

BOLT #13: Standardising WatchTowers

Sergi Delgado-Segura



PISA
RESEARCH

LIGHTNING TRANSACTIONS IN 1 MIN



commitment transactions

funding transaction

from: A	to: AB
---------	--------



LIGHTNING TRANSACTIONS IN 1 MIN



funding transaction



commitment transactions



**close
channel**

A thick black arrow pointing downwards from the stack of commitment transactions.

LIGHTNING TRANSACTIONS IN 1 MIN



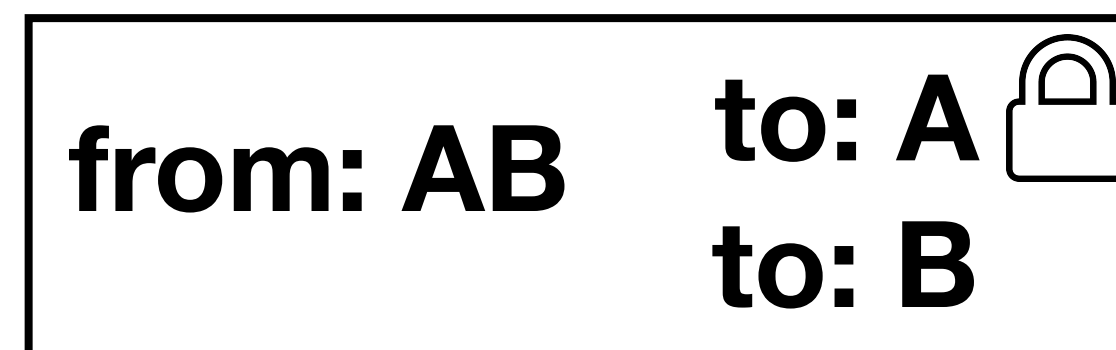
funding transaction



commitment transactions



**close
channel**



closing transaction

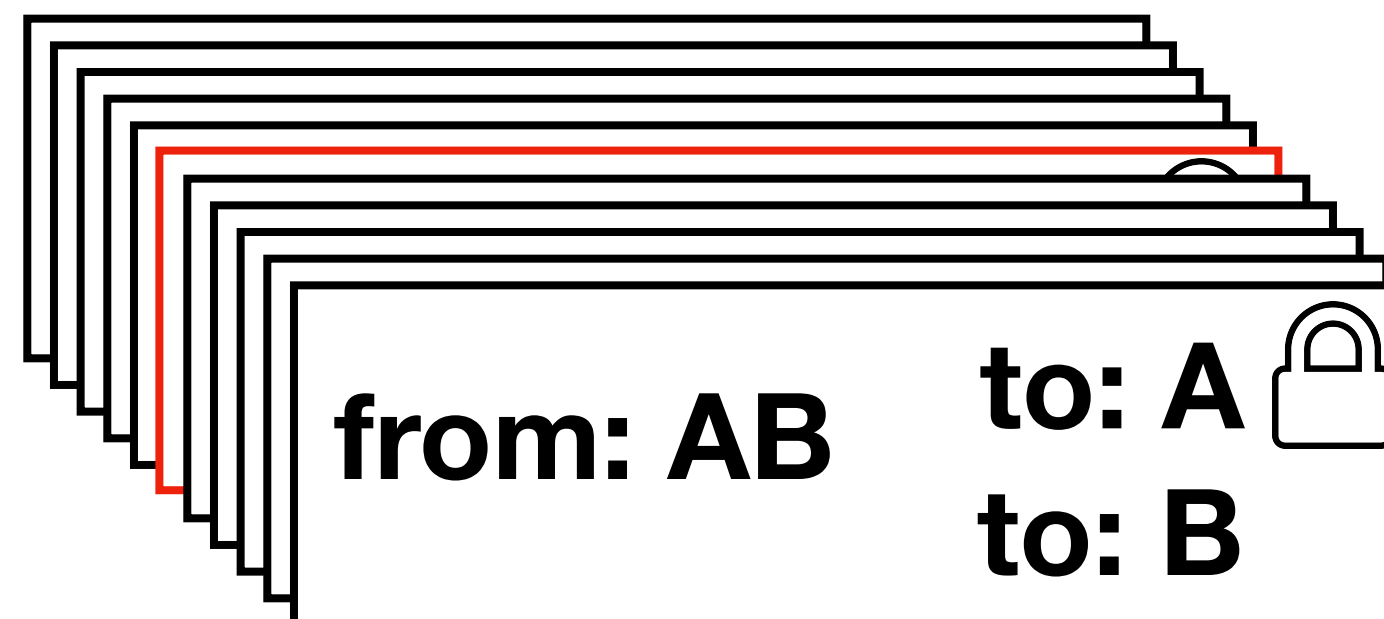
LIGHTNING TRANSACTIONS IN 1 MIN



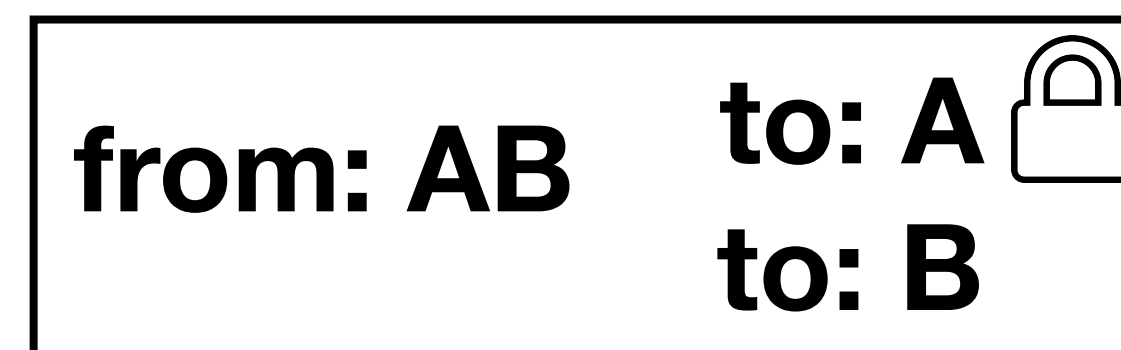
funding transaction



commitment transactions



**close
channel**

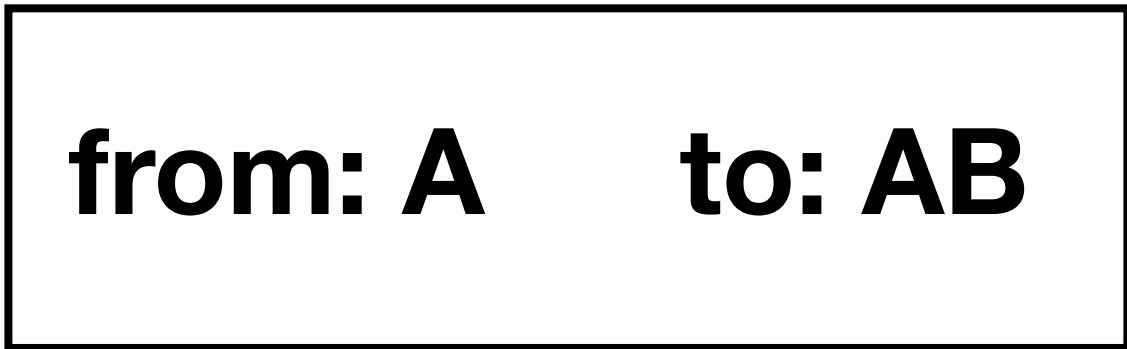


closing transaction

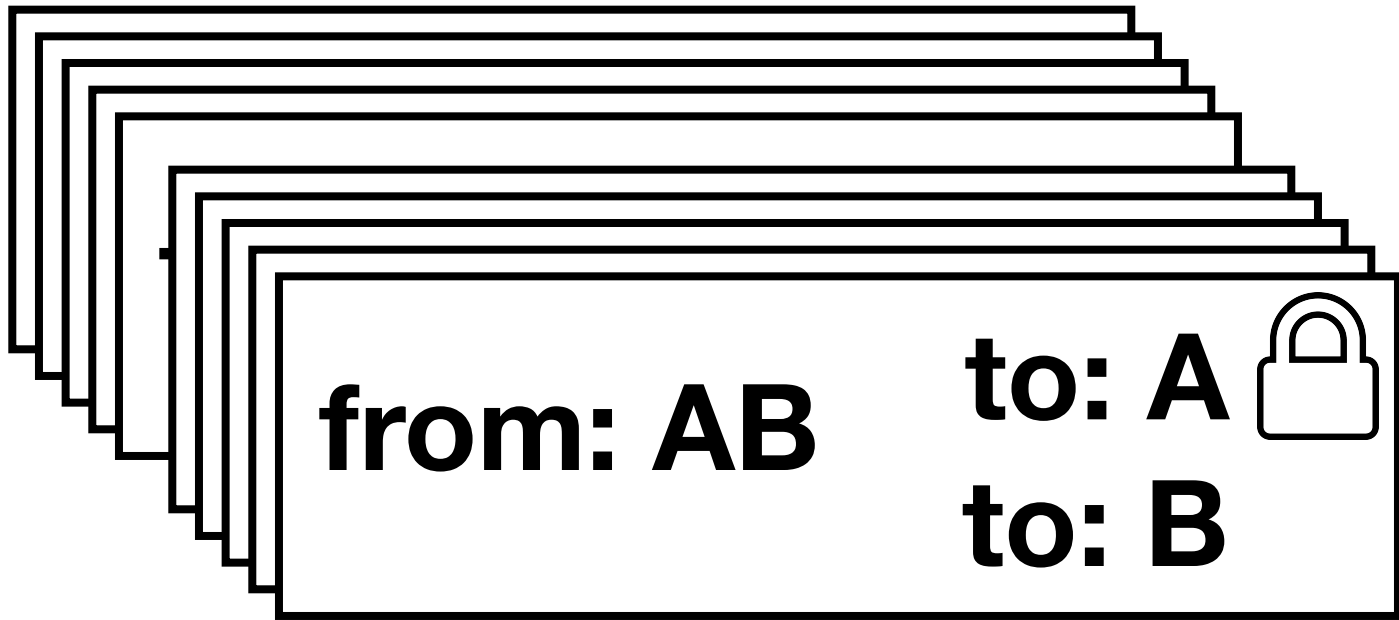
LIGHTNING TRANSACTIONS IN 1 MIN



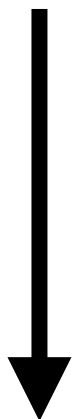
funding transaction



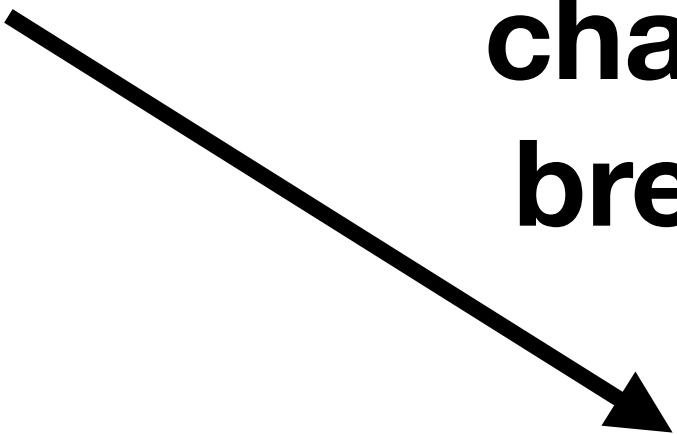
commitment transactions



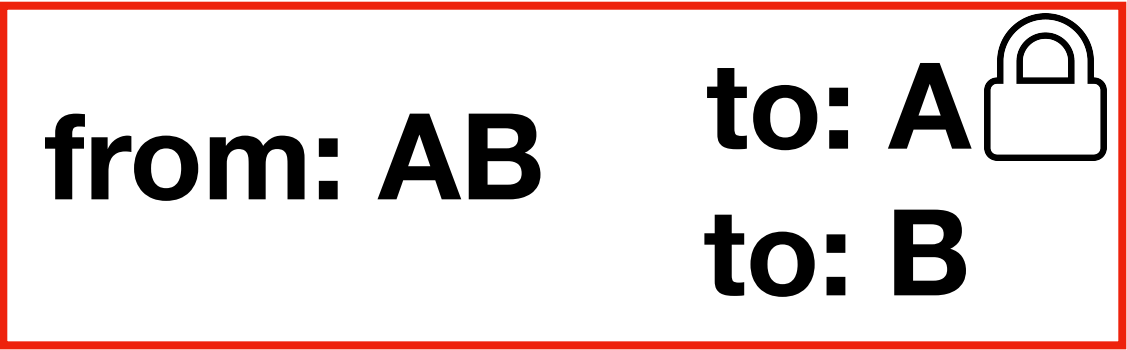
close
channel



channel
breach



closing transaction



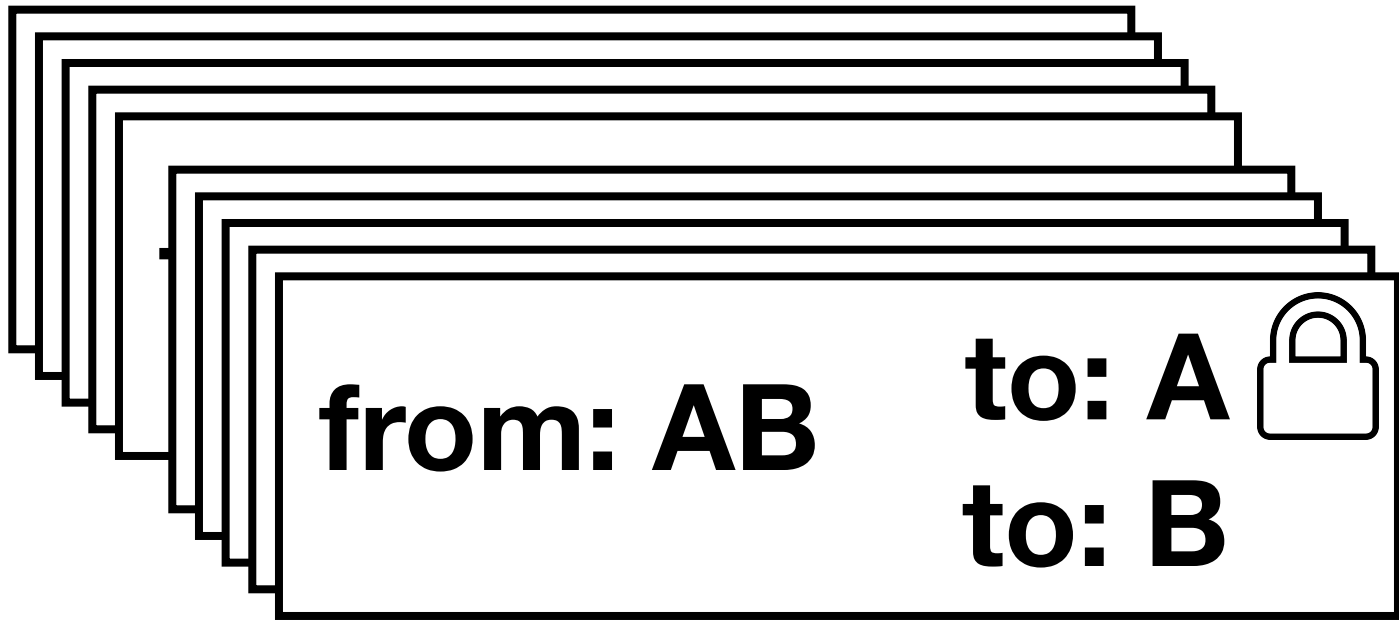
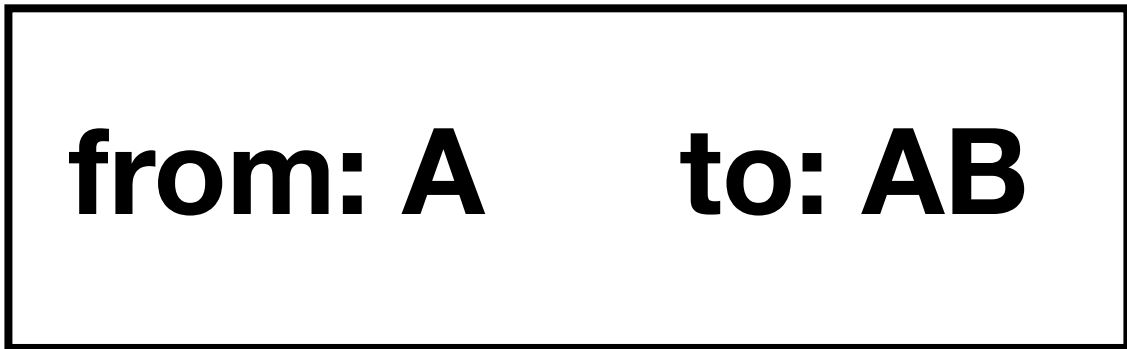
closing transaction

LIGHTNING TRANSACTIONS IN 1 MIN

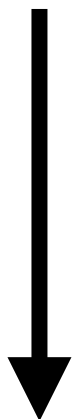


commitment transactions

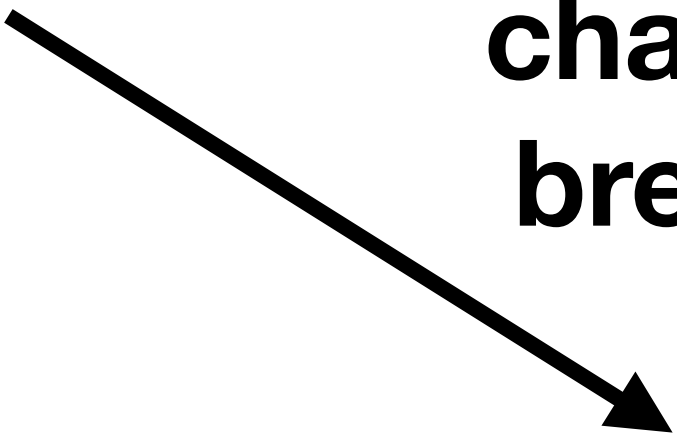
funding transaction



close
channel



channel
breach



closing transaction

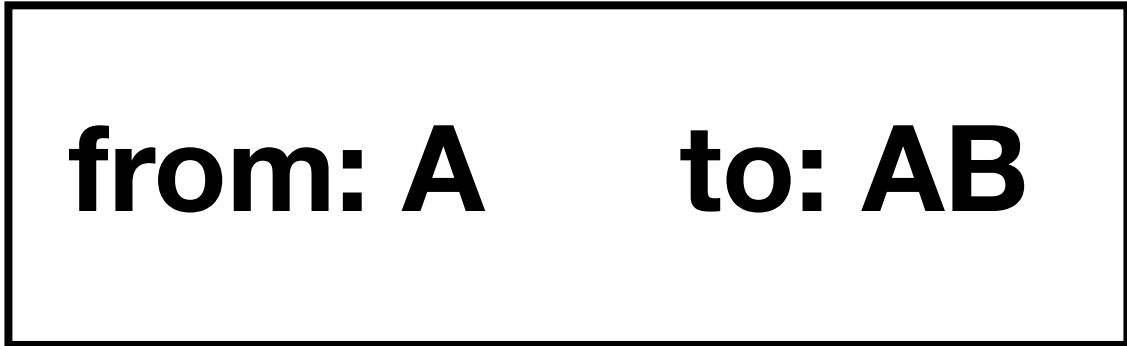


closing transaction

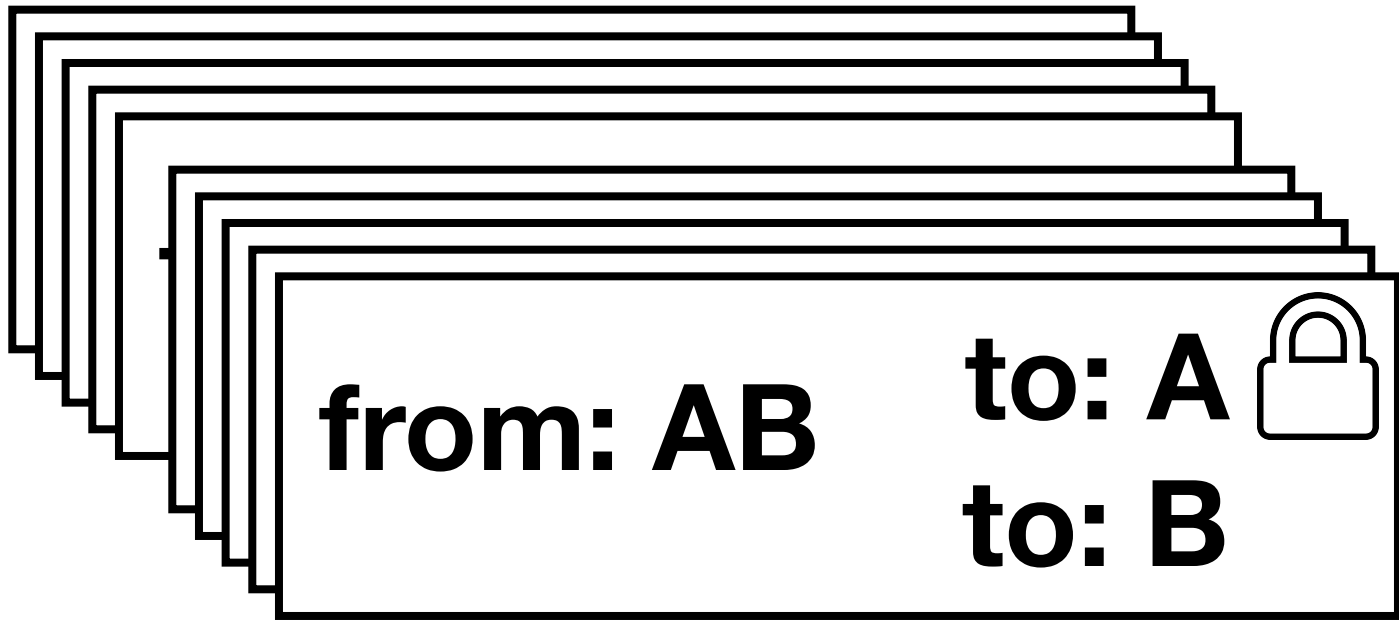
LIGHTNING TRANSACTIONS IN 1 MIN



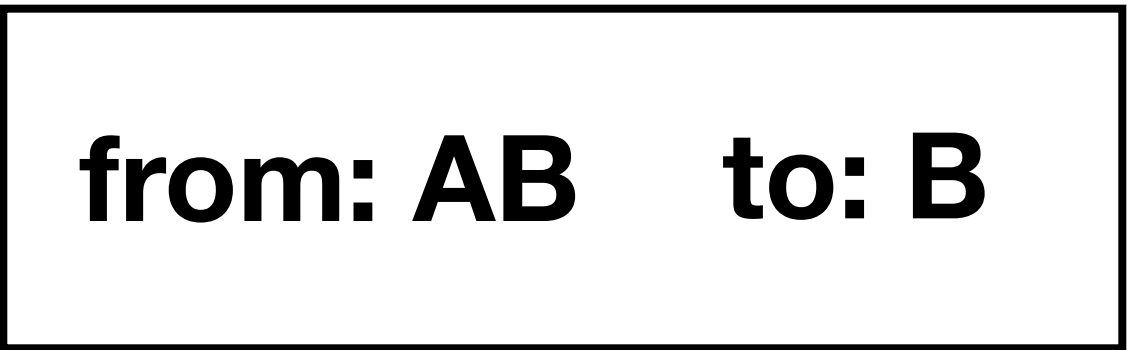
funding transaction



commitment transactions



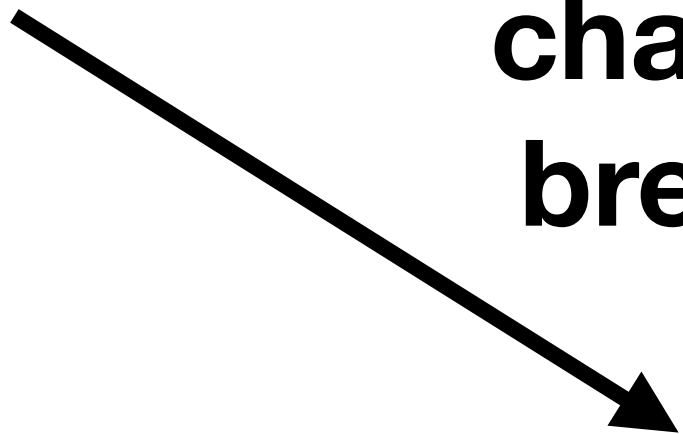
penalty transaction



**close
channel**



**channel
breach**



closing transaction



closing transaction



BASIC WATCHTOWER PROTOCOL



BASIC WATCHTOWER PROTOCOL





BASIC WATCHTOWER PROTOCOL



BASIC WATCHTOWER PROTOCOL





Patrick McCorry  @paddypisa · Jan 12

What should we call the bitcoin watchtower:

@sr_gi @lightning @LNconf


btc-watchtower


64.8%


pisa-watchtower


35.2%


142 votes · Final results

 6

 1

 5






74810b012346c9a6

@orionwl

Replying to @paddypisa @sr_gi and 2 others

the Eye of Satoshi 

11:28 AM · Jan 13, 2020 · [Twitter Web App](#)

1 Retweet

19 Likes

BASIC WATCHTOWER PROTOCOL



BASIC WATCHTOWER PROTOCOL



[...]
commitment_txid,
penalty_tx,
[...]



BASIC WATCHTOWER PROTOCOL



[...]
commitment_txid,
penalty_tx,
[...]



BASIC WATCHTOWER PROTOCOL

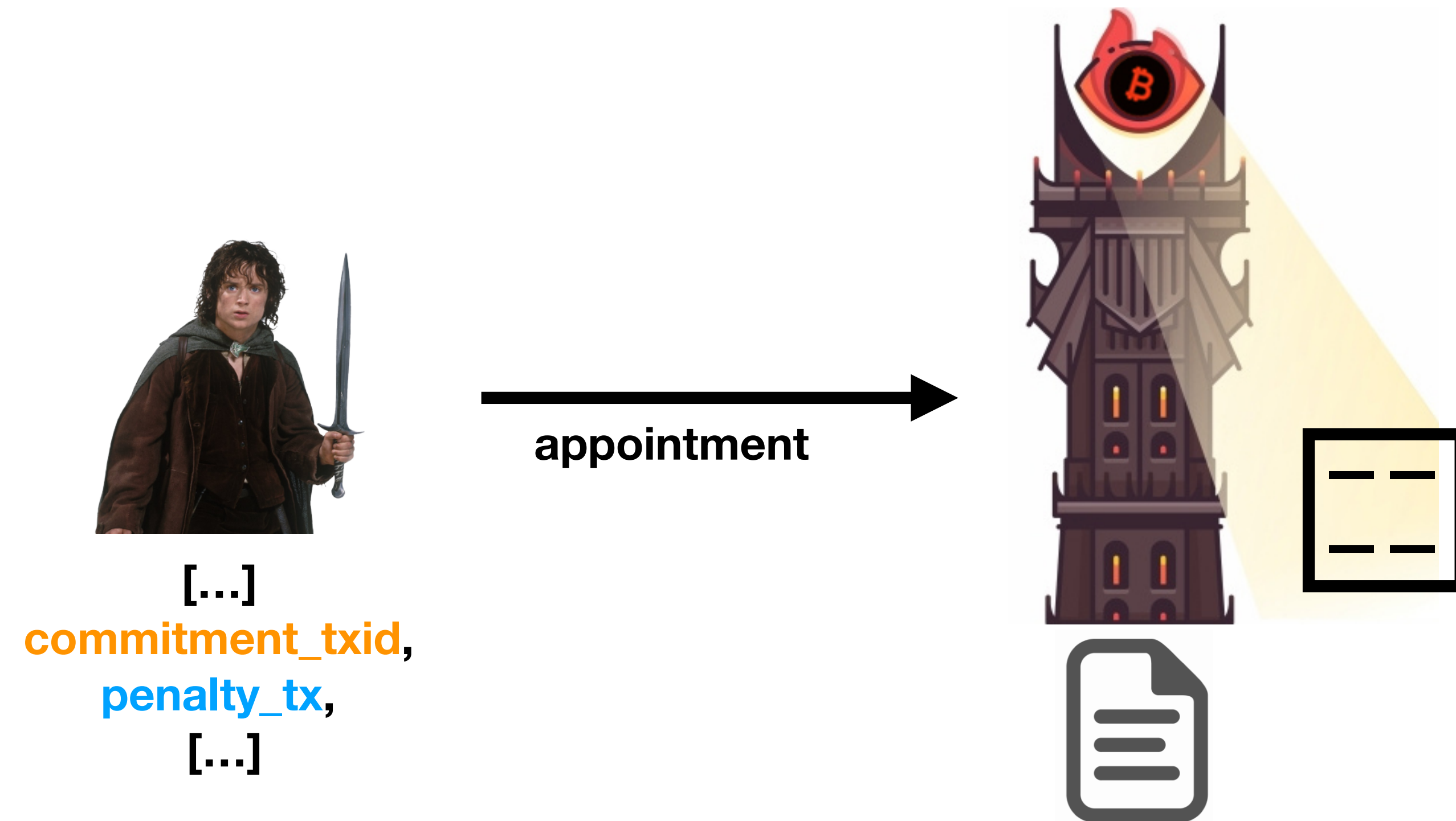


[...]
commitment_txid,
penalty_tx,
[...]

→
appointment



BASIC WATCHTOWER PROTOCOL



BASIC WATCHTOWER PROTOCOL

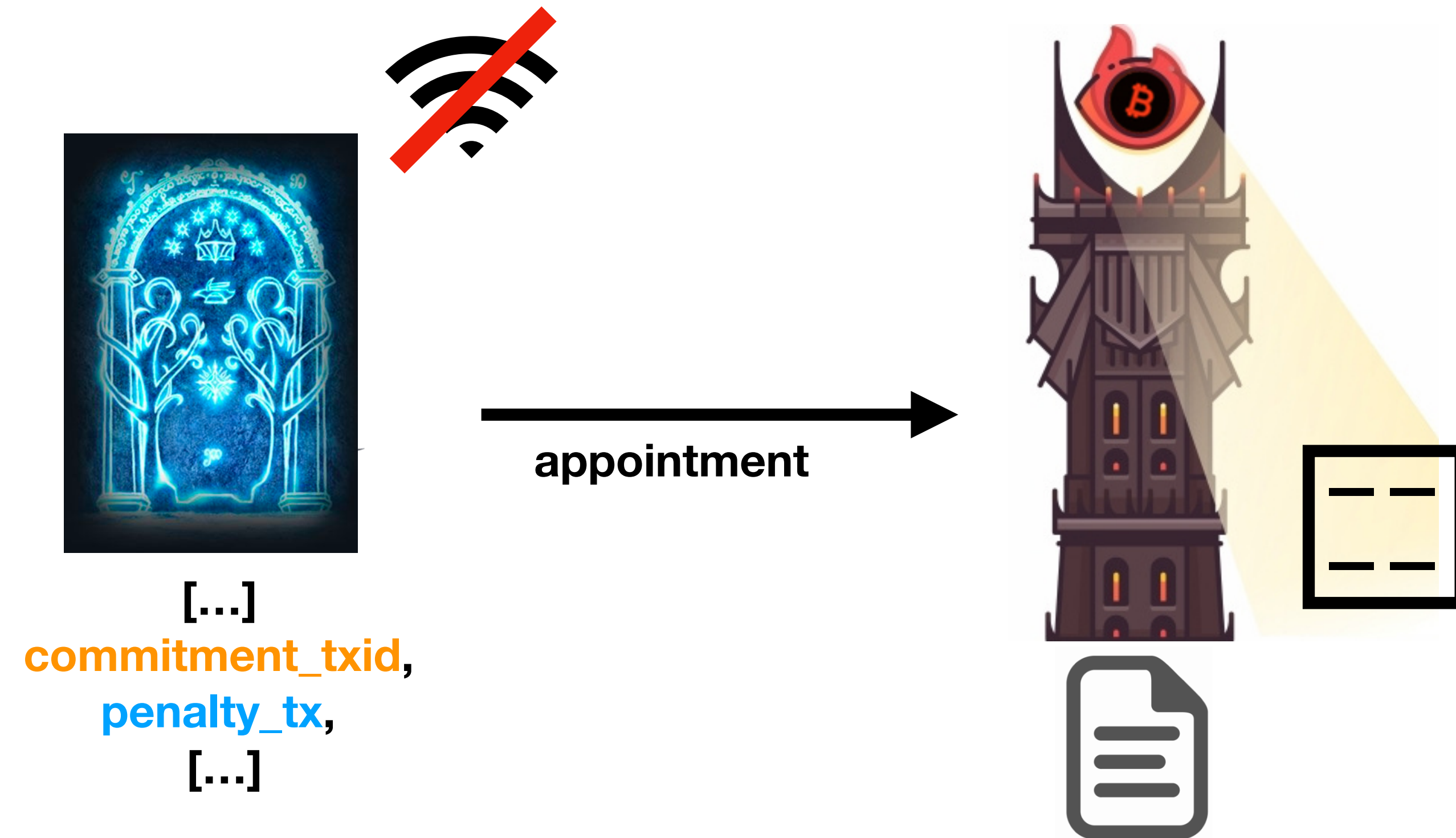


[...]
commitment_txid,
penalty_tx,
[...]

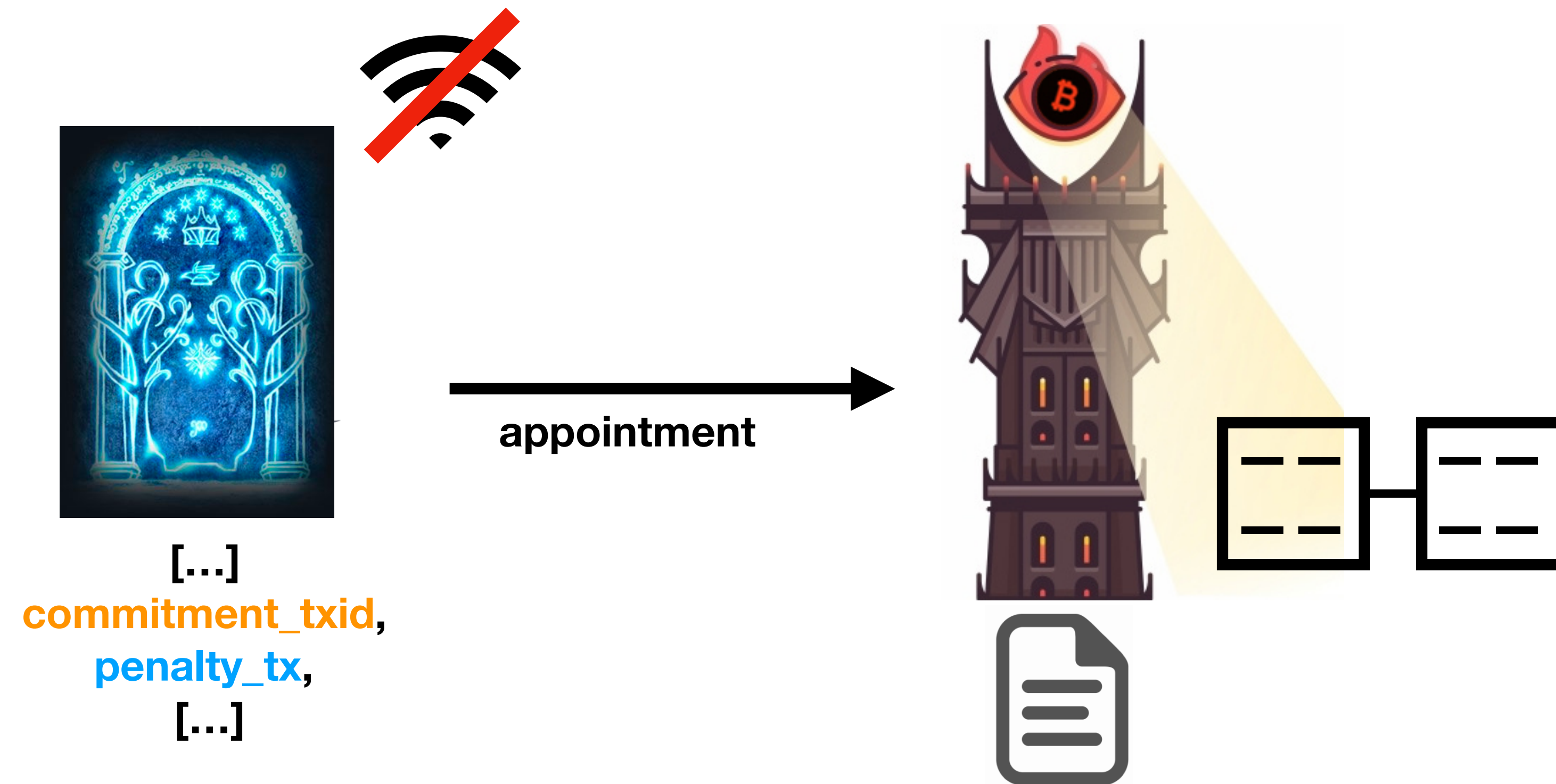
→
appointment



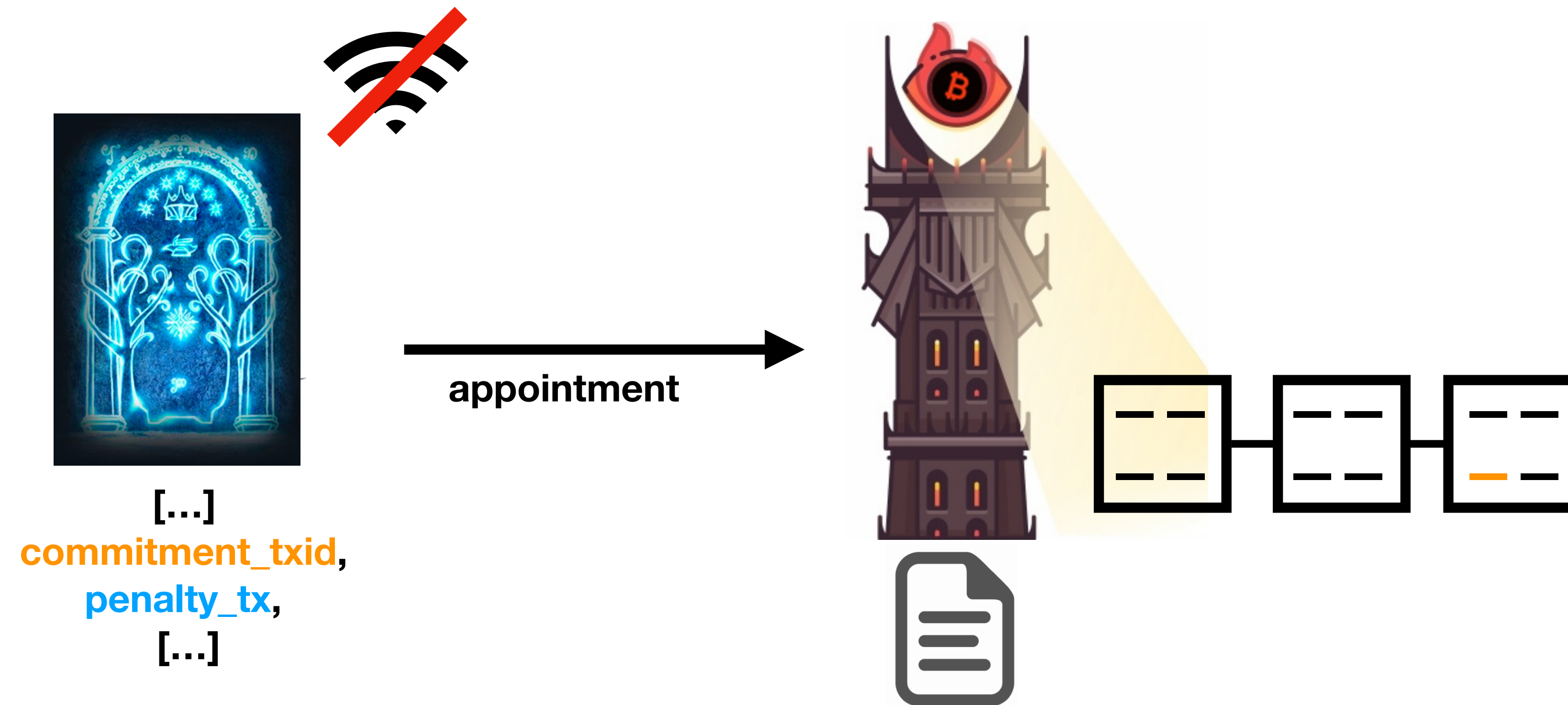
BASIC WATCHTOWER PROTOCOL



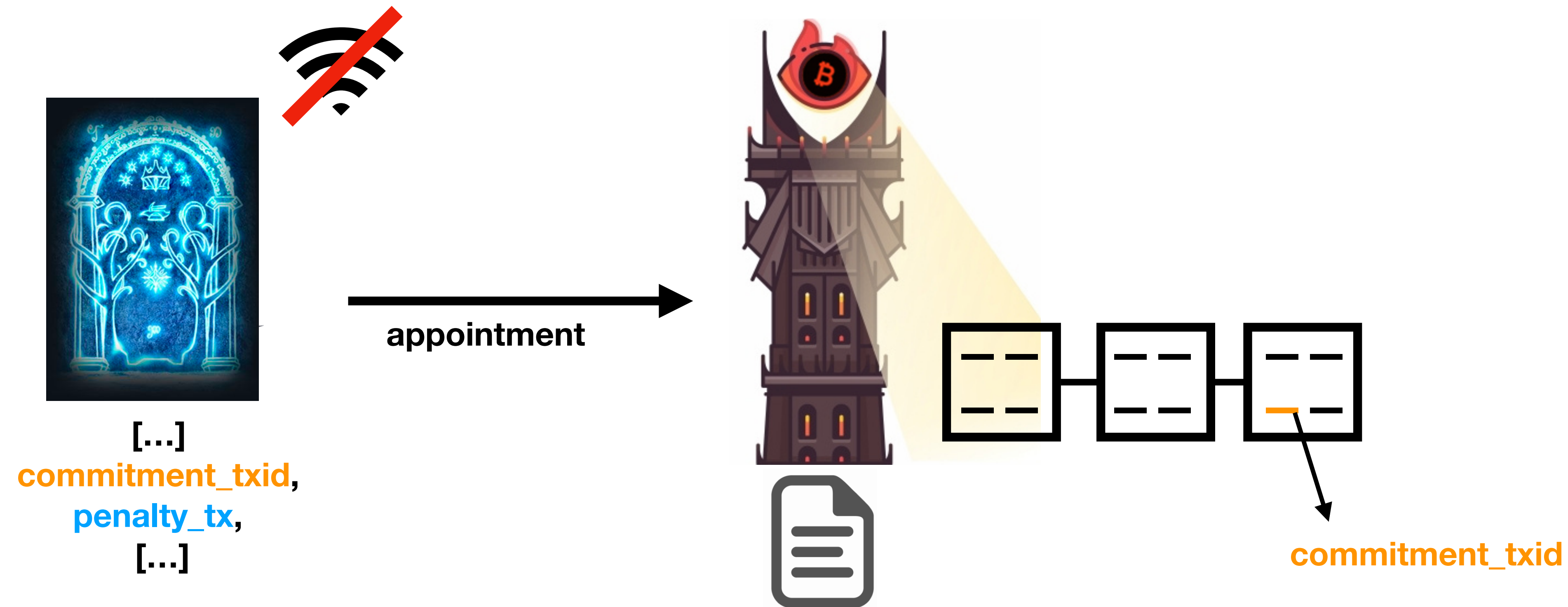
BASIC WATCHTOWER PROTOCOL



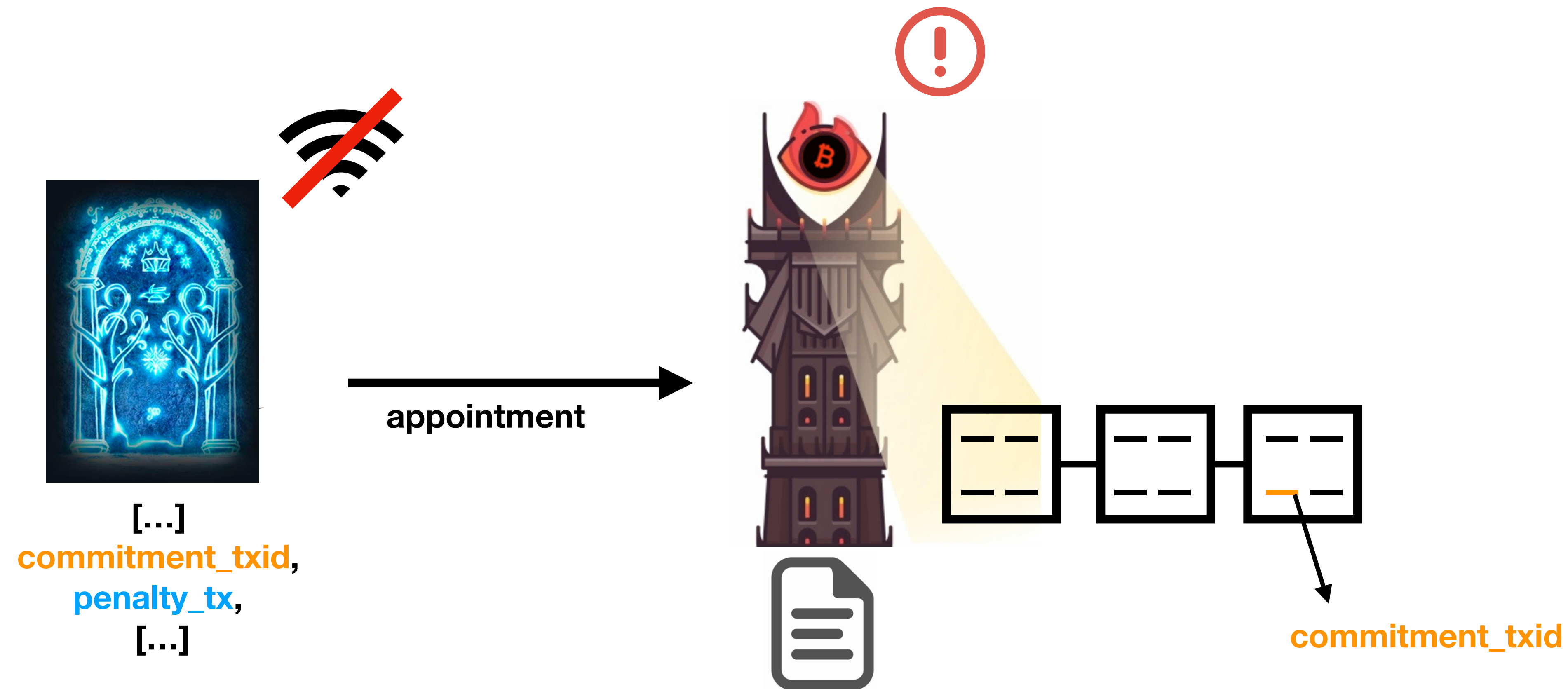
BASIC WATCHTOWER PROTOCOL



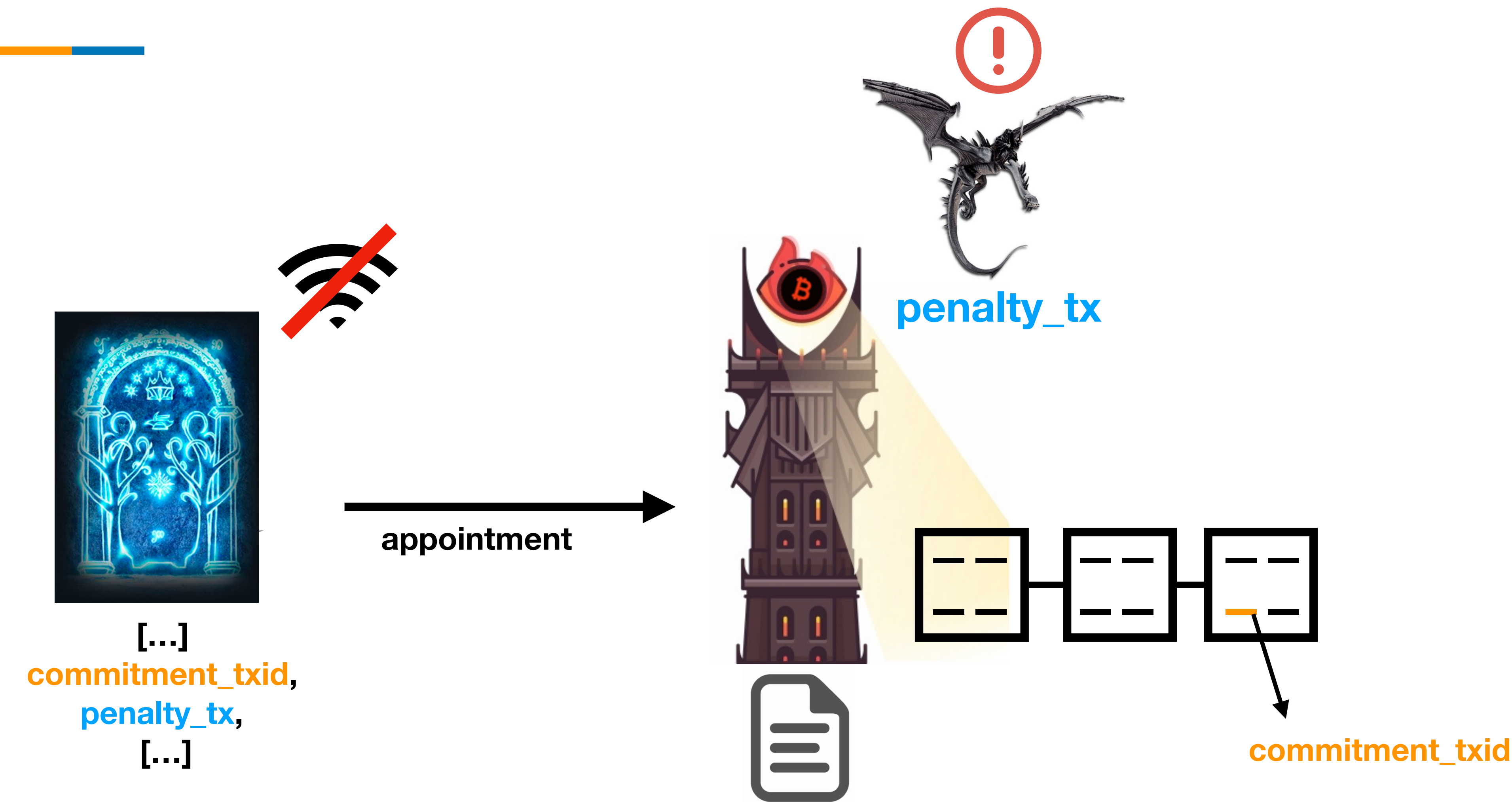
BASIC WATCHTOWER PROTOCOL



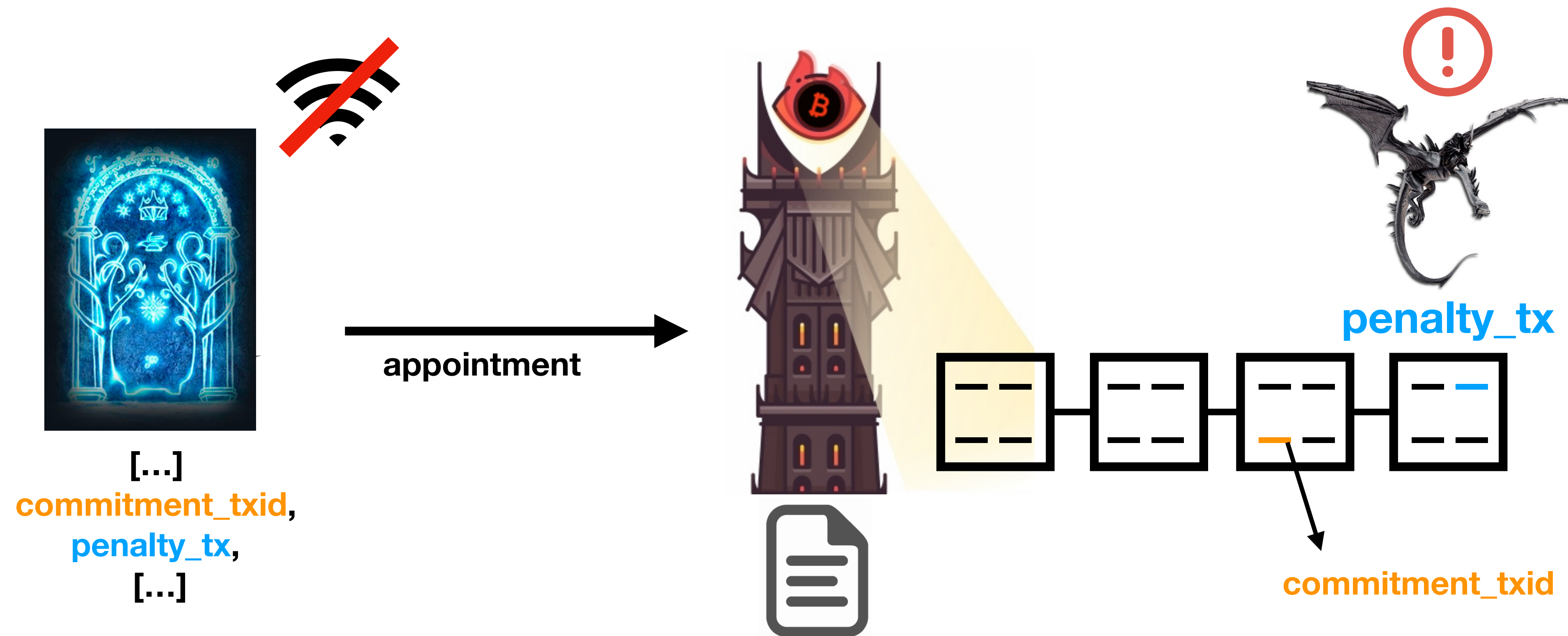
BASIC WATCHTOWER PROTOCOL



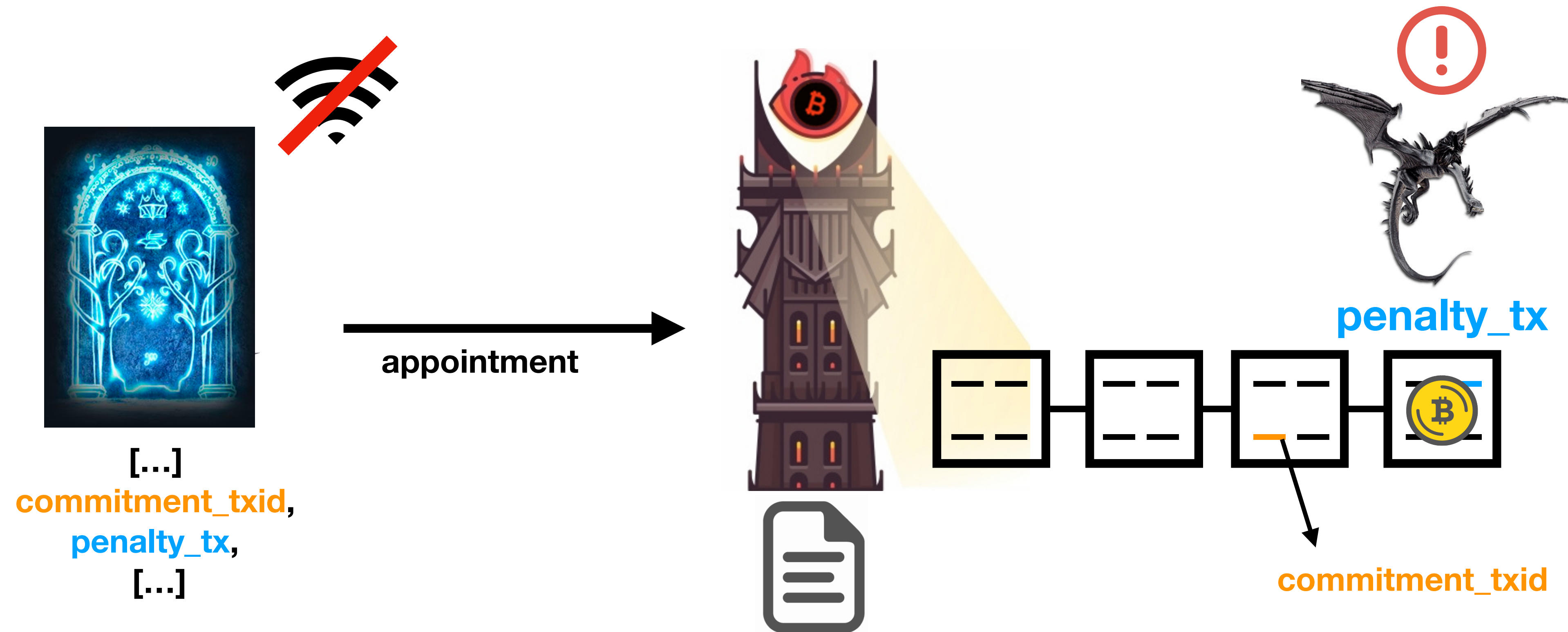
BASIC WATCHTOWER PROTOCOL



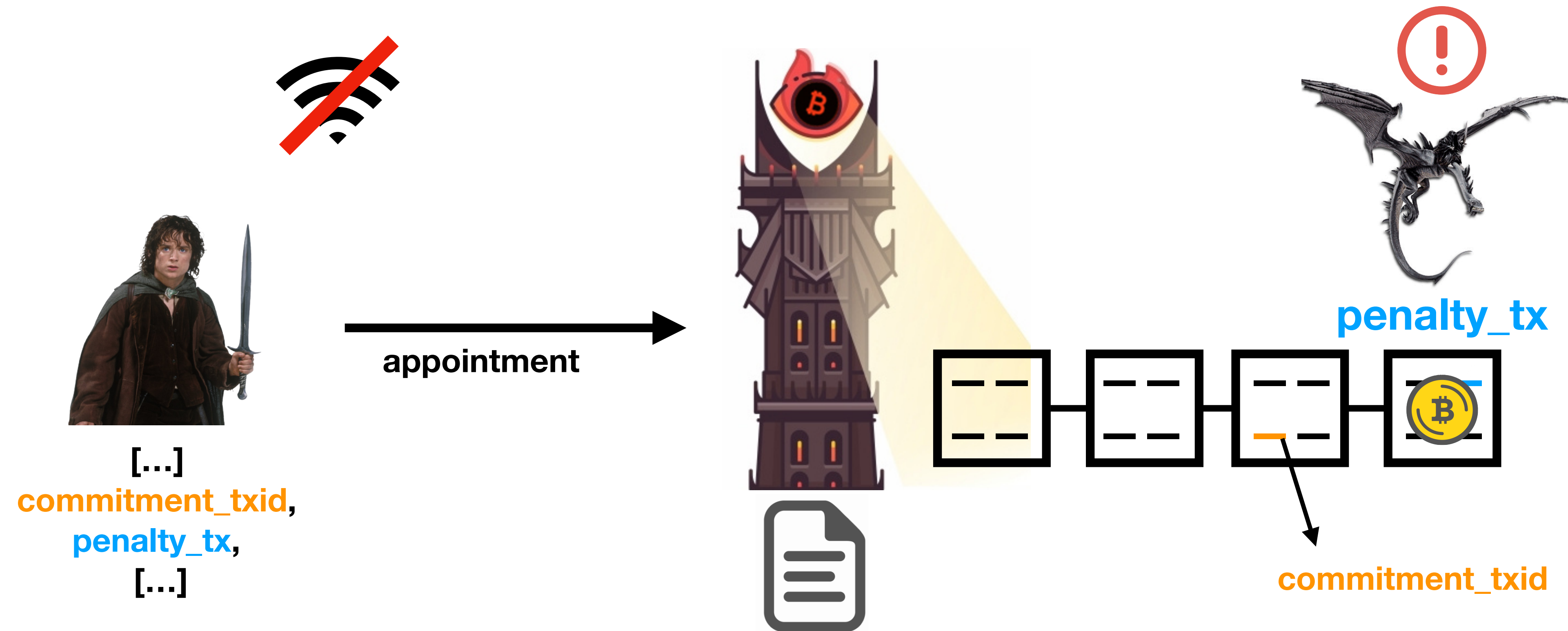
BASIC WATCHTOWER PROTOCOL



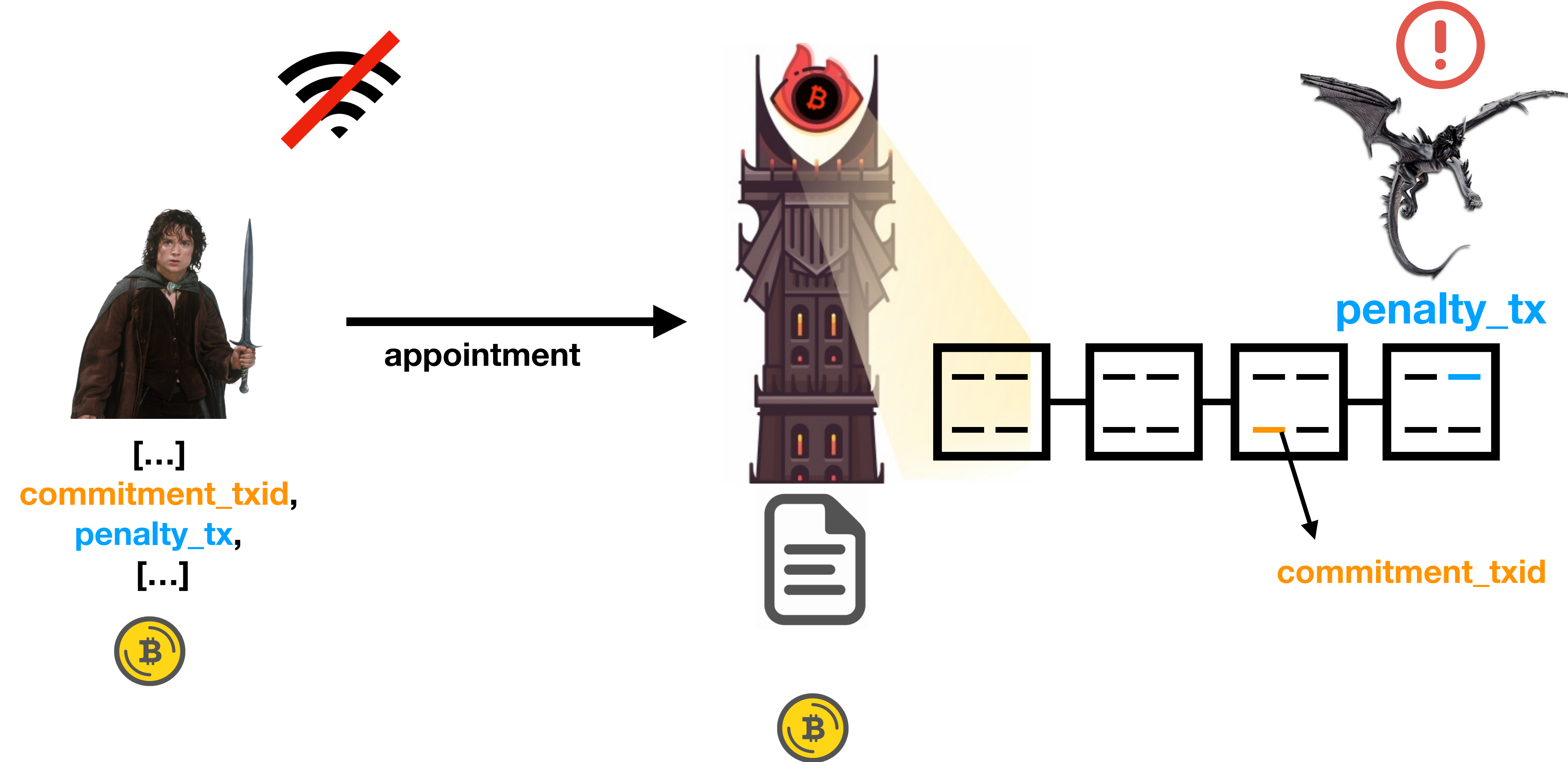
BASIC WATCHTOWER PROTOCOL



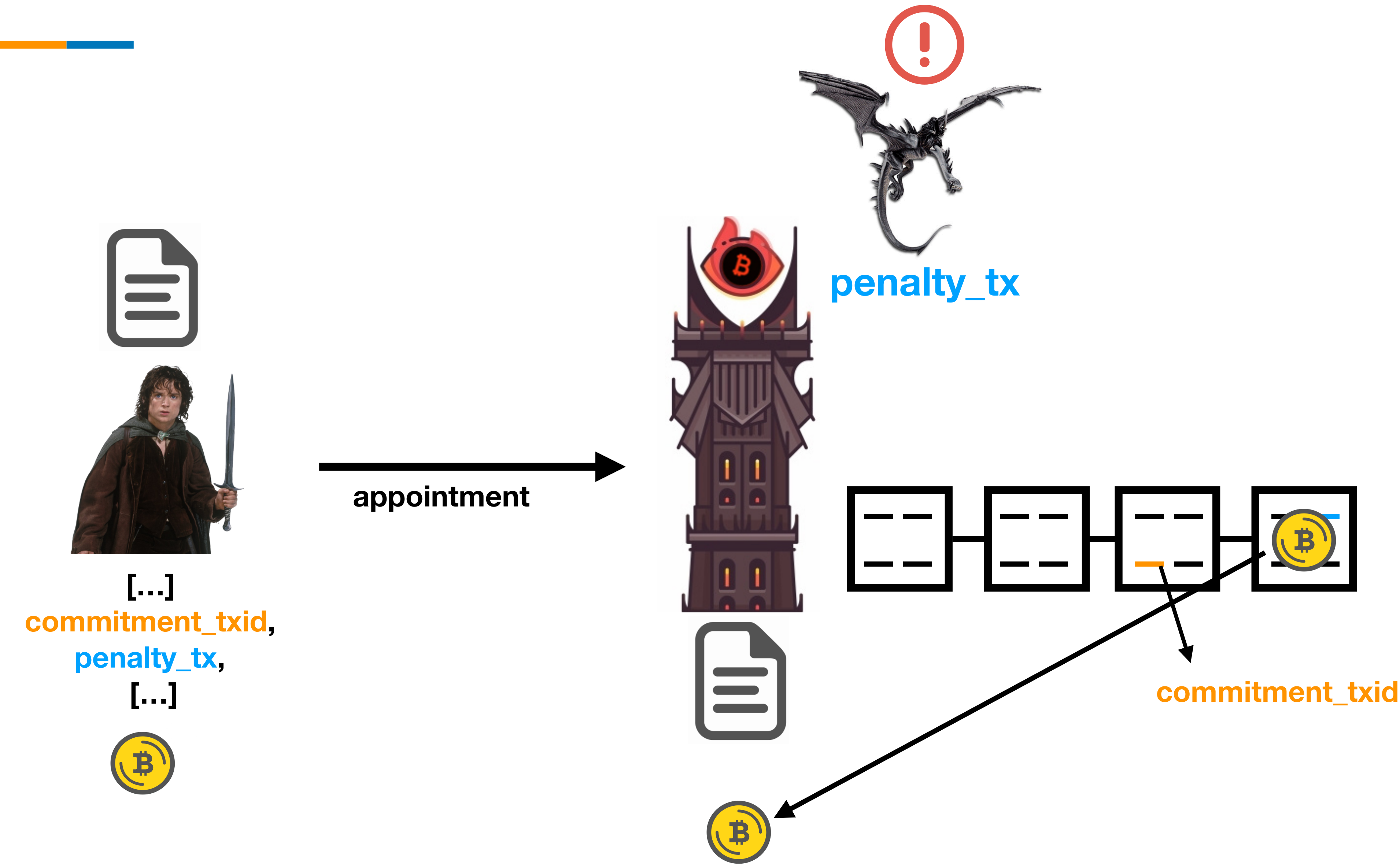
BASIC WATCHTOWER PROTOCOL



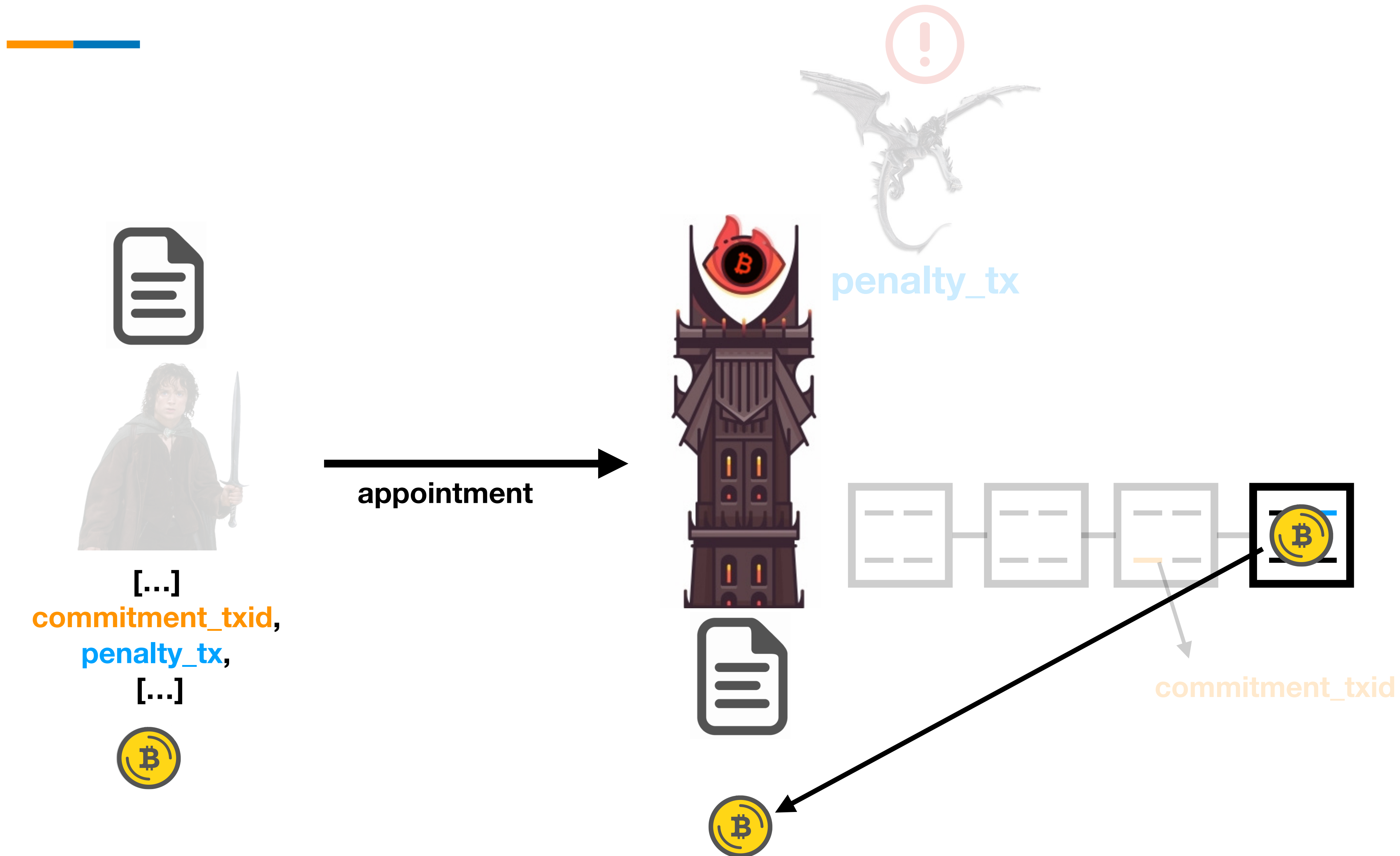
BASIC WATCHTOWER PROTOCOL



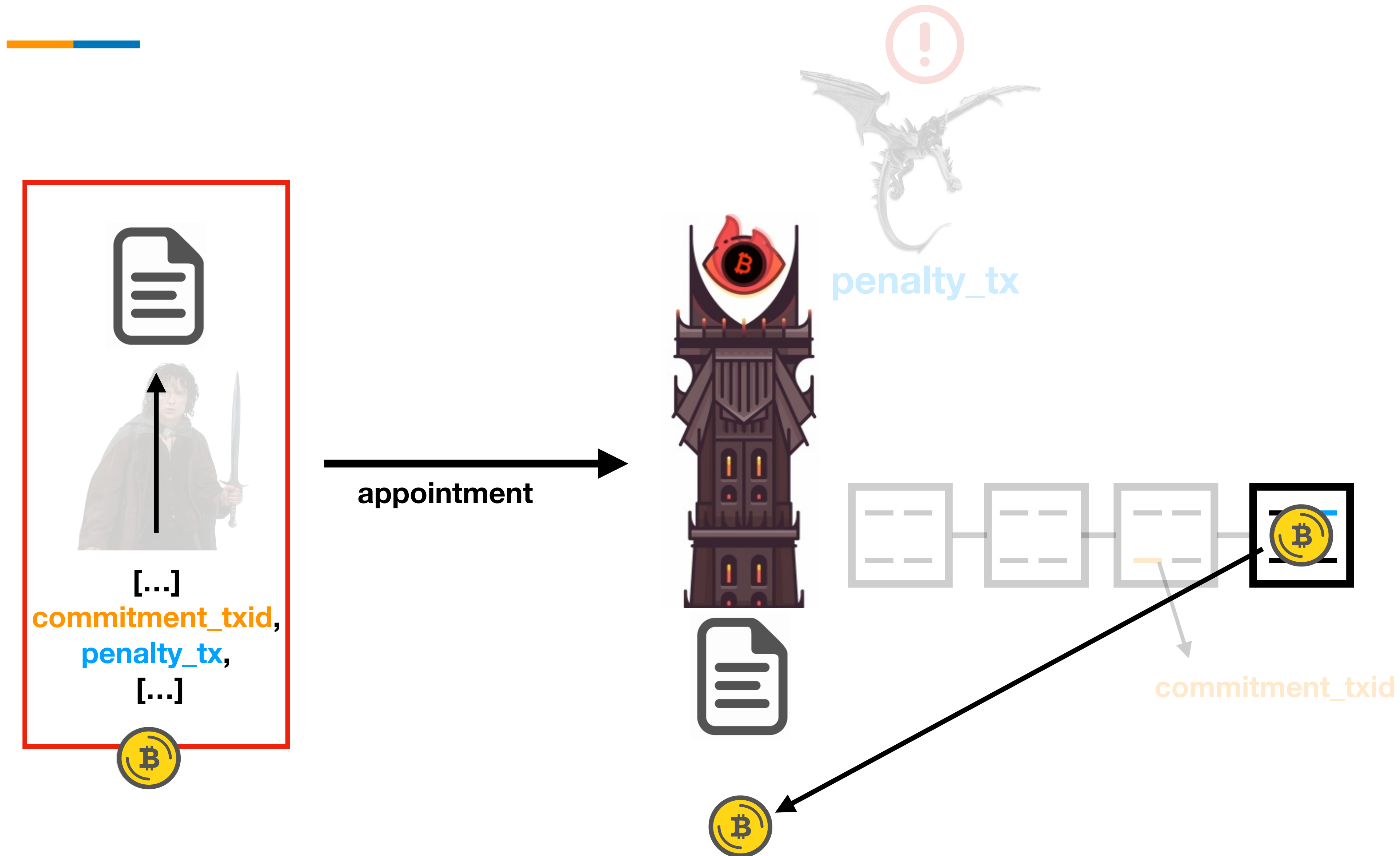
BASIC WATCHTOWER PROTOCOL



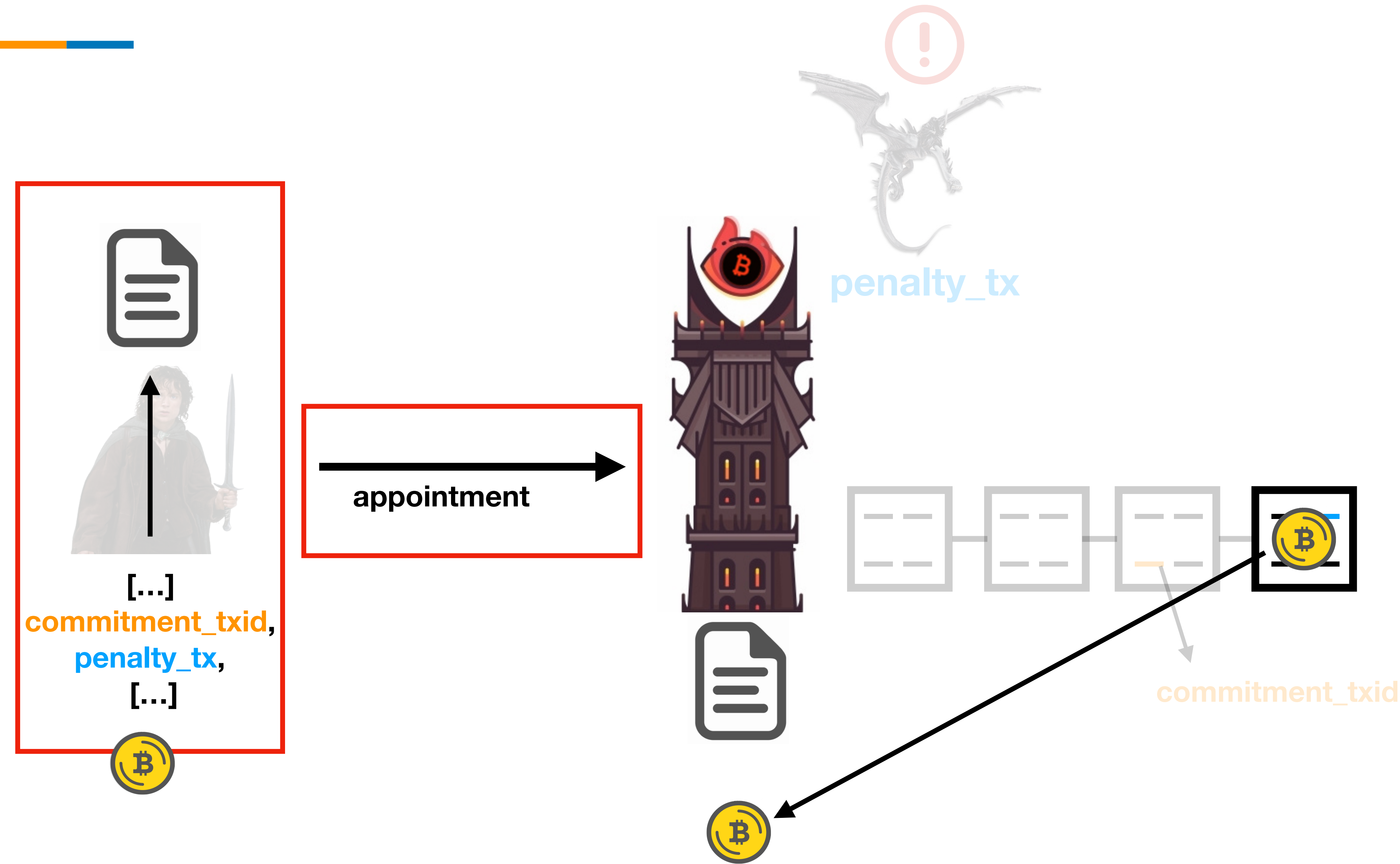
BASIC WATCHTOWER PROTOCOL



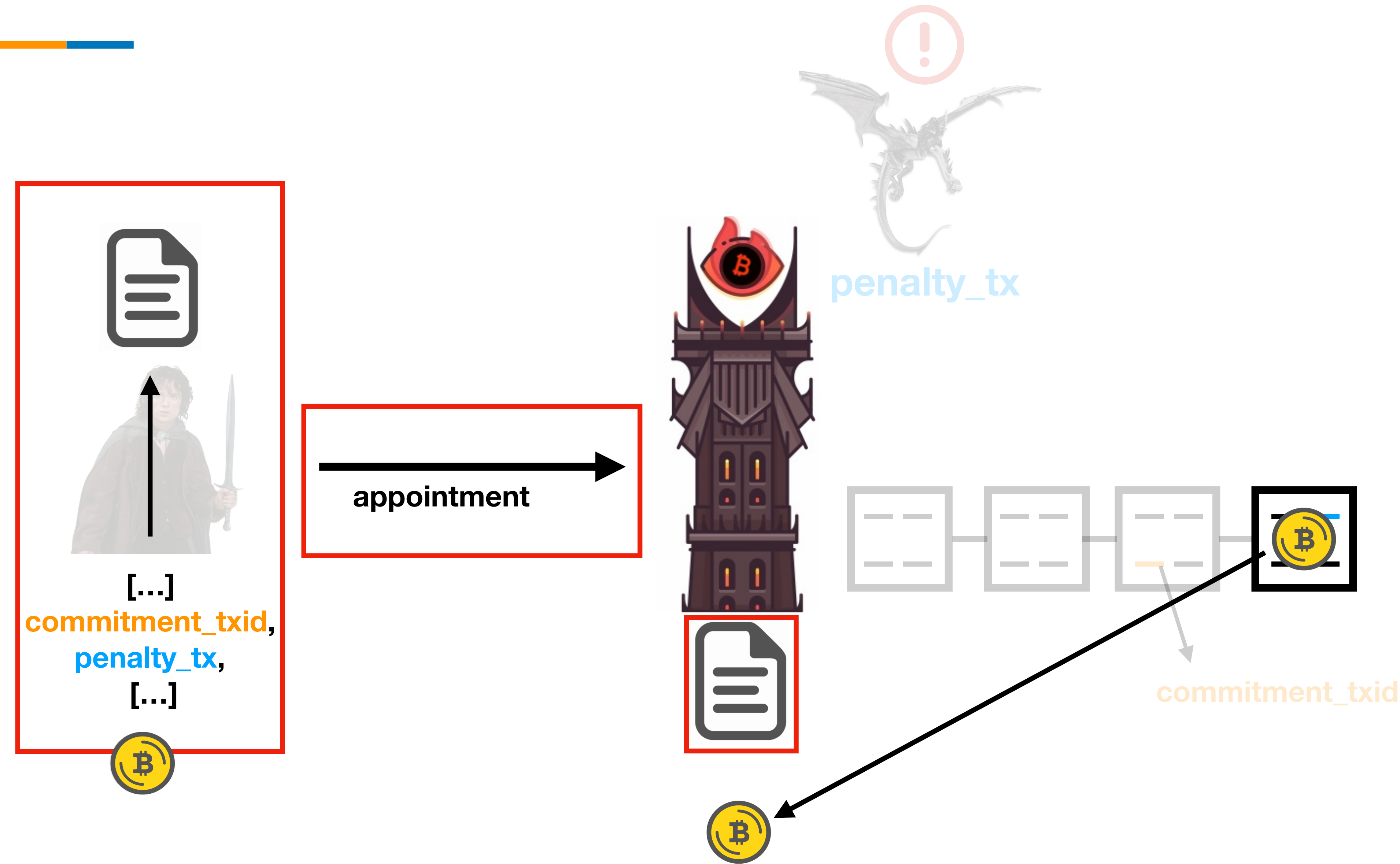
BASIC WATCHTOWER PROTOCOL



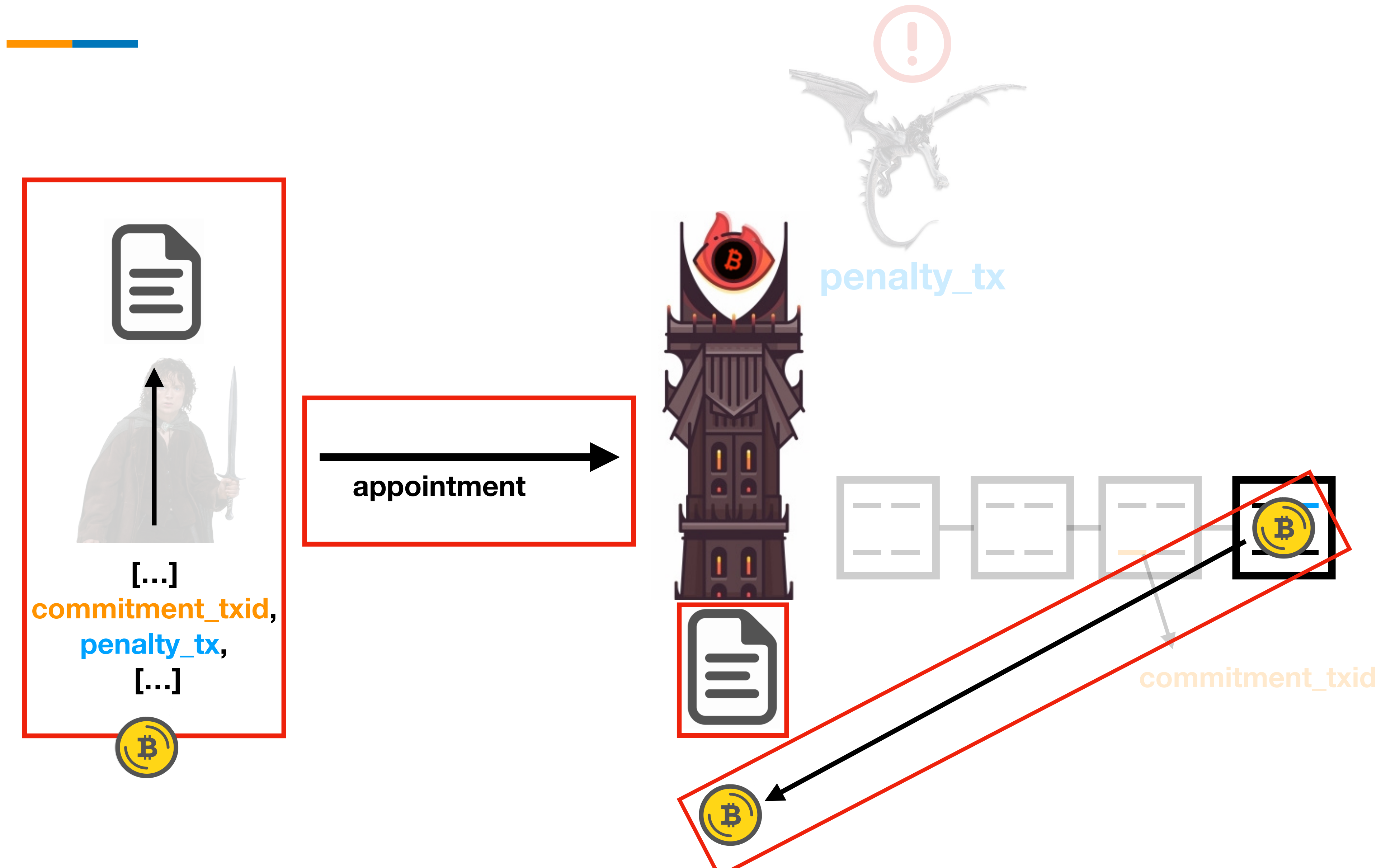
BASIC WATCHTOWER PROTOCOL



BASIC WATCHTOWER PROTOCOL



BASIC WATCHTOWER PROTOCOL



WATCHTOWER DESIGN TRADEOFFS



PRIVACY



What does the Watchtower know about the node?

ACCESS



Who can use the Watchtower?

STORAGE



What does the Watchtower have to store?

COST



What is the user cost to use the Watchtower?

NO PRIVACY VS FULL PRIVACY



NO PRIVACY



The user sends the penalty transaction as clear text

- ✓ Can verify data is a transaction
- ✗ Cannot verify transaction is valid
- ✗ Payment information is leaked

FULL PRIVACY



The user sends an encrypted penalty transaction

- ✓ Data only leaked on breach (less)
- ✗ Cannot verify data is a transaction
- ✗ Heavier computation

NO PRIVACY VS FULL PRIVACY



NO PRIVACY



FULL PRIVACY



✗ Multiple versions of the same penalty transaction can be sent

NO PRIVACY VS FULL PRIVACY



NO PRIVACY



FULL PRIVACY



✗ Multiple versions of the same penalty transaction can be sent

STORAGE



NO PRIVACY VS FULL PRIVACY



NO PRIVACY



FULL PRIVACY



✗ Multiple versions of the same penalty transaction can be sent

STORAGE



Therefore, privacy by design seems a better approach

PRIVATE VS PUBLIC ACCESS



PRIVATE ACCESS



A limited number of (trusted) users can use the tower

- ✓ No DoS risk
- ✓ Potentially free service
- ✗ Can't accommodate the whole network

PUBLIC ACCESS



Anyone can use the tower

- ✓ Tower as a service
- Access control required
- Paid service
- ✗ High DoS surface if not properly priced

PRIVATE VS PUBLIC ACCESS

PRIVATE ACCESS



A limited number of (trusted) users can use the tower

LOW STORAGE



LOW / NO COST



PUBLIC ACCESS



Anyone can use the tower

- ✓ Tower as a service
- Access control required
- Paid service
- ✗ High DoS surface if not properly priced

PRIVATE VS PUBLIC ACCESS



PRIVATE ACCESS



A limited number of (trusted) users can use the tower

PUBLIC ACCESS



Anyone can use the tower

LOW STORAGE



LOW / NO COST



HIGH STORAGE



LOW COST



O(N) STORAGE



STORAGE



The required storage is always going to be big (modulo the number of channel updates).

- Highly linked to price
- Strategies to align the incentives of the user and the tower are required
- ✗ One appointment per channel update
- ✗ Easy to DoS a public tower if storage is not properly priced

ALTRUISTIC VS NON-ALTRUISTIC TOWERS



NO COST



Using the tower is free

- ✅ OK for private towers
- ❌ Highly unviable for public towers (highest cost and DoS surface)

LOW COST



The tower charges a fee

- ✅ High traffic = profit
(if properly priced)
- ✅ Data can be deleted
(if incentives are aligned)

ALTRUISTIC VS NON-ALTRUISTIC TOWERS



NO COST



Using the tower is free

PRIVATE ACCESS AND LOW STORAGE



LOW COST



The tower charges a fee

- ✓ High traffic = profit
(if properly priced)
- ✓ Data can be deleted
(if incentives are aligned)

ALTRUISTIC VS NON-ALTRUISTIC TOWERS

NO COST



Using the tower is free

PRIVATE ACCESS AND LOW STORAGE



OR

PUBLIC ACCESS AND ∞ STORAGE



LOW COST



The tower charges a fee

- ✓ High traffic = profit
(if properly priced)
- ✓ Data can be deleted
(if incentives are aligned)

ALTRUISTIC VS NON-ALTRUISTIC TOWERS



NO COST



Using the tower is free

LOW COST



The tower charges a fee

PRIVATE ACCESS AND LOW STORAGE



OR

PUBLIC ACCESS AND HIGH STORAGE



HIGH STORAGE



IDEAL WATCHTOWER (NO ELTOO)



PRIVACY



High privacy

ACCESS



Public access

STORAGE



Non-exploitable $O(N)$ storage

COST



Low cost

IDEAL WATCHTOWER (NO ELTOO)



PRIVACY



High privacy

ACCESS



Public access

STORAGE

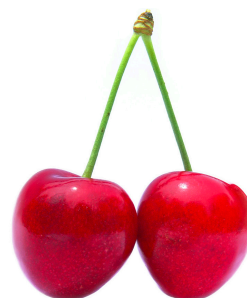


Non-exploitable $O(N)$ storage

COST

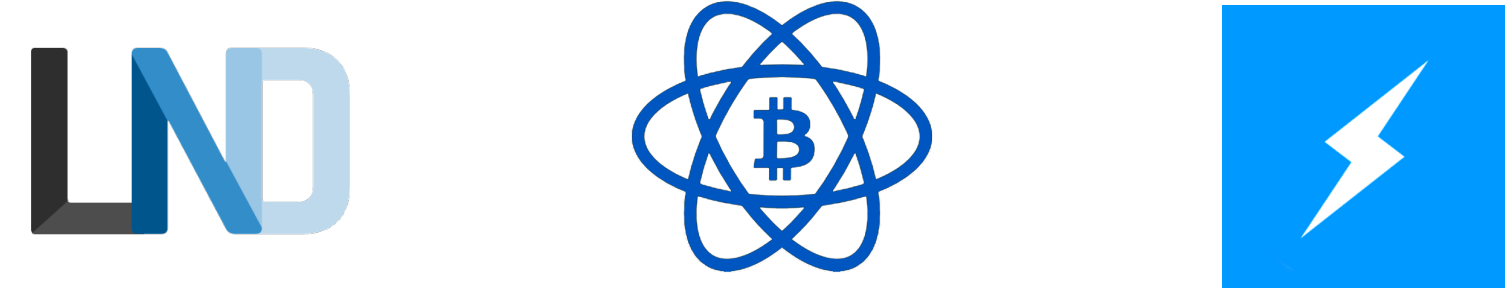


Low cost



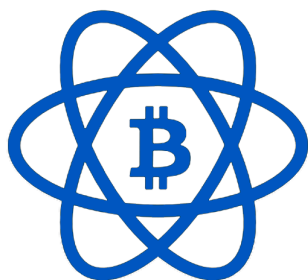
INTEROPERABLE!

IDEAL WATCHTOWER (NO ELTOO)



High privacy			
Public access			
Non-exploitable O(N) storage			
Cost	Free	Free	Low
Interoperable			

IDEAL WATCHTOWER (NO ELTOO)



High privacy



Public access



Non-exploitable $O(N)$
storage



Cost

Free

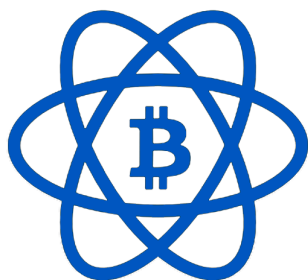
Free

Low

Interoperable



IDEAL WATCHTOWER (NO ELTOO)



High privacy



Public access



Non-exploitable $O(N)$
storage



Cost

Free

Free

Low

Interoperable



PRIVACY VIA MONITOR APPROACH (1/3)



For every channel update:

- The penalty transaction is **encrypted** under a key derived from the commitment transaction id (**sk and iv**)
- A **locator** is also derived from the commitment transaction id
- The tower receives the **encrypted blob and the locator**



PRIVACY VIA MONITOR APPROACH (2/3)



BOLT#13 DRAFT REV1:

User side

cipher = chacha20poly1305

sk = sha256(commitment_txid)

iv = 0

encrypted_blob = encrypt(penalty_tx, sk, iv)

locator = 16 MSB commitment_txid

PRIVACY VIA MONITOR APPROACH (3/3)



Tower side

For every transaction in every new block:

locator = 16 MSB **commitment_txid**

if locator in locators:

sk = sha256(**commitment_txid**)

iv = 0

cipher_text = appointment[locator].encrypted_blob

penalty_tx = decrypt(cipher_text, sk, iv)

REVENUE MODELS

Bounty

The penalty transaction includes an output for the tower.

Per-appointment

The tower is paid beforehand, appointment per appointment.

Subscription

A subscription is paid to the tower that grants access to the user for a certain time/number of appointments.

BOUNTY - REVENUE MODELS



The tower is paid only if a breach happens and the penalty makes it to the chain



Multiple towers can be hired for the price of one



The tower **can** use CPFP to bump the fee of the penalty transaction



It's easy to spam/DoS the tower with junk



PER-APPOINTMENT - REVENUE MODELS



The tower is paid beforehand, even if it does not respond to the breach



A rational user will only hire so many towers



The tower **cannot** use CPFP to bump the fee of the penalty transaction



Spamming the tower has a cost



A payment is required for every update



Updating/deleting appointments is harder



SUBSCRIPTION - REVENUE MODELS



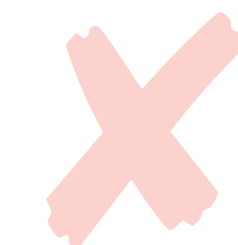
The tower is paid beforehand, even if it does not respond to the breach



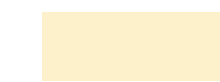
A rational user will only hire so many towers



The tower **cannot** use CPFP to bump the fee of the penalty transaction



Spamming the tower has a cost



Minimises number payment to the tower



Updating/deleting appointments is easier



SUBSCRIPTIONS VS BOUNTY



BOTH MODELS HAVE THEIR PROS AND CONS...

SUBSCRIPTIONS VS BOUNTY

BOTH MODELS HAVE THEIR PROS AND CONS...



SUBSCRIPTION & BOUNTY - REVENUE MODELS



The tower is paid **a fraction of the cost** beforehand, the rest is paid as a bounty



A rational user will only hire so many towers



The tower **can** use CPFP to bump the fee of the penalty transaction



Spamming the tower has a cost



Minimises number payment to the tower



Updating/deleting appointments is easier



USER AUTHENTICATION



- Authenticating the user helps preventing resource abuse
- It is required for the subscription model
- **Message signing using the node's secret key**
 - The tower can check that the node exists
 - Does not require any additional key / auth token
 - Leaks the number of channel updates of the node
- **Message signing using an ephemeral key** (not liked node id)

USER TABS - ALIGNING THE INCENTIVES



- User authentication allows the creation of user tabs
- A tab can be created for every user's channel
- The tab_id can be **random**, or a **derivation of the channel_id**
- If the channel is closed, the user can close the tab on the tower
- The tower can reward users that free space (subscription discounts, update the number of free appointment slots, ...)
- **Appointments can be deleted without tabs, it only makes it easier**

EXTENSIONS



The BOLT should have room for extensions so additional features can be added (e.g: accountability):

- Accountability can generate proof of appointment fulfilment
- Scores can be assigned to to avoid using misbehaving towers
- Scores can be used system-wise or node-wise

QUESTIONS

BONUS TRACK - ATTACKS

ATTACKS ON WATCHTOWERS



ATTACKS ON WATCHTOWERS



ATTACKS ON WATCHTOWERS



ATTACKS ON WATCHTOWERS



ATTACKS ON WATCHTOWERS



Bounty approach

ATTACKS ON WATCHTOWERS



Bounty approach

ATTACKS ON WATCHTOWERS



Bounty approach

ATTACKS ON WATCHTOWERS



Bounty approach

ATTACKS ON WATCHTOWERS



Bounty approach

ATTACKS ON WATCHTOWERS



Bounty approach

ATTACKS ON WATCHTOWERS



Bounty approach



- A) Keep first**
- B) Update first w/
second**
- C) Wipe both**
- D) Keep both**

ATTACKS ON WATCHTOWERS



Bounty approach



- A) Keep first**
- B) Update fist w/
second**
- C) Wipe both**
- D) Keep both**

ATTACKS ON WATCHTOWERS



Bounty approach



- A) Keep first**
- B) Update first w/
second**
- C) Wipe both**
- D) Keep both**

ATTACKS ON WATCHTOWERS



Bounty approach



Appointment front-running

- A) **Keep first**
- B) **Update fist w/
second**
- C) **Wipe both**
- D) **Keep both**

ATTACKS ON WATCHTOWERS



Bounty approach



- A) Keep first
- B) Update first w/
second
- C) Wipe both
- D) Keep both

ATTACKS ON WATCHTOWERS



Bounty approach



- A) Keep first
- B) Update first w/
second
- C) Wipe both
- D) Keep both

ATTACKS ON WATCHTOWERS



Bounty approach



Appointment rewriting



- A) Keep first
- B) Update first w/
second**
- C) Wipe both
- D) Keep both

ATTACKS ON WATCHTOWERS



Bounty approach



- A) Keep first
- B) Update first w/
second
- C) **Wipe both**
- D) Keep both

ATTACKS ON WATCHTOWERS



Bounty approach



- A) Keep first
- B) Update first w/
second
- C) **Wipe both**
- D) Keep both

ATTACKS ON WATCHTOWERS



Bounty approach



Shot in the foot?



- A) Keep first
- B) Update first w/
second
- C) **Wipe both**
- D) Keep both

ATTACKS ON WATCHTOWERS



Bounty approach



- A) Keep first
- B) Update first w/
second
- C) Wipe both
- D) Keep both**

ATTACKS ON WATCHTOWERS



- A) Keep first
- B) Update first w/
second
- C) Wipe both
- D) Keep both**

Bounty approach

ATTACKS ON WATCHTOWERS



- A) Keep first
- B) Update first w/
second
- C) Wipe both
- D) Keep both**

Bounty approach

QUESTIONS
