UNICC UNJSPF

Transforming Public Digital Identity

A Blockchain Case in Action from the UN System

September 2025

Authors

Roman Beck
PhD Professor, Computer Information Systems Department and Blockchain Economist
Bentley University. Boston, USA.

Dino Cataldo Dell'Accio
Chief Information Officer
United Nations Joint Staff Pension Fund (UNJSPF)

Elena Sierra
Business Relationship Manager
United Nations International Computing Centre (UNICC)

Pablo Arribas
Solutions Architect and Blockchain Specialist
United Nations International Computing Centre (UNICC)

Andres Guerrero
Data Solution Architect and Artificial Intelligence Specialist
United Nations International Computing Centre (UNICC)

Massimiliano Falcinelli
Digital Solutions Strategy Lead Officer
United Nations International Computing Centre (UNICC)

Editors

Jean Pierre Mora Casasola
Communications Officer
United Nations International Computing Centre (UNICC).

Mirko Montuori
Public Information Officer
United Nations Joint Staff Pension Fund (UNJSPF).

Layout and Design

Denian Ouyang
Associate Communications Officer (Multimedia)
United Nations International Computing Centre (UNICC).

Required citation: UNJSPF, UNICC. 2025. Transforming Public Digital Identity: A Blockchain Case in Action from the UN System.

Foreword

Dino Cataldo Dell'Accio
Chief Information Officer
UNJSPF

The UNJSPF digital identity solution, the Digital Certificate of Entitlement (DCE) for proof-of-life detailed in this white paper represents a paradigm shift — leveraging blockchain technology to create a secure, accessible, and user-controlled identity infrastructure. In a world where digital identity has become the gateway to essential services, employment, and economic opportunity, blockchain offers unprecedented potential to bridge the gap between the identified and unidentified.

The focus on assurance and auditing of emerging technologies has been a key influence in shaping the development approach of the DCE. In my experience, the intersection of innovation and trust—achieved through the adoption of relevant ISO standards and assurance frameworks—has informed efforts to ensure that emerging technologies deliver their intended benefits while addressing associated risks. This background provided a unique perspective during the design of the DCE, where we implemented a comprehensive risk management framework addressing business, governance, technology, and process aspects. We recognized early that assurance isn't merely about identifying risks but also capitalizing on opportunities—a critical mindset when applying blockchain to solve the global identity crisis.

Moreover, the self-sovereign identity (SSI) paradigm underpinning the UNJSPF solution represents a fundamental rethinking of how identities are managed in the digital age. Unlike traditional systems where identities are controlled by central authorities, blockchain enables individuals to own and manage their identities independently. Through Decentralized Identifiers (DIDs) stored on an immutable blockchain ledger, users maintain portable identities that can be verified without intermediaries. Verifiable Credentials function as digital certificates, cryptographically signed by trusted issuers, enabling secure and selective disclosure of personal information.

This architecture directly addresses the most pressing challenges in identity management today. Data breaches that have compromised millions of identities become substantially less threatening when personal data is no longer centrally stored. The elimination of single points of failure through decentralization dramatically reduces vulnerability to both attacks and system failures. Perhaps most importantly, blockchain returns control of personal information to individuals, allowing them to share only what is necessary with each service provider without relinquishing ownership of their identity.

The DCE solution represents a comprehensive approach to inclusive identity management. Drawing from rigorous audit frameworks, in collaboration with our trusted partner, the United Nations International Computing Centre, we implemented a system that balances security, accessibility, regulatory compliance, along with industry practices and standards. Our architecture incorporates biometric facial recognition, ensuring that physical disabilities or environmental factors don't become barriers to identification. For regions with limited connectivity, we developed offline authentication capabilities, using Kiosks, installed in relevant United Nations field offices.

We explicitly designed the DCE to address the exclusion risks and fill digital divides. Our risk assessment methodology identified vulnerable populations — including remote and rural residents, and individuals with low technical literacy—and implemented specific measures to ensure their inclusion. The technical assurance measures incorporated into the DCE follow key security domains, such as those defined by ISO and ITU. This comprehensive security approach, combined with our focus on accessibility, created a solution that works for everyone.

Business Impact and Societal Benefits

The business case for blockchain-based identity management is compelling. Organizations implementing digital ID solutions have reported higher profitability compared to those using traditional systems. Cost reductions are significant for UNJSPF, with savings in printing, mailing, physical and logical archiving, and manual verification of signatures. Automated processes enabled by secure digital identification greatly improve operational efficiency, while reducing administrative overhead and paper documentation costs.

Beyond these operational benefits, the most profound impact comes from enabling over 70,000 UNJSPF clients to access and perform an essential activity with peace of mind, immediate notification, and confidence about the result.

As we stand at this critical juncture in digital transformation, blockchain presents an unprecedented opportunity to create truly inclusive identity systems. The DCE solution demonstrates how technical innovation when guided by principles of accessibility and human-centred design, can simultaneously deliver business value and positive social impact. I invite you to explore the detailed technical architecture, implementation framework, and evidence-based outcomes presented in the following pages.

The future of identity management lies not in creating more sophisticated barriers but in building bridges to inclusion. With blockchain as public infrastructure for identity, we can ensure that no one is left behind in our increasingly digital society. Our journey toward universal, secure, and self-sovereign identity has just begun, and I believe the approach outlined in this white paper provides a valuable roadmap for the path ahead.

Executive Summary

This white paper explores the transformative potential of blockchain technology as a foundational infrastructure for digital identity management, with a focus on its implementation within the United Nations Joint Staff Pension Fund (UNJSPF). The paper highlights how decentralized identity frameworks can enhance **security**, **operational efficiency**, and **transparency** while aligning with the UN's broader agenda on digital transformation and inclusive governance.

Key insights include:

- **Blockchain and Digital Identity:** Traditional identity management systems face vulnerabilities such as data breaches, identity theft, and user privacy concerns. Blockchain technology offers a decentralized, tamper-resistant alternative that enables secure, seamless and interoperable identity verification across organizations.

- **Case study - Digital Certificate of Entitlement (DCE):** The United Nations Joint Staff Pension Fund (UNJSPF) has deployed a blockchain-based Digital Certificate of Entitlement (DCE) to modernize pension verification, replacing outdated paper-based processes. Utilizing biometrics, artificial intelligence (AI), cryptographic validation, and secure geo-location data, this solution enhances security, operational efficiency and fraud prevention.

- **Business impact and benefits:** By adopting the DCE, UNJSPF has streamlined operations, reduced administrative costs, and implemented a tamper-proof system benefiting thousands of retirees from the UN and 24 other UNJSPF member organizations worldwide. The transition to digital identity solutions has also strengthened fraud prevention measures, improved regulatory compliance with data protection standards, and enhanced the user experience for UNJSPF beneficiaries. It serves as a scalable and shareable digital platform for the modernization of other UN entities and international organizations.

- **Strategic vision:** The paper advocates for collaborative governance models and standardized frameworks to facilitate cross-agency adoption of UN blockchain identity solutions, contributing to the achievement of SDG 16.9 and broader UN digital governance priorities.

As a common digital infrastructure such as blockchain and AI-based digital identity solutions can serve as a blueprint for digital transformation across the UN system. This white paper advocates for collaborative governance models, standardized frameworks, and cross-agency adoption to expand 21st century capabilities in global digital identity management.

Introduction

As the global digital landscape evolves, **decentralized systems** are emerging as a cornerstone of resilient digital infrastructure.

Traditional identity management models—often centralized and siloed—face persistent challenges, including data security risks, limited accessibility, and interoperability gaps. These systems rely on single points of failure, making them vulnerable to data breaches, identity theft, and unauthorized access. Moreover, fragmented identity frameworks often hinder seamless verification across different organizations and jurisdictions.

Blockchain technology offers a transformative solution to these challenges by providing a decentralized, tamper-resistant, and cryptographically secure identity verification system.

Unlike conventional identity databases, blockchain-based identity solutions eliminate reliance on centralized authorities, reducing the risk of data breaches and unauthorized alterations. Through distributed ledger technology (DLT), blockchain ensures data integrity, transparency, and verifiability without compromising user privacy.

Blockchain is the ultimate technology for digital identity verification based on the following premises:

1. **Security and immutability:** Blockchain's cryptographic mechanisms safeguard identity records from tampering and fraud. Once an identity credential is registered on the blockchain, it becomes immutable, ensuring that it cannot be altered or manipulated by unauthorized entities.

2. **Decentralization and user control:** traditional identity systems place control in the hands of centralized institutions, which can be compromised or misused.

3. **Interoperability and seamless verification:** Blockchain's open standards facilitate cross-platform identity verification, enabling different organizations and institutions to authenticate users without duplicating identity records. This eliminates the need for repetitive identity checks, streamlining access to public services, financial institutions, and global humanitarian programs.

4. **Fraud prevention and identity theft protection:** Identity fraud remains a major challenge in digital ecosystems, with bad actors exploiting vulnerabilities in centralized databases. The adoption of artificial intelligence to fight against deepfakes, along with Blockchain's decentralized structure significantly reduces the risk of unauthorized access and identity cloning.

5. **Privacy-preservation:** Verifiable Credentials (VCs) allow secure proof of identity without exposing sensitive personal data.

What is Blockchain and Digital Identity?

1.1 The emergence of blockchain as digital public infrastructure

Blockchain technology has evolved beyond its cryptocurrency origins to emerge as a foundational digital public infrastructure, with governments and institutions worldwide recognizing its transformative potential. Countries such as Brazil with its Brazilian Blockchain Network[1] or the European Union with its European Blockchain Services Infrastructure (EBSI)[2] are actively exploring blockchain as a backbone for national or Europe-wide digital infrastructure, demonstrating how this technology can support public services while ensuring transparency and security. Technology's ability to create trustworthy, decentralized systems has made it particularly attractive for public sector applications as a next-generation infrastructure.

The implementation of **blockchain as public infrastructure** represents a fundamental shift in how governments and supranational institutions can manage and share data, with significant implications for administrative procedures and citizen services.[3] This transformation is particularly evident in areas such as digital identity management, where blockchain-based systems are being developed to create secure, user-centric identity frameworks. Recent developments in digital identity ecosystems, such as the eIDAS 2.0 legislation in the European Union, demonstrate how blockchain can balance government oversight with individual privacy, creating more efficient and transparent public services while maintaining security and data protection standards.

The evolution of blockchain governance in the public sector has led to the **emergence of new conceptual frameworks** that address both technical and organizational challenges. These systems must be designed with built-in flexibility to accommodate future technological advances while maintaining the robust security and transparency that make blockchain valuable as public infrastructure. This has led to the development of **hybrid models** that combine the benefits of both centralized oversight and decentralized operations, particularly in critical infrastructure applications where security and reliability are paramount.

[1] https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-develops-blockchain-network-to-support-id-rollout/
[2] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home
[3] https://www.emerald.com/insight/content/doi/10.1108/itp-05-2020-0343/full/html

1.2 Brief history of digital identity and blockchain

The World Economic Forum defines three **types of digital identities**[4]: Centralized, federated and decentralized. Centralized digital identity is the most common model for managing identities, where the identities are owned and managed by a single organization. Federated digital identities emerged with third-party identity providers which are central system owners who then distribute the information to other digital services. Decentralized digital identities allow the owner of the identity to manage his or her identity independently from other service providers. Those decentralized Identifiers (DIDs) are a relatively new types of identifiers that is created, owned, and controlled by the entity it represents, typically a person, organization, or device. They are globally unique, resolvable with the help of a distributed ledger or blockchain and can be verified cryptographically. This decentralization removes the need for intermediaries, while enhancing privacy and security.

Verifiable Credentials (VCs) are digital statements made by an issuer about a subject that can be cryptographically verified. These credentials can include a wide range of information, such as educational certificates, identity documents, or membership records. VCs are designed to be tamper-evident and can be verified independently of the issuer using cryptographic proofs, ensuring their authenticity and integrity.

Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) led to the emergence of **Self-Sovereign Identity (SSI)**. The concept of decentralized identity traces back more than two decades ago, but it wasn't until the rise of blockchain technology that DIDs became truly viable.[5] The World Wide Web Consortium (W3C) played a crucial role in standardizing both DIDs and VCs for modern digital identity systems that prioritize privacy, security, and user control.[6] This shift represents not just a technological evolution, but a philosophical one, moving away from traditional federated identity management toward a model where individuals have complete sovereignty over their digital credentials and personal data.

[4] https://widgets.weforum.org/blockchain-toolkit/pdf/digital-identity.pdf

[5] https://www.sciencedirect.com/science/article/abs/pii/S138912862300244X

[6] https://www.w3.org/TR/vc-data-model-2.0/

1.3 Digital identification for digital public infrastructures

Digital public infrastructure built on blockchain technology offers transformative potential and addresses several challenges in current identification systems. The integration of VCs and SSI creates a robust framework for secure digital identification while giving individuals unprecedented control over their personal data. This allows for **seamless access to public services**, reduces bureaucratic overhead, and significantly decreases the risk of identity theft and fraud. The distributed nature of blockchain infrastructure also ensures greater system resilience and transparency, making it harder for any single point of failure to compromise the entire system.

However, the implementation of such systems faces substantial challenges that cannot be ignored. Governance decisions around blockchain infrastructure often remain complex, particularly regarding the balance between privacy and transparency. The transition from legacy systems presents significant technical hurdles, requiring investment in both infrastructure and training. Moreover, the need to ensure universal access across different levels of technical literacy poses equity challenges in public service delivery.

Successful implementation depends on achieving the right **balance between decentralization and necessary oversight,** ensuring that the system remains both secure and accessible while maintaining public trust.

Blockchain addresses several challenges in current identification systems

Data breaches

By eliminating central points of failure, blockchain reduces the risk of massive data breaches

Identity theft

The cryptographic nature of blockchain makes it difficult for malicious actors to forge identities.

User privacy

Users have greater control over their personal data, deciding what information to share and with whom.

Interoperability

Blockchain can enables seamless identity verification across different platforms and organizations.

Practical Application at UN Joint Staff Pension Fund

2.1 Seizing benefits of emerging technologies in the UN system

The United Nations International Computing Centre (UNICC), established in 1971, is the largest strategic partner for digital solutions and cybersecurity within the United Nations system. Its main purpose is to design, evaluate and deploy transformational digital solutions to support over 100 partners and clients in fulfilling their mandates.[7]

Over the years, UNICC explored together with UNHCR blockchain-based digital solutions to support refugees[8] or aligned forces with partners such as Hyperledger Foundation[9], all illustrating the general applicability of blockchain solutions in the UN system[10]. A key challenge in all UN system blockchain solutions has been ensuring digital identification in multi-national environments.

To assess the potential of blockchain, UNICC engaged with blockchain experts across the UN, technology partners, and academia. In so doing, UNICC gained deeper insights into the possibilities blockchain may provide in digital identity use cases. **Blockchain and artificial intelligence for digital identification** purposes promises efficiency, transparency, immutability, auditability, and data integrity. While the potential improvements are significant, their actual impact can only be proven through the practical application of the technology. Thus, UNICC and UNJSPF joined forces together with Hyperledger to improve and secure the UN pension process globally by putting a blockchain-supported digital identification infrastructure into production.

[7] https://www.unicc.org/who-we-are/about-us/

[8] https://www.unhcr.org/news/press-releases/unhcr-wins-award-innovative-use-blockchain-solutions-provide-cash-forcibly

[9] https://www.unicc.org/our-impact/strategic-partnerships/

[10] https://unhabitat.org/sites/default/files/2021/10/jiu_rep_2020_7_e.pdf

2.2 The need for digital identification in the UN system

The UNJSPF considered ways to enhance its **seven-decade-old manual verification process** for proof of life by its beneficiaries residing in over 190 countries. This manual process was prone to human error, postal mail delays, and fraud. The stakes were particularly high: A single delayed verification or administrative error could result in the suspension of vital pension benefits to retirees who have dedicated their careers to international public service. This challenge presented not just an administrative burden, but a fundamental question of how international organizations can better serve their constituents in the 21st century.

Consequently, the UNJSPF identified four critical pillars of a viable digital identity infrastructure:

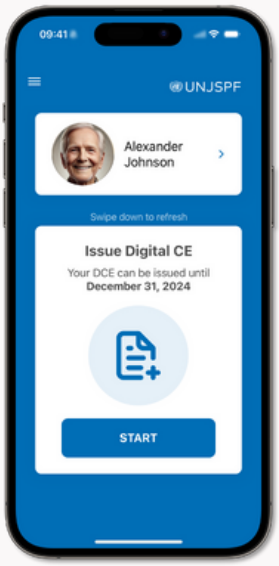
Identity verification, the cornerstone of any benefits system, requires robust digital solutions that can work across borders and jurisdictions.

Existence verification that would transition from paper-based processes to real-time digital confirmation, ensuring continuity of benefits while preventing fraud.

Transaction validation demands an immutable digital record that can withstand scrutiny and audit.

Location verification, an essential feature to accurately delivering benefits under the two-track system, which adjusts payments based on the beneficiaries' residence.

Aligned with the UN Secretary-General's Strategy on New Technologies[11], this digital identity transformation represents more than mere technological advancement. It embodies the **principles of inclusive governance, transparent administration, and sustainable development.**



Case: UNJSPF Certificate of Entitlement

Beneficiaries receiving periodic benefits from the Fund must annually submit a completed certificate of entitlement (CE) to the UNJSPF to confirm their existence. This process, which has been in place for over 70 years, ensures that benefits are not paid to deceased individuals. The certificate includes the pension number and type of benefits, requiring the retiree's signature or thumbprint. Traditionally paper-based, it is now also available digitally.

The process begins with the Fund sending a barcoded certificate to retirees at the end of May, referred to as the first CE mailing. If not returned within three months, a second mailing occurs in early September. To maintain benefit payments, the certificate must be received by the end of the year. Non-compliance results in suspension of payments in the following year.

Beneficiaries not under the two-track system can access and submit their certificates through their Member Self-Service accounts, either by mail or digitally. Those on the two-track system cannot use the MSS for this purpose, as the Fund needs to verify their declared residency. Submission must be original or hand-signed scanned copies; other methods are not accepted.

[11] https://www.un.org/en/newtechnologies/

2.3 Objectives of delivering blockchain-based digital identity

The UNJSPF faced a modernization challenge in its pension entitlement certification process. For over seven decades, the Fund relied on paper-based certificates of entitlement to verify the proof of existence of its beneficiaries—a system that became increasingly unsustainable as its recipient base grew to over 70,000 beneficiaries across 190 countries.

Three key challenges drove the need for transformation. First, the COVID-19 pandemic exposed severe vulnerabilities in the traditional mail-based system, disrupting pension entitlement verifications globally. Second, operational inefficiencies resulted in approximately 1,400 annual payment suspensions due to delivery failures and signature verification issues. Third, the exponential growth of beneficiaries—requiring over 85,000 forms to be processed annually—strained the Fund's manual processing capacity.

The existing system particularly impacted vulnerable beneficiaries. Many elderly pensioners, lacking digital literacy or access to technology, couldn't utilize the available online alternatives. Those under the two-track payment system faced additional challenges, as the UNJSPF needs to capture their location to confirm their place of residence and to apply cost-of-living adjustments.

Hence, a UN blockchain-based digital identification infrastructure could fulfill several key objectives to deliver an inclusive solution for the certificate of entitlement:

1. **Universal legal identity:** In alignment with SDG Target 16.9, which aims to "provide legal identity for all" by 2030, a blockchain-based system was intended to create a standardized, universal process for identity management across UN operations.

2. **Decentralized identity management:** Moving away from centralized identity systems toward a more secure and self-sovereign identity model would gives individuals more control over their personal data.

3. **Operational efficiency:** The system aimed to improve coordination across different UN agencies and humanitarian operations. The objective was to reduce administrative overhead and streamline identity verification for UN retirees.

4. **Enhanced security and privacy:** It was imperative to address infrastructure and information gaps while maintaining high security standards. This was made possible by leveraging blockchain's inherent security features to protect sensitive identity data.

5. **Interoperability and standardization:** By developing a standardized identity infrastructure that could be used across different agencies and programs, while maintaining consistency in identity management.

6. **Sustainable Development Goals (SDGs) integration:** The digital identity infrastructure was designed to support broader UN guidelines on inter-agency collaboration by improving governance, efficiency and accountability.

7. **Cross-border cooperation:** The aim was to facilitate better cross-border cooperation through standardized identity verification that could work across different jurisdictions while respecting local regulations and privacy laws.

2.4 The importance of digital identification in the UN system

The implementation of blockchain-based digital identity systems represents a critical advancement in the United Nations' operational capabilities. It offers new opportunities to address operational challenges while improving operational efficiency, interoperability, and inclusion and significantly reducing administrative overhead.

The system's inherent cryptographic and AI-enabled security ensures the protection of sensitive personal data while maintaining complete audit trails of all transactions, addressing both privacy concerns and accountability requirements and assurance in the face of increasing deepfake threats.

As detailed in table 1, the benefits of blockchain application are even greater for the UN system.

Table 1 - The case for blockchain application in the UN system

Current issues and challenges	Blockchain applicability for the UN system
Centralized databases sometimes with outdated, less secure technology often store sensitive user data, making it more prone to breaches.	**Data security:** Ensuring the security of sensitive user data is crucial for the UN to protect individuals' privacy and maintain trust. Data breaches can lead to severe consequences, including identity theft and misuse of personal information. Enhanced data security is essential for maintaining the integrity and confidentiality of information.
Verifying identities and authenticating users is a time-consuming process.	**Efficiency in operations:** Efficient identity verification and authentication are vital for the UN's operations, allowing for quicker and more effective delivery of services. Faster processes reduce administrative burdens and enhance the overall responsiveness of the organization.
Traditional verification and authentication require more tools, manual processes, and staff, leading to high costs	**Cost management:** Reducing costs associated with verification and authentication allows the UN to allocate resources more effectively. Lower operational costs mean more funds can be directed towards essential programs and services, increasing the impact of the UN's efforts globally.
Fraudulent digital identities are created using people's data.	**Preventing fraud:** Combating identity fraud is critical for the UN to ensure the credibility and reliability of its services. Preventing fraud protects individuals from exploitation and misuse of their identities, fostering trust in the UN's systems and processes.
Internal and external fraudsters often manipulate records for personal gain, especially low-key transactions	**Transparency and accountability:** Ensuring transparency and accountability in record-keeping is fundamental for the UN. An auditable trail of records deters fraud and corruption, promoting ethical practices and reinforcing the organization's commitment to integrity and accountability.

Current Issues and challenges	Blockchain applicability for the UN Ecosystem
Trusting the claims of a person or small group with full data access is risky, as verifying information accuracy is often limited.	**Trust and reliability:** Automated data transparency ensures that all stakeholders have access to verified information, reducing the risk of misinformation. This builds trust among stakeholders and ensures the reliability of data used in decision-making processes, which is crucial for the UN's credibility.
Adapting to increasing user privacy regulations is challenging and requires constant system updates.	**Regulatory compliance:** Complying with privacy regulations like UN Data Privacy Principles, closely aligned with General Data Protection Regulation (GDPR), is essential for the UN to operate within legal frameworks and protect individuals' rights. Streamlining compliance processes ensures that the UN adheres to international standards, avoiding legal issues and maintaining its reputation.
Over 1 billion people lack proof of identity, hindering their access to education, employment, government services, and financial resources.	**Identity accessibility:** Providing verifiable identities is crucial for the UN to support inclusive development and access to essential services. Ensuring that everyone, including marginalized populations, has proof of identity empowers individuals to participate fully in social, economic, and political life, aligning with the UN's mission to promote equality and human rights.

2.5 UNJSPF: The Digital Certificate of Entitlement (DCE) solution

To ensure **robust digital infrastructure** protection, UNJSPF implemented **comprehensive security protocols** through independent expert assessments. The evaluation encompassed 11 critical domains—from network architecture to smart contract integrity—while adhering to international ISO standards. A **parallel privacy assessment** across policy, data management, and organizational frameworks validated DCE's compliance with global best practices.

The **Digital Certificate of Entitlement (DCE) solution** is a biometric-based, secure, tamper-proof identity verification system powered by blockchain and AI technologies. Designed to be secure and fraud-resistant, the DCE ensures seamless validation of pension entitlements for retirees with the UN system and other UNJSPF member organizations.

DCE incorporates artificial intelligence (AI) to enhance biometric recognition, ensuring accurate identity verification while detecting and preventing deepfakes. Fully aligned with the principles of decentralization, the DCE prioritizes user privacy—all personal data remains securely stored on the user's device, with no sensitive information exchanged or centrally stored.

The DCE initiative commenced with a strategic pilot in 2020, targeting a select group of 351 beneficiaries across 43 countries. By leveraging the unique features of blockchain and biometrics, the DCE solution enhances the efficiency, security, immutability, auditability, traceability, and transparency of the annual entitlement procedure, to support the proof-of-life verification, as a mandatory requirement to complete the pension benefit validation.

Furthermore, the use of **blockchain, biometrics, and geo-location technologies** allows the solution to support additional verifications, including **Proof-of-Transaction** and **Proof-of-Location**. The two-phase rollout in May and June of 2020 allowed for critical system optimization, including enhanced security protocols and biometric interface improvements. Following successful pilot completion and comprehensive board review, the solution was **fully implemented in January 2021**, marking a significant step toward digital transformation in benefit distribution systems.

After **five years in production**, the Digital Certificate of Entitlement (DCE) has revolutionized pension verification, with over 43,000 beneficiaries actively using the platform in 2025—accounting **for 53% of the total beneficiary population.**

This digital transformation has led to a **40% reduction in paper-based** Certificate of Entitlement (CE) processing, significantly enhancing operational efficiency through seamless, automated digital workflows.
The DCE's business impact is reflected by the retention rate in 2024. Only 15 beneficiaries opted to return to paper-based processing, despite the option being available to all beneficiaries. This represents a **retention rate of 99.96%**.

2.6 Architecture of blockchain-based identity verification

The DCE solution utilizes a **permissioned blockchain identity system** built on two Hyperledger Foundation frameworks: Indy and Aries.

Hyperledger Indy provides a **decentralized identity management** infrastructure that uses blockchain technology to create a distributed source of truth.[12] The system stores critical cryptographic elements, including public keys and verification proofs, enabling self-sovereign identity management. This architecture supports the implementation of Verifiable Credentials (VCs), which gives organizations the ability to **issue, verify, and revoke** digital credentials through secure cryptographic protocols.

The system operates through a distributed ledger structure comprising four distinct components: a **pool ledger** that identifies network nodes, a **domain ledger** that maintains identity records, a **configuration ledger** that manages network parameters, and an audit ledger that ensures synchronization across the system. These ledgers operate under the Redundant Byzantine Fault Tolerance (RBFT) consensus protocol, which ensures transaction consistency across the network.

Hyperledger Aries extends this infrastructure by implementing **blockchain-agnostic protocols** for digital identity management. Its agent-based architecture facilitates interactions between various entities—credential **holders**, **issuers**, and **verifiers**—while managing connections and communication related to decentralized identities and credential verification processes.

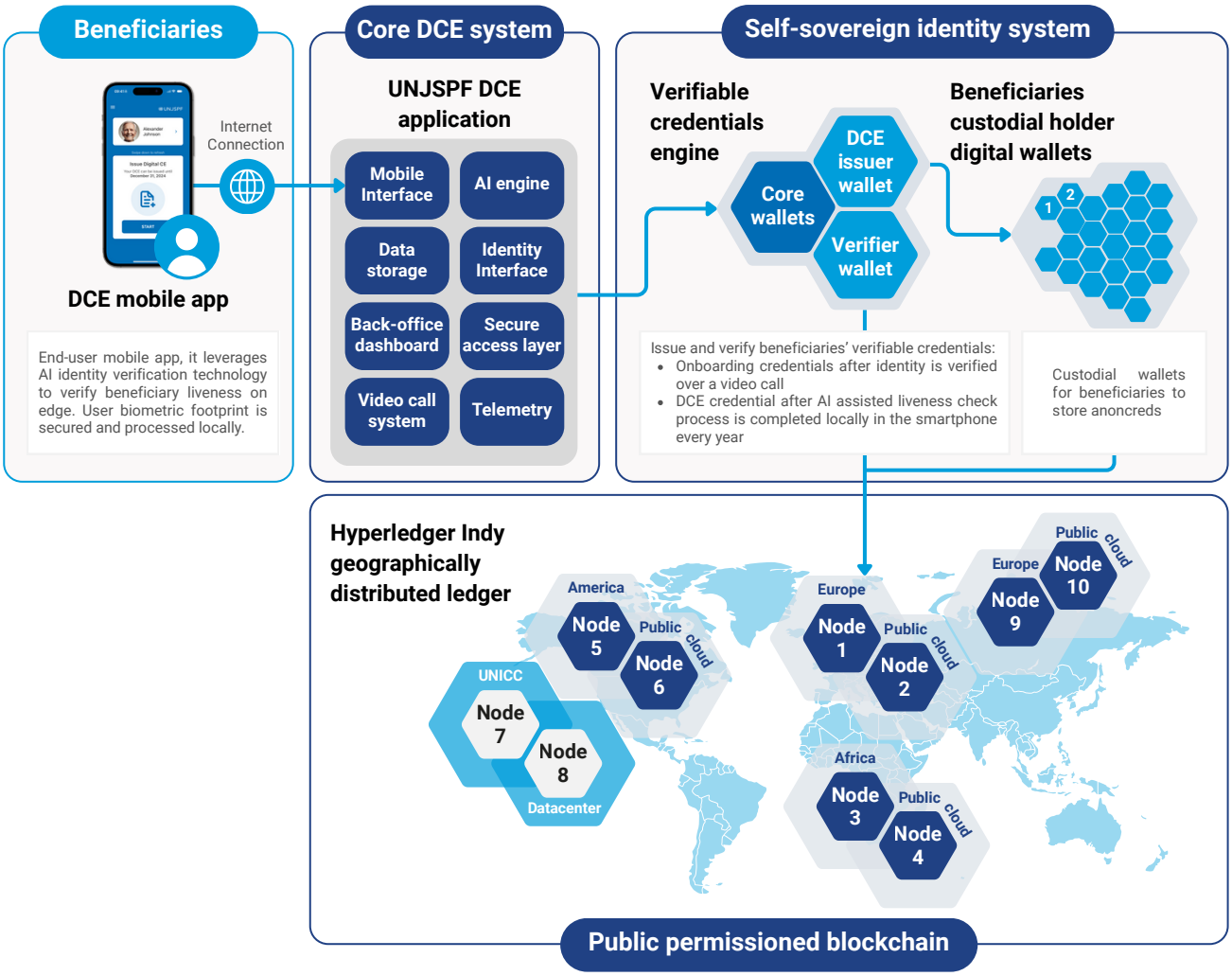
- **Issuers** are responsible for generating and distributing VCs to holders. They define schemas of the digital representations of common credentials for example, educational degrees, certifications, licenses. Credentials are cryptographically signed ensuring authenticity and integrity.

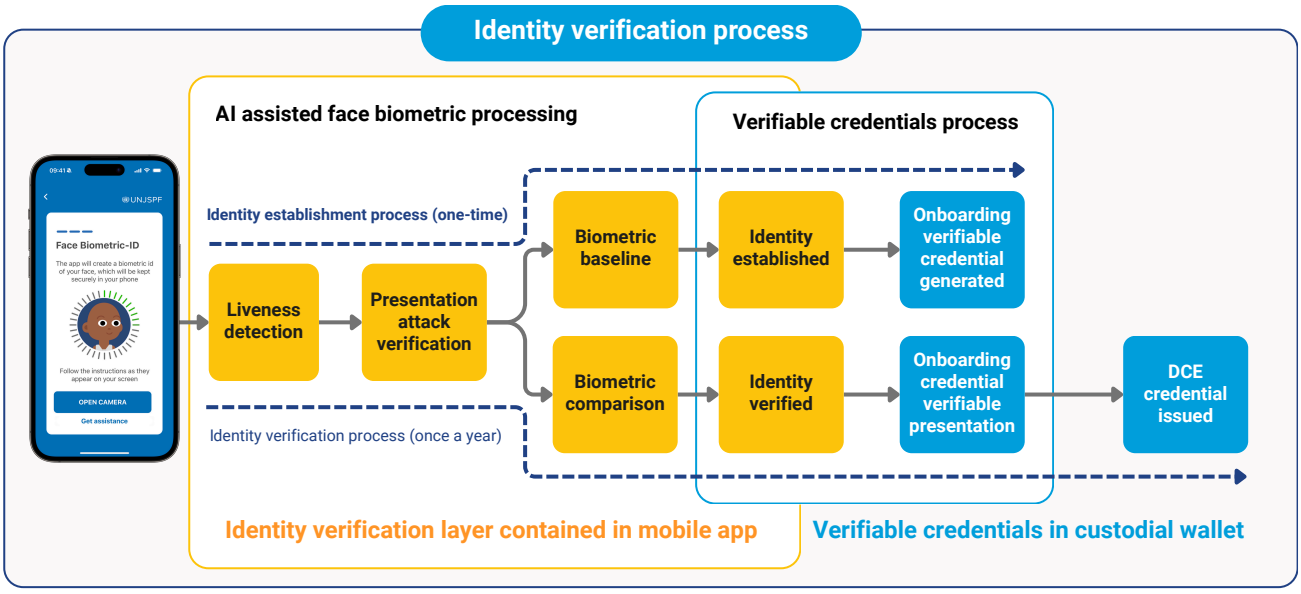
- **Holders** are entities who possess any credentials. These credentials are stored in digital wallets, cryptographically secured files that acts similarly to physical wallets. Holders can selectively share their credentials with verifiers through privacy preserving mechanisms that allow verification without the need of a trusted third party or the issuers themselves.

- **Verifiers** rely on blockchain transparency to verify the authenticity of credentials without any intermediary. When receiving a credential from holders they can independently validate it by means of Zero-Knowledge Proof (ZKP).

[12] https://github.com/hyperledger-archives/indy-sdk/blob/main/docs/getting-started/indy-walkthrough.md

The diagrams below illustrate the **business logic** behind the **DCE architecture**, showcasing its integration of blockchain, biometrics, and AI components.





2.7 Process and service improvements of blockchain-based identification systems

The DCE solution has transformed how identity verification and document management processes are managed within UNJSPF. Since its implementation in 2021, the digital infrastructure has significantly reduced reliance on paper-based certification documents, marking a decisive shift toward **digital process efficiency.**

The adoption rate of the DCE solution demonstrates remarkable progress, with 53% of beneficiaries by 2025, with gradual increase from its initial rollout in 2021. This digital transition has **eliminated the need for paper certifications** among registered DCE users, streamlining operations across multiple dimensions.

Operational process efficiency gains are particularly noteworthy in document processing workflows. The shift away from physical documentation has substantially **reduced processing times previously spent on receiving, opening, scanning, and archiving paper documents.** A key improvement lies in the **signature verification** process, where DCE-enrolled beneficiaries bypass traditional review requirements, creating significant time and resource savings.

The financial impact of this digital transformation is evident in the **reduction of overtime expenses**. Prior to the DCE implementation, UNJSPF processed **more than 60,000 paper certifications annually,** each requiring manual handling for opening, scanning, Enterprise Resource Planning (ERP) system integration, and archiving storage. In terms of the reduction of overtime expenditures through the DCE solution, the UNSPF was able to lower costs through process automation. An analysis after four-year data since the solution went operational, led to quantifying significant savings through **lowering overtime expenditures by 76.5% between 2021 to 2024.**

The most significant improvement occurred in the initial transition period, where overtime expenses during the peak months of June through August dropped by 58.8% between 2021 and 2022. 2024 marked the lowest recorded **overtime expenditure—representing less than a quarter (23.5%) of the 2021 baseline.** The cumulative impact demonstrates that the systematic process automation through the **DCE solution leads to sustained operational savings.** It is expected that the savings become even more significant as new beneficiaries now choose DCE over the traditional CE almost as default option.

Processing savings

The DCE has yielded significant results in 2025, with **digital issuance reaching over 38,800 certificates** — a remarkable achievement in paperless operations. This digitization initiative has effectively **reduced paper certificate printing to 36,852** in 2024, down from 64,443 paper certificate printing in 2020, the year before the DCE solution was implemented. This is marking an **unprecedented reduction in printing levels**, while at the same time, the number of **beneficiaries increased from approximately 65,000 to over 70,000.**

This strategic shift toward digital processing represents a dual victory: **enhancing service delivery** while advancing **environmental sustainability goals.** The substantial adoption of DCE by over 43,000 beneficiaries demonstrates **strong acceptance of digital public infrastructure** solutions, while **streamlining administrative processes.**

The transition has generated **measurable cost efficiencies** through reduced paper form procurement and decreased mailing expenses. More importantly, it has **improved service delivery** by eliminating manual printing requirements for enrolled beneficiaries, creating a more responsive and efficient system, providing **tangible benefits for UNJSPF beneficiaries** while supporting environmental sustainability objectives.

Archiving expenditures

The transition from paper-based to digital processing has significantly transformed document management practices, resulting in tangible cost efficiencies. Over a five-year period, **archiving expenditures decreased by more than 95%,** marking a decisive shift in operational efficiency.

This reduction stems from two key innovations implemented during the COVID-19 pandemic. First, the introduction of email-based communication and a **self-service portal** for beneficiaries fundamentally changed how documents are submitted and processed. Second, and more importantly, the implementation of the **DCE solution** transformed the certification process, **eliminating the need for over 70,000 pieces** of annual paper correspondence.

After implementation, **each subsequent year saw archiving costs drop by roughly half or more** compared to the previous year, with the most dramatic decrease occurring between 2020 and 2021, when expenditures fell by 61%. This downward trend continued steadily, with costs declining by 76% between 2021 and 2022, followed by further reductions of 29% and 24% in subsequent years.

Most notably, beneficiaries who complete their DCE verification before the first mailing cycle are now **automatically considered compliant with Proof-of-Life requirements,** eliminating the need for paper documentation entirely. This streamlined approach not only reduces costs but also enhances user experience and environmental sustainability.

The transformation demonstrates how digital innovation can drive operational efficiency while improving service delivery.

Signature verification cost

The DCE solution has **completely reorganized the signature verification workflows,** marking a significant shift in operational process efficiency. At the core of this evolution lies the **Automatic Signature Verification system.**

The UNJSPF's commitment to implementing blockchain-based verification protocols, prompted by internal audit recommendations, has strengthened the case for digital transformation even further. Even as the **verification scope expanded** to encompass all beneficiaries, the DCE solution has proven remarkably scalable. The system is able to processes verification requests for the beneficiary base exceeding 70,000 beneficiaries with **minimal additional resource investment.**

The impact on cases still requiring attention—those involving thumbprints or requiring additional documentation—has been particularly noteworthy. What once consumed hours of staff time now **requires just a fraction**, with digital workflows reducing processing. This transformation showcases how **digital solutions can scale services** while optimizing resource utilization.

Fraud prevention

Digital identity verification represents a significant advancement in securing benefit distribution systems. The implementation of AI-based **biometric authentication** has markedly **enhanced security protocols**, offering substantially **more protection against fraud and overpayments** compared to traditional signature-based systems. This technological shift addresses one of the most persistent vulnerabilities in benefit distribution: identity verification.

The DCE solution provides a robust, **multi-layered verification process.** Beneficiaries undergo an initial enrolment phase, followed by a direct video consultation with a Digital CE agent who assesses their eligibility against predetermined criteria. Upon approval, the system creates a **secure biometric profile** that serves as the benchmark for all future transactions. This digital transformation has proven more effective and reliable than its paper-based predecessor, significantly reducing the potential for fraudulent claims.

The solution's security framework extends beyond basic biometric authentication. By requiring **precise location data** during DCE issuance, the system maintains strict **oversight of residency requirements**—a critical component of the two-track system.

The personal nature of biometric data ensures that only authorized beneficiaries can access the system, **effectively preventing unauthorized usage** and **fraudulent benefit claims.**

Path Forward for DCE

The **Digital Certificate of Entitlement (DCE)** represents a pioneering example of **process and service innovation,** for the benefit of the whole UN system and other UNJSPF member organizations, offering a transformative approach to digital credentialing.

A multi-agency consortium is envisioned to position DCE as a digital public good. The strategic path forward is to offer **DCE-as-a-Service** to other international organizations, allowing them to benefit from a proven, cost-effective, and interoperable solution.

The DCE Consortium Initiative is in line with the **UN Digital Compact**, which advocates for enhanced **digital cooperation, and shared governance mechanisms**. Additionally, it supports the **Pact for the Future** by reinforcing **collective action, inclusivity, and digital trust** in global governance frameworks.

It is intended to offer DCE as a ready-to-use solution over a Software-as-a-Service model. The consortium will operationalize the service delivery model and define cost-sharing mechanisms by fostering shared ownership and collaboration among international organizations.

The **DCE consortium** model—established by agreement among founding members—will adhere to the following key pillars to ensure equitable collaboration, sustainability, and innovation:

- **UN Shared Service:** aligned with the **UN Mutual Recognition Declaration**, the digital service could leverage economies of scale while fostering cooperation among UN and Multilateral Development Banks.

- **Cost recovery and sharing:** the consortium will operate on a **full cost recovery and sharing model**, ensuring that ongoing maintenance and upgrade fees are distributed equitably among all partners.

- **Governance framework and onboarding:** a comprehensive governance framework will define rules of engagement, operational models with service level agreements, and the roles and responsibilities of participating entities. Clear terms and conditions will guide the onboarding of new members.

- **Steering group for joint decision-making:** consortium members will actively participate in strategic decisions, including the development of new capabilities and functionalities to advance the solution.

- **Evolution and innovation:** the consortium will remain committed to continuous improvement by monitoring technology trends, exploring innovative approaches, and enhancing the solution's functionality, security, and usability

These key pillars will ensure that the DCE remains at the **forefront of technological advancements** and will meet the evolving needs of stakeholders.

DCE Consortium principles

The following overarching principles will guide its structure and operation:

- **Equitable contribution and scalability:** contributions will be based on usage or capacity, ensuring fairness in cost allocation. Larger entities will contribute proportionally more, while smaller users will pay less.

- **Flexibility and transparency:** clear, transparent guidelines will communicate cost calculations, promoting trust and accountability among members. The framework will accommodate changes in individual needs and capabilities.

- **Sustainability:** the model will prioritize long-term sustainability by ensuring that costs are adequately covered to support ongoing maintenance, upgrades, and innovation of the shared digital product.

- **Governance oversight:** robust governance mechanisms will oversee the cost-sharing framework, ensuring adherence to agreed principles. Continuous improvement efforts will optimize cost efficiencies and enhance the value proposition for all participating entities.

Operating model of the Consortium

UNICC will serve as a trusted IT partner to implement the configuration and integrations with the partner organization's back-end systems (e.g., ERP).

The DCE Consortium's **operating model** will consist of two primary components, designed to **ensure both scalability and sustainability** of the DCE solution: one-time onboarding costs: consisting of costs for the full configuration of the DCE; an onboarding nominal fee; and recurring operational support costs.

The Way Forward

Sameer Chauhan
Director
UNICC

The collaboration between UNICC and UNJSPF to develop a blockchain-based digital identity solution marks a meaningful milestone in the digital journey of the United Nations system. Beyond its technological innovation, this initiative illustrates the transformative power of inter-agency collaboration anchored in shared values: trust, efficiency, and service to beneficiaries.

The project has provided not only a technical prototype but also an operational model for how organizations across the UN family can collaborate to design secure, scalable, and inclusive digital public infrastructure. From ideation to deployment, this solution has demonstrated how emerging technologies such as blockchain and decentralized identity can be applied pragmatically to address real-world challenges, increasing transparency and strengthening digital trust.

As the UN's strategic digital partner, UNICC played a pivotal role in architecting, securing, and implementing this solution. The project leveraged our in-house blockchain expertise, cybersecurity services, and cloud infrastructure to ensure compliance with the highest standards of interoperability and data protection. It also reflects our growing portfolio of digital public goods, built with a modular, reusable design that supports adaptation and scale across regions and mandates.

Our experience here underscores a broader lesson: the success of digital identity systems and other DPI solutions hinges not only on technical sophistication, but on governance, interoperability, and partnership. Through this collaboration, we have learned how digital infrastructure can be co-created with agility, how lessons can be transferred across agencies, and how innovation—when rooted in purpose—can unlock value for the entire UN family.

Looking forward, the implications are far-reaching. This initiative opens the door to broader applications of secure digital identity within the UN system and beyond. From facilitating user authentication in service delivery platforms to enabling interoperable credentials and secure data exchange, the foundational principles tested here can inform a wide range of future use cases. This initiative is a foundation on which further UN-wide digital solutions can be built, adapted, and scaled with confidence.

At UNICC, our strategic vision for 2030 is to serve as the UN's digital backbone, providing common, cybersecure digital foundations that empower UN organizations to deliver on their mandates. Whether through blockchain, AI, cloud, or cybersecurity, our mission is to equip partners with responsive and reliable technology that strengthens multilateral outcomes and supports our partners' digital transformation and future.

The spirit of this project aligns fully with the ambitions of UN 2.0 and our shared commitment to innovation, inclusion, and impact. It is a tangible example of how we can reimagine service delivery across the UN ecosystem— not as isolated efforts but as collective, future-ready systems.

As we move forward, this collaboration offers a model for how the UN system can jointly design and deploy impactful digital solutions. By combining technical expertise with a shared purpose, we can continue to build secure, inclusive, and trusted digital infrastructure. The road ahead is digital, collaborative, and driven by a common mission. And together, as one UN, we are well on our way.

UNJSPF

United Nations Joint Staff Pension Fund

1 Dag Hammarskjöld Plaza (DHP)
885 Second Avenue
New York, NY 10017, USA

www.unjspf.org

UNICC

United Nations International Computing Centre

Palais des Nations
1211 Geneva 10
Switzerland

www.unicc.org