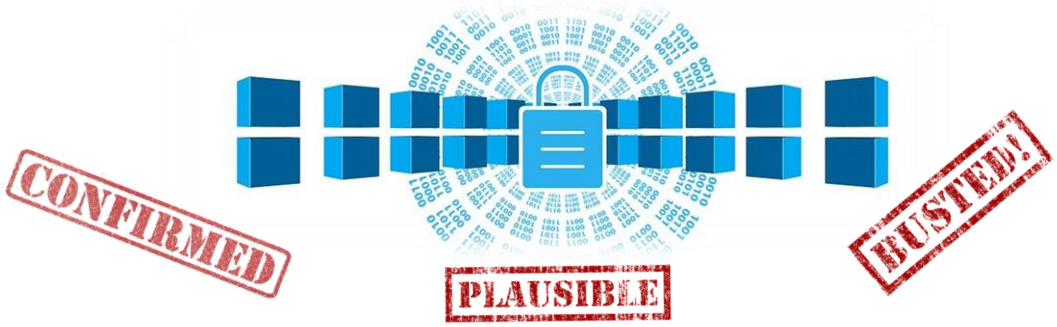


Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Algumas lendas (?) sobre blockchains

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Objetivos

- Discutir algumas **afirmações** relativas a blockchains que costumam soar "**enganosas**"
  - Ou não
- Trazer um **olhar crítico** sobre a **aplicabilidade** de blockchains
  - Antes de discutir cenários reais de aplicação
- Entender o que é o chamado "**hype cycle**", e onde blockchain se encontra
  - Ou, pelo menos, se encontrava quando este material foi produzido

Preâmbulo

"*Pra quem só sabe usar martelo, todo problema é um prego.*" Abraham Maslow, 1966

Blockchain

Problemas em sistemas distribuídos

A “imutabilidade”

- “Mas blockchain não armazena dados imutáveis?”
  - Não: o hash seguro permite **detectar** alterações nos dados; para “prevenção” de alteração, tenha uma cópia íntegra
  - Logo, embora um blockchain possa ser usado, é possível que usar apenas **hashes** seja suficiente (e mais eficiente...)
    - Nota: arquivos registrados via **BitTorrent** são igualmente “imutáveis”, embora não sejam registrados no tempo
  - Imutabilidade não é inerente a blockchains: pode-se **cancelar “imutabilidade”** via consenso (ou outra regra) se solução assim desejar!
    - Ex.: “nós aceitam apagar/modificar bloco se [condição], e naquele ponto hashes não batem” como parte das regras da solução com blockchain
      - Condição: usuário aceita manualmente; assinatura de um número mínimo de entidades; assinatura de uma autoridade; etc.
      - Obs.: basta um `if` no código (não requer coisas como “hash camaleão”)
      - Obs.: alguns nós podem não querer apagar... daí a “imutabilidade”...

A “irretratabilidade”

- “Mas blockchain não garante irretratabilidade de dados?”

  - Não: quem faz isso é uma **assinatura digital** (que pode, obviamente, ser associada a um blockchain)
    - A frase acima é análoga a dizer que “um computador serve para armazenar dados”: não é errado, mas basta um disco/pendrive pra isso, em vez de um computador completo...
  - Em particular, assinatura costuma ser suficiente quando é do **interesse do usuário** apresentar (em vez de omitir) dados gerados por uma entidade considerada confiável para gerá-los
    - Ex.: diplomas universitários e certificações diversas

A “veracidade”

- “Mas blockchain não garante veracidade dos dados colocados nele?”

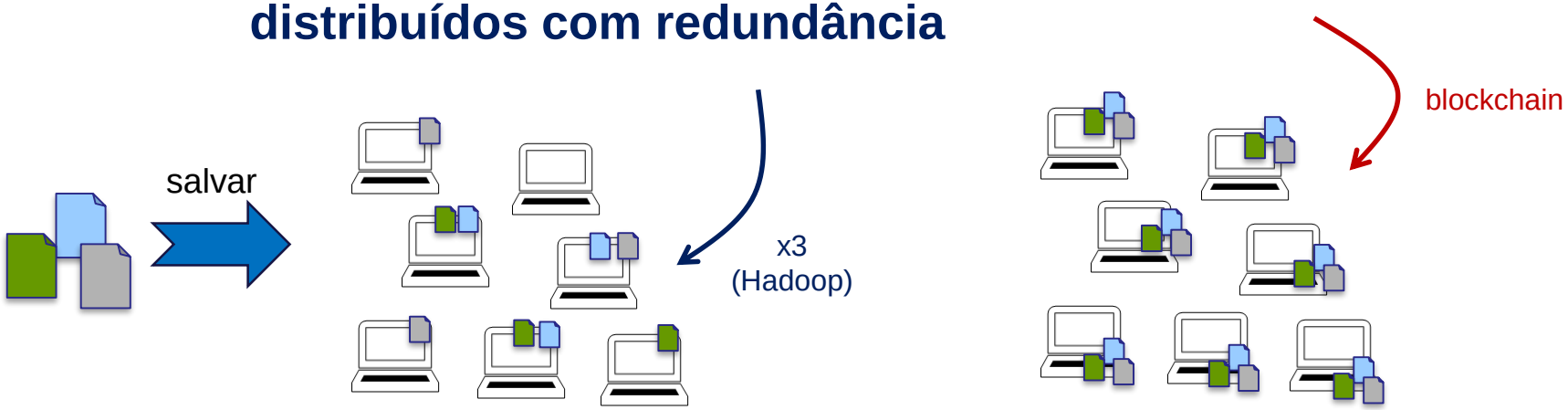
  - Não, blockchain não faz mágica... verificação fica a cargo da **camada de aplicação** sobre o blockchain
  - Blockchain ≠ “Máquina da verdade”

- “Ah, mas se vários nós entrarem em consenso, então significa que os dados são válidos, certo?!”

  - Consenso no Blockchain nada tem a ver com validade dos dados: o **consenso é sobre a <u>ordem</u>** dos eventos
    - E ordem consensual sequer precisa ser a ordem real...
  - De novo: blockchain não faz mágica... verificação fica a cargo da **camada de aplicação** sobre o blockchain
    - Ela deve definir o procedimento de verificação de validade!

“Depósito de dados”

- “Mas blockchain não é uma espécie de sistema de arquivos distribuído, como na nuvem?”
  - Não: no blockchain, os dados são **100% replicados**, não **distribuídos com redundância**



  - Se objetivo é armazenar dados de forma distribuída, você está procurando outras tecnologias, não voltadas a ordenação em si
    - **P2P**: Distributed Hash Table (DHT – ex: Kademlia), BitTorrent, Freenet, InterPlanetary File System (IPFS)
    - Com controlador centralizado (“Big Data”): **Hadoop**

“O” Blockchain

- “Mas não existe ‘o Blockchain’, assim como existe ‘a Internet’?”
  - Não: a Internet é uma estrutura aberta que interconecta várias redes de provedores
  - Cada solução baseada em Blockchain pode:
    - **Construir seu próprio blockchain**, desde seu “bloco gênesis”, de forma totalmente independente de outros blockchains
    - **Usar um blockchain existente**, que tenha as funcionalidades desejadas e regras que possam acomodar a solução alvo, lá armazenando seus dados
    - Criar um blockchains independente de blockchains existentes mas capaz de interoperar com eles (**criar uma “federação”**)
  - **Vários blockchains** atuais suportam essas possibilidades
    - Hyperledger Fabric, Ethereum, XRP Sidechains, Algorand Co-chains, Multichain, ...

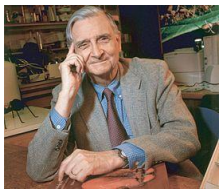
A “abertura” e o “anonimato”

- “Mas blockchains não são acessíveis por qualquer pessoa, de forma anônima?”
  - Não necessariamente: abertura e anonimato não são inerentes a Blockchains
  - Diferentes graus de centralização ao se controlar quem (um nó vs. alguns nós vs. qualquer nó) pode:
    - Validar transações e atualizar blockchain (mineradores)
    - Enviar transações para a rede
    - Visualizar o conteúdo do blockchain
  - Pode-se exigir identificação: certificados emitidos por CA (interna ou externa)

- Algumas ferramentas p/ anonimato (tema de aulas específicas): **pseudônimos, assinaturas cegas, MixNets, Tor, zk-SNARKs, ...**

A leveza do ser

- “Mas blockchain não é uma solução leve e eficiente?”
  - Não necessariamente: vários protocolos de consenso distribuído são computacionalmente **ineficientes**...
    - Ex.: https://cbeci.org (consumo de energia do Bitcoin)
  - E replicação 100% é inerentemente custosa: banda & memória
  - **Nota**: ainda assim, é comumente mais eficiente que sistemas físicos que busca substituir
    - Ex.: **cartórios** são altamente ineficientes e custosos
    - Ex.: **transferência internacional entre bancos** é algo ineficiente, custoso, e sujeito a falhas



“O real problema da humanidade é o seguinte: temos emoções da era Paleolítica, instituições medievais, e tecnologia digna de deuses”

Edward O. Wilson

O peso do ser

- “Ah, mas então todo blockchain é ineficiente, lento, consome muita energia, ...?”
  - Não necessariamente: certas **simplificações** podem permitir consenso eficiente

    - Ex.: se todos os nós se conhecem, pode-se usar consenso bizantino; custo maior é de banda, não de processamento
    - Ex.: se todos os nós se conhecem e têm elevada disponibilidade, pode-se usar mecanismo de sorteio justo (vide aula específica)
    - Ex.: se há alguma “confiança” nos nós (e.g., são entidades puníveis no mundo real), pode-se usar protocolos de revezamento ou votação
  - **Nota**: redes federadas, nas quais os usuários e nós são **identificados** costumam facilitar consenso leve
    - Se usuário fizer gasto duplo: remova duplicação da rede antes de consenso
    - Se nó da federação enviar blocos distintos para a rede: remova nó da federação, e reinicie consenso

Proof-of-leveza

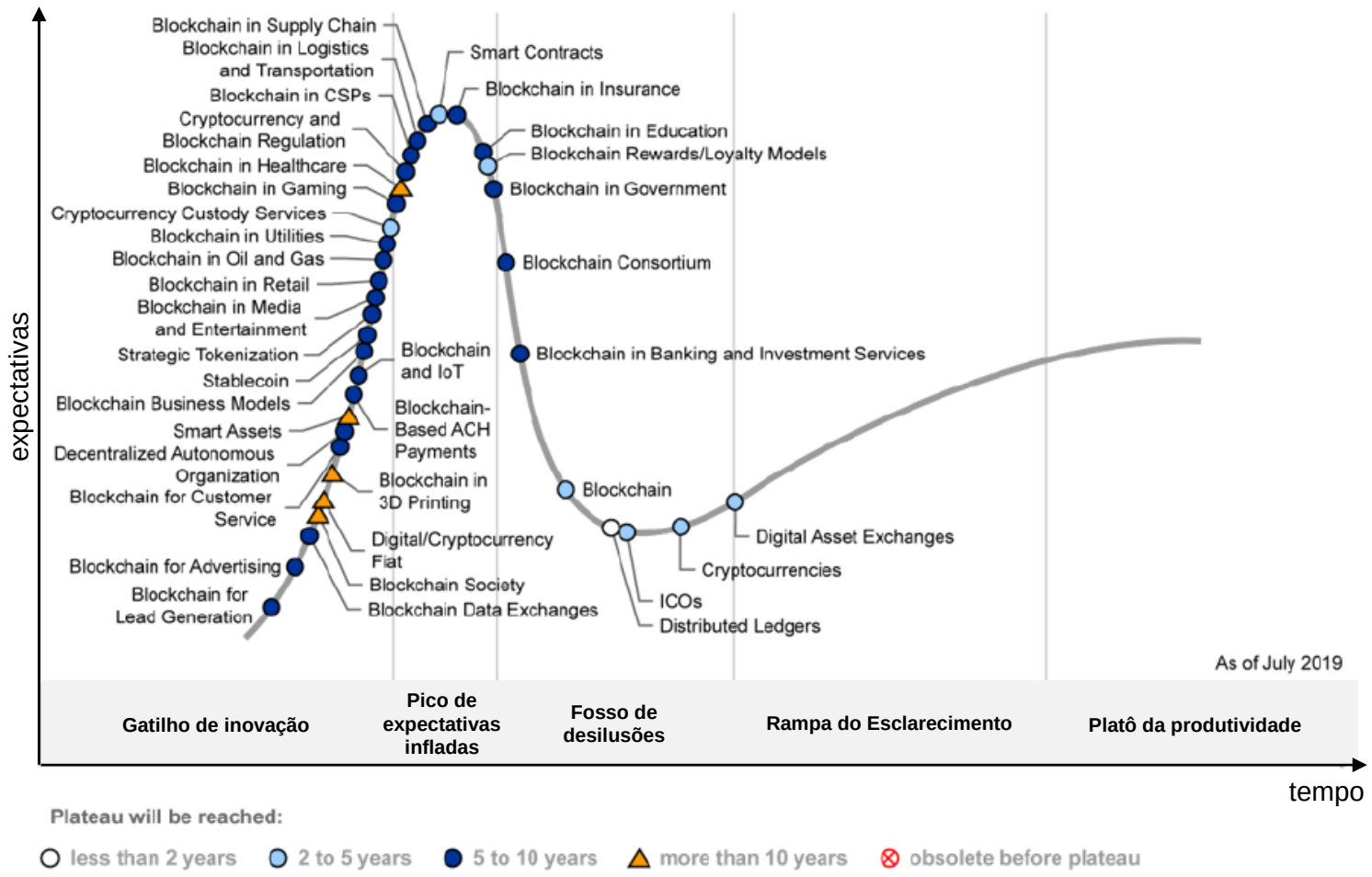
- “Mas não dá pra fazer um Proof-of-Algo mais rápido para criar um consenso eficiente?”
  - Fazer um Proof-of-* rápido em um **cenário genérico** é uma armadilha, pois isso **dificulta o consenso**

    - O resultado é a **geração de muitos forks**: diversas visões da realidade criadas rapidamente, demorando a convergir...
    - **Analogia**: (1) projetam uma bola de demolição;
      (2) percebem que é um problema ela ser muito pesada;
      (3) alguém tem a “genial” ideia de fazer uma bola mais leve;
      (4) a bola leve... não demole...
  - Novamente: consenso eficiente pode ser obtido em cenários federados e/ou quando punição por mau-comportamento pode ser feita off-chain

“Ataque o interlocutor”

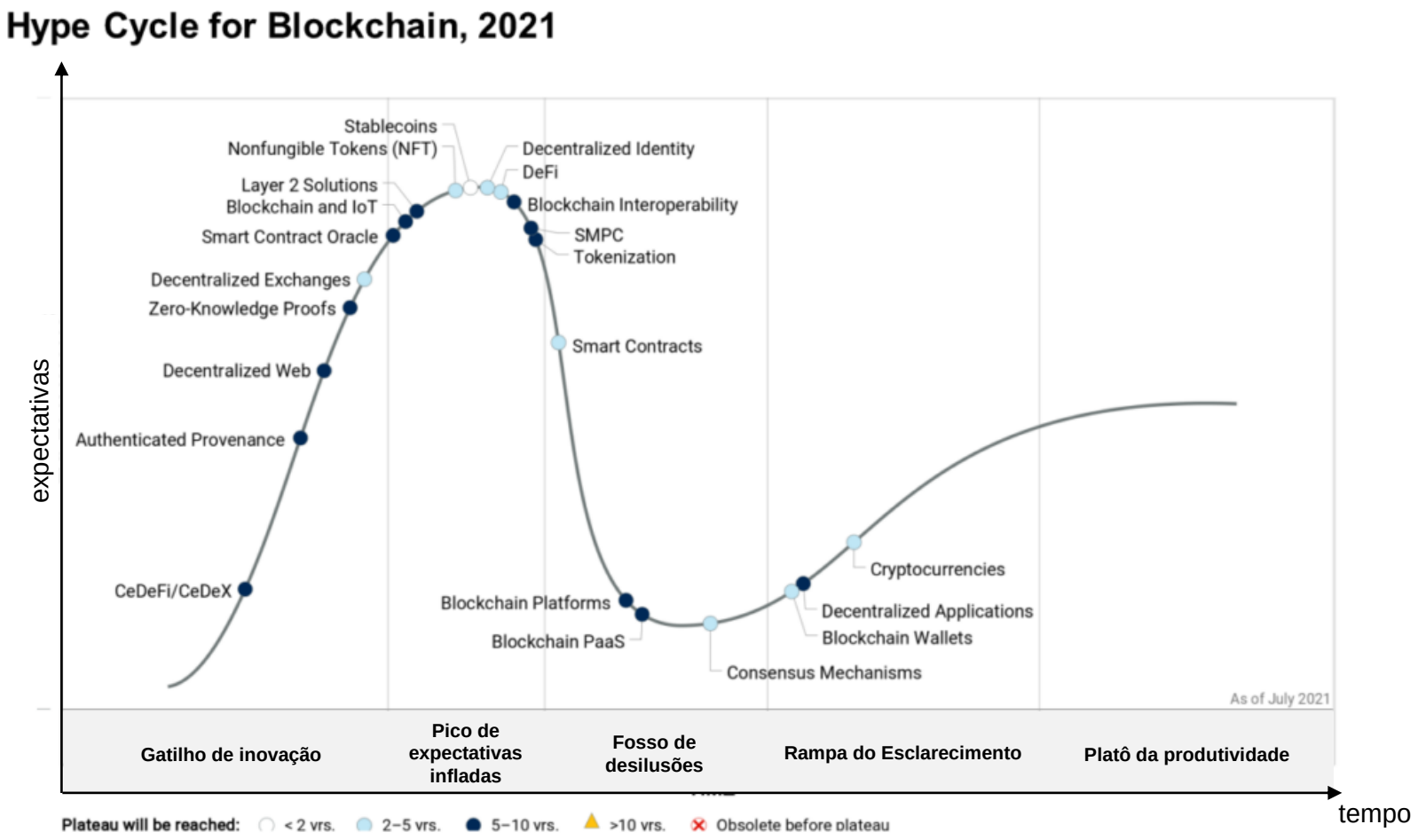
- “Isso não é um olhar um tanto pessimista/limitado?”
- Não exatamente: é somente um **olhar crítico**!
  - Existem sim aplicações nas quais **blockchain é muito útil**...
  - ... assim como existem diversos “vendedores de blockchain” que vendem ilusões
- Toda tecnologia tem um período de “**hype**”
  - Nem tudo é resolvido movendo seus dados/aplicações para uma **nuvem pública** (e.g., **segurança de aplicações**)
  - Nem tudo se resume a **big data** sobre dados **não estruturados** (e.g., sistemas transacionais se beneficiam muito de **dados estruturados** em bancos relacionais)
- **Evite armadilhas: tenha um olhar crítico!**

O conceito de “Hype Cycle”



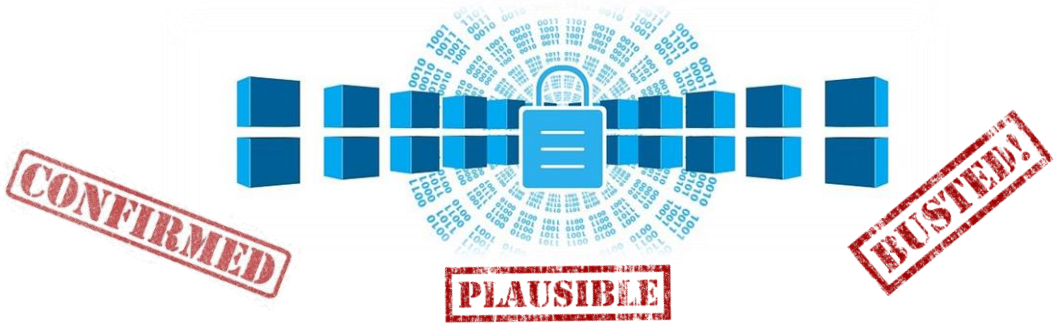
Source: Gartner (Setembro 2019)
ID: 390391

O conceito de “Hype Cycle”



Source: Gartner (Julho 2021)

747513



Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Algumas lendas (?) sobre blockchains

Prof. Dr. Marcos A. Simplicio Jr. – mjunior@larc.usp.br
Escola Politécnica, Universidade de São Paulo

Apoio financeiro: d24n.org <https://d24n.org>
ripple impact | university blockchain research initiative

Referências

- Melhor referência é a diversidade de opiniões: https://www.google.com/search?q=myths+blockchain

- S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". Whitepaper, 2008. URL: https://bitcoin.org/bitcoin.pdf. Veja também (tradução paara português): https://cointimes.com.br/whitepaper-do-bitcoin-traduzido/
- A. Narayanan, J. Bonneau, E. Felten. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction". Princeton University Press, 2016. ISBN: 0691171696. Available: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1
- L. Lantz and D. Cawrey. "Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications". O'Reilly Media, 2020. ISBN: 1492054704
- Stallings, W.; Brown, L. “Computer Security: Principles and Practice” (3rd/4th Ed.), Pearson (2014/2017). ISBN: 9780134794105

Hype cycle: fases