



UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

CENTRO DE INFORMÁTICA

2016.2

A convergência das tecnologias e negócios de
Internet das Coisas e Blockchain

Aluna: Anna Beatriz Sena de Arruda (abs7@cin.ufpe.br)

Orientador: José Carlos Cavalcanti (cavalcanti.jc@gmail.com)

Recife, 12 de Dezembro de 2016

Universidade Federal de Pernambuco
Centro de Informática

Graduação em Sistemas de Informação

A convergência das tecnologias e negócios de Internet das Coisas e Blockchain

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Aluna: Anna Beatriz Sena de Arruda (abs7@cin.ufpe.br)

Orientador: José Carlos Cavalcanti (cavalcanti.jc@gmail.com)

Recife, 12 de Dezembro de 2016

*Dedico este trabalho ao meu avô, Antônio Martins de Sena,
pelo exemplo de vida, força e superação.*

Agradecimentos

Agradeço a minha mãe, Maria de Fátima Sena, por sempre acreditar em mim, me mostrar que tudo era possível através dos estudos e pela dedicação que me proporcionou ingressar em uma universidade.

A minha irmã, Juliene Sena, pelo carinho e por sempre me acolher nos momentos mais difíceis.

Ao meu avô, Antônio Martins de Sena, que dedicou sua vida a formação de caráter e intelectual de todos seus filhos e netos.

A minha tia, Maria José de Sena pelo apoio e acolhimento durante minha jornada na Universidade.

Aos demais familiares que contribuíram para meu crescimento pessoal e intelectual. Em especial, Maria Julia, Caio Henrique e Luiz Carlos Júnior.

Aos meus amigos da faculdade que sempre se mostraram dispostos a me ajudar e me ouvir nos momentos de desespero entre os semestres.

Ao meu orientador José Carlos Cavalcanti, pelos conselhos e disponibilidade para ajudar neste trabalho. Bem como a Yasmine Santos, grande parceira durante toda a jornada no curso.

Ao Centro de Informática (CIn-UFPE) e seus professores e funcionários, por oferecer um ambiente de aprendizado que me estimulou a desenvolver este trabalho.

Por fim, gostaria de agradecer imensamente a todos aqueles que colaboraram para que eu pudesse concluir essa jornada!

Resumo

Vemos Internet das Coisas como um fenômeno emergente de grande significado técnico, social e econômico. Produtos de consumo, bens duráveis, componentes industriais e de utilidade pública, sensores, e outros objetos do cotidiano estão sendo combinados com a conectividade da Internet e com capacidades analíticas de dados poderosas que prometem transformar a forma como nós trabalhamos, vivemos e nos divertimos.

Ao mesmo tempo em que IoT torna-se popular, o Blockchain é anunciado como o quinto grande paradigma de mudança na computação, depois do mainframe, computadores pessoais, a Internet e as redes sociais, uma vez que irá mais uma vez alterar significativamente a nossa maneira de viver e trabalhar.

A junção dessas duas novas formas de conectividade deverá trazer grandes benefícios e, apesar do entendimento acerca desses paradigmas, muitas dúvidas ainda pairam no domínio público sobre como exatamente operam, o que se faz necessário para adotá-las e como combinar seus benefícios.

Nesse contexto, este estudo tem como objetivo a abordagem de conceitos relacionados a Blockchain e IoT, e de como essas tecnologias podem operar juntas quebrando paradigmas e despertando um novo olhar sobre a mudança tanto de infraestrutura, quanto de plataformas e de aplicações para serviço.

Palavras-chave: Internet das Coisas, Blockchain, conectividade.

Abstract

We see Internet of Things as an emergent phenomenon of great technical, social and economic significance. Consumer goods, durable goods, industrial and public utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytics capabilities that promise to transform the way we work, live and have fun.

While IoT becomes popular, the Blockchain is advertised as the fifth big paradigm shift in computing, mainframe, personal computers later, the Internet and social networks, a time that will once again change the way we live and work.

The junction of these two new forms of connectivity should bring great benefits and despite the understanding about these paradigms, many questions still hang in the public domain about exactly how they operate, what it is necessary to adopt them and how to combine its benefits.

In this context, this study aims at the approach of Blockchain-related concepts and IoT, and how these technologies can operate together breaking paradigms and awakening a new look at the change of both infrastructure, as platforms and applications for service.

Keywords: Internet of things, Blockchain, Connectivity.

Lista de Figuras

Figura 1 - Capacidade dos produtos inteligentes conectados	16
Figura 2 - A Nova Pilha da Tecnologia	21
Figura 3 - Livro de Negócios	23

Sumário

1. Introdução.....	10
1.1. Motivação.....	10
1.2. Objetivos e Contribuições.....	12
1.3. Estrutura do Documento	12
2. O Mundo Conectado	13
2.1. As Três Ondas da Tecnologia da Informação	13
2.1.1 A Primeira Onda.....	13
2.1.2 A Segunda Onda.....	14
2.1.3 A Terceira Onda	14
2.2 A Internet das Coisas.....	15
2.3 Capacidade dos Produtos Conectados	16
2.3.1 Monitoramento	17
2.3.2 Controle	18
2.3.3 Otimização	18
2.3.4 Autonomia.....	19
2.4 Uma Nova Visão de Negócio	20
2.5 Considerações Finais	22
3. Blockchain.....	23
3.1 Livro de Negócios.....	23
3.2 O Que é Blockchain?.....	24
3.3 Hashing e Timestamping	26
3.4 Hyperledger	27
3.5 Usos do Blockchain	28
3.6 Obstáculos para o Blockchain.....	30
3.6.1 Escalabilidade.....	30

3.6.2 Consumo de Energia e Custos	31
3.6.3 Velocidade da Transação.....	31
3.6.4 Segurança.....	32
3.6.5 Capital Humano	32
3.6.5 Vida dos Cidadãos	32
3.7 Considerações Finais	33
4. Blockchain e Internet das Coisas.....	34
4.1 O Problema do Modelo Centralizado	34
4.2 Descentralização das Redes IoT.....	35
4.3 Utilizações Concretas de Blockchain e IoT	38
4.4 Considerações Finais	40
5. Conclusão e Trabalhos Futuros	42
6. Bibliografia	44

1. Introdução

Neste capítulo, será feita uma introdução sobre este Trabalho de Graduação. Na Seção 1.1, há uma discussão sobre a motivação para desenvolver este trabalho. Na Seção 1.2, são apresentados os objetivos específicos que se deseja alcançar. A Seção 1.3 contém como o trabalho foi organizado.

1.1. Motivação

A Internet, parte vital do cotidiano de todos, teve sua origem no final dos anos 70 com um conceito inovador. Seria uma infraestrutura de rede aberta que permitiria a conexão de outras redes sem a presença de um órgão ou governança centralizadora, apenas com as regras e definições básicas para garantir a comunicação entre todos.

Com o advento da World Wide Web (WWW), a Internet ganhou apelo fora do meio em que foi criada (militar e acadêmico) e tornou-se a grande rede mundial de comunicações que conhecemos. Sobre essa infraestrutura aberta surgiram diversas aplicações de troca de arquivos e acesso remoto[1].

A ideia de conectar objetos é discutida desde 1991, quando a conexão TCP/IP e a internet que conhecemos hoje começou a se popularizar. Em 1999, Kevin Ashton do MIT propôs o termo Internet das Coisas que segundo ele se baseia na ideia de estarmos presenciando o momento em que duas redes distintas - a rede de comunicação humana (exemplificada na internet) e o mundo real das coisas - precisam se encontrar. Um ponto de encontro onde não mais apenas “usaremos um computador”, mas onde um “computador se use” independente, de modo a tornar a vida mais eficiente. Os objetos - as “coisas” - estarão conectados entre si em rede, de modo inteligente, e passarão a “sentir” o mundo ao redor e interagir[2].

Hoje, no entanto, a IoT faz emergir desafios significativos que podem ficar à frente dos seus potenciais benefícios. Manchetes na mídia sobre a invasão de dispositivos conectados à Internet, preocupações com vigilância, e receios sobre privacidade já capturaram a atenção do público. Desafios técnicos permanecem e se

tornam mais complexos à medida que o número de atores envolvidos cresce, e novos desafios políticos, legais e de desenvolvimento estão emergindo[3].

Como uma alternativa viável aos desafios citados existe a tecnologia Blockchain, que tem seu nome derivado de de uma cadeia formada por uma sucessão de blocos.

Blockchain é anunciado como o quinto grande paradigma de mudança na computação, depois de mainframe, computadores pessoais, a Internet e as redes sociais, uma vez que irá mais uma vez alterar significativamente a nossa maneira de viver e trabalhar.

Em termos simples, uma Blockchain é um livro ou registo acessível ao público digital. Todas as transações envolvendo, por exemplo, a criptomoeda bitcoin são guardadas no registo, e qualquer pessoa com os códigos de acesso pode verificar a propriedade da moeda virtual a qualquer momento. No entanto, é preciso investigar um pouco mais para que seja possível revelar as vantagens e perspectivas futuras desta nova tecnologia.

Além do que foi citado no parágrafo anterior, o carácter revolucionário da Blockchain reside no fato de que ela é descentralizada, o que significa que funciona independentemente de uma autoridade central. A descentralização é conseguida salvando automaticamente uma cópia de todo o registo (ou seja, a Blockchain) no computador de cada membro da rede a partir da adesão e quando qualquer alteração é feita, como cada membro tem uma cópia atualizada do Blockchain, a transação é comparada com a versão mais recente antes de ser validada, a fraude torna-se praticamente impossível.

Quanto a sua criação, o Blockchain foi originalmente desenvolvido para permitir a criação e comércio de bitcoin. No entanto, logo ficou claro que a tecnologia tinha muitas outras aplicações possíveis.

Este trabalho aborda conceitos e soluções que unem Blockchain e Internet das Coisas a fim de mostrar todo o potencial da união dessas duas tecnologias.

1.2. Objetivos e Contribuições

Este trabalho tem como objetivo a abordagem, de forma simples e didática, de conceitos e aplicações de Internet das Coisas e Blockchain tanto separadamente quanto em conjunto.

A definição desses paradigmas já é conhecida por estudantes e simpatizantes de tecnologia, porém é necessário ainda um olhar mais aprofundado. É comum que algumas pessoas saibam do que se tratam as tecnologias abordadas, mas não do que se faz necessário para que elas operem em seu negócio.

Em linhas gerais, o principal objetivo deste trabalho é investigar como a tecnologia associada a Internet das Coisas e Blockchain convergem entre si cobrindo aspectos como:

- ✓ Conceitualização de cada uma das tecnologias.
- ✓ Utilização das duas tecnologias unidas.

1.3. Estrutura do Documento

Os próximos capítulos deste trabalho estão estruturados da seguinte forma: no Capítulo 2, são apresentados conceitos relacionados a Internet das Coisas e suas aplicações. No Capítulo 3, definição de Blockchain e suas aplicações, no Capítulo 4 serão combinados os conceitos e apresentados usos em conjunto das duas tecnologias. Por fim, no Capítulo 5, estão presentes a conclusão deste trabalho e possíveis trabalhos futuros relacionados ao tema.

2. O Mundo Conectado

Este capítulo aborda os principais conceitos relacionados a Internet das Coisas. Na Seção 2.1, há uma descrição sobre as ondas da tecnologia que culminaram nos produtos conectados. Na Seção 2.2, são apresentados os conceitos centrais de Internet das Coisas. Na Seção 2.3, capacidades dos produtos conectados. Na Seção 2.4, são discutidos como a Internet das Coisas e os produtos conectados vem mudando significativamente o meio de produção. Na Seção 2.5, há uma breve conclusão sobre o que foi discutido ao longo do capítulo é apresentada.

2.1. As Três Ondas da Tecnologia da Informação

Ao longo dos últimos 50 anos, a tecnologia da informação vem reformulando radicalmente a concorrência e estratégias de mercado; atualmente estamos à beira de uma terceira transformação, mas antes de abordar essa terceira onda vamos lembrar o que foram as duas ondas anteriores[4].

2.1.1 A Primeira Onda

Antes do advento da tecnologia moderna, os produtos eram mecânicos e as atividades eram realizadas usando processos manuais. Na primeira onda de TI, durante as décadas de 60 e 70, as atividades individuais começaram a ser automatizadas, tarefas como processamento de pedidos, pagamento de contas, design e fabricação de produtos e planejamento de recursos passaram a ser assistidas por computadores culminando num drástico aumento de produtividade, de certa forma tal aumento foi justificado pela capacidade de se capturar e analisar grandes quantidades de dados em cada atividade. Tudo isso levou a padronização dos processos e levantou um dilema para as empresas sobre como obter benefícios operacionais mantendo estratégias distintas.

2.1.2 A Segunda Onda

A ascensão da internet, com sua onipresença e preço baixo desencadeou a segunda onda, impulsionando as transformações das décadas de 80 e 90 onde as atividades não eram mais independentes e pertencentes apenas a empresa. A segunda onda permitiu uma integração entre as atividades individuais, com fornecedores externos, canais e clientes.

As duas primeiras ondas originaram ganhos absurdos no crescimento, produtividade e em toda a economia.

Quando se transformam os processos, os produtos também são afetados e é nesse contexto que surge a terceira onda[4].

2.1.3 A Terceira Onda

A terceira onda é onde o produto se transforma e também passa a ser beneficiado pelo avanço da internet, hardware e software.

Sensores embutidos, processadores, software e conectividade passam a fazer parte dos produtos, juntamente com uma capacidade de gerar dados que na maioria das vezes é armazenado e analisado por alguns aplicativos. Tal análise impulsiona melhorias no desempenho e funcionalidade do produto.

Mais um salto na produtividade e economia está sendo desencadeado por esses novos produtos. Além disso, produzi-los vai remodelar a cadeia de valor mais uma vez mudando a concepção, marketing, venda e relação pós-venda, criando uma necessidade de novas atividades além da análise de dados, como segurança.

A terceira onda apresenta o potencial de ser a maior já existente, provocando mais inovação, mais ganhos de produtividade e crescimento econômico que as duas anteriores.

A última onda trouxe a tona a Internet das Coisas, que será abordada no tópico seguinte.

2.2 A Internet das Coisas

A informação está saindo dos computadores tradicionais e indo para o mundo ao nosso redor, tal fato implica em uma mudança ainda maior que a chegada da internet ou de dispositivos multimídia, por ser mais voltado a interação humana.

A diminuição de tamanho dos hardware alinhado ao aumento de suas capacidades, a confiabilidade das memórias, a redução de custos, o gerenciamento eficiente de energia e o avanço das telecomunicações tornaram possível adicionar funções antes inimagináveis em produtos da era industrial incluindo televisões, carros, telefones, câmeras e até mesmo livros. Com o advento da capacidade digital, os produtos citados passaram a oferecer novas funções, a ter novos preços e ainda a serem apresentados de uma forma nova, transformando sua produção, seu uso, seu design e sua distribuição.

Dessa forma a Internet das Coisas, tema central do capítulo que se segue, é uma evolução dentro do paradigma de computação ubíqua que consiste na onipresença de objetos, as chamadas “coisas”, que possuem três elementos principais: componentes físicos, componentes “inteligentes” e componentes de conectividade. Componentes inteligentes amplificam as capacidades e valor dos componentes físicos, a conectividade amplia as capacidades e valor do componente “inteligente” e permitem que alguns deles existam até mesmo fora do produto físico. O resultado de tudo isso é um ciclo vicioso de melhoria de valor.

Conceitualmente, o primeiro órgão a definir a Internet das Coisas (IoT), em 2005, foi a International Telecommunication Union (ITU), agência das Nações Unidas para tecnologias da informação e comunicação. A ITU publicou um relatório sobre tendência de uma nova geração de internet, chamada Internet das Coisas. Nesse relatório, Internet das Coisas foi definida como a conexão de todos os objetos e dispositivos do cotidiano a todos os tipos de redes: intranet, peer-to-peer e a internet global que conhecemos[5].

Como visto no parágrafo anterior, o conceito de IoT não é novo, mas atualmente está em seu auge devido aos avanços de hardware. No mais, todos os conceitos que podem existir para o termo, culminam em uma visão de que há um

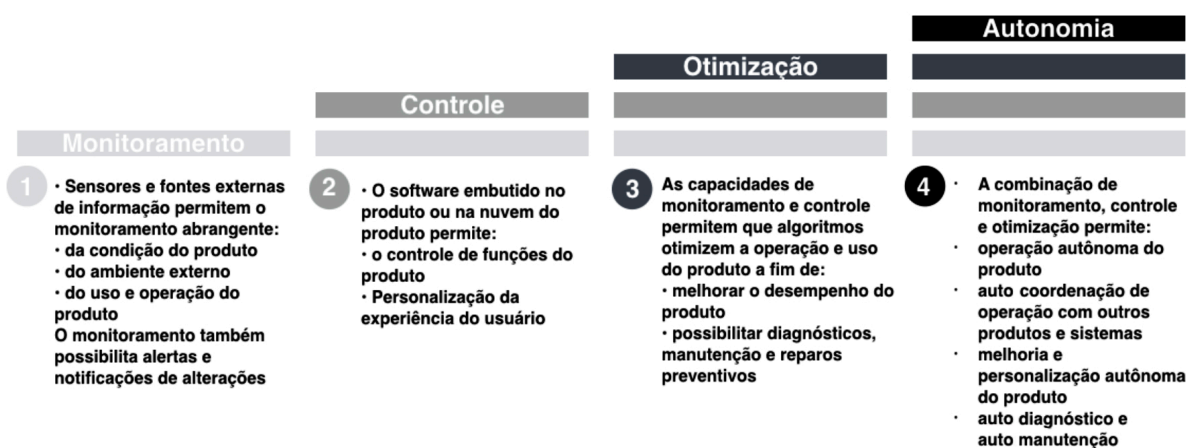
mundo no qual objetos do nosso cotidiano são equipados com uma lógica digital, sensores e conexão à internet. Esse cenário deixou de existir apenas no mundo imaginário e já está presente no mundo real.

Atualmente a Internet das Coisas está crescendo e sensores estão sendo instalados a taxas cada vez maiores. Em pouco tempo um mundo coberto de coisas conectadas vai se tornar realidade, com essa conexão surge uma enorme promessa para o futuro de outras tecnologias, e pesquisa em geral. No entanto, essa promessa depende de quão acessíveis estão os bilhares de dados gerados e também da sua propriedade, pois modelos atuais de de privacidade de usuário e compartilhamento de dados não são escaláveis a esse nível[6].

2.3 Capacidade dos Produtos Conectados

Podemos agrupar em 4 áreas as capacidades dos produtos conectados em quatro áreas: monitoramento, controle, otimização e autonomia (ver quadro “Capacidade dos produtos inteligentes e conectados”) Cada um baseia-se em seu precedente, ou seja, um produto deve ter capacidade de controle para ter capacidade de monitoramento[4].

Figura 1 - Capacidade dos produtos inteligentes conectados



Fonte: The Linking Open Data cloud diagram 1

¹ <https://goo.gl/r0arrK>

2.3.1 Monitoramento

Produtos conectados permitem um monitoramento abrangente das condições, operações e ambiente externo a ele por meio de sensores e fontes de dados externas.

O monitoramento permite que o fabricante e o cliente acompanhem as características operacionais e o histórico de um produto e compreendam melhor como esse produto é realmente usado. Os dados mencionados tem importantes implicações para áreas como design (reduzindo a superengenharia), segmentação de mercado (através da análise e padrões de uso por tipo de cliente) e serviço pós-venda (permitindo envio de manutenções pontuais e corretas).

Dados de monitoramento podem também revelar problemas de conformidade da garantia, novas oportunidades de venda ou ainda a necessidade de uma capacidade adicional do produto por conta da alta utilização. Em alguns casos o monitoramento é o elemento central da criação de valor, como em dispositivos médicos.

O medidor digital de glicose Medtronic² usa um pequeno dispositivo detector de glicose (ou sensor) que é inserido logo abaixo da pele ou estômago. O sensor mede os níveis de glicose a cada cinco minutos, e envia as informações via transmissor sem fio a um monitor que pode ser usado no cinto ou em um bolso.

O monitor contínuo ajuda a ficar atento aos seus níveis de glicose, e a saber como eles mudam dependendo da ingestão de alimentos, dos exercícios e da medicação. O monitor também alerta pacientes e médicos até 30 minutos antes de um paciente atingir um nível limite de glicemia, permitindo procedimentos adequados e no tempo certo[8].

As capacidades de monitoramento podem abranger múltiplos produtos. A Joy Global³, fabricante de equipamentos de mineração, monitora indicadores de condições operacionais, segurança, e serviços de previsão para uma vasta gama de máquinas em múltiplas minas e em diferentes países para fazer análises

² <http://www.medtronicbrasil.com.br/your-health/diabetes/device/continuous-glucose-monitor/what-is-it/>

³ <http://www.joyglobal.com/pt>

comparativas.

2.3.2 Controle

Os produtos podem ser controlados por comandos remotos ou algoritmos, que podem estar incorporados no produto ou na nuvem. Os algoritmos são mais utilizados em condições quase imperceptíveis pelo usuário, por exemplo, desligar uma válvula caso a pressão aumente muito ou desligar as luzes de um edifício-garagem caso não seja detectado movimento ou presença de alguém.

O controle por software, localizado na nuvem ou no produto, permite a personalização do produto em um nível que não se mostrava rentável ou nem mesmo possível há tempos atrás. Essa tecnologia permite ao usuário personalizar controlar sua interação com o produto. Por exemplo, a lâmpada Philips Hue⁴ permite que o usuário controle a sua tonalidade, luminosidade, quando acender e apagar e ainda a mudar para a cor vermelha caso seja detectada a presença de um intruso[9]. A Doorbot, uma espécie de campainha e fechadura inteligente conectada, envia um vídeo para o smartphone ou tablet do proprietário quando alguém toca a campainha. É possível saber quem está do outro lado da porta e ainda abrir a fechadura remotamente[10].

2.3.3 Otimização

A soma do grande fluxo de dados resultantes do monitoramento com a capacidade de controlar a operação permite a otimização do produto de diversas formas, muitas das quais não eram possíveis anteriormente. Algoritmos e capacidade analítica de dados de uso ou históricos podem ser aplicados para melhorar radicalmente a produção, utilização e eficiência.

Em turbinas eólicas, por exemplo, um microcontrolador pode ajustar cada pá para que em cada rotação capte o máximo de energia possível. Cada turbina pode

⁴ <http://www2.meethue.com/pt-br/o-que-é-a-hue/>

ser ajustada não só para melhora de desempenho, mas também para minimizar o impacto sobre a eficiência de outras turbinas próximas.

O monitoramento em tempo real das condições do produto permite a otimização dos serviços de reparo, fazendo manutenção preventiva e realizando consertos remotamente. Com isso, as empresas reduzem o tempo de inatividade do produto e a necessidade de envio de técnicos para realizar os reparos. Mesmo que seja necessário um conserto no local, as informações já repassadas pelo produto sobre o que está quebrado, que peças são necessárias e como fazer o reparo reduzem custos de serviço e aumentam o índice de resolução do problema na primeira visita.

A Diebold⁵, fabricante de caixas eletrônicos, monitora seus produtos para que aos primeiros sinais de problemas ele sejam avaliados e se possível a manutenção seja feita remotamente. Caso não seja possível corrigir o problema remotamente, técnicos que já receberam um diagnóstico detalhado do problema, uma recomendação de procedimento de reparo, e muitas vezes, as peças necessárias são enviados para fazer manutenção. Os caixas da Diebold também são atualizados com melhorias de recursos, geralmente de forma remota.

2.3.4 Autonomia

Aninhando monitoramento, controle e otimização consegue-se garantir que os produtos conectados tenham alcancem um nível até então inatingível de autonomia. Num nível mais simples está o iRobot, um aspirador de pó que usa sensores para limpar diferentes pisos. Alguns produtos mais sofisticados são capazes de aprender sobre o ambiente e adaptar-se as preferências dos usuários.

Produtos autônomos também podem atuar em conjunto com outros produtos e sistemas. O valor dessas capacidades pode crescer exponencialmente à medida que mais e mais produtos forem se tornando conectados. Por exemplo, a eficiência de uma rede elétrica aumenta quando há mais medidores inteligentes conectados permitindo que a empresa operadora identifique padrões de demanda e atue com

⁵ <http://www.dieboldnixdorf.com.br/2-servicos>

base neles.

Finalmente, há produtos que podem funcionar com autonomia completa, aplicando algoritmos que utilizam dados sobre seu desempenho e seu ambiente e aproveitando sua capacidade de se comunicar com outros produtos. Operadores humanos apenas monitoram o desempenho ou supervisionam o conjunto ou o sistema, em vez de unidades separadas. O sistema de mineração Longwall da Joy Global, por exemplo, pode operar com autonomia no subsolo, supervisionado por um centro de controle da mina na superfície. O equipamento é monitorado continuamente quanto ao desempenho e a possíveis defeitos. Quando há problemas que exigem a intervenção humana, são enviados técnicos ao subsolo[4].

2.4 Uma Nova Visão de Negócio

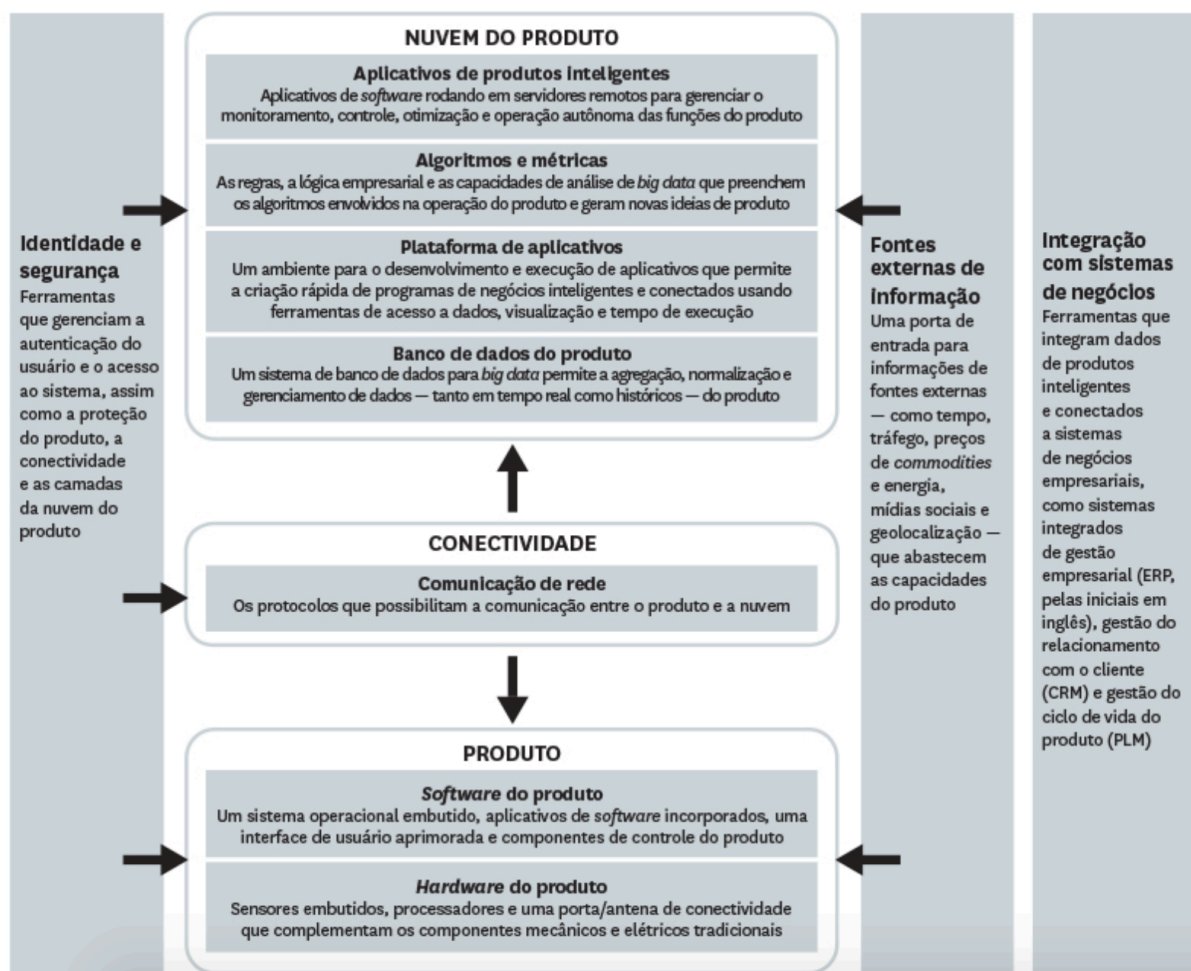
Produtos conectados estão surgindo em todos os setores da indústria e serviços. De acordo com o Gartner, 215 bilhões de dispositivos estarão conectados à internet até 2020[7] e cada casa de família irá conter até 500 dispositivos em rede e, apesar do que foi relatado, os dados provenientes dessas conexões facilitam análise, planejamento antecipado, gerência e tomada de decisões inteligentes pelos sistemas de forma autônoma. Nesse contexto, podemos ver que não somente os produtos, mas também os serviços de diversos setores, tais como: educação, transporte, saúde, governança, varejo, logística, agricultura, produção industrial, automação, gestão de processos etc., já estão se beneficiando de várias formas com a IoT.

A IoT traz a tona um novo modelo de negócios, tal modelo força as organizações de diversos setores a ajustar e rever suas estratégias a fim de obter sucesso no mercado digital que vem crescendo exponencialmente. Muitas empresas enfrentam dificuldades para compreender a complexidade sem precedentes de desenvolver modelos de negócios adequados à evolução das tecnologias digitais[6].

Por conta disso, os produtos que fazem uso da Internet das Coisas exigem que as empresas construam uma infra-estrutura inteiramente nova, composta por uma série de camadas conhecida como "pilha tecnológica" (ver quadro "A nova

pilha de tecnologia"). Incluindo aplicativos de software, um sistema operacional incorporado no produto, hardware, conexão com banco de dados e análise desses dados[4].

Figura 2 - A Nova Pilha da Tecnologia



Fonte: *The Linking Open Data cloud diagram*⁶

Essa tecnologia permite não só o rápido desenvolvimento e operação dos produtos, mas também a coleta, compartilhamento e análise de quantidades potencialmente enormes de dados gerados dentro e fora dos produtos e que não estavam disponíveis antes. Construir e manter a pilha de software para IoT requer investimentos substanciais em uma variedade de novas habilidades como desenvolvimento de software, análise de dados, engenharia de software e segurança de dados; que raramente são encontradas em empresas de manufatura.

⁶ <https://goo.gl/r0arrK>

2.5 Considerações Finais

Este capítulo apresentou conceitos centrais sobre Internet das Coisas. A IoT possibilita a criação de novas formas de relacionamento com o consumidor e a forma como as empresas competem e geram valor. A Internet das Coisas abre as portas para um mundo de melhorias, tanto na função e capacidade do produto quanto na satisfação e conforto humano. Os produtos passarão a ser mais seguros, eficientes, confiáveis e mais utilizados, já que manutenções serão feitas no tempo certo, economizando tempo, dinheiro, matéria-prima e recursos do meio ambiente.

A era dos produtos inteligentes muda a trajetória das empresas desde que essas mesmas empresas aceitem e se adaptem ao novo mercado e as novas oportunidades.

3. Blockchain

Este capítulo aborda os principais conceitos relacionados a tecnologia Blockchain. Na Seção 3.1, há uma descrição sobre livros de negócios. Na Seção 3.2, são apresentados os conceitos centrais de Blockchain. Na Seção 3.3, são apresentados os métodos que tornam a tecnologia segura. Na Seção 3.4, é apresentado o Hyperledger. Na Seção 3.5, São apresentados usos da tecnologia abordada. Na seção 3.6, ps desafios enfrentados para e na seção 3.7 uma breve conclusão sobre o que foi discutido ao longo do capítulo é apresentada.

3.1 Livro de Negócios

No mundo conectado e integrado que vivenciamos hoje, atividades econômicas acontecem o tempo todo em todo lugar. Fornecedores, clientes, bancos, parceiros, produtores e outras partes interessadas controlam seus ganhos e exercem suas vontades sobre seus objetos de valor conhecidos como ativos.

Existem 2 tipos de ativos, os tangíveis e físicos como imóveis e automóveis e os intangíveis e virtuais como títulos, patentes e ações. O processo de transferência de bens é conhecido como transações.

Como mencionado, as transações envolvem diversos participantes como compradores, vendedores e agentes intermediários (como os bancos) que registam essas transações em um livro de negócios[11].

Um livro de negócios é algo semelhante a imagem abaixo:

Figura 3 - Livro de Negócios

TIPO DE CONTA	DINHEIRO				
DATA DA TRANSAÇÃO	DETALHES DA TRANSAÇÃO	REFERÊNCIA	DÉBITO	CRÉDITO	BALANÇO
01/01/2016	Despesas de Janeiro	Ref#01	R\$ 2.000		R\$2.000
02/01/2016	Imposto Retido	Ref#02		R\$ 2.100	(R\$ 100)

Os livros de negócios em uso atualmente apresentam varias deficiências derivadas de sistemas centralizados baseados em terceiros como instituições financeiras. São ineficientes, caros, de difícil interpretação, sujeitos a uso indevido e fraude. Cópias dos livros de transação realizadas fora de sincronia levam a decisões erradas baseadas em dados incorretos.

Sistemas baseados em confiança e centralizados culminam em obstáculos no tempo de aprovação das transações. A possibilidade de fraude e falta de transparência exigem uma reversão ou o fornecimento de um seguro caro que assegure as transações. Todos esses fatores contribuem para a perda de oportunidades de negócios.

Em meio ao cenário de turbulência surge uma nova oportunidade, o Blockchain. Tal tecnologia traz consigo a promissora ideia de transações asseguradas por múltiplos computadores sem a necessidade de um agente intermediário.

3.2 O Que é Blockchain?

Blockchain é um livro-razão que é composto por duas partes: uma rede peer-to-peer e um banco de dados distribuído descentralizado[13].

Blockchain é um registro de transações. Um sistema descentralizado para o intercâmbio de ativos. Ele usa um livro comum, que pode ser público ou privado, para registrar a história das transações que ocorrem em uma rede peer-to-peer (P2P) altamente escalável. Sua integridade é baseada em um mecanismo de consenso e não em uma infra-estrutura baseada em confiança[11].

Alguns conceitos são primordiais no processamento de rede Blockchain.

A rede P2P é uma arquitetura de redes de computadores onde cada um dos pontos (conhecidos como nós) da rede funciona tanto como cliente quanto como

⁷ <https://goo.gl/8cqcVJ>

servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central[13]. Por funcionar de forma descentralizada impede que qualquer participante consiga controlar sua infra-estrutura ou debilitar o sistema. Os integrantes (indivíduos, organizações, atores estatais ou uma combinação de todos eles) da rede são todos iguais, aderindo aos mesmos protocolos[11].

Banco de dados distribuído é uma coleção de várias bases de dados logicamente inter-relacionadas, distribuídas por uma rede de computadores, ou seja, vários computadores pelo mundo tendo as mesmas informações atualizadas simultaneamente com garantia de confiabilidade dessas informações. No caso do Blockchain, esse banco de dados é formado a partir de uma série de blocos (cada bloco contém uma série de informações) que juntos formam uma cadeia. É deste ponto que surge o nome “cadeia de blocos” ou Blockchain[13].

À medida que se adicionam novas transações, essas novas transações são guardadas em um novo bloco de acordo com o momento que ela foi processada. O conjunto Informação + tempo forma um bloco e o conjunto de blocos formam uma cadeia de blocos.[13].

A confirmação e validação das transações é feita por meio de um consenso, que garante que os "livros de negócios" partilhados na rede são cópias exatas, reduzindo o risco de fraude e adulterações, já que essas adulterações teriam que ser feitas em muitos locais exatamente ao mesmo tempo. Para chegar a um consenso, todos os envolvidos devem concordar com a transação e validá-la. Os participantes também podem estabelecer regras para as validações[11].

Após as transações serem validadas, são empilhadas no bloco, uma assinatura ou “hash” é adicionada no final do bloco. O hash é linkado ao bloco anterior da cadeia. Estes hashes formam as ligações para que seja possível voltar entre as cadeias até chegar ao bloco gênese (o primeiro bloco de todos desde a instalação do Blockchain). Esse hash inclui o número do bloco atual e o número do próximo bloco da cadeia. Também inclui a data e o momento em que foi assinado o bloco atual, além da quantidade de transações inclusas nesse bloco[13].

3.3 Hashing e Timestamping

A tecnologia Blockchain reúne duas funções-chave: hashing e timestamping seguro.

Hashing executa um algoritmo de computação sob um conteúdo, o resultado disso é uma cadeia de caracteres alfanuméricos que não pode ser revertida para o conteúdo original. Por exemplo, cada arquivo de genoma humano pode ser transformado em uma sequência hash de 64 caracteres com um identificador privado para esse conteúdo[14]. O hash representa o conteúdo exato do arquivo original. Sempre que o conteúdo precisa ser checado, o mesmo algoritmo hash é executado sobre o arquivo original e o resultado deve ser o mesmo se o arquivo não tiver sido alterado.

O hash é curto o suficiente para ser incluído como texto em uma transação Blockchain, que assim fornece a função de timestamp (uma sequência de caracteres ou informação codificada que identifica quando um evento ocorreu, geralmente informando data e hora) seguro de quando ocorreu uma transação específica. O Blockchain pode servir como um registro de documento.

O hashing é feito por diversos e diferentes computadores. Se todos concordam com o resultado obtido, o bloco recebe uma assinatura digital única[15]. A ideia chave é usar hashes como uma forma de atestar a integridade de ativos, a funcionalidade de hashing aninhado a timestamp suporta a ideia do Blockchain como uma nova classe de tecnologia[14].

Como abordado, essas funções servem como uma forma permanente e pública de registrar e armazenar informações e também encontrar essas mesmas informações mais tarde com um explorador de bloco e o ponteiro de endereço. A função principal é verificar um recurso por meio de um registro público.

3.4 Hyperledger

O Hiperledger⁸ é um projeto de código aberto criado para avançar e unificar a tecnologia Blockchain. É uma colaboração global incluindo líderes em finanças, bancos, Internet das Coisas, cadeias de suprimentos, tecnologia e manufatura[17].

O projeto tenta unificar todas as abordagens de código aberto do Blockchain que existem atualmente. De acordo com a página inicial do Hyperledger o projeto está desenvolvendo um framework de Blockchain de propósito geral e que possa ser utilizado em vários setores.

A parte significativa do projeto em comparação a outros é a participação de grandes nomes. Os membros fundadores da iniciativa incluem ABN AMRO, Accenture, ANZ Bank, Blockchain, BNY Mellon, Calastone, Cisco, CLS, CME Group, ConsenSys, Credits, The Depository Trust & Clearing Corporation (DTCC), Deutsche Börse Group, Digital Asset Holdings, Fujitsu Limited, Guardtime, Hitachi, IBM, Intel, IntellectEU, J.P. Morgan, NEC, NTT DATA, R3, Red Hat, State Street, SWIFT, Symbiont, VMware e Wells Fargo[16].

As metas atuais do Hyperledger são as de combinar projetos em aplicações práticas de Blockchain: o Rippled, um registrador distribuído, que trata de diversos pagamentos entre diferentes moedas utilizando livros de ordem da Open Blockchain, da IBM, uma estrutura de baixo nível que implementa contratos inteligentes, recursos digitais, repositórios de registro, redes orientadas a consenso e a segurança criptográfica do Hyperledger, da Digital Asset, que é um servidor de Blockchain pronto para implantação com uma API de cliente atualmente disponível para uso por parte de empresas de serviços financeiros.

Ele funciona ao utilizar um registro de transação apenas de adição que é projetado para ser replicado entre múltiplas organizações separadas, todas sem um nexo de controle. (A empresa matriz, a Digital Asset Holdings, emprestou o nome registrado Hyperledger para o projeto de código aberto como parte de sua contribuição).

A IBM vem contribuindo com milhares de linhas de código para o projeto,

⁸ <https://www.hyperledger.org>

deixando claro que acredita que a tecnologia aberta é a melhor forma de criar uma implementação verdadeiramente aplicável do Blockchain para o mercado empresarial e de negócios atual.

Em uma nota na The Block Chain Conference, realizada em São Francisco, em fevereiro, o diretor Global de Ofertas de Blockchain da IBM, John Wolpert, disse que "precisamos evoluir a internet para deixá-la economicamente ciente, e essa internet não vai ser uma aplicação, ela será a estrutura". Ele vê o Hyperledger como o projeto que está explorando a melhor versão dessas tecnologias, para construir essa estrutura[16].

3.5 Usos do Blockchain

A tecnologia Blockchain carrega um potencial que adiciona maior eficiência e segurança as atividades de uma empresa. Abaixo estão listados alguns potenciais usos dessa tecnologia separados por áreas[12]:

- Internet das Coisas: gerenciamento de dispositivos
- Cuidados com a saúde: registros médicos eletrônicos, banco de doenças, histórico de pacientes, receitas médicas, contratos com planos de saúde.
- Serviços financeiros: notas fiscais, dívidas e obrigações de empresas, plataformas de negociação, acordos de recompra e crédito, câmbio, direitos autorais
- Seguro: processamento de reclamações, vendas, títulos de propriedade
- Industrial: processo de fabricação, estoque
- Governo: licitações, impostos, votação
- Interprofissional: gerenciamento de identidade, gestão de ativos de capital
- Outras indústrias: jogos, música

Ilustrando os tópicos acima existem casos como o da cantora britânica Imogen Heap⁹ que disponibilizou seu álbum no Ujo¹⁰ uma plataforma baseada no Ethereum¹¹ capaz de transferir cada valor depositado pro dono da música sem precisar do ECAD¹², que atualmente tem esse papel. Ou seja, a plataforma poderia repassar, diretamente, cada parte para cada participante em uma produção. Se uma música, por exemplo, foi escrita por alguém que mora nos Estados Unidos mas executada por um artista brasileiro em um estúdio britânico, cada um poderia receber diretamente do consumidor a parte que lhe cabe nesse comércio.

O Ethereum é um sistema baseado no Blockchain que é fruto de uma campanha no crowdfunding que rendeu 21 milhões de dólares para sua construção. Com base nisso já existem outras aplicações funcionando, como o Ujo. Usando o Ethereum é possível também lançar campanhas de crowdfunding sem precisar de intermediários como é feito hoje com o Catarse¹³, IndieGogo¹⁴ e outros.

O site do Ethereum ainda disponibiliza uma serie de outras ferramentas para outros inúmeros fins.

A indústria de cinema e publicidade também será fortemente impactada pelos sistemas que usam Blockchain. Atores e atrizes que trabalharam num comercial, por exemplo, poderiam receber diretamente do requerente da propaganda a cada exibição e de acordo com a audiência.

Os problemas com direitos autorais serão bem menores. Artistas, músicos, produtores e outros ramos seriam bem melhor recompensados do que são atualmente por sistemas como Spotify¹⁵ e AppleMusic¹⁶.

No caso do Brasil, a lei Rouanet, que acabaria por deixar de existir já que a

⁹ https://pt.wikipedia.org/wiki/Imogen_Heap

¹⁰ <https://ujomusic.com>

¹¹ <https://www.ethereum.org>

¹² <http://www.ecad.org.br/pt/Paginas/default.aspx>

¹³ <https://www.catarse.me>

¹⁴ <https://www.indiegogo.com>

¹⁵ <https://www.spotify.com/br/>

¹⁶ <http://www.apple.com/br/music/>

ideia é deixar tudo mais fácil e rastreável. Programas sociais como Bolsa Família não dependeriam de tanto esforço para serem repassados aos beneficiários, um programa poderia transferir diretamente os impostos recebidos pelo governo para o pagamento de benefícios sociais como esse e outros semelhantes. A Receita Federal teria outras funções ou seria substituída por desenvolvedores que oferecem suporte e intermediam de modo menos ativo o repasse de impostos evitando fraudes e sonegação.

O comércio, de uma forma geral, também pode ser reinventado. Aplicações como o Etsy¹⁷ e Mercado Livre¹⁸, terão que repensar sua forma obter lucro. Em sites como esses um percentual da venda fica com o site e outra parcela é retida pelo banco por fazer a transação. Uma plataforma chamada OpenBaazar¹⁹, ainda em versão beta e que tem o mesmo propósito das anteriores, vai possibilitar um mercado descentralizado sem intermediários na internet.

3.6 Obstáculos para o Blockchain

A tecnologia Blockchain veio a tona no final de 2008, quando Satoshi Nakamoto criou a criptomoeda Bitcoin. Somente nos últimos anos a atenção saiu do Bitcoin e migrou para o enorme potencial da tecnologia que funcionava por traz dele. Embora possa parecer que Blockchain vai resolver muitos dos problemas do mundo, ainda é uma tecnologia muito jovem com muitos de desafios a superar[18].

3.6.1 Escalabilidade

A escalabilidade é uma questão importante e a idéia de Blockchain é que cada nó na web distribuída tem uma cópia completa do Blockchain. Portanto, se você deseja iniciar a validação de transações no bloco, primeiro você precisa fazer o download do bloco inteiro. Uma possível alternativa seria baixar somente as últimas

¹⁷ <http://www.etsy.com>

¹⁸ <http://www.mercadolivre.com.br>

¹⁹ <https://openbazaar.org>

centenas de blocos. O Blockchain inteiro ainda estaria disponível, mas somente em alguns nós. A escalabilidade não é um problema para blocos privados. Embora seja mais caro do que um único banco de dados centralizado, se você somar os custos envolvidos em todos os bancos de dados centralizados substituídos pelo Blockchain, ainda é muito mais barato.

3.6.2 Consumo de Energia e Custos

A validação de transações requer computadores robustos para resolver quebra-cabeças complicados que requerem uma tremenda quantidade de poder de computação, o que ainda é muito caro.

Estimativas mostram que a quantidade de energia necessária para a cadeia de bits Bitcoin para operar, é medido como o equivalente ao consumo de energia da Dinamarca até 2020[18].

Além disso, todo esse poder de computação está fazendo cálculos difíceis que não servem ao "interesse público" além de validar as transações. Seria ótimo se um algoritmo de consenso pudesse ser desenvolvido que realmente contribui para o interesse público, semelhante ao que foi feito com reCAPTCHA, que foi usado para o treinamento de redes neurais.

3.6.3 Velocidade da Transação

Atualmente, o Blockchain faz em média algo em torno de 7 transações por segundo. O fundador da Ethereum, Vitalik Buterin, afirma que Ethereum é capaz de fazer 8 transações por segundo. Se você compara isso com VISA, que é capaz de lidar com 2000 transações, e um pico de 56000 transações, por segundo, fica claro que a quantidade de transações que podem ser liquidadas por segundo é um grande desafio para Blockchains. Se Blockchains desejam substituir a web atual, isso deve ser aumentado drasticamente[18].

3.6.4 Segurança

A cadeia de blocos em si ainda não foi hackeada, embora tenha sido ao vivo há mais de 8 anos. No entanto, muitos dos serviços que o rodeiam já foram. As Organizações Autônomas Descentralizadas (DAO) foram hackeadas (devido a um bug em um contrato inteligente) e, posteriormente, quase perderam 50 milhões de dólares, o que só poderia ser evitado devido a uma dificuldade. Mt Cox, a maior troca de bitcoin do mundo, foi cortada e, como resultado, US \$ 460 milhões desapareceram. Além disso, a Bitfinex, uma plataforma de troca bitcoin de Hong Kong, perdeu US \$ 70 milhões. Esses hacks não ajudam a imagem segura de bitcoin e de criptografia. Embora bitcoin seja apenas uma aplicação do Blockchain, as pessoas podem não se sentir confortáveis com essas preocupações de segurança envolvendo Blockchains[18].

3.6.5 Capital Humano

A tecnologia Blockchain continua crescendo e se reiventando, como resultado, não muitos desenvolvedores têm dominado trabalhando com Blockchain relacionadas com outras tecnologias. Já existem centenas de startups Blockchain que necessitam de mão de obra. Como resultado, as organizações que querem passar para a web distribuída, encontram cada vez mais obstáculos na contratação de pessoas capazes. Como no caso de Big Data há alguns anos, levará tempo até que as universidades atinjam e comecem a desenvolver os cursos certos para a web distribuída. Isso pode atrasar o desenvolvimento de novas aplicações.

3.6.5 Vida dos Cidadãos

A tecnologia Blockchain poderia ser terrível para a privacidade e direito de auto-expressão das quais gozamos hoje.

Imaginamos que alguém cometeu um pequeno delito como roubar um pão em uma padaria aos 14 anos e foi para a delegacia, com o uso do Blockchain, seu delito

seria registrado em seu bloco. Quando essa mesma pessoa tentar concorrer a algum cargo importante pode perder a vaga por ter um registro como esse.

A tecnologia seria ótima para evitar corrupção e abusos de poder, poderia ser utilizado para pagamento de funcionários públicos, prestação de contas, fazendo um OpenData automático de gastos do governo. Porém, seria necessário um amadurecimento da democracia.

O anonimato nessas plataformas pode ser uma opção, desde que não sejam implementadas pelo governo. Já existe um enorme problema com a vigilância sobre o que faz o cidadão comum, pra onde vai, como se desloca, que doença tem etc, não precisamos de um sistema de registros que, somado à Internet das Coisas, possa rastrear tudo que fazemos.

3.7 Considerações Finais

A tecnologia Blockchain representa uma maneira fundamentalmente nova de fazer negócios. Ela inaugura uma próxima geração de vários aplicativos altamente escaláveis, robustos e inteligentes para o registro e troca de ativos físicos, virtuais, tangíveis e intangíveis. Graças aos conceitos-chave de segurança criptográfica, consenso descentralizado e um livro público compartilhado (com sua visibilidade devidamente controlada e autorizada), a tecnologia Blockchain pode alterar profundamente a forma como organizamos nossas atividades econômicas, sociais, políticas e científicas.

É certo que existem obstáculos que ressaltam a importância de continuar desenvolvendo e aprimorando a tecnologia, mas seu futuro promissor é algo quase inegável.

4. Blockchain e Internet das Coisas

Este capítulo aborda os principais conceitos relacionados a união das tecnologias Blockchain e Internet das Coisas. Na Seção 4.1, há uma descrição sobre os problemas enfrentados pela Internet das Coisas graças ao modelo centralizado. Na Seção 4.2, são apresentadas possíveis estratégias para a descentralização das redes IoT. Na Seção 4.3, são apresentadas utilizações concretas de Blockchain e IoT e na seção 4.7 uma breve conclusão sobre o que foi discutido ao longo do capítulo.

4.1 O Problema do Modelo Centralizado

Como mencionado anteriormente, a Internet das Coisas é uma indústria em rápido crescimento destinada a transformar casas, cidades, fazendas, fábricas e praticamente tudo o mais, tornando-os inteligentes e mais eficientes[19].

As possibilidades são praticamente incontáveis, especialmente quando o poder da Internet das Coisas é combinado com o de outras tecnologias, tais como a aprendizagem de máquina. Mas alguns obstáculos importantes surgirão à medida que bilhões de dispositivos inteligentes passarem a interagir entre si e com seus proprietários. Enquanto estes desafios não podem ser atendidos com os modelos atuais que estão apoiando as comunicações da Internet das Coisas, empresas de tecnologia e investigadores estão esperando para lidar com eles através do Blockchain[20].

O cenário atual de IoT depende de modelos de comunicação centralizados, mais conhecidos como paradigma servidor/cliente. Todos os dispositivos são identificados, autenticados e conectados por meio de servidores em nuvem que possuem grandes capacidades de armazenamento e processamento. A conexão entre os dispositivos tem que passar exclusivamente pela internet, mesmo que eles estejam a poucos metros de distância.

Enquanto este modelo centralizado tem funcionado perfeitamente nas últimas décadas e continuará a apoiar pequenas redes de IoT, torna-se problemático quando

o número de nós de rede cresce à casa dos milhões, gerando bilhões de transações, porque vai aumentar exponencialmente os requisitos computacionais e, por extensão, os custos.

Os servidores também podem se tornar um gargalo e um único ponto de falha, o que tornará as redes da Internet das Coisas vulnerável a negação de serviço (DoS / DDoS) , onde os servidores são direcionados e derrubados por ser inundado com o tráfego a partir de dispositivos comprometidos. Isso pode impactar criticamente os ecossistemas IoT, especialmente quando assumem tarefas mais sensíveis. Além disso, as redes centralizadas serão difíceis de estabelecer em muitos setores industriais, como grandes fazendas, onde os nós IoT se expandirão em áreas amplas com escassas redes de conectividade.

As soluções disponíveis para esses problemas são caras por causa da infraestrutura e custos elevados com manutenção de nuvem, grandes servidores e equipamentos de rede. O aumento dos dispositivos conectados aninhado a grande quantidade de dados por eles gerados irá aumentar os custos substancialmente.

Mesmo que os desafios citados no parágrafo anterior sejam superados, os servidores localizados na nuvem continuarão sendo um ponto de estrangulamento, que pode interromper toda a rede e a diversidade de propriedade dificulta a comunicação máquina-a-máquina (M2M) .

Não há nenhuma plataforma única que conecta todos os dispositivos e nenhuma garantia de que os serviços em nuvem oferecidos por diferentes fabricantes sejam interoperáveis e compatíveis[20].

4.2 Descentralização das Redes IoT

Um primeiro passo para a resolução dos problemas que foram abordados até o momento é uma base descentralizada para identificação e descoberta dos dispositivos.

Uma abordagem descentralizada da rede de IoT resolveria muitos dos problemas. A adoção de um modelo padronizado de comunicação peer-to-peer para

processar centenas de bilhões de transações entre dispositivos reduzirá significativamente os custos associados à instalação e manutenção de grandes centros de dados centralizados e distribuirá as necessidades de computação e armazenamento entre os bilhões de dispositivos que formam redes IoT . Isso impedirá falhas em qualquer nó único em uma rede e impedirá um colapso.

No entanto, o estabelecimento de comunicações peer-to-peer apresentará seu próprio conjunto de desafios, entre eles a questão da segurança e a segurança da Internet das Coisas é muito mais do que apenas sobre a proteção de dados sensíveis. A solução proposta terá de manter a privacidade e segurança em grandes redes da Internet das Coisas e oferecem alguma forma de validação e consenso para transações para evitar a falsificação e roubo[20].

A introdução de tecnologias como Blockchain pode oferecer registros globais e descentralizados dos dispositivos na rede, como sua identidade e chaves. Ao contrário dos sistemas centralizados em que os endereços são atribuídos num contexto hierárquico (device @ host, com o host a obter a sua identidade através da atribuição de um endereço IP ou registo de um nome de domínio DNS), uma abordagem baseada em blocos é mais ágil, o registro direto de propriedades de segurança também seria possível, uma vez que cada identidade registrada pode ser associada à chave pública do dispositivo, permitindo assim um cenário de comunicação mais seguro e uma maior confiança na rede global[21].

O conceito de Blockchain pode ser diretamente portado para redes IoT para lidar com a questão da escala, permitindo que bilhões de dispositivos compartilhem a mesma rede sem a necessidade de recursos adicionais. Blockchain também aborda a questão do conflito de autoridade entre os diferentes fornecedores, fornecendo um padrão em que todos têm estacas e benefícios iguais[20].

Isso ajuda a desbloquear comunicações M2M que eram praticamente impossíveis sob modelos anteriores, e permite a realização de casos de uso totalmente novo.

A tecnologia Blockchain poderia fornecer uma maneira de rastrear o histórico único de dispositivos individuais, gravando um registro de trocas de dados entre ele e outros dispositivos, serviços web e usuários humanos.

Blockchains também poderia permitir que dispositivos inteligentes se tornassem agentes independentes, realizando autonomamente uma variedade de transações. Como uma máquina de venda automática que não só pode monitorar e relatar seu próprio estoque, como também pode solicitar lances de distribuidores e pagar pela entrega de novos itens automaticamente, com base, obviamente, no histórico de compras de seus clientes. Ou um conjunto de eletrodomésticos inteligentes que podem alternar a prioridade de uso de modo que a máquina de lavanderia e máquina de lavar louça funcionam em um momento adequado, minimizando o custo da eletricidade contra os preços da grade atual. Ou um veículo que pode diagnosticar, agendar e pagar por sua própria manutenção.

Tal como está, o Blockchain tem o potencial de ajudar a ultrapassar os obstáculos para alcançar o crescimento desejado na Internet das Coisas, devido às seguintes propriedades[22]:

- Escala: Blockchain é verdadeiramente escalável, pois ele pode escalar da mesma forma que uma torrente consegue escalar centenas de milhares de pares;
- Padronização: Tem potencial para padronizar toda a rede;
- Segurança: a segurança é embutida. O fato de que o Blockchain é distribuído entre dezenas de milhares de computadores significa que o hacking é quase impossível ou inviável;
- Transparência: como o endereço público de criptografia do emissor e receptor de cada evento é gravado, e tudo está disponível para inspeção;
- Privacidade: pode oferecer grande melhoria em termos de privacidade, como os usuários estão sob pseudônimo e pode executar operações de imediato, sem a necessidade de qualquer tipo de autenticação pessoal;
- Imunidade: Blockchain é imune à censura já que nenhuma autoridade única tem o controle geral sobre ele (devido à sua estrutura descentralizada). Se o banco de dados de uma instituição ou de um sistema de nuvem cair, os usuários não poderão realizar transações de dados com ele, o que, em muitos casos, pode ter consequências graves. Com Blockchain, os usuários

podem ter acesso contínuo, aberto, sem qualquer risco potencial de interrupção.

4.3 Utilizações Concretas de Blockchain e IoT

Um novo paradigma na concepção de aplicativos habilitados para IoT pode emergir das tecnologias mais avançadas de blocos inteligentes que estão sendo desenvolvidas. A combinação Internet das Coisas e Blockchain está ganhando impulso e vem sendo aplicada tanto por gigantes do mundo tecnológico quanto startups.

A IBM e Samsung criaram o ADEPT (Automated descentralizada P2P Telemetry), um sistema que usa Blockchain para oferecer suporte a Internet das Coisas descentralizada, que permite que milhares de milhões de dispositivos transmitam transações entre pares e realizem auto-manutenção. A plataforma foi testada em vários cenários, incluindo um que envolve uma máquina de lavar inteligente que pode automaticamente pedir e pagar por detergente com bitcoins ou éteres e será capaz de negociar através de contratos inteligentes com base no seu proprietário[19].

Em um dos primeiros papers²⁰ da IBM que aborda o uso de Blockchain em Internet das Coisas, é descrito como novos dispositivos podem ser registrados inicialmente num Blockchain universal (quando montado pelo fabricante) e mais tarde transferido para Blockchains regionais (depois de ser vendido para comerciantes ou clientes) onde eles podem interagir de forma autônoma com outros dispositivos que compartilham o Blockchain.

A combinação da Internet das Coisas e Blockchain também está criando a possibilidade de uma economia circular, onde os recursos podem ser compartilhados e reutilizados em vez de comprados uma vez e descartados após o uso.

O projeto Ethereum, que é bastante complexo, é mais uma aplicação da Blockchain. Ele se concentra no tempo de desenvolvimento e segurança de pequenas aplicações, e na capacidade de diferentes aplicações interagirem com

²⁰ <https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF>

eficiência. O projeto faz isso construindo o que é, essencialmente, uma camada final: um Blockchain com uma linguagem de programação incorporada, permitindo que qualquer pessoa escreva contratos inteligentes e aplicações descentralizadas (DAPPs) ou organizações autônomas descentralizadas (DAOs) onde podem criar suas próprias regras arbitrárias de propriedade, formatos de transações e funções de transição de estado.

Blockchain também permitirá a monetização de dados, onde os proprietários de dispositivos e sensores da Internet das Coisas pode compartilhar os dados da Internet das Coisas geradas em troca de micropagamentos em tempo real. Tilepay, por exemplo, oferece um mercado on-line descentralizado seguro onde os usuários podem registrar seus dispositivos na Blockchain e vender seus dados em tempo real em troca de moeda digital.

Filament é uma startup que está investindo em Internet das Coisas e Blockchain com foco em aplicações industriais, tais como agricultura, indústria e petróleo e gás. A startup usa sensores sem fios, chamados Taps que criam redes de malha autônomas de baixa potência que permitem às empresas gerenciar operações físicas de mineração ou fluxos de água em campos agrícolas sem depender de alternativas de nuvem centralizadas. A empresa usa a tecnologia Blockchain para identificar e autenticar dispositivos e também cobrar por serviços de rede e dados.

Blockchain e IoT também têm casos de uso interessantes que podem ajudar a tornar as fontes de energia renováveis, onde a energia produzida por painéis solares IoT gera valor em criptomoedas. Qualquer pessoa que ingressar na rede pode fazer investimentos em tecnologia de energia renovável. Chain of Things é um consórcio que está explorando o papel de Blockchain em lidar com as questões de escala e de segurança na Internet das Coisas. Em uma hackathon recente realizada em Londres, o grupo demonstrou o uso de Blockchain e Internet das Coisas em um estudo de caso envolvendo uma pilha de energia solar projetado para fornecer dados confiáveis, verificáveis e renováveis, reduzindo as possibilidades de fraude. O sistema facilita o processo em que um painel solar se conecta a um registrador de dados, rastreia a quantidade de energia solar produzida, entrega com segurança esses dados a um nó e os registra em um ledger distribuído que é sincronizado

através de uma rede global mais ampla de nós.

A extensão EXP é uma criptografia de informações, aplicativos e plataforma de contrato descentralizado. É um dos primeiros a ser distribuído de forma justa, controlado democraticamente e administrado pela comunidade. Através do uso de contratos inteligentes e tecnologia de blocos descentralizados, ele é executado não por qualquer indivíduo ou grupo, mas pelos usuários de Expanse em si[22].

A gigante australiana de telecomunicações Telstra é outra empresa que pretende alavancar o uso da tecnologia Blockchain em casas inteligentes. Os hashes criptográficos do firmware do dispositivo são armazenados em uma cadeia de bloqueios privada para minimizar o tempo de verificação e obter a resistência à violação e a detecção de violação em tempo real.

Como a maioria dos dispositivos domésticos inteligentes são controlados por meio de aplicativos para dispositivos móveis, a Telstra expande ainda mais o modelo e adiciona informações biométricas do usuário aos hashes Blockchain a fim de vincular a identidade do usuário e evitar que dispositivos móveis comprometidos assumam a rede. Desta forma, o Blockchain será capaz de verificar tanto a identidade de dispositivos IoT quanto a identidade das pessoas interagindo com esses dispositivos.

Como mencionado nas aplicações da tecnologia, a Blockchain apresenta muitas promessas para o futuro da IoT. Desafios permanecem, como modelos de consenso e os custos computacionais de verificação de transações. Mas ainda estamos nos estágios iniciais do desenvolvimento de cadeias de blocos, e esses obstáculos serão eventualmente superados, abrindo o caminho para muitas possibilidades[19].

4.4 Considerações Finais

Ainda não é possível afirmar que o futuro da Internet das Coisas depende do Blockchain. Certamente as startups que estão atualmente testando e melhorando esse campo ainda não são suficientes para criar um efeito de rede que provoque a entrada de mais empresas no uso de suas ideias.

Blockchain apresenta inúmeras possibilidades em relação à segurança cibernética e da Internet das Coisas. Com os dispositivos cada vez mais baratos, o poder de computação está se tornando cada dia maior. Blockchain oferece uma oportunidade para estabelecer um sistema confiável, que permite protocolos de mensagens peer-to-peer (altamente criptografado), compartilhamento seguro de dados distribuídos e uma maneira de coordenar todos os dispositivos que lhes permite validar cada transação. Todos os sinais apontam para um futuro em que Blockchain desempenha um papel importante na Internet das Coisas.

5. Conclusão e Trabalhos Futuros

A união e aplicação das tecnologias Blockchain e Internet das Coisas não é livre de falhas e/ou deficiências. Ainda existem alguns obstáculos que precisam ser superados. De um lado há disputa entre desenvolvedores sobre a arquitetura da tecnologia Blockchain subjacente, que tem desde o seu princípio problemas decorrentes do aumento no número de transações e crescimento da rede. Algumas destas questões são inevitavelmente aplicadas à extensão da cadeia de blocos para Internet das Coisas.

Tais implicações foram reconhecidas por empresas de tecnologia e várias soluções incluindo árvores-concorrentes, mini-Blockchains e cadeias laterais, estão sendo testadas para corrigir o problema.

O poder de processamento e o aumento no consumo de energia também são pontos de preocupação. A criptografia e a verificação de transações Blockchain são operações computacionalmente intensivas e requerem uma potência considerável para realizar, o que está faltando em muitos dispositivos que contam com a Internet das Coisas. O mesmo vale para o armazenamento, já que os registros Blockchain começam a crescer em tamanho e precisam ser redundantemente armazenados em nós de rede.

As redes da Internet das Coisas autônomas alimentados por Blockchain irão colocar desafios aos modelos de negócios que os fabricantes estão buscando, que inclui relações de assinatura de longo prazo com fluxos de receita contínua e uma grande mudança econômica e nos modelos de negócios e se fará necessário.

Apesar de toda a confiança passada pela tecnologia Blockchain, ainda é muito cedo para dizer se Blockchain será a resposta definitiva para os problemas da indústria de IoT em rápida evolução. A união das duas tecnologias, como já mencionado, ainda não é perfeita, no entanto, é uma combinação muito promissora para o futuro da Internet das Coisas, onde redes descentralizadas e autônomas terão um papel decisivo.

Na sequência do presente estudo surgiram alguns pontos que se revelaram interessantes para uma abordagem mais detalhada. A seguir são referidos sumariamente possíveis objetos de uma futura investigação:

- Um aprofundamento no estudo da plataforma Ethereum e como são criadas as inúmeras vertentes disponíveis por ela;
- Um estudo experimental, de forma que sejam vistos na prática os pontos positivos e negativos da união de Blockchain e Internet das Coisas;
- Um estudo de como a tecnologia Blockchain poderia ser desenvolvida e aplicada em outras vertentes, não somente em IoT.

6. Bibliografia

1. TIME MJV. **Da internet ao Blockchain**, 2016. Disponível em: <<http://blog.mjv.com.br/da-internet-ao-Blockchain>>. Acesso em: 28 de setembro 2016.
2. FINEP. **Kevin Ashton – entrevista exclusiva com o criador do termo “Internet das Coisas”**, 2015. Disponível em: <<http://finep.gov.br/noticias/todas-noticias/4446-kevin-ashton-entrevista-exclusiva-com-o-criador-do-termo-internet-das-coisas>>. Acesso em: 28 de setembro 2016.
3. POETAS.IT, (2016) **IoT - Uma Estratégia para o Brasil / Consolidação de uma visão unificada para orientação e proposição de políticas públicas sobre Internet das Coisas no Brasil v.1.0**. Disponível em: <www.cesar.org.br/poetas.it/visionstatement> Acesso em 25 de agosto de 2016
4. HBR - Harvard Business Review. **How Smart, Connected Products Are Transforming Competition**, 2014. Disponível em: < https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition&usg=ALkJrhgHowoDLFU_i5bFjZAKIBwWtgUJvw> Acesso em: 21 de outubro de 2016
5. ITU, (2005). **Internet reports–The internet of things**. Disponível em: <<https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internet-of-Things-2005.pdf>> Acesso em: 20 de outubro de 2016
6. S. H. Hashemi, F. Faghri, P. Rausch and R. H. Campbell, **"World of Empowered IoT Users,"** 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), Berlin, 2016. Disponível em: <<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7471347&isnumber=7471335>> Acesso em : 21 de outubro de 2016
7. Gartner, (2014). **Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015**. Disponível em: <<http://www.gartner.com/newsroom/id/2905717>>. Acesso em: 21 de outubro de 2016

8. Medtronic. **Sobre o dispositivo**. Disponível em: <<http://www.medtronicbrasil.com.br/your-health/diabetes/device/continuous-glucose-monitor/what-is-it/>> Acesso em: 05 de novembro de 2016
9. Veja. **Philips inicia venda de lâmpadas controladas pelo smartphone no Brasil**. Disponível em: <<http://veja.abril.com.br/tecnologia/philips-inicia-venda-de-lampadas-controladas-pelo-smartphone-no-brasil/>> Acesso em 05 de novembro de 2016
10. Corretor Tech. **Com a campanha Wi-fi as chaves dos imóveis serão apenas detalhes**. Disponível em: <<http://corretortech.com.br/com-essa-campainha-as-chaves-do-imoveis-serao-apenas-detalhes/>> Acesso em: 05 de novembro de 2016
11. IBM. **Blockchain basics: Introduction to business ledgers**. Disponível em: <http://www.ibm.com/developerworks/cloud/library/cl-Blockchain-basics-intro-bluemix-trs/index.html?utm_source=dwtv&utm_medium=iottv&utm_term=Blockchain&utm_campaign=The%20convergence%20of%20IoT%20and%20Blockchain> Acesso em 09 de novembro de 2016
12. IBM. **Blockchain basics: Glossary and use cases**. Disponível em: <<https://www.ibm.com/developerworks/cloud/library/cl-Blockchain-basics-glossary-bluemix-trs/index.html>> Acesso em 09 de novembro de 2016
13. Portal CD Brasil. **Criptomoeda (Bitcoin) e Blockchain – Fim da certificação digital?** Disponível em: <<http://portalcdbrasil.com.br/criptomoeda-bitcoin-e-blockchain-fim-da-certificacao-digital/>> Acesso em 09 de novembro de 2016
14. SWAN, Melanie. **Blockchain: Blueprint for a New Economy**. Estados Unidos: O'Reilly, 2015
15. Originalmy. **Como a tecnologia Blockchain pode mudar a forma como fazemos negócios**. Disponível em: <<http://blog.originalmy.com/2016/01/22/como-a-tecnologia-Blockchain-pode-mudar-a-forma-como-fazemos-negocios/>> Acesso em: 15 de novembro de 2016
16. Computerworld. **Blockchain: O que é e como funciona**. Disponível em: <<http://computerworld.com.br/blockchain-o-que-e-e-como-funciona>> Acesso em 15 de novembro de 2016

17. Hiperledger. **About**. Disponível em: <<https://www.hyperledger.org/about>> Acesso em: 15 de novembro de 2016
18. Datafloq. **What is the Blockchain – part 3 – Blockchain Startups and Five Challenges to Overcome**. Disponível em: <<https://datafloq.com/read/what-is-Blockchain-part-3-startups-five-challenges/2381>> Acesso em 15 de novembro de 2016
19. Venturebeat. **How Blockchain can change the future of IoT**. Disponível em: <<https://cdn.ampproject.org/c/venturebeat.com/2016/11/20/how-Blockchain-can-change-the-future-of-iot/amp/>> Acesso em: 20 de novembro de 2016.
20. TechCrunch. **Decentralizing IoT networks through Blockchain**. Disponível em: <[https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-Blockchain/?ncid=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Techcrunch+\(TechCrunch\)&sr_share=twitter](https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-Blockchain/?ncid=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Techcrunch+(TechCrunch)&sr_share=twitter)> Acesso em 20 de novembro de 2016
21. Coincenter. **How can Blockchains improve the Internet of Things?** Disponível em: <<https://coincenter.org/entry/how-can-Blockchains-improve-the-internet-of-things>> Acesso em 30 de novembro de 2016
22. DesignSpark. **When the Blockchain Technology meets the Internet of Things**. Disponível em: <<https://www.rs-online.com/designspark/when-the-Blockchain-technology-meets-the-internet-of-things>> Acesso em 30 de novembro de 2016