

*BLOCKCHAIN
APLICADA À COMPUTAÇÃO NA NUVEM
"BLOCKCHAIN MEETS CLOUD COMPUTING: A SURVEY"*

Docente: Antônio Jorge Abelém
Discentes: Jacqueline Teixeira, Joaquim Viana, Jônatas Moraes.

Belém - PA
2023

O survey

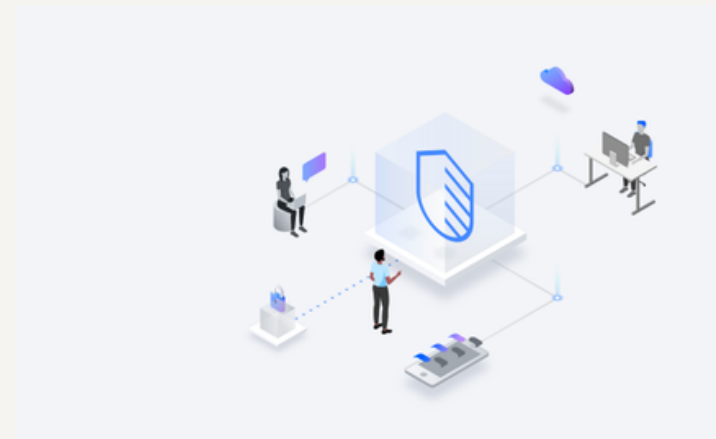
É um levantamento que explora a interseção entre blockchain (cadeia de blocos) e computação em nuvem. Fornecendo uma visão geral abrangente sobre como essas duas tecnologias emergentes podem ser combinadas e os benefícios resultantes dessa combinação.



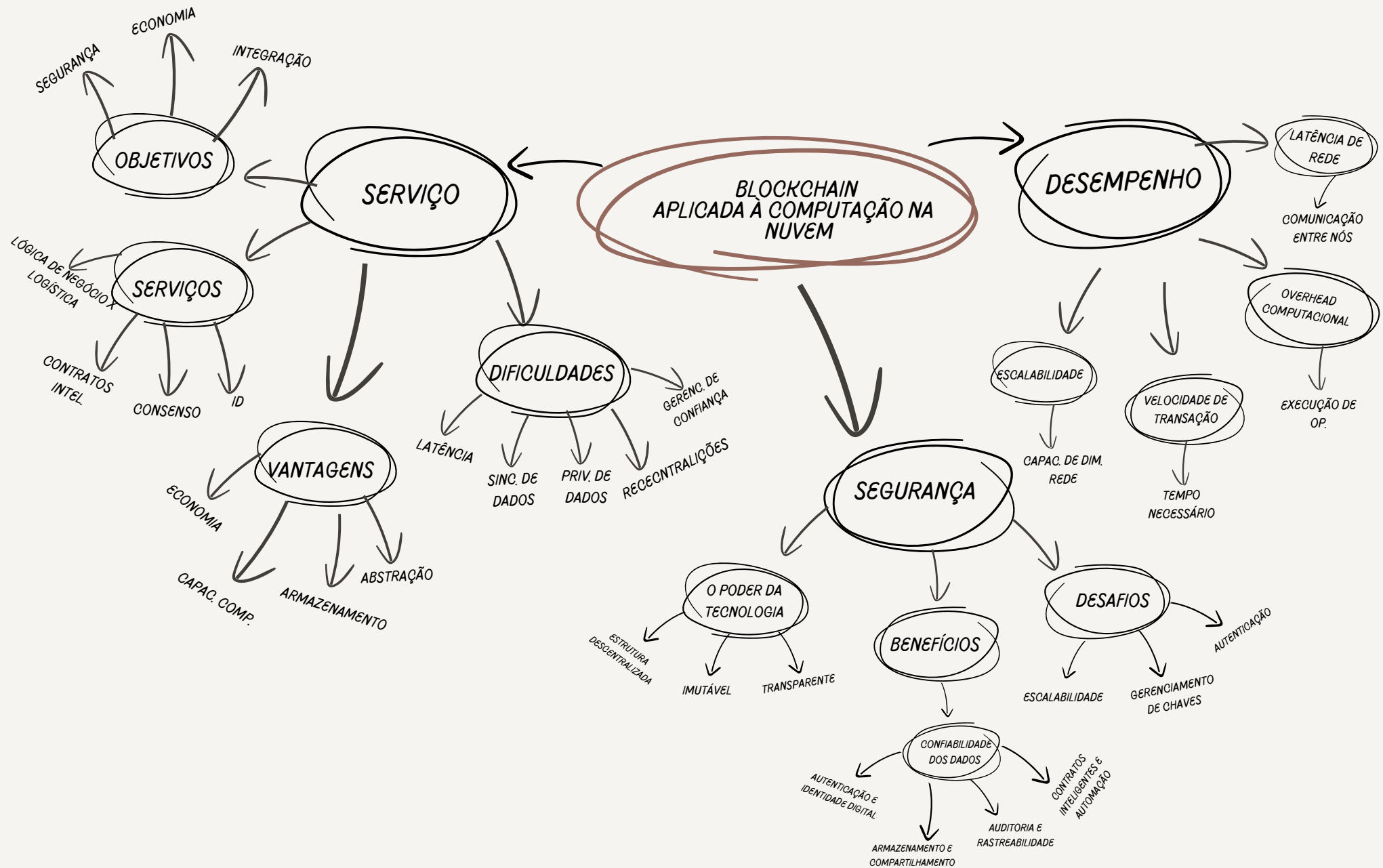
Descrição dos Tópicos

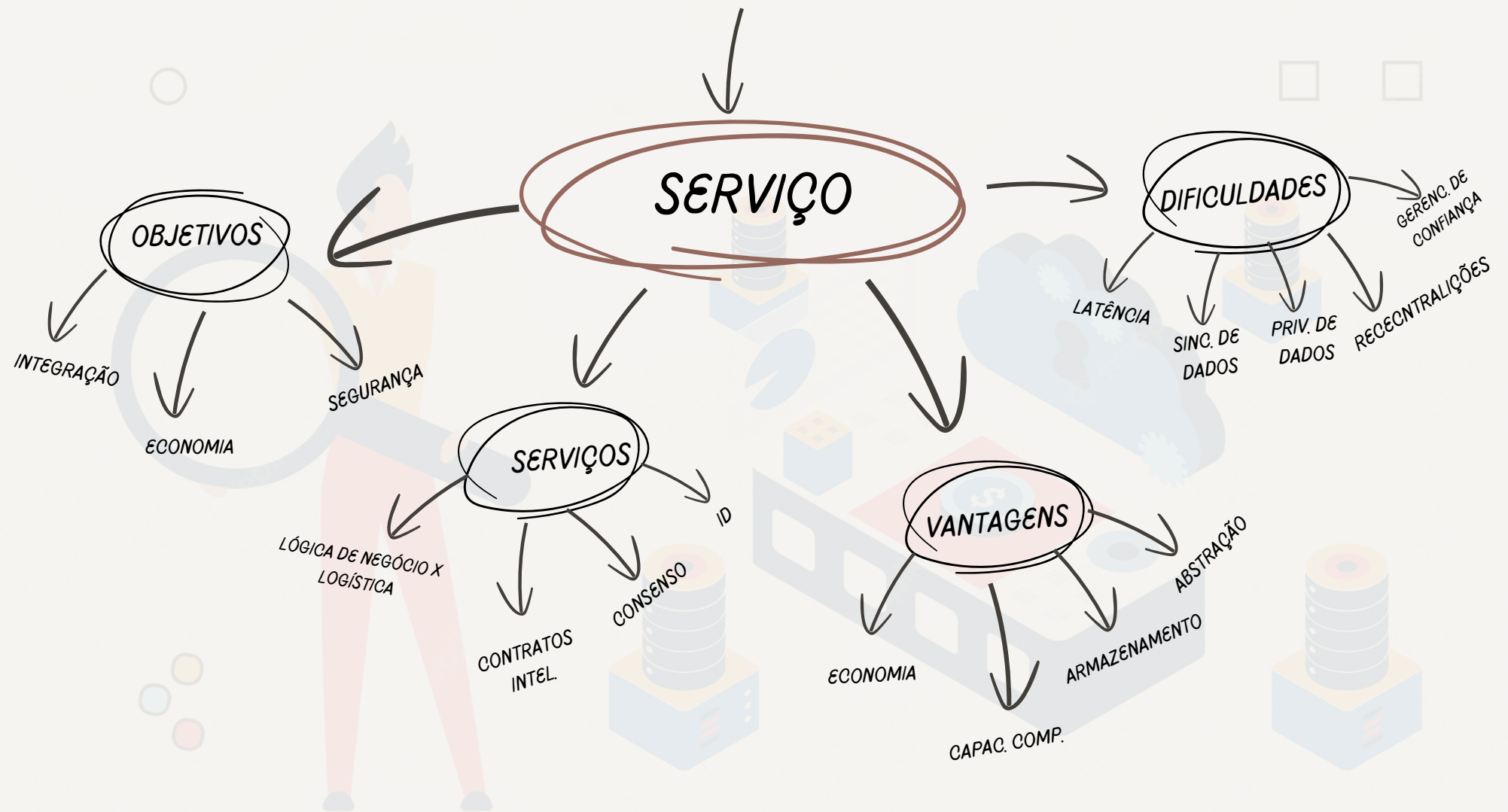


O artigo mergulha em uma análise detalhada sobre a interseção entre Blockchain e computação em nuvem, com ênfase nos aspectos de: serviços, segurança e desempenho.



Mapa Mental





Blockchain como serviço - BaaS

Modelo de negócio que visa oferecer infraestrutura blockchain em nuvem como recurso computacional para oferecer suporte à outras aplicações. O principal intuito é permitir que os clientes direcionem o seu foco nos aspectos do seu negócio em si e as complexidades do blockchain fiquem por conta dos provedores do serviço.



Objetivos e vantagens

Integração

Possibilidade de integrar, de forma confiável, diferentes processos de um mesmo negócio ou de diferentes negócios relacionados.

Armazenamento

Alta capacidade de armazenamento dos provedores de serviços em nuvem.

Economia

Menores gastos tanto em infraestrutura quanto treinamento, manutenção e detalhes de mais baixo nível.

Abstração

Retira do usuário a responsabilidade com aspectos técnicos para focar nos aspectos de governança e etc.

Segurança

Confidencialidade, privacidade e controle de acesso à dados sensíveis.

Capacidade Computacional

Capacidade de escalar as transações com pouco impacto no desempenho.

Lógica de negócios x logística

Compartilhar dados de forma segura e confidencial entre si e com seus próprios clientes de transporte, despachantes de carga e outros participantes do ecossistema sob uma sólida estrutura de gerenciamento e governança de dados.

Blockchain Use Cases

Oracle and CargoSmart Team to Speed up the Technical Collaboration across Nine Market Leaders to Transform Global Shipping Industry



Pagamentos globais

Transferências internacionais são processos cansativos e burocráticos. Esse processo é realizado com solicitações entre vários bancos com diferentes responsabilidades. Através do blockchain, todos os envolvidos podem participar de uma única rede e podem estar cientes das transações registradas na blockchain.

FORBES > MONEY > CRYPTO & BLOCKCHAIN

Amazon Steps Up Blockchain Commitment; Web Services Partners With Digital Currency Group

Laura Shin Senior Contributor @

I write and podcast about crypto/blockchain technology.

Follow

May 2, 2016, 12:00pm EDT

TECH TRANSFORMERS

Google-backed blockchain start-up Ripple raises \$55 million from big banks

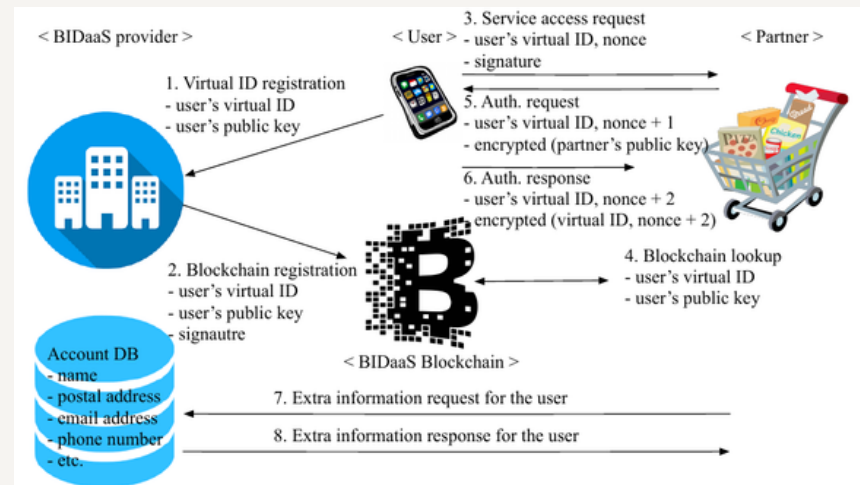
PUBLISHED THU, SEP 15 2016-9:23 AM EDT | UPDATED THU, SEP 15 2016-9:27 AM EDT

ID virtual baseado em blockchain (BIDaaS)

Infraestrutura de gerenciamento e autenticação de um provedor de BIDaaS para parceiros através de chaves públicas e privadas e assinatura digital.

TABLE I: Notations

Notation	Definition
\mathcal{S}^{usr}	Virtual ID of a user
K_{pri}^{usr}	Private key of the user
K_{pub}^{usr}	Public key of the user
K_{pri}^{pro}	Private key of a BIDaaS provider
K_{pub}^{pro}	Public key of the BIDaaS provider
K_{pri}^{ptn}	Private key of a partner
K_{pub}^{ptn}	Public key of the partner
$Sig_{K_{pri}}(\cdot)$	Signature with the private key K_{pri}
$E_{K_{pub}}(\cdot)$	Encryption with the public key K_{pub}
r	Nonce



Desafios

Latência

Alguns sistemas IoT demandam velocidade na comunicação

Privacidade de dados

Ainda é necessário meios para proteger dados em sistemas BIDaaS.

Sincronização de dados

Sincronização entre blockchains multi-cadeias ainda necessita de pesquisa.

Recentralizações/Ger. de confiança

Provedores de serviços podem ter conexões com partes interessadas

SEGURANÇA

O PODER DA TECNOLOGIA

ESTRUTURA
DESCENTRALIZADA

IMUTÁVEL

TRANSPARENTE

BENEFÍCIOS

CONFIABILIDADE DOS DADOS

AUTENTICAÇÃO E
IDENTIDADE DIGITAL

ARMAZENAMENTO E
COMPARTILHAMENTO

AUDITORIA E
RASTREABILIDADE

CONTRATOS INTELIGENTES E
AUTOMAÇÃO

DESAFIOS

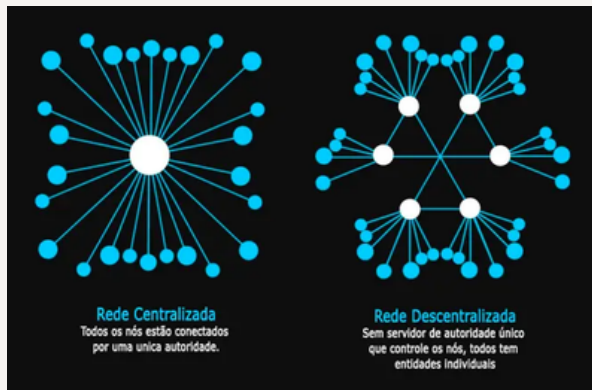
ESCALABILIDADE

GERENCIAMENTO
DE CHAVES

AUTENTICAÇÃO

O poder da Tecnologia

ESTRUTURA DESCENTRALIZADA



Refere-se à transferência do controle e de decisões de uma entidade centralizada (indivíduo, organização ou grupo) para uma rede distribuída.

IMUTÁVEL

Nenhum participante poderá violar uma transação depois que alguém registrá-la no ledger compartilhado. Se o registro de uma transação apresentar erro, você deverá adicionar uma nova transação para revertê-lo, e ambas as transações estarão visíveis na rede.



TRANSPARENTE



Estabelece regras sobre o consentimento dos participantes para o registro das transações. Você só poderá registrar novas transações quando a maioria dos participantes da rede der seu consentimento.

Benefícios

CONFIABILIDADE DOS DADOS

AUTENTICAÇÃO E IDENTIDADE DIGITAL

Usar a blockchain como um registro imutável de identidades, é possível garantir a veracidade das informações e reduzir os riscos de ataques de falsificação ou roubo de identidade. permite que os usuários tenham controle sobre suas próprias informações, fortalecendo a privacidade e a segurança.

ARMAZENAMENTO E COMPARTILHAMENTO

Ao usar a criptografia e a estrutura distribuída da blockchain, os dados podem ser armazenados de forma descentralizada, tornando-os menos vulneráveis a ataques de hackers ou falhas em servidores centrais. Além disso, a natureza imutável da blockchain garante a integridade dos dados, permitindo que as partes confiem nas informações armazenadas.

Benefícios

CONFIABILIDADE DOS DADOS

AUDITORIA E RASTREABILIDADE

Ao registrar todas as transações em uma blockchain, é possível ter um histórico completo e verificável de atividades. Isso permite que auditorias sejam realizadas de forma mais eficiente e confiável, facilitando a detecção de fraudes e a conformidade com regulamentações.

CONTRATOS INTELIGENTES E AUTOMAÇÃO

Esses contratos são executados automaticamente quando as condições predefinidas são atendidas, eliminando a necessidade de intermediários e reduzindo os riscos de erros ou fraudes. Com a transparência e a imutabilidade da blockchain, as partes envolvidas podem confiar nas condições e resultados acordados nos contratos inteligentes.

Desafios para Segurança

ESCALABILIDADE

Velocidade com que consegue processar um determinado número de operações, medida pela taxa de transações por segundo (TPS).

GERENCIAMENTO DE CHAVES

Consiste em armazenar, proteger, organizar e garantir o uso adequado delas, gerir seu ciclo de vida e manter cópias.

AUTENTICAÇÃO

Provar a existência de um documento, através do registro desse documento em uma Rede Blockchain Pública

DESEMPENHO

ESCALABILIDADE

CAPAC. DE DIM.
REDE

VELOCIDADE DE
TRANSAÇÃO

TEMPO
NECESSÁRIO

OVERHEAD
COMPUTACIONAL

EXECUÇÃO DE
OP.

LATÊNCIA DE
REDE

COMUNICAÇÃO
ENTRE NÓS

Fatores que afetam o desempenho

ESCALABILIDADE:

Capacidade de uma rede blockchain lidar com um aumento no número de transações e participantes sem comprometer seu desempenho. A falta de escalabilidade pode afetar negativamente o desempenho da rede blockchain de várias maneiras:

- Atrasos nas transações
- Congestionamento da rede
- Aumento dos custos

VELOCIDADE DE TRANSAÇÃO:

Rapidez com que as transações são processadas e confirmadas em uma rede blockchain. A velocidade de transação pode afectar no desempenho da rede blockchain de várias maneiras:

- Eficiência e experiência do usuário
- Congestionamento da rede
- Tempo de confirmação

Fatores que afetam o desempenho

OVERHEAD COMPUTACIONAL:

Refere-se aos recursos adicionais exigidos para executar operações relacionadas à blockchain que podem afetar o desempenho geral do sistema. PEx.: Criptografia, Consenso, Armazenamento de dados. O overhead computacional afeta o desempenho da rede blockchain de várias maneiras:

- Tempo de processamento
- Capacidade de processamento
- Consumo de recursos

Fatores que afetam o desempenho

LATÊNCIA DE REDE:

Refere-se ao tempo de resposta entre a solicitação de uma transação na rede blockchain e o recebimento da resposta. É influenciada por vários fatores: distância física entre os nós da rede, velocidade de conexão de rede, carga de tráfego na rede, etc. A latência de rede pode afetar o desempenho da rede blockchain de várias maneiras:

- Tempo de confirmação
- Experiência do usuário
- Sincronização da rede
- Ataques de duplo gasto

Para lidar com os desafios de **escalabilidade**, várias soluções têm sido propostas:

- Implementação de algoritmos de consenso mais eficientes: Proof of Stake (PoS), em vez do Proof of Work (PoW).
- Implementação de técnicas como a divisão em fragmentos (sharding) e o uso de canais de pagamento (payment channels).

Para melhorar a **velocidade de transação**, várias soluções têm sido propostas:

- Otimização dos algoritmos de consenso
- Uso de técnicas de compressão de dados
- Uso de canais de pagamento.

Soluções propostas para melhorar o desempenho

Para minimizar o **overhead computacional**, várias soluções têm sido propostas:

- Otimizações de algoritmos
- Escolha de algoritmos de criptografia eficientes
- Implementação de técnicas de compressão de dados
- Alocação eficiente de recursos e equilíbrio adequado entre segurança e eficiência na escolha do algoritmo de consenso.

Soluções propostas para melhorar o desempenho

Para melhorar o desempenho da rede blockchain em relação à **latência de rede**, podem ser adotadas medidas como:

- Melhoria da infraestrutura de rede
- Algoritmos de consenso eficientes
- Uso de tecnologias de escalonamento

Desafios e Oportunidades

São discutidos os desafios e as limitações enfrentados na integração de blockchain e computação em nuvem, como escalabilidade, custos, complexidade técnica, regulamentações e interoperabilidade entre diferentes plataformas.



Conclusão

Oferecendo uma visão geral abrangente do uso conjunto de blockchain e computação em nuvem, explorando suas vantagens, desafios e oportunidades, o trabalho fornece assim, um valioso recurso para pesquisadores, profissionais e interessados nessas áreas.



BLOCKCHAIN APLICADA À COMPUTAÇÃO NA NUVEM

OBRIGADO!

Discentes: Jacqueline Teixeira, Joaquim Viana, Jônatas Moraes.

Docente: Antônio Jorge Abelém

Belém - PA

2023