Universidade Paulista – UNIP

Matheus Stein Penayo

IOTA: Uma alternativa para ambientes de Internet das Coisas

Limeira

2018

Universidade Paulista – UNIP

Matheus Stein Penayo

IOTA: Uma alternativa para ambientes de Internet das Coisas

Trabalho de conclusão de curso apresentado a banca examinadora da Universidade Paulista – UNIP, como requisito parcial à obtenção do Bacharelado em Ciência da Computação sob a orientação dos Prof. Me. Antonio Mateus Locci, Prof. Me. Marcos Vinicius Gialdi e Prof. Me. Sergio Eduardo Nunes.

Limeira

2018

Matheus Stein Penayo

IOTA: Uma alternativa para ambientes de Internet das Coisas

Trabalho de conclusão de curso apresentado a banca examinadora da Universidade Paulista – UNIP, como requisito parcial à obtenção do Bacharelado em Ciência da Computação sob a orientação dos Prof. Me. Antonio Mateus Locci, Prof. Me. Marcos Vinicius Gialdi e Prof. Me. Sergio Eduardo Nunes.

Aprovada em ___ de _____ de 2018

BANCA EXAMINADORA

_____

Prof. Dr. Nome Completo

_____

Prof. Me. Nome Completo

_____

Prof. Esp. Nome Completo

DEDICATÓRIA

Dedico esse trabalho a minha família por sempre me apoiar desde o inicio dessa jornada, minha querida namorada por me acompanhar e apoiar durante toda essa evolução profissional e pessoal, aos meus amigos e colegas de classe por todos os momentos e desafios vivenciados juntos, aos meus professores por me orientarem e guiarem nesses 4 anos e especialmente para meu avô que sempre foi uma inspiração em minha vida.

“É perigoso sair porta afora, Frodo. Você pisa na Estrada, e se não controlar seus pés, não há como saber até onde você pode ser levado…”

(Bilbo - A Sociedade do Anel, O Senhor dos Anéis).

RESUMO

A Internet das Coisas é uma revolução tecnológica com o intuito de conectar os objetos do nosso dia a dia à rede mundial de computadores. Com o avanço dessa inovação, cada vez mais surgem eletrodomésticos, meios de transporte, instrumentos que fazem parte da nossa vida, conectados à Internet. O propósito da IoT é unir o mundo físico ao digital, de forma distribuída e assim transformando em apenas um só. Justifica-se que a IoT será uma realidade em alguns anos e causará grandes mudanças em nossa sociedade. Para evitar ataques cibernéticos aos dispositivos e garantir a segurança e privacidade aos dados dos usuários, serão necessárias tecnologias para proteger os ambientes e permitir a comunicação entre os objetos inteligentes. O objetivo desse estudo é contribuir com o avanço da IoT, propondo uma alternativa, através da criptmoeda IOTA e sua tecnologia *Tangle*, de um *backbone* ambientes de IoT. O estudo qualifica-se pela pesquisa bibliográfica exploratória qualitativa através de livros e artigos a respeito de IoT, criptomoedas e IOTA. Espera-se que com a utilização da tecnologia pesquisada no presente trabalho, ecossistemas de IoT possam ser projetados baseados nela, atingindo assim os objetivos propostos. Portando, por meio do *Tangle*, cujo embasamento teórico fundamenta-se em um teorema matemático chamado DAG: Gráfico Acíclico Dirigido (do inglês, *Directed Acyclic Graph)* a rede proporciona uma alta escalabilidade e velocidade de transação, além de micro transações, resistência quântica e criptografia. Diante deste cenário, a IOTA apresenta-se como uma infraestrutura para interconectar os dispositivos ligados à Internet, permitindo uma troca de dados veloz, segura e em tempo real, contribuindo com a evolução da Internet das Coisas.

Palavras-chave: Escalabilidade, Internet das Coisas (IoT), IOTA, *Tangle*, *Backbone*, Gráfico Acíclico Dirigido.

ABSTRACT

The Internet of Things is a technological revolution in order to connect the objects of our day by day to the network of computers. With of this innovation advancement, more and more appliances, means of transportation, instruments that are part of our lives, connected to the Internet are emerging. The purpose of IoT is to hang together the physical world to the digital world, in a distributed way and thus transforming into only one. It is justified that IoT will be a reality in a few years and will cause great changes in our society. To prevent cyber-attacks on devices and warrant the security and privacy of users' data, technologies will be needed to protect environments and enable communication between smart objects. The objective of this study is to contribute with the advancement of IoT, proposing an alternative, through IOTA cryptocurrency and its Tangle technology, of a backbone IoT environments. The study qualifies by qualitative exploratory bibliographic research through books and articles regarding IoT, cryptocurrency and IOTA. Is expected that with the use of the technology researched in the present study, IoT ecosystems could be projects based on it, by reaching the proposed goals. Thus, through the Tangle, whose theoretical basis is based on a mathematical theorem called DAG: Directed Acyclic Graph, the network provides a high scalability and transaction speed, as well as micro transactions, quantum resistance and encryption. Given this scenario, IOTA presents itself as an infrastructure to interconnect the devices connected to the Internet, allowing a fast, secure and real-time data exchange, contributing to the evolution of the Internet of Things.

Keywords: Scalability, Internet of Things, IOTA, Tangle, Backbone, Directed Acyclic Graph.

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

A Internet das Coisas (do inglês *Internet of Things*) é uma revolução tecnológica que promete causar grande impactos e mudanças na nossa maneira de viver. Atualmente grande parte das residências possuem algum dispositivo conectado à Internet, onde geralmente são *smartphones*, *notebooks* ou *smart* TV's. Agora imagine o seguinte cenário em que, além desses dispositivos, diversos objetos da casa estejam conectados à Web, como geladeira, sistemas de som, alarme, lâmpadas, etc. A proposta não é de que o usuário navegue por sites através dos objetos, como em um computador convencional, a ideia é de que a conectividade com a Internet permita uma comunicação M2M (*machine-to-machine*) entre esses instrumentos do nosso dia a dia para que possam ficar mais eficientes ou receber funções complementares. Nesse sentido, uma geladeira, por exemplo, poderia emitir um aviso quando um alimento está perto de acabar e, simultaneamente, pesquisar na Internet quais mercados oferecem o melhor preço para aquele determinado produto. Esse é apenas um exemplo dos diversos que a IoT (Internet das Coisas) pode contribuir com nossa sociedade.

O termo Internet das Coisas surgiu pela primeira vez em 1999 pelo pesquisador britânico do Massachusetts Institute of Technology (MIT) Kevin Ashton, considerado o primeiro especialista em IoT, que em entrevista a FINEP (Financiadora de Estudos e Projetos) disse que a ideia se baseia em um ponto de encontro onde não mais apenas usaremos um computador, mas onde o computador se use independentemente, de modo a tornar a vida mais eficiente. Os objetos, as "coisas", estarão conectadas entre si e em rede, de modo inteligente, e passarão a sentir o mundo ao redor e interagir.

O grande desafio a ser enfrentado daqui para frente com o aumento cada vez mais significativo desses objetos conectados à Internet e seu volume de dados são as informações dos usuários que estarão mais expostas a ataques cibernéticos que serão mais comuns, portanto serão necessários sistemas de gerenciamento para os ambientes e de proteção para tais ameaças. Diante desse cenário surgem tecnologias criadas diretamente para a indústria de IoT, como é o caso da IOTA, uma criptomoeda desenvolvida para ser embarcada em dispositivos inteligentes, que por meio dessa

pesquisa, será demonstrado de que maneira será possível enfrentar tais questionamentos.

2. OBJETIVO

O desenvolvimento dessa pesquisa tem os seguintes objetivos, primeiramente o tecnológico: contribuindo diretamente com o estudo de Internet das Coisas, como a criptomoeda IOTA e sua tecnologia *Tangle* podem ser um sistema que gerenciem os dispositivos conectados à Internet, permitindo uma comunicação, troca de dados e transações entre os mesmos e que mantenham os dados dos usuários seguros, e no segundo caso, o social: a partir do desenvolvimento da Internet das Coisas, como ela pode beneficiar a sociedade de uma forma ágil e inteligente.

3. JUSTIFICATIVA

Pressupondo que a Internet das Coisas será uma realidade em alguns anos e causará grandes mudanças em nossa sociedade, será necessário evitar ataques cibernéticos aos dispositivos e garantir a segurança e privacidade aos dados dos usuários. Dessa forma, serão necessárias tecnologias para proteger os ambientes e permitir a comunicação entre os objetos inteligentes.

4. METODOLOGIA

O estudo qualifica-se pela pesquisa bibliográfica exploratória qualitativa através de livros e artigos a respeito da Internet das Coisas e da criptomoeda IOTA. Onde a primeira etapa visa explicar um contexto da IoT em nossa sociedade e sua evolução histórica, em seguida uma explicação sobre criptomoedas e sua origem. Após a compreensão desses contextos, será apresentada a moeda IOTA e de que maneira sua tecnologia *Tangle* atua, chegando a conclusão de como ela pode funcionar em dispositivos de Internet das Coisas.

5. FUNDAMENTAÇÃO TEÓRICA

5.1 LINHA TEMPORAL IOT

Em setembro de 1991, Mark Weiser escreveu o artigo *The Computer for the 21st Century* na *Scientific American*, que pode ser considerado um dos pioneiros no estudo de *IoT* (*Internet of Things*) , no qual o texto aborda o tema de “computação ubíqua”, que segundo o autor seria o oposto da Realidade Virtual, onde um ambiente virtual é criado com o intuito de simular o mundo real. Já na computação ubíqua o autor afirma que os dispositivos serão conectados em todos os lugares de maneira natural para realizar as atividades dispostas que o ser humano não se preocuparia em instalar e configurar recursos computacionais.

Mas a expressão *Internet of Things* foi só aparecer em 1999, em uma palestra para a multinacional *Procter & Gramble,* o pesquisador britânico Kevin Ashton apresentava um novo sistema RFID e suas potencialidades na cadeia de abastecimento e rastreamento de produtos. Para chamar a atenção dos executivos ele utilizou o termo *Internet of Things*, enfatizando que os computadores poderiam executar tarefas com um aproveitamento e precisão melhor que os seres humanos, assim os objetos poderiam se conectar à Internet, gerando um ambiente mais inteligente.

Em junho de 2000 surgiu o primeiro eletrodoméstico “inteligente”, em um evento na Coreia do Sul. A empresa que apresentou o aparelho foi a LG, com sua geladeira inteligente que era conectada à Internet e gerenciada por um sistema da própria empresa. Na época o presidente da multinacional dos Estados Unidos relatou que o eletrodoméstico esfriava alimentos, mas também *“Consumers can use the Internet refrigerator as a TV, rádio, Web appliance, videofone, bulletin board, calendar and digital câmera”.*

A começar de 2005, o debate a respeito da Internet das Coisas se propagou, começou a gerar questionamentos acerca de privacidade e segurança de dados pelos governos. E neste ano a Internet das Coisas ganhou relevância e se transformou em pauta do *International Telecommunication Union (ITU)* em um relatório de tecnologias emergentes publicado anualmente pela agência das Nações Unidas e passou a destacar-se como o próximo passe da tecnologia.

Ainda em 2005, foi lançado o Nabaztag, um objeto com forma de um coelho que conectado à Internet, poderia ser programado para receber previsão do tempo, ler e-mails ou notícias, entre outros. O Nabaztag foi o primeiro objeto inteligente a ser comercializado em grande escala.

Figura 1 – Exemplos de Nabaztag

No ano de 2006, o autor Adam Greenfield lançou o livro Everyware, no qual demonstrava sua preocupação e visão a respeito dos objetos conectados. O trabalho de Greenfield mostra a eventual capacidade positiva da Internet das Coisas e Computação Ubíqua para a sociedade e os possíveis riscos em relação a privacidade e segurança.

Em 2008-2009, segundo pesquisa realizada pela multinacional Cisco IBSG (*Internet Business Solutions*), existiam mais objetos conectados, como *smartphones, tablets* e computadores do que a população mundial. Portanto essa época pode ser considerada como o período de nascimento da Internet das Coisas.

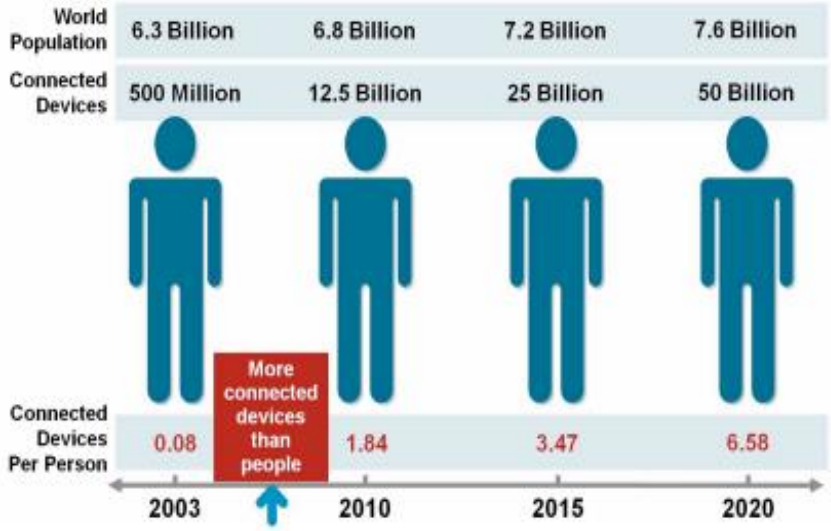

Figura 2 – The Internet of Things Was “Born” Between 2008 and 2009

Fonte: Cisco IBSG, 2011.

Ainda em 2008 o autor Rob Van Kranemburg publicou *The Internet of Things,* um livro que tal como Everyware de Greenfield, propõe um novo paradigma em que os objetos geram informação. Tal livro ainda é considerado uma das principais referências quando se trata de Internet das Coisas.

Por volta de março de 2012, a União Europeia sugeriu uma consulta pública com o intuito dos cidadãos exporem suas necessidades e inseguranças em relação à Internet das Coisas, consequentemente Londres sediou o 1 *Open IoT Assembly* , que foram dois dias de debates em que pessoas livremente contribuíram para a elaboração de um documento com os princípios de transparência e bom uso das informações no contexto de Internet das Coisas.

Em 2018, a Internet das Coisas pode ser considerada uma realidade e segundo o site alemão de estudos e estatísticas *Statista,* cerca de 23,35 bilhões de coisas estão conectadas e em uso, e com previsão de 75 bilhões até 2025, assim então a Internet das Coisas tornou-se uma força e pretende mudar o modo como vivemos.

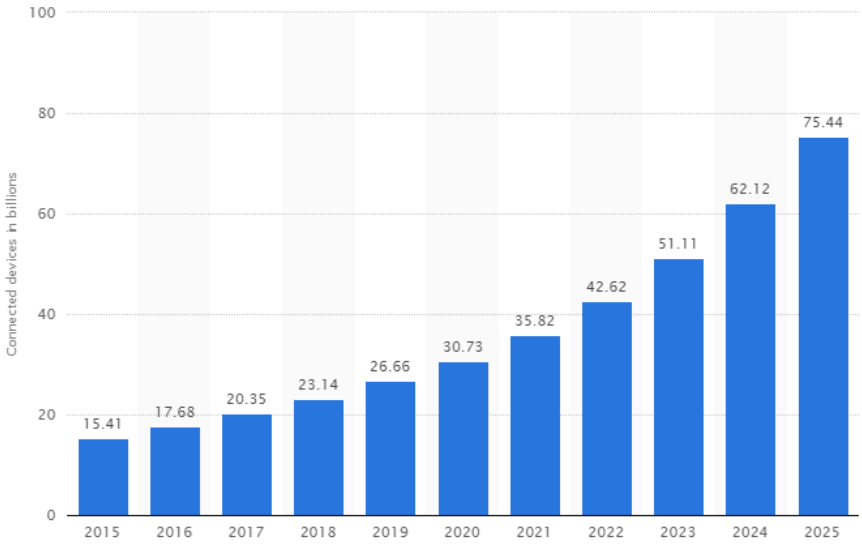

Figura 3 – Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).

Fonte: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

5.2 CRIPTOMOEDAS

Os primeiros registros a respeito de uma moeda digital datam de 1998 em uma lista de discussão *cypherpunk*. Nela existia uma proposta de criação de um novo formato de dinheiro que não necessitasse do controle de um órgão centralizador para viabilizar ou realizar transações, e que fosse criptografado. (HAAS, 2013)

De acordo com o autor citado acima, a expressão *cypherpunk,* referente à criptografia, faz um trocadilho com outra expressão conhecida como *cyberpunk*, nome da subcultura underground aliada a tecnologias de informação e cibernética, conhecida também pela sua resistência ao "*establishment*" e ao "*mainstream*". No qual *cyber*, significa *cybernetic* e, *cypher* representa criptografia.

A força de oposição representada pelo movimento *cypherpunk* teve como propósito devolver ao individuo o controle sobre sua própria liberdade em ambientes de rede. Tal que o grupo sempre defendeu utilizar sistemas anônimos, em que a criptografia de dados desempenhou um papel fundamenta.

Até o surgimento do Bitcoin, em 2008, criado por Satoshi Nakamoto, que até hoje em dia não teve sua identidade revelada, conhecido apenas por seu pseudônimo, transações online sempre necessitaram a presença de um terceiro que intermediasse com segurança, como explicitado abaixo,

> Se Maria quisesse enviar 100 u.m. ao João por meio da internet, ela teria que depender de serviços de terceiros como PayPal ou Mastercard. Intermediários como o PayPal mantêm um registro dos saldos em conta dos clientes. Quando Maria envia 100 u.m ao João, o PayPal debita a quantia de sua conta, creditando-a na de João. Sem tais intermediários, um dinheiro digital poderia ser gasto duas vezes. Imagine que não haja intermediários com registros históricos, e que o dinheiro digital seja simplesmente um arquivo de computador, da mesma forma que documentos digitais são arquivos de computador. Maria poderia enviar ao João 100 u.m. simplesmente anexando o arquivo de dinheiro em uma mensagem. Mas assim como ocorre com um e-mail, enviar um arquivo como anexo não o remove do computador originador da mensagem eletrônica. Maria reteria a cópia do arquivo após tê-lo enviado anexado à mensagem. Dessa forma, ela poderia facilmente enviar as mesmas 100 u.m. ao Marcos. Em ciência da computação, isso é conhecido como o problema do "gasto duplo", e, até o advento do Bitcoin, essa questão só poderia ser solucionada por meio de um terceiro de confiança que empregasse um registro histórico de transações. (ULRICH, p.16, 2014)

Com a chegada do Bitcoin, pela primeira vez, o problema citado acima, de gasto duplo, pode ser solucionado sem a participação de um terceiro, o Bitcoin o faz distribuindo o registro histórico a todos os usuários do sistema através de uma rede

peer-to-peer[1]*.* Todas as transações que ocorrem no Bitcoin são registradas em uma espécie de livro-razão[2] público e distribuído chamado *blockchain* (correntes de blocos ou simplesmente um registro público de transações), que pode ser considerado um grande banco de dados público, contendo histórico de todas as transações realizadas. Assim que uma nova transação ocorre, ela é verificada pelo *blockchain* afim de assegurar que os mesmos bitcoins não tenham sido previamente gastos, eliminando assim o problema do gasto duplo. Essa rede global *peer-to-peer*, composta por milhares de usuários, torna-se o próprio intermediário, assim Maria e João, citados no exemplo acima, podem transacionar sem a necessidade de terceiros.

Através da revolução causada pelo Bitcoin e o *blockchain,* hoje em dia de acordo com o site *Coin Market Cap*[3], existem aproximadamente 2080 criptomoedas, em que cada uma busca criar sua identidade, como é exemplo da IOTA, que segundo a *IOTA Fundation* (2018) é o primeiro livro-razão distribuído de código aberto que está sendo construído para potencializar o futuro da Internet das Coisas com micro transações e integridade para máquinas.

5.3 IOTA

A IOTA foi criada em 2015 por David Sønstebø, Sergey Ivancheglo, Dominik Schienere e Serguei Popov e é gerenciada por uma organização sem fins lucrativos chamada *IOTA Fundation*, que de acordo com a mesma, a tecnologia do *blockchain* prometia uma visão convincente: redes descentralizadas permitindo a inovação aberta e transações *peer-to-peer* sem intermediários ou taxas. Em última análise, eles nunca foram construídos para executá-lo integralmente, devido a falhas técnicas inerentes ao seu design. À medida que a adoção de *blockchain* aumentou na última década, os primeiros que a adotaram foram atingidos com tempos de transação lentos e altas taxas. Como as recompensas financeiras pela validação das transações de *blockchain* se tornaram cada vez mais competitivas, suas redes também se tornaram cada vez mais centralizadas em torno de alguns atores poderosos. Mas a necessidade de

[1] Peer-to-peer: par a par ou, simplesmente, de ponto a ponto (ULRICH, p.18, 2014)
[2] Livro razão: é o nome dado pelos profissionais de contabilidade ao agrupamento dos registros contábeis de uma empresa que usa o método das partidas dobradas. Nele é possível visualizar todas as transações ocorridas em dado período de operação de uma empresa. (ULRICH, p.18, 2014)
[3] Disponível em: www.coinmarketcap.com

sistemas descentralizados e sem permissão permanece e só aumentou nos últimos anos.

Ao resolver as ineficiências do *blockchain*, a IOTA, baseada na revolucionária tecnologia distribuída, *Tangle*, é o elo que falta para a Internet das Coisas. Potenciando uma camada de liquidação de transações segura, escalável e sensível, a IOTA capacitará as máquinas e os seres humanos a participarem do crescimento de novas economias descentralizadas - a mais importante delas é a economia de máquinas. (IOTA, 2018)

O *Tangle* ainda propicia que a IOTA tenha mais um diferencial em relação as outras criptomoedas, não existem mineradores e não são cobradas tarifas para a validação de transações, que segundo Popov (2018, p. 2, tradução livre[4]),

> No começo do emaranhado, havia um endereço com um saldo que continha todos os tokens. A transação gênese[5] enviou estes tokens para vários outros endereços “fundadores”. Vamos salientar que todos os tokens foram criados na transação gênese. Nenhum token será criado no futuro, e não haverá mineração no sentido que mineradores recebam recompensas monetárias “surgidas do nada”. (POPOV, p. 2, 2018)

Em entrevista ao site *The Merkle* (2016), especializado em criptomoedas, o cofundador da IOTA David Sønstebø disse quais os diferencias da IOTA em relação a outras moedas,

> A IOTA é o primeiro sistema de pagamento, não apenas entre plataformas de criptografia, mas no mundo digital, que é totalmente sem taxas. Esta é a chave que abre novas portas para serviços anteriormente impossíveis que exigem micro transações verdadeiras. No emergente ecossistema da IoT, veremos que as máquinas são tanto prosumidores quanto consumidores de recursos tecnológicos. São esses recursos tecnológicos que trata a Internet das Coisas; sejam dados, armazenamento, energia computacional, largura de banda, eletricidade ou qualquer outro serviço utilitário. Ser capaz de trocar isso em tempo real em quantidades exatas é o fundamental para esta tecnologia.[6]

Portanto essa moeda é um dos maiores avanços desde o nascimento do Bitcoin, e o objetivo especifico da IOTA não é substituir as criptomoedas com *blockchain*, mas sim criar uma simbiose, em que ambas as tecnologias trabalhem com

---

[4] The genesis is described in the following way. In the beginning of the tangle, there was an address with a balance that contained all of the tokens. The genesis transaction sent these tokens to several other “founder" addresses. Let us stress that all of the tokens were created in the genesis transaction. No tokens will be created in the future, and there will be no mining in the sense that miners receive monetary rewards “out of thin air".

[5] Transação gênese: A gênese é descrita do seguinte modo. No começo do emaranhado, havia um endereço com um saldo que continha todos os tokens. A transação gênese enviou estes tokens para vários outros endereços “fundadores”.

[6] Disponível em: https://nulltx.com/we-interview-david-sonstebo-co-founder-of-iota/

benefícios mútuos. E como já anteriormente citado, o foco primordial está na Internet das Coisas, sendo adotada nessa indústria como circulante no mercado M2M (machine-to-machine), que está em formação e em futuro próximo será uma realidade.

5.3.1 TANGLE

Diferente do blockchain, o *Tangle* não possui um grupo de mineradores ou validadores dedicados ao processamento de transações, todos que enviam uma transação são responsáveis pela validação de outras transações. Além dessa, as principais características são que não há taxas possibilitando micro transações, estrutura de dados leve para a IoT, grande escalabilidade e velocidade, demonstrando-se ser ideal para ambientes de IoT.

5.3.1.1 DAG

O Tangle é tecnicamente chamado de DAG, do inglês, *Directed Acyclic Graph*, no qual o *Directed* significa que aponta para um caminho, *Acyclic* que não é circular, ou seja, não entra em *loop* e *Graph* nesse caso significa que o *Tangle* em si é o livro-razão para armazenar as transações.

Figura 4 – DAG
Fonte: O Autor

O funcionamento básico do *Tangle*, acontece da seguinte maneira: toda rede possui um *node*, que pode ser considerado um computador ou algum dispositivo que está emitindo uma transação, todas as transações podem ser chamadas de sites, como demonstrado na figura 5, o seguinte o *node* emitiu o site A.

Figura 5 – Node

Fonte: O Autor

Enquanto o node continua enviando transações na rede, elas vão criando conexão, que são chamadas de *edges*, que são os responsáveis para validar as transações anteriores, conforme ilustrado na figura 6.

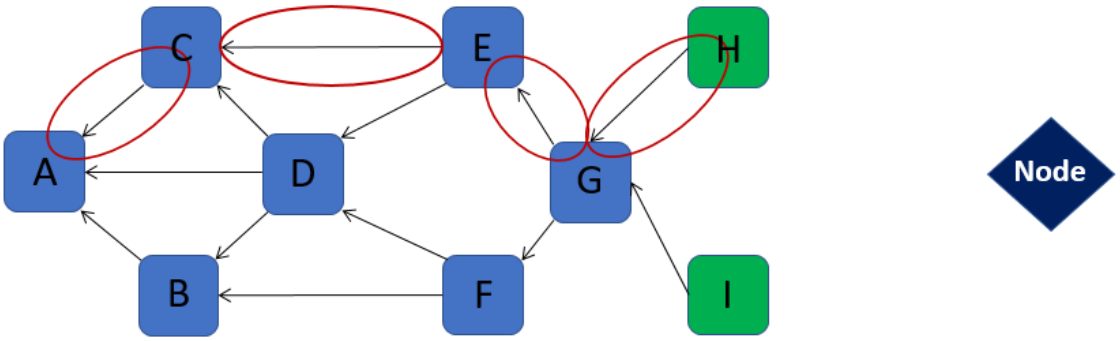

Figura 6 – Edges

Fonte: O Autor

A regra para validação de transações no *Tangle* funciona da seguinte maneira: quando uma nova transação chega, ela deve aprovar outras duas transações anteriores, ilustrado na figura 8. Os sites que se localizam no final, exemplificados pela cor verde são transações não confirmadas, chamadas de *tips,* como ilustradas na figura 7. (POPOV, p.2, 2018)

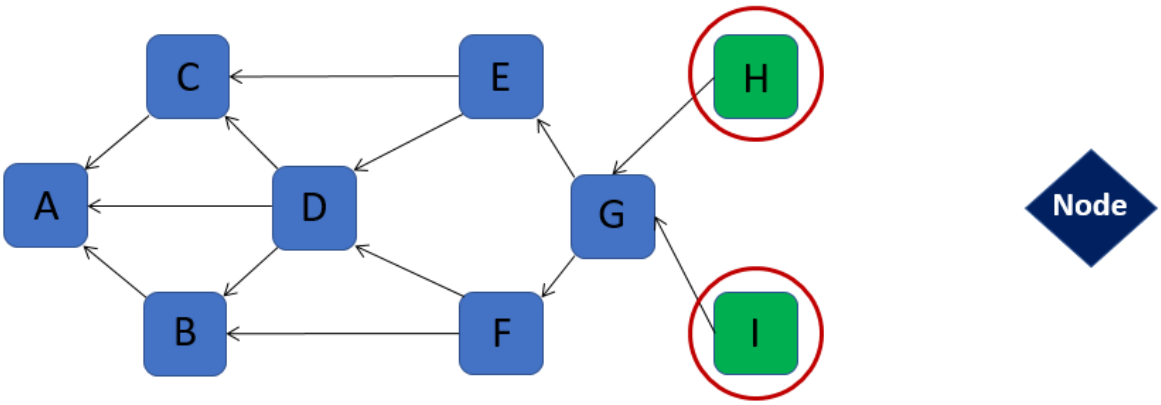

Figura 7 – Tips

Fonte: O Autor

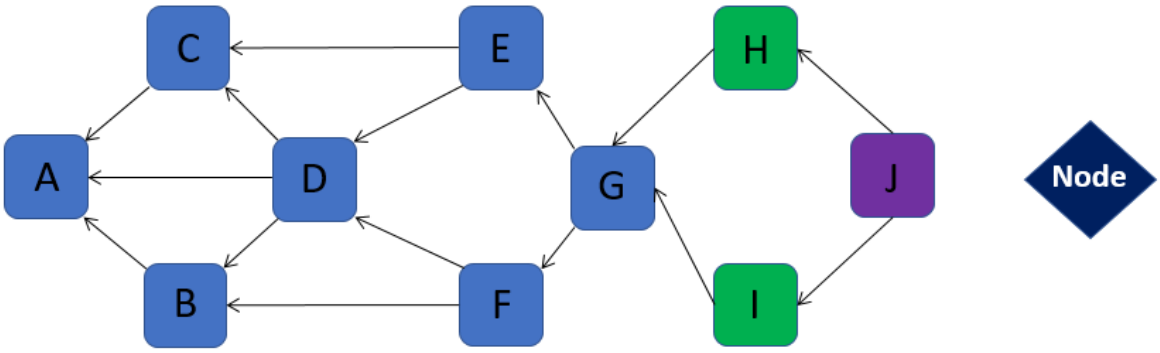

Figura 8 – Nova Transação

Fonte: O Autor

Assim que uma nova transação valida outras duas, as mesmas tornam-se parte do *Tangle*, e a nova transação aguarda uma outra que a valide, ilustrado na figura 9, demostrando assim, que a IOTA pode ser embarcada em dispositivos de Internet das Coisas, pois eles mesmo poderão validar as transações, sem a necessidade de alguma intervenção externa.

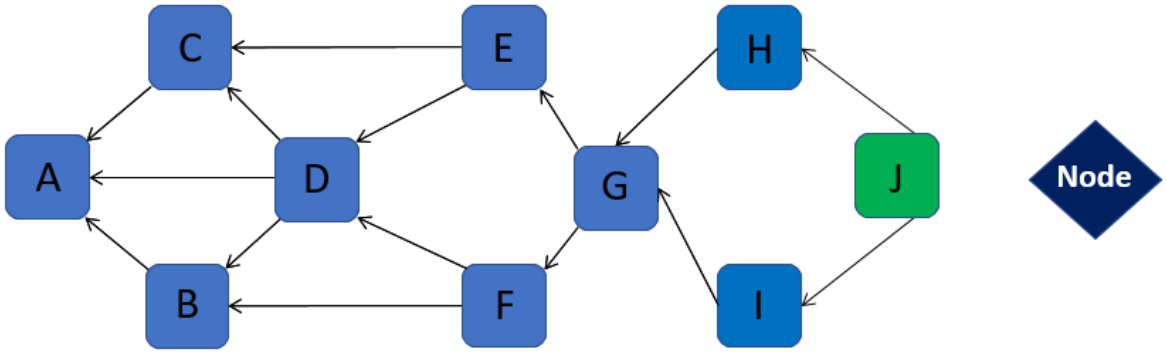

Figura 9 – Parte do *Tangle*

Fonte: O Autor

5.3.1.2 PERSONAL WEIGHT (PESO PESSOAL)

O peso de uma transação é proporcional a quantidade de trabalho que um nó emitente investiu nela. Na atual configuração da IOTA, o peso pode somente assumir 3^n , onde o n é um número inteiro positivo que pertence a algum intervalo não-vazio de valores aceitáveis, ilustrado na figura 10. Segundo POPOV (2018, p. 5, tradução livre[7]),

> De fato, é irrelevante saber como o peso foi obtido na prática. É importante apenas que todas as transações têm um número inteiro positivo, seu peso, ligado a ela. Em geral, a ideia é que uma transação com um peso maior é mais “importante” do que uma transação com um peso menor. Para evitar envio de spam e outros estilos de ataque, é assumido que nenhuma entidade pode gerar uma abundância de transações com pesos “aceitáveis” em um curto período de tempo. (POPOV, p.5, 2018)

Outra noção extremamente relevante é o peso acumulado de uma transação, que é definido como próprio peso de uma transação especifica, mais a soma de pesos próprios de todas as transações que aprovam direta ou indiretamente esta mesma transação, exemplificado na figura 11, onde o site D tem o peso acumulativo de 9, que são as somas dos pesos pessoais dos sites F, G, H, I, diretamente ou indiretamente.

[7] In fact, it is irrelevant to know how the weight was obtained in practice. It is only important that every transaction has a positive integer, its weight, attached to it. In general, the idea is that a transaction with a larger weight is more “important" than a transaction with a smaller weight. To avoid spamming and other attack styles, it is assumed that no entity can generate an abundance of transactions with “acceptable" weights in a short period of time.

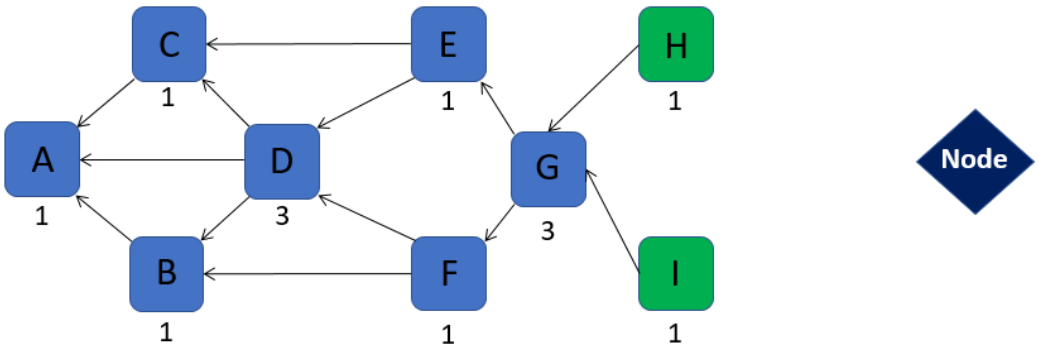

Figura 10 – Peso Pessoal

Fonte: O Autor

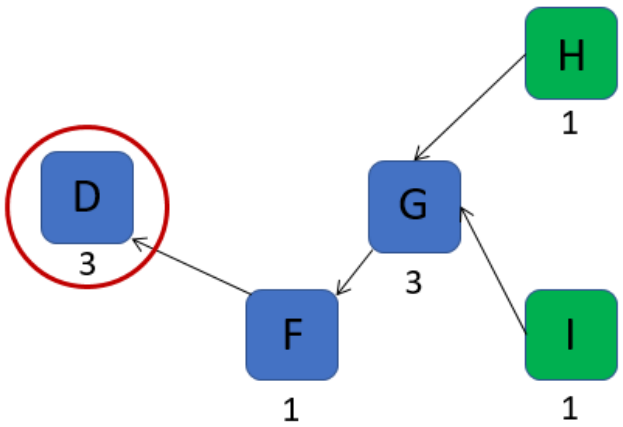

Figura 11 – Peso acumulado

Fonte: O Autor

O peso dos sites é de extrema importância, pois eles realmente contribuem com a rede, devido a medida que as transações se tornam mais antigas, elas “engordam”, ou seja, tornam-se mais confiáveis para transações desconfiáveis ou apresentariam risco ao *Tangle*.

5.3.1.3 ALGORITMO MARKOV CHAIN MONTE CARLO (MCMC)

Com um grande aumento do número de transações, haverá várias *tips* não confirmadas no início do *Tangle,* no entanto quando uma transação é emitida por um

node existe um algoritmo chamado *Markov Chain Monte Carlo*, que basicamente seleciona duas *tips* aleatoriamente, com o intuito de evitar que alguém trapaceie validando apenas suas próprias transações.

5.3.1.4 ESCACABILIDADE

A IOTA foi criada para ser leve o suficiente para permitir que transações sejam enviadas e comprovadas por notebooks, carros, todos os dispositivos que possam ser relacionados a Internet das Coisas, diferente do *blockchain* que quanto mais pessoas usam o sistema mais lento ele se torna. Com o *Tangle*, devido ao fato que cada transação precisa validar outras duas, quanto mais usuários a rede possuir mais rápida ela se mantém. (POPOV, 2018)

5.3.1.5 PROOF OF WORK

Para entender a segurança do *Tangle*, é necessário entender sobre prova de trabalho (do inglês *Proof of Work*). Seu funcionamento é baseado em um *hash*, que foi inventado por Adam Back em 1998 para a prevenção de spam nos e-mails, trata-se apenas de um conjunto de letras e números escrita de forma hexadecimal que representa algum tipo de informação como texto ou arquivos, onde o computador ou outro tipo de dispositivo conectado a rede, como é no caso do *Tangle*, precisa resolver um simples quebra cabeça para validar alguma informação. No caso da IOTA é no momento de validar as duas transações anteriores. O Computador precisa “adivinhar” um código alfanumérico chamado *Nonce*, o desempenho da máquina ao resolver o *Nonce* é chamado de *Hashing Power*, e quanto mais Hashing Power o computador tiver, mais confiável ele torna-se na rede para aprovar outras transações, garantido assim segurança nas informações.

No caso da IOTA, é muito mais simples de resolver do que por exemplo no *blockchain*, que também utiliza do *proof of work,* devido ao foco em Internet das Coisas, no qual uma geladeira apropriada a IoT poderia resolver esse quebra cabeça,

desse modo as maquinas tornam-se os próprios mineradores da rede. Segundo POPOV a proposta do Tangle é, (2018, p.3, tradução livre[8])

> A ideia principal do emaranhado é a seguinte: para emitir uma transação, usuários devem trabalhar para aprovar outras transações. Portanto, usuários que emitem uma transação estão contribuindo para a segurança da rede. Assume-se que os nós verificam se as transações aprovadas não são conflitantes. Se um nó descobre que uma transação está em conflito com a história do emaranhado, o nó não aprovará a transação conflitante de uma maneira direta ou indireta. Conforme uma transação recebe aprovações adicionais, ela é aceita pelo sistema com um nível maior de confiança. Em outras palavras, será difícil fazer o sistema aceitar uma transação de gasto duplo. É importante observar que nós não impomos quaisquer regras para escolha de quais transações um nó irá aprovar. Ao invés disso, nós argumentamos que se um número grande de nós seguir alguma regra de “referência”, então para qualquer nó fixo é melhor aderir a uma regra do mesmo tipo4. Isso parece uma suposição razoável, especialmente no contexto da IoT, onde os nós são chips especializados com firmware pré-instalado. (POPOV, p.3, 2018)

5.3.1.6 COORDINATOR

Na iota cada usuário é um minerador e eles estão apenas minerando quando estão enviando transações - um ataque de dupla despesa de 51% torna-se tão simples quanto um invasor com *hardware* sofisticado que possui mais poder de computação do que o usuário normal com *hardware* de uso geral, a iota ainda está em beta e o *Tangle* está em um estado vulnerável, alguém pode atacar com uma tonelada de poder computacional bruto, no entanto, há duas coisas reforçando a segurança agora para evitar qualquer grande ataque, número um: o coordenador, resumidamente, são como rodinhas de treinamento para o iota. Como bitcoin, ethereum e todos os outros protocolos distribuídos antes dele, a IOTA precisa de um mecanismo de integração para fornecer 34% de proteção contra-ataques em seus primeiros dias. Devido à arquitetura única subjacente da IOTA, isso assume a forma de um "Coordenador". O "Coordenador", é essencialmente rodas de treinamento para a rede até que a

[8] The main idea of the tangle is the following: to issue a transaction, users must work to approve other transactions. Therefore, users who issue a transaction are contributing to the network's security. It is assumed that the nodes check if the approved transactions are not conflicting. If a node finds that a transaction is in conflict with the tangle history, the node will not approve the conflicting transaction in either a direct or indirect manner. As a transaction receives additional approvals, it is accepted by the system with a higher level of confidence. In other words, it will be difficult to make the system accept a double-spending transaction. It is important to observe that we do not impose any rules for choosing which transactions a node will approve. Instead, we argue that if a large number of nodes follow some “reference" rule, then for any fixed node it is better to stick to a rule of the same kind. This seems to be a reasonable assumption, especially in the context of IoT, where nodes are specialized chips with pre-installed firmware.

quantidade de atividade orgânica na contabilidade seja suficiente para onde possa se desenvolver sem assistência, no ponto em que o Coordenador é permanentemente desligado. Número dois: *Hashing power*, o *white paper* também fornece as contas e basicamente afirma que se um invasor obtiver 10% do poder de *hashing* da rede, sua chance de manipular a rede é de apenas 0,00001135, basicamente quase impossível, mesmo que se consiga 34% do poder de *hashing* da rede, eles ainda têm apenas 29% de chance de manipular o emaranhado em seu benefício, então, uma ameaça precisa de três vezes o poder *hash* de todo o trabalho realmente garantir uma manipulação bem-sucedida.

5.3.1.7 RESISTÊNCIA QUÂNTICA

Sabe-se que um computador quântico suficientemente grande pode ser muito eficiente para lidar com problemas que dependem de tentativa e erro para encontrar uma solução. O processo de encontrar um *nonce* para gerar um bloco Bitcoin é um bom exemplo desse problema.

Atualmente, é preciso verificar uma média de 268 *nonces* para encontrar um *hash* adequado que permita gerar um novo bloco. Sabe-se que um computador quântico precisaria Θ (√N) operações para resolver um problema que é análogo ao desafio Bitcoin. Este mesmo problema precisaria Θ (N) operações em um computador clássico. Portanto, um computador quântico seria cerca de p 268 = 234 ≈ 17 bilhões de vezes mais eficiente em minerar a *blockchain* do Bitcoin do que um computador clássico. Além disso, é importante notar que se uma *blockchain* não aumenta sua dificuldade em resposta para o poder de *hashing* aumentado, haveria uma taxa aumentada de blocos órfãos.

Pelo mesmo motivo, um ataque de "grande peso" também seria muito mais eficiente em um computador quântico. No entanto, limitando o peso por cima, efetivamente evitaria um ataque de computador quântico também. Isto é evidente na iota porque o número de *nonces* que é preciso verificar a fim de encontrar um *hash* adequado para a emissão de uma transação não é exageradamente grande. Em média, é em torno de 3^8. O ganho de eficiência para um computador quântico "ideal "seria, portanto, da ordem de $3^4 = 81$, que já é bastante aceitável. Mais importante ainda, o algoritmo usado na implementação iota é estruturado de tal forma que o

tempo para encontrar um *nonce* não é muito maior do que o tempo necessário para outras tarefas que são necessárias para emitir uma transação. Essa última parte é muito mais resistente contra a computação quântica e, portanto, dá ao *Tangle* muito mais proteção contra um adversário com um computador quântico quando comparado à *blockchain* (do Bitcoin).

5.3.2 APLICAÇÕES COM A IOTA

Com a tecnologia do *Tangle*, não existem mineradores e taxas, mas existe uma alta escalabilidade e segurança. Assim, ela pode ser considerada uma inovação ideal para a indústria de Internet das Coisas, que pode ser exemplificado com alguns casos, como por exemplo: imagine um carro que possuísse sua identidade na rede e sua própria carteira digital, esse carro com a IOTA implementada agora pode pagar por estacionamentos, pagar combustível, pedágios e até ser alugado para ganhar dinheiro. Pode-se imaginar então, uma frota de carros todos com suas identidades e sua carteira digital utilizando esses serviços.

Outro exemplo seriam as placas solares em um condomínio ou em um bairro onde as casas possuíssem a IOTA, desta forma poderiam armazenar energia solar e vendê-la para os vizinhos ou compartilha-la. Dentre esses, a citada algumas vezes geladeira, poderia identificar o produto que estaria em falta, localizar na região o mercado com o melhor preço e com a e através da moeda realizar o pedido e entrega do mesmo na residência. Esses são apenas alguns dos inúmeros exemplos que a IOTA e a Internet da Coisas podem contribuir para nossa sociedade.

6. CONSIDERAÇÕES FINAIS

Como vimos ao decorrer do artigo, a Internet das Coisas traz diversos benefícios e oportunidades para nossa sociedade revolucionando nossa maneira de viver, no entanto, com essa evolução vêm grandes desafios e preocupações, um destes e motivo de Internet das Coisas ainda não emplacar de vez, o que fazer quanto à segurança na transmissão de um volume cada vez mais crescente de dados. Expostos à web, muito além de computadores e smartphones, a vida dos usuários

pode correr uma série de riscos, como a comunicação vulnerável entre objetos e internet, a ponto de sofrer algum tipo de ataque cibernético, seja para indisponibilidade, mau funcionamento, controle do dispositivo e até vazamento de informações.

A segurança da informação para esse tipo de realidade exige distintas técnicas usadas no segmento de segurança virtual, pois se trata de diferentes objetos, com diferentes configurações, capacidade de processamento e armazenamento. De acordo com a consultoria *McKinsey Global Institute (MGI)*, o impacto econômico da Internet das Coisas será de 3,9 a 11,1 trilhões por ano em 2025, significando 11% da economia mundial.

Figura 12 – The Internet of Things offers a potential economic impacto of $4 trillion to $11 trillion a year in 2025

Fonte: McKinsey Global Institute analysis

Diante deste cenário, os usuários serão o maior potencial econômico, onde lhes trará maior conveniência, melhores produtos e serviços com o uso de Internet das Coisas.

Portanto, a criptomoeda IOTA e sua rede *Tangle*, surgem como possíveis soluções para que ambientes como o da Internet das Coisas se desenvolvam de maneira muita mais segura e eficaz. Através do DAG, a rede proporciona uma alta escalabilidade e velocidade de transação, além de micro transações, resistência quântica e segurança de dados. Através da implantação da IOTA em um ecossistema de IoT, é possível desenvolver uma gestão de segurança, partindo da parte física, com componentes eletrônicos e estruturação até a entrada dos objetos no *Tangle*, tendo assim um controle e uma confiança para que a Internet das Coisas possa cada vez mais torna-se parte do nosso dia a dia, abrindo um leque de oportunidades de grande impacto organizacional, tecnológico, social e cultural.

7. REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, A. CyberPunk e Pós-Modernismo. **BOCC**. Disponível em: <http://www.bocc.ubi.pt/pag/amaral-adriana-cyberpunk-posmordenismo.pdf.> Acesso em: 10/11/2018

EVANS, D. **The Internet Of Things:** How the Next Evolution of the Internet Is Changing Everything. Disponível em: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>. Acesso em: 24/08/2017

FINEP. "**Entrevista com Kevin Ashton criador do termo Internet das Coisas**". Disponível em: <http://finep.gov.br/noticias/todas-noticias/4446-kevin-ashton-entrevista-exclusiva-com-o-criador-do-termo-internet-das-coisas>. Acesso em: 22/08/2017

HAAS, G. **Cypherpunk:** o ativismo do futuro. 2013. Disponível em: <https://www.tecmundo.com.br/criptografia/41665-cypherpunk-o-ativismo-do-futuro.htm.> Acesso em: 17/11/2018.

IOTA**. "A Criptomoeda para a Internet of Things"**. Disponível em: <http://iotabrasil.com/p/iota.html>. Acesso em: 20/11/2017

IOTA. **"The Tangle"**. Disponível em: <https://iota.org/IOTA_Whitepaper.pdf>. Acesso em 14/03/2018

IOTA. **What is IOTA?.** Disponível em: <https://www.iota.org/get-started/what-is-iota>. Acesso em: 02/11/2018.

MANCINI, M. **Internet das Coisas: História, Conceitos, Aplicações e Desafios**. Disponível em: <https://pmisp.org.br/documents/acervo-arquivos/241-internet-das-coisas-historia-conceitos-aplicacoes-e-desafios/file>. Acesso em: 24/08/2017

PIRES, H.F. Bitcoin: a moeda do cyberespaço. **GEO USP 2017.** Disponível em < http://www.revistas.usp.br/geousp/article/download/134538/130348/>. Acesso em: 17/11/2018.

RODRIGUES, F.F; KLEINSHMIDT, H.J; **Estudo de Aplicações da Internet das Coisas em um Ambiente Acadêmico**. Disponível em: <http://www.revistaespacios.com/a14v35n13/14351309.html>. Acesso em: 24/08/2017

SANTOS, B. P.; SILVA, L. A. M.; CELES, C. S. F. S.; NETO, J. B. B.; PERES, B. S.; VIEIRA, M. A. M.; VIEIRA, L. F. M.; GOUSSEVSKAIA, L. A. A. F. **Internet das Coisas:** da Teoria à Prática. Disponível em: <http://homepages.dcc.ufmg.br/~bruno.ps/wp-content/uploads/2016/05/minicurso-sbrc-2016.pdf. Acesso em: 22/08/2017

SINGER, T. **Tudo Conectado: Conceitos e Representações da Internet das Coisas**. Disponível em: <http://files.educacao-e-tics.webnode.com/200000031-3af843cee5/Internet%20das%20Coisas%20-%20IOT%20Talyta%20Singer.pdf>. Acesso em: 23/08/2017

SøNSTEBø, D. **IOTA**. 2016. Entrevista a Eduardo Gómez. Disponível em: <https://nulltx.com/we-interview-david-sonstebo-co-founder-of-iota/.> Acesso em: 15/11/2018.

PIRES, H.F. Bitcoin: a moeda do cyberespaço. **GEO USP 2017.** Disponível em < http://www.revistas.usp.br/geousp/article/download/134538/130348/>. Acesso em: 17/11/2018.

POPOV, S. **The Tangle**. 2018. Disponivel: <https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf>. Acesso em: 13/11/2-18.

ULRICH, F. **Bitcoin a moeda da era digital.** 1ª ed. São Paulo: Mises Brasil, 2014