
**PROTEÇÃO DE BENS DIGITAIS CONTRA PIRATARIA E PLÁGIO:
TENDÊNCIAS FUTURAS E OS PROBLEMAS ENFRENTADOS**

**PROTECTION OF DIGITAL GOODS AGAINST PIRACY AND PLAGIARISM:
FUTURE TRENDS AND THE PROBLEMS FACED**

Arthur Martins Pereira¹

Mário Henrique Akihiko da Costa Adaniya²

RESUMO

Com o avanço da tecnologia nas últimas décadas e a crescente dependência de ativos digitais, a proteção eficaz desses bens virtuais e digitais tornou-se fundamental tanto para empresas quanto para indivíduos. Neste contexto, essa pesquisa aborda os desafios da pirataria, roubo e plágio de ativos digitais, destacando suas implicações econômicas e de segurança. A pesquisa visa analisar abordagens inovadoras e tendências atuais na proteção de bens virtuais e digitais, bem como identificar as principais estratégias preventivas para as ameaças mencionadas. Para isso, será realizada uma revisão sistemática da literatura, explorando práticas recomendadas e tecnologias emergentes, incluindo criptografia, marcas d'água digitais, Gestão de Direitos Digitais (DRM), *fingerprinting digital*, inteligência artificial (IA) e *blockchain*. Espera-se que os resultados ofereçam orientações práticas para a gestão e proteção de ativos digitais, além de insights sobre tendências futuras e tecnologias em evolução nesta área. No entanto, a pesquisa reconhece limitações devido à natureza em constante evolução dos desafios relacionados à pirataria, roubo e plágio de ativos digitais.

187

Palavras-chave: bens digitais; ativos digitais; pirataria digital; blockchain; gestão de direitos digitais.

ABSTRACT

With the advancement of technology in recent decades and the growing dependence on digital assets, effective protection of these virtual and digital assets has become fundamental for both companies and individuals. In this context, this research addresses the challenges of piracy, theft and plagiarism of digital assets, highlighting their economic and security implications. The research aims to analyze innovative approaches and current trends in the protection of virtual and digital assets, as well as identify the main preventive strategies for the mentioned threats. To this end, a systematic literature review will be carried out, exploring best practices and emerging technologies, including cryptography, digital watermarks, Digital Rights Management (DRM), Digital Fingerprinting, artificial intelligence (AI) and Blockchain. The results are expected to offer practical guidance for managing and protecting digital assets, as well as insights into future trends and evolving technologies in this area. However,

¹ Centro Universitário Filadélfia de Londrina - UniFil

² Centro Universitário Filadélfia de Londrina - UniFil

the re- search recognizes limitations due to the constantly evolving nature of challenges related to piracy, theft and plagiarism of digital assets.

Keywords: digital goods; digital assets; digital piracy; blockchain; digital rights management.

1 INTRODUÇÃO

Nos últimos anos, o avanço tecnológico transformou a maneira como interagimos com o mundo, tornando a proteção de ativos digitais uma preocupação fundamental. De informações confidenciais à propriedade intelectual, esses ativos intangíveis sustentam a economia digital, exigindo abordagens inovadoras para sua gestão.

Neste mundo interconectado, novos desafios surgem com as mudanças nas demandas dos usuários e crescentes ameaças cibernéticas. A proteção e gerenciamento de bens digitais evoluem constantemente, com a criptografia, autenticação multifator, *firewalls* e *backups* sendo algumas das medidas essenciais. A tecnologia *blockchain* e a inteligência artificial (IA) também emergem como soluções promissoras.

188

No entanto, persiste o problema da pirataria, roubo e plágio de bens digitais, com facilidade de cópia e distribuição em grande escala. Questões de direitos autorais estão no centro das discussões e, soluções como criptografia, marcas d'água digitais, *Digital Rights Management* (DRM) e conscientização pública são empregadas, e a vigilância de redes P2P é fundamental.

Esta pesquisa analisa os métodos e tendências atuais de proteção de ativos digitais contra pirataria e plágio. Para alcançar esse objetivo, foi realizada uma revisão bibliográfica, buscando identificar tendências e medidas preventivas promissoras em constante evolução. Além disso, explorando os desafios e soluções para contribuir para um ambiente digital mais seguro.

2 ASPECTOS TEÓRICOS DA PESQUISA

2.1 O que são bens digitais e virtuais

Primeiramente, é fundamental compreender o que são exatamente esses bens

digitais e por que desempenham um papel tão crucial em nossa era digital. Bens digitais são ativos incorpóreos que existem principalmente no ambiente digital da Internet. Eles podem ter valor econômico e até mesmo valor pessoal para indivíduos e organizações. A característica distintiva desses bens é a sua natureza intangível e a capacidade de serem distribuídos, acessados e consumidos por meio de dispositivos eletrônicos, como computadores, smartphones, tablets e outros dispositivos conectados à Internet (Zampier, 2017).

Alguns exemplos comuns de bens digitais são: mídias digitais, como arquivos de fotos, vídeos, músicas, conteúdos interativos, como jogos eletrônicos, representam uma parte significativa dos bens digitais. Criptomoedas e outros ativos financeiros digitais também são uma grande parte dos ativos digitais nos dias atuais. E-books, publicações digitais, softwares e aplicativos são outros exemplos relevantes desses bens nos dias atuais, e são alguns dos tipos mais consumidos atualmente.

Uma característica única dos bens digitais comparados a bens físicos é a sua capacidade de reprodução e distribuição rápida e econômica. Diferente dos bens físicos, os bens digitais podem ser copiados ilimitadamente sem que sua qualidade seja afetada. Além disso, a forma de distribuição dos bens digitais é muito econômica e rápida o que os tornam convenientes para os consumidores. Atualmente os bens digitais desempenham um papel fundamental na economia global, eles impulsionam inovações tecnológicas, o comércio eletrônico, a cultura digital e a conectividade global. E graças a sua natureza versátil e escalável eles são um recurso valioso para empresas, criadores de conteúdo e consumidores em todo o mundo.

189

2.2 As ameaças da pirataria, roubo e plágio

A área de ativos digitais enfrenta uma série de desafios e ameaças, com foco particular na segurança e nos direitos autorais desses bens. Neste trabalho, abordaremos três dos problemas mais significativos que afetam essa área atualmente: pirataria, roubo e plágio. Essas ameaças persistem e causam prejuízos substanciais a indivíduos e empresas a cada ano.

2.2.1 Pirataria

A origem da pirataria digital remonta às primeiras décadas da era digital, quando a facilidade de copiar e distribuir conteúdos digitais se tornou uma realidade. Nos anos 80 e 90 a disseminação de software, músicas e filmes piratas se tornou bem comum, graças a criação dos disquetes e futuramente a internet. Isso foi impulsionado pela demanda por conteúdos gratuitos e acessíveis, bem como por desafios legais para as empresas que buscavam proteger seus direitos autorais.

Holt (2015) descreve a pirataria digital como um incêndio que se espalhou descontroladamente, e ela não está mais restrita a apenas a uma região geográfica, tornando-se uma ameaça global que afeta diversas indústrias. Devido a facilidade com que arquivos digitais podem ser copiados e compartilhados a pirataria digital foi capaz de ultrapassar diversas fronteiras e alcançou audiências em todo o mundo. (Holt, 2015)

Um exemplo notório da pirataria digital ocorre na indústria do entretenimento, onde filmes, séries e músicas são frequentemente alvo de práticas ilegais de distribuição. Milhões de cópias não autorizadas são compartilhadas online, resultando em perdas que ultrapassam a marca dos bilhões de dólares anualmente. Além das consequências financeiras, a pirataria também prejudica a reputação das empresas e mina a capacidade de investir em novos projetos e inovações, além dela também representar riscos para aqueles que consomem produtos piratas, pois não é possível garantir que esses produtos ou as plataformas onde são disponibilizados realmente sejam seguros para os consumidores. Outra indústria muito afetada pela pirataria é a indústria de videogames, grande parte dos jogos que se tornam populares acabam sofrendo com a pirataria, esse é um dos grandes motivos de estúdios de jogos terem adotado uma abordagem diferente, eles começaram a disponibilizar seus jogos de forma gratuita, utilizando outras formas de monetizá-los, assim reduzindo a pirataria deles.

2.2.2 Roubo

O roubo de ativos digitais refere-se à apropriação não autorizada desses bens.

Isso pode incluir a invasão de sistemas de armazenamento de dados para roubar informações confidenciais, como dados pessoais de clientes ou segredos comerciais. Esse crime é frequentemente cometido por hackers individuais ou em grupos. Esse tipo de crime iniciou desde o crescimento da economia digital, diversos indivíduos e empresas passassem a enfrentar ameaças cibernéticas. O início do século XXI marcou um grande aumento deste tipo de crime, o que exigiu um fortalecimento das medidas de segurança cibernética.

De acordo com Breitinger e Baggili (2019), o roubo de ativos digitais é uma prática que representa uma ameaça constante no mundo digital, com atacantes se aproveitando de falhas e vulnerabilidades para obter acesso não autorizado a informações confidenciais e propriedades intelectuais. Com a evolução da tecnologia cada vez mais rápida, novas medidas de segurança devem ser desenvolvidas para proteger esses ativos. (Breitinger; Baggili, 2019).

Um exemplo notável é o aumento de ataques cibernéticos direcionados a empresas e organizações governamentais. Esses ataques comprometem a segurança dos dados e podem ter repercussões devastadoras. Quase todos os anos surgem notícias de grandes vazamentos de dados de alguma grande empresa ou plataformas online são apresentados e, muitos desses casos estão relacionados aos vazamentos de dados pessoais dos usuários e empregados dessas organizações. Esses dados roubados acabam sendo comercializados mais tarde de forma ilegal.

191

2.2.3 Plágio

Assim como a pirataria digital, o plágio também tem suas raízes na facilidade de copiar e colar conteúdos na era da internet. À medida que a informação se tornou amplamente disponível online, muitas pessoas começaram a copiar textos, ideias e trabalhos alheios sem dar o devido crédito. A prática do plágio digital se tornou mais evidente com a popularização de ferramentas de busca e verificação de plágio, e as instituições educacionais e empresas passaram a adotar políticas mais rigorosas para combater essa forma de desonestidade acadêmica e profissional.

O plágio envolve a reprodução não autorizada de conteúdo digital, muitas vezes sem atribuição adequada ao criador original. Isso afeta escritores, criadores

de conteúdo, pesquisadores e artistas, minando a integridade do trabalho original e prejudicando o mérito de seus criadores. É um desafio particularmente relevante em ambientes acadêmicos e artísticos, onde a originalidade e a autoria são altamente valorizadas.

Brown e Holt (2018) explicam que atualmente o plágio é uma preocupação crescente na área dos ativos digitais, isso se deve ao quão fácil é copiar e colar conteúdos digitais, isso acabou gerando muitas oportunidades para que houvessem apropriações indevidas desses ativos digitais. O plágio digital é um desafio para criadores de conteúdos, educadores e para a aplicação da lei. (Brown; Holt, 2018)

Um exemplo mais recente que causou discussões sobre a natureza do plágio digital foi o surgimento de IAs treinadas para desenhar ou editar imagens. Essa tecnologia gerou diversas discussões, especialmente entre artistas que tiveram suas obras e estilos utilizados no treinamento dessas IAs sem o seu consentimento.

2.3 Estado atual do Mercado de Ativos Digitais

O mercado de ativos digitais é um setor em constante expansão e desempenha um papel significativo na economia digital. O mercado de ativos digitais tem suas raízes nas décadas de 1990 e 2000 no período em que a internet e tecnologias digitais estavam se popularizando e crescendo. À medida que a internet crescia, novas oportunidades surgiram para criar, distribuir e comercializar conteúdos e produtos digitais. A música, com o lançamento do iTunes da Apple em 2001 foi uma das pioneiras nesse mercado, com muitas outras formas de conteúdo digital surgindo em seguida.

O crescimento do mercado de ativos digitais é considerável e continua a crescer. Seu tamanho exato pode variar dependendo da fonte e período de análise, mas após a análise de notícias em sites como o Forbes e o *Fortune Business Insights* em 2023, é estimado que ele tenha ultrapassado a marca de 3.97 bilhões de dólares globalmente e é previsto que até 2030 ele já tenha alcançado a marca de 12.29 bilhões de dólares, abrangendo diversos tipos de conteúdos e serviços digitais. Um dos principais fatores para o crescimento desse mercado está conectado ao aumento no uso de dispositivos conectados à internet, serviços de streaming, a expansão do comércio eletrônico e a conveniência dos downloads digitais. Outro fator que ajudou

nesse crescimento acelerado foi a pandemia do COVID-19, já que durante o isolamento as pessoas buscavam por mais formas de entretenimento e conteúdos digitais. Espera-se que nos próximos anos esse crescimento continue, impulsionado pela alta e contínua demanda por ebooks, serviços de streaming, jogos digitais, aplicativos e outros produtos digitais.

Algumas das maiores empresas atualmente estão muito envolvidas nessa área, alguns exemplos são a Google, Amazon, Microsoft e Apple. Graças a essas grandes empresas, o mercado de ativos digitais continua a se expandir mais a cada ano, com novos tipos de ativos sendo desenvolvidos e comercializados. Além das empresas mencionadas, muitas outras estão envolvidas no mercado de ativos digitais, incluindo empresas de jogos eletrônicos, estúdios de cinema e música, editoras de livros digitais, desenvolvedores de software e muito mais. Além disso, é possível notar a evolução de tecnologias emergentes, como realidade virtual e aumentada, que estão abrindo novas oportunidades para a criação e distribuição de ativos digitais.

2.4 Principais Tecnologias e Técnicas em Uso Nessa Área

193

Para proteger os ativos digitais e enfrentar as ameaças da pirataria, plágio e roubo, uma série de diferentes tecnologias e técnicas têm sido desenvolvidas e aplicadas ao longo dos anos. Essa seção irá explorar algumas das principais abordagens em uso nessa área, incluindo: marca d'água digital, fingerprinting digital, criptografia e blockchain.

2.4.1 Marca d'Água Digital

A marca d'água digital é uma técnica essencial no contexto da proteção de ativos digitais. Ela desempenha um papel fundamental na identificação e na segurança de diversos conteúdos digitais, sendo empregada de maneira abrangente para garantir a autenticidade e a integridade de diversos tipos de arquivos digitais. Sua implementação envolve a inserção de dados discretos no conteúdo digital, e geralmente são imperceptíveis para humanos. Ao implementar os dados dessa forma se garante que a qualidade original do arquivo em questão não seja comprometida, geralmente

elas contêm informações como logotipos, assinaturas e códigos exclusivos, proporcionando mais camadas de proteção.

Megías, Kuribayashi e Qureshi (2020) mencionam três tipos de Marcas D'água Digitais, elas são a marca d'água robusta, marca d'água frágil e a marca d'água semi-frágil. A marca d'água robusta é projetada para resistir a múltiplos ataques maliciosos ou modificações benignas e é usada principalmente para a proteção de direitos autorais e controle de cópias, porém ela é incapaz de determinar se o conteúdo foi adulterado.(Megías; Kuribayashi; Qureshi, 2020).

A marca d'água frágil por outro lado é projetada para ser destruída a qualquer tipo de modificação, sejam ataques acidentais ou intencionais. Seu objetivo é detectar qualquer manipulação não autorizada dos conteúdos, não importa o quão pequena a mudança seja. Vale mencionar que ela também permite a recuperação dos conteúdos originais(não marcados) após identificar os conteúdos marcados.

Por fim a marca d'água semi-frágil, o foco dela é em equilibrar a robustez com a vulnerabilidade, ela é projetada para ser robusta contra modificações incidentais ou menores, mas pode ser frágil contra ataques maliciosos, isso a torna adequada para a autenticação de conteúdo.

No contexto da proteção de direitos autorais de bens digitais, as marcas d'água digitais possuem um papel crucial ao garantir que criadores e proprietários de conteúdos digitais sejam capazes de monitorar seus bens e criações de forma eficaz. Ao integrarem uma marca d'água digital nos arquivos digitais, os detentores de direitos autorais são capazes de rastrear a origem e a autoria do conteúdo, os auxiliando a garantir uma maior proteção para essas propriedades intelectuais.

Muitas agências que trabalham com o licenciamento de mídias e distribuição de conteúdos digitais dependem muito das marcas d'água para garantirem que seus ativos digitais sejam distribuídos de forma segura e controlada. A implementação dessa tecnologia permite que essas entidades sejam capazes de rastrear as trajetórias de distribuição de seus conteúdos, além de protegê-los contra o uso não autorizado e a aplicação de direitos autorais. Dessa forma tanto os conteúdos digitais quanto o mercado de propriedade intelectual tem sua integridade e sustentabilidade preservados.

2.4.2 Fingerprinting Digital

O *Fingerprinting* Digital é uma técnica que desempenha um papel essencial para a proteção de ativos digitais contra a pirataria e distribuição ilegal. Como explicado por Megías, Kuribayashi e Qureshi (2020) ela funciona através da criação de uma impressão digital que é única e específica para um arquivo digital específico por meio de suas características distintivas, essa impressão funciona como uma espécie de assinatura digital exclusiva para o arquivo em questão. (Megías; Kuribayashi; Qureshi, 2020).

Essa técnica se desenvolveu em resposta a evolução e aumento da pirataria e distribuição ilegal de conteúdos digitais, esses problemas se tornaram grandes desafios para a indústria do entretenimento e para os detentores de direitos autorais. A abordagem oferecida pelo *Fingerprinting* Digital é eficaz na identificação e rastreamento de cópias ilegais de arquivos sujeitos a direitos autorais, isso é especialmente útil para sistemas de gerenciamento de direitos digitais (*Digital Rights Management*).

Nos sistemas DRM o *Fingerprinting* Digital é usado como uma forma de proteger diversos conteúdos digitais, como vídeos, imagens e músicas, por exemplo. A impressão digital única que cada arquivo recebe permite que os detentores de direitos autorais sejam capazes de identificar cópias ilegais desse arquivo e então eles tomam as devidas medidas para impedir a distribuição não autorizada desses conteúdos.

Atualmente muitas empresas de entretenimento e distribuidoras de conteúdo dependem do *Fingerprinting* Digital como uma ferramenta para detectar e prevenir a pirataria digital. Assim que alguma cópia ilegal é identificada as empresas podem tomar medidas para fazer cumprir os direitos autorais que possuem sobre esses bens e para protegê-los, o que além de proteger os interesses dos criadores também protege a integridade do mercado de ativos digitais. Portanto, é possível notar que o papel do *Fingerprinting* Digital é fundamental para a defesa dos direitos autorais e na manutenção de um mercado digital por meio de conteúdo íntegro e legítimo.

E de acordo com Hsieh (2014), no futuro poder ser possível combinar as marcas d'água digitais com o fingerprinting digital, utilizando essas duas técnicas em conjunto para conseguir uma maior proteção para ativos digitais. (Hsieh *et al.*, 2014)

2.4.3 Criptografia

A criptografia moderna desempenha um papel crucial na proteção de dados e informações confidenciais em diversas áreas da tecnologia. Na área de ativos digitais ela é crucial na proteção contra ameaças de roubo e plágio de dados, além de proteger ativos digitais da pirataria.

De acordo com Kessler (2003), a criptografia é a ciência de escrever em códigos secretos. Ela é uma técnica bem antiga e existem registros de seu uso desde séculos antes da invenção de qualquer máquina. A criptografia não é apenas usada para proteger dados de roubo ou alterações, mas ela também pode ser usada para autenticá-los. (Kessler, 2003)

Ela é uma técnica que envolve a conversão de dados para um formato ilegível, conhecido como texto cifrado, que só pode ser decifrado por um indivíduo ou sistema que possuam a chave de descryptografia apropriada. Existem muitas técnicas de criptografia que são utilizadas na área da tecnologia, as mais comuns são a criptografia assimétrica, a criptografia simétrica e as funções de Hash, cada é usada de maneiras e ambientes diferentes.

Atualmente a criptografia é uma das tecnologias mais importantes para a segurança de dados, seja em transações financeiras, comunicações ou no armazenamento seguro de dados e informações sensíveis. Conforme nosso mundo se torna mais conectado, a segurança dos dados de indivíduos e organizações se torna algo de extrema importância, e a criptografia é uma solução muito eficiente para atender essas demandas.

Na indústria de ativos digitais a criptografia desempenha um papel essencial na segurança das transações e no armazenamento de ativos digitais, garantindo que apenas os destinatários autorizados tenham acesso a esses bens.

Uma tecnologia que vem sendo muito adotada nessa área e que utiliza a criptografia é a *blockchain*, nela a criptografia é utilizada para garantir segurança no armazenamento e para que os registros das transações sejam imutáveis.

2.4.4 Blockchain

Após a análise de diversas pesquisas e artigos, como o feito por Levis *et al.* (2021), foi possível concluir que tecnologia *blockchain* originalmente foi desenvolvida como tecnologia adjacente das criptomoedas, mais especificamente do Bit coin, e recentemente ela vem desempenhando um papel muito importante em relação a proteção de ativos digitais. Resumidamente, o *blockchain* é uma estrutura de dados distribuída que registra transações de forma imutável, em outras palavras, uma vez que informações são registradas, não é possível apagar ou alterar elas. (Levis; Fontana; Ughetto, 2021)

Embora ela tenha começado como uma solução para transações financeiras e ser principalmente usada em conjunto com criptomoedas, sua aplicação expandiu para a autenticação e proteção de ativos digitais, atualmente ela também é muito utilizada na área de NFTs (*Non Fungible Tokens*), como mostrado nas pesquisas de autores como Borri (2022). (Borri; Liu; Tsyvinski, 2022)

A principal vantagem oferecida pela *blockchain* é uma camada adicional de segurança, que garante que os ativos digitais armazenados nela não sejam falsificados ou copiados sem autorização. O *blockchain* está revolucionando a autenticação de ativos digitais. Sua natureza descentralizada e inalterável assegura que a proveniência e a autenticidade dos ativos digitais possam ser verificadas de maneira confiável. Esta característica é particularmente valiosa na proteção de obras de arte digital, propriedade intelectual e até mesmo bens virtuais dentro de jogos online.

A tecnologia *blockchain* oferece uma solução poderosa para rastrear a proveniência de diferentes ativos digitais, fornecendo uma camada de autenticação confiável no mercado de ativos digitais atual e futuro. Sua aplicação está revolucionando a forma como protegemos e validamos a autenticidade de bens digitais, criando um ambiente mais seguro e confiável para criadores e consumidores.

2.4.5 Autenticação Multifator

Outra tecnologia utilizada na área é a autenticação multifator (*Multi Factor Authentication*), ela é principalmente usada para aumentar a segurança de sistemas

e contas digitais. Esse método de autenticação requer que o usuário forneça duas ou mais formas de verificação para confirmar sua identidade antes de acessar um sistema ou conta. Geralmente, essas formas de verificação incluem algo que o usuário sabe (como uma senha), algo que o usuário possui (como um smartphone ou um cartão de segurança), ou algo relacionado ao corpo do usuário (como uma impressão digital ou reconhecimento facial).

Após uma análise da pesquisa conduzida por Ometov (2018), foi entendido que o principal motivo para o crescente uso da MFA se deve ao grande aumento de segurança que ela fornece por conta das múltiplas camadas que ela pode possuir e, mesmo que uma delas acabe sendo violada as outras ainda estarão lá para proteger as informações ou ativos que elas guardam. A MFA torna consideravelmente mais difícil para invasores obter acesso não autorizado, uma vez que requer mais do que apenas a adivinhação de senhas, tornando-a uma ferramenta valiosa na proteção de ativos digitais contra ameaças de segurança. (Ometov *et al.*, 2018).

Outro ponto mencionado por Ometov (2018), é a possibilidade da autenticação multifator continuar a evoluir, uma direção promissora para essa tecnologia é a biometria baseada em comportamento. Ela se trata de uma análise de certas ações do usuário, como sua forma de escrever ou falar, buscando por padrões, isso tornaria possível a criação de novos tipos de camadas de proteção para a MFA. Esse método pode oferecer abordagens inovadoras para a autenticação de usuários, aproveitando características únicas de seu comportamento para aumentar a segurança digital. A biometria comportamental é uma tendência emergente que pode revolucionar a maneira como autenticamos e protegemos nossos ativos digitais no futuro.

A evolução da MFA está sendo impulsionada pela necessidade de segurança cada vez maior em um ambiente digital em constante mudança. À medida que as ameaças se tornam mais sofisticadas, as organizações e os usuários continuam a adotar métodos de autenticação mais avançados para proteger seus ativos digitais e informações pessoais. A segurança digital é uma prioridade em constante evolução e, a MFA desempenha um papel crucial nesse contexto.

Essas cinco tecnologias são algumas das mais utilizadas atualmente, e é graças a elas que a área de ativos digitais vem se tornando mais segura. É possível que no futuro diversas outras técnicas e tecnologias sejam desenvolvidas, especialmente

com a constante evolução das ameaças que afetam essa área.

2.5 As Tendências e Tecnologias Atuais e Futuras da Área de Ativos Digitais

Uso da Inteligência artificial (IA): Atualmente é possível notar uma grande evolução em relação às tecnologias que utilizam IA. Elas estão se tornando mais avançadas e estão sendo incluídas em diversos campos da tecnologia, incluindo seu crescente papel na proteção de ativos digitais. (Zhang *et al.*, 2022) Os algoritmos de IA são capazes de analisar padrões de comportamento para identificar atividades suspeitas, como tentativas de pirataria, plágio ou o roubo de ativos digitais. Além disso as IAs também podem melhorar as medidas de segurança, devido a sua capacidade de adaptação, o que as torna muito úteis na luta contra ameaças que estão em constante evolução.

Tecnologia de Blockchain Avançada: Atualmente o uso do *blockchain* não está mais limitado apenas às criptomoedas. No campo de ativos digitais, o *blockchain* está sendo utilizado na criação de registros imutáveis de autenticidade e proveniência. Conforme essa tecnologia evolui, podemos esperar sistemas mais robustos e seguros para a autenticação e proteção de ativos digitais. E da mesma forma que essa tecnologia passou a ser adotada em conjunto com os NFTs, como é explicado por Borri (2022), é possível que no futuro ela seja utilizada em conjunto com outros tipos de bens virtuais. (Borri; Liu; Tsyvinski, 2022)

Rastreamento de Direitos Autorais em Tempo Real: Novas tecnologias estão sendo desenvolvidas com o objetivo de permitir que criadores e proprietários de conteúdo possam rastrear o uso de seus ativos digitais em tempo real. Isso não só irá aumentar muito a proteção desses bens contra a pirataria, mas também auxiliará no gerenciamento de direitos autorais, garantindo uma compensação adequada aos criadores pelo uso de seus trabalhos. Tecnologias como a *blockchain* já adotam essa técnica, como visto em seu uso com NFTs (Borri; Liu; Tsyvinski, 2022). Isso é um dos fatores que tornam a *blockchain* tão segura para ativos digitais.

Assinaturas Digitais Avançadas: Como discutido anteriormente na pesquisa realizada por Hsieh *et al.* (2014), e nas informações fornecidas por Megías (2020), as assinaturas digitais como as marcas d'água digitais e o *fingerprinting* digital estão

evoluindo para fornecer um maior nível de segurança. Elas não são apenas usadas para confirmar a autenticidade de conteúdos digitais, mas também para rastrear e registrar quem acessou ou modificou esses conteúdos, garantindo assim um maior grau de transparência e segurança. (Hsieh *et al.*, 2014), (Megías; Kuribayashi; Qureshi, 2020).

Regulamentações e Leis Para a Proteção de Bens Digitais: Uma pesquisa que aborda esse aspecto dos bens digitais foi realizada por Stuckey (2023), ela explica como exatamente as leis de direitos autorais são aplicadas atualmente no ambiente online (Stuckey, 2023). Atualmente diversos governos e organizações estão adotando regulamentações mais restritivas em relação a proteção de bens digitais. Em sua maioria elas são leis de direitos autorais mais abrangentes ou punições mais severas para infratores desses direitos.

3 A METODOLOGIA UTILIZADA E A COLETA DE INFORMAÇÕES

Durante a pesquisa, foram utilizadas diversas fontes de informação, incluindo bases de dados acadêmicos renomados, como o IEEE Xplore, Google Acadêmico e o MDPI. A seleção dos documentos utilizados nesta pesquisa seguiu critérios rigorosos de relevância. Esses critérios englobam o título, palavras-chave relacionadas ao tema da pesquisa, o ano de publicação do documento, uma leitura inicial de seu resumo e a credibilidade das fontes.

A metodologia de pesquisa envolveu a busca, seleção e análise de vários artigos e livros, a seleção dos trabalhos ocorreu da seguinte forma. Primeiro foram acessadas as bases de dados mencionadas anteriormente, em seguida foram utilizadas palavras chave para buscar por trabalhos relacionados ao tema, essa busca inicial incluiu apenas artigos de 2019 até 2023. Após essa seleção inicial, uma leitura breve de seus resumos foi realizada com o objetivo de definir se eles continham informações sobre o tema, também foram analisadas as suas referências. Os trabalhos que pareciam mais relevantes foram escolhidos e analisados de forma mais aprofundada, as principais informações que foram buscadas eram sobre, as ameaças da pirataria, roubo e plágio, técnicas e tecnologias utilizadas na área, e informações atuais sobre o mercado de ativos digitais, etc. Os trabalhos que possuíam essas informações foram

escolhidos para serem analisados por completo e incluídos nessa pesquisa

Apesar da análise inicial ter sido de grande importância, algumas informações não foram encontradas. Então uma segunda busca por trabalhos acadêmicos foi realizada, porém dessa vez não havia um período específico selecionado para os trabalhos que foram encontrados. Alguns dos trabalhos escolhidos durante essa segunda pesquisa já eram datados e desatualizados, mas ainda foi possível adquirir informações valiosas através deles.

Porém, alguns problemas surgiram com essas buscas, havia uma escassez de artigos relacionados a esse tema específico, e a maioria dos livros que eram relevantes para essa pesquisa exigiam pagamento para o acesso completo de seus conteúdos. Portanto, algumas informações acabaram não sendo encontradas, mais especificamente, dados sobre o crescimento atual do mercado de ativos digitais e do uso das tecnologias aqui mencionadas. Por conta disso acabou sendo necessário buscar por esses dados em sites de notícias como o Forbes e o Fortune Business Insight, ou outras bases de dados acadêmicas, isso permitiu que a maioria das informações em falta fossem encontradas.

201

Vale ressaltar que as informações sobre as técnicas e tecnologias discutidas neste trabalho foram comparadas com as de sites e pesquisas acadêmicas, o que ajudou a garantir a precisão e consistência das informações encontradas.

Essa abordagem metodológica permitiu a obtenção de uma maior compreensão sobre os métodos e estratégias mais utilizados na proteção de ativos digitais, e sobre como as ameaças enfrentadas afetam essa área. Além disso, esta metodologia proporcionou insights sobre as tecnologias e métodos que podem moldar o futuro da proteção de ativos digitais, demonstrando como podem influenciar seu desenvolvimento.

4 DISCUSSÃO

4.1 Tecnologias e Métodos de Proteção Mais Adotados

Durante a pesquisa, ficou evidente que a evolução dos métodos e tecnologias de proteção para os ativos digitais foi algo fundamental no combate da pirataria,

plágio e roubo desses ativos. E ao longo dos anos muitas técnicas e tecnologias foram desenvolvidas

A criptografia é uma técnica fundamental para a proteção de ativos digitais, diversas tecnologias usadas hoje em dia utilizam a criptografia para melhorar sua segurança, a blockchain é um bom exemplo disso. Kessler (2003) descreveu que existem diversas formas de criptografia, e a chave é saber utilizar a forma mais eficiente para a tarefa que se deseja cumprir.

Já tecnologias de assinatura digital como as marcas d'água e o fingerprinting digital são extremamente úteis para identificar a autoria de algum bem e rastrear quaisquer cópias ilegais dele, Megías, Kuribayashi e Qureshi (2020) explicam sobre os diferentes tipos de marcas d'água e como funcionam. Os autores também discutem várias formas de utilizar técnicas de fingerprint para buscar por cópias pirateadas, assim protegendo os direitos autorais dos criadores e detentores desses conteúdos. As assinaturas digitais são frequentemente utilizadas por órgãos governamentais e organizações privadas como uma forma de marcar documentos importantes, e também de garantir sua integridade. Apesar de ambas serem técnicas de assinatura digital, elas têm funções diferentes, as Marcas D'água são especialmente úteis para prevenir que algum bem seja alterado, copiado ou adulterado, assim combatendo principalmente a adulteração e roubo de conteúdos digitais. Já o Fingerprint é mais utilizado como uma forma de rastrear um bem específico e quaisquer cópias dele que excitam em uma rede ou sistema, assim combatendo principalmente o roubo e a pirataria, porém ele não é capaz de impedir que o bem em questão seja pirateado, ele apenas rastreia essas cópias.

A blockchain é outra tecnologia que vem sendo bem utilizada nessa área nos últimos anos, ela é principalmente utilizada para a proteção de ativos digitais como as criptomoedas, atualmente todas as criptomoedas existentes no mercado são armazenadas em suas respectivas blockchains. Mais recentemente, como apresentado por Borrie Liu (2022) em sua pesquisa, ela passou a ser usada com os NFTs no fim de 2021 e início de 2022, é bem possível que essa tecnologia passe a ser aplicada em outros tipos de bens digitais no futuro. Em 2023 algumas pesquisas realizadas pela Ernst & Young reportaram que cerca de 38% dos trabalhadores do Estados Unidos relataram que a blockchain já vem sendo utilizada em suas empresas. O principal foco

da blockchain está em garantir a segurança e integridade dos ativos e transações armazenadas dentro dela, tornando quase impossível de se alterar essas informações.

Para finalizar, um dos métodos de proteção que vem sendo mais adotados nos últimos anos é a MFA. Ometov (2018) destaca que a MFA é muito utilizada na proteção de sistemas e contas digitais, dificultando a entrada indevida de invasores.

De acordo com a LastPass em 2019, foi reportado que 57% das empresas e organizações globalmente já utilizavam a MFA, e esse uso continua crescendo, especialmente por conta do alto nível de proteção que ela oferece, foi calculado que a MFA pode prevenir cerca de 80% à 90% dos ataques cibernéticos. Mas existem alguns pontos negativos, ela aumenta o tempo necessário para o login dos usuários, ela exige um mais hardware e software para ser implantada e utilizada e, apesar de providenciar maior proteção ela não é completamente invulnerável a ataques.

4.2 O Estado das Ameaças Enfrentadas Nessa Área

203

Apesar de existirem diversas tecnologias, técnicas e métodos de proteção para os ativos digitais, as ameaças da pirataria, plágio e roubo continuam a ser um problema constante. Após a análise das pesquisas de autores como, Holt (2018), Brown (2015) e Breitinger (2018), foi concluído que essas ameaças continuam a causar perdas enormes para o setor de ativos digitais. Um exemplo disso é a pirataria de filmes e séries, a ascensão das plataformas de streaming foi um fator que tornou muito mais fácil piratear essas mídias, pois elas já estão sendo distribuídas em um formato digital dentro das plataformas de streaming. Foi calculado que em 2022 sites piratas receberam cerca de 215 bilhões de visitas, isso foi 18% mais do que em 2021. Cerca de 80% da pirataria digital pode ser atribuída a serviços de streaming ilegais e quase 24% da largura de banda global da Internet é usada para a pirataria.

No caso do plágio de bens digitais, ele continua a afetar diversos tipos de ativos digitais, como jogos, documentos acadêmicos e músicas. Recentemente surgiu uma discussão que parece ter relação com esse problema, essa discussão está relacionada aos desenvolvimentos de IA's com a capacidade de desenhar ou editar imagens que começou a se disseminar em meados de 2022. O treinamento dessas

IAs ocorre através de um banco de dados de obras de arte feitas por humanos, na maioria dos casos sem o consentimento dos artistas, o que levou muitos deles a ficarem irritados pois estavam tendo seus estilos e obras copiados pelas IA's sem receber nenhum crédito, esse assunto ainda é discutido especialmente entre a comunidade artística online. Recentemente com o ChatGPT também surgiram algumas discussões sobre o assunto, foi calculado que atualmente cerca de 90% dos estudantes utilizam o ChatGPT em suas tarefas, e muitos professores e instituições estão preocupados que plágio comece a se tornar mais frequente.

Essas ameaças não afetam apenas aos criadores e detentores desses ativos, mas também causam riscos à segurança para os consumidores e para a integridade do mercado de ativos digitais, gerando perdas consideráveis todos os anos.

4.3 Sobre o Futuro Desta Área

O futuro da área de ativos digitais é bem promissor, ela já cresceu muito ao longo dos últimos anos, e especialmente nas áreas do entretenimento, como livros, filmes, jogos e serviços de streaming. O nosso mundo continua se tornando cada vez mais conectado, com a tecnologia e o mundo digital se tornando mais e mais presentes no nosso cotidiano, novas tecnologias, como as IAs, já estão começando a se tornar um grande foco para as empresas de tecnologia, e como discutido por Zhang (2022), o potencial das IAs na área de cibersegurança é bem alto. Os autores destacam que é provável que a área de bens digitais também seja afetada por elas. As IAs poderão vir a se tornar muito importantes para a segurança dos ativos digitais e na aplicação de direitos autorais, nos próximos anos é muito provável que veremos elas começando a serem mais implementadas, mesmo que de uma forma mais discreta.

Tecnologias como a blockchain, marcas d'água digitais e fingerprinting também podem acabar evoluindo, a blockchain tem um grande potencial, atualmente ela é principalmente usada com as criptomoedas, já que esse foi seu propósito inicial, recentemente com o surgimento dos NFTs a blockchain também passou a ser utilizada com eles, e no futuro ela pode passar a ser implantada em diversos campos, como a gestão de identidade, a área de saúde ou até votações eletrônicas. Algumas dessas possibilidades são discutidas por Levis (2021) em seu artigo, porém é importante men-

cionar que a blockchain é, e provavelmente continuará a ser, principalmente utilizada na proteção de dados ou bens com valor econômico e as transações relacionadas a eles.

Outro ponto importante é o aumento na implantação de novas leis para a proteção de direitos autorais em diversos países, essas leis em conjunto com punições mais rígidas podem vir a se tornar um recurso ainda mais importante na proteção de ativos digitais, incentivando os mercados nacionais desses bens. O artigo escrito por Stuckey (2023) detalha bem essas leis e como funcionam. Também existe um crescimento na conscientização pública sobre tais práticas, com campanhas educacionais visando explicar os perigos que essas ameaças representam, não apenas para as empresas mas também para o público geral.

Porém, apesar dos avanços positivos nessa área, os desafios que ela enfrenta também poderão se adaptar e continuar a causar problemas, a pirataria, plágio e o roubo não são problemas que irão desaparecer tão cedo, especialmente com essas práticas sendo tão lucrativas para os infratores.

Resumindo, essa área tem muito potencial para se desenvolver e se tornar ainda mais parte do nosso dia a dia, novas tecnologias são desenvolvidas e as antigas melhoradas, tudo com o foco de melhorar a segurança para esses ativos, mas as ameaças também estão a se adaptar e evoluir em resposta. A luta contra a pirataria, o plágio e o roubo de ativos digitais não acabará tão cedo, o que podemos fazer atualmente é conscientizar a população, buscar que novas leis para a proteção de bens digitais sejam aplicadas, e apoiar tecnologias, técnicas e outros avanços que busquem melhorar a segurança dessa área, tanto para os criadores e detentores desses ativos quanto para seus consumidores.

5 CONCLUSÃO

Ao longo da nossa pesquisa, vários conhecimentos sobre essa área foram adquiridos e compilados. Os resultados dessa pesquisa destacam a necessidade contínua de inovações e aprimoramentos para as estratégias de segurança utilizadas nessa área, bem como uma compreensão mais aprofundada dos desafios enfrentados por criadores, detentores de direitos e consumidores nesse ambiente

digital em constante mudança.

Os resultados também revelaram a importância crítica das tecnologias e dos métodos de proteção que estão sendo adotados, incluindo a criptografia, autenticação multifator, o blockchain, a marca d'água digital, além de muitas outras. Essas soluções vem desempenhando um papel fundamental na segurança dos ativos digitais, promovendo a autenticidade e a integridade desses ativos, além de reforçar os direitos autorais.

No entanto, apesar dos diversos avanços para a proteção dos ativos digitais, as ameaças enfrentadas por eles continuam a evoluir e se adaptar. Após certos eventos, como a pandemia do COVID19, muitas empresas e organizações começaram a fazer uma transição para meios digitais, isso aumentou ainda mais a presença do mundo digital no nosso dia a dia e, por conta disso, também houve um aumento da frequência e na extensão em que a pirataria, o roubo e o plágio de ativos digitais ocorrem nessa área, e isso vem gerando grandes perdas tanto para indivíduos quanto para as grandes empresas que trabalham com essa área. Portanto, apesar das tecnologias e técnicas utilizadas nessa área serem capazes de proteger os ativos digitais em boa parte do tempo, não é o suficiente para acabar com essas ameaças completamente, isso faz com que métodos de proteção mais robustos e eficazes sejam necessários.

Analisando o futuro dessa área é importante reconhecer o potencial promissor de novas tecnologias, como a IA, ou no aprimoramento das já existentes, como o blockchain, para reforçar ainda mais a segurança e a aplicação de direitos autorais. A implementação de leis mais rígidas em nível nacional e internacional também é um passo crucial para a proteção dos direitos de criadores e detentores de ativos digitais e propriedade intelectual, dessa forma impulsionando um crescimento sustentável e ético desse setor.

Embora a luta contra a pirataria, o roubo e o plágio de ativos digitais possa permanecer desafiadora, é fundamental continuar educando o público e promovendo uma conscientização mais ampla sobre os riscos e impactos dessas práticas ilícitas. Ao apoiar o desenvolvimento contínuo de tecnologias avançadas, estratégias eficazes e regulamentações robustas, podemos garantir um ambiente digital mais seguro e protegido para criadores, detentores de direitos e consumidores, promovendo assim

um ecossistema digital mais resiliente e ético para as gerações futuras.

5.1 Trabalhos Futuros

Esse trabalho abordou vários pontos relacionados a área de ativos digitais, foi discutido sobre algumas das ameaças que ela enfrenta, as melhores técnicas e tecnologias utilizadas atualmente, sobre o estado do mercado dessa área e brevemente sobre o futuro dela.

Porém esse trabalho acabou não se aprofundando muito nesses tópicos, então seria possível que futuros trabalhos abordem alguns destes tópicos de forma mais aprofundada, eles poderiam discutir apenas sobre a pirataria, o plágio ou o roubo de ativos digitais, discutindo sobre a ameaça que o problema escolhido representa e como combatê-lo. Também poderiam ser desenvolvidas pesquisas que discutam sobre o futuro de certas tecnologias e técnicas utilizadas na área, elas poderiam falar sobre as assinaturas digitais, sobre como as IAs irão afetar essa área tanto positivamente quanto negativamente, sobre o futuro da blockchain, etc.

207

Outra possibilidade seria a realização de uma pesquisa similar a essa daqui a vários anos, analisando ameaças que a área enfrenta, quais tecnologias são usadas para a segurança e quais ainda estão sendo desenvolvidas, dando uma visão geral do estado da área de ativos digitais nesse período. Resumindo, apesar dessa pesquisa ser tão aprofundada, ela poderia servir como uma base para outras pesquisas relacionadas a essa área, ela seria muito útil, principalmente por conta da falta de pesquisas similares nessa área.

REFERÊNCIAS

BORRI, N.; LIU, Y.; TSYVINSKI, A. The economics of non-fungible tokens. *Available at SSRN 4052045*, 2022.

BREITINGER, F.; BAGGILI, I. *Digital Forensics and Cyber Crime*. [S.l.]: Springer, 2019.

BROWN, S. C.; HOLT, T. J. *Digital piracy: A global, multidisciplinary account*. [S.l.]: Routledge, 2018.

HOLT, T. *Digital Piracy*. [S.l.]: Oxford University Press, 2015.

HSIEH, S. L. *et al.* Combining digital watermarking and fingerprinting techniques to identify copyrights for color images. *The Scientific World Journal*, Hindawi, v. 2014, 2014.

KESSLER, G. C. An overview of cryptography. Gary C. Kessler, 2003.

LEVIS, D.; FONTANA, F.; UGHETTO, E. A look into the future of blockchain technology. *Plos one*, Public Library of Science San Francisco, CA USA, v. 16, n. 11, p. e0258995, 2021.

MEGÍAS, D.; KURIBAYASHI, M.; QURESHI, A. Survey on decentralized fingerprinting solutions: Copyright protection through piracy tracing. *Computers*, v. 9, n. 2, 2020. Disponível em: <https://www.mdpi.com/2073-431X/9/2/26>. Acesso em: 23 out. 2023.

OMETOV, A. *et al.* Multi-factor authentication: A survey. *Cryptography*, MDPI, v. 2, n. 1, p. 1, 2018.

STUCKEY, K. D. *Internet and online law*. [S.l.]: Law Journal Press, 2023.

ZAMPIER, B. *Bens digitais: cybercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais*. Editora Foco, 2017. Disponível em: <https://books.google.com.br/books?id=6mM3tAEACAAJ>. Acesso em: 23 out. 2023.

208

ZHANG, Z. *et al.* Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access*, v. 10, p. 93104–93139, 2022.

AGRADECIMENTOS

Meus agradecimentos vão para o meu orientador, o professor Mário Henrique Akihiko da Costa Adaniya, ele me ajudou e me guiou através dos problemas e dificuldades que eu tive durante o desenvolvimento dessa pesquisa, eu não teria conseguido chegar tão longe sem a ajuda dele.

Eu também agradeço aos meus pais, irmão e família, que me apoiaram e me incentivaram a completar essa pesquisa, mesmo nos meus momentos de maior dificuldade.