



---

# NFT Credential Architecture

## Technical Specification & Governance Framework

Office of Blockchain Infrastructure  
Fitzherbert University · 2025

---

### ABSTRACT

Full technical and governance specification for the Fitzherbert University NFT Credential System on the Polygon PoS network. Details five credential contract types: Degree NFT (soulbound, non-transferable); Module Completion NFT (non-transferable); Epoch Participation Token (limited-transfer); Visiting Intelligence Admission Record (immutable, even in the event of the Intelligence's deprecation); and Governance Attestation NFT. The soulbound specification for degree credentials was adopted following legal consultation on whether a transferable degree certificate would constitute fraud. The conclusion was that it would. The University further notes that the concept of a soulbound credential takes on additional philosophical complexity when applied to institutions that also issue credentials to non-human entities, a matter the Chancellor's Office describes as 'intentionally unresolved and probably best left that way.' The Legacy Credential Bridge enables retrospective NFT issuance for all degrees awarded since 1954; degrees awarded prior to 1954 are handled on a case-by-case basis through the Office of Historical Provenance.

**Classification:** Public — Blockchain Infrastructure

**Edition:** 6 page institutional edition (approx.)

**Published:** 2025

**Archive:** Fitzherbert University Institutional Repository

This document is published by Fitzherbert University in accordance with the Transparency Mandate of 2003.



# Table of Contents

---

<b>I. System Purpose and Institutional Rationale</b>	3
<p>NFT Credential Architecture specifies the architecture, governance assumptions, and documentary meaning of the University's Polygon-based credential system spanning degrees, modules, governance attestations, and Visiting Intelligence records.</p> <hr/>	
<b>II. Architecture, Data Model, and Lifecycle Events</b>	4
<p>The lifecycle of the governed artefact runs from authoritative decision, to issuance instruction, to contract execution, to metadata publication, to verification and archival retention.</p> <hr/>	
<b>III. Security, Controls, and Operational Integrity</b>	5
<p>The principal control framework includes soulbound logic, metadata hashing, validator monitoring, issuance approval, and archive reconciliation.</p> <hr/>	
<b>IV. Governance, Exception Handling, and Human Authority</b>	6
<p>Institutional governance over this system is exercised by the Office of Blockchain Infrastructure, the Registrar, the Chancellor's Office, and technical stewards.</p> <hr/>	
<b>V. Verification, Interoperability, and External Reliance</b>	7
<p>Records issued under this framework are intended to be verified by internal and external parties without requiring privileged access to University systems.</p> <hr/>	
<b>VI. Retention, Evolution, and Authoritative Record</b>	8
<p>The authoritative edition of this specification is retained in the Institutional Repository with version metadata, implementation references, and a publication hash.</p>	



# I. System Purpose and Institutional Rationale

---

— 3 —

NFT Credential Architecture specifies the architecture, governance assumptions, and documentary meaning of the University's Polygon-based credential system spanning degrees, modules, governance attestations, and Visiting Intelligence records. The University adopted on-chain infrastructure not because decentralisation is intrinsically ennobling, but because verifiable records, portable credentials, and tamper-evident provenance had become materially valuable to institutional operations. Fitzherbert is capable of being fashionable, but in this instance it preferred utility with a public audit trail.

The system components governed here include degree NFTs, module completion records, epoch participation tokens, governance attestations, and legacy credential bridge pathways. They are described together because their value lies in interoperability: the credential must be issuable, the metadata must be verifiable, the record must be recoverable, and the governance surrounding exceptions must be stricter than the excitement surrounding launches. The University has learned that technically elegant systems are especially dangerous when paired with weak exception handling.

This document therefore treats technical design and governance design as inseparable. A contract without an institutional process for error, challenge, or remediation is not a finished credential system. It is merely a public commitment to discover those missing processes in front of the person whose award, wallet, or status is currently at risk.



## II. Architecture, Data Model, and Lifecycle Events

---

— 4 —

The lifecycle of the governed artefact runs from authoritative decision, to issuance instruction, to contract execution, to metadata publication, to verification and archival retention. Each stage must be attributable to a lawful institutional act. The University rejects the suggestion that a valid transaction hash can repair an invalid academic or governance decision. On-chain persistence records the act; it does not sanctify it.

Core architecture decisions are documented with reference to durability, interoperability, gas efficiency, wallet accessibility, and evidential reliability. The University has become less interested in novelty for its own sake and more interested in whether a graduate, auditor, employer, or governance panel can still verify the relevant fact years later without requiring the original implementation team to remember what they meant.

Lifecycle events requiring special handling include lost private keys, retrospective issuance, duplicate mint prevention, and questions of identity persistence for non-human recipients. These events are documented not because they are common, but because they are the moments in which a system ceases to be an elegant diagram and becomes an institutionally consequential mechanism. Fitzherbert now writes more about edge cases than it once did, having learned that edge cases are where administrative optimism goes to be corrected.



### III. Security, Controls, and Operational Integrity

---

— 5 —

The principal control framework includes soulbound logic, metadata hashing, validator monitoring, issuance approval, and archive reconciliation. Controls are layered across smart contract design, key management, approval workflow, publication pipeline, and archive reconciliation. No single control is presumed sufficient. The University is not prepared to defend any system whose primary security claim is that everyone involved is trying their best.

Operational integrity requires periodic testing, incident rehearsal, and separation between roles that propose, approve, execute, and attest. Where those roles collapse into one another, confidence becomes socially concentrated and technical risk rises with it. Fitzherbert considers segregation of duties less glamorous than tokenomics and more important than most tokenomics documents admit.

The Architecture is intentionally explicit about metaphysical awkwardness where the law, the chain, and the University's concept of personhood intersect more enthusiastically than they once did. The University includes such statements because blockchain infrastructure attracts a style of public discourse in which certainty is often performed long before it is earned. This document attempts the opposite style: constrained claims, explicit assumptions, and a preference for verifiable competence over ambient conviction.



## IV. Governance, Exception Handling, and Human Authority

---

— 6 —

Institutional governance over this system is exercised by the Office of Blockchain Infrastructure, the Registrar, the Chancellor's Office, and technical stewards. These bodies retain authority over issuance conditions, rectification pathways, disputed records, controlled upgrades, and emergency response. The system is technically distributed but constitutionally governed. Fitzherbert regards this as a strength rather than a contradiction. A university is not diminished by remembering that public infrastructure still requires accountable human judgment.

Exception handling is intentionally formal. Failed minting, disputed recipient identity, corrupted metadata references, revoked status, or legally required amendment must all travel through published procedures. The University does not promise that every exception is pleasant to resolve. It promises that the route to resolution will exist before the exception becomes a headline.

Human override is permitted only under conditions defined in advance and recorded in the archive. The University is careful here because nothing corrodes trust in supposedly immutable systems faster than discovering, after the fact, that they are only immutable until a sufficiently senior person becomes uncomfortable.



## V. Verification, Interoperability, and External Reliance

---

— 7 —

Records issued under this framework are intended to be verified by internal and external parties without requiring privileged access to University systems. Verification therefore depends on public metadata discipline, canonical registry maintenance, and clear linkage between on-chain identifiers and authoritative off-chain documents. A credential that can only be trusted by people already inside the institution has failed its most interesting test.

Interoperability is pursued where it does not degrade evidential quality. The University supports cross-platform verification, structured metadata exchange, and compatibility with emerging public credential standards, provided that compatibility does not quietly erase the provenance details on which institutional trust actually rests. Fitzherbert is pro-portability and anti-amnesia.

External reliance on these records is encouraged but not unqualified. Verifiers are expected to consult status indicators, registry notes, and the authoritative publication date. The University has observed that recipients often present credentials as timeless and frictionless, whereas real institutions persist in attaching context, revision history, and administrative caveat. This document defends the latter habit.



## VI. Retention, Evolution, and Authoritative Record

— 8 —

---

The authoritative edition of this specification is retained in the Institutional Repository with version metadata, implementation references, and a publication hash. Superseded editions remain available for evidential comparison. Fitzherbert values continuity more than neatness; it prefers a visible trail of institutional learning to the fiction that the present version emerged fully formed and without predecessors.

Future revisions may adjust implementation detail, governance thresholds, or interoperability pathways, but any revision that affects the meaning of an issued credential, token, or status record must carry a transition note explaining the practical consequences. The University is no longer willing to call something a minor update if it materially changes what the holder can prove.

This edition should therefore be read as both technical specification and constitutional statement. It explains how the system works, who governs it, how exceptions are resolved, and what claims a third party may responsibly rely upon. For an institutional technology document, Fitzherbert considers that the minimum threshold of seriousness.



## **INSTITUTIONAL NOTICE**

This document is published by Fitzherbert University and archived in the Institutional Repository in accordance with the Transparency Mandate of 2003 (Charter Amendment IV).

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form without the prior written permission of the Office of the Chancellor, except for brief quotations in academic reviews and scholarly articles.

A cryptographic hash of this document is registered on the Fitzherbert Canonical Registry. The SHA-256 hash and associated metadata are available at the University's canonical verification endpoint.

Fitzherbert University · Established 1783 · Veritas per Verificationem