Universidade Federal de Pernambuco
Centro de Informática

Bacharelado em Ciência da Computação

Análise sobre otimização de Blockchain para Internet das Coisas

Rafael Nunes Machado

Trabalho de Graduação

Recife
14 de dezembro de 2018

Universidade Federal de Pernambuco
Centro de Informática

Rafael Nunes Machado

Análise sobre otimização de Blockchain para Internet das Coisas

Trabalho apresentado ao Programa de Bacharelado em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: *Prof. Paulo André da Silva Gonçalves*

Recife
14 de dezembro de 2018

Imagination will often carry us to worlds that never were, but without it we go nowhere.

—CARL SAGAN

Resumo

A adoção de sistemas de Internet das Coisas vem se expandindo rapidamente, entretanto, apesar de sua grande utilidade, ainda enfrenta desafios relacionados à segurança e privacidade de seus usuários, devido ao amplo compartilhamento de informações sobre suas vidas pessoais. Características intrínsecas desta rede como heterogeneidade de dispositivos, ausência de centralização, grande escala e, consequentemente, grande superfície de ataque amplificam esses problemas. As características propostas no protocolo de redes Blockchain apresentam um grande potencial de usabilidade na indústria de Internet das Coisas, haja vista a necessidade de comunicação entre nós descentralizados de maneira segura e a manutenção da privacidade desta comunicação. Porém as implementações iniciais desse protocolo mostram definições que se tornam inaplicáveis no contexto de IoT devido à falta de poder computacional, necessidade de baixa latência e possibilidade de escalabilidade. Este trabalho realiza um estudo aprofundado sobre as características de redes Blockchain que podem apresentar benefícios a partir de sua implementação em sistemas de Internet das Coisas. Após destrinchar a definição de sistemas de Internet das Coisas e mostrar o funcionamento de redes Blockchain, este trabalho detalha as otimizações realizadas em redes Blockchain para seu uso em diversas aplicações BIoT. Por fim, é descrito o possível futuro para aplicações BIoT e as oportunidades de pesquisas relacionadas através da implementação das arquiteturas apresentadas em cenários reais.

Palavras-chave: Internet das coisas, Blockchain, IoT, BIoT, Smart Contracts, Segurança da Informação, Criptografia

Abstract

Internet of Things adoption is expanding rapidly, however, despite it's high utility, it still faces challenges related to users security and privacy, due to the constant sharing of information about their personal lives. This problems are amplified due to this network's intrinsic characteristics such as devices heterogeneity, descentralization, big scale and attack surface. The Blockchain protocol proposes definitions that could be benefitial to the industry of IoT, whereas the necessity for secure and private comunication between descentralized nodes. However the first implementation of this protocol have shown characteristics that are inapplicable on IoT systems, due to the lack of CPU power, necessity for low latency and high escalabity. This project studies the characteristics of the Blockchain protocol that could bring benefits through its implementation in IoT systems. After defining Internet of Things systems and mentioning the workflow of the Blockchain protocol, the optimizations on the Blockchain protocol for its use on BIoT applications are described. Finally, it is mentioned the possible future for BIoT applications and the related research opportunities in the implementation of the presented architectures on real case scenarios.

Keywords: Internet of Things, Blockchain, IoT, BIoT, Smart Contracts, Information Security, Cryptography

Sumário

Lista de Figuras

Lista de Tabelas

CAPÍTULO 1

Introdução

Neste capítulo será explicada a motivação por trás da temática escolhida e o contexto em que o campo de estudo atual se encontra. Na seção 1.1 encontra-se o contexto e motivação de estudo, na seção 1.2 encontram-se descritos os objetivos deste projeto e, por fim, na seção 1.3 encontra-se uma breve estruturação das seções escritas neste documento.

1.1 Contexto e motivação

A Internet das Coisas (do inglês, Internet of Things - IoT) é definida como uma rede que conecta uma coleção de dispositivos com identificadores únicos com a Internet (1). Estes dispositivos apresentam características de sensores ou tomadores de decisões e possuem potencial de mutabilidade programacional. Desta forma, através do identificador único e das propriedades de sensores, é possível coletar informações sobre o dispositivo e realizar operações de alteração no seu estado a partir de qualquer lugar, em qualquer momento, por outro dispositivo.

A adoção de sistemas de Internet das Coisas vem se expandindo rapidamente e, em algumas previsões, estima-se que o número de dispositivos IoT alcance a 26 bilhões por volta do ano de 2020 (2) (o equivalente à 30 vezes o número de dispositivos estimados existentes em 2009). Além disso, há previsões do crescimento de comunicações entre máquinas - sem envolvimento humano - de 780 milhões em 2016 para 3.3 bilhões até 2021 (2), o que pode estar relacionado às indústrias de casas inteligentes, transporte, defesa e segurança pública, vestimentas e realidade aumentada. Desta forma, é imprescindível construir protocolos e arquiteturas que proporcionem camadas apropriadas para os serviços consumidos e disponibilizados por dispositivos IoT através da Internet.

Apesar de sua grande utilidade, a Internet das Coisas levanta problemas relacionados à segurança e privacidade de seus usuários, visto o amplo compartilhamento de informações sobre suas vidas pessoais para possibilitar tomadas de decisões. Características intrínsecas desta rede como heterogeneidade de dispositivos, ausência de centralização, grande escala e, consequentemente, grande superfície de ataque amplificam esses problemas (3).

Blockchain foi o termo empregado para um sistema de blocos encadeados criptograficamente de maneira segura. Esta tecnologia pode ser considerada a base para o funcionamento do Bitcoin e outras criptomoedas existentes atualmente. O protocolo proposto em (4) tinha como objetivo propor uma rede peer-to-peer de pagamentos onde não fosse necessária a validação de transações por uma entidade confiável e centralizada. Entretanto a tecnologia de Blockchain é adaptável de forma a extinguir a centralização em cenários de indústrias financeiras, hospitalares, de utilidades, imobiliárias e governamentais. Com o uso da nova tecnologia é

possível executar operações - que previamente só eram possíveis através do intermédio de uma autoridade central - de uma forma descentralizada, sem intermediários e com o mesmo grau de confiança.

As características propostas no protocolo de redes Blockchain apresentam um grande potencial de usabilidade na indústria de Internet das Coisas, visto a necessidade de comunicação entre nós descentralizados de maneira segura e a manutenção da privacidade desta comunicação. A segurança no sistema do Bitcoin pode ser relacionada principalmente à necessidade de resolução de um desafio criptográfico, chamado de Proof-of-Work, para que novos blocos de transações sejam adicionadas à rede Blockchain. Do ponto de vista de privacidade, a identidade dos usuários que realizam transações é definida por uma chave pública potencialmente mutável, o que aumenta a proteção a respeito da origem dos dados.

Entretanto, o protocolo inicial de redes Blockchain foi desenvolvido com o intuito de solucionar um problema monetário e, portanto, possui definições que tornam-se inaplicáveis no mundo da Internet das Coisas (3). Dentre definições que podem vir a ser impraticáveis para esta rede, pode-se listar as seguintes:

- Alta necessidade de recursos computacionais para validação de transações através do modelo de Proof-of-Work;
- Alta latência devido aos mecanismos aplicados para evitar que usuários utilizem a mesma moeda em transações distintas;
- Problemas de escalabilidade relacionadas à quantidade de mineiros na rede e a necessidade de atingir o consenso entre os mesmos.

Apesar dos desafios de implementação no contexto de Internet das Coisas, novas criptomoedas e arquiteturas vêm sendo propostas com tecnologias que mitigam alguns dos problemas descritos. O protocolo Ripple, por exemplo, foi criado com o intuito de aumentar a velocidade e diminuir o custo da validação de transações através da substituição do protocolo de Proof-of-Work por um novo algoritmo de consenso entre os nós verificadores distribuídos (5). Outro exemplo, é a criptomoeda IOTA que propôs um novo sistema - aprimorado a partir do Blockchain - chamado The Tangle (6). Este, por sua vez, apresenta uma proposta de possibilitar microtransações de moedas para compra e venda de informações entre dispositivos conectados na Internet das Coisas.

1.2 Objetivos

Este trabalho visa um estudo aprofundado sobre as características de redes Blockchain que podem apresentar benefícios a partir de sua implementação em redes de Internet das Coisas. Desta forma, o objetivo geral deste projeto é analisar a aplicabilidade de redes Blockchain para o contexto de Internet das Coisas.

Os objetivos específicos deste projeto são os seguintes:

- Categorizar os desafios de sistemas de Internet das Coisas que podem se beneficiar da uso de redes Blockchain;

- Destacar os problemas associados e possíveis pontos de falha das arquiteturas de redes Blockchain;
- Analisar as arquiteturas de otimização de redes Blockchain propostas para solucionar os desafios de Internet das Coisas;

1.3 Estrutura do trabalho

Este trabalho encontra-se catalogado em quatro capítulos. No segundo capítulo são detalhadas a definição do que pode ser definido como Internet das Coisas, assim como os desafios do ponto de vista tecnológico e de segurança enfrentados por sistemas dessa natureza. No terceiro capítulo é descrito o funcionamento de redes Blockchain e os protocolos de consenso distrubuído mais comumente utilizados. Além disso também são descritos os tipos de redes Blockchain e os desafios de escalabilidade e segurança enfrentados por essa tecnologia emergente. No quarto capítulo é mostrado as áreas que já mostram alguma adoção da tecnologia de Blockchain acerca sistemas de Internet das Coisas e as otimizações realizadas nas arquiteturas de redes Blockchain para a solução de alguns dos desafios de sistemas IoT. Por fim, no capítulo cinco encontram-se as conclusões desse trabalho.

CAPÍTULO 2

Internet das coisas (Internet of Things)

A Internet das Coisas (do inglês, Internet of Things (IoT)) é uma tecnologia emergente que vem sendo vista como o futuro da sociedade do ponto de vista de gerenciamento e autonomia de dispositivos. Entretanto, preocupações como a segurança de seus usuários e escalabilidade na comunicação autônoma têm estimulado pesquisas sobre novas formas de estruturar e proteger redes dessa natureza (7). A primeira seção deste capítulo será direcionada para definir o que pode ser considerado como Internet das Coisas, enquanto na seção 2.2 serão explicados as definições de escopo de sistemas IoT possibilitanto a distinção entre cenários pequenos e grandes. Por fim, na seção 2.3 serão destrinchadas algumas das dificuldades enfrentadas por estas redes nos âmbitos de autenticação de dispositivos, segurança, anonimização, escalabilidade e poder computacional para processamento de informações.

2.1 A Definição de Internet das Coisas

É comum encontrar definições distintas do que é a Internet das Coisas (Internet of Things) em artigos acadêmicos de acordo com o ciclo temporal em que os mesmos foram escritos. Devido a isso, Minerva, Biru e Rotondi(1) buscaram desenvolver uma definição neutra que englobe todos os tipos de redes presentes no espectro da Internet das Coisas. De acordo com Minerva, Biru e Rotondi(1), as redes que são comumente definidas como Internet das Coisas são os sistemas cyber-físicos e as redes de sensor sem fio.

2.1.1 Sistemas cyber-físicos

Esta categoria pode ser descrita como um sistema de dispositivos que controlam entidades físicas. São sistemas mecânicos e elétricos (como sensores e meios físicos de comunicação) inseridos em produtos ou materiais que se comunicam através de uma rede utilizando componentes de software. O objetivo desses sistemas é a tomada de decisões independentes e individuais para controle de sistemas de produção ou logística a partir de informações compartilhadas entre os dispositivos. Desta forma, esse tipo de rede possui características que vão além do mínimo que pode ser descrito como Internet das Coisas, haja vista que é um sistema de comunicação entre dispositivos conhecidos que partilham informações para atingir um certo objetivo final com maior eficiência.

2.1.2 Redes de sensor wireless

As redes de sensor wireless são compostas por sensores autônomos que monitoram condições físicas ou de ambiente (como som, temperatura, pressão, etc.) e, de forma cooperativa, transmitem essas informações através da Internet para uma central de processamento. Estas redes possuem diversos nós, onde cada um destes é conectado a um ou vários sensores. O objetivo principal desse tipo de sistema é a coleta coordenada de informações.

2.1.3 Sistemas de IoT

Por mais que os sistemas cyber-físicos e de redes de sensor wireless se encaixem como parte da Internet das Coisas, há outros tipos de redes que não encontram-se contempladas por essas especificações, entretanto também são categorizadas como IoT. Devido a isso, Minerva, Biru e Rotondi(1) definiram as seguintes características necessárias para que uma rede possa ser categorizada como parte da Internet das Coisas:

Interconexão entre os dispositivos: A primeira característica de IoT, e uma das mais importantes, é a de interconexão entre as diversas C̈oisasc̈onectadas à rede. Estas C̈oisass̈ão definidas como quaisquer dispositivos físicos relevantes para a perspectiva do usuário ou aplicação.

Conexão dos dispositivos com a Internet: Outra característica inerente ao sistema é a conectividade dos dispositivos presentes na rede à Internet.

Dispositivos unicamente identificáveis: O sistema deve ser composto por dispositivos que podem ser diferenciados a partir de um identificador único.

Ubiquidade: Esta característica define a necessidade de que a rede esteja disponível a qualquer momento e a partir de qualquer lugar. Entretanto essa disponibilidade não necessariamente precisa ser em qualquer lugar global e nem a qualquer hora do dia. Esse conceito aplica-se a disponibilidade em qualquer lugar onde o dispositivo é necessário e a qualquer momento em que é preciso.

Capacidade sensorial ou de atuação: Sensores ou tomadores de decisão devem estar conectados aos dispositivos que fazem parte da rede de Internet das Coisas. Esta característica é a que a agrega a inteligência presente neste tipo de rede.

Inteligência embutida: Presença de dispositivos dinâmicos e inteligentes com comportamento independente e funções de processamento com o intuito de estender as capacidades humanas.

Capacidade de comunicação interoperacional: O sistema deve ter um protocolo de comunicação interoperacional baseado nos padrões definidos para que seja possível a comunicação com outras redes IoT.

Configuração própria independente: Esta característica é crucial para redes IoT devido a grande heterogeneidade de dispositivos presentes neste tipo de rede como sensores, tomadores de decisão, dispositivos de armazenamento, celulares, dispositivos de monitoramento, etc. Desta forma, o direcionamento natural é que os dispositivos conectados à estas redes se gerenciem e se configurem independentemente nos âmbitos de utilização de recursos (energia, banda de comunicação, etc) e configuração de hardware/software. A configuração própria independente consiste principalmente nas ações de descoberta de serviços na rede, organização de rede e disponibilidade de serviços e recursos.

Programabilidade: A programabilidade é outra característica requerida por redes dessa natureza. Deve ser possível a mutação de uma variedade de comportamentos do dispositivo a partir de comandos do usuário sem que sejam necessárias alterações físicas no dispositivo.

2.2 Escopo de sistemas de Internet das Coisas

Sistemas de Internet das Coisas podem apresentar variações no tamanho do escopo englobando desde pequenos sistemas compostos por alguns sensores e dispositivos unicamente identificáveis até redes massivas contendo milhões de dispositivos com a capacidade de prover serviços extremamente complexos (Figura 2.1). Desta forma, Minerva, Biru e Rotondi(1) categorizam sistemas IoT em dois tipos a partir de seu escopo: cenários pequenos e grandes.

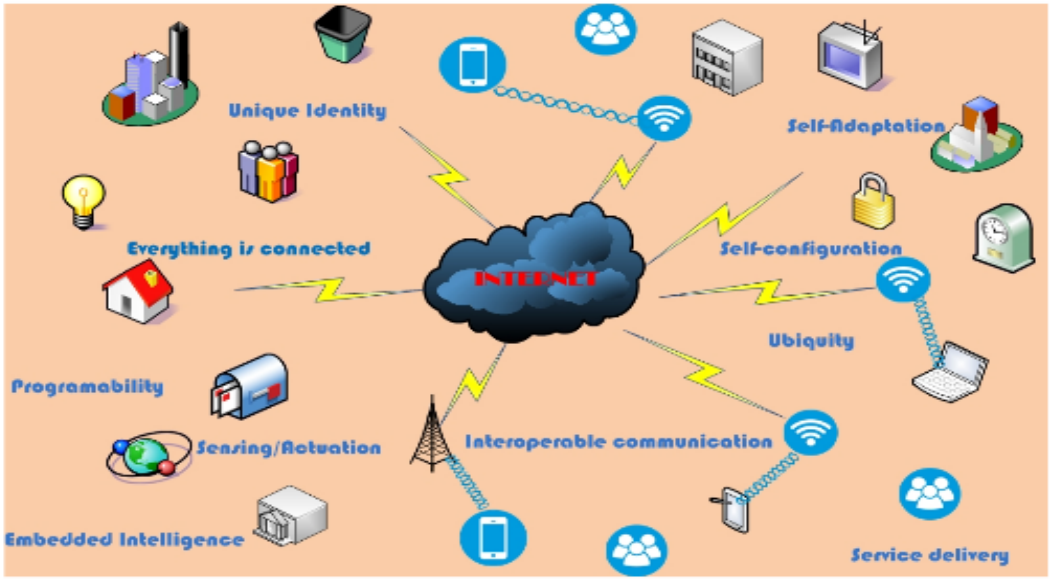

Figura 2.1 Cenário grande de escopo de Sistema IoT. Fonte: Artigo (1)

O contexto em que o menor sistema IoT possível pode ser criado consiste em apenas um dispositivo unicamente identificável conectado à Internet. Neste cenário de baixa complexidade, o dispositivo pode estar conectado a um sensor ou atuador e possuir a possibilidade de

programabilidade para atender as características definidas na seção anterior. Entretanto, contextos dessa natureza não trazem grandes dificuldades em sua implementação e gerenciamento, pois normalmente são gerenciados por um único domínio administrativo (1).

Os problemas relacionados às redes de Internet das Coisas surgem a partir do crescimento da complexidade destas redes no momento em que milhões de dispositivos passam a fazer parte de uma mesma rede IoT. No contexto de um cenário grande, as redes de Internet das Coisas possuem diversos domínios administrativos que nem sempre possuem ligações explícitas entre si para que os próprios dispositivos sejam capazes de se comunicar mais facilmente. Neste contexto, a complexidade torna-se exponencial ao ponto em que elementos como escalabilidade, lógica distribuída e segurança tornam-se essenciais.

2.3 Desafios de segurança na Internet das Coisas

Apesar de sua grande utilidade, a Internet das Coisas levanta problemas relacionados à segurança e privacidade de seus usuários, haja vista o amplo compartilhamento de informações sobre suas vidas pessoais para possibilitar a tomada de decisões. Além disso, características intrínsecas desta rede como heterogeneidade de dispositivos, restrições de poder computacional e energia, ausência de centralização, grande escala e, consequentemente, grande superfície de ataque amplificam o desafio de manter a segurança nestas redes. Em 2016 houve relatos de ataques massivos de negação de serviço contra diversas instituições a partir de uma Botnet chamada Mirai. Estima-se que esta Botnet era constituída por 233 mil dispositivos IoT, enquanto outra Botnet chamada Bashlight era estimada como controladora de 963 mil dispositivos IoT (8). O impacto causado devido ao comprometimento de sistemas de Internet das Coisas resultaram em ataques massivos e perdas de milhares de dólares com problemas de disponibilidade de serviços.

Os problemas levantados em redes IoT podem ser divididos em duas categorias: desafios tecnológicos e desafios de segurança (9). Os desafios tecnológicos podem ser descritos como limitações relacionadas à protocolos de comunicação sem fio, escalabilidade, consumo de energia e a natureza distribuída da rede. Em contrapartida os desafios de segurança podem ser definidos como as preocupações acerca da garantia na autenticação de dispositivos, confidencialidade na comunicação, integridade nas informações trocadas entre dispositivos, etc.

No momento de implementação de qualquer tipo de sistema, inclusive redes de Internet das Coisas, os princípios básicos de segurança da informação devem ser levados em consideração. Estes princípios podem ser divididos da seguinte forma (10):

- Confidencialidade
- Integridade
- Disponibilidade

2.3.1 Confidencialidade

O princípio da confidencialidade é a garantia de que apenas usuários ou dispositivos autorizados devem ter acesso à informação (11).

É imprescindível garantir a confidencialidade dos dados trafegados na rede de forma que apenas dispositivos autorizados sejam capazes de receber as informações enviadas. Além disso, também é necessário garantir que dispositivos de uma rede não revelem informações para outros dispositivos vizinhos de forma não autorizada (por exemplo dados coletados por um sensor sendo visualizados por outro sensor da mesma rede).

Devido ao baixo poder computacional associado à heterogeneidade de redes dessa natureza, um dos desafios da manutenção desse princípio estão ligados à necessidade de desenvolvimento de algoritmos de encriptação de dados e sistemas de gerenciamento das chaves destes algoritmos que não necessitam de muito poder de processamento. Outro desafio é o desenvolvimento de protocolos únicos - que podem ser implementados em qualquer dispositivo que seja classificado como parte da Internet das Coisas - para garantir a forma como as informações serão gerenciadas, armazenadas, protegidas e trafegadas na rede de maneira eficiente (9).

2.3.2 Integridade

O princípio da integridade afirma que adulterações, modificações ou exclusões dos dados devem ser realizadas apenas por usuários ou dispositivos autorizados (11).

Sistemas IoT são baseados na constante troca de informações entre dispositivos, o que salienta a importância da garantia de que os dados fornecidos sejam legítimos para que o objetivo do sistema seja alcançado. Desta forma, no quesito de integridade, é necessário que as trocas de informações entre os diversos dispositivos seja confiável ao nível em que os dados trafegados entre os mesmos não sejam adulterados no canal de comunicação por motivos intencionais ou não. A manutenção do princípio de integridade pode ser interpretada como a garantia de segurança fim a fim entre dispositivos em redes IoT.

O controle do tráfego normalmente é gerenciado através de firewalls e protocolos de comunicação, entretanto, por motivos de baixo poder computacional e heterogeneidade dos dispositivos presentes em redes dessa natureza, a garantia desse princípio nas informações presentes nos próprios dispositivos torna-se um desafio (9).

2.3.3 Disponibilidade

O princípio da disponibilidade descreve que o acesso às informações deve estar disponível para usuários ou dispositivos autorizados sempre que for necessário (11).

O princípio de segurança da informação de disponibilidade entra em sintonia com uma das características intrínsecas de sistemas de Internet das Coisas que é a ubiquidade. De forma a atingir as expectativas quanto a sistemas IoT, é importante que tanto as informações quanto o acesso aos próprios dispositivos estejam disponíveis para usuários autorizados sempre que forem necessários.

2.3.4 O desafio da autenticação e autorização de dispositivos

Apesar de não ser considerado como um princípio da segurança da informação, a autenticação de dispositivos em sistemas de Internet das Coisas também pode ser considerada um dos principais requisitos para a manutenção da segurança nestes sistemas. Os princípios da segurança da informação salientam a necessidade de sempre fornecer, alterar e disponibilizar informações e serviços para dispositivos ou usuários autenticados (10). Entretanto, no contexto de sistemas de Internet das Coisas em que dispositivos possuem maleabilidade em sua localização e são gerenciados de forma descentralizada, criar ou adotar mecanismos de identificação e garantia de que dispositivos realmente são quem eles afirmam ser tornam-se desafios complexos (9).

A existência de diversos dispositivos heterogêneos descentralizados culmina na recorrente necessidade de interações iniciais entre dispositivos que nunca se comunicaram previamente. A partir disso, o desenvolvimento de mecanismos capazes de autenticar dispositivos mutuamente em cada interação torna-se imprescindível para a proteção do sistema contra usuários mal intencionados ou dispositivos defeituosos. Falhas na implementação destes mecanismos podem resultar na quebra dos princípios de segurança e, consequentemente, na violação da privacidade de usuários ou na manipulação indevida de dados cruciais para o funcionamento de sistema críticos.

2.4 Resumo

Devido a aspectos temporais, há artigos acadêmicos que possuem definições distintas no que se refere à Internet das Coisas o que termina por limitar redes desta natureza a tipos de rede que encontram-se englobadas no espectro de IoT como sistemas cyber-físicos e redes de sensores sem fio. Sistemas da Internet das Coisas podem ser definidas como redes que atendem aos requisitos de interconexão entre os dispositivos, conexão dos dispositivos com a Internet, dispositivos unicamente identificáveis, ubiquidade, capacidade sensorial ou de atuação, inteligência embutida, capacidade de comunicação interoperacional, configuração própria ou independente e programabilidade.

Sistemas IoT podem ser compostos por apenas um dispositivo ou milhões e, portanto, seu escopo pode ser dividido em cenários pequenos e cenários grandes. As maiores dificuldades identificadas em sistemas de Internet das Coisas encontram-se nos cenários grandes, onde problemas como escalabilidade, lógica distribuída e segurança tornam-se exponencialmente complexos.

Os desafios encontrados em sistemas de Internet das Coisas podem ser divididos em duas categorias: desafios tecnológicos e desafios de segurança. O primeiro pode ser descrito como desafios de escalabilidade, canais de comunicação sem fio, etc. Enquanto o segundo pode ser exemplificado como as dificuldades na autenticação de dispositivos, integridade, confidencialidade e disponibilidade de dispositivos na rede.

Ao destrinchar os desafios de segurança em redes de Internet das Coisas é imprescindível levar em conta a forma como os princípios de segurança da informação são tratados nesse contexto. Os três princípios são confidencialidade, integridade e disponibilidade que podem ser descritos, respectivamente, como:

- Garantia de que apenas usuários ou dispositivos autorizados possuam acesso às informação.
- Adulterações, modificações ou exclusões de dados devem ser realizadas apenas por usuários ou dispositivos autorizados.
- O acesso às informações deve estar disponível para usuários ou dispositivos autorizados sempre que for necessário.

Por fim, para garantir que os princípios da segurança da informação sejam aplicados, a definição de que dispositivos são autorizados a acessar, visualizar e realizar alterações em informações é crucial. Esta autenticação torna-se um desafio em sistemas dessa natureza devido a grande heterogeneidade de dispositivos presentes na rede de forma descentralizada que resulta na realização de interações iniciais constantes entre dispositivos que nunca se comunicaram.

CAPÍTULO 3

Blockchain

Blockchain foi o termo empregado para um sistema de blocos encadeados criptograficamente de maneira segura. Esta tecnologia pode ser considerada a base para o funcionamento do Bitcoin e outras criptomoedas existentes atualmente. No contexto do protocolo do Bitcoin, a utilização de Blockchain tem como objetivo final propor uma rede peer-to-peer de pagamentos onde não fosse necessária a validação de transações por uma entidade confiável e centralizada (4). Desta forma, as validações deixam de ser feitas a partir de confiança e são substituídas por provas criptográficas que possibilitam a transações entre duas partes sem a necessidade de que uma terceira parte confiável esteja envolvida. Na seção 3.1 é destrinchado o funcionamento de sistemas Blockchain, assim como seus protocolos de consenso distribuído, enquanto na seção 3.2 é descrita a tecnologia de Smart Contracts que foi adicionada à algumas redes Blockchain mais recentes como o Ethereum. Na seção 3.3 são comentados os tipos de Blockchain existentes de acordo com disponibilidade ao público e permissionamento de nós e na seção 3.4 são descritas os principais desafios que redes Blockchain enfrentam nos quesitos de segurança, escalabilidade e custo computacional.

3.1 Funcionamento de sistemas Blockchain

Apesar de muitas vezes ser associado puramente à criptomoeda Bitcoin, o sistema de Blockchain pode ser utilizado em diversas áreas de aplicação com algumas variações em sua implementação. Como o protocolo do Bitcoin foi desenvolvido com o intuito de criar uma rede de pagamentos descentralizados, há algumas características associadas a ele que não são imprescindíveis para sistemas Blockchain, entretanto foram adicionadas para aumentar a robustez da rede monetária.

3.1.1 Identidade e Privacidade

Os usuários da rede Blockchain são definidos por um par de chaves criptográficas: uma pública e uma privada. A chave pública é a que representa a carteira do usuário, enquanto a chave privada é a que possibilita a assinatura de transações desta carteira para uma carteira nova. O uso dessas chaves é baseado no conceito de criptografia assimétrica, onde a chave privada de um usuário pode ser utilizada para assinar digitalmente algum dado - que pode ser facilmente verificado com chave pública - ou decifrar informações que foram cifradas com a chave pública do usuário (12). Desta forma, a chave privada age como uma identidade do usuário de modo que qualquer dispositivo que possua a chave pública associada ao usuário pode verificar as

assinaturas geradas por ele e pode cifrar informações para ele.

Do ponto de vista de identidade e privacidade, usuários são anônimos aos olhos do sistema, haja vista que um novo par de chaves pode ser criado a qualquer momento para qualquer usuário. Entretanto, como todas as transações da rede podem ser consultadas, ao conhecer a chave pública de um usuário, é possível visualizar todo o histórico de transações registradas daquela carteira específica.

3.1.2 Transações de informações

Antes de explicar como funcionam as transações, é importante definir o que são as moedas que serão transacionadas. Uma moeda pode ser definida como um conjunto de informações digitalmente assinadas por um usuário com sua chave privada representando que este é o dono daquela moeda no momento de sua criação. No caso do Bitcoin, esta informação representa uma quantidade.

As transações são definidas como uma cadeia de assinaturas digitais. Cada dono de moeda a transmite para outro usuário através da assinatura digital do hash da transação anterior desta moeda e da chave pública do usuário para quem a moeda está sendo enviada (Figura 3.1).

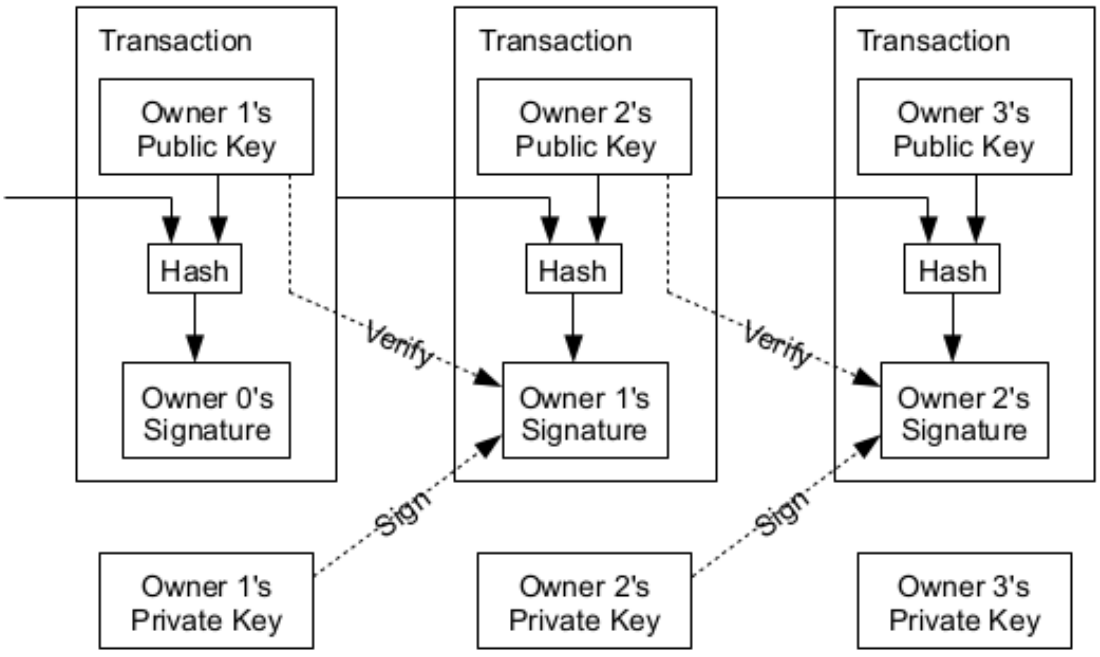

Figura 3.1 Exemplo de cadeia de blocos de transações. Fonte: Artigo (4)

Qualquer usuário com acesso à Internet pode verificar as assinaturas presentes na transação para validar se a moeda foi de fato transferida. Especificamente para o caso de dinheiro digital, como em criptomoedas, é impraticável que as transações sejam feitas através da menor unidade de moeda para possibilitar a maleabilidade nos valores transferidos. Desta forma, as transações

têm como entrada a quantidade total de moedas de um usuário e como saída dois valores: a quantidade de moedas que serão transferidas e a quantidade de moedas que serão retornadas para o usuário que está realizando a transação. Por fim, para realizar uma transação, o usuário deve enviá-la para a rede para que esta seja propagada para todos os nós que deverão validar e adicionar a transação à cadeia de blocos.

3.1.3 Protocolo distribuído de consenso

Por se tratar de um sistema distribuído, o Blockchain requer que um protocolo de consenso distribuído seja utilizado para que os blocos de transação sejam adicionados corretamente à cadeia de blocos. Este protocolo é o responsável por garantir que usuários maliciosos não insiram transações indevidas e fraudulentas no histórico de transações, portanto tem o intuito de garantir a corretude do sistema.

Os protocolos distribuídos tentam solucionar o Problema dos Generais Bizantinos que é descrito como a dificuldade de confiar nas decisões em grupo de generais que podem ser potencialmente maliciosos (13). Neste problema o império bizantino decide conquistar uma cidade e possui N exércitos liderados por N generais. Para conseguir conquistar a cidade com sucesso, todos os exércitos devem atacar ao mesmo tempo. Ao receber o comando de atacar ou recuar, os generais devem transmitir essa informação para os generais mais próximos à eles. Entretanto, alguns generais são infiltrados do inimigo e podem passar a informação errada para os generais mais próximos. Desta forma, a definição deste problema é a dificuldade de se atingir um consenso descentralizado sobre algo entre diversas pessoas que nem sempre são totalmente confiáveis.

Com o passar do tempo, diversos protocolos de consenso foram desenvolvidos com o intuito de otimizar cada vez mais a validação das transações. Os protocolos mais aceitos e amplamente utilizados atualmente são: Proof-of-Work e Proof-of-Stake.

3.1.3.1 Proof-of-Work

O algoritmo de Proof-of-Work foi o escolhido para ser utilizado em algumas criptomoedas, como o Bitcoin e, inicialmente, o Ethereum. Este algoritmo se baseia no conceito de que o nó que validará as transações presentes no próximo bloco da cadeia deve demonstrar uma prova do seu trabalho através de poder computacional.

Este algoritmo envolve a busca por um valor que, quando aplicado uma função de hash (como SHA-256), resulte em um hash que tenha um formato predeterminado. No caso do Bitcoin, é requerido que o hash se inicie com um número pré-determinado de bits 0 (4). O trabalho médio é exponencial ao número de bits 0 necessários e, para verificar se o trabalho realizado é válido, basta uma única operação de hash para validar o resultado. A modificação do hash resultante de um bloco se dá através da variação de um parâmetro arbitrário presente nos blocos chamado Nonce (Figura 3.2). Uma vez que todo o trabalho tenha sido executado, não há como alterar as informações presentes no bloco sem que todo o trabalho tenha que ser refeito.

A abordagem de Proof-of-Work também soluciona o problema de determinar o consenso da maioria da rede. Se a decisão de consenso for baseada em um voto pra cada endereço IP, um

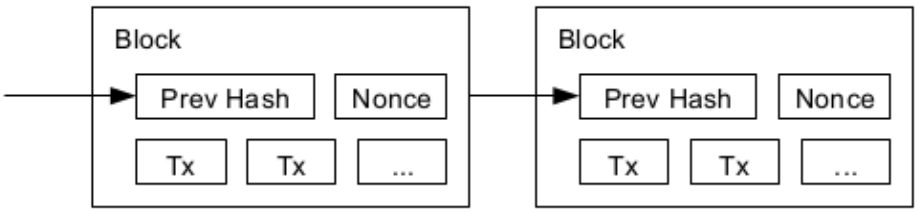

Figura 3.2 Blocos gerados em rede Blockchain baseada em Proof-of-Work. Fonte: Artigo (4)

atacante que pudesse alocar a maior quantidade de IPs teria o maior poder de decisão dentro da rede. No contexto de Proof-of-Work, cada CPU capaz de processar informações corresponde a um voto na rede. A decisão da maioria na rede sobre quais transações são válidas é representada pela cadeia de bloco mais longa e, portanto, é a que prevalece nas decisões tomadas pelos nós sobre os próximos blocos a serem adicionados na cadeia.

Um atacante que quisesse alterar um bloco passado teria que refazer o trabalho para a criação do novo bloco e refazer todos os blocos subsequentes à ele até que esta cadeia maliciosa se tornasse uma cadeia maior do que a cadeia sendo computada por nós honestos. Sendo assim, a corretude da cadeia de blocos só pode ser afetada caso um atacante possua a maioria do poder computacional da rede (51%). Nesse cenário, o atacante seria capaz de produzir blocos fraudulentos mais rápido do que os nós honestos da rede poderiam construir blocos legítimos e, como a maior cadeia sempre prevalece, o atacante seria capaz de fraudar transações com sucesso.

Para compensar o sempre crescente poder computacional de CPUs e a variação de quantidade de nós que estão validando transações, a dificuldade do trabalho é determinada por uma média de números de blocos por hora. Desta forma, caso estejam sendo gerados mais blocos do que a média por hora, a dificuldade aumenta e vice-versa.

Em redes monetárias como o Bitcoin, os nós que validam as transações recebem incentivos monetários ao adicionar novos blocos na cadeia. A primeira transação de um novo bloco adicionado é considerada uma transação especial, onde são criadas novas moedas que são transferidas para a carteira do nó criador do bloco. Além das moedas da transação especial, o nó que criou o bloco também tem o direito de coletar as taxas de transferência das transações presentes neste bloco. Os usuários da rede que enviam taxas de transferência maiores têm suas transações confirmadas e validadas mais rapidamente devido à coleta dessas taxas por parte dos nós que validam as transações.

3.1.3.2 Proof-of-Stake

O Proof-of-Stake foi criado com o intuito de solucionar algumas das dificuldades presentes no PoW como o alto custo de energia para manutenção do funcionamento do sistema. Neste algoritmo alternativo, os nós que desejam validar transações devem comprovar a posse de moedas para poder ter a chance de adicionar o próximo bloco na cadeia.

O PoS funciona através do envio de uma transação especial que bloqueia as moedas enviadas pelos nós validadores durante o processo de consenso (14). Em seguida, a criação e

concordância entre os nós validadores sobre qual será o próximo bloco adicionado à cadeia é feita a partir de um algoritmo de consenso, portanto existem diversas variações do Proof-of-Stake. Os dois algoritmos mais utilizados são: Chain-Based Proof-of-Stake e BFT-Style Proof-of-Stake (14).

No Chain-Based Proof-of-Stake um validador é escolhido a cada período de tempo de forma pseudo-aleatória para criar um novo bloco com a referência de um bloco anterior (normalmente o último bloco da maior cadeia prévia). Sendo assim, com o passar do tempo, a maioria dos blocos convergem em uma cadeia principal crescendo constantemente.

Em BFT-Style Proof-of-Stake os validadores são aleatoriamente encarregados de propor blocos, entretanto o consenso de quais blocos deverão ser adicionados à cadeia é feito de acordo com um processo de múltiplos turnos onde cada validador vota em um bloco para ser adicionado à cadeia. No final do processo, todos os validadores honestos e online concordam se o bloco final escolhido é parte da cadeia ou não.

O consenso através de algoritmos Proof-of-Stake se suporta a partir das penalidades caso algum atacante queira fraudar a rede. Nós validadores submetem moedas próprias para serem trancadas durante o processo de validação e, caso um nó validador tente fraudar o processo, suas moedas são descartadas. Se não for identificado nenhum tipo de tentativa de fraude de um nó validador, este é recompensado com uma quantidade de moedas em retorno. Desta forma, ao contrário do PoW - que funciona através da ideologia de segurança a partir do poder computacional e queima de energia - a segurança de sistemas que utilizam PoS vem do potencial econômico colocado em risco (15).

Teoricamente em sistemas PoS é possível que os nós validadores se juntem para ter a maioria da rede e poder fraudar transações (51% do dinheiro dos nós validadores). Entretanto, em cenários em que nós maliciosos comecem a fraudar transações, a comunidade pode realizar um hard-fork da rede Blockchain e remover os depósitos realizados pelos atacantes. Desta forma, os nós validadores maliciosos irão perder todo o dinheiro que foi colocado à risco para realizar as validações e a comunidade será capaz de se recuperar do ataque rapidamente (15).

3.2 Smart Contracts

O Ethereum foi a primeira criptomoeda a implementar o conceito de Smart Contracts com o intuito de potencializar as capacidades de uma rede Blockchain garantindo a autonomia de transações a partir de cláusulas previamente acordadas entre usuários.

Smart Contracts são definidos como um protocolo de transação computadorizado que executa os termos de um contrato preestabelecido (16). Estes contratos traduzem as cláusulas contratuais em um software ou hardware que tem a capacidade de garantir que as cláusulas serão cumpridas sem a necessidade de um intermediário entre as duas partes do contrato e garantem a robustez contra exceções acidentais ou ocorrência de atividades maliciosas.

No contexto de Blockchain, Smart Contracts são scripts armazenados na rede. Estes contratos são análogos à stored procedures no contexto de bases de dados relacionais. Como esses scripts encontram-se armazenados na rede de Blockchain, eles possuem uma chave pública própria que os identificam para os usuários. Para ativar a execução de um contrato desta natureza, é necessário realizar uma transação para seu endereço (sem necessariamente enviar moedas, a

depender das cláusulas do contrato). Após a realização da transação, o contrato é executado independentemente e automaticamente de acordo com suas cláusulas e seu resultado é propagado pela rede. Desta forma, a partir do desenvolvimento de Smart Contracts é possível realizar processamentos e transações na rede de forma autônoma para objetivos variados. Através desta tecnologia, usuários são capazes de firmar um contrato que só será cumprido quando certas circunstâncias definidas forem atingidas (16).

Como os Smart Contracts têm endereços próprios, eles também têm a capacidade de armazenar ou transferir moedas. Um dos exemplos de uso de Smart Contracts seria a criação de um contrato responsável por transferir uma propriedade para a primeira pessoa que pagasse R$10.000 pro seu dono. Neste contrato, quando a função de transferir propriedade fosse executada com o envio de R$ 10.000, este dinheiro seria enviado para a carteira do vendedor e ao mesmo tempo o registro de propriedade que está sendo vendida seria automaticamente transferida para a carteira do usuário que realizou a transferência. Todo esse processo seria realizado sem a necessidade de uma terceira entidade para firmar a confiança entre os dois participantes do contrato e todas as cláusulas do contrato estariam definidas publicamente na rede Blockchain, podendo ser facilmente verificadas pelas duas partes.

3.3 Tipos de Blockchain

Existem modelos distintos de implementação de redes Blockchain que são escolhidos de acordo com as informações presentes, a disponibilidade dos dados e em que ações podem ser realizadas pelos usuários da rede (2). Estes modelos podem variar entre público ou privado e com permissionamento ou sem permissionamento. É importante ressaltar que alguns autores tratam os modelos público/sem permissionamento e privado/com permissionamento como sendo sinônimos, entretanto, por mais que isso seja coerente para redes Blockchain de criptomoedas, não é o caso para os cenários de uso de Blockchain em Internet das Coisas. Nos cenários de IoT é importante distinguir entre autenticação (quem pode acessar a rede: privado ou público) e autorização (que ações dispositivos IoT podem executar na rede: sem permissionamento ou com permissionamento)(2). Entretanto, estes conceitos ainda encontram-se em debate e podem diferir na literatura entre trabalhos distintos. A Tabela 3.1 exibe algumas características de cada um dos tipos.

	Com permissionamento	**Sem permissionamento**
Pública	Qualquer usuário pode fazer parte da rede, entretanto apenas determinados nós podem validar transações	Qualquer usuário pode fazer parte da rede e atuar como um nó validador
Privada	Acesso restrito à usuários predeterminados e apenas nós específicos podem validar transações	Acesso restrito à usuários predeterminados, entretanto todos os usuários da rede podem atuar como nó validador

Tabela 3.1 Tabela com tipos de rede Blockchain

Em redes Blockchain públicas, qualquer dispositivo pode se juntar à rede - sem a necessidade da aprovação de uma terceira entidade - sendo capaz de atuar como um usuário comum ou como um nó validador. No caso de redes privadas, o dono restringe o acesso à rede. Diversas redes privadas também implementam permissionamento para controlar quais usuários podem realizar transações, criar Smart Contracts ou agir como nó validador na rede, entretanto isso não é uma regra. Também é possível a criação de redes Blockchain privadas sem permissionamento. Uma empresa seria capaz de utilizar uma rede Blockchain privada apenas para dispositivos internos baseada na rede Ethereum (sem permissionamento). Um exemplo de rede Blockchain que é pública, entretanto possui permissionamento é o Ripple (5). Os nós que possuem permissões de agir como validadores são apenas alguns selecionados pela empresa Ripple Labs, entretanto qualquer usuário pode acessar a rede, criar um par de chaves identificadoras e transferir tokens.

Além disso, há redes de Blockchain que utilizam tokens (por exemplo: Ripple (5)), enquanto outras não utilizam (por exemplo: Hyperledger (17)). Tokens não necessariamente estão relacionados à existência de uma criptomoeda, mas podem ser utilizados como mecanismos internos para registrar a ocorrência de eventos em determinados instantes.

3.4 Desafios de redes Blockchain

A tecnologia de Blockchain vem sendo aplicada em diversas áreas, entretanto há desafios relacionados à redes dessa natureza que limitam seu uso e algumas vezes até o tornam impraticável em cenários específicos. Os desafios associados à Blockchain são principalmente destacados como problemas de custo computacional, escalabilidade e segurança.

3.4.1 Custo Computacional e Escalabilidade

Inicialmente, o primeiro caso de implementação de uma rede Blockchain foi a criptomoeda Bitcoin. Esta criptomoeda revolucionou a forma como transações podem ser realizadas, eliminando a necessidade de intermediários para garantir o envio de moedas para qualquer lugar do mundo. Entretanto, como pioneira, a tecnologia proposta apresentou alguns problemas que vêm sendo discutidos até hoje pela comunidade que a mantém.

Para a validação de transações, inicialmente foi utilizada a abordagem de Proof-of-Work que promove a validação de transações através do processamento de um desafio cuja resolução requer um alto custo computacional e, consequentemente, um alto gasto de energia (4). Além disso, para balancear a melhora constante de processadores e GPUs, a dificuldade associada ao desafio é aumentada de tempos em tempos. Este aumento com o passar do tempo foi mostrando a ineficiência que a abordagem de Proof-of-Work traz em diversos cenários (por exemplo: Internet das Coisas). O gasto de energia anual para a manutenção da rede Bitcoin chega a ser equivalente à energia consumida por países inteiros devido à ineficiência do PoW (18). Contudo, novas técnicas de validação de transações vêm sendo criadas e implementadas com o objetivo de minimizar a alta necessidade de poder computacional e energia provenientes do uso do Proof-of-Work. Uma das novas abordagens que vem sendo amplamente utilizada é a Proof-of-Stake.

Outro desafio que é amplamente discutido é a questão da escalabilidade da rede Blockchain. Como todos os blocos de todas as transações realizadas são guardados para possibilidade de visualização a qualquer momento, a necessidade de armazenamento disponível nos nós validadores tem se tornado um problema. Há pouco tempo uma das soluções que a comunidade do Bitcoin implementou para mitigar este problema foi a possibilidade de se tornar um nó validador leve que não possui todas as transações realizadas, mas possui um número determinado das mais recentes. Entretanto ainda há a necessidade da existência de nós validadores completos na rede que contém todas as transações já realizadas na história da moeda.

Além disso, outra questão que é discutida no âmbito da escalabilidade é o potencial de transações por hora que a moeda tem. No caso do Bitcoin, há um limite no tamanho do bloco que contém transações, ou seja, cada bloco contém um número limitado de transações. E, conforme explicado por Nakamoto(4), a cada hora há um número médio esperado de blocos adicionados à rede. Caso a rede esteja validando mais blocos do que a média, a dificuldade do desafio do Proof-of-Work é aumentada e, consequentemente, o número de blocos validados volta para a média. Desta forma, a cada hora há um número limitado de transações que podem ser validadas e, com o crescimento da rede, a demora para realização de transações pode se tornar inviável para algumas aplicações. Em 2017, houveram fases em que transações de Bitcoin chegaram a demorar horas e tiveram taxas de transferência muito altas para serem realizadas (19). Outra criptomoedas vêm enfrentando este desafio - com o objetivo de prover maior velocidade na realização de transações - através da abordagem de outro protocolo de consenso distribuído. A Ripple (5), por exemplo, utiliza um protocolo de consenso proprietário com nós permissionados para realizar validações e garante a realização de transações em cerca de 3 segundos.

3.4.2 Segurança de redes Blockchain

A preocupação acerca da segurança de redes Blockchain que afeta todos os tipos e casos de uso de redes dessa natureza é o cenário em que um atacante possui a maioria do poder de decisão dos nós validadores. A depender do protocolo de consenso distribuído que está sendo utilizado, a maioria do poder de decisão pode significar 51% do poder computacional - no caso do Proof-of-Work - 51% do poder monetários dos nós validadores - no caso do Proof-of-Stake - ou a maioria do que seja o ponto central do protocolo de consenso. Em 2018, segundo Hertig(20), houveram casos reportados de pelo menos cinco criptomoedas - baseadas em Proof-of-Work - afetadas por ataques dessa natureza.

Os principais danos que pode ser causados a partir de um cenário de maioria de poder de decisão são a geração de transações fraudulentas e a negação de serviço para alguns usuários da rede através da não inclusão de suas transações nos blocos da cadeia. Esse é um dos ataques mais devastadores que pode ocorrer no cenário de redes Blockchain e, após sua ocorrência, não há solução que mitigue os danos causados sem a necessidade de realizar modificações na lista dos blocos anexados à cadeia. Ao realizar modificações na cadeia de blocos transações legítimas presentes nos mesmos blocos que as transações fraudulentas podem terminar sendo revertidas e, em determinados cenários que a transação não pode ser repetida - como por exemplo um cenário de uma compra de produto - essas alterações podem trazer grandes prejuízos para os usuários da rede.

Em redes que utilizam a proposta de Proof-of-Work, por mais que a modificação na cadeia

dos blocos seja realizada, ainda é incerta a garantia de que o atacante não vai continuar tendo a maioria dos nós validadores na nova rede após as modificações. O criador do Ethereum - Vitalik Buterin - argumenta em (15) que a utilização de um protocolo de consenso baseado em Proof-of-Stake pode limitar ao máximo a manipulação do mercado e, caso ataques de maioridade de poder de decisão forem executados, a comunidade pode simplesmente coordenar uma modificação na cadeia de blocos para retornar ao que era antes do ataque ser realizado. Além disso ainda seria possível deletar o depósito dos atacantes, haja vista que nesse protocolo de consenso os fundos dos nós validadores ficam presos até o final do processo de verificação. A moeda Ripple (5), por sua vez, utiliza uma rede Blockchain permissionada, então apenas nós validadores autorizados pela empresa Ripple Labs são capazes de validar transações. Essa abordagem reduz abruptamente o risco de ataques de maior poder de decisão, entretanto faz com que a rede tenha uma característica significantemente mais centralizada do que redes da natureza do Bitcoin ou Ethereum.

Ademais, outra preocupação constante sobre a segurança de redes de Blockchain se trata da possibilidade de impersonificar usuários da rede. Alguns usuários costumam utilizar sementes - como frases ou palavras - para a geração de seu par de chaves criptográficas. Entretanto, dependendo da complexidade das palavras utilizadas, é possível que um atacante consiga gerar a mesma chave privada utilizada por um usuário legítimo da rede e, consequentemente, obter acesso aos fundos armazenados em sua carteira. Em janeiro de 2018 houve relatos de cerca de U$ 4 milhões roubadas de carteiras de usuários da criptomoeda IOTA através de um ataque dessa natureza (21). Os usuários utilizaram sementes de um site malicioso para a geração de suas chaves criptográficas e, consequentemente, os atacantes também conseguiram gerar as mesmas chaves que os usuários legítimos. Isso os deu o poder de transferir fundos das carteiras das vítimas através do uso de sua chave privada. Outra versão deste mesmo problema é a criação de carteiras vulneráveis que exponham a chave privada do usuário. Desta forma, atacantes podem ser capazes de recuperar a chave privada do usuário a partir de seu dispositivo e comprometer as moedas da carteira da vítima.

3.5 Resumo

Apesar de comumente associada à criptomoeda Bitcoin, redes Blockchain possuem diversas áreas de possível atuação que podem ser efetivas de acordo com alguma variações em sua implementação.

Usuários de redes Blockchain são definidos por pares de chaves criptográficas (pública e privada) que são utilizadas para verificar e assinar transações respectivamente. As moedas transacionadas em redes Blockchain podem variar seu conteúdo, podendo ser compostas por diversas informações digitalmente assinadas pelo usuário dono dos dados. Uma transação é uma assinatura digital de um usuário em uma moeda de sua posse com a chave pública de um outro usuário que será o novo dono daquela moeda. Qualquer usuário com acesso à Internet pode verificar se a moeda foi de fato transferida.

Por ser um sistema distribuído não centralizado, para garantir que blocos de transação sejam adicionados corretamente à cadeia de blocos, é necessário utilizar um protocolo de consenso distribuído entre os nós que validam as transações a serem adicionadas. Os protocolos de

consenso mais comumente utilizados atualmente são o Proof-of-Work e o Proof-of-Stake. O algoritmo de Proof-of-Work se baseia na busca por um valor que, quando aplicado a uma função de hash, resulte em um Hash que possua um formato específico predeterminado. Enquanto o algoritmo de Proof-of-Stake funciona de forma que os nós validadores devem submeter moedas para entrar no processo de validação de blocos de transações. Após o envio das moedas, há mais de uma abordagem para selecionar qual será o novo bloco adicionado à cadeia, entretanto os mais utilizados são: Chain-Based Proof-of-Stake e BFT-Style Proof-of-Stake. O primeiro determina que um dos nós validadores será escolhido de forma pseudo-aleatória e selecionará o próximo bloco a ser adicionado, enquanto o segundo determina que os nós validadores propõe blocos aleatórios e, no final, há um processo de seleção de qual bloco será adicionado através dos votos de todos os nós validadores através de rounds de votação.

Smart Contracts são definidos como um protocolo de transação computadorizado que executa os termos de um contrato preestabelecido. Estes contratos traduzem cláusulas contratuais em um software ou hardware que tem a capacidade de garantir que as cláusulas serão cumpridas sem a necessidade de um intermediário entre as duas partes do contrato e garantem a rosbustez contra exceções acidentais ou ocorrência de atividades maliciosas.

Existem modelos distintos de implementação de redes Blockchain que são escolhidos de acordo com a disponibilidade de acesso aos dados e o permissionamento dos nós da rede. Os modelos podem variar entre redes Blockchain públicas ou privadas e com permissionamento ou sem permissionamento. Entretanto, estes conceitos ainda encontram-se em debate e podem diferir na literatura em trabalhos distintos.

Os desafios associados à tecnologia de redes Blockchain são principalmente destacados como problemas de custo computacional, escalabilidade e segurança. Os problemas de custo computacional e escalabilidade estão associados as questões de custo de energia consumido - principalmente em redes que utilizam o protocolo de consenso distribuído PoW - necessidade de armazenamento de toda a cadeia de blocos da moeda em nós da rede e o controle do número de blocos que podem ser adicionados à cadeia por determinado período de tempo - que pode acarretar na lentidão da aprovação de uma quantidade massiva de transações. Enquanto o principal desafio relacionado à segurança trata-se dos cenários em que atacante possuem a maioria do poder de decisão das redes Blockchain e, portanto, são capazes de adicionar transações fraudulentas à cadeia de blocos mantida como a oficial.

CAPÍTULO 4

Blockchain no contexto de Internet das Coisas

Este capítulo aborda a utilização da tecnologia de redes Blockchain dentro do contexto de aplicações para Internet das Coisas. Na seção 4.1 são mencionados cenários em que esta tecnologia já encontra-se empregadas e os problemas que são solucionados com seu uso, enquanto na seção 4.2 são destrinchadas as soluções propostas por autores para os principais desafios que circundam sistemas IoT como gerenciamento de DNS, gerenciamento de recursos, gerenciamento de informações, autenticação, controle de acesso e redes de micropagamentos.

4.1 Blockchain vs Internet das Coisas

A necessidade de utilização de uma estrutura descentralizada confiável vem se mostrando essencial para a manutenção da arquitetura da Internet das Coisas sustentável (22). Do ponto de vista dos fabricantes de dispositivos, o modelo centralizado apresenta um grande custo de manutenção para situações corriqueiras como, por exemplo, a atualização contínua do firmware de milhões de dispositivos. Enquanto do ponto de vista de usuários, há a necessidade de confiança em dispositivos que se comunicam com uma central de forma transparente (23). Essas questões podem ser resolvidas com abordagens peer-to-peer - sem necessidade de confiança em todos os dispositivos envolvidos - escaláveis como modelos adaptados da tecnologia de Blockchain para a distribuição de dados de forma segura.

Para a situação de atualizações de software, há a possibilidade de utilização de um sistema de arquivos peer-to-peer descentralizado como o IPFS (24). Neste cenário, todos os dispositivos de um fabricante operam em uma mesma rede de Blockchain através da qual o fabricante disponibilizaria um Smart Contract para que dispositivos verifiquem o hash da última atualização de firmware na rede. As primeiras requisições para download da atualização seriam disponibilizadas pelo fabricante, entretanto, depois de uma certa quantidade de downloads, o fabricante pode deixar de disponibilizar o binário em sua infraestrutura e os dispositivos que não o obtiveram ainda podem recorrer aos outros dispositivos presentes na rede que já baixaram a atualização. Como o fabricante ainda disponibilizará o hash do arquivo no Smart Contract, o dispositivo poderá realizar o download a partir de outro nó e verificar se o arquivo recebido de fato é o criado pelo fabricante.

Em um contexto onde a rede Blockchain proporciona uma camada de pagamentos com uma criptomoeda arbitrária, há a possibilidade de criação de um mercado de serviços entre dispositivos. No exemplo anterior, dispositivos que armazenassem uma cópia do arquivo original enviado pelo fabricante poderiam cobrar um valor por manter o arquivo disponibilizado em sua infraestrutura. Uma das moedas existentes no mercado atualmente que tem a proposta de viabi-

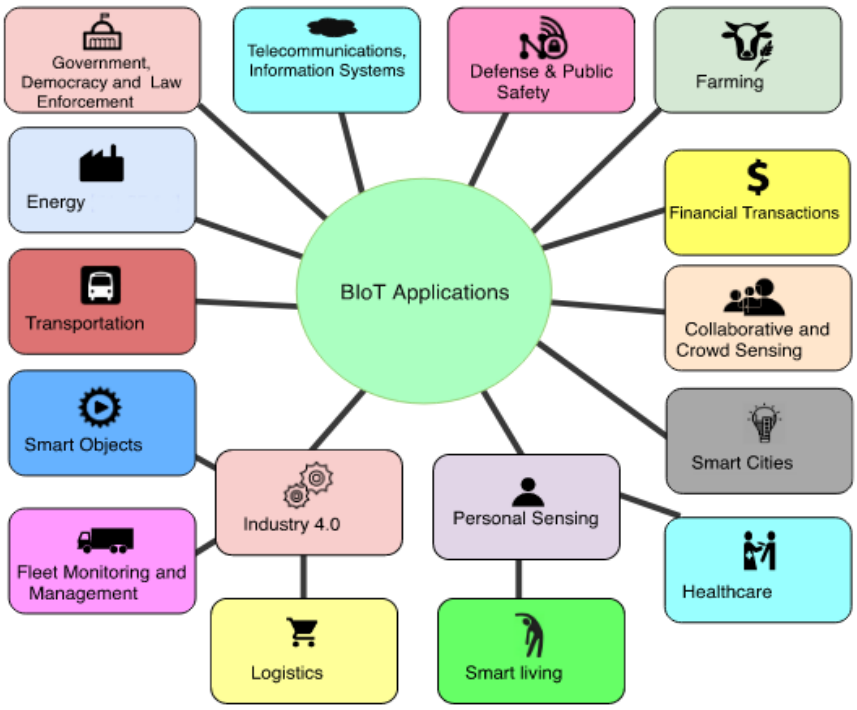

Figura 4.1 Áreas de atuação de aplicações BIoT. Fonte: Artigo (2)

lizar microtransações para serviços dessa natureza é a IOTA (6). Esta criptomoeda utiliza uma tecnologia chamada Tangle que é uma adaptação do modelo Blockchain - inicialmente proposto por Satoshi Nakamoto no Bitcoin - com o objetivo da utilização em sistemas de Internet das Coisas.

Seguindo a mesma linha de comércio entre dispositivos, pode-se citar o setor de energia onde a integração entre dispositivos IoT com uma rede Blockchain com camada de pagamentos poderia proporcionar a compra e venda de energia automaticamente. Por exemplo, LO3Energy (25) apresenta uma proposta de um mercado peer-to-peer descentralizado de energia renovável em uma vizinhança. Painéis solares gravam seus excessos de energia coletada em um Blockchain e os vendem para vizinhos que necessitam de energia através de Smart Contracts.

Outro contexto em que Blockchain pode ser utilizado é em aplicações agriculturais de Internet das Coisas. Em (26) é proposto um sistema de rastreamento para monitoramento do transporte de mantimentos chineses. O sistema é baseado no uso de RFID (Radio Frequency Identification) e uma rede Blockchain com o intuito de melhorar a segurança e qualidade da comida ao mesmo tempo que reduz o custo com a logística do gerenciamento dos dispositivos IoT.

A tecnologia de Blockchain pode ser aplicada em diversas áreas de Internet das Coisas com o objetivo de solucionar mais de um tipo de problema. Na Figura 4.1, encontram-se descritas algumas áreas de atuação que já possuem pesquisas relacionadas a adoção de redes Blockchain.

4.2 Otimização de Blockchain para Internet das Coisas

A tecnologia de Blockchain pode ser utilizada para solucionar diversos problemas associados à sistemas de Internet das Coisas. A depender do objetivo da rede, o design e definição de como esta irá funcionar pode variar para combater dificuldades futuras de escalabilidade e segurança. Um modelo de rede Blockchain que tem como objetivo resolver um problema de autenticação de dispositivos não precisará disponibilizar uma camada de pagamentos por exemplo. A Figura 4.2 mostra um infografo dos desafios de Internet das Coisas que apresentam pesquisas para sua solução através da implementação de redes Blockchain.

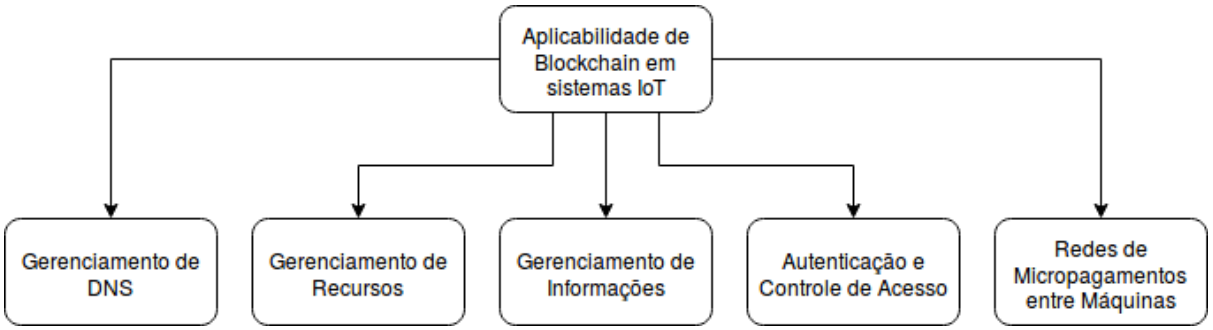

Figura 4.2 Áreas de aplicabilidade de redes Blockchain em sistemas IoT.

4.2.1 Gerenciamento de DNS

O sistema de DNS atual utiliza uma abordagem centralizada acerca do processo de resolução de nomes. Com a rápida evolução da Internet das Coisas, este sistema - que é parte fundamental da infraestrutura da Internet para possibilitar o acesso a endereços de recursos - enfrenta desafios acerca de escalabilidade, privacidade e robustez. O gerenciamento centralizado em módulos desse sistema torna essa tecnologia suscetível à falhas em larga escala a partir de ataques persistentes e, além disso, induz um atraso na sincronização de arquivos de zona conforme o crescimento do sistema (27).

4.2.1.1 DNSLedger

Em (27) é proposta uma solução para utilizar a tecnologia de Blockchain na criação de um sistema de resolução de nomes descentralizado, chamado DNSLedger. Esse sistema pode ser categorizado como uma rede Blockchain pública, porém permissionada, haja vista que nem todos os nós são capazes de realizar alterações na rede e o sistema deve ser gerenciado por algum tipo de consórcio de empresas.

O DNSLedger possui duas cadeias de blocos: a cadeia Root e a cadeia TLD (Top-Level Domain). Na primeira são armazenadas as informações do funcionamento da cadeia TLD, enquanto a segunda é que define o funcionamento do sistema. As cadeias TLD são as responsáveis por armazenar as informações acerca dos nomes presentes em cada domínio. Por exemplo, a TLD .com gerencia todos os nomes de domínios derivados de .com (Figura 4.3).

Entretanto, como muitas organizações grande possuem um segundo ou terceiro nível de resolução de nomes de domínio, usuários também são capazes de alterar sua própria configuração de resolução de nomes e estabelecer suas próprias cadeias de DNS internas.

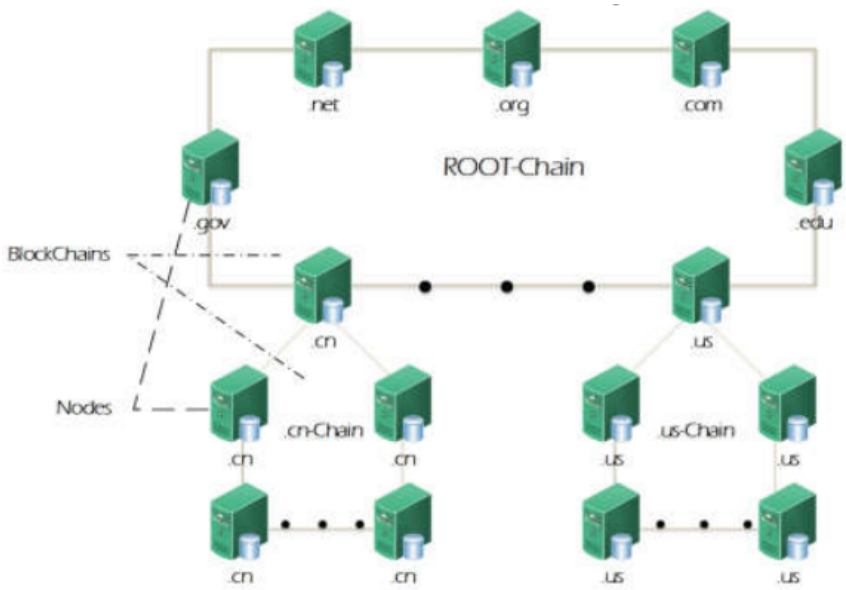

Figura 4.3 Arquitetura do DNSLedger. Fonte: Artigo (27)

Os nós desse sistema são responsáveis por manter as informações presentes no Blockchain e, ao mesmo tempo, prover serviços de resolução de nomes para usuários. Por exemplo, os nós da cadeia TLD .com são os servidores que provêm serviços de DNS para rede .com. Além disso, cada cadeia TLD pode selecionar um ou dois de seus nós para participar da cadeia Root. As chaves públicas correspondentes à cada um dos nós da rede também encontram-se armazenadas nas cadeias de Blockchain para verificações de autenticidade dos nós.

Informações de DNS são divididas em identificação e label. O label contém os dados sobre quem é o dono de um domínio, enquanto a identificação diz respeito ao mapeamento utilizado no protocolo. Por motivos de otimização, no DNSLedger as informações de label são armazenadas em um sistema de arquivos baseado em Blockchain e os dados de identificação são armazenados em um banco de dados. Entretanto, alterações nos dados presentes no banco de dados só podem ser realizadas através do Blockchain do DNSLedger.

Inicialmente um usuário precisa enviar três informações para adquirir um nome de domínio: nome do domínio, informações pessoais e chave pública. Após validar as informações recebidas, o sistema grava as informações na rede Blockchain. Por fim, a partir da chave privada do usuário, é possível realizar alterações nas informações de seu domínio armazenadas na rede e, inclusive, atualizar a chave pública salva.

4.2.2 Gerenciamento de recursos

Dispositivos IoT precisam enviar informações para infraestruturas de Cloud remotos para serem processados, entretanto esse modelo centralizado apresenta desafios de escalabilidade para

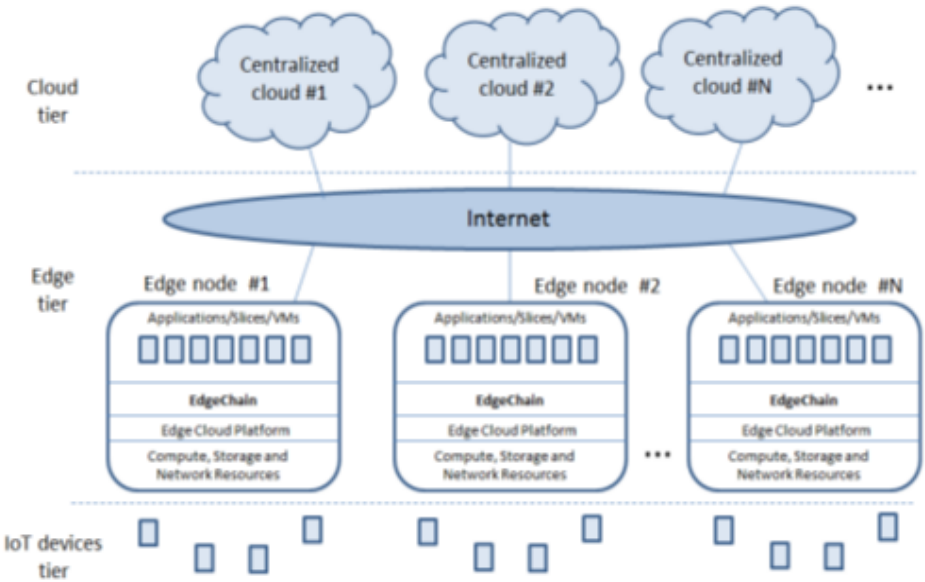

Figura 4.4 Estrutura da arquitetura EdgeChain. Fonte: Artigo (28)

sistemas IoT de cenário grande devido à grande quantidade de dados gerados e transmitidos (28).

4.2.2.1 EdgeChain

Com o objetivo de solucionar esse problema e proporcionar uma maior segurança para a estrutura da rede, Pan et al.(28) propõe uma arquitetura de sistema baseada em Edge Computing e Blockchain, chamada EdgeChain. Essa arquitetura consiste de uma rede Blockchain permissionada que é controlada por servidores Edge, ou seja, servidores às margens da rede IoT (Figura 4.4). Estes servidores agem como os validadores de transações e cada dispositivo IoT possui uma carteira com moedas de crédito. Para obtenção de recursos dos servidores Edge, é preciso usar as moedas de crédito de um dispositivo.

As permissões de cada dispositivo e a políticas de acesso à recursos são definidas através de Smart Contracts na rede Blockchain, o que traz robustez ao sistema. Após a confirmação da transação de pagamento, a Edge Cloud irá prover recursos de computação, memória e armazenamento ao dispositivo que solicitou as permissões de acesso.

4.2.3 Gerenciamento de Informações

A expansão recente da Internet das Coisas e, consequentemente a explosão no volume de informações produzidas por dispositivos inteligentes fez com que surgisse a necessidade do uso de centros de bancos de dados fora dos sistemas IoT para o gerenciamento e armazenamento de informações (29). Entretanto, há muitos desafios relacionados à manutenção dessa arquitetura devido ao crescimento da heterogeneidade e quantidade de dispositivos IoT, assim como a necessidade de alta disponibilidade em tempo real de informações, escalabilidade, resiliência,

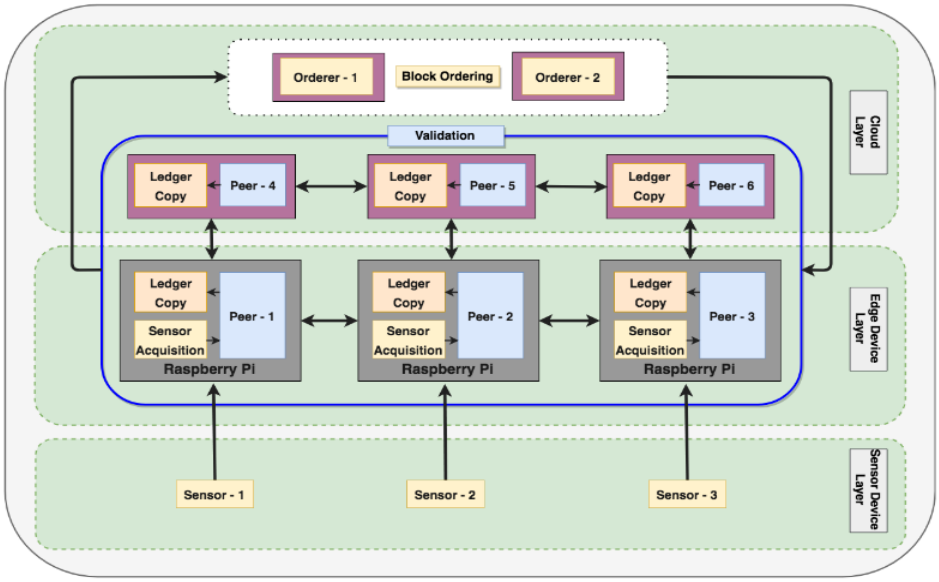

Figura 4.5 Design de arquitetura descentralizada de gerenciamento de informações. Fonte: Artigo (30)

segurança e baixa latência na comunicação.

4.2.3.1 Rede Blockchain Privada e Permissionada

Em (30) é proposta uma solução utilizando a rede Blockchain Hyperledger Fabric. Nessa solução a rede é privada e permissionada, portanto seu acesso é controlado por uma entidade ou empresa. O Hyperledger Fabric divide a função dos nós validadores em duas: peer nodes e orderer nodes. Os peer nodes são os nós que são responsáveis por validar as transações e manter as informações da cadeia. Enquanto os orderer nodes são os nós que fazem o protocolo de consenso entre si sobre a ordenação da cadeia e propagam os blocos para toda a rede. Desta forma, a rede é dividida nas camadas dos dispositivos edge e dos nós da Cloud. Os dispositivos edge serão os peer nodes e deverão validar as transações e os nós da Cloud que deverão fazer a ordenação dos blocos e propagar essas informações para todos os dispositivos da rede (Figura 4.5).

4.2.3.2 Rede Blockchain com Armazenamento Centralizado

Em (31) é proposta uma outra arquitetura alternativa construída a partir da rede Blockchain Ethereum. Nessa solução é argumentado o uso da rede Blockchain apenas para o armazenamento do hash das informações cifradas enquanto o armazenamento dos dados é feito em um ambiente considerado seguro e confiável, composto por componentes de Intel SGX. Para acessar os dados armazenados, usuários precisam solicitar permissão através de uma API de Smart Contracts responsável por gerenciar o controle de acesso às informações de dispositivos. Se o acesso for permitido, o hash dos dados é retornado para o usuário e este é utilizado para recuperar as informações armazenadas através da plataforma SGX (Figura 4.6).

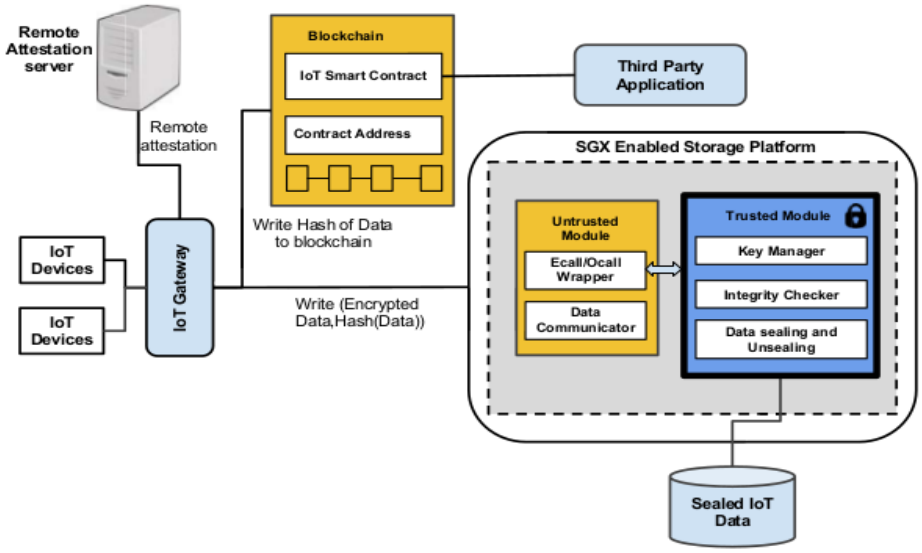

Figura 4.6 Design de arquitetura com armazenamento centralizado. Fonte: Artigo (31)

Inicialmente, os usuário se registram na rede Ethereum através da geração de um par de chaves pública/privada e, em seguida, podem associar seus dispositivos IoT através de um Hashmap presente no Smart Contract do sistema. A partir dessa associação apenas usuários marcados como donos do dispositivo serão capazes de acessar os dados armazenados pelo mesmo.

4.2.3.3 Rede Blockchain com Armazenamento Descentralizado

Em (32) é proposta uma solução alternativa à (31) - em que o armazenamento das informações é realizada em um sistema centralizado. Wang et al.(32) sugerem a utilização de uma rede de armazenamento descentralizada chamada IPFS e argumentam sobre as vantagens na capacidade de armazenamento contra um sistema centralizado. Wang et al.(32) dividem o sistema em três partes: dispositivos IoT, rede Blockchain e sistema de armazenamento IPFS.

A rede funciona com cada dispositivo tendo um par de chaves identificadoras únicas. Ao solicitar alguma informação, um dispositivo IoT realiza uma transação contendo a chave pública do dispositivo, a chave pública do provedor de serviço e o dado que está sendo solicitado. Enquanto isso, os provedores de serviço constantemente consultam a rede Blockchain com sua chave pública em busca de alguma solicitação de informações proveniente de dispositivos IoT. Ao identificar uma transação solicitando uma informação, o provedor de serviços realiza uma nova transação para a rede Blockchain seguindo o mesmo fluxo do dispositivo IoT (Figura 4.7). Após a transação de resposta ser enviada, o dispositivo IoT pode acessar as informações disponibilizadas a partir de uma consulta na rede Blockchain com sua chave pública.

Figura 4.7 Design de arquitetura com armazenamento descentralizado. Fonte: Artigo (32)

4.2.4 Autenticação e controle de acesso

Dispositivos de sistemas de Internet das Coisas encontram-se suscetíveis a uma variedade de ataques, entretanto uma das principais preocupações são relacionadas a autenticação e controle de acesso no contexto desses sistemas. Recentemente mais de 150 mil dispositivos IoT foram comprometidos e a investigação realizada identificou que a principal causa do comprometimento foram falhas no controle de acesso (33). Portanto a adoção de sistemas impróprios de controle de acesso e autenticação de dispositivos pode causar grandes danos econômicos e relativos à privacidade de usuários e empresas.

4.2.4.1 ControlChain

(33) propõe uma solução através da utilização de redes Blockchain chamada ControlChain. Esta arquitetura utiliza quatro redes Blockchain distintas categorizadas da seguinte forma:

Context Blockchain: Blockchain que armazena informações contextuais obtidas de sensores e dados processados. As informações presentes nessa cadeia também podem ser utilizadas como regras para controle de acesso. Por exemplo se existir uma regra em que vídeos só podem ser transmitidos quando a rede estiver com pouco tráfego, a tentativa de consulta à uma informação de vídeo nesse Blockchain será recusada em casos de alto tráfego de rede.

Relationships Blockchain: Rede responsável por armazenar as credenciais e relacionamentos de todos os dispositivos e usuários. Nesta rede também é definido quem é o usuário dono de cada dispositivo.

Rules Blockchain: Esta rede armazena as informações sobre controle de acesso dos dispositivos de acordo com seus donos. Os usuários que possuem permissões de acesso à dispositivos são descritos nessa cadeia.

Accountability Blockchain: Blockchain que armazena as informações de log de permissões e negações de acessos realizados na rede.

As decisões de controle de acesso são tomadas a partir da consulta de três Blockchains e o resultado dessa decisão é armazenado em outra rede Blockchain (Figura 4.8). A rede de Relationships Blockchain tem como objetivo principal garantir a autenticidade de usuários e dispositivos, enquanto a rede de Rules Blockchain utiliza essas informações para realizar o controle de acesso à informações através de regras predeterminadas.

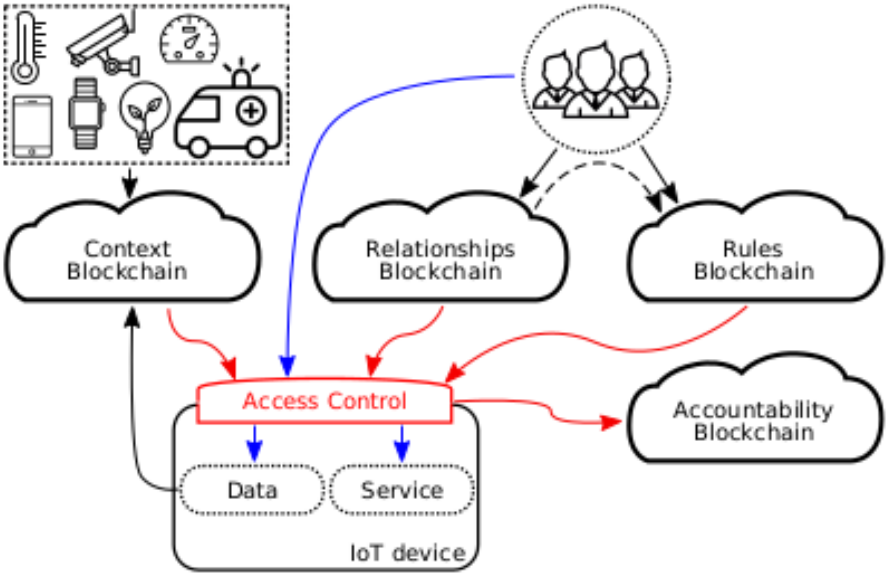

Figura 4.8 Arquitetura proposta ControlChain. Fonte: Artigo (33)

4.2.4.2 Arquitetura baseada em Smart Contracts

Em (34), Novo(34) propõe uma arquitetura baseada em uma rede Blockchain pública e sem permissionamento. Em sua solução, Novo(34) sugere o uso de Hubs de Gerenciamento que serão conectados aos dispositivos IoT para fazer a interface com a rede Blockchain. A decisão dessa abordagem foi tomada devido à falta de poder computacional de dispositivos IoT. Desta forma, os hubs de gerenciamento são responsáveis por transferir as informações entre a rede Blockchain e os dispositivos. Todo o controle de acesso das informações é definido em um único Smart Contract (Figura 4.9). Os usuários podem se conectar à rede para realizar alterações nos dispositivos - através de transações para os Hubs de Gerenciamento - e consultar informações armazenadas pelos dispositivos que os pertencem.

Nesta arquitetura, Novo(34) defende que é necessário manter uma criptomoeda na rede Blockchain para que haja o incentivo para os nós validadores continuarem verificando as transações realizadas. Em sua solução, para obter informações dos dispositivos, os usuários precisam realizar transações e pagar as taxas necessárias para que os seus dispositivos possam escrever as informações coletadas na rede Blockchain. Entretanto, para a consulta de informações já armazenadas na rede não há necessidade de realizar transações e nem pagar taxas de transferência.

Rifi et al.(35) propõe uma abordagem similar, entretanto argumenta a alternativa de uso de múltiplos Smart Contracts, ao invés de apenas um central. Cada usuário pode emitir seu Smart Contract para o gerenciamento de seus dispositivos e, através de uma política de Publisher e Subscriber, os donos seriam capazes de fornecer acesso à outros usuários autorizados. Publishers são categorizados como os dispositivos que enviam informações para a rede, enquanto os Subscribers são os usuários autorizados que consomem essas informações.

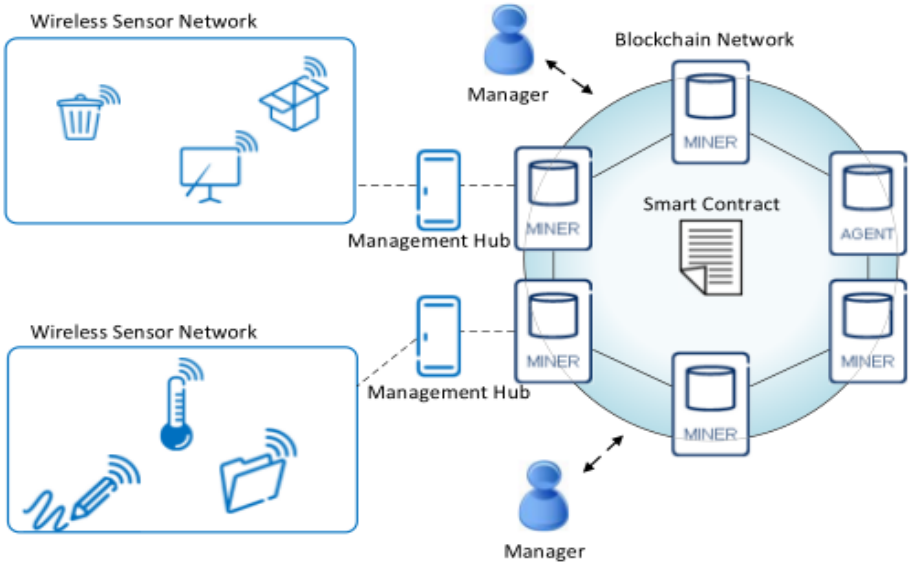

Figura 4.9 Modelo proposto por Oscar Novo. Fonte: Artigo (34)

4.2.4.3 IoTChain

Alphand et al.(36) apresentam uma solução de autorização e controle de acesso para recursos através de uma arquitetura chamada IoTChain. Nesta arquitetura é utilizada uma rede Blockchain pública não permissionada que é a responsável por identificar os dispositivos, os servidores de recursos e os Smart Contracts necessários para o funcionamento do sistema. Por ser pública e sem permissionamento, qualquer usuário pode acessar a rede Blockchain de autorização e agir como um nó validador de transações. As entidades presentes nesta arquitetura são descritas como:

Servidores de Recursos: Armazenam os recursos disponibilizados.

Donos dos Recursos: São os donos dos servidores de recursos e dos recursos armazenados neles.

Servidores Proxy: Armazenam os recursos encriptados quando os servidores de recursos são altamente restritos.

Servidores de Chave: Geram as chaves necessárias para cifrar e decifrar os recursos. Tokens de acesso: Descrevem as permissões de acesso de um usuário específico e recursos específicos. Rede Blockchain de autorização: Geram e controlam os tokens de acesso através de Smart Contracts.

Inicialmente, um dono de recurso cria um Smart Contract e o publica na rede Blockchain de autorização (Figura 4.10). Este contrato gerará um token de acesso para um usuário que atingir as especificações determinadas nas cláusulas do Smart Contract. Este token contém informações sobre os recursos que o usuário associado possui permissões de acesso.

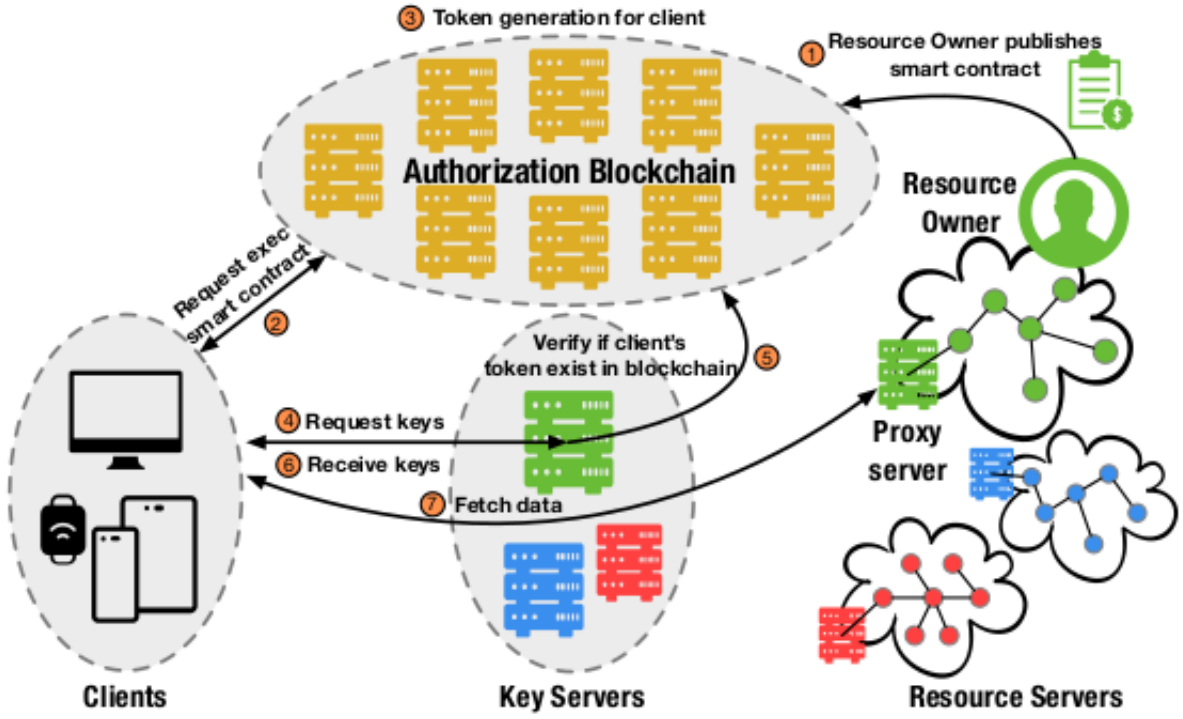

Figura 4.10 Arquitetura do IoTChain. Fonte: Artigo (36)

No momento em que um usuário deseja acessar o recurso de algum dono específico, o mesmo realiza uma transação para o Smart Contract publicado por este dono e, caso as condições predispostas forem satisfeitas, o cliente será associado com um token de acesso. Este token referencia a chave pública do usuário a quem está associado, descreve as permissões de acesso e possui um tempo de validade. Cada contrato deve criar tokens de acesso diferentes de acordo com o usuário que está requisitando os recursos.

Em seguida, o usuário solicita as chaves de encriptação para o servidor de chaves com o objetivo de ser capaz de decifrar os recursos requisitados previamente. Como o servidor de chaves possui uma cópia da cadeia de blocos da rede de autorização, o mesmo verifica qual Smart Contract possui um token de acesso associado ao usuário solicitante. Para verificar a autenticidade do usuário, o servidor de chaves cria um desafio baseado na chave pública associada ao token de acesso e envia para o usuário resolver. Este desafio só poderá ser resolvido por quem possuir a chave privada associada à chave pública que está gravada no Smart Contract, portanto este processo garante a autenticidade de quem está requisitando a informação.

Ao responder o desafio com sucesso, o servidor de chaves fornece as chaves necessárias para o usuário poder acessar os recursos requisitados através dos servidores de proxy ou servidores de recursos.

Este processo possibilita que usuários possam ter seus acessos adicionados ou excluídos de forma simples e rápida através dos Smart Contracts.

4.2.4.4 BCTrust

Hammi, Bellot e Serhrouchni(37) sugerem uma abordagem diferenciada através de um novo protocolo de consenso na arquitetura do BCTrust. Em (37), argumenta-se o uso de uma rede Blockchain privada e permissionada em que apenas um dispositivo gerenciador de um cluster de dispositivos possui um par de chaves pública/privada e, consequentemente, possui permissões de escrita na rede Blockchain.

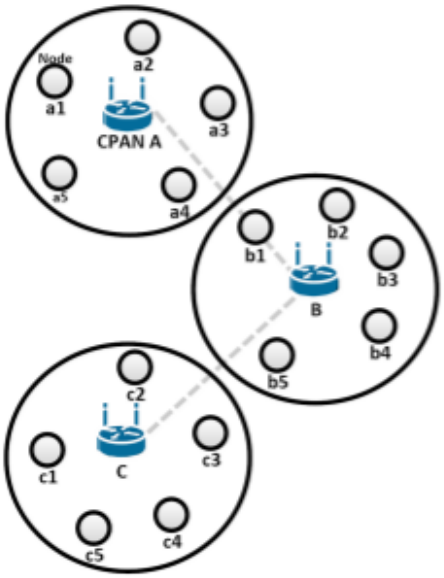

Figura 4.11 Arquitetura do BCTrust. Fonte: Artigo (37)

O protocolo de consenso proposto no BCTrust pode ser assimilado à frase: o amigo do meu é amigo também é meu amigo. O protocolo funciona de forma que, ao se conectar ao cluster A, por exemplo, um dispositivo a1 estabelece uma associação segura com chaves simétricas com o CPAN-A - dispositivo gerenciador do cluster A. A partir dessa associação, o CPAN-A envia uma transação para rede Blockchain com a informação CPAN-A: a1_ok. Essa transação sinaliza na rede que o CPAN-A valida a autenticidade de a1 e possui a chave simétrica associada ao dispositivo a1 previamente autenticado com ele.

Em seguida, caso o dispositivo a1 deseje se mover para um segundo cluster B, no momento em que a1 tenta se associar com CPAN-B, este acessa a rede Blockchain e verifica que a1 já foi validado por CPAN-A. Desta forma, CPAN-B requisita a chave simétrica associada à a1 e propaga para a rede Blockchain uma transação CPAN-B: a1_ok. O mesmo processo se repete conforme a1 varia entre clusters e o CPAN correspondente sempre requisita a chave simétrica do dispositivo através do CPAN mais próximo que já tenha validado o dispositivo a1 (Figura 4.11).

O problema com essa abordagem é a forma como se garante que a1 é quem ele diz ser. Como a1 só possui uma chave simétrica como seu identificador, é difícil garantir que esta chave simétrica não foi roubada por outros dispositivos e está sendo utilizada indiscriminadamente. Hammi, Bellot e Serhrouchni(37) não deixa claro como essa verificação das chaves simétricas

utilizadas por dispositivos é realizada, apenas menciona que um vetor de inicialização (IV) também é utilizado pelos dispositivos para a cifra das mensagens, entretanto, na comunicação entre CPANs essa informação também é enviada.

4.2.5 Sistemas de micropagamentos entre máquinas

Redes Blockchain como o Bitcoin com o foco em transações de moedas possuem muitas desvantagens para serem utilizadas em aplicações genéricas como sistemas IoT (6). A importância de micropagamentos deverá crescer na indústria de Internet das Coisas e soluções de pagamento como o Bitcoin em que pagamentos de taxas de transferências esporadicamente são maiores do que os valores sendo transacionados são impraticáveis (6). Conforme mostrado em algumas arquiteturas anteriores, os micropagamentos serão ferramentas fundamentais na venda e troca de informações de dispositivos em sistemas IoT.

4.2.5.1 IOTA

Em (6) é exposta uma proposta de alteração de redes Blockchain como alternativa para a realização de micropagamentos, inclusive tendo como foco a realização de pagamentos entre máquinas de forma simples. Esta rede é chamada de Tangle e transaciona a criptomoeda IOTA, criada especificamente para o uso em sistemas de Internet das Coisas. A principal ideia da rede Tangle é que para emitir uma transação, um usuário precisa trabalhar para aprovar outras transações da rede. Desta forma, usuários que estão utilizando a rede também estão contribuindo para sua segurança e estabilidade. Na Tangle não há distinções entre nós e nós validadores, todos nós são responsáveis por aprovar transações e realizar transações. Para emitir uma transação, um nó escolhe duas outras transações (de acordo com um algoritmo), checa se as duas transações não são conflitantes e, se forem, as transações não são aprovadas. Em seguida, para criar uma transação válida, o nó resolve um problema criptográfico similar ao do Proof-of-Work, onde é necessário encontrar um Nonce para que o hash deste valor concatenado com as informações da transação emitida possua uma determinada forma estabelecida no protocolo.

Apesar de utilizar um protocolo de consenso parecido com o Proof-of-Work, não há mineração de novas moedas no protocolo da criptomoeda IOTA. A forma de estímulo para que usuários continuem validando transações é a necessidade de validação para a emissão de novas transações. Além disso, cada nó mantém a estatística de quantas transações estão sendo emitidas por seus nós vizinhos e, caso um deles não esteja realizando validações constantes, ele é considerado um nó preguiçoso e rejeitado na rede.

Um dos pontos principais de distinção entre redes Blockchain e a rede Tangle é que o primeiro é baseado em uma cadeia de blocos, enquanto o segundo é baseado em uma estrutura de grafos diretos acíclica (Figura 4.12). Popov(6) argumentam que a estrutura de grafo reduz o tempo de confirmação de transações e melhora a segurança em geral da rede.

4.2.6 Arquitetura alternativa baseada em redes Blockchain

Há arquiteturas de redes Blockchain direcionadas especificamente para alguns dos desafios enfrentados pela Internet das Coisas. Entretanto, devido a grande variedade de aplicações de sis-

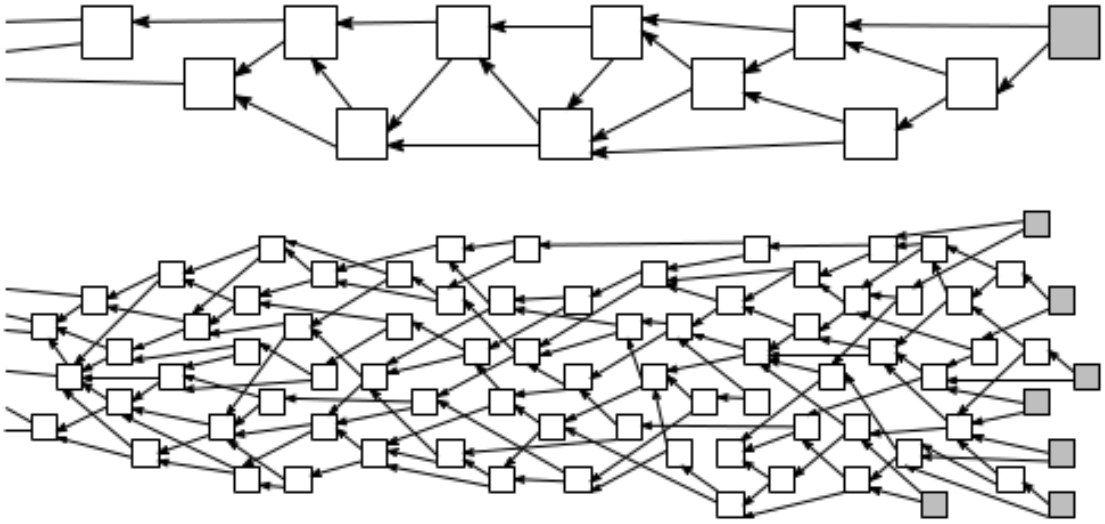

Figura 4.12 Rede de blocos da rede Tangle

temas dessa natureza, nem sempre é possível utilizar um desses modelos como a única rede do sistema IoT. Especificamente no contexto de casas inteligentes, a transparência nos processos de armazenamento e disseminação de informações proporcionada por redes Blockchain pode vir a se tornar um problema sério do ponto de vista de privacidade e segurança dos usuários de sistemas dessa natureza.

4.2.6.1 Arquitetura alternativa para Casas Inteligentes

Com o intuito de orquestrar uma arquitetura baseada em redes Blockchain para aplicar no contexto de casas inteligentes mantendo a privacidade e segurança de seus usuários, Dorri, Kanhere e Jurdak(3) propõe um modelo multinível de Blockchain. Os níveis podem ser definidos como a rede da casa inteligente e a rede da comunicação geral (Figura 4.13).

No cluster da casa inteligente, Dorri, Kanhere e Jurdak(3) propõe o uso de uma cadeia de blocos similar à de uma rede Blockchain, entretanto o único nó validador é um dispositivo gerenciador central (SMH) que possui mais poder computacional do que dispositivos IoT ordinários. Além disso, há um dispositivo dentro da casa responsável por armazenar as informações da cadeia de blocos. Esta configuração é similar à uma rede Blockchain, entretanto tem um aspecto centralizado haja vista que apenas um nó é responsável pelo gerenciamento de todas as transações. O SMH possui uma chave simétrica compartilhada para sua comunicação com todos os dispositivos da casa e a política de que transações devem ser aceitas e gravadas na cadeia de bloco é definida pelo dono da casa. Para armazenar, requisitar ou compartilhar informações os dispositivos da casa devem gerar transações para o SMH.

Na rede de comunicação geral, Dorri, Kanhere e Jurdak(3) argumenta o uso de uma rede Blockchain pública e permissionada. Os nós dessa rede podem ser SHM, outros dispositivos com grande poder computacional ou computadores. Para reduzir o consumo de banda de rede e a latência da comunicação, os nós da rede são divididos em clusters. Os dispositivos de

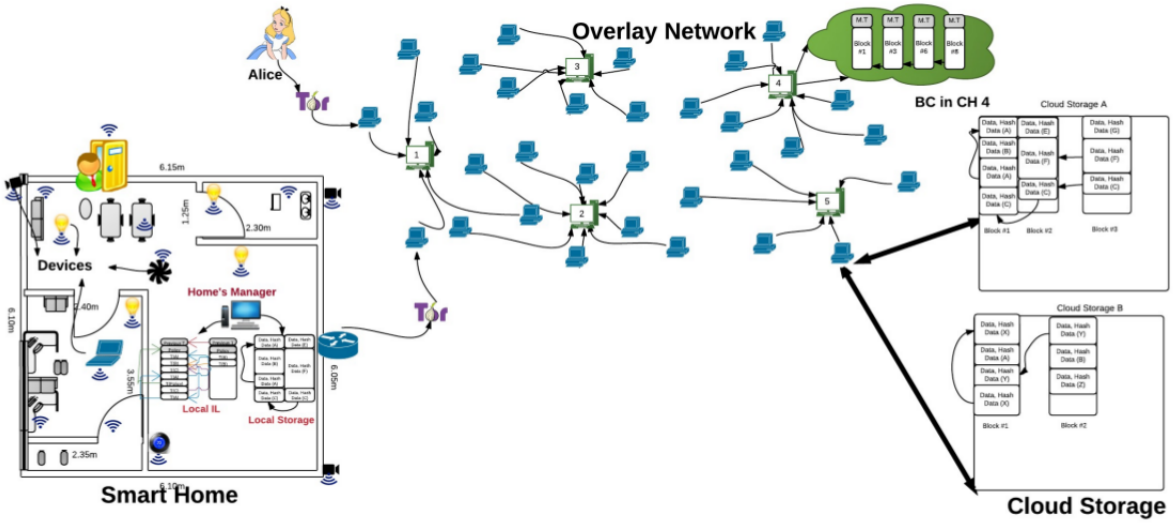

Figura 4.13 Arquitetura proposta para o contexto de casas inteligentes. Fonte: Artigo (3)

cada cluster são responsáveis por eleger um gerenciador (CH) que será o representante daquele cluster na rede. Qualquer nó pode mudar de cluster livremente caso esteja com uma latência muito alta. Cada CH possui um par de chaves pública/privada que é utilizado para gerar novos blocos a serem adicionados à cadeia. Os CH mantêm duas listas correspondentes às chaves dos requisitores (lista de chaves públicas que podem acessar dados dos SMHs conectados nesse cluster) e chaves dos requisitados (lista de chaves públicas dos SMHs conectados nesse cluster que podem ser acessados).

A rede Blockchain mantida pelos CHs possuem transações multisig, ou seja, as transações precisam ser assinadas tanto pelo nó requisitor quanto pelo nó requisitado para que sejam consideradas transações válidas. Além disso, cada transações possui duas saídas de resultados que indicam o número total de transações aceitas ou rejeitadas pelos requisitados que são criados pelo gerador da transação atual.

Para a manutenção do consenso sobre os blocos a serem adicionados na rede Blockchain de comunicação geral, os autores propõe um novo protocolo de consenso distribuído baseado em confiança distribuída para validar as transações. O protocolo proposta se baseia na continuidade dos blocos válidos emitidos por CHs. Inicialmente, como o CH não emitiu nenhum bloco ainda, todas as transações emitidas por ele são validadas pelos outros CHs da rede. As validações são realizadas verificando as permissões do requisitor e requisitado e se as transações foram corretamente assinadas. Na rede, cada CH mantém um nível de confiança dos outros CHs da rede baseado em evidência direta ou indireta. O CH A tem evidência direta da confiança do CH B, caso o CH A já tenha validado algum bloco de transações do CH B. Caso CH A receba um bloco de CH B e não tenha confiança nele, entretanto outros CH que o CH A confia validaram o bloco, o CH A tem evidência indireta que o CH B é confiável. Mesmo CHs considerados confiáveis ainda têm parte das transações verificadas para previnir comportamentos maliciosos na rede por CHs recentemente comprometidos.

Number of Successfully verfied blocks	10	20	30	40	50
Percentage of transactions should be verfied	80%	60%	40%	30%	20%

Figura 4.14 Evidência do número de transações processadas de acordo com confiança da rede. Fonte: Artigo (3)

Ao implementar essa rede com 50 nós, os autores obtiveram uma redução de 75% de dados tráfegados e 50% do tempo de processamento de dados em comparação ao uso da rede Blockchain do Bitcoin devido à redução da necessidade de validação de todas as transações de CHs confiáveis (Figura 4.14).

CAPÍTULO 5

Conclusões

A transição do mundo direcionado para informações vem se mostrando acelarada e a tecnologia de redes Blockchain pode vir a prover para sistemas de Internet das Coisas uma plataforma para distribuição de informações confiáveis de forma descentralizada sem a necessidade de incluir intermediários ou centrais gerenciadoras.

Este trabalho mostra os avanços realizados na construção de uma definição apropriada para sistemas de Internet das Coisas e otimizações realizadas para o emprego de redes Blockchain no contexto de diversas áreas em que aplicações BIoT já vem sendo aplicadas. As arquiteturas descritas propõe solucionar problemas enfrentados no mundo real atualmente, entretanto ainda possuem pouca evidência de uso na prática. Portanto ainda é incerta a eficiência das soluções propostas por alguns autores em cenários reais. Entretanto notáveis avanços foram realizados nessa área de pesquisa durante os últimos anos e mostraram evoluções marcantes para as preocupações associadas à segurança, privacidade e escalabilidade de sistemas IoT.

Por fim, pode-se concluir que, como em toda inovação tecnológica, não há uma arquitetura perfeita que solucione todos os problemas enfretados pelas aplicações criadas para as diversas áreas de uso de sistemas de Internet das Coisas. Entretanto, há arquiteturas que soluciam problemas presentes em mais de uma área de uso podendo ser utilizadas em conjunto com outras tecnologias para prover um sistema com funcionamento mais resiliente e otimizado. Os avanços mostrados nesse trabalho podem vir a causar impactos positivos significativos na forma de como a indústria de IoT funciona atualmente e como os sistemas são confeccionados.

Referências Bibliográficas

1 MINERVA, R.; BIRU, A.; ROTONDI, D. *Towards a definition of the Internet of Things (IoT)*. 2015. <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>.

2 FERNANDEZ-CARAMES, T. M.; FRAGA-LAMAS, P. A review on the use of blockchain for the internet of things. *IEEE Access*, v. 6, p. 32979–33001, 2018. ISSN 2169-3536.

3 DORRI, A.; KANHERE, S. S.; JURDAK, R. Towards an optimized blockchain for iot. In: *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*. [S.l.: s.n.], 2017. p. 173–178.

4 NAKAMOTO, S. *Bitcoin: A peer-to-peer electronic cash system*. 2009. <http://www.bitcoin.org/bitcoin.pdf>.

5 SCHWARTZ, N. Y. D.; BRITTO, A. *The Ripple Protocol Consensus Algorithm*. 2014. <https://ripple.com/files/ripple_consensus_whitepaper.pdf>.

6 POPOV, S. *The Tangle*. 2017. <https://iota.org/IOTA_Whitepaper.pdf>.

7 MAHMOUD, R. et al. Internet of things (iot) security: Current status, challenges and prospective measures. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. [S.l.: s.n.], 2015. p. 336–341.

8 GOODIN, D. *Brace yourselves - source code powering potent IoT DDoSes just went public*. 2016. <https://arstechnica.com/information-technology/2016/10/brace-yourselves-source-code-powering-potent-iot-ddoses-just-went-public>.

9 DORRI, A.; KANHERE, S. S.; JURDAK, R. Towards an optimized blockchain for iot. In: *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*. [S.l.: s.n.], 2017. p. 173–178.

10 MERKOW, M. S.; BREITHAUPT, J. *Information Security: Principles and Practices*. [S.l.]: Pearson IT Certification; 2 edition, 2014.

11 PROJECT, O. *Security by Design Principles*. 2016. <https://www.owasp.org/index.php/Security_by_Design_Principles>.

12 KATZ, J.; LINDELL, Y. *Introduction to Modern Cryptography, Second Edition*. 2nd. ed. [S.l.]: Chapman & Hall/CRC, 2014. ISBN 1466570261, 9781466570269.

13 VAIDYA, K. *The Byzantine General's Problem*. 2016. <https://medium.com/all-things-ledger/the-byzantine-generals-problem-168553f31480>.

14 VAIDYA, K. *Proof-of-Stake FAQs*. 2018. <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#what-is-proof-of-stake>.

15 BUTERIN, V. *A Proof of Stake Design Philosophy*. 2016. <https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51>.

16 CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and smart contracts for the internet of things. *IEEE Access*, v. 4, p. 2292–2303, 2016. ISSN 2169-3536.

17 PROJECTS, T. L. F. *Hyperledger*. 2018. <https://www.hyperledger.org/>.

18 UMPIERES, R. T. *MineraÃ§Ã£o de Bitcoin jÃ¡ gasta mais energia do que 159 paÃses juntos*. 2017. <https://www.infomoney.com.br/mercados/bitcoin/noticia/7112594/mineracao-bitcoin-consome-mais-energia-que-159-paises-juntos>.

19 MARQUES, D. *O que fazer se a sua transaÃ§Ã£o Bitcoin ficar presa*. 2017. <https://guiadobitcoin.com.br/o-que-fazer-se-a-sua-transacao-bitcoin-ficar-presa>.

20 HERTIG, A. *Blockchain's Once-Feared 51% Attack Is Now Becoming Regular*. 2018. <https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular>.

21 ROCCO, G. *Emptied IOTA Wallets Hackers Steal Millions Using Malicious Seed Generators*. 2018. <https://www.ccn.com/a-number-of-iota-wallets-emptied-by-hackers-due-to-online-seed-generators>.

22 BRODY, P.; PURESWARAN, V. *Device democracy: Saving the future of the Internet of Things*. 2014. <http://www-935.ibm.com/services/us/gbs/thoughtleadership/Internetofthings>.

23 ANGWIN, J. *Own a Vizio Smart TV? It's Watching You.* 2015. <https://www.propublica.org/article/own-a-vizio-smart-tv-its-watching-you>.

24 BENET, J. *IPFS Content Addressed, Versioned, P2P File System*. 2014. <https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf>.

25 ORSINI, L.; COLLINS, B. *LO3Energy*. 2015. <https://lo3energy.com/>.

26 TIAN, F. An agri-food supply chain traceability system for china based on rfid amp;amp; blockchain technology. In: *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*. [S.l.: s.n.], 2016. p. 1–6. ISSN 2161-1904.

27 DUAN, X. et al. Dnsledger: Decentralized and distributed name resolution for ubiquitous iot. In: *2018 IEEE International Conference on Consumer Electronics (ICCE)*. [S.l.: s.n.], 2018. p. 1–3. ISSN 2158-4001.

28 PAN, J. et al. Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal*, p. 1–1, 2018. ISSN 2327-4662.

29 SHARMA, P. K.; CHEN, M.; PARK, J. H. A software defined fog node based distributed blockchain cloud architecture for iot. *IEEE Access*, v. 6, p. 115–124, 2018. ISSN 2169-3536.

30 SONG, J. C. et al. Blockchain design for trusted decentralized iot networks. In: *2018 13th Annual Conference on System of Systems Engineering (SoSE)*. [S.l.: s.n.], 2018. p. 169–174.

31 AYOADE, G. et al. Decentralized iot data management using blockchain and trusted execution environment. In: *2018 IEEE International Conference on Information Reuse and Integration (IRI)*. [S.l.: s.n.], 2018. p. 15–22.

32 WANG, Z. et al. Iot security model and performance evaluation: A blockchain approach. In: *2018 International Conference on Network Infrastructure and Digital Content (IC-NIDC)*. [S.l.: s.n.], 2018. p. 260–264. ISSN 2575-4955.

33 PINNO, O. J. A.; GREGIO, A. R. A.; BONA, L. C. E. D. Controlchain: Blockchain as a central enabler for access control authorizations in the iot. In: *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*. [S.l.: s.n.], 2017. p. 1–6.

34 NOVO, O. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet of Things Journal*, v. 5, n. 2, p. 1184–1195, April 2018. ISSN 2327-4662.

35 RIFI, N. et al. Towards using blockchain technology for iot data access protection. In: *2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB)*. [S.l.: s.n.], 2017. p. 1–5.

36 ALPHAND, O. et al. Iotchain: A blockchain security architecture for the internet of things. In: *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. [S.l.: s.n.], 2018. p. 1–6. ISSN 1558-2612.

37 HAMMI, M. T.; BELLOT, P.; SERHROUCHNI, A. Bctrust: A decentralized authentication blockchain-based mechanism. In: *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. [S.l.: s.n.], 2018. p. 1–6. ISSN 1558-2612.