Hyperledger Cactus
Academic Paper Discussion #9

HYPERLEDGER CACTUS

Western Hemisphere Meeting 4th March 2021

Agenda

1. Updates
2. Proposal for Cactus Interoperability Protocol

Papers

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

Component-focused paper - Validators and Connectors for Blockchain Interoperability

Useful References

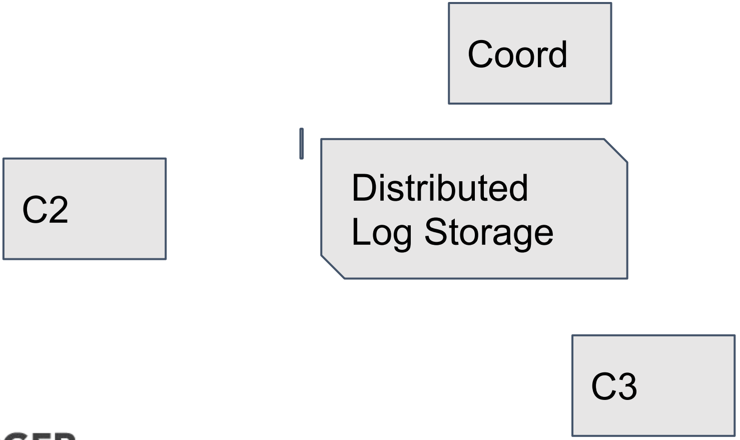
1. **HERMES: Fault-Tolerant Middleware for Blockchain Interoperability:** https://www.techrxiv.org/articles/preprint/HERMES_Fault-Tolerant_Middleware_for_Blockchain_Interoperability/14120291

Presents efforts from IETF on gateway-to-gateway asset transfers. Cactus is a generalization of these efforts.

Cactus Interoperability Protocol

CIP

Instantiation of consortium plugin that provides trust to cross-chain operations



Cactus Interoperability Protocol

CIP

Instantiation of consortium plugin that provides accountability to cross-chain operations

1. Setup
2. Validate
3. Connect
4. Check

Cactus Interoperability Protocol

CIP - Setup

Init nodes - setup private log, setup crypto, setup permissions

Trusted coordinator creates consortium - by setting up distributed log storage (DLS), and based on each node configuration creates a consortium profile, which is sent to all nodes

Consortium profile validation - by each node. Includes which BLP can be used, addresses of other cactus nodes, DLS, permissions, etc

Cactus Interoperability Protocol
CIP - Validate

On BLP Event - each time a BLP fires an event, this event is put on the DLS

A Quorum of validators signs the event - and records it on the DLS

The DLS containing signed events is the basis for trust in a cactus consortium

Cactus Interoperability Protocol

CIP - Connect

On BLP Event - a produced, valid event should trigger a response

Connector election - based on the consortium profile or chosen in runtime;

Connector generates a response - The connector issues a transaction and saves a proof at the DLS. This is the basis for disputes

Cactus Interoperability Protocol

CIP - Check

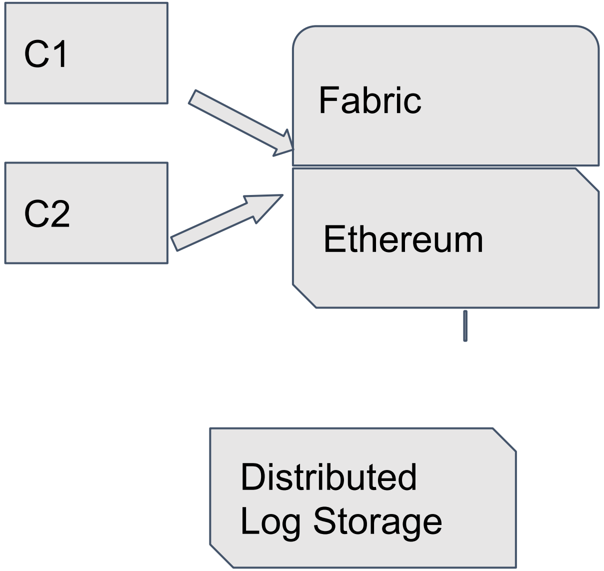
After a connector reacts to an event - a validator participating on the connectors' DLT may check the connectors actions

Disputes can be issued - if the action does not follow the rules

If a dispute is successful, the consortium can act

Cactus Interoperability Protocol

CIP Example



C1 -> C2 (Eth)
C2 -> C1 (Fabric token representing note)
Recorded on DLS

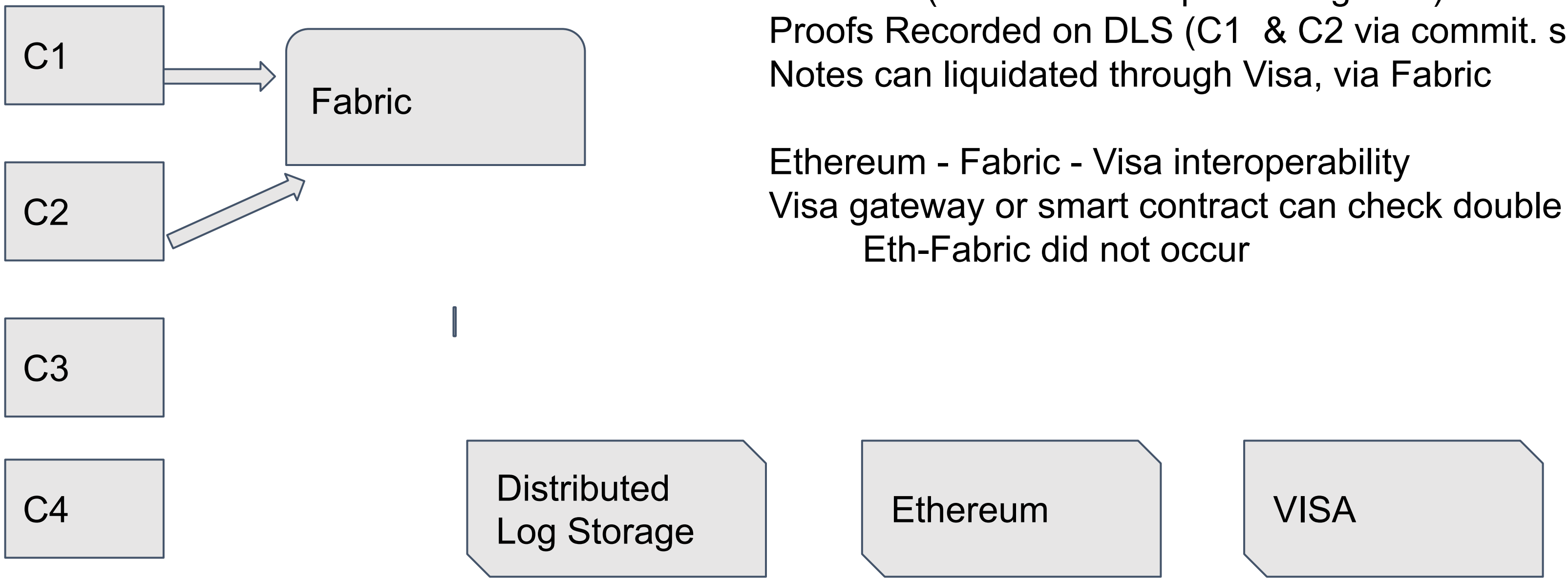
C1->C2($, via payment network, settle Fabric)

Ethereum - Fabric interoperability to Fiat
DLS to audit Eth transfers + Fabric mint + Fabric settlements

DLS can be public or permissioned, several degrees of robustness (see paper)

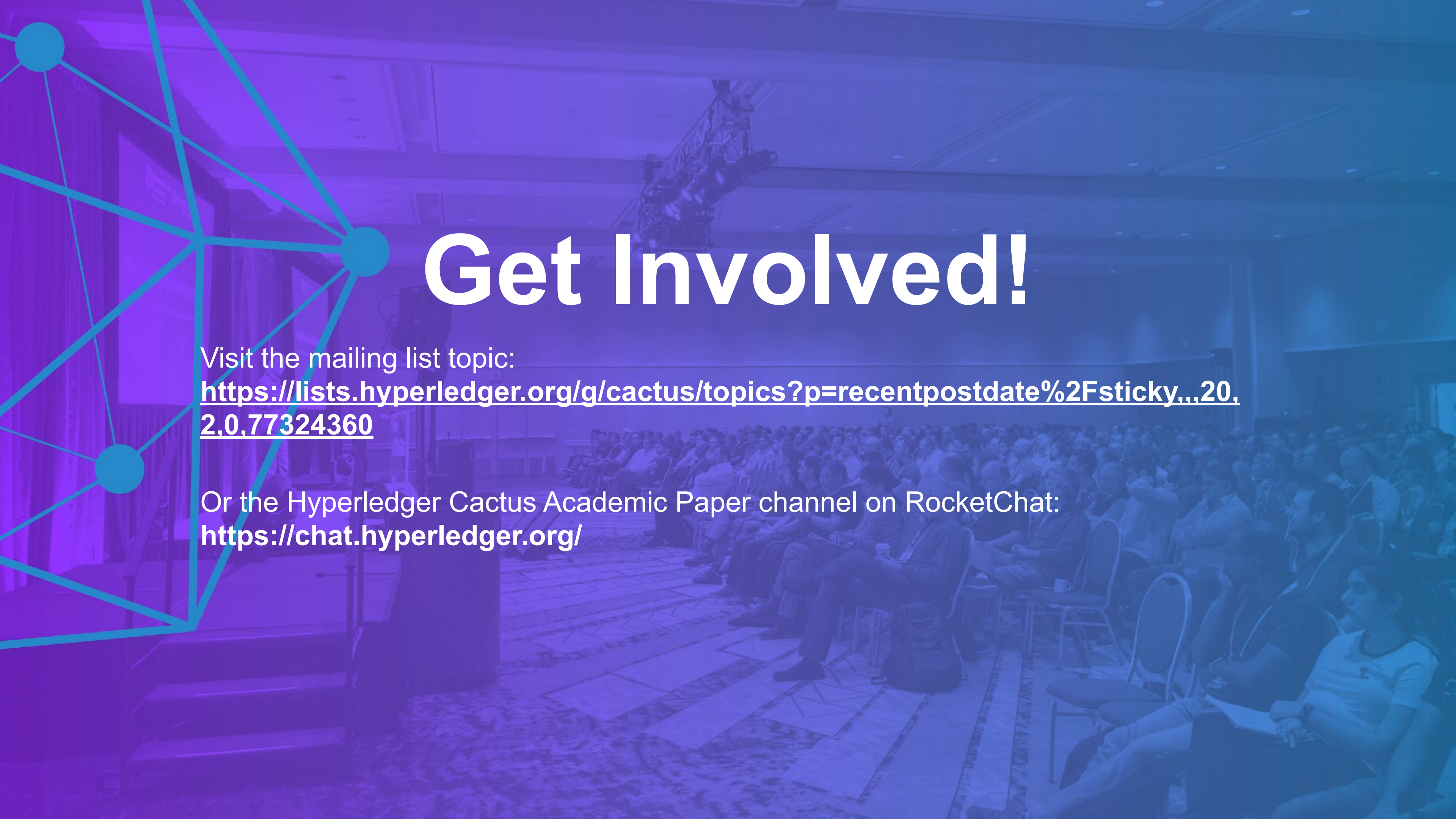
Cactus Interoperability Protocol

CIP Example++



C3 -> C1 (Eth)
C1 -> C3 (Fabric token representing note)
Proofs Recorded on DLS (C1 & C2 via commit. schemes
Notes can liquidated through Visa, via Fabric

Ethereum - Fabric - Visa interoperability
Visa gateway or smart contract can check double spend
Eth-Fabric did not occur



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/