University POLITEHNICA of Bucharest

Faculty of Automatic Control and Computers,
Engineering and Management of Business Systems

RESEARCH REPORT

Hardware Supply on Blockchain

Scientific Adviser:
Prof. Gabriel Neagu

Author:
Adriana Dincă

Bucharest, 2019

Contents

List of Figures

Chapter 1

Introduction

1.1 Report Overview

In this report we aim to prove the advantages of using Hyperledger Fabric by building a supply chain system that is transparent for all the entities involved in this process and to reduce the time consumption of the acquisition procedures. Ixia has an exhausting CAPEX process for acquiring the hardware devices needed by the development and QA teams so we believe that building a system based on Blockchain that solves the transparency and bottleneck issues is the perfect fit for replacing the existing procedures.

1.1.1 Project Description

Hyperledger Fabric is a opensource framework developed by IBM and supported by the Linux Foundation that offers a permissioned private Blockchain solution. The framework is developed for private companies that know exactly the type of entities that are involved in their processes and what are their roles. Therefore the Hyperledger Fabric is suitable for solving the hardware devices supply chain transparency and bottleneck issues and to restrict the access of the participants involved in accordance with their position in the company. The hardware supply chain is CAPEX process that requires special approvals and priority analysis which is time consuming and often hard to track.

1.1.2 Project Objectives and Motivation

Hardware supply is an important aspect of the Ixia's employee daily work. Many software applications developed by Ixia teams run on dedicated hardware and in many situations only one employee can use that hardware at a time. The existing CAPEX procedure is very complicated and the time between ordering a new device and receiving it can be really long. It may happen that the team doesn't need it anymore at the time the device was received. The dedicated hardware is expensive (some chassis may cost up to $50000) so not receiving it on time may cost the department a lot of money and it can also delay the releases.

On each quarter, the manager has the responsibility of determining what are the hardware needs of the team and send the list to her/his superior for approval. Also, the manager has to check the price of the devices requested and if the costs are over the CAPEX budget, the hardware list should be prioritized. After completing the list and set the priorities if needed, the manager has to fill an *Internal Sales Order* on an internal platform. The hardware manufacturing managers have to check if there're are new ISOs for their teams to build or if they have the devices on stock. If the hardware machines are on stock they will be delivered to the department/manager that requested them. If there's no hardware with the desired specification on stock, the manager has to schedule it for manufacturing. Also, the manufacturing managers need to make sure that the financial transaction was done successfully before delivering the hardware so they have to discuss with the financial department and validate that everything is ok. A huge disadvantage of this procedure is the lack of transparency regarding the status of the order and the time estimation until receiving the order. In addition to this the costs may differ due to the international tax changes.

The **Hardware Supply Chain on Blockchain** project is a supply business network that solves both the transparency and the access' restrictions. This system is using Hyperledger Composer framework for modeling the business network: participants, transaction and assets and connects to the Hyperledger Fabric via its API to add transactions in the Blockchain database and to manage participants's access accordingly with their roles in the network.

Chapter 2

Project Technologies and Software

2.1 Hyperledger Project

Hyperledger is an open source project focused on Blockchain technology that aims to bring IoT, supply chain, finance, banking and manufacturing together. Is is hosted by the Linux Foundation and includes leaders from all the mentioned areas.

The Blockchain is a peer-to-peer distributed network, each participant of the network has its own copy of the ledger, and any transaction is validated by the majority of participants. The validation is done by solving Byzantine Generals Problem via consensus. The Hyperledger project offers solutions based on Blockchain and adds the possibility of creating *smart contracts* and has a large number of assistive tools to facilitate the embrace of Blockchain. All projects developed under the umbrella of Hyperledger and Linux Foundation are applications that use a ledger of transactions to establish transparency, accountability and trust. These projects are for a wide variety of business areas by providing the infrastructure, tools and frameworks to build applications based on Blockchain easily and in a short period of time. Additionally these applications follow the legal constrains by keeping the network closed to authorized participants that can be made accountable for their actions.

The project was launched in 2016 under the guidance of many important corporations such as IBM, Intel, etc. The first codebases that were released to the public were Hyperledger Fabric - a product that was the work result of three organizations (OpenBlockchain from IBM, libconsensus from Blockstream and the smart contracts from Digital Asset) and Hyperledger Sawtooth from Intel. These two frameworks were offering support for growing the development of Blockchain business solutions. Later on, there were other projects released that continued to offer assistive tools to support this growth. All projects that were released under the Hyperledger project were supervised by the Hyperledger Technical Steering Committee, a group of eleven specialists that were elected from the technical contributor community. In May 2016 the Linux Foundation and the corporate members involved in Hyperledger project elected an Executive Director to make sure that this idea has all the resources needed to be successful. In this position was placed the co-founder of Apache Software Foundation - Brian Behlendorf. The project became so successful so at the end of the next year the Hyperledger counted seven more projects and the number of members increased to more that 200.

The most successful projects were Hyperledger Sawtooth - multi-language support for distributed ledger, Hyperledger Fabric - the distributed ledger written in GO language, Hyperledger Composer - framework for accelerating the process of developing Blockchain applications, Hyperledger Iroha - the distributed ledger written in C++ and Hyperledger Indy - distributed ledger for decentralized identities. All these frameworks and tools are used in real-life applications except for Hyperledger Composer which is still in incubation. The Hyperledger Composer is an assistive tool for developers to facilitate the process of building a business network using the Hyperledger Fabric. It was proven that Hyperledger Composer is hard to maintain so the Hyperledger board decided to stop the development of new features and to keep the existing functionalities compatible with the new versions of Hyperledger Fabric. The main focus of the community is to add more features to Hyperledger Fabric framework which has a modular architecture so adding new features can be done quickly and without affecting the pre-existent functionalities.

In the following sections we are going to describe the Hyperledger Fabric and Composer frameworks. The Blockchain technology promises a revolution as big as the Web and the Hyperledger group understood its potential so they formed a Blockchain incubator to offer support to any bright idea related with Blockchain technology, smart contracts and the business world.

2.2 Hyperledger Fabric

2.2.1 General aspects

Hyperledger Fabric is an implementation of a distributed ledger developed mostly in Golang. The framework uses also other languages and technologies such as Javascript, Go or Java for smart contracts (chaincode), SDK in Node.js, Python, Java, Go and Rest. It is a solution for a secure, high-performance and permissioned Blockchain based network that has a modular architecture that allows plugins for any new features with no impact on the core functionalities.

Before getting into more details about the features provided by this framework it is important to mention that it is developed for enterprise use cases so the solution must solve the identity issue for transaction of type know-your-customer or the money laundering issue by offering transparency to authorities as participants with advanced permissions in the network. Thus this framework is permissioned which means that the participants are not anonymous, their identity is known by the other participants so they can be made accountable for their actions. The framework network is private and the transaction content is confidential so it can contain business sensitive information. In [1], Elli Androulaki and others are presenting the Hyperledger Fabric as a distributed operating system with all characteristics from the following paragraph.

More than that the framework offers the possibility of selecting a consensus protocol based on the business needs. For example, if the business network is used by a single enterprise or it is governed by a authorized identity there's no need for using the Byzantine Fault Tolerant (BFT) protocol so it may sufficient to go with a simplified version such as Crash Fault Tolerant (CFT) consensus protocol. As a result, the Hyperledger Fabric eliminates the low latency of transaction validation and improves the network performance. The framework doesn't required CPU power for mining or for smart contract execution so the cost is similar with any distributed system.

The Hyperledger Fabric has a wide community of developers and activists that help with the development and maintaining of Fabric codebase. The number of contributors has grown to more than 200 members and the organizations involved to 35 so the project benefits of a diverse set of skills. With such a support the future of this project is really promising. It has modular and pluggable architecture so it can bring innovation to many industries.

2.2.2 Technical aspects

Modularity is one of the main characteristics of Hyperledger Fabric. It was designed to have a modular architecture so it can be used by a large number of industries from manufacturing to finance.

The project was designed to be modular so all the components can be plugged in/out. The list of components is composed of:

- an *ordering service* that makes sure that the order of transaction is correct and that the all peers receives the blocks of transactions via broadcast; the ordering services can be plugged in/out and it runs in an independent environment (e.g Docker container named *hyperledger/fabric-orderer*);
- a *membership service provider* that enables only authorized entities to take part in the network(e.g a Docker container named *hyperledger/fabric-ca*); any entity that wants to connect to the business network has to have a cryptographic identity created by the business network Certification Authority (CA);
- *smart contracts* are applications that run independently in docker containers or other isolated environments and store agreements between network members; these smart contracts are named *chaincode* and they can be written in almost any programming language;
- a variety of *DBMS* options to store the ledger; a common option is CouchDB that runs in a Docker container named *hyperledger/fabric-couchdb*;
- more application's constrains for approval and validation policy;
- an optional *peer-to-peer gossip service* to leverage messages to all the peers by broadcast; makes sure that everyone receives up-to-date information about the ledger transactions and fills in any gaps if one node missed some of the broadcasts.

The chaincode (smart contract) is an application that facilitates and verifies the execution of a digital agreement between one or more network participants. The ledger is responsible for executing the digital contract at the time that it need to be applied. In a business network one or more digital contracts can co-exist and everyone that is connected to that network can create a contract. The network is responsible for validating that application code and it should be consider invalid until it is validated using order-execute architecture. In most blockchain systems the smart contracts follow the rule order-execute so to reach consensus the order-execute design should be deterministic. Building a deterministic architecture is quite challenging and the code should be written in domain-specific programming languages (e.g Ethereum developed a DSL - Solidity for their decentralized applications) in most of the cases. Additionally this architecture brings performance issues due to the fact that transactions are added sequentially in the ledger.

The Hyperledger Fabric tries to solve the overhead of using the order-execute approach by proposing a new architecture type - execute-order-validate. This new design is composed by three stages. In the first stage the transactions are checked for correctness and if so they are immediately executed. After that, they are ordered using a consensus protocol and in the last stage they are validated according to an endorsement policy and added to the ledger. As a result of this approach the Hyperledger Fabric solves the issue of using DSL and non-determinism by removing any inconsistency and reduces the performace overhead. By removing any non-deterministic problem, the smart contracts can be written in any standard programming language. The first supported languages are Go and Node.js but the board of Hyperledger plans to support more popular programming languages such as Java in the future releases.

Permissioned blockchain refers to restricting the access to the network to a known group of participants that are worth it to be trusted. It is not necessary that participants may know each other but all of them should be vetted by a trustful authority. The Fabric is using a permissioned blockchain system so each member of the business network can easily be identified and if his/her actions (e.g deploying a smart contract or changing the configuration of the network) are malicious that member can be made accountable and pay for them. In a permissionless blockchain system it is very hard to identify the real person that stood behind a certain action so Hyperledger Fabric is more suitable for business. The Certification Authority is one instrument that can vet for the business network members and any respectful business can easily obtain the authorization to participate in the network.

Privacy and confidentiality is key for most of the business use-cases therefore any solution used has to guarantee that the data cannot be available to the public. In permissionless systems the transactions' data is available to every node in the blockchain network so such a system fails to fulfill the privacy business requirements. The main approach of permissionless blockchain systems is to encrypt their data. However, this solution is far from perfect because businesses can hold enough computational power to break any encryption in a reasonable amount of time. The approach of permissioned systems is to restrict the distribution of private data to only the involved participants via a channel. The Hyperledger Fabric allows any member of the network to create channels for different purposes so they can share confidential data with authorized members. Another solution that can solve this issue for both for permissionless and permissioned blockchains is the Zero Knowledge Proofs (ZKP) but it is an area under research so in the meantime creating channel to share data with authorized entities is a good alternative.

As mentioned above, the Hyperledger Fabric offers support for pluggable components for many of its features. The ordering service is a pluggable module that is responsive for achieving consensus of ordering transactions. In the literature is mentioned two consensus algorithms: Crash Fault Tolerant (CFT) and Byzantine Fault Tolerant (BFT). For these two algorithms there can be more than one implementation. For example, the Hyperledger Fabric has two possible implementations for the CFT algorithm: Kafka (based on Zookeeper) and *etcd* library from Raft.

The performance of Hyperledger Fabric depends on a variety of parameters: the number of nodes of the network, the number and size of transactions and hardware limitations so it is difficult to generalize the performance of the Hyperledger Fabric project. In order to determine the performance of a Business Network based on Fabric, the Hyperledger team has developed another project called Hyperledger Caliper. The community is contributing to define the set of measures that affect performance and scalability to help Caliper team build a powerful framework for benchmarking.

Taking all these into account, the Hyperledger Fabric is one of the best solution for permissioned distributed systems that integrates the blockchain technology. The Hyperledger community is really involved in improving and building strong solutions for blockchain business networks and the Hyperledger Fabric project has the biggest support from the community. Fabric supports a wide range of industries: from banking, manufacturing, supply chain to retail, healthcare, etc.

2.3 Hyperledger Composer

Chapter 3

Project Implementation

3.1 Functionalities

Chapter 4

Project Use Cases

4.1 ISG CAPEX Procedure

The *Hardware Supply on Blockchain* use cases are ordering a new hardware device or returning the merchandise authorization(RMA). ISG(Ixia Solution Group) teams are focused on developing software solutions starting with testing the network performance, getting network visibility by monitoring the traffic or finding security threats before compromising any data. Therefore teams need specialized hardware devices such as routers, gateways, switches to more powerful machines as packet brokers, ESXI servers, clusters, etc. The ISG division offers deep expertise in network testing, security and visibility which requires investing in powerful hardware equipment. In each quarter of the financial year the ISG division has a CAPEX budget to invest in hardware so each team can request new hardware devices. Each manager has the responsibility of identifying the hardware requirements by consulting his/her team and assuring that the total cost doesn't exceed the budget in which case the devices list should be prioritized.

When the CAPEX requirements list is completed, the manager can proceed to order them. For ordering the equipment he/she will use the *Hardware Supply on Blockchain* system.

The RMA procedure can be performed by the team manager as soon as he/she is informed about the hardware malfunction. Most hardware devices have an warranty period where they can be replaced or repaired free of charges by the manufacturing divisions.

4.2 Use Case Description

Chapter 5

Conclusion

Bibliography

[1] Vita Bortnikov Christian Cachin Konstantinos Christidis Angelo De Caro David Enyeart Christopher Ferris Gennady Laventman Yacov Manevich Srinivasan Muralidharan Chet Murthy Binh Nguyen Manish Sethi Gari Singh Keith Smith Alessandro Sorniotti Chrysoula Stathakopoulou Marko Vukolić Sharon Weed Cocco Jason Yellick Elli Androulaki, Artem Barger. Hyperledger fabric: A distributed operating system for permissioned blockchains. Appears in proceedings of EuroSys 2018 conference, https://arxiv.org/abs/1801.10228v2. Accessed Mar. 2019.