**FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"**
**Curso Superior de Tecnologia em Segurança de informação**

Anderson Luis dos Santos
Evandro Tampelini Goulart

# Criptomoedas: A moeda e o Sistema de Segurança nas Informações

**Americana, SP**
**2022**

**FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"**

**Curso Superior de Tecnologia em Segurança da Informação**

Anderson Luis dos Santos Silva

Evandro Tampelini Goulart

# Criptomoedas: A Moeda e o Sistema de Segurança nas Informações

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Dr. Ivan Menerval da Silva

Área de concentração: Tecnologia em Segurança da Informação.

**Americana, SP.**

**2022**

Anderson luís dos Santos Silva
Evandro Tampelini Goulart

# TÍTULO
## A Moeda e o Sistema de Segurança nas Informações

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em **Segurança da informação** pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 01 de dezembro de 2022

**Banca Examinadora:**

Ivan Menerval da Silva (Presidente - Orientador)
Doutor em Engenharia de produção
Fatec – Faculdade de Tecnologia de Americana – Ralph Biasi.

Renato Kraide Soffner (Banca 02)
Doutor em Educação
Fatec – Faculdade de Tecnologia de Americana – Ralph Biasi.

Maxwel Vitorino da Silva (Banca 03)
Mestre em Teconologia
Fatec – Faculdade de Tecnologia de Americana – Ralph Biasi.

# RESUMO

O presente trabalho abordou o uso e a segurança das criptomoedas que ganharam notoriedade após grande avanço tecnológico, criado após anos de estudos. O nosso principal objetivo será referente à segurança das informações que esse invento trouxe, mostrando o lado positivo e negativo de se utilizar essa moeda que demorou vários anos para ser desenvolvida e ser aceita no mercado financeiro sem controle estatal ou de órgãos financeiros.

Abordaremos sua crescente utilização no dia a dia, suas origens e conceitos, modalidades mais utilizadas e por fim, que o ponto crucial e a finalidade da presente monografia, seus riscos e benefícios direcionados para a segurança da informação e descrevendo minunciosamente o que ocorre após adquirir uma moeda digital, bem como, suas garantias na exposição de dados pessoais nos negócios assumidos.



Palavras-chave: criptomoedas, mercado financeiro, digital, segurança, informação, dados, garantias, riscos.

## ABSTRACT

The present work will address the cryptocurrencies that gained notoriety after the great technological advance, being created after several studies for years. Our main objective will refer to the security of the information that this invention brought, showing the positive and negative side of using this currency that took several years to be developed and accepted in the financial market without having any state control or financial agencies.

We will approach its growing use in everyday life, its origin and concepts, the most used modalities and finally, which is the crucial point and purpose of this monograph, its risks and benefits aimed at information security, describing in detail what happens after acquire a digital currency, as well as its guarantees in the exposure of personal data in the businesses undertaken.


Keywords: cryptocurrencies, financial market, digital, security, information, data, guarantees, risks.

# SUMÁRIO

# 1. Introdução

O avanço tecnológico está a cada dia mais impactante na sociedade e em cada momento é possível descobrir algo novo a ser inventado, por exemplo, a utilização de moedas digitais que facilita no investimento ou na compra de serviços e produtos, as chamadas criptomoedas.

Esse novo fenômeno de investimentos na área digital que mexeu com o mercado financeiro está sendo usado a cada dia mais por empresas e por grandes investidores devida a sua volatilidade, ou seja, a moeda em alta valorização no dia a dia, e a não interferência política de qualquer país ou de órgãos investidores, bem como, o seu uso ser facilitado.

Além disso, a transferência é extremante segura e o que interessa diretamente para nós ao longo desse trabalho e também.

# 2. Origem

O nome internet deriva da junção de duas palavras de origem inglesa, Internacional network. Traduzindo para o português, rede internacional. Ou seja, a internet é uma rede mundial de computadores interligados que, por meio dela, dados e informações são transmitidos para qualquer usuário que nela esteja conectado.

> A história da criação e do desenvolvimento da Internet é a história de uma aventura humana extraordinária. Ela põe em relevo a capacidade que tem as pessoas de transcender metas institucionais, superar barreiras burocráticas e subverter valores estabelecidos no processo de inaugurar um mundo novo. Reforça também a ideia de que no processo de que a cooperação e a liberdade de informação podem se mais propícias à inovação do que a competição e os direitos de propriedade. (CASTELLS, 2003, pág. 13).

A Internet é sem dúvida, uma das maiores invenções do século XX. Desde que surgiu, abriu as portas para novos desenvolvimentos tecnológicos que continuam avançando até no dia de agora, fazendo parte do nosso dia-a-dia influenciando e transformando o modo de como vivemos e nos relacionamos. Atualmente, viver sem a Internet é simplesmente impensável e isso porque a maioria das coisas ao nosso redor está relacionada a internet.

Por esse motivo, decidimos buscar na linha do tempo um pouco da história da Internet, explorando suas origens e passando pelos momentos principais de sua evolução para entender seus efeitos no mundo globalizado e na transformação digital que marca o século XXI.

A internet é tão essencial no nosso dia a dia que não conseguimos parar para pensar em como era a vida sem ela. Mas a verdade é que a internet é uma invenção relativamente contemporânea, que surgiu com fins militares durante a Guerra Fria.

Há 40 anos atrás, enquanto os principais meios de comunicação eram o telégrafo e o telefone, os computadores eram grandes máquinas que realizavam cálculos e armazenavam informações. De forma geral, seu uso tinha fins exclusivamente científicos e governamentais.

Então, como foi que chegamos à chamada era da Informação, na qual a tecnologia invade todos os aspectos de nossas vidas? Se quisermos encontrar uma resposta para essa pergunta, precisamos retroceder na história da Internet.

Em 1957, os Estados Unidos e a União Soviética protagonizavam a Guerra Fria, um embate em termos ideológicos, econômicos, políticos, militares e, é claro, tecnológicos. A internet é tão essencial no nosso dia a dia que não conseguimos parar para pensar em como era a vida sem ela. Mas a verdade é que a internet é uma invenção relativamente contemporânea, que surgiu com fins militares durante a Guerra Fria.

A rede Arpanet era responsável por trocar informações entre militares e cientistas durante a Guerra Fria. A rede pertencia ao Departamento de Defesa dos Estados Unidos, era financiada pela NASA (Nacional Administration Aeronautics and Space) e pelo Pentágono, e tinha a intenção de não interromper a comunicação mesmo em caso de bombardeio.

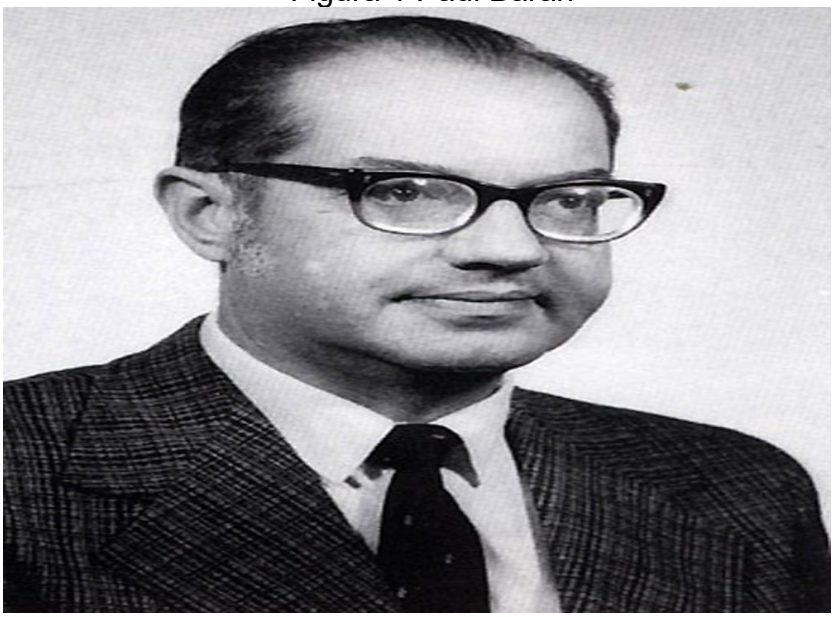
Os primeiros estabelecimentos ligados através da rede Arpanet foram a Universidade de Utah, a Universidade da Califórnia (polos de Los Angeles e Santa Bárbara) e o Instituto de Pesquisa de Stanford.

Em 1989, foi criada a World Wide Web, popularmente conhecida como web, pelo físico e pesquisador do MIT (Massachusetts Institute of Technology) Timothy John Berners-Lee, que traduzida para o português significa “rede de alcance mundial”. Ela é a plataforma que tornou popular a internet que hoje conhecemos.

> A web pode ser definida como um conjunto de recursos que possibilita navegar na Internet por meio de textos hipersensíveis com hiper-referências em forma de palavras, títulos, imagens ou fotos, ligando páginas de um mesmo computador ou de computadores diferentes. A web é o segmento que mais cresce na internet e a cada dia ocupa espaços de antigas interfaces da rede. (VILHA, 2002, pág. 20).

Um nome importante por trás da Arpanet foi o de Paul Baran (1926-2011), um cientista especializado em comunicação digital que ajudou a impulsionar o desenvolvimento da red.

Figura 1 Paul Baran



Fonte:https://www.ebiografia.com/quem_criou_internet/

Na figura 1 podemos ver a imagem de Paul Baran que foi um engenheiro elétrico que desenvolveu os fundamentos técnicos da Arpanet. Ele nasceu no dia 29 de abril de 1926, na Polônia, e nos primeiros anos de da década de 60 teve a ideia de desenvolver os *message blocks*, isto é, pequenos blocos de mensagem contendo informações que são reconstruídas quando chegam ao destino

Em 1982 a Arpanet passou a ser mais usada no meio acadêmico (a princípio apenas nos Estados Unidos, depois em outros países da Europa). O uso comercial aconteceu cinco anos mais tarde, no começou em 1987, primeiro nos Estados Unidos.

Kahn e Cerf criaram juntos os protocolos TCP/IP, a arquitetura de internet, que foram as bases para que pudéssemos ter acesso à rede universal que temos hoje. Eles desenvolveram o IP para transmissão das informações através da Arpanet, o que lhes rendeu o título de "pais da internet".

Robert Elliot Kahn nasceu no dia 23 de dezembro de 1938 em Brooklyn, Nova Iorque, e se tornou um importante engenheiro elétrico. Kahn se formou em

engenharia pelo City College of New York em 1960 e depois fez o mestrado e o doutorado na área.

O cientista da computação Vinton Cerf nasceu no dia 23 de junho de 1943 em Connecticut e foi o mais importante parceiro de Robert Elliot Kahn. Os dois foram responsáveis pela criação de regras técnicas que permitiram que vários computadores distintos (de diferentes marcas) pudessem entrar numa mesma rede para partilharem informações.

Berners-Lee nasceu em Londres, Inglaterra, filho de Conway Berners-Lee e Mary Lee Woods. Estudou na escola primária Sheen Mount e depois na Emanuel School em Londres, de 1969 a 1973. Depois estudou no The Queen's College, em Oxford, de 1973 a 1976, onde diplomou-se em Física.

Enquanto atuava como um contratante independente no CERN, de junho a dezembro de 1980, Berners-Lee propôs um projeto baseado no conceito de hipertexto para facilitar a partilha e atualização de informações entre os pesquisadores. Enquanto isso, ele construiu um protótipo de sistema denominado ENQUIRE.

Depois de deixar o CERN, em 1980, foi trabalhar na John Poole's Image Computer Systems, Ltd, em Bournemouth, na Inglaterra, mas retornou ao CERN em 1984 como efetivo. Em 1989, o CERN foi o maior nó da internet na Europa, e Berners-Lee viu a oportunidade de unir hipertexto com internet.

Em 1989, foi criada a World Wide Web, popularmente conhecida como web, pelo físico e pesquisador do MIT Timothy John Berners-Lee, que traduzida para o português significa “rede de alcance mundial”. Ela é a plataforma que tornou popular a internet que hoje conhecemos.

O primeiro site foi construído no CERN e foi posto online em 6 de agosto de 1991. Info.cern.ch foi o endereço da primeira web site e servidor web da história, rodando em um computador NeXT no CERN.

Não há imagens da tela desta página original e, em qualquer caso, alterações foram feitas diariamente com a informação disponível na página WWW quando o projeto desenvolveu-se. Pode-se encontrar uma cópia mais tardia (1992) no website do World Wide Web Consortium. Havia uma explicação sobre o que a World Wide Web era e como alguém poderia usar um browser e configurar um servidor web.

Nesse período compreendido entre 1994 e 1996, as páginas que predominavam eram as produzidas em HTML (Hyper Text Markup Language) estáticas. Após isso as páginas começaram a apresentar algumas atividades dinâmicas através do uso do Java script e Applet feitos em Java. Nesse período poucas pessoas tinham o privilégio do acesso à internet, onde suas atividades eram basicamente chats, buscas, notícias e páginas pessoais.

Em 2003, a web passa a ganhar uma nova denominação, a web 2.0. Não que ela tenha ocorrido ocasionada por revoluções tecnológicas, mas sim por uma mudança de foco, onde percebeu-se a necessidade de transformar sites estanques, estáticos em uma posição de troca de conteúdo. Tim O'Reilly, precursor do uso do termo da web 2.0, citado por Vaz (2008), diz que:

> Web 2.0 é a mudança para uma internet como plataforma, e um entendimento das regras para obter sucesso nesta nova plataforma. Entre outras, a regra mais importante é desenvolver aplicativos que aproveitem os efeitos de rede para se tornarem melhores quanto mais são usados pelas pessoas, aproveitando a inteligência coletiva. (Pág. 44).

Uma grande mudança comportamental com o advento da web 2.0 foi o crescimento das redes de relacionamento e compartilhamento de informação. Na web 2.0 é possível que os softwares encontrados na internet funcionem em seu computador sem a necessidade da instalação do mesmo, além disso, eles podem se integrar e formar uma plataforma que oferece diversos serviços através de um só. A característica mais marcante da web 2.0 é o entretenimento.

Os usuários estão sempre em busca de sites que ofereça novas oportunidades de experiência. E assim a web 2.0 passa a gerar um grande impacto sobre os conteúdos publicados nas websites, pois, através dela, diversas ferramentas foram geradas, a fim de permitir ao usuário a oportunidade de participar da produção e organização do mesmo.

# 3. Segurança da informação

A Segurança da informação refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

> Traduzindo essa definição formal, podemos dizer que a segurança da informação é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócios. (SMUDERS; BAARS, 2018, p. 16)

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal-intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A maioria das definições de Segurança da Informação pode ser sumarizada como a proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas. A SI(Segurança da Informação) não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma. É importante lembrar que a SI também cobre

toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias e outros.

> O Sistema de gestão de segurança da informação é parte de um Sistema de gestão global da organização para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação, baseado na abordagem de riscos do negócio. O sistema de gestão inclui estrutura organizacional, politicas, atividades de planejamento, responsabilidades, práticas, procedimentos processos e recursos. (ARANTES TEIXEIRA FILHO, SOCRATES: 2015, P.03).

A tríade CIA (Confidentiality, Integrity and Availability) — Confidencialidade, Integridade e Disponibilidade — representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são não-repúdio (irretratabilidade), autenticidade e conformidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação. Portanto os atributos básicos da segurança da informação, segundo os padrões internacionais (ISO/IEC 17799:2005) são os seguintes:

**Confidencialidade:** propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;

**Integridade:** propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente). O ciclo de vida da informação orgânica - criada em ambiente organizacional - segue as três fases do ciclo de vida dos documentos de arquivos; conforme preceitua os canadenses da Universidade do Quebec (Canadá): Carol Couture e Jean Yves Rousseau, no livro Os Fundamentos da Disciplina Arquivística;

**Disponibilidade:** propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;

**Autenticidade:** propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;

A proteção das informações e as estratégicas nos dias atuais de um mundo moderno e tecnológico onde a empresa passa ou deverei passar pelo profissional de segurança de informação e que deve também estar preparado para desempenhar seu papel sem margens de erro. Um bom profissional de Segurança da Informação é capaz de monitorar riscos e projetar respostas adequadas a cada um deles, protegendo as máquinas contra o acesso de *hackers* e espiões. Além disso, ele também pode evitar a apropriação de dados sigilosos por criminosos que buscam fraudar e aplicar golpes na empresa. Em uma era onde quem tem a informação tem o poder, fica claro que é muito importante saber usar estas informações de maneira inteligente. Bem como, é fundamental que as informações estejam disponíveis em tempo hábil e protegidas de acordo com seu nível de sigilo.

As informações precisam chegar no lugar certo, para a pessoa certa e no tempo certo. Velocidade e qualidade da informação viraram diferencial competitivo nos negócios. Com tantas informações importantes sendo trocadas, é despertado o interesse de pessoas com más intenções no uso destes dados. Basta acompanhar as notícias para descobrir uma nova invasão na rede de um banco ou o roubo de informações de uma grande empresa ao redor do mundo. Os crackers e outras pessoas especializadas em corromper a segurança de sistemas da informação também estão avançando em suas estratégias. Por isso, a cada dia se faz mais importante para as organizações terem profissionais especializados e dedicados em proteger estas informações.

> Pode ser que, nesse meio tempo que for usado como reserva financeira, a bitcoin pode desvalorizar muito e inviabilizar você desconverter o seu patrimônio num momento futuro, por conta de situações como esta que não recomendo que se faça isso com porcentagens grandes do seu atual patrimônio (PRIMO, 2017).

A segurança da informação é uma grande aliada de empresas, pois é responsável por evitar que qualquer pessoa distribua, de forma indevida, dados sobre vendas, margem de lucro, concorrentes, entre outras. Em um mundo no qual diversas tarefas são realizadas ao mesmo tempo e e-mails confidenciais podem ser

enviados em apenas um clique, é fundamental que exista proteção para eventuais erros.

Nesses casos, a Segurança da Informação permite construir políticas e métodos que são empregados na circulação de dados confidenciais e são controlados pelo departamento de Tecnologia da Informação (TI) de uma empresa.

## 4. CRIPTOMOEDAS

O avanço tecnológico está a cada dia mais impactante na sociedade e em cada momento é possível descobrir algo novo a ser inventado, como por exemplo, a utilização de moedas digitais que facilita no investimento ou na compra de serviços e produtos, as chamadas criptomoedas.

Esse novo fenômeno que mexeu positivamente com o mercado financeiro está sendo usado a cada dia mais por empresas e por grandes investidores devida a sua volatilidade, ou seja, a moeda em alta valorização no dia a dia, e a não interferência política de qualquer país ou de órgãos investidores, bem como, o seu uso ser facilitado.

> Todo e qualquer tema que envolve as moedas virtuais são um tanto quanto subjetivos, não em questão à sua objetividade, mas sim à efetiva atuação e quais expectativas se criam ao redor deste locus econômico. As visões que pairam sobre as criptomoedas são das mais difusas, há quem acredite que elas são apenas “febre” e, também, há quem sustente a tese de que elas são o futuro do sistema monetário, duas visões que dividem espaços extremos dentro da economia. (LEUZINGER, 2022).

Além disso, a transferência extremante segura é outro fator que interessa diretamente na nossa monografia e será abordado ao longo desse trabalho, e também, sobre as consequências para aquele que investe e seus riscos ao adotar essa medida.

## 4.1. A ORIGEM DA CRIPTOMOEDA

Não há como definir um único inventor da criptomoedas, porém, aquele que mais se destacou foi o Satoshi Nakamoto, mesmo mantendo sua identidade preservada, foi o que ganhou maior visibilidade por criar a criptomoeda mais utilizada, a chamada Bitcoin.

> A grande sacada do Bitcoin, talvez uma de suas maiores vantagens, é que a moeda digital dispensa o intermediário, o “terceiro” na transação. É um sistema peer-to-peer. Não é necessário confiar em um banco que guardará seu dinheiro. Você tampouco precisa assegurar-se de que uma empresa de liquidação de pagamentos processará corretamente o seu pedido. Acima de tudo, você não precisa rezar para que um banco central não deprecie a moeda. (ULRICH 2014, p. 65)

Satoshi objetivava criar uma moeda bem mais moderna do que as existentes no mercado financeiro e em 2009 procedeu a invenção dessa com a visão de evitar o controle do Estado, permitindo que fosse utilizada de forma descentralizada sem depender da política ou de instituições financeiras para o seu uso e ainda, que houvesse ampla dificuldade em quebrar o segredo da chave.

> Mas para a valorização do bem produzido pela empresa, essas moedas serão criadas de forma que um dia terminem suas emissões, assim, para que ela possua mais valor ao longo do tempo, sendo assim uma moeda deflacionária (PASSOS, 2001).

A Bitcoin não foi a única criada, outras moedas foram desenvolvidas antes do ano de 2009, como no ano de 1983, foi produzida uma moeda anônima digital chamada ecash por David Chaum com a proteção criptografada. Nesse mesmo sentido, no ano de 1995, inventou outra moeda chamada digicash, que

diferentemente da anterior, permitia o compartilhamento para outras pessoas e ainda garantia o anonimato de seu proprietário.

Porém, ao longo do tempo e a partir de 2009, após o desenvolvimento de novos sistemas, que surgiram outras implementações e criações de diversas moedas digitais que possuem agora como base o blockchain que é a fonte principal para o funcionamento correto das criptomoedas.

Por conta da facilidade de criação e da grande procura de empresas e investidores não há como mensurar a quantidade de moedas existentes no mercado financeiro atualmente.

## 4.2 CONCEITO DE CRIPTOMOEDAS

A criptomoeda é a mais nova aposta para o mercado financeiro, pois consiste na utilização de dinheiro totalmente digital, sendo que não há o controle de qualquer país, órgão ou instituição financeira.

O objetivo de sua criação inicialmente era para facilitar a realização de pagamentos em blockchain, ou seja, transferência de uma pessoa para a outra sem a necessidade de um banco como intermediador, porém, com o seu constante uso foi possível adotar como meio de troca entre as pessoas, podendo comprar serviços e produtos por meio de moeda digital.

Outro mecanismo que pode ser adotado é o de investimentos, viabilizando ao investidor obter várias moedas digitais e efetuar maiores lucros, conforme o aumento do valor da moeda no mercado financeiro diariamente, o que chamou muito a atenção de grandes empresários.

> Considerando o atual arranjo monetário de moedas fiduciárias de papel, a maior parte da massa monetária é constituída de meros dígitos eletrônicos no ciberespaço, dígitos estes criados, controlados e monitorados pelo vasto sistema bancário sob a supervisão de um banco central. Dinheiro material ou físico é utilizado apenas em pequenas compras do dia a dia. O cerne do nosso sistema monetário já é digital e intangível. (ULRICH 2014, p. 63)

Desta forma, o grande pilar para o invento de uma moeda digital é o blockchain, como abordado acima, ele é essencial como fonte de todas as informações, considerado ainda, como livro contábil público, tendo nele armazenado todos os dados que forem passados entre os usuários e ainda tem a função primordial de impedir que aquele que obtenha o acesso possa modificar ou excluir dados já inclusos sem autorização do dono.

Além disso, cada criptomoeda gerada possui um valor particular e há sim a possibilidade de conversão da moeda, exceto para moeda física, como por exemplo, o dólar ou os reais transferidos ao cartão de crédito ou outra conta bancária. Vale destacar ainda, que não serão aplicadas a todos os casos, a regra é que ocorra a troca por meio de por produtos ou serviços de determinada empresa e a exceção é a conversão para real ou dólar.

## 4.3 AS CRIPTOMOEDAS MAIS UTILIZADAS

Existem atualmente dezenas de tipos de criptomoedas, devido a sua facilidade em desenvolvimento na implantação e na aprovação de alguns sistemas para seu eficaz funcionamento financeiro.

Abaixo, traremos os tipos de criptomoedas mais utilizadas, tendo em vista que não há como mensurar ou abordar certamente a quantidade de moedas já existentes no mundo todo.

- BITCON (BTC)

Criada no ano de 2009, essa moeda foi desenvolvida 100% de forma digital e até hoje é a mais procurada e usada no mundo todo por sua troca ser realizada de forma descentralizada e tem seu incentivo de utilização pelos países como Japão e
Austrália.

> Um ponto comum nos atributos avançados do Bitcoin é a reduzida necessidade de confiança no fator humano, a confiança é substituída por comprovação matemática. É a criptografia moderna garantindo a solidez da moeda (ŠURDA, 2012).

Para que possa ser adquirida, o usuário deverá criar uma carteira digital no site oficial chamado blockchain e assim a moeda será armazenada livre de impostos ou de taxas. Além disso, a pessoa que deseja adquirir essa modalidade de criptomoeda deve realizar uma transação comercial para possuir mais moedas possibilitando a troca em produtos ou serviços.

Figura 2 Bitcoin

Fonte:https://www.mulherbela.com.br/moeda-bitcoin-fisica-banhada-a-ouro-colecionavel.

- BITCOIN CASH

Apesar de possuir o mesmo nome que a primeira inventada, Bitcoin, elas possuem suas diferenças, não podendo ser comparada no seu desenvolvimento e na sua segurança.

Essa modalidade foi criada em 2017, com o intuito de ser uma versão mais atualizada, moderna e de substituir a original por possuir blocos de transações maiores chegando-se a 1,4 megabyte.

Figura 3 Bitcoin Cash

Fonte: https://www.pngwing.com/pt/free-png-nchuy

- ETHEREUM (ETHER)

Criada em 2013, essa moeda facilita seu uso por realizar contratos inteligentes e efetuar aplicações de forma descentralizada e isso a faz ser diferenciada da Bitcoin. Muitos especialistas consideram que essa espécie é uma evolução tecnologia apresentada na blockchain com maior capitalização no mercado financeiro, ficando apenas atrás da Bitcoin.

> Ethereum é uma plataforma de Blockchain descentralizada, de código aberto, que permite qualquer pessoa a criar e usar aplicações descentralizadas que utilizem a tecnologia Blockchain. Não possui um dono ou controlador e contou com colaboradores de todos os cantos do mundo. Ao contrário do Bitcoin, o Blockchain do Ethereum foi estruturado para ser adaptável e flexível. (MIRANDA E SALVATORE 2018, p. 5).

Outro fator importante é que essa moeda atualmente é considerada a mais segura pela sua dificuldade na quebra de segurança para chegar a ter o acesso completo ao sistema, causando assim danos aos envolvidos.

Desta forma, com exemplo, pode ser utilizada essa criptomoeda para adquirir o poder computacional em computadores mundiais, bem como, pode ser utilizada como rede de apostas que não tenham necessariamente um dono.

Figura 4 Ethereum


Fonte:https://einvestidor.estadao.com.br/investimentos/dogecoin-a-criptomoeda-do-momento-e-imune-ao-criptocrash/

- DOGECOIN (DOGE)

Surgiu no ano de 2013 como um meme, uma brincadeira, e ganhou a atenção de grandes investidores por ter a característica de ultra volatilidade. Foi produzida após ter o código aberto da blockchain, o que permite que qualquer pessoa tenha acesso de forma gratuita, assim apresentada a diferencia com a Bitcoin.

Essa criptomoeda tem seu valor atribuído somente pelo tamanho da doação, ou seja, quanto mais interesse houver e maior for o investimento mais o seu valor irá subir.

Figura 5 Dogecoin


Fonte:https://einvestidor.estadao.com.br/investimentos/dogecoin-a-criptomoeda-do-momento-e-imune-ao-criptocrash/

- LITECOIN (LTC)

A Litecoin é uma criptomoeda criada no ano de 2011 por meio do mesmo código que a Bitcoin, porém, ainda assim, as duas apresentam suas particularidades. Na prática a Litecoin é também conhecida como a criptomoeda de prata, enquanto a Bitcoin é considerada a de ouro.

> O Litecoin jamais foi desenvolvido com a ideia de substituir a mineração dos bitcoins, e sim, organizar em conjunto a mineração de ambos. Assim como no bitcoin, o litecoin também passa pelo evento de halving – que consiste na divisão do valor do prêmio de mineração pela metade - a cada quatro anos, aproximadamente. O algoritmo que é utilizado pelo Litecoin no estabelecimento do

> processo matemático de mineração é o Scrypt – algoritmo de mineração que garante a criptografia e segurança da moeda. (PERCIVAL, 2009).

Foi criada com a finalidade de facilitar nas realizações de pagamentos possuindo atuação de forma descentralizada e de não ter nenhum ponto de falha por ser considerada a quarta moeda mais segura no mundo da internet.
Uma de suas diferenças com a Bitcoin está na velocidade das transações sendo a Litecoin mais rápida, 2,4 minutos comparada com aquela e mais fácil para ser adquirida.

Figura 6 Litecoin


Fonte:https://www.toyshow.com.br/presentes-e-decoracao-geek/moeda-decorativa-litecoin-ltc-trader-criptomoedas-evali

- CARDANO

É considerada como a terceira geração das criptomoedas já inventadas e sua sistematização é a mesma utilizada na Bitcoin, ou seja, o blockchain nas transações. O objetivo de sua criação foi para ajudar os países que não tem facilidade de acesso aos bancos o que dificulta na realização de transações.

Outro ponto muito importante é a metodologia utilizada por essa criptomoeda, ela é totalmente baseada por códigos criados por cientistas, engenheiros e desenvolvedores o que torna por si só uma barreira a mais de segurança.

Figura 7 Cardano


Figura 8Fonte: https://moneyinvest.com.br/criptomoeda-cardano-ada-vira-sucesso-apos-aumento-de-50-no-fim-de-semana/

- POLKADOT (DOT)

É a mais recente criação Asiática no meio das criptomoedas, sendo oficialmente lançada em 2020. Possui a capacidade de reunir vários blockchain para atingir uma segurança extrema na utilização de redes ou no acréscimo de novas cadeias dentro do mesmo bloco.

As conexões múltiplas com os demais blocos facilitam e aumentam o número de transações possíveis por essa moeda, ainda, permite que tenha um token próprio e outros benefícios a mais para aqueles que desejam adquirir.

Figura 9 Polkadot

Fonte:https://br.freepik.com/vetores-premium/moeda-de-ouro-polkadot-dot-conceito-de-token-de-criptomoeda-troca-de-dinheiro-digital_22852990.htm

Para ilustrar o que foi abordado nesse tópico do trabalho, observaremos o gráfico que demonstra de forma explicava as criptomoedas mais utilizadas no ano de 2022 entre o mês de janeiro até março do mesmo ano e seus respectivos valores.

Figura 10 – Moedas mais utilizadas em 2022 (janeiro – março)

Principais criptomoedas »

Adicione ao seu site »

| Nome | Código | Preço (USD) | Capitalização | Vol. (24h) | Vol. Total | Var (24h) | Var (7d) |
|---|---|---|---|---|---|---|---|
| Bitcoin | BTC | 48.741,1 | $919,37B | $30,16B | 31,55% | +6,28% | +3,43% |
| Ethereum | ETH | 4.029,68 | $477,59B | $20,29B | 21,23% | +6,87% | +6,05% |
| Binance Coin | BNB | 531,91 | $88,60B | $1,58B | 1,65% | +4,09% | +1,01% |
| Tether | USDT | 1,0004 | $76,22B | $64,95B | 67,94% | -0,01% | -0,07% |
| Solana | SOL | 180,000 | $55,47B | $2,10B | 2,20% | +4,69% | +16,35% |
| Cardano | ADA | 1,2657 | $43,17B | $1,26B | 1,32% | +4,33% | +3,03% |
| USD Coin | USDC | 0,9995 | $42,29B | $4,22B | 4,41% | -0,02% | -0,17% |
| XRP | XRP | 0,89131 | $41,82B | $3,95B | 4,14% | +5,36% | +12,97% |
| Terra | LUNA | 82,9035 | $30,68B | $3,53B | 3,69% | +9,28% | +46,10% |
| Avalanche | AVAX | 118,77 | $28,76B | $2,31B | 2,42% | +15,11% | +48,76% |

Fonte Disponível em: <https://www.idinheiro.com.br/como-ganhar-dinheiro-comcriptomoedas/ > Acesso em: 15.04.2022.

## 5.BLOCKCHAIN: O SISTEMA DE TECNOLOGIA POR TRÁS DA CRIPTOMOEDA

O chamado blockchain que já citamos ao decorrer da monografia é o sistema que garante a segurança e a eficácia na utilização das criptomoedas. Antes de adentrarmos na explicação desse sistema temos que deixar claro a existência da diferença entre o Bitcoin e do Blockchain, ou seja, por mais que suas histórias deram início no mesmo instante e suas origens sejam coincidentes eles possuem funções e finalidades diferentes.

O blockchain é uma programação existente que possui combinações algorítmicas que permite a gravação de dados transferidos de uma pessoa a outra, enquanto o Bitcoin foi a primeira moeda que após ser objeto de invenção digital apresentou a possibilidade de utilização no meio digital. Portanto, o que dá base para a funcionalidade do bitcoin é o blockchain assim, ambos estão interligados.

> O Blockchain é uma plataforma de banco de dados distribuído, ou seja, uma maneira de armazenar de forma imutável dados digitais para que possam ser compartilhados de forma segura entre redes e usuários. Como uma rede peer-to-peer, combinada com um servidor de data-stamping distribuído, os bancos de dados Blockchain podem ser gerenciados de forma autônoma. Não há necessidade de um administrador – os usuários são os administradores. (CIO, 2017).

Assim, a sistematização do blockchain é o que dá base de segurança nas transações entre as pessoas e permite com que não haja necessidade de ter um terceiro nas relações para a conclusão do processo, como por exemplo, fiscalização de um banco, instituições ou órgãos financeiros.

Se pudéssemos enxergar ou ter uma noção da aparência dessa rede, veríamos um formato que aparente com uma corrente ou uma cadeia sendo entrelaçado um bloco ao outro conforme explica o autor Marco Agner (2018):

O que ocorre é que cada bloco tem um identificador único que é criado a partir do hash de seu cabeçalho que serve tanto como identificador único deste objeto na rede quanto como prova de toda informação incluindo as transações contida nele.

> Esta característica faz com que a blockchain possa ser visualizada como uma corrente de blocos com os hashes do bloco anterior como elo criptográfico entre cada bloco: (citação p. 74, MARCO AGNER).

Uma outra definição de forma explicativa, pelo autor Peter Kent (2021):

Blockchain são tipos de bancos de dados. Um banco de dados é apenas uma coleção de dados estruturados. Digamos que você junte um punhado de nomes, endereços de ruas, de e-mail e números de telefone e os digite em um processador de textos. Isso não é um banco de dados, é apenas um amontado de textos. Mas digamos que você insira esses dados em uma planilha.

> O tempo de execução deste processo varia muito, atualmente demorando em média cerca de 30 minutos (BLOCKCHAIN, 2018). Uma vez que a transação é validada, o registro dessa transação é adicionado ao blockchain, que armazena o registro de todas as transações já feitas na rede Bitcoin. Nenhuma transação envolvendo bitcoins é registrada no blockchain sem antes passar pelo processo de mineração. (ANTONOPOULOS, 2014).

Desta forma, esses blocos são ligados por uma matemática combinada entre eles e por outros que ainda possam existir no futuro e ainda, assim que o bloco é criado junto com ele nasce um único identificador com o esforço computacional sendo resultado do proof-of-work (Blocos que são armazenadas as transações mais recentes dentro do bloco) sendo o principal responsável pelo elo criado e que dá sustentabilidade ao blockchain.

Após entendermos sobre como é criada essa cadeia que fortalece o blockchain falaremos o que se encontra por trás desses blocos que são os chamados mineradores que possui a função extremamente importante de compatibilizar os dados entre os usuários com os demais blocos a serem criados e que dá a efetiva utilização nas transações.

Os mineradores sempre estarão presentes nas moedas digitais independente de sua modalidade, tendo em vista que, ele é responsável por cruzar os dados para verificar a sua veracidade que são informados ente os usuários das transações e realizam esse “trabalho” por meio de criptografias.

Desta forma, o inventor das criptomoedas pensou em cada detalhe e aderiu ao produto (moeda digital) a segurança adequada, por meio do blockchain, para que não fosse possível e corriqueiro a prática de crimes, como por exemplo, o roubo das criptomoedas.

Portanto, todos os dados compartilhados ficam armazenados como uma forma de registro de informações compartilhadas e essa operação pode ser visualizada por todos os adquirentes das moedas, possibilitando o controle entre eles e garantindo a confiabilidade e o aumento de pessoas nas redes para realizarem seu uso de forma segura.

> A tecnologia Blockchain têm como principais propriedades a descentralização, uma vez que dispensa a necessidade de uma terceira parte para fazer a transação; a integridade, pois todos os conjuntos de dados são replicados em diferentes pontos da rede de maneira segura; e a transparência, visto que todas as transações registradas na blockchain são públicas. (SAMPAIO, et al., 2018).

Além disso, com o sistema de software do blockchain é vedada a alteração de dados sem a devida autorização exigida, e caso seja efetuada a alteração os

usuários que compartilham da mesma rede saberão através de uma notificação e deverão concordar ou não com o que lhe é apresentado.

Por isso, se faz necessário a duplicação de blockchain em diversos computadores tendo como benefícios a dificuldade de haver o hacker ou a manipulação dos dados.

Agora entraremos na parte mais técnica de toda essa sistematização.Dentro desse sistema é importante existir um hash que vale como um número geralmente comprido, não pode ser curto, que é considerado uma impressão para dados, ou seja, cada número criado será um dado dentro do bloco.

> [...] O protocolo PoW envolve escanear um valor utilizando a função hash5 , como a função SHA-256, onde o hash começa com n bits 0. O trabalho médio requerido é exponencial ao número de bits 0 e podem ser verificados utilizando um único hash. (NAKAMOTO, 2008, p.3).

Os atos são sequenciados da seguinte forma:

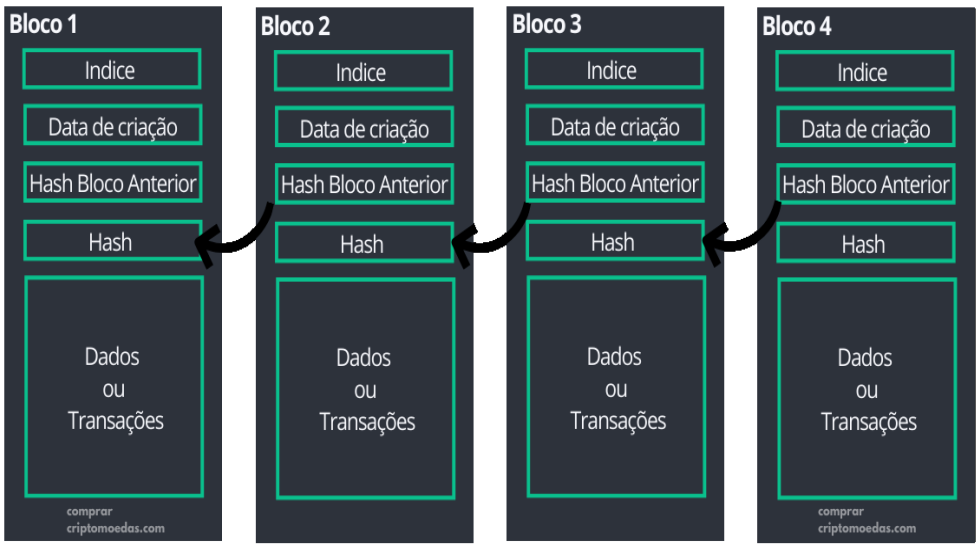
1. O computador coleta e valida todas as transações realizadas pelo usuário e adicionam as referidas informações ao blockchain;
2. Após realizar a coleta das informações necessárias é preciso criar um hash e para isso um bloco de dados deve ser criado passando por um algoritmo e posteriormente é devolvida essas informações. Não é possível haver repetição de números sendo que cada dado possuirá o seu em específico, como por exemplo, 000000000000000000297f87446dc8b8855ae4e2b35260dc4af61e1f5eec579Th.
Com isso, se houver a mudança de algum número ou letra será apontado pelos usuários a incompatibilidade dos dados originais com os de agora fornecidos;
3. A identificação é adicionada ao bloco das transações;
4. Bloco é devidamente adicionado ao blockchain;
5. Se houver a possibilidade de novas transações essas serão coletadas e adicionadas ao próximo bloco, não ao mesmo já existente, ou seja, um bloco adicional;
6. O hash deve estar completo com todas as operações que foram realizadas e assim poderá ser adicionado ao bloco atual;

7. Com a realização de adicionar um bloco ao outro o hash é novamente emitido e encaminhado ao bloco agora existente;

8. Esse procedimento é repetido quantas vezes forem necessárias e os blocos vão se interligando e formando cadeias com os dados do dia e da hora da transação.

De uma forma mais exemplificativa a imagem abaixo mostra como ocorre essa operação:

Figura 11 Blocos de hash para a criação da cadeia de dados nas transações




Fonte: https://comprarcriptomoedas.com/o-que-e-uma-blockchain/

> Todas as transações que ocorrem no Bitcoin são registradas em uma espécie de livro caixa público e distribuído chamado de Blockchain (corrente de blocos), o que nada mais é do que um grande banco de dados público, contendo o histórico de todas as transações relacionadas. (ULRICH, 2014).

Conforme demonstrado na imagem, cada bloco é dividido por um hash que são ligados pela impressão digital da anterior, ou seja, cada um possui uma numeração para então incluída dentro do blockchain, não sendo possível descartar adicionar mais blocos sem passar por esse processo. E outro ponto importante a ser destacado, o blockchain é imutável o que torna muito difícil sofrer alterações.

## 6.CRIPTOMOEDAS E A SEGURANÇA DA INFORMAÇÃO

A criptomoeda é o meio mais seguro para se investir ou realizar transações comerciais com moedas digitais no mercado financeiro virtual, e como apontado diversas vezes, o que garante a segurança na transmissão de dados e compartilhamento de informações é a chamada blockchain. O blockchain é um sistema criado como um caderno contábil e por isso é fonte de segurança de extremamente confiabilidade e difícil quebra por possuir o código complexo de ser alterado, o que é quase impossível.

> Para que os bitcoins sejam transferidos de forma segura, a rede Bitcoin utiliza a criptografia assimétrica. (NAKAMOTO, 2008). A diferença entre criptografia simétrica e assimétrica é que na simétrica os algoritmos simétricos de uma chave (um pedaço de informação que controla a operação de um algoritmo) são usados tanto para criptografar quanto para descriptografar, enquanto que na criptografia assimétrica há duas chaves, sendo uma a chave pública, para encriptar as mensagens, e a privada, para desencriptar. As chaves são completamente independentes uma das outras. (ANTONOPOULOS, 2014)

O sistema conta com criptografia de ponta a ponta, o que dificulta possíveis invasões e além disso, para que qualquer usuário consiga proceder na alteração de blocos ou dados já cadastrados, é necessário que todos os usuários conectados em seus computadores aprovem tal procedimento, não podendo ocorrer de forma arbitrária. Por isso, não há uma autoridade especifica responsável para acompanhar as transações, devendo ser observada por cada pessoa que compõe o grupo se todas as informações registradas e validades estão corretas.

Esse tema possui relevância direta na segurança da informação tendo em vista que, deve ser garantia uma forma de confiabilidade de dados e de informações do investidor, e além disso, deve ser abordado o contrário esclarecendo a todos os investidores e a terceiros do que se trata a criptomoeda e qual sua funcionalidade e assim ser disponibilizada as devidas descrições e como serão resolvidas as possíveis dúvidas.

Outro ponto importante a ser abordado são as informações armazenadas e os possíveis riscos na realização do negócio que devem ser descritas na norma de segurança da criptomoeda.

O exemplo mais corriqueiro é o da primeira moeda como já abordado no decorrer do trabalho, Bitcoin, que será analisa abaixo.

Como garantia de segurança será utilizada e aplicada pela primeira norma a preservação da confidencialidade, disponibilidade, integridade, sigilo e autenticidade das informações, e posteriormente será orientado de forma clara ao investidor sobre seus ativos e a sua operabilidade das gestões no mercado. Desta forma, em seguida será assegurada a proteção de dados pessoais, o acesso será negado para aqueles que não possuírem a devida autorização e será evitado o vazamento de qualquer informação dada ao mercado. E por fim, serão definidos os procedimentos específicos e a gestão de riscos que podem vir a ocorrer.

> O princípio central do Bitcoin é a descentralização, e isto tem suas implicações na segurança. Em um modelo centralizado, como um banco tradicional, a responsabilidade do sistema é do próprio banco, diferentemente de um sistema descentralizado como o Bitcoin, onde esta responsabilidade é de todos os usuários finais. (ANTONOPOULOS, 2014).

A norma acima exposta como exemplo é aplicada em uma determinada moeda existente no mercado, podendo as demais adotarem e incluírem outros requisitos de informação, dependendo de suas atividades exercidas.

Ainda, importante ressaltar que, não há hierarquia quanto a garantia de informação, ou seja, todos que possuem acesso, como funcionário, entidades internas ou externas devem ser dadas o mesmo direito de poder ter ciência de todo o conteúdo informativo referente aquilo que está sendo investido.

A proteção não é limitada, abrange também casos como os de dados que são excluídos, destruídos ou modificados sem a devida autorização, podendo também as empresas investidoras ou a alguma legislação específica vigente determinar prazo para a exposição dos dados necessários para se obter a criptomoedas.

O que deverá também ser garantido pela segurança da informação é o controle da rede de acesso, seja ela de internet ou qualquer outra pública, é obrigatório passarem pelo acesso de conexões – Firewall – que monitora as informações passadas, bem como, protege de possíveis ataques e de vírus, ou seja, deve ser devidamente criptografada.

Portanto, com a crescente utilização de criptomoedas no mundo, está surgindo a chamada Web 3.0 que tem como finalidade dar mais visibilidade e ser adotado como tendência a utilização de criptomoedas em aplicativos online.

Essa modalidade tem se mostrado como será a internet do futuro, possibilitando a criação de comunidades online onde permite que vários usuários façam parte e assim possam alimentar o blockchain (sistema que permite receber informações de envio na internet). Com isso, há facilidade no emprego das criptomoedas, assegurando seu uso de conteúdo digital de forma descentralizada e quanto mais dados digitais forem compartilhados mais valores entrarão para a comunidade.

## 7.COMO REFORÇAR A SEGURANÇA

São dadas diversas opções para os usuários das moedas digitais, podendo desta forma, reformar a segurança e dificultar ainda mais o vazamento de informações.

- **SEGURANÇA DA CARTEIRA**

A carteira de criptomoedas é utilizada normalmente por pessoas que querem se assegurar de qualquer possibilidade de roubo de suas moedas, devido ao tamanho de sua senha.

Desta forma, o melhor investimento atualmente se encontra na carteira digital administradas por corretoras de criptomoedas ou de qualquer empresa que atue nessa área.

> Uma carteira de hardware é um dispositivo físico eletrônico, desenvolvido com o propósito de proteger bitcoins. Para que os bitcoins destas carteiras possam ser gastos, eles precisam estar conectados ao computador,

> telefone ou tablete. Carteiras de hardware mantém as chaves privadas em um ambiente off-line, sendo desta maneira protegidas de malwares e cibercriminosos. Para ter acesso a carteira de hardware, seria necessário roubar a carteira em si. (TUWINER, 2018).

As carteiras são digitais, porém, seu acesso pode ser online ou como considerada por alguns, as chamadas carteiras físicas. Como por exemplo, tokens que podem fornecer o suporte ao seu proprietário para mais de 300 moedas e para adquirir esse serviço, é necessário o pagamento de uma taxa para as transações.

Nesse mesmo sentido, outra modalidade de carteira a ser adotada é chamada de hardware wallet, com o objetivo de armazenar as criptomoedas e transferir para as corretoras apenas quando o interessado quiser negociar, assim, será evitado os riscos de terem seus dados expostos por muito tempo e só possuirá acesso aqueles que o proprietário desejar, tanto que é a considerada mais segura de todas as modalidades. Além disso, se caso o aparelho for perdido as suas criptomoedas continuaram seguras e poderão ser tranquilamente recuperadas através das palavras-chave de segurança.

Existem também as criptomoedas disponibilizadas para aparelho móvel, utilizada por colecionadores de moedas e possui ainda zero taxa para a sua transferência. Sua segurança é extrema por exigir dois fatores otimizados.

E para finalizar, ainda existe a modalidade menos utilizada que é a criptomoeda de papel, tendo em vista que papel é um objeto que com o tempo se deteriora e como para ter acesso a suas moedas é necessário a leitura dos dois QR Code, pode se tornar impossibilitada por esse fator.

- **PROTEÇÃO DE PATRIMÔNIO**

A finalidade de escolher-se a modalidade de criptomoeda correta é uma segurança a mais dentro do patrimônio do investidor ou do empresário, tendo em vista que há possibilidades de sofrer com os diversos impactos da mutabilidade do valor da criptomoeda investida e isso poderia ser evitado com a referida proteção. Assim seria mais seguro e a variedade de preços conforme estabelecido em lei da

oferta e da demanda possibilitaria a compra de moedas diversificadas sem qualquer risco.

Essa espécie de acréscimo na segurança vem crescendo atualmente na sociedade, pela sua confiabilidade e pela aposta que tem feito os grandes investidores pela opção de “trabalho” com a moeda digital.

No Brasil aplica-se mais o uso no Bitcoin, por ser considerada uma moeda completa e a mais segura já inventada, diferentemente dos países como a Rússia e a Ucrânia que adotaram na prática a proteção ao patrimônio como regra.

## 8.REGULAMENTAÇÕES BRASILEIRAS

Com a nova revolução da economia e a mudança no mercado financeiro em todo o mundo, foi perceptível a necessidade da criação de uma regulamentação como mais uma vez, forma de segurança para todos na sociedade.

> No Brasil, não há nenhuma lei especifica sobre moedas virtuais. Porém, há um projeto de lei de 2015 (PL[7] 2303/2015) do deputado Aureo, que defende a regulamentação das criptomoedas. O projeto está, atualmente, sendo avaliado por uma comissão especial. (R7, 2017)

O que fez as pessoas ficarem com mais inseguranças foram as crescentes ondas de crimes de lavagem de dinheiro, financiamento ao terrorismo e demais regras tributárias que não eram existentes para as criptomoedas.

Com isso, no Brasil surgiu a criação de diversos projetos de lei que regulamentam a criptomoeda e que de forma direta traz aos seus interessados a segurança não apenas virtual, mas também, a física por meio de leis, como por exemplo, PL 2.303/15, PL 2.060/10 e PL 3.825/19. Vale destacar que, são ainda projetos de lei propostos para votação, não está em vigência ainda.

## 9.NOVA MODALIDADE DE INTERNET

Com a evolução tecnológica de informações e de segurança para os dados das pessoas, surgiu recentemente a possibilidade da criação de uma nova internet mundial, a chamada Web 3 ou Web 3.0, com a base principal que é utilizada corriqueiramente nas criptomoedas, ou seja, traz essa relevância para o mercado financeiro e implementa novos protocolos de uso.

Foi visado essa necessidade da criação de uma internet mais moderna mundialmente por ser a atual, que estamos todos acostumados a utilizar, guiada pelo código do blockchain, diferentemente como ocorre com a Web 3 que permite aos seus usuários fazerem uso de suas criptomoedas de forma anônima e descentralizada no compartilhamento de dados, o que não é possível nos tempos de hoje.

O anonimato será altamente baseado pela criptografia já existente, mas agora de forma mais segura possuindo uma corrente de blocos e mais restrita sendo que cada um será responsável pela criação da “chave” do seu próprio conteúdo, tudo isso ocorrerá por meio de seu registro, sem que terceiros consigam captar alguma informação ou algo que a pessoa está querendo dizer.

O que será alterado na prática é não haver mais a necessidade de uma corretora para intermediar as relações, realizando as transferências e a administração das criptomoedas. Desta forma, possibilita que o proprietário negocie seus ativos com qualquer pessoa, bem como, poderá se beneficiar de aplicações e negócios também.

Portanto, podemos afirmar que essa nova invenção é de segurança resistente e veio como solução para ataques ou futuros roubos que podem ocorrer.

## VANTAGENS E DESVANTAGENS DE UTILIZAR A CRIPTOMOEDA

Como já abordado acima, a criptomoeda é a mais nova invenção e aposta do mercado financeiro no mundo todo e pode futuramente ser a única forma de se utilizar dinheiro sendo descartado o papel. Nesse tópico iremos abordar as vantagens e as desvantagens sobre se adquirir as criptomoedas.

Inicialmente iremos abordar sobre as vantagens:

**VANTAGENS:**

- **Controle total sobre os ativos**: por ter sua característica principal da descentralização, a criptomoeda permite que todos tenham acesso a sua compra e seu armazenamento, bem como, que efetue transferências sem haver interferência política ou econômica;
- **Alta liquidez**: devido ao seu alto consumo e a possibilidade de elevada rentabilidade, essa é uma das vantagens que mais tem atraído empresas e investidores. Se utilizadas e investidas de forma correta o retorno ao proprietário será de lucros maiores ao imaginado;
- **Inclusão financeira**: atualmente há possibilidade de alguns lugares do mundo aceitarem que as comprar e os pagamentos sejam realizados por meio de criptomoedas, o que possibilita o acesso para todas as pessoas e em qualquer parte do mundo.
- **Diversificação das moedas**: A sua diversificação na carteira de investimentos tem sido o ponto chave para os investidores tomar a decisão de adquiri-las. Atualmente existem milhares de espécies de criptomoedas que podem ser escolhidas pelos usuários, porém, deve-se estar atendo as suas particularidades e funções de uma para com a outra.
- **Estabilidade**: para que a moeda possa ser lançada no mercado financeiro e para a sua circulação, deve sempre estar atrelada a algum tipo de ativo. A mais comum delas é o dólar, sendo sempre negociadas respeitando o seu valor atual.
- **Longo prazo**: o investimento em criptomoedas se tornar uma boa opção a longo prazo, devido ao desenvolvimento de novas plataformas com o passar do tempo e outro ponto importante é o valor que essas moedas vão adquirindo ao após ano. Os lucros vão chegando na medida que vai sendo investido e nem sempre é possível obter essa visão e conclusão em um primeiro momento.

Portanto, como já abordamos os pontos positivos e as vantagens de se adquirir uma criptomoeda, trataremos a seguir sobre as desvantagens e os riscos que essa prática pode levar.

**DESVANTAGENS:**

- **Alta volatilidade**: se torna uma desvantagem para o investidor por ter estabilidade no valor de sua moeda investida, em um mês ela pode estar gerando muitos lucros, como pode no mês seguinte estar dando prejuízo por conta da variedade de preços existentes dentro do mercado financeiro.
- **Golpes e fraudes**: conforme dados apresentados no site, Finance One, as fraudes com criptomoedas ocorrer de forma corriqueira e aumentam de ano a ano. No ano de 2020, US$ 2,99 bilhões foram desviados representando um crescimento de 40,7% se comparado ao ano anterior. Ainda, detalhou que é previsto que esse crime cresça em 41% ao ano.

O BITCOIN é a moeda mais desejada por todos e por isso se torna um alvo para a prática de fraudes e golpes entre os criminosos, permanecendo em segundo lugar a ETHEREUM. Por isso na hora de realizar comprar de produtos ou serviços e até mesmo para se investir deve ser analisado os riscos que as moedas trazem e se a segurança fornecida é realmente eficaz para que se sinto protegido e confiante com o negócio a ser realizado.

- Falta de regulamentação dos governos: No Brasil atualmente não existe uma norma jurídica que regule as transações e como será celebrado o negócio jurídico entre as partes, o que ocasiona uma insegurança em relação ao que está sendo investido e a como será o seu retorno.

Outro ponto que merece atenção, é o fato das criptomoedas serem totalmente descentralizadas e privadas, ou seja, há como o usuário negociar de forma sempre anônima com as outras pessoas não sendo capaz de ser apresentado um histórico para saber se a pessoa que deseja realizar a transação tem alta aceitação nas empresas e nos sites onde concluiu o negócio, sendo assim, difícil a sua comprovação de credibilidade.

A solução que poderá ser criada para que os investidores se sintam mais “seguros” e que consequentemente não lhe cause mais danos é investir apenas na quantidade que se sentir confortável e dificultar escolhendo a moeda mais segura os riscos de fraude e de golpes que podem ser aplicados.

O ideal seria todo empresário ou investidor expor apenas 5% da sua quantidade de moedas.

Por fim, importante salientar que não é apenas os crimes de fraude e golpes que estão sujeitos a quem deseja celebrar o negócio, mas sim, o anonimato do usuário pode facilitar e financiar os crimes de terrorismo internacional, tráfico de armas e até o tráfico de drogas.

## CONSIDERAÇÕES FINAIS

O estudo para e a realização dessa monografia proporcionou nos um entendimento mais abrangente com relação às moedas digitais e o seu funcionamento no mercado financeiro.

Com essa análise foi possível verificar a importância da segurança da informação em suas transações financeiras, nesses casos quando tratamos de criptomoedas, tendo em vista que, além do sistema blockchain ter a função de armazenar os dados se faz necessário a presença constante da criptografia como proteção que impossibilita que invasores possam conseguir obter o acesso aos dados e assim utilizá-los como quiser.

Além disso, por mais que haja sistemas e proteções que impedem as fraudes e os golpes, deve ser prezado a boa-fé de cada pessoa e sua transparência nas ofertas apresentadas daquele que disponibiliza compra de produtos e serviços ou naquele que realiza a transferência das moedas para outros usuários.

Por fim, abordamos os riscos de se adquirir a criptomoeda, e infelizmente quanto mais for consumido pelo mercado financeiro e adepto a sociedade ma ior será os seus riscos de fraudes e golpes, não sendo possível reduzir esse número a zero, tanto que a moeda mais utilizada a BITCOIN atualmente é a mais visada e a que mais se utilizam para aplicar golpes.

Mas temos como premissa que com o avanço da tecnologia os riscos tendem a ser reduzidos gradativamente e a segurança aumentada consequentemente, graças ao constante investimento em pesquisa na área de segurança e as graduações especificas em segurança da informação, tal que agora concluímos na Fatec Americana.

## REFERÊNCIAS


ALAGAR. Porque o Blockchain impactará no futuro dos pagamentos. Alagar, 2021. Disponível em: https://algartech.com/pt/blog/por-que-o-blockchainimpactara-no-futuro-dos-pagamentos/#:~:text=Blockchain%3A%20o%20futuro%20dos%20pagamentos%20di gitais&text=O%20Blockchain%20permite%20que%20duas,garantir%20a%20legitimi dade%20do%20pagamento. Acesso em: 23 Mar. 2022;

ARANHA, Christian. Bitcoin blockchain e muito dinheiro, uma nova chance para o mundo. 2ª ed. Rio de Janeiro: Valentina, 2020. Disponível em: https://forumturbo.org/wp-content/uploads/wpforo/attachments/73677/6924-2020Bitcoin-Blockchain-e-muito-dinheiro-by-Christian-Aranha-z-lib-org.pdf. Acesso em:
15. Abr. 2022;

ALVEZ, Paulo. Dogecoin: o que é e como funciona a criptomoeda. Techtudo, 2021. Disponível em: https://www.techtudo.com.br/listas/2021/07/dogecoin-o-que-ee-como-funciona-a-criptomoeda.ghtml. Acesso em: 20 Mar. 2022;

ANTONOPOULOS, M. Andreas. Mastering Bitcoin. 1° Edição. Sebastopol: O'Reilly Media, Inc. 2014;

AGNER, Marco. Bitcoin para Programadores. Instituto de Tecnologia & Sociedade do Rio, 2018. Disponível em: https://itsrio.org/wp-content/uploads/2018/06/bitcoinpara-programadores.pdf. Acesso em: 15. Abr. 2022;

Brasil Econômico (Org.). Bitcoin: 3 formas de utilizar a criptomoeda de forma inteligente. IG, 03 out 2017. Disponível em:. Acesso em: 10 out. 2022;

CAMPOS, Roberto. Criptomoedas: quem inventou e como surgiu? XPEED, 2021. Disponível em: https://xpeedschool.com.br/blog/criptomoedas-quem-inventoue-como-surgiu/ Acesso em: 23 Mar. 2022;

CABRAL, Carlos: trilhas em segurança da informação caminhos e ideias para a proteção de dados. Brasport, 2015. Disponível em; https://www.google.com.br/books/edition/Trilhas_em_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o/CeInBgAAQBAJ?hl=en&gbpv=1&dq=seguran%C3%A7a+da+informa%C3%A7%C3%A3o&printsec=frontcover. Acesso em 21 Maio de 2022;

CUNHA, Marcelo Carneiro. Uma história sobre hackers e a internet e sobre várias outras coisas também. Galera Record, 2011. Disponível em: https://www.google.com.br/books/edition/Super/6jCYypMVgb0C?hl=en&gbpv=1&dq=hist%C3%B3ria+da+internet&printsec=frontcover. Acesso em Maio de 2022.

Coinbase. Preço de Polkadot. Coinbase. Disponível em: https://www.coinbase.com/pt/price/polkadot. Acesso em: 15 Abr. 2022;

Foxbit. O que é Ethereum. Foxbit. Disponível em: https://foxbit.com.br/o-que-e-ethereum/. Acesso em: 24 Mar. 2022;

Foxbit. O que é Litecoin? Foxbit. Disponível em: https://foxbit.com.br/o-que-e-litecoin/. Acesso em: 25 Mar. 2022;

GZH Economia. O que é e como funciona a mineração de criptomoedas. GZH Economia,2022.Disponívelem:https://gauchazh.clicrbs.com.br/economia/noticia/2022/02/o-que-e-e-como-funcionaa-mineracao-de-criptomoedas-ckzpz7ce20067015ph5f6mi0d.html#:~:text=Para%20fazer%20a%20minera%C3%A7%C3%A3o%2C%20as,todas%20as%20informa%C3%A7%C3%B5es%20sobre%20t ransa%C3%A7%C3%B5es. Acesso em: 15. abr. 2022;

GUIMARÃES, Pedro. Carteira de criptomoedas: o que é e como funciona? iSardinha Então vamos lá, 2021. Disponível em: https://investidorsardinha.r7.com/aprender/carteira-de-criptomoedas/#:~:text=A%20diferen%C3%A7a%20na%20carteira%20de%20criptom oedas%20est%C3%A1%20no%20tamanho%20da%20senha.&text=Basicamente%2 C%20a%20chave%20privada%20%C3%A9,a%20seus%20fundos%20de%20criptos
Acesso em: 01. Abr. 2022;

HOLANDA, Letícia. Web 3: conheça a internet do futuro inspirada pelas criptomoedas. Metrópoles, 2022. Disponível em: https://www.metropoles.com/brasil/ciencia-e-tecnologia-br/web3-conheca-a-internetdo-futuro-inspirada-pelas-criptomoedas. Acesso em: 30 Mar. 2022;

HOLANDA, Letícia. Web 3: conheça a internet do futuro inspirada pelas criptomoedas. Metrópoles, 2022. Disponível em: https://www.metropoles.com/brasil/ciencia-e-tecnologia-br/web3-conheca-a-internet%20do-futuro-inspirada-pelas-criptomoedas. Acesso em: 30 Março. 2022;

InfoMoney. Criptomoedas: Um guia para dar aos primeiros passos com as moedas digitais. InfoMoney. Disponível em: https://www.infomoney.com.br/guias/criptomoedas/. Acesso em: 20 mar. 2022;

InfoMoney. Guia sobre Bitcoin: conheça a origem da primeira criptomoeda do mundo. InfoMoney. Disponível em: https://www.infomoney.com.br/guias/o-que-e-bitcoin/. Acesso em: 30 mar. 2022;

INVESTIMENTOS, Toro. Conheça as principais e mais valiosas criptomoedas do mercado. Blog Toro, 2022. Disponível em: https://blog.toroinvestimentos.com.br/principais-

criptomoedas#:~:text=As%20dez%20principais%20criptomoedas%20com,coment ad os%20do%20mercado%20financeiro%20atualmente. Acesso em: 30 Mar. 2022;

KENT, Peter; BAIN, Tyler. Mineração de Criptomoedas para Leigos. 2021. Disponível em:https://altabooks.com.br/wpcontent/uploads/2021/07/AMOSTRA_MineracaodeCriptomoedasPL.pdf. Acesso em:
15. Abr. 2022;

LEUZINGER, Bruno. Os Bitcoins são as novas "tulipas". Draft. 2018. Disponível em:. Acesso em: 10 out. 2022.

MASSADAR, Rafael. Dicas de como identificar fraudes com criptomoedas. FinanceOne, 2021. Disponível em: https://financeone.com.br/como-identificarfraudes-com-criptomoedas/. Acesso em: 30 Mar. 2022;

Mercado Bitcoin. O que é Bitcoin Cash? Vale a pena investir nessa cripto em 2022?. Mercado Bitcoin. Disponível: https://blog.mercadobitcoin.com.br/oque-e-bitcoin-cash. Acesso em: 15 abr. 2022;

Notícias ICEV, Instituto de Ensino Superior. Blockchain: explicando a tecnologia por trás das criptomoedas. ICEV Instituto de Ensino Superior. Disponível em: https://www.somosicev.com/blockchain-explicando-tecnologia-portras-das-criptomoedas/. Acesso em: 15. Abr. 2022;

NUNES, Melissa. Como ganhar dinheiro com criptomoedas? 6 formas. iDinheiro, 2022. Disponível em? https://www.idinheiro.com.br/como-ganhar-dinheiro-comcriptomoedas/. Acesso em: 15. Abr. 2022;
PENA, Rodolfo F. Alves. Bitcoin. Uol, 2021. Disponível em: https://mundoeducacao.uol.com.br/geografia/bitcoin.htm. Acesso em: 23 Mar. 2022;

PERCIVAL, Colin. Stronger key derivation via sequential memory-hard functions. Disponível em: Acesso em: 10 nov. 2022;

REDAÇÃO. Entenda agora como transformar Bitcoin em dinheiro de verdade. FinanceOne, 2022. Disponível em: https://financeone.com.br/como-transformarbitcoin-dinheiro/#:~:text=Existem%20v%C3%A1rias%20formas%20para%20transformar, eur os%20e%20qualquer%20outra%20moeda. Acesso em: 25 Mar. 2022;

RICO, Time. Criptomoedas: o que são, como funcionam e como investir? Riconnect, 2021. Disponível em: https://riconnect.rico.com.vc/blog/criptomoedas. Acesso em: 20 Mar. 2022;

SAMPAIO et al. (2018). Blockchain e a revolução do consenso sob demanda. Disponível em. Acesso em 10 de out de 2022;

SURDA, Peter. Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?. 2012. 93 p. Disponível em:. Acesso em: 10 nov. 2022;

SOUSA, Renato. Criptomoedas se destacam como defesa de patrimônio em países como Rússia e Ucrânia, mas brasileiros também devem pensar em Bitcoin (BTC), em ano de eleição, diz diretor do mercado Bitcoin. Seu Dinheiro;

SMULDERS, André; BAARS Hans. fundamentos de segurança da informação. Brasport, 2018. Disponível em: https://www.google.com.br/books/edition/Fundamentos_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3/1CVFDwAAQBAJ?hl=en&gbpv=1&dq=seguran%C3%A7a+da+informa%C3%A7%C3%A3o&printsec=frontcover. Acesso em 21 Maio de 2022;

TUWINER, Jordan. Tipos de Carteira. Disponível em. Acesso em 02 de novembro de 2018.

Time BL, Consultoria Digital. Regulação das Criptomoedas no Brasil e no Mundo. BL, Consultoria Digital. Disponível em: https://blconsultoriadigital.com.br/regulacao-das-criptomoedas/. Acesso em: 01. Abr.2022;

TEXEIRA FILHO, Sócrates Arantes; segurança da informação descomplicada. Brasília, 2015. Disponivel em: https://www.google.com.br/books/edition/Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_Descomplicada/iB5KEAAAQBAJ?hl=en&gbpv=1&dq=seguran%C3%A7a+da+informa%C3%A7%C3%A3o&printsec=frontcover. Acesso em: 21 Maio de 2022.

ULRICH, Fernando. Bitcoin: a moeda na era digital. 1. ed. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.