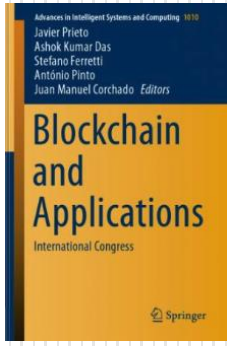
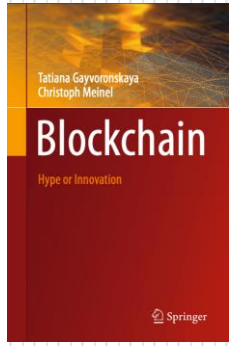
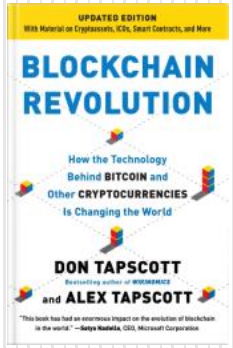
Blockchain

Revisão, com foco em exercícios

Prof. Fernando Escobar, PMP – MSc. https://www.linkedin.com/in/fernandoescobar/ @professorfernandoescobar







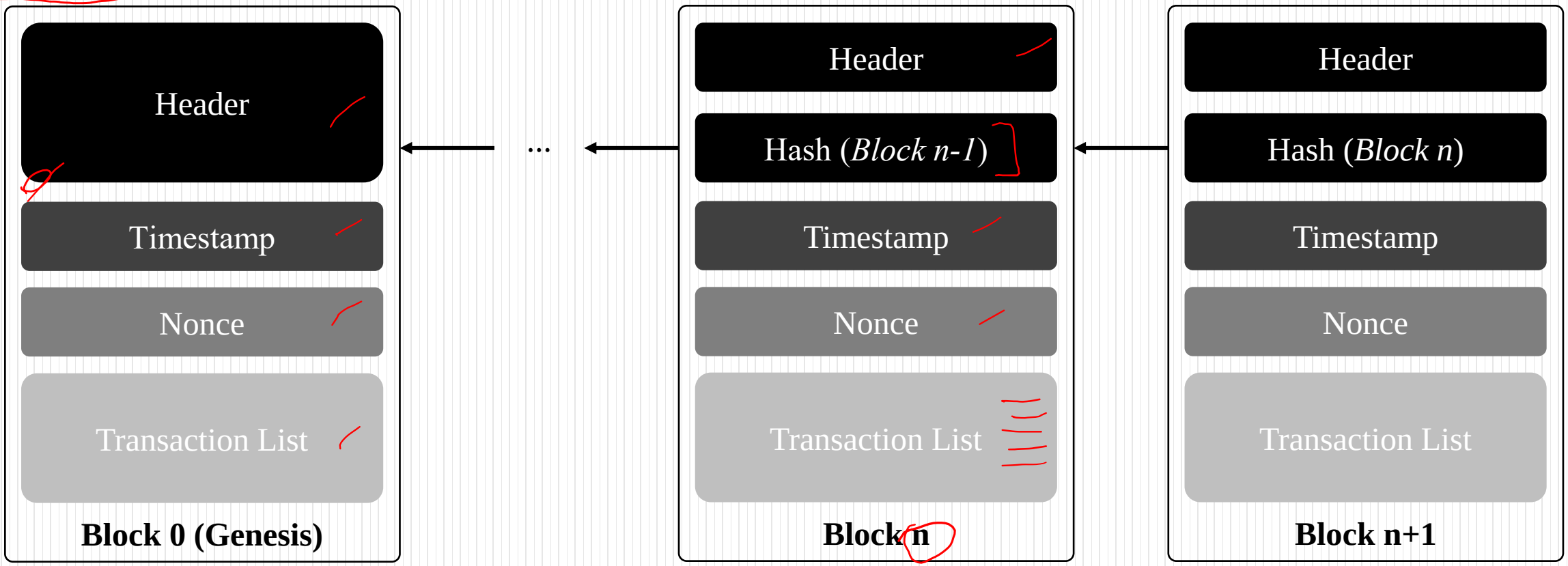
PROVAS DE TI
TUDO PARA VOCÊ PASSAR

BLOCKCHAIN

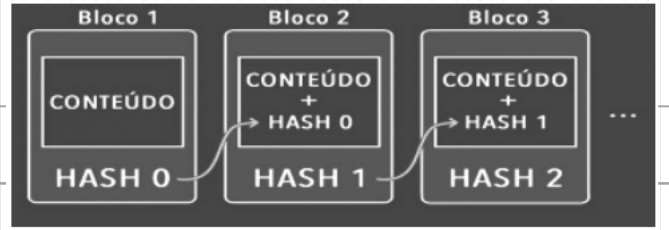
Conceitos

Uma blockchain é uma cadeia de blocos que pode ser usada para armazenar e compartilhar dados de maneira **distribuída, transparente e resistente a adulterações**.

Cada bloco consiste em dados e é vinculado a outros blocos usando ponteiros. Essa ligação em cadeia garante a integridade e resistência à violação na blockchain.



RESOLUÇÃO DE QUESTÃO



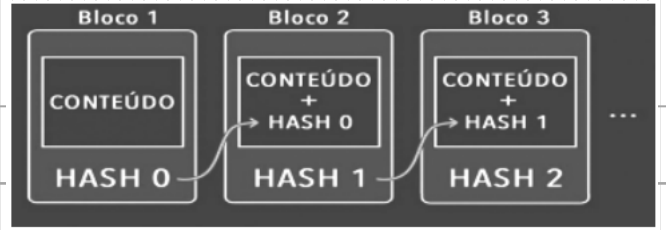
CESPE - Analista (SERPRO) / 2021

Julgue o item a seguir, relativo a blockchain e smart contracts.

De acordo com a seguinte figura, blockchain corresponde a uma lista ordenada de blocos em que cada bloco em um blockchain é encadeado ao bloco anterior, de maneira a conter um hash da representação do bloco anterior, e, assim, as transações históricas no blockchain não podem ser excluídas ou alteradas sem se invalidar a cadeia de hashes.

- Certo
- Errado

RESOLUÇÃO DE QUESTÃO



CESPE - Analista (SERPRO) / 2021

Julgue o item a seguir, relativo a blockchain e smart contracts.

De acordo com a seguinte figura, blockchain corresponde a uma lista ordenada de blocos em que cada bloco em um blockchain é encadeado ao bloco anterior, de maneira a conter um hash da representação do bloco anterior, e, assim, as transações históricas no blockchain não podem ser excluídas ou alteradas sem se invalidar a cadeia de hashes.

- ✅ Certo
- Errado

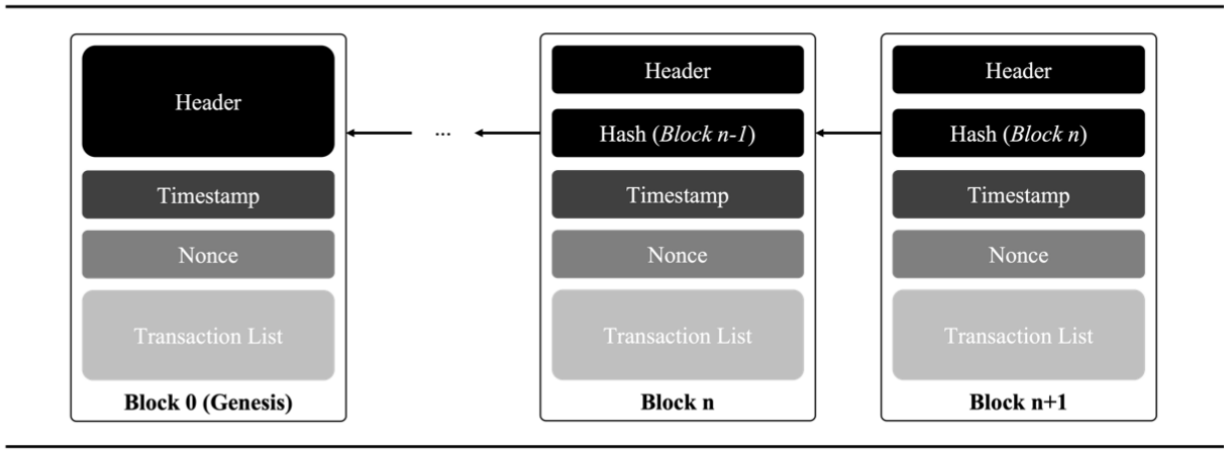


Figure 5. Blockchain block structure.

RESOLUÇÃO DE QUESTÃO

Quadrix - Assistente (CRN 4ª Região) / 2022
Existem diversas definições para o termo blockchain. Quando utilizado para nomear uma estrutura de dados, o termo blockchain refere-se a dados reunidos em unidades chamadas de blocos.
• Certo • Errado

RESOLUÇÃO DE QUESTÃO

Quadrix - Assistente (CRN 4ª Região) / 2022

Existem diversas definições para o termo blockchain. Quando utilizado para nomear uma estrutura de dados, o termo blockchain refere-se a dados reunidos em unidades chamadas de blocos.

- ✅ Certo
- Errado

Uma blockchain é uma cadeia de blocos que pode ser usada para armazenar e compartilhar dados de maneira **distribuída, transparente e resistente a adulterações**.

Cada bloco consiste em dados e é vinculado a outros blocos usando ponteiros. Essa ligação em cadeia garante a integridade e resistência à violação na blockchain.

RESOLUÇÃO DE QUESTÃO

IDIB – Assistente Técnico (CREMEPE) / 2021

“Armazena informações de forma cronológica em uma lista de blocos interligados que possuem um número de identificação próprio e outro de seu antecessor, visando identificar sua origem. Cada bloco armazena um conjunto de informações que também recebem um identificador único e imutável” (LUCENA; HENRIQUES, 2016). A definição acima se refere a uma tecnologia que, na visão de Swan (2015), tem a capacidade de modificar todos os setores da sociedade. Trata- se do

- a) Blockchain
- b) SIGAD
- c) Altcoins
- d) Criptos

RESOLUÇÃO DE QUESTÃO

IDIB – Assistente Técnico (CREMEPE) / 2021

“Armazena informações de forma cronológica em uma lista de blocos interligados que possuem um número de identificação próprio e outro de seu antecessor, visando identificar sua origem. Cada bloco armazena um conjunto de informações que também recebem um identificador único e imutável” (LUCENA; HENRIQUES, 2016). A definição acima se refere a uma tecnologia que, na visão de Swan (2015), tem a capacidade de modificar todos os setores da sociedade. Trata- se do

- a) Blockchain
- b) SIGAD
- c) Altcoins
- d) Criptos

BLOCKCHAIN

Conceitos

“

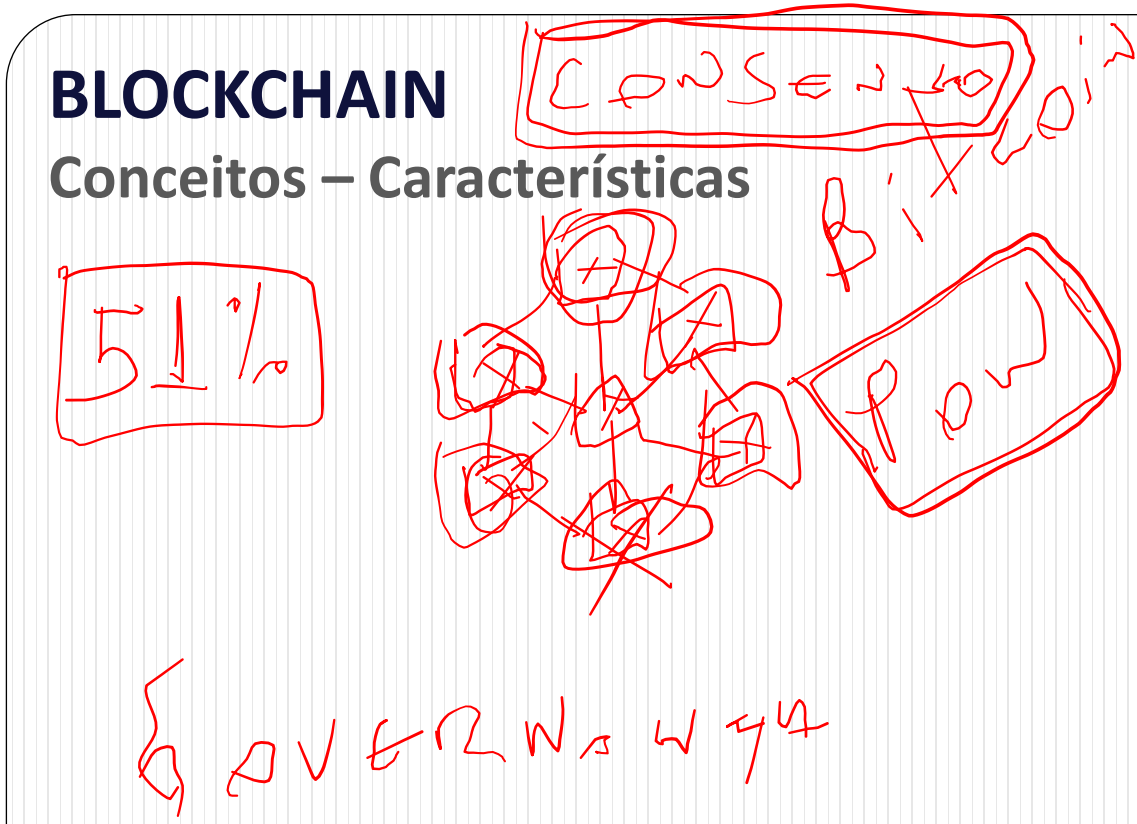
Blockchain (...) é distribuído: (...) não há banco de dados central para hackear.

Blockchain é público: qualquer um pode visualizá-lo a qualquer momento porque ele reside na rede, não dentro de uma única instituição encarregada de auditar transações e manter registros.

Blockchain é criptografado: usa criptografia pesada envolvendo chaves públicas e privadas (...) para manter a segurança virtual.” – Tapscott, 2018

BLOCKCHAIN

Conceitos – Características

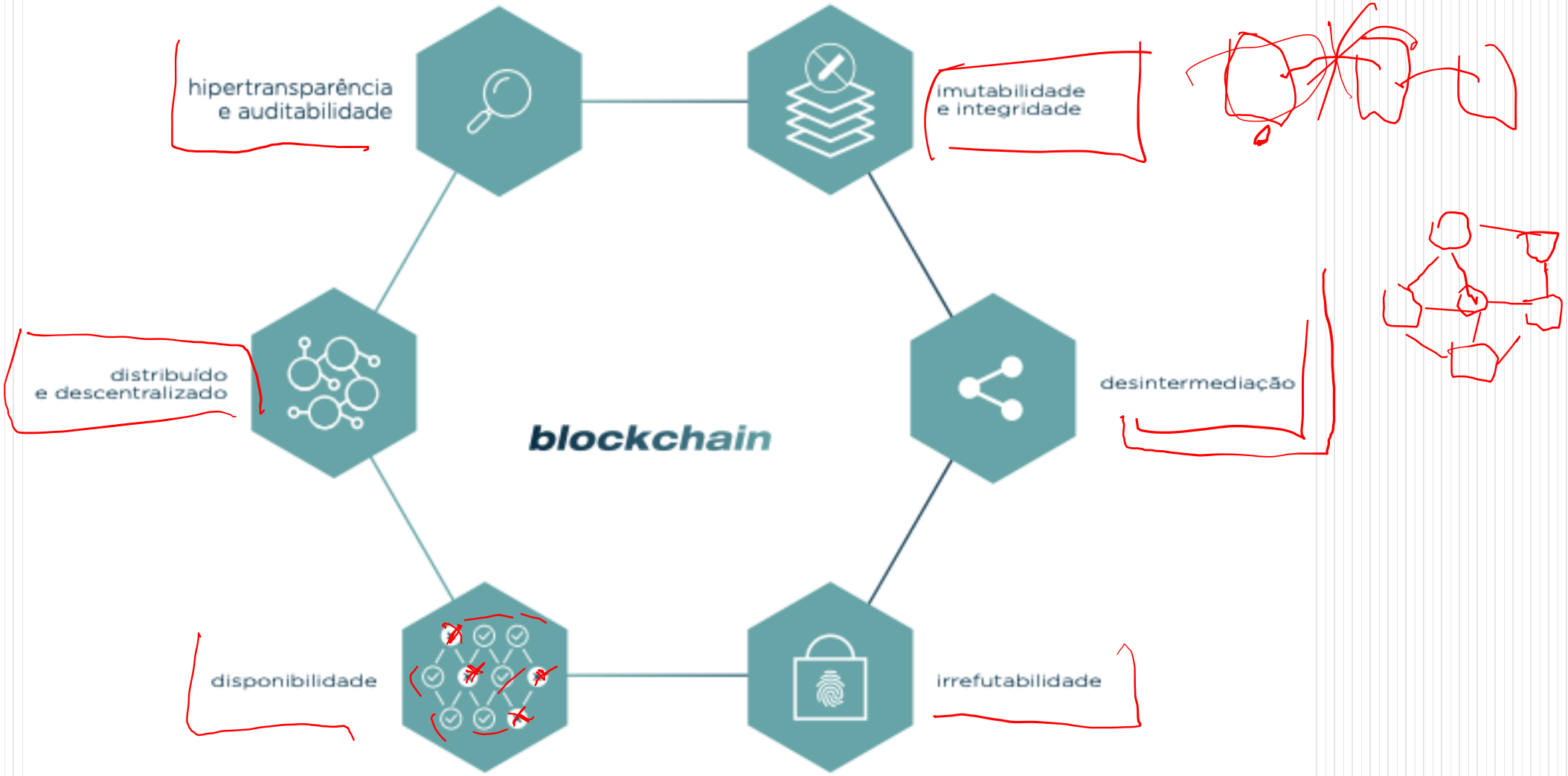


https://101blockchains.com/wp-content/uploads/2019/01/Caracter%C3%ADsticas-chaves-da-tecnologia-blockchain.png

BLOCKCHAIN

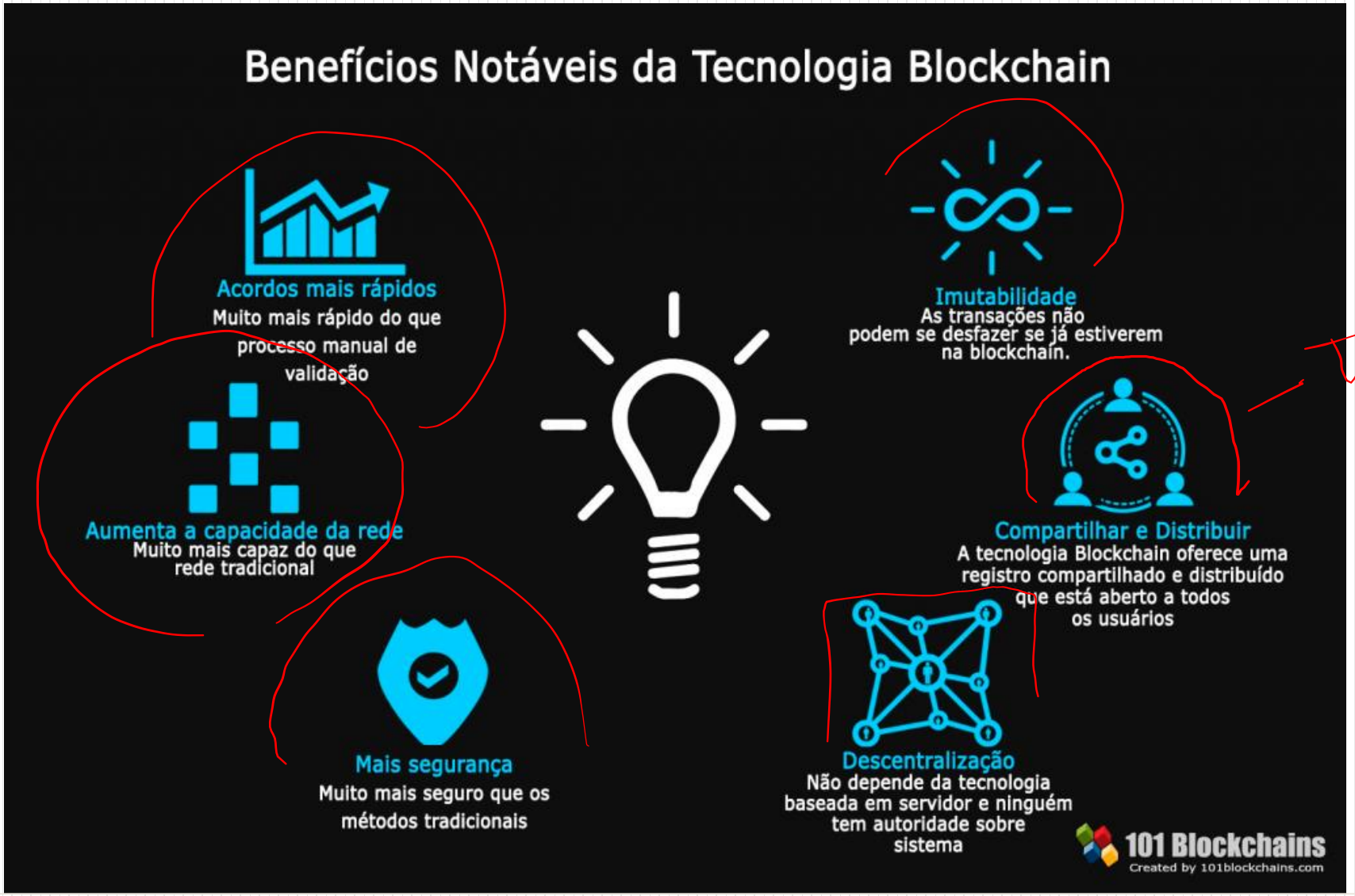
Conceitos – Propriedades

FIGURA 7 - PROPRIEDADES DA TECNOLOGIA *BLOCKCHAIN*



BLOCKCHAIN

Conceitos – Benefícios



https://ajuda.foxbit.com.br/wp-content/uploads/2021/03/Benefi%CC%81cios-nota%CC%81veis-da-tecnologia-Blockchain-1024x680.png

RESOLUÇÃO DE QUESTÃO

CESPE - Analista (SERPRO) / 2021

Julgue o item a seguir, relativo a blockchain e smart contracts.
Uma característica de blockchain é o fato de que seus registros de dados são mantidos em um banco de dados distribuído e são protegidos contra adulteração e revisão até mesmo dos operadores dos nós do armazenamento de dados.

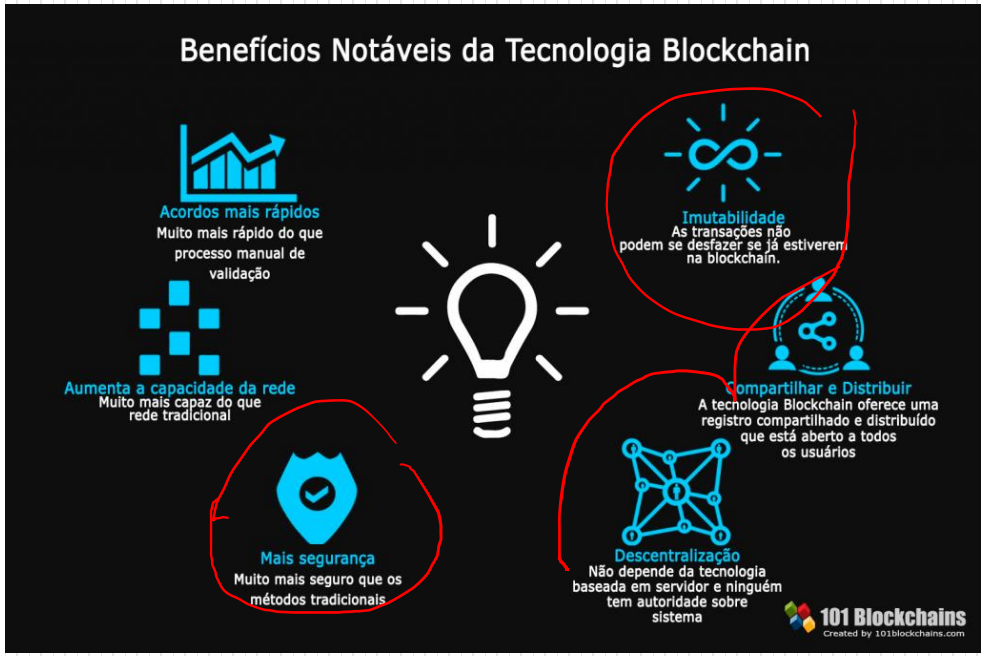
- Certo
- Errado

RESOLUÇÃO DE QUESTÃO

CESPE - Analista (SERPRO) / 2021

Julgue o item a seguir, relativo a blockchain e smart contracts.
Uma característica de blockchain é o fato de que seus registros de dados são mantidos em um banco de dados distribuído e são protegidos contra adulteração e revisão até mesmo dos operadores dos nós do armazenamento de dados.

- ✅ Certo
- Errado



CONSENSO

RESOLUÇÃO DE QUESTÃO

Quadrix - Assistente (CRN 4ª Região) / 2022
A blockchain é uma das novas tecnologias voltadas, exclusivamente, para a validação e a autenticação de informações bancárias. Essa ferramenta, entretanto, não consegue realizar algumas ações, como, por exemplo, prover integridade em sistemas de software distribuídos.
• Certo • Errado

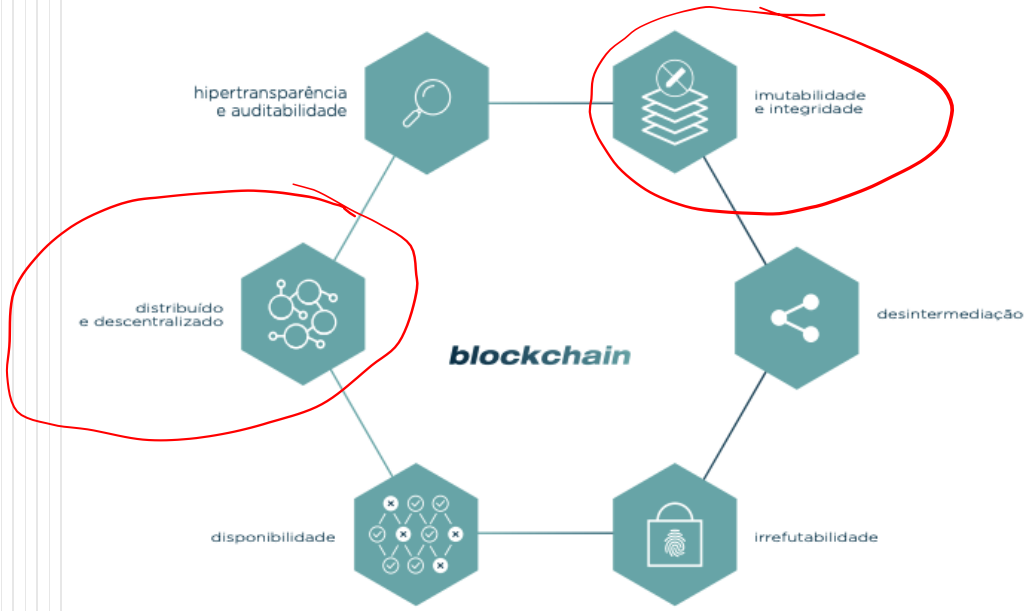
RESOLUÇÃO DE QUESTÃO

Quadrix - Assistente (CRN 4ª Região) / 2022

A blockchain é uma das novas tecnologias voltadas, exclusivamente, para a validação e a autenticação de informações bancárias. Essa ferramenta, entretanto, não consegue realizar algumas ações, como, por exemplo, prover integridade em sistemas de software distribuídos.

- Certo
- ✅ Errado

FIGURA 7 - PROPRIEDADES DA TECNOLOGIA *BLOCKCHAIN*



RESOLUÇÃO DE QUESTÃO

IADES – Escriturário (BRB) / 2019

Com base nas características e nas possíveis aplicações para a blockchain, assinale a alternativa correta.

- a) A blockchain é uma lista de tamanho fixo de registros interligados a partir de criptografia, em que cada bloco contém dados relativos à transação, um timestamp e um hash criptográfico do próximo bloco.
- b) A blockchain é uma espécie de base de dados pública e centralizada, que é usada para registrar transações na nuvem, de forma que qualquer registro envolvido não possa ser alterado retroativamente sem a alteração de todos os blocos subsequentes.
- c) Mesmo que fosse possível atacar e controlar mais de 50% de uma rede verificadora de transações blockchain, não seria possível reverter transações já realizadas ou realizar gastos duplos.
- d) A invenção da blockchain para uso no bitcoin tornou-o a primeira moeda digital a resolver o problema do gasto duplo sem a necessidade de envolver uma autoridade confiável ou servidor central como mediador. A blockchain remove a característica de reprodutibilidade infinita de um ativo digital.
- e) A blockchain demonstrou potencial apenas como base tecnológica para as criptomoedas, sendo, portanto, improvável que outras indústrias encontrem novas aplicações em razão das diversas limitações que apresentam.

RESOLUÇÃO DE QUESTÃO

IADES – Escriturário (BRB) / 2019

Com base nas características e nas possíveis aplicações para a blockchain, assinale a alternativa correta.

- a) A blockchain é uma lista de tamanho fixo de registros interligados a partir de criptografia, em que cada bloco contém dados relativos à transação, um timestamp e um hash criptográfico do próximo bloco.
- b) A blockchain é uma espécie de base de dados pública e centralizada, que é usada para registrar transações na nuvem, de forma que qualquer registro envolvido não possa ser alterado retroativamente sem a alteração de todos os blocos subsequentes.
- c) Mesmo que fosse possível atacar e controlar mais de 50% de uma rede verificadora de transações blockchain, não seria possível reverter transações já realizadas ou realizar gastos duplos.
- ✅ d) A invenção da blockchain para uso no bitcoin tornou-o a primeira moeda digital a resolver o problema do gasto duplo sem a necessidade de envolver uma autoridade confiável ou servidor central como mediador. A blockchain remove a característica de reprodutibilidade infinita de um ativo digital.
- e) A blockchain demonstrou potencial apenas como base tecnológica para as criptomoedas, sendo, portanto, improvável que outras indústrias encontrem novas aplicações em razão das diversas limitações que apresentam.

BLOCKCHAIN

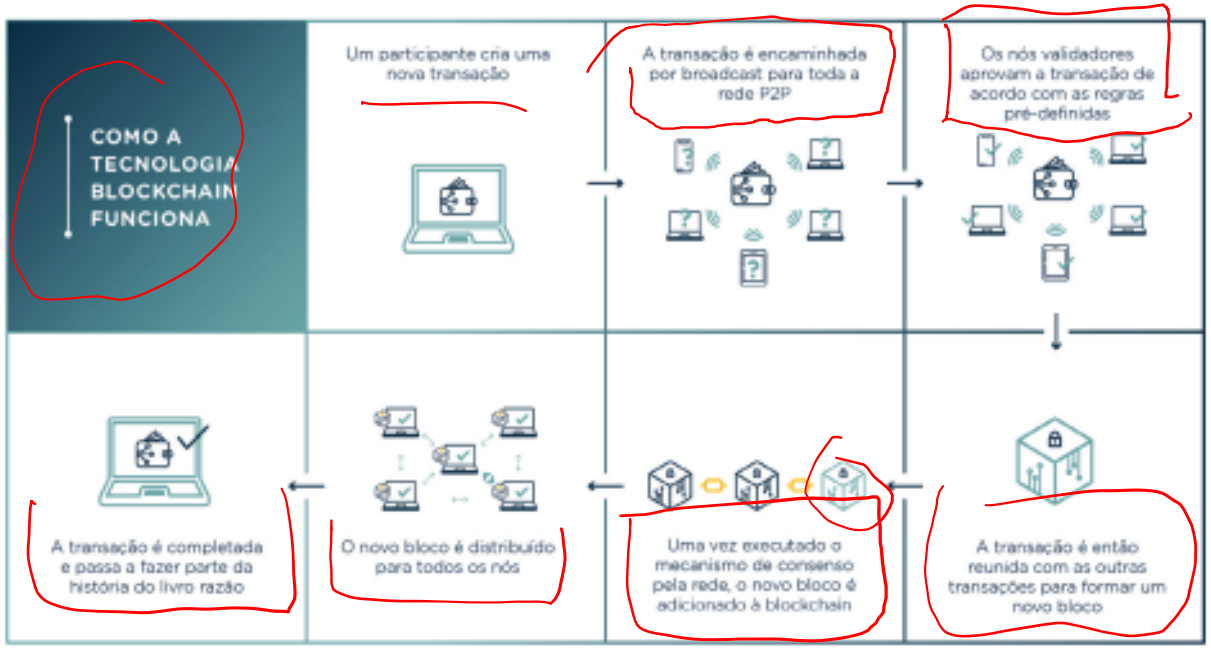
Conceitos – Transação

Na blockchain, cada nova transação é registrada em um bloco compartilhado e sincronizado por vários nós, em uma abordagem de **livro-razão distribuído digitalmente, sem controle central**.

Mecanismos de consenso fornecem segurança à blockchain e uma forma de verificar sua precisão, sustentando sua irrevogabilidade.

A blockchain armazena as informações exatas, ordenadas cronologicamente, em nós distintos, e as informações só serão adicionadas quando os nós tiverem consenso.

FIGURA 3 - FUNCIONAMENTO GENÉRICO DE UMA *BLOCKCHAIN*



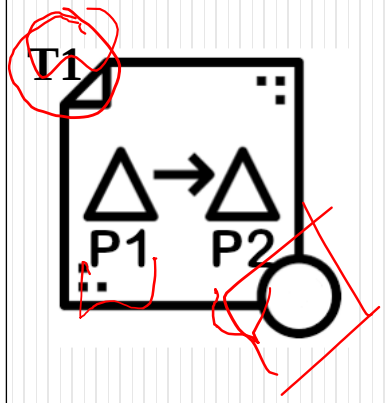
FONTE: COMISSÃO EUROPEIA (ADAPTADO)

BLOCKCHAIN

Conceitos – Transação

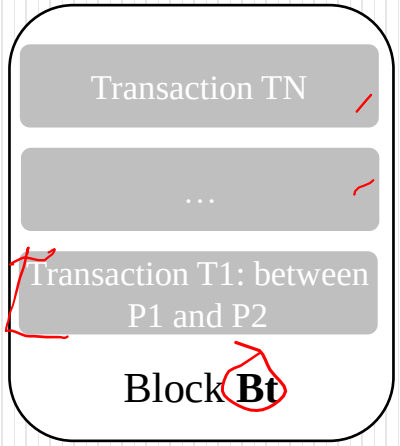
1. Transaction requested

P1 broadcasts the transaction **T1** (between **P1** to **P2**) to the network



2. Mining

Each node gathers a set of transactions into one block **Bt**

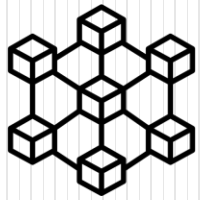


3. Broadcast

One node broadcasts the mined-block **Bt** to all peers in the network

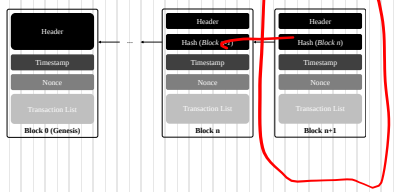
4. Validation

Validation of the block **Bt** by all the peers in the network



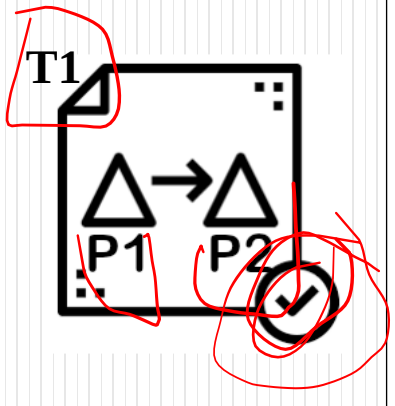
5. Adding

Each node adds the block **Bt** to the blockchain



6. Transaction completed

The transaction **T1** is complete between **P1** and **P2**



RESOLUÇÃO DE QUESTÃO

FUNDATEC – Analista de Planejamento, Orçamento e Gestão (SPGG-RS) / 2022

De uma forma geral, um(a) _____ é um software que funciona como um livro-razão distribuído pelos nós de uma rede. O que distingue esse livro-razão dos bancos de dados ou softwares tradicionais é a sua natureza de resistência à adulteração, pois a alteração dos dados de um bloco requer a manipulação de todos os outros blocos anteriores. Assinale a alternativa que preenche corretamente a lacuna do trecho acima.

- a) Transformação digital
- b) Contrato inteligente
- c) Registro imutável
- d) Blockchain
- e) Repositório compartilhado

RESOLUÇÃO DE QUESTÃO

FUNDATEC – Analista de Planejamento, Orçamento e Gestão (SPGG-RS) / 2022

De uma forma geral, um(a) _____ é um software que funciona como um livro-razão distribuído pelos nós de uma rede. O que distingue esse livro-razão dos bancos de dados ou softwares tradicionais é a sua natureza de resistência à adulteração, pois a alteração dos dados de um bloco requer a manipulação de todos os outros blocos anteriores. Assinale a alternativa que preenche corretamente a lacuna do trecho acima.

- a) Transformação digital
- b) Contrato inteligente
- c) Registro imutável
- ✅ d) Blockchain
- e) Repositório compartilhado

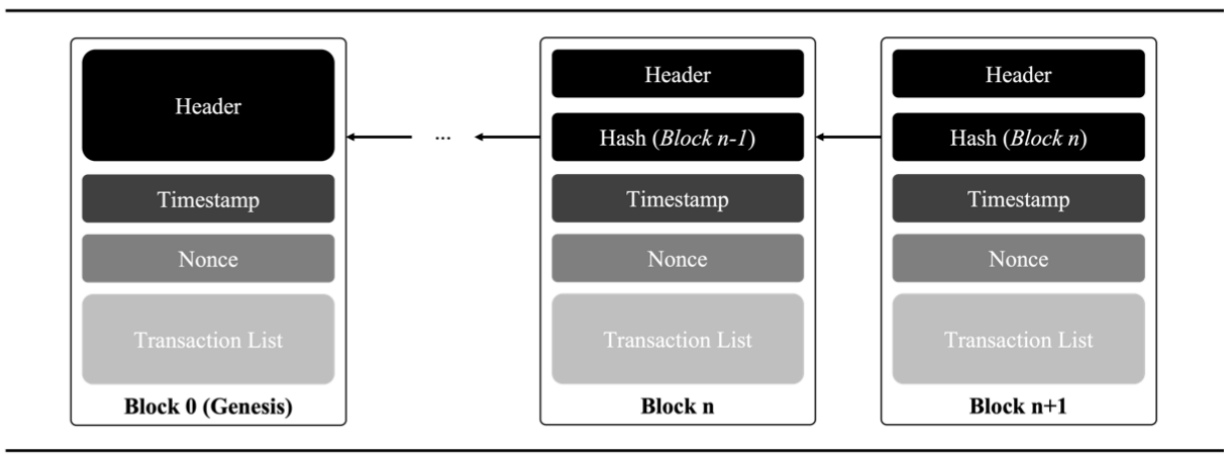


Figure 5. Blockchain block structure.

RESOLUÇÃO DE QUESTÃO

CESGRANRIO – Escriturário (Banco do Brasil) / 2021

A blockchain é um tipo específico de banco de dados distribuído, no qual há uma cadeia de blocos ordenados e interligados, com garantia de ordem cronológica. Os dados registrados nos blocos podem variar de transações financeiras a contratos inteligentes. Na blockchain da bitcoin, as entidades que registram novos blocos na cadeia são chamadas de

- a) registradores
- b) mineradores
- c) trabalhadores
- d) gerenciadores
- e) conectores

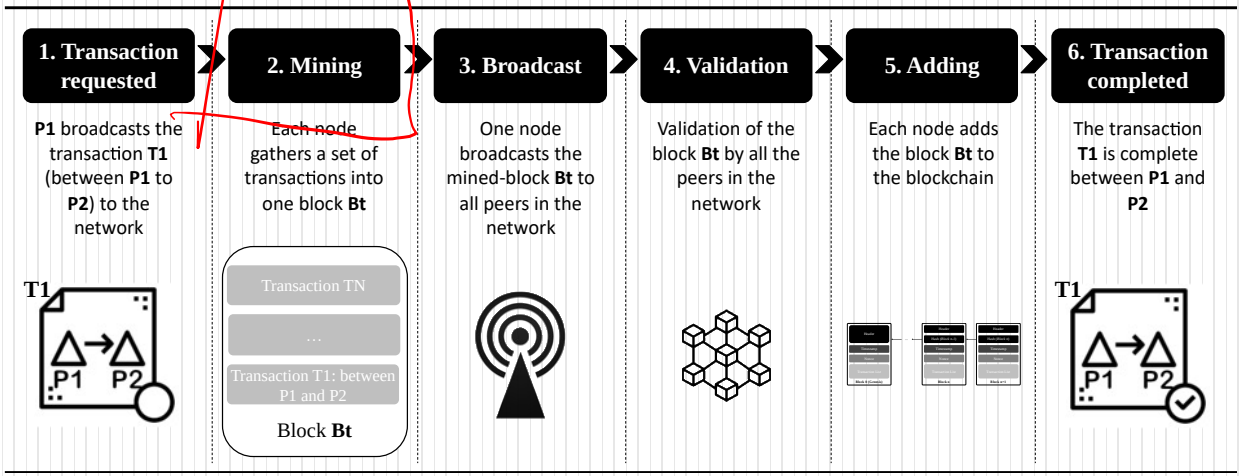
RESOLUÇÃO DE QUESTÃO

CESGRANRIO – Escriturário (Banco do Brasil) / 2021

A blockchain é um tipo específico de banco de dados distribuído, no qual há uma cadeia de blocos ordenados e interligados, com garantia de ordem cronológica. Os dados registrados nos blocos podem variar de transações financeiras a contratos inteligentes. Na blockchain da bitcoin, as entidades que registram novos blocos na cadeia são chamadas de

- a) registradores
- ✅ b) mineradores
- c) trabalhadores
- d) gerenciadores
- e) conectores

MINERAÇÃO



RESOLUÇÃO DE QUESTÃO

CESPE – Professor IC (SEED-PR) / 2021

Existe uma tecnologia que torna o livro-razão independente de aplicativos e de participantes individuais, replicando-o em uma rede distribuída para criar um registro consensual de autoridade de eventos significativos. Nesse contexto, o livro-razão distribuído é uma lista de registros transacionais irrevogáveis assinados criptograficamente, sendo essa lista ordenada cronologicamente e compartilhada por todos os participantes de uma rede.
Assinale a opção que apresenta o nome da tecnologia de que trata o texto anterior.

- a) rede virtual privada (VPN, do inglês Virtual Private Network)
- b) blockchain
- c) criptografia por chave simétrica
- d) criptografia por chave pública
- e) HTTPS (hypertext transfer protocol secure)

RESOLUÇÃO DE QUESTÃO

CESPE – Professor IC (SEED-PR) / 2021

Existe uma tecnologia que torna o livro-razão independente de aplicativos e de participantes individuais, replicando-o em uma rede distribuída para criar um registro consensual de autoridade de eventos significativos. Nesse contexto, o livro-razão distribuído é uma lista de registros transacionais irrevogáveis assinados criptograficamente, sendo essa lista ordenada cronologicamente e compartilhada por todos os participantes de uma rede.
Assinale a opção que apresenta o nome da tecnologia de que trata o texto anterior.

- a) rede virtual privada (VPN, do inglês Virtual Private Network)
- ✅ b) blockchain
- c) criptografia por chave simétrica
- d) criptografia por chave pública
- e) HTTPS (hypertext transfer protocol secure)

FIGURA 3 - FUNCIONAMENTO GENÉRICO DE UMA *BLOCKCHAIN*

FONTE: COMISSÃO EUROPEIA (ADAPTADO)

RESOLUÇÃO DE QUESTÃO

IPEFAE – Advogado (Pref. Águas da Prata - SP) / 2021

As inovações digitais atuais continuam a surpreender pela criatividade e impacto que determinam em diversos estratos sociais, como as presentes nas denominadas redes sociais e na Inteligência artificial, com o emprego de diversificados algoritmos. Uma funcionalidade recente bem impactante que exibe enorme potencial é a de blockchain, que consiste em uma tecnologia de registro distribuído, que visa a descentralização como medida de segurança. São bases de registros e dados distribuídos e compartilhados que tem a função de criar um índice global para todas as transações que ocorrem em um determinado mercado. Sobre esta inovação, assinale abaixo a alternativa que contém informação **incorreta** sobre a mesma:

- a) A blockchain funciona como um livro-razão só que de forma pública, compartilhada e universal, que cria consenso e confiança na comunicação direta entre duas partes (ou seja, sem o intermédio de terceiros).
- b) A blockchain cresce constantemente na medida em que novos blocos completos são adicionados a ela por um novo conjunto de registros. Os blocos não são adicionados de modo linear e cronológico, mas aleatórios e salteados num determinado espaço de tempo, o que confere flexibilidade e massividade ao sistema.
- c) A blockchain é vista como a principal inovação tecnológica do bitcoin, visto que é a prova de todas as transações na rede.
- d) O projeto original do blockchain tem servido de inspiração para o surgimento de novas criptomoedas e de bancos de dados distribuídos.

RESOLUÇÃO DE QUESTÃO

IPEFAE – Advogado (Pref. Águas da Prata - SP) / 2021

As inovações digitais atuais continuam a surpreender pela criatividade e impacto que determinam em diversos estratos sociais, como as presentes nas denominadas redes sociais e na Inteligência artificial, com o emprego de diversificados algoritmos. Uma funcionalidade recente bem impactante que exibe enorme potencial é a de blockchain, que consiste em uma tecnologia de registro distribuído, que visa a descentralização como medida de segurança. São bases de registros e dados distribuídos e compartilhados que tem a função de criar um índice global para todas as transações que ocorrem em um determinado mercado. Sobre esta inovação, assinale abaixo a alternativa que contém informação **incorreta** sobre a mesma:

- a) A blockchain funciona como um livro-razão só que de forma pública, compartilhada e universal, que cria consenso e confiança na comunicação direta entre duas partes (ou seja, sem o intermédio de terceiros).
- b) A blockchain cresce constantemente na medida em que novos blocos completos são adicionados a ela por um novo conjunto de registros. Os blocos não são adicionados de modo linear e cronológico, mas aleatórios e salteados num determinado espaço de tempo, o que confere flexibilidade e massividade ao sistema.
- c) A blockchain é vista como a principal inovação tecnológica do bitcoin, visto que é a prova de todas as transações na rede.
- d) O projeto original do blockchain tem servido de inspiração para o surgimento de novas criptomoedas e de bancos de dados distribuídos.

Blockchain

Tecnologias principais (core technologies)

BLOCKCHAIN

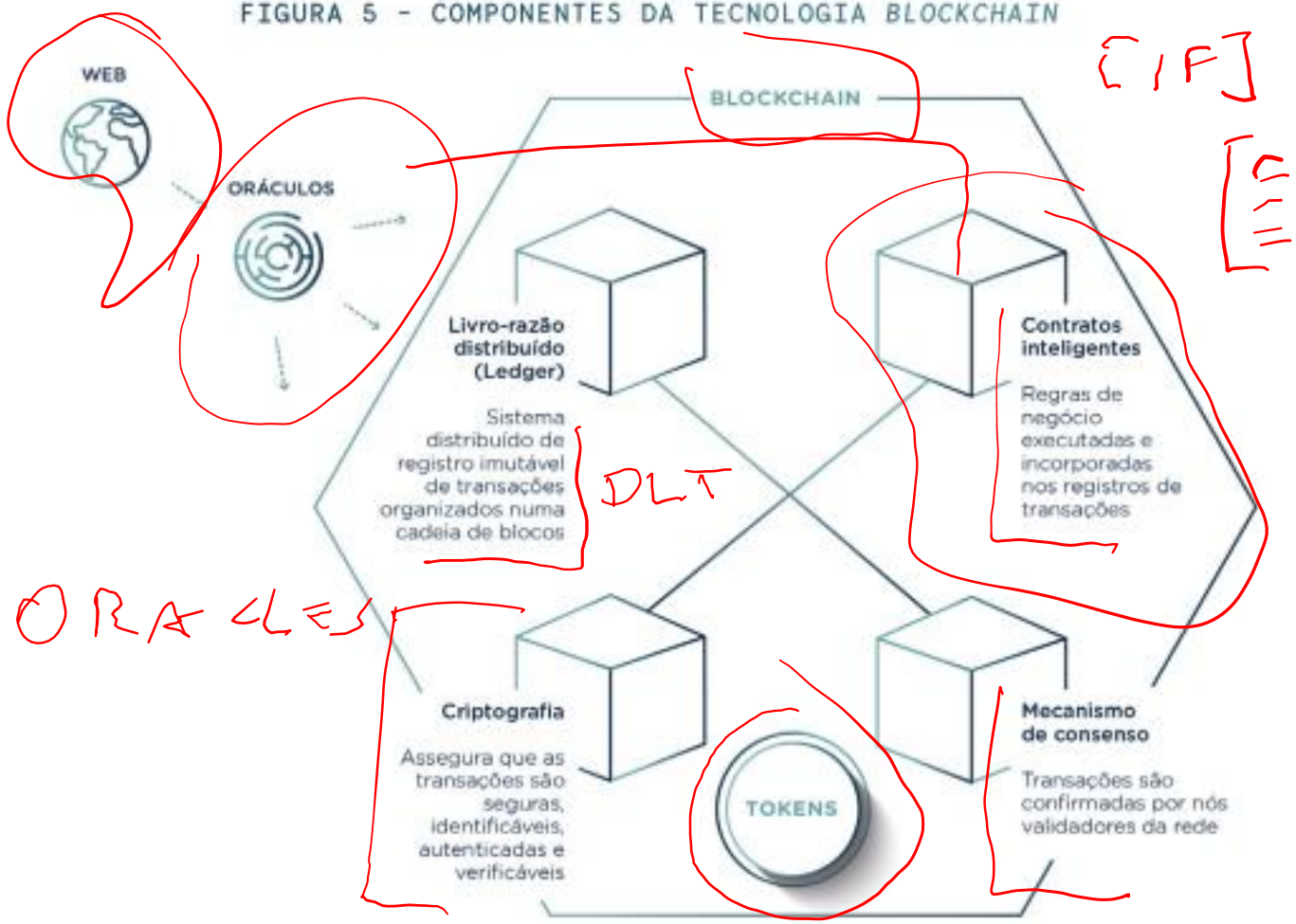
Core Technologies

“

Blockchain é a integração de core technologies como um livro-razão distribuído (**Distributed Ledger Technology – DLT**) que usa **mecanismos de consenso** para transmitir dados, com **criptografia de chave pública** para garantir transmissão e segurança, e aplica contratos inteligentes (**Smart Contracts**) para executar transações.

Tasca e Tessone (2017)

FIGURA 5 - COMPONENTES DA TECNOLOGIA *BLOCKCHAIN*



RESOLUÇÃO DE QUESTÃO

CESPE - Analista (SERPRO) / 2021

Julgue o item a seguir, relativo a blockchain e smart contracts.
Blockchain é uma plataforma de código aberto que foi a primeira capaz de executar a tecnologia de contratos inteligentes e aplicações descentralizadas, oferecendo confiança e consenso nas informações trocadas entre seus usuários.

- Certo
- Errado

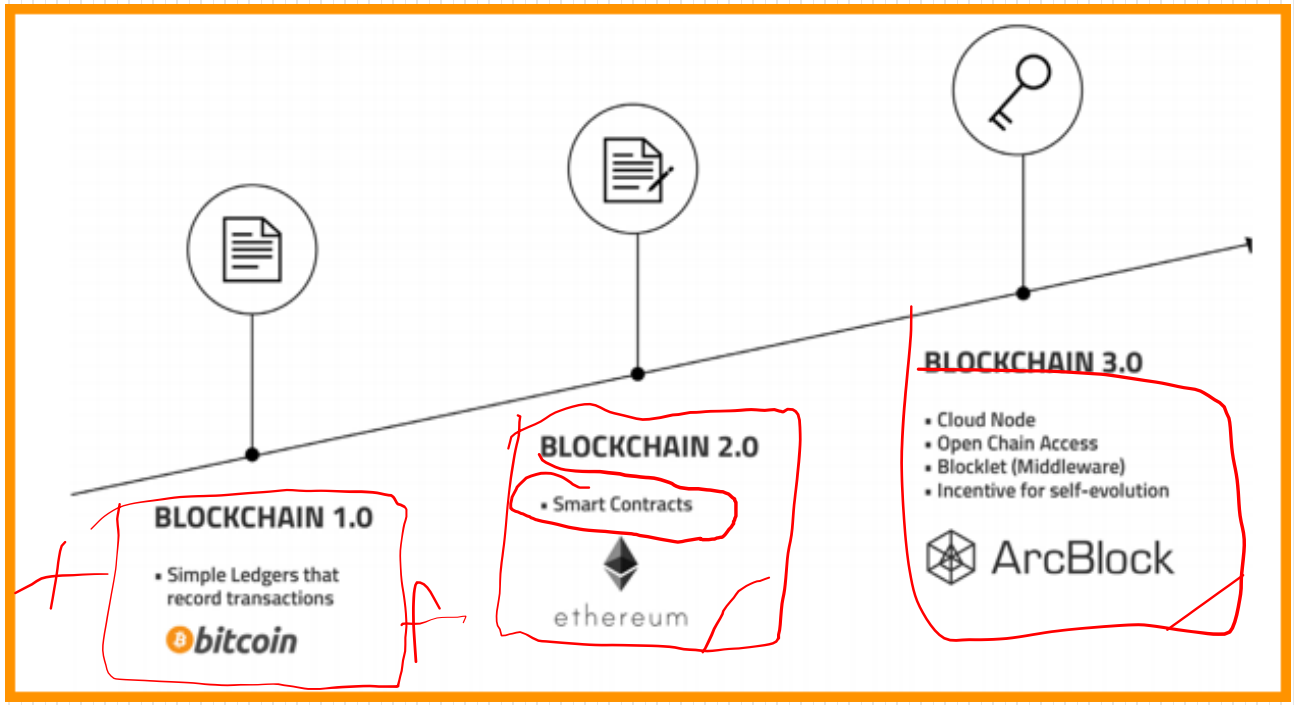
RESOLUÇÃO DE QUESTÃO

CESPE - Analista (SERPRO) / 2021

Julgue o item a seguir, relativo a blockchain e smart contracts.

Blockchain é uma plataforma de código aberto que foi a primeira capaz de executar a tecnologia de contratos inteligentes e aplicações descentralizadas, oferecendo confiança e consenso nas informações trocadas entre seus usuários.

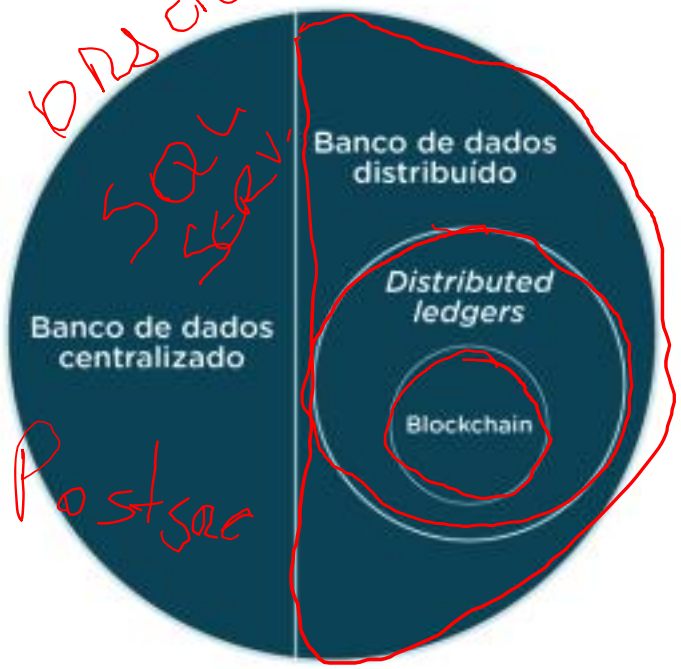
- Certo
- ✅ Errado



BLOCKCHAIN

Core Technologies – Distributed Ledger Technology (DLT)

FIGURA 4 - DIFERENÇA ENTRE TECNOLOGIAS



Banco de dados distribuído

- não existe um "*master database*" central;
- provê um grau de tolerância a falhas caso alguns nós falhem;
- banco de dados tradicionais são, em geral, operados por uma entidade única que mantém um estrito controle de acesso para a rede;

***Distributed Ledger Technology* (DLT)**

- mecanismo de consenso é baseado em um modelo de ameaças de adversários, assumindo que nem todos participantes são honestos;
- o banco de dados deve ser capaz de sincronizar e executar mesmo se um certo número de nós estão agindo de forma maliciosa;
- nós individuais precisam ser capazes de: **a)** verificar e validar, de forma independente, transações que alteram o estado do banco de dados e **b)** recriar todo o histórico de transações, de forma independente;

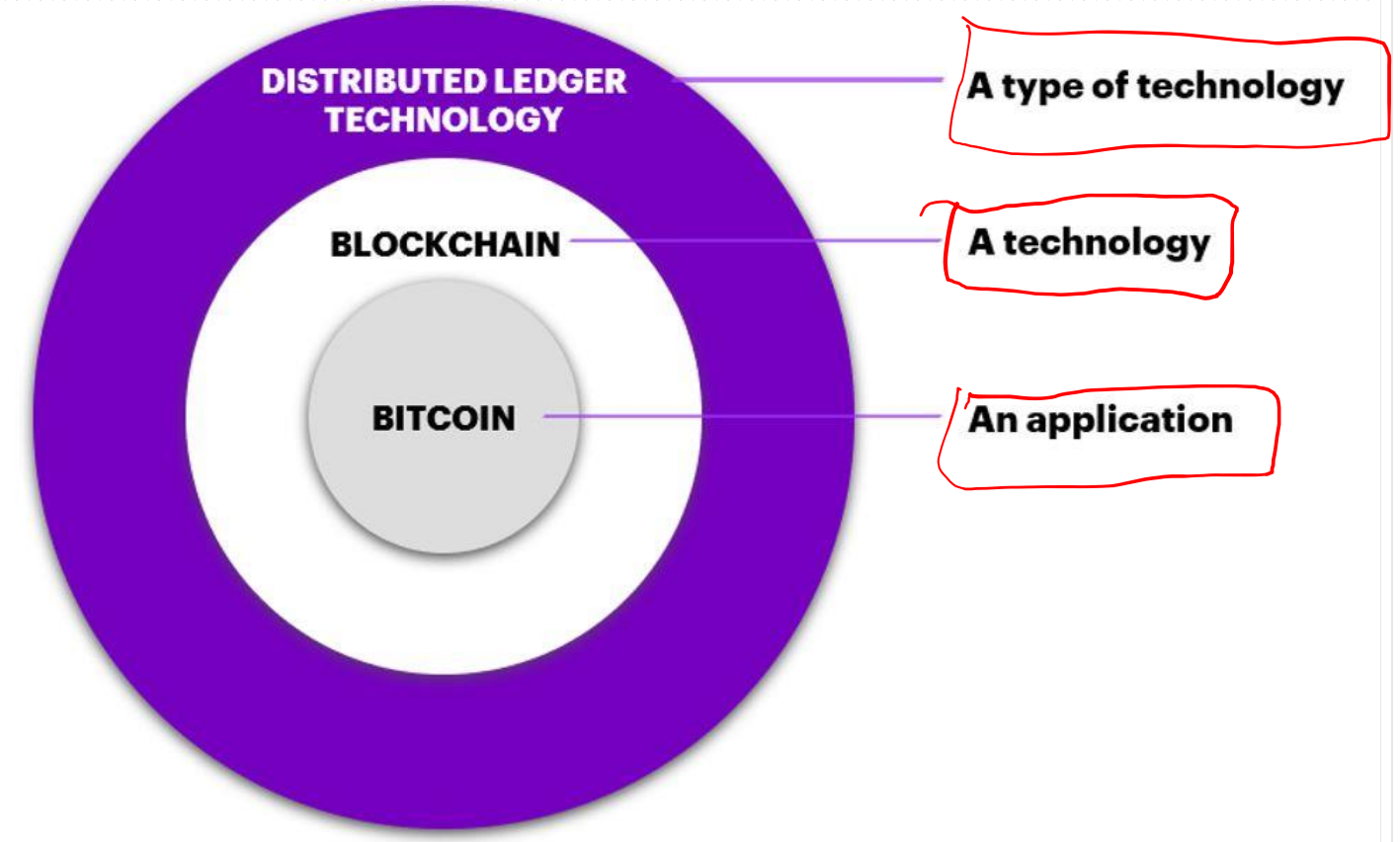
Blockchain

- usa uma estrutura de dados especial, *append-only*, que é composta por transações em lotes de blocos, os quais são ligados sequencialmente de forma inviolável, determinando a ordem das transações no sistema;

FONTE: UNIVERSIDADE DE BERKELEY E FÓRUM ECONÔMICO MUNDIAL (ADAPTADOS)

BLOCKCHAIN

Core Technologies – Distributed Ledger Technology (DLT)



https://acn-marketing-blog.accenture.com/wp-content/uploads/2020/04/Redefining-blockchain-image-1.jpg

RESOLUÇÃO DE QUESTÃO

CESGRANRIO – Escriturário (Banco do Brasil) / 2021

Uma investidora está querendo saber a relação entre a blockchain e o bitcoin.
Em sua pesquisa, ela esclareceu sua dúvida, ao descobrir que

- a) blockchain é o meio utilizado para registrar e armazenar transações de bitcoin
- b) blockchain é a tecnologia de inteligência artificial aplicada na bitcoin
- c) bitcoin é uma moeda digital e blockchain é uma moeda em blocos
- d) bitcoin é tecnologia usada para implementar a blockchain
- e) bitcoin e blockchain são duas formas de implementar criptomoedas

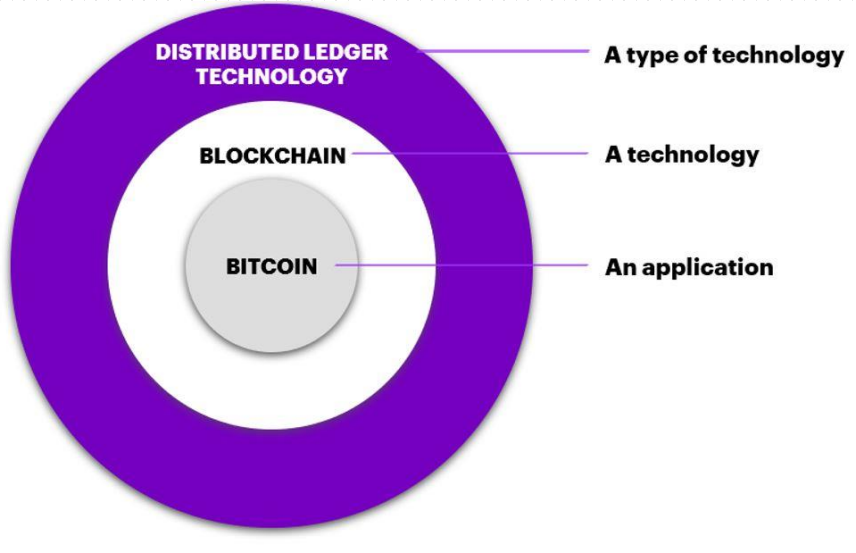
RESOLUÇÃO DE QUESTÃO

CESGRANRIO – Escriturário (Banco do Brasil) / 2021

Uma investidora está querendo saber a relação entre a blockchain e o bitcoin.
Em sua pesquisa, ela esclareceu sua dúvida, ao descobrir que

✅a) blockchain é o meio utilizado para registrar e armazenar transações de bitcoin

- b) blockchain é a tecnologia de inteligência artificial aplicada na bitcoin
- c) bitcoin é uma moeda digital e blockchain é uma moeda em blocos
- d) bitcoin é tecnologia usada para implementar a blockchain
- e) bitcoin e blockchain são duas formas de implementar criptomoedas



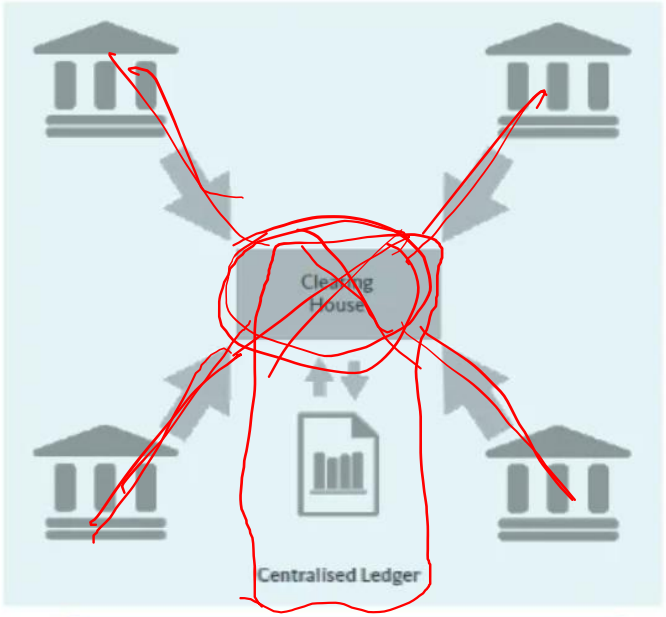
BLOCKCHAIN

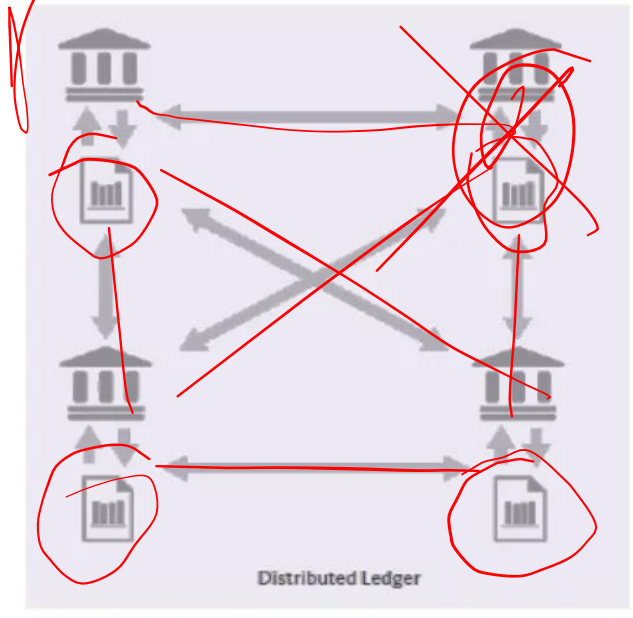
Core Technologies – Distributed Ledger Technology (DLT)

Um livro-razão distribuído é essencialmente um **banco de dados de ativos que pode ser compartilhado** em uma rede de vários sites, geografias ou instituições.

Todos **os participantes de uma rede podem ter sua própria cópia** idêntica do livro-razão.

Quaisquer **alterações no livro-razão são refletidas em todas as cópias** em minutos ou, em alguns casos, em segundos.





Tradicional

Centralizado
Rede Permissionada
Banco de dados Centralizado
Trusted Organization

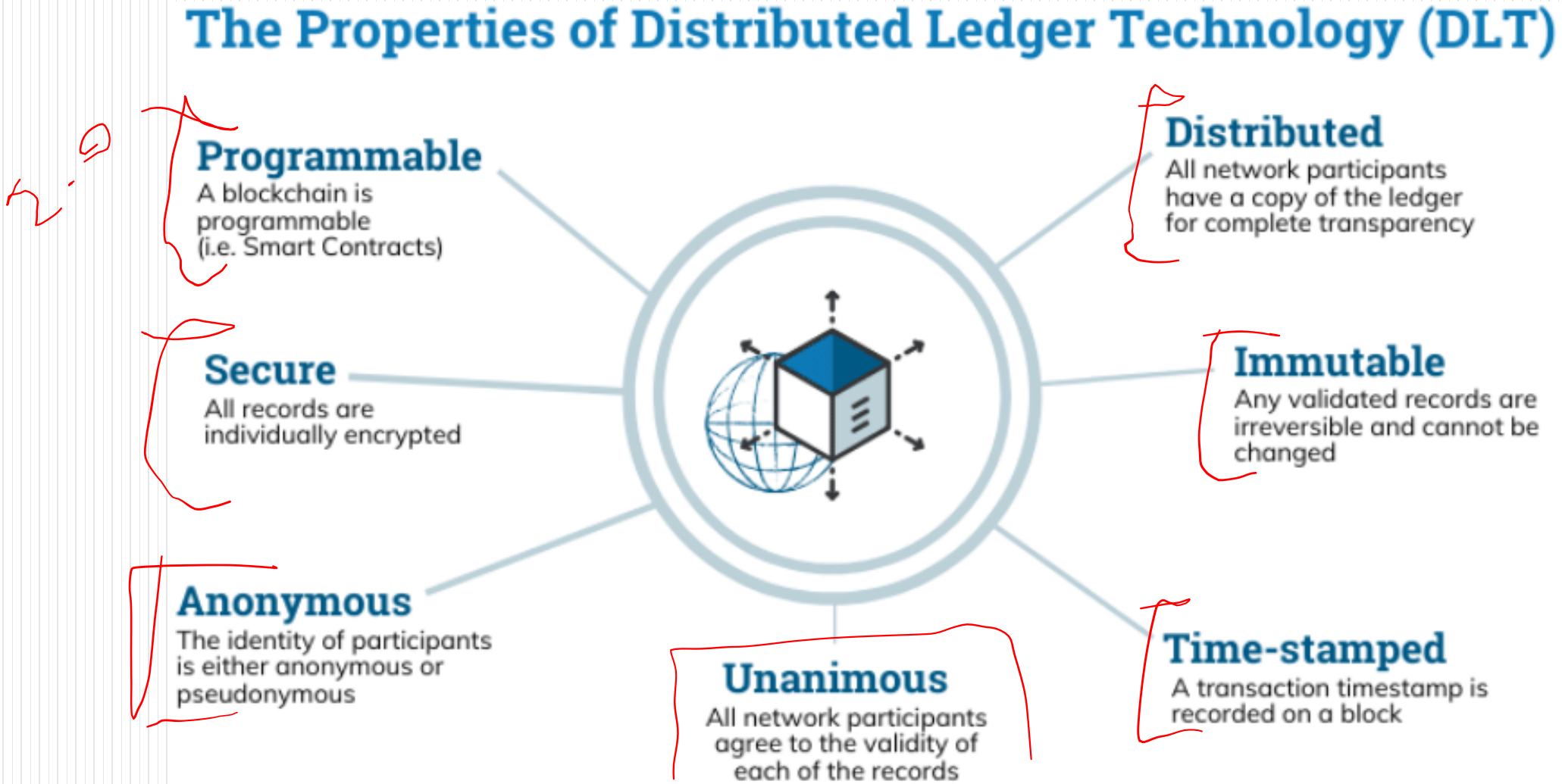
DLT

Descentralizado
Rede Permissionada ou não
Banco de dados Distribuído
Untrusted Organization

https://cdn.ttgtmedia.com/rms/onlineimages/cio-distributed__vs_central_ledger-f_mobile.png

BLOCKCHAIN

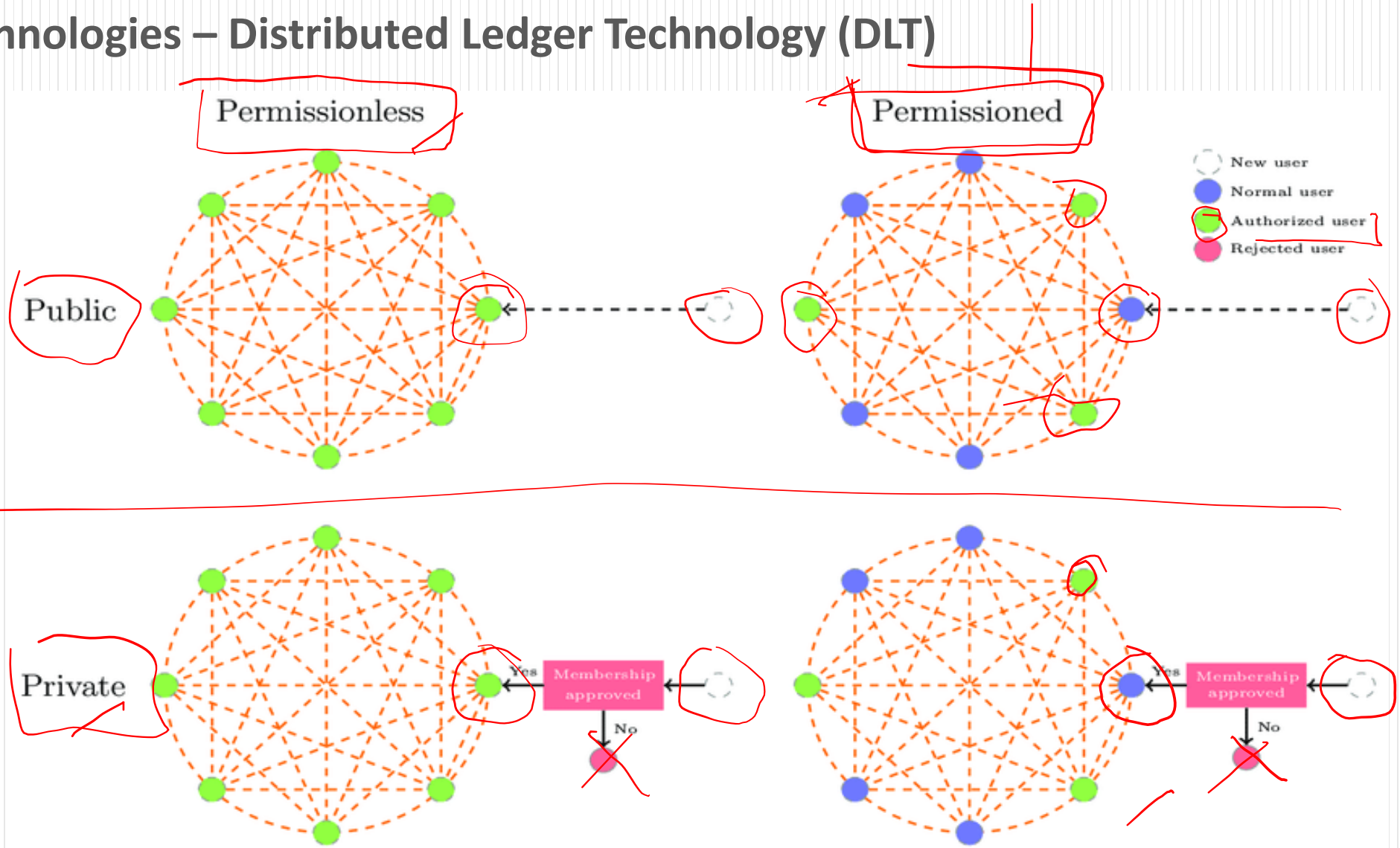
Core Technologies – Distributed Ledger Technology (DLT)



https://www.researchgate.net/profile/Mrityunjay-Ghosh/publication/355223429/figure/fig1/AS:1079123124457479@1634294410909/The-properties-of-distributed-ledger-technology-39.ppm

BLOCKCHAIN

Core Technologies – Distributed Ledger Technology (DLT)

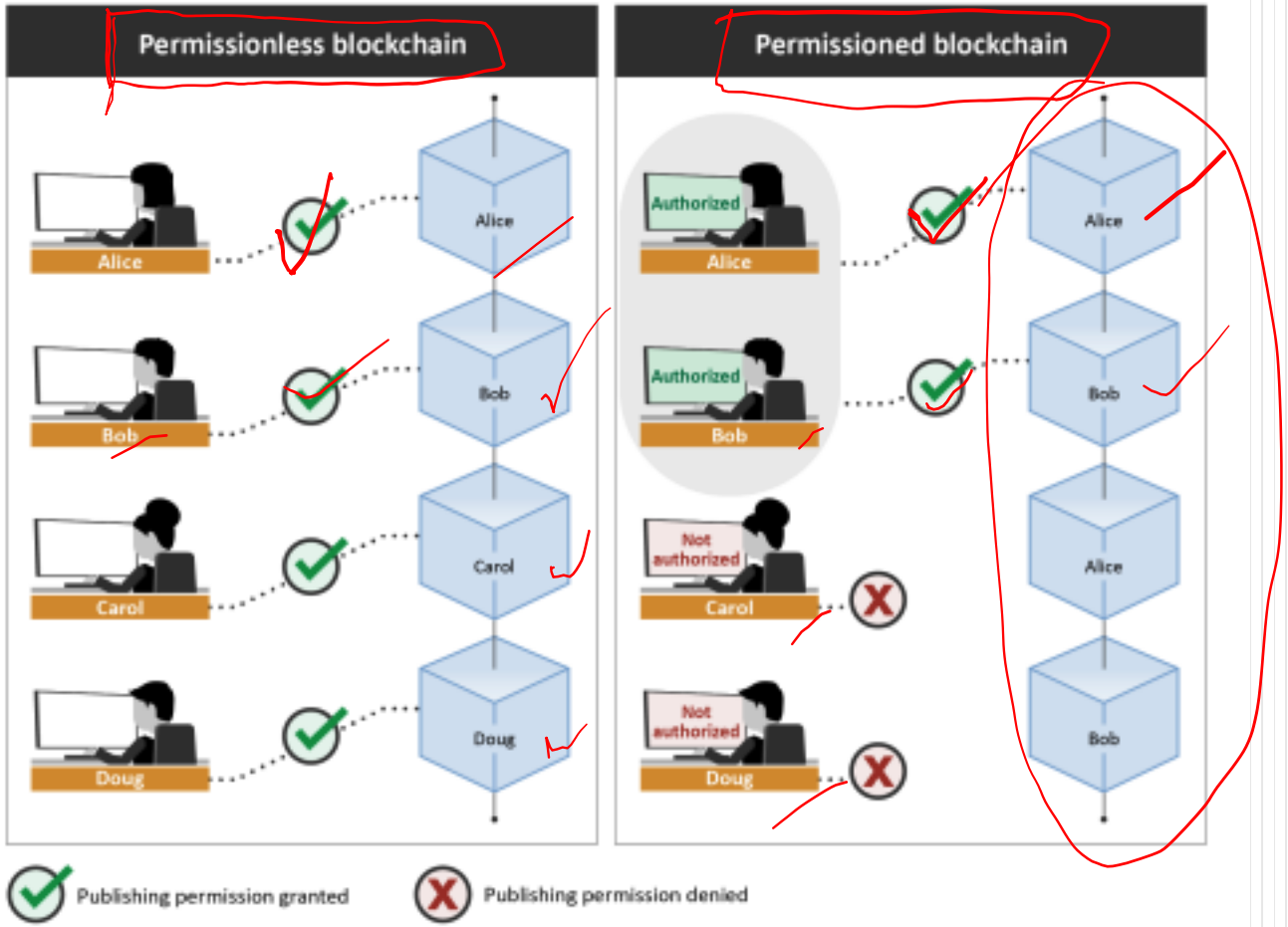


https://www.researchgate.net/profile/Muhammad-Fahad-Zia/publication/338623380/figure/fig3/AS:850307034669059@1579740403727/Classification-of-DLT-architectures-based-on-network-access-and-authorization.png

BLOCKCHAIN

Core Technologies – Distributed Ledger Technology (DLT)

Figure 4: Comparing a permissionless blockchain to a permissioned blockchain



Source: GAO. | GAO-22-104625

https://www.gao.gov/assets/gao-22-104625.pdf

RESOLUÇÃO DE QUESTÃO

FCC – Analista (METRO-SP) / 2019

Considere o fragmento de texto abaixo.

Um dos tipos de sistemas distribuídos em franco crescimento atualmente utiliza criptografia assimétrica para garantir segurança nas transações sem um agente de confiança intermediador. Essas transações são agrupadas e armazenadas em unidades encadeadas e interligadas por meio de códigos hash, de forma que a unidade seguinte indique o hash da unidade anterior. Todas as transações realizadas no sistema são registradas em uma espécie de livro de registros, de acesso público, permitindo a rastreabilidade das transações na rede. Dentre as aplicações desse tipo de sistema distribuído estão as Decentralized Application – DAPP e smart contracts.

O sistema distribuído e o local onde são registradas as transações do sistema são, respectivamente,.

- a) Blockchain e Immutable Ledger.
- b) Common Object Request Broker e Trezor.
- c) Common Object Request Broker e Immutable Consensus Book.
- d) Remote Distributed System e Immutable Register Book.
- e) Blockchain e Bookchain.

RESOLUÇÃO DE QUESTÃO

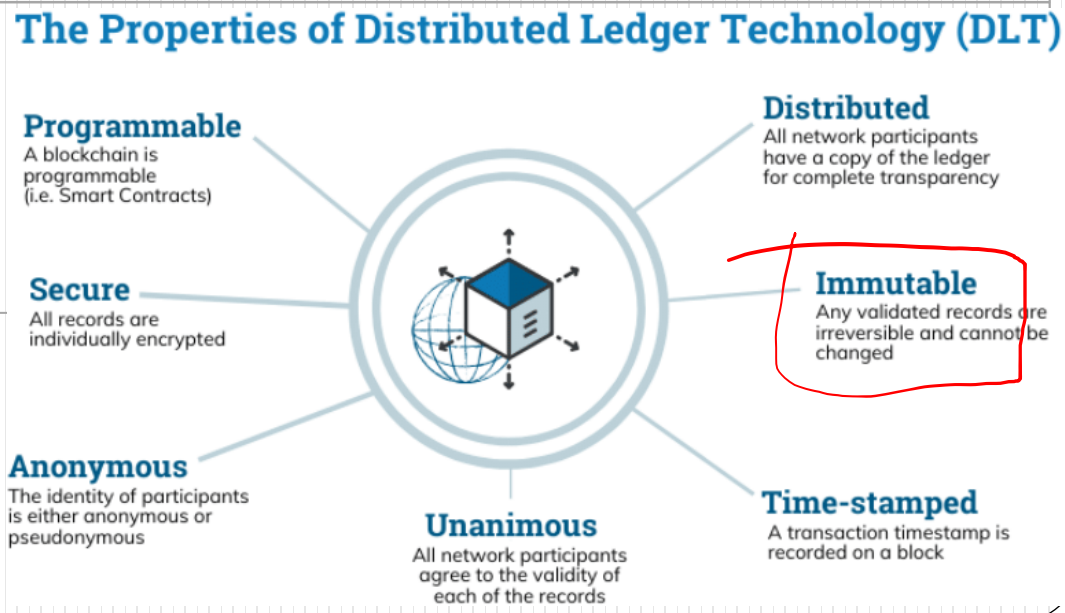
FCC – Analista (METRO-SP) / 2019

Considere o fragmento de texto abaixo.

Um dos tipos de sistemas distribuídos em franco crescimento atualmente utiliza criptografia assimétrica para garantir segurança nas transações sem um agente de confiança intermediador. Essas transações são agrupadas e armazenadas em unidades encadeadas e interligadas por meio de códigos hash, de forma que a unidade seguinte indique o hash da unidade anterior. Todas as transações realizadas no sistema são registradas em uma espécie de livro de registros, de acesso público, permitindo a rastreabilidade das transações na rede. Dentre as aplicações desse tipo de sistema distribuído estão as Decentralized Application – DAPP e smart contracts.

O sistema distribuído e o local onde são registradas as transações do sistema são, respectivamente,.

- ✅ a) Blockchain e Immutable Ledger.
- b) Common Object Request Broker e Trezor.
- c) Common Object Request Broker e Immutable Consensus Book.
- d) Remote Distributed System e Immutable Register Book.
- e) Blockchain e Bookchain.



BLOCKCHAIN

Core Technologies – Mecanismos de Consenso

Alcançar o consenso é fundamental na computação distribuída.

O objetivo da DLT é produzir um conjunto de registros que são validados por meio de um consenso multipartidário
(tudo na ausência de uma autoridade central substituída por um conjunto de soluções criptográficas e incentivos econômicos que convergem para evitar atualizações ilícitas e conciliar discrepâncias.)

Mecanismo de consenso é uma técnica de autenticação e validação de um valor ou transação em uma DLT ou blockchain **sem a necessidade de confiar em uma autoridade central**.

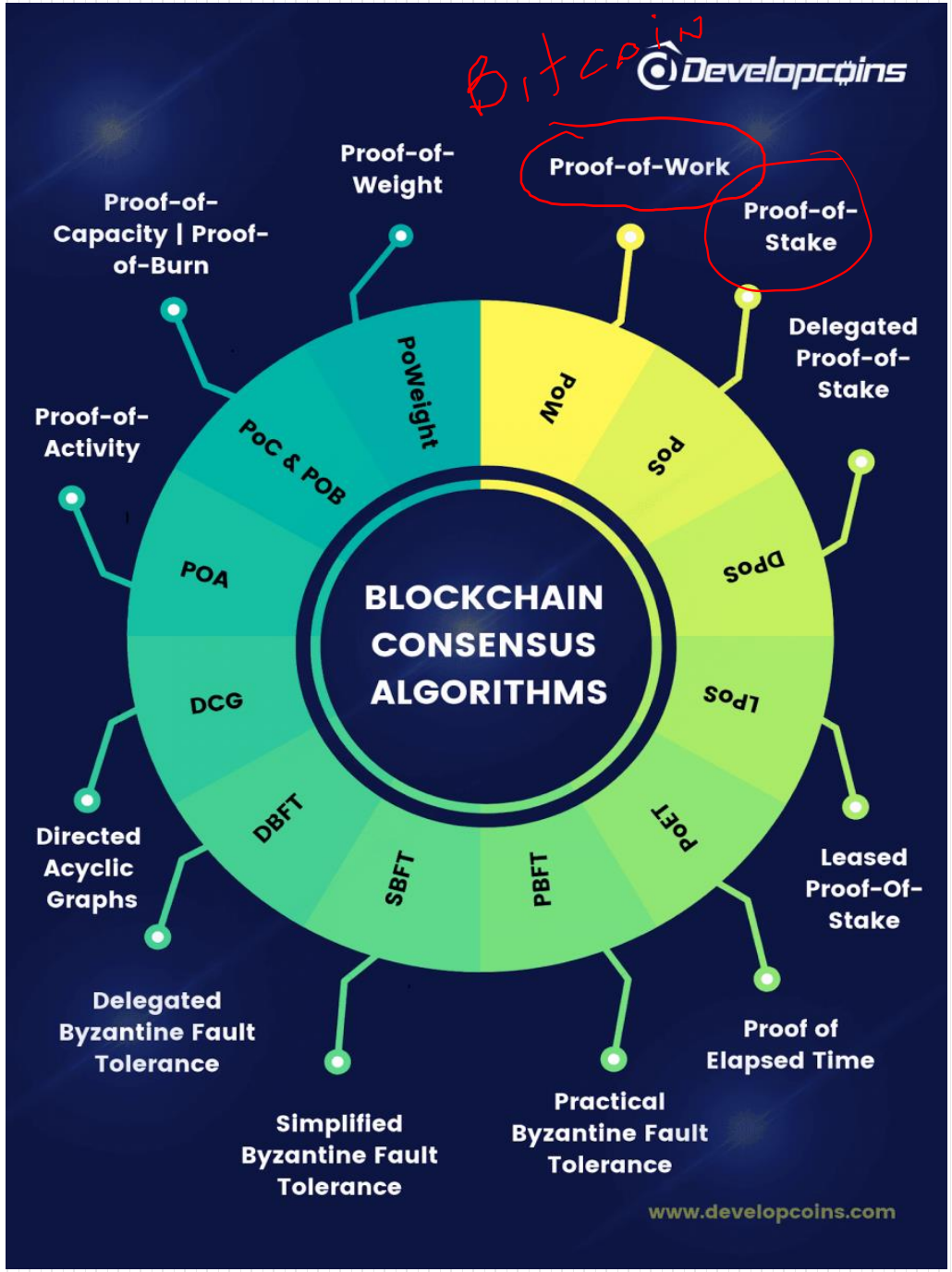
Os mecanismos de consenso têm que lidar com nós (partes) “egoístas” e “maliciosos”.

Devem ser resilientes a falhas dos nós, partição de rede, atraso de mensagens e mensagens não ordenadas e corrompidas.

BLOCKCHAIN

Core Technologies – Mecanismos de Consenso

https://0xzx.com/wp-content/uploads/2019/06/20190629-39.png



BLOCKCHAIN

Core Technologies – Criptografia de chave pública

A **criptografia é o elemento central da DLT**, em particular para implementações de blockchain.

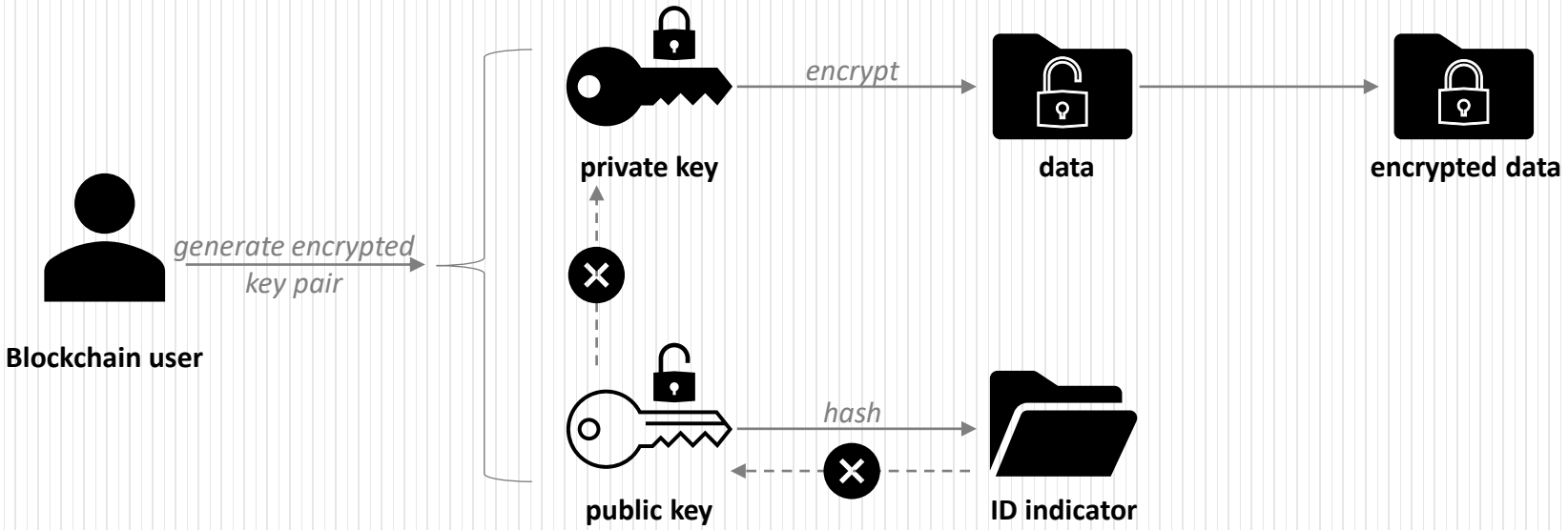
Blockchain usa **criptografia de chave pública**, um esquema de **criptografia assimétrica**, aumentando sua segurança.

Como?

- Cada nova transação é “hasheada” (uma função de hash é aplicada ao conteúdo original).
- Esses hashes de transação são agrupados em um bloco que pode conter um número limitado de transações.
- Finalmente, os blocos são assinados com uma assinatura digital, que vincula o remetente ao conteúdo do bloco, como a assinatura de um contrato.

BLOCKCHAIN

Core Technologies – Criptografia de chave pública



RESOLUÇÃO DE QUESTÃO

FUNDATEC – Agente Técnico (CEASA-RS) / 2022

A criptografia de chave pública requer um algoritmo de cifração e duas chaves: uma privada e outra pública. Enquanto a primeira chave deve ser guardada em local seguro e não acessível por outros participantes, a segunda deve ser compartilhada publicamente, o que gera uma fragilidade potencial, já que alguém mal-intencionado pode compartilhar uma chave dizendo ser de outra pessoa. Para resolver esse tipo de vulnerabilidade é que existe:

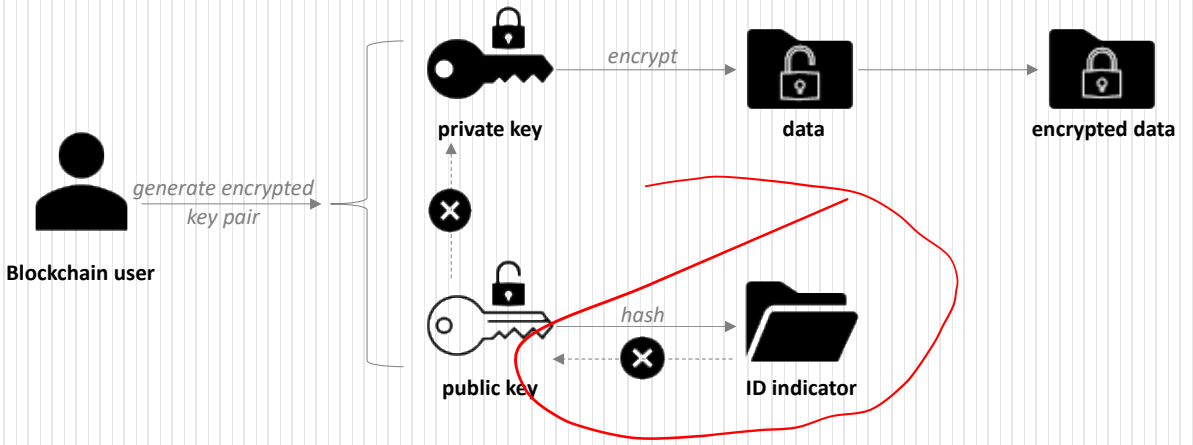
- a) A assinatura digital
- b) A assinatura eletrônica
- c) A blockchain
- d) O certificado de chave pública
- e) O protocolo SSL

RESOLUÇÃO DE QUESTÃO

FUNDATEC – Agente Técnico (CEASA-RS) / 2022

A criptografia de chave pública requer um algoritmo de cifração e duas chaves: uma privada e outra pública. Enquanto a primeira chave deve ser guardada em local seguro e não acessível por outros participantes, a segunda deve ser compartilhada publicamente, o que gera uma fragilidade potencial, já que alguém mal-intencionado pode compartilhar uma chave dizendo ser de outra pessoa. Para resolver esse tipo de vulnerabilidade é que existe:

- a) A assinatura digital
- b) A assinatura eletrônica
- c) A blockchain
- ✅ d) O certificado de chave pública
- e) O protocolo SSL



BLOCKCHAIN

Core Technologies – Smart Contracts

Solidity → Ethereum

O termo “contratos inteligentes” foi forjado pela primeira vez pelo criptógrafo Nick Szabo em um artigo de 1997.

Os contratos inteligentes combinam protocolos com interfaces de usuário para formalizar e proteger relacionamentos em redes de computadores.

São derivados de princípios jurídicos e da teoria econômica, baseados em protocolos confiáveis e seguros.

Apesar do nome, os contratos inteligentes não são “inteligentes” nem “contratos” estritamente.

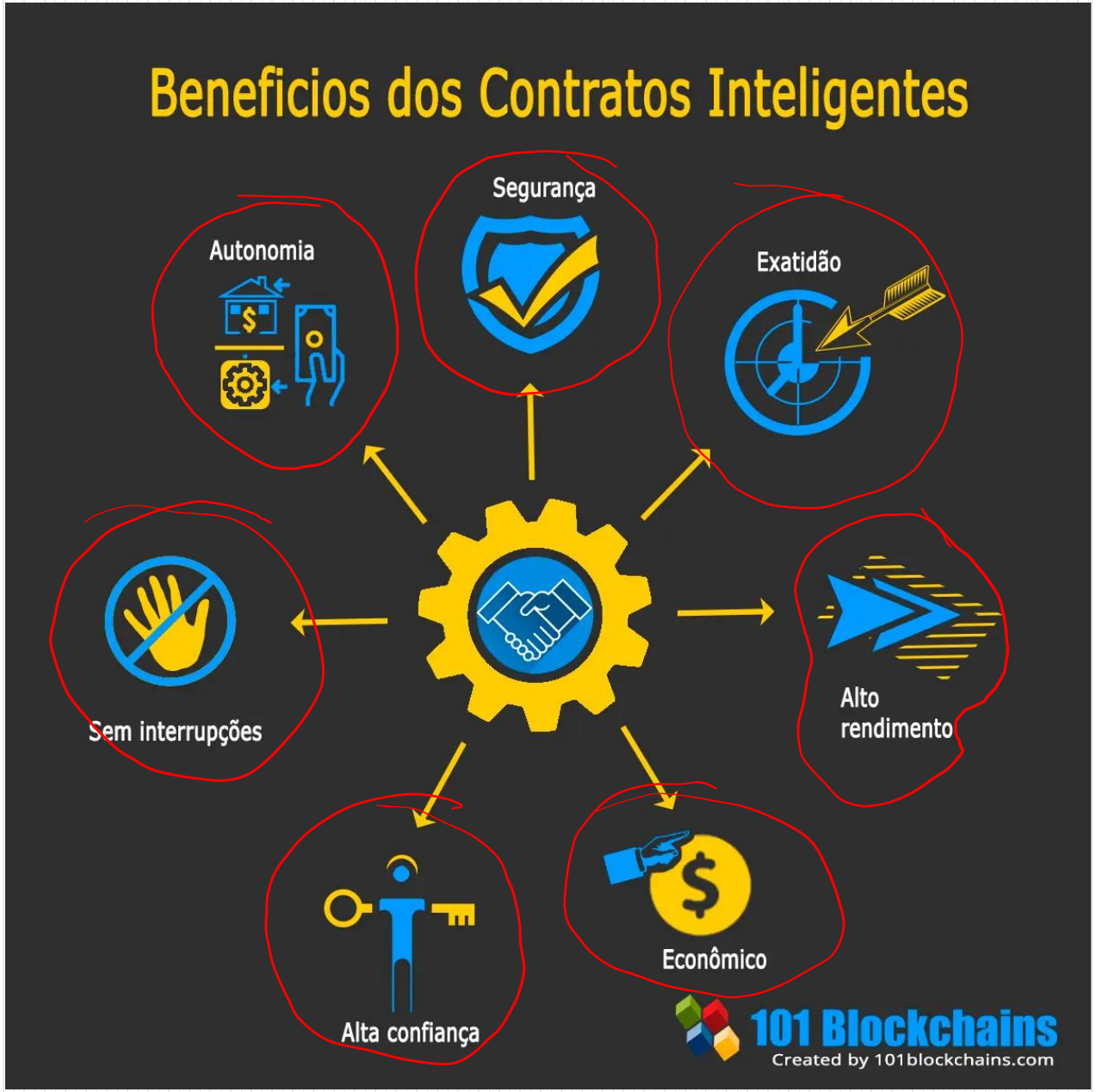
> *Embora chamados de contratos inteligentes, eles não são autônomos ou adaptativos (características que remetem a “inteligentes”), nem contratos na implicação legal.*

São evidências de um conjunto de regras de engajamento ou um meio tecnológico de implementação de um contrato ou acordo (Deshpande et al., 2017; Rauchs et al., 2018).

São transações executadas programaticamente na blockchain quando determinadas condições sao satisfeitas.

BLOCKCHAIN

Core Technologies – Smart Contracts



https://101blockchains.com/wp-content/uploads/2018/09/Benef%C3%ADcios-dos-Contratos-Inteligentes.png

BLOCKCHAIN

Core Technologies – Smart Contracts

ORACLE

Creation → **Deployment** → **Self-Execution** → **Completion**

Design, implementation and validation

Contracts stored on blockchain

Auto-execute contract statements once triggered

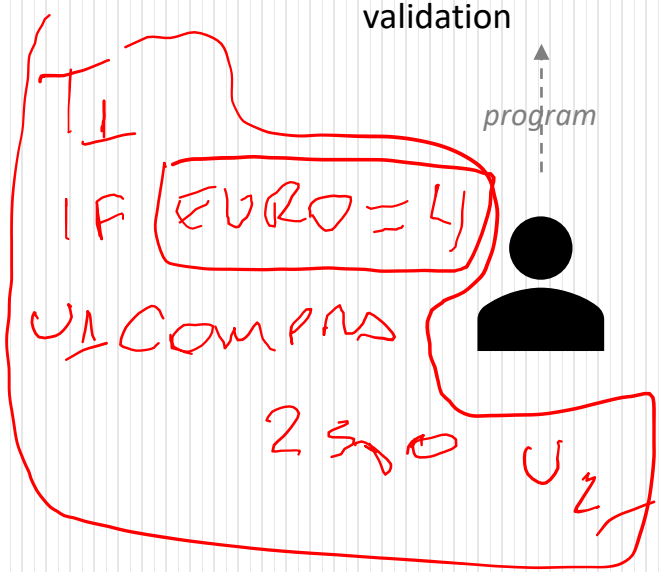
State updating and digital assets allocated

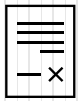
program

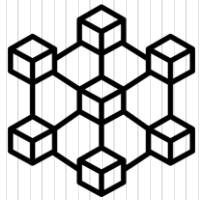
write as a transaction in the blockchain

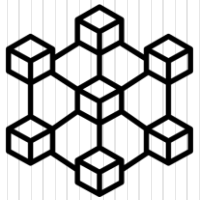
write as a transaction in the blockchain

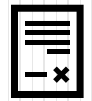
write as a transaction in the blockchain

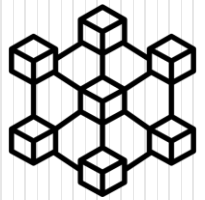












RESOLUÇÃO DE QUESTÃO

CESPE - Analista (SERPRO) / 2021

Julgue o item a seguir, relativo a blockchain e smart contracts.
Smart contracts são indicadores de desempenho em uma única página e seus fornecedores oferecem, tipicamente, um conjunto predefinido de relatórios com elementos estáticos e estrutura estanque.

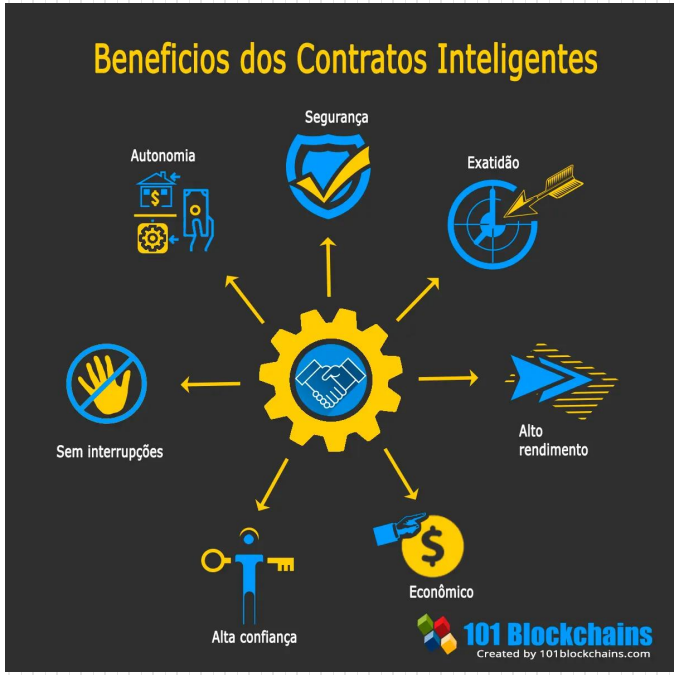
- Certo
- Errado

RESOLUÇÃO DE QUESTÃO

CESPE - Analista (SERPRO) / 2021

Julgue o item a seguir, relativo a blockchain e smart contracts.
Smart contracts são indicadores de desempenho em uma única página e seus fornecedores oferecem, tipicamente, um conjunto predefinido de relatórios com elementos estáticos e estrutura estanque.

- Certo
- ✅ Errado



https://miro.medium.com/max/1400/1*Z5ISfUaEs48Hhu0DKXWiwQ.png

BLOCKCHAIN

Blockchain (Noun): A distributed digital ledger that uses peer-to-peer consensus within a decentralized network to validate transactions and a hashing algorithm to cryptographically link them in a chronological "chain" of records.

Fluree

0 Copied and shared across computers known as 'nodes' in a network

1 Computerized record of all historical transactions chronologically ordered

2 Shares resources directly between nodes, bypassing third party servers, with specialized communication protocols

3 Every transaction must be approved (or rejected) by the network by consensus mechanisms (examples include: PBFT, PoW, PoS)

4 Hosted by many nodes simultaneously; controlled by no single entity; data is accessible by anyone within the network

5 Public Networks, where anyone can participate [Bitcoin, Ethereum]; Private Networks with permissioned access and read/write rules [Hyperledger, Fluree]

6 Transactions may include: moving currency, updating a standard enterprise record, transferring ownership of an asset, etc

7 Converting transaction data into a fixed-length string of numbers and letters that cannot be reverse-engineered (i.e. SHA-256)

8 The hashing process of a new block includes meta-data from the previous block's hash output. This link makes the chain "immutable"

9 A full, immutable, time-ordered history of transactions approved by the network

Fim

Continue com a gente nas redes sociais

PROVAS DE TI
TUDO PARA VOCÊ PASSAR