Trabalho de Tecnologia e Inovação

**BLOCKCHAIN E COMPUTAÇÃO DESCENTRALIZADA**

Por Geovanna Diniz, Laura Farias, Maria Eduarda Sanches e Willamy Ricardo Andreotti

3°E TECH

**Tópicos abordados**

1. Computação descentralizada e Blockchain
2. Funcionamento do Blockchain
3. Contratos inteligentes e Identidades digitais
4. Computação Confidencial e Segurança na Web3

**1. Computação Descentralizada e Blockchain**

**O que é computação descentralizada?**

A computação descentralizada é um tipo de processamento e armazenamento de dados em que a computação não está concentrado em um único servidor, mas sim distribuído entre diversos dispositivos ou nós de uma rede. Esse modelo contrasta com a computação tradicional, onde grandes empresas ou instituições detêm o controle sobre servidores centrais.

Na computação descentralizada, os recursos são compartilhados por múltiplos plataformas, reduzindo a dependência de uma única entidade e tornando o sistema mais seguro, resiliente e resistente a censura.

**Benefícios:**

* **Maior Segurança**, sem um único ponto de falha, ataques cibernéticos tornam-se mais difíceis e dados armazenados em vários nós reduzem o risco de perda total por falhas
* **Resistência à Censura**, nenhuma entidade pode controlar ou restringir o acesso às informações e útil em países com restrições à liberdade de expressão.
* **Autonomia do Usuário,** os usuários possuem maior controle sobre seus próprios dados, sem depender de terceiros. Exemplos: Carteiras de criptomoedas permitem transações sem bancos.
* **Maior Disponibilidade**, sistemas descentralizados podem continuar operando mesmo que alguns nós falhem. Exemplo: A rede Bitcoin nunca parou desde sua criação em 2009.
* **Redução de Custos e Intermediários**, elimina a necessidade de intermediários (bancos, cartórios, servidores centralizados) e transações financeiras podem ser feitas diretamente entre usuários.

**O que é blockchain?**

Blockchain é uma tecnologia de registro distribuído que permite armazenar e validar informações de forma segura, transparente e imutável, sem a necessidade de uma autoridade central. Ele é muito comparado com um livro-razão digital descentralizado, onde os dados são organizados em blocos interligados, formando uma cadeia contínua, daí o nome "blockchain", ou "cadeia de blocos".

Cada bloco contém um conjunto de registros, como transações financeiras, contratos inteligentes ou qualquer outro dado, um código único chamado hash, e um link para o bloco anterior. Isso garante que qualquer tentativa de alteração em um bloco afete toda a cadeia, tornando a manipulação dos dados praticamente impossível.

**Principais Características do Blockchain**

### **Descentralização**, não há uma autoridade central controlando os dados.

### **Imutabilidade,** uma vez registrado, um bloco não pode ser alterado sem comprometer toda a cadeia.

* **Segurança,** usa criptografia avançada para garantir a integridade das informações.
* **Transparência,** qualquer pessoa pode verificar os registros, mas sem comprometer a privacidade.

**2. Funcionamento do Blockchain**

O sistema de blockchain é formado por uma cadeia de blocos e tenta garantir completamente a segurança, isso acontece de diversas formas durante a criação de uma transação.

**Estrutura de blocos**

Primeiramente, as informações de uma transação (por exemplo: produto, remetente, destinatário, quando, onde etc.) são adicionadas a um **bloco**, cada bloco recebe um hash como identificador único e um hash de referência ao bloco anterior. Os blocos confirmam o tempo exato e a sequência de transações.

**Consenso**

Antes que uma transação seja adicionada à cadeia os participantes da rede precisam concordar que ela é válida, existem mecanismos para isso, os mais comuns são **proof of work** **(PoW)** e **proof of stack(PoS)**. PoW exige que os usuários da rede participem de uma ‘corrida’ para resolver um problema matemático que consiste em encontrar um hash correspondente ao da transação atual, para isso são necessários computadores caros e especializados, o vencedor adiciona a transação e recebe uma recompensa em bitcoins. Enquanto isso, o PoS escolhe os validadores pela quantidade de criptomoedas que possuem e com o quanto estão dispostos a ‘travar’ como garantia.

**Imutabilidade**

Nesse sistema, a imutabilidade é extremamente importante para garantir que as informações de uma transação não sejam falsificadas, por isso nenhum bloco pode ser alterado, assim como nenhum bloco pode ser inserido entre outros dois, assim cada bloco reforça a segurança do anterior.

Todos os participantes de uma rede blockchain tem acesso a um livro-razão, onde cada transação é registrada apenas uma vez, caso uma transação tenho um erro, uma nova transação deve ser adicionada para reverter isso, mas o ‘erro’ nunca será deletado, ambas serão visíveis.

Todos esses requisitos garantem a segurança em uma rede que utiliza blockchain, dificultando a realização de fraudes.

**3. Contratos inteligentes e identidade digitais**

**O que são contratos inteligentes?**

Também conhecidos como Smart Contracts (em inglês), os Contratos Inteligentes são modelos de contratos que usam a tecnologia de Blockchain para descentralizar o controle documental e garantir mais segurança. Eles são excelentes exemplos de como de como é possível facilitar processos robustos sem perder a eficácia e a segurança.

Basicamente, consistem em protocolos computacionais de natureza digital que têm as mesmas finalidades de contratos tradicionais, que são estabelecidos entre duas partes ou mais partes. Diferentemente da modalidade firmada em papel, o formato digital não pode ser adulterado ou extraviado, tendo natureza autoexecutável. Os smart contracts têm a mesma validade jurídica de um contrato comum, em papel: formalizar um acordo entre duas ou mais partes, apenas diferenciando-se pelo uso da tecnologia para firmar estes documentos. Antes da emissão do contrato, cláusulas e consequências são programadas.

Após o fechamento do contrato, todas as exigências são ativadas automaticamente, facilitando, por exemplo, cobranças e acompanhamento de processos.

**Como utilizam Blockchain?**

Para que os contratos digitais funcionem igualmente a um contrato convencional, é necessário que estes utilizem uma tecnologia que acompanhe dados compartilhados e permita comunicações de maneira direta e criptografada, viabilizando a sua validação. É exatamente o que a Blockchain, tecnologia que realiza transações seguras e imutáveis de maneira descentralizada e distribuída.

A principal finalidade de utilizar a Blockchain, é a de eliminar a necessidade de haver um intermediário, como acontece nos contratos convencionais. Por ser uma rede totalmente descentralizada, há uma grande vantagem na utilização da blockchain para executar os contratos inteligentes: transparência e segurança.

**Vantagens em comparação a um contrato tradicional**

A primeira vantagem que este tipo de abordagem contratual oferece, é a transparência. Ao ser registrado na rede blockchain, o contrato e todas as suas clausulas estarão totalmente visíveis para todas as partes participantes daquele contrato. A falta de transparência é um problema que contratos convencionais enfrentam, mas que pode ser facilmente resolvido por contratos inteligentes.

A segunda, é a auto execução. Uma vez criado o código, com todas as condições, ele se torna automático. Validade, preço, e outras alterações que um contrato comum pode sofrer, são automaticamente realizadas se o contrato for inteligente, até que alguém se interesse em fechar o contrato.

A terceira característica de um contrato inteligente é a rastreabilidade. Os contratos inteligentes facilitam o rastreamento de uma transação, condições e termos do contrato, então todas as partes podem ver a origem dessas informações.

A última vantagem é a imutabilidade. Não existe, em um contrato tradicional, a garantia de que este nunca sofrerá mudanças sem a visibilidade de ambas as partes, mas isso é possível em um contrato inteligente graças a tecnologia Blockchain, que oferece imutabilidade em suas transações.

**Uso dos contratos digitais**

Pela confiabilidade que os contratos digitais vêm passando por conta de todas as vantagens que oferecem, estão sendo amplamente utilizados em vários setores da sociedade. Um exemplo, são as eleições.

Isso seria muito interessante pois permitiria que as pessoas votassem de suas casas, incentivando as votações em países onde isso é facultativo, além de impedir que fraudes ocorressem, por conta da transparência que os contratos digitais oferecem.

**Identidades convencionais e problemas**

A identidade é parte integrante de uma sociedade e economia funcionais. Integridade e transparência são elementos fundamentais para que nossas posses, bens, e todos os tipos de acesso estejam seguros.

Hoje, para as empresas, a identidade funciona em um armazenamento de dados comerciais de rotinas menos confidencias, o que cria riscos comerciais com o aumento de regulamentações centradas na privacidade do usuário. Para os indivíduos, formas físicas de identificação não estão amplamente disponíveis para todos os humanos por várias razões e processos burocráticos. Aproximadamente 1,1 bilhão de pessoas no mundo não têm uma forma de reivindicar a propriedade sobre sua própria identidade, deixando cerca de um sétimo da população mundial em um estado vulnerável – incapaz de votar, possuir bens, abrir uma conta bancária ou adquirir emprego. A incapacidade de obter documentação limita a liberdade dessas pessoas. Processos complicados de papelada, despesas e falta de acesso e conhecimento sobre identidade pessoal são os principais obstáculos.

Falando sobre identidade digital, a experiência do cenário de identidade do usuário é excepcionalmente fragmentada e insegura. Não há uma maneira padronizada de usar dados gerados por uma plataforma em outra. Além disso, há um elo fraco entre identidades digitais e offline que torna relativamente fácil criar identidades falsas, que criam terreno fértil para interação falsa, o que gera os mais variados tipos de fraudes.

**Identidades digitais**

Assim como os contratos inteligentes, que utilizam a tecnologia Blockchain com a principal finalidade de segurança, as identidades digitais têm o mesmo propósito. Os sistemas de identificação que utilizarem essa tecnologia, podem resolver inúmeros problemas que a sociedade hoje enfrenta utilizando identidades convencionais: inacessibilidade, insegurança de informações e identidades fraudulentas.

Uma vez pareado com uma identidade descentralizada provida através de um sistema Blockchain, os usuários podem apresentar o ID verificado na forma de um código QR para provar sua identidade e acessar determinados serviços, assim como funcionam os acessos digitais e identidades no papel.

**4. Computação confidencial e segurança na web3**

**Computação Confidencial:**

Conceito utilizado para a proteção e segurança dos dados durante o processamento, de forma que ninguém possa visualizar, nem mesmo o provedor da infraestrutura.

Ele é utilizado em ambientes seguros dentro do hardware denominados **Trusted Execution Environments (TEEs)**, onde o código é totalmente seguro e criptografado.

**Web3:**

A web3 é uma ideia baseada na blockchain e descentralização. Seu objetivo é criar uma internet mais aberta, direta e segura, com criptografias ponta a ponta. Essas tecnologias formam uma nova geração da internet, que atualmente é usada por empresas de alto porte devido à maior segurança, escalabilidade e privacidade para os usuários

**Importância:**

Embora as blockchains sejam seguras, suas transações ainda são públicas. Isso quer dizer que qualquer pessoa com acesso à internet pode visualizar e analisar informações que podem ser privadas ou sigilosas. Essa transparência absoluta pode ser um problema em casos como:

* **Sistemas financeiros descentralizados (DeFi)** - Transações podem ser exploradas por bots de front-running.
* **Oráculos de dados** - Informações externas podem ser comprometidas sem um ambiente seguro.
* **Indentidade digital** - Exposição desnecessária dos dados pessoais.

Com Computação Confidencial, é possível ocultar informações sensíveis dentro de contratos inteligentes privados, garantindo o acesso apenas às pessoas autorizadas.

### **Principais Tecnologias**

* **TEE (Trusted Execution Environment)** → Executa código de forma isolada do sistema operacional.
* **Zero-Knowledge Proofs (ZKP)** → Permite comprovar uma afirmação sem revelar os dados.
* **Fully Homomorphic Encryption (FHE)** → Permite cálculos em dados criptografados sem necessidade de descriptografia.

<https://www.youtube.com/watch?v=qy5fbR8eXAE>

**Apresentação dos slides**

<https://www.canva.com/design/DAGgMsGF3dI/b71IiCLHx-fI3jobVZ4u0g/edit?utm_content=DAGgMsGF3dI&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton>

**Bibliografia e referências utilizadas**

<https://consensys.io/blockchain-use-cases/digital-identity>  
<https://redelideres.com/2024/08/16/a-revolucao-da-automacao-de-processos-com-blockchain/>

<https://www.docusign.com/pt-br/blog/contratos-inteligentes>  
<https://www.youtube.com/watch?v=6yyvBZc_Fc0>

https://aws.amazon.com/pt/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

<https://www.ibm.com/br-pt/topics/blockchain>