

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA
BACHARELADO EM ENGENHARIA DE COMPUTAÇÃO

AGUSTIN GABRIEL AMARAL CASTILLO

**NFT (NON-FUNGIBLE TOKEN) COMO UTILITY
TOKEN: UM ESTUDO DE CASO**

SÃO CARLOS -SP
2023

AGUSTIN GABRIEL AMARAL CASTILLO

NFT (NON-FUNGIBLE TOKEN) COMO UTILITY TOKEN: UM ESTUDO DE CASO

Trabalho de conclusão de curso apresentado ao Departamento de Computação da Universidade Federal de São Carlos, para obtenção do título de bacharel em Engenharia da Computação.

Orientador: Prof. Dr. Hélio C. Guardia

São Carlos-SP

2023

Dedico este trabalho ao meu avô Acyr do Amaral que embora não esteja presente para acompanhar essa conquista sempre me desejou isso assim como ao meu amigo José Albolea nos deixou em 2015 mas sempre foi um exemplo para mim de como devemos tratar nossos anos na universidade.

AGRADECIMENTO

Gostaria de agradecer aos meus pais, Andrea e Agustin, e a minha irmã, Tamiris, pelo apoio (financeiro e emocional), durante esses 10 anos de graduação, assim como, ao meu tio, Renato, por ter me inserido na área da computação e me apoiado muito no início da minha carreira profissional.

Agradeço a todos meus amigos do grupo Bavarinha, pela incrível parceria durante os anos de graduação e, com certeza, para o futuro também, e aos moradores da República Passanellas, que dividiram essa jornada comigo, em especial, Joezer Engel, que sempre foi um grande amigo e tem grande parcela nessa conquista. Também agradeço aos meus amigos Gustavo, Guiga, Amanda e Laura, por estarem sempre presentes, torcendo fielmente pela minha felicidade, facilitando o processo. E também agradecer Eduardo e Cassiano que com certeza foram fundamentais para minha formação.

Ao Professor Hélio Crestana Guardia, meu orientador acadêmico, por todo o apoio e toda ajuda fornecida durante o desenvolvimento deste trabalho.

Finalmente, agradeço a todos que de alguma forma contribuíram para que esse trabalho pudesse ser realizado.

*“Os 5 anos de engenharia foram os 10
melhores anos da minha vida”
(Agustin Castillo)*

RESUMO

São declarados como **tokens de utilidade** (*utility tokens*) qualquer ativo digital que tenha a ele atrelado algum benefício, seja este físico ou digital, além de seu valor especulativo. Podem ser considerados como benefícios o acesso a certo grupo de serviços, a participação em sorteios ou eventos, descontos em futuras compras, ou basicamente qualquer qualidade que separe os detentores de tais *tokens* de consumidores comuns. *Tokens* não fungíveis (NFTs) são exemplos de ativos digitais que possuem também como característica o fato de serem únicos e indivisíveis, além de serem validados via mecanismos baseados em *blockchain*. O uso de NFTs como *tokens* de utilidade para acesso a serviços pode representar uma grande revolução em questões de segurança e praticidade, integrando o mundo físico e o mundo virtual. Este trabalho busca fornecer informações sobre o uso de NFTs, abordando suas diversas aplicações, seu funcionamento e o processo de criação, além de explorar formas diferentes de solucionar problemas comuns nos acessos a serviços (sejam eles físicos ou digitais) como duplicidade e/ou compartilhamento de acesso, falsificação de credenciais ou até cambismo. Deste modo, busca-se exemplificar a utilidade dos NFTs na solução de empecilhos atualmente presentes no controle de acesso a serviços, como eventos culturais, assinaturas de *streaming* ou SaaS, mantendo praticidade nos mecanismos de controle de acesso, porém adicionando toda a segurança de um sistema de *blockchain*.

Palavras-chave: Non-fungible token; Blockchain; Utility token;

ABSTRACT

Utility tokens are any digital asset that has a benefit attached to it, whether physical or digital, in addition to its speculative value. Benefits can include access to a certain group of services, participation in prize draws, discounts on future purchases, or basically any quality that separates the holders of such tokens from ordinary consumers. Non-fungible tokens (NFTs) are examples of digital assets that also have the characteristic of being unique and indivisible, as well as being validated via blockchain-based mechanisms. The use of NFTs as utility tokens to access services could represent a major revolution in terms of security and practicality, integrating the physical and virtual worlds. This paper seeks to provide information on the use of NFTs, covering their various applications, their operation and the creation process, as well as exploring different ways of solving common problems in accessing services (whether physical or digital) such as duplicate and/or shared access, credential forgery or even currency exchange. In this way, the aim is to exemplify the usefulness of NFTs in solving the obstacles currently present in controlling access to services, such as cultural events, streaming subscriptions or SaaS, while maintaining the practicality of access control mechanisms, but adding all the security of a blockchain system.

Keyword: Non-fungible token; Blockchain; Utility token;

LISTA DE ILUSTRAÇÕES

Figura 1 - Funcionamento de um login via QR Code (adaptado de YANG,ZHANG,LANTING, 2016)

Figura 2 - Gráfico de dispersão do número de artigos publicados sobre o tema

Figura 3 - Nuvem de palavras elaborada com o uso do software Rayyan

Figura 4 - Exemplo do processo de criação e transferência de um NFT (adaptado de ALNUAIMI et al. 2022)

Figura 5 - Fluxo de criação de um NFT na rede solana

Figura Suplementar 1 - Trecho de código para conexão com a rede solana

Figura Suplementar 2 - Trecho de código utilizado para identificar o usuário da conexão ao Metaplex

Figura Suplementar 3 - Função responsável por criar a coleção de NFTs

Figura Suplementar 4 - Função responsável por criar a CandyMachine

Figura Suplementar 5 - Função de atualização da *Candy Machine*

Figura Suplementar 6 - Função de adição de itens à *Candy Machine*

Figura Suplementar 7 - Função de cunhagem dos NFTs

LISTA DE TABELAS

Tabela 1 - Artigos encontrados, aceitos, rejeitados e duplicados

Tabela 2 - Lista de artigos e suas contribuições para a discussão

LISTA DE SIGLAS

NFT - *Non-fungible token* (Tokens não fungíveis)

DLT - *Distributed Ledger Technologies*

SC - Smart Contracts

QR - Quick Response

SUMÁRIO

1 INTRODUÇÃO	12
1.1 Objetivos	15
2 REVISÃO DE LITERATURA	17
2.1 DISTRIBUTED LEDGER TECHNOLOGIES	17
2.1.1 DLT PRIVADA	18
2.1.2 DLT PÚBLICA	18
2.2 BLOCKCHAIN	18
2.3 NON-FUNGIBLE TOKEN	19
2.3.1 - Aplicações das NFTs	20
2.3.1.1 - Real-World Based NFTS	20
2.3.1.2 - Metaverse Based NFTS	20
2.3.2 - Desafios de implementação	21
2.3.2.1 - Verificabilidade	21
2.3.2.2 - Disponibilidade	21
2.3.2.3 - Negociabilidade	21
2.4 USO DE QR CODES PARA AUTENTICAÇÃO	22
3 MATERIAIS E MÉTODOS	24
3.1 Mapeamento Sistemático	24
3.1.1 Questão Norteadora	25
3.1.2. Palavras-chave e String de busca	25
3.1.3 Critérios de Inclusão e Exclusão dos resultados	25
3.1.4. Desenvolvimento do Mapeamento	25
3.1.5 Saída	26
4. Aplicações e usos de NFTs	31
4.1 Produção e transação e validações de NFTs	31
4.2 Possíveis modelos de negócios com NFTs	33
4.3 Comparação de métodos de autenticação	34
5 Desenvolvimento de plataforma de gerenciamento de NFTs	37
5.1 Geração de chaves de identificação	37
5.2 Criação da coleção de NFTs	38
5.3 Criação da Candy Machine	38
5.4 População da Candy Machine	39
5.5 Cunhagem dos NFTs	39
6 RESULTADOS E DISCUSSÃO	40
7 CONCLUSÕES E TRABALHOS FUTUROS	42
8 REFERÊNCIAS	43
APÊNDICE A	47

1 INTRODUÇÃO

Os atuais modelos de controle de acesso a serviços, como por exemplo par de credenciais login e senha, código de barras, QR Code, entre outros, frequentemente baseiam-se em sistemas de segurança ou verificação que não necessariamente são completamente seguros (JUNEJA, 2020). No caso de logins e senhas, por exemplo, este procedimento pode estar suscetível a diversos modos maliciosos de descobrir as credenciais de um usuário. Além disso, senhas podem ser facilmente compartilhadas entre diferentes usuários, fazendo com que seja possível a um cliente contratar um serviço e compartilhá-lo com diversas pessoas sem custo adicional. Também é relevante o caso de replicação de imagem para códigos de barras ou QR Codes, em que uma imagem do código original, como uma impressão de tela ou até uma fotografia, pode ser escaneada e retornar o mesmo resultado do código original, possibilitando assim a realização de fraudes de acesso, em que uma pessoa replica a imagem de um código e a utiliza para acessar um evento ou serviço, passando-se pelo detentor do direito original.

Frente a esse contexto, as DLTs (*Distributed Ledger Technologies*), como a *blockchain*, emergem como alternativas inovadoras para fazer frente a tais desafios (WANG *et al.*, 2021).

Uma *blockchain* é uma *dlt* baseada em uma estrutura de cadeia de blocos, onde cada bloco tem um código hash único gerado a partir das informações nele armazenadas e todos os blocos, salvo o primeiro, contêm uma referência para o bloco anterior. Deste modo, é possível saber qual é o bloco antecessor direto de um bloco, garantindo que caso haja alguma alteração em algum dos blocos, seu código *hash* correspondente será alterado, de forma que inviabilize a verificação de seu conteúdo, fazendo com que todos os blocos subsequentes se desconectem dele e dos anteriores. Com essa tecnologia, uma *blockchain* consegue garantir a integridade de seus dados, pois uma vez que uma alteração fere toda a estrutura da rede, não há interesse, utilidade, ou mesmo viabilidade alguma em alterar os blocos já inseridos (SHALLIT, 1999; JAVAID *et al.* 2022).

Existem diversas redes *blockchain* atualmente, sendo as mais populares a rede Ethereum, Bitcoin, BSC (*Binance Smart Chain*), Solana e Polygon (BUTERIN, *et al.*, 2014; NAKAMOTO, 2008; HUANGSUYU *et al.*, 2020; YAKOVENKO, 2018).

Cada uma das redes possui seu próprio algoritmo de consenso, que é o

mecanismo responsável por garantir a integridade dos dados antes que os mesmos sejam permanentemente inseridos na rede. Tais algoritmos são divididos em duas categorias, PoS (*proof of stake*) e PoW (*proof of work*). A segunda e mais popular categoria (usada atualmente pela rede Bitcoin), consiste em um programa com cálculos matemáticos, que exigem grande esforço computacional, que são resolvidos pelos computadores presentes na rede, sendo que cada vez que um usuário consegue solucionar um código por completo ele recebe como recompensa uma quantidade de criptomoedas daquela rede.

Já o algoritmo de *proof-of-stake* consiste em usuários da rede bloquearem certa quantidade de seus cripto ativos e se transformarem em validadores da rede. Assim, esses usuários funcionam como pontos da rede para validarem as transações e adicionar informações aos novos blocos. Estes, por sua vez, são recompensados com certas quantidades de cripto-ativos referentes a um percentual definido pela rede de seus ativos bloqueados. Esse funcionamento financeiramente assemelha-se a uma renda fixa onde o dinheiro fica temporariamente bloqueado e recebe-se uma renda mensal a partir do mesmo (KRÓL, 2021).

Dentre essas alternativas, destaca-se o *token* não fungível (NFT), que corresponde a um arquivo de mídia (seja ele imagem, vídeo, arquivo de texto ou até mesmo áudio) assinado digitalmente dentro de uma *blockchain*. Ou seja, trata-se de um arquivo de mídia que tem seus metadados adicionados a um bloco de dados pertencente a uma *blockchain* conjuntamente a um código hash único gerado, preservando dessa forma a originalidade de tal registro e garantindo que aquela mídia representa a unidade inicial e original. O surgimento dos NFTs é relativamente recente, tendo ocorrido em 2014 e avançado significativamente em 2017 (BOIDO; ALIANO, 2023) e desde então, tem despertado rapidamente o interesse de investidores e ganhado popularidade em diversas áreas de aplicação. Embora ainda seja considerado um mercado imaturo, NFTs têm experimentado um crescimento significativo (KHAN *et al.*, 2022).

No âmbito da tecnologia *blockchain*, está ocorrendo uma série de transformações significativas, e os *tokens* não fungíveis (NFTs) desempenham um papel fundamental nessa evolução.

Em meio às restrições e bloqueios que foram impostos durante a pandemia da COVID-19, por exemplo, observou-se um aumento significativo na área,

impulsionado pelo aumento da necessidade das pessoas de passarem longos períodos compartilhando espaços *online*. Essa mudança nas circunstâncias resultou na criação de novos hábitos e comportamentos, incluindo o desenvolvimento bem-sucedido do Metaverso, que está sendo impulsionado pelos dispositivos de realidade aumentada e virtual, os quais operam na camada da experiência (KHATI *et al.*, 2022).

O metaverso é um novo espaço digital visando reproduzir uma sociedade, porém dentro do mundo virtual. Dessa forma, tenta possibilitar a interação entre as pessoas de forma virtual, assim como reproduzir partes comuns da sociedade nesse “novo mundo”, como vestimentas, acessórios, pertences, ativos e até mesmo encontros e eventos sociais. O papel da *blockchain* dentro desta nova tecnologia é justamente o de fornecer a segurança dos dados e garantir que os ativos digitais ali presentes sejam corretamente atrelados aos usuários aos quais pertencem. Com os blocos de dados de uma *blockchain* sendo interligados e validados através do código de hash único de cada bloco, torna-se possível manter a integridade das informações ali mantidas e impedir que as mesmas sejam alteradas ou corrompidas uma vez gravadas nesse banco de dados distribuído.

De maneira geral, é possível “tokenizar”, ou seja gerar uma informação digital correspondente, para uma variedade de ativos, atrelando-os a códigos e informações dentro de uma *blockchain*, com o intuito de validar sua originalidade dentro desta rede de dados. Isso pode ser relevante para objetos como obras de arte, peças musicais, itens colecionáveis, selos postais raros, imóveis e obras de arte físicas, por meio da tecnologia dos *tokens* não fungíveis. Esses ativos podem ser digitalmente representados e registrados em uma *blockchain*, proporcionando uma forma de garantir sua autenticidade, propriedade e rastreabilidade.

Em termos simples, a cunhagem de um NFT envolve a conversão de um arquivo digital específico em um token único e indivisível, representado por um conjunto de metadados e um código hash único presente na *blockchain* de escolha. Esse processo assegura que o conteúdo seja permanentemente registrado em um banco de dados descentralizado ou livro-razão distribuído, onde não poderá ser modificado ou excluído. A imutabilidade, característica essencial dos tokens não fungíveis, representa uma das principais vantagens desses ativos digitais, e pode ser garantida graças ao funcionamento das redes de *blockchain*, o qual consiste em

um conjunto de blocos de dados (cada um deles identificado por um código hash único gerado a partir dos dados do bloco) interligados de forma que apenas o bloco seguinte recebe o código de seu bloco anterior, ou seja, o bloco “N+1” sabe que é subsequente ao bloco “N”, porém o contrário não é verdadeiro. Essa forma de organização permite que, caso as informações de um bloco “N” sejam alteradas, o código hash desse mesmo bloco também será alterado e então o bloco “N+1” não mais o reconhecerá como antecessor e se separará dos blocos anteriores alterados. Com essa organização, é possível fornecer uma prova concreta de autenticidade e propriedade de um item digital.

Após a cunhagem de um arquivo como um NFT, ele passa a ser passível de compra, venda ou negociação de forma segura e transparente no mercado digital (PUTZ *et al.* 2020). Essa tecnologia tende a se expandir e despertar o interesse de um público crescente, à medida que novas aplicações para os NFTs são descobertas ao longo do tempo, pois antes, os mecanismos existentes para a verificação e proteção da propriedade de ativos digitais eram vulneráveis a adulterações, resultando em perdas consideráveis (REHMAN *et al.*, 2021; BELK, 2022).

1.1 Objetivos

Observando o crescente número de pesquisas acerca do tema e da busca por novas tecnologias de segurança, este trabalho visa estudar questões relacionadas à implementação da tecnologia de NFT como alternativa para os modelos de autenticação atualmente usados, e também, avaliar as possíveis aplicações que um *utility token* pode apresentar.

Através de uma revisão sistemática incluindo diversos artigos da área, mostram-se propostas para a inserção de NFTs como alternativa para verificação de posse de ativos (físicos e digitais) assim como usos possíveis de NFTs como *utility tokens*. Um estudo de caso de implementação de uma plataforma de gerenciamento de NFTs também é apresentado.

Com a revisão sistemática este trabalho visa exemplificar quais as atuais aplicações de NFTs já existentes, como os mesmos foram implementados nos projetos já desenvolvidos e com isso confirmar a viabilidade no uso desta tecnologia em modelos de negócio inovadores.

Já o estudo de caso desenvolvido tem como foco exemplificar a forma como uma coleção de NFTs pode ser criada, como realizar o gerenciamento da mesma e também analisar a complexidade envolvida nesse processo, buscando entender quanto esforço seria necessário por parte do responsável por implementar esta tecnologia em uma solução.

2 REVISÃO DE LITERATURA

2.1 *DISTRIBUTED LEDGER TECHNOLOGIES*

DLT (*Distributed Ledger Technology*) é um termo amplo utilizado para descrever sistemas que processam dados de forma descentralizada, envolvendo múltiplas partes interessadas em ambientes confiáveis. Essa tecnologia emergiu como uma solução inovadora para enfrentar desafios associados à confiabilidade, segurança e eficiência na gestão de dados, ganhando destaque com a publicação do whitepaper do Bitcoin por Satoshi Nakamoto (NAKAMOTO, 2008).

Diferentemente dos sistemas centralizados tradicionais, nos quais uma autoridade central é responsável pelo armazenamento e gerenciamento dos dados, um DLT descentraliza a responsabilidade, distribuindo-a entre os participantes da rede. Os dados são registrados em um livro-razão distribuído, compartilhado e mantido por vários nós da rede. Cada nó possui uma cópia idêntica do livro-razão e desempenha um papel ativo na validação e consenso dos registros. Esse mecanismo descentralizado reduz os riscos de fraudes, manipulações ou falhas únicas. Essa rede estruturada e distribuída de nós protege e compartilha dados de forma criptografada em um registro público verificável, garantindo a integridade e a privacidade dos dados, tornando o sistema altamente seguro (BENOS, 2017).

A aplicação da DLT abrange diversos setores, incluindo gerenciamento de informações, pagamentos, aquisições, gestão da cadeia de suprimentos, regulamentações e conformidade, gestão da construção, resolução de disputas e sistemas tecnológicos. Essa tecnologia possibilita a criação de redes confiáveis e transparentes, nas quais as transações e os registros podem ser verificados por todos os participantes, resultando em um aumento da confiança e da eficiência dos processos (LI *et al.*, 2021).

Embora DLTs apresentem benefícios promissores, é relevante ressaltar a existência de seus diferentes tipos, como a DLT privada e a DLT pública. Uma DLT privada envolve a participação de atores específicos que possuem autorização para acessar e validar os dados, enquanto uma DLT pública permite que qualquer usuário da rede participe como um nó validador. Ambas as abordagens possuem vantagens e desafios distintos, e a escolha entre elas depende dos requisitos específicos de cada aplicação.

2.1.1 DLT PRIVADA

Uma DLT privada é caracterizada pela exigência estrita de permissões para os nós participarem da rede. Esses tipos de DLTs adotam uma arquitetura distribuída em vez de descentralizada. Além disso, apresentam menor transparência em sua natureza devido à presença de uma hierarquia de acesso baseada em funções, na qual os validadores são designados manualmente, em contraste com a adoção de um protocolo de consenso (NATARAJAN, 2017).

2.1.2 DLT PÚBLICA

Uma DLT pública, também conhecida como DLT sem permissão, é caracterizada pela sua abertura a qualquer usuário na rede, permitindo que eles ingressem na rede funcionando como um nó da mesma. Essas DLTs seguem protocolos de consenso que permitem que os usuários na rede visualizem e validem transações de dados.

As DLTs públicas também são caracterizadas por sua natureza descentralizada e distribuída, sendo exemplos desse tipo de DLT as criptomoedas Bitcoin e Ethereum, que são construídas com base na tecnologia *blockchain* (NATARAJAN,2017).

2.2 BLOCKCHAIN

A tecnologia *blockchain* é uma estrutura de dados específica e especializada utilizada em sistemas de registros distribuídos. Ela opera como um mecanismo para armazenar e transmitir dados por meio de blocos interligados, formando uma cadeia digital contínua. Essa estrutura é caracterizada pelo uso de métodos criptográficos e algorítmicos avançados, que garantem a integridade, segurança e imutabilidade dos dados registrados (STUBLIC, 2023).

Através do emprego desses mecanismos, a *blockchain* é capaz de registrar e sincronizar informações de forma confiável em uma rede descentralizada, sem depender de uma autoridade central. Essa abordagem descentralizada e praticamente imutável de registro de informações oferece benefícios significativos em termos de transparência, resistência a manipulações e confiança no armazenamento e transmissão de dados.

Na área das artes digitais, por exemplo, a tecnologia de *blockchain* desempenha um papel fundamental e apresenta uma série de casos de uso relevantes. Entre eles, destacam-se os registros de procedência e autenticidade, que permitem rastrear a origem e verificar a autenticidade das obras de arte. Outra aplicação importante é a possibilidade de estruturas de participação fracionada e compartilhamento de benefícios, permitindo que os investidores possam adquirir frações de propriedade de uma obra de arte e compartilhar os retornos financeiros gerados por ela. Adicionalmente, a tecnologia *blockchain* oferece novas formas de registro de direitos autorais, proporcionando maior transparência e segurança no gerenciamento dos direitos de propriedade intelectual. Através de contratos inteligentes baseados em Ethereum e *tokens*, é possível estabelecer acordos e transações específicas relacionadas a investimentos e direitos autorais no contexto das artes (WHITAKER, 2019).

2.3 NON-FUNGIBLE TOKEN

Non-Fungible Tokens (NFTs) são ativos digitais com informações de propriedade baseados em *blockchain* referentes a quaisquer produtos (arquivos digitais) colecionáveis (Boido, Aliano, 2023). Isto é, são metadados validados através da tecnologia de uma *blockchain* legitimando a propriedade de um produto colecionável digital e/ou físico. NFTs ganharam ampla relevância e despertaram interesse de muitos nos últimos anos. Desde sua criação em 2017 até cerca de 2020 pouco se discutiu sobre essa tecnologia ou até mesmo foi possível ver a mesma tendo algum uso relevante. Porém, de 2020 para frente foi possível perceber um crescimento exponencial no interesse sobre o assunto, tendo em vista que em agosto de 2022 haviam 150 artigos publicados sobre o tema, sendo 135 (9% do número total) deles desenvolvidos entre 2021 e 2022 (Nobanee, Ellili, 2023).

Dois principais pontos que atraem muito os colecionadores em relação aos NFTs são o fato de serem atrelados (*linked*) a produtos colecionáveis (físicos ou não) independente de sua escassez (o que por sua vez faz com que seus preços possam ter grandes variações em curtos períodos de tempo, trazendo atenção para seu valor especulativo) e também o fato de serem associados a informações armazenadas em *blockchain*, de forma que todas as transações são de público acesso e permitem a comprovação de autenticidade, fazendo assim com que seja

garantida a segurança das transações.

2.3.1 - Aplicações das NFTs

Existem diversas aplicações para as NFTs, todas baseadas no princípio do uso de NFTs para comprovação de posse de um produto colecionável (físico ou digital), visando facilitar transações envolvendo este produto, de forma que todas as transações mantenham-se registradas na *blockchain* e sejam autenticadas pela rede e por seus usuários.

NFTs podem ser classificadas em dois principais grupos: *Real-World Based NFTs* e *Metaverse Based NFTs*.

2.3.1.1 - Real-World Based NFTS

NFTs baseadas no “mundo real” (ou *Real-World Based*) são os ativos relacionados à comprovação de propriedade de um item físico e palpável existente no mundo real, como por exemplo ingressos, obras de arte físicas, escrituras de propriedades ou até mesmo o documento de um veículo. Esse tipo de NFTs serve como uma proteção digital dentro da *blockchain*, armazenando de forma mais segura a comprovação de posse desses ativos físicos e protegendo o detentor dos mesmos. Entretanto, neste caso é possível ver um certo risco, uma vez que a NFT é atrelada a um produto físico e portanto perde todo seu valor caso o produto deixe de existir, seja destruído ou descartado.

2.3.1.2 - Metaverse Based NFTS

Por sua vez, NFTs baseadas no metaverso (ou *Metaverse Based*) são os ativos atrelados a itens digitais colecionáveis, como um item em um jogo, um acessório para um avatar digital, um “pedaço de terra” digital no metaverso ou até mesmo uma imagem de perfil em uma rede social. Neste caso, NFTs tendem a manter (e muitas vezes escalar) seu valor, visto que são atreladas a um produto que não pode ser facilmente destruído e/ou descartado, um produto que tende a ser “infinito” enquanto o mundo digital dure.

Com os dois subgrupos acima é possível classificar qualquer NFT e ter um melhor entendimento sobre o produto ao qual o *token* é vinculado. Pode-se também entender que o uso de NFTs é capaz de prover uma solução para o registro de

qualquer produto desejado, em uma DLT pública ou privada de fácil acesso e com ferramentas robustas de verificação e autenticação, seja este físico ou digital.

2.3.2 - Desafios de implementação

Embora esta nova tecnologia apresente-se de forma promissora para revolucionar a forma como é tratada a posse e propriedade de ativos digitais ou físicos, existem alguns pontos principais que devem ser considerados para sua real implementação em larga escala (ALI et al. 2023).

2.3.2.1 - Verificabilidade

Os metadados presentes na NFT precisam ser bem desenvolvidos para que seja possível comprovar através dos mesmos a titularidade de um usuário em relação ao produto ao qual a NFT está atrelado. Estes metadados residem na *blockchain* e são geralmente públicos e verificados pelos usuários da mesma.

2.3.2.2 - Disponibilidade

Deve-se sempre ser checada a disponibilidade da rede onde serão realizadas as transações, assim como a disponibilidade dos dados e dos ativos referentes a NFT e, por fim, também a disponibilidade de seus produtos atrelados. Por exemplo, se houver uma NFT atrelada a um produto físico é necessário checar a disponibilidade de tal produto antes que possa haver qualquer transação envolvendo a titularidade do mesmo.

2.3.2.3 - Negociabilidade

Talvez a propriedade principal a ser verificada, refere-se à capacidade de serem realizadas transações com aquela NFT, de forma autêntica e segura, assim como a transferência de posse do produto ao qual ela está atrelada, seja o mesmo físico ou digital.

2.4 USO DE QR CODES PARA AUTENTICAÇÃO

Atualmente, a tecnologia mais utilizada para desempenhar a função de autenticação aqui considerada para os NFTs são os QR Codes.

O mecanismo de QR Codes (*Quick Response Codes*) foi sugerido como uma solução para autenticação digital após pesquisas estadunidenses mostrarem que aproximadamente 60% da população adulta do país teria pelo menos 5 senhas diferentes *on-line*, sendo que cerca de 8% desta população chegava a ter 21 palavras chaves únicas, tornando-se um trabalho extremamente árduo cada vez que é preciso atualizá-las.

A tecnologia QR Code foi proposta como uma alternativa graças à sua facilidade de armazenar informações e de disponibilizá-las aliada ao grande crescimento do uso dos *smartphones*, tornando assim o QR Code uma opção viável devido ao fato de a maioria das pessoas terem acesso a um equipamento pessoal capaz de ler e processar esses códigos (YANG, ZHANG, LANTING, 2016).



Figura 1 - Funcionamento de um login via QR Code (adaptado de YANG,ZHANG,LANTING, 2016)

A Figura 1 ilustra o funcionamento de uma autenticação via QR Code. Inicialmente, o website ou plataforma na qual o usuário deseja se logar irá gerar um QR Code que deve ser escaneado pelo usuário para realizar a autenticação. Após esse procedimento ser realizado, as informações dentro da imagem serão lidas pelo *smartphone* do usuário, e então podem acontecer dois processos diferentes. Opcionalmente, o *smartphone* realiza diretamente a vinculação entre celular e website (como acontece por exemplo no acesso ao modelo virtual do *WhatsApp*), o que geralmente ocorre em aplicativos que trabalham com a vinculação da conta do usuário com um dispositivo móvel específico e único. De forma alternativa, o dispositivo pode abrir algum formulário de permissão onde o usuário verifica este login a partir do dispositivo móvel para realizar a autenticação no website.

Com o uso desta tecnologia, torna-se possível reduzir o uso total de senhas a apenas uma (sendo essa a senha de segurança do próprio dispositivo móvel) e também garantir a segurança desta autenticação, visto que com o uso de um dispositivo móvel verificado e protegido, as senhas do usuário não estarão armazenadas na internet e nem estarão vulneráveis a ataques de *hackers* por exemplo.

Vale ressaltar que ainda assim essa tecnologia apresenta o risco físico onde a perda de um aparelho móvel ou o furto do mesmo coloca o usuário em uma situação de perder o acesso às suas contas ou até mesmo de permitir que quem tenha furtado seu aparelho consiga acessar suas informações.

Embora seja hoje a tecnologia mais utilizada com este fim, os QR Codes apresentam possíveis problemas como facilidade de duplicação, risco de furto de dispositivos e certa vulnerabilidade que poderiam ser solucionados com o uso de NFTs, uma vez que estes se beneficiam da segurança e imutabilidade oferecidas pela *blockchain*, além de não dependerem da existência física do NFT para validar a posse do produto à ele atrelado.

3 MATERIAIS E MÉTODOS

3.1 Mapeamento Sistemático

Tendo em vista os NFTs e suas funcionalidades, este trabalho iniciou-se com a identificação de características e possíveis usos desta tecnologia, que foi realizada na forma de uma pesquisa sistemática.

A condução do mapeamento sistemático adotado nesta pesquisa seguiu a abordagem proposta por Nakagawa *et al.* (2017), composta por três fases: planejamento, execução e análise.

Na fase de planejamento, foram definidos o escopo e os critérios de seleção dos estudos a serem incluídos no mapeamento. Isso envolveu estabelecer as questões de pesquisa, a estratégia de busca, as fontes de pesquisa, as palavras-chave e seus sinônimos, a string de busca, os critérios de seleção (inclusão e exclusão) e os critérios de avaliação de qualidade dos artigos selecionados.

Na fase de execução, foram realizadas buscas abrangentes nas bases de dados selecionadas, utilizando os termos de busca definidos na fase de planejamento aplicando os critérios de inclusão e exclusão, triados de acordo com os critérios de seleção pré-definidos. Seguiu-se com a leitura completa dos artigos identificados, aplicando critérios de qualidade e extraindo os dados relevantes, visando garantir a consistência e a confiabilidade dos resultados.

Por fim, na fase de análise, os dados extraídos foram sintetizados e interpretados, identificando as tendências, lacunas e principais conclusões dos estudos incluídos no mapeamento. Essas informações foram utilizadas para responder às questões de pesquisa definidas no início do estudo e para a divulgação da discussão e dos resultados obtidos nas fases anteriores.

Essas fases são essenciais para auxiliar no processo de construção e avaliação do protocolo, garantindo a efetividade e a confiabilidade do mapeamento sistemático.

3.1.1 Questão Norteadora

As questões de pesquisa de um mapeamento sistemático são formuladas de forma ampla, visando identificar tendências de pesquisa. O objetivo principal foi identificar possíveis tendências de pesquisa, conforme mencionado por Nakagawa *et al.* (2017). Como resultado, o problema ao qual essa pesquisa buscou responder foi: Qual é o estado da arte das aplicações que utilizam NFTs?

3.1.2. Palavras-chave e String de busca

A escolha das bases de dados deu-se de acordo com a sua relevância na área de estudo, sendo estas: ScienceDirect, Scopus e IEEE Digital Library.

Após um levantamento inicial as palavras-chave escolhidas foram *Blockchain*, *Non-fungible token*, *Utility token*, *Authentication*, *multi-tier authentications* e *QR-code*.

Os Strings de busca foram elaborados com base nos termos de interesse, que melhor atenderia aos objetivos da pesquisa,

(“Blockchain” AND “Non-fungible token”) OR (“Blockchain” AND “Utility token”) OR (“Authentication” AND “QR-code”)

3.1.3 Critérios de Inclusão e Exclusão dos resultados

Os critérios de inclusão adotados foram: apenas artigos de pesquisa e revisão já publicados; artigos que respondam às questões norteadoras da pesquisa.

Os critérios de exclusão foram: preprint (trabalhos ainda não publicados); não apresentam vínculo ao tema da pesquisa; não possuem título ou resumo; o texto completo não está disponível para acesso.

3.1.4. Desenvolvimento do Mapeamento

Na etapa de execução foram submetidas as strings em cada uma das bases escolhidas e os resultados foram inseridos na ferramenta de revisão Rayyan.ai para a triagem dos artigos, avaliando títulos e resumos, agilizando a triagem inicial, usando um processo de semi-automação e incorporando um alto nível de usabilidade neste processo.

Foram selecionados os artigos com base nos critérios já estabelecidos de inclusão ou exclusão. Também foram excluídos os arquivos em duplicidade. No total, 20 artigos foram selecionados para leitura completa, avaliação e extração de dados.

O maior motivo de rejeição dos trabalhos encontrados foi por não estarem usando NFTs, aplicabilidade de softwares e projetos não correlatos, uso de outros tipos de *tokens*, análises de risco financeiras ou IOT (internet das coisas) não estando adequados ao tema escolhido na pesquisa.

Plataforma	Encontrados	Aceitos	Rejeitados	Duplicados
Scopus	28	4	24	0
Science Direct	299	6	293	2
IEEE Digital Library	28	10	18	5

Tabela 1. Artigos encontrados, aceitos, rejeitados e duplicados.

Após a seleção, resultou em 4; 6; e 10 artigos para avaliação da qualidade e extração dos dados com base nas perguntas estabelecidas inicialmente das bases científicas Scopus, Science Direct e IEEE Digital Library, respectivamente.

3.1.5 Saída

Foram obtidos, então, os 20 documentos como listado na Tabela 2, sendo que todos foram lidos na íntegra e tabulados de forma a apresentar os resultados obtidos.

nº	Autores	Título	Contribuição
1	(Madine et al., 2022)	<i>Blockchain and NFTs for Time-Bound Access and Monetization of Private Data</i>	Uso da tecnologia blockchain e tokens não fungíveis (NFTs) para permitir o acesso com limite de tempo e monitoramento de dados privados.
2	(Battah et al., 2022)	<i>Blockchain and NFTs for Trusted Ownership, Trading, and Access of AI Models</i>	Uso da tecnologia blockchain e tokens não fungíveis (NFTs) para gerenciar direitos de propriedade e troca de modelos de IA de forma transparente, rastreável, auditável, segura e confiável.

3	(Chen et al., 2022)	<i>Toward Achieving Anonymous NFT Trading</i>	Segurança do usuário, sugere-se um esquema de troca para ocultar o endereço do proprietário do NFT durante a negociação.
4	(Karandikar et al., 2021)	<i>Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure</i>	Sistema de tokenização de ativos de energia para transação entre prosumidores, empresas de energia e provedores de armazenamento.
5	(Arcenegui et al., 2021)	<i>Secure combination of iot and blockchain by physically binding iot devices to smart non-fungible tokens using pufs</i>	NFTs inteligentes para representar dispositivos IoT (ativos físicos inteligentes).
6	(Di Angelo et al., 2021)	<i>Identification of token contracts on Ethereum: standard compliance and beyond</i>	Identificação dos tokens no Ethereum, seus dados de transação, verificando a conformidade dos contratos inteligentes.
7	(Jiménez, 2019)	<i>From the blockchain technology to the token economy</i>	Contextualização, avaliação das potencialidades e problemas das tecnologias blockchain e token.
8	(Colicev, 2023)	<i>How can non-fungible tokens bring value to brands</i>	Relação das NFTs com estratégias de marketing, unindo o físico ao digital.
9	(Far et al., 2022)	<i>A Review of Non-fungible Tokens Applications in the Real-world and Metaverse</i>	Aplicações de NFTs no metaverso: gerenciamento de identidade e direito de propriedade de ativos digitais.
10	(Ali et al., 2023)	<i>A review of the key challenges of non-fungible tokens</i>	Uma visão geral da tecnologia NFT de última geração, padrões e propriedades.
11	(Huynh-The et al., 2023)	<i>Blockchain for the metaverse: A Review</i>	Aplicações do blockchain no metaverso, métodos, perspectivas técnicas e aplicações.
12	(Alnuaimi et al., 2022)	<i>NFT Certificates and Proof of Delivery for Fine Jewelry and Gemstones</i>	Demonstra como os tokens não fungíveis (NFTs) e a blockchain Ethereum podem ser usados para certificação digital, prova de propriedade, histórico de vendas e qualidade e prova de entrega de jóias finas e pedras preciosas.
13	(Hasan et al., 2022)	<i>Incorporating Registration, Reputation, and Incentivization Into the NFT Ecosystem</i>	Proposição de uma solução baseada em blockchain para o ecossistema NFT que incorpora o registro dos atores participantes, envolve um sistema de reputação descentralizado, fornece incentivos aos seus usuários por meio de recompensas e penaliza a má conduta.

14	(Madine et al., 2023)	<i>NFTs for Open-Source and Commercial Software Licensing and Royalties</i>	Sistema de licenciamento de software descentralizado baseado em Tokens Não Fungíveis (NFTs) e blockchain.
15	(Elmay et al., 2022)	<i>Using NFTs and Blockchain for Traceability and Auctioning of Shipping Containers and Cargo in Maritime Industry</i>	Uso de NFT para histórico de propriedade e a rastreabilidade dos contentores de transporte marítimo na indústria.
16	(Gebreab et al., 2022)	<i>NFT-Based Traceability and Ownership Management of Medical Devices</i>	Rastreabilidade de dispositivos médicos com gerenciamento de propriedade usando NFT.
17	(Hawashin et al., 2023)	<i>Using Composable NFTs for Trading and Managing Expensive Packaged Products in the Food Industry</i>	Uso da tecnologia de cadeia de blocos e os NFT para a gestão do comércio de produtos alimentares através da utilização de certificação digital e processo de comércio por contratos inteligentes.
18	(Tavares et al., 2023)	<i>Gamers' Reaction to the Use of NFT in AAA Video Games</i>	NFTs e seu uso em jogos.
19	(Kim et al., 2022)	<i>Perpetual Contract NFT as Collateral for DeFi Composability</i>	Método para lucro a partir de ativos bloqueados usando ERC-721 (NFTs) e contratos perpétuos.
20	(Turki et al., 2023)	<i>NFT-IoT Pharma Chain : IoT Drug traceability system based on Blockchain and Non Fungible Tokens (NFTs)</i>	Teste e validação da eficácia da abordagem na melhoria das cadeias de abastecimento de rastreabilidade dos medicamentos, bem como uma análise dos custos e da segurança da abordagem usando NFTs.

Tabela 2. Lista de artigos e suas contribuições para a discussão

A Tabela 2 exibe a lista dos artigos selecionados para a pesquisa e indica a contribuição de cada um. Com base nos critérios adotados nesta revisão sistemática, foi possível identificar um avanço nas produções científicas relacionadas ao uso das NFTs.

Podemos dividi-los em quatro temáticas, a primeira é a privacidade e monitoramento de dados para segurança do usuário, como a limitação de tempo de acesso a dados sensíveis ou ocultação de detalhes do proprietário (artigos nº 1, 3 e 20), gerando uma maior segurança ao usuário.

Em seguida, temos a questão de gerenciamento de propriedade e transparência nas transações (artigos 2, 9, 12 e 14 até 17 incluso). A combinação de *blockchain* e NFTs oferece uma solução transparente, rastreável e confiável para gerenciar direitos de propriedade, especialmente em licenciamento de softwares,

jogos online, trocas de modelos de IA e propriedade de ativos digitais, assim como no gerenciamento de identidade. Ligado a isso, temos o uso como certificação digital de ativos físicos, ampliando as suas funcionalidades, como dispositivos IoT, itens valiosos, dispositivos médicos, transporte marítimo, produtos alimentícios de alto valor agregado, jóias e pedras preciosas. Essa certificação digital é essencial por conter o histórico de propriedade, de vendas e a garantia de qualidade, incluindo a prova de entrega desses produtos ao destinatário.

Além dessas, temos a monetização através desses ativos digitais, seja através de NFTs e contratos perpétuos a partir de ativos bloqueados (artigos 4, 8, 13, 18 e 19), ou pela tokenização de ativos de energia, estabelecendo um sistema de transações entre empresas de energia, prosumidores e provedores de armazenamento.

Por fim, os artigos (5, 6, 7, 10 e 11) tratam do ecossistema de *blockchain* e NFTs e sua estrutura. Um sistema de reputação descentralizado, com registro de participantes, recompensas e penalidades por má conduta, tornando cada vez mais íntegro, impulsionando a inovação em diversas áreas.

Publicações do tema por ano até 2022

Número de documentos publicados por ano

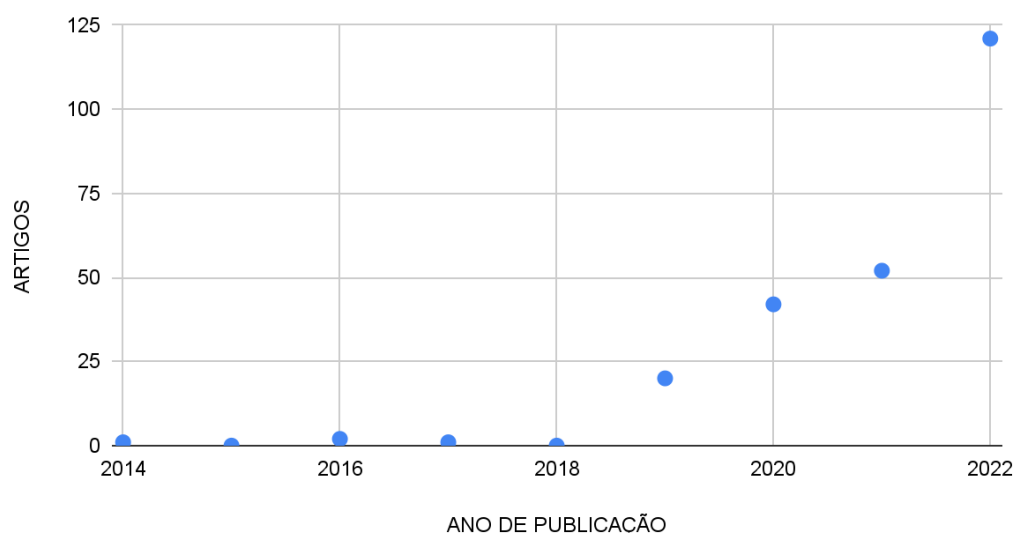


Figura 2 - Gráfico de dispersão do número de artigos publicados sobre o tema

A Figura 2, apresenta o número de publicações por ano foram publicados nos últimos anos (2014 a 2022), 121 só no ano de 2022 o que demonstra o avanço exponencial e relevância da temática abordada.

Através do software Rayyan também foi elaborada uma nuvem de palavras, uma representação visual onde, o tamanho de cada uma das palavras é proporcional à sua frequência nos documentos encontrados.

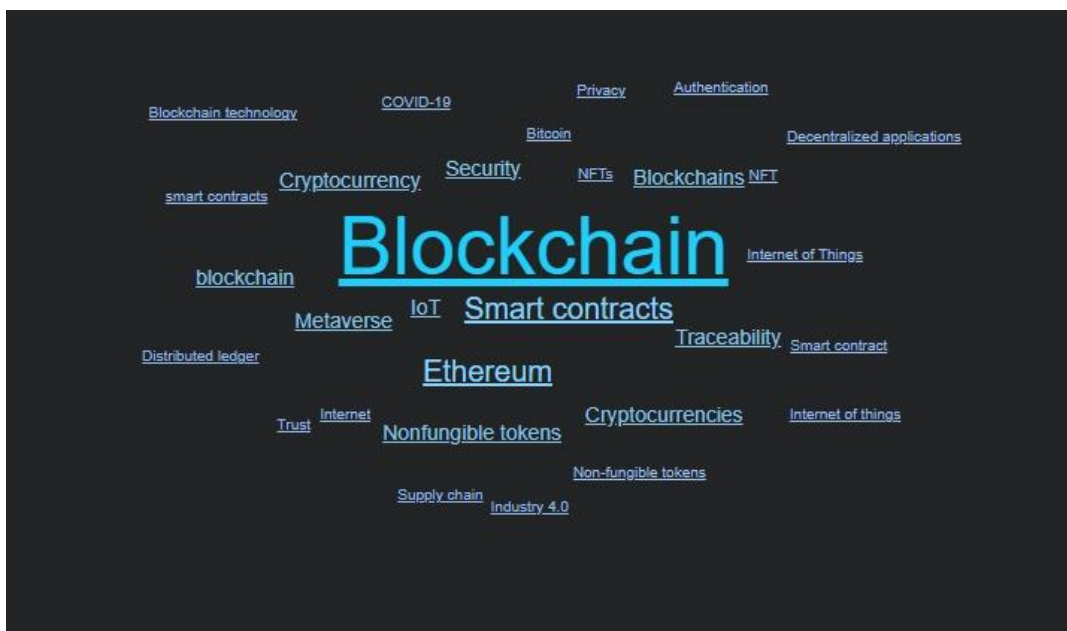


Figura 3 - Nuvem de palavras elaborada com o uso do software Rayyan

4. Aplicações e usos de NFTs

Dadas as propriedades dos NFTs, diferentes usos podem ser previstos para suas aplicações. Ações relacionadas às produções de NFTs e alguns exemplos significativos são apresentados a seguir.

4.1 Produção e transação e validações de NFTs

Antes de propor o uso de NFTs como uma alternativa para os métodos atuais de comprovação de posse e autenticação primeiramente é necessário entender mais a fundo o funcionamento deste processo: como ocorre a criação de NFTs, quem gerencia estes *tokens*, quais são as ferramentas utilizadas para gerenciá-los e como um usuário pode se envolver no processo de compra e venda dos *tokens*.

O principal responsável quando se fala sobre criação (*minting*) e gerenciamento de *tokens* NFT é o protocolo (ou *standart*) usado pela rede. Esse protocolo consiste em uma interface contendo um conjunto de funções como: aceitar pagamento, transferir ativos, checar saldo, entre outros. Cada rede pode contar com mais de um protocolo porém tendo sempre um funcionamento similar. Na rede Ethereum, o protocolo mais popular é o ERC-721, que define como os *Smart Contracts* (SC) - programas que são executados uma vez que certas condições pré-definidas são atingidas - devem interagir com a rede para realizar a criação de um NFT.

Estes *Smart Contracts*, uma vez implantados, são imutáveis, pois são compartilhados com todos os nós presentes na rede e se responsabilizam por chamar as funções contidas no protocolo para realizar as operações padrões de NFTs (criação, transferência, destruição).

Com essas ferramentas disponibilizadas pela rede *blockchain* é possível criar uma aplicação *frontend* descentralizada (ou DAPP) que possibilita ao usuário utilizar estes *Smart Contracts* para criar seus próprios NFTs, assim como comercializá-los abertamente (ALNUAIMI et al. 2022).

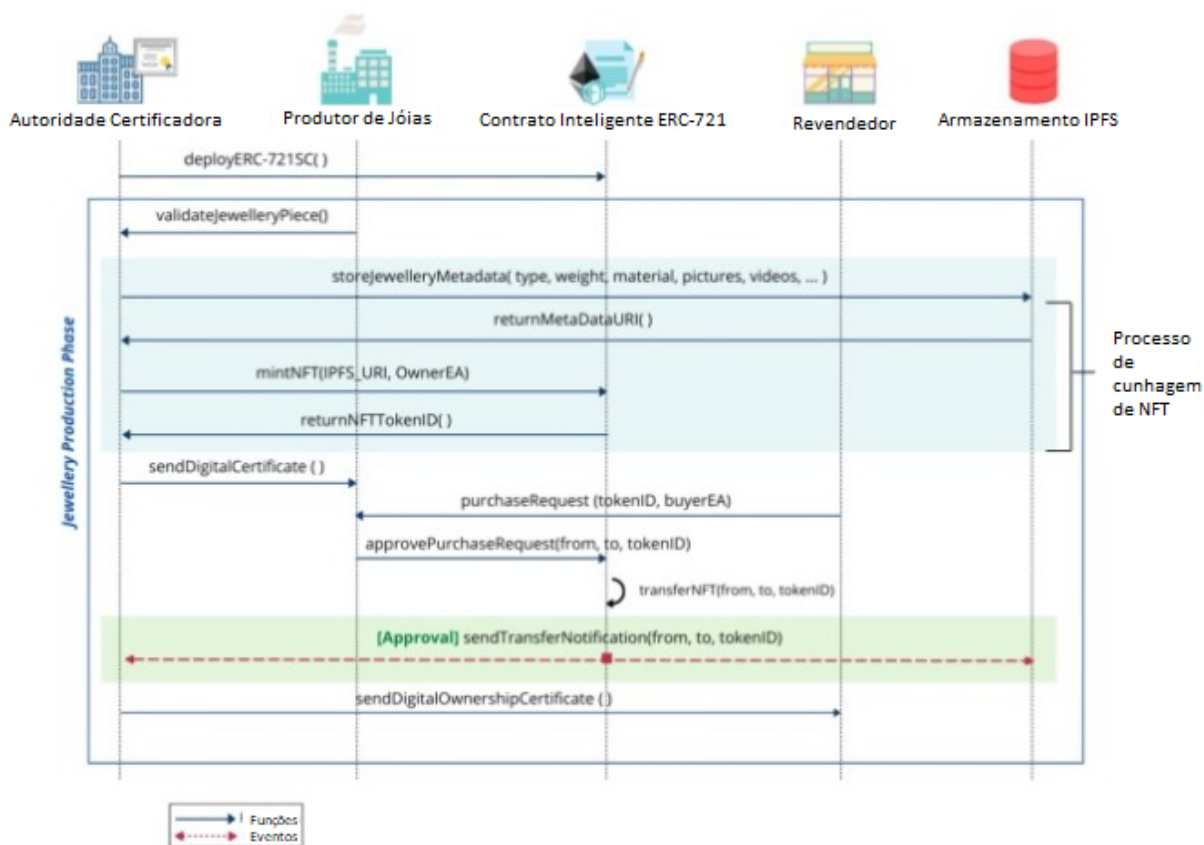


Figura 4 - Exemplo do processo de criação e transferência de um NFT (adaptado de ALNUAIMI et al. 2022)

A Figura 3 exemplifica um fluxo completo de um NFT que é vinculado a uma jóia rara e apresenta o processo desde a criação do produto, sua vinculação a um NFT, a entrega do produto físico e, por fim, a transferência do NFT como certificado digital de posse para o cliente final do produto.

Na primeira etapa do processo, um SC é implantado na rede Ethereum pela autoridade responsável por certificar jóias. Após isso, a entidade responsável pela fabricação das jóias envia os dados referentes ao produto desenvolvido X, validando-o junto à autoridade responsável que, por sua vez, utiliza o SC implantado para chamar a função de criação do NFT, fazendo com que sejam gerados e armazenados na rede Ethereum os metadados referentes àquele NFT, e recebendo uma URI responsável por apontar onde o mesmo está armazenado e, por fim, transfere o certificado digital à fábrica. Então, através de um DAPP *frontend*, o consumidor final pode contatar a fábrica com uma oferta para a compra deste produto que, quando aprovada, dispara o processo de entrega do produto físico (que pode ser feito por qualquer serviço de transporte). Uma vez que a entrega é

seguramente finalizada e anunciada, a fábrica utiliza um SC para realizar a transferência do NFT para o cliente.

Outra função importante que os SCs conseguem chamar do protocolo responsável pelas interações entre SCs e a *blockchain* é a função de validação que, com o ID do *token* NFT, consegue retornar o endereço *hash* associado ao real proprietário do mesmo, garantindo assim que um *token* pertence a um usuário específico.

Por fim, pode-se notar que através de processo similar e baseado neste precedente é possível criar um produto físico, vinculá-lo a um NFT e garantir que a transferência do mesmo só seja realizada após constatada entrega do produto ao consumidor, garantindo assim que só seja possível obter o certificado de posse de seu produto após realizar todo o processo necessário.

4.2 Possíveis modelos de negócios com NFTs

Com a crescente busca e grande facilidade de se criar e comercializar NFTs, surgem inúmeros potenciais modelos de negócio que podem ser desenvolvidos acerca deste tema.

Na seção 4.1 foi apresentado como exemplo um possível modelo de negócio onde poderia ser desenvolvido um *framework* que possa ser utilizado por qualquer tipo de companhia que venda produtos físicos e queira garantir a seus clientes maior segurança e confiabilidade.

Similar a este modelo e aproveitando das tecnologias de validação apresentadas, também seria possível desenvolver um sistema onde a posse de um NFT garantisse o acesso a eventos, como por exemplo, atrelar um NFT a um assento numa partida de futebol e garantir que o usuário que o possuir tenha acesso ilimitado às partidas enquanto em posse do NFT. Isso não só permitiria uma fidelização do cliente como também oferece ao mesmo uma possibilidade de revender o *token* adquirido quando não mais lhe for útil, fazendo com que o produto comprado não se torne uma perda financeira quando não mais lhe interessar.

NFTs também podem ser utilizados para bonificar contribuintes de projetos *open-source* visando trazer algum retorno para quem decide colaborar nessas situações tão relevantes para o desenvolvimento tecnológico (BATTAN et al. 2022).

Num outro cenário, com o constante aumento de desenvolvimento do Metaverso e a incessante busca dos usuários por status dentro da internet, é possível ainda que empresas optem por tratar a venda de acessórios digitais para avatares vinculando um NFT aos mesmos, assim ampliando sua base de clientes para além do mundo real (Colicev, 2023).

4.3 Comparação de métodos de autenticação

Após realizada a revisão da literatura, é possível elencar as vantagens que o uso de NFTs pode trazer aos processos de autenticação e também ao próprio processo de adquirir acesso a serviços ou benefícios especiais, atualmente garantidos por autenticação simples (login e senha comuns) ou por meio de QR Codes.

A primeira melhora possível seria solucionar o problema de segurança existente para os métodos atuais, uma vez que a autenticação via login e senha tem inúmeras vulnerabilidades como vazamento de dados, ataques de *SQL INJECTION*, ou até mesmo casos onde o usuário acessa uma conta em um computador público de forma que alguém possa estar “espionando” enquanto o usuário digita suas palavras chaves. Já o uso de *QR Codes*, embora não apresente essas vulnerabilidades, ainda demonstra riscos como a perda de um dispositivo móvel ou até mesmo o fato de que uma foto do código de um ingresso físico pode ser utilizada para autenticação da mesma forma que o próprio ingresso. Ou seja, uma pessoa pode fotografar seu ingresso e utilizá-lo para acessar um evento no seu lugar, sem que você até mesmo saiba que isso ocorreu.

Já com o uso de NFTs isso seria impossível, pois uma vez que um NFT é atrelado a um ingresso físico, por exemplo. A propriedade deste é garantida através da verificação dos metadados da NFT, que por sua vez estão inseridos em uma *blockchain* que garante sua integridade e imutabilidade. Logo, até que o primeiro usuário transfira sua NFT para outro, a mesma só poderá ser verificada como propriedade deste.

Um problema muito presente em serviços (como *streaming*, acesso a plataformas e etc.) é o compartilhamento de acesso, onde se não for realizada a proteção correta um usuário pode “emprestar” seu *login* e senha para outro, de forma que com apenas um sendo real assinante da plataforma, diversos dispositivos consigam se conectar na mesma. Já com o uso de NFTs, essa prática se tornaria

inviável, pois para realizar a autenticação, o usuário deveria estar de posse da NFT. Ou seja, para compartilhar seu acesso seria necessário que se passe uma NFT ao domínio do usuário com quem deseja-se compartilhar o acesso, e este processo iria impedir o seu próprio acesso à plataforma. Para este caso, vê-se que embora não seja totalmente possível impedir o compartilhamento, é possível garantir que para dividir o acesso com outro usuário você precisaria primeiramente abrir mão do seu acesso enquanto o outro estivesse utilizando.

A implementação desta nova tecnologia de autenticação não só visa resolver problemas já existentes nos antigos métodos mas também oferece novos benefícios e possibilidades, principalmente em prol do consumidor. Ao garantir o acesso via NFT, o consumidor se vê com maior liberdade em relação ao prestador do serviço uma vez que ao finalizar o uso do mesmo não necessariamente precisa cancelá-lo, podendo simplesmente revender a posse a um novo interessado, às vezes até com certa valorização, fazendo assim com que seja mais interessante e rentável a assinatura de um serviço ao invés do consumo único de um produto, por exemplo.

Já para quem vende algum serviço, seja ele *online* ou um evento físico, torna-se interessante o uso da nova tecnologia pela maior facilidade de criar uma fidelidade com o consumidor, uma vez que se torna possível oferecer uma experiência completa ao consumidor, ao invés de um simples produto. O cliente passa a poder adquirir juntamente ao ingresso do evento uma arte colecionável daquela data, por exemplo, que pode ser guardada como recordação ou até repassada para um próximo. Esta possibilidade do repasse faz com que seja possível que o consumidor reduza seu custo, ou até obtenha certo lucro sobre o consumo de um produto, tornando-o assim muito mais acessível e atraente para um consumidor que muitas vezes não teria o poder aquisitivo de adquirir tal produto ou serviço.

As aplicações de NFT como autenticação se estendem amplamente desde o aspecto de solucionar problemas de segurança até a possibilidade de criarem novos modelos de negócio totalmente baseados na fidelidade do cliente e no modelo de colecionismo. Com esta nova tecnologia, um imenso leque de possibilidades se abre tanto para os colecionadores quanto para os organizadores de eventos, provedores de serviços de streaming, vendedores de cursos digitais entre outros.

A autenticação por *tokens* de utilidade possibilita inclusive a facilitação de

muitas burocracias atualmente existentes, visto que uma NFT pode até mesmo ser atrelada à propriedade de terrenos, imóveis, automóveis e etc. Como uma rede *blockchain* proporciona a imutabilidade de dados, assim como sua transparência e provém acesso público às suas informações de transações, seria possível que qualquer usuário consultasse a propriedade de qualquer NFT e dessa forma conseguisse verificar, por exemplo, a qual pessoa pertenceria certo automóvel, ou quem é o dono de um imóvel específico.

5 Desenvolvimento de plataforma de gerenciamento de NFTs

Para exemplificar como pode ser desenvolvido um sistema para gerenciamento de NFTs, foi esquematizado na Figura 5 um diagrama de fluxo demonstrando todo o processo para criação de uma coleção de NFTs dentro da rede Solana (rede escolhida para esse estudo de caso por conta das baixas taxas de transação). Neste diagrama também são apontadas as requisições, as respostas da rede *blockchain* e as funções da ferramenta Metaplex.

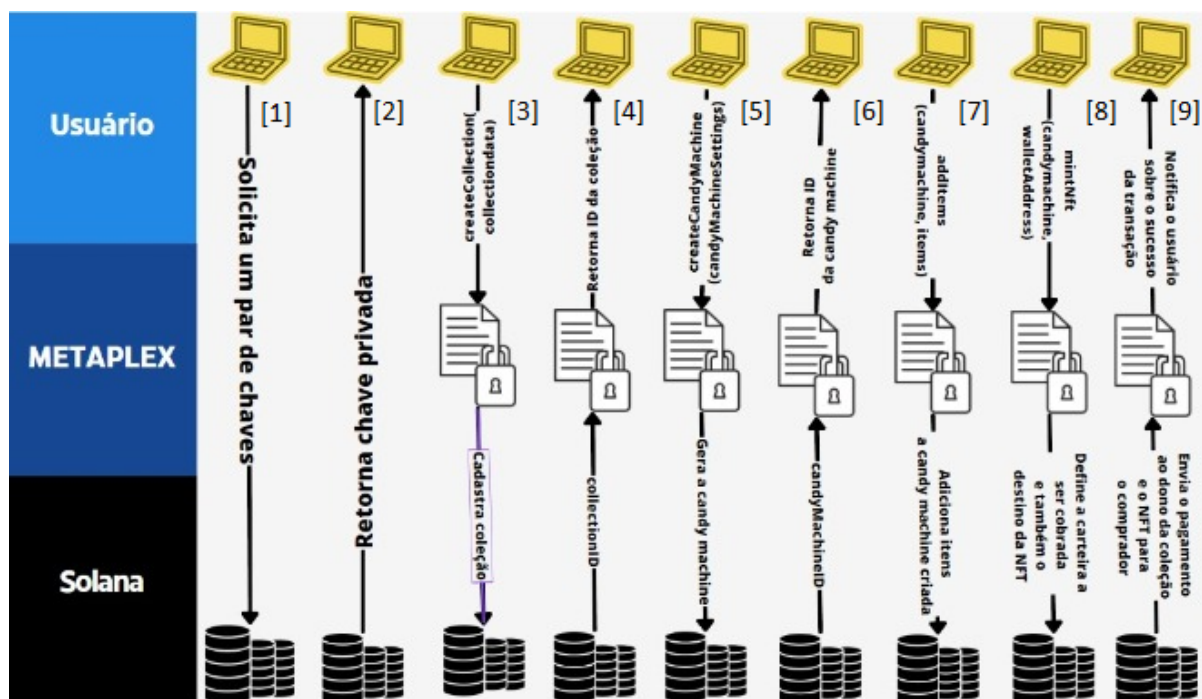


Figura 5 - Fluxo de criação de um NFT na rede solana

5.1 Geração de chaves de identificação

Nessa etapa foram desenvolvidos os trechos de código responsáveis por realizar os processos descritos na Figura 5.

Para realizar a solicitação de um par de chaves dentro da rede [1] é necessário instalar o pacote *solana tool suite*, como ilustrado na Figura 6, para ambientes Linux ou MacOS, ou então, usando o comando da Figura 7 para realizar o download do executável para sistemas Windows.

```
sh -c "$(curl -sSfL https://release.solana.com/v1.16.11/install)"
```

Figura 6 - Comando para instalação do pacote *solana tools suite* em ambiente Linux ou Mac OS

```
cmd /c "curl https://release.solana.com/v1.16.11/solana-install-init-x86_64-pc-windows-msvc.exe --output C:\solana-install-tmp\solana-install-init.exe --create-dirs"
```

Figura 7 - Comando para instalação do pacote *solana tools suite* em ambiente Windows

Após essa instalação, utiliza-se o comando de terminal `solana-keygen new --outfile ./nomeDoArquivo.json` para solicitar o par de chaves à rede solana e indicar o arquivo no qual deve ser armazenada a chave restrita retornada [2].

5.2 Criação da coleção de NFTs

Na segunda etapa, é necessário utilizar uma função presente na ferramenta *metaplex* passando como parâmetro um objeto contendo as propriedades: `name` (nome escolhido para a coleção), `uri`: (url do arquivo contendo os metadados da coleção), `sellerFeeBasisPoints` (taxa arbitrária do vendedor em porcentagem variando entre 0 e 100), `isCollection` com o valor `true` (propriedade responsável por definir que os NFTs pertencentes a esta coleção devem ser agrupados) e `updateAuthority` (propriedade onde será passado o par de chaves gerado para identificar o dono da coleção) [3].

A ferramenta *metaplex* recebe essa chamada, cadastra a nova coleção na rede com os dados passados e recebe como retorno o ID da coleção cadastrada e, por fim, retorna ao usuário este ID [4].

5.3 Criação da Candy Machine

Dentro da rede Solana as NFTs são armazenadas em estruturas chamadas *Candy Machines*. Essas estruturas são máquinas que imitam o funcionamento das máquinas de doce americanas, de forma que após a geração de uma *Candy Machine* é possível preenchê-la com NFTs de uma coleção e então a mesma irá liberar os NFTs um a um mediante ao recebimento do pagamento estipulado.

Logo, com o ID da coleção, é possível utilizar mais uma vez a ferramenta *metaplex* para gerar uma nova *candy machine*, passando para esta função um

objeto de configurações com as propriedades: `itemsAvailable` (um número inteiro definindo máximo de itens da coleção), `maxEditionSupply` (recomendado usar o valor 0 pois define quantas duplicatas podem existir na coleção para cada arte), `creators` (um vetor de objetos contendo cada um deles as propriedades `address` que seria a chave pública do criador e `share` variando de 0 a 100 para definir o percentual de participação deste criador) e por fim `solPayment` (outro objeto com as propriedades `amount` que define o preço de cada NFT e `destination` que recebe a chave pública de quem irá receber esses pagamentos).

Ao executar essa função, o usuário passa esses dados ao `metaplex` que cadastra essa nova *Candy Machine* na rede Solana [5], e então a rede responde com um ID da *Candy Machine* criada ao `metaplex` que por sua vez repassa este ID ao usuário [6].

5.4 População da Candy Machine

Com este ID registrado é possível popular essa máquina com os NFTs a serem vendidos. Esse processo é realizado através da ferramenta *metaplex* novamente, enviando a ela como parâmetro um vetor de objetos contendo os itens a serem adicionados e o ID da máquina a ser populada. Cada objeto possui duas propriedades: `name` (o nome do NFT) e `uri` (a url referente ao objeto). Após receber esses dados, a função de inserção presente no código da `metaplex` é executada e adiciona esses itens àquela *Candy Machine* criada na rede. [7]

5.5 Cunhagem dos NFTs

O processo final de cunhagem do NFT é realizado pela chamada do usuário à função de *mint* da `metaplex` que, por sua vez, repassa à rede a chave pública do usuário de quem deve ser debitada a compra e que deve receber o NFT após a conclusão do processo [8]. Por fim, a rede solana retorna uma resposta de sucesso à `metaplex`, que notifica o usuário sobre o sucesso da transação [9].

Esta lógica descrita pode ser implementada utilizando qualquer linguagem de código que seja capaz de acessar as ferramentas necessárias para comunicação com os *Smart Contracts* da rede escolhida. No apêndice deste trabalho estão disponibilizadas imagens referentes a um código desenvolvido em javascript implementando a lógica.

6 RESULTADOS E DISCUSSÃO

A busca por alternativas aos métodos de segurança atuais é evidente, seja em trabalhos buscando substituir senhas gráficas de autenticação por métodos utilizando arquivos XML (Juneja, 2020), ou com proposição do uso de *Bluetooth Low Energy* como alternativa para *QR Codes* em passagens de ônibus (Ferreira, Dias, Cunha, 2020). Vê-se que a preocupação com o melhoramento e a evolução dos atuais sistemas de segurança e autenticação é constante.

Embora ainda não haja estudos propondo o uso de NFTs como alternativa para autenticação digital, encontra-se um precedente para a substituição de *QR Codes* após a utilização de NFTs para substituir documentos em papel relativos à confecção, compra e venda de jóias e pedras preciosas (Alnuaimi et al. 2022).

Dentro desse estudo, os autores propõem a utilização de NFTs e da rede Ethereum para eliminar a necessidade de uma autoridade centralizada que garante a autenticidade e o certificado de posse de jóias, substituindo-a pela *blockchain* Ethereum, a fim de garantir maior automação, confiabilidade e transparência nos processos existentes desde a confecção das jóias até sua entrega ao consumidor final.

Dessa forma, vê-se possível replicar o processo proposto, uma vez que o mesmo obteve sucesso segundo os autores, para substituição de ingressos físicos para eventos, por exemplo, a fim de combater a falsificação dos mesmos, o cambismo e/ou monopólio de ingressos assim como evitar os riscos de danificação de ingressos impressos.

Entretanto, as NFTs não se apresentam promissoras apenas como substitutos para transações de produtos físicos. Em 2022 já foi proposto o uso de NFTs para garantir maior transparência e segurança para transações envolvendo modelos de Inteligência Artificial (Battah et al. 2022).

As aplicações possíveis para o uso de NFT como *utility tokens* são inúmeras. Há casos em que foi proposto o uso de tais *tokens* para o controle de acesso a software, de forma que a posse de um *token* possa ser utilizada para validar a compra de uma assinatura e, dessa forma garantir, uso único ao responsável pela assinatura da plataforma (Madine et al. 2023), ou para autorizar a presença em

jogos digitais. NFTs também podem ser úteis tanto para permitir que usuários tenham itens únicos e especiais que os diferenciam dos demais jogadores, quanto para criar um sistema de *Play-To-Earn*, em que os jogadores precisam adquirir um NFT para poder jogar e, conforme realizam tarefas ou completam missões dentro do jogo, são recompensados com dinheiro através de criptomoedas (Tavares et al. 2022). Nesta segunda implementação, o intuito é atrair a atenção do jogador para a compra do NFT, permitindo que seja apenas possível jogar após realizar a compra do *token*. Dessa forma, agrega-se valor ao NFT, visto que o acesso ao *game* é exclusivo para os colecionadores, e com as constantes recompensas monetárias por jogar, os cripto jogos passam a ser também um investimento ao invés de apenas mais uma opção de lazer para os usuários.

Muitas dessas possíveis aplicações ainda são bastante embrionárias e em raras vezes foram realmente implementadas fora de um ambiente de teste ou de um estudo dirigido. Dito isso, alguns pesquisadores acreditam que estamos à frente de uma iminente revolução no mercado digital (e até mesmo físico) onde empresas, marcas e negócios que se propuserem a ser pioneiras nessa nova jornada podem se beneficiar, e muito, de se adiantarem em relação ao uso desta nova tecnologia (Colicev, 2023).

7 CONCLUSÕES E TRABALHOS FUTUROS

Em suma, o uso de NFT como *tokens* de utilidade mostra-se extremamente promissor e se apresenta viável em diversas aplicações. Como toda nova tecnologia, ainda tem seus desafios e também sofre muito com a desconfiança, ou até mesmo com o medo do novo à frente da pouca difusão em modelos econômicos já estáveis.

Entretanto, ao realizar estudos acerca dessa nova tecnologia, observa-se que os benefícios e as reais aplicações de NFTs parecem superar seus desafios, além de do fato de estarem aptas a resolver diversos problemas encontrados nos sistemas e modelos atualmente utilizados.

Com a revisão sistemática realizada, foi possível então concluir que o uso de NFTs como *utility tokens*, apesar de embrionário, se mostra bastante viável e promissor, apontando que é possível acreditar que este talvez seja um novo ponto de inflexão do ponto de vista tecnológico e que o mundo pode estar frente a uma nova revolução digital.

A partir desse estudo, desenvolve-se uma proposta de trabalho futuro de desenvolvimento de um *marketplace* para compra e venda de NFTs utilizados como ingressos para partidas de futebol visando assim substituir os tipos de ingresso atuais garantindo maior segurança e também mais valor aos mesmos.

8 REFERÊNCIAS

ALI, Omar et al. A review of the key challenges of non-fungible tokens. *Technological Forecasting and Social Change*, v. 187, p. 122248, 2023.

ALNUAIMI, Noura et al. NFT Certificates and Proof of Delivery for Fine Jewelry and Gemstones. *IEEE Access*, v. 10, p. 101263-101275, 2022.

ARCENEGUI, Javier et al. Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs. *Sensors*, v. 21, n. 9, p. 3119, 2021.

BATTAH, Ammar et al. Blockchain and NFTs for trusted ownership, trading, and access of AI models. *IEEE Access*, v. 10, p. 112230-112249, 2022.

BECKSCHULTE, Sebastian et al. Digital Vehicle Protocol based on Distributed Ledger Technology in Production. *Procedia CIRP*, v. 107, p. 804-809, 2022.

BELK, Russell; HUMAYUN, Mariam; BROUARD, Myriam. Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets. *Journal of Business Research*, v. 153, p. 198-205, 2022. Disponível em: 10.1016/j.jbusres.2022.08.031 Acesso em: 07 de junho de 2023.

BENOS, Evangelos; GARRATT, Rod; GURROLA-PEREZ, Pedro. The economics of distributed ledger technology for securities settlement. Available at SSRN 3023779, 2017.

BOIDO, Claudio; ALIANO, Mauro. Digital art and non-fungible-token: Bubble or revolution?. *Finance Research Letters*, v. 52, p. 103380, 2023.

CHEN, Zhanwen; OMOTE, Kazumasa. Toward achieving anonymous nft trading. *IEEE Access*, v. 10, p. 130166-130176, 2022.

COLICEV, Anatoli. How can non-fungible tokens bring value to brands. *International Journal of Research in Marketing*, v. 40, n. 1, p. 30-37, 2023.

DI ANGELO, Monika; SALZER, Gernot. Identification of token contracts on Ethereum: Standard compliance and beyond. *International Journal of Data Science and Analytics*, p. 1-20, 2021.

ELMAY, Feruz K. et al. Using NFTs and blockchain for traceability and auctioning of shipping containers and cargo in maritime industry. *IEEE Access*, v. 10, p.

124507-124522, 2022.

FAR, Saeed Banaeian et al. A Review of Non-fungible Tokens Applications in the Real-world and Metaverse. *Procedia Computer Science*, v. 214, p. 755-762, 2022.

FERREIRA, Marta; DIAS, Teresa; CUNHA, João. Is Bluetooth Low Energy feasible for mobile ticketing in urban passenger transport? *Transportation Research Interdisciplinary Perspectives*, v. 5, 2020.

GEBREAB, Senay A. et al. NFT-based traceability and ownership management of medical devices. *IEEE Access*, v. 10, p. 126394-126411, 2022.

HARISH, Arjun Rachana et al. Blockchain-enabled digital assets tokenization for cyber-physical traceability in E-commerce logistics financing. *Computers in Industry*, v. 150, p. 103956, 2023.

HASAN, Haya R. et al. Incorporating registration, reputation, and incentivization into the NFT ecosystem. *IEEE Access*, v. 10, p. 76416-76433, 2022.

HAWASHIN, Diana et al. Using Composable NFTs for Trading and Managing Expensive Packaged Products in the Food Industry. *IEEE Access*, v. 11, p. 10587-10603, 2023.

HUYNH-THE, Thien et al. Blockchain for the metaverse: A Review. *Future Generation Computer Systems*, 2023.

JAVAID, Mohd et al. A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, p. 100073, 2022.

JIMENEZ, Maria Nieves Pacheco. From the blockchain technology to the token economy. *Derecho Pucp*, v. 83, p. 61, 2019.

JUNEJA, Kapil. An XML transformed method to improve effectiveness of graphical password authentication. *Journal of King Saud University-Computer and Information Sciences*, v. 32, n. 1, p. 11-23, 2020.

KARANDIKAR, Nikita; CHAKRAVORTY, Antorweep; RONG, Chunming. Blockchain based transaction system with fungible and non-fungible tokens for a community-based energy infrastructure. *Sensors*, v. 21, n. 11, p. 3822, 2021.

KHAN, Farhan et al. Enhancing non-fungible tokens for the evolution of blockchain technology. In: *2022 International conference on sustainable computing and data communication systems (Icscds)*. IEEE, 2022. p. 1148-1153.

KHATI, Prakhyat; SHRESTHA, Ajay Kumar; VASSILEVA, Julita. Non-Fungible Tokens Applications: A Systematic Mapping Review of Academic Research. In: 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2022. p. 0323-0330.

KIM, Hyongsung; KIM, Hyun-Sik; PARK, Yong-Suk. Perpetual Contract NFT as Collateral for DeFi Composability. IEEE Access, v. 10, p. 126802-126814, 2022.

KRÓL, Michał et al. Proof-of-prestige: A useful work reward system for unverifiable tasks. ACM Transactions on Internet Technology (TOIT), v. 21, n. 2, p. 1-27, 2021.

LI, Jennifer; KASSEM, Mohamad. Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction. Automation in construction, v. 132, p. 103955, 2021.

MADINE, Mohammad et al. Blockchain and NFTs for time-bound access and monetization of private data. IEEE Access, v. 10, p. 94186-94202, 2022.

MADINE, Mohammad et al. NFTs for Open-Source and Commercial Software Licensing and Royalties. IEEE Access, v. 11, p. 8734-8746, 2023.

METAPLEX. Candy Machine Settings | Metaplex Docs, c2023. Página inicial. Disponível em: <<https://docs.metaplex.com/programs/candy-machine/candy-machine-settings>>. Acesso em: 25/08/2023.

NAKAGAWA, E. Y., Mendonça, M., & Chaim, M. L. S. (2017). Mapeamento sistemático de literatura: conceitos básicos e aplicação na engenharia de software. In: XXVII Simpósio Brasileiro de Engenharia de Software (SBES)

NATARAJAN, Harish; KRAUSE, Solvej; GRADSTEIN, Helen. Distributed ledger technology and blockchain. 2017.

NOBANEE, Haitham; ELLILI, Nejla Ould Daoud. Non-fungible tokens (NFTs): A bibliometric and systematic review, current streams, developments, and directions for future research. International Review of Economics & Finance, 2022.

PUTZ, B. and PERNUL, G. "Detecting Blockchain Security Threats", 2020 IEEE International Conference on Blockchain (Blockchain), pp. 313320, 2020.

REHMAN, Wajiha et al. NFTs: Applications and challenges. In: 2021 22nd

International Arab Conference on Information Technology (ACIT). IEEE, 2021. p. 1-7.

SHALLIT, Jeffrey. Handbook of applied cryptography. by alfred j. menezes, paul c. van oorschot, and scott a. vanstone, the cryptographic imagination: Secret writing from edgar poe to the internet. by shawn james rosenheim. The American Mathematical Monthly, v. 106, n. 1, p. 85-88, 1999.

STUBLIĆ, Helena; BILOGRIVIĆ, Matea; ZLODI, Goran. Blockchain and NFTs in the Cultural Heritage Domain: A Review of Current Research Topics. Heritage, v. 6, n. 4, p. 3801-3819, 2023.

TAVARES, Rogério et al. Gamers' Reaction to the Use of NFT in AAA Video Games. Procedia Computer Science, v. 219, p. 606-613, 2023.

TRČEK, Denis. Cultural heritage preservation by using blockchain technologies. Heritage Science, v. 10, n. 1, p. 6, 2022.

TURKI, Mariem et al. NFT-IoT Pharma Chain: IoT Drug traceability system based on Blockchain and Non Fungible Tokens (NFTs). Journal of King Saud University-Computer and Information Sciences, v. 35, n. 2, p. 527-543, 2023.

WHITAKER, Amy. Art and blockchain: A primer, history, and taxonomy of blockchain use cases in the arts. Artivate, v. 8, n. 2, p. 21-46, 2019.

APÊNDICE A

Código javascript que implementa a lógica descrita na seção 5

```

2  const { Connection, Keypair, PublicKey } = require('@solana/web3.js');
3  const {
4    Metaplex,
5    keypairIdentity,
6    bundlrStorage,
7    toMetaplexFile,
8    toBigNumber,
9    CreateCandyMachineInput,
10   DefaultCandyGuardSettings,
11   CandyMachineItem,
12   toDateTime,
13   sol,
14   TransactionBuilder,
15   CreateCandyMachineBuilderContext
16 } = require('@metaplex-foundation/js');
17 const secret = require('./keypair.json');
18 const testWallet = require('./testWallet.json');
19 const conn = new Connection('https://api.devnet.solana.com', { commitment: "finalized" });

```

Figura Suplementar 1 - Trecho de código para conexão com a rede solana

```

20 const WALLET = Keypair.fromSecretKey(new Uint8Array(secret));
21 const METAPLEX = Metaplex.make(conn).use(keypairIdentity(WALLET));

```

Figura Suplementar 2 - Trecho de código utilizado para identificar o usuário da conexão ao Metaplex

```

29 async function createCollectionNft() {
30   const { nft: collectionNft } = await METAPLEX.nfts().create({
31     name: 'Test Name',
32     uri: NFT_METADATA,
33     sellerFeeBasisPoints: 0,
34     isCollection: true,
35     updateAuthority: WALLET,
36   });
37   console.log(`✅ - Minted Collection NFT: ${collectionNft.address.toString()}`);
38   console.log(`   https://explorer.solana.com/address/${collectionNft.address.toString()}?cluster=devnet`);
39 }

```

Figura Suplementar 3 - Função responsável por criar a coleção de NFTs

```

43 async function generateCandyMachine() {
44
45   const candyMachineSettings = {
46     itemsAvailable: toBigNumber(3), // Tamanho da coleção: 3
47     sellerFeeBasisPoints: 1000, // 10% Royalties da Coleção
48     symbol: "Test",
49     maxEditionSupply: toBigNumber(0), // 0 reproduções para cada NFT
50     isMutable: true,
51     creators: [{ address: WALLET.publicKey, share: 100 }],
52     collection: {
53       address: new PublicKey(COLLECTION_NFT_MINT), // Can replace with your own NFT or upload a new one
54       updateAuthority: WALLET,
55     },
56   };
57   const { candyMachine } = await METAPLEX.candyMachines().create(candyMachineSettings);
58   console.log(`✅ - Created Candy Machine: ${candyMachine.address.toString()}`);
59   console.log(`   https://explorer.solana.com/address/${candyMachine.address.toString()}?cluster=devnet`);
60 }

```

Figura Suplementar 4 - Função responsável por criar a CandyMachine

```

65 async function updateCandyMachine() {
66
67     const candyMachine = await METAPLEX.candyMachines().findByAddress({ address: new PublicKey(CANDY_MACHINE_ID) });
68     const { response } = await METAPLEX.candyMachines().update({
69         candyMachine,
70         guards: {
71             startDate: {
72                 date: toDateTime("2022-10-17T16:00:00Z")
73             },
74             mintLimit: {
75                 id: 1,
76                 limit: 2,
77             },
78             solPayment: {
79                 amount: sol(0.1),
80                 destination: METAPLEX.identity().publicKey,
81             },
82         }
83     })
84     console.log(`✅ - Updated Candy Machine: ${CANDY_MACHINE_ID}`);
85     console.log(`    https://explorer.solana.com/tx/\${response.signature}?cluster=devnet`\);
86 }

```

Figura Suplementar 5 - Função de atualização da Candy Machine

```

90 async function addItem() {
91     const candyMachine = await METAPLEX.candyMachines().findByAddress({ address: new PublicKey(CANDY_MACHINE_ID) });
92     const items = [];
93     for (let i = 0; i < 3; i++) {
94         items.push({
95             name: `QuickNode Demo NFT # ${i+1}`,
96             uri: NFT_METADATA
97         })
98     }
99     const { response } = await METAPLEX.candyMachines().insertItems(
100     {
101         candyMachine,
102         items: items,
103     },
104     {
105         commitment: 'finalized'
106     }
107 );
108 console.log(`✅ - Items added to Candy Machine: ${CANDY_MACHINE_ID}`);
109 console.log(`    https://explorer.solana.com/tx/\${response.signature}?cluster=devnet`\);
110 }

```

Figura Suplementar 6 - Função de adição de itens à Candy Machine

```

114 async function mintNft() {
115     const candyMachine = await METAPLEX.candyMachines().findByAddress({ address: new PublicKey(CANDY_MACHINE_ID) });
116     let { nft, response } = await METAPLEX.candyMachines().mint(
117     {
118         candyMachine,
119         collectionUpdateAuthority: WALLET.publicKey,
120     },
121     {
122         commitment: 'finalized'
123     }
124 );
125 console.log(`✅ - Minted NFT: ${nft.address.toString}`);
126 console.log(`    https://explorer.solana.com/address/\${nft.address.toString}?cluster=devnet`\);
127 console.log\(`    https://explorer.solana.com/tx/\\${response.signature}?cluster=devnet`\\);
128 }

```

Figura Suplementar 7 - Função de cunhagem dos NFTs