Blockchain and Tangle: The Transaction Security in the IoT Ecosystem

Guilherme Gouveia Martinez
Centro de Matemática, Computação e Cognição
Universidade Federal do ABC (UFABC)
Santo André, São Paulo, Brasil
martinez.guilherme@outlook.com.br

Carlo Kleber da Silva Rodrigues
Centro de Matemática, Computação e Cognição
Universidade Federal do ABC (UFABC)
Santo André, São Paulo, Brasil
carlo.kleber@ufabc.edu.br

ABSTRACT

This article examines the level of security ensured by Blockchain and Tangle technologies when performing transactions in the IoT ecosystem, especially considering the information integrity. To this end, analytical models and simulations are employed to investigate fraud scenarios in which an attacker attempts to modify transactions already recorded in the databases. The results suggest that Tangle technology is much more promising, as it proves to be more competitive in scenarios where potential attackers have outstanding computational processing power. In addition, Tangle technology can deliver scalability that is not observed in the Blockchain technology. In this context, the main contribution of this article is to provide subsidies for the development of real application projects for the IoT ecosystem. General conclusions and future work close this article.

CCS Concepts

•Security and privacy → Network security; Database and storage security; •Networks → *Network algorithms;*

Keywords

Blockchain; Tangle; Internet of Things; Security

1. INTRODUÇÃO

O ecossistema Internet das Coisas (do inglês, *Internet of Things* – IoT) contempla uma abrangente e complexa infraestrutura (lógica e física) de comunicação para diversos objetos inteligentes, como sensores, *notebooks*, geladeiras, sinais de trânsito, TVs, veículos, dentre outros [2, 24].

Esse ecossistema permite a implementação de serviços em distintos domínios de aplicação como, e.g., casas inteligentes, redes elétricas autônomas, contratos inteligentes, gestão de saúde, redes de transporte, redes de vigilância e processos de logística [27, 17].

Ante esse cenário, que envolve a disseminação de informações sensíveis originadas pelas transações entre os objetos, surgem preocupações quanto à segurança das informações, em face de questões relacionadas à confidencialidade, integridade e disponibilidade [6, 12]. Para lidar com essas preocupações, tem sido admitida a implementação da base de dados do ecossistema por meio de tecnologias de registros distribuídos (do inglês, *Distributed Ledger Technologies* - DLTs) [34, 33, 6].

Sob o conceito geral de DLT, a base de dados é construída, mantida e replicada por nós processadores geograficamente distribuídos, interligados segundo uma rede de arquitetura lógica *peer-to-peer* (P2P). Os dados constitutivos dessa base de dados se referem às transações (ou informações resultantes das transações) realizadas pelos objetos inteligentes do ecossistema [6].

De forma independente, cada nó processador realiza alterações na sua réplica local da base de dados, alcançando suas próprias conclusões. Essas alterações locais são então enviadas em *broadcast* pela rede de comunicação para que os demais nós processadores façam a devida verificação. As alterações locais somente são aceitas no ecossistema quando há um consenso entre a maioria dos nós processadores, ou seja, quando há uma convergência sistêmica [33, 6].

Dentre as DLTs existentes, podem-se destacar as tecnologias *Blockchain* [25] e *Tangle* [22] como as promissoras, pois já possuem significativa maturidade tecnológica e são de ampla aceitação e discussão na indústria e na recente literatura acadêmica [13, 20, 30].

A tecnologia *Blockchain* se baseia na construção de uma lista encadeada de blocos de transações, constituindo a base de dados. Os blocos são adicionados conforme são validados. Cada bloco pode conter dezenas de transações e se liga a um único bloco anterior. Sob o aspecto lógico, o nó processador e o cliente são entidades distintas, embora possam ser a mesma máquina física [25, 1, 3].

A tecnologia *Tangle*, por sua vez, se baseia na implementação de um grafo acíclico direcionado (do inglês, *Directed Acyclic Graph* - DAG). Esse DAG constitui a base de dados. Cada vértice do DAG armazena uma única transação e se liga a dois outros vértices anteriores [22]. Adicionar um vértice ao DAG equivale a adicionar uma transação ao DAG. Para que uma transação seja adicionada ao DAG, é necessário que duas outras transações pré-existentes sejam validadas. Todo cliente é um nó processador e vice-versa.

Este contexto de discussão é a motivação para este artigo, cujo objetivo é analisar o nível de segurança garantido

pelas tecnologias *Blockchain* e *Tangle* para as transações realizadas no ecossistema IoT, especialmente no tocante à integridade dos dados. Para tanto, por meio de modelagem analítica e simulações, são realizados experimentos para estimar a probabilidade de fraude, caracterizada pela ação de um atacante que tenciona alterar transações já registradas na base de dados do ecossistema, comprometendo a integridade das informações.

Ante o objetivo anunciado, este artigo provê então uma valiosa contribuição para a literatura especializada, pois relevantes subsídios teóricos e experimentais são ofertados para o possível desenvolvimento de projetos reais de aplicações para o ecossistema IoT.

A organização do restante deste artigo é descrita a seguir. A Seção 2 revisa as tecnologias *Blockchain* e *Tangle*, bem como a aplicabilidade das mesmas no ecossistema IoT. Os trabalhos relacionados estão na Seção 3. A Seção 4 realiza a análise de segurança das DLTs mencionadas, contemplando experimentos, resultados e discussões. Por fim, conclusões gerais e trabalhos futuros constituem a Seção 5.

2. REFERENCIAL TEÓRICO

2.1 Tecnologia Blockchain

Sob a tecnologia *Blockchain*, os nós processadores da rede P2P são chamados de mineradores. Como mencionado, esses nós são os responsáveis por construir, manter e replicar a base de dados, que é uma lista encadeada de blocos de transações.

Para adicionar um bloco à lista encadeada, o minerador deve encontrar a prova de trabalho (do inglês, *proof-of-work*) para o bloco. Isso significa determinar, por meio de tentativas sucessivas, um valor de *nonce* que solucione um desafio matemático, baseado na função *hash* criptográfica SHA-256 [15]. Esse desafio matemático envolve os cabeçalhos de identificação do próprio bloco e de seu antecessor, respectivamente. Esses cabeçalhos permitem estabelecer a ligação lógica entre os blocos [4].

O processo de resolução descrito é denominado mineração. Cada vez que um bloco é minerado, o respectivo minerador recebe uma recompensa. Essa recompensa existe com a finalidade de incentivar a execução do processo de mineração de forma ininterrupta e por um tempo indefinido [4].

Ao alterar um bloco da lista encadeada, tem-se a mudança de seu cabeçalho e a necessidade de refazer a sua mineração. Todavia, como mencionado, cada bloco é ligado ao seu antecessor por meio de *hash* criptográfico, que envolve os cabeçalhos do próprio bloco e de seu antecessor. A alteração de um bloco implica então a alteração de todos os blocos subsequentes a ele na lista encadeada. Quantos mais blocos posteriores houver, mais difícil se torna então a alteração da informação já registrada [29, 24].

2.2 Tecnologia Tangle

Como mencionado, a tecnologia *Tangle* utiliza a estrutura DAG para implementar a base de dados. Ademais, cada vértice do DAG armazena uma única transação e está ligado a dois outros vértices anteriores [22]. Não há recompensa para o trabalho de validação de transações, e os próprios clientes atuam como nós processadores da rede P2P.

Para submeter uma transação, um cliente deve validar duas outras transações pré-existentes no DAG, i.e., dois outros vértices pré-existentes. Validar significa realizar uma prova de trabalho, de maneira semelhante ao que ocorre em *Blockchain*. A função *hash* criptográfica é a Keccak-384 [7], conhecida como SHA-3 [5].

Graficamente, a validação é representada por arestas direcionadas que partem da transação a ser adicionada para duas transações pré-existentes no DAG. A confiabilidade quanto à validade de uma transação se dá em função do número de validações que ela possui: quanto maior é o número de validações que ela possui, maior é a sua confiabilidade. Ressalta-se, porém, que a contagem do número de validações que uma transação possui não considera apenas as validações ocorridas de forma direta, conforme explicado a seguir.

Uma transação T_{xa} pode estar validada tanto direta quanto indiretamente por uma transação T_{xb}. Quando uma transação T_{xb} valida a transação T_{xa} por meio de uma aresta direta (i.e., a aresta liga T_{xb} a T_{xa}), dizemos que a T_{xa} é validada diretamente por T_{xb}. Por outro lado, quando uma transação T_{xb} valida diretamente uma T_{xc} que, por sua vez, valida diretamente uma T_{xa}, dizemos então que T_{xa} é validada indiretamente pela transação T_{xb}, pois há um caminho direcionado da transação T_{xb} até a transação T_{xa} [22].

2.3 IoT e DLTs

Considerando uma visão *top-down*, a arquitetura do ecossistema IoT pode ser dividida nas seguintes cinco camadas hierarquizadas [21, 11, 12]:

1. Camada de Negócio: considera a gerência do ecossistema IoT, contemplando os correspondentes modelos de negócios e de lucro. É importante ressaltar que o sucesso de uma tecnologia não depende apenas da importância da tecnologia, mas também da inovação trazida para a sociedade e dos modelos de negócio e de lucro propostos para a sua implementação;

2. Camada de Aplicação: sua tarefa é baseada nos dados vindos na camada de processamento, abrangendo as diversas aplicações desenvolvidas para o ecossistema IoT como, e.g., transporte inteligente, gerenciamento de logística, autenticação de identidade, serviços baseados em localização e serviços de vigilância;

3. Camada de processamento: armazena, analisa e processa informações provenientes da camada de transporte. As principais técnicas de processamento incluem, e.g., banco de dados complexos, processamento inteligente, computação em nuvem, computação ubíqua e pervasiva, e computação em névoa;

4. Camada de transporte: é também chamada de camada de rede, sendo responsável pela transmissão dos dados, oriundos da camada de percepção, para o centro de processamento por meio de variados tipos de rede (e.g., redes cabeadas, redes sem fio, redes móveis, etc.). As principais tecnologias de comunicação nesta camada incluem: FTTx, 5G, Wi-Fi, Bluetooth, ZigBee, UMB, infravermelho, dentre outras. Como protocolo de endereçamento dos objetos, tem-se, e.g., o conhecido IPv6;

5. Camada de percepção: a principal tarefa desta camada é coletar propriedades físicas, e.g., temperatura, hora e localização, usando sensores, e.g., infravermelho, RFID e código de barras, e convertê-las em sinais digitais para transmissão pela rede de comunicação.

O emprego de DLTs no ecossistema IoT é motivado especialmente pela segurança sistêmica a ser provida, considerando os requisitos de confidencialidade, integridade e disponibilidade [6, 32], definidos a seguir.

A confidencialidade abrange dois conceitos relacionados: a confidencialidade de dados e a privacidade. O primeiro conceito se refere à garantia de que informações privadas ou confidenciais não fiquem disponíveis nem sejam reveladas a indivíduos não autorizados. O foco neste caso são os dados. O segundo conceito é a garantia de que indivíduos controlem ou influenciem quais informações sobre eles podem ser coletadas e armazenadas, e por quem e para quem tais informações podem ser reveladas. Neste caso, o foco são os indivíduos.

A integridade também abrange dois conceitos relacionados: a integridade de dados e a integridade de sistemas. O primeiro conceito tem a ver com a garantia de que informações e programas sejam alterados somente de maneira específica e autorizada. O foco são os dados. O segundo conceito se relaciona à garantia de que um sistema desempenhe sua função pretendida de maneira incólume, livre de manipulação não autorizada, seja esta deliberada ou inadvertida. O foco passa a ser o sistema. Nesse sentido, é fulcral então defender-se contra a modificação ou destruição imprópria de informações, auxiliando na garantia da irretratabilidade (ou não repúdio) e da autenticidade das informações.

Por sua vez, o conceito de disponibilidade se refere à garantia de que os sistemas funcionem prontamente e que não haja a negação de serviço a indivíduos autorizados. A informação ou sistema deve estar disponível no momento em que for necessário. É preciso assegurar que o acesso e o uso das informações sejam confiáveis e realizados no tempo adequado. Uma perda de disponibilidade consiste na disrupção do acesso ou da utilização de informações ou de um sistema de informação. Neste caso, o foco é o sistema computacional.

Para terminar esta seção, é importante ressaltar que este trabalho de pesquisa analisa as DLTs *Blockchain* e *Tangle* visando à garantia de integridade das transações executadas no ecossistema IoT, em especial com foco na Camada 3. Discussões sobre confidencialidade e disponibilidade, bem como sobre as Camadas 1, 2, 4 e 5 são deliberadamente deixadas para trabalhos futuros.

3. TRABALHOS RELACIONADOS

Considerando uma citação preferencialmente cronológica, esta seção discorre sobre alguns dos mais importantes e recentes trabalhos da literatura que se relacionam ou contribuem, direta ou indiretamente, para o objetivo deste artigo de pesquisa.

Os trabalhos de Nakamoto [25] e Popov [22] podem ser considerados como seminais para a adequada compreensão das tecnologias *Blockchain* e *Tangle*. Cada um desses trabalhos retrata a filosofia e o mecanismo geral da operação da respectiva tecnologia, contemplando detalhes do processamento das transações no sistema, indo desde a etapa de validação até a etapa de aceitação na base de dados. Em especial, por meio de modelos matemáticos, são ainda analisadas as formas de ataque que a respectiva base de dados pode sofrer, o que permite estimar o nível de segurança ofertado.

Kokoris-Kogias et al. [19] apresentam o *framework* de gerenciamento de dados Calypso, o qual aplica-se ao ecossistema IoT associado com a tecnologia *Blockchain*. A base de dados é auditável e objetiva-se precipuamente descentralizar o compartilhamento e o gerenciamento do ciclo de vida de dados privados, além de promover a divulgação atômica e justa dos mesmos com a devida segurança. Os resultados dos experimentos, realizados por meio de *benchmarks*, simulações e medições em redes reais, mostram, todavia, alguma limitação de desempenho em face de grandes volumes de dados.

Truong et al. [28] também propõem um *framework*, o qual associa o ecossistema IoT com a *Blockchain*. Este *framework* é nomeado Sash. A base de dados é usada especialmente para armazenar políticas de controle de acesso, cujas alterações são auditáveis publicamente. Adicionalmente, os autores tratam sobre a remuneração do trabalho dos nós processadores e a minimização do *overhead* devido à distribuição de chaves criptográficas, que diretamente impactam a segurança sistêmica. Os experimentos de avaliação baseiam-se em prototipagem usando a plataforma FIWARE e a estrutura Hyperledger Fabric. Ainda que restritos aos cenários investigados, os resultados mostram um desempenho satisfatório do sistema prototipado.

Os trabalhos de Alaba et al. [12] e Minoli e Occhiogrosso [6] se revelam valiosos por realizar uma dissecção completa dos domínios e respectivas aplicações do ecossistema IoT, considerando mais especialmente o aspecto da segurança. Os conceitos de disponibilidade, integridade e confidencialidade são debatidos visando à implementação de aplicações no ecossistema IoT. De certa forma, estes dois trabalhos se complementam, pois o primeiro se detém à IoT, enquanto que o segundo discute IoT combinado com a *Blockchain*. Embora não apresentem resultados experimentais próprios, o caráter descritivo faz dos mesmos importantes referências para o projeto de aplicações no ecossistema IoT.

Os trabalhos de Dorri et al. [9], Dorri et al. [8], Florea [13], e, ainda, Hang e Kim [16] constituem quatro propostas de soluções específicas de segurança para aplicações do ecossistema IoT, como brevemente comentado a seguir.

Dorri et al. [9] propõem um método para utilizar a tecnologia *Blockchain* no contexto de casas inteligentes visando à segurança e à privacidade das informações transmitidas. Por sua vez, Dorri et al. [8] propõem um algoritmo de consenso temporal que consegue, de forma segura, otimizar o tempo de realização da prova de trabalho e a capacidade do sistema em processar transações.

Florea [13] apresenta um método, baseado em prova de conceito, que possibilita de forma segura gerenciar dados de sensores remotos por meio de armazenamento distribuído, implementado com a tecnologia *Tangle*. Por último, Hang e Kim [16] buscam solucionar problemas que arquiteturas centralizadas IoT têm em comum: ataques cibernéticos e ponto central de falha. É apresentada uma plataforma integrada IoT usando a tecnologia *Blockchain* para garantir a integridade dos dados. Deseja-se especialmente oferecer ao proprietário do objeto inteligente uma aplicação que forneça um registro abrangente e imutável, além de permitir fácil acesso em diferentes domínios.

Para encerrar esta citação de trabalhos relacionados, menciona-se o artigo de Mata e Rodrigues [23]. Os autores realizam uma análise competitiva entre as tecnologias *Blockchain* e *Tangle* com foco em aplicações IoT. Os cenários examinados são, todavia, restritos e apenas simulações são consideradas. Os resultados obtidos sugerem a maior atratividade da tecnologia *Tangle*, particularmente pelo fato desta neces-

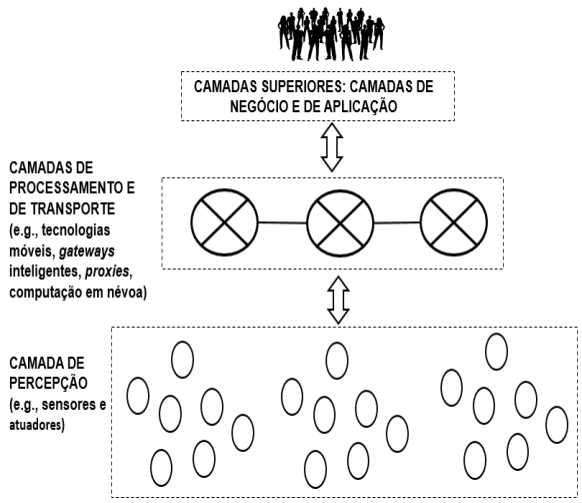

Figure 1: Cenário de aplicação genérica.

sitar de ajustes de configuração sistêmica mais simples para alcançar um satisfatório nível de segurança.

Ante o exposto, a diferenciação e o ineditismo deste artigo se revelam pelo emprego conjunto de modelagem analítica e simulações para mensurar o nível de segurança garantido pelas tecnologias *Blockchain* e *Tangle* quando da execução de transações no ecossistema IoT, considerando especialmente à integridade da informação.

4. AVALIAÇÃO DE PERFORMANCE

Esta seção análisa competitivamente as tecnologias *Blockchain* e *Tangle* visando à integridade das informações armazenadas. Para tanto, modela-se um cenário em que há a ocorrência de uma fraude no sistema e, então, estima-se a probabilidade de sucesso dessa fraude.

A fraude considerada na modelagem analítica (Subseção 4.1) e na simulação (Subseção 4.2) têm por base a mesma abstração vista na Figura 1, que retrata o cenário de uma aplicação genérica executada no ecossistema IoT, como explicado a seguir.

Os elementos da camada de percepção coletam informações do meio ao qual se encontram fisicamente conectados ou integrados. Por exemplo, o elemento individualmente pode ser uma geladeira inteligente, capaz de detectar a falta de um item de consumo em uma residência, ou pode ser um piezômetro, capaz de detectar o atingimento de um nível de segurança em uma barragem. As informações coletadas são então enviadas pela camada de transporte (e.g., empregando tecnologias móveis) para a camada de processamento.

Na camada de processamento se encontra a base de dados do ecossistema IoT, que neste caso é uma lista encadeada (para *Blockchain*) ou um DAG (para *Tangle*). É nesta camada que a base de dados é construída, mantida e replicada pelos nós processadores que, nesta abstração, são constituídos por *proxies* (ou *gateways*) inteligentes, estando geograficamente distribuídos e interligados segundo uma arquitetura lógica P2P.

A partir das réplicas das bases de dados, as camadas superiores executam ações por meio de processos definidos. Por exemplo, considerando a geladeira inteligente, a ação poderia ser a compra do suprimento faltante ou, considerando a barragem monitorada pelo piezômetro, a ação poderia ser o acionamento de um sistema de alarme para evacuação da população de uma determinada área.

A seguir são então detalhados os cenários específicos de fraude para cada uma das tecnologias em análise.

4.1 Modelagem Analítica

4.1.1 Cenário de Fraude sob Blockchain

Um fraudador deseja substituir um bloco legítimo que foi adicionado à lista encadeada por um minerador honesto. Este bloco legítimo contém a transação honesta que o fraudador deseja substituir. Para tanto, o minerador desonesto (e.g., um fraudador) enviará uma versão fraudulenta do bloco legítimo que, no lugar da transação honesta, conterá uma transação fraudulenta. Dessa forma, haverá duas versões para o mesmo bloco, o que resultará em uma bifurcação (i.e., duas ramificações) na lista encadeada: uma ramificação para o bloco honesto e outra para o bloco fraudulento.

Nessa situação, em que há duas versões distintas para o mesmo bloco, a rede considera a chamada Regra da Cadeia mais Longa (do inglês, *Longest Chain Rule* - LCR) [31]. A seleção entre as duas ramificações ocorre quando as próximas provas de trabalho são encontradas, fazendo com que uma das ramificações eventualmente se torne mais longa que a outra. A ramificação mais curta é desprezada, e a transação a ser aceita como válida é aquela que pertence à ramificação mais longa.

Dessa forma, inicia-se uma competição entre o minerador honesto e o minerador fraudador para conseguir ter a cadeia mais longa. Como estratégia, o fraudador espera um certo tempo π após a inserção da transação honesta, na expectativa de que esta já tenha sido aceita no ecossistema por parte dos nós processadores.

Após esse tempo π, considere que z blocos tenham sido adicionados à lista encadeada. Neste instante, o fraudador insere o bloco fraudulento. Isso significa que ele terá então que compensar a desvantagem inicial de z blocos, para então poder tornar sua ramificação mais longa que a ramificação contendo a transação honesta [23, 25].

A probabilidade de que a ramificação do fraudador venha a compensar a desvantagem inicial de z blocos, com relação à ramificação honesta, é modelada a partir de uma distribuição de Poisson, sendo calculada pela Equação 1, apresentada a seguir [25]. Essa formulação implicitamente considera que, durante o tempo de espera π, o minerador fraudador realizou a mineração de k blocos de maneira secreta, ou seja, sem que o sistema tomasse conhecimento. Veja que, nesse caso, a vantagem do minerador honesto em relação ao minerador desonesto é, na verdade, de $(z-k)$ blocos.

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}(1-(q/p)^{z-k}) \quad (1)$$

Onde: os parâmetros p e q representam a probabilidade de que o minerador honesto e o minerador fraudador venham a minerar o próximo bloco, respectivamente; z é o número de blocos minerados pelo minerador honesto após a inserção do bloco contendo a transação honesta, após decorrido o tempo π; e λ é a taxa média do processo de Poisson, sendo dada por $(z.q)/p$.

4.1.2 Cenário de Fraude sob Tangle

Para a tecnologia *Tangle*, como no cenário anterior, um minerador desonesto introduz uma transação fraudulenta após um certo tempo π, decorrido após a inserção de uma transação honesta. Note que, sob *Tangle*, a transação honesta deve validar duas outras transações do ecossistema IoT.

Como estratégia de fraude, a transação fraudulenta valida outra transação mais antiga que aquelas duas que foram selecionadas pela transação honesta. A partir daí, o fraudador deve inserir novas transações que validem a transação fraudulenta, de forma que o número de validações acumuladas ao fim de um certo tempo Δt, decorrido após o tempo π, seja superior ao número acumulado de validações recebido pela transação honesta. Dessa forma, é originada uma espécie de ramo ou ramificação (do inglês, *branch*) a partir da transação fraudulenta, o qual é denominado de ramo parasita [14].

Ante uma visão topológica do correspondente DAG, de um lado temos a *Tangle* principal, i.e., a *Tangle* que contém todas as transações do sistema (excluindo aquelas do ramo parasita), mas incluída a transação honesta; e, do outro lado, temos o ramo parasita, o qual contém então a transação fraudulenta.

Explica-se que o algoritmo *Markov Chain Monte Carlo* (MCMC) é o responsável por selecionar quais são as duas transações a serem validadas pela recém submetida transação, seja ela honesta ou fraudulenta. Sua operação é descrita simplificadamente a seguir.

Duas partículas, também conhecidas como caminhantes aleatórios (do inglês, *random walkers*), são posicionadas em transações quaisquer da *Tangle*. Essas partículas passam então a caminhar de uma transação para outra na *Tangle*, em direção às transações mais recentes [22].

A escolha para qual transação transitar pode se dar ou de maneira aleatória ou de maneira tendenciosa em direção às transações com maior número de validações. Neste trabalho, consideramos a versão tendenciosa, pois assim garante-se maior robustez para o sistema [22].

A Equação 2 estima então a probabilidade de que uma partícula venha a transitar para a ramo parasita (do minerador desonesto) e, consequentemente, venha a selecionar a transação fraudulenta para que esta seja validada [14]. Neste caso, também se admite implicitamente um processo semelhante ao da mineração em secreto que ocorre em *Blockchain*. Todavia, neste caso da *Tangle*, o trabalho em secreto se refere à adição de transações que validam secretamente a transação fraudulenta.

Para entendimento da Equação 2 (vide Figura 2, originalmente publicada em [14]), tem-se o seguinte: λ_{tangle} ($\lambda_{parasita}$) representa a taxa de transações que chegam à *Tangle* principal (ramo parasita); Δt é a quantidade de tempo passada desde a inserção da transação fraudulenta, i.e., logo após decorrido o tempo π; x corresponde à transação onde se encontra a partícula, e a mesma é uma transação comum entre o ramo parasita e o ramo principal; y corresponde à transação fraudulenta que referencia x; z corresponde à transação honesta (ou mesmo uma transação referenciada pela transação honesta); H_{ox} e H_{oy} correspondem aos pesos já alcançados pelas transações x e y, respectivamente, quando da inserção da transação fraudulenta no tempo π. Por fim, o parâmetro α representa o quão tendenciosa é a seleção em direção às transações com maior número de validações, pois aqui consideramos o algoritmo MCMC na versão tendenciosa.

Table 1: Prob. de fraude na *Tangle* para $\Delta t = 0$ s

π (min)	$q = 0,1$	$q = 0,2$	$q = 0,3$	$q = 0,4$
1	573e-51	7,6e-46	3,3e-40	1,4e-34
2	3,0e-102	5,7e-91	1,1e-79	2,1e-68
3	5,2e-153	4,3e-136	3,6e-119	3,0e-102
4	9,0e-204	3,3-181	1,2e-158	4,3e-136
5	1,6e-154	2,5e-226	3,9e-198	6,2e-170

Table 2: Prob. de fraude na *Tangle* para $\Delta t = 30$ s

π (min)	$q = 0,1$	$q = 0,2$	$q = 0,3$	$q = 0,4$
1	7,2e-77	2,1e-68	6,0e-60	1,7e-51
2	1,2e-127	1,6e-113	2,0e-99	2,5e-85
3	2,2e-178	1,2e-158	6,5e-139	3,6e-119
4	3,7e-229	9,0e-204	2,2e-178	5,2e-153
5	6,5e-280	6,8e-249	7,1e-218	7,5e-187

Note que no cenário em que consideram-se $H_{ox} = \lambda_{tangle}.\pi$ e $H_{oy} = 1$ (i.e., peso da própria transação fraudulenta), não há trabalho em secreto executado pelo minerador desonesto; caso contrário, considera-se $H_{oy} = \lambda_{parasita}.\pi$.

4.1.3 Resultados da Modelagem Matemática

Consideramos a taxa de submissão de 2.164 mensagens por segundo no ecossistema IoT. Este valor representa a taxa média de mensagens realizadas por dispositivos IoT em um pequena área da cidade de Santo André, SP, Brasil, de 250 m^2, com densidade populacional aproximada de 3.848,01 hab/km^2 [18] e que, de acordo com a previsão para 2025 [26], cada indivíduo possua nove dispositivos IoT, cada um enviando uma mensagem por segundo.

Para termos cenários equivalentes em *Blockchain* e *Tangle*, associamos a probabilidade de o próximo bloco ser minerado pelo fraudador e pelo minerador honesto da *Blockchain* à taxa de transações na *Tangle* principal e no ramo parasita, respectivamente, assim: $\lambda_{parasita} = q.(2.164)$ e $\lambda_{tangle} = 2.164$. Os resultados obtidos estão nas Tabelas 1, 2, 3, e na Figura 3. Neste estudo, considera-se $H_{oy} = \lambda_{parasita}.\pi$, i.e., o fraudador aumentou o peso cumulativo da transação fraudulenta durante o tempo de espera, o que caracteriza a mineração em secreto.

A partir dos resultados das Tabelas 1, 2 e 3, tem-se o seguinte. Sob *Tangle*, para $\Delta t = 0$ s, as probabilidades de fraude são insignificantes, independentemente da capacidade do fraudador (dada pela probabilidade q), e do tempo de espera $\pi \leq 1$ min. Para maiores valores de Δt, a probabilidade de fraude diminui ainda mais.

A partir dos resultados da Figura 3, tem-se o seguinte. Sob *Blockchain*, as probabilidades de fraude podem ser significativas. Por exemplo, para $\pi = 10$ min e $\Delta t = 0$ s, a probabilidade de fraude já alcança $\approx 0,82$ para a capacidade de fraude de 40% (i.e., $q = 0,4$). Mesmo quando $\pi = 60$ min (para $\Delta t = 0$ s e $q = 0,4$), a probabilidade de fraude, apesar de ter sido reduzida, ainda é significativa (i.e., $\approx 0,5$).

Os cenários onde $q \geq 0,5$ não são aqui considerados, pois, de acordo com a Equação 1, para $q \geq 0,5$, a probabilidade de fraude é igual a 1,0 para a *Blockchain*. No caso da *Tangle*, conforme Equação 2, a probabilidade de fraude se mantém constante quando o fraudador possui a mesma capacidade da rede, e tende a 1,0 quando é maior.

$$P_{xy} = \frac{e^{-\alpha(H_{ox}+\Delta t.\lambda_{tangle})}}{e^{((H_{ox}+\Delta t.\lambda_{tangle}+H_{oy}+\Delta t.\lambda_{parasita})-H_{oz}+\Delta t.\lambda_{tangle})} + e^{-\alpha(H_{ox}+\Delta t.\lambda_{tangle})}} \quad (2)$$

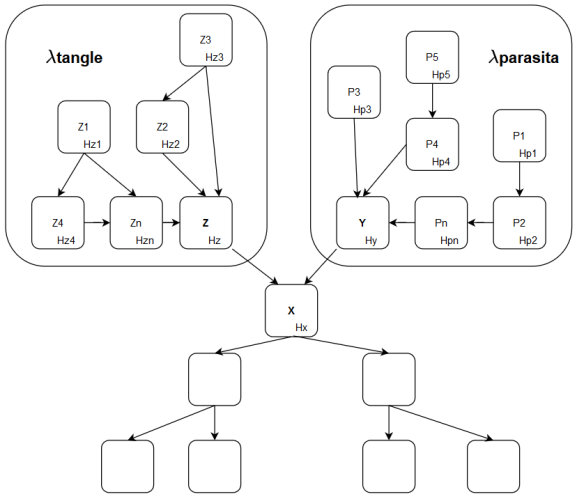

Figure 2: Representação do cenário avaliado.

Table 3: Prob. de fraude na *Tangle* para $\Delta t = 90$ s

π (min)	$q = 0,1$	$q = 0,2$	$q = 0,3$	$q = 0,4$
1	1,2e-77	1,6e-113	2,0e-99	2,5e-85
2	2,2e-178	1,2e-158	6,5e-139	3,6e-119
3	3,7e-229	9,0e-204	2,2e-178	5,2e-153
4	6,5e-280	6,8e-249	7,1e-178	7,5e-187
5	0.0	0.0	0.0	0.0

A partir dos resultados observados é possível concluir que a *Tangle* possui menor probabilidade de fraude que a *Blockchain*. Isso se deve especialmente ao fato de que a *Blockchain* é limitada, por definição de projeto, a gerar apenas um bloco de transações a cada 10 min. Essa limitação impede, portanto, que o sistema possa se beneficiar do aumento do número de transações por unidade de tempo, dado que o tamanho máximo do bloco, em número de transações, termina sendo limitado por ser possível gerar apenas um bloco de transações a cada 10 min.

4.2 Simulação

A simulação é executada por meio da ferramenta Tangram-II [10]. Esta ferramenta foi desenvolvida pela Universidade Federal do Rio de Janeiro com a participação da Universidade da Califórnia em Los Angeles. O Tangram-II permite a análise de desempenho por meio da modelagem de processos, sendo possível resolvê-los tanto analiticamente como por meio de simulações. Os modelos de simulações são implementados a partir da definição de objetos que interagem por troca de mensagens. Essa ferramenta foi escolhida especialmente pela sua destacável usabilidade e disseminação na academia.

O modelo de simulação da *Blockchain* é explicado a seguir. Consideram-se três objetos, sendo eles: *mineração honesta*, *mineração desonesta*, e *poisson source* (Figura 4). O primeiro representa a ramificação gerada pelos mineradores honestos da rede na lista encadeada. O segundo representa a ramificação gerada pelo fraudador na lista encadeada. Por fim, o terceiro é responsável pela geração de blocos que são adicionados à lista encadeada, considerando um processo de Poisson de taxa média de um bloco a cada 10 min.

Table 4: Prob. de fraude na simulação

Tecnologia	$q = 0,1$	$q = 0,2$	$q = 0,3$	$q = 0,4$
Blockchain	3,72e-05	2,08e-05	9,90e-03	2,20e-02
Tangle	1,25e-53	4,94e-48	2,28ee-42	1,38e-36

O modelo de simulação da *Tangle* é explicado a seguir. Consideram-se quatro objetos, sendo eles: *tangle principal*, *ramo parasita*, *poisson source*, *poisson source parasita* (vide Figura 5). O primeiro representa a *Tangle* principal e contém a transação honesta. O segundo é o ramo parasita que referencia à *Tangle* e possui a transação fraudulenta. O terceiro objeto gera as partículas a uma taxa de 2.164 partículas por segundo, considerando um processo de Poisson. Por fim, o quarto objeto gera as transações responsáveis pelo aumento do peso cumulativo da transação fraudulenta a uma taxa de $q.(2.164)$ partículas por segundo. Os valores dessas taxas têm a mesma justificativa do caso da modelagem analítica.

Para o cálculo da probabilidade de fraude na *Blockchain*, toma-se o número de vezes que o fraudador obtém sucesso (i.e., o número de blocos do ramo parasita é maior ou igual a quantidade de blocos da ramificação honesta) em relação à quantidade de blocos gerados no sistema. Nesta modelagem, a mineração em secreto não é considerada e admite-se $\pi = 10$ min.

Por sua vez, a probabilidade de fraude na *Tangle* é calculada a partir da média das probabilidades de que uma partícula selecione o ramo parasita ao longo do tempo. A mineração em secreto é considerada nesta modelagem e admitimos $\pi = 1$ min.

Dessa forma, estamos propositalmente favorecendo a *Blockchain* em detrimento da *Tangle*. Isso se justifica pela grande vantagem da *Tangle* sobre a *Blockchain* já observada nos resultados anteriores da modelagem analítica. A pergunta que desejamos responder agora passa a ser então: a *Tangle* ainda se mostra superior nesse novo cenário em que não há mineração em secreto na *Blockchain*?

Os resultados das simulações têm intervalos de confiança de 95% que estão dentro do limite de 5% dos valores estimados, tendo sido consideradas 15 execuções (rodadas), e um tempo de simulação de 24 horas para cada rodada.

A Tabela 4 apresenta então a síntese dos resultados obtidos, para $q = 0,1; 0,2; 0,3; 0,4$. Podemos ver que, quando o fraudador tem até 40% da capacidade computacional, a *Tangle* tem uma significativa vantagem em relação à *Blockchain*. Neste caso, a probabilidade de fraude é de $\approx 1,38$e-36 na *Tangle*, enquanto, na *Blockchain*, a probabilidade de fraude é de $\approx 0,022$. Conforme a capacidade computacional do fraudador diminui, a diferença entre as tecnologias passa a ser ainda mais evidente. A diferença entre os resultados obtidos por modelagem matemática e simulação para *Tangle* é

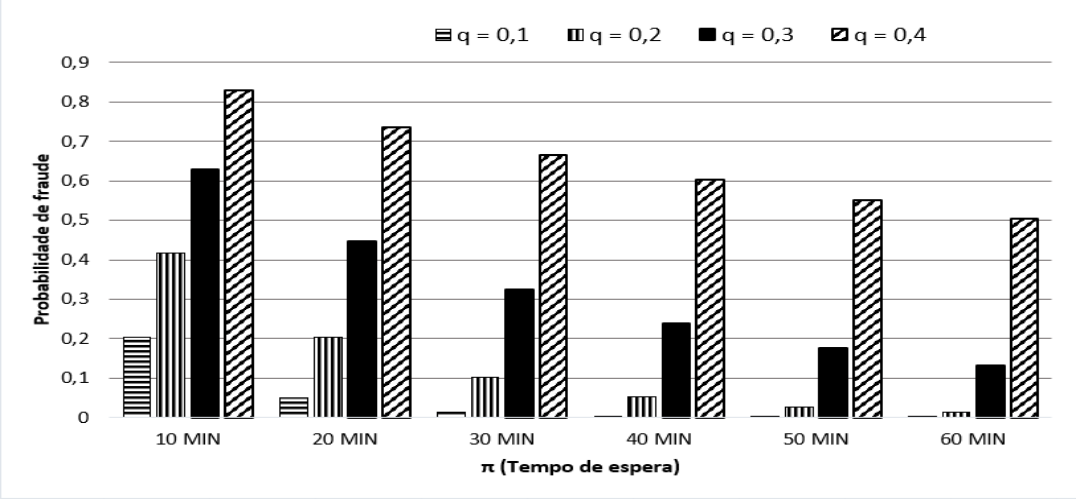

Figure 3: Probabilidade de Fraude para Blockchain.

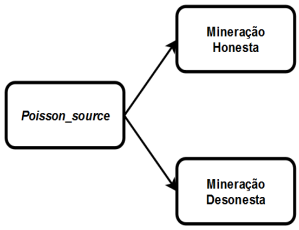

Figure 4: Modelo de simulação da *Blockchain*.

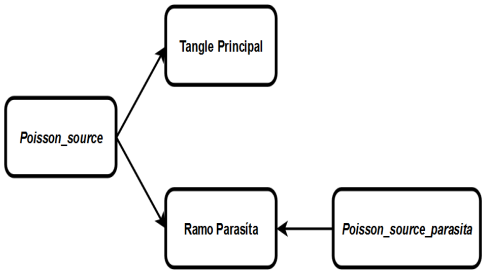

Figure 5: Modelo de simulação da *Tangle*.

insignificante. Todavia, para *Blockchain*, há uma diferença observável. Isso se deve especialmente por não haver mineração em secreto na simulação.

A partir dos resultados obtidos, pode-se então contundentemente concluir que, embora ambas as tecnologias sejam resistentes a ataques de fraude, a tecnologia *Tangle* se mostra bem mais robusta, oferecendo baixa probabilidade de fraude até quando o fraudador possui quase a metade da capacidade de processamento da rede.

É possível ainda concluir que a utilização de *Blockchain* para o ecossistema IoT, considerando seu projeto original, é inteiramente desaconselhável por dois motivos em especial. O primeiro é que a probabilidade de fraude, ainda que em um patamar aceitável, é bem superior àquela observada na tecnologia *Tangle*. Segundo, a *Blockchain* não possui escalabilidade, considerando o número de transações entrantes no sistema, pois a taxa de adição de blocos no sistema é mantido constante por restrição de projeto.

Por fim, conjecturamos que a solução para tentar fazer a *Blockchain* competitiva para o ecossistema IoT passa necessariamente pelo aumento do tamanho do bloco, em número de transações. Essa solução, para sua validação, deve ser acompanhada por uma análise do impacto que o aumento do tamanho do bloco ocasiona na segurança do sistema.

5. CONCLUSÕES FINAIS

Este artigo teve como principal objetivo a avaliação do nível de segurança das tecnologias *Blockchain* e *Tangle*. Para isso, por meio de modelagem matemática e simulação, foram realizados experimentos com o intuito de avaliar a segurança, considerando cenários em que um fraudador busca alterar uma informação já registrada na base de dados, comprometendo a integridade das informações.

Os resultados da modelagem matemática e simulação permitiram ver que as tecnologias *Blockchain* e *Tangle* demonstram um nível satisfatório de segurança quando são considerados ataques de alteração de informações armazenadas na base de dados. Porém, a *Tangle* se mostrou bem mais atrativa, principalmente em cenários onde os fraudadores possuem poder computacional comparável ao da própria rede.

Como trabalhos futuros, indicamos os seguintes três pos-

síveis caminhos. Primeiro, estender a análise aqui realizada para abranger questões relacionadas aos requisitos de privacidade e disponibilidade dos dados das transações no ecossistema IoT. Segundo, avaliar comparativamente o desempenho em *hardware* das tecnologias aqui analisadas no ecossistema IoT. Terceiro, avaliar o impacto na segurança sistêmica em face de um possível aumento do tamanho do bloco da *Blockchain*, visando torná-la mais competitiva para emprego no ecossistema IoT.

6. REFERENCES

[1] M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain, 2nd Edition*. O'Reilly Media, Sebastopol, California, 2017.

[2] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A Survey. *Computer Networks*, 54(15):2787–2805, November 2010.

[3] Blockchain.com. Blockchain Charts, 2020. Available at: https://www.blockchain.com/pt/charts. Accessed on: Feb. 9th, 2020.

[4] C. K. S. Rodrigues and P. C. da Silva. Uma Análise de Algoritmos de Consenso para Blockchain visando à Implementação de Sistemas de Informação Distribuídos Transparentes. *Revista de Sistemas e Computação*, 9(1):163–188, 2019.

[5] N. R. Chandrana and E. M. Manuelb. Analysis of Modified SHA-3. *Procedia Technology*, 24:904–9105, 2016.

[6] D. Minoli and B. Occhiogrosso. Blockchain mechanisms for IoT security. *Internet of Things*, 1-2:1 – 13, 2018.

[7] D. Sonstebo. Curl disclosure, beyond the headline, 2017. Available at:https://blog.iota.org/curl-disclosure-beyond-the-headline-1814048d08ef. Acccessed on: Mar. 3rd, 2020.

[8] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing*, 134:180 – 197.

[9] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, March 2017.

[10] E. de Souza e Silva and R. Figueiredo and R. Leão. The TANGRAM-II integrated modeling environment for computer systems and networks. *ACM SIGMETRICS Performance Evaluation Review*, 36(4):64–69, 2009.

[11] B. E. El-Shweky, K. El-Kholy, M. Abdelghany, M. Salah, M. Wael, O. Alsherbini, Y. Ismail, K. Salah, and M. AbdelSalam. Internet of things: A comparative study. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 622–631, Jan 2018.

[12] Fadele Ayotunde Alaba and Mazliza Othman and Ibrahim Abaker Targio Hashem and Faiz Alotaibi. Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88:10 – 28, 2017.

[13] B. C. Florea. Blockchain and Internet of Things data provider for smart applications. In *2018 7th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–4, June 2018.

[14] G. G. Martinez and C. K. S. Rodrigues. Analisando a segurança das transações do sistema de pagamento eletrônico IOTA. *Brazilian Journal of Development*, 5(9):14469–14497, 2019.

[15] H. Gilbert and H. P. Handschuh. Security Analysis of SHA-256 and Sisters. In M. Matsui and R. J. Zuccherato, editor, *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Computer Science*. Springer, Singapore, Berlin, Heidelberg, 2004.

[16] L. Hang and D. Kim. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors*, 10:2228.

[17] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, B. Kantarci, and S. Andreescu. Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges. In *2015 IEEE International Conference on Services Computing*, pages 285–292, June 2015.

[18] IBGE. População de Santo André, 2010. Available at: https://cidades.ibge.gov.br/brasil/sp/santo-andre/panorama. Accessed on: Mar. 3rd, 2020.

[19] E. Kokoris-Kogias, E. C. Alp, S. D. Siby, N. Gailly, L. Gasser, P. Jovanovic, E. Syta, and B. Ford. Verifiable management of private data under byzantine failures. Technical report, Cryptology ePrint Archive, Report 2018/209, 2018.

[20] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni. Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, 125:251 – 279, 2019.

[21] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, and Hui-Ying Du. Research on the architecture of Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*, volume 5, pages V5–484–V5–487, Aug 2010.

[22] S. Popov. The Tangle – Version 1.4.3. Available at: https://www.iota.org/research/academic-papers. Accessed on: Feb. 9th, 2020.

[23] R. Z. A. Mata and C. K. S. Rodrigues. Uma Análise Competitiva entre as Tecnologias Blockchain e Tangle para o Projeto de Aplicações IoT. *Brazilian Journal of Development*, 5:7961–7979, 2019.

[24] P. Rathee. Introduction to Blockchain and IoT. In S. Kim and G. Deka, editor, *Advanced Applications of Blockchain Technology. Studies in Big Data*. Springer, Singapore, 2020. [Online; accessed on: Mar. 3rd, 2020].

[25] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Available at: https://bitcoin.org/bitcoin.pdf. Accessed on: Feb. 9th, 2020.

[26] B. Safaei, A. M. H. Monazzah, M. B. Bafroei, and A. Ejlali. Reliability side-effects in Internet of Things application layer protocols. In *2017 2nd International Conference on System Reliability and Safety (ICSRS)*, pages 207–212, Dec 2017.

[27] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani. Network-level security and

privacy control for smart-home IoT devices. In *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 163–167, Oct 2015.

[28] H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente. Towards Secure and Decentralized Sharing of IoT Data. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 176–183, July 2019.

[29] V. Dedeoglu and R. Jurdak and A. Dorri and R. C. Lunardi and R. A. Michelin and A. F. Zorzo and S. S. Kanhere. Blockchain Technologies for IoT. In S. Kim and G. Deka, editors, *Advanced Applications of Blockchain Technology. Studies in Big Data*. Springer, Singapore, 2020. [Online; accessed on: Mar. 3rd, 2020].

[30] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu. Blockchain for the IoT and industrial IoT: A review. *Internet of Things*, page 100081, 2019.

[31] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko. Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access*, 6:1513–1524, 2018.

[32] K. Zhang and H. Jacobsen. Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, July 2018.

[33] Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen, and S. Shieh. IoT Security: Ongoing Challenges and Research Opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pages 230–234, Nov 2014.

[34] K. Zhao and L. Ge. A Survey on the Internet of Things Security. In *2013 Ninth International Conference on Computational Intelligence and Security*, pages 663–667, Dec 2013.