Internet das Coisas e Blockchain: segurança e disponibilidade em redes de dispositivos conectados

Robson de Sousa Martins

Tema: Infraestrutura Tecnológica de Sistemas e Serviços

Nº de páginas: 23

Folha de Rosto

Título do Trabalho: Internet das Coisas e Blockchain: segurança e disponibilidade em redes de dispositivos conectados

Tema: Infraestrutura Tecnológica de Sistemas e Serviços

Autor: Robson de Sousa Martins

Currículo: Robson de Sousa Martins é MBA em Desenvolvimento de Soluções Corporativas em Java/SOA, pela Faculdade de Informática e Administração Paulista (FIAP) e Bacharel em Sistemas de Informação, pela Faculdade Batista de Administração e Informática (FBAI). Atuou durante sete anos como Técnico Eletrônico, em projetos de sinalização metroferroviária e manutenção eletrônica, e dez como Analista Programador, no desenvolvimento de *softwares* comerciais. Ingressou no Serpro em 2010, em São Paulo, onde atuou em projetos como o ALM (*Application Lifecycle Management*), ECM *Alfresco* (Processo Verde), BPMS (*Business Process Management Suite*), Sistemas Denatran e SIC/SIEF. Atualmente lidera o grupo de estudo do eixo IoT (*Internet of Things*) no Serpro.

Resumo

É inegável que dispositivos conectados, com sensores, medidores e atuadores estão se tornando comuns nas aplicações de cidades inteligentes, logística, controle predial, gestão energética, saúde pública, agricultura, dentre outras, ao redor do mundo. Sendo assim, acompanhando essa evolução na gestão pública, o Serpro assume o importante papel de norteador dessas tecnologias no país, e, como sempre, preocupado em fornecer soluções com garantia de disponibilidade e total segurança das informações. A proposta de utilizar um modelo de rede distribuído e que oferece confiança entre os pontos – como é o *blockchain*, para fundamentar a comunicação de dispositivos inteligentes – IoT (Internet das Coisas), traz uma alternativa técnica viável e de boa aplicabilidade às novas soluções desenvolvidas pelo Serpro. A ideia é oferecer recursos fundamentais de infraestrutura para a implantação de soluções e serviços com Internet das Coisas, garantindo disponibilidade e segurança das informações. A implantação bem-sucedida desse tipo de solução, além de trazer mercados para novos negócios, e consequente aumento de receitas para o Serpro, também ratifica a empresa em seu notório e já reconhecido compromisso com a segurança da informação. Assim sendo, o Serpro tem a oportunidade de demonstrar seu alinhamento com a inovação tecnológica, em favor da gestão pública eficiente.

Palavras-chave: Internet das Coisas; *Blockchain*; Redes; Infraestrutura; Segurança; Disponibilidade; *Smart Contracts*.

Lista de ilustrações

Lista de abreviaturas e siglas

HTTPS: *Hyper Text Transfer Protocol Secure* (Protocolo Seguro de Transferência de Hipertexto).

IoE: *Internet of Everything* (*Internet* de Tudo).

IoT: *Internet of Things* (*Internet* das Coisas).

M2M: *Machine To Machine* (Máquina para Máquina).

MQTT: *Message Queue Telemetry Transport*.

P2P: *Peer To Peer* (Ponto a Ponto).

REST: *Representational State Transfer* (Transferência de Estado Representacional).

Serpro: Serviço Federal de Processamento de Dados.

TIC: Tecnologia de Informação e Comunicação.

Sumário

Introdução

> Se tivéssemos computadores que soubessem tudo sobre as coisas em geral – usando dados que coletassem sem a nossa ajuda – seríamos capazes de rastrear e contar tudo, e reduzir bastante o desperdício, a perda e os custos. Nós saberíamos quando é necessário substituir, reparar ou fazer um *recall* de um produto, e se estão novos ou ultrapassados. Precisamos capacitar os computadores com seus próprios meios de coletar informações, para que possam ver, ouvir e cheirar o mundo sozinhos, com toda a sua glória aleatória (ASHTON, 2009, tradução nossa).

Kevin Ashton, ao fim dos anos 90, durante suas pesquisas na Procter & Gamble, vislumbrou um mundo onde todas as coisas poderiam estar conectadas, fornecendo dados para melhorar nossos processos do dia a dia. Assim nasceu o conceito de Internet das Coisas (*Internet of Things*), ou simplesmente IoT. Essa ideia foi bastante avançada à época, já que não havia tecnologia suficiente para materializar tal conectividade. Não haviam processadores pequenos o suficiente para serem embarcados nos objetos. As fontes de energia eram grandes e ineficientes. As redes sem fio eram lentas e caras, e não cobriam grandes áreas.

Hoje, muitas dessas barreiras foram superadas. A evolução tecnológica diminuiu o custo, reduziu o volume, aumentou o desempenho de dispositivos eletrônicos. Redes de curta e longa distância cobrem áreas espalhadas pelo planeta, com uma performance nunca antes imaginada. Protocolos como IPv6 permitem o endereçamento de bilhões de dispositivos numa rede como a Internet. Nuvem e virtualização ajudam a gerenciar servidores de aplicação.

Sendo assim, IoT tem crescido em pouco tempo, assumindo proporções exponenciais. O Grupo de Internet das Coisas da Cisco (IoTG) prevê que haverá mais de 50 bilhões de dispositivos conectados em 2020 (EVANS, 2011).

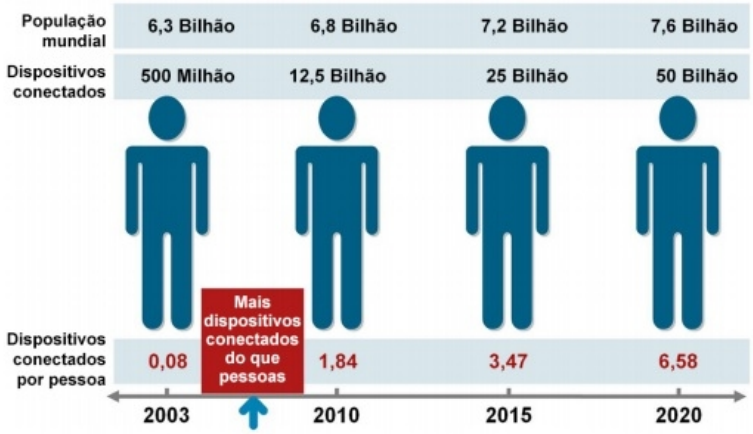

Figura 1 – Crescimento de Internet das Coisas (IoT) no mundo
Fonte: EVANS, 2011 (tradução nossa)

Porém, junto ao crescimento vertiginoso de IoT, cresce a demanda por soluções confiáveis, disponíveis e seguras, já que esse se torna um gargalo evidente nas aplicações onde bilhões de dispositivos trocam informações. Este trabalho se propõe a demonstrar uma alternativa tecnológica para a infraestrutura de aplicações IoT que requeiram exatamente as características de disponibilidade e segurança (confiabilidade).

Internet das Coisas (IoT)

A Internet das Coisas (em inglês, *Internet of Things*), conhecida pela sigla IoT, é basicamente a capacidade conferida a diferentes objetos de se comunicar através de redes interligadas (por exemplo, a *Internet*) com a finalidade de interagir com o ambiente físico ao seu redor, por meio de sensoriamento e atuação, ou seja, reação a eventos (MATTERN; FLOERKEMEIER, 2010). Com isso, a *Internet* se expande para além do conceito de apenas "computadores conectados em uma grande rede mundial" (TANENBAUM; WETHERALL, 2011), mas algo próximo ao definido por alguns autores como IoE (*Internet of Everything*, ou Internet de Tudo), que engloba a conexão inteligente de pessoas, objetos, dados e processos (CISCO, 2014).

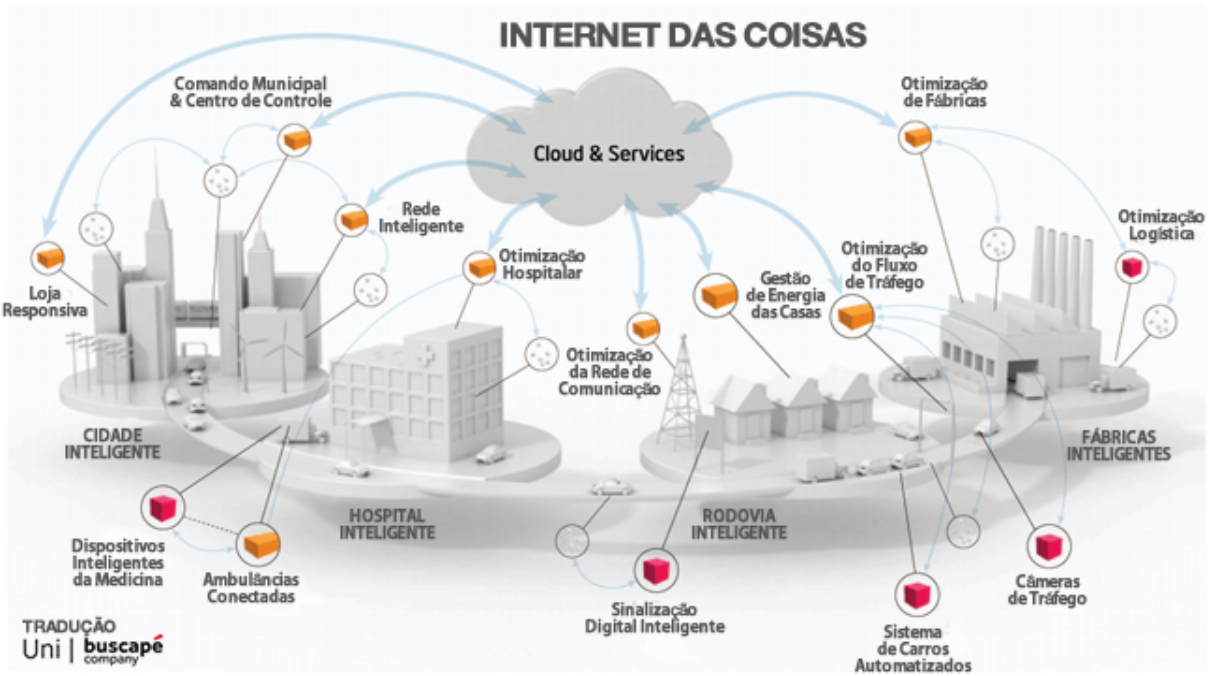

Figura 2 – Internet das Coisas (IoT)
Fonte: SATIZ, 2015 (tradução: UNIBUSCAPÉ, 2015)

A IoT surgiu a partir dos avanços de várias áreas, como microeletrônica, telecomunicações, sensoriamento e processamento de sinais, computação em

nuvem e sistemas embarcados. Além disso, outras tecnologias, como inteligência artificial, computação cognitiva, *data warehouse* (extração e mineração de dados), são também comumente associadas a aplicações de IoT.

De fato, IoT tem recebido bastante atenção tanto da academia quanto da indústria (GARTNER, 2016), devido ao seu potencial de uso nas mais diversas áreas da atividade humana.

Alguns autores (ASHTON, 2009; FORBES, 2014; WANG et al., 2015) apontam que a IoT é a nova revolução da Tecnologia da Informação e Comunicação (TIC). Sendo assim, a IoT possivelmente deva ser encarada como um meio de alcançar algo maior, como a computação ubíqua (computação presente em todos os lugares, de forma transparente, a serviço da humanidade).

Arquitetura

Uma típica aplicação de IoT apresenta uma arquitetura basicamente formada por alguns elementos (ELIZALDE, 2015):

- Os objetos ("*things*"), também conhecidos como "*smart objects*", contém algum tipo de dispositivo (*device*) de *hardware* e um *software* embarcado, e possuem a função de receber estímulos do ambiente, processar esses estímulos, atuar no ambiente, e ainda transmitir ou receber informações remotamente por uma rede.
- Uma plataforma de comunicação, composta por módulos de *hardware*, *software*, protocolos de rede, equipamentos como *gateways* e outros. Sua finalidade é possibilitar a conectividade dos objetos ("*things*").
- Uma plataforma remota, especialmente via *Internet*, e em nuvem (*cloud*), que tem por finalidade realizar a comunicação com os objetos ("*things*") e abrigar as aplicações baseadas nos dados obtidos/enviados a esses objetos.

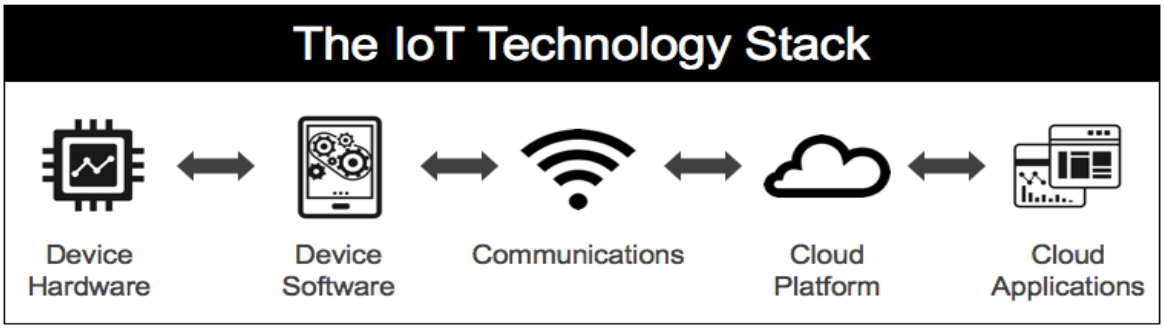

Figura 3 – Arquitetura básica de IoT
Fonte: ELIZALDE, 2015

Desafios

A adoção de IoT está crescendo significativamente no mundo, o que produz uma demanda exponencial por mais dispositivos conectados. Esse ritmo de crescimento acelerado expõe cada vez mais os usuários dessas soluções a problemas que devem ser encarados como verdadeiros desafios-chave para a utilização da tecnologia. Alguns desses desafios:

- **Escalabilidade**: toda a infraestrutura de Internet das Coisas deve suportar o aumento exponencial de dispositivos conectados. Soluções baseadas em nuvem (*cloud*) centralizadas, cujo roteamento de mensagens se dá através de um único nó, podem ser um gargalo para a ampliação da capacidade de operação.
- **Segurança**: milhões de dispositivos cada vez mais relevantes, enviando e recebendo dados através de uma rede interconectada, geram um volume de dados crítico para seus usuários. A proteção desses dados, de sua privacidade, e de sua autenticidade, é preocupação para cidadãos, governos e corporações. Na atualidade, são comuns dispositivos de baixo custo, projetados sem o mínimo cuidado com a segurança, sendo alvo de ataques e invasões.
- **Falta de padronização**: enquanto fornecedores de soluções IoT aplicam técnicas proprietárias para aprimorar seus produtos, problemas como falta de interoperabilidade provocam um grande desafio para a tecnologia.
- **Custo**: IoT envolve dispositivos de *hardware*, *software* embarcado e equipamentos de rede, além de toda infraestrutura necessária para as aplicações. É portanto, um desafio enorme equalizar “custo x segurança”, por exemplo – mais segurança implica maior poder de processamento, *software* melhor elaborado e testado, infraestrutura mais robusta, etc., o que resulta em elevação de custo.
- **Arquitetura**: modelos baseados em centralização (mesmo que em nuvem) implicam gargalos para a disponibilidade. A qualidade e a estabilidade das conexões (telecomunicações) também representam um desafio para IoT, especialmente nas arquiteturas exclusivamente *online* ou em tempo real.

Blockchain

O *blockchain* é uma base distribuída de dados, que mantém uma lista encadeada de registros (conhecidos como blocos), e que funciona sobre uma arquitetura P2P (*Peer To Peer* – ou Ponto a Ponto).

Blockchain foi uma proposta de Satoshi Nakamoto (codinome), como solução para viabilizar uma rede de transações financeiras de uma moeda virtual, conhecida como Bitcoin (NAKAMOTO, 2008).

O Bitcoin é uma criptomoeda, pois tem sua existência fundamentada em conceitos criptográficos como funções *hash*.

O *blockchain* está fundamentado em uma rede distribuída, onde todos seus membros são nós, e têm visibilidade das transações efetuadas. Não há um agente centralizador na arquitetura. Assim, sem um mediador central, as relações de confiança são executadas colaborativamente pelos nós.

Para que essa base distribuída funcione da maneira proposta, a lista encadeada de blocos conta com funções criptográficas de mão única (assinatura *hash*), registro do tempo da criação ou modificação (*timestamp*), assinatura digital do autor, rede descentralizada P2P, e mecanismo de geração de um novo bloco do *blockchain*. Todos esses mecanismos garantem à arquitetura a robustez necessária, e a prevenção contra fraudes e adulterações indevidas.

As funções criptográficas de mão única (*hash*) são aquelas que permitem a operação em um sentido, mas é completamente inviável realizar no sentido oposto. Por exemplo, dado uma entrada, obtém-se uma saída única. Entradas diferentes produzem diferentes saídas. Com valores de saída, não é possível calcular valores de entrada, mesmo conhecendo de antemão o algoritmo da função. A finalidade dessas funções é tornar inviável e improvável qualquer alteração nos valores registrados no *blockchain*. A alteração de um registro implica num novo valor de *hash* para ele; implica alteração no *hash* do próximo registro, e assim subsequentemente, pois os registros estão encadeados (MATTILA, 2015; NAKAMOTO, 2008).

O registro de tempo da transação (*timestamp*) tem o objetivo de armazenar o elemento temporal de alteração no *blockchain*, evitando assim fraudes ligadas a adulteração de data/hora nas transações.

A assinatura digital visa garantir a autenticidade do proprietário do par de chaves (pública e privada) da transação, naquele determinado nó.

A rede P2P possibilita que os nós (*peers*) avaliem as informações do *blockchain* e aceitem ou rejeitem, por maioria, as alterações realizadas. Essa é a implementação da relação de confiança descentralizada.

A figura 4 traz a ilustração do *blockchain* do Bitcoin original, e mostra como um valor *hash* é calculado e um novo bloco é inserido. Conceitualmente, um bloco pode conter uma ou mais transações, organizadas numa estrutura de árvore (chamada de *Markle Tree*).

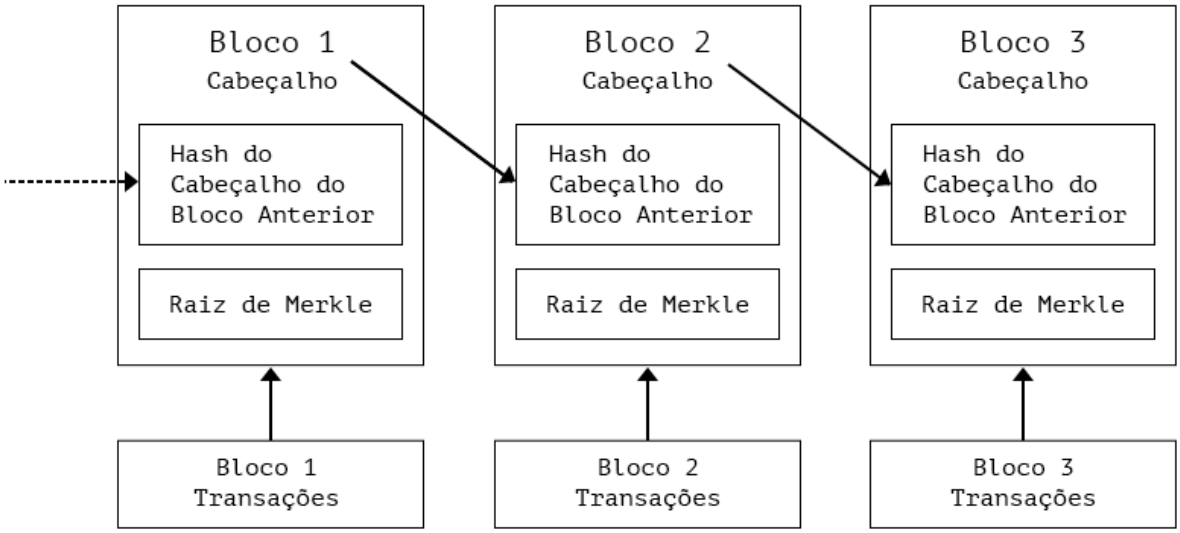

Figura 4 – Modelo simplificado do *Blockchain* do Bitcoin
Fonte: NAKAMOTO, 2008 (tradução nossa)

Uma transação tem seu *hash* calculado. Em seguida, a próxima transação tem o *hash* calculado em conjunto com o valor obtido no cálculo da transação anterior. Isso se segue até a última transação, como uma cadeia. O último *hash* calculado no processo é chamado de *Markle Root*, que está fortemente ligado aos valores e sequência de todas as transações do bloco.

Após esse processo, um *blockchain* necessita da geração de novos blocos. No caso do Bitcoin, e outras criptomoedas, esse processo se chama mineração.

A mineração consiste em uma disputa simultânea entre nós, baseada na resolução de uma função matemática, através de um processamento oneroso. O primeiro nó (*peer*) a encontrar a resposta, tem o direito de criar o bloco, inserir e validar as últimas transações dos outros nós, e ainda receber uma recompensa pelo esforço computacional (uma porção ou taxa de criptomoedas).

Aplicações

Apesar de *blockchain* surgir no contexto de criptomoedas (como o Bitcoin), sua aplicação não está restrita a transações financeiras. Outras áreas têm utilizado o conceito de redes P2P e bases de dados distribuídas em cadeia de confiança como incremento para suas aplicações, como armazenamento de dados, distribuição de mídias, gerência de contratos, administração de propriedade material ou intelectual, votação eletrônica ou participação colaborativa do cidadão nos governos, entidades ou federações descentralizadas, além de outras (KAR, 2016; KELLY; WILLIAMS, 2016; LACEY, 2016; MIZRAHI, 2015; OPARAH, 2016; SUBERG, 2015).

Arquiteturas

Após o surgimento do Bitcoin e do primeiro *blockchain* associado, outras arquiteturas de *blockchain* estão sendo desenvolvidas e utilizadas, como por exemplo o Ethereum.

Dentre as diferenças entre as arquiteturas, uma das mais significativas é o processo de mineração (criação de novos elementos dentro do *blockchain*).

A arquitetura do *blockchain* do Bitcoin tem alguns problemas, como o alto intervalo para confirmação das transações – aproximadamente uma hora, necessidade de um grande poder computacional na mineração – o que torna esse processo concentrado num grupo cada vez mais restrito e poderoso de usuários (HRUSKA, 2014), e o elevado consumo de energia elétrica para executar o processo – estima-se que em 2020 a mineração do Bitcoin consumirá o mesmo em eletricidade que o país da Dinamarca (DEETMAN, 2016).

Já o Ethereum foi criado como uma plataforma P2P para executar aplicações descentralizadas sobre *blockchain*, especialmente *smart contracts* (WOOD, 2014). É uma rede distribuída que se propõe a corrigir muitos dos problemas encontrados no *blockchain* do Bitcoin (especialmente com relação à mineração e ao tempo de validação). Para se utilizar essa plataforma, é necessário adquirir a criptomoeda criada para esse fim, chamada de Ether, cujo valor de mercado está atrás somente do Bitcoin.

Smart Contracts

Nick Szabo introduziu o conceito de *smart contract* (ou contrato inteligente) em 1994, definindo como "um protocolo computacional de transações que executa os termos de um contrato" (SZABO, 1994, tradução nossa).

De fato, Szabo sugeriu traduzir cláusulas contratuais em um código computacional, rodando sobre uma plataforma que garanta relações de confiança descentralizadas (como *blockchain*), com capacidade de autoexecutar seus termos e condições entre as partes pactuadas, sem intervenção humana ou manual (SZABO, 1997).

Smart contracts permitem implementações de pactuação entre partes independente da existência de criptomoedas, portanto inclusive em aplicações distintas da área financeira.

Setores como saúde (*healthcare*), cartórios e registro de bens, registro de patentes e propriedade intelectual, infraestrutura, órgãos de governo, dentre outros, têm encontrado aplicabilidade usando *smart contracts* sobre *blockchain* em redes distribuídas (KAR, 2016; KELLY; WILLIAMS, 2016; LACEY, 2016; MIZRAHI, 2015; OPARAH, 2016; SUBERG, 2015).

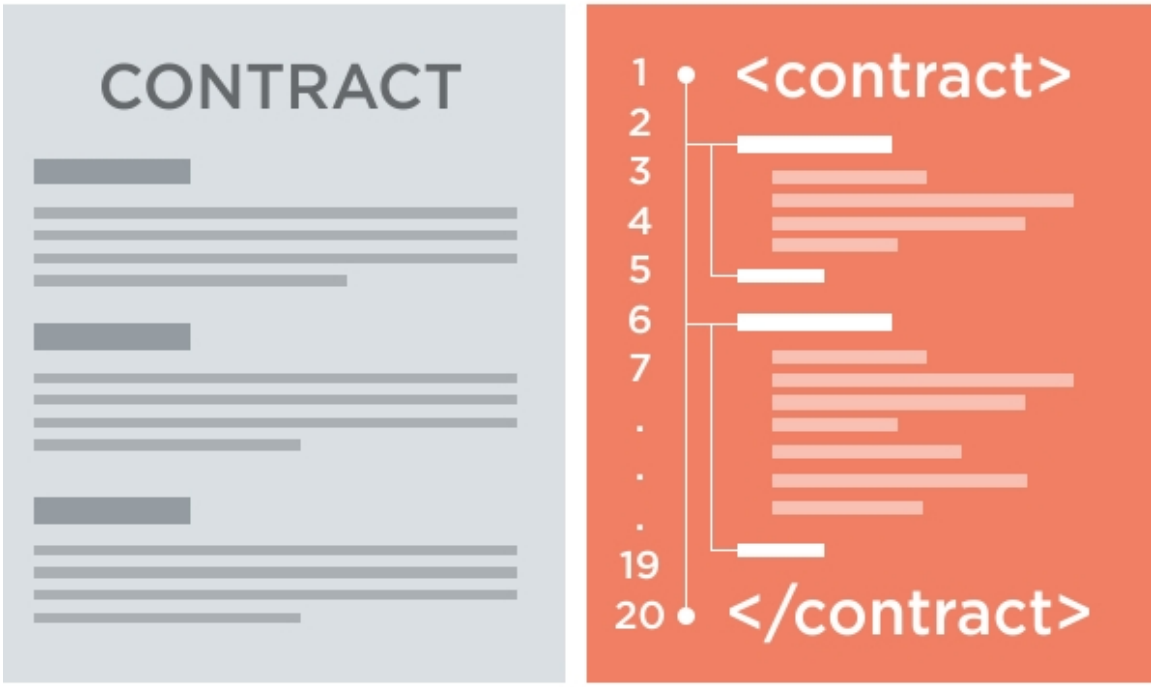

Figura 5 – *Smart Contracts*
Fonte: LEWIS, 2016

Um *smart contract* reside sobre um *blockchain*, é baseado em uma rede P2P distribuída, e contém algumas características básicas (MONAX, 2014):

- Cada *smart contract* tem seu próprio estado, e é disparado por transações inseridas no *blockchain*, e/ou por elementos como *timestamp* (carimbo de tempo) e *timeout* (data de expiração). Ele tem controle sobre a propriedade de cada registro (autoria) no *blockchain*.
- O *smart contract* permite a expressão de sua própria lógica de negócio (descrição do contrato), em linguagem de programação própria.
- Todas as condições de um contrato são expressas em sua lógica, e autoexecutadas em reação a eventos de transação ou tempo.
- Um contrato pode produzir novas transações ou disparar ações de um outro contrato encadeado.
- Um *smart contract* é determinístico: mesmas entradas produzem as mesmas saídas sempre. Um contrato não determinístico (baseado em valores aleatórios), é difícil de ser implementado, pois os nós (*peers*) têm dificuldade em validar valores diferentes resultantes de um mesmo contrato executado nos diferentes pontos.

Infraestrutura: Internet das Coisas e Blockchain

Uma típica aplicação de IoT utiliza uma arquitetura centralizada, onde os dispositivos (objetos inteligentes) são interligados a um *broker* (ponto central de comunicação), normalmente construído sobre a nuvem (*cloud*).

Como ilustrado na figura 6, as aplicações, chamadas a serviços relacionados, persistência e análise de dados (*data mining*) são conectados exatamente ao *broker* IoT, que processa as mensagens enviadas pelos dispositivos.

Esse tipo de arquitetura leva a dois problemas principais: primeiro, uma indisponibilidade do *broker* (ou dos links de comunicação entre os dispositivos e o *broker*) torna a solução momentaneamente inoperante, pois mensagens enviadas pelos/aos dispositivos são perdidas; segundo, um dispositivo invadido ou clonado pode forjar transações, e assim violar a segurança da aplicação.

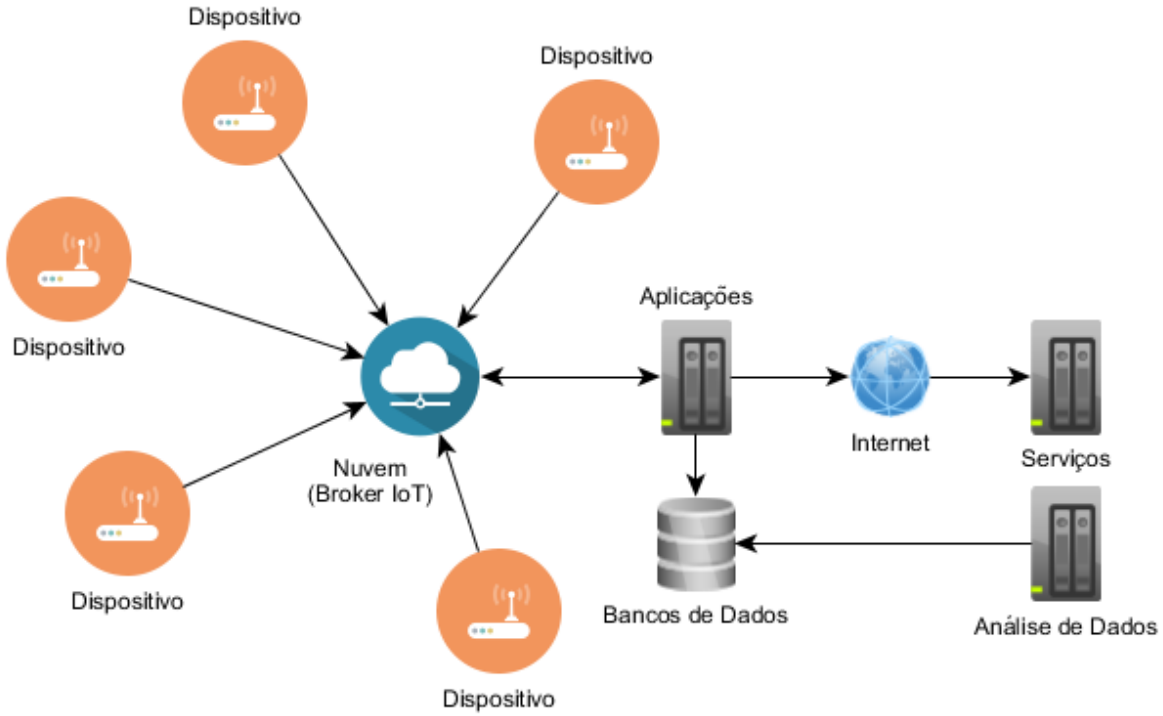

Figura 6 – Típica arquitetura IoT centralizada
Fonte: Elaboração nossa (2017)

Normalmente, para mitigar os problemas de segurança, esse tipo de arquitetura implementa mecanismos de criptografia e certificados digitais para autenticar os dispositivos IoT, exigindo um maior poder computacional de processamento embarcado nesses dispositivos.

Quanto à disponibilidade, soluções alternativas são implementadas com o uso de equipamentos intermediários de comunicação, como *gateways*, ou ainda com a replicação das funcionalidades do *broker* em mais de um ponto atingível da rede (como um servidor local secundário que realiza sincronização periódica com o principal na nuvem).

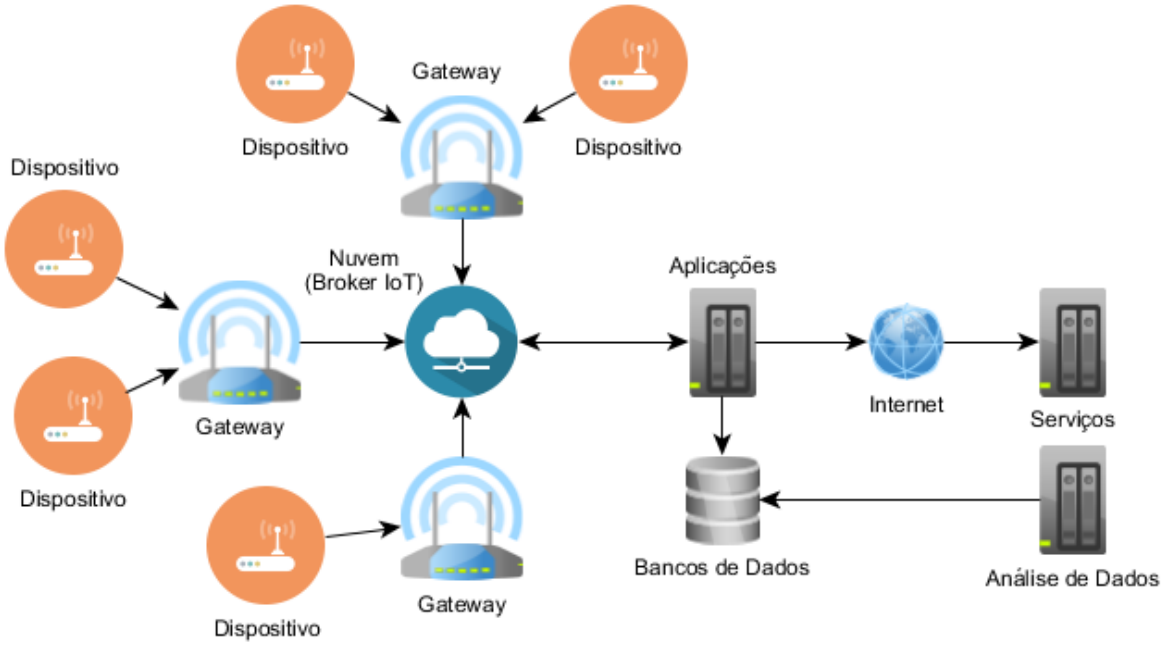

Figura 7 – Arquitetura IoT com *gateways*, centralizada
Fonte: Elaboração nossa (2017)

Ainda sim, nesse tipo de arquitetura, como demonstrado na figura 7, o *broker* IoT centraliza toda a comunicação e validação de transações entre os dispositivos da rede.

Como alternativa a esse tipo de abordagem, este trabalho propõe a utilização de *blockchain* como uma plataforma descentralizada compatível com a natureza P2P distribuída, típica de aplicações IoT.

Num primeiro cenário, cada dispositivo (objeto inteligente, ou *smart object*) se torna um nó (*peer*) de uma rede distribuída P2P, cada qual responsável por processar blocos de transações do *blockchain*.

O *broker* IoT presente na nuvem passa a ser também um nó (ou mais de um, conforme o desenho da infraestrutura) participante da mesma rede *blockchain*. Todos os nós podem criar transações (a partir de mensagens) e validar as transações de outros nós, seguindo os princípios básicos de funcionamento do *blockchain* (MATTILA, 2015; NAKAMOTO, 2008).

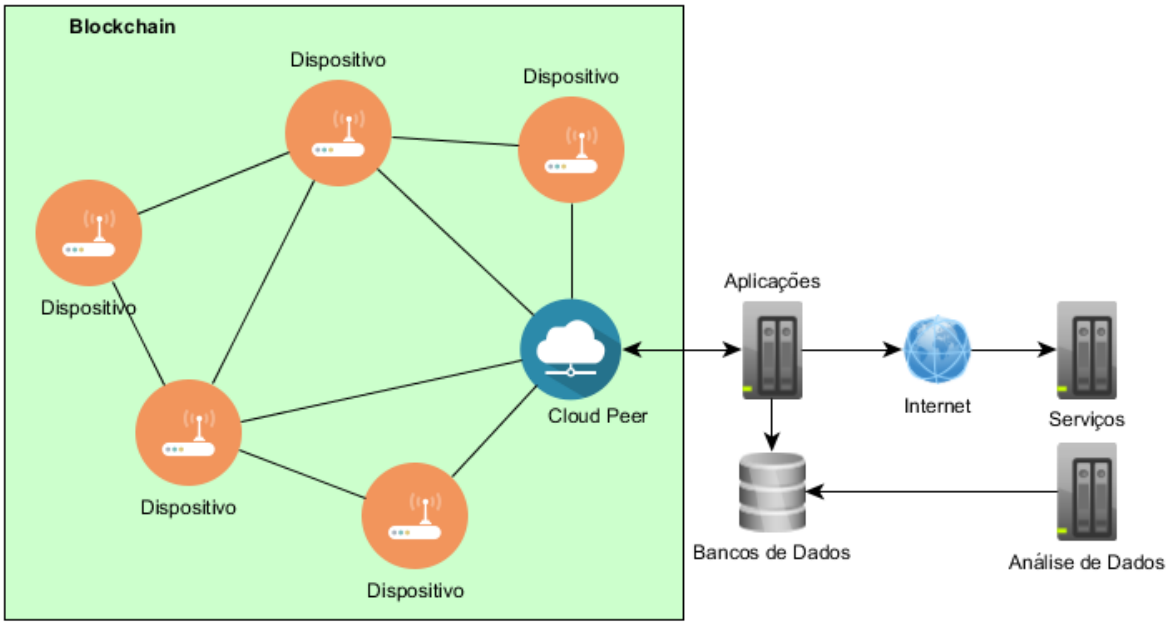

Figura 8 – Arquitetura IoT com *Blockchain*
Fonte: Elaboração nossa (2017)

Esse tipo de arquitetura garante a confiabilidade, já que transações criadas por um dispositivo precisam ser validadas pelos demais, para que sejam incorporadas ao registro de blocos. Uma tentativa de fraudar uma transação (por exemplo, por um dispositivo comprometido ou invadido) pode ser rejeitada por maioria no processo de validação próprio do *blockchain*.

Por outro lado, a disponibilidade é garantida pelo fato de não existir um centralizador na arquitetura. Um dispositivo pode se comunicar com qualquer outro, pois a rede é distribuída (P2P). Isso se assemelha às conexões M2M (*Machine To Machine* – Máquina para Máquina), típicas em arquiteturas IoT.

Entretanto, há alguns pontos críticos a considerar. O processamento de transações pelos nós implica na necessidade de poder computacional embarcado nos dispositivos. Isso nem sempre é possível em aplicações de baixo custo, ou baixo consumo de energia, onde módulos de criptografia e processadores com mais de 16 bits são completamente inviáveis.

Outra questão é a necessidade de sincronização e latência inerentes a redes P2P. Essa topologia de rede otimiza a disponibilidade, porém penaliza o tráfego em tempo real dos dados. Desta forma, aplicações críticas, como as de controle industrial, ou suporte à vida – que necessitam de transferência de dados em tempo real – não podem ser implementadas com esse tipo de arquitetura.

Para utilizar uma rede *blockchain* em conjunto com dispositivos IoT de baixo poder de processamento (ou ainda, cuja conectividade esteja baseada em protocolos de rede não-Internet, como *ZigBee*, por exemplo), um possível cenário consiste no emprego de *gateways*. Esses equipamentos devem ter um poder de processamento adequado para trabalhar com funções criptográficas, cada qual responsável pela comunicação com um (ou mais) desses dispositivos IoT, e além disso, intermediar a rede P2P do *blockchain*, processando as transações como nó (*peer*) dessa rede.

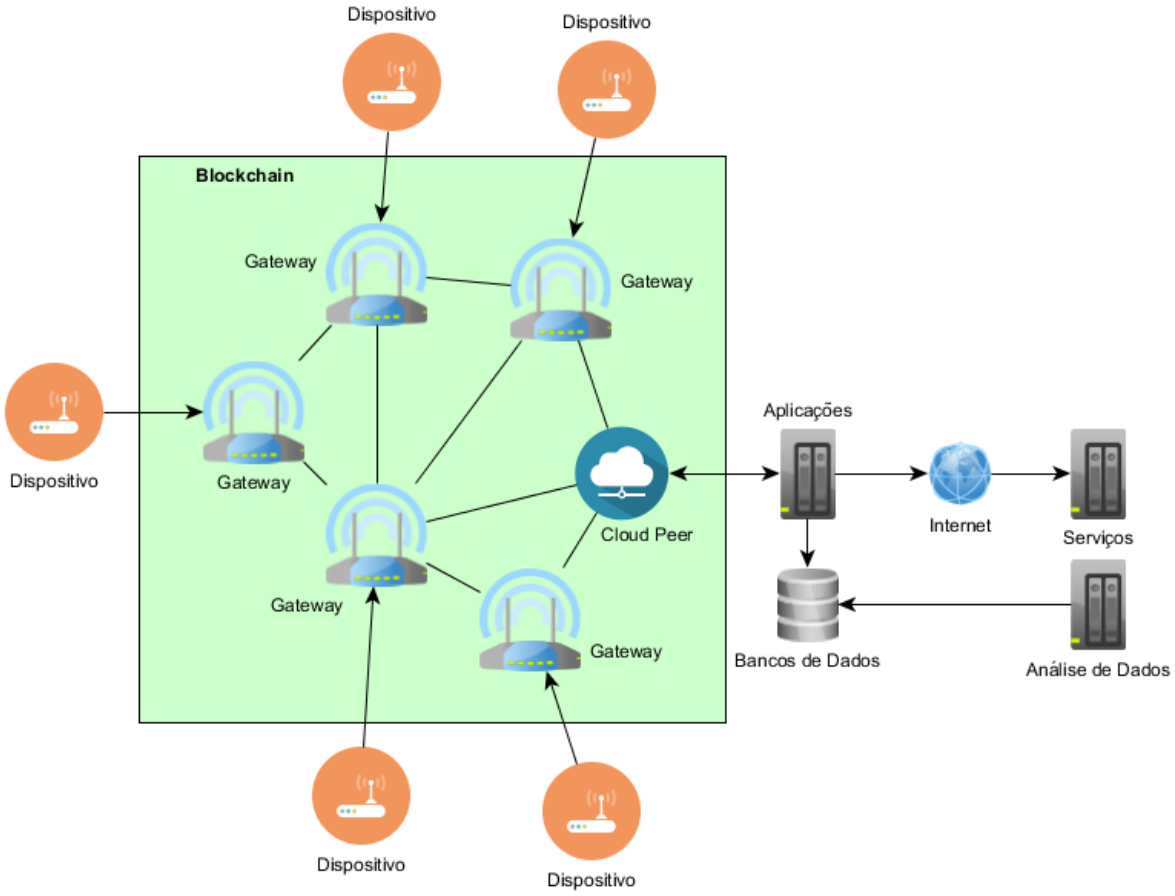

Figura 9 – Arquitetura IoT com *gateways*, usando *Blockchain*
Fonte: Elaboração nossa (2017)

Como ilustrado na figura 9, é uma responsabilidade dos *gateways* implementar os mecanismos de segurança e conectividade entre eles próprios e os dispositivos IoT nesse modelo de arquitetura.

Para se ter uma visão mais aprofundada sobre o tema, e de uma forma mais palpável, este trabalho apresenta um modelo de infraestrutura de IoT baseada em *blockchain*, com um maior detalhamento na figura 10.

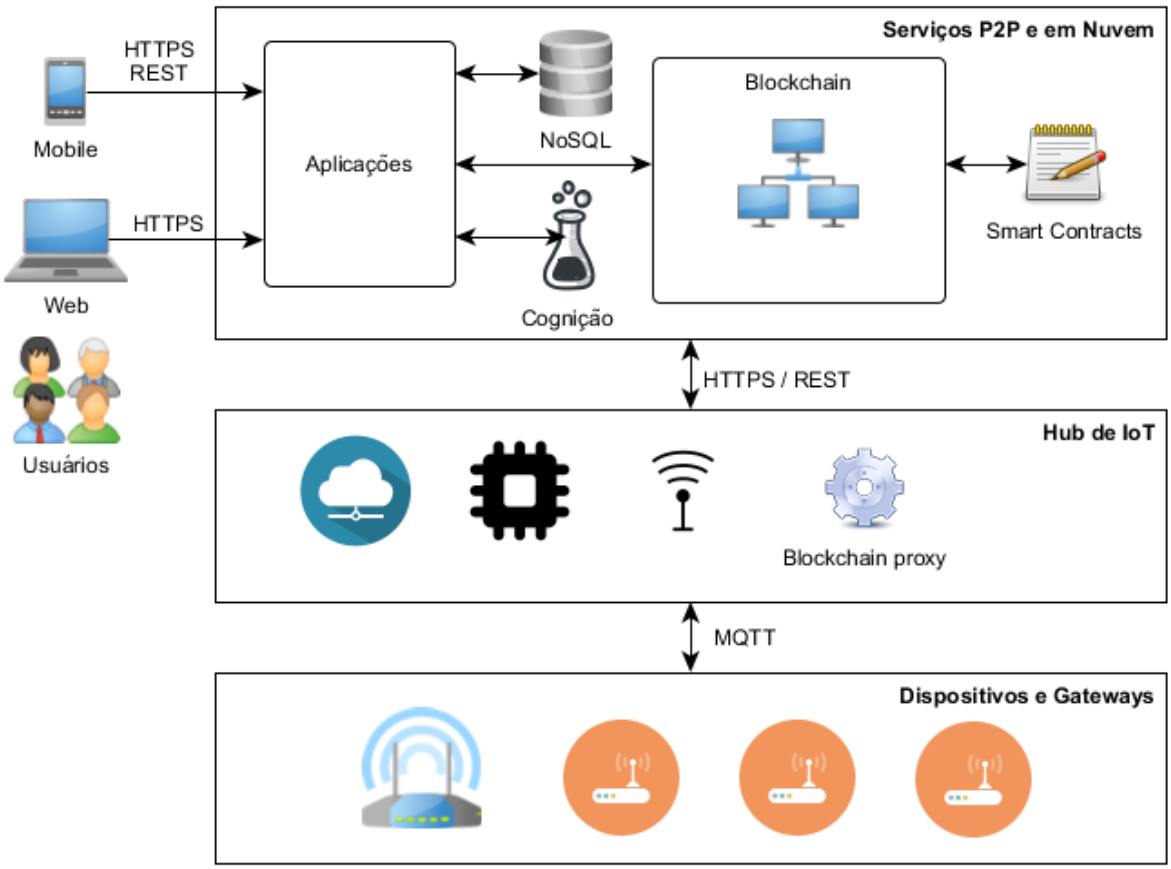

Figura 10 – Modelo de Infraestrutura para IoT com *Blockchain*
Fonte: Elaboração nossa (2017)

O modelo apresenta uma visão implementável de infraestrutura para aplicações IoT baseada em *blockchain* e *smart contracts*, detalhando inclusive algumas de suas partes componentes.

Como camada inferior, são demonstrados os dispositivos (objetos inteligentes ou *smart objects*) e *gateways* intermediários a outros dispositivos.

Normalmente esses dispositivos se comunicam por redes sem fio através de protocolos como MQTT (*Message Queue Telemetry Transport*), ou outros que tenham a mesma finalidade.

Um *Hub* de IoT é uma camada responsável por processar as mensagens recebidas/enviadas pelos dispositivos e fazer ponte (*proxy*) com o *blockchain*. Pode ser um *middleware* na nuvem, um software embarcado em um equipamento (como um *gateway*), ou mesmo um serviço rodando em equipamentos de uma rede privada (ou nuvem privada). Também pode ser implementado dentro de dispositivos IoT que possuam boa capacidade de processamento e disponibilidade energética.

O *blockchain* propriamente dito, com capacidade para executar *smart contracts*, pode ser tanto uma rede pública, como o Ethereum (WOOD, 2014), ou um *blockchain* privado, montado somente sobre nós (*peers*) dentro de uma corporação ou domínio específico.

Bancos de dados NoSQL, motores de cognição (inteligência artificial), aplicações de *big data*, *data mining*, geradores de *dashboard*, integrações entre sistemas e serviços, aplicações *web*, *mobile*, e outros elementos, ainda podem estar interligados ao *blockchain*, em uma nuvem pública, ou mesmo privada.

Exemplo de Aplicação

Como ilustração prática da aplicação de uma infraestrutura de IoT com *blockchain* e *smart contracts*, este trabalho traz um exemplo simplificado, baseado em cadeia logística (*supply chain*), de forma mais específica sobre o transporte de mercadorias via porto, desembarque de contêineres, e distribuição dos produtos nos pontos de venda, conforme apresentado na figura 11.

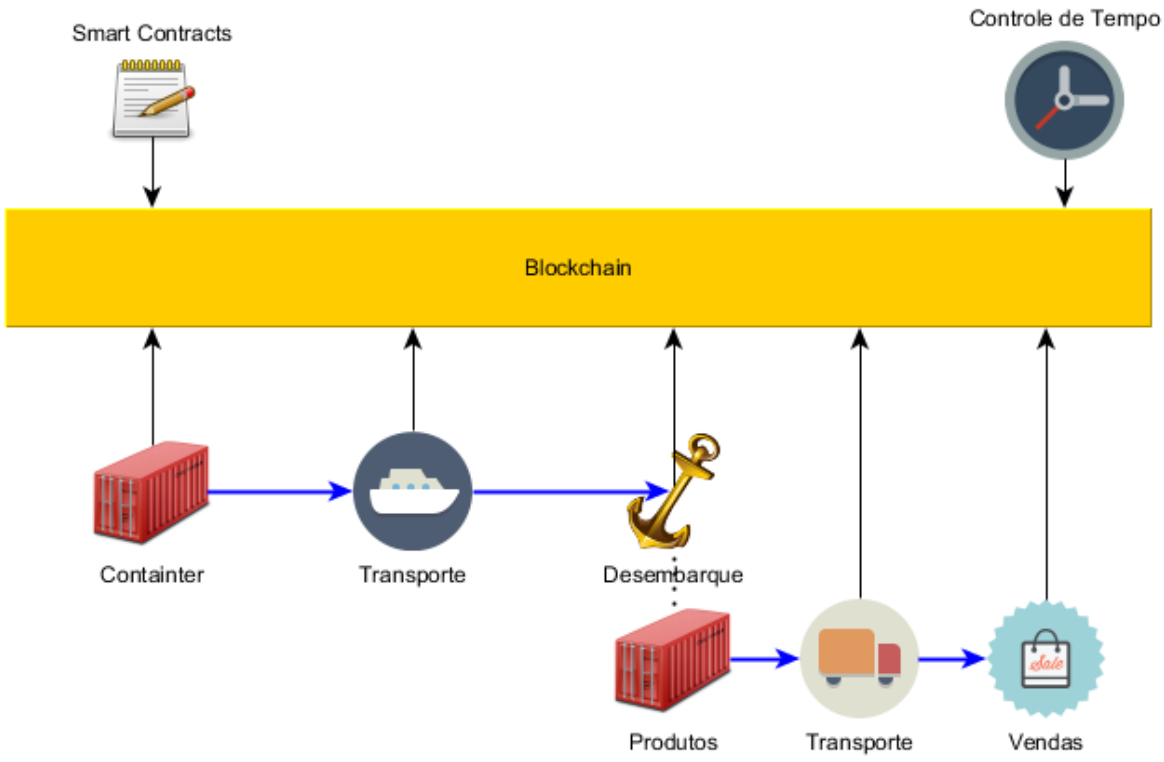

Figura 11 – Exemplo de aplicação para IoT com *Smart Contracts*
Fonte: Elaboração nossa (2017)

Dentro dessa proposta, uma solução é construída usando *blockchain*, *smart contracts* preparados para disparar por controles de tempo de entrada

(*timestamp*) e expiração (*timeout*), e dispositivos IoT espalhados em pontos específicos (*checkpoints*) da cadeia de distribuição e logística.

Quando conjuntos de produtos saem de um fornecedor e são agrupados em contêineres em um porto, um dispositivo envia uma transação ao *blockchain*, informando a data/hora (*timestamp*) de aporto. A sequência de transporte pelo navio só é disparada por um *smart contract* porque a condição de aporto das mercadorias foi cumprida dentro do prazo (antes do *timeout* específico para esse fim). Um atraso na chegada ao porto pode produzir um disparo de outra ação de *smart contract*, por exemplo, a autuação ou punição alfandegária para o transportador ou fornecedor.

Quando um outro *checkpoint* é alcançado (por exemplo, o navio atraca no destino com o contêiner), novamente um dispositivo IoT percebe essa condição, e envia uma mensagem ao *blockchain*, que processa essa transação. De igual modo, um outro *smart contract* verifica o cumprimento do prazo estipulado, automaticamente penaliza os responsáveis por irregularidades, e/ou autoriza o prosseguimento da sequência da cadeia logística.

O mesmo pode ser aplicado para o desembarque das mercadorias, transporte rodoviário, distribuição nos pontos de venda, até chegar ao consumidor final, percorrendo e acompanhando toda a cadeia logística, de forma automática, assim gerando dados, relatórios, dashboards, e eventuais autuações e obrigações tarifárias aos envolvidos no ciclo: fornecedores, transportadores, revendedores, e órgãos fiscalizadores, alfandegários e de governo.

Conclusões

Através do exposto, é possível perceber que as aplicações de Internet das Coisas (IoT) estão emergindo no cenário mundial, e têm grande potencialidade de crescimento também no Brasil. E de maneira inevitável, cresce a demanda por uma infraestrutura capaz de suportar os requisitos de segurança e disponibilidade desse tipo de solução.

Este trabalho demonstrou que, com a utilização de tecnologias inovadoras, como *blockchain* e *smart contracts*, é possível implementar alternativas de infraestrutura para IoT adequadas a atender esse tipo de demanda.

Por fim, a apresentação de um exemplo de aplicação real mostra o potencial de utilização da infraestrutura proposta em diversas soluções de IoT.

Referências

ASHTON, K. **That 'Internet of Things' Thing**. [S.l.]: RFiD Journal, 2009.

CISCO. **Internet of Everything FAQ**. [2014]. Disponível em: <http://ioeassessment.cisco.com/learn/ioe-faq>. Acesso em: 03 ago. 2017.

DEETMAN, S. **Bitcoin Could Consume as Much Electricity as Denmark by 2020**: An environmental researcher modeled pessimistic and optimistic scenarios for Bitcoin's energy consumption over the next few years. 2016. Disponível em: <http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020>. Acesso em: 09 ago. 2017.

ELIZALDE, D. **Internet of Things**: A Primer for Product Managers. 2015. Disponível em: <https://techproductmanagement.com/iot-primer/>. Acesso em: 03 ago. 2017.

EVANS, D. **The Internet of Things**: How the Next Evolution of the Internet Is Changing Everything, 2011. Cisco Internet Business Solutions Group (IBSG). White Paper. Disponível em: <http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf>. Acesso em: 08 ago. 2017.

FORBES. **Internet of Things By The Numbers**: Market Estimates And Forecasts. 2014. Disponível em: <https://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/#2cc6f172b919>. Acesso em: 03 ago. 2017.

GARTNER. **Gartner's 2016 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor**. 2016. Disponível em: <http://www.gartner.com/newsroom/id/3412017>. Acesso em: 03 ago. 2017.

HRUSKA, J. **One Bitcoin group now controls 51% of total mining power, threatening entire currency's safety**. 2014. Disponível em: <http://www.extremetech.com/extreme/184427-one-bitcoin-group-now-controls-51-of-total-mining-power-threatening-entire-currencys-safety>. Acesso em: 09 ago. 2017.

KAR, I. **Estonian Citizens Will Soon Have the World's Most Hack-Proof Health-Care Records**. 2016. Disponível em: <http://qz.com/628889/this-eastern-european-country-is-moving-its-health-records-to-the-blockchain/>. Acesso em: 10 ago. 2017.

KELLY, J.; WILLIAMS, A. **Forty Big Banks Test Blockchain-Based Bond Trading System**. 2016. Disponível em: <https://cryptocurrencytalk.com/topic/45226-forty-big-banks-test-blockchain-based-bond-trading-system/>. Acesso em: 10 ago. 2017.

LACEY, S. **The Energy Blockchain**: How Bitcoin Could be a Catalyst for the Distributed Grid. 2016. Disponível em: <http://www.greentechmedia.com/articles/read/the-energy-blockchain-could-bitcoin-be-a-catalyst-for-the-distributed-grid>. Acesso em: 10 ago. 2017.

LEWIS, A. **A gentle introduction to smart contracts**. 2016. Disponível em: <https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/>. Acesso em: 10 ago. 2017.

MATTERN, F.; FLOERKEMEIER, C. **From the Internet of Computers to the Internet of Things**. Zurich: Institute for Pervasive Computing, 2010.

MATTILA, J. **The Blockchain Phenomenon**. 2015. Disponível em: <http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf>. Acesso em: 08 ago. 2017.

MIZRAHI, A. **A Blockchain-Based Property Ownership Recording System**. 2015. Disponível em: <http://chromaway.com/papers/A-blockchain-based-property-registry.pdf>. Acesso em: 10 ago. 2017.

MONAX. **What are Smart Contracts**. 2014. Monax Documentation. Disponível em: <https://monax.io/explainers/smart_contracts/>. Acesso em: 10 ago. 2017.

NAKAMOTO, S. **Bitcoin**: A peer-to-peer electronic cash system. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 08 ago. 2017.

OPARAH, D. **3 Ways That the Blockchain Will Change the Real Estate Market**. 2016. Disponível em: <http://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/>. Acesso em: 10 ago. 2017.

SATIZ. Technical Publishing & Multimedia. **Internet delle cose**. 2015. Disponível em: <http://www.satiztpm.it/>. Acesso em: 03 ago. 2017.

SUBERG, W. **Factom's Latest Partnership Takes on US Health-care**. 2015. Disponível em: <http://cointelegraph.com/news/factoms-latest-partnership-takes-on-us-healthcare>. Acesso em: 10 ago. 2017.

SWAN, M. **Blockchain**: Blueprint for a New Economy. Sebastopol: O'Reilly Media, 2015.

SZABO, N. **Smart Contracts**. 1994. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>. Acesso em: 10 ago. 2017.

_____. **The Idea of Smart Contracts**. 1997. Disponível em: <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html>. Acesso em: 10 ago. 2017.

TANENBAUM, A.; WETHERALL, D. **Computer Networks**. 5. ed. [S.l.]: Pearson Prentice Hall, 2011.

UNIBUSCAPÉ. Universidade Buscapé Company. **Escola e-commerce**. 2015. Disponível em: <http://www.unibuscapecompany.com/>. Acesso em: 03 ago. 2017.

WANG, F. et al. **A Survey from the Perspective of Evolutionary Process in the Internet of Things**. [S.l.]: International Journal of Distributed Sensor Networks, 2015.

WOOD, Gavin. Ethereum: A secure decentralised generalised transaction ledger. **Ethereum Project Yellow Paper**, v. 151, 2014.