

Pre-Election STAR-Vote Protocol

Controller/Judge's Station



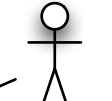
N = # election trustee
k = threshold value
K_i = trustee private/public keypair
K = election public key composed of all trustee public keys
z₀ = random start value

Ballot
BallotStyle
Race
Option

Election Public Bulletin Board

election public key K
election start value z₀

Tally System



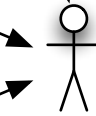
Independent Observer



Independent Verifier



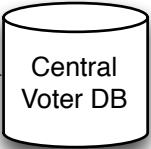
Auditor



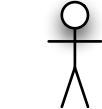
Election Authority



Voter



Central
Voter DB



Election Authority

buildStatusDB :: [(ID Voter, ID Precinct)] -> STM StatusDB
z₀ = getStdGen

10. perform risk-limiting
audit of election

