Key Consistency and Discovery

`draft-wood-key-consistency`

Davidson, Finkel, Thomson, Wood — IETF 110 — Privacy Pass

Motivation
Background

Emerging privacy-focused protocols require a mechanism for clients to discover server public keys

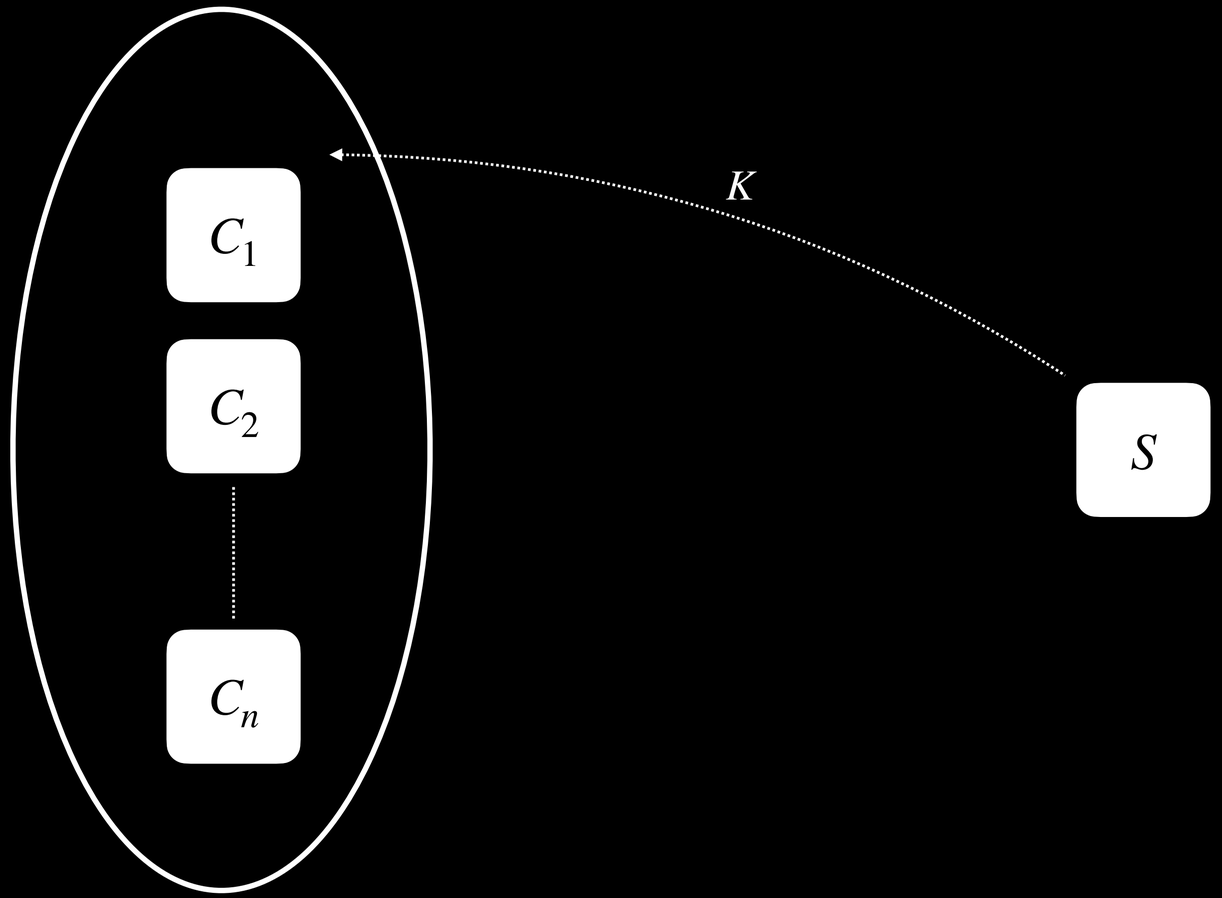
- Privacy Pass: Issuer verification key
- ODoH and OHTTP: Target public encryption key
- Tor: Relay public keys

Common requirements:

1. Unlinkability: Servers cannot *link usage of a key to specific users*
2. Authenticity: Clients use an *authentic* key for the intended server

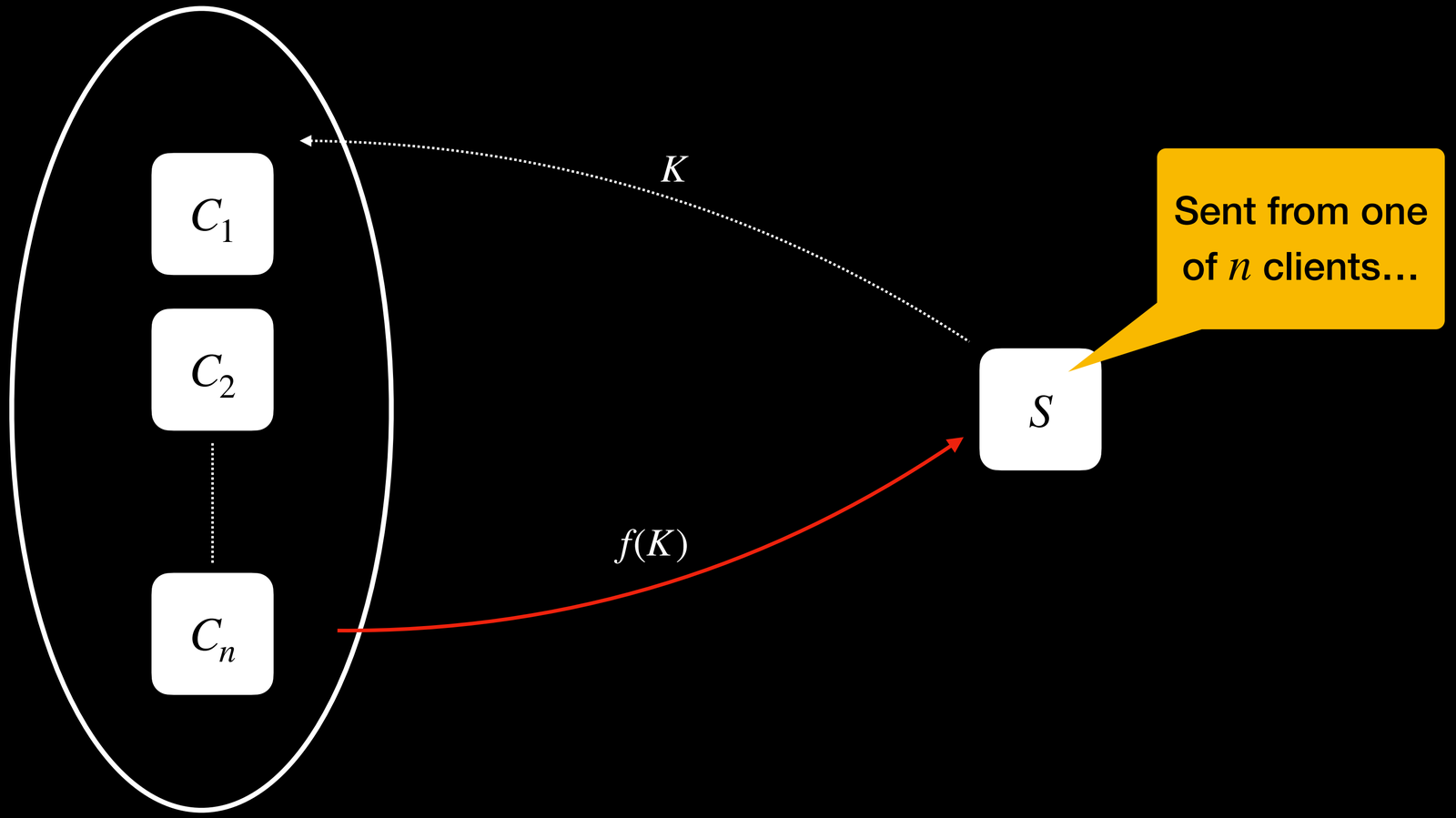
Motivation

Unlinkability

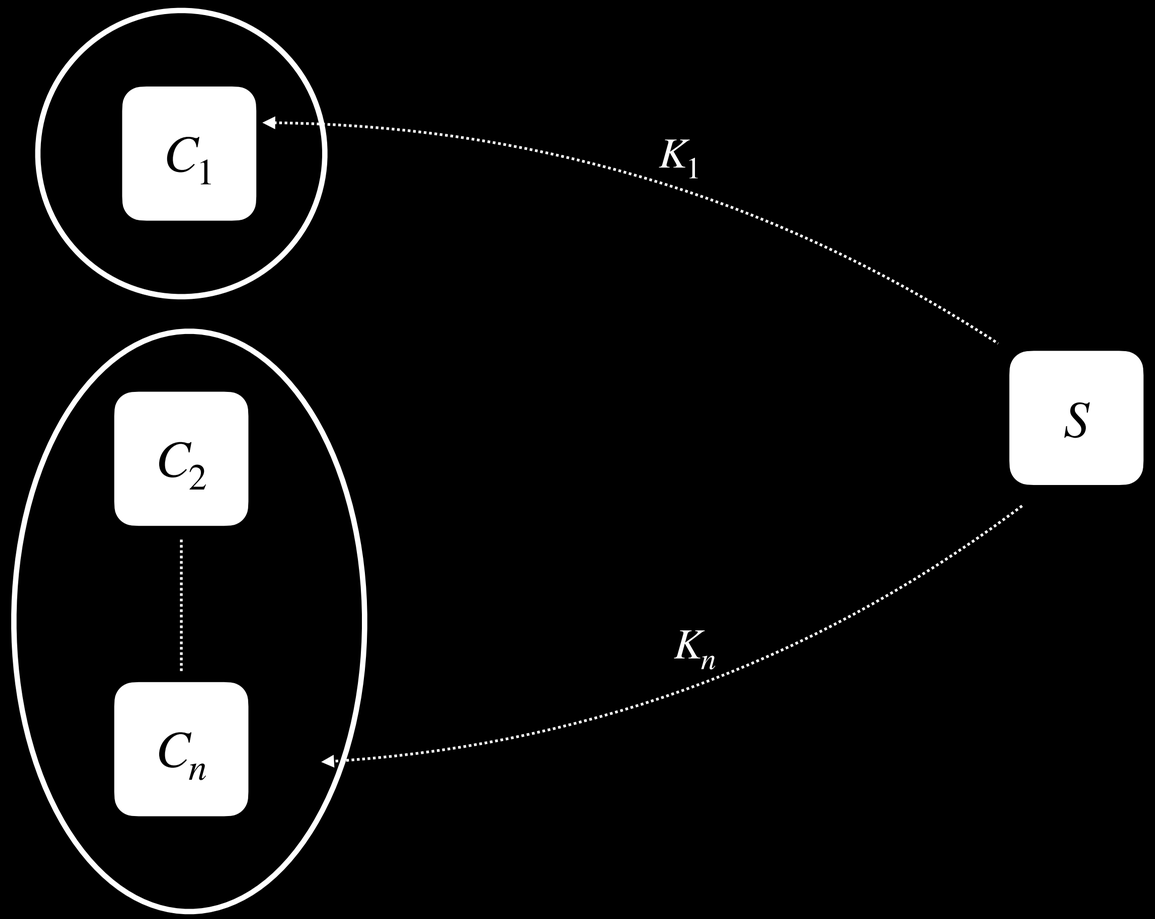


Motivation

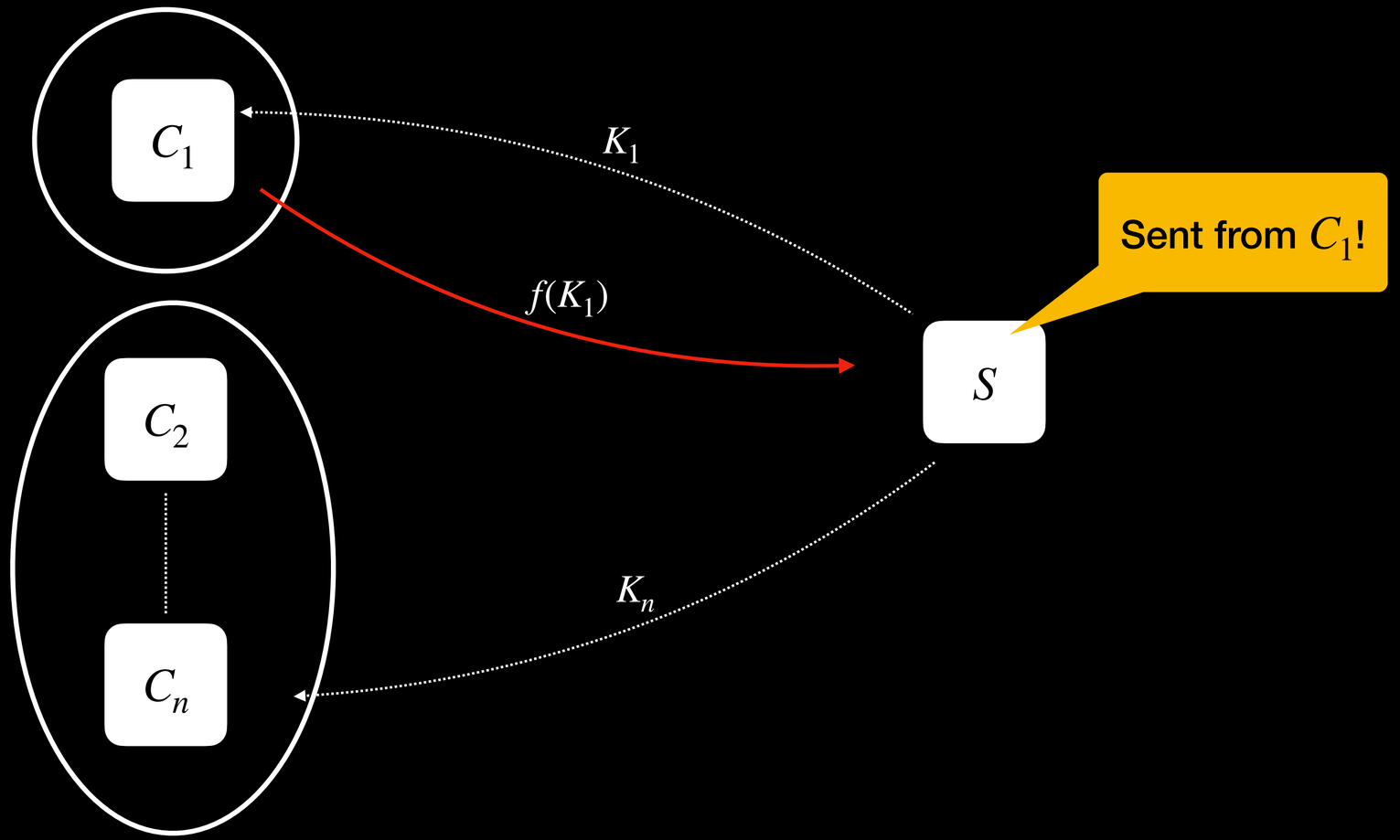
Unlinkability



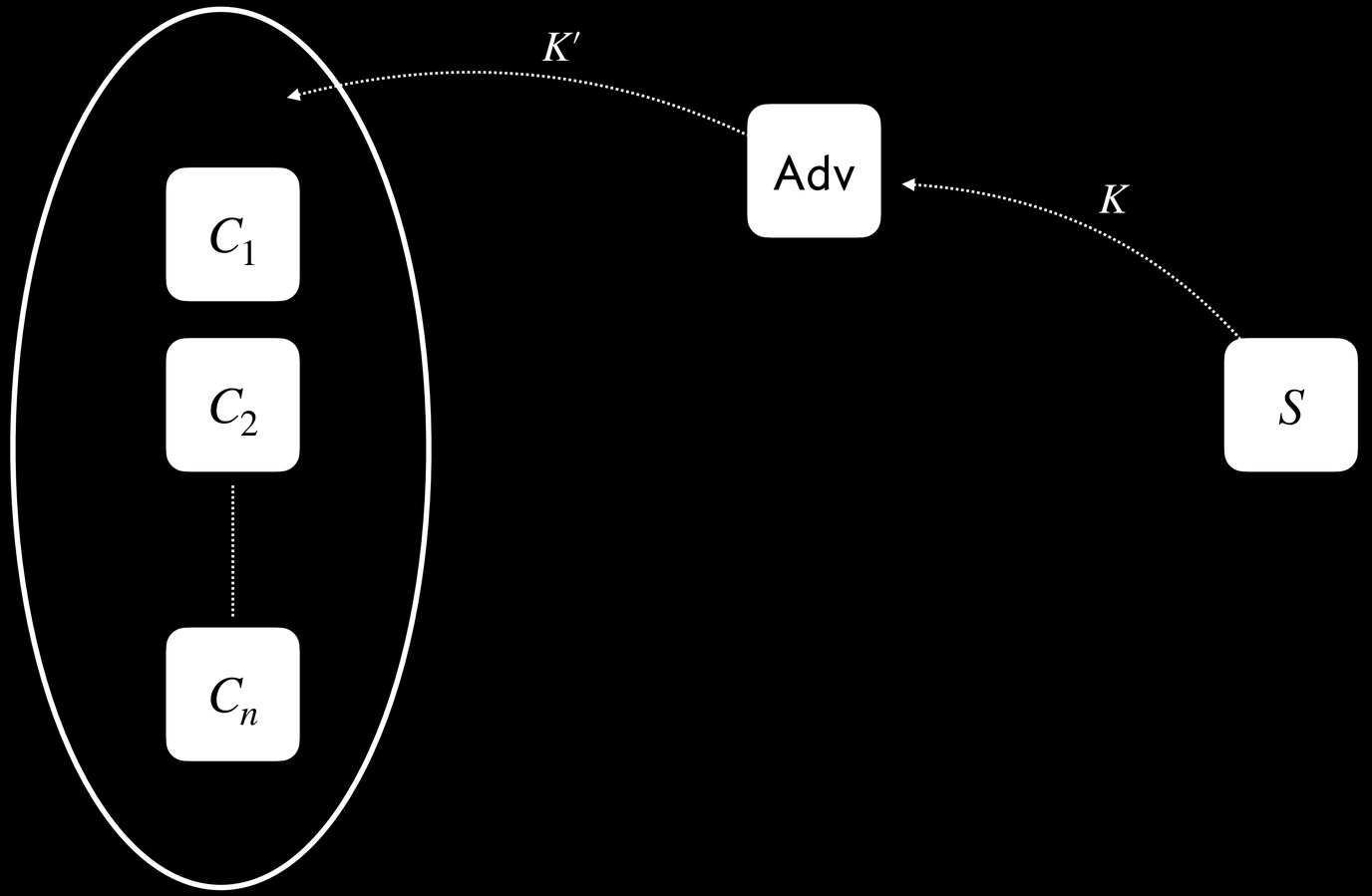
Motivation
Unlinkability



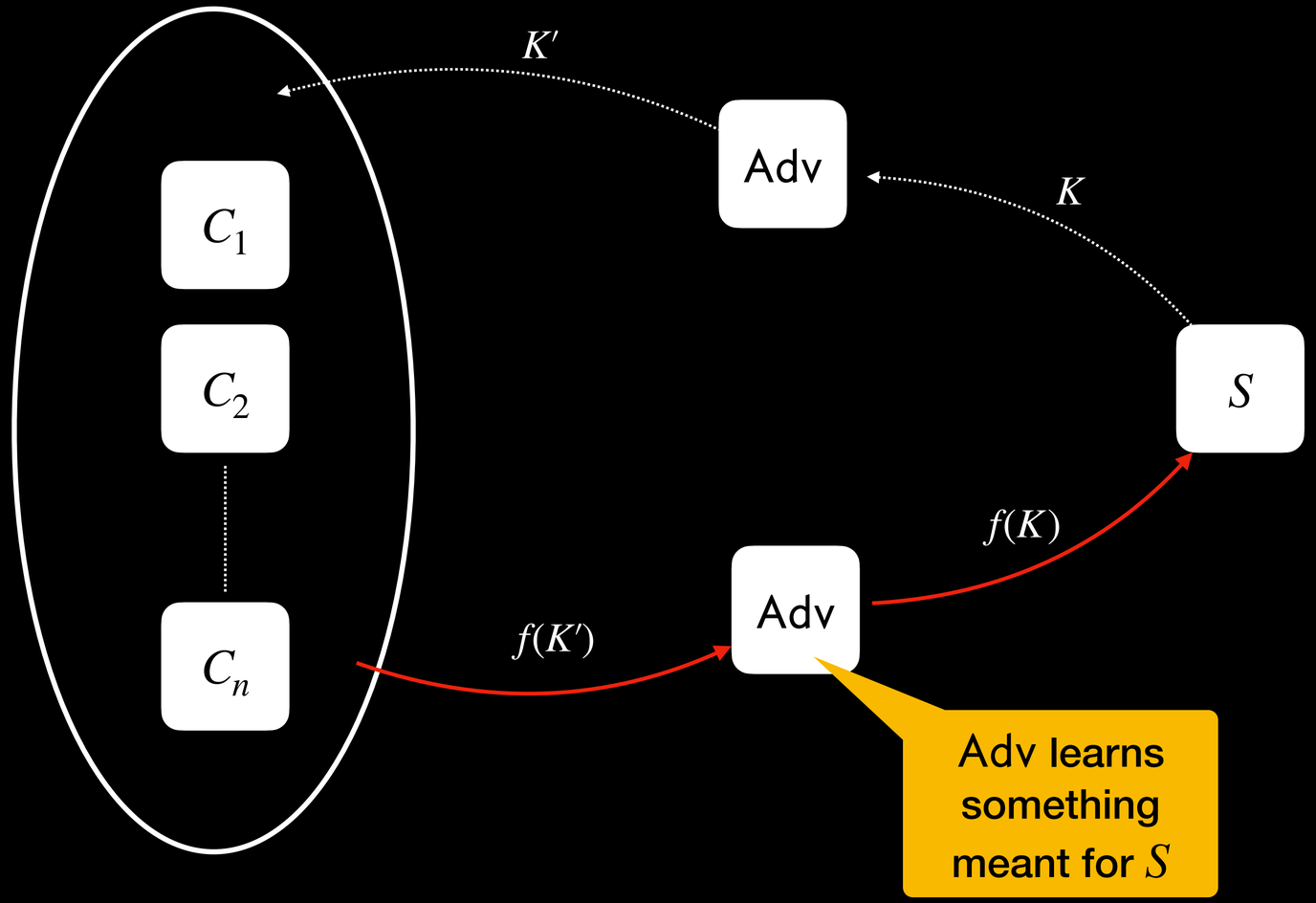
Motivation
Unlinkability



Motivation
Authenticity



Motivation
Authenticity



Unlinkability and authenticity means that all clients in the same anonymity set have a ***consistent*** view of the server's intended key, and that view is ***correct***

Consistency and Correctness

In practice

A key consistency and correctness system (KCCS) is something that provides consistency and correctness for clients

KCCS varies in practice based on:

- Threat model
- Cryptographic dependencies
- Trust model and PKI
- Operational complexity
- External dependencies

Consistency and Correctness

Design space

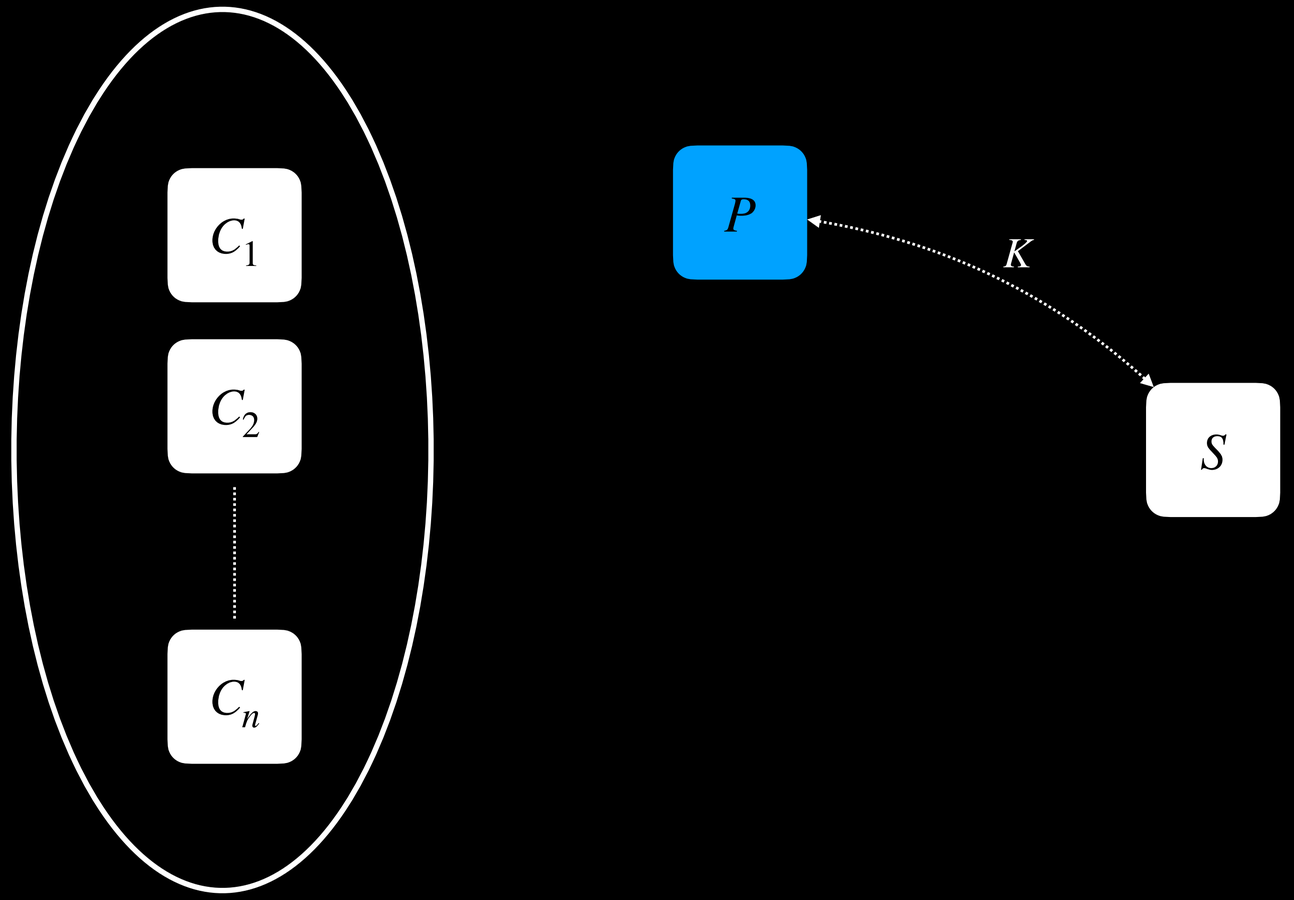
Vary the topology and trust model:

- Fetch through a trusted proxy
- Fetch through multiple less-trusted proxies
- Outsource to an audited or verified data store

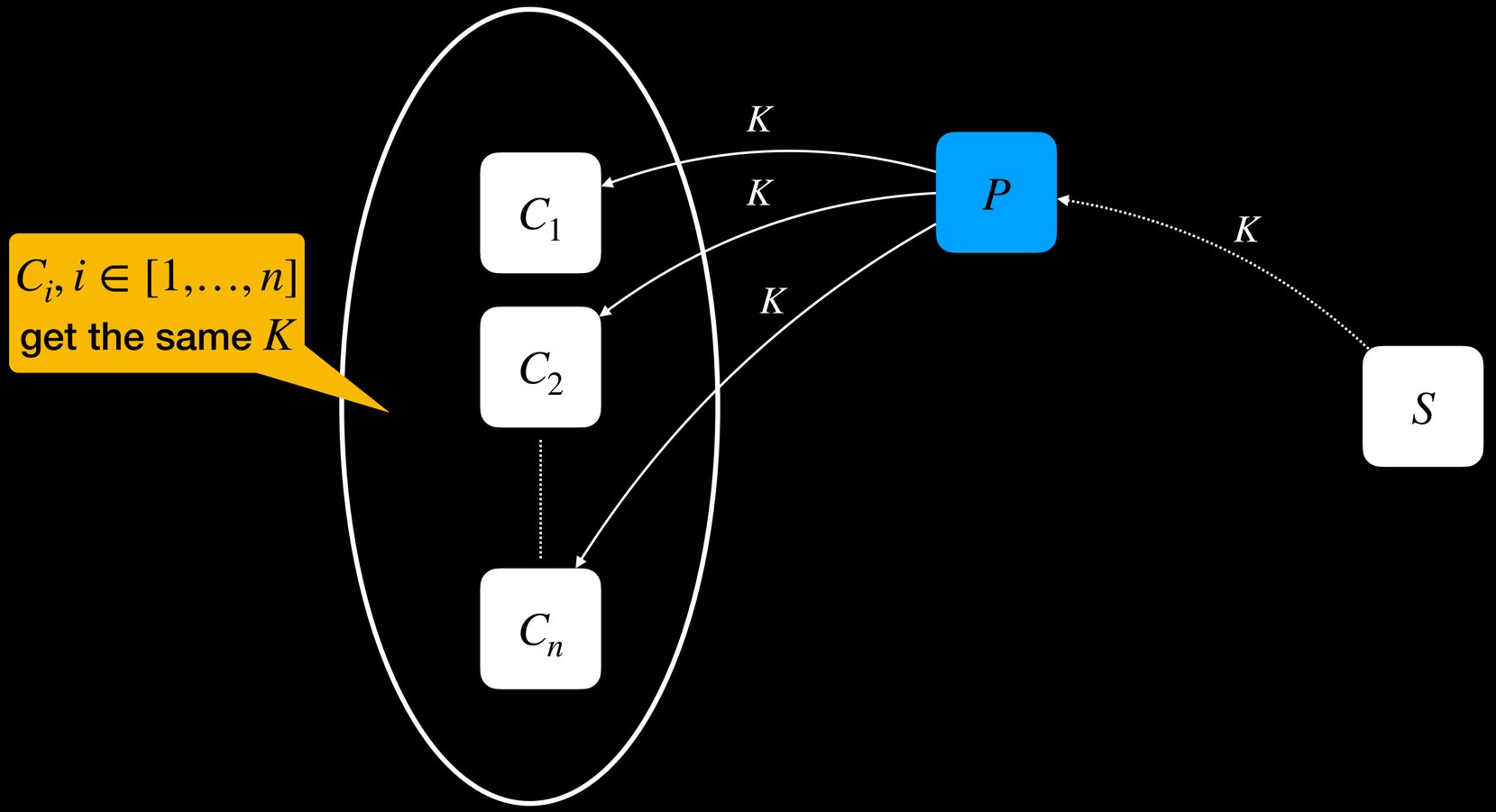
Vary the cryptography:

- Classical signatures vs other primitives

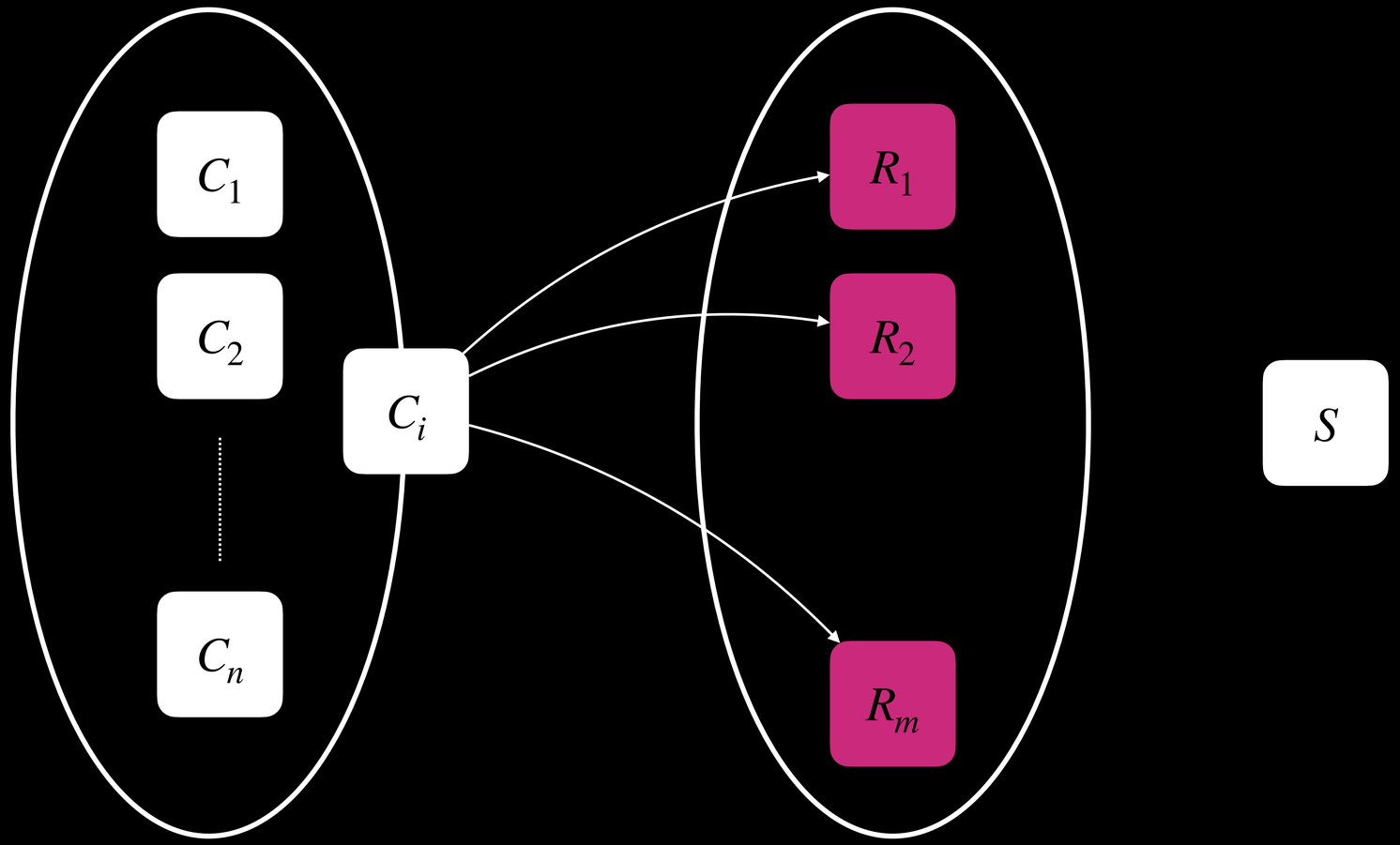
Trusted Proxy Discovery



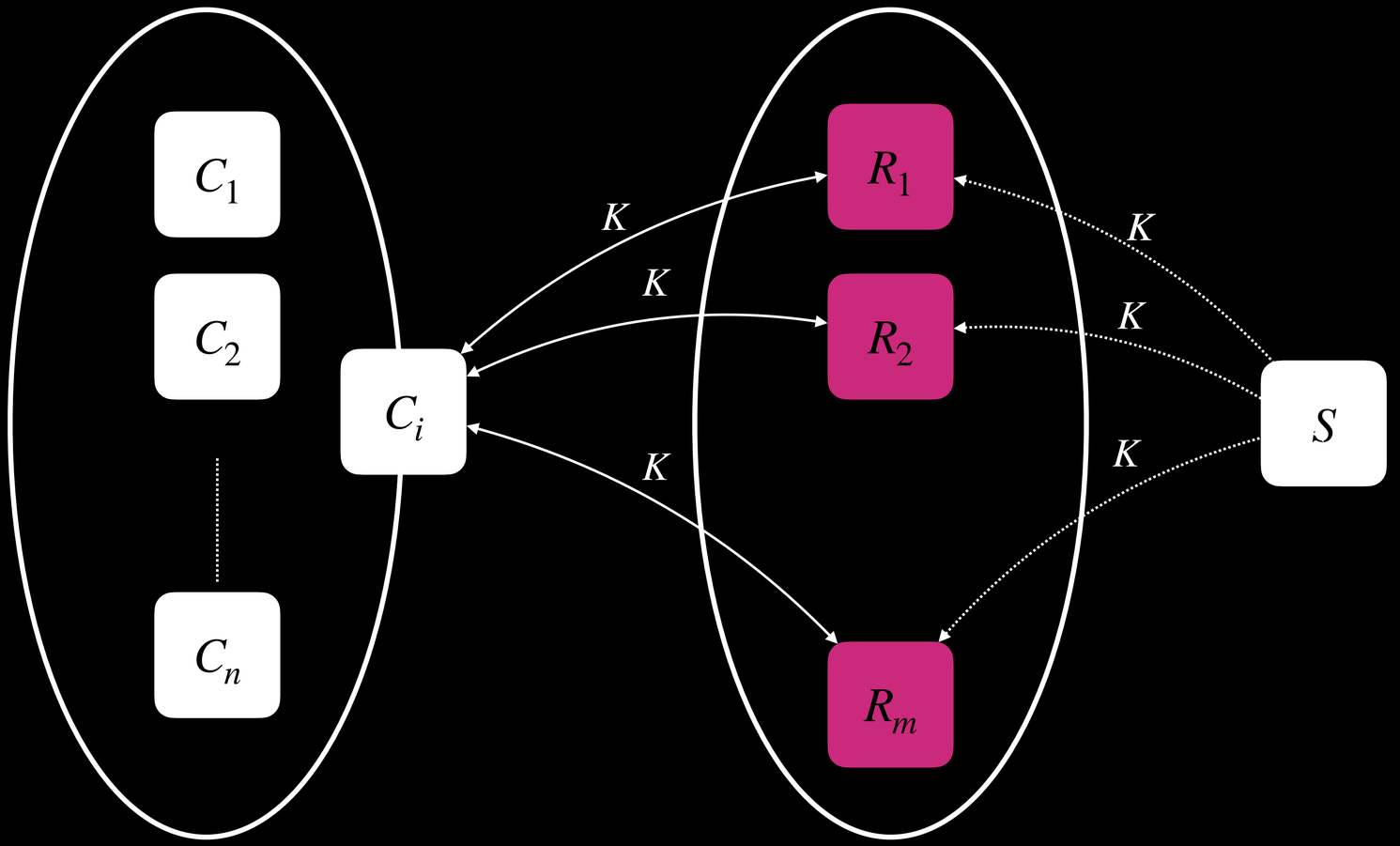
Trusted Proxy Discovery



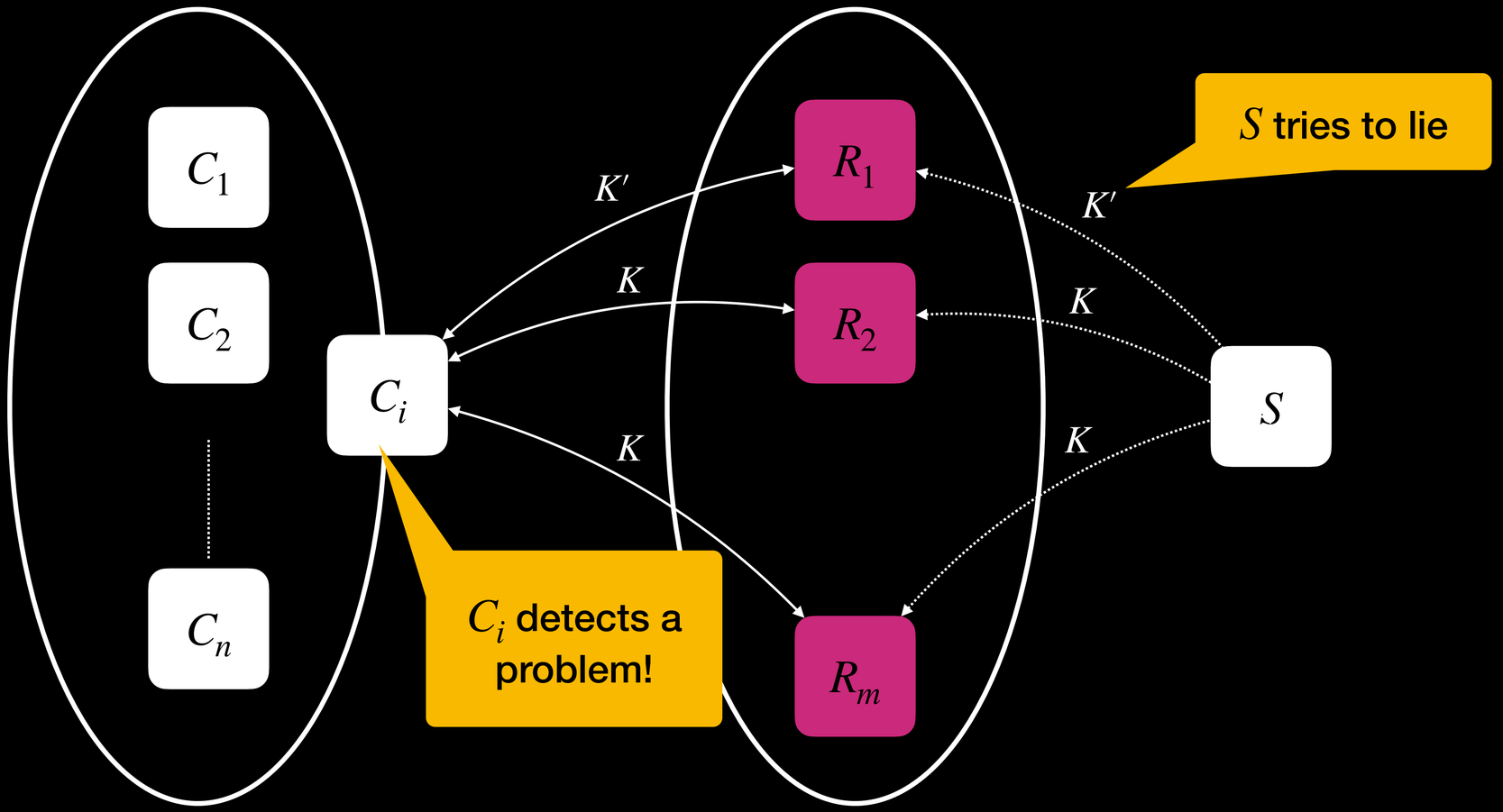
Multi-Proxy Discovery



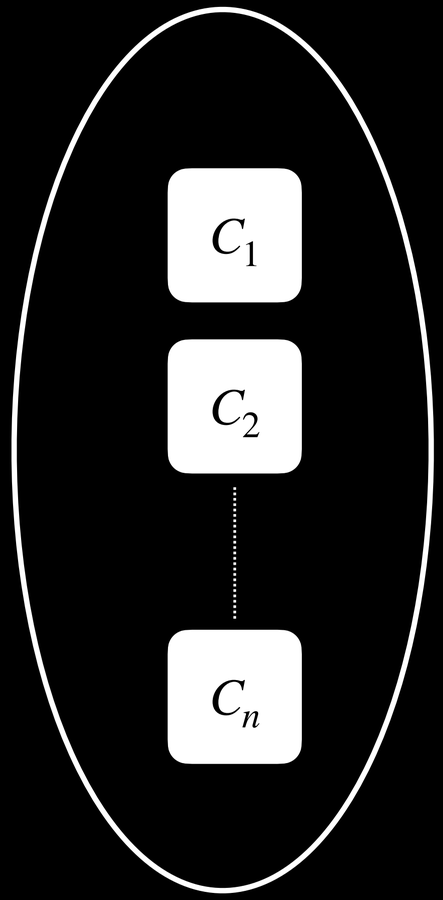
Multi-Proxy Discovery

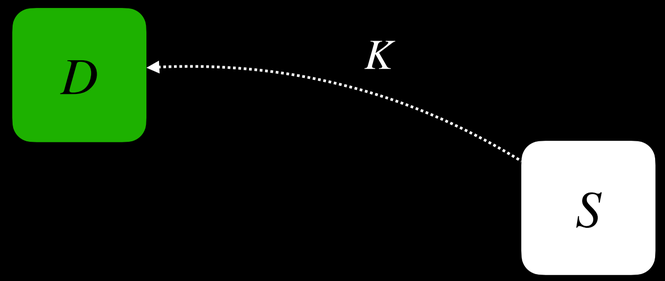


Multi-Proxy Discovery

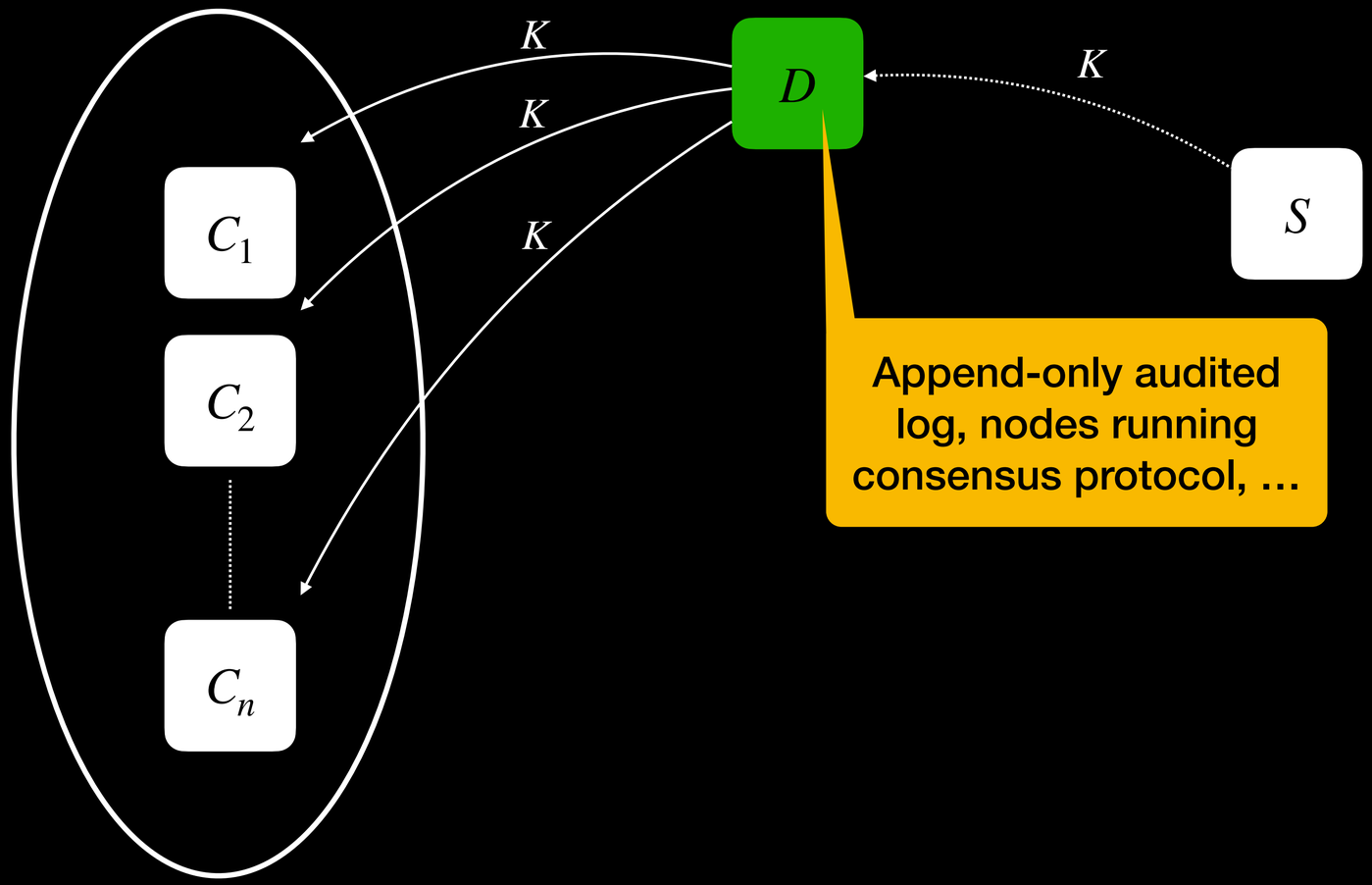


External Database Discovery





External Database Discovery



Wrapping Up

Status and questions for the group

Currently *not meant to be published as an RFC*

Most schemes can be deployed without any new technology

Questions for the group:

- Is this useful?
- How can this document help build reliable key consistency solutions and protocols?