Interconnecting PKI domains using blockchain technology

Erik Andersen

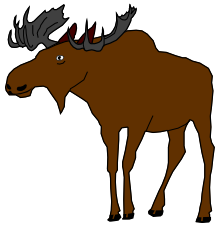
Second ITU-T X.509 day

9 May 2023

Can I

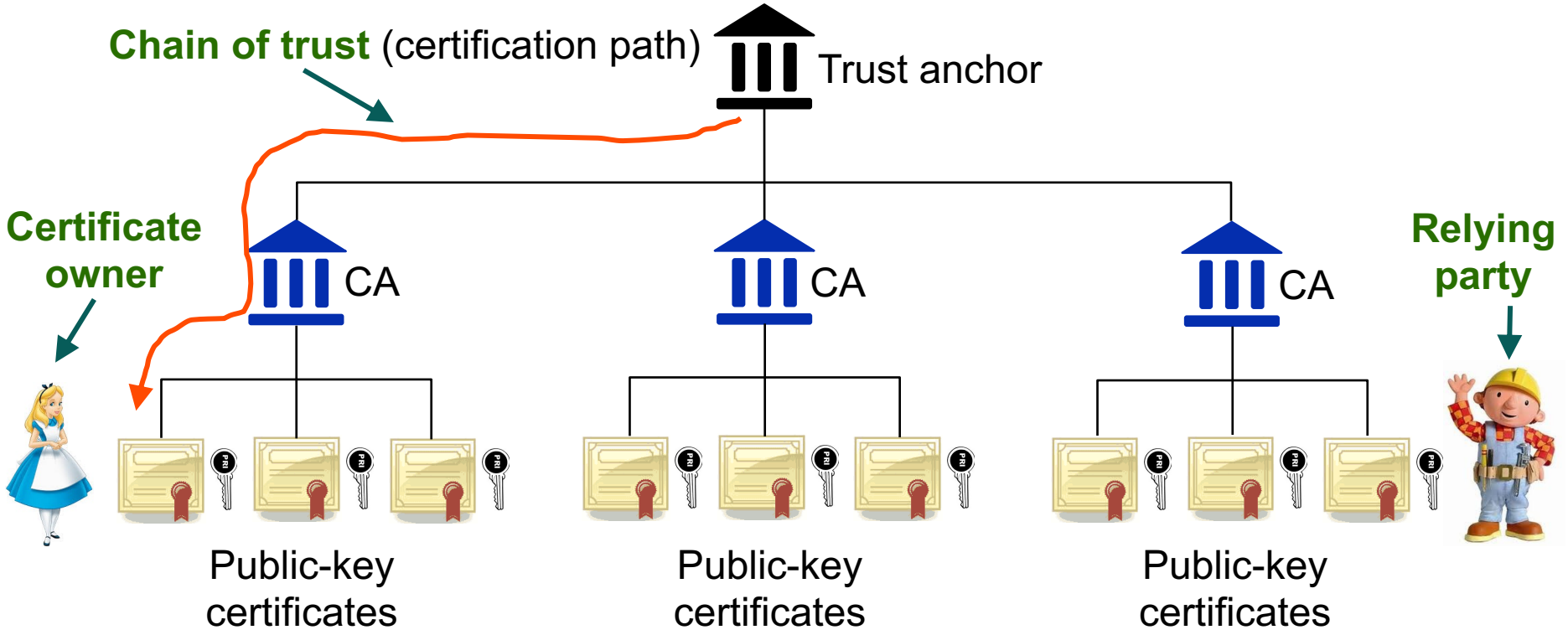
Trust

the content of a certificate?

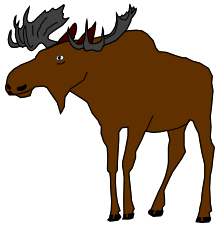


Chain of trust with traditional public-key infrastructure (PKI)

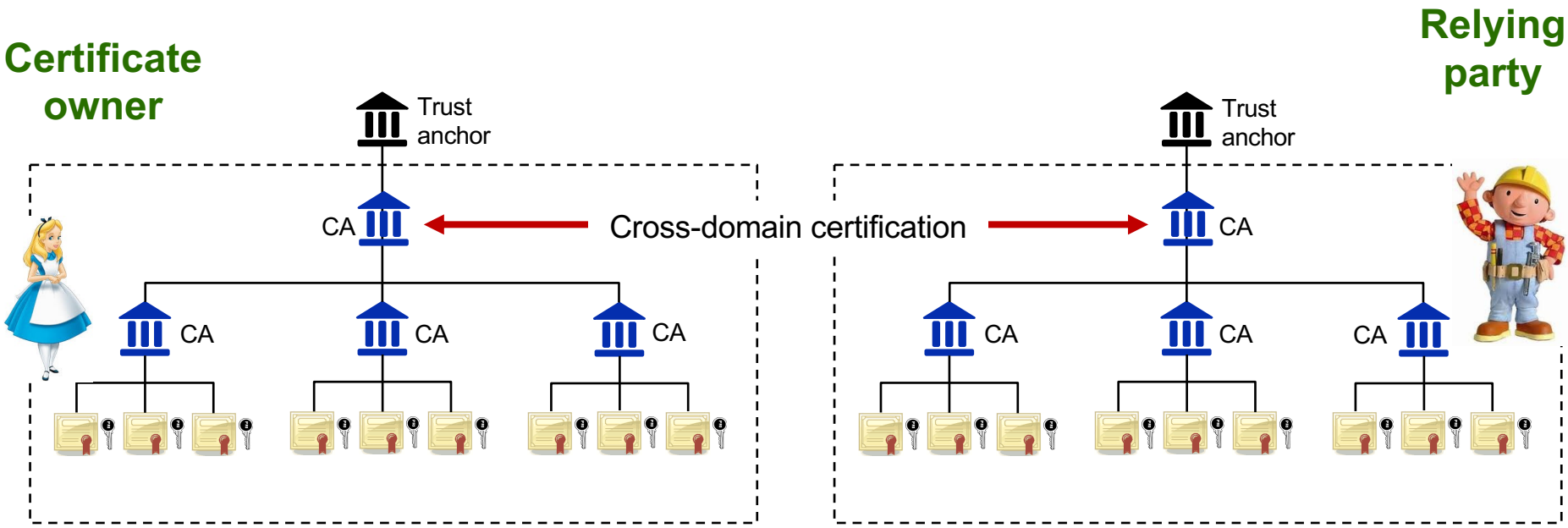
PKI Domain:

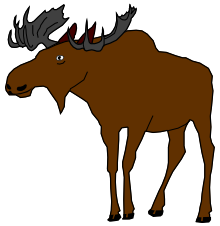


If the relying party and the certificate owner are far apart, then what?

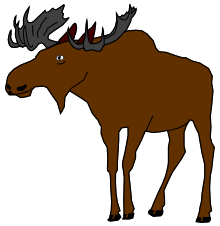


Interconnected Public-key infrastructure (PKI) domain

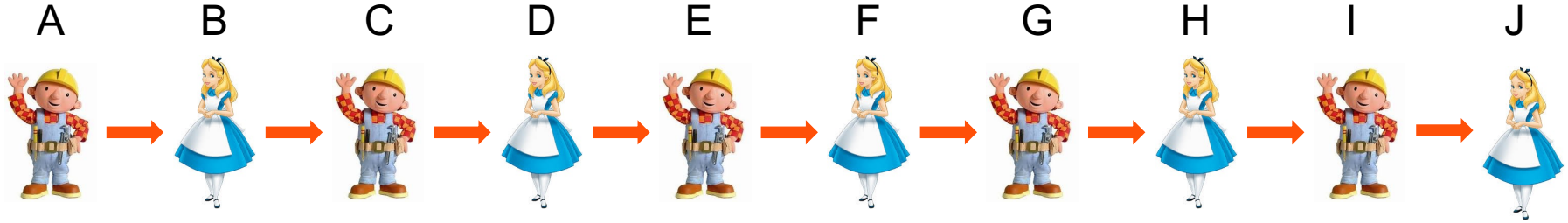




A world-wide federated PKI



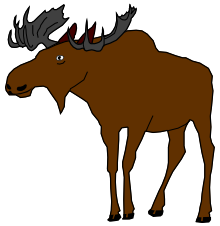
Long chain of trust



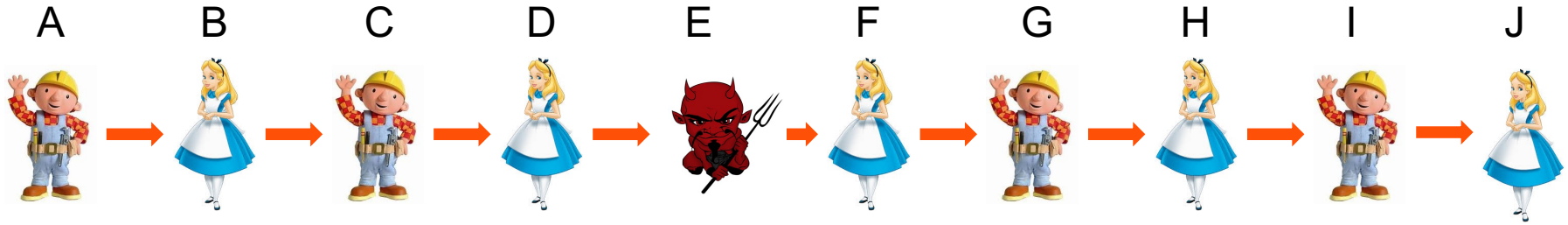
A trust B, B trust C, ... , I trust J

Can A then trust J?

The longer the chain of trust is, the more diluted trust becomes



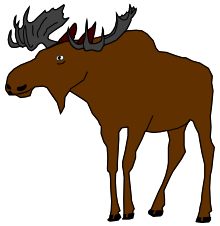
Long chain of trust



A trust B, B trust C, ... , I trust J

Can A then trust J?

The longer the chain of trust is, the more diluted trust becomes

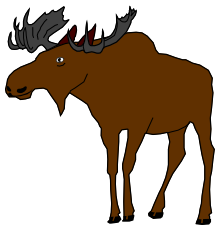


Trust by consensus

It seems problematic to create a world-wide federated PKI having world-wide trust using current PKI trust model.

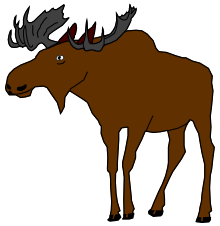
A PKI where trust is obtained by consensus

PKI domains federated using blockchain technology

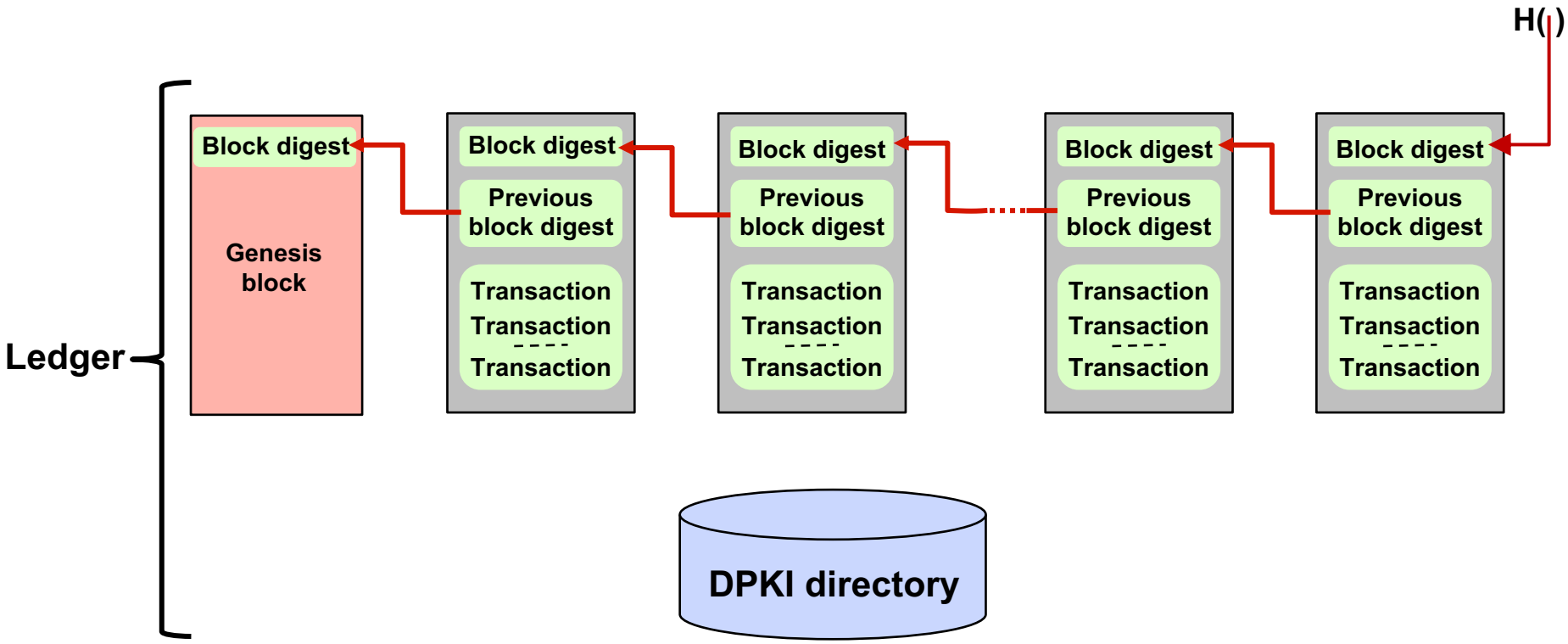


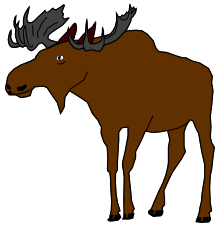
Design approach

- Goal: ITU-T Recommendation | ISO/IEC International Standard
- Current blockchain platforms cannot be used as normative references
- Current blockchain platforms may be used as “inspirations” when specifying a standardized platform
- Hyperledger Fabric is a possible choice, but have more features than needed
  - Used by IBM for business support
  - Has extensive documentation
  - Proven technology
  - Pluckable consensus protocol
  - Includes a state database
- Stellar Consensus Protocol (SCP) possible “inspiration” for consensus protocol
- Much processing will be PKI specific
- Ensure cryptographic algorithm migration capabilities

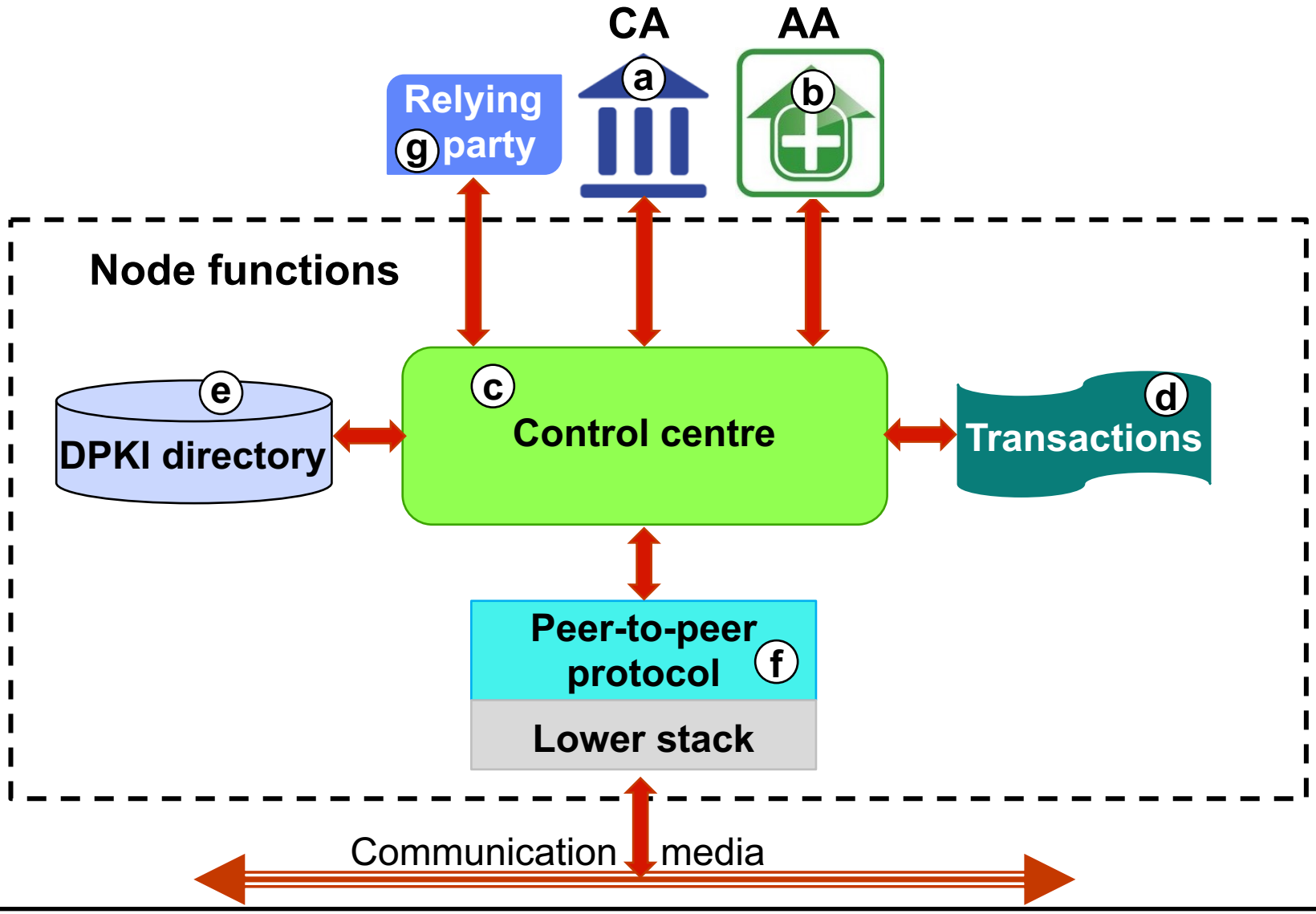


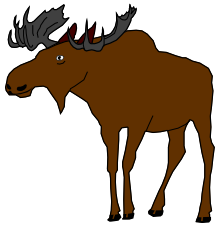
Distributed ledger



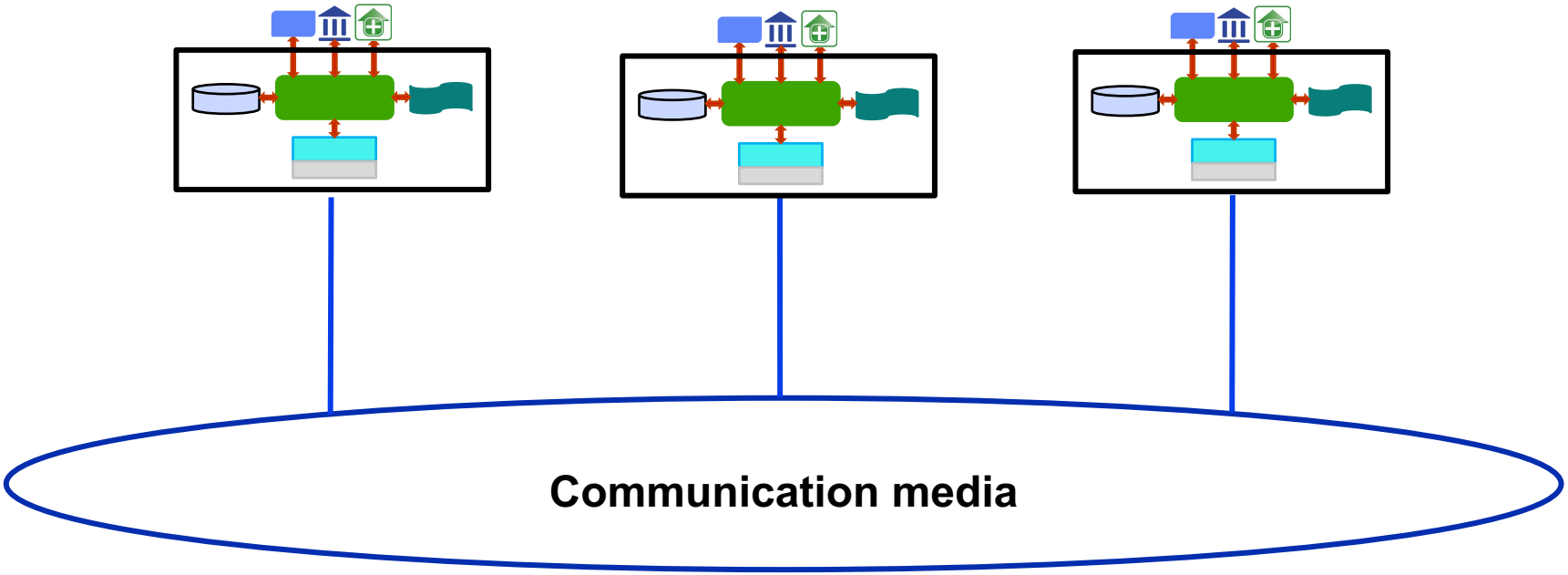


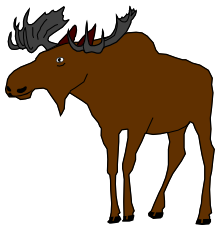
Overall architecture





A figurative representation of the underlying network





Control centre details