Sensor Store: uma loja de dados de IoT usando Tangle

Caio Martins Barbosa[1,2], Vinícius Fernandes Soares Mota[1], Roberta Lima Gomes[1], José Gonçalves Pereira Filho[1]

[1]Departamento de Informática – Universidade Federal do Espírito Santo (UFES)
Av. Fernando Ferrari, 514, 29075-910 - Vitória - ES, Brasil

[2]Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo (PRODEST), Av. João Batista Parra, 465, 29050-925 - Vitória - ES, Brasil

caio.barbosa@outlook.com, {vinicius.mota,
rgomes, zegonc}@inf.ufes.br

Abstract. *In an increasingly connected world, the connected devices that form the so-called Internet of Things (IoT) will become increasingly present in people's daily lives, whether monitoring or acting in the environment around them. The omnipresence of IoT will produce an excessive amount of data on the most diverse physical phenomena. By glimpsing a potential market, this work proposes an architecture for the commercialization of sensor data. Devices data will be published in Tangle, a Distributed Ledger Technologies (DLTs), which will store data immutably and allow payments in IOTA cryptocurrency without the charge of reward fees.*

Resumo. *Em um mundo cada vez mais conectado, os dispositivos conectados, que formam a chamada Internet das Coisas (IoT) se tornarão cada vez mais presentes no cotidiano das pessoas, seja monitorando ou atuando no ambiente ao seu redor. A onipresença da IoT produzirá uma quantidade excessiva de dados sobre os mais diversos fenômenos físicos. Vislumbrando um potencial mercado, este trabalho propõe uma arquitetura para comercialização de dados de sensores. Os dados dos dispositivos estarão publicados na Tangle, uma tecnologia de livros-razão distribuídos (DLTs) que armazenará os dados de forma imutável e permitirá a realização de pagamentos em criptomoeda IOTA sem cobrança de taxas de recompensa.*

1. Introdução

O século XXI será marcado pelo surgimento de uma *commodity* mais valiosa do que petróleo, os dados [The Economist 2017]. Empresas como Amazon, Apple, Google, Facebook e Microsoft disputam uma corrida em que o vencedor se transformará na *Standard Oil Company*[1] da era digital. Essas gigantes da computação sabem o valor e a importância estratégica dos dados para sobrevivência e diferenciação em um mercado

[1] https://pt.wikipedia.org/wiki/Standard_Oil_Company

altamente competitivo. Apple e Amazon são companhias que superaram a marca de 1 trilhão de dólares de valor de mercado [Streitfeld 2018]. Google e Facebook têm receitas baseadas principalmente em publicidade digital, visto que são líderes em anúncios exibidos de acordo com as buscas dos usuários ou com o tipo de conteúdo acessado.

Nesse mercado altamente rentável, os dados produzidos são oriundos das mais diversas fontes, incluindo de dispositivos IoT. Com a previsão da Cisco de 50 bilhões de dispositivos conectados até 2020 [Macaulay *et al*. 2015], a IoT, além de gerar novos e mais sofisticados serviços, também poderá gerar dividendos para os proprietários dos dispositivos. O Google poderá remunerar proprietários de veículos que forneçam localização do automóvel, a fim de compor os seus serviços de mapa de trânsito: Google Maps e Waze. A indústria farmacêutica ao desenvolver novas pesquisas será capaz de comprar dados de frequência cardíaca, pressão arterial, glicose no sangue, horas de sono, atividades físicas, entre outros dados de saúde, de forma a permiti-la superar um dos maiores desafios de pesquisas médicas, o recrutamento de participantes para o estudo.

Considerando os ilimitados cenários de aplicação de sensores, os autores acreditam que para aproveitar o potencial mercado de dados de IoT, mecanismos de comércio precisam ser desenvolvidos de forma que permitam conectar os consumidores com os proprietários dos dispositivos. Tais mecanismos deverão contemplar requisitos que atendam à natureza distribuída, de diferentes capacidades de processamento, armazenamento, comunicação heterogêneos, quando não restritas e, evidentemente, recursos de pagamento.

Este trabalho apresenta uma arquitetura, batizada de Sensor Store, para comercialização de dados de dispositivos utilizando tecnologias de livros-razão distribuídos (DLTs - *Distributed Ledger Technology*) para armazenamento distribuído e pagamentos sem taxas. Na prática, a Sensor Store facilita a conexão entre os consumidores (compradores) e anunciantes (vendedores) de ofertas de dados de sensores.

Devido às características dos dados gerados pela IoT, como tamanho do dado, quantidade e necessidade de escalabilidade, a Sensor Store utiliza a tecnologia Tangle para armazenamento e IOTA para pagamento das transações. A escolha dessa DLT como *backend* da Sensor Store possibilita aos vendedores de dados de IoT e à própria loja desconsiderar questões relativas ao local onde os dados estarão armazenados, ou seja, não há preocupação de manter o funcionamento (licenciamento, backup, atualização de *patchs* de segurança, etc.) de um banco de dados local ou em nuvem, pois os dados dos dispositivos estarão armazenados na Tangle. Além disso, ao vincular o endereço IOTA a um dispositivo, o vendedor é inserido imediatamente em um mercado de dados sem a necessidade de possuir um cartão de crédito, conta bancária ou em empresas de pagamentos on-line, como a PayPal[2]. E, diferentemente da Bitcoin – a mais famosa implementação de Blockchain – o pagamento não sofrerá aplicação de taxas para que ele seja efetivado.

[2] https://www.paypal.com

O restante do documento está organizado como segue. A Seção 2 apresenta dois tipos de tecnologias de livro-razão distribuído. A Seção 3 descreve alguns trabalhos relacionados. A Seção 4 é apresenta o conceito de funcionamento da loja com a Tangle, a arquitetura da loja, bem como o estado atual de implementação. Na Seção 5 dois possíveis cenários de uso da loja são introduzidos. A Seção 6 discute alguns problemas ocorridos durante a implementação. Por fim, a Seção 7 conclui o artigo, tecendo as considerações finais e as perspectivas de trabalhos futuros.

2. Tecnologias de DLTs

A utilização da tecnologia de livros-razão distribuídos (DLTs) se apresenta como um modelo alternativo para o armazenamento de informação uma vez que essa tecnologia se comporta como um tipo de banco de dados que está distribuído entre todos os membros da rede e quaisquer mudanças serão refletidas simultaneamente para todos participantes.

Um caso especial dessas tecnologias são as Blockchains, que implementam a ideia de livros-razão distribuídos por meio de um mecanismo organizacional baseado em encadeamento de blocos de transações. Uma outra tecnologia DLT de destaque é a Tangle que, diferentemente da Blockchain, é implementada em uma estrutura de dados de grafo acíclico direcionado. Ambas as tecnologias são descritas brevemente a seguir.

2.1 Blockchain

A tecnologia Blockchain surgiu em 2008 para apoiar a implementação da criptomoeda Bitcoin [Nakamoto 2008]. Apesar de a idealização original ter sido orientada para pagamentos eletrônicos, as Blockchains foram rapidamente identificadas como de aplicabilidade mais abrangente. Por exemplo, na implementação de gerenciamento de redes virtualizadas [Rebello *et al*. 2018], controle de registros eletrônico de saúde de paciente [Conceição et al. 2018], preservação de documentos digitais acadêmicos [Costa *et al.* 2018], entre outros.

Uma Blockchain opera como um livro-razão que pode registrar transações entre entidades sem um ente centralizador, garantindo assim confiabilidade distribuída no sistema [Wood 2014]. Esses registros são realizados de forma eficiente, permanente e podem ser facilmente verificáveis com base em criptografia. Normalmente, uma Blockchain é gerenciada por uma rede P2P (do inglês *peer-to-peer*), onde os participantes aderem ao protocolo da aplicação e validam os blocos que são criados ao longo da existência da cadeia. Uma vez que um bloco é registrado (inserido na cadeia) pelo coletivo de nós da rede, seus dados não podem ser alterados (imutabilidade) sem a devida alteração de todos os blocos subsequentes a ele.

Na tecnologia Blockchain cada bloco está ligado a apenas um bloco anterior a ele referenciando via um *hash pointer*. No caso de Blockchains como a do Bitcoin, os blocos são adicionados à medida que são validados por um processo matemático de tentativas sucessivas (denominado Prova de Trabalho, ou *Proof of Work*) para determi-

nar o valor que resolve o *hash* criptográfico do bloco de transações. O responsável por adicionar um novo bloco à cadeia recebe uma recompensa, que é um incentivo financeiro para que a processo seja continuamente realizado.

A Blockchain utiliza uma infraestrutura de chaves criptográficas assimétricas para registrar e validar as transações. A criptografia assimétrica prevê a existência de duas chaves uma pública e outra privada, a chave pública é usada para gerar um endereço público para as transações, algo equivalente ao número de uma conta em uma instituição bancária, já a chave privada permite acessar os recursos associados a uma chave pública.

A tecnologia Blockchain possui alguns princípios básicos, são eles segurança, privacidade, descentralização, incentivo à participação na rede e inclusão, que são descritos a seguir.

Atendendo ao princípio segurança, a tecnologia permite que as transações sejam armazenadas de forma segura, sendo virtualmente impossível alterá-las após a inclusão na cadeia e o sua confirmação. Para tanto, seria necessário, como no caso do Bitcoin, o controle de mais da metade do "poder computacional" da rede.

Já no quesito privacidade, uma chave pública não pode ser imediatamente associada a uma pessoa ou instituição, funcionando como um pseudônimo para o usuário. Sendo assim, a tecnologia oferece certo nível de privacidade (pseudo-anonimicidade).

No quesito descentralização, o poder sobre a rede formada pela tecnologia é distribuído entre os participantes da rede, não existe a figura de um órgão central que regula como as transações são realizadas, e as decisões na rede também são tomadas pelo grupo que a forma. Com isso, cada minerador possui uma parcela de "poder de decisão" sobre a rede, proporcional ao seu poder computacional.

No quesito incentivo à participação na rede, existe o papel do minerador. Em geral, os nós da rede empregam energia e poder computacional para validar as transações de um bloco. Mas no caso particular do minerador, ele atua na criação de novos blocos válidos. Para tanto, com base na Prova de Trabalho, uma vez que ele consegue resolver o problema matemático definido pela rede criando um bloco válido, e o seu bloco é inserido com sucesso na cadeia, como recompensa, o minerador recebe novas moedas pelo trabalho realizado.

Por fim, no quesito inclusão, a Blockchain proporciona inclusão econômica, pois permite que recursos sejam transferidos entre dois usuários independentes da posição geográfica dos envolvidos em uma transação. A rede trata as transações sem distinção, taxando cada transação de mesma forma.

2.2 Tangle

No contexto de IoT, em que dispositivos estão constantemente fazendo medições e gerando dados, criptomoedas como a Bitcoin são pouco viáveis para utilização principalmente devido às taxas associadas tenderem ser maiores do que valores a serem cobrados pelos dados dos sensores. Nesse sentido, Popov (2017) desenvolveu a IOTA, uma crip-

tomoeda voltada para a realização de micropagamentos sem cobrança de taxas apoiada na Tangle.

A tecnologia Tangle foi criada para atender as necessidades do projeto IOTA que tem como foco oferecer uma infraestrutura de microtransações para o universo da *Internet of Things.* Sua aplicabilidade, no entanto, não se restringe a pagamentos eletrônicos, mas envolve um escopo bem mais abrangente, tal como ocorre com a tecnologia Blockchain.

Conforme mencionado, diferentemente da Blockchain, em que a implementação é baseada uma lista encadeada de blocos de transações, os quais são adicionados à lista conforme são validados por meio de processo matemático, a Tangle é baseada na implementação de um Grafo Acíclico Direcionado (do inglês, *Directed Acyclic Graph* − DAG). Cada nó do grafo é uma transação e para adicionar uma nova transação na DAG, existe um processo matemático, semelhante à Blockchain, que termina por validar outros duas transações pré-existentes. Justamente devido a essa relação temporal entre as transações, garante-se que o grafo seja acíclico.

A adição de novas transações na Tangle é mais simples do que no Blockchain, sendo assim, ocorre que a validação demanda um esforço computacional bem menor que aquele da mineração na Blockchain, a qual envolve múltiplas transações. Por sua vez, a validação de uma transação pré-existente é simples e pode ser realizada em tempo constante.

As transações na Tangle podem transportar valores monetários ou dados, sejam eles enviados por um carro, monitor cardíaco ou aplicativo de telefone, etc.. O canal MAM, protocolo de comunicação de dados de segunda camada, adiciona a funcionalidade de emitir e acessar um fluxo de dados criptografados [Handy 2017]. Um publicador ao criar um canal MAM envia fluxo de dados por meio de transações para os ouvintes daquele canal, de modo similar a exibição de um vídeo do YouTube[3]. O protocolo de consenso da IOTA adiciona integridade a esses fluxos de mensagens e criptografia de dados. Não sendo possível por parte de terceiros (ouvintes) interferir nas mensagens, por exemplo, enviando *spam* pelo canal. Existem três modos de acesso ao canal: público, restrito e privado. O modo público é acessado por qualquer pessoa que conheça o endereço de publicação dos dados. O modo privado é restrito ao proprietário do canal. E o modo restrito possibilita a qualquer pessoa com o endereço e a chave de acesso consultar o fluxo de dados. A chave de acesso pode ser alterada a qualquer momento pelo proprietário, revogando o acesso aos dados aos ouvintes que não tenham a nova chave.

Na Tangle todos os participantes da rede desempenham a mesma função, isto é, todos os participantes emitem e validam transações. Enquanto que na tecnologia Blockchain isso não é observado. Tal distinção entre dispositivos pode levar a conflitos na mineração de blocos em virtude das recompensas previstas. Nesse caso, uma disputa entre mineradores pode transformar um paradigma de validação concebido originalmen-

[3] https://www.youtube.com/

te descentralizado em um paradigma centralizado, constituído por mineradores de maior capacidade de processamento.

3. Trabalhos Relacionados

Embora a utilização de Blockchain para diversos domínios de problema tenha sido proposta na literatura, poucos trabalhos avaliaram a utilização da Tangle como tecnologia de controle de transações. Os requisitos associados a um sistema de venda de dados de sensoriamento obtidos por dispositivos conectados tornam a Tangle uma tecnologia viável para atender a demanda de centenas de micro vendas ocasionadas pela geração desses dados.

Com uma proposta de negócio semelhante à da Sensor Store, o aplicativo Wibson [Travizano *et al.* 2018] também propõe um *marketplace* para que os usuários disponibilizem os seus dados pessoais para comercialização, de forma análoga aos dispositivos IoT da Sensor Store. Contudo, diferentemente da Sensor Store, o Wibson é baseado no uso da tecnologia Blockchain para prover a infraestrutura de loja descentralizada.

Mišura e Žagar (2017) propõem um modelo de mercado de dados de IoT centralizado tanto no catálogo de dados quanto na própria troca, em que os provedores de dados da IoT registram suas ofertas e ajudam os consumidores a encontrá-los. O modelo proposto apoia-se em uma arquitetura tradicional web: servidor de banco de dados e aplicação (web). Portanto, os dados dos dispositivos estariam armazenados em um banco de dados.

Wörner e Bomhard (2014) abordam uma solução distribuída para criação de um mercado de dados de IoT com pagamento direto em Bitcoin e troca de dados *peer-to-peer* através de Blockchain. Os autores propõem um repositório central para registro dos sensores. O comprador acessa o repositório para selecionar o sensor e pagar pelos dados em Bitcoin. Um websocket é mantido aberto entre comprador e o repositório aguardando a confirmação de pagamento e publicação dos dados do sensor na Blockchain. Como os dados são publicados diretamente na Blockchain sem criptografia, qualquer usuário pode acessá-los.

A IDMoB [Özyılmaz *et al.* 2018] introduz o conceito de uma loja de dados de IoT implementada como um contrato inteligente Ethereum e o Swarm[4] sendo usado como a plataforma de armazenamento distribuído. Ou seja, os autores propõem que o que local para registro dos sensores seja construído como um contrato inteligente Ethereum. Logo, o comprador de dados deverá pesquisar por dispositivos e realizar pagamentos usando funcionalidades de *smart contract*. Os dados de dispositivos não são publicados diretamente na Blockchain, eles são publicados nos arquivos Swarm. E os dados são publicados em intervalos de tempo superiores a 30 minutos.

[4] https://swarm-guide.readthedocs.io/en/latest/

Este trabalho se diferencia dos demais por propor o desenvolvimento de uma loja de IoT suportada pela Tangle, uma tecnologia de livro-razão distribuída em uma estrutura DAG. Além de armazenar os dados publicados pelos sensores, a tecnologia Tangle provê aos consumidores a realização de micropagamentos sem cobrança de taxa e o consumo de dados em tempo real diretamente do vendedor, pois a publicação de dados não demanda esforço computacional. Portanto, o consumidor pode "assinar" um feed e obter os dados em tempo real. Enquanto que na Blockchain a latência de publicação de dados seria muito maior em função do tempo necessário para empacotar as transações e validar o bloco, logo há atraso na publicação de dados.

4. Sensor Store

Considerando as previsões de crescimento da presença de dispositivos de IoT – sensores e atuadores – a proposta deste trabalho é o desenvolvimento de uma loja que possibilite a realização de comércio de dados de tais dispositivos. Os proprietários dos objetos (vendedores) divulgarão suas ofertas de dados na loja, os compradores farão solicitações de compra e a loja gerenciará os contratos. O objetivo da Sensor Store é ser o Mercado Livre[5] para dados de dispositivos, ou seja, um local para que compradores e vendedores, independentemente de serem pessoas físicas ou pessoas jurídicas, possam realizar comércio diretamente entre eles.

De acordo com objetivo apresentado, o papel da Sensor Store é definido por: i) possibilitar os vendedores cadastrarem seus dispositivos e, consequentemente, os anúncios de oferta de dados; ii) identificar o pagamento feito aos vendedores e iii) gerenciar os contratos de compra. A Figura 1 exemplifica o funcionamento básico da Sensor Store.

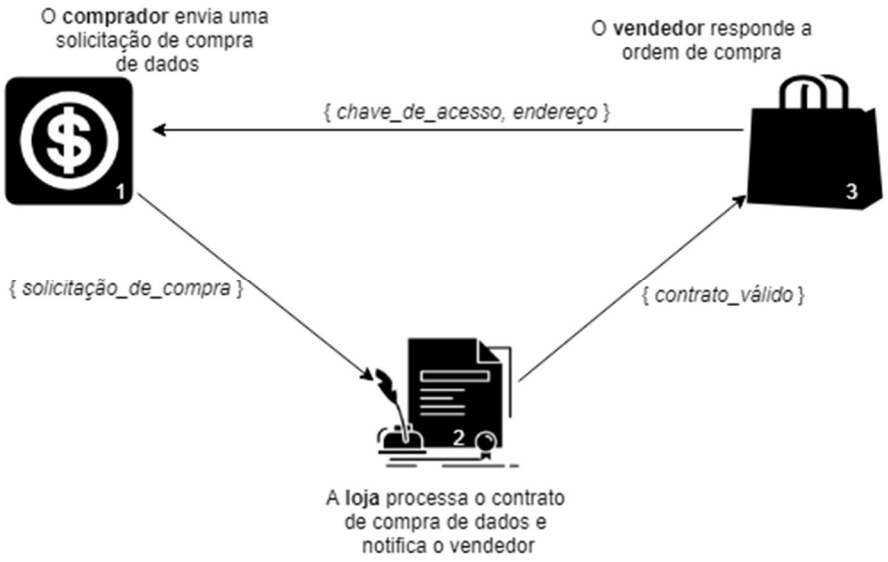

Figura 1. Representação do funcionamento básico da loja

[5] https://www.mercadolivre.com.br/

Em 1) o comprador submete uma solicitação de compra de um anúncio. No passo 2) a loja recebe a solicitação do comprador e passa a monitorar o pagamento a fim de comunicar ao vendedor da compra de anúncio e a existência de um contrato. Uma vez que o vendedor é notificado, no passo 3) ele enviará ao comprador o endereço e a chave de acesso aos dados do dispositivo.

Posto o funcionamento básico da loja, torna-se imperioso o esclarecimento de conceitos que foram abstraídos na representação da Figura 1. A loja é uma aplicação Web de divulgação de anúncios de ofertas de dados, cuja interação com os dispositivos e seus usuários (vendedores e compradores) é estabelecida por meio da tecnologia Tangle. Um comprador de dados ao selecionar uma oferta na Sensor Store executará uma transação de *tokens IOTA* para um endereço Tangle da carteira do vendedor. Por sua vez, a loja monitorará a rede Tangle para identificar a confirmação do pagamento por meio da mudança de estado de "pendente" para "confirmado". Dado que o pagamento seja confirmado, a loja controlará a vigência do contrato e notificará o vendedor por meio de uma transação (zero *IOTA*) a autorização de acesso do comprador (endereço Tangle). O vendedor, ao receber a mensagem de autorização, realizará uma transação (zero *iota*) para o endereço do comprador informando a chave de acesso e o endereço do canal MAM em que os dados serão publicados.

4.1. Arquitetura de Implementação

A proposta de arquitetura para a Sensor Store baseada na tecnologia Tangle é apresentada na Figura 2, onde se vê os seguintes componentes:

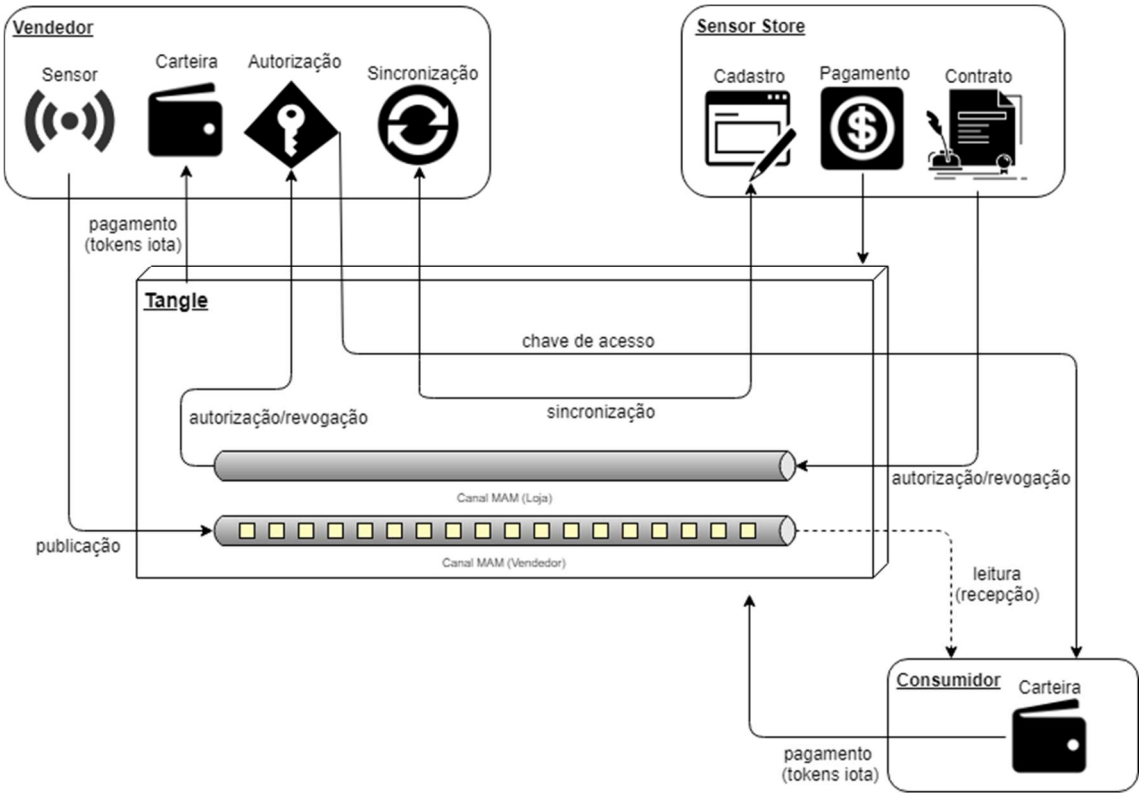

Figura 2. Arquitetura da Sensor Store

- **Tangle**: um *distributed ledger* capaz de realizar transações de pagamento entre o comprador e o vendedor, transações de envio de informações (mensagens) para os dispositivos, além de permitir aos dispositivos a publicação de dados de poluição do ar, temperatura corporal, pressão de pneus, velocidade do veículo, localização, entre outros dados de sensores.
- **Sensor**: é componente (dispositivo IoT) responsável por gerar as medições. Ele deverá ser capaz de publicar os dados na Tangle através do canal MAM do vendedor.
- **Carteira**: uma carteira eletrônica é responsável por armazenar a *seed* (chave privada) e os endereços (chaves públicas) dos usuários. É por meio das chaves públicas e privadas que os usuários (comprador e vendedor) recebem ou enviam *tokens iota* na solução.
- **Canal MAM do vendedor**: este componente é responsável por registrar as medições dos dispositivos na Tangle através de um canal MAM restrito. Os consumidores poderão ler os dados ao passo que as medições forem publicadas, pois um canal MAM tem característica de transmissão (*stream)* de dados.
- **Sincronização**: para que o dispositivo possa vender seus dados na loja, ele precisa ser cadastrado e ser capaz de perceber os eventos gerados pela loja em seu canal MAM privado. Para o dispositivo conseguir ler esses eventos, a loja inicia um processo de negociação para estabelecimento de comunicação similar ao *handshake*[6] do TCP.
- **Autorização**: durante a vigência do contrato, a loja publica em seu canal MAM o início e o término. O módulo de autorização deve ser capaz de perceber esses eventos e enviar a chave de acesso para um novo consumidor, bem como trocar a chave e enviá-la para os consumidores com contratos vigentes, quando um contrato expirar.
- **Canal MAM da Sensor Store**: meio de comunicação da loja com os dispositivos. A loja publicará no canal mensagens direcionadas de autorização ou revogação de acesso à medida que compras sejam realizadas ou contratos expirem.
- **Cadastro de dispositivos**: funcionalidade similar ao cadastro básico dos produtos como de qualquer outra loja. O vendedor deverá fornecer informações básicas sobre o dispositivo, tais como: nome, localização, a propriedade e a unidade de medida, além do modelo de comercialização (tempo ou cota de uso).
- **Pagamento**: os pagamentos entre vendedores e consumidores são realizados pela criptomoeda IOTA. A loja permitirá a seus usuários conectar suas carteiras e efetuarem os pagamentos.
- **Gestão de contratos:** este componente atua em dois momentos distintos: i) início de vigência do contrato: a atuação ocorre pelo monitoramento da

[6] https://en.wikipedia.org/wiki/Handshaking#TCP_three-way_handshake

transação na Tangle de transferência de *tokens iota* entre o comprador e o vendedor até que o estado da transação mude de "pendente" para "confirmado". Concretizada a confirmação de pagamento, este componente publicará no canal MAM da loja as informações de autorização de acesso do comprador; ii) fim de vigência do contrato: uma vez que o contrato expire, o gestor de contrato publicará no canal MAM da loja as informações de revogação de acesso do comprador.

4.2. Transações

Uma transação é a unidade básica de informação manipulada pela solução. Os seguintes tipos de transações são definidos:

- **Pagamento:** transações de pagamentos transferirão *tokens iota* da carteira do comprador para o vendedor. Esse tipo de transação é nativa da Tangle.
- **Publicação:** a publicação de dados é realizada no canal MAM do tipo restrito do vendedor. Esse tipo de transação não exige transferência de *tokens iota*.
- **Autorização/Revogação:** este tipo de transação são mensagens enviadas da loja pelo componente Gestão de Contrato para os dispositivos. O envio de mensagens não gera transferência de *tokens iota*.
- **Sincronização:** as transações de sincronização são realizadas para que a loja informe o endereço do seu canal MAM e conheça o endereço do dispositivo ou quando ocorre a necessidade de trocar a chave de acesso ao canal MAM do dispositivo. Todas as transações geradas na sincronização não consomem *tokens iota*.
- **Chave de Acesso:** este tipo de transação é realizado no início de vigência de um contrato diretamente para o novo consumidor ou no término de vigência de contrato, pois será necessário trocar a chave de acesso e enviá-la para todos os consumidores com contrato em vigência. Essa transação não transfere *tokens iota*.

É importante ressaltar que apesar da Figura 2 conter uma transação "leitura (recepção)", trata-se apenas de uma representação para melhor entendimento da arquitetura. Não acontecendo efetivamente uma transação para ler dados de um canal MAM.

4.3. Estado atual da implementação

O desenvolvimento até o momento contempla uma versão inicial da Sensor Store para cadastro de usuários, cadastro de dispositivos e gestão de contrato. Além disso, uma versão do vendedor (dispositivo) que sincroniza com a loja e publica os dados na Tangle. Portanto, o foco inicial foi o desenvolvimento de funcionalidades que permitissem o cadastro e sincronização de dispositivos, gestão de contrato e a publicação de dados.

A Figura 3 (a) exibe a tela para cadastro de dispositivo. Informações básicas como nome, localização e valor são registradas. A Figura 3 (b) exibe a tela para cadastro de sensor, em que as informações básicas do sensor são registradas em conjunto com o dispositivo no qual o sensor está embutido, além de informações sobre a propriedade e a unidade de medida.

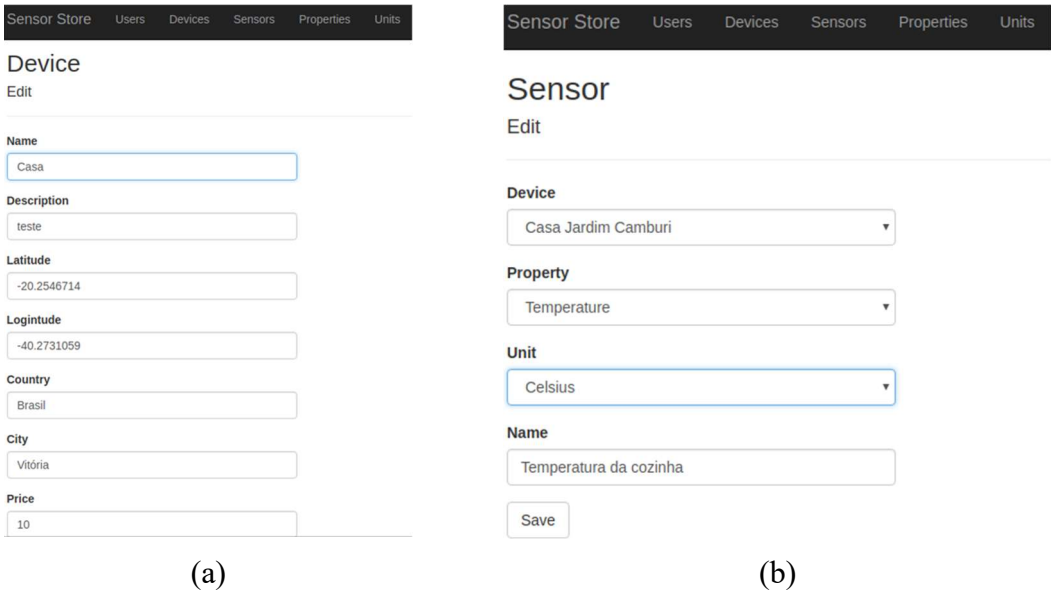

Figura 3. Cadastro de dispositivo e sensor

5. Exemplos de caso de uso

Esta seção apresenta dois casos de uso em que a Sensor Store facilitaria a procura e compra de dados de sensores: *Healthcare* e transporte público. Embora simples, estes cenários servem para ilustrar o potencial da arquitetura proposta.

Considerando um cenário em que uma empresa startup[7] de plano de saúde – *healthtech* (junção de *health* "saúde" em inglês e *tech*, abreviação de *technology*) – deseja estabelecer-se no mercado de Vitória (ES). E que essa *healthtech* pela essência das empresas startups de fornecerem serviços inovadores tem um modelo de negócio em que o cálculo do plano de saúde leva em consideração características endêmicas, por exemplo, malária, febre amarela, câncer, etc.. Para o caso de Vitória, a startup tomou por referência o trabalho de Freitas *et al.* (2016), cujo estudo aponta grande número de morbidade e doenças respiratórias ocasionados pela poluição atmosférica.

Nesse cenário, a *healthtech* consultaria a Sensor Store em busca de dados de sensores de poluição atmosférica de material particulado fino (PM10), dióxido de enxofre (SO2) e ozônio (O3); além de registros de temperatura e umidade. E compraria esses

[7] https://pt.wikipedia.org/wiki/Startup

dados diretamente dos proprietários de sensores, sem a necessidade da empresa criar uma estrutura sensores espalhados pela cidade para atender o seu negócio.

O segundo cenário considera que uma companhia de transporte de passageiros de uma grande cidade deseja desenvolver um portal web de monitoramento de seus ônibus para disponibilizar informações mais precisas sobre as suas viagens, de forma a permitir aos seus usuários o acompanhamento de possíveis atrasos de veículos em função da situação do trânsito. Para isso, a companhia processará leituras de seus próprios veículos e de terceiros transmitidos ao vivo na Tangle. O acesso aos dados de terceiros se dará por compra de dados na Sensor Store. Uma vez que a companhia tenha recebido as chaves de acesso dos veículos de terceiros, ela poderá "se inscrever" no canal MAM de cada veículo e acessar o fluxo de dados, como se fosse um *feed* de RSS.

6. Discussões e limitações da arquitetura

A Tangle ainda é uma tecnologia em desenvolvimento e, como tal, apresenta certa instabilidade e inconsistência. O ambiente de teste da Tangle por vezes gera erros, sendo que muitos deles são pouco documentados. Um problema ocorrido com a publicação de dados no canal MAM era gerado por usar o mesmo *seed* ao iniciar o canal, o que obrigou a publicação de uma mensagem inicial. Caso contrário, ao se recuperar[8] a mensagem, um erro seria gerado.

O pioneirismo da Tangle também é afetado pela escassez de recursos que permitam interagir com ela, por exemplo, bibliotecas, *frameworks*, documentação, códigos-fontes de exemplos, etc.

O processo de revogação, em função da estrutura atual da Tangle, é uma limitação da arquitetura da loja, pois uma vez que um contrato tenha sido encerrado, o componente de gestão de contratos comunicará ao dispositivo por meio do canal MAM o encerramento. Logo, o dispositivo deverá trocar a chave de acesso do seu próprio canal MAM e informar à loja por meio do processo de sincronização sobre a alteração. A loja publicará então uma mensagem em seu canal com a nova chave de acesso encriptada com a chave pública dos compradores. Portanto, esse processo obriga aos compradores ficarem escutando o canal da loja para verificar as possíveis revogações de acesso.

7. Conclusões

Neste artigo, propomos a criação de um local para divulgação de ofertas e comercialização de dados de dispositivos IoT promovida por meio da Tangle, uma *distributed ledger technology* subjacente à loja que provê transferência de *tokens iota* (criptomoeda) e disseminação de mensagens (medições dos dispositivos). A loja, componente web da arquitetura, essencialmente cumpre o papel de ser um *hub* de anúncios de vendas de dados

[8] https://github.com/iotaledger/mam.client.js/issues/5

de dispositivos, similar ao que é o Mercado Livre. Nela os vendedores se registram, cadastram e vendem os seus anúncios para outros usuários, enquanto que a Tangle provê a moeda de pagamento (*IOTA*) e atua como local em que os dados (produto vendido) estão armazenados.

Portanto, mesmo que este trabalho seja a demonstração de conceitos básicos e de um protótipo em evolução para venda de dados de dispositivos IoT em troca de criptomoeda, a proposta apresenta-se como uma solução bastante promissora para conectar vendedores (proprietários de dispositivos) e compradores de dados (consumidores). Por outro lado, por ser uma tecnologia ainda em desenvolvimento, é necessário fazer uma avaliação de desempenho robusta da tecnologia, em cenários diversos e de maior complexidade, para poder avaliar melhor a tecnologia.

Como trabalhos futuros, queremos disponibilizar um protótipo da Sensor Store ao público, o que certamente ajudará no processo de avaliação da robustez da solução. Essa implementação incluirá um modo de conectar a carteira do comprador na loja de forma a permitir fazer o pagamento pela própria loja. Também objetiva-se desenvolver uma solução de *smart contract* em Blockchain com Ethereum. Um aspecto importante a ser considerado no futuro é a adição de novos recursos da Tangle para canal MAM. Há expectativa de que em uma nova versão, haverá a possibilidade de se criarem múltiplos canais. Tal característica simplificará o processo de revogação de acesso.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), do CNPq, da FAPES, do PRODEST e do projeto RNP FUTEBOL.

Referências

Conceição, A.F., Silva, F.S.C., Rocha, V., Locoro, A. e Barguil, J.M.M (2018) "Eletronic Health Records using Blockchain Technology", Workshop Blockchain 2018, Campos do Jordão-SP. Simpósio Brasileiro de Redes de Computadores, 2018.

Costa, R., Faustino, D., Lemos, G., Queiroga, A., Djohnnatha, C., Alves, F., Lira, J. e Pires, M. (2018) "Uso Não Financeiro de Blockchain: Um Estudo de Caso Sobre o Registro, Autenticação e Preservação de Documentos Digitais Acadêmicos", Workshop Blockchain 2018, Campos do Jordão-SP. Simpósio Brasileiro de Redes de Computadores, 2018.

Freitas, C.U., Leon, A. P., Junger, W. e Gouveia, N. (2016) "Poluição do ar e impactos na saúde em Vitória, Espírito Santo. Revista Saúde Publicação. vol.50, 4.

Handy, P. (2017) "Introducing Masked Authenticated Messaging", https://blog.iota.org/introducing-masked-authenticated-messaging-e55c1822d50e

Macaulay, J., Buckalew, L. e Chung, G., (2015) “Internet Of Things In Logistics”.

Mišura, K. e Žagar, M. (2016) “Data marketplace for Internet of Things,” in Proceedings of the 1st IEEE International Conference on Smart Systems and Technologies, SST 2016, pp. 255–260, Croatia, October 2016.

Nakamoto, S. (2008). “Bitcoin: A peer-to-peer electronic cash system.” https://bitcoin.org/bitcoin.pdf.

Popov, S. (2018), “The Tangle” – Version 1.4.3 disponível em: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

Rebello, G.A.F., Alvarenga, I.D., Sanz, I.J. e Duarte O.C.M.B. (2018) “SINFONIA: Gerenciamento Seguro de Funções Virtualizadas de Rede através de Corrente de Blocos”, Workshop Blockchain 2018, Campos do Jordão-SP. Simpósio Brasileiro de Redes de Computadores, 2018.

Streitfeld, D., (2018), “Amazon Hits $1,000,000,000,000 in Value, Following Apple”, https://www.nytimes.com/2018/09/04/technology/amazon-stock-price-1-trillion-value.html.

The Economist, (2017) “The world’s most valuable resource is no longer oil”, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

Travizano, M., Minnoni, M., Ajzenman, G., Sarraute, C., Della Penna, N. (2018), “Wibson: A decentralized marketplace empowering individuals to safely monetize their personal data” - disponível em: https://wibson.org/wp-content/uploads/2018/10/Wibson-Technical-Paper-v1.1.pdf

Wood, G. (2014). “Ethereum: A secure decentralised generalised transaction ledger”. *Ethereum Project Yellow Paper.* https://github.com/ethereum/yellowpaper.

Wörner, D. e Von Bomhard, T. (2014) “When your sensor earns money: Exchanging data for cash with Bitcoin,” inProceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 295–298.