INTRODUÇÃO À INVESTIGAÇÃO

BLOCKCHAIN E AS SUAS APLICAÇÕES

Prof.ª Teresa Gonçalves

Rúben Farinha, 48329
Rodrigo Isaque, 45437

O que é a Blockchain

- A blockchain é um livro de registros digital, descentralizado e imutável
- Registros de transações são mantidos de forma segura e transparente
- Composta por uma rede de computadores interconectados que validam e verificam transações automaticamente, sem intermediários
- Pode ser utilizada em diversos setores como finanças, saúde, logística e administração pública
- Garante transparência, segurança e eficiência nos processos
- É resistente a fraudes e ataques cibernéticos devido à validação descentralizada de transações

Funcionamento

- A Blockchain é composta por uma rede de computadores interconectados (nós)
- Cada nó contém uma cópia do livro de registros (ledger)
- As transações são agrupadas em blocos e adicionadas ao livro de registros de forma sequencial
- Cada bloco é validado por uma rede de nós por meio de um processo de consenso
- Uma vez validado, o bloco é adicionado permanentemente à cadeia de blocos
- Cada bloco contém uma chave hash que é gerada a partir do hash do bloco anterior na cadeia
- Isso garante a integridade da cadeia, uma vez que qualquer tentativa de alteração de um bloco será imediatamente detetada pela rede
- Como resultado, a Blockchain é descentralizada e altamente segura, pois é quase impossível manipular ou corromper os dados na rede.

Smart contracts

- Smart Contracts são contratos autoexecutáveis programados para serem executados quando certas condições são atendidas
- Eles são executados de forma segura e transparente, sem a necessidade de intermediários, usando a tecnologia blockchain
- No setor financeiro, podem automatizar a liquidação de transações, reduzindo custos
- Na logística, podem automatizar o tracking de mercadorias, reduzindo os riscos de roubos ou fraudes
- Em imóveis, podem automatizar a transferência de propriedade, eliminando a necessidade de intervenção de terceiros
- Na área de direitos de autor, podem automatizar o processo de licenciamento, garantindo pagamento aos criadores
- Na votação eletrónica, podem ajudar a garantir a integridade do processo eleitoral, garantindo que os votos sejam contados de forma justa e precisa
- Em resumo, os smart contracts são uma tecnologia inovadora e promissora que pode automatizar muitos processos, reduzindo a necessidade de intermediários e aumentando a transparência e a segurança das transações.

Segurança

- A segurança é uma das principais preocupações na adoção da tecnologia Blockchain, pois esta depende da confiança, imutabilidade e integridade dos dados armazenados nos seus blocos.
- Uma das principais técnicas de segurança utilizadas é a criptografia, onde a utilização de chaves é utilizada na maioria das blockchains, onde chaves privadas são utilizadas para assinar transações e as chaves públicas podem ser usadas para verificar as transações
- A prevenção de ataques de 51% é uma técnica crucial para garantir a segurança na blockchain. Esse tipo de ataque ocorre quando "crypto miners" controlam mais de 50% do poder da rede, o que lhes permite modificar transações passadas ou até mesmo criar transações falsas. Isso pode levar a uma quebra da confiança na rede e comprometer a sua integridade. Por isso, a maioria das blockchains utiliza algoritmos de consenso distribuído, como o "Proof-of-Work" ou o "Proof-of-Stake", que exigem que os "crypto miners" realizem um trabalho para validar transações e criar blocos, reduzindo assim a possibilidade de ataques de 51%.

Proof of work

- O PoW é um algoritmo de consenso usado em muitas blockchains para validar transações e criar blocos.
- O algoritmo envolve a resolução de problemas criptográficos complexos que exigem um grande poder de processamento sendo projetados de maneira a serem difíceis de resolver, mas fáceis de verificar.
- Os "crypto miners" gastam recursos para resolver o problema e criar um bloco contendo transações recentes. O bloco é adicionado à blockchain e validado por outros nós da rede.
- O algoritmo é seguro contra a modificação ou criação de blocos fraudulentos, mas tem desvantagens: é dispendioso em energia, o que faz levantar preocupações ambientais e barreiras à adoção; além disso, pode ter problemas de escalabilidade, com tempos de transação mais longos e taxas mais altas em blockchains com muitas transações.

Proof of Stake

- O PoS é um algoritmo de consenso utilizado em blockchains que difere do PoW na validação de transações e criação de novos blocos.
- No algoritmo os participantes da rede (chamados de stakeholders) bloqueiam uma determinada quantidade de sua criptomoeda como garantia para se tornarem elegíveis a validar transações e criar blocos.
- Os stakeholders são selecionados aleatoriamente para validar transações com base na sua participação na rede, ao invés de competir para resolver problemas criptográficos.
- Para garantir a segurança e integridade da rede, stakeholders são incentivados a agir honestamente e seguir as regras da blockchain. Caso sejam apanhados a fazer algo desonesto, sua garantia pode ser confiscada. Quando um stakeholder cria um bloco, ele é recompensado com um valor da criptomoeda ou taxa de transação proporcional à quantidade de moedas que o validador bloqueou como garantia.

Setor financeiro

- A tecnologia blockchain permite que as transações financeiras sejam executadas diretamente entre as partes, sem a necessidade de intermediários como bancos ou outras instituições financeiras. Isso reduz os custos e aumenta a velocidade das transações.
- A blockchain aumenta a transparência e a segurança das transações financeiras, uma vez que as transações são registadas numa rede descentralizada e imutável. Isso dificulta que alguém adultere ou manipule as transações.
- A tecnologia blockchain pode ser usada para melhorar a eficiência e a segurança do processo de verificação de identidade. As informações de identidade podem ser armazenadas numa blockchain dificultando o acesso ou manipulação de informação ilegal para hackers. Isso pode ajudar a reduzir o risco de roubo de identidade e fraude financeira.
- A blockchain também pode ser usada para criar produtos financeiros, como criptomoedas e tokens, que podem ser negociados na blockchain, permitindo a criação de novos mercados financeiros.

Setor da saúde

- A blockchain pode ser usada para criar uma rede segura e descentralizada onde as informações médicas dos pacientes podem ser compartilhadas de forma transparente e confiável. Isto pode reduzir significativamente os erros médicos, melhorar a precisão do diagnóstico e acelerar o processo de tratamento.
- A blockchain também pode ser usada para ter acesso ao histórico médico de um paciente, permitindo que os profissionais de saúde acessem facilmente informações importantes, como alergias, doenças crónicas e medicamentos prescritos. Isso pode ajudar os médicos a fornecer tratamentos personalizados e mais eficazes aos pacientes.
- No entanto, a implementação bem-sucedida da tecnologia blockchain na área da saúde requer a colaboração e coordenação de vários interessados, incluindo pacientes, provedores de saúde, autoridades reguladoras e empresas de tecnologia

Sistema eleitoral

- Atualmente o processo de eleição usando votações manuais apresentam algumas debilidades tais como possíveis erros e atrasos na contagem dos votos e a segurança que pode levar a uma fraude dos resultados.
- Com a tecnologia blockchain, seria possível a criação duma plataforma online, onde os votos seriam criptografados e registados de forma imutável, o que levaria a um processo mais transparente e confiável, tal como uma maior eficiência na contagem dos votos.
- A plataforma permitiria um sistema de registo único e verificação de votos usando a criptografia e a tecnologia blockchain que ajudaria a combater possíveis tentativas de fraude

Futuro

- A tecnologia blockchain está a atrair atenção de empresas e governos em todo o mundo devido à sua capacidade de criar registos seguros e imutáveis.
- Uma das principais tendências é a melhoria da escalabilidade porém já estão a ser trabalhadas soluções como a implementação de redes de camada 2.
- A blockchain está a ser aplicada em setores além das criptomoedas, como logística, identidade digital, votação eletrónica e propriedade intelectual.
- A segurança é uma preocupação importante, exigindo melhorias em técnicas de segurança e criptografia.
- A questão da regulamentação é um desafio que precisa ser enfrentado, equilibrando a necessidade de regulamentação com a descentralização e a privacidade.
- O futuro da tecnologia blockchain é promissor e cheio de possibilidades, podendo transformar diversos setores da economia e mudar a forma como lidamos com a informação e o valor.