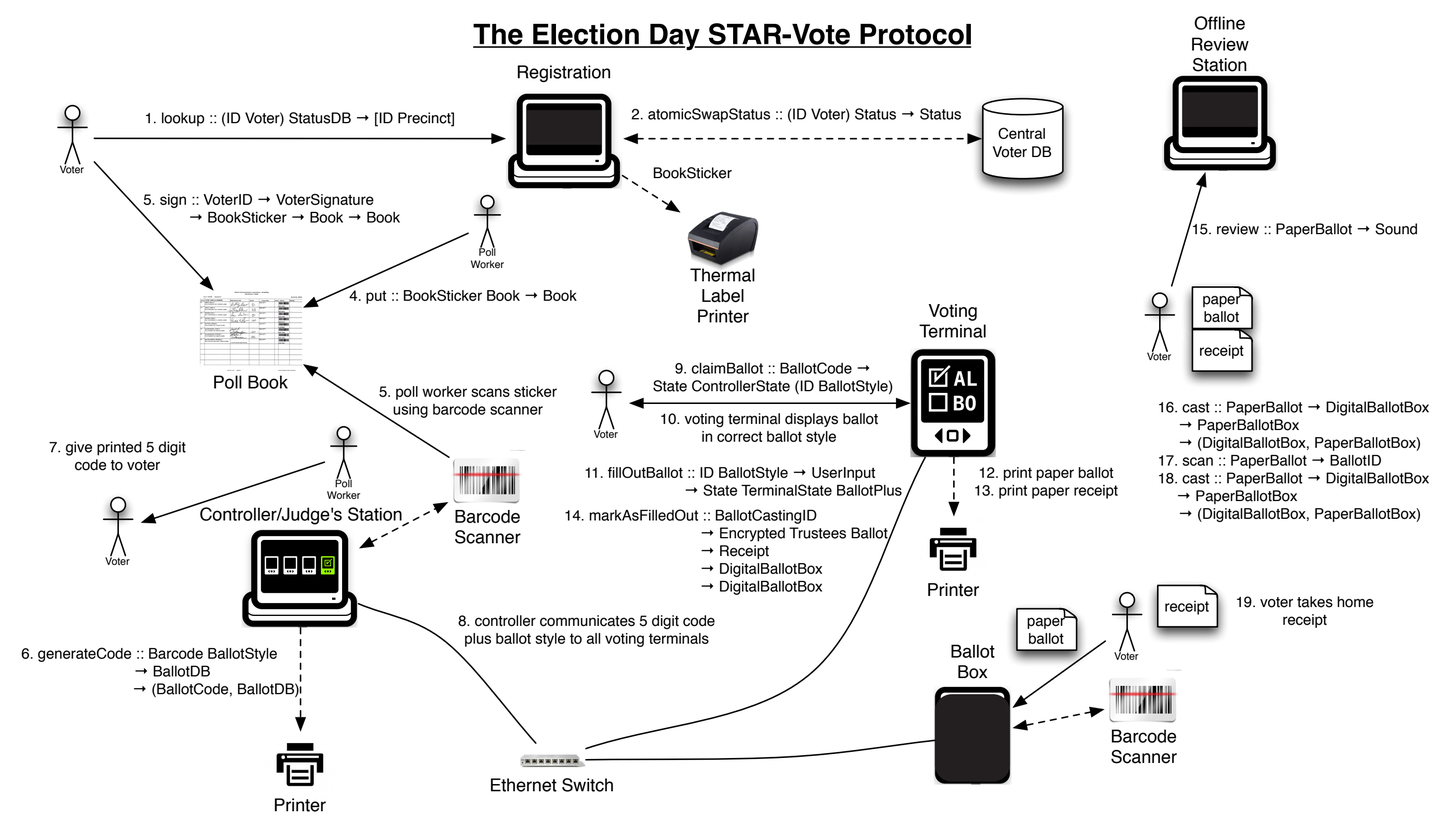
The Election Day STAR-Vote Protocol



HashChain
encryptRecord :: PublicKey
encryptBallot :: PublicKey -> Ballot -> (Encrypted Ballot, Proof Ballot)
encryptRaces :: PublicKey -> BallotId -> [RaceSelection] -> Encrypted [Hash RaceSelection]
encryptRace :: PublicKey
publicHash :: BallotCastingId
internalHash :: BallotCastingId
encrypt :: Binary a => PublicKey -> a -> ByteString
decrypt :: PrivateKey -> ByteString -> ByteString
hash :: Binary a => a -> SerializableBS
(<|>) :: (Binary a, Binary b) => a -> b -> SerializableBS

N = # election trustee
k = threshold value
K_i = trustee private/public keypair
K = election public key composed of all trustee public keys
z_0 = random start value

Ballot
lookup :: Text -> Ballot -> Maybe Selection
insert :: BallotKey -> Selection -> Ballot -> Ballot
empty :: Ballot
races :: Ballot -> [RaceSelection]

ID Voter
ID Precinct
Status
StatusDB

BallotStyle
lookup :: BallotStyleId -> BallotStyles -> Maybe BallotStyle
bRace :: RaceId -> BallotStyle -> Maybe Race
bRaces :: BallotStyle -> [Race]
nextRace :: BallotStyle -> Race -> Maybe Race
prevRace :: BallotStyle -> Race -> Maybe Race
incRace :: Int -> BallotStyle -> Race -> Maybe Race
option :: Text -> Race -> Maybe Option
key :: BallotStyle -> Race -> BallotKey
key' :: BallotStyleId -> RaceId -> BallotKey
fromKey :: BallotKey -> Maybe (BallotStyleId, RaceId)

Datatype Key
<STAR-Vote paper variable> = Haskell Type