

Tecnologia blockchain - IOTA aplicada a rastreabilidade de produtos

RESUMO

As atuais técnicas de trocas de informações durante o transporte de produtos na cadeia de suprimentos causam atrasos e erros humanos. Soluções computacionais geralmente envolvem bancos de dados centralizados hospedados por uma das partes interessadas. Esse contexto desperta o interesse em soluções descentralizadas, confiáveis e seguras, como é o caso da tecnologia Blockchain. O objetivo deste trabalho está na investigação dos desafios e possibilidades de rastrear as informações de produtos durante o processo de transporte utilizando o sistema de registro distribuído (*ledger*) da IOTA. Verificou-se que existem limitações nos atuais sistemas Blockchain voltados para rastreabilidade de produtos, por isso foi proposto um modelo que combina IOTA com dispositivo IoT para acompanhamento da situação dos produtos. A partir do modelo proposto, identificou-se que a tecnologia pode habilitar maior confiança entre os atores da cadeia de suprimentos e fazer parte de novas soluções que evitem prejuízos e erros humanos durante o transporte.

PALAVRAS-CHAVE: Blockchain. Iota. Tangle. Cadeia de suprimentos. rastreabilidade. IoT.

Wellington Fernandes Silvano
Wellington.fernandes@posgrad.ufsc.br

Universidade Federal de Santa Catarina, Santa Catarina - Brasil

Roderval Marcelino
roderval.marcelino@ufsc.br

Universidade Federal de Santa Catarina, Santa Catarina - Brasil

Martin Augusto Gagliotti Vigil
martin.vigil@ufsc.br

Universidade Federal de Santa Catarina, Santa Catarina - Brasil

INTRODUÇÃO

Uma maneira eficaz de melhorar o processo de tomada de decisões de negócios para os atores da cadeia de suprimento consiste em compartilhar informações dos produtos entre todas as partes envolvidas no processo (XIE et. All, 2019). Em geral, as informações são trocadas de maneira semi-digital como e-mails, telefone e aplicativos de banco de dados centralizados (IMERI; KHADRAOUI, 2018), além disso uma enorme quantidade de dados é produzida, mas frequentemente apenas uma fração é capturada e utilizada. Muitas vezes, o compartilhamento ocorre apenas ponto a ponto, pois são registradas em diferentes sistemas de software e compartilhadas em cópias impressas. Estes sistemas pouco conectados implicam em caminhões e contêineres parados, fluxo de caixa preso na forma de mercadorias que aguardam documentos comerciais, perda de documentação, imprecisão no rastreamento das cargas e dados diluídos ou perdidos; os dados originais são encurtados, errados ou enganosos ao alcançar os atores mais abaixo na cadeia (LUND-NIELSEN, 2018).

Em sistemas centralizados, o dono do banco de dados detém o controle da informação, e seu direito de acesso pode ir além do monitoramento dos dados, possibilitando qualquer alteração desses, o que implica na falta de confiança entre as partes, uma vez que as informações compartilhadas podem ser modificadas e não são garantidos os acessos de terceiros a esses dados. No entanto, os recentes avanços em tecnologia de registro distribuído – ou *Distributed Ledger Technology (DLT)* – potencializam o compartilhamento de dados de maneira segura, transparente e imutável. Dentre as DLTs voltadas para IoT destaca-se a IOTA, uma criptomoeda com uma nova arquitetura, que promete alta escalabilidade, sem taxas e baixa latência, focadas em soluções para Internet das Coisas. Segundo Kiel, Arnold e Voigt (2017), até o final de 2020, as empresas gastarão cerca de £ 250 bilhões por ano em IoT; metade desses gastos advém das indústrias de manufatura, transporte e serviços públicos.

A Fundação Iota, responsável pelo desenvolvimento da tecnologia Iota/Tangle, possui entre outros objetivos, atender os requisitos para a “cadeia global de suprimentos”. No entanto, foram realizadas pesquisas em três bases de dados acadêmicas: IEEE Xplore, Web of Science e Scopus com os descritores “IOTA” AND “Tangle”, após as buscas realizadas não foram encontrados resultados relacionados ao uso da tecnologia IOTA na cadeia de suprimentos. O foco deste trabalho está na investigação da possibilidade de rastrear as informações detalhadas dos produtos durante o processo de transporte utilizando IOTA/Tangle.

METODOLOGIA

Essa é uma pesquisa tecnológica, de natureza exploratória que visa investigar os potenciais da tecnologia IOTA para a cadeia de suprimentos. A Primeira parte apresenta uma sinopse sobre a cadeia de suprimentos. A segunda etapa trata da realização de uma revisão bibliográfica sobre aspectos das tecnologias de registro distribuído, seus potenciais e limitações para a cadeia de suprimentos. A terceira etapa investiga os fundamentos da tecnologia IOTA, em artigos publicados na IEEE Xplore, Web of Science, Scopus e Researchgate, além de documentos da Fundação IOTA(blog.iota.org e iota.org). Os artigos foram encontrados com os descritores “IOTA” AND “Tangle”. Na última seção apresentamos nossa visão sobre os

potenciais da IOTA para o rastreamento na cadeia de suprimentos, finalizando com um modelo de aplicação.

CADEIA DE SUPRIMENTOS

A cadeia de suprimentos é composta por fabricantes e prestadores de serviços que trabalham juntos para fornecer produtos e serviços aos consumidores. Inclui todas as atividades relevantes para o fluxo de informações, desde o estágio da matéria-prima até o momento em que as mercadorias são entregues ao usuário final, incluindo informações, materiais e finanças, à medida que eles se movem do fornecedor ao fabricante, ao atacadista, ao varejista ou ao consumidor. O transporte de mercadorias apresenta um dos principais desafios a ser administrado devido à sua intensidade e às diversas partes envolvidas nesse processo. No mundo, bilhões de produtos são projetados, fabricados, entregues e vendidos todos os dias (XIE et al., 2019). Grande parte desse comércio de hoje ainda é baseado em documentos em papel e esses processos desaceleram o comércio internacional gerando impacto significativo na economia.

A Figura 1 ilustra a complexidade da logística internacional, por meio de um exemplo do compartilhamento de informações necessárias no canal marítimo de Dubai. Assim que o importador e o exportador concordam com a forma de pagamento, o exportador fornece documento de conhecimento de embarque, fatura comercial original e certificado de origem. Poucos dias antes da chegada do embarque, o importador apresenta o documento de embarque ao agente marítimo, que entrega a ordem ao importador. O importador também deve enviar o pedido de declaração de importação à alfândega para iniciar o processo de liberação da remessa. Se a remessa for identificada como não arriscada, as cobranças serão realizadas e a liberação é emitida. Nas situações em que a remessa for declarada de risco, a declaração é analisada posteriormente. A saída deste processo de análise pode ser (1) sem uma inspeção, (2) com inspeção, (3) buscar informações adicionais de um cliente, ou (4) buscar opinião. A inspeção refere-se à exigência de inspeção física da remessa pelos despachantes aduaneiros. Buscar opinião se refere ao processo de envolvimento dos despachantes aduaneiros na investigação de diversos componentes da declaração, como avaliação da carga e tarifa (JUMA, 2019).

Figura 1. Cadeia de suprimentos no transporte marítimo.



Fonte: JUMA, 2019 , tradução e redesign feita pelos autores

Além das trocas de documentação entre os atores do canal marítimo, esse produto é transportado para seu destino, que pode não ser o final, implicando em maior complexidade na cadeia. Esses processos podem ser otimizados através do estabelecimento de um mecanismo seguro de compartilhamento de dados que garante a integridade das informações trocadas entre os participantes. Tal objetivo pode ser alcançado estabelecendo-se um mecanismo de compartilhamento de informações baseado em DLTs entre os envolvidos.

TECNOLOGIA DE REGISTRO DISTRIBUÍDO E A CADEIA DE SUPRIMENTOS

Em 2008, em uma lista de discussão de criptografia, surge a ideia por trás do Bitcoin e sua tecnologia adjacente à Blockchain. O Bitcoin é uma forma de dinheiro eletrônico capaz de realizar pagamentos *on-line* diretamente de pessoa para pessoa, sem controle central, de forma a transacionar valores sem intermediários, de maneira segura, controlado por algoritmos de consenso distribuídos entre nós de computação em redes (NAKAMOTO, 2008). A rede Blockchain é uma tecnologia de registro distribuído (em inglês, *Distributed Ledger Technologies — DLT*), que são conjuntos de dados distribuídos em vários locais, usando redes peer-to-peer, onde as alterações no *ledger* são refletidas na rede (WALPORT, 2016), através de um mecanismo de consenso, para que as informações replicadas não possam ser alteradas por um usuário ou um grupo de usuários (FLOREA, 2018).

Com o surgimento e a popularidade da criptomoedas, como o Bitcoin, a nova arquitetura de descentralização e as tecnologias de contabilidade distribuída do Blockchain atraíram atenções de vários campos, incluindo áreas não financeiras e IoT (LIN et al., 2019). A Blockchain têm despertado o interesse de governos, instituições financeiras, empresas de alta tecnologia, inclusive o mercado de capitais (YUAN; WANG, 2018). Trabalhos têm definido Blockchain como "uma tecnologia de transferência e armazenamento de dados transparente e segura que funciona sem um órgão de controle central" (LEE; PILKINGTON, 2017), no entanto o entendimento dos autores deste artigo essa definição pode ser mais abrangentemente relacionada a *Distributed Ledger Technology* que inclui o Tangle da IOTA. No paradigma da IoT, a tecnologia de contabilidade distribuída também pode ser considerada uma plataforma para fornecer um modelo seguro que deve ser capaz de possibilitar comunicações entre partes que não necessariamente precisam confiar uns nos outros (MONDRAGON, et al. 2018).

Na literatura encontramos diversos trabalhos voltados ao uso de DLTs para cadeia de suprimentos, esses trabalhos costumam apresentar como principais características a imutabilidade da informação e os contratos inteligentes em Blockchains (MONDRAGON, et al. 2018; IMERI; KHADRAOUI, 2018). O sistema de rastreabilidade baseado no Blockchain ganhou muita popularidade porque sua descentralização e prevenção de violação de dados podem fornecer soluções para as deficiências dos sistemas convencionais. Estas características são entendidas como potenciais para fazer registros efetivos do ciclo de vida dos produtos: histórico de fabricação, características dos transportes utilizados, tipo de manuseio e forma de armazenagem com seus respectivos registros de data e hora.

Já vimos que para as empresas, as informações do produto são muito úteis no gerenciamento da cadeia de suprimentos; mais informações sobre produtos

podem ajudar entidades (por exemplo, fornecedores, transportadores, distribuidores e varejistas) nas cadeias de suprimentos a prever tendências do mercado e tomar decisões de negócios. Portanto, o compartilhamento de dados é visto como um requisito importante no gerenciamento da cadeia de suprimentos. Outra justificativa para o uso da Blockchains para a cadeia de suprimento está na necessidade dos novos consumidores, pois estes estão exigindo mais informações sobre qualidade e segurança dos alimentos. Há um crescente interesse por informações sobre os produtos, como por exemplo, a localidade da produção, os processos, quais as matérias-primas e informações do revendedor. Com a prevalência da Internet e dos smartphones, os dias em que os consumidores sabiam pouco sobre um produto, exceto as notícias na televisão, se foram. Atualmente, os consumidores são incentivados e capazes de acessar qualquer informação que desejam sobre um produto, embora isso não seja tão conveniente. Segundo alguns autores, é essencial aumentar a transparência e a rastreabilidade da produção de alimentos junto com a cadeia de suprimentos. Seria muito mais eficaz se os consumidores pudessem adquirir facilmente qualquer informação relacionada aos alimentos agro-alimentares antes de comprar. (TSE, et al; 2017).

Por fim, na literatura encontram-se diversos trabalhos relacionados ao uso das DLTs para cadeia de suprimentos, no entanto, são poucas as informações referentes ao acompanhamento on-line dos dados de transporte de um determinado produto. Se estimam diversas perdas durante o transporte de cargas, principalmente cargas perecíveis, como frutas e carne. Um controle maior sobre o transporte dessas mercadorias habilitaria maior confiança entre quem produz e quem compra o produto, principalmente quando existe uma separação geográfica muito grande entre as partes, como é o caso de produtos exportados.

Apesar dos potenciais da Blockchain para resolver esses problemas, algumas limitações relativas ao design desses sistemas inviabilizam esse tipo de aplicação. Ao mesmo tempo que a imutabilidade e a descentralização seriam relevantes para o compartilhamento de dados de forma segura, transparente e imutável, os custos e tempos envolvidos dificultam sua implantação. Para que se possa compreender melhor essa situação, podemos usar uma Blockchain típica como exemplo, o protocolo do Bitcoin Core, que limita os blocos a 1 MB de tamanho. Cada bloco contém no máximo cerca de 4.000 transações (GÖBEL; KRZESINSKI, 2017). Os Blocos são adicionados ao Blockchain em média a cada 10 minutos, portanto a taxa de transação é limitada a cerca de 7 transações por segundo (GÖBEL; KRZESINSKI, 2017). Caso exista uma alta demanda por transações, estas podem demorar muito a entrarem na rede, dada a quantidade limitada de informações por bloco e o tempo médio de novas validações. Os mineradores (computadores participantes da rede Blockchain) fazem a validação de transações e gastam seu poder computacional para validar e guardar o histórico de transações, por isso recebem incentivos financeiros, via taxa, e em alguns casos criação de novas moedas. Portanto, a maioria dos sistemas de Blockchain possui taxas para recompensar mineradores pela verificação das transações (FLOREA, 2018). Esses incentivos são variáveis; com aumento da demanda, é necessário maior incentivo para favorecer uma transação perante outras (oferta e demanda), inviabilizando microtransações (MARINO; MOISO; PETRACCA, 2018). Por fim, pode-se dizer que o *design* dos atuais sistemas Blockchain não são adequados para trocar dados em tempo real.

CARACTERÍSTICAS DA TECNOLOGIA IOTA/TANGLE

IOTA é uma tecnologia de registro distribuído na forma de uma criptomoeda pública, de código livre (*open source*) que persegue o objetivo de se tornar o protocolo dos dispositivos IoT (POPOV, 2018; DIVYA; BIRADAR, 2018). Assim como o Bitcoin usam uma espécie de banco de dados DLT; com os recursos de imutabilidade, segurança, redundância, redução de custos e transparência. O Bitcoin/Blockchain usam os mineradores para validar as transações e conseqüentemente taxas a serem pagas para que se possa adicionar a transação no “banco de dados”. Este procedimento envolve longos tempos de aprovação e baixa escalabilidade.

O Tangle, não possui blocos, apenas transações que ocorrem em paralelo (umas às outras) e não há taxas para a validação de transações. Isto permite uma rápida inclusão das transações, o que torna o projeto muito mais adequado para ser usado em troca de dados (LAMTZIDIS; GIALELIS, 2018). Isso é possível porque todos os participantes da rede emitem e validam transações e são responsáveis pelo consenso, diferente da Blockchain, na IOTA não existem mineradores. (SARFRAZ, 2019). O custo de uma transação envolve apenas o custo computacional para validar outras duas transações, ou seja, não há taxa de transação, o que é criticamente importante para IoT (SILVANO; MARCELINO, 2020).

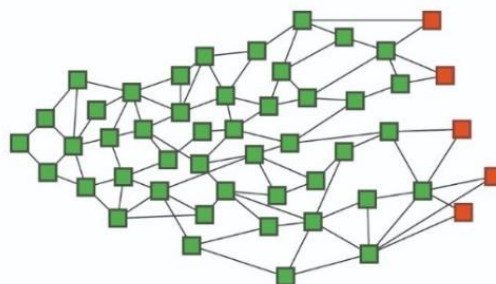
O Tangle da IOTA usa Grafos acíclicos dirigidos (em inglês: *Directed Acyclic Graph — DAG*), como estrutura de dados em que cada transação faz referência e aprova duas transações anteriores, este DAG é nomeado Tangle e cada nó do grafo é uma transação. A Figura 2 apresenta uma ilustração minimalista das arquiteturas Blockchain e Tangle.

Figura 2. Ilustração sintética da arquitetura da rede Blockchain e Tangle

a) Blockchain



b) Tangle (DAG)



Fonte: os autores

Os procedimentos para anexar uma transação ao Tangle ocorrem da seguinte maneira: (1) um nó escolhe duas outras transações para aprovar, de acordo com o “algoritmo de seleção de ponta” Markov Chain Monte Carlo (MCMC); (2) O nó verifica se as duas transações estão ou não em conflito, e não aprova transações conflitantes; (3) Para um nó emitir uma transação válida, ele deve resolver uma espécie de prova de trabalho (em inglês, *proof-of-work - PoW*), isto é conseguido encontrando um nonce, tal que o *hash* daquele nonce é concatenado com alguns

dados da transação aprovada (POPOV, 2018), (4) Depois disso, o usuário transmite o sua transação para rede, que vira uma “*tip*” (transação sem aprovação); (5) A “*tip*” aguarda aprovação; assim que tiver suas primeiras aprovações já está na rede.

Cada vez que um usuário transfere dados ou unidades monetárias (lotas), um novo endereço é gerado no qual as unidades restantes do usuário serão transferidas. Isso decorre do uso de um esquema de assinatura única do tipo Winternitz (W-OTS). Uma transferência é emitida através do estabelecimento de várias transações como parte de um pacote que indica o endereço de origem (entrada), o endereço do receptor (saída) e as transações que levam a assinatura da transação da entrada (meta-transação). Para criar um pacote válido, a soma do valor das transações de um pacote deve ser 0 (LAMTZIDIS; GIALELIS, 2018)

Como as transações ocorrem em paralelo, existe a possibilidade da transação ser “abandonada”, ou seja, não ficar permanentemente na rede. A atual definição de consenso de IOTA exige que uma transação confirmada seja referenciada (direta ou indiretamente) por uma transação assinada por um computador central, que é emitida a cada 10 segundos (IOTA, 2020); todas as transações aprovadas por ele são consideradas como 100% confiáveis (GAL, 2018), isso significa que os tempos de confirmação de um transação devem ficar em torno de 10 segundos, geralmente um pouco mais. Ao contrário das transações de valor, as transações de valor zero não requerem confirmação e são transmitidas entre os nós da rede imediatamente após serem emitidas. Como resultado, a camada de dados IOTA é completamente descentralizada e a existência do Coordenador não a afeta de forma alguma.

Como uma grande quantidade de dados pode ser enviada, a rede pode crescer muito rapidamente, especialmente por permitir transações com valor zero ou somente dados. Para isso existem os “*snapshots*” locais, eles apagam as transações, apenas os saldos permanecem (endereços com saldo da conta > 0), todo o resto é excluído (SØNSTEBØ, 2017). Os *snapshots* locais do Tangle ocorrem nos *Full nodes*, e podem ser realizados de forma manual ou totalmente automático. Entender isso é crucial para projetos que precisam preservar históricos de dados.

Uma aplicação frequente para IoT é a transmissão de dados de sensores. A IOTA permite o envio de transações sem a troca de valores, portanto um endereço pode ser utilizado para guardar dados de medição, no entanto, como as transações são públicas, é possível que um invasor interfira com spams. Outra questão relevante está na possibilidade de controlar acesso desses dados por outros usuários. O ‘Mensagens autenticadas mascaradas’ (em inglês, *Masked Authenticated Messaging — MAM*) foi desenvolvido para resolver essas questões. O MAM atua como um protocolo de comunicação de dados, criptografando e autenticando fluxos de dados; ele é um módulo que funciona junto com o protocolo IOTA e fornece funções para enviar e ler fluxos de mensagens usando o Tangle. A criptografia das mensagens é conhecida como “criptografia pós-quântica”, acredita-se que os algoritmos criptográficos pós-quânticos sejam seguros contra um ataque de computador quântico suficientemente forte. (BROGAN; BASKARAN; RAMACHANDRAN, 2018). A criptografia e o sistema de autenticação visam garantir que as mensagens não possam ser alteradas e que realmente partiram de um remetente específico. Como essas mensagens fazem parte do *ledger* distribuído, as transações contribuem para a segurança da rede,

aumentando o poder total de *hashing* e se beneficiando das propriedades de integridade de dados da rede, à medida que outras transações continuam a referenciá-las indiretamente (HANDY, 2017).

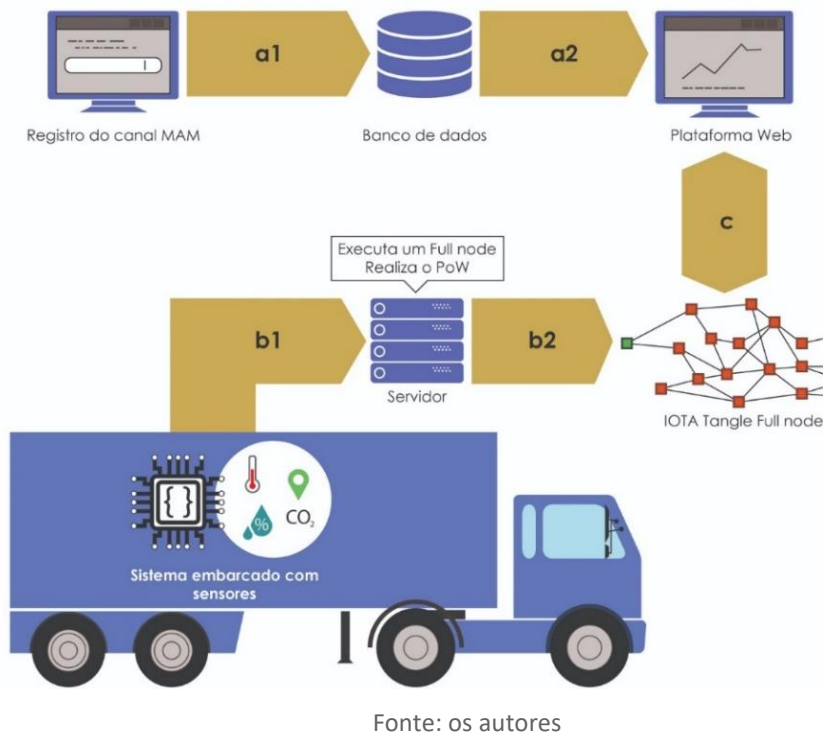
MODELO DE APLICAÇÃO: IOTA NO TRANSPORTE DE CARGAS

A IOTA torna possível enviar dados para a rede distribuída de forma barata e segura, devido à pequena prova de trabalho necessária para executar uma transação, proporcionando implantação em larga escala a custos acessíveis. Além disso, as aprovações têm baixa latência, pois não há necessidade de consenso imediato em todos os nós da rede, possibilitando as primeiras aprovações e o acompanhamento mais próximo da realidade do produto e da inviolabilidade dos dados coletados e armazenados. A criptografia MAM é outro forte atrativo dessa tecnologia, garantindo mais segurança para fluxos de dados.

Com IOTA a rastreabilidade do produto pode ir para além do registro estático, ou dependente de um sistema de RFID, as informações do produto dentro de um sistema de transporte podem ser visualizadas em tempo quase real, mantendo as características de um DLT como a imutabilidade da informação e descentralização dos dados. Um bom exemplo de aplicação dessa tecnologia para a cadeia de suprimentos, é a aplicação deste ao acompanhamento de situação de uma determinada carga durante seu transporte.

Como já dito, as informações compartilhadas entre as partes envolvidas são a espinha dorsal de uma operação correta do transporte. E a IOTA pode habilitar isso. Informações relacionadas aos produtos, data, hora e situação da carga em cada momento podem ser obtidas e validadas por meio do Tangle. Um sistema de transporte (caminhão, contêiner..) carregando carne, frutas ou qualquer outro alimento que exija controle pode ser acompanhado por meio de um sistema embarcado com sensores; os dados são coletados e publicados no Tangle com uma frequência definida. A conectividade desses dispositivos com a IOTA, pode ser feita, por exemplo, via rede celular (2G, 3G, 4G, 5G), que por sua vez envia para um servidor que realiza a prova de trabalho necessária para anexar as informações no IOTA/Tangle, enviando os dados para o *Full node* IOTA. A Figura 3 ilustra o modelo proposto.

Figura 3. Modelo de aplicação para acompanhamento de cargas em movimento utilizando IOTA



Detalhes do modelo proposto:

Detalhes do modelo proposto:

a1) Registo do canal IOTA dos sensores no sistema da Web;

a2) Registo de canal no banco de dados;

b1) Os sensores coletam dados do ambiente (temperatura, umidade, CO₂, O₂, geolocalização...) e são enviados via rede rede celular para um servidor que roda um *Full node* IOTA;

b3) Os dados são enviados para a rede Tangle (*Full node*) e posteriormente replicados na rede;

c) Um *Front-end Web*, apresenta os dados e verifica se há informações atípicas, em caso positivo informar às partes interessadas, caso contrário, apenas mostram os dados;

Provedores de nó completo públicos podem ficar sobrecarregados com solicitações de transações, por isso rodar um *Full node* no servidor, garante um ponto de entrada seguro para os dados no Tangle, especialmente se as transações forem ativamente geradas por meio dele. O modelo apresentado permite que vários sistemas de transporte sejam acompanhados utilizando um único servidor, otimizando recursos. Além disso, a prova de trabalho é terceirizada para o servidor, diminuindo o poder computacional e espaço em disco do sistema embarcado, crucial em sistemas IoT.

O principal diferencial do modelo apresentado é a transparência dos dados e imutabilidade da informação; devido à descentralização conseguida com IOTA. Todos os dados são facilmente auditados por qualquer ator da cadeia de

suprimentos. A tecnologia habilita maior confiança entre fabricante, transportadoras, vendedor e usuário final. As perdas podem ser evitadas com controle real da situação da carga. Sensores podem indicar em qual momento o sistema foi inadequadamente ou corretamente transportado.

Os custos do modelo proposto estão ligados ao poder computacional para realizar o *PoW*, *hardware*, sensores, e plano de conectividade com a internet. Para garantir o histórico dos dados válidos por um longo período, é relevante para gestão da cadeia de suprimentos, discutir a necessidade de guardar os dados por um longo prazo, tendo em vista que na IOTA ocorrem os "*snapshots*", manter um IOTA *Full node* garante que os dados não serão apagados sem conhecimento prévio. No entanto, o que será feito com as transações antigas, após o "*snapshot*"? Uma opção é guardar transações antigas apenas para conferências futuras em bancos de dados ou em uma Blockchain. Para que isso não se torne um fator limitador da tecnologia é relevante que o tempo entre os "*snapshot*" seja bem discutido. Esse tempo deve levar em consideração o período de uso mais comum do dado e a capacidade de armazenagem disponível.

CONSIDERAÇÕES FINAIS

A disponibilidade de novas DLTs, como da IOTA, pode dar suporte a um setor dominado por um grande volume de transações advindas de dispositivos IoT. O design das tecnologias Blockchain não foi desenvolvido para lidar com essas necessidades, pois possuem dificuldades intrínsecas de oferecer suporte ao grande volume de transações com baixo custo para o comércio global da cadeia de suprimentos. Tudo indica que o *design* da IOTA/Tangle é adequado para este domínio, pois permite que transações de valor zero possam ser usadas, sem taxas adicionais e essas mesmas transações ajudam a proteger a integridade da rede.

Foi apresentado um modelo da tecnologia IOTA/Tangle como parte de uma solução segura e imutável para acompanhamento de cargas perecíveis, em movimento. As características propostas abrem horizontes para o uso do *Ledger* distribuído na cadeia de suprimentos. Com esse modelo em funcionamento, relatório da situação real da carga pode ser compartilhado com os atores envolvidos, o que evitaria os serviços semi-digitais utilizados hoje em dia, evitando erros humanos e prejuízos durante o transporte.

A IOTA/Tangle pode ser uma das tecnologias responsáveis por uma nova visão de gestão na cadeia de suprimentos a nível global, oferecendo maior confiança, segurança, e com menos perdas de produtos e informações. Como trabalhos futuros, os autores do artigo pretendem desenvolver uma prova de conceito a partir do exposto neste documento para identificar novos desafios e validar o modelo proposto.

Blockchain technology - IOTA applied to product traceability

ABSTRACT

Current information exchange techniques during the transportation of products in the supply chain cause delays and human errors. Computational solutions usually involve centralized databases hosted by one of the stakeholders. This context arouses interest in decentralized, reliable, and secure solutions such as Blockchain technology. The objective of this work is to investigate the challenges and possibilities of tracking product information during the transportation process using the distributed *ledger* of IOTA. It was found that there are limitations in the current Blockchain systems aimed at product traceability, so it was proposed a model that combines IOTA with IoT devices to monitor the status of products. Based on the proposed model, it was identified that technology can enable greater trust between the actors in the supply chain and be part of new solutions that avoid losses and human errors during transport.

KEYWORDS: Blockchain. Iota. Tangle. Supply chain. traceability.

AGRADECIMENTOS

Agradecimentos ao ilustrador Eduardo Eising, responsável pela elaboração das figuras. Agradecimentos à FAPESC, pelo auxílio financeiro de apoio a pesquisa de mestrado realizada no laboratório de pesquisa aplicada (LPA). Edital CP FAPESC Nº 05/2019 - Programa FAPESC/CAPES de Recursos humanos em CTI Bolsa de Mestrado – (SGPE – FAPESC - 00347/2020)

REFERÊNCIAS

AGOSTINHO, Carlos et al. Towards a sustainable interoperability in networked enterprise information systems: trends of knowledge and model-driven technology. **Computers in Industry**, v. 79, p. 64-76, 2016.

CHRISTOPHER, Martin. Logistics & supply chain management. **Pearson education limited**, 2011.

DIVYA, M.; BIRADAR, Nagaveni B. IOTA-next generation block chain. **International Journal Of Engineering And Computer Science**, v. 7, n. 04, p. 23823-23826, 2018.

GAL, Allon. The tangle: an illustrated introduction. **Iota Blog**, 31/01/2018. Disponível em: <<https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4>>. Acesso em: 24/04/2020.

GÖBEL, Johannes; KRZESINSKI, Anthony E. Increased block size and Bitcoin blockchain dynamics. In: **2017 27th International Telecommunication Networks and Applications Conference (ITNAC)**. IEEE, 2017. p. 1-6.

IMERI, Adnan; KHADRAOUI, Djamel. The security and traceability of shared information in the process of transportation of dangerous goods. In: **2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)**. IEEE, 2018. p. 1-5.

IOTA Foundation. Chrysalis (IOTA 1.5) Phase 1 Now Live on Mainnet. 30/04/2018. Disponível em: <<https://blog.iota.org/chrysalis-iota-1-5-phase-1-now-live-on-mainnet-958ec4a4a415>> Acesso em: 19/08/2020.

JUMA, Hussam; SHAALAN, Khaled; KAMEL, Ibrahim. A survey on using blockchain in trade supply chain solutions. **IEEE Access**, v. 7, p. 184115-184132, 2019.

LAMTZIDIS, Odysseas and GIALELIS, John. An IOTA Based Distributed Sensor Node System. **2018 IEEE Globecom Workshops (GC Wkshps)**, Abu Dhabi, United Arab Emirates, 2018, pp. 1-6.

LEE, Jong-Hyouk; PILKINGTON, Marc. How the blockchain revolution will reshape the consumer electronics industry [future directions]. **IEEE Consumer Electronics Magazine**, v. 6, n. 3, p. 19-23, 2017.

LIN, Qijun et al. Food safety traceability system based on blockchain and epcis. **IEEE Access**, v. 7, p. 20698-20707, 2019.

LUND-NIELSEN, Jens . The challenges facing today's supply chains. **Iota Blog**, 20/12/2018. Disponível em: < <https://blog.iota.org/the-challenges-facing-todays-supply-chains-aaa9d3d9fc6d>> Acesso em: 12/07/2020.

MARINO, Francesco; MOISO, Corrado; PETRACCA, Matteo. Automatic contract negotiation, service discovery and mutual authentication solutions: A survey on the enabling technologies of the forthcoming IoT ecosystems. **Computer Networks**, 2018.

MONDRAGON, Adrian E. Coronado; MONDRAGON, Christian E. Coronado; CORONADO, Etienne S. Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry. In: **2018 IEEE International Conference on Applied System Invention (ICASI)**. IEEE, 2018. p. 1300-1303.

NAKAMOTO, Satoshi et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

KIEL, Daniel; ARNOLD, Christian; VOIGT, Kai-Ingo. The influence of the Industrial Internet of Things on business models of established manufacturing companies—A business level perspective. **Technovation**, v. 68, p. 4-19, 2017.

YUAN, Yong; WANG, Fei-Yue. Blockchain and cryptocurrencies: Model, techniques, and applications. **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, v. 48, n. 9, p. 1421-1428, 2018.

STRUGAR, Dragos et al. On M2M micropayments: a case study of electric autonomous vehicles. **2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)**. IEEE, 2018. p. 1697-1700

SØNSTEBØ, D. Iota development roadmap. **Iota Blog**, 31/03/2017. Disponível em: <<https://blog.iota.org/iota-development-roadmap-74741f37ed01>> Acesso em: 22/04/2020.

POPOV, Serguei. The tangle. **IOTA.org**. 30/04/2018. Disponível em: <<https://www.iota.org/research/academic-papers>> Acesso em: 22/04/2020.

FLOREA, Bogdan Cristian. Blockchain and Internet of Things data provider for smart applications. **2018 7th Mediterranean Conference on Embedded Computing (MECO)**. IEEE, 2018. p. 1-4.

SILVANO, Wellington Fernandes; MARCELINO, Roderval. Iota Tangle: A cryptocurrency to communicate Internet of Things data. **Future Generation Computer Systems**, v. 112, p. 307-319, 2020.

SLUIJS, C. Antwerp Start-up T-Mining Develops Blockchain Solution for Safe, Efficient Container Release. **t-mining**. 28/06/2017. Disponível em: <<https://t-mining.be/news1/2018/1/4/secure-container-release>> Acesso em: 24/04/2020.

TSE, Daniel et al. Blockchain application in food supply information security. In: **2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)**. IEEE, 2017. p. 1357-1361

WALPORT, MGCSA et al. Distributed ledger technology: Beyond blockchain. **UK Government Office for Science**, v. 1, 2016

WANG, J.; WU, P.; WANG, X.; SHOU, W. "The outlook of blockchain technology for construction engineering management." **Frontiers of engineering management** 4, no. 1, 2017

XIE, Junfeng et al. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. **IEEE Communications Surveys & Tutorials**, 2019.

YEOW, Kimchai et al. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. **IEEE Access**, v. 6, p. 1513-1524, 2017.

Recebido: 26/04/2020

Aprovado: 18/09/2020

DOI: 10.3895/rts.v17n46.12091

Como citar: SILVANO, W.F.; MARCELINO, R.; VIGIL, M.A.G. Tecnologia blockchain - IOTA aplicada a rastreabilidade de produtos. **Rev. Technol. Soc.**, Curitiba, v. 17, n. 46, p. 201-215, jan./mar., 2021. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/12091>. Acesso em: XXX.

Correspondência:

Direito autoral: Este artigo está licenciado sob os termos da Licença Creative Commons-Atribuição 4.0 Internacional.

