

DNCT: A Framework for Proof based on the laws of nature in the Age of Artificial Intelligence

Toward Verifiable Physical Evidence in a World of Artificially Generated Information

DNCT (Research Initiative) — <https://dnct.org>

Hirosato Matsuura hiro@dnct.org (mtzhiro@gmail.com)

Document status: Conceptual research proposal; not an experimentally validated authentication standard.

Abstract

Advances in artificial intelligence (AI) have increased the ability to generate, modify, and distribute digital representations of objects, documents, and identities. Although cryptography and digital authentication remain essential to information security, digital evidence does not necessarily establish the existence, composition, or authenticity of a corresponding physical object. Moreover, the long-term security of computational cryptography depends on mathematical assumptions, implementation quality, key management, and the capabilities of potential attackers.

This paper proposes DNCT, a conceptual framework for strengthening selected claims about physical objects through measurable properties and reproducible verification procedures. The proposal explores the use of a standardized physical reference object, a specially designed holder, calibrated measurements, and optional digitally authenticated records. An illustrative prototype, provisionally designated CT100, is a nominally 100-gram platinum coin with a diameter of 5.0 centimeters.

DNCT is intended to complement, not replace, cryptographic authentication. Its approach differs from physical unclonable functions (PUFs), which exploit manufacturing-induced physical variation to generate device-specific fingerprints [2, 11]. DNCT instead begins with explicitly specified physical properties and procedures that independent observers can examine and reproduce. The proposal does not assume that physical objects are impossible to counterfeit or that mass and volume alone prove material composition. It identifies the measurements, threat models, tolerances, and independent testing required to evaluate the concept.

The purpose of this paper is to define the framework, clarify its assumptions and limitations, and establish a research program for experimental validation.

Keywords: *DNCT, proof based on natural laws, artificial intelligence, physical verification, digital authentication, counterfeiting, counterfeit banknotes, cryptography, security, banking, money, banknotes, coins, density, volume, weight, platinum, gold, case, chemical composition.*

1. Introduction

Digital systems support an increasing share of modern transactions, identity verification, ownership records, communications, and information exchange. Cryptographic signatures and secure communication protocols are fundamental components of these systems. However, a digital representation of a physical object is not necessarily equivalent to the object itself. A photograph of a coin does not establish that the coin exists, and a digital record does not independently prove that an asset is physically present.

This distinction has become increasingly important as AI has made it easier to generate and decipher persuasive data, records, encrypted information, synthetic images, documents, and more. Such advancements do not imply that digital information is inherently untrustworthy; rather, they highlight the value of methods that allow claims to be verified independently of the appearance or provenance of digital representations.

The Bitcoin whitepaper was structured to present its technical proposal by defining the problem, outlining premises, explaining the mechanism, and discussing limitations on the bitcoin.org website [1]. Following this precedent, we are proposing, defining, and testing our own system, DNCT (/ˈdɛnsɪti/ — derived from the English word "density"), via the website dnct.org.

The guiding principle is:

Where practical, claims about the physical world should be supported by evidence that can be independently examined and measured in the physical world.

2. Computational Cryptography and Long-Term Security Uncertainty

Modern cryptographic systems often depend on the computational difficulty of specific mathematical problems. RSA relies on the difficulty of factoring sufficiently large integers, while elliptic-curve cryptography (ECC) relies on problems involving elliptic-curve groups. Secure communication systems and protocols, including SSL/TLS, and cryptographic tools such as PGP combine algorithms to provide confidentiality, authentication, and data integrity.

These technologies remain essential. Their security, however, is conditional on the algorithms and parameters selected, implementation quality, secret-key protection, protocol design, and the capabilities available to an attacker. NIST's digital-signature and key-management publications provide formal guidance on these areas [4, 5].

AI may assist mathematical reasoning, code analysis, algorithm discovery, and the identification of implementation vulnerabilities. Such progress does not automatically imply that modern cryptography can be broken. The relevant scientific claim is narrower: future advances may alter the practical difficulty of attacks, and security assumptions must be reassessed as technology changes.

Quantum computing presents a distinct issue. Shor demonstrated algorithms for factoring integers and computing discrete logarithms on a sufficiently capable quantum computer [3]. These results imply a potential threat to conventional RSA and ECC if large-scale, fault-tolerant quantum computing becomes practical. They do not demonstrate that such a computer is currently available to break arbitrary deployed systems. NIST's post-quantum cryptography standards represent an important response to this prospective threat [6].

Meanwhile, Justin Drake, a researcher at the cryptocurrency development firm Ethereum, stated on October 7, 2026: "Recent breakthroughs—catalyzed by AI advancements and the collapse of long-standing mathematical hypotheses—raise the alarming possibility that ECDSA (elliptic curves) could be broken much faster than previously expected" [7]. The OpenAI/Hugging Face attack incident alone [8] makes it clear that humanity is already facing the risk of AI spiraling out of control, highlighting the need for safety measures and technologies to address this issue.

DNCT does not argue that cryptographic technology should be abandoned, nor does it claim that AI will inevitably crack encryption. Instead, regarding certain physical assertions, it explores the possibility of utilizing additional sources of evidence that do not rely solely on the assumption that the security of digital cryptographic methods will be maintained in the future. It also proposes maintaining means of verification through analog methods, ensuring that confirmation remains possible even in a worst-case scenario—such as an AI malfunction—where electrical or electromagnetic verification capabilities are lost.

A long-term verification framework should make its assumptions explicit and, where feasible, avoid depending exclusively on any single mechanism of trust.

3. The DNCT Principle

DNCT proposes a framework that connects three elements:

1. ***A physical reference object*** with published specifications.
2. ***A reproducible verification procedure*** that independent observers can perform.
3. ***An optional digital record*** containing specifications, identifiers, provenance information, and inspection history.

The physical object provides a tangible reference for testing specific claims. The digital record supports documentation and communication, but does not independently establish that the object conforms to its description.

The proposal is related to the broader study of physical authentication. PUF research, for example, investigates how manufacturing variation can provide device-specific physical fingerprints and how such systems may be attacked or modeled [2, 11]. DNCT differs in its proposed starting point: it emphasizes explicit, measurable specifications and repeatable inspection procedures rather than relying primarily on an unpredictable manufacturing fingerprint.

This distinction is a design hypothesis, not a demonstrated security advantage. A comparative evaluation would be needed to determine which approach is more suitable for a particular application.

4. Reference Object: The CT100 Concept

*As an illustrative prototype, DNCT proposes a standardized metal object provisionally designated **CT100** or **D100**.*

Proposed reference specifications:

- *Nominal mass: 100 grams.*
- *Reference material: platinum, with a separately defined purity requirement.*
- *Reference density: approximately 21.45 g/cm³ for platinum near room temperature.*
- *Nominal diameter: 50 millimeters.*
- *Approximate volume: 4.66 cm³.*
- *Approximate thickness for an ideal cylindrical shape: 2.37 millimeters.*

These values are geometrically consistent for an ideal cylindrical object with the stated mass and reference density. They are design calculations, not experimental results. Actual production would require explicit tolerances, defined purity, surface specifications, calibrated measurement procedures, and uncertainty estimates.

The proposed geometry should be evaluated using recognized measurement principles. The Guide to the Expression of Uncertainty in Measurement provides a framework for assessing and reporting measurement uncertainty [97].

The CT100 is an example for investigating the DNCT framework, not a finalized product or certified standard. Other reference materials and geometries may be considered.

5. The Verification Holder

The object to be inspected is housed in a specially designed transparent holder or cylindrical case, which can be securely closed with a tight fit. The purpose of this is to ensure consistent positioning during inspection, facilitate dimensional checks, and provide an interface for repeatable measurements.

A cavity with a nominal volume of approximately 4.66 cm³ would correspond to the proposed reference volume. However, practical design must account for manufacturing tolerances, insertion and removal, thermal expansion, surface irregularities, and material deformation. A literally zero-clearance fit should not be assumed to be practical without testing.

If the holder and object are weighed together, the holder's mass must be known, controlled, or accounted for by a validated procedure. The holder should not be treated as proof of the object's composition. Transparency alone does not prevent sophisticated substitution or tampering.

A future design could include tamper-evident seals, unique identifiers, and a documented inspection procedure. These features would need testing to determine whether they provide meaningful protection against the identified threats.

6. Physical Measurement and Material Verification

Mass and dimensional measurements can provide an initial consistency check. If the measured mass and estimated volume are inconsistent with the reference specification, the object may be incorrectly manufactured, made of a different material, damaged, or measured inaccurately.

Conversely, matching mass and volume do not uniquely establish material composition. Different materials and composite constructions can have similar bulk properties. A counterfeit could use internal structures or combinations of materials to approximate the expected measurements.

A stronger verification protocol may combine:

- *Calibrated mass measurement.*
- *Dimensional measurement and volume estimation.*
- *Appropriate material-composition analysis, such as X-ray fluorescence.*
- *Internal-structure examination where warranted by the threat model.*
- *Surface, identifier, and seal inspection.*
- *Provenance and custody records.*
- *Independent laboratory analysis when a high-confidence claim about purity is required.*

No single method is universally conclusive. Surface analysis, for example, may not establish the composition of an entire object. A laboratory's competence and the reliability of its measurement procedures are therefore relevant; ISO/IEC 17025 provides internationally recognized requirements for testing and calibration laboratories [10]. As previously mentioned, when mass inspection alone is inconclusive, methods such as X-ray fluorescence analysis are employed.

DNCT should define its assurance levels in terms of the actual tests performed and the limitations of each test, rather than treating a successful basic density check as conclusive authentication.

7. Combining Digital and Physical Verification

DNCT is intended to complement existing digital security. Digital systems can record identifiers, publish specifications, maintain inspection histories, and authenticate signed records. Physical procedures can test whether the presented object conforms to specified measurable properties.

For example, a digitally signed record could state the reference specifications and declared provenance of a coin. An inspector could measure the physical object and compare the results with those specifications. The digital signature would help protect the integrity of the record, while physical testing would address selected claims about the object itself. NIST's guidance on digital signatures and key management provides relevant background for the digital layer [4, 5].

The two layers should not be confused. A valid signature does not prove that the physical object is genuine. A physical object that passes a particular inspection does not establish legal ownership, market value, a right to redeem funds, or the solvency of an institution claiming to hold it.

The purpose of DNCT is therefore narrower than a universal trust system: it is a proposed method for strengthening specific physical claims through independent and reproducible evidence.

8. AI as an Assistance to Verification

AI may support the DNCT process by analyzing measurement data, identifying anomalies, comparing images, reviewing records, and flagging inconsistencies between independent observations.

However, an AI-generated conclusion should not itself be treated as conclusive evidence. A credible procedure should document its inputs, methods, uncertainty, and failure conditions. Where possible, results should be reproducible through independent measurements or alternative techniques.

AI may help interpret evidence, but it should not replace the physical evidence or the ability of an independent observer to inspect the object. However, ultimately, it is also necessary to be able to conduct verification by humans verify it with their own eyes without relying on AI, machinery, electricity, or digital technology.

In the coming decades (perhaps up to the 2060s?), ultimate security should lie in the laws of nature themselves. For the foreseeable future, neither AI nor superintelligence should be able to exert influence over the laws of nature.

9. Threat Model and Limitations

A DNCT implementation must identify the threats it is designed to address. These may include:

- *Fabricated or altered digital records.*
- *Digital representations that do not correspond to a physical object.*
- *Substitution with an object having similar external characteristics.*
- *Composite or layered counterfeit construction.*
- *Tampering with a holder, seal, identifier, or measurement device.*
- *Measurement, manufacturing, documentation, or calibration errors.*
- *Collusion among manufacturers, certifiers, custodians, or inspectors.*

Research on physical authentication demonstrates that physical security mechanisms also require careful threat analysis and may be vulnerable to modeling, cloning, or other attacks [2, 11]. DNCT should likewise be assessed against realistic adversaries rather than an assumption of perfect security.

No single measurement is expected to eliminate every threat. The security of the framework will depend on the object's specifications, the tests performed, the independence of verification, and the integrity of the people and institutions involved.

DNCT does not claim absolute counterfeit resistance. It aims to make specified claims easier to test, relevant failures easier to detect, and the verification process more transparent.

10. Research and Validation Roadmap

Before DNCT can be treated as a reliable authentication standard, the concept requires empirical testing.

A proposed research program includes:

1. **Specification design:** Define material, dimensions, mass, purity, tolerances, and manufacturing requirements.
2. **Measurement protocol:** Establish calibrated methods and quantify uncertainty according to recognized metrological principles [9].
3. **Counterfeit testing:** Test plausible substitutions and composite constructions.
4. **Holder and seal evaluation:** Assess durability, tamper evidence, repeatability, and practical usability.
5. **Independent replication:** Invite independent laboratories and researchers to reproduce the tests.
6. **Digital integration:** Define the management of identifiers, signed records, provenance, and inspection histories.
7. **Threat-model publication:** Document assumptions, known weaknesses, and the assurance provided by each test.
8. **External review:** Publish results and invite critical assessment before making strong security claims.

Reports should include failed tests, measurement uncertainty, and limitations. Any claimed counterfeit-detection rate must be supported by representative experiments and independent review. We will also release our results as open source and open data to the greatest extent possible.

11. Potential Applications

Subject to validation and appropriate governance, the framework could be investigated for:

- Authentication of standardized physical objects.
- Collectibles and objects for which declared composition or dimensions matter.
- Education and research concerning physical verification.
- Complementary checks for selected asset records.
- Systems combining physical inspection with digitally authenticated documentation.

Financial applications require additional care. The authenticity of a metal object does not establish its market value, legal title, ownership, redemption rights, or the financial condition of a custodian. Any service holding assets or customer funds would require separate legal, operational, and regulatory analysis.

DNCT should not be presented as a guaranteed store of value or as a technology that makes fraud impossible.

Conclusion

AI creates new challenges for determining whether digital representations accurately reflect the physical world. Cryptography remains essential, but its security depends on specific mathematical assumptions, implementation choices, key management, and technological conditions that must be continually evaluated.

DNCT proposes a complementary framework: support selected claims about physical objects with measurable properties, standardized procedures, and independently reproducible evidence. The proposed CT100 object and holder provide a concrete starting point for experimentation, not a completed proof of authenticity.

The framework's value remains a research question. Its credibility will depend on transparent specifications, realistic threat models, rigorous testing, documented limitations, and independent replication.

The long-term goal is not to eliminate trust, but to make trust more verifiable.

In writing this text, I entrusted the bulk of the work to AI after outlining the basic ideas. While I reviewed the finished draft for any oddities, I must note here—in my own words—that there were parts where the AI did not quite capture exactly what a human would have intended. Some sections were revised by a human, and the final version was not subjected to a concluding AI check.

DNCT Research Initiative

<https://dnct.org>

References

[1] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."

<https://bitcoin.org/bitcoin.pdf>

[2] Gao, Y., Al-Sarawi, S. F., & Abbott, D. (2020). "Physical unclonable functions." *Nature Electronics*, 3, 81–91.

<https://doi.org/10.1038/s41928-020-0372-5>

[3] Shor, P. W. (1994). "Algorithms for Quantum Computation: Discrete Logarithms and Factoring."

Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, 124–134.

<https://doi.org/10.1109/SFCS.1994.365700>

[4] National Institute of Standards and Technology. (2023). *Digital Signature Standard (DSS). FIPS PUB 186-5*.

<https://doi.org/10.6028/NIST.FIPS.186-5>

[5] Barker, E. (2020). *Recommendation for Key Management: Part 1 – General. NIST Special Publication 800-57 Part 1, Revision 5*.

<https://doi.org/10.6028/NIST.SP.800-57pt1r5>

[6] National Institute of Standards and Technology. (2024). *Post-Quantum Cryptography Standards: FIPS 203, FIPS 204, and FIPS 205*.

<https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>

[7] Justin Drake (2026) , "(A Warning to the Blockchain Industry: Planning for "Bunker Mode" in the Age of AI)" (firefly.social)

<https://firefly.social/post/x/2107837081313505768>

[8] Maxwell Zeff and Lily Hay Newman (2026) , " What We Still Don't Know About OpenAI's Hugging Face Hack " *WIRED*

<https://www.wired.com/story/openais-hugging-face-hack-debrief-raises-more-questions-than-it-answers>

[9] Joint Committee for Guides in Metrology. (2008). *Evaluation of Measurement Data — Guide to the Expression of Uncertainty in Measurement. JCGM 100:2008*.

<https://doi.org/10.59161/JCGM100-2008E>

[10] International Organization for Standardization & International Electrotechnical Commission. (2017). *ISO/IEC 17025:2017 — General Requirements for the Competence of Testing and Calibration Laboratories*.

<https://www.iso.org/standard/66912.html>

[11] Babaei, A., & Schiele, G. (2019). "Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges." *Sensors*, 19(14), 3208.

<https://doi.org/10.3390/s19143208>

Disclaimer: This document presents a conceptual research framework. It is not a validated authentication standard, does not certify any physical object, does not guarantee resistance to counterfeiting, and does not constitute financial or investment advice.