

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
FACULDADE DE TECNOLOGIA DE CAMPINAS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO EMPRESARIAL

RENE JOSÉ ROBLES ROMAN BERALDO

**COMO A TECNOLOGIA BLOCKCHAIN PODE SER
BENÉFICA NA ÁREA DE GESTÃO**

CAMPINAS

2022

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
FACULDADE DE TECNOLOGIA DE CAMPINAS
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO EMPRESARIAL

RENE JOSÉ ROBLES ROMAN BERALDO

**COMO A TECNOLOGIA BLOCKCHAIN PODE SER
BENÉFICA NA ÁREA DE GESTÃO**

Trabalho de Graduação apresentado por Rene José Robles Roman Beraldo, como pré-requisito para a conclusão do Curso Superior de Gestão Empresarial, da Faculdade de Tecnologia de Campinas, elaborado sob a orientação do Prof. Dr. Jaime Cazuhiro Ossada.

CAMPINAS

2022

FICHA CATALOGRÁFICA
CEETEPS - FATEC Campinas - Biblioteca

B482c

BERALDO, Rene José Robles Roman
Como a tecnologia blockchain pode ser benéfica na área de gestão.
Rene José Robles Roman Beraldo.
Campinas, 2022.
32 p.; 30 cm.

Trabalho de Graduação do Curso de Gestão Empresarial -
Faculdade de Tecnologia de Campinas.
Orientador: Prof. Dr. Jaime Cazuhiro Ossada.

1. Blockchain. 2. Contratos inteligentes. 3. Futuro. 4. Gestão
Empresarial. 5. Tecnologia. I. Autor. II. Faculdade de Tecnologia de
Campinas. III. Título.

CDD 004

Catálogo-na-fonte: Bibliotecária: Aparecida Stradiotto Mendes – CRB8/6553

TG GE 22.2

RENE JOSÉ ROBLES ROMAN BERALDO

Como a Tecnologia Blockchain pode ser benéfica na área de Gestão.

Trabalho de Graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Gestão Empresarial, pelo CEETEPS / Faculdade de Tecnologia – Fatec Campinas.

Campinas, 06 de dezembro de 2022.

BANCA EXAMINADORA



Jaime Cazuhira Ossada
Fatec Campinas



Edson Massola Junior
Fatec Campinas



Manoel Gonçalves Filho
Fatec Campinas

DEDICATÓRIA

Dedico este trabalho a todos os que me ajudaram ao longo dessa caminhada.

RESUMO

O mundo tornou-se um lugar completamente novo a partir da década de 90 com o advento da internet e o início da descentralização. Alguns anos depois surgiu um dos protocolos mais importantes para o século 21: a blockchain. O presente trabalho tem como objetivo realizar uma análise sobre os impactos do uso de contratos inteligentes na blockchain, enunciar o conceito de blockchain, suas aplicações, o porquê de sua utilização, analisar os benefícios, desvantagens, perigos e compreender a influência da tecnologia blockchain no futuro da gestão. O trabalho tem como natureza aplicada com uma abordagem de pesquisa qualitativa, objetivos de uma pesquisa exploratória e procedimentos técnicos baseados em pesquisa bibliográfica por meio de livros, artigos, jornais e pesquisa na internet. E nos resultados é comentado sobre o potencial da utilização da tecnologia blockchain no futuro caso melhorias sejam implementadas para que determinadas desvantagens apresentadas sejam eliminadas proporcionando diversos benefícios aos usuários que estiverem utilizando de tal tecnologia.

Palavras-chave: blockchain, contratos inteligentes, futuro, gestão empresarial, tecnologia

ABSTRACT

The world has become a completely new place since the 1990s with the advent of the internet and the beginning of decentralization. A few years later, one of the most important protocols for the 21st century emerged: the blockchain. The present work aims to carry out an analysis of the effects of using smart contracts on the blockchain, enunciate the concept of blockchain, its applications, the reason for its use, analyze the benefits, remain, dangers and understand the influence of blockchain technology on the future of management. The work has an applied nature with a qualitative research approach, exploratory research objectives and technical procedures based on bibliographical research through books, articles, newspapers and internet research. And in the results it is commented on the potential use of blockchain technology in the future, if improvements are implemented so that certain experiences are eliminated, providing various benefits to users who are using such technology.

Key words: blockchain, business management, future, smart contracts, technology

LISTA DE FIGURAS

Figura 1 - Bloco.....	11
Figura 2 - Corrente de blocos	12
Figura 3 - Sequência de blocos.....	13
Figura 4 - <i>Hash</i> de segurança	14
Figura 5 - <i>Hash</i> de segurança contra fraude	15

SUMÁRIO

1	INTRODUÇÃO	7
1.1	JUSTIFICATIVA	8
1.2	OBJETIVOS	8
1.2.1	Objetivos específicos	8
1.3	METODOLOGIA	9
2	REVISÃO BIBLIOGRÁFICA	9
2.1	BLOCKCHAIN	9
2.2	CONTRATOS INTELIGENTES	15
2.2.1	Aplicações de contratos inteligentes	17
2.2.2	Aplicações descentralizadas (dApps)	19
2.3	BENEFÍCIOS DOS CONTRATOS INTELIGENTES COM A TECNOLOGIA BLOCKCHAIN	20
2.4	DESVANTAGENS E PERIGOS DE CONTRATOS INTELIGENTES COM A TECNOLOGIA BLOCKCHAIN.....	24
3	CONCLUSÃO	28
3.1	PRINCIPAIS OBSERVAÇÕES	29
3.2	IMPLICAÇÕES FUTURAS.....	29
4	REFERÊNCIAS	31

1 INTRODUÇÃO

O mundo digital e o mundo real se mesclaram de tal forma, no presente século, que os indivíduos que estão associados ao meio não conseguem se dissociar mais dele pois, a todo momento, é necessário utilizar de alguma tecnologia digital, seja no trabalho ou fazendo as coisas que costumamos desfrutar durante os momentos de lazer. A todo momento encontramos pessoas com aparelhos digitais, sejam celulares, tablets, notebooks ou até mesmo aparelhos que possuem inteligência artificial para realizar a integração de vários sistemas através de aplicativos. Um evento claro a respeito dessa manifestação pode ser associado a um jogo de futebol, por exemplo, em que no início do século os torcedores acompanhavam os jogos sem um contato tão expressivo com telefones celulares e, atualmente, muitas pessoas utilizam de seus aparelhos para registrar tais momentos por meio de fotos, vídeos e até mesmo compartilhando em suas redes sociais, como Twitter, Facebook e Instagram.

Em 1994, quando as redes de Internet foram liberadas para fins comerciais, iniciou-se um processo de descentralização, que até então pouquíssimas pessoas tinham algum conhecimento sobre tal assunto visto que não sabiam o que poderia ser modificado no mundo naquela época, uma vez que os sistemas, até a década de 90, eram centralizados, ou seja, um poder central conectava pontos ou pessoas através de tal poder central. Um exemplo simples de poder central eram os bancos que são fontes confiáveis para preservar o dinheiro com segurança, assim como nas transações em que para deslocar dinheiro de um indivíduo para o outro existia o intermédio de um banco como poder central para realizar tal operação mediante de autorizações, burocracias, taxas e limites.

Todavia, em 2008 surgiu o Bitcoin, com a tecnologia blockchain, que trouxe um sistema distribuído (descentralizado) em que o poder central deixou de possuir seu papel, e distribuiu tal papel para todos os usuários. Outros exemplos práticos semelhantes ao Bitcoin, são: utilização dos correios por meio do intermédio de envio mensagens de um usuário “a” para um usuário “b” e mediante tal prestação são cobradas taxas para a intermediação realizada, e assim as taxas são coletadas e os consumidores de tal serviço são obrigados a respeitar os limites e prazos de tal poder central para enviar uma mensagem. Então com o sistema SMTP (Simple Mail Transfer Protocol ou Protocolo de Transferência de Correio Simples) tornou-se possível enviar e-mails para qualquer usuário que utilize o mesmo protocolo, assim como o envio de Bitcoins por intermédio da blockchain para outros usuários. (ULRICH, 2014)

Após o surgimento da tecnologia blockchain um próximo passo foi realizado em 2013 pelo russo-canadense Vitalik Buterin com a criação do Ethereum que, assim com o Bitcoin, o

Ethereum é, também, uma tecnologia blockchain e seu maior diferencial está associado aos contratos inteligentes (smart contracts) que por meio de regras pré-estabelecidas, de forma automatizada e sem a necessidade de um poder central geram transações entre os usuários que utilizam de tal tecnologia.

1.1 JUSTIFICATIVA

Por se tratar de um tópico atual, de relevância e com um horizonte completamente novo de estudos relacionados à tecnologia blockchain associada aos sistemas de gestão, o presente trabalho tem como resultado pretendido uma análise de como a utilização dessa nova tecnologia pode impactar na geração de contratos inteligentes por meio da tecnologia blockchain com o objetivo de compreender as implicações e influências do uso de uma tecnologia nova e de potencial no campo de negócios jurídicos. Além disso tal trabalho busca quebrar paradigmas em respeito aos sistemas centralizados vigentes e proporcionar uma abordagem completamente nova em respeito aos sistemas distribuídos que estão surgindo, como a blockchain, visto que resistência e comodidade diante ao mercado jamais serão soluções em um era de tantas mudanças e revoluções tecnológicas. Para mais, existem alguns exemplos que demonstram que tal resistência diante tecnologias que estão surgindo e é completamente sem sentido como os bancos centrais afirmando que o Bitcoin não é uma boa ideia, os correios contra a utilização de e-mail, jornais contra a utilização da internet, bilheterias contra o sistema de transmissões ao vivo (streaming), estações de rádio contra a televisão e taxis contra a utilização de aplicativos de serviço de viagem. (ULRICH, 2014)

1.2 OBJETIVOS

Analisar o uso de contratos inteligentes utilizando da tecnologia blockchain no âmbito da gestão.

1.2.1 Objetivos específicos

- Enunciar o que é e o porquê da utilização da tecnologia blockchain;
- Identificar contratos inteligentes, suas aplicações e as aplicações descentralizadas;
- Analisar e compreender os benefícios, desvantagens e perigos da utilização da tecnologia blockchain para contratos inteligentes;

1.3 METODOLOGIA

Técnica é derivada da palavra grega *tékhne*, que significa "arte". Se o método é visto como um caminho, a técnica pode ser vista como um caminho a pé. A técnica indica a operacionalização do método segundo regras definidas, nos mínimos detalhes. É o culminar de anos de prática e precisa de destreza na execução. Mais de uma metodologia pode ser utilizada no mesmo processo. A distinção entre método e técnica é comparável àquela entre gênero e espécie em termos de semântica. (KOTAIT *apud* OLIVEIRA, 2011).

De acordo com Marconi e Lakatos (2019), uma pesquisa pode ser classificada pela natureza, abordagem, objetivos e procedimentos técnicos. Assim, a natureza desta pesquisa é classificada como uma pesquisa aplicada que busca analisar os principais impactos do uso da tecnologia blockchain na área de gestão empresarial. A abordagem se integra em uma pesquisa qualitativa, visto que, busca ter caráter exploratório e subjetivo, estimulando os leitores a pensar a respeito do tema. Os objetivos apresentam característica de uma pesquisa exploratória, uma vez que, não existem tantas informações a respeito da tecnologia blockchain incorporada na gestão empresarial. E, por último, os procedimentos técnicos são baseados em pesquisa bibliográfica, isto é, materiais que já foram elaborados, sobretudo, livros, artigos e jornais científicos a partir do ano de 2010 como período considerado para levantamento dos dados, buscando por palavras chave, como: blockchain, gestão e contratos inteligentes com base nos dados do google acadêmico e repositório da Universidade Federal de Santa Catarina.

2 REVISÃO BIBLIOGRÁFICA

Nesta seção será apresentado o desenvolvimento teórico do trabalho enunciando conceitos, correlacionando à informações citadas, análise e compreensão do assunto abordado.

2.1 BLOCKCHAIN

Em 18 de Agosto de 2008 surgiu a primeira criptomoeda chamada de bitcoin e em conjunto com ela o protocolo chamado Blockchain (corrente de blocos). Mediante um website de registro de domínios anônimos surgiu o primeiro site: bitcoin.org criado pelo pseudônimo Satoshi Nakamoto. No mesmo ano, em 31 de Outubro, o papel branco (documento que informa a respeito de informações e dados sobre o protocolo blockchain, também chamado de *whitepaper*) foi escrito e liberado em uma obscura, porém fascinante, lista de e-mails pelo site Metzdown. (LEWIS, 2018) E assim iniciou-se a história de um dos protocolos mais importantes do século 21: a blockchain.

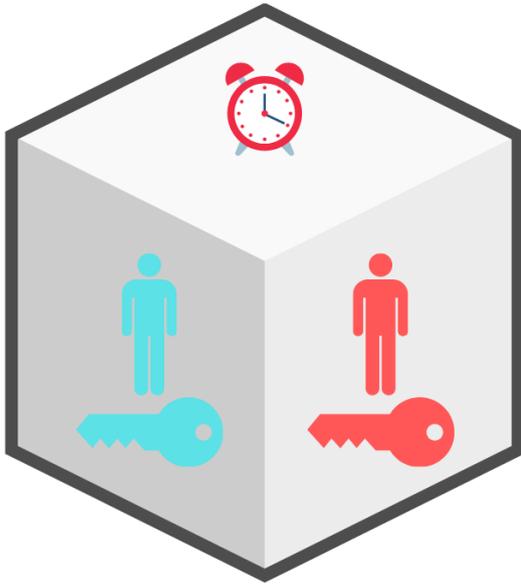
Naturalmente ouve-se a palavra “blockchain” em maior parte dos casos, porém é possível também ouvir a frase “tecnologia blockchain” em diversos contextos e pode tornar-se algo confuso porque diferentes pessoas utilizam essas palavras para significar coisas diferentes segundo o autor. De acordo com Lewis apud Walch (2018) blockchain são as regras ou padrões de como um livro-razão é criado e mantido, além disso diferentes tecnologias possuem diferentes regras de participação, diferentes regras de rede, especificações para como criar transações, métodos de armazenamento de dados e diferentes mecanismos de consenso conforme o autor. Quando uma rede é criada, a blockchain ou livro-razão de registro está inicialmente vazio de transações, como um novo livro-razão físico encadernado em couro conforme o autor. Alguns exemplos de tecnologias blockchain, são: Bitcoin, Ethereum, NXT, Corda, Fabric e Quorum (tradução livre).

Livros blockchain são instâncias específicas de livros-razão que contém suas respectivas transações ou registros. Pensando em bancos de dados normais, existem alguns tipos de bancos de dados como Oracle, bancos de dados MySQL etc. Cada tipo funciona de maneira um diferente, embora todos tenham objetivos semelhantes: armazenamento eficiente, classificação e recuperação de dados. Assim como várias instâncias do mesmo tipo de banco de dados: uma empresa pode usar mais de um banco de dados Oracle e assim é com blockchains. Algumas tecnologias blockchain operam de uma maneira, outras operam de maneira ligeiramente diferente e é possível ter várias instâncias de qualquer tecnologia blockchain, em livros-razão separados. (LEWIS, 2018)

Em decorrência das diversas tecnologias blockchain, o presente trabalho utilizará da tecnologia blockchain Ethereum para exemplificar, de maneira geral, como os protocolos blockchain funcionam para a geração dos contratos inteligentes.

Basicamente, a blockchain é uma corrente de blocos de informação e cada bloco tem a mesma função de uma página de um livro-razão em que são anotadas informações de um usuário “a” que envia uma informação para um usuário “b” com informações de chave (código destinado a registrar a transação realizada na blockchain) pública e privada da transação de cada usuário (figura 1), além disso cada bloco é gerado a cada 10 minutos. (ANDONI, 2018)

Figura 1 - Bloco



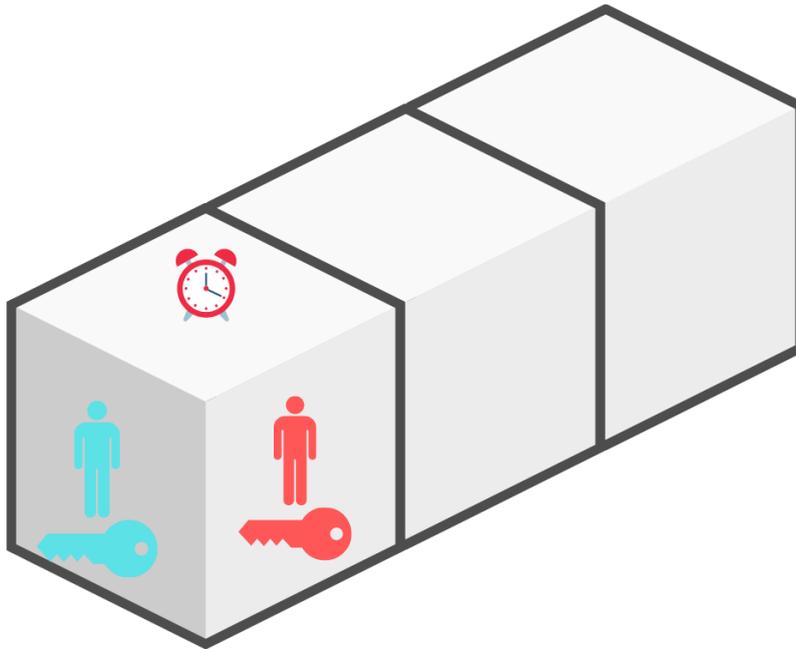
Bloco

Fonte: ANDONI (2018)

Ademais, estes blocos ficam armazenados para todo o sempre enquanto a blockchain e a Internet existirem tais blocos e informações que foram realizadas desde o início do protocolo serão registradas no livro-razão público, online e de fácil acesso em tempo real representado na figura 2.

Figura 2 - Corrente de blocos

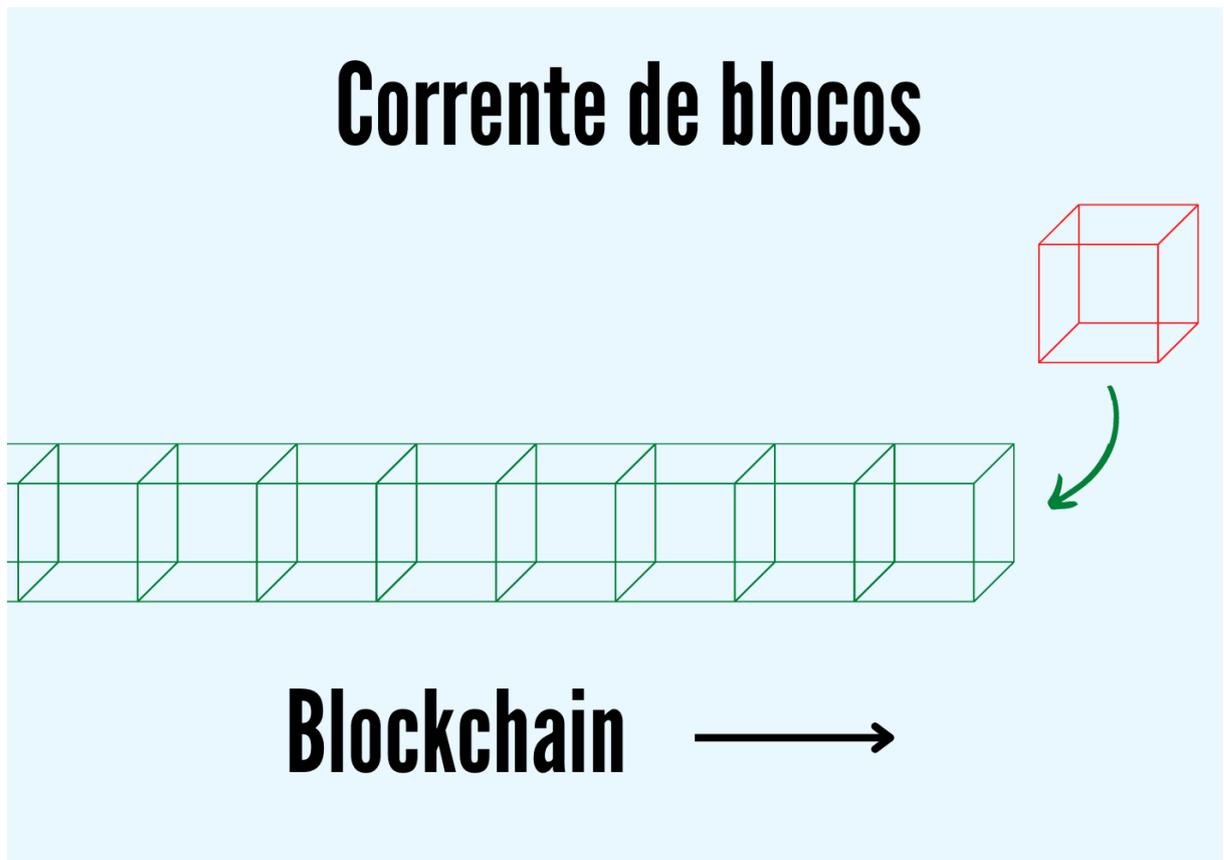
Corrente de blocos



Fonte: ANDONI (2018)

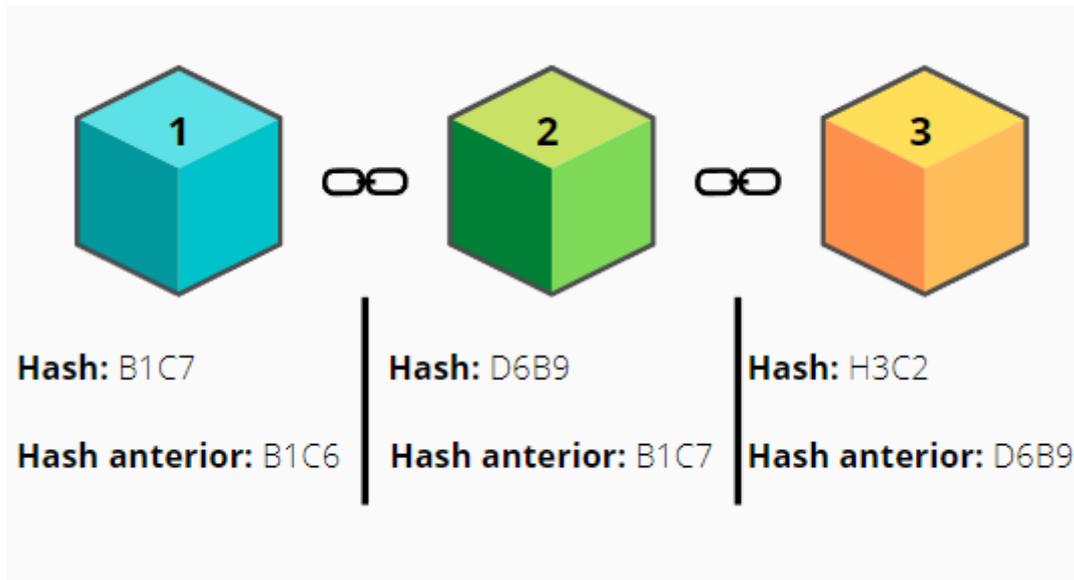
Desse modo a blockchain funciona como uma corrente de blocos em que cada bloco, que possui um conjunto de informações, é adicionado em cadeia (figura 3). E a medida que o tempo se passa mais “robusta”, maior e cada vez mais impenetrável se torna essa cadeia de blocos. Atualmente, por exemplo, seriam necessários mais de 4 bilhões de dólares para, em uma tentativa de 10 minutos, refazer todas as transações de bitcoin de trás para frente e de frente para trás para que seja possível modificar qualquer tipo de informação contida na blockchain também chamado de golpe 51% (devido ataques que foram realizados com sucesso em moedas populares com poucos usuários).

Figura 3- Sequência de blocos



Fonte: ANDONI (2018)

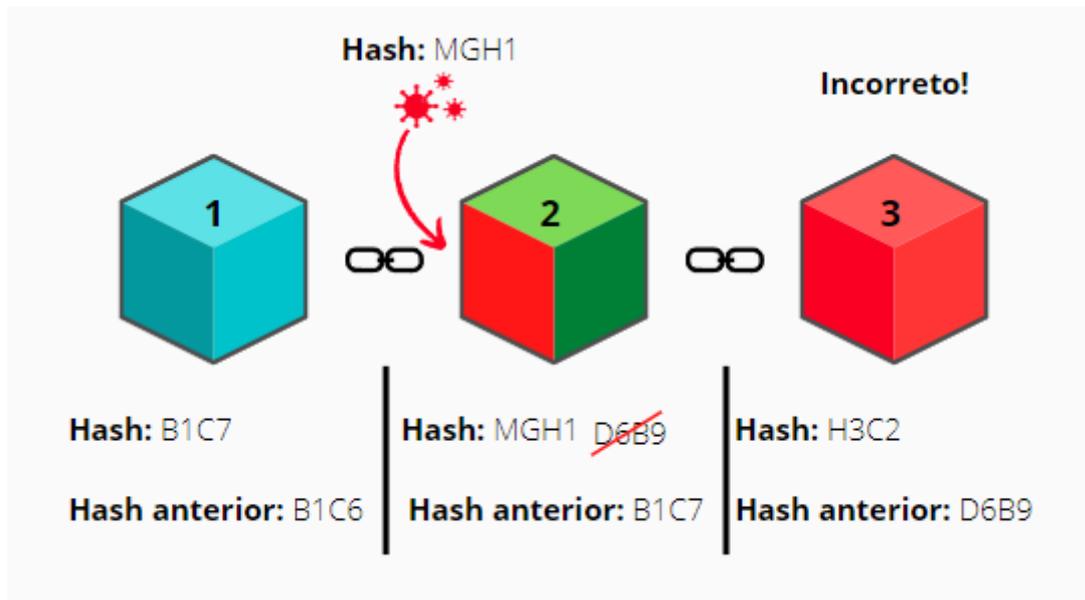
Portanto, toda informação armazenada na blockchain possui uma chance próxima de zero de ser invadida em decorrência da sua complexidade graças a corrente de blocos. Para mais a blockchain é tão poderosa, também, devido ao sistema de *hash* (impressão digital) em que cada bloco de informação que é adicionado, de todas as transações, possui esse sistema de *hash*, ou seja, é o que torna cada dado um dado, que está na blockchain, único. Então, tal dado único sempre vai possuir uma “herança” e toda vez que um novo bloco é criado e são adicionadas novas transações naquele bloco e é necessário que ele tenha uma conexão (ligação direta através de *hash*) com o bloco anterior gerado (*hash* do bloco) representado na figura 4.

Figura 4 - Hash de segurança

Fonte: ANDONI (2018)

Caso algum usuário tente modificar alguma informação seja ela de envio ou de alteração de valores durante a geração do bloco, automaticamente o *hash* é modificado e, portanto o *hash* não será reconhecido pela rede e, assim, tal transação não será validada para que ocorra sua autorização pela blockchain, daí então a rede blockchain tranca todos os blocos posteriores ao bloco com o *hash* diferente do *hash* do bloco anterior, gerando, assim, um sistema de segurança contra diversos tipos de fraude (figura 5) que poderiam ocorrer na blockchain e por esse motivo da tecnologia blockchain ser considerada um sistema seguro e que, futuramente, esteja em diversas empresas no futuro.

Figura 5 - Hash de segurança contra fraude



Fonte: ANDONI (2018)

2.2 CONTRATOS INTELIGENTES

Segundo Zupan (2020) Nick Szabo propôs, pela primeira vez, contratos inteligentes (CI) em 1996, e eles ganharam popularidade como resultado das melhorias "Blockchain 2.0" na tecnologia blockchain. Sem a ajuda de um terceiro confiável, os contratos inteligentes são frequentemente projetados para garantir a justiça entre duas ou mais entidades participantes. O conflito é resolvido de forma justa por meio do sistema judicial, que é a autoridade em que as partes envolvidas confiam. De maneira semelhante, o proprietário do contrato inteligente o configura e o publica no blockchain. Interagindo com ele estão as entidades que aceitam os critérios do CI. Qualquer contrato inteligente genérico em uma blockchain deve atender aos requisitos listados abaixo. Em primeiro lugar, uma vez publicado no blockchain, os termos do CI não podem ser modificados, nem mesmo pelo proprietário. Em segundo lugar, o mecanismo de consenso do sistema blockchain subjacente e a programação criada para impor os requisitos do CI. Portanto, sem envolver um terceiro confiável, isso garante justiça às partes participantes.

Contratos inteligentes (CI) são pedaços de código de computador arbitrário que expressam uma ou mais partes da lógica de negócios. Em contraste com o código de computador padrão, o código de contrato inteligente é implementado em uma rede blockchain, executado e seus resultados são verificados pelos blocos da rede. Para validar o gasto duplo e descrever como novas moedas são criadas e utilizadas, as regras e os critérios para uma

transação bem-sucedida no Bitcoin são expressos usando uma linguagem simples de pilha. É crucial que os contratos inteligentes usados sejam precisos e tenham comportamento determinístico. Houve vários casos em que os invasores se aproveitaram de falhas no código de um contrato inteligente para seu próprio ganho: uma instância bem conhecida é o hack no CI usado pela Organização Autônoma Descentralizada (DAO) na rede blockchain Ethereum.

Existem várias implementações de blockchain diferentes, incluindo Ethereum, Hyperledger Fabric, Hyperledger Sawtooth e outras. Todos eles oferecem uma plataforma de processamento de transações distribuídas baseada em blockchain que permite o uso de contratos inteligentes para definir a lógica de negócios. No entanto, eles fazem uso de diversas características, incluindo tipos distintos de blockchain, algoritmos de consenso e linguagens de design de contrato inteligente. O código desenvolvido para impor a lógica de negócios é chamado de contrato inteligente no Ethereum e outras implementações de blockchain, enquanto o Chaincode é como o Hyperledger Fabric se refere ao mesmo código. Enquanto o Hyperledger Fabric, por exemplo, emprega linguagens de programação comuns como Go, Node.js e Java para produzir chaincode, o Ethereum usa uma linguagem de programação de contrato inteligente especificamente construída chamada Solidity. (ZUPAN, 2020)

De acordo com Alharby e Moorsel (2017) um contrato inteligente é um código executável que é executado na blockchain para facilitar, executar e fazer cumprir os termos de um contrato. O principal objetivo de um contrato inteligente é executar automaticamente os termos de um contrato assim que as condições especificadas forem atendidas (tradução livre). Assim, os contratos inteligentes prometem baixas taxas de transação em comparação com os sistemas tradicionais que exigem um terceiro confiável para fazer cumprir e executar os termos de um contrato. No entanto, a ideia não veio à tona até o surgimento da tecnologia blockchain, o contrato inteligente pode ser pensado como um sistema que libera ativos digitais para todas ou algumas partes envolvidas, uma vez que as regras pré-definidas arbitrárias tenham sido cumpridas.

Muitas definições diferentes de um contrato inteligente têm sido discutidas na literatura. De acordo com Stark (2016) contrato inteligente significa um código que é armazenado, verificado e executado na blockchain (tradução livre). A capacidade deste contrato inteligente depende inteiramente da linguagem de programação para expressar o contrato e os recursos da blockchain. Basicamente, um contrato legal inteligente é um código para completar ou substituir contratos legais. A capacidade deste contrato inteligente não depende de tecnologia, mas sim de instituições legais, políticas e empresariais. Além disso, existem dois tipos de contratos inteligentes: os determinísticos e não determinísticos. Os contratos inteligentes

determinísticos são contratos inteligentes que, quando executados, não requerem nenhuma informação de uma parte externa (de fora da blockchain). E contratos inteligentes não determinísticos são contratos que dependem de informações de uma parte externa, chamados de oráculos ou *feeds* de dados. Por exemplo, um contrato que exige de informações meteorológicas atuais para serem executados, o que não está disponível na blockchain.

Em seguida serão apresentados tópicos de enunciação da tecnologia Ethereum, sua diferença com a tecnologia blockchain Bitcoin, seus benefícios, as aplicações descentralizadas e seus usos para a elucidação dos leitores.

2.2.1 Aplicações de contratos inteligentes

De acordo com Alharby (2017) os contratos inteligentes podem ser usados em uma variedade de aplicações diferentes. Alguns exemplos dessas aplicações são:

- Propriedade inteligente e a Internet das Coisas: A Internet abriga bilhões de nós que se comunicam entre si por meio do compartilhamento de dados. Permitir que esses nós troquem ou acessem várias propriedades digitais sem a necessidade de um terceiro confiável é um uso potencial para contratos inteligentes baseados em blockchain. Várias empresas estão analisando esse caso de uso. Por exemplo, a startup alemã Slock.it usa contratos inteligentes baseados em Ethereum para alugar, vender ou compartilhar qualquer coisa (como comprar ou vender um carro) sem o uso de um terceiro confiável;
- Gerenciamento de direitos musicais: um uso possível é registrar os direitos de propriedade de uma música em um blockchain. Uma vez que uma música é utilizada para um produto ou serviço, um contrato inteligente pode garantir que os proprietários sejam pagos. Além disso, garante que o dinheiro seja compartilhado entre os proprietários da música. Uma empresa chamada Ujo está analisando a aplicação de contratos inteligentes baseados em blockchain no negócio da música;
- O comércio eletrônico pode ser usado para ajudar terceiros não confiáveis (como um fornecedor e um cliente) a realizar negócios sem o envolvimento de um terceiro confiável. Os custos associados à negociação seriam reduzidos como consequência. Somente quando o cliente estiver satisfeito com o bem ou serviço recebido, os contratos inteligentes liberarão o dinheiro para o vendedor.

Votação eletrônica, atividades comerciais, pagamentos de hipotecas, gerenciamento de direitos digitais, seguro automóvel, armazenamento distribuído de arquivos, mercado imobiliário, contratos de trabalho, gerenciamento de identidade e cadeia de suprimentos são alguns outros usos potenciais.

Ribeiro (2019) também aborda algumas aplicações no Governo e Sociedade, como:

- **Dados públicos:** faz sentido que o uso inicial dessas redes seja capturar e armazenar dados públicos. No Brasil, histórias de fraude usando informações privadas como CPF, carteiras de motorista e registros de propriedade de terras são frequentemente relatadas. Essas fraudes poderiam ser diminuídas ou mesmo eliminadas se fossem salvas em uma blockchain porque, a capacidade de alterar dados que já foram salvos em uma blockchain requer um poder computacional extremamente alto, que atualmente só pode ser alcançado por computadores quânticos. Além disso, a transparência pode ser usada para tornar os dados auditáveis, como gastos do governo, acessíveis a todos os cidadãos, minimizando assim a corrupção institucional.
- **Registro de votos:** o Instituto Internacional para Democracia e Assistência Eleitoral anunciou em 2018 que mais de 30 nações, incluindo o Brasil, empregam o método de urna eletrônica. No entanto, há uma discussão substancial sobre a segurança desses sistemas. Uma equipe de segurança da informação da UNICAMP realizou uma série de testes nas urnas utilizadas nas eleições brasileiras de 2017, e o resultado foi a identificação de problemas sistêmicos significativos. A equipe avançou em suas tentativas de influenciar os votos e conseguiu alterar a mensagem que o usuário via após votar. Esta é apenas uma das várias investigações que demonstram quão frágil é a tecnologia em uso e, como resultado, grupos continuam se opondo à adoção generalizada de sistemas de votação computadorizados. Algumas iniciativas utilizam a tecnologia encontrada nas redes blockchain por meio de Contratos Inteligentes para oferecer um mecanismo de votação mais seguro que os sistemas convencionais. Agora e WaveVote são dois exemplos.
- **Transporte urbano:** com o objetivo de melhorar a mobilidade urbana da cidade, a Secretaria Municipal de Planejamento de Teresina (Piauí) anunciou em 2018 uma cooperação com a IBM Hyperledger para a criação de uma rede blockchain. O plano é usar o sistema para registrar dados sobre transporte público, incluindo registros de viagens, atendimento de pedidos de serviço e muito mais.

- **Gestão de saúde:** Os sistemas de gestão hospitalar são frequentemente pouco claros e usados incorretamente. Frequentemente, os pacientes precisam se registrar novamente com as mesmas informações básicas em vários departamentos do hospital dentro da mesma região. Todo o histórico de exames, consultas e medicamentos fornecidos a um paciente pode ser acessado publicamente por qualquer organização de saúde por meio de uma rede blockchain. Consequentemente, como consequência é possível obter maior eficiência no serviço com a maior agilidade no processamento de dados do pacientes, redução de erros provocado por dados incorretos, evolução dos serviços oferecendo informações consistentes a laboratórios, por exemplo, que ajudem na otimização das técnicas, maior controle sobre armazenamento e logística de medicamentos.

2.2.2 Aplicações descentralizadas (dApps)

Segundo Gates (2017) as aplicações descentralizadas são aplicações de fonte aberta não controladas por alguma pessoa ou entidade que executa uma blockchain distribuída ou rede de computadores. Os dApps (aplicações descentralizadas) não possuem um servidor central, em vez disso os usuários se conectam entre si através de conexões chamadas de *peer to peer* (pessoa para pessoa). Já as aplicações padrão, são controladas por uma entidade e executadas em um servidor centralizado que é propenso a *hackers* ou tempo de inatividade caso o servidor fique desligado (*off-line*). Uma aplicação descentralizada não possui um único servidor ou entidade controlada. Ela funciona atravessando a rede de computadores e as mudanças são decididas através dos usuários. Desse modo não há um ponto central que pudesse ser quebrado ou *hackeado* pois se um computador na rede fica desligado (*off-line*), a aplicação não é afetada visto que existem milhares de outros computadores funcionando ao mesmo tempo e mesmo que algum computador na rede seja *hackeado* ele não pode realizar mudanças sem autorização pois maior parte da rede deve concordar com tais mudanças impostas.

2.3 BENEFÍCIOS DOS CONTRATOS INTELIGENTES COM A TECNOLOGIA BLOCKCHAIN

Nos primeiros capítulos foram abordados conceitos sobre blockchain, contratos inteligentes e suas aplicações. Alguns dos benefícios foram brevemente mencionados, portanto nesta seção serão apresentados os benefícios dos contratos inteligentes com a tecnologia blockchain com mais detalhes.

De acordo com Gates (2017) existem 8 benefícios associados a tecnologia blockchain, que são:

- Transparência;
- Remoção de intermediários;
- Descentralização;
- Confiança;
- Segurança;
- Ampla variedade de usos;
- Custos reduzidos;
- Maior velocidade de transação.

Diante os 8 benefícios listados por Gates (2017) inicia-se, portanto com o primeiro deles: a transparência. Os sistemas baseados em blockchain oferecem melhorias na transparência em comparação com a manutenção de registros e livros razão existentes. As alterações no livro razão são visíveis para todos na rede e a transação não pode ser alterada ou excluída uma vez inserida no blockchain. Com a manutenção de registros existente, uma pessoa pode alterar o banco de dados e ocultar a alteração das pessoas. Houve inúmeros exemplos em que casos maciços de fraude não foram detectados, pois os livros não eram transparentes. Essa falta de transparência permitiu que as pessoas alterassem entradas ou manipulassem dados sem que as pessoas soubessem das alterações.

A tecnologia baseada em blockchain fornece transparência a todas as pessoas na rede, com transações visíveis para todos os computadores conectados. A maioria dos computadores conectados ao blockchain deve aprovar transações ou alterações no blockchain, impedindo que as transações sejam ocultadas ou manipuladas. Todas as alterações são quase em tempo real; esse processo ocorre à medida que as transações são aprovadas e adicionadas ao blockchain. Esse cenário de uma pessoa em uma organização roubando dinheiro ou ocultando perdas da

empresa manipulando entradas em livros é menos provável de ocorrer em um livro distribuído baseado em blockchain.

A mudança para blockchain em diferentes setores fornece transparência em várias áreas. Com uma transação financeira, você pode acompanhar o status da transferência no blockchain em tempo real, em vez de não saber o status de uma transação até que ela seja concluída, o que geralmente é fácil com o sistema atual. Essa mesma transparência se aplica a qualquer coisa de valor registrada no blockchain.

O segundo benefício a ser abordado diz respeito a remoção de intermediários pois a maioria das transações hoje entre pessoas exige que intermediários, como bancos, forneçam confiança e segurança para as transações. Uma vantagem da tecnologia blockchain sobre os sistemas existentes é a capacidade de remover intermediários, permitindo que as transações ocorram diretamente entre as pessoas, em vez de envolver terceiros. Isso beneficia bilhões de pessoas no mundo que vivem em países onde não podem confiar em intermediários de terceiros devido a governos corruptos, altos índices de criminalidade, má regulamentação das empresas, manutenção manual de registros ou opções legais limitadas para buscar reivindicações. blockchains são particularmente úteis nesses casos em que a confiança nos intermediários não existe e a transação direta com as pessoas também é difícil ou arriscada.

A descentralização de um banco de dados blockchain é um componente chave de como os intermediários podem ser removidos ao mesmo tempo, aumentando a transparência e a confiança. blockchains são mantidos em um único ledger compartilhado, em vez de vários ledgers que são gerenciados de forma privada por diferentes instituições. Pessoas e empresas não precisam abrir mão do controle para uma única instituição ao usar um blockchain. Isso torna a colaboração entre as partes mais rápida e fácil de gerenciar. Para usar o exemplo de um grupo de bancos transferindo ativos entre si, nas estruturas e sistemas atuais, cada banco manteria seus próprios livros e registros de transações separadamente. Ao usar um livro-razão baseado em blockchain, eles só precisariam reconciliar as transações em um livro-razão compartilhado ao qual todos os bancos teriam acesso e concordariam com o registro correto das transações.

A estrutura descentralizada do blockchain é uma vantagem para empresas que podem ser concorrentes, mas estão trabalhando juntas como parte de um grupo ou consórcio do setor. Uma empresa pode ser cautelosa ao entregar dados ou colaborar em um banco de dados de propriedade de um concorrente. Concorrentes trabalhando juntos, onde uma parte possui todos os dados, podem envolver longos contratos legais e nenhum acordo de divulgação que proteja a privacidade e o acesso dos dados. No entanto, com um sistema baseado em blockchain, os

concorrentes podem trabalhar juntos em um banco de dados compartilhado sobre o qual todos têm acesso e controle total.

Bancos de dados centralizados são propensos a hackers, perda de dados e corrupção. A blockchain não possui banco de dados central que seja ponto de falha, manipulação e corrupção de dados. Todos os computadores na rede blockchain têm uma cópia do blockchain, reduzindo o risco de perda de dados. E caso algum usuário tentasse manipular dados em uma blockchain seria necessário hackear mais de 50% dos computadores da rede ao mesmo tempo; algo que é completamente inviável.

Em respeito a confiança, os métodos atuais para transações entre pessoas requerem confiança e um intermediário para facilitar o processo. A blockchain permite que os intermediários sejam removidos, mantendo a confiança e a segurança entre as pessoas envolvidas na transação. A confiança é colocada na rede blockchain em vez de um terceiro. As redes blockchain são geralmente descentralizadas, com todas as pessoas conectadas à rede tendo acesso ao blockchain. A remoção de intermediários, transparência aprimorada e estrutura descentralizada do blockchain tornam-se um elemento essencial para o aumento da confiança entre as entidades em uma transação que é um importante benefício não tangível desses trocadores.

O quinto benefício é a segurança pois os dados inseridos na blockchain são imutáveis, o que significa que não podem ser alterados ou modificados. Cada bloco de dados no blockchain também pode ser rastreado até o primeiro "bloco de gênese". A imutabilidade dos dados inseridos em blocos combinados conectados desde o primeiro bloco no blockchain cria uma trilha de auditoria fácil de seguir de cada transação no blockchain.

Ao longo da história foram inúmeros os casos de fraude e manipulação de dados. Muitas vezes, quando a fraude é cometida, a trilha que leva à ocorrência da fraude é alterada, tornando a investigação difícil e demorada. A trilha de dados pode ter sido alterada tanto que é impossível rastrear a transação e a fraude. Com um sistema baseado em blockchain, as transações anteriores não podem ser alteradas deixando um rastro claro do que ocorreu no blockchain. Conforme mencionado na seção, em respeito ao terceiro benefício, descentralização do blockchain, alterar uma transação existente exigiria controlar mais de 50% dos computadores da rede ao mesmo tempo, o que é quase completamente inviável. Se isso ocorresse, também seria rapidamente detectado pelos outros computadores conectados à rede. A segurança do blockchain não é perfeita, mas os sistemas existentes atualmente provaram estar longe de ser seguros diversas vezes. O que resolve problemas de segurança em sistemas convencionais, embora a fraude

possa nunca ser totalmente eliminada, o blockchain fornece uma trilha de auditoria clara de volta ao ponto chave, permitindo que as tentativas de fraude sejam facilmente identificadas.

Devido a sua ampla variedade de usos quase tudo de valor pode ser registrado no blockchain, a frase "qualquer coisa de valor", não significa necessariamente valor financeiro. Livros, registro de propriedade, identidade digital, licença de direitos autorais, arquivos digitais ou qualquer coisa que possa ser gravada no banco de dados. Como o exemplo de licenças de copyright (direito autoral), estes são ativos de valor, mas as licenças são apenas dados ou números armazenados em um banco de dados. O valor vem dessas licenças que protegem a propriedade e a renda derivada do que os direitos autorais protegem. Existem organizações e associações que controlam e gerenciam licenças de direitos autorais em um banco de dados centralizado. Essas licenças são ativos de valor que podem ser armazenados no blockchain, eliminando a necessidade das organizações que controlam as licenças. Ativos de valor como criptomoedas, licenças e outros ativos digitais podem existir apenas no blockchain como ativos blockchain nativos, tornando-os mais fáceis de gerenciar do que os registros de propriedade existentes.

A tecnologia blockchain é uma nova tecnologia facilmente acessível, especialmente com inovações recentes, como a plataforma Ethereum e contratos inteligentes. Isso permite que qualquer pessoa desenvolva aplicativos que utilizem a tecnologia blockchain. A blockchain tem o potencial de mudar quase todos os setores do mundo. Os projetos em desenvolvimento mostram o impacto que a tecnologia blockchain pode ter na vida cotidiana, com muitas empresas já desenvolvendo seus próprios sistemas blockchain.

Em respeito à redução de custos a tecnologia blockchain pode reduzir significativamente os custos em diversos setores, removendo os intermediários envolvidos no processo de registro e transferência de ativos. Cada intermediário ou camada envolvida na transação adiciona custos ao registro e transferência de ativos. Nos sistemas atuais, ao transferir ativos ou registrá-los, geralmente há vários livros-razão e bancos de dados que cada organização mantém. Um livro razão distribuído permite que as partes transfiram ativos em um livro razão compartilhado, reduzindo os custos de manutenção de vários livros razão em cada organização. Manter registros ou bancos de dados é caro e geralmente um processo manual com muitas pessoas envolvidas na verificação da integridade de cada registro. Os livros razão distribuídos baseados em blockchain reduzem os custos substituindo os livros razão individuais por um compartilhado, fornecendo liquidação e auditoria em tempo real de todas as partes conectadas à rede sempre que uma transação ocorre.

E, por último, há o benefício de maior velocidade de transação em que os sistemas baseados em blockchain não apenas reduzem os custos envolvidos nas transações, mas também aumentam drasticamente a velocidade. Ao remover intermediários e liquidar transações em um livro razão distribuído compartilhado, os livros razão baseados em blockchain podem liquidar transações quase instantaneamente. Se alguém transferiu dinheiro de uma conta bancária, é possível notar que os fundos estão sendo retirados de sua conta; no entanto, eles não foram recebidos na outra conta até dias depois. Da mesma forma, com compras com cartão de crédito, as transações podem aparecer como pendentes por vários dias no extrato do cartão de crédito. Para os lojistas, eles fornecem mercadorias ao comprador, mas não recebem o pagamento dias depois, quando a empresa de cartão de crédito liquida a transação.

Nestes exemplos acima, sistemas baseados em blockchain estão sendo desenvolvidos para aumentar a velocidade dessas transações. No entanto, não se limita apenas a esses exemplos, qualquer tipo de transação ou transferência pode usar a tecnologia blockchain para aumentar a velocidade das transações.

2.4 DESVANTAGENS E PERIGOS DE CONTRATOS INTELIGENTES COM A TECNOLOGIA BLOCKCHAIN

Apesar de existirem diversos benefícios associados aos contratos inteligentes com a tecnologia blockchain não significa que seja uma tecnologia impecável e muito menos uma solução para todos os problemas dentro da indústria. Há uma ampla gama de razões convincentes para mudar de sistemas existentes para sistemas baseados na blockchain. No entanto, também existem desvantagens e riscos que não devem ser ignorados.

A tecnologia blockchain está sendo apontada por muitos como a solução para todos os problemas nas indústrias e no mundo no momento. Há novas startups de blockchain e criptomoedas lançadas todos os dias prometendo fazer de tudo, desde perturbar os sistemas bancários até eliminar a pobreza mundial. Muitas das alegações são uma reminiscência da internet nos primeiros dias. Embora a internet tenha mudado o mundo, muitas das alegações foram exageradas, os prazos não eram realistas e muitas startups previstas para serem bem-sucedidas faliram.

Por esse motivo Gates (2017) aponta 5 desvantagens e perigos relacionados ao uso da tecnologia blockchain, que são:

- Sem controle centralizado;

- Risco de ataque 51%;
- Custo;
- Falta de escalabilidade;
- Regulação e integração.

Os sistemas baseados em blockchain são projetados para substituir intermediários de terceiros, devolvendo a responsabilidade e o controle aos indivíduos envolvidos nas transações. Este controle é colocado com a maioria das pessoas na rede, criando problemas com relação ao controle da blockchain. A natureza descentralizada de muitas blockchains significa que a rede deve concordar e decidir a direção futura da rede e da blockchain. Com uma rede e software tradicionais, se uma organização quiser fazer uma alteração, ela não poderá fazer essa alteração após a aprovação dos departamentos relevantes da organização. Com uma rede blockchain descentralizada como o Bitcoin, as mudanças devem ser acordadas por uma certa maioria da rede, isso pode ser superior a 50%, mas pode chegar a 70% a 80% da rede. Um exemplo recente disso foi a divisão na rede Bitcoin sobre a implementação do SegWit (Segregated Witness) ou do Bitcoin Unlimited.

Se alguém pudesse controlar mais de 50% dos computadores em uma rede blockchain, eles controlariam as transações na blockchain. Um usuário mal-intencionado que controla mais de 50% dos computadores em uma rede blockchain é conhecido como "ataque de 51%". Aproveitando esse controle sobre uma rede de criptomoedas, eles teoricamente seriam capazes de bloquear novas transações de confirmação, transações reversas e permitir o temido "gasto duplo" de moedas. Um ataque de 51% em uma rede blockchain é teórico, pois seria difícil controlar uma quantidade tão grande da rede. No entanto, existem enormes fazendas de mineração na China, Rússia e outras partes do mundo que controlam grande parte do poder de computação das redes blockchain. Se essas grandes fazendas de mineração colaborassem, elas poderiam assumir as redes blockchain e manipulá-las em seu benefício. Mesmo sem controlar 51% da rede, eles ainda podem manipular a rede alocando seu poder de computação de uma forma que influencie o desenvolvimento futuro da rede.

Como mencionado anteriormente, a segurança criptográfica é superior aos métodos de segurança existentes; no entanto, se alguém perder sua chave para sistemas baseados em blockchain, não poderá recuperá-la. As pessoas optam por escrever suas chaves privadas em papel ou armazená-las em seus computadores, para não esquecê-las, eliminando assim os benefícios da segurança adicional e potencialmente tornando o sistema menos seguro. Outro

benefício das redes blockchain é remover intermediários de terceiros. O processo de conexão com redes blockchain, envio de transações, configuração de chaves privadas é complicado e arriscado para muitas pessoas. Muitas pessoas preferem dar acesso às suas chaves privadas a intermediários de terceiros com carteiras da web ou software semelhante, o que elimina outro benefício principal das redes blockchain.

O algoritmo de prova de trabalho que muitas redes blockchain usam requer prova de que o poder e os recursos de computação foram contribuídos para a rede antes que um bloco seja adicionado à rede. Essa prova está na forma de uma resposta a um quebra-cabeça que é anexado ao bloco para que a rede confirme se está correto. Resolver esse quebra-cabeça requer uma enorme quantidade de poder de computação e eletricidade. Alguns especialistas calculam que a cada meia hora a rede Bitcoin usa a mesma quantidade de eletricidade que a média das famílias dos EUA em um ano inteiro. A família média dos EUA usa de 10 a 12.000 kWh de eletricidade a cada ano, aproximadamente o mesmo que seria necessário para gerar quatro Bitcoins no valor de cerca de US\$ 1.000,00 (no ano de 2017). Devido aos altos custos de eletricidade para executar computadores em redes blockchain usando esse algoritmo de prova de trabalho, há uma vantagem para países onde a eletricidade é barata ou para organizações que têm acordos especiais com empresas de energia. À medida que a dificuldade dos quebra-cabeças no blockchain do Bitcoin aumenta, o consumo de eletricidade aumenta, tornando ainda mais caro e intensivo em recursos para executar uma blockchain com algoritmo de prova de trabalho em larga escala.

Na taxa atual de consumo de energia, os custos de eletricidade de executar uma blockchain usando o algoritmo de prova de trabalho torna inviável lidar com o número de transações por empresas de cartão de crédito como Visa ou MasterCard. Este é um dos fatores que está afetando atualmente a escalabilidade da blockchain. Um bloco é adicionado à blockchain Bitcoin, por exemplo, a cada 10 minutos, cada bloco contém atualmente cerca de 2.000 transações, o que significa que a rede bitcoin está processando cerca de 3 transações por segundo. Devido aos limites de tamanho do bloco, a rede Bitcoin só é capaz de lidar com cerca de 7 transações por segundo. A Visa realizou testes com a IBM, concluindo que a rede Visa é capaz de lidar com mais de 20.000 transações por segundo. Se alguém entrar em uma loja e usar seu cartão de crédito, mas não tiver dinheiro suficiente no cartão para fazer a compra, o sistema de cartão de crédito rejeitará a transação. O Bitcoin Blockchain não possui um mecanismo como este. Uma transação no blockchain do Bitcoin levará no mínimo 10 minutos para ser adicionada, as empresas de blockchain podem esperar que vários outros blocos sejam adicionados antes de aceitar a transação, para garantir que a transação não seja revertida.

Comparando a diferença entre esses dois métodos, se alguém entrar em uma loja para pagar com Bitcoin, o dono da loja pode ter que esperar uma hora para garantir que a transação seja confirmada com vários blocos adicionados a blockchain no topo do bloco que contém o transação. Existem redes blockchain que são mais rápidas que a rede Bitcoin. No entanto, nenhum tem o mesmo nível de popularidade ou aceitação como forma de pagamento do Bitcoin. Mesmo as blockchains e criptomoedas que possuem tempos de confirmação de transação mais rápidos ainda não têm capacidade de escalar o nível das redes de pagamentos financeiros existentes, como Visa ou Mastercard. Devido a esses problemas de escalabilidade, muitas pessoas veem a implementação do blockchain em grande escala nada mais do que um registro oficial (livro razão) de informações com carimbo de data/hora.

Os ativos baseados em blockchain enfrentam um processo de regulamentação e problemas de integração com os sistemas existentes. Governos e bancos são resistentes a mudanças devido à escala e ao custo de substituição dos sistemas existentes. A menos que os sistemas baseados em blockchain possam provar que fornecerão economias de custos significativas ou benefícios para justificar a substituição dos sistemas existentes, é incomum que grandes instituições, como governos ou bancos, os usem em breve.

O governo da Estônia está testando sistemas baseados em blockchain, mas a Estônia tem uma população de menos de 1,5 milhão. Existem cidades nos EUA, China e outros países com 10 vezes essa população, embora os sistemas baseados em blockchain possam funcionar em pequena escala, não é tão fácil integrá-los na escala necessária para governos como os EUA ou grandes bancos. O consórcio R3 e o ripple são exemplos de ledgers baseados em blockchain ou distribuídos que estão sendo integrados a muitas empresas financeiras de diferentes países. Existem empresas financeiras que estão retendo sua transição para o uso de um livro-razão baseado em blockchain por causa da "pequena" escala em que um blockchain foi testado. Se um grande número de instituições financeiras mudar para uma tecnologia nova e não testada e a estiver usando quando os problemas forem descobertos, isso poderá representar um risco significativo para os mercados financeiros e os dados dos clientes. Também houve preocupações do Conselho de Supervisão de Estabilidade Financeira (FSOC) de que alguns sistemas baseados em blockchain poderiam ser mais vulneráveis a fraudes do que se entende atualmente com testes em pequena escala. Outro problema com várias instituições financeiras que adotam um sistema baseado em blockchain compartilhado ou livro-razão distribuído é a área em que os reguladores trabalham. Um sistema baseado em blockchain pode, teoricamente, abranger muitas jurisdições regulatórias diferentes e fronteiras nacionais, escurecendo ainda mais as águas entre os reguladores e a jurisdição pela qual uma transação deve ser tratada. As

grandes instituições financeiras estarão dispostas a mudar para qualquer sistema em que a regulamentação governamental não seja clara. Os riscos financeiros e comerciais são altos se os governos não tiverem regulamentações claras sobre como os ativos baseados em blockchain são tratados. Preocupações com a regulamentação, o custo da integração, juntamente com a falta de aplicativos em larga escala de sistemas baseados em blockchain, levará a uma lenta aceitação da tecnologia por grandes instituições financeiras e governos.

Por fim, apresenta-se um quadro resumindo os objetivos do trabalho, o que foi apresentado e os autores respectivamente:

Quadro 1 - Objetivos, identificação e autores utilizados

Objetivos	O que foi identificado	Autor
Identificar os contratos inteligentes	Conceito de contratos inteligentes	Maher Alharby
Aplicações dos contratos inteligentes	Aplicações de contratos inteligentes com blockchain	
Enunciar o que é e o porquê da utilização da tecnologia blockchain	Conceito de blockchain	Merlinda Andoni
Aplicações descentralizadas	Aplicações descentralizadas	Mark Gates
Analisar e compreender os benefícios, desvantagens e perigos da utilização da tecnologia blockchain	Benefícios, desvantagens e perigos da blockchain	
Aplicações do contratos inteligentes	Aplicações de contratos inteligentes no governo e sociedade	Lucas Ribeiro
Identificar os contratos inteligentes	Definição de contratos inteligentes	Josh Stark

Fonte: Próprio autor

3 CONCLUSÃO

A tecnologia blockchain possui sua origem definida em meados do ano de 2008 por meio do pseudônimo Satoshi Nakamoto. E mediante um protocolo para que os conceitos e funcionamento fossem enunciados surgiu o Bitcoin. Desde então o mundo, a partir daquele ano passou a ter contato com uma das tecnologias mais promissoras do mundo: a blockchain.

Graças aos sistemas de armazenamento que utilizam correntes de blocos e tecnologias de criptografia para proteção de dados o Bitcoin teve como principal objetivo a descentralização de transações financeiras entre usuários do mundo todo com a ajuda de um sistema transparente, confiável e seguro. Em seguida, no ano de 2013 através do russo-canadense Vitalik Buterin mais um passo para o desenvolvimento da tecnologia Blockchain surgiu: a tecnologia Ethereum. Por via dela deu-se início a uma plataforma de computação distribuída para o funcionamento de aplicações feitas por desenvolvedores para pagamento de poder de computação na rede ao executar aplicações descentralizadas por meio da criptomoeda Ether.

A partir do surgimento da tecnologia Ethereum observou, então, a possibilidade da utilização da blockchain para uma ampla variedade de usos, como: registros de propriedade, identidades digitais, licenças de direitos autorais, arquivos digitais ou qualquer coisa que possa ser gravada no banco de dados.

Ademais o tema blockchain possui extrema relevância tanto no meio acadêmico quanto no meio empresarial visto que é um tópico atual, de grande relevância e com um horizonte completamente novo. Buscando gerar valor acadêmico para toda a comunidade científica, para o estudante e futuros leitores.

E, finalmente, concluir que os objetivos propostos de análise do uso de contratos inteligentes, enunciar o conceito da tecnologia blockchain, suas aplicações, o porquê de sua utilização, benefícios e desvantagens em conjunto com compreensão da influência da tecnologia blockchain no futuro da gestão foram discorridos durante a apresentação do presente trabalho.

3.1 PRINCIPAIS OBSERVAÇÕES

Mediante ao exposto observa-se que a tecnologia blockchain possui inúmeras vantagens, como: transparência, segurança e custos reduzidos. No entanto, por ser uma tecnologia nova, também possui algumas desvantagens decorrente aos sistemas operantes existentes, como: custos, falta de escalabilidade e problemas de regulação e integração. Por esse motivo a tecnologia blockchain possui potencial para que seja utilizada no futuro caso melhorias sejam implementadas para que determinadas desvantagens sejam eliminadas proporcionando diversos benefícios aos usuários que estiverem utilizando de tal tecnologia. Ademais a tecnologia blockchain pode também proporcionar inúmeros benefícios devido a sua ampla variedade de usos como para a geração de contratos inteligentes, registro de propriedade, identidades digitais, licenças de direito autoral, arquivos digitais etc. Visto que enquanto tal tecnologia existir as informações contidas nela se permanecerão por muito tempo.

3.2 IMPLICAÇÕES FUTURAS

No presente momento a única implicação futura a ser constatada como um fato é que a humanidade presenciará por mudanças significativas, durante os próximos anos, em respeito à forma como dados, transações financeiras e diversas outras tecnologias que não são associadas à blockchain sejam utilizadas. Já em respeito à tecnologia blockchain diversas previsões podem

ser feitas, como: geração de trabalho para usuários que estejam estudando em respeito ao assunto, surgimento de novas empresas (startups) especializadas em tecnologia blockchain, aumento na velocidade na geração de blocos, investimentos voltados para financiamento de empresas, regulamentação da tecnologia blockchain em diversos bancos e países, além de tremendas contribuições para governos e universidades. E por esses e diversos outros motivos a tecnologia blockchain possui enorme potencial para se tornar uma tecnologia promissora para o futuro da humanidade permitindo que a torne mais próspera, bem sucedida e saudável para as próximas gerações que estejam por vir. Além disso, também abre oportunidade para novos estudos voltados à tecnologia blockchain com objetivo de proporcionar maior enriquecimento ao assunto.

4 REFERÊNCIAS

ALHARBY, Maher; VAN MOORSEL, Aad. **Blockchain Based Smart Contracts: a systematic mapping study**. Computer Science & Information Technology (Cs & It), [S.L.], v. 7, p. 125-140, 26 ago. 2017. Academy & Industry Research Collaboration Center (AIRCC). <https://arxiv.org/ftp/arxiv/papers/1710/1710.06372.pdf>.

ANDONI, Merlinda; ROBU, Valentin; FLYNN, David; ABRAM, Simone; GEACH, Dale; JENKINS, David; MCCALLUM, Peter; PEACOCK, Andrew. **Blockchain technology in the energy sector: a systematic review of challenges and opportunities**. Renewable And Sustainable Energy Reviews, [S.L.], v. 100, p. 143-174, fev. 2019. Elsevier BV. <http://dx.doi.org/10.1016/j.rser.2018.10.014>.

GATES, Mark. **Blockchain: ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money**. California: Wise Fox Publishing, 2017.

LEWIS, Antony. **The basics of bitcoins and blochains: an introduction to cryptocurrencies and the technology that powers them**. Florida: Mango Publishing Group, 2018.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 8a Edição. Editora Atlas, São Paulo, SP, 2019. Disponível na biblioteca virtual integrada da FATEC em: <<https://integrada.minhabiblioteca.com.br/#/>>. Acesso em: 06/05/2020.

OLIVEIRA, Maxwell Ferreira de. **Metodologia científica: um manual para a realização de pesquisas em Administração**. Catalão: UFG, Biblioteca da UFG, 2011.

RIBEIRO, Lucas; MENDIZABAL, Odorico. **Introdução à Blockchain e Contratos Inteligentes: Apostila para Iniciante**. Santa Catarina: Universidade Federal de Santa Catarina, 2019. 56 p.

STARK, Josh. **Making sense of blockchain smart contracts**. 2016. Disponível em: <https://www.coindesk.com/markets/2016/06/04/making-sense-of-blockchain-smart-contracts/>. Acesso em: 30 maio 2022.

ULRICH, Fernando. **Bitcoin - A moeda na era digital**. São Paulo: Mises Brasil, 2014.

ZUPAN, Nejc; KASINATHAN, Prabhakaran; CUELLAR, Jorge; SAUER, Markus. Secure Smart Contract Generation Based on Petri Nets. **Blockchain Technology For Industry 4.0**, [S.L.], p. 73-98, 2020. Springer Singapore. http://dx.doi.org/10.1007/978-981-15-1137-0_4.