PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
Programa de Pós-Graduação em Administração e Programa de Pós-Graduação em Economia FEA/PUC-SP

SUSTENTABILIDADE

DESAFIO 6

CONVERGÊNCIA MUNDIAL DAS TIs

Disciplina Sustentabilidade 2s 2019
Turma: ADM-NA91
Prof. Dr. Arnoldo José de Hoyos Guevara

Richie Powar Mu Han Lee

São Paulo – SP
2019

SUMÁRIO

INTRODUÇÃO 4
CAPÍTULO I: CONVERGÊNCIA MUNDIAL DAS Tis 4
1.0 - Qual o Nível de Segurança da Convergência Mundial das TIs aos Usuários? 4
1.1 – Conceitos 5
1.1.1 - A Importância da Segurança Cibernética 7
1.1.2 - Início da Segurança Ibernética no Brasil 8
1.2 - Quais os Benefícios da Convergência Mundial das TIs aos Usuários? 10
1.2.1 - Conceitos do Big Data 11
1.2.2 - Conceitos da Inteligência Artificial 12
1.2.3 - Conceitos de Cloud Computing 12
1.2.4 - Conceitos da Internet das Coisas – IoT 13
1.2.5 - Benefícios da Indústria 4.0 na Logística 13
CAPÍTULO II. BLOCK CHAIN 14
2.0 - Conceitos Básicos 14
2.1 - Conceito sobre a Criptografia de Chave Pública 14
2.1.1 - Conceito sobre a Função Hash 15
2.1.2 - Conceito sobre a Assinatura Digital 17
2.1.3 - Conceito sobre Redes P2P 19
2.2 - Funcionamento do Blockchain 21
2.2.1 - A Cadeia de Blocos 21
2.2.2 - Transações (Registros) 22
2.2.3 - Validação de blocos (Mineração) 22
2.3 - Segurança do Blockchain 23
2.3.1 - Ataque 51% 23
2.3.2 - Chaves e Aleatoriedade 24
2.3.3 - Confidencialidade e Anonimato 25
CAPÍTULO III. SOCIETY 5.0 26
3.0 - Trilhando o Caminho para *Society 5.0* 26
CONCLUSÃO 32
REFERÊNCIAS BIBLIOGRÁFICAS 33

INTRODUÇÃO

O tema abordado por esse trabalho acadêmico é um tema bastante polêmico, bem intuitivo pelo menos para grande maioria das pessoas e oferecem informações bem relevantes acerca dos assuntos tecnológicos da atualidade. Essa convergência mundial das TIs impacta a todos da sociedade global e influência de forma gigantesca, já se pode perceber uma grande revolução industrial, onde a tecnologia está presente em tudo, considerado como a quarta revolução industrial. Nesse trabalho será conceituado alguns pontos dessa quarta revolução industrial e mostrar como tudo está interconectado e é influenciado também.

Esse trabalho acadêmico tem o intuito e o objetivo de esclarecer, demonstrar e fornecer informações importantíssimas acerca das tecnologias envolvidas e mais discutidas da atualidade e sobre o conceito dessa quarta revolução industrial.

Será demonstrado nesse trabalho utilizando dados retirados de artigos acadêmicos, livros, monografias, anotações em aula e notícias.

A abordagem feita aqui no trabalho sobre essa nova sociedade e era da tecnologia podem trazer muitos benefícios à sociedade como mais segurança e mais praticidade em muitas coisas do dia a dia, mas também não se pode esquecer o outro lado da moeda, onde a tecnologia pode trazer crises no futuro do trabalho e falta de privacidade. Então até que ponto a tecnologia beneficia a sociedade e até qual ponto deve utilizar a tecnologia e também de que forma usar, isso depende de cada usuário e de todos os envolvidos.

Muito importante também ver que todos dentro dessa convergência mundial das TIs deve fazer sua parte e manter a segurança dessa nova onda de tendências tecnológicas no eixo e ver os dois lados da moeda.

Visto o apresentado, coloca-se como problema de pesquisa: Qual o nível de segurança e os benefícios da convergência mundial das tecnologias de informações e comunicações aos usuários?

CAPÍTULO I: CONVERGÊNCIA MUNDIAL DAS TIs

1.0 - Qual o Nível de Segurança da Convergência Mundial das TIs aos Usuários?

Segundo Canongia; Mandarino (2009), foi criado uma reunião, a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), na qual ocorreu em março de 2009, para discussão de pontos importantes e recomendações acerca do assunto e do surgimento da nova Sociedade da Informação.

> Os pontos a serem destacados sobre esta nova Sociedade da Informação, lá apresentados foram: a) convergência de tecnologias, aumento significativo de sistemas e redes de informação, aumento crescente de acesso à Internet, avanços das tecnologias de informação e comunicação; b) aumento das ameaças e das vulnerabilidades, apontando para a urgência de ações na direção da criação, manutenção e fortalecimento da cultura de segurança; e, c) ambiente em constante, e rápidas mudanças. (CANONGIA; MANDARINO, 2009, p. 24).

Ainda constatando sobre um fator mencionado de grande destaque na reunião foi sobre o tema Cultura da Segurança como uma estratégia dos países e nações. Alguns pontos bem importantes sob o assunto como: as partes envolvidas devem assegurar a segurança de acordo com suas habilidades e competências, e devem ser sensibilizados em relação aos riscos referentes à segurança de sistemas e redes de informações; todos os envolvidos, o governo, as empresas e outros como pesquisadores devem se preocupar e se responsabilizarem acerca da segurança da informação. (CANONGIA; MANDARINO, 2009).

Segundo Canongia; Mandarino (2009), os países que fazem parte e são membros da OCDE, estão desenvolvendo suas estratégias referentes à segurança na Sociedade da Informação baseando-se em nove princípios conforme descritos e listados abaixo:

> 1) sensibilização sobre riscos – seguir normas e boas práticas, implantar controles, e estar em alerta sobre todo tipo de interconectividade e interpendência de sistemas e redes de informação; 2) responsabilidade – entender a importância de avaliar e atualizar sistematicamente as políticas, práticas, medidas e procedimentos de segurança adotados para sistemas e redes de informação; 3) resposta – agir pró ativamente e em cooperação, prevenindo, detectando e respondendo aos incidentes; 4) ética – respeitar interesses legítimos de todas as partes envolvidas; elaborar e adotar práticas exemplares na condução da segurança de sistemas e redes de informação; 5) democracia – seguir e fortalecer valores fundamentais de uma sociedade democrática na segurança de sistemas e redes de informação; 6) avaliação de riscos – minimizar ameaças e vulnerabilidades por meio de ações que sejam amplas o bastante para englobar os fatores críticos internos e externos

> (tecnologias, físicos, humanos, políticos, serviços de terceiros). A avaliação de risco tanto permitirá determinar o nível de risco aceitável quanto facilitará a adoção de medidas de controle apropriadas ao tipo de informação a ser protegida; 7) concepção – integrar segurança como elemento essencial no processo de planejamento, modelagem, criação e gestão de sistemas e rede de informação, com soluções inovadoras; 8) gestão da segurança – coordenar e integrar a avaliação de riscos e a capacidade de resposta e resolução de incidentes, bem como a auditoria de sistemas e redes de informação, para criar um sistema coerente de segurança da informação; e, 9) reavaliação – examinar e reavaliar a segurança de sistemas e redes de informação, e introduzir as necessárias mudanças nas respectivas políticas, estratégias, medidas e procedimentos. (CANONGIA; MANDARINO, 2009, p. 24).

Com todas essas estratégias tomadas por países na tentativa de manter sempre as informações atualizadas e seguras é um passo importantíssimo ao cenário atual das convergências mundiais das TIs, sendo um objeto de estudo e "essencial à manutenção e preservação das infraestruturas críticas de um país, tais como saúde, energia, defesa, transporte, telecomunicações, da própria informação, entre outras." (CANONGIA; MANDARINO, 2009, p. 25).

1.1 - Conceitos

De acordo com Willian Gibson em seu romance "Neuromancer" (2005) *apud* Canongia; Mandarino (2009), o ciberespaço (ou espaço cibernético) é definido e descrito como um espaço onde não há parte física desenvolvida por redes de computador, mais especificamente a internet, onde os usuários e pessoas participantes podem se comunicar de forma livremente de diferentes formas, através de mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros.

Referente aos conceitos de Segurança Cibernética também da Defesa Cibernética, ainda estão sendo formados, desenvolvidos e construídos com a existência de diferentes agentes, no país. Em um momento inicial compreende-se o escopo de atuação da Segurança Cibernética com aspectos, comportamentos e atitudes tanto de prevenção como também para reprimir. Em relação à Defesa Cibernética entende-se como inúmeras ações operacionais para combater ataques ofensivos. (CANONGIA; MANDARINO, 2009).

Segundo, o Glossário das Forças Armadas (MD35-G-01;2007) *apud* Canongia; Mandarino (2009, p.26), "o termo defesa é entendido como o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança, ou ainda, como reação contra qualquer ataque ou agressão real ou iminente".

De acordo com a *International Communications Union,* ITU (2007) *apud* Canongia; Mandarino (2009), o conceito de Segurança Cibernética, "Cybersecurity", é definida como uma maneira de prover proteção contra o acesso, manipulação e destruição não autorizada de recursos críticos e bens. Tanto esses recursos e bens diferem e dependem com certeza do nível de desenvolvimento dos países. Outro fator também importante que depende é o que cada país considera como seu próprio recurso crítico e até que ponto estão dispostos a se esforçarem bem como realizarem avaliações do risco, na qual pretendem aceitar, por motivos e consequências através das medidas inadequadas de segurança cibernética.

> Adicionalmente, para certo número de países desenvolvidos, há outras ameaças tais como fraude, proteção do consumidor, e privacidade, as quais consideram também como soluções da cybersecurity, forma de proteger e manter a integridade das infraestruturas críticas nos setores financeiro, de saúde, da energia, do transporte, das telecomunicação, da defesa, e de outros. (ITU, 2007, p. 10 *apud* CANONGIA; MANDARINO, 2009, p. 26).

Segundo informações da ITU, as áreas de grande impacto e importância, dos países que são membros da OCDE, para a divulgação e promoção da *cybersecurity* são:

> a) Áreas de elevada atenção: Combate ao crime cibernético, Criação em nível nacional de CERTs/CSIRTs (Computer Emergency Response Teams/Computer Security Incident Response Teams); Aumento da cultura de segurança cibernética e suas atividades; e Promoção da educação; b) Áreas com menos atenção: Pesquisa e Desenvolvimento; Avaliação e monitoramento; e Atendimento às pequenas e médias empresas (PMEs). (SUND, 2008 *apud* CANONGIA; MANDARINO, 2009, p. 26).

No Brasil foram adotados dois conceitos no âmbito da esfera pública que dão fundamentação e embasamento à abordagem da segurança cibernética, sendo assim, o primeiro, denominado de "infraestrutura crítica da informação" e o segundo definido como "ativos da informação". (BRASIL, 2009 *apud* CANONGIA; MANDARINO, 2009, p. 27).

> No âmbito do governo federal brasileiro, considera-se "infraestrutura crítica da informação" o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. E, complementarmente, consideram-se "ativos de informação", os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios, e as pessoas que a eles têm acesso. (BRASIL, 2009 *apud* CANONGIA; MANDARINO, 2009, p. 27).

1.1.1 - A Importância da Segurança Cibernética

Desde meados do ano de 2009, já existiam muitos debates, discussões e fóruns sobre assuntos que envolvam termos e expressões como "ataques cibernéticos", "segurança cibernética", "espaço cibernético", "regulamentação da Internet", "direitos de privacidade", "crimes cibernéticos", "violação de direitos de propriedade intelectual", entre outros. Tudo isso faz com que as autoridades, líderes de vários países fiquem de olho e ponham toda a atenção no uso da Internet, a interconectividade das redes e a convergência digital nesse novo surgimento da Sociedade da Informação e seus desafios. (CANONGIA; MANDARINO, 2009).

> Um bom retrato da atualidade, a exemplificar, foi o ocorrido em julho de 2009, em que o sítio do Departamento de Defesa dos EUA foi invadido por 4 dias consecutivos, numa ação que atualmente tem sido comum por parte dos chamados hackers, de tentativa de saturação de acesso e conexão a um determinado sítio da Internet até que o mesmo seja interrompido e seu acesso bloqueado. E, da mesma forma, sítios do governo da Coréia do Sul sofreram com ação similar, tornando lento o acesso à Internet naqueles mesmos dias do início de julho. Dados dos serviços de inteligência de ambos os países informaram que tal ataque cibernético partiu de 16 países, inclusive dos EUA e da Coréia do Sul, fazendo uso de cerca de 20 mil computadores domésticos e 80 provedores da Internet. (SILVA, 2009 *apud* CANONGIA; MANDARINO, 2009, p. 27).

De acordo com a MICROSOFT (2008) *apud* CANONGIA; MANDARINO (2009), uma grande empresa muito bem reconhecida e renomada no mercado de TI do mundo, destacou em seu relatório, *Microsoft Security Intelligence Report,* dezesseis pontos críticos referentes à segurança e à privacidade na Internet, nos últimos seis meses, sendo eles quatro como, por exemplo:

> 1) exploração de vulnerabilidade de browser: as máquinas baseadas no Windows XP foram as mais atacadas, representando cerca de 40,9% do total de ataques monitorados pela empresa; 2) exploração de vulnerabilidade do sistema Office: a vulnerabilidade mais frequentemente explorada foi uma simples e antiga, representando 91,3% dos ataques examinados, mesmo que a solução de tal vulnerabilidade tenha sido disponibilizada pela empresa há dois anos (CVE-2006-2492), indicando por consequência uma ameaça, qual seja, a ação dos usuários de não atualização das versões do sistema Office de forma sistemática; 3) softwares maliciosos: a tendência mais significativa observada foi a detecção de aumento bastante expressivo de softwares maliciosos em muitos países e regiões no mundo, sendo que a depender da cultura de cada Nação há um tipo que mais se salienta. Por exemplo, na China malwares que modificam browsers prevalecem, ao passo que no Brasil os alvos são malwares para captura de senha e fraudes bancárias prevalecendo o cavalo de tróia conhecido como Trojanspy:win32/Bancos, e na Coréia os vírus são os mais comumente disseminados, em especial os

> conhecidos Win32/Virut e o Win32/Parite; e, 4) emails: mais de 97% dos emails que trafegaram na Internet, mais especificamente no Hotmail que é o monitorado pela empresa, foram indevidos, ou seja, foram enviados por meio de spams ou de ataques cibernéticos nos casos de intenção maliciosa. (MICROSOFT, 2008 *apud* CANONGIA; MANDARINO, 2009, p. 28).

Em relação ao governo brasileiro, os resultados de uma pesquisa realizada em 2007 pelo Tribunal de Contas da União (TCU) em 250 órgãos públicos, apontam vários problemas, fraquezas e deficiências na gestão de Governança de Tecnologia da Informação, pontos referentes à Segurança da Informação foram os mais acentuados. (DOU, 2002 *apud* CANONGIA; MANDARINO, 2009).

> Segundo as palavras de Raphael Mandarino Junior, o diretor do departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, em entrevista realizada em 2009 para a Revista Galileu, "Nós temos 320 grandes redes. Chamo-as de grandes redes porque cada uma pode ter suas sub - redes: o Exército, por exemplo, tem redes no Brasil inteiro, mas eu conto como uma só. O Brasil recebe 2.000 (dois mil) ataques por hora nessas redes – isso são apenas tentativas de invasão para roubar dados, não estou contando vírus e spams. (...) Nem sempre é uma pessoa que faz o ataque. Em muitos casos alguém invade um computador, usa um software – robô, e fica tentando atacar as redes do governo várias vezes. Eu detecto o ataque e identifico de que computador ele vem, então notifico o administrador daquela rede. Normalmente eu chego no computador que foi invadido para invadir o nosso, não ao computador do hacker. Mas ao menos eu fecho essa porta". (CANONGIA; MANDARINO, 2009, p. 29).

Os ataques cibernéticos e ciberterrorismo são uma tendência mundial. No Brasil esses mesmos são mais graves, pois ainda são assuntos específicos e conhecimentos específicos de poucos, assim como, os recursos financeiros são muito baixos e insuficientes. (WOLOSZIN, 2009 *apud* CANONGIA; MANDARINO, 2009).

Por todos esses motivos e fatores que o tema sobre a segurança cibernética vem sendo tratado cada vez mais intensamente no âmbito governamental e mundial, por essa mesma razão esse assunto é bem importante. (CANONGIA; MANDARINO, 2009).

1.1.2 - Início da Segurança Ibernética no Brasil

Segundo a publicação do relatório de ameaças à segurança, elaborado pela Sophos no começo de 2007 *apud* CANONGIA; MANDARINO (2009), indica de que a China foi o maior responsável na produção de 30% dos softwares maliciosos virtuais espalhados pelo mundo inteiro no ano de 2006. Em segundo lugar vem o Brasil, com cerca de 14,2%, conforme divulgação na época pelo Núcleo Operacional da Sociedade da Informação no Brasil.

Recentemente, foi desenvolvido e publicado a Instrução Normativa IN GSIPR No. 01/2008 define que a Segurança da Informação e Comunicações (SIC), "são ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações." (CANONGIA; MANDARINO, 2009, p. 37).

> Neste contexto, destacam-se os avanços até então alcançados, como resposta à percepção de necessidade de prover quadros no campo de conhecimento de SIC, desde 2006 até julho de 2009, pelo DSIC/GSIPR, em que foram utilizados recursos orçamentários destinados à formação de recursos humanos da seguinte forma: a) eventos de sensibilização tipo palestras sobre o tema para um público estimado de 24 mil pessoas tanto no Brasil quanto no exterior; b) eventos de conscientização tipo seminários, oficinas e congressos para 2.372 servidores públicos distribuídos por mais de 40 instituições da administração pública federal espalhados em diversas capitais pelo Brasil; c) eventos de capacitação tipo cursos básicos e de fundamentos para 395 servidores públicos de 38 instituições da administração pública federal em Brasília, Rio de Janeiro, São Paulo, Porto Alegre e Fortaleza; e, d) eventos de especialização tipo curso de pósgraduação para 80 servidores públicos e militares de 23 instituições da administração pública federal, em duas turmas. No processo de evolução, está planejado para 2009 a formatação e execução de cursos básicos de fundamentos e de especialização à distância. (CANONGIA; MANDARINO, 2009, p. 39).

A definição inicial e mais plausível para Estratégia Cibernética no Brasil é a palavra "arte", pois se trata de uma tarefa única que exige muita criatividade, conhecimento profundo e detalhado das características próprias de cada Estado e Sociedade. Assim sendo, foram indicadas algumas condições essenciais para existência e a continuidade da Sociedade da Informação no Brasil:

> a) conhecer o grau de vulnerabilidade do país em relação aos seus sistemas de informação e as suas infraestruturas críticas de informação; b) Identificar os serviços críticos essenciais da infraestrutura de informações para o funcionamento da infraestrutura crítica; c) determinar o grau de dependência dos serviços das infraestruturas críticas de informações sobre as infraestruturas críticas; d) desenvolver uma metodologia comum para avaliar a vulnerabilidade das infraestruturas críticas de informação dos seus sistemas e de seus serviços; e) elaborar uma metodologia para avaliações de risco em segurança cibernética; f) conceber um sistema de medidas preventivas contra ataques cibernéticos; g) compreender que a segurança cibernética só se dará plenamente se, na informatização de seus sistemas críticos, o conceito de segurança da informação e comunicações forem observados de forma eficiente; h) estabelecer que às aquisições de produtos e serviços usados em sistemas críticos devam ser testados e certificados por critérios próprios à APF; i) desenvolver algoritmos criptográficos próprios e estabelecer critérios para seu uso; j) construir o marco legal contra ataques cibernéticos; k) estabelecer programas de cooperação entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional; l) estreitar parcerias e

> ações colaborativos com o setor privado; m) desenvolver programa nacional de capacitação em segurança cibernética e recrutamento, que seja construído à partir da visão interdisciplinar que o tema requer, nos níveis básico técnico, graduação, especialização, mestrado e doutorado; e, n) promover e fortalecer a pesquisa, o desenvolvimento, e a inovação em segurança cibernética e temas correlatos. (CANONGIA; MANDARINO, 2009, p. 42).

Em questões políticas, econômicas e sociais, nessa era atual da nova Sociedade da Informação, que são muito dependentes da "base educacional, do desenvolvimento científico e tecnológico, e da capacidade de articulação e de promoção de parcerias de uma nação, que seja formulada a estratégia de segurança cibernética brasileira". (CANONGIA; MANDARINO, 2009, p. 43).

> Certamente, a segurança cibernética requer um maior diálogo e consequente fortalecimento nas relações da tríplice hélice (governo, academia e setor privado), bem como, o fortalecimento, em nível nacional e internacional, da cooperação técnica e da inserção do país em fóruns de formação de opinião e de decisão. (CANONGIA; MANDARINO, 2009, p. 43).

Por fim, ainda existem muitos pontos ainda para serem tratados, dialogados e construídos para enfrentar e superar esse grande desafio da segurança cibernética. (CANONGIA; MANDARINO, 2009).

1.2 - Quais os Benefícios da Convergência Mundial das TIs aos Usuários?

Inicialmente será demonstrada a Indústria e a Logística 4.0, uma evolução conceitual e prática, na qual, promove e adequa empresas e indústrias a uma nova ordem e nova visão global competitiva. Essa evolução traz mudanças nas formas de produção ou operação de produtos, serviços e informações, utilizando maquinários computadorizados, robôs na linha produtiva, impressoras 3D, ou quaisquer outros componentes "inteligentes". (SELETTI; MORAES; SANTOS et al, 2019).

> Como justificativas para a escrita de um trabalho com o tema Logística 4.0, destaca-se que, é uma tendência tecnológica recente, que nasce totalmente digital e com capacidade de integrações facilitando um ambiente industrial avançado; tem grande flexibilidade em seu sistema e componentes. É também um elemento-chave para uma logística descentralizada e customizada, sendo utilizada nos mais variados segmentos e portes empresariais, ou mesmo, facilitando e reduzindo a cadeia logística; os estudos significativos sobre o tema, também o insere em tópicos como, a criação de ambientes favoráveis à inovação, colaborações de instituições público-privadas, não apenas por propor uma forma de uso para as tecnologias recentes, mas também, como um

> potencial elemento estratégico da Indústria 4.0. (SELETTI; MORAES; SANTOS et al, 2019, p. 2).

Com o avanço tecnológico e a existência de muitas atualizações dos sistemas produtivos inteligentes, os objetivos das empresas e indústrias serão cada vez mais voltados às exigências, necessidades dos consumidores e clientes, produzindo de forma totalmente personalizada. (Revista Mundo Logística *apud* SELETTI; MORAES; SANTOS et al, 2009).

> Assim, o conceito de Logística 4.0 pode ser resumido pelo aperfeiçoamento de uma logística ancestral, que tem como proposta básica, mais necessidade de investimentos tecnológicos e, com eles, espera-se alcançar incremento de seu market share, ideia disseminada após a quarta revolução industrial, reconhecida como período da Indústria 4.0 (BARRETO et al., 2017 *apud* SELETTI; MORAES; SANTOS et al, 2009, p. 3).

Graças ao uso de soluções como *Big Data, IA – Inteligência Artificial, Cloud Computing, Internet das Coisas,* entre outras, emerge essa Nova Indústria capaz de aliar o uso da tecnologia para crescer organizacionalmente, automatizar processos, aumentando a produtividade e ter ganhos na eficiência operacional. (SELETTI; MORAES; SANTOS et al, 2019).

1.2.1 - Conceitos do Big Data

O termo *Big-Data*, pode ser definido como o armazenamento de grandes quantidades de dados a cada instante, a partir, da existência e operação de milhões de sistemas conectados a uma rede. (MACHADO, 2018 *apud* SELETTI; MORAES; SANTOS et al, 2019).

> Como ressalta Ribeiro (2014) *apud* SELETTI; MORAES; SANTOS et al (2019), o "Big Data" opera também como um sistema de busca e recomendação que parte de perfis de usuários inerentes que podem ser reunidos ou relacionados a demais perfis que, por exemplo, quando acrescidos de históricos de compras dados originados por redes sociais, podem assegurar descobertas de novos produtos a serem ofertados.

A capacidade humana para analisar dados e informações é limitada, logo, é necessário à criação de instrumentos para auxiliar na execução das tarefas aos profissionais da informação que cuidam do *Big Data* das organizações. (Hurwitz et al, 2016 *apud* SELETTI; MORAES; SANTOS et al, 2019).

1.2.2 - Conceitos da Inteligência Artificial

A Inteligência Artificial, conhecida também como, IA, ou AI, *artificial intelligence,* do inglês, representa a inteligência parecida com a humana demonstrada através de mecanismos e softwares, na qual, conseguem perceber seu ambiente e tomar atitudes que otimizem as chances de sucesso. (CHRISLEY; BEGGER, 2000 *apud* SELETTI; MORAES; SANTOS et al, 2019).

> Como características básicas, os sistemas de IA apresentam também, capacidade de raciocínio, ou seja, aplica regras lógicas a um conjunto de dados disponíveis para chegar a uma conclusão; aprendizagem, aprende com os erros e acertos de forma que, em oportunidades futuras, o mesmo agirá de maneira mais eficaz; reconhecimento de padrões, tanto visuais e sensoriais, como também, padrões de comportamento e, inferência, a capacidade de conseguir aplicar o raciocínio nas situações cotidianas (DA SILVA; SPANHOL, 2018 *apud* SELETTI; MORAES; SANTOS et al, 2019).

1.2.3 - Conceitos de Cloud Computing

O *Cloud Computing* ou Computação em Nuvem pode ser definido como uma forma de operar em todos os lugares e plataformas, por meio da Internet, como se estivesse operando pelo próprio computador. (MARCHISOTTI et al. (2019) *apud* SELETTI; MORAES; SANTOS et al, 2019).

O uso dessa arquitetura de *Cloud Computing* é uma maneira de mudar a forma de operar a TI, substituindo o modelo bem antiquado embasado na compra de equipamentos por um modelo inovador fundamentado na compra de serviços, logo, a junção do *Cloud Computing* com a "virtualização, teoricamente permite obter o melhor dos mundos: otimização do uso dos recursos e flexibilidade para o usuário." (VERAS (2015); KORBES; WILDNER (2016) *apud* SELETTI; MORAES; SANTOS et al, 2019, p. 4).

> É uma tecnologia que acrescenta valor ao conceito de Indústria 4.0, potenciando a computação, monitorização, gestão e controle industrial, sendo propósito principal, fazer com que um Programmable Logic Controller (PLC) se comunique com um serviço de nuvem através de um dispositivo intermediário. Os PLCs são utilizados para controle de máquinas e processos industriais, mas usualmente ficam isolados do exterior no âmbito de fornecer informação. Ao interligá-los com o serviço de nuvem, a informação pretendida pode ser enviada para uma base de dados para posteriormente ser analisada, possibilitando que o usuário facilmente some informações recolhidas do PLC aos serviços disponibilizados pela nuvem e, que também permite que cada controlador seja integrado aosserviços relacionados com monitorização, previsão e gestão de dados (TAURION, 2009 *apud* SELETTI; MORAES; SANTOS et al, 2019, p. 5).

1.2.4 - Conceitos da Internet das Coisas – IoT

A IoT, ou "Internet das Coisas" ou, do inglês, *Internet of Things*, é definida como uma relação dos objetos físicos com os virtuais, ambos ligados à internet. (SELETTI; MORAES; SANTOS et al, 2019).

> Já para Singer (2012) *apud* SELETTI; MORAES; SANTOS et al. (2019, p.5), a IoT também se resume pelo modo como os objetos físicos são conectados através de sensores inteligentes e softwares, transmitem dados para uma rede e, se comunicam com o usuário e entre si como se fosse um "grande sistema nervoso", possibilitando troca de informações entre diversos pontos. Como resultado positivo desse relacionamento, temse um planeta mais responsivo e inteligente, assim como, pessoas cada vez mais, entendendo melhor como as coisas funcionam e como funcionam juntas, para melhor servir essas pessoas.

1.2.5 - Benefícios da Indústria 4.0 na Logística

Existem muitos benefícios e alguns deles são como, por exemplo: redução de custos; aumento da satisfação dos clientes e maior foco na estratégia de negócios. (SELETTI; MORAES; SANTOS et al, 2019).

CAPÍTULO II. BLOCK CHAIN

2.0 - Conceitos Básicos

A tecnologia, Block Chain é totalmente nova e uma tendência mundial atual. Aqui será apresentado e citado alguns conceitos básicos para compreensão do funcionamento e uso dessa nova tecnologia. (PIMENTA, 2016).

Para a melhor compreensão da tecnologia, BlockChain será utilizado de referência o modelo atual existente do Bitcoin, logo será esclarecido sobre o conceito de criptografia de chave pública, redes P2P e função de Hash. (PIMENTA, 2016).

2.1 - Conceito sobre a Criptografia de Chave Pública

Tal conceito de chave pública, ou criptografia assimétrica se baseia num método criptográfico utilizando-se de duas chaves diferentes, uma delas é a chave pública que serve para criptografar e a outra, a chave privada utilizada para descriptografar a mensagem. É um método e um modelo contrário ao modelo de chave privada ou simétrica, na qual é usada a mesma chave tanto para criptografar e descriptografar a mensagem. Segue abaixo a Figura 1 e Figura 2 para demonstrar as duas formas existentes de criptografia. (PIMENTA, 2016).

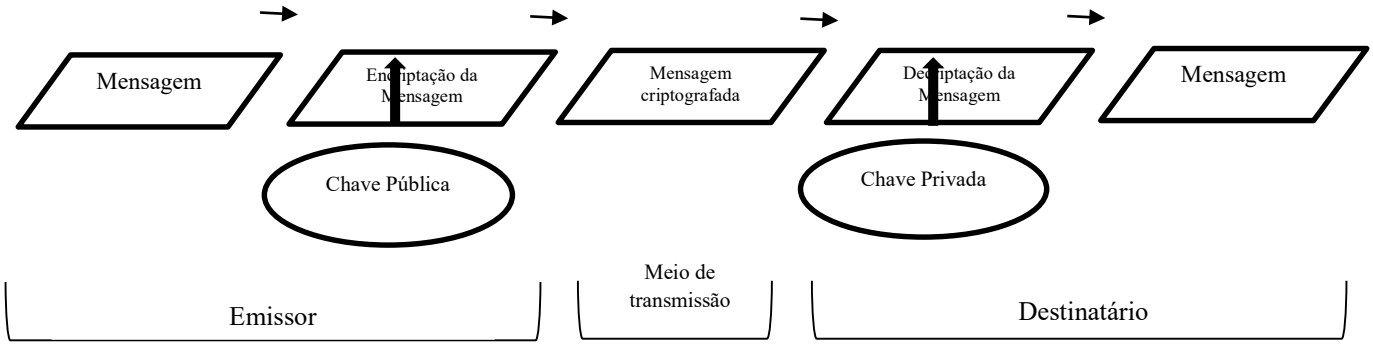

Figura 1. Criptografia de Chave Pública
Fonte: Pimenta, 2016 *apud* Salomaa, 1996, *adaptado*

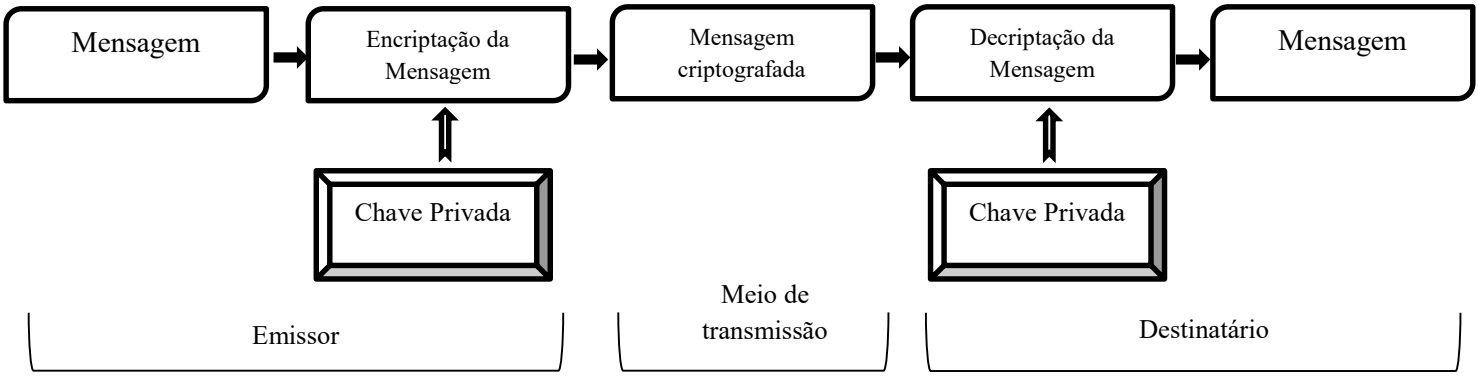

Figura 2. Criptografia de Chave Privada
Fonte: Pimenta, 2016 *apud* Salomaa, 1996, *adaptado)*

> Em um sistema de criptografia assimétrica, a chave pública é divulgada abertamente para todos que queiram enviar uma mensagem ao dono da chave ou verificar a autenticidade de uma mensagem por ele enviada. A chave privada, por sua vez, é mantida em segredo e qualquer pessoa com acesso a ela será capaz de decodificar a mensagem criptografada ou atestar a autenticidade da mensagem por meio de uma assinatura digital. (PIMENTA, 2016, p. 18).

"A segurança de um sistema criptográfico assimétrico está na diferença entre o caminho de ida e o caminho de volta da operação matemática em que a criptografia está fundamentada." (Pimenta, 2016 *apud* Impagliazzo, 1989, p. 18)

Segundo Pimenta (2016), nos dias de hoje, a Criptografia de Curvas Elípticas (CCE), é vista e considerada como a mais eficiente e a mais utilizada dentro das aplicações do Blockchain. A Criptografia CCE tem seus fundamentos e embasamentos nas propriedades matemáticas das curvas elípticas, descritas pela equação abaixo:

$$y^2 = x^3 + ax + b$$

"As chaves públicas e privadas do algoritmo são calculadas a partir de repetidas operações de adição de coordenadas polares, obtidas pela interseção da curva elíptica com diversas retas tangentes; uma explicação detalhada do funcionamento da CCE." (Pimenta, 2016 *apud* Hankerson et al, 2006, p.18).

> É importante ressaltar que uma chave criptográfica possui a propriedade de descriptografar a mensagem criptografada pela chave correspondente. Tanto a chave pública quanto a chave privada podem ser usadas para criptografar uma mensagem, dependendo da finalidade para a qual a criptografia é utilizada. De modo geral, a criptografia com a chave pública provê confidencialidade, enquanto a criptografia com a chave privada provê autenticidade. (PIMENTA, 2016, p. 19).

2.1.1 - Conceito sobre a Função Hash

De acordo com o Pimenta (2016), a função Hash é identificada como uma função matemática com as propriedades descritas na tabela abaixo.

Tabela 1 – Propriedades da Função Hash
Fonte: Pimenta, 2016

Entrada	Sequência de caracteres de qualquer tamanho.
Saída	Sequência de caracteres de tamanho fixo.
Eficiência	O tempo de execução da função para uma entrada de n caracteres deve ser O(n).

As propriedades acima definem uma função Hash de maneira geral. Porém, há mais duas propriedades denominadas de resistentes a colisões e anti-reversão que caracterizam uma função Hash criptográfico. (Pimenta, 2016 *apud* Narayanan et al, 2016).

Essa colisão pode acontecer quando duas ou mais entradas diferentes produzem o mesmo Hash de saída, como mostra na Figura 3 abaixo.

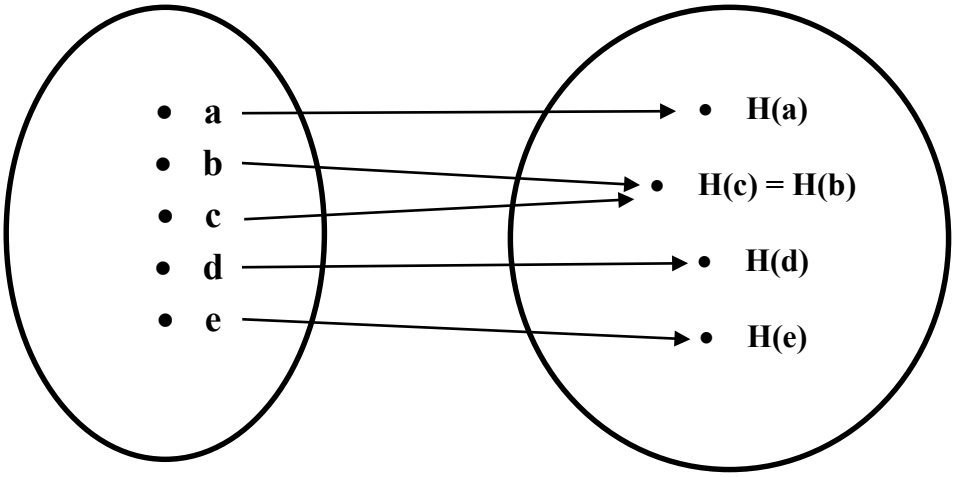

Figura 3. Colisão em uma funçãoHhash
Fonte: Pimenta, 2016 *apud* Narayanan et al, 2016, adaptado

> Ser resistente a colisões significa que a probabilidade de duas entradas produzirem o mesmo Hash deve ser pequena. Note que não se pode afirmar a impossibilidade da ocorrência de colisão, uma vez que o domínio dessa função é composto de todas as sequências de caracteres possíveis e a imagem pelo conjunto de sequencia de caracteres de um tamanho fixo. Se o domínio da função é um conjunto infinito e a imagem um conjunto finito, as colisões são inevitáveis. No entanto, boas funções de Hash apresentam baixíssimas probabilidade de colisão. Na prática, é quase impossível a ocorrência de uma colisão natural. A resistência a colisão permite a utilização do hash como síntese de mensagem (do inglês message digest). Por exemplo, para verificar que um arquivo baixado de um servidor na nuvem corresponde ao arquivo desejado, basta fazer a comparação de seus hashes ao invés de comparar todo o arquivo. (Pimenta, 2016 *apud* Narayanan et al, 2016, p. 20).

Ser anti-reversão indica que não dá para obter a mensagem da entrada x a partir doHhash h(x).

"Esta característica é alcançada fazendo com que a probabilidade dos Hashes na saída da função obedeçam uma distribuição uniforme. Na prática, isto significa que não é possível correlacionar caracteres na entrada e na saída da função apenas observando a frequência com que eles aparecem." (Pimenta, 2016 *apud* Narayanan et al, 2016, p. 20).

> Uma das principais utilizações de função hash na tecnologia blockchain é na construção de árvores de Merkle – árvores binárias de hash. A árvore é construída das folhas para a raiz, realizando o hash por pares. Quando há um numero impar de folhas, a última folha é duplicada e hasheada consigo mesma. Esta estrutura permite uma rápida verificação das entradas iniciais da função e reduz em um único hash a representação de todas as entradas (a raiz da Árvore de Merkle ou Merkle Root). (Pimenta, 2016 *apud* Okupski, 2014, p. 21).

A Figura 4 abaixo irá ilustrar a construção de uma árvore de Merkle.

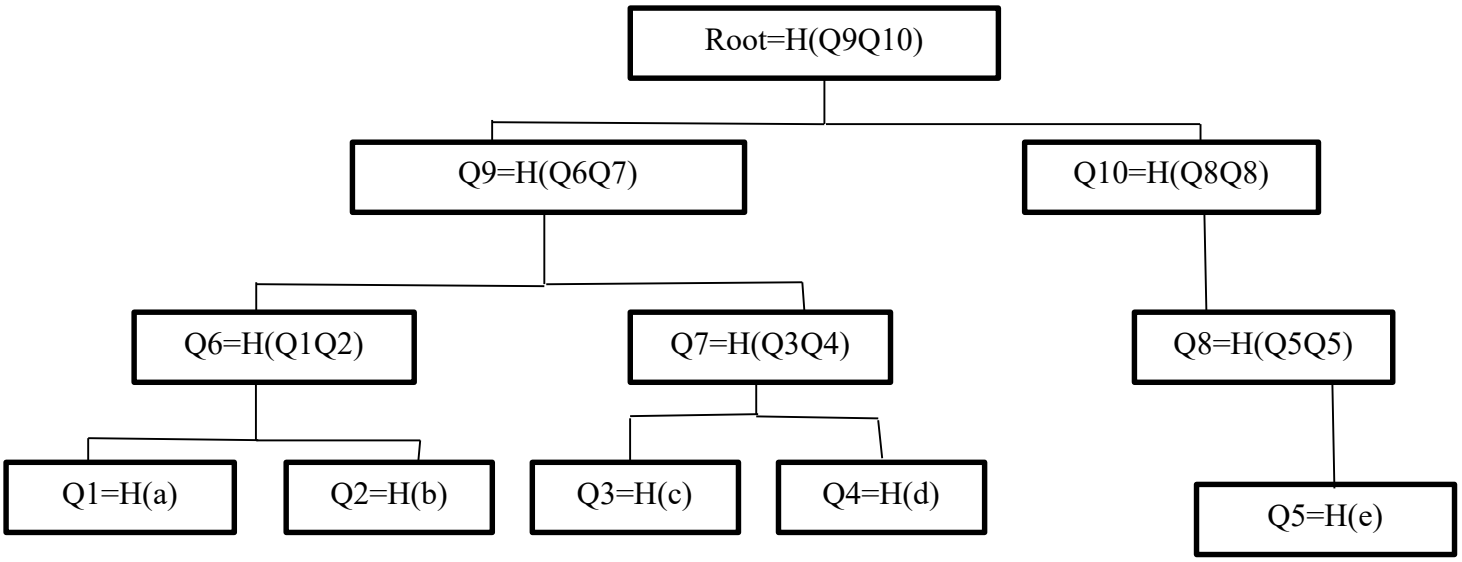

Figura 4. Ilustração de uma Árvore de Merkle
Fonte: Pimenta, 2016 *apud* Okupski, 2014

2.1.2 - Conceito sobre a Assinatura Digital

A assinatura digital é a aplicação criptográfica no meio digital, essa possui os mesmos princípios de uma assinatura convencional. Em uma assinatura convencional, na qual, já é bem

conhecida por todos existem duas propriedades bem importantes e essenciais como a autenticidade, na qual, todos possam reconhecer o dono da assinatura, porém, apenas o autor deverá saber fazer; e, o endosso, a assinatura deve estar vinculada apenas ao documento pretendido ser endossado e a nenhum outro. (Pimenta, 2016).

A existência dessas duas propriedades dá a garantia e a segurança de que uma assinatura não poderá ser forjada, copiada e nem usada em um documento para o qual a mesma não foi feita. Em relação a uma assinatura digital, espera-se o cumprimento dessas mesmas propriedades e condições. A criptografia assimétrica pode ser utilizada para prover essas duas características dentro do processo de blockchain. (Pimenta, 2016).

> Um par de chaves criptográficas é composto por uma chave pública e uma chave privada; que apenas a chave privada pode descriptografar o que foi criptografado com a chave pública e que apenas a chave pública pode descriptografar o que foi criptografado com a chave privada. Logo a propriedades de autenticidade e endosso podem ser alcançadas aplicando-se a criptografia de maneira inversa. A mensagem é criptografada (assinada) com a chave privada e descriptografada (verificada) com a chave pública. Perceba que neste modelo o objetivo é autenticidade e não confidencialidade da mensagem. A informação estará visível para qualquer pessoa que possuir a chave pública, e qualquer pessoa em posse desta chave poderá verificar que a mensagem foi emitida pelo proprietário da respectiva chave privada. (Pimenta, 2016, p. 22).

Para tornar a assinatura digital mais eficiente existe outra maneira, na qual, é adicionada o conceito de função Hash. (Pimenta, 2016).

Na tecnologia Blockchain, não tem a necessidade e muito menos o interesse de prover confidencialidade às informações. Ao contrário disso, o Blockchain se fundamenta e tem como essência ser uma cadeia de registros públicos visando e objetivando sempre a autenticidade para o ótimo funcionamento do Blockchain, ou seja, é de suma importância de que cada registro no bloco seja realizado somente pelas pessoas autorizadas a fazer. Por essa razão, a criptografia no Blockchain é na maioria das vezes aplicada como assinatura e não como encriptação da mensagem. (Pimenta, 2016 *apud* Okupski, 2014).

> O Blockchain do Bitcoin faz uso de uma curva elíptica específica, a secp256k1‖, que prove segurança de 128 bits, ou seja, a dificuldade para se quebrar um par de chaves é aproximadamente a dificuldade de se realizar 2ˆ128 operações de criptografia simétrica, o que caracteriza um alto nível de segurança no cenário tecnológico atual. (Pimenta, 2016 *apud* Johnson et al, 2001, p. 23).

2.1.3 - Conceito sobre Redes P2P

O modelo de arquitetura de rede denominada de P2P se contrapõe ao modelo tradicional e convencional conhecido como cliente-servidor. Redes P2P fazem o uso de uma arquitetura descentralizada, ou seja, cada máquina, chamada de nó, consegue executar ao mesmo tempo as funções de cliente e servidor, totalmente diferente da arquitetura tradicional cliente-servidor, na qual, uma máquina cliente somente consegue enviar solicitações e aguardar pela resposta do servidor. (Pimenta, 2016).

Abaixo a Figura 5 e a Figura 6 irão demonstrar os dois modelos existentes e citados na descrição acima.

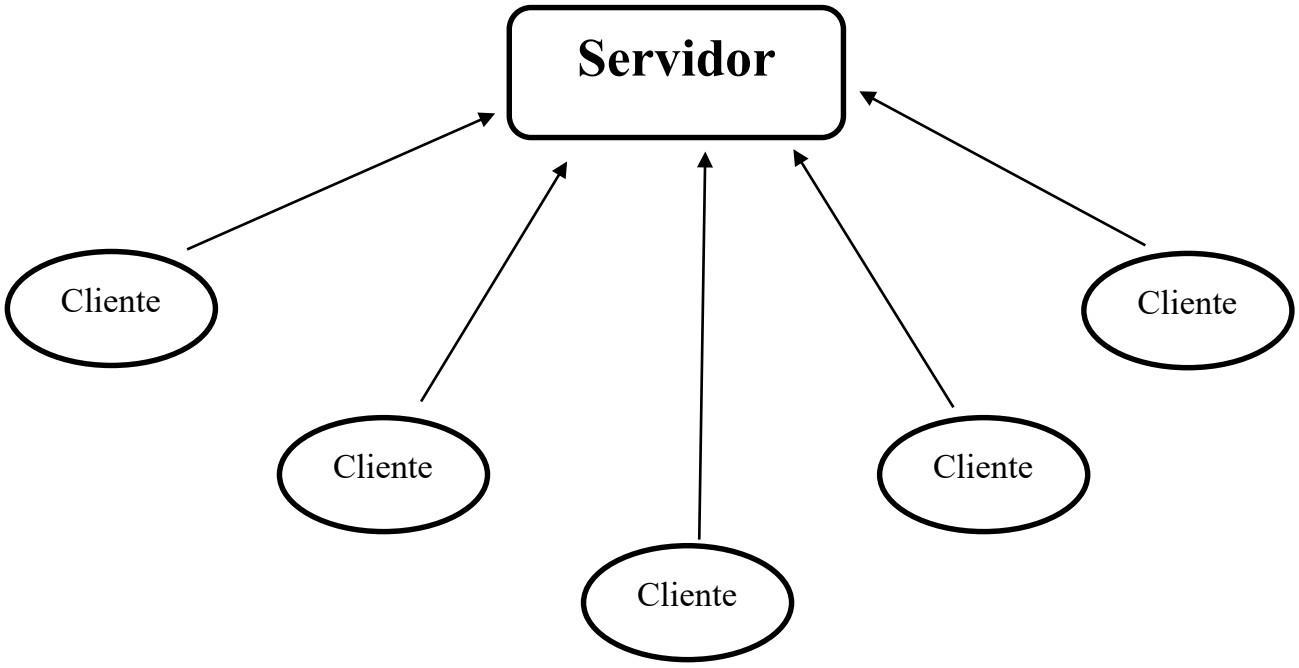

Figura 5. Arquitetura cliente-servidor
Fonte: Pimenta, 2016 *apud* Wang, 2009, *adaptado*

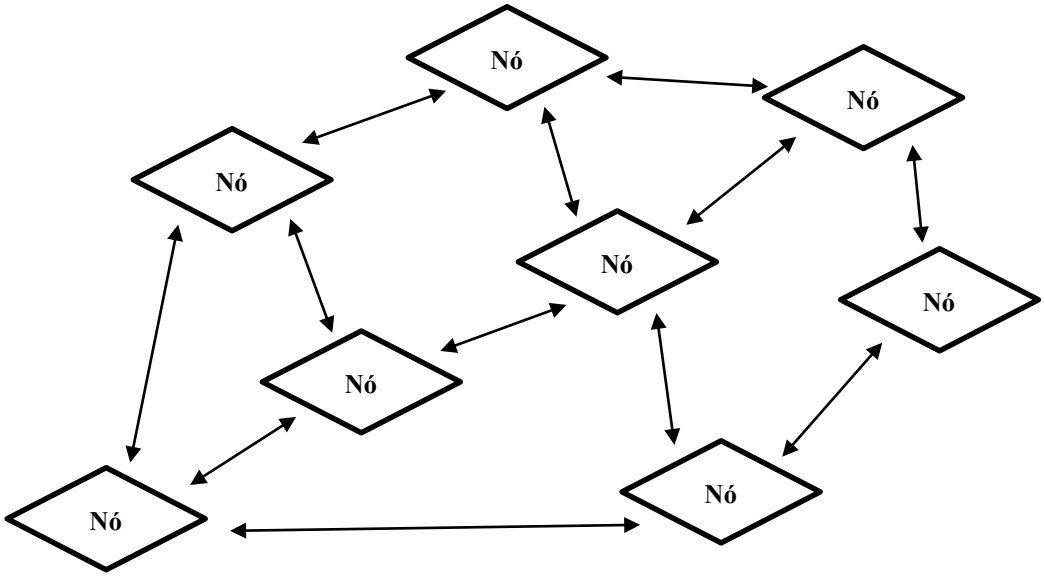

Figura 6. Arquitetura P2P
Fonte: Pimenta, 2016 *apud* Wang, 2009, *adaptado*

No modelo denominado cliente-servidor o desempenho do servidor é reduzido ao passo de que o número de solicitações e requisições dos clientes aumentam. Diferente do que acontece em redes P2P, onde o desempenho geral da rede aumenta ao passo de que crescem os números de nós dentro da rede. Normalmente, cada nó dentro da rede pode realizar o upload tanto como o download ao mesmo tempo e o surgimento de novos nós dentro da rede como a existência de saída de outro nós, tudo isso caracteriza um modelo muito flexível e bem transparente ao usuário final. (Pimenta, 2016).

"Uma característica interessante de redes p2p é capacidade de tolerância a erros. Quando um nó é desconectado da rede, a aplicação p2p pode continuar a operar utilizando outros nós que permanecem ativos. Na arquitetura cliente-servidor a conexão é interrompida se um servidor é desligado." (Pimenta, 2016, p. 25).

Outra importantíssima característica das redes P2P utilizados no Blockchain, é o fato de que é descentralizado. Informações transmitidas por um nó dentro da rede são rapidamente copiadas e passadas para máquinas em diversos lugares ao redor do mundo, sendo praticamente impossível apagar ou alterar registros espalhados em um número tão grande de nós. (Pimenta, 2016).

> No Blockchain do Bitcoin, quando um novo nó é adicionado à rede, ele envia uma mensagem a um ou mais nós específicos gravados no código do programa, chamados de nós sementes (do inglês seed nodes), requisitando outros nós da rede endereços de nós com os quais possa se conectar. Este processo se repete com os nós recém aprendidos até que o nó adicionado esteja conectado à vários outros nós da rede de maneira razoavelmente aleatória. Uma vez conectado à rede e com os registros do Blockchain atualizados, o nó está apto a publicar novos registros através de um algoritmo de broadcasting (também chamado de algoritmo de flooding ou gossip protocol). De maneira simplificada, o nó envia o registro recém criado a todos os nós com o qual está conectado. Ao receber um novo registro, cada nó verifica se se trata de um registro novo ou se já o recebeu anteriormente. Caso seja um novo registro o nó adiciona o registro à sua lista e o replica para todos os nós a ele conectado. Caso o registro já tenha sido recebido anteriormente, ele simplesmente o ignora. Isto impede que mensagens fiquem trafegando indefinidamente pela rede. (Pimenta, 2016, p. 25).

2.2 - Funcionamento do Blockchain

O Blockchain é considerado como uma cadeia de múltiplos registros imutáveis, públicos e distribuídos.

> Cadeia porque os registros estão cuidadosamente encadeados uns aos outros por meio de chaves públicas, entradas e saídas. Imutáveis porque uma vez que o registro é inserido na cadeia, ele não pode mais ser alterado. Públicos porque a única condição necessária para que um cidadão possa ter acesso aos registros do Blockchain é que ele tenha acesso à internet, e distribuídos porque esta cadeia de registro não está armazenada em um único servidor central, ao contrário, está replicada em milhões de máquinas distribuídas pelo mundo todo e nenhuma empresa ou indivíduo pode reivindicar a propriedade destes registros. (Pimenta, 2016, p. 26).

2.2.1 - A Cadeia de Blocos

"O Blockchain está estruturado na forma de blocos encadeados. Cada bloco possui uma área de transações e uma área de cabeçalho." (Pimenta, 2016, p. 26).

A Figura 7 abaixo irá mostrar como funciona o encadeamento dos blocos.

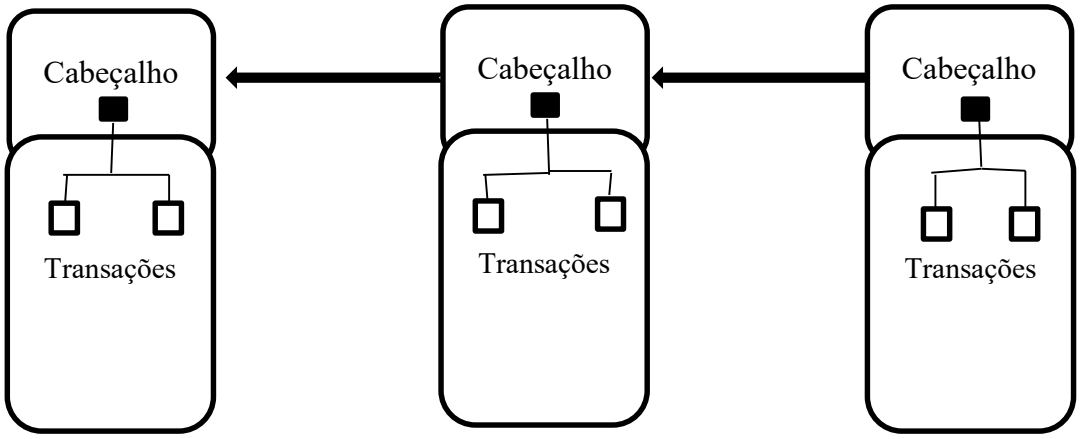

Figura 7. Cadeia de Blocos do blockchain
Fonte: Pimenta, 2016 *apud* Okupski, 2014, *adaptado*

> Na área de transações estão todas as transações coletadas por aquele bloco. Na área de cabeçalho se encontram o hash do cabeçalho do bloco anterior e a raiz da árvore de Merkle das transações presentes no campo de transações. Dessa forma, cada bloco está ligado ao bloco anterior, formando uma cadeia de blocos e cada transação está representada no cabeçalho por meio da raiz da árvore de Merkle em que foi coletada. (Pimenta, 2016 *apud* Narayanan et al, 2016, p. 26).

Um fato curioso e interessante sobre a questão e propriedade de imutabilidade presente no Blockchain é de que em boa parte de sua segurança vem através da sua estrutura encadeada dos blocos. Já que em cada bloco contém em seu cabeçalho o Hash do cabeçalho do bloco anterior, se for alterar um bloco da cadeia obrigatoriamente deverá alterar todos os blocos posteriores, o que exige com certeza uma capacidade de processamento absurda, sendo de que novos blocos estão sendo adicionados por outros nós constantemente.

> "A utilização da árvore de Merkle permite detectar qualquer alteração nas transações, uma vez qualquer alteração nas transações do bloco resulta em uma alteração na raiz da árvore de Merkle inserida no cabeçalho do bloco. Assim, a dificuldade para se alterar um registro do Blockchain cresce à medida que novos nós são adicionados à rede." (Pimenta, 2016 *apud* Okupski, 2014).

2.2.2 - Transações (Registros)

As transações assim como os blocos estão encadeados no Blockchain. Existem alguns campos que compõem uma transação, dentre eles são os Metadados é o campo que contém informações da transação como Id e tamanho; entradas, o vetor com as informações de cada entrada da transação e saídas, também é o vetor com as informações de cada saída da transação. (Pimenta, 2016 *apud* Okupski, 2014).

"O campo Metadados reúne informações gerais da transação como o tamanho da transação em bytes, quantidade de entradas e saídas, versão do protocolo e o id da transação, obtido a partir do cálculo de seu Hash SHA256." (Pimenta, 2016, p. 28).

> O campo Entradas apresenta uma lista numerada de entradas desta transação. Cada entrada de uma transação deve fazer referencia a saída de outra. Logo, neste campo há uma lista de id's de outros registros e o respectivo número da saída. Estas saídas devem ser computadas como entradas nesta transação. Ainda no campo entrada são adicionadas uma assinatura digital e uma chave pública responsáveis por confirmar que aquela transação está autorizada a utilizar as saídas indicadas no campo Entradas. O campo saída apresenta uma lista numerada de saídas que devem ser utilizadas como entradas de transações futuras. Este campo apresenta ainda um hash de chave pública que possui informações que condicionam a utilização dessas saídas por outra transação. (Pimenta, 2016, p. 28).

2.2.3 - Validação de blocos (Mineração)

No momento de que a transação é validada ela já está pronta para ser coletada por um bloco e passar pelo processo de mineração, que acontece da seguinte forma, um nó minerador da rede coleta as transações na qual deseja inserir no Blockchain dentre todas as transações validadas recebidas, calcula a raiz da árvore de Merkle e depois passa a executar o algoritmo de prova de trabalho (em inglês, *proof of work*).

> Uma prova de trabalho é um desafio criptográfico utilizado para garantir que um nó realizou uma certa quantidade de trabalho. O Bitcoin, em particular, utiliza uma prova de trabalho baseada no modelo de Adam Back (Nakamoto, 2008), outras aplicações do Blockchain utilizam variações deste modelo, mas que tenham os mesmos dois princípios: a) garantir que o nó realizou uma quantidade predefinida de processamento e b) garantir que a prova entregue é objetivamente verificável. Tipicamente, uma prova de trabalho é um processo

> probabilístico e a probabilidade de sucesso depende da dificuldade estabelecida. (Pimenta, 2016, p. 30).

"No Bitcoin, por exemplo, a prova de trabalho é encontrar um valor chamado nonce cujo duplo Hash SHA256 desse valor com a raiz de Merkle seja igual ou menor que um parâmetro T." (Pimenta, 2016, p. 30).

> A busca por esse valor é feita por tentativa e erro. Quanto menor o parâmetro T, menor a probabilidade de sucesso e mais difícil é conseguir realizar a prova de trabalho. Quanto maior o parâmetro T, maior a probabilidade e mais fácil encontrar um nonce válido. O protocolo do Bitcoin ajusta o parâmetro T automaticamente a cada 2016 blocos para garantir que as provas de trabalho e, consequentemente, a mineração de um bloco aconteça, em média, a cada 10 minutos. Outros Blockchains ajustam esse parâmetro para que a mineração aconteça em intervalos menores, de alguns segundos por exemplo. Quando a prova de trabalho é vencida, o nó pode avisar toda rede que resolveu o desafio e inserir o bloco validado na cadeia de blocos. Ao realizar esta operação, o minerador recebe como recompensa uma quantia na unidade de valor utilizada pelo Blockchain, além da diferença entre o valor de entrada e saída das transações, caso exista. (Pimenta, 2016, p. 30).

2.3 - Segurança do Blockchain

Em relação a essa nova tecnologia e tendência mundial, o Blockchain, existem muitas pesquisas sobre o assunto no âmbito da segurança. "Muitos afirmam que não é possível alcançar um nível satisfatório de segurança na tecnologia, enquanto outros afirmam que poucas tecnologias no mundo oferecem a segurança provida pelo Blockchain." (Pimenta, 2016, p. 33).

2.3.1 - Ataque 51%

51% é conhecido como um ataque quando um ou mais nós da rede alcançam a capacidade de processamento total igual ou superior a 51% da capacidade de processamento de toda a rede. (Pimenta, 2016).

"Como o atacante possui mais da metade da capacidade de processamento da rede, a bifurcação da cadeia (também chamado de fork) com os registros fraudados cresceria de maneira mais rápida que a bifurcação autêntica, validando transações que deveriam ser descartadas. Isto é chamado de ataque 51%." (Pimenta, 2016, p. 33).

Referente a esse tipo de ataque deve ser ressaltado alguns pontos importantes:

> - Não há registros de que este ataque tenha alguma vez alcançado sucesso desde a implementação do primeiro Blockchain em 2009. (Pimenta, 2016 *apud* Eyal e Sirer, 2014, p. 33);
> - Caso um minerador possuísse 51% ou mais da capacidade de mineração da rede, seria mais vantajoso minerar as transações e receber as recompensas do

> protocolo do que efetuar um ataque à rede. (Pimenta, 2016 *apud* Nakamoto, 2008, p. 33);
> - A possibilidade de se alcançar 51% da capacidade de processamento total da rede do Blockchain do Bitcoin é muito pequena. (Pimenta, 2016, p. 33);
> - Outras tecnologias de Blockchain, implementadas após o Bitcoin, como o Litecoin, realizam um a prova de trabalho mais 'democrática' de modo que a simples capacidade de processamento não representa uma grande vantagem sobre os outros mineradores. (Pimenta, 2016 *apud* Torres, 2013, p. 33);
> - Há propostas em alguns lugares do mundo, como no Reino Unido, para a regularização do processo de mineração de modo a impedir a existência de um minerador com tamanha capacidade de processamento. (Pimenta, 2016 *apud* UK Gov, 2015, p. 34).

Pensando de forma teórica é possível imaginar esse gênero de ataque, porém de forma prática é muito mais difícil de acontecer. O que pode acontecer que muitos temem é o fato de existir um super minerador trazendo assim uma perca de confiança na tecnologia, também uma desvalorização da aplicação. (Pimenta, 2016).

2.3.2 - Chaves e Aleatoriedade

"Para a utilização do Algoritmo de Assinatura Digital com Curvas Elípticas - ECDSA - uma boa fonte de aleatoriedade é essencial, pois há uma grande chance de vazamento da chave caso a fonte de aleatoriedade não seja eficiente." (Pimenta, 2016 *apud* Narayanan et al, 2016, p. 34).

Existe essa vulnerabilidade do algoritmo de assinatura digital DSA. Por isso a grosso modo é comum em aplicações que utilizam desse algoritmo pedir aos usuários de que movimentem o mouse e digitem textos aleatórios no teclado enquanto a chave é gerada. (Pimenta, 2016 *apud* Poole, 2003).

"Uma vez comprometida a chave privada na criptografia assimétrica a segurança está toda comprometida também, pois qualquer transação pode ser assinada indevidamente. " (Pimenta, 2016, p. 34).

> Na prática, porém, percebe-se que a maior vulnerabilidade do sistema não está nem na criptografia nem no protocolo, mas na parte humana do sistema. (Pimenta, 2016 *apud* Krombholz, 2015) cita que em uma pesquisa com cerca de 1000 usuários da moeda bitcoin, mais de 10% deles já havia perdido algum valor em virtude de falha humana, e conclui que o sistema apresenta baixa resiliência a este tipo de falha. A utilização do Blockchain em seu modelo convencional não permite a recuperação de chaves perdidas, seja por esquecimento, morte ou qualquer outro motivo, o que resulta em uma grande quantidade de registros deixados para trás na cadeia de transação. (Pimenta, 2016, p. 34).

2.3.3 - Confidencialidade e Anonimato

Segundo Pimenta (2016), muitos críticos mencionam o fato da tecnologia apresentar propriedades que facilitam o comércio de produtos ilegais, terrorismo, lavagem de dinheiro e atividades ligadas ao tráfico de drogas. Em relação a isso algo precisa ficar bem claro, na tecnologia Blockchain não existe a questão da confidencialidade, muito pelo contrário, o Blockchain "é uma cadeia de registros totalmente pública e todas as transações realizadas por ele estão disponíveis para qualquer cidadão com acesso à internet." (Pimenta, 2016, p. 35).

> A confusão normalmente acontece por um motivo: o Blockchain não trabalha com pessoas, trabalha com Hashes de endereços públicos. Embora seja comum dizer que Alice transferiu uma quantia x para Bob utilizando alguma moeda digital, o que acontece na verdade é que a chave privada de Alice assinou um registro de transferência de valor para a chave pública de Bob. No entanto, os nomes de Bob e Alice nunca foram gravados no Blockchain, apenas suas assinaturas e chaves públicas. Neste sentido, é correto dizer que o Blockchain não exige identificação, mas não está correto dizer que ele prove confidencialidade. (Pimenta, 2016, p. 35).

A identificação do usuário muitas vezes acontece em aplicativos terceiros que adicionam regras de identificação ao protocolo da tecnologia, seguindo um conjunto de regras conhecidos como KYC (*Know Your Customer*). (Pimenta, 2016).

> Em resumo, o Blockchain prove um alto nível de transparência e rastreabilidade das transações. É possível rastrear qualquer valor até a sua transação coinbase por mais antiga que seja. A possibilidade de operar a tecnologia sem a necessidade de identificação é bastante atraente para operadores do comércio ilegal, mas de modo algum invalidam o uso da tecnologia de maneira adequada, apenas apontam para a necessidade de modernização dos instrumentos legislativos. (Pimenta, 2016, p. 35).

CAPÍTULO III. SOCIETY 5.0

3.0 - Trilhando o Caminho para *Society 5.0*

É uma sociedade que ajuda a criar soluções de vários problemas e desafios envolvidos da sociedade incorporando inovações tecnológicas da quarta revolução industrial como por exemplo: *IoT*, *Big Data*, Inteligência Artificial, Robótica e uma economia compartilhada dentro das indústrias e na vida social. A Sociedade do Futuro será uma na qual existirá e será criado sempre novos valores e serviços continuamente, fazendo com que as pessoas vivam de maneira mais sustentável e mais confortáveis. (ABECONOMICS, 2019).

Essa é a *Society 5.0* de forma introdutória, uma sociedade muito inteligente. O Japão irá liderar essa nova visão de sociedade, levando a frente essa ideia e sua realização ao resto do mundo. (ABECONOMICS, 2019).

A figura 8 abaixo irá mostrar como a sociedade humana evoluiu com o passar do tempo desde a *Society 1.0* até a mais atual e nova *Society 5.0*. Primeiramente existia uma sociedade mais arcaica fundamentada no instinto animal de sobrevivência com o foco e objetivo totalmente voltado à caça, uma busca incessante por alimento, denominada de *Society 1.0*, após veio a *Society 2.0*, uma sociedade totalmente fundamentada na agricultura, ou seja, uma sociedade agrária, logo em seguida, uma sociedade baseada em produtos industriais, a sociedade industrial, denominada de *Society 3.0*, a próxima sociedade é aquela fundamentada em informações, ou seja, uma sociedade da informação, a *Society 4.0*, a mais atual sociedade na qual o mundo todo está a caminho é a *Society 5.0*, a era da tecnologia em massa como exemplos: a inteligência artificial, *big data* e *IoT*. (ABECONOMICS, 2019).

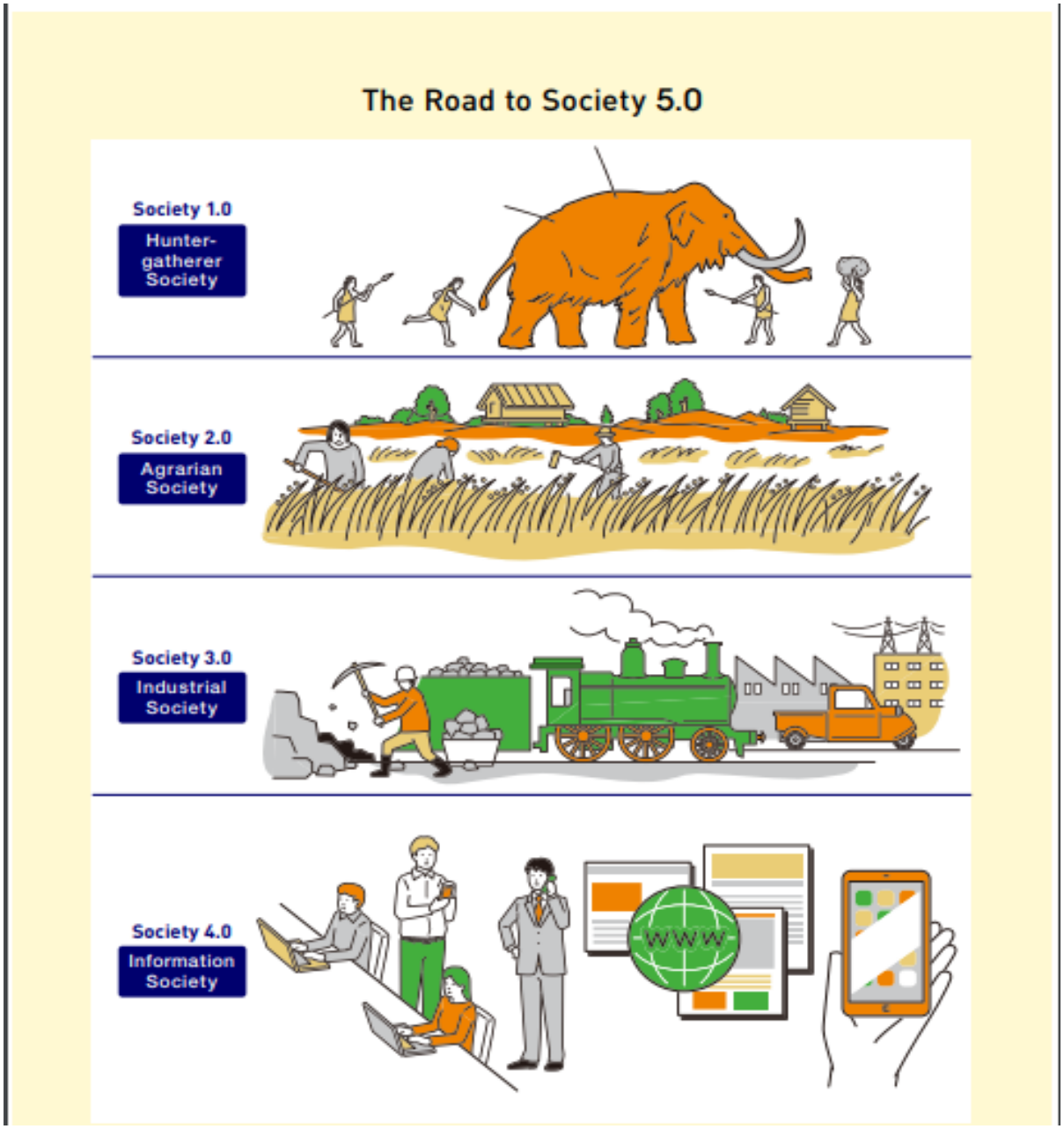

Figura 8. Trilha para a Society 5.0
Fonte: ABECONOMICS, 2019

Entrando nessa nova sociedade, *Society 5.0*

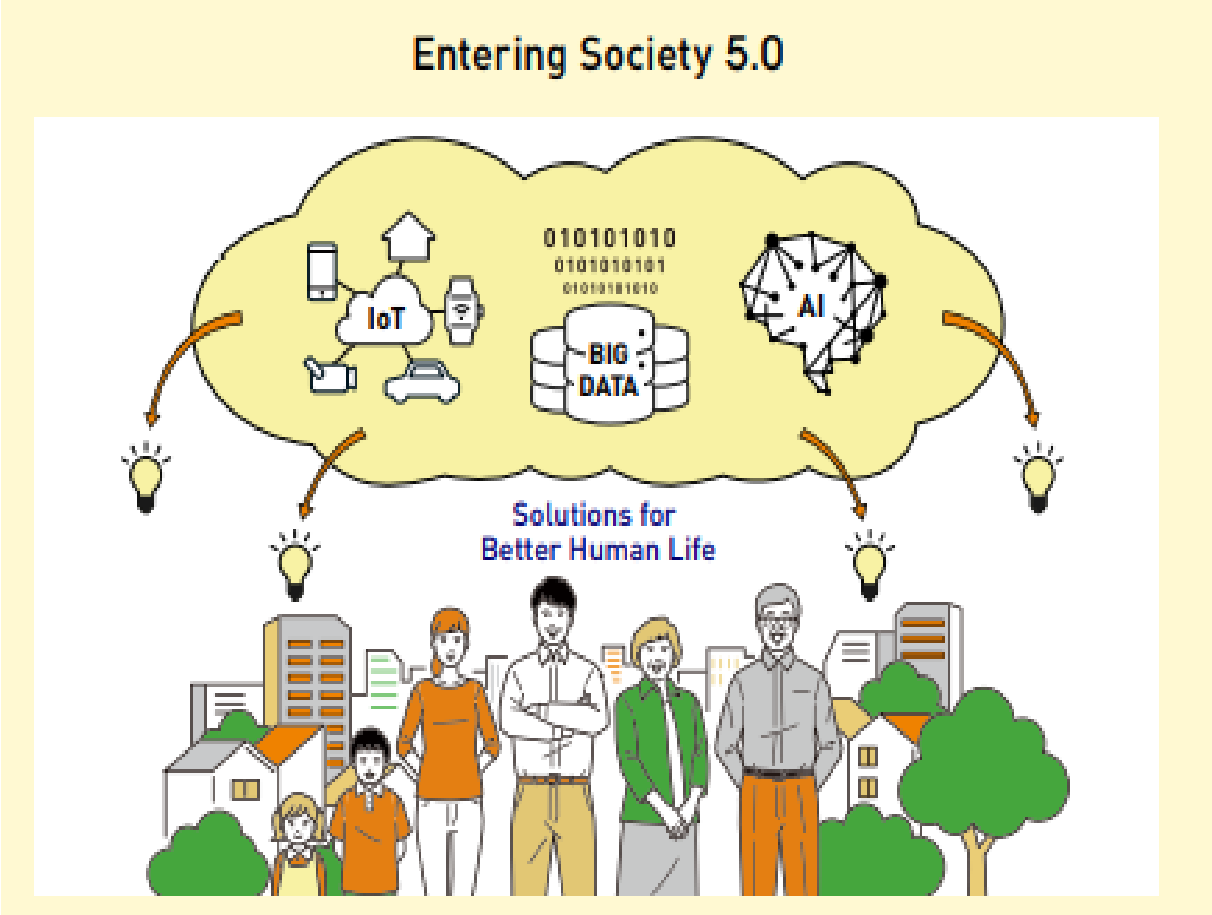

Figura 8. Trilha para a Society 5.0
Fonte: ABECONOMICS, 2019

O *Big Data* coletado pela *IoT* será utilizado e convertido em um novo tipo de inteligência artificial e será alcançado e distribuído em cada canto da sociedade. Com essa mudança na sociedade para uma forma de *Society 5.0* todas as pessoas irão usufruir de uma vida mais confortável e sustentável, pois nessa nova sociedade somente serão providenciados produtos e serviços em quantidades necessárias e no momento de que realmente houver necessidade. (ABECONOMICS, 2019).

O Japão possui vantagens de que essa *Society 5.0* seja possível comparado com o resto do mundo, mais especificamente dois fatos essenciais para tudo isso ser possível. O primeiro ponto é de que o país asiático possui um acúmulo abundante de dados reais, baseados em dados médicos e da saúde retirados de um sistema universal de cuidados com a saúde e uma vasta operação com milhares de dados retirados de instalações, atualmente o Japão está situado em um meio que realmente possui muitos dados reais de que são utilizados na economia e na indústria. O segundo fato é de que o país cultiva uma tecnologia bem avançada através de "monozukuri"; o Japão é excelente em fabricar coisas e com anos de pesquisa, será possível

criar produtos vantajosos usando a tecnologia da informação como por exemplo: *Big Data* e a inteligência artificial e assim liberar os mesmos dentro da sociedade. (ABECONOMICS, 2019).

Com essas vantagens apresentadas por esses dois fatos o Japão irá superar primeiro desafios sociais provenientes da redução da população ativa e produtiva, envelhecimento da população local e problemas envolvendo energia e meio ambiente comparado com outras nações. Logo surgirá uma economia vibrante promovendo produtividade e cirando novos mercados dentro da sociedade. Com isso o Japão será o ponto focal para expandir esse modelo de nova sociedade, a *Society 5.0* ao resto do mundo. (ABECONOMICS, 2019).

A *Society 5.0* irá mudar o mundo trazendo muitos benefícios e soluções aos problemas já existentes dentro da sociedade moderna e em específico do Japão como apresentados nas Tabelas 2, 3, 4 e 5 abaixo:

Tabela 2 – Assistência Médica
Fonte: ABECONOMICS, 2019

Problemas	**Soluções**
A população japonesa está envelhecendo mais rápido comparado com outros países. O país está sofrendo com o aumento dos gastos provenientes da saúde e segurança social. Aumento da demanda com cuidados aos idosos.	1- Conectar e compartilhar informações sobre os médicos incluindo o histórico dos checkups, o tratamento e o histórico das enfermeiras.
	2 - Introduzir serviços de assistência médica e cuidados médicos remotos.
	3 - Utilizar inteligência artificial e robôs nas enfermarias para dar suporte oferecendo assim independências às pessoas.

Conectando e compartilhando dados médicos que estão espalhados em vários hospitais diferentes, o tratamento médico poderá ser mais eficiente baseados nos dados oferecidos. Com os cuidados médicos remotos os idosos não irão mais necessitar ir aos hospitais frequentemente. A própria pessoa poderá mensurar e gerencias seus dados médicos até medir os batimentos

cardíacos em casa, tudo isso auxiliará e fará com que seja possível estender a expectativa de vida das pessoas de forma mais saudável. (ABECONOMICS, 2019).

Tabela 3 – Mobilidade
Fonte: ABECONOMICS, 2019

Problemas	Soluções
Declínio da população em áreas de subpopulações rurais trazem um acesso bem restrito ao transporte público. O aumento acelerado do segmento de E-Commerce traz uma escassez de motoristas.	1- Promover o uso de veículos autônomos como taxistas e ônibus de transporte público para disponibilizar às subpopulações rurais de forma mais ágil.
	2 - Melhorar a eficiência da distribuição e da logística introduzindo inovações como por exemplo: um único motorista utilizar um sistema de veículo sem pessoas que tenha um caminhão de carga em um comboio e também a utilização de drones.

Pessoas de subpopulações que habitam áreas e lugares mais afastados possuem bastantes dificuldades para fazerem compras e visitarem hospitais pelo fato de existirem poucos transportes públicos. Porém com os veículos autônomos será possível viajar de forma mais prática e fácil enquanto com os drones será possível receber qualquer coisa que alguém precise. Assim a escassez dos motoristas na cadeia de distribuição não será uma preocupação e nem problema. (ABECONOMICS, 2019).

Tabela 4 – Infraestrutura
Fonte: ABECONOMICS, 2019

Problemas	Soluções
Deterioração da infraestrutura pública durante o período do crescimento econômico acelerado do Japão criando assim uma escassez de mão de obra qualificada e consequentemente um aumento da carga financeira referente a fiscalização e manutenção.	1- Os sensores, a inteligência artificial e os robôs serão utilizados para fiscalizar e manter as estradas, pontes, túneis e barragens.

Implementando novas tecnologias incluindo a Tecnologia da Informação e Comunicação (em inglês conhecido como *Information and Communication Technology* (ICT)), robôs, sensores para fiscalização, inspeção e manutenção de sistemas tudo isso requere

habilidades e técnicas especializadas, detectar lugares que precisam de reparos e manutenções pode ser feito de forma bem rápida, ágil e fácil. Após conseguir implementar essas tecnologias acidentes inesperados que acontecem de repente serão minimizados e o tempo gasto para construir será reduzido, também ao mesmo tempo a segurança e a produtividade aumentarão. (ABECONOMICS, 2019).

Tabela 5 – Fintech
Fonte: ABECONOMICS, 2019

Problemas	Soluções
Uma grande parte das transações financeiras do Japão ainda são realizadas em espécie, dinheiro de papel e os procedimentos dos bancos são bem complicados. A usabilidade da tecnologia da informação dentro das companhias ainda é bem limitada e os serviços financeiros convencionais são muito lerdos.	1- Usar a tecnologia BlockChain para transferir o dinheiro.
	2 - Introduzir interfaces de programações de aplicativos abertos (do inglês application programming interfaces (API)) para empresas FinTechs e bancos.
	3 - Promover o processo de pagamento sem dinheiro ou melhor com pouco dinheiro.

Enviar remessas para o exterior lá no Japão ainda é um processo complicado, pois é uma grande perca de tempo e exige pagamentos de taxas bancárias. A tecnologia do BlockChain irá reduzir esse tempo gasto e os custos trazendo também mais segurança e garantia em transações econômicas globais. (ABECONOMICS, 2019).

CONCLUSÃO

Com o trabalho acadêmico pode se concluir que ainda existe um caminho longo para trilhar sob essas novas tendências tecnológicas mundiais, tratativas de até onde a segurança alcança dentro dessa sociedade totalmente interconectada.

Com a leitura dos vários estudos e artigos a respeito é possível notar que as tecnologias oferecem um grau de confiança e de segurança também, porém não se deve esquecer e deixar de lado de que os usuários devem ficar ligados e espertos sob a segurança e a guarda de suas informações pessoais e tomar certos cuidados de não expor as mesmas de qualquer maneira e visar sempre a segurança também em transações financeiras eletrônicas.

De certa forma a sociedade está em constantes mudanças e transformações o ideal agora é que todos devem se atualizar e aprender como se comportar dentro dessa quarta revolução industrial e dessa nova forma de ver a sociedade como um todo aonde é tudo interconectado e totalmente tecnológico.

Outro ponto a esclarecer e citar é sobre a crise do futuro do trabalho que está se alterando e modificando com essa nova onda de convergência mundial das TIs, trazendo assim termos que até antes não existiam como Uberização, 99zação e entre outros, principalmente em países em desenvolvimento e emergentes como o Brasil.

Essa onda de robotização nas indústrias, utilizações de IoT e de inteligências artificias nas fábricas também estão com certeza alterando o rumo do futuro do trabalho, trazendo desemprego à população que antes tinham um emprego e assim tornando o país cada vez tecnológico e substituindo a mão de obra das pessoas por máquinas.

Mas essa realidade nos países emergentes e em desenvolvimento como o Brasil pode ser mudada se usar de fundamento o Japão e sua nova visão de sociedade, a *Society 5.0*.

REFERÊNCIAS BIBLIOGRÁFICAS

1[] ABECONOMICS; REALIZING SOCIETY 5.0. Japão, 2019. Disponível em: <https://www.japan.go.jp/abenomics/_userdata/abenomics/pdf/society_5.0.pdf>. Acesso em: 06 novembro. 2019.

[2] CANONGIA; MANDARINO. SEGURANÇA CIBERNÉTICA: O DESAFIO DA NOVA SOCIEDADE DA INFORMAÇÃO. Brasília, 2009. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 18 setembro. 2019.

[3] KHARPAL, A. WITH XI'S BACKING, CHINA LOOKS TO BECOME A WORLD LEADER IN BLOCKCHAIN AS US POLICY IS ABSENT. < https://www.cnbc.com/2019/12/16/china-looks-to-become-blockchain-world-leader-with-xi-jinping-backing.html >

[4] PIMENTA, Timoteo. TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS. Brasília, 2016. Disponível em: <http://bdm.unb.br/handle/10483/16252>. Acesso em: 16 outubro. 2019.

[5] SELETTI; MORAES; SANTOS et al. INDÚSTRIA 4.0 e LOGÍSTICA 4.0: INOVAÇÃO, INTEGRAÇÃO, SOLUÇÕES E BENEFÍCIOS REAIS DECORRENTES DO MUNDO VIRTUAL. São Paulo, 2019. Disponível em: <http://fateclog.com.br/anais/2019/IND%C3%9ASTRIA%204.0%20E%20LOG%C3%8DSTICA%204.0%20INOVA%C3%87%C3%83O%2C%20INTEGRA%C3%87%C3%83O%2C%20SOLU%C3%87%C3%95ES%20E%20BENEF%C3%8DCIOS%20REAIS%20DECORRENTES%20DO%20MUNDO%20VIRTUAL.pdf>. Acesso em: 20 setembro. 2019