TRÁFEGO DE DADOS EM DISPOSITIVOS IoT DE MANEIRA SEGURA, UTILIZANDO TECNOLOGIA *BLOCKCHAINS*

Fúlvio Belato de Freitas Barichello[1]

Carlos Eduardo de França Roland[2]

Resumo

O planeta está, a cada dia, mais conectado pela internet, e quase tudo o que se faz em termos de comunicação de dados passa, necessariamente, pela rede mundial de computadores. Objetos conectados à internet vêm se popularizando e já fazem parte do cotidiano da população: *smartphones*, carros, casas, máquinas industriais, implementos agrícolas em fazendas. A segurança de dados que trafegam entre estes dispositivos reflete diretamente na segurança física das pessoas envolvidas no seu uso. Os dispositivos que coletam, armazenam e transmitem dados na rede mundial definem a Internet das Coisas (ou IoT). Objetos IoT invadidos por pessoas ou computadores maliciosos fazem com que estes aparelhos respondam de maneira imprevisível e diferente da planejada por seus usuários, ficando o real controle destes dispositivos sob a custódia dos invasores. Desde que combinados com equipamento de processamento digital de dados, estes objetos tornam-se capazes de utilizar a tecnologia Blockchains para prevenir perda de controle e de dados. Este estudo, caracterizado por uma pesquisa bibliográfica exploratória, buscou identificar como ser possível se atingir maiores níveis de segurança operacional de sistemas de automação baseados na comunicação por internet, através da tecnologia de criptografia e validação de transações utilizada pelas moedas digitais, especialmente a tecnologia Blockchains implementada originalmente na criação da Bitcoin. Os resultados dos estudos são apresentados neste artigo que são discutidos proporcionando que se considere ser uma alternativa técnica plausível para solucionar as questões de segurança existentes nessa classe de sistemas de informação, sendo ainda necessário se aprofundar a avaliação da viabilidade econômica de sua implementação para uso real.

Palavras-chave: Cadeias de Blocos. Criptografia. Internet das Coisas. Segurança de dados. Segurança de transações.

Abstract

The planet is increasingly connected to the Internet every day, and almost everything that is done in terms of data communication necessarily goes through the world wide web. Objects connected to the internet are becoming popular and are already part of everyday life, such as smartphones, cars, houses, industrial machines, farm implements. The security of data that travels between these devices reflects directly on the physical security of the people involved in their use. Devices that collect, store, and transmit data on the worldwide web define the Internet of Things (or IoT). IoT

[1] Graduando em Análise e Desenvolvimento de Sistemas pela Fatec Dr. Thomaz Novelino – Franca/SP. Endereço eletrônico: f.barichello@bol.com.br

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

objects invaded by malicious people or computers make these devices respond unpredictably and differently than intended by their users, leaving the real control of these devices in the custody of the attackers. When combined with digital data processing equipment, these objects are able to use blockchain technology to prevent loss of control and data. This study, characterized by exploratory bibliographic research, sought to identify how is it possible to achieve higher levels of operational safety of automation systems based on internet communication through the encryption and transaction validation technology used by digital currencies, especially the blockchains technology originally implemented in the creation of Bitcoin. The results of the studies are presented in this article that are discussed providing a plausible technical alternative to solve the security issues in this class of information systems, which is still necessary to develop further research to evaluate the economic viability of its implementation in real systems.

Keywords: *Blockchains. Cryptography. Data security. IoT. Transaction Security.*

1 Introdução

Tecnologia apresentada por Satoshi Nakamoto ao criar a Bitcoin, o Blockchain permitiu que criptomoedas (ou moedas virtuais) se tornassem realidade e não necessitassem de um intermediador para comprovar e validar suas movimentações financeiras digitais. Isso revolucionou o mercado e trouxe muito mais transparência às negociações.

Trilhando um caminho próprio, *blockchains* vêm sendo utilizados em outras áreas além das criptomoedas, como por exemplo: jurídica, logística, saúde e agronegócios. O impacto da tecnologia *blockchain* na sociedade nos próximos anos será enorme, e um dos setores que promete ter um casamento perfeito para uso é o da Internet das Coisas (IoT do termo em inglês Internet of Things).

O planeta está, a cada dia, mais conectado pela internet, e quase tudo o que se faz em termos de comunicação de dados passa, necessariamente, pela rede mundial de computadores. Objetos conectados à internet vem se popularizando e já fazem parte de cotidiano: *smartphones*, carros, casas, máquinas industriais, implementos agrícolas em fazendas.

O objetivo do presente estudo foi entender os principais desafios destacados no uso de dispositivos de IoT, tais como manter a proteção de dados e a privacidade dos usuários, verificar na literatura disponível as possíveis soluções em desenvolvimento, e apresentar como os dispositivos de IoT podem ter a segurança no seu uso ampliada com o emprego do *blockchain*, detalhando como aplicar esta tecnologia ao tráfego e ao armazenamento de dados de transações entre os

componentes de sistemas automatizados de coleta, armazenamento e processamento de dados por redes sem fio. A metodologia utilizada foi a de pesquisa bibliográfica exploratória em livros, artigos científicos e em manuais técnicos.

O estudo é apresentado neste artigo que é estruturado nesta Introdução, seguida da apresentação das bases conceituais dos elementos envolvidos no tema e na questão de pesquisa, para então descrever uma possível implementação de Blockchains no contexto de sistemas de IoT. Em seguida são apresentados e discutidos os resultados alcançados na pesquisa e tecidas as Considerações Finais do projeto. Por fim são apresentadas as Referências utilizadas no desenvolvimento do trabalho de pesquisa.

2 Referencial Teórico

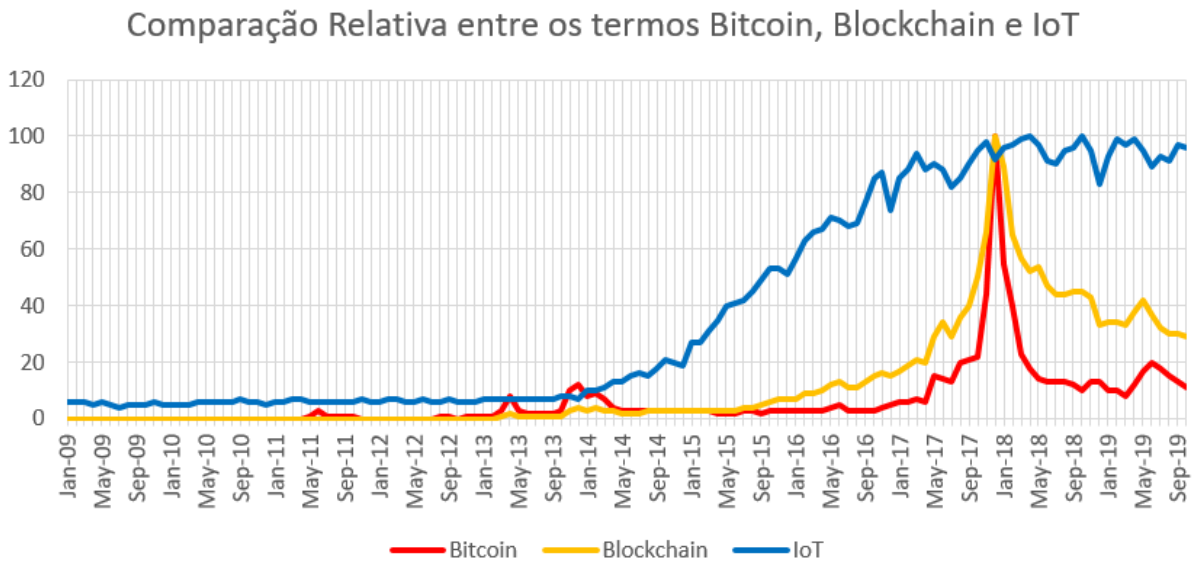
Desde janeiro de 2014 vê-se, pelas estatísticas publicadas pela Google, um aumento crescente no interesse em todo o mundo pelo termo IoT no seu mecanismo de buscas na internet. Neste mesmo período destaca-se também o interesse pelos termos Blockchain e Bitcoin, sendo que ambos atingem o pico máximo de procura em dezembro de 2017 (Figura 1), justamente no período de maior valorização do Bitcoin em sua história, cotada em aproximadamente US$ 20.000 cada unidade da moeda virtual (GOOGLE, 2019a; 2019b; 2019c, e 2019d).

Em termos absolutos a Bitcoin é mais procurada pelos usuários do mecanismo de busca que Blockchain e IoT (Figura 2). Isso provavelmente se deve à associação da moeda virtual a aspectos da sua valorização financeira.

Apesar de estar altamente vinculado à Bitcoin, as aplicações de Blockchain vão muito além das criptomoedas. Visando a desvinculação do termo à moeda virtual, propostas de empregar a tecnologia Blockchain em setores que estão em ascensão, como IoT, parecem inevitáveis.

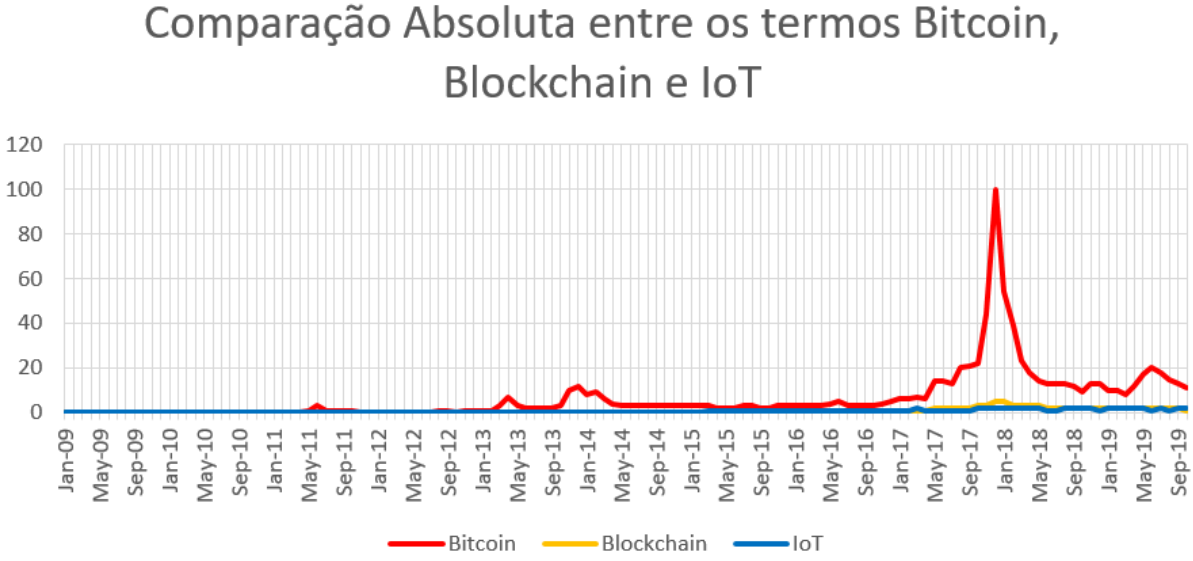
ISSN: 2595-5942

Figura 1 – Comparação Relativa entre os termos Bitcoin, Blockchain e IoT



Fonte: o autor, adaptado de GOOGLE (2019)

Figura 2 – Comparação Absoluta entre os termos Bitcoin, Blockchain e IoT



Fonte: o autor, adaptado de GOOGLE (2019)

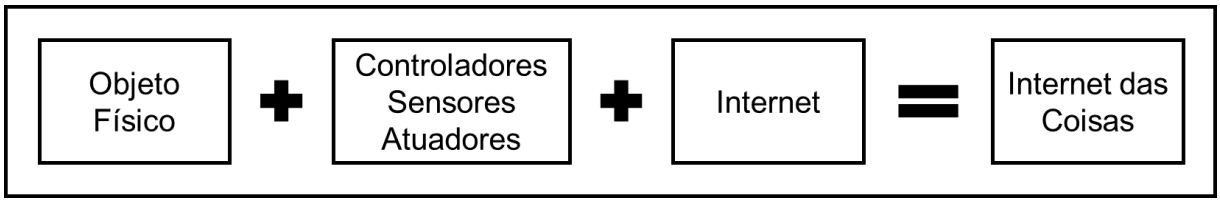
Para facilitar o entendimento do modelo teórico formulado para uso da tecnologia no contexto da IoT, é necessário que sejam elucidados os fundamentos das tecnologias envolvidas. São assim tratados os conceitos e características da IoT e logo após abordados os conceitos do Blockchain.

2.1 Internet of Things (IoT)

Internet das Coisas pode ser definida como uma rede global que conecta computadores, sensores e atuadores através de protocolos de internet (PFISTER,

2011). Para uma rápida compreensão do que é a internet das coisas, pode-se sintetizar o seu significado através da Figura 3.

Figura 3 – Equação do IoT



Fonte: o autor, adaptado de McEWEN e CASSIMALLY (2014)

Os controladores são sistemas que têm como finalidade comparar a saída de seu próprio sistema com o comando realizado em sua entrada e propiciar um sinal de controle capaz de reduzir o erro da saída ao mais próximo a zero. Existem seis tipos de controladores diferentes, sendo que cada um tem uma aplicação recomendada: liga-desliga, proporcional, integral, proporcional-integral (P-I), proporcional-derivativo (P-D) e proporcional-integral-derivativo (P-I-D) (GROOVER, 1988).

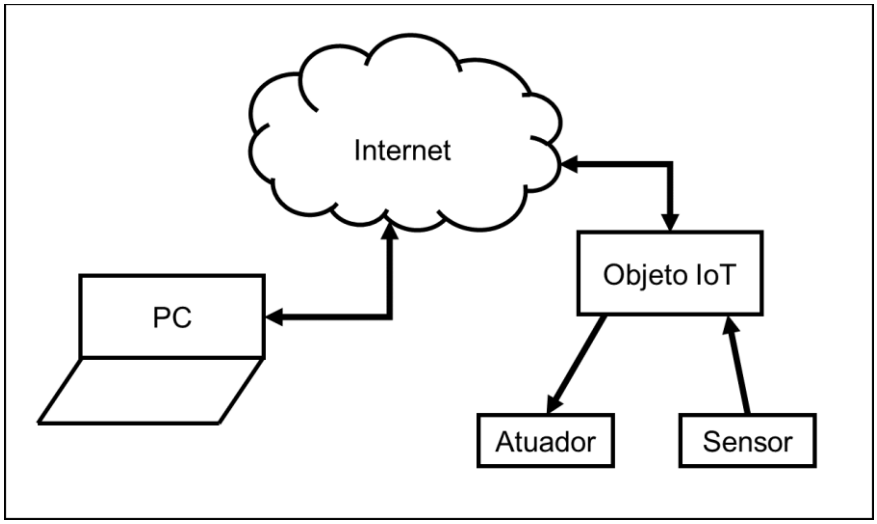
Os atuadores convertem um sinal recebido do controlador em um movimento físico de controle. Este sinal de entrada pode ser realizado por meios pneumáticos, hidráulicos, mecânicos ou eletrônicos, bem como a combinação deles (GROOVER, 1988).

Sensores são aparelhos responsáveis por sentir o ambiente onde estão inseridos. O exemplo clássico de sensor é o termômetro de mercúrio, que expande seu volume conforme o aumento de temperatura, tornando-se possível acompanhar o seu crescimento através de uma escala acoplada. Na prática, os sensores mais utilizados são aqueles capazes de converter uma grandeza física em um sinal elétrico. Esta variação de energia pode ser facilmente interpretada por circuitos eletrônicos e sistemas informatizados a eles conectados (STEVAN, 2015).

Mesmo sem perceber a população é monitorada por sensores a todo momento, e os diferentes tipos de sistemas coletam dados continuamente: desde máquinas de vendas até carros inteligentes. Para se ter uma ideia do quão próximo a Internet das Coisas está do cotidiano humano, considere que a IoT está nos pertences pessoais de todas as pessoas: no *smartphone*, na *smartTV,* na *smartHome*, etc. se tornando a IoYT (do termo em inglês *Internet of Your Things*) (BARB, 2015).

A Figura 4 ilustra um sistema IoT onde o PC é um computador conectado à internet; o Objeto IoT pode ser literalmente qualquer coisa de nosso dia a dia (geladeira, carteira, tênis, pulseira, relógio de pulso), que também está conectado à internet; além disso um sensor e um atuador estão conectados a este Objeto IoT.

Figura 4 – Internet conectando Computador e Objeto IoT

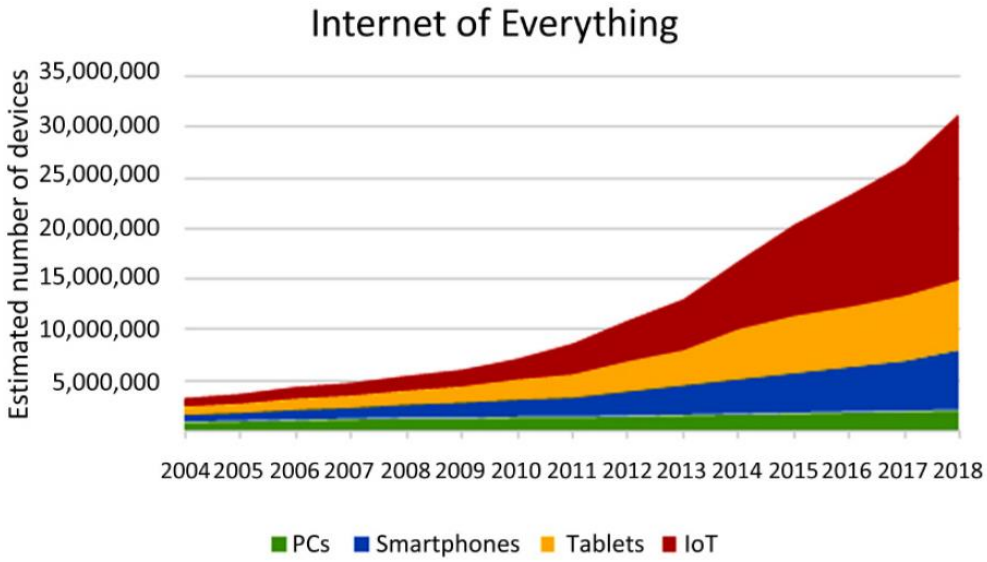


Fonte: o autor

Com um aumento contínuo no poder de processamento de dados por parte de sistemas informatizados, e com a queda, também contínua, nos preços dos componentes de *hardware* fica cada vez mais fácil empregar dispositivos IoT na vida humana (SCHWAB, 2016).

Segundo Barb (2015), organizações que conseguem monitorar seus dados saem na frente quanto às oportunidades de negócios que podem ser geradas. A tendência de crescimento no número de aparelhos IoT é muito acentuada, e pode ser observada na Figura 5.

Figura 5 – Tendência de Crescimento para o IoT



Fonte: Buyya e Dastjerdi (2016)

Schwab (2016) cita os diversos pontos positivos no uso do IoT como: aumento na eficiência dos recursos; elevação da produtividade; melhora na qualidade de vida; eficiência na logística; surgimento de novos negócios; maior precisão no monitoramento, controle e previsão de dados. Entretanto essa maior conexão também evidencia pontos negativos da IoT: perda de privacidade; diminuição dos postos de trabalho (não qualificados); ameaça da segurança digital por conta de *hackers*; maior complexidade e perda de controle.

Justamente para ampliar a segurança dos dispositivos IoT, o uso do *blockchain* promete ter um casamento perfeito.

2.2 Blockchain

No ano de 2008, sob o pseudônimo de Satoshi Nakamoto, foi publicado o artigo Bitcoin: A Peer-to-Peer Electronic Cash System (*Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer (ponto-a-ponto)* em tradução livre), que revolucionou o mundo da tecnologia. O trabalho de Satoshi compilou diversas ideias documentadas anteriormente para descrever a criação de uma moeda digital que não precisa de nenhum intermediário: o Bitcoin. Foi a implementação do *blockchain* que tornou possível a existência de criptomoedas.

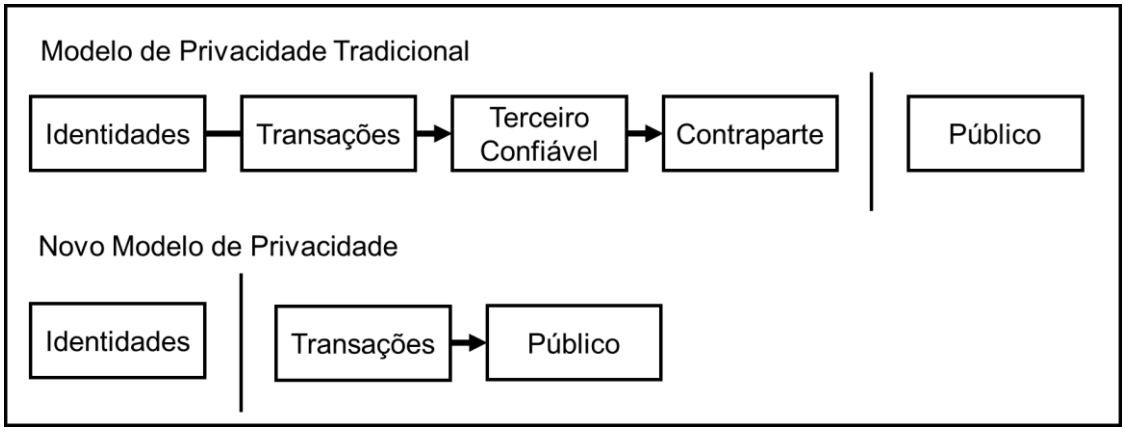
Nakamoto (2008) pontua que em uma transação financeira convencional, as duas partes envolvidas, comprador e vendedor, necessitam de uma terceira parte intermediária (por exemplo um banco) que tenha a confiança de ambos para que o

negócio seja concluído com sucesso. Por não haver confiança neste modelo, são geradas despesas extras para se garantir a idoneidade da relação. Além dos próprios custos operacionais de se realizar o movimento financeiro, ainda existem os custos da mediação dos conflitos existentes entre as partes envolvidas.

No modelo de privacidade tradicional as informações referentes às transações podem ser acessadas exclusivamente pelas partes envolvidas e pelo seu intermediário confiável. Isso faz com que os comerciantes captem muito mais dados pessoais de seus clientes do que realmente é necessário para concretizar-se o pacto, além de se ter que compartilhar estes dados com o intermediário. Um grave defeito existente neste sistema é a aceitação de um determinado percentual de fraudes envolvendo as negociações, pois elas nem sempre têm a sua validação realizada corretamente (NAKAMOTO, 2008).

Para excluir a participação de um terceiro, o autor propõe que todas as transações sejam públicas, passíveis de verificação e baseadas no tempo, protegendo-se as identidades dos envolvidos por meio de criptografia. Isto permite que mesmo partes que não tenham confiança entre si possam negociar, pois os registros tornam-se permanentes e irreversíveis. Surge assim o *blockchain*. A Figura 6 exemplifica as diferenças entre os modelos de privacidade.

Figura 6 – Modelo de Privacidade Tradicional versus Novo Modelo de Privacidade.



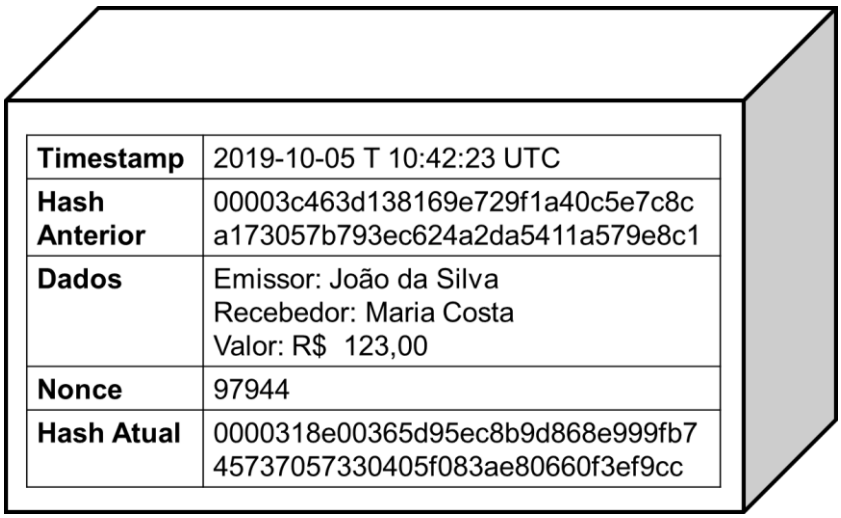
Fonte: adaptado de Nakamoto (2008)

O *blockchain* funciona como uma lista de registros permanentes, contendo todas as transações ocorridas de maneira precisa, e gravadas em ordem cronológica. Sendo muitas vezes comparado a um livro razão em contabilidade, o termo *blockchain*

pode ser traduzido do inglês como blocos em cadeia, ou cadeia de blocos, onde cada bloco representa uma transação (MACIEL, 2018).

Todos os blocos presentes em um *blockchain* possuem uma estrutura básica em comum. O *timestamp* (do inglês, marca temporal) é a data e a hora em que o bloco foi criado; os dados do bloco recebem tudo aquilo que se queira armazenar no *blockchain* (emissor, receptor, valores), pode-se dizer que são o conteúdo daquele bloco; o *hash* anterior é a identidade do bloco inserido por último no *blockchain*; o *nonce* é um campo numérico que varia, conforme a necessidade, até que se tenha um *hash* atual que atenda aos parâmetros pré-estabelecidos pela rede; e o *hash* atual é identidade deste bloco, gerada a partir de todos os outros campos dentro do bloco (MACIEL, 2018). A estrutura de um bloco pode ser observada na Figura 7. É importante observar que a privacidade dos dados foi revelada apenas por motivos didáticos.

Figura 7 – Um Bloco do *Blockchain.*



Fonte: o autor (2019)

Para criar os *hashes*, Nakamoto sugere a utilização da criptografia SHA-256. A função *hash* produz um número hexadecimal com tamanho fixo de 256 bits a partir de uma sequência de caracteres. Essa função é determinística, ou seja, para uma mesma entrada gera-se um mesmo *hash*; mas, a partir do *hash*, não é possível gerar a entrada original. Para a validação do bloco são gerados *hashes* variando o *nonce* de forma que um determinado número de dígitos zero apareça no início do *hash*. Cada zero no início de um *hash* aumenta exponencialmente a dificuldade de quebra de sua criptografia por meio de força bruta. Existem inúmeros tipos de funções *hash*, e cada

uma atua de forma diferente da outra, mas todas geram uma saída que parece aleatória (ZHENG, 2017).

No *blockchain*, os *hashes* são criados tendo como base a junção de todos os caracteres dos elementos inseridos no bloco (*timestamp*, *hash anterior*, *dados* e *nonce*). A corrente do *blockchain* é caracterizada pela necessidade de um bloco conter o *hash* gerado pelo bloco anterior (ZHENG, 2017).

Para se garantir a integralidade e a segurança dos dados no *blockchain* é preciso estar acordado entre os nós da rede as características de cada bloco neste *blockchain*, em particular no *hash* gerado. Sendo considerada a impressão digital do bloco, o *hash* só fica com a aparência necessária (por exemplo iniciando com quatro dígitos zero) caso se acrescente ao bloco o campo *nonce*. O termo *nonce* vem da contração de duas palavras da língua inglesa: *number* (número) e *once* (uma vez). Como a saída criptografada e os demais dados no bloco possuem um caráter fixo, tem-se que variar o *nonce* até que seja encontrado um número único tal que satisfaça a condição pactuada (NAKAMOTO, 2008). Ao processo da procura pelo *nonce* que satisfaça a essa condição dá-se o nome de prova-de-trabalho (do inglês, *Proof-of-Work* ou PoW). É também chamado popularmente de mineração, pela semelhança com a procura por algo valioso.

A prova-de-trabalho foi apresentada como uma forma de se evitar o envio de e-mails em massa (*spams*): para cada e-mail postado o computador deveria realizar um pequeno cálculo matemático antes de realmente conseguir enviá-lo. Isso faria com que o disparo de milhares de e-mails simultaneamente ficasse computacionalmente difícil, sem prejudicar o envio de uma quantidade de e-mails reduzida (DWORK e NAOR, 1992).

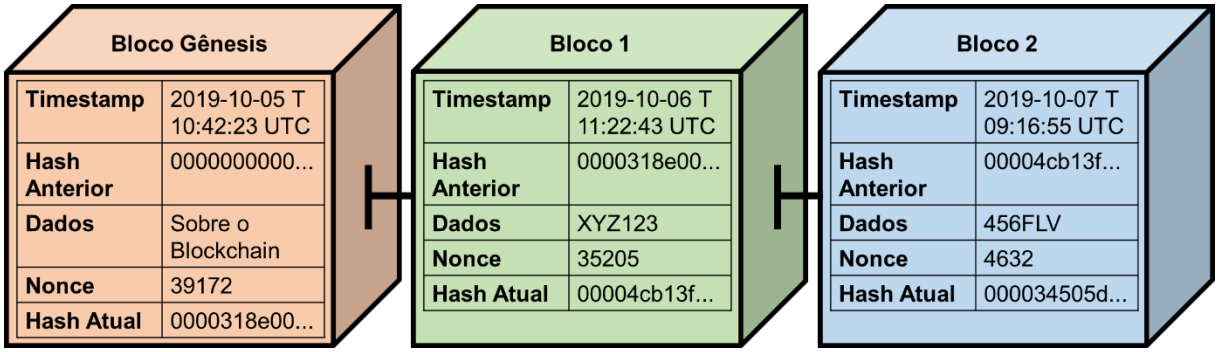
Se por um lado a prova-de-trabalho leva certo tempo para ser realizada, de outro tem-se que sua validação pode ser alcançada quase que de forma instantânea: possuindo todos os dados do bloco (incluindo o *nonce*) e aplicando a função acordada, basta se comparar os *hashes* para que se tenha certeza de que o bloco é válido (NAKAMOTO, 2008).

Na operação da tecnologia *blockchain* todas as partes envolvidas são chamadas de nós da rede, e trabalham individualmente para garantir a veracidade do *blockchain*. Quanto mais rápido o *nonce* é validado pelos nós da rede, mais difícil torna-se quebrar a sequência de blocos.

Como a procura por um *nonce* consome recursos de processamento e energia elétrica, Nakamoto (2008) idealizou a existência de uma remuneração para o nó capaz de encontrar a prova-de-trabalho para um bloco em primeiro lugar, antes dos demais. Isso desestimula a participação de computadores maliciosos na rede, que deixam de tentar burlar o sistema e passam a contribuir na construção de um ambiente saudável na rede.

O primeiro bloco do *blockchain* é denominado Gênesis, e possui características particulares: o *hash* anterior é zero e os dados contém as instruções técnicas sobre o *blockchain*, conforme pode ser observado na Figura 8.

Figura 8 – Blocos Conectados Formando o *Blockchain.*



Fonte: o autor (2019)

Nakamoto (2008) menciona os passos necessários para que seja possível uma rede *blockchain*:

1. Novas transações são transmitidas para todos os nós.
2. Cada nó coleta novas transações e as armazena em um bloco.
3. Cada nó trabalha para encontrar uma prova-de-trabalho difícil o suficiente para o seu bloco.
4. Quando um nó encontra uma prova-de-trabalho, ele transmite o bloco para todos os nós.
5. Os nós aceitam o bloco somente se todas as suas transações são válidas e já não foram gastas.
6. Os nós expressam sua aceitação do bloco, trabalhando na criação do próximo bloco na cadeia, usando o *hash* do bloco aceito como o *hash* anterior.

O Quadro 1 sintetiza os conceitos envolvidos nos componentes das criptomoedas.

Quadro 1 – Componentes de criptomoedas

Elemento	Características
Criptomoedas	Moedas digitais que existem apenas no meio virtual. Utilizam o *blockchain* como sistema de registro de transações. Podem ser, além de moedas, plataformas de desenvolvimento. São conhecidas por possuir grande flutuação em seu valor, e por possuir variados usos alternativos, negativos e positivos.
Blockchain	Uma forma de banco de dados que se assemelha a um livro-razão contábil, onde todas as informações são vinculadas, evitando alterações indesejadas de terceiros. Pode ser usado para vários fins, sendo visto como uma tecnologia inovadora, capaz de afetar positivamente vários mercados.
Bitcoin	Primeira criptomoeda desenvolvida. Surgiu após a crise de 2008. É descentralizada e funciona de forma par-a-par (peer-to-peer). Desde sua criação ocupa o posto de principal criptomoeda em circulação, possuindo o maior valor comercial, servindo de base para todas as outras concorrentes que surgiram com o tempo.

Fonte: o autor, adaptado de Maciel (2018, p. 65)

3 Aplicação de Blockchains em sistemas IoT

Conhecendo o conceito por trás de um sistema *blockchain* e reconhecendo os dispositivos encontrados em um sistema IoT, pode-se criar um cenário que una as duas tecnologias.

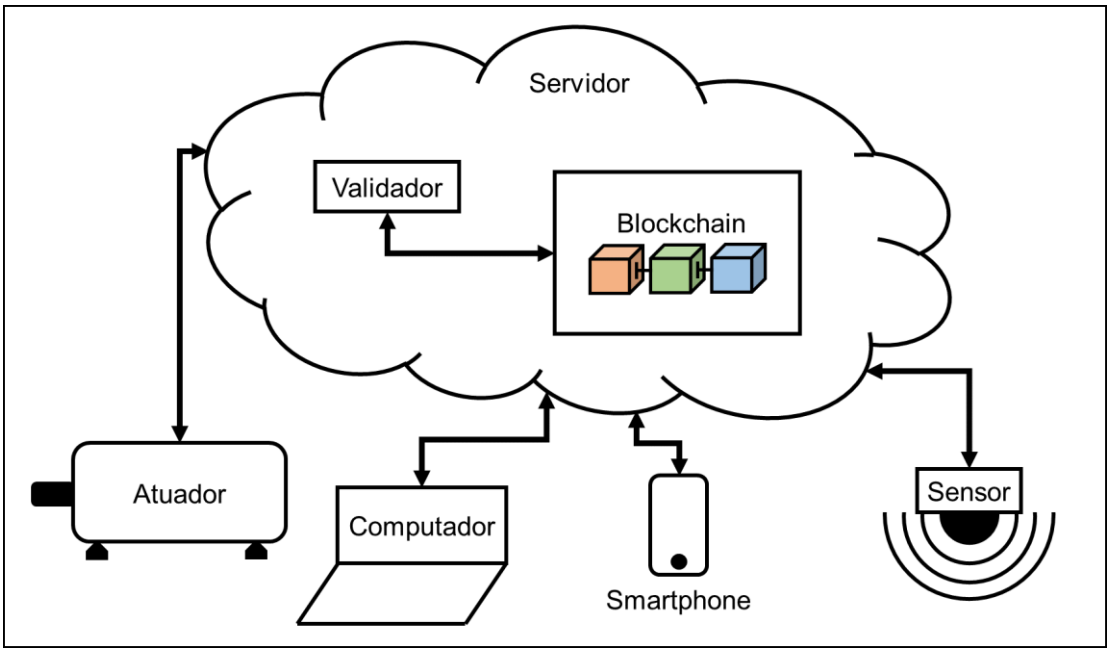
O cenário deste sistema é elaborado pensando-se em uma organização privada. Por ser uma empresa, imagina-se que os recursos disponíveis (financeiros, de *hardware* e de armazenamento) serão empregados em quantidade suficiente para o funcionamento da rede. Desta maneira, não é preciso que seja criada nenhuma forma de recompensa para mineradores externos à organização para realizarem as provas-de-trabalho, tendo em vista que o benefício almejado pela mineração é o pleno funcionamento do sistema. Considera-se que todos os elementos presentes nesta rede possuem poder de processamento e armazenamento capazes de realizar uma prova-de-trabalho.

Para tornar o sistema mais flexível e evitar que os nós da rede contenham uma cópia completa do *blockchain*, que a cada novo bloco fica maior e mais pesado,

propõe-se utilizar o armazenamento dos dados em nuvem. O servidor fica então responsável por armazenar o conteúdo do *blockchain* e disponibilizá-lo a todos os demais nós da rede.

Na Figura 9 apresentam-se os elementos presentes neste cenário: servidor, sensores, atuadores e demais aparelhos eletroeletrônicos que sejam capazes de se conectar à internet. Os nós apresentados não são excludentes, ou seja, podem participar da rede realizando mais de um papel, dependendo da aplicação.

Figura 9 – Sistema IoT Empregando *Blockchain*



Fonte: o autor (2019)

As características de cada um dos elementos neste sistema são descritas a seguir.

O *servidor* fica responsável por disponibilizar o *timestamp*, armazenar uma cópia completa do *blockchain* e validar os blocos enviados a ele, testando se o *hash* gerado pelos demais elementos é autêntico. Sendo aceito, o bloco entra no *blockchain*. Caso ocorra uma colisão de blocos, o servidor fica com o primeiro bloco que chegar. Além disso o servidor informa aos nós da rede se o bloco submetido à sua aprovação foi aceito. Caso o bloco não tenha sido validado, o componente deve realizar uma nova prova-de-trabalho para os seus dados.

O sensor mede as grandezas físicas do ambiente durante um período pré-determinado, por exemplo a cada hora, e armazena estes dados, inserindo-os em um

bloco na região destinada aos dados. Deve então solicitar ao servidor o *timestamp* e o *hash* do último bloco validado e colocá-los no bloco. Logo após, o sensor tem de realizar a prova-de-trabalho. Ao encontrar um *hash* que inicie com quatro dígitos zero, por exemplo, o sensor deve submeter o *hash* encontrado para validação pelo servidor. Caso o bloco não tenha sido validado, o sensor recebe a notificação e reinicia o ciclo, pegando os dados que ainda não foram aceitos e acrescentando-os aos novos dados coletados para criação de um novo bloco.

Os *aparelhos eletroeletrônicos*, como computadores e *smartphones*, ficam responsáveis por realizar a interface do sistema, através de um aplicativo, com os usuários que desejam monitorar os dados presentes no *blockchain*. Esses usuários também podem executar comandos nos atuadores e visualizar dados dos sensores pelo aplicativo. Para tanto, todas as instruções solicitadas pelos usuários devem seguir um procedimento análogo ao realizado pelo sensor: o comando deve entrar em um bloco na área destinada aos dados; o aplicativo solicita ao servidor o *timestamp* e o último *hash* válido; realiza a prova-de-trabalho; submete ao servidor e aguarda mensagem de validação. Caso seja necessário realiza-se uma nova prova-de-trabalho, até que seu comando seja incluído no *blockchain*.

O atuador monitora o *blockchain* para realizar operações após receber ordens de um bloco recém inserido no *blockchain*.

4 Resultados e discussão

A segurança de dados proporcionada pelo modelo apresentado neste estudo reflete diretamente na segurança física das pessoas envolvidas em sistemas de IoT. Objetos IoT invadidos por pessoas ou computadores maliciosos fazem com que estes aparelhos respondam de maneira imprevisível e diferente da planejada por seus detentores (usuários), ficando o real controle destes dispositivos sob a custódia dos invasores. Desde que combinados com equipamento de processamento digital de dados, estes objetos tornam-se capazes de utilizar a tecnologia Blockchains e, consequentemente, prevenir perda de controle e de dados.

A confiança nos dados armazenados pelo modelo, advinda do uso de *blockchains*, agrega valor a todos os componentes envolvidos no processo. Saber que as probabilidades de fraudes foram minimizadas permite a tomada de decisões

assertivas por parte dos gestores desta classe de sistemas e garante retornos financeiros.

Este modelo pode ser empregado em ambientes absolutamente diversos e complexos. A seguir elucidam-se algumas das possibilidades de aplicação da tecnologia e os elementos que podem incorporar as características requeridas para unir IoT e *blockchain*.

O primeiro exemplo é o de uma casa inteligente (*Smarthouse)*. Nessa casa conectada os usuários controlam os elementos de automação presentes em cada ambiente, tanto sensores quanto atuadores, através de um *smartphone*. Pode-se ter diversos tipos de sensores nesta casa: de chuva, de luminosidade, de temperatura, de presença, câmeras de segurança. Entre os possíveis atuadores estão: equipamentos para abrir e fechar cortinas, controles de iluminação e aquecimento de piscinas, varais de roupas retráteis, travamento e destravamento e abertura e fechamento de portas e portões, equipamentos para aquecimento e vibração de camas, sistemas de som, operação de micro-ondas e geladeiras, dentre outros.

A possibilidade de criar ambientes altamente controlados, capacita o setor industrial como um ambiente propício à implementação do modelo de *Smartindustries*. Na indústria estão presentes inúmeros tipos de sensores, tais como: indutivos, capacitivos, fotoelétricos, lasers, ultrassônicos, magnéticos, de pressão, de posição, de imagem. O monitoramento de máquinas conectadas em rede local contribui para o gerenciamento das operações, controle de processos, e a realização das manutenções periódicas e preventivas destes equipamentos evitando paradas desnecessárias que oneram o processo produtivo. Como exemplo de atuadores empregados na indústria tem-se: hidráulicos, pneumáticos e elétricos, controlando esteiras, comportas, motores, braços robóticos, sistemas de aquecimento e refrigeração citando apenas os mais comuns, mas a lista é extensa.

Com a automatização de processos, os gestores ficam focados no planejamento da indústria, supervisionando e controlando os resultados para alcançar maiores qualidade e produtividade com menores custos.

Com o agronegócio forte no Brasil e a ampliação de investimentos na agricultura de precisão, o uso de IoT com *blockchains* se encaixa perfeitamente visando a segurança dos dados coletados no campo. São as chamadas *Smartfarms* que passam a fazer uso intensivo da tecnologia para aumento da produtividade. O uso de máquinas e equipamentos autônomos no campo está isento de uma série de

ISSN: 2595-5942

questões legais e éticas, uma vez que para tratores ou colheitadeiras operarem sem intervenção humana, não é necessário se cumprir os mesmos requisitos impostos, por exemplo, aos veículos autônomos que trafegam em vias públicas. No campo não há semáforos, cruzamento de ruas e pedestres, sendo que a operação de uma máquina agrícola no campo pode ser planejada nos escritórios da indústria agrícola com uso de simuladores. Poucas variáveis externas atuam nessas operações de campo que necessitam intervenções, simplificando significativamente a lógica de controle dos sistemas de automação.

Os sensores mais comuns, aplicados à área agrícola são, por exemplo, os usados em micro estações meteorológicas como os sensores de velocidade usados em anemômetros, os de temperatura dos termômetros, medidores de pressão atmosférica, de umidade dos pluviômetros, sensores de acidez e alcalinidade dos pHmetros, sensores de luzes infravermelhas e ultravioletas. Processos que podem ser beneficiados pela tecnologia IoT associada aos *blockchains* são, por exemplo, para o controle de irrigação através da coleta de dados do estado hídrico das áreas de plantio, e o estado nutricional das plantas; a detecção de plantas daninhas e de pragas por exemplo, por análise de imagens coletadas por *drones,* a contagem e seleção de grãos por forma e cor, dentre outros.

Apesar do foco deste estudo ter sido no uso das tecnologias de IoT com *blockchains* no contexto das organizações privadas, este modelo teórico pode ser empregado em cidades inteligentes, as *Smartcities*. Diferentemente do contexto das agroindústrias, as cidades possuem alto grau de complexidade e variedade em seus ambientes e processos a serem automatizados, demandando ainda maior segurança das transações envolvidas entre os dispositivos interconectados.

Visando principalmente a mobilidade urbana, a segurança e o saneamento básico, tem-se como exemplo de sensores para coleta de dados: para medição do nível do leito de córregos e rios, para monitoramento de gás encanado, para controle de iluminação pública, para monitoramento de ambientes, alarmes de terremotos e desmoronamentos, controle de distribuição de água e de coleta de esgotos, e para controle de qualidade da geração e da distribuição de energia elétrica. Como exemplo de atuadores para as *smartcities* lista-se as lâmpadas de led, os sinalizadores para controle de tráfego (semáforos, painéis de informação, indicadores visuais dinâmicos), válvulas de controle de fluxo, bombas de reservatórios d'água, sirenes, e alguns dos citados no uso por *smartfarms* especialmente os de monitoramento climático.

ISSN: 2595-5942

Considerações finais

Ao longo do desenvolvimento deste trabalho foram apresentados o conceito e as características de funcionamento dos *blockchains,* como as suas características construtivas e os desafios que permeiam a sua implantação. O uso do *blockchain* em criptomoedas fez com que transações financeiras virtuais se tornassem mais seguras e transparentes.

A massificação de aparelhos conectados à internet e o aumento considerável no poder de processamento e armazenamento realizado por estes, facilitaram o desenvolvimento de diversas soluções que antes ficavam restritas à imaginação de entusiastas por tecnologia. Entretanto esta alta taxa de conectividade também trouxe diversos riscos à segurança dos dados envolvidos.

Este trabalho surgiu a partir da reflexão de se agregar as qualidades de segurança do *blockchain* com a alta conexão apresentada pelos dispositivos IoT. Originalmente foi idealizado o desenvolvimento de um protótipo que contemplasse a implementação de *blockchain* e IoT, para testar efetivamente o seu uso. Todavia durante as pesquisas realizadas foi constatado que a aplicação do modelo teórico apresentado neste trabalho é extensa e relativamente complexa tendo sido necessário reduzir o escopo da pesquisa aos aspectos conceituais da aplicação de *blockchains* à IoT.

Apesar de ter sido verificada a viabilidade conceitual de utilização da tecnologia para segurança de transações entre dispositivos de IoT, é necessário aprofundamento no detalhamento das especificações técnicas dos equipamentos disponíveis no mercado que suportem a implementação da tecnologia, para analisar a viabilidade técnica e econômica de sua aplicação na mitigação de riscos. Fica, assim, como sugestão de trabalhos futuros aos interessados neste tema, a aplicação dos conceitos discutidos, implementando o modelo apresentado na construção de um protótipo real, para testar e verificar a viabilidade da associação da tecnologia Blockchains aos sistemas de IoT, inclusive com a possibilidade de mensuração dos custos envolvidos neste processo.

As tecnologias apresentadas neste trabalho possuem material bibliográfico publicado majoritariamente na língua inglesa, existindo um amplo campo de estudos e compartilhamento de conhecimento no contexto das pesquisas acadêmicas e científicas brasileiras.

ISSN: 2595-5942

Referências

BARB, Edson. **Get started with the Internet of Things in your organization:** Introducing the Microsoft Azure Internet of Things Suite. Redmond: Microsoft Corporation, 2015. 7 p.
BUYYA, Rajkumar; DASTJERDI, Amir Vahid. **Internet of Things:** Principles and Paradigms. 1 ed. Cambridge: Elsevier, 2016. 354 p.

DWORK, Cynthia; NAOR, Moni. **Pricing via Processing or Combatting Junk Mail.** www.hashcash.org/papers/, [S. l.], p. 1-11. 1992. Disponível em: www.hashcash.org/papers/pvp.pdf. Acesso em: 2 out. 2019.

GOOGLE. **Google Trends: bitcoins.** Disponível em:<https://trends.google.com/trends/explore?date=2009-01-01%202019-11-12&q=bitcoin>. Acesso em 12.nov.2019a.

_____. **Google Trends: IoT.** Disponível em: <https://trends.google.com/trends/explore?date=2009-01-01%202019-11-12&q=Iot>. Acesso em: 12.nov.2019b.

_____. **Google Trends: blockchain.** Disponível em: <https://trends.google.com/trends/explore?date=2009-01-01%202019-11-12&q=blockchain>. Acesso em: 12.nov.2019c.

_____. **Google Trends: IoT, Blockchain, e Bitcoin.** Disponível em: <https://trends.google.com.br/trends/explore?date=2009-01-01%202019-10-22&q=IoT,Blockchain,Bitcoin>. Acesso em: 12.nov.2019d.

GROOVER, Mikell P.; WEISS, Mitchell; NAGEL, Roger N.; ODREY, Nicholas G. **Robótica:** Tecnologia e Programação. 1 ed. São Paulo: McGraw-Hill, 1988. 401 p.

MACIEL, Felipe A. **Introdução às Criptomoedas: uma análise de possíveis impactos na Economia, Investimentos e Contabilidade.** 2018. Disponível em: <>. Acesso em: 12.nov.2019.

McEWEN, Adrian; CASSIMALLY, Hakim. **Designing the Internet of Things.** Chichester: John Wiley And Sons, Ltd., 2014. 324 p.

NAKAMOTO, Satoshi. **Bitcoin:** A Peer-to-Peer Electronic Cash System. www.bitcoin.org, [S. l.], p. 1-9. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 31 set. 2019.

PFISTER, Cuno. **Getting Started with the Internet of Things.** Sebastopol: O'reilly Media, 2011. 176 p.

SCHWAB, Klaus. **The Fourth Industrial Revolution.** Cologny / Geneva: World Economic Forum, 2016. 172 p.

STEVAN JUNIOR, Sergio L.; SILVA, Rodrigo A. **Automação e Instrumentação Industrial com Arduino:** teoria e projetos. 1 ed. São Paulo: Érica, 2015. 296 p.

ZHENG, Zibin; *et al.* **An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.** 2017. IEEE 6th Internation Congress on Big Data. Disponível em: <https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends>. Acesso em 12.nov.2019.