Universidade Federal do Espírito Santo

Blockchain como servidor de um jogo online: uma análise com proof of stake

Trabalho de Conclusão de Curso I

Aluno: Caio Vianna Rizzo
Orientador: Prof. Wilian Hiroshi Hisatugu

Dezembro 2018
São Mateus, ES

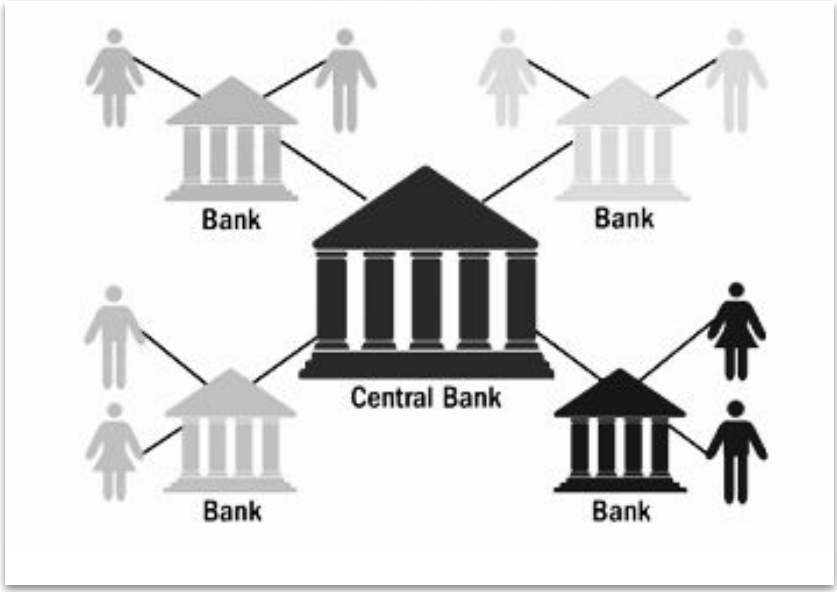
Indice

- Introdução
- Bitcoin
- Blockchain
- Projeto

Introdução

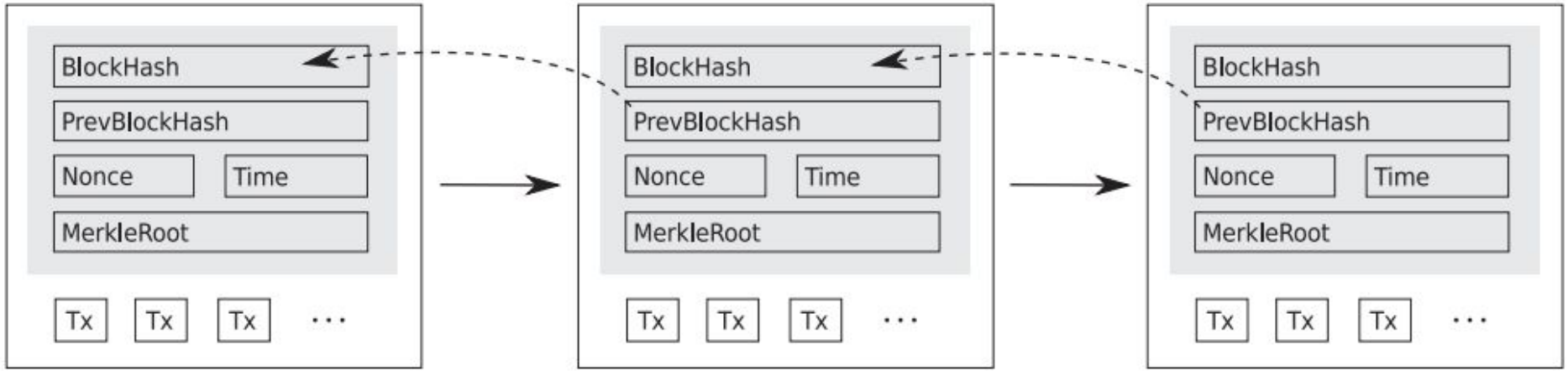
Universidade Federal do Espírito Santo

- Dinheiro e moeda
- Sistema bancário atual
- Bitcoin
- Todos são o banco
- Gasto duplo



Bitcoin

- Proof of work
- Timestamp server
- Transações
- Rede peer-to-peer



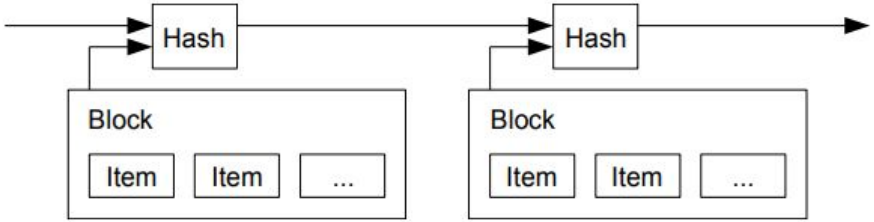
Bitcoin - Proof of Work

Universidade Federal do Espírito Santo

- Mineradores
- Hash
  - One way hash - unidirecional
  - Alterações em dados gera alterações de hash
- Cálculo do hash
  - Nonce, hash do bloco anterior, hash das transações do bloco
  - Target - Taxa de dificuldade da rede
  - SHA256
  - Através de força bruta - usando poder de processamento
  - Maior poder de processamento gera maior vantagem
- Garantia de não alteração
- Quorum
  - Poder computacional

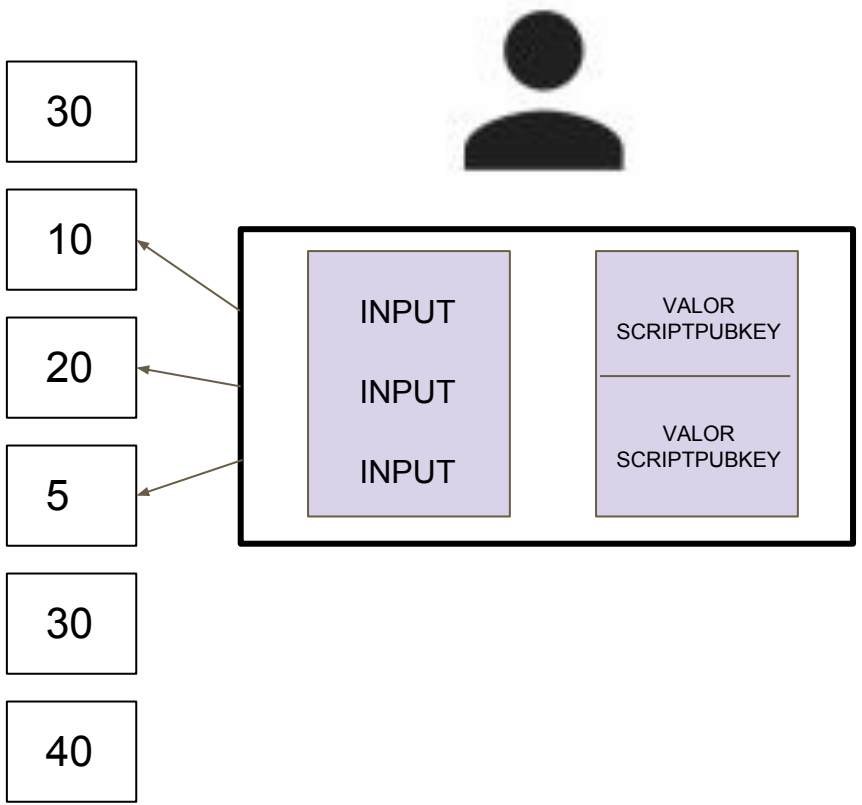
Bitcoin - Timestamp

- A rede garante a ordem
- Obriga oredenação total



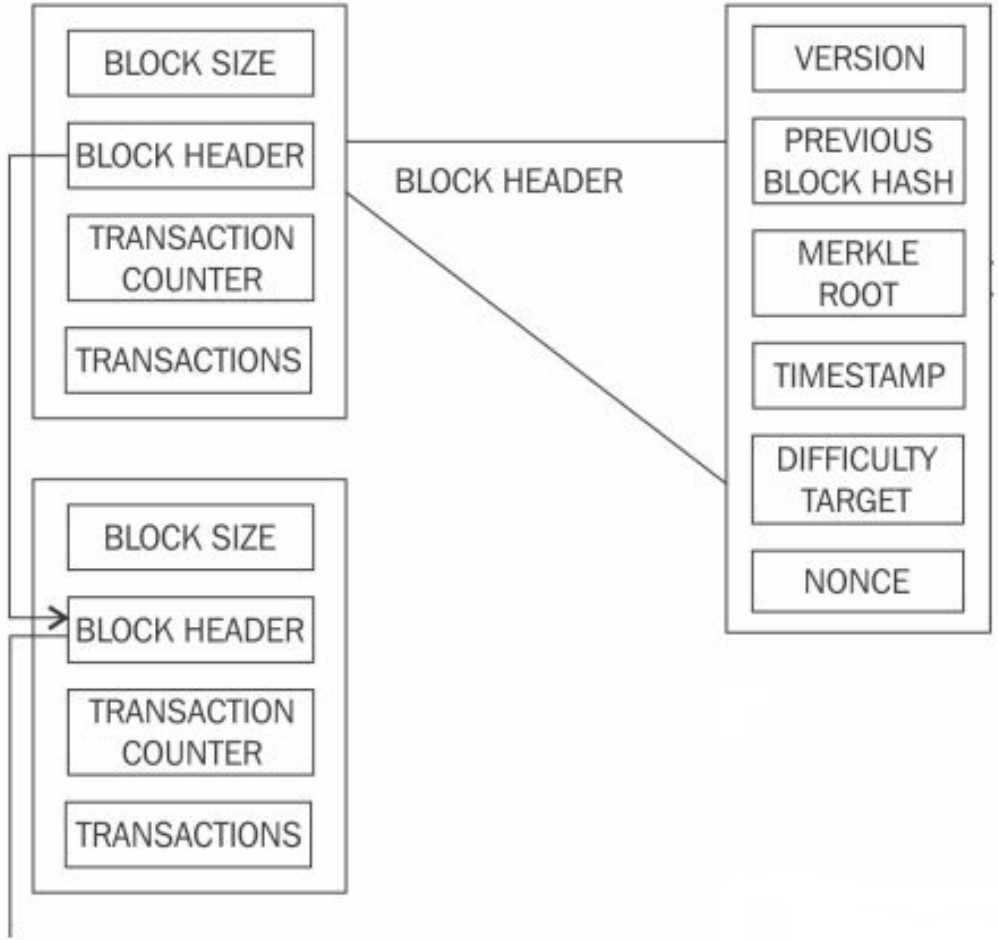
Bitcoin - Transação

- Carteiras
  - Mantem controle de privatekey e publickey
- Formas de conseguir o dinheiro
  - Gênesis block
  - Transferência
  - CoinBase
  - Gorjeta
- Input e Output
- Assinatura



Bitcoin - Rede

- Peer to peer
  - Cliente e Servidor
- TCP
- Inundação
- Broadcast/Multicast
- Funcionamento Geral


BLOCK SIZE
BLOCK HEADER
TRANSACTION COUNTER
TRANSACTIONS
BLOCK HEADER
VERSION
PREVIOUS BLOCK HASH
MERKLE ROOT
TIMESTAMP
DIFFICULTY TARGET
NONCE
BLOCK SIZE
BLOCK HEADER
TRANSACTION COUNTER
TRANSACTIONS

Blockchain

Universidade Federal do Espírito Santo

- Transparência
  - Apenas o header para verificar se uma transação foi validada
  - Não precisa saber quem foi o mineiro e nem onde ele está
- Privacidade
  - Ninguém sabe quem são donos das carteiras
- Escalabilidade
  - Quanto mais nós, maior a rede
  - Árvore de merkle
  - Mensagem de Inventário - na inundação antes de enviar a transação
  - Para entrar na rede os nós não fazem solicitação (Bitcoin)

Blockchain

- Concorrência e Consenso
  - Mineiros acham blocos válidos ao mesmo tempo e prevalece a da maior cadeia
- Tolerância a Falhas
  - Todos nós completos tem réplica
  - Sem ataque bizantino - Quorum

Estado da arte

Universidade Federal do Espírito Santo

- Mudanças na arquitetura para outras moedas
  - Scrypt : mais rápida e com mesmo nível segurança
  - Proof of Stake : menos energia.
  - Proof of Space : menos energia e melhorar os problemas do Proof of Work
  - Ethereum : uma nova abordagem

Proof of Stake

- PeerCoin - Proof of Stake
  - Diferente do Proof of Work
  - Ecologicamente correto
  - CoinAge : Dinheiro x Tempo
  - Transação especial : minerador para ele mesmo
  - Mais CoinAge gera mais facilidade

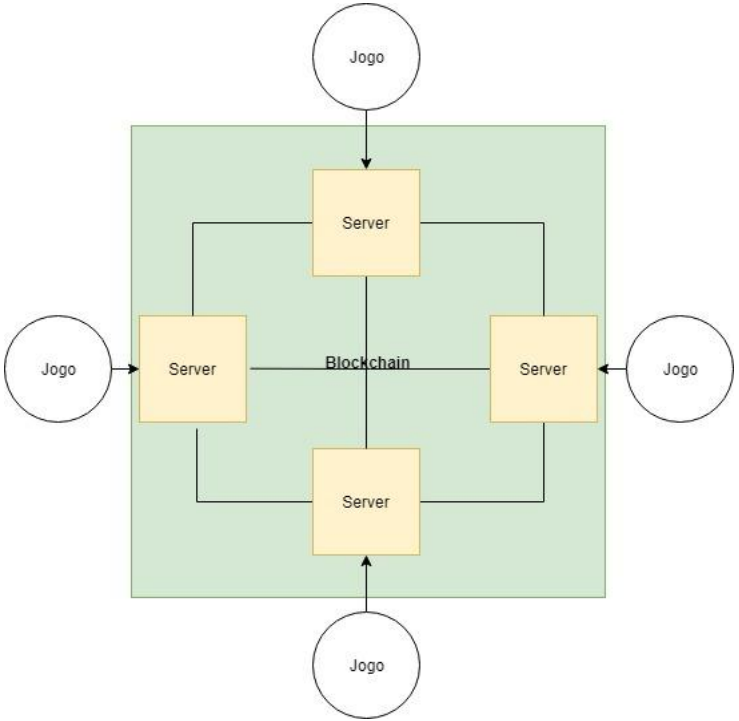
Projeto - Objetivos

- Implementação de um servidor em Blockchain
- Implementação de um jogo multiplayer online que usará o servidor
- Criação do protocolo de camada sessão específico
  - Regras de sincronização da troca de mensagens
  - Padronização das mensagens
- Prova de conceito
  - Mostrar a ordenação total dos eventos
  - Integridade dos dados armazenados

Universidade Federal do Espírito Santo

Servidor em Blockchain

- Para cada processo de jogo existirá um processo de servidor local.
- Processos de servidores Locais ficam responsáveis pela administração da Blockchain
- Conexões TCP com outros servidores formando a rede.
- Envio de comando/resultado do comando.



Universidade Federal do Espírito Santo

Jogo

- Estratégia
- Focado em administração de recursos
  - Ilhas, Ouro, Pedra, Madeira, Comida, População e Exército
- Principais ações do jogador:
  - Explorar Ilhas
  - Atacar Jogadores
  - Criar Exército
  - Alocar trabalhadores em recursos
- Patentes

Conclusões

- Considerações finais
  - Dinheiro e Proof of stake
- Estado atual
- Próximas etapas

Universidade Federal do Espírito Santo

Referências

S. Nakamoto, (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System,”, [Online]. Available: https://bitcoin.org/bitcoin.pdf.

S. King e S. Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake”, pp. 1-6, Agosto 2012.

I. Bashir, Mastering Blockchain, Birmingham, UK: Packt Publishing, Março 2017

F. Tschorsch, B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies”, IEEE Communications Surveys & Tutorials Journal, vol.18, no. 3, pp. 2084-2123, Agosto 2016.

Universidade Federal do Espírito Santo

Obrigado!

Histórico

Universidade Federal do Espírito Santo

- Anos 90 com cypherpunk
  - Moedas Digitais
- David Chaum com Digicash

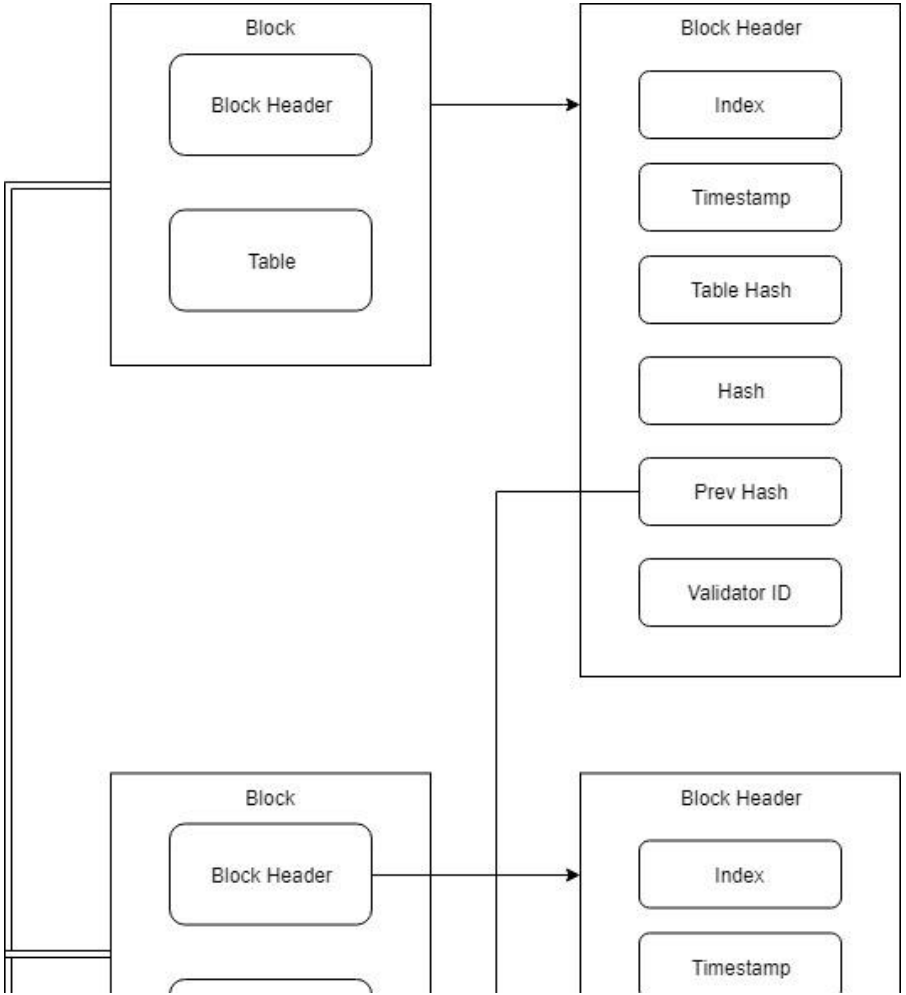
- Crise financeira e Bitcoin

Bitcoin

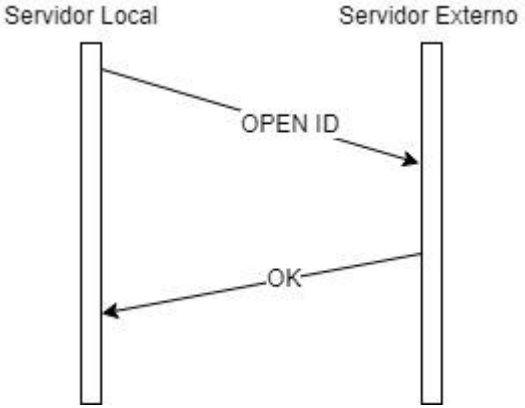
- Todos são o banco
  - Usuários comuns
  - Usuários completos - Mineradores
- Ledger distribuido
- Double spending
- Nascimento da Blockchain

Universidade Federal do Espírito Santo

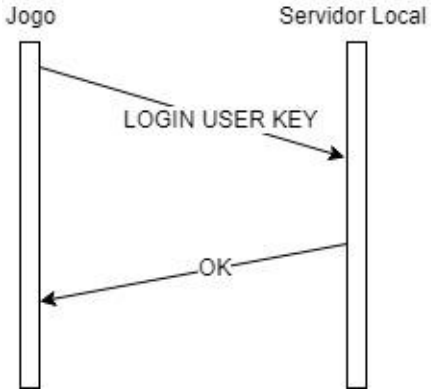
- O que armazenar
- Segurança baseada em confiança
- Analisar dados muito discrepantes



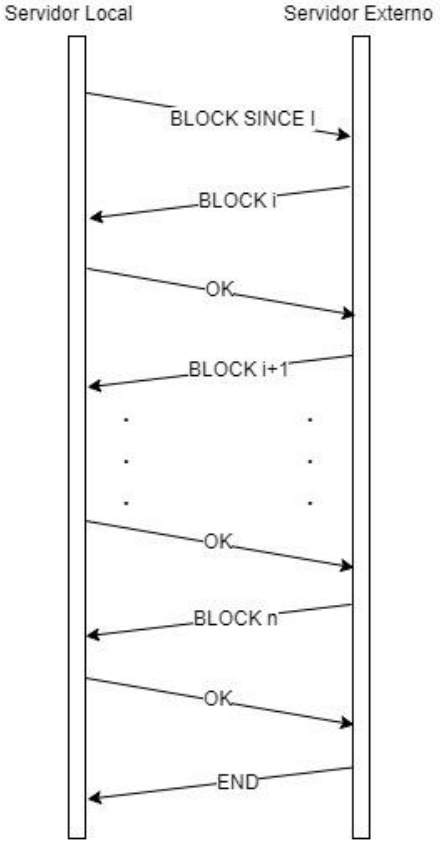
Estrutura dos Blocos



Inicialização de Servidor



Login de Usuário



Requerimento e
Envido de blocos

Exemplos de funcionamento

Universidade Federal do Espírito Santo

Protocolo

- Construído sobre o TCP
- Funcionamento de *stop-and-wait*
- Responsável pelas comunicações
  - Jogo - Servidor Local
  - Servidor Local - Demais Servidores da Blockchain
- Funções
  - Comunicar eventos de jogador
  - Requisição de blocos da Blockchain
  - Espalhamento de blocos validados