



Using Distributed Ledger to Manage Trust Among Data Exchanges

Rohit Mital, KBR

Proud history, bright future.

© 2020 by KBR Inc. Published by The Aerospace Corporation with permission.

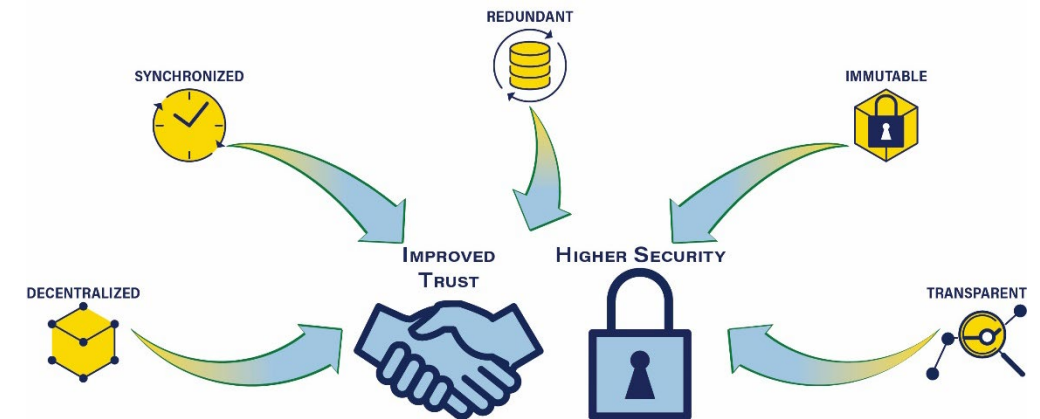
Improving Trust in Zero Trust Architecture (ZTA)

- ZTA leverages users, their locations whether to trust a user, machine or application seeking access to a particular part of the enterprise
- ZTA draws on technologies such as multifactor authentication, IAM, orchestration, analytics, encryption, scoring, file system permissions, etc.

Trust is inherently not a good thing

Trust is relative

In ZTA there is no implicit trust — the trust level is explicitly and dynamically calculated based on context.



Distributed Ledger can potentially improve trust by providing context to the data through an immutable digital passport

Agenda

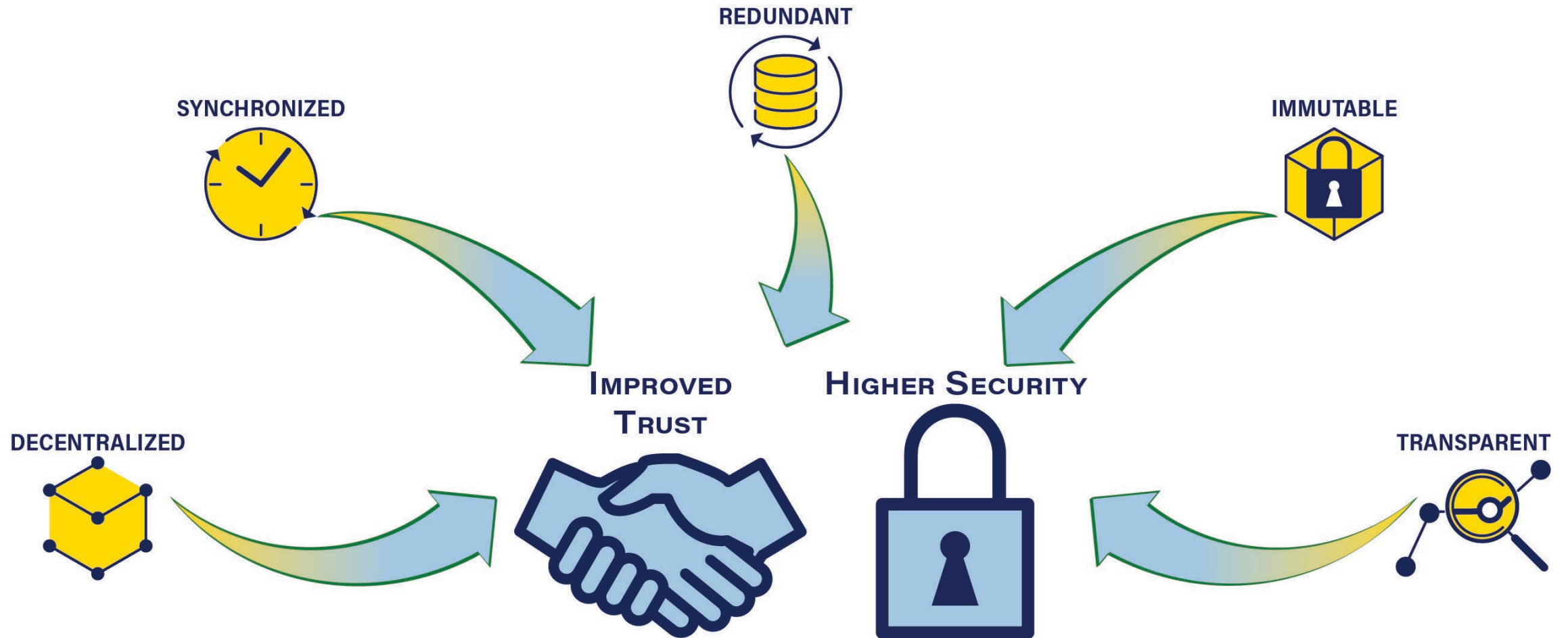
- Distributed Ledger Technology/Blockchain
- Applying Blockchain to Data Exchange
- Prototype
- Findings

Understanding Blockchain

- A Distributed Ledger Technology (DLT) is a database of digital data that is spread across multiple sites in a network
- Blockchain is a **cryptographically** secured, **immutable** and **distributed** ledger of **transactions** stored in data structures called "**blocks**"
- Blockchain Support Technologies
 - Smart Contracts: Digital code that runs automatically on blockchain network
 - Consensus: Process of keeping the ledger transactions synchronized
 - Participants : Entities that govern the blockchain updates
- Blockchain, smart contracts, consensus, and participants come together in creating a blockchain network

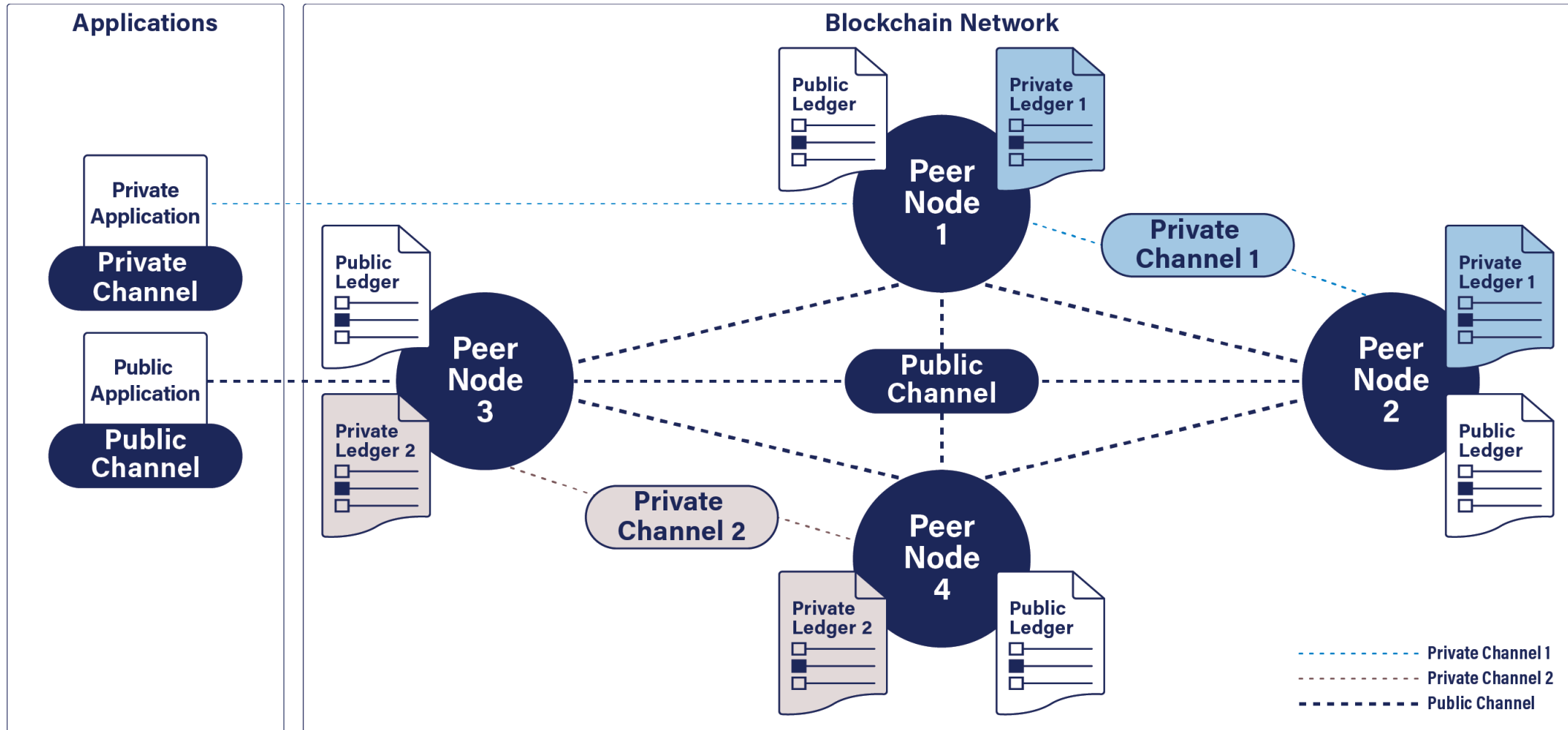
Blockchain Characteristics

These characteristics lead to two big advantages:



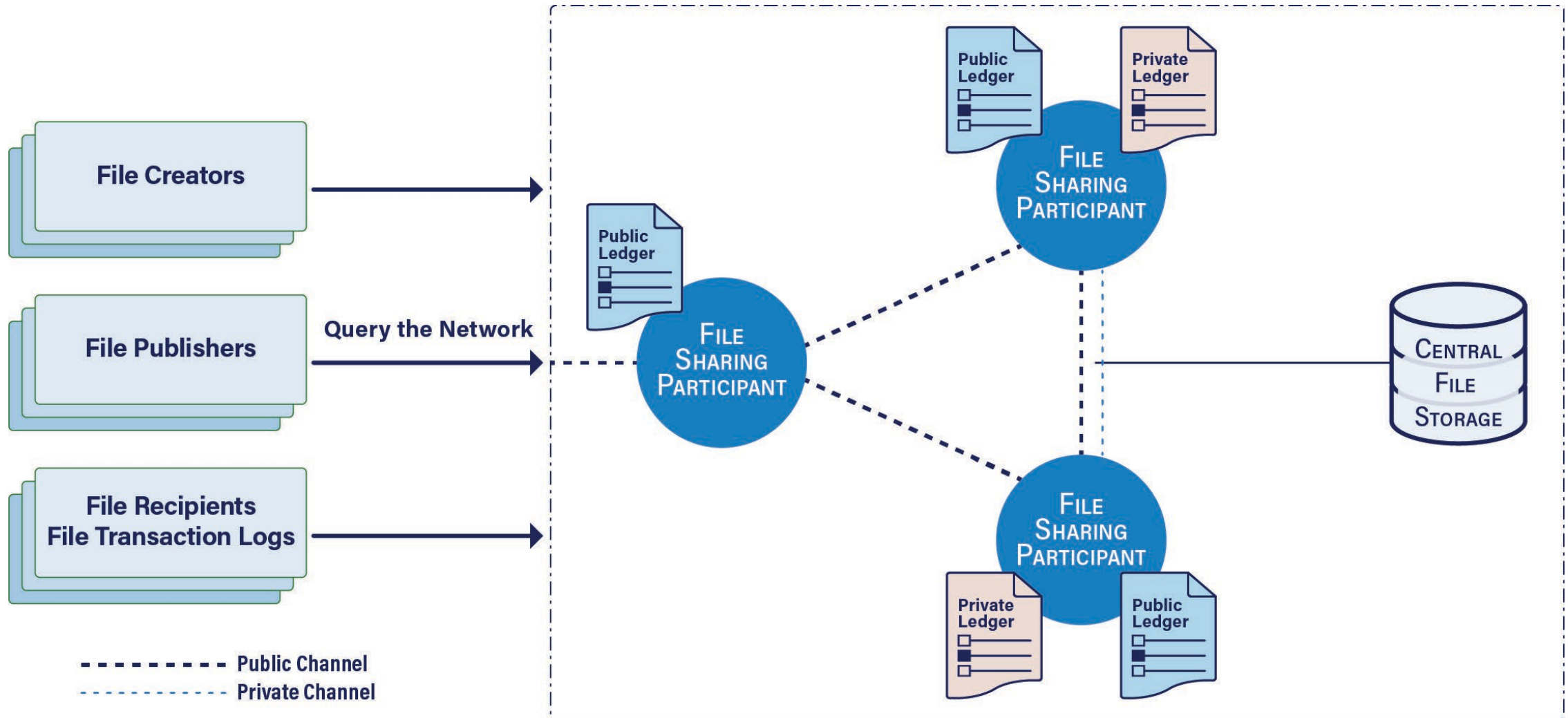
Blockchain Network

Blockchain Network Illustration



Applying Blockchain To Data Exchange

Data Exchange : Conceptual Architecture

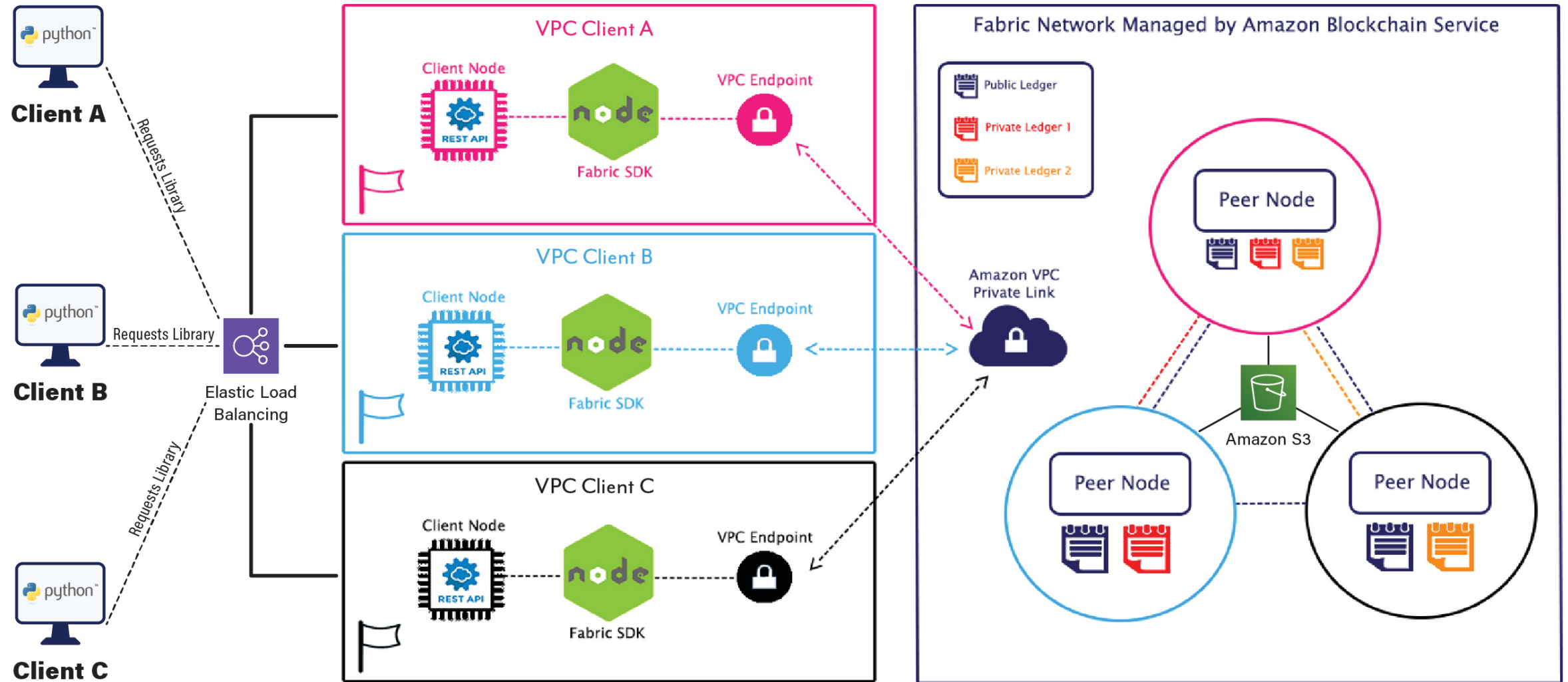


Blockchain Addressing Trust when receiving data

- **Question 1:** Can DLT provide an effective technical solution to “addressing zero-trust when acquiring data from non-federal data sources” on a global network of data providers?
- **Question 2:** Can the use of DLT provide a digital passport for each of the data files?
- **Question 3:** Can DLT offer a decentralized, democratized, universally acceptable governance mechanism for managing file exchanges?

Prototype: Data Exchange Blockchain Network

Prototype Design



Prototype Implementation Details

- Successfully deployed a Hyperledger Fabric network to AWS.
- The working prototype demonstrates the following functionality:
 - Creating, sending, and receiving files using an S3 bucket as CFS.
 - Sending file metadata to the AWS Managed Blockchain via a REST server
 - Data validated by chaincode prior to being committed to the ledger or allowing the client to perform the requested action.
 - Two channels (“public” and “private”) that restrict access to the ledger to members who belong to that channel.
 - Querying ledgers on a per-channel basis using the file URI as a search term and returning the results to the user.

Findings

Answers to DLT Questions

- **Question 1:** Can DLT provide an effective technical solution to “addressing zero-trust when acquiring data from non-federal data sources” on a global network of data providers?
 - Answer: With limitations
- **Question 2:** Can the use of DLT provide a digital passport for each of the data files?
 - Answer: Yes
- **Question 3:** Can DLT offer a decentralized, democratized, universally acceptable governance mechanism for managing file exchanges
 - Answer: Yes

DLT/Blockchain: Preliminary Conclusion

■ Key Advantages

- Decentralized, distributed paradigm eliminates single point of failure
- Digital Passport for files provides provenance of files
- Redundancy and availability provided by distributed ledger

■ Key Disadvantages

- Immutability implies continuous growth in storage
- Introduces complexity due to managing network members

Q&A