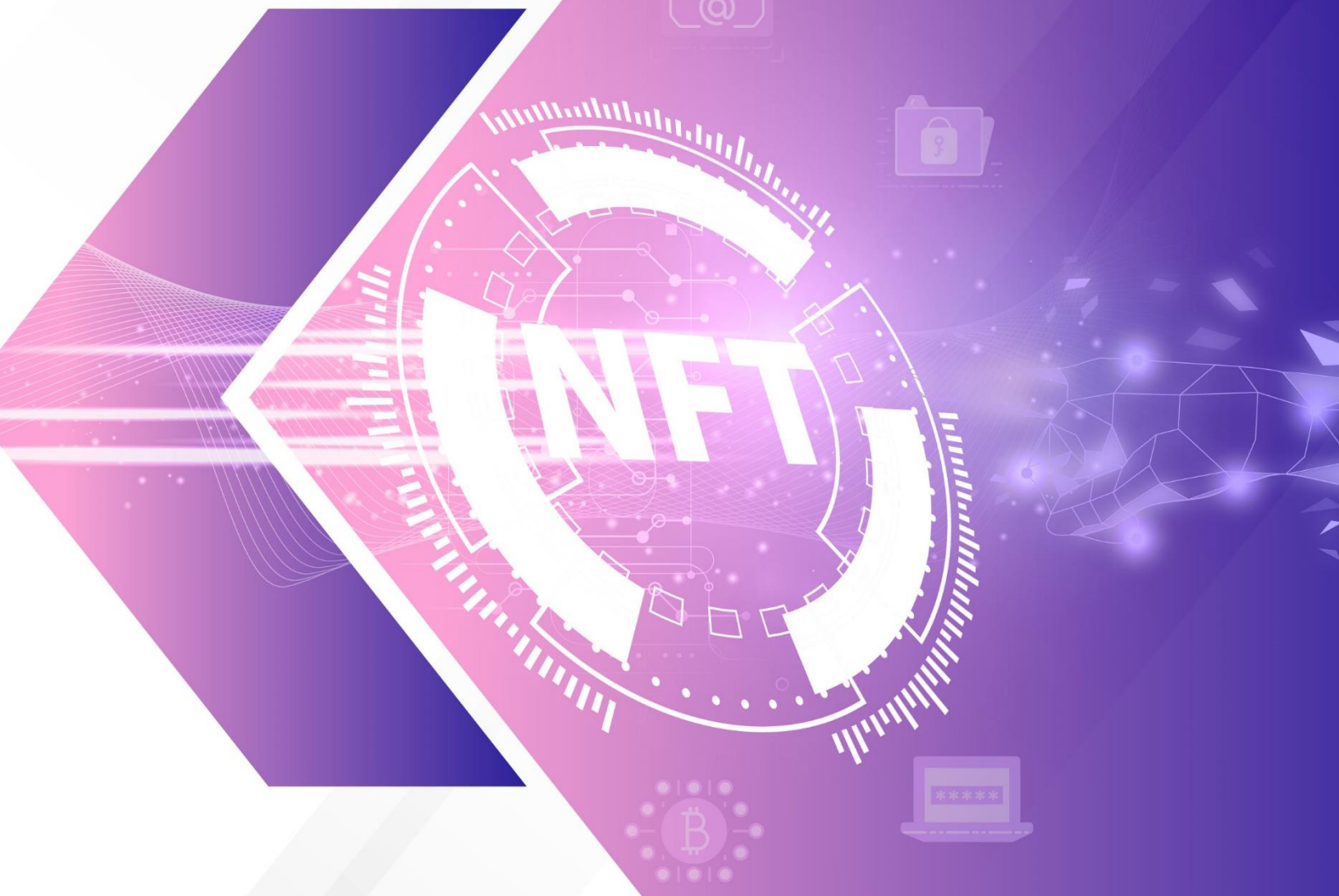
CYBERSECURITY CENTRE of EXCELLENCE

A joint initiative of DSCI & Government of Telangana

DSCI PROMOTING DATA PROTECTION

A NASSCOM® Initiative



NFTs AND CYBERSECURITY

NFTs and Cybersecurity

Table of Contents:

1 NFTs Overview

1.1 NFT

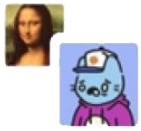
NFTs (Non-Fungible Tokens) are distinctive digital assets with ownership based on blockchain technology. Digital artwork, collectables, VR products, and others are a few examples of NFTs. In simpler terms, if an item is semi-fungible, and non-fungible items is illustrated below [1].

Fungible

My Rs. 10 is valued the same as your Rs. 10

Semi-Fungible

We both have tickets to the show, although the seat numbers could alter the value



Non-Fungible

Represents something unique in value

(Source: "What is a Non-Fungible Token (NFT)?": **https://support.opensea.io/hc/en-us/articles/360063450733-What-is-a-Non-Fungible-Token-NFT-)**

1.2 NFTs in the Metaverse Economy

The Metaverse is a collaborative virtual environment that provides experiences that span social media networks and reality. Since Metaverse is such a broad topic, this section only briefly addresses NFTs in the Metaverse. Several of the NFTs have been showcased on VR platforms, which has accelerated the interest in the development of a digital universe and the possibility of NFTs being a part of the "Metaverse."

NFTs are quickly becoming the Metaverse's foundational technology. The Sandbox [111], a Metaverse project, has already been employing NFTs to showcase digital land, virtual furniture and decor, and so forth. Top brands and celebrities from various industries, such as Atari, Snoop Dogg, and the South China Morning Post, all own plots of digital land in the Sandbox, which uses NFTs to represent metaverse real estate.

1.3 Why are NFTs important?

Technically an NFT is a unique token on the blockchain. NFTs are intended to offer you something unique like the ownership of the work. In short, NFTs are distinct digital assets that cannot be duplicated or exchanged for another of identical value.

It is essential to note that purchasing an NFT does not imply ownership of the digital asset altogether. It only grants ownership of a unique digital token. In the context of digital artworks, the artist retains ownership of the original piece. Meanwhile, the NFT owner has the token transaction and a hash code indicating ownership. They can't sell the digital asset, but they can resell the token [2].

While the world is getting progressively digital, maintaining data privacy is more imperative than ever. NFTs could be used to develop blockchain-based solutions that establish tamper-proof transaction records [3].

2 Technical Features & Standards of NFTs

We show technical features associated with the NFT's activities in this section. These features serve as the foundation for a successful NFT scheme [4].

2.1 Blockchain

Blockchain is a decentralised and attached-only database that ensures the integrity of a collection of data records that are linked and secured using cryptographic techniques [5]. The perennial Byzantine challenge [6] has a solution in blockchain, which is now being agreed upon by a broad network of untrustworthy participants. Any changes to the recorded data will invalidate all subsequent data since the data shared on the blockchain becomes immutable once it is confirmed in the majority of distributed nodes. Ethereum [7] is the most prevalent blockchain platform utilised in NFT schemes, as it provides a secure environment for smart contract execution. Furthermore, Flow [8], EOS [9], Hyperledger [10][11], and Fast Box [12] are among the solutions that have developed their customised chain-engines or blockchain platforms to support their specialised services.

2.2 Cybersecurity management through the Blockchain Technology

In the field of cyber security, blockchain technology has set new standards. It protects various organisations from cyber-attacks by providing a decentralised platform for data security and storage. It could be used to maintain track of people's information as well. As a distributed database, blockchain technology maintains a record of the growing list of data records identified as blocks. Every block contains a cryptographic hash of the preceding block and the encrypted transaction information. One of its most noteworthy characteristics is its immutability. Furthermore, It's also used to authenticate users' identities and make sure they're not being exploited. Due to its secure and transparent nature, blockchain technology is reliable and tamper-proof. As a result, they're ideal for storing sensitive information [3].

2.2.1 Decentralised Technology

The blockchain network enables users to store information in a decentralised manner which could be used for high-level encryption. Because the framework is decentralised, no single entity can regulate the hacker's identity. However, hacking threats on the network are now extremely difficult since they would require attacking 51% of the system at the same time.

2.2.2 Smart Contracts

Smart contracts are self-executing contracts that utilise blockchain technology to automatically enforce the conditions of a deal. Since they are tamper-proof and transparent, they facilitate trust and security in a business. Investors could also use them to manage identities. This helps in preventing identity fraud and theft. To maintain order-sensitive executions, many NFT solutions [14][15][16][17][18] depend on smart contract-based blockchain platforms.

Smart contracts allow unknown parties and decentralised participants to undertake fair exchanges without the need for a trusted third party, and they also advocate a unified method for developing applications across a wide range of industries. State-transition mechanisms underpin the applications that run on top of smart contracts. All participants share the states that contain the instructions and parameters, ensuring transparency in the delivery of these instructions.

2.3 Ethereum Blockchain

Many NFTs are part of the Ethereum blockchain to a greater extent. Ethereum is a cryptocurrency, similar to bitcoin, dogecoin, XRP, and others, but its blockchain also facilitates these NFTs, which hold additional information that distinguishes Ethereum from other cryptocurrencies [19].

Ethereum aims to develop a protocol for building decentralised applications that offer a unique set of tradeoffs that would be useful for a wide range of decentralised applications, with a focus on instances where agile development time, protection for small and sparsely used applications, and the tendency for various applications to interact very efficiently are all essential. Ethereum implements this by developing the best possible abstract foundational layer. The built-in Turing-complete system in the blockchain allows anyone to write DApps (decentralised applications) and smart contracts with their own arbitrarily defined ownership, transaction configurations, and state transition features.

Because of the extra powers of Turing-completeness, blockchain, value-awareness, and state, one can write smart contracts and cryptographic boxes that hold a value and automatically unlock it if specific conditions are satisfied on top of the platform, due to additional power when compared to Bitcoin scripting [20].

2.4 Benefits of using Ethereum

- ➔ The token metadata and transaction history can be verified by anyone. As a result, proving ownership history is simple.
- ➔ It's unlikely to steal ownership of a transaction once it's been confirmed.
- ➔ Since Ethereum is never down, your tokens are always accessible to sell.
- ➔ Trading NFTs can be performed peer-to-peer without the constraint for platforms that are inclined to accept huge commissions.
- ➔ The backend of all Ethereum based platforms is the same. In simpler terms, all Ethereum platforms can interact effectively with one another, making NFTs transferable across platforms. You can easily trade or exchange NFTs on multiple platforms.
- ➔ You can list your NFTs on several platforms simultaneously as a creator, and each product will have the most updated ownership information.

2.5 Ethereum Standards to build NFTs

Several of the Ethereum development standards mainly focus on token interfaces. These standards aid in the composability of smart contracts, ensuring that, for instance, when a new project releases a token, it is interoperable with current decentralised exchanges.

On Ethereum, the following are among the most widely used token standards: [21]

ERC-20: This standard issues fungible tokens on Ethereum once the conditions are met. This standard renders tokens identical to one another. For instance, an ERC-20 Token works similar to ETH, which means that one Token is identical to the other Tokens concerning both value and type [22]. This is how a lot of public chains and Ethereum - based DApps [26][27] obtain their initial funding. ERC-20 is a standard that indicates the value of fungible assets and can be used to manage crowdfunding campaigns, ICOs and introduce new cryptocurrencies on the marketplace.

ERC-721: ERC-721 [28][23] offers a non-fungible token standard, which is different from fungible tokens. This is a one-of-a-kind token that can be differentiated from others. Every NFT contains a uint256 tokenId variable, and the combination of uint256 tokenId and contract address is globally distinct. Furthermore, the tokenId can be utilised as an input parameter to develop special identifications like photos of arms and ammunition, amazing kittens, or attributes. ERC-721 is a digital asset ownership token that's often utilised as a non-fungible token (NFT) in the gaming market, Metaverse platforms, and NFT marketplaces.

ERC-1155 (Multi-Token Standard): ERC-1155 is a prominent standard for managing numerous token kinds in contracts. A single deployed contract can comprise some combination of fungible, non-fungible, and even semi-fungible tokens in some circumstances. The ERC-1155 token may also perform the same functions as the ERC-20 and ERC-721 tokens, or even both simultaneously. And, most importantly, this standard enhances the performance, increases development

efficiency, and fixes noticeable implementation problems of both standards namely the ERC-20 and ERC-721 standards [24].

ERC-1155 technically enhances the functionalities of tokenId by allowing each of them to represent different customizable token kinds independently. Customised information, including metadata, availability, timestamp, or other attributes, may be included in this field. ERC1155, a multi-utility token standard, is extensively employed in online gaming. NFTs such as gaming avatars, and fungible native currencies are now available in games [4].

The illustration in **Figure-1** shows the Anatomy of the ERC-20, ERC-721, and ERC-1155 standards:

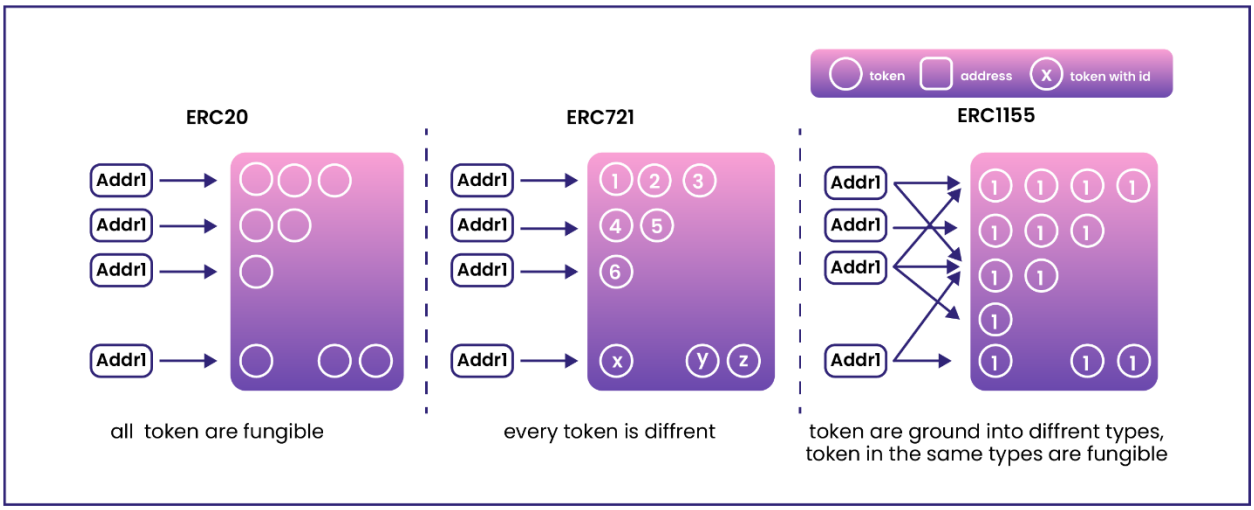


Figure-1: Anatomy of ERC-20, ERC-721 and ERC-1155
(Source: "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges," arXiv:2105.07447 [cs.CR] (2021)**)**

The ERC-721 [23] standard is used to build the bulk of NFTs. Other standards, such as the ERC-1155 standard [25], allow for semi-fungible tokens, which are particularly beneficial in the gaming industry [29].

Furthermore, all Ethereum transactions have a cost associated with them called 'gas,' which is prohibitively expensive. This has a substantial impact on the scalability of NFTs based on ETH standards. Consequently, to improve scalability, Ethereum is transitioning from proof-of-work (PoW) [94] to proof-of-stake (PoS) [93] for its consensus mechanism.

2.6 Other NFT Standards

The Non-Fungible Token (NFT) standards outline how to build NFTs on a specific blockchain. Although Ethereum may be the first blockchain platform to support NFTs, it was not designed particularly for them. Platforms such as Flow [8] and Tezos [91] were designed with NFTs in mind. Furthermore, these two blockchains are gaining momentum on the Ethereum platform in the NFT space [95].

Flow Blockchain: Flow started as a result of the popular NFT-based game CryptoKitties [15], which allows users to breed, buy, sell, and exchange digital cats. CryptoKitties became extremely popular, and the transactions overloaded the Ethereum blockchain network. The developers of the game Dapper Labs [92] sought to fix this issue by creating Flow, a blockchain built specifically for crypto-collectables and games. NBA Top Shot [16], a prominent NFT-based digital collectables platform, was also built by Dapper Labs.

Flow employs a consensus mechanism known as proof of stake [93]. Proof of Stake blockchains are more environmentally friendly than traditional blockchains that use the Proof of Work [94] mechanism for their consensus. To validate the amount of energy utilised by their blockchain network, Flow and Deloitte Canada collaborated to conduct an exhaustive energy consumption review [97]. Based on the analysis and research, the results have shown that Flow uses only 0.18 GWh annually [96], which is much less energy than other blockchain networks such as Bitcoin [98], Ethereum [99], Solana [100], and Polygon [101]. Simply put, minting an NFT on Flow uses less energy than performing a Google search or posting on Instagram.

Flow features "Upgradeable Smart Contracts" [102], which are smart contracts that may be launched in a "beta state" and then progressively updated until the original authors are satisfied. The smart contract becomes immutable once all key stakeholders are satisfied with it. Flow is designed with scalability in mind. Consequently NBA Top Shot, MotoGP, UFC, NFL, Samsung, Google, Ubisoft, along with several other notable organisations have joined the flow blockchain ecosystem.

Tezos Blockchain: Tezos is a decentralised blockchain ledger that employs a liquid-proof stake consensus mechanism. Tezos consumes nearly 2 million times less energy than Ethereum, making it a more environmentally friendly option. The platform's developers understand that lower transaction costs are necessary for widespread adoption and convenience. FA2 is Tezos's only Non-Fungible Token standard. The FA2 token standard, also referred to as the TZIP-12 [103] on Tezos, is a unified token contract interface that supports a variety of token types. It allows developers to build and invent new token types that can support sophisticated token interactions while keeping a standard API across third-party applications and wallets. These token structures can contain NFTs as well as a variety of transmutable gaming elements.

Tezos' diverse set of applications has attracted major corporations. Ubisoft, a French video game company, has joined the Tezos network as "bakers," who assist in validating new transactions, securing the network, and generating new tokens. Tezos was recently chosen by Formula One racing teams Red Bull Racing Honda and McLaren Racing to start building NFT-based fan experiences.

While Ethereum is currently the primary focus, many other NFT standards are gaining traction on other chains. Starting with EOS, DGoods [30], which was created by the Mythical Games team [31], aims to provide a feature-rich cross-chain standard. The Cosmos project is also working on an NFT module [32] that will be included in the Cosmos SDK [33][34]. It is clear that in the future, there will be many more NFT standards to choose from. NFTs are anticipated to power the next generation of games and media tools, as well as several other use cases like digital identity,

healthcare, finance, and logistics applications. Therefore, while determining which platform and token standard to use, it is critical to grasp the complexities, nuances, and transaction fee structures of every alternative standard and platform.

3 Protocols and Properties of NFTs

3.1 NFT Protocols

NFT needs a foundational distributed ledger containing records, as well as exchangeable transactions for peer-to-peer trading. To put this in context, a distributed ledger can be thought of as a special type of database for storing NFT information. We'll assume that the ledger has basic security, completeness, and availability features in this instance.

Consequently, we recognize two design patterns for the NFT framework. The first protocol is built from top to bottom by developing NFTs from the initiator and also selling them to the consumer, following a very simple yet conventional approach. The latter approach, on the other hand, reverses this path by establishing an NFT template from which each user can develop their own unique NFTs. It should be emphasised that when executed on blockchain platforms, each of them follow a nearly identical workflow. The core operational mechanics underpinning the workflow of an NFT system are illustrated in **Figure-2** [4].

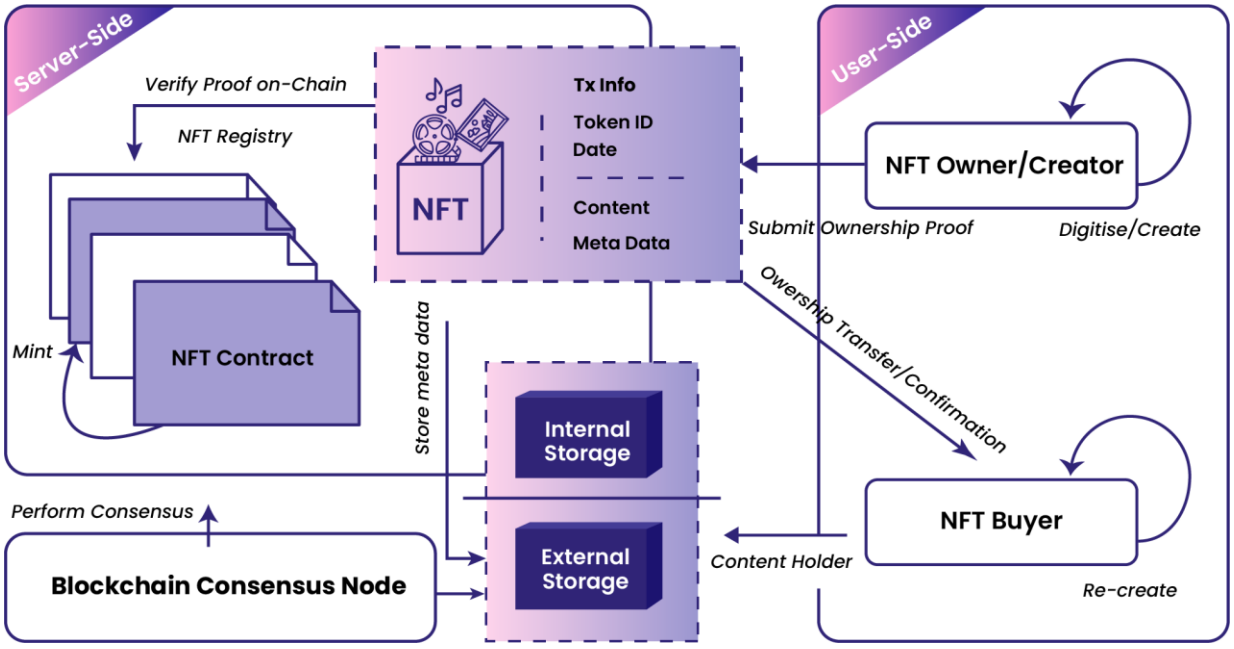


Figure-2: Workflow of an NFT System

(Source: "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges," arXiv:2105.07447 [cs.CR] (2021)**)**

3.1.1 Top to Bottom

The NFT protocol has two roles in the First Design Pattern: NFT owner and NFT buyer (e.g. CryptoPunks [14]).

Digitise: An NFT owner verifies that the file, title, and description are all accurate. After that, one can convert the raw data into a suitable format.

Store: Outside of the blockchain, an NFT owner stores the data in an external database. Keep in mind that, even though this operation consumes more gas, one is permitted to store the raw data within a blockchain.

Sign: The NFT owner approves a transaction with his signature and transmits it to a smart contract, along with the hash of NFT data.

Mint & Trade: The minting and trading procedure begins after the smart contract receives the transaction with the NFT data. The architecture of the Ethereum Token Standards, as stated in the previous section, is the key mechanism underpinning NFTs.

Confirm: After the transaction has been confirmed, the minting process is complete. Using this method, NFTs will be persistently tied to a special blockchain address as credible evidence.

3.1.2 Bottom to Top

The NFT protocol in the Second Design Pattern has two roles: NFT creator and NFT buyer. Since an NFT product is formed due to random seeds when a customer bids for it, in most circumstances a buyer can also operate as a creator. This expands the functionality concerning user customization.

Template Creation: The project creator uses the smart contract to create a template that contains various basic rules for the game, such as character appearance, weapons systems, and accessories.

Randomise: Once a buyer has placed a bid on an NFT, one can customise the NFT product by adding a variety of extra characteristics to the basic lines. These extra features are chosen at random from a database that's been predefined initially.

Mint & Trade: Again when the relevant smart contract is triggered, the minting and trading process begins.

Confirm: Smart contracts are used to carry out all of the operations. When the consensus process is completed, the created NFT will be permanently kept on-chain.

Essentially, an NFT system is a blockchain-based application with a limited capacity for each block. Every new NFT transaction must be sent to trigger the smart contract, and all linked blocks will have established a long-term history that is. everlasting. The NFT metadata and ownership details are appended to a new block when the transaction is confirmed, assuring that the NFT's history remains consistent and the ownership is preserved.

3.2 NFT Properties

NFTs obtain various unique properties due to blockchains. The following are a few of them [35]:

Standardisation: In the digital world, traditional digital assets such as event tickets and domain names lack a consistent representation. A video game's in-game collectables are usually presented differently compared to an event ticketing system. Developers can create universal, reusable, inheritable standards for all non-fungible assets by representing them on public blockchains. Basic primitives like ownership, exchange, and minimal access control are included. Additional standards, for instance, specs for displaying an NFT can be overlaid on top for rich and detailed presentation within applications.

These are akin to other digital building blocks such as the JPEG or PNG image file format, HTTP for inter-computer requests, and HTML / CSS for web content representation. On top of that, blockchains offer a layer that provides developers with a complete set of stateful primitives to develop applications.

Interoperability: Non-fungible token standards make it convenient for non-fungible tokens to freely move between ecosystems. Whenever a developer releases a new NFT project, the NFTs are instantly available on several different wallet providers, open for trading on marketplaces, and also displayable within virtual worlds. This is feasible since open standards offer APIs for reading and writing data that are clear, coherent, and trustworthy.

Tradeability: Free trading on public marketplaces is the most enticing feature enabled by interoperability. Users can now move items from their original ecosystems and into a marketplace in which they can use advanced trading features like eBay-style auctions [36], bidding [37], bundling [38], and the opportunity to sell in any currency, including stable coins [39] and application-specific currencies [40].

Furthermore, for game developers, in particular, asset tradability represents a shift from a closed to a public, free-market economy. From resource supply to pricing to capital constraints, game developers no longer need to oversee every aspect of their economy. Instead, they can delegate the arduous task to free markets!

Liquidity: NFTs with instant tradability will have more liquidity. NFT markets can appeal to a wide range of consumers, from experienced traders to newcomers, allowing assets to be exposed to a broader group of buyers. NFTs extend the marketplace for unique DApps in the same manner that the 2017 ICO boom gave birth to a new asset class propelled by immediately liquid tokens.

Immutability and provable scarcity: Developers can use smart contracts to set clear restrictions on the number of non-fungible tokens and specify enduring attributes that cannot be altered after the tokens are released. For instance, a developer can programmatically restrict the number of rare items that can be generated while maintaining the supply of more common items unrestricted. Developers can also encode those specific properties on-chain to ensure that they do not alter over time. This is particularly intriguing in the artworks domain, which is primarily concerned with the verifiable rarity of an original item.

Programmability: NFTs are fully programmable, just as traditional digital assets. CryptoKitties [15] included a breeding mechanism in the contract that reflects the virtual cats. Many modern NFTs include more advanced mechanisms, such as forging, random generation, crafting, redeeming, and so on. The design world is loaded with opportunities.

4 Cybersecurity features in NFTs

NFTs work in collaboration with other security aspects to promote and influence cybersecurity. NFTs improve cybersecurity since they are difficult to replicate and link to other digital assets. Cryptography usage is also beneficial to security. NFTs also use a smart encryption and validation approach to enhance the security of digital assets. Every piece of work has a unique digital signature that identifies the creator. NFTs also add an extra degree of security for businesses and individuals who would like to safeguard their digital assets [3].

4.1 Smart Encryption and Validation

To strengthen the security of digital assets, NFTs use a "smart encryption and validation" mechanism. Their technology is robust and elegant, allowing anyone with internet access to effortlessly exchange them. In public and private blockchains, smart encryption and validation are utilised in NFTs to manage security and identity. Although blockchain technology appears to be reliable, many individuals are unfamiliar with the industry.

The encryption and validation mechanism used by NFTs is unparalleled. Each unit includes a digital signature that prohibits it from being replicated. Such innovations are raising the standard for the statistics industry as it is focused on database security. Furthermore, NFTs also control others from stealing other people's artwork.

4.2 Secure Storage

The immutability of blockchain technology ensures that data can't be modified or destroyed once it's been recorded. Blockchain technology's unique features make it an ideal platform for NFTs. Due to its decentralised nature, blockchain is resistant to hacking and exploitation. Because of the authenticity and immutability of blockchain technology, storing NFTs on it is a preferred solution.

Furthermore, NFT projects on their underlying public ledgers are essentially decentralised applications. The following are some of the most important characteristics [4]:

- **Verifiability** - The ownership of the NFT, as well as its token metadata, may be verified publicly.
- **Transparency** - The operations of NFTs, such as minting, selling, and buying, are all available to the public.

- **Tamper-resistance** - After the transactions are acknowledged as confirmed, the NFT metadata and trading records are constantly preserved and cannot be changed.
- **Atomicity** - A single atomic, consistent, isolated, and durable (ACID) transaction can be used to exchange NFTs. The NFTs can all be in the same execution state simultaneously.

5 Cybersecurity Risks

Governments, corporations, and individuals all have a compelling need for cybersecurity, which is exacerbated by the rapid technological innovations and ever-changing cyber threat landscape. Blockchain is a promising infrastructure technology that has the potential to be used in a variety of cybersecurity applications. Decentralisation, verifiability, and immutability are characteristics that can help achieve data authenticity, reliability, and integrity [41].

Many risks come with having a variety of opportunities. The absence of time and conditions that enable stress testing the limits of any new applications is inherent in any technology breakthrough.

5.1 Security Evaluation using STRIDE

A blockchain, storage, and web application are all part of an NFT system. The NFT system's security evaluation is complicated since any component might act as an attacking interface, making the entire system vulnerable to an adversary. As a result, Threat Modelling should be at the core of the Security Development Lifecycle (SDL), as it facilitates software architects to detect and mitigate possible security vulnerabilities early on when they are relatively simpler and cost-effective to handle [43].

Therefore, we use the STRIDE threat and risk assessment model, which addresses all facets of a system's security, including authenticity, integrity, non-repudiability, availability, and access control [4]. Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of Service, and Elevation of privileges are all part of the STRIDE. Loren Kohnfelder and Praerit Garg, two Microsoft engineers, created STRIDE in the late 1990s. STRIDE's objective is to develop a system that meets the CIA's triad (confidentiality, integrity, and availability) [44].

Table 1: STRIDE Model Overview

Category	Description
Spoofing (Authenticity)	It entails gaining unauthorised access to a system and then impersonating another entity using another user's user credentials
Tampering (Integrity)	Illegal data modification, like unauthorised alterations to

	persistent data that compromises data integrity
Repudiation (Non-repudiation)	The security property of non-repudiability, or a system's ability to fight repudiation threats, is related to the scenario where the author of a statement cannot refute it. For instance, a user who buys an item may be required to sign for it upon receipt. The supplier can then use the acknowledged receipt as proof that the package was received by the user
Information Disclosure (Confidentiality)	Information is exposed to unauthorised users, which is a breach of confidentiality
Denial of Service (Availability)	A Denial of Service (DoS) attack is a kind of network attack where the attacker attempts to make a service inaccessible to its users by disrupting its normal operations. To improve system availability and reliability, one must defend against DoS threats
Elevation of privileges (Authorisation)	An unprivileged user acquires privileged access and thus has the accessibility to infiltrate or damage the entire system. Threats of elevation of privilege include instances where an attacker has successfully infiltrated all system defences and has become a part of the trusted system itself, which is a very risky circumstance

Table 2: Security Evaluation of NFTs using STRIDE

STRIDE	Threat Definition	Mitigation Approach
Spoofing	• A malicious attacker could take advantage of authentication vulnerabilities while minting or selling NFTs • Compromising the user's private key to fraudulently transfer ownership of NFTs	• A comprehensive verification of the smart contract • To mitigate private key leakage, use a cold storage hardware wallet to store your digital assets
Tampering	• Illegal alteration of NFT data, that compromises its integrity. Although following a successful transaction, the metadata and ownership of NFTs cannot be illicitly altered. Nevertheless, data held outside of the blockchain can still be	• When trading NFTs, provide both the hash data and the actual data to the NFT buyer

	tampered with	
Repudiation	• An attacker might tamper with the hash data, or the hash data could link with the attacker's address	• Implementing a multi-signature contract can help to alleviate this problem partially because each binding should be confirmed by more than one person
Information Disclosure	• The state information, along with any state changes, and instruction code in smart contracts are fully transparent in the NFT system since they are publicly accessible to an observer. As a result, a malicious attacker can simply link a certain NFT buyer or seller using the hash and transaction	• To safeguard the user's privacy, NFT developers should employ privacy-preserving smart contracts rather than conventional smart contracts
Denial of Service (DOS)	• The availability of the NFT service is violated by DoS attacks, which can be exploited by cybercriminals	• The use of a hybrid blockchain architecture with a weak consensus algorithm [13] could help in mitigating this issue. Since the consensus process is an essential part of distributed systems, it provides a powerful way to reach an agreement on the network's current state
Elevation of privileges	• A poorly written smart contract may cause NFTs to lose their selling permissions	• Smart contracts should be subjected to formal verification

5.2 How can enterprises defend against Cyber-Threats on NFTs?

At a larger scale, most NFTs are connected to the Ethereum network. Apart from the expensive cost of many of these tokens, there is also the issue of cybersecurity threats to consider. Since

most blockchain records are not even large enough to hold an entirely digital image file, NFTs leverage a blockchain-encrypted web address to establish connections to NFT assets. This indicates that NFT buyers would not receive any blockchain-based tokens in exchange for the thing they are buying. They receive access to links on public websites that allow enterprises to verify the token's legitimacy. The value of NFTs might vanish overnight if these enterprises are out of business or if their sites are compromised.

Even more alarming is the fact that when marketplaces broaden and NFT prices stabilise, this risk will only grow. There is a lack of comprehensive regulation in this field. That implies that companies may find it nearly impossible to assure exploit-based data is not sold to the highest bidder and used to breach their networks. As a result, companies must manage these tokens as their security systems evolve. In reality, NFT defence can be established by incorporating the following [2]:

5.2.1 Zero-Trust Frameworks

The Zero-Trust architecture is an effective technique of preventing unauthorised users from gaining access to a blockchain credential. An advanced zero trust security strategy can help enterprises manage the risks of a disconnected business environment by giving users appropriate access to the resources they need while diminishing the likelihood of asset loss. Instead of assuming an identity, the focus is on verifying identity. It's a framework and strategy for securely connecting the authorised users to the appropriate information at the right moment and under the right set of circumstances, all while protecting your company from cyber threats.

5.2.2 Asset Monitoring

Because cyberattacks like distributed denial of service, ransomware, and phishing often target NFT marketplaces. As a result, IT teams must constantly monitor assets to respond to prospective cyberattacks. Furthermore, proactive monitoring of valuable intellectual property stored on networks is essential. In this way, one can restrict adversaries from stealing it and altering NFTs without the company's knowledge.

5.2.3 Network Monitoring

Enterprises should also establish enhanced network monitoring tools designed to detect potential exfiltration vulnerabilities such as pilfering wallet content [106][107] before the attacker gains access to the blockchain. This could be implemented, by expanding beyond simple access and verification tools to active behavioural monitoring and analysis technologies, such as integrating machine learning models and behavioural rules to add more context to the network, log, and vulnerabilities, perpetrators may be detected more promptly and precisely. Organisations can proactively suspend potentially risky sessions in this manner, preventing unauthorised users from gaining access to NFT data.

5.3 Challenges in the NFT Landscape

This section covers both system-level concerns created by blockchain-based platforms and social aspects such as governments, regulation, and society, as well as some prevalent challenges from the standpoint of functionality, reliability, governance, and scalability.

Slow Confirmation: For efficient and secure management, NFT-related procedures are often carried out by transmitting transactions through the smart contract (such as mint, sell, exchange). Current NFT systems, on the other hand, are closely linked with their underlying blockchain networks, resulting in severely slow NFT confirmation. To address this issue, blockchain systems must be redesigned [45], their structure should be optimised [46][47], and the consensus mechanisms need to be improved [48]. Existing blockchain technologies are unable to meet these requirements.

High gas prices: High gas prices seem to be a serious issue for NFT exchanges, particularly when minting NFTs on a large scale, which involves uploading metadata to the blockchain network. Because smart contracts require computation power and storage to be handled, every NFT-related transaction is more expensive than a basic transfer transaction. Its widespread adoption is hindered by expensive fees originating from complex processes and excessive congestion.

Anonymity: The anonymity and security of NFTs are still understudied at this time. The Ethereum network, which underpins most NFT transactions, only offers pseudo-anonymity rather than absolute anonymity or privacy. Users can hide their identities to some extent if the public is unaware of the connections between their true identities and corresponding addresses. Due to their sophisticated cryptographic primitives and security assumptions, current privacy-preserving approaches such as homomorphic encryption [49], zero-knowledge proof [50], ring signature [51], multi-party computation [52] haven't been utilised to NFT-related schemes.

Governance Consideration: NFTs encounter obstacles from the government, such as Legal Pitfalls and Taxable Property Issues. NFTs are confronted with legal and regulatory challenges in a wide range of circumstances [53][54]. Commodities, cross-border transactions, sensitive information, and so on are many potentially impacted domains. Before diving into the NFT tracks, it's essential to understand the regulatory scrutiny and legal challenges that come with them. The regulatory environment for cryptocurrencies, as well as NFT sales, is strict in several countries, such as India and China. As a result, conducting thorough research before investing major tokens in NFTs is a must.

NFT Interoperability: Current NFT ecosystems are disconnected. Users can only transact inside the same ecosystem once they've chosen a specific product. This is because of the blockchain infrastructure that underpins it. Interoperability and cross-chain communication are always stumbling blocks to DApp adoption. Only with the cooperation of external trusted parties can cross-chain communications be established. Fortunately, Ethereum is the underlying platform for the majority of NFT-related projects. This implies they have identical data structures and can communicate using the same conventions.

6 NFT Regulation

NFTs have given the crypto-verse a significant amount of monetization potential and enabled creators to collect revenue for their efforts. Nevertheless, they have been receiving a lot of criticism recently as lawmakers consider their regulations. Globally, major jurisdictions are struggling to regulate NFTs. For instance, the Financial Action Task Force (FATF) recommendations necessitate countries to execute measures and controls to counteract money laundering and terrorist financing, as well as the European Commission's recently published Regulation of Markets in Crypto-assets (MiCA) proposal, an EU-wide regulatory initiative aimed at regulating crypto-asset issuers and crypto-asset service providers (CASPS). These regulatory developments, together with the growing involvement of institutional players, indicate how mainstream the crypto-industry will evolve [112].

The need for an overarching regulatory framework is indeed greater than ever before, considering the decentralised nature of blockchain technology as well as the borderless nature of how its services might be delivered. The following aspects would need to be considered in the development of such legislation:

- ➔ Conflict settlement and legal enforceability.
- ➔ Privacy concerns, particularly under the GDPR (General Data Protection Regulation) framework in the EU.
- ➔ Consumer, or end-user, protection.
- ➔ AML (Anti-Money Laundering), CFT (Countering the Financing of Terrorism), and KYC (Know Your Customer) considerations.

Due to the existing shortcomings of AML and KYC checks conducted by DeFi platforms, DeFi projects have the potential to be utilised for money laundering. Furthermore, technological advancements in the field of digital art may pose money laundering risks. Since, NFTs have been used to codify the ownership of a unique digital asset, such as a work of high-value digital art, and are maintained through smart contracts and digital wallets. Because it is derived cryptographically, an NFT transaction is publicly verifiable, auditable, and digitally unique.

Criminals can utilise NFTs to conduct self-laundering by purchasing one with illicit funds and then transacting amongst themselves to establish sales records on the blockchain [113]. The NFT might then be sold to an unsuspecting person who would compensate the perpetrator with funds that were not linked to a previous crime. Direct peer-to-peer transactions with NFT-secured artwork without the use of an intermediary are also possible. These digital artworks are intrinsically simpler to transfer amongst transacting parties than conventional art due to the capacity of NFTs to transmit via the internet without any concern regarding physical location and across borders nearly instantaneously rendering digital art vulnerable to exploitation by those

attempting to launder the illicit proceeds. After all, value can be moved without encountering the financial, regulatory, or investigative costs associated with the physical shipment.

Over the years, the U.S. congressional committees and government agencies in the United States have questioned what digital assets meant for the global and domestic economy [114]. Concerns have been raised about the government's ability to regulate such assets. NFTs are difficult to pinpoint from a regulatory standpoint. Fungible tokens can represent a wide range of rights and obligations and are often classified into three distinct legal categories (security, currency, and utility) like NFTs. In terms of functionality, NFTs have the potential to tread substantially further than fungible tokens. They can serve a variety of purposes, including security and IP rights.

Governments have attempted to directly address the NFT regulation dilemma by breaking down NFTs into various functional categories, much like fungible tokens. Electronic money, financial instruments, and collective investment instruments, for instance, are NFTs categorised in Luxembourg. However, NFTs can theoretically perform a wide range of other functions, making understanding how to value revenues earned from them nuanced. This is why the frameworks incorporated into NFT marketplaces, as well as the self-regulation initiatives, are so important. Platforms and developers of NFTs must have a responsibility to define the NFTs very clearly once they've been minted, as this will be important to the development of marketplace frameworks.

7 Use Cases of NFTs

The innovation of NFTs has resulted in crypto art and digital collectables, but it does not end there. NFTs can be used to determine the authenticity of several unique and special goods, from logistics to real estate. Although this NFT ecosystem is still in its early stages, there are several impactful projects to investigate, and a few of them are already delivering substantial value to consumers and creators.

This section presents the benefits of NFTs and will also explore the common fields that may benefit from them.

Gaming Industry: NFT has huge potential in the gaming community. CrytpoKitties [15], Cryptocats [55], CryptoPunks [14], Meebits [56], and Axie Infinity [57] are a few of the existing crypto games. The special rewards entice many investors to participate in the games, driving NFTs to prominence. The NFT also offers ownership records for items in games and endorses economic marking in the ecosystem, which benefits both devs and gamers. Particularly, game developers, that are NFT publishers of the attributes (such as weapons and skins), can earn royalties every time their attributes are sold online on the marketplace. Gamers can obtain exclusive game items that are only available to them. This will result in a mutually profitable framework in which both gamers and devs benefit from the NFT marketplace [4].

Flourishing Virtual Events: Conventional virtual events conducted online depend on credibility and technologies provided by centralised companies. Though blockchain has taken over numerous types of activities such as raising funds via ICOs, IFOs, and IEOs, its applicability is currently limited to a small number of events. The inherent characteristics of NFTs, such as uniqueness, ownership, and liquidity, dramatically expand the spectrum of blockchain applications. This allows each person to connect to a particular event, almost like the patterns we see in our daily lives.

NFTs can be linked with event tickets to enable access to an event. These tickets can give proof of authenticity, royalties from secondary sales, and even repurpose digital tickets into one-of-a-kind special edition souvenirs [58]. This could be better understood with the example of the ticketing event. Consumers should trust a third party when purchasing tickets in a conventional event ticket market. Consequently, acquiring counterfeit or illicit tickets is a possibility. In severe cases, the very same ticket may be resold several times or acquired by extraction from ticket photos uploaded online. The term "NFT-based ticket" refers to a ticket generated by the blockchain to show eligibility to any event, such as entertainment or sports. It is unique and scarce, which means the ticket holder cannot resell it once it has been purchased. For key stakeholders such as the event manager and the customer, the blockchain-based smart contract enables a transparent ticket trading mechanism. Rather than relying on third parties, customers can purchase and sell crypto tickets directly from the smart contract [4].

Physical items: Physical item tokenization isn't as advanced as it is for digital assets. The use of NFTs to link real-world assets can aid to digitise the process of proving ownership. Numerous projects are exploring the tokenization of real estate, rare fashion items, and other things. Since NFTs are fundamentally deeds, someday we'll be able to purchase a car or a property with Ethereum and obtain the deed in the form of an NFT. It's not difficult to envisage a world where your Ethereum wallet serves as the key to your car or home whilst technology advances. You can utilise NFTs as collateral in decentralised loans [59] since valuable assets like automobiles and real estate can be represented on Ethereum.

It's also essential to note that linking a physical object to an NFT should make it simpler to legally transfer that physical item while operating within its legal and regulatory frameworks.

Consider the example of using NFTs in real estate [108]. One of the downsides of real estate investing is the hassle of transferring property ownership. Currently, purchasing a property or acquiring an equity line of credit entails a significant amount of paperwork. The transaction process is enhanced using an NFT, allowing a buyer to take ownership of a particular property in minutes. Since cyber fraud is prevalent in digital transactions, one may attain higher levels of security and data integrity by using blockchain and NFT technology. This safeguards both sellers and buyers making asset transfers considerably more straightforward.

The first stage in selling real estate as an NFT is to undertake the appropriate legal preparations to ascertain that it adheres to regulations. This necessitates the involvement of legal counsel with blockchain experience. Maintaining compliance with the law is often a priority, but with the advent of new technologies, it becomes more challenging. You can enter the NFT into an NFT

marketplace to sell it to potential buyers once you've completed all the appropriate paperwork, disclosures, and reports to give it the legal power to represent proof of ownership. Buyers will place bids on the property, and the auction winner will pay in fiat money or cryptocurrency.

Propy [110], a company backed by Silicon Valley leading figures and the National Association of Realtors, is now transforming the real estate sector by employing smart contracts to automate the sales process. Propy recently introduced real estate-backed NFTs in the United States [109] by developing the technological and legal framework for turning real estate properties into NFTs. Propy claims that the transaction is stored on the immutable blockchain and that legal documents proving ownership are accessible. Propy intends to expand this service globally, providing a unified framework for real estate purchases based on blockchain technology. Currently, if the sale is successful, the buyers will receive a Florida-based investment property, as well as ownership rights to a US-based entity that owns the property. It is not fractional ownership, but rather a DeFi asset that may be borrowed against.

Genomics: Genomics [60][61] is an area in genetics that deals with the sequencing and examination of a genome. It is a field of biology that emphasises the structure, operation, development, characterization, and modification of genomes. A genome represents a complete set of DNAs that includes all of an organism's genes. Given the extremely sensitive nature and uniqueness of genetic data, it's imperative to maintain the protection of privacy by employing sophisticated systems with layers of genetic information that necessitate both regulatory and logical privacy protection. The interpretation, structure, and application of genetic data are all appropriate and analogous to the uniqueness of a non-fungible token.

On and off the blockchain, the NFT design is particularly beneficial for maintaining the ownership rights of highly unique and valuable assets. As a result, adopting NFTs could help make genomic data accessible outside the ongoing integration and across multiple contexts whilst also allowing for robust governance and management by the genetic data proprietor or authorised guardian [42].

Artwork: Since a digital replica of digital artworks can be generated, non-fungible tokens have helped to overcome long-standing challenges in maintaining scarcity in digital art. Although there is counterfeit art in the world today, we can usually authenticate it. The bulk of the value of crypto art comes from digitally validating its legitimacy and ownership. The valuation of NFTs isn't always determined by the artwork that is linked to them. Often, demonstrating ownership of a particular asset is more essential. Crypto art is one of the most popular NFT applications because of this functionality [62]. Creators of NFTs might also issue "shares" for their work. This encourages followers and investors to own a piece of an NFT without having to buy the whole thing. This continues to expand the opportunities available for both NFT minters and collectors. Holding a fraction of an NFT will probably entitle you to engage in a decentralised autonomous organisation (DAO) for asset management in the near future [29].

Finance: It's common to overlook the fact that not every NFT is based on music, painting, or collectable items. NFTs also deliver distinct financial benefits in decentralised finance (DeFi)[63]. Many will still have some artwork as well, but their significance is determined by their utility.

JustLiquidity, for instance, has an NFT staking model [64]. A user can stake a pair of tokens in a pool for a set period in exchange for an NFT that allows them to join the next pool. When you engage in the new pool, the NFT works as an entry ticket and is destroyed once you enter the pool. Based on the access they offer, this model generates a secondary market for these NFTs [62].

Furthermore, smart contracts are also well-suited to business models like online insurance, peer-to-peer lending (P2P lending), and equity crowdfunding. The agility feature of smart contracts can substantially decrease transaction costs and enhance efficiency, thereby avoiding onerous clearing and delivery [65][66]. Whereas, conventional financial trading requires coordination by central agencies.

Internet of Things (IoT): The traceability of data and operations created and performed by IoT devices is one of the most attractive features of blockchain technologies for an IoT ecosystem. To govern IoT devices as distinct and immutable, Non-Fungible Tokens (NFTs) built on the ERC-721 standard can be employed. However, the development of this use case is still novel [67]. Smart contracts, as well as IoT, can not only enhance information sharing between devices easier, but they can also help individuals automate time-consuming operations in a cryptographically secure way [68][69].

An NFT might verify to a smart contract that you are in a certain location at a specific moment, which could be suitable for practical trackers. A smart contract could then trigger something in the digital world to happen. This is similar to minting an NFT that relies on real-world data as proof.

IoTeX [104] is a company dedicated to securing the Internet of Things. IoTeX is kicking things off with "proof of presence" based on reliable data from the Pebble Tracker. Pebble Tracker allows blockchain and IoT developers to interact with real-world data. Using a built-in secure element akin to those used in smartphones for FaceID and crypto wallets, the Pebble Tracker device can monitor and cryptographically sign real-world data like location, light, climate, and motion [105].

Logistics and Supply-Chain: The immutability and transparency features of blockchain technology guarantee that the supply chain information is accurate and secure making it beneficial for the logistics industry. It's essential to know where food, commodities, and other perishable things have been along with the duration. The Decentralised Blockchain Technology can be designed to generate immutable smart contracts using NFTs. An NFT even has the advantage of being able to identify unique products. We can trace a product with meta-data on its sources, journey, and warehousing location using an NFT.

There are numerous prospective possibilities for incorporating NFTs into the supply chain. Most of them, on the other hand, necessitates the usage of the same infrastructure at each point of the supply chain. With so many diverse stakeholders involved on a global scale, implementing these solutions into operation can be challenging. This aspect has resulted in only a faint number of real-world applications.

IBM's Foot Trust and MAERSK's TradeLens system are two big blockchain logistics services currently available. Both rely on Hyperledger Fabric, an IBM blockchain that permits NFTs to be utilised. However, whether NFTs play a significant role in their activities is uncertain [62].

8 NFTs solutions among Different Industries

8.1 Hyperledger Fabric

The Linux Foundation's open-source project [70], Hyperledger Fabric, is a de facto standard and a modular blockchain framework for professional blockchain platforms. Hyperledger Fabric is designed to serve as a basis for building modular applications and services. Plug-and-play components, like consensus and membership services, are possible with Hyperledger Fabric. Its modular and flexible architecture caters to a wide range of industry applications. Hyperledger Technologies is used by many NFT use cases, including finance, banking, supply-chain management, cybersecurity, manufacturing, healthcare, and so on, to develop standardised, enterprise-grade blockchain systems and codebases that offer genuine industry results [71].

It offers a powerful technique to reach a consensus that allows for scalability while maintaining privacy and performance. It features sophisticated privacy controls, ensuring that only the data you want to be shared is shared with the "permissioned" (known) participants in the network. This means that rather than an unrestricted network of anonymous participants, we can develop decentralised faith in a network of known participants. This enables enterprises to make appropriate decisions more quickly, saving time, capital, and risk [72].

Security, usability, robustness, performance, and feature set have all been consistently improved by the Hyperledger Fabric community, all of which are crucial to enterprise clients. There are currently no other distributed ledger technology frameworks that have widespread adoption among the leading cloud service providers such as AWS, Google, Azure, Oracle, and IBM [73].

Furthermore, Hyperledger technologies, specifically Hyperledger Fabric [75], continues to be the norm for the organisations on the Forbes list, 2022 Blockchain 50 [74], that have incorporated blockchain technology as a fundamental basis of their company operations. Hyperledger technologies have been used by at least 13 of the companies on this list to build their strategic networks, greatly surpassing any other technology or system used in these sorts of deployments. Companies on the list also mention Hyperledger Besu [76], Hyperledger Indy [77], and Hyperledger Cactus [78], indicating the value of the Hyperledger Foundation's multi-project strategy [79].

8.1.1 IBM and Hyperledger Fabric

In 2021, IBM has open-sourced a major portion of Hyperledger Fabric Tokens along with other distributed ledger code to encourage the implementation of the prominent open-source enterprise blockchain. The company contributed the original code and is still a significant

maintainer of Hyperledger Fabric. Tokens are used in a large variety of blockchain applications [80], which Fabric does not support natively [81]. IBM Research recently designed and developed two blockchain components termed Fabric Smart Client and Fabric Token SDK [82] to enable token exchange in an enterprise context. Furthermore, the IBM Blockchain Platform Console, a previously licenced technology that makes it easier to manage a blockchain network, has also been open-sourced.

IBM advises firms against solely relying on open source to establish a production blockchain system. Commercial distributions with tools and support are available from IBM and other companies. The IBM Blockchain Platform [83] is IBM's commercial Hyperledger Fabric distribution, which offers comprehensive 24x7x365 support and service level agreements (SLAs) for the open-source solution. It features the most powerful set of productivity tools to develop, govern, and manage any blockchain solution.

One of the current token exchange systems' shortcomings is the inability of privacy protection beyond rudimentary pseudonymization [84]. Transactions in Bitcoin, for instance, are pseudonymous and disclose the amount of Bitcoin exchanged. This makes them traceable and linkable, posing vulnerabilities that would be extremely risky in other environments like enterprise networks, supply chains, or finance. The Fabric Token SDK, on the other hand, uses a modular, privacy-preserving mechanism for exchanging assets in a permissioned blockchain system, with fine-grained auditing support. This indicates that the token management system now has a privacy level that may be configured.

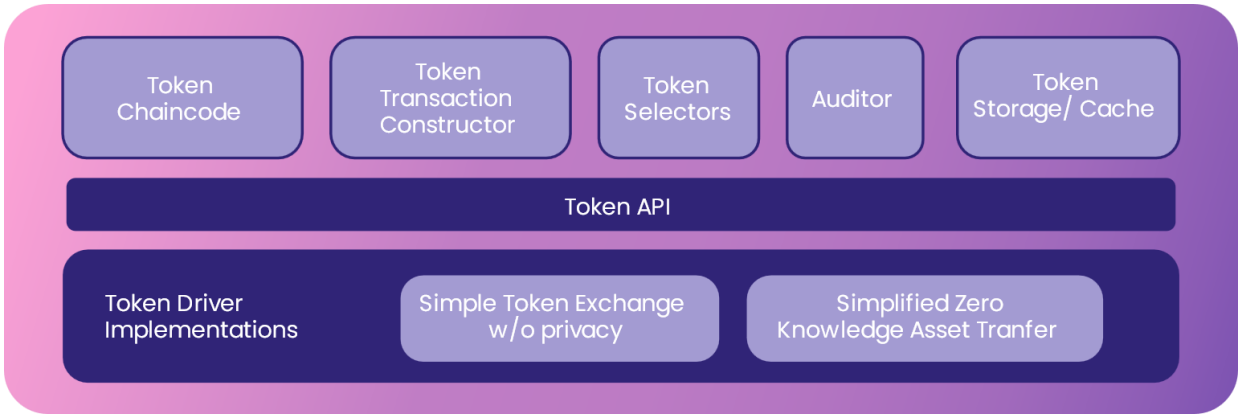


Figure-3: Modular Fabric Token SDK Architecture
(Source: "Making fungible tokens and NFTs safer to use for enterprises (2021)":
https://www.ibm.com/blogs/blockchain/2021/06/making-fungible-tokens-and-nfts-safer-to-use-for-enterprises/)

The Fabric Token SDK architecture is illustrated in **Figure-3**. The Token API, an API-based model of token exchange processes, is at the core of the Fabric Token SDK architecture. These APIs, in particular, assume that you have access to a ledger and can help you build and validate token redemption, transfer, issuance, and swap requests. The Token API can be set up to operate with one or more drivers that implement certain operations with varying levels of privacy, scalability, and performance. The framework also permits for the configuration of an authorised auditor who

has unrestricted access to the system's asset-exchange events. These features are essential for a token management system that maintains governance, user privacy protection, and regulatory compliance.

Fabric clients can use the Token API's set of Fabric-specific components to choose the ideal tokens to spend (token selectors), build token exchange requests (Token Transaction Constructor), keep track of owned tokens (Token Cache), begin Fabric smart contracts to validate them (Token Chaincode), and allow auditors to perform audit functions (Token Auditor).

8.2 Tokenization of Intellectual property by IBM and IPwe

IBM and IPwe [85] are collaborating to streamline corporate patents by developing a tokenization ecosystem that will enable an intellectual property to be considered as a business asset. The tokenization of intellectual property (IP) will make it easier to sell, trade, commercialise, or otherwise monetise patents, as well as provide fresh liquidity to investors and innovators [86].

While NFTs have traditionally been used to represent digital art, collectables, and even notable Tweets, the early use of IP-based NFTs could signal a shift in how inventors and corporations handle IP. Tokenization increases transparency while also making associated transactions smoother and less expensive. This is envisioned to impact not only major corporations with an extensive amount of intellectual property but also small and medium-sized enterprises (SMEs) and even individual IP owners. Patents as digital assets are particularly useful for SMEs since they allow IP to be leveraged as collateral or evidence of an organisation's value, as well as being more quickly utilised when seeking funding.

The IPwe Platform, which is maintained on IBM Cloud [87] and supported by IBM Blockchain [88], will store and share these NFTs. The IPwe Platform also drives the Global Patent Marketplace, which enables patent owners and other stakeholders to transact, buy, sell, licence, research, finance, and commercialise their patents. IPwe was the first one to develop a patent marketplace on the blockchain, partnering with IBM. The development of NFTs will only serve to expedite the possibility for IP to be considered as a liquid asset, which has normally been infamously challenging to manage, value, and transact.

For more than 3 years, IBM and IPwe have joined forces on the IPwe Platform, utilising IBM's extensive expertise in distributed ledgers and artificial intelligence to help preserve ownership information, create patent and asset allocation analytics, execute transactions, and advance the next intelligent generation of intellectual property (IP) pooling, which is a contract between numerous patent owners to collectively licence their IP.

8.3 Visa

Visa is a reliable network and a prominent financial services corporation in digital payments, with products or services available on cards, laptops, tablets, mobile devices, and others in over 200 countries across the world. Visa believes that non-fungible tokens (NFTs) will play an essential role in shaping the future of commerce, social networking, entertainment, and finance as cryptocurrencies and non-fungible tokens (NFTs) gain momentum and generate headlines. NFTs

have the potential to be a valuable catalyst for the creator economy, lowering the entrance barrier for individual creatives looking to make a living via digital commerce [89].

8.3.1 Focus Areas in Crypto and NFTs

Small and medium-sized businesses (SMBs) could benefit greatly from NFTs. SMBs may now sell online and attract customers all over the world due to the advent of e-commerce. NFTs let small enterprises utilise public blockchains to create digital commodities that can be transferred to a crypto wallet instantaneously. Visa intends to harness its expertise in facilitating smooth and secure digital transactions to enable NFT-commerce available and usable for sellers and buyers [89].

In this section, we'll go through Visa's key areas of focus in the crypto and NFT space.

Accessibility of Digital Currency: Visa is collaborating with 50 of the most mainstream cryptocurrency exchanges to make it smooth and straightforward to convert and spend cryptocurrency with a Visa card from any of the 70 million Visa-accepting merchants throughout the world. Although crypto platforms and wallets were once just used to store cryptocurrencies, they are now also being used to store NFTs. As new crypto wallets and platforms emerge, having access to multiple wallets will become particularly crucial. Since having a single universal crypto wallet is improbable, crypto platforms will need to provide customers with a range of options when connecting their wallets. Visa can expand its ecosystem of crypto wallets and is well-positioned to facilitate this accessibility and flexibility [58] due to its collaboration with Anchorage Digital [90].

Blockchain Research: Visa is responsible for guiding and advancing ideas that influence commerce, especially in cryptocurrencies and the NFT space. Visa's research team has been evaluating blockchain technology for some years, and their findings have resulted in several interesting advancements. These include novel methods of privacy-preserving cryptography and techniques to implement new kinds of crypto commerce securely and efficiently, like offline digital currency transactions. Furthermore, Visa is working to make it possible for consumers to buy digital assets using the techniques they are already familiar with, like cards as well as the Visa network [58].

Secure Flow of Digital Currency: Visa is expanding into a network of networks that facilitates the secure transfer of funds across a wide range of payment processes. For instance, Visa is assisting international marketplaces in identifying Visa Crypto Partner Wallets which are capable of safely receiving US Dollar Coin (USDC) payouts, allowing those marketplaces to pay their vendors in another country. The objective is that these vendors will have more alternatives and will be able to convert and spend their earnings at any Visa-accepting merchant using their visa credentials within their digital currency wallet.

Furthermore, Visa is also strengthening its infrastructure to support the settlement of stablecoins, a type of digital currency, starting with USDC on the Ethereum network. Visa seeks to extend the boundaries of its network, making it easily accessible to the rising ecosystem of

crypto-native enterprises and connecting to blockchain networks such as Ethereum, which serves as a hub for crypto services and commerce [58].

Digital Currency Innovation Hub: Visa has launched an international innovation hub wherein like-minded parties involved can cooperate on cryptocurrency and blockchain technologies. Partners obtain access to industry insights and cooperate carefully with Visa's Product, Visa Consulting & Analytics, and Innovation Centre industry experts to uncover digital currency trends and opportunities, as well as design and test ideas for new cryptocurrency technologies [58].

Visa Crypto APIs: Visa is supporting banking institutions and fintech companies lacking a digital currency service who would like to build one, by providing Crypto APIs to buy and sell cryptocurrency through digital banking applications. Visa now allows the purchase of Bitcoin, however, this infrastructure could pave the way for a wider range of assets, such as NFTs [58].

9 References

[1] What is a Non-Fungible Token (NFT)?: https://support.opensea.io/hc/en-us/articles/360063450733-What-is-a-Non-Fungible-Token-NFT-

[2] Token Resistance: Tackling the New NFT Threat Landscape (2021): https://securityintelligence.com/articles/new-threat-landscape-nfts/

[3] Blockchain, NFTs and the New Standard for Identity and Security (2022): https://www.entrepreneur.com/article/403417

[4] Qin Wang, Rujia Li, Qi Wang, Shiping Chen, "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges," arXiv:2105.07447 [cs.CR] (2021)

[5] Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol with chains of variable difficulty. In: CRYPTO. pp. 291–323. Springer (2017)

[6] Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. In: Concurrency: the Works of Leslie Lamport, pp. 203–226 (2019)

[7] Wood, G., et al.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper 151(2014), 1–32 (2014)

[8] Flow Blockchain: https://www.onflow.org

[9] By William Quigley, CEO, WAX | Jonathan Yantis, COO, WAX | Lukas Sliwka, CTO, WAX | Malcolm CasSelle, Strategic Advisor, WAX, “WAX Protocol White Paper” https://github.com/worldwide-asset-exchange/whitepaper (2019)

[10] Hong, S., Noh, Y., Park, C.: Design of extensible non-fungible token model in hyperledger fabric. In: Proceedings of the 3rd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. pp. 1–2 (2019)

[11] Bal, M., Ner, C.: Nftracer: a non-fungible token tracking proof-of-concept using hyperledger fabric. arXiv preprint arXiv:1905.04795 (2019)

[12] Fast box: https://www.fastbox.org/#GetStarted

[13] Wang, Q., Li, R.: A weak consensus algorithm and its application to high-performance blockchain. In: IEEE INFOCOM 2021-IEEE Conference on Computer Communications (INFOCOM). IEEE (2021)

[14] Cryptopunks: https://www.larvalabs.com/cryptopunks
[15] Cryptokitties: https://www.cryptokitties.co
[16] NBA Top Shot: https://nbatopshot.com/
[17] Picasso punks: https://opensea.io/collection/picassopunks
[18] Hashmasks: https://www.thehashmasks.com/
[19] NFTs, explained (2021): https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq
[20] Ethereum Whitepaper (2014): https://ethereum.org/en/whitepaper/
[21] Token Standards: https://ethereum.org/en/developers/docs/standards/tokens/
[22] ERC-20 Token Standard: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
[23] ERC-721 Non-Fungible Token Standard: https://ethereum.org/en/developers/docs/standards/tokens/erc-721/
[24] ERC-1155 Multi-Token Standard: https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/
[25] ERC-1155: The Crypto Item Standard (2018): https://blog.enjincoin.io/erc-1155-the-crypto-item-standard-ac9cf1c5a226
[26] Cai, W., Wang, Z., et al.: Decentralized applications: The blockchain-empowered software system. IEEE Access 6, 53019–53033 (2018)
[27] Raval, S.: Decentralized applications: harnessing Bitcoin's blockchain technology. " O'Reilly Media, Inc." (2016)
[28] William, E., Dieter, S., Jacob, E., Nastassia, S.: Eip-721: Erc-721 non-fungible token standard (2018) : https://eips.ethereum.org/EIPS/eip-721
[29] Non-fungible tokens (NFT): https://ethereum.org/en/nft/
[30] DGoods: https://dgoods.org/
[31] Mythical Games: https://mythical.games/
[32] NFT Module: https://github.com/cosmos/cosmos-sdk/issues/4046
[33] Cosmos SDK: https://github.com/cosmos/cosmos-sdk
[34] WHAT IS ERC-721?: http://erc721.org
[35] The Non-Fungible Token Bible: Everything you need to know about NFTs (2020): https://opensea.io/blog/guides/non-fungible-tokens/
[36] Introducing eBay-style Auctions for Crypto Collectibles (2019): https://opensea.io/blog/announcements/introducing-ebay-style-auctions-for-crypto-collectibles/
[37] How to bid on crypto collectibles using OpenSea (2018): https://opensea.io/blog/tutorials/how-to-bid-on-crypto-collectibles/
[38] Introducing bundles (2018): https://opensea.io/blog/announcements/introducing-bundles/
[39] Buy and sell crypto collectibles with Dai (2018): https://opensea.io/blog/announcements/buy-and-sell-crypto-collectibles-with-dai/
[40] Buy and sell collectibles with MANA! (2018): https://opensea.io/blog/announcements/buy-and-sell-crypto-collectibles-with-mana/
[41] Reza M. Parizi, Ali Dehghantanha, Amin Azmoodeh, and Kim-Kwang Raymond Choo, "Blockchain in Cybersecurity Realm: An Overview." In: Blockchain Cybersecurity, Trust and Privacy pp 1-5 (2020): https://link-springer-com.libproxy.viko.lt/chapter/10.1007/978-3-030-38181-3_1

[42] Daniel Uribe and Gisele Waters, “Privacy Laws, Genomic Data and Non-Fungible Tokens,” The JBBA, the Journal of the British Blockchain Association (Peer Reviewed) (2020)
[43] Microsoft Threat Modeling Tool threats (2022): https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
[44] What is STRIDE and How Does It Anticipate Cyberattacks? (2021): https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/
[45] Wang, Q., Yu, J., Chen, S., Xiang, Y.: Sok: Diving into dag-based blockchain systems. arXiv preprint arXiv:2012.06128 (2020)
[46] Wang, G., et al.: Sok: Sharding on blockchain. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. pp. 41–61 (2019)
[47] Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., Gervais, A.: Sok: Layer-two blockchain protocols. In: International Conference on Financial Cryptography and Data Security. pp. 201–226. Springer (2020)
[48] Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., Danezis, G.: Sok: Consensus in the age of blockchains. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. pp. 183–198 (2019)
[49] Wang, Q., Qin, B., Hu, J., Xiao, F.: Preserving transaction privacy in bitcoin. Future Generation Computer Systems 107, 793–804 (2020)
[50] Wang, Y., Kogan, A.: Designing confidentiality-preserving blockchain-based transaction processing systems. International Journal of Accounting Information Systems 30, 1–18 (2018)
[51] Noether, S.: Ring signature confidential transactions for monero. IACR Cryptol. ePrint Arch. 2015, 1098 (2015)
[52] Raman, R.K., et al.: Trusted multi-party computation and verifiable simulations: A scalable blockchain approach. arXiv preprint arXiv:1809.08438 (2018)
[53] Fairfield, J.: Tokenized: The law of non-fungible tokens and unique digital property. Indiana Law Journal, Forthcoming (2021)
[54] Johnson, K.N.: Decentralized finance: Regulating cryptocurrency exchanges. William & Mary Law Review 62 (2021)
[55] Cryptocats: https://cryptocats.thetwentysix.io
[56] Meebits: https://meebits.larvalabs.com
[57] Axie Infinity: https://axieinfinity.com
[58] NFTs Engaging Today’s Fans in Crypto and Commerce, Visa NFT Whitepaper (2021): https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-nft-whitepaper.pdf
[59] Decentralized finance (DeFi): https://ethereum.org/en/defi/
[60] What is Genomics? (2020): https://www.azolifesciences.com/article/What-is-Genomics.aspx
[61] A reference standard for genome biology (2018).
[62] Top 7 NFT Use Cases (2021): https://academy.binance.com/en/articles/top-7-nft-use-cases
[63] The Complete Beginner's Guide to Decentralized Finance (DeFi) (2019): https://academy.binance.com/en/articles/the-complete-beginners-guide-to-decentralized-finance-defi
[64] What Is Staking? (2019): https://academy.binance.com/en/articles/what-is-staking

[65] I. Allison, “Game-changers FreeMyVunk and Digix allow video gamers to trade virtual assets for physical gold,” (2015): https://www.ibtimes.co.uk/game-changers-freemyvunk-digix-allow-video-gamers-trade-virtual-assets-physical-gold-1534436
[66] A. Mizrahi, “Everex helps migrant workers send remittance back to Myanmar via Ethereum,” (2016): https://www.financemagnates.com/cryptocurrency/education-centre/everex-helps-migrant-workers-send-remittance-back-to-myanmar-via-ethereum/
[67] Javier Arcenegui, Rosario Arjona, and Iluminada Baturone, "Secure Management of IoT Devices Based on Blockchain Non-fungible Tokens and Physical Unclonable Functions." In: Applied Cryptography and Network Security Workshops pp 24-40 (2020): https://link.springer.com/chapter/10.1007/978-3-030-61638-0_2
[68] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things, ” in IEEE Access, vol. 4, pp. 2292-2303, (2016)
[69] Shuai Wang, Yong Yuan (Corresponding author, Senior Member, IEEE), Xiao Wang, Juanjuan Li, Rui Qin, Fei-Yue Wang (Fellow, IEEE), “An Overview of Smart Contract: Architecture, Applications, and Future Trends,” 2018 IEEE Intelligent Vehicles Symposium (IV) Changshu, Suzhou, China (2018)
[70] Hyperledger Fabric Documentation: https://hyperledger-fabric.readthedocs.io/en/latest/
[71] Case Studies powered by Hyperledger technologies: https://www.hyperledger.org/learn/case-studies
[72] What is Hyperledger Fabric?: https://www.ibm.com/topics/hyperledger
[73] Open, Proven, Enterprise-grade DLT, Hyperledger Fabric Whitepaper (2020): https://www.ibm.com/downloads/cas/0XMOQJNP
[74] Forbes Blockchain 50 2022, “Cryptocurrencies hog the spotlight, but blockchain’s biggest innovations are below the surface, saving billions each year for the world’s largest companies” (2022) : https://www.forbes.com/sites/michaeldelcastillo/2022/02/08/forbes-blockchain-50-2022/?sh=3ffd8ce131c6
[75] Hyperledger Fabric: https://www.hyperledger.org/use/fabric
[76] Hyperledger Besu: https://www.hyperledger.org/use/besu
[77] Hyperledger Indy: https://www.hyperledger.org/use/hyperledger-indy
[78] Hyperledger Cactus: https://www.hyperledger.org/use/cactus
[79] Hyperledger Technologies Dominant for Enterprise Blockchain Deployments on 2022 Forbes Blockchain 50 (2022): https://www.hyperledger.org/blog/2022/02/09/hyperledger-technologies-dominant-for-enterprise-blockchain-deployments-on-2022-forbes-blockchain-50
[80] Blockchain tokenization in enterprises and beyond (2021): https://www.ibm.com/blogs/blockchain/2021/02/blockchain-tokenization-in-enterprises-and-beyond/
[81] IBM open sources Hyperledger Fabric Tokens, other blockchain code (2021): https://www.ledgerinsights.com/ibm-open-sources-hyperledger-fabric-tokens-other-blockchain-code/
[82] Making fungible tokens and NFTs safer to use for enterprises (2021): https://www.ibm.com/blogs/blockchain/2021/06/making-fungible-tokens-and-nfts-safer-to-use-for-enterprises/
[83] IBM Blockchain Platform: https://www.ibm.com/blockchain/platform
[84] What is Pseudonymization?: https://www.trendmicro.com/vinfo/us/security/definition/pseudonymization

[85] IPwe: https://ipwe.com
[86] IPwe and IBM Seek to Transform Corporate Patents With Next Generation NFTs Using IBM Blockchain (2021): https://newsroom.ibm.com/2021-04-20-IPwe-and-IBM-Seek-to-Transform-Corporate-Patents-With-Next-Generation-NFTs-Using-IBM-Blockchain
[87] IBM Cloud: https://www.ibm.com/cloud
[88] IBM Blockchain: https://www.ibm.com/blockchain
[89] VISA: NFTs mark a new chapter for digital commerce (2021): https://usa.visa.com/visa-everywhere/blog/bdp/2021/08/18/nfts-mark-a-1629328216374.html
[90] Anchorage Digital: https://www.anchorage.com
[91] Tezos: https://tezos.com
[92] Dapper Labs: https://www.dapperlabs.com
[93] Proof-of-Stake (POS): https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
[94] Proof-of-Work (POW): https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/
[95] Non Fungible Token (NFT) Standards: An Overview (2021): https://hackernoon.com/non-fungible-token-nft-standards-an-overview-w71y34y3
[96] How much energy does Flow use? (2021): https://flow.com/sustainability
[97] New findings from Deloitte Canada reveal minting an NFT on Flow takes less energy than a Google search or Instagram post (2022): https://www.onflow.org/post/flow-blockchain-sustainability-energy-deloitte-report-nft
[98] Bitcoin Energy Consumption Index: https://digiconomist.net/bitcoin-energy-consumption/
[99] Ethereum Energy Consumption Index: https://digiconomist.net/ethereum-energy-consumption/
[100] Solana's Energy Use Report (2021): https://solana.com/news/solana-energy-usage-report-november-2021
[101] Polygon: The Eco-Friendly Blockchain Scaling Ethereum (2021): https://blog.polygon.technology/polygon-the-eco-friendly-blockchain-scaling-ethereum-bbdd52201ad/
[102] Flow Primer: https://www.onflow.org/primer
[103] Non-Fungible Tokens on Tezos Using FA2: https://assets.tqtezos.com/docs/token-contracts/fa2/2-fa2-nft-tutorial
[104] IoTeX: https://iotex.io
[105] IoT Privacy Company IoTeX Is Envisioning the Future of NFTs (2021): https://www.coindesk.com/tech/2021/05/03/iot-privacy-company-iotex-is-envisioning-the-future-of-nfts/
[106] BitRAT Propagates via NFT Lures (2022): https://cyware.com/news/bitrat-propagates-via-nft-lures-357501e1
[107] BHUNT - New Password Stealer Aiming for Crypto Wallets (2022): https://cyware.com/news/bhunt-new-password-stealer-aiming-for-crypto-wallets-d11133d5
[108] NFTs And The Future Of Commercial Real Estate (2022): https://www.forbes.com/sites/forbesbusinesscouncil/2022/02/16/nfts-and-the-future-of-commercial-real-estate/
[109] Propy launches NFT platform in the US, allowing real-world property to be bought as an NFT (2022):

https://techcrunch.com/2022/01/27/propy-launches-nft-platform-in-the-us-allowing-real-world-property-to-be-bought-as-an-nft/
[110] Propy: https://propy.com/browse/
[111] Sandbox: https://www.sandbox.game/en/
[112] DeFi: Defining the future of finance | PwC (2021)
[113] Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art | The U.S. Treasury Department (2022)
[114] NFT Regulation Looms Large, So Let's Start With the Proper Framework | NASDAQ (2021): https://www.nasdaq.com/articles/nft-regulation-looms-large-so-lets-start-with-the-proper-framework