EXIN Blockchain

FOUNDATION

Certified by EXIN

Exame simulado

Edição 202202

Conteúdo

Introdução

Este é o exame simulado EXIN Blockchain Foundation (BLOCKCHAINF.PR). As regras e regulamentos do exame do EXIN se aplicam a este exame.

Este exame consiste de 40 questões de múltipla escolha. Cada questão de múltipla escolha possui um certo número de alternativas de resposta, entre as quais apenas uma resposta é a correta.

O número máximo de pontos que pode ser obtido neste exame é 40. Cada resposta correta vale 1 ponto. Você precisa de 26 pontos ou mais para passar no exame.

O tempo permitido para este exame é de 60 minutos.

Boa Sorte!

Exame simulado

1 / 40
Qual é uma vantagem dos blockchains públicos?

A) Não usam terceiros desinteressados para proteger os blocos, pois todos os participantes têm um interesse direto.
B) São mais resistentes às fraudes por usar nós federados para combatê-las.
C) São abertos a todas as pessoas do mundo, sem requisitos de permissão nem de licença.
D) Suas redes são construídas por empresas com fins lucrativos e o funcionamento da rede é garantido.

2 / 40
O que é um blockchain?

A) Um banco de dados centralizado que mantém um subconjunto de todas as transações em todos os nós
B) Um banco de dados cliente-servidor presente em um número limitado de nós ao mesmo tempo
C) Um banco de dados distribuído contendo um registro de todas as transações na rede
D) Um banco de dados autônomo contendo um histórico de todas as transações na rede

3 / 40
Qual é a função de um nó leve em uma rede blockchain?

A) Armazenar o histórico completo de todas as transações da rede
B) Armazenar criptomoedas compradas para todos os usuários de uma rede blockchain
C) Verificar as transações se servindo do trabalho dos nós completos

4 / 40
O que **não** é uma classificação de um tipo de nó?

A) Nó completo
B) Nó leve
C) Nó de Merkle
D) Nó de mineração

5 / 40
Um instrumento ao portador utilizado para transferir valor entre duas partes em uma rede blockchain.

Que instrumento é este?

A) Uma DApp
B) Um hash criptográfico
C) Um nó
D) Um token

6 / 40
Qual é uma característica **chave** dos blockchains públicos?

A) Permitem que um usuário eleja nós para processar as transações.
B) Permitem que qualquer pessoa participe de uma rede blockchain.
C) Permitem o controle sobre quem pode participar e em que nível.
D) Permitem que apenas partes confiáveis operem seu blockchain.

7 / 40
O que é um exemplo de uso da criptografia em um blockchain?

A) Acesso a blockchains privados ou híbridos utilizando uma chave privada
B) Criação de criptomoeda como recompensa para os nós de mineração
C) Proteção de blockchains contra ataques de 51% por parte de nós corruptos
D) Proteção de transferências de criptomoeda entre destinatários

8 / 40
Como os blockchains usam criptografia de chave privada e chave pública?

A) A criptografia assimétrica permite que um emissor transfira criptomoeda para uma chave pública. O destinatário pode então acessar esses fundos com sua chave privada e mantê-la em sua carteira.
B) Na criptografia de chave pública, uma única chave é usada para criptografar e descriptografar a transação. O emissor usa esta chave para enviar criptomoeda, que ficará na carteira do destinatário após a descriptografia.
C) A criptografia simétrica permite que um emissor transfira criptomoeda para um destinatário, que poderá então acessar seus fundos quando o emissor lhe der acesso à sua chave privada.
D) O algoritmo no blockchain criptografa e armazena as chaves privadas e públicas em todas as carteiras do usuário. Em seguida, o usuário acessa os fundos com sua frase de recuperação de vinte palavras.

9 / 40
Como as redes blockchain híbrido combatem os ataques de 51%?

A) Com um controlador central, que garante a segurança de cada nó da rede
B) Com um algoritmo de prova de trabalho (PoW), que permite aos mineradores proteger a rede
C) Com um mecanismo de incentivos para os mineradores, que recebem moeda por proteger a rede
D) Com raízes da árvore de Merkle, que permitem que a rede volte ao seu último bloco válido

10 / 40
Como os blockchains funcionam como registros?

A) Mantendo um histórico de todas as transações já realizadas na rede
B) Mantendo grande quantidade de dados das transações, como um banco de dados centralizado
C) Atualizando periodicamente o blockchain com todos os balanços de todas as carteiras

11 / 40
Qual é a tarefa dos mineradores em uma rede blockchain?

A) Agir como um terceiro único para agregar transações e instaurar confiança na rede por meio da autoridade dos mineradores
B) Na qualidade de computadores, permitir o acesso à blockchain, garantindo que a quantidade de nós corruptos permaneça baixa
C) Na qualidade de nós, competir por uma recompensa ao calcular o nonce criptográfico correto para possibilitar a transação
D) Definir as regras de consenso que devem ser seguidas e intervir quando essas regras não são cumpridas

12 / 40
Que descrição se aplica **apenas** ao algoritmo de consenso de prova de trabalho (PoW)?

A) Um algoritmo de consenso colaborativo em que as contas aprovadas realizam a validação.
B) Um algoritmo de consenso colaborativo facilitado por mineradores (farmers), que disponibilizam a memória não utilizada de seus computadores para viabilizar as transações.
C) Um algoritmo de consenso em que a validação é realizada para o fluxo inteiro de transações, incluindo tanto a exatidão dos dados quanto a sequência das transações.
D) Um algoritmo rápido e de baixo custo em que um nó necessita depositar criptomoeda para garantir a transação.
E) Um algoritmo de consenso não competitivo em que a validação é realizada pelos nós eleitos, que enviam criptomoeda para um endereço onde ela não pode ser recuperada.
F) Um algoritmo que inclui validação colaborativa, realizada por validadores escolhidos fora do consenso.
G) Um algoritmo que funciona em um ambiente de execução confiável e comprova a hora em que a transação foi realizada.
H) Um algoritmo competitivo intensivo e dispendioso, em que cada nó de mineração do blockchain compete para proteger os blocos.

13 / 40
Um algoritmo de consenso competitivo que foi desenvolvido porque os blockchains tinham dificuldade em atender às exigências de velocidade das transações.

Que algoritmo de consenso é este?

A) Prova de participação delegada (DPoS)
B) Prova de queima
C) Prova de participação (PoS)
D) Prova de trabalho (PoW)

14 / 40
Qual algoritmo de consenso é o **menos** eficiente em termos de energia?

A) Prova de participação delegada (DPoS)
B) Prova de autoridade (PoA)
C) Prova de espaço (PoSpace)
D) Prova de trabalho (PoW)

15 / 40
Qual é uma vantagem de se usar o algoritmo de consenso de prova do tempo decorrido (PoET) em vez de prova de trabalho (PoW)?

A) Em um blockchain sem permissão, é mais fácil utilizar o PoET que o PoW, pois o PoET usa um sistema de loteria seguro para a seleção de nós.
B) Geralmente, o custo da transação é menor no PoET que no PoW, pois o hardware necessário é mais genérico no PoET que no PoW.
C) O PoET é muito mais seguro que o PoW, pois o PoET suporta o ambiente de execução confiável (TEE) ao marcar as transações com carimbo de data/hora.
D) O PoET é geralmente mais rápido que o PoW. Como no PoET a seleção de nós é aleatória, há menos nós que competem por validação que no PoW.

16 / 40
Um hacker tenta corromper o histórico das transações em um blockchain para gastar um token ou uma criptomoeda duas vezes.

O que é **mais** provável que o hacker tenha feito?

A) Mudado a transação em seu nó e então a propagado na rede
B) Editado o contrato inteligente e resgatado criptomoeda do investidor
C) Ganho o controle de mais de 51% da capacidade de processamento da rede
D) Executado um hard fork na rede, criando uma nova rede blockchain

17 / 40
As redes blockchain são vulneráveis aos ataques de 51%.

Qual rede os hackers teriam **mais** interesse de invadir?

A) Bitcoin
B) Fabric
C) Ripple

18 / 40
Uma das maiores ameaças à comunidade blockchain é o narcisismo das pequenas diferenças.

Qual é o resultado deste narcisismo das pequenas diferenças?

A) Uma comunidade ridiculariza uma outra por pequenas diferenças, resultando em uma maior colaboração.
B) A comunidade se preocupa e trabalha para resolver pequenas diferenças que não são percebidas por grupos externos.
C) A comunidade desenvolveu vários projetos similares que brigam por pequenas diferenças.
D) A comunidade fica mais unida e trabalha junto de modo colaborativo para resolver problemas comuns.

19 / 40
Como um golpista usa o esquema Ponzi?

A) Convence as vítimas a pagar para receber algo de maior valor posteriormente.
B) Encontra investidores e em seguida despeja os tokens desses investidores para provocar um colapso financeiro.
C) Paga dividendos aos investidores iniciais usando os fundos dos investidores subsequentes.
D) Rouba cartões de crédito e os usa para adquirir dinheiro, bens ou propriedades.

20 / 40
Qual característica da rede blockchain serve também para protegê-la?

A) Quanto mais nós completos independentes, mais difícil será comprometer os dados no blockchain.
B) Quanto menor a quantidade de mineradores no blockchain, maiores serão os incentivos para proteger a rede.
C) Quanto mais centralizado o controle do blockchain, mais difícil será proteger os dados e evitar fraudes.
D) Quanto mais complicado for o algoritmo de prova de trabalho (PoW), maior será a recompensa para proteger a rede.

21 / 40
Como as informações podem ser protegidas em um blockchain?

A) Usando uma rede ponto a ponto (P2P) fechada que compartilha informações entre plataformas
B) Usando uma distribuição de criptomoedas aos mineradores através da rede
C) Usando criptografia assimétrica, que consiste em uma chave pública e outra privada
D) Usando tecnologia de registro distribuído (DLT), que registra as informações na origem

22 / 40
Como o blockchain usa uma testemunha pública?

A) Um tribunal ou uma biblioteca digitais têm o papel de testemunha pública para armazenar informações de referência.
B) Um nó da rede blockchain atesta a veracidade e a autenticidade da informação.
C) Uma pessoa envia uma transação através de uma rede pública para ser recompensada como uma testemunha pública.
D) Um nó preferencial pode ser eleito para atestar a veracidade e a autenticidade da informação.

23 / 40
O blockchain permite uma identidade auto-soberana.

Como o blockchain faz isso?

A) Permitindo que terceiros centralizados ofereçam informação de identidade válida e fácil de usar
B) Permitindo que cada pessoa tenha um controle exclusivo do seu dinheiro, propriedade e identidade
C) Permitindo que os governos emitam facilmente identidades com certificados digitais avançados
D) Permitindo que apenas empresas de internet ofereçam repositórios de identidade pessoal de excelente segurança

24 / 40
Os blockchains públicos dão um incentivo para encorajar os usuários a minerar blocos e proteger a rede.

Que incentivo é este?

A) Permissão para que os usuários criem tokens para vender em mercados secundários.
B) Nenhum. Não há recompensa porque os blockchains públicos são feitos em software livre.
C) Recompensas em dinheiro pela operação dos nós de mineração.
D) Recompensas em criptomoeda pela mineração.

25 / 40
Uma organização deseja desenvolver contratos inteligentes baseados em tecnologia blockchain, mas não quer que seus funcionários se sobrecarreguem para manter a segurança do blockchain.

Que tipo de blockchain é o **mais** adequado para esta organização?

A) Blockchain híbrido
B) Blockchain privado
C) Blockchain público

26 / 40
Qual é uma característica **chave** da rede Hyperledger?

A) É uma rede blockchain público e uma das mais antigas, existindo desde 2009.
B) É privada, de software livre e pode executar a tecnologia de registro distribuído (DLT) própria de cada participante.
C) Usa criptomoeda como mecanismo de recompensa, o que a torna mais segura.
D) Usa o algoritmo de consenso de prova de participação (PoS) como sua principal medida de segurança.

27 / 40
Qual é o **melhor** caso de uso dos contratos inteligentes?

A) Digitalizar e automatizar contratos juridicamente vinculativos por meio de inteligência artificial (IA)
B) Importar a execução de contratos no sistema legal usando criptomoedas
C) Garantir pagamento automático por ações ou eventos predeterminados nos contratos de seguro
D) Estender um blockchain de Bitcoin, a plataforma mais conhecida de contrato inteligente, ao sistema judiciário

28 / 40
Em qual cenário um contrato inteligente é a **melhor** solução para o problema?

A) Um barman quer forçar os clientes a pagar por suas bebidas com a transferência de criptomoeda para sua carteira.
B) Uma diretora financeira quer receber uma notificação do seu smartwatch quando seu marido chegar em casa.
C) Uma empresa de energia quer comprar automaticamente energia quando os preços atingirem um valor predeterminado.
D) Uma seguradora quer indenizar um fazendeiro sempre que o gerente de caso julgar que é o melhor a ser feito.

29 / 40
Qual é a finalidade das DApps?

A) Executar contratos inteligentes com a lógica de negócios no front-end de uma aplicação independente
B) Apenas gerenciar criptomoedas, sem nenhum sistema de voto incorporado para a governança do blockchain
C) Executar aplicações em uma rede ponto a ponto (P2P), ampliando os contratos inteligentes de forma a ser mais que simples transferência de valores
D) Apoiar as aplicações que funcionam em vários fornecedores de nuvem (cloud) públicos, evitando a dependência tecnológica (lock-in) e fraude

30 / 40
Qual é o papel de uma organização autônoma descentralizada (DAO)?

A) Direcionar o problema do principal-agente, com colaboração e aceitação das ações dentro das regras acordadas
B) Incluir, no sistema judiciário atual, contratos inteligentes online regulamentados usando blockchains públicos
C) Oferecer contratos inteligentes online complexos sem nenhum vínculo com ativos offline tangíveis ou intangíveis
D) Fornecer uma plataforma de contrato de um blockchain privado em que os usuários possam executar suas aplicações online

31 / 40
Qual é a **maior** contribuição da tecnologia blockchain à proteção dos dados de identidade?

A) Eliminação de terceiros por meio do fornecimento de armazenamento de dados seguro em um servidor de usuário
B) Codificação de todos os dados de saúde, que serão salvos em um blockchain privado sem permissão
C) Proteção dos dados que foram enviados na internet por meio de um algoritmo de criptografia
D) Fornecimento de dados pessoais sem revelar os dados reais que comprovam esses dados pessoais

32 / 40
Qual é a vantagem de se usar redes blockchain com a internet das coisas (IoT)?

A) Permitir aos usuários do blockchain monitorar e acessar veículos autônomos
B) Evitar um ataque de falsificação (spoofing) usando a identidade segura armazenada no blockchain
C) Habilitar um software que se autoprograma para resolver problemas sem intervenção humana
D) Resolver cálculos complexos e dispendiosos com o uso de mineração no Hyperledger Fabric

33 / 40
A tecnologia blockchain viabilizou os mercados descentralizados.

Qual é uma vantagem de um mercado descentralizado?

A) É baseado em tecnologia de software livre, então pode ser usado sem nenhum investimento.
B) Sua operação não está sob licença, logo é mais bem gerenciado.
C) É relativamente barato, dado o uso de criptomoeda, e muito acessível.
D) É à prova de falsificações, resistente a tentativas de encerramento e confiável devido aos contratos inteligentes.

34 / 40
Como o blockchain melhora as cadeias de suprimentos?

A) Com a criação automática de acordos comerciais entre as duas partes
B) Com a criação de mercados centralizados seguros para negociar mercadoria
C) Com a estabilização das moedas nacionais dos países envolvidos
D) Com a transferência da propriedade tokenizada por meio de um sistema de software

35 / 40
A Autoridade Monetária de Singapura (MAS) e a empresa de blockchain R3 fizeram uma parceria.

O que realizaram juntas?

A) Criaram contratos inteligentes e moedas estáveis.
B) Simplificaram a transmissão interbancária de mensagens.
C) Possibilitaram os primeiros pagamentos interbancários sem limitações de fuso horário.
D) Lançaram transferências eletrônicas usando criptografia.

36 / 40
O que é uma moeda fiduciária digital?

A) Uma moeda em forma digital que representa as reservas financeiras de um país
B) Uma moeda digital que cria um mercado de dívida transparente e sem fronteiras
C) Um sistema online que permite a realização de transações sem uma conta bancária

37 / 40
Como a tecnologia blockchain beneficia o setor de seguros?

A) Ao evitar requisitos de conformidade das autoridades nacionais, o que reduz as despesas gerais
B) Ao garantir a precisão dos dados e automatizar os microsseguros, o que reduz custos
C) Ao instaurar prêmios flexíveis pagos pelos clientes, o que aumenta o lucro
D) Ao criar um modo de pagamento digital, o que simplifica a regularização dos sinistros

38 / 40
Como a tecnologia blockchain ajuda a proteger os direitos de propriedade intelectual (PI)?

A) Incluir transações de PI em contratos inteligentes
B) Registrar um evento e estabelecer o cronograma
C) Registrar a criação de pacotes de software
D) Enviar uma transação e receber o direito à PI

39 / 40
Qual é um exemplo de um governo promovendo ativamente o uso de blockchain?

A) A China criou um sandbox regulatório que lhe permite monitorar atentamente os experimentos na mineração de blockchain e criar a sua própria criptomoeda.
B) A Estônia oferece um programa de e-Residência, disponível para qualquer pessoa no mundo que tenha interesse em ter um negócio online dentro da União Europeia.
C) A Autoridade Monetária de Singapura (MAS) criou moeda digital do banco central para pagamentos entre bancos por meio da tecnologia de registro distribuído (DLT).

40 / 40
Por que se descreve o blockchain como a tecnologia que acrescenta uma camada de confiança à internet?

A) Por permitir a pessoas e grupos trabalhar juntos sem ter que confiar uns nos outros ou estabelecer autoridade
B) Por criar um túnel VPN dedicado entre duas ou mais partes para realizar transferência de fundos online
C) Por fornecer um mecanismo ao governo para criar a sua própria moeda fiduciária digital em substituição à moeda física
D) Por fornecer autenticação de múltiplos fatores para criar e atualizar registros de transações de criptomoeda de modo seguro

Gabarito de respostas

1 / 40
Qual é uma vantagem dos blockchains públicos?

A) Não usam terceiros desinteressados para proteger os blocos, pois todos os participantes têm um interesse direto.
B) São mais resistentes às fraudes por usar nós federados para combatê-las.
C) São abertos a todas as pessoas do mundo, sem requisitos de permissão nem de licença.
D) Suas redes são construídas por empresas com fins lucrativos e o funcionamento da rede é garantido.

A) Incorreto. Esta é uma vantagem dos nós do blockchain com permissão, que são redes privadas que usam parte da tecnologia blockchain, não em sua totalidade. A maioria não realiza mineração nem possui uma criptomoeda própria. Assim, não há terceiros desinteressados. Os blocos e as transações são processados por participantes identificados.
B) Incorreto. Pode haver nós federados tanto em blockchains públicos quanto em privados. Além do mais, pode haver blockchains públicos sem federação. A federação ocorre quando o sistema, ou melhor, o usuário do sistema, elege nós para processar as transações.
C) Correto. Esta é uma vantagem dos blockchains públicos, que são abertos a qualquer pessoa do mundo para participar das funções da rede. Os únicos limitadores são acesso à internet, hardware e eletricidade. (Literatura: A, Capítulo 1.1)
D) Incorreto. Por definição, blockchains públicos são desenvolvidos em uma licença aberta, como Apache ou licença MIT. Não há mecanismos de bloqueio, solicitação de permissão ou taxa de licenciamento.

2 / 40
O que é um blockchain?

A) Um banco de dados centralizado que mantém um subconjunto de todas as transações em todos os nós
B) Um banco de dados cliente-servidor presente em um número limitado de nós ao mesmo tempo
C) Um banco de dados distribuído contendo um registro de todas as transações na rede
D) Um banco de dados autônomo contendo um histórico de todas as transações na rede

A) Incorreto. O blockchain é um banco de dados descentralizado e distribuído ponto a ponto (P2P), em que todos os nós mantêm um registro de todas as transações.
B) Incorreto. O blockchain consiste em bancos de dados distribuídos P2P.
C) Correto. É um banco de dados distribuído P2P com carimbo de data/hora que mantém um registro de todas as transações que já ocorreram na rede. (Literatura: A, Capítulo 1.1)
D) Incorreto. O blockchain é um banco de dados descentralizado e distribuído P2P, contendo o histórico de todas as transações.

3 / 40
Qual é a função de um nó leve em uma rede blockchain?

A) Armazenar o histórico completo de todas as transações da rede
B) Armazenar criptomoedas compradas para todos os usuários de uma rede blockchain
C) Verificar as transações se servindo do trabalho dos nós completos

A) Incorreto. Um nó não necessariamente armazena o histórico completo de todas as transações da rede. Isso só é válido para um nó completo.
B) Incorreto. Um nó não armazena criptomoeda propriamente dita, mas blocos que contêm o histórico de todas as transações.
C) Correto. Os nós leves verificam as transações se servindo do trabalho dos nós completos. (Literatura: A, Capítulo 1.1)

4 / 40
O que **não** é uma classificação de um tipo de nó?

A) Nó completo
B) Nó leve
C) Nó de Merkle
D) Nó de mineração

A) Incorreto. Os nós completos precisam de todos os registros das novas transações. Eles mantêm todos os cabeçalhos dos blocos, que identificam um bloco único e contêm um hash criptográfico do bloco anterior. Todos esses dados se somam e ocupam muito espaço.
B) Incorreto. Os nós leves verificam as transações se servindo do trabalho dos nós completos. Eles apenas baixam os cabeçalhos de todos os blocos e então checam as transações utilizando um sistema conhecido como verificação de pagamento simplificado (SPV).
C) Correto. A raiz da árvore de Merkle não é um tipo de nó, mas um hash criptográfico que permite a um blockchain híbrido voltar ao seu último bloco válido conhecido caso a rede seja atacada. (Literatura: A, Capítulo 1.1)
D) Incorreto. Um minerador é um tipo de nó que adiciona transações a novos blocos. Os mineradores competem para conquistar o direito de criar um novo bloco completo por meio da resolução de um problema matemático complexo. Cada minerador escreverá a sua resposta no cabeçalho do bloco e, caso estiver correta, o minerador será recompensado com criptomoeda.

5 / 40
Um instrumento ao portador utilizado para transferir valor entre duas partes em uma rede blockchain.

Que instrumento é este?

A) Uma DApp
B) Um hash criptográfico
C) Um nó
D) Um token

A) Incorreto. Aplicações descentralizadas (DApps) são aplicações executadas em uma rede ponto a ponto (P2P), não em um único sistema. As DApps são desenvolvidas com contratos inteligentes, porém usam outros serviços, como envio seguro de mensagens, e frequentemente possibilitam a um número ilimitado de participantes interagir sob um dado conjunto de regras.
B) Incorreto. Uma função de hash é utilizada para proteger os dados em um bloco de transações. Um hash criptográfico é a saída de um processo matemático que gera uma sequência de números e letras de tamanho fixo.
C) Incorreto. Um nó é um computador conectado a uma rede blockchain. Ele executa o software para a rede, mantendo-a saudável graças à transferência de informações ao longo da rede para outros nós.
D) Correto. Um token é um instrumento ao portador utilizado para a transferência de valor entre duas partes em uma rede blockchain. (Literatura: A, Capítulo 1.1)

6 / 40
Qual é uma característica **chave** dos blockchains públicos?

A) Permitem que um usuário eleja nós para processar as transações.
B) Permitem que qualquer pessoa participe de uma rede blockchain.
C) Permitem o controle sobre quem pode participar e em que nível.
D) Permitem que apenas partes confiáveis operem seu blockchain.

A) Incorreto. Nós federados de blockchains podem existir tanto em blockchains públicos quanto em privados. A federação ocorre quando o sistema, ou melhor, o usuário de um sistema, elege nós para processar as transações.
B) Correto. Blockchains públicos permitem que qualquer um participe da rede, desde que tenha acesso a internet, hardware e eletricidade. (Literatura: A, Capítulo 1.1)
C) Incorreto. Blockchains híbridos controlam quem pode participar e qual é o nível de participação em que cada nó pode operar.
D) Incorreto. Blockchains privados permitem que apenas partes confiáveis operem seu blockchain.

7 / 40
O que é um exemplo de uso da criptografia em um blockchain?

A) Acesso a blockchains privados ou híbridos utilizando uma chave privada
B) Criação de criptomoeda como recompensa para os nós de mineração
C) Proteção de blockchains contra ataques de 51% por parte de nós corruptos
D) Proteção de transferências de criptomoeda entre destinatários

A) Incorreto. Não se usa criptografia para acessar blockchains privados ou híbridos, mesmo que eles utilizem chaves privadas e públicas.
B) Incorreto. Algumas redes blockchain recompensam nós de mineração com criptomoeda. Entretanto, não é isso que a criptografia faz.
C) Incorreto. A criptografia ajuda a proteger os blockchains, mas não necessariamente contra um ataque de 51%.
D) Correto. A criptografia assimétrica usada pela tecnologia blockchain permite que o emissor transfira criptomoeda para o destinatário sem que outra pessoa possa roubá-la. (Literatura: A, Capítulo 2.1)

8 / 40
Como os blockchains usam criptografia de chave privada e chave pública?

A) A criptografia assimétrica permite que um emissor transfira criptomoeda para uma chave pública. O destinatário pode então acessar esses fundos com sua chave privada e mantê-la em sua carteira.
B) Na criptografia de chave pública, uma única chave é usada para criptografar e descriptografar a transação. O emissor usa esta chave para enviar criptomoeda, que ficará na carteira do destinatário após a descriptografia.
C) A criptografia simétrica permite que um emissor transfira criptomoeda para um destinatário, que poderá então acessar seus fundos quando o emissor lhe der acesso à sua chave privada.
D) O algoritmo no blockchain criptografa e armazena as chaves privadas e públicas em todas as carteiras do usuário. Em seguida, o usuário acessa os fundos com sua frase de recuperação de vinte palavras.

A) Correto. A criptografia assimétrica permite a qualquer pessoa criptografar uma mensagem com a chave pública do destinatário. No entanto, a mensagem criptografada apenas pode ser lida com a chave privada do destinatário. A criptografia assimétrica permite que o emissor transfira criptomoeda para o destinatário sem que haja a possibilidade de roubo por terceiros. Ela permite, ainda, que a transferência seja realizada sem nenhum encontro ou troca de informações entre o emissor e o destinatário. Desde que o emissor possua a chave pública do destinatário, é possível lhe enviar criptomoeda. (Literatura: A, Capítulo 2)
B) Incorreto. A criptografia de chave pública usa duas chaves, uma pública e outra privada. Os usuários que desejam enviar criptomoeda a um novo endereço assinam a transação com sua chave privada e então a enviam à chave pública, conhecida como endereço. O destinatário então usa sua chave privada para acessar os fundos.
C) Incorreto. Os blockchains não usam este tipo de criptografia, pois ela usa apenas uma chave. Neste caso, os usuários teriam que se reunir para trocar informações.
D) Incorreto. Os blockchains têm apenas o endereço público para a criptomoeda. A chave privada é guardada de forma segura por seu proprietário. As frases de recuperação podem ser usadas para recuperar chaves públicas em caso de perda.

9 / 40
Como as redes blockchain híbrido combatem os ataques de 51%?

A) Com um controlador central, que garante a segurança de cada nó da rede
B) Com um algoritmo de prova de trabalho (PoW), que permite aos mineradores proteger a rede
C) Com um mecanismo de incentivos para os mineradores, que recebem moeda por proteger a rede
D) Com raízes da árvore de Merkle, que permitem que a rede volte ao seu último bloco válido

A) Incorreto. As raízes da árvore de Merkle são uma maneira de proteger redes híbridas. Blockchains híbridos não possuem um controlador central.
B) Incorreto. A criptografia é uma funcionalidade de segurança genérica de qualquer tipo de blockchain, não sendo específica às redes híbridas.
C) Incorreto. Um mecanismo de incentivos funciona bem nos blockchains públicos, mas não nos híbridos.
D) Correto. Redes blockchain híbridas são protegidas pelos hashes criptográficos das raízes da árvore de Merkle, que permitem que a rede volte ao seu último bloco válido caso seja corrompida. (Literatura: A, Capítulo 1.1)

10 / 40
Como os blockchains funcionam como registros?

A) Mantendo um histórico de todas as transações já realizadas na rede
B) Mantendo grande quantidade de dados das transações, como um banco de dados centralizado
C) Atualizando periodicamente o blockchain com todos os balanços de todas as carteiras

A) Correto. Os blockchains são contas públicas amplamente distribuídas que permitem a qualquer um ver quem possui qual criptomoeda e o histórico completo desta moeda ao longo do tempo. É possível encontrar todas as transações, bem como as partes envolvidas em cada transação. (Literatura: A, Capítulo 2.1)
B) Incorreto. Os blockchains são registros amplamente distribuídos que mantêm uma quantidade limitada de dados das transações. O limite de tamanho é restrito porque eles são distribuídos. Logo, é impraticável compartilhar e reconciliar grande quantidade de dados.
C) Incorreto. As carteiras não mantêm um registro privado, mas recebem dados do balanço do blockchain.

11 / 40
Qual é a tarefa dos mineradores em uma rede blockchain?

A) Agir como um terceiro único para agregar transações e instaurar confiança na rede por meio da autoridade dos mineradores
B) Na qualidade de computadores, permitir o acesso à blockchain, garantindo que a quantidade de nós corruptos permaneça baixa
C) Na qualidade de nós, competir por uma recompensa ao calcular o nonce criptográfico correto para possibilitar a transação
D) Definir as regras de consenso que devem ser seguidas e intervir quando essas regras não são cumpridas

A) Incorreto. A necessidade de um terceiro único era exatamente o que Satoshi queria evitar com a criação da tecnologia blockchain.
B) Incorreto. Os mineradores não são responsáveis pelo acesso ao blockchain.
C) Correto. Os mineradores competem por uma recompensa ao tentar calcular o nonce criptográfico. (Literatura: A, Capítulo 1.1)
D) Incorreto. Os mineradores não definem as regras no blockchain. Em vez disso, operam no ambiente definido pelas regras.

12 / 40
Que descrição se aplica **apenas** ao algoritmo de consenso de prova de trabalho (PoW)?

A) Um algoritmo de consenso colaborativo em que as contas aprovadas realizam a validação.
B) Um algoritmo de consenso colaborativo facilitado por mineradores (farmers), que disponibilizam a memória não utilizada de seus computadores para viabilizar as transações.
C) Um algoritmo de consenso em que a validação é realizada para o fluxo inteiro de transações, incluindo tanto a exatidão dos dados quanto a sequência das transações.
D) Um algoritmo rápido e de baixo custo em que um nó necessita depositar criptomoeda para garantir a transação.
E) Um algoritmo de consenso não competitivo em que a validação é realizada pelos nós eleitos, que enviam criptomoeda para um endereço onde ela não pode ser recuperada.
F) Um algoritmo que inclui validação colaborativa, realizada por validadores escolhidos fora do consenso.
G) Um algoritmo que funciona em um ambiente de execução confiável e comprova a hora em que a transação foi realizada.
H) Um algoritmo competitivo intensivo e dispendioso, em que cada nó de mineração do blockchain compete para proteger os blocos.

A) Incorreto. Esta é a definição de prova de autoridade (PoA).
B) Incorreto. Esta é a definição de prova de capacidade (PoC) e de prova de espaço (PoSpace)
C) Incorreto. Esta é a definição de Hyperledger Fabric.
D) Incorreto. Esta é a definição de prova de participação (PoS).
E) Incorreto. Esta é a definição de prova de queima.
F) Incorreto. Esta é a definição de prova de participação delegada (DPoS).
G) Incorreto. Esta é a definição de prova do tempo decorrido (PoET).
H) Correto. Esta é a definição de PoW. (Literatura: A, Capítulo 3.1)

13 / 40
Um algoritmo de consenso competitivo que foi desenvolvido porque os blockchains tinham dificuldade em atender às exigências de velocidade das transações.

Que algoritmo de consenso é este?

A) Prova de participação delegada (DPoS)
B) Prova de queima
C) Prova de participação (PoS)
D) Prova de trabalho (PoW)

A) Incorreto. O DPoS é um esforço colaborativo. Os nós que validam as transações recebem a mesma recompensa. As partes interessadas elegem as testemunhas que irão validar as transações e criar blocos para a rede.
B) Incorreto. A prova de queima é um algoritmo de consenso não competitivo.
C) Correto. O PoS é um algoritmo de consenso competitivo criado como uma alternativa ao PoW porque os blockchains tinham dificuldade em atender às exigências de velocidade das transações. Os nós do PoS não mineram criptomoeda. Os usuários podem usar parte da sua criptomoeda, de um blockchain, para fazer uma caução. Esta caução permite que o usuário "aposte" que realizará a transação honestamente, segundo as regras do sistema de consenso. Se o usuário não o fizer, irá perder sua criptomoeda. (Literatura: A, Capítulo 3.2)
D) Incorreto. O PoW é um algoritmo de consenso competitivo em que cada nó de mineração do blockchain compete para proteger os blocos. O PoW permite a participação de qualquer pessoa na criação e manutenção do sistema, mas é muito competitivo. Os nós que desejem ser competitivos e recompensados com criptomoeda terão que operar equipamentos especializados. O PoS foi criado como uma alternativa ao PoW para atender às exigências de alta velocidade das transações.

14 / 40
Qual algoritmo de consenso é o **menos** eficiente em termos de energia?

A) Prova de participação delegada (DPoS)
B) Prova de autoridade (PoA)
C) Prova de espaço (PoSpace)
D) Prova de trabalho (PoW)

A) Incorreto. O DPoS é um esforço colaborativo. Neste sistema de consenso, os nós que validam as transações recebem a mesma recompensa. O DPoS é eficiente em termos de energia e não queima eletricidade ao minerar.
B) Incorreto. Os blockchains de PoA têm um algoritmo de consenso colaborativo. Neste sistema, as transações e os blocos são validados pelas contas aprovadas. Os nós validadores executam o software de consenso, o que os permite pôr as transações em blocos. Dado o número limitado de validadores, o algoritmo é eficiente em termos de energia.
C) Incorreto. Em vez de usar capacidade de processamento para competir para proteger o blockchain, este algoritmo usa a memória não utilizada. Os blockchains de PoSpace podem ser uma alternativa mais justa e mais ecológica a outros blockchains. Eles podem ser utilizados para desenvolver aplicações e transferir valores.
D) Correto. Este algoritmo é, por seu projeto, dispendioso e de alta intensidade energética. O custo e a dificuldade para obter bitcoins foram intencionais na economia de token. Assim como minerar ouro, não é barato nem fácil minerar, e se acredita que a dificuldade e escassez dos bitcoins impulsionam parte do valor do ativo. (Literatura: A, Capítulo 3.1)

15 / 40
Qual é uma vantagem de se usar o algoritmo de consenso de prova do tempo decorrido (PoET) em vez de prova de trabalho (PoW)?

A) Em um blockchain sem permissão, é mais fácil utilizar o PoET que o PoW, pois o PoET usa um sistema de loteria seguro para a seleção de nós.
B) Geralmente, o custo da transação é menor no PoET que no PoW, pois o hardware necessário é mais genérico no PoET que no PoW.
C) O PoET é muito mais seguro que o PoW, pois o PoET suporta o ambiente de execução confiável (TEE) ao marcar as transações com carimbo de data/hora.
D) O PoET é geralmente mais rápido que o PoW. Como no PoET a seleção de nós é aleatória, há menos nós que competem por validação que no PoW.

A) Incorreto. O PoET é usado principalmente em redes com permissão dado que os nós precisam se identificar. Além do mais, o sistema de loteria do PoET tem problemas de segurança.
B) Incorreto. O PoET tem custos de transação mais baixos, mas a causa não é hardware genérico, pois o PoET precisa de hardware específico.
C) Incorreto. O PoET não é mais seguro que o PoW. Mesmo que fosse, a segurança não seria relacionada ao carimbo de data/hora, pois este mecanismo apenas funciona em um ambiente onde os nós são conhecidos.
D) Correto. A menor quantidade de nós competindo torna o PoET mais rápido. (Literatura: A, Capítulo 3.1 e 3.5)

16 / 40
Um hacker tenta corromper o histórico das transações em um blockchain para gastar um token ou uma criptomoeda duas vezes.

O que é **mais** provável que o hacker tenha feito?

A) Mudado a transação em seu nó e então a propagado na rede
B) Editado o contrato inteligente e resgatado criptomoeda do investidor
C) Ganho o controle de mais de 51% da capacidade de processamento da rede
D) Executado um hard fork na rede, criando uma nova rede blockchain

A) Incorreto. Outros nós não aceitariam esta transação porque isso criaria uma sidechain mais curta que o blockchain já existente. O hacker não tem capacidade de mineração suficiente em um nó para criar uma cadeia maior.
B) Incorreto. É pouco provável que o contrato inteligente tenha sido hackeado, já que o hacker tenta gastar os tokens duas vezes.
C) Correto. Foi isso que aconteceu em um ataque à rede da Ethereum Classic. O hacker era um minerador mal-intencionado que reverteu o histórico das transações. O feito só foi possível porque ele ganhou o controle de mais de 51% da capacidade de processamento da rede (ataque de 51%). (Literatura: A, Capítulo 10.1)
D) Incorreto. Não aconteceu nenhum hard fork da rede, pois não houve nenhuma mudança radical no protocolo da rede.

17 / 40
As redes blockchain são vulneráveis aos ataques de 51%.

Qual rede os hackers teriam **mais** interesse de invadir?

A) Bitcoin
B) Fabric
C) Ripple

A) Correto. Os mineradores usam sua capacidade de processamento e eletricidade para gerar nova criptomoeda, como os bitcoins. Se a rede ficar concentrada demais, mineradores criminosos podem corrompê-la impunemente. Este tipo particular de vulnerabilidade é conhecido como ataque de 51%, sendo 51% um ponto crítico para muitos blockchains. Se menos que 51% dos nós forem independentes, a rede será revertida. (Literatura: A, Capítulo 10.1)
B) Incorreto. A Hyperledger Fabric não possui criptomoeda. Como há pouco a ser roubado, os hackers têm menos interesse de invadi-la.
C) Incorreto. Diferentemente da rede Bitcoin, que não requer que os usuários confiem nos outros membros da rede ou os conheçam, a infraestrutura inteira da Ripple requer que, de certo modo, todas as partes se conheçam e tenham confiança mútua. Um participante de um mercado financeiro deve confiar nos emissores dos ativos que possui. Similarmente, um operador de nó deve confiar que os outros nós em sua lista de validadores não conspirarão para impedir que as transações válidas sejam confirmadas. Como há confiança e incentivos compatíveis com a cooperação, esta rede é menos propensa a sofrer um ataque de 51%.

18 / 40
Uma das maiores ameaças à comunidade blockchain é o narcisismo das pequenas diferenças.

Qual é o resultado deste narcisismo das pequenas diferenças?

A) Uma comunidade ridiculariza uma outra por pequenas diferenças, resultando em uma maior colaboração.
B) A comunidade se preocupa e trabalha para resolver pequenas diferenças que não são percebidas por grupos externos.
C) A comunidade desenvolveu vários projetos similares que brigam por pequenas diferenças.
D) A comunidade fica mais unida e trabalha junto de modo colaborativo para resolver problemas comuns.

A) Incorreto. Não há colaboração. As divergências nas comunidades chegam até o código, dividindo a comunidade repetidas vezes.
B) Incorreto. As comunidades são mais propensas a ridicularizar umas as outras e se tornar hipersensíveis a coisas pequenas.
C) Correto. Comunidades com territórios adjacentes e relacionamentos próximos são mais propensas a brigar. (Literatura: A, Capítulo 10.2)
D) Incorreto. O que acontece é justamente o contrário. As comunidades são mais propensas a se ridicularizar que a colaborar.

19 / 40
Como um golpista usa o esquema Ponzi?

A) Convence as vítimas a pagar para receber algo de maior valor posteriormente.
B) Encontra investidores e em seguida despeja os tokens desses investidores para provocar um colapso financeiro.
C) Paga dividendos aos investidores iniciais usando os fundos dos investidores subsequentes.
D) Rouba cartões de crédito e os usa para adquirir dinheiro, bens ou propriedades.

A) Incorreto. Isto é a fraude de pagamento antecipado.
B) Incorreto. Isto é a fraude de manipulação de mercado.
C) Correto. No esquema de Ponzi à moda antiga, o golpista paga dividendos aos investidores iniciais usando os fundos dos investidores subsequentes. (Literatura: A, Capítulo 10.3)
D) Incorreto. Isto é furto de identidade e fraude no cartão de crédito.

20 / 40
Qual característica da rede blockchain serve também para protegê-la?

A) Quanto mais nós completos independentes, mais difícil será comprometer os dados no blockchain.
B) Quanto menor a quantidade de mineradores no blockchain, maiores serão os incentivos para proteger a rede.
C) Quanto mais centralizado o controle do blockchain, mais difícil será proteger os dados e evitar fraudes.
D) Quanto mais complicado for o algoritmo de prova de trabalho (PoW), maior será a recompensa para proteger a rede.

A) Correto. A distribuição é uma das principais medidas de segurança de um blockchain. (Literatura: A, Capítulo 1.1)
B) Incorreto. O incentivo para os mineradores não é a segurança do blockchain.
C) Incorreto. Um controlador central pode aumentar a segurança do blockchain ao trabalhar apenas com nós confiáveis.
D) Incorreto. A complexidade do PoW não contribui para a segurança do blockchain.

21 / 40
Como as informações podem ser protegidas em um blockchain?

A) Usando uma rede ponto a ponto (P2P) fechada que compartilha informações entre plataformas
B) Usando uma distribuição de criptomoedas aos mineradores através da rede
C) Usando criptografia assimétrica, que consiste em uma chave pública e outra privada
D) Usando tecnologia de registro distribuído (DLT), que registra as informações na origem

A) Incorreto. P2P é o tipo da rede usada, não uma medida de segurança por si só.
B) Incorreto. Criptomoeda é o valor usado para o câmbio, não uma ferramenta de segurança.
C) Correto. A criptografia assimétrica permite a qualquer pessoa criptografar uma mensagem com uma chave pública. No entanto, a mensagem criptografada apenas pode ser lida com a chave privada correta. (Literatura: A, Capítulo 2.1)
D) Incorreto. A DLT é a tecnologia global do blockchain, não é propriamente uma medida de segurança.

22 / 40
Como o blockchain usa uma testemunha pública?

A) Um tribunal ou uma biblioteca digitais têm o papel de testemunha pública para armazenar informações de referência.
B) Um nó da rede blockchain atesta a veracidade e a autenticidade da informação.
C) Uma pessoa envia uma transação através de uma rede pública para ser recompensada como uma testemunha pública.
D) Um nó preferencial pode ser eleito para atestar a veracidade e a autenticidade da informação.

A) Incorreto. Os blockchains são essencialmente um arquivo digital, porém não precisam de um tribunal ou uma biblioteca digitais separados para o papel de testemunha pública. Isso é o que os nós fazem.
B) Correto. Cada nó da rede blockchain testemunha informações. Todos os nós atestam sua veracidade e autenticidade posteriormente, tal como os tribunais, bibliotecas e arquivos são lugares onde as pessoas armazenam informações para referência posterior. (Literatura: A, Capítulo 2.4)
C) Incorreto. São os nós que têm o papel de testemunhas públicas, não as pessoas. Os nós nem sempre recebem recompensas por agir como testemunha pública.
D) Incorreto. Todos os nós da rede blockchain testemunham as informações, não apenas os nós preferenciais.

23 / 40
O blockchain permite uma identidade auto-soberana.

Como o blockchain faz isso?

A) Permitindo que terceiros centralizados ofereçam informação de identidade válida e fácil de usar
B) Permitindo que cada pessoa tenha um controle exclusivo do seu dinheiro, propriedade e identidade
C) Permitindo que os governos emitam facilmente identidades com certificados digitais avançados
D) Permitindo que apenas empresas de internet ofereçam repositórios de identidade pessoal de excelente segurança

A) Incorreto. Os sistemas centralizados podem ficar comprometidos e os documentos podem ser falsificados ou alterados, dificultando a verificação das identidades. O Facebook chegou às manchetes em 2018, após compartilhar os dados pessoais de mais de 87 milhões de clientes com a Cambridge Analytica, que é um terceiro. As informações foram então usadas para manipular o comportamento dos indivíduos. A conveniência e a facilidade de utilização comprometeram muitas identidades pessoais e informações financeiras.
B) Correto. A tecnologia blockchain possibilitou uma mudança nos conceitos de autopropriedade. Deu vida nova aos movimentos sociais relacionados à moral e aos direitos naturais de cada pessoa de ter controle exclusivo sobre seu dinheiro, propriedade de identidade. (Literatura: A, Capítulo 6.1)
C) Incorreto. Uma identidade auto-soberana é gerenciada pelo próprio indivíduo, não por um terceiro. Uma pessoa autentica a si mesma e não depende de um terceiro para validar e comprovar suas credenciais.
D) Incorreto. Há apenas um pequeno grupo de empresas que controlam a emissão dos certificados de segurança de sites, fazem curadoria e cultivam as identidades online. Esta centralização levou à hospedagem, em servidores centralizados, de volumes imensos de dados pessoais de todos os usuários da internet. Os servidores podem ser - e são - invadidos.

24 / 40
Os blockchains públicos dão um incentivo para encorajar os usuários a minerar blocos e proteger a rede.

Que incentivo é este?

A) Permissão para que os usuários criem tokens para vender em mercados secundários.
B) Nenhum. Não há recompensa porque os blockchains públicos são feitos em software livre.
C) Recompensas em dinheiro pela operação dos nós de mineração.
D) Recompensas em criptomoeda pela mineração.

A) Incorreto. Normalmente, os mineradores recebem criptomoeda diretamente.
B) Incorreto. Mesmo baseados em licença aberta e com software livre, os blockchains públicos ainda oferecem recompensas por mineração.
C) Incorreto. Os mineradores recebem criptomoeda, não moeda tradicional.
D) Correto. Os blockchains públicos geralmente dão criptomoeda como recompensa pela mineração. (Literatura: A, Capítulo 1.1)

25 / 40
Uma organização deseja desenvolver contratos inteligentes baseados em tecnologia blockchain, mas não quer que seus funcionários se sobrecarreguem para manter a segurança do blockchain.

Que tipo de blockchain é o **mais** adequado para esta organização?

A) Blockchain híbrido
B) Blockchain privado
C) Blockchain público

A) Incorreto. Em um blockchain híbrido, o nível de participação de cada nó pode ser controlado. Se as organizações não querem usar seus funcionários para proteger o blockchain, esta não é a melhor opção.
B) Incorreto. Os blockchains privados são mais como as redes confiáveis. Os membros da rede são conhecidos e os contratos podem ser alterados. Ainda que ofereçam melhorias em comparação aos processos de negócios em papel, não têm nem a mesma finalidade nem aplicabilidade das redes públicas.
C) Correto. Um blockchain público minimiza a possibilidade de se alterar os contratos inteligentes no blockchain. A segurança de um blockchain público não depende de um número pequeno de funcionários, sendo mais adequada aos planos da organização. (Literatura: A, Capítulo 1 e 10.1)

26 / 40
Qual é uma característica **chave** da rede Hyperledger?

A) É uma rede blockchain público e uma das mais antigas, existindo desde 2009.
B) É privada, de software livre e pode executar a tecnologia de registro distribuído (DLT) própria de cada participante.
C) Usa criptomoeda como mecanismo de recompensa, o que a torna mais segura.
D) Usa o algoritmo de consenso de prova de participação (PoS) como sua principal medida de segurança.

A) Incorreto. A Hyperledger não é uma rede blockchain pública e foi criada em 2015 pela Fundação Linux.
B) Correto. A Hyperledger é uma rede privada porém de software livre e, portanto, ajuda às pessoas a executar a sua própria DLT. (Literatura: A, Capítulo 4.4)
C) Incorreto. A Hyperledger não utiliza criptomoeda como mecanismo de recompensa nem como medida de segurança.
D) Incorreto. A Hyperledger não usa o algoritmo de consenso de PoS.

27 / 40
Qual é o **melhor** caso de uso dos contratos inteligentes?

A) Digitalizar e automatizar contratos juridicamente vinculativos por meio de inteligência artificial (IA)
B) Importar a execução de contratos no sistema legal usando criptomoedas
C) Garantir pagamento automático por ações ou eventos predeterminados nos contratos de seguro
D) Estender um blockchain de Bitcoin, a plataforma mais conhecida de contrato inteligente, ao sistema judiciário

A) Incorreto. Os contratos inteligentes são criados por desenvolvedores e executados por álgebra booleana, matemática e criptografia. Um contrato juridicamente vinculado, por outro lado, é criado por um advogado e executado por um sistema judiciário. A maioria dos contratos inteligentes não é juridicamente vinculativa. IA e contratos inteligentes podem ser usados juntos, mas este não é o melhor caso de uso.
B) Incorreto. Os contratos legais são executados por um sistema judiciário e não têm as mesmas limitações dos contratos inteligentes. Mesmo em um processo civil, a violação de uma ordem judicial de pagamento é passível de acusação de desacato e prisão, ou os fundos podem ser automaticamente resgatados de uma conta. As leis são mais flexíveis, já os softwares são mais rigorosos. As leis e os contratos são interpretados por pessoas que têm opções legais. O código é interpretado normalmente de um único modo. Se ocorre algo imprevisto, significa que há um erro que deve ser corrigido.
C) Correto. Um contrato agrário inteligente pode garantir o pagamento automático do seguro. Em caso de geada e dano na plantação, o fazendeiro receberá o pagamento. (Literatura: A, Capítulo 5.1)
D) Incorreto. O blockchain de Bitcoin não é tão conhecido por ter contratos inteligentes, embora já houvesse referência a eles no artigo que primeiramente propôs a rede de Bitcoin. Os contratos inteligentes no Bitcoin utilizam um código de operação (opcode), que foi apresentado por Peter Todd como Proposta de Melhoria do Bitcoin (BIP) 65.

28 / 40
Em qual cenário um contrato inteligente é a **melhor** solução para o problema?

A) Um barman quer forçar os clientes a pagar por suas bebidas com a transferência de criptomoeda para sua carteira.
B) Uma diretora financeira quer receber uma notificação do seu smartwatch quando seu marido chegar em casa.
C) Uma empresa de energia quer comprar automaticamente energia quando os preços atingirem um valor predeterminado.
D) Uma seguradora quer indenizar um fazendeiro sempre que o gerente de caso julgar que é o melhor a ser feito.

A) Incorreto. Este não é um cenário em que um contrato inteligente seria útil. Contratos inteligentes não forçam uma outra parte a disponibilizar fundos.
B) Incorreto. Um contrato inteligente é celebrado entre duas ou mais partes. Neste cenário, não há uma segunda parte e, portanto, um contrato inteligente não é a melhor solução.
C) Correto. Este é um bom exemplo em que um contrato inteligente é útil. (Literatura: A, Capítulo 5.1)
D) Incorreto. Contratos inteligentes são acionados em eventos predeterminados. A disposição da empresa para indenizar não é uma maneira ótima de usar um contrato inteligente, pois ele não aciona automaticamente o código.

29 / 40
Qual é a finalidade das DApps?

A) Executar contratos inteligentes com a lógica de negócios no front-end de uma aplicação independente
B) Apenas gerenciar criptomoedas, sem nenhum sistema de voto incorporado para a governança do blockchain
C) Executar aplicações em uma rede ponto a ponto (P2P), ampliando os contratos inteligentes de forma a ser mais que simples transferência de valores
D) Apoiar as aplicações que funcionam em vários fornecedores de nuvem (cloud) públicos, evitando a dependência tecnológica (lock-in) e fraude

A) Incorreto. Contratos inteligentes formam o back-end e em geral são apenas uma pequena parte de uma aplicação descentralizada (DApp).
B) Incorreto. As DApps são divididas em três grandes categorias, segundo sua finalidade: 1) DApps para administrar dinheiro; 2) DApps que, apesar de usar dinheiro, foram desenvolvidas para outra finalidade, como um jogo; 3) DApps para governança, como um sistema de voto. Essas aplicações de governança são chamadas de “organizações autônomas descentralizadas”, geralmente abreviadas como DAOs.
C) Correto. As DApps ampliam os contratos inteligentes para ser mais que simples transferências de valores de A a B. As DApps são desenvolvidas com os contratos inteligentes, porém usam outros serviços, como envio seguro de mensagens, e com frequência permitem a interação de um número ilimitado de participantes sob um dado conjunto de regras. (Literatura: A, Capítulo 5.3)
D) Incorreto. DApps são aplicações que funcionam em uma rede P2P em vez de em um único sistema. As DApps podem ser ferramentas, programas, jogos, entre outros, que conectam diretamente usuários e fornecedores.

30 / 40
Qual é o papel de uma organização autônoma descentralizada (DAO)?

A) Direcionar o problema do principal-agente, com colaboração e aceitação das ações dentro das regras acordadas
B) Incluir, no sistema judiciário atual, contratos inteligentes online regulamentados usando blockchains públicos
C) Oferecer contratos inteligentes online complexos sem nenhum vínculo com ativos offline tangíveis ou intangíveis
D) Fornecer uma plataforma de contrato de um blockchain privado em que os usuários possam executar suas aplicações online

A) Correto. O conceito de DAO foi criado para resolver o que em economia é conhecido como o "problema do principal-agente", que é um dilema que acontece quando um "agente" pode tomar decisões no lugar de um outro agente, porém é influenciado por seu próprio interesse. O "agente" pode decidir correr mais risco, uma vez que não arcará de fato com o custo do risco. (Literatura: A, Capítulo 5.4)
B) Incorreto. O código e as capacidades das DAOs não isentam indivíduos do cumprimento dos regulamentos e das leis.
C) Incorreto. As DAOs funcionam por meio de regras codificadas em seus contratos inteligentes. Elas são totalmente online, embora possam administrar ativos offline, como imóveis e recursos naturais.
D) Incorreto. Todos os blockchains públicos são DAOs, como o Bitcoin, o Ethereum, o Factom, entre outros. As DAOs podem ser mais do que blockchains públicos, podendo ser usadas para gerenciar qualquer tipo de organização humana, como empresas, fundos de investimento e até mesmo governos.

31 / 40
Qual é a **maior** contribuição da tecnologia blockchain à proteção dos dados de identidade?

A) Eliminação de terceiros por meio do fornecimento de armazenamento de dados seguro em um servidor de usuário
B) Codificação de todos os dados de saúde, que serão salvos em um blockchain privado sem permissão
C) Proteção dos dados que foram enviados na internet por meio de um algoritmo de criptografia
D) Fornecimento de dados pessoais sem revelar os dados reais que comprovam esses dados pessoais

A) Incorreto. Não tem sentido usar um blockchain no servidor do usuário, pois o blockchain é supostamente um registro distribuído.
B) Incorreto. A codificação de dados pessoais em um blockchain sem permissão não tem sentido, pois um blockchain sem permissão não é suficientemente seguro para isso.
C) Incorreto. Não tem sentido proteger informação enviada previamente na internet, pois essa informação pode já estar adulterada.
D) Correto. Fornecer informação sem revelar os dados reais é uma das funções importantes de um blockchain. (Literatura: A, Capítulo 6.1)

32 / 40
Qual é a vantagem de se usar redes blockchain com a internet das coisas (IoT)?

A) Permitir aos usuários do blockchain monitorar e acessar veículos autônomos
B) Evitar um ataque de falsificação (spoofing) usando a identidade segura armazenada no blockchain
C) Habilitar um software que se autoprograma para resolver problemas sem intervenção humana
D) Resolver cálculos complexos e dispendiosos com o uso de mineração no Hyperledger Fabric

A) Incorreto. Isso seria uma situação perigosa, pois os veículos autônomos estariam suscetíveis a ataques de spoofing ou invasões. Há muitas empresas desenvolvendo tecnologias que utilizam blockchain para proteger dispositivos de IoT.
B) Correto. A IoT pode utilizar a identidade segura do blockchain para evitar um ataque de spoofing em que uma parte mal-intencionada se faz passar por um outro dispositivo para lançar um ataque para roubar dados ou provocar algum outro transtorno. (Literatura: A, Capítulo 6.3)
C) Incorreto. Esta é a vantagem de se usar redes blockchain com inteligência artificial (IA).
D) Incorreto. Não há mineração no Hyperledger Fabric. A Matrix AI fornece uma solução que torna fácil combinar aprendizado de máquina com contratos inteligentes. A plataforma altera o modo de execução dos contratos inteligentes, melhorando sua velocidade, flexibilidade, facilidade e segurança. A Matrix usa sua capacidade de mineração para resolver cálculos complexos e dispendiosos de IA.

33 / 40
A tecnologia blockchain viabilizou os mercados descentralizados.

Qual é uma vantagem de um mercado descentralizado?

A) É baseado em tecnologia de software livre, então pode ser usado sem nenhum investimento.
B) Sua operação não está sob licença, logo é mais bem gerenciado.
C) É relativamente barato, dado o uso de criptomoeda, e muito acessível.
D) É à prova de falsificações, resistente a tentativas de encerramento e confiável devido aos contratos inteligentes.

A) Incorreto. O uso de tecnologia de software livre não determina a necessidade – ou não - de um investimento. Além do mais, nem todos os blockchains são baseados em software livre.
B) Incorreto. O fato de estar sob licença não determina se um produto é bem gerenciado ou não.
C) Incorreto. Não é necessariamente verdade que mercados descentralizados sejam mais baratos que outros mercados.
D) Correto. O blockchain se assegura de que cada um seja quem diz ser, protegendo a transferência de valores sem a necessidade de terceiros. (Literatura: A, Capítulo 6.5)

34 / 40
Como o blockchain melhora as cadeias de suprimentos?

A) Com a criação automática de acordos comerciais entre as duas partes
B) Com a criação de mercados centralizados seguros para negociar mercadoria
C) Com a estabilização das moedas nacionais dos países envolvidos
D) Com a transferência da propriedade tokenizada por meio de um sistema de software

A) Incorreto. Acordos comerciais podem ser programados nos contratos inteligentes, mas o blockchain não cria esses acordos comerciais.
B) Incorreto. O blockchain pode ajudar a tornar os mercados descentralizados mais seguros, mas definitivamente não ajuda a criar mercados centralizados.
C) Incorreto. O blockchain não ajuda a estabilizar as moedas nacionais.
D) Correto. O blockchain pode transferir valor, ou propriedade tokenizada, por meio de apenas um sistema de software. (Literatura: A, Capítulo 7.1)

35 / 40
A Autoridade Monetária de Singapura (MAS) e a empresa de blockchain R3 fizeram uma parceria.

O que realizaram juntas?

A) Criaram contratos inteligentes e moedas estáveis.
B) Simplificaram a transmissão interbancária de mensagens.
C) Possibilitaram os primeiros pagamentos interbancários sem limitações de fuso horário.
D) Lançaram transferências eletrônicas usando criptografia.

A) Incorreto. A Everex está envolvida no desenvolvimento dos contratos inteligentes e moedas estáveis para suportar as iniciativas de moeda digital dos bancos centrais e comerciais.
B) Incorreto. A rede mundial da Sociedade de Telecomunicações Financeiras Interbancárias Mundiais (SWIFT) se tornou a entidade responsável pela maioria dos pagamentos internacionais. Ainda que não movimente dinheiro, essa rede facilita a transmissão de mensagens entre bancos, permitindo de fato aos bancos se comunicarem diretamente para simplificar o processo de transferência internacional de dinheiro.
C) Correto. A Autoridade Monetária de Singapura fez uma parceria com a empresa de blockchain R3 e realizou o primeiro pagamento interbancário utilizando a tecnologia blockchain em 2016. O projeto demonstrou que os bancos podiam realizar transações e liquidar 24 horas por dia, e não estavam mais limitados por fusos horários e horário comercial. (Literatura: A, Capítulo 7.2)
D) Incorreto. Foi a Western Union que lançou a transferência eletrônica de fundos de uma pessoa ou entidade para outra por meio de uma rede de telégrafos, ajudando de fato a movimentar dinheiro dentro ou através das fronteiras. A Western Union ainda lida com a maioria das remessas pessoais a nível global.

36 / 40
O que é uma moeda fiduciária digital?

A) Uma moeda em forma digital que representa as reservas financeiras de um país
B) Uma moeda digital que cria um mercado de dívida transparente e sem fronteiras
C) Um sistema online que permite a realização de transações sem uma conta bancária

A) Correto. A moeda fiduciária digital é definida como a representação em forma digital da moeda de um dado país. É emitida e regulada pela autoridade monetária competente desse país. (Literatura: A, Capítulo 8.1)
B) Incorreto. A moeda fiduciária digital não tem nenhuma relação com os mercados de dívida.
C) Incorreto. A moeda fiduciária digital serve apenas para quem tem conta bancária. Ela se destina a balanço de pagamentos internacionais, não a transações individuais.

37 / 40
Como a tecnologia blockchain beneficia o setor de seguros?

A) Ao evitar requisitos de conformidade das autoridades nacionais, o que reduz as despesas gerais
B) Ao garantir a precisão dos dados e automatizar os microsseguros, o que reduz custos
C) Ao instaurar prêmios flexíveis pagos pelos clientes, o que aumenta o lucro
D) Ao criar um modo de pagamento digital, o que simplifica a regularização dos sinistros

A) Incorreto. As atividades do blockchain devem estar em conformidade com a legislação e a regulamentação.
B) Correto. A tecnologia blockchain permite às seguradoras proporcionar mais valor para os contratos já existentes. (Literatura: A, Capítulo 8.3)
C) Incorreto. O blockchain não define o prêmio pago pelos clientes.
D) Incorreto. O blockchain não define como o pagamento será efetuado para a seguradora.

38 / 40
Como a tecnologia blockchain ajuda a proteger os direitos de propriedade intelectual (PI)?

A) Incluir transações de PI em contratos inteligentes
B) Registrar um evento e estabelecer o cronograma
C) Registrar a criação de pacotes de software
D) Enviar uma transação e receber o direito à PI

A) Incorreto. Um contrato inteligente funciona como um contrato online entre duas ou mais partes. Os contratos inteligentes são acordos digitais ou conjunto de regras que regem o acesso à PI.
B) Correto. A PI é baseada no conceito de justiça, “quem fez o que e quando” e a primeira pessoa a fazer algo deve ter o direito ao benefício comercial por esses esforços. O uso de blockchain permite confirmar que algo já existia em um dado momento e as informações podem ser verificadas por terceiros. (Literatura: A, Capítulo 8.4)
C) Incorreto. A tecnologia blockchain é usada para registrar um evento relacionado à criação de uma PI.
D) Incorreto. Não é possível confirmar o direito à PI com o simples envio de uma transação.

39 / 40
Qual é um exemplo de um governo promovendo ativamente o uso de blockchain?

A) A China criou um sandbox regulatório que lhe permite monitorar atentamente os experimentos na mineração de blockchain e criar a sua própria criptomoeda.
B) A Estônia oferece um programa de e-Residência, disponível para qualquer pessoa no mundo que tenha interesse em ter um negócio online dentro da União Europeia.
C) A Autoridade Monetária de Singapura (MAS) criou moeda digital do banco central para pagamentos entre bancos por meio da tecnologia de registro distribuído (DLT).

A) Incorreto. A China não possui sua própria criptomoeda.
B) Incorreto. A Estônia lançou as carteiras de identidades digitais para serviços online e passou a oferecer cidadania como um serviço, tornando-se o primeiro país a oferecer e-Residência. A Estônia cria uma identidade digital, disponível para qualquer pessoa no mundo que tenha interesse em ter um negócio online dentro da União Europeia. Entretanto, a e-Residência não é um software que pode ser distribuído nem promove exclusivamente a tecnologia blockchain.
C) Correto. A Autoridade Monetária de Singapura criou moeda digital do banco central usando DLT. A primeira fase do projeto começou em 2016, quando a Autoridade Monetária de Singapura demonstrou sua capacidade de realizar um pagamento interbancário doméstico usando um token equivalente ao dólar de Singapura emitido pelo banco central. (Literatura: A, Capítulo 9.2)

40 / 40
Por que se descreve o blockchain como a tecnologia que acrescenta uma camada de confiança à internet?

A) Por permitir a pessoas e grupos trabalhar juntos sem ter que confiar uns nos outros ou estabelecer autoridade
B) Por criar um túnel VPN dedicado entre duas ou mais partes para realizar transferência de fundos online
C) Por fornecer um mecanismo ao governo para criar a sua própria moeda fiduciária digital em substituição à moeda física
D) Por fornecer autenticação de múltiplos fatores para criar e atualizar registros de transações de criptomoeda de modo seguro

A) Correto. O blockchain permite a pessoas, governos e negócios trabalhar juntos de um modo justo e aberto, sem estabelecer anteriormente confiança, propriedade e autoridade. (Literatura: A, Capítulo 9.4)
B) Incorreto. A VPN não é uma aplicação da tecnologia blockchain.
C) Incorreto. A moeda fiduciária digital é uma das aplicações da tecnologia blockchain.
D) Incorreto. A tecnologia blockchain usa funções de hash para fornecer o traço de imutabilidade.

Avaliação

A tabela a seguir mostra as respostas corretas às questões apresentadas neste exame simulado.

Questão	Resposta	Questão	Resposta
1	C	**21**	C
2	C	**22**	B
3	C	**23**	B
4	C	**24**	D
5	D	**25**	C
6	B	**26**	B
7	D	**27**	C
8	A	**28**	C
9	D	**29**	C
10	A	**30**	A
11	C	**31**	D
12	H	**32**	B
13	C	**33**	D
14	D	**34**	D
15	D	**35**	C
16	C	**36**	A
17	A	**37**	B
18	C	**38**	B
19	C	**39**	C
20	A	**40**	A

Contato EXIN

www.exin.com