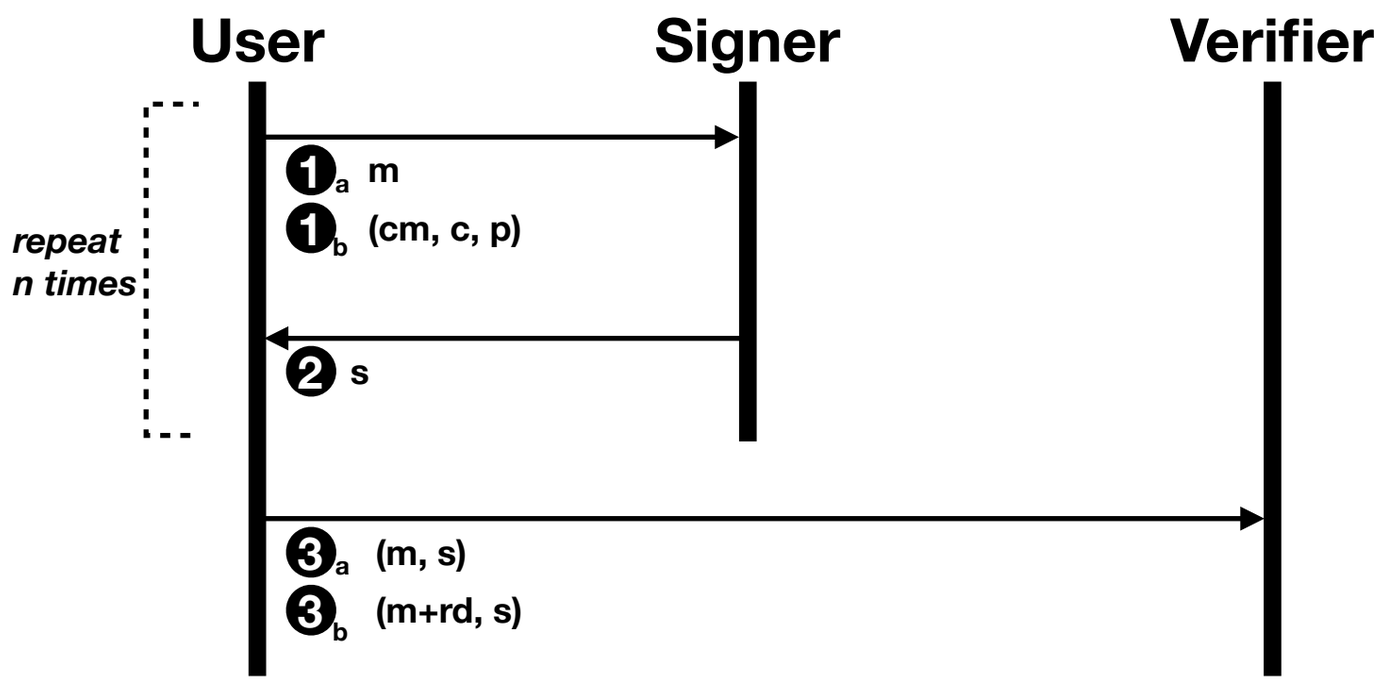
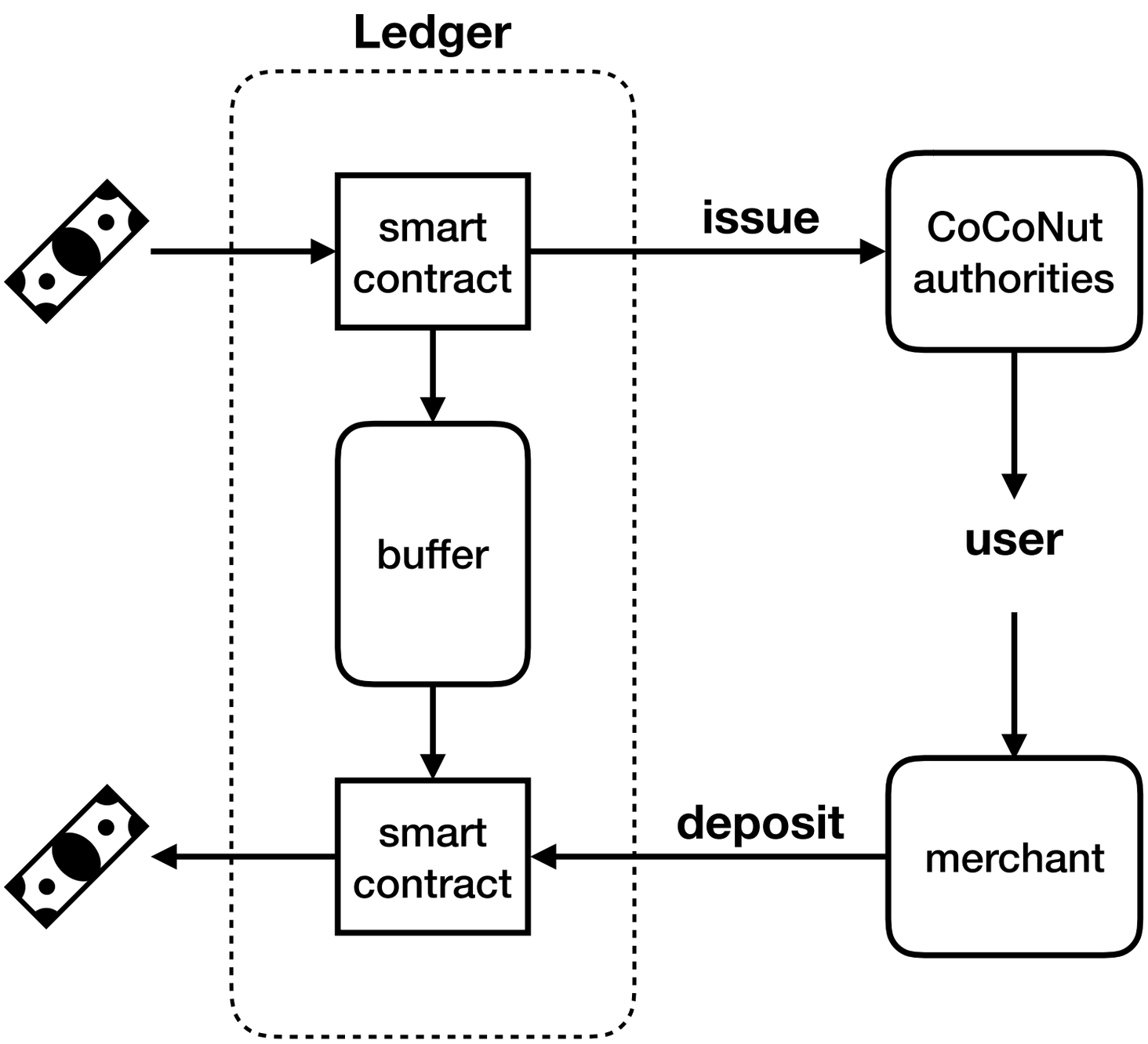
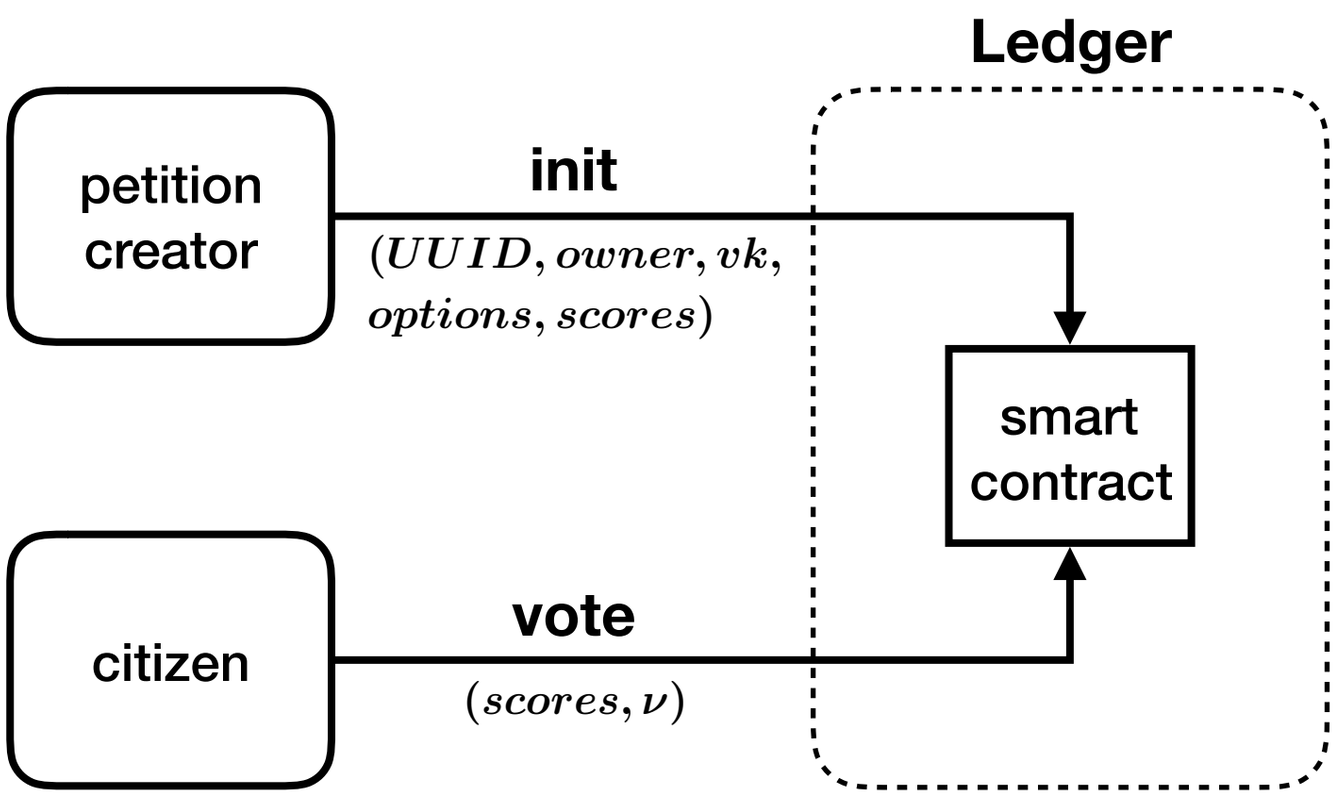
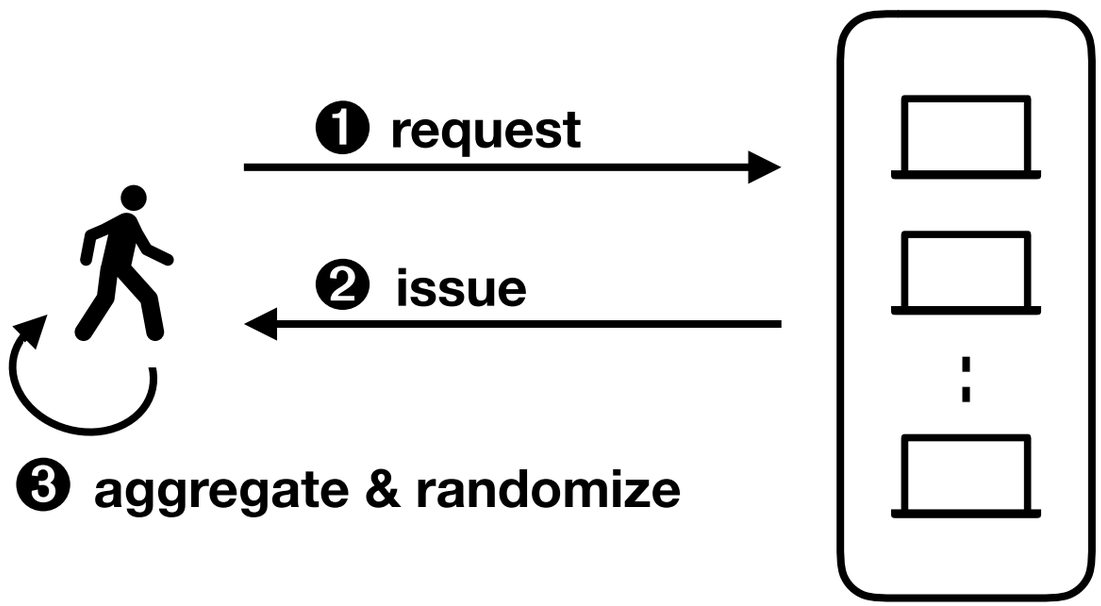
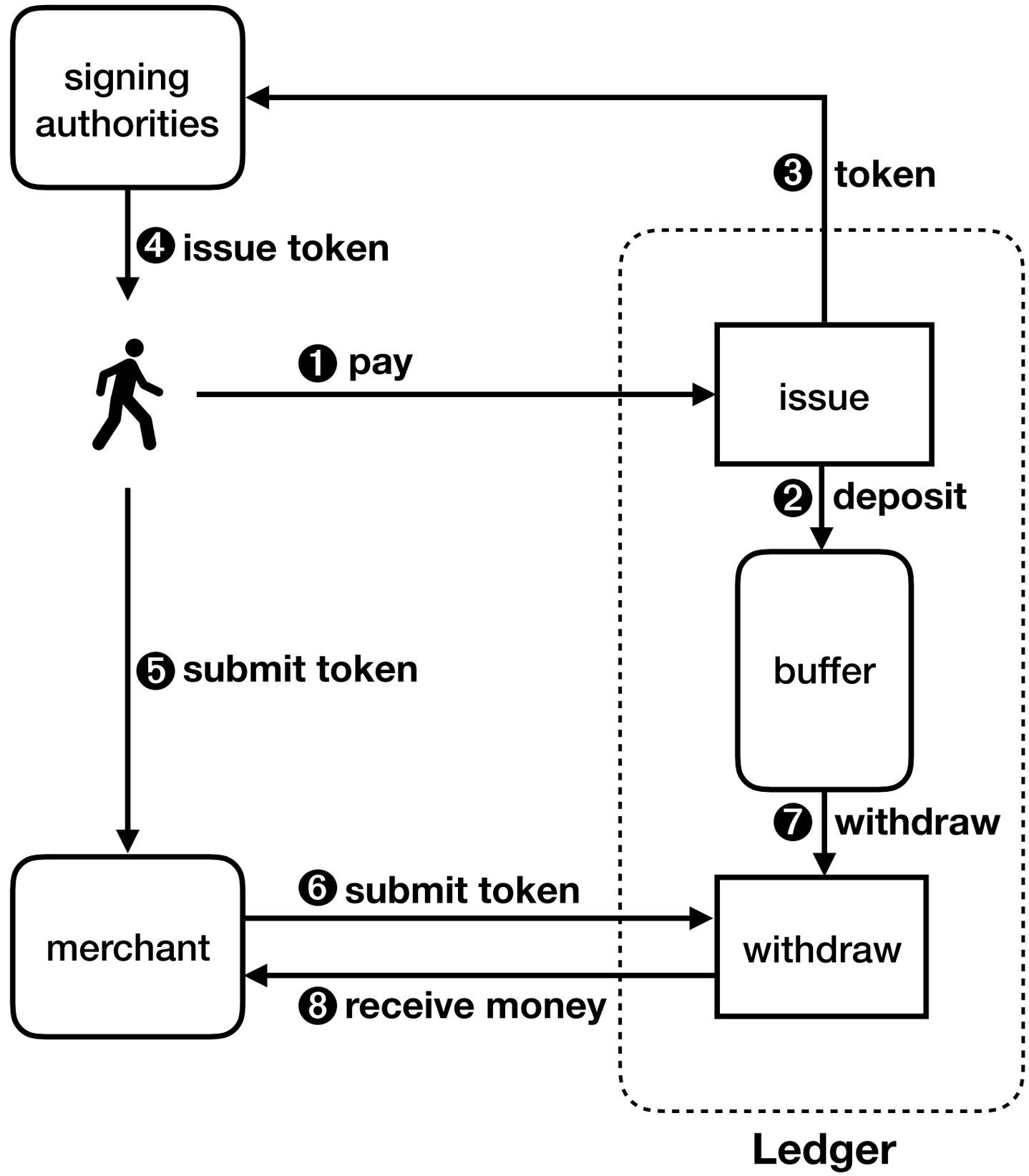
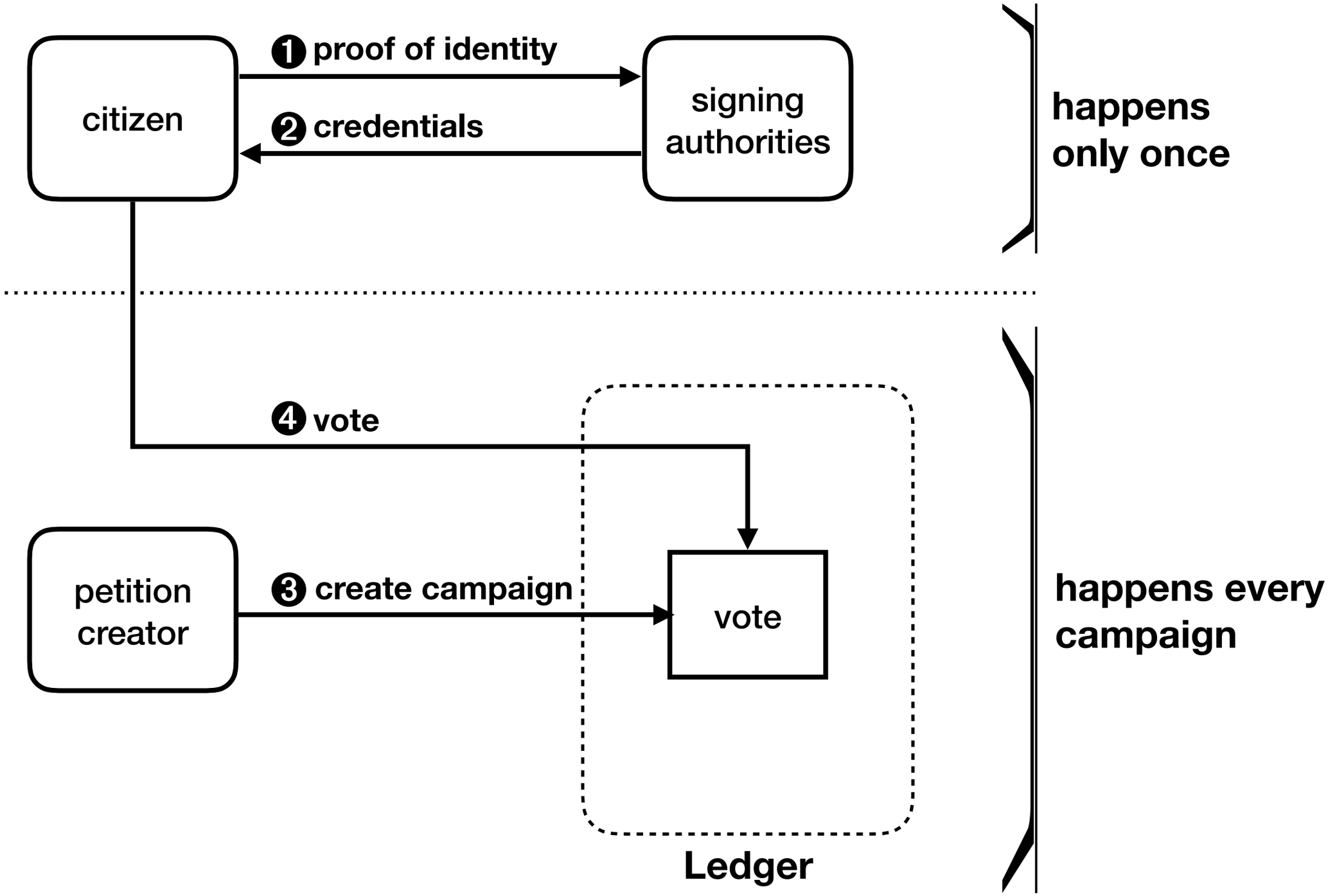

User
Signer
Verifier
repeat
n times
1a m
1b (cm, c, p)
2 s
3a (m, s)
3b (m+rd, s)

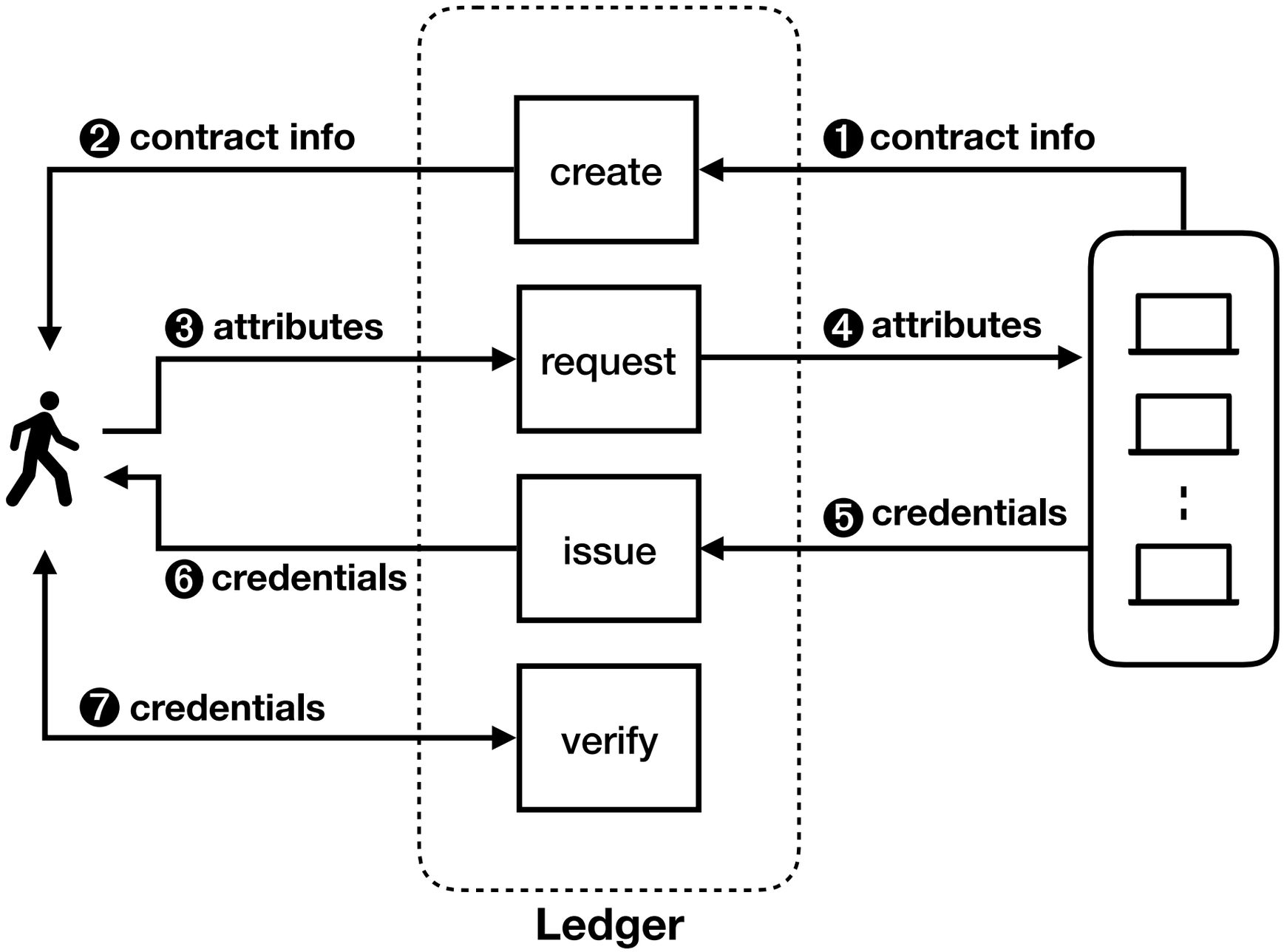

Ledger
smart contract
issue
CoCoNut authorities
buffer
user
smart contract
deposit
merchant

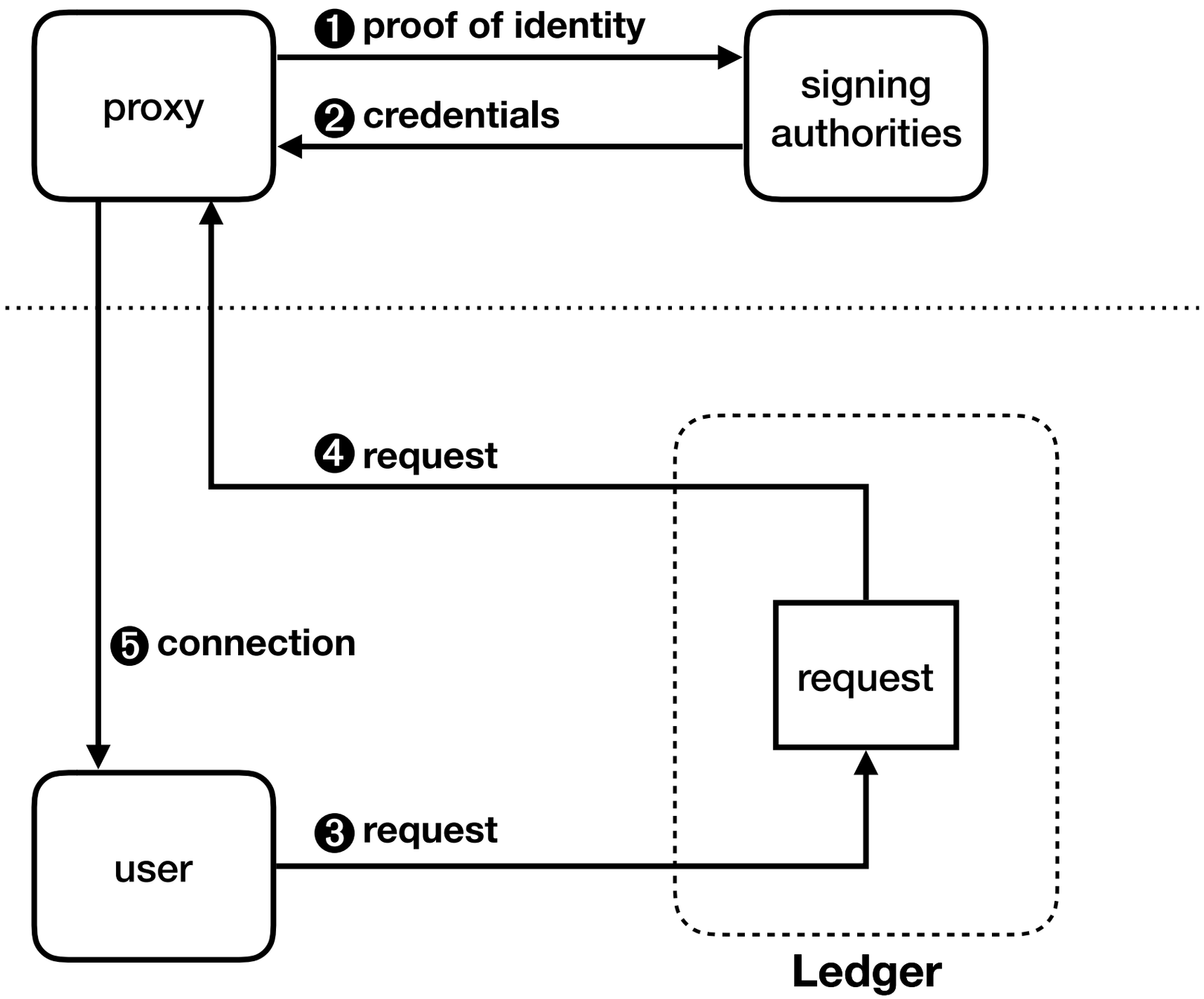

Ledger
petition creator
init
$(UUID, owner, vk, options, scores)$
smart contract
citizen
vote
$(scores, \nu)$

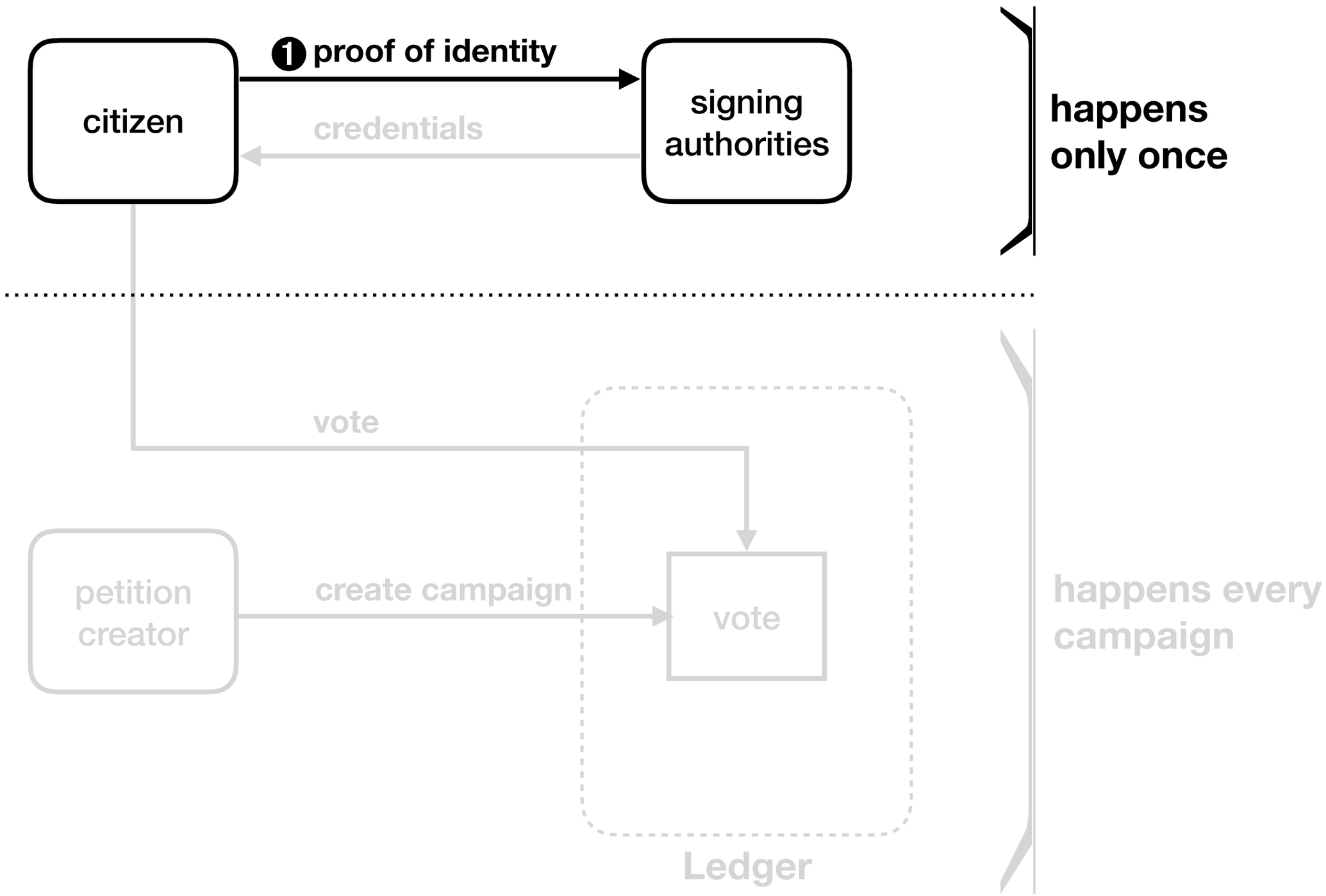

❶ request
❷ issue
❸ aggregate & randomize

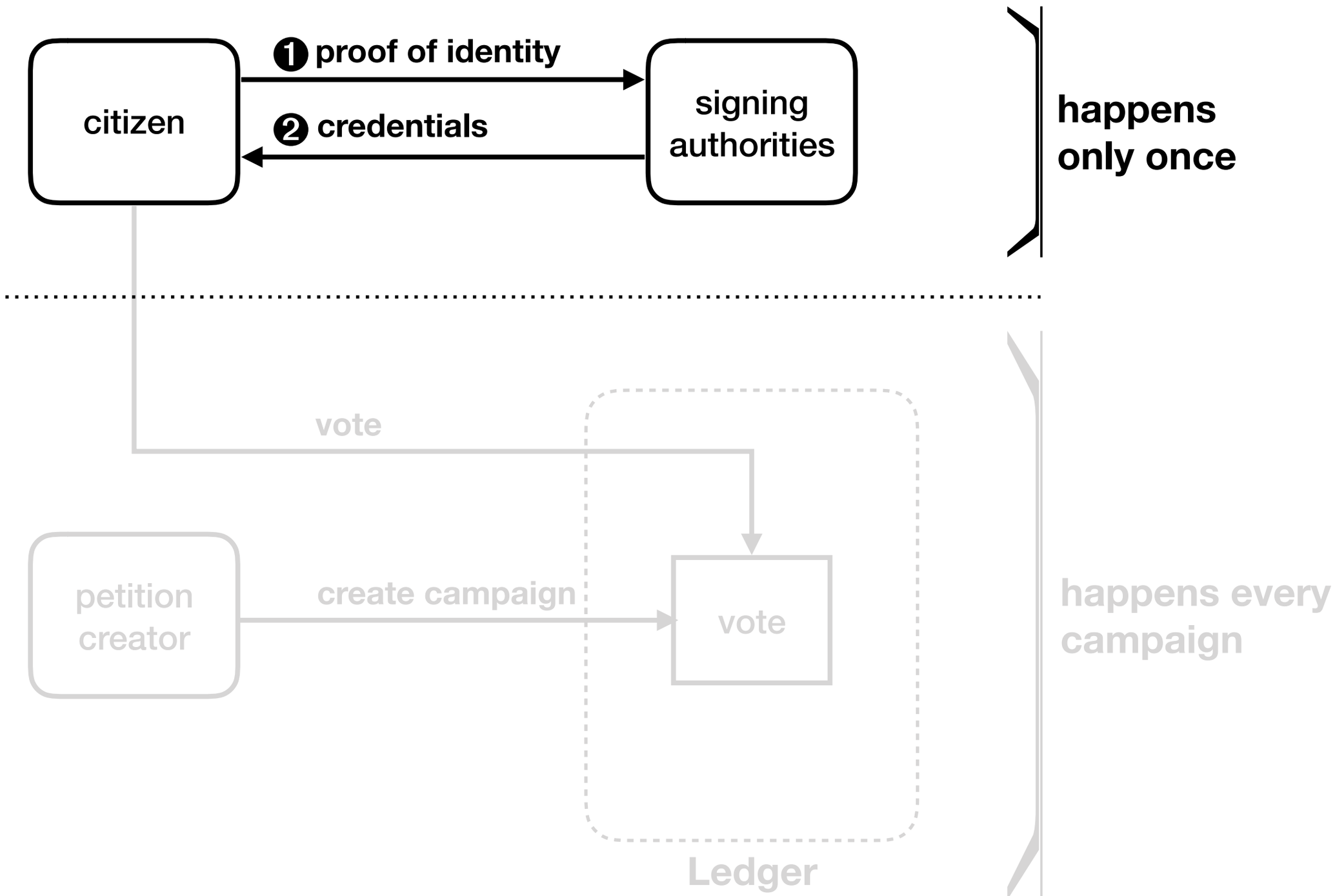

signing authorities
❸ token
❹ issue token
❶ pay
issue
❷ deposit
buffer
❺ submit token
❼ withdraw
❻ submit token
merchant
withdraw
❽ receive money
Ledger

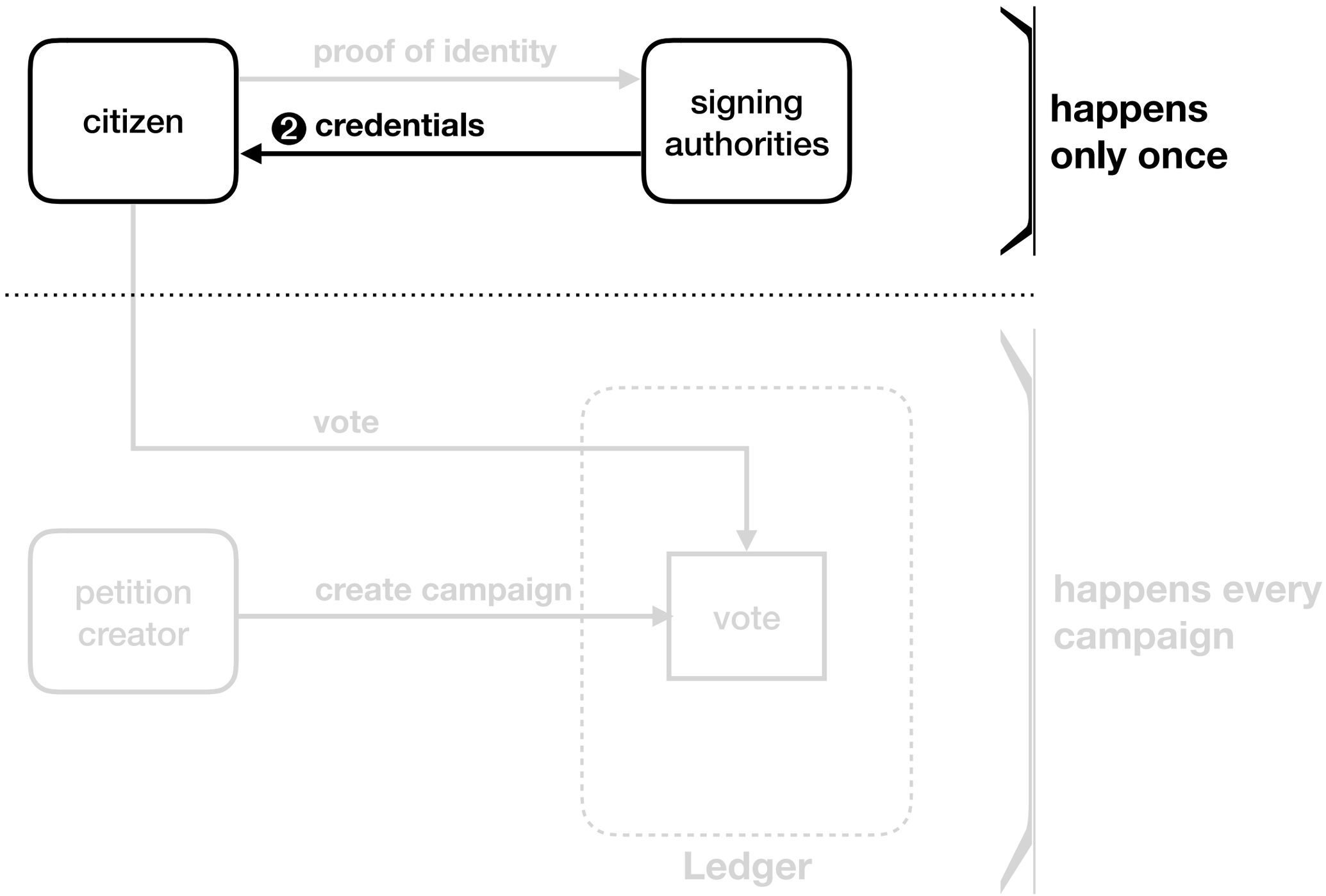

citizen
❶ proof of identity
❷ credentials
signing authorities
happens only once
❹ vote
petition creator
❸ create campaign
vote
Ledger
happens every campaign

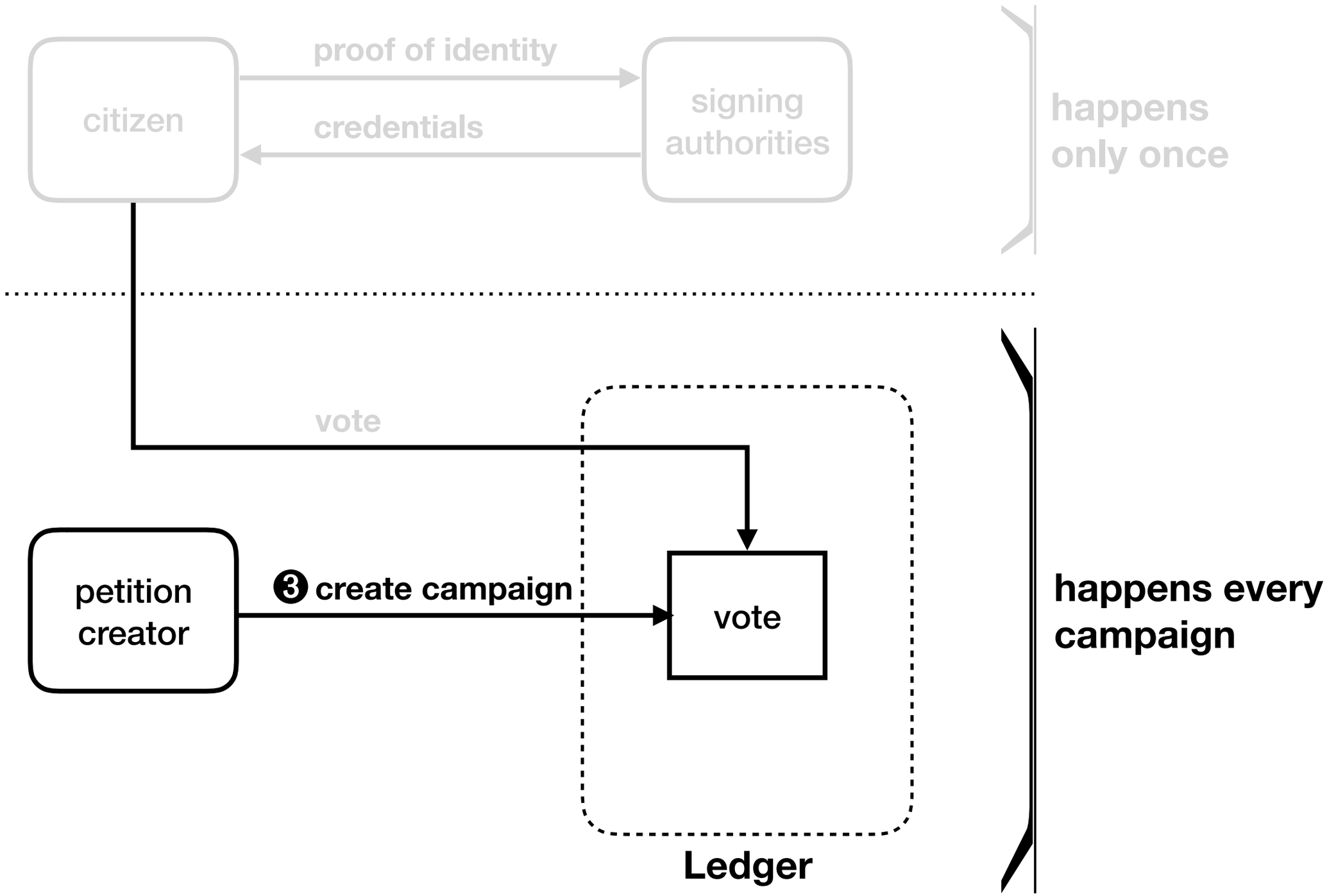

❷ contract info
create
❶ contract info
❸ attributes
request
❹ attributes
issue
❺ credentials
❻ credentials
❼ credentials
verify
Ledger

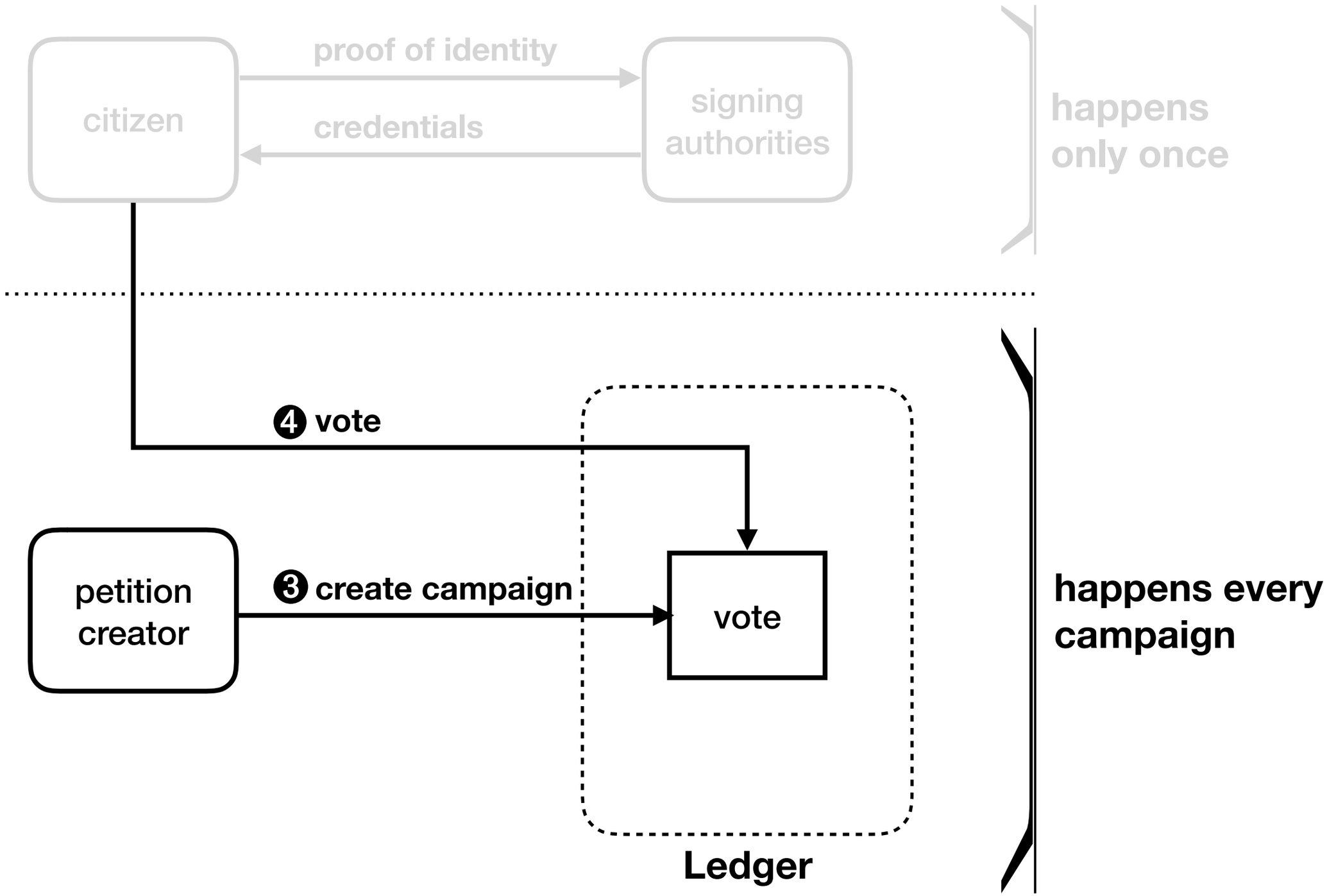

proxy
❶ proof of identity
signing authorities
❷ credentials
❹ request
❺ connection
request
user
❸ request
Ledger

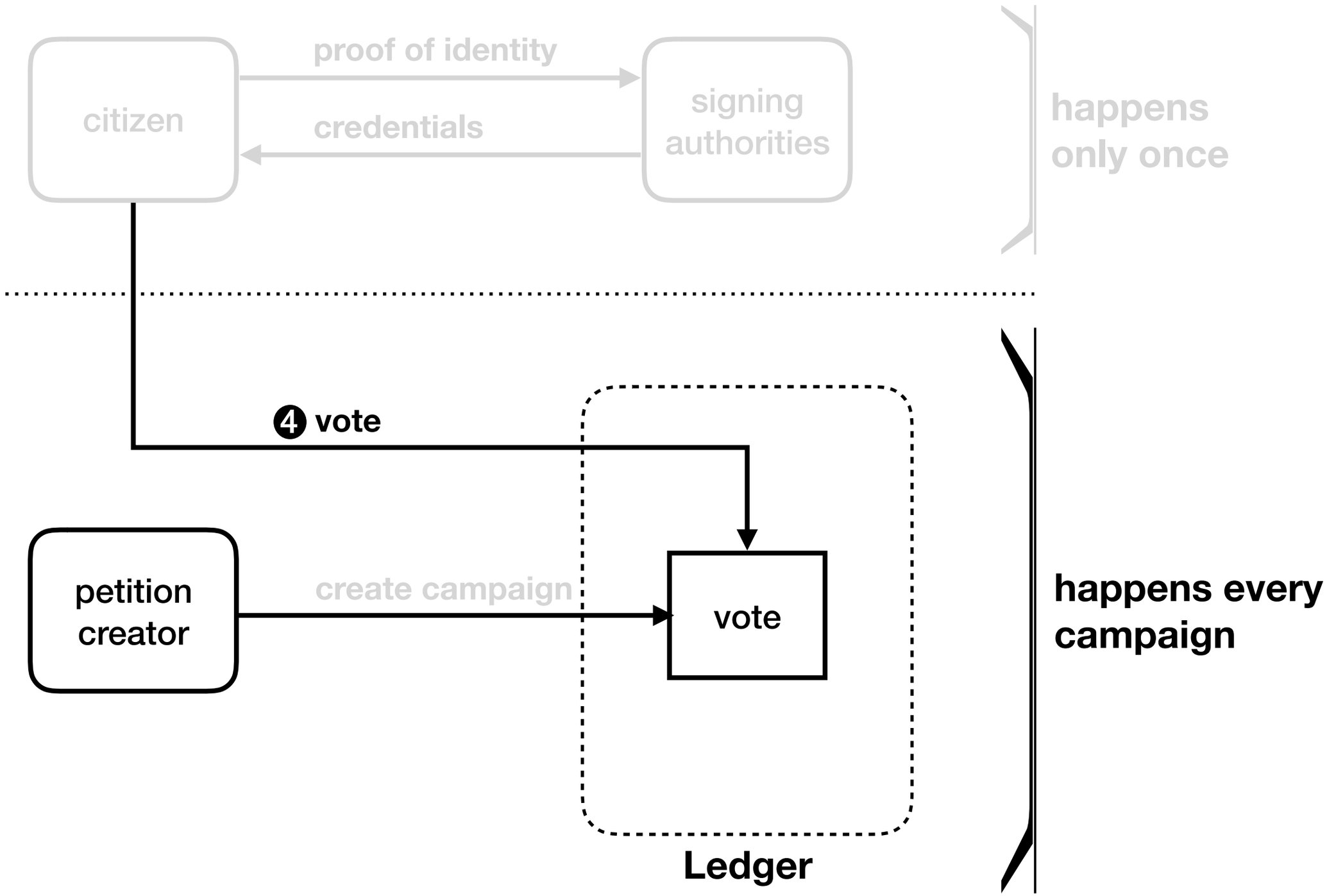

citizen
❶ proof of identity
signing authorities
credentials
happens only once
vote
petition creator
create campaign
vote
Ledger
happens every campaign


citizen
❶ proof of identity
❷ credentials
signing authorities
happens only once
vote
petition creator
create campaign
vote
Ledger
happens every campaign


citizen
proof of identity
signing authorities
❷ credentials
happens only once
vote
petition creator
create campaign
vote
Ledger
happens every campaign


citizen
proof of identity
credentials
signing authorities
happens only once
vote
petition creator
❸ create campaign
vote
Ledger
happens every campaign


citizen
proof of identity
credentials
signing authorities
happens only once
❹ vote
petition creator
❸ create campaign
vote
Ledger
happens every campaign


citizen
proof of identity
credentials
signing authorities
happens only once
❹ vote
petition creator
create campaign
vote
Ledger
happens every campaign