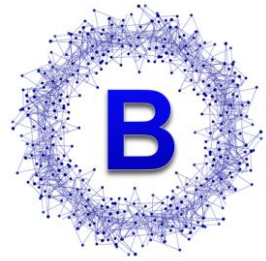


Blockchain

Sem o Hype!

(ou: pra que serve um Blockchain?)

Prof. Dr. Marcos A. Simplicio Jr.
Escola Politécnica, USP

Time Stamp Authority (TSA)

- Entidade que gera "carimbo de tempo"
  - Certifica horário em que evento é registrado no sistema
- Útil em qualquer sistema em que a ordem de eventos precisa ser determinada
  - Exemplo: cenário de comunicação instantânea

A: Vem pra casa hoje?	A: Vem pra casa hoje?
B: Umas 19	B: Lógico que não
A: Andou flertando com alguém no trabalho? 🔪	A: Andou flertando com alguém no trabalho? 🔪
B: Lógico que não	B: Umas 19
A: ❤️	A: 😡

VS

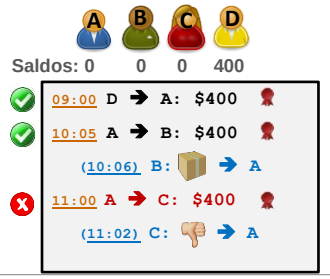
Blockchain: uma TSA distribuída

- **Cenário**: transações monetárias na web
- **Problema**: como saber se usuário tem saldo suficiente no momento da compra?
  - Solução 1: confiança em banco... e taxas...

Blockchain: uma TSA distribuída

- **Cenário**: transações monetárias na web
- **Problema**: como saber se usuário tem saldo suficiente no momento da compra?
  - Solução 2: sabendo o saldo inicial e todas as transações realizadas ➔ ao verificar o instante das transações...

    ... podemos fazer a conta nós mesmos!

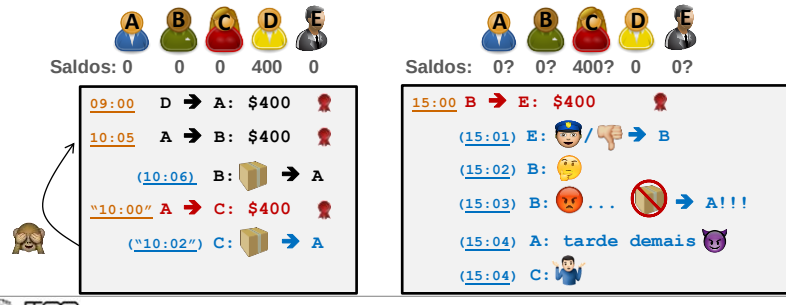


← **Assinatura digitais** garantem autenticidade, integridade e irretratabilidade das transações
Ex.: D assina "D ➔ A : 400"

*(confiança é **distribuída**)*

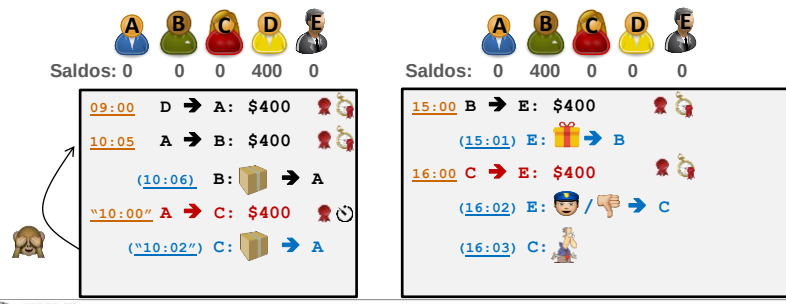
Blockchain: uma TSA distribuída

- **Cenário**: transações monetárias na web
- **Problema**: como saber se usuário tem saldo suficiente no momento da compra? ➔ analisar transações...
  - ... mas sem relógio confiável, instantes de tempo podem ser falsificados por usuários desonestos!



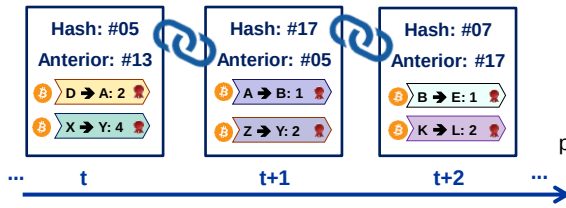
Blockchain: uma TSA distribuída

- **Cenário**: transações monetárias na web
- **Problema**: como saber se usuário tem saldo suficiente no momento da compra? ➔ analisar transações **& tempo**
  - Solução 1: **Autoridade de Carimbo de Tempo** (TSA) assina os instantes de tempo (confiança e taxas...)



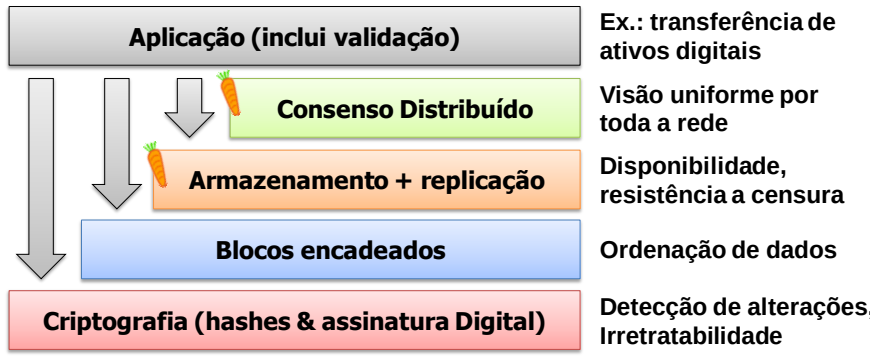
Blockchain: uma TSA distribuída

- **Cenário**: transações monetárias na web
- **Problema**: como saber se usuário tem saldo suficiente no momento da compra? ➔ analisar transações **& tempo**
  - Solução 2: **Blockchain**, que funciona como "TSA P2P" -- nós "concordam com a ordem" (consenso)
    - Obs.: **validação** dos dados é tarefa da camada de **aplicação** (**consenso é sobre a ordem** desses dados já validados)



Blocos válidos (ex.: assinatura correta e saldo positivo) colocados em ordem

Blockchain: módulos



- 🥕 : operação do módulo costuma exigir incentivos
- **Importante**: algumas aplicações precisam apenas de alguns desses módulos!

Blockchain: módulos essenciais (?)

Ex.: transferência de ativos digitais

Visão uniforme por toda a rede

Disponibilidade, resistência a censura

Ordenação de dados

Detecção de alterações, Irretratabilidade

Blockchain: *"A structure for storing data in which groups of valid transactions, called blocks, form a chronological chain, with each block cryptographically linked to the previous one."* **MIT Technology Review**
https://www.technologyreview.com/s/610885/a-glossary-of-blockchain-jargon/

➔ Potencial uso de Blockchain como "**append-only log**" (mais adiante)

Blockchain: quando usar?

- Blockchain **completo** necessário se problema tem as seguintes características:
  - Requisitos funcionais incluem **ordenação de eventos**
    - Mas não requer **instantes reais de tempo**
  - **Altamente distribuído**: **sem confiança** entre as partes
    - Se houver **entidade confiável** (ex.: TSA): provavelmente mais eficiente tirar proveito dessa confiança
  - **Preferencialmente** : há **incentivos claros** para a participação dos usuários no sistema
    - Sem isso: consenso e replicação dependem de altruísmo ("pelo bem do sistema")

Blockchain: aplicações potenciais

- **Transferência de ativos (virtuais)**: **killer app**
  - **Ordenação de eventos**: necessário para saber quem é o dono atual do ativo
    - Não são necessários **instantes reais de tempo**: em geral, não importa se o ativo foi recebido há anos ou há segundos, mas apenas quem é o dono atual
  - Sistema **totalmente distribuído**: sem intermediários
    - Eliminar **entidade confiável** permite aumentar resistência a falhas e disponibilidade, além de potencialmente evitar taxas
  - **Sem confiança**: usuários podem tentar cometer fraudes
    - Consenso previne que a "visão de mundo" fraudulenta prevaleça: apenas uma instância do ativo no sistema
  - Ex. comum: moedas (**Bitcoin**, **criptomoedas**, **Ripple, ...**)
    - **Incentivo:** moedas e "pelo bem da economia"

Blockchain: aplicações potenciais

- Variantes de **transferência de ativos (virtuais)**:

  - **Contratos** diversos: posse, promessa de dívida, ...
    - Substituição de **cartório físico**, que tem estrutura (semi-)centralizada
    - **Importante**: eventos no blockchain não confrontáveis com eventos registrados fora do blockchain (e.g., em cartórios físicos) ➔ ordenação exigiria **instantes reais de tempo**
    - Inclui **smart contracts**: em suma, "contrato = programa executável"

  - Em jogos: **contas**, **itens colecionáveis**, **ouro/gemas**, ...
    - Ex.: figurinhas, cartas em jogos de colecionáveis
    - Tradicionalmente implementado com arquiteturas centralizadas controladas pelo gerador dos itens (**entidade confiável**)
    - Mas pode haver **redução de custos** com arquitetura distribuída
- **Desafio**: como convencer usuários a investir recursos computacionais no processo de consenso ("**incentivo**")?

Blockchain: aplicações potenciais

- Cuidados com **transferência de ativos reais**:

  - É necessário "**tokenizar**" ativos: como garantir que a representação digital de ativo de fato corresponde a um ativo real?
    - Conceito também conhecido como "**digital twins**"
  - Alguns casos **mais fáceis**: veículos (chassis, renavam); casas (número de matrícula); pessoas (CPF+foto+digitais); obras de arte (únicas, com atestado de autenticidade feito por perito)

    - Nota: sistema cartorial atual garante **posse inicial**
  - Alguns **mais difíceis (?)**: produtos agropecuários; produtos químicos; objetos sem identificador único
    - Nota: como impedir **geração, duplicação** ou **substituição** de ativos?
  - **Ações** sobre ativos reais não dispensam **entidade confiável**

    - Entidade registra no Blockchain assinatura digital sobre a ação: manutenção de equipamento, vacinação de rebanho, ...

Blockchain "básico"

- Há cenários em que replicação total e consenso não são críticos: blockchain como **estrutura de dados**

  - Uma única entidade "semi-confiável" gerencia **entrada de blocos** e **publica atualizações** periódicas
  - **Monitores** armazenam "cauda" do Blockchain

    - Opcionalmente, também podem armazenar conteúdo completo, ou apenas partes de interesse
  - **Tentativas de alteração** de dados pretéritos é facilmente detectada por monitores: **auditabilidade**

    - Recuperação em caso de armazenamento dos dados

- Permite criar **logs transparentes e verificáveis**

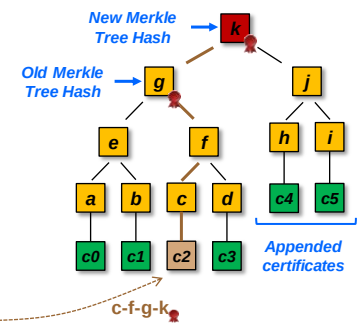
  - Mesmo se entradas não são verificáveis (e.g., ativo real)
  - Princípio por trás de DLTs (*Distributed Ledger Technology*)

Blockchain "básico": Certificate Transparency

- Certificados na web: **Infraestrutura de Chaves Públicas (ICP)**
  - Segurança do sistema depende da segurança de Autoridades Certificadores (ACs): "In ACs we **trust**!"
- Mas... E se uma **CA for comprometida**...?
  - Ou simplesmente não seguem a **diligência devida**...?
- Isso nunca deveria acontecer... mas acontece...
  - DigiNotar (2011): comprometida por hackers
  - Symantec (2015): certificados inválidos p/ Google e Opera
  - Outros: https://www.certificate-transparency.org/what-is-ct

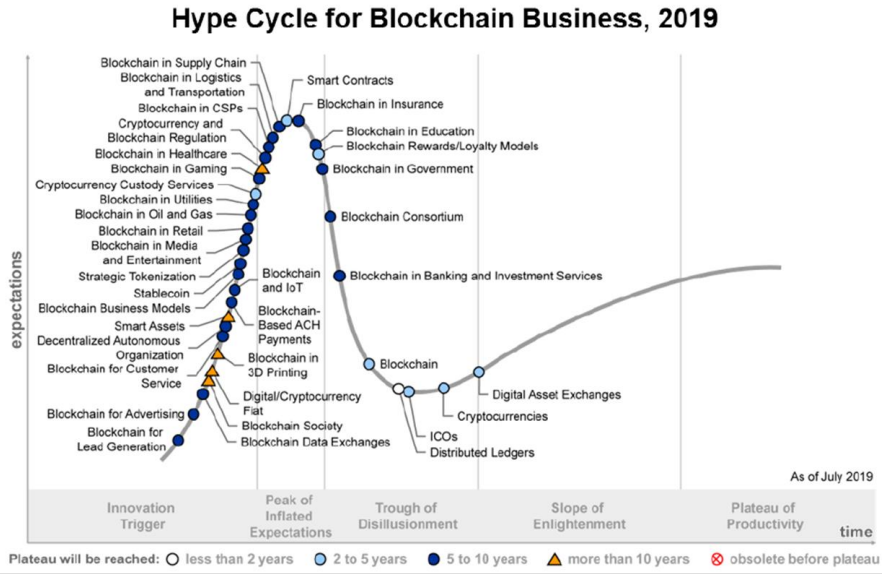
Blockchain "básico": Certificate Transparency

- **Logs públicos** de certificados, com política de "**append-only**"
  - Árvore de Merkle, mas poderia ser um blockchain "linear"
  - **Verificável**, mesmo se não confiável
- **Navegador** só aceita certs logados
  - Força CAs a publicar suas ações
  - Verificação: nós no **caminho até raiz**



- **Monitores** verificam conteúdo, e **mantêm raiz** da árvore
  - Detectam certificados com **extensões estranhas**, ou **tentativa de deleção** por servidor que mantém log público
- **Donos de domínios** têm **visibilidade** dos certificados
  - Podem pedir **revogação** em caso de emissão inválida

Blockchain: aplicações potenciais



Fonte: Gartner, Setembro 2019 (ID 390391)

18

Brigado!!!

- Prof. Dr. Marcos A. Simplicio Jr.
- Escola Politécnica, USP
- E-mail: mjunior@larc.usp.br
- http://lattes.cnpq.br/6874544707185541