

**Ernane Rosa Martins  
(Organizador)**

# **A Abrangência da Ciência da Computação na Atualidade**

**Ernane Rosa Martins**

(Organizador)

# A Abrangência da Ciência da Computação na Atualidade

Atena Editora  
2019

2019 by Atena Editora  
Copyright © Atena Editora  
Copyright do Texto © 2019 Os Autores  
Copyright da Edição © 2019 Atena Editora  
Editora Executiva: Prof<sup>a</sup> Dr<sup>a</sup> Antonella Carvalho de Oliveira  
Diagramação: Karine de Lima  
Edição de Arte: Lorena Prestes  
Revisão: Os Autores

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores. Permitido o download da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

### **Conselho Editorial**

#### **Ciências Humanas e Sociais Aplicadas**

Prof. Dr. Álvaro Augusto de Borba Barreto – Universidade Federal de Pelotas  
Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná  
Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília  
Prof. Dr. Constantino Ribeiro de Oliveira Junior – Universidade Estadual de Ponta Grossa  
Prof<sup>a</sup> Dr<sup>a</sup> Cristina Gaio – Universidade de Lisboa  
Prof. Dr. Deyvison de Lima Oliveira – Universidade Federal de Rondônia  
Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná  
Prof<sup>a</sup> Dr<sup>a</sup> Ivone Goulart Lopes – Istituto Internazionele delle Figlie de Maria Ausiliatrice  
Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense  
Prof<sup>a</sup> Dr<sup>a</sup> Lina Maria Gonçalves – Universidade Federal do Tocantins  
Prof<sup>a</sup> Dr<sup>a</sup> Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Prof<sup>a</sup> Dr<sup>a</sup> Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa  
Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará  
Prof<sup>a</sup> Dr<sup>a</sup> Vanessa Bordin Viera – Universidade Federal de Campina Grande  
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

#### **Ciências Agrárias e Multidisciplinar**

Prof. Dr. Alan Mario Zuffo – Universidade Federal de Mato Grosso do Sul  
Prof. Dr. Alexandre Igor Azevedo Pereira – Instituto Federal Goiano  
Prof<sup>a</sup> Dr<sup>a</sup> Daiane Garabeli Trojan – Universidade Norte do Paraná  
Prof. Dr. Darllan Collins da Cunha e Silva – Universidade Estadual Paulista  
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul  
Prof<sup>a</sup> Dr<sup>a</sup> Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia  
Prof. Dr. Jorge González Aguilera – Universidade Federal de Mato Grosso do Sul  
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará  
Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas

#### **Ciências Biológicas e da Saúde**

Prof. Dr. Benedito Rodrigues da Silva Neto – Universidade Federal de Goiás  
Prof.<sup>a</sup> Dr.<sup>a</sup> Elane Schwinden Prudêncio – Universidade Federal de Santa Catarina  
Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria  
Prof. Dr. José Max Barbosa de Oliveira Junior – Universidade Federal do Oeste do Pará

Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Profª Drª Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão  
Profª Drª Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa  
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande

### **Ciências Exatas e da Terra e Engenharias**

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto  
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná  
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará  
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista

### **Conselho Técnico Científico**

Prof. Msc. Abrãao Carvalho Nogueira – Universidade Federal do Espírito Santo  
Prof. Dr. Adaylson Wagner Sousa de Vasconcelos – Ordem dos Advogados do Brasil/Seccional Paraíba  
Prof. Msc. André Flávio Gonçalves Silva – Universidade Federal do Maranhão  
Prof.ª Drª Andreza Lopes – Instituto de Pesquisa e Desenvolvimento Acadêmico  
Prof. Msc. Carlos Antônio dos Santos – Universidade Federal Rural do Rio de Janeiro  
Prof. Msc. Daniel da Silva Miranda – Universidade Federal do Pará  
Prof. Msc. Eliel Constantino da Silva – Universidade Estadual Paulista  
Prof.ª Msc. Jaqueline Oliveira Rezende – Universidade Federal de Uberlândia  
Prof. Msc. Leonardo Tullio – Universidade Estadual de Ponta Grossa  
Prof.ª Msc. Renata Luciane Polsaque Young Blood – UniSecal  
Prof. Dr. Welleson Feitosa Gazel – Universidade Paulista

<b>Dados Internacionais de Catalogação na Publicação (CIP) (eDOC BRASIL, Belo Horizonte/MG)</b>	
A161	A abrangência da ciência da computação na atualidade [recurso eletrônico] / Organizador Ernane Rosa Martins. – Ponta Grossa, PR: Atena Editora, 2019.  Formato: PDF Requisitos de sistema: Adobe Acrobat Reader Modo de acesso: World Wide Web Inclui bibliografia ISBN 978-85-7247-488-7 DOI 10.22533/at.ed.887190908  1. Computação – Pesquisa – Brasil. I. Martins, Ernane Rosa. CDD 004
<b>Elaborado por Maurício Amormino Júnior – CRB6/2422</b>	

Atena Editora  
Ponta Grossa – Paraná - Brasil  
[www.atenaeditora.com.br](http://www.atenaeditora.com.br)  
contato@atenaeditora.com.br

## APRESENTAÇÃO

A área da Ciência da Computação apresenta atualmente uma constante ascensão, seus profissionais estão sendo cada vez mais valorizados e requisitados pelas empresas, tornando-a mais importante, prestigiada e reconhecida. As empresas de todos os portes e setores necessitam de profissionais qualificados desta área, que apresentem potencial para promover inovação, desenvolvimento e eficiência.

A Ciência da Computação é uma área com amplas possibilidades de atuação, como por exemplo: a elaboração de programas e softwares, o gerenciamento de informações, a atuação acadêmica, a programação de aplicativos mobile ou ainda de forma autônoma. A abrangência da Ciência da Computação exige de seus profissionais conhecimentos diversos, tais como: novos idiomas, pensamento criativo, capacidade de comunicação e de negociação, além da necessidade de uma constante atualização de seus conhecimentos.

Dentro deste contexto, este livro aborda diversos assuntos importantes para os profissionais e estudantes desta área, tais como: API de localização da google, identificação de etiquetas RFID, ferramentas para recuperação de dados, ensino de computação, realidade virtual, interação humano computador, gestão do conhecimento, computação vestível, gerência de projetos, big data, mineração de dados, Internet das coisas, monitoramento do consumo de dados na Internet, pensamento computacional, análise de sentimentos, filtros ópticos, rede óptica elástica translúcida, algoritmo de roteamento, algoritmo de atribuição espectral, algoritmo de utilização de regeneradores e algoritmo genético.

Assim, certamente que os trabalhos apresentados nesta obra exemplificam um pouco a abrangência da área de Ciência da Computação na atualidade, permitindo aos leitores analisar e discutir os relevantes assuntos abordados. A cada autor, nossos agradecimentos por contribuir com esta obra, e aos leitores, desejo uma excelente leitura, repleta de boas reflexões.

Ernane Rosa Martins

## SUMÁRIO

<b>CAPÍTULO 1</b> .....	<b>1</b>
UMA ABORDAGEM SOBRE SISTEMA DE LOCALIZAÇÃO MOBILE	
Paulo Roberto Barbosa	
<b>DOI 10.22533/at.ed.8871909081</b>	
<b>CAPÍTULO 2</b> .....	<b>6</b>
UMA ABORDAGEM BIDINÂMICA PARA A IDENTIFICAÇÃO DE ETIQUETAS RFID	
Shalton Viana dos Santos	
Paulo André da S. Gonçalves	
<b>DOI 10.22533/at.ed.8871909082</b>	
<b>CAPÍTULO 3</b> .....	<b>23</b>
TESTE DE FERRAMENTAS DE RECUPERAÇÃO DE IMAGENS PARA SISTEMAS DE ARQUIVOS EXT3 E EXT4	
Diego Vinícius Natividade	
<b>DOI 10.22533/at.ed.8871909083</b>	
<b>CAPÍTULO 4</b> .....	<b>34</b>
REDIMENSIONAMENTO DO ENSINO DA COMPUTAÇÃO NA EDUCAÇÃO BÁSICA: O PENSAMENTO COMPUTACIONAL, O UNIVERSO E A CULTURA DIGITAL	
Melquisedec Sampaio Leite	
Sônia Regina Fortes da Silva	
<b>DOI 10.22533/at.ed.8871909084</b>	
<b>CAPÍTULO 5</b> .....	<b>47</b>
REALIDADE VIRTUAL, UTILIZANDO DAS MELHORES PRÁTICAS DA INTERAÇÃO HUMANO COMPUTADOR	
Bruno Moreira Batista	
Guiliano Rangel Alves	
Hellen Corrêa da Silva	
Rhogério Correia de Souza Araújo	
<b>DOI 10.22533/at.ed.8871909085</b>	
<b>CAPÍTULO 6</b> .....	<b>52</b>
ORGANIZAÇÃO DO CONHECIMENTO PARA A MEMÓRIA EMPRESARIAL: UM RELATO TÉCNICO SOBRE A EXPERIÊNCIA DO SEBRAE/RJ	
Leandro Pacheco de Melo	
<b>DOI 10.22533/at.ed.8871909086</b>	
<b>CAPÍTULO 7</b> .....	<b>65</b>
GERÊNCIA DE PROJETOS EM COMPUTAÇÃO VESTÍVEL: DIRETRIZES PARA O DESENVOLVIMENTO DE PRODUTOS VESTÍVEIS INTELIGENTES	
Renan Gomes Barreto	
Lucas Oliveira Costa Aversari	
Renata Gomes Barreto	
Gabriela Ferreira Marinho Barreto	
<b>DOI 10.22533/at.ed.8871909087</b>	

<b>CAPÍTULO 8</b> .....	<b>76</b>
EXPLORING <i>BIG DATA</i> CONTENT AND INFORMATION METRICS: INTERSECTIONS AND ANALYSIS TO SUPPORT DECISION-MAKING	
Rafael Barcellos Gomes Vânia Lisboa da Silveira Guedes	
<b>DOI 10.22533/at.ed.8871909088</b>	
<b>CAPÍTULO 9</b> .....	<b>92</b>
DEMOCHAIN - FRAMEWORK DESTINADO A CRIAÇÃO DE REDES BLOCKCHAIN HÍBRIDAS PARA DISPOSITIVOS IOT	
Lorenzo W. Freitas Carlos Oberdan Rolim	
<b>DOI 10.22533/at.ed.8871909089</b>	
<b>CAPÍTULO 10</b> .....	<b>107</b>
CONSUMO DO TRÁFEGO DE DADOS EM APLICAÇÕES DE VÍDEO SOB DEMANDA- YOUTUBE E NETFLIX	
Patricia Emilly Nóbrega da Silva Éwerton Rômulo Silva Castro	
<b>DOI 10.22533/at.ed.88719090810</b>	
<b>CAPÍTULO 11</b> .....	<b>112</b>
COMPUTAÇÃO NA ESCOLA: ABORDAGEM DESPLUGADA NA EDUCAÇÃO BÁSICA	
Christian Puhmann Brackmann Marcos Román-González Rafael Marimon Boucinha Dante Augusto Couto Barone Ana Casali Flávia Pereira da Silva	
<b>DOI 10.22533/at.ed.88719090811</b>	
<b>CAPÍTULO 12</b> .....	<b>128</b>
COLETA DE DADOS E ANÁLISE DE SENTIMENTOS NAS REDE SOCIAIS ON LINE	
Maurilio Alves Martins da Costa Bruna Emidia de Assis Almeida Fraga	
<b>DOI 10.22533/at.ed.88719090812</b>	
<b>CAPÍTULO 13</b> .....	<b>137</b>
ANÁLISE DO IMPACTO DO CASCATEAMENTO DE FILTROS ÓPTICOS EM UM CENÁRIO DE REDES ÓPTICAS ELÁSTICAS	
Gabriela Sobreira Dias de Carvalho William Silva dos Santos Lucas Oliveira de Figueiredo Helder Alves Pereira	
<b>DOI 10.22533/at.ed.88719090813</b>	

<b>CAPÍTULO 14</b> .....	<b>143</b>
ANÁLISE DE REDE ÓPTICA ELÁSTICA TRANSLÚCIDA CONSIDERANDO DIFERENTES ALGORITMOS DE ROTEAMENTO	
Arthur Hendricks Mendes de Oliveira	
William Silva dos Santos	
Helder Alves Pereira	
Raul Camelo de Andrade Almeida Júnior	
<b>DOI 10.22533/at.ed.88719090814</b>	
<b>CAPÍTULO 15</b> .....	<b>149</b>
ANÁLISE DE REDE ÓPTICA ELÁSTICA TRANSLÚCIDA CONSIDERANDO ALGORITMOS DE ATRIBUIÇÃO ESPECTRAL	
Arthur Hendricks Mendes de Oliveira	
William Silva dos Santos	
Helder Alves Pereira	
Raul Camelo de Andrade Almeida Júnior	
<b>DOI 10.22533/at.ed.88719090815</b>	
<b>CAPÍTULO 16</b> .....	<b>155</b>
A NEW MULTI OBJECTIVE APPROACH FOR OPTIMIZING P-MEDIAN MODELING IN SCHOOL ALLOCATION USING GENETIC ALGORITHM	
Clahildek Matos Xavier	
Marly Guimarães Fernandes Costa	
Cícero Ferreira Fernandes Costa Filho	
<b>DOI 10.22533/at.ed.88719090816</b>	
<b>SOBRE O ORGANIZADOR</b> .....	<b>168</b>
<b>ÍNDICE REMISSIVO</b> .....	<b>169</b>

## DEMOCHAIN - FRAMEWORK DESTINADO A CRIAÇÃO DE REDES BLOCKCHAIN HÍBRIDAS PARA DISPOSITIVOS IOT

### Lorenzo W. Freitas

Departamento de Engenharias e Ciência da  
Computação  
Universidade Regional Integrada do Alto Uruguai  
e das Missões – Santo Ângelo, RS – Brazil  
lorenzofreitas@aluno.santoangelo.uri.br

### Carlos Oberdan Rolim

Departamento de Engenharias e Ciência da  
Computação  
Universidade Regional Integrada do Alto Uruguai  
e das Missões – Santo Ângelo, RS – Brazil  
ober@san.uri.br

**RESUMO:** O uso da tecnologia Blockchain no contexto da IoT (Internet of Things) está sendo cada vez mais explorado pela comunidade acadêmica e a indústria. No entanto, essa implantação pode ser custosa ou inviável pois a Blockchain pode exigir recursos computacionais que não são obtidos facilmente com o uso de dispositivos IoT. Assim, esse trabalho apresenta o framework Demochain cuja função é auxiliar no desenvolvimento de plataformas blockchains híbridas no contexto de IoT.

**ABSTRACT:** The use of Blockchain technology in the context of Internet of Things (IoT) is increasingly being explored by the academic community and industry. However, such deployment may be costly or impracticable

since Blockchain may require computational resources that are not easily obtained with the use of IoT devices. Thus, this work presents the Demochain framework whose function is to assist in the development of hybrid blockchains platforms in the context of IoT.

### 1 | INTRODUÇÃO

Uma importante área de pesquisa na Computação que está apresentando um rápido crescimento é a Internet das Coisas (IoT). Segundo Gartner (2017), o gasto total em dispositivos e serviços de IoT atingiu quase US \$ 2 trilhões em 2017, e haverá mais de 20 bilhões de “coisas” conectadas em todo o mundo até 2020.

Entretanto, apesar de possuir a natureza distribuída, a maioria das soluções IoT ainda dependem de arquiteturas que seguem o modelo cliente servidor. Embora esse modelo arquitetural possa funcionar hoje, o crescimento da IoT sugere que novas arquiteturas deverão ser propostas no futuro [Caramés e Lamas 2017]. Uma alternativa que vêm sendo explorada pela comunidade acadêmica e a indústria é o emprego de blockchains devido a sua, capacidade de manter os registros imutáveis sem perder segurança, com algoritmos que tratam nodos maliciosos.

Com esse cenário e a falta de padronização dos dispositivos IoT devido a seus diferentes objetivos existe uma dificuldade na implementação e modelagem de uma rede blockchain personalizada para dispositivos IoT [Conoscenti et al, 2016]. Assim, o presente trabalho apresenta o Demochain, um framework voltado para a criação de redes blockchain híbridas para dispositivos IoT. Um dos diferenciais do Demochain é a sua capacidade de oferecer opções para mesclar e combinar diferentes níveis na arquitetura e também funcionalidades da blockchain pura (totalmente descentralizada), variando seus protocolos e criptografias, construindo assim, uma blockchain híbrida. Além disso, pode-se ressaltar que a maior contribuição do Demochain é a possibilidade de facilitar a modelagem e a prototipação de novas redes blockchain em ambientes variados.

## 2 | FRAMEWORK PROPOSTO

O framework construído foi chamado de Demochain e foi pensado para diminuir a complexidade na conexão dos dispositivos. Portanto, vários conceitos utilizados em blockchains tradicionais foram simplificados. Ele foi desenvolvido com a linguagem Go [Google 2009] e foi utilizada uma abordagem de orientação a objetos com o padrão Decorator em sua implementação [Schmager, Frank 2010]. A arquitetura que foi implementada é multicamadas, baseada no trabalho de Li e Zhang (2017). Nessa arquitetura, cada nodo na rede pode assumir dois papéis: ser um nodo centralizador (Edge Node), que serve para controlar o acesso dos nodos abaixo na camada, ou ser um nodo de alto nível (High-Level Node), também chamado de nodo filho, onde são adicionado blocos e executado o protocolo de consenso.

Com isso tem-se um modelo descentralizado com alguns níveis de centralização, porém não totalmente distribuído. A Figura 1 apresenta a arquitetura do Demochain.

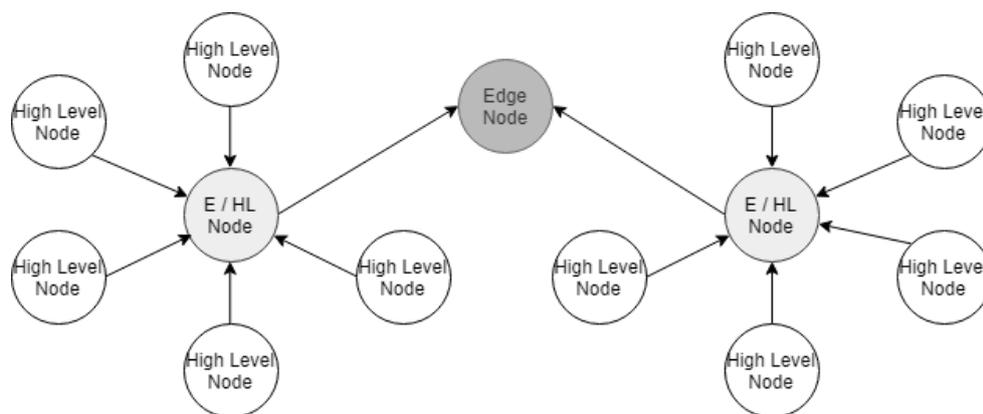


Figura 1. Arquitetura implementada.

Ao escolher o esquema de criptografia para o framework, foi levado em consideração não apenas a segurança fornecida de acordo com a carga computacional, mas também o consumo de energia, fazendo um trade-off entre segurança e consumo. Foram implementados quatro algoritmos de criptografia assimétrica: RSA, Ed25519,

Secp256k1 e ECDSA. A identificação dos nodos ocorre utilizando a pilha TCP em sua forma tradicional. Portanto, um mesmo dispositivo pode estar rodando várias instâncias do Demochain, desde que em portas distintas.

No Demochain a blockchain é replicada para todos os nós. Entretanto o diferencial deste framework é que a execução do consenso é por nível. Protocolo consenso consiste em um mecanismo que determina as condições a serem alcançadas para concluir que um acordo foi alcançado em relação às validações dos blocos para ser adicionado ao blockchain [Zheng et al. 2017]. Foram implementados três protocolos de consenso: PoW (Proof of Work), PoS (Proof of Stake) e PBFT (Practical Byzantine Fault Tolerance).

## 2.1 Proof of Work (PoW)

Algoritmos de consenso PoW, ou Prova de Trabalho baseiam-se no fato de que um nó malicioso tem que executar muito trabalho do ponto de vista computacional para atacar a rede, e por isso, é menos provável que ele vá querer atacar. O trabalho realizado geralmente envolve fazer alguns cálculos até que uma solução seja encontrada, um processo que é comumente conhecido como mineração. No caso da blockchain do Bitcoin, a mineração consiste em encontrar um número aleatório, chamado de número nonce que fará o hash SHA256 do cabeçalho do bloco para ter no início certo número de zeros. Portanto, os mineradores têm que demonstrar que eles realizaram certa quantidade de trabalho para resolver o problema. Uma vez resolvido o problema, é realmente fácil para outros nodos verificar se a resposta obtida é válida. No entanto, este processo de mineração faz a blockchain ineficiente em taxa de transferência, escalabilidade [M. Vukolić 2015], e também em termos de consumo de energia, o que não é desejável em uma IoT rede.

## 2.2 Proof of Stake (PoS)

PoS ou Prova de Participação é um mecanismo de consenso que requer menos recursos computacionais e potência do que PoW [BitFury Group 2015], por isso consome menos energia. Em uma blockchain baseado em PoS, assume-se que as entidades com mais participação na rede são os menos interessados em atacá-lo. Assim, os nodos precisam provar periodicamente que eles possuem certa quantidade de participação na rede (por exemplo, moeda ou quantidade de dados coletados a partir de sensores). Podemos comparar o PoS há uma loteria, onde é realizado um sorteio e escolhido um nodo que irá dizer se o bloco que está sendo enviado pela rede é válido ou não, por consequência, o nodo que tiver mais participação recebe mais “fichas” neste sorteio, e tem mais chances de validar o bloco. O nodo que realiza o sorteio pode ou não ser pré-definido.

## 2.3 Practical Byzantine Fault Tolerance (PBFT)

PBFT [M. Castro e B. Liskov 1999] ou Tolerância de Falhas Bizantinas Prática é um algoritmo de consenso que resolve o problema dos generais bizantinos, recomendado para ambientes assíncronos. PBFT assume que menos de um terço dos nós são maliciosos. Para cada bloco a ser adicionado à cadeia, um líder é selecionado para ser encarregado de encomendar a transação. Essa seleção deve ser apoiada por pelo menos 2/3 de todos os nós, que devem ser conhecidos pela rede.

## 2.4 Implementação do consenso

No Demochain o PoW funciona da maneira clássica, é imposta uma dificuldade e é realizada uma tentativa aleatória de encontrar uma Hash utilizando SHA256 que comece com o número de zeros da dificuldade. Na figura 2 temos um exemplo de Hash's geradas de acordo com a dificuldade do PoW, onde é possível verificar o número de zeros no início da Hash.

### Dificuldade 1

012b46ed9cf86cab3fd08708ec3ee868528044e87931b2d00dd21c4fbae5d919

### Dificuldade 2

001ca89c82993d99e3477a11c08687caa5c8fb6760cd93ef25de45dc2746e8b4

### Dificuldade 3

000ca89c82993d99e3477a11c08687caa5c8fb6760cd93ef25de45dc2746e8b4

Figura 2. Dificuldade do Proof of Work.

Como o PoW processa os blocos apenas com os próprios recursos, sem depender da aprovação dos demais nodos, no Demochain utilizando o PoW é possível realizar a validação e geração de novos blocos independente da conexão com o seu Edge Node, portanto mesmo um dispositivo estando desconectado da rede, ao se reconectar ele consegue sincronizar os blocos validados, isso se ele estiver executando a mesma instância, pois esses blocos ficam armazenados em memória, entretanto caso sua execução seja interrompida e ele não estiver conectado na rede os blocos validados são perdidos, já que foi implementado apenas um arquivo físico de Blockchain que mantém o conteúdo atualizado conforme o conteúdo atual que está circulando na rede. Uma implementação com dois arquivos de Blockchain, um atualizado conforme a rede e outro com o conteúdo "local" é uma possível melhoria, conforme é sugerido em [Liang et al. 2017].

A razão dessa funcionalidade é dar liberdade ao desenvolvedor dizer quando deve ser o envio dos blocos, não precisando ser necessariamente logo após a validação dos mesmos, o que em um cenário de concorrência de criptomoedas não faz sentido, mas em redes privadas pode fazer, dependendo dos objetivos de cada um.

A implementação proposta para o PoS é baseada no trabalho de Dan Larimer

(2014), também chamado de DpoS (Delegate Proof of Stake). A diferença do DPOs para o PoS “clássico” é que são delegados representantes para a realização do sorteio para a governança da rede com critérios predeterminados. Nesse caso a cada bloco gerado será solicitado um sorteio ao Edge Node, que irá direcionar o bloco ao vencedor para realizar a validação. Esse sorteio acontece no escopo de apenas um nível de rede, porém após ser validado o bloco é passado aos demais níveis. A figura 3 demonstra o funcionamento do PoS.

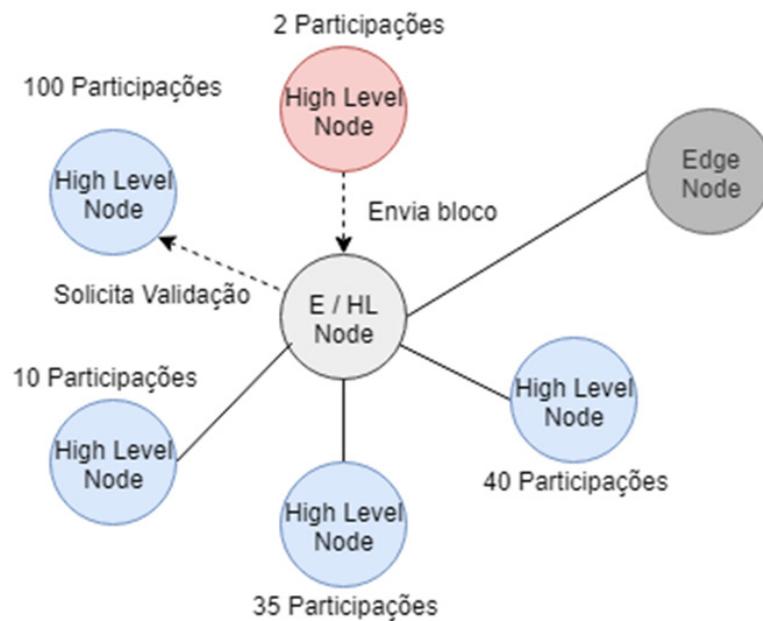


Figura 3. Funcionamento do PoS.

A implementação proposta para o PBFT também tem alterações. Assim como no PoS, toda validação deverá ser solicitado ao Edge Node da rede, porém ele irá enviar o bloco para todos os nodos do mesmo nível, ou seja, todos os High Level Nodes. Após o mesmo irá contabilizar quem aprovou e quem desaprovou o bloco. Se pelo menos 2/3 de seus High Level Nodes aprovarem o bloco, então é decretado que o bloco é válido. Assim como o PoS o protocolo executa em um nível da rede, porém ao ser validado o bloco é passado aos demais níveis. A figura 4 demonstra o funcionamento do PBFT.

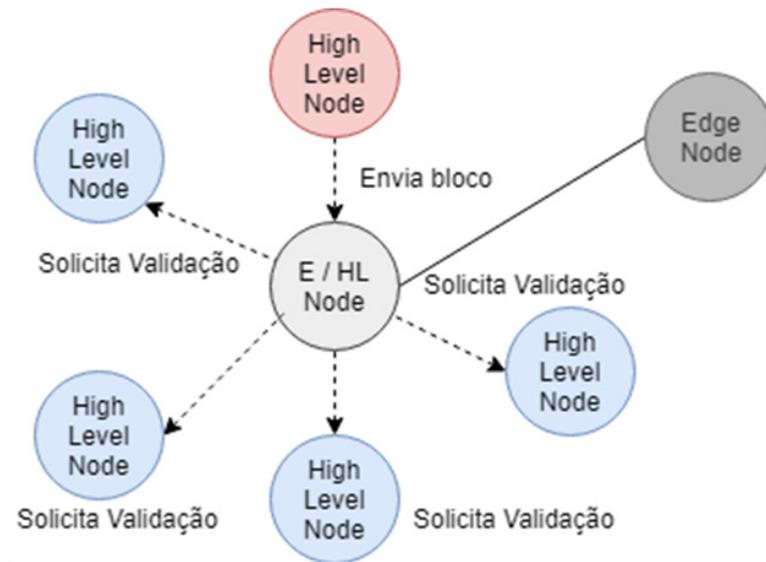


Figura 4. Funcionamento do PBFT.

Uma observação importante é que como os protocolos PoS e PBFT irão executar em apenas um nível da rede, uma preocupação que o desenvolvedor deve ter é a divisão dos Edge Nodes, pois quanto menos High Level Nodes vinculados a ele maior a chance de um nó intruso realizar uma ação maliciosa, pois são protocolos probabilísticos.

Será suportado apenas um protocolo de consenso rodando em todos níveis de rede. Uma possível melhoria seria permitir cada High-Level Layer estar rodando um tipo de protocolo de consenso, ou mesmo não ter nenhum implementado, podendo apenas estar inserindo os blocos e os compartilhando sem protocolo de consenso, entretanto isso exigiria um esquema mais complexo de armazenamento e uma compressão dos dados validados de cada nível da rede, fazendo com que cada High-Level Layer tivesse uma blockchain diferente da outra em seu formato.

## 2.5 Mensagens

A troca de mensagens se dá de maneira simples, podendo ter um ou dois fluxos em cada conexão, um de recebimento e outro para envio. Caso o desenvolvedor defina uma rede não permissionada sempre será aberto os fluxos de recebimento e de envio, porém é possível definir também uma rede permissionada. Isso permite com que o desenvolvedor defina nodos apenas de backup das informações para eventuais falhas. Na figura 5 temos um exemplo ilustrativo de uma rede permissionada com o Demochain.

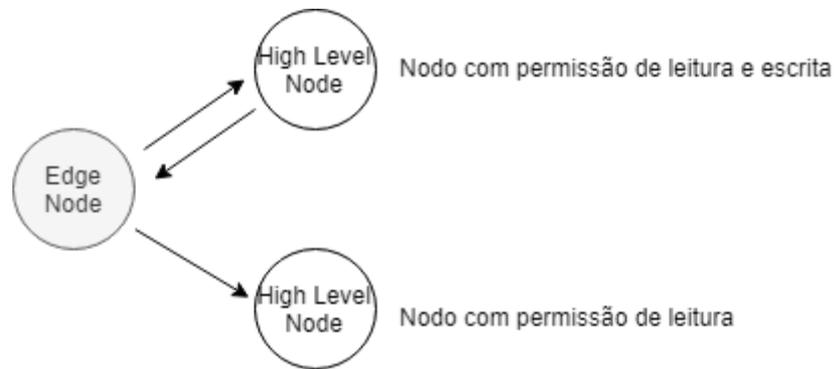


Figura 5. Rede permissionada com nodo de leitura.

Em uma primeira versão o demochain envia a Blockchain por inteira a cada mensagem trocada, o que a um longo prazo pode gerar gargalos na rede. Um controle mais complexo de troca de mensagens não foi implementado.

## 2.6 Estrutura dos blocos

A estrutura de blocos utilizadas pelo Demochain possui semelhanças e diferenças com as estruturas tradicionais utilizadas em criptomoedas. É importante ressaltar que normalmente em criptomoedas um bloco é formado de transações, sendo que toda transação tem um “recipient”, podendo ou não ter um “sender”. No Bitcoin por exemplo, em uma transação comum temos um “sender” que envia valor para o “recipient”, porém quando um novo bloco é minerado é chamado de “Coinbase”, pois não tem um “sender”. Como esse framework não é voltado para criptomoedas foi utilizado um conceito mais simples somente com blocos, pois a princípio a validação que será aplicada nos dados coletados não deverá ser passada para outros Nodos. Abaixo temos a estrutura de bloco que o Demochain implementa:

- Index: Índice sequencial único que é incrementado a cada nova adição de blocos na blockchain.
- Timestamp: Carimbo de data e hora do momento da adição do bloco.
- Data: Dados que foram validados.
- Hash: Hash gerada para o bloco.
- PrevHash: Hash do bloco anterior.
- Consensus: Consenso utilizado para a validação do bloco.
- Nonce: Número Nonce é utilizado apenas para o consenso Proof of Work.
- Target: Target do nodo onde foi validado o bloco. Podemos dizer que corresponde ao “dono” do bloco.

## 2.7 Armazenamento

Para o armazenamento será gravado em um arquivo que servirá para manter os

blocos já validados por todos os nodos. O arquivo será gravado com extensão “.bc” com um Json não indentado com todos os dados da blockchain. Na figura 6 temos um exemplo de um bloco gerado com a estrutura de bloco do Demochain, e na figura 7 temos o mesmo bloco armazenado no arquivo “.bc”.

```
[
  {
    "Index":0,
    "Timestamp":"2018-11-17 19:02:25.834476 -0200 -02 m=+3.635126501",
    "Data":"0",
    "Hash":"f1534392279bddbf9d43dde8701cb5be14b82f76ec6607bf8d6ad557f60f304e",
    "PrevHash":"",
    "Consensus":{
      "TypeConsensus":1,
      "Difficulty":3
    },
    "Nonce":"",
    "Target":"QmbiS1uqyVvXzV2pYdife8vJeZZRtW4TQiNEP4Dj1ckNiG"
  }
]
```

Figura 6. Bloco json indentado.

```
[{"Index":0,"Timestamp":"2018-11-17 19:02:25.834476 -0200 -02 m=+3.635126501","Data":"0","Hash":"f1534392279bddbf9d43dde8701cb5be14b82f76ec6607bf8d6ad557f60f304e","PrevHash":"","Consensus":{"TypeConsensus":1,"Difficulty":3},"Nonce":"","Target":"QmbiS1uqyVvXzV2pYdife8vJeZZRtW4TQiNEP4Dj1ckNiG"}]
```

Figura 7. Bloco json não indentado.

A seguir serão apresentados os resultados de simulações de uso do framework com o objetivo de demonstrar a performance de cada protocolo de consenso sobre um mesmo desenho de arquitetura.

### 3 | RESULTADOS

Todos os códigos bem como testes realizados estão disponíveis em Freitas (2018). Os resultados foram obtidos com o uso de equipamentos para simular um ambiente IoT. A Tabela 1 demonstra a configuração do hardware utilizado para os testes do Demochain.

Código	Descrição	Processador	Memória RAM	Sistema Operacional
H01	Notebook	Intel Core i5 2x 2.20 GHz	4 Gigabytes	Windows 10 Pro
H02	Raspberry Pi	BCM2835	512 Megabytes	Raspbian Stretch Lite

Tabela 1. Tabela de hardware para experimentação.

Para testar o desempenho do framework foi utilizado as métricas descritas por S.

Angelis (2017), que são comumente usadas para medir aplicações descentralizadas. A Tabela 2 descreve as métricas utilizadas.

<b>Código</b>	<b>Nome</b>	<b>Descrição</b>
M01	Taxa de validação (Throughput)	Mede o número de blocos gerados com sucesso por segundo.
M02	Latência (Latency)	Mede o tempo entre envio e confirmação do bloco relativo em milissegundos.
M03	Escalabilidade (Scalability)	Média em milissegundos das mudanças de latência, conforme é aumentado o número de nodos na rede.
M04	Tempo Total (Total Time)	Mede o tempo total em minutos de execução do programa de teste.

Tabela 2. Tabela de métricas para experimentação.

A fim de simular dados reais de ambientes IoT foi utilizado um dataset público [Ortiz, J. e Gottschlich, N. 2016]. A Tabela 3 descreve o dataset utilizado.

<b>Código</b>	<b>Descrição</b>	<b>Referência</b>
D01	Dados de consumo de eletricidade doméstica com 60.640 medições coletadas entre janeiro de 2007 e junho de 2007 (6 meses).	[Ortiz, J. e Gottschlich, N. 2016]

Tabela 3. Tabela de datasets para experimentação.

Para testar o framework foi definido cenários de experimentação, no qual para cada cenário foi criado um aplicativo de testes que importa o Demochain. Os cenários possuem dois objetivos principais, demonstrar exemplos de como utilizar o framework e analisar o seu desempenho. Nas subseções seguintes está descrito cada cenário, seu objetivo e seus resultados.

### 3.1 Cenário 1

O Objetivo deste cenário é comparar desempenho de geração de blocos, utilizando as métrica M01 e M04. Para isso foi implementado um nodo único para testar o protocolo de consenso Proof of Work com diferentes níveis de dificuldade utilizado o dataset D01 como entrada de dados. A cada execução do Proof of Work foi incrementada a sua dificuldade, variando de 1 a 5. A Tabela 4 demonstra os resultados obtidos deste cenário, e as figuras 8 e 9 demonstram os resultados retirados da tabela 4

	Taxa de validação (blocos p/ segundo)	Tempo Total (minutos)
<b>PoW 1</b>	10 Blocos	434 min
<b>PoW 2</b>	8 Blocos	543 min
<b>PoW 3</b>	5 Blocos	869 min
<b>PoW 4</b>	3 Blocos	1.448 min
<b>PoW 5</b>	1 Bloco	4.344 min

Tabela 4. Resultados da validação do PoW aplicando as métricas M01 e M04.

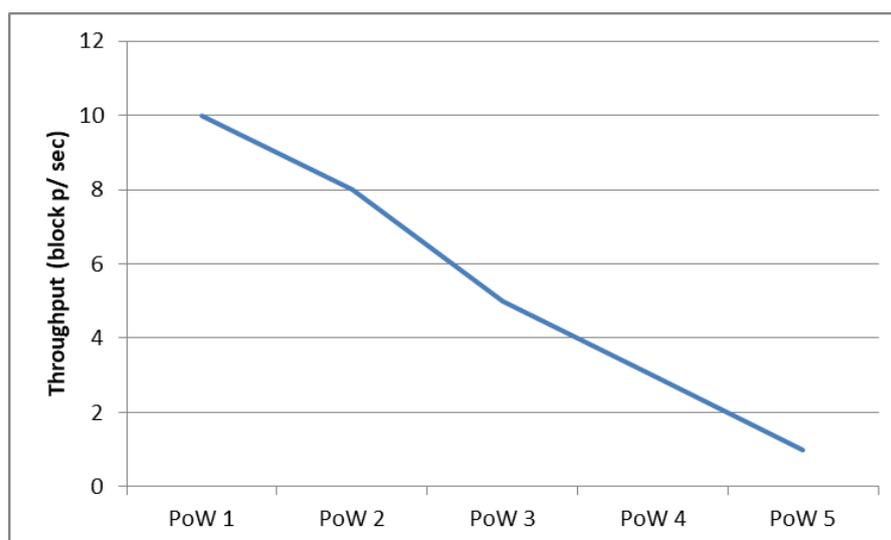


Figura 8. Aplicação da métrica M01 sobre o PoW.

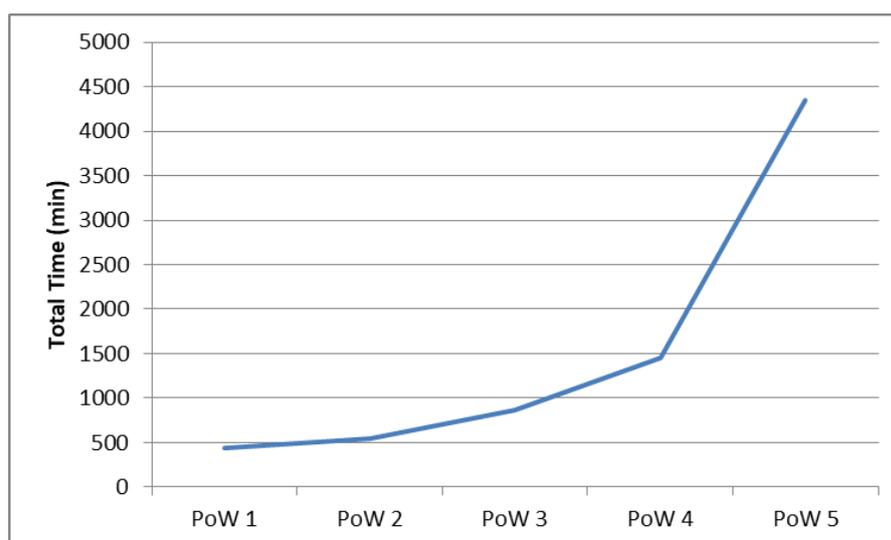


Figura 9. Aplicação da métrica M04 sobre o PoW.

Os resultados obtidos neste cenário demonstram que o Proof of Work tem um desempenho razoável na validação dos blocos até a dificuldade 3, portanto é uma boa alternativa para os nodos que não ficam conectados a todo momento, pois o seu

processamento não depende da rede.

### 3.2 Cenário 2

O objetivo deste cenário é comparar desempenho de cada protocolo de consenso, utilizando as métricas M01, M02, M03 e M04. Para isso foi implementado um rede com até 15 nodos dispostos nos hardwares H01 e H02, utilizando a criptografia RSA, com o dataset D01 como entrada de dados, sendo que foi utilizado o Proof of Work apenas com dificuldade 3. Todos os nodos estavam rodando sobre um mesmo nível de rede, ou seja, todos respondiam para o mesmo Edge Node.

A Tabela 5 apresenta a aplicação da métrica M01 sobre os três protocolos de consenso, considerando a variação do número de nodos na rede, e a figura 10 demonstra com um gráfico de linhas os resultados desta tabela.

	PoW 3	PoS	PBFT
<b>1 Nodo</b>	5 blocos	25 blocos	20 blocos
<b>2 Nodos</b>	4,7 blocos	21 blocos	15,7 blocos
<b>5 Nodos</b>	4,2 blocos	15 blocos	11 blocos
<b>10 Nodos</b>	3,5 blocos	10,5 blocos	6,5 blocos
<b>15 Nodos</b>	2,5 blocos	6,5 blocos	2,6 blocos

Tabela 5. Taxa de validação (Throughput) em blocos p/ Segundo.

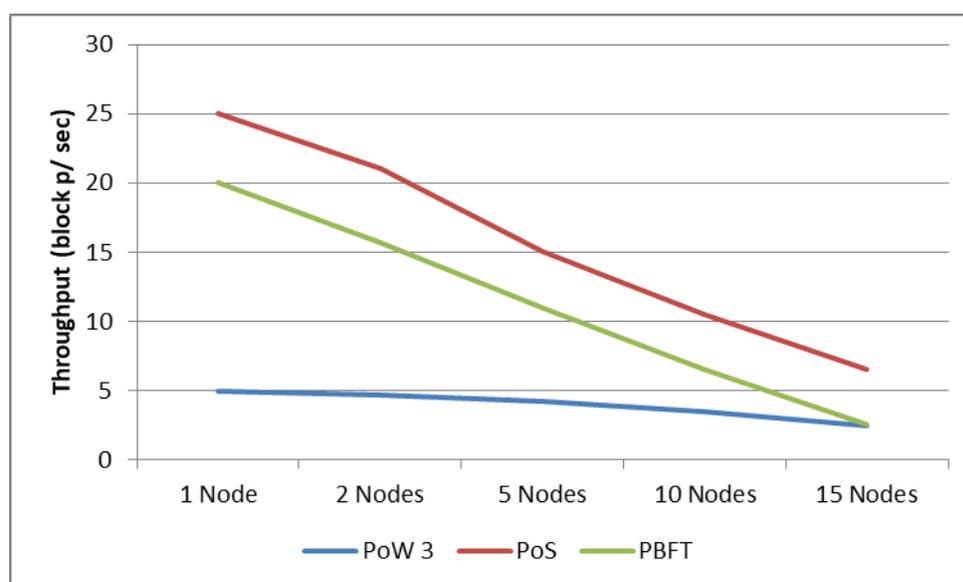


Figura 10. Aplicação da métrica M01.

A Tabela 6 apresenta a aplicação da métrica M02 sobre os três protocolos de consenso, considerando a variação do número de nodos na rede, e a figura 11 demonstra com um gráfico de linhas os resultados desta tabela.

	PoW 3	PoS	PBFT
<b>1 Nodo</b>	200 ms	40 ms	50 ms
<b>2 Nodos</b>	212 ms	47 ms	64 ms
<b>5 Nodos</b>	238 ms	66 ms	90 ms
<b>10 Nodos</b>	285 ms	96 ms	154 ms
<b>15 Nodos</b>	400 ms	153 ms	384 ms

Tabela 6. Latência (Latency) em milisegundos.

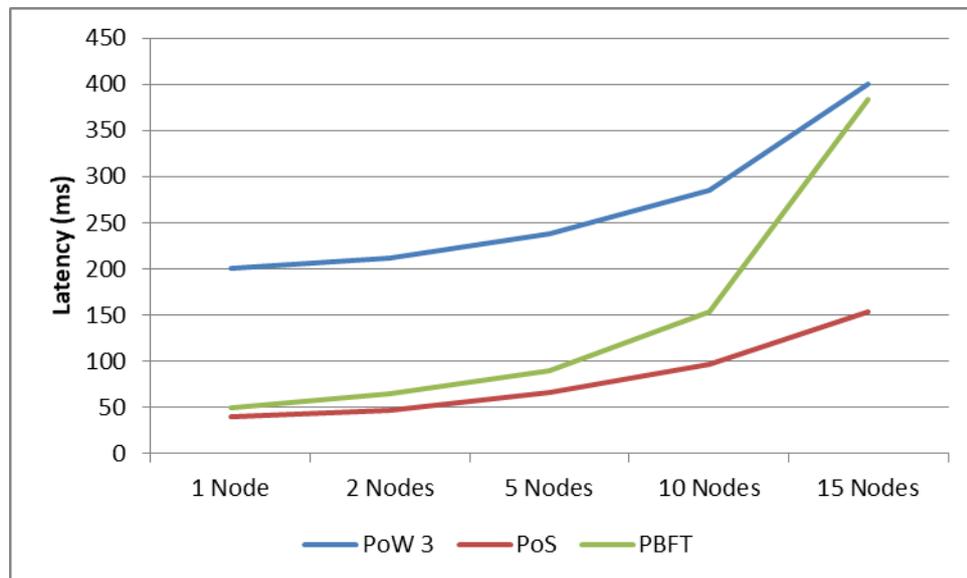


Figura 11. Aplicação da métrica M02.

A Tabela 7 apresenta a aplicação da métrica M03 sobre os três protocolos de consenso, considerando a variação do número de nós na rede, e a figura 12 demonstra com um gráfico de barras os resultados desta tabela.

	PoW 3	PoS	PBFT
<b>Média de Latência p/ Nodo</b>	13,33 ms	7,53 ms	22,26 ms

Tabela 7. Escalabilidade (milisegundos).

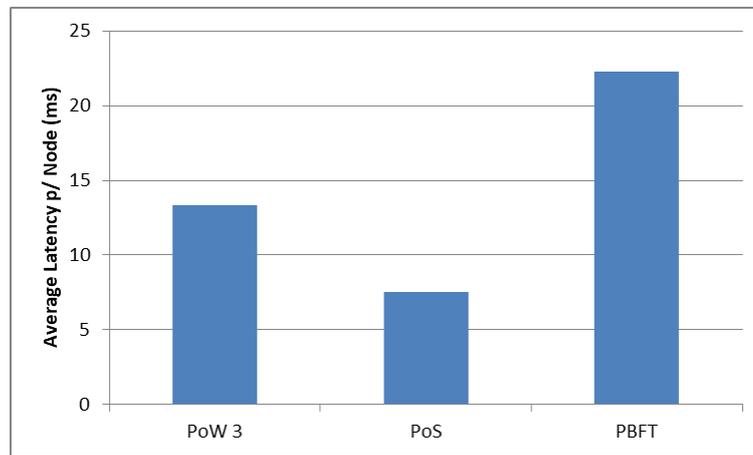


Figura 12. Aplicação da métrica M03.

A Tabela 8 apresenta a aplicação da métrica M04 sobre os três protocolos de consenso, considerando a variação do número de nodos na rede, e a figura 13 demonstra com um gráfico de linhas os resultados desta tabela.

	PoW 3	PoS	PBFT
<b>1 Nodo</b>	869 min	174 min	217 min
<b>2 Nodos</b>	462 min	103 min	138 min
<b>5 Nodos</b>	207 min	58 min	79 min
<b>10 Nodos</b>	124 min	41 min	67 min
<b>15 Nodos</b>	116 min	44 min	111 min

Tabela 8. Tempo total da execução.

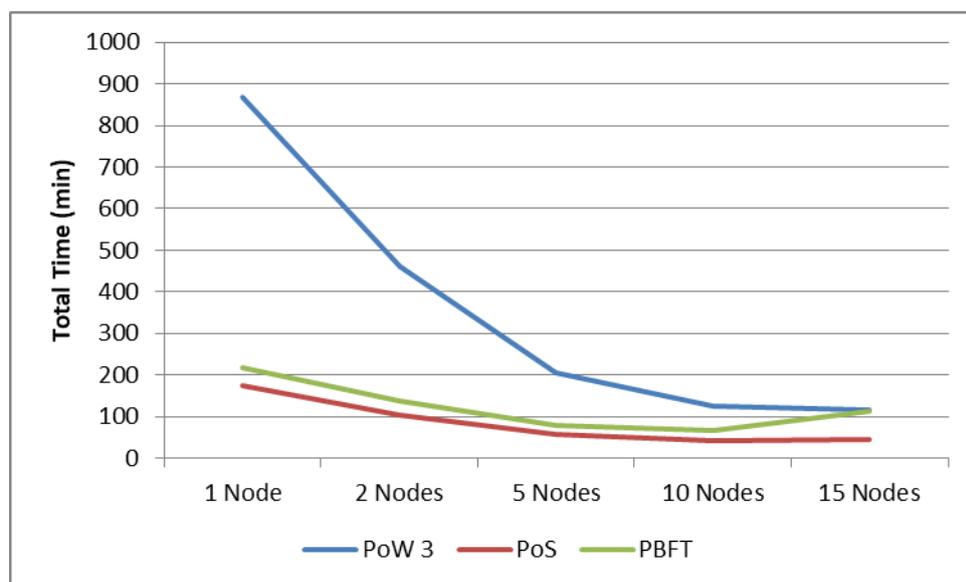


Figura 13. Aplicação da métrica M04.

Do ponto de vista de desempenho pode-se notar que o protocolo PoW é o menos performático, pois necessita de poder computacional para achar uma Hash específica com força bruta, porém é o mais escalável de todos já que a performance isolada de cada nodo não é influenciada pelos demais, apenas pelo seu próprio processamento, já para os protocolos PoS e PBFT a performance vai variar de acordo com a arquitetura modelada, já que a validação dos blocos é coletiva, depende da conexão com outros nodos, entretanto vale ressaltar que dependendo da disposição dos nodos, o nível de segurança varia, pois em um nível com apenas 2 nodos, por exemplo, caso um dos nodos se torne malicioso 50% do nível da rede está infectada, e como os outros níveis apenas “aceitam” os blocos deste nível infectado toda a rede pode ficar comprometida.

## 4 | CONCLUSÃO

Esse artigo teve por objetivo apresentar o Demochain, um framework para a criação de redes blockchain híbridas para dispositivos IoT. O trabalho realizado até o momento demonstra que o framework proposto é capaz de auxiliar no desenvolvimento de redes blockchain híbridas para ambientes IoT. O estudo realizado e o framework desenvolvido propiciaram a abstração de diversos conhecimentos, possibilitando assim que trabalhos relacionados possam ser desenvolvidos utilizando este como base em diversos aspectos.

Assim, pode-se concluir que não existe uma solução única se tratando de redes blockchain para dispositivos IoT. No entanto, a adoção de um framework para auxílio no desenvolvimento abre uma ampla possibilidade de novas soluções cada vez mais performáticas em diferentes contextos.

Como trabalhos futuros pode ser apontado a implementação de novos protocolos de consenso nesta arquitetura híbrida, com a possibilidade de cada camada estar rodando o seu próprio consenso, além de novos controles de armazenamento e envio da blockchain, e também utilizar outras métricas de desempenho e segurança para testes com este framework, em diferentes ambientes IoT.

## REFÊRENCIAS

Bitfury Group (2015). “Proof of Stake versus Proof of Work. White Paper”. [LINK DE ACESSO](#). Último Acesso: 29/11/2018.

Castro, M. e Liskov, B. (1999). “Practical Byzantine fault tolerance”.

Conoscenti, M., Vetrò, A. e De Martin, J. C. (2016). “Blockchain for the Internet of Things: A systematic literature review”.

De Angelis, Stefano. (2017). “Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains”.

Fernández Caramés, M., Fraga Lamas, D. P. (2017). “A Review on the Use of Blockchain for the Internet of Things”.

Freitas, L. (2018). Github com códigos do Demochain. Disponível em <https://github.com/LorenzoWF/Demochain>. Último acesso em 29/11/2018.

Gartner (2017). “Leading the IoT – Gartner Insights on how to lead in a connected world”.

Google (2009). Golang site oficial. Disponível em <https://golang.org>. Último Acesso: 29/11/2018.

Larimer, Dan (2014). “DPOS Description on Bitshares”.

Li, C. e Zhang, L. J. (2017). “A blockchain based new secure multi-layer network model for Internet of Things”.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K. e Njilla, L. (2017). “Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability”.

Ortiz, J. e Gottschlich, N. (2016). Base de dados “Household Power Consumption”. Disponível em <https://data.world/databeats/household-power-consumption>. Último Acesso: 29/11/2018.

Schmager, Frank (2010). “Evaluating the GO Programming Language with Design Patterns”.

Vukolić, M. (2018). “The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication”.

Zheng, Z., Xie, S., Dai, H. e Wang, H. (2017). “An overview of blockchain technology: Architecture, consensus, and future trends”.

## **SOBRE O ORGANIZADOR**

**Ernane Rosa Martins** - Doutorado em andamento em Ciência da Informação com ênfase em Sistemas, Tecnologias e Gestão da Informação, na Universidade Fernando Pessoa, em Porto/Portugal. Mestre em Engenharia de Produção e Sistemas, possui Pós-Graduação em Tecnologia em Gestão da Informação, Graduação em Ciência da Computação e Graduação em Sistemas de Informação. Professor de Informática no Instituto Federal de Educação, Ciência e Tecnologia de Goiás - IFG (Câmpus Luziânia) ministrando disciplinas nas áreas de Engenharia de Software, Desenvolvimento de Sistemas, Linguagens de Programação, Banco de Dados e Gestão em Tecnologia da Informação. Pesquisador do Núcleo de Inovação, Tecnologia e Educação (NITE), certificado pelo IFG no CNPq. ORCID: <https://orcid.org/0000-0002-1543-1108>

## ÍNDICE REMISSIVO

### B

Big data 76, 77

### C

Computação 2, 5, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 65, 67, 92, 112, 114, 115, 116, 117, 119, 120, 124, 127, 168, 169

Computação vestível 67

Comunicação 39, 42, 68, 75, 148, 154

Conhecimento 52, 53, 58, 59, 60, 61, 62, 70, 76

### D

Dispositivos 35

### E

Ensino 34, 35, 37, 40, 41, 42, 43, 45, 46, 107, 125, 127

### G

Gestão do conhecimento 63

### I

Informação 39, 52, 53, 56, 57, 58, 61, 63, 76, 89, 90, 91, 148, 154, 168

Internet 5, 7, 21, 22, 43, 57, 58, 92, 105, 106, 107, 112, 113, 115, 132

Internet das coisas 5

### M

Monitoramento 135

### O

Organização do conhecimento 54

### P

Programação 43, 168

### R

Recuperação de dados 24

Redes 21, 43, 130, 131, 137, 141, 148, 153, 154

### S

Sistemas de arquivos 24, 33

### T

Tecnologia 57, 60, 75, 112, 143, 148, 149, 154, 168

Testes 26, 27, 28, 29, 30, 31, 32, 122

Agência Brasileira do ISBN  
ISBN 978-85-7247-488-7

