

Blockchain 101

Thiago Nóbrega

<https://github.com/thiagonobrega>

Disclaimer

Informações Importantes

O que não vamos aprender

- Crypto ativos
- Valuation
- Balanceamento de Carteira



Concetitos de Criptografia

- Funções Hash
- Assinaturas Digitais

Introdução

Blockchain

TL;DR

“Blockchain is a immutable append only transaction log”



Receita Federal

Casos de uso

- E-GOV
 - b-CPF
 - Assinatura de Contratos
 - validação de documentos





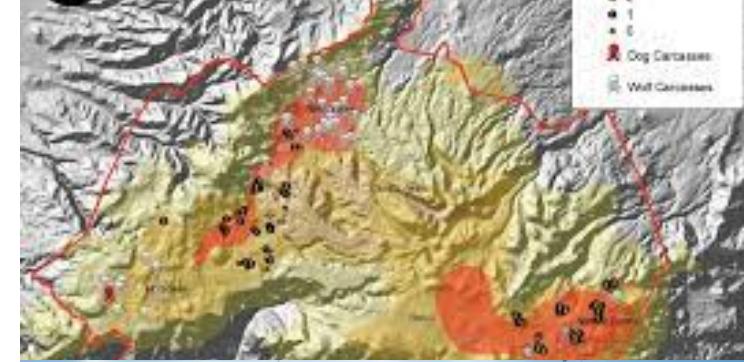
Casos de uso

- Financial & Commercial Service [1]
 - Nasdaq
 - [Honduran land](#)
 - Diamond Track

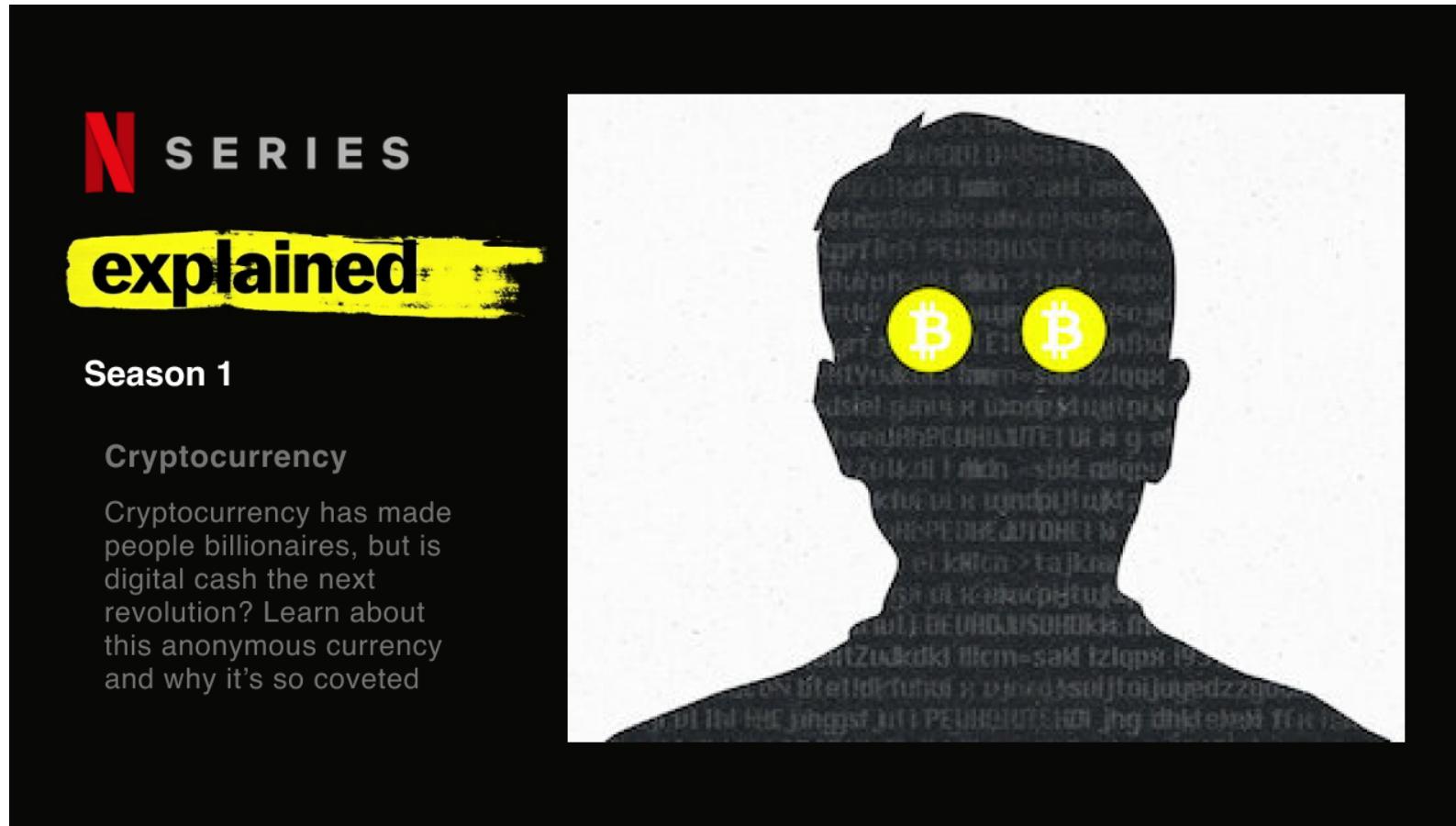


Casos de uso

- Geospatial
 - Secure sharing of geospatial wildlife data (SIGMOD) [2]
 - Geofences UAV (SIGSPATIAL) [3]
- Health System [4-6]
 - Medical records
 - Medical Images
- Smartcity



Curiosidades e Histórico



<https://www.netflix.com/watch/80243756>

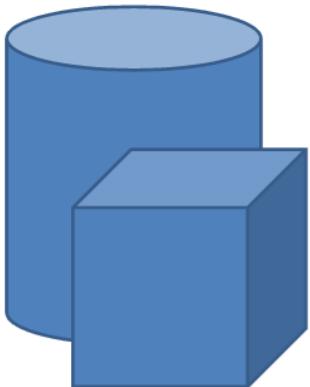
Quais razões levaram a adoção da Blockchain em tantos cenários diferentes?

Características

- Decentralizado
- Imutável (*Temper Evident*)
- Transparente/Auditável
- Pode ser utilizado por adversários (*Distrustful Parties*)

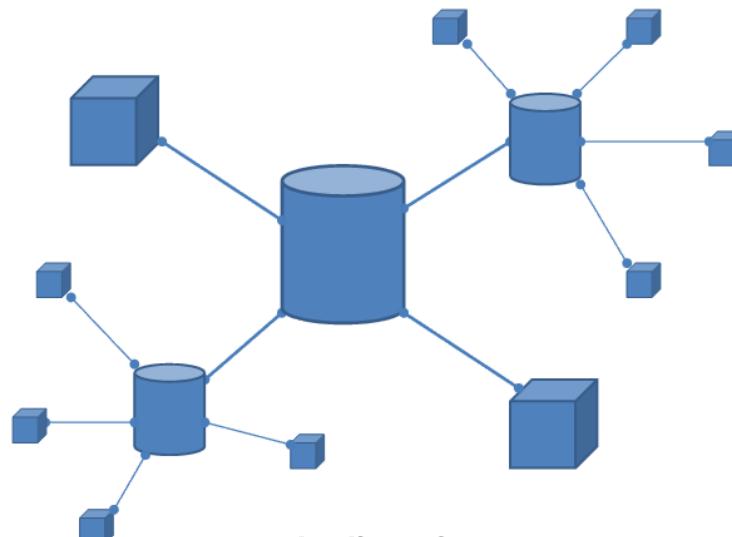
Características da rede

Distribuição de dados



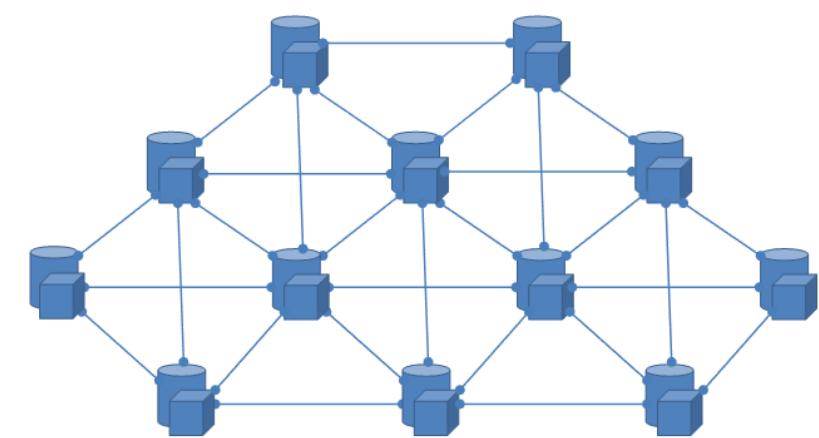
Centralized

one node does everything



Distributed

nodes distribute work to sub-nodes



Decentralized

nodes are only connected to peers

Tipos de rede

Permissionaria (permissioned)

Publicas

Controle decentralizado

i.e., cryptomoedas

Não permissionaria (permissionless)

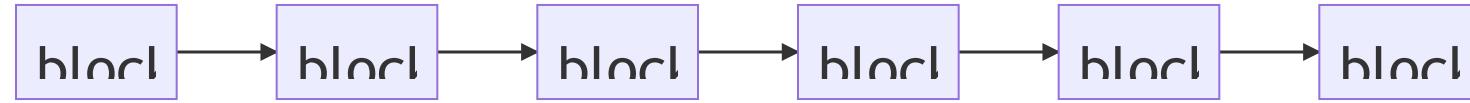
Privadas (ou consorcio)

Controle centralizado*

i.e., Banco Central, LACChain

Imutável

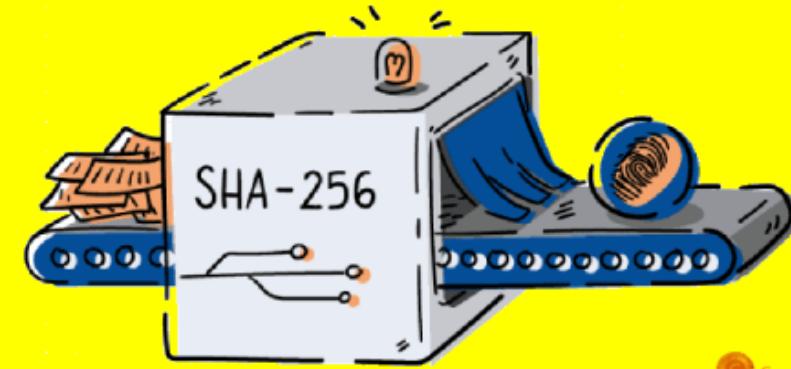
Estrutura da blockchain



Funções Hash

- distribuição uniforme
- determinístico
- resistende a colisão

Working of SHA-256 Algorithm Explained
SHA-256 Encryption



 CryptoSoftwares —

Hashing

$$h(x) = x \bmod 2^{256}$$

Funções Hash

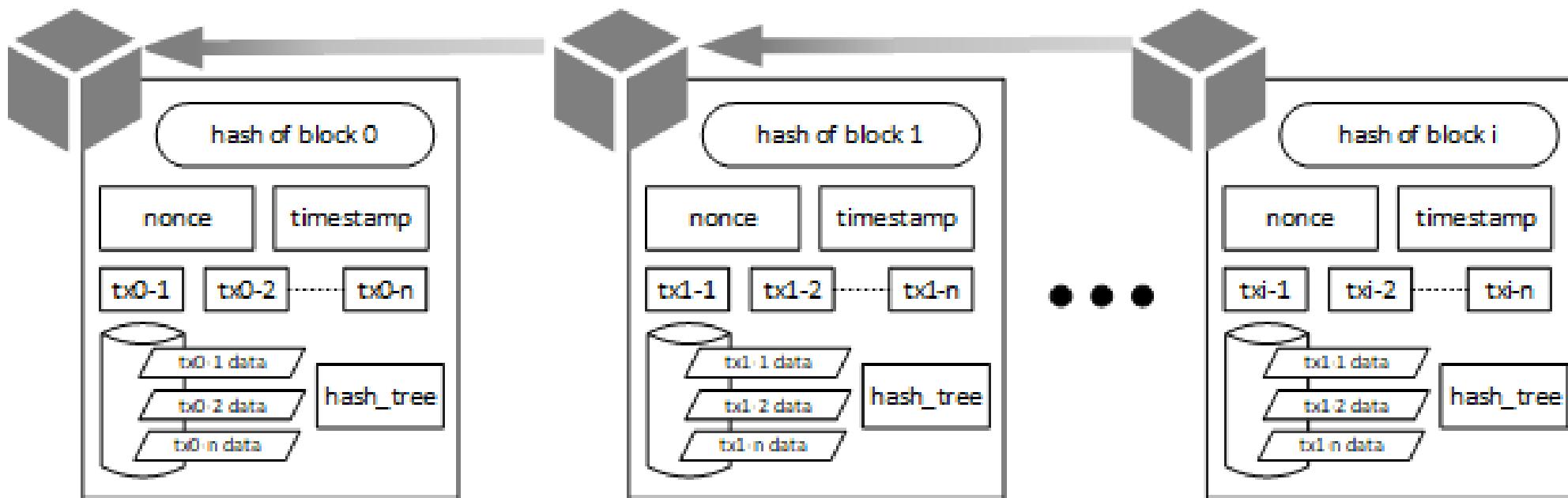
- Message Digest (md5)
 - 128 bits
- Secure Hash Algorithm (SHA)
 - 256 bits

Exemplo da utilização de Hash

Estrutura da blockchain



Detalhe do encadeamento



Exemplo do encadeamento

Transparente/Auditável

Proveniência/procedencia do dado

Proveniência de dados

1. O quê?
2. Quando?
3. Quem?

Como o blockchain identifica as autores das alterações dos dados?

Criptografia Assimétrica

Criptografia Assimétrica

$M \leftarrow$ mensagem plana

$C \leftarrow$ mensagem codificada

$chave_pub \leftarrow$ chave pública

$chave_priv \leftarrow$ chave privada

$n \leftarrow$ tamanho da chave em bits

- $\text{codifique}(M, chave_pub) = M^{chave_pub} \bmod n$
- $\text{decodifique}(C, chave_priv) = C^{chave_priv}$

Assinatura Digital

Assinatura

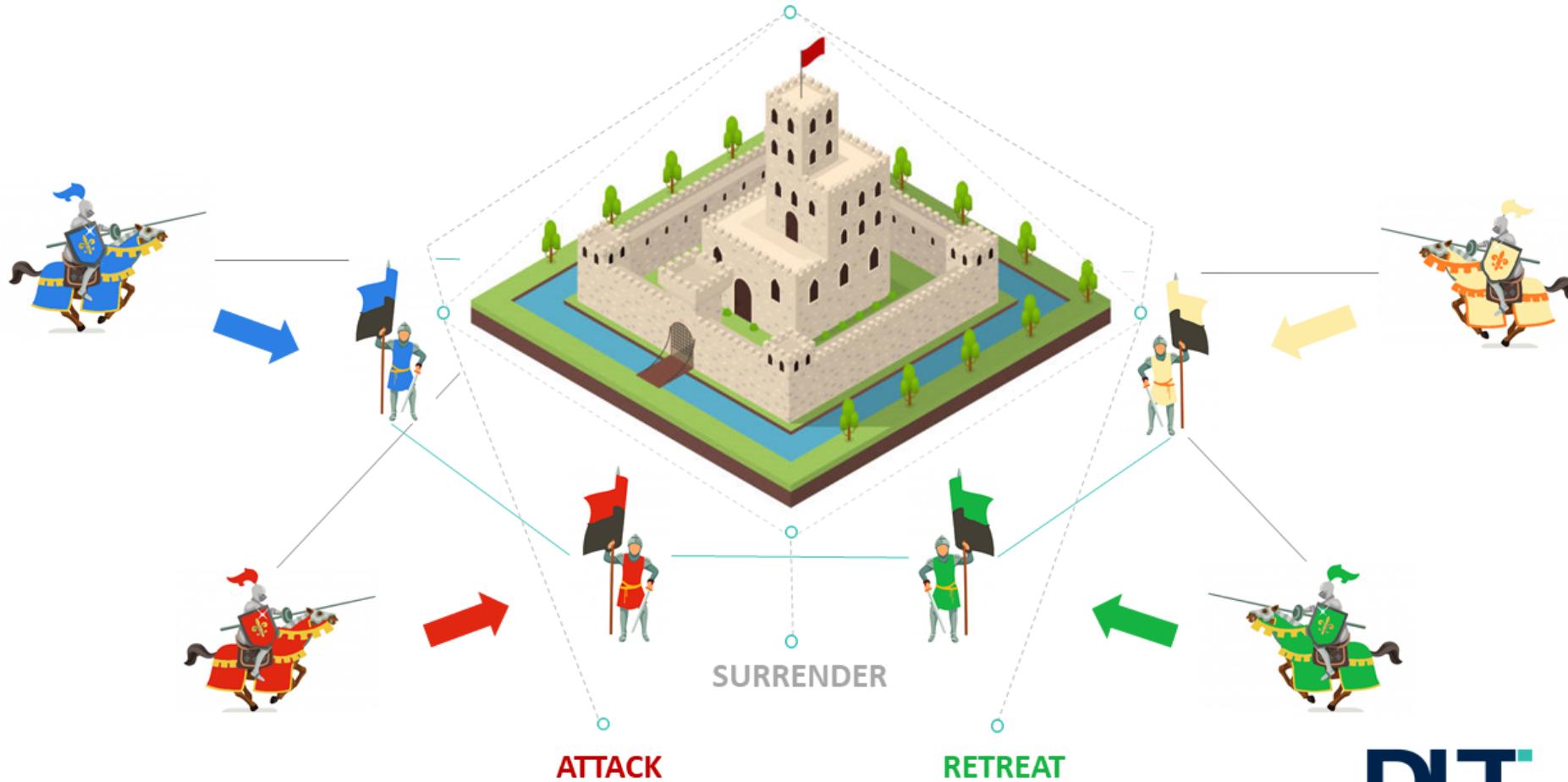
Assinatura Digital

Validação da Assinatura

Distrustful Parties

Algoritmos de consenso

Byzantine Generals' Problem



Algoritmos de consenso das blockchains

- PoW (Proof of Work)

Prova de Trabalho

Miner

Miners receive block rewards

- PoS (Proof of Stake)

To become a validator, a coin owner must "stake" a specific amount of coins (i.e., Ethereum 32 ETH)

validators

Validators receive transactions fees as rewards

- Proof-Of-Authority (PoA)

Limitadores do uso da Blockchain

Limitadores do uso da Blockchain

Alto custo de armazenamento

Privacidade dos dados

Blockchain é um tipo de sistema de gerenciamento de dados?

Sim

"Untangling blockchain: A data processing view of blockchain systems"

[8-12]

Tipos de sistemas

SGBDs tradicionais

Mysql, Oracle, Postgres, SQLServer

SGBDs distribuídos

VoltDB, Oracle*, CosmosDB

Sistemas de arquivo distribuídos

HDFS (Apache Hadoop)

Comparativo

| | Controle Centralizado | Transparente | Consultas | Storage | T. Falha |
|------------------|-----------------------|--------------|-----------|---------|------------------|
| BDs tradicionais | sim | não | complexas | grande | não |
| BDs distribuidos | sim | não | complexas | grande | não bizantina |
| HDFS | sim | não | não | grande | não bizantina |

Comparativo

| | Controle Centralizado | Transparente | Consultas | Storage | T. Falha |
|------------------|-----------------------|--------------|-------------|---------|-------------|
| BDs tradicionais | sim | não | complexas | grande | não |
| BDs distribuidos | sim | não | complexas | grande | n.bizantina |
| HDFS | sim | não | não | grande | n.bizantina |
| Blockchain | não | sim | chave-valor | pequena | bizantina |

Comparativo de transações por segundo

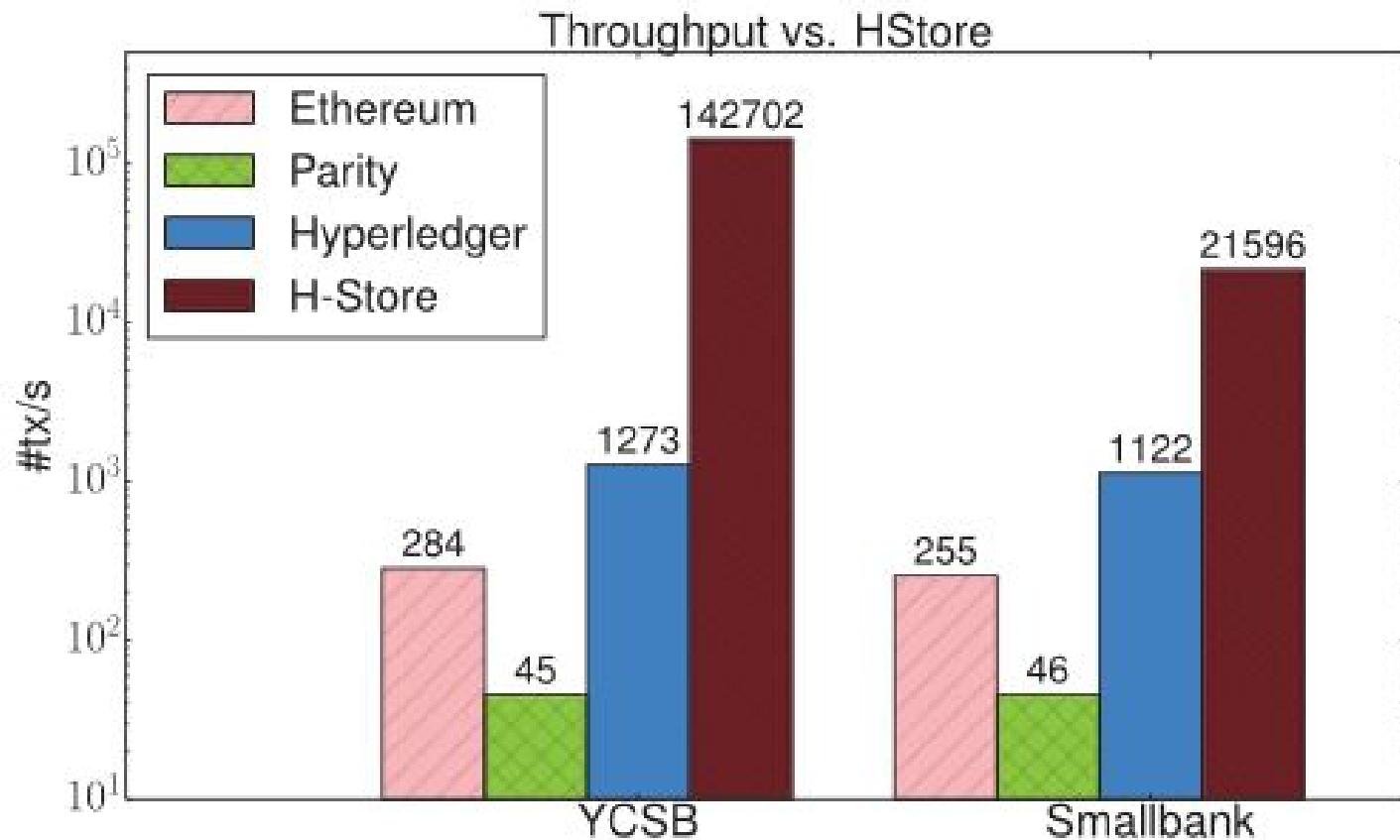


Fig. 7. Performance of the three blockchain systems versus H-Store.

[9]

Quando não utilizar blockchain

Restrições quanto ao número de operações por segundo

Privacidade de armazenamento

Custo de Armazenamento

Tema do próximo encontro

Como escrever aplicações decentralizadas utilizando Blockchain