



Check for updates

1
2
3
4
5
6
7
8
9
10

NIST Internal Report NIST IR 8472 ipd

Non-Fungible Token Security

Initial Public Draft

Peter Mell
Dylan Yaga

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8472.ipd>

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**NIST Internal Report
NIST IR 8472 ipd**

Non-Fungible Token Security

Initial Public Draft

Peter Mell
Dylan Yaga
*Computer Security Division
Information Technology Laboratory*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8472.ipd>

August 2023



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

29 Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in
30 this paper in order to specify the experimental procedure adequately. Such identification does not imply
31 recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or
32 equipment identified are necessarily the best available for the purpose.

33 There may be references in this publication to other publications currently under development by NIST in
34 accordance with its assigned statutory responsibilities. The information in this publication, including concepts and
35 methodologies, may be used by federal agencies even before the completion of such companion publications. Thus,
36 until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain
37 operative. For planning and transition purposes, federal agencies may wish to closely follow the development of
38 these new publications by NIST.

39 Organizations are encouraged to review all draft publications during public comment periods and provide feedback
40 to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
41 <https://csrc.nist.gov/publications>.

42 **NIST Technical Series Policies**

43 [Copyright, Use, and Licensing Statements](#)

44 [NIST Technical Series Publication Identifier Syntax](#)

45 **Publication History**

46 Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added upon final publication]

47 **How to Cite this NIST Technical Series Publication:**

48 Mell P, Yaga D (2023) Non-Fungible Token Security. (National Institute of Standards and Technology,
49 Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8472 ipd.
50 <https://doi.org/10.6028/NIST.IR.8472.ipd>

51 **Author ORCID iDs**

52 Peter Mell: 0000-0003-2938-897X

53 Dylan Yaga: 0000-0003-4058-3645

54 **Public Comment Period**

55 August 31, 2023 – October 16, 2023

56 **Submit Comments**

57 NISTIR8472@nist.gov

58
59 National Institute of Standards and Technology
60 Attn: Computer Security Division, Information Technology Laboratory
61 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

62 **All comments are subject to release under the Freedom of Information Act (FOIA).**

63 **Abstract**

64 Non-fungible token (NFT) technology provides a mechanism to enable real assets (both virtual
65 and physical) to be sold and exchanged on a blockchain. While NFTs are most often used for
66 autographing digital assets (associating one’s name with a digital object), they utilize a strong
67 cryptographic foundation that may enable them to regularly support ownership-transferring sales
68 of digital and physical objects. For this, NFT implementations need to address potential security
69 concerns to reduce the risk to purchasers. This publication explains NFT technology and then
70 identifies and discusses a list of 27 potential security issues. All of the identified issues can be
71 addressed through use of a systematic security approach that promotes a secure design and
72 implementation.

73 **Keywords**

74 blockchain; definition; ERC-721; non-fungible token; properties; security; smart contract.

75 **Reports on Computer Systems Technology**

76 The Information Technology Laboratory (ITL) at the National Institute of Standards and
77 Technology (NIST) promotes the U.S. economy and public welfare by providing technical
78 leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test
79 methods, reference data, proof of concept implementations, and technical analyses to advance
80 the development and productive use of information technology. ITL’s responsibilities include the
81 development of management, administrative, technical, and physical standards and guidelines for
82 the cost-effective security and privacy of other than national security-related information in
83 federal information systems.

84 **Audience**

85 This publication is intended for readers who want to better understand how NFTs function at a
86 technical level and the associated potential security risks. This includes both purchasers of NFTs
87 and developers of NFT implementations.

88 **Call for Patent Claims**

89 This public review includes a call for information on essential patent claims (claims whose use
90 would be required for compliance with the guidance or requirements in this Information
91 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
92 directly stated in this ITL Publication or by reference to another publication. This call also
93 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
94 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

95 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
96 in written or electronic form, either:

97 a) assurance in the form of a general disclaimer to the effect that such party does not hold
98 and does not currently intend holding any essential patent claim(s); or

99 b) assurance that a license to such essential patent claim(s) will be made available to
100 applicants desiring to utilize the license for the purpose of complying with the guidance
101 or requirements in this ITL draft publication either:

102 i. under reasonable terms and conditions that are demonstrably free of any unfair
103 discrimination; or

104 ii. without compensation and under reasonable terms and conditions that are
105 demonstrably free of any unfair discrimination.

106 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
107 on its behalf) will include in any documents transferring ownership of patents subject to the
108 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
109 the transferee, and that the transferee will similarly include appropriate provisions in the event of
110 future transfers with the goal of binding each successor-in-interest.

111 The assurance shall also indicate that it is intended to be binding on successors-in-interest
112 regardless of whether such provisions are included in the relevant transfer documents.

113 Such statements should be addressed to: NISTIR8472@nist.gov

114	Table of Contents	
115	1. Introduction	1
116	1.1. Scope	3
117	2. Background	3
118	2.1. Blockchains	3
119	2.2. Smart Contracts.....	3
120	2.3. Tokens	4
121	3. Definition, Properties, and Security Evaluations	5
122	3.1. NFT Definition.....	5
123	3.2. NFT Properties	5
124	3.3. Security Evaluation of NFT Properties	6
125	3.3.1. Contract-Provided Properties	6
126	3.3.2. Blockchain-Provided Properties.....	10
127	3.3.3. Human Management-Provided Properties.....	12
128	4. List of Potential Security Concerns	13
129	5. Token Standards	15
130	5.1. ERC-20: Fungible Token Standard	15
131	5.2. ERC-721: Non-Fungible Token Standard	15
132	5.3. Other NFT Standards	16
133	6. Marketplaces and Exchanges	17
134	7. Conclusion	18
135	References	19
136	Appendix A. List of Symbols, Abbreviations, and Acronyms	21
137	Appendix B. Fractional Token Example	22
138		

139 1. Introduction

140 Non-fungible token (NFT) technology provides a mechanism to enable real assets (both virtual
141 and physical) to be sold and exchanged on a blockchain. It does this by creating a unique
142 blockchain token to represent each *asset*. A blockchain smart contract manages a group of tokens
143 and enables them to be securely transferred between blockchain accounts. The verification of
144 NFT ownership by an account is straightforward. This architecture provides a strong
145 cryptographic foundation for NFT sales.

146 NFTs are commonly used for photography, digital art, trading cards, and music [1]. Usually,
147 what is purchased is the right to “autograph” a digital asset with a blockchain ledger entry. In this
148 case, ownership rights are not usually conveyed to the purchaser [6], and the autographing right
149 is not necessarily exclusive. In other cases, sales of the digital tokens are intended by the seller to
150 convey a sale of ownership rights over the linked digital assets. Someday, the technology may
151 broadly support the secure record of physical asset sales (e.g., real estate or cars). NFTs can also
152 be used for more utilitarian purposes, such as voting rights, membership, or benefits [2].

153 The first NFT was published in 2014 [3]. The market remained nascent for years but then grew
154 dramatically in 2021 and peaked at \$18 billion dollars [4]. The most expensive NFT bought by a
155 single person went for \$69.3 million in 2021 [5]. The market peaked at that point and has
156 dropped significantly. For example, an NFT of the first tweet was sold in 2021 for \$2.9 million;
157 it was put up for auction in April 2023 and received the highest bid of \$280 [36].

158 The purpose of this publication is to evaluate NFT technology and identify potential security
159 concerns. This will promote the secure development of NFT implementations and raise
160 awareness as to possible security concerns. The focus is on the smart contract representation and
161 sales of NFTs and associated blockchain aspects.

162 A descriptive definition is provided to enable the reader to understand NFTs from a technical
163 perspective. An NFT is not the asset “owned” but rather a data record within a smart contract.
164 This definition is used to derive a set of properties inherent to NFTs. Each of these properties is
165 then evaluated to identify 27 potential security concerns that should be addressed by NFT
166 implementations.

167 A legal discussion and analysis of NFTs is out of scope for this paper; the focus here is on the
168 technology. However, the legal aspects are just as important as the technical ones. Art Law &
169 More says that

170 The creation, distribution, ownership and trading of NFTs are new phenomena
171 which raise a plethora of legal issues, many of which are ambiguous or
172 unresolved... [For example,] there is practically no case law, legislation or
173 regulation addressing smart contracts. This creates questions as to whether smart
174 contracts are actually legally binding. [6]

175 Another major concern is that the purchase of an NFT does not necessarily convey the copyright
176 (i.e., the purchaser cannot make, sell, or publicly display copies). Rather, the copyright often
177 remains with the original owner, making such NFTs “digital autographs” [6]. For example, the
178 previously cited \$69.3 million NFT purchase did not convey the copyright of the art to the
179 purchaser [21]. This is analogous to the physical world where the purchase of a painting or
180 baseball card rarely conveys copywrite; if it does convey then “the transfer must be express and

181 in writing” [37]. In general, the legal issues surrounding NFTs remain legally murky or
182 unresolved. This is a new area undergoing maturation and legal precedent remains to be set. A
183 discussion of the legal issues are available from [6], [2], and [37].

184 The remainder of this publication is organized as follows. Section 2 provides a short background
185 on blockchains and tokens. Section 3 provides a descriptive NFT definition, a list of NFT
186 properties, and related security considerations for each property. Section 4 is a summary of the
187 27 potential security concerns identified in Section 3.3. Section 5 reviews notable NFT
188 standards. Section 6 discusses NFT marketplaces. Section 7 is the conclusion.

189

190 **1.1. Scope**

191 The focus of this paper’s research was on the most common NFT technology used, that based on
192 the Ethereum Request for Comment 721 Non-Fungible Token Standard (ERC-721) and
193 equivalent standards on other blockchains. All non-ERC-721 based NFT systems are out of
194 scope of this paper.

195
196 An early example of a non-ERC-721 NFT are Colored Coins on the Bitcoin blockchain. These
197 encode unique information within a coin’s metadata to allow it link to some asset while making
198 it unique from all others. The metadata is encoded onto a Satoshi, which is the smallest unit of
199 transfer for Bitcoin. Such coins are then changed from being fungible (i.e., interchangeable) to
200 non-fungible (unique). Another newer example is Bitcoin Request for Comment 20 (BRC-20)
201 [34]. This encodes JSON metadata onto a Satoshi in a manner similar to Colored Coins but
202 utilizing different methods.

203
204 Security analyses of NFT marketplaces are also out of scope. The focus in this work is on the
205 NFT smart contracts and the services they provide (although this work does cover security
206 concerns with non-blockchain stored assets and asset information). Security analyses of NFT
207 marketplaces are available from [31] and [32].

208 **2. Background**

209 This section provides definitions for blockchains, smart contracts, and tokens as a foundation for
210 the discussion of NFTs in Section 3.

211 **2.1. Blockchains**

212 According to NIST IR 8202, *Blockchain Technology Overview*, blockchains are “tamper evident
213 and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central
214 repository) and usually without a central authority (i.e., a bank, company, or government)” [22].
215 NIST IR 8202 then provides a more formal definition:

216 Blockchains are distributed digital ledgers of cryptographically signed
217 transactions that are grouped into blocks. Each block is cryptographically
218 linked to the previous one (making it tamper evident) after validation and
219 undergoing a consensus decision. As new blocks are added, older blocks
220 become more difficult to modify (creating tamper resistance). New
221 blocks are replicated across copies of the ledger within the network, and
222 any conflicts are resolved automatically using established rules. [22]

223 **2.2. Smart Contracts**

224 NIST IR 8202 defines a smart contract as follows:

225 ...a collection of code and data (sometimes referred to as functions and
226 state) that is deployed using cryptographically signed transactions on the
227 blockchain network. The smart contract is executed by nodes within the
228 blockchain network; all nodes must derive the same results for the

229 execution, and the results of execution are recorded on the blockchain.
230 [22]

231 In simpler terms, a smart contract is program that runs on a blockchain. It processes transactions
232 and records state while leveraging the cryptographic security of the blockchain.

233 **2.3. Tokens**

234 In the cryptocurrency community, the term token does not have an agreed upon definition. For
235 the purposes of this publication, a token is a data record that is a digital representation of an asset
236 (physical or virtual), managed by a smart contract, and stored on a blockchain. Tokens are not
237 generally transferable between the smart contracts managing them, meaning that they are tied to
238 a particular blockchain smart contract address. Each token represents some asset (e.g.,
239 cryptocurrency, digital artwork). Smart contract tokens usually follow one or more community
240 token standards to enable interoperability with user wallets, exchanges, and other contracts (see
241 Section 5). The transference of a token from one wallet to another involves the updating of the
242 token owner's address within the managing smart contract.

243 There are two types of tokens: fungible and non-fungible. A definition of NFTs is provided in
244 Section 3. Fungible tokens are identical and interchangeable. They represent cryptocurrencies
245 that are not native to a blockchain and are instead managed by smart contracts (e.g., stablecoins).
246 In contrast, a native blockchain cryptocurrency is tied to the blockchain itself and is used to pay
247 for blockchain gas (e.g., Bitcoin and Ethereum). Smart contracts represent fungible tokens by
248 keeping a list of addresses that own tokens and how many tokens each address owns. Fungible
249 tokens are often represented in smart contracts using the Ethereum Request for Comments (ERC)
250 standard ERC-20 or a similar standard on a non-Ethereum blockchain. This is discussed in
251 Section 5.1.

252 **3. Definition, Properties, and Security Evaluations**

253 This section provides a definition for NFTs, related properties, and an evaluation of each
254 property to reveal potential security concerns.

255 **3.1. NFT Definition**

256 The definition provided below is intended to be descriptive and inclusive of all NFTs in use
257 today. It is not intended to define what is and what is not an NFT, nor is it intended to limit
258 future NFT technology. The purpose of the definition and resultant properties is to enable the
259 reader to understand current technology and to provide a foundation for an exploration of
260 potential security issues.

261 A non-fungible token (NFT) is an owned, transferable, and indivisible
262 data record that is a digital representation of a physical or virtual linked
263 asset. The data record is created and managed by a smart contract on a
264 blockchain.

265 NFTs are often represented by standard ERC-721 in smart contracts on Ethereum or a similar
266 standard on another blockchain (see Section 5 on token standards for more details). These
267 standards provide minimum functionality to be implemented by NFT implementations.
268 Additional functionality is possible, even expected. For example, NFT smart contracts may have
269 an owner role that can perform management functions (e.g., [28]). Such functionality can include
270 upgrading to a new smart contract (e.g., [29]). Such upgrades can provide the owner arbitrary
271 functionality, including the expiring or delisting of purchased NFTs (e.g., [29]).

272 **3.2. NFT Properties**

273 The following non-exhaustive set of NFT properties can be derived from this definition. Most
274 correctly functioning and secured NFT implementations will contain these properties (see
275 Section 3.3 for caveats to this).

- 276 1. **Owned:** NFTs designate ownership by recording a blockchain address.
- 277 2. **Transferable:** Owners and designated approved entities can transfer the ownership of
278 NFTs to other addresses.
- 279 3. **Indivisible:** NFTs cannot be subdivided (although the ownership may be fractionalized).
- 280 4. **Linked:** NFTs have references to the asset that they represent.
- 281 5. **Recorded:** NFTs are smart contract data records stored on a blockchain.
- 282 6. **Provenance:** NFTs have their chain of ownership recorded.
- 283 7. **Permanence:** NFTs are normally indestructible (although some are designed to be
284 burned).
- 285 8. **Immutable:** The asset that an NFT represents cannot be modified.
- 286 9. **Unique:** Each NFT represents a unique asset.

287 10. **Authentic:** Each NFT asset is what the NFT claims it to be (e.g., artwork from a
288 particular artist).

289 11. **Authorized:** Each NFT asset has been authorized by an owner to be sold as an NFT.

290 3.3. Security Evaluation of NFT Properties

291 This section evaluates potential security issues related to each property presented in Section 3.2.
292 Some of these properties should be provided by the NFT smart contract. Some are inherently
293 provided by the underlying blockchain. Some should be provided by the human management of
294 the NFT smart contract. All of these security issues are addressable through use of a systematic
295 security approach to both design and implementation (such as [35]).

296 3.3.1. Contract-Provided Properties

297 A properly constructed NFT smart contract should provide the properties of *owned*, *transferable*,
298 *indivisible*, and *linked*. These properties are described below.

299 3.3.1.1. Owned

300 An NFT is often colloquially and incorrectly referred to as the “owned” asset. For example, a
301 person may say that they own an NFT when referring to a piece of digital artwork. However,
302 from a technical point of view, the NFT is a separate entity from the artwork. What an NFT
303 owner definitively owns is a cryptocurrency token (they may or may not also own the linked
304 asset). As defined previously, a cryptocurrency token is a data record managed by a smart
305 contract and stored on a blockchain. The data record contains the metadata (i.e., a collection of
306 data values) necessary to manage the NFT ownership and to link the NFT to a referenced asset.

307 This distinction is important because ownership of the token does not necessarily legally indicate
308 ownership of the related asset (e.g., digital artwork). This is because a smart contract does not
309 necessarily have the legal authority to designate ownership of a referenced asset (technically,
310 anyone can create an NFT linked to anything). Exploring this legal issue is out of scope for this
311 work. However, seller of NFTs should clearly convey the rights provided to purchasers and
312 buyers should understand the stated rights prior to purchase.

313 It is tempting to think of these tokens like physical bills that can be handed from one person to
314 another to change ownership. However, NFTs are maintained with the associated smart contract.
315 This is because the tokens are data records of the smart contract that must stay with the smart
316 contract and are, thus, normally locked into a specific smart contract and blockchain. The
317 owner’s cryptocurrency wallets then record the smart contract address and a token identifier
318 (they don’t hold the token as a physical wallet holds a bill). It is the smart contract that manages
319 the tokens and is the authoritative repository for those tokens.

320 Smart contracts represent NFT ownership by keeping a list of unique tokens (i.e., data records)
321 along with the owner of each token. The owner is identified only by a blockchain. The data fields
322 typically recorded for a non-NFT purchase are not present. There is no name, physical address,
323 phone number, or other identifying data. This keeps the owners pseudonymous (identified only

324 by their blockchain address). This is done for privacy concerns because all data stored by the
325 smart contract is public on the blockchain.

326 If a blockchain account is compromised, then a malicious actor could obtain ownership rights for
327 all NFTs owned by that account. This could happen, for example, through a blockchain wallet
328 being hacked or through a blockchain account private key being stolen. The actor can then
329 submit blockchain transactions to the NFT smart contract to transfer all of the blockchain
330 account's NFTs to an account that they own (i.e., stealing the NFTs). They would likely then
331 quickly sell the NFTs to avoid the (unlikely) possibility that the initial owner could convince the
332 smart contract manager to reverse the transactions that stole the NFTs.

333 **3.3.1.2. Transferable**

334 The NFT smart contract provides functions to enable the transfer of tokens between owners. As
335 previously discussed, the transfer of a token is simply an update to the ownership field in the
336 token's smart contract data record. The owner is allowed to transfer a token to another
337 blockchain address by submitting a blockchain transaction. Typically, the owner is also allowed
338 to approve another address to take possession of the token as well as approve one or more
339 accounts to manage tokens on the owner's behalf. See Section 5.2 for more details.

340 The smart contract may or may not be designed to allow the contract manager to transfer tokens.
341 If the manager can transfer tokens, then stolen tokens could be restored. However, this becomes
342 challenging if stolen tokens are quickly sold because there would then exist two owners who had
343 spent funds and been granted NFT ownership by the smart contract. It could also be challenging
344 for an owner to prove to the manager that their tokens were stolen, for example when an attacker
345 steals a purchaser's private key and executes an otherwise valid transaction to change ownership
346 of the NFT.

347 The default for smart contract NFTs following widely adopted standards is for the manager to
348 not be able to transfer tokens. This makes the restoration of stolen tokens impossible, but it also
349 provides owners with assurance that the manager will not confiscate their tokens (either
350 maliciously or because of a legal order). However, NFT smart contracts likely have a mechanism
351 to allow managers to update the code of the smart contract to provide for maintenance and
352 upgrading of the NFT management infrastructure. The updated code could provide managers
353 new privileges (including token transfer abilities) over both existing and to-be-created tokens.

354 If the smart contract contains coding errors, there may be a vulnerability that enables an attacker
355 to steal tokens. An evaluation of possible vulnerabilities in NFT contracts is available from [30].
356 The attacker would then likely sell the tokens quickly to obtain cryptocurrency because after
357 launching the attack, their approach would be publicly visible on the blockchain. Others could
358 then launch the same attack, or the contract manager could use the same vulnerability to restore
359 tokens to their owners. If the contract manager can regain control of the smart contract, tokens
360 could be restored. However, the attacker would still have the funds obtained through illegal
361 token sales and the sold tokens would each have two owners (the original owners to whom the
362 tokens are restored and the subsequent purchasers that unwittingly bought the stolen tokens).

363 **3.3.1.3. Indivisible**

364 NFTs have the property that they are indivisible. This distinguishes them from fungible tokens
365 that are divisible. An example of a divisible token would be a stable coin worth \$1. This fungible
366 token could be divided into two tokens, each worth \$0.50. Since these assets are represented
367 using numbers, it is simple to divide them.

368 However, an NFT that represents a piece of digital artwork could not be divided in the same
369 manner. Digital assets are typically non-fungible, meaning that they cannot be simply cut in two
370 without damaging the original asset.

371 On a more technical level, an NFT is a token (explained in Section 2.3). A token is represented
372 in a smart contract by a data record. Indivisibility then refers to the inability to divide the NFT
373 data record into multiple parts. Data records do not naturally divide; they represent values for a
374 fixed set of variables.

375 Some NFT owners may wish to divide their NFT by providing fractionalized ownership. The
376 actual NFT itself is not split into multiple parts but instead locked into a new fractional NFT
377 smart contract that then creates a specified number of new fungible tokens. These new fungible
378 tokens represent shares of ownership of the NFT and can be traded, purchased, and sold on
379 marketplaces (see Section 6) that specialize in fractional NFT sales (such as [7]). The largest
380 fractional NFT sale to date – “The Merge” digital art – was bought jointly by 28,000 purchasers
381 for \$91.8 million [5].

382 Typically, a fractional NFT smart contract has a function that allows a buyout that can reverse
383 the fractionalization process. This enables the original owner or a fractional investor to reclaim
384 all of the ERC-20 fractional tokens and unlock the ERC-721 NFT from the fractional
385 management smart contract. Unlocking the NFT means transferring ownership away from the
386 fractional smart contract to the new owner.

387 One method of a buyout function is an auction. It requires a buyer to transfer a set amount of a
388 specific ERC-20 fractional token to the smart contract. This then begins a time-limited auction in
389 which all fractionalized owners can bid to keep their fractional shares. If the buyer wins, all
390 ERC-20 tokens are returned to the smart contract, and the buyer becomes the sole owner of the
391 NFT. If the other users outbid the buyer and win the auction, then the buyout was unsuccessful,
392 and the NFT remains fractionalized. If the NFT is successfully bought out, the fractionalized
393 owners are compensated proportionally to the number of fractions that they held. If the buyout is
394 unsuccessful, then the buyer is compensated with the amount that the remainder of fractionalized
395 owners bid, and the fractionalized owners are proportionally compensated with the ERC-20
396 fractional tokens that the buyer originally transferred to initiate the buyout.

397 Other buyout systems may be utilized instead of an auction system, such as an immediate
398 purchase at a specified exit price.

399 Appendix C provides an example of fractionalizing an NFT and then someone buying it back at
400 an auction.

401 **3.3.1.4. Linked**

402 Every NFT must be linked to the asset that it represents. More specifically, each NFT data record
403 must have a field or fields that uniquely identify and link to an asset. This collection of

404 information is referred to as the NFT's metadata. The metadata may contain additional
405 descriptive information that is not necessary for identification. An example of such data would
406 be the secure hash of a digital image along with the image's title, creation date, artist name, and a
407 public URL. Metadata can be included in the NFT data record but is often stored publicly and
408 only a link to the metadata is stored on the blockchain. There are multiple approaches to link an
409 NFT to an associated asset using metadata [8].

410 The metadata can store the asset itself on the blockchain, inside the smart contract. This
411 approach is the most secure as it leverages the integrity of the blockchain itself, but it can be
412 expensive to store data there. This is rarely done for NFTs.

413 The more common approach is to store on the blockchain a URL or content identifier to an
414 external data source that hosts the digital asset. Non-blockchain public data publishing is much
415 cheaper. Sometimes the identifier will link directly to an asset. This link is usually not to a
416 particular server, but instead to a file storage service. These storage services can be centralized
417 (but internally distributed with redundancy) or fully decentralized (e.g., with the InterPlanetary
418 File System (IPFS) protocol [9]). Either way, the off blockchain linkage complicates security as
419 an additional attack surface is added to the NFT architecture.

420 Further complicating the architecture, the linking information is usually not to the asset itself but
421 instead to a publicly accessible JSON table of NFT identifiers that provides the URLs for each
422 asset and other metadata [33]. This double linking architecture allows for the asset URLs to be
423 updated by the manager of the table (e.g., NFT marketplace). Note how the owner of the table
424 maintains continued control over where each NFT is linked.

425 It is critical that the metadata correctly identifies and links to the asset represented by the NFT. A
426 delinked NFT is unlikely to maintain its value. An NFT might be delinked if the original
427 metadata is incorrect, never being linked to any actual asset. NFTs can also be delinked if the
428 public table maintaining the asset URLs fails, is deleted, or is changed. Even for NFT data
429 records with direct URLs to their asset, the server could cease to exist or fails in some way (e.g.,
430 corrupted files). One study, with a sample size of 12 353 NFTs, found that 25 % of NFTs were
431 linked to assets that were either lost or inaccessible [33].

432 If an attacker breaks into the public table mapping NFT identifiers to URLs, the NFT could be
433 delinked, or the links and associated metadata could be changed. This could enable an attacker to
434 swap a cheap NFT asset that they bought for someone else's very expensive one by swapping
435 URLs in the public link table. This could also enable the owner of the table to delink NFT
436 owners from the assets that they purchased. There would be no need to change anything on the
437 blockchain or to access the smart contract. The owner could simply modify the metadata to
438 delink an NFT from its associated asset. Someone who purchased an expensive NFT could be
439 left owning a worthless delinked token on the NFT smart contract.

440 NFTs for physical objects, often referred to as *physical NFTs*, link to their associated physical
441 asset by including a unique identifier in their metadata. This unique identifier is then materially
442 attached to the physical object [26]. This could be accomplished through the use of a near field
443 communication (NFC) tag, QR code, or simply permanently embedding the identifier in the
444 physical asset. For significant assets (e.g., real estate), a linkage would need to be made to the
445 public records to prevent fraud. This is a nascent area around which legal precedents have not
446 been established [26].

447 **3.3.2. Blockchain-Provided Properties**

448 The associated underlying blockchain should provide the properties of *recorded*, *provenance*,
449 *permanence*, and *immutable*. These properties are described below.

450 **3.3.2.1. Recorded**

451 An NFT is a cryptocurrency token. Tokens are data records managed by a smart contract. Smart
452 contract state is *recorded* on a blockchain. This property of NFT state being recorded on a
453 blockchain grants the smart contract and associated NFT the benefits of leveraging a blockchain
454 architecture. These benefits include the properties of *provenance*, *permanence*, and *immutable*
455 (discussed in the following subsections).

456 The recording of an NFT on a blockchain normally it makes information about the NFT and its
457 ownership (the metadata) public information. Owner accounts are pseudonymous, meaning that
458 the owners are anonymous but information about their accounts (i.e., which NFTs they own) is
459 public. Accounts may be de-anonymized when an account owner provides personal information
460 (e.g., name and address) when making a purchase using cryptocurrency. This can be mitigated by
461 cryptocurrency users maintaining multiple accounts (separating NFT purchases from other
462 purchases).

463 **3.3.2.2. Provenance**

464 A fundamental property of a blockchain is its ability to track tokens over their entire lifetime.
465 The creation event, every transaction involving it, and the destruction event are all recorded. The
466 blockchain records when these events occurred, as well as the sender and receiver of the
467 transactions. The blockchain provides a complete history of ownership of the token.

468 This complete history of ownership is beneficial to anyone who wishes to validate the
469 authenticity of a token. It is a simple endeavor to work back from any point of a token's
470 transaction history and determine its origin and where it has been. The ability to validate a
471 token's history can help a user determine whether a token is fraudulent or legitimate.

472 A blockchain could undergo an attack (e.g., 51% attack [25]) that enables a malicious entity to
473 change the blockchain history, but this is unlikely for established and widely used blockchains
474 due to the significant resources dedicated to maintenance of those chains (e.g., either mining
475 processing power or large staked holdings).

476 **3.3.2.3. Permanence**

477 A fundamental property of a blockchain is its ability to record data in a near-permanent manner
478 based on its decentralized storage and cryptographic mechanisms. Other than the previously
479 referenced 51% attack [25], there are some exceptions to a blockchain's permanence.

480 One way to sidestep the property of permanence is to "burn" the NFT. Transferring an NFT to an
481 address that no one can access renders any further use of the NFT impossible. For example,
482 sending any transaction to the Ethereum address
483 "0x00" will effectively destroy whatever is sent
484 because there is no known private key that resolves to this address (and it is extremely unlikely

485 for someone to find it) so no one can access the account. Other blockchains have specific
486 addresses that the underlying blockchain code will prevent from sending transactions but can still
487 receive transactions. These are hard coded burn addresses, so even if someone were to discover a
488 private key that would resolve to that address, they could not claim any asset associated with it.

489 There may be legitimate use cases for burning an NFT, such as to provide proof of burning to
490 receive an upgraded NFT in a different smart contract or if the NFT is a consumable object in a
491 blockchain-based video game (i.e., a unique item that provides some benefit for the player). Even
492 though the NFT is burned, it still technically exists in the smart contract on the blockchain.

493 Another way to sidestep the property of permanence would be for the NFT's smart contract to
494 have the ability to call a method `selfdestruct()`. In practice, this method is used by many smart
495 contracts to stop its execution and remove the current state from the blockchain (previous states
496 are still recorded in past blocks). While there is nothing to technically prevent an NFT smart
497 contract from using the `selfdestruct()` or similar method, it is strongly discouraged. The NFT
498 smart contract manages the tokens and records all information about them, including ownership.
499 If a NFT smart contract could call a `selfdestruct()` method, then all of its associated information
500 would be removed from the blockchain's current state and become effectively lost. Since all of
501 the NFT information is contained within the smart contract, a user wallet does not reflect that it
502 owned an NFT but simply that it sent funds to an address. Potential buyers of an NFT are
503 strongly encouraged to limit their investment risk by ensuring that the smart contract will provide
504 permanence through either direct inspection or trusting the services of another firm that evaluates
505 smart contracts.

506 Another issue with permanence is if the NFT content is too large to be stored within the smart
507 contract, and the smart contract instead contains a pointer (e.g., uniform resource locator (URL)
508 or URI) to an external storage source (e.g., IPFS or some other external data). If the data source
509 should cease to host the NFT itself, then the owner may lose access to the actual NFT content.
510 This is related to the material covered by the linkage property in Section 3.3.1.5.

511 **3.3.2.4. Immutable**

512 An NFT is expected to have the property of being unchanging or immutable. NFT smart
513 contracts enforce this in their code. However, a vulnerability in the smart contract could enable a
514 malicious entity to change NFT data records.

515 More fundamentally, this is a property provided by the blockchain to ensure that ledger entries
516 are not altered. This normally holds but is not guaranteed. True immutability – to never be
517 changed under any circumstances ever – is not achieved. While blockchains are effectively
518 immutable, there have been cases in which a blockchain has been altered by group consensus
519 (e.g., [27]). True immutability of digital data is very difficult if not impossible to achieve. Under
520 normal operating conditions, a blockchain provides a cryptographically secure ledger that resists
521 alterations of recorded data (a tamper-resistant design), and a participant can detect and discard
522 alterations (a tamper-evident design) if desired. This may lead to a chain split (or cryptocurrency
523 fork) where a portion of the users accept the alterations, while another portion does not, leading
524 to incompatible blockchain records between them. By combining tamper-resistant and tamper-
525 evident designs, a blockchain can provide a near immutable ledger.

526 **3.3.3. Human Management-Provided Properties**

527 The human management of the NFT smart contract should provide the properties of *unique*,
528 *authentic*, and *authorized*. These properties are described below.

529 **3.3.3.1. Unique**

530 The non-fungible aspect of an NFT requires that only one exists. From a technical perspective,
531 this is guaranteed because the NFT smart contract ensures that the data record owned by the
532 purchaser is one-of-a-kind and has a single owner. However, that does not mean that the linked
533 asset is uniquely owned by that data record. The issuer may sell multiple NFTs linked to the
534 same asset (e.g., for digital trading cards). This may be analogous to an artist making a limited
535 run of identical copies of a specific piece of art.

536 Alternatively, there may be multiple smart contracts with data records linked to that asset. The
537 same virtual object could be sold on multiple NFT marketplaces. To check for this, one could
538 compare the hash values of the virtual object with other virtual objects being sold. However, one
539 could change just a single pixel of a virtual image to obtain a completely different hash value. An
540 artist could also have made many copies of the same artwork, or duplicates of original art are
541 being sold in NFT form.

542 **3.3.3.2. Authentic**

543 In an NFT sale, it is implied that the linked asset is what the seller claims it to be. However, an
544 asset could be a forgery whose origin is misrepresented. The seller may claim to have created
545 something that they simply copied off of the internet, or they may attribute the artwork to
546 another artist to increase the sale price. To a large extent, the purchaser must rely on the selling
547 smart contract and the associated NFT marketplace for this.

548 **3.3.3.3. Authorized**

549 The smart contract guarantees that only the current owner of an NFT can sell an NFT data
550 record. However, whether the original seller is in fact authorized to sell an NFT that is linked to a
551 particular asset is a legal question that is out of scope for this publication. From a technical point
552 of view, anybody can sell an NFT linked to anything. This creates a potential for
553 misrepresentation or fraud that must be addressed by non-technical controls (e.g. a legal
554 framework). What is being directly sold is the smart contract data record, and the owner of the
555 linked asset does not need to be involved. Ownership of the data record might convey rights over
556 the linked asset, but that is a legal question. In many cases, the buyer does not obtain any rights
557 whatsoever to the linked asset. For example, one NFT marketplace clearly specifies that “the
558 purchase of an NFT does not give the buyer the right to every copy of the underlying work, nor
559 the right to reproduce, distribute, commercially exploit, publicly perform, or publicly display the
560 NFT or objects included as part of the work” [20]. In such cases, the right being provided the
561 purchaser is the privilege to digitally autograph the asset and to subsequently sell that right to
562 another.

563

564 **4. List of Potential Security Concerns**

565 This section lists 27 potential security concerns that can exist with NFT ownership and smart
566 contract management of tokens. The identified security concerns are organized by NFT property.

567 **Owned** (Section 3.3.1.1)

- 568 1. An NFT purchaser may be deceived into thinking that they are purchasing an asset
569 instead of a smart contract data record that contains a reference to the asset (possibly
570 conferring no rights over the asset at all).
- 571 2. A smart contract may create a token linked to an asset without the legal authority to do so
572 for that asset since, technically, anyone can create an NFT linked to anything.
- 573 3. If a blockchain account is compromised, the malicious actor can transfer all NFTs
574 associated with that address to an address owned by the actor.
- 575 4. Stolen tokens will likely be sold immediately by malicious actors for cryptocurrency,
576 preventing easy restoration of the tokens even if a mechanism is available to do so.

577 **Transferable** (Section 3.3.1.2)

- 578 5. There is likely no smart contract mechanism to restore stolen tokens to their rightful
579 owner.
- 580 6. If a smart contract enables the contract manager to restore stolen tokens, this feature
581 could be used by the manager to confiscate, freeze, or unilaterally transfer tokens.
- 582 7. A smart contract may not allow a manager to restore stolen tokens, but the smart contract
583 may have a manager-controlled update mechanism whereby this feature could be added
584 in the future (enabling the previously mentioned security concern).
- 585 8. Coding errors in the smart contract could enable attackers to steal tokens and transfer
586 them to their accounts.

587 **Indivisible** (Section 3.3.1.3)

- 588 9. Fractional ownership increases the NFT attack surface by involving an additional third-
589 party smart contract that handles the fractional ownership.
- 590 10. Owners of fractional shares may not be aware that they could lose their shares through a
591 forced buyout.

592 **Linked** (Section 3.3.1.4)

- 593 11. Inaccurately stored metadata (either done maliciously or accidentally) can delink an NFT
594 from the asset it represents and make it worthless.
- 595 12. Server errors that make a digital asset unavailable (e.g., corrupted file, server failure, or
596 storage service discontinuation) could effectively delink an NFT from the asset it
597 represents and make it worthless.
- 598 13. If the off-blockchain table linking NFT identifiers to URLs is compromised, an attacker
599 could delink NFTs from their assets and/or change which NFTs represent which assets.
- 600 14. If off-blockchain tables are used to link NFT identifiers to URLs, the owner of the table
601 could use their access to delink NFTs and/or change which NFTs represent which assets.

602 **Recorded** (Section 3.3.2.1)

603 15. An NFT owner may not realize that their account and information on the NFTs that their
604 account owns are public information on the associated blockchain.

605 16. While blockchain accounts are anonymous, they can be de-anonymized through account
606 owner purchases that include personally identifying information (e.g., name and address).

607 **Provenance** (Section 3.3.2.2)

608 17. A blockchain could undergo an attack enabling changes to blockchain history (this is
609 unlikely with established blockchains).

610 **Permanence** (Section 3.3.2.3)

611 18. An NFT may be burned (accidentally or maliciously) by sending it to an address no one
612 has access to.

613 19. An NFT smart contract could self-destruct, destroying the managed NFTs.

614 **Immutable** (Section 3.3.2.4)

615 20. If the smart contract code contains a vulnerability, the data records could be changed by a
616 malicious actor.

617 21. Blockchains are occasionally changed through participant consensus or have their chains
618 split into distinct and different versions when consensus is not reached on resolving a
619 major issue.

620 22. A blockchain split will result in the duplication of NFT contracts, which in turn results in
621 NFT owners having the same NFTs on two blockchains. They could sell one and keep the
622 other, causing significant issues for NFTs that convey ownership rights over their linked
623 asset.

624 **Unique** (Section 3.3.3.1)

625 23. Buyers may not be aware that an exchange is selling the same NFT multiple times (e.g.,
626 permitting a limited number of autographs for video clips).

627 24. The same asset (or copies with unperceivable changes to humans) could be sold
628 simultaneously by multiple NFT exchanges or smart contracts.

629 **Authentic** (Section 3.3.3.2)

630 25. An asset linked to an NFT may be a forgery or an authentic original artwork whose origin
631 is misrepresented or attributed to a different creator (e.g., to increase its perceived value).

632 **Authorized** (Section 3.3.3.3)

633 26. The seller may not be authorized to sell an NFT linked to a particular asset.

634 27. The buyer may be deceived into not receiving the rights over the linked asset that they
635 think they are obtaining by purchasing an NFT.

636 **5. Token Standards**

637 NFT standards build upon the work done in fungible token standards and modify token
638 definitions so that each token is unique. Standards are critical for all types of cryptocurrency
639 tokens so that cryptocurrency exchanges can easily adopt them, smart contracts can accept and
640 manage them, and user wallets can buy and sell new token types. Such standards define the
641 services and interfaces for token smart contracts. The standards are typically represented in the
642 form of code that has mandatory inheritable functions. They are often created and managed
643 within cryptographic communities and are, thus, community standards that are not associated
644 with traditional formal standards bodies.

645 Many token standards [10] are in the form of an Ethereum Request for Comment (ERC) [11]
646 because Ethereum was the first blockchain platform to provide tokens. ERCs are standards for
647 Ethereum, and they provide requirements for smart contract interface design. Currently, many
648 blockchains provide token management, and ERCs have been ported to equivalent versions on
649 other platforms to support this (there are also independent standards efforts on other platforms).

650 **5.1. ERC-20: Fungible Token Standard**

651 ERC-20 was the first fungible token standard [13]. It defines a minimum interface for smart
652 contracts that provide interchangeable and identical tokens. Compliant contracts provide
653 functions that return the following state information:

- 654 1. The name of the token,
- 655 2. The symbol,
- 656 3. The total token supply,
- 657 4. The balance for each owner, and
- 658 5. The amount that an “approved” spender is allowed to transfer from an owner’s account.

659 Additional required functions manage the token transfers:

- 660 1. The owner transfers a specified number of their tokens to an address.
- 661 2. The owner approves an address to transfer a certain number of their tokens.
- 662 3. An approved spender transfers a specified number of tokens from one address to another
663 address (limited by the amount specified by the owner).

664 An ERC-20-compliant smart contract must emit an “event” for every transfer and address
665 approval. An event is an entry in a blockchain log and is, thus, publicly viewable by all
666 blockchain users.

667 **5.2. ERC-721: Non-Fungible Token Standard**

668 ERC-721 functions similarly to ERC-20. It defines a minimum interface for smart contracts that
669 provide unique tokens. Compliant contracts provide functions that return the following state
670 information:

- 671 1. The owner of an NFT,

- 672 2. The number of NFTs assigned to each owner,
673 3. The address “approved” to transfer an NFT, and
674 4. Whether or not an address is an “authorized operator” for another address.

675 Additional required functions manage the token transfers:

- 676 1. The owner, an approved address, or an authorized operator transfers tokens from one
677 address to another.
678 2. The owner, an approved address, or an authorized operator “safely” transfers tokens from
679 one address to another (checking that the recipient smart contract is capable of receiving
680 NFTs).
681 3. The owner or an authorized operator sets the address that is “approved” to transfer an
682 NFT.
683 4. The owner updates the status of an address relative to being an “authorized operator” to
684 manage all of their NFTs.

685 Like ERC-20, a compliant smart contract must emit an “event” for every transfer, address
686 approval, and “authorized operator” change of status.

687 The transfer “safely” function is based on ERC-165 [14]. The NFT contract checks to see
688 whether the recipient of an NFT is a smart contract or a user by checking the code size of the
689 recipient address. If the recipient is a contract, the NFT contract calls the “onERC721Received”
690 function in the recipient contract. It checks for a return value of the Keccak-256 hash of a
691 specified string (comprising the function call and its parameters). If the correct return value is not
692 supplied (possibly because the “onERC721Received” function does not exist), then the transfer
693 is reverted.

694 An example ERC-721 smart contract is available at [15].

695 **5.3. Other NFT Standards**

696 ERC-1155 provides for both fungible and non-fungible tokens in the same smart contract [16].
697 With ERC-1155, a single smart contract can simultaneously support ERC-721 and ERC-20
698 functionality while managing multiple token types.

699 ERC-2309 provides “a standardized event emitted when creating/transferring one, or many non-
700 fungible tokens using consecutive token identifiers” [17].

701 ERC-4400 enables a “consumer” role for NFTs [18]. Consumers can perform limited operations
702 upon NFTs without owning them. For example, if an NFT represents a parcel of digital land in a
703 virtual universe, a consumer of the NFT might be allowed to modify the property (as if they were
704 renting it) but would not be the owner (could not transfer ownership).

705 ERC-4907 enables a “user” role for NFTs [19]. Users can use the NFT for a specified period of
706 time, but they cannot transfer ownership of the NFT or enable other users. An example would be
707 a virtual tool in a game that allows a user to build virtual objects but only during their specified
708 time limit.

709

710 **6. Marketplaces and Exchanges**

711 NFT marketplaces (also called exchanges) enable users to buy, sell, and mint (i.e., create) NFTs
712 [23]. The marketplaces should provide some level of verification for the posted NFTs. The oldest
713 was launched in 2017, making both NFTs and their exchanges relatively new technology.

714 These marketplaces have an attack surface separate from the associated NFT smart contracts and
715 may be the target of hacking activity. As mentioned in Section 1.1, a security analysis of NFT
716 marketplaces is out of scope of this publication (but see [31] and [32]). Here, a brief overview of
717 NFT marketplace security models is provided.

718 NFTs can be bought through direct purchase, by participating in an auction, or by making an
719 offer. For exchanges that use a decentralized finance (DeFi) approach, customers need their own
720 cryptocurrency wallet (either software or hardware). Alternatively, exchanges may use a
721 centralized finance (CeFi) approach in which customers use custodial wallets provided by the
722 exchanges. In the CeFi model, the exchange is the custodian of the cryptographic keys and holds
723 the NFTs on behalf of their customers (analogous to an investment firm acting as a custodian and
724 holding stock for its clients). In the DeFi mode, the purchaser uses a wallet to hold the
725 cryptographic keys that grant them ownership of the NFTs.

726 In both approaches, a malicious entity could compromise the user-owned wallet (for DeFi NFT
727 approaches) or the custodial wallet system (for CeFi NFT approaches). The former requires the
728 user to secure their own wallet; many cryptocurrency wallet users have had their cryptographic
729 keys stolen. The latter requires the user to trust the CeFi custodian to secure their NFTs in
730 custodial wallets; cryptocurrency custodial systems have been hacked, resulting in the loss of
731 user assets. There is no guaranteed security for crypto assets. Guidance for the security of
732 cryptographic wallets is out of scope for this publication, though many resources are available
733 online (e.g., [24]).

734 While some take credit cards and other forms of traditional payment (usually with an additional
735 processing fee), marketplaces may only accept cryptocurrency, which is the preferred form of
736 payment. This is because NFT data records are managed by smart contracts, and smart contracts
737 only accept cryptocurrency. Also, marketplaces may not be able to handle fiat currencies due to
738 associated regulatory requirements. Also, accepting fiat currency requires additional
739 centralization of the marketplace architecture and many strive to maintain a decentralized model.

740 **7. Conclusion**

741 Currently, most NFT sales are of the digital autographing type. This makes most NFTs prestige
742 purchases where the buyer obtains the right from the linked asset’s copyright holder to uniquely
743 link their name to the asset in a smart contract data record on a blockchain. However, NFTs are
744 also used for actual sales of assets (both digital and physical) as well as for utilitarian purposes
745 such as voting rights, membership, and benefits. These latter use cases necessitate a robust and
746 secure design and implementation of NFTs.

747 Presently, many NFT implementations have achieved a high level of security. NFT reliance on
748 blockchains and smart contracts provides secure cryptographic methods for establishing and
749 publicly recording ownership. The NFT smart contracts provide the NFT properties of *recorded*,
750 *owned*, *transferable*, *indivisible*, and *linked*. The blockchain ensures *provenance*, *permanence*,
751 and *immutable*. Human NFT management provides the properties of *unique*, *authentic*, and
752 *authorized*.

753 Despite a solid cryptographic foundation, there are potential security concerns related to these
754 NFT properties, this work identified 27 by evaluating the 11 NFT properties. Each of these can
755 be addressed through considering security upfront and creating a secure design and
756 implementation. Adoption of a systematic security approach, such as the NIST Risk
757 Management Framework [35], can help address these potential concerns. While further research
758 should be conducted in this area, the security analysis in this work did not reveal any non-
759 addressable weaknesses that would undermine the overall approach and technology.

760

761

762 **References**

- 763 [1] Investopedia (2023) *Non-Fungible Token (NFT): What It Means and How It Works*.
764 Available at <https://www.investopedia.com/non-fungible-tokens-nft-5115211>
- 765 [2] Holbein (2022) *Evolving Legal Issues for NFTs*. Available at
766 <https://www.jdsupra.com/legalnews/evolving-legal-issues-for-nfts-5461995>
- 767 [3] Mettei (2023) *Code is Not Law: Case on Who Owns the First NFT Dismissed by Judge*.
768 Available at [https://www.artnews.com/art-news/news/kevin-mccoy-quantum-case-](https://www.artnews.com/art-news/news/kevin-mccoy-quantum-case-dismissed-free-holdings-sothebys-1234662076)
769 [dismissed-free-holdings-sothebys-1234662076](https://www.artnews.com/art-news/news/kevin-mccoy-quantum-case-dismissed-free-holdings-sothebys-1234662076)
- 770 [4] BCC Publishing (2022) *Non-Fungible Tokens (NFTs): Global Market*. Available at
771 <https://www.bccresearch.com/market-research/information-technology/nft-market.html>
- 772 [5] Shewale (2023) *12 Most Expensive NFTs Ever Sold*. Available at
773 <https://www.demandsage.com/most-expensive-nfts>
- 774 [6] Clark, Aujla, Gould (2021) *What are the Legal Issues Concerning Non-Fungible Tokens*
775 *(NFTs)?* Available at [https://artlawandmore.com/2021/07/08/what-are-the-legal-issues-](https://artlawandmore.com/2021/07/08/what-are-the-legal-issues-concerning-non-fungible-tokens-nfts)
776 [concerning-non-fungible-tokens-nfts](https://artlawandmore.com/2021/07/08/what-are-the-legal-issues-concerning-non-fungible-tokens-nfts)
- 777 [7] Fractional (2023) *Buy and Sell Fractions of NFTs*. Available at <https://fractional.art>
- 778 [8] Nico (2021) *How to Make an NFT in 14 Lines of Code*. Available at
779 <https://www.freecodecamp.org/news/how-to-make-an-nft>
- 780 [9] IPFS (2023) *What is IPFS*. Available at <https://docs.ipfs.tech/concepts/what-is-ipfs>
- 781 [10] Ethereum (2022) *Ethereum Development Standards*. Available at
782 <https://ethereum.org/en/developers/docs/standards>
- 783 [11] Crypto.com (2022) *What are Token Standards? An Overview*. Available at
784 <https://crypto.com/university/what-are-token-standards>
- 785 [12] Crypto.com (2023) *What is the BRC-20 Token Standard for Bitcoin?* Available at
786 <https://crypto.com/university/brc-20-token-standard-bitcoin>
- 787 [13] Ethereum (2023) *ERC-20 Token Standard*. Available at
788 <https://ethereum.org/en/developers/docs/standards/tokens/erc-20>
- 789 [14] Zhang (2019) *Ethereum Standard ERC165 Explained*. Available at
790 <https://medium.com/@chiqing/ethereum-standard-erc165-explained-63b54ca0d273>
- 791 [15] OpenZeppelin (2023) *ERC721.sol*. Available at [openzeppelin-contracts/ERC721.sol at](https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/ERC721.sol)
792 [master · OpenZeppelin/openzeppelin-contracts · GitHub](https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/ERC721.sol)
- 793 [16] OpenZeppelin (2023) *ERC-1155 Multi-Token Standard*. Available at [openzeppelin-](https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/ERC1155.sol)
794 [contracts/ERC1155.sol at master · OpenZeppelin/openzeppelin-contracts · GitHub](https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/ERC1155.sol)
- 795 [17] Papanikolas (2019) *ERC-2309: ERC-721 Consecutive Transfer Extension*. Available at
796 <https://eips.ethereum.org/EIPS/eip-2309>
- 797 [18] Ivanov (2021) *ERC-4400: EIP-721 Consumable Extension*. Available at
798 <https://eips.ethereum.org/EIPS/eip-4400>
- 799 [19] Anders, Lance, Shrug (2022) *ERC-4907: Rental NFT, an Extension of EIP-721*. Available at
800 <https://eips.ethereum.org/EIPS/eip-4907>
- 801 [20] Verisart (2023) *What is an NFT?* Available at [https://help.verisart.com/en/articles/5647641-](https://help.verisart.com/en/articles/5647641-what-is-an-nft)
802 [what-is-an-nft](https://help.verisart.com/en/articles/5647641-what-is-an-nft)
- 803 [21] Wikipedia (2023) *Everydays: the First 5000 Days*. Available at
804 [https://en.wikipedia.org/wiki/Everydays:_the_First_5000_Days#:~:text=Sundaresan%20rec](https://en.wikipedia.org/wiki/Everydays:_the_First_5000_Days#:~:text=Sundaresan%20receives%20rights%20to%20display,view%20through%20a%20web%20browser)
805 [eives%20rights%20to%20display,view%20through%20a%20web%20browser](https://en.wikipedia.org/wiki/Everydays:_the_First_5000_Days#:~:text=Sundaresan%20receives%20rights%20to%20display,view%20through%20a%20web%20browser)

- 806 [22] Yaga D, Mell P, Roby N, Scarfone K (2018), Blockchain Technology Overview. (National
807 Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal
808 Report (IR) NIST IR 8202. <https://doi.org/10.6028/NIST.IR.8202>
809 [23] Rodeck (2023) *Top NFT Marketplaces of June 2023*. Available at
810 <https://www.forbes.com/advisor/investing/cryptocurrency/best-nft-marketplaces>
811 [24] Hojjati (2022) *How to Secure Your Crypto Wallet Against Hacks*. Available at
812 <https://www.digicert.com/blog/how-to-secure-your-crypto-wallet-against-hacks>
813 [25] Frankenfield (2022) *51% Attack: Definition, Who is at Risk, Example, and Cost*. Available
814 at <https://www.investopedia.com/terms/1/51-attack.asp>
815 [26] Binance (2022) *Physical NFTs: Bridging the Gap Between Digital and Physical Worlds*.
816 Available at [https://www.binance.com/en/blog/nft/physical-nfts-bridging-the-gap-between-](https://www.binance.com/en/blog/nft/physical-nfts-bridging-the-gap-between-digital-and-physical-worlds-7460772280213595786)
817 [digital-and-physical-worlds-7460772280213595786](https://www.binance.com/en/blog/nft/physical-nfts-bridging-the-gap-between-digital-and-physical-worlds-7460772280213595786)
818 [27] Wikipedia (2023) *The DAO (organization)*. Available at
819 [https://en.wikipedia.org/wiki/The_DAO_\(organization\)](https://en.wikipedia.org/wiki/The_DAO_(organization))
820 [28] Bored Ape Yacht Club (2023). *Contract*
821 *0xBC4CA0EdA7647A8aB7C2061c2E118A18a936f13D*. Available at
822 <https://etherscan.io/address/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d#code>.
823 [29] OpenSea (2022). *Announcing a contract upgrade*. Available at
824 <https://opensea.io/blog/articles/announcing-a-contract-upgrade>
825 [30] Yang, Shuo, Jiachi Chen, and Zibin Zheng. "Definition and Detection of Defects in NFT
826 Smart Contracts." arXiv preprint arXiv:2305.15829 (2023). Available at
827 <https://arxiv.org/pdf/2305.15829.pdf>
828 [31] Stöger, Felix, et al. "Demystifying Web3 Centralization: The Case of Off-Chain NFT
829 Hijacking." Available at <https://fc23.ifca.ai/preproceedings/156.pdf>
830 [32] Das, Dipanjan, et al. "Understanding security issues in the NFT ecosystem." Proceedings of
831 the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022.
832 Available at <https://arxiv.org/pdf/2111.08893.pdf>
833 [33] Wang, Ziwei, Jiashi Gao, and Xuetao Wei. "Do NFTs' Owners Really Possess their Assets?
834 A First Look at the NFT-to-Asset Connection Fragility." Proceedings of the ACM Web
835 Conference 2023. 2023. Available at <https://arxiv.org/pdf/2212.11181.pdf>
836 [34] Sharma (2023). *BRC-20 Tokens: A Primer*. Available at
837 <https://research.binance.com/static/pdf/BRC-20%20Tokens%20-%20A%20Primer.pdf>
838 [35] Joint Task Force (2018). Risk Management Framework for Information Systems and
839 Organizations: A System Life Cycle Approach for Security and Privacy. NIST SP 800-37
840 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
841 [36] Thubron (2023). *Auction for the \$2.9 million Jack Dorsey tweet NFT has a high bid of*
842 *\$1,871*. Available at [https://www.techspot.com/news/99510-auction-29-million-jack-](https://www.techspot.com/news/99510-auction-29-million-jack-dorsey-tweet-nft-has.html)
843 [dorsey-tweet-nft-has.html](https://www.techspot.com/news/99510-auction-29-million-jack-dorsey-tweet-nft-has.html)
844 [37] Dreben, Pennington (2021). Nonfungible Tokens and Copyright: Diligence Issues to
845 Consider. Available at [https://www.morganlewis.com/pubs/2021/04/nonfungible-tokens-](https://www.morganlewis.com/pubs/2021/04/nonfungible-tokens-and-copyright-diligence-issues-to-consider)
846 [and-copyright-diligence-issues-to-consider](https://www.morganlewis.com/pubs/2021/04/nonfungible-tokens-and-copyright-diligence-issues-to-consider)
847
848
849

850 **Appendix A. List of Symbols, Abbreviations, and Acronyms**

851 **BRC**

852 Bitcoin Request for Comment

853 **ERC**

854 Ethereum Request for Comment

855 **F-NFT**

856 Fractionalized non-Fungible Token

857 **IR**

858 Interagency or Internal Report

859 **NFT**

860 Non-Fungible Token

861 **IPFS**

862 InterPlanetary File System

863 **URI**

864 Uniform Resource Identifier

865 **URL**

866 Uniform Resource Locator

867

868 **Appendix B. Fractional Token Example**

869 Consider a person buying an image NFT from a marketplace. The NFT smart contract records
870 the owner's blockchain address in the NFT's data record. To fractionalize, the owner transfers
871 the NFT to a fractionalized NFT (F-NFT) smart contract. The original NFT smart contract
872 records the F-NFT contract as the owner. The NFT is now "locked" in the F-NFT contract. The
873 F-NFT contract then sells 10 ERC-20 tokens for 1 ETH each and gives the proceeds to the
874 original owner, minus a fee. Five users buy the tokens:

- 875 • Alice: 4 \$JPEG
- 876 • Bob: 1 \$JPEG
- 877 • Carol: 2 \$JPEG
- 878 • Dave: 1 \$JPEG
- 879 • Erin: 2 \$JPEG

880 The F-NFT contract specifies a buyout function that requires at least four of the tokens be
881 deposited to start the auction. Eventually, Alice decides that she wants the whole NFT to herself
882 and deposits her four tokens to initiate the buyout.

883 Alice bids 1.1 ETH per token. If she wins, she will need to pay 6.6 ETH to purchase the
884 remaining six tokens and claim the original NFT for herself. The other fractional owners would
885 then split the 6.6 ETH proportionally according to the number of ERC-20 tokens that they hold.

886 If Bob, Carol, Dave, and Erin collectively bid 1.2 ETH per token and outbid Alice, they would
887 then pay 4.8 ETH to Alice and receive a fraction of the four ERC-20 tokens that Alice had
888 deposited, proportional to the amount that each owner contributed. If each of them paid 1.2 ETH,
889 then they would each gain one additional token (representing fractional ownership) after
890 outbidding Alice.

891

892