# Demochain - Framework destinado a criação de redes blockchain híbridas para dispositivos IoT

**Lorenzo W. Freitas[1], Carlos Oberdan Rolim[2]**

[1]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, 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 Io*

## 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.

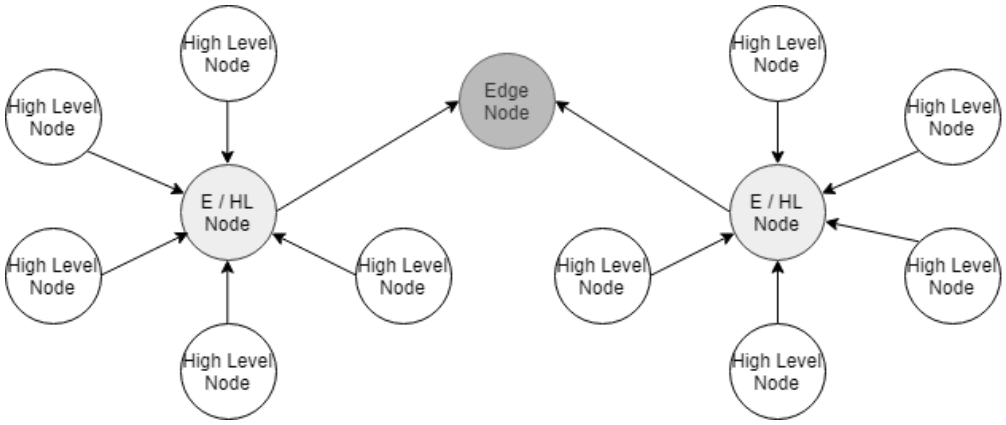


**Figura 1. Arquitetura implementada.**

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).

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.

**Tabela 1. Tabela de hardware para experimentação.**

| 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 |

Para os cenários que tem por objetivo testar o desempenho do framework foi utilizado as métricas descritas por S. Angelis (2017), que são comumente usadas para medir aplicações descentralizadas, sendo elas Taxa de validação, Latência, Escalabilidade e Tempo Total de Execução. A fim de simular dados reais de ambientes IoT foi utilizado um dataset público [Ortiz, J. e Gottschlich, N. 2016].

Foi realizado teste com até 15 Nodos utilizando a criptografia RSA, dispersos entre os Hardwares H01 e H02, sendo que todos estavam rodando sobre um mesmo nível de rede, ou seja, todos respondiam para o mesmo Edge Node. A Figura 2 apresenta o tempo total de execução em minutos sobre os três protocolos de consenso, considerando a variação do número de nodos na rede, sendo que o PoW estava com dificuldade 3.

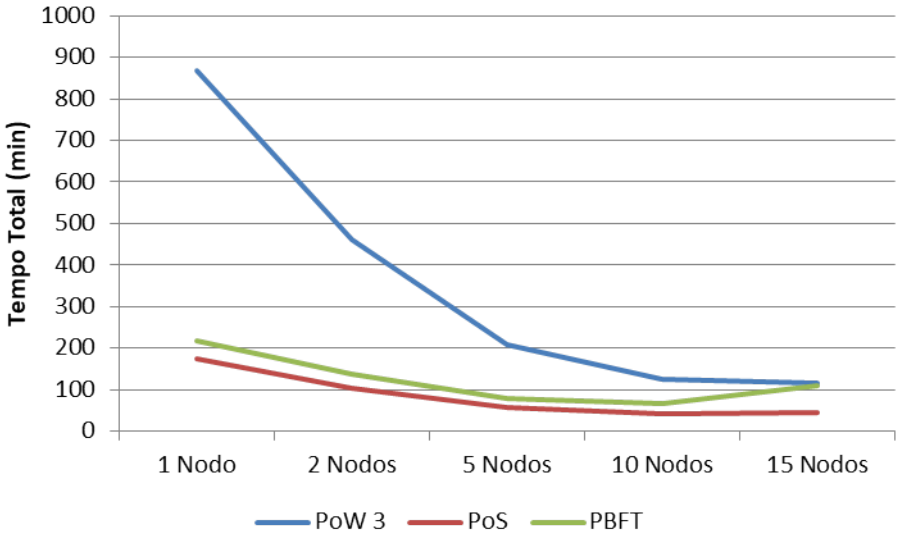


**Figura 2. Tempo total de execução sobre o Dataset**

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.

## 5. Referências


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

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

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

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

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

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

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

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.

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

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