UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS QUIXADÁ

CURSO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

AFONSO BARBOSA DE SOUZA NETO

BLOCKCHAIN COMO ALTERNATIVA PARA AUTENTICAÇÃO E CONTROLE DE ACESSO EM INTERNET DAS COISAS

QUIXADÁ

2018

AFONSO BARBOSA DE SOUZA NETO

BLOCKCHAIN COMO ALTERNATIVA PARA AUTENTICAÇÃO E CONTROLE DE ACESSO EM INTERNET DAS COISAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas de Informação.

Orientador: Prof. Me. Marcos Dantas Ortiz

QUIXADÁ

2018

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S713b Souza Neto, Afonso Barbosa de.
Blockchain como alternativa para autenticação e controle de acesso em internet das coisas / Afonso Barbosa de Souza Neto. – 2018.
41 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Sistemas de Informação, Quixadá, 2018.
Orientação: Prof. Me. Marcos Dantas Ortiz.

1. Internet das Coisas. 2. Blockchain (Databases). 3. Redes de computadores-Segurança. I. Título.
CDD 005

AFONSO BARBOSA DE SOUZA NETO

BLOCKCHAIN COMO ALTERNATIVA PARA AUTENTICAÇÃO E CONTROLE DE ACESSO EM INTERNET DAS COISAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas de Informação.

Aprovada em: __/__/____.

BANCA EXAMINADORA

Prof. Me. Marcos Dantas Ortiz (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. David Sena Oliveira
Universidade Federal do Ceará (UFC)

Prof. Dr. Paulo Antônio Leal Rego
Universidade Federal do Ceará (UFC)

À minha família, por sua capacidade de acreditar em mim e investir em mim. Mãe, seu cuidado e dedicação foi que deram, em alguns momentos, a esperança para seguir. Pai, sua presença significou segurança e certeza de que não estou sozinho nessa caminhada.

AGRADECIMENTOS

Agradeço a todos que contribuíram no decorrer desta jornada, em especialmente: A Deus, a quem devo minha vida. A minha família que sempre me apoiou nos estudos e nas escolhas tomadas. Ao orientador Prof. Marcos Dantas que teve papel fundamental na elaboração deste trabalho. Aos meus colegas pelo companheirismo e disponibilidade para me auxiliar em vários momentos.

"A menos que modifiquemos a nossa maneira de pensar, não seremos capazes de resolver os problemas causados pela forma como nos acostumamos a ver o mundo."

(Albert Einstein)

RESUMO

Desde sua criação, a internet vem sofrendo diversas transformações entre essas uma em especial vem chamando atenção a Internet das coisas(IoT) que nada mais é do que objetos diversos conectados a internet e provendo serviços aos usuários, dentre esses objetos pode-se citar eletrodomésticos, vestíveis, meios de transporte entre outros. A ideia é, cada vez mais, conectar o mundo físico ao digital. Para assegurar a segurança desses dispositivos, e dos próprios usuário, é necessário que os mecanismos de segurança atendam às características próprias da IoT. Com esse pressuposto este trabalho apresenta uma proposta de segurança para IoT baseado em *Blockchain*, modelo que busca a descentralização como medida de segurança. Para atingir esse objetivo a proposta utiliza o mesmo conceito de *Blockchain* aplicado em criptomoedas, porém com um mecanismo de consenso baseado na confiança entre os nós. A aplicação do protótipo em um cenário de teste possibilitou demonstrar que o modelo proposto é capaz de obter resultados consistentes, para o determinado domínio e aplicação.

Palavras-chave: Internet das Coisas. Blockchain. Segurança de redes.

ABSTRACT

Since its creation, the internet has undergone several transformations between these one in particular has been calling attention the Internet of Things (IoT) that is diverse objects connected to the Internet and providing services to users, to mention electric appliances, wearable, means of transport among others. The idea is, more and more, to connect the physical world with digital. To ensure the safety of these devices, and of the users themselves, it is necessary that the security mechanisms meet IoT's own characteristics. With this assumption this work presents a security proposal for IoT based on Blockchain, a model that seeks decentralization as a security measure. To achieve this goal the proposal uses the same concept of Blockchain applied in crypto-coins, but with a consensus mechanism based on trust between nodes. The application of the prototype in a test scenario made it possible to demonstrate that the proposed model is able to obtain consistent results for the given domain and application.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ALGORITMOS

LISTA DE ABREVIATURAS E SIGLAS

CH	*Cluster Head*
HRA	*Home Registration Authority*
IoT	*Internet of Things*
OBM	*Overlay Block Mangers*
PoW	*Proof of Concept*
RA	*Registration Authority*
RFID	*Radio-Frequency IDentification*
SH	*Smart Home*

SUMÁRIO

1 INTRODUÇÃO

A *Internet of Things* (IoT) vem atraindo a atenção de vários pesquisadores e entusiastas da área de tecnologia, por ser considerada uma evolução da internet que não apenas interage com o mundo físico, mas também colhe informação do ambiente e usa padrões existentes na internet para prover serviços, análises e comunicação de informações (GUBBI *et al.*, 2013). A IoT tem impactos significativos em vários aspectos da vida cotidiana e comportamento de usuários em potencial. Do ponto de vista de um usuário particular, os efeitos mais óbvios da introdução da IoT é visível nos campos do trabalho e da doméstica. Nesse contexto, a automação residencial e a vida assistida são apenas alguns exemplos de possíveis cenários de citação em que o novo paradigma tem um papel importante (ATZORI *et al.*, 2010). Por sua natureza descentralizada e escalável a IoT necessita de segurança e privacidade nas suas transações (FAROOQ *et al.*, 2015). Modelos de seguranças tradicionais tendem a centralizar todo o processamento em um único local, o que acaba dificultando a escalabilidade. Portanto soluções de segurança e privacidade devem ser implementadas conforme as características descentralizada e heterogêneas de dispositivos IoT. A *Blockchain* (BC) tem o potencial de agregar a IoT, e juntas compor uma ferramenta poderosa.

A maior parte dos dispositivos que constituem a IoT são de baixa capacidade de energia e pouco poder computacional. Esses dispositivos devem dedicar a maior parte do seu tempo executando a atividade principal o que faz com que a tarefa de suporte à segurança e privacidade um desafio. Em muitos métodos propostos a segurança é altamente centralizada, não sendo necessariamente adequado a IoT devido a necessidade de escalabilidade (ROMAN *et al.*, 2013).

A *Blockchain* foi proposta junto com a criação do *Bitcoin*, a primeira criptomoeda totalmente descentralizada (NAKAMOTO, 2008), cujo objetivo é deixar o processo de autenticação e criação de novas moedas com os membros da rede de maneira confiável e auditável. Usuários *Bitcoin* são conhecidos por uma chave pública modificável, gerando e transmitindo transações para a rede para transferir dinheiro. Essas transações são armazenadas em blocos, quando um bloco está cheio é encadeado a *Blockchain* por meio de um processo de mineração. Para minerar um bloco, alguns nós específicos na rede tentam resolver um quebra-cabeça criptográfico chamado *Proof of Work*(Prova de trabalho). O primeiro nó que conseguir resolver o quebra-cabeça envia o bloco para a *Blockchain*. Essa prova de trabalho tem a característica de ser muito difícil solucionar e muito fácil verificar se está correta (DORRI *et al.*, 2017a). Devido

a esse mecanismo de consenso entre os nós, a *Blockchain* possui algumas vantagens, entre elas maior transparência pois todas as transações são publicas e auditáveis , menos intermediários e algumas implementações possuem automação de ações como o caso do *Ethereum* (WOOD, 2014).

Os dispositivos IoT podem se beneficiar dessa natureza descentralizada da *Blockchain* como medida de segurança, onde nós não confiáveis podem trocar informação de maneira confiável, assim como acontece no *Bitcoin*. Os vários benefícios proporcionados pela *Blockchain*, conforme descritos anteriormente, torna uma solução atraente para abordar o problema de autenticação e controle de acesso em IoT. Contudo a forma como está implementada no *Bitcoin* não pode ser adotada pela IoT por esses motivos:

- **Complexidade do algoritmo de consenso:** como será visto na seção 3.1 e 5.4 tanto o *Proof of Work* como *Proof of Stake* requerem grande quantidade de poder computacional e tempo que são requisitos que dispositivos IoT não atendem.
- **Latência:** existe um atraso associado a confirmação de um novo bloco na rede *Bitcoin*. As transações podem levar algumas horas para serem confirmadas e mesmo assim não é um problema grande. Dispositivos IoT tem requisitos de atraso mais rigoroso.

Este trabalho tem como objetivo solucionar o problema de autenticação e controle de acesso em redes IoT, por meio da tecnologia *Blockchain* propondo um algoritmo de consenso e um modelo de confiança entre os nós.

Este trabalho está organizado da seguinte forma: o Capítulo 2, apresenta os principais objetivos deste trabalho. O Capítulo 3 discute os conceitos chave envolvidos. O Capítulo 4 serão apresentados os principais trabalhos relacionados, que tratam dos temas de segurança em IoT e *Blockchain*. O Capítulo 5 discute o modelo proposto aplicado neste trabalho e 6 apresentação dos resultados.

2 OBJETIVOS

Neste capítulo será apresentado o objetivo geral e os objetivos específicos deste trabalho.

2.1 Objetivo Geral

O objetivo deste trabalho é desenvolver um modelo de segurança baseado em *Blockchain* para cenários IoT, para solucionar o problema de autenticação e controle de acesso em *smart homes*.

2.2 Objetivos Específicos

a) Integrar a tecnologia *Blockchain* aos dispositivos IoT de maneira leve e escalável.
b) Desenvolver um algoritmo de consenso adequado para IoT.
c) Permitir que dispositivos IoT se comuniquem sem a necessidade de uma entidade centralizadora.

3 FUNDAMENTAÇÃO TEÓRICA

Nessa seção, serão abordados os principais conceitos relacionados a este trabalho e qual a contribuição de cada conceito para o desenvolvimento do trabalho.

3.1 Blockchain

A *Blockchain* pode ser definida como um banco de dados distribuídos onde cada nó armazena um conjunto de blocos, e cada bloco da cadeia aponta para o seu antecessor (NAKAMOTO, 2008). Foi criada junto com a invenção do *Bitcoin* por Satoshi Nakamoto em 2008, projetada para promover segurança entre troca de ativos financeiros por meio de nós não confiáveis, sem a necessidade de uma instituição centralizada. O trabalho de (NAKAMOTO, 2008) introduziu um sistema confiável, não mutável e auditável, servindo como um grande livro-razão distribuído. Normalmente instituições como bancos e cartórios são responsáveis por validar o registro de uma transação (por exemplo, transferências bancárias). Com o sistema proposto por (NAKAMOTO, 2008) o uso dessas instituições tornam-se dispensáveis, pois os próprios usuários da rede são responsáveis de gerenciar cada transação. Usuários *Bitcoin* são conhecidos por uma chave pública mutável, gerada e transmitida para a rede para transferência de recursos. Essas transações são postas em um bloco e anexadas a *Blockchain* por um processo de mineração. Para minerar um bloco, alguns nós específicos na rede conhecidos como mineradores tentam solucionar um problema matemático. O mineiro que solucionar o problema primeiro envia o bloco para a rede e recebe a recompensa.

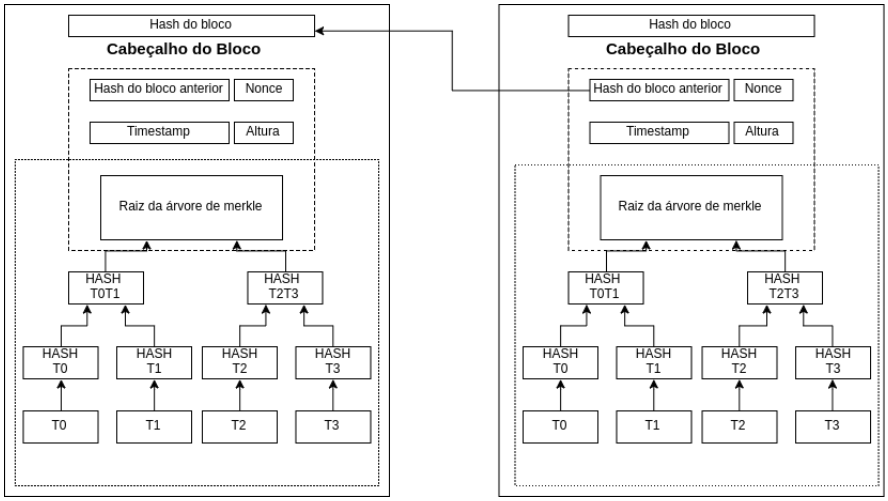
3.1.1 Estrutura de um Bloco

A figura 1 mostra a estrutura básica em um bloco.

Em (CHICARINO *et al.*, 2017) é descrito em seu texto, as partes principais de um bloco: transações e cabeçalho. As transações são agrupadas e armazenadas no bloco. O cabeçalho possui diversos campos, entre eles os mais importantes são: *Hash* do bloco, *Hash* do bloco anterior, *Nonce*, *Timestamp*, dificuldade, Altura e Raiz da árvore de merkle.

- **Hash do bloco:** É o principal identificador do bloco, é obtido pelo processo de resumo criptográfico do próprio bloco. Ao contrário dos demais campos do cabeçalho o *hash* do bloco é computado isoladamente pelo processo de mineração.

Figura 1 – Estrutura de blocos simplificada



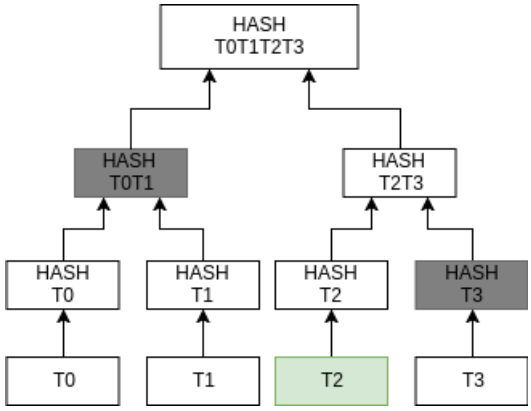
Fonte: Elaborada pelo autor
Ref:(NAKAMOTO, 2008)

- **Hash do bloco anterior:** Este campo do cabeçalho possibilita que um bloco seja ligado a seu antecessor, criando uma cadeia de blocos sequencial onde se algum bloco intermediário da cadeia for alterado, o bloco seguinte perde sua referencia, invalidando a toda a cadeia.
- **Nonce:** É o número variável usado para alterar a saída da função *hash* do cabeçalho. A mudança dessa variável é usada para determinar o *hash* final de um bloco, já que valores diferentes geram *hash* diferentes. Na rede do *Bitcoin* esse processo de escolha de um *Nonce* apropriado é conhecido como *Proof of work*. O *Nonce* é incrementado a partir do zero até encontrar um *hash* que se adéqua a dificuldade da rede (NAKAMOTO, 2008). A dificuldade caracteriza-se por uma quantidade variável de bits 0's no inicio do *Hash* do bloco.
- **Dificuldade:** Colisão parcial de bits em um *hash*. A rede *Bitcoin* assume como dificuldade uma quantidade variada de zeros no início do *Hash* do bloco, isso se deve ao fato de a rede se adequar a quantidade de mineradores que podem aumentar ou diminuir em determinadas épocas. Se muitos blocos forem descobertos em um curto período de tempo a dificuldade é recalculada para gerar aproximadamente um bloco a cada dez minutos. Por exemplo imagine que a dificuldade da rede é três, então um nó mineiro vai tentar por força bruta incrementar o *Nonce* até encontrar um *hash* que inicie com três zeros. É possível notar que quanto maior a dificuldade maior é o tempo necessário para encontrar um *hash*

apropriado. A dificuldade é variável para se ajustar a quantidade de nós mineiros, em geral quanto mais mineradores maior a dificuldade (NAKAMOTO, 2008).

- **Timestamp:** O *Timestamp* identifica o momento em que o bloco foi minerado e prova que os dados devem ter existido no tempo para entrar no *hash* (NAKAMOTO, 2008).
- **Raiz da árvore de merkle:** Também conhecida como árvore de *hash* ou simplesmente árvore merkle, é uma árvore binária completa, usada para armazenar um resumo dos dados e verificar com rapidez de se uma transação pertence ao bloco (MERKLE, 1987). Para construir uma árvore de merkle, as folhas devem ter tamanho par, caso haja um número ímpar a última folha é duplicada. As folhas são agrupadas em duplas para formarem o pai, dessa forma recursivamente os pais são agrupados em grupos até chegar na raiz. A Figura 2 mostra uma árvore merkle com as transações T0,T1,T2 e T3. Para verificar se a transação T2

Figura 2 – Árvore de merkle



Fonte: Elaborada pelo autor
Ref: (EVANS, 2011)

está no bloco, basta retornar o caminho até a raiz. No exemplo acima o *hash*(T3) seria usado para calcular o *hash*(T2T3) e o *hash*(T0T1) seria usado para calcular a raiz *hash*(T0T1T2T3T4), concluindo que a transação pertence ao bloco.

O trabalho proposto usará uma variação da *Blockchain*, com blocos estruturados de maneira a atender as demandas da rede IoT e criar uma reputação que os nós usarão para estabelecer confiança entre si, como será apresentado na Seção 5.4. Ao contrario do *Bitcoin* onde uma transação representa uma troca de ativo financeiro, neste trabalho uma transação irá representar uma solicitação de acesso a um dispositivo IoT.

3.2 Consenso na rede

Em uma *Blockchain* as transações não são gerenciadas por uma entidade central, agrupadas em blocos e verificadas por todos os membros da rede. Os membros da rede ou simplesmente nós se comunicam usando a internet. Um usuário mal intencionado pode tentar comprometer a integridade de um bloco criando transações falsas ou atribuindo a si falsas moedas. O grande diferencial do *Bitcoin* é que os nós conseguem chegar a mesma conclusão e fabricar o mesmo bloco desde que 51% dos nós sejam confiáveis, alcançar o consenso garante que cada nó concorde com o estado atual da *Blockchain* mantendo assim a cadeia consistente.

O mecanismo de consenso é composto por duas etapas: a validação de um bloco e a escolha da maior cadeia. Quando uma transação é criada ela é transmitida para todos os nós. Cada nó armazena novas transações em um bloco até que atinja a quantidade máxima para então ser minerado. Quando um nó encontra um *hash* apropriado, ele transmite o bloco para os demais nós que iniciam um processo de verificação das transações. Os nós aceitam o bloco somente se todas as transações nele forem válidas e se as moedas já não tiverem sido gastas anteriormente (NAKAMOTO, 2008).

Os nós expressam sua aceitação do bloco anexando-o a sua *Blockchain* e trabalhando na criação do próximo bloco, usando o *hash* do bloco aceito como o *hash* anterior. Os nós sempre consideram a cadeia mais longa como válida. Se dois nós transmitem versões diferentes do próximo bloco simultaneamente, eles podem receber os blocos em ordens diferentes (NAKAMOTO, 2008). Nesse caso, os nós armazenam duas cadeias: uma principal e uma secundária esse processo é conhecido como *fork*. Se uma parte dos mineradores adotar um bloco e a outra parte adotar o outro, essas duas cadeias irão coexistir até que uma fique maior que a outra. Se em algum momento uma cadeia ultrapassar a outra em quantidade de blocos, de acordo com o consenso a maior cadeia sempre é a correta, então o *fork* é resolvido e a outra cadeia é considerada invalida.

Em seções anteriores foi mostrado que o *Bitcoin* usa o *Proof of Work* para gerar novos blocos que basicamente utiliza o poder computacional e tempo para resolver um problema criptográfico, porém existem outros mecanismos como a Prova de Posse(PoS do inglês *Proof of Stake*) (KING; NADAL, 2012). O PoS requer que o usuário tenha uma certa quantidade de moedas para criar um novo bloco, a escolha é feita de maneira probabilística e as chances de um usuário ser escolhido depende da quantidade de moedas armazenadas. Neste trabalho o consenso se divide em duas etapas: confiança entre os nós e a escolha do nó que irá minerar o bloco. A

confiança entre os nós não esta associado ao conceito de *Blockchain* vistos até agora, por isso será explicada na Seção 5.4

3.3 Internet das Coisas

A Internet das coisas(IoT do inglês *Internet of Things*) como o próprio nome diz, é a tecnologia que está em tudo câmeras, carros, eletrodomésticos etc. É usada para designar processos que envolvam objetos conectados em rede e que produzam e/ou processem informação em tempo real e de forma autônoma (SINGER, 2012). A Figura 3 representa uma visão geral dos dispositivos IoT conectados.

Figura 3 – Visão geral da IoT

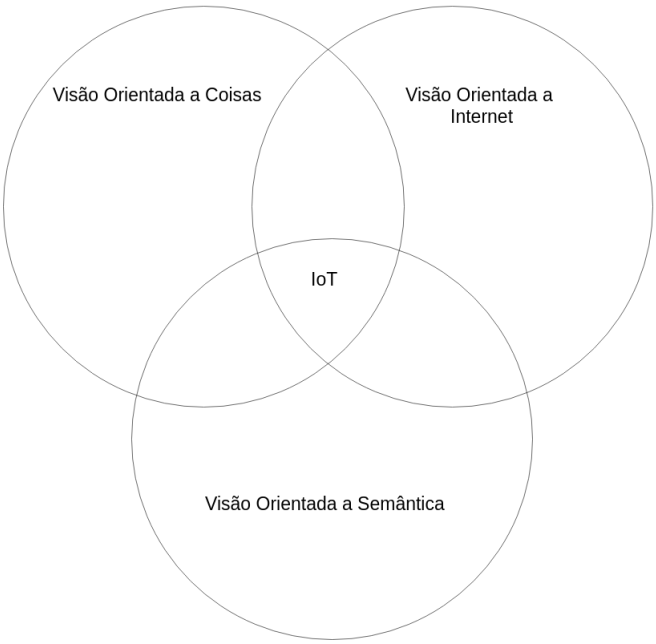
Fonte: Imagem da internet[1]

No trabalho de (SANTAELLA *et al.*, 2013) mostra que a IoT é uma evolução natural dos dispositivos pessoais ligados a rede teleinformática e dispositivos de comunicação móvel. Como consequência a computação está cada vez mais ubíqua saltando para objetos do cotidiano e neles implantando dados e identidades além da capacidade de comunicação. A ubiquidade refere-se à noção de algo que está presente em todos os lugares e em todos os momentos, persistente, sempre disponível e atuante. De acordo com (SINGER, 2012) a IoT tem agregado diferentes conceitos em que a ideia de objetos conectados que trocam informação entre si é bastante ampla e faz com que muitas tecnologias e aplicações diferentes atendam pelo nome de Internet das Coisas. Uma tentativa de resumir os diferentes pontos da IoT é feita por (ATZORI *et al.*, 2010), onde é destacado com três visões principais: orientado a "coisas", orientado a "internet"e orientado a "semântica"como ilustrado na Figura 4. Visão orientada a coisas foi a primeira definição de IoT

[1] Disponível em: <http://www.partnerone.com.br/?p=2625> Acessado em junho 2018.

as coisas consideradas eram itens simples e usavam geralmente *Radio-Frequency IDentification* (RFID). Visão orientada a Internet semanticamente significa uma rede mundial de dispositivos conectados, onde esses dispositivos são endereçáveis e possuem protocolos de comunicação. O endereçamento exclusivo do objeto, representação e o armazenamento das informações trocadas se torna a questões mais desafiadoras, trazendo diretamente para uma terceira perspectiva da IoT, Visão orientada a semântica.

Figura 4 – Diferentes visões para IoT



Fonte:Adaptado de (ATZORI *et al.*, 2010)

Os dispositivos neste trabalho farão parte de uma *Smart Home* (SH) e podem ser divididos em três categorias: dispositivos de acesso, de monitoramento e de armazenamento.

4 TRABALHOS RELACIONADOS

Os autores em (SAHRAOUI; BILAMI, 2014) propõem uma nova forma de autenticação e controle de acesso para tornar dispositivos IoT seguros contra acesso não autorizado. O método proposto baseia-se em duas autoridades de autenticação: *Registration Authority* (RA) e *Home Registration Authority* (HRA). O RA é projetado para facilitar o processo de autenticação de dispositivos. Todos os dispositivos são registrados com o RA. Da mesma forma, o HRA facilita o processo de autenticação para os usuários. Quando um usuário deseja acessar dados de um determinado dispositivo, a requisição é primeiro enviado para o RA. O RA verifica a autenticidade do usuário com o HRA. Assumindo que o usuário é autenticado, o RA gera uma chave compartilhada para comunicação entre o usuário e o dispositivo.

A analise de segurança mostra que o modelo é seguro, porém a necessidade de cada dispositivo ter um RA e cada usuário um HRA pode ocasionar problemas de escalabilidade, no projeto proposto a *Blockchain* é administrada por um *Cluster Head* (CH), Seção 5.1, e cada *smart home* gerecia seus dispositivos internos.

O trabalho de (STEGER *et al.*, 2018) propõe uma arquitetura baseada em *Blockchain* para atualização de software automotivo segura. A proposta é avaliar a implementação da *Proof of Concept* (PoW) em um sistema de atualização de software sem fio fornecendo uma comunicação segura e eficiente entre todas as partes envolvidas. Os veículos inteligentes consistem em uma unidade simples que controla tarefas. Cada unidade comunica-se entre si e com o fabricante que por sua vez verifica e distribuiu a nova versão de software que será instalada nas unidades.

Os nós são agrupados em *clusters* onde é eleito um líder para gerenciar a *Blockchain* semelhante ao proposto neste projeto, mas os autores usam *Proof of Concept* como algoritmo de concesso, que demanda muito processamento, enquanto neste trabalho é utilizado consenso em duas etapas: confiança entre os nós (validação) e a escolha do nó que irá minerar o bloco.

O trabalho de (DORRI *et al.*, 2017b) inspirou este trabalho. O autor propõem um modelo de segurança baseado em *Blockchain*, leve e escalável para Internet das Coisas. O método proposto baseia-se na criação de uma arquitetura em dois níveis: local onde os dispositivos são gerenciados por uma *Blockchain* local e uma rede *overlay* onde os gerentes de bloco *Overlay Block Mangers* (OBM) gerenciam uma *Blockchain* publica, confirmando e verificando novos blocos. O algoritmo de consenso garante que um bloco gerado é selecionado aleatoriamente entre os nós e é limitado no numero de blocos que pode gerar. Para introduzir a aleatoriedade entre os blocos, cada OBM deve esperar por um tempo antes de gerar um novo bloco.

Grande parte deste trabalho basei-se no trabalho de (DORRI *et al.*, 2017b): cenário dividido em rede local e sobreposição, nós que gerenciam a *Blockchain* e parcialmente a estrutura dos blocos, no entanto, neste trabalho os algoritmo de consenso e confiança são diferentes voltados para redução da demenada de processamento.

A Tabela 1 apresenta as principais semelhanças e diferenças dos trabalhos citados neste capítulo com o trabalho proposto.

Tabela 1 – Comparação entre os trabalhos relacionados e o trabalho proposto

	Sahraoui (2014)	**STEGER (2018)**	**Dorri (2017)**	**Trabalho proposto**
Consenso	-	Proof of Concept	Escolha aleatório do minerador	Escolha probabilística do minerador
Autenticação e Controle de acesso	RA e HRA	-	Estrutura de blocos locais	Estrutura de blocos locais
Verificação das transações	-	Assinatura do fabricante	Verifica as permissões do solicitante	Verifica as permissões do solicitante
Blockchain	-	Cada nó tem a mesma versão da Blockchain	Nós podem ter diferentes versões da Blockchain	Cada nó tem a mesma versão da Blockchain
Encadeamento dos blocos	-	Blocos encadeados	Transações encadeadas	Blocos encadeados

Fonte: Elaborado pelo autor

5 MODELO PROPOSTO

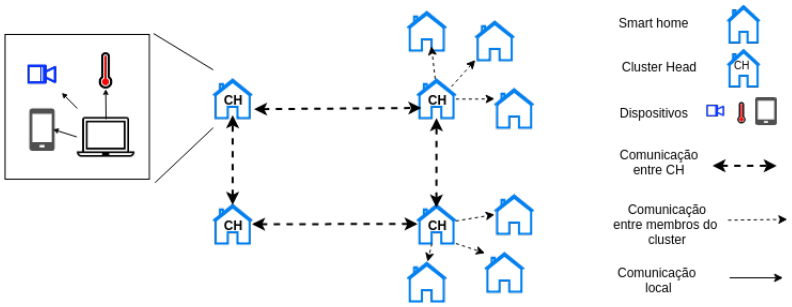
Nesta seção são apresentados os passos para implementação do modelo proposto.

5.1 Rede de Sobreposição

Imaginando o contexto de uma casa inteligente, mas pode ser aplicado em outros ambientes de IoT, o projeto consiste em dois níveis principais: a casa inteligente(SH do inglês *smart home*) e uma rede de sobreposição. Dispositivos IoT estão localizados no nível SH. Na rede de sobreposição estão todas as SH conectadas e é semelhante a uma rede *peer-to-peer* que se refere a um estilo de arquitetura distribuída completamente descentralizada, em que todos os nós são equivalentes em termos de funcionalidade e tarefas que executam (BARCELLOS; GASPARY, 2006).

Para reduzir o atraso na rede, agrupamos as SHs em *clusters* e cada *clusters* elege um líder (CH do inglês *Cluster Head*). A *Blockchain* é mantida por dispositivos de altos recursos na rede de sobreposição. Os CHs processam transações de entrada e transações de saída que são geradas por outros CH. Espera-se que um nó selecionado como CH permaneça online por um longo período de tempo e tenha recursos suficientes para processamento de blocos e transações. Quando algum dispositivo solicitar acesso, o CH cria uma transação e a envia para os CH candidatos (ver Seção 5.2). A transação é armazenada em um local separado até a escolha de um novo nó mineiro para juntar todas as transações em um bloco, validar e envia-las para a rede. A figura 5 ilustra o a interação entre os diferentes membros da rede. Cada *smart home* possui uma

Figura 5 – Cenário do trabalho proposto



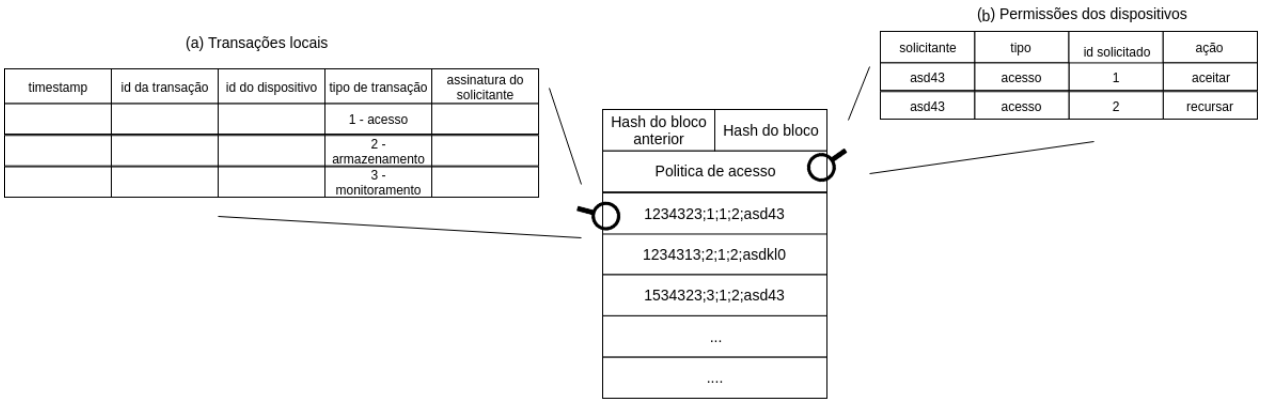
Fonte: Elaborada pelo autor

Blockchain local para armazenar as permissões de cada dispositivo. Dessa forma, gerencia todas as transações de saídas e de entrada locais.

5.2 Estrutura dos blocos

Os blocos são usados para armazenar as transações geradas pelos CHs. Uma transação é definida como uma solicitação de acesso a um dispositivo IoT. A comunicação entre os dispositivos se dá através de transações que são armazenadas em blocos visíveis apenas para os CHs. Elas podem ser de três tipos: acesso, armazenamento ou monitoramento. Transações de armazenamento em geral tem a função de armazenar alguma informação do dispositivo em locais como a nuvem ou em um disco local. A transação de acesso é usada por dispositivos que queiram acessar alguma informação em outros dispositivos ou nos locais de armazenamento. As transações de monitoramento apenas concedem acesso ao dispositivo como por exemplo acesso a uma câmera de monitoramento. Transações podem ocorrer em uma rede local ou na rede de sobreposição. Transações locais são armazenadas na *Blockchain* local e são compostas por cinco campos: *timestamp* tempo de criação da transação, id da transação inteiro que identifica a transação como única, id do dispositivo chave publica do dispositivo solicitado, tipo da transação como ilustrado na Figura 6(a) e assinatura do solicitante chave publica do dispositivo solicitante. As permissões dos dispositivos são armazenadas no cabeçalho Figura 6(b). A figura 6 ilustra um bloco local e seus campos.

Figura 6 – Bloco local

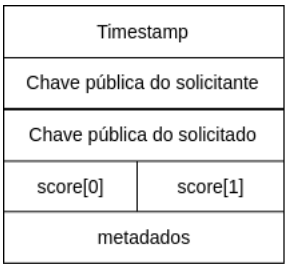


Fonte: Elaborada pelo autor
Ref: (DORRI *et al.*, 2017a)

Transações dos nós de sobreposição são realizadas entre os CHs e sua estrutura é formada pelos campos: *timestamp*, chave pública do solicitante, chave pública do solicitado, metadados e score. *Timestamp* é tempo que a transação foi criada, chave pública do solicitante e solicitado é a identidade dos dispositivos, metadados contém a informação do tipo da transa-

ção(acesso, monitoramento e armazenamento) por último a score é o resultado da verificação da transação, se foi bem sucedida score[0] armazena verdadeiro e score[1] falso, se a transação falhou score[0] recebe falso e score[1] verdadeiro como na Figura 7. Os blocos da camada de

Figura 7 – Estrutura da transação da rede de sobreposição



Fonte: Elaborada pelo autor
Ref: (DORRI *et al.*, 2017a)

sobreposição seguem uma estrutura semelhante a apresentada na Figura 1, com as seguintes diferenças: a variável *Nonce* não é necessária já que a mineração ocorre de outra maneira, no cabeçalho é adicionado um campo de reputação,que estabelece o grau de confiança entre ver Seção 5.5, que incrementa ao criador do bloco a quantia de 1, por último as transações são armazenadas em forma de lista.

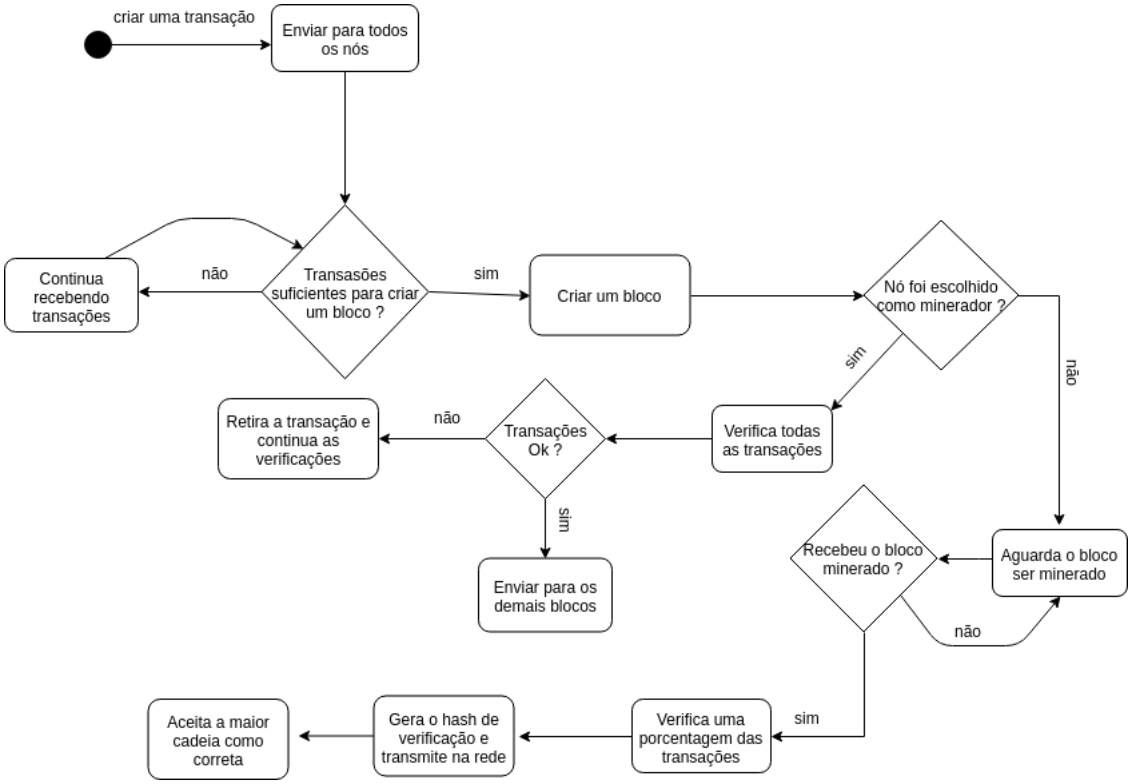
5.3 Comportamento do Nó

A figura 8 apresenta o comportamento básico do funcionamento de um nó do trabalho proposto que será detalhado nas próximas seções. Neste modelo uma transação é definida como: uma solicitação de acesso a um dispositivo(termostato, alarme de incêndio, sistema de som, lâmpadas etc). O acesso pode partir de um usuário na rede ou de outro dispositivo a solicitação deve seguir o modelo como da imagem acima sendo validada pelos próprio membros da rede. Os nós mineiros são dispositivos com um maior poder computacional e disponibilidade(celulares, computadores, *Beaglebone*), Esses são os responsáveis por organizar e gerenciar toda a rede.

5.4 Consenso

Quando um CH é escolhido como minerador, ele verifica todas as transações do bloco e envia em *broadcast* para os demais CHs na rede e então espera por um período variável para que não faça parte da próxima eleição de minerador. Assim como no *Bitcoin* (NAKAMOTO,

Figura 8 – Visão geral do comportamento de um nó



Fonte: Elaborado pelo autor

2008) uma transação é efetivada quando uma determinada quantidade de blocos seguintes são verificados e adicionados ao *Blockchain*. Os CHs podem manter 3 estados possíveis: seguidor, candidato e líder, seguidores são os CHs que não irão participar da eleição do próximo nó, candidatos são os CHs aptos a participar e por ultimo o líder é o CH escolhido. Dessa forma, quando o bloco é minerado o CH espera por um tempo variável e passa para o estado de seguidor.

Como não é possível garantir que todos os CHs que irão verificar o bloco sejam confiáveis, o algoritmo de consenso trabalha com a ideia de maior cadeia. Alguns CHs que verificam o bloco podem atribuir falsos acessos a dispositivos e comprometer a integridade do bloco e da rede ou pode corrigir uma transação falsa gerada por algum minerador mal intencionado. A cadeia mais longa é marcada como válida e cadeias distintas são descartadas. Para isso, o algoritmo usa um *hash* no cabeçalho do bloco chamado *hash* de verificação. Sua função é assinar o bloco após a verificação das transações. Se o *hash* da verificação for igual ao *hash* do bloco minerado, então nenhuma transação foi modificada. Se o *hash* for diferente então o CH alterou alguma transação do bloco e portanto, cria-se um *fork* na *Blockchain*. Assim tem-se dois ramos da cadeia: um principal e outro secundário, que irão coexistir até uma possuir

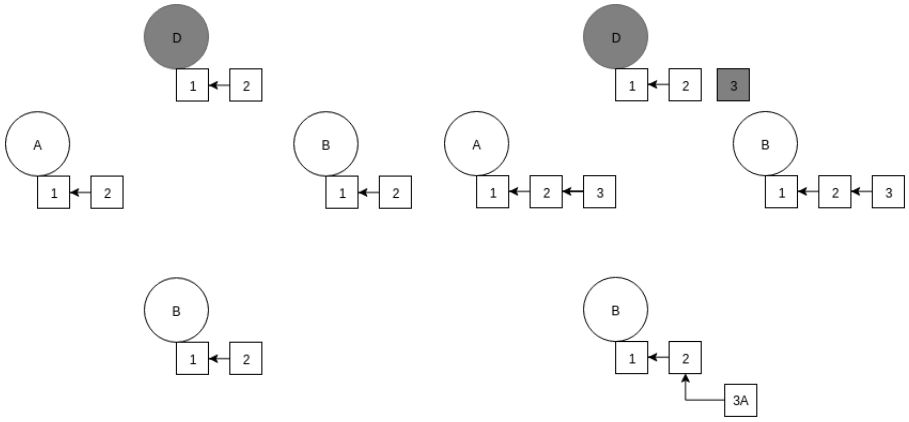
a maior quantidade de blocos.

A Figura 9 exemplifica o conceito de maior cadeia. Na Figura 9(a) é dado o estado inicial dos blocos com o nó **D** como minerador e o restante são nós de verificação. Na Figura 9(b) o **D** minera o bloco 3 e envia para os demais. Cada nó verifica as transações e gera seu próprio *hash* de verificação. O nó **B** tentou criar uma transação falsa alterando assim seu *hash* de verificação. Por ultimo, Figura 9(c), o bloco verificado é transmitido para a rede e anexado aos outros blocos. Percebe-se que o ramo como mais blocos (1,2,3,3) passa a ser o ramo correto resolvendo o *fork* da rede. Por fim, os blocos duplicados podem ser descartados, restando os blocos (1,2,3).

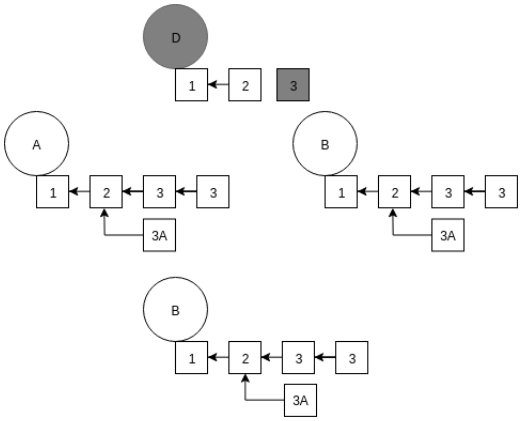
Figura 9 – Exemplo de cadeira mais longa

(a) Estado inicial dos blocos

(b) Cada um gera seu hash de verificação



(c) Cada nó envia sua verificação



Fonte: Elaborada pelo autor

O Algoritmo 1 representa a rotina que é executada sempre que um novo bloco é gerado para rede. Após a escolha no minerador o CH escolhido executa a verificação das transações pelo campo metadados da transação, que contém informações sobre o CH que gerou a transação e do dispositivo solicitado. Os demais CH's executam o algoritmo de confiança, que

basicamente analisa a tabela de confiança.

Algoritmo 1: Algoritmo de consenso

```
begin
    inicializa o evento com time zero;
    minererador = escolhaMinerador();
    if minererador == VERDADEIRO then
        repeat acesso = verificarPermissao(bloco.trasacao[i].metadados.);
        transacao[i].status = acesso;
        until acabar as transações;
        geraHashDeVerificacao(bloco);
    else
        confiança();
    end
    escolhaDaMaiorCadeia();
end
```

Fonte: Elaborada pelo autor

A última rotina a ser executada é a escolha da maior cadeia representada pelo Algoritmo 2 no qual o CH aguarda a chegada dos demais blocos e em seguida armazena o *hash* de verificação em uma lista. No fim do processo anexa a *Blockchain* a maior cadeia de *hash*.

Algoritmo 2: Maior cadeia

```
begin
    listaHash = vazio;
    repeat bloco = recevBloco();
    id = buscarHash(bloco.hashverificacao,listaHash);
    if id > 0 then
        listaHash[id].quantidade = +1;
    else
        addNaLista(bloco.hashverificacao);
    end
    until quantidade de CH;
    anexar na Blockchain a maior cadeia;
end
```

Fonte: Elaborada pelo autor

5.5 Confiança

Os nós criam confiança um no outro a medida que sua confiança aumenta. Usa-se dois critérios para estabelecer a confiança entre os nós: quantidade de transações verificadas e

sua reputação. A quantidade de **transações** verificadas representa o numero total de transações que um CH minerou. A reputação representa a quantidade de **blocos** minerados anteriormente por um CH. A Tabela 4 mostra a quantidade de transações que precisarão ser verificadas (em porcentagem). Como visto nesta tabela, quanto maior a confiança no minerador menor será a quantidade de transações que precisarão ser verificadas reduzindo a demanda de processamento.

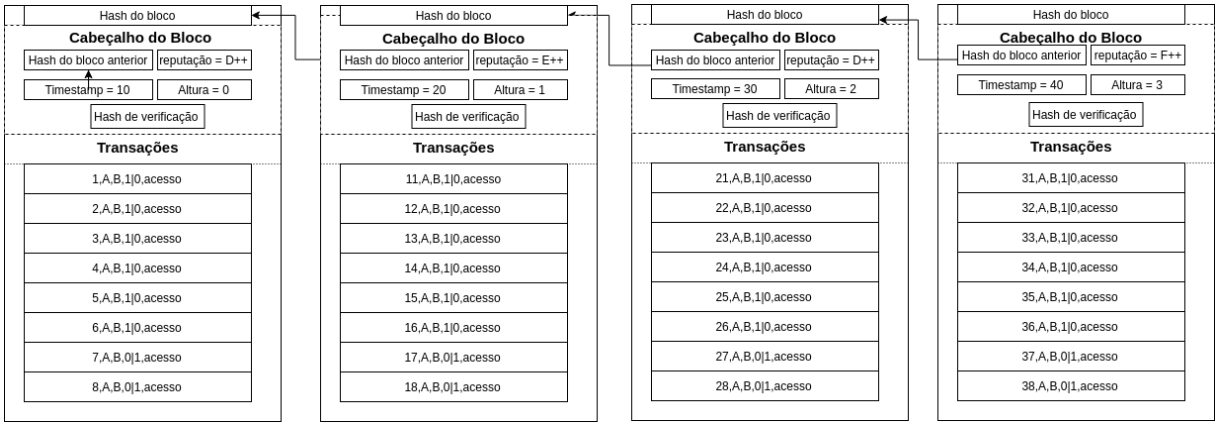
Tabela 2 – Tabela de confiança

Quantidade de transações verificados anteriormente						
Reputação		>=10 e <20	>= 20 e <30	>=30 e <40	>= 40 e <50	>= 50
	>=5 e <10	80%	70%	60%	50%	40%
	>=10 e <15	70%	60%	50%	40%	30%
	>=15 e <20	60%	50%	40%	30%	30%
	>=20 e <25	50%	40%	30%	30%	20%
	>=25	40%	30%	30%	20%	20%

Fonte: Elaborado pelo autor

Para exemplificar a confiança entre CHs, dado um estado de *Blockchian* como o da Figura 10, é possível estabelecer a confiança no nó percorrendo todos os blocos. Assumindo que a *Blockchain* está em um estado válido, o CH **D** minerou um novo bloco e enviou na rede. Os demais CHs executam o algoritmo para estabelecer a confiança no CH **D**. Eles calculam a reputação do CH comparando o *hash* do bloco com o *hash* de verificação. Se forem diferentes, a contagem no bloco é descartada e passa ao bloco anterior, se forem iguais, contabiliza a reputação e quantidade de transações. Ao fim de todo o processo, é retornada uma tupla contendo a reputação e a quantidade de transações. Neste exemplo, a confiança no CH **D** seria: Reputação +2 e transações +16. A Tabela 4 mostra que esse CH ainda não tem confiança suficiente, então todas as transações deverão ser verificadas.

Figura 10 – Estrutura da Blockchain do trabalho proposto



Fonte: Elaborada pelo autor

6 AVALIAÇÃO DO MODELO PROPOSTO

Nesta seção serão como foram efetuados os testes de validação e a apresentação dos resultados.

6.1 Introdução

A apresentação dos resultados demonstrada neste capítulo objetiva promover uma visão geral do processo permitindo a avaliação e discussão dos resultados tendo com referencia o trabalho de (DORRI *et al.*, 2017a), trabalho no qual este é baseado. A simulação foi feita usando a ferramenta de simulação NS3 com estrutura baseada no trabalho de (GERVAIS, 2016), que implementa uma versão do *Bitcoin* usando o NS3, e para troca de mensagem do bloco foi usado a implementação Json para C++ desenvolvida por (TENCENT, 2016) . Este capítulo está dividido em duas partes, sendo:

- Cenários de Aplicação: apresenta de maneira geral o cenário informado, característica da organização dos nós bem como explicação das métricas utilizadas. Promove uma visão geral das possibilidades de análise a partir do modelo e do cenário proposto.
- Análise dos Resultados: apresenta os principais resultados encontrados e expõem suas análises através de gráficos.

6.2 Cenário de Aplicação

O cenário simulado corresponde à estrutura dos nós de sobreposição, nós mineradores ou CH, abstraindo toda a estrutura da *smart home* ou seja a simulação contempla apenas o funcionamento da estrutura da Seção 5. Isso se deu ao fato do simulador(NS3) não fornecer ferramentar adequadas para avaliar os dispositivos Iot (como ferramentas para medir o consumo de energia ou poder computacional). A fim de simplificar a comunicação entre CH e a *smart home*, as permissões dos dispositivos são armazenadas no CH bem como a estrutura da *Blockchain*. As permissões seguem o modelo da política de acesso conforme a Figura 6. A estrutura da *Blockchain* é representada por uma variável inteiro e uma lista de blocos. As transações, que representam uma solicitação de acesso a um dispositivo, são criadas de forma aleatória seguindo o modelo da Figura 7 sempre antes da mineração do bloco. O comportamento da simulação segue conforme a Figura 8.

As métricas adotadas na validação do projeto foram: i) tempo médio de validação

de uma transação, ii) tempo de mineração do bloco, iii) quantidade de transações falsas que alcançaram sucesso. O tempo de validação de uma transação representa o tempo que uma transação levou para ser efetivada ou seja o acesso do usuário foi aceito ou recusado. Assim como no *Bitcoin*, ou qualquer outra criptomoeda, uma transação é considerada efetivada quando ela for minerada em um bloco e quando for sucedida por uma quantidade mínima de blocos. Neste trabalho a quantidade adotada como padrão foi cinco blocos. O tempo de mineração do bloco mede o algoritmo de confiança, pois, a quantidade de transações que precisará ser verificada diminui à medida que um CH aumenta sua reputação. A Tabela 4, que mede a confiança de um CH, foi modificada a fim de simplificar o teste e a análise dos resultados. A mudança ocorreu na quantidade de transações verificadas que foi diminuída pela metade. Por fim a quantidade de transações falsas que alcançaram sucesso representa a taxa de falha do modelo em relação a um usuário mal intencionado.

Os gráficos gerados possuem barras de erro, em torno das médias das vinte replicações, utilizando um intervalo de confiança de 95%.

Todas as métricas foram coletadas a partir da *Blockchain* gerado ao final de cada simulação, para isso foi criado um nó de controle que exerce apenas a função de gerar a *Blockchain* ao final da execução, esse nó não participa de nenhuma etapa de mineração. Foram feitas simulações utilizando dez, quinze e vinte CH's, cada um gerando até cinco transações por bloco.

Todos os experimentos foram realizados em uma única máquina que dispõe das seguintes configurações: processador Intel Core Intel Core i5-5200U CPU 2.20GHz 4, 7.7 GB de memória RAM e sistema operacional Ubuntu 18.04.1 LTS 64 bits e a versão 3.28 do NS3. Implementação disponível no GitHub do autor[1].

Tabela 3 – Configuração da simulação

Parâmetro	**Valor**
Cenário	Sobreposição
Geração das transações	Aleatório
Quantidade de CH	5,10,15,20
Taxa (transação/CH)	Aleatório (1 a 4)
Número de rodadas	20
Intervalo de Confiança	95%

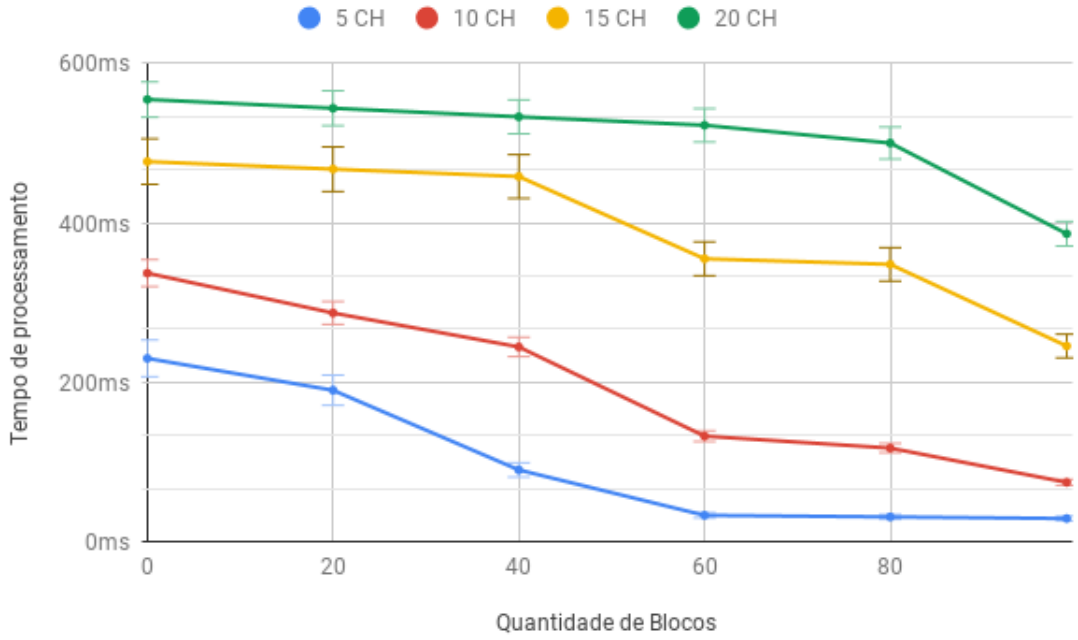
Fonte: Elaborado pelo autor

[1] Disponível em: <https://github.com/afonsoneto121/tcc>

6.3 Análise dos Resultados

6.3.1 Tempo de mineração do bloco

Figura 11 – Tempo de mineração do Bloco



Fonte: Elaborada pelo autor

O modelo proposto usa um algoritmo de confiança distribuída que diminui o número de transações que devem ser verificadas à medida que os CH's adquirem confiança um nos outros (veja seção 5.5). Foi usado uma quantidade variada de CH (dez, quinze e vinte) em cada rodada da simulação com uma instância de *Blockchain* com 100 blocos. Foi utilizado uma versão reduzida da tabela de confiança,Tabela 4, a fim de se observar a diminuição no tempo de mineração do bloco.

Tabela 4 – Tabela de confiança

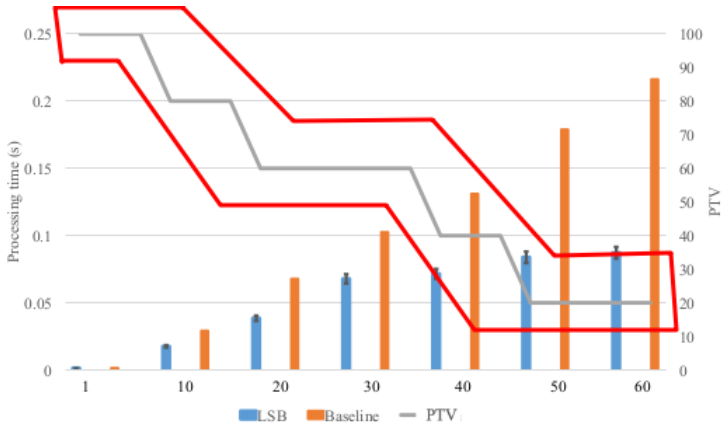
	Quantidade de transações verificados anteriormente					
Reputação		>=10 e <20	>= 20 e <30	>=30 e <40	>= 40 e <50	>= 50
	>=1 e <5	80%	70%	60%	50%	40%
	>=5 e <10	70%	60%	50%	40%	30%
	>=10 e <15	60%	50%	40%	30%	30%
	>=15 e <20	50%	40%	30%	30%	20%
	>=20	40%	30%	30%	20%	20%

Fonte: Elaborado pelo autor

Como pode ser observado na Figura 11, o experimento mostra como o algoritmo de confiança trabalha reduzindo o tempo de mineração do bloco. Devido à concorrência entre os CH's, sua reputação cresce de forma mais lenta o que impacta diretamente no tempo de mineração. Com uma quantidade menor de CH, o tempo de mineração do bloco tende a diminuir mais rápido (gráfico azul da Figura 11), já com uma quantidade maior de CH é possível perceber que o tempo de mineração reduz porém de forma mais lenta (gráfico verde da Figura 11).

Comparando os resultados encontrados com o trabalho de (DORRI *et al.*, 2017a), Figura 12, o autor usa duas implementações de *Blockchain*: uma que o autor chama de *Baseline*, corresponde a uma implementação sem o algoritmo de confiança, e outra LSB, que corresponde a implementação do autor com o algoritmo de confiança. PTV representa a quantidade de transações verificadas em porcentagem, vale destacar que não é considera,no tempo de mineração, outras tarefas como verificação de listas de chaves, geração de novos blocos, etc. Os resultados encontrados neste trabalho ficaram um pouco acima dos encontrados por (DORRI *et al.*, 2017a), analisando a área destacada nota-se que o algoritmo de confiança adotado por (DORRI *et al.*, 2017a) chega a quantidade mínima de verificações(20%) visto que o critério adotado para sua tabela de confiança se resume à quantidade de transação verificadas anteriormente.

Figura 12 – Comparação do tempo de mineração do Bloco

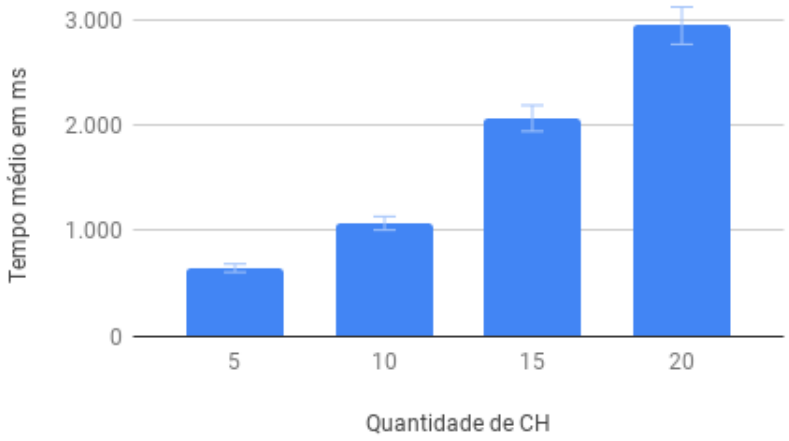


Fonte: (DORRI *et al.*, 2017a)

6.3.2 Tempo médio de validação de uma transação

A Figura 13 mostra o tempo médio que uma transação leva para ser devidamente efetivada. A contagem do tempo inicia-se quando um bloco é devidamente minerado. O estado

Figura 13 – Tempo médio de validação de uma transação



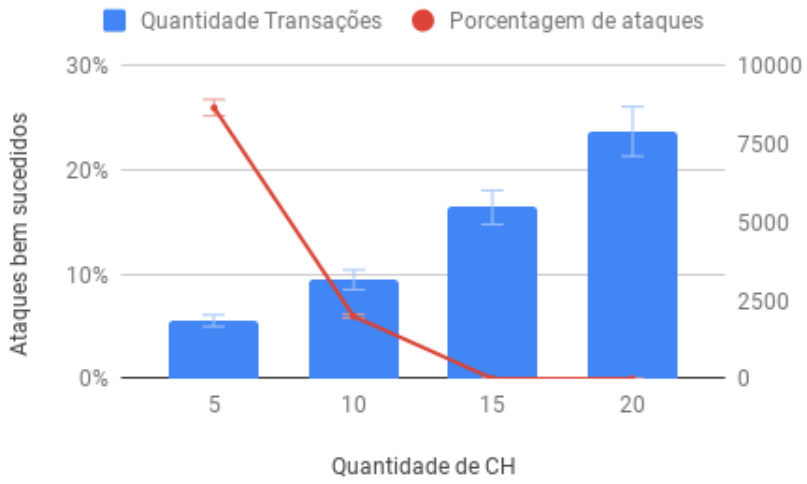
Fonte: Elaborada pelo autor

atual do projeto ainda não é capaz de computar o tempo total de uma transação, diferença de tempo desde a solicitação de acesso por parte do usuário até a efetiva resposta da rede cedendo o acesso ou negando-o. A efetivação da transação segue conforme funcionam nas criptomoedas, uma transação é efetivada quando uma quantidade mínima de blocos é minerado. Essa quantidade mínima é igual a cinco, isso significa que as transações do bloco 1 só vão ser efetivadas quando o bloco 6 for minerado, o mesmo segue para os demais blocos. O resultado encontrado mostra que devido à concorrência entre os CH's o algoritmo de consenso não consegue ser totalmente eficiente reduzindo o tempo das transações, isso significa que a reputação de um CH aumente de forma mais lenta fazendo com que mais blocos sejam verificados por completo. Além desse fator um número maior de CH faz com que se aumente o número de mensagens trocadas influenciando nos resultados encontrados.

6.3.3 Quantidade de transações falsas descobertas

Para essa simulação foi usado uma versão contendo cinco CHs para diversificar os resultados. Diferente das simulações anteriores, em que as transações eram geradas de modo aleatório, nesta a rede segue um padrão previamente estabelecido. Para cada rodada da simulação aproximadamente um terço dos CH's é marcado como usuário mal intencionado, criando uma transação falsa por bloco. Ao final da simulação foi contabilizado a quantidade de transações que alcançaram sucesso. A Figura 14 demostra os resultados encontrados, indicando que a medida que mais CH's participam do processo de mineração menor é chance de uma transação falsa

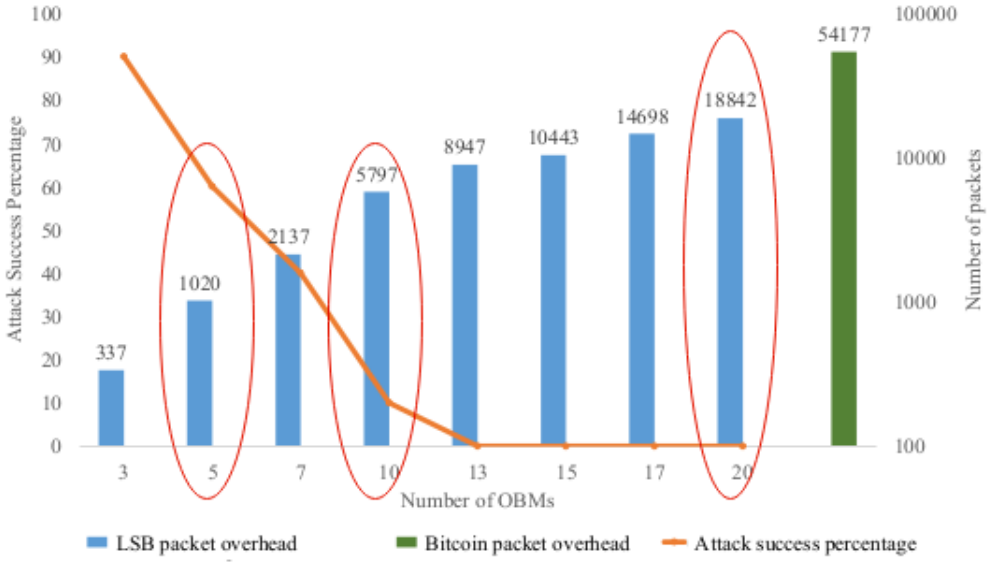
Figura 14 – Quantidade de transações falsas descobertas



Fonte: Elaborada pelo autor

alcançar sucesso, a partir de quinze CH's nenhuma transação falsa conseguiu ser bem sucedida. Observando as áreas destacadas na Figura 15 nota-se uma pequena melhora nos resultados

Figura 15 – Resultados de Dorri para transações falsas



Fonte: (DORRI *et al.*, 2017b)

encontrados, que se deve ao fato do algoritmo de confiança usado neste trabalho usar critérios mais rígidos para aumentar a reputação de um CH.

7 CONSIDERAÇÕES FINAIS

Este trabalho apresenta uma abordagem diferente para segurança de dispositivos inteligente em *smart homes* utilizando uma abordagem semelhante a (DORRI *et al.*, 2017b). No decorrer do trabalho, conseguiu-se atingir os objetivos de: desenvolver um algoritmo de consenso adequado ara IoT e permitir que dispositivos IoT se comuniquem sem a necessidade de uma entidade centralizadora.

Dentro do modelo proposto a organização dos dispositivos, estrutura das *smart homes* e a formação dos CH não puderam ser testados, pela falta de suporte do simulador utilizado e principalmente por questões de tempo. O mais adequado seria simular as *smart homes* usando o simulador Cooja (CONTIKI, 2016), pois este possui recursos já desenvolvidos para simulação de dispositivos IoT. Como trabalho futuro, além da implementação do componente já citado, pode-se melhorar os testes usando o próprio escalonador de eventos no NS3 para coordenar as transações com o intuito de verificar o funcionamento da estrutura de maior cadeia e seus impactos para os resultados já encontrados.

REFERÊNCIAS

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. **Computer networks**, Elsevier, v. 54, n. 15, p. 2787–2805, 2010.

BARCELLOS, A. M. P.; GASPARY, L. P. Segurança em redes p2p: princípios, tecnologias e desafios. In: **Simposio Brasileiro de Redes de Computadores (24.: 2006 maio: Curitiba, PR). Anais dos minicursos. Curitiba:[sn], 2006.** [S.l.: s.n.], 2006.

CHICARINO, V. R.; JESUS, E. F.; ALBUQUERQUE, C. V. de; ROCHA, A. A. d. A. In: **Uso de Blockchain para Privacidade e Segurança em Internet das Coisas**. [S.l.: s.n.], 2017.

CONTIKI. **Contiki**. 2016. Disponível em: <http://www.contiki-os.org/>. Acesso em: 10 Nov. de 2018.

DORRI, A.; KANHERE, S. S.; JURDAK, R.; GAURAVARAM, P. Blockchain for iot security and privacy: The case study of a smart home. In: IEEE. **Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on**. [S.l.], 2017. p. 618–623.

DORRI, A.; KANHERE, S. S.; JURDAK, R.; GAURAVARAM, P. Lsb: A lightweight scalable blockchain for iot security and privacy. **arXiv preprint arXiv:1712.02969**, 2017.

EVANS, D. A internet das coisas: como a próxima evolução da internet está mudando tudo. **CISCO IBSG**, 2011.

FAROOQ, M. U.; WASEEM, M.; KHAIRI, A.; MAZHAR, S. A critical analysis on the security concerns of internet of things (iot). **International Journal of Computer Applications**, Foundation of Computer Science, v. 111, n. 7, 2015.

GERVAIS, A. **Repositório GitHub**. 2016. Disponível em: <https://github.com/arthurgervais/Bitcoin-Simulator.git>. Acesso em: 12 Jun. de 2018.

GUBBI, J.; BUYYA, R.; MARUSIC, S.; PALANISWAMI, M. Internet of things (iot): A vision, architectural elements, and future directions. **Future generation computer systems**, Elsevier, v. 29, n. 7, p. 1645–1660, 2013.

KING, S.; NADAL, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. In: **Self-published paper**. [S.l.: s.n.], 2012. v. 19.

MERKLE, R. C. A digital signature based on a conventional encryption function. In: SPRINGER. **Conference on the Theory and Application of Cryptographic Techniques**. [S.l.], 1987. p. 369–378.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. **Working Paper**, 2008.

ROMAN, R.; ZHOU, J.; LOPEZ, J. On the features and challenges of security and privacy in distributed internet of things. **Computer Networks**, Elsevier, v. 57, n. 10, p. 2266–2279, 2013.

SAHRAOUI, S.; BILAMI, A. Compressed and distributed host identity protocol for end-to-end security in the iot. In: IEEE. **Next Generation Networks and Services (NGNS), 2014 Fifth International Conference on**. [S.l.], 2014. p. 295–301.

SANTAELLA, L.; GALA, A.; POLICARPO, C.; GAZONI, R. Desvelando a internet das coisas. **Revista GEMInIS**, v. 4, n. 2, p. 19–32, 2013.

SINGER, T. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1–15, 2012.

STEGER, M.; DORRI, A.; KANHERE, S. S.; RÖMER, K.; JURDAK, R.; KARNER, M. Secure wireless automotive software updates using blockchains: A proof of concept. In: **Advanced Microsystems for Automotive Applications 2017**. [S.l.]: Springer, 2018. p. 137–149.

TENCENT. **Repositório GitHub**. 2016. Disponível em: <https://github.com/Tencent/rapidjson.git>. Acesso em: 10 Nov. de 2018.

WOOD, G. Ethereum: A secure decentralised generalised transaction ledger. **Ethereum Project Yellow Paper**, v. 151, p. 1–32, 2014.