UNIVERSIDADE FEDERAL DO MARANHÃO

Curso de Ciência da Computação

Elijunior Maciel da Silva

BlockChain como alternativa para segurança e privacidade em dispositivos IoT

São Luís/MA

2021

Elijunior Maciel da Silva

BlockChain como alternativa para segurança e privacidade em dispositivos IoT

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Areolino de Almeida Neto

São Luís/MA

2021

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Maciel da Silva, Elijunior.
BlockChain como alternativa para segurança e privacidade em dispositivos IoT / Elijunior Maciel da Silva. - 2021.
58 f.

Orientador(a): Areolino de Almeida Neto.
Monografia (Graduação) - Curso de Ciência da Computação, Universidade Federal do Maranhão, São Luis, 2021.

1. BlockChain. 2. IoT. 3. Privacidade. 4. Segurança. I. Almeida Neto, Areolino de. II. Título.

Elijunior Maciel da Silva

BlockChain como alternativa para segurança e privacidade em dispositivos IoT

Monografia apresentada ao curso de Ciência da Computação da Universidade Federal do Maranhão, como parte dos requisitos necessários para obtenção do grau de Bacharel em Ciência da Computação.

Trabalho aprovado em São Luis – MA , _____ de Abril de 2021

_____

Prof. Dr. Areolino de Almeida Neto
(Orientador)
Universidade Federal do Maranhão

_____

Prof. Dr. Mario Antonio Meireles Teixeira
Examinador 1
Universidade Federal do Maranhão

_____

Prof. MSc. Antonio de Abreu Batista Júnior
Examinador 2
Universidade Federal do Maranhão

São Luís/MA

2021

Agradecimentos

Primeiro agradeço a Deus, que está comigo e me deu a oportunidade de viver e força para não desistir dos meus sonhos e objetivos.

Em segundo, agradeço aos meus pais Elinaldo e Nelizania, que sempre acreditaram no meu potencial e não mediram esforços para que eu realizasse meus sonhos, sem eles nada disso seria possível, amo muito vocês e obrigado por tudo.

Agradeço às minhas avós Domingas e Luíza (*in memoriam*), que mesmo partindo cedo, nunca mediram amor e cuidados à mim quando criança. Tenho certeza que ficariam orgulhosas da pessoa que me tornei.

À minha irmã Naldiane e ao meu sobrinho Pietro, que mesmo não contribuindo diretamente para a minha graduação, sempre me motivaram a seguir meus objetivos.

Um agradecimento muito especial à minha amiga Carol, que desde o primeiro dia de curso vem me ajudando em tudo, muito obrigado pelos conselhos dados a mim nos momentos que mais precisei.

Agradeço aos Apaixonados, grupo de amigos do curso que ganhei na graduação, muito obrigado à Stheffane, ao Cláudio, à Paulina e ao Icaro, vocês foram essenciais nessa jornada.

Aos meus amigos do curso de serviço social, vocês foram incríveis por me acolher tantas vezes, agradeço à Cleoma, Willaine, Rayssa, Tássia e Karina.

Agradeço imensamente aos meus melhores amigos do coração, Ana Cléa, Paulo Rafael e Délis, passamos por momentos únicos nesses anos de amizades e por isso agradeço todo apoio dado, a todos os risos e momentos que estiveram comigo nos meus piores instantes, amo vocês.

Agradeço também às orações e palavras de sabedoria de dona Zedite e dona Beta, que sempre me deram palavras de conforto para enfrentar os momentos difíceis dessa jornada e nunca esqueceram de colocar-me em suas orações.

Agradeço profundamente à dona Laura e família, que sempre me acolheram em momentos de dificuldade e deram-me muito amor, acolheram -me como uma segunda família e serei eternamente grato a vocês por isso.

Aos meus ex-orientadores de pesquisa, Prof. Dr. Mário e Prof. Dra. Simara, que me proporcionaram oportunidade de inserir-me na ciência, proporcionando-me conhecimento e investigação científica.

Agradeço imensamente ao professor de filosofia Vicente Juciê, meu ex-orientador de extensão do curso de Física em 2013. Obrigado por ser a pessoa que abriu tanto minha mente para o fazer ciência. Você foi essencial nesse processo.

Por fim, agradeço ao meu orientador deste trabalho de monografia, Prof. Dr. Areolino, pela paciência e conhecimento repassado à mim nesses meses de orientação.

"A persistência é o caminho do êxito."

(Charles Chaplin)

Resumo

A Internet das Coisas (IoT) refere-se a uma revolução tecnológica que tem como objetivo conectar os itens usados do dia a dia à internet. Cada vez mais surgem eletrodomésticos, meios de transporte e até mesmo tênis, roupas e maçanetas conectadas à Internet e a outros dispositivos, como computadores e smartphones. No entanto, a falta de medidas de segurança torna a IoT vulnerável às ameaças, à privacidade e à segurança. Com sua "segurança por projeto", Blockchain pode ajudar no tratamento dos principais requisitos de segurança na IoT. Características do BlockChain, como imutabilidade, transparência, auditabilidade, a criptografia de dados e a resiliência operacional podem ajudar a resolver a maioria das deficiências arquitetônicas da IoT. Este trabalho de conclusão de curso de graduação apresenta um estudo aprofundado sobre as características de redes Blockchain e IoT e sua integração um com o outro. E por fim, serão demonstrados alguns trabalhos que usaram esta integração para prover maior segurança de dados.

Palavras-Chaves: BlockChain, IoT, Segurança, Privacidade;

Abstract

The Internet of Things (IoT) refers to a technological revolution that aims to connect everyday items used to the internet. Household appliances, means of transport and even sneakers, clothes and doorknobs connected to the Internet and other devices such as computers and smartphones are appearing more and more. However, the lack of security measures makes the IoT vulnerable to threats, privacy and security. With its "security by design", Blockchain can help address key security requirements in the IoT. BlockChain features, such as immutability, transparency, auditability, data encryption and operational resilience can help solve most of the architectural deficiencies in the IoT. This graduation course work presents an in-depth study on the characteristics of Blockchaine IoT networks and their integration with each other. Finally, some works that used this integration to provide greater data security will be demonstrated.

Keywords: BlockChain, IoT, Security, Privacy;

Lista de ilustrações

Lista de abreviaturas e siglas

UFMA	Universidade Federal do Maranhão
IoT	Internet of Things
LLNs	Low Power and Lossy Networks
TIC	Tecnologia daInformação e Comunicaçã
NIST	National Institute of Standards and Technology
RSA	Rivest–Shamir–Adleman
ECC	Elliptic-curve cryptography
IP	Internet Protocol
IA	Inteligencia Artificial
P2P	Peer-to-Peer
TTP	Trusted Third Party
PoW	Proof of Work
IBM	International Business Machines
EVM	Ethereum Virtual Machine
TLD	Top-Level Domain
API	Application Programming Interface
DHT	Distibuted Hash Table)
DACs)	Corporações Autônomas Distribuídas
DNS	Domain Name System
TI	Tecnologia da Informação
BIoT	Blockchain Internet of Things

Sumário

1 INTRODUÇÃO

A rápida evolução da miniaturização da eletrônica e das tecnologias de comunicação sem fio contribuiu para avanços sem precedentes em nossa sociedade. Isso resultou não somente em um aumento no número de dispositivos eletrônicos adequados para muitas áreas, mas também em uma redução em seus custos de produção e em uma mudança de paradigma do mundo real para o digital.

Com o crescimento de dispositivos inteligentes e redes de alta velocidade, a Internet das Coisas (IoT – do inglês Internet of Things) ganhou ampla aceitação e popularidade como o principal padrão para redes com baixa perda de energia (LLNs) com recursos limitados. A IoT capacita qualquer "coisa" para conectar-se e comunicar-se, assim, convertendo o mundo físico em um enorme sistema de informação. Várias tecnologias, como computação em nuvem e aprendizado de máquina para análise de dados e modelagem de informações, estão rapidamente se tornando uma parte integrante da malha IoT. O enorme avanço no campo da IoT está causando crescimento também nos negócios de Tecnologia da Informação e Comunicação (TIC). A IoT está permitindo o desenvolvimento de novos métodos de negócios e um de seus aspectos mais essenciais reside no aprimoramento de dados que afetará o crescimento do mercado de TIC.

De acordo com a Cisco (2016), estima-se que 500 bilhões de objetos estarão conectados à Internet até 2030 e, em 2018, o número de dispositivos IoT já era maior do que a população mundial (Yu et al., 2018).

Ao mesmo tempo que a IoT poderá proporcionar-nos benefícios valiosos, ela também aumentará os nossos riscos de exposição a diversas ameaças de segurança e privacidade, algumas dessas ameaças são novas e bem particulares desta tecnologia. Antes do advento da Internet das Coisas, a maioria das ameaças de segurança estavam relacionadas ao vazamento de informações e a negação de serviço. Com a IoT, as ameaças à segurança vão muito além do roubo de informações ou da impossibilidade de uso de determinados serviços. Essas ameaças podem agora estar potencialmente relacionadas com as vidas reais, inclusive de segurança física.

Uma forma de fornecer confiabilidade em dados de IoT é por meio de um serviço distribuído com a confiança de todos os seus participantes, que garante que os dados permaneçam imutáveis.

Nesse sentido, uma nova tecnologia que nasceu como a primeira criptomoeda descentralizada tem o potencial de oferecer uma solução para o problema de confiabilidade dos dados: o Bitcoin, que revolucionou os mecanismos de transferência de dinheiro. O Bitcoin é suportado por um protocolo que detalha a infraestrutura responsável por garantir

que as informações permaneçam imutáveis ao longo do tempo. Este protocolo é conhecido como o BlockChain e tem sido aplicado em muitas outras áreas, e a imutabilidade da informação é garantida em aplicações que vão além das criptomoedas.

1.1 Objetivo

Este trabalho visa a 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.

1.1.1 Objetivos Específicos

- Categorizar os desafios de sistemas de Internet das Coisas que podem se beneficiar do 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;
- Analisar o contexto e identificar questões em aberto para pesquisas futuras.

1.2 Justificativa

Com a presença cada vez maior de objetos IoT e sua visibilidade na Internet, a segurança, ou seja, o acesso dos usuários legítimos aos recursos é a principal preocupação. Por um lado, a natureza ubíqua da IoT incentiva a criação de aplicativos inovadores para o usuário final, mas, por outro lado, a falta de medidas de segurança pode levar a problemas críticos, como pessoas sujeitas a danos físicos ou roubo devido ao *hacking* do sistema de alarme inteligente. A segurança tem outro aspecto: a preocupação com a privacidade associada a isso. Empresas centralizadas que gerenciam dados confidenciais de usuários podem usá-los de forma ilegítima, levando a uma violação de privacidade (Novo, 2018).

Agrava a situação o fato de que há alguns anos pensar em um cenário com bilhões de dispositivos conectados era bastante improvável e, por isso, os aspectos de segurança nem sempre foram considerados na fase de *design* dos produtos. Na verdade, de acordo com estudos conduzidos mundialmente pela empresa Gartner, os gastos com segurança IoT chegaram a US $ 1,5 bilhão em 2018 e, em 2022, metade de todos os orçamentos de segurança para IoT irá para remediação de falhas, *recalls* e falhas de segurança em vez

de proteção. Portanto, a expansão progressiva dos negócios relacionados a este tipo de ambientes sempre conectados implica em novos desafios tecnológicos e implicações sobre a segurança, a privacidade e a interoperabilidade desses ambientes.

Tem havido um enorme esforço nos últimos anos para lidar com os problemas de segurança no paradigma da IoT. Algumas dessas abordagens destinam-se a problemas de segurança em uma camada específica, enquanto outros objetivam fornecer segurança de ponta a ponta para a IoT. Alaba et al. (2017) categorizaram os problemas de segurança em termos de aplicativo, arquitetura, comunicação e dados. Da mesma forma, outra pesquisa, de Granjal, Monteiro e Sá Silva (2015), discute e analisa questões de segurança para os protocolos definidos para IoT.

IoT trouxe consigo um aumento da quantidade de informações pessoais que serão entregues e compartilhadas entre os dispositivos conectados. Assim, embora não seja uma demanda nova ou exclusiva deste novo cenário, a privacidade é um elemento importante que, em virtude de suas especificidades, demanda mecanismos capazes de auditar e controlar acesso nestes ambientes.

Neste contexto que Blockchain também se insere, pois, essa tecnologia pode ser usada para autenticar, autorizar e auditar os dados gerados pelos dispositivos. Além disso, em virtude de sua natureza descentralizada, elimina a necessidade de confiança em terceiros e não possui um ponto único de falha.

1.3 Trabalhos Relacionados

Nos últimos anos, os pesquisadores têm tentado resolver o problema de integração de BlockChain com IoT. Reyna et al. (2018) analisaram os desafios emergentes da integração da IoT e BlockChain. Eles apresentaram possíveis formas de integração e plataformas que estão integrando IoT e BlockChain em um contexto geral. As aplicações disruptivas nesta área foram destacadas em adição a uma revisão das plataformas BlockChain disponíveis para abordar esses desafios.

Kouicem, Bouabdallah e Lakhlef (2018) forneceram uma pesquisa abrangente top-down das propostas de segurança e privacidade mais recentes em IoT. Foi discutido particularmente os benefícios que novas abordagens, como BlockChain e Rede Definida por Software podem trazer segurança e privacidade em IoT em termos de flexibilidade e escalabilidade. Finalmente, foi dado uma classificação geral das soluções e comparação com base em parâmetros importantes.

Marmol et al. (2018) fizeram um levantamento do estado da arte em que o Blockchain foi usado para fornecer algum nível de privacidade e segurança para IoT e apresentaram uma variante de um ataque de mineração egoísta, que foi chamado de Stalker . O Stalker

é uma mineração maliciosa que visa bloquear um minerador específico de publicar seus blocos.

Christidis e Devetsikiotis (2016) forneceram uma taxonomia sobre a BlockChain avaliando prós e contras da introdução de BlockChain na IoT. Várias ideias foram propostas, como o uso de BlockChain e InterPlanetary File System (IPFS) para atualizar o *firmware* dos dispositivos IoT por ativação de contratos inteligentes.

Conoscenti, Vetrò e De Martin (2016) realizaram uma revisão sistemática da literatura para verificar se os casos de uso documentados no estado da arte confirmam a possibilidade de armazenamento de dados em diferentes pares, tendo a segurança do Blockchain para garantir sua autenticidade e impedir acesso não autorizado. Também, investigam quais são os principais fatores que afetam os níveis de integridade, anonimato e adaptabilidade do BlockChain.

1.4 Estrutura do Trabalho

O restante do trabalho está organizado da seguinte forma: No segundo capítulo, "Fundamentação Teórica", serão apresentados os conceitos principais à segurança e criptografia como base para o entendimento referente à Internet das Coisas e BlockChain, visto que compõem a base teórica necessária para compreensão do tema, no final deste capítulo também será abordado sobre os desafios que o Blockchain traz.

A seguir no terceiro capítulo, "Aplicabilidade do BlockChain em IoT", será abordado o processo para a otimização da integração do Blockchain à Internet das Coisas, além de demonstração de casos de usos para promover a segurança e privacidade e ferramentas de controle de acesso aos dados.

Por fim, serão apresentadas as conclusões deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

A revolução tecnológica ocorrida nas últimas décadas destaca o papel de novas tendências, seus estudos e suas aplicações. Para o entendimento do contexto no qual este trabalho está inserido, faz-se necessário a apresentação de um referencial teórico. A rede IoT sofre de diferentes tipos de comportamentos e ataques devido aos recursos limitados e restrições de espaço de memória. Neste capítulo, concentramos-nos principalmente nos princípios teóricos de segurança, BlockChain e Internet das Coisas, após, partiremos para a investigação dos desafios de segurança na proteção do processo de roteamento de IoT e processo de autenticação de dispositivo na comunidade IoT.

2.1 Princípios de Segurança e Criptografia

2.1.1 Princípios Fundamentais de Segurança

Segurança e privacidade são princípios básicos de qualquer sistema de informação. Referimos-nos a segurança como a combinação de integridade, disponibilidade e confidencialidade. Normalmente é possível obter segurança usando uma combinação de autenticação, autorização e identificação. Esses conceitos são definidos a seguir por Stallings (1995):

- **Confidencialidade**: Na segurança da informação, a confidencialidade "é a propriedade de que as informações não sejam disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados". Embora semelhantes à "privacidade", as duas palavras não são intercambiáveis. Em vez disso, a confidencialidade é um componente da privacidade que visa proteger nossos dados de visualizadores não autorizados. Exemplos de comprometimento da confidencialidade de dados eletrônicos incluem roubo de laptop, roubo de senha ou e-mails confidenciais enviados a pessoas incorretas.

- **Disponibilidade**: Para que qualquer sistema de informação atenda ao seu propósito, a informação deve estar disponível quando necessário. Isso significa que os sistemas de computação usados para armazenar e processar as informações, os controles de segurança usados para protegê-las e os canais de comunicação usados para acessá-las devem estar funcionando corretamente. Os sistemas de alta disponibilidade têm como objetivo permanecer disponíveis o tempo todo, evitando interrupções no serviço devido a quedas de energia, falhas de hardware e atualizações do sistema. Garantir a disponibilidade também envolve a prevenção de ataques de negação de serviço, como uma inundação de mensagens recebidas no sistema de destino,

essencialmente forçando-o a desligar. Blockchain alcança este objetivo ao permitir que os usuários estabeleçam conexão com vários usuários e ao manter os blocos de maneira descentralizada com várias cópias dos blocos na rede.

- **Autenticação, Autorização e Auditoria**: Busca verificar a identidade de quem realiza uma determinada função em um sistema, verificar que direitos esse usuário possui e armazenar informações de uso desse usuário. A estrutura da Blockchain é totalmente desenvolvida para garantir estas três funções, pois somente os usuários que possuem as chaves privadas podem realizar transações, e todas as transações são públicas e auditáveis.

- **Integridade**: Em segurança da informação, integridade de dados significa manter e garantir a precisão e integridade dos dados ao longo de todo o seu ciclo de vida. Isso significa que os dados não podem ser modificados de maneira não autorizada ou não detectada. Isso não é a mesma coisa que integridade referencial em bancos de dados, embora possa ser visto como um caso especial de consistência, conforme entendido no modelo ACID clássico de processamento de transações. Os sistemas de segurança da informação normalmente fornecem integridade de mensagens juntamente com confidencialidade.

- **Não-repúdio**: O não-repúdio neste contexto, implica que uma parte de uma transação não pode negar ter recebido uma transação, nem pode a outra parte negar ter enviado uma transação.

A privacidade pode ser definida como o direito que um indivíduo tem em não compartilhar suas informações. Os usuários do Bitcoin usam um pseudônimo (endereço) para realizar suas transações. Normalmente, cada usuário possui centenas de endereços. Uma transação pode ser vista como uma cadeia de assinaturas que comprovam a posse e a transferência de valores, de maneira auditável. Assim uma das preocupações é que essas transações possam revelar informações do usuário que vão além de simplesmente uma identificação, como hábitos de compra e locais frequentados do usuário.

O conceito de privacidade em Blockchain consiste em manter o anonimato e a desvinculação de transações. O anonimato de transações exige que não seja possível vincular uma transação particular a um usuário, para isto, o usuário utiliza um endereço diferente a cada nova transação. A desvinculação das transações exige que duas transações do mesmo indivíduo não possam ser vinculadas como tal.

2.1.2 Criptografia e Função Hash

Criptografia

Durante séculos, a criptografia foi usada para impedir que humanos não autorizados leiam as comunicações uns dos outros. Um algoritmo de criptografia obtém uma mensagem legível e a converte em uma mensagem ilegível com a intenção de manter as mensagens seguras. Existem dois métodos para fazer isso. A primeira é a criptografia de chave simétrica, que normalmente é o que a maioria das pessoas pensam em relação à criptografia. Pode ser comparado ao uso de uma chave em um cadeado. A mesma chave pode ser usada para bloquear e desbloquear o cadeado.

O segundo método é a criptografia de chave pública, que na verdade é a forma mais usada de criptografia. A criptografia de chave pública depende de uma chave pública e uma chave privada para criptografar e descriptografar o texto. A chave pública é disponibilizada a todos e pode ser usada para criptografar o texto, mas apenas a chave privada pode descriptografá-lo.

A eficiência de um sistema de criptografia pode ser medida considerando:

- **Carga Computacional**: Mede a eficiência com que os algoritmos podem implementar as transformações com as chaves públicas e privadas.
- **Tamanho da Chave**: O NIST indica o uso de pares de chave (pública, privada) com tamanhos, em bits, para cada tipo de implementação: RSA (1088,2048), DAS (1026,160), e ECC (161,160). O ECC apresenta grande vantagem nesse aspecto.
- **Tamanho de Banda**: Corresponde a quantidade de bits necessária para transmitir uma mensagem, após codificar ou assinar.

Função Hash

Hashing, ou um algoritmo de *hash*, é um processo unilateral que mapeia dados de entrada de comprimento variável para dados de comprimento fixo. É uma técnica que usa uma operação matemática para reduzir uma quantidade aleatória de dados de entrada (chamada de chave *hash*) em uma sequência de bits de comprimento fixo de uma forma que é muito impraticável para reverter em computadores modernos.

Um dos usos mais frequentes para o *hash* é verificar a integridade de arquivos. Por exemplo, ao assinar digitalmente um documento, a pessoa que o recebe, além de verificar a chave usada para a assinatura, também compara o *hash* fornecido pelo emissor do documento com o calculado na hora do recebimento. Caso o documento sofra alguma alteração, os resumos serão diferentes. O tamanho da saída do *hash* depende do algoritmo usado, mas o importante é que ela seja sempre do mesmo tamanho, não importando o

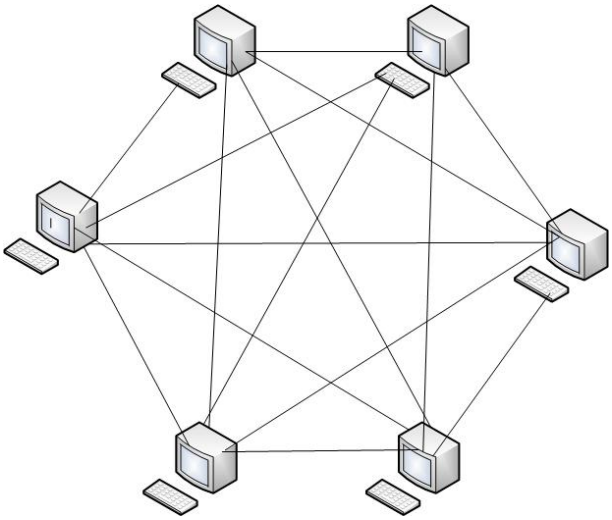
tamanho da entrada. Exemplos de algoritmos de *hash* são o SHA-256 e o RIPEMD160, ambos usados pelo Bitcoin. Os algoritmos de *hash* devem possuir algumas características:

- **Unidirecionalidade**: conhecido um resumo h(M), deve ser computacionalmente impossível encontrar M a partir do resumo.
- **Compressão**: a partir de uma mensagem de qualquer tamanho, o resumo h(M) deve ter uma longitude fixa.
- **Facilidade de cálculo**: deve ser fácil calcular h(M) a partir de uma mensagem M.
- **Difusão**: o resumo h(M) deve ser una função complexa de todos os bits da mensagem M: se se modifica um só bit da mensagem M, o *hash* h(M) deverá mudar a metade dos seus bits aproximadamente.
- **Colisão fraca**: será computacionalmente impossível, conhecido M, encontrar outro M' tal que h(M) = h(M'). Isto se conhece como resistência débil às colisões.
- **Colisão forte**: será computacionalmente difícil encontrar um par (M, M') de forma que h(M) = h(M'). Isto se conhece como resistência forte às colisões.

Rede Peer-to-Peer (P2P)

Segundo a definição do dicionário Português-Inglês, peer to peer significa, de pares em pares. Isso quer dizer que os computadores da rede estão todos interligados em uma cadeia descentralizada, onde cada um possui funções equivalentes não havendo uma hierarquia entre eles. Todos os usuários são clientes e servidores, funcionando, assim, de forma totalmente independente e livre da existência de um servidor central.

Figura 1 – Representação de uma rede peer-to-peer



Fonte: (Renan Bernardo Valadão, 2008)

A vantagem de uma arquitetura de rede descentralizada é que ela é bem mais difícil de ser interrompida, pois não existe mais um ponto de falha. Porém a busca neste tipo de rede é muito lenta e não é garantido que a consulta terá algum resultado, porque o arquivo desejado pode estar a uma distância muito grande para ser alcançado.

Existem quatro funções que podem ser assumidas por um nó na rede: roteamento; base de dados Blockchain; mineração; e carteira. Um nó completo possui todas as quatro funções, mas todos os nós possuem pelo menos a função de roteamento. Estas funções foram separadas, pois nem todos os participantes da rede precisam executar todas as funções. Um usuário comum, por exemplo, que busca somente um meio de pagamento possui apenas a carteira e o roteamento. Desta forma, ele pode se conectar à rede e realizar transações somente com um celular, sem a necessidade de armazenar toda a cadeia de blocos.

Rede P2P e o Bitcoin

O Bitcoin é uma rede *peer-to-peer* e, portanto, não possui autoridade central com encargos para emitir, verificar e/ou gerenciar as transações. Todo o processo de verificação das transações (conferência das bitcoins no blockchain) se dá através do *proof-of-work* de usuários que disponibilizam poder computacional ao sistema. Tais usuários são denominados “mineradores”. O termo é emprestado dos mineradores de ouro, pois estes usuários são recompensados com as novas bitcoins criadas pelo sistema. A cada dez minutos, uma quantidade definida e conhecida por todos é introduzida no sistema

distribuída de maneira aleatória entre os mineradores, usuários que cederam potencial computacional para estruturar o funcionamento da rede.

2.2 Internet das Coisas (IoT)

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 (Mahmoud et al., 2015).

Figura 2 – Visão geral da IoT

Fonte: (ZIGURAT, 2020)

A IoT visualiza um mundo totalmente conectado, onde as coisas são capazes de comunicar dados e interagir umas com as outras. Isso possibilita uma representação digital do mundo real, por meio da qual muitos aplicativos inteligentes em uma variedade de setores podem ser desenvolvidos. Isso inclui: Casas inteligentes, *weareables*, cidades inteligentes, saúde, automotivo, meio ambiente, água inteligente, rede inteligente, etc. As soluções de IoT estão sendo implantadas em muitas áreas, otimizando a produção e digitalizando as indústrias. Os aplicativos IoT têm características muito específicas, eles geram grandes volumes de dados e requerem conectividade e energia por longos períodos. Isso junto com as limitações de memória, capacidade do computador, redes e fonte de alimentação limitada representam um grande desafio.

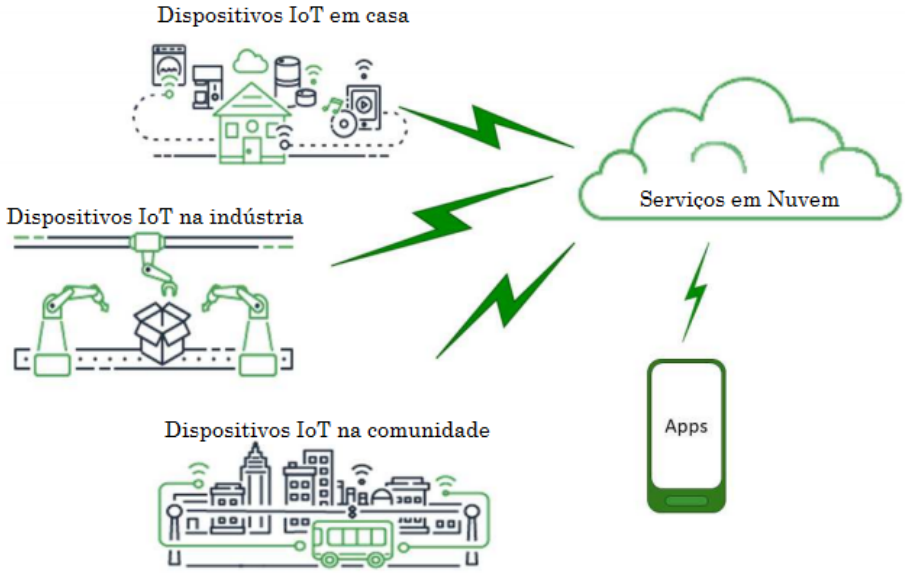
Uma "coisa"na internet das coisas pode ser uma pessoa com um implante de monitor cardíaco, um animal de fazenda com um transponder de biochip , um automóvel que tem sensores embutidos para alertar o motorista quando a pressão do pneu está baixa ou qualquer outro produto natural ou artificial que pode ser atribuído a um endereço de protocolo da Internet (IP) e é capaz de transferir dados em uma rede.

Um ecossistema IoT consiste em dispositivos inteligentes habilitados para *web* que usam sistemas incorporados, como processadores, sensores e *hardware* de comunicação, para coletar, enviar e agir sobre os dados que adquirem de seus ambientes. Os dispositivos IoT compartilham os dados do sensor que coletam conectando-se a um *gateway* IoT ou outro dispositivo de borda onde os dados são enviados para a nuvem para serem analisados localmente. Às vezes, esses dispositivos se comunicam com outros dispositivos relacionados e agem de acordo com as informações que recebem uns dos outros. Os dispositivos fazem a maior parte do trabalho sem intervenção humana, embora as pessoas possam interagir com os dispositivos - por exemplo, para configurá-los, dar-lhes instruções ou acessar os dados.

Os protocolos de conectividade, rede e comunicação usados com esses dispositivos habilitados para web dependem amplamente dos aplicativos IoT específicos implantados.

A Internet das Coisas ajuda as pessoas a viver e trabalhar de maneira mais inteligente, bem como a obter controle total sobre suas vidas. Além de oferecer dispositivos inteligentes para automatizar casas, a IoT é essencial para os negócios. A IoT fornece às empresas uma visão em tempo real de como seus sistemas realmente funcionam, fornecendo percepções sobre tudo, desde o desempenho das máquinas até a cadeia de suprimentos e operações logísticas.

Figura 3 – Principais componentes da IoT



Para a IoT evoluir, um conjunto específico de tecnologias teve que se unir e avançar simultaneamente. Entre eles temos:

- **Conectividade**: Este enorme crescimento no volume de dados de IoT só poderia ter acontecido com uma conectividade de nuvem e Internet suficientemente robusta para enviar e receber dados. Atualmente, muitos dispositivos IoT dependem de uma rede Wi-Fi local para sua capacidade de transmitir dados complexos e volumosos.
- **Tecnologia de Sensores**: Com o aumento constante na demanda por inovação em sensores de IoT, o mercado passou de poucos fornecedores de nicho caros para uma indústria de fabricação de sensores altamente globalizada e de preço competitivo. Desde 2004, o preço médio dos sensores IoT caiu mais de 70%, acompanhado por um aumento impulsionado pela demanda em melhor funcionalidade e diversidade nesses produtos.
- **Poder Computacional**: Espera-se que os 40 zetabytes de dados que os dispositivos IoT geram atualmente quase dobrem nos próximos cinco anos - e assim por diante exponencialmente depois disso. Para usar e aproveitar todos esses dados, as empresas modernas exigem quantidades cada vez maiores de memória e poder de processamento. A corrida para conseguir isso tem sido rápida e competitiva, e tem impulsionado a crescente relevância e aplicabilidade da IoT.
- **Inteligencia Artificial e Aprendizagem de Máquina**: essas tecnologias oferecem às empresas a capacidade de não apenas gerenciar e processar grandes quantidades

de dados de IoT, mas também de analisar e aprender com eles. Quanto maiores e mais diversificados forem os conjuntos de dados, mais robustos e precisos serão os *insights* e informações que a análise avançada com base em IA pode fornecer. O aumento dos dispositivos IoT cresceu muito junto com o avanço da inteligência artificial.

- **Computação em Nuvem**: Com a capacidade de fornecer capacidade de processamento e armazenamento de alto volume sob demanda, os serviços de IoT em nuvem abriram caminho para que os dispositivos de IoT reunissem e transmitissem conjuntos de dados cada vez maiores e complexos. As soluções de nuvem privada também possibilitaram que as empresas gerenciem maiores volumes e tipos de dados de IoT, mantendo a segurança de um sistema fechado.

2.3 BlockChain

O problema da confiança nos sistemas de informação é extremamente complexo quando não são fornecidos mecanismos de verificação ou auditoria, principalmente quando se trata de informações sigilosas, como transações econômicas com moedas virtuais. Nesse contexto, Satoshi Nakamoto, em (NAKAMOTO, 2008) apresentou dois conceitos radicais que tiveram grande repercussão. O primeiro deles é o Bitcoin, uma criptomoeda virtual que mantém seu valor sem o apoio de qualquer autoridade centralizada ou entidade financeira. Em vez disso, a moeda é mantida coletivamente e com segurança por uma rede P2P descentralizada de atores que constituem uma rede auditável e verificável. O segundo dos conceitos, cuja popularidade foi ainda mais longe do que a própria criptomoeda, é o blockchain.

Blockchain é o mecanismo que permite que as transações sejam verificadas por um grupo de atores não confiáveis. Ele fornece um livro razão distribuído, imutável, transparente, seguro e auditável. O blockchain pode ser consultado de forma aberta e completa, permitindo o acesso a todas as transações ocorridas desde a primeira transação do sistema, podendo ser verificada e conferida por qualquer entidade a qualquer momento. O protocolo blockchain estrutura as informações em uma cadeia de blocos, onde cada bloco armazena um conjunto de transações Bitcoin realizadas em um determinado momento. Os blocos são ligados entre si por uma referência ao bloco anterior, formando uma cadeia.

Para oferecer suporte e operar com o blockchain, os pares de rede tem que fornecer, a seguinte funcionalidade: roteamento, armazenamento, carteira de serviços e mineração. De acordo com as funções que oferecem, diferentes tipos de nós podem fazer parte da rede.

A função de roteamento é necessária para participar da rede P2P, o que inclui a transação e a propagação do bloco. A função de armazenamento é responsável por manter uma cópia da cadeia no nó (a cadeia inteira para nós completos e apenas uma parte dela

para nós leves). As carteiras de serviços fornecem chaves de segurança que permitem aos usuários solicitar transações, ou seja, operar com seus Bitcoins. Finalmente, a função de mineração é responsável por criar novos blocos resolvendo a prova de trabalho. Os nós que realizam a prova de trabalho (ou mineração) são conhecidos como mineradores e recebem bitcoins recém-gerados e taxas como recompensa. O conceito de prova de trabalho é uma das chaves para permitir um consenso sem confiança na rede blockchain. A prova de trabalho consiste em uma tarefa computacionalmente intensiva necessária para a geração de blocos. Este trabalho deve ser complexo de resolver e ao mesmo tempo facilmente verificável depois de concluído.

Assim que o minerador conclui a prova de trabalho, ele publica o novo bloco na rede e o restante da rede verifica sua validade antes de adicioná-lo à cadeia. Como a geração de blocos é realizada simultaneamente na rede, a cadeia de blocos pode ramificar-se temporariamente em diferentes ramos (produzidos por diferentes mineradores). Esta discrepância é resolvida considerando que o ramo de blocos mais longo é aquele que será considerado válido. Isso, junto com a natureza intensiva do processo de geração de blocos, fornece um novo mecanismo de consenso distribuído e sem confiança. É muito caro para um atacante mal-intencionado modificar um bloco e corromper a cadeia de blocos, pois o resto dos mineradores confiáveis ultrapassaria o atacante no processo de geração de blocos e, portanto, o ramo confiável dos blocos invalidará aquele gerado pelo atacante. Em termos técnicos, para que um bloco manipulado seja adicionado com sucesso à cadeia, seria necessário resolver a prova de trabalho mais rápido do que o resto da rede, que é computacionalmente muito caro, requer controle de pelo menos 51% dos recursos de computação na rede.

Devido à grande capacidade computacional necessária para modificar o BlockChain, a corrupção de seus blocos é praticamente impossível. Isso significa que, mesmo que os participantes não sejam completamente honestos sobre o uso do Bitcoin, um consenso é sempre alcançado na rede, desde que a maior parte da rede seja formada por participantes honestos. A solução proposta por Nakamoto foi uma grande revolução na confiabilidade dos sistemas descentralizados de atores não confiáveis.

O BlockChain é apenas um sistema de banco de dados distribuído baseado em regras de consenso que permitem a transferência de valor entre entidades. Existem muitos sistemas distribuídos baseados em algoritmos de consenso, mas o BlockChain é o único que possui simultaneamente as três propriedades a seguir:

- **sem confiança**: Não há necessidade de possuir uma identidade digital certificada. As entidades envolvidas não se conhecem, mas podem, de qualquer forma, trocar dados sem ter que saber suas respectivas identidades.

- **sem permissão**: Ninguém decide quem pode ou não operar na rede BlockChain. Não há permissões nem controladores.
- **resistente à censura**: Sendo a BlockChain uma rede sem controladores, onde as entidades confiam apenas na qualidade dos algoritmos criptográficos que regem a operação, qualquer pessoa pode realizar transações na BlockChain. Uma transação, uma vez enviada e aceita, não pode ser interrompida ou censurada.

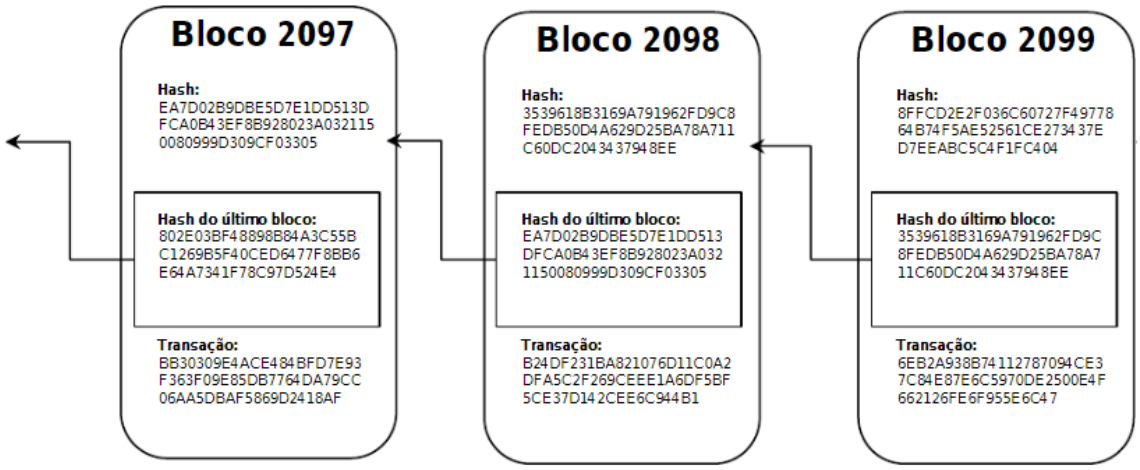
Além disso, a BlockChain pode ser categorizado em dois tipos com base em seu funcionamento: sem permissão e com permissão. Um BlockChain permitido limita os atores que podem participar do consenso do estado do sistema. Em um BlockChain com permissão, apenas uma seleção limitada de usuários tem direitos para validar as transações. Também pode restringir o acesso a atores aprovados que podem criar contratos inteligentes. Por outro lado, o BlockChain sem permissão permite que qualquer pessoa entre na rede, participe do processo de verificação de bloco para chegar a um consenso e também crie contratos inteligentes.

A tecnologia BlockChain é baseada em quatro conceitos centrais:

- **Rede ponto a ponto**: esta solução remove o TTP (Trusted Third Party) central, implicando que todos os nós da rede têm os mesmos privilégios. Nesta rede, os nós podem interagir uns com os outros utilizando um par de chaves privadas / públicas. A chave privada é usada para assinar transações e a chave pública é usada como um endereço acessível na rede.
- **Livro-razão aberto e distribuído**: Imagina-se um livro-razão como um livro contábil que reúne todas as transações da rede em ordem cronológica. Essa estrutura de dados não é uma entidade centralizada, mas cada nó tem sua própria cópia dela. O livro-razão é aberto e público para todos. Todos na rede podem ver onde está o ativo e quantos ativos cada um tem em sua conta também. Além disso, cada nó da rede pode decidir se uma transação é válida ou não válida.
- **Sincronização de cópias contábeis**: Nesse tipo de cenário, em que os nós têm sua própria cópia do mesmo livro-razão, é necessária uma maneira de sincronizar os livros-razão entre os nós. Para atingir tal objetivo, três etapas principais são necessárias (a) para transmitir publicamente as novas transações para a rede, (b) para validar as novas transações, e (c) para adicionar as transações validadas aos livros.
- **Mineração**: Em um sistema distribuído, há atrasos na rede e nem todos os nós recebem as transações (bloco de transações, para ser mais preciso) ao mesmo tempo. Portanto, é necessário evitar que cada nó adicione uma transação à cadeia porque a cadeia deve ter apenas uma ramificação válida e ordenada.

Os mineiros são nós únicos que podem adicionar transações à cadeia. Os mineradores vão competir entre si para entender quem será o primeiro a pegar a nova transação, validá-la e colocá-la no livro razão (corrente). O primeiro mineiro que fizer isso receberá uma recompensa financeira. Para ser o primeiro, um minerador precisa validar a transação e resolver um jogo de adivinhação matemática. Dessa forma, apenas um minerador por vez será capaz de adicionar transações ao BlockChain. Além disso, para evitar ataques ao sistema como o conhecido "ataque de gasto duplo"(KARAME; ANDROULAKI; CAPKUN, 2012), é necessária uma solução para tornar o “jogo” difícil para os mineiros desonestos. Esta solução é essencialmente para tornar caro (investir muito poder de processamento do computador) para os adversários adicionarem transações. Este jogo matemático é denominado Prova de Trabalho (PoW) e é uma operação de hashing inverso para determinar um número (nonce) de modo que o hash SHA-256 do par "conjunto de dados", representativo do bloco (conjunto de transações), e o "nonce"escolhido, seja menos do que um determinado limite . Figura 4 mostra o fluxo para adicionar um novo bloco ao BlockChain. Na próxima subseção será aprofundado o assunto de mineração.

Figura 4 – Fluxo de adição de blocos



2.3.1 Mineração

A mineração é o processo responsável por atualizar a Blockchain, pelo qual alguns nós especiais, chamados de mineradores, incluem as transações em um bloco e geram um cabeçalho válido para essas transações. O mineradores gastam muita energia para realizar a Prova de Trabalho, por esse motivo precisam ser recompensados. A primeira transação do bloco é sempre uma transação especial chamada de *Coinbase*. Ela tem dois propósitos, incluir novas moedas ao sistema e recompensar o minerador. Na rede Bitcoin, a mineração tem dois propósitos. Primeiramente, incluir novas moedas ao sistema e em segundo lugar proteger as transações realizadas. Para gerar esse cabeçalho os mineradores devem calcular

a árvore de merkle das transações, verificar a dificuldade estabelecida, incluir a estampa de tempo e realizar uma série de cálculos a fim de encontrar um nonce que satisfaça a dificuldade em vigor. Assim será descrito a importância da dificuldade e como ela se ajusta automaticamente, além de mostrar um passo a passo do processo de mineração.

A mineração consiste em gerar um novo bloco. Para isso o minerador primeiro cria um "rascunho"de um bloco. É sobre esse rascunho que ele vai trabalhar até que obtenha um bloco viável para ser enviado aos todos os nós da rede. O rascunho é a estrutura de dados que vai comportar os dados do cabeçalho e as transações. Após criar essa estrutura em branco, o minerador preenche alguns campos do cabeçalho: hash do bloco anterior, estampa de tempo, versão e dificuldade. Restando preencher a raiz da arvore de merkle, o nonce e agrupar as transações.

As transações, ao serem geradas, são enviadas via *broadcast* a todos os nós vizinhos e estes reencaminham aos seus vizinhos. Os mineradores, ao receberem uma mensagem com uma transação, às armazenam em uma base de dados de transações ainda não mineradas. As transações permanecem temporariamente em uma espécie de fila com prioridade até que sejam retiradas para ser incluídas em um novo bloco. Cada minerador possui uma fila diferente de transações, e pode selecionar quais transações ele vai incluir nesse novo bloco. Após selecionar quais transações serão incluídas ele irá gerar uma árvore de merkle e incluir o valor da sua raiz no cabeçalho.

Agora falta achar o valor do nonce que fará parte do novo bloco. Esta é a etapa demorada do processo, requer um grande poder computacional dos mineradores e consequentemente um enorme gasto de energia. Para se ter ideia do tempo para achar um hash válido atualmente são comercializados dispositivos especializados em calcular hash, esses dispositivos atingem a marca de 9TH/s, ou seja conseguem calcular nove trilhões de hash por segundo, que com a dificuldade atual da rede Bitcoin seriam necessários 13 anos para achar um hash válido.

Assim que o nonce é encontrado o nosso rascunho fica completo e portanto o bloco está pronto para ser enviado a todos os nós da rede. Os nós da rede ao receberem um novo bloco iniciam uma série de verificações a fim de validar o bloco e chegar a um consenso em caso de bifurcações ("*forks*").

Consenso e Prova de Trabalho

A cadeia de blocos não é criada por uma autoridade central. Os blocos são criados independentemente pelos mineradores da rede. Os nós, usando as informações que são transmitidas através de conexões inseguras, conseguem chegar à mesma conclusão e fabricar o mesmo registro público que todos os outros nós. Atingindo assim um consenso global. Os nós completos armazenam toda cadeia com os blocos que foram validados por ele. Quando diversos nós possuem os mesmos blocos em sua cadeia principal é considerado que eles

chegaram ao consenso. Esta subseção descreve as regras de validação de cada bloco e como o consenso é alcançado e mantido e também explica alguns dos vários mecanismos de consenso que são utilizados atualmente.

O mecanismo de consenso é composto por duas etapas: validação do bloco e seleção da maior cadeia. Estas duas etapas são realizadas de maneira independente por cada nó. Os blocos são enviados em *broadcast* pela rede, e cada nó ao receber um novo bloco o retransmite aos seus vizinhos, mas antes desta retransmissão o nó faz a validação do bloco a fim de garantir que somente blocos válidos sejam propagados. Existe uma extensa lista de verificação a ser seguida, dentre elas:

- Estrutura do bloco;
- Verificar se o hash do cabeçalho atende a dificuldade estabelecida;
- Tamanho do bloco dentro dos limites projetados;
- Verificação de todas as transações;
- Verificação da estampa de tempo.

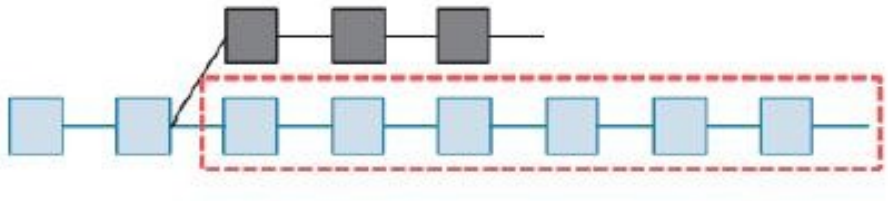
Por definição da Blockchain cada bloco tem somente um pai, mas pode ocorrer uma situação em que um ou mais mineradores gerem novos blocos quase ao mesmo tempo, fazendo com que haja um ou mais filhos com um mesmo pai. Neste caso, entende-se que ocorreu um *fork*, uma bifurcação, na cadeia. A última etapa do mecanismo de consenso serve exatamente para selecionar qual destes blocos fará parte da cadeia principal e qual será descartado. Isso é possível em virtude da prova de trabalho, fundamental para o mecanismo de consenso adotado, pois como vimos anteriormente para gerar o bloco, mineradores gastam muita energia em busca de um bloco válido

Como é possível a ocorrência de bifurcações, os nós armazenam os blocos sem pai (órfãos) e mantém duas cadeias, uma principal e uma secundária. Os blocos órfãos acontecem quando dois blocos são gerados em espaços curtos de tempo e chegam em ordem inversa, ou seja, um bloco foi recebido e não faz referência a um bloco na cadeia. Ele é armazenado por um período de tempo, caso o nó receba um bloco que seja pai do órfão ele será incluídos na cadeia em sua ordem correta. Note que neste caso não houve a ocorrência de uma bifurcação, os blocos apenas foram recebidos fora de ordem.

Como existem diversos mineradores gerando blocos de forma descentralizada, os novos blocos enviados por eles podem chegar a diferentes nós em momentos diferentes, o que pode resultar em visões diferentes. Para ficar mais claro quando dois mineradores geram blocos fazendo referência a um mesmo pai ocorre a bifurcação, e os outros mineradores deverão escolher qual bloco eles irão adotar como referência. Se uma parte dos mineradores

adotar um bloco e outra parte adotar o outro, essas duas cadeias irão coexistir até que uma fique maior que a outra. Para resolver esta situação, os nós que se comportam de maneira honesta, de acordo com o mecanismo de consenso, sempre irão adotar a maior cadeia e o *fork* estará resolvido. A corrente principal é a maior cadeia, aquela onde há a maior quantidade de trabalho acumulada. Na Figura 5 os blocos cinza bifurcaram da cadeia principal, como os blocos azuis alcançaram uma altura maior, passaram a ser a cadeia principal. Os blocos cinzas são descartados e suas transações são consideradas como não confirmadas, devendo ser incluídas futuramente em outros blocos.

Figura 5 – Bifurcação da cadeia de blocos



Fonte: (Renata Kroska, 2018)

Uma das preocupações mais comuns para os sistemas de moedas digitais é a possibilidade do gasto duplo, quando um usuário malicioso gasta um mesmo valor em duas transações diferentes da cadeia. Note que para ocorrer a tentativa de um gasto duplo é necessário uma bifurcação, pois se o gasto ocorrer na mesma cadeia, quando o novo bloco for criado, ele não passará nas verificações iniciais de consistência e será descartado. Com o fork, o usuário malicioso faz um gasto e envia para rede, gasta a mesma quantia novamente em outro lugar e começa a minerar sobre esse gasto. Desta forma, há a possibilidade de ele conseguir minerar um bloco e realizar o fork. A partir deste momento, a rede estará dividida e como mencionado anteriormente haverá uma corrida que será vencida pela maior cadeia. Uma das transações será descartada e o gasto duplo será rejeitado. Como uma das cadeias irá ser aceita pela rede e, a outra descartada, eventualmente o gasto duplo será detectado. É usualmente aceito na rede Bitcoin que uma transação é considerada confirmada quando existem seis novos blocos com altura maior que a sua, pois será necessário muito esforço para alterá-la.

Um cenário de ataque contra o mecanismo de consenso é chamado de "ataque de 51%". Nesse cenário, um grupo de mineradores, controlando uma maioria (51%) do poder de *hash* total da rede, conspira para atacar o Bitcoin. Com a habilidade de minerar a maioria dos blocos, os mineradores atacantes podem gerar bifurcações deliberadas na Blockchain, gerar transações de gasto duplo ou executar ataques de negação de serviço

(DoS) contra endereços ou transações específicas. Um ataque de bifurcação/gasto duplo é um ataque onde o atacante faz com que blocos já confirmados sejam invalidados ao fazer uma bifurcação em um nível abaixo deles, com uma posterior re-convergência em uma cadeia alternativa. Com poder suficiente, um atacante pode invalidar seis ou mais blocos em uma sequência, invalidando transações que antes eram consideradas imutáveis (com seis confirmações). Note que o gasto duplo só pode ser feito nas transações do próprio atacante, para as quais o atacante pode produzir uma assinatura válida. Fazer um gasto duplo da própria transação é rentável quando, ao invalidar uma transação, o atacante puder receber um pagamento irreversível ou um produto sem ter que pagar por isso.

Alcançar o consenso em um sistema distribuído é um desafio. Os algoritmos de consenso devem ser resilientes a falhas de nós, particionamento da rede, atrasos de mensagens, mensagens que chegam fora de ordem e corrompidas. Eles também têm que lidar com nós egoístas e deliberadamente maliciosos. Vários algoritmos tem sido propostos para resolver isso, cada um realizando o conjunto de suposições necessárias em termos de sincronia, transmissões de mensagens, falhas, nós maliciosos, desempenho e segurança das mensagens trocadas. Para uma rede Blockchain, alcançar consenso garante que todos os nós na rede concordem com um estado global consistente da cadeia de blocos.

2.3.2 Contratos Inteligentes

Um contrato inteligente é um programa de computador ou um protocolo de transação que se destina a executar, controlar ou documentar automaticamente eventos e ações legalmente relevantes de acordo com os termos de um contrato ou acordo. Os objetivos dos contratos inteligentes são a redução da necessidade de intermediários confiáveis, custos de arbitragem e execução, perdas por fraude, bem como a redução de exceções maliciosas e acidentais.

Com a implementação do Ethereum em 2015 , com base em blockchains ,"Contrato inteligente"é usado principalmente no sentido de computação de propósito geral que ocorre em um blockchain ou livro-razão distribuído. O Instituto Nacional de Padrões e Tecnologia dos Estados Unidos descreve um "contrato inteligente"como uma "coleção de código e dados que é implantado usando transações assinadas criptograficamente na rede blockchain". Nesta interpretação, usada por exemplo pela Ethereum Foundation ou IBM, um contrato inteligente não está necessariamente relacionado ao conceito clássico de contrato, mas pode ser qualquer tipo de programa de computador. Um contrato inteligente também pode ser considerado um procedimento armazenado seguro , pois sua execução e efeitos codificados, como a transferência de algum valor entre as partes, são estritamente impostos e não podem ser manipulados, depois que uma transação com detalhes específicos do contrato é armazenada em um blockchain ou livro-razão distribuído . Isso ocorre porque a execução

real dos contratos é controlada e auditada pela plataforma, não por quaisquer programas arbitrários do lado do servidor que se conectam à plataforma.

No domínio da criptomoeda, os contratos inteligentes são assinados digitalmente da mesma forma que uma transação de criptomoeda é assinada. As chaves de assinatura são mantidas em uma carteira criptografada . Algoritmos tolerantes a falhas bizantinos permitiram a segurança digital por meio da descentralização para formar contratos inteligentes.

Contratos Inteligentes são definidos como um protocolo de transação computadorizado que executa os termos de um contrato preestabelecido (Christidis; Devetsikiotis, 2016). 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, Contratos Inteligentes 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 Contratos Inteligentes 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 (Christidis; Devetsikiotis, 2016).

Como os contratos inteligentes têm endereços próprios, eles também têm a capacidade de armazenar ou transferir moedas. Um dos exemplos de uso de Contratos Inteligentes 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.

Ethereum, é o *framework* mais conhecido e utilizado para contratos inteligentes. Ethereum é uma máquina virtual descentralizada, que executa programas chamados

contratos a pedido dos usuários. Contratos são escritos em uma linguagem Turing-completa *bytecode*, chamado EVM bytecode [Wood, 2014]. Um contrato é um conjunto de funções, cada uma definida por uma sequencia de instruções *bytecode*. Uma característica notável dos contratos é que eles podem transferir éter (uma criptomoeda similar ao Bitcoin) para/de usuários e para outros contratos. As transações são usadas para:

- criar novos contratos;
- invocar funções de um contrato;
- transferência de ether para contratos ou para outros usuários.

Todas as transações são registradas em uma Blockchain pública. A sequência de transações na Blockchain determina o estado de cada contrato, e o saldo de cada usuário.

Na Figura 6 é apresentado um exemplo de código para um contrato inteligente básico escrito para uso na Blockchain Ethereum. É apresentado um código básico, na linguagem solidity, para a criação de um *token* digital que no ecossistema Ethereum pode representar qualquer bem negociável: moedas, certificados de ouro, etc. Como todos os *tokens* implementam algumas características básicas de uma maneira padrão, isso também significa que esse *token* será instantaneamente compatível com a carteira Ethereum e qualquer outro cliente ou contrato que use os mesmos padrões.

Figura 6 – Exemplo de Contrato Inteligente

```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

Fonte: (Ethereum, 2017)

Uma vez que os contratos têm um valor econômico, é crucial garantir que a sua execução seja executada corretamente. Os potenciais conflitos na execução de contratos (devido, por exemplo, a falhas ou ataques) são resolvidos através de um protocolo de consenso baseado em PoW. Idealmente, a execução de contratos é garantida, mesmo com a presença de um usuário malicioso, desde que ele não possua a maioria do poder computacional da rede. A rede Ethereum atualmente usa um algoritmo de consenso PoW, chamado Ethash, criado especificamente para Ethereum. Foi construído para dificultar seu processamento por meio de hardwares específicos, como o chips ASICs.

A segurança do processo de consenso baseia-se na suposição de que é mais conveniente para um minerador seguir o protocolo do que tentar atacá-lo. Para manter esse pressuposto, os mineradores recebem alguns incentivos econômicos para executar os cálculos exigidos pelo protocolo. Parte desses incentivos é dada pelas taxas de execução pagas pelos usuários em cada transação, ou etapa de execução de um contrato. Um atacante até poderia então criar um contrato com uma execução longa, mas ele ficaria caro demais, pois ele necessitaria pagar taxas a cada etapa do processo. Desta forma, as taxas limitam a quantidade de etapas de execução de um contrato, impedindo assim ataques de negação de serviço que usam computações demoradas.

2.3.3 Categorias de BlockChain com base no acesso aos dados

As blockchains podem ser classificadas de acordo com o tipo de acesso aos dados e participação no processo de validação de um bloco à cadeia. Quanto ao tipo de acesso, pode ser:

- **Pública**: O mecanismo de consenso está aberto a todos. O objetivo de uma cadeia sem permissão é permitir que qualquer pessoa contribua com dados. Isso cria a chamada resistência da censura, o que significa que nenhum ator pode evitar que uma transação seja adicionada à cadeia. Os participantes mantêm a integridade da cadeia ao chegar a um consenso quanto ao seu estado. Qualquer um pode se juntar à rede e participar do processo de verificação de blocos para criar consenso e também criar contratos inteligentes. Ter um sistema sem permissão implica assumir que pode não haver confiança entre os nós, portanto, um mecanismo de consenso fortemente distribuído deve ser imposto.

- **Privada**: Participantes no processo de consenso estão pré-selecionados. Quando um novo registro é adicionado, a integridade do livro razão é verificada por um processo de consenso realizado por um número limitado de atores confiáveis. Isso torna a manutenção de um registro compartilhado muito mais simples do que o processo de consenso sem permissão. As cadeias de blocos permitidas fornecem conjuntos de dados altamente verificáveis porque o processo de consenso cria uma assinatura

digital, que pode ser vista por todas as partes. As características que derivam de sistemas confiáveis podem abrir a possibilidade de evitar um protocolo de consenso computacionalmente exigente, como a PoW.

Apesar da tecnologia blockchain ser comumente referenciada pela rede Bitcoin ou ligada às criptomoedas, diversas redes foram propostas e são utilizadas nos dias atuais, para os mais variados cenários. Exemplos de blockchain públicas e sem permissionamento são Bitcoin e Ethereum, enquanto que Hyperledger e Ripple são com permissionamento.

2.3.4 Desafios

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.

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 (NAKAMOTO, 2008). 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 (Rodrigo Tolotti, 2017). 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 (2008), 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 (Guia do Bitcoin, 2021). Outras 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 (CHASE; MACBROUGH, 2018), 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.

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 Alyssa Hertig (2018), 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 (Vitalik Buterin, 2016) 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 (CHASE; MACBROUGH, 2018), 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 (Gregory Rocco, 2018). 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 Aplicação do BlockChain na IoT

Os dispositivos na IoT coletam, geram e processam dados, enviam estas informações através da internet, produzindo uma gigantesca massa de informação a ser usada pelos mais diversos serviços.

Apesar dos benefícios, problemas críticos relacionados a privacidade podem emergir. A Blockchain pode ter um papel fundamental no desenvolvimento de aplicações descentralizadas que irão executar em bilhões de dispositivos. Entender como e quando esta tecnologia pode ser usada para prover segurança e privacidade é um desafio, diversos autores apontam esses desafios, dos quais citam-se Conoscenti, Vetrò e De Martin (2016).

Neste capítulo é explorado como a Blockchain pode ser usada para beneficiar as aplicações de segurança para Internet das Coisas, como aplicações descentralizadas que permitem que objetos inteligentes interajam com segurança e privacidade.

Além disso, serão apresentados os ataques mais comuns abordados na literatura, tais como: minerador egoísta , gasto duplo e o eclipse.

3.1 Otimização BlockChain para IoT

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. A seguir será demonstrado alguns desafios enfrentado na Internet das Coisas e em seguida algumas pesquisas que tentam solucionar estes desafios através da implementação de redes Blockchain.

3.1.1 Gerenciamento de Recursos

Dispositivos IoT precisam enviar informações para infraestruturas de Cloud remotos para serem processadas, entretanto esse modelo centralizado apresenta desafios de escalabilidade para sistemas IoT de cenário grande devido à grande quantidade de dados gerados e transmitidos (PAN, 2016).

EdgeChain

Com o objetivo de solucionar esse problema e proporcionar uma maior segurança para a estrutura da rede, Pan (2016) 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 7). 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 contratos inteligentes 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.

3.1.2 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 (Duan et al., 2018).

DNSLedger

Em (Duan et al., 2018) 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 8). 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.

3.1.3 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 (Sharma; Chen; Park, 2018). 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, segurança e baixa latência na comunicação.

Rede Blockchain com Armazenamento Centralizado

Em Ayoade et al. (2018) é proposta uma 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 9).

Rede Blockchain com Armazenamento Descentralizado

Em (Wang et al., 2018) é proposta uma solução alternativa à (Ayoade et al., 2018) - em que o armazenamento das informações é realizada em um sistema centralizado. Wang et al. (2018) 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. (2018) 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 10). 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.

3.1.4 Anonimidade e controle de acesso em IoT

É bom ressaltar que a anonimidade provida pelo uso da Blockchain não é absoluta, por isso ela é comumente chamada de pseudo-anonimidade. É possível, em certas circunstâncias, de-anonimizar o dono da transação, ou seu endereço IP. Para deanonimizar as transações

existem algumas técnicas específicas, Conoscenti, Vetrò e De Martin (2016) as dividiu em quatro:

- **Múltiplas Entradas**: Em alguns casos para realizar determinado gasto é necessário reunir saldo de diversas contas. Caso seja preciso guardar o saldo total da carteira em uma única conta, é possível realizar a transferência dos saldo menores para uma única conta, esse procedimento é chamado de transação com múltiplas entradas. Como, para realizar esta transação, é necessário possuir a chave privada de cada entrada é sensato supor que todas as contas pertencem a um mesmo usuário. A partir deste momento é possível associar os endereços a um usuário.
- **Endereços de Troco**: Como já visto, todas as transações no Bitcoin são transferências de recursos. Por definição do protocolo, É obrigatório gastar todo o saldo associado a uma determinada chave. Caso o valor da transação seja menor que o valor da entrada, essa transação irá gerar troco. O valor do troco deve retornar ao dono e por isso deve ser endereçado a uma saída com destino ao próprio usuário. Caso o usuário use sempre o mesmo endereço para receber o troco de suas transações, pode-se associar este endereço aos endereços de entrada anteriores e descrever exatamente todos os gastos de um usuário, além da possível correlação com fontes secundárias de informação como sites de redes sociais.
- **Associação ao IP**: A rede Bitcoin é uma rede sobreposta a rede IP. Grande parte das mensagens da rede são transmitidas em *broadcast* para os vizinhos diretos de cada nó. Uma grande quantidade de vizinhos permite a um nó extrair algum conhecimento da rede, como sua topologia, quem são os nós mineradores, localização dos nós e seu endereço IP.
- **Uso de Serviços Centralizados**: Os usuários podem, por diversos motivos, não guardar e gerenciar suas próprias chaves privadas e delegam essa função a serviços terceirizados. Alguns autores como Möser, Böhme e Breuker (2013) acham um isso risco a privacidade, pois esta entidade pode vazar seus dados, suas identidades e seus recursos, e até mesmo utilizar os recursos de terceiros, pois a prova de propriedade se dá pela posse da chave privada que está nas mãos de terceiros.

Segundo Conoscenti, Vetrò e De Martin (2016) são necessários cuidados extras a fim de mitigar estes problemas. Os dispositivos IoT devem se configurados para: sempre usar um endereço diferente para receber troco; sempre gerar um endereço novo para cada recebimento recursos; não usar serviços terceirizados. Essas medidas não são suficientes para prover anonimidade total, mas proverão um certo grau de segurança em manter as identidades preservadas, evitando principalmente correlacionar um determinado dispositivo ao seu dono.

É possível também usar a Blockchain para armazenar dados e prover controle de acesso a eles. Suponha que um sensor de presença queira armazenar seus histórico diário na Blockchain. Ele irá gerar uma transação com os dados a serem armazenados, e assinará essa transação com sua chave secreta, assim todos saberão qual sensor é dono desses dados. O sensor indicará como saída da transação as chaves públicas com direito de ler seus dados. Ele enviará esta transação aos mineradores de sua rede, que autenticarão a transação e a incluirão no próximo bloco. Como a Blockchain é pública todos os usuários tem acesso a seus dados, e saberão que um determinado usuário tem o direito de ler o histórico produzido pelo do sensor de presença. Mas, somente aqueles detentores das chaves privadas, que fazem par com a públicas indicadas pelo sensor, conseguirão ler o histórico diário que foi disponibilizado pelo sensor.

Möser, Böhme e Breuker (2013) propoem o FairAccess, um *framework*, que usa a Blockchain para habilitar aos usuários controlar seus próprios dados. Ele reutiliza o código do Bitcoin e introduz alguns novos tipos de transação usados para controlar o acesso aos dados, como: "*grant*"e "*revoke access*". O modelo prevê a existência de alguns atores: recurso a ser compartilhado; o dono do recurso; e os usuários. As transações são usadas para controlar o acesso dos usuários e a Blockchain é usada servir como local para armazenamento e leitura das permissões. Os autores fizeram uma prova de conceito com um Raspberry PI com uma câmera("Recurso"). Foi criado um usuário "dono do recurso"e outro usuário "utilizador". O Dono controla o acesso ao recurso através de transações enviadas a Blockchain. Assim para conceder acesso ao usuário ele envia uma transação do tipo *grant access* e a envia ao usuário, como se estivesse vendendo um produto com Bitcoin. Esta transação será minerada pela rede, o que significa dizer que será verificado que o dono possui a chave privada referente ao recurso e a transação será incluída na Blockchain. A partir deste ponto o utilizador solicitará acesso diretamente ao recurso que verifica na Blockchain se existe uma transação que lhe garanta acesso, neste caso o usuário conseguirá acessar a câmera.

Uma das principais críticas ao armazenamento de dados na Blockchain é o uso de estrutura de dados que não foram projetadas para armazenar grandes quantidades de informação. Assim, caso o bloco comece a ser usado com esse fim, haverá diversas cópias de um mesmo arquivo sendo mantidas na rede, uma vez que a cadeia inteira é mantida de foma descentralizada. Além do desperdício de espaço, há a forma ineficiente de gerenciar estes dados. Com o intuito de usar a segurança provida pela Blockchain, Zyskind, Nathan e Pentland (2015) combinam o uso do armazenamento de dados fora da cadeia com o controle de acesso na cadeia de blocos. O armazenamento é realizado com um sistema de DHT (distibuted hash table) sendo mantido por um conjunto de nós da rede previamente selecionados. Os dados são replicados de maneira eficiente pelos nós de forma a garantir a alta disponibilidade e repartida de forma que nenhum nó tenha o arquivo inteiro. A Blockchain é então usada de forma a gerenciar onde esses dados estão distribuídos e quem

tem acesso a eles. Para isso, são gerados dois novos tipos de transação, uma para prover o controle de acesso e outro para controlar a distribuição dos dados no DHT.

3.1.5 Transações eletrônicas em IoT

O futuro da IoT é se tornar uma rede de dispositivos autônomos que podem interagir uns com os outros e com seu ambiente, e tomar decisões inteligentes sem a intervenção humana. Este é o lugar onde a Blockchain pode ajudar a alavancar a IoT e formar uma base que suportará a economia compartilhada baseada em comunicações máquina - máquina. Em (WöRNER; BOMHARD, 2014) os autores descreveram uma implementação prototípica simples do processo de troca de dados por dinheiro eletrônico entre um sensor e um requisitante, utilizando a rede Bitcoin. O sistema é composto de três partes:

- **Dispositivo IoT Cliente**: Precisa cumprir as seguintes tarefas: anotar uma solicitação de dados ao receber um pagamento e ser capaz de criar e publicar uma transação contendo os dados solicitados.
- **Cliente requisitante**: Precisa poder enviar pagamento ao endereço Bitcoin do sensor e deve monitorar alterações na Blockchain até detectar a transação com os dados enviados pelo dispositivo IoT.
- **Repositório de dispositivo IoT**: Onde os sensores podem ser registrados ou podem ser encontrados pelos solicitantes. Uma entrada no repositório de sensores deve conter pelo menos o endereço do Bitcoin, quais os dados que ele oferece, o preço e metadados adicionais como localização, tags, etc.

Um endereço Bitcoin é anexado ao dispositivo IoT que precisa anotar uma solicitação de dados ao receber Bitcoins e precisa ser capaz de criar e publicar uma transação contendo os dados solicitados. A maneira usada pelos desenvolvedores para utilizar a própria rede Bitcoin para vender dados é a utilização da transação do tipo *OP RETURN*.

Esse trabalho demonstrou um processo simples usando a rede Bitcoin com certas limitações, como por exemplo: os dados adquiridos estão disponíveis publicamente na Blockchain. Isso pode ser resolvido criptografando os dados com a chave pública do solicitante, em que o cliente requisitante descriptografa os dados usando sua chave privada.

Em (Zhang; Wen, 2015), os autores propõem uma arquitetura de comércio eletrônico projetada especificamente para as mercadorias IoT, baseada no protocolo do Bitcoin. Foram utilizadas Corporações Autônomas Distribuídas (DACs) como a entidade de transação para lidar com os dados de dispositivos e propriedade inteligente negociados. Nesse modelo as pessoas podem negociar com DACs para obter mercadorias IoT, utilizando criptomoedas

baseadas no protocolo Bitcoin. Para trocar os dados do dispositivo são usados chaves eletrônicas e contratos inteligentes.

São propostas 4 camadas para o modelo IoT de comércio eletrônico, que são: camada técnica básica; camada de infraestrutura; camada de conteúdo e camada de intercâmbio. A camada técnica básica inclui o módulo do mecanismo de classificação das mercadorias, módulo de algoritmo de crédito para efetuar o gerenciamento das carteiras e o módulo Blockchain Bitcoin, que foi a criptomoeda adotada pelo projeto. A camada de infraestrutura contém a plataforma do serviço de informações IoT e a plataforma de contratos inteligentes. A camada de conteúdo inclui duas partes: entidades participante e as mercadorias IoT. As Entidades consistem em DAC e seres humanos. DACs são executados automaticamente sem a interferência do ser humano, cada DAC pode comprar produtos de outros DAC como clientes, enquanto isso, todos podem emitir suas próprias mercadorias IoT. As mercadorias são propriedades inteligentes e dados coletados de sensores. As propriedades inteligentes podem ser obras

de arte, bens duráveis como carros, casas e energia como eletricidade, água, gás e óleo que podem ser controlados e quantificadas por dispositivos digitais por chaves eletrônicas ou sistema de controle de acesso. A camada de intercâmbio inclui o sistema de transações P2P que é o núcleo do modelo de negócios da IoT juntamente com com a criptomoeda escolhida que é a Bitcoin.

O emprego da tecnologia Blockchain com a finalidade de introduzir a funcionalidade de transações econômicas para IoT foi abordado por uma série de propostas e aplicativos, incluindo:

- **Filament**(CROSBY, 2016): um sistema desenvolvido para permitir que os dispositivos tenham identidades únicas em um livro público e possam descobrir, comunicar e interagir uns com os outros de forma autônoma e distribuída. Além disso, os dispositivos envolvidos podem trocar valor diretamente ou indiretamente com uma ampla gama de entidades. Por exemplo, eles poderiam vender dados sobre condições ambientais para uma agência meteorológica. O objetivo é criar um diretório de dispositivos inteligentes que permita que os dispositivos IoT Filament se comuniquem de forma segura, executem contratos inteligentes e enviem microtransações. A pilha de tecnologia de Filament usa cinco tecnologias: *blockname*; *telehash*; contratos inteligentes; *pennybank* e BitTorrent. Usando o *blockname*, os dispositivos são capazes de criar um identificador exclusivo que é armazenado em uma parte do chip incorporado no dispositivo e gravado no bloco. O Telehash, por sua vez, fornece comunicações criptografadas de ponta a ponta e o BitTorrent permite o compartilhamento de arquivos. Os pagamentos pelo uso dos dispositivos são tratados por contratos inteligentes, o que permite que os termos dos pagamentos

e o acesso ao dispositivo sejam controlados por esses programas. O Filament usa um protocolo baseado em Bitcoin que foi desenvolvido para microtransações em sua plataforma, chamado Pennybank, devido a restrições específicas de dispositivos IoT. Os dispositivos IoT não são de alta potência e nem sempre estão online. Assim, o Pennybank cria um serviço de garantia entre dois dispositivos IoT, permitindo que eles liquidem as transações quando estiverem conectados on-line.

- **IOTA** (POPOV, 2015): 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. Popov (2015) argumenta que a estrutura de grafo reduz o tempo de confirmação de transações e melhora a segurança em geral da rede.

3.1.6 Soluções Gerais

Nesta subseção, os trabalhos que propõem soluções genéricas são agrupados. Essas soluções podem ser aplicadas a cada campo do ambiente IoT. Por exemplo, Wörner e Bomhard (2014) propõem um sistema que permite que os sensores troquem Bitcoins com dados. Cada nó possui um endereço que é a chave de publicação do Bitcoin. Essencialmente,

quando um cliente solicita dados de um sensor após descobri-lo em um repositório de sensores, ele envia uma transação endereçada à chave pública desse sensor (incluindo Bitcoins). O sensor responderá enviando uma transação ao cliente incluindo dados. Esta abordagem, na verdade, é uma generalização da solução apresentada em (Zhang; Wen, 2015) e, portanto, é apenas uma aplicação possível de tal tecnologia para permitir compra de dados do sensor na IoT.

Outro novo sistema com o objetivo de realizar tarefas analíticas em dados é apresentado por Xu et al. (2018). O sistema proposto é denominado Sapphire e utiliza o BlockChain como sistema de armazenamento. A ideia principal é explorar o poder de computação do dispositivo IoT para executar software (contratos inteligentes) para realizar cálculos nos dados provenientes de um ambiente inteligente (cidades, redes e edifícios). Dessa forma, o benefício é duplo: (i) reduzir a transferência de dados na rede IoT e (ii) melhorar o tempo de execução utilizando computação paralela em um sistema de armazenamento distribuído. Semelhante ao ADEPT da IBM (IBM, 2015), Sapphire consiste em três tipos diferentes de nós, a saber: nós super, regulares e leves. Esta classi fi cação é feita para atribuir a cada tipo de nó diferentes tarefas de acordo com o recurso de que dispõe. Por exemplo, os nós leves têm poucos recursos e, portanto, não armazenam todo o BlockChain nem realizam tarefas analíticas nos dados de IoT. Os dispositivos IoT (nó super e regular) executam algoritmos nos dados e enviam o resultado final de volta aos usuários. Ouaddah, Elkalam e Ouahman (2017) também propõem esse tipo de uso de BlockChain. Os autores aqui utilizam os conceitos de "Token"e "Contrato inteligente"para atingir seu objetivo. O modelo de controle de acesso proposto é chamado de FairAccess e usa um “contrato inteligente” para fazer cumprir as políticas de acesso e informar as decisões de autorização. Um dos conceitos importantes em BlockChain é o UTXO.

É um valor restrito a um proprietário específico. O UTXO consumido em uma transação é chamado de entrada e o UTXO criado por uma transação é chamado de saída. A ideia dos autores é criar um token de autorização que seja uma assinatura digital que dá o direito de acesso a um destinatário dessa transação. O fluxo funciona da seguinte maneira: Um usuário “A” envia uma solicitação para um proprietário de recurso (RO) “B”. O RO primeiro cria um *token* criptografado com o solicitante PUBk e, em seguida, define as políticas de acesso usando a RO-wallet que funciona como PEP. PEP transforma políticas em um “*script* de desbloqueio” em GrantAccess Transaction e transmite a transação na rede BlockChain que funciona como um Policy Decision Point (PDP). No final, a transação é adicionada ao BlockChain, e o token é registrado na carteira do solicitante. Para obter o acesso aos recursos, o usuário “A” inicialmente faz a varredura em sua carteira para obter o token e depois cria uma transação “GetAccess” para obter o acesso ao recurso do dispositivo “B”. Na entrada desta transação, “A” insere o UTXO = Token de uma transação GrantAccess anterior registrada no BC. Quando “A” tenta acessar recursos do dispositivo “B”, este pode verificar a validade do token.

A IBM, em colaboração com 30 outras empresas bancárias e de TI, deseja desenvolver um BlockChain próprio. Ele se chamará Hyperledger (IBM, 2015). O Hyperledger é um software (San Francisco, CA, Estados Unidos) que visa criar um BlockChain escalável, permitindo que as organizações façam negócios com qualquer pessoa sem a necessidade de confiança mútua. O Hyperledger quer chegar aonde o BlockChain ainda não chegou, adicionando aos recursos clássicos do BlockChain novos processos para verificação mais precisa da identidade das pessoas envolvidas. O Fabric, que antes era um projeto IBM chamado Open BC, tornou-se o primeiro projeto incubado no Hyperledger e seu nome foi alterado para Fabric (IBM, 2015). O Fabric implementa a tecnologia do BlockChain de forma bastante fl exível e, segundo os autores, o mesmo Bitcoin poderia ser obtido utilizando o Fabric como uma simples especialização. Ele pode hospedar contratos escritos em qualquer linguagem de desenvolvimento. Três conceitos arquitetônicos principais são bastante típicos para qualquer tecnologia de razão distribuída (i) o livro razão: um registro universal que contém o status e as transações do sistema. É organizado como blocos vinculados criptograficamente; (ii) a transação: um pedido para executar uma função no razão. A função é implementada por um código executável chamado chaincode (Contrato Inteligente); (iii) o chaincode: código que implementa uma função que pode alterar o estado do sistema. O chaincode também é armazenado no razão.

Hyperledger BC conta três módulos principais, a saber: (I) membros lidando com tarefas sobre registro e gerenciamento de identidade; (ii) BlockChain e transações que são os núcleos do sistema. Esses módulos gerenciam todos os serviços de BlockChain, como algoritmos de consenso, razão distribuída, gerenciamento de armazenamento e protocolo de comunicação p2p (gRCP ou Rest (obsoleto)); e (iii) Chaincode essa é a lógica do negócio.

4 Conclusão

A transição do mundo direcionado para informações vem mostrando-se acelerada 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.

A combinação de Blockchain e IoT pode ser bastante poderosa, pois o Blockchain pode dar resiliência a ataques e a capacidade de interagir com os pares de forma confiável e auditável. A contínua integração de Blockchain no domínio IoT causará transformações significativas em vários setores, trazendo novos modelos de negócios e nos fazendo reconsiderar como os sistemas e processos existentes são implementados.

Blockchain, portanto, apresenta muitas oportunidades promissoras para o futuro da IoT. Os desafios, no entanto permanecem, como custos computacionais de verificação de transações e segurança. Mas ainda está nos estágios iniciais de pesquisa e desenvolvimento, e esses obstáculos serão eventualmente superados, abrindo o caminho para muitas possibilidades.

Referências

ALABA, F. A.; OTHMAN, M.; HASHEM, I. A. T.; ALOTAIBI, F. Internet of things security: A survey. *Journal of Network and Computer Applications*, v. 88, p. 10–28, 2017. ISSN 1084-8045. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1084804517301455>. Citado na página 14.

Alyssa Hertig. *Blockchain's Once-Feared 51Regular*. 2018. Access date: 05 Mar. 2021. Disponível em: <https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular>. Citado na página 36.

Ayoade, G.; Karande, V.; Khan, L.; Hamlen, K. 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. Citado na página 40.

CHASE, B.; MACBROUGH, E. Analysis of the xrp ledger consensus protocol. *arXiv preprint arXiv:1802.07242*, 2018. Citado 2 vezes nas páginas 36 e 37.

Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access*, v. 4, p. 2292–2303, 2016. ISSN 2169-3536. Citado 2 vezes nas páginas 15 e 32.

Conoscenti, M.; Vetrò, A.; De Martin, J. C. Blockchain for the internet of things: A systematic literature review. In: *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*. [S.l.: s.n.], 2016. p. 1–6. Citado 3 vezes nas páginas 15, 38 e 41.

CROSBY, M. Blockchain technology: Beyond bitcoin. 2016. Citado na página 44.

Duan, X.; Yan, Z.; Geng, G.; Yan, B. 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. Citado na página 39.

Ethereum. *Confiança e Blockchain*. 2017. Access date: 05 Mar. 2021. Disponível em: <https://www.ethereum.org/token>. Citado na página 33.

Granjal, J.; Monteiro, E.; Sá Silva, J. Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys Tutorials*, v. 17, n. 3, p. 1294–1312, 2015. Citado na página 14.

Gregory Rocco. *Emptied IOTA Wallets: Hackers Steal Millions Using Malicious Seed Generators*. 2018. Access date: 05 Mar. 2021. Disponível em: <https://www.ccn.com/a-number-of-iota-wallets-emptied-by-hackers-due-to-online-seed-generators/>. Citado na página 37.

Guia do Bitcoin. *O que fazer se a sua transação Bitcoin ficar "presa"*. 2021. Access date: 05 Mar. 2021. Disponível em: <https://guiadobitcoin.com.br/o-que-fazer-se-a-sua-transacao-bitcoin-ficar-presa/>. Citado na página 36.

IBM. Adept: An iot practitioner perspective. 2015. Citado 2 vezes nas páginas 46 e 47.

KARAME, G. O.; ANDROULAKI, E.; CAPKUN, S. Double-spending fast payments in bitcoin. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery, 2012. (CCS '12), p. 906–917. ISBN 9781450316514. Disponível em: <https://doi.org/10.1145/2382196.2382292>. Citado na página 27.

KOUICEM, D. E.; BOUABDALLAH, A.; LAKHLEF, H. Internet of things security: A top-down survey. *Computer Networks*, v. 141, p. 199–221, 2018. ISSN 1389-1286. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128618301208>. Citado na página 14.

Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. 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. Citado na página 21.

MARMOL, F. G.; JESUS, E. F.; CHICARINO, V. R. L.; ALBUQUERQUE, C. V. N. de; ROCHA, A. A. d. A. A survey of how to use blockchain to secure internet of things and the stalker attack. *Security and Communication Networks*, Hindawi, v. 2018, p. 9675050, 2018. ISSN 1939-0114. Disponível em: <https://doi.org/10.1155/2018/9675050>. Citado na página 14.

Möser, M.; Böhme, R.; Breuker, D. An inquiry into money laundering tools in the bitcoin ecosystem. In: *2013 APWG eCrime Researchers Summit*. [S.l.: s.n.], 2013. p. 1–14. Citado 2 vezes nas páginas 41 e 42.

NAKAMOTO, S. On blockchain and its integration with iot. challenges and opportunities. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Citado 3 vezes nas páginas 24, 35 e 36.

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, 2018. Citado na página 13.

OUADDAH, A.; ELKALAM, A. A.; OUAHMAN, A. A. Towards a novel privacy-preserving access control model based on blockchain technology in iot. In: ROCHA, Á.; SERRHINI, M.; FELGUEIRAS, C. (Ed.). *Europe and MENA Cooperation Advances in Information and Communication Technologies*. Cham: Springer International Publishing, 2017. p. 523–533. ISBN 978-3-319-46568-5. Citado na página 46.

PAN, J. Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts. 2016. Citado na página 38.

POPOV, S. The tangle. In: . [S.l.: s.n.], 2015. Citado na página 45.

Renan Bernardo Valadão. *O que são redes P2P e como funcionam?* 2008. Access date: 15 jan. 2021. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/Anos-anteriores/2008-2/trabalhos_vf/renan_bernardo/p2p.html>. Citado na página 20.

Renata Kroska. *Confiança e Blockchain*. 2018. Access date: 05 Abr. 2021. Disponível em: <https://www.linkedin.com/pulse/confian%C3%A7a-e-blockchain-renata-kroska/>. Citado na página 30.

REYNA, A.; MARTíN, C.; CHEN, J.; SOLER, E.; DíAZ, M. On blockchain and its integration with iot. challenges and opportunities. *Future Generation Computer Systems*, v. 88, p. 173–190, 2018. ISSN 0167-739X. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X17329205>. Citado na página 14.

Rodrigo Tolotti. *Mineração de Bitcoin já consome mais energia do que 159 países juntos.* 2017. Access date: 05 Mar. 2021. Disponível em: <https://www.infomoney.com.br/mercados/mineracao-de-bitcoin-ja-consome-mais-energia-do-que-159-paises-juntos/>. Citado na página 35.

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. Citado na página 40.

STALLINGS, W. *Network and Internetwork Security: Principles and Practice*. Prentice Hall, 1995. (Prentice-Hall International editions). ISBN 9780780311077. Disponível em: <https://books.google.com.br/books?id=WrwQAQAAMAAJ>. Citado na página 16.

Vitalik Buterin. *A Proof of Stake Design Philosophy.* 2016. Access date: 05 Mar. 2021. Disponível em: <https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51>. Citado na página 37.

Wang, Z.; Dong, X.; Li, Y.; Fang, L.; Chen, P. 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. Citado na página 40.

WöRNER, D.; BOMHARD, T. von. When your sensor earns money: Exchanging data for cash with bitcoin. In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication.* New York, NY, USA: Association for Computing Machinery, 2014. (UbiComp '14 Adjunct), p. 295–298. ISBN 9781450330473. Disponível em: <https://doi.org/10.1145/2638728.2638786>. Citado 2 vezes nas páginas 43 e 45.

XU, Q.; AUNG, K. M. M.; ZHU, Y.; YONG, K. L. A blockchain-based storage system for data analytics in the internet of things. In: _____. *New Advances in the Internet of Things.* Cham: Springer International Publishing, 2018. p. 119–138. ISBN 978-3-319-58190-3. Disponível em: <https://doi.org/10.1007/978-3-319-58190-3_8>. Citado na página 46.

Yu, B.; Wright, J.; Nepal, S.; Zhu, L.; Liu, J.; Ranjan, R. Iotchain: Establishing trust in the internet of things ecosystem using blockchain. *IEEE Cloud Computing*, v. 5, n. 4, p. 12–23, 2018. Citado na página 12.

Zhang, Y.; Wen, J. An iot electric business model based on the protocol of bitcoin. In: *2015 18th International Conference on Intelligence in Next Generation Networks.* [S.l.: s.n.], 2015. p. 184–191. Citado 2 vezes nas páginas 43 e 46.

ZIGURAT. *What Do the Next Five Years Hold For the IoT?* 2020. Access date: 20 Fev. 2021. Disponível em: <https://www.e-zigurat.com/innovation-school/blog/what-do-the-next-five-years-hold-for-the-iot/>. Citado na página 21.

Zyskind, G.; Nathan, O.; Pentland, A. . Decentralizing privacy: Using blockchain to protect personal data. In: *2015 IEEE Security and Privacy Workshops*. [S.l.: s.n.], 2015. p. 180–184. Citado na página 42.