

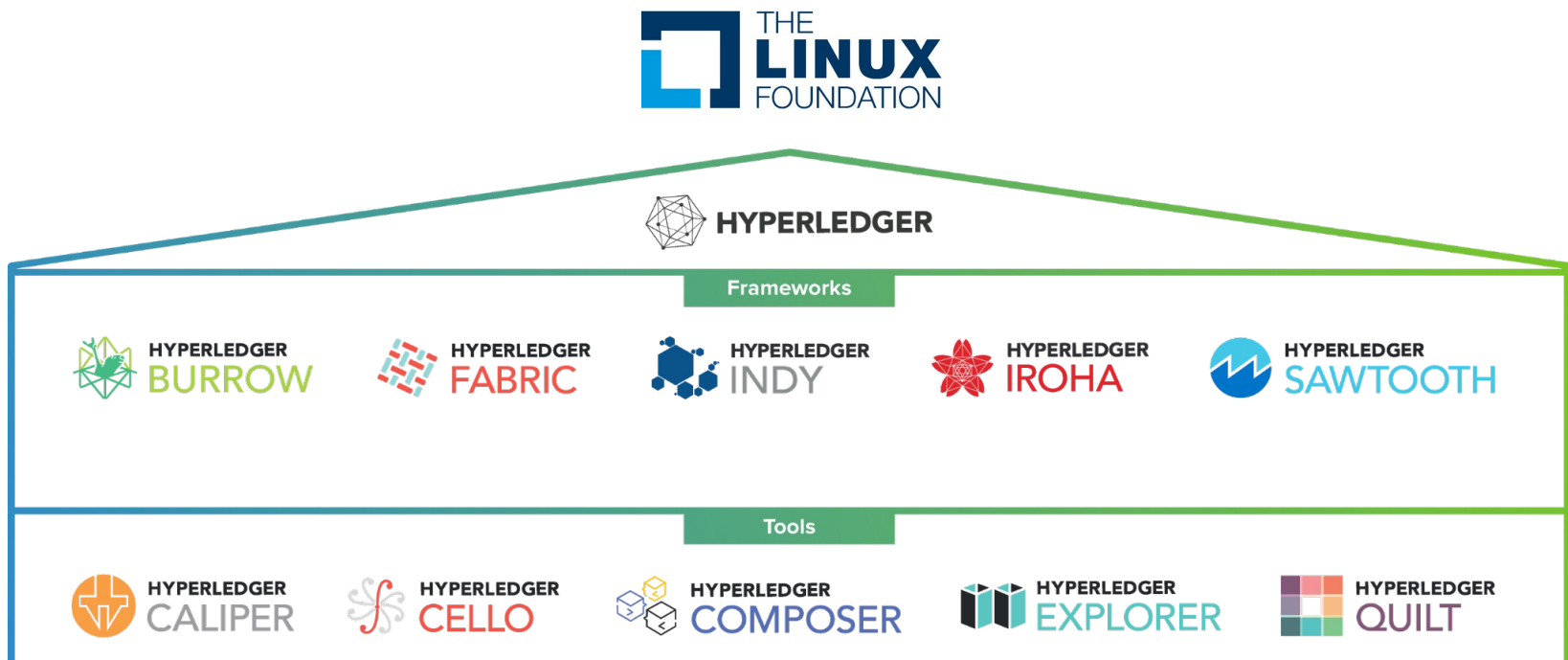
Blockchain, Criptomoedas & Tecnologias Descentralizadas

Introdução ao Hyperledger Fabric **Conceitos Básicos**


Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Pedro H. Barcha Correia – pedro.correia@usp.br
Escola Politécnica, Universidade de São Paulo

Hyperledger

- Projeto da Linux Foundation, iniciado em 2015
- Contribuições: IBM, Intel e outras
- Frameworks e ferramentas com código aberto



Hyperledger Fabric

- Software Livre 
 - Pode ser executado, copiado, modificado e redistribuído pelos usuários
 - Código aberto
 - Licença Apache 2.0
- Framework para construção de **blockchains permissionadas**
 - Os participantes recebem permissão para participar da rede, apesar de não confiarem uns nos outros necessariamente
 - Redes não-públicas: **privadas** e **consorciadas**. Ideais para cenários corporativos e organizacionais

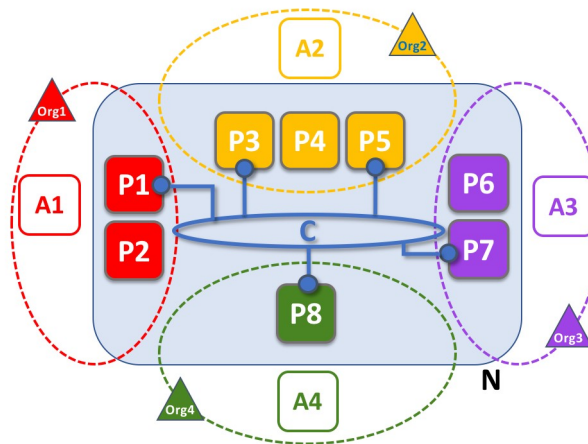
Fabric: redes customizáveis

- Regras de rede (e.g. papéis, políticas)
- Contratos inteligentes
 - Chaincodes
 - **Go**, Node.js e Java
- Mecanismos de consenso
 - Padrão: Raft (CFT)
 - Próprios (inclusive BFTs)

	Tolerância	Custo	Cenário (exemplo)
Crash Fault Tolerance (CFT)	Falhas	Baixo	Rede privada empresarial
Byzantine Fault Tolerance (BFT)	Falhas e nós maliciosos	Alto	Redes públicas

Estrutura da blockchain

- Organizações
 - Redes que podem ser independentes
 - Contêm os nós e podem possuir uma aplicação própria
- Canais
 - Canais de comunicação entre nós de distintas organizações
 - Garantem a privacidade dos dados
 - Nós podem participar de vários canais



	Blockchain Network		Ledger
	Channel		Application
	Peer		Principal PA (e.g. A1, P5) communicates via channel C.
			Organization
		Organization R owns application A1 and peers P1, P2.	

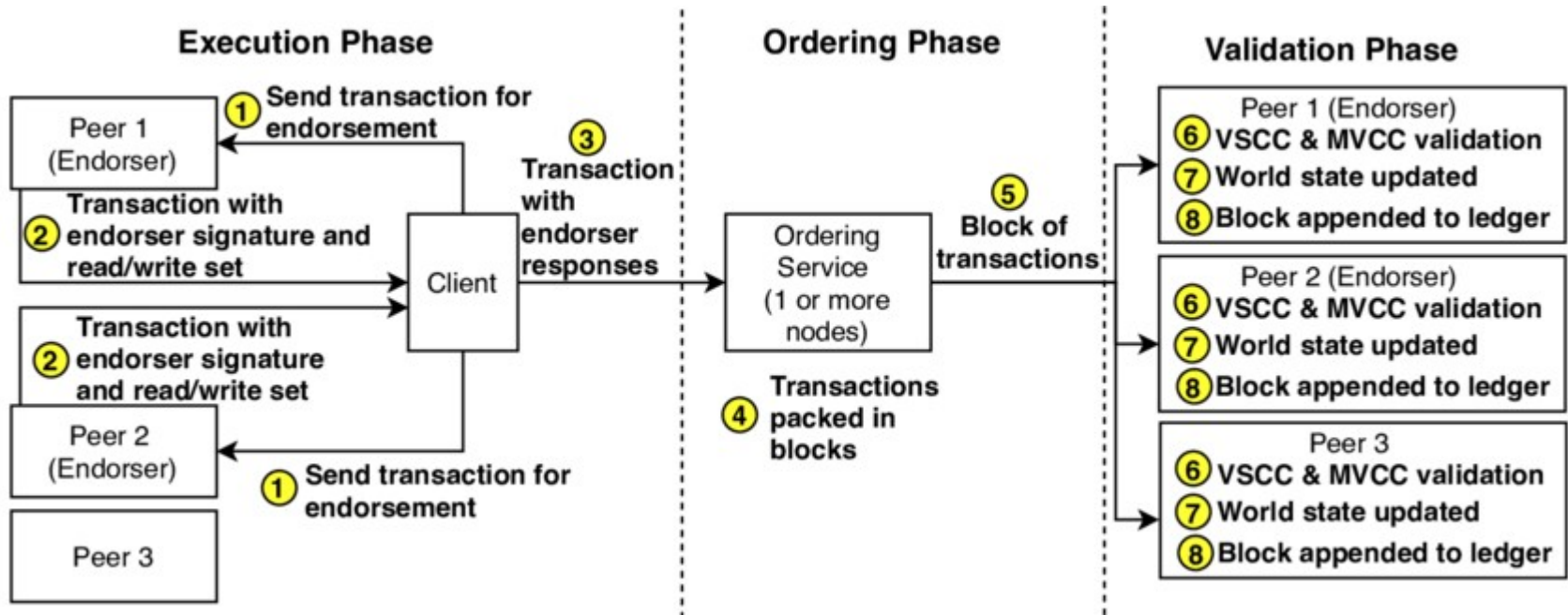
Organização da rede

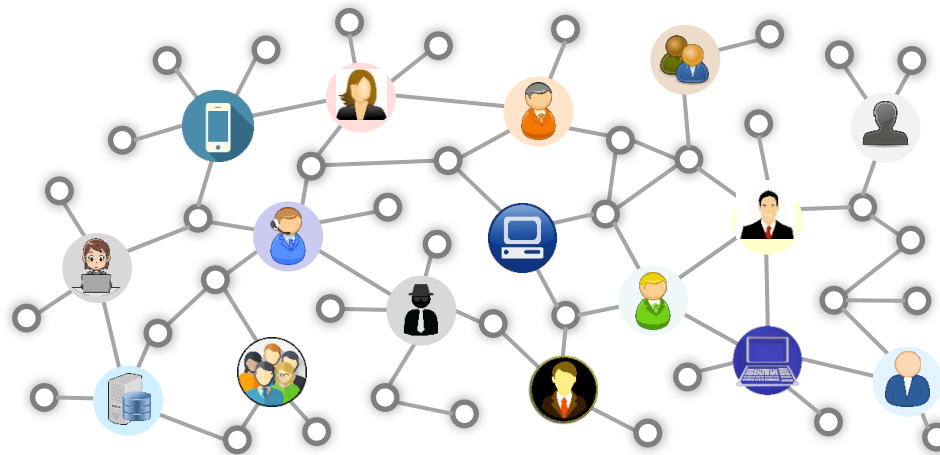
- Principais tipos de de nós:
 - **Cliente**
 - Atua em nome do usuário final
 - **Peer** (nó validador)
 - Hospeda a ledger, executa os contratos inteligentes e valida as transações
 - Pode ou não ser de **endosso (endorsing peer)**, o qual **simula a transação** em cima do seu ledger atual, gerando o **read/write set** (i.e. o que deve ser mudado)
 - **Ordenador (ordering):**
 - **Verifica as políticas** das transações recebidas (e.g. se todos os nós de endosso devem assinar, isso aconteceu?)
 - **Verifica** se os **read/write sets** recebidos dos nós de endosso batem
 - **Ordena as transações** recebidas utilizando o mecanismo de consenso
 - Gera e distribui blocos

Autoridade certificadora (certificate authority, CA)

- Permite a identificação de usuários, nós e organizações
- Todos os nós validam as assinaturas recebidas, realizam suas tarefas e assinam o resultado antes de passá-lo adiante

Fluxo das transações





Blockchain, Criptomoedas & Tecnologias Descentralizadas

Introdução ao Hyperledger Fabric **Conceitos Básicos**

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br

Pedro H. Barcha Correia - pedro.correia@usp.br

Escola Politécnica, Universidade de São Paulo

Referências

- Documentação do Hyperledger Fabric (2020). Introdução. URL: <https://hyperledger-fabric.readthedocs.io/pt/release-2.2/whatis.html>
- Documentação do Hyperledger Fabric (2020). Pares. URL: <https://hyperledger-fabric.readthedocs.io/pt/latest/peers/peers.html>
- Documentação do Hyperledger Fabric (2022). Fluxo de Transação. URL: <https://hyperledger-fabric.readthedocs.io/pt/release-2.2/txflow.html>
- Visualização do Raft. The secret lives of data. <https://thesecretlivesofdata.com/raft/>
- In Search of an Understandable Consensus Algorithm. Paper original do Raft. <https://raft.github.io/raft.pdf>