Hyperledger Cactus

Academic Paper Discussion #7

HYPERLEDGER
CACTUS

Western Hemisphere Meeting 21th January 2021

Agenda

1. Updates
2. Cactus protocol

Updates

Overleaf project updated - set of desired properties, structure, feedback appreciated

Papers

Security-focused paper - Hyperledger Cactus: A Distributed Operating System Enabling Blockchain Interoperability

Component-focused paper - Validators and Connectors for Blockchain Interoperability

Hyperledger Cactus: A Distributed Operating System Enabling Blockchain Interoperability

RQ1) What is a secure cross-blockchain transaction?

RQ2) What are the properties that a pair of blockchains need to assure, to enable secure cross-blockchain transactions?

RQ3) Can a trusted relay enable secure cross-blockchain transactions in a decentralized way?

Hyperledger Cactus: A Distributed Operating System Enabling Blockchain Interoperability

Propose CIP - Cactus interoperability protocol,

a generic cryptographic blockchain interoperability protocol, capable of realizing complex cross-blockchain logic.

Idea

Express the security properties (RQ1) of CIP via an ideal functionality Fcip, proving that CIP realizes Fcip in the UC framework.

CIP should connect public blockchains, private blockchains, other DLTs, and centralized systems (with different trust assumptions for each, see RQ2).

Should support flexible dApps (rooted on Business Logic Plugins, BLPs), managed by a consortium, where executions either finish with verifiable correctness or abort, where misbehaving parties are held accountable

Challenges

C1 - How to prove the state of a BLP, and the state stored in underlying ledgers.

C2- How to guarantee accountability to misbehaving parties

C3 - How to proceed in case of misbehavior? Financial atomicity, requiring nodes to hold collateral? Attempt of “reverting transactions”? Using legal frameworks?

CIP Components

Ledger View Generator - software that generates views from the underlying ledgers and expose them in a trusted repository. Uses validators and connectors.

BLP View Generator - generates a view on the decisions (i.e., transactions added to the transaction queue of the participants of the consortium) - consortium members' accountability

Transaction Processing Unit/API Server - Receives an endorsed transaction, by the Cactus participants using a BLP, and triggers them against the target ledgers.

Pcip - Plvg, Pblp, Pnode, Pcli, Pbc

Pcip has three phases: setup, execution, accountability

CLI -> Node
Node -> LVG
LVG -> BC

BPL -> Node
BLP -> BC

Validators and Connectors for Blockchain Interoperability

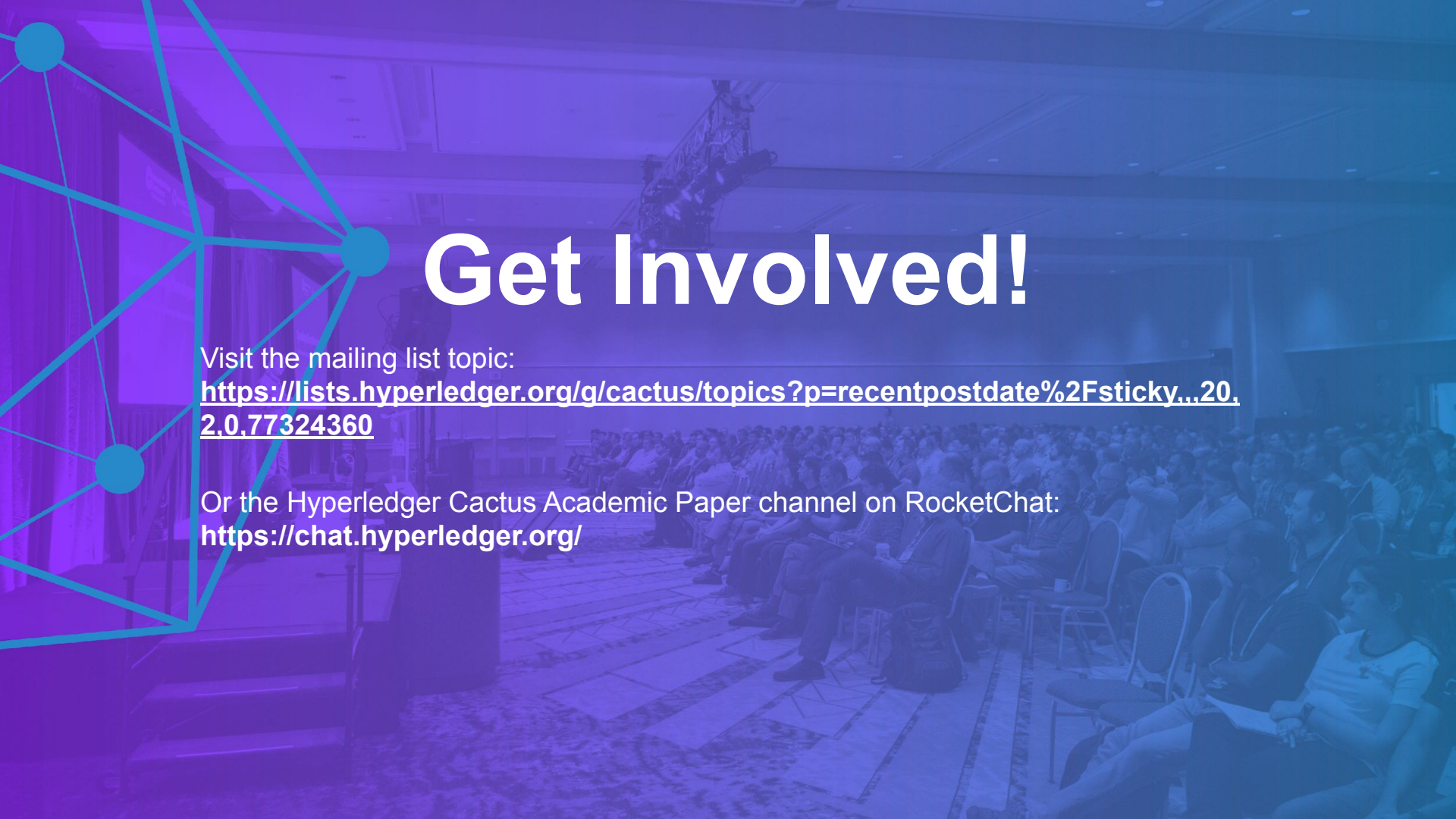
RQ1: Which properties should validators and connectors have, in order to assure security properties needed by Cactus?

RQ2: Can a (decentralized) quorum of validators and connectors be a reliable basis for oracle services, and, generally, blockchain interoperability?

Idea: Propose a model for validators and connectors

Validators and Connectors for Blockchain Interoperability

Good start: Foundational Oracle Patterns: Connecting Blockchain to the Off-chain World, 2020, Mühlberger et al.



Get Involved!

Visit the mailing list topic:
https://lists.hyperledger.org/g/cactus/topics?p=recentpostdate%2Fsticky,,,20,2,0,77324360

Or the Hyperledger Cactus Academic Paper channel on RocketChat:
https://chat.hyperledger.org/