Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

ESTUDO DE USO DE *BLOCKCHAIN* PARA RESOLVER ASPECTOS DE SEGURANÇA EM IoT

Edilson Chagas Porta[1]

Carlos Eduardo de França Roland[2]

Resumo

Dentre as mais recentes tecnologias, podem-se destacar duas por possuírem particularidades essenciais na geração e transmissão de dados com resultados satisfatórios em relação à praticidade e segurança: a Internet das Coisas (IoT) com sua grande capacidade de permitir a interação de equipamentos de forma independente de usuários, podendo ser operados em uma rede global de máquinas capazes de trocar informações entre si e operarem de forma autônoma para tomada de decisões, abrindo uma série de possiblidades de desenvolvimento de novos dispositivos; e a tecnologia de *blockchains* que permite a transmissão de dados em uma rede distribuída, na qual os envolvidos podem interagir uns com os outros sem um intermediário confiável, de maneira segura e verificável, fornecendo contratos inteligentes e automatizando processos. No presente estudo exploratório dessas tecnologias destacam-se duas questões que devem ser consideradas na implantação de *blockchains* para operar com IoT para se buscar soluções alternativas, como o poder de processamento dos dispositivos e a privacidade dos dados transmitidos. Como conclusão pode-se considerar que a combinação *blockchain*-IoT é poderosa e pode causar transformações significativas em vários setores da atividade humana, abrindo caminho para novos modelos de negócios e para o desenvolvimento de novos aplicativos distribuídos.

Palavras-chave: Criptografia. *Hash*. Segurança de Dados. Sistemas Distribuídos. *Token*.

Abstract

Among the most recent technologies, two can be highlighted because they have essential characteristics in the generation and transmission of data with satisfactory results regarding practicality and security: the Internet of Things (IoT) with its great capacity to allow the interaction of equipment in a way independent of users, and can be operated in a global network of machines capable of exchanging information among themselves and operating autonomously for decision making, opening a series of possibilities for developing new devices; and blockchain technology that enables data transmission over a distributed network in which people who are involved can interact with one another without a reliable intermediary in a secure and verifiable way, providing intelligent contracts and automating processes. In the present exploratory study of these technologies, two issues should be considered in

[1] Graduando em Análise e Desenvolvimento de Sistemas pela Fatec Dr Thomaz Novelino – Franca/SP. Endereço eletrônico: edilson.java@gmail.com.
[2] Docente no curso de Análise e Desenvolvimento de Sistemas pela Fatec Dr Thomaz Novelino – Franca/SP. Endereço eletrônico: carlos.roland@fatec.sp.gov.br

the implementation of blockchains to operate with IoT to find alternative solutions, such as the processing power of the devices and the privacy of the transmitted data. In conclusion, the blockchain-IoT combination is powerful and can cause significant transformation in various sectors of human activity, paving the way for new business models and the development of new distributed applications.

Keywords: *Cryptography. Data Security. Distributed systems. Hash. Token.*

1 Introdução

A IoT refere-se à integração de objetos físicos (coisas) e virtuais conectados à internet para a coleta, transmissão e armazenamento de enorme quantidade de dados em sistemas de computação em nuvem para obtenção de informações e serviços em escala inimaginável. A IoT está em constante expansão, sendo cada vez mais utilizada entre os usuários de vários setores como: assistência médica, *warehousing*, transporte e logística.

As atuais soluções de IoT baseadas em armazenamentos centralizados, com grande tendência na criação de novos produtos e serviços, podem não atender aos desafios de segurança, escalabilidade, disponibilidade, e gerenciamento destes dispositivos.

O surgimento das criptomoedas, sendo a Bitcoin a mais conhecida, é fundamentado no uso de *blockchains* como o sistema de registro, armazenamento e certificação que universalmente valida e garante os dados de transações.

A utilização do *blockchain* como uma solução com suas principais características arquiteturais de segurança das operações, descentralização de armazenamento, integridade das informações e imutabilidade dos dados, torna-se uma solução para atender e superar os desafios encontrados na IoT.

O *blockchain* atraiu recentemente o interesse de empresas, investidores e usuários preocupados com a segurança de seus dados, surgindo uma ampla oportunidade de criação de diversos produtos e serviços domésticos, industriais, de finanças, de saúde, de transações imobiliárias, e para o setor governamental.

Com a integração do *blockchain*, os aplicativos que poderiam ser anteriormente executados apenas por meio de um intermediário confiável, podem agora realizar transações de forma descentralizada, com isenção de autoridade central certificadora, alcançando funcionalidade, e com alto grau de certeza, o que não é possível no modelo convencional de certificação de transações. Os

blockchains possibilitam a realização de transações em redes sem confiança, porque as partes podem transacionar mesmo que não confiem entre si, sem a necessidade de atuação de um intermediário confiável, resultando em agilidade na conciliação e confiança entre as partes envolvidas.

A criptografia, que é uma característica chave das redes *blockchain*, traz segurança às transações de interações na rede, com a geração de contratos inteligentes de execução automática, baseados na tecnologia de *hashing*, que é uma função computacional que mapeia dados de comprimento variável em chaves de comprimento fixo. Usadas em criptografia, funções *hash* permitem que se verifique a integridade de dados que foram mapeados a um valor *hash*, dificultando a reconstrução dos dados originais quando estes não forem conhecidos.

Com o aumento da criação de novos dispositivos e mais pessoas utilizando, resultando no aumento do volume de acesso à rede para troca de informações, foi despertado o uso do *blockchain* em redes de IoT, atraindo pesquisadores e desenvolvedores.

O objetivo do presente estudo bibliográfico exploratório é analisar as formas de conectar, proteger e gerenciar o grande volume de dispositivos de IoT; identificar aplicações existentes analisando os processos utilizados, apresentando como o *blockchain* é capaz de auxiliar a segurança de transações entre dispositivos de IoT.

Para identificar pontos importantes, deve-se entender o conceito dessas duas tecnologias, levando-se em consideração o estado da arte de cada uma bem como as tendências para os próximos anos; se destacar as maneiras como *blockchain* e IoT podem ser utilizados em conjunto atendendo aos requisitos fundamentais das aplicações sem comprometimento de performance e de segurança, oferecendo aos leitores interessados em conhecer ou utilizar produtos e serviços de IoT, uma visão clara sobre os desafios e informações relevantes para sua adoção.

2 Blockchain

O *blockchain* é o equivalente a um livro-razão contábil, que registra transações financeiras de crédito e débito, distribuído que mantém a lista de transações armazenada em diversos servidores participantes da rede, substituindo um servidor central. Todos computadores participantes da rede *blockchain,* chamados de nós da rede, sempre têm acesso a uma cópia atualizada do livro-razão

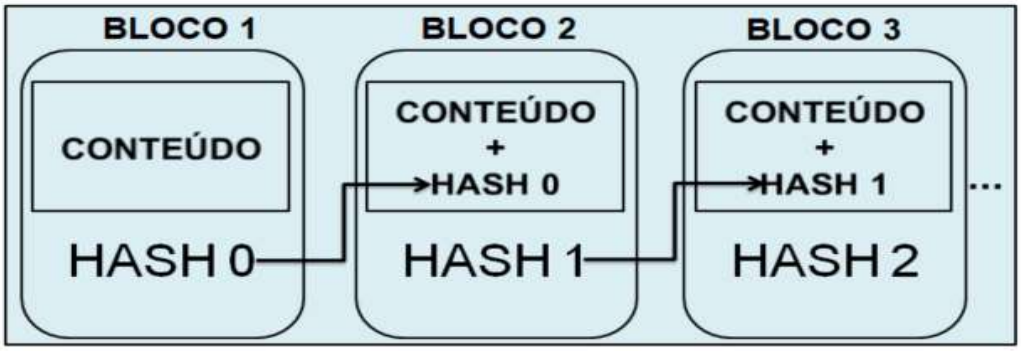
criptografado. Uma das principais características do *blockchain* é que ele é um banco de dados distribuído, ou seja um banco de dados que existe em várias cópias mantidas em vários computadores.

A definição original foi criada e publicada em 2008 por Satoshi Nakamoto e o código de implementação foi lançado como código aberto em janeiro de 2009 (WATTERS, 2016).

Inicialmente introduzido na criação da moeda digital *Bitcoin* para resolver diversos problemas, como o resultado de como os nós da rede (os chamados mineiros) acrescentam uma transação validada, mutuamente acordada, em um registro de transações que estabelece e garante quem possui o que.

A Figura 1 mostra como os blocos em um *blockchain* são encadeados e como os *hashs* estabelecem a dependência entre eles, tornando imutável quaisquer das transações no bloco, garantindo a veracidade de todas elas.

Figura 1 – Exemplo de blocos de transações em uma corrente



Fonte: adaptado de TECNOBLOG (2018)

Cada bloco na corrente transporta uma lista de transações e um *hash* do bloco precedente, a exceção a isso é o primeiro bloco da corrente, chamado gênesis, comum a todos os clientes em uma rede *blockchain*. Imagine um bloco de registros de transações acrescidos de dados de data e hora e do *hash* do bloco anterior, mapeados a um novo valor *hash* criptográfico. A referência ao *hash* do bloco precedente estabelece o vínculo entre eles, criando assim uma corrente de blocos, ou seja, um conjunto encadeado de blocos dos dados que estão sendo trocados na rede. O uso de criptografia assimétrica possibilita autenticação, integridade e não repúdio à rede.

Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

Para entender melhor como funciona um *blockchain*, é necessário examinar como uma rede *blockchain* é implementada. Assume-se que cada usuário transaciona na rede através dos nós. Os usuários interagem com o *blockchain* por meio de um par de chaves privadas/públicas para criarem suas próprias transações, que são endereçáveis na rede por meio de sua chave pública (IEEEXPLORE, 2018).

Cada transação assinada é transmitida pelo nó de um usuário para seus pares de uma só vez; os pares vizinhos certificam-se de que esta transação recebida é válida antes de retransmiti-la. Transações inválidas são descartadas, e as válidas são espalhadas por toda a rede. As transações que foram coletadas e validadas pela rede usando o processo descrito, durante um intervalo de tempo acordado, são ordenadas e empacotadas em um bloco candidato com registro de data e hora. O bloco candidato criado é transmitido para a rede para ser minerado. A mineração é o processo de verificação da integridade dos dados das transações do bloco, associados ao *hash* do bloco anterior, buscando-se um número de identificação do novo bloco até que se encontre um valor *hash* com uma característica pré-determinada, como por exemplo, as quatro primeiras posições da chave contendo zeros. Se for o caso, o nó mineiro adiciona o bloco à corrente. Se esse não for o caso, o bloco candidato é descartado, as transações retornam à rede para inclusão em novo bloco candidato, gerando o final de uma rodada. Este processo é realizado de forma repetitiva (IEEEXPLORE, 2018).

Para evitar problemas nesse ambiente distribuído permitindo que a rede alcance o consenso, cada rede *blockchain* precisa estabelecer os limites de tempo que as transações de dados devem cumprir em um bloco candidato. Essas regras dependem do aplicativo, sendo cumpridas em cada cliente *blockchain* que o utiliza para decidir se um bloco de transações de entrada é válido.

Consequentemente, para serem retransmitidos para a rede ou não, os nós precisam concordar com as transações que são listadas no bloco recém-minerado, caso contrário, as cópias individuais do *blockchain* em cada nó irão divergir, e os registros de movimentação terão uma visão diferente do estado global do bloco, não sendo possível que a rede mantenha uma cronologia autorizada única, ou seja, um *blockchain*.

Qualquer nó que possa resolver esse quebra-cabeça gera a chamada prova de participação (do inglês *proof-of-stake* ou PoS), conseguindo moldar o próximo bloco da corrente. Como uma função de *hash* criptográfico unidirecional está

envolvida, qualquer outro nó pode facilmente verificar se a resposta satisfaz o requisito e pode adotar esse bloco para o bloqueio de blocos da célula.

Note que uma bifurcação ainda pode acontecer na rede, quando dois nós concorrentes geram blocos quase simultaneamente. Nesse caso o mecanismo prova de trabalho (*proof-of-work* ou PoW) determina que os nós devam adotar o método que demanda a maior quantidade de trabalho. Assim, é improvável que os dois concorrentes gerem o próximo bloco simultaneamente, e o bloco mais longo será adotado pelos nós como o correto, permitindo que a rede chegue a um consenso sobre a ordem correta dos eventos (IEEEXPLORE, 2018).

A prova de participação é uma alternativa de trabalho inovadora que requer muito menos cálculos de CPU para mineração. Nela as chances de um nó explorar o próximo bloco são proporcionais ao equilíbrio desse nó. Os esquemas de PoS têm suas próprias forças, fraquezas, e implantações efetivas onde estão se mostrando bastante complexas (IEEEXPLORE, 2018).

Em redes privadas, no entanto, onde os participantes estão na lista de permissões, mecanismos dispendiosos de consenso como o PoW não são necessários, praticamente eliminando a necessidade de um incentivo econômico para a mineração e o uso de uma série de protocolos consensuais.

2.1 *Blockchain* e Contratos Inteligentes

Dentro do contexto de *blockchains*, os contratos inteligentes são programas de computadores armazenados na cadeia que controlam a transferência de moedas digitais ou ativos entre partes sob certas condições. Podem ser considerados como análogos aos procedimentos (chamados *stored procedures*) mantidos em Sistemas de Gerenciamento de Bancos de Dados Relacionais (SGBD), uma vez que eles permanecem inseridos na sua estrutura.

Os contratos inteligentes têm um único direcionamento e uma transação associada, que executa de forma independente e automaticamente um *script* de processamento na rede, de acordo com o que foi incluído na transação de disparo. Um contrato inteligente não só relata um acordo entre partes como nos contratos tradicionais, mas também pode impor automaticamente essas obrigações.

Isso é feito a partir dos dados da transação como entrada em um processo que associa um valor, chamado de *token*, através de um algoritmo de *hash* que

Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

garante a veracidade dos dados da transação. Os contratos com suas chaves são inseridos em blocos de dados e mantidos em sistemas de armazenamento descentralizado. Transferências de ativos digitais utilizando *tokens* podem ser conseguidas facilmente e de maneira criptograficamente verificáveis (ROUSE, 2018).

Contratos inteligentes são complexos e podem ser usados em uma grande variedade de registro de transações tais como processos jurídicos, apólices de seguro, acordos de financiamento, até aplicações financeiras. Os contratos inteligentes têm o potencial de eliminar intermediários em questões legais e financeiras, particularmente simplificando e automatizando rotinas e processos repetitivos pelos quais se pagam taxas a advogados e bancos (ROUSE, 2018).

Um contrato inteligente devidamente escrito é determinista. A mesma entrada de dados sempre produzirá um mesmo *token*. Caso se escreva um contrato não determinístico, quando ele for verificado por nós da rede, retornará resultados aleatórios, evitando que a rede chegue a um consenso sobre seu resultado de execução, tornando-o inválido. As partes que realizam a transação na cadeia de blocos e o código de validação podem ser inspecionados por todos os participantes da rede. Como todas as interações em um contrato ocorrem por meio de mensagens assinadas no *blockchain*, todos os participantes da rede obtêm um rastreamento criptograficamente verificável das operações do contrato (IEEEXPLORE, 2018).

Cadeias de blocos que suportam transações permitem transferências de ativos entre contrapartes que não confiam umas nas outras. No entanto com processos de validação de várias etapas, é garantida a confiança da transação entre as partes mutuamente desconfiadas. As entidades de validação conseguem inspecionar o código e identificar seus resultados antes de decidir se envolver com o contrato, obtendo certeza de execução, pois o código já está implantado em uma rede que nenhum deles controla totalmente, obtendo veracidade sobre os processos reconhecendo que as interações estão alinhadas. A possibilidade de disputas é eliminada quando todos os resultados possíveis são contabilizados, uma vez que os participantes não podem discordar do resultado final do processo de validação. Os contratos inteligentes operam como atores autônomos, cujo comportamento é completamente previsível, tal que, eles são confiáveis para impulsionar qualquer lógica onde possa ser expressa como uma função computacional de entrada de dados (IEEEXPLORE, 2018).

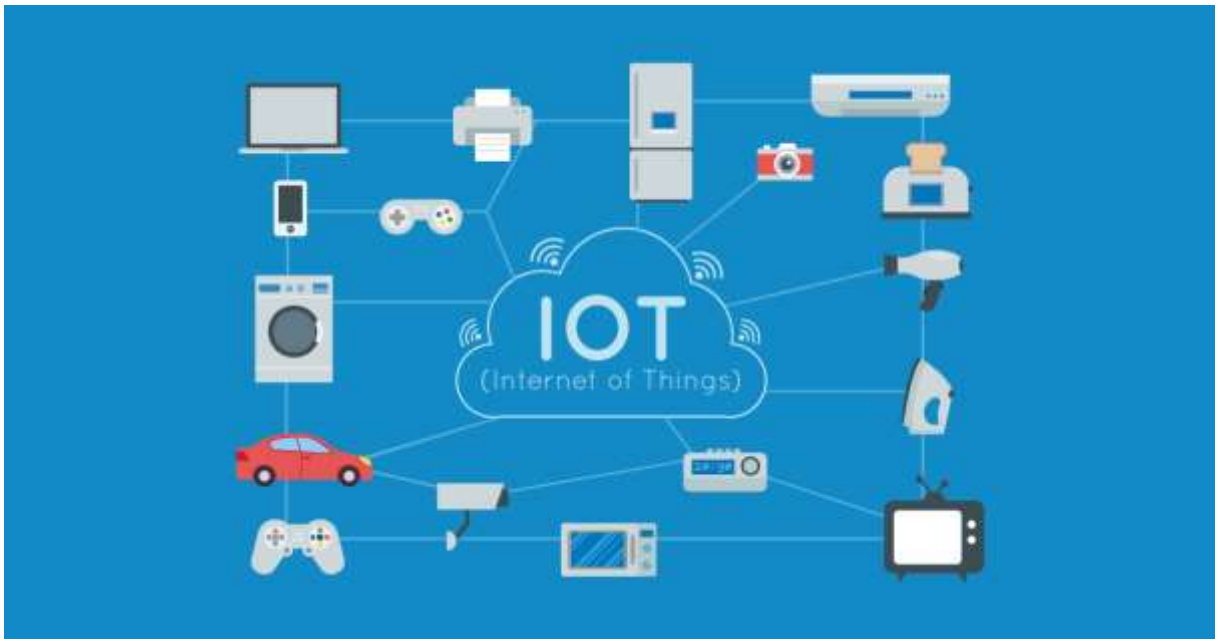
Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

Os contratos também incorporam a lista de membros com endereços de chaves públicas que votam em seu comportamento. É um sistema ponto-a-ponto (do inglês *peer-to-peer*) robusto e verdadeiramente distribuído que é tolerante a falhas de nó com uma rede que pode identificar os conflitos, resolvendo os problemas automaticamente (HACKERNOON, 2017).

3 Internet das coisas (IoT)

A Internet das Coisas (IoT), é um novo paradigma e conceito de tecnologia, imaginado como uma rede global de máquinas e dispositivos capazes de interagir entre si, realizando tarefas de forma autônoma, oferecendo produtos e serviços inteligentes. A Figura 2 mostra a arquitetura, componentes e possibilidades da IoT.

Figura 2 – Exemplo de uma rede IoT



Fonte: MARQUES (2017)

A IoT é reconhecida como uma das áreas mais importantes da tecnologia futura, e está chamando grande atenção de usuários e indústrias, mostrando um grande potencial e um novo conceito de dispositivos baseados em rede.

Gartner (2017) prevê que a IoT, irá atingir 20 bilhões de dispositivos até 2020, alimentando um mercado que valerá pelo menos US$ 3 trilhões.

O verdadeiro valor da IoT para empresas pode ser percebido quando os dispositivos conectados são capazes de se comunicar uns com os outros e integrar com sistemas de estoque gerenciados por fornecedores, suporte a clientes, aplicativos de *Business Intelligence* e analistas de negócios. Da linha de produção, armazenagem e distribuição para varejo a prateleiras de lojas, a IoT está se transformando em processos de negócios, fornecendo informações mais precisas e visibilidade em tempo real do fluxo de materiais e produtos. Empresas investirão na IoT para redesenhar fluxos de trabalho de fábrica, melhorando o rastreamento de materiais e os custos de distribuição. Além da adoção de IoT por fabricantes, várias indústrias de serviços estão adotando a tecnologia para aumentar a receita através de serviços inteligentes para se tornarem líderes no mercado (TIESPECIALISTA, 2018).

Sistemas de monitoramento e controle coletam dados sobre equipamentos incluindo o seu desempenho, o uso de energia e condições operacionais, e permitem acompanhar constantemente o desempenho em tempo real, em qualquer lugar e a qualquer hora. Os dispositivos de IoT precisam garantir que os dados transitem corretamente em tempo hábil. Conteúdos de um pacote de dados, considerando desde o registro de sua abertura até o recebimento pelo sistema controlador devem ser garantidos, sinalizando quando partes forem adulteradas ao longo do caminho. Embora os aplicativos de coleta de dados e controle dos processos não necessariamente requeiram visualização de dados, mais e mais aplicações de IoT, centradas no ser humano, fornecem visualizações apresentadas de forma gráfica aos usuários finais, de forma intuitiva e de fácil compreensão, permitindo a interação com o meio ambiente.

É importante que os aplicativos de IoT sejam projetados para operações autônomas, de modo que os dispositivos possam monitorar o ambiente, identificar problemas, comunicar-se entre si e potencialmente resolver problemas de forma automatizada.

4 Blockchain e IoT

A integração do IoT com o *blockchain* está gerando um novo conceito em eletrodomésticos. A IBM e Samsung apresentaram o uso de *blockchain* em lavadoras de roupas autônomas capazes de realizar diagnósticos em seus

Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

componentes, em produtos de limpeza das roupas, e ainda realizar serviços de pós-venda com base no uso de contratos inteligentes (GANTAIT; PATRA; e MUKHERJEE, 2018).

A empresa Filament, fornecedora de *hardware* e *software* de IoT para aplicações industriais como agricultura, manufatura e indústrias de petróleo e gás, oferece sistemas que através de sensores sem fio criam redes autônomas de baixa potência que permitem às empresas gerenciar operações físicas, sem depender de infraestrutura de armazenamento centralizado. A identificação e a intercomunicação dos dispositivos são asseguradas por uma corrente de blocos que mantém a identidade única de cada nó da rede (TIESPECIALISTAS, 2016).

O setor automobilístico tem investido fortemente em aplicações de IoT integradas com *blockchains*. As cadeias de blocos são utilizadas para garantir o trânsito seguro de dados atualizados, para garantir transações entre os fornecedores da cadeia das montadoras, entre empresas de financiamento de automóveis, seguradoras, prestadores de serviços, e os proprietários dos veículos. Os dados coletados pelos sensores acoplados aos acessórios dos automóveis estão integrados com *blockchain* para garantir as tomadas de decisões automatizadas em tempo real (GANTAIT; PATRA; e MUKHERJEE, 2018).

A implantação de IoT com *blockchains* pode auxiliar na segurança das informações geradas por equipamentos médicos nos tratamentos cirúrgicos e ambulatoriais. Originados de dispositivos sensores ligados aos pacientes, os dados são armazenados com segurança em registros distribuídos e os dispositivos de controle envolvidos acessam os conteúdos obedecendo as regras inteligentes determinadas pelo *blockchain*, oferecendo informações certificadas em tempo real (GANTAIT; PATRA; e MUKHERJEE, 2018). Além de aplicações em veículos autônomos e na medicina, os autores citam aplicações de IoT com *blockchains* em sistemas de gerenciamento de cadeias de suprimentos, gerenciamento de serviços públicos de energia, água e esgoto, de utilidades, na automação residencial, dentre outras aplicações possíveis.

Em segundo plano a abordagem de troca de pacotes de dados através da transparência possibilita a solução de questões de confiabilidade e segurança com uso de modelos *peer-to-peer* dimensionáveis, originalmente sem confiança. Os *blockchains* fornecem soluções eficientes para essa classe de problema.

Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

Considere como exemplo a necessidade de manutenção da operação de redes de dispositivos de IoT. Cada nó da rede é um componente composto por dispositivos digitais construídos fundamentalmente por *hardware* e *software.* Como a dinâmica dos processos controlados por tais dispositivos é grande precisando ser adaptadas a novos contextos constantemente, a manutenção do *software* embarcado (*firmware*) em cada nó é impraticável se não realizada também automaticamente. Para garantir que todos os dispositivos IoT de sua rede sejam mantidos atualizados com alta garantia de segurança, o fabricante implanta um contrato inteligente com base em *blockchains* que permita ser consultado por cada nó cliente da rede *peer-to-peer* para identificar novas atualizações do *firmware* para instalação. O uso de chaves de criptografia (*hash*) garantem a integridade do registro das atualizações. Além disso, numa rede *blockchain* em que transações que precisam de validação ocorrem, há a possibilidade de remuneração pelos serviços de autenticação das cadeias de blocos, abrindo caminho para um mercado de serviços entre os dispositivos. Como exemplo, os dispositivos que armazenam uma cópia do *blockchain* ou que validam as cadeias podem ser remunerados pelo processamento, custeando suas infraestruturas ou gerando lucro, sustentando a oferta da tecnologia de transmissão de dados com *blockchains* para uso geral.

4.1 Privacidade de dados de IoT com *Blockchains*

IoT consiste de dispositivos que geram, processam, e trocam quantidades de dados de segurança, assim como informações sensíveis à privacidade, ficando vulneráveis a ataques cibernéticos. Dispositivos de IoT são leves e de baixo consumo de energia. A energia disponibilizada aos dispositivos e seu poder de processamento devem ser prioritariamente focados para a execução de funcionalidades de sua aplicação, tornando a tarefa de suportar segurança e privacidade de forma econômica um desafio. Métodos tradicionais de segurança são onerosos para IoT em termos de consumo de energia e sobrecarga de processamento. Assim aplicações de IoT demandam garantias de leveza, escalabilidade, segurança distribuída e privacidade. A tecnologia de *blockchains* tem o potencial de superar os desafios por sua natureza distribuída, segura e privada (DORRI *et al.*, 2017).

Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

Em comparação com um banco de dados centralizado e adequadamente configurado, uma solução *blockchain* geralmente terá um desempenho inferior, resultando em menor velocidade de processamento de transações. Em geral esse impacto no desempenho é a penalidade paga pela descentralização e resiliência sem confiança. Essa situação é ainda mais acentuada em *blockchain* que utilizem contratos inteligentes em função da ocorrência de conflitos de mineração. Se dois mineradores resolverem um mesmo bloco simultaneamente, então ter-se-á duas cadeias de blocos diferentes na rede, e será necessário esperar pelo próximo bloco para resolver o conflito. Mineradores processarão a cadeia 1, enquanto outros processarão a cadeia 2. O primeiro minerador que encontrar um novo bloco para a cadeia, resolverá o conflito. Se o novo bloco foi minerado sobre a cadeia 1, então a cadeia 2 se torna inválida, a recompensa pela mineração do bloco anterior é creditada para o minerador da cadeia 1, e as transações que faziam parte da cadeia 2 e não foram adicionadas ao *blockchain* voltam ao reservatório de transações para serem adicionadas aos próximos blocos (MOUJAHID, 2018). Abreviadamente, se existir um conflito entre cadeias de blocos, a maior cadeia vence a disputa como mostrado na Figura 3.

Figura 3 – Resolvendo conflitos em *blockchains*

Fonte: MOUJAHID (2018)

A despeito dos benefícios da IoT, a grande quantidade de dados gerados pelos dispositivos pode levar a problemas de privacidade. Os dados gerados podem revelar informações pessoais dos usuários, incluindo seus comportamentos e preferências. Para introduzir privacidade de dados de usuários de IoT, a proposta é desenvolver a IoT descentralizada, com funções de privacidade definidas no projeto. Na era da informação, onde riqueza passa a ser definida como a posse e o acesso a dados no lugar de ativos contábeis, democratizar dados de IoT dando plena autoridade aos usuários sobre seus dados vai promover um revolucionário modelo de comércio digital. O gerenciamento descentralizado de dados de IoT permitirá que

Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

usuários compartilhem ou vendam dados coletados com seus dispositivos sem intermediação de terceiros como já ocorre com as moedas virtuais, sendo Bitcoin a mais conhecida (ALI, DOLUI e ANTONELLI, 2017).

As cadeias de blocos e as operações de rede *peer-to-peer* se mostram cruciais para atingir essa meta. O *blockchain* é uma estrutura de dados ponto-a-ponto distribuída que representa um livro-razão de transações de troca de dados imutável. Na rede *blockchain* os registros das transações são distribuídos entre todos os nós, e cada nó confirma a validade de todos os blocos de transações adicionadas. Como a mesma cópia da cadeia é mantida por todos os nós usando algoritmos de consenso ponto-a-ponto, não há uma autoridade central para certificar as transações. Dessa forma *blockchains* permitem transações certificadas em um ambiente inseguro. Com base em um modelo de dados descentralizados para a privacidade da IoT, foi proposta a arquitetura de rede associando *software* de *blockchain* com o Sistema de Arquivos Ponto-a-Ponto Interplanetário (IPFS da sigla em inglês: Interplanetary Peer-to-Peer File System) para permitir controle de acesso (ALI, DOLUI e ANTONELLI, 2017).

Os autores afirmam que o *blockchain* fornece um registro imutável de todas as operações de dados de IoT incluindo a criação de dados pelos sensores e os acessos aos dados. Os dispositivos de IoT utilizados para um caso específico são agrupados em cadeias de blocos privadas, chamadas de *sidechains*. Os usuários podem possuir múltiplas *sidechains*, e cada rede de *sidechains* é responsável por manter um registro seguro das operações de dados ocorridas no seu contexto. As redes *sidechain* são conectadas num padrão modular que roda seu próprio *blockchain.* O consórcio *blockchain* é responsável por registrar com segurança qualquer requisição de acesso a quaisquer dados de IoT de usuários, e realizar o controle de acesso dessas requisições de entrada. O desenvolvimento de plataformas de *blockchain* é constante, e considerações de implementação devem ser feitas quando aplicadas à IoT.

Considerações finais

Conforme apresentado, a combinação de *blockchain* e IoT é poderosa. A tecnologia *blockchain* oferece soluções *peer-to-peer* resistentes, verdadeiramente distribuídas e descentralizadas. A capacidade de interagir de maneira confiável, com

Revista EduFatec: educação, tecnologia e gestão
V.1 N.1 janeiro-junho/2018

base em contratos inteligentes permite automatizar processos complexos de certificação de transações em várias etapas, possibilitando a interação entre dispositivos de IoT atendendo a um grande volume de geração de dados.

Os dispositivos de IoT são os pontos de contato com o mundo físico que quando suportados operacionalmente pela tecnologia *blockchain* para certificação da troca de dados, permite a automatização de fluxos de processos de controle com absoluta segurança.

No entanto alguns desafios ainda são evidentes. Um dos mais significativos se refere à questão do poder de computação necessário para validação dos blocos para inserção no *blockchain*. A criptografia e a verificação de transações de *blockchain* podem exigir um poder de processamento considerável, que pode não estar disponível em dispositivos de IoT.

O desenvolvimento do presente estudo possibilitou a análise de como a combinação de *blockchain* e IoT está sendo tratada atualmente, obtendo uma ampla visão sobre os aspectos de segurança e dos desafios a serem superados. A reflexão acerca dos benefícios e dificuldades ao se trabalhar com estas tecnologias permitiu avaliar diferentes recursos e como esses recursos podem ser adotados para um resultado eficaz.

De um modo geral, ambas as tecnologias demostraram um grande potencial de aplicabilidade, desde a descentralização do armazenamento dos dados, até aspectos de segurança e privacidade, passando pelos contratos inteligentes, que combinados possibilitam a interação segura de dispositivos inteligentes.

Setores de significativa importância social e econômica como saúde e educação poderão ser beneficiados, mostrando ser um passo importante para a construção de um mundo melhor e mais igualitário.

A especificação de cada tecnologia individual possibilitou criar uma visão mais clara e objetiva para, a partir deste conhecimento, aprofundar estudos para a implantação em contextos reais de aplicações de IoT.

Dada a relevância do tema, abre-se um leque de oportunidades para o desenvolvimento de novos projetos que visem experimentar e testar aspectos de segurança para garantir produtos e serviços que atendam as diferentes necessidades dos usuários com segurança e privacidade.

Agradecimentos

Agradeço a Deus por ter me dado saúde e sabedoria para superar as dificuldades.

A esta universidade, seu corpo docente e os orientadores.

À minha esposa, pelo amor, apoio e compreensão nos momentos de minha ausência dedicados ao estudo superior, que sempre me fizeram entender que o futuro é feito a partir da constante dedicação no presente.

Referências

ALI, M. S.; DOLUI, K.; ANTONELLI, F. **IoT Data Privacy via Blockchains and IPFS**. 2017. Disponível em: https://www.researchgate.net/publication/320853144_IoT_data_privacy_via_blockchains_and_IPFS. Acesso em: 06/06/2018.

DORRI, A.; KANHERE, S. S.; JURDAK, R.; GAURAVARAM, P. **Blockchain for IoT Security and Privacy:** The Case Study of a Smart Home. 2017. Disponível em: https://www.researchgate.net/publication/312218574_Blockchain_for_IoT_Security_and_Privacy_The_Case_Study_of_a_Smart_Home. Acesso em: 06/06/2018.

GANTAIT, A.; PATRA, J.; MUKHERJEE, A. **Integre dados de dispositivo a contratos inteligentes no IBM Blockchain**. 2018. Disponível em: https://www.ibm.com/developerworks/br/cloud/library/cl-*blockchain*-for-cognitive-iot-apps-trs/index.html. Acesso em: 26/05/2018

GARTNER. **Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017**, Up 31 Percent From 2016. 2017. Disponível em: https://www.gartner.com/newsroom/id/3598917. Acesso em: 29/05/2018.

HACKERNOON. **When IoT meets *Blockchain***. Disponível em: https://hackernoon.com/when-iot-meets-*blockchain*-%EF%B8%8F-892fecdaf00c. Acesso em: 23/05/2018

IEEEXPLORE. ***Blockchains* and Smart Contracts for the Internet of Things**. Disponível em: https://ieeexplore.ieee.org/document/7467408/ . Acesso em: 22/05/2018

MARQUES, K. L. **Internet das Coisas (IoT):** O que é? Aonde vive? Como se alimenta...!?. 2017. Disponível em: https://becode.com.br/internet-das-coisas/. Acesso em: 29/05/2018.

MOUJAHID, A. **A Practical Introduction to Blockchain with Python**. 2018. Disponível em: http://adilmoujahid.com/posts/2018/03/intro-blockchain-bitcoin-python/. Acesso em: 06/06/2018.

PORTALGSTI. **Os 05 Principais Desafios da Internet das Coisas**. Disponível em: https://www.portalgsti.com.br/2016/09/os-05-principais-desafios-da-internet-das-coisas.html. Acesso em: 29/05/2018

ROUSE, Margaret. **Smart Contract.** 2018. Disponível em: https://searchcompliance.techtarget.com/definition/smart-contract:. Acesso em: 26.05.2018.

TECNOBLOG. **Como funciona *blockchain* e bitcoins**. Disponível em: https://tecnoblog.net/227293/como-funciona-blockchain-bitcoin/. Acesso em: 19/05/2018

TIESPECIALISTA. ***Blockchain* e IoT uma combinação perfeita.** Disponível em: https://www.tiespecialistas.com.br/*blockchain*-e-iot-uma-combinacao-perfeita/. Acesso em: 27/05/2018

WATTERS. **The *Blockchain* for Education:** An Introduction. Disponível em: http://hackeducation.com/2016/04/07/*blockchain*-education-guide/. Acesso em 18/05/2018.