DOI: 10.5748/19CONTECSI/PSE/ESD/7101

INTEGRAÇÃO ENTRE IOT E BLOCKCHAIN: DESAFIOS E OPORTUNIDADES

Lara D. V. Nascimento
Programa de Pós-Graduação em Sistema e Computação - Universidade Salvador (UNIFACS) – Salvador

Integração entre IoT e Blockchain: desafios e oportunidades

LLLLLL[1], PPPPP[1]

[1]uuuuuuuuuuuuuuuuuuuuuuuuu

lllllll@gmail.com, ppppppppp@gmail.com

Abstract. *Internet of Things and Blockchain are technologies which lately have been quite explored in researches both in academia and industry. The former is gaining space in applications related to smart environments, whilst the later evolves as an infrastructure to support the development of distributed applications. As far as the convergence between these two emerging areas is concerned, researches propose the use of blockchain to build more reliable and robust IoT systems. This paper presents both technologies, as well as the main advantages and challenges on the integration between them. Furthermore, some proposed architectures are discussed, in order to demonstrate the impact of using blockchain in current IoT systems.*

Resumo. *Internet of Things (IoT) e Blockchain são tecnologias que têm sido bastante exploradas em pesquisas recentes, seja no meio acadêmico, seja na indústria. A primeira vem ganhando espaço em aplicações relacionadas a ambientes inteligentes, enquanto a segunda evolui como uma infraestrutura para o desenvolvimento de aplicações distribuídas. No que tange à convergência entre essas áreas emergentes, as pesquisas propõem o uso de blockchain para construir sistemas IoT mais confiáveis e robustos. Esse artigo apresenta as duas tecnologias e as principais vantagens e desafios da integração entre elas. Além disso, algumas arquiteturas propostas são discutidas, para demonstrar o impacto do uso de blockchain em sistemas IoT.*

1. Introdução

Internet das coisas – ou *Internet of Things (IoT)* – refere-se a uma rede dispositivos físicos interconectados através da internet, em geral, com o objetivo de coletar dados para dar suporte a uma tomada decisão mais inteligente. Dessa forma, IoT viabiliza a conversão do mundo físico em um enorme sistema de informações (Panarello et al., 2018). Essa natureza ubíqua, por sua vez, incentiva a criação de novos produtos disponíveis para consumidores finais, o que amplia ainda mais o alcance da tecnologia. Assim, atualmente existem aplicações de IoT em diversas áreas, a exemplo de transportes, cadeias digitais de suprimento, segurança e vigilância, manufatura, cuidados com a saúde, processamento de alimentos, dentre outras (Li et al., 2012).

Com a crescente presença desses sensores e outros dispositivos, grandes quantidades de dados são transmitidos para a nuvem, servidores privados ou outro tipo de sistema centralizado, onde softwares mais complexos são capazes de processá-los e analisá-los

(Viriyasitavat et al., 2019). Esse modelo centralizado e o fato de que todos os objetos estão acessíveis a partir da internet tornam possível o uso não autorizado dos dados, não apenas por parte de *hackers*, mas das próprias empresas responsáveis por gerenciar as informações sensíveis, que podem vender ou revelar dados de forma ilegítima. Assim, a expansão progressiva desse paradigma de interconexão entre os mundos físico e digital também traz novos desafios relacionados a segurança e privacidade (Panarello et al., 2018).

Além das vulnerabilidades de segurança e privacidade, existem outros desafios a serem superados no contexto das aplicações de Internet das coisas, a exemplo da heterogeneidade dos sistemas, da fraca interoperabilidade e da restrição de recursos computacionais dos dispositivos (Dai et al., 2019). Dessa forma, se, por um lado, o avanço da IoT fomenta a criação de novos modelos de negócio, a carência de soluções efetivas para superar seus problemas característicos dificulta a expansão desses modelos em larga escala.

Diversas tecnologias estão associadas às aplicações de Internet das coisas, a exemplo da Computação em Nuvem, Arquitetura Orientada a Serviços e Aprendizado de Máquina. Recentemente, a tecnologia Blockchain tem sido estudada como uma solução promissora, capaz de agregar privacidade e confiança aos sistemas IoT. Essa tecnologia ganhou notabilidade por ser a base da criptomoeda Bitcoin (Nakamoto, 2008) e é capaz de rastrear, coordenar e executar transações, e armazenar de forma segura informações provenientes de uma grande quantidade de dispositivos, constituindo assim uma possível alternativa aos atuais sistemas centralizados (Fernández-Caramés & Fraga-Lamas, 2018). Uma rede blockchain promove ainda a escalabilidade, ao simplificar os processos de negócios, através da eliminação da necessidade de ter um terceiro confiável para intermediar transações (Reyna et al., 2018).

Tanto IoT quanto blockchain são redes distribuídas e *Peer-to-Peer*; possuem, portanto, uma compatibilidade conceitual natural (F. Chen et al., 2020). Além do aspecto topológico, os principais fundamentos de uma rede blockchain, que estão associados a suas características mais relevantes, são: (1) um livro-razão (blockchain *ledger*), que garante a imutabilidade das transações armazenadas; (2) cada transação é validada por todos os participantes, a partir de um mecanismo de consenso pré-definido.

Embora a tecnologia blockchain possa beneficiar as aplicações de IoT, existem também desafios a serem superados para que todo o potencial dessa união possa ser aproveitado. Assim, esse trabalho tem como objetivo apresentar as duas tecnologias, as motivações para integrá-las, bem como as dificuldades dessa integração.

O trabalho está organizado da seguinte forma: a seção 2 traz uma visão geral sobre IoT, destacando os principais desafios em aberto. Na seção 3, é dada uma introdução sobre a tecnologia blockchain. Na seção 4, são apresentadas as motivações para a convergência entre IoT e blockchain. A seção 5 trata das possíveis arquiteturas de um sistema IoT baseado em blockchain, comparando-as com os modelos tradicionais. Por fim, a seção 6 destaca os principais desafios da integração entre as tecnologias e a seção 7 encerra o artigo com as conclusões.

2. Internet das coisas

O termo IoT refere-se a uma rede global de dispositivos identificáveis, interoperáveis e interconectados, que utiliza a Internet como a principal estrutura de comunicação

(Viriyasitavat et al., 2019). Tais dispositivos estabelecem um mapeamento entre o mundo real e o mundo digital, usando dispositivos de computação *front-end* e serviços *back-end* (F. Chen et al., 2020). O dispositivo *front-end* pode ser um sistema computacional embarcado, equipado com sensores, a exemplo de sensores de temperatura, etiquetas e leitores *Radio Frequency Identification* (RFID), dispositivos vestíveis (*wearables*), câmeras, detectores de fumaça, dentre outros. Já o sistema *back-end*, que é um *software*, integra, processa e analisa as informações coletadas e podem também retornar os resultados analisados para os usuários.

O avanço do uso de *smartphones* ampliou ainda mais as possibilidades de aplicação de IoT na vida cotidiana, pois, além de serem equipados com processadores mais poderosos e maior capacidade de armazenamento, facilitam a interação de seus usuários com outros objetos IoT presentes no ambiente.

Além do uso individual, os Sistemas Ciberfísicos – ou *Cyber Physical Systems* (CPS) – têm contribuído para o avanço da Internet das coisas em ambientes industriais (Viriyasitavat et al., 2019). A partir da união entre CBS e IoT, surgiram as fábricas inteligentes, capazes de, através de *softwares*, monitorar de perto as informações produzidas por um conjunto de dispositivos heterogêneos embarcados.

Nota-se que, por sua própria natureza, as aplicações de IoT possuem características únicas, as quais influenciam diretamente a utilização de blockchain (Viriyasitavat et al., 2019). A seguir, as principais características são listadas e brevemente descritas.

- Distribuição: os dispositivos são implantados em localidades geograficamente distribuídas. A computação das informações e a provisão de serviços podem estar situadas nas bordas da rede, bem próximas aos dispositivos, ou em plataformas centralizadas na nuvem;
- Capacidade computacional: os dispositivos IoT variam desde pequenos sensores embarcados, com recursos extremamente limitados, como capacidade de processamento, armazenamento e autonomia da bateria, a servidores avançados de alta capacidade, como na Computação em Névoa - ou *Fog Computing*. A restrição de recursos pode resultar em vulnerabilidade dos dispositivos a ataques maliciosos (Dai et al., 2019);
- Grande quantidade de dispositivos e dados: a quantidade de dados produzidos por dispositivos inteligentes está crescendo exponencialmente, devido à expansão dos sistemas IoT;
- Heterogeneidade: sistemas IoT envolvem múltiplos dispositivos, cada um com suas diferenças tanto em termos de *software* quanto de *hardware*, seguindo ainda diferentes padrões e protocolos de comunicação. Consequentemente, há variedade de tipos de dados (estruturados, semiestruturados e não estruturados). A heterogeneidade é ainda a raiz de outros desafios, como interoperabilidade, privacidade e segurança (Dai et al., 2019).
- Dinâmica: sistemas IoT são muito dinâmicos, pois os dispositivos são conectados e desconectados da rede a qualquer momento. Dispositivos, *software* e redes podem ter falhas ou ser comprometidos. A volatilidade dos dispositivos é muito comum em ambientes IoT.

- Mobilidade: dispositivos como *smartphones* e aqueles embarcados em veículos têm, por natureza, alto grau de mobilidade. Isso significa que eles podem estar sob diferentes domínios de administração ao longo de seu ciclo de vida;
- Ubiquidade de serviços: IoT oferece uma ampla gama de serviços, que podem ser acessados em todo o planeta. Muitos deles oferecem funcionalidades similares, porém com diferentes requerimentos e qualidade de serviço;
- Vulnerabilidade quanto à privacidade: é desafiador preservar a privacidade dos dados em IoT, devido à complexidade, descentralização e heterogeneidade dos sistemas. Outro aspecto que influencia nessa característica é a tendência em integrar IoT com Computação em Nuvem para aumentar a capacidade computacional e de armazenamento, pois, ao transferir dados confidenciais a servidores na nuvem ligados a terceiros, a privacidade dos sistemas IoT pode ser comprometida (Zhou et al., 2017);
- Vulnerabilidade de segurança: descentralização e heterogeneidade também geram dificuldades para garantir a segurança da rede. Soluções típicas, como autenticação, autorização e criptografia da comunicação, nem sempre são adequadas para os sistemas IoT devido à limitação de recursos dos dispositivos. Ademais, sistemas IoT tornam-se vulneráveis a ataques devido à falta de atualização dos *firmwares* de segurança no tempo correto (Roman et al., 2013);
- Complexidade de redes: diversos protocolos de rede e de comunicação coexistem em um sistema IoT. Alguns protocolos de redes típicos são: NFC, Bluetooth, 6LowPAN, WirelessHART, SigFox, LoRa e NB-IoT, cada um oferecendo diferentes serviços de rede (Dai et al., 2019). Por exemplo, 6LowPAN e WirelessHART possuem, normalmente, cobertura curta – menos de 100m, enquanto tecnologias LPWAN podem alcançar de 1km a 10km (M. Chen et al., 2017), (Khutsoane et al., 2017).

A integração com outras tecnologias vem colaborando com os sistemas IoT, de modo a contornar algumas de suas limitações intrínsecas. Por exemplo, a Computação de Borda – ou *Edge Computing* – móvel pode aumentar a capacidade dos nós da rede IoT, transferindo as tarefas de computação intensiva para servidores de borda (He et al., 2018). Nesse contexto, os avanços recentes da tecnologia Blockchain oferecem soluções para alguns desafios apresentados, como a fraca interoperabilidade e vulnerabilidades de privacidade e segurança, e podem melhorar a questão da heterogeneidade dos sistemas (Panarello et al., 2018).

3. Blockchain

3.1. Visão Geral

A tecnologia blockchain – ou *Blockchain Technology* (BCT) – foi inicialmente utilizada para promover transações comerciais independentemente de instituições intermediárias, como bancos ou Governos, através de uma nova moeda, denominada Bitcoin (Nakamoto, 2008). No entanto, graças à sinergia de tecnologias que a blockchain promove, ela vem sendo explorada em diferentes contextos, que vão além dos casos de uso financeiros (Panarello et al., 2018).

Em termos de estrutura, uma blockchain é formada por um conjunto de blocos, em que cada bloco possui, além de seus próprios dados, o *hash* do bloco anterior, formando assim uma cadeia interligada (F. Chen et al., 2020).

Com relação ao mecanismo de funcionamento, pode-se conceituá-la como um livro-razão – ou *ledger* – distribuído, sendo que cada nó mantém uma cópia idêntica do *ledger*. Para que a sincronização de informações seja possível, é necessário que os nós entrem em consenso a cada novo bloco a ser adicionado à rede. Por sua vez, o consenso é geralmente alcançado elegendo-se um *minerador*, que é um nó especial, responsável por consolidar as transações validadas em um novo bloco e distribuí-lo para toda a rede. O processo em que os mineradores competem para ganhar o direito de faturar um bloco é denominado *mineração* e o mecanismo que permite a mineração é denominado *mecanismo de consenso* (Narayanan et al., 2016).

Existem diversos tipos de mecanismos de consenso. As duas blockchains mais conhecidas, Ethereum e Bitcoin, utilizam o *Proof of Work (PoW)*. Nesse mecanismo, os mineradores inicialmente mapeiam as transações executadas através da rede e verificam se a assinatura de cada uma é válida. A partir daí, os dados transacionais são empacotados em um bloco candidato a ser adicionado à rede. Para que o bloco seja de fato aceito, o minerador precisa encontrar um número arbitrário, denominado *nonce*, que satisfaça a condição pré-determinada para a formação do *hash*. Uma vez que o *nonce* é encontrado, o minerador transmite o bloco para a rede. Se, por um lado, é difícil chegar a esse número, por outro, é bastante fácil de verificar que ele de fato é o número correto e atende às condições estabelecidas. Depois que outros mineradores fazem essa validação e aceitam o bloco, esse torna-se o mais novo bloco oficial da cadeia. Então, os mineradores passam a competir para montar o próximo bloco.

3.2. Contratos Inteligentes

Contratos Inteligentes – ou *Smart Contracts* – podem ser definidos como um conjunto de compromissos pré-definidos, transcritos em formato digital, incluindo acordos através dos quais as partes podem fazer cumprir o acordado (Szabo, 2018). A tecnologia blockchain ofereceu um excelente ambiente para que os contratos inteligentes fossem explorados, pois a descentralização e a sua natureza à prova de alterações permite que eles sejam confiáveis (Savelyev, 2016).

Os *Smart Contracts* são utilizados não apenas para contratos legais e comerciais, mas também são comumente utilizadas como uma plataforma automatizada para a troca de informações (F. Chen et al., 2020). Assim, eles podem ser utilizados para o gerenciamento do controle de acesso a dispositivos IoT, detectando a utilização fraudulenta dos dados coletados.

Com o advento dos Contratos Inteligentes, o escopo da tecnologia blockchain foi ampliado, permitindo não apenas o armazenamento de informações, mas também a codificação de processos lógicos na forma de transações (Viriyasitavat et al., 2019).

4. Convergência IoT e blockchain - motivações

Graças a sua topologia distribuída, similar à dos sistemas IoT, e sua capacidade intrínseca de garantir segurança, privacidade e eliminar pontos únicos de falhas, a tecnologia blockchain pode ser utilizada para criar arquiteturas seguras e descentralizadas, no contexto das aplicações de Internet das coisas (Viriyasitavat et al.,

2019). A união das duas tecnologias tem os seguintes benefícios potenciais, comparando-se com os sistemas IoT atuais (Dai et al., 2019):

- Aumento da interoperabilidade: se dá através da transformação dos dados heterogêneos, provenientes dos dispositivos IoT, e posterior armazenamento na blockchain. Considerando a existência de uma rede P2P, que funciona acima da camada de comunicação dos sistemas IoT, e em cima da qual a blockchain será estabelecida, há ainda uma melhora de interoperabilidade decorrente da facilidade em estabelecer a comunicação através do acesso à Internet, abstraindo as diversas redes fragmentadas;
- Aumento da segurança: por um lado, a segurança será garantida, pois os dados serão armazenados através de transações executadas nas blockchains, seguindo o processo de encriptação e assinatura digital. Adicionalmente, a segurança pode ser incrementada através da atualização automática do *firmware* dos dispositivos IoT, o que é fundamental para reduzir vulnerabilidades (Christidis & Devetsikiotis, 2016);
- Rastreabilidade e confiabilidade dos dados: intrinsecamente, dados de uma blockchain podem ser identificados e verificados a qualquer tempo. Além disso, a propriedade de imutabilidade assegura a confiabilidade dos dados, já que é bastante difícil alterar ou falsificar transações armazenadas em uma blockchain;
- Interações autônomas entre os dispositivos: através da rede blockchain, os dispositivos IoT ou subsistemas são capazes de interagir entre eles, prescindindo assim de intermediários, tais como governos ou outras empresas. Os Contratos Inteligentes reforçam ainda mais essa capacidade, ao permitir que essas interações ocorram de forma automática, a partir de gatilhos pré-definidos, ligados ao negócio.

Apesar de todos esses benefícios, é importante ressaltar que a tecnologia blockchain nem sempre é a melhor solução para um sistema IoT (Fernández-Caramés & Fraga-Lamas, 2018). Para determinar se o uso de blockchain é apropriado, deve-se decidir se as seguintes características são relevantes para a aplicação a ser desenvolvida:

- Descentralização: uma aplicação IoT necessita desse atributo quando não existe confiança mútua entre os participantes ou em relação a uma entidade terceira;
- Trocas entre os nós – relações P2P: tipicamente, a comunicação se dá dos nós para *gateways*, que roteiam dados para um servidor remoto na nuvem. Na prática, a interação direta entre os nós não é comum e ocorre em aplicações bem específicas;
- Sistema de pagamento: algumas aplicações estão ligadas a transações econômicas com terceiros e, portanto, necessitam dessa função. É possível que essa necessidade seja suprida por sistemas de pagamento tradicionais, embora eles normalmente estejam associados ao pagamento de taxas transacionais e à existência de bancos ou outros intermediários;
- Sistema de distribuição robusto: sistemas distribuídos podem ser construídos a partir de serviços na nuvem ou outros sistemas tradicionais de computação distribuída (Datla et al., 2012). Portanto, essa característica não é suficiente para

justificar a utilização de blockchain. É preciso também que não haja confiança na entidade responsável pelo sistema distribuído;

- Coleção de microtransações: algumas aplicações exigem a manutenção do registro de cada transação, para manter a rastreabilidade, para fins de auditoria ou devido a técnicas de *BigData* que serão aplicadas posteriormente (Cai et al., 2017).

5. Arquitetura

5.1. Modelos tradicionais

Segundo (Dai et al., 2019), um típico sistema de IoT consiste em três subsistemas representados por camadas: a primeira é a Camada de Percepção, onde estão situados os diversos dispositivos; a segunda é a Camada de Comunicação, através da qual os dispositivos *wireless* ou *wired* podem se conectar com os *gateways*, *WiFi Acess Points* (APs) e pequenas ou macro estações-base, formando uma rede permeada por diversos tipos de protocolo de comunicação. Por fim, a terceira é a Camada de Aplicação, que pode dar suporte às mais diversas aplicações.

Em (Fernández-Caramés & Fraga-Lamas, 2018), algumas arquiteturas tradicionais de IoT são discutidas. A primeira, denominada Arquitetura baseada em nuvem, é aquela em que os dados coletados pela camada dos nós são encaminhados diretamente para a nuvem, através dos *gateways* IoT, onde praticamente todo o processamento é efetuado. Esse modelo possui uma importante limitação: basta que um dos nós esteja comprometido para interromper toda a rede, por um ataque de negação de serviço – *Denial of Service* (DoS), por exemplo. Se um dos dispositivos conectados à nuvem ou a um servidor central for violado, os demais nós podem ser comprometidos também. Por outro lado, um sistema baseado em blockchain não depende de um único servidor central ou da nuvem. Além disso, todas as transações são verificadas, o que permite a detecção de atividades maliciosas provenientes de dispositivos comprometidos e a rejeição dessas tentativas de atualização do estado da rede.

5.2. Arquiteturas propostas

Existem muitos desafios a serem superados nas arquiteturas tradicionais, devido ao rápido crescimento tanto na diversidade quanto no número de dispositivos conectados à Internet (Sharma et al., 2018). Os modelos atuais não foram projetados para entregar requerimentos como alta disponibilidade, fornecimento de dados em tempo real, escalabilidade, segurança, resiliência e baixa latência. Por isso, novas propostas têm sido apresentadas, algumas agregando a tecnologia blockchain.

Para viabilizar a integração entre IoT e blockchain, a referência (Dai et al., 2019) propõe uma camada blockchain intermediária, situada entre as camadas de Comunicação e Aplicação, composta, por sua vez, por cinco subcamadas: a Subcamada de Dados, que coleta os dados das camadas mais inferiores, criptografa e empacota com assinatura digital; a Subcamada de Rede, uma rede P2P sobreposta à Camada de Comunicação que consiste em uma abstração das redes de comunicação inferiores, consequentemente oferecendo um acesso de rede universal entre diferentes redes. A Subcamada de Consenso está relacionada com o mecanismo de consenso, necessário para a validação dos blocos de dados; Subcamada de Incentivo, responsável por tarefas como emissão e distribuição de moeda digital, desenho do mecanismo de recompensa

para os mineradores e tratamento dos custos de transação; por fim, a Subcamada de Serviços provê serviços baseados em blockchain para os diversos usuários.

Essa proposta é interessante, pois oferece uma abstração das camadas mais baixas dos sistemas IoT, consequentemente ocultando sua heterogeneidade. Adicionalmente, essa camada intermediária é capaz de prover serviços – basicamente, *Application Programming Interfaces* (APIs) para dar suporte a diferentes aplicações. Dessa forma, a dificuldade do desenvolvimento de aplicações é reduzida também, graças ao nível de abstração alcançado.

Outras duas arquiteturas são apresentadas em (Fernández-Caramés & Fraga-Lamas, 2018) e representam uma evolução em relação à denominada Arquitetura baseada em nuvem, por transferir parte da carga de processamento da nuvem para a borda da rede. Esse reequilíbrio é considerado fundamental para sistemas IoT, já que, com o crescimento do número de dispositivos conectados, a quantidade de conexões a serem tratadas pela nuvem aumentaria também, e assim, seria necessário expandir sua capacidade (Triantafillou et al., 2003). Assim, a Computação de borda e a Computação em névoa - *Edge e Fog computing* – podem ser utilizadas para dar suporte a aplicações fisicamente distribuídas, com baixa latência e capazes de reduzir o tráfego de rede e a carga computacional em sistemas de computação em nuvem tradicionais.

A *Fog computing* é considerada um subconjunto da *Edge computing* (Dolui & Datta, 2017). Na segunda, além dos *gateways* fog, que podem ser representados por *Single Board Computers* (SBC), tais como Raspberry Pi (*Teach, Learn, and Make with Raspberry Pi*, n.d.) ou BeagleBone (*BeagleBoard.Org - Community Supported Open Hardware Computers for Making*, n.d.), existem também as chamadas *cloudlets*, que, na prática, consistem em um ou mais computadores de ponta que atuam como uma versão reduzida da nuvem. A principal vantagem das *cloudlets* é que elas são capazes de fornecer respostas em alta velocidade para tarefas computacionais intensivas demandadas pelos dispositivos – por exemplo, rodar um dos nós de uma blockchain -, o que não seria possível para um *gateway fog*, com recursos mais limitados.

Em (Stanciu, 2017), outra arquitetura para sistemas blockchain baseados em IoT é apresentada, utilizando o conceito de *Edge computing*. O modelo consiste em duas camadas: a primeira controla os dispositivos e processos, enquanto a superior supervisiona a inferior. Na camada superior, o modelo utiliza a plataforma blockchain *Hyperledger Fabric* (*Hyperledger Fabric – Hyperledger*, n.d.), que dá suporte à implementação de contratos inteligentes para executar as tarefas de supervisão. Já os nós das bordas formam a camada inferior e são baseados em uma arquitetura de microsserviços que faz uso de *Docker containers* e *Kubernetes*.

Software Defined Networking (SDN) também tem sido sugerida para implementar sistemas IoT baseados em blockchain. Em (Sharma et al., 2018), propõe-se uma arquitetura de nuvem distribuída, com a utilização de SDN para controlar nós do tipo fog – os *fog node*s - de uma rede IoT. Nesse caso, a nuvem é utilizada para desempenhar tarefas computacionais mais intensas. Paralelamente, é possível fornecer acesso aos dados com baixa latência, graças à computação em névoa, em que os *fog nodes* ficam distribuídos, provendo serviços e interagindo com a blockchain.

Fog nodes são entidades de computação de névoa distribuídas, que permitem a implantação de serviços de névoa e são formados por vários recursos computacionais na borda da rede IoT. Usando diferentes tecnologias, todos os dispositivos físicos

associados a um *fog node* são conectados, agregados e abstraídos para serem considerados como uma única entidade lógica.

A arquitetura consiste em três camadas. Na borda da rede, está situada a camada de dispositivos, na qual os mais diversos ambientes são monitorados. Os dados filtrados são então enviados para serem consumidos localmente na segunda camada, que é a camada da névoa, ou *fog layer*. Essa camada consiste em controladores SDN distribuídos e de alto desempenho. Cada um dos *fog nodes* cobre um determinado grupo de dispositivos, sendo responsável pela análise dos dados e entrega de serviços em tempo hábil. Por fim, a *fog layer* entrega os resultados dos dados processados para a camada de nuvem, que é mais abrangente e provê o monitoramento e controle de uma área maior.

Para a camada de nuvem, é proposta uma arquitetura de nuvem distribuída baseada em blockchain. Nesse modelo, o usuário pode selecionar um provedor de recursos a partir de um repositório. Então, o selecionado fornece o serviço, que pode ser a execução de uma tarefa, por exemplo, e o registra na forma de uma transação da blockchain. Finalmente, o usuário paga e recompensa ao fornecedor do serviço. Esse modelo pode facilitar o uso de recursos sob demanda, executando algoritmos de otimização através dos contratos inteligentes, o que pode incluir o pagamento automático após a conclusão do serviço solicitado. Adicionalmente, graças à tecnologia blockchain, é possível alcançar a rastreabilidade do uso dos recursos, o que torna possível verificar o nível de serviço acordado entre o cliente e o fornecedor.

Para a *fog layer*, os autores propõem que, em cada um dos *fog nodes*, os controladores SDN estejam conectados de uma maneira distribuída usando a tecnologia blockchain, provendo serviços escaláveis, confiáveis e de alta disponibilidade. Cada controlador é habilitado com uma função de análise da regra de fluxo e outra de migração de pacotes, para assegurar a rede durante ataques de saturação.

6. Principais desafios

Apesar dos potenciais benefícios que a tecnologia blockchain pode agregar aos sistemas IoT, ela não foi desenvolvida explicitamente para esse tipo de ambiente. Por isso, são necessários alguns ajustes para otimizar essa integração e aumentar seu desempenho em diferentes cenários. Nesse contexto, existem muitos aspectos capazes de influenciar uma aplicação baseada na união das duas tecnologias, mas os principais, que mais têm sido debatidos, são o desempenho alcançado e a escolha do mecanismo de consenso (Fernández-Caramés & Fraga-Lamas, 2018).

Em (Sukhwani et al., 2017), é feita uma análise relacionada ao desempenho, para entender se o mecanismo de consenso *Practical Byzantine Fault Tolerance* (PBFT) pode ser um gargalo em redes com um grande número de nós. O experimento realizado mostra que o tempo médio para alcançar o consenso cresce com o aumento do número de nós. Outro estudo, (Vukolić, 2015), faz uma comparação entre a escalabilidade do mecanismo *Proof-of-Work* (PoW) e de outros métodos baseados em *Byzantine Fault Tolerance* (BFT), e sugere que o desempenho do PoW pode ser melhorado ao ser misturado com o protocolo BFT.

Em (Viriyasitavat et al., 2019), é apresentada uma visão sobre os principais desafios da integração entre IoT e blockchain. O primeiro ponto levantado é o tempo para a aceitação final da transação. Seguindo a mesma linha do estudo anterior, defende-se

que, em aplicações para as quais o tempo é um fator crítico, que é o caso de muitos cenários que utilizam IoT, mecanismos mais eficientes do que o PoW podem ser empregados, especialmente no caso de uma blockchain privada.

Outro aspecto discutido é o alto consumo de recursos, principalmente ao considerar as blockchains públicas, que normalmente optam pelo PoW como mecanismo de consenso. Esse mecanismo está atrelado a um processo de mineração que torna a blockchain ineficiente em termos de taxa de transferência, escalabilidade e consumo de energia (Vukolić, 2015), o que não é desejável em aplicações IoT.

7. Conclusão

IoT e blockchain são avanços tecnológico em amplo crescimento, que dão origem a novas oportunidades de negócios, com potencial para revolucionar as mais diversas áreas de aplicação. Por isso mesmo, vêm crescendo em termos de pesquisas e investimentos por parte das indústrias. O artigo mostrou os aspectos que precisam ser melhorados dos sistemas IoT e que benefícios a união com a tecnologia blockchain pode agregar. Além disso, foram apresentadas algumas arquiteturas propostas, que são modelos que modificam as arquiteturas convencionais com o objetivo principal de aumentar a escalabilidade e o desempenho das aplicações IoT. Existem alguns estudos que já propõem aplicações específicas, relacionados a diferentes domínios de aplicação, como saúde, energia, cidades inteligentes, logística e agricultura. Apesar de não ser possível encontrar uma solução universal, aplicável a todos os cenários, essas propostas são importantes para confirmar, na prática, as limitações previstas e, principalmente, fomentar pesquisas voltadas para a união entre Blockchain e IoT, área que é tão promissora quanto emergente.

Referências

BeagleBoard.org - community supported open hardware computers for making. (n.d.). Retrieved September 13, 2021, from https://beagleboard.org/

Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2017). IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges. *IEEE Internet of Things Journal*, *4*(1), 75–87. https://doi.org/10.1109/JIOT.2016.2619369

Chen, F., Xiao, Z., Cui, L., Lin, Q., Li, J., & Yu, S. (2020). Blockchain for Internet of things applications: A review and open issues. *Journal of Network and Computer Applications*, *172*(March), 102839. https://doi.org/10.1016/j.jnca.2020.102839

Chen, M., Miao, Y., Hao, Y., & Hwang, K. (2017). Narrow Band Internet of Things. *IEEE Access*, *5*, 20557–20577. https://doi.org/10.1109/ACCESS.2017.2751586

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A Survey. *IEEE Internet of Things Journal*, *6*(5), 8076–8094. https://doi.org/10.1109/JIOT.2019.2920987

Datla, D., Chen, X., Tsou, T., Raghunandan, S., Hasan, S. M. S., Reed, J. H., Dietrich, C. B., Bose, T., Fette, B., & Kim, J. H. (2012). Wireless distributed computing: A

survey of research challenges. *IEEE Communications Magazine*, *50*(1), 144–152. https://doi.org/10.1109/MCOM.2012.6122545

Dolui, K., & Datta, S. K. (2017). Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. *GIoTS 2017 - Global Internet of Things Summit, Proceedings*. https://doi.org/10.1109/GIOTS.2017.8016213

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, *6*(c), 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685

He, J., Wei, J., Chen, K., Tang, Z., Zhou, Y., & Zhang, Y. (2018). Multitier Fog Computing With Large-Scale IoT Data Analytics for Smart Cities. *IEEE Internet of Things Journal*, *5*(2), 677–686. https://doi.org/10.1109/JIOT.2017.2724845

Hyperledger Fabric – Hyperledger. (n.d.). Retrieved September 13, 2021, from https://www.hyperledger.org/use/fabric

Khutsoane, O., Isong, B., & Abu-Mahfouz, A. M. (2017). IoT devices and applications based on LoRa/LoRaWAN. *Proceedings IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, *2017-January*, 6107–6112. https://doi.org/10.1109/IECON.2017.8217061

Li, Y., Hou, M., Liu, H., & Liu, Y. (2012). Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things. *Information Technology and Management 2012 13:4*, *13*(4), 205–216. https://doi.org/10.1007/S10799-012-0121-1

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Narayanan, A., Bonneau, J., Felten, E., & Miller, A. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. https://books.google.com/books?hl=pt-BR&lr=&id=LchFDAAAQBAJ&oi=fnd&pg=PP1&ots=AsnEg_4JoI&sig=O806EV5z6UrFxHPejHlfqmB7HN4

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. In *Sensors (Switzerland)* (Vol. 18, Issue 8). https://doi.org/10.3390/s18082575

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems*, *88*, 173–190. https://doi.org/10.1016/J.FUTURE.2018.05.046

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/J.COMNET.2012.12.018

Savelyev, A. (2016). Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.2885241

Sharma, P. K., Chen, M. Y., & Park, J. H. (2018). A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. *IEEE Access*, *6*, 115–124. https://doi.org/10.1109/ACCESS.2017.2757955

Stanciu, A. (2017). Blockchain Based Distributed Control System for Edge Computing. *Proceedings - 2017 21st International Conference on Control Systems and Computer, CSCS 2017*, 667–671. https://doi.org/10.1109/CSCS.2017.102

Sukhwani, H., Martínez, J. M., Chang, X., Trivedi, K. S., & Rindos, A. (2017). Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric). *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, *2017-September*, 253–255. https://doi.org/10.1109/SRDS.2017.36

Szabo, N. (2018). *Smart Contracts : Building Blocks for Digital Markets*.

Teach, Learn, and Make with Raspberry Pi. (n.d.). Retrieved September 13, 2021, from https://www.raspberrypi.org/

Triantafillou, P., Ntarmos, N., Nikoletseas, S., & Spirakis, P. (2003). NanoPeer networks and P2P worlds. *Proceedings - 3rd International Conference on Peer-to-Peer Computing, P2P 2003*, 40–46. https://doi.org/10.1109/PTP.2003.1231502

Viriyasitavat, W., Anuphaptrirong, T., & Hoonsopon, D. (2019). When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities. *Journal of Industrial Information Integration*, *15*(May), 21–28. https://doi.org/10.1016/j.jii.2019.05.002

Vukolić, M. (2015). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9591*, 112–125. https://doi.org/10.1007/978-3-319-39028-4_9

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and Privacy for Cloud-Based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 26–33. https://doi.org/10.1109/MCOM.2017.1600363CM