**BlockChain – Conceitos Gerais**

**TÓPICO 2.1: Basics - BlockChain**

**- LEDGERS -** A função geral dos livros contábeis pode não ter mudado muito, mas a forma como eles cumprem

sua função mudou bastante. Agora, os livros contábeis são frequentemente aplicativos com um banco de dados por trás deles. Um aplicativo cliente se conecta ao banco de dados principal, lê os dados atuais e envia atualizações. No entanto,isso está sujeito a adulteração ou perda de dados.

Com acesso direto ao arquivo de origem, o arquivo pode ser editado e trocado, e o usuário final pode nunca perceber.

**- DISTRIBUTED LEDGERS** - Os livros-razão distribuídos aproveitam as vantagens dos livros-razão tradicionais ou gerais e os tornam mais resilientes. Em vez de ter uma única cópia dos dados mestres, um livro-razão distribuído compartilha o conjunto completo de dados entre vários participantes (membros) da rede; cada membro possui uma cópia completa dos dados.

Isto tem vários benefícios. Nenhum ponto possui o arquivo de dados mestre, portanto nenhum ponto pode corromper o arquivo de dados mestre.

Se você perder um dos pontos finais, os demais pontos finais ainda manterão todos os dados. E quando alguém tenta fazer uma atualização nos dados de um livro-razão distribuído, todos os outros pontos finais estão envolvidos no processo de aceitação ou rejeição da atualização. Em um livro-razão distribuído, quaisquer atualizações devem ser acordadas pelos outros – o que torna muito difícil hackear.

**- BLOCKCHAIN -** Blockchain é um livro-razão distribuído que adiciona imutabilidade.

Imutabilidade significa que uma vez que algo é escrito, não pode ser editado ou removido.

Com o blockchain, os dados não podem ser modificados. O histórico completo dos dados pode ser rastreado até o início do blockchain.

Blockchain é uma cadeia de transações, contida em blocos, daí o nome blockchain.

- O distributed ledger e o blockchain compartilham muitas características.

Um diferencial importante entre os dois é a imutabilidade do blockchain.

- Nesta lição, você aprendeu que um exemplo bem conhecido de tecnologia blockchain é a criptomoeda Bitcoin.

Você também aprendeu que os livros-razão distribuídos (distributed ledgers) ampliam os recursos do livro-razão

tradicional (ledgers), compartilhando dados com diversas partes, e que o blockchain é um tipo de livro-razão

distribuído. Finalmente, você aprendeu como a tecnologia blockchain está sendo aproveitada em vários setores.

**- DESCENTRALIZAÇÃO** -> A descentralização significa que cada membro de uma blockchain possui uma cópia completa dos dados.

Cada membro que possui uma cópia dos dados protege contra maus atores, melhora a recuperação de desastres e promove alta disponibilidade

A descentralização significa que cada membro tem uma cópia completa de todas as informações, proporcionando alta disponibilidade,

recuperação rápida e proteção contra malfeitores.

**- TRANSPARENCIA** -> Outra peça do blockchain que aumenta a confiança é a transparência.

Transparência significa que as informações armazenadas na blockchain são visíveis para os membros da blockchain.

O Blockchain mantém um registro completo de todas as transações, e esse registro está disponível para todos os membros,

tornando o blockchain uma tecnologia muito transparente.

A transparência ajuda a construir confiança porque todos os envolvidos no blockchain podem ver o histórico.

**- IMUTABILIDADE** -> Imutabilidade significa simplesmente que algo não pode ser editado ou alterado. Você pode atualizar as informações em um blockchain adicionando dados, que serão adicionados em um novo bloco.

No entanto, uma vez que um bloco faz parte da cadeia, as informações desse bloco não podem ser alteradas. Ela gera confiança

Lembre-se de que a imutabilidade era uma diferença fundamental entre o blockchain e o livro-razão distribuído.

Que benefício a imutabilidade oferece ao blockchain em relação ao livro-razão distribuído?

Depois que as informações são inseridas em um blockchain, elas não podem ser editadas ou apagadas.

A imutabilidade trabalha com transparência para construir ainda mais confiança.

A incapacidade de uma blockchain ser editada retroativamente significa que os dados são exatamente o que foram inseridos inicialmente.

**- AUDITABILIDADE** -> A auditabilidade é outro benefício do uso do blockchain. A auditabilidade refere-se ao quão prontamente disponível e acessível algo está para auditar. O Blockchain, contando com os demais benefícios já discutidos, é uma plataforma bastante auditável.

A auditabilidade do blockchain aproveita os outros benefícios. Um auditor possui um registro de auditoria completo para cada interação

com os dados em um blockchain. Eles também podem comparar os dados de diferentes membros para verificar a autenticidade dos dados.

**Blocos** - Os blocos são a unidade básica de informação no blockchain.

Lembre-se de que um conjunto de transações resulta na criação de um novo bloco e adicionado ao blockchain após o bloco anterior.

***Transaction Data****: Os dados da transação são as informações reais relevantes para o blockchain. As informações contidas dependerão em grande parte do propósito da transação e do blockchain. Blockchains financeiros podem ver um acréscimo de fundos. Os blockchains da cadeia de suprimentos podem fazer com que um item mude de custódia em um ponto de envio.*

*Blockchains de informações de saúde podem ver informações relacionadas a uma consulta médica. Independentemente do tipo de blockchain, todos os blocos também conterão metadados sobre a transação.*

***Criptographic Hash****: Um bloco também contém um hash criptográfico do bloco anterior na blockchain. Um hash criptográfico é uma sequência única de caracteres que só pode ser criada usando as informações do bloco e a chave cifrada. O hash é único, de modo que nenhum outro bloco, combinado com a chave, produziria o mesmo hash. Adicionalmente, se algum dos dados fosse alterado no bloco, o hash também mudaria. Este processo de criação de um hash criptográfico do bloco anterior está relacionado à imutabilidade do blockchain.*

*Como o hash criptográfico é exclusivo das informações exatas que estavam no bloco anterior quando o hash foi criado, qualquer tentativa de modificar as informações do bloco anterior faria com que o hash mudasse. Essa reação acontece para cada bloco do blockchain.*

*Por exemplo, suponha que alguém tente modificar o primeiro bloco em uma blockchain de quatro blocos. O quarto bloco possui um hash criptográfico dos dados do terceiro bloco.*

*O terceiro bloco possui um hash para o segundo. E o segundo bloco tem um hash para o primeiro. Ao modificar os dados no primeiro bloco, o hash criptográfico no segundo bloco mudaria. Essa alteração de dados no segundo bloco causaria uma alteração no hash criptográfico no terceiro bloco.*

*A alteração dos dados no terceiro bloco alteraria o hash contido no quarto bloco.*

*Ao usar hashes criptográficos para o bloco anterior como parte do conjunto de dados de um novo bloco, o blockchain torna quase impossível fazer uma alteração indetectável nos dados que já estão gravados na cadeia.*

***TimeStamp****:* *A terceira informação em um bloco em uma blockchain é um carimbo de data/hora. Os carimbos de data e hora servem a dois propósitos. O propósito óbvio de um carimbo de data/hora é saber quando um bloco foi adicionado ao blockchain. Devido ao carimbo de data/hora fazer parte de um bloco, o hash criptográfico já discutido irá variar de acordo com o carimbo de data/hora.*

*Isso significa que tentar enviar um bloco editado com um carimbo de data/hora modificado enfrentará o mesmo problema com a alteração de hashes e, em última análise, será rejeitado pelo blockchain.*

*Um segundo propósito do timestamp é mostrar que os blocos estão em ordem cronológica de criação. Isto é importante para a auditabilidade do blockchain, porque garante que qualquer auditoria possa validar as informações do pedido anexadas ao blockchain.*

**Peer-to-peer network** - Rede ponto a ponto

O uso de uma rede ponto a ponto ajuda a tornar o blockchain tolerante a falhas, transparente e distribuído.

**Consensus Mechanisms** - Mecanismos de consenso

A imutabilidade das blockchains está diretamente relacionada aos mecanismos de consenso. Um mecanismo de consenso é um conjunto de regras implementadas pela blockchain que determina como todos os membros reconhecem uma adição de bloco válida.

Os mecanismos de consenso são como cada membro de uma blockchain sabe que a informação que está recebendo é válida. Sem um mecanismo de consenso, qualquer pessoa poderia enviar uma atualização ao blockchain e a cadeia seria atualizada.

Finalmente, os mecanismos de consenso permitem a natureza distribuída da blockchain. Através dos mecanismos de consenso, os peers são capazes de compartilhar atualizações no blockchain e garantir que todos na rede peer-to-peer estejam usando o mesmo conjunto de dados. Os tipos de mecanismo são: Proof of work, proof of stage

O proof of work, A prova de trabalho é um mecanismo de consenso no qual os membros resolvem quebra-cabeças matemáticos. O primeiro membro a resolver o quebra-cabeça é confiável e é capaz de criar o próximo bloco no blockchain. Este mecanismo de consenso prioriza o membro que se esforça mais para resolver um quebra-cabeça para determinar quem escreve o próximo bloco. Embora seja uma prova de trabalho blockchain dá a cada membro uma oportunidade igual para criar o próximo bloco, pode ser muito intensivo em processos (e, portanto, intensivo em energia).

Já o proof of stage, Num mecanismo de prova de participação, quanto mais criptomoeda um membro tiver, maior confiança será dada a esse membro. Com esse aumento de confiança, aumenta a probabilidade de ser o membro que cria o próximo bloco no blockchain. A prova de aposta consome muito menos recursos do que a prova de trabalho. No entanto, a prova de aposta não trata todos os membros igualmente. Em vez disso, concentra-se em quais membros têm mais moedas.

**Smart Contract** - Contratos inteligentes:

Outro conceito central do blockchain é um contrato inteligente. Um contrato inteligente é um contrato executado sem qualquer ação adicional exigida por terceiros. Com um contrato inteligente, você estabelece os termos e condições do contrato. Assim que os termos e condições do contrato forem cumpridos no blockchain, o contrato é executado automaticamente – sem que você precise realizar nenhuma ação.

**Blockchain types** – tipos de Blockchain:

Existem três tipos principais de blockchains: permissionless, permissioned, and consortium. O tipo de blockchain determinará quão amplamente o blockchain será compartilhado e quem terá a capacidade de fazer atualizações no blockchain

* Um **blockchain sem permissão (permissionless)**, também conhecido como blockchain público, é um blockchain aberto. Todas as informações em um blockchain sem permissão podem ser visualizadas por todos os membros, e todos os membros têm o mesmo poder de fazer atualizações no blockchain. Como um blockchain sem permissão é público, qualquer pessoa pode se tornar membro do blockchain, leia as informações e contribua. Um blockchain sem permissão é ótimo para colaboração ampla e irrestrita. No entanto, ele tem o mínimo de controle sobre quem pode ver quais informações.
* Um **blockchain permitido ou privado(permissioned),** é um blockchain no qual a adesão é controlada por uma autoridade central. Apesar de ter uma autoridade central que determina quem está autorizado a ser membro da blockchain e fazer atualizações, o princípio descentralizado da blockchain ainda se aplica. Um blockchain permitido permite aproveitar o poder do blockchain e, ao mesmo tempo, manter informações relevantes protegidas da visão pública. Um blockchain permitido também permite controlar quem é elegível para ser membro do blockchain.
* Um **blockchain de consórcio(consortium),** é um meio termo entre sem permissão e com permissão. Um blockchain de consórcio ainda restringe o acesso ao blockchain, mas possui uma autoridade central mais distribuída. Isso permite um conjunto maior de membros do que um blockchain permitido, ao mesmo tempo que protege as informações da disponibilidade do público em geral. Um exemplo de blockchain de consórcio pode ser se você fizer parceria com duas outras empresas. Cada empresa seria capaz de controlar quem, de sua organização, são membros do blockchain. Isto alavanca uma maior colaboração e partilha do que se cada empresa estabelecesse a sua própria blockchain privada, sem transparência para os outros parceiros. No entanto,mesmo com o aumento do compartilhamento, o blockchain do consórcio ainda mantém suas informações e as de seus parceiros restritas apenas àqueles que fazem parte do blockchain.

Nesta lição, você explorou os benefícios e as relações do blockchain e seus conceitos principais.

Você aprendeu que os mecanismos de consenso permitem que os membros saibam que um novo bloco é válido. Os mecanismos de consenso também permitem que os membros saibam como criar blocos válidos para distribuir pela blockchain.

Você também aprendeu como o hash criptográfico aumenta muito a imutabilidade do blockchain e protege contra a edição de um bloco anterior no blockchain.

A lição terminou com uma discussão sobre os diferentes tipos de blockchains,

e cobriu alguns dos benefícios dos blockchains públicos e privados e como um blockchain de consórcio poderia trazer benefícios de ambos.

O que é uma blockchain framework?

Uma estrutura de blockchain é o conjunto de padrões nos quais um blockchain opera. Pense em uma estrutura como um software empresarial. O software empresarial tem um propósito geral para o qual foi projetado, um conjunto de requisitos para ajudá-lo a operar com eficiência e um conjunto de diretrizes sobre como interagir com ele.

Algumas considerações importantes ao escolher uma estrutura blockchain são:

* + Seu caso de uso específico
  + Mecanismos de consenso disponíveis e seus benefícios e desafios
  + Fácil de usar
  + A comunidade de desenvolvedores
  + Requisitos de licenciamento
  + Maturidade da estrutura blockchain
  + Roteiro futuro da estrutura blockchain

Duas estruturas de blockchain populares são Ethereum e Hyperledger Fabric.

***Ethereum:***

Ethereum é um blockchain de criptomoeda público ou sem permissão que fornece um amplo conjunto de recursos para usar contratos inteligentes, executar aplicativos e executar código. Ethereum atualmente opera com um mecanismo de consenso de prova de trabalho. Ethereum 2.0 pretende usar um mecanismo de consenso de prova de participação, reduzindo a intensidade da computação, mas priorizando membros com mais moedas (ou Ether).

***Hyperledger Fabric:***

Hyperledger Fabric é uma estrutura de blockchain modular, autorizada (ou privada), focada no compartilhamento de informações com a segurança e a confiança do blockchain, mas mantendo a privacidade quando necessário. Se você se lembra do módulo Benefícios do Blockchain, o Hyperledger Fabric oferece suporte a canais. Com canais, você pode controlar quais informações em um blockchain são visíveis para diferentes pares.

Resumo

O blockchain framework é um pacote de soluções de software para blockchain. Ele vem com funções comumente usadas, módulos básicos, pacotes de código repetíveis e assim por diante. Também possui os padrões para simplificar o desenvolvimento, implantação e manutenção da solução blockchain.

A estrutura determinará quais mecanismos de consenso estão disponíveis; se o blockchain suporta cadeias privadas, públicas ou de consórcio; e como as informações nos blocos são compartilhadas na rede blockchain.

**Barreiras para configurar blockchain**

Existem diferentes barreiras ao configurar uma rede blockchain. Os desafios que você deve considerar incluem configurar a rede real, garantir que sua rede seja capaz de escalar, gerenciar custos e manter a rede segura são todos desafios que você deve considerar.

**Estabelecendo a rede (network)**

Para estabelecer uma rede blockchain, você precisa decidir sobre uma estrutura blockchain e então configurar a blockchain. Dependendo da estrutura blockchain usada, você pode ter que decidir sobre seus mecanismos de consenso e colocá-los em funcionamento, configurar a rede para acesso privado ou público, determinar como novos membros ingressam e saem do grupo e assim por diante. Tudo isso deve ser feito e ao mesmo tempo garantir que você tenha o poder de computação para fazer o blockchain decolar e funcionar.

**Dimensionando sua rede**

Quando a rede blockchain estiver instalada e funcionando, você precisa ter certeza de que ela poderá continuar a crescer. O dimensionamento do blockchain vem em duas variedades: dimensionamento do número de membros ou dimensionamento do poder de processamento dos membros. A capacidade de dimensionar seu blockchain é crucial para manter ou até mesmo melhorar sua taxa de transação (a taxa na qual as transações no blockchain são processadas).

---

***Resumo da lição***

A manutenção de uma rede blockchain envolve diferentes barreiras a serem superadas, desde os primeiros passos de escolha de sua estrutura de blockchain, criação de seu primeiro bloco e estabelecimento da rede.

Depois que a rede estiver estabelecida, você precisará descobrir como lidar com o dimensionamento da rede, ambos adicionando membros ou adicionando poder de computação adicional.

Com a escalabilidade do blockchain vêm custos potencialmente crescentes. Ter um mecanismo para compartilhar de forma justa os custos de manutenção de uma blockchain entre os participantes pode diminuir a carga sobre uma única entidade e ajudar a distribuir melhor a carga.

Finalmente, ter uma rede blockchain segura significa ser capaz de controlar quem está ingressando na sua rede privada ou de consórcio. Com todas essas preocupações em mente, é hora de passar para o próximo módulo.

***Introdução ao Blockchain Gerenciado (Managed Blockchain)***

O Managed Blockchain coloca a descentralização e a imutabilidade do blockchain ao seu alcance. O Blockchain gerenciado permite que você crie um blockchain rapidamente, usando a confiabilidade e a escalabilidade da Nuvem AWS. O Managed Blockchain oferece resiliência, escalabilidade, e otimização de custos da Nuvem AWS, ao mesmo tempo que oferece controle total sobre seu aplicativo blockchain.

O Managed Blockchain oferece suporte a duas estruturas populares de blockchain:

* **Hyperledger Fabric** é um blockchain permitido que é adequado para uma situação em que você precisa de controles rígidos de privacidade e segurança com um grupo conhecido de membros. O Hyperledger Fabric também oferece a capacidade de criar canais, compartilhar informações apenas com os membros que precisam ter visibilidade dos dados.
* **Ethereum** é um blockchain sem permissão que é adequado quando é necessário um blockchain altamente distribuído e com total transparência. Como um blockchain público, todos os membros do blockchain podem ver todos os dados nos blocos.

O Managed Blockchain disponibiliza essas duas estruturas para você em uma solução totalmente gerenciada. Isso significa que você pode se concentrar em seu blockchain e deixar que a AWS se preocupe em manter o hardware, a segurança e a rede necessários para manter o blockchain em funcionamento.

Você pode usar o console, a AWS CLI e APIs para interagir com sua rede blockchain.

***Resumo da lição***

O Managed Blockchain resolve muitas das preocupações ou problemas com a configuração de uma rede blockchain. O Managed Blockchain é simples de configurar, pode ser dimensionado a qualquer momento e aproveita o AWS KMS para manter sua rede segura na nuvem.

**Outros usos do blockchain**

A imutabilidade, a natureza distribuída e a transparência do Blockchain oferecem benefícios que vão muito além da criptomoeda. De aplicações de saúde ao governo, e da agricultura às finanças, o blockchain está apenas começando a ser explorado e ainda não está perto de todo o seu potencial.

**Assistência médica (healthcare)**

Blockchain na área da saúde tem vários cenários de uso potencial. Considere os registros de atendimento ao paciente. A criação de um blockchain do Hyperledger Fabric com canais permitiria que todos os provedores compartilhassem informações dos pacientes com segurança e confiança. Cada visita ao consultório ou hospital seria documentada em um arquivo imutável.

Cada provedor poderia ver quais notas foram inseridas anteriormente, quando foram inseridas e quem as inseriu. Os provedores também poderiam revisar quaisquer atualizações anteriores do registro de saúde. Sabendo que ninguém pode apagar informações sem registrá-las, o prestador e o hospital também têm uma maior confiança na integridade do registo de saúde.

**Governo**

-O governo é uma área com maior potencial para adoção e uso de blockchain. No setor governamental, tudo, desde votação até compras, impostos e saúde pública, tem potencial de blockchain.

**Agricultura**

-Conforme discutido anteriormente neste treinamento, a agricultura é uma indústria natural para blockchain. A capacidade de rastrear um item desde a fazenda onde foi colhido até o destino final dá aos consumidores maior confiança na maneira e no método como os itens são colhidos.

**Finanças e comércio**

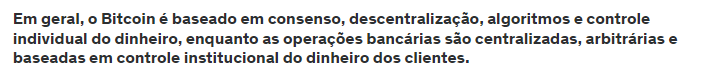
-Finanças e comércio são outro segmento com amplo potencial para a adoção do blockchain à medida que a tecnologia amadurece. A descentralização e a imutabilidade do blockchain tornam-no uma combinação ideal para transações financeiras e comerciais.

***Resumo da lição***

À medida que a blockchain evolui, o seu impacto irá abranger todos os setores. Alguns setores já estão se envolvendo no blockchain para ver como podem expandir o uso além do foco inicial na criptomoeda. A natureza inerente do Blockchain – imutável, transparente e descentralizada – o torna bem posicionado para ajudar a resolver problemas de negócios em um ambiente cada vez mais dinâmico, mudando o mundo do comércio eletrônico.

BITCOIN E CRIPTOGRAFIA

Tabela

Descrição gerada automaticamente 

1. Para que servem assinaturas digitais?

As assinaturas digitais são uma forma autenticar documentos virtualmente.

1. Que propriedades queremos para uma assinatura digital?

Impossível de falsificar, fácil de verificar e atrelada ao documento.

1. Qual a função da chave secreta?

A chave secreta permite a geração de assinaturas digitais, em conjunto com o documento a ser assinado.

1. Qual a função da chave pública?

Tendo a chave pública da pessoa que assinou, a assinatura e o documento virtual assinado, qualquer um pode verificar se a assinatura digital é autêntica.

1. Quais características a CentralCoin tem em comum com o Bitcoin? a. Praticamente tudo. A única diferença é que na CentralCoin existe uma autoridade central que verifica as transações e mantém a blockchain, enquanto no Bitcoin isto é feito em uma rede descentralizada.
2. Quais informações ficam armazenadas na blockchain da CentralCoin? c. Transações de criação e de transferência de moedas CentralCoins.
3. Como funciona a transação de transferência de moedas? c. O usuário precisa indicar que possui saldo suficiente em sua carteira. Essas moedas são alteradas para refletir o novo proprietário.
4. O que o Banco Central verifica em cada transação de transferência? c. A autenticidade da assinatura digital utilizada, se a soma das moedas consumidas é maior do que as moedas criadas e se o usuário de fato tem a posse das moedas utilizadas.

Para Pensar: O banco central sabe o saldo na CentralCoin mantendo um registro interno de todas as transações de criação e transferência de moedas. Ele verifica essas transações sempre que uma transferência é solicitada, garantindo que o usuário tenha saldo suficiente para a transação.

1. Quais as características da rede Bitcoin? b. Distribuída, sem hierarquia, segue um protocolo de consenso.
2. O que é um nó da rede Bitcoin? É um computador que esteja conectado a rede bitcoin
3. O que diferencia um full node de um lite node? O full node em geral, armazena toda blockchain e é capaz de operar independente
4. Como a blockchain garante consenso na rede Bitcoin? e. As transações de Bitcoin só se tornam efetivas quando são inseridas na blockchain, e a mineração garante que todos os nós mantenham a mesma blockchain armazenada.
5. O que é um nonce e qual a função dele? e. O nonce é um valor numérico sem significado que é adicionado a cada bloco da blockchain. Os mineradores alteram o valor do nonce tentando cumprir com o requisito do proof of work.
6. O que dá ao minerador o direito de adicionar o próximo bloco da cadeia? a. Conseguir criar um bloco cujo hash tenha um determinado número de zeros.
7. De onde surgiram os Bitcoins em circulação? c. Todos os Bitcoins em circulação surgiram da mineração. A cada quatro anos, o número de Bitcoins criados a cada novo bloco é reduzido pela metade.
8. O que são mining pools? b. São esquemas cooperativos entre mineradores, em que todos trabalham tentando montar blocos, e os Bitcoins auferidos são distribuídos entre todos os participantes de acordo com o trabalho computacional de cada um.

Para Pensar: Com menos mineradores no futuro, a velocidade de criação de novos blocos pode diminuir, o que pode resultar em uma redução na velocidade de confirmação de transações e, potencialmente, em custos de transação mais elevados durante períodos de congestionamento da rede. Isso pode afetar a eficiência e a escalabilidade da rede Bitcoin.

1. Para que serve a mineração? b. A mineração impede o gasto duplo no sistema Bitcoin.
2. O que é gasto duplo? a. É, literalmente, gastar a mesma moeda Bitcoin duas vezes.
3. O que acontece se há uma bifurcação na blockchain? d. Enquanto os dois ramos tiverem o mesmo tamanho, alguns mineradores vão trabalhar em um ramo e outros, no outro. Assim que um minerador consegue estender um desses ramos, ele passa a ser o ramo mais longo, e portanto todos os mineradores passam a trabalhar nesse ramo. O outro bloco da bifurcação é esquecido.
4. Como um hacker pode explorar uma bifurcação na cadeia para enriquecer? d. Ele pode pagar alguém, receber o que comprou, e então criar uma bifurcação imediatamente antes do bloco em que estava o pagamento que fez. Se ele for capaz de fazer com que a nova bifurcação seja adotada, o pagamento contido no primeiro bloco será esquecido, e ele poderá gastar o mesmo dinheiro novamente.

Para Pensar: Se um hacker conseguir 51% do hash power, ele teria controle suficiente sobre a rede para realizar ataques, como gasto duplo e bifurcações maliciosas. Isso comprometeria a segurança e a confiança na rede Bitcoin, pois ele poderia alterar transações passadas, reverter transações recentes e, essencialmente, assumir o controle da blockchain. Isso seria prejudicial para a integridade e a confiabilidade da rede como um todo.

Revisão

* A blockchain é um registro público e imutável de todas as transações já realizadas desde a criação do bitcoin
* Identidade : Chave Pública
* Segurança: assinaturas digitais e chave secreta
* Rede peer-to-peer e protocolo de consenso novos blocos
* Mineradores: criam novos blocos com as novas transações válidas. Competem pelo direito de adicionar o próximo bloco à cadeia através de proof of work, recebem novos bitcoins como recompensa

O que é um “saldo” em bitcoins? a. É a soma de todas as moedas que foram criadas e destinadas às chaves públicas que você controla, e que você ainda não destruiu para fazer transações.

 Como o sistema de assinaturas digitais é usado para dar segurança às transações? b. Todas as transações precisam ser assinadas digitalmente. Somente quem controla a chave secreta atrelada à chave pública que está fazendo a transferência é capaz de criar a assinatura digital.

 Cite um motivo para se ter mais de um par de chaves públicas/secretas? d. Para evitar perder todos os seus Bitcoins caso você perca ou tenha uma chave secreta roubada.

 O que significa a “posse” de determinada quantidade de moedas? a. Significa saber qual a chave secreta associada com a chave pública para a qual essas moedas foram destinadas

Para Pensar: Sem uma agência central, a validade dos pares de chaves públicas e secretas é garantida pela criptografia e pela verificação descentralizada realizada pelos nós da rede Bitcoin. Cada transação é verificada pelos mineradores, que garantem que apenas transações autênticas, assinadas digitalmente com chaves válidas, sejam aceitas na blockchain. Isso garante a integridade e a segurança das transações sem a necessidade de uma autoridade central.

1. Quais são as características desejadas para uma carteira? Disponibilidade, segurança e conveniência
2. O que acontece se eu perder as informações contidas em minha carteira de papel? d. Se você não tiver essa informação em outro lugar, será impossível recuperar seus Bitcoins.
3. Quais as vantagens de uma carteira de hardware e quando é recomendável usá-la? e. É a carteira mais segura e permite a recuperação dos Bitcoins em caso de perda. Por ser relativamente cara, é recomendada para quem pretende utilizar quantidades significativas de Bitcoin.
4. Quão seguras são as carteiras de software? d. Tão seguras quanto o computador/smartphone do usuário.

Para pensar:

Os hackers que invadem servidores de carteiras online visam roubar as chaves privadas dos usuários armazenadas nesses servidores. Com essas informações, podem transferir os Bitcoins dos usuários para suas próprias carteiras, realizar gastos duplos ou outras atividades maliciosas que comprometem os fundos dos usuários. Isso ocorre porque as chaves privadas concedem acesso direto aos Bitcoins de um usuário.

Parte superior do formulário

1. Como funcionam as exchanges? a. As exchanges conectam pessoas interessadas em comprar com pessoas interessadas em vender Bitcoin, cobrando uma pequena taxa para isso.
2. Na prática, como são comprados e vendidos Bitcoins? b. Em websites. As pessoas depositam dinheiro e Bitcoins na conta e chave pública da exchange, respectivamente, trocam dinheiro por bitcoins, e então requisitam que a exchange deposite o resultado da troca em alguma conta/chave pública fornecida.
3. Como a falta de regulamentação aumenta os riscos das exchanges? e. Não existe nenhum tipo de controle sobre os seus Bitcoins ou seu dinheiro sob custódia da exchange
4. Por que manter dinheiro na exchange é arriscado? e. Todas estão corretas. c. Por acumularem um grande volume de Bitcoins, estes websites são alvos frequentes de hackers.

Para pensar:

Para identificar esquemas de pirâmide, é essencial estar atento a sinais de alerta, como promessas de retornos financeiros exagerados e rápidos, recrutamento constante de novos participantes sem foco em produtos ou serviços genuínos, falta de transparência sobre a fonte real dos ganhos e uma estrutura que depende fortemente do recrutamento contínuo para sustentar os retornos dos participantes antigos. Além disso, a falta de uma base sólida e sustentável pode levar a colapsos repentinos, causando perdas significativas para os participantes mais recentes.

1. O Bitcoin é verdadeiramente anônimo?b. Não exatamente, pois é possível rastrear transações dentro do Bitcoin.
2. Se alguém conseguir associar sua identidade com sua chave pública, quais as consequências? d. A pessoa poderá rastrear todas as suas movimentações de Bitcoins associados a essa chave pública.
3. Como é possível descobrir a identidade por trás de uma chave pública? e. Todas estão corretas.
4. Por que é importante manter o anonimato no Bitcoin? e. Porque uma vez perdido o anonimato, todas as suas movimentações, assim como a quantidade de Bitcoin em sua posse, serão públicos.

Para pensar: Sim, existem situações legítimas em que o Bitcoin pode funcionar melhor do que o sistema bancário tradicional. Por exemplo, em transações internacionais, o Bitcoin pode ser mais rápido e mais barato do que os métodos convencionais de transferência de dinheiro, especialmente em países onde o acesso aos serviços bancários é limitado. Além disso, para pessoas que desejam evitar a burocracia e os controles governamentais sobre suas finanças, o Bitcoin oferece uma alternativa descentralizada e pseudônima.