Hyperledger Cactus Identity Management

June 10th, 2020
Everything said or implied here is subject to change
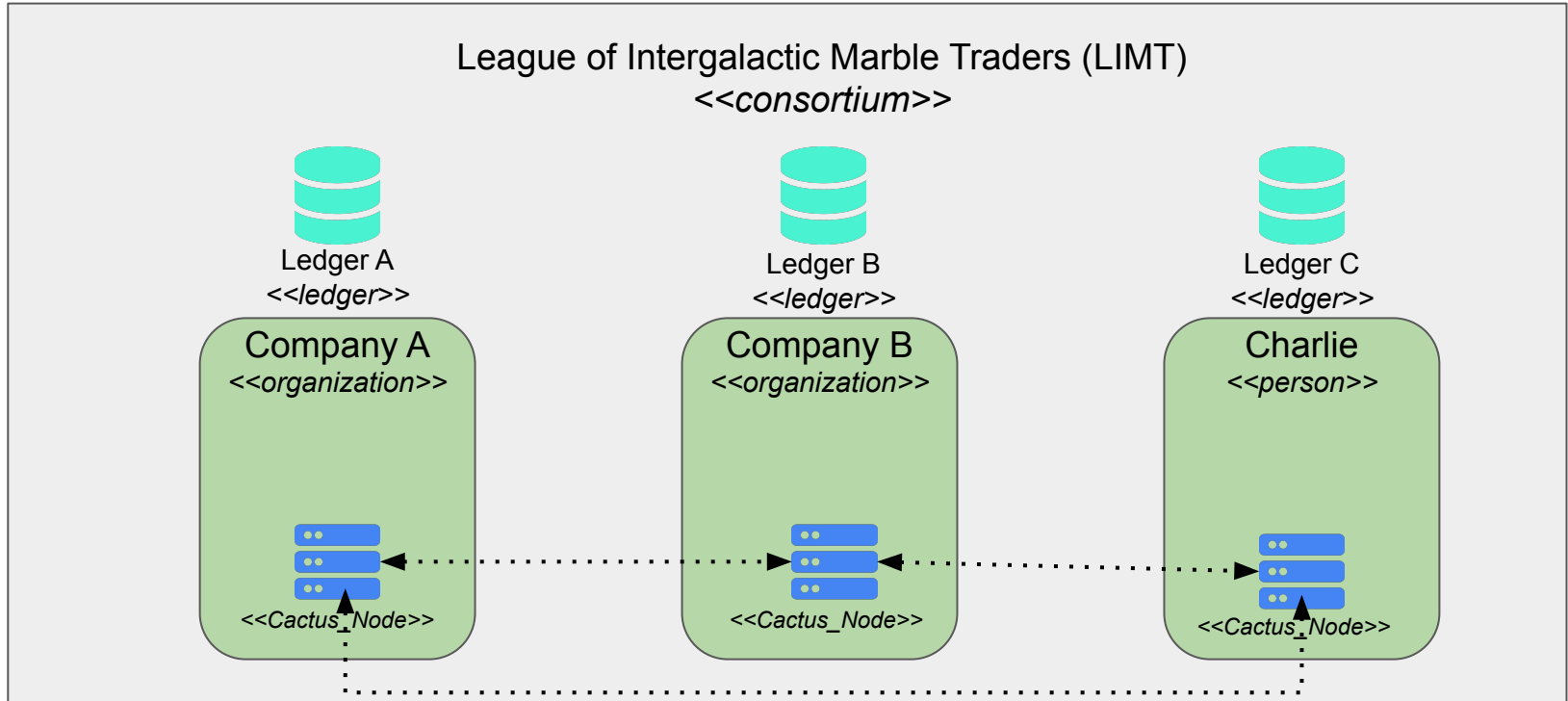
Safe Harbor

- Code presented/demoed here is on a feature branch of my personal fork of the repo

- Ideas/designs are subject to change or complete removal/abandonment based on maintainer feedback

- Reaching consensus among the maintainers about any of these items is not guaranteed

DRAFT - not yet proposed or approved by maintainers

Terminology - Consortium

- Consists of a set of members who can be:
    - Business entities
    - Private person
    - Any autonomous life-form capable of operating IT infrastructure (Cactus nodes)

Terminology - Consortium

League of Intergalactic Marble Traders (LIMT)
<<consortium>>

Ledger A
<<ledger>>

Ledger B
<<ledger>>

Ledger C
<<ledger>>

Company A
<<organization>>

Company B
<<organization>>

Charlie
<<person>>

<<Cactus_Node>>
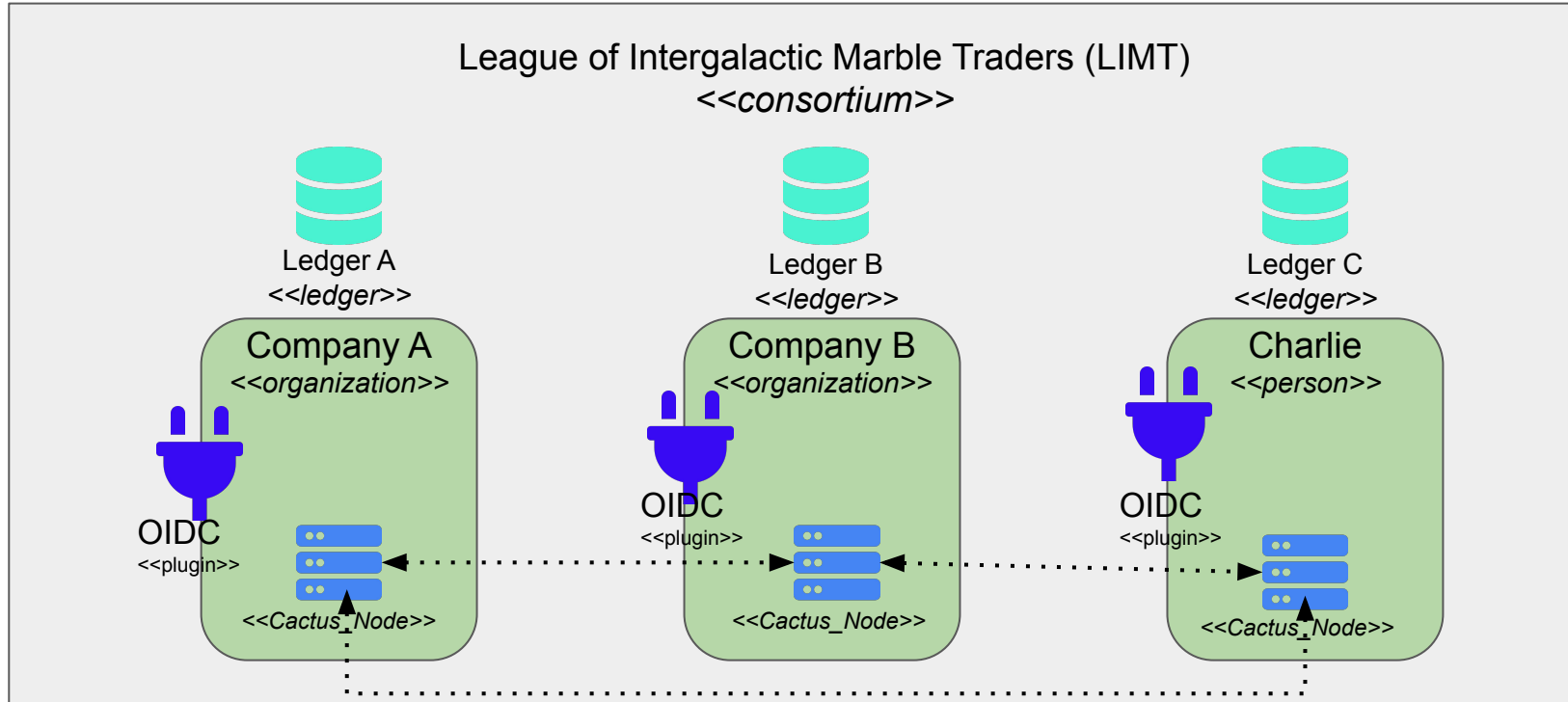
<<Cactus_Node>>

<<Cactus_Node>>

Idea - Open ID Connect

- Each consortium member should be able to provide their own identities that can be weaved together into a seamless user experience by applications
- Identity solution should remain in "plugin land"
  - "plugin land" like user space in the Linux kernel
  - "core land" like kernel space in the Linux kernel

DRAFT - not yet proposed or approved by maintainers

Idea - Open ID Connect #2

- In OIDC speak each consortium member is their own
  - Resource Provider
  - Identity Provider
  - User can opt-in on a per consortium <u>member</u> basis to authorize applications, different scopes, etc.
- Avoid centralized storage of anything (which is one of the design goals of OIDC/OAuth AFAIK)

OIDC Plugin

League of Intergalactic Marble Traders (LIMT)
<<consortium>>

Ledger A
<<ledger>>

Ledger B
<<ledger>>

Ledger C
<<ledger>>

Company A
<<organization>>

Company B
<<organization>>

Charlie
<<person>>

OIDC
<<plugin>>

OIDC
<<plugin>>

OIDC
<<plugin>>

<<Cactus_Node>>

<<Cactus_Node>>

<<Cactus_Node>>

DRAFT - not yet proposed or approved by maintainers

Idea - Open ID Connect #3

- Leverage standard OAuth authorization flows to allow user to log in via any one of the consortium member's Cactus nodes or via a common DNS host representing the entire consortium.

Current Code State

- Feature branch, not yet proposed as a pull request
- OIDC plugin is operational, but not yet polished or tested
  - Security audit required

Current Code State

- Feature branch, not yet proposed as a pull request
- OIDC plugin is operational, but not yet polished or tested
  - Security audit required

Code Demo