



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba  
Campus Campina Grande  
Coordenação do Curso Superior de Tecnologia em Telemática

# **Tokens Não Fungíveis (NFT): características técnicas e oportunidades para profissionais de TI**

José Werlandiê A. Lacerda

Orientador: Elmano Ramalho Cavalcanti

Campina Grande, setembro de 2022

© José Werlandiê A. Lacerda



Instituto Federal de Educação, Ciência e Tecnologia da Paraíba  
Campus Campina Grande  
Coordenação do Cursos Superior de Tecnologia em Telemática

## **Tokens Não Fungíveis (NFT): características técnicas e oportunidades para profissionais de TI**

José Werlandiê A. Lacerda

Monografia apresentada à Coordenação do Curso de Telemática do IFPB - Campus Campina Grande, como requisito parcial para conclusão do curso de Tecnologia em Telemática.

Orientador: Elmano Ramalho Cavalcanti

Campina Grande, setembro de 2022

L131t Lacerda, José Werlandiê A.

Tokens não fungíveis (NFT): características técnicas e oportunidades para profissionais de TI / José Werlandiê A. Lacerda. - Campina Grande, 2022.

60 f. : il.

Trabalho de Conclusão de Curso (Curso de Tecnologia em Telemática) - Instituto Federal da Paraíba, 2022.

Orientador: Prof.Dr. Elmano Ramalho Cavalcanti.

1. Blockchain 2. Criptomoedas 3. Tokens não fungíveis - oportunidades I. Título.

CDU 004

# Tokens Não Fungíveis (NFT): características técnicas e oportunidades para profissionais de TI

José Werlandiê A. Lacerda

---

Orientador: Elmano Ramalho Cavalcanti

---

Membro da Banca: David Candeia Medeiros Maia

---

Membro da Banca: Katyusco de Farias Santos

Campina Grande, Paraíba, Brasil

Setembro/2022

# Agradecimentos

Gostaria de demonstrar minha gratidão principalmente ao meu grande amigo Theo, por ter me incentivado a procurar um tema ao qual tenho familiaridade e gosto, e ter inspirado a ideia. Também gostaria de expressar minha gratidão a meu pai e minha mãe por todo o apoio durante a jornada acadêmica, por fim agradecer ao meu orientador pela paciência e toda ajuda durante todo o trabalho.

# Resumo

Embora NFTs tenham um elevado potencial nos atuais mercados descentralizados, bem como uma gama de usos limitada apenas pela criatividade do desenvolvedor, a maioria das pessoas ainda a desconhecem. Muitas oportunidades promissoras podem ser destacadas. Este trabalho estima chamar a atenção para essa questão na medida em que apresenta uma visão geral sobre o estado-da-arte dos NFTs, detalhando suas principais características e as tecnologias utilizadas e suas principais oportunidades de aplicação no mercado. O principal objetivo desse trabalho é criar um material que co-relacione e destaque as oportunidades de atuação no mercado de NFT por profissionais da área de TI. Aplicou-se um questionário com estudantes do IFPB, *campus* Campina Grande, matriculados em cursos da área de informática. A análise dos dados revelou que a grande maioria dos participantes desconhece do potencial do mercado NFT. As principais oportunidades de atuação destacadas nesse trabalho fazem parte da Web3, a exemplo dos eventos virtuais, métodos de controle de acesso, aplicativos descentralizados, jogos e mineração de dados.

**Palavras-chave:** NFT, *blockchain*, criptomoedas, oportunidades.

# Abstract

While NFTs have high potential in today's decentralized markets, as well as a range of applications limited only by the creativity of the developer, most people are still unaware of it. Many promising opportunities can be highlighted. This work intends to draw attention to this issue by presenting an overview of the state of the art of NFTs, detailing their main characteristics and technologies used and their main opportunities for application in the market. The main objective of this work is to create a material that relates and highlights the opportunities for IT professionals to work in the NFT market. A questionnaire was applied to students from the IFPB, *campus* Campina Grande, enrolled in informatics-related courses. Data analysis revealed that the vast majority of participants are unaware of the potential of the NFT market. The main roles for IT professionals in the NFT market are inside the web3 ecosystem, such as virtual events, access control methods, decentralized applications, online games and data mining.

**Keywords:** NFT, blockchain, cryptocurrencies, opportunities.

# Sumário

<b>Lista de Abreviaturas</b>	<b>x</b>
<b>Lista de Figuras</b>	<b>xi</b>
<b>1 Introdução</b>	<b>1</b>
1.1 Justificativa . . . . .	2
1.2 Objetivos . . . . .	3
1.3 Relevância e Contribuições . . . . .	3
1.4 Organização do Documento . . . . .	4
<b>2 Fundamentação Teórica</b>	<b>5</b>
2.1 Blockchain . . . . .	5
2.1.1 Propriedades . . . . .	8
2.1.2 Processo de Validação e Consenso . . . . .	9
2.1.3 Blockchain/Tokenização . . . . .	12
2.2 Criptomoedas . . . . .	12
2.2.1 Altcoin e Token . . . . .	14
2.2.2 Contratos Inteligentes . . . . .	15
2.2.3 Ethereum . . . . .	17
2.3 Tokens não fungíveis (NFT) . . . . .	19
2.3.1 História . . . . .	20
2.3.2 Conceito de um NFT . . . . .	21
2.3.3 Características dos NFTs . . . . .	21
2.3.4 Componentes . . . . .	22
2.3.5 Padrões de projeto . . . . .	24
2.3.6 Padrões de Token . . . . .	26
<b>3 Metodologia</b>	<b>28</b>
3.1 Hipótese . . . . .	29
<b>4 Análise dos Dados</b>	<b>32</b>
4.1 Discussão . . . . .	37

<b>5 Oportunidades</b>	<b>39</b>
5.1 Web3 . . . . .	39
5.1.1 Eventos Virtuais . . . . .	41
5.1.2 Chaves/controlado de acesso . . . . .	42
5.1.3 DApps . . . . .	42
5.1.4 Mineração de dados . . . . .	44
<b>6 Considerações Finais e Sugestões para Trabalhos Futuros</b>	<b>46</b>
6.1 Sugestões para Trabalhos Futuros . . . . .	47
<b>Referências Bibliográficas</b>	<b>48</b>

# Lista de Abreviaturas

ACID	<i>Atomicity Consistency Isolation Durability Programming</i> (Atomicidade, Consistência, Isolamento, Durabilidade)
ASICs	<i>Application-specific integrated circuit</i> (Circuito Integrado para Aplicações Específicas)
DApps	<i>Aplicativos descentralizados</i> (Aplicativos descentralizados)
DeFi	<i>Finanças Descentralizadas</i>
ERC	<i>Ethereum Request for Comments</i> (Solicitação de Comentários do Ethereum)
ETH	<i>Ether</i>
EVM.	<i>Ethereum Virtual Machine</i> (Máquina Virtual Ethereum)
ICO	<i>Initial Coin Offering</i> (Oferta Inicial de Moedas)
ID	<i>Identificador</i>
IFPB	<i>Instituto Federal da Paraíba</i>
IPFS	<i>Interplanetary File System</i> (Sistema de Arquivo Interplanetário)
LTC	<i>Litecoin</i>
NFT	<i>Non-Fungible Tokens</i> (Tokens Não Fungíveis)
P2P	<i>Peer to Peer</i> (Par a Par)
PoS	<i>Proof of Stake</i> (Prova de participação)
PoW	<i>Proof of Work</i> (Prova de trabalho)
PoA	<i>Proof of Authority</i> (Prova de Autoridade)
DPoS	<i>Delegated Proof of Stake</i> (Prova de Posse Delegada)
PoB	<i>Proof of Burn</i> (Prova de Queima ou Destruição)
SAND	<i>The Sandbox</i> (A caixa de areia)
TI	<i>Tecnologia da Informação</i>
USD	<i>United States Dollar</i> (Dollar dos Estados Unidos)

# Lista de Figuras

2.1	Exemplo de Bloco de uma blockchain [GOUVEIA 2021] . . . . .	6
2.2	Estrutura da básica blockchain [GOUVEIA 2021] . . . . .	7
2.3	Atualização de uma blockchain [Rebello <i>et al.</i> 2019] . . . . .	8
2.4	Exemplo simples de contrato inteligente . . . . .	15
2.5	Funcionamento básico de um contrato inteligente [Bruno Cardoso 2018] . . . .	16
2.6	Código básico para um contrato inteligente construído na plataforma <i>ethereum</i> [Bruno Cardoso 2018] . . . . .	17
2.7	Diagrama adaptado do Ethereum EVM [Ethereum Articles 2022] . . . . .	18
2.8	Fluxo de trabalho dos sistemas NFT [Wang <i>et al.</i> 2021] . . . . .	24
2.9	Padrões de Token NFT [Wang <i>et al.</i> 2021] . . . . .	27
3.1	Gráfico de interesse a respeito de NFT dos últimos 12 meses [ <i>orig.google Trends</i> ] . . . . .	30
3.2	Capitalização total do mercado NFT [Coingecko 2022] meses . . . . .	30
4.1	Relação total de participantes . . . . .	32
4.2	Divisão, percentual por curso . . . . .	32
4.3	Percentual em barras para o 3º questionamento . . . . .	33
4.4	Relação das respostas em barras . . . . .	35
4.5	Conhecimento sobre o mercado de NTF's e suas oportunidades" . . . . .	36
4.6	Nível de interesse dos participantes. . . . .	37
4.7	Análise conclusiva . . . . .	37
4.8	Relação das respostas . . . . .	38

# Capítulo 1

## Introdução

Os *tokens* não fungíveis (do inglês, *Non-fungible tokens* - NFT), é uma tecnologia de potencial que em forma exponencial que promete revolucionar o desenvolvimento da economia digital baseada na tecnologia *blockchain* [Fairfield 2022]. Um NFT é um tipo especial de ativo digital ou *tokens* que pode ser comprovado como único e cada um possui uma quantidade limitada ou seja, um item fungível, como o dinheiro, exemplo uma nota de de dois reais pode ser trocada por outra igual e de mesmo valor, já como seu nome já informa “*token* não fungível” não, ele vai representa algo específico, único, que não pode ser substituído [Blockchain e team 2021].

Grandes projetos experimentaram NFTs em vários casos de uso, incluindo jogos, identidade digital, licenciamento, certificados e obras de arte. Além disso, os NFTs possibilitam interoperabilidade de ativos através de diversas plataformas. Para ser específico, através do uso de um NFT um criador como por exemplo um artista ou desenvolvedor pode facilmente provar a existência e propriedade de ativos digitais na forma de vídeos, imagens, artes, ingressos de eventos, etc. O criador também pode ganhar *royalties* [Ethereum Articles 2022] cada vez que uma negociação é bem-sucedida em qualquer mercado NFT. Qin Wang professor da *Southern University of Science and Technology* afirma que "negociabilidade de histórico completo, liquidez profunda e interoperabilidade conveniente permitem que a NFT se torne uma solução promissora para a proteção de qualquer propriedade digital [Wang *et al.* 2021].

O NFT surgiu em 2017, sua valorização e popularização ocorreu entre o final do ano 2020 e início do ano de 2021, onde a venda de NFT foi estimada em 12 milhões no mês de dezembro de 2020 e atingiu um valor de 340 milhões em apenas dois meses (fevereiro de 2021) [Wang *et al.* 2021]. Esse desenvolvimento fez com que o NFT atraísse o olhar de diversos investidores com projetos audaciosos acumulando em agosto 2022 uma capitalização de mercado de 20,3 bilhões USD [Coingecko 2022]. Existe um interesse manifestado pelas pessoas em vários tipos de NFTs apesar do *Google Trends* revelar que este, tem diminuído bastante desde agosto. Mas, ainda é possível notar uma participação entusiasmada em projetos como jogos ou até mesmo negócios relacionados de compra e venda de ativos. Pode ser citado como exemplo o *CryptoKitties* um dos primeiros projetos NFT a ganhar visibilidade, o jogo foi

construído na rede *Ethereum*. Este jogo é um dos primeiros exemplos de um caso de uso de *blockchain* que não para uma moeda digital [Wang *et al.* 2021].

Posteriormente outros projetos também obtiveram grande sucesso, incluindo *Picasso Punks*, *Hashmasks*, *3DPunks*, *CryptoCats*, *NFT box*, *mir4*, *Ni no Kuni*, e etc [Binance Academy 2021]. Além de jogos e colecionáveis, os NFTs também promovem o desenvolvimento de arte, evento de bilheteria, e finanças [Ethereum Articles 2022]. Outros tipos de mercados circundantes se beneficiam dos NFTs, como *websites* de estatísticas (e.g. *NonFungible*, *DappRadar*, *NFT bank*, *DefiPulse*, *Coingecko*), que desempenham papéis de extrema importância onde os dados estatísticos são fornecidos ao público de forma atualizada e transparente, e *websites* onde a negociação pode ser realizada de forma segura como é o exemplo do *marketplace* (outros exemplos: *cryptoslam*, *Opensea*, *SuperRare*, *Nifty Gateway*, *Rarible*, *Zora*) [Wang *et al.* 2021].

Embora NFTs tenham um elevado potencial nos atuais mercados descentralizados, e uma gama de usos limitada apenas pela criatividade do desenvolvedor, existe muitos que a desconhecem ou não a credibilizam. Muitas oportunidades promissoras podem ser destacadas. A tecnologia NFT não se limita apenas na compra e venda de ativos! Este trabalho estima chamar a atenção para essa questão na medida em que apresenta uma visão geral sobre o estado-da-arte dos NFTs, informando a respeito de suas principais características e as tecnologias utilizadas (e.g. *blockchain*) destacando as oportunidades de atuação nesse mercado por profissionais da área de teleinformática.

## 1.1 Justificativa

No artigo periódico titulado de “*A Guide to Collectible Crypto and Non-Fungible Tokens* (NFTs) [Binance Academy 2020]” publicado pela *Academy Binance* diz que a criação do *Bitcoin* introduziu o conceito de escassez digital (do inglês, *trustless*). Antes disso, o custo de uma cópia digital de qualquer item era praticamente zero. Com a tecnologia *blockchain*, a escassez digital programável tornou-se possível isso significa que antes um item digital era infinito, poderia haver infinitas cópias do mesmo qualquer um poderia simplesmente copiar e salvar aquele, diminuindo assim o valor inicial do item original até ele não possuir valor algum. Escassez digital dita que “o bem mesmo que digital deve ter uma existência limitada” [Binance Academy 2021].

O NFT expande essa ideia podendo ser negociados livremente com valores personalizados de acordo com sua idade, raridade, liquidez, etc. Isso estimulou muito o mercado de aplicativos descentralizados (DApp)<sup>1</sup>. Pode ser citado como exemplo de DApp o *CryptoKitties*<sup>2</sup> um jogo eletrônico que opera na *blockchain* do *Ethereum*, onde o *CryptoKitty* mais caro chegou a ser vendido pelo equivalente a USD\$117 mil em EHT. O potencial de uso de NFT

---

<sup>1</sup>DApp é o aplicativo que é construído em uma rede descentralizada que combina um contrato inteligente e uma interface de usuário *frontend*

<sup>2</sup><https://www.cryptokitties.co/>

parece óbvio, principalmente dentro da aquisição de ativos digitais isso faz com que seja natural, até mesmo esperado ou até necessário um estudo que se atente aos benefícios dessa tecnologia [Wang *et al.* 2021].

Conversando com estudantes do IFPB (Instituto Federal da Paraíba) foi possível notar que mesmo com a popularidade dos NFTs muitos estudantes da área de TI desconhecem o seu potencial e a gama de oportunidades que esta tecnologia oferece, talvez porquê exista bastante literatura sobre *NFTs* oriunda de blogs, *wikis*, postagens em fóruns, códigos e outras fontes como as plataformas descentralizadas baseadas na rede *ethereum*, que é de fácil acesso ao público, mas de forma geral, boa parte de todo o conteúdo encontrado a respeito dos NFTs tem como foco sua compra e venda dentro dos mercados ativos, transmitindo a ideia de que NFT se resume apenas a compra e venda de ativos virtuais. O principal objetivo desse trabalho é criar um material que co-relacione e destaque as oportunidades de atuação no mercado de NFT por profissionais da área de TI. Diante do exposto, o trabalho a ser elaborado visa responder a seguinte questão: **De que formas um futuro profissional de TI pode aderir/beneficiar-se deste mercado?**

## 1.2 Objetivos

O principal objetivo desse trabalho é criar um material que co-relacione e destaque as oportunidades de atuação no mercado de NFT por profissionais da área de TI. Para chegar a essa resolução, os seguintes objetivos específicos serão considerados:

- **Visão geral do estado-da-arte:** Apresentar uma visão geral a respeito dos aspectos históricos e contextualizar o estado-da-arte no estudo dos NFTs.
- **Análise técnica:** Apresentar suas tecnologias, explicar suas principais características, contextualizar protocolos, padrões e suas principais propriedades.
- **Lançar formulário:** Este formulário não apenas tem como objetivo validar o trabalho, mas servir de métrica para informar o nível de conhecimento a respeito dos NFTs apresentado pelos estudantes.
- **Identificar e informar as futuras oportunidades no campo:** Descrever de forma direta as oportunidades de atuação na área dos NFTs, desde do seu desenvolvimento a sua aplicação em campos distintos.

## 1.3 Relevância e Contribuições

A tecnologia NFT está apenas no começo, com muitos projetos sendo desenvolvidos, e muitos novos que ainda vão surgir porque ela já se provou ser revolucionária, e bastante lucrativa, não apenas pela sua tecnologia inovadora, mas pelas oportunidades de aplicações futuras em

diversos cenários e ampla gama de novas aplicações. Com essa base, as contribuições para este trabalho são fornecidas da seguinte forma:

1. Em primeiro lugar, criar um material com uma forte base bibliográfica, abstraindo as soluções NFT atuais, especificamente, identificando os principais componentes técnicos que são usados para construir NFTs, e falar sobre suas aplicações que vão além da compra e venda de ativos digitais.
2. Em segundo lugar, a maior contribuição deste trabalho é discutir e destacar as oportunidades futuras que o mercado de NFT abre para os profissionais de TI.

## 1.4 Organização do Documento

O trabalho está organizado em seis partes, que permitirão ao leitor uma melhor divisão de informações e conseqüentemente um melhor entendimento dos objetivos que este trabalho visa alcançar.

1. No primeiro capítulo é feita a apresentação e introdução ao tema, demonstrando a justificativa, definição dos objetivos e expondo as contribuições que este trabalho deseja alcançar.
2. No segundo capítulo, apresenta-se a fundamentação teórica do trabalho. Noções fundamentais de funcionamento dos NFTs um pouco da sua história junto a suas tecnologias, conceitos importantes para estabelecer uma base de conhecimento que ajuda a validar a importância deste trabalho.
3. O terceiro capítulo consiste na apresentação da metodologia utilizada na construção deste trabalho.
4. O quarto capítulo consiste na apresentação dos resultados obtidos a respeito da análise do formulário aplicado, que visa validar a motivação da pesquisa, e servir de métrica na escolha das oportunidades do mercado NFT que serão informadas.
5. O quinto capítulo consiste na exposição e discussão a respeito das oportunidades no mercado NFT, desde de aplicações para a tecnologia, a possíveis investimentos.
6. O sexto capítulo expõe as considerações finais do estudo realizado e apresenta algumas sugestões de trabalhos futuros.

# Capítulo 2

## Fundamentação Teórica

Neste capítulo é apresentada a visão geral do estado-da-arte utilizando-se da revisão teórica da literatura. Para facilitar a compreensão dos tópicos relacionados ao tema da pesquisa, esta seção está dividida em três partes:

1. O primeiro tem como escopo a questão da tecnologia *Blockchain*. Apresenta-se um breve histórico, seguido de uma explicação resumida a respeito de suas propriedades, processo de validação e consenso.
2. O segundo apresenta as criptomoedas, um breve histórico, características, alguns exemplos de moedas populares e mencionada a EVM.
3. Na terceira parte é discutido um pouco sobre a historia dos NFTs, curiosidades, e cronologia de seu surgimento com ênfase em seus principais marcos, é dado atenção as características e seus componentes técnicos, por fim é informado com auxílio de exemplos oriundos de artigos, padrões de projeto que podem ser utilizados para o entendimento do que se diz respeito a construção de um NFT. *token*.

### 2.1 Blockchain

A tecnologia *blockchain* surgiu em 2008. Com a proposta de operar como uma corrente de dados distribuídos que mantém um registro em forma de blocos que está em constante crescimento, assim protegido contra adulteração e revisão, tornando desnecessária a comparação e correspondência de quaisquer registro mantido separadamente [Witte 2016] ou seja ela permite que as decisões sejam tomadas coletivamente entre todos os participantes da rede eliminando assim a necessidade de uma entidade centralizadora. Um grande exemplo de tecnologia que utilizada *blockchain* é a criptomoeda *bitcoin* [Rebello *et al.* 2019].

No artigo "Correntes de Blocos: Algoritmos de Consenso e Implementação na Plataforma Hyperledger Fabric" [Rebello *et al.* 2019] é exposto uma definição mais técnica do que seria uma *blockchain*. Uma *blockchain* é uma estrutura de dados distribuída que garante a confiabilidade sem necessitar de uma autoridade central comum a todas as entidades. Também é



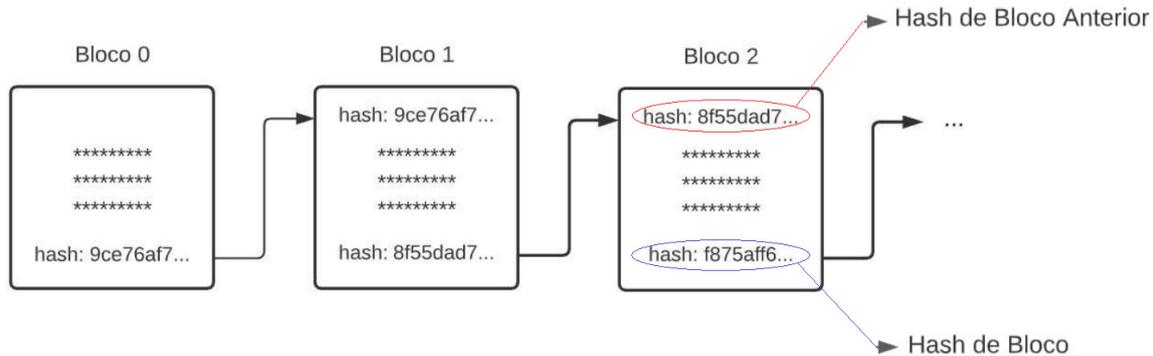
**Figura 2.1:** *Exemplo de Bloco de uma blockchain [GOUVEIA 2021]*

descrita como sendo uma tecnologia de livro-razão distribuído (do inglês, *Distributed Ledger Technology* - DLT) que utiliza máquinas independentes, denominadas de nós mineradores, para gravar, compartilhar e sincronizar transações em um sistema de controle descentralizado sobre uma rede par a par (do inglês peer-to-peer - P2P) [Rebello *et al.* 2019]. Jan Hendrik Witte no artigo "The Blockchain: A Gentle Four Page Introduction" [Witte 2016] expressa que um *blockchain* é projetado com base em duas ideias matemáticas bem estabelecidas:

- A primeira é a criptografia de chave pública que é um sistema que usa pares de chaves para criptografar e autenticar informações. Exemplo, Werlan possui um par de chaves uma chave pública e outra privada, a pública como o nome sugere, pode ser amplamente distribuída sem afetar a segurança, a chave privada é conhecida apenas por ele, então se Elmano criptografar uma mensagem utilizando a chave pública de werlan, apenas werlan com sua chave privada vai ser capaz de descriptografar a mensagem [Witte 2016].
- A segunda é a chave de *hash* ela é uma chave onde é aplicado qualquer função totalmente definida que recebe uma sequência alfanumérica de comprimento arbitrário e a reduz a uma de comprimento finito predefinido. Por exemplo a função *hash* conhecida como MD5 recebe o nome "Werlan", resulta no hash "79f48f61e57e74ee101971e748364 73a". Sua confiabilidade vem de algumas propriedades como por exemplo a que diz respeito à não invertibilidade desse tipo de função. Ou seja, deve ser praticamente impossível pegar um valor de *hash*, e aplicar uma função inversa e obter o dado de entrada, em outras palavras não tem como descobrir a chave apenas como *hash* [Witte 2016].

A partir destas ideias e das definições que foram apresentadas é possível explicar um *blockchain* como uma corrente de dados que estão ligados por um esquema de *hash* com cada unidade de informação chamada de nó minerador que é um bloco. Um exemplo de bloco pode ser visto na Figura.2.1 [GOUVEIA 2021]. Cada bloco deve possuir as informações sobre sua operação, e todo e qualquer bloco da sequência deve conter a referência ao seu bloco anterior, seu próprio *hash* que vai funcionar como sua identidade (ID), a data em que está sendo gerado, e dependendo da função específica do *blockchain* ao qual o bloco está sendo inserido, mais informações são necessárias para tornar o bloco válido (e.g. *hash's* referentes aos tipos de transações) o que vai definir se o bloco entra ou não na corrente são os protocolos

de consenso. [Rebello *et al.* 2019]. Uma vez que o bloco é adicionado a corrente ela se torna uma *blockchain*, não só validando a transação contida, mas como todas as outras transações posteriores, mantendo a integridade da corrente [Maciel 2019]. Uma ilustração da estrutura da Corrente de Blocos pode ser vista na Figura 2.2.



**Figura 2.2:** Estrutura da básica blockchain [GOUVEIA 2021]

A grande vantagem do *blockchain*, vem do fato de que as informações não vão estar armazenadas em apenas um nó, elas vão estar distribuídas por todos os nós pertencentes a corrente, e eles também não vão estar guardados em um único local, eles vão estar espalhados em centenas ou milhares de computadores por todo o globo [Maciel 2019]. No *blockchain* também está presente o conceito de permissões (do inglês *permissionless*). A rede normalmente é operada de forma livre, onde os nós são acordados sem a necessidade de intermédio por parte de uma entidade centralizada, mas é possível acionar regras, que restringem as ações de cada nó, este método normalmente é utilizado por empresas privadas e garantindo através dos contratos inteligentes [Maciel 2019].

No artigo "Correntes de Blocos: Algoritmos de Consenso e Implementação na Plataforma Hyperledger Fabric" [Rebello *et al.* 2019] possui uma figura 2.3 que ilustra o funcionamento de um *blockchain* como um livro-razão distribuído através de um protocolo de consenso genérico. É exibido um nó minerador da rede que deseja inserir um novo bloco, alterando o estado atual  $S$  do *blockchain*, inicia uma rodada de consenso reunindo as transações válidas recebidas de usuários em um novo bloco a ser proposto. A seguir, o bloco proposto é validado localmente de acordo com políticas pré-definidas e é difundido na rede. Dependendo do protocolo de consenso adotado, o bloco proposto pode ser adicionado imediatamente, de forma assíncrona, ao *blockchain* do nó minerador que propôs o bloco, ou de forma síncrona em todos os nós mineradores ao fim da rodada. A figura mostra o caso de um protocolo no qual o estado  $S$  é alterado para  $S'$  no nó minerador que propôs o bloco antes da difusão [Rebello *et al.* 2019].

Ao receber o bloco proposto, cada nó minerador valida o bloco independentemente e, caso aprove o bloco, o adiciona à corrente de blocos e chega ao estado  $S'$ . O algoritmo de validação de um bloco e de cada transação deve ser acordado previamente por todos os nós mineradores. Todo protocolo de consenso possui um mecanismo de atualização para obter o

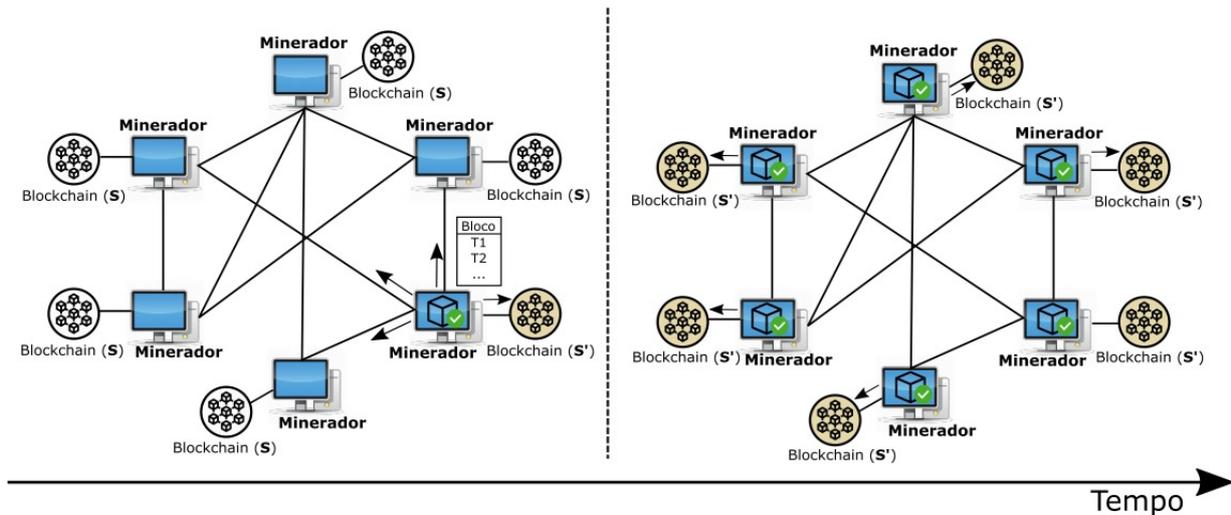


Figura 2.3: Atualização de uma blockchain [Rebello et al. 2019]

estado mais recente e corrigir discrepâncias de estado resultantes de blocos não aprovados, garantindo a consistência da corrente de blocos em toda a rede [Rebello *et al.* 2019].

### 2.1.1 Propriedades

A *blockchain* possui propriedades que proveem benefícios às aplicações e sistemas baseados nesta tecnologia. Suas principais propriedades são [Rebello *et al.* 2019]:

- **Descentralização.** Sua execução é realizada de maneira distribuída, através do estabelecimento de consenso entre todos os participantes da rede. Não há uma entidade centralizadora;
- **Desintermediação.** Elimina a necessidade de um intermediário confiável para a troca de ativos. Os ativos podem ser trocados diretamente pela rede e a confiança é estabelecida através de consenso;
- **Imutabilidade.** Os dados armazenados em uma *blockchain* são imutáveis. Não é possível modificar ou recriar qualquer dado incluído na *blockchain* de forma retroativa. Toda sua atualização é realizada de forma incremental;
- **Irrefutabilidade.** Os dados são armazenados *blockchain* em forma de transações assinadas, que não podem ser alteradas devido à propriedade de imutabilidade. Portanto, o emissor de uma transação jamais pode negar sua existência;
- **Transparência.** Todos os dados armazenados na *blockchain* são acessíveis por todos os participante da rede. Em *blockchain* públicas, como o *Bitcoin* e o *Ethereum*, as transações são abertas para qualquer usuário com acesso à Internet;

- **Auditabilidade.** Como consequência da transparência, todo participante pode verificar, auditar e rastrear os dados inseridos na *blockchain* para encontrar possíveis erros ou comportamentos maliciosos. No caso de *blockchain* federadas, o processo de auditoria pode responsabilizar um malfeitor na rede;
- **Disponibilidade.** As *blockchain* são estruturas replicadas em cada participante da rede e, portanto, a disponibilidade do sistema é garantida mesmo sob falhas, devido à redundância de informações;
- **Anonimidade.** Os usuários e nós mineradores de uma *blockchain* são identificados por chaves públicas ou identificadores únicos que preservam suas identidades. É possível utilizar uma chave pública em cada transação, evitando a rastreabilidade do usuário e conferindo um grau a mais de anonimidade [Rebello *et al.* 2019].

Na construção do *blockchain*, e para garantir todas as suas características e funcionalidades é preciso manter três propriedades em mente. São elas: O tamanho da rede (do inglês, *Network size*), a profundidade do *blockchain* (do inglês, *Blockchain depth*) e o conhecido como Ataque de 51% (do inglês, *51% Attack*) [Binance Academy 2021] [Witte 2016]. Todas as três são explicadas no manuscrito *The Blockchain: A Gentle Four A Page Introduction* escrito por J. H. WITTE [Witte 2016]. De forma resumidas elas dizem que:

- **Tamanho da Rede.** É fundamental que a rede distribuída seja grande, para que isso seja possível incentivos são oferecidos a todos os que participam do processo de mineração, estes são providos de pequenas taxas ganhas a cada transação confirmada.
- **Profundidade do *blockchain*.** Todos que participam da rede distribuída sempre atualizarão sua versão do *blockchain* para a mais antiga. Porque mesmo que alguém consiga manipular o último bloco modificando seus valores, vai gerar um *hash* repetido, desvalidando assim aquela que foi modificada, ou seja, quanto mais profunda for a corrente, mais difícil será de alguém conseguir interferir nela, pois para ter sucesso ele teria que reconstruir todos os blocos existentes.
- **Ataque de 51%.** Se um único ou um grupo usuários maliciosos, o agindo em conjunto, controlar mais de 50% da taxa total do *hashing* de rede para um *blockchain*, eles são capazes de substituir o mecanismo de consenso da rede e cometer atos maliciosos, como gastos duplos. Este é um risco a se considerar mas, que se torna muito improvável devido à magnitude da rede. À medida que a rede cresce graças a sua profundidade, a possibilidade de uma única pessoa ou entidade obter poder computacional suficiente para sobrecarregar todos os outros participantes fica cada vez mais improvável.

### 2.1.2 Processo de Validação e Consenso

O consenso refere-se ao conjunto de regras que permite a manutenção e atualização do livro-razão e garante a confiabilidade dos registros nele contidos, ou seja, sua confiabilidade,

autenticidade e precisão. O consenso pode variar trazendo vantagens e desvantagens com base em diferentes características, por exemplo, velocidade de transação, eficiência energética, escalabilidade, resistência à censura e resistência à adulteração [Tasca e Tessone 2017]. O conjunto de regras compõem a estrutura do processo de validação necessário para superar problemas de segurança, sem consenso, a transação não é possível e não é registrada ao *blockchain* porque nunca são acordados [Business blockchain hq 2022]. Existem diferentes maneiras de chegar a um consenso. Algumas delas são:

- **Prova de trabalho** (*Proof of Work - PoW*): Nessa configuração, dispositivos de computação, geralmente chamados de mineradores, conectados a uma rede ponto a ponto, realizam a tarefa de validar as transações propostas para adição ao registro completo de transações válidas existentes. A geração de um bloco que pode ser anexado ao *blockchain*, tornando assim válidas todas as transações nele incluídas, requer resolver a inversão de uma função criptográfica, que só pode ser feita por força bruta. Em PoW, a probabilidade de um minerador minerar um novo bloco depende da razão entre o poder computacional que ele dedica a essa tarefa e o poder computacional instantâneo total de todos os mineradores conectados à rede. Especificamente, os mineradores devem encontrar uma solução para uma função de *hash* unidirecional computando novos valores de *hash* com base na combinação dos valores de *hash* anteriores contidos na mensagem, as novas transações no bloco que eles criam e possíveis variações. A solução é tal que o novo valor de *hash* começará com um determinado número de zeros  $\leq$  alvo [Tasca e Tessone 2017]. Esses cálculos são executados por máquinas dedicadas (ASICs-Circuito integrado de aplicação específica do inglês Application-specific integrated circuit) que são muito caras e consomem muitos recursos, contribuindo para uma grande desperdício energético para mineradores de criptomoedas. Devido a esse esquema, nos últimos anos, os mineradores se aglomeraram em torno de *pools* de mineração (ou piscinas de mineração) [Tasca e Tessone 2017]. A desvantagem clara do mecanismo PoW, portanto, é que a ineficiência inerente nos requisitos de recursos e os investimentos em grande escala necessários levaram à centralização de longo prazo do poder de mineração.
- **Prova de Posse ou prova de participação** (*Proof of Stake - PoS*): O PoS vincula a geração de blocos à prova de propriedade de uma certa quantidade de ativos digitais (por exemplo, bitcoin) vinculados ao *blockchain*. A probabilidade de um determinado provador ser selecionado para verificar o próximo bloco cresce em relação à parcela de ativos que aquele provador possui dentro do sistema. A suposição subjacente é que os usuários com uma grande parcela da riqueza do sistema são mais propensos a fornecer informações confiáveis em relação ao processo de verificação e, portanto, devem ser considerados com maior confiabilidade) [Tasca e Tessone 2017]. Nos últimos anos, a prova de participação têm se destacado devido ao desejo do *Ethereum* de abandonar a prova de trabalho para implementar PoS [BitFury Group 2015].

- **Prova de Queima ou Destruição** (*Proof of Burn - PoB*): Este método de verificação é bastante raro. Basicamente, ele exige que, para um bloco ser verificado, uma determinada quantidade de um recurso digital (uma criptomoeda, por exemplo) tem que ser enviado a um endereço público inválido, que por sua vez destrói o recurso e o torna inacessível para sempre. Embora a motivação para PoB seja nobre (resolver os problemas de gasto energético em sistemas Pow), frequentemente os recursos digitais “queimados” no processo são exatamente criptomoedas que usam PoW, o que dá aos sistemas PoB os exatos mesmos problemas de sistemas PoW [Tasca e Tessone 2017].
- **Prova de Posse Delegada** (*Delegated Proof of Stake - DPoS*): Os nós mineradores utilizam seus ativos para eleger delegados em um quórum que define o bloco a ser adicionado. A quantidade de votos de um minerador é proporcional aos seus ativos [Kiayias *et al.* 2017].
- **Prova de Autoridade** (*Proof of Authority - PoA*): Atribui maior autoridade a certos nós, esta autoridade pode ser delegada pelo próprio responsável por uma transação ou até por outra autoridade previamente determinada. Esse esquema de delegar autoridade a certos nós é mais comum em redes centralizadas ou hierárquicas, onde as autoridades podem ser simplesmente inseridas no código do sistema. Estas autoridades podem receber um conjunto de chaves privadas especiais com as quais “assinar” os blocos válidos, isso torna o processo de validação de bloco com PoA praticamente idêntico a validação de transação [Tasca e Tessone 2017].
- **Prova de Capacidade de Armazenamento** (*Proof of Capacity - PoC*): Também conhecida como *proof of storage* ou *proof of space*, funciona de maneira muito similar ao PoW, exceto que, ao invés de tentar computar *hashes*, o validador tem que dedicar espaço na memória para a solução de um problema. A quantidade de memória dedicada ao processo de validação aumenta a probabilidade do minerador obter um bloco válido [Tasca e Tessone 2017]. PoC se comporta da mesma maneira que PoW e apresenta as mesmas desvantagens do ponto de vista de segurança e escalabilidade. O que ocorre é a simples troca de poder computacional por espaço na memória. Se comparada ao enorme desperdício de energia observado em PoW, se torna uma alternativa mais econômica já que espaço de memória é um recurso menos crítico para outras atividades [Tasca e Tessone 2017].
- **Híbridos**: Sistemas híbridos são sistemas que utilizam mais de um método na validação de blocos. Um exemplo seria a criptomoeda Nano, que utiliza uma combinação de PoS para validação de blocos, mas exige do usuário a execução de uma PoW para validar transações. Sistemas PoS frequentemente são híbridos por questões de segurança [Tasca e Tessone 2017].

### 2.1.3 Blockchain/Tokenização

Criptomoedas e outros registros de transferência de propriedade são os usos mais comuns das tecnologias *blockchain*. Em criptomoedas, os participantes do sistema que contribuem para o processo de verificação, se selecionados por alguma regra para emitir um novo bloco no *blockchain*, recebem a possibilidade de emitir uma transação sem emissor (chamado “coin-base”) para si mesmos. Por um lado, esta é uma forma habitual de introduzir novos ativos no sistema. Por outro, introduz um incentivo para que os usuários participem do processo de verificação, o que leva a uma maior confiabilidade do sistema [Tasca e Tessone 2017]. O esquema de incentivo deve ser fornecido em um *token*, cujo valor é atribuído justamente pelo custo associado à sua produção. Dessa modalidade surgiu a tokenização: um *token* atua como um título digital ao portador, cuja propriedade é determinada pelos dados incorporados no *blockchain* [Tasca e Tessone 2017]. A propriedade dos *tokens* é transferível entre os titulares usando outras transações com metadados de “transferência” associados. Isso não requer a aprovação de nenhuma outra autoridade [Tasca e Tessone 2017].

Essa solução de incentivo mencionada acima não é a única possível. Por exemplo, na rede *Ethereum* além do *token* nativo, *Ether*(ETH), novos *tokens* arbitrários podem ser criados e trocados por meio de contratos inteligentes. Além disso, as possibilidades de moeda nativa presentes, por exemplo, em *Ripple*<sup>1</sup>, permitem diferentes casos de uso de tecnologias *blockchain*, como transferências de ativos por meio de *tokens* e *exchanges* (exchange é uma plataforma digital que oferece a compra, a venda e a troca de criptoativos) [Tasca e Tessone 2017].

## 2.2 Criptomoedas

Uma criptomoeda foi definida por Jan Lansky como um tipo de moeda digital que conta com provas criptográficas para confirmação de transações. Ele afirma que as criptomoedas geralmente alcançam uma combinação única de três recursos, garantia de anonimato limitado, independência da autoridade central e proteção contra ataques de gastos duplos [Lansky 2018]. A primeira moeda foi a *eCash* criada por David Chaum, fundador da empresa *Digi-cash* em 1989 [Wikipedia contributors 2022]. Em 1996, surgiu as moedas digitais de ouro (do inglês, *Digital gold gurrency*). Nesse mesmo ano a agência de Segurança Nacional publicou um artigo intitulado *How to Make a Mint: the Cryptography of Anonymous Electronic Cash*, descrevendo um sistema de criptomoeda [stringfixer team 2021], em sequência veio a *b-money* criada por Wei Dai, ele registrou sua patente em conjunto com a *Microsoft*, sua criptomoeda utilizava o conceito PoW, o seu trabalho mais tarde foi referenciado no *whitepaper* (Livro branco ou relatório) escrito por Satoshi Nakamoto criador do *Bitcoin* em 2009 [Ethereum Articles 2022].

---

<sup>1</sup>Ripple é um protocolo de pagamento distribuído, que também tem uma moeda nativa de seu sistema, a XRP [Raquel Balarin 2022].

Satoshi Nakamoto usou a SHA-256, uma função *hash* criptográfica, como esquema de prova de trabalho. Em sequência o *Namecoin* foi criado como uma tentativa de formar um DNS (*Domain Name System* – Sistema de nome de domínio) descentralizado (Abril de 2011). A primeira criptomoeda bem sucedida em usar uma função diferente a SHA-256, usava o *scrypt* como função de *hash*, foi o *Litecoin* (Outubro 2011). O *Peercoin* foi a primeira a usar um híbrido de prova de trabalho e prova de participação. Em 6 de agosto de 2014, o Reino Unido anunciou que seu tesouro foi comissionado para um estudo acerca das criptomoedas, seu objetivo era descobrir se elas poderiam desempenhar algum papel na economia do reino unido, este estudo teve um grande impacto no desenvolvimento das mesmas [stringfixer team 2021].

O artigo escrito por Jan Lansky denominado *Possible State Approaches to Cryptocurrencies* [Lansky 2018] tem como um dos objetivos principais definir as propriedades de um sistema de criptomoedas para criar uma definição formal, dentro do escopo do trabalho ele defende que um sistema de criptomoedas atente a seis condições [Lansky 2018], apresentado de maneira resumida elas são:

1. O sistema não requer uma autoridade central, seu estado é mantido por meio de consenso distribuído.
2. O sistema mantém uma visão geral das unidades de criptomoeda e sua propriedade.
3. O sistema define se novas unidades de criptomoeda podem ser criadas, o sistema define as circunstâncias de sua origem e como determinar a propriedade dessas novas unidades.
4. A propriedade de unidades de criptomoeda pode ser provada exclusivamente por criptografia.
5. O sistema permite que transações sejam executadas, nas quais a propriedade das unidades criptográficas é alterada. Um extrato de transação só pode ser emitido por uma entidade que comprove a propriedade atual dessas unidades.
6. Se duas instruções diferentes para alterar a propriedade das mesmas unidades criptográficas forem inseridas simultaneamente, o sistema executará no máximo uma delas.

Uma 2.<sup>a</sup> geração de criptomoedas surgiu em 2014, elas utilizavam-se de contratos inteligentes e funcionalidades mais avançadas, exemplo a *Ethereum* e *Monero*, [Peck 2012]. Também surgiu a *RaiBlocks*, que ganhou bastante destaque por resolver problemas conhecidos do *Bitcoin*, tais como as taxas, demora nas transações e o alto consumo de energia. Em 2018 a moeda foi renomeada para Nano [yan Lucas 2018].

### 2.2.1 Altcoin e Token

*Altcoins* são criptomoedas alternativas ao *Bitcoin*. A maioria dos *altcoins* surgiu a partir de bifurcações do código-fonte do *Bitcoin*, com o intuito de modificar alguns parâmetros internos da rede do *Bitcoin* ou adicionar novas características, a depender do objetivo de cada *altcoin* [Vigna 2011]. Exemplos de *Altcoins* de sucesso são os *Namecoins*, *Litecoin* e *Dogecoin*.

1. *Namecoin* (NMC) é famosa por ter sido a primeira bifurcação do código-fonte do *Bitcoin*. Foi lançada em abril de 2011, utiliza o mesmo esquema de prova de trabalho do *Bitcoin*. Atualmente, existem 14 bilhões NMC em circulação, atingindo um valor de mercado de aproximadamente 6 milhões de dólares [Coinmarketcap 2009].
2. *Litecoin* (LTC) é a *altcoin* mais conhecida derivada a partir de uma bifurcação do *Bitcoin*. É a criptomoeda par a par que teve o seu código-fonte bifurcado mais vezes, seguido do próprio *Bitcoin*. Foi lançado oficialmente em 13 de outubro de 2011, e possui poucas variações em relação ao *Bitcoin*. Entre as principais diferenças, destacam-se a taxa de processamento de blocos (2 minutos e 30 segundos, em comparação aos 10 minutos do *Bitcoin*) que foi escolhido em função de dificultar a ocorrência de gasto duplos e o algoritmo de prova de trabalho utilizado, que ao contrário do SHA-256, utiliza o *scrypt* cujo plano de implementação inicial tinha como propósito evitar que GPUs tivessem vantagem sobre CPUs durante o processo de mineração [Coinmarketcap 2009].
3. *Dogecoin*(D) é baseada no “meme” popular da internet o “*doge*” e possui como logotipo um Shiba Inu. A moeda digital de código aberto foi criada por Billy Markus de Portland, Oregon e Jackson Palmer de Sydney, Austrália, sendo um fork do *Litecoin* ocorrido em dezembro de 2013. Os criadores do *Dogecoin* o imaginaram como algo divertido, uma criptomoeda descontraída que teria maior apelo, indo além do público alvo do *Bitcoin*, já que foi baseada em meme de cachorro. O CEO da Tesla Elon Musk postou alguns *tweets* na mídia social dizendo que *Dogecoin* seria sua moeda favorita [Coinmarketcap 2009].

*Token* é um código numérico, criado inicialmente para serviços *e-banking*, para oferecer segurança em acessos digitais. O *Token*, era fornecido por meio de um dispositivo físico, e era utilizado para fornecer uma senha de instantânea de acesso. Assim, ao acessar sua conta bancária por meio digital, o usuário utilizava seus dados pessoais, sua senha individual e, ainda, o *token*, para maior segurança. O *token* ainda é utilizado com o sistema financeiro. O *token* existe em uma *blockchain* e representa um determinado ativo ou uma utilidade. Ou seja é o registro de um ativo em formato digital [“MCT” 2021].

Uma forma fácil e direta de caracterizar um *token* é como um sistema gerador de senhas, com o intuito de proteger usuários. De modo que o *token* também é utilizado para representar

algum ativo financeiro, que tem valor de mercado, como um objeto, um contrato, uma moeda ou uma propriedade. Um *token* pode vir a representar um criptoativo, quando inserido em uma *blockchain*, funcionando como uma espécie de contrato, e garantindo a custódia de um ativo para quem o possui [MCT 2021].

### 2.2.2 Contratos Inteligentes

Os contratos inteligentes, (do inglês, smart contracts), permitem executar de forma automática um programa previamente definido. Essa invenção passou a ser fortemente utilizada após o lançamento das criptomoedas, mais especificamente seu banco de dados distribuído [Ethereum Articles 2022]. Ao contrário de um código computacional tradicional, que funciona em servidores dedicados, as rotinas dos contratos inteligentes são executadas pelos próprios usuários da rede [Ethereum Articles 2022]. Nesse sentido, um contrato inteligente nada mais é que um código que pode definir regras estritas e consequências da mesma forma que um documento legal tradicional, estabelecendo as obrigações, benefícios e penalidades que podem ser devidas a qualquer das partes em várias circunstâncias diferentes, proporcionando confiabilidade nas relações entre a rede [Bruno Cardoso 2018]. Os contratos inteligentes usam a lógica “se... , então...” (do inglês, if/then) para criar contratos digitais que se autoexecutam, que autor-reforçam e que são contingentes. Um exemplo pode ser visto na Figura 2.4.

```
pragma solidity ^0.4.20;

contract MyToken {

    /* Isso cria um array com todos os saldos */
    mapping (address => uint256) public balanceOf;

    /* Inicializa o contrato com tokens de fornecimento inicial para o criador do contrato */
    function MyToken(
        uint256 initialSupply
    ) public {
        balanceOf [msg . sender] = initialSupply;           // Dê ao criador todos os tokens iniciais

    /* Enviar moedas */
    function transfer(address _to, uint256 _value) public {
        require (balanceOf [msg . sender] >= _value) ;      // Verifique se o remetente tem o suficiente
        require(balanceOf [_to] + _value >= balanceOf[_to]); // Verifique se há estouros

        balanceOf [msg . sender] -= _value;                // Subtrair do remetente
        balanceOf [_to] += _value;                          // Adicionar o mesmo ao destinatário
    }
}
```

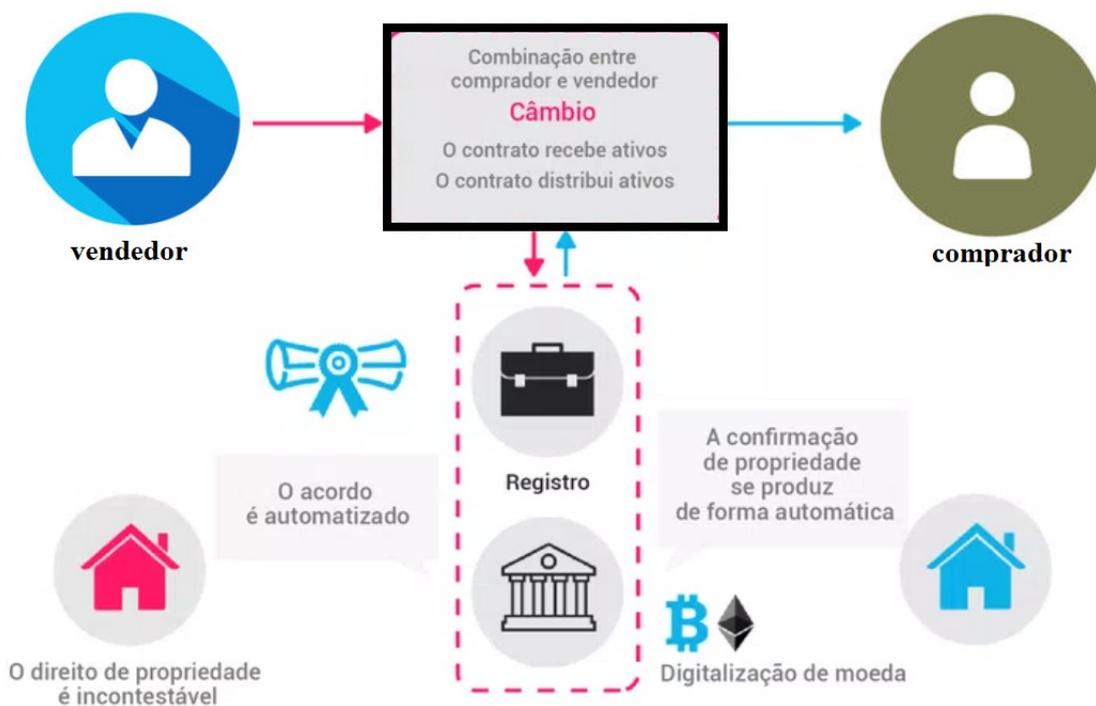
**Figura 2.4:** Exemplo simples de contrato inteligente

Ao se definir o que é um contrato inteligente as seguintes afirmações se tornam verdade, e são utilizadas como características na hora de programá-lo: [Ethereum Articles 2022]

- Os contratos inteligentes são digitais e programáveis.

- Os contratos inteligentes são executados em computadores, e ficam armazenados na rede de forma descentralizada.
- O que diferencia um contrato inteligente de um programa comum é sua capacidade de execução de forma autônoma, sem a necessidade de intervenção humana.
- Apesar de autônomo, seria leviano afirmar que tais contratos são inteligentes. A inteligência do código-fonte depende exclusivamente da capacidade de quem o criou.
- Não há nenhum mecanismo nativo para assegurar que este contrato inteligente seja isento de falhas.
- Não é possível impedir ou censurar as instruções contidas neste contrato.

Uma vez desenvolvido, o contrato inteligente é encriptado e guardado na *blockchain*, sendo partilhado com os computadores que fazem parte da rede, que verificam a legitimidade do contrato. Embora partes do contrato inteligente sejam públicas, a encriptação previne qualquer um de acessar os seu conteúdo [Ethereum Articles 2022]. O funcionamento básico de um contrato inteligente pode é ilustrado por meio de infográfico exibido na Figura 2.5.



**Figura 2.5:** *Funcionamento básico de um contrato inteligente [Bruno Cardoso 2018]*

Os contratos inteligentes podem funcionar como contas “multi-assinaturas”, de modo que os fundos são gastos apenas quando uma porcentagem exigida de pessoas concordam, eles podem gerenciar acordos entre usuários, fornecer utilidade para outros contratos (semelhante ao funcionamento de uma biblioteca de software), armazenar informações sobre um aplicativo, como informações de registro de domínio ou registros de associação [Bruno Cardoso

2018]. É importante frisar que os contratos inteligentes podem ser codificados em qualquer *Blockchain*, mas a rede mais utilizada é a do *ethereum*, principalmente porque fornece capacidade ilimitada de processamento e criação de aplicações [Ethereum Articles 2022]. Um exemplo de código para um contrato inteligente básico que foi escrito na plataforma *ethereum* pode ser visualizado na Figura 2.6.

```

/* Permitir que outro contrato gaste alguns tokens em seu nome */
function approve (address _spender, uint256 _value)
returns (bool success) {
    allowance [msg.sender] [_spender] = _value;
    return true;

/* Aprove e depois comunique o contrato aprovado em um único tx */

function approveAndCall (address _spender, uint256 _value, bytes _extraData)
returns (bool success) {
    tokenRecipient spender = tokenRecipient (_spender);
    if (approve (_spender, _value) ) {
        spender . receiveApproval (msg.sender, _value, this, _extraData);
    }
    return true;

/* Um contrato tenta obter as moedas */
function transferFrom (address _from, address _to, uint256 _value) returns (bool success) {

    if (balanceof [_from] < _value) throw; // Verifique se o remetente tem o suficiente

    if (balanceof [_to] + _value < balanceof[_to]) throw; // Verifique se há estouros

    if (value > allowance [_from] [msg.sender]) throw; // Cheque abono

    balanceof [_from] -= _value; // Subtrair do remetente

    balanceof [_to] += _value; // Adicione o mesmo ao destinatário
    allowance [_from] [msg.sender] -= _value;
    Transfer (_from, _to, _value);
    return true;

/* Esta função sem nome é chamada sempre que alguém tenta enviar éter para ela */
function () {
    throw; // Evita o envio acidental de éter
}

```

**Figura 2.6:** Código básico para um contrato inteligente construído na plataforma *ethereum* [Bruno Cardoso 2018]

### 2.2.3 Ethereum

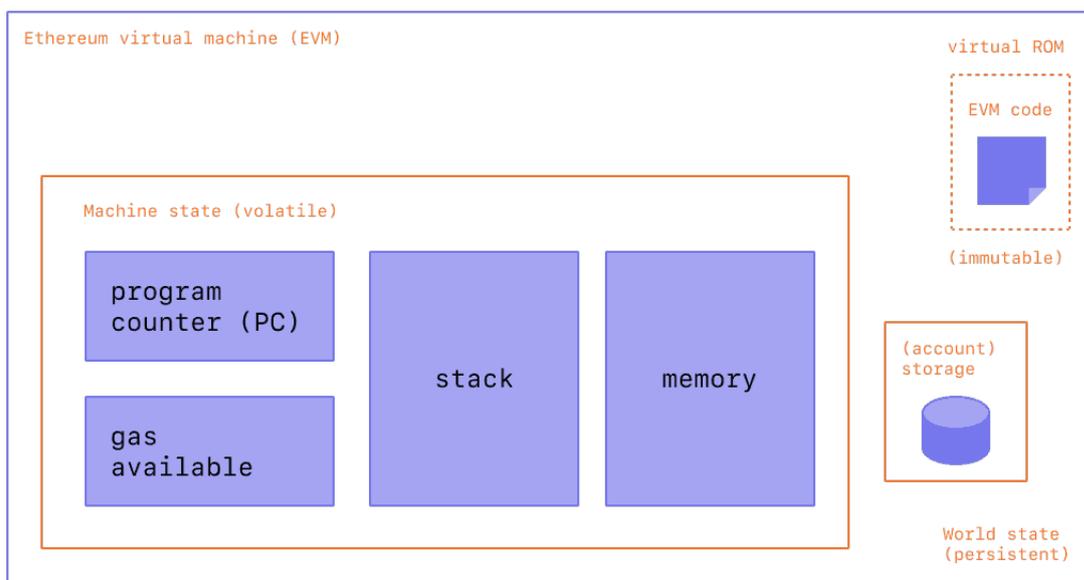
Na própria plataforma é definido que o *ethereum* é uma tecnologia para construir aplicativos, deter ativos, transacionar e se comunicar sem ser controlado por uma autoridade central, em outras palavras a *ethereum* é uma plataforma descentralizada capaz de executar contratos inteligentes [Ethereum Articles 2022]. O *ethereum* foi fundado por Vitalik Buterin em janeiro de 2014 [Buterin 2018], e lançado oficialmente em 2015, uma curiosidade a respeito de sua origem é que a plataforma foi um projeto de financiamento coletivo (do inglês *crowdfunding*) [Wikipédia 2022], o terceiro maior projeto já financiado desta forma na história. Hoje em dia é impossível falar sobre NFT sem citar a *ethereum*, porque ela deu o pontapé para o surgimento de uma nova economia digital, com novos criptoativos, Finanças Descentralizadas (DeFi), Ofertas Iniciais de Criptomoedas (ICOs), Tokens não fungíveis (NFT) e games do metaverso, como Decentraland (MANA) e The Sandbox (SAND) [Raquel Balarin 2022].

Como é descrito na plataforma da *ethereum* ela se baseia na mesma inovação do *bitcoin*, com algumas grandes diferenças. Ambos permitem que você use dinheiro digital sem provedores de pagamento ou bancos. Mas, o *ethereum* é programável, ela visa levar a tecnologia do *blockchain* e os contratos inteligentes para “tudo” que possa ser programado [Ethereum

Articles 2022]. Ser programável significa que qualquer um pode construir aplicativos que usam o *blockchain* para armazenar dados ou controlar o que seu aplicativo pode fazer. A plataforma possui sua própria criptomoeda, o *ether*, que é usado para pagar certas atividades na rede *ethereum* [Ethereum Articles 2022]..

O princípio é que toda transação, registro, execução de código distribuído, assinatura de contrato digital, ou qualquer outra aplicação executada na rede do *ethereum*, seja paga em *ether*. Como é definido na própria plataforma, no universo *ethereum*, há um único computador canônico (chamado de *Ethereum Virtual Machine*, ou EVM). Todos que participam da rede mantêm uma cópia do estado deste computador. Além disso, qualquer participante pode transmitir uma solicitação para que este computador realize uma computação arbitrária. Sempre que tal solicitação é transmitida, outros participantes da rede verificam, validam e realizam o cálculo desta forma são recompensados com *ether*. Essa execução provoca uma mudança estatal no EVM, que é cometido e propagado em toda a rede [Ethereum Articles 2022].

O EVM foi construído através de algumas linguagens de programação existentes, e é capaz de rodar algoritmos de várias complexidades. O estado do *Ethereum* é uma grande estrutura de dados que contém não apenas todas as contas e saldos, mas um estado de máquina, que pode mudar de bloco para bloco de acordo com um conjunto pré-definido de regras, e que pode executar código de máquina arbitrário. As regras específicas de mudança de estado de bloco para bloco são definidas pelo EVM [Ethereum Articles 2022]. A estrutura pode ser vista na Figura 2.7.



**Figura 2.7:** Diagrama adaptado do *Ethereum EVM* [Ethereum Articles 2022]

O EVM se comporta como uma função matemática: dada uma entrada, produz uma saída determinística. Portanto, é bastante útil descrever mais formalmente o *ethereum* como

tendo uma função de transição de estado [Ethereum Articles 2022]:

$$Y(S, T) = S' \quad (2.1)$$

Dado um antigo estado (S) e um novo conjunto de transações válidas (T), a função de transição do estado *Ethereum*  $Y(S, T)$  produz um novo estado de saída válido  $S'$ . No contexto do *Ethereum*, o estado é uma enorme estrutura de dados chamada *Merkle Patricia Trie* modificada, que mantém todas as contas vinculadas por *hashes* e redutíveis a um único *hash* de raiz armazenado na *blockchain*. As transações são instruções criptograficamente assinadas por contas. Existem dois tipos de transações: aquelas que resultam em chamadas de mensagens e aquelas que resultam na criação de contratos. A criação de contratos resulta na criação de uma nova conta de contrato contendo bytecode de contrato inteligente compilado. Sempre que outra conta faz uma chamada de mensagem para esse contrato, ela executa seu bytecode [Ethereum Articles 2022].

## 2.3 Tokens não fungíveis (NFT)

Em um dos artigos disponibilizados pela *Binance Academy*<sup>2</sup>, um de seus contribuidores conhecido como John Ma definiu os NFTs como um tipo de *token* criptográfico que representa um ativo único que são versões *tokenizadas* de ativos digitais ou do mundo real. Eles funcionam como provas verificáveis de autenticidade e propriedade dentro de uma rede *blockchain* [Binance Academy 2021]. Já em um relatório publicado pela *European Blockchain Observatory*,<sup>3</sup> um NFT é definido como um tipo especial de ativo digital ou *token* que pode ser comprovado como único e não intercambiável com outro *token* de ativo digital é por isso que é referido como um “*token não fungível*” [Blockchain e team 2021].

É acordado que o NFT é um tipo *altcoin* derivado dos contratos inteligentes da rede *ethereum*, inicialmente descrito nas propostas de melhoria do padrão (EIP)-721 [William Entriken 2018] e posteriormente desenvolvido no padrão EIP-1155 [Witek Radomski 2018], mas o NFT se popularizou fora do ecossistema cripto também conhecido como DeFi (*Decentralized Finance* [Tainá Freitas 2021]), pelo elevado valor que obra de arte NFT conhecida como “*Everydays The First 5000 Days* [Jacob Kastrenakes 2021]” atingiu no primeiro leilão de NFT realizado por uma grande casa de leilões tradicional. O artista norte-americano Mike Winkelmann (conhecido como Beeple), embolsou a quantia de US\$ 69 milhões isto em 11 de março de 2021 [Blockchain e team 2021].

<sup>2</sup>(Binance Academy é uma plataforma vinculada a exchange Binance com o objetivo de educar a respeito das criptomoedas e da tecnologia blockchain por meio de artigos revisados e disponibilizados periodicamente)

<sup>3</sup>*European Blockchain Observatory* é uma iniciativa da Comissão Europeia para acelerar a inovação em *blockchain* e o desenvolvimento do ecossistema blockchain dentro da UE.

### 2.3.1 História

O artista Kevin McCoy criou o primeiro NFT em 2014 juntamente com o empreendedor Anil Dash, toda a jornada da concepção da ideia até a execução do projeto é descrito na revista *The Atlantic*.<sup>4</sup> A jornada se dá início no museu de arte Contemporânea *Seven on Seven em Nova York* que era palco de novas ideias que conectavam tecnologia e arte [Dash 2021]. Anil Dash apresentou um projeto que tinha como foco conceder aos artistas adicionais fontes de renda, além de dar eles um maior controle sobre sua arte, evitando que seus trabalhos em mídia (como vídeos musicas trabalhos de artes digitais) fossem plagiados ou repostados. O NFT criado foi utilizado como demonstração do projeto, McCoy usou uma rede *blockchain* chamada de *Namecoin* para registrar um vídeo que sua esposa tinha feito anteriormente, e que o empreendedor Anil Dash havia comprado pelo valor de quatro dólares [Dash 2021].

Em 2014, uma plataforma financeira chamada *Counterparty* foi criada em cima do *blockchain do Bitcoin*. A *Counterparty* desprovia de uma ampla gama de ferramentas, incluindo carteiras digitais, uma funcionalidade de agente de custódia e uma câmara de compensação. Além disso, permitia a criação de ativos e contava com uma *exchange*<sup>5</sup> descentralizada, além de uma moeda nativa conhecida como XCP. A *Counterpart* tornou-se o lar de vários projetos e ativos não fungíveis, incluindo um jogo de cartas colecionáveis. Já em 2015 poucos meses após a criação da rede *ethereum* foi criado o projeto *Etheria* o escopo do projeto era apresentar aos usuários um mundo virtual aberto composto de peças hexagonais que podem ser compradas, vendidas e “construídas”, como NFT [Blockchain e team 2021].

Em 2017, obteve-se um marco na indústria NFT John Watkinson e Matt Hall criaram os *CryptoPunks* [4] que eram personagens únicos nativos da *blockchain ethereum*. Eles utilizam da característica de escassez programável nos ativos digitais, e a quantidade de personagens seria limitada a 10.000 e não haveria dois personagens iguais além que diferentes atributos teriam diferentes níveis de escassez, e os atributos combinados definiriam a raridade geral aumentando ainda mais o valor de certos personagens. No mesmo teve a introdução do padrão ERC-721, e nele foi construído o jogo virtual *CryptoKitties* [10], ele era semelhante aos *CryptoPunks* com a diferença que apresentava versões de desenhos animados de gatos e permitia aos jogadores “adotar”, “criar”, e negociá-los virtualmente [Blockchain e team 2021].

Em 2021 veio a explosão e popularização dos jogos NFTs e de seu comércio interno. Os jogos NFT, são diferentes de apenas manter cripto-colecionáveis em sua carteiras virtuais, ou simples jogos de que se compunham de figurinhas digitais, Um jogo NFT usará NFTs em suas regras, mecanismos e interações com jogadores. Por exemplo, um jogo pode representar seu personagem ou avatar único como um NFT. Itens digitais que você encontra durante o jogo também podem ser NFTs. Em seguida, você pode trocar ou negociar seus NFTs com

---

<sup>4</sup>*The Atlantic* é uma revista americana e editora multiplataforma. Sua plataforma virtual, *TheAtlantic.com*, fornece cobertura e análise diária de notícias de última hora, política e assuntos internacionais, educação, tecnologia, saúde, ciência e cultura.

<sup>5</sup>As *exchanges* são as corretoras de criptoativos. Em outras palavras, as *exchanges* são plataformas eletrônicas que facilitam todo a compra, venda e troca das criptomoedas e dos *tokens*.

outros jogadores para obter lucro [Binance Academy 2021]. Alguns jogos jogos NFTs também oferecem a opção dos jogadores minerar suas distintas criptomoedas dentro dos jogos, que podem ser armazenadas em carteiras virtuais e mais tarde negociadas no *marketplace*. Exemplos de jogos de jogos NFTS que ajudaram nesse processo de popularização, Axie Infinity [3], bomber crypto [1] e Mir4 [2] [Binance Academy 2021].

### 2.3.2 Conceito de um NFT

Para melhor compreensão do conceito, é útil comparar um NFT com um *token* ou ativo fungível. Os *tokens* fungíveis, que são os mais comuns no reino *blockchain*, são *tokens* em que um possui as mesmas características de qualquer outro e, portanto, podem ser facilmente substituídos por qualquer *token* idêntico. A ilustração mais familiar de um ativo “fungível” é o dinheiro, pois uma nota de 10 reais pode ser trocada por qualquer outra nota de 10 reais. Por outro lado, exemplos reais de ativos não fungíveis incluem ingressos para eventos, registros legais de propriedade de ativos, como títulos de propriedade, bem como obras de arte ou colecionáveis [Blockchain e team 2021].

### 2.3.3 Características dos NFTs

Embora seja impossível considerar todas as variações e padrões, é possível identificar algumas características amplamente aceitas e fundamentais que são compartilhadas entre a maioria das implantações de NFT. Estes incluem exclusividade, transparência e comprovação de propriedade, programabilidade de ativos, e imutabilidade dos registros [Blockchain e team 2021]. A exclusividade é garantida por dois fatores a singularidade (do inglês, *Uniqueness*) e a raridade:

- **Singularidade:** Com NFTs é possível produzir um número limitado de *tokens*, sendo cada um individualmente identificável. Um exemplo popular são as 10.000 NFTs únicas emitidas pela *CryptoPunks*. Embora em alguns casos seja plausível ter NFTs semelhantes, como é o caso de séries numeradas do trabalho digital de um artista [Blockchain e team 2021].
- **Raridade:** A raridade em NFTs pode vir de várias formas e pode ser artificial, numérica ou histórica.

1. A raridade artificial refere-se à singularidade do NFT conforme determinado por seu código, ou as especificidades de sua emissão. Para entender melhor esse conceito, observa-se novamente o exemplo dos *Cryptopunks*. Conforme determinado por sua emissão, apenas 1,75% do total de *Cryptopunks* possui um recurso de Máscara Médica. Comparando isso com os 24,59% de chance de ter um Brinco, podemos denotar que um *punk* (unidade de *Cryptopunks*) com Máscara Médica sempre será mais raro do que aquele com Brinco [Blockchain e team 2021].

2. A raridade numérica está intimamente ligada à artificial e, como tal, é relativamente intuitiva de entender. Considere o exemplo de um artista popular lançando 100 cópias digitais de seu último álbum de música como NFTs. Intuitivamente, aquelas 100 cópias que vêm com a “assinatura digital” do artista e podem ser de propriedade verificável, serão mais escassas e, portanto, raras, do que simplesmente fazer *streaming* do álbum no *Spotify*. É útil pensar nisso como o análogo de possuir um álbum físico que é assinado pelos artistas e outro que não é [Blockchain e team 2021].
3. Por último a raridade histórica, refere-se ao significado histórico de um NFT. Isso vem em muitas formas diferentes. Por exemplo, parte do fascínio dos *Cryptopunks* é que eles foram alguns dos primeiros NFTs generativos já emitidos, portanto, são especiais nesse sentido. Além disso, como os *blockchains* registram um histórico imutável de propriedade, alguns NFTs podem ser historicamente significativos, pois eram de propriedade de entidades ou indivíduos notáveis. Por exemplo a camisa utilizada por um jogador famoso ou uma caneta utilizada por um cantor também famoso, acabam tendo maior valor do que itens iguais a eles [Blockchain e team 2021].

A transparência e comprovação de propriedade surgem de três fatores de extrema relevância no contexto dos NFTs que representam ativos tangíveis do mundo real, a prova de propriedade de ativos subjacentes, potencial de propriedade fracionária e rastreamento de proveniência de ativos. Já a imutabilidade é uma qualidade inerente a todos os *tokens* baseados em *blockchain*. Os *tokens*, bem como as informações incorporadas nos *tokens*, são altamente resistentes à adulteração, sem comprometimento do protocolo *blockchain* subjacente. Isso resulta em confiança e transparência substanciais. Por fim a programabilidade, isso é considerado por muitos um importante fator de diferenciação que separa os NFTs dos ativos do mundo real. Além de permitir a expressão artística ou comercial, os NFTs podem ser programados de qualquer maneira que o software programável possa – por exemplo, para garantir que os artistas continuem a receber resíduos ou direitos morais durante toda a vida útil de uma obra e não apenas na primeira venda. Além disso, os aplicativos experimentais mostram como os NFTs podem ser usados como garantia para uma infinidade de aplicativos DeFi, semelhante a uma hipoteca [Blockchain e team 2021].

### 2.3.4 Componentes

A plataforma *blockchain* mais utilizada em esquemas NFT é a *Ethereum* [Ethereum Articles 2022], fornecendo um ambiente seguro para executar os contratos inteligentes. Os contratos inteligentes foram originalmente introduzidos por Szabo [Academy 2021], com o objetivo de acelerar, verificar ou executar a negociação digital. Baseado em *blockchain*, contratos inteligentes adotam linguagens de *script turing completeness* (turing-completo ou compu-

tacionalmente universal) para alcançar funcionalidades complicadas e executar replicação completa de transição de estado sobre algoritmos de consenso para obter consistência final [Academy 2021]. Contratos inteligentes permitem a criação de protocolos sem confiança. Isso significa que duas partes podem assumir compromissos, sem ter que conhecer ou confiar uma na outra. Eles podem ter certeza de que se as condições não forem cumpridas, o contrato não será executado. Fora isso, o uso de contratos inteligentes pode eliminar a necessidade de intermediários, reduzindo significativamente os custos operacionais assim propondo um método unificado para criar aplicativos em uma ampla gama de indústrias [Academy 2021]. A maioria das soluções NFT depende de plataformas *blockchain* baseadas em contratos inteligentes para garantir suas negociações [Ethereum Articles 2022].

O endereço e a transação do *blockchain* são os conceitos essenciais em criptomoedas. Um endereço *blockchain* é um identificador exclusivo para um usuário que utilizado na hora enviar e receber os ativos, se comportando semelhante a uma conta bancária. Consiste em um número fixo de números alfanuméricos caracteres gerados a partir de um par de chave pública e chave privada. Para transferir NFTs, o proprietário deve comprovar a posse da chave privada correspondente e enviar os ativos para outro(s) endereço(s) com a assinatura digital correta. Essa operação simples geralmente é realizada usando uma carteira de criptomoedas e é representada como o envio de uma transação para envolver contratos inteligentes no padrão ERC-777 [Wang *et al.* 2021].

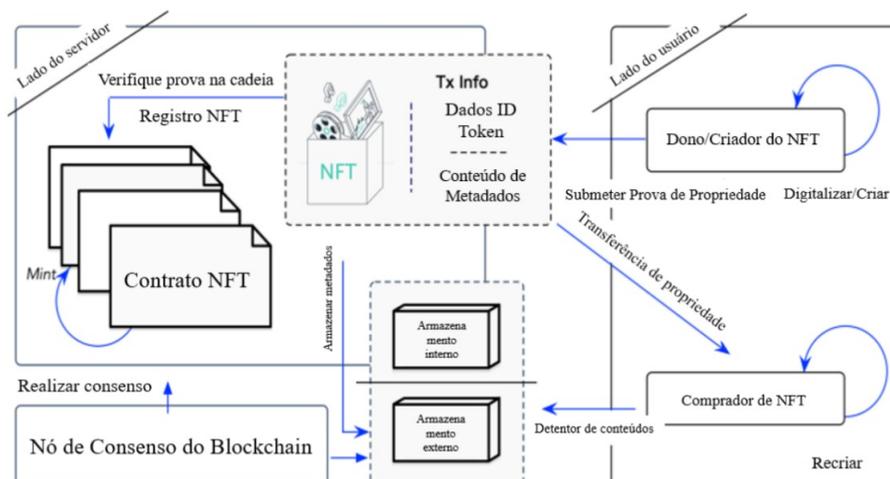
Um componente importante a apresentar é a codificação de dados. Codificação é o processo de conversão de dados de um formulário para outro [Ricarte]. Normalmente, muitos arquivos são codificados em formatos compactados eficientes para economizar espaço em disco ou em um formato não compactado para alta qualidade/resolução. Nos principais sistemas de *blockchain*, como *Bitcoin* e *ethereum*, eles empregam valores hexadecimais para codificar elementos de transação, como nomes de funções, parâmetros e valores de retorno [Wang *et al.* 2021]. Isso implica que os dados NFT brutos devem seguir essas regras. Se alguém afirma que possui a propriedade intelectual baseada em NFT, ele possui essencialmente a parte original dos valores hexadecimais assinados pelo criador. Outros podem copiar livremente os dados brutos, mas não podem reivindicar o original. Com base nisso, pode-se observar que as atividades relacionadas a NFT (por exemplo, compra/venda/negociação/leilão) devem ser processadas nessas quatro fases, semelhante ao procedimento básico de processamento de contratos inteligentes [Wang *et al.* 2021].

Os padrões do *token ethereum* garantem que um determinado ativo se comportará de uma maneira específica e especificam como as pessoas podem interagir com as funções básicas do ativo [Ethereum Articles 2022]. Vários padrões *ethereum* suportam a criação e negociação de NFTs. Por exemplo, o ERC-721 [William Entriken 2018], proposto em 2018 é usado exclusivamente para criar NFTs. Ele fornece funcionalidades como transferir *tokens* de uma conta para outra, obter o saldo atual de uma conta, obter o proprietário de um *token* específico e obter o fornecimento total de um *token* disponível na rede [Ethereum Articles 2022]. O ERC-1155 [Witek Radomski 2018] proposto no mesmo ano também pode ser usado

para criar NFTs.

### 2.3.5 Padrões de projeto

Com a finalidade de explicar o processo de criação de um NFT, Qin Wang apresenta dois padrões de projeto para o paradigma NFT, com ênfase em seus protocolos, padrões de *token* e propriedades de chave [Wang *et al.* 2021]. O primeiro é o chamado *Design top-down* (cima para baixo) ele é aplicado sobre um intuito muito simples, construir NFTs do indicador e depois vendê-los ao comprador. Em contraste, o segundo padrão de projeto inverte esse caminho, definir um NFT e cada usuário ter o poder de criar seu próprio NFT, a ele é dado o nome *Bottom-up* (baixo para cima). Deve-se notar que, ambos seguem um fluxo de trabalho muito semelhante quando executados em sistemas *blockchain* o que significa que designs diferentes não alterarão o mecanismo operacional subjacente. [Wang *et al.* 2021]. O fluxo de trabalho dos sistemas NFT é ilustrado na Figura 2.8



**Figura 2.8:** Fluxo de trabalho dos sistemas NFT [Wang *et al.* 2021]

O primeiro padrão de projeto a ser apresentado é *top-down*. O protocolo aplicado a este consiste em dois papéis, proprietário da NFT e comprador da NFT [Wang *et al.* 2021]. Ele segue da seguinte maneira:

- **Digitalização NFT.** Um proprietário de NFT verifica se o arquivo, título e descrição são completamente precisos. Em seguida, ele digitaliza os dados brutos em um formato adequado [Wang *et al.* 2021].
- **Loja NFT.** Um proprietário de NFT armazena os dados brutos em um banco de dados externo fora do *blockchain*. Observe que ele também pode armazenar os dados brutos dentro de um *blockchain*, apesar de essa operação consumir possuir um gasto [Wang *et al.* 2021].

- **Sinal NFT.** O proprietário da NFT assina uma transação, incluindo o *hash* dos dados da NFT e, em seguida, envia a transação para um contrato inteligente [Wang *et al.* 2021].
- **NFT Mint&Trade (cunhar e trocar).** Depois que o contrato inteligente recebe a transação com os dados NFT, o processo de cunhagem e negociação começa. O principal mecanismo por trás dos NFTs é a lógica dos *Token Standards* <sup>6</sup> [Wang *et al.* 2021].
- **Confirmação NFT.** Uma vez que a transação é confirmada, o processo de cunhagem é concluído. Por essa abordagem, os NFTs se vincularão para sempre a um endereço *blockchain* exclusivo como evidência de persistência [Wang *et al.* 2021].

O segundo padrão a ser apresentado é o *bottom-up*. o seu protocolo consiste em dois papéis: criador de NFT e comprador de NFT. Na maioria dos casos, um comprador também pode atuar como criador porque um produto NFT é criado com base em sementes aleatórias quando um comprador faz lances por ele. Isso estende as funções em termos de personalização do usuário [Wang *et al.* 2021]. Ele vai seguir da seguinte maneira:

- **Criação de modelo.** O fundador do projeto inicia um modelo por meio do contrato inteligente para configurar várias regras básicas, como diferentes recursos (estilo de personagem, armas ou acessórios) no jogo [Wang *et al.* 2021].
- **NFT customização.** Uma vez que um comprador faz um lance para um NFT, ele pode personalizar o produto NFT com um conjunto de recursos adicionais além das linhas básicas. Esses recursos adicionais são selecionados aleatoriamente de um banco de dados que foi predefinido no estado inicial [Wang *et al.* 2021].
- **NFT Mint&Trade.** Depois que o contrato inteligente recebe a transação com os dados NFT, o processo de cunhagem e negociação começa [Wang *et al.* 2021].
- **Confirmação NFT.** Todos os procedimentos são realizados por meio de contratos inteligentes. O NFT gerado será armazenado persistentemente na cadeia quando o procedimento de consenso for concluído [Wang *et al.* 2021].

Em um sistema *blockchain*, cada bloco tem uma capacidade limitada. Quando a capacidade de um bloco ficar cheia, outras transações entrarão em um bloco futuro vinculado ao bloco de dados original. No final, todos os blocos vinculados criaram um histórico de longo prazo que permanece permanente. O sistema NFT, em essência, é um aplicativo baseado em *blockchain*. Sempre que um NFT é cunhado ou vendido, é necessário enviar uma nova transação para invocar o contrato inteligente. Após a confirmação da transação, os metadados

---

<sup>6</sup>Um padrão de *token* é uma interface, e um conjunto de regras, que um contrato inteligente deve respeitar para ser compatível com os padrões comuns. Normalmente, os padrões de *token* definem como os *tokens* podem ser transferidos e como manter um registro consistente dessas transferências na rede Tezos

da NFT e os detalhes de propriedade são adicionados a um novo bloco, garantindo assim que o histórico da NFT permaneça inalterado e a propriedade seja preservada [Wang *et al.* 2021].

### 2.3.6 Padrões de Token

O padrão de *token* mais usado vem do ERC-20<sup>7</sup> [Vogelsteller 2015]. Ele introduz o conceito de *tokens* fungíveis que podem ser emitidos em cima da rede *ethereum* uma vez que satisfaçam os requisitos. A *ethereum* e a *BinanceNFT* são responsáveis pela maior parte da divulgação deste padrão, DApps que surgem baseados em *blockchain* muitas vezes obtêm financiamento inicial suficiente devido a esta divulgação [Wang *et al.* 2021]. O padrão ERC-721 [William Entriken 2018] foi teorizado especificamente para NFTs ele que introduz um *token* não fungível que difere do *token* fungível. Ou seja, o tornando único. A NFT tem uma variável `uint256` chamada *tokenId*, e o par de endereço do contrato e `uint256 tokenId` é exclusivo. O *tokenId* pode ser usado como entrada para gerar identificações especiais, características que vão diferenciar fisicamente cada NFT por exemplo imagens na forma de cães pode se diferenciar de outras criando padrões únicos e em seu código fonte [Wang *et al.* 2021].

Wang Qin explica que o padrão ERC-1155 (Padrão Multi Token) [Witek Radomski 2018] estende a representação de *tokens* fungíveis e não fungíveis. Ele fornece uma interface que pode representar qualquer número de *tokens*. Nos padrões anteriores, cada *tokenId* em contato contém apenas um único tipo de *token*. Por exemplo, o ERC-20 faz com que cada tipo de *token* seja implantado em contratos separados. Além disso, o ERC-721 implanta o grupo de *tokens* não fungíveis em um único contrato com as mesmas configurações. Em contra partida, o ERC-1155 estende a funcionalidade do *tokenId*, onde cada um deles pode representar independentemente diferentes tipos de token configuráveis [Wang *et al.* 2021]. O campo pode conter suas informações personalizadas, como meta-dados, tempo de bloqueio, data, fornecimento ou quaisquer outros atributos [3]. A Figura 2.9 ilustra a estrutura básica de um *token* em cada padrão mencionado.

Os esquemas NFT são essencialmente aplicações descentralizadas, portanto independente do padrão em qual foi construído eles aproveitam os benefícios e propriedades atribuídas a *blockchain* a qual o mesmo vai esta vinculado, de tau maneira que é possível resumir suas propriedades da seguinte forma [Wang *et al.* 2021].

- **Verificabilidade.** O NFT com seus metadados de *token* e sua propriedade podem ser verificados publicamente.
- **Disponibilidade.** O sistema NFT nunca cai. Alternativamente, todos os *tokens* e NFTs emitidas estão sempre disponíveis para venda e compra.

---

<sup>7</sup>ERC-20 é um padrão de desenvolvimento para criação de tokens fungíveis (ou seja, intercambiáveis) na rede Ethereum, como moedas digitais, stablecoins, tokens de governança e tokens de segurança.

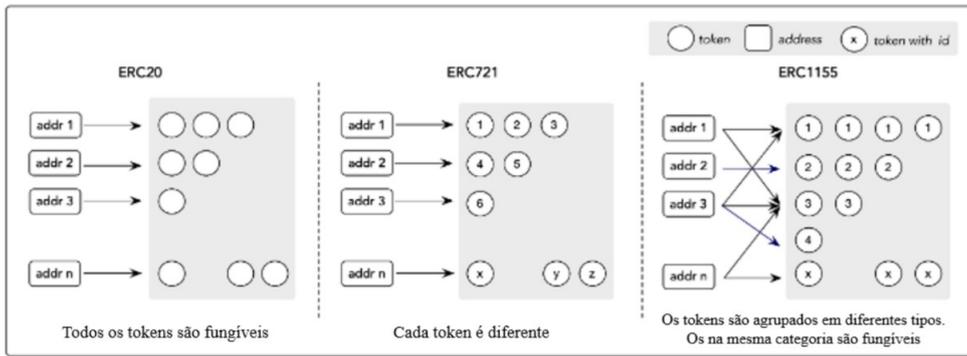


Figura 2.9: Padrões de Token NFT [Wang et al. 2021]

- **Resistência à adulteração.** Os metadados NFT e seus registros de negociação são armazenados de forma persistente e não podem ser manipulados uma vez que as transações sejam consideradas confirmadas.
- **Usabilidade.** Cada NFT tem as informações de propriedade mais atualizadas, que é fácil de usar e informações claras.
- **Atomicidade.** A negociação de NFTs pode ser concluída em uma transação atômica, consistente, isolada e durável (ACID). Os NFTs podem ser executados no mesmo estado de execução compartilhado.
- **Negociabilidade.** Cada NFT e seus produtos correspondentes podem ser negociados e trocados arbitrariamente.

# Capítulo 3

## Metodologia

Este trabalho considera a hipótese de que estudantes dos cursos da área de computação do IFPB, *campus* Campina Grande, tanto do ensino médio quanto do superior, possuem pouco conhecimento sobre a tecnologia NFT, desconhecendo as oportunidades que a mesma pode oferecer para atuação de um profissional de TI no mercado de trabalho.

Dessa forma, considerou-se a questão **De que formas um futuro profissional de TI pode aderir/beneficiar-se deste mercado?** Com base na hipótese apresentada, esta pesquisa é abordada como exploratória [Gil 2002]. Ela não apenas tem como foco resolver um problema, com base na revisão bibliográfica, mas também tem como escopo investigar o caso, levantar questionamentos, desenvolver e apresentar novas ideias com base em um estudo do objeto.

Para a plena execução do trabalho, foram utilizados três procedimentos técnicos: (1) a pesquisa bibliográfica, visto que parte dos dados que compõem este estudo estão já analisados e publicados em meios escritos e eletrônicos, como livros, artigos científicos e páginas da internet; (2) e pesquisa documental, que é caracterizada pelo uso de fontes mais diversificadas e dispersas; algumas delas não possuem tratamento analítico, tais como blogs e wikis; (3) e uma pesquisa quantitativa, com vistas a validar a hipótese e auxiliar na compreensão dos dados obtidos.

De forma detalhada, o presente trabalho foi construído com base nas seguintes etapas:

- **Levantamento bibliográfico.** Seleção das fontes bibliográficas utilizadas como referencial teórico da pesquisa, com o objetivo de reconhecer os aspectos técnicos e históricos do objeto de estudo: NFT. Além de escritos oficiais como artigos científicos publicados, trabalhos de conclusão de curso, periódicos e um livro foram utilizados, assim como notícias e artigos veiculados em sites especializados sobre o ecossistema dos NFTs e suas tecnologias. Os principais artigos utilizados neste pesquisa foram:

*“Demystifying Non Fungible Tokens (NFTs)” [Blockchain e team 2021], “Non-Fungible Token (NFT): Overview Evaluation Opportunities and Challenges” [Wang et al. 2021], “A Taxonomy of Blockchain Technologies: Principles of Identification and Classification” [Tasca e Tessone 2017], “Correntes de Blocos: Algoritmos de Consenso e Imple-*

mentação na Plataforma *Hyperledger Fabric*” [Rebello *et al.* 2019], e “*Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*” [Fairfield 2022] e

Os trabalhos de conclusão de curso de maior destaque foram: “Introdução às criptomoedas: Uma Análise de Possíveis Impactos na economia, investimentos e contabilidade” [Maciel 2019], “*Blockchain*” [GOUVEIA 2021] e “Tecnologia *Blockchain* e as suas possíveis aplicações no processo de comunicação científica” [Figueiredo 2022].

Os materiais informais em destaque desta pesquisa foram a *Binance Academy* e *Ethereum Academy*.

- **Construção e divulgação do questionário.** Por meio da plataforma *Google forms*, foi elaborado um questionário com nove quesitos (Apêndice A). O questionário foi enviado para as listas de e-mails dos estudantes dos cursos superiores de Telemática e de Engenharia da Computação e dos cursos técnicos de Manutenção e Suporte em Informática.
- **Análise das respostas obtidas.** Foi realizada uma análise quantitativa das respostas obtidas com o formulário que foi enviado aos estudantes matriculados no IFPB. A identidade dos participantes da pesquisa foi mantida em sigilo para proteção dos mesmos e evitar qualquer tipo de constrangimento. Os dados não foram baixados nem salvos em servidores físicos. O arquivo csv gerado continua salvo no *Google Drive*, onde todo acesso foi feito de forma online com auxílio de VPN para maior proteção e apenas com o uso do e-mail institucional. O único colaborador que teve acesso aos dados foi o orientador deste trabalho.
- **Indicação das oportunidades de atuação no mercado NFT.** Por fim, após a análise e discussão dos dados, foi realizada uma investigação usando como métrica os resultados obtidos a fim de levantar um material conciso e informativo a respeito das oportunidades que rege o mercado NFT com ênfase na área de TI.

## 3.1 Hipótese

Resumidamente, os tokens não-fungíveis representam uma tecnologia que permite adquirir e validar propriedade de arquivos digitais. Esta tecnologia depende da tecnologia de *blockchain* herdando assim suas propriedades e características e sua prática é possível graças aos padrões de melhoria apresentados pela plataforma descentralizada *ethereum*, o ERC-721 e ERC 1155. Apenas com o conceito básico que é “adquirir e validar arquivos digitais”, abre-se um leque de possibilidades de onde e como esta tecnologia pode ser aplicada, justificando assim a grande quantidade de projetos NFT existentes no mercado, e projetos que estão em desenvolvimento como exemplo de Star Atlas, Imaginary Ones, Illuvium, Invisible Friends, SolSand, Autograph.

É possível observar pelo serviço *Google Trends* que o interesse de pesquisa a respeito dos NFT vem reduzindo desde o início do ano, como pode ser visualizado na Figura 3.1. Entretanto, mesmo com a queda da quantidade de buscas, o comércio de NFT tem sido bastante lucrativo, como pode ser visto na Figura 3.2, que exhibe dados de volume de *trading*<sup>1</sup> das últimas 24 horas do dia 13 de agosto 2022 retirados da *CoinGecko*<sup>2</sup>. Um valor superior a 2 bilhões de dólares e uma capitalização total de mercado superior a 21 bilhões de dólares. A título de comparação, na semana anterior à apresentada, a capitalização total de mercado estava em um valor de 20 bilhões, demonstrando assim um aumento de 5% na capitalização em apenas uma semana.

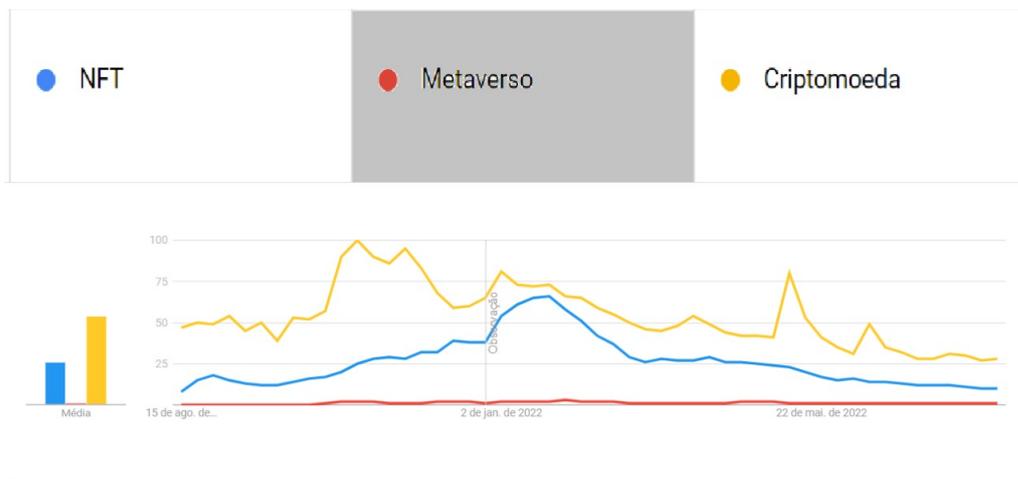


Figura 3.1: Gráfico de interesse a respeito de NFT dos últimos 12 meses [orig.google Trends]

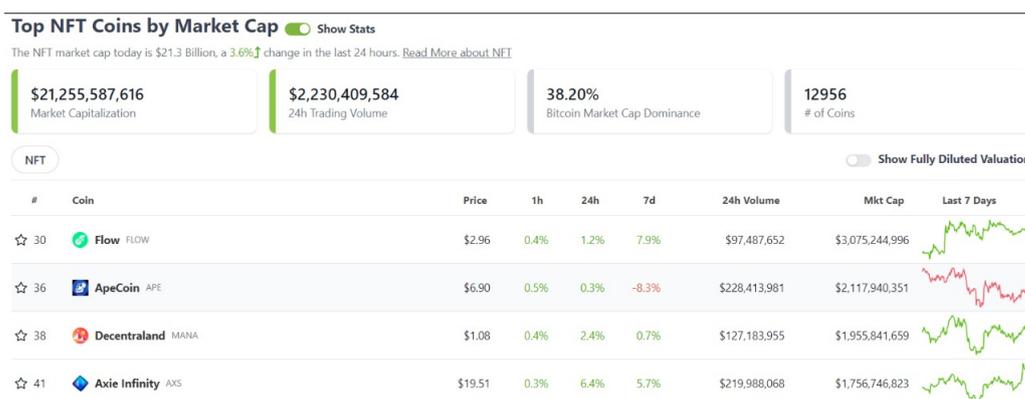


Figura 3.2: Capitalização total do mercado NFT [Coingecko 2022] meses

A principal motivação deste trabalho partiu da hipótese de que estudantes de cursos de tecnologia do IFPB, *campus* Campina Grande, podem não estar cientes das oportunidades de atuação nesse mercado, as quais vão além de entrar no mercado através das plataformas do *marketplace*, mas também por meio de atuações de desenvolvimento e/ou pesquisa. Afinal,

<sup>1</sup>Prática de compra, venda e troca de ativos no marketplace.

<sup>2</sup>CoinGecko é uma plataforma que agrupa dados sobre o mercado cripto

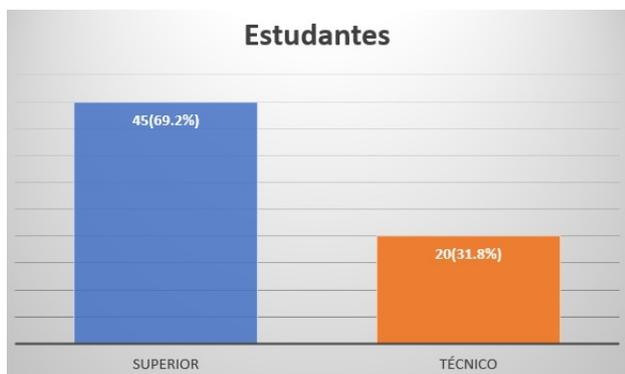
o que torna o NFT valioso é sua tecnologia, seu conceito pode ser aplicado a diversas áreas como por exemplo segurança de sistemas de TI, que é uma temáticas importante para um estudantes de um curso superior de telemática. Dito isso, o capítulo seguinte apresenta a análise das respostas obtidas com o questionário seguida .

# Capítulo 4

## Análise dos Dados

Como já informado na metodologia, o formulário foi enviado a estudantes matriculados no IFPB. Não foi concedida nenhuma recompensa àqueles que respondessem o formulário. No e-mail enviado havia apenas um breve informe a respeito do objetivo central da pesquisa, “destacar e informar as oportunidades de atuação no mercado de NFTs por profissionais da área de teleinformática”. A ideia era observar quantos estudantes demonstrariam interesse no tema com base no valor total de respostas obtidas.

Após um intervalo total de três semanas, obteve-se um total de 65 respostas, as quais podem ser divididas em dois grupos de estudantes: um grupo majoritário de estudantes dos cursos superiores (engenharia de computação e telemática); e estudantes do ensino médio matriculados no curso técnico em manutenção e suporte em informática (figuras 4.1 e 4.2).



**Figura 4.1:** Relação total de participantes



**Figura 4.2:** Divisão, percentual por curso

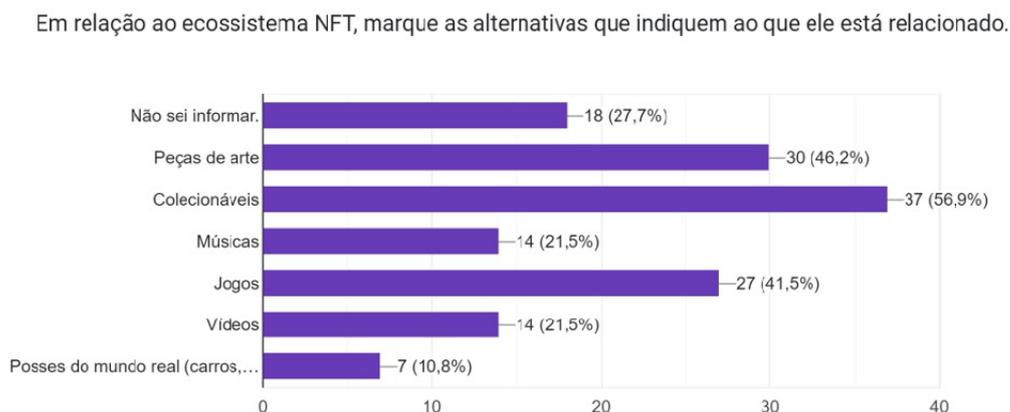
O questionário foi composto de nove perguntas de múltipla escolha. As duas primeiras perguntas solicitavam o nome do curso e em qual período o estudante se encontrava. O propósito foi observar se havia relação entre o tempo e tipo de curso com o nível de conhecimento a respeito do ecossistema NFT. A resposta a esta investigação é aplicada ao decorrer da análise individual de cada questionamento.

Em sequência, é dada uma lista de itens, e apresentado o seguinte informe: “Em relação ao ecossistema NFT, marque as alternativas que indiquem ao que ele está relacionado”. A

lista era composta dos seguintes termos: peças de arte, colecionáveis, músicas, jogos, vídeos, posses do mundo real (carros, imóveis, etc), e também existia a possibilidade de marcar a opção “não sei informar”. Nesse questionamento o tempo de curso não possui grande influência, visto que os 18 que marcaram a opção “não sei informar” estão divididos entre todos os dois grupos e três cursos e espalhados entre todos os períodos. Já o curso denota um valor significativo, já que aqueles que marcaram todas as opções válidas, ou pelo menos as mais populares, estavam matriculados nos cursos de engenharia de computação. Dos 47 que relacionaram o NFT a algum dos itens da lista é possível fazer algumas observações:

- 80% (37 de 47) acreditam que o NFT está correlacionado a itens colecionáveis, sendo que 10 estudantes marcaram apenas itens colecionáveis.
- O segundo item mais marcado foi peças de arte, com 30 de 47. Deste grupo, duas pessoas marcaram apenas peças de arte.
- O item menos marcado foi ‘Posses do mundo real’, marcado por 7 de 47, dos quais somente um marcou apenas essa opção.

Neste ponto já é perceptível um desconhecimento a respeito da abrangência de uso de um NFT, dado que mesmo dentro do grupo que demonstrou certo conhecimento a respeito, apenas seis estudantes marcaram todas as opções, já que todos os itens podem ser relacionados a NFT. No geral, para tornar-se um NFT é preciso ser algum item digital (e.g., jogos, músicas, obras de arte digitais). Entretanto, os NFTs também podem ser vinculados a obras de arte e posses do mundo real como objetos físicos. Nesses casos, a chave privada para uma carteira contendo o NFT geralmente é embutida ou fornecida com a peça. A relação total das respostas do primeiro questionamento pode ser observada na Figura 4.3.



**Figura 4.3:** Percentual em barras para o 3º questionamento

Como foi expresso na Seção 2.3.1, o NFT tem sua origem associada a *ethereum*, que é um tipo de criptomoeda derivada dos contratos inteligentes. A plataforma do *ethereum*

permite que os desenvolvedores criem e implementem aplicativos descentralizados. Além disso, qualquer serviço centralizado pode ser descentralizado usando a plataforma.

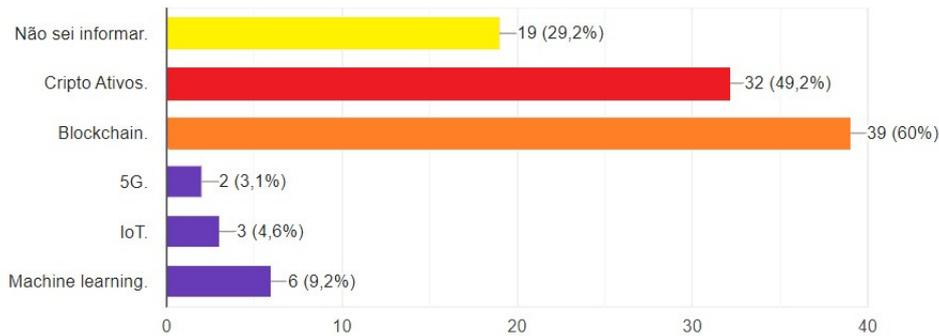
O potencial da plataforma *ethereum* é de criar aplicativos não limitados por outra coisa que não seja a criatividade daqueles que a usam. Para criar um NFT, é preciso estar familiarizado com o conceito de cunhar (transformar em moeda). A criação de um *token* exige uma *blockchain* específica, que pode ser a da *ethereum*, e a carteira digital mais utilizada é a *metamask* que justamente funciona nesta rede. Ou seja, a *ethereum* está intimamente relacionada aos NFTs, de forma que conhecer a plataforma já é um grande passo que facilita não apenas no entendimento do ecossistema NFT como também auxilia em sua aplicação. Devido a sua popularidade, é natural acreditar que mesmo sem conhecer NFTs, muitos dos estudantes, ao menos ouviram falar da plataforma. Para confirmar essa dedução foi inserido no formulário a pergunta “Você já ouviu falar da *Ethereum*?”, em que a maioria (73,8%) respondeu afirmativamente. Alguns dos alunos que não souberam informar ao que o ecossistema dos NFTs estava relacionado, também marcaram que sim, confirmando que mesmo não sabendo informar ao que os NFTs se relacionam, é notório a popularidade da plataforma. Também não se percebeu influência entre o tempo de curso ou a diferença de curso nos resultados dessa questão.

Outro levantamento foi saber se os participantes tinham conhecimento a respeito das tecnologias que estavam relacionadas ao NFT. Como já mencionado, o NFT só existe por causa da tecnologia *blockchain* e da rede *Ethereum*. A pergunta “Quais tecnologias estão relacionadas aos NFTs ?” teve esse propósito. Na lista de opções apresentadas, foram adicionadas algumas que não possuíam relação direta com NFTs. A lista completa de itens consistia nos seguintes termos: criptoativos, *blockchain*, 5G, IoT e *machine learning*. Analisando as respostas (Figura 4.4), é possível observar que:

- Poucos participantes marcaram as alternativas erradas. Três escolheram 5G, quatro, IoT, e sete *Machine learning*.
- A maioria soube relacionar o NFT a pelo menos uma de suas tecnologias, visto que 39 de 65 selecionaram *Blockchain*.
- Pôde-se observar que poucos participantes marcaram as opções erradas (i.e., IoT e 5G).

Até aqui, já é possível observar que para os que demonstraram algum nível de conhecimento a respeito da tecnologia NFT:

- De 65, apenas três demonstraram um total conhecimento a respeito da tecnologia, acertando todas as questões até este ponto.
- É possível observar que o tempo de curso tem impacto nas respostas, sendo que dos três estudantes em questão, dois eram alunos do 9º período de Engenharia de Computação e um do 7º período do curso de Telemática.



**Figura 4.4:** *Relação das respostas em barras*

Levando em consideração que todos os participantes eram de cursos de tecnologia, julgou-se pertinente perguntar também se os estudantes saberiam criar um NFT. Os dados refletiram que (Figura 4.5):

- 48 de 65 responderam que não.
- Nesse grupo, está contido um grande número de participantes que havia correlacionado os NFTs a pelo menos uma tecnologia ou a itens de seu ecossistema, 20 de 48.
- Para os que marcaram que sim, nota-se que em sua maioria já cursou pelo menos 5 períodos de curso superior, e para os estudantes de nível técnicos, estão alocados no 3° ano.

Atualmente, criar um NFT não é uma tarefa limitada a desenvolvedores, pois existem empresas especializadas que facilitam esse tipo de registro. Os interessados em cunhar podem recorrer a plataformas a exemplo da *OpenSea*<sup>12</sup>. A única coisa que é preciso fazer é possuir um ativo e inserir valores. Todo o trabalho é feito de forma automática pelas plataformas, que, além do registro, da custódia e da transferência, podem cuidar da curadoria, da comercialização e da distribuição dos NFTs, restando ao dono do ativo apenas colher o resultado da operação. Vale ressaltar que esse tipo de operação é majoritariamente voltada para itens que vão ser lançados no *marketplace*. Para outros tipos de aplicação do NFT, é necessário algum tipo de conhecimento específico.

Dado o crescimento do mercado e a popularização da tecnologia *blockchain* é esperado que, mesmo sem ter total conhecimento a respeito da tecnologia NFT, os participantes já tivessem ouvido falar de seu mercado. Para investigar essa suposição, foi requisitado no questionário: “Marque o que você sabe a respeito do mercado de NFT’s e suas oportunidades”. Os participantes poderiam escolher dentre três opções: “Eu nunca ouvir falar sobre o mercado de NFT’s”, “Eu ouvir falar sobre o mercado de NFT’s, mas não sei especificar quais são suas

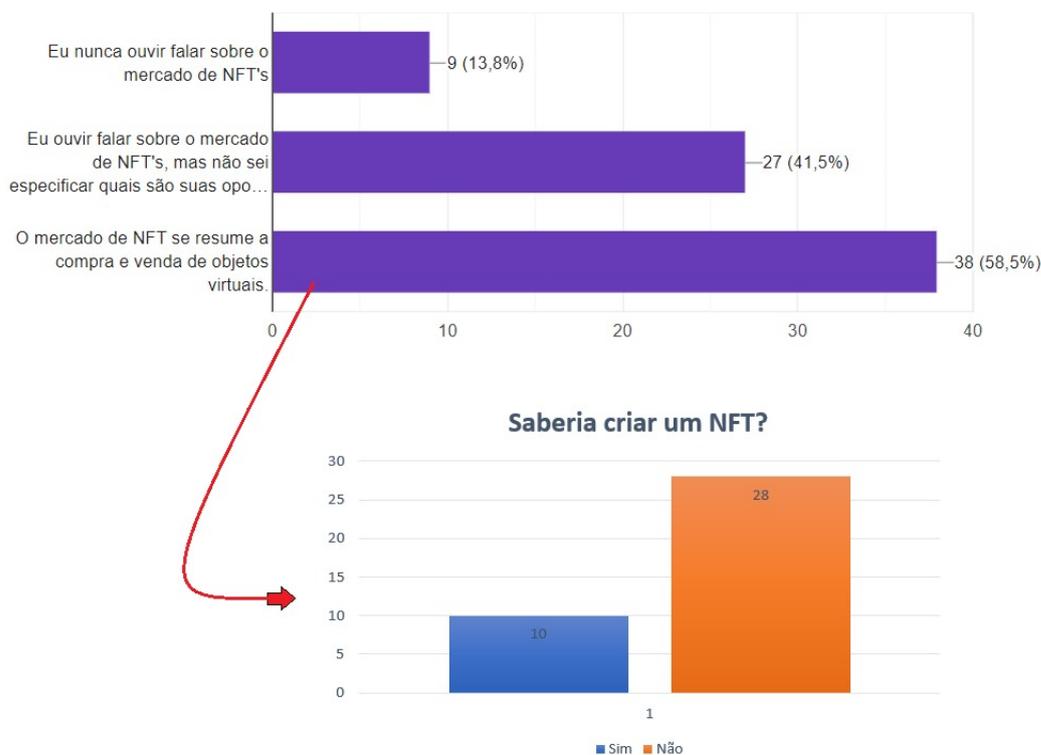
<sup>1</sup>OpenSea é um mercado para compradores e vendedores de tokens não fungíveis (NFTs). A plataforma também disponibiliza meio para cunho de nNFT de maneira simplificada.

<sup>2</sup><https://opensea.io/>

oportunidades.“ e “O mercado de NFT se resume a compra e venda de objetos virtuais.” A resposta dessa pergunta confirma uma suposição feita no início deste trabalho, de que os estudantes tinham pouco conhecimento sobre NFT. Quase 60% dos participantes acreditam que o mercado de NFT se resumem a compra e venda de objetos virtuais (Figura 4.5). Além disso se observarmos apenas estes 60% que representa 38 participantes:

- Dos 11 estudantes que informaram saber criar um NFT, 10 deles estão contidos neste grupo.
- Os 28 restantes, demonstraram ter certo conhecimento a respeito da tecnologia, relacionando a mesma a ativos digitais, jogos, músicas e etc,

Essa última afirmação não está completamente equivocada, mas ela limita muito a aplicação da tecnologia. O conceito de *token não fungível* basicamente está relacionado ao registro de um ativo em *blockchain*. Dessa forma, qualquer ativo que tenha apenas um dono pode virar um ativo digital. Não necessariamente para ser comercializado, um exemplo simples de uso alternativo está na certificação de uma ID digital, que pode ser usada para acesso único ou identificação. Nesse exemplo o NFT não estaria sendo utilizado como produto a ser comercializado, mas a tecnologia está sendo utilizada para manter uma identidade única e segura.



**Figura 4.5:** *Conhecimento sobre o mercado de NTF's e suas oportunidades*"

Para contribuir na validação da pesquisa, fez-se ainda a seguinte pergunta: “Você está informado a respeito das oportunidades de atuação no mercado de NFT ? Se sua resposta

for não, indique seu nível de interesse.”. Evidentemente, o objetivo dessa pergunta é saber se o participante conhece o mercado e, caso não, se gostaria de ser informado. Com as respostas que podem ser conferidas na Figura 4.6, a maioria informou que não estava informada e que gostaria de saber a respeito, o que contribui positivamente para a relevância deste trabalho.

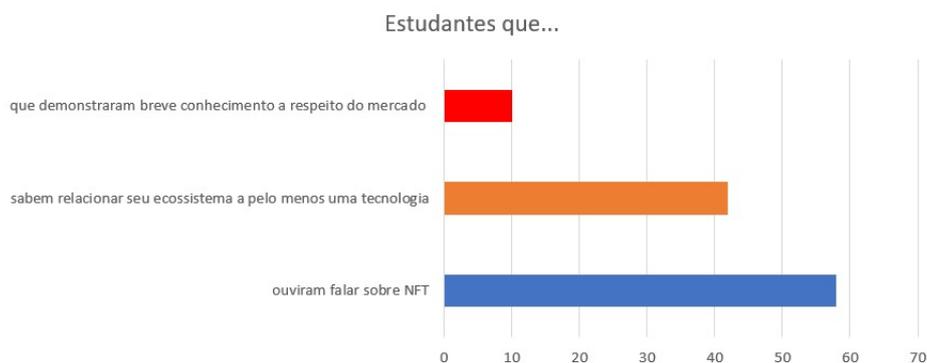


**Figura 4.6:** *Nível de interesse dos participantes.*

## 4.1 Discussão

Foi possível verificar que a maioria dos participantes desconhece do total potencial deste mercado, mas também demonstram querer conhecer mais sobre NFT. Essa afirmação foi feita sobre a seguinte investigação e que pode ser vista na Figura 4.7, em que:

- 58 de 65, demonstraram ao menos ter ouvido falar sobre NFT.
- 42 de 65 souberam relacionar ao mínimo de uma tecnologia que possui relação direta com seu ecossistema.
- Mas apenas 10 de 65 tinham conhecimento sobre o mercado.



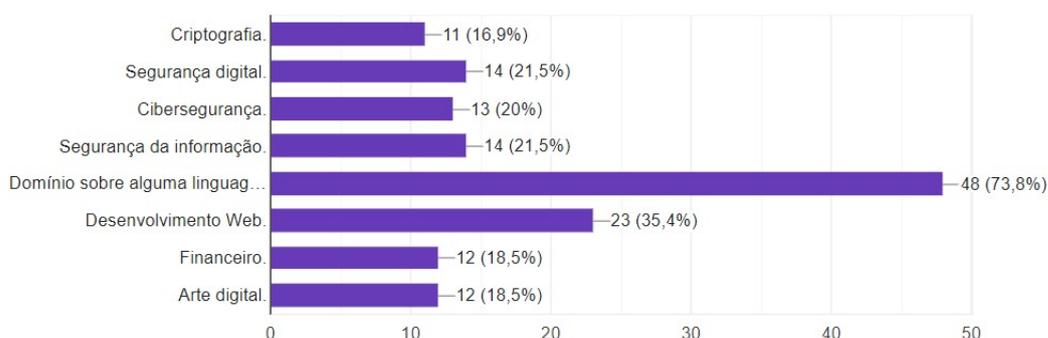
**Figura 4.7:** *Análise conclusiva*

Com base nessa última afirmação, foi feita uma investigação correlacionando as respostas obtidas individualmente, de modo que foi possível determinar um perfil para os sete participantes que não demonstraram interesse a respeito do mercado NFT. Notou-se que:

- Seis dos sete já ouviram falar da *Ethereum*.
- Cinco dos sete conseguiram associar o NFT a *blockchain*,
- E os sete indicaram que ‘O mercado de NFT se resume a compra e venda de objetos virtuais’.

Como foi sugerido na introdução deste trabalho, um dos fatores que fazem com que profissionais da área de TI desconheçam do potencial do NFT é exatamente o preconceito em relação a tecnologia. É claro que a compra e venda de ativos digitais representa grande parte do mercado NFT, mas ele não se resume apenas a isto. Outros mercados vêm se beneficiando com os NFTs, como por exemplo a indústria de jogos, eventos virtuais, segurança da informação, desenvolvimento de DApp’s e até mesmo o recente *Metaverso*<sup>3</sup>. Conhecer a tecnologia não apenas possibilita mais oportunidades para se trabalhar no *marketplace*, mas também conhecer as áreas onde esta tecnologia pode ser aplicada, concedendo a estes profissionais uma vantagem sobre os que desconhecem a tecnologia.

Caso fosse de interesse dos participantes serem informados a respeito das oportunidades oferecidas pelo mercado NFT, foi adicionado ao formulário uma questão que tinha como objetivo servir de métrica para a investigação a respeito das áreas específicas a serem informadas. Dada a variedade de oportunidades que o NFT oferece, esse questionamento serviu de base de escolha de quais pre-requisitos o trabalho deveria focar. O quesito era “Marque os tópicos abaixo que você tem um nível de conhecimento satisfatório”. As respostas podem ser vistas na Figura 4.8.



**Figura 4.8:** *Relação das respostas*

Com base nas repostas obtidas, o formulário valida de forma quantitativa que dentro do grupo de estudantes que participaram da pesquisa, a maioria gostaria de saber mais a respeito do mercado NFT. Com base nessa métrica, o próximo capítulo é dedicado a trazer informes sobre as mais promissoras oportunidades, dentre carreiras e possíveis tendências que devem surgir juntamente com o advento do mercado NFT.

<sup>3</sup>Metaverso é a terminologia utilizada para indicar um tipo de mundo virtual que tenta replicar a realidade através de dispositivos digitais.

# Capítulo 5

## Oportunidades

Uma das principais oportunidades de atuação e aplicação junto ao mercado NFT é a própria Web3. Aplicativos descentralizados, finanças descentralizadas, tokens não-fungíveis e criptomoedas compartilham da mesma palavra-chave: “descentralização”, e todos utilizaram como base a tecnologia *blockchain*. Entender um pouco o que é Web3 ajuda a visualizar de maneira natural as oportunidades no mercado NFT, tanto em seu desenvolvimento quanto em sua aplicação. Como a grande maioria apontou conhecer pelo menos uma linguagem de programação, foi escolhido áreas de aplicação, onde seu principal pre-requisito é possuir conhecimento em programação.

### 5.1 Web3

O termo Web3 foi cunhado em 2014 pelo britânico Gavin Wood, cofundador da criptomoeda *ethereum*, ao lado russo-canadense Vitalik Buterin. Wood partiu da ideia de que era necessário “remodelar a internet”: criar uma nova arquitetura com um protocolo específico para que os serviços fossem descentralizados [Wang *et al.* 2022]. Para tornar isso em realidade, wood criou a *Web3 Foundation* com o objetivo de financiar equipes de investigação e desenvolvimento que estão construindo as bases da Web3, e criou a *Parity Technologies*, uma empresa de infraestrutura *blockchain*, com sede em Berlim (Alemanha), quem tem como foco a “web descentralizada”.

O principal objetivo da Web3 é “trazer a internet de volta a sua origem”, Em seu início, a internet foi um protocolo aberto e descentralizado, sua centralização se deu início em 1990 com as grandes empresas de tecnologia que conhecemos hoje. A Web3 promete descentralizar a rede e limitar a influência das grandes empresas de tecnologia, permitindo que as pessoas possam escolher em qual centro de dados suas informações serão armazenadas [Wang *et al.* 2022]. Um relatório publicado pela *IP Capital Partners*<sup>1</sup> em dezembro 2021 com o título “*Web3: Cripto, Blockchain, NFT (We3-CBN)*”, discorre de forma simples e direta como os princípios da Web3 podem ser utilizados na prática e na evolução do mercado financeiro

---

<sup>1</sup>Empresa de gestão de recursos Brasileira

digital, partindo do próprio paradigma “dinheiro na internet” [Web3-cbn 2021].

No relatório é dito que hoje o dinheiro é basicamente digital, lidamos com ele via aplicativos bancários, e contas podem ter seu débito automatizado ao se vincularem por meios de pagamento como cartões de crédito e débito. O pix também é um modo digital que se popularizou durante o período da pandemia (outubro de 2020). Com isso em mente uma rede ou sistema comercial construído dentro dos parâmetros da Web3 pode receber pagamentos de forma global e de maneira instantânea de qualquer outro participante da rede apenas comunicando o endereço de sua conta, e toda a segurança seria garantida devido as características de uma rede *blockchain* [Web3-cbn 2021]. Exemplo:

- Desenvolvedores podem introduzir aos serviços de paginação virtuais botões, que com apenas um clique do usuário, realizam uma cobrança de qualquer valor dada a prestação do serviço seja lá qual for (jogos, compra e venda de produtos, visualização de colecionáveis, serviços streaming, etc). E os usuários precisam apenas associar uma carteira digital como o exemplo da *MetaMask*,<sup>2</sup> aos seus navegadores ou celulares para participarem desse sistema. A promessa, num estágio maduro da tecnologia, é que eliminem taxas de transação e atrito de cadastro, tornando microtransações digitais algo trivial.

A tokenização (discorrida na subseção 2.1.3) tem grande aplicação dentro da Web3. Na Web3 é conceituado que usuários possam criar, deter e transferir ativos digitais, de maneira que sejam únicos e que possam representar suas propriedades de direito a algo físico ou digital, este é garantido por meio dos *tokens* (Definido na subseção 2.2.1). No relatório Web3-CBN [Web3-cbn 2021] é indicado que a Web3 possibilita a associação de *tokens* a códigos abertos, permitindo assim a remuneração em desenvolvimento de redes *open source*. Deste forma programadores possuem um incentivo financeiro para lançar seu códigos em soluções abertas, agilizando assim o processo de desenvolvimento de novos serviços [Web3-cbn 2021]. Exemplo de plataformas que já aplicam este tipo de incentivo financeiro de programação em *open source* é *Ethereum* e a *polygon*<sup>3</sup>.

De maneira resumida Web3, é um ecossistema descentralizado online baseado na tecnologia de *blockchain*. Ou seja, os serviços e páginas online serão produzidos em uma rede de computadores imutável e que garantirá a funcionalidade deles sem censura e restrições por parte de uma única instituição, oferecendo maior controle para o usuário. Seus conceitos e características facilitam a transferência de valores através de ativos digitais, a tecnologia que consegue englobar todas as características presentes na Web3 é o NFT. Com isso em foco apresento nos tópicos sub-sequentes algumas oportunidades de aplicação na Web3 que é possível graças à tecnologia NFT.

---

<sup>2</sup>*MetaMask* é uma carteira de criptomoeda de software usada para interagir com o *blockchain Ethereum*

<sup>3</sup>Polygon trata-se de um projeto com um protocolo que permite uma estrutura capaz de construir e conectar redes *Blockchain* que sejam compatíveis com a rede *Ethereum*

### 5.1.1 Eventos Virtuais

Outra grande oportunidade que entra em destaque são os eventos virtuais. A Web3 se torna palco para artistas e organizadores de eventos. Os eventos online tradicionais contam com empresas centralizadas que fornecem confiança e tecnologia. A *blockchain* já assume vários tipos de atividades, como arrecadar dinheiro (através das criptomoedas), mas suas aplicações são restritas a uma pequena variedade de eventos. As NFTs estendem muito o escopo destas aplicações com a ajuda de suas propriedades adicionais (singularidade, propriedade, liquidez). Isso permite que cada indivíduo se vincule a um evento específico.

Ingresso NFT (do inglês, *NFT Ticketing*), são ativos digitais que mantêm suas credenciais de acesso a um evento. Eles também podem ser usados para criar uma experiência mais imersiva aos fãs, ao oferecer vantagens extras, tais como reuniões, mercadorias exclusivas, universo expandido e muito mais. Graças à codificação que é feita sobre uma rede *blockchain*, as opções ficam limitadas apenas pela criatividade do desenvolvedor e da proposta do evento em particular. Um grande exemplo de uso no escopo desta modalidade foi a *Binance* ter oferecido aos participantes do Primavera Sound 2022 NFTs POAPs (*Proof of Attendance Protocols*) exclusivos, com a intenção de tornar a experiência no festival ainda mais rica e personalizada. Os portadores de ingressos foram convidados a fazer o download do aplicativo da *Binance* para solicitar seu NFT POAP, que poderia ser usado para desbloquear experiências únicas em seu estande [Binance Academy 2021]. As vantagens do ingresso NFT se estendem a:

1. Um bilhete baseado em NFT é único e sua escassez é garantida mediante as propriedades já mencionadas dos NFT na fundamentação deste trabalho.
2. Credibilidade na compra, mediada pelos contratos inteligentes, aumenta a confiança por parte do comprador que obtém a certeza de que não vai ser vítima de fraude, pois seu ingresso também não pode ser falsificado ou duplicado.
3. A posse e os direitos do ingresso ficam a cargo do dono, dando a ele poder sobre o mesmo, desta forma se assim ele quiser, ele pode revender, leiloar ou dar o bilhete sem infringir nenhuma política.

Para futuros profissionais dos cursos de tecnologia da informação que desejem trabalhar diretamente dentro do âmbito do desenvolvimento um pré requisito é o domínio em programação orientada a objetos (POO) e programação estruturada. Um dos pilares da POO que é extremamente importante nesse tipo de modalidade é a abstração. Como aqui lida com uma representação de um objeto real (ingresso), tem-se que imaginar o que esse objeto irá realizar dentro do sistema. O paradigma da POO é um modelo de análise, projeto e programação baseado na aproximação entre o mundo real e o mundo virtual. O processo de desenvolvimento vai ser realizado em uma rede *blockchain*. Um exemplo de plataforma que pode ser usada para este tipo de projeto é a EVM (*Ethereum virtual machine 2.2.3*), a

qual oferece a liberdade para os programadores utilizarem várias linguagens de programação como C, java e python. O domínio sobre o processo de cunhagem também é um pré-requisito de extrema importância devido ao processo de *tokenização* dos ingressos.

### 5.1.2 Chaves/controlado de acesso

Dando ênfase a uma modalidade de sistemas de TI, é possível citar o próprio processo de autenticação. Os sistemas de TI comumente implementam regras para controle de acesso aos recursos, de modo que avalia os direitos de acesso de um usuário com base em uma política.

O uso de *tokens* na criação de chaves de acesso já é uma prática comum, representando o direito de acesso aos recursos. Os NFTs podem executar este papel com maior segurança. Por exemplo, o OAuth2.0, que é um padrão popular para autenticação, é um protocolo de autorização de padrão aberto que permite a terceiros acessarem dados de um usuário sem a obrigatoriedade de informar suas credenciais. Nesse padrão, utiliza-se de um *token* de acesso [Blockchain e team 2021].

Devido à escassez programável, o desenvolvedor ou administrador pode determinar a escassez exata de um NFT. Isso pode ser utilizado para transformar chaves de acesso em NFT com a finalidade de abrir portas físicas do mundo real, já que é possível criar múltiplas chaves para uma determinada porta, com cada chave tornando-se um NFT [Blockchain e team 2021].

Devido à característica de ser programável, cada NFT pode ter seus atributos únicos permitindo assim a criação de uma hierarquia de acesso, cada chave com poder de acesso diferente, funções externas únicas e etc. O acesso será garantido através das políticas dos contratos inteligentes. Um profissional que apresente um sistema de controle de chaves baseado em NFT para uma empresa, possuirá um diferencial no mercado, já que o mesmo estará ofertando um produto novo, mais seguro e moderno.

### 5.1.3 DApps

A criação de aplicativos sempre foi um mercado promissor. Os DApps são uma extensão desse mercado. Dentro da plataforma *ethereum*, considerada a plataforma mais utilizada na construção de DApps, é possível achar sua definição: um aplicativo descentralizado (DApp) é aquele construído em uma rede descentralizada que combina um contrato inteligente e uma interface de usuário *front-end*. Um DApp tem seu código interno executado em uma *blockchain*, podendo ser desenvolvido em qualquer linguagem de programação. Suas principais características e diferenças de aplicativos normais são:

1. Descentralizado - DApps operam sobre uma rede *blockchain*;
2. Determinístico - DApps desempenham a mesma função, independentemente do ambiente em que são executados

3. Turing completo - DApps podem executar qualquer ação dados os recursos necessários.
4. Isolados - DApps são executados em um ambiente virtual (e.g., EVM) de modo que se o contrato inteligente for construído com uma falha humana, ele não afetará o funcionamento da rede *blockchain*, sobre a qual ele está executando.

Não é do escopo deste trabalho explicar como desenvolver ou todas as características de um DApp, mas apenas informar que esse mercado é promissor. Todos os jogos e aplicativos de sucesso exemplificados ao longo desta monografia são DApps. As carteiras digitais, que seguram as criptomoedas, assim como os NFTs também são exemplos de DApps. Uma sugestão para qualquer profissional que tenha interesse em desenvolver um DApp é conhecer a plataforma da *ethereum*, a qual disponibiliza artigos completos e códigos armazenados no Github com o objetivo de ensinar a desenvolver esses tipos de aplicativos [Ethereum 2021].

## Jogos

NFT tem um grande potencial na indústria de jogos. Também é fato que os jogos NFT são exemplos de DApps. No mercado existem alguns exemplos de grandes sucessos como *CryptoKitties*, *mir4*, *Ni no kuni*, *CryptoPunks*, *Meebits*, *Axie Infinity* e muitos outros. *GameFi* é como este mercado ficou conhecido. A grande diferença de um jogo NFT para um jogo tradicional é que tudo dentro do universo do jogo pode ser cunhado como um NFT permitindo que os jogadores transfiram itens do jogo para fora do mundo virtual. Isso permite que os jogadores negociem seus itens no *marketplace*, trocando-os por criptomoedas, comumente *altcons* desenvolvidas pela empresa do jogo, que podem ser negociadas em corretoras de criptomoedas como é o exemplo da *BinanceNFT*.

Nesta modalidade se destacam duas oportunidades. A primeira é o desenvolvimento de jogos. Para poder desenvolver um jogo NFT, vai ser preciso executá-lo em uma rede descentralizada, e também será necessário que o desenvolvedor possua uma quantidade de *bitcoins*, que pode ser particionada e transformada em uma *altcoin* que funciona como incentivo aos jogadores. Um ponto a se destacar é que os jogos NFT geram os chamados *play-to-earn*, desta tendência, os jogadores recebem recompensas, como *tokens* e, ocasionalmente, seus personagens itens de jogo e etc, variando da mecânica e política do jogo pode virar um NFT. Quanto mais eles jogam, mais eles ganham (modalidade chamada de *farming*). Geralmente, os *tokens* ganhos são necessários como parte de algum processo de criação ou mecânica específica do jogo.

Explicação resumida do que seria o processo de *farming*, nesse processo o usuário abre uma conta para jogar e ganhar uma moeda virtual que nesse exemplo vai ser chamada de "werlancoin", esta moeda pode ser exportada e guardada em uma carteira virtual disponibilizada pela empresa do jogo, uma vez que esta operação é completa, a moeda dentro do jogo é zerada, evitando assim o problema do duplo-gasto, com a moeda dentro da carteira o usuário pode trocar essa "werlancoin" por uma *altcoin* patrocinada pela empresa, vamos

chamar essa moeda de “empresacoin”. O valor da “empresacoin” depende exclusivamente da popularidade do jogo, porque quem vai comprar essa moeda são outras pessoas que querem jogar ou investir no jogo, e usuários que precisam desta moeda para comprar itens ou melhorias dentro do jogo (processo chamado de queima). A “empresacoin” agora pode ser negociada, o usuário vai vender essa moeda em troca da moeda de governança da carteira, uma moeda popular hoje entre jogos NFT é a *wemix*, uma vez feita a venda o jogador vai precisar exportar o *wemix* para uma *exchange*. A partir da *exchange* o jogador pode fazer um saque por pix ou pode entrar no mercado de *trading*.

A segunda oportunidade que apresento é devido o *farming*, esta modalidade é extremamente custosa, porque ele se assemelha muito com o processo de mineração por prova de trabalho, utilizado pelo *bitcons*, isso porque é comum usuários de jogos NFT, criarem múltiplas contas, de um jogo e executa-las em múltiplos processos, demandando grande poder computacional, levando ao se utilizar de diversas máquinas como é feito em poços de mineração. A virtualização em VMs é uma opção mais barata, tanto do ponto de vista do consumo de energia como economia de poder computacional. Além que é possível construir VMs personalizadas para jogos e sistemas específicos que podem ser negociadas para usuários de *farming*. Uma pratica bastante lucrativa principalmente para profissionais recém-formados que ainda não entraram no mercado de trabalho ou estudantes de tecnologia que ainda estão em processo de formação.

O processo de virtualização pode ser realizado em ferramentas gratuitas como o *virtual box*<sup>4</sup>, as ferramentas específicas a serem instaladas vai depender das especificações particulares de cada jogo, das carteiras virtuais que vão ser utilizadas, e das limitações de rede exigidas pela empresa do jogo isso vai demandar um grande conhecimento em Administração de Sistemas e Administração de Serviços, também vai exigir conhecimento do mercado *GameFi*, já que a venda das VMs vai ser realizada com suporte das mídias e canais de comunicações de relevâncias ao público consumidor de deste mercado. Essas mídias normalmente estão divididas em servidores no discord<sup>5</sup> ou em fóruns disponibilizados pelo site na empresa responsável pela distribuição do jogo.

#### 5.1.4 Mineração de dados

A última grande oportunidade que este trabalho vai destacar é a mineração de dados. Mineração de dados é o processo de encontrar anomalias, padrões e correlações em grandes conjuntos de dados para prever resultados. O mercado NFT possui uma gigante concorrência, com novas *altcoin's* surgindo todos os dias. Assim, usar modelos analíticos para dar sentido aos dados de mercado, e prever seus comportamentos é altamente relevante, tanto para empresas quanto para entusiastas do mercado, principalmente para os que atuam no mercado de *trading*.

---

<sup>4</sup><https://www.oracle.com/br/virtualization/virtualbox/>

<sup>5</sup>Discord é um aplicativo de voz sobre IP proprietário e gratuito, projetado inicialmente para comunidades de jogos.

Existem empresas hoje que foram fundadas nesta premissa, minerar dados a respeito de cripto ativos no geral e democratizar o acesso a estes. Além de fornecer relatórios gráficos a respeito da capitalização das criptomoedas entre outras modalidades, cito como exemplo aqui a *coinbase*<sup>6</sup>, *coingecko*<sup>7</sup> e *marketwatch*<sup>8</sup>. Um minerador de dados também pode utilizar os NFT para gerar *royalties* sobre todo e qualquer conjunto de dados criado pelo mesmo. Um minerador de dados que saiba como cunhar um ativo, por exemplo, após um processo de mineração a respeito das “werlancoins”, ele pode cunhar os resultados da sua pesquisa e promover os dados para empresas ou pessoas através de plataformas do *marketplace*, de modo que sempre que sua pesquisa for utilizada ele vai capitalizar sobre a mesma, da mesma forma que um músico é capitalizado quando sua música é ouvida no *Spotify*.

---

<sup>6</sup><https://www.coinbase.com/pt>

<sup>7</sup><https://www.coingecko.com/pt>

<sup>8</sup><https://www.marketwatch.com/>

## Capítulo 6

# Considerações Finais e Sugestões para Trabalhos Futuros

Muitas oportunidades surgem com o advento do NFT, seu simples conceito abre diversas portas de aplicação, limitados apenas pela criatividade do desenvolvedor, alguns projetos utilizando NFT, demonstram bastante potencial, mesmo assim muitos estudantes não conhecem esse potencial, e limitam bastante a ideia do que seria um NFT, a principal proposta deste trabalho, foi trabalhar sobre essa hipótese, para isso foi construído um questionário com o auxílio do *google forms* e enviado para estudantes de 3 cursos (Telemática, Engenharia de Computação e Manutenção Suporte e Informática) matriculados no *IFPB* campus de campina grande. Com base nas respostas deste questionário foram feitas uma análise que serviram como métrica para escolha de oportunidades de atuação no mercado que utilizam a tecnologia NFT. Para chegar nessas conclusões, foi realizado uma intensa revisão bibliográfica a respeito da tecnologia.

Há muitas evidências de que o NFT é uma tecnologia promissora. Suas características, combinada com a criatividade de um profissional de tecnologia, podem abrir portas no mercado de trabalho. É fundamental apontar que o que faz o NFT ganhar destaque na mídia ou até mesmo a atenção de grandes investidores, é sua aplicação no mercado DeFi. Transformar itens colecionáveis, criar *altcoin*, e capitalizar no *marketplace*, são opções que vão além dos profissionais de tecnologia. NFT tem sido muito usado no mercado de arte, e neste ano (2022) está sendo explorado principalmente no mercado de jogos. O mercado de jogos que se torna um meio de entrada gratuita e bastante tentadora para estudantes, ou profissionais recém-formados que ainda não tiveram oportunidade de atuar diretamente no mercado de trabalho. Modalidade que tomou bastante força durante o rígido período da pandemia. Essa tecnologia torna possível os conceitos da Web3 que é descentralização e dar maior controle aos usuários, existem muitos projetos em desenvolvimento e muitos que ainda estão por vir. O NFT já faz parte do nosso presente, e muito vai compor o futuro, criatividade e inovação são as ferramentas que movem as engrenagens do desenvolvimento.

## 6.1 Sugestões para Trabalhos Futuros

Pelo escopo do trabalho e limite de tempo estipulado para seu desenvolvimento não foi possível denotar todas as possíveis aplicações do NFT. Diante do exposto, seguem algumas sugestões de temas de trabalho.

1. Estender o trabalho. Levar o questionário para outros cursos de tecnologias de outras instituições, afim de aumentar a margem de dados a serem analisadas, e verificar se a hipótese levantada também é verdadeira fora no "universo" do IFPB. Explorar mais mercados e mais aplicações para a tecnologia NFT, seria possível também pensar em introduzir entrevistas a criadores, ou investidores desse mercado, como ponto de construir uma base mais forte ou até mesmo tutoriais atualizados sobre a aplicação no mercado.
2. Chaves/controlado de acesso. O controle de acesso está em constante evolução. Mas na mesma velocidade que a segurança aumenta, as formas de burlar esses controles crescem, fazendo com que grandes empresas constantemente procurem novas formas de aprimorar seu controle de acesso. Um projeto que tenha como foco desenvolver uma chave de controle de acesso junto à tecnologia NFT pode ser bastante promissor e rentável.
3. O que pode se tornar um NFT? Para muitos esta pergunta parece óbvia, "um ativo digital", mas, no momento que diz que é possível cunhar um item real em forma de NFT, sua resposta começa a se tornar cada vez mais complicada. Um trabalho que se dedique a explorar ao máximo este conceito, testar, e investigar o que pode não ou não se tornar um NFT, ao ponto de criar um definição clara e objetiva, poderia ter tanto valor acadêmico quanto comercial, já que daria suporte a novas ideias e áreas de aplicação.

# Referências Bibliográficas

[1] 1. *Bombcrypto?* Disponível em: Larva Labs <<https://bombcrypto.io/>>, Acesso em: 20 de maio de 2022. 21

[10] 10. *cryptokitties*. Disponível em: <<https://www.cryptokitties.co/>>. Acesso em: 010 de maio de 2022. 20

[2] 2. *mir4global?* Disponível em: Larva Labs <<https://www.mir4global.com/?lang=pt>>, Acesso em: 20 de maio de 2022. 21

[3] 3. *axieinfinity*. Disponível em: Larva Labs <<https://axieinfinity.com/>>, Acesso em: 20 de maio de 2022. 21

[3] 3. *Um Guia de Cripto Colecionáveis e Tokens Não Fungíveis(NFTs)*. Disponível em: <<https://academy.binance.com/pt/articles/a-guide-to-crypto-collectibles-and-non-fungible-tokens-nfts#header-4>>. Acesso em: 09 de maio de 2022. 26

[4] 4. *CryptoPunks*. Disponível em: Larva Labs <<https://www.larvalabs.com/cryptopunks>>, Acesso em: 20 de maio de 2022. 20

[Academy 2021] ACADEMY, B. *What Are Smart Contracts*. 2021. Disponível em: <<https://academy.binance.com/en/articles/what-are-smart-contracts>> May 11, 2022, Acesso em: 20 de maio de 2022. 22, 23

[Binance Academy 2020] Binance Academy. *A Guide to Collectible Crypto and Non-Fungible Tokens (NFTs) — Binance Academy, Binance Articles*. 2020. <<https://academy.binance.com/pt/articles/a-guide-to-crypto-collectibles-and-non-fungible-tokens-nfts#header-4>>. [Online; accessed 9-August-2022]. 2

[Binance Academy 2021] Binance Academy. *What Are NFT Games and How Do They Work?* 2021. Disponível em: Larva Labs <<https://academy.binance.com/en/articles/what-are-nft-games-and-how-do-they-work>>, Acesso em: 20 de maio de 2022. 21

[Binance Academy 2021] Binance Academy. *What Are NFT Games and How Do They Work? — Binance Academy, Binance Articles*. 2021. <<https://academy.binance.me/en/articles/what-are-nft-games-and-how-do-they-work>>. [Online; accessed 9-August-2022]. 2, 9, 19, 21, 41

[BitFury Group 2015] BitFury Group. *Proof of Stake versus Proof of Work*. 2015. <<https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf>>. [Online; accessed 19-maio-2022]. 10

- [Blockchain e team 2021] BLOCKCHAIN, O. E.; TEAM, F. Demystifying non-fungible tokens (nfts). By The European Union Blockchain Observatory Forum, 2021. 1, 19, 20, 21, 22, 28, 42
- [Bruno Cardoso 2018] Bruno Cardoso. *Contratos inteligentes: descubra o que são e como funcionam*. 2018. Disponível em: <<https://brunonc.jusbrasil.com.br/artigos/569694569/contratos-inteligentes-descubra-o-que-sao-e-como-funcionam>> Acesso em: 16 de maio de 2022. xi, 15, 16, 17
- [Business blockchain hq 2022] Business blockchain hq. *Blockchain Explained*. 2022. <<https://businessblockchainhq.com/blockchain-explained/>>. [Online; accessed 17-maio-2022]. 10
- [Buterin 2018] BUTERIN, V. Ethereum: a next-generation cryptocurrency and decentralized application platform. 2014. URL: <https://bitcoinmagazine.com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/>[accessed 2019-01-10][WebCite Cache ID 75JdRivrX], 2018. 17
- [Coingecko 2022] Coingecko. *Top NFT Coins by Market Cap*. 2022. <<https://www.coingecko.com/en/categories/non-fungible-tokens-nft>>. [Online; accessed 9-August-2022]. xi, 1, 30
- [Coinmarketcap 2009] Coinmarketcap. *Dogecoin*. 2009. <<https://coinmarketcap.com/pt-br/currencies/dogecoin/>>. [Online; accessed 05-maio-2022]. 14
- [Coinmarketcap 2009] Coinmarketcap. *Litecoin*. 2009. <<https://www.bitcointrade.com.br/criptomoedas/litecoin/>>. [Online; accessed 05-maio-2022]. 14
- [Coinmarketcap 2009] Coinmarketcap. *Namecoin*. 2009. <<https://coinmarketcap.com/pt-br/currencies/namecoin/>>. [Online; accessed 05-maio-2022]. 14
- [Dash 2021] DASH, A. *NFTs Weren't Supposed to End Like This*. 2021. Disponível em: <<https://www.theatlantic.com/ideas/archive/2021/04/nfts-werent-supposed-end-like/618488/>> Acesso em: 16 de maio de 2022. 20
- [Ethereum 2021] ETHEREUM. *Exemplo de código fonte no github*. 2021. Disponível em: <<https://github.com/scaffold-eth/scaffold-eth>> Acesso em: 14 de agosto de 2022. 43
- [Ethereum Articles 2022] Ethereum Articles. *INTRO TO ETHEREUM*. 2022. Disponível em: <<https://ethereum.org/en/developers/docs/intro-to-ethereum/>> Acesso em: 16 de maio de 2022. xi, 15, 16, 17, 18, 19
- [Ethereum Articles 2022] Ethereum Articles. *NON-FUNGIBLE TOKENS*. 2022. <<https://ethereum.org/en/nft/>>. [Online; accessed 9-August-2022]. 1, 2, 12, 22, 23
- [Fairfield 2022] FAIRFIELD, J. A. Tokenized: The law of non-fungible tokens and unique digital property. *Ind. LJ*, HeinOnline, v. 97, p. 1261, 2022. 1, 29
- [Figueiredo 2022] FIGUEIREDO, P. G. S. M. V. Non-fungible tokens: Propriedades, aplicações e novos desafios. Pontifícia Universidade Católica de Goiás, 2022. 29
- [Gil 2002] GIL, A. C. Como classificar as pesquisas. *Como elaborar projetos de pesquisa*, v. 4, n. 1, 2002. 28
- [GOUVEIA 2021] GOUVEIA, L. D. Blockchain. Universidade Federal de Campina Grande, 2021. xi, 6, 7, 29

- [Jacob Kastrenakes 2021] Jacob Kastrenakes. *Beeple sold an NFT for \$69 million.* 2021. <<https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million>>. [Online; accessed 16-maio-2022]. 19
- [Kiayias *et al.* 2017] KIAYIAS, A. *et al.* Ouroboros: A provably secure proof-of-stake blockchain protocol. In: *Annual international cryptology conference*. [S.l.: s.n.], 2017. p. 388. 11
- [Lansky 2018] LANSKY, J. Possible state approaches to cryptocurrencies. *Journal of Systems integration*, Journal of Systems Integration, v. 9, n. 1, p. 19, 2018. 12, 13
- [Maciel 2019] MACIEL, F. A. Introdução as criptomoedas: uma análise de possíveis impactos na economia, investimentos e contabilidade. 2019. 7, 29
- ["MCT"2021] "MCT", M. c. T. *WHAT IS TOKEN AND WHAT IS IT RELATIONSHIP TO CRYPTOCURRENCY?* 2021. <<https://www.clear.com.br>>. [Online; accessed 05-maio-2022]. 14, 15
- [Peck 2012] PECK, M. E. The cryptoanarchists' answer to cash. *IEEE Spectrum*, IEEE, v. 49, n. 6, p. 56, 2012. 13
- [Raquel Balarin 2022] Raquel Balarin. *Ethereum: como surgiu a segunda criptomoeda mais valiosa do mundo?* 2022. <<https://www.infomoney.com.br/guias/o-que-e-ethereum/>>. [Online; accessed 20-maio-2022]. 12, 17
- [Rebello *et al.* 2019] REBELLO, G. *et al.* Correntes de blocos: Algoritmos de consenso e implementação na plataforma hyperledger fabric. *Sociedade Brasileira de Computação*, 2019. xi, 5, 6, 7, 8, 9, 29
- [Ricarte] RICARTE, I. L. M. *Codificação*. Disponível em: <<https://www.dca.fee.unicamp.br/cursos/EA876/apostila/HTML/node8.html>>, Acesso em: 20 de maio de 2022. 23
- [stringfixer team 2021] stringfixer team. *Minting Cryptocurrency.* 2021. <[https://stringfixer.com/pt/Mining\\_\(cryptocurrency\)](https://stringfixer.com/pt/Mining_(cryptocurrency))>. [Online; accessed 12-maio-2022]. 12, 13
- [Tainá Freitas 2021] Tainá Freitas. *O que é DeFi e como funcionam as finanças descentralizadas?* 2021. <<https://www.startse.com/artigos/o-que-e-defi-decentralized-finance/>>. [Online; accessed 20-maio-2022]. 19
- [Tasca e Tessone 2017] TASCA, P.; TESSONE, C. J. Taxonomy of blockchain technologies. principles of identification and classification. *arXiv preprint*, 2017. 10, 11, 12, 28
- [Vigna 2011] VIGNA, P. *Which Digital Currency Will Be the Next Bitcoin.* [S.l.]: The Wall Street Journal, 2011. 14
- [Vogelsteller 2015] VOGELSTELLER, V. B. F. *EIP-20: Token Standard.* 2015. Disponível em: <<https://eips.ethereum.org/EIPS/eip-20>>, Acesso em: 20 de maio de 2022. 26
- [Wang *et al.* 2021] WANG, Q. *et al.* Non-fungible token (nft): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*, 2021. xi, 1, 2, 3, 23, 24, 25, 26, 27, 28
- [Wang *et al.* 2022] WANG, Q. *et al.* Exploring web3 from the view of blockchain. *arXiv preprint arXiv:2206.08821*, 2022. 39

[Web3-cbn 2021] WEB3-CBN, E. I. C. P. *Web3: Cripto, Blockchain, NFT*. 2021. Disponível em: <<https://ip-capitalpartners.com/reports/web-3/>>. Acesso em: 017 de agosto de 2022. 40

[Wikipedia contributors 2022] Wikipedia contributors. *Ecash — Wikipedia, The Free Encyclopedia*. 2022. <<https://en.wikipedia.org/w/index.php?title=Ecash&oldid=1087749319>>. [Online; accessed 11-August-2022]. 12

[Wikipédia 2022] WIKIPÉDIA. *Ethereum — Wikipédia, a enciclopédia livre*. 2022. <<https://pt.wikipedia.org/w/index.php?title=Ethereum&oldid=63490990>>. [Online; accessed 30-abril-2022]. 17

[William Entriken 2018] William ENTRIKEN, D. S. J. E. N. *EIP-721: Non-Fungible Token Standard*. 2018. <<https://eips.ethereum.org/EIPS/eip-721>>. [Online; accessed 20-maio-2022]. 19, 23, 26

[Witek Radomski 2018] Witek RADOMSKI, A. C. P. C. J. T. E. B. R. S. *EIP-1155: Non-Fungible Token Standard*. 2018. <<https://eips.ethereum.org/EIPS/eip-1155>>. [Online; accessed 20-maio-2022]. 19, 23, 26

[Witte 2016] WITTE, J. H. The blockchain: a gentle four page introduction. *arXiv preprint*, 2016. 5, 6, 9

[yan Lucas 2018] yan Lucas. *Tudo sobre Nano: A Criptomoeda Instantânea e Sem Taxas*. 2018. <<https://portaldobitcoin.uol.com.br/tudo-sobre-raiblocks/>>. [Online; accessed 05-maio-2022]. 13



## Documento Digitalizado Ostensivo (Público)

### Entrega de trabalho de conclusão de curso

**Assunto:** Entrega de trabalho de conclusão de curso  
**Assinado por:** Jose Werlandie  
**Tipo do Documento:** Tese  
**Situação:** Finalizado  
**Nível de Acesso:** Ostensivo (Público)  
**Tipo do Conferência:** Cópia Simples

Documento assinado eletronicamente por:

- José Werlandiê Aureliano Lacerda, ALUNO (201821210036) DE TECNOLOGIA EM TELEMÁTICA - CAMPINA GRANDE, em 16/09/2022 13:09:18.

Este documento foi armazenado no SUAP em 16/09/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifpb.edu.br/verificar-documento-externo/> e forneça os dados abaixo:

Código Verificador: 627010  
Código de Autenticação: cb5be0909b

