



Designation: D8558 – 24

Standard Guide for Verification of a Certificate of Authentication Used to Track Products through Their Supply Chain by Utilizing Blockchain Technology¹

This standard is issued under the fixed designation D8558; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This guide was written to introduce the concept of tracking physical and digital goods as well as crypto assets for transactions or marketing and branding purposes on a Web3 blockchain technology storage platform. This represents a significant shift in technology, where blockchain assets are available on a public digital ledger, open for all to view and verify. It marks a paradigm shift from the private cloud storage currently used in Web2 infrastructure platforms. This guide provides minimum requirements for the secure verification of a Certificate of Authentication (COA) used to track any product through their supply chain by utilizing Blockchain Technology. The implementation of blockchain technology can enhance the transparency, traceability, and trustworthiness of the supply chain, ensuring product quality and authenticity while reducing the potential for fraud, tampering, and other malicious activities. Each Certificate of Authenticity (COA) is minted on the blockchain, featuring a screenshot of the summary page on the front of a Non-Fungible Token (NFT) with the unique traits of that lab report tagged as metadata. Examples of this metadata include the name of the lab, the name of the client, the unique identifier of the sample tested, and the date the test was performed. To enhance the tracking and security of these COAs, various tracking devices can be linked to the COA on the blockchain, depending on the product's specific needs and the nature of the supply chain. These devices include RFID tags, QR codes, holograms, micro transponders, and embeddable watermarks. Each serves a unique purpose, from instant verification via QR codes to advanced security and tracking through RFID and micro transponders. Holograms and embeddable watermarks provide additional layers of security, making counterfeiting significantly more challenging and verifying authenticity more straightforward and reliable.

1.2 Certificates of Authenticity (COA's) should be verified by authorized parties in accordance with the applicable regu-

lations within the authority having jurisdiction. It is the requirement of each party to ensure compliance and legal authority for the verification process.

1.3 A verification plan, based on a risk assessment, should be in place and executed for tracking products using a Certificate of Authenticity on the blockchain. The verification plan should identify/address:

1.3.1 The assets and data to be protected and the identified threats to those assets and data during the phases of the supply chain process. An example of this is a lab report that copied onto the blockchain with the image of the summary page on the front of the Non Fungible Token (NFT).

1.4 The specific verification measures to be deployed in the COA tracking program commensurates with the value of the physical assets being tracked and are broken into three key areas. Physical security measures for a COA ensure that the hard copies of the certificate, as well as any samples or products associated with it, are stored safely and are protected from unauthorized access, tampering, or damage. Tracking devices used to track the physical products could include RFID, QR codes or micro transponders. Technical security measures for a COA revolve around protecting the The digital versions or electronic records of the certificate once it is minted onto the blockchain. Administrative security measures for a COA encompass policies, protocols, and practices to oversee its lifecycle, ensuring compliance, authenticity, and trust through regular audits, training, and defined responsibilities.

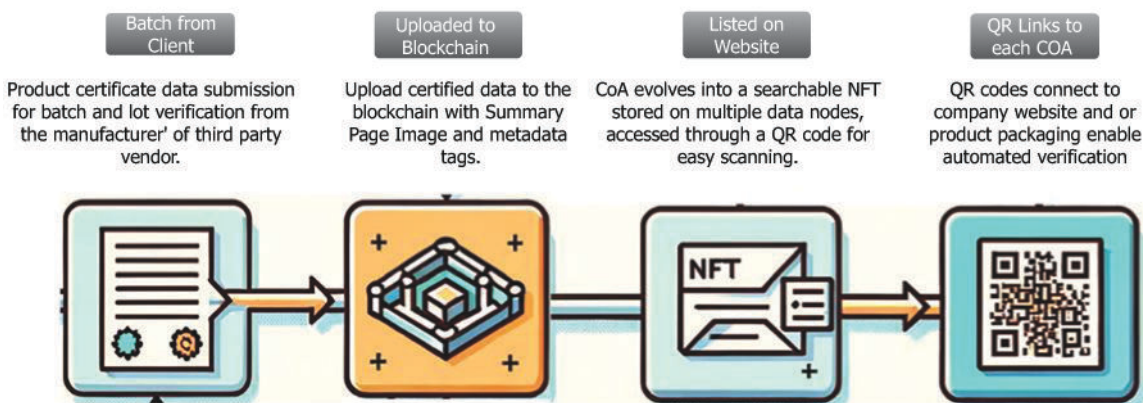
1.5 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.6 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

¹ This guide is under the jurisdiction of ASTM Committee F49 on Digital Information in the Supply Chain and is the direct responsibility of Subcommittee F49.06 on Clarity, Measurement, and Authenticity of Information.

Current edition approved July 1, 2024. Published July 2024. DOI: 10.1520/D8558-24.

How It Works - CoA Validation and Minting Data Flow



2. Referenced Documents

2.1 *ASTM Standards*:²

D8270 Terminology Relating to Cannabis

3. Terminology

3.1 Definitions are in accordance with Terminology D8270, unless otherwise indicated.

3.2 *Definitions of Terms Specific to This Standard*:

3.2.1 *block, n*—in blockchain technology, refers to the list of records, also known as transactions, bundled together with a predetermined size and linked to the previous block.

3.2.2 *blockchain, n*—a decentralized and distributed digital ledger technology recording transactions across numerous computers. The recorded data cannot be altered retroactively, ensuring transparency and security in data management.

3.2.3 *certificate of authentication, n*—a Certificate of Authentication (COA) is a document provided by an authoritative source that verifies the authenticity of an item. This certificate serves as a seal of assurance, indicating that the item in question is genuine and not a forgery or counterfeit.

3.2.3.1 *Discussion*—COAs are commonly used in the art world, collectibles market, and other areas where authenticity is paramount. Typically, a COA will include specific details about the item, such as its origin, any unique characteristics, the name of the authenticator, and possibly a unique serial number.

3.2.4 *cryptocurrency, n*—a type of digital or virtual currency using cryptography for security. Operates independently of a central bank, typically based on blockchain technology.

3.2.5 *decentralization, n*—refers to the distribution of functions, powers, people, or things away from a central location or authority. In blockchain, it signifies no single entity having control over the entire network.

3.2.6 *digital currency, n*—a decentralized digital currency, without a central bank or single administrator. It can be sent from user to user on the peer-to-peer Digital Currency network without intermediaries.

3.2.7 *distributed ledger, n*—a database existing across several locations or among multiple participants. In blockchain technology, it enables transactions to have public “witnesses”, reducing the need for trust.

3.2.8 *ERC-721, n*—ethereum request for comments (ERC) 721 is a data standard for creating non fungible tokens, meaning each token is unique and cannot be divided or directly exchanged for another ERC-721 token. The ERC-721 standard allows creators to issue unique crypto assets like NFTs via smart contracts.

3.2.9 *ERC-1155, n*—ERC-1155 is a multi-token standard on the Ethereum blockchain. It was designed to enable a single smart contract to manage multiple token types, both fungible and non-fungible.

3.2.10 *gas, n*—in blockchain, a unit measuring the amount of computational effort required to execute certain operations in the blockchain network.

3.2.11 *hash, n*—in blockchain, a function converting an input of letters and numbers into an encrypted output of a fixed length.

3.2.12 *immutable, adj*—immutability is the ability of a blockchain ledger to remain unchanged, unaltered, and memorable. Each of the blocks of information, like facts or transaction details, is carried out with the help of a cryptographic principle or a hash value.

3.2.13 *ledger, n*—in blockchain, a ledger is a record of all completed transactions.

3.2.14 *metadata, n*—metadata describes just attributes of the NFT, attributes like trait type, company name, product type, date of test and unique identifier of that test.

3.2.15 *mining, v*—in blockchain technology, the process of adding transaction records to the blockchain’s public ledger using computer processing power.

² For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at www.astm.org/contact. For *Annual Book of ASTM Standards* volume information, refer to the standard’s Document Summary page on the ASTM website.

3.2.16 *NFTs, n*—non-fungible tokens (NFTs) are unique digital assets representing ownership of specific items or pieces of content. Unlike cryptocurrencies, which are fungible and interchangeable, NFTs are distinct and not exchangeable on a one-for-one basis.

3.2.17 *node, n*—in blockchain, any computer connecting to the blockchain network.

3.2.18 *private key, n*—in blockchain technology, a sophisticated form of cryptography allowing users to access their cryptocurrency.

3.2.19 *proof of stake, n*—a type of consensus mechanism used by blockchain networks to achieve distributed consensus. It requires users to show ownership of a certain number of cryptocurrency tokens.

3.2.20 *proof of work, n*—a consensus algorithm in a blockchain network used to confirm transactions and produce new blocks to the chain.

3.2.21 *public key, n*—in blockchain technology, a cryptographic code allowing users to receive cryptocurrencies into their accounts.

3.2.22 *smart contracts, n*—self-executing contracts with the terms of the agreement between parties coded directly into them. Stored and replicated on the blockchain, they are supervised by the network of computers running the blockchain.

3.2.23 *token, n*—a type of cryptocurrency representing assets or utility and residing on its own blockchain. Tokens can represent any tradable goods or assets.

3.2.24 *tracking devices, n*—tracking device for COAs on the blockchain refers to tools, such as RFID, QR codes, or micro transponders, utilized to monitor and verify the authenticity of products connected to the COA by physically attaching these tracking devices to the products by unit, batch or lot as it moves through the supply chain.

3.2.25 *trustless, adj*—trustlessness is fundamental to blockchain technology, eliminating the need for intermediaries like banks or central authorities in transactions.

3.2.25.1 *Discussion*—This means individuals can engage in crypto payments and smart contracts directly with others, without relying on a third party's integrity or security. Essentially, it empowers individuals with full control and assurance in their cryptocurrency dealings.

3.2.26 *wallet, n*—in blockchain, a digital place where a user stores their cryptocurrency.

4. Significance and Use

4.1 Non-fungible tokens (NFTs) as unique digital certificates that verify the history and details of products – like a special label on a package or a report in a lab – tracking them from creation to delivery using a secure online system known as Blockchain Technology. Unlike regular digital money (cryptocurrencies), which are all the same and can be swapped one for another, each NFT is one-of-a-kind and can be used to track a single unit batch or lot of a product line. They can not just be exchanged equally because each has its special features, history, and sometimes even digital signatures, making it

unique to the product they are authenticating. These NFTs are made and managed on special digital platforms that ensure they stay unique and secure. This allows them to be viewed in a clear and trustworthy record of their history and authenticity.

4.2 *Importance of NFT Authentication with Blockchain Timestamps*—Authenticating an NFT is the process of verifying that it is genuine and not a counterfeit or unauthorized copy. One innovative method of authentication involves creating a snapshot of a Certificate of Authenticity (COA) for the NFT and placing it with a timestamp on the blockchain. This blockchain timestamp provides an immutable and verifiable record of the NFT's origin and authenticity. Authentication helps maintain the integrity of the products tracked with that COA, builds trust among participants, and protects the value of physical assets. By leveraging blockchain's timestamp capabilities and verifying the authenticity of an NFT, wholesalers and consumers can be confident in their purchases in any marketplace.

4.3 *Overview of the Authentication Process*—Authenticating an NFT on the blockchain involves examining the digital asset's underlying smart contract, metadata, digital signature, and transaction history. These components, along with various tools and services, can be used to verify the NFT's origin, ownership, and uniqueness. The authentication process typically includes the following steps:

4.3.1 *Examining the NFT's Smart Contract*—This involves analyzing the code and structure of the smart contract that governs the NFT, ensuring that it conforms to established standards, such as ERC-721 or ERC-1155, and checking for any irregularities or signs of tampering.

4.3.2 *Verifying the NFT's Metadata*—Metadata is the information associated with an NFT, such as its name, description, image, and creator. By verifying the metadata, individuals can ensure that it matches the intended digital asset and has not been altered or manipulated.

4.3.3 *Confirming the Digital Signature*—Digital signatures are cryptographic tools used to confirm the authenticity and integrity of digital data. They can be used to verify that an NFT was created by its claimed creator and has not been tampered with.

4.3.4 *Checking the NFT's Transaction History*—By examining the NFT's transaction history on the blockchain, individuals can trace its ownership and provenance, ensuring that it has been legitimately acquired and transferred. By following these steps and using the appropriate tools and resources, individuals can authenticate an NFT on the blockchain and have confidence in the digital asset's legitimacy and value.

5. System Requirements – Understanding NFTs and Blockchain Technology

5.1 *How NFTs Work*—Non-fungible tokens (NFTs) are unique digital assets stored on a blockchain. They are created using smart contracts, which are self-executing agreements with the terms of the contract directly written into code. This code is responsible for managing the ownership, transfer, and other rules associated with each specific NFT.

5.2 NFTs are typically based on token standards like ERC-721 and ERC-1155, which define a set of rules and functions