INSTITUTO DE INFORMÁTICA
Universidade Federal de Goiás

Blockchain

Matheus Martins, Tauan Coutinho

INSTITUTO DE INFORMÁTICA
UFG

UFG
UNIVERSIDADE FEDERAL DE GOIÁS

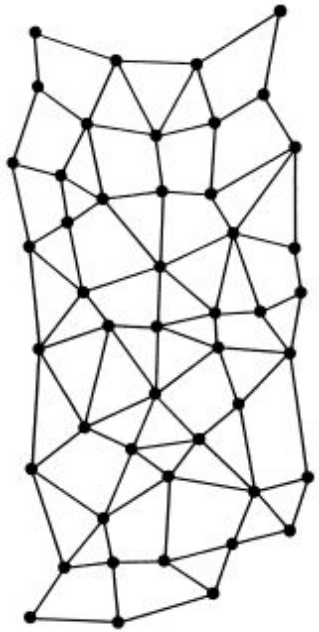
Agenda

- Blockchain
  - Definição
  - Resumos criptográficos
  - Assinaturas digitais
  - Algoritmos de consenso
- Blockchain: pública x privada
  - Ethereum
  - Hyperledger Fabric
- Aplicação
- Considerações finais

O que é Blockchain?

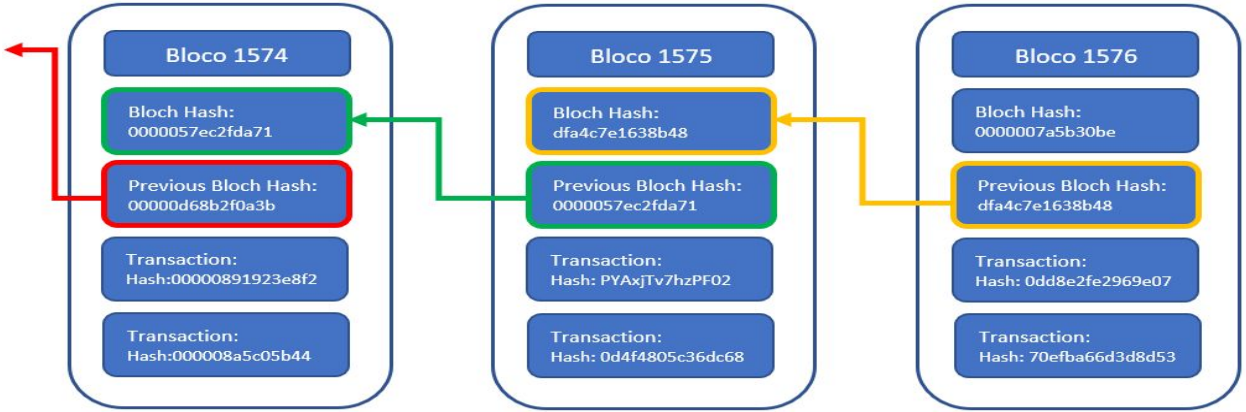
Definição

- Blockchain é uma cadeia de blocos, que faz parte de um sistema de registro coletivo
- Banco de dados Distribuído e descentralizado



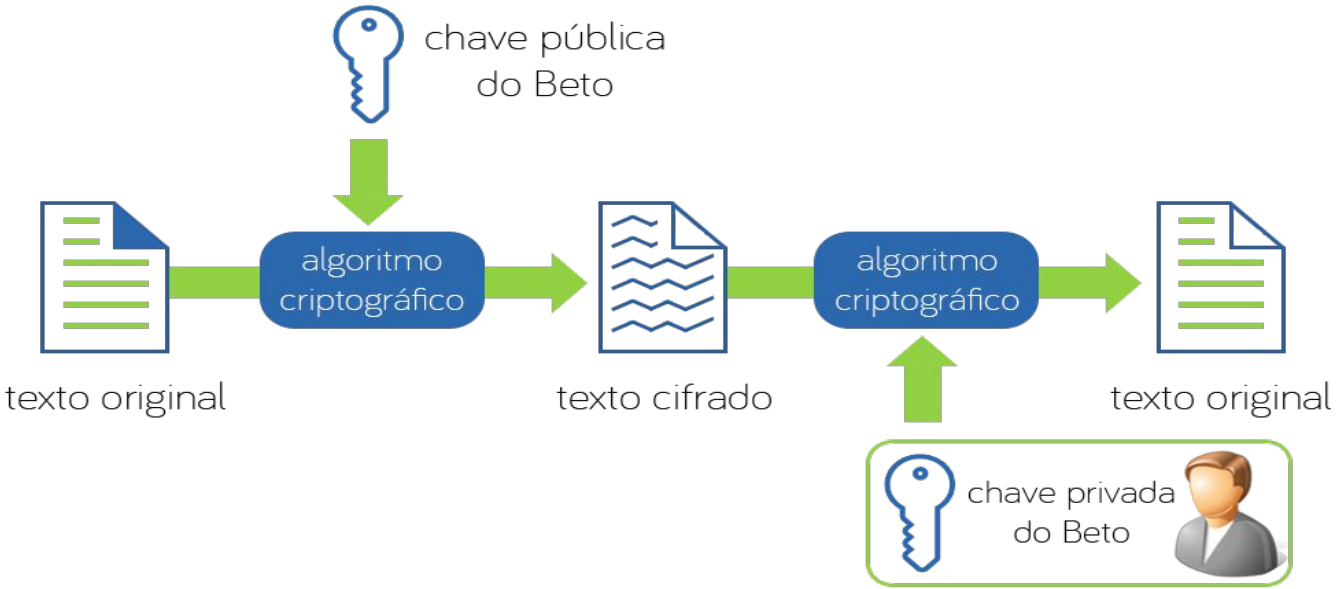
Resumos criptográficos

- ❏ Resistência à colisão
- ❏ Ocultação



Assinaturas digitais

- Chave pública e privada
- Certificados digitais
  - IPC: Infraestrutura de Chave Pública



Algoritmos de consenso

- Algoritmos de consenso são um processo de tomada de decisão para um grupo.
- PoW - Proof-of-Work
- PoS - Proof-of-Stake

Blockchain: Pública x Privada

Blockchain Pública

- Qualquer entidade pode integrar a rede, mantendo a anonimidade em sua participação
- Única propriedade passível de confiança é a imutabilidade do estado da Blockchain
- Utilizam um incentivo econômico para lidar com a falta de confiança e o custo de participação
- Promove transações transparentes
- Bitcoin, Ethereum

Blockchain Privada

- Participação na rede sujeita a um convite
- Todos os participantes são conhecidos, identificados e frequentemente controlados
- Operam sobre um certo modelo de governança
- Risco de ações maliciosas é reduzido neste tipo de blockchain
- Ideal para interesses privados e corporativos
- Hyperledger Fabric

Contratos inteligentes

- *“Um protocolo de transação informatizado que executa os termos de um contrato” - Nick Szabo*
- Representa a lógica de negócio da aplicação que utiliza blockchain
- Funciona como uma aplicação distribuída confiável
- Recebe sua confiabilidade e segurança da blockchain e do consenso entre os pares
- Operam sobre uma determinada arquitetura (order-execute)
- Necessário lidar com o determinismo das operações

Ethereum

- Implementação de blockchain pública
- Plataforma de desenvolvimento de aplicações descentralizadas
- Contratos inteligentes são denominados “Dapps”
- Possui sua moeda digital: Ether
- Ações que demandam poder computacional na plataforma são recompensadas em Ether

Hyperledger Fabric

- Implementação de blockchain privado
- Plataforma de desenvolvimento de aplicações descentralizadas
- Contratos inteligentes são denominados “chaincode”
- Primeira plataforma do gênero a suportar linguagens de propósito geral (Java, Go, Node.js)
- Possui arquitetura altamente modular e configurável
- Não utiliza criptomoeda

Aplicação

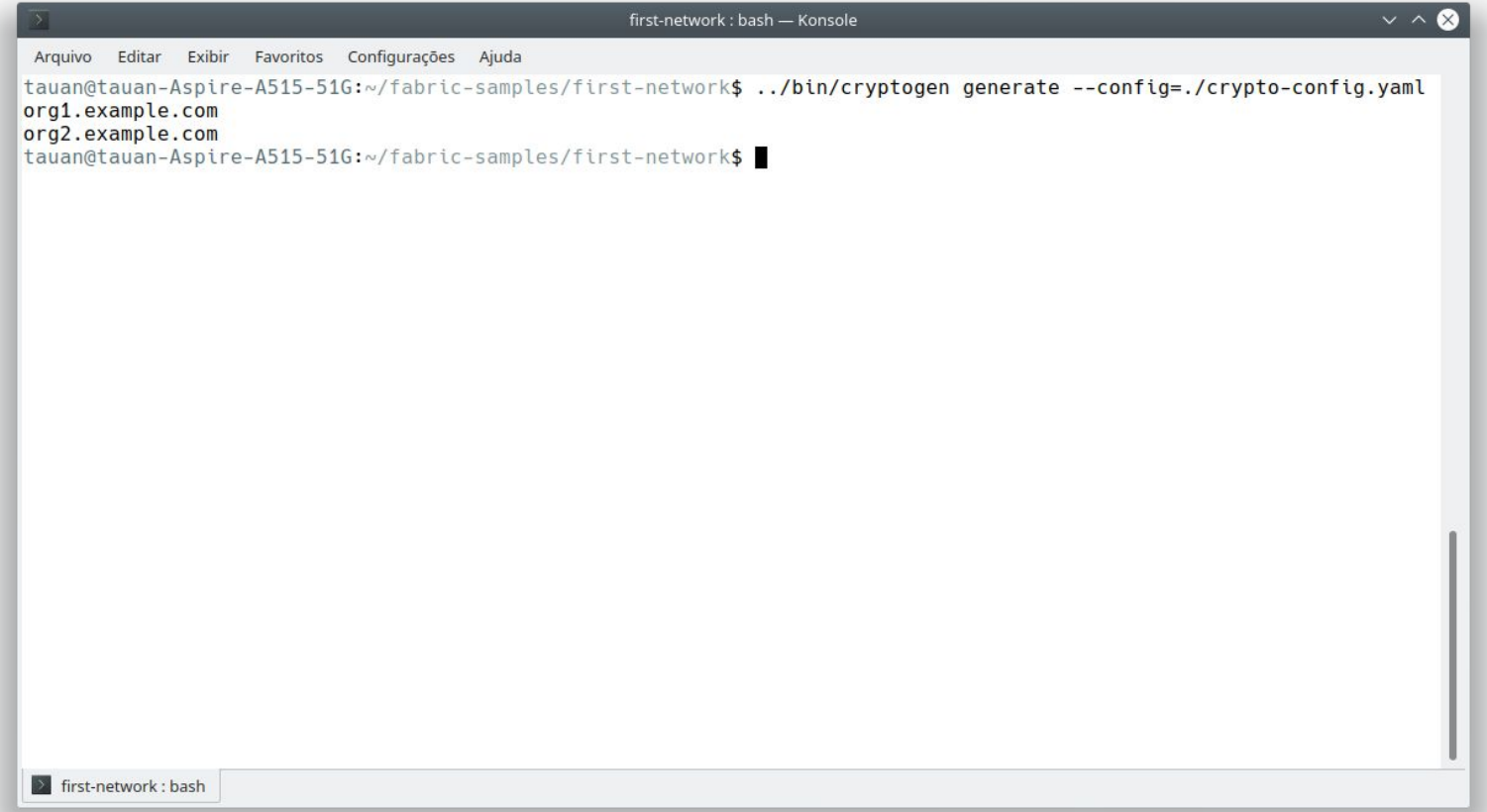
Hyperledger Fabric Network

- Construção de uma rede utilizando Hyperledger Fabric
- Rede formada por duas organizações, as quais possuem dois pares cada.
- Formação do canal através da instalação do chaincode
- Operações básicas entre os pares

1º passo: Material criptográfico

- Geração de material criptográfico para as entidades da rede
- Possibilita a autenticação para a comunicação e a realização de transações entre as entidades
- Certificados relacionados entre as organizações e seus respectivos pares

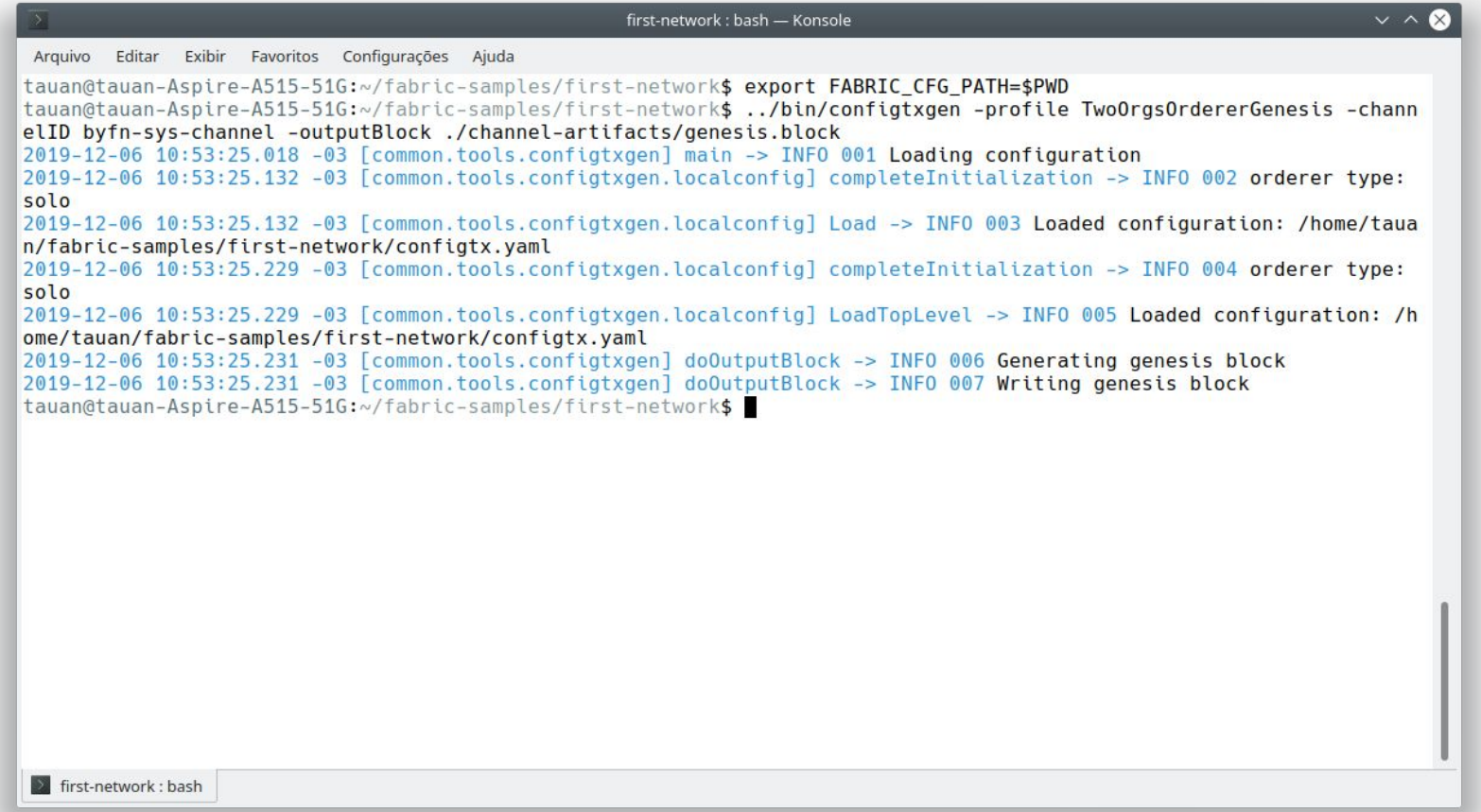
1º passo: Material criptográfico



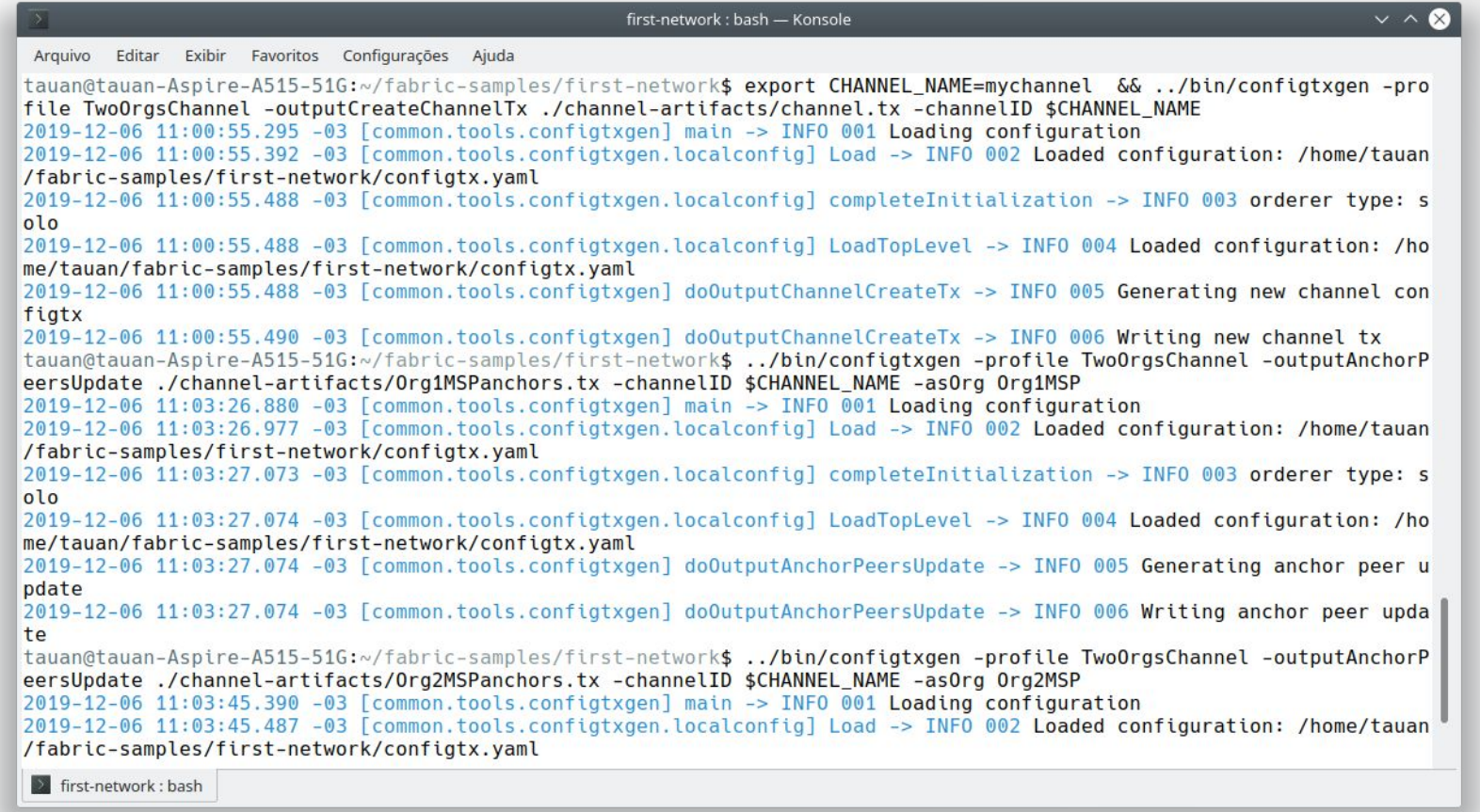
2º passo: Configuração de transações

- Geração de arquivos de configuração para transações
- Arquivos gerados:
  - Genesis Block
  - configuration transaction
  - Anchor peer transactions

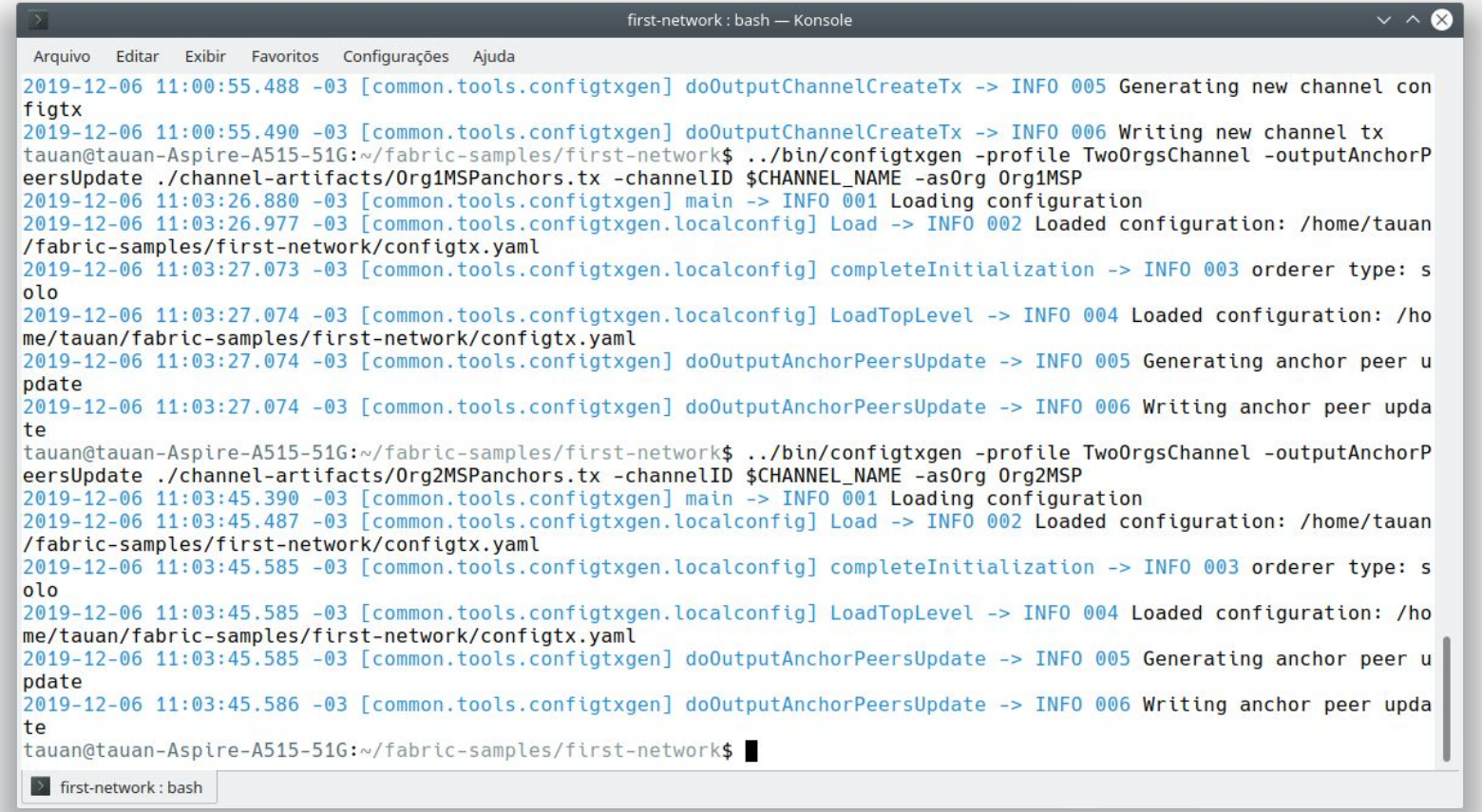
2º passo: Configuração de transações



2º passo: Configuração de transações



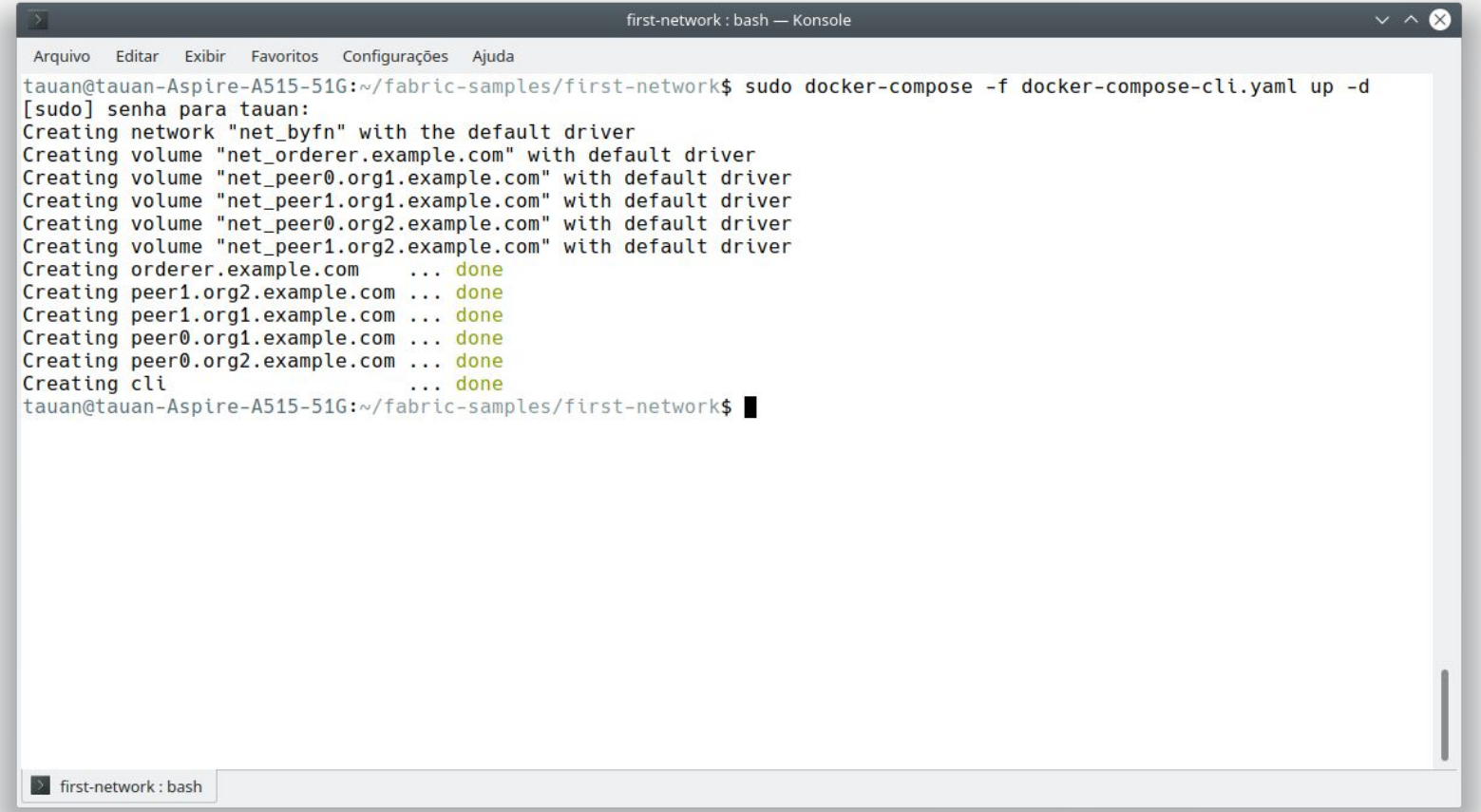
2º passo: Configuração de transações



3º passo: Iniciar a rede

- Utilizaremos o Docker-compose para iniciar as imagens previamente estabelecidas para iniciar a rede
- Operações serão iniciadas a partir do bloco genesis criado

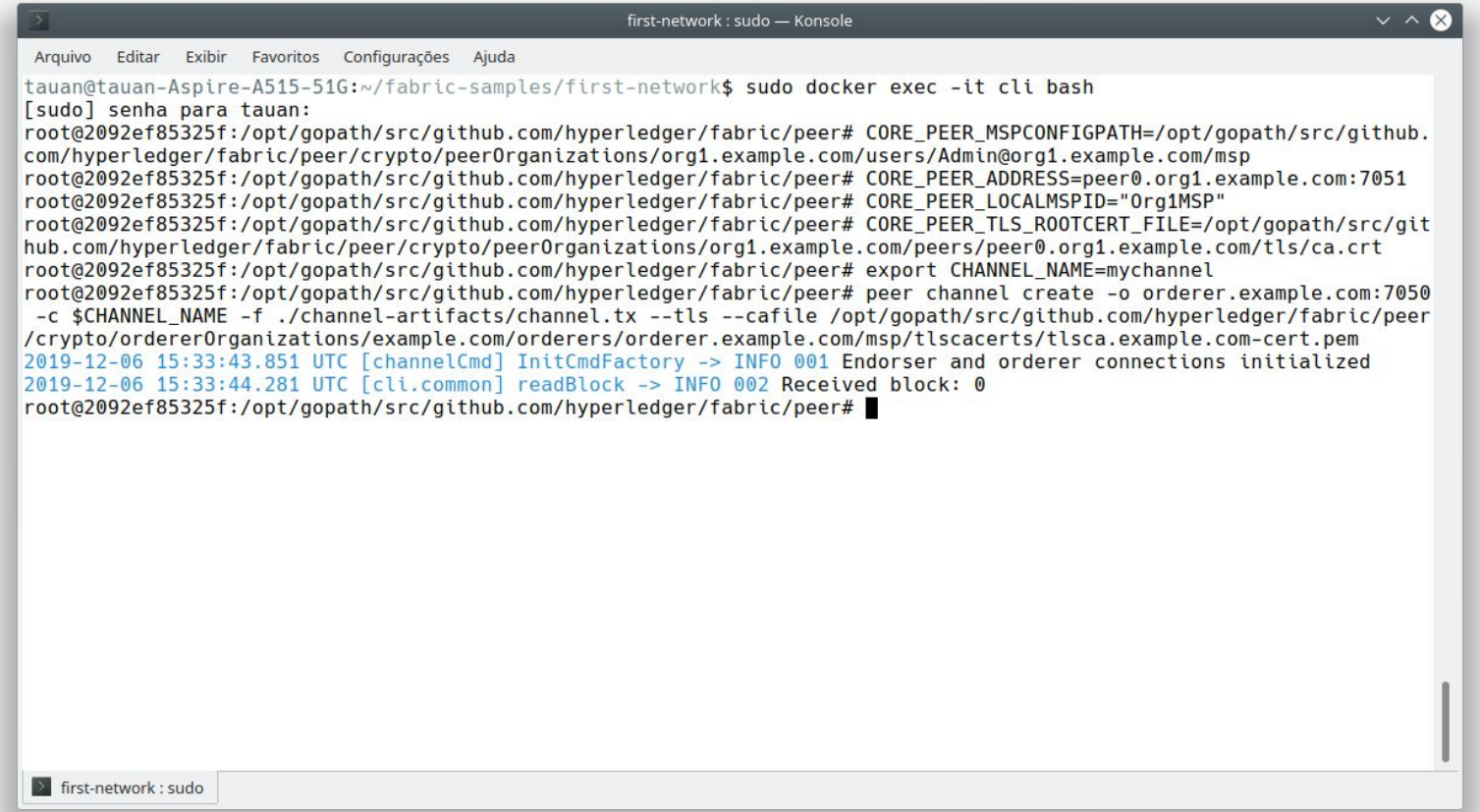
3º passo: Iniciar a rede



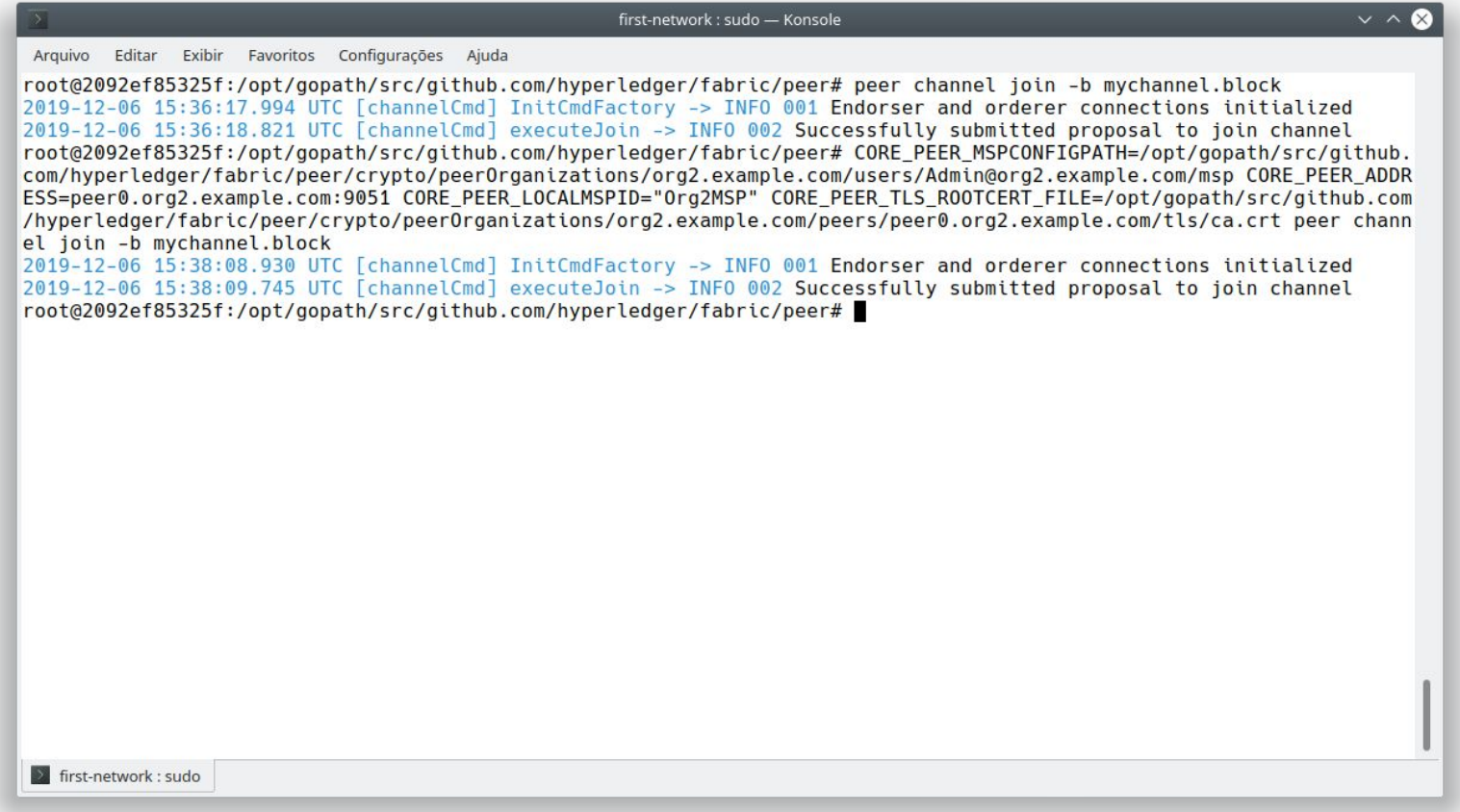
4º passo: Criando o canal

- Nesta etapa iremos utilizar os arquivos de configuração de transação de canal para estabelecer a criação do canal e a inclusão dos pares componentes de cada organização no canal

4º passo: Criando o canal



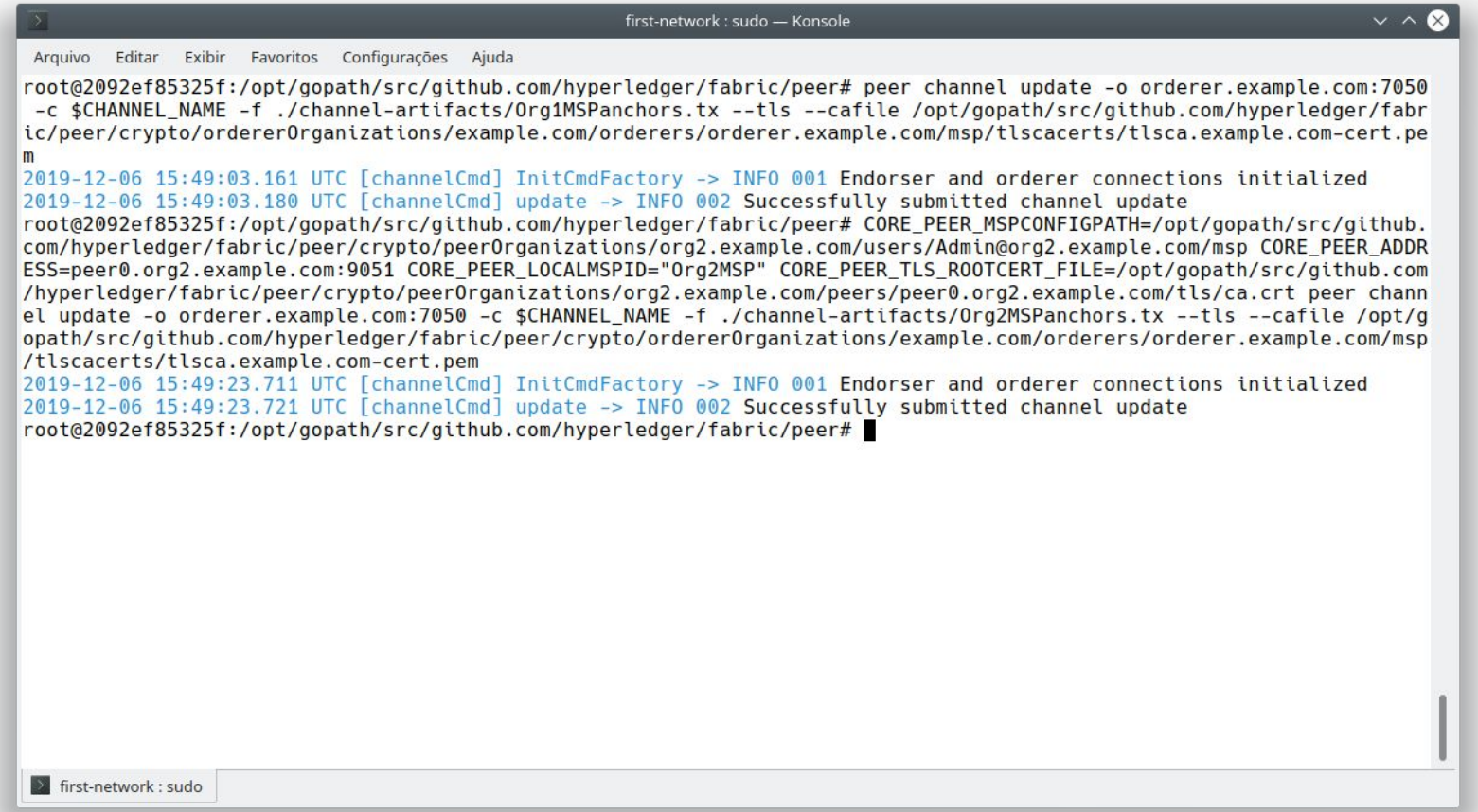
4º passo: Criando o canal



5º passo: Definindo pares âncoras

- Nesta etapa iremos atualizar o canal para definir os pares âncoras de cada organização
- Estes pares serão peer0 de ambas as organizações (Org1 e Org2)

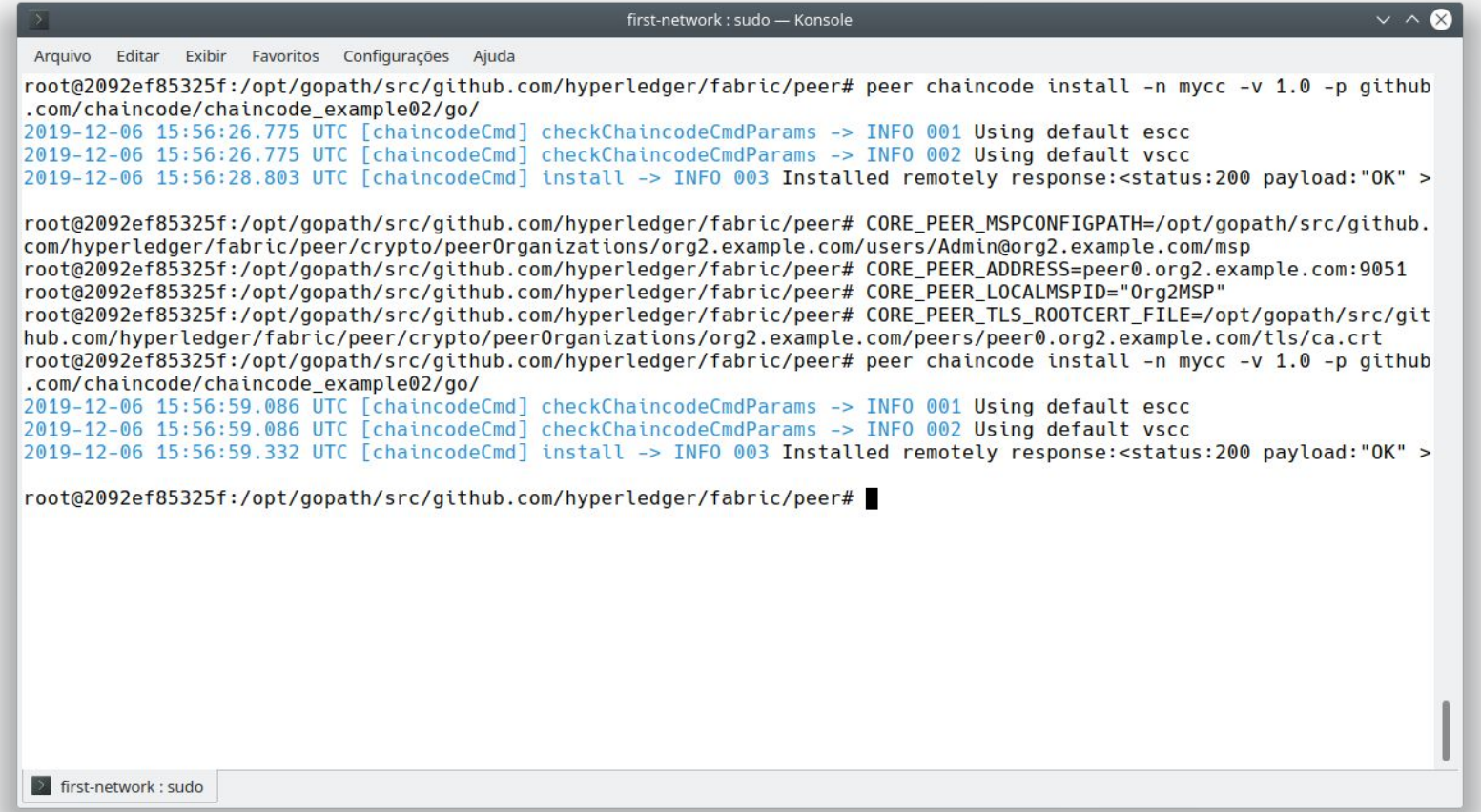
5º passo: Definindo pares âncoras



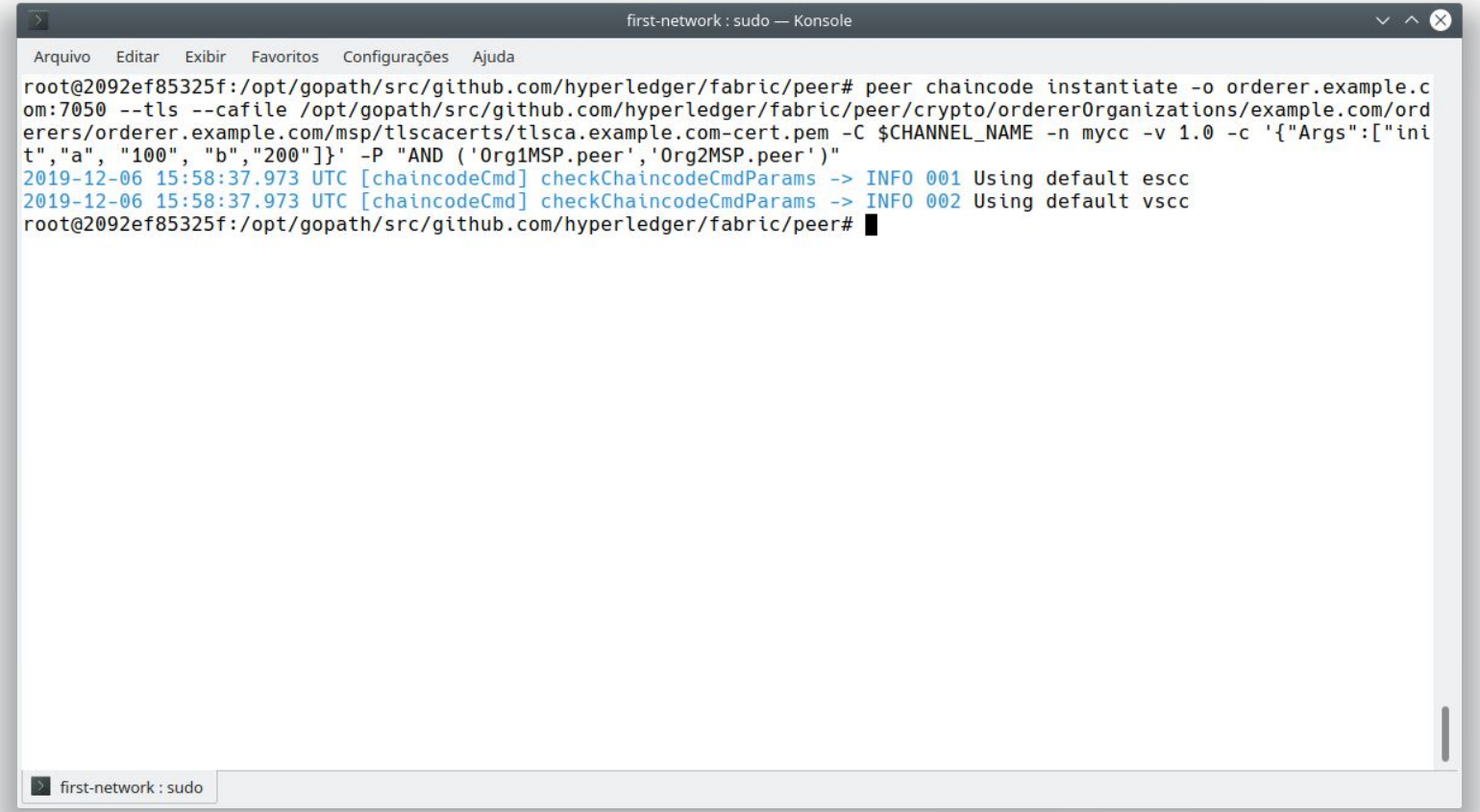
6º passo: Instalação do chaincode

- Iremos utilizar um chaincode já existente
- O processo de instalação é realizado primeiro nos pares, então o chaincode é instanciado no canal

6º passo: Instalação do chaincode



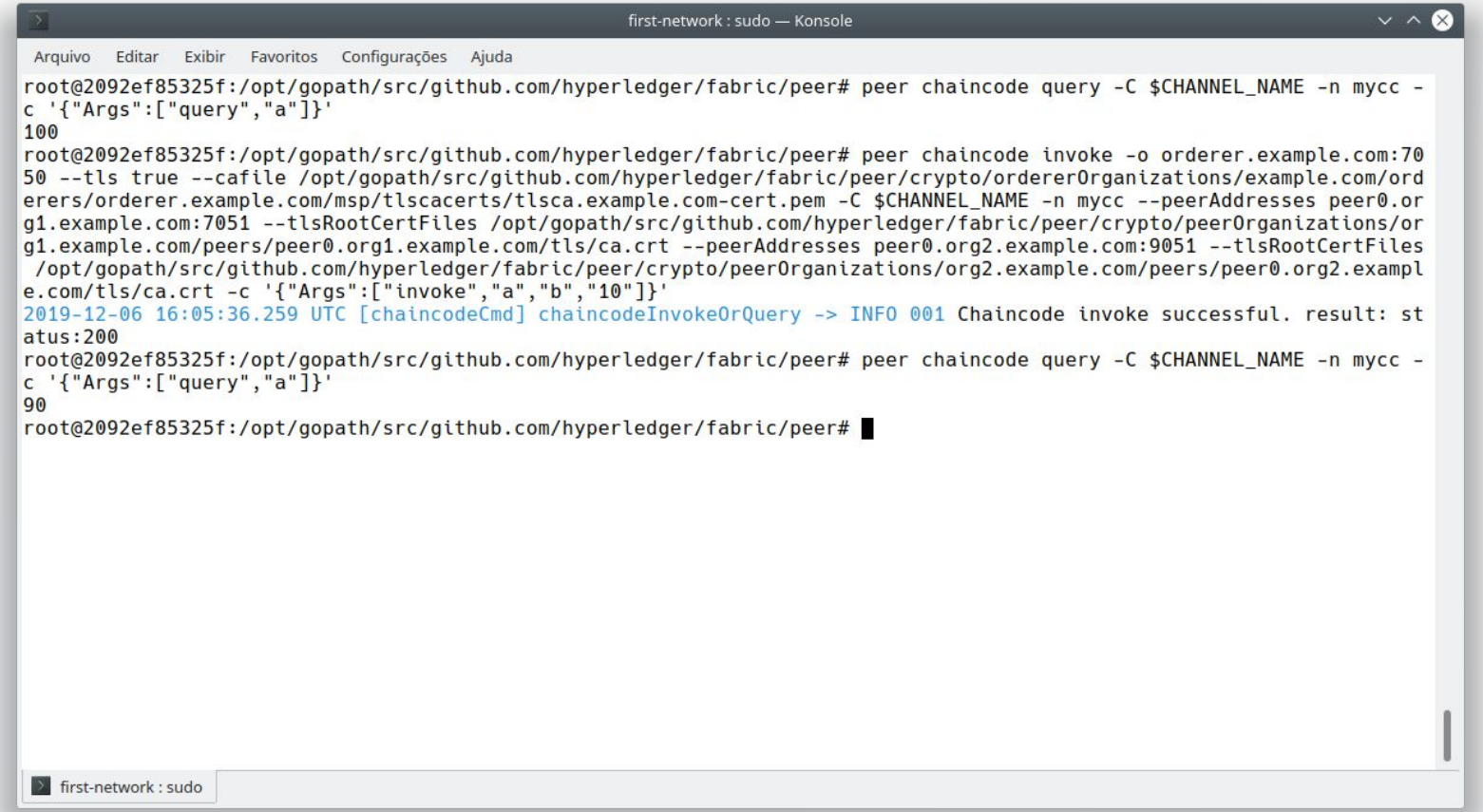
6º passo: Instalação do chaincode



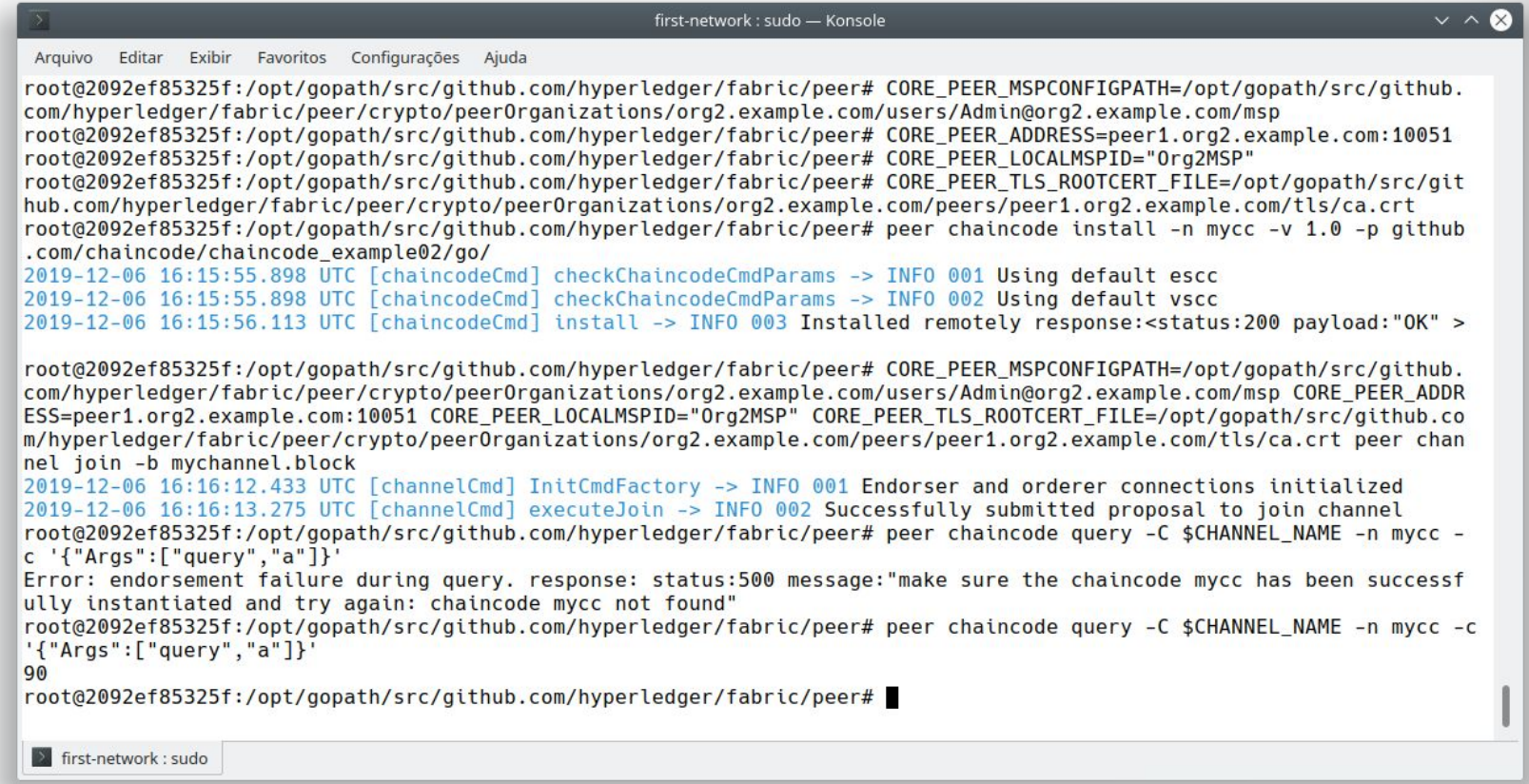
Operações no canal

- Iremos demonstrar algumas operações no canal para verificar a corretude de estabelecimento do mesmo
- Consultas e transferências baseadas no valores ‘a’ e ‘b’ instanciados pelo chaincode no canal

Consultas e transferência



Instalação do chaincode em um novo par



Considerações finais

- Esta aplicação mostra o funcionamento básico do hyperledger fabric, relacionando seus artefatos e softwares adicionais (docker)
- Hyperledger fabric possui ferramentas para serviços de ordenação (Raft, Kafka) e persistência de dados (CouchDB)
- Esta plataforma de desenvolvimento possibilita uma diversidade de aplicações com os benefícios do blockchain e a praticidade proposta no estabelecimento da rede.

Obrigado!