Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Algumas aplicações “questionáveis”

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

Objetivos

- Continuar **olhar crítico** sobre a aplicações de blockchains: cenários de uso duvidosos
  - Usam blockchain como **“máquina da verdade”**
  - Utilidade de uma **ACT** não é clara
  - Parecem mais ligados a **logs transparentes**
- Propostas reais, derivadas de reais, ou sugeridas em conversas informais, mas:
  - Soluções similares às aqui apresentadas podem fazer perfeito sentido!!!
  - Objetivo é incentivar olhar crítico e **“fazer as perguntas certas”**, não fazer crítica vazia!!!

Blockchain: aplicações revolucionárias (será?)

- Coleta de assinaturas para projetos de lei de iniciativa popular
  - **Requisito**: assinaturas de (I) ao menos 1% do eleitorado nacional; (II) 0,3% dos eleitores de ao menos 5 estados
    - Não podem ser incluídos assuntos diversos ao projeto original (“jabutis”): caso das “10 medidas de combate à corrupção”
  - **Problema**: Câmara alega não ter condições de conferir a veracidade das assinaturas
    - Comum: parlamentar “adota” proposta... e em propostas de parlamentares não há restrição a jabutis...
  - **Solução**: Blockchain ??
  - Não tem “**ordem de eventos**” aqui ➔ **Solução real**: bastam as **assinaturas digitais** com verificabilidade (e.g., via ICP)

Blockchain: aplicações revolucionárias (será?)

- Provar que tomou vacina [para COVID-19]

  - **Problema**: site do Ministério Saúde saiu do ar, dificultando acesso ao comprovante de vacina
  - **Solução**: Blockchain??
  - Não tem "**ordem de eventos**" nesse cenário ➔ **Solução real**: bastam as **assinaturas digitais** correspondentes
    - Armazenados por usuários, sem depender de sites p/ verificação
  - ~~Nem **log transparente** soa útil~~: utilidade seria contra temor de **entidades confiáveis** de saúde reescreverem passado
    - Ex.: "forjar comprovante antigo cria impressão de imunização"
      - Mas nada impede comprovante falso emitido no presente...
    - Ex.: "podem eliminar comprovante antigo da base de dados"
      - Mas posse de assinatura digital elimina risco...

Vide próximo slide

- **Log transparente** é sim útil em um cenário real (ainda que surreal):
  - Sistema usado para apagar registros antigos
  - **E** não é do interesse do usuário apresentar prova de que o registro existia
    - Quando há tal interesse, assinatura digital costuma bastar: irretratabilidade
- Blockchain soa a exagero:
  - Replicação completa vs. algum grau de replicação para disponibilidade
    - Difícil apagar todas as cópias
  - Consenso distribuído vs. ordem definida por servidor central
    - Nível federal, ou por estado

terra

Capa › Notícias › Brasil › Política

Política

Vacina falsa de Bolsonaro: Secretário admite ter usado senha de enfermeira para excluir dados do SUS

João Carlos de Sousa Brecha incluiu informações de ex-presidente no sistema do Ministério de Saúde, segundo a PF

Redação Terra

23 jun 2023 - 09h29 (atualizado às 11h30) Compartilhar Ver comentários

À PF, Bolsonaro voltou a dizer que não se vacinou e negou participação em qualquer iniciativa para adulterar o próprio cartão de vacinação e o da filha

Foto: Reprodução

Blockchain: aplicações revolucionárias (será?)

- Votação eletrônica: registro de votos em Blockchain
  - **Problema**: como saber se meu voto foi contabilizado? Fraude no software ou na totalização pode desviar meu voto!
  - **Solução**: Blockchain??

    - Normalmente não há "**ordem de eventos**" nesse cenário...
    - Pelo contrário: ordenar votos pode levar a **insegurança** se a ordem dos eleitores for conhecida (vide TPS 2012*)!
  - **Solução real, supondo software honesto**: assinaturas digitais e divulgação de resultados pela urna
    - Ex. (Brasil): urna assina boletim de urna (BU) na seção eleitoral, prevenindo falsificação/omissão posterior na totalização
    - Nota: várias cidades pequenas fazem totalização paralela usando BUs assinados… não precisam de blockchain pra isso…

*D. Aranha et al. (2014). (In)segurança do voto eletrônico no Brasil. In: Cadernos Adenauer 1/2014: Justiça Eleitoral, 117-133, 2014. URL: https://sites.google.com/site/dfaranha/pubs/aranha-karam-miranda-scarel-12-pt

Blockchain: aplicações revolucionárias
(será?)

- Votação eletrônica: registro de votos em Blockchain
  - **Problema**: como saber se meu voto foi contabilizado? Fraude no software ou na totalização pode desviar meu voto!
  - **Solução**: Blockchain??
    - Normalmente não há "**ordem de eventos**" nesse cenário...

  - **Solução real, sem assumir software honesto:**
    - **Impressão de voto** para conferência posterior: requer custódia adequada de votos em papel, para evitar fraudes ali
      - Ex.: proteção física, assinaturas digitais, ...
    - **Auditabilidade fim-a-fim** (end-to-end – E2E): comprovante de voto entregue a usuário, que pode conferir sua inclusão na totalização
      - Votos assinados e cifrados para preservar sigilo do voto.
      - Ex.: Helios, ElectionGuard, Wombat, VoteXX, …

Blockchain: aplicações revolucionárias (será?)

- Votação eletrônica: registro de votos em Blockchain
  - **Problema**: como saber se meu voto foi contabilizado? Fraude no software ou na totalização pode desviar meu voto!
  - **Solução**: Blockchain??
    - Normalmente não há "**ordem de eventos**" nesse cenário...

  - Há interesse em **logs transparentes** para dados públicos.
    - Ex.: hashes de software, chaves públicas das urnas usadas, lista de boletins de urnas recebidos, ...
    - Permite detecção de tentativas de alterações pós-pleito (ex.: "urna usada na votação substituída por urna na casa de fraudador")
  - Leitura sugerida: S. Park, M. Specter, N. Narula, R. Rivest. "Going from bad to worse: from Internet voting to blockchain voting". Journal of Cybersecurity, Volume 7, Issue 1, 2021. URL: https://doi.org/10.1093/cybsec/tyaa025

Blockchain: aplicações revolucionárias
(será?)

- Verificação de dados reais quaisquer
  - **Problema**: como saber se um usuário tem a experiência alegada em certa atividade? Ou qual é a qualidade de produtos ou serviços ofertados por uma empresa?
  - **Solução**: registrar os dados em um blockchain, para validação pelos vários nós participando do consenso??
  - Não tem "**ordem de eventos**" nesse cenário…
    - Blockchain não é uma **"máquina da verdade"**: validação de dados é papel da **aplicação** construída sobre blockchain!
    - Se é **difícil validar** sem blockchain, assim será com blockchain!
  - **Solução real**: difícil… o mais próximo são sistemas de reputação, mas nunca é 100% garantido…
    - Ex. (centralizado): ReclameAqui, Google, Ebit
    - Ex. (distribuído): assinaturas digitais por pares/terceiros

Blockchain: aplicações revolucionárias (será?)

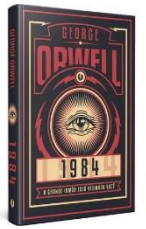
- Plataforma padronizada para compartilhamento de documentos diversos

  - **Problema**: diversas empresas com formatos internos distintos, dificultando soluções integradas
  - **Solução**: usar Blockchain??
  - Não tem "**ordem de eventos**" nesse cenário ➔ **Solução real**: padronizar formatos
    - Pode ser "o formato usado no Blockchain" se desejado: mas seria "Blockchain como sopa de pedra", ou seja, apenas como subterfúgio para levar à adoção do mesmo padrão…
  - Diversas linguagens criadas com o objetivo de promover padronização: RDF, JSON, XML, Gellish …
    - Nota: várias opções de padrão costuma dificultar padronização… https://xkcd.com/927/

Blockchain: aplicações revolucionárias (será?)

- **“Plataforma de transparência global”**
  - **Objetivo**: eliminar **informações privilegiadas** controladas por grupos específicos, que delas tiram proveito
  - **Solução**: Blockchain??
  - Só dá para obrigar registro de dados no Blockchain quando esse registro é necessário para a operação do Sistema
    - Ex. (troca de ativos): a passagem do ativo digital p/ novo dono

  - Qualquer informação privilegiada adicional pode ser omitida ou falsificada
    - Ex. (troca de ativos): a razão pela qual o ativo digital foi vendido, ou qual ativo real foi trocado por ele
  - A “solução” p/ eliminar problemas causados por entidades com informação privilegiada é essencialmente uma:



Blockchain: aplicações revolucionárias (será?)

- Auditoria de Redes Definidas por Software
  - SDN: *Software Defined Network,* tecnologia que permite maior **programabilidade de equipamentos de rede**, como switches e roteadores
  - **Problema**: manter log das ações de um controlador SDN, para posterior auditoria dessas ações:
  - **Solução**: Blockchain??
  - Controlador é **entidade confiável** central em redes SDN: pode realizar ações e não registrar no blockchain ➔ **Solução real**: switches armazenam requisições assinadas pelo controlador (?)
    - Obs.: não previne **ações indevidas pelos switches**, ou **apagamento de logs** locais, mas ao menos permite verificar comandos do controlador em switch íntegro

Blockchain: aplicações revolucionárias (será?)

- Validação de componentes fornecendo um serviço (ex.: contêineres em ambiente em nuvem)

  - **Problema**: como garantir que um contêiner no sistema não está comprometido (e.g., executando em um cluster incorreto, sob controle do atacante) – computação confiável
  - **Solução**: Blockchain ??
    - Contêineres podem entrar em consenso sobre validade de seus pares antes de dar continuidade à comunicação, não?
  - Não tem "**ordem de eventos**" aqui, e consenso em blockchain é sobre ordem de eventos ➔ **Solução real**: plataformas de identificação, verificação e validação de serviços, como Secure Production Identity Framework For Everyone (SPIFFE)
    - Agentes fazem medições de parâmetros do contêiner (e.g., localização, dono, etc) e emite credenciais após validação

spiffe

Blockchain: aplicações revolucionárias (será?)

- Identidade centrada no usuário

  - **Problema**: cada usuário precisa gerenciar muitas identidades e atributos, registrados em diferentes locais
    - Usuário controla: onde dados são armazenados, quem acessa o que, e como sua identidade é apresentada (e.g., nome social)
    - Sistema deve fornecer provas de autenticidade
  - **Objetivo**: centrar no usuário o controle sobre seus documentos e atributos, podendo fornecer a quem desejar, quando desejar

  - **Solução**: usar Blockchain??
  - Não tem exatamente "**ordem de eventos**" nesse cenário ➔ **Solução mais próxima de real**: *Identity Management* (IdM)
    - Várias soluções (des)centralizadas, com formatos padronizados: **OpenID**, **OAuth**, **Web of Trust (uso no PGP), Self-certifying File System (SFS)**
      - Identidade baseada em e-mail e/ou em certificados digitais
    - **Mas nenhuma delas (nem blockchains) resolve 100% dos problemas…**

Blockchain: aplicações revolucionárias (será?)

- Identidade centrada no usuário

  - **Problema**: cada usuário precisa gerenciar muitas identidades e atributos, registrados em diferentes locais
    - Usuário controla: onde dados são armazenados, quem acessa o que, e como sua identidade é apresentada (e.g., nome social)
    - Sistema deve fornecer **provas de autenticidade**
  - **Objetivo**: centrar no usuário o controle sobre seus documentos e atributos, podendo fornecer a quem desejar, quando desejar

  - **Solução**: usar Blockchain??
  - Não tem exatamente "**ordem de eventos**" nesse cenário ➔ **Solução mais próxima de real**: *Identity Management* (IdM)
    - Autenticidade: ainda requer **autoridades** p/ emitir e verificar atributos associados a identidade
      - Descentralização se verificador decide em quem confiar
    - Potencial interesse de **logs transparentes** para identificar emissão e revogação indevidas (Transparência de Certificados)

Blockchain: aplicações revolucionárias (será?)

- Identidade centrada no usuário

  – **Problema**: cada usuário precisa gerenciar muitas identidades e atributos, registrados em diferentes locais
    - Usuário controla: **onde dados são armazenados**, **quem acessa o que**, e como sua identidade é apresentada (e.g., nome social)
    - Sistema deve fornecer **provas de autenticidade**

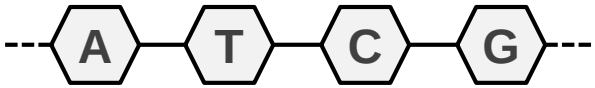
  – **Objetivo**: centrar no usuário o controle sobre seus documentos e atributos, podendo fornecer a quem desejar, quando desejar

  – **Solução**: usar Blockchain??

  – Não tem exatamente "**ordem de eventos**" nesse cenário ➔ **Solução mais próxima de real**: *Identity Management* (IdM)
    - **Não há controle completo** sobre armazenamento/acesso: quem obtém os dados pode repassá-los sem registrar o fato…
    - **DHTs** úteis para: **busca descentralizada** de IDs; **histórico de acessos** por entidades **idôneas** (as inidôneas sempre podem **omitir acessos**…)
      – **Disponibilidade** sem replicação total: mais eficiente que blockchain…

Blockchain: aplicações revolucionárias
(será?)

- Curando o câncer com Blockchain
  - “Blockchain = Conjunto de dados verídicos e imutáveis”



- Alguma que vocês já tenham visto?
  - Agradeço contribuições para expandir esta lista!
- Se nunca viram algo assim, recomendo ler:
  - https://medium.com/@mehmettoral/blockchain-as-the-cure-for-cancer-or-how-a-hammer-was-mistaken-for-a-painting-643741abf972

Conclusão: “sem o hype”

Eu

(e, espero, quem fizer este curso)

Entusiastas de Blockchain

Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Algumas aplicações “questionáveis”

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

USP

Referências

- “Como funciona a iniciativa popular no Brasil”. URL: https://blog.inteligov.com.br/como-funciona-a-iniciativa-popular-no-brasil/
- D. Aranha, M. Karam, A. Miranda, F. Scarel (2014). (In)segurança do voto eletrônico no Brasil / Vulnerabilidades no software da urna eletrônica brasileira. In: Cadernos Adenauer 1/2014: Justiça Eleitoral, 117-133, 2014. URL: https://sites.google.com/site/dfaranha/pubs/aranha-karam-miranda-scarel-12-pt
- B. Adida, O. Marneffe, O. Pereira et al. (online). Helios Voting: Trust the vote. URL: https://vote.heliosvoting.org/
- J. Benaloh et al. (online). ElectionGuard official website. URL: https://www.electionguard.vote/
- A. Rosen, A. Ta-Shma, B. Riva, et al. (online). Wombat Voting System. URL: https://wombat.factcenter.org/
- D. Chaum, R. Carback, J. Clark, C. Liu, M. Nejadgholi, B. Preneel, A. Sherman, M. Yaksetig, F. Zagórski (2020). VoteXX Project - Voting without the booth. URL: https://votexx.org/
- OpenID (online). Welcome to OpenID Connect. URL: https://openid.net/connect/
- OAuth (online). Open Authorization (OAuth) 2.0. URL: https://oauth.net/2/
- IPFS (online). Interplanetary File System (IPFS) powers the Distributed Web. URL: https://ipfs.io
- A. Ulrich, R. Holz, P. Hauck, G. Carle (2011). "Investigating the OpenPGP Web of Trust". Computer Security – ESORICS 2011. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer: 489–507. doi:10.1007/978-3-642-23822-2_27. ISBN 978-3-642-23822-2.

Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Algumas aplicações “questionáveis”

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

USP

Blockchain: aplicações revolucionárias (será?) – revisitado

- Provar que tomou vacina [para COVID-19]

  - **Problema**: site do Ministério Saúde saiu do ar, dificultando acesso ao comprovante de vacina
  - **Solução**: Blockchain??
  - Não tem "**ordem de eventos**" nesse cenário ➔ **Solução real**: bastam as **assinaturas digitais** correspondentes
    - Armazenados por usuários, sem depender de sites p/ verificação
  - ~~Nem **log transparente** soa útil~~: utilidade seria contra temor de **entidades confiáveis** de saúde reescreverem passado
    - Ex.: "forjar comprovante antigo cria impressão de imunização"
      - Mas nada impede comprovante falso emitido no presente...
    - Ex.: "podem eliminar comprovante antigo da base de dados"
      - Mas posse de assinatura digital elimina risco...

Vide próximo slide

- **Log transparente** é sim útil em um cenário real (ainda que surreal):
  - Sistema usado para **apagar registros antigos**
  - **E** não é do interesse do usuário apresentar prova de que o registro existia
    - Quando há tal interesse, assinatura digital costuma bastar: irretratabilidade
- Blockchain soa a exagero:
  - Replicação completa vs. algum grau de replicação para disponibilidade
    - Difícil apagar todas as cópias
  - Consenso distribuído vs. ordem definida por servidor central
    - Nível federal, ou por estado

terra

Capa › Notícias › Brasil › Política

Política

Vacina falsa de Bolsonaro: Secretário admite ter usado senha de enfermeira para excluir dados do SUS

João Carlos de Sousa Brecha incluiu informações de ex-presidente no sistema do Ministério de Saúde, segundo a PF

Redação Terra

23 jun 2023 - 09h29 (atualizado às 11h30) Compartilhar Ver comentários

À PF, Bolsonaro voltou a dizer que não se vacinou e negou participação em qualquer iniciativa para adulterar o próprio cartão de vacinação e o da filha

Foto: Reprodução

Blockchain, Criptomoedas & Tecnologias Descentralizadas

Blockchain sem o hype:

Algumas aplicações “questionáveis”

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

USP