Blockchain
Introdução e Aplicações

PROF. GLADSTONE ARANTES JR, DSC

Bitcoin → Origem da Blockchain

2008

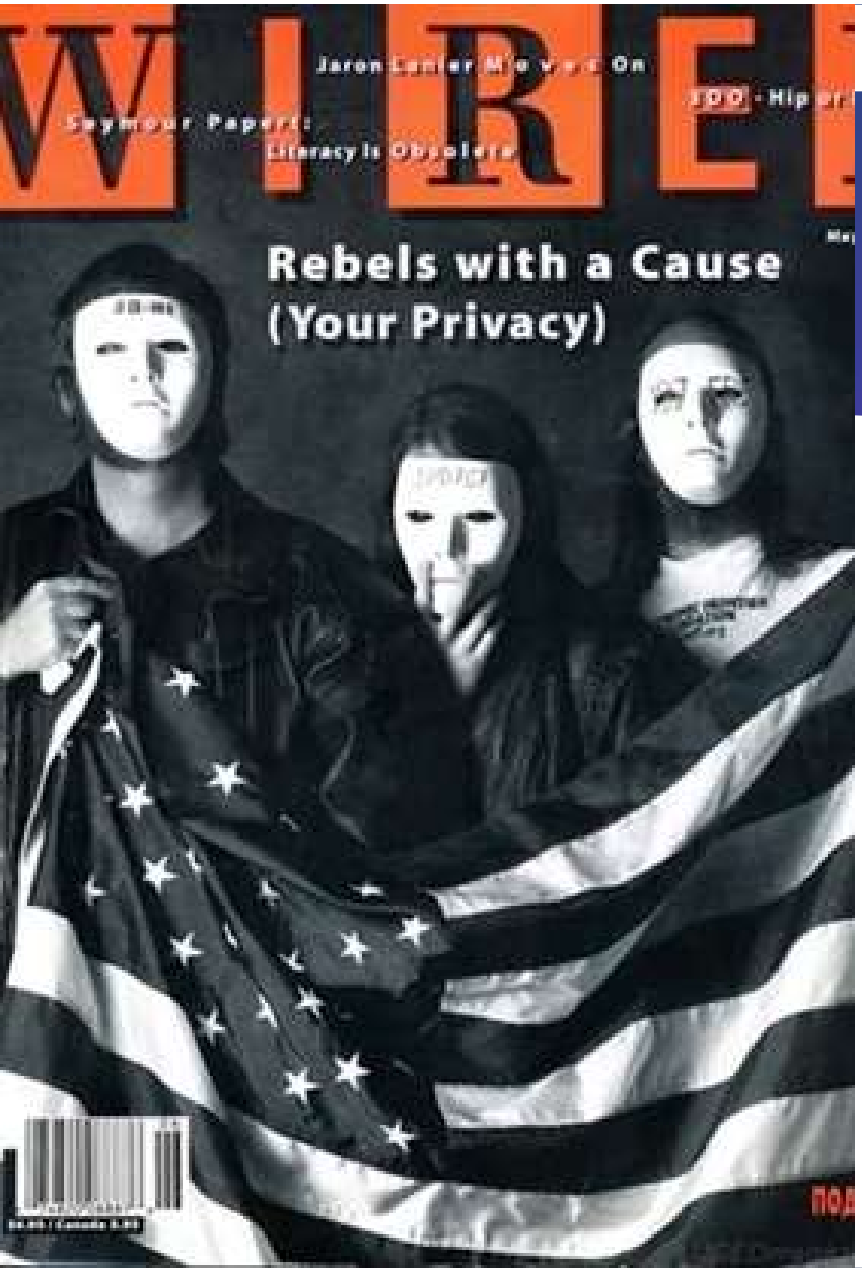
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to
financial institution. Digital signatures provide
benefits are lost if a trusted third party is still re
We propose a solution to the double-spending pro
The network timestamps transactions by hashi
hash-based proof-of-work, forming a record that
the proof-of-work. The longest chain not only
events witnessed, but proof that it came from th
long as a majority of CPU power is controlled b
attack the network, they'll generate the longest
network itself requires minimal structure. Mess
basis, and nodes can leave and rejoin the netw
proof-of-work chain as proof of what happened w

2009

Hoje: mais de 21.000 criptomoedas no mercado
US$ 0,94 Tri (+40% BTC)



Origens Históricas → Cypherpunks

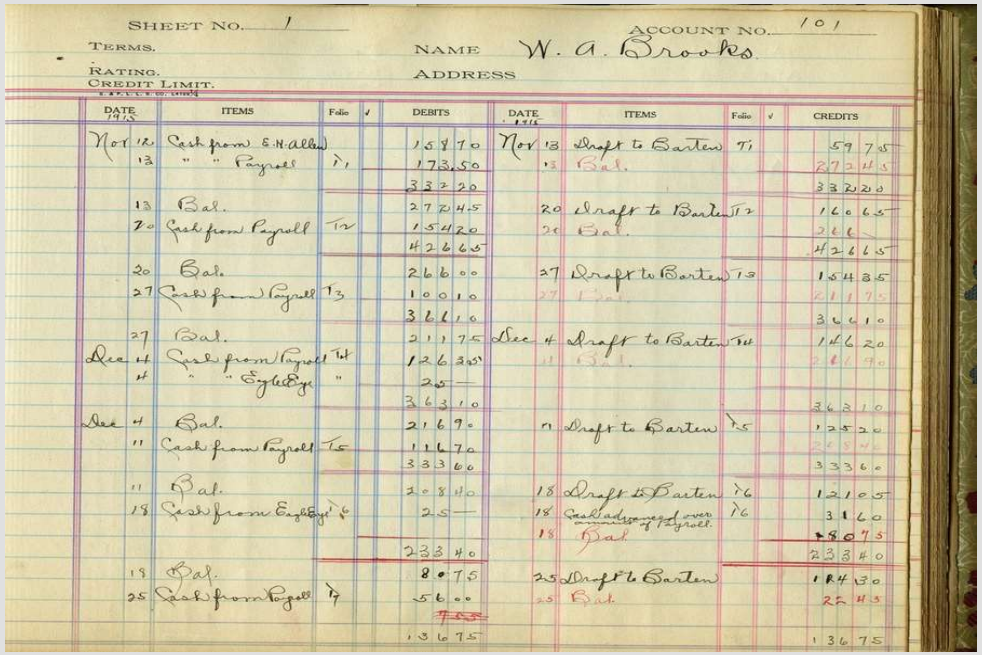
- Liberdade.
- Privacidade (cypher).
- Do It Youself.
- Resiliência a "ataques".
- Descentralização.

Transação em dinheiro vivo → Referência de privacidade

Cópia

Original

Blockchain é um *LEDGER*



SHEET NO. 1 ACCOUNT NO. 101

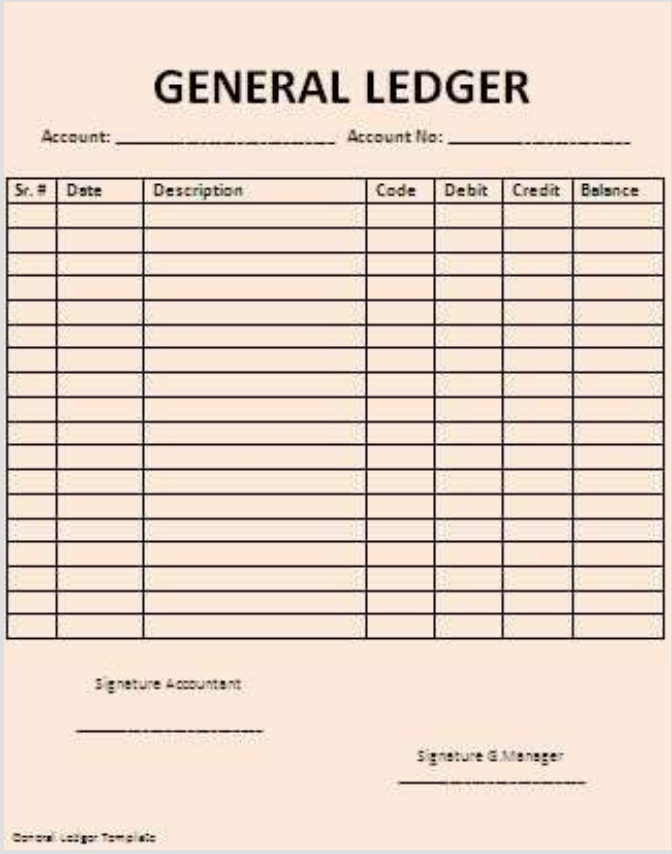
TERMS. NAME W. A. Brooks

RATING. ADDRESS

CREDIT LIMIT.

DATE 1915	ITEMS	Folio	✓	DEBITS	DATE 1915	ITEMS	Folio	✓	CREDITS
Nov 12	Cash from S. H. Allen			158 70	Nov 13	Draft to Barton	T1		59 75
13	" " Payroll	J1		173 50	13	Bal.			273 45
				332 20					332 20
13	Bal.			273 45	20	Draft to Barton	T2		160 65
20	Cash from Payroll	T2		154 20	20	Bal.			266 —
				426 65					426 65
20	Bal.			266 00	27	Draft to Barton	T3		154 35
27	Cash from Payroll	T3		100 10	27	Bal.			211 75
				366 10					366 10
27	Bal.			211 75	Dec 4	Draft to Barton	T4		146 20
Dec 4	Cash from Payroll	T4		126 30	4	Bal.			191 90
4	" " Eglet Eye	"		20 —					
				363 10					363 10
Dec 4	Bal.			219 90	11	Draft to Barton	T5		125 20
11	Cash from Payroll	T5		116 70					208 40
				336 60					333 60
11	Bal.			208 40	18	Draft to Barton	J6		121 05
18	Cash from Eglet Eye	J6		25 —	18	Cash advanced over amount of Payroll	J6		31 60
					18	Bal.			80 75
				233 40					233 40
19	Bal.			80 75	25	Draft to Barton			184 30
25	Cash from Payroll	J7		56 00	25	Bal.			22 45
				136 75					136 75

Chaves e carteiras



GENERAL LEDGER

Account: _____ Account No: _____

Sr. #	Date	Description	Code	Debit	Credit	Balance

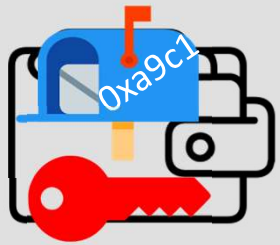
Signature Accountant

_____

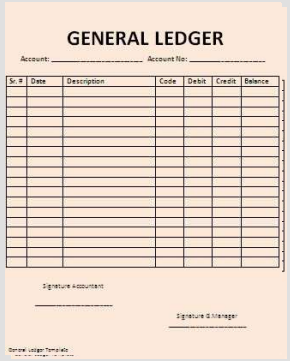
Signature G.Manager

_____

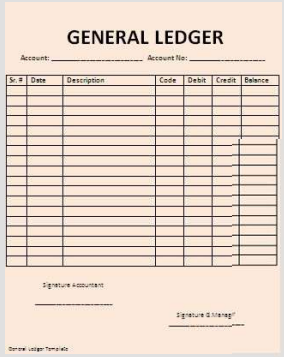
General Ledger Template

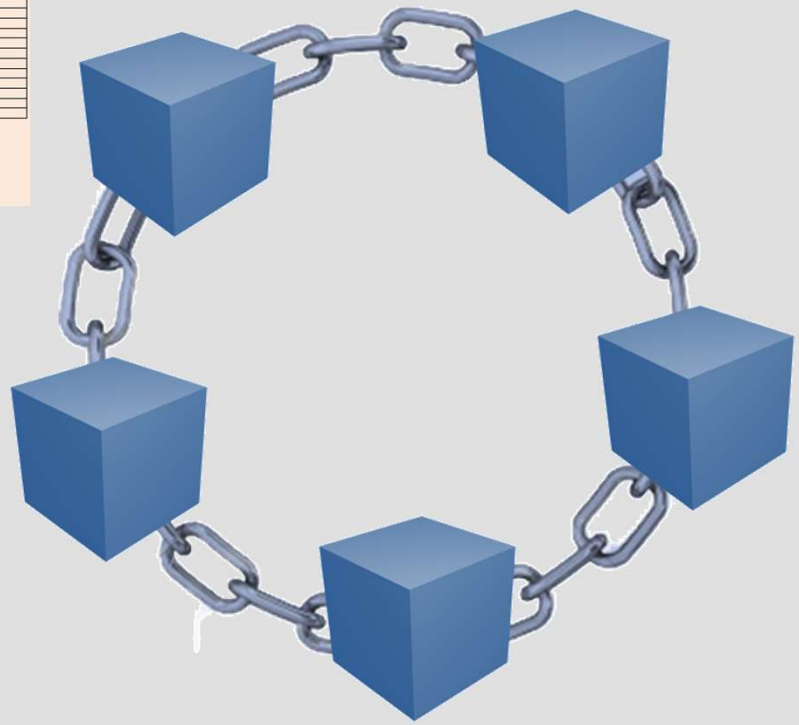


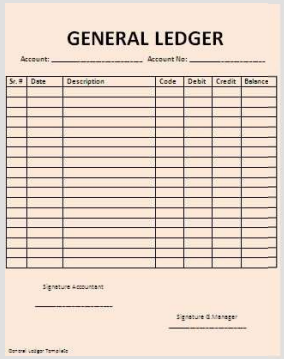
Ledger distribuído

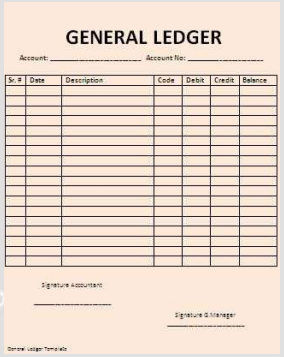


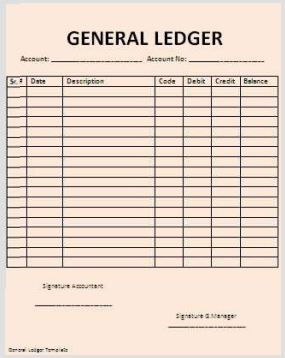
Ledger distribuído











Uma solução para construção do consenso distribuído

Consenso distribuído

Algoritmo que leva sistemas decentralizados a chegar a um resultado único que será aceito por todos.

Proof of Work na rede Bitcoin: MINERAÇÃO

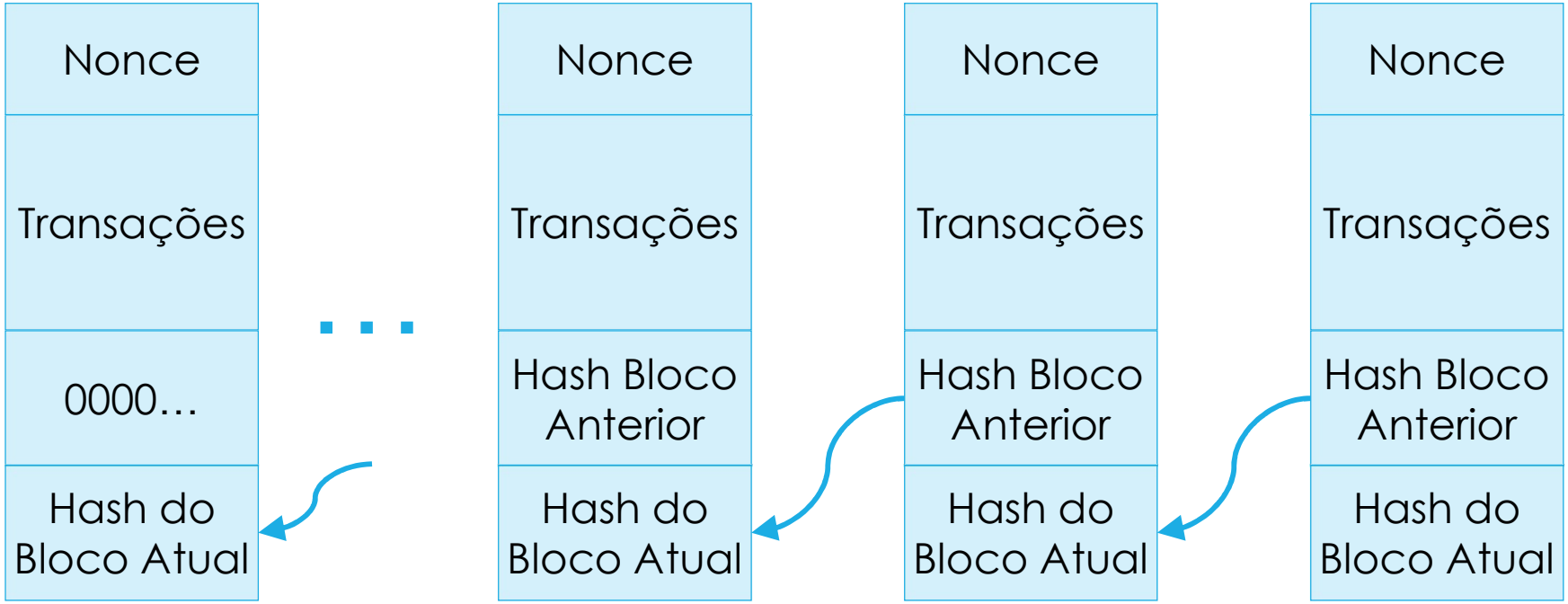
COMPETIÇÃO entre MINERADORES para resolver um DESAFIO COMPUTACIONAL por tentativa e erro.

Compromisso vem da prova de que tempo e recursos foram investidos pelo minerador.

O VENCEDOR recebe o direito de gravar o próximo bloco da blockchain e recebe Bitcoins como RECOMPENSA.

Parque minerador de Bitcoin

Enfim, a *block chain*...



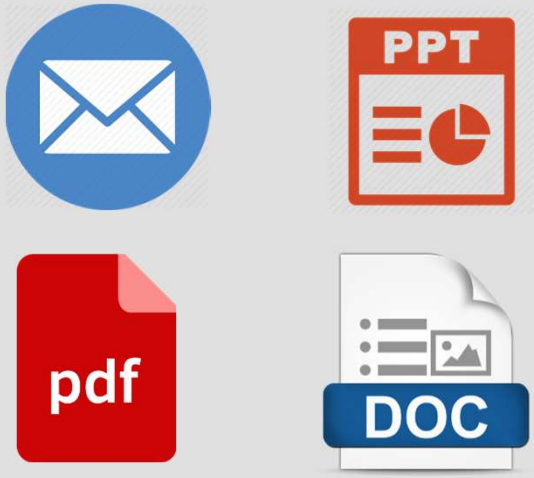
Genesis Block

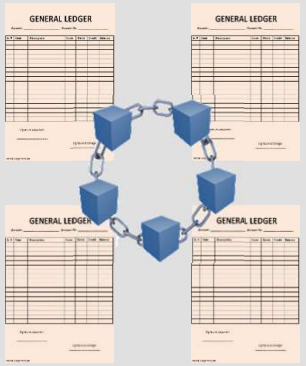
”Política monetária”

- São criados a cada 10 minutos.
- Quantidade é reduzida pela metade a cada 4 anos.
- 2009 → 50. Hoje → 6,25.
- Limite em 2140 → 21 milhões de bitcoins.
- Mais de 18 milhões emitidos.
- 1 bitcoin pode ser dividido em até 100 milhões de ”satoshis”.

Escassez na Internet – O Ouro Digital

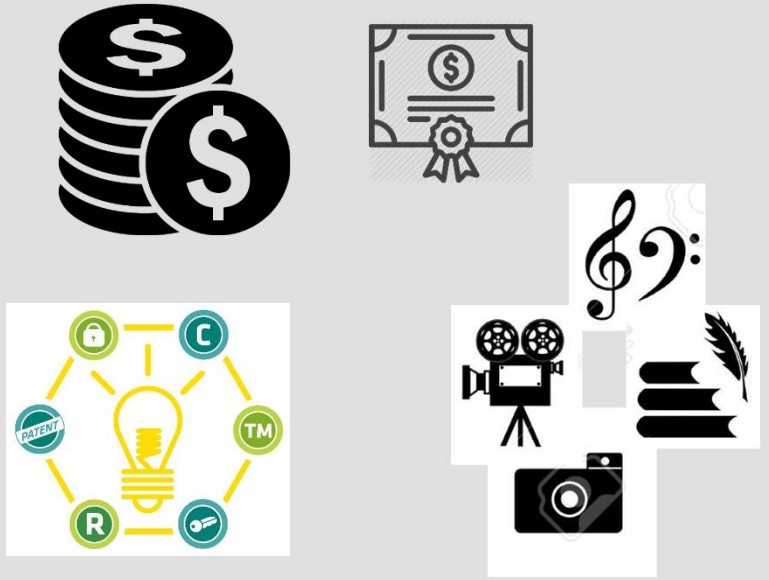
DA INTERNET DA INFORMAÇÃO





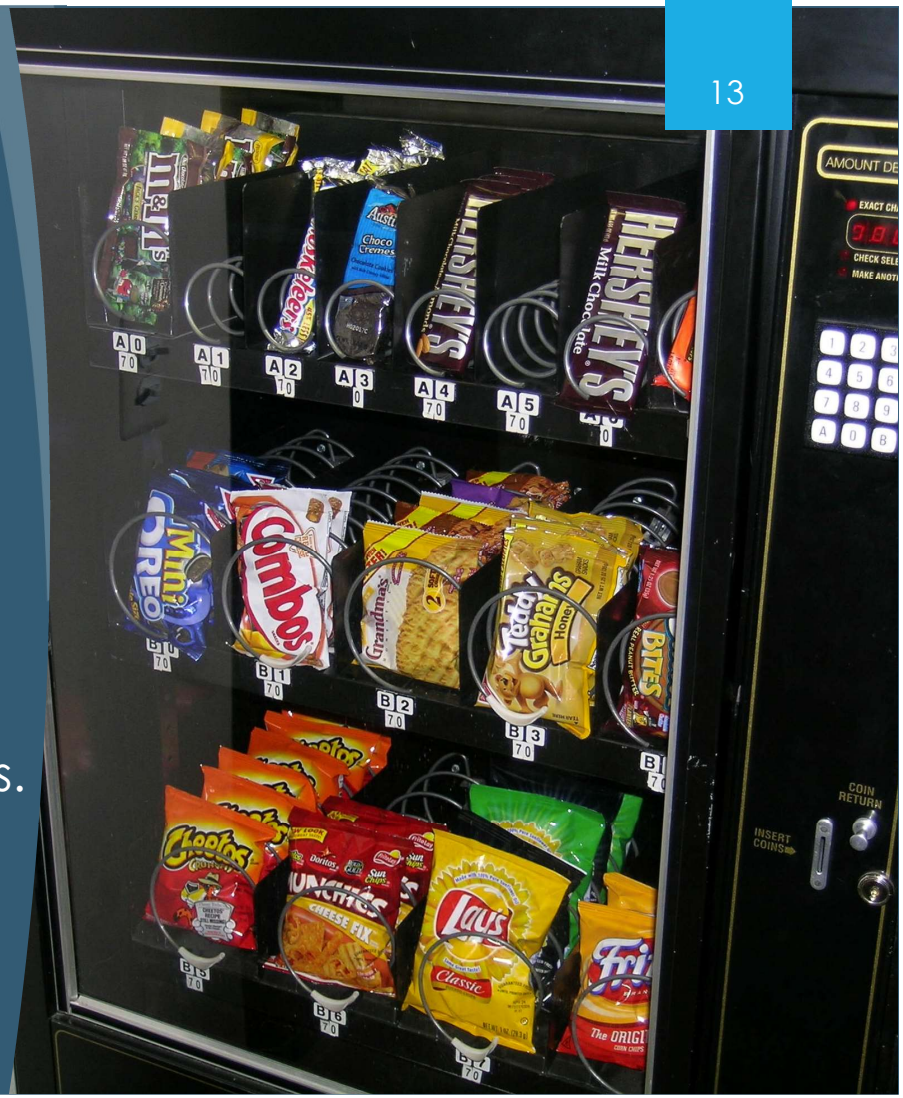
DLT
Distributed
Ledger
Technology
ou
BLOCKCHAIN

PARA A INTERNET DO VALOR



Smart Contracts

- https://youtu.be/ZE2HxTmxfrI
- Nick Szabo 1997.
  - Cientista da computação, criptógrafo, estudioso de direito.
- Contract?
  - Sistema que coordena ações entre partes.
- Smart?
  - Automatizado.
- Na blockchain → Tecnologia institucional.



Ethereum

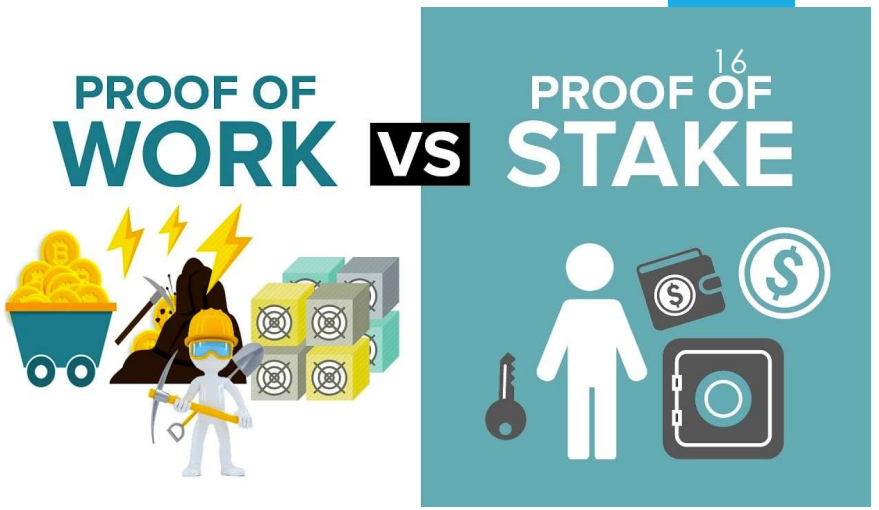
- Criado por Vitalik Buterin em 2015.
- Criptomoeda própria: Ether.
- Conceito de "Computador universal".
- Executa a *Ethereum Virtual Machine* (EVM).
- Linguagem mais comum é a Solidity, que é compilado para o código da EVM.
- Solidity é uma linguagem *Turing Complete*.
- Bitcoin também tem *smart contracts*, mas é uma linguagem de pilha limitada e sem *loops*.

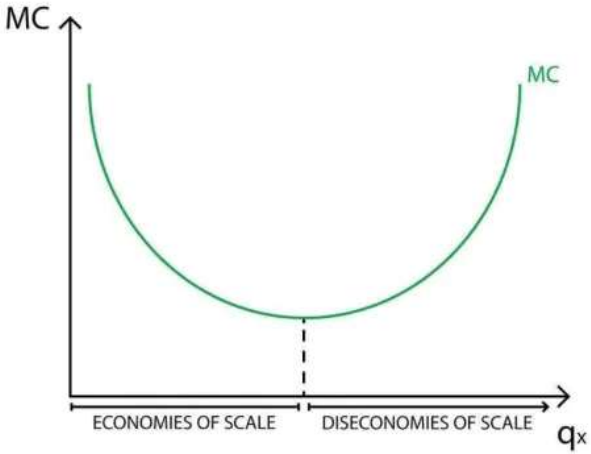
Ethereum

```
contract MyToken
{
    mapping (address => uint256) public balanceOf;

    constructor (uint256 initialSupply)
    {
        balanceOf[msg.sender] = initialSupply;
     }

    function transfer(address to, uint256 value) public
    {
        require(balanceOf[msg.sender] >= value);
        balanceOf[msg.sender] - = value;
        balanceOf[to] += value;
    }
}
```

Proof of Stake

- Block producer sorteado na proporção do stake.
- Not mining/miner → Forging/validator.
- Baixo consumo de energia.
- Maior escalabilidade.
- Menos concentração.
- https://youtu.be/M3EFi_POhps

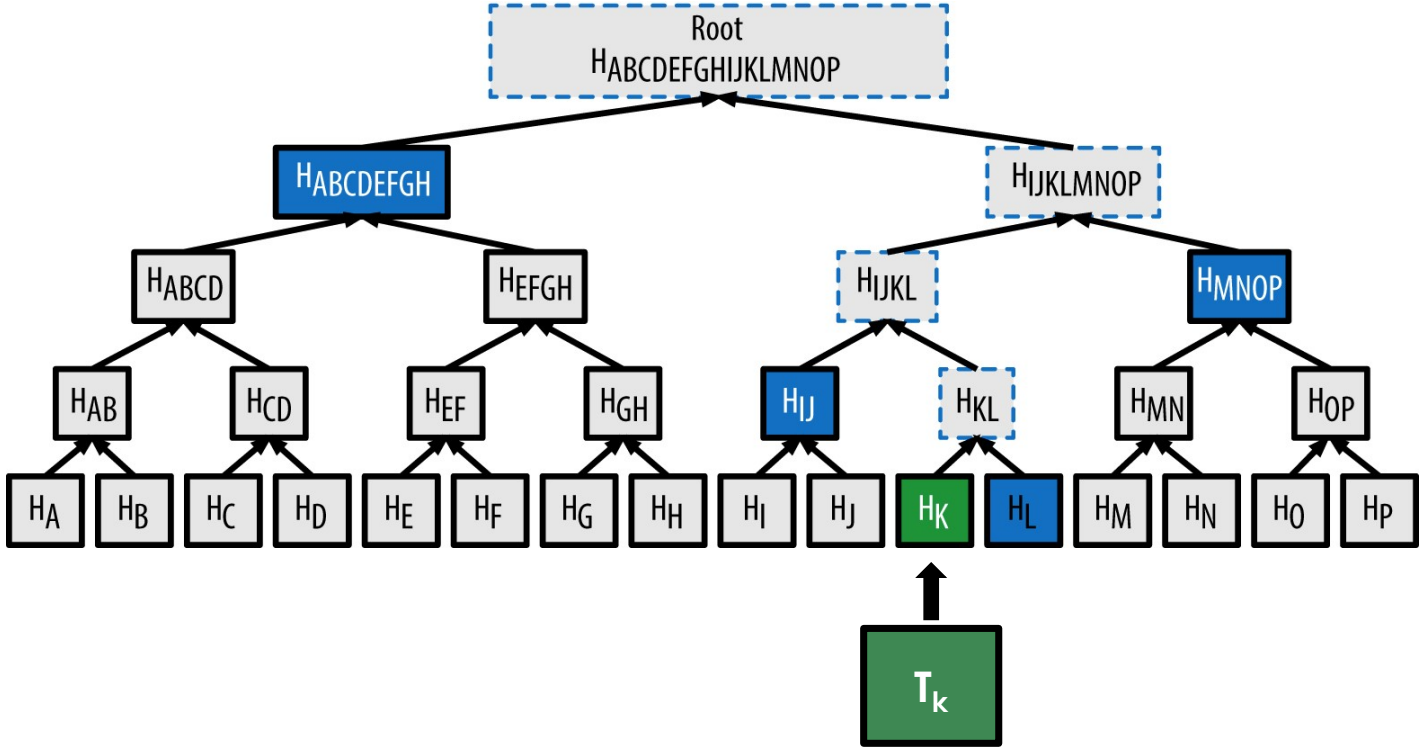




Soluções de Layer 2

- BTC → Lightning Network (https://youtu.be/rrr_zPmEiME).
  - Usa recursos de script do BTC.
  - Cria canais cujos fundos são alocados on chain.
  - Canal é fechado com saldo final liberado on chain.
  - Transações de pequeno valor.
  - Alto desempenho.

Merkle Proofs



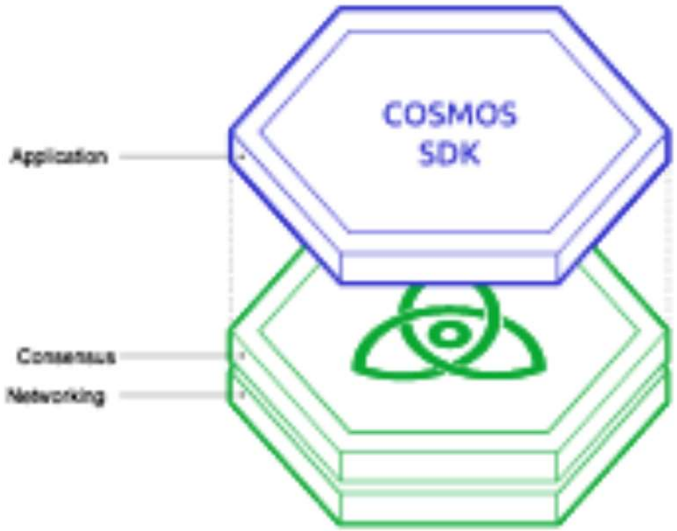
- Permite provar que uma transação estava em um bloco mesmo que:
  - Tenha sido armazenado apenas um *hash*.
  - Com pouco processamento e pouco espaço.

Tecnologias de Suporte

- ZKP —> Zero Knowledge Proof
  - ZK-SNARK
    - Usado para privacidade, geralmente L1
    - Succinct Non-interactive Argument of Knowledge
  - ZK-Rollup
    - Usado para escalabilidade, geralmente L2
- https://youtu.be/OcmvMs4AMbM

Soluções L1 - Cosmos - Internet de Blockchains

- Tendermint BFT – Networking and consensus. Público ou privado.
- ABCI (Application Blockchain Interface) – Qualquer linguagem na camada de aplicação.
- SDK - Reduz custo de implementação de aplicações.
- Blockchains têm alguma independência técnica e de governança.



Desafios

- Taxa de transações
- Consumo de energia
- Experiência do usuário
- Governança
- Regulação
- Geopolítica

Existem Propostas para Soluções Técnicas da Maioria dos Problemas

Valor da Blockchain

- Artigo: Simple Economics of Blockchain (Catalini – MIT).
- […] we rely on economic theory to explain how two key costs affected by blockchain technology - **the cost of verification of state**, and the **cost of networking** - change the types of transactions that can be supported in the economy.
  - https://portaldobitcoin.uol.com.br/so-possivel-fazer-com-blockchain/
- Whereas the reduction in the cost of verification is what allows Bitcoin to settle transactions without an intermediary, the **reduction in the cost of networking is what allowed its ecosystem to scale** in the first place.
- Whereas the utopian view has argued that blockchain has the potential to transform every digital service by removing the need for intermediaries, we argue it is more likely to **change the nature of intermediation by reducing the market power of intermediaries**, and by progressively redefining how they add value to transactions.

DLTs Permissionadas

- Permissionadas x Não permissionadas (públicas):
  - Participação no consenso.
  - Acesso ao *ledger*.
- Algoritmos mais simples: *Proof of Authority*.
  - Não lidam com *Sybil attack*.
  - Não demandam existência de criptomoedas.
  - Não consomem muita energia.
- Não se aplica a redução do custo de networking.

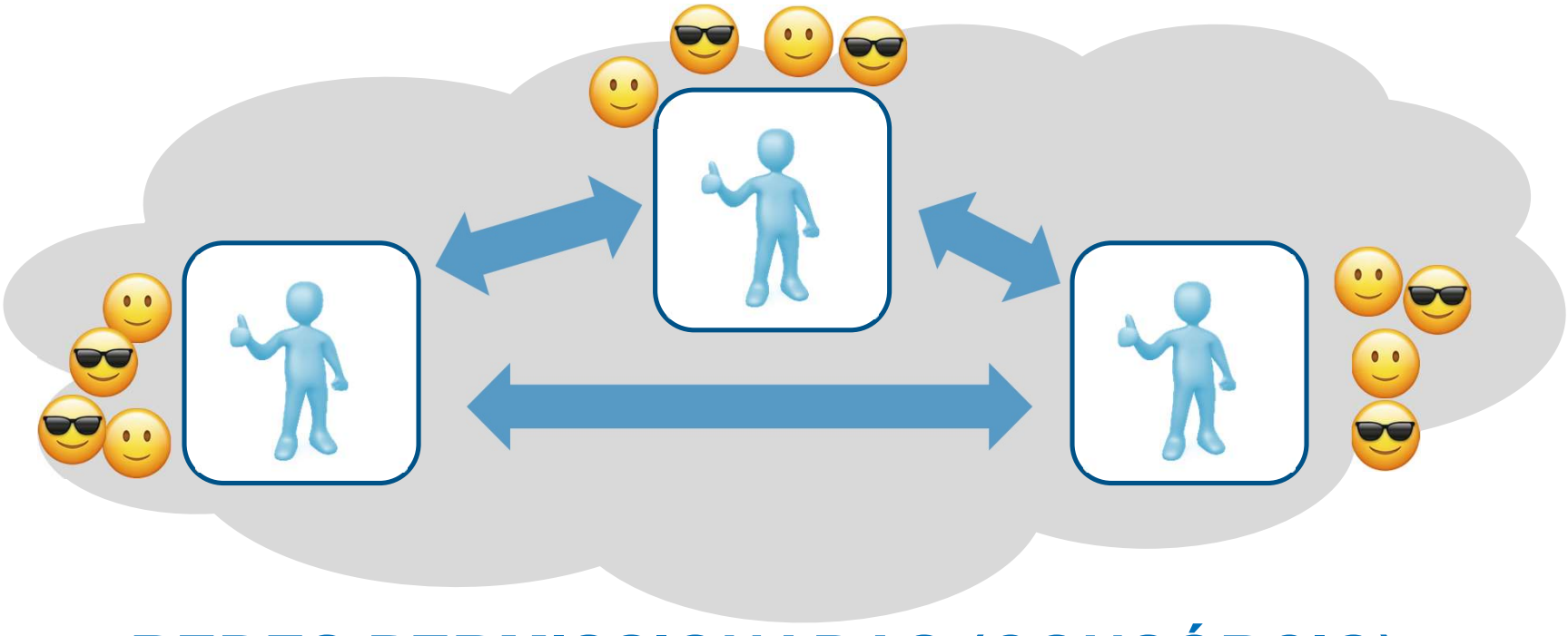
Quorum

HYPERLEDGER FABRIC

corda

Modelos Típicos de Negócio

Modelos Típicos de Negócio



REDES PERMISSIONADAS (CONSÓRCIO)

Tipos de DLTs

Acesso ao *Ledger*

Participação no Consesnso	Permissionada	Pública
Permissionada	HYPERLEDGER FABRIC, corda	RBB, LACCHAIN, EOS
Pública		Ethereum, Bitcoin

Redes Híbridas (Público-Permissionadas)

- Vantagens de ambas as arquiteturas.
  - Menos riscos como as permissionadas (técnicos, regulatório, de imagem etc).
  - Tão descentralizadas e transparentes quanto as públicas.
- Governos e interesse público são potenciais aplicações.
- Rede Blockchain Brasil.
  - Acordo entre BNDES e TCU, com abertura para adesões.
  - Dataprev, Serpro, MG, ES, RNP, CPqD e PUC-RJ.
  - Propósitos: fomentar inovação em transparência; confiança.

Aplicações de Blockchains Permissionadas

Cadeias de valor

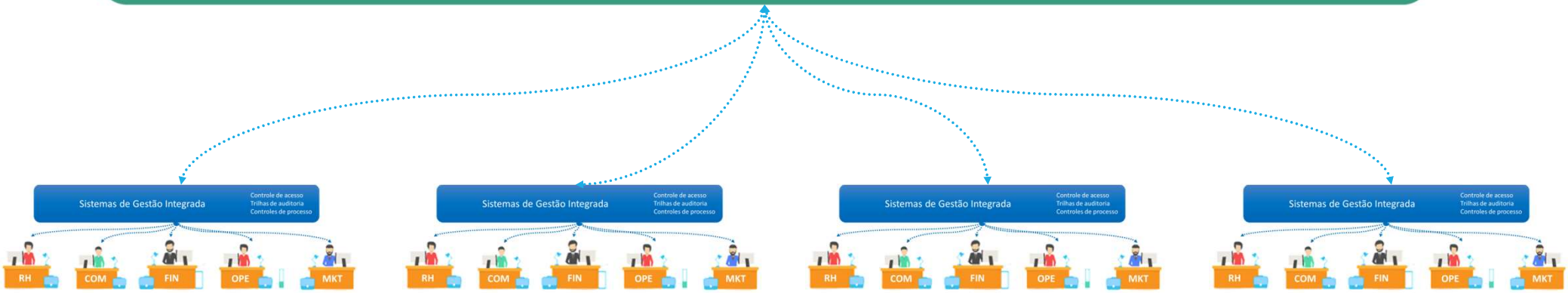
Qualidade
Rastreabilidade
Conformidade
Legalidade
Procedência
Certificação
Transparência

Blockchains Permissionadas // Novas Cadeias de Valor

Blockchains Permissionadas // Novas Cadeias de Valor

Blockchains Permissionadas // Novas Cadeias de Valor

Sistemas com Suporte de Blockchain



Bitcoin x Dólar x CDBC

- Diretrizes do Bacen:
  - https://www.bcb.gov.br/detalhenoticia/548/noticia
- LIFT Challenge Real Digital:
  - https://www.bcb.gov.br/detalhenoticia/612/noticia

bitcoin

DeFi

Decentralized Finance

DeFi – O que é?

- Referência: DeFi Beyond the Hype. The Emerging World of Decentralized Finance. Maio 2021. Wharton Wharton Blockchain and Digital Asset Project (Universidade da Pensilvânia) e World Economic Forum.
  - Serviços financeiros descentralizados.
  - Operação e liquidação com necessidade reduzida de confiança.
    - Baseado em *smart contracts*.
  - *Non custodial* → Cliente é responsável pela custódia dos ativos (chave privada).
  - Aberto e programável.
    - Seguem a filosofia *open source*.
  - *Money legos*.
- Sem barreira de entrada (*permissionless*) e sem KYC etc.

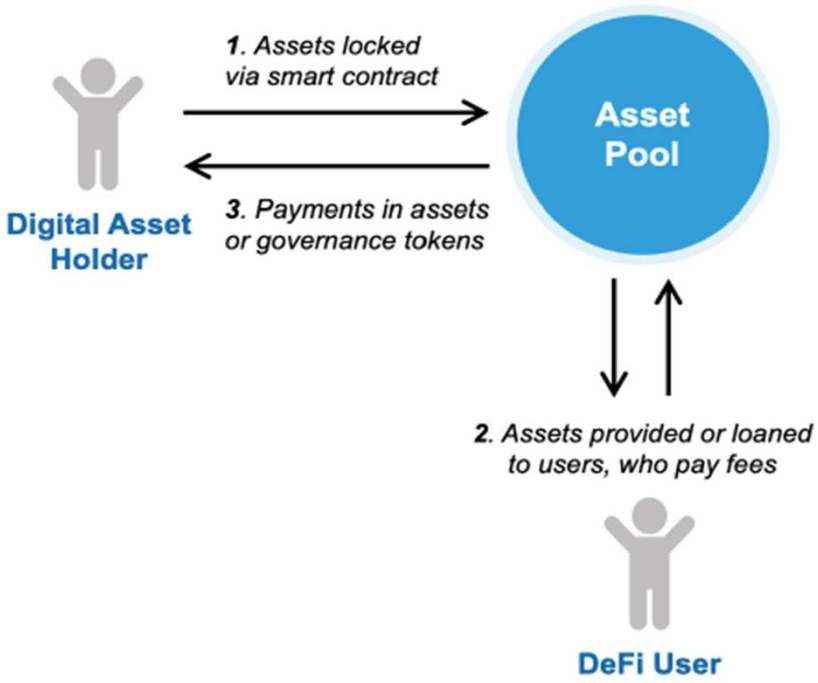
DeFi – Principais serviços

- *Stablecoins.*
- *Decentralized exchanges* - DEXes.
- Empréstimos.
- Derivativos.
- Seguros.
- Serviços agregadores (como os de *yield farming*).
- CeDeFi.
  - Aplicações DeFi sobre infraestruturas não tão descentralizadas.
  - Binance Smart Chain.

Incentivos

- Objetivos.
  - Liquidez.
  - Governança do protocolo.
- Diferentes formas de cobrança/remuneração.
  - Juros pagos por tempo de *lock-up*.
  - Taxas de liquidação.
  - *Liquidity mining* → Pagamento em tokens do próprio serviço.
- *Yield farming* → Busca de melhores retornos pela realocação de fundos.
- Busca por relacionamento de mais longo prazo.

FONTE: WHARTON AND WEF REPORT

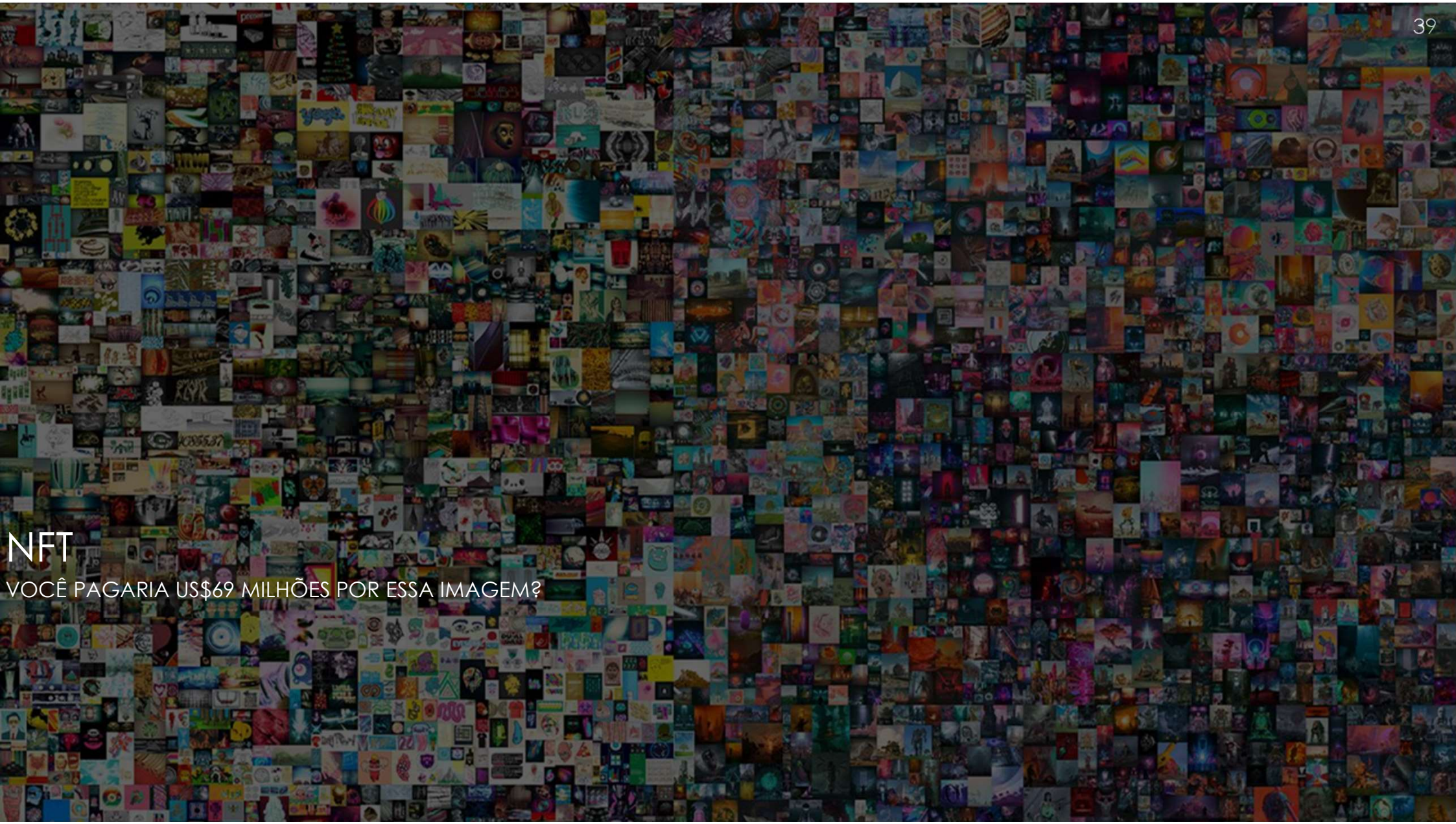


NFT

Non Fungible Tokens

NFT – O que é?

- Ativo é fungível quando trocar um item por outro não faz diferença.
  - Ouro, *commodities*, notas de dinheiro etc.
  - Atributo importante de ativos que se tornam dinheiro.
- Ativo não fungível representa algo que não pode ser trocado por outro sem que isso faça diferença.
  - Digital ou do mundo real.
- O uso mais comum tem sido para colecionáveis digitais.
  - Colecionáveis digitais (ex.: cryptokitties), arte, cartões de jogadores, itens em jogos (incluindo terrenos), endereços, itens de um metaverso, DNS etc.
- Podem evoluir para direitos de propriedade físicas.
- https://nonfungible.com



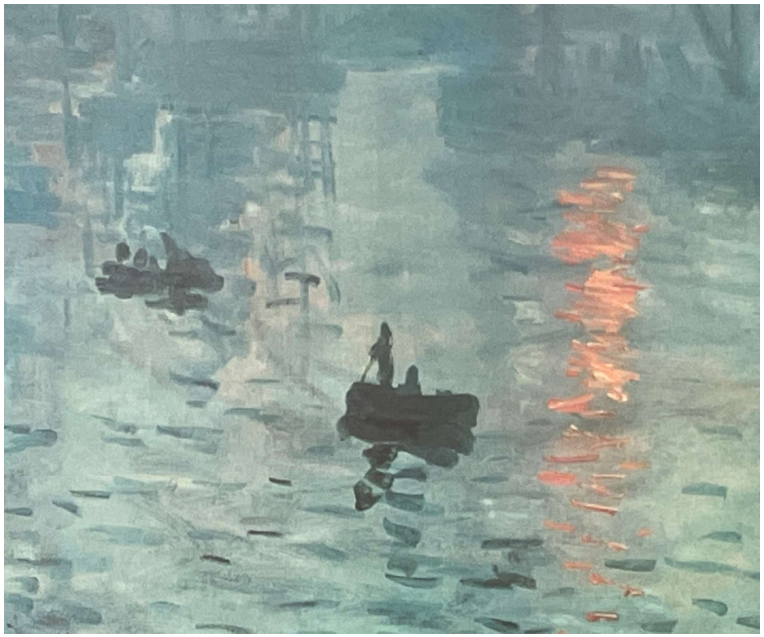
NFT

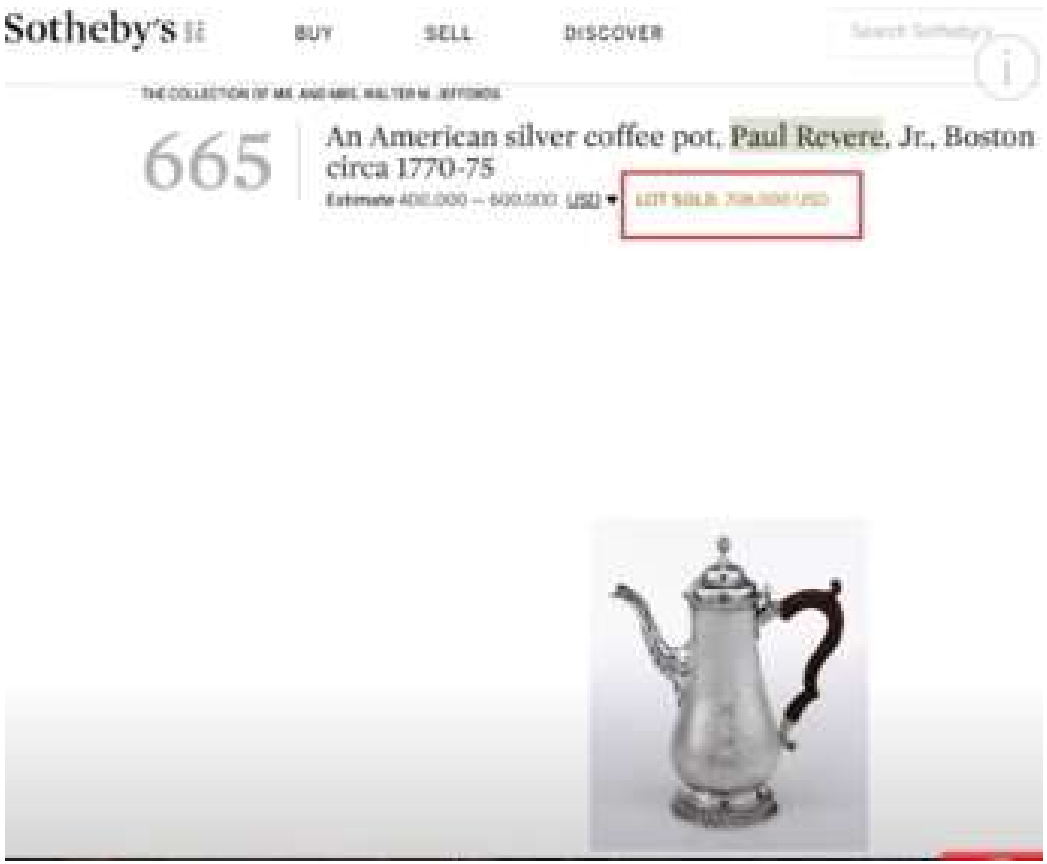
VOCÊ PAGARIA US$69 MILHÕES POR ESSA IMAGEM?

NFT

E US$170K POR ESSE BICHINHO?

NFT e a originalidade





NFT

E US$700K POR ESSA TAÇA?

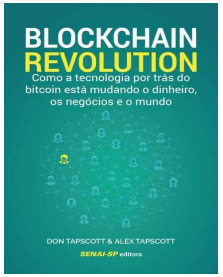
HTTPS://YOUTU.BE/E6GLSIYYIE0

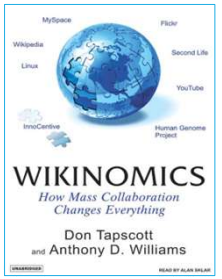
CANAL COIN BUREAU.

DAOs

Decentralized Autonomous Organizations

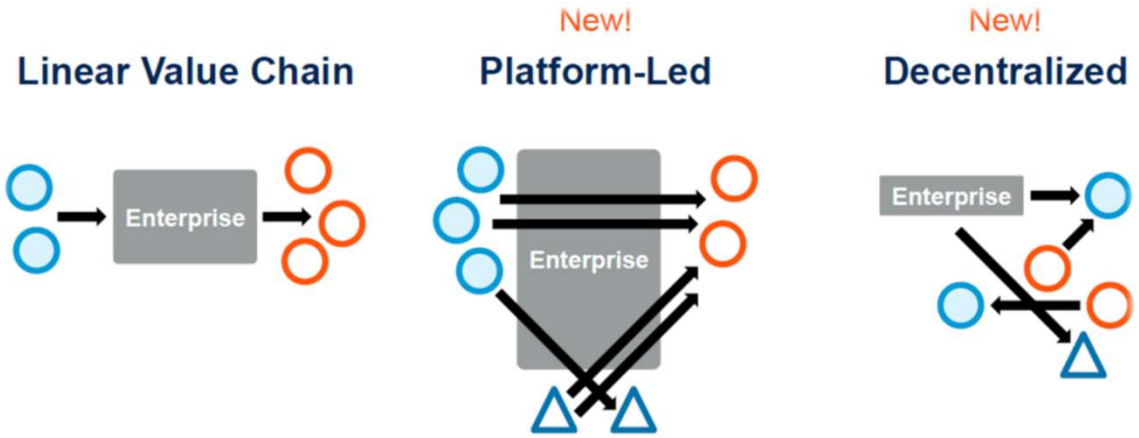
A promessa

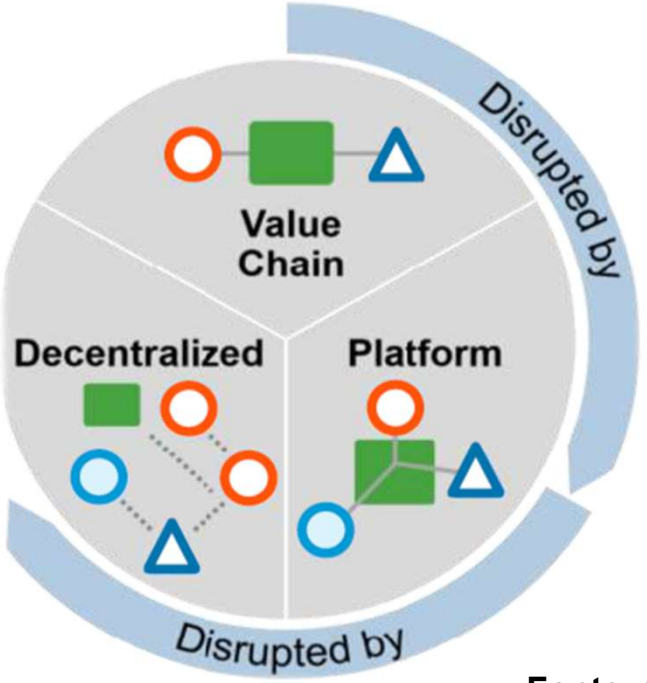




Criação de uma economia verdadeiramente colaborativa

O futuro após as plataformas?





Fonte: Gartner

Decentralized Autonomous Organizations

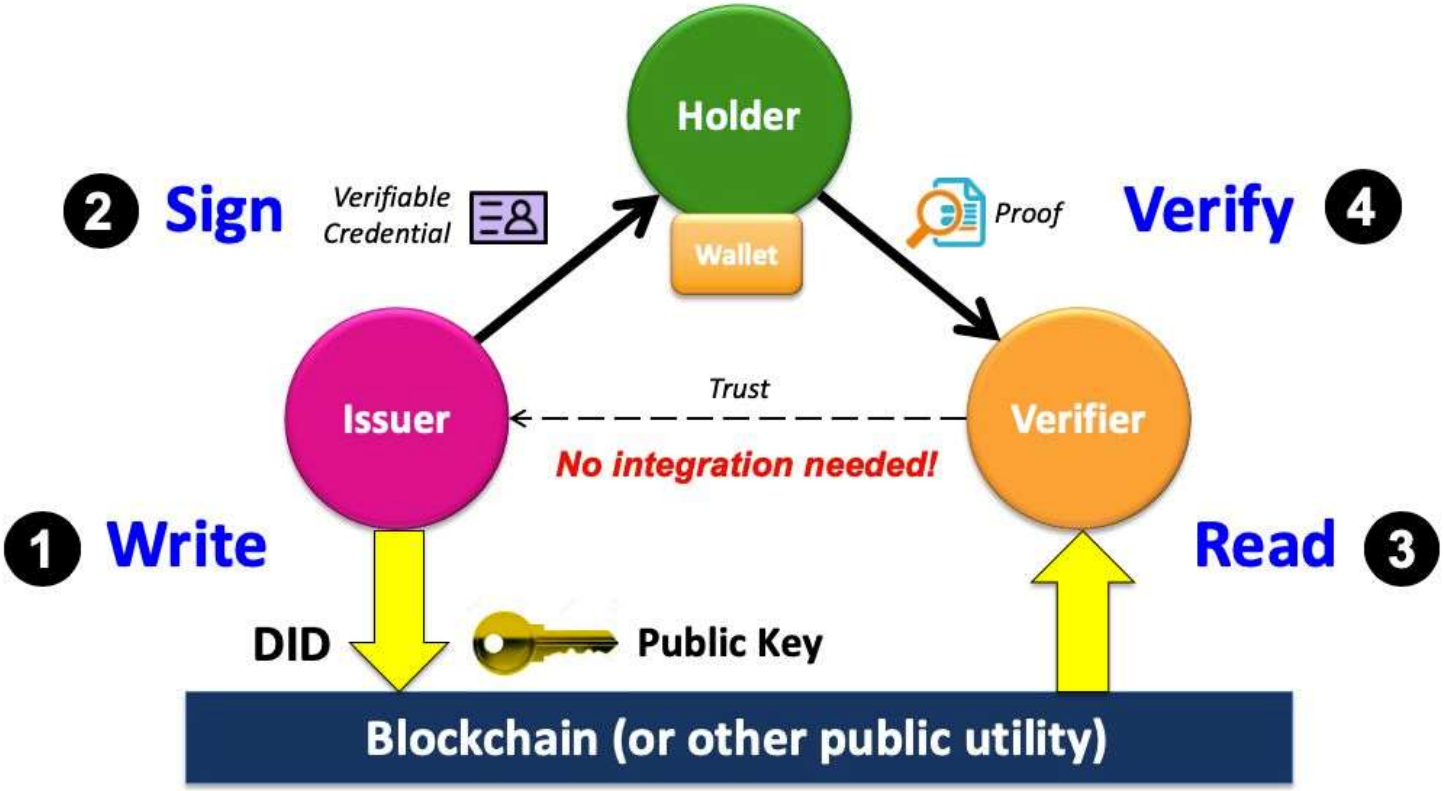
Decentralized Autonomous Organizations

- Costumeiramente, um token define o peso dos votos.
  - Viés financeiro.
  - Soluções como DAOStack tentavam separar tokens financeiros de tokens de reputação.
  - Outras opções são possíveis: caso do DAO da Escadaria Selaron.
- Soluções para dar validade jurídica a DAOs.
  - DAO LLC no Wyoming e Delaware.
  - OtoCo.io → "On-chain legal entities and legal tools for crypto freelancers, web3 teams, and DAOs".

Decentralized Identity

Identidades Auto Soberanas e Credenciais Verificáveis

Self Sovereign Identity

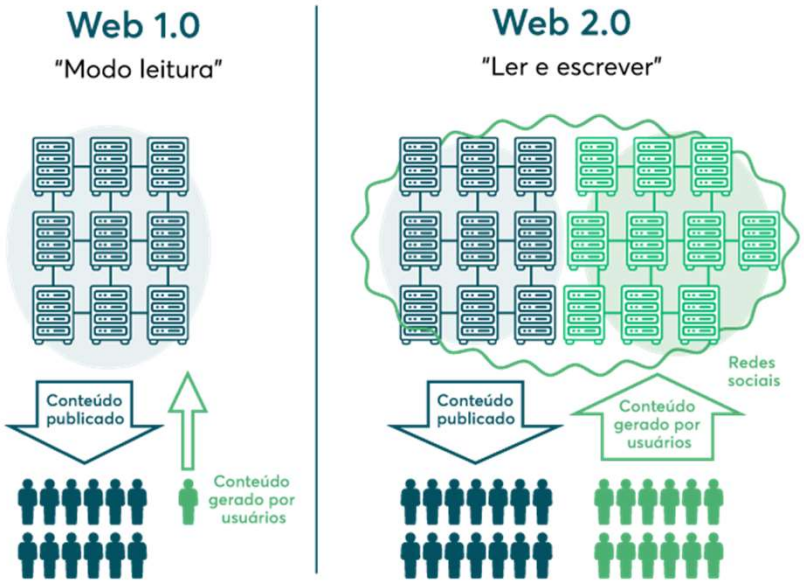


Web 3.0

Decentralized Web Business Architecture

Web 3.0

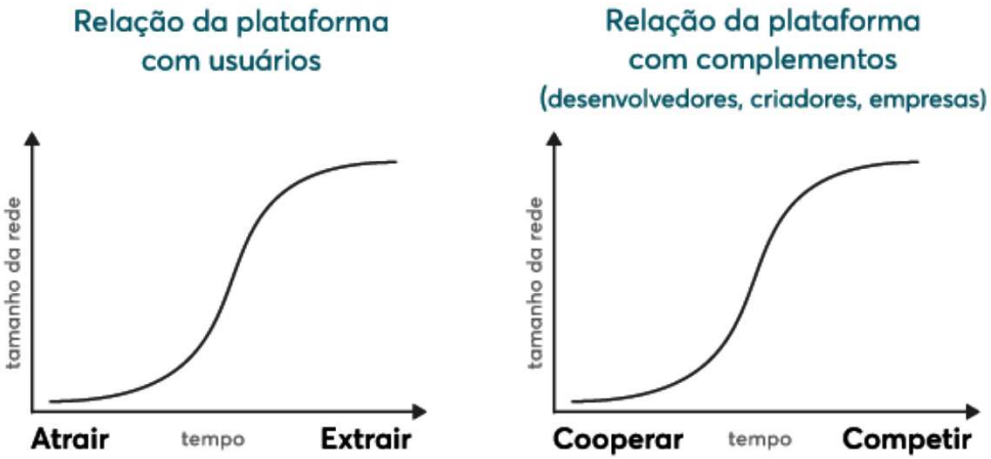
- Na Web 1.0, as empresas proviam informações e, no nível mais avançado, serviços.
- A Web 2.0 trouxe as plataformas orquestradoras de mercado os *matchmakers*.
- A Internet foi "centralizada".
  - Não há mais tanto World Wide Web.
- Para muita gente, a Internet são as plataformas.
  - Redes sociais, Uber etc.



https://ip-capitalpartners.com/reports/web-3/

Web 3.0

- Mercado de externalidades (efeitos de rede): quanto maior a rede, mais valor.
  - O foco é criar a rede a qualquer custo.
- No que tange à economia dos dados:
  - 300 Gbytes/s produzidos.
  - 1% processado.
  - Em silos → Seus dados não são seus.
    - Como os dados bancários antes do Open Banking (Finance).
  - Vantagens para desproporcional para "senhores feudais" dos dados.
    - Inclusive países.



https://ip-capitalpartners.com/reports/web-3/

Web 3.0

- Dados dos usuários.
  - Nas carteiras.
    - Extensão das identidades descentralizadas e NFTs.
  - Possíveis "bancos" ou cooperativas de informações, gerando renda para usuários.
  - Dados mais disponíveis para processamento de modelos.
- Identidades autossoberanas e credenciais verificáveis viabilizando reputação.
- Composição de serviços.
- Monetização do open source.

Web 3.0

Tokens Fungíveis

Tokens Não Fungíveis

Credenciais Verificáveis

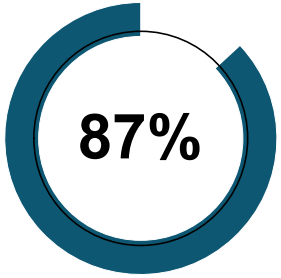
Diversos (?) “Dinheiros”

Perspectiva Histórica

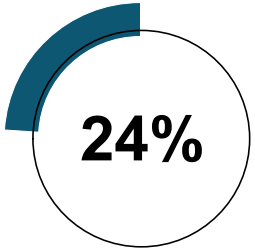
Desconfiança

An Implosion of Trust

Edelman trustbarometer 2017 | ANNUAL GLOBAL STUDY



entrevistados preocupados com corrupção



grau de confiança no governo

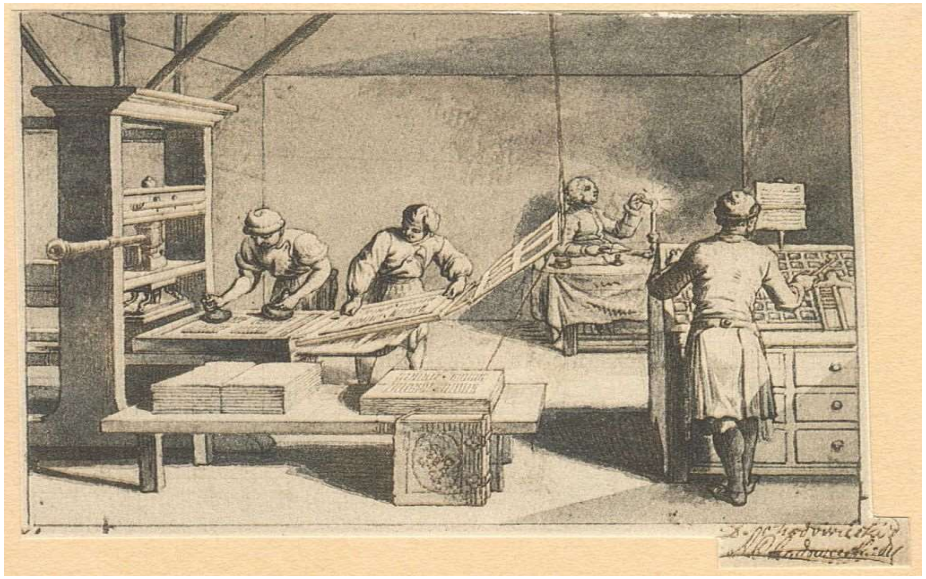
26ª posição de 28 países pesquisados

A confiança chega a pé e vai embora de Ferrari.
Mark Carney, presidente do Banco da Inglaterra

BANK OF ENGLAND

Perspectiva histórica

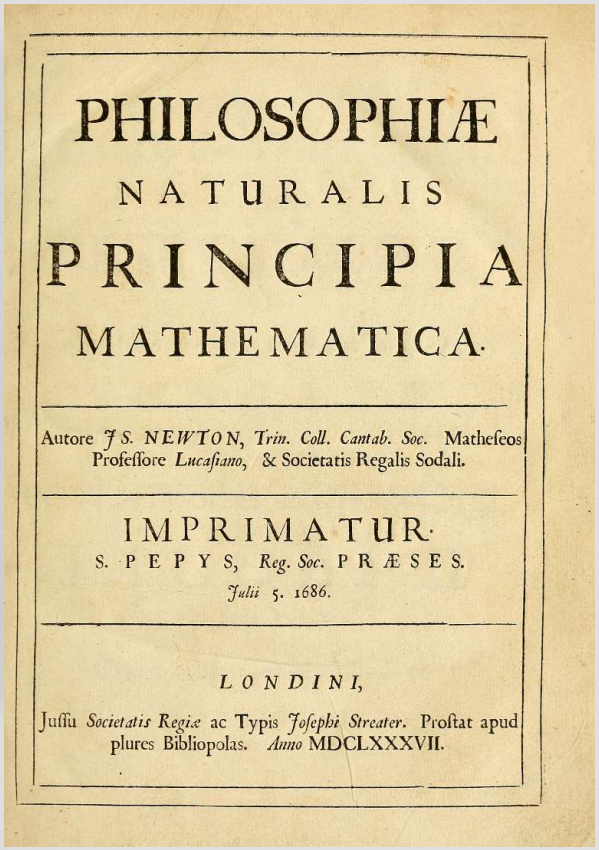
1989
Sir Tim Berners Lee



1450
Gutenberg

The Truth

The Power



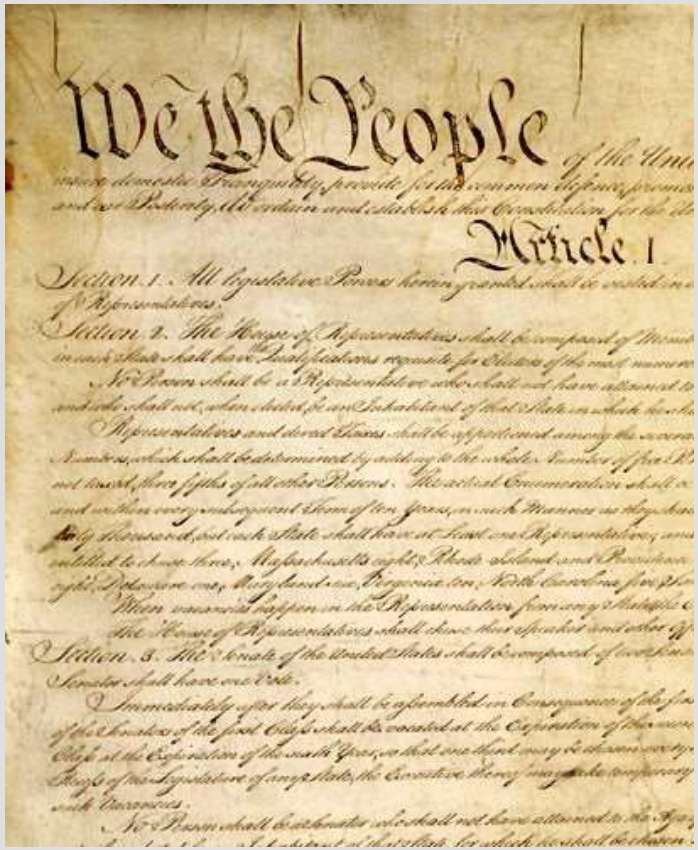
PHILOSOPHIÆ
NATURALIS
PRINCIPIA
MATHEMATICA.

Autore *J S. NEWTON, Trin. Coll. Cantab. Soc.* Matheſeos Profeſſore *Lucaſiano*, & Societatis Regalis Sodali.

IMPRIMATUR.
S. PEPYS, *Reg. Soc.* PRÆSES.
Julii 5. 1686.

LONDINI,
Juſſu *Societatis Regiæ* ac Typis *Joſephi Streater.* Proſtat apud plures Bibliopolas. *Anno* MDCLXXXVII.

Decentralizing The Truth

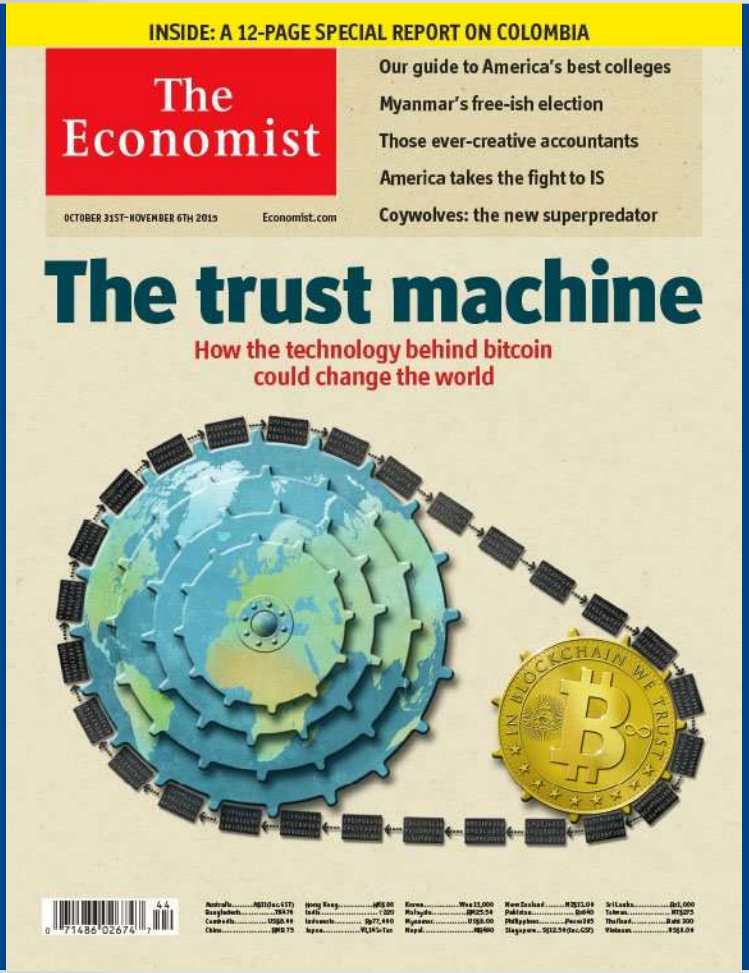


We the People

Article 1

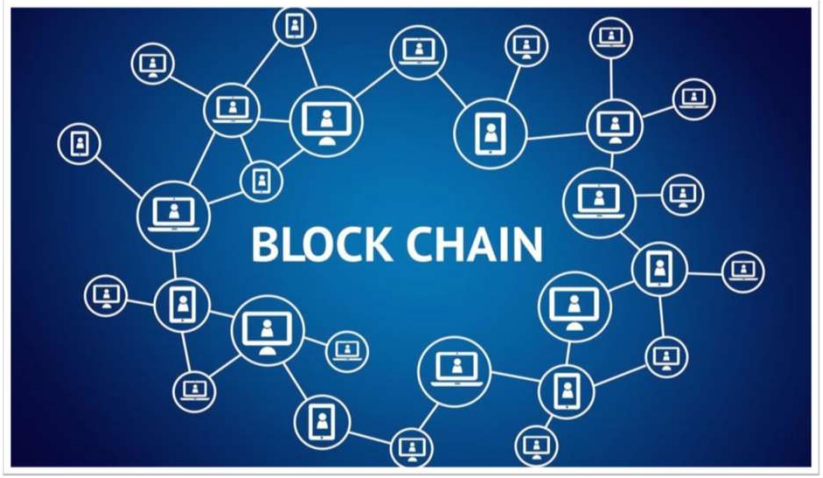
Decentralizing The Power

Trustless Trust



A MÁQUINA DA CONFIANÇA

Perspectiva histórica

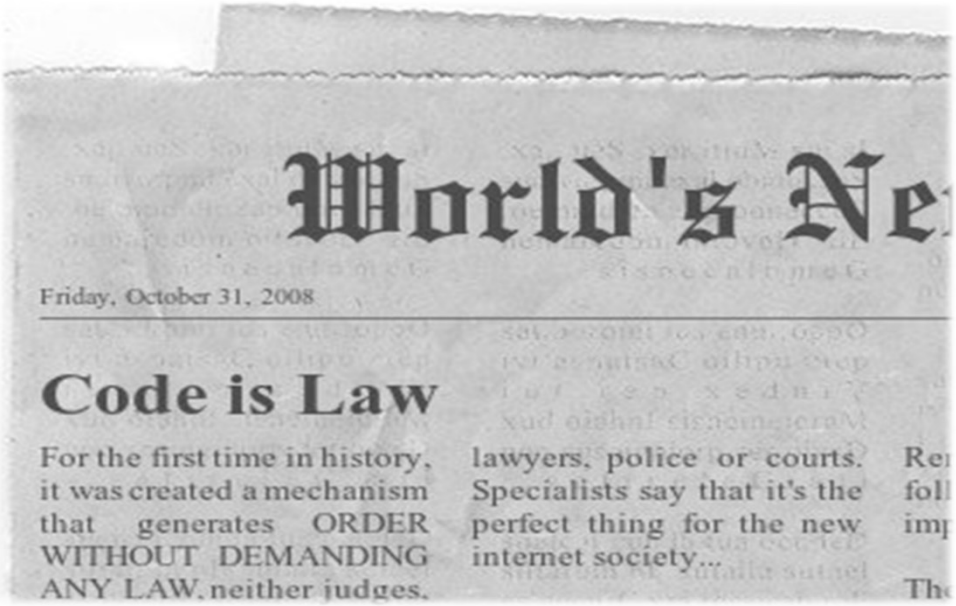


2008 A.D. – Satoshi Nakamoto
Internet (Global)

4000 B.C. – ???
Sumerian (Mesopotamia)

https://portaldobitcoin.uol.com.br/das-tabuas-de-argila-da-babilonia-ao-blockchain-da-sociedade-global/

Perspectiva histórica



World's Ne

Friday, October 31, 2008

Code is Law

For the first time in history, it was created a mechanism that generates ORDER WITHOUT DEMANDING ANY LAW, neither judges, lawyers, police or courts. Specialists say that it's the perfect thing for the new internet society...

Lex Cryptographia

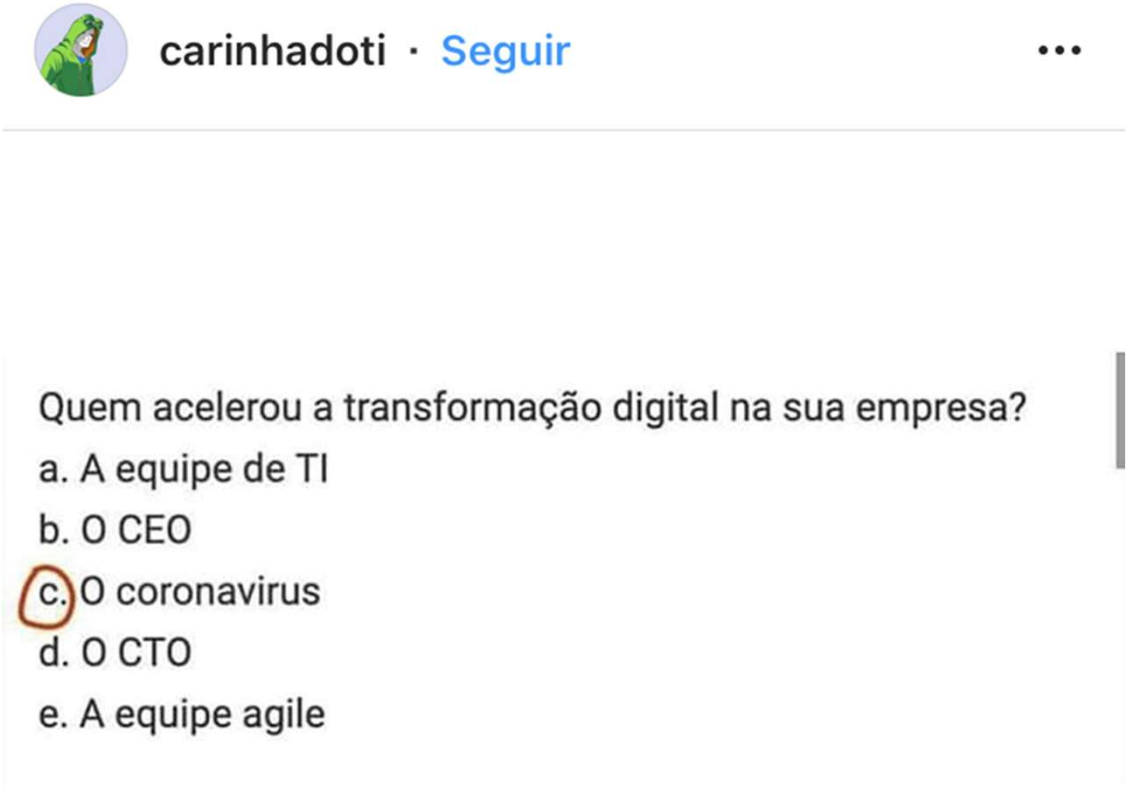
Transição Geracional

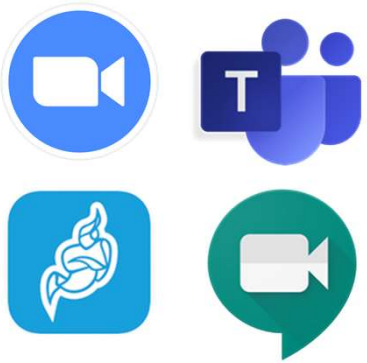
Geração Z
a caminho das decisões

Millenials
na fase adulta:
24-39 anos

Geração Alfa:
a primeira
100% digital

Pandemia COVID





- **Gerações menos digitais foram empurradas para o digital.**
- **Nômades digitais.**
- **Empresas digitais podem estar em qualquer lugar.**

Desmaterialização

https://youtu.be/1h3Qcdl8bKg

Metaverso → A Realização do Cyberespaço
A desmaterialização do espaço

Dinheiros digitais

Bitcoin as a Legal Tender

Stable Coins

Central Bank Digital Currencies

Contratos sem fronteiras
Empresas descentralizadas
Identidades descentralizadas
Outros ativos tokenizados e descentralizados

Government as a Service

Qual o próximo *business* a sofrer disrupção?

MÚSICA

TURISMO

MÍDIA E IMPRENSA

FINANÇAS

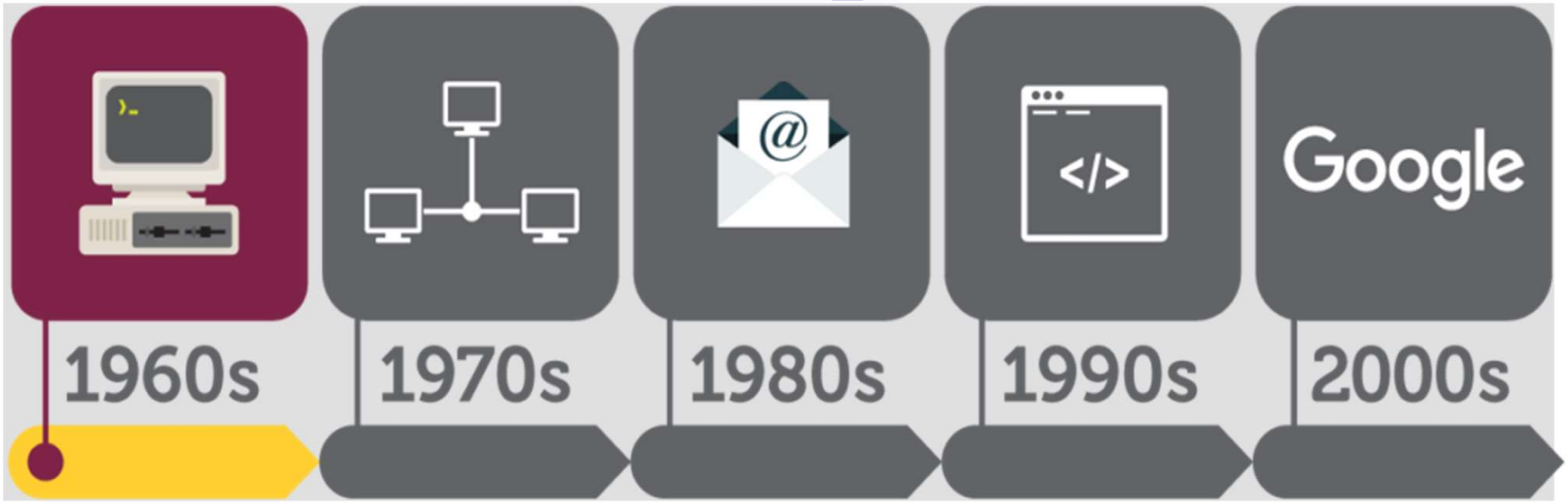
TRANSPORTE

SAÚDE

ESTADO NACIONAL?


Where Are
We Now?

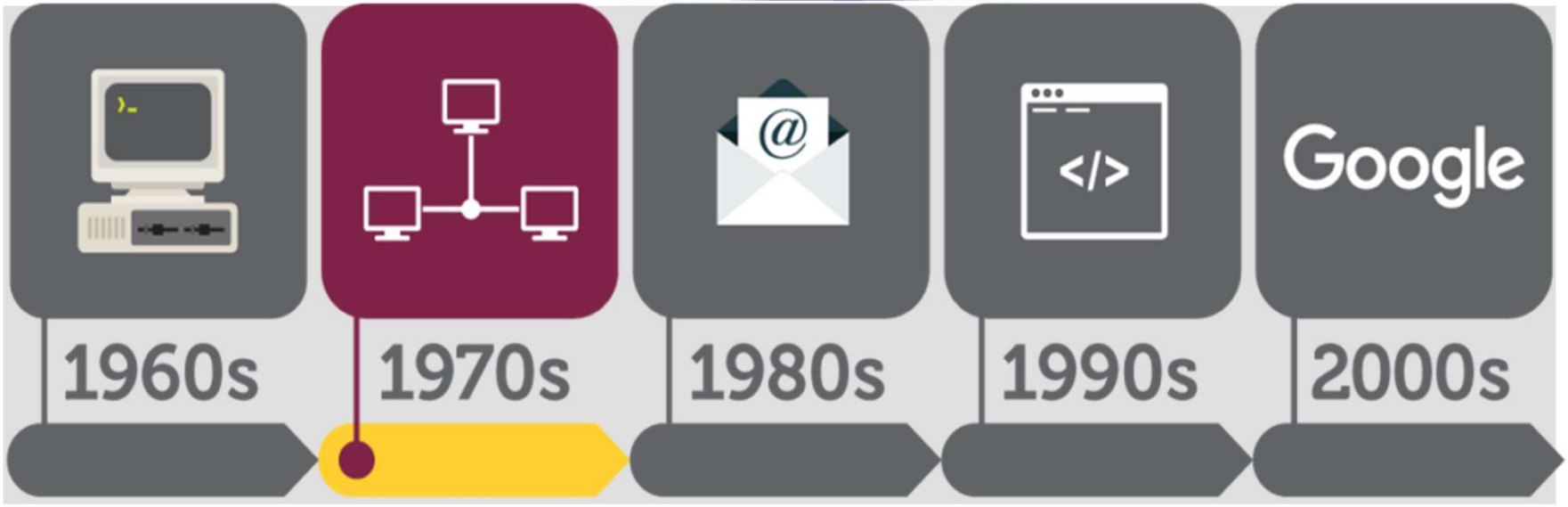
A Internet como paralelo



Proposta de roteamento por pacotes

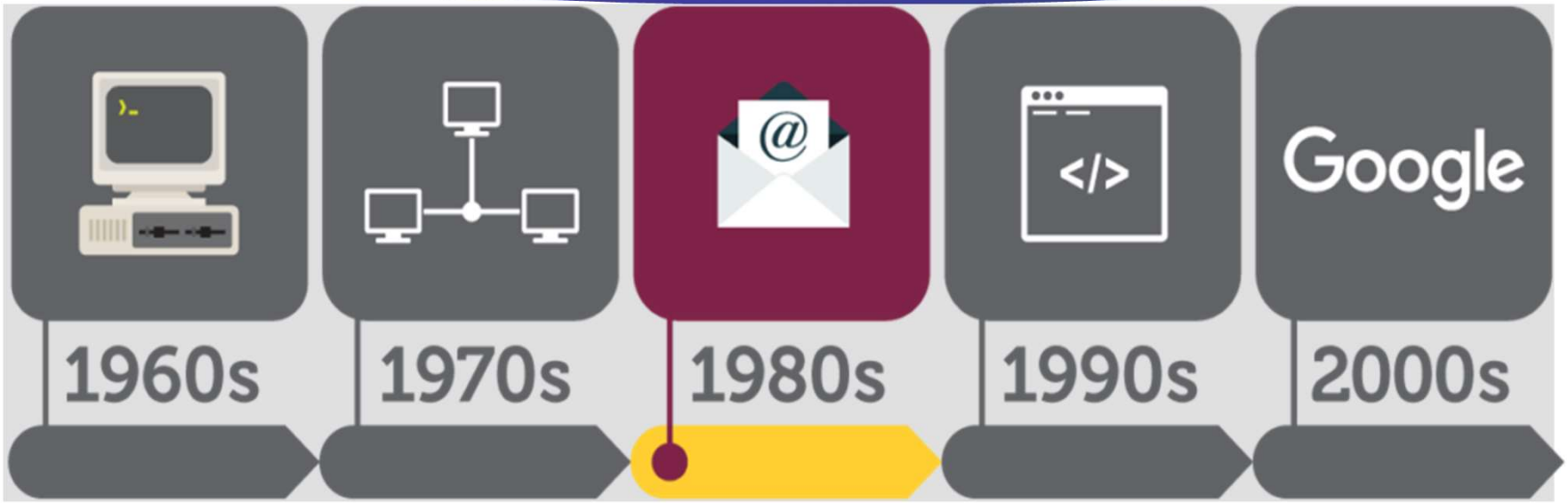
Criação da ARPANet

A Internet como paralelo



Criação do TCP/IP

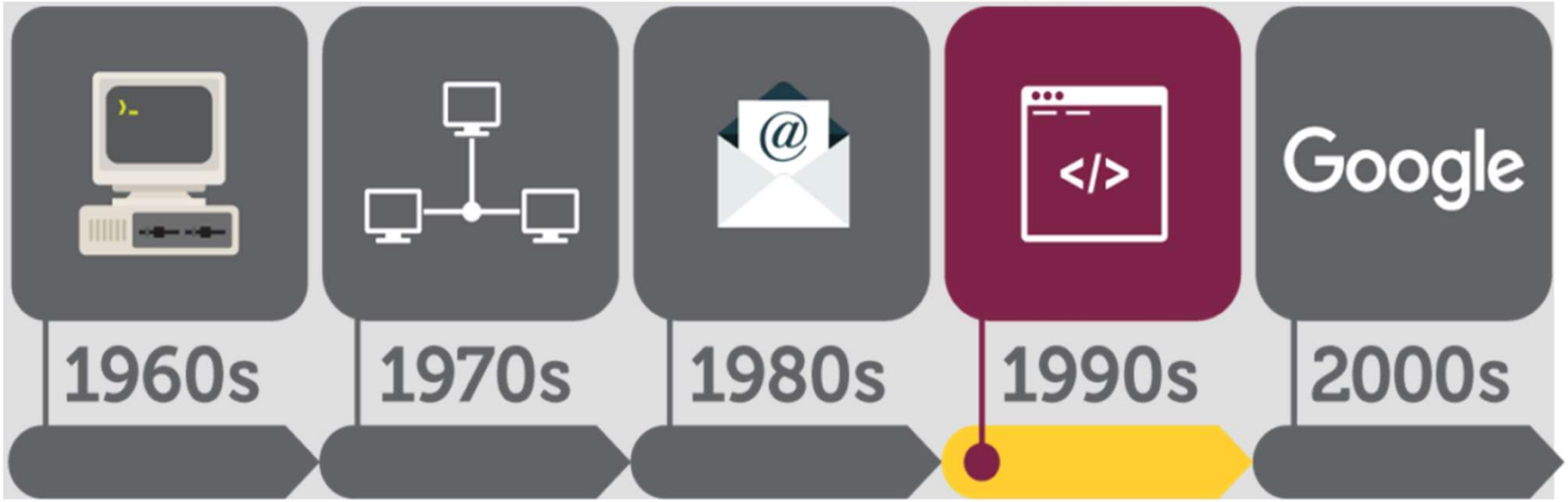
A Internet como paralelo



Criação do DNS

Primeiro registro: symbolics.com

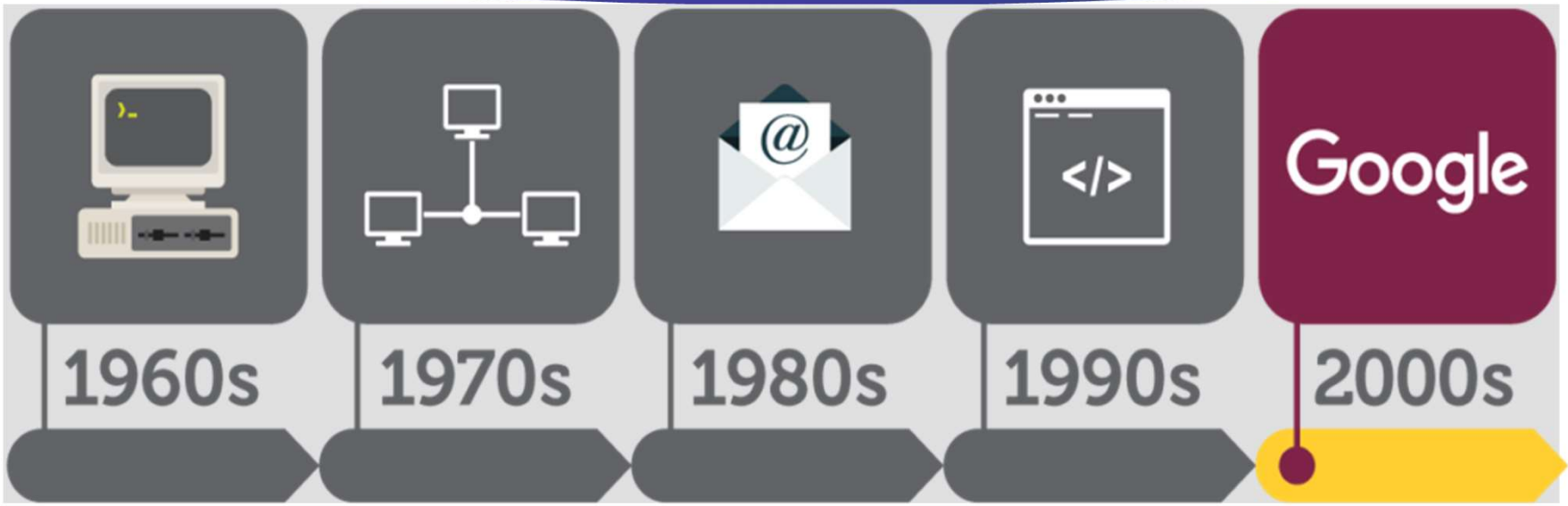
A Internet como paralelo



Sir Tim Berners-Lee cria o WWW

HTML + URL + HTTP

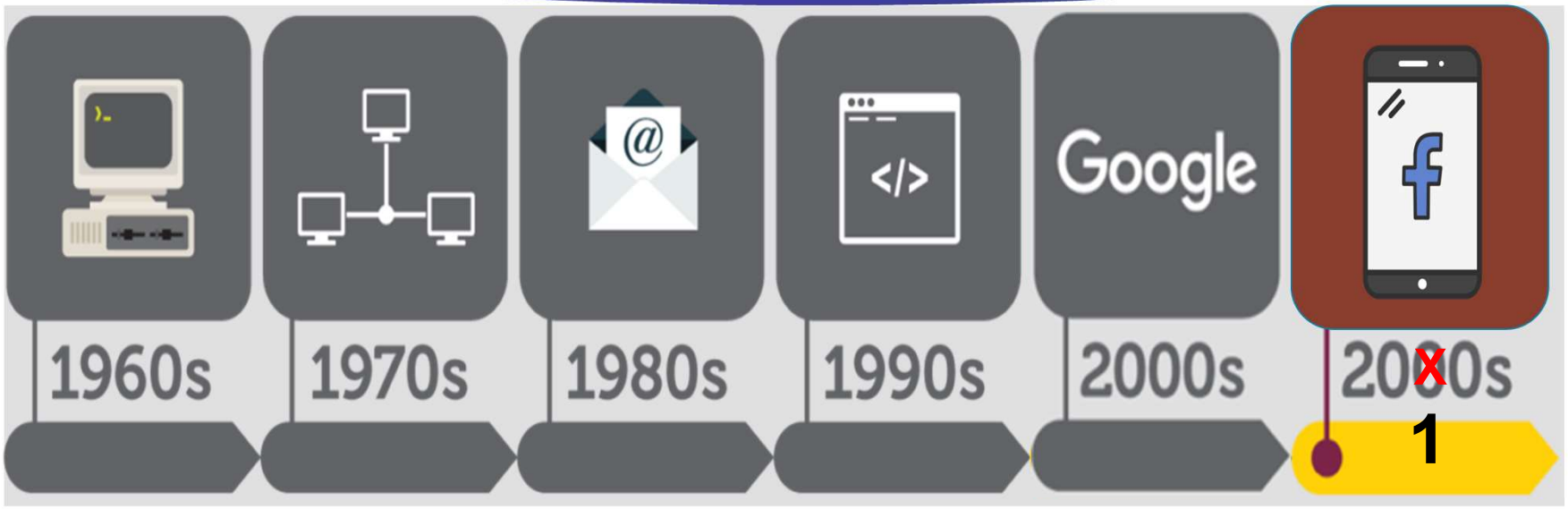
A Internet como paralelo



Estouro da bolha .com

Início da Web 2.0

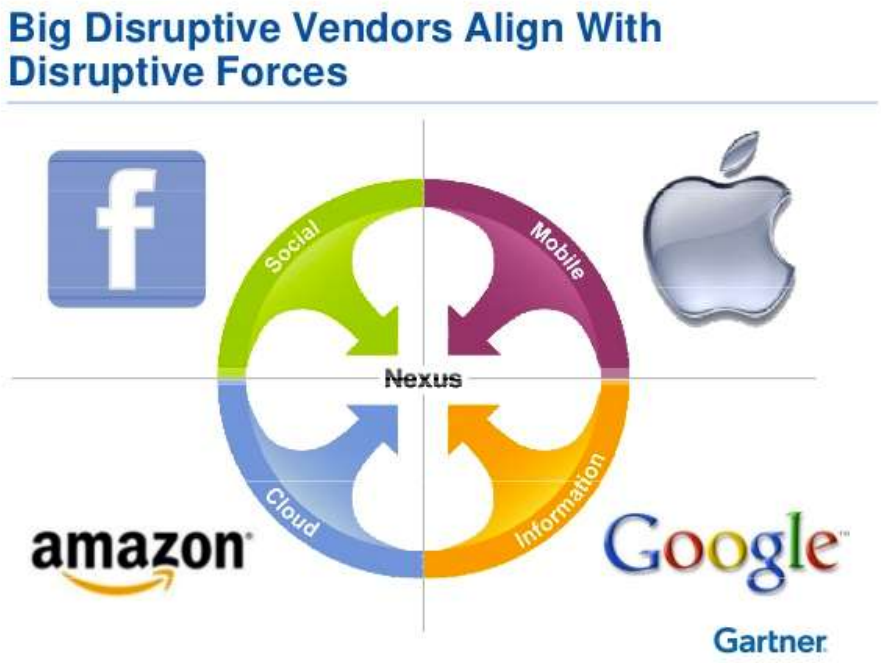
A Internet como paralelo



Convergência com outras tecnologias

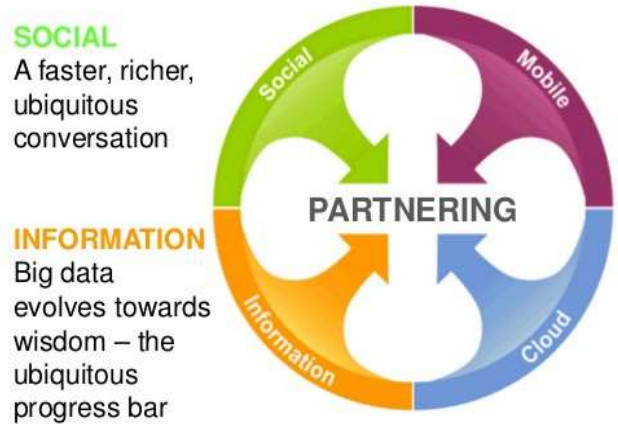
Data-based business models supremacy

Convergência tecnológica



Convergência anterior → Web 2.0

Convergence of Four Independent Trends are Shaping New Business Models



Source: Gartner, Nexus of Forces

Qual a próxima convergência???

Inteligência artificial

IoT

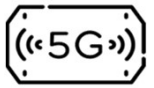
Drones

Blockchain DLT

Big Data/ Data Science

Robótica

Realidade virtual / aumentada



Internet 5G

Impressão 3D

Harvard Business Review

TECHNOLOGY

The Truth About Blockchain

by Marco Iansiti and Karim R. Lakhani

FROM THE JANUARY–FEBRUARY 2017 ISSUE