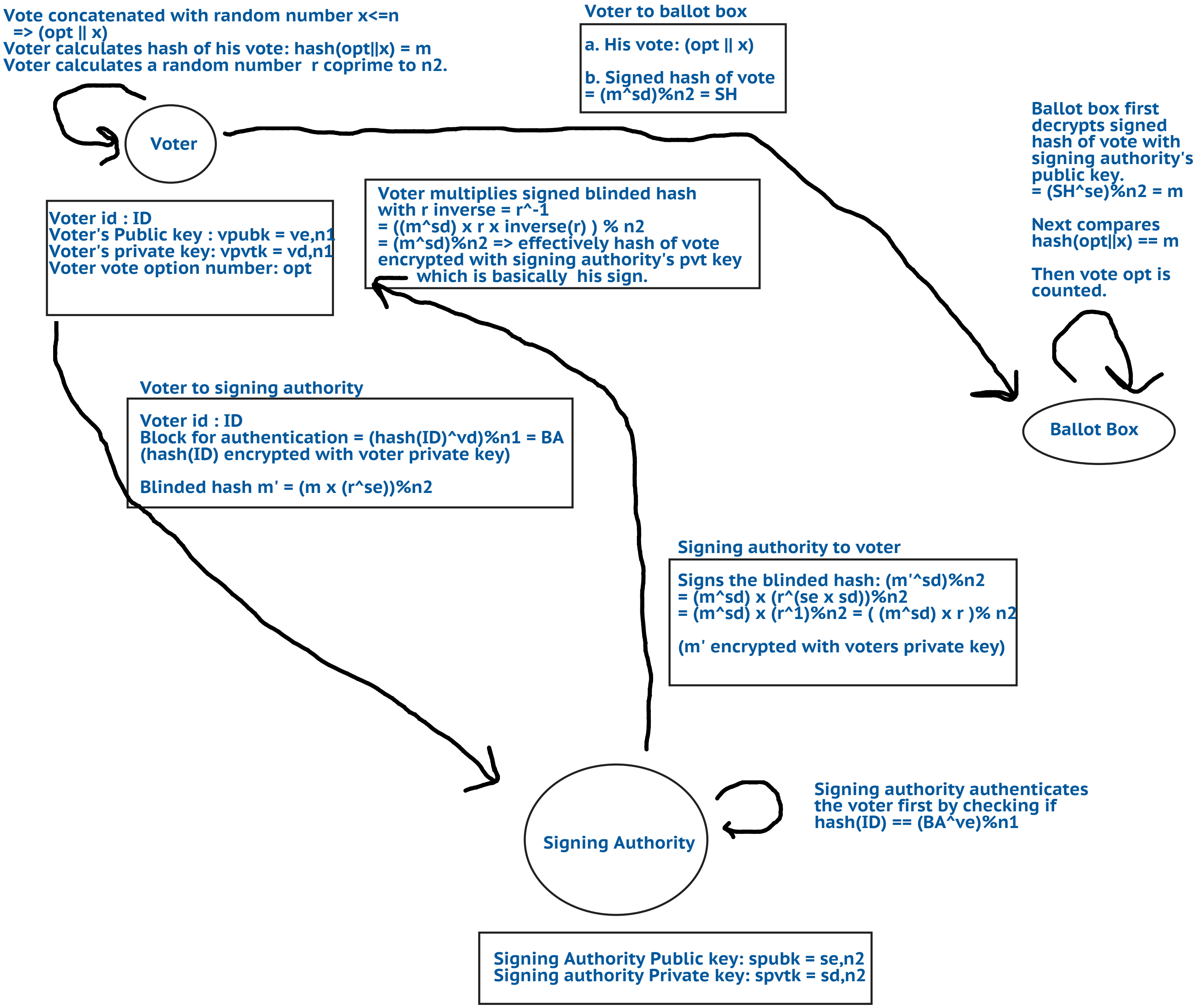
SECURE VOTING MECHANISM WITH BLIND SIGNATURES



Vote concatenated with random number x<=n
=> (opt || x)
Voter calculates hash of his vote: hash(opt||x) = m
Voter calculates a random number r coprime to n2.

Voter id : ID
Voter's Public key : vpubk = ve,n1
Voter's private key: vpvtk = vd,n1
Voter vote option number: opt

Voter to ballot box

a. His vote: (opt || x)

b. Signed hash of vote
= (m^sd)%n2 = SH

Voter multiplies signed blinded hash
with r inverse = r^-1
= ((m^sd) x r x inverse(r)) % n2
= (m^sd)%n2 => effectively hash of vote
encrypted with signing authority's pvt key
which is basically his sign.

Ballot box first
decrypts signed
hash of vote with
signing authority's
public key.
= (SH^se)%n2 = m

Next compares
hash(opt||x) == m

Then vote opt is
counted.

Voter to signing authority

Voter id : ID
Block for authentication = (hash(ID)^vd)%n1 = BA
(hash(ID) encrypted with voter private key)

Blinded hash m' = (m x (r^se))%n2

Signing authority to voter

Signs the blinded hash: (m'^sd)%n2
= (m^sd) x (r^(se x sd))%n2
= (m^sd) x (r^1)%n2 = ((m^sd) x r)% n2

(m' encrypted with voters private key)

Signing authority authenticates
the voter first by checking if
hash(ID) == (BA^ve)%n1

Signing Authority Public key: spubk = se,n2
Signing authority Private key: spvtk = sd,n2