

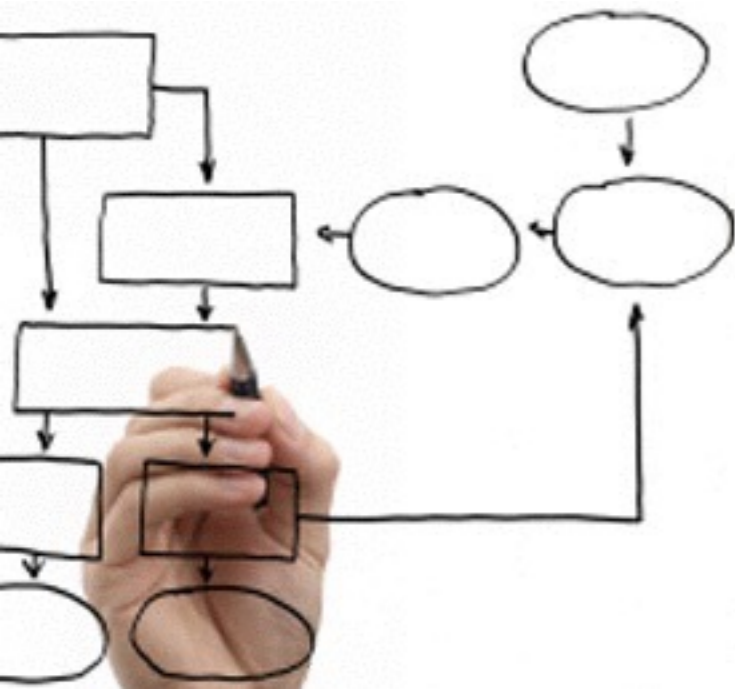
# Methods for the specification and verification of business processes

MPB (6 cfu, 295AA)

Roberto Bruni

<http://www.di.unipi.it/~bruni>

14 - Sound by construction



# Object



We show a technique to build sound  
Workflow nets

# Soundness proof by construction

## Idea

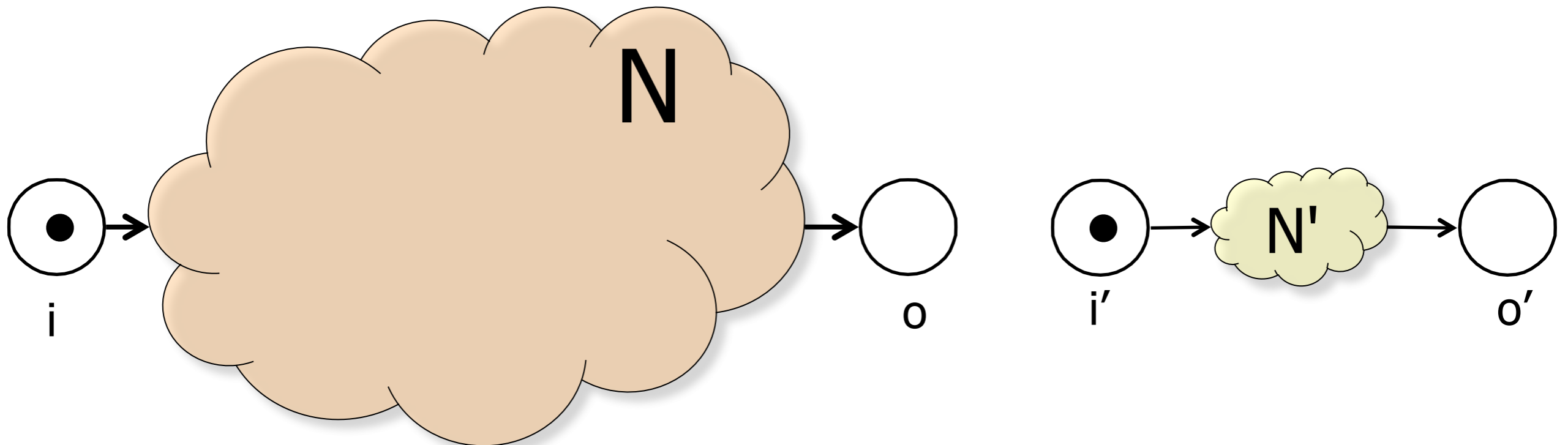
1. Find a suitable set of "building blocks"

they are (small) workflow nets  
that can be (easily) proved  
to be **sound** and  
to be **safe** (1-bounded)

2. Define composition patterns so that  
by composing **safe and sound** WF nets  
we get **safe and sound** WF nets

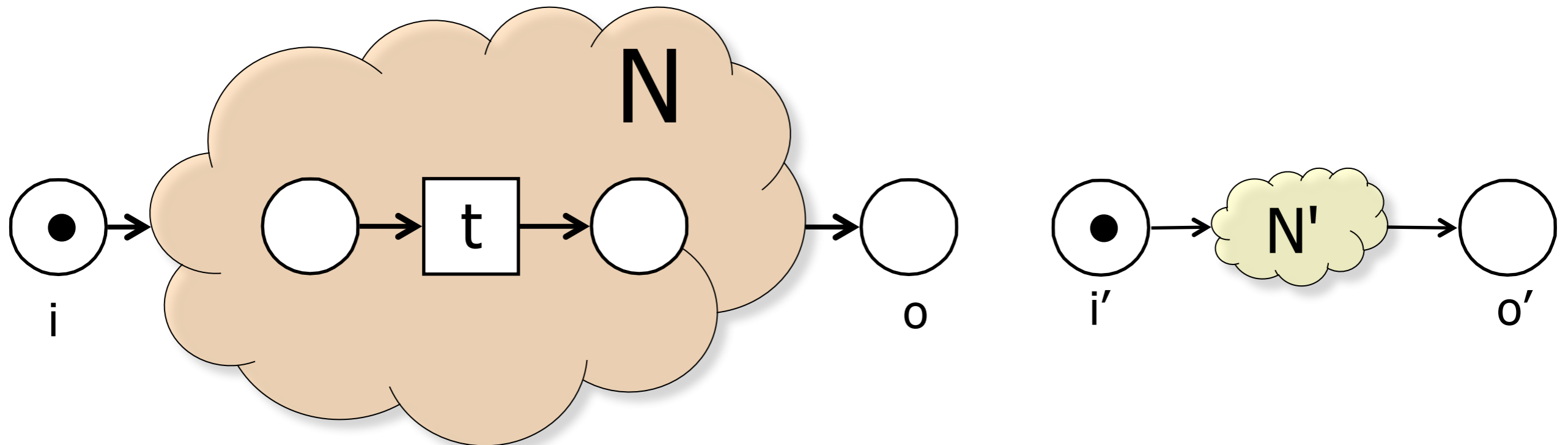
# Sound and safe by composition

Let  $N$ ,  $N'$  be two safe and sound workflow nets



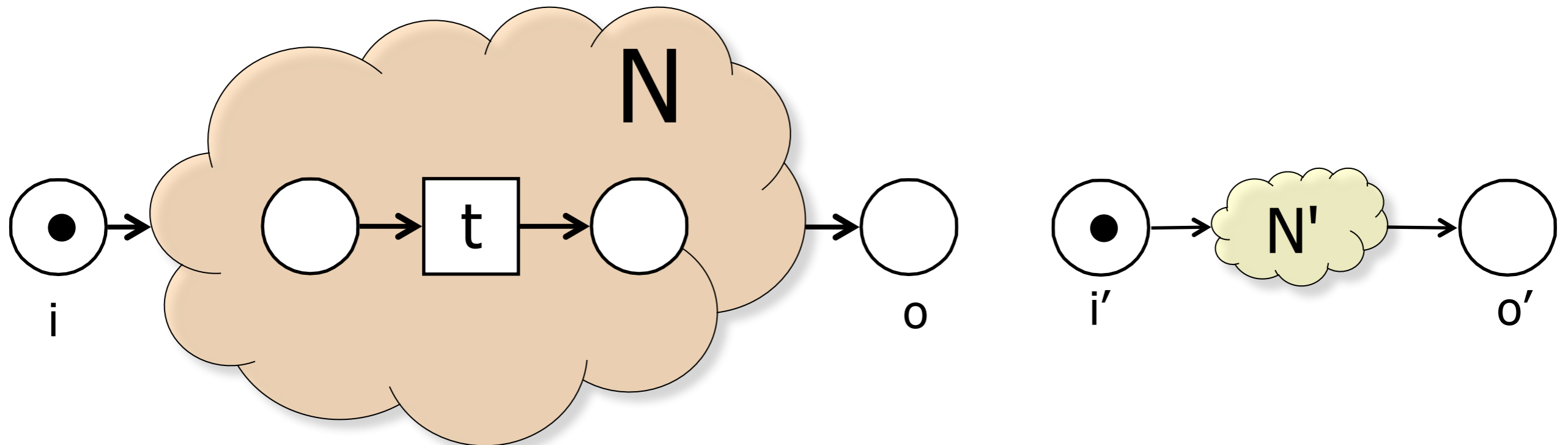
# Sound and safe by composition

Let  $t$  be a task of  $N$  with exactly one input and one output place



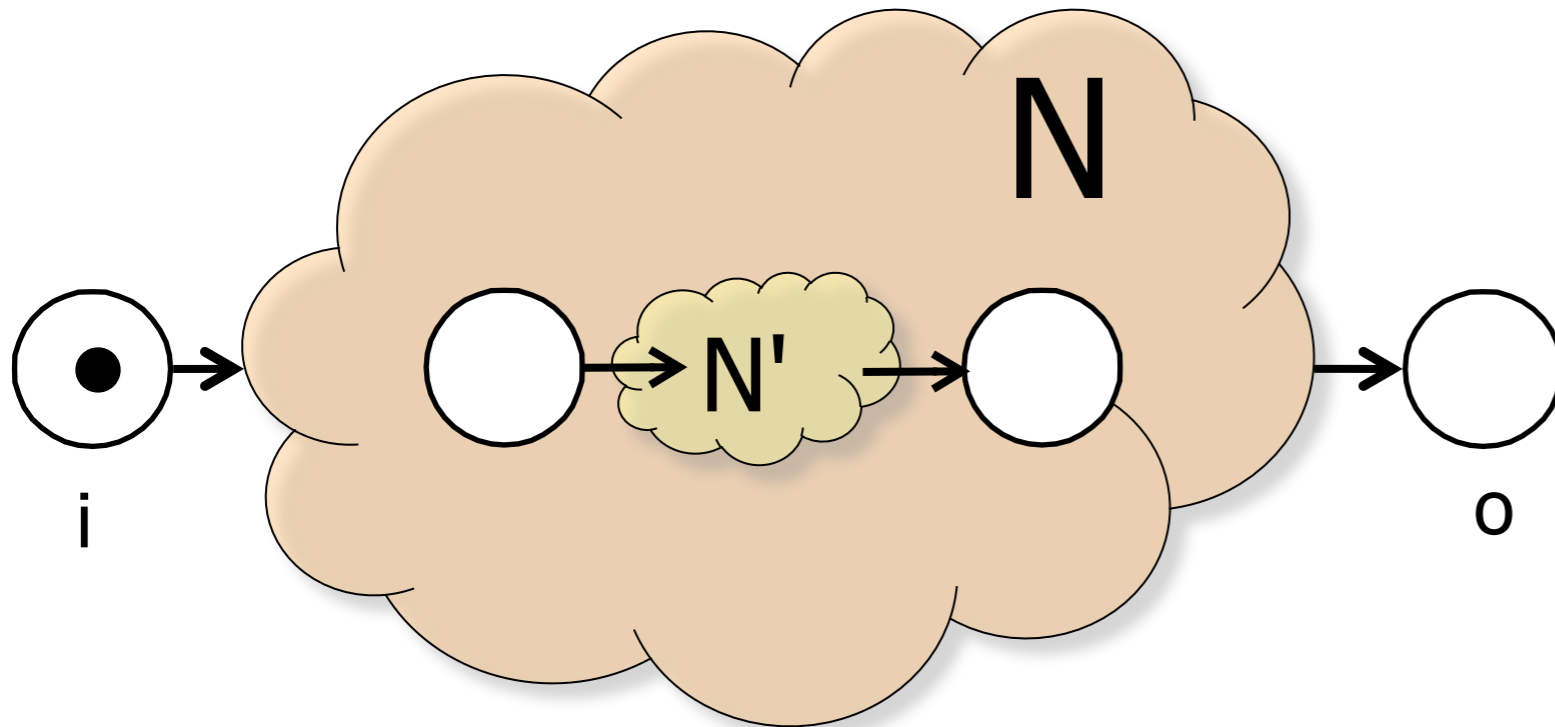
# Sound and safe by composition

Let  $N[N'/t]$  denote the net obtained by replacing the task  $t$  in  $N$  by  $N'$



# Sound and safe by composition

The net  $N[N'/t]$  is  
a **sound and safe workflow net**  
(proof omitted)



# Proof sketch

## **Intuitively**

a sound workflow net behaves as a transition:  
it takes one token from its input place and  
it produces one token to its output place  
(but not atomically)

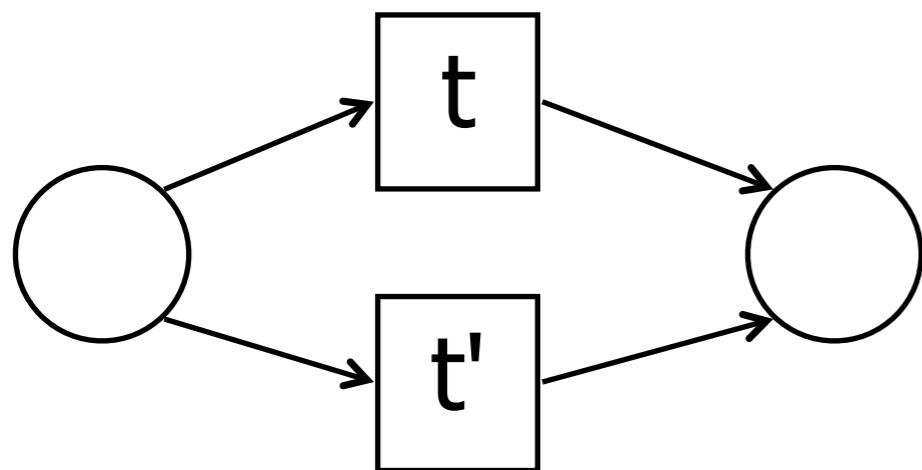
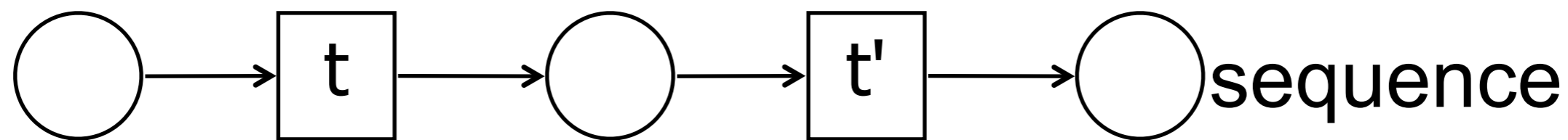
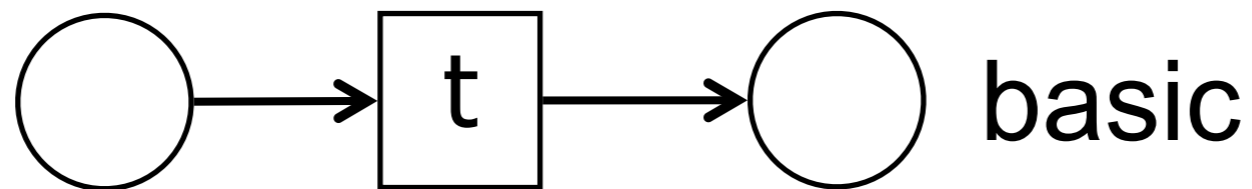
## **Formally**

the crux of the proof is showing a bijective correspondence  
between

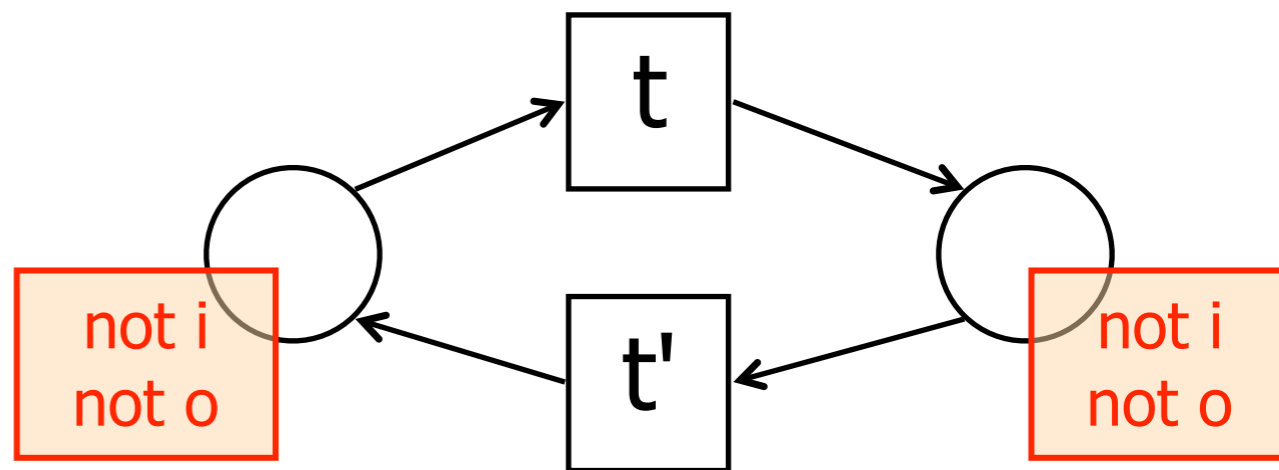
markings of the composed net  $N[N'/t]$   
and the pairs of markings in  $N$  and  $N'$



# Some Building Blocks 1

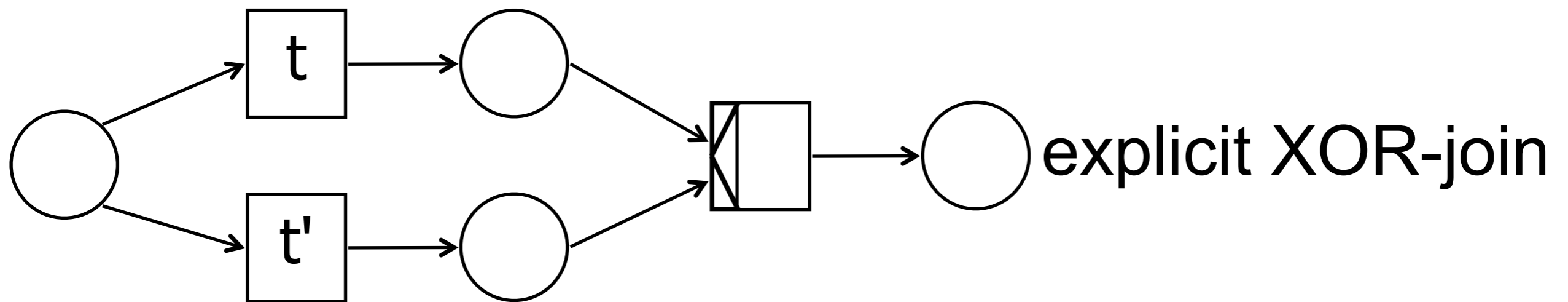
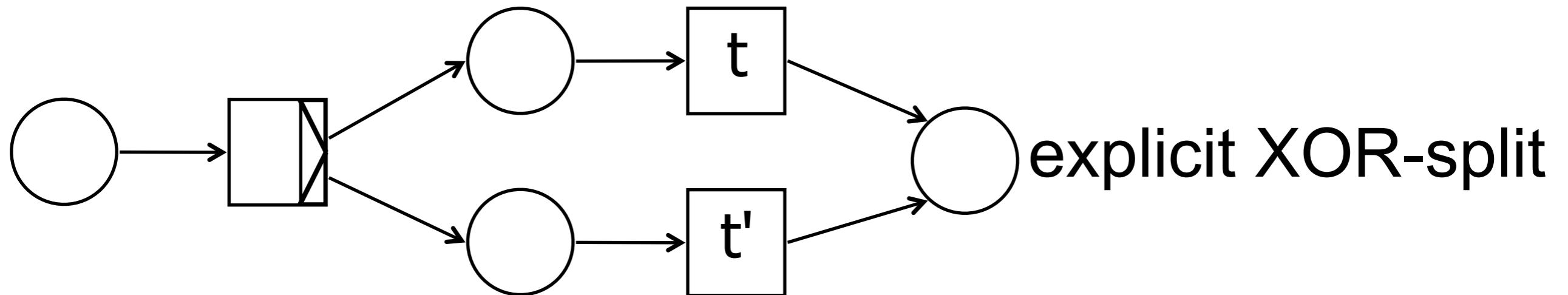


implicit XOR

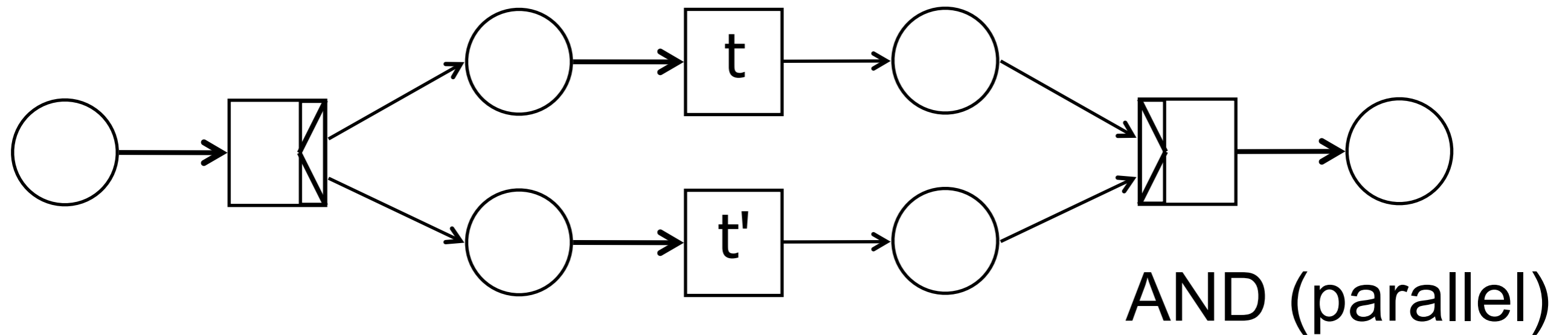


iteration

# Some Building Blocks 2

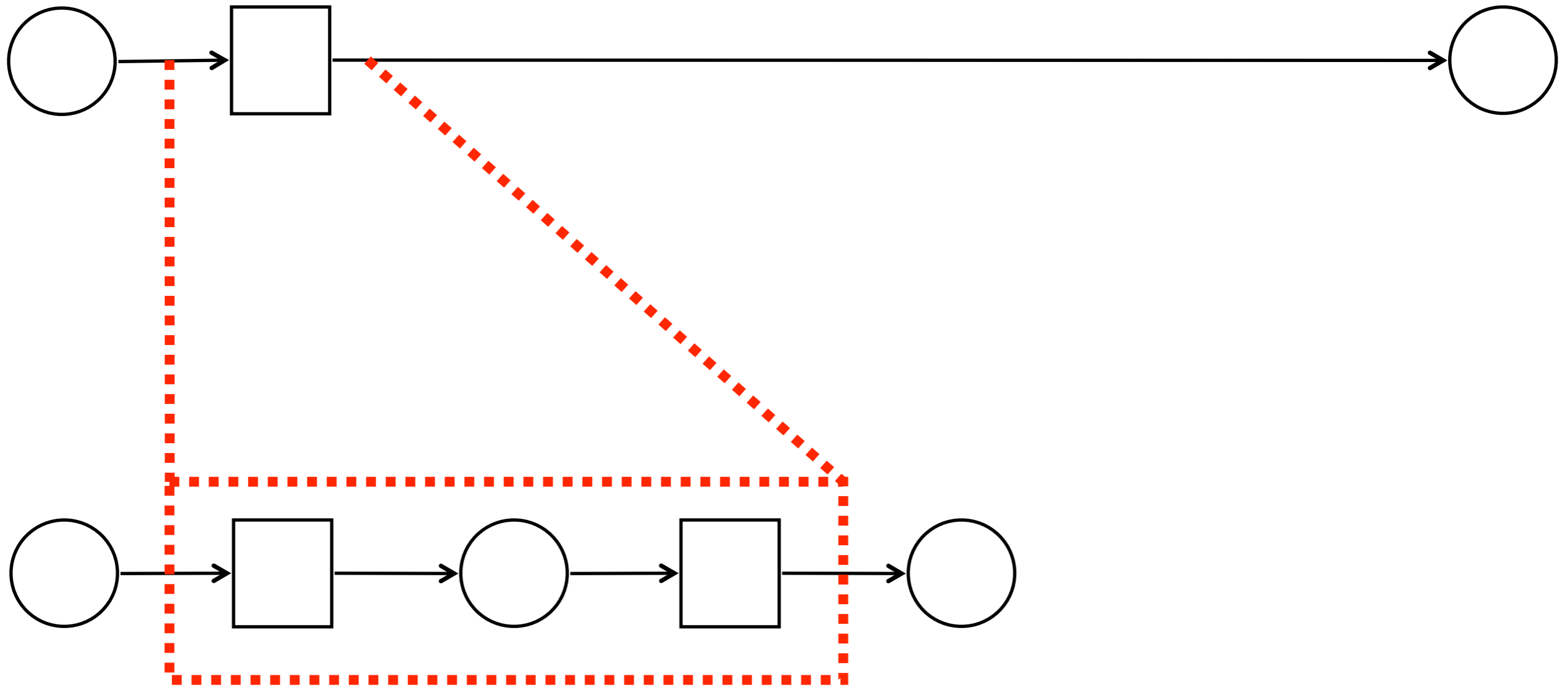


# Some Building Blocks 3

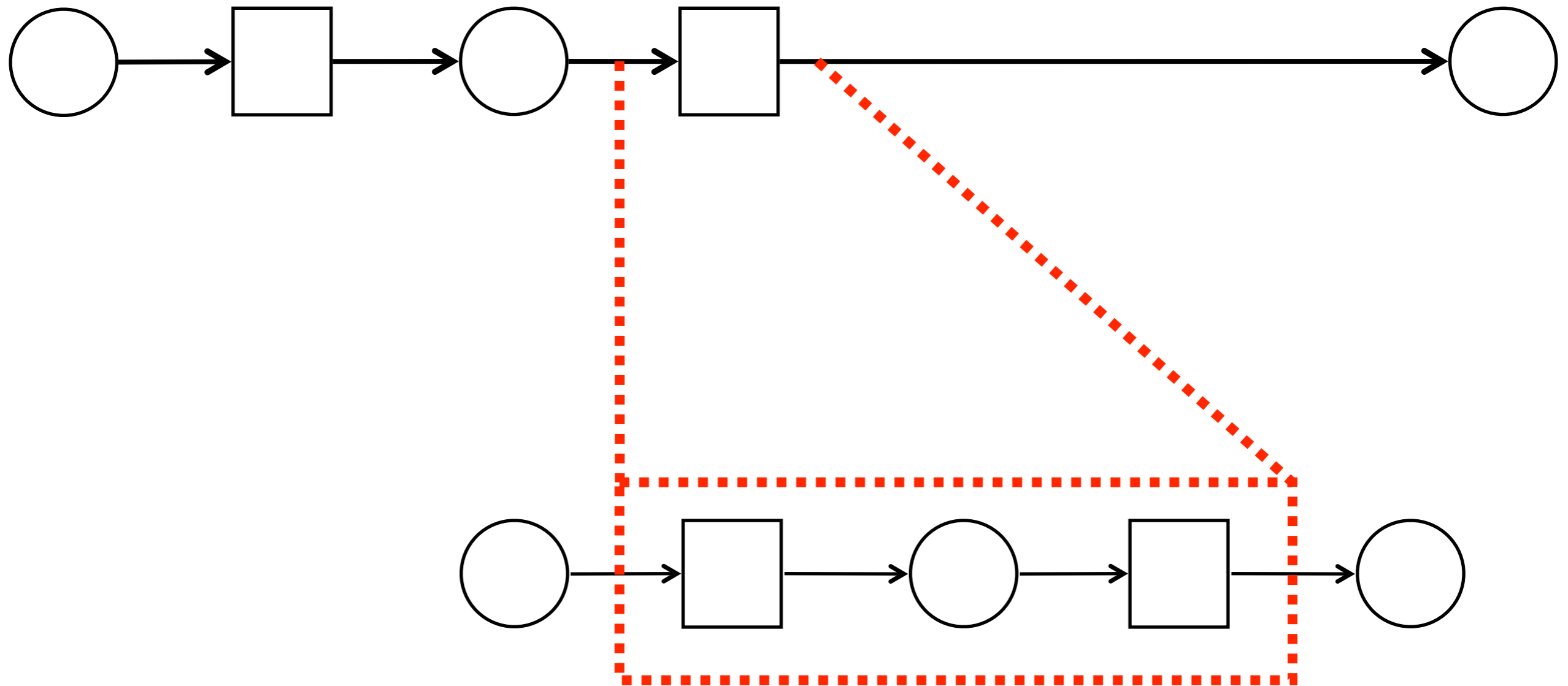


But you can define more blocks on your own

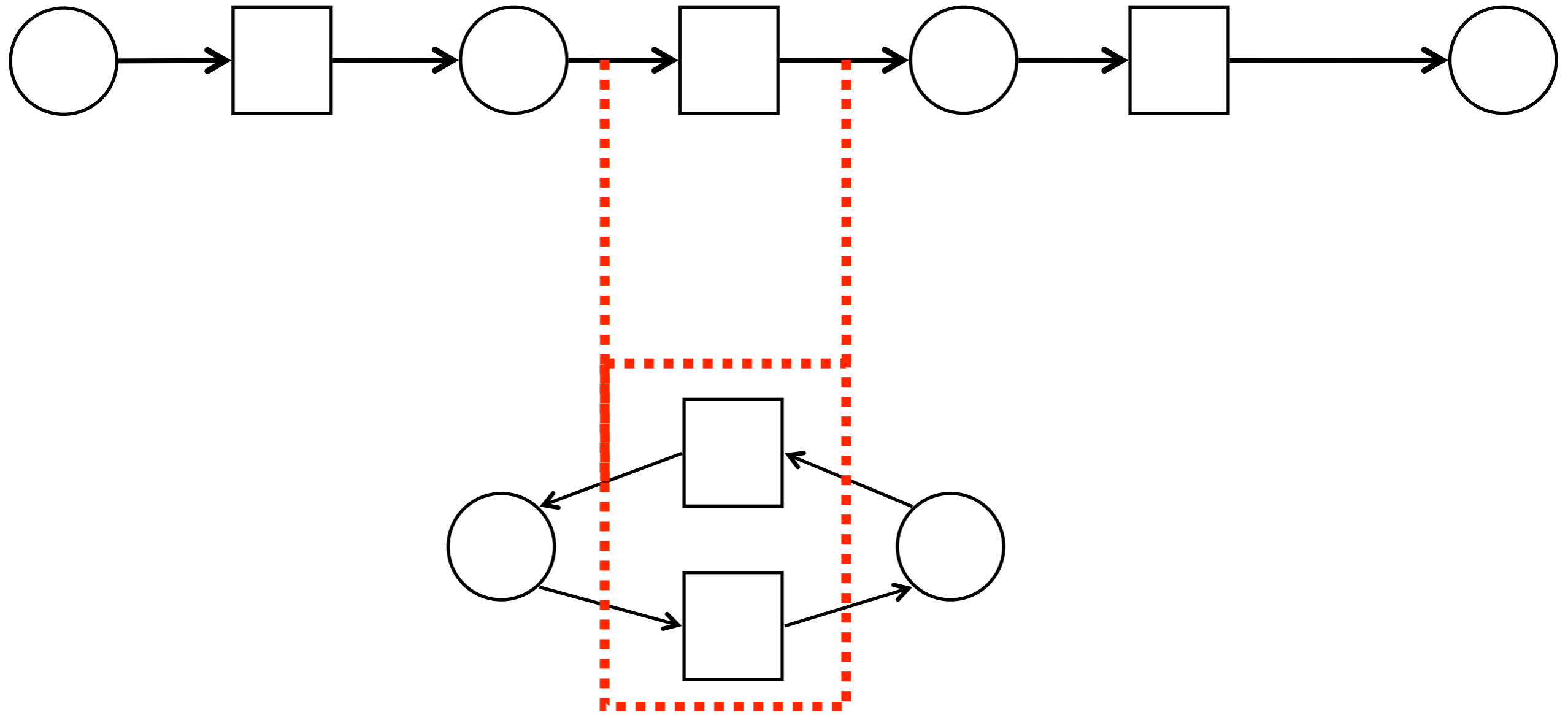
# Example



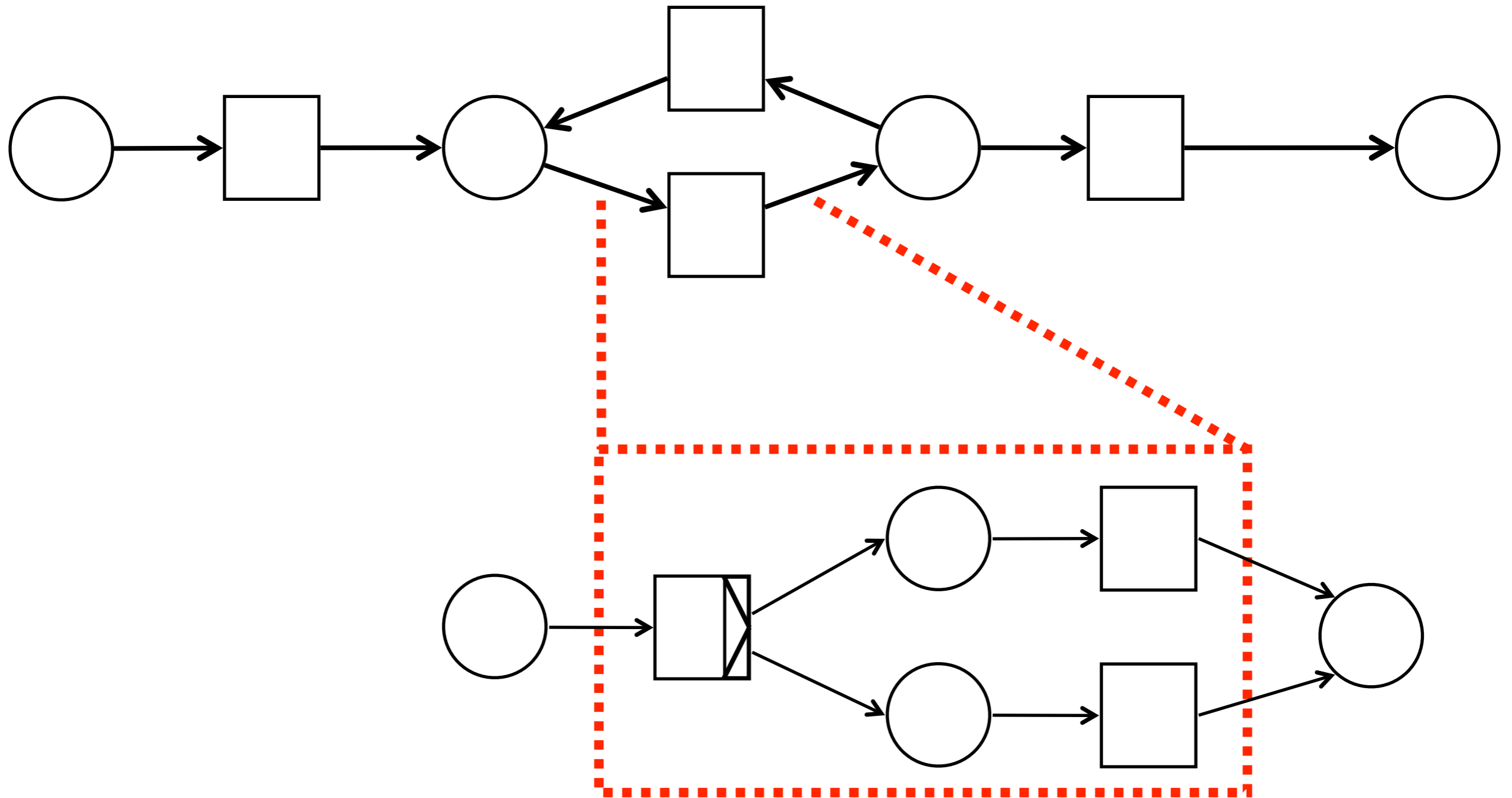
# Example



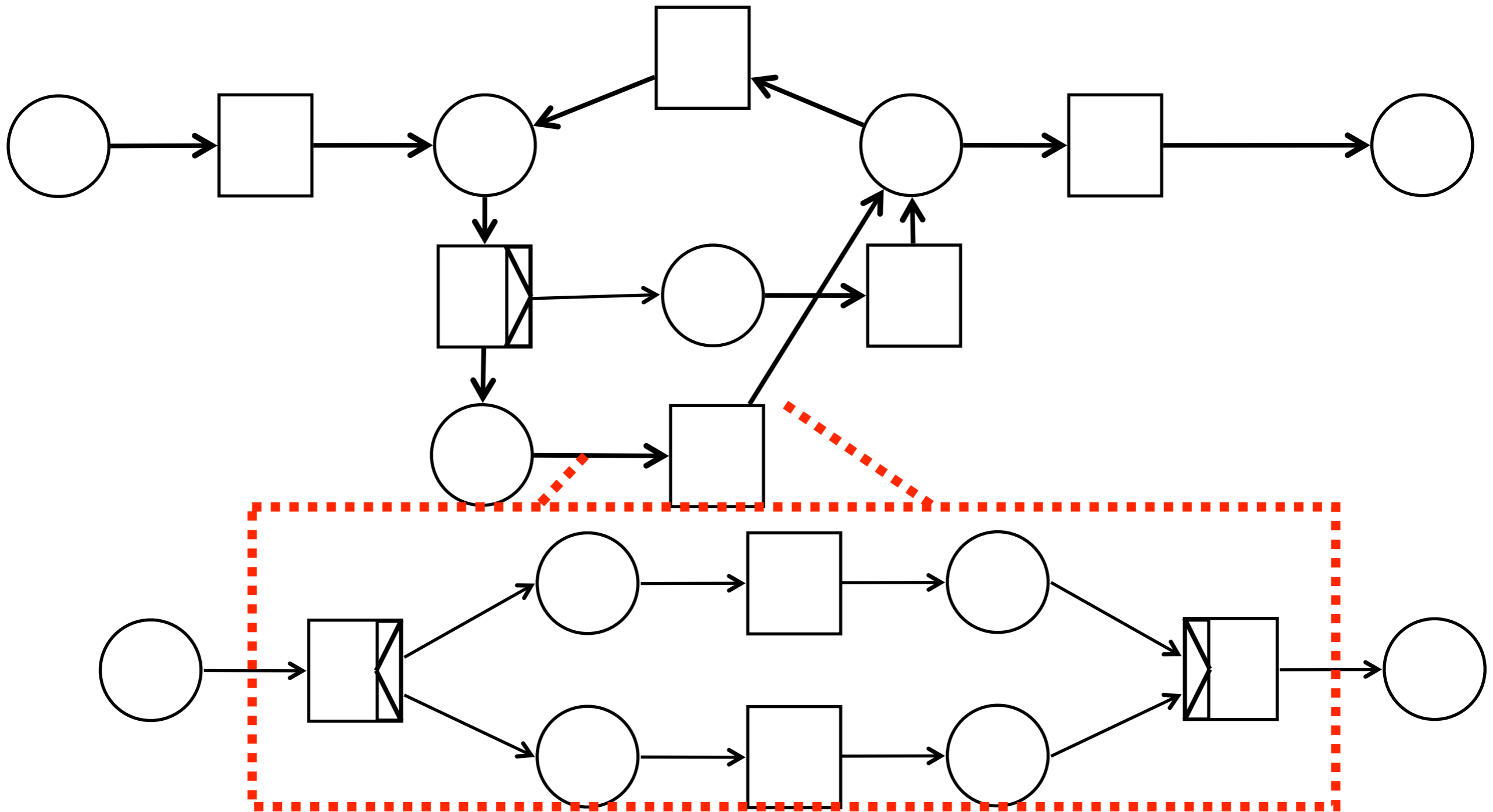
# Example



# Example

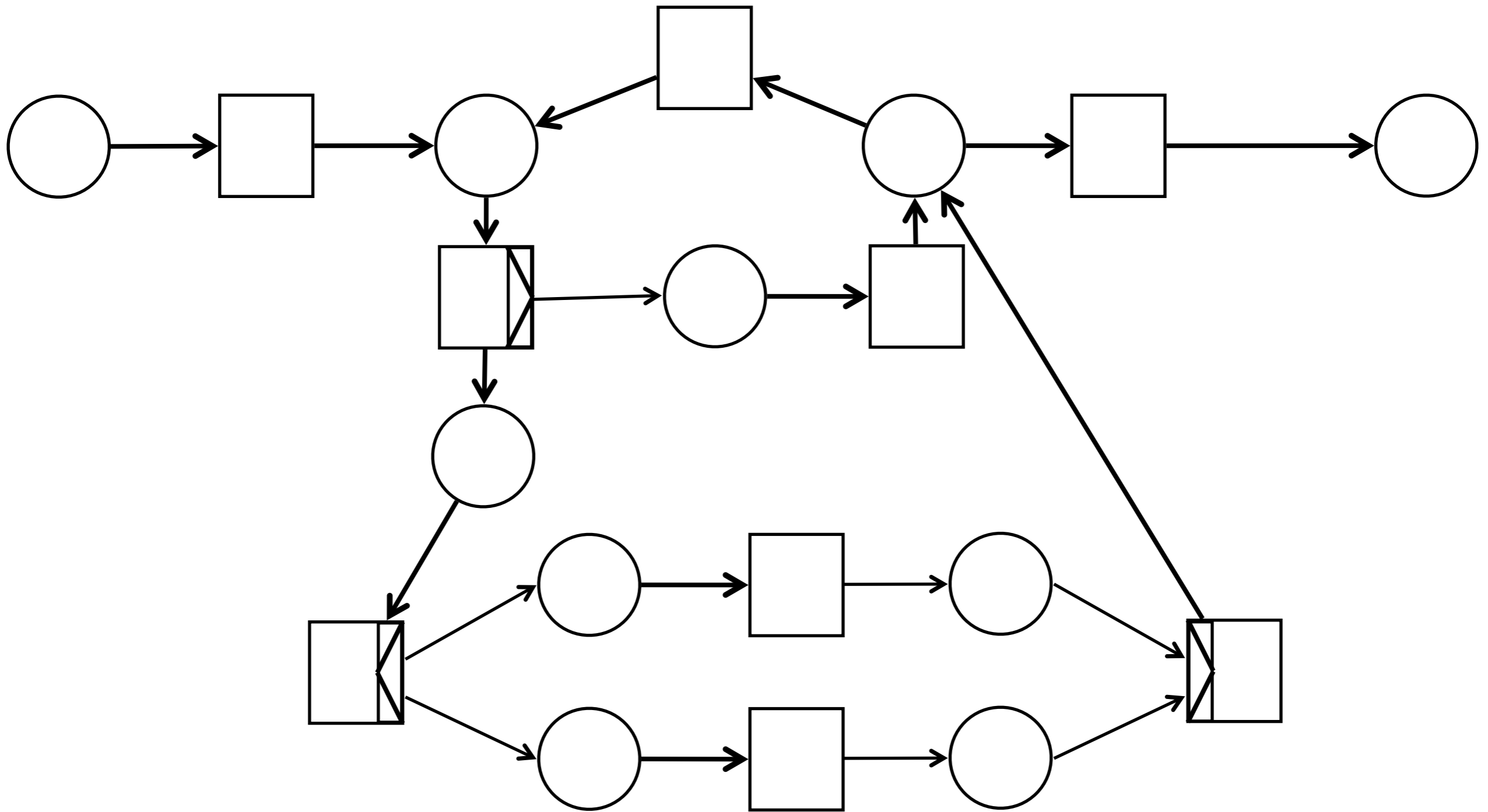


# Example



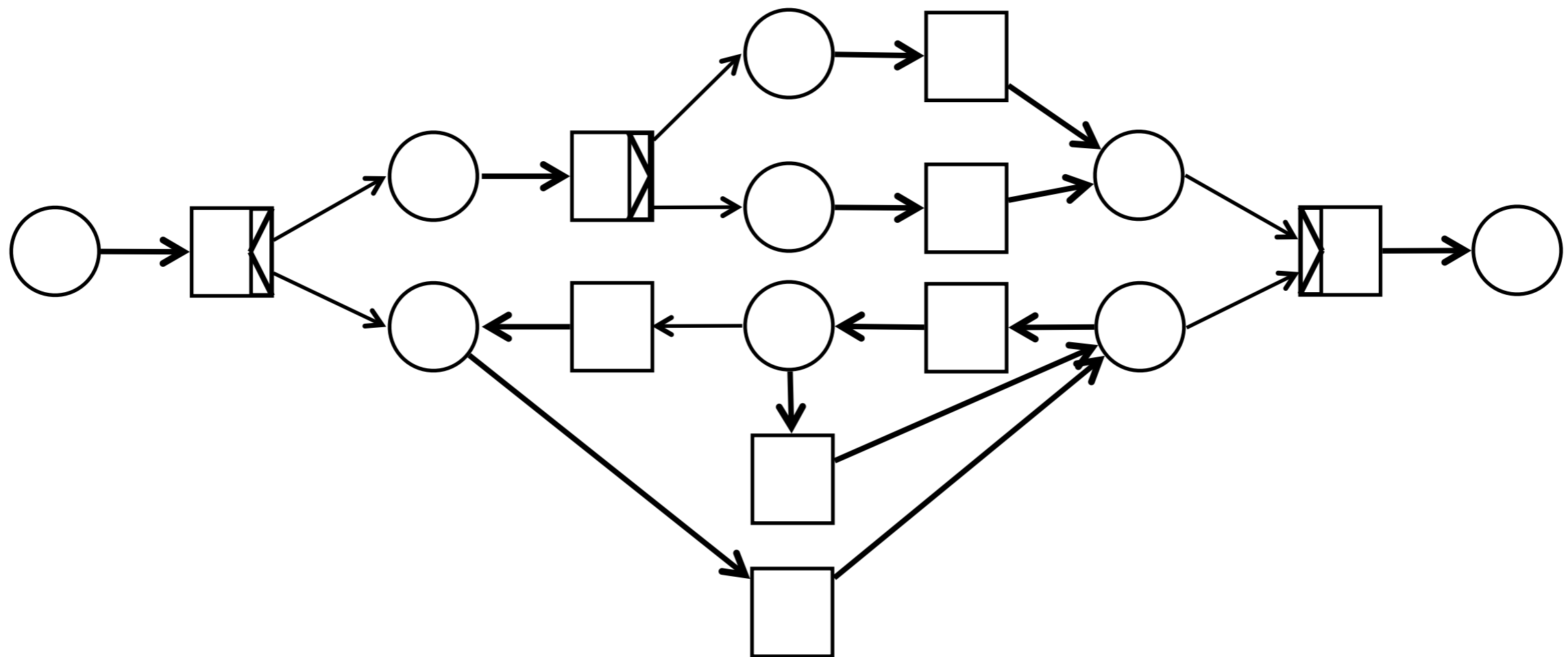


# Example



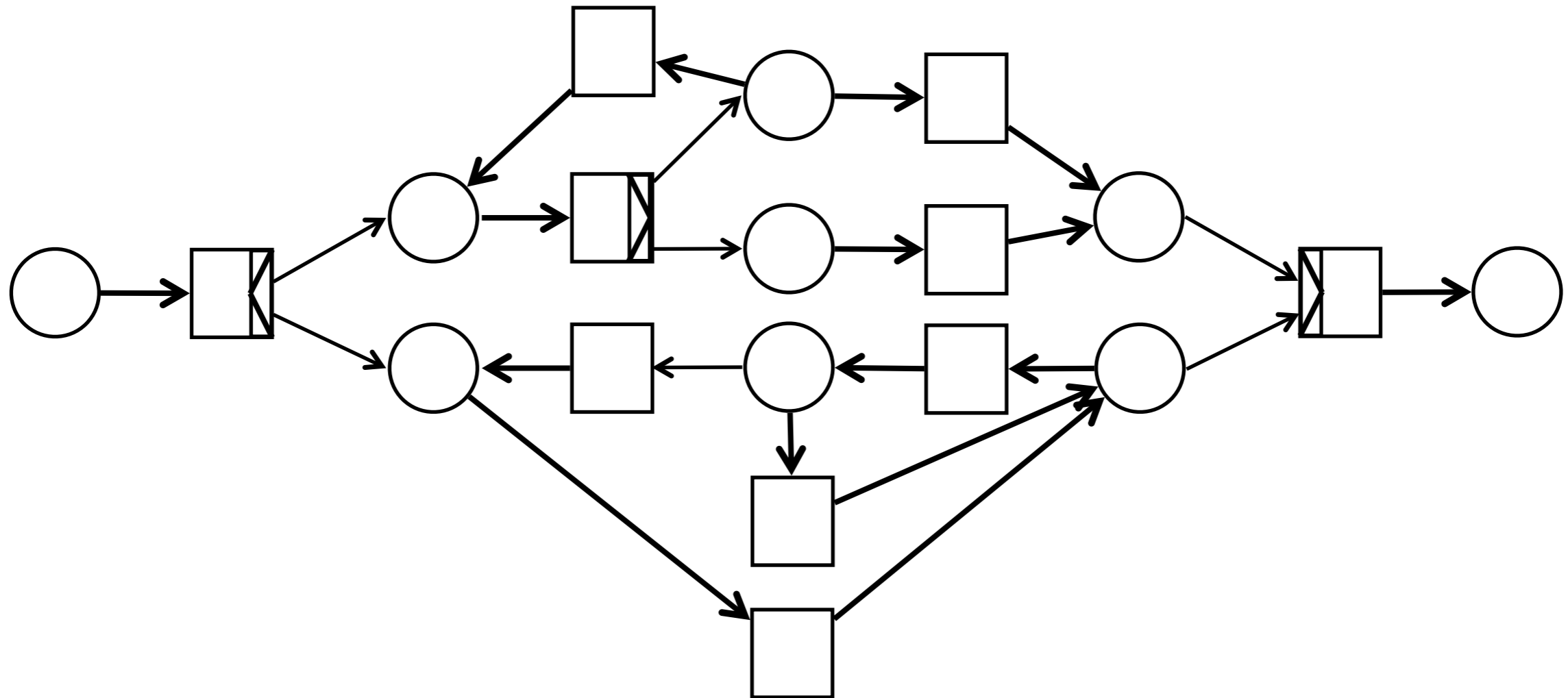
# Exercise

Prove that the net below is  
a safe and sound workflow net



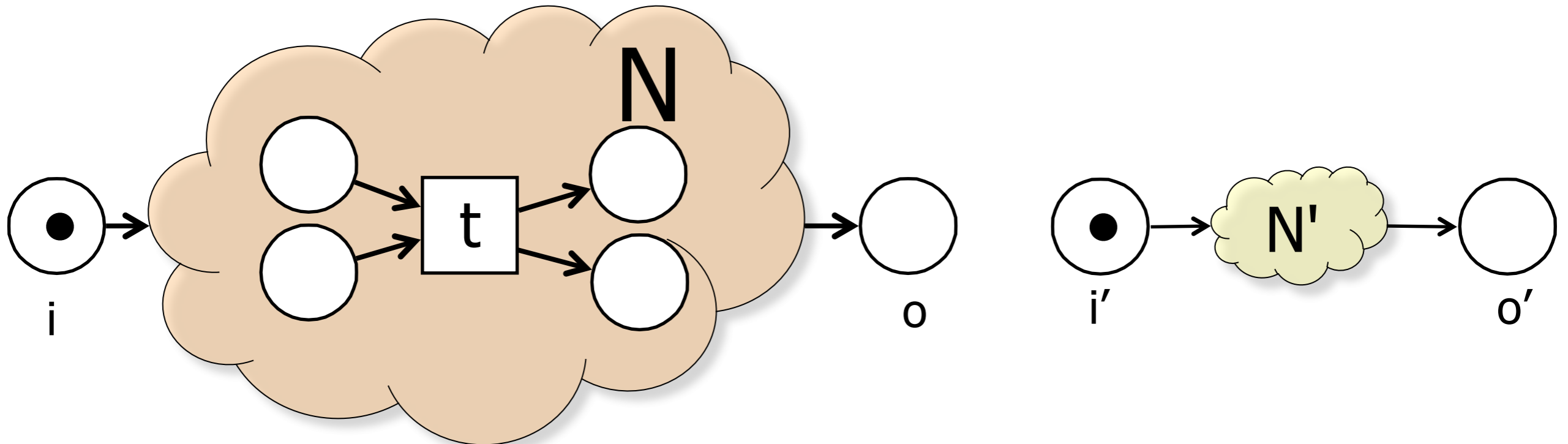
# Exercise

Prove that the net below is a safe and sound workflow net (hint: "desugar" it)



# Generalization

We would like to progressively refine transitions with multiple incoming and outgoing arcs



# Two facts

**Lemma:** Let  $N$  be a sound WF net.  
If  $(i,t) \in F$  then the pre-set of  $t$  is  $\{i\}$

(otherwise  $t$  would be a dead transition)

**Lemma:** Let  $N$  be a sound WF net.  
If  $(t,o) \in F$  then the post-set of  $t$  is  $\{o\}$

(otherwise  $t$  would be dead or proper completion would not hold)

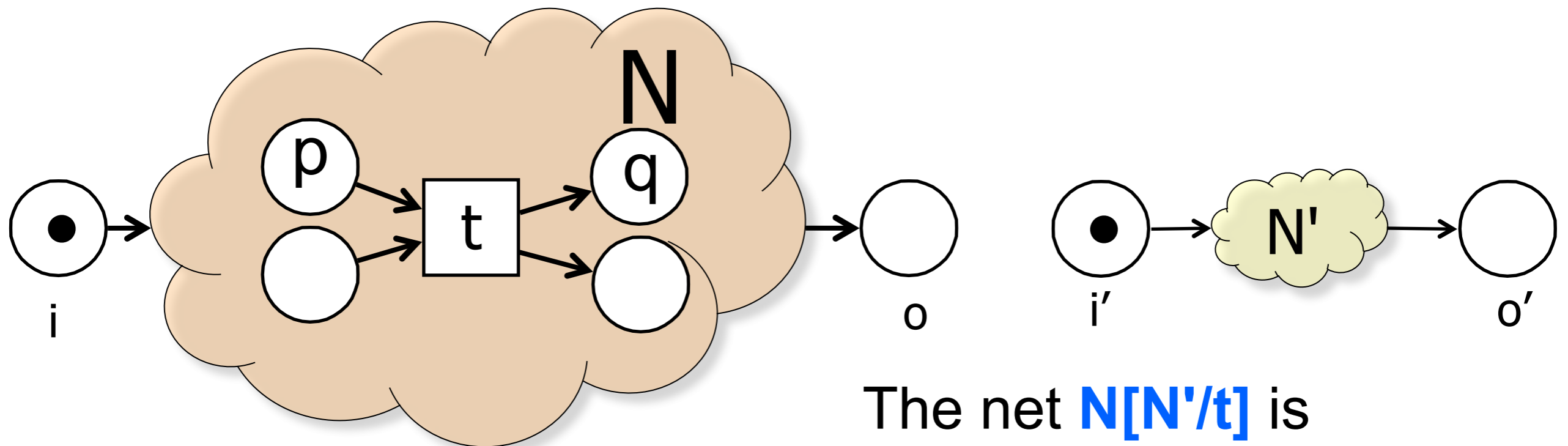
# General replacement

Let  $T_{i'} = \{ u \mid \bullet u = \{i'\} \}$ .

Let  $T_{o'} = \{ v \mid v\bullet = \{o'\} \}$ .

If  $(p, t) \in F_N, u \in T_{i'}$  then  $(p, u) \in F_{N[N'/t]}$

If  $(t, q) \in F_N, v \in T_{o'}$  then  $(v, q) \in F_{N[N'/t]}$



The net  $N[N'/t]$  is  
a **sound and safe workflow net**

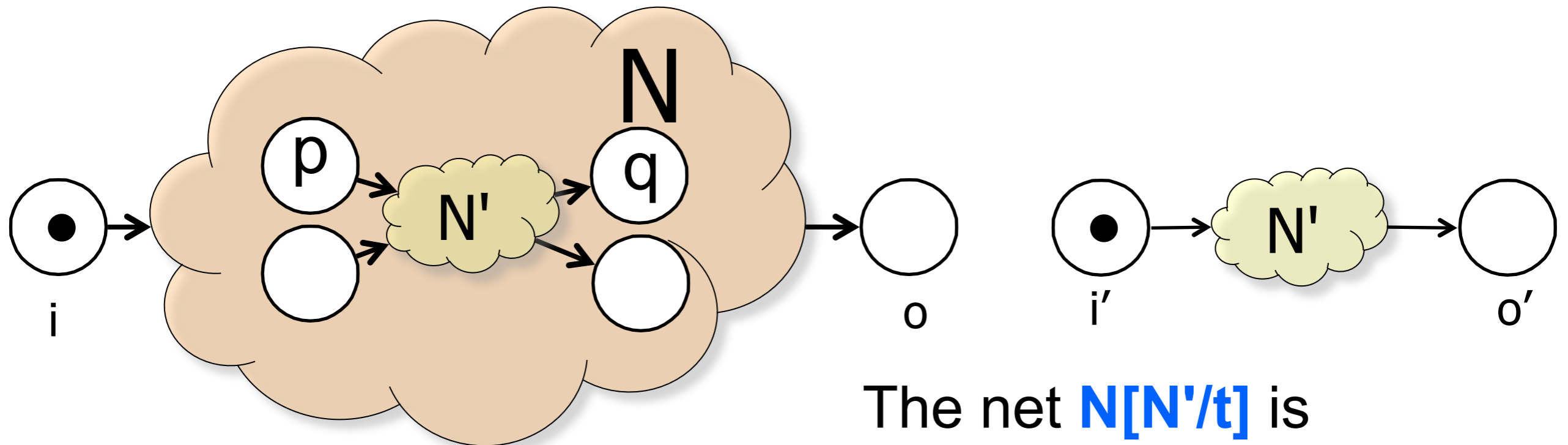
# General replacement

Let  $T_{i'} = \{ u \mid \bullet u = \{i'\} \}$ .

Let  $T_{o'} = \{ v \mid v\bullet = \{o'\} \}$ .

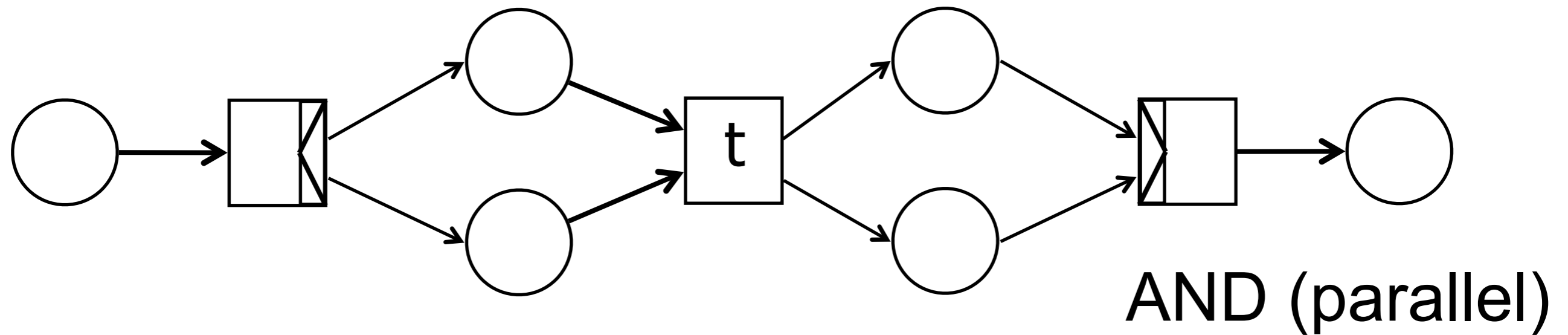
If  $(p, t) \in F_N, u \in T_{i'}$  then  $(p, u) \in F_{N[N'/t]}$

If  $(t, q) \in F_N, v \in T_{o'}$  then  $(v, q) \in F_{N[N'/t]}$



The net  $N[N'/t]$  is  
a **sound and safe workflow net**

# Some Building Blocks 4



But you can define more blocks on your own



# Exercise

Prove that the net below is a safe and sound workflow net

