

# Streamlet: consensus in 5 minutes

Benjamin Chan

Elaine Shi

*Cornell University*

Every CS undergrad should know three things:

Every CS undergrad should know three things:

1. How to sort a list

Every CS undergrad should know three things:

1. How to sort a list
2. Whether OWFs exist :)

Every CS undergrad should know three things:

1. How to sort a list
2. Whether OWFs exist :)
3. How to solve byzantine agreement

Every CS undergrad should know three things:

1. How to sort a list
2. Whether OWFs exist :)
3. How to solve byzantine agreement

(ok, maybe not)

Every CS undergrad should know three things:


1. How to sort a list
2. Whether OWFs exist :)
3. How to solve byzantine agreement ←hard!!

Every CS undergrad should know three things:

1. How to sort a list
2. Whether OWFs exist :)
3. How to solve byzantine agreement ← **complicated!!**



Every CS undergrad should know three things:




Screamlet  
to the rescue!


1.

2.

3. How to solve byzantine agreement ← complicated!!


Every CS undergrad should know three things:



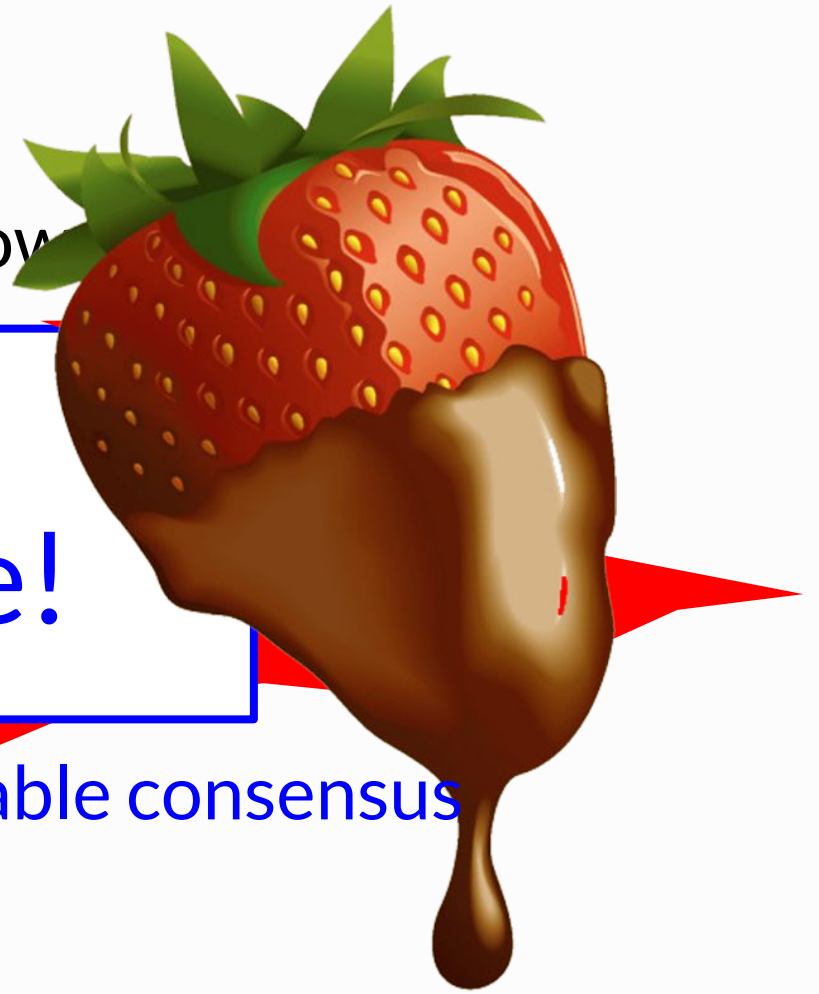
creamlet  
to the rescue!

Short & sweet, simple, teachable consensus

Every CS undergrad should know

creamlet  
to the rescue!

Short & sweet, simple, teachable consensus



Streamlet: consensus in 3 minutes

Streamlet: ~~consensus~~ in 3 minutes

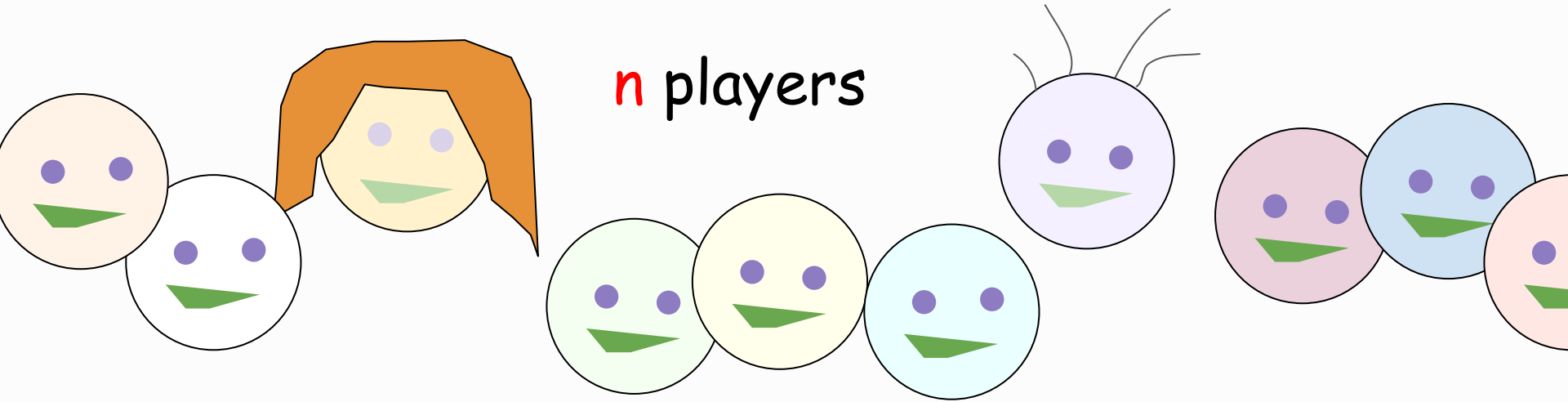
~~byzantine agreement~~

blockchain (permissioned)

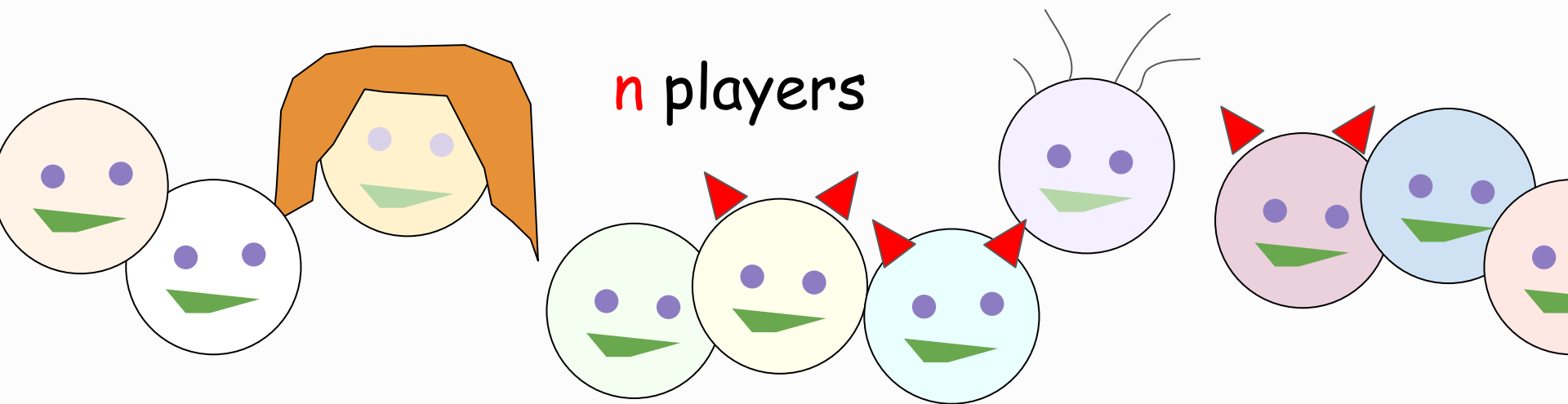
Streamlet: ~~consensus~~ in 3 minutes

~~byzantine agreement~~

blockchain (permissioned)



Streamlet: ~~consensus~~ in 3 minutes  
~~byzantine agreement~~  
blockchain (permissioned)



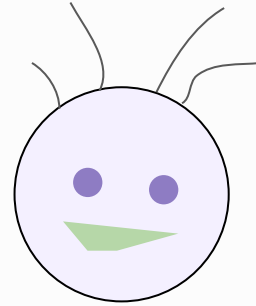
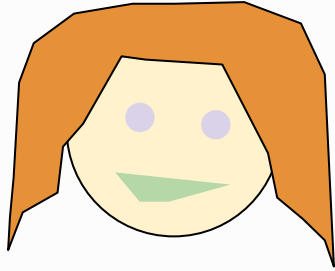
$f < n/3$  malicious

Streamlet: ~~consensus~~ in 3 minutes

~~byzantine agreement~~

blockchain (permissioned)

Alice



Bob

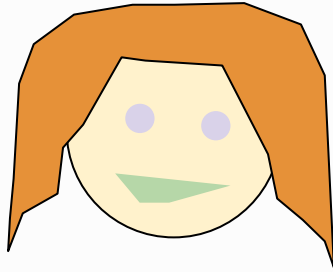


Streamlet: ~~consensus~~ in 3 minutes

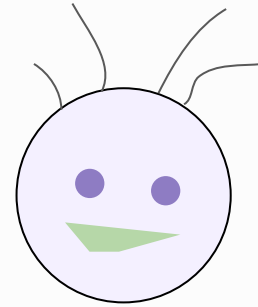
~~byzantine agreement~~

blockchain (permissioned)

Alice



messages



Bob

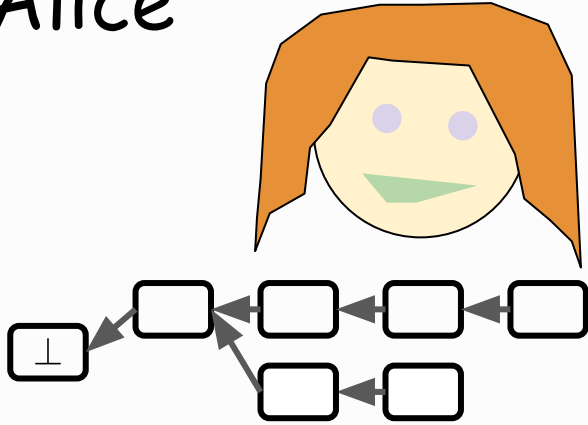
(partially synchronous)

Streamlet: ~~consensus~~ in 3 minutes

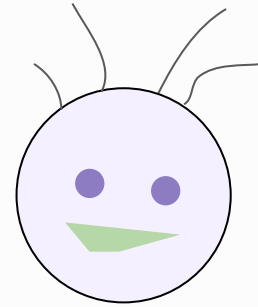
~~byzantine agreement~~

blockchain (permissioned)

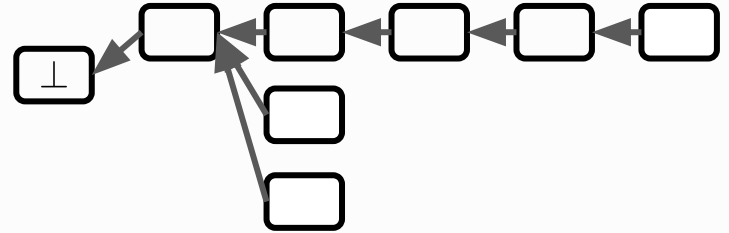
Alice



messages



Bob

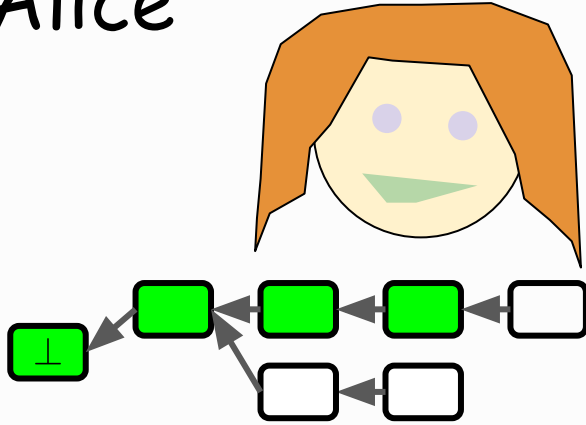


Streamlet: ~~consensus~~ in 3 minutes

~~byzantine agreement~~

blockchain (permissioned)

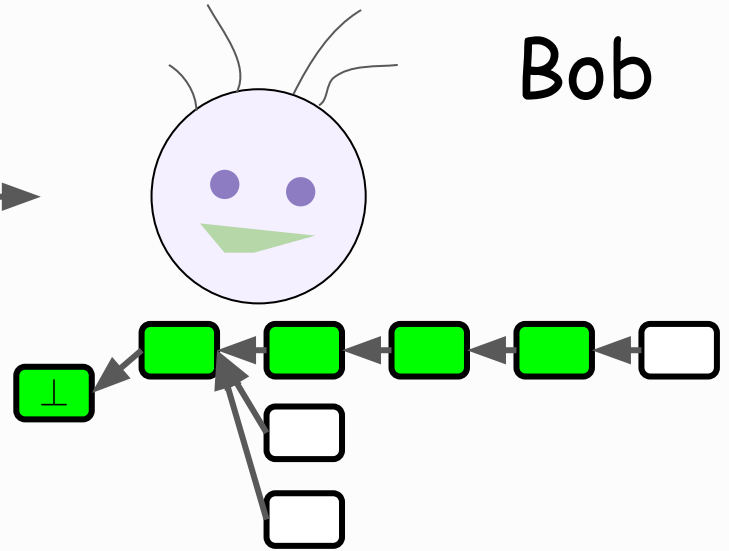
Alice



messages



Bob

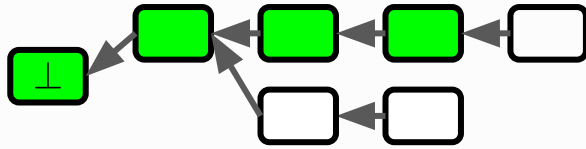
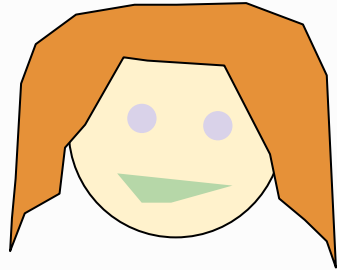


Streamlet: ~~consensus~~ in 3 minutes

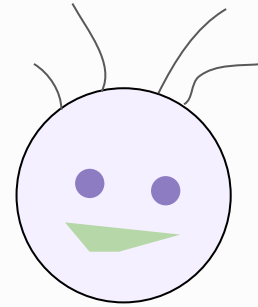
~~byzantine agreement~~

blockchain (permissioned)

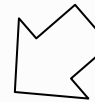
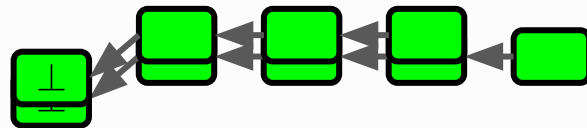
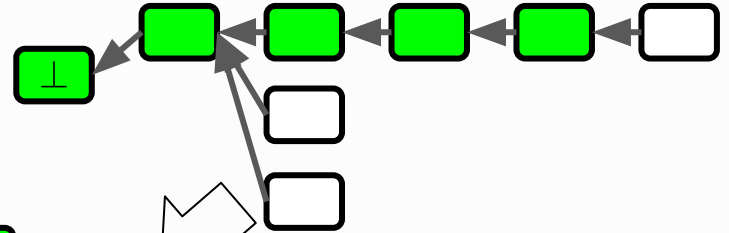
Alice



messages

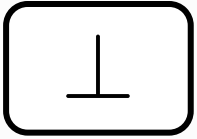


Bob



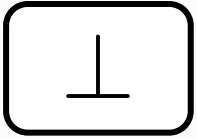
# Streamlet: blockchain in 2.5 minutes

epochs



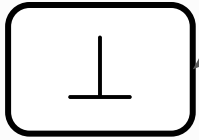
# Streamlet: blockchain in 2.5 minutes

epoch 1



# Streamlet: blockchain in 2.5 minutes

epoch 1

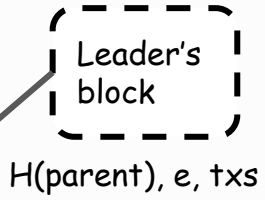
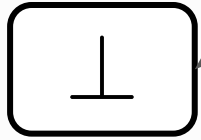


Leader



# Streamlet: blockchain in 2.5 minutes

epoch 1



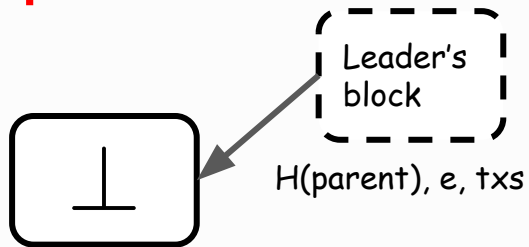
Leader





# Streamlet: blockchain in 2.5 minutes

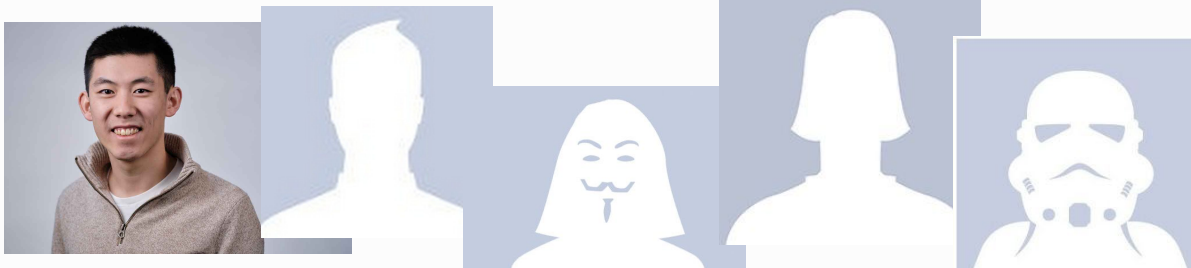
epoch 1



Leader

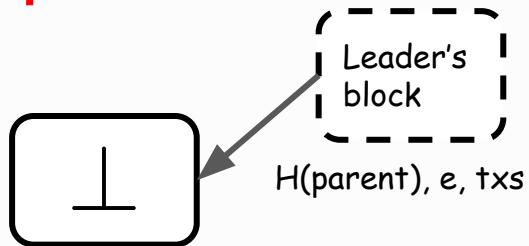


Voters



# Streamlet: blockchain in 2.5 minutes

epoch 1

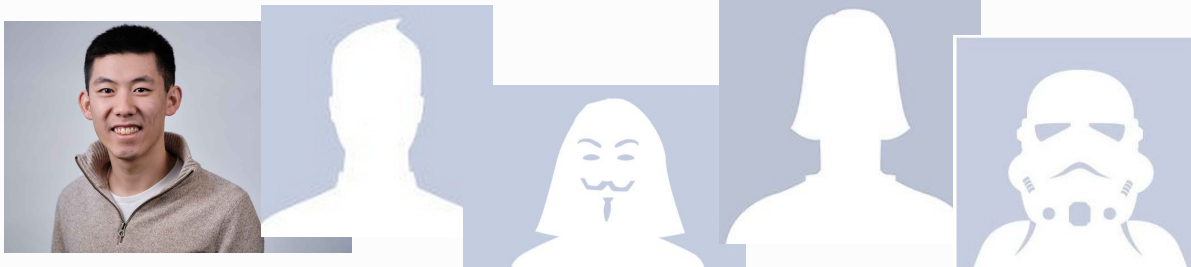


Leader



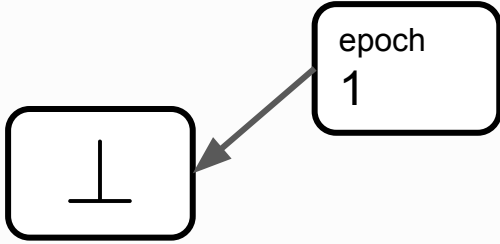
Voters

$\geq 2n/3$  votes



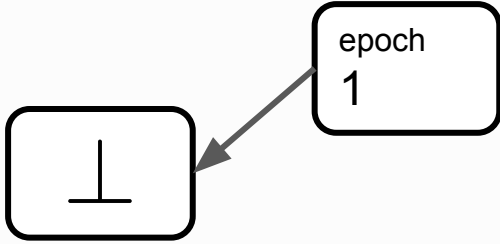
# Streamlet: blockchain in 2.5 minutes

epoch 1



# Streamlet: blockchain in 2.5 minutes

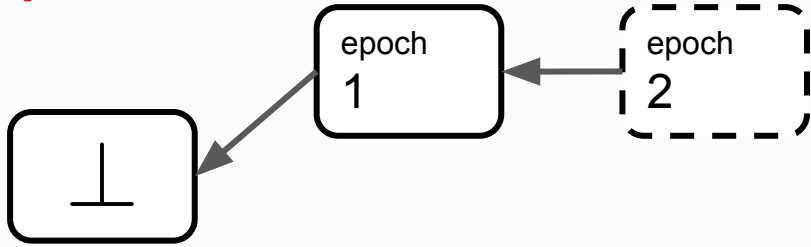
epoch 1



"notarized"

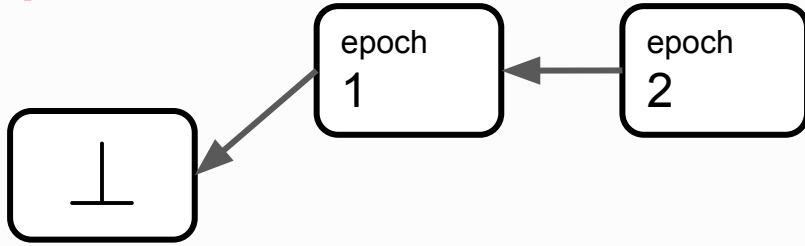
# Streamlet: blockchain in 2.5 minutes

epoch 2



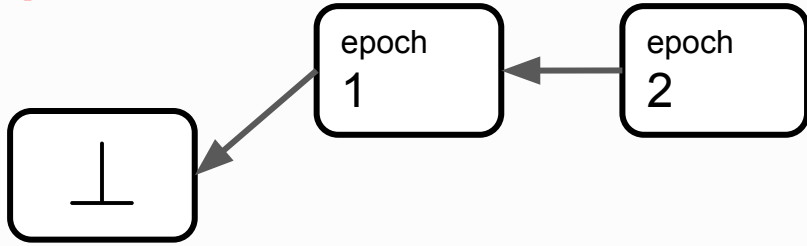
# Streamlet: blockchain in 2.5 minutes

epoch 2



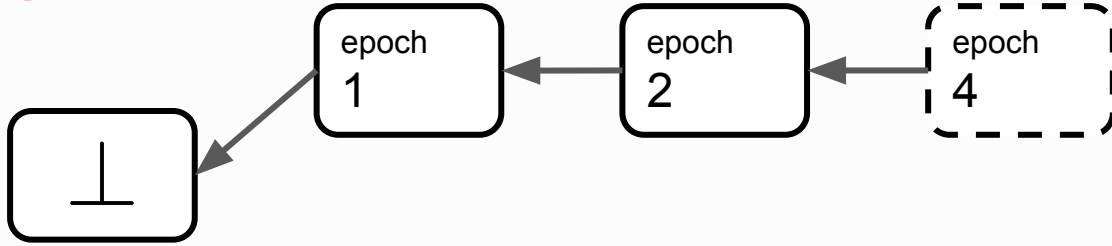
# Streamlet: blockchain in 2.5 minutes

epoch 3



# Streamlet: blockchain in 2.5 minutes

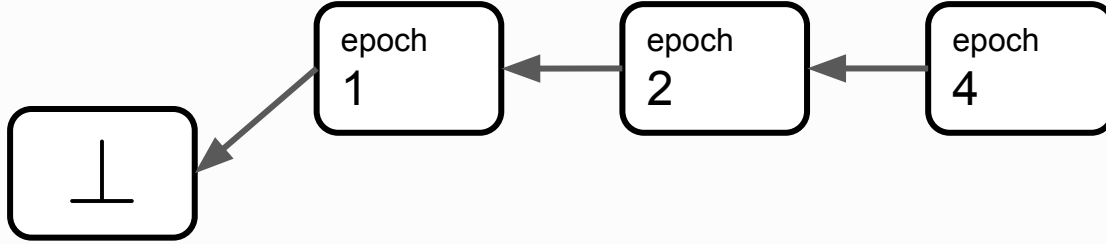
epoch 4





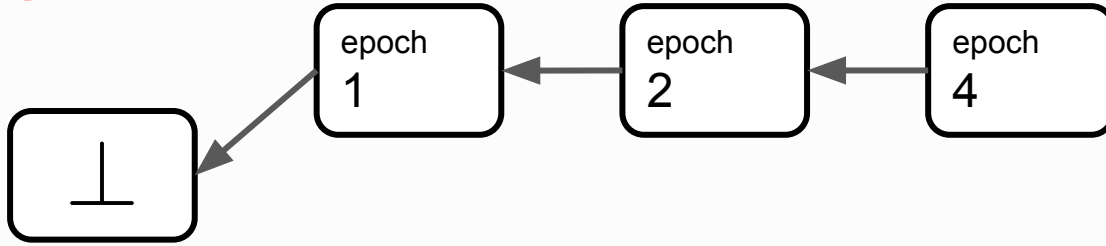
# Streamlet: blockchain in 2.5 minutes

epoch 4



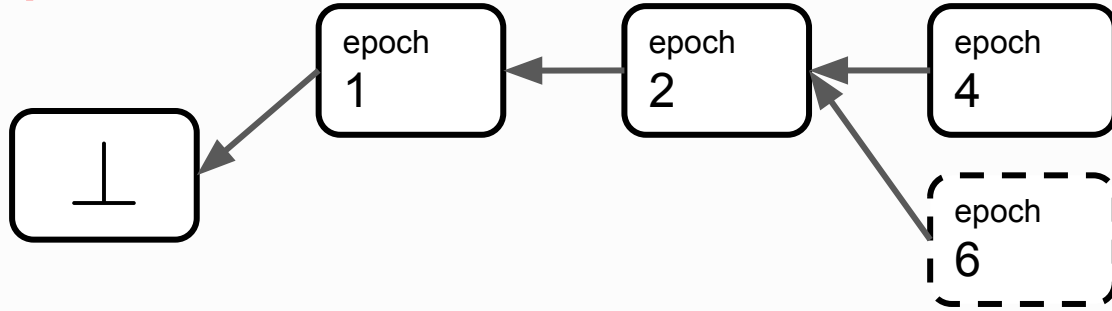
# Streamlet: blockchain in 2.5 minutes

epoch 5



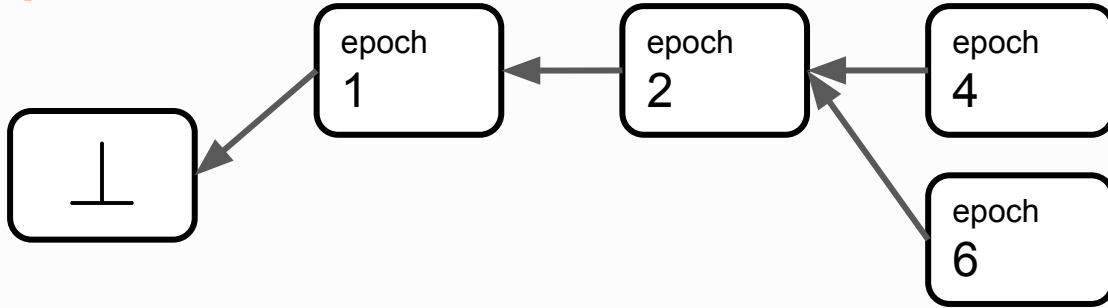
# Streamlet: blockchain in 2.5 minutes

epoch 6



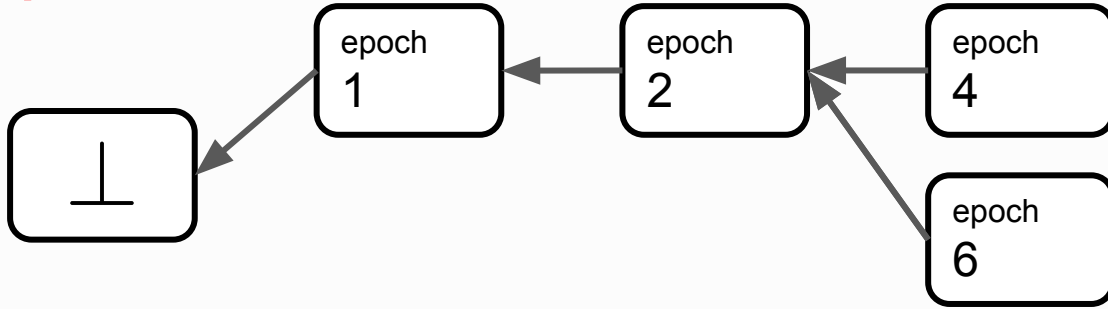
# Streamlet: blockchain in 2.5 minutes

epoch 6



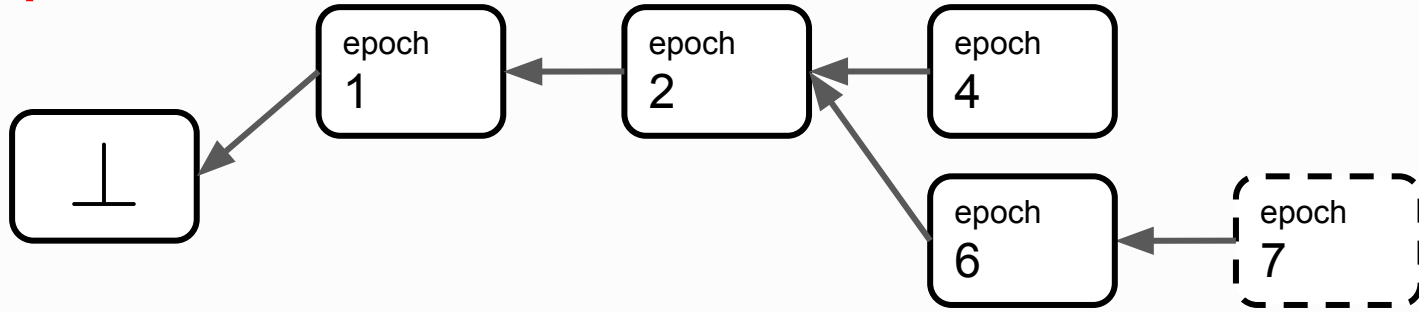
# Streamlet: blockchain in 2.5 minutes

epoch 6



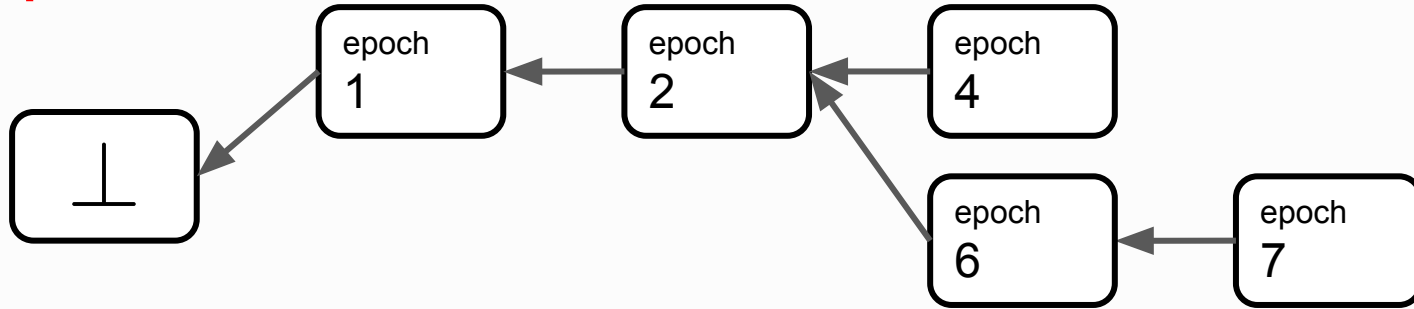
# Streamlet: blockchain in 2.5 minutes

epoch 7



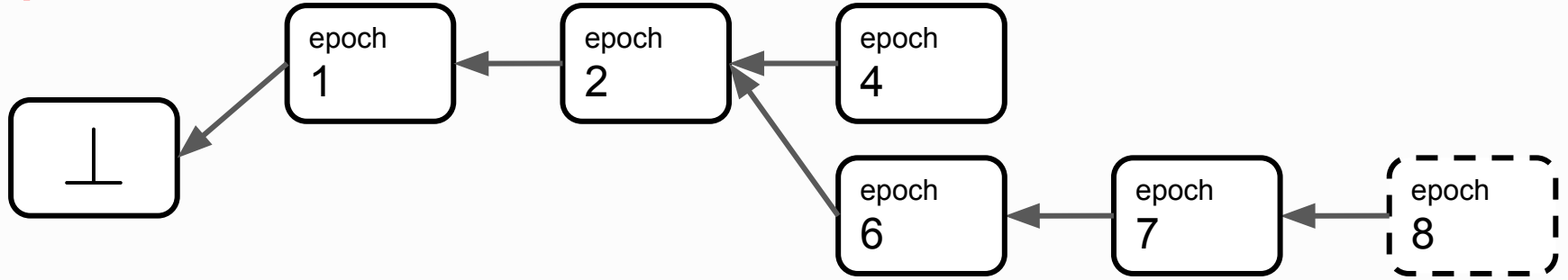
# Streamlet: blockchain in 2.5 minutes

epoch 7



# Streamlet: blockchain in 2.5 minutes

epoch 8

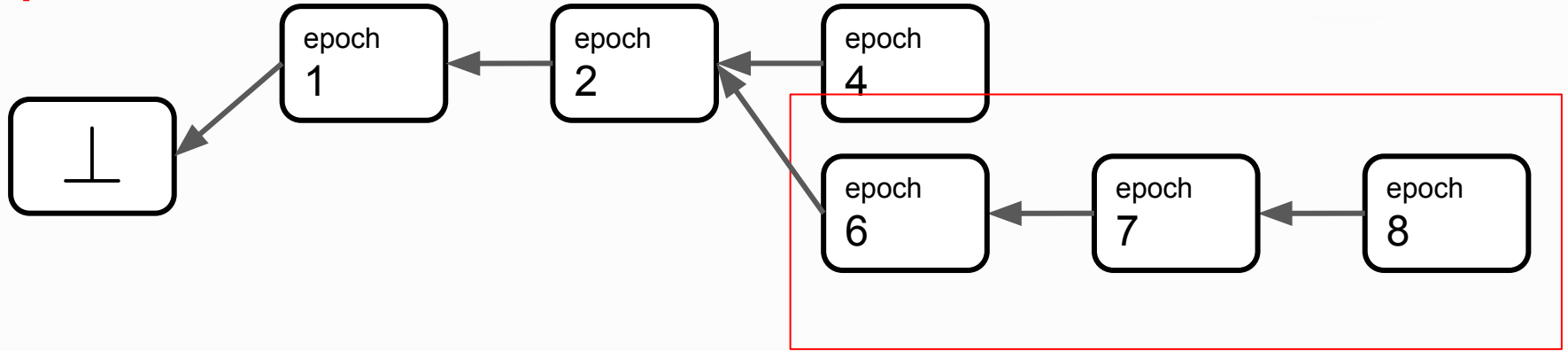




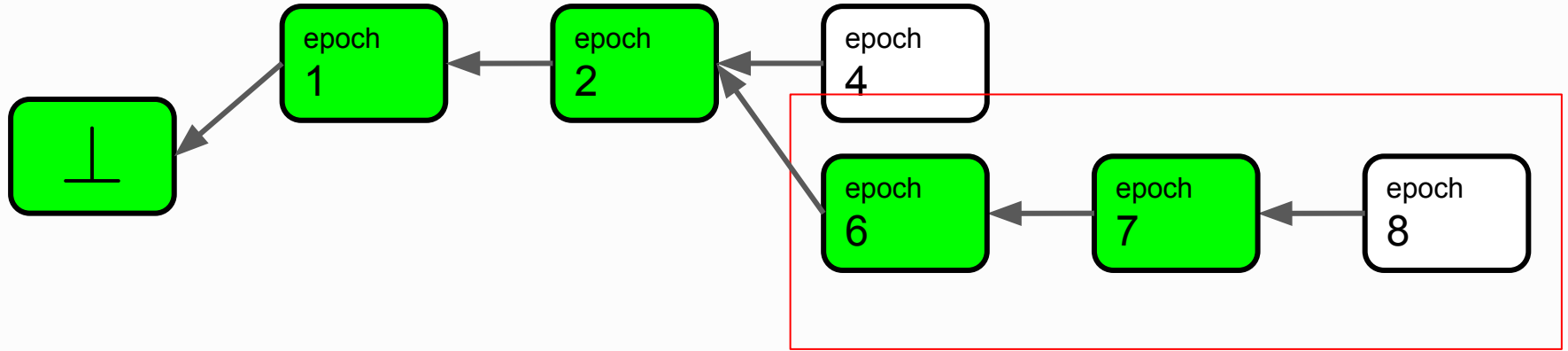
# Streamlet: blockchain in 2.5 minutes



epoch 8



# Streamlet: blockchain in 2.5 minutes



# Streamlet: blockchain in 2 minutes

In every epoch  $e = 1, 2, 3...$

- ❑ leader proposes a block  $b$
- ❑ voters vote for  $b$

finalize

# Streamlet: blockchain in 2 minutes

In every epoch  $e = 1, 2, 3\dots$

- ❑ leader proposes a block  $b$  **extending longest notarized chain**
- ❑ voters vote for  $b$  **i.f.f. it extends longest notarized chain**

finalize

# Streamlet: blockchain in 2 minutes

$>2n/3$  players vote for a block  $\rightarrow$  “notarized”

In every epoch  $e = 1, 2, 3\dots$

- ❑ leader proposes a block  $b$  extending longest notarized chain
- ❑ voters vote for  $b$  i.f.f. it extends longest notarized chain

finalize

# Streamlet: blockchain in 2 minutes

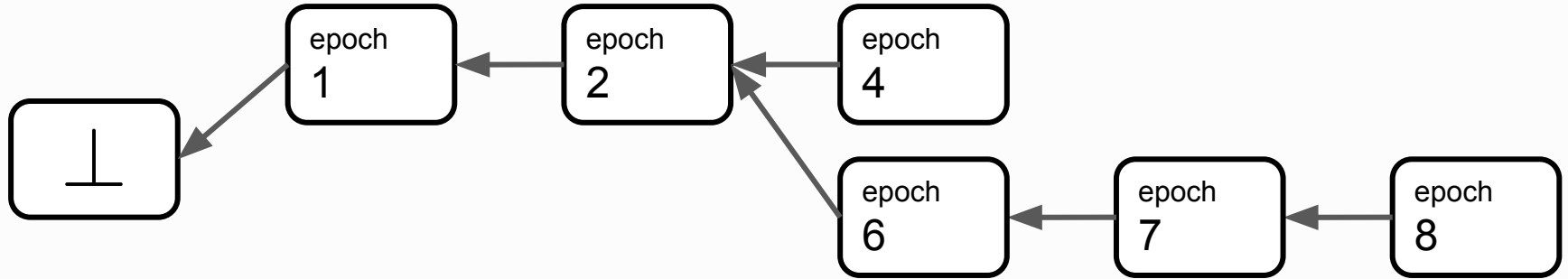
$>2n/3$  players vote for a block  $\rightarrow$  “notarized”

In every epoch  $e = 1, 2, 3\dots$

- ❑ leader proposes a block  $b$  extending longest notarized chain
- ❑ voters vote for  $b$  i.f.f. it extends longest notarized chain

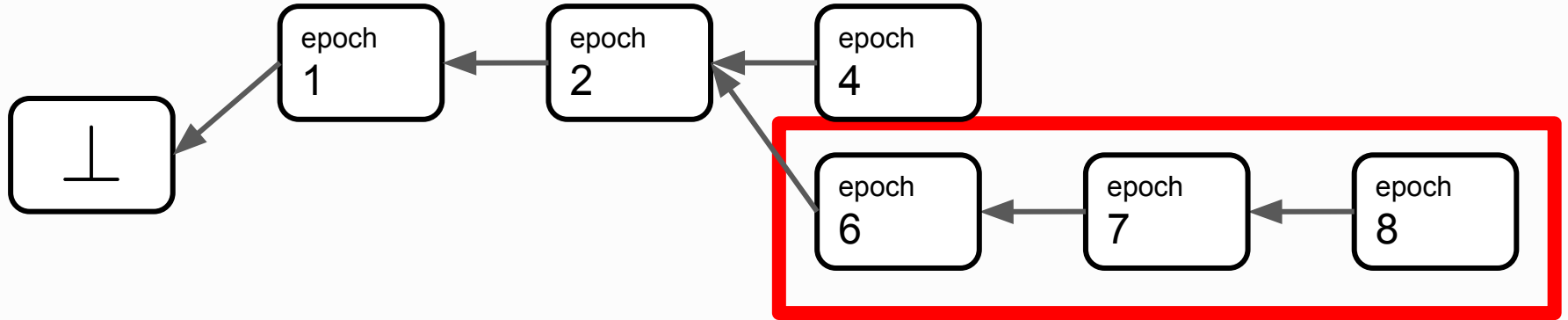
finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block

# Streamlet: blockchain in 2 minutes



finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

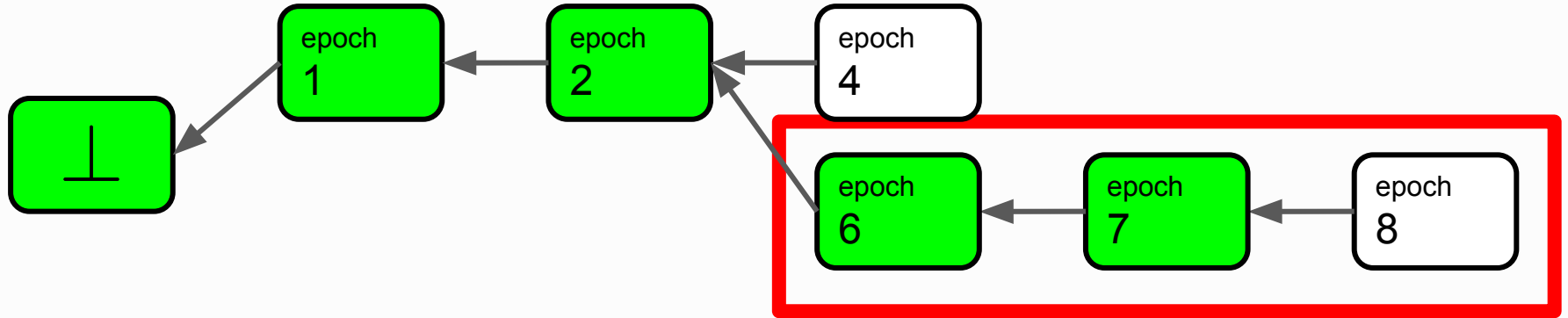
# Streamlet: blockchain in 2 minutes



finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

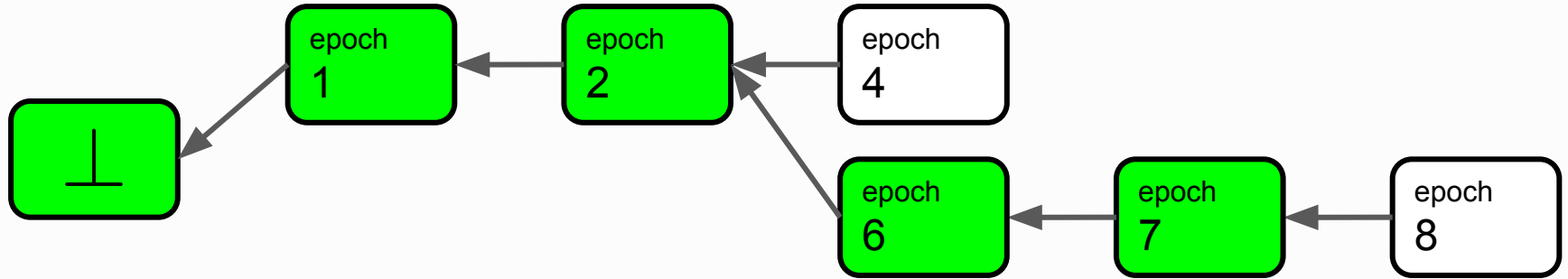


# Streamlet: blockchain in 2 minutes



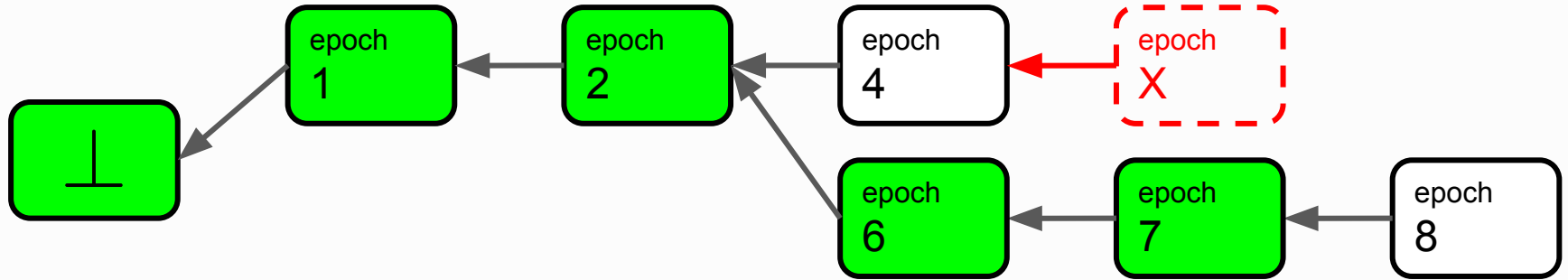
finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

# Streamlet: blockchain in 2 minutes



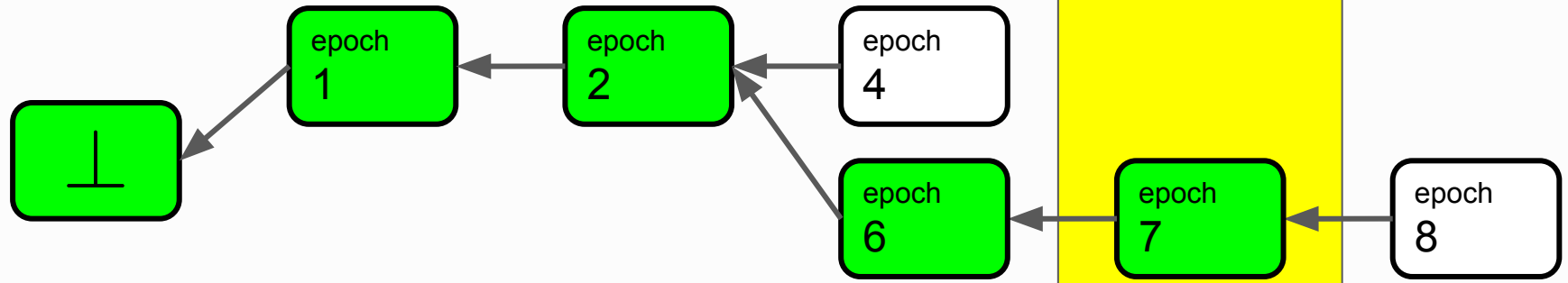
finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

# Streamlet: blockchain in 2 minutes



finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

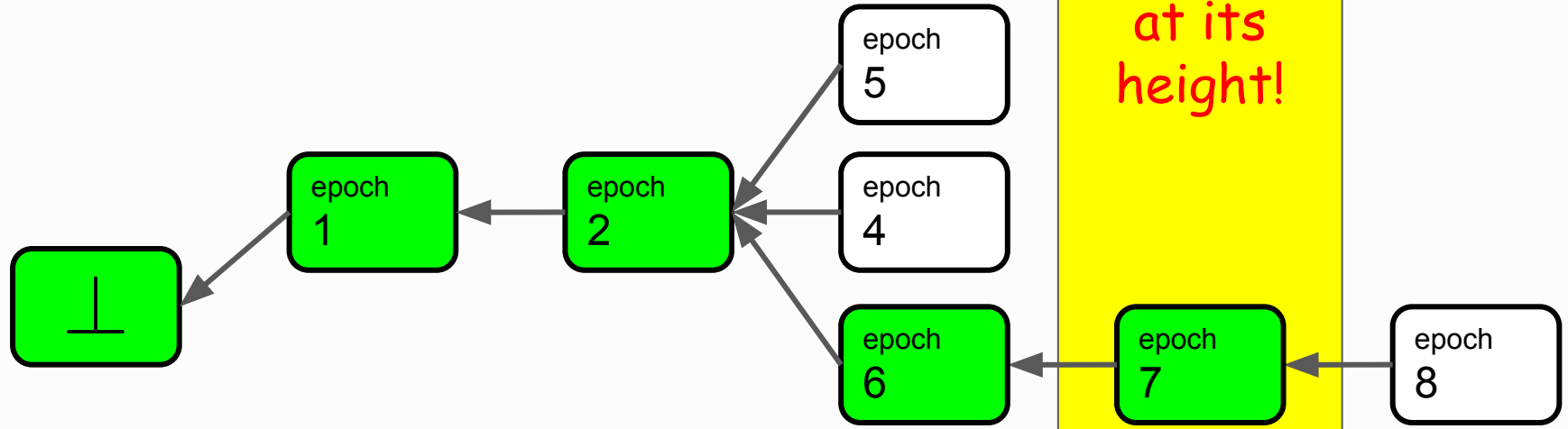
# Streamlet: blockchain in 2 minutes



Unique  
at its  
height!

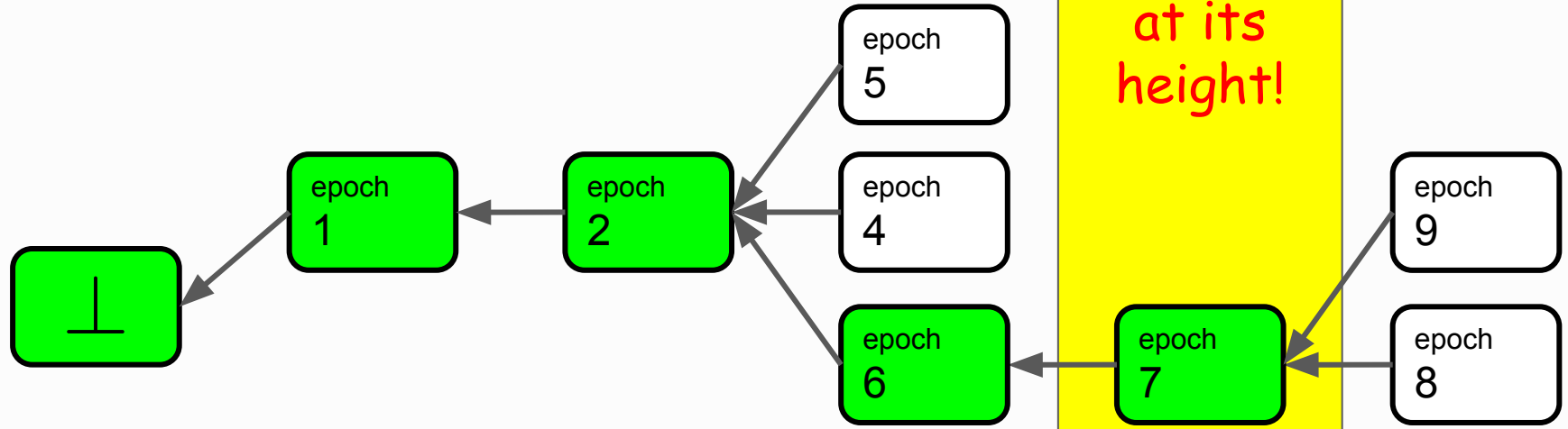
finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block

# Streamlet: blockchain in 2 minutes



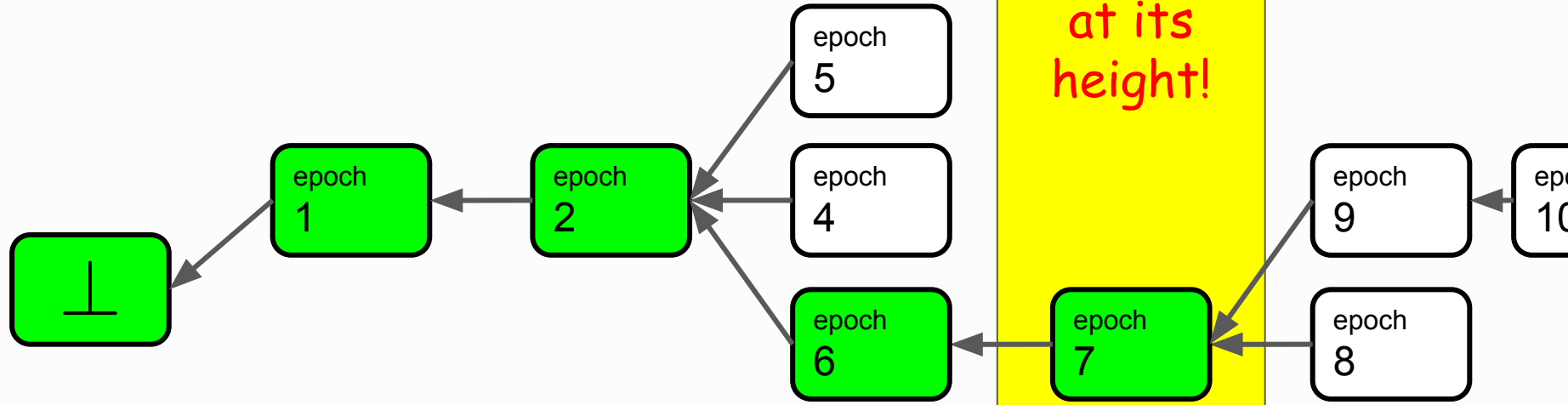
finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block

# Streamlet: blockchain in 2 minutes



finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block

# Streamlet: blockchain in 2 minutes



Unique  
at its  
height!

finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block

# Streamlet: a perfect protocol (for you) to teach!

- $n$  players,  $f < n/3$  malicious.
- partially synchronous
- $>2n/3$  players vote for a block  $\rightarrow$  “notarized”

In every epoch  $e = 1, 2, 3\dots$

- ❑ leader proposes a block  $b$  extending longest notarized chain
- ❑ voters vote for  $b$  i.f.f. it extends longest notarized chain

finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block



# Streamlet: a perfect protocol (for you) to teach!

- $n$  players,  $f < n/3$  malicious
- partially synchronous
- $> 2n/3$  players vote for a block



[eprint.iacr.org/2020/088](https://eprint.iacr.org/2020/088)



In every epoch  $e = 1, 2, 3, \dots$

- ❑ leader proposes a block  $b$  extending longest notarized chain
- ❑ voters vote for  $b$  if it extends longest notarized chain

finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block

# Streamlet: a perfect protocol (for you) to teach!

- $n$  players,  $f < n/3$  malicious
- partially synchronous
- $> 2n/3$  players vote for a block



[eprint.iacr.org/2020/088](https://eprint.iacr.org/2020/088)  
(or Elaine's book)



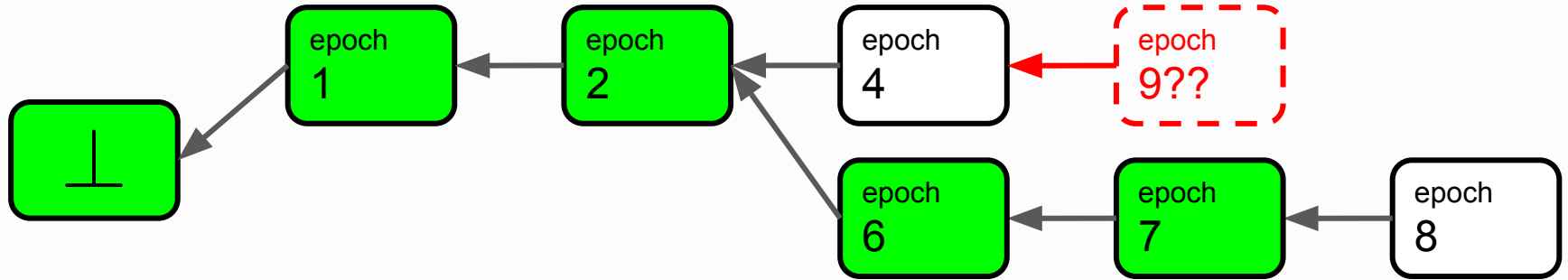
In every epoch  $e = 1, 2, 3, \dots$

- ❑ leader proposes a block  $b$  extending longest notarized chain
- ❑ voters vote for  $b$  if it extends longest notarized chain

finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block

Slides for which I have no time

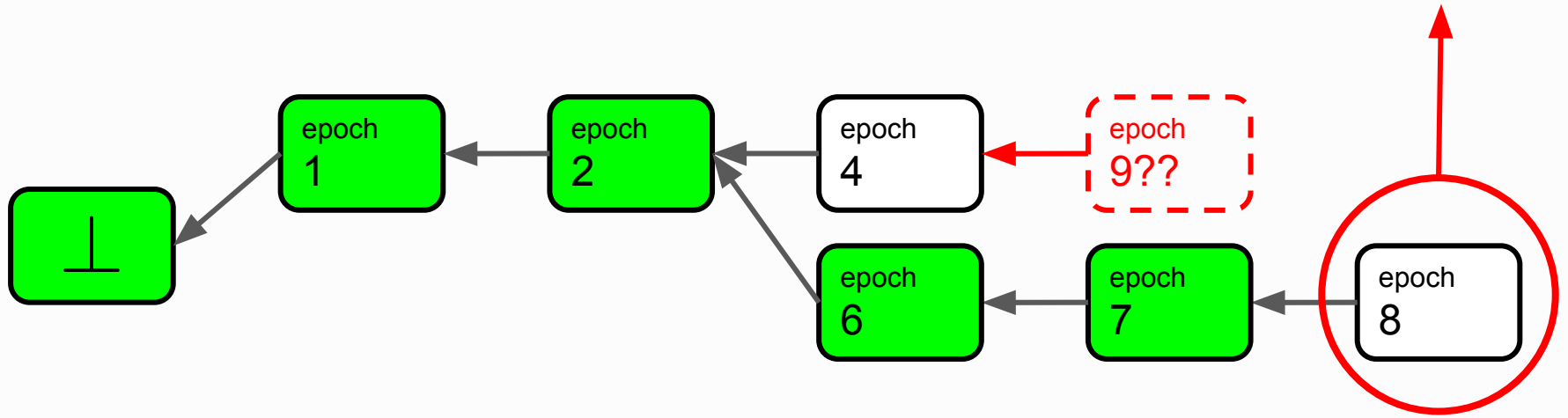
# Streamlet: blockchain in 2 minutes



finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

# Streamlet: blockchain in 2 minutes

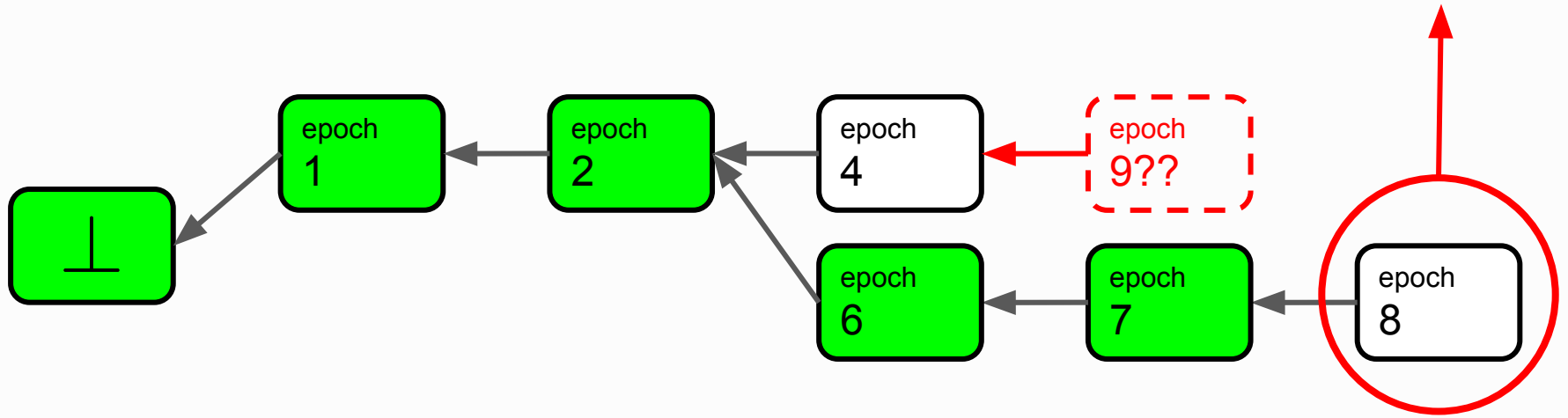
2/3s have seen notarized epoch 7 block!



finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

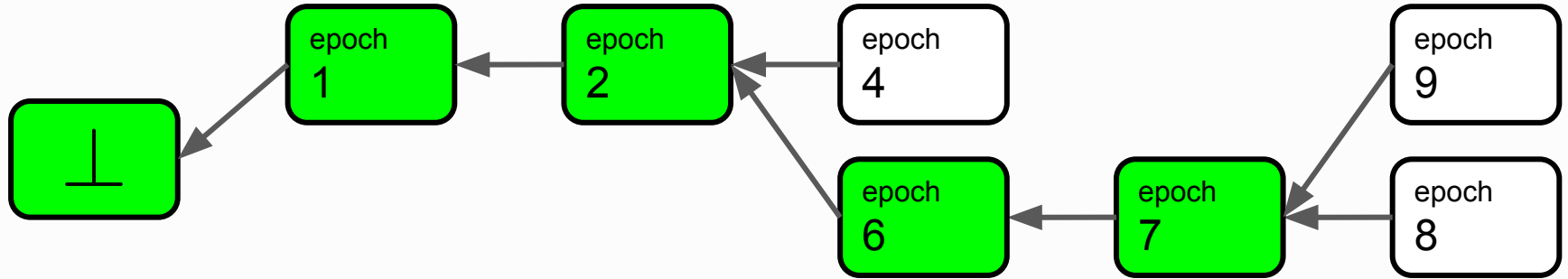
# Streamlet: blockchain in 2 minutes

2/3s have seen notarized epoch 7 block!



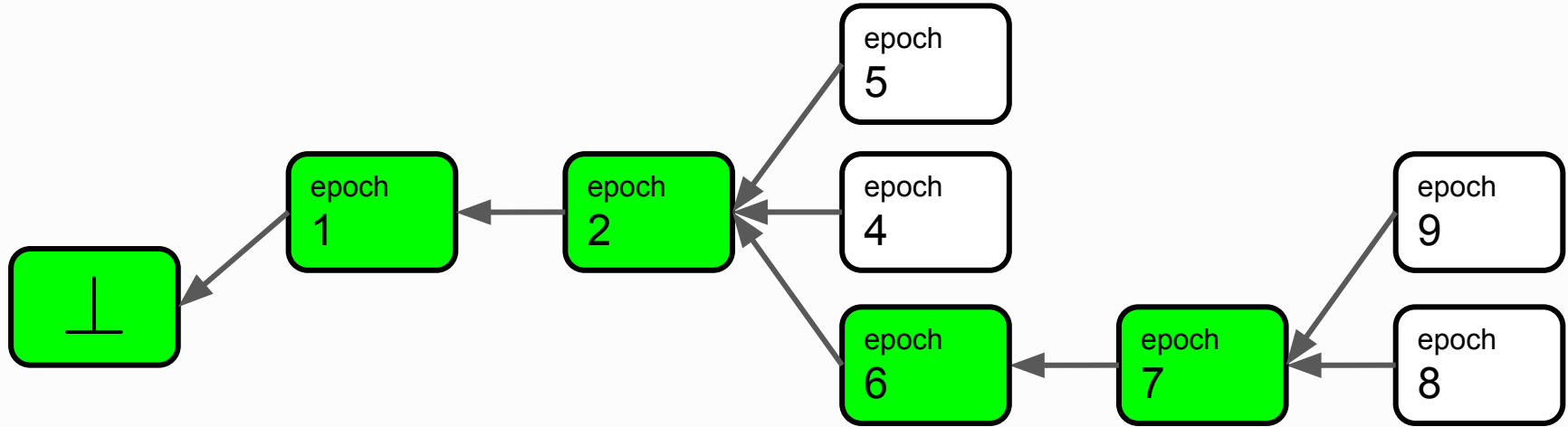
finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

# Streamlet: blockchain in 2 minutes



finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block

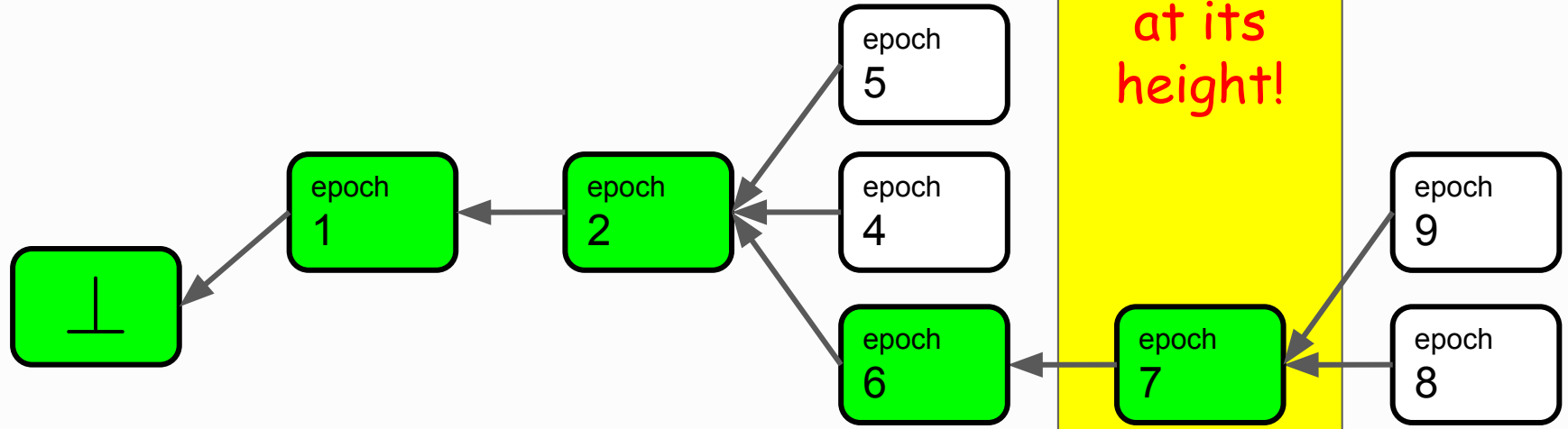
# Streamlet: blockchain in 2 minutes



finalize any chain ending in **3 notarized blocks with consecutive epochs**, chopping off last block



# Streamlet: blockchain in 2 minutes



finalize any chain ending in 3 notarized blocks with consecutive epochs, chopping off last block