Fundamentos e desafios do blockchain 3.0

Erikson J. de Aguiar

erjulioaguiar@usp.br

Quem sou eu ?

Intermídia

- Aluno de mestrado no **ICMC - USP**
- BSc. Ciência da Computação - **UENP**
- Santa Mariana - PR
- **Áreas de concentração:**
  - Sistemas distribuídos
  - Redes
  - IoT
  - Blockchain
  - Privacidade

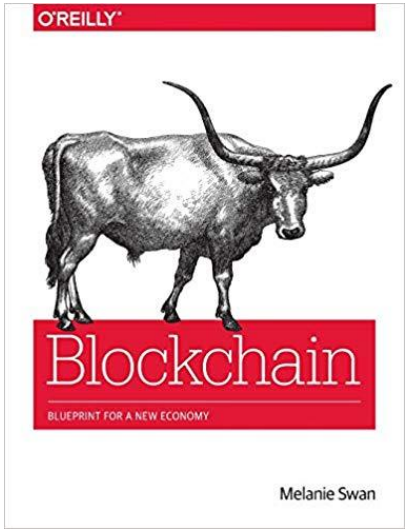
https://eriksonjaguiar.github.io/

Agenda

- Introdução ao blockchain
- Características do blockchain
- Tipos de rede blockchain
- Protocolos de consenso
- Contratos inteligentes
- Desafios do blockchain
- Estudos de caso
- Oportunidades

Introdução ao blockchain

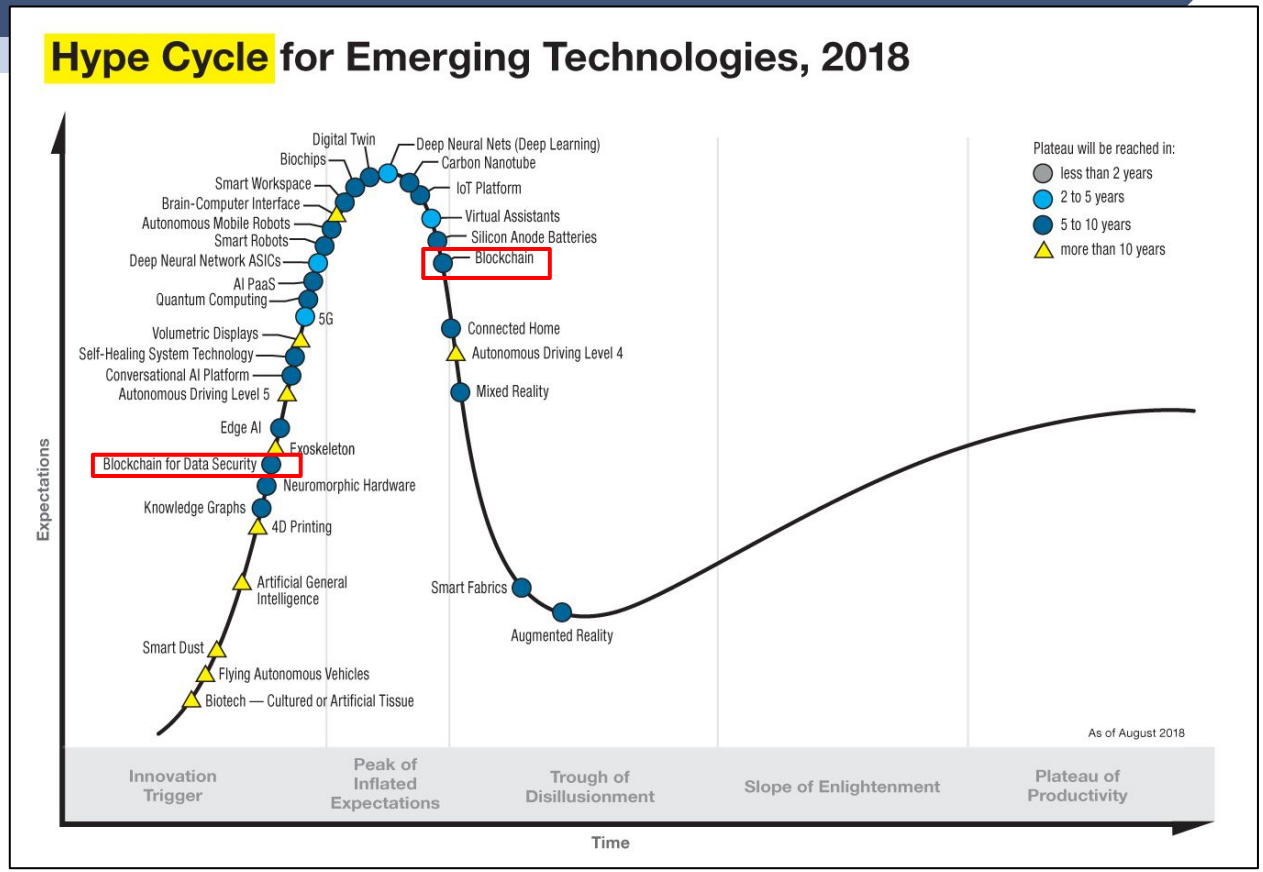
Por que blockchain 3.0 ?



(SWAN, 2015)

- Classificação de blockchain:
  - blockchain 1.0: Bitcoin
  - blockchain 2.0: Contratos inteligentes
  - blockchain 3.0: vários campos de aplicação (Atual)
- **Blockchain não é somente Bitcoin**

Potencial do blockchain



Fonte: (GARTNER, 2018)

Potencial do blockchain

- **2009-2020:** Integração do blockchain nas empresas com as tecnologias existentes
- **2016-2020:** Trata de aplicações específicas que utiliza de tokens e descentralização
- **2021-2025:** Soluções completamente baseadas em blockchain
- **Depois de 2025:** Contratos autônomos, DAOs e microtransações

Fonte: (GARTNER, 2018)

Arquitetura do Bitcoin

- Apresenta a primeira arquitetura do blockchain (2008-2009)
- Criado por Satoshi Nakamoto
- Tem um livro-razão público
- Utiliza o protocolo de consenso PoW (Mineração)
- A moeda digital é um token que é trocado entre os participantes da rede

Fonte: (NAKAMOTO, 2008)

Cypherpunks

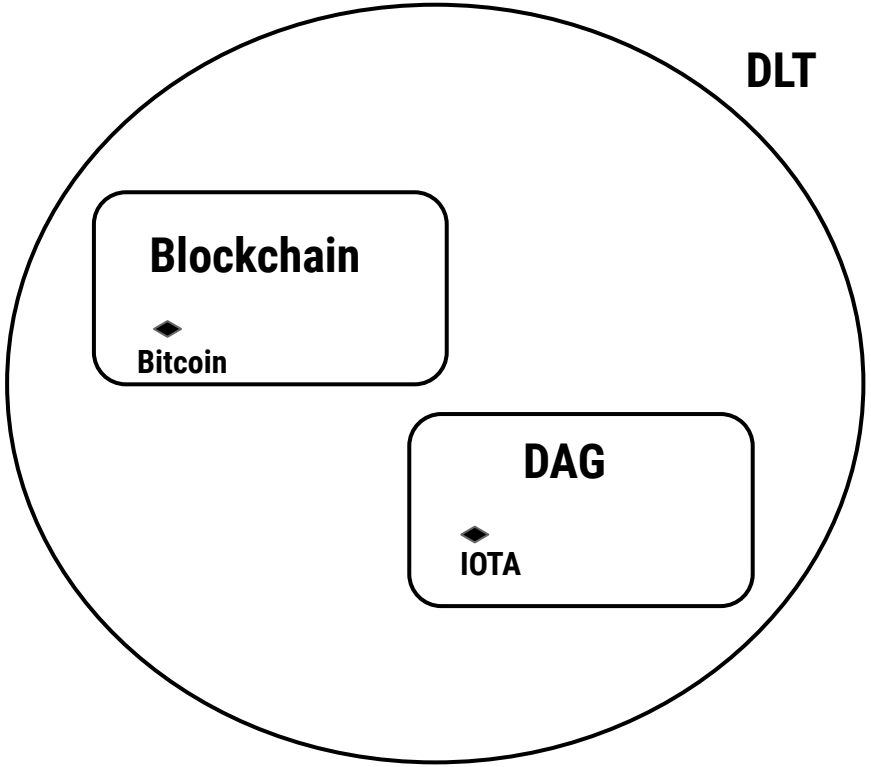
- Há uma teoria que eles criaram o blockchain
- Pessoas envolvidas no movimento Cyberpunk:
  - Adam Back - Inventor do Hashcash
  - Nick Szabo - Contratos inteligentes
  - Bram Cohen - Criador do BitTorrent
  - Julian Assange - Criador do Wikileaks

Grupos que trabalham com blockchain

- **ICMC/USP - Prof. Dr. Jó Ueyama (Brasil)**
- Unifesp e ITA (Brasil)
- USC - Prof. Bhaskar Krishnamachari (EUA)
- ETH Zurich - Prof. David Basin (Suíça)
- Stanford - Prof. David Mazières (EUA)

Características do blockchain

Definição do blockchain

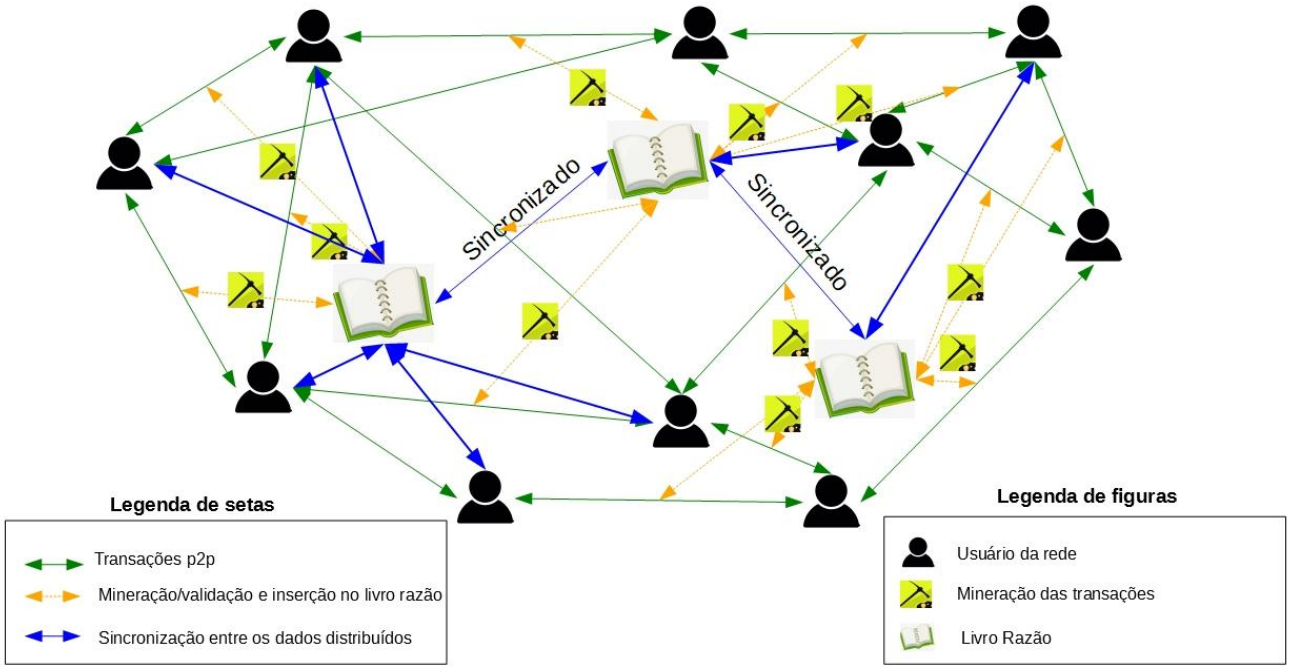


Definição do blockchain

- É uma tecnologia de livro-razão distribuída - DLT
- Tem como estrutura de dados blocos encadeados
- É uma tecnologia de livro-razão replicado e distribuído
- Fundamentada em um rede **P2P**
- Não precisa de um terceiro confiável

Fonte: (RIFI et al., 2017)

Definição do blockchain

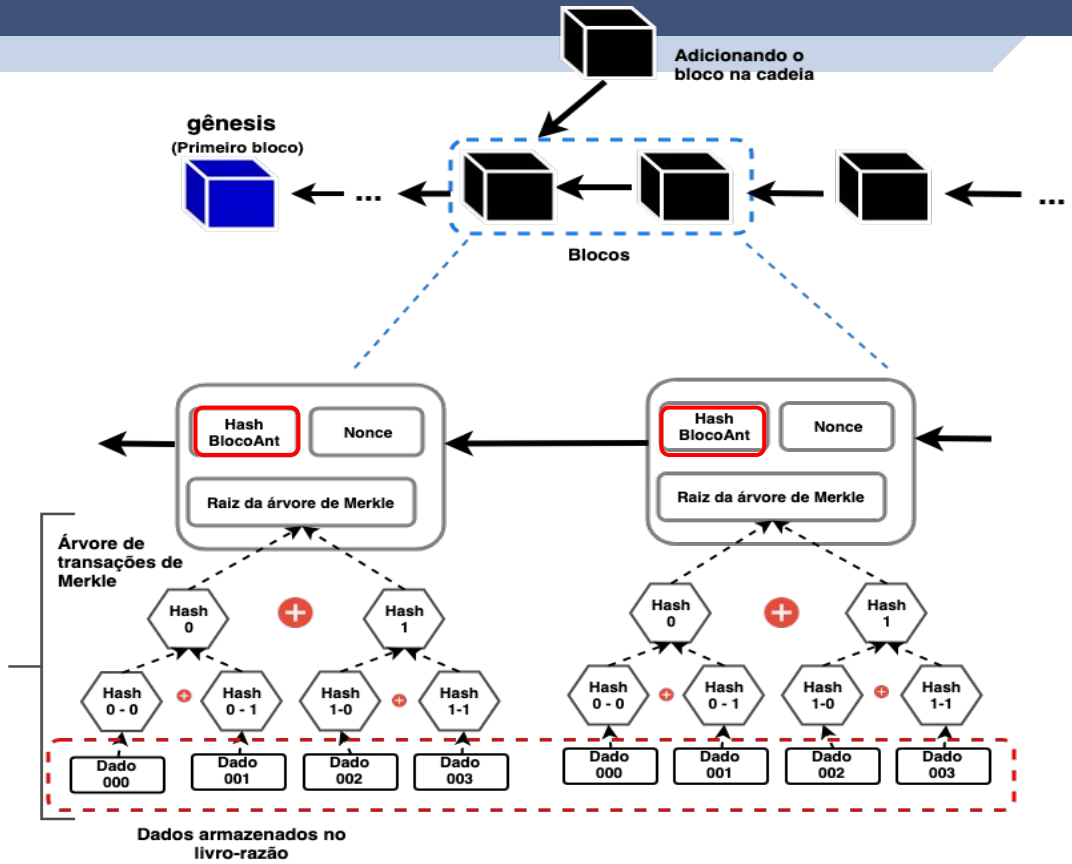


Conceitos básicos: Funções Hash

- Definição:
  - h = H(m)
  - m = mensagem de tamanho variável
  - Não tem função inversa
  - Algoritmo SHA-256 - Ferramenta

Fonte: (STALLINGS, 2017)

Conceitos básicos: bloco



Fonte: (DINH et al., 2017)

Conceitos básicos: bloco

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c817010000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Block hash

0000000000000000 e067a478024addfe cdc93628978aa52d 91fabd4292982a50

Fonte: (DINH et al., 2017)

Características fundamentais

- **Desintermediação:** Sistemas realizando acordo de forma direta entre si, sem um terceiro confiável
- **Disponibilidade e integridade:** Livro-razão replicado
- **Transparência e Auditabilidade:** Livro-razão público
- **Imutabilidade dos dados:** Devido ao ponteiro Hash o livro-razão é imutável
- **Anonimidade:** Realizar transações sem que terceiros tenham acesso

Fonte: (GREVE et al., 2018)

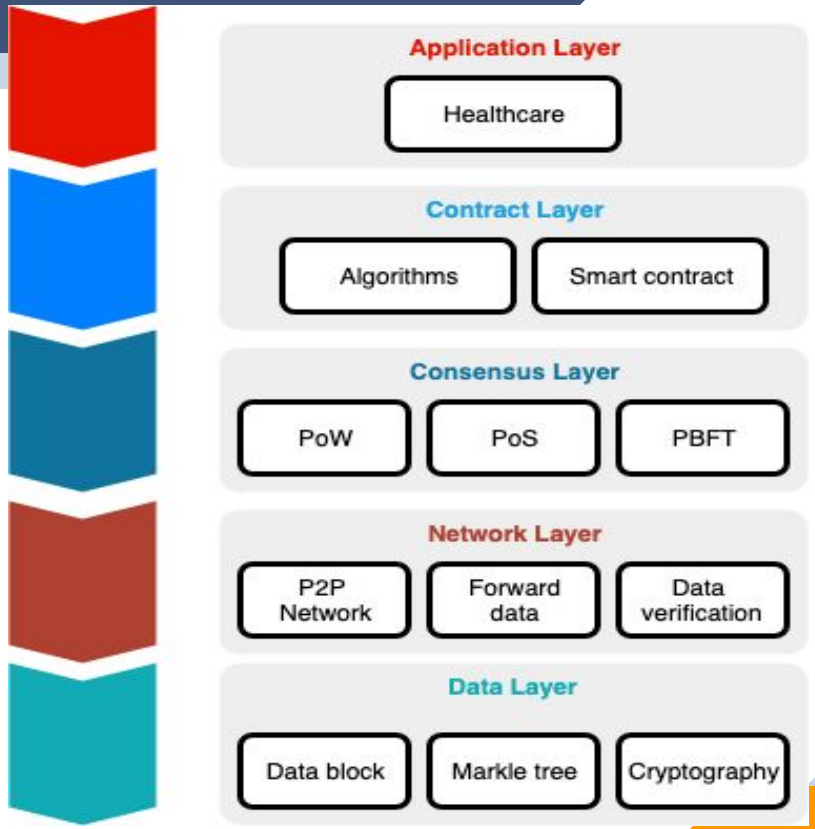
Características fundamentais

- **Incentivo:** Modelo de negócios baseado no incentivo por validar uma transação

Fonte: (GREVE et al., 2018)

Camadas do blockchain

- Camada de aplicação
- Camada de contrato
- Camada de rede
- Camada de dados



Fonte: (YUAN; WANG, 2017)

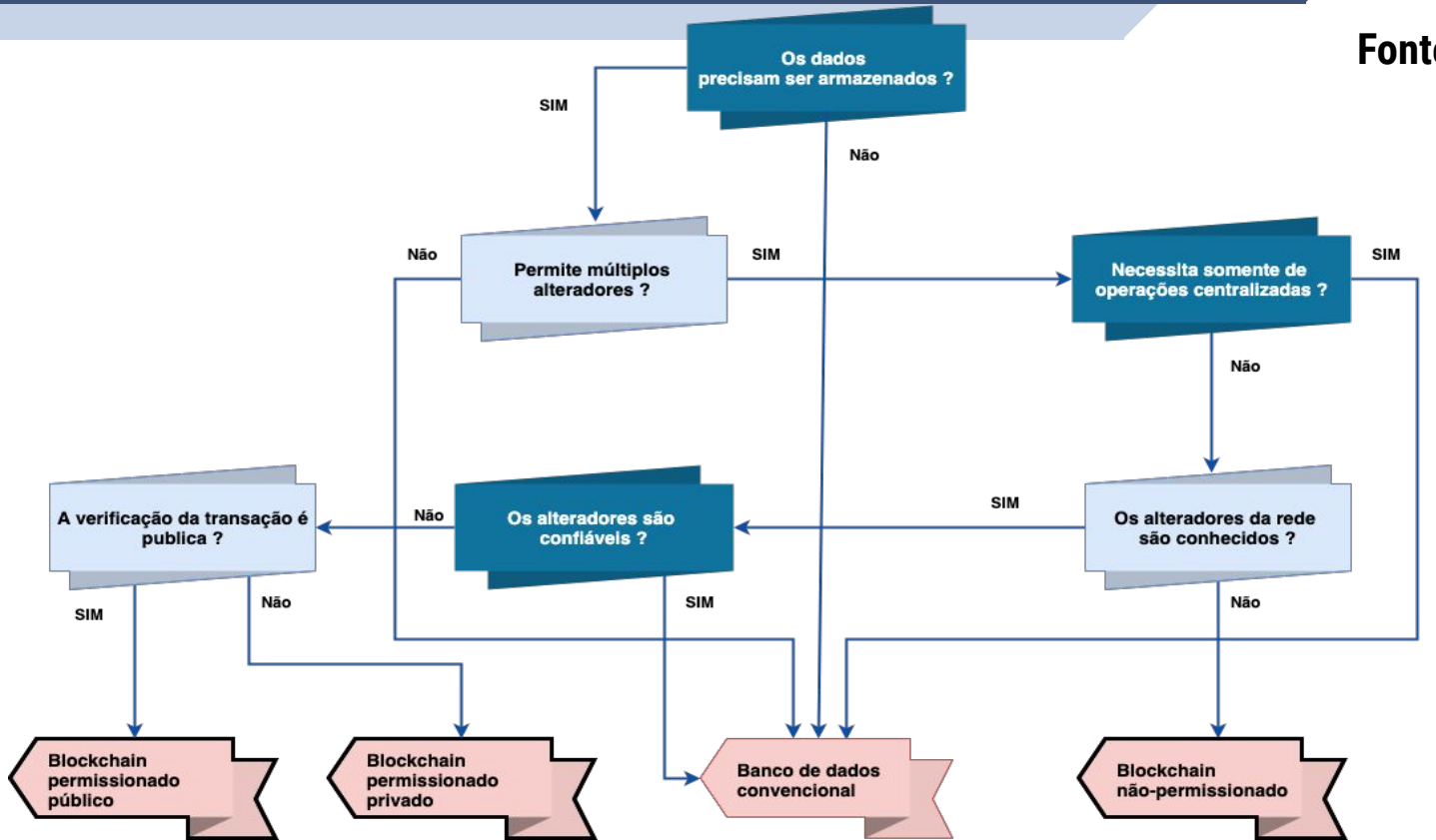
Tipos de redes blockchain

Descrição

Fonte: (WUST; GERVAIS, 2017)

- Podemos classificar as redes em três tipos:
  - **Permissionado público:** Nos específicos realizam o consenso
  - **Permissionado privado:** Um única organização controla a rede
  - **Não-permissionado:** Qualquer nó pode fazer o consenso e ler o livro-razão

Como escolher o tipo de rede?



Fonte: (WUST; GERVAIS, 2017)

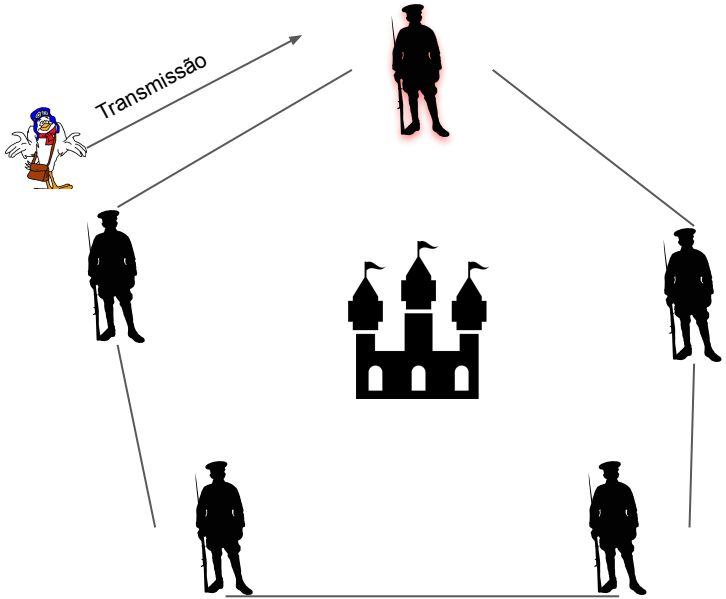
Protocolos de consenso

Definição

- Estabelece um acordo entre as partes para determinar se um transação é válida
- Inspirado no **Hashcash**
- Temos protocolos públicos e privados
- Bitcoin (público)
- Hyperledger Fabric (Privado)

Fonte: (RIFI et al., 2017)

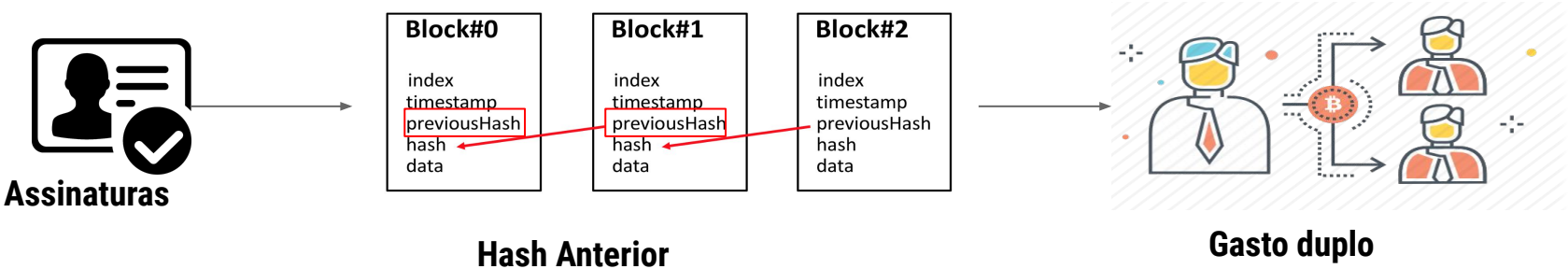
Problema dos generais Bizantinos



Fonte: (LAMPORT; SHOSTAK; PEASE, 1982)

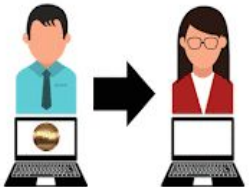
Problema dos generais Bizantinos

Verificação da transação

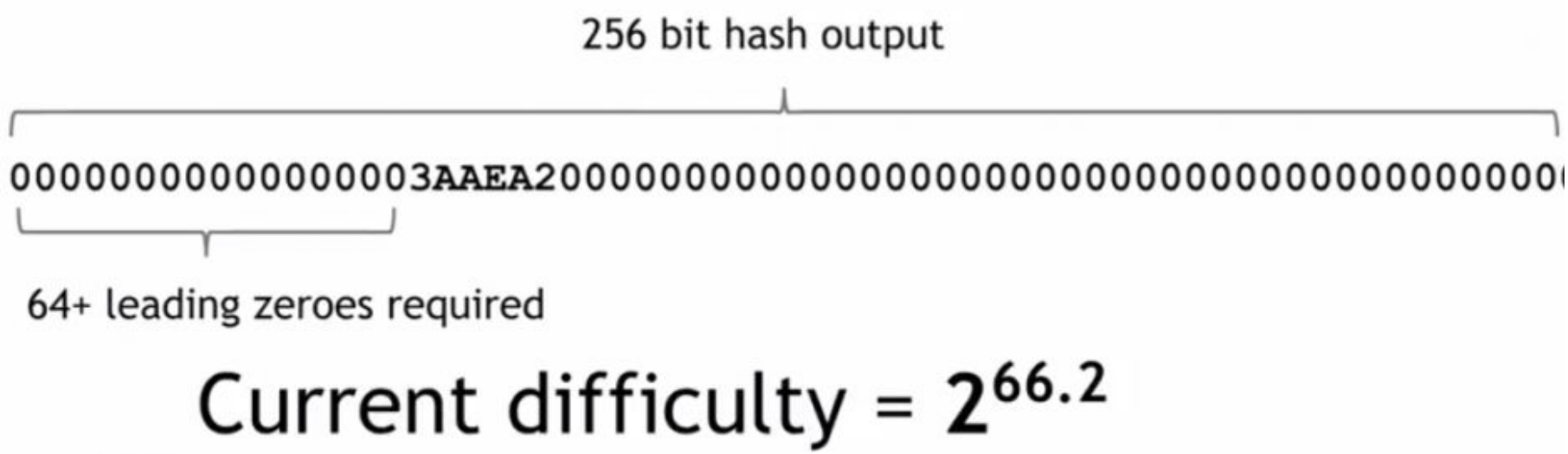


Fonte: (GREVE et. al., 2018)

Prova de trabalho

A -> B	Envia T Para a Rede	Resolver o Desafio	Consenso	T Finalizada
 A B	 Lança o Desafio	PoW  Alto Custo* 1º Resolver Envia S para Rede 10 min	 Novo Nó Add (Refresh Ledger)  PoW	 Recompensa 

Prova de trabalho



Fonte: (NAKAMOTO, 2008)

Outros protocolos

- ***Proof of Stake* (PoS)**
  - Reduzir o custo de validação
  - É baseado na posse da criptomoeda
- **PBFT**
  - Baseado em votação para validar o bloco
  - Os nós falhos < número total / 3
  - aguarda a confirmação de 2*(f + 1) nós

Fonte: (GREVE et. al., 2018) e (MINGXIAO et al., 2017)

Contratos inteligentes

Definição

- O termo contrato inteligente for definido por **Nick Szabo**
- Determina que uma transação eletrônica siga termos de um contrato
- Os contratos inteligentes tem o objetivo de satisfazer tarefas comuns
  - Comprar algo online
  - Trocar um ativo
- Reduzir o número de fraudes

Fonte: (GREVE et. al., 2018)

Ferramentas de implementação

- **Hyperledger Fabric:**
  - Privado
  - Provê escalabilidade
  - Utiliza o PBFT
  - Gerenciado pela IBM
  - Linguagem CTO, GO e JavaScript

https://composer-playground.mybluemix.net/editor

- **Ethereum:**
  - Público
  - Utilizado o PoS
  - Token GAS
  - Linguagem GO e Solidity

https://remix.ethereum.org

Hyperledger Composer

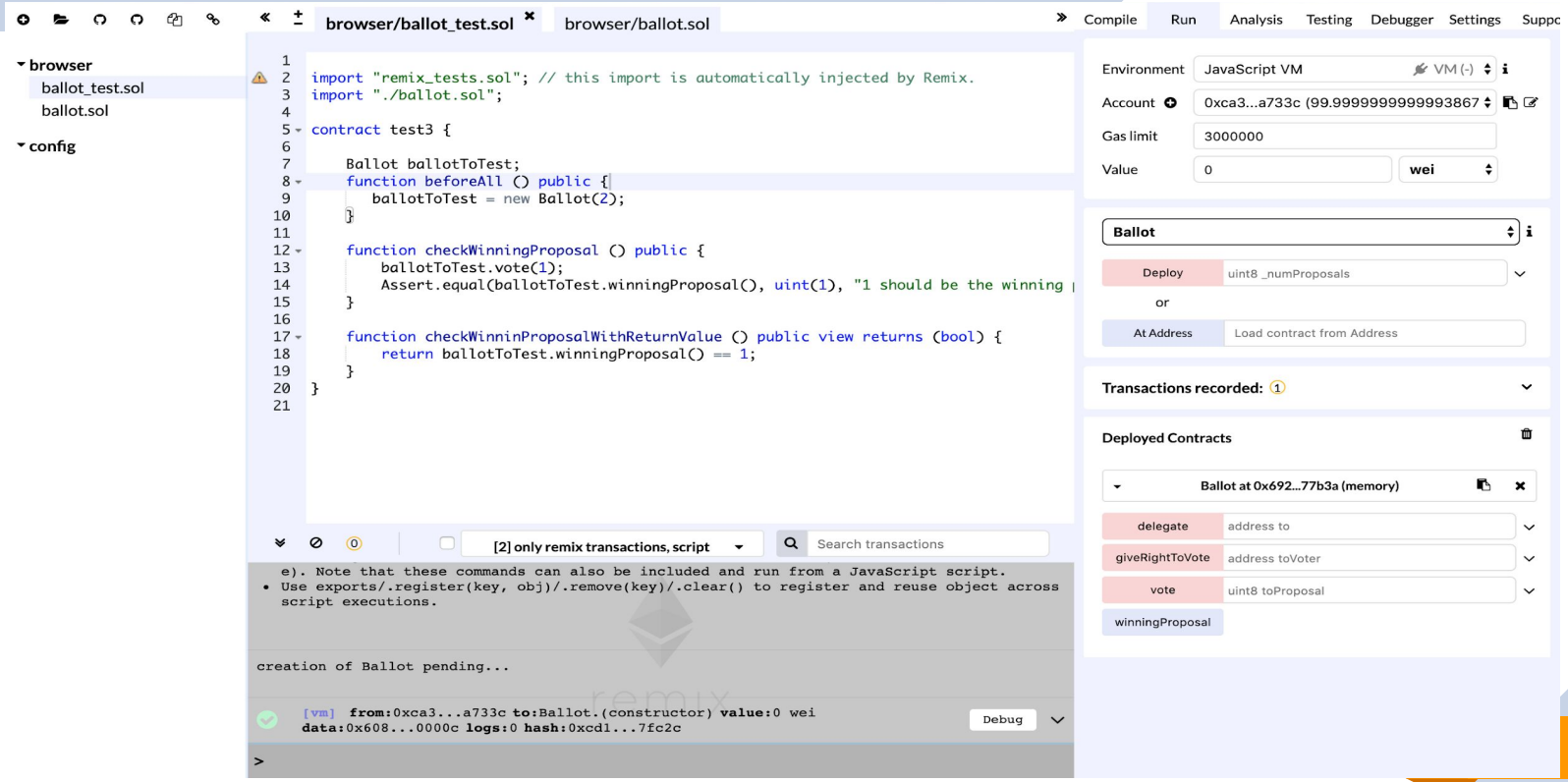
Script File lib/sample.js

```
async function sampleTransaction(tx) {  // eslint-disable-line no-unused-vars

    // Save the old value of the asset.
    const oldValue = tx.asset.value;

    // Update the asset with the new value.
    tx.asset.value = tx.newValue;

    // Get the asset registry for the asset.
    const assetRegistry = await getAssetRegistry('org.example.basic.SampleAsset');
    // Update the asset in the asset registry.
    await assetRegistry.update(tx.asset);

    // Emit an event for the modified asset.
    let event = getFactory().newEvent('org.example.basic', 'SampleEvent');
    event.asset = tx.asset;
    event.oldValue = oldValue;
    event.newValue = tx.newValue;
    emit(event);
}

```

Model File models/sample.cto

```
namespace org.example.basic

asset SampleAsset identified by assetId {
  o String assetId
  --> SampleParticipant owner
  o String value
}

participant SampleParticipant identified by participantId {
  o String participantId
  o String firstName
  o String lastName
}

transaction SampleTransaction {
  --> SampleAsset asset
  o String newValue
}

event SampleEvent {
  --> SampleAsset asset
```

Remix Solidity



Desafios do blockchain

Desafios

- Latência
- Throughput
- Largura de banda
- **Segurança**
- **Privacidade**
- Usabilidade
- Desperdício de recursos (Energia)

Fonte: (SWAN, 2015)

Segurança

- Gasto duplo
  - Saldo A = $ 100
  - TA -> A ⟶ B - Timestamp:2019-03/08-10:30:00 ($ 100)
  - TB -> A ⟶ C - Timestamp:2019-03/08 - 10:30:00 ($ 100)
  - Cadeia mais longa
- Perda da chave para acesso da carteira
- Falsificação das assinaturas

Fonte: (SWAN, 2015)

Privacidade

- Trata de dados pessoais do usuário
- Duas classes:
  - Privacidade de transação
  - Privacidade de identidade

Fonte: (FENG et al., 2019)

Técnicas de privacidade

- Criptografia homomórfica
- Prova de conhecimento zero
- Criptografia baseada em atributos
- Multi-Party computation - SGX Intel
- Mixing

Fonte: (FENG et al., 2019)

Estudos de caso

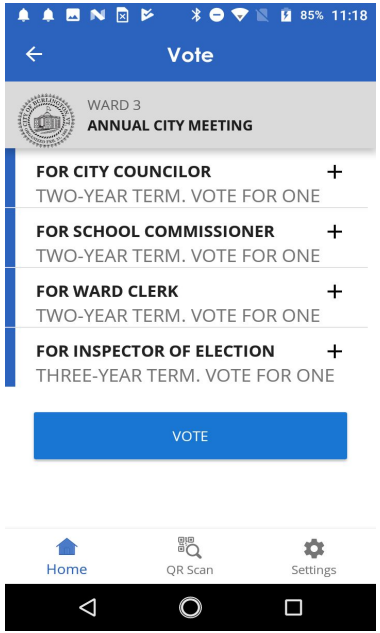
Financeiro

- BNDES Token
- Blockchain público
- Para registrar a distribuição de recursos
- Como empréstimos para instituições públicas
- API Web para acesso

Fonte: (ARANTES JR. et al., 2018)

Governamental

- Voted
- Aplicação baseada em blockchain para voto eletrônico
- Foi testado no Oeste da Virgínia - EUA
- Blockchain privado
- Eleitor tem um Id que referencia sua carteira
- Aplicativo é o Voatz



Saúde e IoT

- Monitoramento de pacientes utilizando IoT
- O dados são enviados para um Gateway
- O Gateway transfere as informações para servidor público em um rede blockchain
- Controle no acesso dos dados do paciente

Oportunidades de pesquisa

Oportunidades

- Melhorias na autonomia dos protocolos de consenso
- Garantir a privacidade dos usuários
- Tornar os contratos inteligentes autônomos (IA)
- Metodologias para modelagem de contratos

Oportunidades

- Melhoria na usabilidade das aplicações descentralizadas
- Prover escalabilidade as aplicações descentralizadas
- Seguir políticas de proteção a dados como a LGPD ou GDPR
- Melhor gerenciamento na distribuição das chaves

Considerações finais

Conclusões

- Blockchain é muito mais que só BTC
- É aplicado a qualquer área
- Está no início e ainda apresentando várias limitações
- Podemos construir Dapps

Perguntas ??

Obrigado!

Fundamentos e desafios do blockchain 3.0

Erikson J. de Aguiar

erjulioaguiar@usp.br

ICMC USP SÃO CARLOS

Intermídia

Referências

- SWAN, M. Blockchain: Blueprint for a new economy. [S.l.]: "O'Reilly Media, Inc.", 2015
- NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. 2008. Acessado em: 01-062019 [White paper]. Disponível em: <https://bitcoin.org/bitcoin.pdf>
- RIFI, N.; RACHKIDI, E.; AGOULMINE, N.; TAHER, N. C. Towards using blockchain technology for eHealth data access management. In: 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME). IEEE, 2017. p. 1–4. ISBN 978-1-53861642-0
- STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas. [S.l.]: Pearson, 2017.
- Barcellos, Antonio Marinho Pilla, and Luciano Paschoal Gaspary. Segurança em redes p2p: Princípios, tecnologias e desafios. Simpósio Brasileiro de Redes de Computadores 2006

Referências

- STALLINGS, W. Criptografia e Segurança de Redes: Princípios e Práticas. [S.l.]: Pearson, 2017.
- Barcellos, Antonio Marinho Pilla, and Luciano Paschoal Gaspary. Segurança em redes p2p: Princípios, tecnologias e desafios. *Simpósio Brasileiro de Redes de Computadores 2006*
- DINH, T. T. A.; WANG, J.; CHEN, G.; LIU, R.; OOI, B. C.; TAN, K.-L. BLOCKBENCH: A Framework for Analyzing Private Blockchains. In: Proceedings of the 2017 ACM International Conference on Management of Data - SIGMOD '17. ACM Press, 2017. p. 1085–1100. ISBN 9781450341974. Disponível em: <https://dl.acm.org/citation.cfm?id=3064033>
- GREVE, Fabíola et al. Blockchain e a Revolução do Consenso sob Demanda. **Livro de Minicursos do SBRC**, v. 1, p. 1-52, 2018
- YUAN, Y.; WANG, F. Blockchain and cryptocurrencies: Model, techniques, and applications. IEEE Transactions on Systems, Man, and Cybernetics: Systems, v. 48, n. 9, p. 1421–1428, Sep. 2018. ISSN 2168-2216

Referências

- Wüst, K.; Gervais, A. Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). [s.n.], 2018. p. 45–54. Disponível em: <https://ieeexplore.ieee.org/document/8525392>
- MINGXIAO, D.; XIAOFENG, M.; ZHE, Z.; XIANGWEI, W.; QIJUN, C. A review on consensus algorithm of blockchain. In: EEE International Conference on Systems, Man, and Cybernetics, SMC 2017. [s.n.], 2017. p. 2567–2572. ISBN 9781538616451. Disponível em: <https://ieeexplore.ieee.org/document/8123011>
- FENG, Q.; DEBIAO, H.; ZEADALLY, S.; KHAN, M. K.; KUMAR, N. A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, v. 126, p. 45–58, 2019. ISSN 1084-8045. Disponível em: <http://www.sciencedirect.com/science/article/ pii/S1084804518303485>