A Tutorial on Blockchain and Hyperledger Fabric

Alessandro Sorniotti
IBM Research - Zurich
aso@zurich.ibm.com

Marko Vukolić
IBM Research - Zurich
mvu@zurich.ibm.com

I. Motivation and Goals

Blockchain technology, initially driven by Bitcoin, is both an exciting emerging industry, but also a fascinating blend of different computer science areas such as distributed systems, security, cryptography, programming languages, formal verification, etc.

Hyperledger Fabric [1] is an open source system for deploying and operating blockchains and one of the Hyperledger projects hosted by The Linux Foundation, licensed under Apache 2.0 license. It focuses on permissioned blockchains, in which participants in the blockchain network are first vetted by other participants or some (de)centralized admission authority. As such it targets blockchain and distributed ledger technology across different industrial and business use cases, in addition to being amenable to so-called public blockchain deployments.

The goal of this tutorial is to educate attendees in the basic principles of permissioned and permissionless blockchain technology. Then we discuss Hyperledger Fabric in detail, covering its unique architecture, the rationale behind it as well as its most important distributed systems and security aspects. Finally we include a set of hands-on exercises where attendees will be able to learn how to deploy Hyperledger Fabric, but also how to develop basic distributed applications on Fabric. At the end of the tutorial, attendees will have basic knowledge of blockchain technology as well as how to use Hyperledger Fabric.

II. Content and Organization

The tutorial starts from covering basics of blockchain technology, covering typical assumptions, use cases and challenges. Then, we dive into blockchain implementations. We discuss permissioned and permissionless blockchains, detailing Proof-of-Work consensus and state-machine-replication (voting) consensus protocols [3]. These serves us as a lead to introduce the classical order-execute architecture of blockchains [1]. We then point out limitations of order-execute and conclude this part of tutorial with discussion on open research challenges in blockchain.

We turn then to Hyperledger Fabric [1], and present its architecture, design rationale as well as its distributed systems and security aspects. We introduce Execute-Order-Validate architecture of Fabric and its hybrid application execution model mixing passive and active replication. We then detail execution and validation phases of Fabric, focusing on parallelism. We explain Fabric's modular consensus service and its existing CFT and BFT [2] implementations. We conclude with describing other components of Fabric such as Membership Service Providers, Gossip, Ledger and others.

The last part of the tutorial consists of hands-on exercises. These cover deployment of Fabric, developing chaincode applications with standard validation and validation of customization. This also covers different ways of implementing a cryptocurrency in Fabric.

Below is the detailed outline of the tutorial:

1) Introduction to Blockchain
    a) What is a blockchain?
    b) History of Blockchains
    c) Typical assumptions
    d) Use cases
    e) General challenges
2) Permissionless vs. Permissioned blockchain
    a) Introduction to Proof of Work
    b) Introduction to BFT state-machine replication
    c) Order-Execute (OE) blockchain architecture
    d) Limitations of OE architecture
    e) Challenges and open research problems
3) Hyperledger Fabric system architecture
    a) Requirements
    b) Execute-Order-Validate (EOV) architecture
    c) Execution/Validation in Fabric
    d) Ordering service modularity
    e) Other components: MSP, Gossip, Ledger, etc.
4) Hyperledger Fabric hands-on exercises
    a) System deployment
    b) Developing chaincode with standard validation
    c) Customizing validation
    d) Developing a UTXO cryptocurrency in Fabric
5) Conclusion

References

[1] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Eurosys'18*, 2018.

[2] J. Sousa, A. Bessani, and M. Vukolić. A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. In *DSN'18*, 2018.

[3] M. Vukolić. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *Open Problems in Network Security - IFIP WG 11.4 International Workshop, iNetSec*, pages 112–125, 2015.