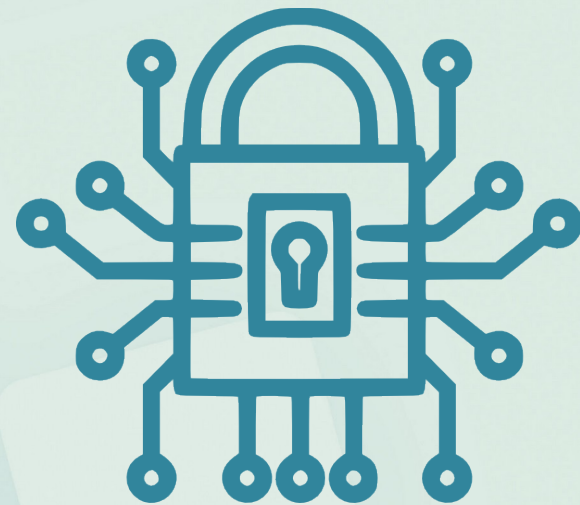


INSTITUTO FEDERAL

Sertão Pernambucano

Segurança da Informação

Criptografia



Prof. Heraldo Gonçalves Lima Junior

9. Assinatura Digital

- Uma assinatura digital é fundamental para garantir a segurança, autenticidade e integridade dos dados em uma mensagem, software ou documento digital.



9. Assinatura Digital

- A assinatura digital vem como código, que é anexado aos dados graças às duas chaves de autenticação mútua.
- **O remetente cria a assinatura digital usando uma chave privada** para criptografar os dados relacionados à assinatura, com o **receptor obtendo a chave pública do assinante para descriptografar os dados.**

10. NFT

- Como a criptografia pode ser utilizada para proteger **itens digitais únicos**?





10. NFT

- Os NFTs são **ativos criptográficos não fungíveis** que se tornaram rapidamente populares no mundo digital.
- Garantidos pela criptografia, os NFTs **protegem os direitos autorais de qualquer tipo de mídia digital** — seja um GIF, JPEG, fotos, vídeos, mensagens ou arquivos de áudio.

10. NFT

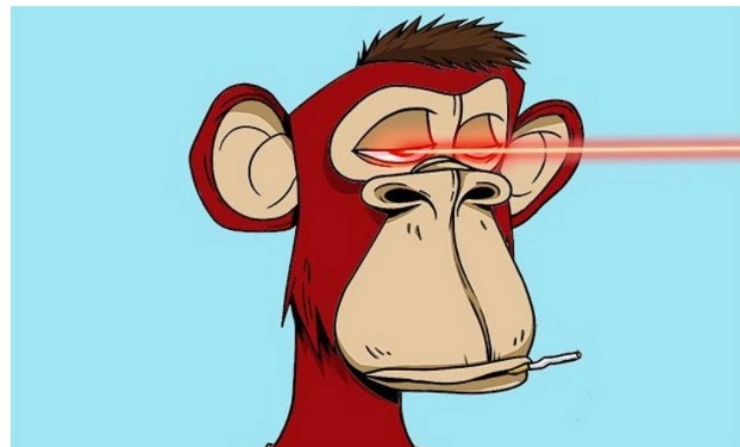
ESPORTES

Neymar vira colecionador de NFTs e compra duas artes por R\$ 6,2 milhões

Jogador mudou sua foto de perfil nas redes sociais para imagem de um macaco da coleção da Bored Ape Yacht Club

Matheus Ruas

22/01/2022 - 06:02 / Atualizado em 23/01/2022 - 11:53



Neymar e os companheiros de PSG, Verrati e Paredes, anunciaram a compra do NFT da Bored Ape Yacht Club
Foto: Reprodução

10. NFT

- O que são bens não fungíveis?
- O bitcoin é um bem fungível.



10. NFT

- O Código Civil, em seu artigo 85, traz a definição de bens fungíveis.
- **Lei 10.406, de 10 de janeiro de 2002**
- Art. 85. São fungíveis os móveis que podem substituir-se por outros da mesma espécie, qualidade e quantidade.

10. NFT





tilt uol

SAC  EMAIL  ENTRE ASSINE UOL

FIQUE POR DENTRO ▾ TEC A SEU FAVOR ▾ NOVOS HÁBITOS PAPO CABEÇA ▾ FICÇÃO CIENTÍFICA? ▾ COLUNAS NEWSLETTERS ÚLTIMAS

NEGÓCIOS

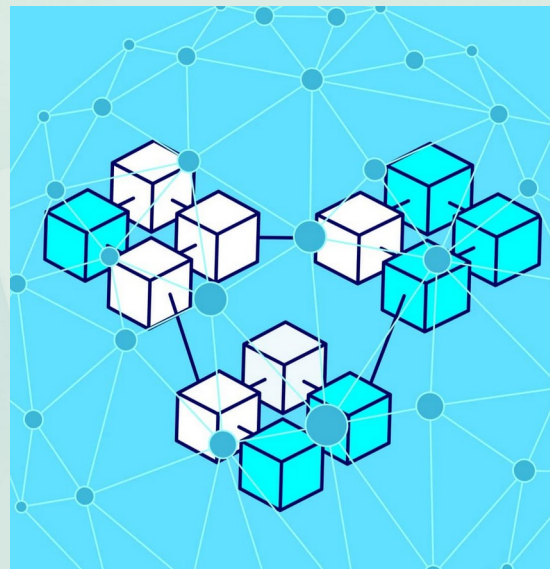
Ricaço compra obra de arte digital com tecnologia
NFT por US\$ 70 milhões

PUBLICIDADE



10.1. Como a criptografia possibilita a proteção dos NFTs

- A base do NFT é o Blockchain;
- Ele **permite rastrear a troca de certas informações pela internet**, criando uma rede de blocos entre os envolvidos nessa troca.



10.1. Como a criptografia possibilita a proteção dos NFTs

- Cada NFT possui um hash;
- Essa característica permite que os NFTs atuem como uma **prova de origem e inviabiliza qualquer tentativa de falsificação.**



10.2. As múltiplas possibilidades de uso do NFT

- Atualmente, o NFT já é utilizado em diversos setores, como na área de **imóveis, jogos virtuais, venda de ingressos para eventos, licenciamento de marcas, entre outros.**

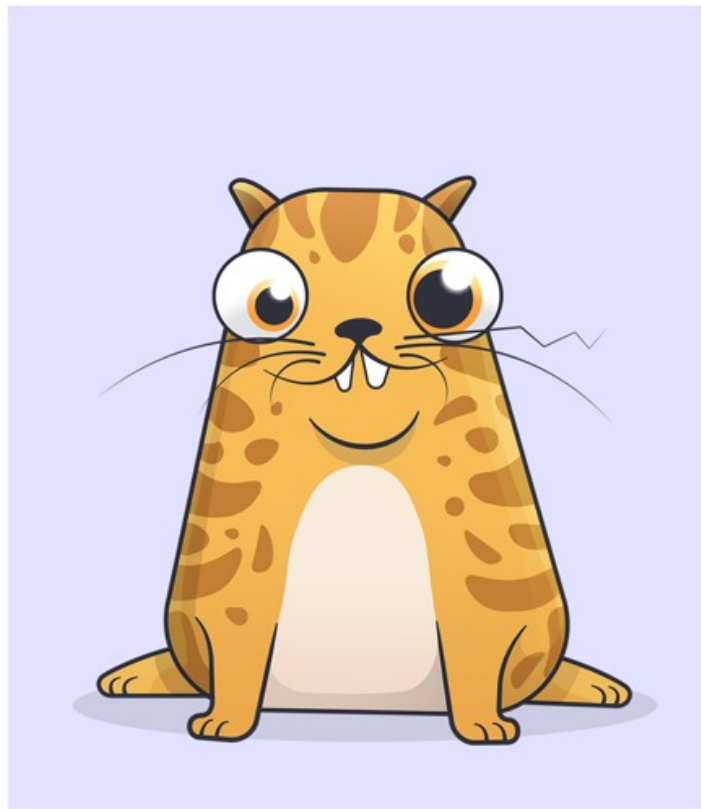
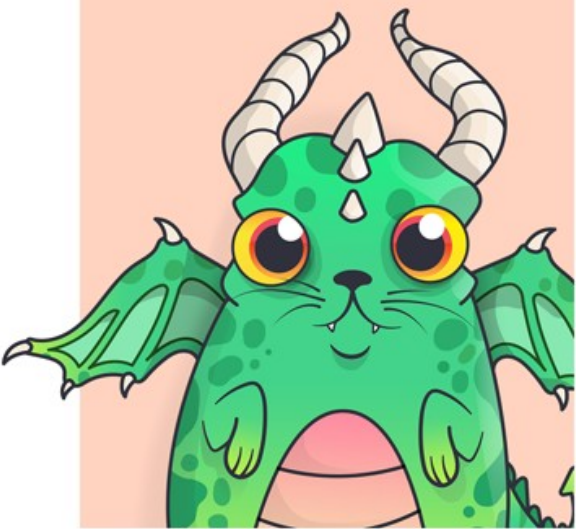


KINGS OF LEON

POWERED BY YELLOWHEART

NFT YOURSELF

CryptoKitties



[HOME](#)[ARTISTAS](#)[POVOS PARTICIPANTES](#)[CADASTRO DE ARTISTAS](#)[FALE CONOSCO](#)

[Início](#) > [Notícias](#) > [Games](#) > [GTA RP adiciona NFTs de carros exclusivos por até R\\$ 1 mil](#)

[Notícias](#)[Games](#)

GTA RP adiciona NFTs de carros exclusivos por até R\$ 1 mil

Segundo o CEO da Outplay, Paulo Benetti, neste primeiro momento apenas automóveis serão oferecidos como NFT, mas a ideia é, no futuro, outras conquistas no Cidade Alta sejam monetizadas em algum momento.

19 de outubro de 2021

👁 576

💬 0

11. Criptografia pós-quântica

- A corrida para criar novas formas de proteger os dados e as comunicações da ameaça representada por computadores quânticos superpoderosos já começou.



11.1. Computação Quântica

- A física quântica prevê alguns comportamentos de partículas que **vão muito além do “sim” e “não”, do “verdadeiro” e “falso”.**
- Essa limitação que forma o bit é simplesmente aniquilada quando falamos na computação quântica e dá origem ao **qubit, ou bit quântico.**

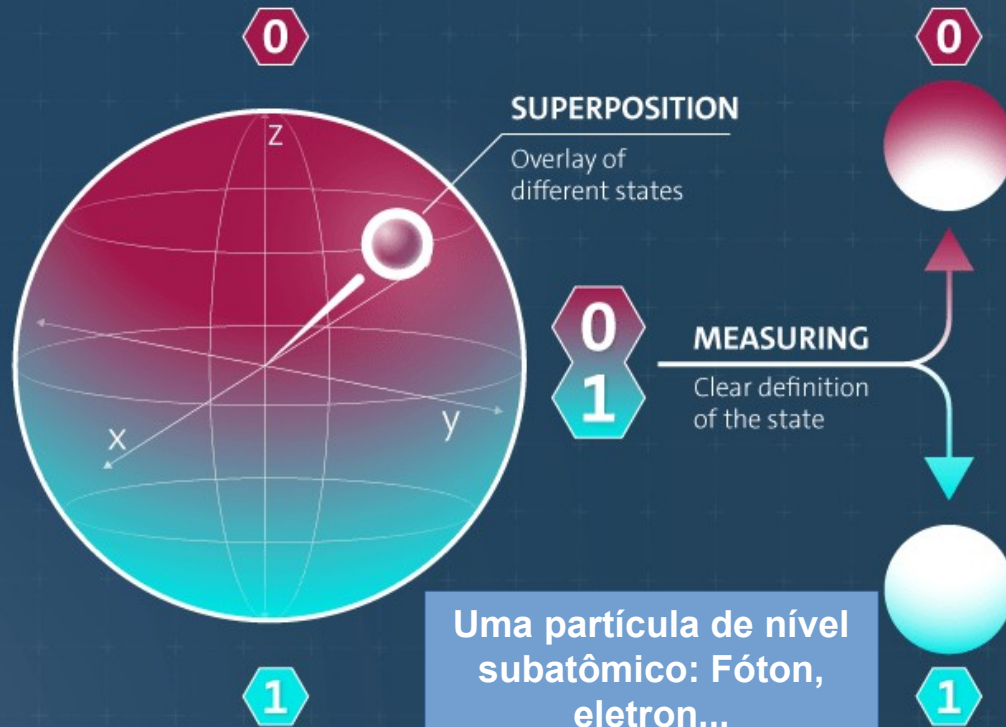
Classical Bit

Binary system



quantum bit “qubit”

Arbitrarily manipulable two-state quantum system



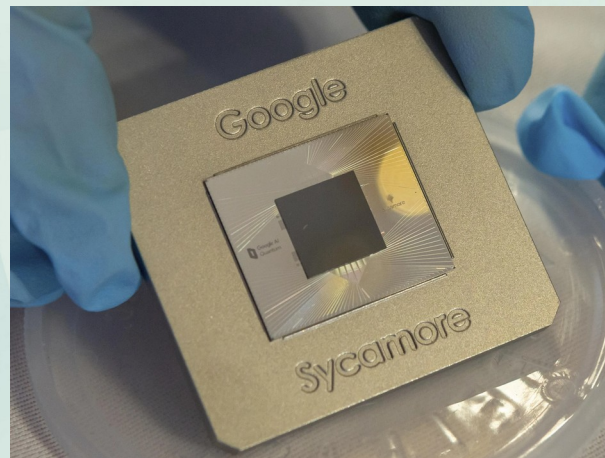
Uma partícula de nível subatômico: Fóton, elétron...

Várias combinações de zero e um ao mesmo tempo.

pode avaliar diferentes combinações de resultados simultaneamente

11.2. Supremacia Quântica

- O momento em que um computador quântico **consegue resolver com rapidez uma tarefa que seria impossível de ser resolvida** mesmo com o computador clássico mais poderoso do mundo.



11.2. Supremacia Quântica

Verificar se um gerador de números aleatórios realmente produzia números aleatórios:

- **Computador comum mais poderoso do planeta:**
 - 10 mil anos
- **Sycamore (quântico):**
 - 200 segundos

11.3. O que é criptografia pós-quântica?

- A corrida para criar novas formas de proteger os dados e as comunicações da ameaça representada por computadores quânticos superpoderosos já começou.

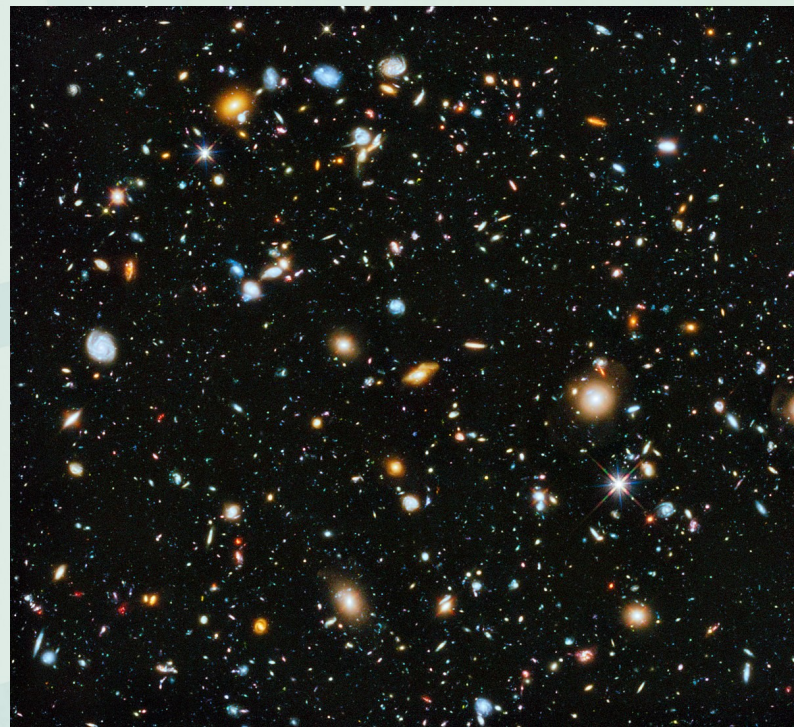


11.3. O que é criptografia pós-quântica?

- Hackers podem tentar decifrar um código testando todas as variações possíveis de uma chave até que funcione.
- Atualmente são utilizados pares de chaves muito longos, como a implementação **RSA de 2.048 bits**, que processa uma **chave com 617 dígitos decimais**.

11.3. O que é criptografia pós-quântica?

- Uma máquina quântica com **300 qubits poderia representar mais valores do que átomos no universo observável.**

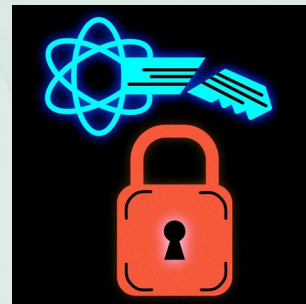


11.3. O que é criptografia pós-quântica?

- Um relatório sobre computação quântica publicado no ano passado pelas National Academies of Sciences, Engineering, and Medicine (NASEM) dos EUA previu que um poderoso computador quântico executando o algoritmo de Shor seria capaz de decifrar uma implementação de **RSA de 1.024 bits em menos de um dia.**

11.3. O que é criptografia pós-quântica?

- A CRIPTOGRAFIA PÓS-QUÂNTICA é o desenvolvimento de novos tipos de enfoques criptográficos que podem ser **implementados usando os computadores clássicos de hoje, mas serão imunes aos ataques quânticos de amanhã.**



11.4. Linhas de defesa

- Uma linha de defesa é **aumentar o tamanho das chaves digitais** para que o número de permutações que precisam ser pesquisadas usando o poder de computação bruto aumente significativamente.

12. Blockchain

- Blockchain se tornou uma expressão comum em assuntos relacionados aos famosos Bitcoins, e por vezes os dois termos chegam a se confundir um pouco.



12.1. Como surgiu o Blockchain?

- Em 2008, foi apresentado ao grupo de discussão “The Cryptography Mailing” um artigo contendo os princípios de funcionamento de uma criptomoeda denominada **Bitcoin**.
- A proposta era a criação de uma moeda digital mundial que funcionasse em uma **rede peer-to-peer (ponto a ponto)**.

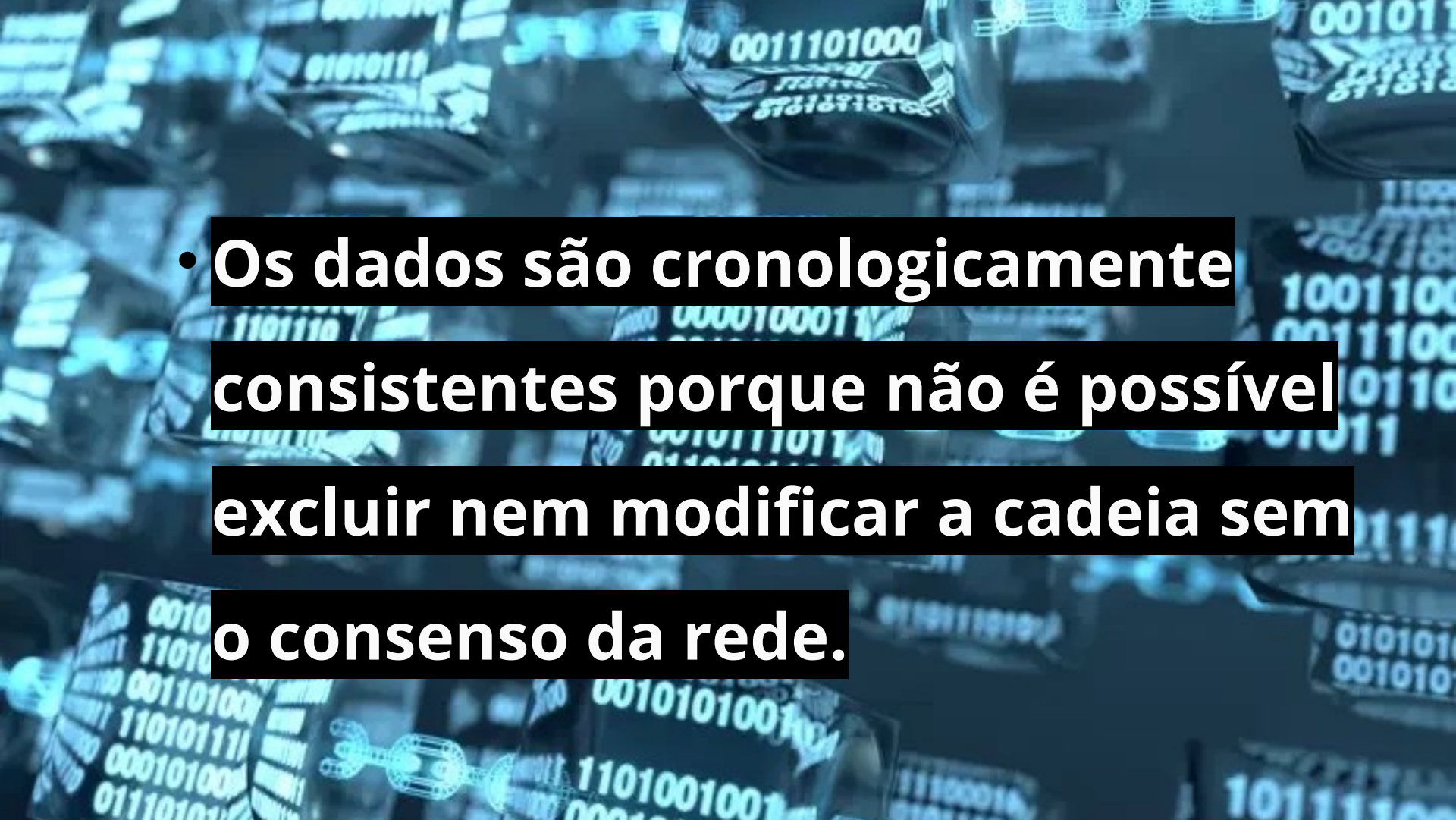
12.1. Como surgiu o Blockchain?

- Já em 2009, a rede Bitcoin começou a funcionar com o lançamento de seu primeiro cliente e hoje estima-se que haja mais **16 milhões da criptomoeda em circulação.**



12.2. O que é o Blockchain?

- Podemos dizer que o Blockchain se trata de um **sistema distribuído de base de dados**, mantido e gerido de forma **descentralizada e compartilhada**, no qual **todos os participantes são responsáveis por armazenar e manter a base de dados**.

- 
- The background is a dark blue field filled with glowing binary code (0s and 1s) and faint, stylized network diagrams. The text is overlaid on this background in white, bold font, with each line of text contained within a black rectangular box.
- Os dados são cronologicamente consistentes porque não é possível excluir nem modificar a cadeia sem o consenso da rede.

12.3. Porque essa tecnologia é importante?

- As tecnologias de bancos de dados tradicionais lançam vários desafios para o registro de transações financeiras.
- Por exemplo, considere a venda de um imóvel.



12.3. Porque essa tecnologia é importante?

- Para evitar problemas legais, uma terceira parte confiável precisa supervisionar e validar as transações.

GERENCIADOR DE IMOVEIS - CONTROLE DE VENDAS E LOCAÇÕES

Imóveis

Informações | Chácara/Terreno | Proprietário | Imobiliária | Fotos | WEBSITE

Código: 11050 | Cód. Web: | Tipo Imóvel: COMERCIAL | Ativo: S | Status: Locado | Valor: 100.000,00 | Valor Negociável: | Idade: 10

Para Fins: Aluguel | Descrição: RUA CENTRAL - DESCRIÇÃO DO IMÓVEL | Endereço: AV. DONA GERTRUDES, 7- SALA 02

Cidade: ATIBAIA | UF: SP | Bairro: ALVINÓPOLIS | CEP: 83303-001

Face: NORTE | Zona: R1 | Tipo Casa: Geminada | Metragem: 40X20 | Área Ter.: 800 | Área Const.: 500 | Topografia: Estrada | Estrada: Asfaltada

RGI/U. Consuidora: | Laje: Sem Laje | T.Garagem: Sem Cob. | T. Piso: Carpete | Pintura: Boa | Ocupada: Não

Informe a quantidade

Dormitório: 1 M | Suite: 3 M | Banheiro: 4 P | Cozinha: 1 G | Living: 1 | Garagem: 4

Esquina | Jardim | Quintal | Rua calçada | Rua ilumin. | Escoto | Escada | Laje | Água encan. | Financiament

Corredor | Jardim | Piscina | Sala de Visita | Lavabo | Churrasqueira | Fogão a lenha | Lareira | Forno a lenha | Terraço

Dispensa | Sala de Vídeo | Q.Esporte | Pomar | Salão de Festa | Área de Serviço | Meio Lote | Aceita Auto | Aceita Moto | Aceita Terreno

Gravar(F1) | Incluir(F2) | Cancelar(F3) | Excluir | Ficha | Simplificado | Venda | Imprimir(F6) | Pesquisar(F4) | Sair(F5)

12.3. Porque essa tecnologia é importante?

- A blockchain reduz esses problemas criando um sistema descentralizado, **à prova de violações**, para registrar transações.
- A blockchain cria um ledger, ou seja, um registro, para o comprador e outro para o vendedor. Todas as transações devem ser aprovadas pelas duas partes.

12.4. Como diferentes setores usam a blockchain?

- A blockchain é uma tecnologia relativamente recente que está sendo adotada de forma inovadora por vários setores.

12.4.1. Energia

- Empresas de energia usam a tecnologia blockchain para criar plataformas de **comercialização de energia entre pares** e facilitar o acesso a **energias renováveis**.



12.4.2. Financeiro

- Os sistemas financeiros tradicionais, como os bancos ou a bolsa de valores, usam os serviços de blockchain para gerenciar pagamentos, contas e o mercado comercial online.



12.4.3. Mídia e entretenimento

- Empresas de mídia e entretenimento usam os sistemas de blockchain para **gerenciar dados de direitos autorais**. A verificação de direitos autorais é essencial para a compensação justa dos artistas.



12.4.5. Varejo

- Empresas de varejo usam a blockchain para **monitorar a movimentação de mercadorias** entre fornecedores e compradores.



12.5. Quais são os recursos da tecnologia blockchain?

- **Descentralização:**

A descentralização na blockchain refere-se à **transferência do controle e de decisões** de uma entidade centralizada (indivíduo, organização ou grupo) para uma rede distribuída.

12.5. Quais são os recursos da tecnologia blockchain?

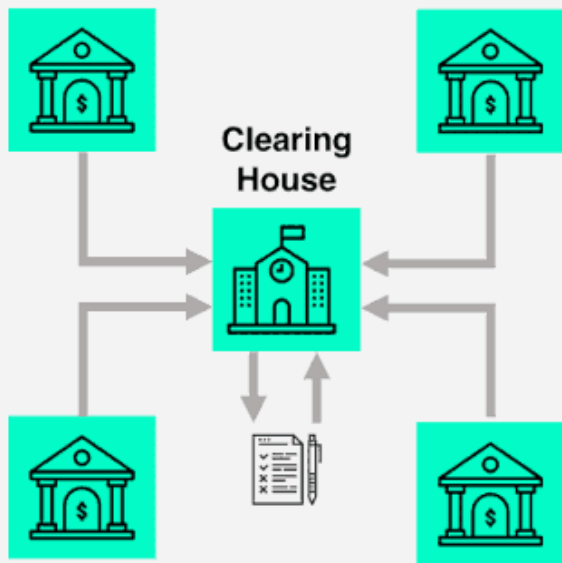
- **Imutabilidade:**
- Imutabilidade significa **algo que não pode ser mudado ou alterado**. Nenhum participante poderá violar uma transação depois que alguém registrá-la no ledger compartilhado.

12.5. Quais são os recursos da tecnologia blockchain?

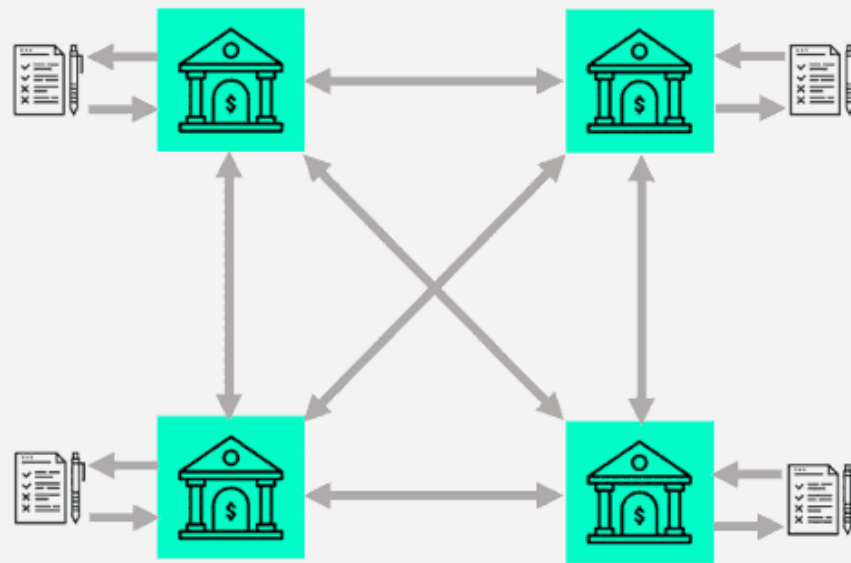
- **Consenso:**
- Um sistema de blockchain estabelece regras sobre o consentimento dos participantes para o registro das transações. **Você só poderá registrar novas transações quando a maioria dos participantes da rede der seu consentimento.**

12.6. Quais são os principais componentes da tecnologia blockchain?

- **Um ledger distribuído:**
- Um ledger distribuído é o **banco de dados compartilhado na rede blockchain que armazena as transações**, como um arquivo compartilhado que todos os membros da equipe podem editar.



Ledger Centralizado



Ledger Distribuido

12.6. Quais são os principais componentes da tecnologia blockchain?

- **Contratos inteligentes:**
- As empresas usam contratos inteligentes para **autogerenciar seus contratos** comerciais, sem a necessidade de assistência de uma terceira parte.



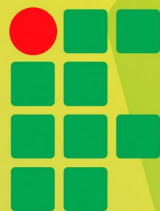
12.6. Quais são os principais componentes da tecnologia blockchain?

- **Criptografia de chave pública:**
- A criptografia de chave pública é um **recurso de segurança para identificar de forma exclusiva** os participantes em uma rede blockchain.

Para mais informações sobre Blockchain

- <https://aws.amazon.com/pt/what-is/blockchain/>

Obrigado!
Vlw! Flw!



INSTITUTO FEDERAL
Sertão Pernambucano