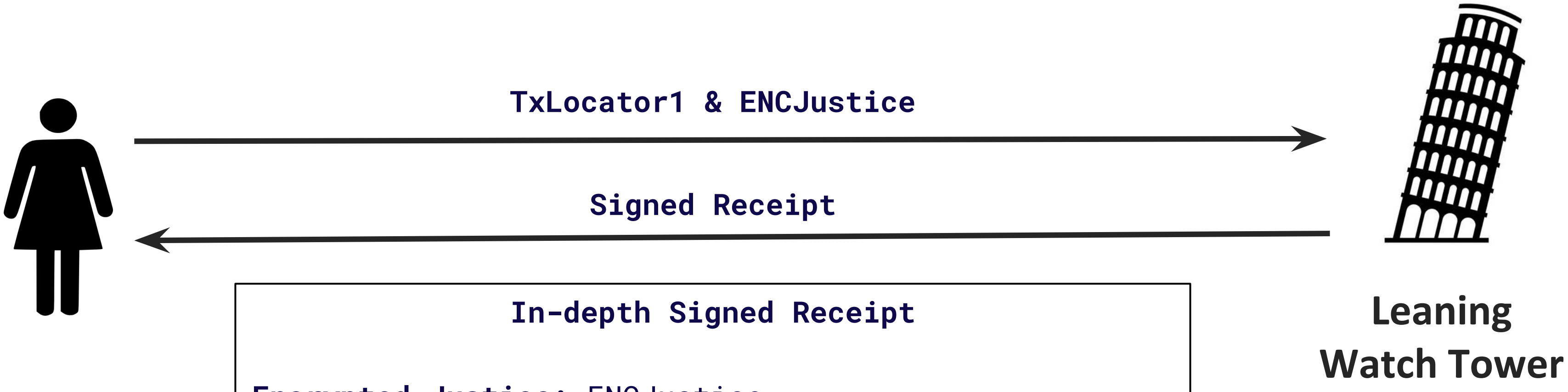
`TxLocator1 & ENCJustice`

Leaning
Watch Tower

PISA (Monitor) @ Scaling Bitcoin '19



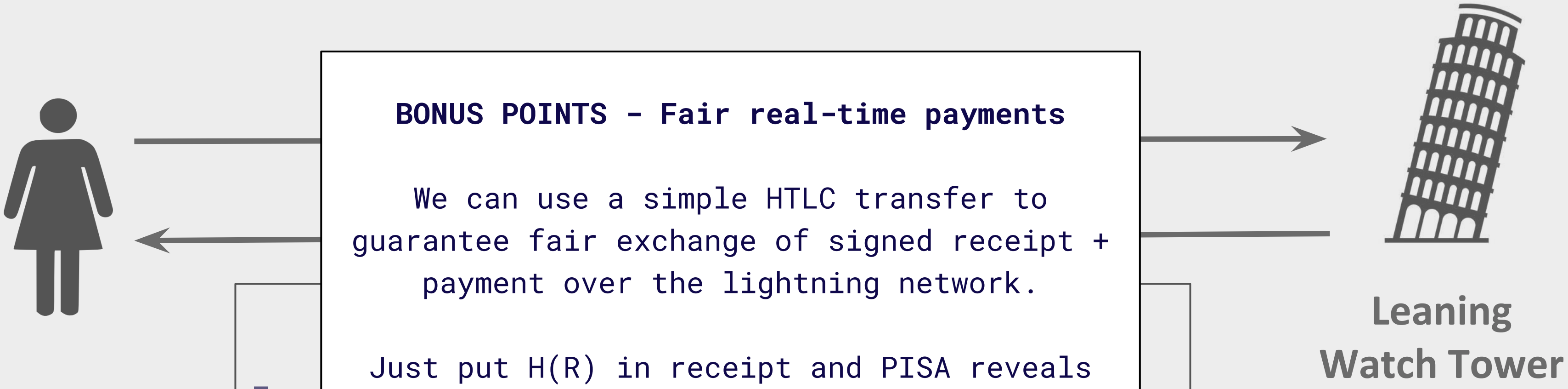
PISA (Monitor) @ Scaling Bitcoin ‘19



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



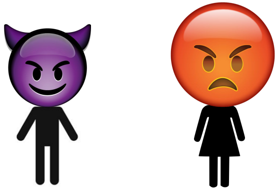
BONUS POINTS - Fair real-time payments

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.

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

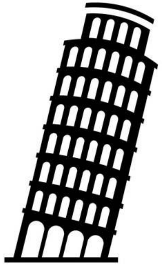
Monitor (Tadge) @ Scaling Bitcoin ‘16



Scenario

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

How can Alice prove wrongdoing?

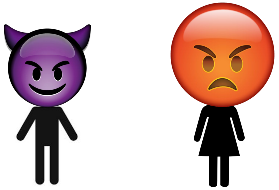


Leaning Watch Tower

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

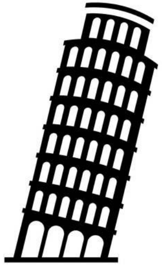
...	Block 10	Block 11	...	...	Block 110
		~~State 1~~			Bob wins

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}

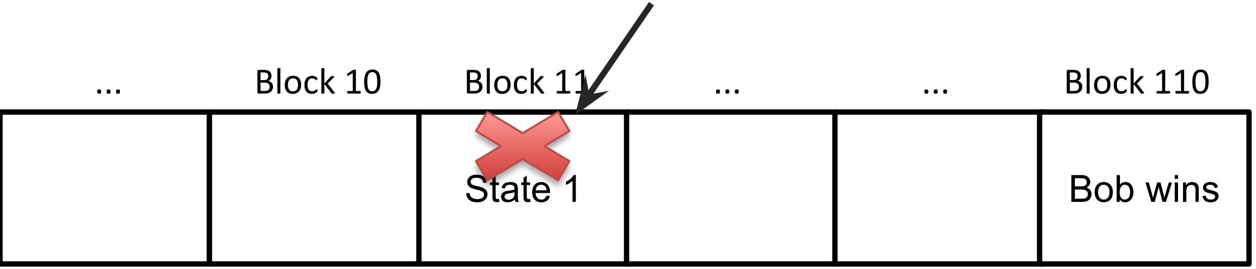


Leaning Watch Tower

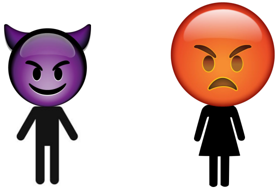
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice

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

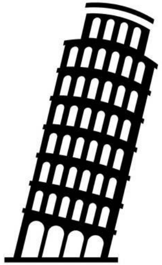


Monitor (Tadge) @ Scaling Bitcoin ‘16



In-depth Signed Receipt

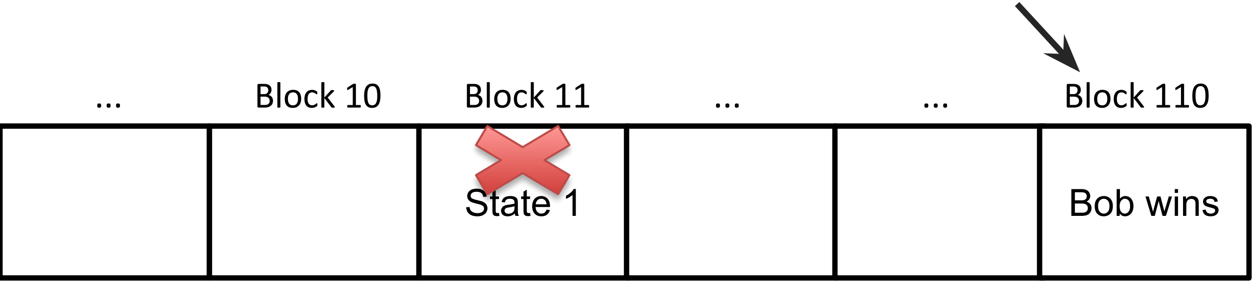
Encrypted Justice: ENCJustice
Transaction Locator: TxLocator1
Appointment Start: Block 10
Appointment Expiry: Block 500
Minimum Dispute Period: 50 blocks
Signature by PISA: σ_{PISA}



Leaning Watch Tower

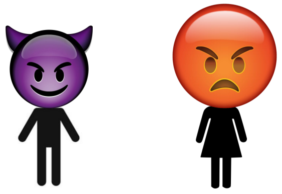
Anyone can decrypt ENCJustice and verify:

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



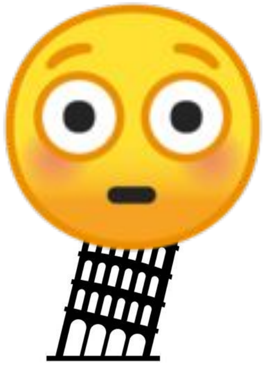
TxLocator1:ENCJustice
TxLocator2:ENCJustice
TxLocator3:ENCJustice
TxLocator4:ENCJustice
TxLocator5:ENCJustice
TxLocator6:ENCJustice
TxLocator7:ENCJustice

Monitor (Tadge) @ Scaling Bitcoin ‘16



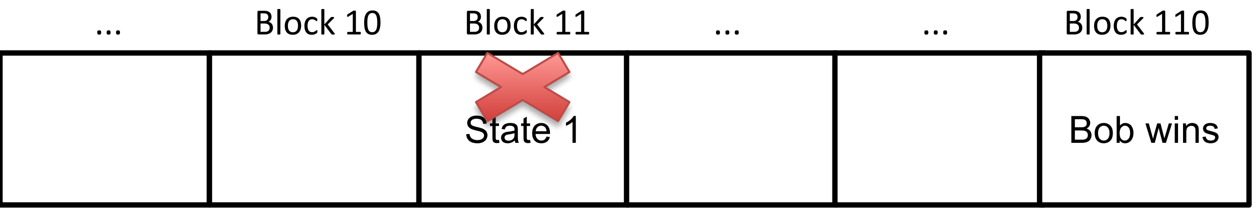
Reputational Accountability, not Financial
Publicly verifiable that PISA accepted the job and failed to do its duty by the customer.

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

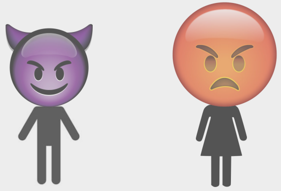


Leaning
Watch Tower

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



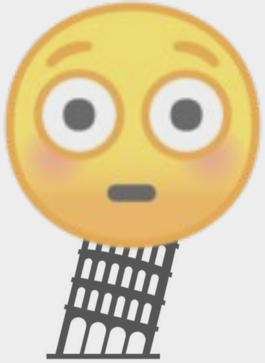
Monitor (Tadge) @ Scaling Bitcoin ‘16



Reputational Accountability, not Financial

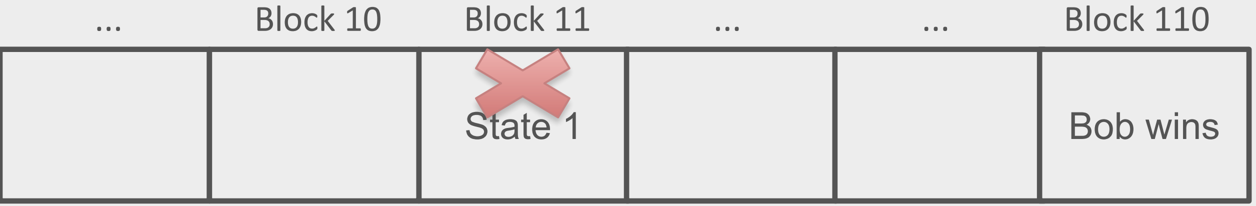
Publicly verifiable that PISA accepted the job and

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



Leaning Watch Tower

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



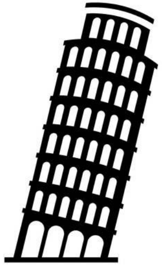
PISA - THE GOOD

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 Watch Tower

Simple Protocol

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

PISA - THE GOOD, BAD

Channel-Privacy

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

O(1) OR O(N) Storage

Depends on the underlying channel construction (or if ENCJustice is stored on-chain via OUTPOST)

Accountability

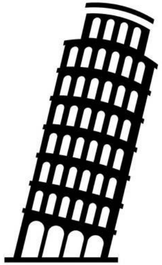
We can prove to anyone that a PISA-tower cheated.

Security Deposit hard

While there is “skin in the game”, it may be under-collateralised. Provisions (2015) can help.

Simple Protocol

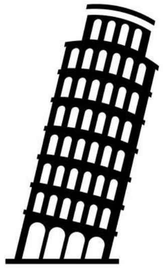
Adopting a signed receipt for different channel constructions is relatively straight-forward.



Leaning Watch Tower

PISA - THE GOOD, BAD, AND THE UGLY

Channel-Privacy By re-using the Monitor protocol, PISA doesn’t know what channel is being watched!	**O(1) OR O(N) Storage** Depends on the underlying channel construction (or if ENCJustice is stored on-chain via OUTPOST)	**Accountability** We can prove to anyone that a PISA-tower cheated.
Security Deposit hard While there is “skin in the game”, it may be under-collateralised. Provisions (2015) can help.	**Simple Protocol** Adopting a signed receipt for different channel constructions is relatively straight-forward.	**Consensus Upgrade** We need a new OP_CODE for the slashing condition. Very likely, will not get into Bitcoin soon.



Leaning Watch Tower

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)

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.

TX + State Intertwined == bumping fee is HARD

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

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.

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 - WHERE ARE WE NOW?

PRIVATE TEST

Thanks to a heroic effort by Sergi Delgado (speaker yesterday), we have a working basic PISA implementation.

Do you want to try out our watch tower?

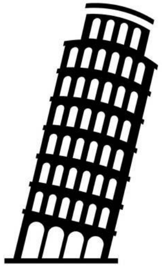
Please contact us!

Signed Receipt BOLT
Coming soon to a wallet near you!

(after guinea pigs try out our demo!)

Encrypted Justice: ENCJustice
Transaction Locator: TxLocator1
Appointment Start: Block 10
Appointment Expiry: Block 500
Minimum Dispute Period: 50 blocks
Cipher + Hash Function: AES-ACM & SHA256
Signature by PISA: σ_{PISA}

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.

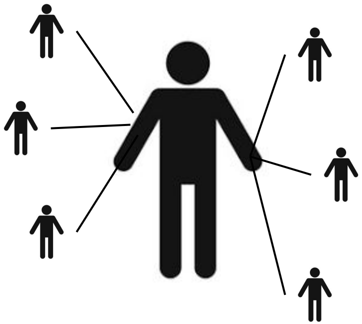
What can a watch tower do?

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

What can a watch tower NOT do?

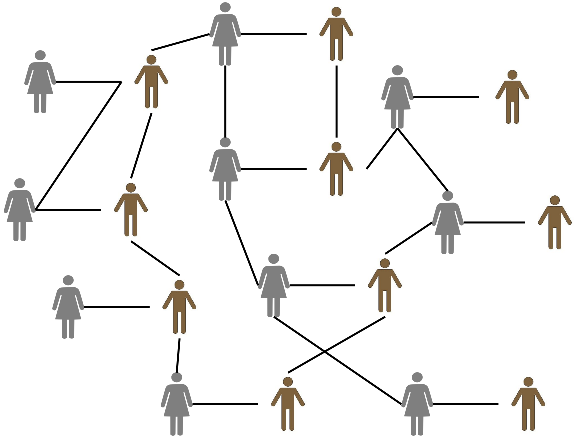
Protect hubs against insider threats, theft of signing keys, etc.

PISA - Final word about "watchers" and their emerging role



Payment channel hubs

Customers generally trust hubs (we see this today), but for hubs, all their coins are "effectively" in a hot wallet and **every customer is an adversary.**



Routing Nodes

Peers will open channels with anyone to search out popular routes / best fees. They WON'T know or trust their counterparty. So a watch tower is essential.

P/SA RESEARCH

STARKWARE

LIGHTNING

RAIDEN

L4

ARWEN

connext

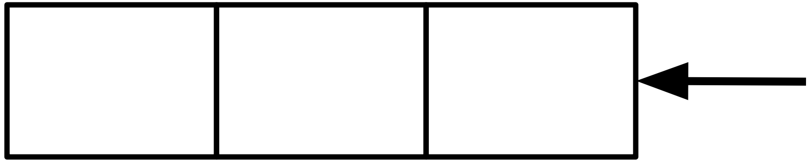
eclairmobile

Lightning Network Bitcoin wallet

Blockstream

LIQUIDITY·NETWORK

pg Plasma Group



Settlement System and Root of Trust of all Layer 2

https://pisa.watch

PisaResearch
paddypisa