# Hyperledger Fabric

Subjects: Computer Science, Information Systems

Contributor: Filippos Pelekoudas-Oikonomou , José C. Ribeiro , Georgios Mantas , Georgia Sakellari , Jonathan Gonzalez

Hyperledger Fabric is a distributed ledger platform for developing applications with modular architecture. Support for pluggable consensus protocols is one of the platforms most distinguished features.

hyperledger fabric

## 1. Introduction

Hyperledger Fabric has been proposed by Androulaki et al. [1] and developed by Linux Foundation [2], and it is a distributed ledger platform for developing applications with modular architecture [3]. This platform provides pluggable consensus protocols (mainly PBFT-based) and a private-permissioned blockchain model. It is suitable for deploying IoT applications for stakeholders that partially trust each other. This implementation platform has low scalability due to the nature of PBFT algorithms and 33.33% (1/3) adversary tolerance. However, it provides high privacy and throughput and supports the development of smart contracts.

Support for pluggable consensus protocols is one of the platforms most distinguished features. This support makes it possible to tailor the platform more effectively to specific use cases and trust models. For instance, fully byzantine fault-tolerant consensus may be deemed redundant and an undue drag on performance and throughput when it is deployed within a single business or when it is controlled by a trusted authority. In circumstances such as these, a consensus protocol that is crash fault-tolerant (CFT) may be more than sufficient; however, in a multi-party, decentralized use case, a consensus protocol that is byzantine fault-tolerant (BFT) may be necessary [4]. For all these reasons, HF can be a viable blockchain platform to develop upon lightweight blockchain-based security solutions for IoMT networks [5][6].

In HF, the workflow from the initiation of a transaction to the update of the ledger involves several stages, as shown in **Figure 1**. As a first step, a transaction is initiated by a client. Secondly, the transaction is sent along with other transactions into the endorsing peers. Then it is endorsed by the set of designated endorsing peers according to the specified endorsement policy. These peers simulate the execution of the transaction and generate a proposal response that includes the outcome and read/write sets. Following this, the transactions along with the collected endorsed proposal responses are sent to the ordering service. The ordering service establishes a consensus on the order of the transactions and assembles them into a block. Then the block is appended to the chain and transferred to the peers that update their local copy of the ledger and endorse the updates. The ledger is then updated across all peers, ensuring the consistency of the data among the network participants. This workflow guarantees a secure, transparent, and auditable process for updating the ledger in HF.

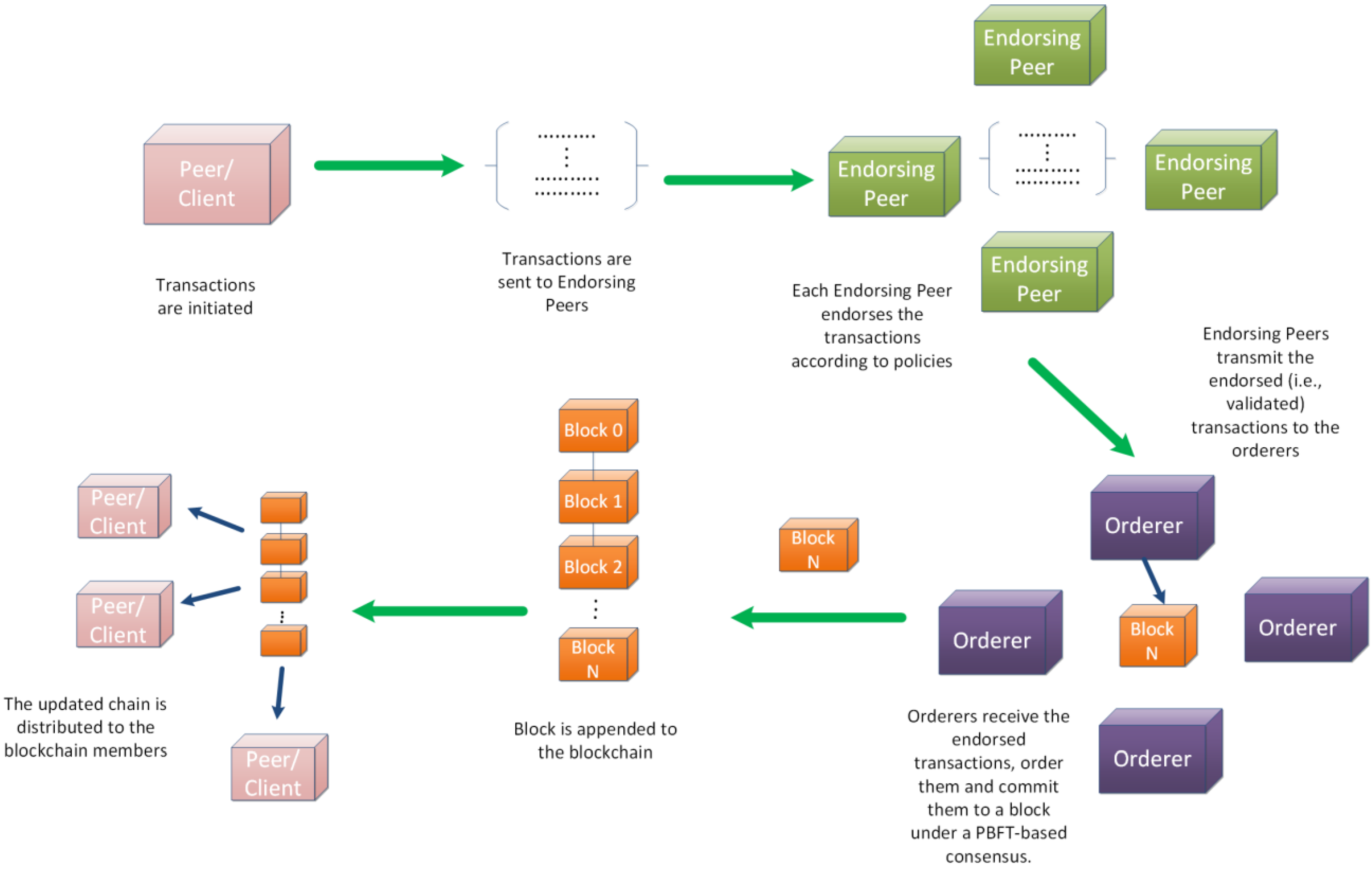
Peer/ Client
Transactions are initiated
Transactions are sent to Endorsing Peers
Endorsing Peer
Endorsing Peer
Endorsing Peer
Endorsing Peer
Each Endorsing Peer endorses the transactions according to policies
Endorsing Peers transmit the endorsed (i.e., validated) transactions to the orderers
Orderer
Block N
Orderer
Orderer
Orderer
Orderers receive the endorsed transactions, order them and commit them to a block under a PBFT-based consensus.
Block N
Block 0
Block 1
Block 2
Block N
Block is appended to the blockchain
Peer/ Client
Peer/ Client
Peer/ Client
The updated chain is distributed to the blockchain members

**Figure 1.** Transaction Workflow in HF.

## 2. Hyperledger Fabric

The main components of HF are the following:

*Blockchain Network*: This can be understood as a collection of nodes that form a Peer-to-Peer (P2P) network in which every node shares a common distributed ledger and complies to the state of the ledger through a consensus protocol. In the case of HF, the blockchain network can provide, besides the distributive ledger, the feature of chaincode, a form of smart contract, that can be utilized to generate transactions that are then transmitted to each peer node in the network and immutably recorded on their copy of the distributed ledger.

*Peer*: This is the main component of the blockchain network. Peers are the parts of the network where the blockchain ledger and the chaincode are hosted. Peers can also host SDK and APIs, through which network users can interact with applications and services. Peers are separated into two categories: (a) anchor peers and (b) endorsement peers. The former are responsible for distributing the blocks to the latter, while endorsement peers are responsible for endorsing the chaincode that is invoked by clients. Endorsement policies are pre-specified by the chaincode and define the number of peers that are needed to execute and endorse the specific chaincode.

*Ordering Service*: Different from the permissionless blockchains (e.g., Bitcoin, Ethereum) that come to consensus with a probabilistic process, HF uses the orderer node that, as the name indicates, orders the transactions. The group of ordering nodes compose the ordering service. After the ordering of the transaction, the deterministic consensus of the Hyperledger Fabric follows. Ordering is taking place in the specific nodes, and it is separated from the endorsing of transactions that takes place in peers. HLF provides three implementations of ordering service: Solo, Kafka, and Raft [7].

*Certificate authority (CA):* This is a tool that, as the name indicates, generates certificates for admins, users, peers, orderers, or applications in the form of an X.509 certificate [8] to identify the aforementioned blockchain network entities. Besides the identity for the entities that is issued by CA, CA also defines the privileges of the entities over the network.

*Chaincode*: This is the piece of code that acts as an application and provides functionalities to the established blockchain network, and it is carried in a Docker container. For this implementation, node.js language for chaincode implementation is going to be used, but in other cases chaincode can be written in programming languages such as Go or Java.

*Channels*: These provide the communication between the nodes of the network. They comprise organizations, peers for each member, and the distributed ledger, as well as the chaincode. Channels are the places where transactions are proposed and handled. In Hyperledger fabric a node can participate in more than one channel and transmit information and data privately.

*Endorsement policies*: Endorsement policies specify the number of peers on a channel that are necessary to execute the chaincode of a transaction and endorse the results of this execution for the transaction to be credited as valid. As part of the transaction validation process performed by the peers, each validating peer verifies that the transaction has the correct number of endorsements.

*Membership Service Provider (MSP)*: MSP is a component of HF that abstracts membership activities. An MSP detaches all cryptographic processes and protocols underlying certificate issuance, certificate validation, and user authentication and allows peers to validate incoming transaction requests from clients and sign transaction outcomes. An MSP can establish its own concept of identity, as well as the rules by which identities are managed and authenticated.

As described, HF’s unique qualities make it a highly scalable system for permissioned blockchains that supports changeable trust assumptions, enabling the platform to accommodate a vast array of industrial use cases (e.g., banking, supply chain and more) from which one of them is on the scope of this research work: healthcare. The lightweight nature of HF, is what makes this platform a suitable choice for HF-based security architecture for IoMT-based health monitoring systems, keeping into consideration both the design needs as well as the resource constraint nature of IoMT nodes.

The support for private transactions is one of the key reasons why HF is ideal for IoT networks. HF enables private transactions between specific parties, preserving the confidentiality of sensitive data while offering modular architecture, which allows it to be tailored to the exact requirements of an IoT network. Scalability is another significant property of HF that makes it suited for IoT networks. The volume of data created by an IoT network grows in direct proportion to the number of devices in the network. HF is built to manage massive amounts of data and can be horizontally scaled to accommodate more devices and transactions. Finally, the consensus method of HF is well-suited for IoMT networks as it ensures that all network participants agree on the state of the ledger, which is critical in an IoMT network because numerous devices may perform transactions at the same time.

In conclusion, Hyperledger Fabric's support for private transactions, modular architecture, scalability, and consensus mechanisms make it an appropriate blockchain platform for IoT networks [1][9][10].

## References

1. Androulaki, E.; Barger, A.; Bortnikov, V.; Muralidharan, S.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Murthy, C.; Ferris, C.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018.
2. Projects—Linux Foundation. Available online: https://www.linuxfoundation.org/projects/ (accessed on 8 June 2022).
3. Hyperledger Fabric—Hyperledger Foundation. Available online: https://www.hyperledger.org/use/fabric (accessed on 24 January 2022).
4. Introduction—Hyperledger-Fabricdocs Main Documentation. Available online: https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html (accessed on 8 June 2022).
5. Pelekoudas Oikonomou, F.; Ribeiro, J.; Mantas, G.; Bastos, J.; Rodriguez, J. A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems. In Proceedings of the 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 5–8 September 2021.
6. Oikonomou, F.P.; Mantas, G.; Cox, P.; Bashashi, F.; Gil-Castineira, F.; Gonzalez, J. A Blockchain-based Architecture for Secure IoT-based Health Monitoring Systems. In Proceedings of the 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Porto, Portugal, 25–27 October 2021; pp. 1–6.

7. Shalaby, S.; Abdellatif, A.A.; Al-Ali, A.; Mohamed, A.; Erbad, A.; Guizani, M. Performance Evaluation of Hyperledger Fabric. In Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 608–613.
8. X.509: Information Technology—Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks. Available online: https://www.itu.int/rec/T-REC-X.509-201910-I/en (accessed on 8 June 2022).
9. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.
10. Pelekoudas-oikonomou, F.; Zachos, G.; Papaioannou, M.; De Ree, M.; Ribeiro, J.C.; Mantas, G.; Rodriguez, J. Blockchain-Based Security Mechanisms for IoMT Edge Networks in IoMT-Based Healthcare Monitoring Systems. Sensors 2022, 22, 2449.

Retrieved from https://encyclopedia.pub/entry/history/show/112278