BLOCKCHAIN E OS MEIOS DE PAGAMENTO:

Um Estudo Sobre a Segurança e a Privacidade

Felipe Lopes Cruz
Faculdade de Tecnologia de Assis
felipe.cruz27@fatec.sp.gov.br

Igor Candela Reis
Faculdade de Tecnologia de Assis
igor.reis5@fatec.sp.gov.br

Cleber Henrique de Oliveira
Faculdade de Tecnologia de Assis
cleber.oliveira16@fatec.sp.gov.br

RESUMO

As negociações acompanham a sociedade há muito tempo, impulsionando a oferta de produtos e serviços. Com isso, surgiram variados meios de pagamento: das cédulas e moedas aos cartões e aplicativos digitais. Embora protegidos, esses sistemas não são invioláveis, expondo dados pessoais e valores a riscos. Casos de falhas de segurança e fraudes comprometem a confiança da população, gerando a busca por alternativas mais seguras e privativas. As criptomoedas surgem como opção de transação direta e anônima, baseadas em blockchains — estruturas tecnológicas que registram e validam operações de forma criptografada e descentralizada. Como o conhecimento popular sobre finanças digitais ainda é limitado, o tema requer estudo. Este trabalho, fundamentado em pesquisas bibliográficas de artigos validados, sites relevantes e orientações especializadas, investiga a segurança e a privacidade nas soluções financeiras, especialmente nas emergentes. Busca identificar vulnerabilidades, esclarecer aspectos pouco discutidos e reforçar a importância de sistemas financeiros confiáveis, promovendo o conhecimento e a confiança dos cidadãos.

Palavras-chave: Blockchain; criptomoedas; segurança; privacidade; meios de pagamento

ABSTRACT

Negotiations have accompanied society for a long time, driving the supply of products and services. As a result, various payment methods have emerged — from cash and coins to cards and digital applications. Although protected, these systems are not inviolable, exposing personal data and financial values to risks. Cases of security breaches and fraud undermine public trust, leading to the search for safer and more private alternatives. Cryptocurrencies emerge as an option for direct and anonymous transactions, based on blockchains — technological structures that record and validate operations in an encrypted and decentralized manner. Since public knowledge about digital finance is still limited, the topic requires further study. This work, based on bibliographic research from validated articles, relevant websites, and specialized guidance, investigates security and privacy in financial solutions, especially emerging ones. It seeks to identify vulnerabilities, clarify underexplored aspects, and reinforce the importance of reliable financial systems, promoting knowledge and public trust.

Keywords: Blockchain; cryptocurrencies; security; privacy; means of payment.

1 INTRODUÇÃO

Há muito tempo a sociedade tem se relacionado com alguns métodos de transações, desde a troca de bens ou tarefas, até os atuais meios que envolvem propriedades digitais. Com a expansão do acesso a produtos e serviços, o conceito de valor foi instaurado nos mais diversos suportes, que passaram a ser administrados com o desenvolver dos Estados. As nações emitem cédulas e moedas, as operadoras coordenam cartões de crédito e débito, já os desenvolvedores autorizados, criam aplicativos de pagamento. Atualmente, se aceito como remuneração, qualquer coisa é dinheiro (Nery; Costa, 2021).

Todos os meios habituais de pagamento apresentam recursos sofisticados de segurança e privacidade, mesmo assim, podem sofrer ataques mal-intencionados. A falsificação de dinheiro, clonagem de cartões e o roubo de dados de aplicativos bancários são alguns exemplos, dentre uma variedade de fraudes. Ações maliciosas são problemas que insultam a fé e comprometem a confiança da população. Induzem dúvidas, se certa movimentação é verídica e se as informações pessoais estão em sigilo (Alvares; Teixeira; Frango, 2021; Tatum; Santos, J. A. B. dos; Russo, 2016).

As criptomoedas representam um dos fatores impactantes ao ambiente financeiro, originalmente restrito aos meios de pagamento tradicionais. Surgiram como valores exclusivamente digitais, permitindo transferências de pessoa a pessoa e simplificando operações de compras e investimentos. São conhecidas pelos altos níveis de segurança e privacidade, utilizando algoritmos criptográficos e sistemas de chaves. Como um novo palpite para o mercado, essas moedas virtuais se baseiam em descentralização, ou seja, não estão relacionadas a moedas oficiais, governos ou instituições financeiras, mas sim uma estrutura de segurança própria (Silva; Goulart, 2022).

O blockchain é a estrutura de segurança utilizada pelas criptomoedas, um modelo de base de dados apresentado junto a Bitcoin — a moeda virtual mais famosa. Com uma enorme capacidade para transformar os mais diversos setores, funciona como um registro público, analisável, inalterável, distribuído entre participantes e sem servidor central, que armazena um histórico de todas as operações realizadas. Com fortes propriedades de privacidade e segurança, submete para validação todos os processos dos usuários, que sempre são criptografados. É um sistema robusto, que objetiva gerar a confiabilidade e englobar os princípios de integridade, confidencialidade e disponibilidade em seus serviços (Chicarino *et al*., 2017; Greve *et al*., 2018).

Os potenciais dos recursos citados incentivam diversas pesquisas. Os autores Alvares, Teixeira e Frango (2021) propuseram um trabalho acerca da utilização de um blockchain em

conjunto com os meios de pagamento, no qual informam: os desenvolvimentos e definições de ambos os recursos; as práticas mal-intencionadas recorrentes a tais meios; o roteiro de estudos; a proposta de integração, com protótipo e resultados. Os pesquisadores Chicarino *et al*. (2017) sugerem um estudo sobre o blockchain em combinação com dispositivos IoT, evidenciando: as explicações necessárias para um bom entendimento; as aplicações IoT; os princípios de segurança da informação; alguns aprofundamentos teóricos apropriados; a proposta relativa ao tema, com exemplos de uso.

O artigo proposto objetiva investigar os potenciais de segurança e privacidade das blockchains utilizadas para criptomoedas e, também, dos meios tradicionais de pagamento, verificando suas resistências a ameaças. Para tal, serão contextualizados os métodos financeiros comuns e emergentes, examinadas as explorações de suas fragilidades e será reforçada a necessidade por sistemas seguros.

Convém a esta pesquisa contribuir com a garantia da confiança populacional na área financeira, nos seus recursos protetivos, assim como aperfeiçoar os conhecimentos, comumente não minuciosos, acerca dos criptoativos, das maneiras usuais de pagamento e vulnerabilidades exploradas.

2 DESENVOLVIMENTO

Muitos elementos podem ser associados ao cotidiano das pessoas. Alguns desses, em virtude do desenvolver comercial da sociedade, estão integrados ao nível de serem indispensáveis. Os meios de pagamento são formas para remunerar os produtos obtidos e serviços contratados, sendo essenciais no saldar de alguma compra. Funcionam como objetos de troca, possuindo valor e alta variedade. Aqueles cujo uso é quase instintivo podem ser considerados tradicionais (Furini, 2020).

2.1 Meios tradicionais

Dentre os meios de pagamento existentes, há aqueles mais conhecidos. Sendo em razão da longevidade, disponibilidade, inovação, praticidade, segurança ou privacidade, as cédulas e moedas, os cartões e aplicativos de pagamento são métodos comumente incluídos nas atividades financeiras da população mundial.

2.1.1 Cédulas e moedas

As cédulas e moedas são, possivelmente, o meio mais tradicional de se realizar operações bancárias em toda a sociedade, consideradas a medida de valor oficial das nações. O dinheiro em espécie continua simplificando as transações cotidianas. É emitido pela entidade central de uma economia e distribuído ao povo, que será responsável por repassá-lo múltiplas vezes, atribuindo-o utilidade (Banco Central do Brasil, [s. d.]).

Os recursos de segurança são integrados fisicamente e variam, entre nações e gerações. As cédulas da segunda família do real, por exemplo, contêm número de série, marca-d'água, quebra-cabeça, fio de segurança, região que muda de cor, faixa holográfica, número escondido, microimpressões, elementos fluorescentes, áreas em alto-relevo, textura no papel, matérias-primas próprias e dimensões padronizadas. As moedas, da mesma família, incluem materiais específicos, impressões detalhadas, cortes precisos e tamanhos característicos (Banco Central do Brasil, [s. d.]).

2.1.2 Cartões

Os cartões representam um meio de pagamento popular e globalmente aceito, sendo os precursores da integração entre os ambientes monetários e tecnológicos. Fundamentam-se como uma inovação, em comparação ao dinheiro, trazendo uma maneira mais rápida, prática e conveniente de se realizar movimentações financeiras. Tais transações são mais indiretas, envolvendo entre o pagador e o beneficiário, o processador, emissor, adquirente e a bandeira. Com suas particularidades, os cartões marcaram a evolução dos sistemas de pagamento, continuando a crescer em abrangência e valores (Furini, 2020; Santos, A. C. dos, 2023).

O cenário dos cartões é comumente relacionado a recursos de segurança e exigência de dados. Um cartão: contém número, senha, validade, CVV e titular; exige de seu portador, ao ser solicitado, informações pessoais, como endereço e renda; utiliza métodos de autenticação, bloqueio e aprendizagem de máquina, analisando modelos comportamentais, de padrões, histórico, localizações. Tudo está sempre sob desenvolvimento contínuo, sendo afetado por ações preventivas, leis de proteção de dados e regras rígidas (Santos, A. C. dos, 2023).

2.1.3 Aplicativos de pagamento

Os aplicativos são o meio mais atual de movimentações financeiras. Difundidos globalmente, atuam como atalhos nas transações que normalmente envolvem dinheiro, cartões ou transferências bancárias, integrando os potenciais da tecnologia. Essas aplicações, com

dados devidamente cadastrados, podem emular uma operação de cartão, enviar e receber valores, entre outros. Tudo a partir da tela de um celular, por exemplo. É, seguramente, um avanço a favor da facilidade, mobilidade e do conforto (Alvares; Teixeira; Frango, 2021).

Os recursos de segurança desse meio também utilizam de uma junção do tradicional com o tecnológico, empregando autenticação — como a biométrica —, proteção da privacidade, tráfego e armazenamento seguros das informações — com criptografia —, sistemas de monitoramento de comportamentos, recursos de detecção de irregularidades, certificados digitais, tokenização, códigos de segurança, rastreabilidade, priorização e avaliação de riscos, regras concordantes as leis e exigências habituais de operações com contas bancárias (Ciso Advisor, 2023; Veroneze; Silveira, 2023).

2.2 Criptomoedas

As criptomoedas são uma nova tendência no âmbito financeiro, o dinheiro digital e seguro que facilita transações diretas pela internet. Tal meio de troca utiliza os avanços tecnológicos, impactando o mercado com métodos inovadores, resistentes, sigilosos, desburocratizados, financeiramente inclusivos e gerencialmente não concentrados de se manipular bens e quantias (Barbosa *et al*., 2022; Furini, 2020; Silva; Goulart, 2022).

Os autores Barbosa *et al*. (2022) e Silva e Goulart (2022) comentam acerca da história dos criptoativos, evidenciando que essa é mais profunda do que aparenta. Embora tenham se popularizado somente nos últimos anos, modelos desse tipo de moeda existem desde a década de 80, com diferentes implementações surgindo e desaparecendo de tempos em tempos. Exemplares como eCash e e-Gold antecederam aquele que marcaria a categoria, o Bitcoin. Sendo idealizado em 2008 e tendo as operações iniciadas em 2009, baseou o funcionamento e regulamento de toda a variedade de moedas virtuais atualmente existente.

Os estudos de Barbosa *et al*. (2022), Furini (2020) e Silva e Goulart (2022) apresentam os aspectos, no mínimo interessantes, do funcionamento das criptomoedas. Sobre movimentações financeiras, permitem pagamentos, transferências, investimentos, compras, vendas e acesso a produtos e serviços. Acerca da autonomia, eliminam intermediários — bancos, órgãos reguladores e Estados —, possibilitando aos usuários interações de pessoa a pessoa e gerenciamentos próprios. Quanto ao valor, regulam-se pela oferta e demanda do mercado externo, de maneira instável, deflacionam-se por limites máximos de emissão e não incluem impostos ou taxas. A respeito do sistema, operam majoritariamente em redes de código aberto chamadas de blockchain. Em relação a possíveis conversões para moedas oficiais, só se realizam por trocas entre partes ou mediante corretoras de criptomoedas.

Para gerir dinheiro é necessário confiança. Convenientemente, para aplicações ou negócios os ativos virtuais são reconhecidos em segurança e privacidade. As criptos utilizam criptografia, identificador único, duas chaves — pública e privada — e somente dados não pessoais. Seus utilizadores, meros caracteres em uma rede blockchain, podem armazená-las em carteiras completamente digitais, que exigem senhas para o acesso, ou em carteiras de hardware, que ainda requerem sua conexão física a um dispositivo (Barbosa *et al*., 2022; Furini, 2020; Silva; Goulart, 2022).

2.3 Blockchain

A blockchain é a estrutura na qual se operam a maioria das criptomoedas. Caracterizando uma inovação rompedora dos padrões tradicionais de ambientes financeiros, trata-se de programação, uma arquitetura de banco de dados descentralizada, distribuída, imodificável, criptografada, pessoa a pessoa, de código aberto, globalmente acessível e que utiliza seu próprio funcionamento para prover segurança e privacidade. O conceito atual das blockchains surgiu em conjunto com o criptoativo Bitcoin, quando Nakamoto (2008) propôs um sistema de transações eletrônicas que não necessitavam de confiança, empregando comprovações matemáticas (Chicarino *et al*., 2017; Greve *et al*., 2018; Silva; Goulart, 2022).

Uma blockchain não tem servidor central, funcionando através de replicação e compartilhamento nos dispositivos de seus participantes. Internamente, opera por meio do encadeamento de conjuntos de dados, agindo como um livro de contabilidade examinável nos âmbitos financeiros. As transações de criptomoedas são: assinadas pelo emissor, com sua chave privada; endereçadas ao receptor, com a identificação de sua carteira; publicadas aos demais partícipes; validadas por eles, verificando os fundos existentes e assinaturas necessárias; escolhidas e agrupadas em um bloco. O bloco é: finalizado, com sua conexão ao registro anterior da sequência e seu resumo criptográfico único sendo adicionados; divulgado aos outros usuários; aprovado por esses, examinando os dados incluídos; permanentemente integrado ao encadeamento. Bifurcações da corrente, decorrentes de blocos simultâneos, são resolvidas com o fluxo operacional adotando a maior cadeia. Adicionalmente, contratos inteligentes podem ser implementados em blockchains, permitindo a realização automática de conjuntos de instruções que podem servir para muitas funções diferentes (Buterin, 2013; Chicarino *et al*., 2017; Greve *et al*., 2018).

Os autores Chicarino *et al*. (2017) e Greve *et al*. (2018) destacam os envolvidos em uma rede blockchain, assim como suas funções. Os participantes possuem chaves privadas, públicas e endereços de carteira, que, respectivamente, comprovam suas identidades, atestam suas

ações e os identificam por meio de pseudônimos. Essas pessoas, denominadas nós, são autônomas e responsáveis pelo funcionamento constante e correto do sistema, dado que não existem intermediários ou administradores. Para garantir decisões comuns e progresso as operações, são utilizados variados mecanismos de consenso. A prova de trabalho, de posse e a tolerância a falhas bizantinas prática, modelos mais comumente encontrados, definem um líder entre os usuários através da resolução de desafios criptográficos, de probabilidades ponderadas pela quantia de criptomoedas possuídas e da sucessão ordenada, nessa ordem. A tarefa desse líder é publicar seu bloco aos demais, para que seja consensualmente validado e integrado a blockchain.

Os pesquisadores Chicarino *et al*. (2017) e Greve *et al*. (2018) também caracterizam uma blockchain pelas suas dimensões. Esse sistema pode ser empregado de maneira pública, com livre acesso a participação, ou permissiva/privada, com entrada controlada e autorizada, em tarefas de diversas áreas. Vinculada a segurança da informação, garante a imutabilidade dos dados armazenados — integridade —, privacidade ao conteúdo das transações — confidencialidade — e um servidor replicado sempre operante — disponibilidade.

3 METODOLOGIA

Baseado em ideias de caráter informativo e com possibilidades insuficientes a aplicações práticas, este estudo se realizou por meio de uma revisão bibliográfica. Com um planejamento efetivo feito no início, decidiu-se quais métodos de pagamento seriam abordados, quais ferramentas de apoio a pesquisa poderiam ser integradas e qual seria a sequência de atividades a cumprir.

Foram explorados, detalhadamente, os aspectos de segurança, privacidade e o funcionamento das cédulas e moedas, criptomoedas, blockchains, dos cartões e aplicativos bancários. Coletaram-se informações acerca das fragilidades de tais meios, assim como dos ataques que as exploram. Os dados eram interpretados, tratados e, através de documentos compartilhados em nuvem, documentados.

Todo o referencial teórico foi adquirido a partir de fontes seguras. Foram utilizadas publicações fundamentadas, como artigos científicos, acadêmicos e documentações disponibilizadas por órgãos financeiros. Empregaram-se bases de dados reconhecidas, como Google Scholar e servidores de universidades, além de sites de credibilidade. O uso de inteligência artificial ocorreu com o intuito de guiar e sugerir, não sendo exagerado.

Para a análise do material, aplicou-se a abordagem qualiquantitativa, uma série de discussões internas e orientação especializada, sempre visando identificar os pontos essenciais

ao trabalho. Como critério de seleção, a relevância temática e a pertinência ao escopo da investigação foram verificadas.

4 ANÁLISE DE RESULTADOS E DISCUSSÃO

Para verificar o desempenho verídico dos meios de pagamento, contextualizados de maneira teórica até então, convém a análise de algumas informações relevantes baseadas na realidade. Contrapondo certos exemplos de explorações de fragilidades aos mecanismos de segurança dos meios em questão, se torna perceptível que tais recursos não são infalíveis, mas significantemente robustos, funcionais e passíveis de melhorias contínuas.

4.1 - Meios tradicionais

Os métodos tradicionais apresentam vulnerabilidades de contexto correspondente — são aquelas mais comuns, conhecidas pelo público.

Sobre as cédulas e moedas incidem-se práticas como a falsificação. Simples indivíduos mal-intencionados, redes criminais ou associações criminosas, espalhados por todo o planeta, adquirem segredos industriais, capacitam-se em copiar e guiam oficinas clandestinas de contrafação. Utilizando de equipamentos cada vez mais modernos, como maquinários gráficos sofisticados, e da grande acessibilidade a mercados, conseguem forjar de maneira parcial o dinheiro físico e comercializá-lo até por serviços postais. Uma pesquisa recente do Banco Central do Brasil (2024) evidencia a presença de valores contrafeitos nas atividades de 46.9% e 36.4% dos comércios e da população estudados. Para dificultar ações ilegais ao meio ainda mais difundido de transações existem os elementos de segurança — número de série, marca-d'água, quebra-cabeça, fio de segurança, região que muda de cor, faixa holográfica, número escondido, microimpressões, elementos fluorescentes, áreas em alto-relevo, textura no papel, materiais específicos, dimensões padronizadas —, já citados e de difícil recriação, assim como o conhecimento do público acerca desses (Banco Central do Brasil, [s. d.]; Europol, 2025; Ramazzini, 2022).

No cenário dos cartões bancários, desenrolam-se casos de fraudes. De indivíduos atuando sozinhos a amplos grupos criminosos, fraudadores, de todas as partes do globo, utilizam as credenciais de terceiros para aquilo que desejarem, incluindo uso próprio e comercialização do material adquirido. Capacitando-se continuamente em inúmeras técnicas ilícitas, deturpam a conformidade do sistema de cartões através de: fraude de identidade, roubando os dados pessoais de titulares — nome, endereço, data de nascimento — e realizando operações financeiras em seus nomes; fraude interna, utilizando elementos de pagamento e identificação,

mantidos em empresas, para a prática de crimes; skimming, instalando ferramentas que capturam informações em terminais de pagamento; phishing, persuadindo os usuários a revelarem bases confidenciais — senhas, por exemplo; malware, infectando dispositivos com softwares maliciosos que obtêm fatos sigilosos — contas, palavras-passe — e/ou redirecionam a sites falsificados; carding, o englobado de todas as atividades fraudulentas do contexto. No geral, os golpistas ganham valores e propriedades, movimentam mais de 500 milhões de libras em um único ano, enquanto as vítimas e empresas emissoras nem ficam cientes de qualquer utilização fraudatória. Como os impactos pessoais, financeiros e reputacionais são negativos, medidas — informações únicas e individuais, dados pessoais, como endereço e renda, métodos de autenticação e bloqueio, machine learning, modelos comportamentais, de padrões, histórico e localizações, desenvolvimento contínuo, ações preventivas, leis de proteção de dados, regras rígidas —, citadas anteriormente, são adotadas por esse meio de pagamento, a fim de dificultar ações ilegais (APWG, 2025; Krebs, 2025; Santos, A. C. dos, 2023; Sulaiman; Schetinin; Sant, 2022).

O contexto dos aplicativos de pagamento é, de certa forma, semelhante ao dos cartões, mas com características mais digitais. Utilizando como meio de funcionamento os dispositivos móveis, que no Brasil existem em número maior do que habitantes, são altamente populares e funcionam como verdadeiras carteiras virtuais. Suas proximidades a dados pessoais, valores e maneiras rápidas de se movimentar grandes quantias atraem, novamente, indivíduos maliciosos, que buscam acessos indevidos e fraudes que os beneficiem. Dentre as estratégias usadas, alguns recentes métodos de golpes, novas ameaças, são: mudança de titularidade, em que o golpista, contactando a operadora, consegue a posse de certo número de telefone, para posteriormente receber as chaves de acesso a contas de aplicativos bancários; falso qrcode, no qual o malfeitor envia um código de resposta rápida para a vítima, que ao ser escaneado, envia-a para um site de phishing, que adquirirá seus dados, ou instala um malware em seu dispositivo; uso não autorizado de NFC, em que um infrator aproxima, discretamente, um aparelho, que contém um programa capaz de coletar dados de cartões, a um outro dispositivo móvel, da vítima, que contenha comunicação de campo próximo, clonando tais informações. As aplicações de pagamento, que utilizam ou não o Pix, empregam métodos — autenticação, proteção da privacidade, tráfego e armazenamento seguros das informações, sistemas de monitoramento de comportamentos, recursos de detecção de irregularidades, certificados digitais, tokenização, códigos de segurança, rastreabilidade, priorização e avaliação de riscos, regras concordantes as leis, exigências habituais de operações com contas bancárias —, anteriormente citados, para atenuar atividades desonestas (APWG, 2025; Ciso Advisor, 2023; Krebs, 2025; Veroneze; Silveira, 2023).

4.2 - Criptomoedas e blockchain

Como o panorama de funcionamento das blockchains, em qualquer tipo de utilidade, é um tanto mais técnico e algoritmicamente lógico, com instruções específicas e matemática envolvida, os métodos de explorações de fragilidades tiveram de se adaptar. Os ataques devem se focar em vulnerabilidades específicas do código ou da infraestrutura da implementação, se buscam ter uma chance de sucesso. Na realização do chamado “gasto duplo”, é explorada uma característica que não está presente em moedas físicas, a capacidade de serem utilizadas para mais de uma ação ao mesmo tempo. Um usuário desonesto pode realizar transações simultâneas a partir de uma mesma quantia de criptomoedas, para destinos diferentes. Se uma parte dos mineradores, responsáveis pela validação dos blocos, considerar uma das movimentações como válida, e outra parte julgar como verídica uma das outras transferências, a corrente se bifurcará, possibilitando que o indivíduo mal-intencionado receba algum retorno de ambos os destinatários de seu valor gasto único. Em um outro tipo de ataque, conhecido como “eclipse”, um nó honesto tem todas as suas conexões a rede monopolizadas pelo atacante. Manipulando o funcionamento das tabelas de endereços da vítima, um utilizador malicioso pode isolá-la, impedi-la de publicar blocos e forçá-la a trabalhar em sua cadeia. Os recursos de segurança das blockchains — auditabilidade, integridade, consenso distribuído entre usuários, imutabilidade, descentralização, criptografia, confidencialidade, entre outros — oferecem uma base sólida para proteger o sistema contra essas e outras ameaças (Chicarino et al., 2017; Greve et al., 2018).

5 CONSIDERAÇÕES FINAIS

A partir do conteúdo estudado, percebe-se que os elementos de segurança e privacidade dos meios de pagamento, tradicionais ou emergentes, são robustos e confiáveis. As cédulas utilizam recursos físicos que dificultam falsificações, os cartões e aplicativos de pagamento se apoiam em tecnologias mais avançadas, como criptografia e sistemas de monitoramento, prevenindo fraudes. Já as criptomoedas, e o sistema em que estão inseridas, blockchain, trazem uma nova forma de realizar movimentações financeiras, baseada em descentralização, transparência, auditabilidade e anonimidade.

Nenhum dos sistemas pode ser considerado totalmente imune a falhas. Golpes, fraudes e ataques virtuais ainda acontecem, indivíduos mal-intencionados buscam por vantagens indevidas, exigindo que as medidas de proteção continuem sendo aprimoradas. Ainda assim, é possível afirmar que os meios de pagamento atuais combinam responsabilidade com proteção dos dados. Percebe-se a evolução dos métodos financeiros como mais do que apenas

conveniência, e sim o esforço constante na busca por um sistema transparente e capaz de inspirar confiança nas pessoas.

6 REFERÊNCIAS

ALVARES, C. S.; TEIXEIRA, R. D.; FRANGO, I. **Privacidade e Segurança nos Meios de Pagamentos em Conjunto com Blockchain**. 2021. Trabalho de Conclusão de Curso (Curso Superior em Computação e Informática) – Faculdade de Computação e Informática, Universidade Presbiteriana Mackenzie, São Paulo, 2021. Disponível em: https://adelpha-api.mackenzie.br/server/api/core/bitstreams/c40f811e-6baa-4d5f-b370-1b3e2789d1d0/content. Acesso em: 26 maio 2025.

APWG. **Phishing Activity Trends Report**: 1st Quarter 2025. [*s. l.*]: APWG, 2025. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q1_2025.pdf. Acesso em: 9 nov. 2025.

BANCO CENTRAL DO BRASIL. **O Brasileiro e sua Relação com o Dinheiro**. [*s. l.*]: Banco Central do Brasil, 2024. Disponível em: https://www.bcb.gov.br/content/cedulasemoedas/pesquisabrasileirodinheiro/Apresentacao_brasileiro_relacao_dinheiro_2024.pdf. Acesso em: 9 nov. 2025.

BANCO CENTRAL DO BRASIL. **O Caminho do Dinheiro**. [*s. l.*]: Banco Central do Brasil, [s. d.]. Disponível em: https://www.bcb.gov.br/cedulasemoedas/caminhododinheiro. Acesso em: 26 maio 2025.

BANCO CENTRAL DO BRASIL. **Segunda Família do Real**. [*s. l.*]: Banco Central do Brasil, [s. d.]. Disponível em: https://www.bcb.gov.br/cedulasemoedas/segundafamilia. Acesso em: 9 nov. 2025.

BARBOSA, G. A. Q. B. *et al*. Criptomoedas: Uma Análise Sobre a Evolução da Moeda e sua Tributação no Brasil. **Revista das Faculdades Santa Cruz**, [*s. l.*], v. 13, n. 1, p. 1-50, 2022. Disponível em: https://periodicos.unisantacruz.edu.br/index.php/revusc/article/view/11/11. Acesso em: 26 maio 2025.

BUTERIN, V. **Ethereum White Paper**: A Next Generation Smart Contract & Decentralized Application Platform. [*s. l.*]: Blockchainlab, 2013. Disponível em: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Acesso em: 26 maio 2025.

CHICARINO, V. R. L. *et al*. Uso de Blockchain para Privacidade e Segurança em Internet das Coisas. *In*: NUNES, R. C.; CANEDO, E. D.; SOUSA JÚNIOR, R. T. **Minicursos do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. Brasília, DF: Sociedade Brasileira de Computação, 2017. Disponível em: https://www.researchgate.net/publication/321966650_Uso_de_Blockchain_para_Privacidade_e_Seguranca_em_Internet_das_Coisas. Acesso em: 25 maio 2025.

CISO ADVISOR. Ataques a Dispositivos Móveis Disparam 187% em um Ano. **CISO Advisor**, [*s. l.*], 30 jun. 2023. Disponível em: https://www.cisoadvisor.com.br/ataques-a-dispositivos-moveis-aumentaram-187-em-um-ano. Acesso em: 9 nov. 2025.

EUROPOL. Millions in Counterfeit Cash Seized in Major International Haul. **Europol**, [*s. l.*], 20 Aug. 2025. Disponível em: https://www.europol.europa.eu/media-press/newsroom/news/millions-in-counterfeit-cash-seized-in-major-international-haul. Acesso em: 9 nov. 2025.

FURINI, I. C. **Mercado de Meios de Pagamento no Brasil**: Visão Histórica e Tendências Globais. 2020. Trabalho de Conclusão de Curso (Curso Superior em Ciências Econômicas) – Faculdade de Ciências Econômicas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2020. Disponível em: https://lume.ufrgs.br/bitstream/handle/10183/216349/001120489.pdf?sequence=1&isAllowed=y. Acesso em: 26 maio 2025.

GREVE, F. *et al*. Blockchain e a Revolução do Consenso sob Demanda. *In*: MINICURSOS do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. [*s. l.*]: Sociedade Brasileira de Computação, 2018. Disponível em: https://www.researchgate.net/publication/324808918_Blockchain_e_a_Revolucao_do_Consenso_sob_Demanda. Acesso em: 25 maio 2025.

KREBS, B. How Phished Data Turns into Apple & Google Wallets. **Krebs on Security**: In-depth Security News and Investigation, [*s. l.*], 18 Feb. 2025. Disponível em: https://krebsonsecurity.com/2025/02/how-phished-data-turns-into-apple-google-wallets. Acesso em: 9 nov. 2025.

NAKAMOTO, S. **Bitcoin**: A Peer-to-Peer Electronic Cash System. [*s. l.*]: Bitcoin, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 26 maio 2025.

NERY, A. M. V.; COSTA, F. S. A. Dos Réis ao Bitcoin. **Revista Brasileira de Administração Política**, [*s. l.*], v. 11, n. 2, p. 105-123, 2021. Disponível em: https://periodicos.ufba.br/index.php/rebap/article/view/47087/25487. Acesso em: 26 maio 2025.

RAMAZZINI, R. Os Atentados Contra a Segurança Monetária do Brasil. **Poder360**, [*s. l.*], 12 abr. 2022. Disponível em: https://www.poder360.com.br/opiniao/os-atentados-contra-a-seguranca-monetaria-do-brasil. Acesso em: 9 nov. 2025.

SANTOS, A. C. dos. **Aprendizado de Máquina Aplicado na Detecção de Fraudes em Cartão de Crédito**. 2023. Monografia (Bacharelado em Estatística) – Departamento de Estatística, Instituto de Ciências Exatas e Biológicas, Universidade Federal de Ouro Preto, Ouro Preto, 2023. Disponível em: https://www.monografias.ufop.br/bitstream/35400000/6454/7/MONOGRAFIA_AprendizadoM%c3%a1quinaAplicado.pdf. Acesso em: 9 nov. 2025.

SILVA, A. L. S.; GOULART, E. T. **Criptomoedas**: A Moeda e o Sistema de Segurança nas Informações. 2022. Trabalho de Conclusão de Curso (Curso Superior em Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”, Americana, 2022. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/12644/1/20222S_Evandro%20Tampellini%20Goulart_OD01381.pdf. Acesso em: 26 maio 2025.

SULAIMAN, R. B.; SCHETININ, V.; SANT, P. Review of Machine Learning Approach on Credit Card Fraud Detection. **Human-Centric Intelligent Systems**, Luton, v. 2, p. 55-68, 5 May 2022. Disponível em: https://link.springer.com/content/pdf/10.1007/s44230-022-00004-0.pdf. Acesso em: 9 nov. 2025.

TATUM, C. T. S.; SANTOS, J. A. B. dos; RUSSO, S. L. Contrafação de Cédulas Brasileiras e Tecnologias Utilizadas para Proteção do Bem Fiduciário. **VII International Symposium on Technological Innovation**, Aracaju, v. 3, n. 1, p. 575-581, set. 2016. Disponível em: https://ri.ufs.br/bitstream/riufs/13765/2/ContrafacaoCedulasBrasileiras.pdf. Acesso em: 26 maio 2025.

VERONEZE, B. O.; SILVEIRA, V. F. **Aplicativos Móveis em Dispositivos Android**: Privacidade e Segurança. 2023. Trabalho de Conclusão de Curso (Curso Superior em Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana “Ministro Ralph Biasi”, Americana, 2023. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/15371/1/20232S_Breno%20de%20Oliveira%20Veroneze_OD1868.pdf. Acesso em: 9 nov. 2025.