Aula 004 - Descentralização

No contexto de Blockchain

Prof. Rogério Aparecido Gonçalves[1]

[1] *Universidade Tecnológica Federal do Paraná (UTFPR)*

Departamento de Computação (DACOM)

rogerioag@utfpr.edu.br

25 de agosto de 2022

Resumo

Descentralização não é um conceito novo. Tem sido usado como estratégia de gerenciamento ao longo do tempo. A ideia básica é distribuir o controle e a autoridade para as periferias de uma organização ao invés de se ter um controle central total. No contexto de blockchain, uma das bases fundamentais é que não há uma única autoridade central que está no controle da rede.

Sumário

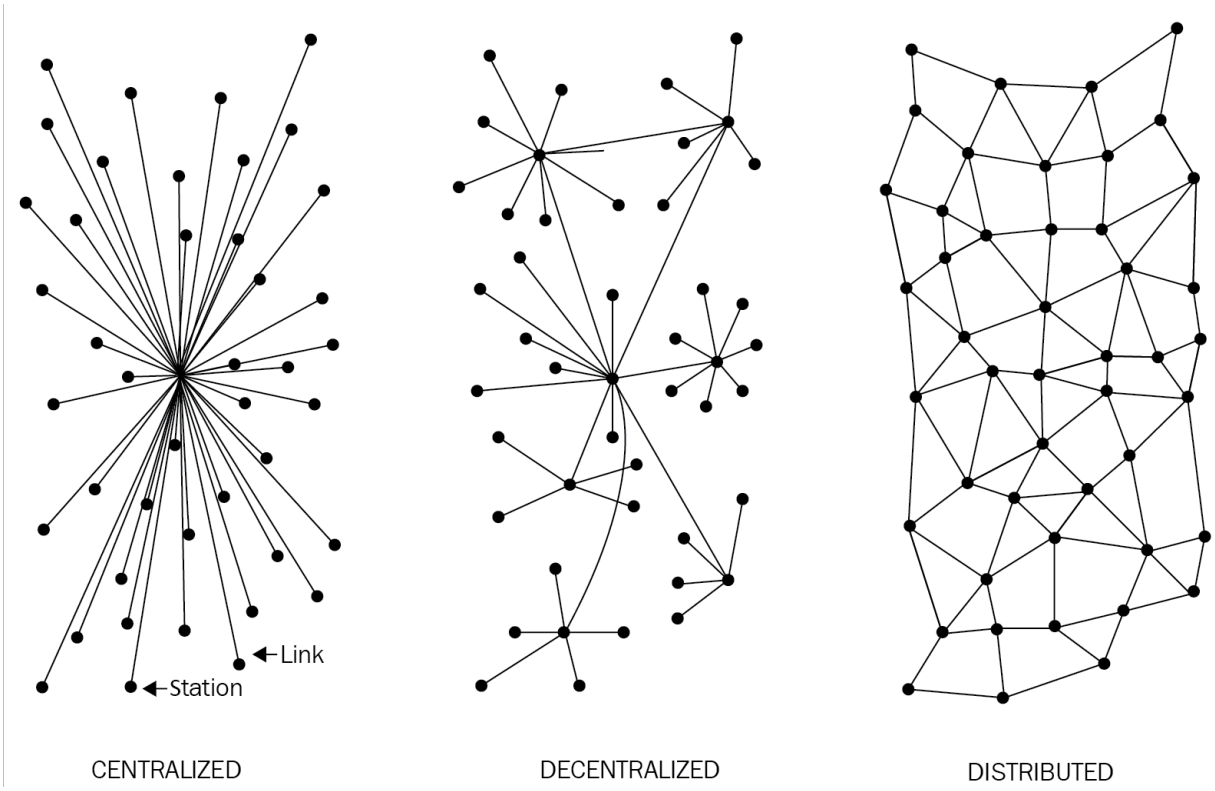
1 Introdução

1.1 Objetivos

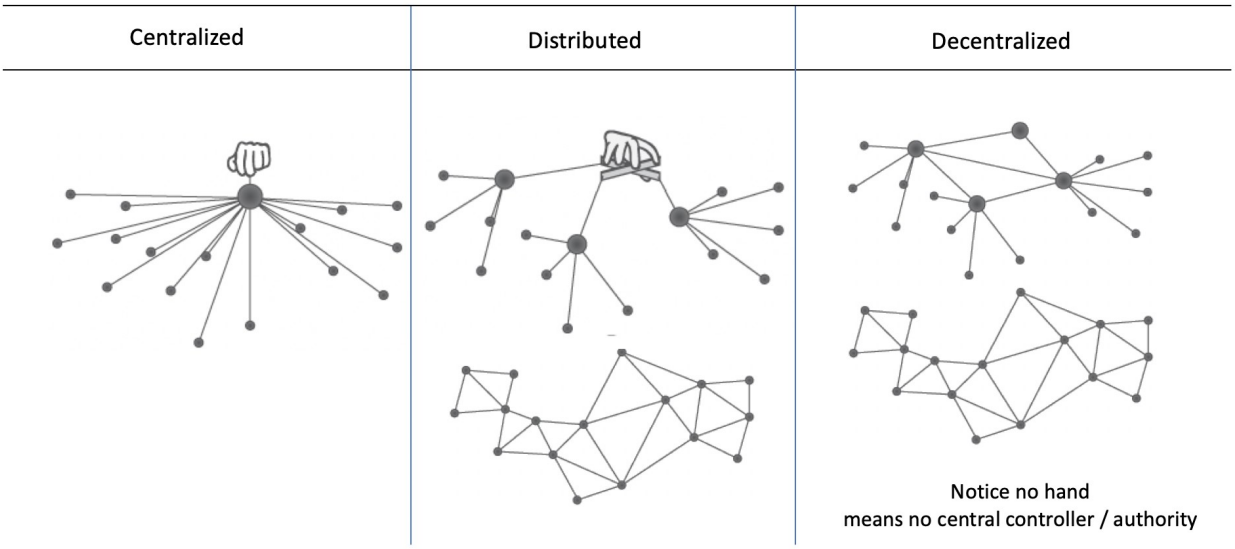
- Definição do conceito de Descentralização no contexto de *Blockchain*.
- Aplicações Descentralizadas (DApps).

2 Descentralização

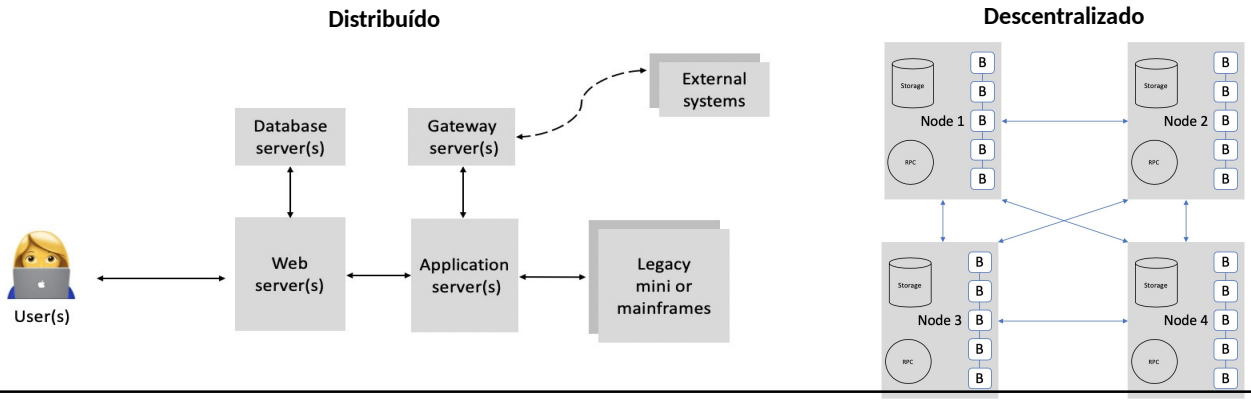
2.1 Definição de Descentralização



- **Sistemas Centralizados:** São os convencionais sistemas Cliente-Servidor.
- **Sistemas Distribuídos:** Sistemas com dados e computação espalhados/distribuídos por múltiplos nós de uma rede. Mas ainda com uma autoridade central. Orquestração de serviços, por exemplo. Banco de dados em um nó, e serviços de aplicações em outros nós.
- **Sistemas Descentralizados:** São sistemas onde os nós não são dependentes de um nó principal *(master)*, o controle é distribuído entre os diversos nós. A inovação que tem surgido no paradigma descentralizado com aplicações descentralizadas é o **consenso descentralizado**, o que possibilita aos usuários concordarem com alguma coisa via algoritmos de consenso sem a necessidade de uma terceira parte central, confiável, intermediária provedora de serviço.



2.2 Diferenças entre distribuído e descentralizados



Característica	Centralizado	Descentralizado
Propriedade	Provedor de Serviços	Todos os usuários
Arquitetura	Cliente/Servidor	Distribuída, diferentes topologias
Segurança	Básica	Mais seguro
Alta Disponibilidade	Não	Sim
Tolerância a falhas	Básica, único ponto de falha	Altamente tolerante, serviço é replicado
Resistência a Conluios	Básica, está sobre o controle de um grupo ou de um único indivíduo	Alta, algoritmos de consenso garantem a defesa contra adversários
Arquitetura da Aplicação	Aplicação Única	Aplicação replicada em todos os nós da rede
Confiança	Consumidores tem que confiar no provedor do serviço	Confiança mútua não é necessária
Custo para o consumidor	Alto	Baixo

2.3 Métodos de Descentralização

- Dois métodos podem ser utilizados para a descentralização:
  - **Desintermediação:** Sistema Financeiro x Bitcoin.
  - **Competição:** Sistema que cada contrato inteligente possa escolher um provedor de dados entre vários, baseado na reputação, *score*, *reviews* e qualidade do serviço.

- Entre os benefícios da descentralização estão: *transparência, eficiência, econonia de custos, desenvolvimento de ecossistemas confiáveis e em alguns casos privacidade e anonimato.*
- Desafios: *segurança, bugs, erros humanos.*

Exemplo

Por exemplo, em um sistema descentralizado como Bitcoin ou Ethereum, onde a segurança é normalmente fornecida por chaves privadas, como podemos garantir que um ativo ou token associado a essas chaves privadas não possa ser inutilizado devido a negligência ou bugs no código? E se as chaves privadas forem perdidas devido à negligência do usuário? E se, devido a um bug no código do contrato inteligente, o aplicativo descentralizado se tornar vulnerável a ataques?

2.4 É necessário utilizar um Blockchain?

Questão	Sim/Não	Solução Recomendada
É necessário altas taxas de transferência de dados?	Sim	Use um banco de dados tradicional
	Não	Uma base de dados central pode ainda ser útil se outros requisitos forem atendidos. Por exemplo, se os usuários confiam um nos outros, então talvez não haja necessidade de um blockchain. Entretanto, se eles não confiam ou a confiança não possa ser estabelecida por alguma razão, blockchain pode ser útil.
Atualizações são controladas centralmente?	Sim	Use uma base de dados tradicional
	Não	Pode ser investigado como uma blockchain pública ou privada pode ajudar.
Usuários confiam um nos outros?	Sim	Use uma base de dados tradicional.
	Não	Use um Blockchain Público
Usuários são anônimos	Sim	Use um Blockchain Público
	Não	Use um Blockchain Privada
O consenso deve ser mantido dentro de um consórcio?	Sim	Use um Blockchain Privado.
	Não	Use um Blockchain Público
A imutabilidade estrita dos dados é necessária?	Sim	Use um Blockchain
	Não	Use uma base de dados tradicional central

- **Responder a todas essas questões ajuda na decisão sobre a necessidade de usar ou não um *Blockchain*.**

2.5 Como descentralizar?

- O que está sendo descentralizado?
- Que nível de descentralização é necessário?
- Qual Blockchain será usado?
- Que estímulos estão sendo utilizados?

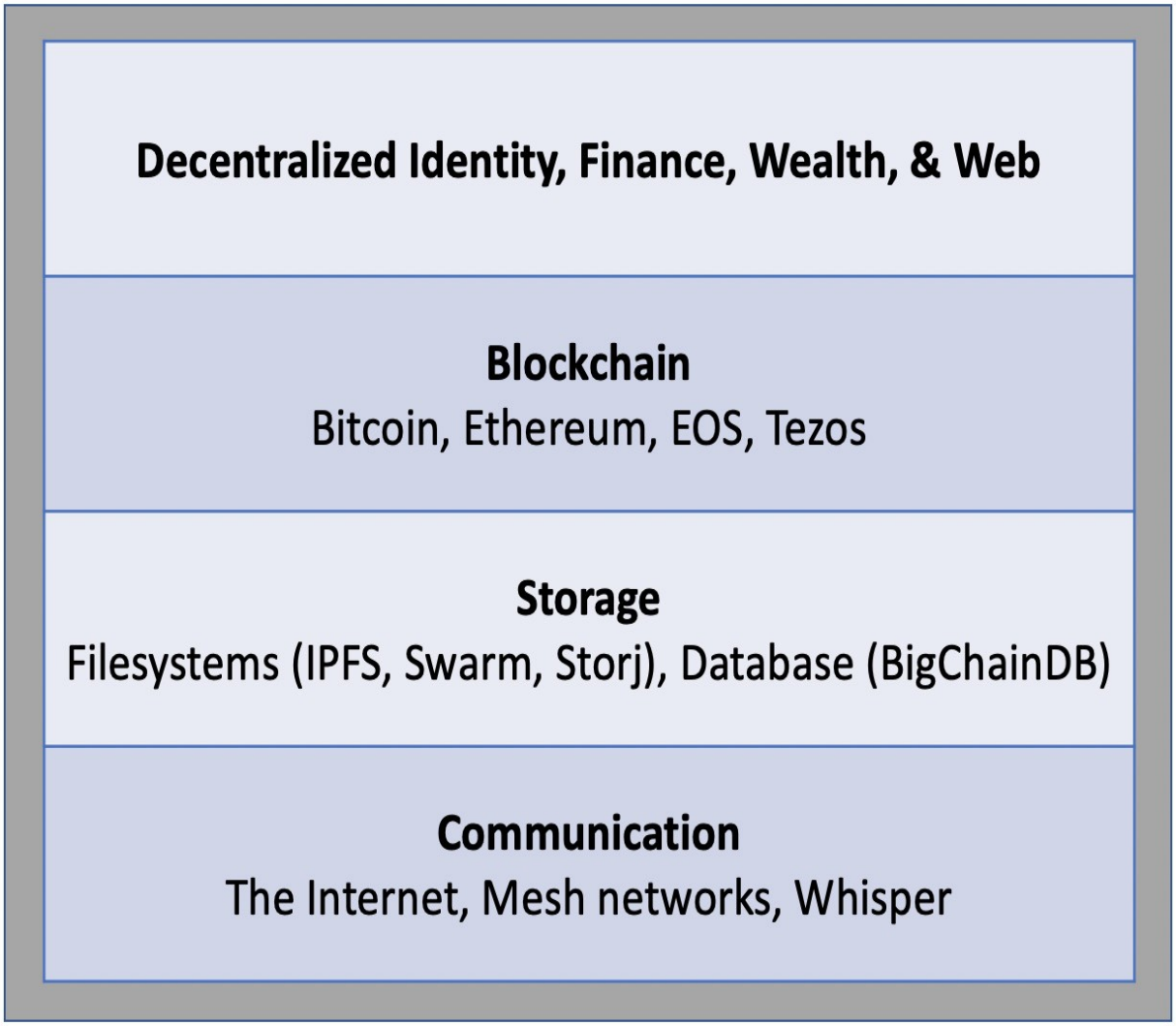
O que está sendo descentralizado?

  - Identificação do sistema que está sendo descentralizado. Podendo ser qualquer sistema, tal como um sistema de identidade ou um sistema de negociação.
- **Que nível de descentralização é necessário?**
  - Qual o nível de descentralização necessário, pode ser uma desintermediação completa ou parcial.
- **Qual Blockchain será usado?**
  - Determinação qual *blockchain* é adequado para uma aplicação particular. Podendo ser um *blockchain* do `Bitcoin`, do `Ethereum`, ou algum outro *blockchain* que é conside-
- **Qual mecanismo de segurança será usado?**
  - Questão fundamental, como a segurança de um sistema descentralizado será garantida. Um exemplo, um mecanismo baseado na atomicidade, onde as transações executam por completo ou não executam, fortalecem a integridade do sistema. Outros mecanismos podem considerar reputação, que permite variar os degraus de confiança em um sistema.

2.6 Blockchain e Ecossistema Completo de Descentralização

Este modelo ilustra como um Ecossistema Completo Descentralizado poderia trabalhar:

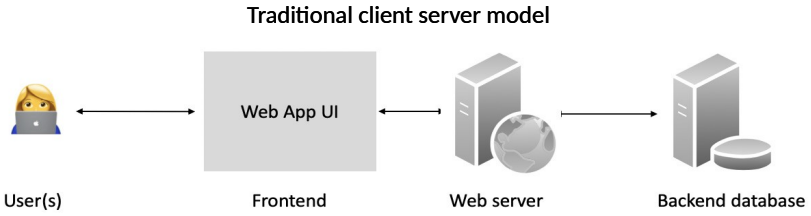
- Comunicação
- Armazenamento
- Poder Computacional
- Identidade e saúde

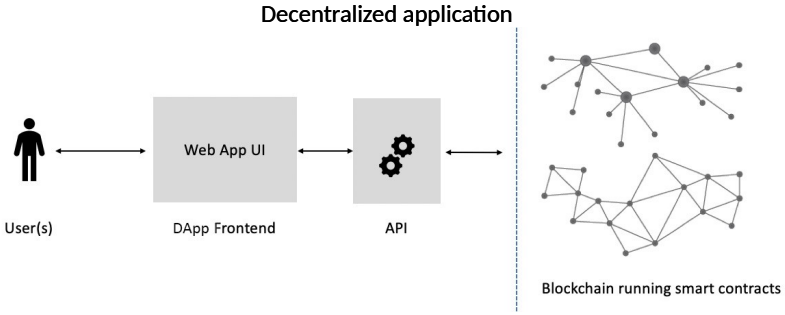


2.7 Aplicações Descentralizadas (DApps)

- Aplicações Descentralizadas (DApps) pode ser categorizadas em:
  - Type 1 (Executa em seu próprio *blockchain* dedicado)
  - Type 2 (Usa um *blockchain* público existente)
  - Type 3 (Usa protocolos das DApps do Type 2)
- Requisitos de uma `DApp`
  - Completamente *Open Source*.
  - Operações devem ser criptograficamente segura.
  - Armazenado em um livro razão público.
  - *Tokens* gerados sob um mecanismo de consenso.

2.8 Design de uma DApp





2.9 DO, DAO, DAC, DAS, DApp

- Propriedades de algumas tipos de entidades descentralizadas.
- Organizações Descentralizadas (DOs), Organizações Autônomas Descentralizadas (DAOs), Corporações Autônomas Descentralizadas (DACs), Sociedades Autônomas Descentralizadas (DASes) e DApps.

Entity	Autonomous?	Software?	Owned?	Capital?	Legal status	Cost
DO	No	No	Yes	Yes	Yes	High
DAO	Yes	Yes	No	Yes	Unsettled	Low
DAC	Yes	Yes	Yes	Yes	Unsettled	Low
DAS	Yes	Yes	No	Possible	Unsettled	Low
DApp	Yes	Yes	Yes	Optional tokens	Unsettled	Use case dependent

2.10 Plataformas para Descentralização

- `Ethereum`
- `MaidSafe`
- `Lisk`
- `EOS`

2.11 Tendências

- Web Descentralizada
  - Web 1: A *World Wide Web* original.
  - Web 2: the era when more service-oriented and web-hosted applications started to emerge
  - Web 3: A visão da internet ou web descentralizada.
- Identidade Descentralizada

- Finanças Descentralidas (DeFi)

2.12 *Word Cloud*

2.13 Leitura Recomendada

Leitura Recomendada

Capítulo 2: Decentralization
Livro: IMRAN BASHIR. Mastering Blockchain : Distributed Ledger Technology, Decentralization, and Smart Contracts Explained, 2nd Edition.

3 Próximas Aulas

3.1 Próximas Aulas: Tecnologia Blockchain

- Criptografia

4 Referências

4.1 Referências

Imran, Bashir. 2018. *Mastering Blockchain : Distributed Ledger Technology, Decentralization,*

and Smart Contracts Explained, 2nd Edition. Packt Publishing. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=1789486&lang=pt-br&site=eds-live&scope=site.