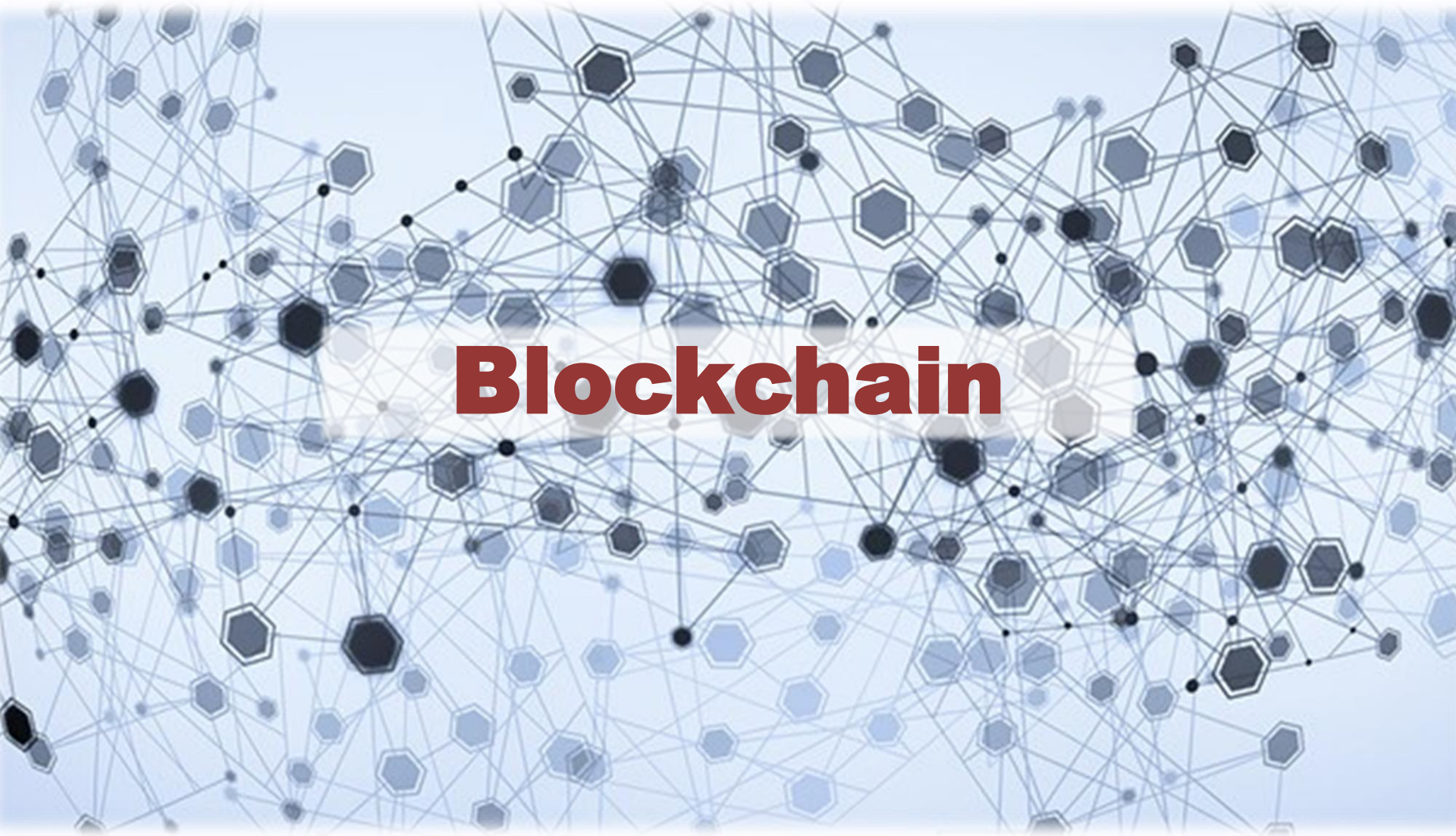
inovalab

Coordenadoria da Administração Tributária - CAT
Diretoria de Informações - DI

GOVERNO DO ESTADO
SÃO PAULO
Secretaria da Fazenda


Blockchain

Por que é relevante?

O que é Blockchain?

Como o Blockchain pode afetar a AT?

Ativo

Pode ser entendido como a **resposta**

que temos a uma **necessidade**

específica e persistente,

à qual associamos um valor.

Pedra RAI submersa

Evolução de um ativo

Redução do custo de transação

Escassez

Necessidade: Memória

Meio: Câmera fotográfica
Filme em rolo

Ativo: Fotografia Impressa

Comoditização

Necessidade: Memória

Meio: Câmera digital

Ativo: Fotografia Digital

Democratização

Necessidade: Memória

Meio: Smartphone

Ativo: *Foto no Instagram*

Baseado em: GARTNER - BSYML6 - ID2a - To the Point Blockchain - Surfing the Democratiza - 332369

Escassez

Padrão Ouro

Comoditização

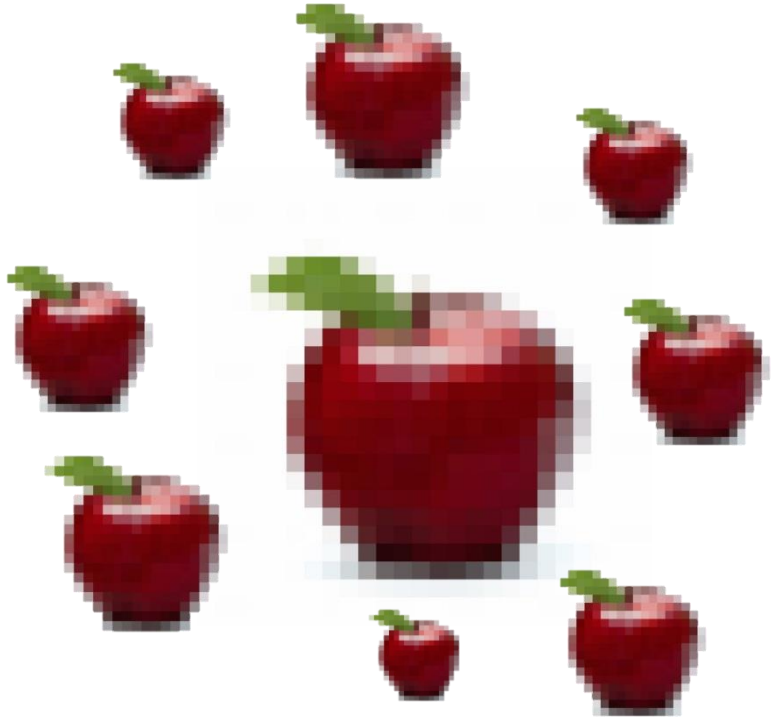
Moeda Fiduciária

Democratização

Criptomoedas

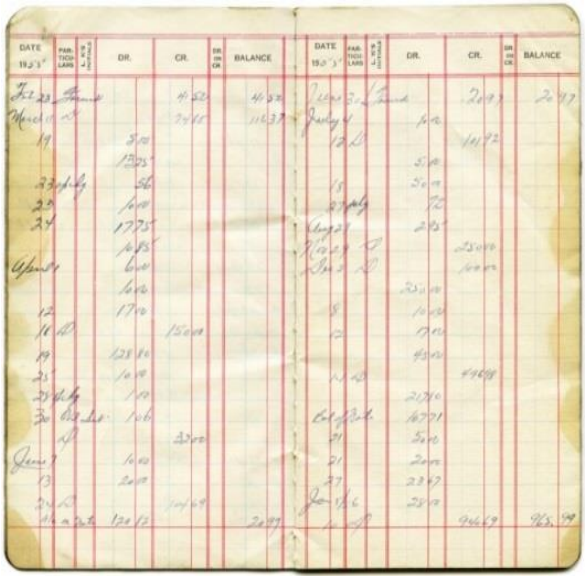
Moeda

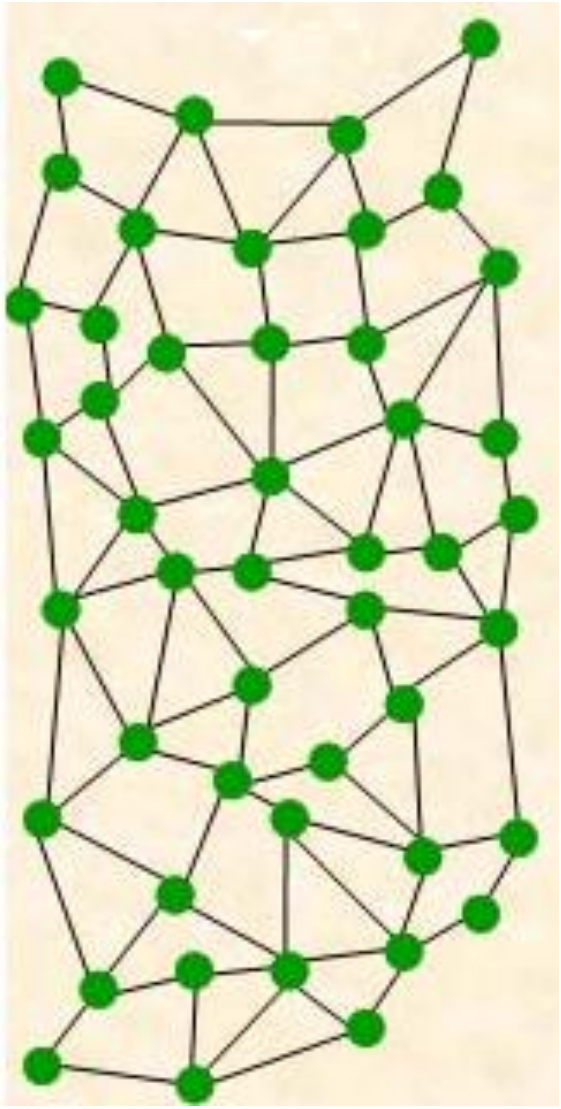
Baseado em: GARTNER - BSYML6 - ID2a - To the Point Blockchain - Surfing the Democratiza - 332369



Problema do Gasto Duplo

Livro Razão





Rede Distribuída

Viabilizar a transação de **Ativos Digitais,** por meio de uma **base de dados distribuída,** que permite armazenar informações em uma lista sempre crescente de registros verificáveis.

Livro-razão compartilhado

Por que é relevante?

O que é Blockchain?

Como o Blockchain pode afetar a AT?

2008 – Satoshi Nakamoto publica o artigo:

"Bitcoin: A Peer-To-Peer Electronic Cash System"

Esse artigo descrevia uma versão

de dinheiro eletrônico que permitiria que pagamentos online

fossem feitos diretamente de uma parte para outra

sem passar por uma instituição financeira.

Termo técnico: **DLT** ***(Distributed Ledger Technology)***

Um blockchain funciona como **base de dados descentralizada**, operada por computadores que pertencem a uma rede *peer-to-peer* (P2P), composta de nós clientes e servidores (mineradores/validadores).

Clientes são dispositivos que usam os serviços da rede;

Servidores são dispositivos encarregados de manter e verificar a integridade dos registros.

Transação

Dois indivíduos decidem trocar um ***Ativo Digital***

moeda digital,
escritura de imóvel,
certidão de nascimento,
grau educacional,
dados de seguro,
voto etc.

e iniciam a transação em uma rede P2P.

A transação é **criptografada** e

transmitida para cada nó da rede P2P.

O sistema ordena as transações recebidas - em um

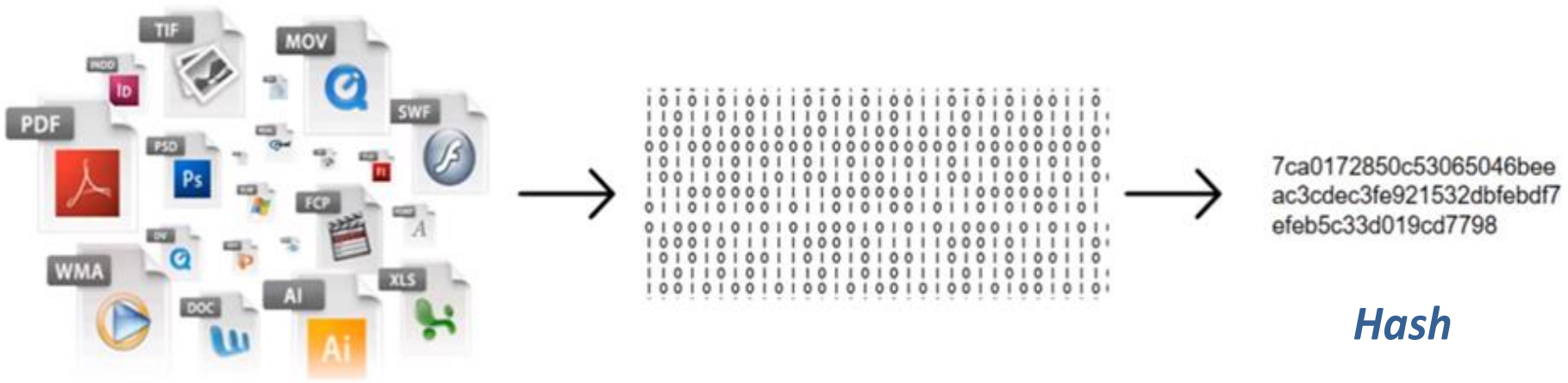
determinado momento - em grupos chamados **blocos**!

CHAVE PÚBLICA		
Endereço - DE	**Endereço - PARA**	**VALOR**
d6460d863cc7403c4d48eb8682d87784	549a46e93886df2928ed40724bde1705	2.357,20
7c93ed2e30dffdf4a67f5bde21da903d	c51ff2f6489025d6790f89b9db63855a	9.350,00
d12c96b54cda157b9e9b76b6d282cd3d	8dbe0cbef71fdd218f39623ea9ba374c	35,00
2fc02975227331db65e2daf78998780d	76dd7636fda92d792d2a064bc36a766c	392,50
99dcaf168dd3d7116e12663e2c572c90	bb4991985575019b7ec8b52b4e1876ec	634,00

Criação da CADEIA

Cada bloco é marcado com um ***hash***,

um resultado exclusivo!



Criação da CADEIA

Os diversos **blocos** são ligados entre si em ordem cronológica.

(formando uma cadeia)

VALOR	*transaction id*	BLOCO	HASH do BLOCO Anterior	HASH FINAL
135,20	16363fe...	34	5a458685fb42d09540bf16c696487d08	2bd77a9fc445d5263e2c7d074fae8885
4,00	2a303f...	34		
0,52	76ebb6...	34		
2.357,20	549a46...	35	2bd77a9fc445d5263e2c7d074fae8885	c836896ff5718674f9b5a5a9f940cc40
9.350,00	c51ff2...	35		
35,00	8dbe0c...	35		
392,50	76dd7...	35		
634,00	bb499...	35		

Se, a partir da cópia local em um computador, uma pessoa conseguir:

- quebrar a criptografia da assinatura digital **e**
- mudar os dados de uma transação qualquer, ou mesmo
- excluir uma transação do blockchain

Não conseguirá validar essa versão

frente a todas as demais cópias do blockchain.

Quanto mais cresce a blockchain,

maior se torna a **segurança** das transações mais antigas!

Princípios de Segurança

- **Integridade**
  garantia de que os dados não podem ser alterados intencionalmente ou por eventos fortuitos – criptografia

- **Disponibilidade**
  o serviço estará ativo quando solicitado, mesmo com pane em um nó servidor – rede distribuída

- **Confidencialidade**
  garantia de que a informação não será obtida por pessoas não autorizadas – chave pública *"criptografia do endereço"*

- **Autenticação, Autorização e Auditoria**
  somente usuários com as chaves privadas podem realizar transações, e todas as transações são públicas e auditáveis

- **Não repúdio**
  usuário não pode negar uma ação – assinatura com a chave privada

Tipos de Blockchain

Público (sem permissão)

Qualquer pessoa pode se juntar à rede e participar do processo de validação de blocos e de consenso.

Blockchain abertos

vantagem de escala

mineradores

prova de trabalho

Permissionário (com permissão)

Participantes do processo de validação e consenso são pré-selecionados.

Blockchain consorciados

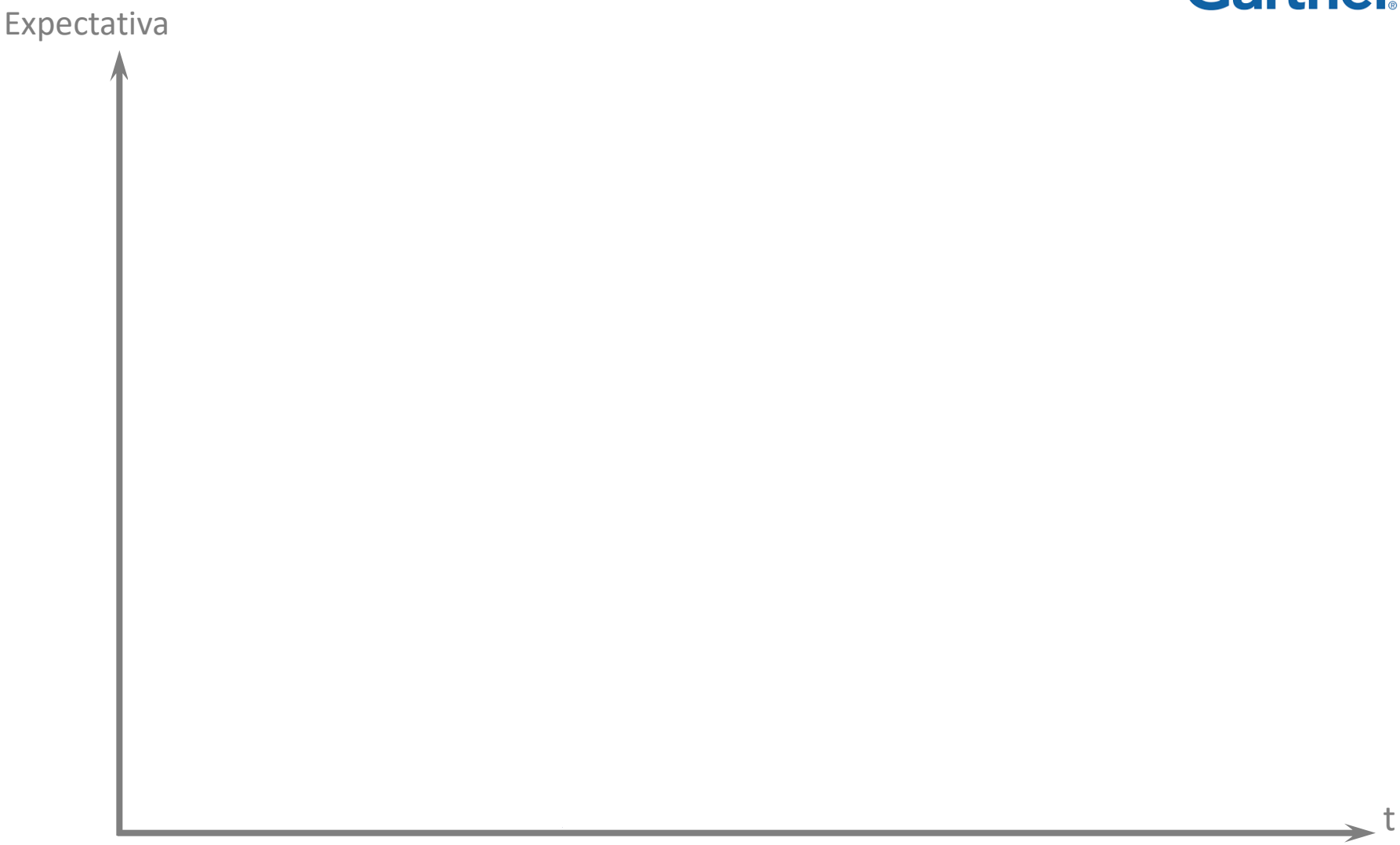
vantagem de desempenho

validadores

regras parametrizáveis

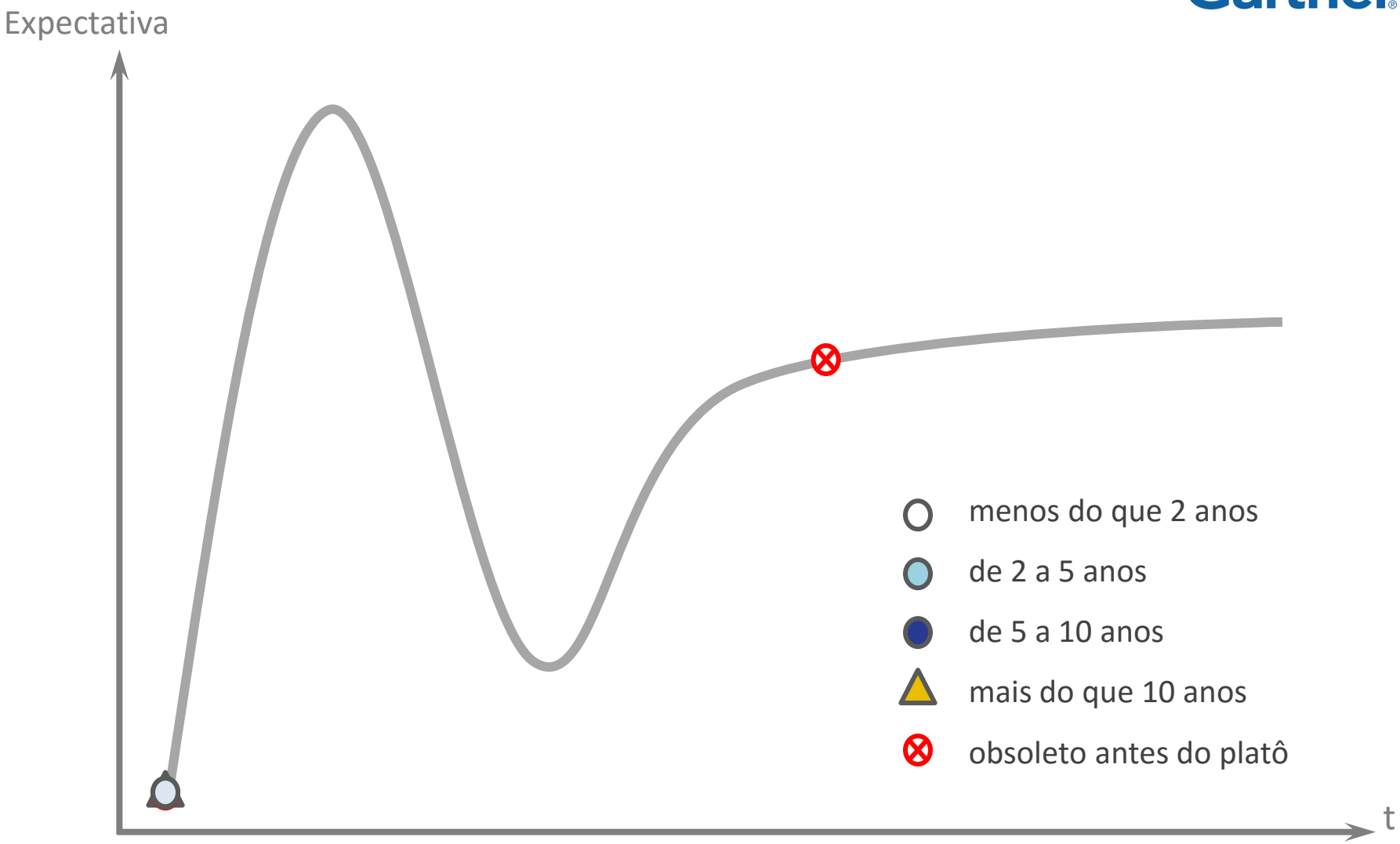
Hype Cycle

Gartner



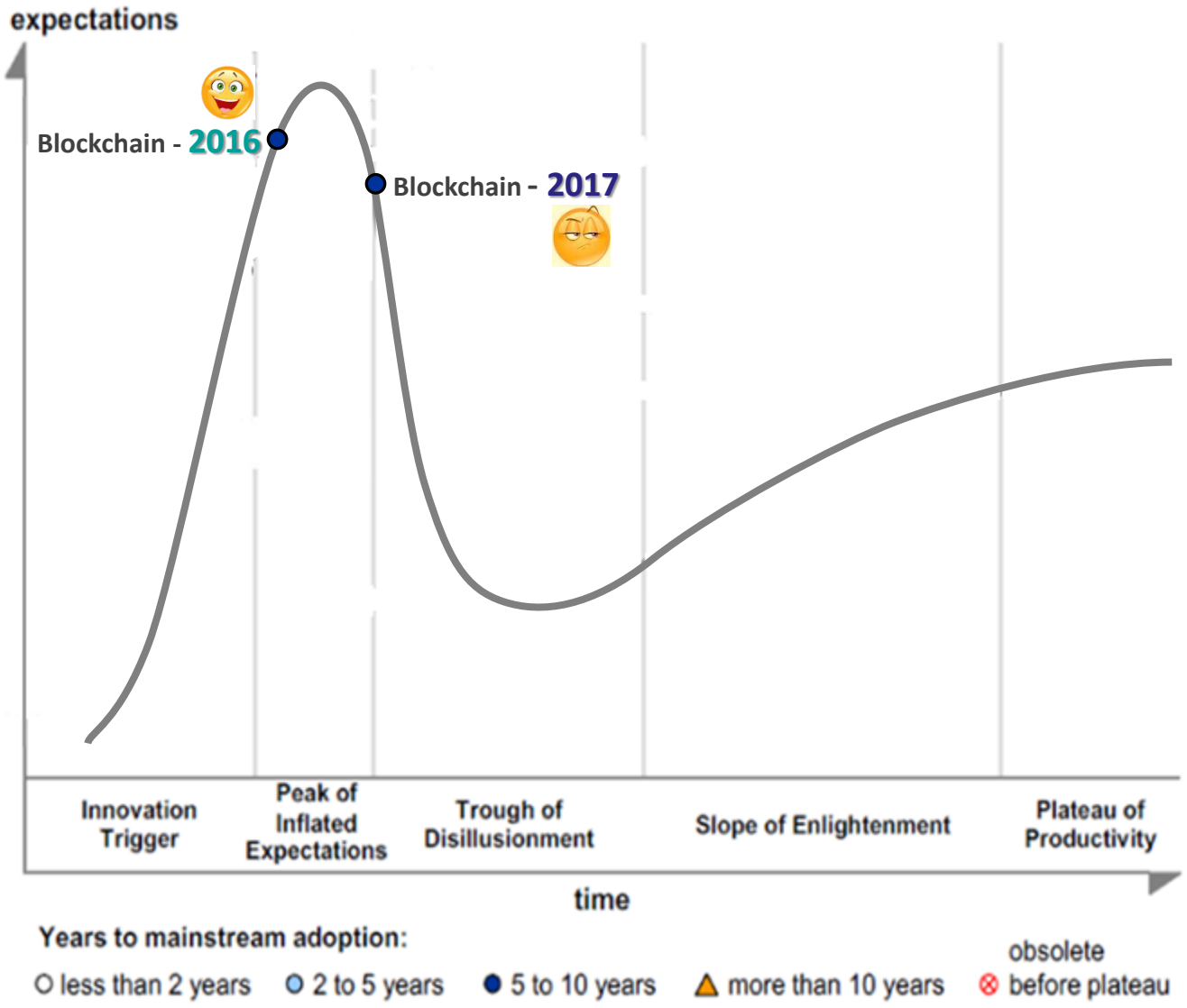
Hype Cycle

Gartner



Maturidade do Blockchain

Gartner



inovalab

Por que é relevante?

O que é Blockchain?

Como o Blockchain pode afetar a AT?

A criação de “livros-razão” distribuídos e imutáveis encontra aplicação em vários setores, sobretudo naqueles que dependem da **acumulação e do uso de dados** para executar suas funções.

As transações podem ser registradas de modo descentralizado, criando uma trilha de **rastreio e auditagem transparente** e praticamente impossível de falsificar.

Possíveis usos do blockchain na Administrações Tributárias

- Rastrear onde e quando foi recolhido o IVA;
- Ajudar as empresas a fornecerem um conjunto consistente de dados a autoridades tributárias múltiplas;
- Dar às autoridades tributárias e a outros órgãos reguladores maior confiança nos dados que recebem;
- Verificar, a partir dos registros na blockchain, as premissas envolvidas no cálculo do valor agregado na cadeia de negócios globais em diferentes jurisdições;
- Proporcionar maior visibilidade a micro-transações, como as realizadas por indivíduos.

https://www.pwc.co.uk/issues/futuretax/how-blockchain-technology-could-improve-tax-system.html

Benefícios

- Autoriza uma decisão *(eliminação do intermediário)*
- Estabelece um sistema de registro *(contabilização distribuída)*
- Acompanhamento de registro *(informação em tempo real)*
- Prova de autenticidade *(controle – usuários identificados)*
- Cria uma trilha de auditagem *(rastreabilidade)*
- Compartilhamento imparcial de dados *(conformidade)*
- Incrementa comunicação *(coordenação entre autoridades)*
- Registro imutável *(segurança)*

Ambiente Nacional, SEFAZ Virtual, SEFAZ Virtual de Contingência

Uso potencial

- Autoriza uma decisão *(Autorização de DF-e e eventos)*
- Estabelece um sistema de registro *(Ambiente Nacional)*
- Acompanhamento de registro *("Distribuição" imediata)*
- Prova de autenticidade *(CCC, CNE)*
- Cria uma trilha de auditagem *(Impede acessos indevidos)*
- Compartilhamento imparcial de dados *(Acesso 3º - mantido o sigilo fiscal)*
- Incrementa comunicação *(Art. 37, XXII, CF/88)*
- Registro imutável *(Confiança no modelo)*

Algumas **Incertezas Críticas**

- Quais as **vantagens e desvantagens** em relação a uma solução centralizada?
- Qual a contribuição potencial do blockchain **para eliminar a redundância de informação exigida por autoridades diversas**? *(simplificação tributária)*
- Uma rede blockchain permissionária (ao propiciar o anonimato) pode ser configurada de modo a **dificultar o acesso a informações pelo fisco**? *(facilitar a sonegação?)*
- Qual o **impacto econômico**, no curto e médio prazo, da evolução da tecnologia no mundo e no Brasil?
- Ao proporcionar novos modelos de negócios, a tecnologia pode **comprometer a coerência** entre o tributo tradicional e a atividade geradora de valor?

Essas e outras **incertezas** serão debatidas pela

Administração Tributária de São Paulo e especialistas em Blockchain

Painel – 25 de abril de 2018

organizado pelo InovaLab

realizado pela AFRESP.

Convidamos os colegas da AT

a participarem!

Auditório da AFRESP:

Av. Brigadeiro Luís Antônio, 4843

Jardim Paulista – São Paulo / SP

Obrigado

Marcelo Luiz Alves Fernandez

mlfernandez@fazenda.sp.gov.br