

# Aplicações Descentralizadas Baseadas em Blockchain

Noeli A. Pimentel Vaz

Sistemas Distribuídos - Prof. Sérgio T. de Carvalho  
Instituto de Informática | UFG



# Roteiro

- Contextualização
- Objetivo da Pesquisa
- Fundamentos de Sistemas Distribuídos
- Blockchain
  - Redes
  - Plataformas
- Aplicações Descentralizadas - dApps
  - Decisões para o desenvolvimento de dApps
- Arquiteturas de dApps baseadas em Blockchain
- Considerações Finais



# Contextualização

- Evolução da utilização da Internet com o uso de redes de alta velocidade (5G e pós 5G)
- Necessidade de tecnologias/ ferramentas com menor grau de centralização visando reduzir problemas com violação de dados, censura, pontos únicos de falhas, além de outros
- Tecnologias de ledgers distribuídos (*Distributed Ledger Technology* - DLT) possuem características descentralizadas
- Blockchain tem sido apresentada como uma tecnologia facilitadora para prover a descentralização em aplicações



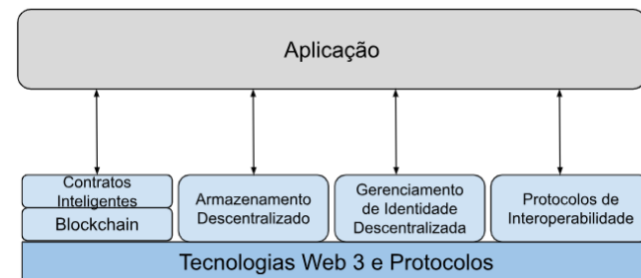
# Contextualização

- **Blockchain resolve um problema central:** muitas organizações desejam compartilhar dados de forma distribuída, mas nenhum proprietário único seria confiável para todos os usuários.
- As tecnologias Blockchain permitem transações diretas de forma segura e transparente, gerando confiança em sistemas que operam com a eficiência de uma rede peer-to-peer.



# Contextualização

- Web descentralizada  $\longleftrightarrow$  Web 3.0
- Nas aplicações a descentralização pode ser proporcionada para todos os blocos de construção (back-end, front-end e armazenamento de dados), ou somente para parte deles.
- Ao eliminar o agente intermediário entre o usuário e a aplicação de fato, as aplicações descentralizadas (Decentralized Application - dApp) utilizam em sua estrutura as tecnologias da Web 3.0.



# Objetivo da Pesquisa

- Compreender as tecnologias que compõem o conhecimento necessário para o desenvolvimento das aplicações descentralizadas baseadas em blockchain.
- Propor uma Arquitetura para dApps baseadas em Blockchain.
- Desenvolver um estudo de caso para aplicação dos conceitos.

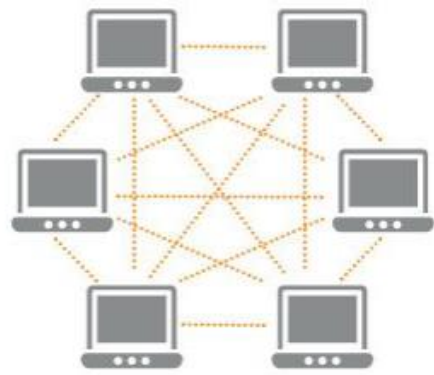


# Fundamentos de Sistemas Distribuídos

- Redes Peer to Peer - P2P
- Coordenação e consenso
- Protocolos de comunicação
- Questões relacionadas a escalabilidade



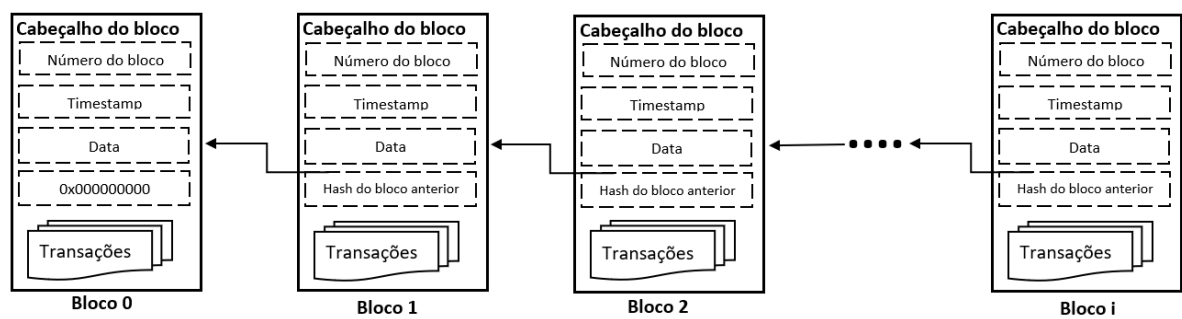
# Blockchain - Principais componentes



Redes P2P



Transações



Blocos



Mecanismo de Consenso





# Redes Blockchain

- O objetivo da blockchain é a realização de transações de forma segura, aberta e imutável
- A operação dos componentes demanda uma infraestrutura de suporte, que pode variar dependendo da sua implementação
- Uma rede blockchain requer uma rede distribuída de nós com poder computacional suficiente para processar e validar as transações



# Redes Blockchain

- Greve et al. (2018) destacam que o consenso da blockchain é fortemente voltado ao tipo de rede a que se destina.
- Redes blockchain podem ser classificadas em:
  - Pública
  - Privada/ Federada
  - Permissionada (*permissioned*)
  - Não permissionada (*permissionless*)



# Redes Blockchain Públicas

- Nós são desconhecidos e é permitida a entrada e a saída aleatórias de nós da rede
- Não há controle dos seus participantes, e a rede pode funcionar em escala mundial
- Exemplos: Bitcoin, Ethereum e Solana
- Podem exigir alguma forma de mecanismo de incentivo aberto e baseados em mineração, com recompensas na forma de criptomoeda
- Os mineradores entram em uma competição com base no poder computacional (e.g., PoW da Bitcoin), poder de posse (e.g., PoS da Ethereum) ou outras capacidades relevantes para a eleição e que não podem ser monopolizados



# Redes Blockchain Privadas

- Os nós da rede são identificados, autorizados e autenticados
- As entradas e saídas de nós estão condicionadas por permissões e, em geral, funcionam em escala menor abrangendo corporações ou organizações em que os participantes possuem papéis bem definidos
- Exemplos são os protocolos PoA (proof of authority) ou Prova de Autoridade, disponíveis no Hyperledger Fabric e Hyperledger Besu



## Redes Blockchain Híbridas / Consorciadas

- O principal diferencial está no mecanismo de consenso, que funcionaria com um conjunto de participantes da rede trabalhando como validadores com algum nível de confiança.
- A vantagem de uso do consenso PoA para a blockchain é que os nós validam as transações mais rapidamente que os consensos PoS ou PoW, porém o consenso PoA é considerado menos descentralizado, pois demanda uma quantidade de nós validadores de confiança (predefinidos ou não).
- Iniciativas como a Rede Blockchain Brasil (RBB) se enquadra nesse tipo de rede.

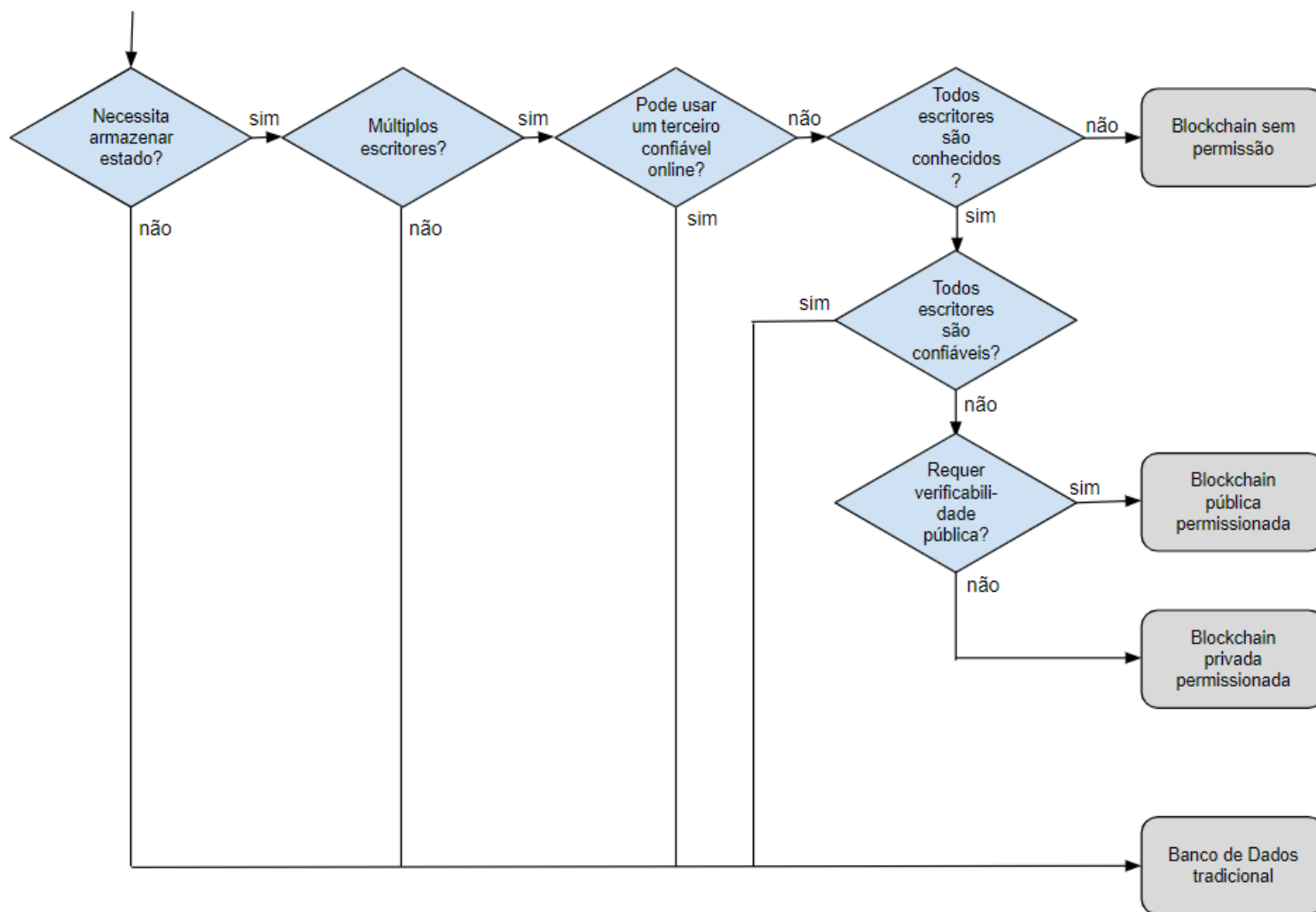


# Redes Blockchain

- A escolha do mecanismo de consenso dependerá dos requisitos, objetivos específicos e decisões do projeto em desenvolvimento.
- Alguns projetos podem preferir **eficiência e velocidade** (PoA), enquanto outros podem optar por **descentralização e segurança** (PoS).
- Nesse sentido, a escolha do tipo de rede blockchain (pública, privada, híbrida/consórcio) segue as mesmas diretrizes.



## Decisões sobre o tipo de rede Blockchain



Fonte: Adaptado de WÜST & GERVAIS, 2018.



# Plataformas de Blockchain

- Os projetos Hyperledger e Ethereum são as principais referências em termos de plataformas blockchain e desenvolvimento de contratos inteligentes.
- Hyperledger se insere no contexto de blockchains privadas e Ethereum no de blockchains públicas.







# Plataforma Blockchain - Hyperledger

- É uma plataforma de código aberto mantida pela Linux Foundation
- A IBM propõe o Fabric, o mais utilizado por organizações que desenvolvem aplicações privadas baseadas em blockchain
- Caracterizada como uma rede permissionada, estabelece uma maior confiança na rede e utiliza o consenso baseado em PoA



# Plataforma Blockchain - Ethereum



- Oferece uma rede pública, sem necessidade de controle de seus participantes
- Caracterizada por uma rede em que não há qualquer confiança entre os nós
- Já utilizou o consenso PoW e, atualmente, usa o consenso PoS



## dApp baseada em Blockchain

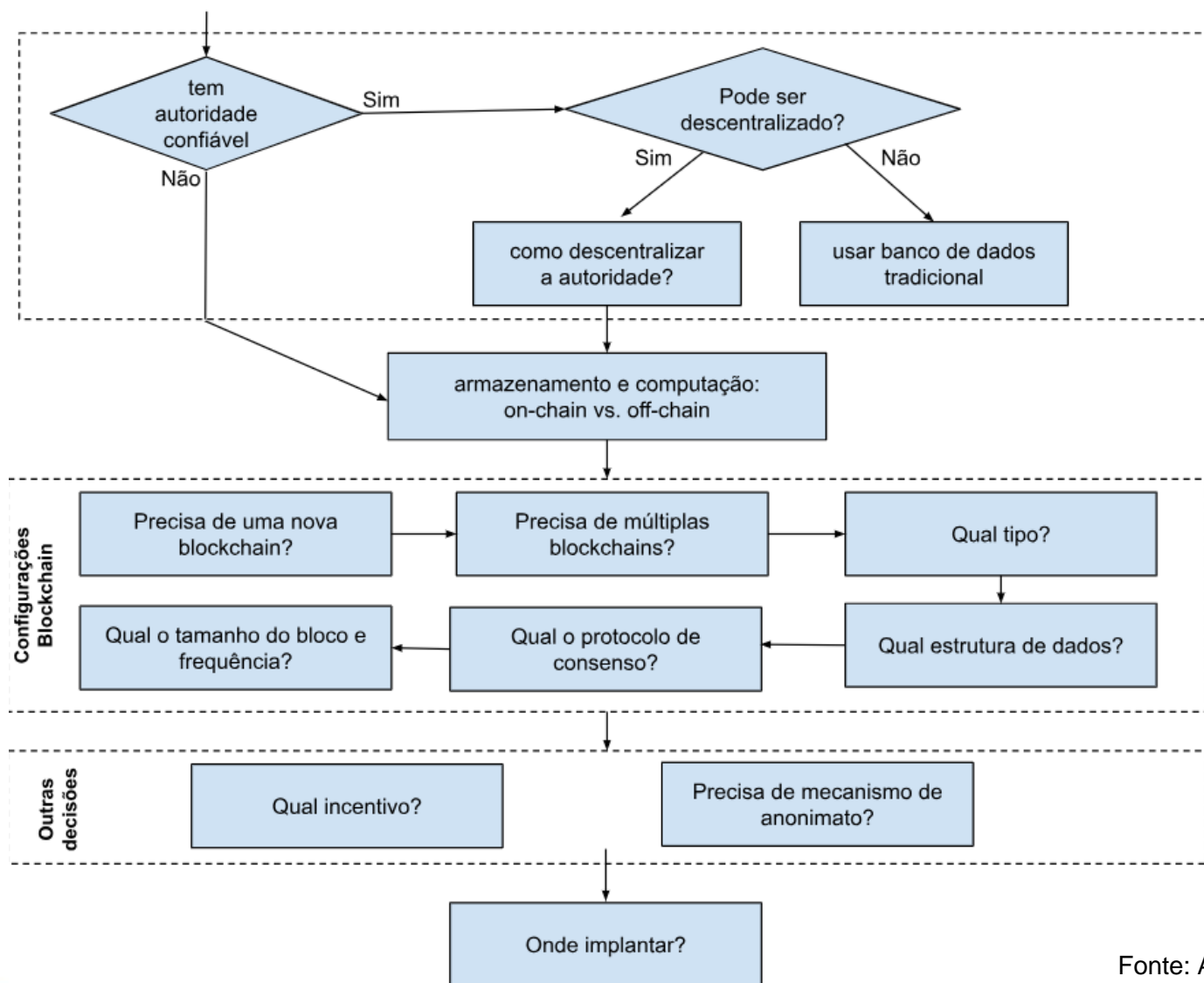
Uma aplicação descentralizada pode ser considerada, como uma aplicação web aberta, desenvolvida sobre serviços de infraestrutura P2P.

Um dos requisitos para criar dApps tem sido o uso de plataformas de blockchain descentralizadas, como a Ethereum.

As dApps podem ser visualizadas nas áreas de entretenimento, finanças (DeFis), redes sociais, navegadores e serviços de tecnologia descentralizados.



# Decisões para o desenvolvimento de dApps baseadas em Blockchain



Fonte: Adaptado de XU et al., 2018.



## dApp baseada em Blockchain

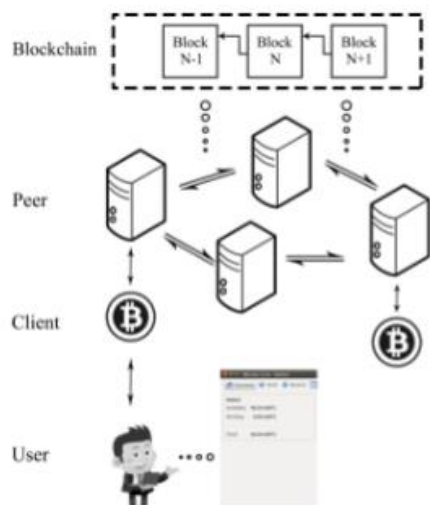
Fazer uso de blockchain em projetos, inclui compreender a concepção de dApps.

Uma visão arquitetural pode facilitar essa abordagem, como uma forma de guiar a construção de aplicações que tenham como base a blockchain.

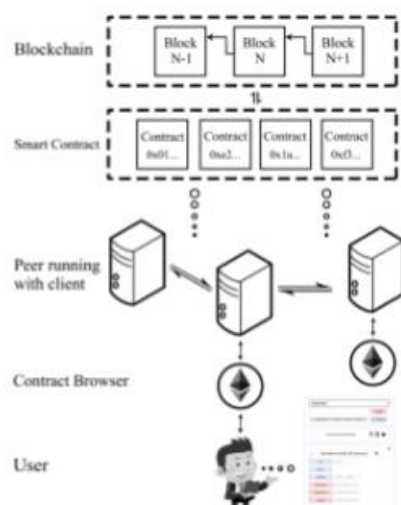


# Arquiteturas de dApps baseadas em Blockchain

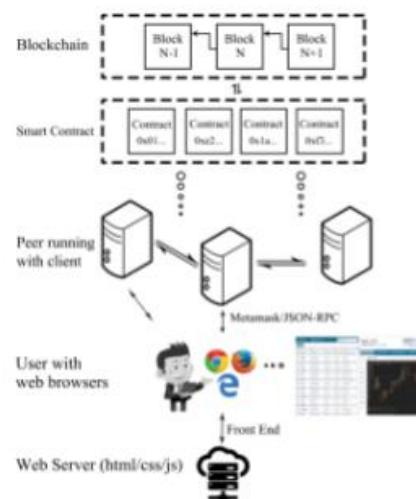
Zheng et al. (2023) apresentam a evolução de arquiteturas de dApps.



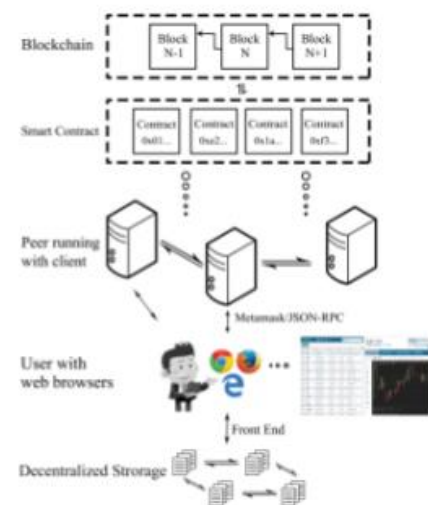
(a) Native Client as a DApp



(b) Smart Contract as a DApp



(c) Web & Contract as a DApp



(d) Fully-decentralized DApp

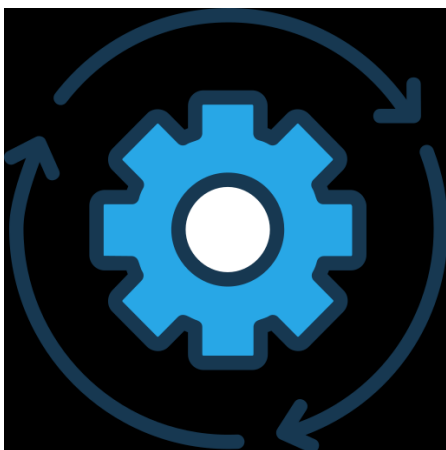
Arquiteturas de DApp. ZHENG et al., 2023.



# Arquiteturas de dApps baseadas em Blockchain

Para definição do grau de descentralização (total ou parcial) durante a concepção arquitetural de dApps, é preciso avaliar duas dimensões:

## Operacional



## Dados



# Arquiteturas de dApps baseadas em Blockchain

## Operacional

Envolve o tipo de rede blockchain envolvida e o emprego de contratos inteligentes

Totalmente descentralizada: rede blockchain pública

Parcialmente descentralizada: rede blockchain privada

## Dados

É analisado considerando o serviço de armazenamento usado pela aplicação

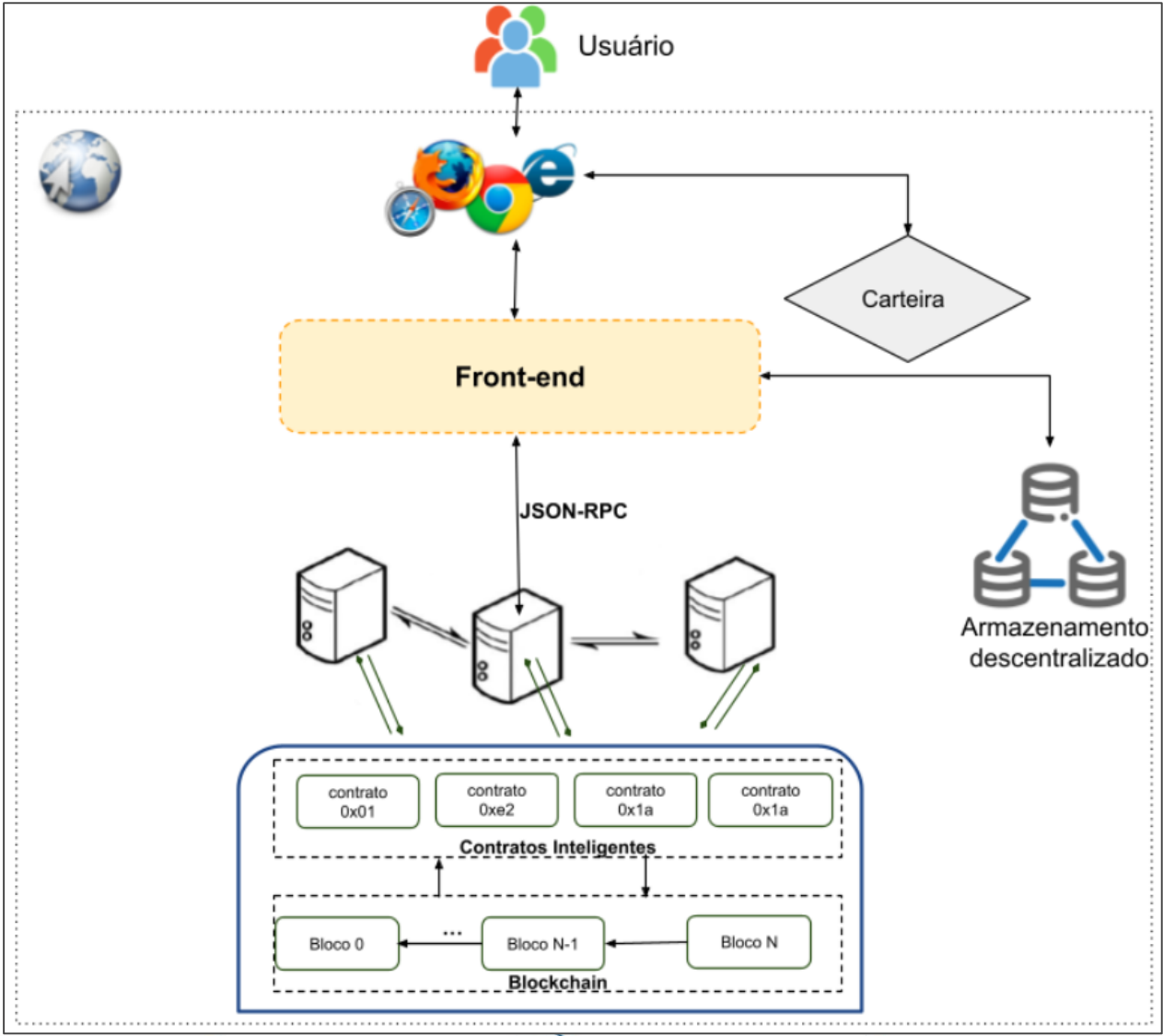
Totalmente descentralizada: armazenamento por meio de uma rede P2P

Parcialmente descentralizada: armazenamento centralizado





# Proposta de Arquitetura para dApps baseada em Blockchain



# Proposta de Arquitetura para dApps baseada em Blockchain

## Pontos Importantes

Infraestrutura para serviços de blockchain

Rede de servidores de hardware dedicados

Servidores virtualizados controlados por um provedor de nuvem

Descentralização do front-end da aplicação

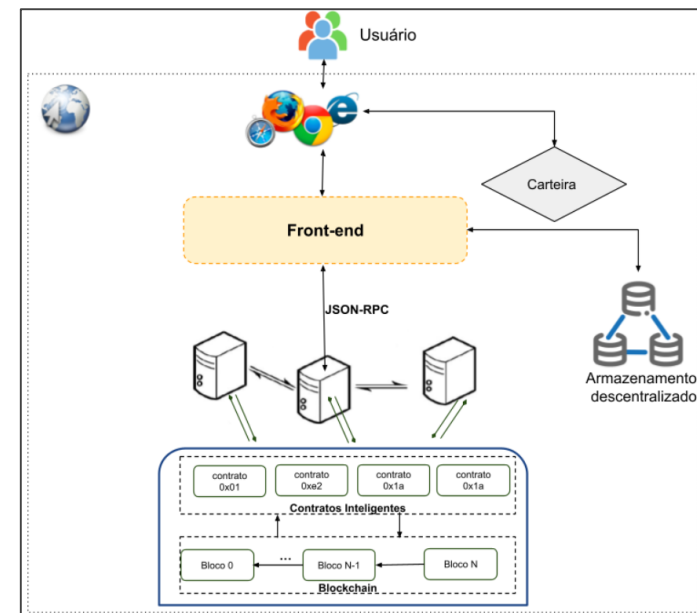
Armazenamento descentralizado de dados sensíveis

Identidades descentralizadas

Limitações da blockchain em termos de

velocidade das transações e custo do gas

Stack de desenvolvimento de acordo com as decisões de projeto



# Considerações Finais

Estudo buscou pavimentar o caminho para um entendimento mais amplo das dApps baseadas em blockchain

Identificou as principais decisões relacionados às características da plataforma blockchain, visto que ainda é apresentado de forma esparsa na literatura

Uma visão arquitetural de uma dApp baseadas em blockchain colabora com o entendimento das tecnologias utilizadas no ecossistema da Web 3.0

Próximos passos:

Buscar trabalhos primários que apresentam dApps em área específica

Definição da *stack* voltada para principais decisões de projeto

Implementar dApps para as principais *stacks* propostas



# Referências

- A. M. Antony e G. Wood, Mastering Ethereum: Building Smart Contracts and DApps, 2nd ed. O'Reilly Media, 2018.
- COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim; et al. Sistemas distribuídos. Grupo A, 2013. E-book. ISBN 9788582600542. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788582600542/>. Acesso em: 18 jun. 2023.
- GREVE, Fabíola Greve et al. Blockchain e a Revolução do Consenso sob Demanda. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)-Minicursos, 2018.
- WÜST, Karl; GERVAIS, Arthur. Do you need a blockchain?. In: 2018 crypto valley conference on blockchain technology (CVCBT). IEEE, 2018. p. 45-54.
- X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, e P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in 2017 IEEE international conference on software architecture (ICSA). IEEE, 2017, p. 243–252.
- ZHENG, Peilin et al. Blockchain-based Decentralized Application: A Survey. IEEE Open Journal of the Computer Society, 2023.



# Aplicações Descentralizadas Baseadas em Blockchain

Noeli A. Pimentel Vaz

Sistemas Distribuídos - Prof. Sérgio T. de Carvalho  
Instituto de Informática | UFG

